Administration Documentation for Cisco Unified MeetingPlace Release 7.1
PART

Quick Start Configuration

- Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing
- Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing
Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing

Release 7.1
Revised: April 3, 2011 8:30 pm

This module describes how to quickly configure your Cisco Unified MeetingPlace system for basic voice and video conferencing. Advanced configuration instructions are available in the other topics in this guide.

- Configuring Basic Voice & Video Conferencing, page 1
- Verifying Basic Voice and Video Conferencing Using the Telephone User Interface, page 2
- Verifying Basic Voice and Video Conferencing Using the End-User Web Interface, page 4

Configuring Basic Voice & Video Conferencing

Before You Begin

- Install the Application Server and Media Server
- Configure the Media Server

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>High-Level Task</th>
<th>Where to Find Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
<td>Logging In to the Cisco Unified MeetingPlace Administration Center module</td>
</tr>
<tr>
<td>Step 2</td>
<td>Change the default passwords for the admin profile.</td>
<td>Changing System Administrator Passwords for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Step 3</td>
<td>Install licenses.</td>
<td>Installing and Managing Licenses for Cisco Unified MeetingPlace module</td>
</tr>
</tbody>
</table>
### Verifying Basic Voice and Video Conferencing Using the Telephone User Interface

Use this procedure to verify the basic configuration for voice and video conferencing, e-mail notifications, and dial-out calls.

<table>
<thead>
<tr>
<th>High-Level Task</th>
<th>Where to Find Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 4</strong></td>
<td>Configure the Audio Settings, Video Settings, and Global Settings on the Meeting Configuration Page. Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace. Configuring Meetings and Ports in the Configuring Meetings for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>(Optional) Connect to an external SMTP server for e-mail notifications. Configuring the SMTP Servers in the Configuring E-Mail Notifications for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>(Optional) Enable dial-out privileges for profiled users by setting the Can dial out (does not apply to Cisco WebEx meetings) field to Yes for the System user group. Enabling Dial-Out Privileges for Users in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module.</td>
</tr>
</tbody>
</table>
| **Step 7**      | Add user profiles. Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module:  
  - Methods for Adding User Profiles  
  - Adding User Profiles Manually  
  or  
  At a minimum, manually add a test user profile. To test e-mail notifications, the user profile requires a valid e-mail address whose messages you can access. |
| **Step 8**      | Configure video privileges through the Video usage user profile field. Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module:  
  - Adding or Editing a User Group Manually  
  - Editing a User Profile  
  or  
  Add or edit a user profile. For example, add or edit a test user profile to test e-mail notifications. To test e-mail notifications, the user profile requires a valid e-mail address whose messages you can access. |
| **Step 9**      | Configure the access phone numbers that users call to attend meetings. Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace module. |
| **Step 10**     | (Optional) Configure video terminal profiles. Adding or Editing a Video Terminal Profile in the Configuring Endpoints for Cisco Unified MeetingPlace module. |
| **Step 11**     | Connect to the call-control device that routes calls to Cisco Unified MeetingPlace. Configuring Call Control for Cisco Unified MeetingPlace module. |

**What to Do Next**
- If you already installed and configured a Cisco Unified MeetingPlace Web Server, then proceed to the “Verifying Basic Voice and Video Conferencing Using the End-User Web Interface” section on page 4.
- Otherwise, proceed to the “Verifying Basic Voice and Video Conferencing Using the Telephone User Interface” section on page 2.
Tip

If you already set up and configured your Web Server, then you may instead go to the “Verifying Basic Voice and Video Conferencing Using the End-User Web Interface” section on page 4.

Before You Begin

Complete the “Configuring Basic Voice & Video Conferencing” section on page 1.

Procedure

Step 1
Log in to the Administration Center.

Step 2
Configure one user profile to enable the scheduling of video meetings:
   a. Select User Configuration > User Profiles.
   b. Find the user profile that you want to modify.
   c. Select Edit in the same row as that user profile.
   d. In the Video usage field, select Can attend + host video meetings + reserve video ports.
   e. Select Save.

Step 3
Call Cisco Unified MeetingPlace using one of the access phone numbers on the Usage Configuration Page.

Step 4
Press 3# to log in as the user whose profile you modified in Step 2.

Step 5
Follow the voice prompts to enter the Profile number and Profile password, and to record a user name.

Note
To test that e-mail notifications work, the user profile must include a valid e-mail address whose messages you can access.

Step 6
Press 22 to schedule a meeting.

Step 7
Follow the voice prompts to schedule a test meeting using these parameters:
   • Time: 5 minutes in the future
   • Duration: 30 minutes
   • Number of locations: 4

Step 8
Write down the test meeting ID number when stated by the voice prompts.

Step 9
Hang up.

Step 10
Verify that the user receives an e-mail notification about the test meeting.

Step 11
Verify that you can dial in to the voice meeting:
   a. Call the access phone number in the e-mail notification.
   b. Enter the test meeting ID and press #.
   c. If prompted, record your name.
   d. If you are using a video endpoint, then you will see your own video reflected back to you. For example, on Cisco Unified Video Advantage, the local and remote windows will display the same video.
   e. From other phones or video endpoints, call into the same test meeting.
Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing

Verifying Basic Voice and Video Conferencing Using the End-User Web Interface

f. If you have multiple video endpoints in the meeting, then verify that the video participants can see each other.

Step 12 Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.

Step 13 Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.

Note If you want to enable dial-out privileges for guest users, then edit the guest user profile.

Step 14 Set Can dial out (does not apply to Cisco WebEx meetings) to Yes.

Step 15 Verify that you can dial out from the voice meeting:
   a. While in the voice meeting, press #3 to dial out to another phone or video endpoint.
   b. Follow the voice prompts to connect the other phone or video endpoint to the meeting.
   c. If you have multiple video endpoints in the meeting, then verify that the video participants can see each other.

Step 16 Hang up all phones and video endpoints.

Troubleshooting Tips
If the dial-out call fails:

• Make sure that the phone line is not in use when the system tries to call you.

• Make sure that you can successfully call the dialed-out number from another phone.

• Make sure that the phone number you enter uses the same format that you would use to dial the phone number from an office phone. For example, if you only need to dial the last four digits to reach other office phones, then enter only four digits for an office phone. Similarly, if you enter your personal cell phone number, then you might need to include a 9 and the complete telephone number with area code.

• For additional troubleshooting help, see these modules:
   – Troubleshooting Telephone Issues for Cisco Unified MeetingPlace
   – Troubleshooting Video Issues for Cisco Unified MeetingPlace
   – Troubleshooting User Access Issues for Cisco Unified MeetingPlace

What to Do Next
To enable web conferencing, proceed to the Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module.

Verifying Basic Voice and Video Conferencing Using the End-User Web Interface

Use this procedure to verify the basic configuration for voice and video conferencing, e-mail notifications, and dial-out calls.
Tip
If you do not have a configured Web Server, then instead go to the “Verifying Basic Voice and Video Conferencing Using the Telephone User Interface” section on page 2.

Before You Begin
Complete these tasks:

- Configuring Basic Voice & Video Conferencing, page 1
- Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module

Procedure

Step 1
Log in to the Administration Center.

Step 2
Configure one user profile to enable the scheduling of video meetings:

d. Select User Configuration > User Profiles.

e. Find the user profile that you want to modify.

f. Select Edit in the same row as that user profile.

g. In the Video usage field, select Can attend + host video meetings + reserve video ports.

h. Select Save.

Step 3
Sign in to the end-user web interface as the user whose profile you modified in Step 2:

- Enter the User ID and User password from the Cisco Unified MeetingPlace user profile.
- If you configured Directory Service, then enter the username and password from the external directory.

Note
To test that e-mail notifications work, the user profile must include a valid e-mail address whose messages you can access.

Step 4
Select Schedule Meeting to set up a test meeting using these parameters:

- Time: 5 minutes in the future
- Duration: 30 minutes
- Number of Participants: 4

Step 5
Select Schedule.

Step 6
Verify that the user receives an e-mail notification about the test meeting.

Step 7
Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.

Step 8
Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.

Note
If you want to enable dial-out privileges for guest users, then edit the guest user profile.

Step 9
Set Can dial out (does not apply to Cisco WebEx meetings) to Yes.
Verifying Basic Voice and Video Conferencing Using the End-User Web Interface

Step 10 Verify that you can dial in to the meeting:
   a. Call the access phone number in the e-mail notification.
   b. Enter the test meeting ID and press #.
   c. If prompted, record your name.
   d. If you are using a video endpoint, then you will see your own video reflected back to you.
      For example, on Cisco Unified Video Advantage, the local and remote windows will display the
      same video.
   e. From other phones or video endpoints, call into the same test meeting.
   f. If you have multiple video endpoints in the meeting, then verify that the video participants can see
      each other.

Step 11 Verify that the system can dial out to you:
   a. Select the URL in the e-mail notification.
   b. If prompted, enter the User ID and User password.
   c. Check to have the system call you.
   d. Enter a phone number.
   e. Select Connect.
   f. Verify that the system calls that phone or video endpoint and connects it to the voice meeting.

Step 12 Hang up all phones and video endpoints.

Troubleshooting Tips
If the dial-out call fails:
   • The web meeting room may display a pop-up message with helpful information.
   • Make sure that the phone line is not in use when the system tries to call you.
   • Make sure that you can successfully call the dialed-out number from another phone.
   • Make sure that the phone number you enter uses the same format that you would use to dial the
     phone number from an office phone. For example, if you only need to dial the last four digits to reach
     other office phones, then enter only four digits for an office phone. Similarly, if you enter your
     personal cell phone number, then you might need to include a 9 and the complete telephone number
     with area code.
   • For additional troubleshooting help, see these modules:
     – Troubleshooting Telephone Issues for Cisco Unified MeetingPlace
     – Troubleshooting Video Issues for Cisco Unified MeetingPlace
     – Troubleshooting User Access Issues for Cisco Unified MeetingPlace
Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing

About Web Conferencing Configuration

- Configuration Restrictions, page 1
- Cisco Policy for Use of Third-Party Software, page 2
- Proxy Servers, page 2

Configuration Restrictions

Cisco Unified MeetingPlace Web Conferencing deployments that are customized beyond the built-in configuration capabilities of the product, or beyond the documented configuration settings, procedures, or instructions, are not supported by Cisco Systems.

Examples of such customizations include, but are not limited to, the following: modifying web page templates, changing HTML or Javascript code, changing IIS running parameters or applying custom ASP pages or ISAPI filters, modifying SQL server configuration or authentication method, and modifying Windows OS security through IPSec policies and NTFS ACL.
Cisco Policy for Use of Third-Party Software

The Cisco Unified MeetingPlace Web Conferencing documentation describes the system, end user, and other requirements for the use of the Web Conferencing software. Failure to meet these requirements or the introduction of unsupported third-party products may interfere with the operation of the Web Conferencing software, and may affect Cisco support for the Web Conferencing product.

Proxy Servers

Cisco Unified MeetingPlace Web Conferencing supports most proxy servers on the market. If you are accessing it through a proxy server, set the proxy server as follows:

- Timeout value from 120 seconds to 300 seconds.
- Cache expiration policy set to “Explicit Expiration Information Only.”

Related Topics
- Configuring a Web Server Behind a Proxy, page 5

Roadmap for Configuring Basic Web Conferencing

Before You Begin

- Set up your system for voice and video meetings. See the Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing module.
- Make sure that you have already installed the web-conferencing licenses on the Cisco Unified MeetingPlace Application Server.

Procedure

<table>
<thead>
<tr>
<th>High-Level Task</th>
<th>Where to Find Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Sign in to the Cisco Unified MeetingPlace Web Administration page.</td>
<td>Using the Cisco Unified MeetingPlace Web Administration Page, page 3</td>
</tr>
<tr>
<td><strong>Step 2</strong> (Optional) Change the format of the Web Server hostname from an IP address to a hostname.</td>
<td>Changing the Web Server Hostname From an IP Address to a Hostname in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module</td>
</tr>
<tr>
<td><strong>Step 3</strong> Set your Web Server options.</td>
<td>Setting Your Web Server Options, page 3</td>
</tr>
<tr>
<td><strong>Step 4</strong> Configure the click-to-attend links through the Cisco Unified MeetingPlace Administration Center.</td>
<td>Configuring Click-to-Attend Links in the Configuring E-Mail Notifications for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td><strong>Step 5</strong> (Optional) Configure the Web Server if it is behind a proxy and will require connection to the Cisco WebEx meeting room.</td>
<td>Configuring a Web Server Behind a Proxy, page 5</td>
</tr>
<tr>
<td><strong>Step 6</strong> (Optional) Configure a site of multiple Web Servers.</td>
<td>Configuring a Site, page 5</td>
</tr>
</tbody>
</table>
Using the Cisco Unified MeetingPlace Web Administration Page

The Cisco Unified MeetingPlace Web Administration page allows you to complete various configuration and maintenance tasks through a convenient graphic user interface.

Note
When navigating within the Web Administration pages, do not use the Back button on your web browser to go to a previous page. Use the links available in the user interface instead.

Before You Begin
You must have a Cisco Unified MeetingPlace profile with System Manager privileges to access this and all subsequent web administration pages.

Procedure

Step 1 Sign in to the end-user web interface by using your System Manager-level profile.
Step 2 Select Admin.
Step 3 Select an option on the Administration page to begin configuration.

Setting Your Web Server Options

From the Web Server administration page, you can configure features and functionality for local Web Servers. This includes enabling Secure Sockets Layer (SSL), Web Server Authentication, and configuring denial-of-service handling, which provides for better performance at the capacity threshold of the server.

The customizations you select on the local Web Server override functionality that is normally allowed by individual class-of-service or meeting console permissions.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Web Server.
Step 4 Scroll down to the “View” section of the screen.
Step 5 Select the name of the Web Server that you want to configure.
This populates the “Edit” section of the screen with predefined settings.
Step 6 Configure the following parameters in the “Web Server Specific” section.
Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing

Setting Your Web Server Options

Note

The Web Server hostname was populated during the Cisco Unified MeetingPlace Web Conferencing installation. The Hostname [Home Page] was assigned the first IP address in the Operating System. The Hostname [Web Conferencing] was assigned the second IP address in the Operating System. You should not need to redefine these unless you want users to be able to access the Web Server by using the fully qualified domain name (FQDN) of the server or you plan to configure SSL for this server. If enabling SSL, you must use hostnames rather than IP addresses.

- Require SSL
- Trust Web Server Authentication
- Max Concurrent Web Conference Users
- Performance Tuning
- Verbose Logging

Step 7

Configure the “Web Server Customization Values” section.

- Select Yes to enable a feature.
- Select No to disable a feature.
- Select (Site Default) to synchronize the feature on this Web Server with that already configured for the site.

Note

You can configure site information on the Site administration page.

Step 8

Select Submit.

Related Topics

- Changing the Web Server Hostname From an IP Address to a Hostname in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module
- Field Reference: Web Server Specific Fields in the Web Administration References for Cisco Unified MeetingPlace module
- Field Reference: Web Server Customization Values in the Web Administration References for Cisco Unified MeetingPlace module
- Configuring a Site, page 5
- Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing module
- Configuring Shared Storage in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module
- How to Configure Secure Sockets Layer in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module
- Configuring External Access to Cisco Unified MeetingPlace Web Conferencing module
Configuring a Web Server Behind a Proxy

Complete this procedure if you are configuring a Cisco Unified MeetingPlace Web Server behind a proxy and plan to connect to the Cisco WebEx meeting room.

Procedure

Step 1 Open an Internet Explorer browser window.
Step 2 Select Tools > Internet Options > Connections.
Step 3 Select LAN Settings.
Step 4 Check Use a Proxy server for your LAN.
Step 5 Check Bypass proxy server for local addresses.
Step 6 Select Advanced.
Step 7 Enter your proxy information and exceptions for local connections.
Step 8 Select OK.

Related Topics
- Proxy Servers, page 2

Configuring a Site

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Site.
Step 4 From the “View” section of the page, select the name of the site you want to configure.
   Information about this site populates the “Edit” section of the page.
Step 5 Select field options to configure the site.
   The Site Name entry on the Site administration page must match the Web Server Name entry on the Web Server administration page. This must be consistent for each site. If these entries do not match, searches will not display the same site name.
   The “Warn before Rolling onto Site” field is part of the WebConnect feature and is not supported in this release.
Step 6 Select Yes for all parameters in the Site Customization Default Values section.
   Choosing Yes synchronizes all of the Web Servers in this site to share the same parameters.
Step 7 Select Submit.
Step 8  Repeat Step 4 through Step 7 for each remaining site listed in the “View” section of the Site administration page.

Troubleshooting Tips
To delete a site from your image, select it and select **Delete**. You can only delete external sites from an image.

Related Topics
- Field Reference: Site Configuration Page in the Web Administration References for Cisco Unified MeetingPlace module
Basic System Configuration

- Logging In to the Cisco Unified MeetingPlace Administration Center
- Installing and Managing Licenses for Cisco Unified MeetingPlace
- Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace
- Configuring Languages for Cisco Unified MeetingPlace
- Configuring Meetings for Cisco Unified MeetingPlace
- Configuring E-Mail Notifications for Cisco Unified MeetingPlace
- Configuring Recordings for Cisco Unified MeetingPlace
- Configuring Attendant Settings for Cisco Unified MeetingPlace
Logging In to the Cisco Unified MeetingPlace Administration Center

Restrictions for Logging In to the Administration Center

- Only users of type System administrator or Attendant can log in to the Administration Center.
- If you configured Directory Service on your system, then the Administration Center can be accessed only by users who are authenticated locally by the Cisco Unified MeetingPlace database. Specifically, the isLocalUser setting in the user profile must be set to Yes. This prevents unauthorized access even if external directory passwords are compromised.

Related Topics
- About User Types in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Cisco Unified MeetingPlace Directory Service module

Logging In to the Administration Center For the First Time

Procedure

Step 1 Go to http://application-server/admin/.
Step 2 Enter the username you configured during the installation procedure.
Step 3 Enter the password you configured during the installation procedure. The password is case-sensitive.
Step 4 Select Log In.
Related Topics

- Recovering the User Password for the admin Profile, page 3

What to Do Next

Proceed to “Changing the Passwords for the admin Profile” in the Changing System Administrator Passwords for Cisco Unified MeetingPlace module.
Installing and Managing Licenses for Cisco Unified MeetingPlace

Restrictions for Licenses

- By default, every Cisco Unified MeetingPlace system comes with six trial voice licenses, six trial web licenses, and six trial video licenses. If you do not purchase additional licenses, the six trial web licenses expire after 60 days.
- Depending on your system configuration, you may not be able to take advantage of all the licenses you purchase. The Cisco Unified MeetingPlace system lets you purchase more licenses than your current system capacity.
- The system does not consider the expiration date of a license when users schedule meetings; instead, the system checks and enforces the expiration date when users join meetings. The system displays a message if a license is about to expire.

Related Topics
- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace

How to Install and Manage Licenses

If you purchase license SKUs with your Cisco Unified MeetingPlace order, then your order comes with a Product Authorization Key (PAK). You obtain a license file by providing the PAK and the MAC address of your server in a form on Cisco.com. Through the Administration Center, you upload the license file to Cisco Unified MeetingPlace to install all purchased licenses in that order.
How to Install and Manage Licenses

Note
The new licenses take effect immediately. You do not need to reinstall or restart the Cisco Unified MeetingPlace operating system and application when you add licenses.

- Determining the MAC Address of your System, page 2
- Obtaining the License File, page 2
- Installing the License File, page 3
- Displaying Licenses, page 4
- Downloading Licenses, page 4

Determining the MAC Address of your System

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Licenses > Install Licenses.

The MAC address is listed in the Host ID (MAC address) field.

Related Topics
- Install Licenses Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Obtaining the License File

The license file contains all the purchased licenses in your order.

Before You Begin
- Find the Product Authorization Key (PAK) that came with your order.
- Complete the “Determining the MAC Address of your System” section on page 2.

Procedure

Step 1 Go to http://www.cisco.com/go/license.
Step 2 If prompted, log in with your Cisco.com user ID and password.
Step 3 Enter the PAK from your Cisco Unified MeetingPlace order.
Step 4 Confirm the order information and select Continue.
Step 5 Fill out all the required fields on the registration form. In particular:
  - Make sure that your e-mail address is correct, because the license file will be e-mailed to you.
  - Enter the MAC address of your Cisco Unified MeetingPlace server.
Installing and Managing Licenses for Cisco Unified MeetingPlace

How to Install and Manage Licenses

Step 6  Select Submit.
Cisco Systems sends you an e-mail containing the license file.

Step 7  Save the license file to a location where you can access it from the Administration Center.

Related Topics
• Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace

Installing the License File

Before You Begin
Complete the “Obtaining the License File” section on page 2.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Maintenance > Licenses > Install Licenses.
Step 3  Select one of the following radio buttons:
• Upload new license file—Choose this option to delete all previously installed licenses before installing the license file. Select this option only when uploading licenses to your system for the first time, or in the unlikely event that you must install an entirely new set of licenses.
• Append incremental license file—Choose this option to keep all the previously installed licenses and to add additional licenses from the license file.
Step 4  Enter the fully-qualified filename in the License file to use field or select Browse to search for the file.
Step 5  Select Install License.

Troubleshooting Tips
If the Application Server hostname is longer than 32 characters, you may not be able to install licenses. If this occurs, use the net command to change the hostname. Note, however, that changing the Application Server hostname requires a system restart and may require other configuration tasks. See the net command description in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module.

Related Topics
• Install Licenses Page in the Administration Center Page References for Cisco Unified MeetingPlace module
• Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace

What to Do Next
Proceed to the “Displaying Licenses” section on page 4 to verify license installation.
Displaying Licenses

Complete this task to display the number and types of licenses that are installed on your system, which licenses are enabled, and any further license limitations that are specific to your system.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Licenses > Licenses Summary.

Related Topics
- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace
- Licenses Summary Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Downloading Licenses

Use this task to back up your license files.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Licenses > Licenses Summary or Install Licenses.
Step 3 Select Download License.
Step 4 In the File Download dialog box, select Save.
Step 5 Navigate to the directory where you want to save the exported file.
Step 6 Select Save.
Step 7 If the Download Complete dialog box appears, select Close.

Related Topics
- Displaying Licenses, page 4
- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace
- Install Licenses Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Restrictions for Access Phone Numbers and Notification Labels

The telephone pop-up notification box in the full web meeting room can display only a limited number of characters. Because this limitation applies to all characters, including the meeting ID, HTML tags, spaces, and punctuation, the number of label characters that get displayed may vary for each meeting.

We recommend that you minimize the number of characters entered in the label fields to avoid the character limitation. If you exceed the maximum number of characters, the information displayed in the telephone pop-up notification box is automatically modified in the following ways, in the presented order, until the number of characters falls below the maximum:

1. The headings in the pop-up notification box are deleted, for example “Dial in from your phone.”
2. Bold characters are changed to normal characters.
3. The text in the Label for access phone number 3 field is changed to “Or: ”.
4. The text in the Label for access phone number 4 field is changed to “Or: ”.

To verify that the phone numbers and labels correctly appear in the telephone pop-up notification box in the full web meeting room, take the following actions:

1. Schedule a web and voice meeting using a 17-digit meeting ID (maximum allowed characters).
2. Join the full web meeting.
3. In the top right corner of the full web meeting room, roll your mouse pointer over the telephone icon to display the pop-up notification box content.

If you are not satisfied with the appearance of the meeting phone numbers and notification labels, reduce the number of characters in the notification labels.
Related Topics
- Configuring E-Mail Notifications for Cisco Unified MeetingPlace, page 1

Configuring Access Phone Numbers and Notification Labels

You can configure up to four phone numbers and descriptive labels for users to dial in to Cisco Unified MeetingPlace. These phone numbers and labels appear in the following places:

- E-mail notifications
- End-user web interface
- Telephone pop-up notification box in the full web meeting room
- Cisco Unified IP Phone screens (only when subscribed to Cisco Unified MeetingPlace PhoneView)

Before You Begin
- This task requires a system restart, which terminates all existing call connections. Proceed only during a scheduled maintenance period or during a period of extremely low usage.

Note  When you restart the Web Server, all manual changes made to the registry are lost.
- Read the “Restrictions for Access Phone Numbers and Notification Labels” section on page 1.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select System Configuration > Usage Configuration.
Step 3  Configure the following fields:
- Label for access phone number 1
- Access phone number 1
- Label for access phone number 2
- Access phone number 2
- Label for access phone number 3
- Access phone number 3
- Label for access phone number 4
- Access phone number 4
Step 4  Select Save.
Step 5  Restart the system by entering sudo mpx_sys restart in the CLI.

Related Topics
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace module

**What To Do Next**

Configure your call-control device to route calls to Cisco Unified MeetingPlace. See the Configuring Call Control for Cisco Unified MeetingPlace module.
Configuring Languages for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:30 pm

Cisco Unified MeetingPlace supports a growing number of languages available for voice prompts, e-mail notifications, the end-user web interface, and web meeting rooms.

Note
To see which languages are supported, see the Release Notes for Cisco Unified MeetingPlace at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_release_notes_list.html.

- Language Restrictions, page 1
- Configuring Languages Other Than U.S. English, page 1
- Enabling Installed Languages, page 2
- Specifying Languages for Users, page 3

Language Restrictions

- The administrative user interfaces use only U.S. English text.
- Only U.S. English is supported on the system when Cisco Unified MeetingPlace is integrated with Cisco WebEx.

Related Topics
- Integrating Cisco Unified MeetingPlace with Cisco WebEx module

Configuring Languages Other Than U.S. English

By default, all voice prompts, e-mail notifications, end-user web interfaces, and web meeting rooms use U.S. English. To use a different language or to enable end users to choose from multiple languages, complete these high-level tasks.

Before You Begin
Read the “Language Restrictions” section on page 1.
Enabling Installed Languages

Before You Begin

- Purchase, download, and install the languages license. See the “How to Install and Manage Licenses” section on page 1.
- This task may require a system restart, which terminates all existing call connections. Proceed only during a scheduled maintenance period or during a period of extremely low usage.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Usage Configuration.
Step 3 Configure the Language fields to enable one or more installed languages.
Step 4 Select Save.
Step 5 Restart the system by entering sudo mpx_sys restart in the CLI.

Note You do not need to restart the system if you are only switching the order in which the languages appear in these fields.

Procedure

<table>
<thead>
<tr>
<th>High-Level Task</th>
<th>Where to Find Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> (For multiple languages only) Purchase, download, and install the languages license. Without the languages license, you can only enable one language on the system. With the installed languages license, you can enable up to four languages on Cisco Unified MeetingPlace.</td>
<td>How to Install and Manage Licenses, page 1</td>
</tr>
<tr>
<td><strong>Step 2</strong> Enable the languages.</td>
<td>Enabling Installed Languages, page 2</td>
</tr>
<tr>
<td><strong>Step 3</strong> (For multiple languages only) Configure language preferences in the user groups or user profiles. <strong>Note</strong> End users may override this setting by selecting a language through the end-user web interface or over the phone. See the User Guide for Cisco Unified MeetingPlace at <a href="http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_user_guide_list.html">http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_user_guide_list.html</a>.</td>
<td>Specifying Languages for Users, page 3</td>
</tr>
<tr>
<td><strong>Step 4</strong> (For the Cisco Unified MeetingPlace PhoneView only) Install and configure matching languages in Cisco Unified Communications Manager for the Cisco Unified IP Phones.</td>
<td>Integrating Cisco Unified MeetingPlace With Cisco Unified IP Phone module</td>
</tr>
</tbody>
</table>
Specifying Languages for Users

The language setting in each user group or user profile affects the following items:

- Language used in e-mail notifications received by the user.
- Language used after logging in to the end-user web interface, from which users schedule, find, and attend meetings.
- Voice prompt language heard by the user after successful authentication.
  During active meetings, however, voice prompts heard by all meeting participants use the meeting language. If the meeting scheduler does not specify the meeting language, then the Language configured in the user profile of the meeting owner becomes the meeting language.
- Default language used in the web meeting room for meetings that are scheduled by the user.
  All meeting participants see the same language used in the web meeting room. By default, scheduled meetings use the language in the user profile of the meeting owner, but a different language may be selected while scheduling the meeting.
- Language used in reservationless meetings that are set up by the user.
  All reservationless meeting participants see the web meeting room in the language specified in the user profile of the meeting owner. Users cannot select a different language.
- Format in which the date appears in the end-user web interface.
- Language that appears on the Cisco Unified IP Phone screen when subscribed to the Cisco Unified MeetingPlace PhoneView.

Before You Begin
Enable the languages. See the “Enabling Installed Languages” section on page 2.

Restriction

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration.
Step 3 To configure a user group, select User Groups. To configure an individual user profile, select User Profiles.
Step 4 To configure an existing user group or user profile, select Edit. To configure a new user group or user profile, select Add New.
Step 5 Configure the Language field.
**Specifying Languages for Users**

**Step 6**  
Select *Save*.

**Step 7**  
Repeat this task for all user groups and user profiles for which you want to configure language preferences.

---

**Related Topics**

- [Field Reference: Add User Profile Page and Edit User Profile Page](Administration Center Page References for Cisco Unified MeetingPlace) in the *Administration Center Page References for Cisco Unified MeetingPlace* module
- [Dial-Out Features and Voice Prompt Languages](Configuring Dial-Out Features for Cisco Unified MeetingPlace) in the *Configuring Dial-Out Features for Cisco Unified MeetingPlace* module
Configuring Meetings for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:30 pm

Profiled users can schedule meetings to begin immediately or sometime in the future. Unlike a reservationless meeting, a scheduled meeting gives the scheduler control over meeting details. System administrators, in turn, have control over which parameters can be specified by meeting schedulers.

- Configuring Meetings and Ports, page 1
- Configuring Reservationless Meetings, page 2
- Configuring Continuous Meetings, page 4
- Displaying Meeting Times Using a 12- or 24-Hour Clock, page 5
- Configuring Parameters that Affect Sound and Video Quality, page 5
- Configuring Meeting Categories, page 6
- About Cisco Unified MeetingPlace Meeting Prefixes, page 7
- Changing the Default Meeting Template for Meetings Scheduled From the End-User Web Interface, page 8
- Changing the Default Meeting Template for Meetings Scheduled From Microsoft Outlook, page 9

Restrictions
You can schedule a maximum of 4,500 meetings per 24-hour period and a maximum of 400,000 meetings overall. If you exceed either of these limits an alarm is generated.

Configuring Meetings and Ports

Before You Begin
- Read the Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace to determine the port and capacity settings for your system.
- Install the appropriate licenses. See the Installing and Managing Licenses for Cisco Unified MeetingPlace module.
Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Meeting Configuration.
Step 3 Configure the fields.
Step 4 Select Save.

Related Topics
- Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Recordings for Cisco Unified MeetingPlace module

Configuring Reservationless Meetings

Reservationless meetings begin immediately and have the following special characteristics:

- Anyone may join a reservationless meeting, unless a meeting password is in use.
- Anyone can access reservationless meeting recordings and attachments.
- The meeting ID for a reservationless meeting is the Profile number of the meeting owner.
- A meeting instance is created on demand when someone joins a meeting with a reservationless meeting ID. The meeting is terminated immediately when the last participant leaves.
- By default, the meeting subject is the Last name of the meeting owner.
- The system treats each instance of a reservationless meeting as a separate entity with its own unique conference ID, displayed as ConfNum in reports and exported data.
- Participants who join a reservationless meeting before the owner does are placed in a waiting room (where they cannot communicate with each other) until the meeting owner arrives, unless the following statements are true:
  - The Allow any profiled user to initiate field on the Usage Configuration Page is set to Yes.
  - A profiled user starts the meeting from the telephone user interface (TUI).


Restrictions

- Because meeting IDs cannot be longer than 17 digits, users with Profile numbers longer than 17 digits cannot own reservationless meetings.
- Reservationless meeting IDs are permanently reserved and cannot be used for scheduled meetings.
- E-mail notifications are not sent for reservationless meetings.
- Reservationless meetings cannot be lecture-style meetings.
Before You Begin

- Reservationless meetings are enabled by default. Therefore, you only need to perform this task in the following cases:
  - If you want to disable reservationless meetings either system-wide or for specific users.
  - If you previously disabled reservationless meetings and want to reenable them.
- Many fields on the Meeting Configuration Page apply to reservationless meetings. Complete the “Configuring Meetings and Ports” section on page 1.

Procedure

Step 1
Log in to the Administration Center.

Step 2
Enable reservationless meetings on the system:

a. Select System Configuration > Usage Configuration.

b. Set the Enable reservationless meetings field to Yes.

c. (Optional) Configure these other fields:
   - Allow any profiled user to initiate
   - Bill initiator
   - TUI menu is reservationless only
   - Owner can press 2 in TUI to initiate

Step 3
Enable reservationless meetings for users:

a. Select User Configuration.

b. Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.

c. Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.

d. Set the Use reservationless field to Yes.

e. (Optional) Configure these other user profile fields:
   - Show reservationless meetings in public listing
   - Meeting password required
   - Reservationless allow Internet access

f. Select Save.

g. Repeat Step 3 for all user groups and user profiles for which you want to enable reservationless meetings.

Related Topics

- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Configuring Continuous Meetings

A continuous meeting is a type of scheduled, recurring meeting that reserves the meeting ID and ports indefinitely, so that participants may join the meeting at any time on any day. These special characteristics apply to continuous meetings:

- A continuous meeting is in session only when at least one participant is in the meeting.
- The system treats all instances of a continuous meeting as a single entity with common unique conference ID, displayed as ConfNum in reports and exported data.
- Continuous meeting information does not appear in reports or exported data until after the meeting becomes empty.
- Billing reports do not count the minutes during which continuous meetings are empty.

Restrictions

- Only users of type System administrator can schedule continuous meetings.
- Continuous meetings cannot be recorded.
- A maximum of 1000 continuous meetings can be scheduled on the system.
- Continuous meetings cannot expand port reservations as users join. If all the reserved ports for a continuous meeting are in use, then additional users may join the meeting only if floater ports are available. This restriction applies to audio and video ports.

It is common, however, to schedule continuous meetings with zero ports so that no resources are held when the meeting is not in session.

- If a continuous meeting is not scheduled with reserved video resources, then video may be used only if Video floater ports are configured and are available at that time. A continuous meeting instance cannot exceed 24 hours, after which time the system drops all calls in the meeting. Nevertheless, meeting participants may immediately rejoin to restart the meeting.

- In Cisco Unified Communications Manager environments, the length of each call is also limited by the Maximum Call Duration Timer service parameter in Cisco Unified Communications Manager. Continuous meeting participants whose calls are dropped for this reason may immediately rejoin the meeting.

We recommend that you disable the Maximum Call Duration Timer by setting it to 0. See “Configuring the Maximum Call Duration in Cisco Unified Communications Manager” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.

Before You Begin

Complete the “Configuring Meetings and Ports” section on page 1.

Note

By performing this task, you grant System administrator privileges to the specified users.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select User Configuration > User Profiles.

Step 3 Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.
Step 4  Set the Type of user field to System administrator.
This user will now see the continuous meeting option while scheduling recurring meetings.

Step 5  Select Save.

Step 6  Repeat Step 2 through Step 5 for all user profiles for which you want to enable the scheduling of continuous meetings.

Related Topics
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Displaying Meeting Times Using a 12- or 24-Hour Clock

Procedure

Step 1  Log in to the Administration Center.

Step 2  Select System Configuration > Usage Configuration.

Step 3  In the 24-hour time field, select Yes to display meeting times by a 24-hour clock or select No to display meeting times by a 12-hour clock.

Step 4  Select Save.

Related Topics
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Configuring Parameters that Affect Sound and Video Quality

Before You Begin
You must enable Quality of Service (QoS) in your network to minimize IP packet loss, packet delay, and delay variation (or jitter) of voice packets. In particular, you must enable Differentiated Services Code Point (DSCP), also called DiffServ, which is the QoS mechanism supported by Cisco Unified MeetingPlace.

Note
The Cisco Unified MeetingPlace default DiffServ settings conform to the recommendations in the Cisco Unified Communications Solution Reference Network Design (SRND). If your network already conforms to these recommendations, then no QoS configuration is required.
Configuring Meetings for Cisco Unified MeetingPlace

Configuring Meeting Categories

Meeting categories help you organize reports. The system comes with a preconfigured meeting category named Standard, which cannot be deleted.

As the system administrator, you can add meeting categories and assign a default meeting category to each user group or user profile. You can also enable end users to specify the meeting category for each meeting they schedule. End users can use meeting categories to find meetings.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Add or edit a meeting category:</td>
</tr>
<tr>
<td></td>
<td>a. Select <strong>System Configuration &gt; Meeting Categories</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>Add New</strong>, or select an existing meeting category.</td>
</tr>
<tr>
<td></td>
<td>c. Configure the fields.</td>
</tr>
<tr>
<td></td>
<td>d. Select <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>e. Repeat Step 2 as required.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Assign a default meeting category to a user group or user profile:</td>
</tr>
<tr>
<td></td>
<td>a. Select <strong>User Configuration</strong>.</td>
</tr>
<tr>
<td></td>
<td>b. Select <strong>User Groups</strong> or <strong>User Profiles</strong>, depending on whether you want to configure a user group or an individual user profile.</td>
</tr>
<tr>
<td></td>
<td>c. Select <strong>Edit</strong> or <strong>Add New</strong>, depending on whether you want to configure an existing or a new user group or user profile.</td>
</tr>
<tr>
<td></td>
<td>d. Configure the <strong>Default meeting category</strong> field.</td>
</tr>
<tr>
<td></td>
<td>e. Select <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

Related Topics

- Field Reference: Media Parameters Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Step 4  Show or hide the Meeting Category option on the end-user web scheduling page:
  a.  Sign in to the end-user web interface by using your administrator-level profile.
  b.  Select **Admin**.
  c.  Select **User Interface Fields**.
  d.  Select **Scheduling Details Page**.
    e. Enable or disable the meeting category field.

**Related Topics**
- Field Reference: Add Meeting Categories Page and Edit Meeting Categories Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Exporting Meeting Categories in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
- Importing Meeting Categories in the Importing Data into Cisco Unified MeetingPlace module

### About Cisco Unified MeetingPlace Meeting Prefixes

When you schedule a meeting, Cisco Unified MeetingPlace attaches a prefix to an internally referenced meeting name. The prefix varies depending on the meeting configuration.

**Note**  The meeting name described above is not displayed to the user. This meeting name is not related to the meeting identifier or dialing plan.

For example, you configure a meeting with the following settings:

Select **System Configuration** > **Meeting Configuration** > **Global Settings**.

You can select High Rate or Standard Rate:
- Standard rate (384 kbps maximum)
- High rate (2 Mbps maximum)

When you select **Media Server Configuration** > **Resource Management** > **Meeting Types**, the following service prefixes are available: 60001-60006.

There are two prefixes for standard rate (384 kbps):
- 60003: Standard Rate Video High Capacity Audio (Audio+Video 384)
- 60006: Standard Rate Video High Quality Audio (Audio+Video 384)

There are two prefixes for high rate (2 Mbps maximum):
- 60004: High Rate Video High Capacity Audio (Audio+Video (Capacity Plus) 2048)
- 60005: High Rate Video High Quality Audio (Audio+Video (Capacity Plus) 2048)
Each MCU in your system has predefined services that must be the same on all the MCUs. Cisco does not recommend that you modify these services because doing so can cause your system to have problems. These predefined services correspond to quality of service including two options for audio and three (including “none”) for video, giving you six service prefixes.

When a meeting starts, it has a predetermined setting for audio and video based primarily on system configuration. The system selects a service prefix by searching for a service on the MCU that matches the audio and video settings.

You configure your services in the administration center. For audio you can choose higher capacity G.711 and G.729 (without LEC on G.729) or lower capacity G.711 and G.729 with LEC, or G.722 and iLBC. For video you can choose between standard rate (384 Kb) and high rate (2048 Kb). These selections (including the option of no video) determines which of the six service prefixes are used. Note that these settings are global. You cannot choose your settings on a per-meeting basis.

Changing the Default Meeting Template for Meetings Scheduled From the End-User Web Interface

By default, meetings scheduled from the Cisco Unified MeetingPlace end-user web interface use the Collaborative meeting template.

Before You Begin

- If you are not familiar with meeting templates, see “Meeting Templates” in the Creating and Modifying Meeting Templates and Layouts module.
- Performing this task changes the system-wide default meeting template. Nevertheless, individual users can select a different meeting template while scheduling meetings.

Restriction

You cannot select a custom meeting template as the default meeting template. You can only choose from the following options: Collaborative, Presentation, and Webinar.

Caution

Performing this task requires that you restart the Cisco Unified MeetingPlace Web Conferencing services. Proceed only during a scheduled maintenance period.

Procedure

Note

When you restart the Web Server, all manual changes made to the registry are lost.

Step 1

On the Web Server, navigate to C:\Program Files\Cisco Systems\MPWeb\Template.

Step 2

Open the wcSchedBasics.tpl file using a text editor such as Wordpad.

Step 3

Find and change the order of the following lines, so that the line for the desired default meeting template appears before the others.

```javascript
```
Step 4  Save the updated file.
Step 5  Restart the Cisco Unified MeetingPlace Web Conferencing services.
Step 6  Repeat this procedure for all Web Servers in the internal cluster.

Note  Setting the default meeting template does not affect meetings scheduled by copying an existing meeting.

Verifying
Log out of the Cisco Unified MeetingPlace end-user web interface, log back in, and then schedule a meeting. Verify that the desired meeting template is used by default.

Related Topics

- Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- Configuring the Cisco Unified MeetingPlace Web Conferencing User Interface module
- Changing the Default Meeting Template for Meetings Scheduled From Microsoft Outlook, page 9

Changing the Default Meeting Template for Meetings Scheduled From Microsoft Outlook

By default, Cisco Unified MeetingPlace meetings that are scheduled from Microsoft Outlook use the Collaborative meeting template.

Before You Begin

- This task requires familiarity with editing text files in the Linux environment, for example, by using the Linux vim command.
- If you are not familiar with meeting templates, see “Meeting Templates” in the Creating and Modifying Meeting Templates and Layouts module.
- Performing this task changes the system-wide default meeting template. Nevertheless, individual users can select a different meeting template while scheduling meetings.

Restriction
You cannot select a custom meeting template as the default meeting template. You can only choose from the following options: Collaborative, Presentation, and Webinar.
Caution

Performing this task requires that you restart the Apache Tomcat services and the Cisco Unified MeetingPlace Web Conferencing services. Proceed only during a scheduled maintenance period.

Procedure

Step 1 Log in to the Application Server CLI as the mpxadmin user.

Step 2 Enter su to get root privileges.

Step 3 Navigate to the following directory:

/opt/cisco/meetingplace/web/current/bases/main/webapps/outlook/WEB-INF/classes/com/cisco/meetingplace/outlook/bundles

Step 4 View the BreezeTemplates.properties file.

```
[root@example-appserver bundles]# cat BreezeTemplates.properties
3=Webinar
2=Presentation
1=Collaborative
ORDER=1, 2, 3
```

The current default template is item 1, which in this example (and by default) is the Collaborative template.

Proceed only if you want to specify a different default meeting template.

Step 5 Change the order by updating the order parameter so that the desired default meeting template (first item in the list) is item 1.

Step 6 Verify that the file is correct and that there are no typographical errors.

In the following example, the order is changed to use the Presentation template by default:

```
[root@example-appserver bundles]# cat BreezeTemplates.properties
3=Webinar
2=Collaborative
1=Presentation
ORDER=2, 1, 3
```

Step 7 Restart the Apache Tomcat services.

```
[root@example-appserver bundles]# /etc/init.d/mpx_tomcat restart
```

Step 8 Restart the Cisco Unified MeetingPlace Web Conferencing services.

Example

In the following example, the order is changed to use the Presentation template by default:

```
[root@example-appserver bundles]# cat BreezeTemplates.properties
3=Webinar
2=Presentation
1=Collaborative
ORDER=1, 2, 3
[root@example-appserver bundles]# cat << END > BreezeTemplates.properties
> 3=Webinar
> 2=Presentation
> 1=Collaborative
> ORDER=2, 1, 3
```

Caution

Performing this task requires that you restart the Apache Tomcat services and the Cisco Unified MeetingPlace Web Conferencing services. Proceed only during a scheduled maintenance period.

Procedure

Step 1 Log in to the Application Server CLI as the mpxadmin user.

Step 2 Enter su to get root privileges.

Step 3 Navigate to the following directory:

/opt/cisco/meetingplace/web/current/bases/main/webapps/outlook/WEB-INF/classes/com/cisco/meetingplace/outlook/bundles

Step 4 View the BreezeTemplates.properties file.

```
[root@example-appserver bundles]# cat BreezeTemplates.properties
3=Webinar
2=Presentation
1=Collaborative
ORDER=1, 2, 3
```

The current default template is item 1, which in this example (and by default) is the Collaborative template.

Proceed only if you want to specify a different default meeting template.

Step 5 Change the order by updating the order parameter so that the desired default meeting template (first item in the list) is item 1.

Step 6 Verify that the file is correct and that there are no typographical errors.

In the following example, the order is changed to use the Presentation template by default:

```
[root@example-appserver bundles]# cat BreezeTemplates.properties
3=Webinar
2=Collaborative
1=Presentation
ORDER=2, 1, 3
```

Step 7 Restart the Apache Tomcat services.

```
[root@example-appserver bundles]# /etc/init.d/mpx_tomcat restart
```

Step 8 Restart the Cisco Unified MeetingPlace Web Conferencing services.

Example

In the following example, the order is changed to use the Presentation template by default:

```
[root@example-appserver bundles]# cat BreezeTemplates.properties
3=Webinar
2=Presentation
1=Collaborative
ORDER=1, 2, 3
[root@example-appserver bundles]# cat << END > BreezeTemplates.properties
> 3=Webinar
> 2=Presentation
> 1=Collaborative
> ORDER=2, 1, 3
```
>  END
[root@example-appserver bundles]# cat BreezeTemplates.properties
3=Webinar
2=Presentation
1=Collaborative
ORDER=2, 1, 3
[root@example-appserver bundles]# /etc/init.d/mpx_tomcat restart
Stopping tomcat:                                                   [ OK ]
Starting tomcat:                                                   [ OK ]
[root@example-appserver bundles]#

Verifying
Restart Microsoft Outlook and schedule a Cisco Unified MeetingPlace meeting. Verify that the desired meeting template is used by default.

Related Topics
- How to Log in to the CLI in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module
- Changing the Default Meeting Template for Meetings Scheduled From the End-User Web Interface, page 8
Configuring E-Mail Notifications for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:30 pm

Cisco Unified MeetingPlace generates e-mail notifications and sends them to the meeting owner and invitees whenever a meeting is scheduled, rescheduled, or cancelled.

- Restrictions for E-Mail Notifications, page 1
- Configuring Click-to-Attend Links, page 2
- Configuring the SMTP Servers, page 2
- Configuring E-Mail Notification Retries, page 3
- Configuring User Preferences for E-Mail Notifications, page 3

Restrictions for E-Mail Notifications

- E-mail notifications are not generated for reservationless meetings.
- E-mail notifications are not sent when only the meeting length is modified for a scheduled meeting.
- Only the first 18 characters of the meeting subject appears in e-mail notifications.
- Only users who have a valid E-mail address in the user profile may send or receive e-mail notifications.

Related Topics
- Customizing E-Mail Notifications for Cisco Unified MeetingPlace module
Configuring Click-to-Attend Links

Perform this task to enable valid click-to-attend links in e-mail notifications and in MeetingPlace Conference Manager.

**Procedure**

1. Log in to the Administration Center.
2. Select **System Configuration > Usage Configuration**.
3. Configure the fields in the **Click-to-Attend Link Configuration** section.
4. Select **Save**.

**Related Topics**
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Installing MeetingPlace Conference Manager module

Configuring the SMTP Servers

For Cisco Unified MeetingPlace to send e-mail notifications, one of the following must be configured:

- At least one SMTP server
- Microsoft Outlook integration

**Note**
To send e-mail notifications, Cisco Unified MeetingPlace does *not* use the mail server information that you entered while installing the operating system (OS). Even if you want both the OS and the Cisco Unified MeetingPlace application to use the same SMTP server, you must re-enter the server information through the Administration Center by performing this procedure.

After the initial system startup, Cisco Unified MeetingPlace uses the primary SMTP server to send e-mail notifications. If the system fails to send e-mail notifications through the primary SMTP server, the system immediately switches to using the secondary SMTP server, if configured. The system continues to use the secondary SMTP server until a problem occurs; then the system automatically switches to using the primary SMTP server.

**Before You Begin**
If you want to use Microsoft Outlook exclusively for e-mail notifications, then do not perform this task. Instead, see the Integration Note for Installing and Configuring Microsoft Outlook with 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).

**Restriction**
Transport Layer Security (TLS) is not supported for SMTP e-mail notifications.
Configuring E-Mail Notifications for Cisco Unified MeetingPlace

### Configuring E-Mail Notification Retries

You can configure how many times and how frequently the system attempts to resend notifications that have failed. This configuration also applies to the back-end deployment of Microsoft Outlook integration, which enables Cisco Unified MeetingPlace to send Microsoft Outlook calendar notifications for meetings that are scheduled from the Cisco Unified MeetingPlace end-user web interface.

**Procedure**

1. Log in to the Administration Center.
2. Select **System Configuration > E-Mail Notifications > SMTP Server Configuration**.
3. Configure the fields.
4. Select **Save**.

**Related Topics**

- Field Reference: SMTP Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring User Preferences for E-Mail Notifications, page 3

### Configuring User Preferences for E-Mail Notifications

You can configure the behavior of e-mail notifications for each user group or individual user, for example:

- E-mail type and format.
- Whether notifications are sent for meeting updates or cancellations.
• Who can send or receive notifications.
• What notifications include, such as participant lists, meeting passwords, or attachments.

Before You Begin
• To enable the use of the Microsoft Exchange or IBM Lotus Notes formats, you first need to set up
  the integrations. See the following at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html:
  – Integration Note for Installing and Configuring Microsoft Outlook with Cisco Unified
    MeetingPlace
  – Integration Note for Installing and Configuring IBM Lotus Notes with Cisco Unified
    MeetingPlace
• Avoid changing e-mail notification settings once Cisco Unified MeetingPlace is in use, because
  users might already rely on a certain behavior, such as having all invited meeting participants
  receive e-mail notifications for new or changed meetings. Changing that behavior may result in lost
  productivity. If you must change the e-mail notification settings after Cisco Unified MeetingPlace
  has been in use, then make sure that you alert your users to the changes.
• You can configure the e-mail notification settings in user groups or user profiles. We recommend
  that you configure the settings in user groups to help you keep e-mail notification settings as
  consistent as possible across your user base.
• Only users who have a valid E-mail address in the user profile may send or receive e-mail
  notifications. E-mail addresses cannot be configured in user groups.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Groups or User Profiles, depending on whether you want to configure a user group or an
  individual user profile.
Step 3 Select Edit or Add New, depending on whether you want to configure an existing or new user group or
  user profile.
Step 4 Configure these fields:
  • E-mail type and format
  • Fields in the Notifications section
Step 5 Select Save.

Related Topics
• Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center
  Page References for Cisco Unified MeetingPlace module
About Recordings

- Recording Resources and Port Usage, page 1
- Options for Starting Meeting Recordings, page 2

Recording Resources and Port Usage

The system comes with 50 recording resources. Recording resources are reserved for scheduled meetings that are owned by users whose Can record meetings user profile field is set to Yes.

While recording each meeting, the system uses the following:

- One recording resource
- One voice port
- One video port (meetings for which video resources are reserved)

Only the voice portion of the meeting is recorded in video-enabled meetings for which video resources are not reserved for participants.

Note: The system does not use any web ports while recording the web portion of meetings.

When a meeting recording starts the system attempts to use a voice port (and a video port if video resources were reserved for the meeting) in the following order:

1. Port that was reserved for the meeting
2. Any unreserved port  
3. Floater port  
   If the system fails to obtain a voice port, then the meeting cannot be recorded until a voice port is released.  
   If the system fails to obtain a video port, then only a voice port is used, and only the voice and web portions of the meeting will be recorded.

**Note**  
Cisco recommends that you configure additional floater ports if you expect many meetings to be recorded at the same time. See the following:  
- System Capacity in the Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace  
- Configuring Meetings and Ports in the Configuring Meetings for Cisco Unified MeetingPlace module

**Related Topics**  
- Installing and Managing Licenses for Cisco Unified MeetingPlace module  
- Recording Size in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module  
- Configuring Audio Conversion module

**Options for Starting Meeting Recordings**

- Users with recording privileges can enter #61 in the TUI during the meeting.  
- Meeting moderators can select **Meeting > Record Meeting** in the web meeting room.  
- The system automatically records meetings in the following cases:  
  - User profiles are configured to automatically record meetings that are scheduled by the user. See Table 1.  
  - While scheduling a meeting, the user (with recording privileges) sets **Automatically start recording** to Yes on the More Options page.

**Note**  

Table 1 describes how to configure the **Auto-start recording** user profile field to affect whether and how the system automatically starts recording meetings.
Configuring Recordings for Cisco Unified MeetingPlace

Prerequisites for Recording

To record the video portions of meetings, you must install the videorecording license. See the Installing and Managing Licenses for Cisco Unified MeetingPlace module.

We recommend that you use an external storage device to prevent the Web Server from running out of disk space. See “Configuring Shared Storage” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module.

If you do not use an external storage device, then make sure that you monitor the Alarm Table. If any Web Server disk space shortage issues appear, take immediate action to transfer the recordings to an external storage device.

Caution

The Web Server will become inoperable if all the disk space is consumed. Specifically, the end-user web interface will become inaccessible. Also, because recordings on the Application Server will not be replicated to the Web Server, those recordings may be deleted from the system before they can be converted for user playback.

Related Topics

- Recording Resources and Port Usage, page 1
- Recording Size in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

Related Topics

- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Recording Resources and Port Usage, page 1
- Enabling Users to Record Meetings, page 5

---

### Table 1  User Profile Field Combinations for Automatically Starting Recordings

<table>
<thead>
<tr>
<th>Auto-start recording Field Value</th>
<th>When to Use This Combination of User Profile Field Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>Yes</td>
<td>You want the system to automatically record all meetings that are scheduled by the user.</td>
</tr>
</tbody>
</table>
| Yes                              | You want a meeting participant (with recording privileges) to start recording meetings that are scheduled by the user.  
  If all meeting participants leave after the meeting recording is started, then you want the system to automatically restart recording if anyone rejoins the meeting. |
| No                               | You want meeting participants (with recording privileges) to be able to record meetings that are scheduled by the user without worrying about other meetings utilizing all recording resources. |
| No                               | This combination is automatically configured if you disable recording privileges for the user by setting the Can record meetings field to No. |
Restrictions for Recording

- Video-enabled meetings are restricted to a maximum meeting recording length of 6 hours, even if no video participants actually attend. Specifically:
  - In the user profile of the meeting scheduler, if the Video usage field enables the user to host video meetings, then the meeting recording cannot exceed 6 hours. If this limit is reached during a meeting, the system automatically stops the recording.
  - There is no meeting recording length restriction for meetings scheduled by users whose Video usage user profile field is set to Can attend video meetings. Because these users cannot host video meetings, the meetings they schedule are not video-enabled.

- The default system configuration for video-enabled recording requires H.264 to be the highest priority in the list of supported video codecs for 7.1.
  - Log into Audio blade.
  - Select MCU > Services.
  - Highlight the service code and select edit > Advanced video Settings.
  - Add H.264 to Selected and make to be the first in the list.

- The system allows a maximum of 50 concurrent meeting recordings. Nevertheless, the supported number of concurrent recordings depends on the Application Server model, the configured and utilized capacity of your system, and the type of media (voice, video, web) being recorded.


- Cisco Unified MeetingPlace does not record Cisco WebEx meetings, even though the audio portion is held on the Cisco Unified MeetingPlace system. This restriction applies to all meetings that are scheduled to use Cisco WebEx web conferencing, even if participants never join the web meetings. Instead, Cisco WebEx meetings are recorded through Cisco WebEx Network-Based Recording (NBR) and stored on the Cisco WebEx site. The recording capacity is determined by the Cisco WebEx account.

- The Application Server can store up to:
  - 500 hours of audio recordings or 80 hours of video recordings on a Cisco MCS 7835.
  - 1000 hours of audio recording or 160 hours of video recordings on a Cisco MCS 7845.

Cisco Unified MeetingPlace meeting recordings are only initially stored on the Application Server. Shortly after each recorded meeting ends, the Replication Service copies the meeting recording from the Application Server to the Web Server, where the recording is converted and stored for user playback.

Every day at 2 a.m. (local server time), the system purges all recordings on the Application Server that are older than 24 hours. To display the available disk space for recordings (/mpx-record directory) on the Application Server, log in to the CLI and enter df -k.

**Note**

If the /mpx-record disk space on the Application Server ever becomes 90% utilized, the system generates a minor alarm and does not allow any more recordings to begin until sufficient disk space is freed by the daily 2 a.m. purge. If recordings in progress cause the disk space to become 97% utilized, then the system stops all recordings. In the unlikely event that the disk space becomes 100% utilized, the system generates a major alarm, and you need to contact Cisco TAC.
How to Configure Recordings

- Enabling Users to Record Meetings, page 5
- Enabling Guest Users to Record Meetings, page 6
- Configuring System-Wide Recording Parameters, page 7

Enabling Users to Record Meetings

**Before You Begin**
See the “Prerequisites for Recording” section on page 3.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>User Configuration</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>User Groups</strong> or <strong>User Profiles</strong>, depending on whether you want to configure a user group or an individual user profile.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select <strong>Edit</strong> or <strong>Add New</strong>, depending on whether you want to configure an existing or a new user group or user profile.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Set the <strong>Can record meetings</strong> field to Yes.</td>
</tr>
</tbody>
</table>
| Step 6 | (Optional) Configure the following fields:  
  - **Who can access**  
  - **Auto-start recording** |
| Tip    | See “User Profile Field Combinations for Automatically Starting Recordings” on page 3. |
| Step 7 | Select **Save**. |
Related Topics

- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Options for Starting Meeting Recordings, page 2
- Restricting Access to Recordings and Attachments in the Securing the Cisco Unified MeetingPlace System module
- Configuring System-Wide Recording Parameters, page 7

What To Do Next

To give recording privileges to guests, proceed to the “Enabling Guest Users to Record Meetings” section on page 6.

Enabling Guest Users to Record Meetings

Before You Begin

See the “Prerequisites for Recording” section on page 3.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select System Configuration &gt; Usage Configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Set the Guests can lock and record meetings field to Yes.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Save.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select User Configuration &gt; User Profiles.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Enter guest in the search field.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select Edit for the guest profile.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Set the Can record meetings field to Yes.</td>
</tr>
<tr>
<td>Step 9</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>

Related Topics

- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring System-Wide Recording Parameters, page 7
Configuring System-Wide Recording Parameters

Procedure

Step 1  Log in to the Administration Center.

Step 2  Select System Configuration > Meeting Configuration.

Step 3  Configure the following fields:

- Maximum meeting message length (minutes)
- Maximum meeting name length (seconds)
- Maximum participant name length (seconds)

Step 4  Select Save.

Related Topics

- Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restricting Access to Recordings and Attachments in the Securing the Cisco Unified MeetingPlace System module
- Recording Size in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module
- Configuring Audio Conversion module
Configuring Attendant Settings for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:30 pm

- Configuring Attendant Privileges
- Configuring Operator Assistance

Configuring Attendant Privileges

You can configure which Administration Center and MeetingPlace Conference Manager capabilities are available to users of type Attendant.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Usage Configuration.
Step 3 Configure the Attendant Privileges fields.
Step 4 Select Save.

Related Topics
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- About User Types in the Administration Center Page References for Cisco Unified MeetingPlace module
- Using MeetingPlace Conference Manager module
Configuring Operator Assistance

Cisco Unified MeetingPlace can be configured to forward calls to the help desk Attendant in the following situations:

- A caller dials 0 for operator assistance.
- A caller does not enter a number at a voice prompt.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Usage Configuration.
Step 3 Configure the following fields:
  - Attendant phone—Enter the help desk or attendant phone number.
  - Dial attendant on timeout—Set this field to Yes.
Step 4 Select Save.

Related Topics

- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Call Control for Cisco Unified MeetingPlace module
P a r t

User and Endpoint Configuration

- Configuring User Profiles and User Groups for Cisco Unified MeetingPlace
- Configuring Cisco Unified MeetingPlace Directory Service
- Changing the User Status in Cisco Unified MeetingPlace User Profiles
- Configuring Endpoints for Cisco Unified MeetingPlace
Configuring User Profiles and User Groups for Cisco Unified MeetingPlace

How to Configure User Groups

User groups contain information that can be inherited by user profiles. In each user profile, the Group name field identifies the user group to which the user profile belongs. Many of the fields in the user profile can be set to the group default, which means that the field value in the assigned user group becomes the field value used in the user profile. When you configure a field in a user group, that field is automatically updated in each user profile within the group, provided that the field is set to group default in the user profile.

To override a user group field configuration within an individual user profile, set the field in the user profile to a value other than group default. Further updates to the field in the user group will not affect the field in the user profile.

- System User Group, page 1
- Recommendations for User Groups, page 2
- Adding or Editing a User Group Manually, page 2
- Searching for a Specific User Group, page 3
- Deleting a User Group, page 4

System User Group

Cisco Unified MeetingPlace comes preconfigured with a user group called System. Except for the name, all fields in the System user group can be modified. You cannot, however, delete the System user group. The values configured in the System user group are used as the default values in new groups that are added manually or by import.
The System user group is assigned to user profiles as follows:

- By default, the System user group is assigned to the preconfigured user profiles.
- If no configured filters apply, then the System user group is assigned to Directory Service user profiles as they are imported from Cisco Unified Communications Manager into Cisco Unified MeetingPlace.
- If a user group is deleted, then any user profiles that were assigned to that user group are automatically assigned to the System user group.

Related Topics:
- About Preconfigured User Profiles, page 5
- Configuring Cisco Unified MeetingPlace Directory Service module

Recommendations for User Groups

- Add at least one user group, so that you can easily manage and configure system administrator profiles separately from end-user profiles. For example, a simple setup can use the following two user groups:
  - Administrator—Assign to the preconfigured admin profile and to the user profiles of any other system administrators. Enable all privileges for users in this group.
  - System (preconfigured)—Assign to end-user profiles and to the preconfigured guest profile, which is used as a template for new user profiles. Some guest profile fields are also applied to guest users.
- If you use the find me dial-out feature with non-direct-dial pagers, then you need at least one user group for each pager system phone number that is shared by your users.
- Before importing any user profiles, make sure that you create or import the user groups to which the imported user profiles belong.
- Use as many group default settings as you can in your user profiles:
  - The more group default settings you have in each user profile, the more easily you can maintain user profiles for similar users.
  - The more group default settings you have in the preconfigured guest profile, the more easily you can create user profiles for similar users, because the guest profile is used as a template for new user profiles.

Related Topics:
- System User Group, page 1

Adding or Editing a User Group Manually

Before You Begin
- To instead add or edit a batch of multiple user groups, see the “Adding or Editing User Groups by Import” section on page 5.
- Read the “Recommendations for User Groups” section on page 2.
### Configuration of User Profiles and User Groups for Cisco Unified MeetingPlace

#### How to Configure User Groups

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Select **User Configuration > User Groups**.

**Step 3** Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.

**Step 4** Configure the fields.

**Step 5** Select **Save**.

**Step 6** Verify that your new user group appears in the **User Groups Page**.

**Related Topics**

- Field Reference: Add User Group Page and Edit User Group Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- System User Group, page 1
- Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

**What To Do Next**

Proceed to “Updating All Groups” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module if you want the new or modified user group settings to take effect immediately. Otherwise, any changes or additions you make will take effect after the next Replication Service update, which occurs nightly.

### Searching for a Specific User Group

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Select **User Configuration > User Groups**.

**Step 3** Enter the name of the user group that you are looking for.

- The entire name is not required.
- The search tool is not case sensitive.

**Step 4** Select **Search**.

**Step 5** If the list of name matches is too long for you to quickly find a particular user group, perform one of the following actions:

- Enter the entire name of the user group that you are looking for and select **Search**.
- At the bottom right corner, use the page navigation tools, such as the arrows and Go buttons, to browse the long list of user groups.

**Step 6** To view the profile configuration for a particular user group, select **Edit** in the same row as the user group.
Related Topics

- Field Reference: Add User Group Page and Edit User Group Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Deleting a User Group

Before You Begin

- To instead delete a batch of multiple user groups, see the “Deleting User Groups by Import” section on page 6.
- If user profiles belong to a user group that gets deleted, those user profiles are automatically assigned to the system group.
- Deleting user groups is an irreversible operation. Before you delete user groups, consider creating a backup copy so that you can later retrieve the deleted user groups if necessary. Use one of the following options:
  - Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module
  - Exporting User Groups in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module

Restriction

You cannot delete the system user group.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration > User Groups.
Step 3 Search for the user group that you want to delete.
Step 4 Check the check box in the same row as the user group that you want to delete. You may select multiple user groups.

Make sure that you uncheck any check boxes for user groups that you want to keep in the Cisco Unified MeetingPlace database.

Step 5 Select Delete Selected.
Step 6 When the confirmation pop-up window appears, select OK.
Step 7 Verify that the deleted user group does not appear in the User Groups Page.

Related Topics

- Searching for a Specific User Group, page 3
How to Configure User Profiles

The Cisco Unified MeetingPlace database should have a user profile for every person who sets up meetings and attends meetings regularly. Unprofiled users, called guest users, may attend meetings that are not restricted to profiled users only. System administrators are responsible for maintaining the directory of users and their associated privileges.

- Benefits of Being a Profiled User, page 5
- About Preconfigured User Profiles, page 5
- Methods for Adding User Profiles, page 7
- Adding User Profiles Manually, page 8
- Searching for a Specific User Profile, page 9
- Editing a User Profile, page 10
- Deleting a User Profile, page 10

Restrictions
Your system is limited to 250,000 user profiles. If you exceed this number an alarm is generated.

Benefits of Being a Profiled User

Although unprofiled users may attend unrestricted meetings as guests, only profiled users may perform the following actions:

- Start or own reservationless meetings
- Schedule and manage meetings
- Update and maintain some of their own user profile settings
- Attend meetings and access recordings that are restricted to profiled users
- Be contacted by phone or pager at the time of their meetings

Related Topics
- Guest Profile Fields That Apply to Guest Users, page 6

About Preconfigured User Profiles

Cisco Unified MeetingPlace comes preconfigured with these user profiles:

- Admin Profile, page 5
- Recorder Profile, page 6
- Guest Profile, page 6

Admin Profile

Use the preconfigured admin profile to log in to the Administration Center for the first time.
After this initial login, the system administrator typically creates a separate user profile for each individual who will act as system administrator. You may, however, choose to continue to use the admin profile to log in to the end-user web interface and the Administration Center.

Related Topics

- Logging In to the Cisco Unified MeetingPlace Administration Center module

**Recorder Profile**

The preconfigured recorder profile is applicable only when Cisco Unified MeetingPlace is integrated with Cisco WebEx. Cisco WebEx Network-Based Recording (NBR) uses the recorder profile to access and record the audio portion of Cisco WebEx meetings.

Related Topics

- Configuring the Cisco WebEx Audio Recorder in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module

**Guest Profile**

The system uses the preconfigured guest profile primarily as a template for new user profiles, but some field values are applied to guest users.

- Guest Profile Fields That Apply to New User Profiles, page 7

**Guest Profile Fields That Apply to Guest Users**

Guest users are unprofiled users or users who access Cisco Unified MeetingPlace without logging in. Only the following fields in the preconfigured guest profile apply to guest users:

- **First name**—Used in meeting participant lists, reports, and video labels of live conferences.
  
  If you want to change the video label of the guest profile, make sure to put all of the text that you want displayed into the **First name** field. Video labels are displayed in the lower left corner of the video window.

- **Last name**—Used in meeting participant lists and reports.
  
  The last name of the guest profile is not displayed in the video label of a live conference. If you want to change the video label of the guest profile, make sure to put all of the text that you want displayed into the **First name** field.

- **Type of user**—End user (cannot be modified).

- **E-mail type and format**—Used in e-mail notifications sent to invitees that are not invited from the Cisco Unified MeetingPlace directory.

- **Language**—Affects the following:
  
  - End-user web interface used to schedule, find, and attend meetings.
  
  - Voice prompts for the following dial-out features when initiated by guest users: **Find Me** and **Dial Out From Within a Meeting**.

  - E-mail notifications sent to invitees that are not selected from the Cisco Unified MeetingPlace directory.

- **Can dial out (does not apply to Cisco WebEx meetings)**—Whether guests have dial-out privileges.
Can record meetings—Whether guests can start and stop recording from the telephone user interface (TUI) only. Guests cannot start and stop meeting recordings from web meeting room, because only meeting moderators may do so.

Note: In the guest profile, the Can record meetings field applies to guest users only when the Guests can lock and record meetings field on the Usage Configuration Page is also set to Yes.

Guest Profile Fields That Apply to New User Profiles

The preconfigured guest profile serves as a template for new user profiles. For example, if you configure the Maximum meeting length (minutes) field to 90 in the guest profile, then all new user profiles will have this field initially set to 90.

All guest profile fields are applied to new user profiles, except those in the following list:

- First name
- Last name
- User ID
- User password
- Profile number
- Profile password

Remember that if you change the Group name in a user profile, then all fields that are set to "group default" will inherit values from the new user group.

Related Topics
- How to Configure User Groups, page 1

Methods for Adding User Profiles

Timesaver: Create or import user groups before you create or import user profiles. User profiles inherit user group configurations, so you can avoid configuring most fields for each user.

There are three ways to populate the Cisco Unified MeetingPlace database with user profiles. The method used to add each user profile to Cisco Unified MeetingPlace determines the authentication method used for user login attempts. See Table 1.
Adding User Profiles Manually

Manually creating user profiles through the Administration Center is useful for:
- Adding one or a few new users to the database when you cannot use Directory Service to add them.
- Adding temporary user profiles for visitors.

Before You Begin
- To instead add a large number of user profiles, then see one of the following:
  - Configuring Cisco Unified MeetingPlace Directory Service module
  - Adding or Editing User Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module
- Create user groups before you create individual user profiles.
  
  Many user profile attributes are inherited from the assigned user group. This mechanism allows you to avoid configuring most fields for individual users. See the “How to Configure User Groups” section on page 1.
- The guest profile serves as a template for new user profiles. To speed up the process of creating user profiles, configure as many fields as are applicable in the guest profile to group default.

Procedure

**Step 1** Log in to the Administration Center.

**Step 2** Select User Configuration > User Profiles.

**Step 3** Select Add New.

**Step 4** Enter or change the values in the fields.

---

Table 1: Methods for Adding User Profiles and Authenticating Users

<table>
<thead>
<tr>
<th>Method of Adding User Profiles</th>
<th>Authentication Method</th>
</tr>
</thead>
</table>
| Through Directory Service import (recommended) | External AXL authentication  
| By import                      | Depends on isLocalUser user profile import field:  
  - Yes—Locally on Cisco Unified MeetingPlace  
  - No—External AXL authentication |
| Manually                       | Locally on Cisco Unified MeetingPlace |

Related Topics
- Configuring Cisco Unified MeetingPlace Directory Service module
- Adding or Editing User Profiles by Import, page 7
- Adding User Profiles Manually, page 8
Tip If you select the group default option in any field, the value that is inherited from the assigned user group appears in parentheses in that field.

Step 5 Select Save.
Step 6 Verify that your new user profile appears on the User Profiles Page.

What To Do Next
Proceed to “Updating All User Profiles” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module if you want the new user profiles to be available immediately for meeting invitations. Otherwise, any changes or additions you make will take effect after the next Replication Service update, which occurs nightly.

Related Topics
• Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
• Methods for Adding User Profiles, page 7
• Guest Profile Fields That Apply to New User Profiles, page 7
• Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

Searching for a Specific User Profile

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration > User Profiles.
Step 3 Choose whether to search by user ID or name (either first or last name).
Step 4 Enter the user ID, first name, or last name of the user profile that you are looking for.
   • The entire name is not required.
   • The search tool is not case sensitive.
Step 5 Select Search.
   • If the search results are too large, enter the entire user ID, entire first name, or entire last name of the user profile that you are looking for, and select Search.
   • At the bottom right corner, use the page navigation tools, such as the arrows and Go buttons, to browse the long list of user profiles.
Step 6 To view a specific user profile, select Edit in the same row as the user profile.

Related Topics
• Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Editing a User Profile

Before You Begin

- If you are editing a Directory Service user profile, then make sure that you modify the correct Source of the user profile field configuration. See “Directory Service User Profile Configuration” in the Configuring Cisco Unified MeetingPlace Directory Service module.

- To edit a batch of multiple user profiles instead of a single user profile, see “Adding or Editing User Profiles by Import” in the Importing Data into Cisco Unified MeetingPlace module.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select User Configuration > User Profiles.
Step 3  Find the user profile that you want to modify.
Step 4  Select Edit in the same row as that user profile.
Step 5  Enter or change the values in the fields.
Step 6  Select Save.

Related Topics

- Searching for a Specific User Profile, page 9
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

What To Do Next

Proceed to “Updating All User Profiles” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module if you want the modified user profile settings to take effect immediately. Otherwise, any changes or additions you make will take effect after the next Replication Service update, which occurs nightly.

Deleting a User Profile

Before You Begin

- To instead delete a batch of multiple user profiles, see “Deleting User Profiles by Import” in the Importing Data into Cisco Unified MeetingPlace module.

- Deleting user profiles is an irreversible operation. Before you delete user profiles, consider creating a backup copy so that you can later retrieve the deleted user profiles if necessary. Use one of the following options:

  - Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module

  - Exporting User Profiles in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
Configuring User Profiles and User Groups for Cisco Unified MeetingPlace

How to Configure User Profiles

Note

Passwords are not exported. Therefore, to import any previously deleted user profiles, you will need to provide a User password (EncryptedUserPWD or upwd) and Profile password (EncryptedProfilePWD or prfpwd) for each user.

Restrictions

- (Cisco WebEx integration only) Deleting user profiles on Cisco Unified MeetingPlace does not disable access to Cisco WebEx. You must deactivate those users through the Cisco WebEx Site Administration.
- You cannot delete the preconfigured admin, guest, or recorder user profiles.

Procedure

**Step 1** Log in to the Administration Center.

**Step 2** Select User Configuration > User Profiles.

**Step 3** Find the user profile that you want to delete.

**Step 4** Check the check box in the same row as the user profile that you want to delete. You may select multiple user profiles.

Make sure that you uncheck any check boxes for user profiles that you want to keep in the Cisco Unified MeetingPlace database.

**Step 5** Select Delete Selected.

**Step 6** When the confirmation pop-up window appears, select OK.

**Step 7** Verify that the deleted user profile does not appear in the User Profiles Page.

Related Topics

- Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Deactivating Cisco WebEx User Profiles in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module
Configuring Cisco Unified MeetingPlace Directory Service

Directory Service enables the system to populate and synchronize the Cisco Unified MeetingPlace user database with the Cisco Unified Communications Manager user database, which is typically integrated with an LDAP directory.

Specifically, Directory Service simplifies user profile administration by doing the following:

- Imports user profiles from Cisco Unified Communications Manager to Cisco Unified MeetingPlace.
- Periodically updates the Cisco Unified MeetingPlace database with new or modified user entries in the Cisco Unified Communications Manager database.
- Periodically checks the Cisco Unified Communications Manager database for inactive user entries, and deletes those user profiles from the Cisco Unified MeetingPlace database.
- Enables the system to use AXL authentication to authenticate Cisco Unified MeetingPlace Directory Service users against the external directory.
- Supports fully encrypted LDAP integration when Secure LDAP (SLDAP) is enabled on Cisco Unified Communications Manager and the LDAP server.

**Note**
SSL for the Cisco Unified MeetingPlace Application Server is not required to support Secure LDAP integration. You must, however, make sure that the configured AXL URL begins with “https” instead of “http.”

**Related Topics**
- Directory Service User Profile Configuration, page 2
- Directory Service User Profile Deletion, page 4
- Directory Service isLocalUser Setting In User Profiles, page 4
- External AXL Authentication for Directory Service Users, page 6
- Configuring Cisco Unified MeetingPlace Directory Service, page 1

### Directory Service User Profile Configuration

During the initial Directory Service import of a user profile, the fields are configured as described in Table 1. If the corresponding Cisco Unified Communications Manager user profile is modified, then the next Directory Service user profile update or full synchronization reconfigures the Cisco Unified MeetingPlace user profile fields as specified in Table 1.

**Note**
To change any of the User Profile Fields in Table 1, you must configure the corresponding Source.

<table>
<thead>
<tr>
<th>Source</th>
<th>User Profile Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>Directory Service import process</td>
<td>isLocalUser—This is always set to No in each Directory Service user profile.</td>
</tr>
</tbody>
</table>
## Table 1  
**User Profile Field Configuration Through Directory Service (continued)**

<table>
<thead>
<tr>
<th>Source</th>
<th>User Profile Fields</th>
</tr>
</thead>
</table>
| Cisco Unified Communications Manager user database | The following fields are required for creating a User Profile.  
- User ID  
- First name  
- Last name  
- Profile number  
  - Release 7.0.2 and later releases—See the “Assigning Profile Numbers to Directory Service Users” section on page 24.  
  - Release 7.0.1—Unique number based on the Telephone Number in Cisco Unified Communications Manager.  
    If the Telephone Number is not available in Cisco Unified Communications Manager, then Cisco Unified MeetingPlace randomly generates a unique Profile number during the initial import of the user profile. As long as the phone number remains unavailable in Cisco Unified Communications Manager, the Profile number is not overwritten by Directory Service user profile updates or full synchronizations.  
- User status  
- E-mail address  
- Main phone number  
The User ID field cannot be an empty value. Unless otherwise specified, the field in the Cisco Unified MeetingPlace User Profile is left blank if the corresponding field in Cisco Unified Communications Manager is empty. |
| User group filters or Group name in user profile | Group name—See the “Assigning User Groups for Directory Service Users” section on page 19. |
| Time zone filters or Time zone in user group or user profile | Time zone—See the “Assigning Time Zones to Directory Service Users” section on page 21. |
| Guest Profile (first import only) | All user profile fields not mentioned previously in this table are initially populated with the values configured in the Guest Profile. You can then modify the individual user profile fields through the Administration Center. The values will not be overwritten by Directory Service user profile updates or full synchronizations.  
Restrictions:  
- Remember that all user profile fields set to “Group default” inherit their value from the user group. If the Group name is modified through Directory Service filters or department number changes, then the user profile fields will be modified accordingly.  
- The following fields are not populated at all through Directory Service. Because Directory Service users are not authenticated by Cisco Unified MeetingPlace, these password fields are not imported and cannot be modified through Cisco Unified MeetingPlace:  
  - User password and User password confirm  
  - Profile password and Profile password confirm |
Related Topics
- Directory Service isLocalUser Setting In User Profiles, page 4
- Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Configuring Cisco Unified MeetingPlace Directory Service module

Directory Service User Profile Deletion

The system periodically checks Cisco Unified Communications Manager for inactive user entries and deletes those user profiles from Cisco Unified MeetingPlace. Specifically:

- (For Cisco Unified Communications Manager with LDAP integration) When a user is deleted or disabled in the LDAP directory, the corresponding user entry in Cisco Unified Communications Manager becomes inactive.
  Every 24 hours, Cisco Unified Communications Manager deletes user entries that have been inactive for more than 24 hours.
- Every 8 hours, Cisco Unified MeetingPlace checks the value of the Update users interval field on the Directory Service Configuration Page.
  - If the Update users interval field value is less than 24 hours, then no action is taken.
  - If the Update users interval field value is 24 hours or more, then the system checks Cisco Unified Communications Manager for any inactive users, and deactivates those users in Cisco Unified MeetingPlace by setting the User status user profile field to Inactive.
  The system does not import or update user profiles using this 8-hour cycle. Instead, the importing and updating of user profiles occurs at the configured Update users interval.
- According to the configured Update users interval, the system deletes the following user profiles from Cisco Unified MeetingPlace:
  - Users that are inactive in Cisco Unified Communications Manager.
  - Directory Service users that are inactive in Cisco Unified MeetingPlace.
  The system also imports and updates user profiles at the configured Update users interval.

Related Topics
- Directory Service User Profile Configuration, page 2
- Configuring Cisco Unified MeetingPlace Directory Service module

Directory Service isLocalUser Setting In User Profiles

Each user profile in Cisco Unified MeetingPlace includes an isLocalUser setting, which determines:

- Whether the user is authenticated externally through AXL authentication.
- How the user profile settings are configured.
**Note**  
The `isLocalUser` setting cannot be configured through the Administration Center. If you manually set `isLocalUser` to No by adding or editing user profiles by import, note that the user profiles may be affected during the next Directory Service user update:

- Any inactive user entries found in Cisco Unified Communications Manager will be deleted from the Cisco Unified MeetingPlace database.
- Some user profile fields will be overwritten by data from Cisco Unified Communications Manager and by Directory Service filters.

See the “Directory Service User Profile Configuration” section on page 2.

---

**Related Topics**

- [About Directory Service, page 1](#)
- [Adding or Editing User Profiles by Import](#)
- [Methods for Adding User Profiles](#)
External AXL Authentication for Directory Service Users

Directory Service users are those whose `isLocalUser` user profile field is set to No. Which external device authenticates a Directory Service user depends on:

- Whether the user logs in over the phone or web.
- Whether Cisco Unified Communications Manager uses LDAP directory integration.

<table>
<thead>
<tr>
<th>Directory Service User Login Method</th>
<th>Device Used to Authenticate the Directory Service User</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>With LDAP Integration</td>
</tr>
<tr>
<td>Phone</td>
<td>Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>Web</td>
<td>LDAP directory</td>
</tr>
</tbody>
</table>

Related Topics

- Directory Service `isLocalUser` Setting In User Profiles, page 4
- User Authentication for Cisco Unified MeetingPlace module
- Configuring Cisco Unified MeetingPlace Directory Service module

Restrictions for Directory Service

- Cisco Unified Communications Manager 4.x and earlier releases are not supported.
- Directory Service with two sites is not supported when Application Server Failover is in use. The database replication methods used for these options are incompatible with each other.
- The following restrictions apply to Directory Service users (users whose `isLocalUser` user profile field is set to No):
  - Because the user is not authenticated locally, the User ID, User password, and Profile password fields cannot be modified through Cisco Unified MeetingPlace by the user or by the system administrator.
  - The following password-related fields on the Usage Configuration Page do not apply to Directory Service users: Change profile password (days), Minimum user password length, Change user password (days), and Maximum profile login attempts.
  - The user profile fields that are populated by Cisco Unified Communications Manager or through Directory Service filters can be modified through Cisco Unified MeetingPlace. Nevertheless, such modifications need to be manually updated in the LDAP directory, or in Cisco Unified Communications Manager when LDAP integration is not in use. Otherwise, those modifications will be lost during the next Directory Service user update.
  - The user is always authenticated externally. Therefore, if the connection fails between Cisco Unified MeetingPlace and the authenticating device, the user cannot log in to Cisco Unified MeetingPlace.

If Cisco Unified Communications Manager fails, then you can use a redundant Cisco Unified Communications Manager for authentication only. On the Directory Service Configuration Page, temporarily change the AXL URL field to specify the redundant Cisco Unified Communications Manager, and set the Update users interval field to the largest available value (six months) to temporarily stop the database synchronization. When you select the largest
available value, the Cisco Unified MeetingPlace system ignores the Set Cisco Unified Communications Manager sync schedule to match the Update users Interval setting, even if you have it checked.

When you switch the AXL URL field back to the primary Cisco Unified Communications Manager, make sure that you also set the Update users interval field to the previous value.

The Update users interval field change is required because user updates, imports, and deletions are not supported from a redundant Cisco Unified Communications Manager, even if it is integrated with the same LDAP directory as the primary Cisco Unified Communications Manager. This is because Directory Service user updates are tied to a field that is unique to each Cisco Unified Communications Manager server.

- The maximum lengths of some user profile fields are shorter in Cisco Unified MeetingPlace than in Cisco Unified Communications Manager. Make sure that the Cisco Unified Communications Manager user field lengths do not exceed the maximum number of characters stated in Table 3.

<table>
<thead>
<tr>
<th>Table 3</th>
<th>Maximum Length of Directory Service User Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cisco Unified MeetingPlace Field</strong></td>
<td><strong>Cisco Unified Communications Manager Field</strong></td>
</tr>
<tr>
<td>First name</td>
<td>First name (FirstName)</td>
</tr>
<tr>
<td>Last name</td>
<td>Last name (LastName)</td>
</tr>
<tr>
<td>User ID</td>
<td>User ID (UserId)</td>
</tr>
<tr>
<td>E-mail address</td>
<td>Mail ID (EmailAddress)</td>
</tr>
<tr>
<td>Main phone number</td>
<td>Telephone Number (PhoneNumber)</td>
</tr>
</tbody>
</table>

- The following restrictions apply to user profile deletions, because to determine which user profiles to delete, the system periodically checks Cisco Unified Communications Manager for inactive user entries and deletes those user profiles from Cisco Unified MeetingPlace.
  - If you delete a user from Cisco Unified Communications Manager, the corresponding user profile remains in Cisco Unified MeetingPlace. You must manually delete or deactivate the user profile in Cisco Unified MeetingPlace.
  - If you replace the LDAP directory with which Cisco Unified Communications Manager is integrated, then all Directory Service users from the first LDAP directory will remain in Cisco Unified MeetingPlace database until you manually delete them.

To avoid this database clutter, you can delete all entries in the database by entering the dbupdate command before you switch from one LDAP directory to another.

Caution
Deleting all database entries is an irreversible operation. Before you run the dbupdate command, consider backing up and archiving the database. See the Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module.

Related Topics
- Directory Service isLocalUser Setting In User Profiles, page 4
- External AXL Authentication for Directory Service Users, page 6
- Directory Service User Profile Configuration, page 2
How to Configure Cisco Unified Communications Manager for Directory Service

- Activating Cisco AXL Web Services and Cisco DirSync on Cisco Unified Communications Manager, page 8
- How to Configure LDAP Integration on Cisco Unified Communications Manager, page 9
- Configuring LDAP Authentication for Cisco Unified Communications Manager, page 11
- Creating an Application User in Cisco Unified Communications Manager, page 12
- How to Configure the End User PIN in Cisco Unified Communications Manager, page 13
- Viewing the Department Number for Users in Cisco Unified Communications Manager, page 15

Activating Cisco AXL Web Services and Cisco DirSync on Cisco Unified Communications Manager

Cisco AXL Web Services enables Cisco Unified Communications Manager to perform AXL authentication for Cisco Unified MeetingPlace users. Cisco DirSync enables Cisco Unified Communications Manager to synchronize the user database with the LDAP directory.

Before You Begin
You perform this task in the Cisco Unified Serviceability pages. Because the pages and menus vary by release, you should check the Cisco Unified Serviceability online help for step-by-step instructions that are specific to your release.

Procedure

Step 1 Go to http://<ccm-server>/ccmservice/, where <ccm-server> is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
Step 2 Log in with your Cisco Unified Communications Manager administrator username and password.
Step 3 Select Tools > Service Activation.
Step 4 If not already checked, then check Cisco AXL Web Service.
Step 5 Check Cisco DirSync if you are using LDAP integration.
Step 6 Select Save.

What to Do Next
If you are using LDAP integration, the proceed to the “How to Configure LDAP Integration on Cisco Unified Communications Manager” section on page 9.
Otherwise, proceed to the “Creating an Application User in Cisco Unified Communications Manager” section on page 12.
How to Configure LDAP Integration on Cisco Unified Communications Manager

- Prerequisites for Configuring LDAP Integration on Cisco Unified Communications Manager, page 9
- Enabling LDAP Synchronization on Cisco Unified Communications Manager, page 10
- Adding an LDAP Directory to Cisco Unified Communications Manager, page 10
- Synchronizing Cisco Unified Communications Manager with the LDAP Directory, page 11

Prerequisites for Configuring LDAP Integration on Cisco Unified Communications Manager

- Complete the “Activating Cisco AXL Web Services and Cisco DirSync on Cisco Unified Communications Manager” section on page 8
- If LDAP integration is already configured for your Cisco Unified Communications Manager, then proceed to the “Creating an Application User in Cisco Unified Communications Manager” section on page 12.
- Some LDAP directories may require different or more complex configurations than the procedures described in this document. To do the following, check the System Requirements and Compatibility Matrix for Cisco Unified MeetingPlace at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html:
  - Verify that your LDAP directory is supported for use with Cisco Unified MeetingPlace.
  - See if a specific configuration is required between Cisco Unified Communications Manager and your LDAP directory.
- This document provides basic instructions for configuring LDAP integration. For detailed information, see the following documents for your version of Cisco Unified Communications Manager:
- You perform these tasks in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you may need to check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Tip
You can select Help > This Page at any time to find detailed information.

Related Topics
- How to Configure LDAP Integration on Cisco Unified Communications Manager, page 9
Enabling LDAP Synchronization on Cisco Unified Communications Manager

**Before You Begin**
Read the “Prerequisites for Configuring LDAP Integration on Cisco Unified Communications Manager” section on page 9.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Go to \http://&lt;ccm-server&gt;/ccmadmin/, where &lt;ccm-server&gt; is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Log in with your Cisco Unified Communications Manager administrator username and password.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select System &gt; LDAP &gt; LDAP System.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Check <strong>Enable Synchronizing from LDAP Server</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Choose the appropriate server type and user ID attribute.</td>
</tr>
<tr>
<td></td>
<td>You can select <strong>Help &gt; This Page</strong> at any time to find detailed information.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Select <strong>Save</strong>.</td>
</tr>
</tbody>
</table>

**What to Do Next**
Proceed to the “Adding an LDAP Directory to Cisco Unified Communications Manager” section on page 10.

Adding an LDAP Directory to Cisco Unified Communications Manager

**Before You Begin**
Complete the “Enabling LDAP Synchronization on Cisco Unified Communications Manager” section on page 10.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to Cisco Unified Communications Manager Administration:</td>
</tr>
<tr>
<td></td>
<td>a. Go to \http://&lt;ccm-server&gt;/ccmadmin/, where &lt;ccm-server&gt; is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td></td>
<td>b. Log in with your Cisco Unified Communications Manager administrator username and password.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select System &gt; LDAP &gt; LDAP Directory.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Add New</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure the fields on the LDAP Directory page.</td>
</tr>
<tr>
<td></td>
<td>You can select <strong>Help &gt; This Page</strong> at any time to find detailed information.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select <strong>Save</strong>.</td>
</tr>
</tbody>
</table>
What to Do Next
Proceed to the “Synchronizing Cisco Unified Communications Manager with the LDAP Directory” section on page 11.

Synchronizing Cisco Unified Communications Manager with the LDAP Directory

Before You Begin
Complete the “Adding an LDAP Directory to Cisco Unified Communications Manager” section on page 10.

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration:
   a. Go to http://<ccm-server>/ccmadmin/, where <ccm-server> is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
   b. Log in with your Cisco Unified Communications Manager administrator username and password.

Step 2 Select System > LDAP > LDAP Directory.

Step 3 Select Find.

Step 4 Select the name of your LDAP configuration entry.

Step 5 Select Perform Full Sync Now.

What to Do Next
Proceed to the “Configuring LDAP Authentication for Cisco Unified Communications Manager” section on page 11.

Configuring LDAP Authentication for Cisco Unified Communications Manager

Before You Begin
Complete the tasks in the “How to Configure LDAP Integration on Cisco Unified Communications Manager” section on page 9.

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration:
   a. Go to http://<ccm-server>/ccmadmin/, where <ccm-server> is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
   b. Log in with your Cisco Unified Communications Manager administrator username and password.

Step 2 Select System > LDAP > LDAP Authentication.

Step 3 Configure the fields on the LDAP Authentication page.
   You can select Help > This Page at any time to find detailed information.
Configuring Cisco Unified MeetingPlace Directory Service

How to Configure Cisco Unified Communications Manager for Directory Service

Step 4 Make sure that you check Use LDAP Authentication for End Users.

Step 5 Select Save.

What to Do Next
Proceed to the “Creating an Application User in Cisco Unified Communications Manager” section on page 12.

Creating an Application User in Cisco Unified Communications Manager

In this task, you create an AXL API user for Cisco Unified MeetingPlace to access the Cisco Unified Communications Manager AXL database for user authentication.

Before You Begin

- If either of the following statements are true, then you may skip this task and proceed to the “How to Configure the End User PIN in Cisco Unified Communications Manager” section on page 13:
  - You already have an AXL API user in the Cisco Unified Communications Manager that you want to use for Cisco Unified MeetingPlace Directory Service.
  - Instead of using an application user with standard AXL API access privileges in Cisco Unified Communications Manager, you would rather use the default administrator user, whose username and password is defined during Cisco Unified Communications Manager installation.

  Note
  If you choose to use the default administrator user, then you will need to update the AXL username or AXL password in Cisco Unified MeetingPlace whenever the Cisco Unified Communications Manager administrator username or password gets modified.

- Complete the “Configuring LDAP Authentication for Cisco Unified Communications Manager” section on page 11.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Procedure

Step 1 Log in to Cisco Unified Communications Manager Administration:
  a. Go to http://<ccm-server>/ccmadmin/, where <ccm-server> is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
  b. Log in with your Cisco Unified Communications Manager administrator username and password.

Step 2 Select User Management > Application User.

Step 3 Select Add New.

Step 4 Configure a User ID, such as mpdsaxl.

Step 5 Configure the Password and Confirm Password fields.

Step 6 Select Add to User Group.
Step 7 Find the **Standard CCM Super Users** group.

Step 8 Check the Standard CCM Super Users group.

Step 9 Select **Add Selected**.

Step 10 Select **Save**.

**What to Do Next**
Proceed to the “How to Configure the End User PIN in Cisco Unified Communications Manager” section on page 13.

**How to Configure the End User PIN in Cisco Unified Communications Manager**

The end user PIN in Cisco Unified Communications Manager is equivalent to the **Profile password** in Cisco Unified MeetingPlace. Directory Service users cannot log in to Cisco Unified MeetingPlace over the phone until the end-user PIN is changed through the Cisco Unified Communications Manager user page.

- Configuring the Credential Policy Default in Cisco Unified Communications Manager 6.x, page 13
- Configuring the End User PIN in Cisco Unified Communications Manager, page 14

**Configuring the Credential Policy Default in Cisco Unified Communications Manager 6.x**

This task enables Directory Service users to log in to Cisco Unified MeetingPlace over the phone.

**Before You Begin**

- This task applies only to Cisco Unified Communications Manager 6.x and later releases. If you are using Cisco Unified Communications Manager 5.x, then you must configure the end user PINs individually. See the “Configuring the End User PIN in Cisco Unified Communications Manager” section on page 14.
- Complete the “Creating an Application User in Cisco Unified Communications Manager” section on page 12.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release. For details about any field, select **Help > This Page**.

**Procedure**

Step 1 Go to [http://<ccm-server>/ccmadmin/](http://<ccm-server>/ccmadmin/), where `<ccm-server>` is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Log in with your Cisco Unified Communications Manager administrator username and password.

Step 3 Select **User Management > Credential Policy Default**.

Step 4 Select **Default Credential Policy** for the End User PIN.

Step 5 Enter the default PIN in the **Change Credential** and **Confirm Credential** fields.
Configuring Cisco Unified MeetingPlace Directory Service

How to Configure Cisco Unified Communications Manager for Directory Service

Step 6 To prevent toll fraud, we recommend that you check User Must Change at Next Login.

Step 7 Select Save.

Note If this setting is set, each user will have to go into http://<CUCM-ipaddress>/ccmuser and change their password. The user must in the “Cisco Unified Communications Manager User group on Cisco Unified Communications Manager to access this page.

What to Do Next
If you want to configure individual end user PINs, proceed to the “Configuring the End User PIN in Cisco Unified Communications Manager” section on page 14.
Otherwise, proceed to the “How to Configure Cisco Unified MeetingPlace for Directory Service” section on page 16.

Configuring the End User PIN in Cisco Unified Communications Manager

This task enables Directory Service users to log in to Cisco Unified MeetingPlace over the phone if a default credential policy is not in place.

Before You Begin
- Complete the “Creating an Application User in Cisco Unified Communications Manager” section on page 12
- If you are using Cisco Unified Communications Manager 6.x, then complete the “Configuring the Credential Policy Default in Cisco Unified Communications Manager 6.x” section on page 13.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release. For details about each field, select Help > This Page.

Procedure

Step 1 Go to http://<ccm-server>/ccmadmin/, where <ccm-server> is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Log in with your Cisco Unified Communications Manager administrator username and password.

Step 3 Select User Management > End User.

Step 4 Select Find.

Step 5 Select the User ID.

Step 6 Configure the PIN and Confirm PIN fields.

Step 7 If you configured a PIN that may be accessed or guessed by someone other than the intended user, then we recommend completing the following steps to prevent toll fraud:
   a. Select Edit Credential.
   b. Check User Must Change at Next Login.
   c. Select Save.
Step 8  Select Save.
Step 9  Repeat Step 5 through Step 8 for each user.

What to Do Next
Proceed to the “How to Configure Cisco Unified MeetingPlace for Directory Service” section on page 16.

Viewing the Department Number for Users in Cisco Unified Communications Manager

If you plan to configure Directory Service filters to user groups, then perform this task to obtain the department numbers for your users.

Before You Begin
You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Restrictions
If Cisco Unified Communications Manager uses LDAP directory integration, then you cannot modify the department number for users in Cisco Unified Communications Manager.

Procedure

Step 1  Go to http://<ccm-server>/ccadmin/, where <ccm-server> is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
Step 2  Log in with your Cisco Unified Communications Manager administrator username and password.
Step 3  Select User Management > End User.
Step 4  Select Find.
Step 5  Look for the numbers in the Department column.
Step 6  (Optional) Select the Department column title to sort user entries by department number.
Step 7  (Optional) In the Rows per Page field, select a larger number of entries to display.
Step 8  Use the navigation buttons in the bottom right corner to view more pages of user entries.

What To Do Next
Proceed to the “Configuring Directory Service Filters for User Groups” section on page 20.
How to Configure Cisco Unified MeetingPlace for Directory Service

- Saving and Then Clearing the User and Meeting Data on One Application Server, page 16
- Configuring User Database Replication for Two Sites, page 17
- Restoring User and Meeting Data on Application Servers, page 18
- How to Configure User Profiles for Directory Service Users, page 19
- Configuring Directory Service in Cisco Unified MeetingPlace, page 25

Saving and Then Clearing the User and Meeting Data on One Application Server

Perform this task only if the following are true:
- You have two Cisco Unified MeetingPlace sites.
- Both Application Servers contain user or meeting data that you want to keep.
- Database replication is not already in use.

Before You Begin
- On both Application Servers, perform an L0 backup. See “Backing Up Data Using the CLI” in the Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module.
- Designate one site as “Site 1,” and complete the following procedure on the Application Server in “Site 2.”

Procedure

Step 1  In the Administration Center, complete the following tasks in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module:

- Exporting User Profiles
- Exporting User Groups
- Exporting Meetings

Step 2  Log in to the CLI as the root user.

Step 3  Save user and meeting recordings by entering the following:

a.  cd /mpx-record
b.  tar cvf user-recordings.tar $MP_HOME/afs/custom/userprofile
c.  tar cvf conf-recordings.tar /mpx-record/conf

Step 4  Enter the cleardb command to delete user profiles, user groups, meetings, and recordings from the database.
Configuring User Database Replication for Two Sites

Perform this task only if you have two Cisco Unified MeetingPlace sites. User database replication enables the two sites to have synchronized user profiles and user groups.

Note
In this document, a “site” refers to a complete Cisco Unified MeetingPlace system installation, which includes one active Application Server, one active Media Server, and one or more Web Servers.

Before You Begin
- Make sure that each Application Server has only one IP address. Remove any other IP addresses by using the net command.
- Configure the Domain Name System (DNS) server for forward and reverse DNS lookup of the hostname–IP address pair for each Application Server. Verify by running the nslookup hostname and nslookup ip-address commands.
- For this task, the Application Server that contains valuable data is in “Site 1.”
- If both Application Servers contain user or meeting data that you want to keep, then designate one site as “Site 1,” and complete the “Saving and Then Clearing the User and Meeting Data on One Application Server” section on page 16 on the Application Server in “Site 2.”
- If you do not have a recent backup, run a complete L0 database backup on the Application Server that contains valuable data by completing one of the following tasks in the Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module:
  - Configuring Backups and Archiving
  - Backing Up Data Using the CLI

Restrictions
User database replication for two sites is not supported with Application Server Failover.

Procedure

Step 1
Log in to the CLI of the Application Server in Site 2.

Step 2
Enter su to get root privileges.

Step 3
Enter the following command using the hostname of the Application Server in Site 1:

mp_replication init -s2 -r hostname-site1

Step 4
Log in to the CLI of the Application Server in Site 1.

Step 5
Enter su to get root privileges.
Step 6 Enter the following commands using the hostname of the Application Server in the specified site:

```
mp_replication init -s 1 -r hostname-site2
mp_replication switchON -r hostname-site2 -S -F hostname-site1
```

These commands initiate the initial synchronization between the two sites and establishes database replication between the two sites to keep the data synchronized.

---

Related Topics

- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module

What to Do Next

If you need to restore user and meeting data from the second Application Server, then proceed to the “Restoring User and Meeting Data on Application Servers” section on page 18.

If you are configuring RSNA without Directory Service, then return to “How to Configure User Profiles for RSNA” in the Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module.

Otherwise, proceed to the “How to Configure User Profiles for Directory Service Users” section on page 19.

---

Restoring User and Meeting Data on Application Servers

Perform this task only if you have two Cisco Unified MeetingPlace sites.

Before You Begin

- Find the files that you exported in the “Saving and Then Clearing the User and Meeting Data on One Application Server” section on page 16.
- Complete the “Configuring User Database Replication for Two Sites” section on page 17.
- Perform the following procedure on only one Application Server.

Procedure

Step 1 In the Administration Center, complete the following tasks in the Importing Data into Cisco Unified MeetingPlace module:

- Adding or Editing User Groups by Import
- Adding or Editing User Profiles by Import
- Scheduling Meetings by Import

Step 2 Log in to the CLI as the `mpxadmin` user.

Step 3 Restore user and meeting recordings by entering the following:

a. `cd /mpx-record`
b. `tar xvf user-recordings.tar`
c. `tar xvf conf-recordings.tar`
Related Topics
- Importing Data into Cisco Unified MeetingPlace module

What To Do Next
If you are configuring RSNA without Directory Service, then return to “How to Configure User Profiles for RSNA” in the Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module.

Otherwise, proceed to the “How to Configure User Profiles for Directory Service Users” section on page 19.

How to Configure User Profiles for Directory Service Users

Use these tasks to specify how the system configures certain user profile settings during Directory Service user profile imports from Cisco Unified Communications Manager and during Directory Service user profile updates.

Note
To understand how all user profile fields are configured by Directory Service imports and updates, see the “Directory Service User Profile Configuration” section on page 2.

- Assigning User Groups for Directory Service Users, page 19
- Configuring Directory Service Filters for User Groups, page 20
- Assigning Time Zones to Directory Service Users, page 21
- Configuring Directory Service Filters for Time Zones, page 22
- Modifying Directory Service Filters and Applying the Filters to Previously Imported Directory Service User Profiles, page 24
- Assigning Profile Numbers to Directory Service Users, page 24

Assigning User Groups for Directory Service Users

By default, the system assigns imported Directory Service users to the System User Group.

Before You Begin
If you have multiple Application Servers for multiple sites or for Application Server Failover, perform this task on only one active Application Server.

Procedure

Step 1 Log in to the Cisco Unified MeetingPlace Administration Center.


Step 3 Configure the User groups for imported users field:
- Use filters—At first import and at each Directory Service user update, the system applies the user group filters, which assign the user group based on the department number of each imported user.
- Manually set (initially to System)—The first time each Directory Service user is imported, the user is assigned to the preconfigured System User Group. You can then manually modify the Group name user profile field, the value of which is not overwritten during future Directory Service user updates.
Step 4 Select Save.

Related Topics
- Field Reference: Directory Service Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Directory Service User Profile Configuration, page 2

What To Do Next
Proceed to the “Configuring Directory Service Filters for User Groups” section on page 20 if you set the User groups for imported users field to Use filters.
Otherwise, proceed to the “Assigning Time Zones to Directory Service Users” section on page 21.

Configuring Directory Service Filters for User Groups

Use this procedure to configure filters that assign users to specified user groups based on the Department field in Cisco Unified Communications Manager.

Before You Begin
- If you have multiple Application Servers for multiple sites or for Application Server Failover, perform this task on only one active Application Server.
- Configure the system to use Directory Service filters to assign user groups. See the “Assigning User Groups for Directory Service Users” section on page 19.
- Configure user groups. See the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module.
- Obtain the department numbers for the users. See the “Viewing the Department Number for Users in Cisco Unified Communications Manager” section on page 15.

Restrictions
If you modify existing Directory Service filters for user groups, only the following are affected:
- Subsequently imported Directory Service user profiles that did not already exist in Cisco Unified MeetingPlace.
- Subsequently updated Directory Service user profiles whose user accounts were modified in the LDAP directory or Cisco Unified Communications Manager.

To apply modified user group filters to Directory Service users that have already been imported to Cisco Unified MeetingPlace, see the “Modifying Directory Service Filters and Applying the Filters to Previously Imported Directory Service User Profiles” section on page 24.

Procedure

Step 1 Log in to the Cisco Unified MeetingPlace Administration Center.
Step 2 Select User Configuration > Directory Service > Directory Service Filters for Groups.
Step 3 Select Add New or Edit.
Step 4 Configure the fields described in Table 4.
Configuring Cisco Unified MeetingPlace Directory Service

How to Configure Cisco Unified MeetingPlace for Directory Service

21

Step 5

Select **Save**.

Related Topics

- Directory Service User Profile Configuration, page 2

What To Do Next

Proceed to the “Assigning Time Zones to Directory Service Users” section on page 21.

Assigning Time Zones to Directory Service Users

By default, the system assigns the local time of the Application Server to Directory Service users.

Before You Begin

If you have multiple Application Servers for multiple sites or for Application Server Failover, perform this task on only one active Application Server.

Procedure

**Step 1**

Log in to the Cisco Unified MeetingPlace Administration Center.

**Step 2**

Select **User Configuration > Directory Service > Directory Service Configuration**.

**Step 3**

Configure the **Time zones for imported users** field:

- Use filters—You can specify whether to apply only preconfigured, only custom, or both preconfigured and custom time zone filters. Preconfigured filters are automatically populated when you install the Application Server. The specified filters are applied to Directory Service user profiles at each **Update users interval**.

  When the same **Phone prefix** is used in a custom filter and in a preconfigured filter, the system applies the custom filter.

- Use user group settings—The time zones of the assigned user groups are reapplied to Directory Service user profiles at each **Update users interval**.

- Manually set time zones—The first time a Directory Service user is imported, the time zone of the assigned user group is applied to the user profile. You can then manually modify the **Time zone** field, the value of which is not overwritten during future Directory Service user updates.
Configuring Cisco Unified MeetingPlace Directory Service

Step 4 (Release 7.0.2 and later releases) If the following conditions apply, then configure the Custom TZ pattern length field:

- You enabled the use of custom filters in Step 3.
- Spaces or punctuation are not included in the Telephone Number field in Cisco Unified Communications Manager.

Step 5 Select Save.

Related Topics

- Field Reference: Directory Service Configuration Page in the Administration Center Page
- References for Cisco Unified MeetingPlace module
- Directory Service User Profile Configuration, page 2

What To Do Next

If you configured the Time zones for imported users field to apply custom time zone filters, then proceed to the “Configuring Directory Service Filters for Time Zones” section on page 22.
Otherwise, proceed to the “Assigning Profile Numbers to Directory Service Users” section on page 24.

Configuring Directory Service Filters for Time Zones

Use this procedure to add custom filters that configure the Region and Time zone for each Directory Service user based on the first digits of the Telephone Number field in Cisco Unified Communications Manager. The system comes with preconfigured time zone filters to which you can add custom filters.

The number of phone number digits that the system uses to match a time zone filter depends on the punctuation and spacing in the Telephone Number field in Cisco Unified Communications Manager. See Table 5. A leading “+” indicates an international number.

If there is no punctuation or spacing in the Telephone Number field in Cisco Unified Communications Manager, the system uses the first number of digits specified in the Custom TZ pattern length field to match a time zone filter.

<table>
<thead>
<tr>
<th>Sample Phone Number in Cisco Unified Communications Manager</th>
<th>Phone prefix Used to Match a Time Zone Filter</th>
</tr>
</thead>
<tbody>
<tr>
<td>+12 34 555-0123</td>
<td>+12 34</td>
</tr>
<tr>
<td>12-345-555-0123</td>
<td>12</td>
</tr>
<tr>
<td>(1234)555-0123</td>
<td>1234</td>
</tr>
<tr>
<td>123-555-0123</td>
<td>123</td>
</tr>
<tr>
<td>1235550123</td>
<td>123</td>
</tr>
</tbody>
</table>
Before You Begin

- Enable the use of custom filters. See the “Assigning Time Zones to Directory Service Users” section on page 21.
- If the system does not find a matching phone prefix, then the system assigns the local time of the Application Server.
- If you have multiple Application Servers for multiple sites or for Application Server Failover, then perform this task on only one active Application Server.

Restrictions

- You cannot modify a preconfigured filter, but you can create a custom filter that overrides the preconfigured one.
  
  If the system finds the same Phone prefix in a custom filter and in a preconfigured filter, then the system applies the custom filter.
- If you modify existing Directory Service filters for time zones, only the following are affected:
  - Subsequently imported Directory Service user profiles that did not already exist in Cisco Unified MeetingPlace.
  - Subsequently updated Directory Service user profiles whose user accounts were modified in the LDAP directory or Cisco Unified Communications Manager.

To apply modified time zone filters to Directory Service users that have already been imported to Cisco Unified MeetingPlace, see the “Modifying Directory Service Filters and Applying the Filters to Previously Imported Directory Service User Profiles” section on page 24.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Cisco Unified MeetingPlace Administration Center.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Select Add New or Edit.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure the fields described in Table 6.</td>
</tr>
</tbody>
</table>

**Table 6 Field Reference: Add Time Zone Filter Page, Edit Time Zone Filter Page, and View Time Zone Filter Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone prefix</td>
<td>The system applies this filter when this value matches the first digits of the telephone number of the imported user.</td>
</tr>
<tr>
<td>Region</td>
<td>Determines which options become available in the Time zone field.</td>
</tr>
<tr>
<td>Time zone</td>
<td>Time zone assigned to imported user profiles that match the Phone prefix.</td>
</tr>
</tbody>
</table>

Step 5 Select Save.

Related Topics

- Directory Service User Profile Configuration, page 2
Configuring Cisco Unified MeetingPlace Directory Service

How to Configure Cisco Unified MeetingPlace for Directory Service

What To Do Next
Proceed to the “Assigning Profile Numbers to Directory Service Users” section on page 24.

Modifying Directory Service Filters and Applying the Filters to Previously Imported Directory Service User Profiles

Complete this procedure only if you need to modify existing user group or time zone filters and apply those filters to Directory Service user profiles that have already been imported to Cisco Unified MeetingPlace.

Procedure

<table>
<thead>
<tr>
<th>High-Level Task</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Delete the user profiles from Cisco Unified MeetingPlace.</td>
<td>Complete one of the following tasks:</td>
</tr>
<tr>
<td></td>
<td>• Deleting a User Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td></td>
<td>• Deleting User Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td><strong>Step 2</strong> Configure the Directory Service filters for user groups.</td>
<td>Complete one or both of the following tasks:</td>
</tr>
<tr>
<td></td>
<td>• Configuring Directory Service Filters for User Groups, page 20</td>
</tr>
<tr>
<td></td>
<td>• Configuring Directory Service Filters for Time Zones, page 22</td>
</tr>
<tr>
<td><strong>Step 3</strong> Import the user profiles from Cisco Unified Communications Manager.</td>
<td>1. Go to the Directory Service Configuration Page.</td>
</tr>
<tr>
<td></td>
<td>2. Check Update Now.</td>
</tr>
<tr>
<td></td>
<td>3. Check Perform full sync with Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td></td>
<td>4. Select Save.</td>
</tr>
</tbody>
</table>

What To Do Next
Proceed to the “Configuring Directory Service in Cisco Unified MeetingPlace” section on page 25.

Assigning Profile Numbers to Directory Service Users

By default, the system assigns the Telephone Number field entry in Cisco Unified Communications Manager as the Profile number for each Directory Service user.

Before You Begin
• This configuration option was introduced in Release 7.0.2.
• If you have multiple Application Servers for multiple sites or for Application Server Failover, then perform this task on only one active Application Server.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Cisco Unified MeetingPlace Administration Center.</th>
</tr>
</thead>
</table>
Step 3  Configure the **Generate profile number using** field:

- **Use phone number as profile number**
  The system assigns the Telephone Number field entry in Cisco Unified Communications Manager as the **Profile number** for each Directory Service user.
  If the Telephone Number for a user is blank or conflicts with an existing **Profile number** in Cisco Unified MeetingPlace, then the system will instead use a six-digit auto-generated profile number.

- **Use last ‘n’ digits of phone number as profile number**
  You will specify the number of digits in **Step 4**.
  If the Telephone Number for a user is blank, or if applying this method for a user conflicts with an existing **Profile number** in Cisco Unified MeetingPlace, then the system will instead use a six-digit auto-generated profile number.

- **Use 6 digit auto-generated profile number**
  The auto-generated profile numbers start from 100001, and they always contain six digits.

Step 4  Configure the **Number of digits** field if you selected **Use last ‘n’ digits of phone number as profile number** in Step 3.

If the Telephone Number field entry for a user is shorter than the configured **Number of digits**, then the Telephone Number will be used as is as the **Profile number**.

Step 5  Configure the **Apply to** field to choose between the following options:

- Apply profile number configuration to new users only.
- Apply profile number configuration to each user profile that gets imported or updated during Directory Service user profile updates or full synchronizations.

Step 6  Select **Save**.

Related Topics

- Field Reference: Directory Service Configuration Page in the Administration Center Page
- References for Cisco Unified MeetingPlace module
- Directory Service User Profile Configuration, page 2

What To Do Next

Proceed to the “Configuring Directory Service in Cisco Unified MeetingPlace” section on page 25.

---

**Configuring Directory Service in Cisco Unified MeetingPlace**

**Before You Begin**

- Read the “Restrictions for Directory Service” section on page 6.
- Complete these tasks:
  - Creating an Application User in Cisco Unified Communications Manager, page 12
  - How to Configure User Profiles for Directory Service Users, page 19
• If you have multiple Application Servers for RSNA or for Application Server Failover:
  – Configure Directory Service only on one active Application Server.
  – Complete the “Configuring User Database Replication for Two Sites” section on page 17.

Procedure

Step 1  Log in to the Cisco Unified MeetingPlace Administration Center.


Step 3  Configure the AXL username and AXL password fields:
  • If you created an application user in Cisco Unified Communications Manager, then enter the user ID and password for that application user.
  • If you did not create an application user, then enter the username and password for the default administrator user that was configured during the installation of Cisco Unified Communications Manager.

  Note If you choose to use the default administrator user, then you will need to update the AXL username or AXL password in Cisco Unified MeetingPlace whenever the Cisco Unified Communications Manager administrator username or password gets modified.

Step 4  In the AXL URL field, enter https://ip-address:8443/axl/ using the Cisco Unified Communications Manager IP address.

Step 5  Check Update Now.

Step 6  (Release 7.0.2 and later releases) Enter the Application Server hostname in the Hostname for Active Directory Service field.

Step 7  (Optional) To modify the frequency and other settings of user profile synchronization, configure the remaining fields on the Directory Service Configuration Page.

Step 8  Select Save.

Related Topics
• Field Reference: Directory Service Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
• About Directory Service, page 1

What To Do Next
If you are configuring RSNA, then return to “How to Configure User Profiles for RSNA” in the Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module.
Changing the User Status in Cisco Unified MeetingPlace User Profiles

Active, Inactive, and Locked States

Table 1  User Status Options

<table>
<thead>
<tr>
<th>State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Users with an active user profile can log in and use Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td>Inactive</td>
<td>User with an inactive user profile cannot log in to Cisco Unified MeetingPlace. However, they may still attend meetings that are not restricted to profiled users. When an employee leaves your company, you can make the user profile inactive to preserve any meetings scheduled by that employee. If, instead, you delete the user profile, then all past meetings scheduled by that user are purged from the system.</td>
</tr>
<tr>
<td>Locked</td>
<td>Users with a locked user profile cannot log in to Cisco Unified MeetingPlace. However, like users with an inactive profile, they may still attend meetings that are not restricted to profiled users. User profiles can be locked by two methods: The system automatically locks a user profile after a configurable number of failed user login attempts. A system administrator or attendant can manually lock a user profile.</td>
</tr>
</tbody>
</table>

Related Topics

- Unlocking a User Profile, page 2
- Locking or Deactivating a User Profile, page 2
- Deleting a User Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Deleting User Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module
Unlocking a User Profile

Procedure

Step 1  Log in to the Administration Center.
Step 2  Click User Configuration > Locked Profiles.
Step 3  Check the check box in the same row as the user profile that you want to unlock. You may select multiple user profiles.
        Make sure that you uncheck any check boxes for user profiles that you do not want to unlock.
Step 4  Click Set Selected to Active.
Step 5  Click OK in the confirmation pop-up window.
Step 6  Verify that the unlocked user profile does not appear in the View Locked Profiles page.

Related Topics
  • Navigation Reference: View Locked Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
  • Active, Inactive, and Locked States, page 1
  • Locking or Deactivating a User Profile, page 2

Locking or Deactivating a User Profile

Restriction
     The system administrator profile cannot be locked.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Click User Configuration > User Profiles.
Step 3  Find the user profile that you want to lock.
Step 4  Click Edit in the same row as the user profile that you want to lock.
Step 5  Set the User status field to Locked or Inactive.
Step 6  Click Save.

Related Topics
  • Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
  • Active, Inactive, and Locked States, page 1
  • Unlocking a User Profile, page 2
Configuring Endpoints for Cisco Unified MeetingPlace

How to Configure Video Terminal Profiles

- Video Terminal Profiles
- Requirements for Inviting Video Terminal Profiles from Microsoft Outlook, page 2
- Recommended Methods for Using Video Terminal Profiles, page 3
- Adding or Editing a Video Terminal Profile, page 5
- Deleting a Video Terminal Profile, page 6

Video Terminal Profiles

You can configure video terminal profiles (VTPs) for conference room video systems and other video systems that may or may not be shared by multiple users. These profiles serve several distinct purposes:

- When scheduling video meetings through the end-user web interface, users with video-scheduling capabilities can view the availability of video terminals and can reserve one or more video terminals for the meeting. Meeting notifications list the invited video terminals.

- You may configure a VTP so that, when invited, Cisco Unified MeetingPlace will automatically dial out to the terminal at the start of the meeting. You may further configure the VTP to skip all prompts, so that no keypad input from the terminal, other than answering the call, is required to bring the terminal into the meeting.

- Many non-Cisco video terminals are incapable, for a variety of reasons, of negotiating normal entry to a Cisco Unified MeetingPlace meeting. You can set a VTP so Cisco Unified MeetingPlace will dial out to the terminal and skip all prompts. This avoids most of the complex interactions that break these negotiations. This "direct-to-meeting" mechanism allows Cisco Unified MeetingPlace to be compatible with many video terminals that are otherwise incapable of entry.
If a video terminal requires a codec other than H.264, specifically H.263 or H.261, the VTP can be set to specify which codec Cisco Unified MeetingPlace should offer the video terminal.

When Cisco Unified MeetingPlace dials out to a video terminal as a result of a web-initiated command (for example, from the Cisco WebEx Meeting Center client), if the dialed number matches a video terminal profile then (a) the codec specified in the VTP will be used and (b) video will be offered at the start of the call instead of later, at meeting entry. This causes the “direct-to-meeting” mechanism to be used when dialing out by command of a web interface, in addition to when terminals are invited at schedule time.

When dialing into Cisco Unified MeetingPlace from a video terminal, if the calling party phone number matches a VTP, the video codec set in that VTP will be offered to the terminal at the time of meeting entry.

Cisco Unified MeetingPlace is capable of sending and receiving video streams at 4CIF resolution if the terminal is capable of displaying it, the connection is negotiated to use the H.263 video codec, and the Cisco Unified MeetingPlace system is configured for high rate video mode. A VTP is required to tell Cisco Unified MeetingPlace to use H.263 instead of the default H.264.

Note

VTPs do not support the #3 outdial feature. This is because VTPs are not associated with user profiles. Individual users can have video endpoints, but such endpoints are not considered video terminals. VTPs are specifically meant for interoperating with certain kinds of video endpoints to bring in terminals that are either unable to escalate video or need to be offered video upfront. As a result, they have limited feature capabilities.

Requirements for Inviting Video Terminal Profiles from Microsoft Outlook

To enable users to invite a video terminal from the Cisco Unified MeetingPlace scheduling tab in Microsoft Outlook, you need to do the following:

- In Microsoft Exchange (Active Directory), create an end-user profile for the video terminal that includes a valid e-mail address.

- In Cisco Unified MeetingPlace, create a video terminal profile:
  - Use the same E-mail address that is in the Microsoft Exchange end-user profile.
  - Enter the correct Endpoint E.164 number for the video terminal.
  - Set the Method of attending to Outdial to terminal.

- Train your users to invite video terminals in the same way that they invite other Microsoft Exchange–profiled users.

We recommend that you standardize the names and e-mail addresses that you use for video terminals, and publish or communicate this information to your users.

Note

Inviting a video terminal from Microsoft Outlook does not reserve the resource on Cisco Unified MeetingPlace. To prevent video terminals from being double-booked, we recommend that you configure Microsoft Exchange to enable the video terminals to automatically accept and decline meeting requests, similar to conference room reservations.
Configuring Endpoints for Cisco Unified MeetingPlace

How to Configure Video Terminal Profiles

Related Topics

- Field Reference: Add Video Terminal Profile Page and Edit Video Terminal Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module

Recommended Methods for Using Video Terminal Profiles

- Direct-to-Meeting Mode for Invited Terminals, page 3
- Alternative to Direct-to-Meeting Mode for Invited Terminals, page 4
- Mode for Personal Video Terminals, page 4

Direct-to-Meeting Mode for Invited Terminals

Direct-to-meeting mode refers to the recommended method of using a video terminal that enables consistent video negotiation, specifically:

1. You configure the VTP as follows:
   a. Set the Method of attending field to Outdial to terminal.
   b. Set the Skip meeting entry voice prompts on outdial field to Yes.

2. For each meeting to which the video terminal is invited, the system dials out to the video terminal when the meeting starts.

We recommend that you:

- Configure shared video terminals, such as those in conference rooms, for direct-to-meeting mode for convenient meeting entry and to ensure successful video negotiation.
- Configure personal video terminals, such as those on individual desktops, for direct-to-meeting mode only when required for compatibility. Cisco-brand video terminals do not require video terminal profiles for compatibility.
- Train your users to invite shared video terminals while scheduling meetings.
- Train your users how to reconnect any accidentally disconnected video terminals. If a video terminal cannot rejoin the meeting by calling in or by dialing out to the video terminal, a voice meeting participant (with dial-out privileges) can press #33 to dial out to all missing invitees, including the video terminal.

Note

A side effect of the direct-to-meeting mode is that Cisco Unified MeetingPlace will not ask for a password when dialing out to the video terminal, even if a password is required for the meeting. This is because some terminals which need direct-to-meeting for compatibility are not capable of entering a password. Consider whether this behavior is acceptable before you configure a VTP for direct-to-meeting mode.

Note

While the direct-to-meeting mode permits many otherwise incompatible terminals to join a Cisco Unified MeetingPlace meeting, some features can cause connections with some finicky terminals to drop. These include entering a breakout session (#1), dialing out to another endpoint (#31), and exiting to the main menu (#9).
Alternative to Direct-to-Meeting Mode for Invited Terminals

If you do not want to configure VTPs for Direct-to-Meeting Mode for Invited Terminals, but still want to invite them to a meeting separate from inviting users, you and your users can instead use the following method to ensure successful video negotiation:

1. You set the Method of attending VTP field to “Have terminal call in.”
2. For each meeting to which the video terminal is invited, a voice meeting participant (with dial-out privileges) dials out to the video terminal and to all missing invitees by pressing #33.

If an accidentally disconnected video terminal fails to rejoin a meeting either by calling in or by dialing out to the video terminal, then a voice meeting participant (with dial-out privileges) can press #33 to reconnect to the video terminal.

If you choose this alternative method, then we recommend that you:

- Train your users how to:
  - Invite video terminals while scheduling meetings.
  - Dial out to the video terminal by pressing #33.

- Configure each VTP with a Video terminal name that includes information about how to successfully connect to the video terminal. For example:
  - Sample1 Room (#33 calls missing invitees)
  - Sample2 Room (System calls at mtg start)

**Note**

At most, only the first 60 characters of the Video terminal name will appear on the scheduling page. Depending on the specific web browser and window size, even a smaller number of characters may appear. Therefore, make sure that you use concise video terminal names.

Using an informative Video terminal name can help meeting schedulers select video terminals appropriately for their meetings, but you must train them accordingly.

- If multiple video terminals are required for a meeting, then the meeting scheduler may want to invite video terminals that have the same Method of attending.
- If the Method of attending is set to Have terminal call in, then the meeting scheduler may want to invite only video terminals and no users. Any users who are invited will also be dialed out when a meeting participant (with dial-out privileges) enters #33 in the TUI.

Mode for Personal Video Terminals

The above cases apply when Cisco Unified MeetingPlace dials out to an explicitly invited terminal, which is typically the case only for shared terminals. A VTP is also useful if a personal desktop terminal has special needs, such as:

- When dialing in from the terminal, you want to specify the video codec that will be offered to the terminal at meeting entry.
- When the dial-out call is triggered from a web interface, you want to specify the video codec and ensure that video will be offered at the beginning of the call. This ensures treatment much like the "direct-to-meeting" mode, which gives the best chance of interoperability.
When dialing in or out, the phone number of the terminal is checked against the VTP table. If there is a match, the special treatment is given to that terminal. Before checking for a match, the phone number is translated using the same tables as the Auto Attend feature.

**Adding or Editing a Video Terminal Profile**

**Before You Begin**

- To instead add or edit a batch of multiple video terminal profiles, see “Adding or Editing Video Terminal Profiles by Import” in the Importing Data into Cisco Unified MeetingPlace module.
- Create user groups before you create VTPs. The following settings can be inherited from the assigned user group:
  - Region
  - Time zone
  - All Notifications settings
This mechanism saves you from configuring those fields for individual video terminals. See “Adding or Editing a User Group Manually” in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module.
- (For Microsoft Outlook integration) Read the “Requirements for Inviting Video Terminal Profiles from Microsoft Outlook” section on page 2.
- To verify that the video terminal is compatible with Cisco Unified MeetingPlace, see the System Requirements and Compatibility Matrix for Cisco Unified MeetingPlace at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html.

**Restrictions**

Some video terminals may not consistently negotiate video unless one of the following options are used:

- Direct-to-Meeting Mode for Invited Terminals, page 3
- Alternative to Direct-to-Meeting Mode for Invited Terminals, page 4

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Select User Configuration > Video Terminal Profiles.

**Step 3** Select Add New or Edit.

**Step 4** Enter or change the values in the fields.

If you select the group default option in any field, the value that is inherited from the assigned user group appears in parentheses in that field.

**Step 5** Select Save.
Related Topics

- Field Reference: Add Video Terminal Profile Page and Edit Video Terminal Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module
- Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

What To Do Next

Proceed to “Updating All Video Terminals” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module if any of the following apply to you:

- You want a new VTP to be available immediately for meeting invitations.
- You want any modified VTP settings to take effect immediately.

Otherwise, any changes or additions you make will take effect after the next Replication Service update, which occurs nightly.

Deleting a Video Terminal Profile

Before You Begin

- To instead delete a batch of multiple video terminal profiles, see “Deleting Video Terminal Profiles by Import” in the Importing Data into Cisco Unified MeetingPlace module.
- Deleting video terminal profiles is an irreversible operation. Before you delete VTPs, consider creating a backup copy of the VTPs so that you can later retrieve the deleted video terminal profiles if necessary. Use one of the following options:
  - Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module
  - Exporting Video Terminal Profiles, page 4

Procedure

**Step 1**
Log in to the Administration Center.

**Step 2**
Select User Configuration > Video Terminal Profiles.

**Step 3**
Find the video terminal profile that you want to delete.

**Step 4**
Check the check box in the same row as the video terminal profile that you want to delete. You may select multiple entries.

Make sure that you uncheck any check boxes for video terminal profiles that you want to keep in the Cisco Unified MeetingPlace database.

**Step 5**
Select Delete Selected.

**Step 6**
When the confirmation pop-up window appears, select OK.

**Step 7**
Verify that the deleted VTP does not appear in the Video Terminal Profiles Page.
Auto-answer devices are audio or video endpoints that are incapable of entering the dual-tone multi-frequency (DTMF) signals that are required to use the telephone user interface (TUI). Many auto-answer devices automatically answer calls even when people are not present or using the device.

Related Topics
- Configuring User Profiles for Auto-Answer Devices, page 7
- Modifying When the System Disconnects Auto-Answer Devices from Meetings, page 7

Modifying When the System Disconnects Auto-Answer Devices from Meetings

To prevent auto-answer devices from wasting system resources, Cisco Unified MeetingPlace automatically disconnects auto-answer devices from meetings. Perform one of the following procedures to modify when auto-answer devices are disconnected from meetings.

Procedure for Release 7.0.2

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Meeting Configuration.
Step 3 Configure the following fields:
- Meeting controls device—If your Cisco Unified MeetingPlace system is integrated with Cisco WebEx, then set this field to Yes. Otherwise, the Cisco WebEx audio recorder will not work.
- Connected until meeting ends
- Disconnect when all continuous meeting parties leave—Set this field to Yes if the previous two fields are also set to Yes. Otherwise, the system will never automatically disconnect auto-answer devices from continuous meetings.
Step 4 (Optional) Modify the following fields which affect when auto-answer devices are disconnected and ports are released.

- Disconnect empty port (minutes)
- Early meeting port release (minutes)

Step 5 Select Save.

Procedure for Release 7.0.1

Step 1 Log in to the Administration Center.

Step 2 Select System Configuration > Remote Server Configuration.

Step 3 Configure these fields:

- Meeting controls device—If your Cisco Unified MeetingPlace system is integrated with Cisco WebEx, then set this field to Yes. Otherwise, the Cisco WebEx audio recorder will not work.
- Connected until meeting ends
- Disconnect when all continuous meeting parties leave—Set this field to Yes if the previous two fields are also set to Yes. Otherwise, the system will never automatically disconnect auto-answer devices from continuous meetings.

Step 4 Select Save.

Step 5 (Optional) Modify the Meeting Configuration Page fields that also affect when auto-answer devices are disconnected and ports are released.

a. Select System Configuration > Meeting Configuration.

b. Configure these fields:

- Disconnect empty port (minutes)
- Early meeting port release (minutes)

c. Select Save.

Related Topics

- Field Reference: Remote Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring the Cisco WebEx Audio Recorder in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module
PART

Call Configuration

- Configuring Call Control for Cisco Unified MeetingPlace
- Configuring Dial-Out Features for Cisco Unified MeetingPlace
- Configuring the Auto Attend Feature for Cisco Unified MeetingPlace
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace
- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace
Prerequisites for Configuring Call Control

- Learn the benefits and restrictions of each supported call-control deployment option, and choose the best option for your Cisco Unified MeetingPlace system. Understand your deployment so that you know ahead of time which call-control devices you need to configure. See the Planning Guide for Cisco Unified MeetingPlace at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html.


- Install the call-control devices as described in the installation documentation for those devices.

- Verify that the Cisco Unified IP Phones and other endpoints are connected and added to the database of your call-control devices.

- Verify that you can place and receive internal and external calls on the Cisco Unified IP Phones and other endpoints.


Related Topics

- Configuring Access Phone Numbers and Notification Labels module
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace module
How to Configure Call Control for Voice Conferencing

Complete this task to connect Cisco Unified MeetingPlace to supported call-control devices.

Before You Begin
Complete the “Prerequisites for Configuring Call Control” section on page 1.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Call Configuration > SIP Configuration.
Step 3 Configure the fields on the SIP Configuration Page.
Step 4 Select Save.

Related Topics

Field Reference: SIP Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module

What to Do Next
Proceed to the “Configuring Cisco Unified Communications Manager 6.x or a Later Release: SIP Trunk to Cisco Unified MeetingPlace” section on page 3.
Configuring Cisco Unified Communications Manager 6.x or a Later Release: SIP Trunk to Cisco Unified MeetingPlace

Before You Begin

- Complete the “Configuring SIP on Cisco Unified MeetingPlace” section on page 2.
- We recommend that you configure a Calling Search Space in Cisco Unified Communications Manager that does the following:
  - Allows dial-out calls to meeting participants and the help desk Attendant.
  - Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate telephone numbers.
  
- We recommend that you create a SIP trunk security profile in Cisco Unified Communications Manager specifically for Cisco Unified MeetingPlace.
  
  See “Configuring a SIP Trunk Security Profile in Cisco Unified Communications Manager for Cisco Unified MeetingPlace” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.
- If you want to prevent conference disruption by music when a user places a call on hold, then complete the “Configuring Cisco Unified Communications Manager: Music On Hold” task in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Procedure

Step 1 Go to http://ccm-server/, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Log in with your Cisco Unified Communications Manager administrator username and password.

Step 3 Select Device > Trunk.

Step 4 Select Add New.

Step 5 In the Trunk type field, select SIP Trunk.

Step 6 Select Next.

Step 7 Configure the fields described in Table 1.
### Table 1  
**Fields for Adding a SIP Trunk in Cisco Unified Communications Manager 6.x or a Later Release**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter a unique identifier for this trunk, such as the name or IP address of the Cisco Unified MeetingPlace server.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>The device pool must use a codec that is compatible with the conferencing gateway (or bridge). For security and toll fraud prevention, use a device pool and an automatic alternate routing (AAR) group that will block any undesired phone numbers from being dialed out.</td>
</tr>
<tr>
<td>AAR Group</td>
<td></td>
</tr>
</tbody>
</table>
| Media Resource Group List     | (Optional) If Cisco Unified MeetingPlace–supported endpoints are registered to this Cisco Unified Communications Manager, then we recommend that you choose one of the following to prevent conference calls from being disrupted by music whenever a user places a call on hold:  
  - Default value of <None>.  
  - A Media Resource Group List that does not contain music on hold resources.  
  
  **Note** See “Configuring Cisco Unified Communications Manager: Music On Hold” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module. |
| Media Termination Point Required | Uncheck this check box.                                                                                                                                                                                 |
| Destination Address           | The DNS hostname or IP address of the Cisco Unified MeetingPlace Application Server. In an Application Server Failover deployment, make sure you enter the shared hostname and IP address of eth0.                     |
| Destination Port              | Keep the default value of 5060.                                                                                                                                                                            |
| SIP Trunk Security Profile    | Select the SIP trunk security profile that you created specifically for Cisco Unified MeetingPlace. If you did not create a SIP trunk security profile, then select the default Non Secure SIP Trunk Profile. |
| Rerouting Calling Search Space| Make sure you set this value appropriately to ensure that call transfers (out to attendant or other systems) are successful. Consult your Communications Manager administrator for the appropriate CSS to use. |
| DTMF Signaling Method         | Select No Preference.                                                                                                                                                                                   |

**Step 8** Configure all other required fields appropriately for your current deployment.

If you configured a Calling Search Space to block unwanted dial-out calls, then apply the Calling Search Space accordingly to the SIP trunk.

**Tip** For field descriptions, select Help > This Page.

**Step 9** Select Save.
Configuring Cisco Unified Communications Manager 6.x or a Later Release: Route Patterns

Route patterns enable Cisco Unified Communications Manager to route calls to Cisco Unified MeetingPlace by associating phone numbers with the SIP trunk.

Before You Begin

- Complete the “Configuring Cisco Unified Communications Manager 6.x or a Later Release: SIP Trunk to Cisco Unified MeetingPlace” section on page 3.
- Write down each of the following phone numbers from the Cisco Unified MeetingPlace Administration Center:
  - Access phone numbers configured on the Usage Configuration Page
  - Direct Inward Dial (DID) numbers—only if you enable DID through the Route calls to meeting ID that matches DID field
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Procedure

Step 1  Go to http://ccm-server/, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2  Log in with your Cisco Unified Communications Manager administrator username and password.

Step 3  Select Call Routing > Route/Hunt > Route Pattern.

Step 4  Select Add New.

Step 5  Configure the fields described in Table 2.
How to Configure Call Control for Voice Conferencing

Step 6 Configure all other required fields appropriately for your current deployment.

Tip
For field descriptions, select Help > This Page.

Step 7 Select Save.

Step 8 Select OK to any pop-up dialog box messages that you see.

Step 9 Repeat this procedure as necessary to route calls to each access phone number and DID number for your Cisco Unified MeetingPlace system.

### Table 2 Fields for Adding a Route Pattern in Cisco Unified Communications Manager 6.x or a Later Release

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Pattern</td>
<td>Enter the Cisco Unified MeetingPlace phone number.</td>
</tr>
<tr>
<td>Requirements:</td>
<td>• This number must not conflict with any other route pattern defined in this Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter any spaces in this field.</td>
</tr>
<tr>
<td>Gateway/Route List</td>
<td>Select the Device Name of the SIP trunk to Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td>Call Classification</td>
<td>Select OnNet.</td>
</tr>
<tr>
<td>Provide Outside Dial Tone</td>
<td>Uncheck the check box.</td>
</tr>
</tbody>
</table>

### Related Topics
- SIP Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Access Phone Numbers and Notification Labels module
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace module

### What to Do Next
If you are using Cisco Unified Communications Manager 6.1 or a later release to provide front-end signaling for Cisco Unified MeetingPlace, then proceed to one of the following sections:

- Configuring SIP Trunks Between Cisco Unified Communications Manager 5.x and Cisco Unified MeetingPlace 6.1 or a Later Release, page 7
- Configuring Inter-Cluster Trunks Between Cisco Unified Communications Manager 4.x or 5.x and Cisco Unified Communications Manager 6.1 or a Later Release, page 9

Otherwise, proceed to the “Verifying the Call-Control Configuration” section on page 13.
Configuring SIP Trunks Between Cisco Unified Communications Manager 5.x and Cisco Unified MeetingPlace 6.1 or a Later Release

Perform this task if you have already deployed Cisco Unified Communications Manager 5.x and are using Cisco Unified Communications Manager 6.1 or a later release to provide front-end signaling for Cisco Unified MeetingPlace.

Before You Begin

- You may instead choose to configure inter-cluster trunks (instead of SIP trunks) between Cisco Unified Communications Manager 5.x and Cisco Unified Communications Manager 6.1 or a later release. If this is the case, then do not perform this task. Instead, see the “Configuring Inter-Cluster Trunks Between Cisco Unified Communications Manager 4.x or 5.x and Cisco Unified Communications Manager 6.1 or a Later Release” section on page 9.
- Complete the “Configuring Cisco Unified Communications Manager 6.x or a Later Release: Route Patterns” section on page 5.
- Perform this task on both of the following servers:
  - Cisco Unified Communications Manager 5.x
  - Cisco Unified Communications Manager 6.1 or a later release
- We recommend that you configure a Calling Search Space in Cisco Unified Communications Manager that does the following:
  - Allows dial-out calls to meeting participants and the help desk Attendant.
  - Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate telephone numbers.


- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Procedure

**Step 1** Go to [http://ccm-server/ccmadmin/main.asp](http://ccm-server/ccmadmin/main.asp), where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

**Step 2** Log in with your Cisco Unified Communications Manager administrator username and password.

**Step 3** Select Device > Trunk.

**Step 4** Select Add New.

**Step 5** In the Trunk Type field, select SIP Trunk.

**Step 6** Select Next.

**Step 7** Configure the fields described in Table 3.
Step 8 Configure all other required fields appropriately for your current deployment.

If you configured a Calling Search Space to block unwanted dial-out calls, then apply the Calling Search Space accordingly to the SIP trunk.

Tip For field descriptions, select Help > This Page.

Step 9 Select Save.
Step 10  Repeat this task so that both of the following servers are configured with SIP trunks that point to each other:

- Cisco Unified Communications Manager 5.x
- Cisco Unified Communications Manager 6.1 or a later release

Related Topics
- Configuring Operator Assistance in the Configuring Attendant Settings for Cisco Unified MeetingPlace module

What to Do Next
Proceed to the “Configuring Cisco Unified Communications Manager 4.x or 5.x: Route Patterns” section on page 11.

Configuring Inter-Cluster Trunks Between Cisco Unified Communications Manager 4.x or 5.x and Cisco Unified Communications Manager 6.1 or a Later Release

Perform this task if you already deployed Cisco Unified Communications Manager 4.x or 5.x and are using Cisco Unified Communications Manager 6.1 or a later release to provide front-end signaling for Cisco Unified MeetingPlace.

Before You Begin
- You may instead choose to configure SIP trunks (instead of inter-cluster trunks) between Cisco Unified Communications Manager 5.x and Cisco Unified MeetingPlace 6.1 or a later release. If this is the case, then do not perform this task. Instead, see the “Configuring SIP Trunks Between Cisco Unified Communications Manager 5.x and Cisco Unified MeetingPlace 6.1 or a Later Release” section on page 7.
- Complete the “Configuring Cisco Unified Communications Manager 6.x or a Later Release: Route Patterns” section on page 5.
- Perform this task on both of the following servers:
  - Cisco Unified Communications Manager 4.x or 5.x
  - Cisco Unified Communications Manager 6.1 or a later release
- We recommend that you configure a Calling Search Space in Cisco Unified Communications Manager that does the following:
  - Allows dial-out calls to meeting participants and the help desk Attendant.
  - Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate telephone numbers.
  - Allows dial-out calls to meeting participants and the help desk Attendant.
  - Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate telephone numbers.
  - Allows dial-out calls to meeting participants and the help desk Attendant.
  - Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate telephone numbers.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.
How to Configure Call Control for Voice Conferencing

**Procedure**

**Step 1** Go to http://ccm-server/ccmadmin/main.asp, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

**Step 2** Log in with your Cisco Unified Communications Manager administrator username and password.

**Step 3** Select Device > Trunk.

**Step 4** Select Add New.

**Step 5** In the Trunk type field, select Inter-Cluster Trunk (Non-Gatekeeper Controlled).

**Step 6** Select Next.

**Step 7** Configure the fields described in Table 4.

**Table 4 Fields for Adding an Inter-Cluster Trunk in Cisco Unified Communications Manager**

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter a unique identifier for this trunk, for example:</td>
</tr>
<tr>
<td></td>
<td>- If you are configuring Cisco Unified Communications Manager 4.x or 5.x, then enter the name or IP address of the Cisco Unified Communications Manager 6.1 (or a later release) server that provides front-end signaling for Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td></td>
<td>- If you are configuring Cisco Unified Communications Manager Release 6.1 (or a later release), then enter the name or IP address of the Cisco Unified Communications Manager 4.x or 5.x server.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>If no device pools are defined, select Default.</td>
</tr>
<tr>
<td></td>
<td>If device pools are already defined, then either create a new device pool or choose an existing device pool for a region with a codec that is compatible with the conferencing gateway (or bridge).</td>
</tr>
<tr>
<td>Media Resource Group List</td>
<td>(Optional) If Cisco Unified MeetingPlace–supported endpoints are registered to this Cisco Unified Communications Manager, then we recommend that you choose one of the following to prevent conference calls from being disrupted by music whenever a user places a call on hold:</td>
</tr>
<tr>
<td></td>
<td>- Default value of &lt;None&gt;.</td>
</tr>
<tr>
<td></td>
<td>- A Media Resource Group List that does not contain music on hold resources.</td>
</tr>
<tr>
<td>Note</td>
<td>See “Configuring Cisco Unified Communications Manager: Music On Hold” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.</td>
</tr>
<tr>
<td>Media Termination Point</td>
<td>Uncheck this check box.</td>
</tr>
<tr>
<td>Required</td>
<td>Identify the target server, specifically:</td>
</tr>
<tr>
<td>Server 1 IP Address/Host Name</td>
<td>- If you are configuring Cisco Unified Communications Manager 4.x or 5.x, then specify the Cisco Unified Communications Manager 6.1 (or a later release) server that provides front-end signaling for Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td></td>
<td>- If you are configuring Cisco Unified Communications Manager Release 6.1 (or a later release), then specify the Cisco Unified Communications Manager 4.x or 5.x server.</td>
</tr>
</tbody>
</table>
Step 8 Configure all other required fields appropriately for your current deployment.

If you configured a Calling Search Space to block unwanted dial-out calls, then apply the Calling Search Space accordingly to the SIP trunk.

Tip For field descriptions, select Help > This Page.

Step 9 Select Save.

Step 10 Repeat this task so that both of the following servers are configured with SIP trunks that point to each other:

- Cisco Unified Communications Manager 4.x or 5.x
- Cisco Unified Communications Manager 6.1 or a later release

What to Do Next
Proceed to the “Configuring Cisco Unified Communications Manager 4.x or 5.x: Route Patterns” section on page 11.

Configuring Cisco Unified Communications Manager 4.x or 5.x: Route Patterns

Use this procedure to configure route patterns to enable Cisco Unified Communications Manager 4.x or 5.x to route calls that are placed to Cisco Unified MeetingPlace phone numbers. The route patterns associate the Cisco Unified MeetingPlace phone numbers with one of the following, depending on your deployment:

- Inter-cluster trunk to the Cisco Unified Communications Manager Release 6.1 (or a later release) server that provides front-end signaling for Cisco Unified MeetingPlace
- (Cisco Unified Communications Manager 5.x only) SIP trunk to the Cisco Unified Communications Manager Release 6.1 (or a later release) server that provides front-end signaling for Cisco Unified MeetingPlace

Before You Begin

- Complete the “Configuring SIP on Cisco Unified MeetingPlace” section on page 2.
- Complete one of the following items, depending on your deployment:
  - Configuring SIP Trunks Between Cisco Unified Communications Manager 5.x and Cisco Unified MeetingPlace 6.1 or a Later Release, page 7
  - Configuring Inter-Cluster Trunks Between Cisco Unified Communications Manager 4.x or 5.x and Cisco Unified Communications Manager 6.1 or a Later Release, page 9
- Write down each of the following phone numbers from the Cisco Unified MeetingPlace Administration Center:
  - Access phone numbers configured on the Usage Configuration Page
  - Direct Inward Dial (DID) numbers—only if you enable DID through the Route calls to meeting ID that matches DID field
• You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Procedure

Step 1 Go to http://ccm-server/ccmadmin/main.asp, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2 Log in with your Cisco Unified Communications Manager administrator username and password.

Step 3 Select Call Routing > Route/Hunt > Route Pattern.

Step 4 Select Add New.

Step 5 Configure the fields described in Table 5.

Table 5 Fields for Adding a Route Pattern in Cisco Unified Communications Manager 4.x or 5.x

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Route Pattern</td>
<td>Enter the Cisco Unified MeetingPlace phone number.</td>
</tr>
<tr>
<td></td>
<td>Requirements:</td>
</tr>
<tr>
<td></td>
<td>• This number must not conflict with any other route pattern defined in this Cisco Unified Communications Manager cluster.</td>
</tr>
<tr>
<td></td>
<td>• Do not enter any spaces in this field.</td>
</tr>
</tbody>
</table>

| Gateway/Route List     | Select the Device Name of one of the following, depending on your deployment: |
|                        | • Inter-cluster trunk to the Cisco Unified Communications Manager Release 6.1 (or a later release) server that provides front-end signaling for Cisco Unified MeetingPlace. |
|                        | • (Cisco Unified Communications Manager 5.x only) SIP trunk to the Cisco Unified Communications Manager Release 6.1 (or a later release) server that provides front-end signaling for Cisco Unified MeetingPlace. |

| Call Classification    | Select OffNet.                                                          |

Step 6 Configure all other required fields appropriately for your current deployment.

Tip For field descriptions, select Help > This Page.

Step 7 Select Save.

Step 8 Select OK to any pop-up dialog box messages that you see.

Step 9 Repeat this procedure as necessary to route calls to each access phone number and DID number for your Cisco Unified MeetingPlace system.

Related Topics

• Configuring Access Phone Numbers and Notification Labels module
• Configuring Direct Inward Dial for Cisco Unified MeetingPlace module
What to Do Next
Proceed to the “Verifying the Call-Control Configuration” section on page 13.

Verifying the Call-Control Configuration

Procedure

Step 1 Call one of the Cisco Unified MeetingPlace access phone numbers configured on the Usage Configuration Page of the Administration Center.

Step 2 Verify that you hear the Cisco Unified MeetingPlace voice prompts.

Troubleshooting Tips
See the Troubleshooting Telephone Issues for Cisco Unified MeetingPlace module.

Related Topics
- Verifying Basic Voice and Video Conferencing Using the Telephone User Interface in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing module
- Verifying Basic Voice and Video Conferencing Using the End-User Web Interface in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing module
- Configuring Access Phone Numbers and Notification Labels module
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace module

What To Do Next
- If your network includes H.323 video endpoints, proceed to the “How to Configure Call Control for Video Conferencing with H.323 Endpoints” section on page 13.
- For Cisco Unified Communications Manager environments, we recommend disabling the Music on Hold (MoH) feature for Cisco Unified MeetingPlace. See “Configuring Cisco Unified Communications Manager: Music On Hold” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.

How to Configure Call Control for Video Conferencing with H.323 Endpoints

- How to Configure the Cisco IOS Gatekeeper, page 14
- Configuring Cisco Unified Communications Manager 6.1 or a Later Release: H.323 Endpoints, page 17
How to Configure the Cisco IOS Gatekeeper

Perform one of the following tasks, depending on which device provides dial plan resolution for your network:

- Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided By Gatekeeper, page 14
- Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided by Cisco Unified Communications Manager, page 15

Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided By Gatekeeper

Choose this configuration option if the Cisco IOS gatekeeper provides dial plan resolution for all devices in your network.

Before You Begin

- Configure voice call control. See the “How to Configure Call Control for Voice Conferencing” section on page 2.
- Configure the gatekeeper Cisco Unified Communications Manager. For instructions on adding the gatekeeper, see the Cisco Unified Communications Manager online help.
- You perform this task in the Cisco IOS command-line interface (CLI) of the router. For more information about the Cisco IOS commands used in this procedure, see the Cisco IOS Commands Master List for your Cisco IOS release.

Procedure

Step 1 On the Cisco router, enter privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.

Router# enable

Step 2 Enter global configuration mode.

Router# configure terminal

Step 3 Enter gatekeeper configuration mode.

Router# gatekeeper

Step 4 Define the zone controlled by the gatekeeper.

Router(config-gk)# zone local gk-zone-name domain-name

Step 5 Specify which subnets the gatekeeper will accept discovery and registration messages sent by endpoints in those subnets.

Router(config-gk)# no zone subnet gk-zone-name default enable
Router(config-gk)# zone subnet gk-zone-name subnet1-address(/bits-in-mask | mask-address) enable
Router(config-gk)# zone subnet gk-zone-name subnet2-address(/bits-in-mask | mask-address) enable
**Step 6**  Define a technology prefix, which is stripped before checking for the zone prefix. Configure calls to hop off at the gatekeeper, regardless of the zone prefix in the destination address. The **default-technology** option specifies to use gateways registering with this prefix option as the default for routing any addresses that are otherwise unresolved.

Router(config-gk)# gw-type-prefix type-prefix hopoff gk-zone-name default-technology

**Step 7**  Disable proxy communications with local terminals for calls between local and remote zones.

Router(config-gk)# no use-proxy gk-zone-name default inbound-to terminal
Router(config-gk)# no use-proxy gk-zone-name default outbound-from terminal

**Step 8**  Enable the gatekeeper.

Router(config-gk)# no shutdown

---

**Example**

```
! gateway
   zone local mp2-video example.com
   no zone subnet mp2-video default enable
   zone subnet mp2-video 10.20.120.50/32 enable
   zone subnet mp2-video 10.10.1.0/24 enable
   gw-type-prefix 2#* hopoff mp2-video default-technology
   no use-proxy mp2-video default inbound-to terminal
   no use-proxy mp2-video default outbound-from terminal
   no shutdown
!
```

**What to Do Next**

Proceed to one of the following sections in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing module:

- Verifying Basic Voice and Video Conferencing Using the Telephone User Interface
- Verifying Basic Voice and Video Conferencing Using the End-User Web Interface

**Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided by Cisco Unified Communications Manager**

Choose this configuration option if the following are true:

- All H.323 video endpoints register to this Cisco IOS gatekeeper.
- Cisco Unified Communications Manager provides dial plan resolution and becomes the master call-control point for all devices in your network.

**Before You Begin**

- Configure voice call control. See the “How to Configure Call Control for Voice Conferencing” section on page 2.
- Add this gatekeeper to Cisco Unified Communications Manager. For instructions on adding the gatekeeper, see the Cisco Unified Communications Manager online help.
- You perform this task in the Cisco IOS command-line interface (CLI) of the router. For more information about the Cisco IOS commands used in this procedure, see the Cisco IOS Commands Master List for your Cisco IOS release.
Procedure

Step 1  On the Cisco router, enter privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.

Router# enable

Step 2  Enter global configuration mode.

Router# configure terminal

Step 3  Enter gatekeeper configuration mode.

Router# gatekeeper

Step 4  Define the zone controlled by the gatekeeper. Specify which gatekeeper interface to use for Registration, Admission, and Status (RAS) signaling. Force all intra-zone calls, in addition to calls that enter and leave the zone, to use this gatekeeper.

Router(config-gk)# zone local gk-zone-name domain-name ras-IP-address invia gk-zone-name outvia gk-zone-name enable-intrazone

Step 5  Define a technology prefix that matches what you configure for the H.323 endpoints in Cisco Unified Communications Manager. The default-technology option specifies to use gateways registering with this prefix option as the default for routing any addresses that are otherwise unresolved.

Router(config-gk)# gw-type-prefix type-prefix default-technology

Step 6  Disable proxy communications with local terminals for calls between local and remote zones.

Router(config-gk)# no use-proxy local-zone-name default inbound-to terminal
Router(config-gk)# no use-proxy local-zone-name default outbound-from terminal

Step 7  Enable the gatekeeper.

Router(config-gk)# no shutdown

Example

```
! gatekeeper
zone local MP-Zone1 example.net 192.168.2.50 invia MP-Zone1 outvia MP-Zone1 enable-intrazone
! gw-type-prefix 1* default-technology
no use-proxy MP-Zone1 default inbound-to terminal
no use-proxy MP-Zone1 default outbound-from terminal
no shutdown
!```

What To Do Next

Proceed to the “Configuring Cisco Unified Communications Manager 6.1 or a Later Release: H.323 Endpoints” section on page 17.
Configuring Cisco Unified Communications Manager 6.1 or a Later Release: H.323 Endpoints

Perform this task only if Cisco Unified Communications Manager provides dial plan resolution for your network.

**Before You Begin**
- Complete the “Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided by Cisco Unified Communications Manager” section on page 15.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

**Procedure**

1. Go to http://ccm-server/, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Log in with your Cisco Unified Communications Manager administrator username and password.
3. Select Device > Phone.
4. (Optional) To display a list of existing phone entries, select Find.
5. Select Add New.
6. Select H.323 Client in the Phone Type field.
7. Select Next.
8. Configure the fields described in Table 6.

**Table 6**  Fields for Adding an H.323 Endpoint in Cisco Unified Communications Manager 6.1 or a Later Release

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter the IP address of the H.323 endpoint.</td>
</tr>
<tr>
<td>Device Pool</td>
<td>Select Default.</td>
</tr>
<tr>
<td>Outgoing Caller ID Pattern</td>
<td>Enter the extension or phone number of the H.323 endpoint.</td>
</tr>
<tr>
<td>Gatekeeper Name</td>
<td>Select the gatekeeper that you configured in the “Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided by Cisco Unified Communications Manager” section on page 15.</td>
</tr>
<tr>
<td>E.164</td>
<td>Enter the E.164 phone number used by the H.323 endpoint.</td>
</tr>
<tr>
<td>Technology Prefix</td>
<td>Enter the technology prefix (type-prefix) that you configured in Step 5 in the “Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided by Cisco Unified Communications Manager” section on page 15.</td>
</tr>
<tr>
<td>Zone</td>
<td>Enter the zone name (gk-zone-name) that you configured in Step 4 in the “Configuring the Cisco IOS Gatekeeper: Dial Plan Resolution Provided by Cisco Unified Communications Manager” section on page 15.</td>
</tr>
</tbody>
</table>
**Step 9**  Configure all other required fields appropriately for your current deployment.

**Tip**  For field descriptions, select *Help > This Page*.

**Step 10**  Select *Save*.

**Step 11**  Select *OK* to any pop-up dialog box messages that you see.

**Step 12**  Repeat this procedure to add each H.323 endpoint to Cisco Unified Communications Manager.

**What to Do Next**

Proceed to one of the following sections in the *Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing* module:

- Verifying Basic Voice and Video Conferencing Using the Telephone User Interface
- Verifying Basic Voice and Video Conferencing Using the End-User Web Interface
Dial-Out Features and Voice Prompt Languages

Dial-out features allow users to quickly and easily join meetings and add other users to meetings in session. Table 1 describes the Cisco Unified MeetingPlace dial-out features, which can be initiated only by users with the “Can call out of meetings” field set to Yes in their user profiles.

Table 1 also specifies which voice prompt language each dial-out feature uses. During active meetings, however, voice prompts heard by all meeting participants use the meeting language. If the meeting language is not specified while scheduling the meeting, then the Language configured in the user profile of the meeting owner becomes the meeting language.
About the Find Me Feature

With the Find Me dial-out feature, Cisco Unified MeetingPlace calls the meeting invitees when a meeting begins. This feature is available only to profiled users and can be enabled or disabled in each user profile. Cisco Unified MeetingPlace can call up to three devices, in the order specified in the user profile, to try to reach the user.

- Supported Devices for the Find Me Feature, page 2
- How the Find Me Feature Works with Pagers, page 3
- Restrictions for Using the Find Me Feature with Pagers, page 3

Supported Devices for the Find Me Feature

Cisco Unified MeetingPlace can call the following devices, in the order specified in the user profile:

- Phone—The person who answers the phone is prompted to join the meeting. Depending on the user profile and meeting configurations, the person may also be prompted for a user password or meeting password.
- Direct-dial pager—Pager is directly reached by a phone number.
- Non-direct-dial pager—Pager is reached by a phone number and a PIN.
### How the Find Me Feature Works with Pagers

Both direct- and non-direct-dial pagers display the following items in a single numeric string:

- Phone number entered in the Access phone number 1 field in the Usage Configuration page
- Meeting ID

When you have configured the Find Me feature to call a pager, the following behavior applies.

<table>
<thead>
<tr>
<th>Direct-Dial Pager</th>
<th>Non-Direct-Dial pager</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. When the meeting begins, Cisco Unified MeetingPlace dials the pager service by using the phone number that is configured in the Pager number user profile field.</td>
<td>1. When the meeting begins, Cisco Unified MeetingPlace dials the pager service by using the phone number that is configured in the Phone number for non-direct-dial pagers user group field.</td>
</tr>
<tr>
<td>2. After the pager service answers, Cisco Unified MeetingPlace sends its own access phone number, which is configured in the Access phone number 1 field in the Usage Configuration page.</td>
<td>2. Cisco Unified MeetingPlace sends the pager-specific PIN or user ID, which is configured in the Pager number user profile field.</td>
</tr>
<tr>
<td>3. Cisco Unified MeetingPlace sends the meeting ID.</td>
<td>3. After the pager service answers, Cisco Unified MeetingPlace sends its own system access phone number, which is configured in the Access phone number 1 field in the Usage Configuration page.</td>
</tr>
<tr>
<td>4. Cisco Unified MeetingPlace sends the meeting ID.</td>
<td>4. Cisco Unified MeetingPlace sends the meeting ID.</td>
</tr>
</tbody>
</table>

### Restrictions for Using the Find Me Feature with Pagers

The following restrictions apply when you have configured the Find Me feature to call pagers:

- Only numeric pager output is supported. From the Access phone number 1 field in the Usage Configuration page, only the characters 0-9, #, and * are processed and sent to pagers. All other characters are discarded.
- In the pager output, there is no indication of where the access phone number ends and where the meeting ID begins. These values are combined into a single numeric string in the pager output.
The pager output does not include meeting passwords.

- If the length of the numeric string sent to the pager exceeds the pager limit, then the pager will not be able to display all the digits.

Cisco Unified MeetingPlace sends RFC 2833 digits in the Real-Time Transport Protocol (RTP) stream. These pager digits must be converted to in-band audio dual-tone multi-frequency (DTMF) signals. The gateway that converts the VoIP traffic in your network to the public switched telephone network (PSTN) must convert RFC 2833 digits to in-band DTMF signals. See the documentation for your specific gateway and software release to verify this capability.

Cisco Unified MeetingPlace cannot send pager digits in the following ways:
- In the SIP signaling stream or channel
- Directly as in-band audio DTMF signals

There may be a significant delay between when Cisco Unified MeetingPlace calls a pager and when the pager vibrates, flashes, or beeps. If the Search order for find me user profile field is configured to call a phone after calling a pager, then the phone may receive the call before the pager vibrates, flashes, or beeps. Therefore, we recommend that you or the end user take one or both of the following actions:
  - Select Pager in only the Third option of the Search order for find me user profile field.
  - If the user wants to receive only a page and no phone calls when a meeting begins, then leave the Main phone number and Alternate phone number user profile fields blank.

You cannot select Pager more than once in the Search order for find me user profile field, but leaving the Main phone number and Alternate phone number user profile fields blank effectively disables those options.

Related Topics
- About the Find Me Feature, page 2
- Configuring the Find Me Dial-Out Feature, page 5
- Dial-Out Features and Voice Prompt Languages, page 1

Enabling Dial-Out Privileges for Users

Before You Begin
If you want to configure the Find Me dial-out feature, then instead see the “Configuring the Find Me Dial-Out Feature” section on page 5.

Procedure

1. Log in to the Administration Center.
2. Select User Configuration.
3. Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.
4. Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.
Configuring Dial-Out Features for Cisco Unified MeetingPlace

Configuring the Find Me Dial-Out Feature

Before You Begin
Read the “About the Find Me Feature” section on page 2.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration.
Step 3 Configure user groups:
   a. Select User Groups.
   b. To configure an existing user group, select Edit. To configure a new user group, select Add New.
   c. Configure these fields:

<table>
<thead>
<tr>
<th>User Group Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone number for non-direct-dial pagers</td>
<td>(Required only for non-direct dial pagers)</td>
</tr>
<tr>
<td></td>
<td>Phone number to access the pager system</td>
</tr>
<tr>
<td>Can dial out (does not apply to Cisco WebEx meetings)</td>
<td>(Optional) Yes</td>
</tr>
<tr>
<td>Ask for profile password</td>
<td>(Optional) Yes</td>
</tr>
</tbody>
</table>

   d. Select Save.

Note If you want to enable dial-out privileges for guest users, then edit the guest user profile.

Step 5 Set Can dial out (does not apply to Cisco WebEx meetings) to Yes.
Step 6 (Optional) Set Ask for profile password to Yes.
Step 7 Select Save.
Step 8 Repeat this procedure for all user groups and user profiles for which you want to enable dial-out privileges.

Related Topics
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center
- Dial-Out Features and Voice Prompt Languages, page 1
- Restricting Dial-Out Privileges for Guest Users in the Securing the Cisco Unified MeetingPlace System module
- Restricting Dial-Out Privileges for Profiled Users in the Securing the Cisco Unified MeetingPlace System module
e. Repeat Step 3 for all user groups for which you want to configure the Find Me feature.

**Step 4**

Configure user profiles:

a. Select **User Profiles**.

b. To configure an existing user profile, select **Edit**. To configure a new user profile, select **Add New**.

c. Configure these fields:

<table>
<thead>
<tr>
<th>User Profile Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group name</td>
<td>(Required only for non-direct dial pagers) User group configured in Step 3 with the correct Phone number for non-direct-dial pagers.</td>
</tr>
<tr>
<td>Main phone number</td>
<td>Configure at least one phone or pager number.</td>
</tr>
<tr>
<td>Alternate phone number</td>
<td></td>
</tr>
<tr>
<td>Alternate phone number 2</td>
<td></td>
</tr>
<tr>
<td>Pager number</td>
<td></td>
</tr>
<tr>
<td>Method of attending</td>
<td>Have system find user</td>
</tr>
<tr>
<td>Search order for find me</td>
<td>Order in which the system should attempt to call the user</td>
</tr>
<tr>
<td>Can dial out (does not apply to Cisco WebEx meetings)</td>
<td>Yes or Group Default (Yes)</td>
</tr>
<tr>
<td>Ask for profile password</td>
<td>(Optional) Yes or Group Default (Yes)</td>
</tr>
</tbody>
</table>

d. Select **Save**.

e. Repeat Step 4 for all user profiles for which you want to configure the Find Me feature.

**Step 5**

(Optional) Configure the system dial-out settings:

a. Select **System Configuration > Usage Configuration**.

b. Configure these fields:

   - **Number of retry attempts**
   - **Delay between retries (sec)**

c. Select **Save**.

**Related Topics**

- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Dial-Out Features and Voice Prompt Languages, page 1
Configuring Blast Dial-Out Calls

Blast dial-out calls come in two forms:

- Initiated by the system—While scheduling a continuous meeting, the scheduler sets Outdial all invitees when first person joins to Yes on the More Options page.
- Initiated by a user—During a meeting, the scheduler (with dial-out privileges) enters #33 in the TUI to dial out to all missing invitees.

Before You Begin

- To enable user-initiated blast dial-out calls, complete the “Enabling Dial-Out Privileges for Users” section on page 4.
- No specific configuration is required to use blast dial-out calls. This optional procedure describes how to configure fields that affect the behavior of all dial-out calls, including blast dial-out calls.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Administration Center.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select System Configuration &gt; Usage Configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Configure the following fields, which affect all dial-out calls:</td>
</tr>
<tr>
<td></td>
<td>• Number of retry attempts</td>
</tr>
<tr>
<td></td>
<td>• Delay between retries (sec)</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Save.</td>
</tr>
</tbody>
</table>

Related Topics

- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Continuous Meetings in the Configuring Meetings for Cisco Unified MeetingPlace module
Configuring the Auto Attend Feature for Cisco Unified MeetingPlace

Auto Attend Feature

The auto attend feature simplifies how users join meetings or log in over the phone. If a user calls the system from a phone number in the user profile, then the user is immediately authenticated and placed into the relevant meeting.

You can enable or disable the auto attend feature for specific user profiles and user groups. When enabled, you can also specify the following:

- Whether the user automatically enters meetings or is only automatically logged in.
- Whether the user must enter the Profile password.

The feature works as follows:

1. A user calls Cisco Unified MeetingPlace.
2. The system reads the automatic number ID (ANI), which is the phone number from which the user called.
3. The system modifies the ANI according to the translation rules on the Auto Attend Translation Configuration Page, if any apply.
4. If the (modified) ANI exactly matches the Main phone number or Alternate phone number in one user profile, then the system checks all meetings (except continuous meetings) as follows:
   - Whether the user owns or is invited to any meetings that are in session or that are scheduled to begin.
   - Whether the user was a participant in any meetings that are still in session.
   - Whether anyone is in the waiting room of the reservationless meeting owned by the user.
5. If multiple meetings or no meetings are found, then the system authenticates the user and lets the user select the meeting.

6. If only one meeting is found, then the caller hears the meeting ID confirmation and is prompted to do one of the following:
   - Press 1 to attend the meeting.
   - Press * to hear menu options for authenticated users.

The caller may hear additional prompts in the following situations:
   - You configure the Auto attend requires profile password user profile field to Yes.
   - Meeting requires a password.
   - Caller needs to record a name or location.

Related Topics
- Examples of Auto Attend Translation Rules, page 2
- Adding or Editing an Auto Attend Translation Rule, page 4
- Enabling the Auto Attend Feature, page 5

Examples of Auto Attend Translation Rules

Sample Phone Numbers in User Profiles
Suppose that an organization uses 5-digit extensions and requires callers to enter a 9 to access an outside line. A user with the phone number 555-0123 may enter any of the following in the Main phone number or Alternate phone number user profile fields:
   - 50123—5-digit extension
   - 95550123—7-digit phone number preceded by 9 to get an outside line
   - 914085550123—10-digit phone number (including area code) preceded by 9 to get an outside line

Sample ANI Formats
Depending on where the call originated, an ANI might use one of these formats:
   - 50111—call from within an organization that uses 5-digit extensions
   - 5550111—local call from outside the organization using the full 7-digit number
   - 4085550111—call from another area code outside the organization
### Sample Auto Attend Translation Rules

**Table 1  Sample Auto Attend Translation Rules**

<table>
<thead>
<tr>
<th>Combination of Field Values</th>
<th>How the System Would Use This Translation Rule</th>
</tr>
</thead>
<tbody>
<tr>
<td>Digits to match</td>
<td>Match string</td>
</tr>
<tr>
<td>0</td>
<td>—</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>5</td>
<td>5</td>
</tr>
<tr>
<td>7</td>
<td>555</td>
</tr>
<tr>
<td>7</td>
<td>555</td>
</tr>
<tr>
<td>10</td>
<td>408555</td>
</tr>
<tr>
<td>10</td>
<td>408555</td>
</tr>
<tr>
<td>7</td>
<td>—</td>
</tr>
<tr>
<td>7</td>
<td>—</td>
</tr>
<tr>
<td>10</td>
<td>—</td>
</tr>
<tr>
<td>10</td>
<td>408</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Auto Attend Feature, page 1](#)
- [Adding or Editing an Auto Attend Translation Rule, page 4](#)
- [Field Reference: Add Translation Rule Page and Edit Translation Rule Page in the Administration Center Page References for Cisco Unified MeetingPlace](#)
Adding or Editing an Auto Attend Translation Rule

Defining Automatic Number Identification (ANI) translation rules enables the system to match different ANI formats to the phone numbers in user profiles. There are multiple ways that phone numbers may be entered in user profiles, and there are multiple ways that ANIs may be received from the telco switch.

**Before You Begin**
- This task requires a system restart, which terminates all existing call connections. Proceed only during a scheduled maintenance period or during a period of extremely low usage.

**Note** When you restart the Web Server, all manual changes made to the registry are lost.
- See the “Examples of Auto Attend Translation Rules” section on page 2.

**Restriction**
(Release 7.0.1 only) Do not modify the preconfigured auto attend translation rule, which must be configured as follows:
- **Digits to match** field is set to 0.
- Both the **Match string** and **Replace by** fields are left blank.

To find the preconfigured auto attend translation rule, look for the entry on the Auto Attend Translation Configuration Page with the dimmed check box.

**Procedure**

**Step 1** Log in to the Administration Center.
**Step 2** Select **System Configuration > Call Configuration > Auto Attend Translation Configuration**.
**Step 3** To add a new rule, select **Add New**. To edit an existing rule, select **Edit**.
**Step 4** Configure the fields.
**Step 5** Select **Save**.
**Step 6** Restart the system by entering `sudo mpx_sys restart` in the CLI.

**Related Topics**
- **Field Reference: Add Translation Rule Page and Edit Translation Rule Page** in the Administration Center Page References for Cisco Unified MeetingPlace module
- **Navigation Reference: Auto Attend Translation Configuration Page** in the Administration Center Page References for Cisco Unified MeetingPlace module
- **Auto Attend Feature, page 1**

**What to Do Next**
Proceed to the “Enabling the Auto Attend Feature” section on page 5.
Enabling the Auto Attend Feature

By default, the auto attend feature is disabled. We recommend that you enable this feature for all users.

Before You Begin
- Complete the “Adding or Editing an Auto Attend Translation Rule” section on page 4.
- For each user profile in which the auto attend feature is enabled, anyone who calls Cisco Unified MeetingPlace from a phone number configured in the Main phone number or Alternate phone number field will be logged in using that particular user profile.

Therefore, you may want to require profile passwords or disable the auto attend feature for users whose specified endpoints may be used by multiple people.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Administration Center.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select User Configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select User Groups or User Profiles.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Configure these fields:</td>
</tr>
<tr>
<td></td>
<td>• Auto attend mode</td>
</tr>
<tr>
<td></td>
<td>• Auto attend requires profile password</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Save.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Repeat this task for all user groups and user profiles for which you want to enable the auto attend feature.</td>
</tr>
</tbody>
</table>

Related Topics
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Auto Attend Feature, page 1
Configuring Direct Inward Dial for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:30 pm

The Direct Inward Dial (DID) feature enables users to call directly into a meeting by dialing the meeting ID, instead of dialing one of the Cisco Unified MeetingPlace access phone numbers on the Usage Configuration Page.

Before You Begin
Configure your call-control device to route DID calls to the Application Server.
For example, in Cisco Unified Communications Manager, configure a route pattern for each meeting ID that you want to make available for DID. Configure these route patterns to send calls to the trunk that leads to the Cisco Unified MeetingPlace Application Server. See the Configuring Call Control for Cisco Unified MeetingPlace module.

Restrictions
DID callers can join meetings as profiled users through the auto attend feature. If, however, the Auto attend mode user profile field is set to None, then the DID caller can join meetings only as a guest.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Usage Configuration.
Step 3 Set the Route calls to meeting ID that matches DID field to Yes.
Step 4 Select Save.

Related Topics
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring the Auto Attend Feature for Cisco Unified MeetingPlace module
Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace

About RSNA

- RSNA
- RSNA Reserved Meeting Server, page 2

RSNA

The Reservationless Single Number Access (RSNA) feature allows multiple Cisco Unified MeetingPlace systems to appear as one system to the user community. Any user who hosts (as a profiled user) or attends (as a profiled user or as a guest) a reservationless meeting can join the meeting by dialing the access phone number of the Cisco Unified MeetingPlace system that is local to that user, regardless of which system is hosting the meeting. Users are then redirected to the system that is hosting the meeting.
RSNA Reserved Meeting Server

The RSNA Reserved Meeting Server feature allows a single Application Server to host reserved meetings within an RSNA-based network. Typically, all meeting reservations are on the one designated Reserved Meeting Server. When users attend meetings by accessing their local server, if their local server does not recognize the meeting ID, it transfers the user to the Reserved Meeting Server.

Note

The server times must be synchronized between the local Application Server and the Reserved Meeting Server.

The local server attempts to transfer calls to the Reserved Meeting Server if all of the following conditions are true:

- The Reserved Meeting Server feature has been configured on the local server:
  The local server must be configured with a remote server record in which the Reserved Meeting Server check box is checked.
  If you want any user profiles to identify the remote Reserved Meeting Server as the Schedule home server, then create a duplicate remote server record in which you do the following:
    - Do NOT check the Reserved Meeting Server check box.
    - Enter a Home Server number in the range 0 to 999.
    - Make sure that all other fields are identical between the duplicate records for the Reserved Meeting Server.
- The meeting ID that the user entered does not match the meeting ID of any meetings scheduled around that time on the local server.
- The meeting ID that the user entered does not match any user profile, active or not.
- The user confirms the meeting ID.

In addition, consider the following behavior of the RSNA Reserved Meeting Server feature:

- This feature does not prevent meetings from being scheduled locally and will not warn or transfer a user who attempts to schedule a meeting locally.
- If a meeting is scheduled on a server other than the Reserved Meeting Server, this feature will not facilitate attendance of that meeting.
- A locally scheduled meeting always takes precedence over a remote one. This rule applies even if a local meeting recently ended and the user hears that meeting is over.
- If the meeting does not exist on the remote system, the system prompts the user for a meeting ID after the transfer.
- Users choose which server to schedule the meeting on from the Server drop-down box on the Scheduling page. To restrict users from choosing a server other than the Reserved Meeting Server, you may need to disable the Server drop-down box from the scheduling page. This restriction does not apply if the user dials into a local server and uses the TUI to schedule the meeting. In that case the meeting will be scheduled on a local server.

Restrictions

Meeting recordings are stored only on the web server that is associated with the schedule home server for the meeting owner. You must know the URL of the web server that you assigned to the meeting owner to access meeting recordings.
Prerequisites for RSNA

- Plan and install your Cisco Unified MeetingPlace systems for RSNA, as described in the following documents:
- Any endpoints that directly access Cisco Unified MeetingPlace must support SIP and the SIP REFER method of transferring calls, as specified in RFC 3515.

Restrictions for RSNA

- Only two RSNA systems (sites) are currently supported.
- Single-URL access for Cisco Unified MeetingPlace Web Conferencing is currently not supported.
- The system cannot strongly authenticate users by password when they are transferred between servers. This causes the following restrictions for profiled users who are transferred into a meeting:
  - Recorded names are not permanently stored on the system.
  - When leaving the meeting, the users are treated as unidentified.

How to Configure RSNA

- Enabling RSNA, page 4
- Configuring the Remote Servers, page 4
- How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment, page 5
- How to Configure User Profiles for RSNA, page 8
Enabling RSNA

Complete this task on each Cisco Unified MeetingPlace system for which you want to enable RSNA.

**Before You Begin**
Read the following topics:

- Prerequisites for RSNA, page 3
- Restrictions for RSNA, page 3

**Procedure**

1. Log in to the Administration Center.
3. Set the Enable RSNA field to Yes.
4. Select Save.

**Related Topics**

- Field Reference: Remote Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module

**What To Do Next**
Proceed to the “Configuring the Remote Servers” section on page 4.

Configuring the Remote Servers

Complete this task on each RSNA system.

**Before You Begin**
Complete the “Enabling RSNA” section on page 4.

**Procedure**

1. Log in to the Administration Center.
3. Select Add New, or select an existing entry.
5. Select Save.
6. Repeat Step 3 through Step 5 to add a server entry for each remote RSNA system.
How to Configure RSNA

Complete the following tasks, in the order shown, on each Cisco Unified Communications Manager node that is attached to a Cisco Unified MeetingPlace RSNA system.

- Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System, page 5
- Configuring Cisco Unified Communications Manager: SIP Route Patterns to Remote RSNA Systems, page 7

Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System

In this task, you connect the local Cisco Unified Communications Manager to each remote Cisco Unified MeetingPlace RSNA system.

Before You Begin

- Configure non-RSNA call-control for each Cisco Unified MeetingPlace system as described in the Configuring Call Control for Cisco Unified MeetingPlace module.

- We recommend that you create a SIP trunk security profile in Cisco Unified Communications Manager specifically for Cisco Unified MeetingPlace.

See “Configuring a SIP Trunk Security Profile in Cisco Unified Communications Manager for Cisco Unified MeetingPlace” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.

- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Procedure

Step 1  Go to http://ccm-server/, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2  Log in with your Cisco Unified Communications Manager administrator username and password.

Step 3  Select Device > Trunk.

Step 4  Select Add New.
Step 5 In the Trunk type field, select **SIP Trunk**.

Step 6 Select **Next**.

Step 7 Configure the fields described in Table 1.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Device Name</td>
<td>Enter a unique identifier for this trunk, such as the name or IP address of the remote Cisco Unified MeetingPlace Application Server.</td>
</tr>
<tr>
<td>Device Pool AAR Group</td>
<td>The device pool must use a codec that is compatible with the conferencing gateway (or bridge). For security and toll fraud prevention, use a device pool and an automatic alternate routing (AAR) group that will block any undesired phone numbers from being dialed out.</td>
</tr>
<tr>
<td>Media Termination Point Required</td>
<td>Uncheck this check box.</td>
</tr>
<tr>
<td>Destination Address</td>
<td>The DNS hostname or IP address of the remote Cisco Unified MeetingPlace server.</td>
</tr>
<tr>
<td>Destination Port</td>
<td>Keep the default value of <strong>5060</strong>.</td>
</tr>
<tr>
<td>SIP Trunk Security Profile</td>
<td>Select the SIP trunk security profile that you created specifically for Cisco Unified MeetingPlace. If you did not create a SIP trunk security profile, then select the default <strong>Non Secure SIP Trunk Profile</strong>.</td>
</tr>
<tr>
<td>DTMF Signaling Method</td>
<td>Select <strong>No Preference</strong>.</td>
</tr>
</tbody>
</table>

Step 8 Configure all other required fields appropriately for your current deployment.

**Tip** For field descriptions, select **Help > This Page**.

Step 9 Select **Save**.

Step 10 Repeat this task to add a SIP trunk to each remote Cisco Unified MeetingPlace RSNA system.

**What to Do Next**

Proceed to the “Configuring Cisco Unified Communications Manager: SIP Route Patterns to Remote RSNA Systems” section on page 7.
Configuring Cisco Unified Communications Manager: SIP Route Patterns to Remote RSNA Systems

In this task, you enable the local Cisco Unified Communications Manager to route calls to each remote Cisco Unified MeetingPlace RSNA system.

Before You Begin
- Complete the “Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System” section on page 5.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

Restriction
By associating a SIP route pattern to a SIP trunk, you can no longer put the SIP trunk in a route group. If, for some reason, you need to put the SIP trunk in a route group, then create duplicate SIP trunks. Specifically, for each SIP trunk that is associated with a SIP route pattern, create an identical SIP trunk that is not associated with a SIP route pattern.

Procedure

Step 1 Go to http://ccm-server/, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
Step 2 Log in with your Cisco Unified Communications Manager administrator username and password.
Step 3 Select Call Routing > SIP Route Pattern.
Step 4 Select Add New.
Step 5 Configure the fields described in Table 2.

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pattern Usage</td>
<td>Select <strong>IP Address Routing</strong>.</td>
</tr>
<tr>
<td>Pattern</td>
<td>Enter the IP address of the remote Application Server.</td>
</tr>
<tr>
<td>Note</td>
<td>This value must match the SIP Agent Address 1 field that was configured on the local Cisco Unified MeetingPlace system to identify the remote system.</td>
</tr>
<tr>
<td>SIP Trunk</td>
<td>Select the SIP trunk that you configured in the “Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System” section on page 5.</td>
</tr>
</tbody>
</table>

Tip
For field descriptions, select Help > This Page.

Step 6 Configure all other required fields appropriately for your current deployment.

Step 7 Select Save.
Step 8  Select OK to any pop-up dialog box messages that you see.

Step 9  Repeat this task to add a SIP route pattern to each remote Cisco Unified MeetingPlace RSNA system.

What to Do Next

Repeat the tasks in the “How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment” section on page 5 for each Cisco Unified Communications Manager node that is attached to a Cisco Unified MeetingPlace RSNA system.

Then proceed to the “How to Configure User Profiles for RSNA” section on page 8.

How to Configure User Profiles for RSNA

The following fields in each user profile must have the exact same values on both RSNA systems:

- User ID
- User password
- Profile number
- Profile password
- Schedule home server

This is typically accomplished by completing the following tasks:

<table>
<thead>
<tr>
<th>High-Level Task</th>
<th>Where to Find Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1  Configure the Schedule home server field through user groups.</td>
<td>Configuring the Schedule Home Server Field in User Groups or User Profiles, page 8</td>
</tr>
<tr>
<td>Step 2  Synchronize the user database between the two sites.</td>
<td>Configuring User Database Replication for Two Sites in the Configuring Cisco Unified MeetingPlace Directory Service module</td>
</tr>
<tr>
<td>Step 3  (Optional) Configure Directory Service on one RSNA system to synchronize Cisco Unified MeetingPlace user profiles with Cisco Unified Communications Manager and configure external AXL authentication.</td>
<td>Configuring Cisco Unified MeetingPlace Directory Service module</td>
</tr>
<tr>
<td>Step 4  If you configured Directory Service on one RSNA system, then configure external AXL authentication on the other (non–Directory Service) system.</td>
<td>Enabling External User Authentication on the Non–Directory Service RSNA System, page 9</td>
</tr>
</tbody>
</table>

Configuring the Schedule Home Server Field in User Groups or User Profiles

Complete this task on each RSNA system.

Before You Begin

Complete the tasks in the “How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment” section on page 5 for each Cisco Unified Communications Manager node that is attached to a Cisco Unified MeetingPlace RSNA system.
Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace

How to Configure RSNA

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration.
Step 3 Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.

Tip Because Directory Service does not synchronize this particular configuration, we recommend that you configure user groups and allow the user profiles to inherit the group default values.

Step 4 Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.
Step 5 Configure the Schedule home server field to match the Home Server number remote server field.
Step 6 Select Save.
Step 7 Repeat this procedure for all user groups and (if necessary) user profiles.

Related Topics
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- How to Configure User Profiles for RSNA, page 8

What To Do Next
Proceed to “Configuring User Database Replication for Two Sites” in the Configuring Cisco Unified MeetingPlace Directory Service module.

Enabling External User Authentication on the Non–Directory Service RSNA System

By performing this task, you enable Directory Service users to log in to either RSNA system. Note that the same Cisco Unified Communications Manager server is used for authentication.

Before You Begin
Complete Step 1 through Step 3 in the “How to Configure User Profiles for RSNA” section on page 8.

Procedure

Step 1 On the non–Directory Service system, log in to the Cisco Unified MeetingPlace Administration Center.
Step 3 Configure the following fields, using the exact same values that you entered on the Directory Service–configured system:
- AXL username
- AXL password
- AXL confirm password
- AXL URL
**Step 4**  
Do not modify any of the other fields on the Directory Service Configuration Page.

- If you think you accidentally modified any of the other fields, then select **Cancel** and return to Step 2.
- If you think you accidentally modified *and saved* any of the other fields, then do the following:
  - Make sure that Perform full sync with Cisco Unified Communications Manager is unchecked.
  - Make sure that Hostname for Active Directory Service either matches the value configured on the Directory Service-configured system or is left **blank**.

**Step 5**  
Select **Save**.

**Related Topics**

- Field Reference: Directory Service Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- How to Configure User Profiles for RSNA, page 8
PART

Web Conferencing Configuration

- Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager
- Connecting the Cisco Unified MeetingPlace Application Server to a Web Server
- Managing Cisco Unified MeetingPlace Web Conferencing Services
- Configuring Audio Conversion
- Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage
- Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing
- Configuring the Cisco Unified MeetingPlace Web Conferencing User Interface
- Configuring External Access to Cisco Unified MeetingPlace Web Conferencing
- Configuring Cisco Unified MeetingPlace Web Conferencing and SQL Server
- Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing
Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager

About the Gateway SIM

The Gateway System Integrity Manager (Gateway SIM) is a common component of Cisco Unified MeetingPlace products. Gateway SIM functions as the channel through which Cisco Unified MeetingPlace gateways communicate with the Cisco Unified MeetingPlace Application Server. It improves the reliability and serviceability of all Cisco Unified MeetingPlace applications by detecting gateway outages and logging these errors to the Alarm Table. It also allows you to add and delete gateway units (computers that have Cisco Unified MeetingPlace Web Conferencing or other Cisco Unified MeetingPlace applications installed) from the Application Server.

The Gateway SIM is comprised of two modules:

- **Gateway SIM Agent**—Resides in the MeetingPlace Gateways Configuration Utility on the Web Server. The Gateway SIM Agent sends scheduled updates to the Gateway SIM Manager.
- **Gateway SIM Manager**—Resides on the Cisco Unified MeetingPlace Application Server. If the Gateway SIM Manager does not receive updates when expected, it logs a major alarm to the Alarm Table.

The following table describes the fields in the Gateway SIM Agent.
When to Change the Cisco Unified MeetingPlace Application Server Connection

Cisco Unified MeetingPlace gateway units (computers that have Cisco Unified MeetingPlace Web Conferencing or other Cisco Unified MeetingPlace applications installed) are configured to point to a particular Cisco Unified MeetingPlace Application Server.

Once a unit is attached to an Application Server, you should only detach it for the following reasons:

- **You are replacing an old unit with a new unit.**
  
  In this case, detach the old unit from the Application Server to decommission it.

- **You are replacing the Application Server with a brand new computer but the new Application Server uses the same database from the old server.**

Field or Window | Description
--- | ---
Version | The version number of the Gateway SIM.
Installation Key | The Ethernet address of this Windows computer. It is through this Ethernet address that this computer registers itself into the database of the active Application Server.
Remote Management Enabled | Enables a Cisco support representative to issue remote management requests that can help diagnose problems and restart the Cisco Unified MeetingPlace Web Conferencing Service.
  
  **Note** When you restart the Web Server, all manual changes made to the registry are lost.
Gateway Alarms Enabled | Enables the Gateway SIM to log alarms from this computer to the Alarm Table.
Lower left window | Indicates the FQDN of the Application Server to which this computer is connected.
Lower right window | Contains information about this computer including the following:
  
  - Whether the Gateway SIM on this computer is connected to the Application Server.
  - The unit number assigned to this computer by the active Application Server.
  - The IP address of this computer.
  - Whether link encryption is enabled.
  - Release of the server software that the active Application Server is running.

Related Topics

- [About the Cisco Unified MeetingPlace Web Conferencing Service](#) in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- [Connecting the Cisco Unified MeetingPlace Application Server to a Web Server](#) module
• You are replacing the Application Server with a brand new computer and the new Application Server uses a brand new database.
• You are testing the unit in a lab against a lab Application Server.
  When the unit is ready to be put into production, detach it from the lab Application Server and re-attach it to a production Application Server.

Related Topics
• Changing the Cisco Unified MeetingPlace Application Server Connection Configured in the Gateway SIM, page 4

Opening the MeetingPlace Gateways Configuration Utility

Before You Begin
This procedure is completed on the Cisco Unified MeetingPlace Web Server.

Procedure

Step 1 Go to your system tray.
Step 2 Right-click the Cisco Unified MeetingPlace icon.

Tip
The Cisco Unified MeetingPlace icon resembles a red door.

Step 3 Select Properties.

Related Topics
• Configuring the Gateway SIM, page 3
• Updating SQL Account Access from the MeetingPlace Gateway Configurations Utility in the Configuring Cisco Unified MeetingPlace Web Conferencing and SQL Server module

Configuring the Gateway SIM

Before You Begin
This procedure is completed on the Cisco Unified MeetingPlace Web Server.

Procedure

Step 1 Open the Gateway SIM Agent.
  a. Open the MeetingPlace Gateways Configuration utility.
  b. Select the Gateway SIM tab.
Step 2 (Optional) Check Remote Management Enabled to enable remote management from a Cisco support representative.
**Step 3** (Optional) Check **Gateway Alarms Enabled** to log alarms from this computer to the Cisco Unified MeetingPlace Application Server.

**Step 4** (Optional) Double-click the name of the Application Server that you want to connect to.

- Your active Application Server and the IP address of the gateway computer are prepopulated as “Server Name” and “Client IP Address.”
- If you want to indicate a standby Application Server, which would take over on the network if the active Application Server goes down, enter the name for “Shadow Server Name.”

**Note** If you have an Application Server failover deployment, make sure that the Web Server identifies the active Application Server by using the shared hostname and IP address of eth0.

**Step 5** Select **OK**.

**Step 6** Select **OK** from the Gateway SIM tab.

---

**Related Topics**

- Opening the MeetingPlace Gateways Configuration Utility, page 3
- Configuring Application Server Failover for Cisco Unified MeetingPlace module

---

**Changing the Cisco Unified MeetingPlace Application Server Connection Configured in the Gateway SIM**

Complete this procedure to update the Application Server that the Cisco Unified MeetingPlace Web Server points to.

**Note** If you have an Application Server failover deployment, make sure that the Web Server identifies the active Application Server by using the shared hostname and IP address of eth0.

**Before You Begin**

- In this procedure, we refer to the Web Server as a “unit.”
- Stop the Cisco Unified MeetingPlace Web Conferencing Service and Gateway SIM Service. If other Web Servers share the database with this server, stop the services on those servers as well.
- This procedure is completed on the Web Server.

**Note** Do not restart services until you have completed this procedure.

**Procedure**

**Step 1** Open the Gateway SIM Agent.

a. Open the MeetingPlace Gateways Configuration utility.

b. Select the **Gateway SIM** tab.
Step 2  Delete this unit from the active Application Server.
   a.  Go to the lower-left pane of the Gateway SIM tab.
   b.  Select the name of the Application Server that you want to disconnect from.
   c.  Select Delete.

Step 3  Change the Application Server hostname in the MPWEB database:
   a.  Open Enterprise Manager and navigate to the \Databases folder.
   b.  Select and expand the MPWEB database.
   c.  Select Tables from the left pane.
   d.  Right-click System in the right pane.
   e.  Select Open Table > Return All Rows from the pop-up menu.
   f.  Change the value in the HostName column from the hostname of the old Application Server to the hostname of the new Application Server.

Step 4  Delete all Cisco Unified MeetingPlace Web Conferencing attachment subfolders.
   a.  Go to your Windows Explorer.
   b.  Navigate to the location of your attachment folder, for example, drive:\Web_data\MPWeb\Meetings.
   c.  Delete all of the subfolders. Do not delete the Meetings folder.

Step 5  Add this unit to a new Application Server.
   a.  Open the Gateway SIM Agent.
   b.  Select Add.
      The MeetingPlace Server Entry window displays.
   c.  Enter the new configuration information as follows:

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Name</td>
<td>Enter the hostname of the new Cisco Unified MeetingPlace Application Server.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you use an IP address instead of a hostname for the Application Server, you will have to update the IP address on the Web Server whenever you change the IP address on the Application Server.</td>
</tr>
<tr>
<td>Shadow Server</td>
<td>Leave this field as is.</td>
</tr>
<tr>
<td>Client IP Address</td>
<td>Enter the IP address of the computer on which the Gateway SIM is installed.</td>
</tr>
<tr>
<td>Transfer Destination</td>
<td>Leave this field as is.</td>
</tr>
<tr>
<td>Link Encryption Disabled</td>
<td>Leave this box unchecked to maintain encrypted communications between the Gateway SIM and the Application Server. Encryption uses a 56-bit DES algorithm with a secret key.</td>
</tr>
</tbody>
</table>

   d.  Select OK.
   e.  Select OK again.
Step 6  Restart the Gateway SIM service and the Cisco Unified MeetingPlace Web Conferencing Service. If other Web Servers share the database with this server, restart the services on those servers as well.

Note  When you restart the Web Server, all manual changes made to the registry are lost.

Step 7  Verify that this unit is attached to the new Application Server and that a unit number is assigned.
   a. Open the Gateway SIM Agent.
   b. Make sure that the newly entered Application Server is listed in the left window.

Step 8  Update the Web Server with user and meeting information from the new Application Server.
   a. Open a web browser and sign in to Cisco Unified MeetingPlace.
   b. Select Admin.
   c. Select Replication Service.
   d. Select Update All User Profiles.
   e. Select Submit.
   f. Change the Replication Service Command to Update All Meetings.
   g. Select Submit.

Related Topics
- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- Opening the MeetingPlace Gateways Configuration Utility, page 3
- Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- Configuring Application Server Failover for Cisco Unified MeetingPlace module
Adding or Editing a Web Server Connection

This task enables you to:

- Configure the Gateway SIM connections between the Application Server and the Web Servers.
- Add links to the Web Server from the Administration Center. The links appear in a drop-down menu at the top of each Administration Center page.

After you install and configure the Gateway SIM on the Web Server, the Gateway SIM automatically registers the Web Server to the Application Server by opening an inbound connection from the Web Server to port 5003 on the Application Server. Successfully registered Web Servers are automatically configured on the Web Servers Page, and links to those Web Servers appear in a drop-down menu at the top of each Administration Center page.

If inbound connections are not allowed, such as in segmented meeting access (SMA) deployments or when a firewall is in use, then you need to perform this task to enable the Application Server to open an outbound “reverse connection” to port 5003 on the Web Server.

Before You Begin

- Install Gateway SIM and the Web Conferencing Server Software as described in the “
- Configure Gateway SIM on the Web Server. See Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager in the Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module.
- From the Web Server, write down the following values on the Gateway SIM tab in the MeetingPlace Gateways Configuration Utility:
  - Unit
  - Installation Key (for reverse connection only)
  - Local IP Address (for reverse connection only)
Disabling a Web Server Connection

See Opening the MeetingPlace Gateways Configuration Utility in the Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module.

- If you plan to use a reverse connection, then confirm the following configurations:
  - Outbound connections to port 5003 on the Web Server are not blocked, for example, by a firewall.
  - The Application Server name configured on the Web Server exactly matches the hostname that is displayed by entering the hostname command on the Application Server.

Restrictions
- After you add or enable a Web Server entry, the link to that Web Server does not appear until you log out and log back in to the Administration Center.
- You cannot delete Web Server entries. You can, however, disable them.

Procedure

1. Log in to the Administration Center.
2. Select System Configuration > Web Servers.
3. Select the Unit number of the Web Server.
   If the unit number was unassigned on the Web Server, then select an unused or obsolete Unit number.
4. Enter or confirm the FQDN and Hostname of the Web Server.
5. To enable reverse connection, enter the Installation key and IP address of the Web Server.
6. Set Enabled to Yes.
7. Select Save.
8. Repeat this task for each Web Server in the site.

Related Topics
- Field Reference: Edit Web Server Page
- Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module

Disabling a Web Server Connection

Use this procedure if you need to:
- Disable the Gateway SIM connection between the Application Server and a Web Server.
- Hide the link to the Web Server from the Administration Center.

Restrictions
- After you disable a Web Server entry, the link to that Web Server does not disappear until you log out and log back in to the Administration Center.
- You cannot delete Web Server entries. You can only disable or edit them.
Procedure

Step 1  Log in to the Administration Center.
Step 2  Select System Configuration > Web Servers.
Step 3  Select the Web Server entry.
Step 4  Set Enabled to No.
Step 5  Select Save.

Related Topics
- Field Reference: Edit Web Server Page
Managing Cisco Unified MeetingPlace
Web Conferencing Services

About the Cisco Unified MeetingPlace Web Conferencing Service

The Cisco Unified MeetingPlace Web Conferencing Service is a Windows master service that manages and monitors the following:

- Cisco Unified MeetingPlace Agent Service
- Cisco Unified MeetingPlace Audio Service
- Cisco Unified MeetingPlace Connect Application Service
- Cisco Unified MeetingPlace Connect Gateway
- Cisco Unified MeetingPlace Flash Media Administration Server
- Cisco Unified MeetingPlace Flash Media Server
- Cisco Unified MeetingPlace Replication Service
- Cisco Unified MeetingPlace Video Service

It also configures the MeetingPlace Web (MPWEB) database and the MPWEB slave databases.

The master service is turned on automatically after any reboot or upgrade, at which point it monitors all subsidiary services and runs a database configuration and import tool. If the database version is not up to date, the tool updates the database schema. Similarly, if the database needs to import new strings, the tool imports them. If any services fail, the master service automatically restarts and a major alarm is sent to the Cisco Unified MeetingPlace Application Server.
Cisco Unified MeetingPlace Web Conferencing Service and NTP Servers

If you are using an NTP server, Cisco Unified MeetingPlace will force the Web Server to synchronize its time with the NTP server whenever you restart the Web Conferencing master service. This is regardless of how large the time difference is. Once the master service is started, Cisco Unified MeetingPlace will only synchronize with the NTP server if the time difference is 30 seconds or less. The synchronization will take place once every hour.

**Note**
When you restart the Web Server, all manual changes made to the registry are lost.

**Note**
The first time the Web Conferencing master service comes up, the NTP server is set to the Cisco Unified MeetingPlace Application Server.

**Related Topics**
- Configuring the Web Server to Synchronize with an NTP Server
- How to Manually Synchronize the Web Server with an NTP Server

How to Use the Cisco Unified MeetingPlace Web Conferencing Service

- Stopping All Web Conferencing Services, page 2
- Restarting All Web Conferencing Services, page 3

Stopping All Web Conferencing Services

You must stop all Cisco Unified MeetingPlace web conferencing services before you complete certain procedures, including Gateway SIM upgrades and configuration changes.

**Procedure**

**Step 1**
Go to your Windows Start menu.

**Step 2**
Select Settings > Control Panel > Administrative Tools > Services.

**Step 3**
Right-click Cisco Unified MeetingPlace Web Conferencing and select Stop.

**Step 4**
(Optional) To stop other Cisco Unified MeetingPlace gateway services, including Gateway SIM, right-click the service and select Stop.

**Step 5**
Right-click the IIS Admin Service if it is still running and select Stop.

**Step 6**
Close the Services control panel.
Related Topics
- Restarting All Web Conferencing Services, page 3

Restarting All Web Conferencing Services

Procedure

Step 1  Go to your Windows Start menu.
Step 2  Select Settings > Control Panel > Administrative Tools > Services.
Step 3  Right-click Cisco Unified MeetingPlace Web Conferencing and select Start.
Step 4  Restart any other gateway services you may have stopped by right-clicking the applicable service and choosing Start.
Step 5  Close the Services control panel.

Related Topics
- Stopping All Web Conferencing Services, page 2
Configuring Audio Conversion

Cisco Unified MeetingPlace includes an Audio Service component as part of its web conferencing application that can convert audio, video, and web recordings into various formats. Playback formats include WAV, Windows Media (WMA), MP3, and MP4 formats.

Note
If the Web Server is part of a load balancing configuration, make sure that you set the Audio Conversion setting on all Web Servers so that they match.

- Converting Cisco Unified MeetingPlace Voice Files to WAV Format, page 1
- Converting Cisco Unified MeetingPlace Voice Files to MP3 Format, page 2
- Converting Cisco Unified MeetingPlace Voice Files to MP4 Format, page 3
- How to Convert Cisco Unified MeetingPlace Voice Files to Windows Media Format, page 3

Converting Cisco Unified MeetingPlace Voice Files to WAV Format

WAV files are typically supported by common web browsers and do not require that users have dedicated players.

Before You Begin
See the Recording Size topic in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module for an estimate of how much disk space you will need for this type of audio file. You should always make sure that you have enough disk space available to support all of your recordings and attachments.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Audio Conversion.
Step 4 Select Yes for Convert to WAV.
Configuring Audio Conversion

Converting Cisco Unified MeetingPlace Voice Files to MP3 Format

To listen to such recordings, users must have an MP3 player on their desktops.

Before You Begin
See the Recording Size topic in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module for an estimate of how much disk space you will need for this type of audio file. You should always make sure that you have enough disk space available to support all of your recordings and attachments.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Audio Conversion.
Step 4 Select Yes for Convert to MP3.
Step 5 Select Submit.

What to Do Next
If this Web Server is part of a load balancing configuration, go to each Web Server within the cluster and set the Audio Conversion setting so that they match.
Converting Cisco Unified MeetingPlace Voice Files to MP4 Format

Web Conferencing is bundled with the mp4converter tool for converting synchronized audio and video files to MP4 format. To play back such recordings, users must have an MP4 player, such as QuickTime, on their desktops.

Before You Begin
See the Recording Size topic in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module for an estimate of how much disk space you will need for this type of audio file. You should always make sure that you have enough disk space available to support all of your recordings and attachments.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Sign in to the end-user web interface.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Admin.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Audio Conversion.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select Yes for Convert to MP4.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select Submit.</td>
</tr>
</tbody>
</table>

What to Do Next
If this Web Server is part of a load balancing configuration, go to each Web Server within the cluster and set the Audio Conversion setting so that they match.

How to Convert Cisco Unified MeetingPlace Voice Files to Windows Media Format

Complete the following procedures in the order shown to configure Cisco Unified MeetingPlace to convert audio files to Windows Media format.

Note
See the Recording Size topic in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module for an estimate of how much disk space you will need for this type of audio file. You should always make sure that you have enough disk space available to support all of your recordings and attachments.

- Installing Windows Media Server for Cisco Unified MeetingPlace, page 4
- Configuring Windows Media Server Before Using It For the First Time, page 5
- Converting Cisco Unified MeetingPlace Voice Files to Windows Media Format, page 6
- Configuring Windows Media Server to Stream Audio Recording Playbacks, page 7
Installing Windows Media Server for Cisco Unified MeetingPlace

Web Conferencing supports Windows Media Server to stream audio recording playbacks. The installer file for this component is installed as part of the Cisco MCS OS. Complete this procedure to locate and install Windows Media Server.

**Note**

Make sure that Windows Media Server is configured to use a port other than port 80 so that it does not interfere with Cisco Unified MeetingPlace Web Conferencing in IIS.

**Before You Begin**


**Procedure**

**Step 1**

Select **Administrative Tools > Services** from your Windows Control Panel.

**Step 2**

Set the NT LM Security Support Provider to startup manually.

a. Scroll down to **NT LM Security Support Provider**.

b. Right-click and select **Properties**.

c. Select **Manual** as the Startup Type.

d. Select **Apply**.

e. Select **Start**.

f. Close the Properties window.

**Step 3**

Install the WMS.cab file.

a. Go to **Start > Control Panel > Add or Remove Programs**, and select **Add/Remove Windows Components**.

b. In the Windows Components Wizard, check **Windows Media Services**, and select **Details**.

c. Make sure that Windows Media Services and Windows Media Services snap-in are checked.

d. Select **OK** to close the Window Media Services window, then select **Next**.

e. When it asks for the Windows 2003 CD select **OK**.

f. Enter C:\Utils\WMS in the “Copy files from” field.

g. Select **OK**.

h. Select **Finish**.

**Step 4**

Set the user authentication in Windows Media Server to that of the admin user.

a. Select **Start > Programs > Administrative Services > Windows Media Services**.

b. Select the name of the server that you want to configure in the left pane.

c. Select the **Properties** tab in the right pane.

d. Select **Authentication** in the Category window.

e. Double-click **WMS Anonymous User Authentication**.

f. Change the User ID and Password to that of the admin user.
Configuring Audio Conversion

How to Convert Cisco Unified MeetingPlace Voice Files to Windows Media Format

Step 5

Setup WMS HTTP Server Control Protocol.

a. Go to Start > Programs > Administrative Tools > Windows Media Services.

b. In the Windows Media Services console, highlight your server, then select the Properties tab in the right-hand panel.

c. In the Category section, select Control protocol (if it does not appear, check Show all plug-in categories).

d. In the right-hand panel, right-click WMS HTTP Server Control Protocol and select Properties.

e. Change Use other port (1-65535): to 8082.

The default port (80) conflicts with the Cisco Unified MeetingPlace Web Conferencing application in Internet Information Services [IIS]).

f. Select OK.

g. Right-click WMS HTTP Server Control Protocol and select Enable.

h. In the left-hand panel, expand Publishing Points and select <Default> (on-demand).

i. Select Action from the top menu and select Allow New Connections.

Step 6

Go to Start > Administrative Tools > Computer Management.

Step 7

Expand Services and Applications, then select Services.

Step 8

Restart the Windows Media Service.

What to Do Next

Proceed to the “Converting Cisco Unified MeetingPlace Voice Files to Windows Media Format” section on page 6.

Related Topics

- How to Convert Cisco Unified MeetingPlace Voice Files to Windows Media Format, page 3

Configuring Windows Media Server Before Using It For the First Time

The Windows Media Server must be configured before you can start using it because by default, all users are considered guests. Guests, however, cannot perform many functions on the Cisco MCS platform. You must be a member of the WebUsers group to perform the functions described below.

Follow this procedure to remove the Windows Media Services Guest Account from the Guests group and add it to the WebUsers group. This is the group to which the IIS Anonymous User Account belongs and this group is not as restrictive as the Guests group.

Procedure

Step 1

If the Windows Media Service is running, stop it.

Step 2

Go to Start > Settings > Control Panel.

Step 3

Double-click Administrative Tools.
Configuring Audio Conversion

Converting Cisco Unified MeetingPlace Voice Files to Windows Media Format

Web Conferencing is bundled with the Windows Media Encoder, which converts audio files to WMA format by default. To listen to such recordings, users must have a player on their desktops that plays WMA files, such as Windows Media Player. Complete this procedure to configure Cisco Unified MeetingPlace to convert files to WMA format.

Before You Begin
Make sure that you have Windows Media Server installed and configured on your Cisco MCS server. See the “Installing Windows Media Server for Cisco Unified MeetingPlace” section on page 4.

Restrictions
We do not recommend storing WMA files separately from the main storage location for meeting attachments. The automated purging mechanism cannot operate on separately-stored files.

Troubleshooting Tips
For more information about troubleshooting the Windows Media Server when used with Cisco Unified MeetingPlace, see the following tech note:

How to Convert Cisco Unified MeetingPlace Voice Files to Windows Media Format

Step 4 Double-click Computer Management.
Step 5 Select Local Users and Groups from the left panel.
Step 6 Double-click Users from the right pane.
Step 7 Highlight the user called WMUS_<MACHINE_NAME>, where <MACHINE_NAME> is the name of your computer.
Step 8 Right-click and select Properties.
Step 9 Select the Member Of tab.
Step 10 Highlight Guests.
Step 11 Select Remove.
Step 12 Select Apply.
Step 13 Select Add.
Step 14 Select Advanced.
Step 15 Select Find Now.
Step 16 Highlight the name of the user.
Step 17 Select OK twice.
Step 18 Select Apply.
Step 19 Check the box to enable “WMS Anonymous User Authentication plug-in” from Windows Media Services.
Procedure

Step 1  Create a MPWeb\Meetings folder under <drive>:\wmpub\WMRoot.
Step 2  Sign in to the end-user web interface.
Step 3  Select Admin.
Step 4  Select Audio Conversion.
Step 5  Select Yes for Convert to Windows Media Format.
Step 6  Complete one of the following for Use Windows Media Server:
   • Select Yes if you want to listen to your recordings by using streaming technology.
   • Select No if you want to download and listen to your recordings offline or by using HTTP.
Step 7  Enter the Windows Media Server hostname or IP address.

Note  This Windows Media Server can be installed locally or remotely.

Step 8  Enter <drive>:\wmpub\WMRoot for Windows Media Server Path.
Step 9  (Optional) Enter the name of your Windows Media encoder conversion profile for Windows Media Server Conversion Profile.
   This forces Cisco Unified MeetingPlace to use your Windows Media encoder conversion profile during audio conversion.
Step 10  Select Submit.

Related Topics
   • How to Convert Cisco Unified MeetingPlace Voice Files to Windows Media Format, page 3

Configuring Windows Media Server to Stream Audio Recording Playbacks

Procedure

Step 1  Select Administrative Tools > Services from your Windows Control Panel.
Step 2  Complete the following from the Services window:
   b. Right-click and select Properties.
Step 3  Complete the following from the Properties window:
   a. Select Manual as the Startup Type.
   b. Select Apply.
   c. Select Start.
   d. Close the Properties window.
Step 4  Select Add/Remove Programs from your Windows Control Panel.
Step 5  Scroll down and select **Windows Media Services**.
The Windows Components Wizard displays.
   a. Select **Remote Administration Mode** for Terminal Services Setup.
   b. Select **Next**.
   c. Select **OK** on the Insert Disk window to point to the location of your Windows Media Services files.
   d. Select **Browse** from the Files Needed window.
   e. Navigate to C:\Utils\WMS\WMS.cab.
   f. Select **OK** to install this file.
Cisco Unified MeetingPlace Web Conferencing is designed to manage itself automatically with minimal administrative activities. However, it is important to consider the impact that potential activities can have on network and hardware resources.

- Web Conferencing Data Storage, page 1
- Recording Size, page 2
- Best Practices for Storage Maintenance, page 3
- Configuring Shared Storage, page 4
- How to Update Meetings and User Profiles, page 5

Web Conferencing Data Storage

Storage space is required on the Cisco Unified MeetingPlace Web Server for storing converted meeting recordings and data attachments. It is important to plan for the system demand (disk space) that this kind of storage will require through proper configuration and management.

By default, the Web Server stores all recordings and attachments for meetings held on the server on a local disk. You can change the storage configuration to copy these items to an external backup location (such as a shared network drive on a dedicated storage server, a network-attached storage device, or a storage area network).

Cisco Unified MeetingPlace Web Conferencing checks for available disk space at regular five minute intervals. When the free disk space hits the 20% mark, a minor alarm is sent to the Application Server. When the free disk space hits 5%, a major alarm is sent to the Application Server but the system will not automatically shut down the Web Server. If you attempt to restart the Web Server for any reason when the disk space is less then 5% the Web Server will refuse to start up.

Caution

If you see a minor alarm for a disk space issue on the Web Server in the alarm table, the disk space identified in the alarm table only reflects the first event. The disk space could be better or worse if the alarm table has received more than one of these alarms. Therefore you should take measures to deal with the disk space issue to prevent any potential failure of the Web Server.
Related Topics

- Viewing an Event with the Windows Event Viewer

Recording Size

Even if no documents are shared during a recorded meeting, Web Conferencing periodically records the meeting console and converts the recording into a synchronized voice and web Flash format.

- If no audio participants join the meeting, the meeting console is recorded in Flash format without the voice component.
- If a meeting is scheduled with video enabled, but no video participants attend, Cisco Unified MeetingPlace will still attempt to record audio and video in case a video endpoint eventually joins or an audio endpoint escalates to video.
- If a video participant attends, all audio and video recordings are recorded on the Application Server in a preliminary MP4 format, which is then replicated to the Web Server for proper file conversions. The replicated MP4 file is used to create the WAV file, which is then used to create the MP3 and WMA files. The original MP4 file is converted to H.264 (avc1)/AAC (mp4a) MP4 for playback.

The following table lists the approximate disk space required for various recording types. You can select which types of recording will be available from the Audio Conversion page of the Cisco Unified MeetingPlace Web Administration.

<table>
<thead>
<tr>
<th>Audio or Video Format</th>
<th>Approximate Disk Space Required Per Hour of Recording</th>
</tr>
</thead>
<tbody>
<tr>
<td>WMA format</td>
<td>9 MB</td>
</tr>
<tr>
<td>WAV format (8-bit, 8Khz sampling rate)</td>
<td>27-30 MB</td>
</tr>
<tr>
<td>WAV format (16-bit, 8Khz sampling rate)</td>
<td>54-60 MB</td>
</tr>
<tr>
<td>MP3 format (32 kbits/s, 11Khz sampling rate)</td>
<td>14-15 MB</td>
</tr>
<tr>
<td>MP4 audio only AAC (mp4a)</td>
<td>512 KB</td>
</tr>
<tr>
<td>MP4 video H.264 (avc1)/AAC (mp4a)</td>
<td>150-175 MB</td>
</tr>
</tbody>
</table>

The following table lists the additional disk space required for each web collaboration mode. A web conference can consist of application sharing, a presentation, whiteboard, and annotations. With screen sharing, the actual size of the recording depends on the screen sharing resolution, how often the screen changes, and how well the data compresses.

<table>
<thead>
<tr>
<th>Synchronized Voice and Web Flash Format</th>
<th>Additional Disk Space Required Per Hour of Recording</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sharing an 11-slide, 6.6 MB PowerPoint file with several photo-quality image slides</td>
<td>2 MB</td>
</tr>
</tbody>
</table>
Caution

The Web Server will become inoperable if recordings consume all the disk space. Specifically, the end-user web interface will become inaccessible.

Note

Every day at 2 a.m. (local server time), the system purges all recordings on the Cisco Unified MeetingPlace Application Server that are older than 24 hours.

Related Topics

- Converting Cisco Unified MeetingPlace Voice Files to WAV Format in the Configuring Audio Conversion module
- Converting Cisco Unified MeetingPlace Voice Files to MP3 Format in the Configuring Audio Conversion module
- Converting Cisco Unified MeetingPlace Voice Files to MP4 Format in the Configuring Audio Conversion module
- How to Convert Cisco Unified MeetingPlace Voice Files to Windows Media Format in the Configuring Audio Conversion module

Best Practices for Storage Maintenance

For optimal space usage, we recommend the following best practices:

- Use a shared or network drive to store attachments.
- If you plan to record video, use an external storage device to prevent the Web Server from running out of disk space.
- Regularly check the drive you use to store attachments. Ensure that there is enough disk space for additional recordings.

Note

You cannot manually purge meeting statistics from the Web Server. This ability is controlled by the “Days until meeting statistics purged” parameter on the Cisco Unified MeetingPlace Application Server and cannot be changed for a particular meeting once it is set. Since you cannot change when past meetings are purged from the system, use the Shared Storage feature to move attachments and recordings to a new larger drive when you are running low on disk space.
**Configuring Shared Storage**

By default, the Cisco Unified MeetingPlace Web Server stores all recordings and attachments for meetings held on the server in a content folder on the local disk. We recommend that you change the storage configuration to copy content to a shared external backup location (such as a shared network drive on a dedicated storage server, a network-attached storage device, or a storage area network).

When you configure shared storage for a Web Server or for a cluster of servers, content is copied to the primary external storage device and pulled to the local content folder on each Web Server in the cluster as needed. You can specify a Content Cache Size that determines the percentage of disk space that is taken up by the local content folder before old content is automatically purged to make room for new content. This configuration frees resources on the local server, which is especially helpful in a large cluster of Web Servers.

Complete the following procedure to configure shared storage.

**Restrictions**

- Due to a Windows security restriction, you cannot move or copy files from the shared storage to the local storage when the Cisco Unified MeetingPlace Web Conferencing service is running under the LocalSystem account.
- When moving from one shared location to another, the Windows account that is configured to access the shared storage MUST have write access to both the old and new locations. If it does not, the old content will not be copied from the old location to the new location.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Sign in to the end-user web interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select Admin.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>Select Shared Storage.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Select On for Enabled.</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Locate the Shared Storage Path field.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td>Enter the network-accessible path to the storage directory, for example, \storesrvr\C$\Web_data\MPWeb.</td>
</tr>
</tbody>
</table>

- If you have a security concern with using the far end shared storage admin credentials due to the C$, set up a unique user account that has administrator privileges on the Web Server so that it can access the shared folder with the proper credentials and run the MeetingPlace services. For example, \storesrvr\MeetingPlace\Web_data\MPWeb where the credentials allow access to the MeetingPlace folder.
Note

If you ever need to change the location of the shared remote storage, update the credentials for both the remote storage and the local storage since both will require simultaneous access. If both storage locations do not share the same credentials, the destination storage location will not contain the updated attachments and recordings and users will not be able to access them from the Cisco Unified MeetingPlace web site.

Step 7
Locate the Content Cache Size field.

Step 8
Enter a value between 0 and 100 for the percentage of total disk space to use to cache content on the local server.

Step 9
In the applicable fields, enter a domain, username, and password for a Windows account that will be used to access the directory that you configured in Step 6. If the account is a local account, enter the computer name in the Domain field.

- All Cisco Unified MeetingPlace Web Conferencing services will be reconfigured to “Log On As” the account that you select in this step.
- If improper credentials are used, users may see an “Error: Access is denied” message when they attempt to access a recording or attachment from the Cisco Unified MeetingPlace Web Server.

Step 10
Re-enter the password in the Confirm Password field.

Step 11
Select Save Changes.

Step 12
Select Reboot Server to put the changes into effect.

Note
It may take several hours for the Cisco Unified MeetingPlace Web Conferencing services to come back up. They cannot start again until all the files in the C:\Program Files\Cisco Systems\MPWeb\Meetings and C:\Program Files\Cisco Systems\MPWeb\WebConf\content\7 folders are transferred to the shared storage device. These folders can possibly contain more than 20 GB of data each, so the downtime can be significant.

Step 13
Select OK to confirm the reboot.

The server shuts down and restarts.

What to Do Next
If this server is part of a load-balancing cluster, make sure that you restart the Cisco Unified MeetingPlace Web Conferencing service on the other Web Servers in the cluster. Make sure that there are no meetings going on in the system when you perform the reboot.

Related Topics

How to Update Meetings and User Profiles

- Replication Service, page 6
Replication Service

The Cisco Unified MeetingPlace Replication Service automatically synchronizes the local Web Server database with that of the Cisco Unified MeetingPlace Application Server to update meetings, user profiles, and user group information. The following occurs by default:

- Synchronization occurs every 60 seconds.
- The User Profile Update Interval updates every night.
- The Group Update Interval updates every night.
- Meeting information updates every 60 seconds.

The Replication Service copies audio and video recordings from the Cisco Unified MeetingPlace Application Server and stores the replicated files on the Cisco Unified MeetingPlace Web Server. Pointers to these files are then created in the database. The Replication Service downloads voice files in their original MP4 file format. After voice files are downloaded, the Replication Service queues jobs for conversion by the Audio Service.

The Replication Service also replicates video terminal user profile information from the Application Server. By default, this replication occurs every night.

In the event of a system failure, you can manually invoke the Replication Service operations. Allow up to 20 minutes for any changes made to the Replication Service to take effect.

Updating All Meetings

The Update All Meetings feature is automatically run at midnight every Saturday to synchronize meetings and meeting information between the Cisco Unified MeetingPlace Application Server and the Web Server. You can also manually invoke this feature whenever you want to force the following behavior:

- Meetings and meeting information are downloaded from the Application Server to the Web Server.
- If there are extra meetings on the Web Server, they are purged.
- Meetings are synchronized between the Application Server and Web Server going forward.

Every day at 2 a.m. (local server time), the system purges all recordings on the Cisco Unified MeetingPlace Application Server that are older than 24 hours. Any attachments or recordings that have already been purged from an Application Server are no longer available and hence, not downloaded.

Before You Begin

- The Update All Meetings feature will not retrieve attachments if they have been deleted from local folders on the Web Server. Retrieve these attachments by updating the relevant meeting instead.
- Allow 20 minutes for changes to take effect.
Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage

How to Update Meetings and User Profiles

Procedure

**Step 1** Sign in to the end-user web interface.

**Step 2** Select **Admin**.

**Step 3** Select **Replication Service**.

**Step 4** Select **Update All Meetings** for Replication Service Command.

Any MP4 files that have not yet been converted are downloaded and converted into the desired formats from the Application Server to the Web Server. In addition to attachments, new meetings are also updated.

**Step 5** Select **Submit**.

---

**Updating All User Profiles**

Complete this procedure to update the user profile database on the local Web Server. Allow 20 minutes for changes to take effect.

**Tip**

Synchronize your updates on the Web Server when you update the profile database on the Cisco Unified MeetingPlace Application Server.

Procedure

**Step 1** Sign in to the end-user web interface.

**Step 2** Select **Admin**.

**Step 3** Select **Replication Service**.

**Step 4** Select **Update All User Profiles** for Replication Service Command.

**Step 5** Select **Submit**.

---

**Updating All Video Terminals**

Complete this procedure to update the video terminal profile database on the local Web Server. The amount of time the replication takes depends on the number of video terminals; for example, allow 20 minutes to replicate up to 1000 video terminals.

**Tip**

Synchronize your updates on the Web Server when you update terminals in the Cisco Unified MeetingPlace Media Server Administration.

Procedure

**Step 1** Sign in to the end-user web interface.
Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage

How to Update Meetings and User Profiles

Step 2
Select Admin.

Step 3
Select Replication Service.

Step 4
Select Update All Terminals for Replication Service Command.

Step 5
Select Submit.

Updating All Groups

Complete this procedure to update the user group database on the local Web Server. Allow 20 minutes for changes to take effect.

Tip
Synchronize your updates on the Web Server with when you update the user group database on the Cisco Unified MeetingPlace Application Server.

Procedure

Step 1
Sign in to the end-user web interface.

Step 2
Select Admin.

Step 3
Select Replication Service.

Step 4
Select Update All Groups for Replication Service Command.

Step 5
Select Submit.

Updating a Single Meeting

Complete this procedure to force the Web Server to download meeting information for a single meeting from any Cisco Unified MeetingPlace Application Server. This feature is only effective when the Web Server has lost meeting attachments or recordings.

Restriction
Every day at 2 a.m. (local server time), the system purges all recordings on the Cisco Unified MeetingPlace Application Server that are older than 24 hours. The update will not take place if attachments and recordings have already been purged from the Application Server.

Procedure

Step 1
Sign in to the end-user web interface.

Step 2
Enter the meeting ID of the meeting that you want to update.

Step 3
Select Find Meeting.

Step 4
Select the meeting ID to access the meeting information page.

Step 5
Select Attachments/Recordings.
Step 6  Select **Update Meeting**.

Step 7  Select **OK**.

A new set of files are created including encoded audio files in the desired formats.
Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing

About User Authentication in Cisco Unified MeetingPlace Web Conferencing

By default, the web conferencing application prompts users for login credentials by using an HTML web form, then authenticates them against the Cisco Unified MeetingPlace user profile database. However, you can select to authenticate Cisco Unified MeetingPlace against third-party authentication software that provides different authentication behaviors. This can include different login windows, authentication against other user profile databases, or both.

User Authentication Options in Cisco Unified MeetingPlace Web Conferencing

Cisco Unified MeetingPlace Web Conferencing provides the following authentication configuration options:

- HTTP Basic Authentication (Domain)
Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing

How to Configure MeetingPlace Authentication

- LDAP
- LDAP, then MeetingPlace
- MeetingPlace
- Trust External Authentication
- Windows Integrated Authentication

Integration with third-party authentication software can provide the following benefits:
- Centralized user database—Facilitates profile management.
- Single Sign-On (SSO)—Allows users who have already been authenticated once to have access to all resources and applications on the network without having to re-enter their credentials.

For SSO to work, you must ensure that Cisco Unified MeetingPlace user IDs are set up so that they match the corresponding user IDs used by the third-party authentication software. You can configure Web Conferencing to automatically convert case so that Cisco Unified MeetingPlace user IDs and corresponding user IDs used by third-party authentication software match.

Note
While all authentication methods can be applied to internal or external servers, some authentication methods may not make sense for a DMZ environment. For more information about web conferencing support for DMZ environments, see the Configuring External Access to Cisco Unified MeetingPlace Web Conferencing module.

Restrictions: User Authentication and Load Balancing

In a Cisco Unified MeetingPlace load-balancing cluster, all users must enter the Cisco Unified MeetingPlace system through a designated Cisco Unified MeetingPlace Web Server. In such circumstances, you only need to configure the designated Web Server for your chosen authentication method. You can configure all other Web Servers in the cluster to use the default authentication method—MeetingPlace Web Form Authentication.

If, however, you want to configure other Web Servers in the cluster to use the same authentication method as a failover strategy, you can. Depending on the type of authentication method used though, this configuration can result in undesirable SSO behaviors.

For example, if you configure HTTP Basic Authentication or Windows Integrated Authentication, Cisco Unified MeetingPlace will prompt users for login credentials each time there is a Web Server redirect. This is because you are altering the hostname in the authentication configuration each time you redirect traffic to an active Web Server through a DNS change. If you configure LDAP or MeetingPlace authentication, users will not be prompted again for login credentials during a web conferencing redirect.

How to Configure MeetingPlace Authentication

Authenticating users against the profile database on the Cisco Unified MeetingPlace Application Server is the default user authentication option. You have two options when configuring this type of authentication:
- Logging in with an HTML-based web page form. This is the default option.
- Logging in against a login window rendered by your web browser.
Regardless of the login page users see, user IDs and passwords are sent to the Cisco Unified MeetingPlace Application Server for authentication. Both profiles and user passwords must match. Profiles are not case-sensitive.

- Configuring MeetingPlace Authentication, page 3
- Verifying the MeetingPlace Authentication Configuration by Using the HTTP Form, page 3

## Configuring MeetingPlace Authentication

### Before You Begin
Read the “Restrictions: User Authentication and Load Balancing” section on page 2.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Sign in to the end-user web interface.</td>
</tr>
<tr>
<td>2</td>
<td>Select Admin.</td>
</tr>
<tr>
<td>3</td>
<td>Select Web Server.</td>
</tr>
<tr>
<td>4</td>
<td>Select the name of the Web Server that you want to configure in the “View” section of the page.</td>
</tr>
<tr>
<td>5</td>
<td>Scroll to the Web Authentication section.</td>
</tr>
<tr>
<td>6</td>
<td>Select MeetingPlace for “Step 1: Directory”.</td>
</tr>
</tbody>
</table>
| 7    | Select one of the following options for “Step 2: Login Method”:
|      | Select Web Page Form to see an HTML-based Cisco Unified MeetingPlace login window. This is the default authentication method. |
|      | Select HTTP Basic Authentication to see a login window rendered by your web browser. |
| 8    | Select Submit and wait five minutes for the new configuration to take effect. |

### What to Do Next
(Optional) Proceed to the “Verifying the MeetingPlace Authentication Configuration by Using the HTTP Form” section on page 3.

## Verifying the MeetingPlace Authentication Configuration by Using the HTTP Form

Use a Cisco Unified MeetingPlace end-user profile when completing this procedure.

### Before You Begin
Complete the “Configuring MeetingPlace Authentication” section on page 3.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Open a web browser and navigate to Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td>2</td>
<td>Verify the following end-user behaviors:</td>
</tr>
</tbody>
</table>
How to Configure LDAP Authentication

LDAP authentication compares user login information against the profile database on an LDAPv2-compliant directory server. After users are authenticated by the LDAP server, they are automatically logged in to Cisco Unified MeetingPlace as long as their LDAP user IDs also exist in Cisco Unified MeetingPlace. You can also authenticate users against a multiple LDAP forest configuration.

With LDAP authentication, the following restrictions apply:

- Cisco Unified MeetingPlace Web Conferencing supports only unencrypted LDAP, that is, queries to the LDAP server are in clear text.
- Users cannot log in with their Cisco Unified MeetingPlace passwords for their same LDAP user names.
- LDAP profiles are used for authentication; Cisco Unified MeetingPlace profile passwords are ignored.
- Cisco Unified MeetingPlace enforces e-mail format validation when you have LDAP synchronization configured. If an e-mail address for a particular user does not conform to the standard e-mail format, the user is skipped during the LDAP synchronization process and not imported into the MeetingPlace database.

Standard e-mail format expressions include:

```
^([^w-_.]*\w+@([\da-zA-Z-]+\.)+[\da-zA-Z]{2,6}$
```

**Note**

To authenticate the web conferencing application against the LDAP server, make sure that the LDAP server directory is designed to have all users in one container rather than broken into multiple containers (each representing a child OU).

- Configuring LDAP Authentication, page 4
- Verifying the LDAP Authentication Configuration by Using the Web Page Form, page 6
- Verifying the LDAP Authentication Configuration by Using the HTTP Form, page 7

Configuring LDAP Authentication

**Before You Begin**

Read the “Restrictions: User Authentication and Load Balancing” section on page 2.
How to Configure LDAP Authentication

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select Web Server.
Step 4  Select the name of the Web Server that you want to configure in the “View” section of the page.
Step 5  Scroll to the Web Authentication section.
Step 6  Select LDAP for “Step 1: Directory”.
Step 7  Enter the LDAP hostname in the field provided.
Example: ldap.domain.com
Step 8  Enter the Distinguished Name (DN) information for your directory in the field provided noting the following considerations:

- Cisco Unified MeetingPlace user profile login names are limited to 17 characters; therefore, the LDAP match must be 17 characters or less.
- You can only enter one value for the LDAP Distinguished Name (DN) field. If your users are segregated into multiple organizational units (OUs), you can work around this issue by using either the DOMAIN\USER or user@ou.domain.com format for the DN. When configuring the LDAP Distinguished Name field, enter just %USERNAME%, without specifying an OU, DC, or other parameter.

Note  All users in the LDAP server directory must be in one container rather than broken into multiple containers each representing a child OU.

- %USERNAME% is the username that the user enters when logging in.
- Before sending the request to the LDAP server %USERNAME% is replaced with the username that the user enters in the login username field. No additional modifications are made to the DN value.
- %USERNAME% is case-sensitive, that is, all upper case.
- If you match any of the following circumstances, leave the DN field blank (empty) instead of entering %USERNAME%:
  - You are authenticating against a multiple LDAP forest configuration. Example: CN=%USERNAME%, OU=People, DC=mydomain, DC=com
  - The LDAP server you are using is the LDAP interface on a Microsoft Active Directory server. If this is the case, you must leave the DN field blank (empty) for authentication to work. When configured in this manner, the format of the usernames that the user enters must be DOMAIN\USER or user@ou.domain.com.
  - You want to send user passwords as protected (that is, not as clear text). Entering a value for the DN field sends passwords as clear text.

Note  If you choose to enter a value for the DN field, it is your responsibility to establish a secure connection between the Cisco Unified MeetingPlace web server and the LDAP server. This is not the same as configuring SSL configuration on the web server. The SSL feature in Cisco Unified MeetingPlace protects traffic between the client and web server. You will require a secure connection between the web server and the LDAP server.
Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing

How to Configure LDAP Authentication

Step 9
Select how you want user names transformed for “Username Conversion Function.”
Selecting None applies no transformation to the original user ID string.

Step 10
Select one of the following for “Step 2: Login Method.”
- Select Web Page Form to see an HTML-based Cisco Unified MeetingPlace login window.
- Select HTTP Basic Authentication to see a login window rendered by your web browser.

Step 11
Select Submit and wait five minutes for the new configuration to take effect.

Troubleshooting Tips
If you chose HTTP Basic Authentication as your login method, restart the Cisco Unified MeetingPlace Web Conferencing service after configuring your LDAP authentication. If you do not, users who change their passwords in LDAP will be able to log in to Cisco Unified MeetingPlace by using both their old and new passwords until the Cisco Unified MeetingPlace Web Conferencing service is restarted or after approximately 60 minutes.

Note
When you restart the web server, all manual changes made to the registry are lost.

What to Do Next
Based on your configuration, proceed to one of the following topics:
- Verifying the LDAP Authentication Configuration by Using the Web Page Form, page 6
- Verifying the LDAP Authentication Configuration by Using the HTTP Form, page 7

Verifying the LDAP Authentication Configuration by Using the Web Page Form

Use a Cisco Unified MeetingPlace end-user profile when completing this procedure.

Before You Begin
Complete the “Configuring LDAP Authentication” section on page 4.

Procedure

Step 1
Open a web browser and navigate to Cisco Unified MeetingPlace.

Step 2
Verify the following end-user behaviors:
- If you have a Cisco Unified MeetingPlace profile, you can log in with your LDAP password.
- You cannot log in as a profiled user without a password.

Related Topics
- Configuring LDAP Authentication, page 4
Verifying the LDAP Authentication Configuration by Using the HTTP Form

Use a Cisco Unified MeetingPlace end-user profile when completing this procedure.

**Before You Begin**

Complete the “Configuring LDAP Authentication” section on page 4.

**Procedure**

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Open a web browser and navigate to Cisco Unified MeetingPlace.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Verify the following end-user behaviors:</td>
</tr>
<tr>
<td></td>
<td>• When you access the Cisco Unified MeetingPlace home page, you see an Enter Network Password window.</td>
</tr>
<tr>
<td></td>
<td>• After you enter your LDAP profile user ID and password, you are authenticated to the Cisco Unified MeetingPlace Application Server.</td>
</tr>
<tr>
<td></td>
<td>• The Welcome page displays your name in firstname, lastname order.</td>
</tr>
<tr>
<td></td>
<td>• Sign In and Sign Out links do not display.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring LDAP Authentication, page 4

How to Configure LDAP then MeetingPlace Authentication

This authentication mode attempts to authenticate users against two directories if the need arises. When users first log in, they are authenticated against the LDAP directory. If this authentication fails, the login information is sent to the Cisco Unified MeetingPlace Application Server for a possible match. This behavior allows a company to give non-LDAP users, such as guests or contractors, access to Cisco Unified MeetingPlace.

**Note**

Cisco Unified MeetingPlace enforces e-mail format validation when you have LDAP synchronization configured. If an e-mail address for a particular user does not conform to the standard e-mail format, the user is skipped during the LDAP synchronization process and not imported into the MeetingPlace database. Standard email addresses are in the form user@domain. User is limited to upper and lower case alphanumeric characters and period (dot), dash, and underscore. Domain is limited to alphanumeric characters and period (dot) and dash (no underscore). No spaces are permitted.

- Prerequisites for Configuring LDAP Then MeetingPlace Authentication, page 8
- Configuring the LDAP Then MeetingPlace Authentication, page 8
- Verifying the LDAP Then MeetingPlace Authentication Configuration by Using the Web Page Form, page 9
- Verifying the LDAP Then MeetingPlace Authentication Configuration by Using the HTTP Form, page 10
Prerequisites for Configuring LDAP Then MeetingPlace Authentication

- To authenticate Cisco Unified MeetingPlace Web Conferencing against the LDAP server, make sure that the LDAP server directory is designed to have all users in one container rather than broken into multiple containers (each representing a child OU).
- If a match is made in the LDAP database, the user must provide the proper LDAP password. Three attempts with the incorrect password will lock the LDAP profile of the user.
- Only users who are not found in the LDAP directory are eligible for authentication through the Cisco Unified MeetingPlace directory.
- User IDs in the Cisco Unified MeetingPlace profile database are not case-sensitive.

Related Topics
- How to Configure LDAP then MeetingPlace Authentication, page 7

Configuring the LDAP Then MeetingPlace Authentication

Before You Begin
Read the “Restrictions: User Authentication and Load Balancing” section on page 2.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Web Server.
Step 4 Select the name of the Web Server that you want to configure in the “View” section of the page.
Step 5 Scroll to the Web Authentication section.
Step 6 Select LDAP, then MeetingPlace for “Step 1: Directory”.
Step 7 Enter the LDAP hostname in the field provided.
   Example: ldap.domain.com
Step 8 Enter the Distinguished Name (DN) information for your directory in the field provided noting the following considerations:
   - Cisco Unified MeetingPlace user profile login names are limited to 17 characters; therefore, the LDAP match must be 17 characters or less.
   - You can only enter one value for the LDAP Distinguished Name (DN) field. If your users are segregated into multiple organizational units (OUs), you can work around this issue by using either the DOMAIN\USER or user@ou.domain.com format for the DN. When configuring the LDAP Distinguished Name field, enter just %USERNAME%, without specifying an OU, DC, or other parameter.
     - You are authenticating against a multiple LDAP forest configuration. Example: CN=%USERNAME%, OU=People, DC=mydomain, DC=com.
     - The LDAP server you are using is the LDAP interface on a Microsoft ActiveDirectory server. If this is the case, you must leave the DN field blank for authentication to work. When configured in this manner, the format of the user names that the user enters must be DOMAIN\USER or user@ou.domain.com.
You want to send user passwords as protected (that is, not as clear text). Entering a value for the DN field sends passwords as clear text.

**Note**
If you choose to enter a value for the DN field, it is your responsibility to establish a secure connection between the Cisco Unified MeetingPlace web server and the LDAP server. This is not the same as configuring SSL configuration on the web server. The SSL feature in Cisco Unified MeetingPlace protects traffic between the client and web server. You will require a secure connection between the web server and the LDAP server.

- Consult your LDAP expert for your DN information.

**Step 9**
Select how you want user names transformed for “Username Conversion Function.”
Selecting None applies no transformation to the original user ID string.

**Step 10**
Select one of the following for “Step 2: Login Method”:
- Select **Web Page Form** to see an HTML-based Cisco Unified MeetingPlace login window.
- Select **HTTP Basic Authentication** to see a login window rendered by your web browser.

**Step 11**
Select **Submit** and wait five minutes for the new configuration to take effect.

**What to Do Next**
Based on your configuration, proceed to one of the following topics:
- Verifying the LDAP Then MeetingPlace Authentication Configuration by Using the Web Page Form, page 9
- Verifying the LDAP Then MeetingPlace Authentication Configuration by Using the HTTP Form, page 10

### Verifying the LDAP Then MeetingPlace Authentication Configuration by Using the Web Page Form

Use a Cisco Unified MeetingPlace end-user profile when completing this procedure.

**Before You Begin**
Complete the “Configuring the LDAP Then MeetingPlace Authentication” section on page 8.

**Procedure**

**Step 1**
Open a web browser and navigate to Cisco Unified MeetingPlace.

**Step 2**
Verify the following end-user behaviors:
- You can log in with your LDAP password.
- You cannot log in without a password.
- If you have a Cisco Unified MeetingPlace profile, you can log in and schedule meetings.
• If you do not have a Cisco Unified MeetingPlace profile, you can only attend and search public meetings.

Related Topics
• How to Resolve Authentication Problems in the Troubleshooting Cisco Unified MeetingPlace Web Conferencing module.

Verifying the LDAP Then MeetingPlace Authentication Configuration by Using the HTTP Form

Use a Cisco Unified MeetingPlace end-user profile when completing this procedure.

Before You Begin
Complete the “Configuring the LDAP Then MeetingPlace Authentication” section on page 8.

Procedure

Step 1
Open a web browser and navigate to Cisco Unified MeetingPlace.

Step 2
Verify the following end-user behaviors:
• You can log in with your LDAP password.
• You cannot log in without a password.
• If you have a Cisco Unified MeetingPlace profile, you can log in and schedule meetings.
• This option does not allow you to log in to Cisco Unified MeetingPlace as a guest, that is, without a Cisco Unified MeetingPlace profile.

Related Topics
• How to Resolve Authentication Problems in the Troubleshooting Cisco Unified MeetingPlace Web Conferencing module.

How to Configure Trust External Authentication

Trust External Authentication represents a broad-range of enterprise security software that provides functions like authentication, resource access authorization, Single Sign On (SSO), and intrusion detection. Typically, this software protects your Web Server by installing a DLL plug-in into the Web Server service, for example IIS. This DLL plug-in, also called ISAPI Filter, intercepts user login credentials and passes them to a corporate authentication and authorization server. The software must be able to output user IDs in the HTTP header so that they can be passed to Cisco Unified MeetingPlace for authentication.

Note
Users cannot log in to Cisco Unified MeetingPlace as guests after you have configured this authentication mode.
Customer Premise Equipment (CPE) customers who implement SSO software integrations on their Cisco Unified MeetingPlace Web Servers do so at their own risk and are responsible for understanding the technical implementations and feasibility of SSO integrations on their systems.

By allowing SSO software integrations, we do not claim support for any SSO software packages or vendors.

Using SSO software integrations requires proper configuration of Cisco Unified MeetingPlace Web Conferencing systems through the Admin pages. If your SSO software integration requires a change in the Web Conferencing product source code, your SSO integration becomes an SSO customization, and we do not support customizations by either customers or any other parties.

Any CPE customers who want to integrate SSO packages can contact Cisco Managed Services to obtain a Service Request to implement SSO. This service is offered as a convenience and does not change the scope of the SSO integration: this service is an integration and configuration of the Web Conferencing product, not a customization of the product code.

Customers must first implement SSO software integrations on test or lab servers and verify that the integrated systems work, including Web Conferencing features and operations.

Customers are responsible for ensuring stability of integrated Web Conferencing-SSO systems, including communicating with SSO software vendors for the following reasons:

- To obtain necessary fixes and support
- To troubleshoot functional problems and technical problems, including crashes triggered by the SSO package

Many SSO software products include a web-server extension, called the IIS ISAPI extension or filter. Web Conferencing installs and uses four IIS extensions. Any incompatibility between an SSO software extension and the Web Conferencing extensions can make IIS non-functional or unstable. Any crash of the SSO IIS extension can cause IIS to crash and can generate a full Web Conferencing outage, resulting in a full system restart, ending of in-progress meetings, and disconnecting of Web Conferencing users. Any memory leak in the SSO package or module can make IIS or the whole server unstable, as well.

**Note**

When you restart the web server, all manual changes made to the registry are lost.

Although SSO software integration is productized for the Web Conferencing system, any changes in overall configuration, including Web Conferencing upgrades and SSO package upgrades, can potentially break integrated Web Conferencing-SSO systems.
Terms of Support for Single Sign On Software Integration

Customers must inform Cisco TAC that their Cisco Unified MeetingPlace Web Servers have third-party SSO packages installed and configured with Web Conferencing when opening a service request for Web Conferencing, Cisco Unified MeetingPlace for Microsoft Outlook, or Cisco Unified MeetingPlace for IBM Lotus Notes.

Customers must be able to provide SSO integration details upon request. Inability to provide details can result in Cisco TAC not being able to proceed with service requests.

If a service request is about troubleshooting the SSO integration, Cisco TAC can review the logs and identify whether the problem is on the SSO side or the Web Conferencing side. If the problem is on the SSO side, information will be provided to customers, so they can further troubleshoot with their SSO vendors.

If the service request is about troubleshooting a Web Conferencing problem that does not seem to be connected to the SSO integration, Cisco TAC will proceed per the normal support process. If TAC discovers that the SSO integration plays a role in the problem, information will be provided to customers, so they can further troubleshoot with their SSO vendors.

If Cisco TAC believes the problem is triggered by an SSO package, Cisco TAC can require customers to disable the SSO package to troubleshoot further.

Microsoft Debug Diagnostic tool, also called DebugDiag, may be required for troubleshooting IIS crashes and memory leaks to determine if these problems are produced by the SSO package.

Restrictions for Configuring Trust External Authentication

When configuring Trust External authentication, make sure that the /mpweb/scripts/public/ directory is not protected by SSO. Protecting this directory will prevent web conferencing from functioning properly.

To use SSO, you must enable SSL on the Application Server. If you have a failover system, with active and standby servers, ensure that SSL is installed and configured on the standby server as well as on the active server. This way, SSO will continue to work if the system has to move the standby server for any reason.

Related Topics
- How to Configure Trust External Authentication, page 10

Configuring Trust External Authentication

Before You Begin
- Read the “Restrictions: User Authentication and Load Balancing” section on page 2.
- Read the “Terms for Single Sign On Software Integration” section on page 11.
- Read the “Terms of Support for Single Sign On Software Integration” section on page 12.

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing

How to Configure HTTP Basic Authentication (Domain)

Step 3  Select **Web Server**.

Step 4  Select the name of the Web Server that you want to configure in the “View” section of the page.

Step 5  Scroll down to the Web Authentication section.

Step 6  Select **Trust External Authentication** for “Step 1: Directory.”

Step 7  Enter an appropriate value for an external service for “HTTP Header Containing Username.”

Example: Enter HTTP_SM_USER for SiteMinder.

Step 8  Select how you want user names transformed for “Username Conversion Function.”

Selecting None applies no transformation to the original user ID string.

Step 9  Select **Submit** and wait five minutes for the new configuration to take effect.

What to Do Next
(Optional) Proceed to the “Verifying the Trust External Authentication Configuration” section on page 13.

Verifying the Trust External Authentication Configuration

Use a Cisco Unified MeetingPlace end user profile when completing this procedure.

Before You Begin
Complete the “Configuring Trust External Authentication” section on page 12.

Procedure

Step 1  Open your web browser and navigate to the Cisco Unified MeetingPlace home page.

Step 2  Verify the following end-user behaviors:

- Using a SiteMinder environment, you are immediately authenticated to MeetingPlace with your SiteMinder user ID and password.
- If you have a Cisco Unified MeetingPlace profile, you can log in with your SiteMinder password and schedule meetings.

How to Configure HTTP Basic Authentication (Domain)

The HTTP basic authentication method is a widely used industry-standard method for collecting user ID and password information. It works as follows:

1. Users are prompted by a pop-up login window that is rendered by their web browser.
2. Users enter valid domain user IDs and passwords.

Cisco Unified MeetingPlace profile passwords are ignored and not used in the authentication operation.
3. If the Web Servers accept the login credentials and the user IDs also exist in Cisco Unified MeetingPlace profile databases, users are logged in automatically to Cisco Unified MeetingPlace and are granted access to the Cisco Unified MeetingPlace home page.

Note
The Cisco Unified MeetingPlace profile user ID must match the domain user ID of the user.

The advantage of HTTP Basic Authentication is that it is part of the HTTP specification and is supported by most browsers. The disadvantage is that the password is Base 64-encoded before being sent over the network. Since Base64 is not a true encryption, it can be easily deciphered. You can mitigate this security risk by implementing Secure Socket Layer (SSL) on the Web Server.

- Configuring HTTP Basic Authentication (Domain), page 14
- Verifying the HTTP Basic Authentication (Domain) Configuration, page 15

Configuring HTTP Basic Authentication (Domain)

Before You Begin
Read the “Restrictions: User Authentication and Load Balancing” section on page 2.

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select Web Server.
Step 4  Select the name of the Web Server that you want to configure in the “View” section of the page.
Step 5  Scroll down to the Web Authentication section.
Step 6  Select HTTP Basic Authentication (Domain) for “Step 1: Directory.”
         “Step 2: Login Method” is automatically set to HTTP Basic Authentication and cannot be changed.
Step 7  Enter your default logon domain in the field provided.
Step 8  Select how you want user names transformed for “Username Conversion Function.”
         Selecting None applies no transformation to the original user ID string.
Step 9  Select Submit and wait five minutes for the new configuration to take effect.

What to Do Next
(Optional) Proceed to the “Verifying the HTTP Basic Authentication (Domain) Configuration” section on page 15.
Verifying the HTTP Basic Authentication (Domain) Configuration

Use a Cisco Unified MeetingPlace end-user profile when completing this procedure.

**Before You Begin**
Complete the “Configuring HTTP Basic Authentication (Domain)” section on page 14.

**Procedure**

**Step 1**
Open a web browser and navigate to Cisco Unified MeetingPlace.

**Step 2**
Verify the following end-user behaviors:

- You see an Enter Network Password dialog when accessing the home page.
- If you have a local account on the Windows server and a matching profile user ID, you are authenticated to the Cisco Unified MeetingPlace when you enter your domain user ID and password.
- If you have a Cisco Unified MeetingPlace profile, your name displays on the Welcome page as firstname, lastname and the Sign In link no longer displays.
- You can only log in to Cisco Unified MeetingPlace if you are authenticated by the Cisco Unified MeetingPlace Web Server.
- In IIS, the MPWeb/Scripts folder is set to Basic Authentication.

How to Configure Windows Integrated Authentication

- Windows Integrated Authentication, page 15
- Login Behavior with Windows Integrated Authentication, page 16
- Configuring Windows Integrated Authentication, page 16
- Verifying the Windows Integrated Authentication Configuration, page 17
- Configuring SiteMinder for Use With Cisco Unified MeetingPlace Web Conferencing, page 18

Windows Integrated Authentication

Windows Integrated Authentication (WIA) uses an algorithm to generate a hash based on the credentials and computers that users are using. WIA then sends this hash to the server; user passwords are not sent to the server. If WIA fails for some reason, such as improper user credentials, the browser prompts users to enter their user IDs and passwords. The Windows logon credentials are encrypted before being passed from the client to the Web Server.

**Tip**
You can configure Internet Explorer version 4.0 or later to initially prompt for user information if needed. For more information, see the Internet Explorer documentation.

Windows Integrated Authentication (WIA) is secure, but has the following limitations:

- Only Microsoft Internet Explorer version 4.0 or later supports this authentication method.
• WIA does not work across proxy servers or other firewall applications.
• WIA works only under the browser Intranet Zone connections and for any trusted sites you have configured.
• WIA does not work on Web servers with SSL enabled.

Therefore, WIA is best suited for an intranet environment where both users and the Web Server are in the same domain and where administrators can ensure that every user has Microsoft Internet Explorer. The Web Server must be in a Windows domain.

Refer to Microsoft online documentation to further ensure or verify that your network supports WIA.

Login Behavior with Windows Integrated Authentication

**When WIA Works Properly:**

• Users log in to their workstations by using their Windows NT domain accounts.
• If their NT account user IDs also exist in the Cisco Unified MeetingPlace profile database, users are automatically logged in to Cisco Unified MeetingPlace and granted access to the home page. Cisco Unified MeetingPlace user passwords are ignored and not used in the SSO operation.
  
  The home page does not have Sign In links to the HTML-based login form because users are already logged in through the SSO process.
• If their NT account user IDs do not match any user IDs in the Cisco Unified MeetingPlace directory, users see the Cisco Unified MeetingPlace home page, but with Sign In links to the HTML-based login form. Users must then enter valid Cisco Unified MeetingPlace user IDs and passwords.
• (System administrators only) If a user selects Sign Out from the Cisco Unified MeetingPlace Web Administration, then the user is logged out and returns to the home page. To log back in, the user may select Sign In and enter the valid Cisco Unified MeetingPlace user ID and password.

**When WIA Does Not Work Properly:**

• Users see a popup window prompting them for their Cisco Unified MeetingPlace user IDs and passwords.
• If their credentials are authenticated in the Cisco Unified MeetingPlace directory, users see the Cisco Unified MeetingPlace home page.
• If authentication fails, users are prompted continually for their valid login credentials.

---

**Note**

Cisco Unified MeetingPlace user IDs are not case-sensitive.

**Related Topics**

• Read the “Terms for Single Sign On Software Integration” section on page 11.
• Read the “Terms of Support for Single Sign On Software Integration” section on page 12.

Configuring Windows Integrated Authentication

**Before You Begin**

Read the “Restrictions: User Authentication and Load Balancing” section on page 2.
Restrictions

- Each user must have an account (local or Active Directory) on the Windows NT Server and must also have a Cisco Unified MeetingPlace profile user ID that matches the account name.
- Users must be using Microsoft Internet Explorer version 4.0 or later.
- WIA works only under the browser Intranet Zone connections. By default, only pages without any dots in the URL are considered to be in the Intranet Zone.
- WIA does not work across proxy servers or other firewall applications.

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select Web Server.
Step 4  Select the name of the Web Server that you want to configure in the “View” section of the page.
Step 5  Scroll down to the Web Authentication section.
Step 6  Select Windows Integrated Authentication for “Step 1: Directory.”
   “Step 2: Login Method” is automatically set to HTTP Basic Authentication and cannot be changed.
Step 7  Select how you want user names transformed for “Username Conversion Function.”
   Selecting None applies no transformation to the original user ID string.
Step 8  Select Submit and wait five minutes for the new configuration to take effect.

What to Do Next
(Optional) Proceed to the “Verifying the Windows Integrated Authentication Configuration” section on page 17.

Verifying the Windows Integrated Authentication Configuration

Use a Cisco Unified MeetingPlace end-user profile when completing this procedure.

Before You Begin
Complete the “Configuring Windows Integrated Authentication” section on page 16.

Procedure

Step 1  Open a web browser and navigate to Cisco Unified MeetingPlace.
Step 2  Verify the following end-user behaviors:
   - If you are on the same domain, you are immediately authenticated to the Web Server and see the Welcome page with your name displayed in firstname, lastname order. The Sign In link does not display.
   - If you are on a different domain, you see an Enter Network Password window that includes the Domain field.
• If you are on a different domain, enter your Windows NT account user ID and password. You are then authenticated to the Cisco Unified MeetingPlace Web Server and see the Welcome page with your name displayed in firstname, lastname order. The Sign In link does not display.
• Only users authenticated by the Web Server can log in.
• In IIS, the MPWeb/Scripts folder is set to Integrated Windows Authentication.

Troubleshooting Tips
If you configured your Web Server Home Page hostname by using an IP address or FQDN, you will be prompted for your Windows login information even if you log in by using your domain Windows account.

See “How to Resolve Authentication Problems” in the Troubleshooting Cisco Unified MeetingPlace Web Conferencing module for a workaround to this problem.

See “Setting Your Web Server Options” in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module for information about configuring your Web Server Home Page hostname.

Configuring SiteMinder for Use With Cisco Unified MeetingPlace Web Conferencing
If your deployment includes the SiteMinder application for authentication and single-sign on support, you will need to make the following changes to the SiteMinder configuration so that it can interoperate properly with Cisco Unified MeetingPlace Web Conferencing Release 7.1.

String Blocking in URLs
SiteMinder looks for invalid strings in all URLs before processing. Web Conferencing uses internal URLs that include the “.” character (period), which is blocked by the default SiteMinder configuration. The default block is:

```
badurlchars="./, /., /*, *., ~, \, %00-%1f,%7f-%ff"
```

In order for Web Conferencing to function properly, remove ./ from the badurlchars string, for example:

```
badurlchars="/., /*, *., ~, \, %00-%1f,%7f-%ff"
```

Localhost Redirection and Hostname Blocking in URLs
Web Conferencing uses internal URLs that include connecting to the localhost/loopback on port 8002, for example, http://localhost:8002. When SiteMinder receives a localhost request, it resolves localhost to the actual host name of the server. SiteMinder then looks up the host name in its list of hosts and matches it to the name of an agent. In order for web conferencing to function properly, you must add this agent name to the exception list so that it is not blocked by SiteMinder.

The following example shows the SiteMinder logging for a localhost request on port 8002:

```
[5812/7912][Tue Apr 24 14:00:07 2007][..\..\..\..\..\..\..\..\CSmHttpPlugin.cpp:219][INFO:2] PLUGIN: Read HTTP_HOST value 'localhost:8002'.
[5812/7912][Tue Apr 24 14:00:07 2007][..\..\..\..\..\..\..\..\CSmHttpPlugin.cpp:270][INFO:2] PLUGIN: ProcessResource - Resolved Host 'YOURHOSTNAME:8002'.
[5812/7912][Tue Apr 24 14:00:40 2007][..\..\..\..\..\..\..\CSmHttpPlugin.cpp:290][INFO:1] PLUGIN: ProcessResource - Resolved Agentname 'yourhostname-unprotected' for HTTP_HOST 'YOURHOSTNAME:8002'.
```
In the first line, SiteMinder processes the request to localhost on port 8002. In the second line, localhost is resolved to the actual hostname of the computer (in this example, YOURHOSTNAME). In the third line, YOURHOSTNAME:8002 is resolved to the agent defined in your SiteMinder configuration as yourhostname-unprotected. It is this agent name that must be allowed (not blocked) by SiteMinder in order for the request to succeed.

Accessing Cisco Unified MeetingPlace Web Conferencing When Locked-Out Due to Incorrect User Authentication Setup

If you configure Web Conferencing to use anything other than the MeetingPlace native login form for user authentication, you may not be able to log in to Cisco Unified MeetingPlace through the web due to incomplete user authentication configuration. For example, you configured LDAP, then MeetingPlace user authentication, but failed to enter a valid LDAP hostname or to ensure that the LDAP user IDs existed in MeetingPlace. In such circumstances, you are unable to log into Web Conferencing to correct your configuration errors.

To restore access to the web conferencing application, you can do one of the following:

- Log on to the Cisco Unified MeetingPlace Web Server, open a web browser, and browse to http://localhost:8002. You will be logged in as the technician and can access the admin pages to fix the problem.
- Edit the SQL database and reset the mode to MeetingPlace native login form.

The following SQL procedure describes how to update the Cisco Unified MeetingPlace web conferencing user authentication mode in SQL Server.

**Procedure**

**Step 1**
Open a DOS command window.

**Step 2**
Log in to the SQL server by entering `C:\osql -U userid -P password`, replacing `userid` and `password` with the appropriate value.

**Step 3**
Specify that you want to access the MPWEB database.

  a. Enter `use mpweb`.
  b. Enter `go`.

**Step 4**
Enter `Update web set AuthMode = 1`.

**Step 5**
Enter `Update web set AuthLoginMode = 1`.

**Step 6**
Enter `go`.

The following tables provide mode definitions as a reference.

<table>
<thead>
<tr>
<th>AUTHMODE Command</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>#define SQLCONFIG_AUTHMODE_NONE</td>
<td>0</td>
</tr>
<tr>
<td>#define SQLCONFIG_AUTHMODE_MP</td>
<td>1</td>
</tr>
<tr>
<td>#define SQLCONFIG_AUTHMODE_LDAP</td>
<td>2</td>
</tr>
<tr>
<td>#define SQLCONFIG_AUTHMODE_LDAPMP</td>
<td>3</td>
</tr>
<tr>
<td>#define SQLCONFIG_AUTHMODE_TRUSTEXT</td>
<td>4</td>
</tr>
</tbody>
</table>
### AUTHMODE Command Values

<table>
<thead>
<tr>
<th>AUTHMODE Command</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>#define SQLCONFIG_AUTHMODE_BASIC_DOMAIN</td>
<td>5</td>
</tr>
<tr>
<td>#define SQLCONFIG_AUTHMODE_WIA</td>
<td>6</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AUTHMODE Command</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>#define SQLCONFIG_AUTHLOGINMODE_NONE</td>
<td>0</td>
</tr>
<tr>
<td>#define SQLCONFIG_AUTHLOGINMODE_WEB</td>
<td>1</td>
</tr>
<tr>
<td>#define SQLCONFIG_AUTHLOGINMODE_HTTP</td>
<td>2</td>
</tr>
</tbody>
</table>
Configuring the Cisco Unified MeetingPlace Web Conferencing User Interface

Release 7.1
Revised: April 3, 2011 8:30 pm

The Cisco Unified MeetingPlace web-based user interface is composed of a set of template pages that allow users to complete various Cisco Unified MeetingPlace functions. As a system administrator, you can configure which fields are exposed to your users. This information is preserved in the MPWEB database and remains unaffected by Cisco Unified MeetingPlace Web Conferencing software upgrades. This module describes how to configure the web pages and features that your users see.

- Inserting a Logo on the Cisco Unified MeetingPlace Web Conferencing Home Page, page 1
- How to Configure Which Fields Appear on the User Interface, page 2
- How to Configure Field Names and Descriptions, page 3
- How to Reload a Custom Configuration, page 5
- How to Restore Default User Interface Settings, page 7
- Customizing the Session Expired Page, page 7
- Customizing the User Interface with Cascading Style Sheets, page 8

Inserting a Logo on the Cisco Unified MeetingPlace Web Conferencing Home Page

Complete this procedure to insert either a company logo or a blank logo on the Cisco Unified MeetingPlace home page.

Before You Begin
- Locate a logo 148 x 65 pixels or less and save it as logo.gif. A smaller logo works in this space, but a larger one results in the content of the screen shifting to the right.
- (Optional) If you do not want to include a logo on the Cisco Unified MeetingPlace home page, create a blank file 148 x 65 pixels and save it as logo.gif.
How to Configure Which Fields Appear on the User Interface

• Configuring Which Fields Appear on the User Interface, page 2
• Saving Your Field Configuration Changes, page 3

Configuring Which Fields Appear on the User Interface

Complete this procedure to select which fields appear on each page of the end-user web interface.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select User Interface Fields.
Step 4 Locate the “General” section of the page.
Step 5 Select the name of the Cisco Unified MeetingPlace page that you want to configure.
   The user interface fields for that page appear.
Step 6 Select an object in the Enabled column to expose or hide fields in the Cisco Unified MeetingPlace user interface.
   • A checkmark means that this field is exposed in the user interface.
   • An X means that this field is hidden in the user interface.

Note Hiding a field removes it from the web user interface and disables access to its functionality.

Step 7 Select Back to return to the main User Interface Fields administration page.

What to Do Next

(Optional) Proceed to the “Modifying or Creating a Field Name or Description” section on page 4 if you want to modify the names or descriptions displayed next to your exposed fields.
## Saving Your Field Configuration Changes

Complete this procedure to save an XML copy of the configuration changes that you made in your browser. This is useful if you ever need to reload the configuration.

**Procedure**

1. Step 1: Sign in to the end-user web interface.
2. Step 2: Select Admin.
4. Step 4: Locate the “Actions” section of the page.
5. Step 5: Select Export Custom User Interface Field Configuration.
6. Step 6: Save the resulting XML file to your hard drive by using the Save As option in your browser.

**Related Topics**

- Configuring Which Fields Appear on the User Interface, page 2

## How to Configure Field Names and Descriptions

- Locating a User Interface String, page 3
- Modifying or Creating a Field Name or Description, page 4
- Modifying an Error Message, page 4
- Saving Your Text Configuration Changes, page 5

## Locating a User Interface String

Complete this procedure to find the string ID associated with a field on the Cisco Unified MeetingPlace web user interface. You will need this string ID to do any modifications to the associated text.

**Procedure**

1. Step 1: Sign in to the end-user web interface.
2. Step 2: Browse to the page that contains the UI element you want to modify.
3. Step 3: Right-click next to the UI element and select **View Source**.
   - Notepad displays with the source code for the UI element.
4. Step 4: Open the Find window by pressing **Ctrl + F** on your keyboard.
5. Step 5: Enter your search term and select **Find Next**.
6. Step 6: When you locate the element you want to modify, read across to find its associated string ID, such as **String1234**.
What to Do Next

Proceed to the “Modifying or Creating a Field Name or Description” section on page 4 for instructions on how to modify this string.

Modifying or Creating a Field Name or Description

After configuring which fields will appear on Cisco Unified MeetingPlace web pages, you can select to modify the names or descriptions next to the exposed fields. This requires configuring the relevant strings in the MPWEB database. Such configurations are preserved in the database; therefore, the configurations are not affected by Cisco Unified MeetingPlace Web Conferencing software upgrades. This tool also allows you to create new strings to enter into the MPWEB database.

Before You Begin

If you are modifying the name of a current field, make sure that you know the string ID for that field. See the “Locating a User Interface String” section on page 3 for instructions.

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select User Interface Text.
Step 4  Select Configure Strings.
Step 5  Enter a string ID.
   • If you are modifying a string, enter the ID number for the string that you want to modify, such as 1234.
   • If you are creating a new string, enter a new string ID.
Step 6  Select the language of the string.
Step 7  Select Submit.
   Default and custom information about this string displays.
Step 8  Locate the New String field.
Step 9  Enter the new text that you want to associate with this string.
Step 10 Select Change.
Step 11 Select Done or select Restore Default to revert to the default text.
Step 12 (Optional) Select Look Up a Different String and repeat Step 5 through Step 11.

Modifying an Error Message

Before You Begin

Complete the “Locating a User Interface String” section on page 3 so that you can identify the IDs for the error message strings that you want to modify.
How to Reload a Custom Configuration

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select User Interface Text.
Step 4  Select Configure Strings.
Step 5  Enter the sum of 1 million plus the error number that you want to modify.  
        For example, if you want to modify error 5432, enter 1005432.
Step 6  Select the language of the error message that you want to modify.
Step 7  Select Submit.
        Default and custom information about this string displays.
Step 8  Locate the New String field.
Step 9  Enter the new text that you want to associate with this error number.
Step 10 Select Change.
Step 11 Select Done or select Restore Default to revert to the default text.
Step 12 (Optional) Select Look Up a Different String and repeat Step 5 through Step 11.

Saving Your Text Configuration Changes

Complete this procedure to save an XML copy of the configuration changes you made in your browser.  
This is useful if you ever need to reload the configuration.

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select User Interface Text.
Step 4  Select Export Custom User Interface Strings.
Step 5  Save the resulting XML file to your hard drive by using the Save As option in your browser.

Related Topics

-  Reloading a Saved Text Configuration, page 6

How to Reload a Custom Configuration

-  Reloading a Saved Field Configuration, page 6
-  Reloading a Saved Text Configuration, page 6
Reloading a Saved Field Configuration

**Restriction**
You must have already saved a custom configuration to complete this procedure. See the “Saving Your Field Configuration Changes” section on page 3 for instructions.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stop the Cisco Unified MeetingPlace Web Conferencing Service.</td>
</tr>
<tr>
<td>2</td>
<td>Locate the XML copy of your configuration changes on your hard drive.</td>
</tr>
<tr>
<td>3</td>
<td>Copy the XML file to C:\Program Files\Cisco Systems\MPWeb\DataSvc.</td>
</tr>
<tr>
<td>4</td>
<td>Restart the Cisco Unified MeetingPlace Web Conferencing Service.</td>
</tr>
</tbody>
</table>

**Related Topics**
- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

Reloading a Saved Text Configuration

**Restriction**
You must have already saved a custom configuration to complete this procedure. See the “Saving Your Text Configuration Changes” section on page 5.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stop the Cisco Unified MeetingPlace Web Conferencing Service.</td>
</tr>
<tr>
<td>2</td>
<td>Locate the XML copy of your configuration changes on your hard drive.</td>
</tr>
<tr>
<td>3</td>
<td>Copy it to C:\Program Files\Cisco Systems\MPWeb\DataSvc.</td>
</tr>
<tr>
<td>4</td>
<td>Restart the Cisco Unified MeetingPlace Web Conferencing Service.</td>
</tr>
</tbody>
</table>

**Note**
When you restart the Web Server, all manual changes made to the registry are lost.

**Related Topics**
- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
How to Restore Default User Interface Settings

- Restoring Default Field Settings, page 7
- Restoring Default Text Settings, page 7

Restoring Default Field Settings

⚠️ Caution
Following this procedure removes all of the configurations that were completed with the User Interface Field configuration tool.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select User Interface Fields.
Step 4 Locate the “Actions” section of the page.
Step 5 Select Revert to Default.
Step 6 Select OK in the pop-up window to confirm your action.

Restoring Default Text Settings

⚠️ Caution
This procedure removes all of the text configurations that were completed with the User Interface Text configuration tool.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select User Interface Text.
Step 4 Select Revert to Default.
Step 5 Select OK in the pop-up window to confirm your action.

Customizing the Session Expired Page

Complete this procedure to send profiled users with expired or invalid session IDs to the Session Expired page. For example, you can have this page display an error and redirect users back to a particular site.
Configuring the Cisco Unified MeetingPlace Web Conferencing User Interface

Customizing the User Interface with Cascading Style Sheets

Cisco Unified MeetingPlace Web Conferencing applies cascading style sheets (CSS) to determine the look of the web-based user interface. These CSS files affect all web pages (the home page, meeting scheduling pages, Admin pages, account settings, and so on) but do not affect the meeting console.

When a web page links to multiple CSS files, the styles defined in these files affect the page in a cascading manner—styles applied later in the chain override earlier styles. The Cisco Unified MeetingPlace web pages link first to up to two predefined mpweb.css files (one for the base page and the other for a specific language if the page is not in U.S. English) and then to two customer-definable custom.css files (again for the base page and for another language).

You can create custom.css files to do two things:

- Define specific styles (for example, to change the page background colors). Because these files are not created during installation, they are preserved during upgrades.
- Hide user-interface strings that you cannot hide by using the User Interface Field configuration tool.

Caution
Do not modify the installed mpweb.css files. Modifications to these files are not supported and will not be preserved during upgrades.

Caution
You cannot use the “Restoring Default Text Settings” section on page 7 to re-display strings that you hide by using this procedure. Instead, you will have to delete the text that you enter in this procedure.

Before You Begin

- We recommend that you do not alter the style sheet files unless you are familiar with HTML style sheets.
- If you are hiding user interface strings, complete the “Locating a User Interface String” section on page 3 so that you can identify the IDs for the strings that you want to modify.

Procedure

Step 1
Create a file named custom.css.

Step 2
Apply the custom.css file to a language by completing one of the following:

- Save the file to drive:\Cisco Systems\MPWeb\HTML to apply the file to U.S. English.
- Save the file to drive:\Program Files\Cisco Systems\MPWeb\HTML\xxx, where xxx is one of the following language IDs:
  - English: 000
  - French: 006
Step 3  (Optional) To turn off a string, enter the following information in the file:

```
.string-number
{
    display:none
}
```

Step 4  Apply the desired style in the custom.css file.

Step 5  Save the custom.css file.
Restrictions for Accessing Meeting Data from an External (DMZ) Web Server

External users can access meeting details, attachments, and recordings only within the first 24 hours after the meeting has ended. External users can access this meeting data on the external Web Server by doing one of the following:

- Using the click-to-attend link in the meeting notification.
- Entering the Meeting ID in the end-user web interface on the external Web Server.

Meeting data is available for a longer period to profiled users from the internal Web Server, depending on how the Days until meeting statistics purged field on the Meeting Configuration Page was configured at the time the meeting was scheduled.

Related Topics

- Field Reference: Meeting Configuration Page
- Configuring External Access to Cisco Unified MeetingPlace Web Conferencing
Prerequisites for Configuring SMA-2S

Before you configure SMA-2S, make sure that you install Cisco Unified MeetingPlace Web Conferencing in an SMA-2S deployment.

Note
If you have Cisco Security Agent running, SSH access to the external Web Server will be blocked. You may want to consider other access modules, such as VNC or Remote Desktop, to provide access to the external Web Server.

What to Do Next
Proceed to the “Configuring Redirection of External Meetings” section on page 2.

Configuring Redirection of External Meetings

External meetings are held on an external Web Server so that users can access their meetings from the Internet. Rather than have all of your users log in to a particular external Web Server, configure automatic redirection of all external meetings from your internal Web Servers to a designated external Web Server.

Before You Begin
Complete the “Prerequisites for Configuring SMA-2S” section on page 2.

Procedure

Step 1 Sign in to the end-user web interface on the internal Web Server.
Step 2 Select Admin.
Step 3 Select Web Server.
Step 4 From a blank Web Server Name field, enter the name of a new Web Server to represent your designated external Web Server.
Step 5 Enter the fully qualified domain name (FQDN) of your external Web Server in the Hostname field, that is, hostname.domain.com. If your Web Server is not in a Domain Name Server (DNS), enter the IP address instead.
   • You must be able to resolve this hostname from the internal Web Server.
   • If you are using SSL, make sure that the hostname on the SSL certificate resolves to the external Web Server IP address.
   • If you are using SSL and a segmented DNS, make sure that the DNS name and the SSL certificate name differ.
Step 6 Select Submit to add this Web Server to the database.
This server now appears as part of your list of Web Servers in the “View” section of the page.
Step 7 Return to the main Administration page and select Site.
Step 8 Select the Site Name that represents your cluster of internal Web Servers.
Note  Site Name should have a default value equal to the NetBIO name of the first Web Server you installed in this cluster.

Step 9  Select the external Web Server you just added for DMZ Web Server. This configures the internal Web Servers in this cluster to point to this external Web Server in the case of external meetings.

Step 10  Select Submit.

Tip  The external cluster does not require any additional SQL Server database configurations.

What to Do Next
Proceed to the “How to Test Your SMA-2S Configuration” section on page 3.

How to Test Your SMA-2S Configuration

- Testing Internal Meetings, page 3
- Testing External Meetings, page 4

Testing Internal Meetings

Before You Begin
Complete the “Configuring Redirection of External Meetings” section on page 2.

Procedure

Step 1  Open your web browser to an internal Cisco Unified MeetingPlace website.
Step 2  Sign in by using a Cisco Unified MeetingPlace profile with System Manager privileges.
Step 3  Schedule a meeting with internal access and add two attachment files.
   a.  From the Welcome page, select Schedule Meeting.
   b.  Set your meeting details, including meeting date and time.
   c.  Select No for Allow External Web Participants.
   d.  Select Attachments/Recordings and add two attachments: a document file and a Microsoft PowerPoint attachment, then select OK.
   e.  Select Schedule.
Step 4  Verify that you received a notification for the meeting you scheduled in Step 3.
Step 5  From inside the private corporate network, verify that the internal click-to-attend link in your notification works by selecting the link.

- If you attended a meeting on this Web Server previously, you are directed to the meeting console.
• If you have not attended a meeting on this Web Server previously, the full-access Cisco Unified MeetingPlace web user interface displays.

**Step 6**
From the Internet, verify that the internal click-to-attend link in your notification does not work by selecting the link.

**Step 7**
Verify that you can attend the meeting.

• If you attended a meeting on this Web Server previously, select the click-to-attend link to go directly into the meeting console.

• If you have not attended a meeting on this Web Server previously, enter the meeting ID and select **Attend Meeting** from the Cisco Unified MeetingPlace home page.

**Step 8**
Verify that you are logged in as your profile by making sure that your profile name displays in the meeting console.

---

**What to Do Next**
Proceed to the “Testing External Meetings” section on page 4.

---

**Testing External Meetings**

**Before You Begin**

• You must have a Cisco Unified MeetingPlace profile with System Manager privileges to complete this procedure.

• Complete the “Testing Internal Meetings” section on page 3.

**Procedure**

**Step 1**
Open your web browser to an internal Cisco Unified MeetingPlace website.

**Step 2**
Sign in by using a Cisco Unified MeetingPlace profile with System Manager privileges.

**Step 3**
Schedule a meeting with external access, and add two attachment files by completing the following steps:

a. From the Welcome page, select **Schedule Meeting**.

b. Set your meeting details, including your meeting date and time.

c. Select **Yes** for Allow External Web Participants.

d. Select **Attachments/Recordings** and add two attachments: a document file and a Microsoft PowerPoint attachment, then select **OK**.

e. Select **Schedule**.

**Step 4**
Verify that you received a notification for the meeting you scheduled in **Step 3**.

**Step 5**
Verify that the external click-to-attend link in your notification works by selecting the link.

• If you attended a meeting on this Web Server previously, you are directed to the meeting console.

• If you have not attended a meeting on this Web Server previously, the external attend-only Cisco Unified MeetingPlace web user interface displays.
Step 6 Verify that you can attend the meeting.
   • If you attended a meeting on this Web Server previously, select the click-to-attend link to go directly in to the meeting console.
   • If you have not attended a meeting on this Web Server previously, enter a meeting ID and select Attend Meeting.

Step 7 Verify that you are logged in as your profile by making sure that your profile name displays in the meeting console.

Step 8 Verify that you can access the attachments and slide show from the external Web Server.
   a. From the meeting console, select the Attachments tab to verify that you can open an attachment.
   b. From the meeting console, select the Slides tab to verify that you can see the slides.
   c. Switch to Presentation mode to verify that the first slide displays in the web collaboration window.

How to Disable SMA

This section describes how to disable Segmented Meeting Access (SMA), which you need to do before upgrading the Application Server.

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Site.
Step 4 Select the underlined site name.
Step 5 For the field called “DMZ Web Server”, ensure that the value is set to -none-.
Step 6 Select Submit.
Configuring Cisco Unified MeetingPlace Web Conferencing and SQL Server

Release: 7.1
Revised: April 3, 2011 8:30 pm

All SQL Servers are required to be local to the Cisco Unified MeetingPlace server that is handling the replication. SQL Servers can be “remote” in that they are installed on separate machines within a local data center. However, Release 7.1 does not support attaching to an SQL Server in a remote data center.

**Note**

The SQL commands and operations described in this section are provided only for your convenience and should not be treated as definitive reference. For additional details about these commands and operations, search the Microsoft Knowledgebase for your version of Microsoft SQL Server.

- Accessing Information on the SQL Server Database, page 1
- How to Create and Use a Least-Privileged SQL Account for Web Conferencing, page 2
- Restoring the Cisco Unified MeetingPlace Web Server After Boot Failure, page 4
- How to Change and Apply a New SQL Password to Cisco Unified MeetingPlace Web Conferencing, page 5
- How to Manage the SQL Database Size, page 8
- How to Back Up and Restore MPWEB SQL Database, page 10
- Restoring Cisco Unified MeetingPlace Web Conferencing to a Different Server, page 16
- Relocating the Database, page 21
- Updating the Indices on the SQL Database, page 25
- How to Use a Custom TCP Port for the SQL Server Connection, page 26

## Accessing Information on the SQL Server Database

Use the Database administration page to access information on the SQL Server database.

**Restriction**

All SQL Servers are required to be local to the Cisco Unified MeetingPlace server that is handling the replication. SQL Servers can be “remote” in that they are installed on separate machines within a local data center. However, Release 7.1 does not support attaching to an SQL Server in a remote data center.
Before You Begin
If you have SQL Server installed on a separate machine, make sure that the time on SQL Server is synchronized with the Cisco Unified MeetingPlace Application Server and Web Server.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Sign into the end-user web interface.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select <strong>Admin</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select <strong>Database</strong>.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select a database command.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select <strong>Submit</strong>.</td>
</tr>
</tbody>
</table>

How to Create and Use a Least-Privileged SQL Account for Web Conferencing

By default, the Cisco Unified MeetingPlace Web Conferencing installer suggests using the SQL built-in sa administrator account as the SQL Server user name. Often, a strong password for the sa account is sufficiently secure to protect your system from unauthorized access. However, if you do not want to continue to use a SQL account that has full administration rights after the installation is complete, you can create a SQL account with minimal privileges that is dedicated for use with Cisco Unified MeetingPlace Web Conferencing, and configure the Web Server to use this account.

Complete the following procedures in the order shown to create and use a least-privileged SQL account:

- Creating a Least-Privileged SQL Account for Web Conferencing, page 2
- Updating SQL Account Access from the MeetingPlace Gateway Configurations Utility, page 3

Creating a Least-Privileged SQL Account for Web Conferencing

Caution
If you choose to create a SQL account that is dedicated for use with Cisco Unified MeetingPlace Web Conferencing, ensure that it meets all the specified database role requirements in this procedure. Failure to do so can cause a database connection failure between the web conferencing application and the SQL Server and result in a total outage or broken features.

Note
If Cisco TAC determines that your SQL account does not meet requirements, you will be asked to reconfigure your SQL account and to delete any existing Cisco Unified MeetingPlace Web Conferencing database so that a new database can be created once the account problem is remedied.
Procedure

Step 1 Open the SQL Server Enterprise Manager and create a new login:
   a. On the Start menu, select Programs > SQL Server 2000 > Enterprise Manager.
   b. Select a server group to expand it, then select the name of a server.
   c. Select Security > New Login.
   The SQL Server Login Properties window displays.
Step 2 Enter a name for the login on the General tab.
Step 3 Select SQL Server Authentication.
Step 4 Enter a password for the account.
Step 5 Select MPWEB from the Database drop-down menu to set the MPWEB database as the default database.
Step 6 Select the Database Access tab.
Step 7 Specify the database roles for the MPWEB database:
   a. Check the MPWEB database in the Databases table.
   b. Check the boxes for the following roles in the Database Roles table:
      – db_datareader
      – db_datawriter
      – db_ddladmin
Step 8 Repeat Step 7 for each additional MPWEB slave database.
   The slave databases have names that begin with “MPWEB_”. Depending on your deployment, your SQL Server will have either one or two slave databases.
Step 9 Select OK to complete the account configuration.

Updating SQL Account Access from the MeetingPlace Gateway Configurations Utility

The MeetingPlace Gateway Configurations utility allows you to update the Web Server with the least-privileged SQL login account that you have already created. It does not create a SQL Server login or update the SQL Server for you.

Before You Begin
Change the username and password on SQL Server. See the “Creating a Least-Privileged SQL Account for Web Conferencing” section on page 2 for instructions.

Procedure

Step 1 Stop the Cisco Unified MeetingPlace Web Conferencing Service.
Step 2 Open the MeetingPlace Gateway Configurations utility.
Step 3 Select the Web Conferencing tab.
Step 4  Enter the hostname or IP address of the SQL Server that you want to update in the Server field.
  • Enter local for a local server.
Step 5  Enter the username and password that you applied to the SQL Server.
Step 6  Select OK.
Step 7  Restart the Cisco Unified MeetingPlace Web Conferencing Service.

Note  When you restart the Web Server, all manual changes made to the registry are lost.

Related Topics
  • Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
  • Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
  • Opening the MeetingPlace Gateways Configuration Utility in the Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module

Restoring the Cisco Unified MeetingPlace Web Server After Boot Failure

Information in the Cisco Unified MeetingPlace Web Conferencing SQL database is replicated from the Cisco Unified MeetingPlace Application Server. As changes occur in the Application Server database, the SQL database is updated in real-time.

Each time the Web Server boots up, it compares the Application Server hostname that it has stored in the SQL database with that configured in the Gateway SIM. If the hostnames match, any changes that occur in the Application Server database are replicated to the SQL database in real-time.

If the hostnames do not match, Cisco Unified MeetingPlace Web Conferencing will consider the Application Server to have changed and fail to boot up.

Note  The hostname in the Cisco Unified MeetingPlace Web Conferencing SQL database is the value you entered when you installed the web conferencing application.

Before You Begin
Complete this procedure if you cannot start the Cisco Unified MeetingPlace Web Server because you changed the value of the hostname in the Gateway SIM.

Restrictions
This procedure is strictly limited to the situation where the database on the Cisco Unified MeetingPlace Application Server is the same as the database on the Cisco Unified MeetingPlace Web Server.
Caution

Misuse of this procedure in any other situations will cause database corruption and subsequent Cisco Unified MeetingPlace Web Conferencing functional failures.

Procedure

Step 1 Stop the Cisco Unified MeetingPlace Web Conferencing service.
Step 2 Verify that all web conferencing services are shutdown, including the IIS Admin Service and WWW Publishing Service.
Step 3 Open Enterprise Manager and navigate to the \Databases folder.
Step 4 Select and expand the MPWEB database.
Step 5 Select Tables from the left pane.
Step 6 Right-click System in the right pane.
Step 7 Select Open Table > Return All Rows.
Step 8 Change the value in the HostName column to the desired value.
Step 9 Start the Cisco Unified MeetingPlace Web Conferencing service or reboot the server.

Related Topics

- If the hostnames on the SQL Server and the Gateway SIM do not match because the Application Server has changed, see Changing the Cisco Unified MeetingPlace Application Server Connection Configured in the Gateway SIM in the Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module.
- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

How to Change and Apply a New SQL Password to Cisco Unified MeetingPlace Web Conferencing

Complete the following tasks in the order shown to change the SQL password and apply the new password to Cisco Unified MeetingPlace Web Conferencing:

- Changing the SQL Password If You Know the Old Password, page 5 or
- Changing the SQL Password if You Do Not Know the Old Password, page 6
- Applying the New SQL Password to Cisco Unified MeetingPlace Web Conferencing, page 7.

Changing the SQL Password If You Know the Old Password

Before You Begin
If you do not know the old password, proceed to the “Changing the SQL Password if You Do Not Know the Old Password” section on page 6.
Configuring Cisco Unified MeetingPlace Web Conferencing and SQL Server

How to Change and Apply a New SQL Password to Cisco Unified MeetingPlace Web Conferencing

Procedure

Step 1  Stop the Cisco Unified MeetingPlace Web Conferencing service.

⚠️ Caution  Changing the SQL Server account password while the Cisco Unified MeetingPlace Web Conferencing service is running will result in an immediate outage. Stop the service before continuing with the password change procedure.

Step 2  Open Enterprise Manager.
Step 3  Expand the Security folder.
Step 4  Select Logins.
A list of accounts displays on the right.
Step 5  Double-click the SQL account that you want to change.
Step 6  Change the password in the configuration window.

What to Do Next
Proceed to the “Applying the New SQL Password to Cisco Unified MeetingPlace Web Conferencing” section on page 7.

Related Topics

• Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

Changing the SQL Password if You Do Not Know the Old Password

Before You Begin
If you do know the old password, complete the “Changing the SQL Password If You Know the Old Password” section on page 5 instead.

Procedure

Step 1  Stop the Cisco Unified MeetingPlace Web Conferencing service.

⚠️ Caution  Changing the SQL Server account password while the Cisco Unified MeetingPlace Web Conferencing service is running will result in an immediate outage. Stop the service before continuing with the password change procedure.

Step 2  Open a DOS command window.
Step 3  Log in to SQL Server by entering `C:\osql -E nt_acct`, where `nt_acct` is NT account that has access right to the server.
Step 4  Change the password by entering `sp_password null, new_pwd, sa`, where `null` represents the password that you do not know and `new_pwd` is the new SQL password.
Step 5  Enter go.

Example: Changing the SQL Password by Using osql
This example shows the osql commands executed to log in to osql by using the NT account mpadmin and to change the SQL account SA password from some unknown value to new_pwd.

```
C:\>osql -E mpadmin
1> sp_password null, new_pwd, sa
2>   go
   Password changed
1> exit
```

What to Do Next
Proceed to the “Applying the New SQL Password to Cisco Unified MeetingPlace Web Conferencing” section on page 7.

Related Topics
- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

Applying the New SQL Password to Cisco Unified MeetingPlace Web Conferencing

Before You Begin
- Ensure that the username and password information that you will provide exists on the SQL Server and that the proper database access rights are assigned.

  See the “Creating a Least-Privileged SQL Account for Web Conferencing” section on page 2 for more information.

- Verify that all web conferencing services are stopped, including IIS Admin and WWW Publishing services.

⚠️ Caution
You cannot create or change the username or password on the SQL Server in the Web Conferencing tab. This tab supplies Cisco Unified MeetingPlace Web Conferencing with only the proper SQL database login information.

- Complete either the “Changing the SQL Password If You Know the Old Password” section on page 5 or the “Changing the SQL Password if You Do Not Know the Old Password” section on page 6. You will need this information for Step 3 of this procedure.

Procedure

Step 1  Open the Cisco Unified MeetingPlace Gateway Configurations utility.
Step 2  Select the Web Conferencing tab.
Step 3  Change the old SQL password to the new SQL password.
Step 4  Select Apply.
Step 5  Select OK.

Step 6  Restart the Cisco Unified MeetingPlace Web Conferencing service.

Note  When you restart the Web Server, all manual changes made to the registry are lost.

Related Topics
- Opening the MeetingPlace Gateways Configuration Utility in the Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module
- Modifying the SQL Database Properties to Manage Database Size, page 8
- Examples: Modifying the SQL Database Properties to Manage Database Size, page 9

How to Manage the SQL Database Size

- Modifying the SQL Database Properties to Manage Database Size, page 8
- Examples: Modifying the SQL Database Properties to Manage Database Size, page 9

Modifying the SQL Database Properties to Manage Database Size

The MPWEB database that Cisco Unified MeetingPlace Web Conferencing creates is comprised of two files: MPWEB.mdf and MPWEB.ldf. The MDF file contains the actual data, while the LDF contains changes (both the content and timing) made to that data.

On a SQL server that has been actively and properly managed through regular database backup, this LDF file (also called Transaction Log) remains a reasonable size. However, if the SQL database has not been backed up in a while, this transaction log may become very large.

To help prevent the file from growing too large, configure the following three properties for the MPWEB database:
- Recovery = Simple
- Torn Page Detection = On
- Auto Shrink = On

Caution  This procedure applies only to the MPWEB database. Do not apply this procedure to any MPWEB slave database (these databases have names that begin with “MPWEB_”).

Procedure

Step 1  Open a DOS command window.

Step 2  Log in to SQL Server by entering C:\osql -U userid -P password, replacing userid and password with the applicable value.

Step 3  See the current properties of the database.
   a. Enter sp_helpdb MPWEB.
   b. Enter go.
Step 4  Modify properties.
   a. Enter `alter database mpweb set auto_shrink on, recovery simple, torn_page_detection on`.
   b. Enter `go`.

Step 5  If you are low on disk space because the database file is already large, force an immediate database
        shrink and remove empty space in the database files by entering `dbcc shrinkdatabase ('mpweb', percent)`. where `percent` is the amount of free space that you want to allow.

Examples: Modifying the SQL Database Properties to Manage Database Size

In the following examples, the output is displayed for each command that is used in the “How to Manage the SQL Database Size” section on page 8.

Sample Output for Viewing Current Database Properties
In this example, Recovery Mode is set to FULL and Torn Page Detection and Auto Shrink are not configured on this database.

```
1> sp_helpdb MPWEB
2> go
name     db_size       owner        dbid    created         status      compatibility_level
```

Sample Output for Modifying Database Properties
```
1> alter database mpweb set auto_shrink on, recovery simple, torn_page_detection on
2> go
1> sp_helpdb MPWEB
2> go
name     db_size       owner        dbid    created         status      compatibility_level
```

Sample Output for Decreasing File Size
In this example, the size of the files are decreased in the MPWEB database to allow 10 percent free space in the files of MPWEB.
```
1> dbcc shrinkdatabase ('mpweb', 10)
2> go
DbId    FileId    CurrentSize    MinimumSize    UsedPages    EstimatedPages
-------- -------- -------------- ----------- --------------- --------------
 5      2        2912           1280         2912           1280
(1 row affected)
DBCC execution completed. If DBCC printed error messages, contact your system administrator.
```
How to Back Up and Restore MPWEB SQL Database

Complete the following procedures in the order shown to back up and restore the MPWEB database:

- Creating a Backup File by Exporting the MPWEB Database, page 10
- Examples: Exporting the MPWEB Database to Create a Backup File, page 11
- Restoring the Database, page 12
- Examples: Restoring the Database, page 14
- Restoring Cisco Unified MeetingPlace Web Conferencing to a Different Server, page 16

Creating a Backup File by Exporting the MPWEB Database

This backup file can be restored only on a SQL Server 2000 with equivalent or later service pack installed.

Procedure

Step 1  Export the MPWEB database.

- To export the MPWEB database to create a backup copy while Cisco Unified MeetingPlace Web Conferencing is running (as part of a daily backup procedure, for example), proceed to Step 2.

  or

- To export the MPWEB database so that it can be imported on another SQL Server that can continue operations for this Cisco Unified MeetingPlace Web Server, stop the Cisco Unified MeetingPlace Web Conferencing service and wait for all of the web conferencing services, IIS Admin service, and World Wide Web publishing service to cease.

Step 2  Access the SQL Server.

- If the SQL Server that is hosting the MPWEB database runs on the Cisco Unified MeetingPlace Web Server, access the command prompt.
  a. Select Start > Run.
  b. Enter cmd.

  or

- If the SQL Server hosting the MPWEB database runs on a separate Windows server, locate that Windows server and log on.

Note If you cannot log on to the applicable Windows server, log on to any Windows-based workstation or server on the network that has a valid installation of SQL Server Client tools, including the osql command, so that you can connect remotely to the SQL Server.

Step 3  Connect to SQL Server by using osql with the SA account and the appropriate password.

- Enter osql -U sa -S servername, where servername is the Windows server name.
- If the SQL Server runs locally, you can omit the option -S servername.
- If you are not allowed to connect to this SQL Server as sa, connect by using an account with enough privileges to back up a database.
Step 4 Select a fully qualified path and filename for your database export.

Note If you are connected to the SQL Server by running osql on a remote workstation or server, this path must be valid on the Windows server that hosts SQL Server, not on your local workstation.

Step 5 Export the database.
   a. Enter `backup database MPWEB to disk = 'fullyqualifiedpath',` where `fullyqualifiedpath` is the location that you chose in Step 4.
   b. Enter `go`.

Step 6 Review the informational messages to confirm that the operation is successful.

Step 7 Determine the slave database name(s) on your SQL Server.
   a. Enter `select name from sysdatabases where name like 'MPWEB%'.` 
   b. Enter `go`.

The results should include either one or two slave databases.

Step 8 Back up the slave database(s).
   a. Enter `backup database [MPWEB_XX] to disk = 'C:\temp\mpweb_XX.dat',` where `XX` are the digits of the first slave database and brackets enclose the database name.
   b. Enter `go`.

Step 9 Repeat Step 8 for the second slave database, if applicable.

Step 10 Enter `exit` to exit osql.

Step 11 Save the mpweb.dat and each mpweb_XX.dat file in a safe location, on a tape or network drive on another server, for example.

Related Topics
- Examples: Exporting the MPWEB Database to Create a Backup File, page 11

What to Do Next
Proceed to the “Restoring the Database” section on page 12

Examples: Exporting the MPWEB Database to Create a Backup File

In the following examples, the output is displayed for each command that is used in the “Creating a Backup File by Exporting the MPWEB Database” section on page 10.

Sample Output for Connecting to the SQL Server
```
C:> osql -U sa -S SERVERNAME
Password: password
1>
```

Sample Output for Exporting to the Database
```
1> backup database MPWEB to disk = 'C:\temp\mpweb.dat'
2> go
```
Sample Output for Viewing Informational Messages
Processed 616 pages for database 'MPWEB', file 'MPWEBData' on file 1.
Processed 3 pages for database 'MPWEB', file 'MPWEBLog' on file 1.
BACKUP DATABASE successfully processed 619 pages in 1.709 seconds (2.962 MB/sec)

Sample Output for Determining the Slave Database Name
In this example, the name of the slave database is MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1.
1> select name from sysdatabases where name like 'MPWEB%'
2> go
---------------------------------------------------
<table>
<thead>
<tr>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPWEB</td>
</tr>
<tr>
<td>MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1</td>
</tr>
</tbody>
</table>
---------------------------------------------------

Sample Output for Backing Up the Slave Database
1> backup database [MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1] to disk = 'C:\temp\mpweb_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1.dat'
2> go

Sample Output for Exiting osql
1> exit
C:

Restoring the Database

Before You Begin
- You must have a file called mpweb.dat or mpweb_XX.dat.
- This file must have been exported with the backup database command from a SQL Server release that is earlier or equal to the release of the SQL Server to which you want to import the database. See the “Creating a Backup File by Exporting the MPWEB Database” section on page 10 for instructions.
- If you are restoring the database as part of a failed upgrade and had SSL configured on the original Web Server system, note that you will have to install the SSL certificates again after the restore.

Procedure

Step 1
Access the SQL Server.
- If the SQL Server that hosts the MPWEB database runs on the Cisco Unified MeetingPlace Web Server, access the command prompt.
  a. Select **Start > Run**.
  b. Enter **cmd**.
  or
- If the SQL Server hosting the MPWEB database runs on a separate Windows server, locate that Windows server and log on.
If you cannot log on to the separate Windows server, log on to any Windows-based workstation or server on the network that has a valid installation of SQL Server Client tools including the `osql` command, so you can connect remotely to the SQL Server.

**Step 2**

Connect to SQL Server by using `osql` with the SA account and the appropriate password.

- Enter `osql -U sa -S servername`, where `servername` is the Windows server name.
- If the SQL Server runs locally, you can omit the option `-S servername`.
- If you are not allowed to connect to this SQL Server as SA, connect by using an account with enough privileges to back up a database.

**Step 3**

Check if a database called MPWEB exists on this server.

- Enter `select name from sysdatabases where name like 'MPWEB%'`.
- Enter `go`.

**Step 4**

If a MPWEB database exists, verify that no Cisco Unified MeetingPlace Web Server is currently using this database.

**Step 5** (Optional)

If one or multiple Cisco Unified MeetingPlace Web Servers are using the database, complete the following:

- Log on as an administrator on each server.
- Stop the Cisco Unified MeetingPlace Web Conferencing service.
- Wait for all the Cisco Unified MeetingPlace Web Conferencing services, the IIS Admin service, and the World Wide Web publishing service to stop.
- Enter `drop database MPWEB` to drop the database.
- Enter `go`.

**Step 6**

Before you import your MPWEB database to SQL Server, find out which database physical files are associated with this MPWEB database.

- Enter `restore filelistonly from disk = 'C:\temp\mpweb.dat'`.
- Enter `go`.

**Step 7**

Verify the installation folder of the SQL Server where you want to restore this database and check the physical location of the SQL Server master database.

- Enter `sp_helpfile master`.
- Enter `go`.

**Note**

Unless you have a specific reason to restore your MPWEB database to another disk location, such as for performance and tuning or data recovery, we recommend that you restore the MPWEB database to the default Data folder of this SQL Server installation.

**Step 8**

Restore your database and relocate the database physical files to the correct location.

- Enter `restore database MPWEB from disk = 'C:\temp\mpweb.dat' with move 'MPWEBData' to 'D:\MSSQLServer\Data\MPWEB.MDF', move 'MPWEBLog' to 'D:\MSSQLServer\Data\MPWEB.LDF'`.
- Enter `go`. 
Note: You must use the **with move** clause to successfully restore the database because the database backup file contains physical file locations that are not valid for this SQL Server installation.

**Step 9**
Ensure that the operation was successful by reviewing the informational messages.

**Step 10**
Repeat Step 8 and Step 9 for each slave database to restore the MPWEB_XX slave database files.

**Step 11**
Enter **exit** to exit osql.

---

**Related Topics**
- Examples: Restoring the Database, page 14

**Examples: Restoring the Database**

In the following examples, the output is displayed for each command that is used in the “Restoring the Database” section on page 12.

**Sample Output for Connecting to SQL Server**

```
C:> osql -U sa -S SERVERNAME
Password: password
```

**Sample Output for Checking if the MPWEB Database Exists**

```
1> select name from sysdatabases where name = 'MPWEB'
2> go
```

```
name
---------------------
MPWEB
```

**Sample Output for Dropping the Database**

```
1> drop database MPWEB
2> go
Deleting database file 'D:\MSSQLServer\Data\MPWEB.LDF'.
Deleting database file 'D:\MSSQLServer\Data\MPWEB.MDF'.
```

**Sample Output for Checking Associated Files**

In this example, the MPWEB database was exported from a MSDE 2000 server. The default ‘Data’ folder for this server is D:\MSSQLServer\Data, and the MPWEB database was created with one data file (logical name = ‘MPWEBData’, physical name = D:\MSSQLServer\Data\MPWEB.mdf) and one log file (logical name = ‘MPWEBLog’, physical name = D:\MSSQLServer\Data\MPWEB.ldf).

```
1> restore filelistonly from disk = 'C:\temp\mpweb.dat'
2> go
```

```
---------------------------------------------------------------------
LogicalName      PhysicalName          Type     FileGroupName      Size        MaxSize
----------------- -------------------- -------- ------------------ ---------- -------------
----------------- -------------------- -------- ------------------ ---------- -------------
MPWEBData        D:\MSSQLServer\Data\MPWEB.mdf  D PRIMARY        2490368.000000 35184372080640.000000
MPWEBLog         D:\MSSQLServer\Data\MPWEB.ldf  L NULL            1310720.000000 35184372080640.000000
```
Sample Output for Verifying Folder Installation and Location of SQL Database

In this example, SQL Server (version 2000) was installed in D:\MSSQLServer, and the default 'Data' folder is D:\MSSQLServer\data.

```
1> sp_helpfile master
2> go
```

<table>
<thead>
<tr>
<th>name</th>
<th>filename</th>
<th>filegroup</th>
<th>size</th>
<th>maxsize</th>
<th>growth usage</th>
</tr>
</thead>
<tbody>
<tr>
<td>master</td>
<td>D:\MSSQLServer\data\master.mdf</td>
<td>PRIMARY</td>
<td>15744 KB</td>
<td>Unlimited</td>
<td>10%</td>
</tr>
</tbody>
</table>

```
1>
```

Sample Output for Restoring the MPWEB Database by Using the Move Clause

In this example, additional running upgrade step messages are displayed because the database backup file was created by an earlier version of SQL Server.

```
1> restore database MPWEB from disk = 'C:\temp\mpweb.dat' with move 'MPWEBData' to 'D:\MSSQLServer\Data\MPWEB.MDF', move 'MPWEBLog' to 'D:\MSSQLServer\Data\MPWEB.LDF'
2> go
```

Processed 216 pages for database 'MPWEB', file 'MPWEBData' on file 1.
Processed 1 pages for database 'MPWEB', file 'MPWEBLog' on file 1.
Converting database 'MPWEB' from version 515 to the current version 539.
Database 'MPWEB' running the upgrade step from version 515 to version 524.
Database 'MPWEB' running the upgrade step from version 524 to version 525.
Database 'MPWEB' running the upgrade step from version 525 to version 526.
Database 'MPWEB' running the upgrade step from version 526 to version 527.
Database 'MPWEB' running the upgrade step from version 527 to version 528.
Database 'MPWEB' running the upgrade step from version 528 to version 529.
Database 'MPWEB' running the upgrade step from version 529 to version 530.
Database 'MPWEB' running the upgrade step from version 530 to version 531.
Database 'MPWEB' running the upgrade step from version 531 to version 532.
Database 'MPWEB' running the upgrade step from version 532 to version 533.
Database 'MPWEB' running the upgrade step from version 533 to version 534.
Database 'MPWEB' running the upgrade step from version 534 to version 535.
Database 'MPWEB' running the upgrade step from version 535 to version 536.
Database 'MPWEB' running the upgrade step from version 536 to version 537.
Database 'MPWEB' running the upgrade step from version 537 to version 538.
Database 'MPWEB' running the upgrade step from version 538 to version 539.
To achieve optimal performance, update all statistics on the 'MPWEB' database by running sp_updatestats.
RESTORE DATABASE successfully processed 217 pages in 0.428 seconds (4.136 MB/sec).
```
1>
```

Sample Output for Restoring the MPWEB Slave Database

```
1> restore database [MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1] from disk = 'C:\temp\mpweb_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1.dat' with move 'MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1Data' to 'D:\MSSQLServer\Data\MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1.MDF', move 'MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1Log' to 'D:\MSSQLServer\Data\MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1.LDF'
2> go
```

Sample Output for Exiting osql

```
1> exit
C:>
```
Restoring Cisco Unified MeetingPlace Web Conferencing to a Different Server

Before You Begin
- If you are restoring the database as part of a failed upgrade and had SSL configured on the original Web Server system, note that you will have to install the SSL certificates again after the restore.
- This procedure assumes that you have a backup file that was saved before the upgrade.

Procedure

Step 1  Sign into another Web Server that is running just the operating system.
Step 2  Restore the backup file that was saved before the upgrade.
Step 3  Install Cisco Unified MeetingPlace Web Conferencing on top of it.

How to Detach and Attach the MPWEB SQL Database

This section describes part of the process for relocating the Cisco Unified MeetingPlace Web Server (MPWEB) database to a dedicated Microsoft SQL Server instance.

For performance and management reasons, you can choose to relocate the Cisco Unified MeetingPlace Web Conferencing SQL database (MPWEB) to your own standalone instance of Microsoft SQL Server 2000 or 2005 (in backward compatibility mode).

Note
All SQL Servers are required to be local to the Cisco Unified MeetingPlace server that is handling the replication. SQL Servers can be “remote” in that they are installed on separate machines within a local data center. However, Release 7.1 does not support attaching to an SQL Server in a remote data center.

Complete the following procedures in the order shown to detach and attach the MPWEB SQL database:
- Detaching the Database, page 16
- Examples: Detaching the Database, page 18
- Attaching the Database, page 19
- Examples: Attaching the Database, page 20
- Relocating the Database, page 21

Detaching the Database

You must detach the MPWEB database with the sp_detach_db command from a SQL Server release that is earlier or equal to the release of the SQL Server to which you want to import the database.

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Stop the Cisco Unified MeetingPlace Web Conferencing service.
Step 4  Wait for the Cisco Unified MeetingPlace Web Conferencing services, IIS Admin service, and World Wide Web Publishing service to stop.
Step 5  Access the SQL Server.
  • If the SQL Server hosting the MPWEB database runs on the Cisco Unified MeetingPlace Web Server, access the command prompt:
    a. Select Start < Run.
    b. Enter cmd.
  or
  • If the SQL Server hosting the MPWEB database runs on a separate Windows server, locate that Windows server and log on.

Note  If you cannot log on to the separate Windows server, log on to any Windows based workstation or server on the network that has a valid installation of SQL Server Client tools, including the osql command, so that you can remotely connect to the SQL Server.

Step 6  Connect to SQL Server by using osql with the SA account and the appropriate password.
  • If the SQL Server runs locally, you can omit the -S servername option.
  • If you are not allowed to connect to this SQL Server as SA, connect by using an account that has enough privileges to backup a database.
Step 7  Access the MPWEB database.
  a. Enter use mpweb.
  b. Enter go.
Step 8  Display a list of the database files.
  a. Enter sp_helpfile.
  b. Enter go.
Step 9  Access the SQL Server master database.
  a. Enter use master.
  b. Enter go.
Step 10 Detach the MPWEB database.
  a. Enter sp_detach_db 'MPWEB'.
  b. Enter go.
Step 11 Decide what you should do with the physical files that you identified in Step 8.
  These files constitute your detached database. For example, you can archive these files or use them to attach the associated MPWEB database to another SQL Server.
Step 12 Determine the slave database name(s) on your SQL Server.
  a. Enter select name from sysdatabases where name like 'MPWEB%'.
  b. Enter go.
Step 13 (Optional) For each additional database named MPWEB_XX, repeat Step 7 through Step 11 to detach that database, replacing the database name MPWEB with MPWEB_XX.
The databases are logically linked; therefore, if you want to archive the detached MPWEB database, you must do the same for each MPWEB_XX database. If you want to reattach the MPWEB database to another SQL Server, you must also reattach the MPWEB_XX database(s).

Step 14  Enter `exit` to exit osql.

Related Topics

- Examples: Detaching the Database, page 18
- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

Examples: Detaching the Database

In the following examples, the output is displayed for each osql command that is used in the “Detaching the Database” section on page 16.

Sample Output for Connecting to SQL Server

```
C:> osql -U sa -S SERVERNAME
Password: password
1>
```

Sample Output for Accessing the MPWEB Database

```
1> use mpweb
2> go
```

Sample Output for Displaying a List of Database Files

In this example, the database MPWEB relies on two physical files: C:\MSSQL2K\Data\MPWEB.mdf and C:\MSSQL2K\Data\MPWEB.ldf.

```
1> sp_helpfile
2> go
name    fileid    filename       filegroup  size    maxsize  growth  usage
--------- ---------- --------------------------- --------- ------- --------- -------
MPWEBData             1 C:\MSSQL2K\Data\MPWEB.mdf   PRIMARY 2432 KB Unlimited 1024 KB data only
MPWEBLog              2 C:\MSSQL2K\Data\MPWEB.ldf   NULL      1280 KB Unlimited 10% log only
```

Sample Output for Accessing the SQL Server Master Database

```
1> use master
2> go
```

Sample Output for Detaching the MPWEB Database

```
1> sp_detach_db 'MPWEB'
2> go
```
Sample Output for Determining the Slave Database Name

In this example, the name of the slave database is MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1.

1> select name from sysdatabases where name like 'MPWEB%'
2> go

<table>
<thead>
<tr>
<th>name</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPWEB_E22AF0EC-805F-45D4-8F76-FB0C6378A5EC-1</td>
</tr>
</tbody>
</table>

Sample Output for Exiting osql

1> exit
C:>  

Attaching the Database

Ensure that you have a valid detached MPWEB database, usually two files named MPWEB.mdf (data file) and MPWEB.ldf (log file) though file names may vary.

Procedure

Step 1 Access the SQL Server.

- If the SQL Server to which you want to attach your MPWEB database runs on the Cisco Unified MeetingPlace Web Server, access the command prompt.
  a. Select Start > Run.
  b. Enter cmd.

- If the SQL Server runs on a separate Windows server, locate that Windows server and log on.

  Note  If you cannot log on to that Windows server, log on to any Windows-based workstation or server on the network that has a valid installation of SQL Server Client tools, including the osql command, so that you can remotely connect to the SQL Server.

Step 2 Connect to SQL Server by using osql.

- Enter osql -U sa -S server-name, where server-name is the Windows SQL Server to which you want to attach the MPWEB database.
- If the SQL Server runs locally, you can omit the -S server-name option.

Step 3 Enter your password for the appropriate SA account.

  Note  If you are not allowed to connect to this SQL Server as SA, connect by using an account that has enough privileges to attach a database.

Step 4 Determine if a database named MPWEB already exists on this server.

  a. Enter select name from sysdatabases where name = 'MPWEB'.
How to Detach and Attach the MPWEB SQL Database

Step 5
If no MPWEB database exists, proceed to Step 6.

or

If a MPWEB database exists, ensure that it is not being used by an existing Cisco Unified MeetingPlace Web Server.

Note: You cannot attach a MPWEB database to this SQL Server if an active MPWEB database exists already. Before you proceed, you must detach the existing MPWEB database by completing the “Detaching the Database” section on page 16.

Step 6
To verify the installation folder of the SQL Server to which you want to restore this database, check the physical location of the SQL Server master database.

a. Enter `sp_helpfile master`.
b. Enter `go`.

Note: Unless you have a reason to restore your MPWEB database to another disk location, such as for performance and tuning or data recovery reasons, we recommend that you restore the database to the default data folder of this SQL Server installation.

Step 7
Copy the MPWEB.mdf and MPWEB.ldf files under the data folder that you identified in Step 6.

Step 8
Attach the MPWEB database.

a. Enter `sp_attach_db 'MPWEB','data path\MPWEB.mdf','data path\MPWEB.ldf`.
b. Enter `go`.

Step 9
(Optional) If you have a valid set of files for the MPWEB_XX slave database(s), repeat Step 4 through Step 9 for each slave database, replacing MPWEB with MPWEB_XX to attach that database.

Step 10
Enter `exit` to exit osql.

Examples: Attaching the Database

In the following examples, the output is displayed for each osql command that is used in the “Attaching the Database” section on page 19.

The following examples use the files MPWEB.mdf and MPWEB.ldf:

Sample Output for Connecting to SQL Server
C:> osql -U sa -S SERVERNAME
Password: password
1>

Sample Output for Checking if the MPWEB Database Exists
1> select name from sysdatabases where name = 'MPWEB'
2> go
name
-----------------------------------------------
(0 row affected)
Sample Output for Checking the Physical Location of the SQL Server Master Database

In this example, SQL Server Version 2000 is installed in C:\MSSQL2K, and the default data folder is C:\MSSQL2Kdata.

1> sp_helpfile master
2> go
name filename filegroup size maxsize growth usage
--------------------------------------------------------------------------
master
  C:\MSSQL2K\data\master.mdf
  PRIMARY
  15744 KB           Unlimited 10% data only
1>

Sample Output for Attaching the MPWEB Database

1> sp_attach_db 'MPWEB','data path\MPWEB.mdf','data path\MPWEB.ldf'
2> go

Sample Output for Exiting osql

1> exit
C:>

Relocating the Database

You may want to relocate the database and put the Cisco Unified MeetingPlace application and databases onto different servers. Examples are if the server you are using is running out of disk space, or for performance or backup considerations.

Note

Do not uninstall the local SQL Server if you are using remote SQL Server 2005. If, however, you are using remote SQL Server 2000, then you may choose to uninstall the SQL Server software and delete the MPWEB SQL database files from the Cisco Unified MeetingPlace Web Server.

Procedure

Step 1
Detach the MPWEB SQL databases on the existing (for example, local) SQL Server:
Follow the instructions in the “Detaching the Database” section on page 16.

Step 2
Attach the MPWEB SQL databases to the new SQL Server:
Follow the instructions in the “Attaching the Database” section on page 19.

Step 3
Change the Database Connection settings on your Cisco Unified MeetingPlace Web Conferencing server to point to the new SQL Server:

a. Double-click the orange door icon in the System Tray.
b. Select Web Conferencing.
c. Enter the new SQL server name in the Server field.
d. Enter the new Username and Password.
How to Replace a Cisco Unified MeetingPlace Web Server and Retain the SQL Database

During installation, a MPWEB database is tied to a specific Cisco Unified MeetingPlace Web Server through a unique GUIDWebID that is generated by the Cisco Unified MeetingPlace Web Conferencing installer. This GUIDWebID is stored in the registry and SQL database. Therefore, if you want to transfer the MPWEB SQL database and all attachments from the old server to a new server, the new server must use the same GUIDWebID as the old server. This requires preparing the following three components from the old server to the new server:

- The whole \MPWEB\Meetings folder (including all sub-folders) in zipped or unzipped format.
- The GUIDS.reg file with modifications to add the GUIDWebID and the mpweb slave database filename information. The GUIDS.reg file, as well as the GUIDWebID and DBName registry values, come from the old server.
- A backup of the MPWEB database and mpweb slave database(s) from the old server.

Complete the following procedures in the order shown to replace an existing Cisco Unified MeetingPlace Web Server with a new server and retain the attachments of past meetings so that they are accessible from the new server:

- Preparing the Current Cisco Unified MeetingPlace Web Server, page 22
- Installing the Replacement Cisco Unified MeetingPlace Web Server, page 23
- Building the Replacement Cisco Unified MeetingPlace Web Server, page 24

Preparation the Current Cisco Unified MeetingPlace Web Server

Procedure

**Step 1** Stop all Cisco Unified MeetingPlace Web Conferencing services, including the Gateway SIM service.

**Step 2** Detach this Cisco Unified MeetingPlace Web Server from the Cisco Unified MeetingPlace Application Server.

a. Open the Gateway SIM Agent.

b. From the Gateway SIM tab, write down the hostname or IP address of the Cisco Unified MeetingPlace Application Server for future reference.

Note: You must use the same server reference when you install the new Cisco Unified MeetingPlace Web Server. If the Application Server is specified as a hostname, you will enter that same hostname; if it is specified as an IP address, you will use an IP address later.

c. Select **Delete Unit** to detach this Web Server from the Application Server.

**Step 3** Make a copy of the entire \MPWEB\Meetings folder and its contents.

**Step 4** Make a copy of the GUIDS.reg file.
You can find this file where Cisco Unified MeetingPlace Web Conferencing application files are stored.

Step 5
Open regedit and obtain the registry values for GUIDWebID and DBName.

⚠️ Caution
Ensure that the registry values are correct. Compare the values that you obtained in Step 5 against what you enter in Step 6.

Step 6
Open GUIDS.reg in a text editor and add the GUIDWebID and DBName registry paths and key values.

Step 7
Save the file with these changes.

Step 8
Make a backup of the MPWEB database and the mpweb slave database(s).

Step 9
Copy the attachments, GUIDS.reg and the MPWEB backup, to the new server.

Related Topics
- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module
- Opening the MeetingPlace Gateways Configuration Utility in the Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module
- How to Back Up and Restore MPWEB SQL Database, page 10

What to Do Next
Proceed to the “Installing the Replacement Cisco Unified MeetingPlace Web Server” section on page 23.

Installing the Replacement Cisco Unified MeetingPlace Web Server

Replacement installations of Cisco Unified MeetingPlace Web Conferencing must match the version that was running on the old server. For example, if you are running Release 7.1 on the old server, you must install Release 7.1 or a later release on the new server.

Before You Begin
- Run GUIDS.reg on the new server to add the following four keys in to the registry: GUID IDs for Site, System, Web, and mpweb slave db filename. To run GUIDS.reg, right-click GUIDS.reg, then select merge.
- Have the “Preparing the Current Cisco Unified MeetingPlace Web Server” section on page 22 available to assist you with this procedure.

Procedure

Step 1
Install Cisco Unified MeetingPlace Web Conferencing.

Step 2
Reboot the server when you are prompted at the end of the installation.

After the initial reboot, the installation program continues and may reboot a few more times to complete the installation.
Step 3  When you are prompted for the Cisco Unified MeetingPlace Application Server information, enter the value that you wrote down in Step 2 of the “Preparing the Current Cisco Unified MeetingPlace Web Server” section on page 22.

Step 4  After the installation completes, verify that Cisco Unified MeetingPlace Web Conferencing is functional.

What to Do Next
Proceed to the “Building the Replacement Cisco Unified MeetingPlace Web Server” section on page 24.

Related Topics

Building the Replacement Cisco Unified MeetingPlace Web Server

Before you Begin
- Verify that the release of Cisco Unified MeetingPlace Web Conferencing that is installed on the new server is either the same or later than the release installed on the old server. For example, if you are running Release 7.1 on the old server, you must be running Release 7.1 or a later release on the new server.
- Know how to use Enterprise Manager or the osql drop database command.
  See the “Restoring the Database” section on page 12 for more information about the osql command.

Procedure

Step 1  Stop all Cisco Unified MeetingPlace Web Conferencing services.
Step 2  Use Enterprise Manager or the osql drop database command to delete the MPWEB SQL database. This database was created automatically during the Cisco Unified MeetingPlace Web Conferencing installation.
Step 3  Use either Enterprise Manager or the osql restore database command to restore the old MPWEB database on to the new server.
Step 4  Delete all contents in the \MPWeb\Meetings\ folder.
Step 5  Delete all contents in the \MPWeb\Web\WebConf\Content\7 folder.
Step 6  Restore all the files and attachments from the old server in to \MPWeb\Meetings folder.
Step 7  Restore all the files and attachments from the old server in to \MPWeb\Web\WebConf\Content\7 folder.
Step 8  Reboot the server or restart the Cisco Unified MeetingPlace Web Conferencing service.

Note  When you restart the Web Server, all manual changes made to the registry are lost.

Step 9  Update the Cisco Unified MeetingPlace Web Administration page.
  a.  Sign in to the end-user web interface with a System Manager profile.
b. Select Admin.
c. Select Web Server.
d. Update appropriate fields, such as the Web Server Hostname.

Related Topics
- Changing the Web Server Hostname From an IP Address to a Hostname
- Setting Your Web Server Options
- Stopping All Web Conferencing Services

### Updating the Indices on the SQL Database

The SQL database needs regular maintenance. If the SQL database is running slowly, or if the SQL database is running on a remote SQL server, then you should run this procedure on a nightly or weekly basis.

**Procedure**

**Step 1** Launch SQL Enterprise manager.
**Step 2** Select the Cisco Unified MeetingPlace Web Conferencing database, which is named something similar to MPWEB_<GUID_ID>_<Location>.
   <Location> can be either 1 or 2, depending on whether this is an internal or an external Web Server.
**Step 3** Select Tools > Wizards from the menu options at the top of the window.
**Step 4** Expand on the Management option.
**Step 5** Select Database Maintenance Plan Wizard.
**Step 6** Select Next on the Welcome to the Database Maintenance Plan Wizard page.
**Step 7** Select the database on the Select Database page, then select Next.
**Step 8** Check Reorganize data and index pages on the Update Data Optimization Information page, then select Next.
**Step 9** (Optional) Change the schedule on which this maintenance procedure runs.
**Step 10** Select Next on the Database Integrity Check page.
**Step 11** Uncheck Backup the database on the Specify the database backup plan page, then select Next.
**Step 12** Select Next on the following pages:
   - Specify backup disk directory page
   - Specify the transaction log backup plan page
   - Reports to generate page
   - Maintenance Pan History page
**Step 13** Select Finish on the Completing the maintenance plan wizard page.
How to Use a Custom TCP Port for the SQL Server Connection

**Note**
All SQL Servers are required to be local to the Cisco Unified MeetingPlace server that is handling the replication. SQL Servers can be “remote” in that they are installed on separate machines within a local data center. However, Release 7.1 does not support attaching to an SQL Server in a remote data center.

- Customizing the Port for an SQL Database, page 26
- Customizing the SQL Port for the “Remote” SQL Database, page 26
- Switching to the “Remote” SQL Database on the Custom Port, page 27

**Customizing the Port for an SQL Database**

**Procedure**

**Step 1**
In the SQL server network utility, perform the following:

- **Note**
  To perform this operation in SQL Server 2005, use the SQL Server Configuration Manager tool.

  - a. Select TCP.
  - b. Select Properties
  - c. Change the default port from 1433 to the desired port, then select OK.

**Step 2**
Stop the SQL server.

**Step 3**
Start the SQL server.

**Step 4**
Edit the registry:

  - a. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\ODBC.
  - b. Create a registry key of type DWORD named SlaveDBPort.
  - c. Set the created entry to your desired value for the port.

**Step 5**
Restart the Cisco Unified MeetingPlace Web Conferencing service.

- **Note**
  When you restart the Web Server, all manual changes made to the registry are lost.

**Customizing the SQL Port for the “Remote” SQL Database**

**Note**
All SQL Servers are required to be local to the Cisco Unified MeetingPlace server that is handling the replication. SQL Servers can be “remote” in that they are installed on separate machines within a local data center. However, Release 7.1 does not support attaching to an SQL Server in a remote data center.
Configuring Cisco Unified MeetingPlace Web Conferencing and SQL Server

How to Use a Custom TCP Port for the SQL Server Connection

Procedure

Step 1
Install Cisco Unified MeetingPlace Web Conferencing as usual, choosing remote database (this will install with the default port, 1433).

Step 2
Use the SQL server network utility to change the port on the remote database:

\[Note\]
To perform this operation in SQL Server 2005, use the SQL Server Configuration Manager tool.

a. Select TCP.
b. Select Properties.
c. Change the default port from 1433 to the desired port, then select OK.

Step 3
Stop the SQL server.

Step 4
Start the SQL server.

Step 5
Edit the registry:

a. Go to HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\ODBC.
b. Create a registry key of type DWORD named SlaveDBPort.
c. Set the created entry to your desired value for the port.

Step 6
Select Start > Programs > Administrative Tools > Open Data Sources (ODBC).

Step 7
Select System DSN.

Step 8
Select MPWEB.

Step 9
Select Configure.

Step 10
Select Next on the Microsoft SQL Server DSN Configuration screen.

Step 11
Select Client Configuration.

Step 12
Uncheck Dynamically determine port box.

Step 13
Enter your custom port number, then select OK.

Step 14
Close ODBC.

Step 15
Restart the Cisco Unified MeetingPlace Web Conferencing service.

\[Note\] When you restart the Web Server, all manual changes made to the registry are lost.

Switching to the “Remote” SQL Database on the Custom Port

Procedure

Step 1
Start with the local database on default port 1433.

Step 2
Stop the Cisco Unified MeetingPlace Web Conferencing service.

Step 3
Use the SQL server network utility to change the port on the remote database:
To perform this operation in SQL Server 2005, use the SQL Server Configuration Manager tool.

- Select **TCP**.
- Select **Properties**.
- Change the default port from 1433 to the desired port, then select **OK**.

**Step 4** Stop the SQL server.

**Step 5** Start the SQL server.

**Step 6** Edit the registry:
- Go to HKEY_LOCAL_MACHINE\SOFTWARE\Latitude\ODBC.
- Create a registry key of type DWORD named **SlaveDBPort**.
- Set the created entry to your desired value for the port.

**Step 7** Select **Start > Programs > Administrative Tools > Open Data Sources (ODBC)**.

**Step 8** Select **System DSN**.

**Step 9** Select **MPWEB**.

**Step 10** Select **Configure**.

**Step 11** Change the “Which SQL server do you want to connect to” field to the remote SQL server name.

**Step 12** Select **Next** on the Microsoft SQL Server DSN Configuration screen.

**Step 13** Select **Client Configuration**.

**Step 14** Uncheck **Dynamically determine port box**.

**Step 15** Enter your custom port number, then select **OK**.

**Step 16** Close ODBC.

**Step 17** On the web server, open the MeetingPlace Gateway Configuration utility and select **Web Conferencing**.

**Step 18** Change the database name from (local) to remote database.

**Step 19** Enter the user name and password for the remote database.

**Step 20** Select **Apply**, then **OK**.

**Step 21** Start the Cisco Unified MeetingPlace Web Conferencing service.
Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing

Release 7.1
Revised: April 3, 2011 8:30 pm

We recommend that you monitor heavily used systems at short intervals, such as biweekly or weekly. Monitor systems with lighter use less frequently, such as once a month.

- IIS File Deletion, page 1
- Configuring the Web Server to Synchronize with an NTP Server, page 2
- How to Manually Synchronize the Web Server with an NTP Server, page 3
- How to Manually Synchronize the Web Server in a Domain, page 4
- Changing the Time Zone, page 6
- Checking Which Conferences Are Currently Running, page 7
- Checking the Versions of Local Cisco Unified MeetingPlace Web Conferencing Services, page 8
- How to Schedule a Maintenance Window, page 8
- Optimizing the Performance of a Web Server, page 10
- Rebooting the Server, page 10
- How to Monitor Cisco Unified MeetingPlace Web Conferencing Activities, page 11
- How to Configure the Lumberjack Logging Utility, page 12
- How to Switch the Order of IP Addresses on the Web Server, page 15

IIS File Deletion

Deleting the default SMTP virtual server or the Administration website in IIS does not have any effect on Cisco Unified MeetingPlace Web Conferencing web pages.

Subfolders under wwwroot, such as images, _private, _vti_cnf, _vti_log, _vti_pvt, _vti_script and _vti_txt folders all come from Microsoft FrontPage. Deleting these subfolders can cause difficulty with Microsoft FrontPage when publishing to that server.

Parent Paths are enabled in the Default website, the MPWeb virtual directory and the cgi-bin virtual directory. Enabling Parent Paths allows anonymous users to use ‘.’ to move from the current directory to the parent. Disable this function to prevent such users from traversing the directory tree.
Configuring the Web Server to Synchronize with an NTP Server

Cisco Unified MeetingPlace Web Conferencing automatically sets up the Windows operating system to use the Windows Time Service to synchronize its clock with the NTP server. This keeps the Web Server synchronized with the Cisco Unified MeetingPlace Application Server.

You can also configure the Web Server to synchronize with an alternate NTP server. However, we recommend that all components in a Cisco Unified MeetingPlace system use the Application Server as their NTP time source.

Caution

Do not manually adjust the clock on the Web Server computer. Doing so could cause the Web Server to crash. To make a one-time manual adjustment, stop the Cisco Unified MeetingPlace Web Conferencing master service and restart it.

Note

If the time is not properly synchronized between the Web Server and the Application Server, web recordings may be either completely silent or the audio and web conferencing portions of a web recording will not be timed correctly.

Before You Begin

- Stop the Cisco Unified MeetingPlace Web Conferencing master service. See Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module.
- Be aware of the following:
  - By default, NTP uses UDP port 123. If your Web Server is in the DMZ and your Application Server is not, you will have to open UDP port 123 in your firewall for the default NTP configuration to work. The default configuration is the Web Server synchronizing with the Application Server as the NTP server.
  - If you decide to use an alternate NTP server for your Web Server time synchronization, make sure that your NTP setup keeps the Cisco Unified MeetingPlace Application Server and Web Server perfectly synchronized. If the two servers are not time synchronized, certain features will not work.
  - When you restart the Web Server, all manual changes made to the registry are lost.

Restrictions

Do not adjust the clock on the Windows computer while the web conferencing application is running.

Procedure

Step 1. Double-click the Window Time icon on the Windows system tray.

Step 2. Select the Internet Time tab.

Step 3. Select to automatically synchronize with an Internet time server.

Step 4. Specify your server name inside the Server: field.
How to Manually Synchronize the Web Server with an NTP Server

Complete the following procedures in the order shown.

**Note**
We recommend that all components in a Cisco Unified MeetingPlace system use the Application Server as their NTP time source.

- Querying Which NTP Server You Are Using, page 3
- Setting the NTP Server, page 3
- Checking the Delta Between the Local PC Clock and the NTP Server, page 4
- Manually Synchronizing the Web Server with the NTP Server, page 4

Querying Which NTP Server You Are Using

**Procedure**

**Step 1**
Open a DOS command window.

**Step 2**
Enter the following command: `net time /querysntp`

What to Do Next
Proceed to the “Setting the NTP Server” section on page 3.

Setting the NTP Server

**Procedure**

**Step 1**
Open a DOS command window.

**Step 2**
Enter the following command: `net time /setsntp:xyz` where `xyz` = the ip address or hostname of the NTP server.
What to Do Next
Proceed to the “Checking the Delta Between the Local PC Clock and the NTP Server” section on page 4.

Checking the Delta Between the Local PC Clock and the NTP Server

Before You Begin
• Complete the “Setting the NTP Server” section on page 3.
• Make sure that the Windows Time Service in the Services Control Panel is started.

Procedure

Step 1 Open a DOS command window.
Step 2 Enter the following command: \w32tm /monitor /computers:xyz where xyz is an NTP source.

What to Do Next
Proceed to the “Manually Synchronizing the Web Server with the NTP Server” section on page 4.

Manually Synchronizing the Web Server with the NTP Server

Before You Begin
• Complete the “Checking the Delta Between the Local PC Clock and the NTP Server” section on page 4.
• Make sure that the Windows Time Service in the Services Control Panel is started.

Procedure

Step 1 Open a DOS command window.
Step 2 Enter the following command: \w32tm /resync

How to Manually Synchronize the Web Server in a Domain

Complete the following tasks in the order presented to synchronize the time between your Cisco Unified MeetingPlace Application Server and Cisco Unified MeetingPlace Web Server if your Web Server machine is part of a domain.
• Pointing the Domain Controller to the External NTP Source, page 5
• Changing the Registry Setting on the Web Server, page 5
• Configuring the Application Server to Point to a Different NTP Server, page 6
Pointing the Domain Controller to the External NTP Source

Before You Begin
- This procedure is completed on the Domain Controller that includes the Cisco Unified MeetingPlace Web Server as part of its domain.
- Use export to save all of the registry settings to a flat file.

Procedure

Step 1 Open a command prompt.
Step 2 Enter the following command: `net stop W32Time`
Step 3 Point the domain controller to the external NTP source:
   - Run the following command: `w32tm /config /manualpeerlist:<NTP provider> /syncfromflags:manual /reliable:yes /update`
   - An example of an NTP provider is clock.cisco.com.
Step 4 If the previous command completed successfully, enter the following command: `net start W32Time`
Step 5 Verify that the external NTP source is active:
   - Run the following command: `w32tm /stripchart /<NTP provider> /samples:2/dataonly`
   - The output should show the local time and the external NTP provider time. Compare the two times to confirm that there are not any differences between them.

What to Do Next
Proceed to the “Changing the Registry Setting on the Web Server” section on page 5.

Changing the Registry Setting on the Web Server

Before You Begin
- This procedure is completed on the Cisco Unified MeetingPlace Web Server that is part of the domain.
- Complete the “Pointing the Domain Controller to the External NTP Source” section on page 5.
- Use export to save all of the registry settings to a flat file.

Procedure

Step 1 Open a command prompt.
Step 2 Enter the following command: `net stop W32Time`
Step 3 Run the following command: `w32tm /unregister`
Step 4 Run the following command: `w32tm / register`
Step 5 Change the value of the registry setting “HKLM\SYSTEM\CurrentControlSet\Services\W32Time\Parameters\Type” to `NT5DS`
   Initially, this will be set to NTP.
Step 6 Enter the following command: `net start W32Time`

Step 7 Run `w32tm /dumpreg` to verify that all of the registry settings are correct.

---

**Note**

If you upgrade or reboot the Web Server, all manual changes made to the registry by the W32Time command are lost.

**Note**

Do not expect the Web Server to match the external NTP source immediately after starting the `w32time` service. Synchronizing the time between the two systems will occur gradually.

---

**What to Do Next**

Proceed to the “Configuring the Application Server to Point to a Different NTP Server” section on page 6.

---

**Configuring the Application Server to Point to a Different NTP Server**

The Application Server currently points to the NTP server on the Application Server itself. Complete this procedure to point the Application Server to the NTP server referred to by the domain controller.

**Before You Begin**

- This procedure is completed on the Cisco Unified MeetingPlace Application Server that the Web Server points to.
- Complete the “Changing the Registry Setting on the Web Server” section on page 5.

**Procedure**

**Step 1** Sign in to the Cisco Unified MeetingPlace Application Server by using SSH with valid credentials.

**Step 2** Run the Net command and choose option 1 to list the current configuration.

The current configuration should point to the NTP server that is on the Application Server.

**Step 3** Select option 6 to configure the NTP Service.

**Step 4** When finished, select option 1 again to verify that the NTP provider is set correctly.

---

**Changing the Time Zone**

If the Windows time zone does not match the Cisco Unified MeetingPlace Web Server time zone, you must correct this discrepancy. The time zones may not match because you forgot to set the correct Windows time zone before installing Web Conferencing or because you have to relocate your Web Server from one time zone to another and you need to change the Windows time zone as part of this relocation.
To determine whether the time zones match, open the Web Conferencing log, called GWSIM_eventlog_XXX.txt, and search for the string “time zone”.

If the time zones are the same, you will see a message similar to this:

Information: CompareTimeZone: Time Zones are the same between Cisco Unified MeetingPlace Web Conferencing and Breeze. Cisco Unified MeetingPlace Web Conferencing: (GMT-08) Pacific Standard Time and Breeze: (GMT-08:00) Pacific Time (US)

If the time zones are not the same, the system logs an error and you see a message similar to this:

MasterSvc Error: **** Time Zones are NOT matching between Cisco Unified MeetingPlace Web Conferencing and Breeze. Time Zone Offset-- Cisco Unified MeetingPlace Web Conferencing: GMT:+01 Breeze: GMT:-08

To change the time zone, follow these instructions:

Procedu****

<table>
<thead>
<tr>
<th>Step</th>
<th>Instruction</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Stop the Cisco Unified MeetingPlace Web Conferencing master service on all Cisco Unified MeetingPlace Web Servers that use the same database.</td>
</tr>
<tr>
<td>2</td>
<td>Open the SQL Server Query Analyzer on the computer where the Web Conferencing SQL database is located by following these steps: &lt;br&gt;a. Select Start &gt; Programs &gt; Microsoft SQL Server &gt; Query Analyzer. &lt;br&gt;b. In the SQL Server field, select (local). &lt;br&gt;c. Select SQL Server authentication. &lt;br&gt;d. Enter the login name of “sa” and the password. &lt;br&gt;e. Select OK.</td>
</tr>
<tr>
<td>3</td>
<td>Select Query &gt; Change Database.</td>
</tr>
<tr>
<td>4</td>
<td>Highlight the name of the slave database (such as MPWEB_XXXX_XXXX), and select OK.</td>
</tr>
<tr>
<td>5</td>
<td>Enter the following SQL string: &lt;br&gt;select * from PPS_ENUM_TIME_ZONES</td>
</tr>
<tr>
<td>6</td>
<td>Select Execute Query.</td>
</tr>
<tr>
<td>7</td>
<td>Look through the time zone records and find your time zone ID from the TIME_ZONE_ID field.</td>
</tr>
<tr>
<td>8</td>
<td>Clear the command window by entering: &lt;br&gt;UPDATE PPS_ACL_PREFERENCES SET TIME_ZONE_ID = &lt;local_machine_timezone_id&gt; &lt;br&gt;where &lt;local_machine&gt;timezone_id&gt; is the time zone ID of the local machine.</td>
</tr>
<tr>
<td>9</td>
<td>Select Execute Query.</td>
</tr>
<tr>
<td>10</td>
<td>Start the Cisco Unified MeetingPlace Web Conferencing service on all Cisco Unified MeetingPlace Web Servers.</td>
</tr>
</tbody>
</table>

Checking Which Conferences Are Currently Running

Complete this procedure as a debugging tool to check which conferences are currently running on the Web Server.
Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select **Admin**.
Step 3  Select **Web Conferences**.

A list of currently running web conferences displays with the following properties:

- **Name**—A text identifier made up of the meeting subject and the dialable meeting ID.
- **Current User Count**—Lists the total number of web participants who are currently attending the conference. (Users dialed in to the meeting without an associated web session are not counted here.)
- **Peak User Count**—Lists the highest number of web participants who are concurrently attending the conference at any point since it began. (Users dialed in to the meeting without an associated web session are not counted here.)
- **Active Server**—The origin server that is hosting the meeting.
- **Duration**—Lists the elapsed time since the conference began.

Step 4  *(Optional)* Select **Back** to return to the main Administration screen.

---

**Checking the Versions of Local Cisco Unified MeetingPlace Web Conferencing Services**

Complete this procedure to check the release number of most local Cisco Unified MeetingPlace Web Conferencing modules. Releases of all listed modules, with the exception of Gateway SIM, must match, that is, 7.1.\(x.x\), where \(x.x\) is the same across all modules.

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select **Admin**.
Step 3  Select **Versions**.
Step 4  Review your module versions.
Step 5  Select **Back** to return to the main Administration screen.

---

**How to Schedule a Maintenance Window**

- Reserve All Ports Meetings, page 9
- Scheduling a Maintenance Window, page 9
Reserve All Ports Meetings

When you need to schedule time to perform upgrades or other maintenance activities to the Cisco Unified MeetingPlace system, schedule a Reserve All Ports meeting. When you schedule a Reserve All Ports meeting, the Cisco Unified MeetingPlace system performs the following actions:

- Reserves all available ports, or the maximum number of user licenses available in the system
- Blocks out all new callers for the duration of the scheduled meeting
- Prohibits the extension of in-session meetings that began before the Reserve All Ports meeting begins

Reserve All Ports meetings are scheduled, private meetings. The meeting attributes are the same as for scheduled meetings, with the exceptions described in the following table.

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Frequency</td>
<td>Once</td>
</tr>
<tr>
<td># of calling sites</td>
<td>SysMaintenance</td>
</tr>
<tr>
<td>Record meeting?</td>
<td>No</td>
</tr>
<tr>
<td>Meeting name</td>
<td>SysMaintenance</td>
</tr>
<tr>
<td>Meeting type</td>
<td>All Speaker</td>
</tr>
</tbody>
</table>

Scheduling a Maintenance Window

**Caution**

As a system administrator, it is your responsibility to ensure that no regular meetings are scheduled before scheduling a Reserve All Ports meeting.

**Caution**

Reserve All Ports meetings prevent the system from scheduling any meetings. Also, during a Reserve All Ports meeting, no prompts are played to alert users to the situation. For these reasons, we strongly recommend that you schedule Reserve All Ports meetings during the lowest usage times. In addition, be sure to cancel any Reserve All Ports meetings that you later determine you do not need.

**Before You Begin**

Remember the following information:

- You cannot extend a scheduled Reserve All Ports meeting, but you can reschedule the meeting.
- Only one Reserve All Ports meeting can be scheduled at a time (one Reserve All Ports meeting must be finished or deleted before another can be scheduled).
- If a Reserve All Ports meeting overlaps another scheduled meeting that is then canceled, the Reserve All Ports meeting reserves the ports released by the other meeting.
- Scheduled Reserve All Ports meetings appear in the server exception log, and any changes to a meeting (such as deleting or rescheduling) are shown in the log.
- If callers dial in to the server while a Reserve All Ports meeting is in session (and all ports are reserved), they hear nothing (silence).
- The meeting ID for a Reserve All Ports meeting cannot be changed.
Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing

Optimizing the Performance of a Web Server

Procedure

Step 1 Sign in to the end-user web interface with an Administrator profile.
Step 2 Select Schedule Meeting.
Step 3 Enter your date, time, and duration of your maintenance window.
Step 4 Select More Options.
Step 5 Check Reserve all ports meeting.
Step 6 Select Submit.
Step 7 Select Schedule.

Optimizing the Performance of a Web Server

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Web Server.
Scroll down to the “View” section of the page.
Step 4 Select the name of the Web Server that you want to configure.
Information about this Web Server populates the “Edit” section of the page.
Step 5 Select the setting that best describes your conferencing environment for Performance Tuning.

Note Setting this parameter to the highest level on a computer with inadequate hardware results in poor user performance.

Step 6 Select Submit.

Related Topics
- Field Reference: Web Server Specific Fields

Rebooting the Server

Complete the following procedure to shut down and restart the Web Server computer from the web interface.

Procedure

Step 1 Sign in to the end-user web interface.
How to Monitor Cisco Unified MeetingPlace Web Conferencing Activities

The Windows Event Viewer application and the Cisco Unified MeetingPlace Eventlog application both log all Web Server activities. You can use these logs to monitor or troubleshoot Cisco Unified MeetingPlace Web Conferencing.

- Using the Cisco Unified MeetingPlace Eventlog, page 11
- Running the Windows Performance Monitoring Tool, page 11
- Viewing an Event with the Windows Event Viewer, page 12

Related Topics
- Using Alarms and Logs on Cisco Unified MeetingPlace module
- How to Configure the Lumberjack Logging Utility, page 12

Using the Cisco Unified MeetingPlace Eventlog

The Eventlog application logs all activities specific to Cisco Unified MeetingPlace Web Conferencing services.

Procedure

Step 1 Right-click the Cisco Unified MeetingPlace icon in the system tray.
Step 2 Select Eventlog.
Step 3 Pull the eventlog from the Gateway SIM through the Cisco Unified MeetingPlace Application Server.

Running the Windows Performance Monitoring Tool

Complete this procedure to monitor the Cisco Unified MeetingPlace Web Conferencing performance object in the Windows performance monitoring tool.

Procedure

Step 1 Select Start > Run.
The Run window displays.

Step 2 Enter Perfmon.

Step 3 Select OK.

The Performance window displays.

Step 4 Select the Add (+) button.

The Add Counters window displays.

Step 5 Locate the Performance object field.

Step 6 Select Cisco MeetingPlace Web Conferencing.

A list of counters appear.

Step 7 Select to add or explain specific counters.

- Select a counter from the list and select Explain to get more information about it.
- Select a counter from the list and select Add to enable it.

Related Topics
- Counters Available in the Cisco Unified MeetingPlace Performance Object

Viewing an Event with the Windows Event Viewer

The application log provides detailed information about Cisco Unified MeetingPlace Web Conferencing services. For more information about the Windows Event Viewer, see your Windows documentation.

Procedure

Step 1 Select Start > Control Panel > Administrative Tools > Event Viewer.

Step 2 Select Application from the left pane.

A list of events appear in the right pane.

Step 3 Double-click the event to view it.

How to Configure the Lumberjack Logging Utility

Lumberjack is a logging utility that runs as a background thread. Lumberjack periodically dumps several logs at 24-hour intervals and stores those logs, as well as a specified number of older logs, in a configurable location. All the configuration settings are stored in the registry and worked in to the current registry setting structure of Cisco Unified MeetingPlace. Performance monitor logging configuration settings are stored in definition INI file, so counter list and logging interval can be easily changed.

- Lumberjack Logging Utility, page 13
- Configuring Lumberjack on a Cisco MCS Server, page 13
- Manually Generating a Lumberjack Snapshot, page 14
Lumberjack Logging Utility

Upon startup of the master service, a new thread for Lumberjack begins. Lumberjack reads the configuration values from the registry and INI file to determine behavior. If a performance monitor definition INI file does not exist, Lumberjack automatically creates a file with a predefined counter list and logging interval by using the Lumberjack default values.

Every 24 hours, Lumberjack creates a new Gateway SIM event log for a 24-hour window. If the event log terminates before midnight, Lumberjack restarts it. If the event log runs past midnight of the day that the first call was made, Lumberjack terminates that process. During routing log gathering, Lumberjack also acquires the following information:

- Performance monitor (24-hour window)
- NT Application and System eventlog
- Registry snapshots
- IIS Log

When the master service is running and Lumberjack is enabled, it detects stopped (crashed) services. and collects the following information in a temp folder in the windows temp directory:

- GWSIM eventlog (24 hour window)
- NT Application and System eventlog
- Registry snapshots
- IIS log
- DrWtsn.log and User.dmp
- .exe, .map, and .pdb of downed services
- binaries for authfilt.dll (if downed IIS)

After the information is collected, Lumberjack bundles the files by using pkzipc.exe. This executable file is distributed with MPWEB and located in the DataSvc folder.

The naming convention for the file is lumberjack_timestamp.zip for routine logs and lumberjackCrash_timestamp.zip for crash logs, where timestamp is the time the log gathering started for routine logs and the time of the detected crash for crash logs.

If the master service is simply stopped, the temp directory that is created for routine logs is not deleted so that the logs for one day are bundled together if there is a restart of the master service. This functionality enables the logs that are captured to be reviewed without having to open a zip file and allows for a quicker shutdown and restart of master service because the service does not have to wait to zip files and remove the directory.

Configuring Lumberjack on a Cisco MCS Server

Before You Begin
Read the “Lumberjack Logging Utility” section on page 13.

Procedure

Step 1 Select Start > Run.
The Run window displays.
How to Configure the Lumberjack Logging Utility

Step 2
Enter `regedit`.

Step 3
Change your registry settings for key `HKLM\Software\Latitude\MeetingPlace WebPublisher\General\` and for key `HKLM\Software\Latitude\MeetingPlace Gateway SIM\General\` as shown in the following table:

<table>
<thead>
<tr>
<th>Name (Type)</th>
<th>Description</th>
<th>Data and Default</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server Logging (DWORD)</td>
<td>Enables and disables Lumberjack.</td>
<td>0 - Disabled 1 - Enabled  Default is 1.</td>
</tr>
<tr>
<td>Log Crash History (DWORD)</td>
<td>Specifies the number of old crash logs to store.</td>
<td>Default is 10.</td>
</tr>
<tr>
<td>Log History (DWORD)</td>
<td>Specifies the number of old routine logs to store.</td>
<td>Default is 15.</td>
</tr>
<tr>
<td>Log Location (String)</td>
<td>Specifies where to store the .zip files containing logs.</td>
<td>Default is <code>install-location\Cisco Systems\LogFiles</code>.</td>
</tr>
<tr>
<td>InstallLocation (String)</td>
<td>Used for gathering .dll, .exe, .map, and .pdb files.</td>
<td>Default is set by Cisco MeetingPlace Web Conferencing.</td>
</tr>
</tbody>
</table>

Manually Generating a Lumberjack Snapshot

Logs gathered because of a manual snapshot request have the format `lumberjackSnapshot__timestamp.zip`.

You can locate these logs either in the default LogFiles folder or in the folder that you specified when you completed the “Configuring Lumberjack on a Cisco MCS Server” section on page 13.

Before You Begin
This procedure is completed on the Web Server.

Procedure

Step 1
Right-click the Cisco Unified MeetingPlace red door icon.

Step 2
Select Capture Logs.

The snapshot log gathering process begins.
How to Switch the Order of IP Addresses on the Web Server

Based on the NIC binding order, the system assigns the first IP address to the Hostname [Web Conferencing] and the second IP address to the Hostname [Home Page].

If you ever change an IP address to a hostname or FQDN, be sure that you replace it with the hostname or FQDN corresponding to that IP address. Do not switch the order of the IP addresses or hostnames as this will cause problems.

If you want to switch the order of the IP addresses, complete the following in the order presented. Select the first or second topic based on your system configuration:

- Changing the Binding Order for a System with One IP Address on Each NIC, page 15
- Changing the Binding Order for a System with Two IP Addresses on One NIC, page 15
- Making the Change in the Application, page 16

Changing the Binding Order for a System with One IP Address on Each NIC

Complete this procedure if you have one IP address on each NIC. If you do not, complete the “Changing the Binding Order for a System with Two IP Addresses on One NIC” section on page 15 instead.

Procedure

2. Select Advanced > Advanced Settings.
3. Change the order of the IP addresses/NICs by using the up and down arrows.

What to Do Next
Proceed to the “Making the Change in the Application” section on page 16.

Changing the Binding Order for a System with Two IP Addresses on One NIC

Complete this procedure if you have two IP addresses on a single NIC. If you do not, complete the “Changing the Binding Order for a System with One IP Address on Each NIC” section on page 15 instead.

Procedure

1. Change the primary IP address to the virtual IP address.
2. Change the virtual IP address to the primary IP address.
Making the Change in the Application

**Before You Begin**
Depending on your system, complete one of the following:
- Changing the Binding Order for a System with One IP Address on Each NIC, page 15
- Changing the Binding Order for a System with Two IP Addresses on One NIC, page 15

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Sign in to the end-user web interface.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Select Admin &gt; Web Server.</td>
</tr>
<tr>
<td><strong>Step 3</strong></td>
<td>From the “View” section of the page, select the name of the web server that you want to configure. This populates the “Edit” section of the page with predefined settings.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td>Change the order of the IP addresses for the Hostname [Web Conferencing] and the Hostname [Home Page].</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td>Restart all Cisco Unified MeetingPlace Web Conferencing services.</td>
</tr>
</tbody>
</table>
PART

MeetingPlace Conference Manager

- Installing MeetingPlace Conference Manager
- Using MeetingPlace Conference Manager
Installing MeetingPlace Conference Manager

Release 7.1  
Revised: April 3, 2011 8:30 pm

The MeetingPlace Conference Manager application allows system administrators and Help Desk personnel to manage and monitor in-session Cisco Unified MeetingPlace meetings. It is a Java Swing-based desktop application, which communicates with the Cisco Unified MeetingPlace Application Server through Webservices SOAP API.

- About Java Web Start, page 1
- Downloading and Installing MeetingPlace Conference Manager, page 2
- Uninstalling MeetingPlace Conference Manager, page 3
- Configuring MeetingPlace Conference Manager, page 3
- Changing the Look and Feel of MeetingPlace Conference Manager, page 3

About Java Web Start

Java Web Start is an application-deployment technology developed by Sun Microsystems that gives users the ability to launch full-featured applications with a single click. Java Web Start includes the security features of the Java platform, so the integrity of user data and files is never compromised. In addition, Java Web Start technology enables users to use the latest Java SE technology with any browser.

With Java Web Start, it is possible to launch applications simply by clicking on a Web page link. If the application is not present on the computer of the user, Java Web Start automatically downloads all of the necessary files. It then caches the files on the computer so the application is always ready to be relaunched either from a desktop icon or from the browser link. As a result, users are always presented with the most current version of the application.

For more information about Java Web Start visit its official page at the following: http://java.sun.com/javase/6/docs/technotes/guides/javaws/index.html.
- MeetingPlace Conference Manager Updates, page 1

MeetingPlace Conference Manager Updates

Java Web Start regularly contacts the Cisco Unified MeetingPlace Application Server from which the application is installed in order to check if there is a newer version available. If a newer version is available it is automatically downloaded and started.
Installing MeetingPlace Conference Manager

If the server version could not be checked, the current (cached) version of MeetingPlace Conference Manager is started.

**Note**
Java Web Start may prompt users to provide their Cisco Unified MeetingPlace credentials to access the Application Server.

### Downloading and Installing MeetingPlace Conference Manager

**Before You Begin**

- You must have Java JRE 6.0 or later and Java Web Start installed. See the “About Java Web Start” section on page 1 for information about Java Web Start.
- You must have a Cisco Unified MeetingPlace profile with either System Manager or Attendant privileges.
- Configure the click-to-attend links in the Administration Center. See “Configuring Click-to-Attend Links” in the Configuring E-Mail Notifications for Cisco Unified MeetingPlace module.

**Restriction**
Do not install MeetingPlace Conference Manager on a Cisco Unified MeetingPlace Web Server that is running the Cisco Security Agent (CSA). CSA blocks the MeetingPlace Conference Manager–required connection from the Web Server to the Application Server.

**Procedure**

1. **Step 1** Log in to the Administration Center.
2. **Step 2** Select **Services > Download MeetingPlace Conference Manager**.
   
   **Note** If you do not have Java JRE 6.0 installed, selecting the download link will automatically take you to the Sun download site.

3. **Step 3** Select the link to download MeetingPlace Conference Manager.
4. **Step 4** Choose to save the meetingmanager.jnlp file.
   
   Java Web Start downloads all required files.

5. **Step 5** Double-click the meetingmanager.jnlp icon to start the installation.

6. **Step 6** (Optional) If Java Web Start prompts you for your user credentials, enter your Cisco Unified MeetingPlace username and password to authorize the download from the Application Server.

7. **Step 7** (Optional) If you receive a security warning, select **OK**.

8. **Step 8** Select **Accept** for the license agreement.

Wait for the installation to finish.
Uninstalling MeetingPlace Conference Manager

You can uninstall MeetingPlace Conference Manager by using the Add/Remove Programs feature that comes with your operating system or from the Java Control Panel.

If you have problems uninstalling MeetingPlace Conference Manager, first uninstall Java JRE and then uninstall MeetingPlace Conference Manager by using the Add/Remove Programs feature.

Configuring MeetingPlace Conference Manager

MeetingPlace Conference Manager automatically inherits the Network Settings defined in the Java Control Panel. Java Control Panel, a part of the standard OS Control Panel, is the main configuration utility for all Java Web Start-based applications.

For example, if MeetingPlace Conference Manager needs to use a proxy server in order to access a Cisco Unified MeetingPlace Application Server, make sure that you first define the proxy setting in the Java Control Panel.

For more information, see the Java Control Panel documentation.

Changing the Look and Feel of MeetingPlace Conference Manager

Before You Begin

- This feature was introduced in Release 7.0.2.
- If you have not opened the application, double-click the meetingmanager.jnlp icon on your desktop.

Procedure

Step 1  Select the Properties button.

The Application Properties window displays.

Step 2  Choose one of the available Look and Feel drop-down menu options.

Step 3  Select OK.
Using MeetingPlace Conference Manager

Release 7.1
Revised: April 3, 2011 8:30 pm

- How to Add, Edit, or Remove a Server, page 1
- Logging In to a Server, page 4
- Logging Out from a Server, page 5
- How to Schedule a Meeting, page 5
- How to Search for Meetings, page 9
- How to Update User Information, page 11
- How to Monitor an In-Session Meeting, page 14
- How to Moderate a Question and Answer Session, page 22
- Locating Information About Meetings That Have Ended, page 24
- How to Enable Polling, page 25

How to Add, Edit, or Remove a Server

**Note**
To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

**Caution**
To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

- Adding a New Server, page 2
- Editing an Existing Server, page 2
- Removing an Existing Server, page 3
- Exporting a List of Servers, page 3
- Importing a List of Servers, page 4
Adding a New Server

**Before You Begin**
Double-click the meetingmanager.jnlp icon on your desktop to access the application.

**Procedure**

**Step 1**
Select New Server.
The Server Details window displays.

**Step 2**
Enter the name of the server for Server Name.

**Step 3**
Enter the URL of the server for Server Address.
Example: http://<server>.com or https://<server>.com, where <server> is the name of your Cisco Unified MeetingPlace Application Server.

**Note**
The Server Name and Server Address are mandatory fields.

**Step 4**
(Optional) Enter your Cisco Unified MeetingPlace profile username and password in the fields provided.
If you do not enter a username and password, the system will prompt you for this information each time you attempt to log in to the server.

**Step 5**
Select OK.
This server displays in the Server list.

**Related Topics**
- Importing a List of Servers, page 4

Editing an Existing Server

MeetingPlace Conference Manager allows you to edit your server information. For example, if you enable or disable SSL on the Cisco Unified MeetingPlace Application Server, you will need to edit the server URL in MeetingPlace Conference Manager from http to https.

**Before You Begin**
- If you have not opened the application, double-click the meetingmanager.jnlp icon on your desktop.
- Make sure that you are not logged in to the server that you want to edit. MeetingPlace Conference Manager will not allow you to edit a server that you are currently logged in to.

**Procedure**

**Step 1**
Select a server from the Server Name column.

**Step 2**
Select Edit Server.
The Server Details window displays.

**Step 3**
Edit your fields.
Step 4  Select **OK** to save your edits or **Cancel** to discard your edits.

**Related Topics**
- Configuring SSL for the Cisco Unified MeetingPlace Application Server module

**Removing an Existing Server**

When you remove a server, all information about it is permanently removed.

**Before You Begin**
- If you have not opened the application, double-click the meetingmanager.jnlp icon on your desktop.
- Make sure that you are not logged in to the server that you want to remove. MeetingPlace Conference Manager will not allow you to remove a server that you are currently logged in to.

**Procedure**

**Step 1**  Select a server from the Server Name column.
**Step 2**  Select **Remove Server**.  
A confirmation window displays.
**Step 3**  Select **Yes** to confirm the action or **No** to cancel the action.

**Exporting a List of Servers**

**Before You Begin**
- This feature was introduced in Release 7.0.2.
- If you have not opened MeetingPlace Conference Manager, double-click the meetingmanager.jnlp icon on your desktop.

**Procedure**

**Step 1**  Select the **Properties** button.  
The Application Properties window displays.
**Step 2**  Select **Export**.
**Step 3**  Specify the filename and location for saving the file.
**Step 4**  Select **Export**.

**Related Topics**
- Importing a List of Servers, page 4
Importing a List of Servers

Before You Begin
- This feature was introduced in Release 7.0.2.
- Locate the previously exported list of servers, which must be in XML format.
- If you have not opened MeetingPlace Conference Manager, double-click the meetingmanager.jnlp icon on your desktop.

Procedure

Step 1
Select the **Properties** button.
The Application Properties window displays.

Step 2
Select **Import**.

Step 3
Select the XML file.

Step 4
Select **Import**.

Step 5
Verify that the imported servers appear on the application home page.

Related Topics
- Exporting a List of Servers, page 3
- Adding a New Server, page 2

Logging In to a Server

**Note**
To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

**Caution**
To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

Before You Begin
- If you have not opened the application, double-click the meetingmanager.jnlp icon on your desktop.
- Make sure that your version of MeetingPlace Conference Manager is the same or greater than the server that you are trying to access.

Procedure

Step 1
Select the name of a server from the Server Name column.

Step 2
Select **Login**.
Step 3  (Optional) If you did not enter your username and password when you added the server, the Login to Server window displays. Enter your username and password information then select Login.

Once you are logged in, the Search screen for the chosen server displays.

Troubleshooting Tips
- If you cannot log in to a server due to a username or password that was incorrectly saved, edit the server information. See the “Editing an Existing Server” section on page 2 for instructions.
- You can log in to multiple servers then choose which server you want to monitor by choosing the server from the Server drop-down list on the main page.
- If you unsuccessfully try to log in to the same server three times, you will have to contact the system administrator of the Application Server to unlock your profile.

Logging Out from a Server

Note
To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

Caution
When you log out from a server, all of the in-session meetings on that server are closed.

Caution
To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

Procedure

Step 1  Select the name of a server from the Server Name column.

Note  If you are logged in to the server, the indicator next to the server name is green.

Step 2  Select Logout.

A confirmation window displays.

Step 3  Select Yes to confirm the logout, or Cancel to cancel the action.

How to Schedule a Meeting

- Scheduling a Meeting, page 6
- Scheduling Another Meeting With the Same Parameters, page 7
Scheduling a Meeting

You can schedule a meeting on behalf of other users if you have Attendant or System Manager privileges.

Before You Begin

- Cisco Unified MeetingPlace supports the scheduling of meetings from Conference Manager with over 200 invitees.
- Scheduling and rescheduling of recurring meetings with more than 10 instances should be performed during off-peak times to minimize delays perceived by users joining meetings.
- Scheduling of several large meeting chains concurrently is not recommended because it may cause system delay.

Caution

To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

Procedure

Step 1
Log in to a server.

Step 2
Select Schedule Meeting.

Step 3
Enter your meeting details, such as the meeting ID if you want to define your own, date, time, and duration of the meeting.
- Check Public if you want this meeting to appear in the list of results when users use the Find Meeting feature.
- Check Enable video if you want to reserve video resources for this meeting.

Step 4
(Optional) Select the button next to Recurrence to make this a recurring meeting and set your recurrence pattern.

Step 5
Add invitees from the bottom of the Add Invitee tab.
  a. Enter the user ID of the invitee.
  b. Enter the e-mail address of the invitee.
  c. Choose an audio permission for this invitee.
  d. Select Profile or Guest to indicate whether this invitee has a Cisco Unified MeetingPlace profile.
  e. Select Invite.

Note
If you do not know the user ID of the person you want to invite, use the search function on the top of the Add Invitee tab then use “drag and drop” to drag selected users to the Invitee list.

Step 6
Set the Advanced Options for this meeting.
Step 7  Select **Schedule**.

---

**Related Topics**
- Field Reference: Meeting Scheduling Page in the MeetingPlace Conference Manager References module

**Scheduling Another Meeting With the Same Parameters**

**Procedure**

**Step 1** Log in to a server.

**Step 2** Use the Search for Meetings option to find the meeting that you want to use.
- If the meeting is taking place today, either select **In-Session Meetings** or **All Today’s Meetings**.
- If the meeting is taking place at another time, enter your search parameters and select **Search**.

**Step 3** Select your meeting entry in the Meetings tab to the right.

**Step 4** Select **Edit Meeting**.

The Meetings window appears.

**Step 5** Select **Copy Meeting**.

In the same Meetings window, a new meeting tab appears that includes the settings copied from the selected meeting. The Meeting ID, however, is not copied to the new meeting.

**Step 6** Modify your meeting options.

**Step 7** Select **Schedule**.

---

**Rescheduling a Meeting**

**Restriction**
- You cannot change recurrence parameters when rescheduling a meeting.
- You cannot reschedule a meeting that has already begun.
- Scheduling and rescheduling of recurring meetings with more than 10 instances should be performed during off-peak times to minimize delays perceived by users joining meetings.

**Note**
We do not recommend that you reschedule meeting chains of over 30 occurrences with 500 invitees as it may cause long rescheduling times and system unresponsiveness.
**Procedure**

**Step 1**  Log in to a server.

**Step 2**  Use the Search for Meetings option to find the meeting that you want to reschedule.
   
   a. If the meeting is taking place today, either select **In-Session Meetings** or **All Today’s Meetings**.
   
   b. If the meeting is taking place at another time, enter your search parameters and select **Search**.

**Step 3**  Select your meeting entry in the Meetings tab to the right.

**Step 4**  Select **Edit Meeting**.

The Meetings page displays.

**Step 5**  Modify your meeting options.

**Step 6**  Select **Reschedule**.

Cisco Unified MeetingPlace cancels the original meeting and sends you a meeting cancellation notice followed by a rescheduled meeting notice that describes the modified schedule.

---

**Canceling a Meeting**

**Note**  To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

**Caution**  To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

**Restriction**

- You cannot cancel a meeting that has already begun.

**Procedure**

**Step 1**  Log in to a server.

**Step 2**  Use the Search for Meetings option to find the meeting that you want to cancel.
   
   a. If the meeting is taking place today, either select **In-Session Meetings** or **All Today’s Meetings**.
   
   b. If the meeting is taking place at another time, enter your search parameters and select **Search**.

The Meetings page displays.

**Step 3**  Select your meeting entry in the Meetings tab to the right.

**Step 4**  Select **Edit Meeting**.

The Meetings page displays.

**Step 5**  Select **Cancel**.

**Step 6**  Select **Yes** in the Cancel meeting confirmation window.
Step 7  Select **OK** in the Success window.
Step 8  Select **Close** to close the Meetings window.

---

**How to Search for Meetings**

**Note**
To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

**Caution**
To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

- Modifying the Panes on the Search Page, page 9
- Finding All In-Session and Currently Scheduled Meetings, page 9
- Finding a Meeting by Using an Advanced Search Query, page 10
- Filtering the Search Results List, page 10

---

**Modifying the Panes on the Search Page**

When you first log in to a server, you will see the Search For Meeting page. This page is divided into two configurable panes. Complete this procedure to modify the panes.

**Procedure**

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resize the two search panes.</td>
<td>Use your mouse to move the divider between the two panes.</td>
</tr>
<tr>
<td>Hide a search pane.</td>
<td>Select the arrow at the top of the divider to either hide or show a given pane.</td>
</tr>
</tbody>
</table>

---

**Finding All In-Session and Currently Scheduled Meetings**

MeetingPlace Conference Manager comes with two predefined search queries: to search for all in-session meetings, and to search for all of today’s meetings. When you submit a query, your search results appear in the right pane.
Finding a Meeting by Using an Advanced Search Query

An advanced search query allows you to search for meetings by using one or several variables: Meeting ID number, Scheduler ID number, meeting subject, date interval or meeting state. The search is not case-sensitive.

Before You Begin
• Make sure that you are on the Search For Meeting page of the server that you want to search.
• If you are logged in to multiple servers, you can navigate between them by choosing the server from the Server drop-down list on the main page.

Procedure

Step 1 Enter information for at least one search parameter on the Search For Meeting page.
• Scheduler ID, Subject, and Meeting ID are not case-sensitive.
• Select the calendar icon to choose your From and To dates.
• A meeting day is defined as beginning at 12:00 AM and ending at 11:59 PM.
• Make sure that you check at least one meeting state: Not Started, Ended, Waiting, or In Session.

Step 2 Select Search.
Search results appear in the right pane.

Filtering the Search Results List

After you have completed a search, you can filter the results to obtain a smaller list of search results. Filtering occurs dynamically as you choose your filter attributes.

Before You Begin
Search for a meeting. See either the “Finding All In-Session and Currently Scheduled Meetings” section on page 9 or the “Finding a Meeting by Using an Advanced Search Query” section on page 10 for instructions.

Procedure

Step 1 Look at the right pane of the Search For Meeting page.
Step 2 Choose an attribute from the Filter drop-down box.
Step 3 Enter a value in the “contains” field.
- If you choose “In a Date Range” as your filter, indicate a From and To date range.

Step 4 Check one or more meeting states: Not Started, Ended, Waiting, or In Session.

Troubleshooting Tips
- To sort the list of search results, select the heading of the column by which you want to sort your results.
- To return to an unfiltered list, clear the text fields.

How to Update User Information

Note To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

Caution To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

- Adding a User Profile, page 11
- Searching for a User Profile, page 12
- Modifying the Status of a User Profile, page 12
- Changing the Login Information for a User, page 13
- Updating a User Profile, page 13
- Deleting a User Profile, page 14

Adding a User Profile

Restriction
- This feature was introduced in Release 7.0.2.
- If you are logged in as an attendant, you may not have the correct privileges to add user profiles. These privileges are configured by the system administrator through the Administration Center. See “Configuring Attendant Privileges” in the Configuring Attendant Settings for Cisco Unified MeetingPlace module.

Procedure

Step 1 Log in to a server.
Step 2 Select the Users tab.
Step 3 Select Add User.
Step 4 Enter the user information.
Searching for a User Profile

Complete this procedure to find a user profile in MeetingPlace Conference Manager.

Procedure

Step 1 Log in to a server.
Step 2 Scroll down to the Search For Users section.
Step 3 Search for the user.
   - Select one of the shortcuts for locked or inactive users if they apply.
   - If neither of the shortcuts apply, enter a search parameter and select Search.
Step 4 Select the Users tab to see your search results.
Step 5 (Optional) Filter your search results by username or profile number.

Related Topics
- Modifying the Status of a User Profile, page 12
- Changing the Login Information for a User, page 13
- Updating a User Profile, page 13
- Deleting a User Profile, page 14

Modifying the Status of a User Profile

Complete this procedure to set a user profile as active, inactive, or locked. You can modify the status of one profile or a group of profiles.

Before You Begin
- Any user profiles you want to modify must be on the local server.
- If you are logged in as an attendant, make sure that you have permission to modify user profiles. This is set on the Cisco Unified MeetingPlace Application Server: Admin > System configuration > Usage configuration > Attendant privileges.
- The user status of the admin profile and the recorder profile cannot be set to Locked.

Related Topics
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Searching for a User Profile, page 12
Using MeetingPlace Conference Manager

How to Update User Information

Procedure

Step 1 Log in to a server.
Step 2 Search for the user whose status you want to modify.
Step 3 Select the user entry.
   To choose more than one user entry, press the Ctrl key while selecting more user entries.
Step 4 Select Set status as... and choose the status you want to apply.

Related Topics
   • Searching for a User Profile, page 12

Changing the Login Information for a User

Complete this procedure to change the user password, profile password, or e-mail address of a user. You can also use this procedure to change the user status.

Before You Begin
   • Any user profiles you want to modify must be on the local server.
   • The user status of the admin profile and the recorder profile cannot be set to Locked.

Procedure

Step 1 Log in to a server.
Step 2 Search for the user whose login information you want to modify.
Step 3 Select the user entry.
   To choose more than one user entry, press the Ctrl key while selecting more user entries.
Step 4 Select Change Login Info.
Step 5 Enter your changes.
Step 6 Select Save.

Related Topics
   • Searching for a User Profile, page 12

Updating a User Profile

Before You Begin
This user information must be on the local server.
Procedure

Step 1 Log in to a server.
Step 2 Search for the user whose information you want to update.
Step 3 Select the user entry.
Step 4 Select Edit User to open the Edit user profile window.
Step 5 Enter your changes.
Step 6 Select Save.

Related Topics
- Searching for a User Profile, page 12

Deleting a User Profile

Before You Begin
- This feature was introduced in Release 7.0.2.
- This user information must be on the local server.

Procedure

Step 1 Log in to a server.
Step 2 Search for the user whose profile you want to delete.
Step 3 Select the user entry.
Step 4 Select Delete User.
Step 5 Select Yes.

Related Topics
- Searching for a User Profile, page 12

How to Monitor an In-Session Meeting

Note
To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

Caution
To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.
The Meetings window allows you to monitor meetings in real time, as well as perform various actions related to that meeting. You can monitor several meetings at once. Each meeting is revealed in tab view.

- Finding a Summary of an In-Session Meeting, page 15
- Going to the Meeting Page on the Cisco Unified MeetingPlace Web Server, page 15
- Adding a Profiled User to an In-Session Meeting, page 16
- Adding a Guest User to an In-Session Meeting, page 17
- Controlling a Meeting In-Session, page 17
- Muting Participants During a Meeting, page 18
- Changing the Status of a Participant During a Meeting, page 19
- Moving Participants During a Meeting, page 20
- Finding a Participant in the Participant List, page 21
- Viewing an Event Log for a Meeting, page 22

### Finding a Summary of an In-Session Meeting

Each meeting details page includes meeting summary information including the name of the scheduler, the start time, whether a password is required and so on. Complete this procedure to locate the summary information for a meeting.

**Procedure**

**Step 1** From the Search For Meeting page, select the meeting that you want to view.

**Step 2** Select **Monitor Meeting**.

A Meetings window displays with the selected meeting in tab view.

**Step 3** Look at the right pane of the Meetings window.

**Step 4** If it is not already displayed, select the **Meeting Summary** tab.

**Troubleshooting Tips**

If you are logged in to multiple servers, you can navigate between them by choosing the server from the Server drop-down list on the main page.

### Going to the Meeting Page on the Cisco Unified MeetingPlace Web Server

**Before You Begin**

Make sure that you first set the correct URL for the Web Server on the Application Server. See **Configuring Click-to-Attend Links** in the **Configuring E-Mail Notifications for Cisco Unified MeetingPlace** module.
Adding an Invited User to an In-Session Meeting

Complete this procedure to dial out to users who are already in the web meeting so that they can participate in the audio or video meeting.

Procedure

Step 1 From the Search For Meeting page, select the meeting that you want to view.
Step 2 Select Go to Meeting Page.

Step 3 Select one invitee from the invitees table in the left pane.
Step 4 Right-click the selected invitee to open the context menu.
Step 5 Select Outdial invitee.
Step 6 (Optional) Enter the phone number of the invitee.
Step 7 Select Outdial.

Adding a Profiled User to an In-Session Meeting

The Add Participant tab allows you to quickly add profiled users to a meeting that is currently in-session by calling out to their phones. You can either search for profiled users or enter a phone number if the user does not have a phone number stored as part of their profile.

Procedure

Step 1 From the Search For Meeting page, select the meeting that you want to view.
Step 2 Select Monitor Meeting.
Step 3 Look at the right pane of the Meetings window.
Step 4 If it is not already displayed, select the Add Participant tab.
Step 5 Enter one or more search parameters.
Step 6 Select Search.
Search results are displayed in a list.
Using MeetingPlace Conference Manager

Step 7 Add the user to the meeting by doing one of the following:

- Drag and drop the user in to the Main Room in the left pane or
- Enter a phone number for the user and select Outdial.

The system calls the user so that the user can join the meeting.

Adding a Guest User to an In-Session Meeting

The Add Participant tab allows you to quickly add guest users to a meeting that is currently in-session by calling out to their phones.

Procedure

Step 1 From the Search For Meeting page, select the meeting that you want to view.

Step 2 Select Monitor Meeting.

A Meetings window displays with the selected meeting in tab view.

Step 3 Look at the right pane of the Meetings window.

Step 4 If it is not already displayed, select the Add Participant tab.

Step 5 Select Guest in the lower-right part of the screen.

Step 6 Enter the name of the guest user for User ID.

Step 7 Enter the phone number of the guest user.

Step 8 Select Outdial.

Controlling a Meeting In-Session

While a meeting is in-session, you can control meeting behavior such as locking or unlocking the meeting, starting or stopping recording. You can also end the meeting.

Before you Begin

- This procedure assumes that you are viewing the meeting details page for the meeting that you are monitoring. See the “Finding a Summary of an In-Session Meeting” section on page 15 for instructions.
- All of the buttons mentioned in this procedure are located on the bottom of the Meetings window.

Procedure

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start recording the meeting.</td>
<td>Select Start Recording.</td>
</tr>
<tr>
<td>Stop recording the meeting.</td>
<td>Select Stop Recording. This button only displays if you are currently recording the meeting.</td>
</tr>
</tbody>
</table>
How to Monitor an In-Session Meeting

Using MeetingPlace Conference Manager

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lock the meeting.</td>
<td>Select <strong>Lock Meeting</strong>. This prevents new participants from joining the meeting.</td>
</tr>
<tr>
<td>Unlock the meeting.</td>
<td>Select <strong>Unlock Meeting</strong>. This button only displays if the meeting is currently locked.</td>
</tr>
<tr>
<td>Enable participants to ask questions during lecture-style meetings.</td>
<td>Select <strong>Enable Q&amp;A</strong>.</td>
</tr>
<tr>
<td>Give all users in a lecture-style meeting the permission to speak and ask questions in the meeting.</td>
<td>Select <strong>Open Floor</strong>.</td>
</tr>
<tr>
<td>Remove all users from the speaking area during a lecture-style meeting.</td>
<td>Select <strong>Close Floor</strong>.</td>
</tr>
<tr>
<td>Stop the question and answer session.</td>
<td>Select <strong>Disable Q&amp;A</strong>. This button only displays if a question and answer session is currently in progress.</td>
</tr>
<tr>
<td>End the meeting.</td>
<td>Select <strong>End Meeting</strong>. This closes all components of the meeting: audio, video, and web.</td>
</tr>
</tbody>
</table>

**Troubleshooting Tips**

If you are logged in to multiple servers, you can navigate between them by choosing the server from the Server drop-down list on the main page.

**Mutting Participants During a Meeting**

You can choose to mute one or a number of participants during a meeting so that sound cannot be heard from their phone or video endpoints.

**Before You Begin**

- This procedure assumes that you are viewing the meeting details page for the meeting that you are monitoring.
- Keep the following tips in mind:
  - Sort the list of participants by selecting the Participant column.
  - To choose multiple participants, press the Ctrl key as you select on the names. To choose a contiguous group of participants, select the first name, press the Shift key, then select the last name to automatically choose all of the participants in between.
  - You can also modify participant abilities by right-clicking on the participant name.
  - Users can mute themselves by pressing #5 on their phones.
Procedure

Step 1  Select the name of the participant that you want to affect.

Step 2  Do one of the following:

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mute a participant.</td>
<td>Select <strong>Mute</strong>.</td>
</tr>
<tr>
<td>Unmute a participant.</td>
<td>Select <strong>More &gt; Unmute</strong>.</td>
</tr>
<tr>
<td>Mute most participants.</td>
<td>Select <strong>More &gt; Mute All Except Selected</strong>.</td>
</tr>
</tbody>
</table>

Changing the Status of a Participant During a Meeting

Complete this procedure to rename participants during a meeting, change their speaking status, or remove them from the meeting.

Before You Begin

- This procedure assumes that you are viewing the meeting details page for the meeting that you are monitoring.
- Keep the following tips in mind:
  - Sort the list of participants by selecting the Participant column.
  - You can also modify participant abilities by right-clicking on the participant name.

Procedure

Step 1  Select the name of the participant that you want to affect.

Step 2  Complete one of the following:
Using MeetingPlace Conference Manager

How to Monitor an In-Session Meeting

### Moving Participants During a Meeting

Complete this procedure to move participants from the waiting room to the main room or to a breakout room and back during a meeting. You can see which participants are in which room by selecting the room number in the Meetings window.

The room number displays as M for Main room, W for Waiting room, and 1-9 for each breakout room.

### Tip

Sort the list of participants by selecting the Participant column. You can also move selected participants among rooms by dragging and dropping them to their destination rooms. A destination room must be visible in the Meetings window before you can use the drag and drop feature.

### Before You Begin

- This procedure assumes that you are viewing the meeting details page for the meeting that you are monitoring.
- Keep the following tips in mind:
  - Sort the list of participants by selecting the Participant column.

---

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rename a participant.</td>
<td>Enter a new name in the Rename field then select <strong>Rename</strong>.</td>
</tr>
<tr>
<td>Remove a participant from the meeting.</td>
<td>Select <strong>More &gt; Eject</strong>.</td>
</tr>
<tr>
<td></td>
<td>Confirm the action when prompted by selecting <strong>Yes</strong>.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Due to a product limitation, participants who leave a Cisco WebEx web meeting still appear in the participant list.</td>
</tr>
<tr>
<td>Change the speaking status of the participant.</td>
<td>Select <strong>More &gt; Change ability</strong> then choose the new speaking status that you want to assign.</td>
</tr>
<tr>
<td></td>
<td>• Speaker plus—A user with permanent speaking privileges. During lecture-style meetings this user does not have to be on “the floor” in order to speak. Moderators are usually assigned as Speaker plus.</td>
</tr>
<tr>
<td></td>
<td>• Muted speaker plus—A user with permanent speaking privileges who has been muted.</td>
</tr>
<tr>
<td></td>
<td>• Speaker—A user with standard speaking privileges. During lecture-style meetings this user can only speak when on “the floor”.</td>
</tr>
<tr>
<td></td>
<td>• Muted speaker—A speaker who is muted.</td>
</tr>
<tr>
<td></td>
<td>• Listener—A user with no speaking privileges. During lecture-style meetings this user is granted speaking abilities when on “the floor”</td>
</tr>
</tbody>
</table>

---

**Related Topics**

- [Moderating a Question and Answer Session, page 23](#)
Using MeetingPlace Conference Manager

How to Monitor an In-Session Meeting

- To choose multiple participants, press the Ctrl key as you click on the names. To choose a contiguous group of participants, select the first name, press the Shift key, then select the last name to automatically choose all of the participants in between.
- You can also modify participant abilities by right-clicking on the participant name.
- Users can move themselves to a breakout room by pressing #1 on their phones followed by the number of their breakout room.

Procedure

**Step 1** Select the name of the participant that you want to affect.

**Step 2** Complete one of the following:

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move a participant to a breakout session.</td>
<td>Select More &gt; Move to room then choose the breakout room.</td>
</tr>
<tr>
<td>Return a participant to the main meeting.</td>
<td>Select More &gt; Move to room &gt; Main Room.</td>
</tr>
<tr>
<td>Move all participants of Listener ability from the main room to the waiting room.</td>
<td>Select More &gt; Move to WR.</td>
</tr>
<tr>
<td>Move all participants of Listener ability from the waiting room to the main meeting.</td>
<td>Select More &gt; Move from WR.</td>
</tr>
</tbody>
</table>

Finding a Participant in the Participant List

**Before you Begin**
This procedure assumes that you are viewing the meeting details page for the meeting that you are monitoring.

**Note** Participants who leave a Cisco WebEx meeting still appear in the Participant list.

Procedure

<table>
<thead>
<tr>
<th>If</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>You know the name of the participant you are looking for.</td>
<td>Enter part of the name in the “Name begins with” field.</td>
</tr>
<tr>
<td>You do not know the name of the participant you are looking for.</td>
<td>Sort the Participant column by selecting the column heading then scroll through the list.</td>
</tr>
</tbody>
</table>
Using MeetingPlace Conference Manager

Viewing an Event Log for a Meeting

You can view a log of events that are taking place during a meeting. Examples of meeting events are when a user joins, leaves, or is renamed, when a meeting recording is started or stopped, and when the floor is opened or closed.

As an attendant, you can save the events log locally to your file system.

**Before You Begin**

This procedure assumes that you are viewing the meeting details page for the meeting that you are monitoring.

**Procedure**

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>View the event log.</td>
<td>Select the Event Log tab.</td>
</tr>
<tr>
<td>Erase the list of logged events.</td>
<td>Select Clear Log.</td>
</tr>
</tbody>
</table>

**How to Moderate a Question and Answer Session**

**Note**

To use the MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

**Caution**

To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

- Adding a Participant to the Question and Answer Queue, page 22
- Moderating a Question and Answer Session, page 23

**Adding a Participant to the Question and Answer Queue**

**Tip**

You can also use “drag and drop” to move participants from the main Participant list to the Q&A queue. To allow all participants to ask questions, select Open Floor.

**Before You Begin**

This procedure assumes that you are viewing the meeting details page for the meeting that you are monitoring.
Using MeetingPlace Conference Manager

How to Moderate a Question and Answer Session

Procedure

Step 1  Select the name of the participant that you want to add to the queue.
Step 2  Select More > Add to Q&A Queue.
        The name of the participant displays in the queue.

Moderating a Question and Answer Session

When a Question and Answer session is in progress, you can use the navigation buttons in the Q&A panel to move users within the Q&A queue, to “the floor” where they can ask questions, and back to the main meeting. Users who do not have Speaker Plus privileges lose speaking permissions when they are returned to the main meeting.

Note

Users can move themselves to the Q&A queue by pressing #71 on their phones.

Before You Begin

Add users to the Q&A queue when they indicate that they have a question. See the “Adding a Participant to the Question and Answer Queue” section on page 22.

Procedure

Step 1  Select the name of a user from the Q&A queue.
Step 2  Complete one of the following:
        Tip  You can also use “drag and drop” to move users between the different meeting areas.
Locating Information About Meetings That Have Ended

**Note**
To use the Cisco Unified MeetingPlace Conference Manager, you must have either System Manager or Attendant privileges.

**Caution**
To avoid system issues, we recommend that you limit the usage of concurrent Conference Manager sessions.

Once a meeting has ended, you can still access basic information about it including attendance information and attendance history. Attendance information contains basic user attendance data, whether a user was invited, if the user attended the meeting and in which way. Attendance history contains more detailed data about each participant including join leave times, duration and type.

**Procedure**

**Step 1**
Search for your meeting.
See either the “Finding All In-Session and Currently Scheduled Meetings” section on page 9 or the “Finding a Meeting by Using an Advanced Search Query” section on page 10.

**Step 2**
Double-click the meeting that you want information for.

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Move a user up in the queue.</td>
<td>Select the Move participant up button.</td>
</tr>
<tr>
<td>Move a user down in the queue.</td>
<td>Select the Move participant down button.</td>
</tr>
<tr>
<td>Move a user to the top of the queue.</td>
<td>Select the Move participant to the top button.</td>
</tr>
<tr>
<td>Move a user to the bottom of the queue.</td>
<td>Select the Move participant to the bottom button.</td>
</tr>
<tr>
<td>Move a user from the queue to the “floor” where the user can ask a question.</td>
<td>Select the Give floor to participant button.</td>
</tr>
<tr>
<td>Remove a user from the queue.</td>
<td>Select the Remove participant from Q&amp;A Queue button.</td>
</tr>
<tr>
<td>Move a user from the floor back to the main meeting area.</td>
<td>Select the Remove participant from floor button.</td>
</tr>
<tr>
<td>Rename a breakout room. The new name is displayed next to the breakout room number title in all conference managers monitoring the meeting.</td>
<td>Select Rename room.</td>
</tr>
<tr>
<td>Give all users in the meeting permission to speak and ask questions in the meeting.</td>
<td>Select Open Floor.</td>
</tr>
<tr>
<td>Remove all users from the speaking area.</td>
<td>Select Close Floor.</td>
</tr>
</tbody>
</table>
The Meetings window displays with basic meeting details.

**Step 3** (Optional) To save the attendance history information, do the following:

- a. Select the **Attendance history** tab.
- b. Select **Save**.

---

## How to Enable Polling

Use the polling feature to enhance your Cisco Unified MeetingPlace Conference Manager meeting list so that it indicates which in-session meetings have attendees and guest attendees in them.

Meetings with attendees in them are displayed in bold text. Meetings with guest attendees in them are displayed with an asterisk before the meeting ID. Guest attendees are users that are not logged into the system. Double click a meeting in the list to open its monitoring page.

### Procedure

**Step 1** Click the Properties button in the upper left-hand corner of the Cisco Unified MeetingPlace Conference Manager page. The Application Properties dialog box opens.

**Step 2** Select the **Enable polling for active meetings** checkbox.

**Step 3** Click **OK**.
How to Enable Polling
Part

Integrations

- Integrating Cisco Unified MeetingPlace with Cisco WebEx
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook
- Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface
- Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager
- Integrating Cisco Unified MeetingPlace with Cisco Unified Personal Communicator
- Integrating Cisco Unified MeetingPlace With Cisco Unified IP Phone
Integrating Cisco Unified MeetingPlace with Cisco WebEx

You can integrate Cisco Unified MeetingPlace with Cisco WebEx in one of two ways, using either Cisco WebEx meeting scheduling or Cisco Unified MeetingPlace meeting scheduling.

- **Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace**, page 1
- **Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx**, page 3
- **Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx**, page 7
- **How to Integrate Cisco Unified MeetingPlace with Cisco WebEx**, page 12

### Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace

- **About Cisco WebEx Integration Option 1**, page 1
- **Prerequisites for Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace**, page 2
- **End-User Information for Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace**, page 2

### About Cisco WebEx Integration Option 1

This Cisco WebEx integration option provides:

- Cisco WebEx network-based web conferencing
- Cisco Unified MeetingPlace scheduled and reservationless audio conferencing, web conferencing, scheduling, notifications, and Microsoft Outlook integration.

**Related Topics**

- **Prerequisites for Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace**, page 2
Prerequisites for Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace

- Obtain a Cisco WebEx account and site, such as cisco.webex.com.
- If you did not configure Network Time Protocol (NTP) on the Application Server during installation, then use the `net` command to do so.
- Install the Cisco Unified MeetingPlace Web Server.
- Configure Cisco Unified MeetingPlace Web Conferencing.
- Configure Directory Service.
- If you want end users to be able to download and use the Cisco WebEx plug-in for Microsoft Outlook, then you must enable SSL on the Cisco Unified MeetingPlace Application Server.

Related Topics
- Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module
- Configuring Cisco Unified MeetingPlace Directory Service module
- Configuring SSL for the Cisco Unified MeetingPlace Application Server module
- Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 1
- How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12

End-User Information for Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace

Provide the following information to your end users:

- The URL of the Cisco Unified MeetingPlace end-user web interface (http://web-server/), from which users sign in and perform the following actions:
  - Schedule meetings
  - Attend meetings
  - Access recordings of past meetings that were scheduled to use Cisco Unified MeetingPlace web conferencing.
- Information about accessing recordings of meetings that were scheduled to use Cisco WebEx web conferencing.
After each recorded Cisco WebEx meeting, the meeting owner (host) receives an e-mail from Cisco WebEx that includes a link to the meeting recording. The host can then forward the e-mail so that others can play back the recording.

The host can also access recordings by signing in to the Cisco Unified MeetingPlace end-user web interface and then clicking My WebEx > My Files > My Recordings.

---

**Note**

---

Whether Cisco WebEx or Cisco Unified MeetingPlace executes and stores a meeting recording depends on which web conferencing provider is selected (even if by default) when the meeting is scheduled. This is true even in meetings for which the web component is never used. Therefore, make sure that your end users know where to find their meeting recordings. This can be confusing for users who can choose between Cisco WebEx and Cisco Unified MeetingPlace web conferencing while scheduling meetings.

---

- **Profile number** and **Profile password** for signing in over the phone.
- **User ID** and **User password** for signing in over the web.

---

**Note**

---

All users must sign in through the Cisco Unified MeetingPlace end-user web interface. Signing in directly through the Cisco WebEx end-user web interface is not supported in this Cisco WebEx integration deployment.

---

- Guidelines for users who can choose between Cisco WebEx and Cisco Unified MeetingPlace web conferencing while scheduling meetings.

  For example, you may want your users to choose Cisco Unified MeetingPlace web conferencing for internal meetings and choose Cisco WebEx web conferencing for external meetings.

  - Quick Start Guide: Attending and Scheduling a Cisco Unified MeetingPlace Meeting From Your Phone
  - User Guide for Cisco Unified MeetingPlace

---

**Note**

---

We recommend that you also notify your users of the applicable restrictions in the “Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx” section on page 7.

---

**Related Topics**

- Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 1
- How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12

---

**Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx**

- About Cisco WebEx Integration Option 2, page 4
About Cisco WebEx Integration Option 2

This Cisco WebEx integration option provides:

- Cisco WebEx network-based web conferencing, scheduling, notifications, Microsoft Outlook integration, and IBM Lotus Notes integration.
- Cisco Unified MeetingPlace reservationless audio conferencing.

Prerequisites for Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx

- Obtain a Cisco WebEx account and site, such as cisco.webex.com.
- To use the call out feature from the Cisco WebEx meeting room, you must set the “Guest Outdial” parameter to Yes for the Cisco Unified MeetingPlace guest user profile.
- If you did not configure Network Time Protocol (NTP) on the Application Server during installation, then use the net command to do so.
- If you plan to use Directory Service, then configure Directory Service before integrating Cisco Unified MeetingPlace with Cisco WebEx.
- If you want end users to be able to download and use the Cisco WebEx plug-in for Microsoft Outlook, then you must enable SSL on the Cisco Unified MeetingPlace Application Server.

Related Topics
- Configuring Cisco Unified MeetingPlace Directory Service module
- Configuring SSL for the Cisco Unified MeetingPlace Application Server module
- Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx, page 3
- How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12
End-User Information for Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx

Provide the following information to your end users:

- The URL of the user sign-in site:
  - If you have not configured Directory Service on your Cisco Unified MeetingPlace system, then provide the URL of the Cisco WebEx end-user web interface \( http://site.webex.com/ \).
  - If you have configured Directory Service on your Cisco Unified MeetingPlace system, then provide the URL of the Cisco Unified MeetingPlace Application Server, for example, \( http://application-server/ \).

\[ \text{Note} \quad \text{It takes longer to sign in for the first time through the Cisco Unified MeetingPlace Application Server sign-in page.} \]

- Username and password information:
  
  If you have not configured Directory Service (SSO) on your Cisco Unified MeetingPlace system:
  - Provide each user with their User ID, Profile number, and Profile password. Each user will automatically receive e-mail instructions to set their User password on the Cisco WebEx site.

\[ \text{Note} \quad \text{The User ID and User password are used to sign in over the web. The Profile number and Profile password are used to sign in over the phone.} \]

  - Your system administrator may distribute the Cisco WebEx Productivity Tools via a software distribution method for automatic installation or you may be instructed to download the Cisco WebEx Productivity Tools from your Cisco WebEx site URL.

  - If you manually download and configure the Cisco WebEx Productivity Tools for Microsoft Outlook, IBM Lotus Notes, One Click, or other client applications, follow the steps provided in the “Configuring Cisco WebEx Productivity Tools for the First Time without Directory Service” section on page 6 for initial configuration without Directory Service (SSO).

If Directory Service (SSO) is configured on your Cisco Unified MeetingPlace system:

  - Provide each user with their User ID (which should match their LDAP user ID), User password (which should match their LDAP password), Profile number, and Profile password.

\[ \text{Note} \quad \text{The User ID and User password are used to sign in over the web. The Profile number and Profile password are used to sign in over the phone.} \]

  - All Cisco WebEx host accounts are automatically propagated from Cisco Unified MeetingPlace the first time a user signs in with SSO enabled.

  - Your system administrator may distribute the Cisco WebEx Productivity Tools via a software distribution method for automatic installation or you may be instructed to download the Cisco WebEx Productivity Tools from your Cisco WebEx site URL.
- If using the Cisco WebEx Productivity Tools for Microsoft Outlook, IBM Lotus Notes, One Click, or other client applications, follow the steps provided in the “Configuring Cisco WebEx Productivity Tools for the First Time with Directory Service” section on page 7 for initial configuration.

- Information about accessing meeting recordings.
  After each recorded Cisco WebEx meeting, the meeting owner (host) receives an e-mail from Cisco WebEx that includes a link to the meeting recording. The host can then forward the e-mail so that others can play back the recording.
  The host can also access recordings from the Cisco WebEx end-user web interface by clicking My WebEx > My Files > My Recordings.


**Note** We recommend that you also notify your users of the applicable restrictions in the “Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx” section on page 7.

**Related Topics**
- Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx, page 3
- How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12

### Configuring Cisco WebEx Productivity Tools for the First Time without Directory Service

Complete this procedure to initially configure your Cisco WebEx Productivity Tools for Microsoft Outlook, IBM Lotus Notes, One Click, or other client applications if the following applies:

- You manually download and configure the Cisco WebEx Productivity Tools
- You are completing your initial configuration without Directory Service (SSO).

**Procedure**

**Step 1** In your browser window, enter the Cisco WebEx site URL, for example, http://site.webex.com/.

**Step 2** Download the Cisco WebEx Productivity Tools from the left menu under **Support > Downloads > Productivity Tools**.

**Step 3** Follow the installation instructions.

**Step 4** Open Cisco WebEx One Click.

**Step 5** Click **Edit WebEx settings**.

**Step 6** Enter **http://site.webex.com/** into the Cisco WebEx site URL field.

**Step 7** Enter your Cisco WebEx host account user name and password.

**Step 8** Click **Apply**.

You should now be authenticated into Cisco WebEx Productivity Tools.
Step 9 Test One Click meetings and scheduling meetings from Microsoft Outlook or other Cisco WebEx client integrations.

---

Configuring Cisco WebEx Productivity Tools for the First Time with Directory Service

Complete this procedure to initially configure your Cisco WebEx Productivity Tools for Microsoft Outlook, IBM Lotus Notes, One Click, or other client applications if the following applies:

- You manually download and configure the Cisco WebEx Productivity Tools
- You are completing your initial configuration with Directory Service (SSO).

**Procedure**

**Step 1** Enter your LDAP credentials in the Cisco Unified MeetingPlace sign-in page.
The system automatically redirects you to the Cisco WebEx page, where you will already be signed in.

**Step 2** Open Cisco WebEx One Click.

**Step 3** Click **Edit WebEx settings**.

**Step 4** Enter `webexsitename.webex.com` into the Cisco WebEx site URL field.

**Step 5** Click **Apply**.

**Step 6** The user name and password field should now be greyed out
The system displays a small web browser that takes you to an internal page. You should now be authenticated into Cisco WebEx Productivity Tools.

**Step 7** Test One Click meetings and scheduling meetings from Microsoft Outlook or other Cisco WebEx client integrations.

**Note** You might need to restart Microsoft Outlook for the Cisco WebEx tool bar to appear.

---

Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx

- General Restrictions, page 8
- User Profile Restrictions, page 9
- Video Restrictions, page 10
- End-to-End Encryption Restrictions, page 10
- End-User Restrictions, page 11
General Restrictions

- The required Telephony Service Provider (TSP) connection from the Cisco Unified MeetingPlace Application Server to the WebEx data center can be established either directly or through a SOCKS proxy. HTTP proxies are not supported. Beware that proxies introduce delays that can adversely affect end user experiences. Cisco recommends either not using a proxy or carefully monitoring the communication through the proxy to assure there are no perceptible delays.

- When Cisco Unified MeetingPlace is integrated with Cisco WebEx, the following are not supported:
  - Languages other than U.S. English
  - Reservationless Single Number Access (RSNA)
  - Multiple Cisco Unified MeetingPlace sites

- If you are migrating from one Cisco Unified MeetingPlace release to another, you cannot transfer existing Cisco Unified MeetingPlace web meetings and attachments from the previous release of Cisco Unified MeetingPlace to Cisco WebEx.

  There is currently no workaround. Complete all existing meetings before migrating, or run both deployments concurrently until all existing meetings are completed.

- You can only use Cisco Unified MeetingPlace audio with Cisco WebEx Meeting Center.

  If you also use Cisco WebEx Sales Center or other Cisco WebEx centers, then have your Cisco WebEx customer service manager or account manager split your Cisco WebEx site into two sites:
  - Site A: Cisco WebEx Meeting Center + Cisco Unified MeetingPlace audio
  - Site B: other Cisco WebEx centers + previous audio conferencing provider

  In this split site, your users need to schedule meetings as follows:
  - (About Cisco WebEx Integration Option 1) Schedule Cisco WebEx Meeting Center meetings from Cisco Unified MeetingPlace.
  - (About Cisco WebEx Integration Option 2) Schedule Cisco WebEx Meeting Center meetings from the Cisco WebEx Site A end-user interface (http://SiteA.webex.com/).
  - Schedule all other Cisco WebEx meetings from the Cisco WebEx Site B end-user interface (http://SiteB.webex.com/).

- If you have a split site, Cisco Unified MeetingPlace provides audio conferencing functionality only to the Cisco WebEx site with which it is associated. The other Cisco WebEx site operates independently of Cisco Unified MeetingPlace.

- “Named host” deployments require a Cisco WebEx user account for each profiled user of Cisco Unified MeetingPlace. If there are more Cisco Unified MeetingPlace users than Cisco WebEx users, some users will be able to schedule but not actually join meetings.

  Use one or both of the following workarounds:
  - Obtain a concurrent-user or per-minute Cisco WebEx contract.
  - (About Cisco WebEx Integration Option 1 only) Determine which Cisco Unified MeetingPlace users actually require Cisco WebEx, and enable only these users to schedule Cisco WebEx web meetings. You can do this by configuring the Default web conference provider and Hide web conference provider fields in the user groups or user profiles.
• Usage reports and billing statistics cannot distinguish between web conferences provided by Cisco WebEx and web conferences provided by Cisco Unified MeetingPlace.
  As a workaround, do not enable both types of meetings; choose a single web conferencing provider.
• For information about recording limitations, see the following Cisco WebEx documents:
  – Recording and Playback FAQs
  – WebEx Network Recording Player for Advanced Recording Format (.arf) Files User's Guide

Related Topics
• Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx, page 7
• Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 1
• Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx, page 3
• How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12

User Profile Restrictions

The following Cisco Unified MeetingPlace user profile fields have different restrictions or requirements when the system is integrated with Cisco WebEx:
• The Profile Number field must be a maximum of 8 digits in length.
• First name and Last name—Required fields.
• User ID—Do not modify this field in an existing user profile. Doing so disables future sign-ins to Cisco WebEx by the user.
• User ID and User password—Avoid using diacritical or non-English characters in these fields. Doing so restricts the user from joining the Cisco WebEx web meeting directly after sign-in; instead, the user is sent to the Cisco WebEx site and can join the meeting indirectly from there.
• E-mail address—Required field. Maximum 64 characters. Must be unique on the Cisco WebEx site.
• Main phone number and Alternate phone number—Maximum 30 characters.
• Language—Only U.S. English is supported.
• Time zone—If the value in Cisco Unified MeetingPlace does not map to a Cisco WebEx value during the import or synchronization of a user profile, then the Cisco WebEx user profile uses the default value of the Cisco WebEx site.

Note
See the Time Zone Mapping Between Cisco WebEx and Cisco Unified MeetingPlace module.

Related Topics
• Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx, page 7
• Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 1
• Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx, page 3
• How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12
Video Restrictions

- When you obtain your Cisco WebEx account and site, you choose between Cisco Unified MeetingPlace video conferencing and Cisco WebEx webcam video. The Cisco WebEx site cannot support both types of video at the same time.
- Cisco Unified MeetingPlace video conferencing is not included in the Cisco WebEx recordings.
- Cisco Unified MeetingPlace video conferencing is available only to users with video privileges. Configure the Video usage user profile field appropriately for your users.

Related Topics
- Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx, page 7
- How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12

End-to-End Encryption Restrictions

The following restrictions apply to end-to-end encryption:

- If end-to-end encryption is enabled on the Cisco WebEx site, then the meeting owner (host) must join to start each meeting, even if the meeting does not use end-to-end encryption. Specifically, the following Cisco WebEx features are not supported when end-to-end encryption is enabled for the site:
  - Attendee Join Before Host—This feature enables attendees to join a meeting before the host, eliminating the need for attendees to wait for the host to start a meeting.
  - Scheduling Alternate Hosts—This feature enables the meeting owner (host) to designate other people as alternate hosts to a meeting, allowing them to start and host the meeting in the absence of the scheduled host. Once scheduled, either the host or any alternate host may start a meeting and take on the host role.
- Cisco WebEx Network-Based Recording (NBR) is not supported in end-to-end–encrypted meetings:
  - The audio portion of the end-to-end–encrypted meeting cannot be recorded.
  - The web portion of the end-to-end–encrypted meeting can be recorded only if the users select the PC-based recording option.

The end-to-end encryption configuration can be modified in the following ways:

- The Cisco WebEx administrator can enable or disable end-to-end encryption for the entire Cisco WebEx site.

**Note**
If end-to-end encryption is enabled or disabled, you must restart Cisco Unified MeetingPlace Web Conferencing services to update the site settings cache. When you restart the web server, all manual changes made to the registry are lost. For detailed information, see “Restarting All Web Conferencing Services” in the Managing Cisco Unified MeetingPlace Web Conferencing Services module.

- If end-to-end encryption is enabled on the Cisco WebEx site, then you can configure the privileges in Cisco WebEx user profiles to allow end-to-end encryption session types for the Meeting Center service.
By default, if the Cisco WebEx user profile allows end-to-end encryption for Meeting Center, then all Meeting Center meetings scheduled by that user will use end-to-end encryption. This is always true for About Cisco WebEx Integration Option 1.

- (About Cisco WebEx Integration Option 2 only) If you configure a Cisco WebEx user profile to allow end-to-end encryption:
  - While modifying the Cisco WebEx user profile, the user can specify a default session type to select or deselect end-to-end-encrypted meetings.
  - While scheduling a meeting, the user can select the end-to-end encryption session type.

Related Topics
- Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx, page 7
- Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 1
- Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx, page 3
- How to Integrate Cisco Unified MeetingPlace with Cisco WebEx, page 12

End-User Restrictions

- Restrictions that you may want to communicate to your end users:
  - Anyone may join Cisco WebEx web meetings from the public Cisco WebEx site, unless meeting passwords are in use. Also, anyone may dial out from Cisco WebEx web meetings.
  - Only the meeting owner (host) can start or stop recording a meeting.
  - Cisco WebEx web meetings that are scheduled with zero ports and that are attended by two or more web meeting participants do not get extended; such meetings end at the scheduled end time.
  - Application and desktop sharing in Cisco WebEx web meetings do not support dual-monitor systems.
  - Chinese, Korean, and Japanese character encoding is not supported.
  - See the “Video Restrictions” section on page 10.
- End-user restrictions for About Cisco WebEx Integration Option 1 only:
  - Users can schedule web conferences but not audio conferences from the “My WebEx” portal. Tell your users to schedule meetings from the Cisco Unified MeetingPlace Web Conferencing interface only.
  - All users must sign in through the Cisco Unified MeetingPlace end-user web interface before joining meetings. Joining meetings directly from the Cisco WebEx end-user web interface is not supported in this Cisco WebEx integration deployment.
  - IBM Lotus Notes integration and Cisco Unified MeetingPlace PhoneView is not supported for scheduling Cisco WebEx meetings.
Integrating Cisco Unified MeetingPlace with Cisco WebEx

How to Integrate Cisco Unified MeetingPlace with Cisco WebEx

- Configuring the Cisco WebEx Connection and Scheduling Options, page 12
- Creating and Uploading the Cisco WebEx Certificate, page 14
- Establishing or Resetting the Telephony Connection to Cisco WebEx, page 15
- Configuring Site Settings in the Cisco WebEx Site Administration, page 16
- Customizing Post-Meeting Web Page Settings, page 17
- Allowing the Audio Portion of a Meeting to Continue after Closing the Cisco WebEx Meeting Center Session, page 17
- Configuring Single Sign-On in the Cisco WebEx Site Administration, page 18
- Configuring the Cisco WebEx Audio Recorder, page 19
- Enabling Users to Schedule Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 20
- Transferring User Profiles From Cisco Unified MeetingPlace to Cisco WebEx, page 21
- Deactivating Cisco WebEx User Profiles, page 22
- Modifying Your Cisco WebEx Site Administration Account, page 23

Configuring the Cisco WebEx Connection and Scheduling Options

Before You Begin
- Read the prerequisites for your deployment:
  - Prerequisites for Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 2
  - Prerequisites for Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx, page 4
- Read the “Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx” section on page 7.
- If applicable, obtain the proxy server hostname and port number from your network administrator.
Integrating Cisco Unified MeetingPlace with Cisco WebEx

How to Integrate Cisco Unified MeetingPlace with Cisco WebEx

Obtain the following information from the Cisco WebEx administrator:
- Site ID
- Site name
- Partner ID
- Password for Cisco WebEx Site Administration

Note: The Cisco WebEx Site Provisioning group sends you an email with the Cisco WebEx site ID, Cisco WebEx site name, and the Cisco WebEx partner ID.

Understand the following:
- The Cisco WebEx Site always uses the host ID of “admin” (profile #0001) configured with a secure password. This host ID is dedicated to the Cisco WebEx integration for the user profile from the Cisco Unified MeetingPlace Administration page.
- Add this host ID to your Cisco WebEx site (if this was not already created) using your Cisco WebEx-provided administration account information.
- This host ID and password must match the Cisco Unified MeetingPlace “admin” (profile #0001) and password.
- We recommend that you set up different System Manager-level profiles for IT department personnel use. Do not use the default “admin” account in Cisco Unified MeetingPlace except for Cisco WebEx integration.

Procedure

Step 1
Sign in to the Cisco Unified MeetingPlace Administration Center.

Step 2
Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Site and Server.

Step 3
Set the Web conference scheduling field to:
- Unified MP schedule, Cisco WebEx meeting if you are deploying Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace.
- Cisco WebEx schedule, Cisco WebEx meeting if you are deploying Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx.

Note: Changes to the Web conference scheduling field will take effect after you complete the “Establishing or Resetting the Telephony Connection to Cisco WebEx” section on page 15.

Step 4
Configure the rest of the fields on the Cisco WebEx Site and Server Page. The rest of this information will be provided in an email from the Cisco WebEx Site Administrator.

Step 5
(Optional) Configure a proxy server if your company requires one in order to connect from inside the firewall to the outside internet to your Cisco WebEx site.

Step 6
Click Save.
Creating and Uploading the Cisco WebEx Certificate

Before You Begin
Complete the “Configuring the Cisco WebEx Connection and Scheduling Options” section on page 12.

Caution
If you create a certificate when one is already in use, then you will block further user access to Cisco WebEx through Cisco Unified MeetingPlace. User access will be re-enabled after you upload the new certificate to the Cisco WebEx Site Administration.

Restriction
Use the failoverUtil copyConfigFiles and failoverUtil restoreConfigFiles CLI commands to copy the certificate files and other unreplicated system files from the active server to the standby server. For detailed instructions, see “Configuring the Application Servers in a Failover Deployment” in the Configuring Application Server Failover for Cisco Unified MeetingPlace module.

Procedure

Step 1 Sign in to the Cisco Unified MeetingPlace Administration Center.
Step 2 Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Certificate.
Step 3 Click Create Certificate.
Step 4 Click OK.
Step 5 Click the Certificate location link.
Step 6 Save a local copy of the certificate.
Step 7 Click the Cisco WebEx Site Administration URL link.
Step 8 Sign in if prompted:
   • Enter the User ID of your Cisco Unified MeetingPlace system administrator user profile.
Integrating Cisco Unified MeetingPlace with Cisco WebEx

How to Integrate Cisco Unified MeetingPlace with Cisco WebEx

- Enter the Cisco WebEx site administration password that was provided by your Cisco WebEx administrator.

Step 9  Click SSO Configuration.
Step 10 Click Site Certificate Manager.
Step 11 Click Import Certificate.
Step 12 If a previous certificate is already in place, then click Remove the Certificate.
Step 13 In the Import your certificate field, browse to the local copy of the certificate.
Step 14 Click OK, then Close.

Related Topics
- Field Reference: Cisco WebEx Certificate in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Application Server Failover for Cisco Unified MeetingPlace module

What to Do Next
Proceed to the “Establishing or Resetting the Telephony Connection to Cisco WebEx” section on page 15.

Establishing or Resetting the Telephony Connection to Cisco WebEx

Before You Begin
Complete the “Creating and Uploading the Cisco WebEx Certificate” section on page 14.

Caution
Performing this task causes the system to drop all Cisco WebEx meetings that are in session.

Procedure

Step 1 Sign in to the Cisco Unified MeetingPlace Administration Center.
Step 2 Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Site and Server.
Step 3 Click Reset TSP Connection.
Step 4 Click OK to proceed with the reset.
Step 5 If you recently modified the Web conference scheduling field on the Cisco WebEx Site and Server Page, then wait 10 minutes before you proceed to the next step.
This enables the system to transfer the configuration update to the Web Server.
Step 6 On the Web Server, restart the Cisco Unified MeetingPlace Web Conferencing service.

Note When you restart the Web Server, all manual changes made to the registry are lost.
Troubleshooting Tips

- If the system reports an HTTP communication error, then do the following:
  - Check that the configured Cisco WebEx site name is correct by pointing a browser to the following URL: http://site-name.webex.com.
    
  If the URL is not reachable, and you verified that you configured the correct Cisco WebEx site name, then contact your Cisco WebEx administrator.
  - If your network requires a proxy configuration, then check and correct the Proxy server hostname and Proxy server port field values, which are provided by your network administrator.

- If the system is unable to establish the TSP connection or acquire IP addresses for the TSP primary host and TSP secondary host, then do the following:
  - Make sure that the Application Server is configured to use Network Time Protocol (NTP). If you did not configure NTP during installation, then use the net command to do so now.
  - Create and upload a new Cisco WebEx certificate. See the “Creating and Uploading the Cisco WebEx Certificate” section on page 14.

Related Topics

- Field Reference: Cisco WebEx Site and Server Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

What to Do Next

Proceed to the “Configuring Site Settings in the Cisco WebEx Site Administration” section on page 16.

Configuring Site Settings in the Cisco WebEx Site Administration

Before You Begin

Complete the “Establishing or Resetting the Telephony Connection to Cisco WebEx” section on page 15.

Procedure

Step 1

Go to the Cisco WebEx Site Administration:

a. Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Certificate.

b. Click the Cisco WebEx Site Administration URL link.

c. Sign in if prompted:

  - Enter the User ID of your Cisco Unified MeetingPlace system administrator user profile.
  - Enter the Cisco WebEx site administration password that was provided by your Cisco WebEx administrator.

Step 2

Click Site Settings.

Step 3

Check Allow user to store personal information for joining meetings and call-back teleconference.

Step 4

For About Cisco WebEx Integration Option 1 only:

a. Set Meeting email reminders to Off.

b. Uncheck the following:
- Display feedback form after meeting
- Require strict password for user accounts
- All meetings must have a password
- Require strict passwords for meetings

**Step 5**
Click **Update**.

---

**Related Topics**
- Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 1

**What to Do Next**
Proceed to the “Configuring Single Sign-On in the Cisco WebEx Site Administration” section on page 18.

---

**Customizing Post-Meeting Web Page Settings**

By default when a Cisco WebEx type web meeting has ended, the meeting close webpage directs to www.cisco.com.

The webpage URL can be modified by the system administrator.

**Procedure**

**Step 1**
Sign in to the Cisco Unified MeetingPlace Web Server as an administrator.

**Step 2**
Open Windows Explorer, and browse to C:\Program Files\Cisco Systems\MPWeb\HTML

**Step 3**
Locate the file called bu.html.

**Step 4**
Copy the file to another location.

**Step 5**
Right-click and select **Edit**, to edit the file using Notepad.

**Step 6**
Search for `self.location.href`, and replace `http://www.cisco.com` with your specified URL.

**Step 7**
Close and save the file called bu.html.

---

**Allowing the Audio Portion of a Meeting to Continue after Closing the Cisco WebEx Meeting Center Session**

Follow the steps below to allow the audio portion of a meeting to continue even after the Cisco WebEx portion of the meeting has finished.

**Before You Begin**
Click **Site Settings** then set the following:
- Check **Meeting Center**
- Check **Enable Teleconference Keep-Alive**
• Leave Default Setting (enabled/disabled) unchecked.

Procedure

Step 1 Schedule a Cisco WebEx meeting with several users and attend the meeting.

Step 2 Do the following when ending the meeting:
When the web portion of the meeting is finished, the host ends the meeting by choosing File > End Meeting or by closing the Cisco WebEx meeting room. You see a dialog box called “End Meeting”.

a. Ensure that Keep the teleconference running is checked.

b. Click OK.
The Cisco WebEx meeting rooms close but audio is still connected for all users.

What to Do Next
Proceed to the “Configuring Single Sign-On in the Cisco WebEx Site Administration” section on page 18.

Configuring Single Sign-On in the Cisco WebEx Site Administration

Perform this task to do the following:

• Enable system administrators to click a Cisco WebEx Site Administration URL link in the Cisco Unified MeetingPlace Administration Center to sign in to the Cisco WebEx Site Administration.

• Enable users to sign in to Cisco Unified MeetingPlace from Cisco WebEx using About Cisco WebEx Integration Option 2.

Before You Begin
Complete the “Configuring Site Settings in the Cisco WebEx Site Administration” section on page 16.

Procedure

Step 1 Go to the Cisco WebEx Site Administration:

a. Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Certificate.

b. Click the Cisco WebEx Site Administration URL link.

c. Sign in if prompted:

– Enter the User ID of your Cisco Unified MeetingPlace system administrator user profile.

– Enter the Cisco WebEx site administration password that was provided by your Cisco WebEx administrator.

Step 2 Click SSO Configuration.

Step 3 Configure the Default WebEx Target page URL field with the Cisco WebEx site page where you want end users to go after signing in. Sample URLs that you can use:

• Customer SSO Service Login URL—Already configured for you.

• Default WebEx Target page URL—http://<sitename>.webex.com/
Integrating Cisco Unified MeetingPlace with Cisco WebEx

How to Integrate Cisco Unified MeetingPlace with Cisco WebEx

- Customer SSO Error URL—Already configured for you.

**Step 4**
Uncheck **Require strict password for user accounts and Do not allow reuse of the last # passwords**.

**Step 5**
Click **Update**.

---

**What to Do Next**
Proceed to the “Configuring the Cisco WebEx Audio Recorder” section on page 19.

---

**Configuring the Cisco WebEx Audio Recorder**

Cisco Unified MeetingPlace comes with a preconfigured “recorder” user profile. Cisco WebEx Network-Based Recording (NBR) uses this profile to access and record the audio portion of meetings. Cisco Unified MeetingPlace treats the Cisco WebEx NBR as an auto-answer device.

---

**Note**
This is a required step in order to complete the Cisco Unified MeetingPlace to Cisco WebEx integration; otherwise, the TSP communication is not complete. Even if you do not plan to record meetings, you must perform this task to integrate Cisco Unified MeetingPlace with Cisco WebEx.

---

**Procedure**

**Step 1**
Sign in to the Cisco Unified MeetingPlace Administration Center.

**Step 2**
Click **System Configuration > Cisco WebEx Configuration > Cisco WebEx Audio Recorder**.

**Step 3**
Modify the **Profile number** and **Profile password** fields.

The updated values are automatically copied to the Cisco WebEx site. This profile/password is used by Cisco WebEx to record the audio portion of a meeting when recording is turned on in a Cisco WebEx meeting by the host.

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

**Step 5**
Click **System Configuration > Meeting Configuration**.

**Step 6**
Set **Meeting controls device** to Yes.

**Step 7**
(Optional) Configure the **Connected until meeting ends** field if you want to modify how the Cisco WebEx audio recorder is disconnected at the end of meetings.

**Step 8**
Click **Save**.

**Step 9**
From any phone, dial in to Cisco Unified MeetingPlace.

**Step 10**
Press 3#.

**Step 11**
Sign in using the **Profile number** and **Profile password** of the recorder profile.

By default, the recorder profile number is 0002, but it may be changed by the system administrator.

**Step 12**
When prompted, record a name, such as “Cisco WebEx Recorder.”

Recording a name is required only after the initial configuration of the recorder profile.
Related Topics

- How to Configure Auto-Answer Devices in the Configuring Endpoints for Cisco Unified MeetingPlace module

What to Do Next

- If you are deploying About Cisco WebEx Integration Option 1, proceed to the “Enabling Users to Schedule Cisco WebEx Meetings from Cisco Unified MeetingPlace” section on page 20.
- If you are deploying About Cisco WebEx Integration Option 2, proceed as follows:
  - If Directory Service is not configured on Cisco Unified MeetingPlace, proceed to the “Transferring User Profiles From Cisco Unified MeetingPlace to Cisco WebEx” section on page 21.
  - Otherwise, communicate the necessary information to your end users. See the “End-User Information for Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx” section on page 5.

Enabling Users to Schedule Cisco WebEx Meetings from Cisco Unified MeetingPlace

Perform this task only if you are deploying About Cisco WebEx Integration Option 1.

Before You Begin

- Complete the “Configuring Site Settings in the Cisco WebEx Site Administration” section on page 16.
- Read the “Restrictions for Integrating Cisco Unified MeetingPlace with Cisco WebEx” section on page 7.

Procedure

**Step 1** Sign in to the Cisco Unified MeetingPlace Administration Center.

**Step 2** Click User Configuration.

**Step 3** Click User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.

**Step 4** Click Edit or Add New, depending on whether you want to configure an existing or new user group or user profile.

**Step 5** Configure the following fields:

  - Default web conference provider—Whether Cisco WebEx or Cisco Unified MeetingPlace is selected by default when the user schedules a meeting from the Cisco Unified MeetingPlace end-user web interface.
  - Hide web conference provider—Whether the user can see and change the web conferencing provider while scheduling a meeting from the Cisco Unified MeetingPlace end-user web interface.

**Step 6** (For Cisco Unified MeetingPlace video conferencing) Configure the Video usage field to enable the appropriate video privileges for the user.

**Step 7** (Optional) Set the Meeting password required field to Yes.
Caution

Anyone can join Cisco WebEx meetings that are not password protected, because meetings that are in session are publicly listed on the Cisco WebEx end-user web interface.

Step 8
Click Save.

Step 9
Repeat Step 2 through Step 8 for all user groups and user profiles for which you want to enable the scheduling of Cisco WebEx meetings.

Related Topics
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace, page 1

What to Do Next
Communicate the necessary information to your end users. See the “End-User Information for Integration Option 1: Schedule and Attend Cisco WebEx Meetings from Cisco Unified MeetingPlace” section on page 2

Transferring User Profiles From Cisco Unified MeetingPlace to Cisco WebEx

If you configure Directory Service on your Cisco Unified MeetingPlace system, then a Cisco WebEx user profile is automatically imported or updated from Cisco Unified MeetingPlace when the user successfully authenticates through the Cisco Unified MeetingPlace Application Server (http://application-server/).

If you have not configured Directory Service on Cisco Unified MeetingPlace, then you must perform this task to manually transfer user profiles from Cisco Unified MeetingPlace to the Cisco WebEx Site Administration.

Before You Begin
- Complete this task only if the following are true:
  - You deploy About Cisco WebEx Integration Option 2.
  - Directory Service is not configured on Cisco Unified MeetingPlace.
- If you want to be notified when the transfer is complete, then make sure that your Cisco WebEx Site Administration account includes a valid e-mail address. See the “Modifying Your Cisco WebEx Site Administration Account” section on page 23.
- Complete the “Establishing or Resetting the Telephony Connection to Cisco WebEx” section on page 15.

Restrictions
When Directory Service is not configured on the system, user profiles are not synchronized between Cisco Unified MeetingPlace and Cisco WebEx.

Specifically, if you delete or modify a user profile in Cisco Unified MeetingPlace, the corresponding user profile in Cisco WebEx is not deactivated or updated. You must manually deactivate or modify the user profile(s) through the Cisco WebEx Site Administration.
Similarly, if you deactivate or modify a user profile in Cisco WebEx, the corresponding user profile in Cisco Unified MeetingPlace is not deleted or updated. You must manually delete, deactivate, or modify the user profile(s) through the Cisco Unified MeetingPlace Administration Center.

**Procedure**

**Step 1** Sign in to the Cisco Unified MeetingPlace Administration Center.
**Step 2** Click System Configuration > Cisco WebEx Configuration > Export Profiles for Cisco WebEx.
**Step 3** Click Export.
**Step 4** Click OK.
**Step 5** Save a local copy of the file.
**Step 6** Click the Cisco WebEx Site Administration URL link.
**Step 7** Sign in if prompted:
- Enter the User ID of your Cisco Unified MeetingPlace system administrator user profile.
- Enter the Cisco WebEx site administration password that was provided by your Cisco WebEx administrator.
**Step 8** Click Import/Export Users.
**Step 9** Click Import.
**Step 10** Browse to the file containing the exported Cisco Unified MeetingPlace user profiles.
**Step 11** Click Upload File.

Your import submission is added to a queue whose length and speed depends on the system load at that time. After the import is complete, Cisco WebEx sends confirmation to the e-mail address in your Cisco WebEx Site Administration account.

**Related Topics**
- Configuring Cisco Unified MeetingPlace Directory Service module
- Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx, page 3
- Deactivating Cisco WebEx User Profiles, page 22

**What to Do Next**

Communicate the necessary information to your end users. See the “End-User Information for Integration Option 2: Schedule and Attend Cisco WebEx Meetings from Cisco WebEx” section on page 5

**Deactivating Cisco WebEx User Profiles**

**Before You Begin**

You perform this task in the Cisco WebEx Site Administration. Because the user interface varies by Cisco WebEx release, you should check the Cisco WebEx documentation for step-by-step instructions for your specific release.
Restrictions

- If you deactivate or edit user profiles through the Cisco WebEx Site Administration, you must manually make those changes through the Cisco Unified MeetingPlace Administration Center. Changes made to Cisco WebEx user profiles are not automatically synchronized with the corresponding Cisco Unified MeetingPlace user profiles.
- You cannot delete user profiles from Cisco WebEx.

Procedure

Step 1
Go to the Cisco WebEx Site Administration:

a. Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Certificate.

b. Click the Cisco WebEx Site Administration URL link.

c. Sign in if prompted:
   - Enter the User ID of your Cisco Unified MeetingPlace system administrator user profile.
   - Enter the Cisco WebEx site administration password that was provided by your Cisco WebEx administrator.

Step 2
Click Edit User List.

Step 3
Find the user profile that you want to deactivate.

Step 4
Uncheck Active for that user profile.

Step 5
Click Submit.

Step 6
Repeat Step 3 to Step 5 for each user profile that you want to deactivate.

Related Topics

- Deleting User Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module
- Deleting a User Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module

Modifying Your Cisco WebEx Site Administration Account

This task is typically performed only when you need to modify the e-mail address for receiving Cisco WebEx administration messages.

Before You Begin

You perform this task in the Cisco WebEx Site Administration. Because the user interface varies by Cisco WebEx release, you should check the Cisco WebEx documentation for step-by-step instructions for your specific release.

Procedure

Step 1
Go to the Cisco WebEx Site Administration:

a. Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Certificate.

b. Click the Cisco WebEx Site Administration URL link.
Integrating Cisco Unified MeetingPlace with Cisco WebEx

How to Integrate Cisco Unified MeetingPlace with Cisco WebEx

- Sign in if prompted:
  - Enter the User ID of your Cisco Unified MeetingPlace system administrator user profile.
  - Enter the Cisco WebEx site administration password that was provided by your Cisco WebEx administrator.

Step 2  Click **Edit User List**.

Step 3  Find your user account.

If you signed in using the Cisco Unified MeetingPlace preconfigured admin profile, then the default username is “admin.”

Step 4  Click the name for that user account.

Step 5  Modify the account information.

Step 6  Click **Update**.
Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook

Release 7.1
Revised: April 3, 2011 8:30 pm

This section describes how to enable users to schedule, reschedule, and cancel meetings from the Microsoft Outlook calendar. This Microsoft Outlook integration option is often referred to as the front-end deployment. When users accept an invitation, the meeting information and a click-to-attend link become available from their Microsoft Outlook calendar. The meeting scheduler receives Microsoft Outlook replies that indicate which attendees accepted or declined the invitation.

Note
This document does not describe how to enable Cisco Unified MeetingPlace to send Microsoft Outlook calendar notifications for meetings that are scheduled from the Cisco Unified MeetingPlace end-user web interface. That Microsoft Outlook integration option is often referred to as the back-end deployment. See the following for information about the back-end deployment:

- Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface module

Topics in this section include:

- Prerequisites for Scheduling From Microsoft Outlook, page 1
- Restrictions for Scheduling From Microsoft Outlook, page 2
- How to Enable Scheduling From Microsoft Outlook, page 3
- Customization Options for Scheduling from Microsoft Outlook, page 11
- About the Cisco Unified MeetingPlace Plug-in and Different Versions of Microsoft Outlook, page 11

Prerequisites for Scheduling From Microsoft Outlook

- Install the msft_int license.
- Configure a Cisco Unified MeetingPlace user profile for each user who will schedule Cisco Unified MeetingPlace meetings from Microsoft Outlook.

If you plan to use the Single Sign-On default authentication method, then the Cisco Unified MeetingPlace User ID must match the Microsoft Outlook username.
• Enable Secure Sockets Layer (SSL) on the Application Server.
  – SSL is required only to use the Single Sign-On user authentication method for Microsoft Outlook integration.

• In order for end users to receive complete and correct Cisco Unified MeetingPlace notifications in Microsoft Outlook, the e-mail accounts set up in the Microsoft Outlook client must be configured to use the Server Type option called “Microsoft Exchange Server.” Cisco Unified MeetingPlace for Microsoft Outlook does not support other server types, such as POP3.

• In order for a Microsoft Outlook delegate to schedule Cisco Unified MeetingPlace meetings on behalf of other users, the delegate must have the “Editor” level of delegate access permissions.

• The delegate and delegator must have identical scheduling privileges in their Cisco Unified MeetingPlace profiles in order for the delegate to properly schedule MeetingPlace meetings from Microsoft Outlook.

Note: Microsoft Outlook delegates are completely separate from Cisco Unified MeetingPlace delegates. The Type of user and User ID of delegate fields in Cisco Unified MeetingPlace user profiles do not affect the privileges and capabilities of Microsoft Outlook delegates.

Related Topics
• Installing and Managing Licenses for Cisco Unified MeetingPlace module
• Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
• Configuring SSL for the Cisco Unified MeetingPlace Application Server module

Restrictions for Scheduling From Microsoft Outlook

• Invitees always receive Microsoft Outlook calendar notifications in the Language that is specified in the Cisco Unified MeetingPlace user profile of the meeting owner.

• If meetings scheduled through Microsoft Outlook are modified through the Cisco Unified MeetingPlace end-user web interface (by anyone, regardless of user type):
  – E-mail notifications are not sent for those changes.
  – The Microsoft Outlook calendar of the meeting owner and invitees will not reflect those changes.

• Users of type End user and Delegate can make only limited changes via the Cisco Unified MeetingPlace end-user web interface to meetings that were scheduled from Microsoft Outlook. Specifically, these users can only make changes that cannot be made from Microsoft Outlook, such as specifying alternate hosts for Cisco WebEx meetings.

Users of type Attendant and System administrator can make the same changes as end users and delegates, but they can also delete meetings from the Cisco Unified MeetingPlace end-user web interface.

• We do not support multiple Microsoft Outlook users in a single Microsoft Windows login session. The username that was entered to sign in to Microsoft Windows must match the Microsoft Outlook username, which is typically the mailbox name for the user.
Users are invited from the Microsoft Outlook directory and cannot be invited by Cisco Unified MeetingPlace profile. Cisco Unified MeetingPlace does, however, populate the meeting participant list using the user profiles with e-mail addresses that match those in the Microsoft Outlook meeting invitation.

Meeting schedulers may invite a video terminal from the Microsoft Outlook calendar only if the Requirements for Inviting Video Terminal Profiles from Microsoft Outlook are met.

Only one email notification template, plain-text NotifySchedule.tpl, is used for the Microsoft Outlook calendar notifications. HTML-based notifications are not supported when scheduling meetings from the Microsoft Outlook client.

Delegates are not supported when you enable Single Sign-On (SSO) based on Windows Active Directory credentials.


Meetings that are scheduled while SSL is enabled must be rescheduled with SSL enabled. The system does not support the rescheduling of SSL-enabled meetings when SSL is disabled.

Related Topics

- Requirements for Inviting Video Terminal Profiles from Microsoft Outlook in the Configuring Endpoints for Cisco Unified MeetingPlace module
- How to Configure Video Terminal Profiles in the Configuring Endpoints for Cisco Unified MeetingPlace module

How to Enable Scheduling From Microsoft Outlook

- About Default Authentication Methods for Microsoft Outlook Users, page 3
- Configuring the Default Authentication Method for Microsoft Outlook Users, page 5
- Adding Cisco Unified MeetingPlace Systems to the Plug-In for Microsoft Outlook, page 6
- How to Install the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook, page 7
- Customizing the Cisco Unified MeetingPlace Scheduling Form for Microsoft Outlook, page 10

About Default Authentication Methods for Microsoft Outlook Users

The front-end Microsoft Outlook integration provides two default user authentication methods:

- Remember Me, page 3
- Single Sign-On, page 4

Remember Me

If you choose the Remember Me default user authentication method:

- Users must enable the use of cookies on their browsers.
The first time a user tries to schedule a Cisco Unified MeetingPlace meeting from Microsoft Outlook, the user is prompted to sign in to Cisco Unified MeetingPlace.

If cookies are enabled on the browser, then the user can select the Remember Me option. The stored cookies are then used for future authentication, so the user does not need to sign in each time the user selects the MeetingPlace tab.

If the User password expires, the user is prompted to sign in to Cisco Unified MeetingPlace and change the password. The user can again select the Remember Me option.

Related Topics

- Configuring the Default Authentication Method for Microsoft Outlook Users, page 5

**Single Sign-On**

If you choose a Single Sign-On default user authentication method, users are not prompted to sign in to Cisco Unified MeetingPlace from Microsoft Outlook after successfully signing in to Microsoft Exchange or to the Windows Active Directory domain.

**Note**

- Delegates are not supported when you enable Single Sign-On (SSO) based on Windows Active Directory credentials.
- The Cisco Unified MeetingPlace database contains lower-case versions of user IDs. Make sure that any user IDs you enter or retrieve from Windows Active Directory or Microsoft Exchange are in lower-case before comparing them with user IDs in the Cisco Unified MeetingPlace database.

Requirements for Single Sign-On Authentication:

- If authenticating through Microsoft Exchange, the user must be able to successfully sign in to Microsoft Exchange when the Microsoft Outlook client launches.
- The Microsoft Exchange User ID must match a User ID in Cisco Unified MeetingPlace.
- In a workgroup environment, the domain portion of the user email address (that is, the part after @) must match a configured Outlook Single Sign-On Domain in Cisco Unified MeetingPlace.

For example, from the email address userA@example.com, you would configure “example.com” as a domain in Cisco Unified MeetingPlace.

In a domain environment, the following requirements apply:

- If authenticating through Windows Active Directory, the user must be able to successfully sign in to the Windows Active Directory domain when he signs in to his computer.
- The domain of the client machine must match a configured Outlook Single Sign-On Domain in Cisco Unified MeetingPlace.

Note that the client machine domain may differ from the user domain. For example, a user PC may be in domainA.example.com, while the user account is domainB\username. You would configure “domainA” in Cisco Unified MeetingPlace.

- Each Cisco Unified MeetingPlace user must have a unique username in Microsoft Outlook and Microsoft Exchange that is the same across the entire organization in Active Directory.
For example, suppose that Cisco Unified MeetingPlace user “userA” is associated with two different domains, domain1.example.com and domain2.example.com, both of which you configured in Cisco Unified MeetingPlace. The Single Sign-On authentication method assumes that userA@domain1.example.com and userA@domain2.example.com refer to the same “userA” user profile in Cisco Unified MeetingPlace.

Related Topics
- Configuring the Default Authentication Method for Microsoft Outlook Users, page 5

Configuring the Default Authentication Method for Microsoft Outlook Users

By default, the system uses the Remember Me authentication method. If the configured default authentication method fails, the user is prompted to enter the Cisco Unified MeetingPlace User ID and User password after selecting the MeetingPlace tab in Microsoft Outlook.

Before You Begin
- Complete the “Prerequisites for Scheduling From Microsoft Outlook” section on page 1.
- Read the “Restrictions for Scheduling From Microsoft Outlook” section on page 2.
- Read the “About Default Authentication Methods for Microsoft Outlook Users” section on page 3.
- If configuring Single Sign-On authentication, make sure that SSL is enabled.

Procedure

Step 1  Sign in to the Cisco Unified MeetingPlace Administration Center.
Step 2  Select System Configuration > Outlook Authentication Configuration.
Step 3  Select a default authentication method.
Step 4  If you selected Single sign-on using Exchange or Single sign-on using Active Directory, configure the domains of the Microsoft Outlook users:
   a.  Click Add New, or click an existing entry.
   b.  Enter the domain in the Outlook Single Sign-On Domain field.
   c.  Click Save.
   d.  Repeat Step 4 as needed to configure all domains that are used by your Cisco Unified MeetingPlace for Microsoft Outlook users.
Step 5  Click Save.

What to Do Next
- If you want to make multiple Cisco Unified MeetingPlace systems available for meetings scheduled from Microsoft Outlook, proceed to the “Adding Cisco Unified MeetingPlace Systems to the Plug-In for Microsoft Outlook” section on page 6.
- Otherwise, proceed to the “How to Install the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook” section on page 7.
Adding Cisco Unified MeetingPlace Systems to the Plug-In for Microsoft Outlook

The Cisco Unified MeetingPlace plug-in for Microsoft Outlook enables end users to click a tab within the Microsoft Outlook calendar to access a Cisco Unified MeetingPlace scheduling form. The plug-in comes preconfigured with system information that was entered while installing Cisco Unified MeetingPlace on the Application Server. You can, however, perform this task to enable each user to use one calendar to schedule and manage meetings on multiple Cisco Unified MeetingPlace systems.

When multiple Cisco Unified MeetingPlace systems are available, the user may specify which system to use by default from Microsoft Outlook as follows:

<table>
<thead>
<tr>
<th>For This Microsoft Outlook Version</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Microsoft Outlook 2003</td>
<td>Click <strong>Tools &gt; Options</strong> and select the <strong>MeetingPlace</strong> tab.</td>
</tr>
<tr>
<td>Microsoft Outlook 2007 and 2010</td>
<td>Open the calendar, click the down arrow on the <strong>MeetingPlace</strong> button and select <strong>Settings</strong>.</td>
</tr>
</tbody>
</table>

**Before You Begin**
- Perform this task only if you want to make multiple Cisco Unified MeetingPlace systems available for meetings scheduled from Microsoft Outlook.
- Complete the “Prerequisites for Scheduling From Microsoft Outlook” section on page 1.
- Read the “Restrictions for Scheduling From Microsoft Outlook” section on page 2.

**Procedure**

**Step 1**  Sign in to the Cisco Unified MeetingPlace Administration Center.

**Step 2**  Select **System Configuration > Outlook Plug-In Configuration**.

**Step 3**  Click **Add New**, or click an existing entry.

**Step 4**  Enter the **Name** and **URL** for the Application Server of the Cisco Unified MeetingPlace system.

**Step 5**  Click **Save**.

**What to Do Next**
Proceed to the “How to Install the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook” section on page 7.

**Related Topics**
- Field Reference: Outlook Plug-In Configuration Page, Add Cisco Unified MeetingPlace Server Page, and Edit Cisco Unified MeetingPlace Server Page in the Administration Center Page References for Cisco Unified MeetingPlace module
How to Install the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook

You can install the Cisco Unified MeetingPlace plug-in for Microsoft Outlook by using a setup.exe file or an MSI file. Both setup.exe and MSI detects which Microsoft Outlook version is installed on your computer and installs the appropriate plug-in.

Make sure that you choose one deployment model (.exe file or MSI file) for both initial installation and upgrades. If you choose the MSI deployment model, make sure that you “push” the new MSI file after each Application Server upgrade.

Note
Cisco Unified MeetingPlace for Microsoft Outlook does not support multiple versions of the Cisco Unified MeetingPlace plug-in on the same system.

- Requirements for Client Installation of the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook, page 7
- Installing the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook Locally on the End-User PC, page 8
- Installing the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook with MSI, page 8
- Installing the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook By Using an Automated Distribution Tool, page 9

Related Topics

Requirements for Client Installation of the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook

- Install the Cisco Unified MeetingPlace plug-in for Microsoft Outlook on the PCs of all Microsoft Outlook end users that are connected to your Microsoft Exchange Server. If a Microsoft Outlook end user does not have the plug-in installed when the user clicks the MeetingPlace tab in a received meeting notification, that user may see an error. Users who are not connected to the Microsoft Exchange Server do not see the MeetingPlace tab.

- If Microsoft Outlook delegates will use the Microsoft Outlook calendar to schedule Cisco Unified MeetingPlace meetings on behalf of other users, then each Microsoft Outlook delegate and each person on whose behalf meetings are scheduled must install the Cisco Unified MeetingPlace plug-in for Microsoft Outlook.

Note
Microsoft Outlook delegates are completely separate from Cisco Unified MeetingPlace delegates. The Type of user and User ID of delegate fields in Cisco Unified MeetingPlace user profiles do not affect the privileges and capabilities of Microsoft Outlook delegates.
Installing the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook Locally on the End-User PC

Before You Begin

- Install the msft_int license. See the Installing and Managing Licenses for Cisco Unified MeetingPlace module.
- If you want to enable each user to use one calendar to schedule and manage meetings on multiple Cisco Unified MeetingPlace systems, then complete the “Adding Cisco Unified MeetingPlace Systems to the Plug-In for Microsoft Outlook” section on page 6.
- Read the “Requirements for Client Installation of the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook” section on page 7.

Restriction

This installation option is available only for Windows PCs. The “Download Outlook Plug-In” link on the end-user web interface does not appear for other PCs.

Procedure

Step 1  Sign in to the end-user PC with administrator access.
Step 2  Sign in to the Cisco Unified MeetingPlace end-user web interface of an internal Web Server.
Step 3  Click Download Outlook Plug-In.
Step 4  Click Save.
Step 5  After the setup.exe file is downloaded, complete these steps on the client PC:
   a. Exit the Microsoft Outlook client software.
   b. Run the setup.exe file.
   Note To make the Cisco Unified MeetingPlace scheduling form available to any user who logs in to a specific computer, use the -admin switch to install the client software. Specifically, click Start > Run, then enter <pathname> setup.exe -admin.
   c. Click OK to install.
Step 6  After installation is complete, launch Microsoft Outlook.
Step 7  Verify that you can schedule meetings by clicking the MeetingPlace tab and filling out the scheduling form.
   For details, click Help in the scheduling form.

What to Do Next

(Optional) Proceed to the “Customizing the Cisco Unified MeetingPlace Scheduling Form for Microsoft Outlook” section on page 10.

Installing the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook with MSI

Use the following information to “push” the MSI file out to end-users.

By default, MSI installs the plug-in at $ProgramFiles\Cisco\MeetingPlace\MPOI\MP4OL.dll or MP4OL64.dll.

These are the MSI commands:

- SERVERURL: Cisco Unified MeetingPlace server URL
- ADMIN:
  - Value of 1, when the plug-in is installed for all users. This is the default value.
  - Value of 2, when the plug-in is installed for the current user.
- LOADHIDDENIEWIN: Pass 1 to load a hidden Internet Explorer window after Microsoft Outlook starts up. By default, Internet Explorer is not loaded after Microsoft Outlook starts up.

Installing the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook By Using an Automated Distribution Tool

This section describes how to use an automated distribution system, such as the Microsoft Systems Management Server (SMS), to remotely distribute and install the Cisco Unified MeetingPlace plug-in for Microsoft Outlook.

You can install the Cisco Unified MeetingPlace plug-in for Microsoft Outlook using either or both of the following switches:

- Silent—Suppresses the need for user input.
- Admin—Installs the Cisco Unified MeetingPlace plug-in for Microsoft Outlook for access by all users of a computer.

Before You Begin

- Install the msft_int license. See the Installing and Managing Licenses for Cisco Unified MeetingPlace module.
- If you want to enable each user to use one calendar to schedule and manage meetings on multiple Cisco Unified MeetingPlace systems, then complete the “Adding Cisco Unified MeetingPlace Systems to the Plug-In for Microsoft Outlook” section on page 6.
- Read the “Requirements for Client Installation of the Cisco Unified MeetingPlace Plug-In for Microsoft Outlook” section on page 7.

Restriction

Cisco Systems does not provide technical support for automated distribution tools.

- SMS per-user mode is not supported.
- If you choose to install or uninstall silently while using Window Vista, make sure that you open the command console in “run as administrator” mode.
- Make sure that you close the Microsoft Outlook client before upgrading or uninstalling the Cisco Unified MeetingPlace plug-in.
- If users are signing in to their computers with remote desktop while you are installing, make sure that they restart their computers. Otherwise, the Cisco Unified MeetingPlace for Microsoft Outlook integration may not work correctly.
Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook

How to Enable Scheduling From Microsoft Outlook

Procedure

Step 1  (Optional) Test that the installation switches work correctly by completing these steps from a client PC:
   a. Choose Start > Run and enter: <path to setup.exe>/admin /silent.
   b. Verify that no user prompts appear on the end user PC.
   c. Verify that the following server information exists in the registry:
      - HKCU\software\Latitude\MeetingPlace for Outlook
      - HKU\.default\software\Latitude\MeetingPlace for Outlook (admin)

Step 2  Use an automated distribution tool to distribute and install the setup.exe file on end-user PCs.
Refer to the documentation for your specific automated distribution tool.

Step 3  Instruct the end user to verify successful installation by completing these steps on the end-user PC:
   a. Restart or launch Microsoft Outlook.
   b. Open the calendar.
   c. Verify that the MeetingPlace tab works.

Step 4  Remind end users that they can click Help in the Cisco Unified MeetingPlace scheduling form.

What to Do Next
(Optional) Proceed to the “Customization Options for Scheduling from Microsoft Outlook” section on page 11.

Customizing the Cisco Unified MeetingPlace Scheduling Form for Microsoft Outlook

From Microsoft Outlook, users access the Cisco Unified MeetingPlace scheduling form by creating or opening a calendar appointment and then clicking the MeetingPlace tab. You can choose the information and options that users see in the Cisco Unified MeetingPlace scheduling form.

Procedure

Step 1  Sign in to the Cisco Unified MeetingPlace Administration Center.
Step 2  Click System Configuration > Customize Outlook Interface.
Step 3  Choose the language.
Step 4  Customize or hide fields as desired for the scheduling form specific to that language.
Step 5  Click Save.
Step 6  Repeat this task for each language used on your system.
Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook

Customization Options for Scheduling from Microsoft Outlook

<table>
<thead>
<tr>
<th>Customization Option</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Customizing the scheduling form</td>
<td>Customizing the Cisco Unified MeetingPlace Scheduling Form for Microsoft Outlook, page 10</td>
</tr>
<tr>
<td></td>
<td>Configuring Flex Fields for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Customizing e-mail notification</td>
<td>Customizing E-Mail Notifications for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Changing which meeting template is used by default</td>
<td>Changing the Default Meeting Template for Meetings Scheduled From Microsoft Outlook in the Configuring Meetings for Cisco Unified MeetingPlace module</td>
</tr>
</tbody>
</table>

**About the Cisco Unified MeetingPlace Plug-in and Different Versions of Microsoft Outlook**

The following section describes some differences that you may find when using the Cisco Unified MeetingPlace Release 7.1 plug-in with Microsoft Outlook 2003, 2007, and 2010.

<table>
<thead>
<tr>
<th>Feature</th>
<th>Microsoft Outlook 2003</th>
<th>Microsoft Outlook 2007</th>
<th>Microsoft Outlook 2010</th>
</tr>
</thead>
<tbody>
<tr>
<td>Location of MeetingPlace settings</td>
<td>Settings are found on the MeetingPlace tab (Tools &gt; Option).</td>
<td>MeetingPlace settings are exposed directly as a drop-down item from the MeetingPlace button on the Microsoft Outlook 2007 toolbar.</td>
<td>MeetingPlace settings are exposed directly as a drop-down item from the MeetingPlace button on the Microsoft Outlook 2010 toolbar.</td>
</tr>
<tr>
<td>Notifications</td>
<td>Supports notifications in RTF format.</td>
<td>Supports notifications in plain text format. Does not support RTF format.</td>
<td>Supports notifications in plain text format. Does not support RTF format.</td>
</tr>
<tr>
<td>Single sign-on (SSO) authentication</td>
<td>SSO using Active Directory is not supported. System will default to the Remember Me authentication method instead. SSO using Microsoft Exchange is supported.</td>
<td>Supported using either Active Directory or Microsoft Exchange. Delegates are not supported if you choose SSO with Active Directory.</td>
<td>Supported using either Active Directory or Microsoft Exchange. Delegates are not supported if you choose SSO with Active Directory.</td>
</tr>
</tbody>
</table>
About the Cisco Unified MeetingPlace Plug-in and Different Versions of Microsoft Outlook
Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface

Release 7.1
Revised: April 3, 2011 8:30 pm

This document describes the Microsoft Outlook back-end integration, which enables Cisco Unified MeetingPlace to send Microsoft Outlook calendar notifications for meetings that are scheduled from the Cisco Unified MeetingPlace end-user web interface.

This document does not describe the Microsoft Outlook front-end integration, which enables users to schedule, reschedule, and cancel meetings from the Microsoft Outlook calendar. For information about Microsoft Outlook front-end integration, see the Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module.

Topics in this section include:

- Prerequisites for Sending Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface, page 2
- Restrictions for Sending Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface, page 2
- How to Enable Cisco Unified MeetingPlace to Send Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface, page 3
Prerequisites for Sending Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface

- Install the msft_int license.
- If you are upgrading your Cisco Unified MeetingPlace system, complete the relevant tasks in the “Upgrading Microsoft Outlook for Cisco Unified MeetingPlace” section of the Installation, Upgrade, and Migration Guide for Cisco Unified MeetingPlace Release 7.1.
- In order for end users to receive complete and correct Cisco Unified MeetingPlace notifications in Microsoft Outlook, the e-mail accounts set up in the Microsoft Outlook client must be configured to use the Server Type option called “Microsoft Exchange Server.” Cisco Unified MeetingPlace for Microsoft Outlook does not support other server types, such as POP3.

Related Topics
- Installing and Managing Licenses for Cisco Unified MeetingPlace module
- Configuring SSL for the Cisco Unified MeetingPlace Application Server module

Restrictions for Sending Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface

- You must never delete items from the Cisco Unified MeetingPlace–dedicated mailbox on the Microsoft Exchange Server, including the Deleted Items folder. The system automatically purges the inbox periodically.
- HTML notifications are supported for meetings scheduled from the end-user web interface. Note that this is different from meetings that are scheduled from the Microsoft Outlook client, which supports plain-text notifications only.
- On the Microsoft Outlook scheduling tab, users will see only the attendees whose user profiles have the same configuration for all of the following fields:
  - E-mail type and format
  - Language
  - Receive attachments
To enable users to see a complete list of invitees, set the Include invitee list when scheduled from web user profile field to Yes for all users who schedule meetings.
How to Enable Cisco Unified MeetingPlace to Send Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface

- Uninstalling Cisco Unified MeetingPlace for Microsoft Outlook Gateway From the Web Server, page 3
- Creating a Cisco Unified MeetingPlace–Dedicated E-Mail Account and Mailbox on the Microsoft Exchange Server, page 4
- Configuring Cisco Unified MeetingPlace to Support TLS Encryption, page 5
- Configuring the Cisco Unified MeetingPlace Connection to the Microsoft Exchange Server, page 6

Uninstalling Cisco Unified MeetingPlace for Microsoft Outlook Gateway From the Web Server

Perform this task to make sure that your Web Server does not have the Microsoft Outlook notification gateway installed.

**Before You Begin**

If you have a fresh new Cisco Unified MeetingPlace installation and have never upgraded your system, then you may skip this task. Proceed to the (“Creating a Cisco Unified MeetingPlace–Dedicated E-Mail Account and Mailbox on the Microsoft Exchange Server” section on page 4.

**Procedure**

**Step 1** Stop all Cisco Unified MeetingPlace Web Conferencing services.

**Step 2** Choose Start > Control Panel > Add/Remove Programs.

**Step 3** Select the Cisco Unified MeetingPlace for Microsoft Outlook Gateway.

**Step 4** Click Remove.

**Step 5** Restart the Web Server.

**Step 6** Check the list of programs in Add/Remove Programs to verify that the Cisco Unified MeetingPlace for Microsoft Outlook Gateway was successfully uninstalled.

**Step 7** Repeat this procedure for each Web Server in the site.

**Note**

When you restart the Web Server, all manual changes made to the registry are lost.

**What To Do Next**

- Creating a Cisco Unified MeetingPlace–Dedicated E-Mail Account and Mailbox on the Microsoft Exchange Server, page 4
Creating a Cisco Unified MeetingPlace–Dedicated E-Mail Account and Mailbox on the Microsoft Exchange Server

Related Topics

- Stopping All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

Before You Begin

- Read the following sections:
  - Prerequisites for Sending Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface, page 2
  - Restrictions for Sending Microsoft Outlook Calendar Notifications for Meetings Scheduled from the End-User Web Interface, page 2
- Complete the “Uninstalling Cisco Unified MeetingPlace for Microsoft Outlook Gateway From the Web Server” section on page 3.
- Work with the Microsoft Exchange Server administrator to make sure that SMTP access to the Microsoft Exchange Server is allowed.
- For detailed instructions on how to perform any of these steps, see the documentation for your specific Microsoft Exchange Server.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Create a user on your Microsoft Windows domain, for example, “MeetingPlace.”</td>
</tr>
<tr>
<td>Step 2</td>
<td>Create a mailbox for this user on the Microsoft Exchange Server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Write down the username and password for this e-mail account.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Make sure that this mailbox is allowed to send mail to itself.</td>
</tr>
<tr>
<td>Step 5</td>
<td>If the Microsoft Exchange Server is configured to disable anonymous access via SMTP, then make sure that you grant the Send As permission for all users in the Enterprise for this mailbox. The Send As permission enables each Microsoft Outlook calendar notification to appear to come from the meeting scheduler (instead of the Cisco Unified MeetingPlace–dedicated mailbox) for meetings that are scheduled from the Cisco Unified MeetingPlace end-user web interface.</td>
</tr>
<tr>
<td>Step 6</td>
<td>Verify that the mailbox can send and receive messages.</td>
</tr>
</tbody>
</table>

What to Do Next

If TLS is enabled on your Microsoft Exchange Server, proceed to the “Configuring Cisco Unified MeetingPlace to Support TLS Encryption” section on page 5.

Otherwise, proceed to the “Configuring the Cisco Unified MeetingPlace Connection to the Microsoft Exchange Server” section on page 6.
Configuring Cisco Unified MeetingPlace to Support TLS Encryption

Perform this task if the Microsoft Exchange Server that you integrate with Cisco Unified MeetingPlace is configured to use Transport Layer Security (TLS).

Note
TLS is enabled by default on Exchange 2010. This procedure is required if you are deploying Cisco Unified MeetingPlace in an environment that uses Exchange 2010.

Before You Begin
- Complete the following prerequisite tasks. Refer to the documentation for your Microsoft Exchange Server.
  - Verify that TLS is enabled on the Microsoft Exchange Server.
  - Verify that the Microsoft Exchange Server can successfully receive e-mail from the Internet.
  - Make sure that IIS and SMTP on the Microsoft Exchange Server use the same certificate.
- Complete the “Creating a Cisco Unified MeetingPlace–Dedicated E-Mail Account and Mailbox on the Microsoft Exchange Server” section on page 4.

Procedure

Step 1
Export the TLS certificate from the Microsoft Exchange Server by following these steps:

a. From your Microsoft Windows system, go to the Microsoft IIS Manager.
b. Go to the entry called Web Site and highlight the entry called Default Web Site. Default Web Site is the generic name; it may have a different name on your system.
c. Right click the Default Web Site entry to display the Properties dialog box.
d. Click the Directory Security tab.
e. Click View Certificate.
f. Click the Details tab.
g. Click Copy to File. The system starts the certificate wizard.
h. Select No, do not export the private key and click Next.
i. Select DER encoded binary X.509 (.CER) and click Next.
j. Click Browse to choose a location to save the certificate. Enter a filename and click Save.

Step 2
Log in to the Cisco Unified MeetingPlace CLI as the root user.

Step 3
Copy the certificate to $MP_ROOT/filename.cer, substituting the filename from Step 1j.

Step 4
Move to the security directory by entering the following:

cd $MP_ROOT/jre/jre/lib/security

Step 5
Install the certificate by entering the following and substituting the filename from Step 1j:

./.bin/keytool -keystore cacerts -import -alias exchangeIIS -file $MP_ROOT/filename

Note
The default password for the JDK keytool is changeit.
Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace

Step 6
If the key length of the installed certificate is greater than 2048, then complete these steps:

b. Download the “Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6.”
c. Install this in the $MP_ROOT/jre/jre/lib/security directory.

Step 7
Restart the system by entering mpx_sys restart.

Step 8
Log in to the Administration Center.

Step 9
Click System Configuration > E-Mail Notifications > Exchange Server Configuration.

Step 10
Set the TLS enabled field to true.

---

Note
When you restart the Web Server, all manual changes made to the registry are lost.

What to Do Next
Proceed to the “Configuring the Cisco Unified MeetingPlace Connection to the Microsoft Exchange Server” section on page 6.

Related Topics
- How to Log in to the CLI in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Exchange Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Configuring the Cisco Unified MeetingPlace Connection to the Microsoft Exchange Server

Before You Begin
- Complete the “Creating a Cisco Unified MeetingPlace–Dedicated E-Mail Account and Mailbox on the Microsoft Exchange Server” section on page 4.
- If TLS is enabled on your Microsoft Exchange Server, complete the “Configuring Cisco Unified MeetingPlace to Support TLS Encryption” section on page 5.
- Obtain the following information about the Microsoft Exchange Server:
  - Hostname or IP address
  - Windows domain
  - Username and password for the e-mail account that you created in the “Creating a Cisco Unified MeetingPlace–Dedicated E-Mail Account and Mailbox on the Microsoft Exchange Server” section on page 4.

Restriction
If you are using Microsoft Exchange Server 2007 or 2010, the same machine must host both the Microsoft Exchange Hub Transport server and the Microsoft Exchange Client Access server. The hostname of this machine is what you enter in the Hostname field on the Exchange Server Configuration Page.
Procedure

Step 1 Log in to the Cisco Unified MeetingPlace Administration Center.
Step 2 Click System Configuration > E-Mail Notifications > Exchange Server Configuration.
Step 3 Configure the fields on the Exchange Server Configuration Page.
Step 4 Click Save.

Verifying
Click Test to verify the connection between Cisco Unified MeetingPlace and Microsoft Exchange Server.

What to Do Next
- If you upgraded your Cisco Unified MeetingPlace system from an earlier release, then run the Cisco Unified MeetingPlace–Microsoft Exchange migration process at /opt/cisco/meetingplace/migrationtools/current/notifications/migrateExchangeForICAL.sh.

Note
The migration process may take a long time if many meetings need to be migrated. To speed up the migration process, purge old meetings from the Cisco Unified MeetingPlace–dedicated mailbox, and empty the Deleted Items folder. We recommend that the mailbox have fewer than 1360 appointment items or 32 KB of appointment data before you run the migration process.

- To enable users to receive meeting notifications as calendar appointments in Microsoft Outlook, specify a Microsoft Exchange option in the E-mail type and format user group or user profile fields.

See “Configuring User Preferences for E-Mail Notifications” in the Configuring E-Mail Notifications for Cisco Unified MeetingPlace module.

- To customize the e-mail notifications, proceed to the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module.

Related Topics
- Exchange Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager

Release 7.1
Revised: April 3, 2011 8:30 pm

Note
The names for Cisco Unified CallManager Release 4.3, Release 5.1, and Release 6.0 have been changed to Cisco Unified Communications Manager Release 4.3, Release 5.1, and Release 6.0.
The names of Cisco Unified CallManager Release 4.0, Release 4.1, Release 4.2, and Release 5.0 have not changed and remain the same.

We recommend that you use Cisco Unified Communications Manager to provide call-control and other services for Cisco Unified MeetingPlace and your IP telephony network.

<table>
<thead>
<tr>
<th>Integration Options</th>
<th>Where to Find Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Call control</td>
<td>Configuring Call Control for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Directory service</td>
<td>Configuring Cisco Unified MeetingPlace Directory Service module</td>
</tr>
<tr>
<td>Cisco Unified MeetingPlace</td>
<td>Integrating Cisco Unified MeetingPlace With Cisco Unified IP</td>
</tr>
<tr>
<td>PhoneView</td>
<td>Phone module</td>
</tr>
</tbody>
</table>

Note
Cisco Unified MeetingPlace is not compatible with the call preservation feature of Cisco Unified Communications Manager (CUCM). The call preservation feature allows a call to stay up after the signaling path is lost, for example because of a CUCM node restart. When a call enters that state, Cisco Unified MeetingPlace drops the call at the next session refresh. In the meantime, the preserved call can prevent the user from signing in to Cisco Unified MeetingPlace over the phone or dialing out from the end-user web interface.

This module also describes certain Cisco Unified Communications Manager settings that can affect Cisco Unified MeetingPlace:

1. The session refresh timer is set to 15 minutes by default. This parameter is configurable from Cisco Unified Communications Manager.
Configuring a SIP Trunk Security Profile in Cisco Unified Communications Manager for Cisco Unified MeetingPlace

We recommend that you do the following:

- Create a SIP trunk security profile in Cisco Unified Communications Manager specifically for Cisco Unified MeetingPlace.
- Apply this SIP trunk security profile to SIP trunks to Cisco Unified MeetingPlace systems.

Before You Begin

- This task applies only in Cisco Unified Communications Manager environments.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager online help for step-by-step instructions for your specific release.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Go to <a href="http://ccm-server/">http://ccm-server/</a>, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Sign in with your Cisco Unified Communications Manager administrator username and password.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click System &gt; Security Profile &gt; SIP Trunk Security Profile.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Click Add New.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Configure fields described in Table 1.</td>
</tr>
</tbody>
</table>

Table 1 Fields for SIP Trunk Security Profile Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name, such as SIP Trunk Security Profile for Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td>Device Security Mode</td>
<td>Select Non Secure.</td>
</tr>
<tr>
<td>Incoming Transport Type</td>
<td>Keep the default value of TCP+UDP. If other values are available for this field, then you may instead select the value that matches the Transport setting for this Cisco Unified Communications Manager node on the SIP Configuration Page.</td>
</tr>
<tr>
<td>Outgoing Transport Type</td>
<td>We recommend that you select UDP.</td>
</tr>
<tr>
<td>Enable Digest Authentication</td>
<td>Uncheck this check box.</td>
</tr>
</tbody>
</table>
Table 1  Fields for SIP Trunk Security Profile Configuration (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable Application Level</td>
<td>Uncheck this check box.</td>
</tr>
<tr>
<td>Authorization</td>
<td></td>
</tr>
<tr>
<td>Incoming Port</td>
<td>Make sure this value matches the Port setting for</td>
</tr>
<tr>
<td></td>
<td>thisCisco Unified Communications Manager node on the</td>
</tr>
<tr>
<td></td>
<td>SIPConfiguration Page</td>
</tr>
<tr>
<td></td>
<td>Default: 5060</td>
</tr>
</tbody>
</table>

Step 6  Click Save.

Related Topics
- Configuring Call Control for Cisco Unified MeetingPlace module
- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module

Configuring the Maximum Call Duration in Cisco Unified Communications Manager

The maximum length of a meeting depends on three values, the lowest of which is enforced:
- Maximum meeting length (minutes) field on the Meeting Configuration Page.
- Maximum meeting length (minutes) field in the user profile of the meeting owner.
- Maximum Call Duration Timer service parameter in Cisco Unified Communications Manager.

This task describes how to view and (if necessary) configure the service parameter in Cisco Unified Communications Manager.

Before You Begin
- This task applies only in Cisco Unified Communications Manager environments.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager online help for step-by-step instructions for your specific release.

Procedure

Step 1  Go to http://ccm-server/, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
Step 2  Sign in with your Cisco Unified Communications Manager administrator username and password.
Step 3  Click System > Service Parameters.
Step 4  Select the server.
Step 5  Select the Cisco CallManager service.

Step 6  Find the Maximum Call Duration Timer field.

Step 7  Modify this field only if you require meetings to last longer than the previously configured value.

- A value of 0 disables the timer, which is recommended for continuous meetings where individual calls, as opposed to the meeting as a whole, need to continue indefinitely. Note that disabling this timer might result in some calls failing to ever terminate in cases where some call signaling failure occurs.

- For descriptions of this or any other field on the page, click the field name.

Step 8  Click Save if you modified any parameters.

Related Topics
- Configuring Meetings for Cisco Unified MeetingPlace module
- Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module

Configuring the Maximum Video Call Bandwidth in Cisco Unified Communications Manager

In Cisco Unified MeetingPlace, video calls cannot exceed the lowest maximum bandwidth determined by the following settings:

- Global video mode field on the Meeting Configuration Page.
- Video Call Bandwidth region parameter in Cisco Unified Communications Manager.
- Bandwidth capabilities and configurations of the video endpoints.

This task describes how to view and (if necessary) modify the Video Call Bandwidth in Cisco Unified Communications Manager.

Before You Begin

- This task applies only in Cisco Unified Communications Manager environments.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager online help for step-by-step instructions for your specific release.

Procedure

Step 1  Go to http://ccm-server/, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2  Sign in with your Cisco Unified Communications Manager administrator username and password.

Step 3  Click Device > Trunk.

Step 4  Click Find with or without any search parameters to find the trunks that carry Cisco Unified MeetingPlace calls, for example:

- SIP trunk to Cisco Unified MeetingPlace
• Inter-cluster trunks between Cisco Unified Communications Manager 4.x or 5.x and Cisco Unified Communications Manager 6.1 or a later release.

**Step 5**
Write down the name of each Device Pool that these trunks use.

**Step 6**
Click System > Device Pool.

**Step 7**
Click Find with or without any search parameters to find a device pool that carries Cisco Unified MeetingPlace calls.

**Step 8**
Click the Region for a device pool to go to the Region Configuration page.

**Step 9**
In the Region Relationships area, see the Video Call Bandwidth for each region and audio codec combination.

**Step 10**
(Optional) Use the Modify Relationship to other Regions area to change the Video Call Bandwidth for a particular Region and Audio Codec combination.

**Step 11**
Click Save.

**Step 12**
Repeat Step 6 to Step 11 for each device pool used by the trunks that carry Cisco Unified MeetingPlace calls.

---

**Related Topics**

- Configuring Meetings for Cisco Unified MeetingPlace module

---

**Configuring Cisco Unified Communications Manager: Music On Hold**

In Cisco Unified Communications Manager, you can configure music on hold so that callers hear music when one of your users places a call on hold. This can be disruptive if a user places a conference call on hold. The music, and possible announcements, can prevent other callers on the conference call from hearing each other until the user who placed the call on hold returns to the call.

You can disable music on hold for conference calls by doing the following:

- Creating a Media Resource Group in Cisco Unified Communications Manager for all music on hold resources.
- Adding all phones for which you want to enable music on hold to the Media Resource Group List that contains the music on hold Media Resource Group.
- Making sure that the music on hold Media Resource Group List is not assigned to the SIP trunk that connects Cisco Unified Communications Manager to Cisco Unified MeetingPlace.

**Note**
This procedure is not required if you are using Cisco Unified Communications Manager Release 7.x or later since these systems use an isFocus flag to suppress music on hold.
Restrictions

- This procedure disables music on hold for callers within the same Cisco Unified Communications Manager cluster, but does not disable music on hold for outside callers, including endpoints that are registered to a different Cisco Unified Communications Manager cluster than Cisco Unified MeetingPlace.

- This procedure also disables music on hold for calls between endpoints that are registered to different Cisco Unified Communications Manager servers.

  For example, suppose that your Cisco Unified MeetingPlace call-control deployment includes a Cisco Unified Communications Manager 6.x server and a Cisco Unified Communications Manager 4.x server that are connected to each other by inter-cluster trunks (ICTs). Because these ICTs will not have music on hold resources configured through the Media Resource Group List, then music on hold will be disabled on all calls that pass through these ICTs.

- This procedure shows how to create a new Media Resource Group for music on hold resources. If you instead want to modify existing Media Resource Groups to complete this task, then modify the steps accordingly.

- You perform this task in the Cisco Unified Communications Manager Administration pages.

  Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager online help for step-by-step instructions for your specific release.

Procedure

Step 1  Go to http://ccm-server/ccmadmin/main.asp, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.

Step 2  Sign in with your Cisco Unified Communications Manager administrator username and password.

Step 3  Click Media Resources > Media Resource Group.

Step 4  Click Add New.

Step 5  Configure the fields described in Table 2.

Table 2 Fields for Adding a Media Resource Group

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name, such as MOHGroup.</td>
</tr>
<tr>
<td>Selected Media Resources</td>
<td>Select all of the music on hold servers in the Available Media Resources list, and click the down arrow.</td>
</tr>
</tbody>
</table>

Step 6  Click Save.

Step 7  Click Media Resources > Media Resource Group List.

Step 8  Click Add New.

Step 9  Configure the fields described in Table 3.

Table 3 Fields for Adding a Media Resource Group List

<table>
<thead>
<tr>
<th>Field</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Enter a name, such as MOHList.</td>
</tr>
<tr>
<td>Selected Media Resource Groups</td>
<td>Select the music on hold Media Resource Group (for example, MOHGroup), and click the down arrow.</td>
</tr>
</tbody>
</table>
Step 10  Click Save.

Step 11  Configure all phones for which you want to support music on hold to use the Media Resource Group List (for example, MOHList). You can use the Bulk Administration Tool (BAT) to reconfigure many phones at one time.

Note  Make sure that you do not assign a music on hold Media Resource Group List to the trunk that leads to Cisco Unified MeetingPlace.

Step 12  Repeat this procedure on each Cisco Unified Communications Manager to which Cisco Unified MeetingPlace–supported endpoints are registered.

Related Topics
- Configuring Call Control for Cisco Unified MeetingPlace module
Integrating Cisco Unified MeetingPlace with Cisco Unified Personal Communicator

Release 7.1
Revised: April 3, 2011 8:30 pm

When Cisco Unified MeetingPlace is integrated with Cisco Unified Personal Communicator, users who are in a Cisco Unified Personal Communicator conversation can quickly share data through a private, reservationless, and web-only meeting that is provided by Cisco Unified MeetingPlace.

- About Web-Only Meetings that are Initiated from Cisco Unified Personal Communicator, page 1
- Integrating with Cisco Unified Personal Communicator, page 3
- Additional References for Integrating with Cisco Unified Personal Communicator, page 3

About Web-Only Meetings that are Initiated from Cisco Unified Personal Communicator

- Web-Only Meetings that are Initiated from Cisco Unified Personal Communicator, page 1
- Participant Privileges in Web-Only Meetings that are Initiated from Cisco Unified Personal Communicator, page 2

Web-Only Meetings that are Initiated from Cisco Unified Personal Communicator

The following information applies to Cisco Unified MeetingPlace web-only meetings that are initiated from a Cisco Unified Personal Communicator conversation:

- The person who initiates the Cisco Unified MeetingPlace web-only meeting must have an active user profile in the Cisco Unified MeetingPlace database.
- Meeting passwords and e-mail notifications are not supported for web-only meetings.
- The web-only meeting can only be accessed in the following ways:
  - (For users who are currently using Cisco Unified Personal Communicator) Cisco Unified Personal Communicator automatically opens a browser for all conversation participants when anyone initiates a web-only meeting.
- (For users who are not using Cisco Unified Personal Communicator) The person who initiates the web-only meeting must provide the URL to anyone who is not currently using Cisco Unified Personal Communicator.

These web-only meetings cannot be accessed by any other means, such as through the Find or Attend pages in the Cisco Unified MeetingPlace end-user web interface or through a Cisco Unified IP Phone screen when subscribed to the Cisco Unified MeetingPlace PhoneView.

- The meeting subject that appears in reports is `userid_WEBONLY_MEETING`, where `userid` is the User ID in the Cisco Unified MeetingPlace user profile of the meeting initiator.

**Related Topics**
- Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module

**Participant Privileges in Web-Only Meetings that are Initiated from Cisco Unified Personal Communicator**

- All participants are treated as guest users with presenter privileges in the web meeting room. Therefore, all participants can share data, and only the meeting initiator must have a Cisco Unified MeetingPlace user profile.
- Only one pod, the share pod, is available in the web meeting room. The participant list, chat, and note pods that appear in other types of Cisco Unified MeetingPlace web meeting rooms are not available for web-only meetings.
- Except for the ability to share data, meeting participants do not have in-session controls, such as the ability to lock, record, or end the meeting from within the web meeting room.
- User profile settings do not affect the behavior of these web-only meetings. For example:
  - Even if the **Meeting password required** field in the user profile is set to Yes, no passwords are required to attend web meetings that are initiated from Cisco Unified Personal Communicator.
  - Even though Cisco Unified MeetingPlace treats the meetings that are initiated from Cisco Unified Personal Communicator as private reservationless web meetings, the **Use reservationless** field may be set to No in the Cisco Unified MeetingPlace user profile of the meeting initiator.
  - Even if the user profile **Host web meetings with** field is set to Participant list only, the user may still share data in web meetings that are initiated from Cisco Unified Personal Communicator.
Integrating with Cisco Unified Personal Communicator

Complete these tasks to enable web meetings to be initiated from Cisco Unified Personal Communicator conversations.

Procedure

<table>
<thead>
<tr>
<th>High-Level Task</th>
<th>Where to Find Instructions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong> Install the appropriate licenses on the Cisco Unified MeetingPlace Application Server. For example, install webconf and maxweb licenses that provide enough web ports for both the full web meetings that are initiated from Cisco Unified MeetingPlace and the web-only meetings that are initiated from Cisco Unified Personal Communicator.</td>
<td>Installing and Managing Licenses for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td><strong>Step 2</strong> Enable SSL on the Cisco Unified MeetingPlace Application Server.</td>
<td>Configuring SSL for the Cisco Unified MeetingPlace Application Server module</td>
</tr>
<tr>
<td><strong>Step 3</strong> Make sure that a Cisco Unified MeetingPlace user profile exists for each Cisco Unified Personal Communicator user who might initiate web-only meetings from Cisco Unified Personal Communicator. Typically, both Cisco Unified MeetingPlace and Cisco Unified Personal Communicator are integrated with Cisco Unified Communications Manager, which handles the user authentication.</td>
<td>Configuring Cisco Unified MeetingPlace Directory Service module</td>
</tr>
</tbody>
</table>

Additional References for Integrating with Cisco Unified Personal Communicator

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Software compatibility</td>
<td></td>
</tr>
<tr>
<td>• Supported features</td>
<td></td>
</tr>
</tbody>
</table>
Integrating Cisco Unified MeetingPlace With Cisco Unified IP Phone

Release 7.1
Revised: April 3, 2011 8:30 pm

You can integrate Cisco Unified MeetingPlace with Cisco Unified IP phones so that users can see and manage their meetings on their phones through an application called Cisco Unified MeetingPlace PhoneView. This module describes how to configure the PhoneView service.

- About Cisco Unified MeetingPlace PhoneView, page 1
- How to Configure Cisco Unified MeetingPlace PhoneView, page 3
- Finding an IP Phone Service in Cisco Unified Communications Manager, page 8
- Deleting an IP Phone Service, page 9

Note
Cisco Unified MeetingPlace PhoneView is a Cisco Unified Communications Manager feature. However, this module does not describe how to install or configure Cisco Unified Communications Manager (formerly known as Cisco Unified CallManager) for your network. For additional information, see the list of documents in the “Additional References for Configuring Cisco Unified MeetingPlace PhoneView” section on page 3.

For a list of supported phone models, see the System Requirements and Compatibility Matrix for Cisco Unified MeetingPlace.

About Cisco Unified MeetingPlace PhoneView

Cisco Unified MeetingPlace PhoneView offers users a convenient way to join meetings, start reservationless meetings, view a list of upcoming meetings, and view meeting details. After joining a meeting, a user can perform in-meeting operations such as locking the meeting, recording the meeting, viewing a list of participants, and muting or ejecting participants.
Cisco Unified MeetingPlace PhoneView is available only to Cisco Unified IP Phones that are registered to Cisco Unified Communications Manager. Cisco Unified Communications Manager Express does not support Cisco Unified MeetingPlace PhoneView.

- Cisco Unified MeetingPlace PhoneView and Security, page 2
- Username and Password Requirements for Cisco Unified MeetingPlace PhoneView, page 2
- Language Requirements for Cisco Unified MeetingPlace PhoneView, page 3
- Additional References for Configuring Cisco Unified MeetingPlace PhoneView, page 3

Cisco Unified MeetingPlace PhoneView and Security

Using Cisco Unified MeetingPlace PhoneView may affect the way you secure your Cisco Unified MeetingPlace system or network:

- Cisco Unified IP Phones do not support SSL.
- Once a Cisco Unified IP Phone is subscribed to PhoneView, anyone can use that Cisco Unified IP Phone screen to view the meeting details and invitees of published meetings. To join a meeting through PhoneView, however, you are always prompted for your phone profile password (numeric PIN).
- Each time a Cisco Unified IP Phone accesses PhoneView, the following items are sent as clear text over the network:
  - Username
  - PIN or password
  - Phone number of the Cisco Unified IP Phone

Related Topics

- Username and Password Requirements for Cisco Unified MeetingPlace PhoneView, page 2
- About Cisco Unified MeetingPlace PhoneView, page 1

Username and Password Requirements for Cisco Unified MeetingPlace PhoneView

The username and password required to subscribe to Cisco Unified MeetingPlace PhoneView depends on how the user is authenticated when logging in to Cisco Unified MeetingPlace from a workstation.

<table>
<thead>
<tr>
<th>Cisco Unified MeetingPlace Authentication Method</th>
<th>Required Username for name Parameter</th>
<th>Required Password for wfpassword Parameter</th>
</tr>
</thead>
<tbody>
<tr>
<td>Locally by the Cisco Unified MeetingPlace database</td>
<td>User ID in Cisco Unified MeetingPlace user profile</td>
<td>Profile password in Cisco Unified MeetingPlace user profile</td>
</tr>
<tr>
<td>Externally by Cisco Unified Communications Manager</td>
<td>Username in Cisco Unified Communications Manager</td>
<td>Numeric PIN in Cisco Unified Communications Manager</td>
</tr>
<tr>
<td>Externally by Active Directory, Netscape Directory, or iPlanet Directory</td>
<td>Username in external directory</td>
<td>Numeric PIN in external directory</td>
</tr>
</tbody>
</table>
Related Topics

- About Cisco Unified MeetingPlace PhoneView, page 1

Language Requirements for Cisco Unified MeetingPlace PhoneView

The requirements in this section apply when Cisco Unified MeetingPlace, Cisco Unified Communications Manager, or the Cisco Unified IP Phones are configured for multiple *locales*, which are language versions for specific regions.

- For each language enabled on Cisco Unified MeetingPlace, the matching locale must be installed on Cisco Unified Communications Manager. See the Cisco IP Telephony Locale Installer documentation.

- For each Cisco Unified IP Phone subscribed to Cisco Unified MeetingPlace PhoneView, the user locale specified in Cisco Unified Communications Manager must match the language specified in the Cisco Unified MeetingPlace user profile.

Related Topics

- About Cisco Unified MeetingPlace PhoneView, page 1
- Additional References for Configuring Cisco Unified MeetingPlace PhoneView, page 3

Additional References for Configuring Cisco Unified MeetingPlace PhoneView

- Cisco Unified Communications Manager documentation
  

- Cisco Unified IP Phone end-user documentation
  

- *Quick Start Guide: Using Cisco Unified MeetingPlace Release 7.1 with your Cisco Unified IP Phone*
  

Related Topics

- About Cisco Unified MeetingPlace PhoneView, page 1

How to Configure Cisco Unified MeetingPlace PhoneView

This topic describes how to configure Cisco Unified Communications Manager to enable users to subscribe to and access Cisco Unified MeetingPlace PhoneView. Complete the following procedures in the order shown.

- Adding Cisco Unified MeetingPlace to the List of IP Phone Services on the Cisco Unified Communications Manager, page 4
- Defining Cisco Unified MeetingPlace Service Parameters, page 6
Adding Cisco Unified MeetingPlace to the List of IP Phone Services on the Cisco Unified Communications Manager

Before You Begin

- Read the following sections:
  - Cisco Unified MeetingPlace PhoneView and Security, page 2
  - Username and Password Requirements for Cisco Unified MeetingPlace PhoneView, page 2
  - Language Requirements for Cisco Unified MeetingPlace PhoneView, page 3
- Configure Cisco Unified Communications Manager as the call-control device for Cisco Unified MeetingPlace.

See the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module for instructions.
- For the services to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to this server.

Restrictions

- Cisco Unified IP Phones do not support SSL.
- Cisco Unified MeetingPlace PhoneView is available only to Cisco Unified IP Phones that are registered to Cisco Unified Communications Manager.
- This task is performed in the Cisco Unified Communications Manager pages. Because the pages and menus vary by Cisco Unified Communications Manager release, you may need to see the Cisco Unified Communications Manager online help for more accurate step-by-step instructions than those provided in this procedure. The following procedure refers to Cisco Unified Communications Manager Release 6.1.

Note

The names for Cisco Unified Communications Manager Release 4.3, Release 5.1, and Release 6.0 have been changed to Cisco Unified Communications Manager Release 4.3, Release 5.1, and Release 6.0. The names of Cisco Unified Communications Manager Release 4.0, Release 4.1, Release 4.2, and Release 5.0 have not changed and remain the same.

Procedure

**Step 1** Go to http://ccm-server/ccmadmin/main.asp, where ccm-server is the fully qualified domain name or IP address of the Cisco Unified Communications Manager server.

**Step 2** Log in with your Cisco Unified Communications Manager administrator username and password.

**Step 3** Click Device > Device Settings > Phone Services.

**Step 4** Click Add New in the top left corner.
Step 5  Configure the fields in the Service Information area.

<table>
<thead>
<tr>
<th>For This Field</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Name</td>
<td>Enter a name, for example: <strong>Cisco Unified MeetingPlace</strong>&lt;br&gt;This is the name of the service that appears on the Cisco Unified IP Phone and on the menu of available services on user subscription pages. If you have more than one Cisco Unified MeetingPlace Web Server, name the services appropriately so that users can distinguish among them.</td>
</tr>
<tr>
<td>Service Description</td>
<td>Enter a brief description of what the service provides, for example: <strong>Integrated rich-media conferencing</strong></td>
</tr>
<tr>
<td>ASCII Service Name</td>
<td>Enter a name, for example: <strong>Cisco Unified MeetingPlace</strong>&lt;br&gt;You may also enter a brief ASCII version such as CUMP.</td>
</tr>
</tbody>
</table>
| Service URL          | Enter the URL in the following format, where application-server is the hostname or IP address of the Cisco Unified MeetingPlace Application Server:<br>`http://application-server/ipphone/MPAPI/ipphone/login?serverhost=application-server`<br>The URL identifies where the Cisco Unified MeetingPlace PhoneView application is located.<br><strong>Note</strong> The URL is case sensitive. Requirements:  
  * For this service to be available, the phones in the Cisco Unified Communications Manager cluster must have network connectivity to the Application Server.  
  * In an **Application Server Failover** deployment, use the shared hostname or IP address that you configured on the eth0 interface of both Application Servers.  
  * If you use the hostname (instead of the IP address) in the URL, then configure your DNS server to resolve the Application Server hostname from the Cisco Unified IP Phone.  

Step 6  Click **Save**.

Step 7  (Optional) Click **Add New** to add another Cisco Unified MeetingPlace IP Phone service and repeat Step 5 and Step 6.

What to Do Next  
Proceed to the “Defining Cisco Unified MeetingPlace Service Parameters” section on page 6.
Defining Cisco Unified MeetingPlace Service Parameters

This procedure enables users to be authenticated when they subscribe to the Cisco Unified MeetingPlace service on the Cisco Unified IP Phone User Options (ccmuser) website. It also allows users to access the Cisco Unified MeetingPlace service from their Cisco Unified IP Phones.

Before you Begin

- Complete the “Adding Cisco Unified MeetingPlace to the List of IP Phone Services on the Cisco Unified Communications Manager” section on page 4.
- This procedure assumes that you are still logged in to the Cisco Unified Communications Manager server and on the IP Phone Services Configuration page.

Procedure

**Step 1**
Locate the Service Parameter Information area.

**Step 2**
Configure the ipphone parameter.

  a. Click **New**.

  b. Configure the following fields in the Configure Cisco IP Phone Service Parameter window.

<table>
<thead>
<tr>
<th>For This Field</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Name</td>
<td>Enter <strong>ipphone</strong>.</td>
</tr>
<tr>
<td></td>
<td>• This is the exact query string used to build the subscription URL.</td>
</tr>
<tr>
<td></td>
<td>• This field is case-sensitive.</td>
</tr>
<tr>
<td>Parameter Display Name</td>
<td>Enter <strong>Cisco Unified IP Phone Number</strong>.</td>
</tr>
<tr>
<td></td>
<td>This is the descriptive parameter name displayed to the user on the</td>
</tr>
<tr>
<td></td>
<td>Cisco IP Phone Users Options [ccmuser] website.</td>
</tr>
<tr>
<td>Default Value</td>
<td>Leave blank.</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>Enter <strong>The Cisco Unified IP Phone number that MeetingPlace will use to call you</strong>.</td>
</tr>
</tbody>
</table>

  c. Check **Parameter is Required**.

  d. Click **Save And Close**.

**Step 3**
Configure the name parameter.

  a. Click **New** in the Service Parameter Information area.

  b. Configure the following fields in the Configure Cisco IP Phone Service Parameter window.
c. Check Parameter is Required.

d. Click Save And Close.

**Step 4** Configure the wfpassword parameter.

a. Click New in the Service Parameter Information area.

b. Configure the following fields in the Configure Cisco IP Phone Service Parameter window.

<table>
<thead>
<tr>
<th>For This Field</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Name</td>
<td>Enter <strong>name</strong>.</td>
</tr>
<tr>
<td></td>
<td>* This is the exact query string used to build the subscription URL.</td>
</tr>
<tr>
<td></td>
<td>* This field is case-sensitive.</td>
</tr>
<tr>
<td>Parameter Display Name</td>
<td>Enter <strong>User Name</strong>.</td>
</tr>
<tr>
<td></td>
<td>This is the descriptive parameter name displayed to the user on the Cisco IP Phone Users Options [ccmuser] website.</td>
</tr>
<tr>
<td>Parameter Default Value</td>
<td>Enter <strong>guest</strong>.</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>Enter a description that will help users to enter the correct username when they subscribe to Cisco Unified MeetingPlace PhoneView.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The username required depends on how the user is authenticated when logging into Cisco Unified MeetingPlace from a workstation.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>For This Field</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter Name</td>
<td>Enter <strong>wfpassword</strong>.</td>
</tr>
<tr>
<td></td>
<td>* This is the exact query string used to build the subscription URL.</td>
</tr>
<tr>
<td></td>
<td>* This field is case-sensitive.</td>
</tr>
<tr>
<td>Parameter Display Name</td>
<td>Enter <strong>User PIN</strong>.</td>
</tr>
<tr>
<td></td>
<td>This is the descriptive parameter name displayed to the user on the Cisco IP Phone Users Options [ccmuser] website.</td>
</tr>
<tr>
<td>Default Value</td>
<td>Leave blank.</td>
</tr>
<tr>
<td>Parameter Description</td>
<td>Enter a description that will help users to enter the correct password when they subscribe to Cisco Unified MeetingPlace PhoneView.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> The password required depends on how the user is authenticated when logging into Cisco Unified MeetingPlace from a workstation.</td>
</tr>
</tbody>
</table>
c. Check Parameter is Required.
d. Check Parameter is a Password (mask contents) to mask the password on the screen as the user enters it.
e. Click Save And Close.

Step 5
Take one of the following actions to apply the Cisco Unified MeetingPlace service and parameter changes:

- If the service was modified after subscriptions existed, click Update Subscriptions to rebuild all user subscriptions. You must update subscriptions if you changed the service URL, removed a phone service parameter, or changed the name for a phone service parameter.
- If the service is new and you do not need to rebuild user subscriptions, click Update.

Related Topics
- How to Configure Cisco Unified MeetingPlace PhoneView, page 3
- Username and Password Requirements for Cisco Unified MeetingPlace PhoneView, page 2

What to Do Next
Subscribe Cisco Unified IP Phones to Cisco Unified MeetingPlace PhoneView by taking one or both of the following actions:

- Subscribe individual Cisco Unified IP Phones to Cisco Unified MeetingPlace PhoneView through Cisco Unified Communications Manager. See the Cisco Unified Communications Manager Administration Guide for instructions.
- Notify end users that they can subscribe their own Cisco Unified IP Phones to Cisco Unified MeetingPlace PhoneView. See the User Guide for Cisco Unified MeetingPlace Release 7.1.

Finding an IP Phone Service in Cisco Unified Communications Manager

Procedure

Step 1 Go to http://ccm-server/ccmadmin/main.asp, where ccm-server is the fully qualified domain name or IP address of the Cisco Unified Communications Manager server.
Step 2 Log in with your Cisco Unified Communications Manager administrator username and password.
Step 3 Click Device > Device Settings > Phone Services.
Step 4 Enter a search parameter then click Find.
Step 5 Locate your application in the search results area.
Step 6 Click the name of the IP Phone Service that you want to see.
Deleting an IP Phone Service

Procedure

Step 1 Find the IP Phone Service that you want to delete.
Step 2 Check the checkbox next to the phone service name.
Step 3 Click Delete Selected.

Related Topics

- Finding an IP Phone Service in Cisco Unified Communications Manager, page 8
Part

Security

- Securing the Cisco Unified MeetingPlace System
- Configuring Cisco Unified MeetingPlace Web Conferencing Security Features
- Configuring SSL for the Cisco Unified MeetingPlace Application Server
- User Authentication for Cisco Unified MeetingPlace
- Changing System Administrator Passwords for Cisco Unified MeetingPlace
Securing the Cisco Unified MeetingPlace System

Release 7.1
Revised: April 3, 2011 8:30 pm

- Overview of Security Tasks, page 1
- Using Cisco Security Agent (CSA) on the Application Server, page 3
- Upgrading Cisco Security Agent (CSA) on the Application Server, page 4
- Limiting the Number of Failed User Login Attempts, page 5
- Configuring Requirements for User Passwords, page 6
- Configuring Requirements for Meeting Passwords, page 7
- Restricting Access to Scheduled Meetings, page 8
- Restricting Access to Recordings and Attachments, page 8
- Restricting the Use of Vanity Meeting IDs, page 9
- Restricting Dial-Out Privileges for Guest Users, page 9
- Restricting Dial-Out Privileges for Profiled Users, page 10
- Limiting the Number of Attempted Dial-Out Calls From Voice Meetings, page 11

Overview of Security Tasks

While your company may already have guidelines for securing its computer systems and preventing toll fraud, we also recommend that you perform the tasks listed in Table 1.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Where to Find Information</th>
</tr>
</thead>
</table>
| Restrict dial-out privileges to specific users. | - Restricting Dial-Out Privileges for Guest Users, page 9  
- Restricting Dial-Out Privileges for Profiled Users, page 10 |
Monitor dial-out usage.

We recommend that you configure Cisco Unified Communications Manager with a Calling Search Space that does the following:

- Allows dial-out calls to meeting participants and the help desk Attendant.
- Prevents toll fraud by blocking unwanted dial-out calls, for example, to international or premium-rate telephone numbers.

System Security

Secure the physical location of the servers. Keep the servers in areas protected by lock or card-key systems to prevent unauthorized access to the systems.

Use the Cisco Security Agent on the Application Server.

Use the Secure Socket Layer (SSL) on the Application Server.

Keep the database current. Deactivate or delete the user profiles of employees who leave the company.

Change the default passwords for the admin profile.

On the router that connects Cisco Unified MeetingPlace to the external network, limit external SSH access to Cisco Unified MeetingPlace to the following:

- Safe IP address in your company or organization
- Third-party support personnel
- Cisco IP addresses:
  - 128.107.0.0/16
  - 198.133.219.0/24

Even if you believe that the SSH login credentials are safe, denial of service attacks may still be launched against your system.

### Table 1  Security Recommendations for Cisco Unified MeetingPlace (continued)

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Where to Find Information</th>
</tr>
</thead>
</table>
| Monitor dial-out usage. | - Running Capacity Management Reports, page 11  
- Exporting Information about Dial-Out Calls, page 12  
- Exporting Meetings, page 6 |
| We recommend that you configure Cisco Unified Communications Manager with a Calling Search Space that does the following: | - Administration Guide for your release of Cisco Unified Communications Manager at http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html |
| Secure the physical location of the servers. Keep the servers in areas protected by lock or card-key systems to prevent unauthorized access to the systems. | --- |
| Use the Cisco Security Agent on the Application Server. | - Using Cisco Security Agent (CSA) on the Application Server, page 3  
- Upgrading Cisco Security Agent (CSA) on the Application Server, page 4 |
| Use the Secure Socket Layer (SSL) on the Application Server. | - Configuring SSL for the Cisco Unified MeetingPlace Application Server module |
| Keep the database current. Deactivate or delete the user profiles of employees who leave the company. | - Locking or Deactivating a User Profile in the Changing the User Status in Cisco Unified MeetingPlace User Profiles module  
- Deleting a User Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module |
| Change the default passwords for the admin profile. | - Changing the Passwords for the admin Profile in the Changing System Administrator Passwords for Cisco Unified MeetingPlace module |
| On the router that connects Cisco Unified MeetingPlace to the external network, limit external SSH access to Cisco Unified MeetingPlace to the following: | - Documentation for your specific router and software release |
| Safe IP address in your company or organization  
Third-party support personnel  
Cisco IP addresses:  
- 128.107.0.0/16  
- 198.133.219.0/24 |
Using Cisco Security Agent (CSA) on the Application Server

Table 1  Security Recommendations for Cisco Unified MeetingPlace (continued)

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Where to Find Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete as many of these tasks as are appropriate for your user base.</td>
<td>• Configuring Requirements for User Passwords, page 6</td>
</tr>
<tr>
<td></td>
<td>• Limiting the Number of Failed User Login Attempts, page 5</td>
</tr>
<tr>
<td></td>
<td>• Configuring Requirements for Meeting Passwords, page 7</td>
</tr>
<tr>
<td></td>
<td>• Restricting Access to Scheduled Meetings, page 8</td>
</tr>
<tr>
<td></td>
<td>• Restricting Access to Recordings and Attachments, page 8</td>
</tr>
<tr>
<td></td>
<td>• Restricting the Use of Vanity Meeting IDs, page 9</td>
</tr>
<tr>
<td>Web Server Security</td>
<td>• Installing the Cisco Security Agent in the How to Install the Cisco Unified MeetingPlace Web Conferencing Server module of the Installation, Upgrade, and Migration Guide for Cisco Unified MeetingPlace</td>
</tr>
<tr>
<td>Use the Cisco Security Agent on the Web Servers, especially those in the DMZ.</td>
<td>• System Requirements and Compatibility Matrix for Cisco Unified MeetingPlace</td>
</tr>
<tr>
<td>Use McAfee VirusScan Enterprise on the Web Servers, especially those in the DMZ.</td>
<td>• Documentation provided by McAfee</td>
</tr>
<tr>
<td>Enable SSL on the Web Servers.</td>
<td>• How to Configure Secure Sockets Layer in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module</td>
</tr>
</tbody>
</table>

Using Cisco Security Agent (CSA) on the Application Server

The Cisco Security Agent (CSA) is an application that provides system and data security and allows you to monitor the activities on your system. The CSA is automatically installed on the Application Server with Cisco Unified MeetingPlace and requires no configuration. The red flag at the bottom-right corner of the screen indicates that CSA is running and active on your system.

The CSA consists of a set of rules that govern which users and applications can alter or query critical file systems. It also provides security on ports to minimize unauthorized system logins for malicious purposes. The CSA logs violations of any of the security rules. You may peruse the log periodically to determine what attempted activities were blocked.

Restrictions

Because the CSA application that is included with Cisco Unified MeetingPlace is a standalone version:

• You cannot use the CSA Management Console.

• If a newer version of CSA comes out, you must manually upgrade CSA on the Application Server. See the “Upgrading Cisco Security Agent (CSA) on the Application Server” section on page 4.

Procedure

Step 1  Log in to the console.

Step 2  Right-click the red CSA flag in the bottom right.
Securing the Cisco Unified MeetingPlace System

Upgrading Cisco Security Agent (CSA) on the Application Server

**Before You Begin**
Read the *System Requirements for Cisco Unified MeetingPlace Release 7.1*.

**Procedure**

**Step 1** Go to Cisco.com and find the Cisco Security Agent upgrade file.
The CSA is distributed as an RPM file on a CD or as a file download. The filename will be similar to CSA_5.1.0.95.

**Step 2** Save the file to a convenient location.

**Step 3** From the console, go to the Cisco Unified MeetingPlace operating system login page.

**Step 4** Log in as the root user.

**Step 5** Right-click the desktop and select *New Terminal*.

**Step 6** Navigate to the directory where you saved the CSA upgrade file.

**Step 7** Enter `rpm -e cisco-CSA_package` to uninstall the previous CSA version.

**Step 8** Enter `rpm -Uvh <CSA-upgrade-filename>` to execute the program.
Example: `rpm -Uvh CSA_5.1.0.95`

**Step 3** Choose *Open Agent Panel*.

**Step 4** To change the level of security for your system:
  a. Select *System Security*.
  b. Move the security level slide bar to the new security level.

**Note** We recommend that you keep the security level at medium or high.

**Step 5** Select *Status > Messages > View log* to display the logged security events.

**Step 6** (Optional) Select *Purge log* to remove the entries that appear on the Status > Messages window.
Doing this regularly can help you track new events.

**Note** Selecting *Purge log* does not affect the logs under /var/log/csalog.

**Related Topics**
- Upgrading Cisco Security Agent (CSA) on the Application Server, page 4
Limiting the Number of Failed User Login Attempts

You can configure the number of times in a session that an end user can fail to log in to Cisco Unified MeetingPlace before the user profile becomes “locked.” Users with locked user profiles cannot log in.

Restrictions

- The preconfigured system administrator profile cannot be locked.
- Before reaching the maximum number of login attempts, the user may restart the counter for failed login attempts by:
  - Closing the browser and opening a new one to continue the login attempts.
  - Ending the call to Cisco Unified MeetingPlace and making a new call to continue the login attempts.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Usage Configuration.
Step 3 Configure the Maximum profile login attempts field. A lower value is more secure than a higher value.
Step 4 Select Save.

Related Topics

- Changing the User Status in Cisco Unified MeetingPlace User Profiles module
- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Configuring Requirements for User Passwords

You can increase the security of your system by:

- Requiring long user passwords
- Requiring users to change their user passwords frequently
- Requiring complex user passwords

Restrictions

- This task does not affect Directory Service users, who are authenticated externally through AXL authentication.
- Long or complex passwords and frequent password changes may frustrate your users. Make sure you align your password requirements with those already in use at your company.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select System Configuration > Usage Configuration.

Step 3 Configure the following fields, which determine how long passwords must be:

- Minimum profile password length
- Minimum user password length

Step 4 Configure the following fields, which affect when users are required to change their passwords:

- Change profile password (days)
- Change user password (days)

Step 5 Configure the following fields, which determine how complex the user passwords must be:

- Password contains characters from at least three classes
- No character in the new password repeated more than three times
- Password does not repeat or reverse the user name
- Password is not "cisco", "ocsic" or variation of these

Step 6 Select Save.

Related Topics

- Field Reference: Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring Cisco Unified MeetingPlace Directory Service module
Configuring Requirements for Meeting Passwords

Meeting passwords prevent uninvited people from attending meetings. You can increase the security of your system by:

- Requiring passwords for meetings scheduled by some or all users
- Requiring long meeting passwords

Before You Begin

Meeting password must be communicated to the meeting invitees in order for them to join the meeting:

- Configure user groups and user profiles to include meeting passwords in e-mail notifications. See the “Configuring User Preferences for E-Mail Notifications” section on page 3.
- If not all meeting invitees will receive e-mail notifications, the meeting scheduler or another organizer must manually communicate the meeting password.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Meeting Configuration.
Step 3 Configure the Minimum meeting password length field. A higher value is more secure than a lower value.
Step 4 Select Save.
Step 5 Select User Configuration.
Step 6 Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.
Step 7 Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.
Step 8 Set the Meeting password required to Yes.
Step 9 Select Save.
Step 10 Repeat Step 5 through Step 9 for all user groups and user profiles for which you want to require meeting passwords.

Related Topics

- Field Reference: Meeting Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Restricting Access to Scheduled Meetings

You can restrict uninvited and unprofiled users from attending meetings that are scheduled by some or all users.

Remember, however, that if meeting attendance is restricted to profiled users, then unprofiled external users (such as your customers or business partners) and users with locked profiles cannot attend meetings, even if they are invited.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration.
Step 3 Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.
Step 4 Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.
Step 5 Configure the Who can attend field.
Step 6 Select Save.

Related Topics
- Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Restricting Access to Recordings and Attachments

You can restrict unprofiled users from accessing recordings and attachments for meetings that are scheduled by some or all users. Remember, however, that if access to recordings is restricted to profiled users, then unprofiled external users (such as your customers or business partners) and users with locked profiles cannot access the recordings, even if they were invited to and attended the meetings.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration.
Step 3 Select User Groups or User Profiles, depending on whether you want to configure a user group or an individual user profile.
Step 4 Select Edit or Add New, depending on whether you want to configure an existing or a new user group or user profile.
Step 5 Configure the Who can access field.
Step 6 Select Save.
Restricting the Use of Vanity Meeting IDs

By default, Cisco Unified MeetingPlace allows the meeting scheduler to request a specific meeting ID, such as one that is easy to remember (12345) or one that spells a word (24726 or CISCO). If, however, an uninvited person knows one of the phone numbers for your Cisco Unified MeetingPlace system, that person can easily guess a popular meeting ID and join a meeting that he is not authorized to attend.

You can prevent unauthorized meeting attendance by disabling the ability to request a vanity meeting ID when scheduling a meeting. Instead, a unique, randomly generated ID is assigned to every scheduled meeting. Users cannot change the assigned meeting IDs.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Meeting Configuration.
Step 3 Set the Allow vanity meeting IDs field to No.
Step 4 Select Save.

Restricting Dial-Out Privileges for Guest Users

To prevent toll fraud, you can specify that only profiled users who successfully log in to Cisco Unified MeetingPlace may dial out.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select User Configuration > User Profiles.
Step 3 Find the guest profile.
Restricting Dial-Out Privileges for Profiled Users

To prevent toll fraud, you can restrict dial-out privileges to specific user groups and user profiles.

Procedure

**Step 1** Log in to the Administration Center.

**Step 2** Select **User Configuration**.

**Step 3** To restrict dial-out privileges for specific user groups, select **User Groups**. To restrict dial-out privileges for specific user profiles, select **User Profiles**.

**Step 4** Select a user group or user profile and select **Edit** in the same row.

**Step 5** To restrict dial-out privileges, configure the following fields:

- **Can dial out (does not apply to Cisco WebEx meetings)**—Set to **No**.
- **Ask for profile password**—Set to **Yes**.

**Step 6** Select **Save**.

Related Topics

- **Navigation Reference: User Groups Page** in the Administration Center Page References for Cisco Unified MeetingPlace module
- **Navigation Reference: User Profiles Page** in the Administration Center Page References for Cisco Unified MeetingPlace module
- **Restricting Dial-Out Privileges for Guest Users, page 9**
- **Limiting the Number of Attempted Dial-Out Calls From Voice Meetings, page 11**
Limiting the Number of Attempted Dial-Out Calls From Voice Meetings

To prevent toll fraud, you can specify the maximum number of dial-out calls that each user can try to make from within a meeting.

**Restriction**
This procedure affects only the dial-out calls that the user attempts by pressing #31 from the telephone user interface (TUI). You cannot limit the number of dial-out calls that are attempted from the web meeting room.

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Select **User Configuration**.

**Step 3** To restrict dial-out privileges for specific user groups, select **User Groups**. To restrict dial-out privileges for specific user profiles, select **User Profiles**.

**Step 4** Select a user group or user profile and select **Edit** in the same row.

**Step 5** Configure the **Maximum TUI outdial attempts per meeting** field.

We recommend restricting the dial-out attempts to as low a number as possible while accommodating the dial-out needs of your users.

**Step 6** Select **Save**.

**Related Topics**
- Navigation Reference: User Groups Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Navigation Reference: User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Restricting Dial-Out Privileges for Guest Users, page 9
- Restricting Dial-Out Privileges for Profiled Users, page 10
How to Configure Restricted Meeting ID Patterns

As a system administrator, you can restrict Cisco Unified MeetingPlace from accepting certain meeting ID patterns that you consider unsecure. For example, you can restrict meeting ID patterns that repeat the same digit three times in a row, such as 111 or 222.

Keep the following points in mind when determining which meeting ID patterns to restrict:

- Restricted meeting ID patterns affect both numerical and vanity meeting IDs. Therefore, if you select to restrict patterns that repeat the same digit three times, Cisco Unified MeetingPlace will disallow both the numerical meeting ID “333” and the vanity meeting ID “deepdive,” because “deepdive” translates to 3337383.

- Keep the length of your minimum meeting ID requirement in mind. Repeating the same digit three times when the length of your minimum meeting ID is four digits long can be considered a security risk. However, repeating the same digit three times when the length of your minimum meeting ID is eight digits long may not.

- There is always the chance of a meeting ID hitting the rule pattern and causing a problem. Judicious use of the rule is critical for the reduction of such incidents.

Note

You cannot schedule a meeting with a supported meeting ID pattern through the phone or other scheduling endpoint, then attempt to modify it or reschedule it through the web. This rescheduling behavior is not supported.
Adding Restricted Meeting ID Patterns

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select Restricted Meeting ID Patterns.
Step 4  For Pattern, enter the restricted meeting ID pattern as a regular expression using the Perl syntax.
Example: .*(012|123|234|345|456|567|678|789|890|987|876|765|654|543|432|321|210).*
Step 5  Enter a brief description to explain the intent of the pattern in the field provided.
Example: Block sequences of 3 increasing or decreasing numbers.
Step 6  Select Add.
The pattern displays in the “View” section of the page.
Step 7  Repeat Step 4 through Step 6 for each additional restricted ID pattern.

Related Topics
- How to Configure Restricted Meeting ID Patterns, page 1

Deleting Restricted Meeting ID Patterns

Procedure

Step 1  Sign in to the end-user web interface.
Step 2  Select Admin.
Step 3  Select Restricted Meeting ID Patterns.
Step 4  Scroll down to the “View” section of the screen.
Step 5  Locate the pattern you want to delete.
Step 6  Select Delete.

Related Topics
- How to Configure Restricted Meeting ID Patterns, page 1
How to Configure Secure Sockets Layer

Secure Sockets Layer (SSL) secures information shared in a web conference by encrypting the data for travel across the network.

Complete the following procedures in the order shown to configure SSL.

- Restrictions for Configuring Secure Sockets Layer, page 3
- Changing the Web Server Hostname From an IP Address to a Hostname, page 3
- Creating a New Certificate Signing Request and Obtaining a Certificate File, page 5
- Applying the SSL Certificate, page 6
- Enabling SSL, page 7
- Testing the Web Server Over an HTTPS Connection, page 7
- (Optional) Disabling Support for Low Encryption Ciphers and SSL v2, page 8

Restrictions for Configuring Secure Sockets Layer

- If you are using SSL on an external Web Server, make sure that the hostname on the SSL certificate resolves to the external Web Server IP address.
- If you are using SSL on a system with a segmented DNS, make sure that the hostname on the SSL certificate differs from the segmented DNS name.
- Self-signed certificates are not supported.
- Make sure that both the Hostname [Home Page] and Hostname [Web Conferencing] use hostnames, not IP addresses.
- If users will access your Web Server through a firewall, make sure that TCP port 443 is open inbound on your firewall for both of the hostnames or IP addresses on your server.
- You can use SSL on any Web Server (internal or DMZ); however, you cannot use or configure WIA (Windows Integrated Authentication) on that server.

Related Topics

- How to Configure Secure Sockets Layer, page 3

Changing the Web Server Hostname From an IP Address to a Hostname

The Web Server hostname was populated during the Cisco Unified MeetingPlace Web Conferencing installation. The Hostname [Home Page] was assigned the first IP address in the operating system. The Hostname [Web Conferencing] was assigned the second IP address in the operating system. You should not need to redefine these unless either of the following applies:

- You want users to be able to access the Cisco Unified MeetingPlace Web Server by using the fully qualified domain name (FQDN) of the server or
- You plan to configure SSL for this server. If enabling SSL, you must use hostnames rather than IP addresses.

Before You Begin

This procedure assumes that you have already installed Cisco Unified MeetingPlace Web Conferencing.
Restrictions
Do not perform this procedure if the Web Server is not in a Domain Name Server (DNS).

Procedure

**Step 1**  
Open your web browser and enter the URL of your Web Server.

- For internal Web Servers, the default URL structure is `http://server`, where `server` is the name of your internal Web Server.
- For external (DMZ) Web Servers running Release 7.0.1, the default URL structure is `http://server/mpweb/admin/`, where `server` is the name of your external Web Server.
- For external Web Servers running Release 7.0.2 or later releases, you can only access the administration pages for the external (DMZ) server from the server box itself and only through port 8002. If you try to access the administration pages on the external (DMZ) server by using `http://server/mpweb/admin/`, the system will display a 404 “Page Not Found” error.

To access the administration pages for the external (DMZ) server, you must be on the web server box and enter the following URL: `http://localhost:8002/mpweb/admin/`

**Note**  
If SSL is enabled on your system, you must still enter the URL with http and not https.

The system automatically logs you in as the user called “technician” with technician privileges.

**Step 2**  
Sign in to the end-user web interface.

**Step 3**  
Select **Admin** if you are not already on the Cisco Unified MeetingPlace Web Administration page.

**Step 4**  
Select **Web Server**.

**Step 5**  
Scroll down to the “View” section of the page.

**Step 6**  
Select the name of the Web Server that you want to configure.

Information about this Web Server populates the “Edit” section of the page.

**Step 7**  
For **Hostname [Home Page]**, enter the fully qualified domain name (FQDN) of the primary network interface on the Web Server.

Example: `hostname.domain.com`.

**Note**  
This hostname must be different from that used for Hostname [Home Page]. It must be resolvable by its intended users. Depending on your hostname choice, the hostnames might not have been automatically registered with the DNS during the OS installation. We recommend that you check the DNS, both the forward and reverse lookup zones, and add entries manually if needed.

**Step 8**  
For **Hostname [Web Conferencing]**, enter the FQDN of the secondary network interface on the Web Server.

Example: `hostnamewc.domain.com`. 
Configuring Cisco Unified MeetingPlace Web Conferencing Security Features

How to Configure Secure Sockets Layer

Note
This hostname must be different from that used for Hostname [Home Page]. It must be resolvable by its intended users. Depending on your hostname choice, the hostnames might not have been automatically registered with the DNS during the OS installation. We recommend that you check the DNS, both the forward and reverse lookup zones, and add entries manually if needed.

Step 9
Select Submit.

Step 10
(Optional) If you are working on a Windows system with Internet Explorer, select Test Server Configuration.

Related Topics
• Using the Cisco Unified MeetingPlace Web Administration Page in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module

• Field Reference: Web Server Specific Fields in the Web Administration References for Cisco Unified MeetingPlace module

• How to Resolve Test Server Configuration Problems in the Troubleshooting Cisco Unified MeetingPlace Web Conferencing module

What to Do Next
• Restart the Cisco Unified MeetingPlace Web Conferencing services for changes to the Hostname [Web Conferencing] field to take effect. See Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module for instructions.

Note
When you restart the Web Server, all manual changes made to the registry are lost.

• If you are configuring SSL, proceed to the “Creating a New Certificate Signing Request and Obtaining a Certificate File” section on page 5.

Creating a New Certificate Signing Request and Obtaining a Certificate File

Use the SSL/TLS configuration page to generate certificate signing requests to send to an authorized Certificate Authority in order to apply for a digital identity certificate. You need two certificates: one for the Home Page hostname, and one for the Web Conferencing hostname.

Before You Begin
Complete the “Changing the Web Server Hostname From an IP Address to a Hostname” section on page 3.

Procedure

Step 1
Sign in to the end-user web interface.

Step 2
Select Admin.

Step 3
Select SSL/TLS.
How to Configure Secure Sockets Layer

Step 4  Select the **Edit** icon for the Web Conferencing hostname.

Step 5  Enter your company name and organization unit/department in the applicable fields.

Step 6  Enter the complete, official names of your city/locality and state/province in the applicable fields.

**Note**  Do not use abbreviations.

Step 7  Select your country/region.

Step 8  Select **Generate Request**.

The new certificate signing request (CSR) displays in the text box. The request is signed with an auto-generated private key.

Step 9  Select the **Private Key** link to see the value of the private key.

Step 10  Copy the contents of the CSR text box to a text file and send this file to your certificate provider in return for a certificate file.

**Caution**  If your certificate provider asks for your server type, specify Apache or Custom, not Microsoft or IIS. If you attempt to install a Microsoft or IIS certificate by using the SSL/TLS configuration pages, Cisco Unified MeetingPlace Web Conferencing will not restart when you attempt to reboot the system. Instead it will log an error about the certificate and disable SSL so that you can restart and fix the problem.

Step 11  Select **Back** to return to the main Administration page.

Step 12  Repeat **Step 3** through **Step 11** for the Web Conferencing hostname.

What to Do Next

When you receive the .cer files from your certificate provider, proceed to the “Applying the SSL Certificate” section on page 6.

Applying the SSL Certificate

When you receive the certificate files from your certificate provider, apply the certificates to the Cisco Unified MeetingPlace website by completing the following procedure.

**Before You Begin**

Complete the “Creating a New Certificate Signing Request and Obtaining a Certificate File” section on page 5.

**Procedure**

Step 1  Sign in to the end-user web interface.

Step 2  Select **Admin**.

Step 3  Select **SSL/TLS**.

Step 4  Select the **Edit** icon for the Web Conferencing hostname.
Step 5  Open the certificate file for the Web Conferencing hostname in a text editor, and copy the text to the clipboard.

Step 6  In the text box at the bottom of the page, paste the text from the certificate you obtained for this hostname.

Make sure the text you paste includes the begin and end certificate delimiters.

Step 7  Select **Install Certificate**.

The host is now set up with a certificate.

Step 8  Select **Back** to return to the main Administration page.

Step 9  (Release 7.0.1 systems only) Repeat Step 3 through Step 8 for the Home Page hostname.

---

**What to Do Next**

Proceed to the “Enabling SSL” section on page 7.

---

### Enabling SSL

Complete this procedure to enable the Require SSL field on the Web Server administration page.

**Before You Begin**

- Complete the “Applying the SSL Certificate” section on page 6.
- Make sure that you are still on the SSL/TLS page.

**Procedure**

Step 1  Select **Toggle SSL** to turn SSL on.

Step 2  Select **Reboot Server**.

The server shuts down and restarts.

**Note**  If the Web Server cannot validate the SSL certificates, the server will log an error and toggle SSL to off. In this case, you will need to restart the Cisco Unified MeetingPlace Web Conferencing service and fix the issue, then repeat the steps in this procedure.

**Note**  When you restart the Web Server, all manual changes made to the registry are lost.

**What to do Next**

Proceed to the “Testing the Web Server Over an HTTPS Connection” section on page 7.

---

### Testing the Web Server Over an HTTPS Connection

**Before You Begin**

Complete the “Enabling SSL” section on page 7.
How to Configure Secure Sockets Layer

Procedure

**Step 1** Use a web browser to connect to https://hostname.domain.com, the Fully Qualified Domain Name, of the Web Server.
- If the Cisco Unified MeetingPlace home page displays, the connection to the Home Page hostname is successful.
- If any security warning dialog boxes appear, configure SSL not to show the dialog boxes.
  For detailed information, see Microsoft Knowledge Base Articles 813618 and 257873 on the Microsoft website.

**Step 2** Sign in to the end-user web interface.

**Step 3** Select **Immediate Meeting**.
If the meeting console opens, the connection to the Web Conferencing hostname is successful.

(Optional) Disabling Support for Low Encryption Ciphers and SSL v2

Cisco authorizes Cisco Unified MeetingPlace Web Conferencing customers to disable the support for low encryption ciphers and SSL v2 on their Cisco Unified MeetingPlace Web Servers based on their security requirements.

You must assume all work related to this security hardening as well as the operational consequences of this security lock-down, including the fact that some end-users might be unable to use the Cisco Unified MeetingPlace Web Servers because of incompatible browsers/ client SSL implementation, or encryption strength limitations.

To perform this lock-down for the Microsoft IIS web server component used by Cisco Unified MeetingPlace Web Conferencing, see the following Microsoft Knowledge Base articles:

How to Control the Ciphers for SSL and TLS on IIS (IIS restart required): [http://support.microsoft.com/default.aspx?scid=KB;en-us;q216482](http://support.microsoft.com/default.aspx?scid=KB;en-us;q216482)


How to disable PCT 1.0, SSL 2.0, SSL 3.0, or TLS 1.0 in Internet Information Services (Windows restart required): [http://support.microsoft.com/default.aspx?scid=kb;en-us;187498](http://support.microsoft.com/default.aspx?scid=kb;en-us;187498)

To perform this lock-down for the Adobe Connect application web server used by Cisco Unified MeetingPlace Web Conferencing, see the following Adobe article:


**Note**
You can find the Server.xml file that contains the SSLCipherSuite tag to be edited in the following folder on the Cisco Unified MeetingPlace Web Server: C:\Program Files\Cisco Systems\MPWeb\WebConf\comserv\win32\conf

**Caution**
Any upgrade of the Cisco Unified MeetingPlace Web Conferencing software with a maintenance release will overwrite the changes that you have made in Server.xml. These changes must be re-applied after the upgrade.
How to Replace an Expired Intermediate Certificate for the Home Page

As of April 2006, all SSL certificates issued by VeriSign require the installation of an intermediate Certificate Authority (CA) certificate. The SSL certificates are signed by an intermediate CA using a two-tier hierarchy (also known as trust chain) which enhances the security of SSL certificates. For more information, go to: http://www.verisign.com/support/advisories/page_040611.html.

Topics in this section include:
- Downloading the Updated VeriSign Intermediate CA, page 9
- Creating a Certificate Snap-In, page 9
- Removing the Expired Intermediate CA, page 10
- Installing the New Intermediate CA, page 10

Downloading the Updated VeriSign Intermediate CA

When downloading the intermediate CA certificate, ensure that you select the appropriate one for your SSL certificate: either Secure Site with EV Certificates (Secure Server) or Secure Site Pro with EV Certificates (Global).

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>If you are not sure which certificate you have purchased, follow these steps:</th>
</tr>
</thead>
<tbody>
<tr>
<td>a.</td>
<td>Go to VeriSign Search Certificates page.</td>
</tr>
<tr>
<td>b.</td>
<td>Type your Common Name or Order Number.</td>
</tr>
<tr>
<td>c.</td>
<td>Select Search.</td>
</tr>
<tr>
<td>d.</td>
<td>Select the certificate name for your certificate.</td>
</tr>
</tbody>
</table>

| Step 2 | Go to the VeriSign intermediate CA certificates web page and select the CA certificate for your product. |
| Step 3 | Copy and paste the contents into a text (Notepad) file.                     |
| Step 4 | Save the file as newintermediate.cer.                                       |

Creating a Certificate Snap-In

Procedure

| Step 1 | From the Web server, select Start > Run.                                    |
| Step 2 | In the text box, type mmc.                                                  |
| Step 3 | Select OK.                                                                   |
Removing the Expired Intermediate CA

Procedure

Step 1 From the left pane, double-click Certificate (Local Computer).
Step 2 Select Intermediate Certification Authorities > Certificates.
Step 3 Locate the certificate issued to www.verisign.com/CPS Incorp.by Ref.LIABILITY LTD. (C)97 VeriSign (expiration date of 1/7/2004).
Step 4 Right-click the certificate.
Step 5 Select Delete.
Step 6 From the left pane, select Trusted Root Certification Authorities > Certificates.
Step 7 Locate the certificate issued to Class 3 Public Primary Certification Authority (expiration date of 1/7/2004).
Step 8 Right-click the certificate.
Step 9 Select Delete.

Installing the New Intermediate CA

Procedure

Step 1 From the left pane, select Intermediate Certification Authorities.
Step 2 Right-click Certificates.
Step 3 Select All Tasks > Import.
Step 4 At the Certificate Import Wizard, select Next.
Step 6 Select Next.
Step 7 Select Place all certificate in the following store: Intermediate Certification Authorities.
Step 8 Select Next.
Step 9 Select Finish.
Step 10 Restart the Web Server.

If this does not resolve the issue, then physically reboot the Web Server. The Web Server should now only have one Intermediate CA that expires in 2016.

Note When you restart the Web Server, all manual changes made to the registry are lost.

How to Replace an Expired Intermediate Certificate for Web Conferencing

Note As of April 2006, all SSL certificates issued by VeriSign require the installation of an intermediate Certificate Authority (CA) certificate. The SSL certificates are signed by an intermediate CA using a two-tier hierarchy (also known as trust chain) which enhances the security of SSL certificates.

For more information, go to: http://www.verisign.com/support/advisories/page_040611.html.

1. Follow the steps in the “Downloading the Updated VeriSign Intermediate CA” section on page 9.
   In that procedure, you copied the contents of the intermediate CA certificate into a file called newintermediate.cer.
2. Follow the steps in the “Applying the SSL Certificate” section on page 6.
3. When prompted to copy the certificate, copy the text from file called newintermediate.cer.
4. Add the intermediate certificate provided by your certificate authority provider to the SSL certificate PEM files.

Note When pasting these two certificates within the same PEM file, the order of these certificates matters. The signed server certificate has to be pasted first and then the intermediate certificate should be pasted below the signed server certificate. Be careful when pasting these certificates into the file as extra spaces or dashes can cause problems with the certificate file. Once you make the changes, restart Flash Communication services and the Breeze Application service.
How to Back Up and Restore the SSL Private Key

This section describes how to export and subsequently reimport the SSL private key into the MPWEB database. We recommend that you make this part of your standard backup procedure. You will need to complete these procedures any time you need to move the SSL certificate, for example, from an old Web Server computer to a new Web Server computer or when you are rebuilding a computer.

- Exporting the Private Key, page 12
- Copying and Saving the Private Key for Future Use, page 13
- Importing the Private Key into the MPWEB Database, page 14

Exporting the Private Key

This procedure describes how to export the private key/certificate pair on the Web Server so that you can manually copy the SSL files in case you need to restore SSL on the Web Server.

Procedure

**Step 1** Open the Internet Services Manager on the Cisco Unified MeetingPlace Web Server. Select Start > Programs > Administrative Tools > Internet Information Services Manager.

**Step 2** Navigate to Default Web Site. Select the + sign beside Local Server > Web Sites to open the appropriate directory trees.

**Step 3** Right-click Default Web Site.

**Step 4** Select Properties.

**Step 5** Select the Directory Security tab.

**Step 6** Select Server Certificate.

**Step 7** Select Next.

**Step 8** Select Export the current certificate to a pfx file.

**Step 9** Select Next.

**Step 10** Select Browse and select to save the certificate file to your desktop.

**Step 11** Select Next.

**Step 12** Enter a password to encrypt the certificate.

**Step 13** Enter the password again to confirm it.

**Step 14** Select Next.

The Export Certificate Summary Screen displays and the exported certificate file is now on your desktop.

**Step 15** Select Next.

**Step 16** Select Finish to close the Web Server Certificate wizard.
Step 17 Select OK or Cancel to close the Default Web Site Properties window.

Step 18 Close IIS Manager.

What to Do Next
Proceed to the “Copying and Saving the Private Key for Future Use” section on page 13.

Copying and Saving the Private Key for Future Use

We recommend that you complete this procedure as part of your standard backup procedure on the Web Server.

Before You Begin
Complete the “Exporting the Private Key” section on page 12.

Procedure

Step 1 Open a DOS prompt.
   a. Select Start > Run.
   b. Enter cmd.

Step 2 Enter the path to your desktop in the cmd.exe window.
   Example: C:\> cd "Documents and Settings\Administrator\Desktop"

Step 3 Enter the full path to OpenSSL.exe keeping the following in mind:
   • After -in, enter the full path to where you placed the file when you exported the private key.
   • After -out, enter the full path to where you want to send the exported file.
   Example: C:\Documents and Settings\Administrator\Desktop>\Program Files\Cisco Systems\MPWeb\DataSvc\openssl.exe" pkcs12 -in "\Documents and Settings\Administrator\Desktop\mycertificate.pfx" -out "\Documents and Settings\Administrator\Desktop\mycertificate.pem" -nodes

This converts the PFX format to a PEM format. The mycertificate.pem file will have all the certificates starting with the Private key.

Step 4 Enter the import password when prompted.
This is the password you defined in the Web Server Certificate wizard during the export process.

Step 5 Save the PEM file. You will need it whenever you need to reapply the certificate.

Related Topics
• Exporting the Private Key, page 12
Importing the Private Key in to the MPWEB Database

Before You Begin
Complete the “Copying and Saving the Private Key for Future Use” section on page 13.

Procedure

Step 1 Open SQL Server Enterprise Manager.
Select Start > All Programs > Microsoft SQL Server > Enterprise Manager.

Step 2 Navigate to the MPWEB database.
Select the + sign next to SQL Server Group > LOCAL > Databases > MPWEB to open the appropriate directory trees.

Step 3 Select Tables in the MPWEB directory.
A list of tables opens in the right pane.

Step 4 Right-click Web in the right pane.

Step 5 Select Open table > Return all rows.
The Web database table displays.

Step 6 Scroll to the right until you see the SSLPrivateKey column.

Step 7 Open the PEM file in Notepad.
You saved the PEM file when you copied and saved the private key for future use.

Step 8 Copy the private key in its entirety.
The private key begins with “Begin RSA Private key” and ends with “end RSA private key”.

Step 9 Paste the private key into the SSLPrivateKey field.
a. Select the field before the SSLPrivateKey column.
b. Press the Tab key on your keyboard to select all of the data in the SSLPrivateKey field.
c. Right-click and select Paste to paste the value you copied from Notepad.

Step 10 Click somewhere else on the screen to remove your cursor from the SSLPrivateKey field.

Step 11 Close SQL Server Enterprise Manager.

Step 12 (Optional) Enable SSL if it is not already enabled.

Step 13 Reboot the server.

Related Topics
- Enabling SSL, page 7
- Copying and Saving the Private Key for Future Use, page 13
Allowing Guests to Search Through Public Meetings

Guest users have fewer privileges than users who log in with their profiles. Complete this procedure to allow guests to search through public meetings.

Procedure

Step 1 Sign in to the end-user web interface.
Step 2 Select Admin.
Step 3 Select Web Server.
Step 4 Scroll down to the “View” section of the page.
Step 5 Select the name of the Web Server that you want to configure. Information about this server populates the “Edit” section of the page.
Step 6 Select Yes for Allow Public Meetings in Find Meeting List.
Step 7 Select Yes for Allow Guest Access to Find Meetings Page.
Step 8 Select Submit.

Tip

To allow external users (those outside your firewall) and sites (Cisco Unified MeetingPlace systems outside your network) to access a meeting and the associated meeting materials, make sure that Allow External Web Participants is set to Yes for the meeting.

This parameter is set by the meeting scheduler from the New Meeting scheduling page, and it is only visible if your Cisco Unified MeetingPlace system has an external site—that is, a Web Server located in an Internet-accessible segment of your network, such as in a DMZ zone.

Related Topics

- Field Reference: Web Server Customization Values in the Web Administration References for Cisco Unified MeetingPlace module
Configuring SSL for the Cisco Unified MeetingPlace Application Server

Release 7.1
Revised: April 3, 2011 8:30 pm

To enable Secure Sockets Layer (SSL) to provide secure web communications for the Application Server, you need to obtain and upload a digital identity certificate that the system binds with a private key and password.

- Interfaces Secured by SSL for the Application Server, page 1
- Generating a Certificate Signing Request and Obtaining the Certificate, page 2
- Uploading the Certificate File and Enabling SSL, page 3
- Displaying the Certificate, page 5
- Backing Up the SSL Configuration, page 5
- Restoring the SSL Configuration, page 5
- Disabling SSL, page 6

Interfaces Secured by SSL for the Application Server

Enabling SSL for the Application Server secures web communications with the following interfaces:

- Administration Center
- MeetingPlace Conference Manager
- Microsoft Outlook plug-ins for scheduling Cisco Unified MeetingPlace and Cisco WebEx web conferencing.
- Cisco WebEx integration end-user interface on the Application Server

Note

For information about configuring SSL for web conferencing, see the following modules:

- Configuring Cisco Unified MeetingPlace Web Conferencing Security Features
- Integrating Cisco Unified MeetingPlace with Cisco WebEx
Generating a Certificate Signing Request and Obtaining the Certificate

In this task, you create a certificate signing request (CSR) that you then send to an authorized certificate authority (CA) to apply for a digital identity certificate. The system also creates and stores a private key file and password specifically for that certificate. When you later upload the certificate file, the system binds the certificate file with the system-generated private key file and password to enable SSL.

Before You Begin

- If you created your own certificate and private key, then do not perform this task. Proceed to the “Uploading the Certificate File and Enabling SSL” section on page 3.
- SSL must be disabled to generate CSRs.
- The CSR and resulting certificate use the Application Server hostname that you entered for Ethernet Port 1 (device eth0) during the operating system installation.
  
  If you change this hostname, then you must obtain new certificates.
  
- Self-signed certificates can be used for the application server.
- Make sure that you request a file in one of the following formats:
  - Private keys: PKCS #1, PKCS #8 (PEM or DER encoding), Java keystore
  - Certificates: X.509 (PEM or DER encoding), Java keystore

Caution

If you already installed a valid SSL certificate, then generating a new CSR will make the existing certificate invalid. Proceed only if you are installing the certificate for the first time, if you are replacing an expired or invalid certificate, or if you change the hostname of your Application Server.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Certificate Management > Generate CSRs.
Step 3  Enter values in the fields on the Generate Certificate Signing Request (CSR) Page.

Note  Some CAs do not recognize two-letter state abbreviations, so enter the full name of the state. Also, if you want to use any special (non-alphanumeric) characters, ask your CA for character restrictions.

Step 4  Select Generate CSR only once.
Step 5  Select OK.
Step 6  Select Download CSR.
Configuring SSL for the Cisco Unified MeetingPlace Application Server

Uploading the Certificate File and Enabling SSL

---

**Caution**

After you select **Download CSR**, do not modify any fields on this page, and do not select **Generate CSR** again. Doing so will result in an invalid certificate from the CA.

---

**Step 7**

Select **Save**.

**Step 8**

In the Save As dialog box, perform the following actions:

a. Delete any browser-added text (typically [1] and .txt) from the filename, to make the filename appear in this format: `fully-qualified-domain-name_req.csr`

   Example: meetings.example.com_req.csr

b. In the Save as type field, select **All Files**.

c. Choose the appropriate directory.

d. Select **Save**.

**Step 9**

Send this file to the CA in return for a certificate file.

Make sure that you request a file in one of the following formats:

- Private keys: PKCS #1, PKCS #8 (PEM or DER encoding), Java keystore
- Certificates: X.509 (PEM or DER encoding), Java keystore

---

**Related Topics**

- Field Reference: Generate Certificate Signing Requests (CSRs) Page in the Administration Center
- Page References for Cisco Unified MeetingPlace module
- Troubleshooting the Cisco Unified MeetingPlace Application Server module

**What To Do Next**

- We recommend that you back up and archive your system to save the system-generated private key file and password that are required to validate the certificate that you ordered from the CA. Otherwise, if the system is reinstalled for some reason before you receive and upload the certificate, then you will need to generate a new CSR and obtain a new certificate. See the Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module.
- Proceed to the “Uploading the Certificate File and Enabling SSL” section on page 3.

---

**Uploading the Certificate File and Enabling SSL**

**Before You Begin**

- Obtain the certificate by one of these methods:

  - Obtain a certificate from a trusted CA—See the “Generating a Certificate Signing Request and Obtaining the Certificate” section on page 2. This is the root CA certificate.
  
  - Create your own certificate, private key, and password—If you use this method, note that when a user tries to access one of the Interfaces Secured by SSL for the Application Server, a security alert warns the user that the certificate comes from an untrusted source. The user then has to select **OK** to proceed.
  
  - Self-signed certificates can be used for the application server.
• The application server supports only the following formats:
  – Private keys: PKCS #1, PKCS #8 (PEM or DER encoding), Java keystore
  – Certificates: X.509 (PEM or DER encoding), Java keystore
• If your CA issued a certificate that requires the installation of an intermediate CA certificate:
  1. Obtain the intermediate CA certificate(s) by contacting your CA.
  2. Using a text editor, paste the text of the intermediate CA certificate to the end of the Cisco Unified MeetingPlace certificate file.
  3. In the procedure below, make sure that you upload the combined certificate file that includes both the root and intermediate CA certificates.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Certificate Management > Enable SSL.
Step 3  Enter values in the fields.

Note  If you obtained the certificate from a CA by using the Generate Certificate Signing Request (CSR) Page, then only enter the Certificate file.

Step 4  Select Upload Certificate.

Verifying
If this is the first certificate upload for the system, then proceed to the “Displaying the Certificate” section on page 5.

Otherwise, view the information capture log. See “Obtaining and Viewing the System Information Capture (Infocap) Log” in the Using Alarms and Logs on Cisco Unified MeetingPlace module.

Related Topics
• Field Reference: Enable SSL Page in the Administration Center Page References for Cisco Unified MeetingPlace module
• Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
• Troubleshooting the Cisco Unified MeetingPlace Application Server module
• Certificate or Private Key is in the Wrong Format in the Troubleshooting the Cisco Unified MeetingPlace Application Server module

What to Do Next
• If you use MeetingPlace Conference Manager, then you will need to edit the server URL to use “https” instead of “http.” See “Editing an Existing Server” in the Using MeetingPlace Conference Manager module.
• Proceed to the “Backing Up the SSL Configuration” section on page 5.
Displaying the Certificate

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Certificate Management > Display Certificate.
Step 3 Select Display Certificate.

Backing Up the SSL Configuration

Use this procedure to back up your SSL configuration, including the certificate.

If you ever reinstall the operating system, the SSL files will be deleted. The SSL files may also be lost (but are often preserved) when you reinstall or upgrade the Cisco Unified MeetingPlace application.

Before You Begin
Complete the “Uploading the Certificate File and Enabling SSL” section on page 3.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Certificate Management > Back Up SSL Configuration.
Step 3 Select Back Up SSL Configuration.
Step 4 Select Save.

Related Topics
- Restoring the SSL Configuration, page 5

What to Do Next
To configure SSL for web conferencing, see the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module.

Restoring the SSL Configuration

Before You Begin
Complete the “Backing Up the SSL Configuration” section on page 5.
Configuring SSL for the Cisco Unified MeetingPlace Application Server

Disabling SSL

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Select **Certificate Management > Restore SSL Configuration**.

**Step 3** Browse to the file.

By default, the filename is backupSSLDATA.zip.

**Step 4** Select **Restore SSL Configuration**.

**Related Topics**

- Troubleshooting the Cisco Unified MeetingPlace Application Server module

Disabling SSL

**Before You Begin**

You cannot disable SSL for only one Application Server interface. Completing this task disables SSL for all interfaces listed in the “Interfaces Secured by SSL for the Application Server” section on page 1.

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Select **Certificate Management > Disable SSL**.

**Step 3** Select **Disable SSL**.

**Step 4** Select **OK**.

**What To Do Next**

If you use MeetingPlace Conference Manager, then you will need to edit the server URL to use “http” instead of “https.” See “Editing an Existing Server” in the Using MeetingPlace Conference Manager module.
User Authentication for Cisco Unified MeetingPlace

Cisco Unified MeetingPlace System Authentication

The Cisco Unified MeetingPlace system authenticates users by one of the following methods, depending on what the isLocalUser user profile setting is for each user:

- Locally against the Cisco Unified MeetingPlace user database (isLocalUser is Yes)
- Externally through AXL authentication (isLocalUser is No)

Note: For details, see “External AXL Authentication for Directory Service Users” in the Configuring Cisco Unified MeetingPlace Directory Service module.

Related Topics

- When the System Uses Each Authentication Option, page 2
- Directory Service isLocalUser Setting In User Profiles in the Configuring Cisco Unified MeetingPlace Directory Service module
Third-Party Authentication for Cisco Unified MeetingPlace Web Conferencing

If you do not want to use system authentication for the end-user web interface, then you can use third party authentication software, for example:

- Cisco Unified MeetingPlace Local Authentication (this is the default)
- HTTP Basic Authentication (Domain)
- LDAP (this can provide multiple domain integration)
- LDAP, then MeetingPlace (this provides single domain integration)
- Trust External Authentication
- Windows Integrated Authentication

**Note**

For details, see the Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing module.

Related Topics

- When the System Uses Each Authentication Option, page 2

Integration-Specific Authentication

Some integrations may use authentication options that are separate from and not controlled by Cisco Unified MeetingPlace. Examples:

- Cisco WebEx About Cisco WebEx Integration Option 2
- Microsoft Outlook front-end integration using the Single Sign-On authentication method

Related Topics

- When the System Uses Each Authentication Option, page 2

When the System Uses Each Authentication Option

<table>
<thead>
<tr>
<th>User Login Method</th>
<th>Authentication Method</th>
</tr>
</thead>
<tbody>
<tr>
<td>Over the phone (TUI)</td>
<td>Cisco Unified MeetingPlace System Authentication</td>
</tr>
<tr>
<td>From the Cisco Unified MeetingPlace end-user web interface on the Web Server</td>
<td>Third-Party Authentication for Cisco Unified MeetingPlace Web Conferencing (if configured) Otherwise, Cisco Unified MeetingPlace System Authentication</td>
</tr>
<tr>
<td>From the Cisco Unified MeetingPlace Application Server</td>
<td>Cisco Unified MeetingPlace System Authentication</td>
</tr>
<tr>
<td>From the Cisco WebEx end-user web interface</td>
<td>Cisco WebEx authentication</td>
</tr>
</tbody>
</table>
Table 1  *Cisco Unified MeetingPlace Authentication Options (continued)*

<table>
<thead>
<tr>
<th>User Login Method</th>
<th>Authentication Method</th>
</tr>
</thead>
</table>
| From a Cisco Unified IP Phone with Cisco Unified MeetingPlace PhoneView | **Cisco Unified MeetingPlace System Authentication** of the Profile password is used to *join* meetings from Cisco Unified MeetingPlace PhoneView.  
**Note** As the system administrator, you enter the username and password of the user when you define the Cisco Unified MeetingPlace service parameters in Cisco Unified Communications Manager. This enables the user to subscribe to and use Cisco Unified MeetingPlace PhoneView. |
| From Microsoft Outlook                                  | • **Remember Me**—Cisco Unified MeetingPlace System Authentication and stored cookies.  
• **Single Sign-On**—User logs in to Microsoft Exchange or to Active Directory with matching User ID and Outlook Single Sign-On Domain configured in Cisco Unified MeetingPlace. |

---

1. TUI = telephone user interface

**Related Topics**

- About End-User Authentication Options, page 1
- Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing module
- Integrating Cisco Unified MeetingPlace with Cisco WebEx module
- Integrating Cisco Unified MeetingPlace With Cisco Unified IP Phone module
- About Default Authentication Methods for Microsoft Outlook Users in the Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module
Changing System Administrator Passwords for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:31 pm

This module describes how to change Application Server passwords for the administrator:

- Changing the Passwords for the admin Profile, page 1
- Changing the Password for the root or mpxadmin Account, page 2

Note
For information about other administrator passwords, see the following documents:

- For Web Server passwords, see the following:
  - For the Windows Media Server password, see “Installing Windows Media Server for Cisco Unified MeetingPlace” in the Configuring Audio Conversion module.
  - For the SQL password, see “How to Change and Apply a New SQL Password to Cisco Unified MeetingPlace Web Conferencing” in the Configuring Cisco Unified MeetingPlace Web Conferencing and SQL Server module.
  - For the Web Server shared storage directory password, see “Configuring Shared Storage” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module.

Changing the Passwords for the admin Profile

Note
We recommend that you change the passwords for the preconfigured admin profile to prevent unauthorized access to your system.
Changing System Administrator Passwords for Cisco Unified MeetingPlace

Changing the Password for the root or mpxadmin Account

Use this procedure to recover or change the root or mpxadmin CLI user level password, which is initially set during installation.

Procedure

Step 1  Log in to the Cisco Unified MeetingPlace operating system as the root user.
Step 2  At the password prompt, enter the root password.
        The Cisco Unified MeetingPlace operating system desktop appears.
Step 3  Right-click the desktop.
Step 4  Select New Terminal.
        This brings up a terminal session.
Step 5  At the prompt, enter /root/.security/unimmunize.sh.
Step 6  At the prompt, enter one of the following:
        • passwd root
        • passwd mpxadmin
Step 7  At the New password prompt, enter a new password.

Note  You may see a message that the password you entered is bad. Ignore this message.

Step 8  At the Retype new password prompt, re-enter the same password again.

Step 9  At the prompt, enter /root/security/immunize.sh.

Step 10 On the desktop, select the Red Hat icon.

Step 11 Select Log Out.

Step 12 Select OK.

Related Topics
- Password Recovery for Cisco Unified MeetingPlace module
Advanced Configuration

- Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server
- Configuring Application Server Failover for Cisco Unified MeetingPlace
- Importing Data into Cisco Unified MeetingPlace
- Configuring SNMP on Cisco Unified MeetingPlace
The Cisco Unified MeetingPlace backup and restore functions ensure that the system can recover with minimal data loss in case of database failure or corruption.

**Caution**

We recommend that you do not run reports or backups during peak hours of use, such as on the hour. Doing so may cause the system to fail.

- About Database Backups, Archives, and Restoration, page 1
- How to Back Up, Archive, and Restore Data, page 4

### About Database Backups, Archives, and Restoration

- Database Backups, page 1
- Cleanup Process for Database Backups, page 2
- About Archiving the Database Backup Files and Other Files, page 3

### Database Backups

We highly recommend that you back up and archive the Cisco Unified MeetingPlace Application Server for deployments with both a single Application Server and a deployment with Application Servers deployed for failover. You must set up the backup process on each Application Server individually.

The database backups include IP addresses and hostnames; therefore, you can only restore the backup onto the same Application Server where the backup occurred.

There are three types of database backups:

- **L0 (Level 0) backup.** This is the most common database backup. This is a complete physical and logical backup of the database from which data can be restored.
• L1 (Level 1) backup. The L1 backup is an incremental backup. It contains a backup of all the data that has been changed since the last L0 backup. It takes much less disk space than an L0 backup; however, it cannot be used for full restoration. If the system fails, you must use both the L0 and L1 backup files to restore data.

• L2 (Level 2) backup. The L2 backup is incremental to the L1 backup, so it needs both the L0 and the L1 backups to restore data.

Cisco Unified MeetingPlace uses a combination of L0, L1, and L2 backups and uses an Informix command called ontape for the backup mechanism.

The database backup file is physically located on the system disk of the Application Server. The system disk can contain up to three automatically-created L0 backups: the current L0, plus the previous one or two L0 backups. The L1 and L2 backups are also kept there. All of the older backups are removed from the system disk during the cleanup process.

⚠️ Caution

Use caution if you manually modify the backup files on the local disk or in the archive location. For successful data restoration, the three levels of backup files must be present in the correct order. For example, if the correct L0 and L2 backup files are present while the appropriate L1 backup file is missing, then the data cannot be restored.

You can enable or disable an automatic backup. If the automatic backup is enabled, an L0 backup happens twice a week, every Monday and Thursday at 11:00PM, local server time. The L1 backup is run each day at 1:00AM, local server time, while the L2 backups are done daily at 4:00AM, 8:00AM, 12:00PM, 4:00PM, and 8:00PM, local server time. The schedule is stored in the crontab file.

⚠️ Caution

If you disable automatic backups, the cleanup process continues to run as scheduled in the crontab file. Therefore, if you want to keep backup files that are older than seven days, you must archive them.

Note

Advanced system administrators can change the frequency of the automatic backups by editing the crontab file. Be careful when modifying the cron schedule, which determines the order of the backups.

The automatic backup process also incorporates archiving (if enabled) and cleanup. This ensures that if there is a database corruption or disk failure, in the worst case, less than five hours of data is lost.

Related Topics

• About Database Backups, Archives, and Restoration, page 1
• How to Back Up, Archive, and Restore Data, page 4

Cleanup Process for Database Backups

The cleanup process occurs before every scheduled backup in the crontab file. During the cleanup process, the following files are deleted:

• Backup files older than seven days.
• Unusable files, such as L1 and L2 backup files that are older than the oldest remaining L0 backup file.

⚠️ Note

If you disable automatic backups, the cleanup process continues to run as scheduled in the crontab file. Therefore, if you want to keep backup files that are older than seven days, you must archive them.
About Archiving the Database Backup Files and Other Files

Archiving makes a remote copy of all the backup files and external files, such as licenses, meeting attachments, and voice recordings that have not yet been deleted by the automatic system cleanup processes. If a newly archived file has the same name as an existing archived file, the new file overwrites the old file. Maintaining the archive and the remote system used for storing the archive is the responsibility of the system administrator.

Note
Backup files and archives do not include backup configuration settings, SNMP configuration settings, or SMTP configuration settings.

Automatic archiving can be enabled or disabled. When enabled, it is initiated by and happens after the automatic database backup. There are two options:

- SSH/rsync Archiving Method (Recommended), page 3
- FTP Archiving Method, page 3

SSH/rsync Archiving Method (Recommended)

The remote server to which you archive files must support rsync and SSH connections:

- To archive to a UNIX or Linux server, SSH service and rsync must be enabled on that server. Both SSH service and rsync are included in most UNIX and Linux distributions.
- To archive to a Windows-based server, both an SSH server and an rsync utility must be installed on that server.

Related Topics
- About Database Backups, Archives, and Restoration, page 1
- How to Back Up, Archive, and Restore Data, page 4

FTP Archiving Method

The following restrictions apply to the FTP archiving method:

- The FTP archiving method does not use a secure connection to transfer files to the remote server.
- The FTP archiving method enables the Cisco Unified MeetingPlace server to transfer backup files and other critical files to the remote server; FTP clients cannot transfer files to the Cisco Unified MeetingPlace server.
- Make sure that the remote host login credentials provide the permissions required to create new directories within in the directory specified in the Pathname location of archive field. For example, if you enter “pub” in the Pathname location of archive field, the following directories are automatically created when the archiving script runs:
  - pub/compressed_backup
How to Back Up, Archive, and Restore Data

Configuring Backups and Archiving

You can use the Cisco Unified MeetingPlace Administration Center to configure the system to automatically back up data. This section describes how to configure the parameters for the automatic backups that the system performs.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
</tr>
</tbody>
</table>
| Step 2 | Select Maintenance > Backup and Archive.  
(Release 7.0.1 only) Select Maintenance > Configure Backup. |
| Step 3 | Configure the fields on the Backup and Archive Page.  
(Release 7.0.1 only) Configure the fields on the Configure Backup Page. |
| Step 4 | Perform one of the following actions:  
- To save these values without running the backup program, select Save.  
- To save these values and run the backup process, select Save and Run Backup.  
- To save these values and run the archive process, select Save and Run Archiving. |

Related Topics

- Field Reference: Backup and Archive Page
- About Database Backups, Archives, and Restoration, page 1
- How to Back Up, Archive, and Restore Data, page 4
Backing Up Data Using the CLI

If you choose to disable the automatic back up feature (by selecting No for the Enable automatic backup field on the Backup and Archive Page), you can still manually back up data.

Restriction
Only run one backup (L0, L1, or L2) at a time.

Procedure

Step 1 Log in to the Cisco Unified MeetingPlace operating system as the mpadmin user.
Step 2 At the password prompt, enter the mpadmin password.
Step 3 Right-click on the desktop.
Step 4 From the menu, select New Terminal. This brings up a terminal session.
Step 5 Manually back up the data by entering the following:

```
sudo $MP_DATABASE/db-maintenance/backup.sh <number>
```

where `<number>` is the number of the backup you are running. To make sure you run only one backup at a time, specify 0 for an L0 backup, 1 for an L1 backup, or 2 for an L2 backup.

When the system finishes the backup, it displays a “Backup ended” message.

Step 6 On the desktop, select RedHat > Network Services.
Step 7 Select Log out.

Related Topics
- About Database Backups, Archives, and Restoration, page 1
- How to Back Up, Archive, and Restore Data, page 4

Archiving Data Using the CLI

The archive.sh script forces archiving, regardless if auto-archiving is on or off, as set in the procedure described in the “Configuring Backups and Archiving” section on page 4.

Procedure

Step 1 Log in to the Cisco Unified MeetingPlace operating system as the mpadmin user.
Step 2 At the password prompt, enter the mpadmin password.
Step 3 Right-click on the desktop.
Step 4 From the menu, select New Terminal. This brings up a terminal session.
Step 5 Manually archive the data by entering the following:

```
sudo $MP_DATABASE/db-maintenance/archive.sh
```
Note

The archive.sh script uses remote log-in credentials that are defined in the $MP_DATABASE/db-maintenance/settings.config file. You set these credentials using the procedure described in the “Configuring Backups and Archiving” section on page 4.

When the system finishes the archive, it displays “Archive ended” and “Archive external files ended” messages.

Step 6  On the desktop, select RedHat > Network Services.

Step 7  Select Log out.

Related Topics
- About Database Backups, Archives, and Restoration, page 1
- How to Back Up, Archive, and Restore Data, page 4

Restoring Data Using the CLI

Restoring the data recreates database server data from backed-up storage spaces and logical log files. You may need to restore your data if you need to replace a failed disk that contains database server data, if there is a logic error in a program that has corrupted the database, if you need to move your database server data to a new computer, or if a user accidentally corrupts or destroys data.

Before You Begin
- To restore data up to the time of the failure, you must have at least one L0 backup.
- You must have the backup files in the correct order. For example, if you have the correct L0 and L2 backup files, but not the appropriate L1 backup file, you cannot restore the data. This requires extra caution if you manually back up files on a local disk or in the archiving location.
- You can only restore the data to a server with the same IP and hostname as was originally configured for your backup.
- If you are restoring two Application Servers that are configured in a failover deployment, make sure that the servers are in standby mode before running the restore on them.
- If you are restoring two Application Servers that are configured in a failover deployment, make sure that you turn off replication before running the restore.

Restrictions
- You can only restore a database that is from the same version of Cisco Unified MeetingPlace. You cannot restore a database from a previous version.
- The names of the databases that you are restoring from and restoring to must be the same.

Procedure

Step 1  Log in to the Cisco Unified MeetingPlace operating system as the mpxadmin user.

Step 2  At the password prompt, enter the mpxadmin password.

Step 3  Right-click on the desktop.
Step 4  From the menu, select New Terminal.
This brings up a terminal session.
Step 5  Restore the data by entering the following:

```
sudo $MP_DATABASE/db-maintenance/restore.sh
```
Step 6  At the system prompt, press S to stop the Cisco Unified MeetingPlace application.
Step 7  Choose the type of restore you want. Press A for archive or L for the local disk.
Step 8  If you pressed L, then press Enter three times.
Step 9  If you pressed A, then complete these steps:
   a. Copy all files from the opt/cisco/meetingplace/licenses folder of your latest archive location to the
      /opt/cisco/meetingplace/licenses folder.
   b. Press Enter.
   c. Copy all files from the opt/cisco/meetingplace/afs/custom folder of your latest archive location to
      the /opt/cisco/meetingplace/afs/custom folder.
   d. Press Enter.
   e. Copy all files from the mpx-record folder of your latest archive location to the /mpx-record folder.
   f. Press Enter.
Step 10 Choose an entry from the displayed list of backups,
Step 11 Enter the number associated with the backup entry.
Step 12 When prompted, press R to perform the restore.
When the system finishes the archive, it displays the message: “You restored database successfully.”
If you are restoring an Application Server that is configured in a failover deployment, reboot the server
after the restore is completed.

![Note]
If the server needs to be in active mode after it reboots, switch it to active mode.

Step 13 On the desktop, select RedHat > Network Services.
Step 14 Select Log out.

**Troubleshooting Tips**
- If you restore archived data after you reinstall Cisco Unified MeetingPlace Web Conferencing or the
  entire Cisco Unified MeetingPlace system, the system may not find meetings because the
  Application Server cannot reach the Web Server. If this occurs, then you need to manually edit the
  Web Server connection to use the new Installation key which changed during the reinstallation
  process. For details, see “Adding or Editing a Web Server Connection” in the Connecting the
  Cisco Unified MeetingPlace Application Server to a Web Server module.
- If the Web Server page in the Administration Center appears to have duplicate entries after
  completing the restore, make the old entries inactive, then log in to the Application Server CLI as
  root user and use the gwstatus command to verify that the inactive entries have been removed.

**Related Topics**
- About Database Backups, Archives, and Restoration, page 1
• **How to Back Up, Archive, and Restore Data, page 4**
• **Sending E-Mail Blasts from Cisco Unified MeetingPlace module**

**What To Do Next**

When updating (synchronizing) all meetings on the Web Server, the system purges all the data for meetings that do not exist on the Application Server. Therefore, the next time you or the system updates all meetings, the system purges the following from the Web Server:

- Recordings and attachments for meetings that occurred between the backup time and the restore time.
- Meetings that were scheduled between the backup time and the restore time.

Nevertheless, you or your users may save local copies of recordings before they are purged. You can use an e-mail blast to inform your users of the following:

- Time period (between the most recent backup time and the restore time) of affected meetings.
- Deadline for saving local copies of recordings. This is determined by the next update-all-meetings event, which occurs automatically at midnight every Saturday night (local server time), or when you complete the “Updating All Meetings” section in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module.

If you restored two application servers that were configured in a failover deployment, complete the failover setup on Node 1 and Node 2.

**Related Topics**

- **About Database Backups, Archives, and Restoration**
- **Configuring the Application Servers in a Failover Deployment**
- **Sending E-Mail Blasts from Cisco Unified MeetingPlace**
- **How to Configure Application Server Failover in the Configuring Application Server Failover for Cisco Unified MeetingPlace module**
You can deploy two Application Servers as part of one logical site. Database replication enables the Application Servers to synchronize user profiles, user groups, and meeting data. Only one Application Server is active at any time. If the active server fails, then you can activate the standby server and place the previously active server in standby mode. Each Application Server in a site is called a node.

If the site includes two Media Servers, then one Media Server will be associated with each Application Server. If the site includes only one Media Server, then it is always associated with the active Application Server.

In a failover deployment, each Application Server is configured with two IP addresses—one for each of the following interfaces:

- **eth0**—Physical network interface
  - Assign the same shared hostname and IP address to eth0 on both Application Servers.
  - Anyone who tries to access the shared hostname or IP address will reach the active Application Server.
  - The eth0 interface is disabled on the standby Application Server.

- **eth0:0**—Virtual network interface
  - Assign a unique hostname and IP address to eth0:0 on each Application Server.
  - Use the eth0:0 hostname or IP address to access an Application Server that is in standby mode.
  - The system uses the eth0:0 virtual network interface for database replication between the two nodes.
Prerequisites for Application Server Failover


Determine the hostname, IP address, subnet mask, and default gateway for each of the following:

- Node 1 eth0 and Node 2 eth0—Shared hostname and IP address, for example: meetings.example.com, 10.0.0.1
- Node 1 eth0:0—Unique hostname and IP address, for example: meetings1.example.com, 10.0.0.2
- Node 2 eth0:0—Unique hostname and IP address, for example: meetings2.example.com, 10.0.0.3

Configure the Domain Name System (DNS) server for forward and reverse DNS lookup of all three hostname–IP address pairs. Verify by running the nslookup hostname and nslookup ip-address commands.

Whether you configure Application Server failover before or after you install any Web Server(s) and your call-control devices (such as Cisco Unified Communications Manager), make sure that these devices identify the active Application Server by using the shared hostname and IP address of eth0.
Restrictions for Application Server Failover

- Not all Application Server configurations are replicated between the active and standby servers. If you make any configuration changes after you set up Application Server failover, make sure you follow the “Configuring the Application Servers in a Failover Deployment” section on page 8.
- Directory Service between two Application Servers is not supported in a failover deployment.
- Only the database, Apache Tomcat, and SIM processes run on a standby server, which you will notice if you enter the `mpx_sys status` command on the standby server.
- Do not leave a standby server out of production for a long time, as that can cause the primary server to fail. If the standby server must be brought down for days or weeks at a time, disable replication during this time.
- To use Single Sign On (SSO) authentication with Microsoft Outlook in a failover environment, you must install SSL on both the active server and the standby server.
- If you are using SSL on your system, you must manually transfer all files in the following directories from the active server to the standby server:
  - `/usr/local/enrollment` (for Application Server SSL and single sign-on authentication for users who schedule meetings from Microsoft Outlook)
  - `/opt/cisco/meetingplace/web/current/etc/conf/` (for Cisco WebEx integration)
  Copy the files by using the `failoverUtil copyConfigFiles` command and restore files by using the `failoverUtil restoreConfigFiles` command.

How to Configure Application Server Failover

- Setting Up Failover for Two Newly Installed Application Servers, page 4
- Setting Up Failover for One Existing Application Server and One Newly Installed Application Server, page 6
Setting Up Failover for Two Newly Installed Application Servers

Before You Begin
- Complete the “Prerequisites for Application Server Failover” section on page 2.
- Read the “Restrictions for Application Server Failover” section on page 3.

Procedure

Step 1 Install the first Application Server (Node 1).
During installation, you configure the hostname and IP address of eth0, which is called “Ethernet Port 1(device eth0)” on the Network Setup page.


Step 3 Log in to the CLI of Node 1.
If you are logging in remotely, use the eth0 IP address or hostname.

Step 4 Enter the following command to set up Node 1 for failover:
failoverUtil setDeployment failover

Step 5 Follow the CLI prompts to configure the virtual network interface (eth0:0) with an IP address, subnet mask, default gateway, and hostname.
Node 1 automatically restarts and enters standby mode.

Step 6 Install the second Application Server (Node 2), ensuring the following:
- Node 1 and Node 2 use the exact same IP address and hostname for eth0.
- Time is synchronized between Node 1 and Node 2.

Step 7 Install any licenses on the second Application Server (Node 2) in active mode and reboot the system. For information about licenses, see the About Licenses module in the Planning Guide for Cisco Unified MeetingPlace 7.1 at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html.

Step 8 Log in to the CLI of Node 2.
If you are logging in remotely, use the eth0 IP address or hostname.

Step 9 Enter the following command to set up Node 2 for failover:
failoverUtil setDeployment failover

Step 10 Follow the CLI prompts to configure the virtual network interface (eth0:0) with an IP address, subnet mask, default gateway, and hostname.
Node 2 automatically restarts and enters standby mode.

Step 11 Enter the following command to initialize database replication:
mp_replication init -n 2 -r remote-eth0:0 [-v]
Step 12 Log in to the CLI of Node 1.
If you are logging in remotely, use the Node 1 eth0:0 IP address or hostname.

Step 13 Enter the following commands to initialize and start database replication:
```
mp_replication init -n 1 -r remote-eth0:0 [-v]
mp_replication switchON [-v]
```

Step 14 Enter the following command to change Node 1 from standby mode to active mode:
```
failoverUtil setServer active
```

Note Node must be active to add licenses (step 7).

Verifying
Using the hostname or IP address of the virtual eth0:0 interface, log in to the Administration Center of each node, and verify that the correct failover deployment mode (active or standby) appears at the top of the page.

To verify that the replication was successful, log in to both nodes (eth0:0 interface) as root user and enter the `mp_replication status` command. The following should display in your output:

<table>
<thead>
<tr>
<th>Local Server</th>
<th>Remote Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication Type: Local</td>
<td>Replication Type: Intra-site</td>
</tr>
<tr>
<td>Site: 1</td>
<td>Site: 1</td>
</tr>
<tr>
<td>Node: 1</td>
<td>Node: 2</td>
</tr>
<tr>
<td>State: Active</td>
<td>State: Active</td>
</tr>
<tr>
<td>Status: Local</td>
<td>Status: Connected</td>
</tr>
</tbody>
</table>

Troubleshooting Tips
- If the Administration Center in both nodes displays “Failover deployment. Standby server,” then something may have interrupted the process initiated in Step 14. To resolve this issue, see the `failoverUtil setDeployment failover` command description in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module.
- If you switch on replication with sync via the `mp_replication switchON` command and replication fails, it is possible that a table is locking due to the processes on an active server. To resolve this issue, run the `mp_replication switchON` with sync command again.
- During this process, you may see several error messages. These error messages are expected behavior and informational only. The final message of the command explicitly says if the command ran successfully or not.
  An example of an error message that you can ignore is:
Configuring Application Server Failover for Cisco Unified MeetingPlace

How to Configure Application Server Failover

* Error: '/opt/cisco/meetingplace/database/versions/IIF.10.00.UC5XL/etc/sqlhosts not initialized. xxxxxx is missing'
* Forcing the fix

The final message, which indicates if the process was successful, is:

Database Replication changes for this machine (Host = <hostname>; IP Addr = <ip addr>) is SUCCESSFUL

Related Topics
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module

What To Do Next
Proceed to the “Configuring the Application Servers in a Failover Deployment” section on page 8.

Setting Up Failover for One Existing Application Server and One Newly Installed Application Server

In this task:
- Node 1 is the existing Application Server.
- Node 2 is the new Application Server.

Before You Begin
- Complete the “Prerequisites for Application Server Failover” section on page 2.
- Read the “Restrictions for Application Server Failover” section on page 3.
- Back up and archive the data on the existing Application Server (Node 1). See the Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module.

Caution
Performing this task temporarily brings down your Cisco Unified MeetingPlace system. Proceed only during a scheduled maintenance period.

Procedure

Step 1
Install the second Application Server (Node 2), ensuring the following:
- To reduce system downtime during this procedure, enter the Node 2 eth0:0 (or any valid and currently unused) IP address and hostname when you configure “Ethernet Port 1(device eth0)” on the Network Setup page.
  - This configuration is temporary; you will change the eth0 IP address and hostname to the correct value later in this procedure.
- Node 1 and Node 2 server times must be synchronized with each other.

Step 2
Log in to the CLI of Node 1.
If you are logging in remotely, use the Node 1 eth0 IP address or hostname.
Step 3  Enter the following command to set up Node 1 for failover:

\texttt{failoverUtil setDeployment failover}

Step 4  Follow the CLI prompts to configure the virtual network interface (eth0:0) with an IP address, subnet mask, default gateway, and hostname.

Node 1 automatically restarts and enters \textit{standby} mode.

Step 5  Log in to the CLI of Node 2.

If you are logging in remotely, use the temporary Node 2 eth0 IP address or hostname that you entered during installation in Step 1.

Step 6  Enter the \texttt{net} command to change the Node 2 eth0 IP address and hostname to match the Node 1 eth0 IP address and hostname.

Because Node 1 is still in standby mode, Node 2 is now the active server.

Step 7  Enter \texttt{reboot} to restart Node 2.

Step 8  Log in to the CLI of Node 2, this time using the shared eth0 IP address or hostname.

Step 9  Enter the following command to set up Node 2 for failover:

\texttt{failoverUtil setDeployment failover}

Step 10 Follow the CLI prompts to configure the virtual network interface (eth0:0) with an IP address, subnet mask, default gateway, and hostname.

Node 2 automatically restarts and enters \textit{standby} mode.

Step 11 Enter the following command to initialize database replication:

\texttt{mp\_replication init -n 2 -r remote-eth0:0 [-v]}

Step 12 Log in to the CLI of Node 1.

If you are logging in remotely, use the Node 1 eth0:0 IP address or hostname.

Step 13 Enter the following commands to initialize and start database replication and synchronize existing data:

\texttt{mp\_replication init -n 1 -r remote-eth0:0 [-v]}

\texttt{mp\_replication switchON -S -F from-sync [-v]}

Step 14 Enter the following command to change Node 1 from standby mode to active mode:

\texttt{failoverUtil setServer active}

\section*{Verifying}

Using the hostname or IP address of the virtual eth0:0 interface, log in to the Administration Center of each node, and verify that the correct failover deployment mode (active or standby) appears at the top of the page.

To verify that the replication was successful, log in to both nodes (eth0:0 interface) as root user and enter the \texttt{mp\_replication status} command. The following should display in your output:

<table>
<thead>
<tr>
<th>Local Server</th>
<th>Remote Server</th>
</tr>
</thead>
<tbody>
<tr>
<td>Replication Type: Local</td>
<td>Replication Type: Intra-site</td>
</tr>
<tr>
<td>Site: 1</td>
<td>Site: 1</td>
</tr>
<tr>
<td>Node: 1</td>
<td>Node: 2</td>
</tr>
</tbody>
</table>
Configuring Application Server Failover for Cisco Unified MeetingPlace

How to Configure Application Server Failover

Troubleshooting Tips

- If the Administration Center in both nodes displays “Failover deployment. Standby server,” then something may have interrupted the process initiated in Step 14. To resolve this issue, see the failoverUtil setDeployment failover command description in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module.

- If you switch on replication with sync via the mp_replication switchON command and replication fails, it is possible that a table is locking due to the processes on an active server. To resolve this issue, run the mp_replication switchON with sync command again.

- During this process, you may see several error messages. These error messages are expected behavior and informational only. The final message of the command explicitly says if the command ran successfully or not.

An example of an error message that you can ignore is:

* Error: '/opt/cisco/meetingplace/database/versions/IIF.10.00.UC5XL/etc/sqlhosts not initialized. xxxxxx is missing'
* Forcing the fix

The final message, which indicates if the process was successful, is:

Database Replication changes for this machine (Host = <hostname>; IP Addr = <ip addr>) is SUCCESSFUL

Related Topics

- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module

What To Do Next

Proceed to the “Configuring the Application Servers in a Failover Deployment” section on page 8.

Configuring the Application Servers in a Failover Deployment

Whenever you need to configure the Application Server in a failover deployment, use this procedure to make sure that both the active and standby servers have the same configuration.

Before You Begin

- Complete one of the following tasks:
  - Setting Up Failover for Two Newly Installed Application Servers, page 4
  - Setting Up Failover for One Existing Application Server and One Newly Installed Application Server, page 6
- Determine the hostname or IP address of both of the following virtual network interfaces:
  - eth0:0 of the active server
Configuring Application Server Failover for Cisco Unified MeetingPlace

How to Configure Application Server Failover

- eth0:0 of the standby server

Procedure

Step 1
Go to [http://application-server/admin/](http://application-server/admin/).
Use the shared eth0 hostname or IP address, which always goes to the active Application Server.

Step 2
Log in as a System administrator.

Step 3
Configure the active server.
Take note of any changes you make on pages or fields that are labeled as:
- Copied
- Server-specific
- Partially replicated

Step 4
If you made changes to any copied pages or parameters, then perform the following steps:

a. Log in to the CLI of the active server.
   If you are logging in remotely, use the eth0 IP address or hostname.

b. Enter the following command to compress and transfer the files from the active server to the standby server:
   ```
   failoverUtil copyConfigFiles
   ```

c. Log in to the CLI of the standby server.
   If you are logging in remotely, use eth0:0 IP address or hostname.

d. Enter the following command to decompress the transferred files and put them in the correct directories on the standby server:
   ```
   failoverUtil restoreConfigFiles
   ```

Step 5
If you made changes to any server-specific pages or parameters, then perform the following steps.

Tip
If your workstation screen is large enough to accommodate two full web browser windows without overlapping, then you can simultaneously view the Administration Center for both the active and standby servers. This may help you configure the server-specific parameters to match between the active and standby servers.

a. Go to [http://standby-eth0:0/admin/](http://standby-eth0:0/admin/).
   Use either the hostname or IP address of the virtual eth0:0 interface of the standby Application Server.

b. Log in as a System administrator.

c. Verify that “Failover deployment. Standby server.” appears at the top of the page.

d. Configure the server-specific parameters on the standby server.
What to Do Next

Perform the following from both Application Servers to replicate custom prompts and some configurations from the Primary application server to the Standby application server during a maintenance window or off-peak hours.

Step 1
Log in to the CLI of the active server.

Step 2
If you are logging in remotely, use the eth0 IP address or hostname.

Step 3
Enter the following command to compress and transfer the files from the active server to the standby server:

```
failoverUtil copyConfigFiles
```

This will compress and copy over configuration files and user prompts to the remote server.

Step 4
Log in to the CLI of the standby server.

Step 5
If you are logging in remotely, use eth0:0 IP address or hostname.

Step 6
Enter the following command to decompress the transferred files and put them in the correct directories on the standby server:

```
failoverUtil restoreConfigFiles
```

This action copies over custom prompts including customized system prompts and user name recordings. Without this action .wav files are not replicated to the standby server.

Related Topics
- Logging In to the Cisco Unified MeetingPlace Administration Center module
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Integrating Cisco Unified MeetingPlace with Cisco WebEx module
- Customizing Music and Voice Prompts for Cisco Unified MeetingPlace module
- How to Perform Application Server Failover, page 10

About the Active and Standby Application Server Database

If the active or standby application server database exceeds the specified size, an alarm is sent. The active application server also outdials the administrator to indicate the alarm condition.

How to Perform Application Server Failover

- Performing Application Server Failover, page 11
- Performing Application Server Failover to Switch to the Previous Active Server, page 12
Performing Application Server Failover

Before you perform this task:

- Node 1 is the current active server.
- Node 2 is the current standby server.

After you complete the task:

- Node 1 will be the standby server.
- Node 2 will be the active server.

Before You Begin

Set up Application Server failover by completing one of the following sections:

- Setting Up Failover for Two Newly Installed Application Servers, page 4
- Setting Up Failover for One Existing Application Server and One Newly Installed Application Server, page 6

Caution

Performing this task temporarily brings down your Cisco Unified MeetingPlace system. Perform this task only if the current active server fails, or during a scheduled maintenance period.

Procedure

Step 1

If the Node 1 is up, then complete the following steps:

a. Log in to the CLI of Node 1.
   If you are logging in remotely, use the Node 1 eth0:0 IP address or hostname.

b. Enter the following command to change the server to standby mode:

   `failoverUtil setServer standby`

Step 2

Log in to the CLI of Node 2.

If you are logging in remotely, use the Node 2 eth0:0 IP address or hostname.

Step 3

Enter the following command to change the server to active mode:

`failoverUtil setServer active`

Verifying

Using the hostname or IP address of the virtual eth0:0 interface, log in to the Administration Center of each node, and verify that the correct failover deployment mode (active or standby) appears at the top of the page.

Troubleshooting Tips

If the Administration Center displays the wrong failover mode on either or both servers, then something may have interrupted the process initiated by the `failoverUtil setDeployment failover` command. To resolve this issue, see the `failoverUtil setDeployment failover` command description in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module.
Performing Application Server Failover to Switch to the Previous Active Server

Before you perform this task:

- Node 1 is the current standby server.
- Node 2 is the current active server.

After you complete the task:

- Node 1 will be the active server.
- Node 2 will be the standby server.

Caution

Performing this task temporarily brings down your Cisco Unified MeetingPlace system. Perform this task only if the current active server fails, or during a maintenance period.

- Complete the “Prerequisites for Application Server Failover” section on page 2.
- Back up and archive the data on the currently active Application Server (Node 1). See the Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module.

Procedure

Step 1

If Node 1 was brought to single-server mode, then you will need to do the following:

a. Log in to the Node 1 CLI using the console.
b. Enter the following command to set up failover:
   ```
   failoverUtil setDeployment failover
   ```
c. Follow the CLI prompts to configure the virtual network interface (eth0:0) with an IP address, subnet mask, default gateway, and hostname.

   Node 1 automatically restarts and enters standby mode.

Step 2

Log in to the CLI of Node 1.

If you are logging in remotely, use the Node 1 eth0:0 IP address or hostname.

Step 3

If the database replication configuration was removed from Node 1, then enter the following command to initialize database replication:

```mp_replication init -n 1 -r remote-eth0:0 [-v]```

Step 4

Log in to the CLI of Node 2.

Step 5

Enter the following command to change Node 2 to standby mode:

```failoverUtil setServer standby```

Step 6

Log in to the CLI of Node 1.
Step 7  Enter the following command to synchronize existing data from Node 2 and start database replication:

```
mp_replication switchON [-S -F from-sync] [-v]
```

Step 8  Enter the following command to change Node 1 to *active* mode:

```
failoverUtil setServer active
```

---

**Verifying**

Using the hostname or IP address of the virtual eth0:0 interface, log in to the Administration Center of each node, and verify that the correct failover deployment mode (active or standby) appears at the top of the page.

**Troubleshooting Tips**

If the Administration Center displays the wrong failover mode on either or both servers, then something may have interrupted the process initiated by the `failoverUtil setDeployment failover` command. To resolve this issue, see the `failoverUtil setDeployment failover` command description in the Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module.

**Related Topics**

- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Performing Application Server Failover, page 11
Configuring Application Server Failover for Cisco Unified MeetingPlace

How to Perform Application Server Failover
Requirements for Importing Data

The following requirements apply to user groups, user profiles, video terminal profiles, and meetings:

- Import files must use the comma-separated value (CSV) format.
- The first or second line of the import file contains header fields that specify the order in which data appears in all subsequent lines. The header fields may be in any order.
  
  If the second line contains the header fields, then the first line of the import file contains the product version information, which must exactly match the first line of an equivalent export file from the same Cisco Unified MeetingPlace system.
  
- All subsequent lines of the import file contain the actual data. The data must appear in the order specified in the first line of the import file.
- Each import file must contain the required headers specified in Table 1. For all optional header fields that are not included in the import file, the system uses the default value for the import data.

<table>
<thead>
<tr>
<th>Type of Import File</th>
<th>Purpose</th>
<th>Required Header Fields</th>
</tr>
</thead>
</table>
| User groups         | Adding or deleting | • grpnum
|                     |                   | • Name

Table 1 Required Headers in Import Files
Requirements for Importing Data

If you are importing data that was previously exported, then the field values must retain any leading zeros (0) that were in the original export file.

If you lose the leading zeros, then you will see import errors. For example, if you try to import user profiles whose group numbers are missing leading zeros, then import errors will indicate that the user group cannot be found.

Note that some spreadsheet applications, such as Microsoft Excel, automatically delete leading zeros (0) from cells that the application formats as numbers. See the documentation for your spreadsheet application to make sure that all fields are treated as text instead of numbers.

### Table 1 Required Headers in Import Files

<table>
<thead>
<tr>
<th>Type of Import File</th>
<th>Purpose</th>
<th>Required Header Fields</th>
</tr>
</thead>
<tbody>
<tr>
<td>User profiles</td>
<td>Adding</td>
<td>• EncryptedProfilePWD or prfpwd (for locally authenticated users), or ProfilePWD (for externally authenticated users)</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• EncryptedUserPWD or upwd</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• prfnum</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• uid</td>
</tr>
<tr>
<td></td>
<td>Deleting</td>
<td>• prfnum</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• uid</td>
</tr>
<tr>
<td>Video terminal profiles</td>
<td>Adding</td>
<td>Release 7.0.2 and later releases:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• videoTermName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• videoTermId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• videoEndPtAddStr</td>
</tr>
<tr>
<td></td>
<td>Deleting</td>
<td>Release 7.0.2 and later releases:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• videoTermName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Release 7.0.1:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• uid</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• videoTermName</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• videoTermId</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• videoEndPtAddStr</td>
</tr>
<tr>
<td>Meetings</td>
<td>Scheduling or canceling</td>
<td>• DialableConfID</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ReqLengthOfConf</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• StartDateTimeOfConf</td>
</tr>
</tbody>
</table>
• All values in the import file must be valid. Otherwise, the import file may introduce incorrect relationships in the database and cause erratic system behavior. For descriptions of available import fields, see the following sections of the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module:
  – Import and Export Data Specifications for User Groups
  – Import and Export Data Specifications for User Profiles
  – Import and Export Data Specifications for Video Terminal Profiles
  – Import and Export Data Specifications for Meetings
• The following notes apply to the import file:
  – 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 “Smith, John” for a user ID.
  – All text is case insensitive.

Related Topics
• How To Import Data, page 3
• Examples of Import Files, page 15

How To Import Data

• Setting Up an Import File, page 3
• Adding or Editing User Groups by Import, page 5
• Deleting User Groups by Import, page 6
• Adding or Editing User Profiles by Import, page 7
• Deleting User Profiles by Import, page 8
• Adding or Editing Video Terminal Profiles by Import, page 9
• Deleting Video Terminal Profiles by Import, page 11
• Importing Remote Servers, page 12
• Importing Meeting Categories, page 12
• Scheduling Meetings by Import, page 13
• Canceling Meetings by Import, page 14
• Importing the System Configuration, page 14

Setting Up an Import File

Before You Begin
• Read the “Requirements for Importing Data” section on page 1.
Create an import file template by exporting a similar file that includes field header names. See one of the following sections in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module:

- Exporting User Groups
- Exporting User Profiles
- Exporting Video Terminal Profiles
- Exporting Meetings

Care should be taken when opening a Cisco Unified MeetingPlace export file using Microsoft Excel, which by default removes any leading zeros(0) in the data and results in import errors. For example, to preserve leading zeros (0) in the data using Microsoft Excel 2007:

a. Select Data > From Text.
b. Open the .CSV export file. This launches the File Import Wizard.
c. During Step 3 of the File Import Wizard, you can select the Data Format for each column. By default, Microsoft Excel uses General formatting, which removes all leading zeros (0). Make sure you do the following:
   • Select the column for numbers
   • Under Column data format, select the Text radio button.
   • Repeat this procedure for any other columns. When finished make sure to verify data.

Procedure

Step 1 Use a spreadsheet application, such as Excel, to open a previously exported file.

Step 2 In the spreadsheet application, the required headings are listed in the second row, and the data is listed in all subsequent rows. Perform one of the following actions:

   • If you are modifying existing entries, then delete the rows that you do not want to modify. Do not delete the first two rows.
   • If you are adding entirely new entries, then delete all rows except the first two rows.

Step 3 Enter or modify the information in the appropriate fields.

Caution Make sure that all values in the import file are valid. Invalid entries in the import file may introduce incorrect relationships in the database and cause erratic system behavior.

If you are unsure about what to enter in any field, then we recommend that you delete that entire column (unless it is a required field). For descriptions of each field, see the following sections of the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module:

- Import and Export Data Specifications for User Groups
- Import and Export Data Specifications for User Profiles
- Import and Export Data Specifications for Video Terminal Profiles
- Import and Export Data Specifications for Meetings

Step 4 Save and close the file.
Adding or Editing User Groups by Import

Before You Begin

- If you instead want to add user groups one at a time, then see the “Adding or Editing a User Group Manually” section on page 2.
- Read the “Requirements for Importing Data” section on page 1.
- Create the import file. See the “Setting Up an Import File” section on page 3.
- Unspecified fields for new user groups in the import file use default values from the preconfigured System group.

Restriction

If the import file contains the tzcode header field, then all user groups in the import file must have a valid entry for the field. For any invalid or blank tzcode values, the associated user group is not imported, and an error is logged.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Administration Center.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select <strong>Maintenance &gt; Import Data &gt; Import User Groups</strong>.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Enter values in the fields.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Select <strong>Execute</strong>.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Select <strong>OK</strong> to confirm your request to import records.</td>
</tr>
<tr>
<td>Step 6</td>
<td>The system displays the import status and provides a link to the import log:</td>
</tr>
<tr>
<td></td>
<td>- Select the link to view the import log, which you may print.</td>
</tr>
<tr>
<td></td>
<td>- Select <strong>OK</strong> to close the page.</td>
</tr>
</tbody>
</table>

After you select **OK**, the import log can no longer be viewed or retrieved.

Related Topics

- Examples of Import Files, page 15
- Import User Groups Page, page 49
- System User Group in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module
What To Do Next

Proceed to “Updating All Groups” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module if you want the new or modified user group settings to take effect immediately. Otherwise, any changes or additions you make will take effect after the next Replication Service update, which occurs nightly.

Deleting User Groups by Import

Note

If you want to delete user groups one at a time, see the “Deleting a User Group” section on page 4.

Before You Begin

- Create the import file. See the “Setting Up an Import File” section on page 3.
- Make sure that the import file contains only the user groups that you want to delete.

Restrictions

- You cannot delete the group called system.
- Deleting user groups is an irreversible operation. Before you delete user groups, consider creating a backup copy so that you can later retrieve the deleted user groups if necessary. Use one of the following options:
  - Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module
  - Exporting User Groups in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Maintenance > Import Data > Import User Groups.
Step 3  Enter values in the fields.
  - In the Action to perform field, select “Delete groups from system.”
  - Ignore the Overwrite duplicate information field. Its value does not affect the process.
Step 4  Select Execute.
Step 5  Select OK to confirm your request to import records.
Step 6  The system displays the import status and provides a link to the import log:
  - Select the link to view the import log, which you may print.
  - Select OK to close the page.

After you select OK, the import log can no longer be viewed or retrieved.
You can import user profiles by using a spreadsheet in CSV text file format. This option can be useful for:

- Making minor changes to a large number of user profiles, such as globally changing the domain name in all e-mail addresses.
- Company mergers or initial setup of user profiles when Directory Service is not an option.

**Before You Begin**

- If you instead want to add user profiles one at a time, see the “Adding User Profiles Manually” section on page 8.
- Read the “Requirements for Importing Data” section on page 1.
- Create the import file. See the “Setting Up an Import File” section on page 3.
- Unspecified fields for new user profiles in the import file use default values from the preconfigured guest profile.

**Restrictions**

- You cannot use the import process to modify the User ID (uid) or the Profile number (prfnum) of existing user profiles in the database.
- If the import file contains the tzcode header field, all user profiles in the import file must have a valid entry for the field. For any invalid or blank tzcode values, the associated user profile is not imported, and an error is logged.
- If the import file contains the grpnme, grpnum, or both header fields, all user profiles in the import file must have a valid entry for each included field. Specifically:
  - Import user groups before you import user profiles.
  - If any grpnme and grpnum fields are left blank in the import file, the associated user profiles are not imported, and an error is logged.
  - If any user groups that are specified in the grpnme and grpnum fields do not already exist in the Cisco Unified MeetingPlace database, the associated user profiles are not imported, and an error is logged.
- If the import file does not contain the grpnme or grpnum header fields, the imported user profiles are automatically assigned to the preconfigured System User Group.
- You can import a maximum of 250,000 user profiles.

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Select Maintenance > Import Data > Import User Profiles.

**Step 3** Enter values in the fields.
How To Import Data

Step 4   Select Execute.
Step 5   Select OK to confirm your request to import records.
Step 6   The system displays the import status and provides a link to the import log:
   • Select the link to view the import log, which you may print.
   • Select OK to close the page.
After you select OK, the import log can no longer be viewed or retrieved.

Related Topics
   • Examples of Import Files, page 15
   • Field Reference: Import User Groups Page in the Administration Center Page References for Cisco Unified MeetingPlace module
   • Guest Profile Fields That Apply to New User Profiles in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
   • Methods for Adding User Profiles in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
   • Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

What To Do Next
Proceed to “Updating All User Profiles” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module if any of the following apply to you:
   • You want new user profiles to be available immediately for meeting invitations.
   • You want modified user profile settings to take effect immediately.
Otherwise, any changes or additions you make will take effect after the next Replication Service update, which occurs nightly.

Deleting User Profiles by Import

Before You Begin
   • If you instead want to delete user profiles one at a time, see the “Deleting a User Profile” section on page 10.
   • See the “Requirements for Importing Data” section on page 1.
   • Create the import file. See the “Setting Up an Import File” section on page 3.
   • Make sure that the import file contains only the user profiles that you want to delete.
   • Deleting user profiles is an irreversible operation. Before you delete user profiles, consider creating a backup copy so that you can later retrieve the deleted user profiles if necessary. Use one of the following options:
      – Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module
      – Exporting User Profiles in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
Restrictions

- (Cisco WebEx integration only) Deleting user profiles on Cisco Unified MeetingPlace does not disable access to Cisco WebEx. You must also deactivate those users through the Cisco WebEx Site Administration.
- You cannot delete the preconfigured admin, guest, or recorder user profiles, nor can you delete the user profile with which you are currently logged in.
- If the import file contains the grpnme or grpnum header fields, all user profiles in the import file must have a valid entry for the field. For any invalid or blank values, the associated user profile is not deleted by import.

Procedure

**Step 1** Log in to the Administration Center.

**Step 2** Select Maintenance > Import Data > Import User Profiles.

**Step 3** Enter values in the fields.

In the Action to perform field, select Delete users from system.

**Step 4** Select Execute.

**Step 5** Select OK to confirm your request to import records.

**Step 6** The system displays the import status and provides a link to the import log:
- Select the link to view the import log, which you may print.
- Select OK to close the page.

After you select OK, the import log can no longer be viewed or retrieved.

Related Topics

- Examples of Import Files, page 15
- Field Reference: Import User Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Deactivating Cisco WebEx User Profiles in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module

Adding or Editing Video Terminal Profiles by Import

You can import video terminal profiles by using a spreadsheet in CSV text file format.

**Before You Begin**

- If you instead want to add VTPs one at a time, see “Adding or Editing a Video Terminal Profile” in the Configuring Endpoints for Cisco Unified MeetingPlace module.
- Read the “Requirements for Importing Data” section on page 1.
- Create the import file. See the “Setting Up an Import File” section on page 3.
Restrictions

- You cannot use the import process to modify the user ID (uid), profile number (prfnum), or video terminal ID (videoTermId) of existing VTPs in the database.
- If the import file contains the tzcode header field, all VTPs in the import file must have a valid entry for the field. For any invalid or blank tzcode values, the associated VTP is not imported, and an error is logged.
- If the import file contains the grpnme, grpnum, or both header fields, all VTPs in the import file must have a valid entry for each included field. Specifically:
  - Import user groups before you import VTPs.
  - If any grpnme and grpnum fields are left blank in the import file, the associated VTPs are not imported, and an error is logged.
  - If any user groups that are specified in the grpnme and grpnum fields do not already exist in the Cisco Unified MeetingPlace database, the associated VTPs are not imported, and an error is logged.
- If the import file does not contain the grpnme or grpnum header fields, the imported VTPs are automatically assigned to the preconfigured System User Group.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Import Data > Import Video Terminal Profiles.
Step 3 Enter values in the fields.
Step 4 Select Execute.
Step 5 Select OK to confirm your request to import records.
Step 6 The system displays the import status and provides a link to the import log:
  - Select the link to view the import log, which you may print.
  - Select OK to close the page.

After you select OK, the import log can no longer be viewed or retrieved.

Related Topics

- Examples of Import Files, page 15
- Field Reference: Import Video Terminal Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

What To Do Next

Proceed to “Updating All Video Terminals” in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module if any of the following apply to you:

- You want new VTPs to be available immediately for meeting invitations.
- You want any modified VTP settings to take effect immediately.
Otherwise, any changes or additions you make will take effect after the next Replication Service update, which occurs nightly.

Deleting Video Terminal Profiles by Import

Before You Begin

- If you instead want to delete VTPs one at a time, see “Adding or Editing a Video Terminal Profile” in the Configuring Endpoints for Cisco Unified MeetingPlace module.
- See the “Requirements for Importing Data” section on page 1.
- Create the import file. See the “Setting Up an Import File” section on page 3.
- Make sure that the import file contains only the VTPs that you want to delete.
- Deleting VTPs is an irreversible operation. Before you proceed, consider creating a backup copy so that you can later retrieve the deleted VTPs if necessary. Use one of the following options:
  - Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module
  - Exporting Video Terminal Profiles in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module

Restriction

If the import file contains the grpnme, grpnum, or both header fields, all VTPs in the import file must have a valid entry for the field. For any invalid or blank values, the associated VTP is not deleted by import.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Import Data > Import Video Terminal Profiles.
Step 3 Enter values in the fields.
   In the Action to perform field, select Delete video terminal profiles from system.
Step 4 Select Execute.
Step 5 Select OK to confirm your request to import records.
Step 6 The system displays the import status and provides a link to the import log:
   - Select the link to view the import log, which you may print.
   - Select OK to close the page.

After you select OK, the import log can no longer be viewed or retrieved.

Related Topics

- Examples of Import Files, page 15
- Field Reference: Import Video Terminal Profiles Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Importing Remote Servers

Before You Begin
Find the previously exported remote servers file.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Import Data > Import Remote Servers.
Step 3 Enter the filename or select Browse to find the system configuration file.
Step 4 Choose whether to overwrite duplicate information.
Step 5 Select Execute.

Related Topics
- Exporting Remote Servers in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module

Importing Meeting Categories

Before You Begin
Find the previously exported meeting categories file.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Import Data > Import Meeting Categories.
Step 3 Enter the filename or select Browse to find the system configuration file.
Step 4 Choose whether to overwrite duplicate information.
Step 5 Select Execute.

Related Topics
- Exporting Meeting Categories in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
- Configuring Meeting Categories in the Configuring Meetings for Cisco Unified MeetingPlace module
Scheduling Meetings by Import

Use this procedure to schedule meetings by import. Although you can schedule meetings individually from the end-user web interface, you can schedule multiple meetings at one time by following this procedure.

Before You Begin
Create the import file. See the “Setting Up an Import File” section on page 3.

Restrictions
- An imported meeting cannot be scheduled if any of the following conditions are true:
  - The SchedulerUid field in the import file is blank, and a substitute username is not configured in the Scheduler user ID field on the Import Meetings page.
  - There are not enough voice or web ports available for the imported meeting.
- If the username in the SchedulerUid field does not correspond to an existing user profile, the import process replaces the SchedulerUid entry with the value entered in the Scheduler user ID field on the Import Meetings page.
- Continuous and recurring meetings are scheduled starting from the current time; meeting information from the past is not imported.
- When recurring meetings are imported to Cisco Unified MeetingPlace, each occurrence in the import file is scheduled as an individual meeting with no recurrence pattern.
- You can import a maximum of 400,000 meetings.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Import Data > Import Meetings.
Step 3 Enter values in the fields.
Step 4 Select Execute.
Step 5 Select OK to confirm your request to import the meeting records.
Step 6 The system displays the import status and provides a link to the meeting import log:
  - Select the link to view the import log, which you may print.
  - Select OK to close the page.
After you select OK, the meeting import log can no longer be viewed or retrieved.

Related Topics
- Examples of Import Files, page 15
- Field Reference: Import Meetings Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Canceling Meetings by Import

Use this procedure to use the import process to cancel meetings in the Cisco Unified MeetingPlace database. Although you can cancel meetings individually from the end-user web interface, you can cancel multiple meetings at one time by following this procedure.

Before You Begin
Create the import file. See the “Setting Up an Import File” section on page 3

Restrictions
Only future instances of recurring meetings are cancelled; meeting information from the past is not imported.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Maintenance > Import Data > Import Meetings.
Step 3  Enter values in the fields.
        In the Action to perform field, select Cancel meetings.
Step 4  Select Execute.
Step 5  The system displays the import status and provides a link to the meeting import log:
        • Select the link to view the import log, which you may print.
        • Select OK to close the page.

After you select OK, the meeting import log can no longer be viewed or retrieved.

Related Topics
• Examples of Import Files, page 15
• Field Reference: Import Meetings Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Importing the System Configuration

Before You Begin
• Find the previously exported system configuration file.
• The system ignores any system configuration settings that are missing from the import file. The system displays warning messages for conditions such as missing parameters, invalid parameter values, and inconsistencies.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Maintenance > Import Data > Import System Configuration.
**Step 3**  Enter the filename or select **Browse** to find the system configuration file.

**Step 4**  Select **Execute**.

---

**Examples of Import Files**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Basic Import File Content</th>
</tr>
</thead>
<tbody>
<tr>
<td>User groups</td>
<td>grpnum,Name,ContactID,CanOutdial</td>
</tr>
<tr>
<td></td>
<td>1,group1,username3,Yes</td>
</tr>
<tr>
<td></td>
<td>2,group2,username3,No</td>
</tr>
<tr>
<td>User profiles</td>
<td>uid,upwd,prfnum,prfpwd,fnm,lnm,phnum,ctctuid,grpnme</td>
</tr>
<tr>
<td></td>
<td>username1,password1,206,12345,terry.smith,5550191,username3,system</td>
</tr>
<tr>
<td></td>
<td>username2,password2,207,23456,robin,smith,5550192,username3,system</td>
</tr>
<tr>
<td>Video terminal profiles (Release 7.0.2)</td>
<td>videoTermName,videoTermId,videoEndPtAddStr</td>
</tr>
<tr>
<td></td>
<td>Sample1 Room (System calls at mtg start),1226050345261,5550111</td>
</tr>
<tr>
<td></td>
<td>Sample2 Room (System calls at mtg start),1226050345262,5550112</td>
</tr>
<tr>
<td>Video terminal profiles (Release 7.0.1)</td>
<td>uid,videoTermName,videoTermId,videoEndPtAddStr</td>
</tr>
<tr>
<td></td>
<td>1226050345261,Sample1 Room (System calls at mtg start),1226050345261,5550111</td>
</tr>
<tr>
<td></td>
<td>1226050345262,Sample2 Room (System calls at mtg start),1226050345262,5550112</td>
</tr>
<tr>
<td>Meetings</td>
<td>StartTimeOfConf,DialableConfID,ReqLengthOfConf,allowguestoutdial</td>
</tr>
<tr>
<td></td>
<td>04/05/2006 14:00,12321,120,No</td>
</tr>
<tr>
<td></td>
<td>04/05/2006 16:00,23432,60,No</td>
</tr>
</tbody>
</table>

To force a user to change the user ID password and the profile password the first time that the user signs in to the system, modify these two fields:

- `wfpasswordlastchanged`
- `vupasswordlastchanged`

Set them to "1/1/1970 0:00" in the spreadsheet before importing them. Be sure to keep the full timestamp as well as the date format.

**Related Topics**

- Exporting the System Configuration in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
- Requirements for Importing Data, page 1
- Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module
About SNMP

- You can use SNMP to monitor the Cisco Unified MeetingPlace application and the hardware for the Application Server, Media Server, and Web Servers.
- SNMP versions 1 and 2c are supported. SNMP version 3 is not supported.
- All standard MIB II queries and a set of Cisco Unified MeetingPlace MIB traps are supported. The MIB II queries include the Cisco Unified MeetingPlace Application Server name, location, contact name, and statistics regarding the network interface.
- Traps are used to report events. See Table 1.

   Each major and minor software notification includes an integer exception code and indicates which software module and server reported the alarm. Normally, each alarm instance generates a separate notification. In some cases, however, one specific incident could trigger multiple types of alarms.

Table 1  Cisco Unified MeetingPlace SNMP Traps

<table>
<thead>
<tr>
<th>Name</th>
<th>OID(^1)</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Trap Types</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Major Software Alarm</td>
<td>.1.3.6.1.4.1.7185.3.1.3.0.5</td>
<td>Generated any time Cisco Unified MeetingPlace reports a major software alarm.</td>
</tr>
<tr>
<td>Minor Software Alarm</td>
<td>.1.3.6.1.4.1.7185.3.1.3.0.6</td>
<td>Generated any time Cisco Unified MeetingPlace reports a minor hardware alarm.</td>
</tr>
<tr>
<td><strong>Trap Message Content</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SystemUpTime</td>
<td>1.3.6.1.2.1.1.3.0</td>
<td>Counter for actual Application Server uptime.</td>
</tr>
<tr>
<td>Trap Type</td>
<td>—</td>
<td>See Trap Types.</td>
</tr>
</tbody>
</table>
**Requirements for SNMP**

For Cisco Unified MeetingPlace to support SNMP, you must import these non-standard MIBs into your network management server or SNMP monitoring package:

- CISCO-CDP-MIB.my: Cisco Discovery Protocol
- CISCO-SMI.my: Cisco Enterprise Structure of Management Information
- CISCO-TC.my: Cisco MIB Textual Conventions
- CISCO-VTP-MIB.my: Cisco Voice Technology Protocol MIB
- CISCO-LATITUDE-MIB.my: Cisco Latitude MIB

You can download these MIB files from ftp://ftp-sj.cisco.com/pub/mibs/v2/.

### How To Configure SNMP

- Adding or Editing SNMP Community Strings, page 3
- Displaying or Deleting SNMP Community Strings, page 3
- Adding or Editing SNMP Notification Destinations, page 4
- Displaying or Deleting SNMP Notification Destinations, page 4

---

**Table 1  Cisco Unified MeetingPlace SNMP Traps (continued)**

<table>
<thead>
<tr>
<th>Name</th>
<th>OID</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exception Code</td>
<td>1.3.6.1.4.1.7185.3.1.3.1</td>
<td>Primary code associated with each Cisco Unified MeetingPlace exception condition.</td>
</tr>
<tr>
<td>SwSys Unit</td>
<td>1.3.6.1.4.1.7185.3.1.3.2</td>
<td>Unit number of the Cisco Unified MeetingPlace server that reported the exception. Corresponds to the Unit number used by the Cisco Unified MeetingPlace Gateway System Integrity Manager (Gateway SIM) to identify the server.</td>
</tr>
<tr>
<td>Alarm Description</td>
<td>1.3.6.1.4.1.7185.3.1.3.7</td>
<td>One-line text description of the exception condition. It comprises a string indexed by the exception code filled in with context-specific values.</td>
</tr>
</tbody>
</table>

1. OID = Object Identifier

---

**Related Topics**

- Alarm Severity Levels in the Using Alarms and Logs on Cisco Unified MeetingPlace module
- Using Alarms and Logs on Cisco Unified MeetingPlace module
Adding or Editing SNMP Community Strings

Before You Begin
See the “Requirements for SNMP” section on page 2.

Restrictions
You must not disable the default community string, which is called meetingplace-public. Doing so will cause the application server to give an SNMP “authentication failure” trap every second.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Maintenance > SNMP > Community Strings.
Step 3  Select Add New or select an existing entry.
Step 4  Enter or change values in the fields.
Step 5  Select Save.

Related Topics
- Field Reference: Add SNMP Community String Page and Edit SNMP Community String Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Displaying or Deleting SNMP Community Strings

Restrictions
- You cannot delete the default community string, which is called meetingplace-public.
- You must not disable the default community string, which is called meetingplace-public. Doing so will cause the application server to give an SNMP “authentication failure” trap every second.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Maintenance > SNMP > Community Strings.
Step 3  Check the check box next to each community string that you want to delete, or check the topmost check box to select all community strings.
Step 4  Select Delete Selected.
Step 5  Select OK.

Related Topics
- Fields Reference: Community Strings Page in the Administration Center Page References for Cisco Unified MeetingPlace module
Adding or Editing SNMP Notification Destinations

The system sends a message to the IP address specified in the notification destination whenever a trap or inform condition occurs. A trap reports certain events while an inform condition allows one network management application to send trap information to another.

Procedure

1. Log in to the Administration Center.
2. Select Maintenance > SNMP > Notification Destinations.
3. Select Add New or select an existing entry.
4. Enter or change the values in the fields.
5. Select Save.

Related Topics

- Field Reference: Add SNMP Notification Destination Page and Edit SNMP Notification Destination Page in the Administration Center Page References for Cisco Unified MeetingPlace module

Displaying or Deleting SNMP Notification Destinations

Procedure

1. Log in to the Administration Center.
2. Select Maintenance > SNMP > Notification Destinations.
3. Check the check box next to each notification destination that you want to delete, or check the topmost check box to select all notification destinations.
4. Select Delete Selected.
5. Select OK.

Related Topics

- Field Reference: Notification Destinations Page in the Administration Center Page References for Cisco Unified MeetingPlace module

P A R T

Maintenance

- Running Reports and Exporting Data from Cisco Unified MeetingPlace
- Sending E-Mail Blasts from Cisco Unified MeetingPlace
Running Reports and Exporting Data from Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:31 pm

Use reports for capacity management and to track resource usage. You can also export database tables in a raw format for analysis or reporting in other applications.

- Reports and Exported Data, page 1
- How To Run Reports and Export Data, page 2

Reports and Exported Data

Caution

Cisco recommends that you do not run reports or backups during peak hours of use, such as on the hour. Doing so may cause the system to fail.

Report and export data enables you to monitor resource usage, monitor end-user activity, gather billing information, and watch for toll fraud. For example, you can use the data to determine whether the system has enough licenses and appropriate port and capacity configurations to support the number of calls being made by end users. Two areas of the Administration Center provide useful data that you can analyze and save:

- Reports
- Maintenance > Export Data

The output produced in these two areas differs in format. The reports area provides information that is formatted in tables, either in HTML or plain text. The Export Information area provides data in comma-delimited text files, which you may sort and format using any generally available third-party report-generation application.

Note

Some export options are provided only in XML format. These export options are provided only to save a subset of configurations that you can later import. Do not modify the exported files before importing.

You choose the destination of the generated report output. Table 1 describes the destination options.
Table 1  Report and Export Destination Options

<table>
<thead>
<tr>
<th>Destination</th>
<th>Description for Reports</th>
<th>Description for Exporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Screen</td>
<td>The report output appears on the screen. From the screen output, you have the option to print the information.</td>
<td>The exported data appears on the screen. From the screen output, you have the option to print the information.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Screen output is limited to 500 results. If the report output exceeds 500 results, the report is sent to a file instead of appearing on the screen.</td>
<td><strong>Note</strong> Screen output is limited to 500 results. If the exported data exceeds 500 results, you must choose the File export destination to view the whole report. Otherwise, only the first 500 results appear in the screen output.</td>
</tr>
</tbody>
</table>
| File        | The report output is placed in a file, which you choose to either open or save.  
- For plain text report output, use a text-editing program such as Notepad or Wordpad to view or modify the file.  
- For HTML output, use a web browser to view the file. | The exported data is placed in a text file, which you can either open or save.  
**Note** We recommend that you use the .csv file extension to save the file using the comma-separated values (CSV) file format. Open the saved file with a spreadsheet program such as Microsoft Excel. |
| Printer     | The report output appears on the screen and is sent to a printer. From the screen output, you have the option to print the information again. | The exported data appears on the screen and the Print dialog box is displayed, giving you the option to print the data.  
**Note** Printer output is limited to 500 results. If the exported data exceeds 500 results, you must choose the File export destination to print the whole report. Otherwise, only the first 500 results appear in the printer output. |

Related Topics
- How To Run Reports and Export Data, page 2

How To Run Reports and Export Data
- Exporting User Groups, page 3
- Exporting User Profiles, page 4
- Exporting Video Terminal Profiles, page 4
- Exporting Remote Servers, page 5
- Exporting Meeting Categories, page 6
- Exporting Meetings, page 6
- Exporting Information about Continuous Meetings, page 7
- Exporting Information about Meeting Participants, page 8
- Exporting Information about When Participants Join and Leave Meetings, page 9
- Exporting Information about Scheduling, page 9
- Running a Report about Meeting Cancellations, page 10
Exporting User Groups

Restrictions
Flex fields are not included in exported output.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Export Data > Export User Groups.
Step 3 On the Group Information page:
   a. Choose the output destination from the Destination drop-down list.
      If you plan to use the exported output to create an import file, then select File.
      For restrictions and recommendations for each option, see Table 1.
   b. Choose whether to include field header names in the output.
      If you plan to use the exported output to create an import file, then select Yes.
   c. Select Create Report.
Step 4 Select OK to proceed.
Step 5 If you are exporting data to create an import file, then save the file with a .csv extension.

Related Topics
Topics in the Importing Data into Cisco Unified MeetingPlace module:
   • Examples of Import Files
   • Adding or Editing User Groups by Import
   • Deleting User Groups by Import

What To Do Next
To interpret the exported data, see “Import and Export Data Specifications for User Profiles” in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module.
Exporting User Profiles

Restrictions
- **Flex Fields** are not included in exported output.
- The following fields are left blank for Directory Service users, who are authenticated externally:
  - User password (EncryptedUserPWD)
  - Profile password (EncryptedProfilePWD)

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Maintenance &gt; Export Data &gt; Export User Profiles.</td>
</tr>
</tbody>
</table>
| Step 3 | On the Profile Information page:  
  a. Choose the output destination from the **Destination** drop-down list.  
     If you plan to use the exported output to create an import file, then select **File**.  
     For restrictions and recommendations for each option, see Table 1.  
  b. Choose whether to include field header names in the output.  
     If you plan to use the exported output to create an import file, select **Yes**.  
  c. Select **Create Report**. |
| Step 4 | Select **OK** to proceed. |
| Step 5 | If you are exporting data to create an import file, then save the file with a .csv extension. |

Related Topics
- Configuring Cisco Unified MeetingPlace Directory Service module

Topics in the Importing Data into Cisco Unified MeetingPlace module:
- Examples of Import Files
- Adding or Editing User Profiles by Import
- Deleting User Profiles by Import

What To Do Next
To interpret the exported data, see “Import and Export Data Specifications for User Profiles” in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module.

Exporting Video Terminal Profiles

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select Maintenance &gt; Export Data &gt; Export Video Terminal Profiles.</td>
</tr>
</tbody>
</table>
Step 3  On the Profile Information page:

a. Choose the output destination from the **Destination** drop-down list.
   If you plan to use the exported output to create an import file, then select **File**.
   For restrictions and recommendations for each option, see Table 1.

b. Choose whether to include field header names in the output.
   If you plan to use the exported output to create an import file, select **Yes**.

c. Select **Create Report**.

Step 4  Select **OK** to proceed.

Step 5  If you are exporting data to create an import file, then save the file with a .csv extension.

Related Topics
Topics in the **Importing Data into Cisco Unified MeetingPlace** module:

- Examples of Import Files
- Adding or Editing Video Terminal Profiles by Import
- Deleting Video Terminal Profiles by Import

What To Do Next
To interpret the exported data, see “Import and Export Data Specifications for Video Terminal Profiles” in the **Raw Data Export and Import Specifications for Cisco Unified MeetingPlace** module.

Exporting Remote Servers
An exported remote servers file can be used as a snapshot or backup copy of configured remote servers that you can later import to your system.

Procedure

Step 1  Log in to the Administration Center.

Step 2  Select **Maintenance > Export Data > Export Remote Servers**.

Step 3  Select **Create Report**.

Step 4  Save the file.

Related Topics
- Importing Remote Servers in the **Importing Data into Cisco Unified MeetingPlace** module
Exporting Meeting Categories

An exported meeting categories file can be used as a snapshot or backup copy of configured meeting categories that you can later import to your system.

Procedure

1. Log in to the Administration Center.
2. Select Maintenance > Export Data > Export Meeting Categories.
4. Save the file.

Related Topics
- Importing Meeting Categories in the Importing Data into Cisco Unified MeetingPlace module
- Configuring Meeting Categories in the Configuring Meetings for Cisco Unified MeetingPlace module

Exporting Meetings

Use this procedure to export meetings from the Cisco Unified MeetingPlace database for a specified range of dates, including:

- Continuous meetings that were scheduled or initiated before or during the specified date range.
- Instances of recurring meetings that occur during the specified date range.

Restrictions

- If you export meetings to create a meeting import file, make sure that you specify a range of dates that includes all occurrences of recurring meetings that you want to import. The End date is optional. Also, see “Requirements for Importing Data” in the Importing Data into Cisco Unified MeetingPlace module.
- You cannot export meetings for a specific user, but the export file can be edited to include only the meetings that are owned by a specific user.
- If the meeting owner of an exported meeting does not have an existing user profile, then the SchedulerUid field is left blank in the meeting export file.

Procedure

1. Log in to the Administration Center.
2. Select Maintenance > Export Data > Export Meetings.
3. Specify the output options, as described in Table 2.
Running Reports and Exporting Data from Cisco Unified MeetingPlace

How To Run Reports and Export Data

Table 2  Field Reference: Export Meetings Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>If you plan to use the exported output to create an import file, then select File. For restrictions and recommendations for each option, see Table 1.</td>
</tr>
<tr>
<td>Include field header names</td>
<td>Select Yes if you want to be able to use the exported file to import data.</td>
</tr>
<tr>
<td>Include ended meetings</td>
<td>Whether to include meetings that have already ended in the exported file.</td>
</tr>
<tr>
<td>Start date</td>
<td>Default: yesterday (mm/dd/yyyy)</td>
</tr>
<tr>
<td>End date</td>
<td>If left blank, the exported output includes all future meetings.</td>
</tr>
<tr>
<td></td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
</tbody>
</table>

**Step 4**  Select **Create Report**.

**Step 5**  Select **OK** to proceed.

**Step 6**  If you are exporting data to create an import file, then save the file with a .csv extension.

**Related Topics**
- Scheduling Meetings by Import in the Importing Data into Cisco Unified MeetingPlace module
- Canceling Meetings by Import in the Importing Data into Cisco Unified MeetingPlace module
- Setting Up an Import File in the Importing Data into Cisco Unified MeetingPlace module

**What To Do Next**
To interpret the exported data, see “Import and Export Data Specifications for Meetings” in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module.

Exporting Information about Continuous Meetings

Use this procedure to export raw data about continuous meetings.

**Procedure**

**Step 1**  Log in to the Administration Center.

**Step 2**  Select Maintenance > Export Data > Continuous Meetings Information.

**Step 3**  Specify the output options, as described in Table 3.
Running Reports and Exporting Data from Cisco Unified MeetingPlace

How To Run Reports and Export Data

Step 4
Select Create Report.

Step 5
Select OK.

What To Do Next
To interpret the exported data, see “Export Data Specifications—Continuous Meetings Information” in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module.

Exporting Information about Meeting Participants

Use this procedure to export information about meeting participants who attended meetings during a specified range of dates.

Procedure

Step 1
Log in to the Administration Center.

Step 2
Select Maintenance > Export Data > Meeting Participant Information.

Step 3
On the Meeting Participants Report page:

a. Choose the output destination from the Destination drop-down list.

   For restrictions and recommendations for each option, see Table 1.

b. Choose whether to include field header names in the output.

c. Specify the range of dates for which you want to export information about meeting participants.

d. Select Create Report.

Step 4
Select OK.

Table 3  
Field Reference: Continuous Meetings Information Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Output destination. For restrictions and recommendations for each option, see Table 1.</td>
</tr>
<tr>
<td>Include ended meetings</td>
<td>Whether to include continuous meetings that were canceled. When set to Yes, you can use the Start date field to include only meetings that were canceled after a specific date. Default: No</td>
</tr>
<tr>
<td>Start date</td>
<td>Use this field to exclude continuous meetings that were canceled before a specific date. This field is dimmed when Include ended meetings is set to No. Default: yesterday (mm/dd/yyyy)</td>
</tr>
<tr>
<td>End date</td>
<td>Use this field to exclude continuous meetings that start after a specific date. Default: today (mm/dd/yyyy)</td>
</tr>
</tbody>
</table>
Exporting Information about When Participants Join and Leave Meetings

Use this procedure to export information about meeting participants who joined or left a Cisco Unified MeetingPlace meeting during a specified range of dates.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Export Data > Meeting Participant Join Leave Information.
Step 3 On the Meeting Participant Join Leave Information page:
   a. Choose the output destination from the Destination drop-down list. For restrictions and recommendations for each option, see Table 1.
   b. Choose whether to include field header names in the output.
   c. Specify the range of dates for which you want to export information about when meeting participants join and leave meetings.
   d. Select Create Report.
Step 4 Select OK.

What To Do Next
To interpret the exported data, see “Export Data Specifications—Meeting Participant Join Leave Information” in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module.

Exporting Information about Scheduling

Use this procedure to export information from the Cisco Unified MeetingPlace database about scheduling activity during a specified range of dates.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Export Data.
Step 3 Select one of the following options:
   - Scheduling Failures Information—Failed attempts to schedule meetings
   - Scheduling Statistics Information—Which user interfaces were used to schedule meetings
   - Scheduling Activity By User Information—Which users schedule meetings

What To Do Next
To interpret the exported data, see “Export Data Specifications—Meeting Participant Join Leave Information” in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module.
How To Run Reports and Export Data

Step 4  Configure the fields:
   a. Choose the output destination from the Destination drop-down list.
      For restrictions and recommendations for each option, see Table 1.
   b. Choose whether to include field header names in the output.
   c. Specify the range of dates for which you want to export information about scheduling failures.
   d. Select Create Report.

Step 5  Select OK.

What To Do Next
To interpret the exported data, see the following sections in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module:
- Export Data Specifications—Scheduling Failures Information
- Export Data Specifications—Scheduling Statistics Information
- Export Data Specifications—Scheduling Activity By User Information

Running a Report about Meeting Cancellations

Use this procedure to run a report that provides information about each meeting that was cancelled during a specified range of dates.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Reports > Meeting Cancellation Report.
Step 3  Configure the fields on the Meeting Cancellation Report Page.
Step 4  Select Create Report.
Step 5  Select OK.

What To Do Next
To interpret the exported data, see “Field Reference: Meeting Cancellation Report Page” in the Administration Center Page References for Cisco Unified MeetingPlace module.

Running a Report for Billing

Use this procedure to run a billing report for meetings held in a specified date range. You can run this report regularly to provide a bill-back report for departments in your company.
Procedure

**Step 1**  
Log in to the Administration Center.

**Step 2**  
Select **Reports > Billing Report**.

**Step 3**  
Configure the fields on the **Billing Report Page**.

**Step 4**  
Select **Create Report**.

**Step 5**  
Select **OK**.

**What To Do Next**
To interpret the exported data, see “Field Reference and Output Field Reference: Billing Report Page” in the **Administration Center Page References for Cisco Unified MeetingPlace module**.

---

### Running Capacity Management Reports

**Procedure**

**Step 1**  
Log in to the Administration Center.

**Step 2**  
Select **Reports**.

**Step 3**  
Select one of the following report options:

- **Port Utilization Report**—Compares the number of ports scheduled to the number of ports actually used during a specified period of time. You can use this report to compare resource usage with available capacity during peak and off-peak periods.

- **Unattended Ports Report**—Shows what percentage of scheduled ports were not used during a specified time range. The output can help you determine the appropriate settings for your overbook and floater ports. This report option was introduced in Release 7.0.2.

- **Monthly Usage Report**—Shows the total number of minutes per month that were used on the system for voice conferencing (with or without video) by all users in all meetings. This report option was introduced in Release 7.0.2.
  
  For example, a meeting in which 10 users each participated for 60 minutes would add 600 minutes for the month in which the meeting occurred.

  **Note**  
The system must have been in use for at least one month before you can use this report.

**Step 4**  
Configure the fields which affect the output.

**Step 5**  
Select **Create Report**.

**Step 6**  
Select **OK**.

**What To Do Next**
To interpret the exported data, see one of the following topics:
Running Reports and Exporting Data from Cisco Unified MeetingPlace

How To Run Reports and Export Data

Output Reference: Port Utilization Report in the Administration Center Page References for Cisco Unified MeetingPlace module

Output Reference: Unattended Ports Report in the Administration Center Page References for Cisco Unified MeetingPlace module

Running a Report about Meetings

This report provides information about meetings that occur in the specified date range.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Reports > Meeting Information Report.
Step 3 Configure the fields on the Meeting Information Report Page.
Step 4 Select Create Report.
Step 5 Select OK.

What To Do Next
To interpret the exported data, see “Field Reference and Output Field Reference: Meeting Information Report Page” in the Administration Center Page References for Cisco Unified MeetingPlace module.

Exporting Information about Dial-Out Calls

Use this procedure to export information about outgoing calls that were placed by Cisco Unified MeetingPlace during a specified range of dates.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Export Data.
Step 3 Select Outgoing Calls Information.
Step 4 Configure the fields:
   a. Choose the output destination from the Destination drop-down list.
      For restrictions and recommendations for each option, see Table 1.
   b. Choose whether to include field header names in the output.
   c. Specify the range of dates for which you want to export information about outgoing calls.
   d. Select Create Report.
Step 5 Select OK.
What To Do Next

To interpret the exported data, see “Export Data Specifications—Outgoing Calls Information” in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module.

Exporting the System Configuration

An exported system configuration file can be used as an import file if you need to replace your hardware or reinstall the complete Cisco Unified MeetingPlace system.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Administration Center.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Maintenance &gt; Export Data &gt; Export System Configuration.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Select Create Report.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Save the file.</td>
</tr>
</tbody>
</table>

Related Topics

- Importing the System Configuration in the Importing Data into Cisco Unified MeetingPlace module

Viewing the E-Mail Notification Queue

This task describes how to view the e-mail notification queue and (if necessary) to delete any unsent notifications.

Procedure

<table>
<thead>
<tr>
<th>Step 1</th>
<th>Log in to the Administration Center.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 2</td>
<td>Select Reports &gt; E-Mail Notification Queue Status Report.</td>
</tr>
<tr>
<td>Step 3</td>
<td>To interpret the data, see Table 4.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Table 4</th>
<th>Output Field Reference: E-Mail Notification Queue Status Report Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Meeting ID</td>
<td>Meeting ID, which uniquely identifies the meeting.</td>
</tr>
<tr>
<td>Date</td>
<td>Date and time of the scheduled meeting.</td>
</tr>
<tr>
<td>Requestor</td>
<td>User ID of the meeting owner.</td>
</tr>
<tr>
<td>Method</td>
<td>Always displays “E-mail.”</td>
</tr>
</tbody>
</table>
Step 4  (Optional) To delete any unsent e-mail notifications:
   a. Check the relevant check box(es).
   b. Select **Delete Notification(s)**.

### Related Topics
- [Configuring E-Mail Notifications for Cisco Unified MeetingPlace](#) module

### Table 4  Output Field Reference: E-Mail Notification Queue Status Report Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox Number</td>
<td>Type of e-mail notification:</td>
</tr>
<tr>
<td></td>
<td>• 2—IBM Lotus Notes</td>
</tr>
<tr>
<td></td>
<td>• 3—SMTP</td>
</tr>
<tr>
<td></td>
<td>• 4—Microsoft Exchange</td>
</tr>
<tr>
<td>Description</td>
<td>Describes the status in the queue, for example: New meeting scheduled.</td>
</tr>
<tr>
<td></td>
<td>Queued for delivery.</td>
</tr>
</tbody>
</table>
Sending E-Mail Blasts from Cisco Unified MeetingPlace

You can send an e-mail message to a user group or to all users in the Cisco Unified MeetingPlace database. This can be useful for sending productivity tips, announcing new features, and warning users of scheduled maintenance downtime.

Before You Begin

E-Mail Blasts will be sent using SMTP integration, make sure that the SMTP Server Configuration Page is properly configured.

Procedure

Step 1 Log in to the Administration Center.

Step 2 Select Maintenance > E-Mail Blast.

Step 3 Fill in the fields in Table 1.

Step 4 Select Send.

Table 1 Field Reference: E-Mail Blast Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Group</td>
<td>The user group to which you want to send the e-mail blast.</td>
</tr>
</tbody>
</table>
|         | To send the e-mail blast to all users whose user profiles contain an e-mail address, choose ----- All -----.
|         | Default: ----- None -----                                                   |
| Language| The language in which the e-mail blast is sent.                             |
|         | Default: English (US)                                                      |
| Subject | The subject of the e-mail blast.                                           |
|         | Default: Administrator announcement                                         |
| Body    | The text in the body of the e-mail blast.                                  |
Related Topics

- Configuring E-Mail Notifications for Cisco Unified MeetingPlace module
PART

End-User Interface Customization

- Configuring Flex Fields for Cisco Unified MeetingPlace
- Customizing E-Mail Notifications for Cisco Unified MeetingPlace
- Customizing Music and Voice Prompts for Cisco Unified MeetingPlace
Configuring Flex Fields for Cisco Unified MeetingPlace

You can define custom fields for meetings, user profiles, and user groups. Use these flex fields to track site- or organization-specific information by meeting or user.

You can set the Protection level to control which flex fields appear in or can be modified from the end-user web interface.

<table>
<thead>
<tr>
<th>Type of Flex Field</th>
<th>Default Value of Flex Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Text</td>
<td>(blank)</td>
</tr>
<tr>
<td>Number</td>
<td>0</td>
</tr>
<tr>
<td>Date</td>
<td>Jan 01 1970</td>
</tr>
<tr>
<td>Yes/No</td>
<td>No</td>
</tr>
</tbody>
</table>

Restrictions

- Flex fields are not included in exported output.
- Flex fields cannot be imported.
- If you modify the Type of an existing flex field, then the flex field value in existing user groups, user profiles, and meeting records that contain that flex field will be replaced by the default value applicable to the newly specified Type. See Table 1.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > Flex Fields Configuration.
Step 3 Select one of the flex field entries.
Step 4 Configure the fields on the Edit Flex Fields Page.
Step 5 Select Save.
Related Topics

- Field Reference: Edit Flex Fields Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Configuring the Cisco Unified MeetingPlace Web Conferencing User Interface module
- Customizing the Cisco Unified MeetingPlace Scheduling Form for Microsoft Outlook in the Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module
Customizing E-Mail Notifications for Cisco Unified MeetingPlace

About E-Mail Notification Templates and Language Property Files

E-mail notification templates specify which information to include in the e-mail notifications. The templates also determine the order and formatting used to present the specified information.

Although e-mail notification templates are editable, they are designed to be language-independent by containing tags instead of actual e-mail message content. Each tag is translated by the Cisco Unified MeetingPlace mail system into the text defined in editable language property files. A unique language property file is available for each language you install and enable on the Cisco Unified MeetingPlace server.

Topics in this section include:
- How the Mail System Works, page 1
- Example of Editing an E-Mail Notification Template and a Language Property File, page 2
- Notification Items, page 3

How the Mail System Works

The Cisco Unified MeetingPlace mail system uses the following process to send e-mail notifications to users:

1. The mail system selects the appropriate template, depending on the type of e-mail notification that is required. The templates are listed in Table 2.
2. The mail system identifies the tags in the template:
Customizing E-Mail Notifications for Cisco Unified MeetingPlace

About E-Mail Notification Templates and Language Property Files

a. Plain text in the template is left as plain text in the e-mail notification.

b. A dollar sign ($) indicates the beginning of a tag that is replaced by the definition in the language property file. For example:
   
   $notify_to_join_meeting

c. A space or the end of a line indicates the end of a tag.

3. The mail system checks which language property file to use, depending on the Language configured in the user profile of the e-mail recipient.

4. The mail system creates the e-mail notification by translating the tags in the template to the matching tag definitions in the language property file:
   
   d. An equal (=) sign indicates the beginning of a tag definition. For example:
      
      notify_to_join_meeting = To join the meeting

   e. The end of a line indicates the end of a tag definition.

   f. For each match, the mail system replaces the tag with the content defined in the language property file.

   g. If there is no match, the tag is included in the e-mail notification, including the dollar sign ($).

   h. Tag definitions may contain tags that are defined by other system components, such as the system scheduler. For example:
      
      notify_details=The meeting details are:
      notify_id=ID: $cisco_MTGID

      The scheduler component typically defines tags that appear on the scheduling page of the end-user web interface, such as the name of the meeting owner, meeting subject, and start time.

5. The mail system sends the completed e-mail notification to the SMTP server.

Related Topics

- How to Customize E-Mail Notifications, page 4
- About E-Mail Notification Templates and Language Property Files, page 1

Example of Editing an E-Mail Notification Template and a Language Property File

This example shows how to do the following:

1. Add a new tag, called $custom_greeting, to an e-mail notification template.

2. Define the tag in a language property file.

   Note

   If you enable multiple languages on your system, you must define new tags in all language property files.

The following example shows the placement of the new tag at the beginning of an e-mail notification template:

   $custom_greeting
   $notify_meeting_subject $notify_meeting_name
   $notify_date_time $notify_when
   $notify_dur $notify_duration
$notify_frequency $notify_recur_pattern

The following sample shows the definition of the new tag in the U.S. English language property file:

```
### English (USA) language property file ###
### ALL TEMPLATES
$notify_title=Cisco Unified MeetingPlace meeting notification
$custom_greeting=Good day. You have been invited to the following meeting:
$notify_details=The meeting details are:
$notify_mtg_id=Meeting ID:
$notify_meeting_id=$cisco_MTGID
$notify_id=ID: $cisco_MTGID
```

**Related Topics**
- About E-Mail Notification Templates and Language Property Files, page 1
- How to Customize E-Mail Notifications, page 4

**Notification Items**

The following table provides a list of notification items and tags that are commonly used by Cisco Unified MeetingPlace for Outlook and SMTP notifications.

<table>
<thead>
<tr>
<th>Notification Item</th>
<th>Notification Tag</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting ID</td>
<td>$cisco_MTGID</td>
</tr>
<tr>
<td>Click-to-attend link</td>
<td>$cisco_CtaUrl</td>
</tr>
<tr>
<td>Dial-in number</td>
<td>$cisco_DialIn</td>
</tr>
<tr>
<td>Meeting name</td>
<td>$cisco_TextName</td>
</tr>
<tr>
<td>Password</td>
<td>$cisco_Password</td>
</tr>
<tr>
<td>Meeting type</td>
<td>$cisco_MeetingType</td>
</tr>
<tr>
<td>Meeting template</td>
<td>$cisco_MeetingTemplate</td>
</tr>
<tr>
<td>Scheduler</td>
<td>$cisco_SchedulerFirstName</td>
</tr>
<tr>
<td></td>
<td>$cisco_SchedulerLastName</td>
</tr>
<tr>
<td>Current meeting date</td>
<td>$cisco_Month</td>
</tr>
<tr>
<td></td>
<td>$cisco_Day</td>
</tr>
<tr>
<td></td>
<td>$cisco_Year</td>
</tr>
<tr>
<td>Previous meeting date</td>
<td>$cisco_Orig_Month</td>
</tr>
<tr>
<td></td>
<td>$cisco_Orig_Day</td>
</tr>
<tr>
<td></td>
<td>$cisco_Orig_Year</td>
</tr>
<tr>
<td>Current meeting time</td>
<td>$cisco_Hour</td>
</tr>
<tr>
<td></td>
<td>$cisco_Min</td>
</tr>
<tr>
<td></td>
<td>$cisco_AMPM</td>
</tr>
<tr>
<td></td>
<td>$cisco_TimeZone</td>
</tr>
</tbody>
</table>
How to Customize E-Mail Notifications

Before You Begin

- If you plan to modify any language property files while editing e-mail notification templates, we recommend that you first save a copy of the existing language property files, in case you want to return to the previous versions. See the “Downloading a Language Property File” section on page 8.
- Tags are case-sensitive.
- As you edit the email notification template, keep track of whether you add any tags that begin with “$cisco_”, because these changes will not take effect until after a system restart.
- See the “Example of Editing an E-Mail Notification Template and a Language Property File” section on page 2.
Restrictions

- You cannot customize e-mail notification templates for a single user. Template changes affect all system-generated e-mail notifications.
- E-mail notification graphics cannot be modified or replaced. Also, new graphics cannot be added to e-mail notifications.
- The HTML editor has the following restrictions:
  - Only Internet Explorer enables you to view and edit the HTML output. All supported browsers enable you to view and edit the HTML source.
  - Only Internet Explorer provides the HTML-formatting toolbar.
  - In the HTML-formatting toolbar, the Background Color button can be used only to modify the background color of text. To instead modify the background color of table cells or the entire page, use an external HTML editor, or manually edit the HTML source by clicking the View HTML Source button (<>).
- The HTML templates display only the size and location of each graphic. The actual graphics cannot be previewed through the Administration Center and are displayed only in actual e-mail notifications.
- HTML-formatted Microsoft Outlook calendar notifications will not include any graphics.
- If you upgrade your system from an earlier release, the system overwrites all custom e-mail notification templates and replaces them with the standard e-mail notification templates for the later release.

Nevertheless, during the upgrade process, the system copies all of the previous notification templates to a backup directory: `/opt/cisco/meetingplace/var.<version>/mail/res/email_templates`, where `<version>` identifies the earlier Cisco Unified MeetingPlace release, for example, 7.1.0.66.

Procedure

**Step 1** Log in to the Administration Center.

**Step 2** Select **System Configuration > E-Mail Notifications > E-Mail Notification Templates**.

**Step 3** Using Table 1, decide whether to use the basic editing page or the advanced editing page to edit the e-mail notification master templates.

**Table 1  Basic and Advanced Master Template Editing Functionality**

<table>
<thead>
<tr>
<th>Editing Functionality</th>
<th>Basic</th>
<th>Advanced</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template selection</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Format selection between HTML and text</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Language selection</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>HTML editor¹</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>Language property file editor</td>
<td>—</td>
<td>Yes</td>
</tr>
<tr>
<td>Preview</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>

1. See the **Restrictions** for the HTML editor.

**Step 4** Select **Edit Templates (Basic)** or **Edit Templates (Advanced)**.

**Step 5** Using Table 2, select which template you want to modify.
Table 2  
E-Mail Notification Templates

<table>
<thead>
<tr>
<th>Template</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>EmailBlast</td>
<td>Sends one or all user groups an e-mail message from the system administrator. Typically used to inform users of maintenance tasks that may affect their ability to use Cisco Unified MeetingPlace. See Sending E-Mail Blasts from Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td>NotifyCancel</td>
<td>Notifies the meeting owner and invitees that a single-occurrence meeting was cancelled, or that one occurrence of a recurring meeting was cancelled.</td>
</tr>
<tr>
<td>NotifyCancelAll</td>
<td>Notifies the meeting owner and invitees that all occurrences of a recurring meeting were cancelled.</td>
</tr>
<tr>
<td>NotifyReschedule</td>
<td>Notifies the meeting owner and invitees that the meeting was rescheduled.</td>
</tr>
<tr>
<td>NotifySchedule</td>
<td>Notifies the meeting owner and invitees of a new scheduled meeting.</td>
</tr>
<tr>
<td>NotifyScheduleRes</td>
<td>Notifies invitees about a reservationless meeting. Restriction: Only Microsoft Outlook notifications use this template.</td>
</tr>
</tbody>
</table>

The templates whose names begin with SMTP are used only in e-mail notifications that are sent to an SMTP server. The SMTP e-mail notifications include more meeting details than the others, which are used by integrated clients (such as Microsoft Outlook) that display some of the meeting details (such as the start time and duration) elsewhere in the client user interface.

For templates that have both SMTP and non-SMTP versions, you must modify both versions to keep them consistent with each other. Otherwise, users may receive different information about the same meeting, depending on the E-mail type and format setting in each user profile.

Step 6  
Select which format (HTML or text) you want to modify.

You must modify both the HTML and plain text formats to keep them consistent with each other. Otherwise, users may receive different information about the same meeting, depending on the E-mail type and format setting in each user profile.

Step 7  
Modify the template. See the following topics:
- Editing Area of the Edit Templates (Basic) Page, page 43
- Editing Areas of the Edit Templates (Advanced) Page, page 42

Step 8  
To preview the template, select Preview.

Step 9  
Close the preview window when finished.

Step 10  
To save your template changes, select Save.

Step 11  
Repeat Step 6 through Step 10 for the other (HTML or text) template format.

Step 12  
If you added any tags that begin with “$cisco_”, you need to restart the system to make those changes take effect:
How to Customize E-Mail Notifications

Note
A system restart terminates all existing call connections. Proceed only during a scheduled maintenance period or during a period of extremely low usage.

a. Sign in to the CLI of the Application Server.
b. Enter `mpx_sys restart`.

Related Topics
- About E-Mail Notification Templates and Language Property Files, page 1
- How to Customize E-Mail Notifications, page 4
- Configuring E-Mail Notification Retries in the Configuring E-Mail Notifications for Cisco Unified MeetingPlace module
- Integration Note for Installing and Configuring IBM Lotus Notes with Cisco Unified MeetingPlace

Editing Language Property Files

Language property files define the text translations of tags used in e-mail notification templates.

Before You Begin
- If you plan to edit a language property file through the Cisco Unified MeetingPlace Administration Center, we recommend that you first save a copy of the existing language property file, in case you want to return to the previous version. See the “Downloading a Language Property File” section on page 8.
- Tags are case-sensitive.
- See the “Example of Editing an E-Mail Notification Template and a Language Property File” section on page 2.

Restrictions
You cannot customize language property files or e-mail notification templates for a single user. These changes affect all system-generated e-mail notifications.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select System Configuration > E-Mail Notifications > E-Mail Notification Templates > Edit Language Property Files.
Step 3 Choose the language property file to edit.
Step 4 Modify the language property file.
Step 5 Select Save.
Related Topics

- About E-Mail Notification Templates and Language Property Files, page 1

What To Do Next

Because the same tags are used in multiple templates, you should preview all templates after editing a language property file. See the “Editing Templates for E-Mail Notifications” section on page 4.

Downloading a Language Property File

This task is useful for saving a copy of a working language property file before you edit it, in case you decide to revert to the previous version. You can also download a language property file to your PC, modify it using a text editor such as WordPad, and then upload the language property file to Cisco Unified MeetingPlace.

Procedure

**Step 1** Log in to the Administration Center.

**Step 2** Select System Configuration > E-Mail Notifications > E-Mail Notification Templates > Download Language Property File.

**Step 3** Choose the language property file to download.

**Step 4** Select Download.

**Step 5** Select Open or Save.

If you are prompted with an Open With dialog box, choose a text editor, such as WordPad.

Related Topics

- About E-Mail Notification Templates and Language Property Files, page 1
- Uploading a Language Property File, page 8

Uploading a Language Property File

Performing this task is useful if you edit the language property file and decide to revert to a previously downloaded language property file. You can also upload a language property file that you modified on your PC.

Before You Begin

- Uploaded language property files must have the exact same case-sensitive filename as an existing language property file on the system. For example, the U.S. English language property file name is Templates_en_US.properties.
- To see the valid filename of a language property file, complete Step 1 through Step 4 in the “Downloading a Language Property File” section on page 8. The filename appears in the File Download window.
Procedure

Step 1 Log in to the Administration Center.

Step 2 Select System Configuration > E-Mail Notifications > E-Mail Notification Templates > Upload Language Property File.

Step 3 Select the language.

Step 4 Select Browse, find the language property file, and select Open.

Step 5 Select Upload.

Related Topics

- About E-Mail Notification Templates and Language Property Files, page 1
- Downloading a Language Property File, page 8
- Example of Editing an E-Mail Notification Template and a Language Property File, page 2
Customizing Music and Voice Prompts for Cisco Unified MeetingPlace

About Music and Voice Prompts

Music prompts are a subset of voice prompts. A voice prompt is a single voice file, and a sentence is a string of multiple voice prompts. You cannot customize the order of voice prompts in a sentence, but you can customize individual prompts. Examples of individual prompts include:

- “1”
- “To attend a meeting.”
- “Enter the meeting ID followed by the pound key.”
- Music heard when you are the first to join a meeting and are waiting for others to join.

Because there are only a few music prompts, they are listed in Table 1.

Note


<table>
<thead>
<tr>
<th>Prompt Number</th>
<th>Approximate Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>303</td>
<td>3 minutes</td>
<td>Music heard when the user schedules a meeting by phone and waits for the system to check resource availability and schedule the requested meeting.</td>
</tr>
<tr>
<td>304</td>
<td>3 minutes</td>
<td>Music heard when the first voice meeting participant joins and waits for others to join.</td>
</tr>
</tbody>
</table>
Customizing Music and Voice Prompts for Cisco Unified MeetingPlace

Table 1  Music Prompt Numbers and Durations (continued)

<table>
<thead>
<tr>
<th>Prompt Number</th>
<th>Approximate Duration</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1495</td>
<td>3 minutes</td>
<td>Music heard by users in a waiting room.</td>
</tr>
<tr>
<td>1497</td>
<td>3 seconds</td>
<td>Welcome music heard by users who dial in.</td>
</tr>
</tbody>
</table>

Topics in this section include:
- Guidelines for Creating Custom Voice Prompts, page 2
- Guidelines for Creating Custom Music Prompts, page 2
- File Locations for Music and Voice Prompts, page 3

Guidelines for Creating Custom Voice Prompts

- **Recording environment**—Make sure that the environment is extremely quiet. Do some sample recordings beforehand, and listen to the results. The recorded passages should be free of hissing, pops, frequency distortion, and other types of noise.
- **Silence before and after each prompt**—Each prompt should have between 50 to 100 milliseconds of silence at the beginning and end. Too little silence creates pops when the prompt is concatenated with other prompts (played just after or before other prompts). Too much silence creates awkward gaps in overall speech when several prompts are played together. In some cases, 100 milliseconds might not be enough to eliminate pops at the beginning and end of concatenated prompts. In this case, try increasing the silence to 150 milliseconds. To measure the amount of silence at the beginning or end of a prompt (or to see if there is silence), bring up the prompt in Adobe Audition or a similar voice editing program. Open the file as a 16-bit, 8-kHz .wav or raw PCM file. Adobe Audition allows accurate measurement of silences passages.
- **Format**—Record all prompts in 8 kHz sample rate, u-law, WAV format. Any recording that is not in this format must be processed in Adobe Audition or an equivalent audio editor to convert the recording to the required 8 kHz, mu-law, WAV format.
- **Level**—The average recording level for non-silence sections should be -24 dBm. Avoid very loud recording levels because they can cause clipping, which creates clicks and pops in the middle of the prompts.

Related Topics
- Creating a Custom Voice Prompt, page 6

Guidelines for Creating Custom Music Prompts

Note Because music prompts are subset of voice prompts, the “Guidelines for Creating Custom Voice Prompts” section on page 2 also applies to custom music prompts.
The audio quality of some music may degrade when transmitted over low bit-rate connections, such as those using codecs other than G.711. To reduce audio quality degradation:

- Consider using simple combinations of the following music types, which yield acceptable audio quality when played over low bit-rate connections:
  - voice-only singing
  - bells
  - most brass
  - woodwinds
  - pure tones
  - acoustic guitar
- Avoid music that contains the following, because they may result in poor quality when played over low bit-rate connections:
  - Drums
  - Cymbal crashes
  - Electronic or distorted music

Related Topics
- Guidelines for Creating Custom Music Prompts, page 2

File Locations for Music and Voice Prompts

Where each music or voice prompt is stored depends on its language and whether it is a standard or custom prompt. See Table 2.

<table>
<thead>
<tr>
<th>Prompt Type</th>
<th>File Location</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard</td>
<td>/opt/cisco/meetingplace/afs/prompts/</td>
</tr>
<tr>
<td></td>
<td>Language subdirectory examples:</td>
</tr>
<tr>
<td></td>
<td>• German: /opt/cisco/meetingplace/afs/prompts/de_DE/</td>
</tr>
<tr>
<td>Custom</td>
<td>/opt/cisco/meetingplace/afs/custom/prompts/</td>
</tr>
<tr>
<td></td>
<td>Language subdirectory examples:</td>
</tr>
<tr>
<td></td>
<td>• German: /opt/cisco/meetingplace/afs/custom/prompts/de_DE</td>
</tr>
</tbody>
</table>

Note: The subdirectories only appear if custom prompts exist for that language. For example, if there are no German custom prompts, then the German subdirectory path will not exist.

Related Topics
- How to Customize Music and Voice Prompts, page 4
- Restrictions for Customizing Music and Voice Prompts, page 4
Restrictions for Customizing Music and Voice Prompts

Cisco Unified MeetingPlace does not play custom prompts for languages other than U.S. English for the music and silence prompts in the following list. The system always uses the U.S. English prompts regardless of their availability in other languages.

- sVOICELOGOLOCKED (1497)
- sMUSIC2002A (1494)
- sMUSIC2002B (1495)
- sMUSIC2002C (1532)
- sMUSIC2002D (1533)
- sJAZZ (303)
- sMUSAC (304)
- sPOP (305)
- sSILENCE (214)
- sSILENCELONG (1546)
- sSILENTPAUSE (1498)
- sSILENTPAUSEHALF (1496)
- sWAITALT (1547)

Related Topics
- About Music and Voice Prompts, page 1
- How to Customize Music and Voice Prompts, page 4

How to Customize Music and Voice Prompts

- Main Menu Prompt Reference, page 4
- Customizing Prompts from the Phone, page 6
- Creating a Custom Voice Prompt, page 6
- Creating a Custom Music Prompt, page 7
- Uploading a Custom Music or Voice Prompt, page 9
- Deleting a Custom Music or Voice Prompt, page 10

Main Menu Prompt Reference

If you have auto attend disabled on your system, you will hear the following voice prompts:

- Voice Prompt # 1497: Audio logo
- Voice Prompt # 180: "Welcome to MeetingPlace"
- Voice Prompt # 162: "Enter the meeting ID number, followed by the # key."
- Voice Prompt # 1499: "To start your meeting now..."
Customizing Music and Voice Prompts for Cisco Unified MeetingPlace

How to Customize Music and Voice Prompts

- Voice Prompt # 34: "Press 2 ...
- Voice Prompt # 1739: "...then #.
- Voice Prompt # 150: "To access your profile...
- Voice Prompt # 35: "Press 3 ...
- Voice Prompt # 1739: "...then #.
- Voice Prompt # 1269: "To hear an overview of MeetingPlace functions and features...
- Voice Prompt # 41: "Press 9 ...
- Voice Prompt # 1739: "...then #.
- Voice Prompt # 433: "To reach assistance...
- Voice Prompt # 42: "Press 0 ...
- Voice Prompt # 1739: "...then #.

If you have auto attend enabled on your system, you will hear the following voice prompts:

- Voice Prompt # 1497: Audio logo
- Voice Prompt # 180: "Welcome to MeetingPlace"

If an auto attend password is required, you will hear:

- Voice Prompt # 229: "Enter your password, followed by the # key."
- Voice Prompt # 1518: "For other options, press *.

If the user does not have a recorded name, you will hear:

- Voice Prompt # 294: "The system does not have a recorded name for your profile. This recorded name is used to introduce you to meetings."
- Voice Prompt # 385: "Record your profile name at the tone. When finished, press the # key."
  The user records his name and presses #.
- Voice Prompt # 296: "Your recorded name is ...
  The system plays the user's recorded name.
- Voice Prompt # 383: "To use this as your profile name ...
- Voice Prompt # 45: "... press 1."
- Voice Prompt # 384: "To record a new profile name ...
- Voice Prompt # 149: "To attend a meeting, ..."
- Voice Prompt # 45: "... press 1."
- Voice Prompt # 1524: "To start or schedule a meeting, ..."
- Voice Prompt # 46: "... press 2."
- Voice Prompt # 166: "To change your profile settings or meeting preferences, ...
- Voice Prompt # 47: "... press 3."

If the user does not have reservationless meetings enabled, then prompt 1524 above, is replaced by:

- Voice Prompt # 165: "To schedule, reschedule or list your meetings, ..."
Customizing Prompts from the Phone

The Cisco Unified MeetingPlace phone interface operates by playing a series of voice prompts and requesting key presses or spoken response from users. From a 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.

Creating a Custom Voice Prompt

This task describes how to use the Sound Recorder application to record a custom voice prompt for Cisco Unified MeetingPlace. You may instead use a different commercially available sound recording tool or even obtain professional, studio-recorded prompts.

Note

- You can only create custom prompts by recording and uploading through the Administration Center.
- If you want to create a custom music prompt, see the “Creating a Custom Music Prompt” section on page 7.

Before You Begin

- All voice prompts must be in 8 kHz, G.711 mu-law WAV PCM format.
- Determine the name, number, and file location of the voice prompt that you want to customize. See the following:
  - File Locations for Music and Voice Prompts, page 3
- Read the following:
  - Guidelines for Creating Custom Voice Prompts, page 2
  - Restrictions for Customizing Music and Voice Prompts, page 4

Procedure

Step 1

Open and set up the Sound Recorder application.

a. On your PC, go to Start > Programs > Accessories > Entertainment > Sound Recorder.
b. Choose File > Properties.
c. Select Convert Now....
d. From the Format drop-down list, choose CCITT u-Law.
e. From Attributes, select 8.000 kHz, 8-bit, mono.
f. Select OK.
g. On the Properties for Sound dialog box, select OK.

Step 2
Record the custom voice prompt.

Step 3
Save the custom voice prompt with the same filename as the voice prompt you want to replace. All voice prompt files are called s<number>.wav where <number> corresponds to the prompt number.

What To Do Next
Proceed to the “Uploading a Custom Music or Voice Prompt” section on page 9.

Creating a Custom Music Prompt

This task describes how to convert a source music file to a custom music prompt for Cisco Unified MeetingPlace. The original source music file can be one that you created or a pre-recorded music file of your choosing.

Note
This procedure uses Adobe Audition, but you may instead use CoolEdit or another equivalent commercially available audio editing tool.

Before You Begin

- If you use a pre-recorded music file, make sure you comply with licensing terms or digital rights restrictions.
- Read the following:
  - Restrictions for Customizing Music and Voice Prompts, page 4
- Determine the number and duration of the music file that you want to customize. See Table 1.
- Determine the location of the music file that you want to customize. See the “File Locations for Music and Voice Prompts” section on page 3.

Procedure

Step 1
Use Adobe Audition to convert the source music file to a 16 bit, 8 kHz, mono, linear PCM, headerless file:

a. Open the Adobe Audition application.
b. Choose File > Open to open the source music file.
c. Choose File > Save As.
d. In the Save In field, choose an appropriate folder.
e. In the File Name field, enter the temporary filename.
   Use the following format: s<number>_temp.pcm, where <number> is the Prompt Number.
f. In the Save As Type field, select PCM Raw Data (*.pcm, *.raw).
g. Select Options.

h. In the Data Formatted As field, select 16-bit Intel PCM (LSB,MSB).

i. Select OK.

j. Select Save.

Step 2 Use Adobe Audition to adjust the converted music file to meet the “Guidelines for Creating Custom Voice Prompts” section on page 2:

a. Open Adobe Audition.

b. Choose File > Open to open the s<number>_temp.pcm file.

c. Choose Analyze > Statistics.

d. Note the Average RMS Power for the music file:
   - If the value is between -23 dBm and -25 dBm, then skip to Step 3.
   - If the value is outside this target range, then proceed to Step 2e to correct this deficiency.

e. Choose Edit > Select Entire Wave.

f. Choose Effects > Amplitude > Amplify...

g. Select the Constant Amplification tab.

h. In the Amplification dB field, enter a value equal to the difference between the target level -24 dBm and the measured average level.
   - A positive value applies gain, while a negative value applies attenuation.

i. Press OK.

j. Return to Step 2c.

Step 3 Convert the level-corrected music file to the required 8 kHz, mu-Law PCM WAV format:

a. Choose File > Save As.

b. In the Save In field, select the same folder that you chose in Step 1d.

c. In the File Name field, enter the correct filename for the custom music prompt.
   - Use the following format: s<number>.wav, where <number> is the Prompt Number.

d. In the Save As Type field, select A/mu-Law Wave (*.wav).

e. Select Options.

f. In the Data Formatted As field, select mu-Law 8 bit.

g. Select OK.

h. Select Save.

What To Do Next
Proceed to the “Uploading a Custom Music or Voice Prompt” section on page 9.
Uploading a Custom Music or Voice Prompt

Before You Begin

- Activating a custom prompt requires a system restart, which terminates all existing call connections and deletes all manual changes made to the registry. Proceed only during a scheduled maintenance period or during a period of extremely low usage.
- Read the “Restrictions for Customizing Music and Voice Prompts” section on page 4.
- Complete one of the following tasks:
  - Creating a Custom Voice Prompt, page 6
  - Creating a Custom Music Prompt, page 7
- Music and voice prompts must be in 8 kHz, G.711 mu-law WAV PCM format.
- After you upload a custom prompt and restart the system, the system plays the custom prompt instead of the original prompt. Nevertheless, the original prompt remains intact; custom voice prompts and original voice prompts are stored in separate folders.

Note  When you restart the Web Server, all manual changes made to the registry are lost.

To revert to the original prompt, complete the “Deleting a Custom Music or Voice Prompt” section on page 10.

Procedure

Step 1  Log in to the Administration Center.
Step 2  Select Maintenance > Custom Prompts.
Step 3  Select the language of the custom prompt.
Step 4  Enter the fully-qualified pathname of the custom prompt file, or select Browse to locate the file.

Tip  All music and voice prompt files are called s<number>.wav, where <number> corresponds to the Prompt Number.

Step 5  Select Upload File.
Step 6  Restart the system to activate the custom prompt by entering sudo mpx_sys restart in the CLI.

Note  When you restart the Web Server, all manual changes made to the registry are lost.

Related Topics

- Custom Prompts Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- File Locations for Music and Voice Prompts, page 3
Deleting a Custom Music or Voice Prompt

Before You Begin

- This task requires a system restart, which terminates all existing call connections and deletes all manual changes made to the registry. Proceed only during a scheduled maintenance period or during a period of extremely low usage.
- After you delete a custom prompt and restart the system, the system reverts to playing the original prompt.
- You can only delete custom prompts; you cannot delete standard prompts.

Procedure

Step 1 Log in to the Administration Center.
Step 2 Select Maintenance > Custom Prompts.
Step 3 Perform one of the following actions:
  - To delete one or more custom prompts, select those you want to delete, and select Delete Selected.
  - To delete all custom prompts, select Delete All.
Step 4 Restart the system to activate the standard prompt by entering sudo mpx_sys restart in the CLI.

Note When you restart the Web Server, all manual changes made to the registry are lost.

Related Topics

- Custom Prompts Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
PART

Troubleshooting

- Using Alarms and Logs on Cisco Unified MeetingPlace
- Password Recovery for Cisco Unified MeetingPlace
- Troubleshooting User Access Issues for Cisco Unified MeetingPlace
- Troubleshooting Telephone Issues for Cisco Unified MeetingPlace
- Troubleshooting Video Issues for Cisco Unified MeetingPlace
- Troubleshooting E-Mail Notifications for Cisco Unified MeetingPlace
- Troubleshooting Cisco Unified MeetingPlace Web Conferencing
- Troubleshooting the Cisco Unified MeetingPlace Application Server
- Troubleshooting Cisco Unified MeetingPlace Integration with Cisco WebEx
- Troubleshooting Cisco Unified MeetingPlace Scheduling from Microsoft Outlook
- Troubleshooting Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface
Using Alarms and Logs on Cisco Unified MeetingPlace

About Alarms

Alarms are caused by network connectivity failures and are usually software-related. They can also occur when there is a surge of activity on the network, or when the system detects a configuration issue, such as not having conferencing licenses installed.

When the system generates an alarm:

- Similar alarms are aggregated into the Alarm Table.
- The alarm is captured in the Exception Log.
- If SNMP is configured, then a notification is sent to any registered management stations.

In general, you can use the Alarm Table to check for any problems, and then look in the Exception Log for details.

Related Topics

- Configuring SNMP on Cisco Unified MeetingPlace module
- Viewing the Alarm Table and Clearing Alarms in the Administration Center, page 6
- Alarm Severity Levels, page 2
About Alarms

- Module Numbers, page 3

Alarm Severity Levels

<table>
<thead>
<tr>
<th>Alarm Severity Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAJOR</td>
<td>Action must be taken immediately. A system error occurred that requires manual intervention. You will likely need to contact Cisco TAC. Examples:</td>
</tr>
<tr>
<td></td>
<td>- Less than 50% of a major resource (audio, video, or web) is functional.</td>
</tr>
<tr>
<td></td>
<td>- A major feature (such as Microsoft Outlook integration) is nonfunctional or may soon become nonfunctional.</td>
</tr>
<tr>
<td></td>
<td>- A server is about to run out of disk space.</td>
</tr>
<tr>
<td>MINOR</td>
<td>Investigate the issue to determine if immediate action is needed. An error occurred that does not impact the ability of the system to continue to function. Nevertheless, some corrective action is required. Depending on the issue, you may need assistance from Cisco TAC. Examples:</td>
</tr>
<tr>
<td></td>
<td>- A server has exceeded the recommended threshold of disk space.</td>
</tr>
<tr>
<td></td>
<td>- A blade failure causes less than 50% of a resource capacity to be lost.</td>
</tr>
<tr>
<td></td>
<td>- A configuration error prevents dial-out calls.</td>
</tr>
</tbody>
</table>

Related Topics

Alarm Table

The alarm table can be viewed:
- On the Alarms Page in the Administration Center
- By entering the alarm command
- In the “Alarms” log in the System Information Capture (Infocap) log

The alarm table combines multiple alarms into a single table entry when the following values are the same:
- Code
- Unit
- Software Module
The brief description in an alarm table entry may contain values that are specific to one alarm occurrence, such as an IP address or the available disk space on a Web Server. These values may differ for all alarms that are combined into one table entry. Only the values for the most recent alarm are displayed. To view all alarm occurrences, view the Exception Log.

Entries remain in the alarm table until you clear them. Therefore, the alarm table may display very old information. In contrast, only the alarms generated during a specified time period are displayed in the “ExLog error logs” or “ExLog detailed logs” in the System Information Capture (Infocap) log.

We recommend that you regularly clear the alarm table, so that:

- You can tell at a glance whether any new alarms have been generated since the last time you looked.
- You can distinguish between individual alarms, because there will be fewer counts per table entry.

**Related Topics**

- [How to View the Alarm Table and Clear Alarms, page 5](#)
- [Obtaining and Viewing the System Information Capture (Infocap) Log, page 10](#)

### Exception Log

The exception log contains alarm and error messages. Clearing alarms in the Alarm Table does not clear alarms in the exception log.

You can view the exception log:

- By entering the `errorlog` command or the `viewexlog` command.
- In the “ExLog error logs” or “ExLog detailed logs” in the System Information Capture (Infocap) log.

**Related Topics**

- [Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace](#)
- [Obtaining and Viewing the System Information Capture (Infocap) Log, page 10](#)

### Module Numbers

Use Table 1 to determine which system component corresponds to each module number that may appear in the Alarm Table or Exception Log.

**Table 1**  

<table>
<thead>
<tr>
<th>Internal Error Number</th>
<th>System Component</th>
<th>Module Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>IMC_CLASS_NULL</td>
<td>0</td>
<td>Command line utility</td>
</tr>
<tr>
<td>1024</td>
<td>IMC_CLASS_COMMON</td>
<td>1</td>
<td>Common functions</td>
</tr>
<tr>
<td>2048</td>
<td>IMC_CLASS_SIM</td>
<td>2</td>
<td>System Integrity Manager (SIM)</td>
</tr>
</tbody>
</table>
Table 1  Module Numbers (continued)

<table>
<thead>
<tr>
<th>Internal Error Number</th>
<th>System Component</th>
<th>Module Number</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>3072</td>
<td>IMC_CLASS_CP</td>
<td>3</td>
<td>Call Processing–Media Control Protocol (CPMCP), which is a proxy for the Media Server</td>
</tr>
<tr>
<td>4096</td>
<td>IMC_CLASS_SM</td>
<td>4</td>
<td>Switch manager</td>
</tr>
<tr>
<td>5120</td>
<td>IMC_CLASS_CS</td>
<td>5</td>
<td>Conference scheduler (ConfSchd)</td>
</tr>
<tr>
<td>6144</td>
<td>IMC_CLASS_WS</td>
<td>6</td>
<td>Workstation server</td>
</tr>
<tr>
<td>7168</td>
<td>IMC_CLASS_EXC</td>
<td>7</td>
<td>Exception handler (in SIM)</td>
</tr>
<tr>
<td>8192</td>
<td>IMC_CLASS_VUI</td>
<td>8</td>
<td>Telephone user interface (TUI)</td>
</tr>
<tr>
<td>9216</td>
<td>IMC_CLASS_DB</td>
<td>9</td>
<td>The database server</td>
</tr>
<tr>
<td>10240</td>
<td>IMC_CLASS_VUI_TESTER</td>
<td>10</td>
<td>TUI tester program</td>
</tr>
<tr>
<td>11264</td>
<td>IMC_CLASS_TRACE</td>
<td>11</td>
<td>SIM trace server</td>
</tr>
<tr>
<td>12288</td>
<td>IMC_CLASS_WF</td>
<td>12</td>
<td>Workstation front end</td>
</tr>
<tr>
<td>13312</td>
<td>IMC_CLASS_UTIL</td>
<td>13</td>
<td>Any command line utility</td>
</tr>
<tr>
<td>14336</td>
<td>IMC_CLASS_LSH</td>
<td>14</td>
<td>Shell facility</td>
</tr>
<tr>
<td>15360</td>
<td>IMC_CLASS_DBQ</td>
<td>15</td>
<td>Database query server</td>
</tr>
<tr>
<td>16384</td>
<td>IMC_CLASS_EMAIL_MSG</td>
<td>16</td>
<td>Class to support an error range</td>
</tr>
<tr>
<td>17408</td>
<td>IMC_CLASS_SNMPD</td>
<td>17</td>
<td>Class to support SNMP daemon control</td>
</tr>
<tr>
<td>18432</td>
<td>IMC_CLASS_PO</td>
<td>18</td>
<td>Post office server</td>
</tr>
<tr>
<td>19456</td>
<td>IMC_CLASS_PO_TESTER</td>
<td>19</td>
<td>Post office server tester program</td>
</tr>
<tr>
<td>20480</td>
<td>IMC_CLASS_SIM_MU</td>
<td>20</td>
<td>Multi-unit SIM session control</td>
</tr>
<tr>
<td>21504</td>
<td>IMC_CLASS_FAXGW</td>
<td>21</td>
<td>Fax gateway</td>
</tr>
<tr>
<td>22528</td>
<td>IMC_CLASS_WEBGW</td>
<td>22</td>
<td>Web publisher (overlaps with pegs)</td>
</tr>
<tr>
<td>22528</td>
<td>IMC_CLASS_PEGS</td>
<td>22</td>
<td>Peg server (part of SIM)</td>
</tr>
<tr>
<td>23552</td>
<td>IMC_CLASS_SDBS</td>
<td>23</td>
<td>Shadow database server</td>
</tr>
<tr>
<td>24576</td>
<td>IMC_CLASS_SDBS_TESTER</td>
<td>24</td>
<td>Shadow database server tester program</td>
</tr>
<tr>
<td>25600</td>
<td>IMC_CLASS_GWSIMGR</td>
<td>25</td>
<td></td>
</tr>
<tr>
<td>26624</td>
<td>IMC_CLASS_GWSIMAGENT</td>
<td>26</td>
<td></td>
</tr>
<tr>
<td>27648</td>
<td>IMC_CLASS_STREAMGW</td>
<td>27</td>
<td>Streaming gateway</td>
</tr>
<tr>
<td>28672</td>
<td>IMC_CLASS_CCA</td>
<td>28</td>
<td>Call control agent</td>
</tr>
<tr>
<td>29696</td>
<td>IMC_CLASS_MPDIRSVVC</td>
<td>29</td>
<td>Directory services</td>
</tr>
<tr>
<td>30720</td>
<td>IMC_CLASS_MERGED</td>
<td>30</td>
<td>PCI conversion/merge daemon</td>
</tr>
<tr>
<td>31744</td>
<td>IMC_CLASS_GSCOPE</td>
<td>31</td>
<td>Gyroscope application</td>
</tr>
<tr>
<td>32768</td>
<td>IMC_CLASS_NMPAGENT</td>
<td>32</td>
<td>NMPAgent</td>
</tr>
<tr>
<td>33792</td>
<td>IMC_CLASS_TWATCH</td>
<td>33</td>
<td>Trigger watch</td>
</tr>
<tr>
<td>34816</td>
<td>IMC_CLASS_POCLIENT</td>
<td>34</td>
<td>Post office client</td>
</tr>
</tbody>
</table>
Core Files

Core files are useful for determining what state a program was in before it terminated. A utility called `checkcores` reports new cores found, raises an alarm (EX_CORESPACE), and compresses and archives the cores to the /mpx-record/cores directory.

**Note**

Unless the cause of the core file is already known, all core files should be escalated to Cisco TAC.

During startup, if new cores are found, the following message is echoed to the session after “Starting MeetingPlace application”:

```
NOTE: new core files found in /var
See /mpx-record/cores/checkcores.log for more information
```

If no cores are found, the utility does not log anything. If run interactively, the utility either echoes the two lines shown above if cores are found, or echoes “no cores found”.

A maximum of 10 core files are saved to this location. The approximate total max space required for compressed core images is 200MB. If there is insufficient space in the /mpx-record directory, an alarm is raised:

```
346) MAJ 10006c 4 Mar 22 05:58 Mar 22 06:00 0 SW MODULE=0 insufficient space in /mpx-record filesystem to manage cores
```

A logfile, /mpx-record/cores/checkcores.log, is maintained in the /mpx-record/cores directory. If this logfile grows beyond 100K, it is backed up to checkcores.log.old and a new log is started (only one backup is maintained).

Cores are archived in the form:

```
yymmddhhmmss-path1-path2-path3-core.pid.datetime.gz
```

- `yymmddhhmmss` is the current date/timestamp
- `path1-path2-path3` is the full path translated to hyphen-separated names; for example, /var/mp/nmpagent is translated to var-mp-nmpagent
- `pid` is the process id of the aborted process
- `datetime` is the date/timestamp of the core file creation as displayed by `ls -l`, but in a compressed form (for example, Mar2-14:52, Jan22-09:15).

Related Topics


**How to View the Alarm Table and Clear Alarms**

- Viewing the Alarm Table and Clearing Alarms in the Administration Center, page 6
- Viewing the Alarm Table and Clearing Alarms Using the CLI, page 6
Viewing the Alarm Table and Clearing Alarms in the Administration Center

Procedure

Step 1  Log in to the Administration Center.
Step 2  Click Services > Alarms.
Step 3  (Optional) Clear alarms:
   • To clear one or more alarms, select the entries, and click Delete Selected.
   • To clear all alarms, click Delete All.

Related Topics
- Field Reference: Alarms Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Alarm Table, page 2
- Module Numbers, page 3
- Alarm Severity Levels, page 2

Viewing the Alarm Table and Clearing Alarms Using the CLI

Procedure

Step 1  Log in to the CLI.
Step 2  Enter the alarm command.
   The Alarm Table appears.
   Note the reference number (REFNO) for any alarms that you want to clear.
Step 3  (Optional) Clear alarms:
   • To clear all alarms, enter the clearalarm all command:
   • To clear one alarm, enter the following command, specifying the reference number (REFNO) from the alarm table.

   clearalarm reference-number

Related Topics
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Alarm Table, page 2
Configuring the System to Call You if There is a Major Alarm

Cisco Unified MeetingPlace can be configured to call you if a major alarm occurs. When you answer the phone call, you will be provided with the following information:

- Notification that an error has occurred that requires attention.
- A request to view the alarms.
- A request to acknowledge the alarm call.

**Restriction**

Pagers cannot be used to receive alarm calls.

**Procedure**

1. **Step 1** Log in to the Administration Center.
2. **Step 2** Click **System Configuration > Usage Configuration**.
3. **Step 3** Configure the following fields:
   - **Call capacity MINOR alarm (in percentage)**—Enter a value from 30–100 percent. The call capacity percentage for a minor alarm must be less than the percentage for a major alarm. The default value is 75 percent.
   - **Call capacity MAJOR alarm (in percentage)**—Enter a value from 91–100 percent. The call capacity percentage for a major alarm must be greater than the percentage for a minor alarm.
   - **Call out on major alarm**—Set to **Yes**.
   - **Phone number to call on alarm**—Enter the system administrator’s phone number.
4. **Step 4** Click **Save**.

**Related Topics**

- Usage Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace module

How to View the Current Status of the System

- Viewing the Current Status of the System in the Administration Center, page 8
- Viewing the Current Status of the Software Using the CLI, page 8
Viewing the Current Status of the System in the Administration Center

Use the system status to check the condition of the Cisco Unified MeetingPlace system. The system status shows the following information:

- System status details, such as mode, temperature, and power supply
- Each server name
- Each mailbox name and the number of messages that are in each mailbox
- Each module name and its status
- The CPU usage statistics

**Note** If you want to view the status of the Cisco Unified MeetingPlace system during a particular time period, see the “Obtaining and Viewing the System Information Capture (Infocap) Log” section on page 10.

**Procedure**

**Step 1** Log in to the Administration Center.

**Step 2** Click **Services > System Status**.

**Step 3** Click **View Status**.

**Related Topics**

- Field Reference: System Status Details Page in the Administration Center Page References for Cisco Unified MeetingPlace module
- Module Numbers, page 3
- Viewing the Current Status of the Software Using the CLI, page 8

Viewing the Current Status of the Software Using the CLI

**Procedure**

**Step 1** Log in to the CLI.

**Step 2** Enter the `swstatus` command.

If a module or Web Server is unexpectedly down, check the Alarm Table or the Exception Log for the reason.

**Example**

```
[mpxadmin@example-server ~]$ swstatus
Conference server 7.1.0.67
System mode: Up
Media control: Up

<table>
<thead>
<tr>
<th>MODULE NAME</th>
<th>STATUS</th>
<th>VERSION</th>
</tr>
</thead>
</table>
```
Using Alarms and Logs on Cisco Unified MeetingPlace

Viewing the System Log

The system log captures and buffers high-level details about system software activities. You can choose the severity level that you want to see. The output lists the date and time of the exception, the exception code, the file in which the exception occurs, and a text description of the exception.

**Note**
The system sorts messages by using the date and time that each message was added to the log file. If time is not synchronized across all Cisco Unified MeetingPlace servers, then the time used for sorting may differ from the displayed time stamps, and the log messages may seem to appear out of order. The system uses the time stamp for each message to filter out messages that are outside the specified start and end dates.

**Procedure**

**Step 1** Log in to the Administration Center.
**Step 2** Click Services > Logs > View System Logs.
**Step 3** Configure the fields.
**Step 4** Click View Logs.

**Related Topics**
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Viewing the Current Status of the System in the Administration Center, page 8
Viewing Log Information about System Backups

Go to the View Backup Logs page to see the last Informix backup log file, which lists the processes that occurred during the most recent backups. The page displays log files that are approximately 100KB or less and prompts you to save log files that are larger.

Viewing Backup Log Files

The browser cannot display log files that are larger than approximately 100KB. Cisco Unified MeetingPlace prompts you to save the file to your desktop.

Procedure

1. Sign in to the Administration Center.
2. Click Services > Logs > View Backup Logs.
3. Click Download from the View Backup Logs pane.
   - If the log file is smaller than approximately 100KB, details are displayed on the screen.
   - For large log files, the File Download window displays. Click Save on the File Download window to save the log file to your computer.

Related Topics

- Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module

Obtaining and Viewing the System Information Capture (Infocap) Log

The System Information Capture log provides details about the configuration and failure of the Cisco Unified MeetingPlace system during a particular time period. In general, every bug report should include the System Information Capture log. Running this log generates a very large zip file that you can send to Cisco TAC, who can help you troubleshoot problems. After you download the zip file, be sure to delete it from the /tmp directory to save space on your system.

Note

To display the current status of the Cisco Unified MeetingPlace system, instead of over a specific period of time, see the “Viewing the Current Status of the System in the Administration Center” section on page 8.
Using Alarms and Logs on Cisco Unified MeetingPlace

Configuring the Media Server Logging Levels

11

Note
During normal system use, you may use the su command to switch to the root user level. If you accidentally enter the root password into the command line, it is possible that the root password will be recorded in the BASH history file (~/.bash_history). If this happens, you should use the history –c command to clear the history; otherwise, the root password may be visible to other users and it might be captured as part of the infocap log.

Procedure

Step 1
Log in to the Administration Center.

Step 2
Click Services > Logs > System Information Capture.

Step 3
Enter or change the values on the System Information Capture Page.

Note
To receive better and faster service from Cisco TAC, enter as much information as you can. The details you provide will help Cisco TAC quickly understand and troubleshoot the problem.

Step 4
Click Capture Logs.

Step 5
Click OK.

Step 6
Obtain the data by taking one of the following actions:

• Navigate to the zip file specified on the page. The name of the zip file is based on the date and time parameters that you entered on the System Information Capture Page.

• Click Export to File.

Step 7
To view the System Information Capture log:

a. Extract the files from the zip file.

b. Open the index.html file.

Related Topics
• Field Reference: System Information Capture Page in the Administration Center Page References for Cisco Unified MeetingPlace module

What To Do Next
We recommend that you delete the zip file from the /tmp directory to save space on your system.

Configuring the Media Server Logging Levels

How to Configure Log Levels

On the Configure Log Levels Page, you can define log levels for Cisco Unified MeetingPlace web applications and for the Media Server. The system collects messages for the specified log level and all the levels below it. The higher the log level you specify, the more information is collected. Debug is the highest log level.
Caution

Increasing log levels can severely decrease system performance and even freeze Cisco Unified MeetingPlace. Only change the log levels if Cisco TAC requests that you change them.

This section contains these topics:

- Log Levels, page 12
- Configuring Log Levels, page 12

Log Levels

All log level changes occur during runtime; restarting is not required. These log levels are available:

- **Debug**—All logs are saved. This is the highest setting level.
- **Info**—Important events are logged. This is the default setting.
- **Error**—Only errors and exceptions are logged.
- **Warn**—Only warning errors are logged.

Related Topics

- Configuring Log Levels, page 12

Configuring Log Levels

**Procedure**

1. **Step 1** Log in to the Administration Center.
2. **Step 2** Click **Services > Logs > Configure Log Levels**.
3. **Step 3** Configure the fields.
4. **Step 4** Click **Save**.

Related Topics

- Obtaining and Viewing the System Information Capture (Infocap) Log, page 10
Recovering the Password for the root Account

Use this procedure to recover or change the root user level password, which is initially set during installation.

Procedure

Step 1
Reboot your server.

Step 2
Quickly press the spacebar when the words “GRUB” and “Cisco Unified Communications” appear on the screen.

Note
You have only three seconds to press the spacebar after this text appears. If you miss this window of time, then return to Step 1.

Step 3
The system displays three options. Use the up and down arrow keys to highlight the third entry. It starts with “kernel.”

Step 4
Press e to edit the entry.

Step 5
At the end of the entry, enter a space and then single.

Note
You must type a space before you type single.

Step 6
Press Enter to return the previous screen. The third entry should have the word single at the end.

Step 7
Press b to continue rebooting the server.

Step 8
At the prompt, enter /root/.security/unimmunize.sh.
Recovering the Password for the mpxadmin Account

Use this procedure to recover or change the mpxadmin user level password, which is initially set during installation.

**Procedure**

**Step 1** Log in to the Cisco Unified MeetingPlace operating system as the root user.

**Step 2** At the password prompt, enter the root password. The Cisco Unified MeetingPlace operating system desktop appears.

**Step 3** Right-click on the desktop.

**Step 4** From the menu, select *New Terminal*. This brings up a terminal session.

**Step 5** At the prompt, enter `/root/.security/unimmunize.sh`.

**Step 6** At the prompt, enter `passwd mpxadmin`. This tells the server to set a new password for the user called mpxadmin.

**Step 7** At the New password prompt, enter a new password. For security purposes, the password is displayed as a series of asterisks.

**Note** You may see a message that the password you entered is bad. Ignore this message.

**Step 8** At the Retype new password prompt, re-enter the same password again.

**Step 9** At the prompt, enter `/root/.security/immunize.sh`.

**Step 10** On the desktop, click the Red Hat icon.
## Recovering the User Password for the admin Profile

This task describes how to use the `userutil` command to reset the User password for the preconfigured “admin” profile.

### Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Cisco Unified MeetingPlace operating system as the mpxadmin user.</td>
</tr>
<tr>
<td>Step 2</td>
<td>At the password prompt, enter the mpxadmin password. The system displays the Cisco Unified MeetingPlace operating system desktop.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Right-click on the desktop.</td>
</tr>
<tr>
<td>Step 4</td>
<td>From the menu, select New Terminal. This brings up a terminal session.</td>
</tr>
<tr>
<td>Step 5</td>
<td>At the prompt, enter <code>userutil -p admin &lt;newpassword&gt;</code>.</td>
</tr>
<tr>
<td>Step 6</td>
<td>On the desktop, click the Red Hat icon.</td>
</tr>
<tr>
<td>Step 7</td>
<td>Select Log Out.</td>
</tr>
<tr>
<td>Step 8</td>
<td>Select OK.</td>
</tr>
</tbody>
</table>

### Related Topics
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- About Preconfigured User Profiles in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
Troubleshooting User Access Issues for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:31 pm

Problem Directory Service user cannot log in to Cisco Unified MeetingPlace.

Solution If all Directory Service users cannot log in, then check the AXL configuration settings on the Directory Service Configuration Page. Specifically, make sure:

- The value in the AXL URL field is correct and contains no empty spaces.
- The entries for the AXL username and AXL password fields are correct.

Solution If one or some Directory Service users cannot log in, then check the Cisco Unified MeetingPlace log in the following location: /opt/cisco/meetingplace/web/logs/userweb.out.

There are two reasons a Directory Service user might not be able to log in:

- The user does not exist in Cisco Unified MeetingPlace. Check the log for messages similar to “User <user_name> does not exist in the local database.”
- The user exists in Cisco Unified MeetingPlace but entered the wrong LDAP password. Check the log for messages similar to “addFailedloginAttemptforUser(String username=<user_name>).”

Solution Obtain the system information capture log, and send it to Cisco TAC.

Related Topics

- Configuring Cisco Unified MeetingPlace Directory Service
- Obtaining and Viewing the System Information Capture (Infocap) Log
- How to Resolve Authentication Problems
User Cannot Log In

Problem   An end user cannot log in to Cisco Unified MeetingPlace.

Possible Cause   The user profile is inactive or locked, perhaps due to too many failed login attempts.

Solution   For a locally authenticated user, set the User status field in the user profile to Active.

Solution   For an externally authenticated (Directory Service) user, make sure that the user account is active in the Device Used to Authenticate the Directory Service User field.

Possible Cause   The password has expired for the externally authenticated (Directory Service) user, whose passwords are stored and maintained on the external authenticating device instead of in the Cisco Unified MeetingPlace database.

Solution   Reset the expired password(s) on the Device Used to Authenticate the Directory Service User field.

Possible Cause   The password has expired for the locally authenticated user. The passwords expire after the amount of time specified by the following fields on the Usage Configuration Page:

- Change user password (days) for logging in from a workstation
- Change profile password (days) for logging in over the phone

Solution   Reset the expired password(s) by changing the following password fields in the user profile:

- User password and User password confirm for logging in from a workstation
- Profile password and Profile password confirm for logging in over the phone

Possible Cause   The end user does not exist in the user database. See “Searching for a Specific User Profile” in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module.

Solution   Add the end user to the user database. See “Methods for Adding User Profiles” in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module.

Possible Cause   The end user did not enter the correct User ID, User password, Profile number, or Profile password.

Note   The User password is case-sensitive.

Solution   If the user cannot remember the login information, then view the user profile to determine the correct User ID and Profile number. If necessary, reset the User password and Profile password for the user.

Related Topics

- Editing a User Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- External AXL Authentication for Directory Service Users in the Configuring Cisco Unified MeetingPlace Directory Service module
- How to Resolve Log In Problems in the User Guide for Cisco Unified MeetingPlace
- How to Resolve Authentication Problems
- Additional References for Troubleshooting User Access Issues, page 4
User Cannot Join a Meeting

**Problem** An end user can log in to Cisco Unified MeetingPlace but cannot join a meeting.

**Possible Cause** The user entered an invalid meeting ID.

**Solution** Have the user verify and enter the correct meeting ID.

**Possible Cause** The meeting is scheduled to begin at a different time.

**Solution** Have the user verify and join the meeting at the correct time.

**Possible Cause** The meeting requires a password. To check, go to the Meeting Details page in the end-user web interface.

**Solution** Make sure that the user has the correct password.

**Possible Cause** This meeting is only for users with Cisco Unified MeetingPlace profiles. To check, go to the Meeting Details page in the end-user web interface.

**Solution** Add a user profile for the user.

**Possible Cause** The meeting has reached the configured maximum number of ports per meeting.

**Solution** Configure higher numbers for the following fields on the Meeting Configuration Page:

- Maximum ports per reservationless meeting
- Maximum ports per scheduled meeting

**Possible Cause** (Microsoft Outlook integration only) The user was invited as part of an e-mail distribution list. Because Cisco Unified MeetingPlace for Microsoft Outlook does not expand distribution lists, the individual users on the distribution list are not added to the meeting.

**Solution** (Microsoft Outlook integration only) Instruct your users to do one of the following when scheduling meetings:

- Expand distribution lists before sending invitations.
- Instead of inviting distribution lists, invite the individual users.

**Possible Cause** There are not enough available ports for the meeting.

**Solution** The user needs to wait until a port becomes available.

**Problem** Problem: If you are using Internet Explorer or Firefox and your Cisco Unified MeetingPlace system has SSL enabled, you may encounter problems with the web conferencing meeting room not opening.

**Possible Cause** Possible Cause: The Internet Explorer browser’s Advanced Settings has the option "Check for server certificate revocation" checked and the certificate revocation list that it returned contains obsolete date. That is, the current date is not within the start and end date that the certificate revocation list states as its valid dates. Note that this Internet Explorer setting affects Firefox too.

**Solution** Solution: Uncheck the option "Check for server certificate revocation", restart Internet Explorer (or Firefox) and try joining your meeting again.
Related Topics
- “How to Resolve Join Meeting Problems” section in the User Guide for Cisco Unified MeetingPlace
- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace

Additional References for Troubleshooting User Access Issues

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>User authentication options and when each is used</td>
<td>User Authentication for Cisco Unified MeetingPlace</td>
</tr>
<tr>
<td>Troubleshooting end-user issues</td>
<td>“Troubleshooting and Getting Help in Cisco Unified MeetingPlace” in the User Guide for Cisco Unified MeetingPlace</td>
</tr>
<tr>
<td>Troubleshooting external authentication for Cisco Unified MeetingPlace Web Conferencing (LDAP and Windows authentication)</td>
<td>How to Resolve Authentication Problems</td>
</tr>
</tbody>
</table>
Troubleshooting Telephone Issues for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:52 pm

What to Try First When Troubleshooting Calls, page 1
How to Resolve Problems with Call Connections, page 4
How to Resolve Problems That Occur During Calls, page 13
For End Users: While it may be nearly impossible to avoid, users who are prone to triggering false "#" digits usually speak something like "umm" for a relatively long period of time. These sounds should be avoided or at least shortened. Additional References for Troubleshooting Telephone Issues, page 15

What to Try First When Troubleshooting Calls

• Checking the System Status, Alarms, and Logs, page 1
• Checking the Media Server Status, page 2
• Checking the Audio Licenses, page 3

Checking the System Status, Alarms, and Logs

Procedure

Step 1 Log in to the Administration Center.
Step 2 Check the system status:
   a. Click Services > System Status.
   b. Click View Status.
   c. Verify that the following text appears in the output:
      System mode: Up
      Media control: Up
   d. Verify that none of the modules are in DOWN state.
Troubleshooting Telephone Issues for Cisco Unified MeetingPlace

What to Try First When Troubleshooting Calls

e. If the system status details indicate an unexpected DOWN state, check the Alarm Table or the Exception Log to see why the module or system is down, and resolve the issue.

Step 3 Check the Alarm Table:

a. Click Services > Alarms.
b. If the alarm table displays a relevant alarm entry, check the Exception Log for actual relevance to and details for the failed call.

Checking the Exception Log is recommended because the Alarm Table combines multiple alarm occurrences into a single table entry.

Step 4 Check the system logs:

a. Click Services > Logs > View System Logs.
b. Set the parameters according to your needs.

For example, you may want to first limit the displayed output to major log entries for the day when the issues occurred.
c. Click View Logs.
d. Repeat Step 4 as needed.

For example, if the output does not include any relevant issues, then expand the output to include lower severity levels.

If you see relevant log entries for specific Module Numbers, you can narrow the log output to issues for a specific module.

Related Topics

- Using Alarms and Logs on Cisco Unified MeetingPlace module
- Troubleshooting Video Issues for Cisco Unified MeetingPlace module

Checking the Media Server Status

Procedure

Step 1 Log in to the Administration Center.

Step 2 Click Media Server Administration.

Step 3 Log in to the Media Server Administration.

Step 4 Click Resource Management > MCU.

Step 5 Verify that the following appears for each configured MCU:

- Status—Online
- Connection—Connected

Step 6 If the status of an MCU is unexpectedly offline, then do the following:

a. Click the MCU name.
b. Click the Online radio button.
c. Click OK.
Step 7 If an MCU is online but disconnected, then the MCU does not have network connectivity.

Step 8 Check the network connection status for the MCU Ethernet port:
   a. Log in to the Administration Center.
   b. Click Media Server Administration.
   c. Log in to the Media Server Administration.
   d. Click Resource Management > MCU in the sidebar.
   e. Click the name of an audio blade (MCU) entry.
   f. Click Go TO MCU...
      The Media Server Administrator (MSA) appears in a new browser window.
   g. If prompted, log in to the MSA.
   h. Click Board in the sidebar.
   i. Click the Addressing tab.
   j. Verify that the Ethernet Port status matches the port settings on the switch to which the MCU is connected.

Related Topics
- Troubleshooting Video Issues for Cisco Unified MeetingPlace module

Checking the Audio Licenses

Procedure

Step 1 Log in to the Administration Center.
Step 2 Click Maintenance > Licenses > Licenses Summary.
Step 3 Verify that the correct voice conferencing licenses are installed and enabled on your system.
Step 4 If necessary, reinstall licenses.

Related Topics
- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace
- Installing and Managing Licenses for Cisco Unified MeetingPlace module
- Troubleshooting Video Issues for Cisco Unified MeetingPlace module

How to Resolve Problems with Call Connections

- Dial-In Calls Fail, page 4
- Dial-Out Calls Fail, page 6
Dial-In Calls Fail

**Problem**  Users who call Cisco Unified MeetingPlace hear dead air or a busy signal.

**Solution**  See  “What to Try First When Troubleshooting Calls” section on page 1.

**Possible Cause**  Some third-party terminals are incompatible with and cannot establish connections with Cisco Unified MeetingPlace.

**Solution**  Make sure that your endpoints are supported for use with Cisco Unified MeetingPlace.

**Possible Cause**  Assuming that the phone number was dialed correctly, and that call routing is set up correctly:

- Dead air generally implies that call setup is failing for some reason, or that some device (such as Cisco Unified MeetingPlace or Cisco Unified Communications Manager) is completely unresponsive.

- A busy signal means that some device knew that the call could not be answered and responded with a busy indication. This could mean that a device is down or that all resources (such as ports on Cisco Unified MeetingPlace or bandwidth on a link) are in use.

**Solution**

---

**Step 1**  Log into the CLI.

**Step 2**  To troubleshoot a previous call that occurred at a known time, enter one of the following commands, specifying a start time (-b) shortly before the failed call attempt and a stop time (-e) shortly after the failed call attempt:

- For a call on the current day: `eventlog -G -b hhmm -e hhmm`
  
  For `hhmm`, enter the two-digit hour (in 24-hour format) and two-digit minute, according to the local server time of the Application Server.

- For a call on a previous day: `eventlog -G -b [YY]MMDDhhmm -e [YY]MMDDhhmm`
  
  For `MMDD`, enter the two-digit month and two-digit day. Specify the two-digit year `YY` if you are troubleshooting issues around the start of a new calendar year.

**Step 3**  To troubleshoot a call in real time, complete these steps:

a. Enter the following command:

   `eventlog -G -t`

b. Place a test call to the system.

**Step 4**  Read the log output to see how the system responds to the incoming call.

The following sample log output shows a successfully completed dial-in call:

```
[mpxadmin@example-server ~]$ eventlog -G -b 1030 -e 1040 07/15 10:36:43.14 P 0 RN MC a=013 mcpIncomingCallNotification
```
Step 5  If some log messages appear but the call was not successfully completed, then the call reached Cisco Unified MeetingPlace but was disconnected for some reason.

- If the log messages identify a reason for disconnecting the call, then investigate and resolve those issues.

- Make sure that the Media Server audio blades are synchronized. In the System Information Capture log, check for Media Server log messages that indicate SIP negotiation issues. If the log identifies reasons for SIP negotiation issues, then investigate and resolve those issues.

Step 6  If no log messages appear, then the call never reached Cisco Unified MeetingPlace.

- Check for and reconfigure any firewalls that may be preventing the call from reaching Cisco Unified MeetingPlace.

- Your call control device may not be configured properly. In Cisco Unified Communications Manager, make sure that the route patterns and trunks are configured correctly.

Related Topics
- Configuring Call Control for Cisco Unified MeetingPlace module
- How to Resolve Problems with Call Connections, page 4
- Obtaining and Viewing the System Information Capture (Infocap) Log in the Using Alarms and Logs on Cisco Unified MeetingPlace module
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- Configuring the Media Server Logging Levels in the Using Alarms and Logs on Cisco Unified MeetingPlace module
Dial-Out Calls Fail

**Problem** Dial-out calls do not work.

**Solution** Make sure that the user has dial-out privileges. See “Enabling Dial-Out Privileges for Users” in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module.

**Solution** See the “What to Try First When Troubleshooting Calls” section on page 1.

**Solution** If the failed dial-out calls are trying to reach an H.323 endpoint, then make sure that the directory number (DN) of the endpoint is not the same as any of the service prefixes that are configured in the Media Server. Because you cannot modify the service prefixes, you must instead modify the DN of the endpoint.

When the endpoint DN matches a service prefix, Cisco Unified MeetingPlace forwards the call to the Media Server instead of to the endpoint. To see a list of service prefixes, complete these steps:

1. Log in to the Administration Center.
2. Click **Media Server Administration**.
3. Log in to the Media Server Administration.
4. Click **Resource Management > Meeting Types**.
   
   Service prefixes are listed in the **Prefixes** column.

**Solution** If all dial-out calls are rejected with a “401 Unauthorized” response, then you need to disable digest authentication for the SIP trunk in Cisco Unified Communications Manager. Complete these steps:

1. Go to [http://ccm-server/](http://ccm-server/), where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Log in with your Cisco Unified Communications Manager administrator username and password.
3. Click **Device > Trunk**.
4. Find the SIP trunk for Cisco Unified MeetingPlace.
5. In the same row as that SIP trunk, click the link in the **SIP Trunk Security Profile** column.
   
   The SIP Trunk Security Profile Configuration page appears.
6. Uncheck **Enable Digest Authentication**.

   **Note** If other trunks also use this SIP trunk security profile and require digest authentication, then you should instead create a SIP trunk security profile specifically for the Cisco Unified MeetingPlace SIP trunk. See the Security Guide for your release of Cisco Unified Communications Manager at [http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html](http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html).

7. Click **Save**.

**Solution** Use the CLI to troubleshoot:
Step 1 Log into the CLI.

Step 2 To troubleshoot a previous call that occurred at a known time, enter one of the following commands, specifying a start time (-b) shortly before the call failed and a stop time (-e) shortly after the call failed:

- For a call on the current day: `eventlog -G -b hhmm -e hhmm`
  
  For `hhmm`, enter the two-digit hour (in 24-hour format) and two-digit minute, according to the local server time of the Application Server.

- For a call on a previous day: `eventlog -G -b [YY]MMDDhhmm -e [YY]MMDDhhmm`
  
  For `MMDD`, enter the two-digit month and two-digit day. Specify the two-digit year `YY` if you are troubleshooting issues around the start of a new calendar year.

Step 3 To troubleshoot calls in real time, complete these steps:

a. Enter the following command:

   `eventlog -G -t`

b. Place a test dial-out call by doing one of the following:

   - Use the end-user web interface to dial out to your phone.
   - Open a separate SSH session to the Application Server. As the root user, enter the `activity` command to make a test call without any specific ports.

Step 4 Read the log output as the system attempts to dial out.

The following sample log output shows a successfully completed dial-out call to phone number 1004:

```
mpxadmin@example-server ~$ eventlog -G -b 08281040 | more
08/28 10:40:39.96         RQ CP m=017 CPPLACECALL
08/28 10:40:39.96         SQ MC s=013 mcpPlaceCallRequest
08/28 10:40:39.96 P 0    RR MC s=013 mcpPlaceCallResponse Resp 0
08/28 10:40:39.99         RN MC s=013 mcpCallProgressNotification
08/28 10:40:42.59         RN MC s=013 mcpCallProgressNotification
08/28 10:40:42.62 P 0    RN MC mcpMediaActiveNotification (audio:HC, video:off)
08/28 10:40:42.62 P 0    SE CP m=017 UPDATEDMEDIAEVENT Resp 0
08/28 10:40:42.70 P 0    RC MC s=013 mcpPlaceCallCompletion Resp 0
08/28 10:40:42.70 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:48.31 P 0    RC MC s=013 mcpPlayFileListResponse Resp 0
08/28 10:40:48.31 P 0    RR MC s=013 mcpPlayFileListResp 0
08/28 10:40:48.31 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:48.31 P 0    RC MC s=013 mcpPlayFileListCompletion Resp 0
08/28 10:40:48.31 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:53.75 P 0    RC MC s=013 mcpPlayFileListCompletion Resp 0
08/28 10:40:53.75 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:55.61 P 0    RR MC s=013 mcpPlayFileListRequest
08/28 10:40:55.61 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:55.61 P 0    RC MC s=013 mcpPlayFileListResponse Resp 0
08/28 10:40:55.61 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:56.61 P 0    RR MC s=013 mcpPlayFileListRequest
08/28 10:40:56.61 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:56.61 P 0    RC MC s=013 mcpPlayFileListResponse Resp 0
08/28 10:40:56.61 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:41:02.05 P 0    RC MC s=013 mcpHangupNotification
08/28 10:41:03.64 P 0    SE CP m=017 HANGUPEVENT Resp 0
08/28 10:41:03.64 P 0    RN MC s=013 mcpHangupNotification
08/28 10:41:03.66 P 0    RR MC s=013 mcpHangupNotification
08/28 10:41:03.66 P 0    SE CP m=017 HANGUPEVENT Resp 0
08/28 10:41:03.66 P 0    RN MC s=013 mcpHangupNotification
```

GCID=6E3D0FA9752811DDA3630018FE735D02

```
08/28 10:40:39.96         RQ CP m=017 CPPLACECALL
08/28 10:40:39.96         SQ MC s=013 mcpPlaceCallRequest
08/28 10:40:39.96 P 0    RR MC s=013 mcpPlaceCallResponse Resp 0
08/28 10:40:39.99         RN MC s=013 mcpCallProgressNotification
08/28 10:40:42.59         RN MC s=013 mcpCallProgressNotification
08/28 10:40:42.62 P 0    RN MC mcpMediaActiveNotification (audio:HC, video:off)
08/28 10:40:42.62 P 0    SE CP m=017 UPDATEDMEDIAEVENT Resp 0
08/28 10:40:42.70 P 0    RC MC s=013 mcpPlaceCallCompletion Resp 0
08/28 10:40:42.70 P 0    SR CP m=017 CPPLACECALL Resp 0
08/28 10:40:42.70 P 0    Leg=520093713 Dialed=1004 ANI=outdial
```
In contrast, the following sample log output shows a dial-out call that failed, most likely because the dialed number was invalid and rejected by Cisco Unified Communications Manager. The error response 3105 indicates a general dial-out failure:

08/28 10:39:02.41         RQ CP m=017 CPPLACECALL
08/28 10:39:02.41         SQ MC s=013 mcpPlaceCallRequest
08/28 10:39:02.46  P 0    RR MC s=013 mcpPlaceCallResponse Resp 0
08/28 10:39:02.47         RN MC s=013 mcpCallProgressNotification
08/28 10:39:02.49         RN MC s=013 mcpCallProgressNotification
08/28 10:39:32.48  P 0    RC MC s=013 mcpPlaceCallCompletion Resp 19
08/28 10:39:32.48  P 0    SR CP m=017 CPPLACECALL Resp 3105

Step 5 If the log messages indicate that Cisco Unified Communications Manager or the far-end gateway responded to the call attempts:

- If the log messages identify a reason for disconnecting the call, then investigate and resolve those issues.
- Your call control device may not be configured properly. In Cisco Unified Communications Manager, make sure that the route patterns and trunks are configured correctly.
- In the System Information Capture log, check for Media Server log messages that indicate SIP negotiation issues. If the Media Server log messages identify a reason for the SIP negotiation issues, then investigate and resolve those issues.

Step 6 If the log messages show no response from Cisco Unified Communications Manager or the far-end gateway:

- Check for and reconfigure any firewalls that may prevent calls between Cisco Unified MeetingPlace and the call destination.
- Your call control device may not be configured properly. In Cisco Unified Communications Manager, make sure that the route patterns and trunks are configured correctly.

Step 7 If no log messages appear, then Cisco Unified MeetingPlace was unable to dial out.

- Make sure that Cisco Unified MeetingPlace is configured to find SIP proxies:
  - On the SIP Configuration Page, configure the SIP domain name field to match the SIP domain used by the SIP proxy servers or your local Cisco Unified Communications Manager node. In Cisco Unified Communications Manager, the SIP domain is specified under System > Enterprise Parameters in the Organization Top Level Domain field.
  - On the SIP Configuration Page, configure a SIP Proxy Server by entering at least one Hostname or IP address.
- Make sure that the Media Server is correctly configured.

Related Topics

- Configuring Call Control for Cisco Unified MeetingPlace module in the Administration Center Page
- References for Cisco Unified MeetingPlace module
- Obtaining and Viewing the System Information Capture (Infocap) Log in the Using Alarms and Logs on Cisco Unified MeetingPlace module
- How to Resolve Problems with Call Connections, page 4
Both Dial-In and Dial-Out Calls Fail

Problem: Both dial-in and dial-out calls fail.

Solution: See the “What to Try First When Troubleshooting Calls” section on page 1.

Solution: Make sure that the Media Server is correctly configured.

Solution: Make sure that the autonegotiation and duplex settings are correctly configured between the local switch port and the Cisco Unified MeetingPlace Application Server.

To change the duplex settings on the Application Server, log into the CLI as the root user, and use the net command to change the duplex settings.

Solution: Make sure that the Cisco Unified MeetingPlace Application Server is connected to a single switch port instead of a multiple-device Ethernet bus. Cisco Unified MeetingPlace works best when micro-segmented to use a single switch port. Sharing a bus with other devices can cause excessive collisions, which reduce bandwidth and cause unpredictable bandwidth availability.

Solution: Check for and reconfigure any firewalls between the phone and Cisco Unified MeetingPlace.

Possible Cause: Network congestion. You can take a trace of network traffic as close as possible to the Application Server eth0 port.

Solution: Reduce traffic in the local LAN by adding more switches and distributing the network devices between them.

Solution: Reduce the number of devices (and thus the traffic) on the local LAN by adding more routers to create more (but smaller) LANs. There might also be unused ports on the local router, in which case more routers are not needed.

Solution: Change network device settings to reduce unnecessary traffic. For example, add access lists to the local router to filter out irrelevant traffic.

Possible Cause: Bad frames were received.

Some phones provide network error statistics about how many bad frames have been received. See if the particular phone has these statistics. If so, see if the phone has registered receiving a large number of bad frames.

Solution: Check the configuration of the device that routes calls to Cisco Unified MeetingPlace. In Cisco Unified Communications Manager, make sure that the route patterns and trunks are configured correctly.

Related Topics
- Configuring Call Control for Cisco Unified MeetingPlace module
- How to Resolve Problems with Call Connections, page 4
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module

Established Calls Get Dropped

Problem: Successfully connected calls between users and Cisco Unified MeetingPlace get dropped.

Solution: See the “What to Try First When Troubleshooting Calls” section on page 1.
Solution  If meeting participants are consistently dropped after a certain period of time (for example, 12 hours) after meetings begin, then you may need to change the Maximum Call Duration Timer service parameter in Cisco Unified Communications Manager.

Solution  Use the CLI to troubleshoot:

**Step 1** Log into the CLI.

**Step 2** Enter one of the following commands, specifying a start time (-b) shortly before the call was dropped and a stop time (-e) shortly after the call was dropped:

- For a call on the current day: `eventlog -G -b hhm -e hhm`

  For `hhm`, enter the two-digit hour (in 24-hour format) and two-digit minute, according to the local server time of the Application Server.

- For a call on a previous day: `eventlog -G -b [YY]MMDDhhmm -e [YY]MMDDhhmm`

  For `MMDD`, enter the two-digit month and two-digit day. Specify the two-digit year `YY` if you are troubleshooting issues around the start of a new calendar year.

The following sample log output shows a normal dial-in call that was intentionally disconnected by the caller:

```bash
[mpxadmin@example-server ~]$ eventlog -G -b 1030 -e 1040
07/15 10:36:43.14 P 0   RN MC s=013 mcpIncomingCallNotification
07/15 10:36:43.14 P 0   SE CP m=018 NEWCALLEVENT Resp 0
07/15 10:36:43.14 P 0   Log=134217732 Dialed=90079172.27.106.63: ANI=18819172.27.99.180
07/15 10:36:43.14 P 0   RN MC s=013 mcpIncomingCallNotification
07/15 10:36:43.14 P 0   SE CP m=018 NEWCALLEVENT Resp 0
07/15 10:36:43.14 P 0   Log=134217732 Dialed=90079172.27.106.63: ANI=18819172.27.99.180
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
07/15 10:36:43.14 P 0   RN MC s=013 mcpHangupNotification
07/15 10:36:43.14 P 0   SE CP m=018 HANGUPEVENT Resp 0
```

**Step 3** If the log includes a far-end disconnect event, then the disconnect was probably initiated outside of Cisco Unified MeetingPlace.

Check for errors on the devices between the phone and Cisco Unified MeetingPlace. In a Cisco Unified Communications Manager environment, contact the Cisco Unified Communications Manager administrator to get a call session trace, which may indicate if and why Cisco Unified Communications Manager initiated the disconnect.
Step 4  If the log does not include a far-end disconnect event, then the disconnect was probably initiated by Cisco Unified MeetingPlace.

- If the log messages identify a reason for disconnecting the call, then investigate and resolve those issues.
- Check the Alarm Table or the Exception Log to for issues that may have caused the system to drop calls.

Related Topics
- Configuring the Maximum Call Duration in Cisco Unified Communications Manager in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- How to Resolve Problems with Call Connections, page 4

**Direct Inward Dial (DID) Call Does Not Connect to Meeting**

**Problem**  DID calls do not connect to the designated meeting.

**Solution**  Verify the configuration:

**Step 1**  Verify that the Route calls to meeting ID that matches DID field on the Usage Configuration Page is set to Yes.

**Step 2**  Verify that Cisco Unified Communications Manager is configured with a valid route pattern:

- The Route Pattern field contains the meeting ID.
- The Gateway/Route List field specifies the SIP trunk to Cisco Unified MeetingPlace.

**Step 3**  Schedule a test meeting using these parameters:

- Meeting ID: Use one that already has a matching route pattern in Cisco Unified Communications Manager.
- Time: Now.

**Step 4**  Place a test call to the meeting ID.

**Solution**  Use the CLI to check which DID phone number was received by Cisco Unified MeetingPlace:

**Step 1**  Place a test call to the meeting ID.

**Step 2**  Log into the CLI.

**Step 3**  Enter the following command:

```
eventlog | grep DID/DNIS | head
```

**Step 4**  Read the log output to see which DID phone number was received by the system.

For example, in the following output, the phone (with extension number 7178) dialed the DID phone number 1717.

```
08/11 13:51:54.14 P 0 In Call : DID/DNIS 1717, ANI 7178 ============ (1)
```
**Step 5**  Verify that the DID phone number actually matches the meeting ID of the desired meeting.

**Related Topics**
- Configuring Call Control for Cisco Unified MeetingPlace module
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
- How to Resolve Problems with Call Connections, page 4

---

**User Does Not Receive “Find Me” Calls for a Meeting**

**Problem**  A user does not receive Find Me calls for a meeting.

**Possible Cause**  The meeting was scheduled from Microsoft Outlook. Users are invited from the Microsoft Outlook directory and cannot be invited by Cisco Unified MeetingPlace profile. Therefore, Cisco Unified MeetingPlace treats everyone as a guest user. This limitation prevents the system from automatically dialing out to users using the Find Me feature.

**Solution**  Have the user dial in to the meeting.

**Related Topics**
- About the Find Me Feature in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module

---

**User Does Not Receive “Find Me” Calls to a Non-Direct-Dial Pager**

**Problem**  User does not receive Find Me calls on a non-direct-dial pager.

**Possible Cause**  Non-direct-dial pagers are pagers do not have individual phone numbers. Instead, a common phone number is shared by multiple pagers, each of which is identified by a unique PIN. For details, see “How the Find Me Feature Works with Pagers” in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module.

In Cisco Unified MeetingPlace, the common pager phone number shared is configured in the Phone number for non-direct-dial pagers field in the user group. The PIN, on the other hand, is configured in the Pager number field in the user profile.

Problems occur when the Group name is modified to move a user profile from one user group to another. The Phone number for non-direct-dial pagers for the new user group may not work for the pager.

**Solution**  Check and correct the following settings:
- Phone number for non-direct-dial pagers field in the user group
- PIN in the Pager number field in the user profile

**Related Topics**
- About the Find Me Feature in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module
How to Resolve Problems That Occur During Calls

- System Does Not Detect Key Presses, page 13
- One-Way Audio—User Cannot Be Heard By Other Participants, page 14

System Does Not Detect Key Presses

**Problem**  The system does not detect user input through the telephone user interface (TUI).

**Solution**

---

**Step 1**
Log into the CLI.

**Step 2**
Troubleshoot a call in real time by completing these steps:

- **a.** Enter the following command:
  
  `eventlog -G -t`

- **b.** Place a test call to the system.

- **c.** Press phone keys in response to the voice prompts.

**Step 3**
In the log, look for DTMFEVENT and mcpLegNotification messages, each pair of which would indicate that Cisco Unified MeetingPlace received the user input of a single digit.

The following sample log output shows that at 10:42:04, a caller on port 0 pressed the “1” key on the phone:

```
08/28 10:42:04.95  P 0    RN MC       mcpLegNotification (1)
08/28 10:42:04.95  P 0    SE CP m=017 DTMFEVENT Resp 0
```

**Step 4**
If you do **not** see DTMFEVENT and mcpLegNotification messages in the log, make sure that your call-control devices are set up to transport DTMF digits:

- In Cisco Unified Communications Manager SIP trunks to Cisco Unified MeetingPlace, make sure that the DTMF Signaling Method is set to No Preference.

- If the call passes through a voice gateway, then you may need to configure that gateway to use DTMF relay to transport DTMF digits.

- On the Media Parameters Page, try setting the Enable in-band DTMF detection field to Yes.


**Step 5**
If you **do** see DTMFEVENT and mcpLegNotification messages in the log, check the Alarm Table for TUI-related issues, and resolve them.

---

**Related Topics**

- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module
One-Way Audio—User Cannot Be Heard By Other Participants

**Problem**  User gets one-way audio only. User can hear the voice meeting, but other participants cannot hear the user.

**Solution**  Make sure that the user is not muted:

- Have the user check for a mute button on the phone or video endpoint.

If still in the voice meeting, have the user press #5 on the phone, in case another meeting participant muted the line.

"Talk-Off" (Triggering the Pound Key with Your Voice)

Talk-off is the unexpected detection of a digit (often a # key) by voice systems such as Cisco Unified MeetingPlace.

This is always a statistical possibility due to the imperfect nature of in-band (voice and DTMF sharing the same voice channel) DTMF tone detection algorithms in any voice device (Cisco Unified MeetingPlace, PSTN voice gateways). Ideally, in-band DTMF detection in these devices will correctly detect digits 100% of the time with no false detection of voice as digits. Practically, a small number of errors -- some voice will be falsely detected as a digit (aka "talk-off") -- are allowed. While most cases of talk-off cause no reaction in Cisco Unified MeetingPlace during a meeting -- false detection of any number "1" to "9" or "*" -- and are ignored, false detection of "#" or "0" can cause unexpected Cisco Unified MeetingPlace behavior.

The Cisco Unified MeetingPlace in-band DTMF detector meets the requirements of the "Bellcore Talk-off Test" specifications. The spec allows up to 500 false detections of any digit "0" to "9", "#" and "*" after the three hour test with real voice snippets. Cisco Unified MeetingPlace measures at 356 false detects for all these digits with only four false "#" and four false "0" digit detects during this period. So the Cisco Unified MeetingPlace DTMF detector exceeds the Bellcore spec and changes to the DTMF detection algorithm are very unlikely.

Realistically, though, people are all different. Unfortunately, some voices and speech patterns are more prone to triggering the DTMF detector than others, so certain users may have a much higher probability of seeing this problem.

**Recommendations:**

- For System Administrators: Use out-of-band digit transmission (RFC-2833, KPML) wherever possible. However, using RFC-2833 may only shift the talk-off problem from the Cisco Unified MeetingPlace DTMF detector to a voice gateway DTMF detector.
- For End Users: Use the best possible audio connection -- a land-line or a good IP connection with G.711. In some cases cordless phones may distort speech enough to make a user prone to talk-off.
For End Users: While it may be nearly impossible to avoid, users who are prone to triggering false "#" digits usually speak something like "umm" for a relatively long period of time. These sounds should be avoided or at least shortened.

**Additional References for Troubleshooting Telephone Issues**

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting user access issues</td>
<td>Troubleshooting User Access Issues for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Media Server installation and configuration</td>
<td></td>
</tr>
<tr>
<td>Configuring basic voice and video conferencing</td>
<td>Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video</td>
</tr>
<tr>
<td>Call control configuration</td>
<td>Conferencing module</td>
</tr>
<tr>
<td>QoS, network management, and overall network</td>
<td>Cisco Unified Communications Solution Reference Network Design (SRND) at</td>
</tr>
<tr>
<td>design for Cisco Unified Communications</td>
<td>Troubleshooting Video Issues for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Troubleshooting video issues</td>
<td></td>
</tr>
</tbody>
</table>
For End Users: While it may be nearly impossible to avoid, users who are prone to triggering false "#" digits usually...
Troubleshooting Video Issues for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:31 pm

- What to Try First When Troubleshooting Video, page 1
- How to Resolve Problems with Video Connections, page 3
- How to Resolve Problems with Video Endpoints, page 5
- Additional References for Troubleshooting Video Issues, page 6

What to Try First When Troubleshooting Video

- Checking the System Status, Alarms, and Logs, page 1
- Checking that Video Blades are Associated with Audio Blades in the Media Server, page 2
- Checking Video Licenses, page 3

Checking the System Status, Alarms, and Logs

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to the Administration Center.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the system status:</td>
</tr>
<tr>
<td></td>
<td>a. Click Services &gt; System Status.</td>
</tr>
<tr>
<td></td>
<td>b. Click View Status.</td>
</tr>
<tr>
<td></td>
<td>c. Verify that the following text appears in the output:</td>
</tr>
<tr>
<td></td>
<td>System mode: Up</td>
</tr>
<tr>
<td></td>
<td>Media control: Up</td>
</tr>
<tr>
<td></td>
<td>d. Verify that none of the modules show DOWN status.</td>
</tr>
<tr>
<td></td>
<td>e. If the system status details indicate an unexpected DOWN state, check the Alarm Table or the Exception Log to see why the module or system is down, and resolve the issue.</td>
</tr>
</tbody>
</table>
Step 3 Check the Alarm Table:
   a. Click Services > Alarms.
   b. If the alarm table displays a relevant alarm entry, then check the Exception Log for actual relevance to and details for the failed call.
      Checking the Exception Log is recommended because the Alarm Table combines multiple alarm occurrences into a single table entry.

Step 4 Check the system logs:
   a. Click Services > Logs > View System Logs.
   b. Set the parameters according to your needs.
      For example, you may want to first limit the displayed output to major log entries for the day when the issues occurred.
   c. Click View Logs.
   d. Repeat Step 4 as needed.
      For example, if the output does not include any relevant issues, then expand the output to include lower severity levels.
      If you see relevant log entries for specific Module Numbers, then you can narrow the log output to issues for a specific module.

Related Topics
   • Using Alarms and Logs on Cisco Unified MeetingPlace module

Checking that Video Blades are Associated with Audio Blades in the Media Server

Procedure

Step 1 Log in to the Administration Center.
Step 2 Click Media Server Administration.
Step 3 Log in to the Media Server Administration.
Step 4 Click Resource Management > MCU in the sidebar.
Step 5 Click the name of an audio blade (MCU) entry.
Step 6 Click Go TO MCU...
   The Media Server Administrator (MSA) appears in a new browser window.
Step 7 If prompted, log in to the MSA.
Step 8 Click MCU in the sidebar.
Step 9 Click the Media Processing tab.
Step 10 Verify that the correct video blades (EMPs) are listed with the audio blade (MCU).
       If a video blade is unexpectedly associated (or not associated) with the audio blade, then correct the configuration of the audio and video blades.
Step 11 Return to the Media Server Administration, which is in a different browser window from the Media Server Administrator (MSA).

Step 12 Click Resource Management > MCU in the sidebar.

Step 13 Repeat Step 5 through Step 12 for each audio blade (MCU) in the Media Server.

---

**Checking Video Licenses**

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Log in to the Administration Center.</td>
</tr>
<tr>
<td>2</td>
<td>Click Maintenance &gt; Licenses &gt; Licenses Summary.</td>
</tr>
<tr>
<td>3</td>
<td>Verify that the correct video licenses are installed and enabled on your system. If necessary, reinstall licenses.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace
- Installing and Managing Licenses for Cisco Unified MeetingPlace module

---

**How to Resolve Problems with Video Connections**

- Video Does Not Work, page 3
- Poor Video Quality, page 4

**Video Does Not Work**

**Problem** Video does not work, but audio does.

**Solution** Try pressing the hold button and then the resume button on the phone. This can sometimes clear up transient problems related to video.

**Possible Cause** The meeting scheduler cannot host video meetings, so video is not enabled for the meeting.

**Solution** Check the Video usage setting in the user profile of the meeting scheduler.

**Possible Cause** In Cisco Unified Communications Manager, the DTMF Signaling Method for the SIP trunk to Cisco Unified MeetingPlace is configured to use RFC 2833.

**Solution** Set the DTMF Signaling Method field to No Preference.
Problem  Your MCU blade is offline.

Solution  Open your Media Server administration page. Select Resource Management > MCU. The status of the blade should be “online” and “connected.” If it is not, select the desired MCU link. Ensure the radio button Online has been selected.

Possible Cause  The prefixes from the MCU to the Media Server are not synchronized.

Solution  Synchronize the prefixes from MCU to Media Server.

Possible Cause  Your call was set up using an audio-only prefix.

Solution  Ensure that the call is set up using a video prefix.

Possible Cause  The video rate is not set properly.

Solution  Make sure the video rate in the administration global settings is set properly. Sign in to the Administration Center. Select System Configuration > Meeting Configuration > Global Settings > Global Video Mode. Set the standard rate to 384 kbps maximum. Set the high rate to 2 Mbps maximum.

Possible Cause  MTP is enabled on the trunk from the CUCM to the Cisco MeetingPlace application server.

Solution  Make sure you disable MTP on the trunk from CUCM to the Cisco MeetingPlace application server.

Problem  A video conference call drops after 20 seconds. There is no video or audio on during that time. The SIP B2BUA log from the infoCap shows that Cisco Unified Communications Manager send TIAS with a negative value, [.INFO] [.MESSAGE] b=TIAS:-1000. This is because the "Video Call Bandwidth" field was set to "None" in the Region setting.

Solution  Set the correct value for the "Video Call Bandwidth" field.

Related Topics

- in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Configuring Cisco Unified Communications Manager 6.x or a Later Release: SIP Trunk to Cisco Unified MeetingPlace in the Configuring Call Control for Cisco Unified MeetingPlace module

Poor Video Quality

Problem  The video has a pixelated image or poor quality.

Possible Cause  Network issues are causing packet loss between the endpoint and Cisco Unified MeetingPlace.

Solution  Check the network for and correct any packet loss or excessive bandwidth utilization along the path between the video endpoint and Cisco Unified MeetingPlace.

Possible Cause  (CSCso95109) The input stream is from the Cisco Unified IP Phone 7985. This potentially affects all video calls with Cisco Unified MeetingPlace when the Cisco Unified MeetingPlace Global video mode is set to “standard rate” (384kb).

Solution  In the Administration Center, set the Global video mode field to High rate.

Solution  For full compatibility with Cisco Unified MeetingPlace, upgrade the Cisco Unified IP Phone 7985 to application load 4.1(7) or later.
Related Topics

- See the “Network Management” chapter and the “Call Admission Control, QoS, and Bandwidth” section in the “Cisco Unified MeetingPlace Integration” chapter of the Cisco Unified Communications Solution Reference Network Design (SRND) that applies to your version of Cisco Unified Communications Manager at http://www.cisco.com/go/designzone.
- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace

How to Resolve Problems with Video Endpoints

Note

Make sure that the video endpoints are supported by your release of Cisco Unified MeetingPlace.

- Video Endpoint Gets One-Way Video or No Video, page 5
- Call is Dropped When Entering a Meeting, Entering a Breakout Session, or Entering #31 to Dial Out, page 5
- Jumpy Video, page 6

Video Endpoint Gets One-Way Video or No Video

Problem A video endpoint gets no video or gets only one-way video.

Possible Cause The video endpoint does not support escalation to video via H.323 Empty Terminal Capabilities Set (ECS) or SIP re-INVITE after the voice call is established. This can result in either partial or complete lack of video reception after connecting to a meeting.

Solution Check with the endpoint vendor for a firmware update.

Solution Use the video terminal in Direct-to-Meeting Mode for Invited Terminals.

Related Topics

- How to Configure Video Terminal Profiles in the Configuring Endpoints for Cisco Unified MeetingPlace module

Call is Dropped When Entering a Meeting, Entering a Breakout Session, or Entering #31 to Dial Out

Problem A call is dropped when:

- Video endpoint is about to enter a meeting.
- Video endpoint is about to enter a breakout session.
- Video endpoint user enters #31 in the TUI to initiate a dial-out call.

Possible Cause The video endpoint does not support media transfer via H.323 Empty Capabilities Set (ECS) or SIP re-INVITE.

Solution Check with the endpoint vendor for a firmware update.
Solution Use the video terminal in Direct-to-Meeting Mode for Invited Terminals. See "How to Configure Video Terminal Profiles" in the Configuring Endpoints for Cisco Unified MeetingPlace module. Also:

- Do not attempt to move the video terminal into a breakout session.
- Do not initiate dial-out calls from the video endpoint by entering #31.

Jumpy Video

Problem The video display appears to be unstable.

Possible Cause When the Cisco Unified MeetingPlace Global video mode is set to standard rate, and and video terminals are using the H.264 codec, Cisco Unified MeetingPlace negotiates the video connection at 15 frames per second, which is consistent with the H.264 Level 1.2 specification. However, many video terminals ignore the frame rate limitation for H.264 Level 1.2 and send frames at a higher rate. This overloads the Cisco Unified MeetingPlace video blade and results in corrupted video output. Note that the effect may be observed on terminals other than the one causing the problem.

Solution Identify suspect terminals and check with the endpoint vendor for a firmware update.

Solution Set the Cisco Unified MeetingPlace Global video mode to high rate, or configure the video terminals to use H.263 instead of H.264.

Additional References for Troubleshooting Video Issues

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Video endpoint support</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting call connections</td>
<td>Troubleshooting Telephone Issues for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Media Server installation and configuration</td>
<td></td>
</tr>
<tr>
<td>Basic video conferencing configuration</td>
<td>Quick Start Configuration: Cisco Unified MeetingPlace Basic Voice and Video Conferencing module</td>
</tr>
<tr>
<td>Call control configuration</td>
<td>Configuring Call Control for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>QoS, network management, and overall network design for Cisco Unified Communications</td>
<td>Cisco Unified Communications Solution Reference Network Design (SRND) at</td>
</tr>
</tbody>
</table>

Troubleshooting E-Mail Notifications for Cisco Unified MeetingPlace

User Does Not Receive E-Mail Notifications

**Problem**  User does not receive e-mail notifications.

**Solution**  Check and correct the configuration:

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 1 | Check and correct the E-mail address in the user profile.  
If the user does not have a Cisco Unified MeetingPlace user profile, then make sure that the meeting scheduler entered the correct e-mail address for the user while scheduling the meeting. |
| Step 2 | Check and correct the E-mail type and format in the user profile:  
If the user does not have a Cisco Unified MeetingPlace user profile, then check and correct the E-mail type and format in the Guest Profile. |
| Step 3 | Verify that the system is configured to support the selected E-mail type and format.  
For example, if an SMTP option is selected, then make sure that the SMTP Server Configuration Page is properly configured. |
| Step 4 | Verify that the e-mail server (for example, SMTP server or Microsoft Exchange Server) is up and running. |
| Step 5 | (Microsoft Outlook integration only) Verify that the Cisco Unified MeetingPlace mailbox account on the Microsoft Exchange Server can send and receive e-mail messages. |

**Solution**  Check the logs.
Broken Click-to-Attend Meeting URL in E-Mail Notifications

**Problem**  
E-mail notifications that are sent to meeting invitees contain a broken URL for attending the meeting.

**Solution**  
Correct the Click-to-Attend Link Configuration on the Usage Configuration Page.

**Solution**  
As a short-term workaround, have the user copy the entire click-to-attend link and paste it into the address field of the browser. Delete any spaces or line breaks.

**Solution**  
(Microsoft Outlook integration only) The Microsoft Outlook client of the user or the Microsoft Exchange Server settings may be set to wrap text. For more information, see the following Microsoft Knowledge Base articles:

- [http://support.microsoft.com/support/kb/articles/Q250/5/58.asp](http://support.microsoft.com/support/kb/articles/Q250/5/58.asp)
- [http://support.microsoft.com/support/kb/articles/Q281/8/35.asp](http://support.microsoft.com/support/kb/articles/Q281/8/35.asp)

**Related Topics**
- Configuring Click-to-Attend Links

System Sends Excessive Random E-Mails

**Problem**  
Cisco Unified MeetingPlace sends excessive e-mails that crash your e-mail system.

**Possible Cause**  
The e-mails are generated by the cron script. The cron daemon sends an e-mail report of all its jobs to the e-mail address that is configured in the crontab file.

**Solution**  
Disable the e-mail reports by manually editing the crontab file. Specifically, change the line with MAILTO to read MAILTO= "".

Additional References for Troubleshooting E-Mail Notifications

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting user access issues</td>
<td>Troubleshooting User Access Issues for Cisco Unified MeetingPlace</td>
</tr>
<tr>
<td>Troubleshooting Microsoft Outlook front-end integration</td>
<td>Troubleshooting Cisco Unified MeetingPlace Scheduling from Microsoft Outlook</td>
</tr>
<tr>
<td>Troubleshooting Microsoft Outlook back-end integration</td>
<td>Troubleshooting Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface</td>
</tr>
<tr>
<td>Troubleshooting end-user issues</td>
<td>“How to Resolve Meeting Notification Problems” section in the User Guide for Cisco Unified MeetingPlace.</td>
</tr>
</tbody>
</table>
Troubleshooting Cisco Unified MeetingPlace Web Conferencing

Release 7.1
Revised: April 3, 2011 8:31 pm

This module explains how to troubleshoot common problems that can occur when configuring and maintaining Cisco Unified MeetingPlace Web Conferencing.

- How to Resolve Test Server Configuration Problems, page 1
- How to Resolve Authentication Problems, page 3
- How to Resolve Failed Server Issues, page 5
- How to Resolve Problems With Disk Space, page 9
- How to Resolve Problems During a Meeting, page 9
- How to Resolve Problems When Joining a Meeting, page 11
- How to Resolve Problems When Finding a Meeting, page 14
- How to Resolve Problems With Attachments and Recordings, page 15
- How to Resolve Problems With Secure Sockets Layer, page 23
- How to Resolve Web Server Time Synchronization Problems, page 23
- How to Resolve Web Server Configuration Problems, page 24

How to Resolve Test Server Configuration Problems

- Error Messages, page 2
Troubleshooting Cisco Unified MeetingPlace Web Conferencing

How to Resolve Test Server Configuration Problems

Error Messages

Error Message  Correct configuration.
Explanation  The IP address or DNS name for Hostname [Homepage] and Hostname [Web Conferencing] are specified correctly.

Error Message  Sorry unable to resolve Homepage IP address/hostname using nslookup.
Explanation  The system is unable to reach the DNS name or IP address that you configured for Hostname [Homepage].
Recommended Action  Complete the following procedure to change your entry for Hostname [Homepage].

Step 1  Sign in to end-user web interface.
Step 2  Click Admin > Web Server.
Step 3  From the “View” section of the page, click the name of the web server that you want to configure. This populates the “Edit” section of the page with predefined settings.
Step 4  Edit the entry for Hostname [Home Page].
Step 5  Restart all Cisco Unified MeetingPlace Web Conferencing services.

Note  When you restart the Web Server, all manual changes made to the registry are lost.

Error Message  Sorry unable to resolve Webconference IP address/hostname using nslookup.
Explanation  The system is unable to reach the DNS name or IP address that you configured for Hostname [Web Conferencing].
Recommended Action  Complete the following procedure to change your entry for Hostname [Web Conferencing].

Step 1  Sign in to the end-user web interface.
Step 2  Click Admin > Web Server.
Step 3  From the “View” section of the page, click the name of the web server that you want to configure. This populates the “Edit” section of the page with predefined settings.
Step 4  Edit the entry for Hostname [Web Conferencing].
Step 5  Restart all Cisco Unified MeetingPlace Web Conferencing services.

Note  When you restart the Web Server, all manual changes made to the registry are lost.
How to Resolve Authentication Problems

- LDAP Authentication Problem, page 3
- Windows Authentication Problem, page 4

LDAP Authentication Problem

**Problem** Cisco Unified MeetingPlace Web Conferencing is configured for LDAP authentication, but users are not being properly authenticated.

**Solution** Check the Cisco Unified MeetingPlace eventlog. LDAP messages appear in the eventlog every time an authentication is performed. If the authentication is successful, you will see a message such as the following: LDAP Authenticated user: <username>

If the authentication fails, one of the following error messages will be logged in the eventlog:

**Error Message** LDAP could not find user: <username>

**Explanation** The user was not found (LDAP_NO_SUCH_OBJECT).

**Error Message** LDAP could not authenticate user: <username>

**Explanation** User had bad credentials (LDAP_INVALID_CREDENTIALS); this is typically caused by using the wrong password.

**Error Message** ldap_simple_bind_s failed with error <hexadecimal number>

**Explanation** This message is logged when the authentication fails for any other reason besides user not found or bad credentials. The hexadecimal number in the error code indicates the failure reason. Descriptions of the hexadecimal codes can be found at http://msdn2.microsoft.com/en-us/library/aa367014.aspx.

**Related Topics**
- Using the Cisco Unified MeetingPlace Eventlog in the Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing module
Troubleshooting Cisco Unified MeetingPlace Web Conferencing

How to Resolve Authentication Problems

Windows Authentication Problem

**Problem** Internet Explorer prompts me for my Windows login information when I try to access Cisco Unified MeetingPlace even though I am already logged on to my computer with my domain Windows account.

**Possible Cause** You configured Windows authentication but used an IP address or FQDN when setting your Web Server Hostname [Home Page] parameter. If the server name in a URL request to the Web Server contains any periods, such as the dots in an IP address or a FQDN, the request is automatically routed to Internet Explorer’s Internet Zone, which is configured to not pass Windows credentials to the Web Server.

**Solution** Add the URL string for Cisco Unified MeetingPlace to Internet Explorer’s Trusted Zone or modify Internet Explorer's Internet Zone to automatically pass Windows credentials and log users into a website.

**Related Topics**
- Adding a URL String to Internet Explorer’s Trusted Zone, page 4
- Modifying Internet Explorer’s Internet Zone to Automatically Pass Windows Credentials, page 5

Adding a URL String to Internet Explorer’s Trusted Zone

This is the preferred method for working around Internet Explorer’s Internet Zone configuration.

**Caution** If you choose this workaround, you must apply this change to all end user computers.

**Procedure**

**Step 1** Open Internet Explorer.

**Step 2** Select **Tools > Internet Options**.

**Step 3** Click the **Security** tab.

**Step 4** Click **Trusted Zone**.

**Step 5** Click **Edit**.

**Step 6** Add the URL of your Web Server in the Trusted Sites window.

For example, if you set your Web Server Hostname [Home Page] parameter to *abc.company.com*, then enter **http://abc.company.com** in the list of trusted websites and click **Add**.

**Step 7** Click **OK**.

**Related Topics**
- Changing the Web Server Hostname From an IP Address to a Hostname in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module
Modifying Internet Explorer's Internet Zone to Automatically Pass Windows Credentials

Caution
If you choose this workaround, you must apply this change to all end-user computers.

Procedure

Step 1
Open Internet Explorer.

Step 2
Select Tools > Internet Options.

Step 3
Click the Security tab.

Step 4
Click Internet Zone > Custom Level.

Step 5
Click OK.

How to Resolve Failed Server Issues

Note
When restoring failed servers, users will experience a slight delay before the system regains flawless functionality. This delay is equal to the Load Stats Poll Period value on the Site configuration page * five. The Load Stats Poll Period defaults to one minute. Therefore, the delay defaults to five minutes.

- Web Server Fails During a Conference, page 6
- All Web Servers in a Load Balancing Cluster Have Failed, page 6
- External Users are Disconnected from a Web Conference, page 6
- Error Message: Read Failure in Named Pipe in Audio Service, page 7
- Web Conferencing Does Not Start After Moving Time on the Web Server, page 7
- Time is Not Synchronized Between the Web Server and the Application Server, page 7
- Cannot Start Cisco Unified MeetingPlace Web Conferencing Services, page 8
- Server Crashes When the Shared Storage Location is Interrupted, page 9
Web Server Fails During a Conference

**Problem**  A Web Server fails during a web conference and all users are temporarily disconnected from the web-conferencing portion of their meeting.

**Possible Cause**  There was an Agent Service problem. Other Web Servers in the cluster detected that a server was down and began to exclude it from the load balancing cluster.

**Solution**  Tell users to rejoin their web conference by clicking the click-to-attend link in their meeting notification or by accessing the Current Meeting page from the Web. The meeting console client automatically tries to reconnect the user to the server. If this attempt fails, the meeting console attempts to connect to the server designated as the backup for that meeting. If no connection is made after 15 seconds, the client continues attempting to contact the primary, then the backup server. After 30 unsuccessful attempts, the client stops trying and notifies the user that it is unable to reconnect.

**Possible Cause**  There was a server components problem. Other Web Servers in the cluster were unable to detect that a server was disabled since its Agent Service was fully functional. As a result, the failed Web Server was not excluded from the load balancing cluster and continued to have users routed to it in error.

**Solution**  In the Windows Services control panel, restart the Cisco Unified MeetingPlace Web Conferencing Service. This should restore web-conferencing functionality.

---

**Note**  When you restart the Web Server, all manual changes made to the registry are lost.

All Web Servers in a Load Balancing Cluster Have Failed

**Problem**  All Web Servers in a load balancing cluster are nonfunctional.

**Possible Cause**  The SQL Server database is on a failed server.

**Solution**  Restore the database. Users are unable to conduct web conferences until the database is restored.

External Users are Disconnected from a Web Conference

**Problem**  External users are disconnected from a web conference.

**Possible Cause**  The Web Server in the DMZ has failed.

**Solution**  Configure another server as your external Web Server. Users are unable to conduct external meetings until you complete this step. To configure an external Web Server, see “Configuring Redirection of External Meetings” in the Configuring External Access to Cisco Unified MeetingPlace Web Conferencing module.
Error Message: Read Failure in Named Pipe in Audio Service

**Error Message**  Read Failure in Named Pipe in Audio Service.

**Explanation**  The Cisco Unified MeetingPlace Web Conferencing Service has lost its connection to the Cisco Unified MeetingPlace Audio Service. This could be due to a manual restart or an error.

**Recommended Action**  Do nothing. The Web Conferencing Service will reconnect automatically; the error message is for information only.

Web Conferencing Does Not Start After Moving Time on the Web Server

**Problem**  User moved the time backwards then forward on the Web Server. Now Web Conferencing does not start.

**Possible Cause**  There may be bad “date_begin” values in the pps_acl_quotas table in the MPWEB Slave database used by the Web Server (MPWEB_xxxx). Those dates are initialized at the time when Web Conferencing is installed so if the time was moved backwards, Web Conferencing will refuse to work because it cannot find the proper “disk quota” permissions.

**Solution**  Manually change the “date_begin” values pps_acl_quotas table in the MPWEB Slave database to some time in the past relative to the current system time.

Time is Not Synchronized Between the Web Server and the Application Server

**Problem**  Web Conferencing configures the Windows Time service on the Web Server to synchronize its time with the Application Server. When the Cisco Unified MeetingPlace Web Conferencing master service comes up, it should trigger a time synchronization with the Application Server. This is not happening.

**Solution**  Complete the following workaround.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 1</strong></td>
<td>Stop the Cisco Unified MeetingPlace Web Conferencing master service.</td>
</tr>
<tr>
<td><strong>Step 2</strong></td>
<td>Look at the time on both the Application Server and the Web Server and try to adjust the clock on the Web Server to match the time on the Application Server within 30 seconds.</td>
</tr>
</tbody>
</table>
| **Step 3** | Invoke the Windows Time Service to synchronize between the Web Server and the Application Server:  
  a. Open a DOS command window.  
  b. Enter the following command: `w32tm/resync`  
  c. Enter the following command to see if the time is now within 30 seconds: `w32tm /monitor /computer:hostname_AppServer` |
Cannot Start Cisco Unified MeetingPlace Web Conferencing Services

**Problem** A Web Server fails and then does not come back up. Cannot start Cisco Unified MeetingPlace Web Conferencing services.

**Possible Cause** You configured shared storage for your Web Server using a Windows account that does not have administrator privileges.

**Solution** Reinstall Cisco Unified MeetingPlace Web Conferencing.

**Solution** Complete the following steps to manually remove the shared storage entries from the SQL database tables. This will allow you to start Web Conferencing services and reconfigure shared storage using an account that has administrator privileges on the Web Server.

---

**Step 1** Open SQL Server Enterprise Manager.
Click **Start > All Programs > Microsoft SQL Server > Enterprise Manager**.

**Step 2** Navigate to the MPWEB database.
Click the + signs next to **SQL Server Group > LOCAL > Databases > MPWEB** to open the appropriate directory trees.

**Step 3** Click **Tables** in the MPWEB directory.
A list of tables opens in the right pane.

**Step 4** Right-click **Site** in the right pane.

**Step 5** Select **Open table > Return all rows**.
The Site database table displays.

**Step 6** Scroll to the right and set all entries in the following columns to `<NULL>`:
- **SvcStartAsDomain**
- **SvcStartAsUsername**
- **SvcStartAsPassword**

> **Note** Sometimes the column entries appear to be blank after you enter `<NULL>`. This is okay.

**Step 7** Navigate to the MPWEB slave database in the left pane of the SQL Server Enterprise Manager.
Click the + signs next to **SQL Server Group > LOCAL > Databases > MPWEB_XXXX_XXXX** to open the appropriate directory trees.

**Step 8** Click **Tables** in the MPWEB_XXXX_XXXX directory.
A list of tables opens in the right pane.

**Step 9** Right-click **PPS_CONFIG** in the right pane.

**Step 10** Select **Open table > Return all rows**.
The PPS_CONFIG database table displays.

**Step 11** Delete the row that contains the NAME `config-shared-storage`.
Server Crashes When the Shared Storage Location is Interrupted

Problem  The Web Server crashes when network access to the shared storage location is interrupted.
Solution  Restore access to the shared storage location.

Related Topics
- Configuring Shared Storage in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

How to Resolve Problems With Disk Space

- Error Message: Operation Failed, page 9

Error Message: Operation Failed

Problem  I see this error message on the Web Server: [1228] Operation Failed. Currently on Web Server X, SQLServer Loadtest, MPServer Y.

I then see this error message in the Eventlog window: The log file for database MPWEB is full. Back up the transaction log for the database to free up some log space.

Possible Cause  It is likely that the SQL database files are too large and that users are unable to sign in to Cisco Unified MeetingPlace on the web.
Solution  Complete the following procedure.

Step 1  Go to SQL Enterprise Manager.
Step 2  Select the database Properties page.
Step 3  Select Options > Auto Shrink.
Step 4  Set the database recovery model to Simple or perform a backup of the log.

How to Resolve Problems During a Meeting

- A Few Users Are Dropped From a Meeting, page 9
- All Users Are Dropped From a Meeting, page 10
- Users Continue to Get Dropped From a Meeting, page 11

A Few Users Are Dropped From a Meeting

Problem  A few users were dropped from the web conference, but others maintained their connection.
Solution  Ask those users who lost their connection to close their meeting console window and rejoin the web conference. If the problem persists, complete the following checks:
• Make sure the user web browser and operating system are supported, and that a supported version of Adobe Flash Player is installed. For a list of supported web browsers, see the System Requirements for Cisco Unified MeetingPlace, at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_device_support_tables_list.html.

• If the participant was using a remote access service, like Shiva, to connect to the company LAN, determine if an inactivity timeout disconnected them from the Web Server. To avoid the inactivity timeout, users should periodically issue keyboard or mouse button commands; mouse movements are not registered as activity.

• If accessing through a Virtual Private Network (VPN), make sure the security policy is deactivated.

• Verify that the user can ping the Cisco Unified MeetingPlace Web Conferencing gateway.

All Users Are Dropped From a Meeting

Problem  All of the users in the web conference were dropped.

Possible Cause  All participants left the voice conference and the Disconnect Empty Port Timer ended the entire meeting, including the web conference.

Solution  If the meeting is over, do nothing. Otherwise, schedule a new meeting.

Possible Cause  The meeting scheduler or host ended the meeting.

Solution  If the meeting is over, do nothing. Otherwise, schedule a new meeting.

Possible Cause  If meeting participants are still in the voice conference and the host of the meeting did not stop sharing, an error might have occurred on the Web Server.

Solution  Determine if the Web Server is functioning correctly by completing the following procedure.

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>From the Web Server, open the Windows Services control panel and make sure that the Cisco Unified MeetingPlace Web Conferencing Service is running.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Check the Windows Event Viewer Application log for any errors related to the Web Server.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Check the Event log for any messages related to the Web Server.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Report any major errors to your Cisco support representative.</td>
</tr>
</tbody>
</table>
Users Continue to Get Dropped From a Meeting

**Problem**  Users keep getting disconnected from a web conference (several minutes after they have been reconnected to the web conference, they are disconnected again).

**Possible Cause**  The network bandwidth is too limited to allow users to participate at this time. Users are on a dial-up connection or the network is congested.

**Solution**  If other applications are running in the background that consume additional bandwidth, such as streaming, synchronizing e-mail and so forth, stop these operations during the web conference. Or, use the Optimize Room Bandwidth option in the Meeting menu of the meeting console to lower the bandwidth used by the meeting. (This option is available to System Managers and other meeting moderators.)

**Possible Cause**  Users are connected to a proxy server with lengthy time-out delays.

**Solution**  Alter the connection so that the proxy server time-out setting is longer than five minutes. If this is not permitted, contact your Cisco support representative for instructions on configuring your proxy server and the Cisco Unified MeetingPlace system.

**Related Topics**
- Proxy Servers in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module

---

How to Resolve Problems When Joining a Meeting

- No One Can Join, page 11
- Some Users Cannot Join the Meeting, page 12
- Cannot Join Due to MPAgent Problem, page 12
- Cannot Join Due to Session Problems, page 13
- Problems Dialing Out from the Meeting Console, page 14

**No One Can Join**

**Problem**  No one can join the web conference.

**Possible Cause**  The problem is probably related to the Web Server. For example, a Windows service is down.

**Solution**  To troubleshoot this problem:

1. Make sure the Cisco Unified MeetingPlace Web Conferencing Service is running on the Web Server. For more information about this service, see “About the Cisco Unified MeetingPlace Web Conferencing Service” in the Managing Cisco Unified MeetingPlace Web Conferencing Services module.

2. If there is a problem with a Windows service, go to the \Cisco Systems\MPWeb\datasvc directory and run dcdiags.bat as soon as possible to generate a server log.

3. Check the Eventlog for any messages related to the Web Server. Report any major errors to your Cisco support representative.
4. Check the Windows Event Viewer and Application log, for any errors related to the Windows server.

See the following sections for additional details:

- Some Users Cannot Join the Meeting, page 12
- Cannot Join Due to MPAgent Problem, page 12
- Cannot Join Due to Session Problems, page 13
- How to Resolve Problems When Finding a Meeting, page 14
- Template Cannot Be Found, page 14

### Some Users Cannot Join the Meeting

**Problem** Some users are able to join the web conference but others are not.

**Solution** Make sure that those who are unable to join have the following:

- Network connectivity (that is, are they connected through a switch or a hub?)
- Internet access

If users have network connectivity and Internet access, complete the following checks:

- Make sure that users can view the Connect button from the Cisco Unified MeetingPlace Web Conferencing Meeting Information page.
- Determine if users are attending the web conference over a network or dial-up connection. If users are attending on a dial-up connection, it is possible that the Web Server is disconnecting them because their connection is too slow.
- If external users are unable to join a web conference, it is possible that you configured the Web Server hostname incorrectly. Make sure that you followed the steps in “Changing the Web Server Hostname From an IP Address to a Hostname” in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module.
- If external users are accessing web conferencing through a proxy server, it is possible that you configured the proxy server in a way that does not allow access to the web conference. For proxy server requirements, see in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module.
- It is possible that you need to configure the Web Server to use Secure Sockets Layer (SSL) so that external users can join a web conference using an HTTPS connection. Even if external users are behind a proxy server, they should be able to join a web conference. For SSL configuration details, see “How to Configure Secure Sockets Layer” in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module.

### Cannot Join Due to MPAgent Problem

**Error Message** MPAgent is not available, please try again later.

**Explanation** The Cisco Unified MeetingPlace Agent Service is either down or not responding.

**Recommended Action** Stop and restart the Cisco Unified MeetingPlace Web Conferencing Service.
Note When you restart the Web Server, all manual changes made to the registry are lost.

Note Running some services, such as MPAgent, can use as much as 90 percent of your CPU. Fortunately, these services run at a low priority so the CPU spikes do not impact important system functions.

Related Topics
- About the Cisco Unified MeetingPlace Web Conferencing Service in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

Cannot Join Due to Session Problems

Error Message Session is stale.

Explanation You signed in to Cisco Unified MeetingPlace from a different location than the one you originally used and the system disconnected your first browser connection. If you then go back to the first browser, you will receive a “stale session” notification.

Explanation You signed in to Web Conferencing, but did not participate in the session for over an hour. The system disconnected you to free some room for new users and informs you that your session is stale.

Recommended Action Web Conferencing keeps session information about each user who connects to the home page to find, schedule, or update a meeting or configure account settings. The session information is kept for a minimum of one hour from the your last session up to a maximum of 24 hours. Close the connection with the stale session and try to connect again.

Error Message Your session has expired. You will need to log in again.

Explanation It is possible that you have Content Advisor enabled on your browser. Cisco Unified MeetingPlace Web Conferencing does not support Content Advisor. If Content Advisor is enabled, the following scenario will occur:

1. User tries to access Web Conferencing and a Content Advisor window displays.
2. User clicks Always Allow This Web Site to Be Viewed.
3. User then signs in and clicks Remember Me.
4. When the user clicks an option tab, such as Schedule Meeting, Attend Meeting and so on, the user receives an error message.

Recommended Action Complete the following.

Step 1 Verify that Content Advisor is disabled:
   a. Open your browser.
   b. Go to Tools > Internet Options > Content > Content Advisor.
   c. Disable Content Advisor.
Problems Dialing Out from the Meeting Console

**Problem** A user is unable to dial out to a number by clicking Connect in the meeting console, but the number can be reached by using #31 to dial out.

**Solution** You may need to adjust the translation table on the Cisco Unified MeetingPlace Application Server to account for the R symbol (wait for answer supervision from the far end) that is appended to web outdials. Outdials via #31 do not append the R symbol. Adding R? to the pattern in the translation table matches 0 or 1 occurrences of the R symbol, so that both web and #31 outdials can be matched correctly.

In the following example, the Application Server translation table is configured to prepend a 5 to the dial string 4541:

```
# From  To  Group DestType  Comment
# -----------------------------------------------------
# 4541 5\0 1 GENERIC add 5 to 45451
.*\0 ANYGROUP GENERIC No translation
```

In this case, the cptrace command on the Application Server for a web outdial to extension 4541 results in the following example trace:

```
01/25 11:12:44.75 P NDV State : 13
01/25 11:12:44.75 P NDV Outdial : UserID 100 RetCode 3107
Dest 4541R Trans Dest
01/25 11:12:44.72 P NDV Substate : 4
An outdial via #31 to the same number results in the following output:
01/25 11:07:13.95 P 6 State : 12
01/25 11:07:13.95 P 6 Outdial : UserID 3 RetCode 0
Dest 4541 Trans Dest 54541
01/25 11:07:13.95 P 6 Substate : 7
```

In this case, the translation table should be adjusted to account for the possible addition of the R symbol by adding R? as follows:

```
# From  To  Group DestType  Comment
# -----------------------------------------------------
# 4541R? 5\0 1 GENERIC add 5 to 45451
.*\0 ANYGROUP GENERIC No translation
```

If you need assistance updating the translation tables, contact Cisco TAC.

How to Resolve Problems When Finding a Meeting

- Template Cannot Be Found, page 14

Template Cannot Be Found

**Problem** You see the following error message: Template cannot be found.

**Solution** Verify that the template file specified in the error message or error page exists in the `<drive>:\Program Files\Cisco Systems\MPWeb\Template` directory.
If the template does exist, make sure that the directory permissions allow
Cisco Unified MeetingPlace Web Conferencing to access the template files, that is, set the
Everyone group with full access permissions and then restrict who is a member of that group.

If the templates are not in the \Template directory, re-install the template files.

**Caution**

If a reinstall is run, any customized files that are not read-only are overwritten.

---

### How to Resolve Problems With Attachments and Recordings

- No Recording Space Available, page 15
- Recording Files Not Appearing on the Web, page 16
- Tinny Buzz on WMA Recordings, page 18
- Web Recording is Silent, page 19
- Audio and Video Playback Not Synchronized, page 19
- Cannot Access Attachments From the External Web Server, page 20
- Cannot Attach Files Larger than 10KB to the Web Meeting Room, page 20
- Error: Access is Denied, page 20
- Problems Accessing Meeting Recordings When Using Shared Storage, page 21
- Cannot Play Windows Media Recordings or Attachments, page 22
- Recordings Stuck in “Processing Now” State, page 23

---

### No Recording Space Available

**Problem**  User hears a prompt stating that no recording space is available.

**Possible Cause**  The “No recording space available” prompt plays when there are issues starting up
a recording leg. One example of when this occurs is when someone attempts to start a recording
when recording resources are all used up (currently limited to 100).

**Solution**  Wait before trying to start recording again.

**Possible Cause**  The Recording/Streaming Service (RSS) is not running.

**Solution**  Verify the issue by using the CLI below to show the service is stopped:

```
[root@geldridg-kapp ~]# mpx_sys status
...
rss is stopped...
...
```

To try and get the service running again...

```
[root@geldridg-kapp ~]# service mpx_rssctrl start
Starting MeetingPlace Recording/Streaming Service: [ OK ]
[root@geldridg-kapp ~]#
```
Possible Cause There are no more ports available to turn on recording.

Solution Check the license setting and available ports. You can check ports in use by using the ‘CSTest -s’ CLI command on the Application Server.

Related Topics
- Recording Resources and Port Usage in the Configuring Recordings for Cisco Unified MeetingPlace module

Recording Files Not Appearing on the Web

Problem When the user goes to the Past Meetings page on the end-user web interface, the icon for a recording does not appear.

Possible Cause In comparison with other Cisco Unified MeetingPlace services, the Audio Service conversion process takes a lower priority. Therefore, during the peak hours of Cisco Unified MeetingPlace usage, audio files are converted and posted at a much slower rate. On an idle system, a recording can be accessible in minutes, while during peak hour activity it can take hours.

Solution Give the system some time to do the conversions. If you are still experiencing problems, complete the following checks:

- Go to the Windows Services option (Start > Control Panel > Administrative Tools > Services) and verify that the Cisco Unified MeetingPlace Replication Service and the Cisco Unified MeetingPlace Audio Service are running.

- From the Meeting Information page on the Cisco Unified MeetingPlace web page: Click More Options and verify the Automatically Start Recording parameter. If this parameter is set to Yes, recording will auto-start as soon as the meeting starts. If it is set to No, participants must manually start the recording by either pressing #61 on their phones or by choosing Meeting > Start Recording from the meeting console.

- Schedule a test meeting to check the audio conversion process. The success or failure of this test will give you more information as to the cause of your problem. See Scheduling a Test Meeting to Check the Audio Conversion Process, page 18.

Possible Cause The conversion control is not set properly.

Solution Make sure that the recording files are configured to convert properly by checking the Admin > Audio Conversion page on the Web Server.

Possible Cause The recording file has not completed its conversion process.

Solution Make sure that verbose logging on the Web Server is on then verify the progression of the recording file conversion as indicated by the following example.

Note You can only confirm the existence of a recording file on the Application Server within 24 hours (plus time for the 2AM purge task to run) of the recording. After 24 hours, the file is removed from the Application Server.

Example:

Step 1 Start with the Application Server.
Troubleshooting Cisco Unified MeetingPlace Web Conferencing
How to Resolve Problems With Attachments and Recordings

[mpxadmin@geldridg-kdev ~]$ mtginfo –m <Meeting ID> | more

Step 2
Look for ReadConf of 0x36 (54.)

Step 3
Now go to the conference folder 54 as seen below.

[mpxadmin@geldridg-kapp conf]$ pwd
/opt/cisco/meetingplace/afs/conf/000054
[mpxadmin@geldridg-kapp conf]$ ls -l -t
total 96
drwxrwxr-x  2 mpxadmin mpx 4096 May  9 08:07 000054

Tip
54 will be used for the directory name on the Windows server for the storage of the recording.

Step 4
If a recording occurred, you will see a recorded file named av_rec.mp4.

Step 5
Use the record_file_info command to view the file and check that it is valid and not corrupt.
The file indicates that it is an audio and video recording with specifics about the recording:

[mpxadmin@geldridg-kapp 000054]$ ls
att_20.dat  av_rec.mp4  conf_8888 (8888 is the conf ID from the web schedule page)
[mpxadmin@geldridg-kapp 000054]$ record_file_info av_rec.mp4
av_rec.mp4:
Track   Type    Info
1       audio   G.711 uLaw, 22.616 secs, 64 kbps, 8000 Hz
2       video   H264 Baseline@3, 22.616 secs, 6 kbps, 352x288 @ 14.105058 fps
start 1:
Start time 09 May 2008 08:06:06.678 (1210345566)
Duration: 22.61 (180880, 8000) seconds
Audio Start Sample: 1
Video Start Sample: 1
[mpxadmin@geldridg-kapp 000054]$ 

Step 6
This displays the export of the .mp4 file to the web replication service.

[root@geldridg-kapp ~]# eventlog -G | grep "Export: conf" | grep 0054 | more
05/09 08:06:58.23         Export: conf/000054/av_rec.mp4
[root@geldridg-kapp ~]# 

Step 7
Check the Web Server for the meeting recording.
- The stored converted files for conference folder 54 (which match folder ID 54 on the Application Server) are located at: C:\Program Files\Cisco Systems\MPWeb\Meetings\54
- The files in this directory will have a name such as ‘MtgRec_<xyz>.abc’

Step 8
If verbose logging is on, check the log file for any reason why conversion may not have occurred.
- You can find the log file at: C:\Program Files\Cisco Systems\LogFiles\temp\MPWEB_LBJ_<date>
- You can search the log file for the recorded file using the same name as in Step 7: ‘MtgRec_<xyz>.abc’
Scheduling a Test Meeting to Check the Audio Conversion Process

Procedure

Step 1  Open the Cisco Unified MeetingPlace Web Conferencing Eventlog.
   a. From the Web Server, right-click the Cisco Unified MeetingPlace icon in the system tray.
   b. Select eventlog.

Step 2  Schedule a test meeting.

Step 3  Join the meeting and start recording.

Step 4  Terminate the meeting after a few minutes.

Step 5  In the Eventlog window, or in the Gateway SIM log file, look for the recording conversion progress.

Tip  See the example in Recording Files Not Appearing on the Web, page 16 for an explanation of what the recording file name looks like in the log files.

Related Topics
- Replication Service in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

Tinny Buzz on WMA Recordings

Problem  User hears a tinny buzz on WMA recordings.

Solution  Complete the following to select a higher bitrate WMA encoder profile. You will end up with higher quality audio playback but at the cost of larger WMA files.

Step 1  Launch a web browser and sign in to Cisco Unified MeetingPlace with a system manager profile.

Step 2  Click Admin.

Step 3  Click Audio Conversion.

Step 4  Make sure that Convert to Windows Media Format is set to Yes.

Step 5  Enter a higher bitrate encoder profile for Windows Media Server Conversion Profile:
   - We recommend that you enter Windows Media Audio 8 for Dial-up Modem (CD quality, 64 Kbps).

Step 6  Click Submit.
Web Recording is Silent

**Problem** The web recording is silent or the audio and web conferencing portions of the recording are not timed properly.

**Possible Cause** You are using a remote SQL server and the time on the SQL server is not synchronized with the Cisco Unified MeetingPlace Application Server and Web Server.

**Solution** Synchronize the clock on the remote SQL server with the clocks on the Cisco Unified MeetingPlace Application Server and Web Server.

**Possible Cause** The Web Server and Application Server are not synchronized.

**Solution** Make sure that both servers are synchronized for clocking/NTP.

**Possible Cause** The audio component of the recording was not converted properly.

**Solution** To check this, do the following:

**Step 1** Check the stored converted files in C:\Program Files\Cisco Systems\MPWeb\Meetings\xx where <xx> matches the folder ID on the Application Server.

**Step 2** Locate the file with a SCO-ID in the file name, such as webRecording_20516.

**Step 3** Use the SCO-ID to locate the FLV files and associated MP3 file that plays with the web recording playback. Example, C:\Program Files\Cisco Systems\MPWeb\WebConf\content\7\20516-1\output.

**Related Topics**
- See Configuring the Web Server to Synchronize with an NTP Server in the Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing module.

Audio and Video Playback Not Synchronized

**Problem** The audio and video components of a recording playback are not timed properly.

**Possible Cause** You are not using a supported tool for playback.

**Solution** Make sure that you are using the supported tool for recording playbacks. This release of Cisco Unified MeetingPlace supports the QuickTime player.

**Possible Cause** The Web Server and Application Server are not synchronized.

**Solution** Make sure that both servers are synchronized for clocking/NTP.

**Related Topics**
- See Configuring the Web Server to Synchronize with an NTP Server in the Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing module.
Cannot Access Attachments From the External Web Server

**Problem**  You cannot access attachments from the external Web Server.

**Solution**  Make sure of the following:

- The Cisco Unified MeetingPlace Replication Service on the external Web Server is enabled and running.

Cannot Attach Files Larger than 10KB to the Web Meeting Room

**Problem**  You are in a web meeting room trying to attach a file that is larger than 10KB and you receive an error message that the upload is stuck at 0%.

**Solution**  Be sure that the hostnames for the Home Page and Web Conferencing can be resolved on the Web Server machine.

If the hostnames cannot be resolved by the DNS Server (or a DNS server is not used), these entries should be added to the local hosts file by following these steps:

1. Open the ‘hosts’ file (usually found in C:\WINNT\system32\drivers\etc) with Notepad.
2. Add the entries for ‘Hostname [Home Page]’ and ‘Hostname [Web Conferencing]’ with the corresponding IP addresses, exactly as they are displayed on the Web Server page in the Cisco Unified MeetingPlace Web Administration page.
3. Save the ‘hosts’ file.

**Note**  You do not need to restart Cisco Unified MeetingPlace web services after making this change.

**Related Topics**

- Using the Cisco Unified MeetingPlace Web Administration Page in the Quick Start Configuration: Cisco Unified MeetingPlace Basic Web Conferencing module

Error: Access is Denied

**Problem**  You click the icon to preview a recording or attachment on the Attachments/Recordings page and you get an “Access is denied” error message.

**Possible Cause**  Shared storage is configured with the improper log in credentials.

**Solution**  Check the following:

1. Make sure that the services are running in “Administrator” account (or an account with Administrator credentials that also has credentials for shared storage).
2. Verify that the shared storage has the UNC path.
3. Are you able to access the UNC path from the Web Server machine? If you have Cisco Security Agent enabled, make sure that it is not preventing the access.

Problem A meeting was recorded on an external Cisco Unified MeetingPlace Web Server. When you try to access the recording from an internal Cisco Unified MeetingPlace Web Server, you see an “Access is denied” error message.

Possible Cause There is a configuration error such that the Hostname [Home Page] and Hostname [Web Conferencing] settings for the external Web Server are different from those configured on the internal Web Server. Specifically, the hostname fields have IP addresses configured on the external/internal web pages for the external server, and Hostnames on the other. Having different hostnames in the different configuration locations, even if they resolve to the same IP address, may also cause this problem to appear.

Solution Reconfigure the internal and external Web Servers to both have either IP addresses or hostnames for the Hostname [Home Page] and Hostname [Web Conferencing] settings. As a workaround, the user can dismiss the “Access is denied” error message to access the recording.

Related Topics
- Configuring Shared Storage in the Configuring the Cisco Unified MeetingPlace Web Server for Optimal Data Storage module

Problems Accessing Meeting Recordings When Using Shared Storage

If you are using a non-default location for the meetings folder, for example, if you are using shared storage (such as in a load-balancing system), and if the audio conversion is configured to convert to Windows Media Format and Windows Media Server is used (for streaming), then users cannot access meeting recordings from the Meeting Details -> Attachments page. The system gives an error stating that a link to the audio recording does not exist.

To fix this, you must disable the Windows Media Server NTFS ACL authorization so that you can host remote content on a Windows Media Server publishing point.

You can disable ACL authorization either at the server level or at the plug-in level.

Disabling ACL Authorization at the Server Level

2. Click the local host on the left panel.
3. Choose the Properties tab on the right panel.
5. Disable the WMS NTFS ACL Authorization from Plug-In.
6. Grant read permission on the remote server. If the server and remote share folder are in the same domain, grant the read permissions for the domain user who logs on to the Windows Media Server. If they are in the same workgroup, create the same users on both hosts.

Disabling ACL Authorization at the Plug-In Level

2. Double click the host on the left panel.
3. Double click the publishing points on the left panel.
4. Click the <Default> one (on-demand).
5. Select the Properties tab.
6. Click the Authorization from category on the right panel.
7. Disable the WMS NTFS ACL Authorization from Plug-in.
8. Grant read permission on the remote server. If the server and remote share folder are in the same domain, grant the read permissions for the domain user who logs on to the Windows Media Server. If they are in the same workgroup, create the same users on both hosts.

**Cannot Play Windows Media Recordings or Attachments**

**Problem**  You cannot play Windows Media recordings or attachments.

**Possible Cause**  The Windows Media Server is not installed on the same Windows machine as Cisco Unified MeetingPlace Web Conferencing and the mount point location is incorrect. This affects how your meeting recordings stream.

**Solution**  See your Windows Help for information about correcting the mount point location.

**Possible Cause**  Secure Sockets Layer (SSL) is turned on.

**Solution**  Make sure that Windows Media file is turned on in Windows Media Player. See the “Troubleshooting Problems with Recordings in Windows Media Format” section on page 22.

**Note**  If you are in an SSL environment when trying to play the WMA recording and see a popup message stating that a security problem has occurred, check with your IT department to make sure that the proper security certificate authentication exists on your client machine.

**Troubleshooting Problems with Recordings in Windows Media Format**

**Procedure**

**Step 1**  Open Windows Media Player.

**Step 2**  Select **Tools > Options > File Types**.

**Step 3**  Click **Windows Media file (asf)** so there is a checkmark next to it.

**Step 4**  Click **OK** and try playing your recording or attachment again.

**Related Topics**

If you continue to have problems, try verifying the checks in the “How to Resolve Problems With Attachments and Recordings” section on page 15.
Recordings Stuck in “Processing Now” State

**Problem** Attachment/Recording page of past meeting is stuck in “Processing Now” state. The past meeting may still show up in today’s find meeting page.

**Possible Cause** You are completing a new installation or upgrade that requires connecting to a new AD server and synchronizing many user profiles that may delay conversions.

**Solution** None. The process of synchronizing many user profiles for the first time causes a delay in web activities.

**Possible Cause** In comparison with other Cisco Unified MeetingPlace services, the Audio Service conversion process takes a lower priority. Therefore, during the peak hours of Cisco Unified MeetingPlace usage, audio files are converted and posted at a much slower rate. On an idle system, a recording can be accessible in minutes, while during peak hour activity it can take hours.

**Solution** Give the system some time to do the conversions.

How to Resolve Problems With Secure Sockets Layer

- Security Warnings, page 23

Security Warnings

**Problem** You see the following warning: Name does not match the certificate.

**Possible Cause** It is possible that you did not define this Web Server properly.

**Solution** See Changing the Web Server Hostname From an IP Address to a Hostname in the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module.

How to Resolve Web Server Time Synchronization Problems

If the time on the Cisco Unified MeetingPlace Web Server is different than the time on the Cisco Unified MeetingPlace Application Server, many symptoms arise, such as the following:

- Scheduling and joining web meetings may not be honored
- Recording voice and web meeting files may not be synchronized properly
- Playback may not be possible
- Other time related symptoms may be seen

If the Web Server is part of a Windows domain, the web software overrides the domain NTP default settings.

In Windows, go to System > Eventlog to see W32tm information and errors. This tells you which NTP server the Web Server is syncing with. Once you find the NTP server, use the following command from a DOS prompt to check if there are any communication issues between the Web Server and the NTP server:

```
w32tm /monitor /computers:x.x.x.x
```
Note

This should be the IP address of the Application Server or the shared IP address in a dual Application Server configuration.

If the time is more than 30 seconds off, the Web Server will not synchronize with the Application Server which is synchronized with the corporate NTP server. Perform the following:

1. Stop all Cisco Unified MeetingPlace services.
2. Stop the Windows Time Service.
3. Update the time.
4. Make sure that the time difference between the Application Server and the Web Server is less than 30 seconds.
5. Start the Windows Time Service.
6. Start all Cisco Unified MeetingPlace services.
7. Check the eventlog to make sure that the servers are syncing properly.

How to Resolve Web Server Configuration Problems

- Database Command in Online Administrative Interface Does Not Work, page 24

Database Command in Online Administrative Interface Does Not Work

**Problem** The “Count all entries in tables” function on the Cisco Unified MeetingPlace Web Conferencing online Administrative interface does not work properly.

**Possible Cause** The database account does not have the db_owner role.

**Solution** Add the db_owner role for the MPWEB database user.
Troubleshooting the Cisco Unified MeetingPlace Application Server

Release 7.1
Revised: April 3, 2011 8:31 pm

- Failover Replication Fails After Adding New Node 1, page 1
- How to Solve Problems with the Application Server SSL, page 1
- Error Messages for Application Server SSL, page 4
- Additional References for Troubleshooting SSL for the Application Server, page 7
- Cisco Unified MeetingPlace Time Zone, Daylight Savings, and Clock Errors, page 7
- Performing a Login Audit on the Application Server, page 7

Failover Replication Fails After Adding New Node 1

Problem As part of the failover configuration between two Application Servers, user switched on replication with sync via mp_replication switchON command. The replication failed.

Possible Cause A table is locking due to the processes on an active server. Both servers must be in standby mode before attempting to synchronize them.

Solution Run the mp_replication switchON with sync command again.

How to Solve Problems with the Application Server SSL

- Cannot Load Certificate, page 2
- Cannot Enable SSL, page 2
- SSL Stops Working, page 3
- No SSL Connection, page 3
- Certificate or Private Key is in the Wrong Format, page 3
Troubleshooting the Cisco Unified MeetingPlace Application Server

How to Solve Problems with the Application Server SSL

Cannot Load Certificate

**Problem** After attempting to load the certificate, you see the following error message on the Display Certificate page: Unparseable certificate extensions: 2 [1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
Unparseable AuthorityInfoAccess extension due to java.io.IOException: invalid URI name:file:///SAMPLE.string.com\CertEnroll\SAMPLE.string.com

**Possible Cause** Java.net.URL does not handle UNC paths well, "file://\\" is not a valid URI due to the inclusion of \ characters as defined by RFC 2396.

**Solution** Sign the certificate without the URL that includes the UNC path.

Cannot Enable SSL

**Problem** You cannot enable SSL.

**Possible Cause** While generating CSRs, you clicked the Generate CSR more than once. This causes the system to create a second private key that does not work with the certificate for the CSR that was created and downloaded the first time you clicked Generate CSR.

**Solution** Obtain and upload a new certificate. This time, make sure that you click Generate CSR only once.

**Possible Cause** An extra line was accidentally included at the end of the certificate. To verify, use the Linux `cat` command to either view the certificate file before uploading it, or view your local copy of the certificate file. The uploaded certificate on the Application Server is stored in a binary format, which cannot be viewed via the Linux `cat` command.

In the following sample output, notice the blank line that immediately precedes the “-----END CERTIFICATE-----” line.

```
[root@meeting certs]# cat webapp.cert.pem
-----BEGIN CERTIFICATE-----
MIIDUzCCArygAwIBAgIDBXgLMA0GCSqGSIb3DQEBBAUAMFoxCzAJBgNVBAYTAlVTMRwwGgYDVQQK...
hXEgFMdnnHyFa/Y8rkJ/KWwGVEb5?n2E/AdmIVZ3PYyxjpoDhxhmQCo8I1zVhYzeJWXEdvUcnb
-----END CERTIFICATE-----
[root@meeting certs]#
```

**Solution** Use any Linux editor, such as the `vim` command, to delete the extra line. Then use the Enable SSL Page to upload the corrected certificate.

**Possible Cause** Upon inspection, the modulus and exponent fields do not match between the public certificate file and private key file. If these common portions do not match, the system cannot communicate using SSL.

**Solution** Obtain and upload a new certificate.
SSL Stops Working

**Problem** SSL stops working.

**Possible Cause** You accidentally clicked Generate CSR, which created a new private key that no longer matches the previously uploaded certificate.

**Solution** If you backed up the SSL configuration, restore it. See “Restoring the SSL Configuration” in the Configuring SSL for the Cisco Unified MeetingPlace Application Server module. If you did not back up the SSL configuration, then obtain and upload a new certificate.

**Possible Cause** You performed a fresh installation of the Cisco Unified MeetingPlace application. The installation process deletes any private key files and public certificates on the system.

**Solution** If you backed up the SSL configuration, restore it. See “Restoring the SSL Configuration” If you did not back up the SSL configuration, then obtain and upload a new certificate.

**Possible Cause** The Application Server host name was changed. The CSR and resulting certificate use the Application Server hostname that you entered for Ethernet Port 1 (device eth0) during the operating system installation.

**Solution** Obtain and upload a new certificate.

No SSL Connection

**Problem** SSL connection cannot be established between Cisco Unified MeetingPlace and Microsoft Outlook, and an exception such as the following appears in the logs:

java.lang.SecurityException: Unsupported keysize or algorithm parameters

**Possible Cause** The problem occurs when the certificate contains a key longer than 1024 bits. The cryptography strength limitations placed by the default policy files included with Java Runtime Environment (JRE) give the highest strength cryptography algorithms and key lengths which are allowed for import to all countries.

**Solution** If your country does not place restrictions on the import of cryptography, then you can download the unlimited strength policy files:

2. Download the “Java Cryptography Extension (JCE) Unlimited Strength Jurisdiction Policy Files 6.”
3. Follow the instructions in the README.txt file in the downloaded package. The JRE installation used by Cisco Unified MeetingPlace is in /opt/cisco/meetingplace/jre/.

Certificate or Private Key is in the Wrong Format

**Problem** The certificate or private key is in the wrong format.

**Note** The Application Server supports only the following formats:

- Private keys: PKCS #1, PKCS #8 (PEM or DER encoding), Java keystore
- Certificates: X.509 (PEM or DER encoding), Java keystore
Solution Use the openssl command in the Application Server CLI to convert the file to a supported format. In the following example, an unsupported PKCS12 file is converted to a supported PEM-formatted file:

```
[mpxadmin@application-server ~]$ openssl pkcs12 -in old-file.pfx -out new-file.pem -nodes
```

If the file contained both the certificate and the private key, then the converted file will contain both a PRIVATE KEY block and a CERTIFICATE block. Use a text editor to separate these into two files before uploading them to the Application Server and enabling SSL, following these requirements:

- Each file must contain only one block.
- Include the BEGIN and END lines of each block, for example:

  ```
  -----BEGIN RSA PRIVATE KEY-----
  ...
  -----END RSA PRIVATE KEY-----
  ```

- Do not include any text, including spaces or blank lines, before the BEGIN line and after the END line. A trailing line break after the END line is okay. Some files contain extraneous data before the BEGIN line and after the END line. Remove such data before uploading the file and enabling SSL on the Application Server.

### Error Messages for Application Server SSL

This topic lists error messages that may appear in the Administration Center.

**Error Message** Unparseable certificate extensions: 2 [1]: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false Unparseable AuthorityInfoAccess extension due to java.io.IOException: invalid URI name:file://\\SAMPLE.string.com\CertEnroll\SAMPLE.string.com

**Explanation** Java.net.URL does not handle UNC paths well, "file://\\" is not a valid URI due to the inclusion of ‘\’ characters as defined by RFC 2396.

**Recommended Action** Sign the certificate without the URL that includes the UNC path.

**Error Message** The uploaded certificate does not match any private key on disk. SSL cannot be enabled.

**Recommended Action** Make sure that you are uploading the correct certificate. If necessary, obtain a new certificate, private key, and password.

**Error Message** A certificate was not found in the uploaded file.

**Explanation** There was an error parsing the certificate.

**Recommended Action** Make sure that you are uploading the correct file. If necessary, obtain a new certificate.

- See Certificate or Private Key is in the Wrong Format, page 3.
- If necessary, obtain a new certificate.
**Error Message** Unable to recover the private key. Is the password correct?

**Recommended Action** Make sure that you enter the correct password. If the password is correct, then the key file may be corrupted. If necessary, obtain a new certificate, private key, and password.

- See *Certificate or Private Key is in the Wrong Format, page 3.*
- If necessary, obtain a new certificate, private key, and password.

**Error Message** Unable to locate a private key on disk. SSL cannot be enabled. You may need to generate a new CSR and obtain a new certificate.

**Recommended Action** Generate a CSR and obtain a new certificate. If you created your own certificate, private key, and password, then make sure that you enter all three items at the same time on the Enable SSL Page.

**Error Message** The certificate you are trying to upload expired on `<expiration-time>`. The system time is now `<system-time>`. Cannot enable SSL.

**Recommended Action** Check that the system time is correct. If necessary, obtain a new certificate.

**Error Message** The certificate you are trying to upload is not yet valid. It will be valid from `<valid-start-time>`. The system time is now `<system-time>`.

**Recommended Action** Check that the system time is correct, or wait until the certificate becomes valid.

**Error Message** A CSR already exists. Generating a new CSR will make any certificate you have obtained for the existing CSR unusable. Please make sure you want to do this.

**Recommended Action** You may ignore this message if you are replacing the certificate, private key, and password, or if you did not obtain a certificate for the previously generated CSR. Otherwise, click Cancel and do not generate a new CSR.

**Error Message** Failed to generate CSR. Please try again.

**Explanation** You entered invalid characters in the Generate Certificate Signing Request (CSR) Page if you see an exception in root.out with one of the following messages:

- Improperly specified input name
- Directory string too small
- Incorrect ava format

**Recommended Action** Avoid any special characters, and see the “Field Reference: Generate Certificate Signing Requests (CSRs) Page”
Error Message  Could not parse SSL certificate for Administration Center.

Explanation  The certificate file in the backup archive may be corrupt.

Recommended Action  Make sure that you specify the correct file.

Error Message  This is not a valid SSL configuration archive.

Explanation  You uploaded a backup archive, but it could not be read because it was corrupt or did not contain the expected files.

Recommended Action  Make sure that you specify the correct file.

Error Message  Unable to create backup archive.

Recommended Action  Manually back up the SSL configuration by saving the following files:

- /usr/local/enrollment/certs/keystore
  The keystore file contains the certificate and private key.
- /usr/local/enrollment/<hostname>_req.csr
  This is the certificate signing request (CSR).
- /usr/local/enrollment/webCsr.xml
  The webCsr.xml file contains the keystore password.

To restore SSL from a manual backup:

1. Manually copy the backed up files to the original directories.
2. Go to the Enable SSL Page, which should indicate that the system found a valid certificate.
3. Click OK to the prompt that asks if you want to reuse the system-found certificate to enable SSL.

If the system does not find the valid certificate, then do the following:

1. Go to the Enable SSL Page.
2. Upload the keystore file as both the Certificate file and the Private key file.
3. Enter the Password from the webCsr.xml file.

   The password is the value between the <Password></Password> tags in this element path: EnrollmentClient/Certificates/Keystore/MapStore/Password

Note  There are multiple sets of <Password></Password> tags in the XML file. Make sure you get the password from the specified element path.

Related Topics
- How to Solve Problems with the Application Server SSL, page 1
- Configuring SSL for the Cisco Unified MeetingPlace Application Server module
Additional References for Troubleshooting SSL for the Application Server

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring SSL</td>
<td>Configuring SSL for the Cisco Unified MeetingPlace Application Server module</td>
</tr>
<tr>
<td>Examining the keystore using the keytool utility</td>
<td><a href="http://java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html">http://java.sun.com/javase/6/docs/technotes/tools/windows/keytool.html</a></td>
</tr>
</tbody>
</table>

Cisco Unified MeetingPlace Time Zone, Daylight Savings, and Clock Errors

For countries where Daylight Savings Time (DST) is used, you should apply the following procedure right after the clocks are adjusted one hour forward or backward on the Cisco Unified MeetingPlace server:

**Procedure**

- **Step 1**  Sign in to the Cisco Unified Media Server Administration page.
- **Step 2**  Take each Audio Blade offline.
- **Step 3**  Put each Audio Blade online.

The process of taking the Audio Blade offline and then putting it back online automatically adjusts the Audio Blade clock to match the one hour shift. If you do not perform this procedure, the log information will be wrong.

Performing a Login Audit on the Application Server

You can use audit logs to monitor the activities and commands of users on the Application Server. The psacct utility provides audit log functions. It contains four commands: ac, lastcomm, accton, and sa.

Follow these steps to enable a login audit on the Application Server:

**Procedure**

- **Step 1**  Go to the operating system login page.
- **Step 2**  Log in as the user called root.
- **Step 3**  Enter the password associated with this username.
  The system displays the operating system desktop.
- **Step 4**  Choose Application > System Tools > Terminal.
  The system displays the command line.
**Step 5**  
Follow the instructions in the table.

<table>
<thead>
<tr>
<th>To do the following</th>
<th>Enter this</th>
</tr>
</thead>
<tbody>
<tr>
<td>To enable the <strong>psacct</strong> utility</td>
<td>chkconfig psacct on</td>
</tr>
<tr>
<td>To start the <strong>psacct</strong> utility</td>
<td><code>/etc/init.d/psacct start</code></td>
</tr>
<tr>
<td>To display statistics about the connect time for users</td>
<td><code>$ ac</code></td>
</tr>
<tr>
<td>To display previously executed user commands</td>
<td><code>$ lastcomm &lt;user_id&gt;</code></td>
</tr>
<tr>
<td>To show previous logins</td>
<td><code>last -a</code></td>
</tr>
<tr>
<td>For more information about a command</td>
<td><code>man &lt;command_name&gt;</code></td>
</tr>
</tbody>
</table>
Troubleshooting Cisco Unified MeetingPlace Integration with Cisco WebEx

Release 7.1  
Revised: April 3, 2011 8:31 pm

- Where to Find Cisco WebEx Documentation, page 1
- How to Resolve Problems with the Telephony (TSP) Connection, page 1
- How to Resolve End-User Problems, page 3
- How to Resolve System Administrator Login Problems, page 7
- How to Resolve Recording Problems for Cisco WebEx Web Meetings, page 7
- Additional References for Troubleshooting Cisco Unified MeetingPlace Integration with Cisco WebEx, page 10

Where to Find Cisco WebEx Documentation

You can find Cisco WebEx documentation for both system administrators and end-users on your WebEx site.

Before You Begin

You must have administrator privileges to access the administrator documentation.

Procedure

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Log in to your WebEx site.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Select the appropriate WebEx Center, such as Meeting Center or Sales Center, from the tabs on the top of the page.</td>
</tr>
<tr>
<td>Step 3</td>
<td>On the left navigation bar, select Support &gt; User Guides.</td>
</tr>
</tbody>
</table>

How to Resolve Problems with the Telephony (TSP) Connection

- Checking the Telephony (TSP) Connection Status, page 2
Checking the Telephony (TSP) Connection Status

Procedure

Step 1  Log in to the Administration Center.

Step 2  Check that the Cisco WebEx Adapter is running.
   a. Click Services > System Status.
   b. Click View Status.
   c. See if the following text appears in the output:
      MeetingPlace CiscoWebEx Adaptor is running...

Step 3  If the system status output does not include the previous text, then restart the Cisco WebEx Adapter.

Caution  Completing these steps will cause the system to drop all Cisco WebEx meetings that are in session.
   a. Log in to the Cisco Unified MeetingPlace Administration Center.
   b. Click System Configuration > Cisco WebEx Configuration > Cisco WebEx Site and Server.
   c. Click Restart Cisco WebEx Adapter.

Step 4  View the system log messages regarding the Cisco WebEx telephony (TSP) connection.
   a. Click Services > Logs > View System Logs.
   b. Set the fields as follows:
      – Severity level—information.
      – Start date and End date—Include the day when the issue occurred, and check the check boxes.
      – Module—0, and check the check box.
      – Unit—0, and check the check box.
   c. Click View Logs.
   d. Check the output for messages indicating that the connections to primary, secondary, or both TSP servers were established or lost.

Related Topics
   • How to Resolve Problems with the Telephony (TSP) Connection, page 1
Cisco WebEx Telephony (TSP) Connection is Down

**Problem** Cisco WebEx telephony connection is down. To verify, check the telephony status.

**Possible Cause** The telephony connection is lost because the time difference between the Cisco Unified MeetingPlace and Cisco WebEx is greater than three minutes.

**Solution** Make sure that you configure the Cisco Unified MeetingPlace Application Server to use Network Time Protocol (NTP). You typically configure NTP during the installation of Cisco Unified MeetingPlace. After installation, you can use the `net` command to configure NTP.

**Solution** As a temporary workaround, you can use the `date` command to manually set the time of the Cisco Unified MeetingPlace Application Server to match the Cisco WebEx authentication server time.

**Possible Cause** The Cisco WebEx certificate expired, or a new certificate was created but not yet uploaded.

**Solution** Create and upload a new Cisco WebEx certificate.

**Possible Cause** The Cisco WebEx TSP adapter hostname was not configured to match the Cisco Unified MeetingPlace Application Server hostname.

**Solution** Ask your WebEx Customer Success Manager to verify the Cisco WebEx TSP adapter hostname configuration.

**Related Topics**
- Checking the Telephony (TSP) Connection Status, page 2
- Creating and Uploading the Cisco WebEx Certificate in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module

---

**How to Resolve End-User Problems**

- User Not Redirected to Cisco WebEx Site After Login, page 3
- Users Receive Extra E-Mail Notifications from Cisco WebEx, page 4
- Users See “Error Scheduling Meeting” While Joining Meetings, page 4
- Users Cannot Dial Out From Cisco WebEx Web Meeting, page 5
- Cisco WebEx Web Meeting Phone Control Features Do Not Work, page 5
- Cisco WebEx Web Meeting Does Not Correctly Display Speaker or User Status, page 6
- User Cannot Log In or Join Cisco WebEx Meetings, page 6
- Reconnecting to a Cisco WebEx Meeting, page 6

**Note** Also see the “How to Resolve Recording Problems for Cisco WebEx Web Meetings” section on page 7.

---

**User Not Redirected to Cisco WebEx Site After Login**

**Note** This topic applies only to About Cisco WebEx Integration Option 2.
Problem  After the user logs in through the Cisco Unified MeetingPlace Application Server, the web browser does not automatically go to the Cisco WebEx site.

Solution  Make sure that the user profile meets the following requirements:

- The user profile must contain a First name and Last name.
- The user profile must contain an E-mail address that is:
  - 64 characters or less
  - Unique among user e-mail addresses on the Cisco WebEx site.
- The Main phone number and Alternate phone number fields must be 30 characters or less.

### Users Receive Extra E-Mail Notifications from Cisco WebEx

**Note**  This topic applies only to About Cisco WebEx Integration Option 1.

Problem  Users receive e-mail notifications from both Cisco Unified MeetingPlace and Cisco WebEx.

Solution  In the Cisco WebEx Site Administration Site Settings, make sure that you set Meeting email reminders to Off.

Related Topics

- Configuring Site Settings in the Cisco WebEx Site Administration in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module

### Users See “Error Scheduling Meeting” While Joining Meetings

Problem  Users see the following error message while trying to join a meeting: “Error scheduling meeting.”

Solution  Make sure that you uncheck the following check boxes in the Cisco WebEx Site Settings:

- All meetings must have a password
- Require strict passwords for meetings

Related Topics

- Configuring Site Settings in the Cisco WebEx Site Administration in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module
Users Cannot Dial Out From Cisco WebEx Web Meeting

**Problem** Users cannot dial out from the Cisco WebEx web meeting. When they try to do so, the following message appears: “There was an error attempting to communicate with the telephony bridge.” Instructions for dialing in to the voice meeting also appear.

**Possible Cause** The telephony connection was lost because the time difference between the Cisco Unified MeetingPlace Application Server and the Cisco WebEx authentication server was greater than three minutes; this causes authentication to fail between Cisco Unified MeetingPlace and Cisco WebEx.

**Solution** Make sure that you configure the Cisco Unified MeetingPlace Application Server to use Network Time Protocol (NTP). You typically configure NTP during the installation of Cisco Unified MeetingPlace. After installation, you can use the `net` command to configure NTP.

**Solution** As a temporary workaround, you can use the `date` command to manually set the time of the Cisco Unified MeetingPlace Application Server to match the Cisco WebEx authentication server time.

**Solution** As a temporary workaround, users can follow the displayed instructions to dial in to the meeting, but note that the web meeting room does not associate the audio events of dial-in users with the web meeting participant names.

**Possible Cause** Your Cisco WebEx account is not configured to support dial-out calls.

**Solution** Contact your WebEx Customer Success Manager to make sure that the following are checked in your Cisco WebEx account:
- Call-in teleconferencing
- Call-back teleconferencing
- Global call-back teleconferencing
- Other teleconference service

Cisco WebEx Web Meeting Phone Control Features Do Not Work

**Problem** The following options in the Cisco WebEx web meeting do not work:
- Mute and unmute
- Lock and unlock the audio conference
- Invite by phone

**Possible Cause** The telephony connection between Cisco Unified MeetingPlace and Cisco WebEx was lost. To verify, check the telephony connection status.

**Solution** Try the solutions provided for when the telephony connection is down.

**Related Topics**
- Checking the Telephony (TSP) Connection Status, page 2
- Cisco WebEx Telephony (TSP) Connection is Down, page 3
Cisco WebEx Web Meeting Does Not Correctly Display Speaker or User Status

**Problem** The Cisco WebEx web meeting does not correctly display who is speaking or when users join the audio conference.

**Possible Cause** The telephony connection between Cisco Unified MeetingPlace and Cisco WebEx was lost. To verify, check the telephony connection status.

**Solution** Try the solutions provided for when the telephony connection is down.

**Related Topics**
- Checking the Telephony (TSP) Connection Status, page 2
- Cisco WebEx Telephony (TSP) Connection is Down, page 3

User Cannot Log In or Join Cisco WebEx Meetings

**Problem** A user cannot log in to the Cisco WebEx site or join Cisco WebEx web meetings.

**Possible Cause** The user profile uses the same e-mail address as that of a deactivated Cisco WebEx user. This can occur if an employee leaves and then rejoins the organization, or if an old unused e-mail address is reused by a new employee.

E-mail addresses must be unique on the Cisco WebEx site, even among deactivated users. When the user attempts to log in or join a Cisco WebEx meeting, the e-mail address is considered to be in use.

**Solution** Manually activate and update the Cisco WebEx user profile, making sure that the username and e-mail address match the User ID and E-mail address, respectively, in the corresponding Cisco Unified MeetingPlace user profile. Then have the user schedule and join a Cisco WebEx meeting, which will cause all the other user profile settings to synchronize automatically.

**Problem** A user cannot log in to the Cisco WebEx site and sees an error that says “SSO protocol error (1)”.

**Possible Cause** The URL for the default Cisco WebEx target page is not configured properly.

**Solution** Follow these steps:
1. Log in to the Cisco WebEx site administration area.
2. Select SSO Configuration from the menu on the right.
3. Enter a value for the “Default WebEx Target page URL” such as http://<your site>.webex.com.
4. Click Update.

Reconnecting to a Cisco WebEx Meeting

**Problem** My Cisco WebEx meeting disconnected. How do I reconnect to the same meeting?

**Solution** Cisco WebEx is configured to automatically reconnect whenever you are disconnected from your meeting. If the reconnect fails, do the following:
1. Close the Cisco WebEx browser window.
2. Go to the Cisco Unified MeetingPlace Current Meeting page (which should already be open) and make sure that Join the web conference is checked.
3. Click **Connect** to rejoin the same meeting.

How to Resolve System Administrator Login Problems

- **System Administrator Cannot Log In to Cisco WebEx Site Administration, page 7**

System Administrator Cannot Log In to Cisco WebEx Site Administration

**Problem** A Cisco Unified MeetingPlace system administrator cannot log in to the Cisco WebEx Site Administration.

For example, if the system administrator logs in to the Cisco Unified MeetingPlace Administration Center and clicks one of the **Cisco WebEx Site Administration URL** links, a “user account update failed” or a “user privilege update failed” error may appear.

**Possible Cause** The **Type of user** field in the Cisco Unified MeetingPlace user profile was previously set to **End user**. After logging in to Cisco WebEx as an end user, the **Type of user** field was changed to **System administrator**.

**Solution** An existing Cisco WebEx site administrator must log in to the Cisco WebEx Site Administration and manually change the Account Type of the user to “site administrator.”

How to Resolve Recording Problems for Cisco WebEx Web Meetings

- **Recordings for External Cisco WebEx Meetings Do Not Work, page 7**
- **Cannot Record Any Cisco WebEx Meetings, page 8**
- **A User Cannot Start Recording a Cisco WebEx Meeting, page 8**
- **WebEx Meeting Manager: Options for Starting the Meeting Recording are Grayed Out, page 9**
- **WebEx Recorder Setup: Cisco WebEx User is Asked Where to Record Meeting, page 9**
- **WebEx Recorder Setup: Only the “Do Not Record a Teleconference” Option is Available, page 9**
- **Cisco WebEx Meeting Recordings Contain Music and Voice Prompts, page 9**
- **Cannot Find Cisco WebEx Meeting Recordings, page 9**

Recordings for External Cisco WebEx Meetings Do Not Work

**Possible Cause** The PIN used by Cisco WebEx to log in to Cisco Unified MeetingPlace meetings for the purpose of recording the meeting has expired. PINs for all Cisco Unified MeetingPlace user accounts expire after 6 months. There is no way to change a user account (even an automated user like “recorder”) to not have a PIN that expires.

**Solution** Reset the PIN after it expires by completing the following procedure:

1. Sign in to Cisco Unified MeetingPlace as profiled user 0002 (with user name “recorder”).
   The system prompts you to change your PIN.
2. Change your PIN to something like 87654321.
3. Use the Change Profile Settings menu to change the PIN back to 12345678.
4. Verify that you can log in to user 0002’s account by phone with PIN 12345678.

Recording for external meetings should now work.

**Cannot Record Any Cisco WebEx Meetings**

**Problem** Cannot initiate meeting recordings from any Cisco WebEx web meeting that uses Cisco Unified MeetingPlace audio conferencing.

**Solution** Reset the Profile number and Profile password of the Recorder Profile.

---

**Step 1** Schedule a test meeting, specifying Cisco WebEx as the web conference provider.

**Step 2** Join the web meeting.

**Step 3** Click the Info tab in the WebEx Meeting Manager window.

**Step 4** Write down the Cisco Unified MeetingPlace meeting ID.

**Step 5** Log in to the Cisco Unified MeetingPlace CLI.

**Step 6** Enter the following command to troubleshoot calls in real time:

```
eventlog -t
```

**Step 7** From the web meeting, start the meeting recording.

**Step 8** Look for the meeting ID in the log output to see if the following occurs:

- Cisco Unified MeetingPlace receives a call from the Cisco WebEx NBR.
- Cisco WebEx NBR joins the Cisco Unified MeetingPlace audio conference.

If these do not occur, then open a case with Cisco WebEx.

---

**Related Topics**

- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace module

**A User Cannot Start Recording a Cisco WebEx Meeting**

**Problem** Cannot start the Cisco WebEx recorder.

**Possible Cause** Insufficient storage space. Check your current storage usage at My WebEx > My Files > My Recording.

**Solution** If storage is nearing the limit, either delete unwanted recording files or request additional storage space.
**WebEx Meeting Manager: Options for Starting the Meeting Recording are Grayed Out**

**Problem**  The *Record this meeting* link and the *Meeting > Start Recording* option are grayed out in the WebEx Meeting Manager window.

**Solution**  Only the host can initiate the Cisco WebEx Network-Based Recording. The current host must initiate the meeting recording or pass the host role to the meeting participant who wants to record the meeting.

**Solution**  Contact your WebEx Customer Success Manager for further assistance. The Cisco WebEx site hosting the meeting may not be configured to enable Network-Based Recording.

**WebEx Recorder Setup: Cisco WebEx User is Asked Where to Record Meeting**

**Problem**  When a user tries to start recording a meeting, the WebEx Recorder Setup window displays “Where do you want to record this meeting?”

**Solution**  Network-Based Recording is not the default recorder. When you click Record Meeting from the Cisco WebEx meeting room, make sure that you select *Use network-based recording service* and check *Set as default setting*.

**WebEx Recorder Setup: Only the “Do Not Record a Teleconference” Option is Available**

**Problem**  When a user tries to start recording a meeting, the WebEx Recorder Setup window offers only one option: “Do not record a teleconference.” All other options are grayed out.

**Solution**  Contact your WebEx Customer Success Manager for further assistance. The Cisco WebEx site hosting the meeting may not be configured to enable Network-Based Recording.

**Cisco WebEx Meeting Recordings Contain Music and Voice Prompts**

**Problem**  Cisco WebEx meeting recordings contain waiting room music, voice prompts, and user attendance and departure announcements.

**Solution**  This is expected behavior. Cisco WebEx NBR does not discriminate what audio it records. Waiting room music will be recorded if Cisco WebEx NBR is the first to join a Cisco Unified MeetingPlace voice meeting or joins before the organizer does.

**Cannot Find Cisco WebEx Meeting Recordings**

**Problem**  Cannot find the recorded meeting files.

**Solution**  Only the meeting owner (host) can access Cisco WebEx meeting recordings, which are accessible from the Cisco WebEx site at *My WebEx > Meeting Center > Host a Meeting > My Recorded Meetings*.

If other users want to access the meeting recordings, the host must provide either a streaming playback hyperlink or the .arf file for local playback using the Cisco WebEx Network-Based Recording player.
# Additional References for Troubleshooting Cisco Unified MeetingPlace Integration with Cisco WebEx

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring Cisco WebEx integration</td>
<td>Integrating Cisco Unified MeetingPlace with Cisco WebEx module</td>
</tr>
<tr>
<td>Troubleshooting issues with Cisco Unified MeetingPlace Web Conferencing</td>
<td>Troubleshooting Cisco Unified MeetingPlace Web Conferencing module</td>
</tr>
</tbody>
</table>
Troubleshooting Cisco Unified MeetingPlace Scheduling from Microsoft Outlook

How to Resolve Problems with the MeetingPlace Tab in the Microsoft Outlook Appointment Form

- MeetingPlace Tab Does Not Appear in Microsoft Outlook Calendar Appointments, page 1
- MeetingPlace Tab is Blank or Displays an Error Page, page 2
- Login Required Each Time a User Clicks the MeetingPlace Tab, page 3

MeetingPlace Tab Does Not Appear in Microsoft Outlook Calendar Appointments

**Problem**  MeetingPlace tab does not appear in Microsoft Outlook calendar appointments

**Possible Cause**  Multiple clients are open, or Microsoft Outlook or the end-user PC was shut down improperly.

**Solution**  Complete these steps:

**Step 1**  Exit all Microsoft Outlook clients.

**Step 2**  Check the Task Manager to verify that Microsoft Outlook has shut down.

**Step 3**  Reopen Microsoft Outlook.
Step 4 In Microsoft Outlook, choose File > New > Appointment.

Step 5 Verify that the MeetingPlace tab appears.

Possible Cause Cisco Unified MeetingPlace may not be set as the default form.

Solution In the Administration Center, go to System Configuration > Outlook Plug-In Configuration. Make sure that Make Cisco Unified MeetingPlace form the default appointment form is checked.

Solution In Microsoft Outlook, choose Tools > Options, then look for the MeetingPlace tab. If the tab is available, then click the MeetingPlace tab, and check Make the MeetingPlace Meeting Schedule Form the Default Scheduling Form for All Meetings.

Possible Cause An essential component may be disabled.

Solution In Microsoft Outlook, choose Help > About Microsoft Outlook > Disabled Items. If mp4olxxx.dll is disabled (xxx represents a number), then select it and click Enable. Then restart Microsoft Outlook.

Related Topics
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module

### MeetingPlace Tab is Blank or Displays an Error Page

**Problem** The MeetingPlace tab is blank or displays an error page in Microsoft Outlook calendar appointments.

**Possible Cause** The Application Server URL is not correctly configured in the Cisco Unified MeetingPlace plug-in for Microsoft Outlook.

**Solution** Complete these steps:

Step 1 In Microsoft Outlook, choose Tools > Options.

Step 2 Click the MeetingPlace tab.

Step 3 If multiple Cisco Unified MeetingPlace servers appear, then verify that the correct server is labeled as [Default].

Step 4 Select the [Default] server.

Step 5 Click Edit.

Step 6 Verify that the Server URL is correct.

For example, if you recently enabled or disabled SSL on the Application Server, then you need to modify the Server URL accordingly to begin with either https (SSL enabled) or http (SSL disabled).

Possible Cause The Cisco Unified MeetingPlace Application Server may be down, or network issues are preventing a connection to the server.

Solution Check the system status and the network status, and troubleshoot accordingly.

Related Topics
- Using Alarms and Logs on Cisco Unified MeetingPlace module
Login Required Each Time a User Clicks the MeetingPlace Tab

**Problem** Each time a user clicks the MeetingPlace tab in Microsoft Outlook calendar appointments, the user is prompted to log in.

**Solution** Make sure that the user has the most current version of the Cisco Unified MeetingPlace plug-in for Microsoft Outlook.

**Step 1** In Microsoft Outlook, choose **File > New > Appointment**.

**Step 2** Click the **MeetingPlace** tab.

**Step 3** Check whether “Upgrade to newer version” appears in the appointment window.

- If the text does not appear, then the user already has the most current version of the plug-in.
- Otherwise, click **Upgrade to newer version** and follow the prompts.

**Solution** Make sure that cookies are enabled in the default browser of the user PC. After the initial login to Cisco Unified MeetingPlace, a cookie is saved and used for future logins.

**Solution** If your Cisco Unified MeetingPlace system is configured to authenticate users externally, for example through Integrated Windows Authentication or AXL authentication (for Directory Service users), then verify and correct that configuration.

**Related Topics**
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module
- Configuring Cisco Unified MeetingPlace Directory Service module
- Configuring User Authentication for Cisco Unified MeetingPlace Web Conferencing module

How to Resolve Problems with Scheduling Meetings from Microsoft Outlook

- Meetings Are Scheduled on the Internal Server by Default, page 4
- Missing Invitees List, page 4
- System Configured for SSO Fails to Authenticate, page 4
- Login Required Each Time a User Reschedules a Delegate-Scheduled Meeting, page 4
- Problems Accessing Cisco Unified MeetingPlace for Microsoft Outlook, page 5
- Error Messages Appear When Rescheduling or Opening the First Occurrence of a Recurring Meeting Series, page 5
- Error Message: Microsoft Outlook is Not Your Default E-Mail Client, page 5
Meetings Are Scheduled on the Internal Server by Default

**Problem** All of the meetings a user schedules are on the internal Cisco Unified MeetingPlace Web Server by default. Is it possible to configure the system to automatically schedule meetings on the external Cisco Unified MeetingPlace Web Server by default?

**Solution** Log in to the Cisco Unified MeetingPlace Administration Center and change the “Allow Internet Access” parameter to Yes.

Missing Invitees List

**Problem** User scheduled a meeting through the Cisco Unified MeetingPlace end-user interface, but does not see the list of invitees in the meeting notification.

**Solution** Log in to the Cisco Unified MeetingPlace Administration Center and change the “Include list of invitees when scheduled from Unified MP Web” parameter on the Edit User Profile page to Yes.

System Configured for SSO Fails to Authenticate


**Problem** System is configured to use SSO for authentication to Cisco Unified MeetingPlace. User’s machine recently lost network connectivity and now fails to authenticate when the user opens the MeetingPlace tab from within Microsoft Outlook. After the network connection is restored, user is still unable to access the MeetingPlace scheduling page.

**Possible Cause** The MeetingPlace tab in Microsoft Outlook is an Internet Explorer window and is therefore using the cached information from the last request for authentication. Since the user was disconnected from the Exchange server during the last request, the attempt fails.

**Solution** Close Microsoft Outlook and reopen it once a connection to the Exchange Server has been established.

Login Required Each Time a User Reschedules a Delegate-Scheduled Meeting

**Problem** When a user tries to reschedule a meeting that was previously scheduled by a Microsoft Outlook delegate, the user is prompted to log in to Cisco Unified MeetingPlace. This occurs even when the user previously logged in and checked “Remember Me.”

**Possible Cause** The user and the delegate are using different formats (hostname vs. IP address) for the Cisco Unified MeetingPlace Web Server URL.

**Solution** The user can reschedule the meeting after logging in again, but to avoid the repeated logins, complete these steps on the PCs of both the user and the delegate:
Step 1  In Microsoft Outlook, choose Tools > Options.
Step 2  Click the MeetingPlace tab.
Step 3  Select the name of the Cisco Unified MeetingPlace Web Server.
Step 4  Click Edit.
Step 5  Compare the Server URLs that are configured on the user PC and the delegate PC.
Step 6  If one Server URL uses an IP address while the other Server URL uses a hostname, then change the Server URL format of the user to match the Server URL format of the delegate.

Related Topics

- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module

Problems Accessing Cisco Unified MeetingPlace for Microsoft Outlook

Problem  Cisco Unified MeetingPlace for Microsoft Outlook is on the disabled items list.

Possible Cause  The system may move the integration to the disabled items list if Microsoft Outlook crashes or is closed incorrectly.

Solution  In Microsoft Outlook, choose Help > About Microsoft Outlook > Disabled Items. If mp4olxxx.dll is disabled (xxx represents a number), then select it and click Enable. Then restart Microsoft Outlook.

Error Messages Appear When Rescheduling or Opening the First Occurrence of a Recurring Meeting Series

Problem  The system displays the following message when a user tries to reschedule the first occurrence of a recurring meeting series that is currently in progress: “Operation is not allowed. Meeting in progress.”

The system displays the following message when the user opens this meeting occurrence: “Cannot open this item. You changed one of the recurrences of this item, and this instance no longer exists. Close any open items and try again.”

Solution  Wait a few moments and then try to open the item again.

Error Message: Microsoft Outlook is Not Your Default E-Mail Client

Error Message  Microsoft Outlook is not your default e-mail client.

Solution  Specify the default e-mail client on the user computer by following this procedure.

Step 1  Uninstall the Cisco Unified MeetingPlace plug-in for Microsoft Outlook in Add/Remove Programs.
Step 2  Open Internet Explorer.
Step 3  Choose Tools > Internet Options.
Step 4 Click the Programs tab.
Step 5 Choose Microsoft Outlook in the E-Mail field.
Step 6 Click OK.
Step 7 Reinstall the Cisco Unified MeetingPlace plug-in for Microsoft Outlook.

Related Topics
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module

Additional References for Troubleshooting Cisco Unified MeetingPlace Scheduling from Microsoft Outlook

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Troubleshooting notifications</td>
<td>Troubleshooting E-Mail Notifications for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Troubleshooting problems with joining meetings</td>
<td>User Cannot Join a Meeting</td>
</tr>
<tr>
<td>Troubleshooting end-user issues</td>
<td>“How to Resolve Meeting Notification Problems” in the User Guide for Cisco Unified MeetingPlace.</td>
</tr>
</tbody>
</table>
Troubleshooting Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface

Release 7.1
Revised: April 3, 2011 8:31 pm

- Additional References for Troubleshooting Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface, page 1

Additional References for Troubleshooting Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface

<table>
<thead>
<tr>
<th>Topic</th>
<th>Documentation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Configuring back-end</td>
<td>Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface module</td>
</tr>
<tr>
<td>Microsoft Outlook integration</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting notifications</td>
<td>Troubleshooting E-Mail Notifications for Cisco Unified MeetingPlace module</td>
</tr>
<tr>
<td>Troubleshooting problems with</td>
<td>User Cannot Join a Meeting</td>
</tr>
<tr>
<td>joining meetings</td>
<td></td>
</tr>
<tr>
<td>Troubleshooting end-user issues</td>
<td>“How to Resolve Meeting Notification Problems” section in the User Guide for Cisco Unified MeetingPlace.</td>
</tr>
</tbody>
</table>
PART

Reference Information

- Administration Center Page References for Cisco Unified MeetingPlace
- Web Administration References for Cisco Unified MeetingPlace
- MeetingPlace Conference Manager References
- Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace
- Raw Data Export and Import Specifications for Cisco Unified MeetingPlace
- Time Zone Mapping Between Cisco WebEx and Cisco Unified MeetingPlace
- Application Server File Locations for Cisco Unified MeetingPlace
In the Cisco Unified MeetingPlace Administration Center, the title of each page appears in the blue bar beneath the “Cisco Unified MeetingPlace System Administration Center” banner.

This module describe the fields and options on each page, presented in alphabetical order by page title.

**Add Meeting Categories Page**

To find this page, select **System Configuration > Meeting Categories**. Then select **Add New**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Identifies the meeting category on the scheduling page and in meeting details.</td>
</tr>
<tr>
<td>Owner</td>
<td>User ID of the meeting category owner.</td>
</tr>
<tr>
<td>Description</td>
<td>Enter a description that will help system administrators maintain the meeting categories, for example, how to distinguish one meeting category from another.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Meeting Categories in the Configuring Meetings for Cisco Unified MeetingPlace module
- Meeting Categories Page, page 58

**Add Server Configuration Page**

To find this page, select **System Configuration > Remote Server Configuration > Add New**.

**Note**

In this document, a “system” refers to a complete Cisco Unified MeetingPlace site installation, which includes one active Application Server and one active Media Server. The system may also include one or more Web Servers.
Table 2  
Field Reference: Add Server Configuration Page and Edit Server Configuration Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name of the remote system. This name will appear on the end-user web interface when scheduling meetings.</td>
</tr>
</tbody>
</table>
| Home Server number    | Enter a unique number that identifies the remote server on all RSNA systems. This same value must be used in the Schedule home server user profile field for users that are local to the server. If you check Reserved Meeting Server:  
  - The Home Server number field is cleared and cannot be modified.  
  - In the database, this remote server record is assigned the Home Server number of 777777. |
| Reserved Meeting Server| Whether the remote server is the RSNA Reserved Meeting Server. If you check this:  
  - The Home Server number field is cleared and cannot be modified.  
  - In the database, this remote server record is assigned the Home Server number of 777777. |
| SIP Agent Address 1    | IP address of the remote Application Server(s). The second remote server entry is optional. |
| SIP Agent Address 2    | Reserved for a future release.                                                |
| Routing Unit Number    | Reserved for a future release.                                                |
| Routing Codec          | Reserved for a future release.                                                |
| Web conferencing enabled| Whether Cisco Unified MeetingPlace Web Conferencing is installed and operational on the remote system. Default: No |
| Web URL                | URL of the primary Web Server for the remote system.                          |

Related Topics
- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module
- Configuring Endpoints for Cisco Unified MeetingPlace module
- Remote Server Configuration Page, page 72

Add SNMP Community String Page

To find this page, select Maintenance > SNMP > Community Strings > Add New.

Table 3  Field Reference: Add SNMP Community String Page and Edit SNMP Community String Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community string</td>
<td>Name of the SNMP community string. Restriction: No spaces allowed.</td>
</tr>
<tr>
<td>Accept SNMP packets from any host</td>
<td>Allows the SNMP community string to accept SNMP packets from any host.</td>
</tr>
</tbody>
</table>
Table 3  Field Reference: Add SNMP Community String Page and Edit SNMP Community String Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accept SNMP packets only from these hosts</td>
<td>Allows the SNMP community string to accept SNMP packets only from hosts that you specify.</td>
</tr>
<tr>
<td>Host IP address</td>
<td>If you choose the Accept SNMP packets only from these hosts radio button, enter an IP address and select Insert to allow the SNMP community string to accept SNMP packets from this host.</td>
</tr>
<tr>
<td>Host IP addresses</td>
<td>If you choose the Accept SNMP packets only from these hosts radio button, this field lists all hosts from which this SNMP community string can accept SNMP packets. To remove a host from this list, highlight the IP address and select Remove.</td>
</tr>
<tr>
<td>Access privileges</td>
<td>The access privilege given to this SNMP community string. Access privileges provide security by restricting the ability to alter the Cisco Unified MeetingPlace system.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring SNMP on Cisco Unified MeetingPlace module

Add SNMP Notification Destination Page

To find this page, select Maintenance > SNMP > Notification Destinations > Add New.

Table 4  Field Reference: Add SNMP Notification Destination Page and Edit SNMP Notification Destination Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP address</td>
<td>Restriction: Each notification destination must have a unique IP address.</td>
</tr>
<tr>
<td>Port number</td>
<td>The port number for the notification destination.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>SNMP version 1 supports only traps. SNMP version 2c supports both traps and inform notification types.</td>
</tr>
<tr>
<td>Notification type</td>
<td>Dimmed if you select SNMP version 1.</td>
</tr>
<tr>
<td>Security level</td>
<td>Display only. Value is determined by the selected Community string.</td>
</tr>
<tr>
<td>Community string</td>
<td>SNMP community string to associate with this notification destination.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring SNMP on Cisco Unified MeetingPlace module
Add Translation Rule Page

To find this page, select System Configuration > Call Configuration > Auto Attend Translation Configuration > Add New.

Table 5  Field Reference: Add Translation Rule Page and Edit Translation Rule Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>Enter information to help you and other system administrators understand the translation rule. Example: Converts a 7-digit number to a 5-digit extension.</td>
</tr>
</tbody>
</table>
| Digits to match  | Number of digits that must be in the incoming ANI in order for this rule to be applied. Example: Suppose this field is set to 5:  
- If the ANI is 50123, then the system applies this rule.  
- If the ANI is 0123 or 5550123, then the system does not apply this rule.  
Recommendation: The ANI can vary depending on whether calls are received from internal, external, long distance, or international sources. Use a large enough value to preserve uniqueness for ANI matches. We recommend a value of 4 or 5.  
Restriction: You cannot modify the preconfigured translation rule, in which this field is set to 0. The system uses the preconfigured translation rule to find a user profile phone number that matches the incoming ANI exactly without adding or deleting any digits. |
| Match string     | Apply this rule if this string matches the beginning of the ANI digits. This string is removed from the ANI.  
Example: If this field is set to 555, and the ANI is 5550123, remove the 555 to make the modified ANI equal to 0123. |
| Replace by       | Insert these digits at the beginning of the ANI.  
Example: If this field is set to 5 and the ANI is 0123, then the ANI becomes 50123. |

1. ANI = automatic number ID, or the phone number from which the user called.

Related Topics
- Configuring the Auto Attend Feature for Cisco Unified MeetingPlace module
- Auto Attend Translation Configuration Page, page 26

Add User Group Page

To find this page, select User Configuration > User Groups > Add New.

Note
Most user group fields are identical to user profile fields. Therefore, Table 6 describes only the fields that are specific to user groups. For descriptions of all other user group fields, see Table 7 on page 6, “Field Reference: Add User Profile Page and Edit User Profile Page”.

Table 6  
Field Reference: Add User Group Page and Edit User Group Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>Name by which you want to identify the user group. Recommendation: Use a name that describes the users in the group, such as “Marketing.” Restriction: Unicode is not supported.</td>
</tr>
<tr>
<td>Number</td>
<td>Number used to identify this user group.</td>
</tr>
</tbody>
</table>
| Phone number for non-direct-dial pagers | Shared phone number for a non-direct-dial pager system.¹ PIN numbers to access individual pagers are configured in the Pager number field in individual user profiles. Restrictions:  
  • This field applies only to users whose individual user profiles are configured with a non-direct-dial pager PIN number in the Pager type field.  
  • Only the following characters are used to call the pager: 0-9, #, and *. All other characters are ignored by the system but generate INFO events in the system log. |

All other user group fields are described in Table 7 on page 6, “Field Reference: Add User Profile Page and Edit User Profile Page”.

¹ The required format for phone numbers is determined by the call-control device for your IP telephony network. Therefore, enter phone numbers in the same format used to dial similar numbers from a phone on the same IP telephony network as Cisco Unified MeetingPlace. For example, if calls within your company are made by dialing the last four digits of a phone number, then enter only the last four digits in Cisco Unified MeetingPlace for internal phone numbers. If, however, you want Cisco Unified MeetingPlace to call a phone in a different area code, then you may need to include 91 and the complete telephone number including the area code.

Related Topics
  • Adding or Editing a User Group Manually in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
  • Specifying Languages for Users in the Configuring Languages for Cisco Unified MeetingPlace module
  • Configuring Reservationless Meetings in the Configuring Meetings for Cisco Unified MeetingPlace module
  • Configuring Continuous Meetings in the Configuring Meetings for Cisco Unified MeetingPlace module
  • Configuring Requirements for Meeting Passwords in the Securing the Cisco Unified MeetingPlace System module
  • Restricting Access to Scheduled Meetings in the Securing the Cisco Unified MeetingPlace System module
  • Configuring User Preferences for E-Mail Notifications in the Configuring E-Mail Notifications for Cisco Unified MeetingPlace module
Add User Profile Page

To find this page, select User Configuration > User Profiles > Add New.

Table 7 also describes fields for the following:

- Add User Group Page and Edit User Group page in the Administration Center
  For information about fields that are specific to user groups (not user profiles), see Table 6 on page 5.
- Add User Profile page and Edit User Profile page in MeetingPlace Conference Manager
  For information about finding these pages in MeetingPlace Conference Manager:
  - Adding a User Profile in the Using MeetingPlace Conference Manager module
  - Updating a User Profile in the Using MeetingPlace Conference Manager module

Table 7  Field Reference: Add User Profile Page and Edit User Profile Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identification</td>
<td>First name of the user. Used in meeting participant lists and reports.</td>
</tr>
<tr>
<td></td>
<td>The value of this field in the guest profile is applied to guest users.</td>
</tr>
<tr>
<td></td>
<td>In the guest profile, keep the default value or choose a name that clearly</td>
</tr>
<tr>
<td></td>
<td>indicates a guest meeting participant.</td>
</tr>
<tr>
<td></td>
<td>If you are creating a user profile for an auto-answer device, then enter</td>
</tr>
<tr>
<td></td>
<td>“autoanswerdevice” in this field. See “How to Configure Auto-Answer Devices”</td>
</tr>
<tr>
<td></td>
<td>in the Configuring Endpoints for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td></td>
<td>Restriction: (Cisco WebEx integration only) Do not leave this field blank.</td>
</tr>
<tr>
<td></td>
<td>Defaults for preconfigured user profiles: Guest (guest), Administrator</td>
</tr>
<tr>
<td></td>
<td>(admin), Voice Recorder (recorder).</td>
</tr>
<tr>
<td>First name</td>
<td>First name of the user. Used in meeting participant lists and reports.</td>
</tr>
<tr>
<td></td>
<td>The value of this field in the guest profile is applied to guest users.</td>
</tr>
<tr>
<td></td>
<td>In the guest profile, keep the default value or choose a name that clearly</td>
</tr>
<tr>
<td></td>
<td>indicates a guest meeting participant.</td>
</tr>
<tr>
<td></td>
<td>Defaults for preconfigured user profiles: User (guest), Cisco Unified</td>
</tr>
<tr>
<td></td>
<td>MeetingPlace (admin), Cisco WebEx (recorder).</td>
</tr>
<tr>
<td>Last name</td>
<td>Last name of the user. Used in meeting participant lists and reports.</td>
</tr>
<tr>
<td></td>
<td>The value of this field in the guest profile is applied to guest users.</td>
</tr>
<tr>
<td></td>
<td>In the guest profile, keep the default value or choose a name that clearly</td>
</tr>
<tr>
<td></td>
<td>indicates a guest meeting participant.</td>
</tr>
<tr>
<td></td>
<td>Defaults for preconfigured user profiles: User (guest), Cisco Unified</td>
</tr>
<tr>
<td></td>
<td>MeetingPlace (admin), Cisco WebEx (recorder).</td>
</tr>
</tbody>
</table>
### Table 7  Field Reference: Add User Profile Page and Edit User Profile Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **User ID**       | Unique username by which the user logs in to Cisco Unified MeetingPlace from a workstation. **Note**: Users enter the **User ID** and **User password** to log in to Cisco Unified MeetingPlace from a workstation. Users enter the **Profile number** and **Profile password** to authenticate to Cisco Unified MeetingPlace from a touch-tone phone.  
Restrictions:  
- Unicode is not supported.  
- Uppercase characters are automatically converted to lowercase characters.  
- If this field is dimmed and marked with a padlock icon, the user is authenticated by an external directory, and you cannot modify this field. See “Methods for Adding User Profiles” in the **Configuring User Profiles and User Groups for Cisco Unified MeetingPlace** module.  
- (For Cisco WebEx integration only) Do not modify this field in an existing user profile. Doing so disables future logins to Cisco WebEx by the user. This is also true for system administrator access to the Cisco WebEx Site Administration. Instead of modifying the **User ID**, create a new user profile in Cisco Unified MeetingPlace and deactivate the previous user profile through the Cisco WebEx Site Administration.  
Defaults for preconfigured user profiles: guest (cannot modify), admin, recorder. |
| **User password** | Password used to log in to Cisco Unified MeetingPlace from a workstation.  
Restrictions:  
- Unicode is not supported.  
- If this field is dimmed and marked with a padlock icon, the user is authenticated by an external directory, and you cannot modify this field. See “Methods for Adding User Profiles” in the **Configuring User Profiles and User Groups for Cisco Unified MeetingPlace** module.  
- (Guest profile only) Leave this field blank in the preconfigured guest profile, because this guest profile field is inherited in all new user profiles  
**Note**: If you are adding this information from MeetingPlace Conference Manager, the system permits you to see the password as you type it so that you can easily spell it out to users you are assisting.  
Default for the admin profile: cisco |
| **User password confirm** | Password used to confirm the **User password** entered.  
Restrictions:  
- Unicode is not supported.  
- If this field is dimmed and marked with a padlock icon, the user is authenticated by an external directory, and you cannot modify this field. See “Methods for Adding User Profiles” in the **Configuring User Profiles and User Groups for Cisco Unified MeetingPlace** module.  
- (Guest profile only) Leave this field blank in the preconfigured guest profile, because this guest profile field is inherited in all new user profiles  
**Note**: If you are adding this information from MeetingPlace Conference Manager, the system permits you to see the password as you type it so that you can easily spell it out to users you are assisting.  
Default for the admin profile: cisco |
| **Last changed**  | **Display only**. Date when the **User password** was last modified.  
Restriction: This date does not apply to Directory Service users, whose passwords are stored and controlled by an external device. See “Directory Service User Profile Configuration” in the **Configuring Cisco Unified MeetingPlace Directory Service** module. |
### Table 7  
*Field Reference: Add User Profile Page and Edit User Profile Page (continued)*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Profile number      | Unique number that identifies this user profile. Used to authenticate to Cisco Unified MeetingPlace from a touch-tone phone. Recommendation: Use the phone extension or voice-mail number of the user. Restrictions:  
  - If reservationless meetings are enabled on the system, then the following restrictions apply:  
    - You cannot configure a profile number that matches an existing meeting ID. Similarly, users will not be able to schedule a meeting whose meeting ID matches an existing profile number.  
    - If the profile number is longer than 17 digits, then the user cannot own reservationless meetings. This is because meeting IDs cannot be longer than 17 digits.  
  For more information about reservationless meetings, see “Configuring Reservationless Meetings” in the Configuring Meetings for Cisco Unified MeetingPlace module.  
  - This field is dimmed for the preconfigured recorder profile. To modify, see “Configuring the Cisco WebEx Audio Recorder” in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module.  
  Defaults for preconfigured user profiles: 0000 (guest, cannot modify), 0001 (admin), 0002 (recorder). |
| Profile password    | PIN used to authenticate to Cisco Unified MeetingPlace from a touch-tone phone. Set this as a temporary default PIN. Users must change their profile password when they first connect to Cisco Unified MeetingPlace. Restrictions:  
  - If this field is dimmed and marked with a padlock icon, the user is authenticated by an external directory, and you cannot modify this field. See “Methods for Adding User Profiles” in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module.  
  - This field is dimmed for the preconfigured guest profile.  
  - This field is dimmed for the preconfigured recorder profile. To modify, see “Configuring the Cisco WebEx Audio Recorder” in the Integrating Cisco Unified MeetingPlace with Cisco WebEx module.  
  Default for the admin profile: 24726 (CISCO) |
| Profile password confirm |                                                                                                                                                                                                         |
| Last changed        | *Display only.* Date when the Profile password was last modified. Restriction: This date does not apply to Directory Service users, whose passwords are stored and controlled by an external device. See “Directory Service User Profile Configuration” in the Configuring Cisco Unified MeetingPlace Directory Service module. |
| User status         | Whether this profile is active, inactive, or locked. A user with an inactive user profile cannot log in. The user may still attend meetings that are not restricted to profiled users. See the Changing the User Status in Cisco Unified MeetingPlace User Profiles module. Restriction: The preconfigured admin profile cannot be locked. Default: Group default (Active) |
Table 7  Field Reference: Add User Profile Page and Edit User Profile Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Type of user  | Type of user, the configuration of which restricts the privileges and access available to that user in Cisco Unified MeetingPlace. See the “About User Types” section on page 21.  
Defaults:  
  • Guest profile: **End user** (cannot modify)  
  • Admin profile: **System administrator** (cannot modify)  
  • All others: **End user**                                                                                                                                |
| Group name    | Name of user group to which this user profile belongs.  
Default: System                                                                                                                                                                                                 |
| E-mail address| E-mail address used in e-mail notifications. Must be in the following format:  
1. a-z, A-Z, 0-9  
2. Optional:  
   a. One of these characters: _,-  
   b. a-z, A-Z, 0-9  
3. @  
4. a-z, A-Z, 0-9, -  
5. .  
6. a-z, A-Z, 0-9—Only 2-4 characters are allowed at the end  
Examples:  
  • me.myself@example.com  
  • someone@example.com  
Restriction: (Cisco WebEx integration only) Cannot exceed 64 characters.  
Recommendation: (Guest profile only) Leave this field blank, because this field is inherited by all new user profiles.                                                                                             |
| E-mail type and format | Determines the following:  
  • Type of e-mail notification sent to this user for scheduled meetings.  
  • Format in which this user sends and receives e-mail notifications.  
The value of this field in the guest profile is applied to guest users, who in this case are all meeting invitees that are *not* invited by profile.  
Restriction: To enable the use of the Microsoft Exchange or IBM Lotus Notes formats, you first need to set up the integrations. See one of the following:  
  • *Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface* module  
Default: Group default (SMTP (HTML)) |
**Table 7  Field Reference: Add User Profile Page and Edit User Profile Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Main phone number</td>
<td>Phone number¹ for the system to dial out to the user.</td>
</tr>
<tr>
<td>Alternate phone number</td>
<td>Restrictions:</td>
</tr>
<tr>
<td>Alternate phone number 2</td>
<td>- Only the following characters are allowed:</td>
</tr>
<tr>
<td></td>
<td>- numeric</td>
</tr>
<tr>
<td></td>
<td>- space ( )</td>
</tr>
<tr>
<td></td>
<td>- (),.-</td>
</tr>
<tr>
<td></td>
<td>- The + character is allowed only as the first character in the field.</td>
</tr>
<tr>
<td></td>
<td>- (Cisco WebEx integration only) Cannot exceed 30 characters.</td>
</tr>
<tr>
<td></td>
<td>Recommendation: (Guest profile only) Leave this field blank, because this field is inherited by all new user profiles.</td>
</tr>
<tr>
<td>Pager number</td>
<td>Pager number¹ of user, used for dial-out features. The number you enter depends on the Pager type:</td>
</tr>
<tr>
<td></td>
<td>- For a direct-dial pager, enter the phone number that directly reaches the pager.</td>
</tr>
<tr>
<td></td>
<td>- For a non-direct-dial pager, enter the PIN used to access the specific pager.</td>
</tr>
<tr>
<td></td>
<td>- You configure the shared phone number that the system calls first to reach the pager system in the Phone number for non-direct-dial pagers field in the user group.</td>
</tr>
<tr>
<td></td>
<td>See “How the Find Me Feature Works with Pagers” in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td></td>
<td>Restrictions:</td>
</tr>
<tr>
<td></td>
<td>- The + character is allowed only as the first character in the field.</td>
</tr>
<tr>
<td></td>
<td>- Only the following characters are used to call the pager: 0-9, #, and *.</td>
</tr>
<tr>
<td></td>
<td>- All other characters are ignored by the system but generate INFO events in the system log.</td>
</tr>
<tr>
<td></td>
<td>- See the “Restrictions for Using the Find Me Feature with Pagers” in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td></td>
<td>Recommendation: (Guest profile only) Leave this field blank, because this field is inherited by all new user profiles.</td>
</tr>
<tr>
<td>Pager type</td>
<td>Type of pager:</td>
</tr>
<tr>
<td></td>
<td>- Direct-dial pager—Pager is reached directly by dialing a phone number.</td>
</tr>
<tr>
<td></td>
<td>- Non-direct-dial pager—Pager is reached by dialing a phone number and entering a PIN that specifically identifies the pager.</td>
</tr>
<tr>
<td></td>
<td>- You configure the shared phone number that the system calls first to reach the pager system in the Phone number for non-direct-dial pagers field in the user group.</td>
</tr>
<tr>
<td></td>
<td>Default: Direct-dial pager</td>
</tr>
</tbody>
</table>
**Table 7  Field Reference: Add User Profile Page and Edit User Profile Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Method of attending    | The method by which this user joins meetings that are scheduled by this user, reservationless meetings that this user starts, and meetings to which this user is invited by profile. Options:  
  • Have user call in—User either calls into meetings or uses the Call Me dial-out feature from the web.  
  • Have system find user—Enables the Find Me dial-out feature for this user. Default: Have user call in |
| Search order for find me | The order in which the system attempts to call the user for the Find Me dial-out feature. See “About the Find Me Feature” in the Configuring Dial-Out Features for Cisco Unified MeetingPlace module. Defaults:  
  • First: Main phone  
  • Second: Alternate phone  
  • Third: Pager  
  • Fourth: Alternate phone 2 |
| User ID of delegate    | User ID of the person who is allowed to view, reschedule, end, and delete meetings on behalf of this user. Only users of type Delegate may be entered in this field.  
If this field is left blank, then only users of type Attendant and System administrator can manage meetings on behalf of this user. Restrictions:  
  • When a meeting is rescheduled by a Delegate, Attendant, or System administrator on behalf of another user, the meeting attributes are not changed unless specifically modified through the More Options page.  
  • Microsoft Outlook delegates are completely separate from Cisco Unified MeetingPlace delegates. The Type of user and User ID of delegate fields in Cisco Unified MeetingPlace user profiles do not affect the privileges and capabilities of Microsoft Outlook delegates.  
  • Delegates are not supported with the Microsoft Outlook integration when you enable Single Sign-On (SSO) based on Windows Active Directory credentials. Default: Group default (None) |
| Region                 | Geographical region that determines which options become available in the Time zone field. Default: Other |


<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Time zone</td>
<td>Time zone in which the user typically conducts business. The drop-down menu options depend on which Region is selected. Recommendations:</td>
</tr>
<tr>
<td></td>
<td>• Do not use the default “Local time of Cisco Unified MeetingPlace server,” which is configured during installation and may be modified at any time through the CLI. Time discrepancies may occur between meetings that are scheduled before and after each server time change.</td>
</tr>
<tr>
<td></td>
<td>• See the “About Time Zones” section on page 22.</td>
</tr>
<tr>
<td>Default: Group default (Local time of Cisco Unified MeetingPlace server)</td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>Choose from the languages that were previously installed and activated on the system. See the Configuring Languages for Cisco Unified MeetingPlace module. The value of this field in the guest profile is applied to guest users.</td>
</tr>
<tr>
<td>Default: Group default (English (US))</td>
<td></td>
</tr>
<tr>
<td>Billing code</td>
<td>Billing code that is applied to meetings scheduled by the user. Meeting schedulers can modify the billing code for each meeting. Billing reports are sorted by billing code and then by User ID. Note: If an Attendant or System administrator schedules a meeting on behalf of another user, then the meeting uses the billing code of the meeting scheduler, but the system counts the minutes against the meeting owner (on whose behalf the meeting was scheduled). Recommendations:</td>
</tr>
<tr>
<td></td>
<td>• Follow existing conventions at your company, such as department codes.</td>
</tr>
<tr>
<td></td>
<td>• (Guest profile only) Leave this field blank, because this field is inherited by all new user profiles.</td>
</tr>
<tr>
<td>Default: Group default (None)</td>
<td></td>
</tr>
<tr>
<td>Default meeting category</td>
<td>Meeting category that appears by default on the scheduling page for this user. Unless you hide the field on the end-user web interface, meeting schedulers can specify the meeting category for each meeting. See “Configuring Meeting Categories” in the Configuring Meetings for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td>Default: Group default (Standard)</td>
<td></td>
</tr>
<tr>
<td>Schedule home server</td>
<td>Local Cisco Unified MeetingPlace Application Server assigned to this user. When the user schedules a meeting, the system attempts to schedule the meeting through this Application Server first. If the server does not have enough resources, then the system tries another Application Server, for example, a remote RSNA system. Requirement: This number must match the Home Server number that identifies this server. Note: If you want to assign an RSNA Reserved Meeting Server to this user, then make sure that the system has two remote server records for the reserved meeting server: one with a Home Server number in the range 0 to 999, and one with a checked Reserved Meeting Server check box. For details, see “RSNA Reserved Meeting Server” in the Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td>Default: Group default (0)</td>
<td></td>
</tr>
</tbody>
</table>
### Table 7  
**Field Reference: Add User Profile Page and Edit User Profile Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Permissions</strong></td>
<td></td>
</tr>
<tr>
<td>Use reservationless</td>
<td>Whether the user can own reservationless meetings.</td>
</tr>
<tr>
<td>Default: Group default (Yes)</td>
<td></td>
</tr>
<tr>
<td>Maximum meeting length</td>
<td>User cannot schedule meetings longer than this number of minutes.</td>
</tr>
<tr>
<td>(minutes)</td>
<td>Restrictions:</td>
</tr>
<tr>
<td></td>
<td>• This field does not apply to continuous meetings.</td>
</tr>
<tr>
<td></td>
<td>• If this value differs from the following, then the system uses the lowest value:</td>
</tr>
<tr>
<td></td>
<td>– Maximum meeting length (minutes) field on the Meeting Configuration Page.</td>
</tr>
<tr>
<td></td>
<td>– Maximum Call Duration Timer service parameter in Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Maximum Call Duration in Cisco Unified Communications Manager” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.</td>
</tr>
<tr>
<td>Default: Group default (240)</td>
<td></td>
</tr>
<tr>
<td>Scheduling restriction</td>
<td>Scheduling restrictions for this user:</td>
</tr>
<tr>
<td>(meetings to start within 6 hours of scheduling)</td>
<td>• Unrestricted—User may schedule an unlimited number of meetings.</td>
</tr>
<tr>
<td></td>
<td>• Cannot schedule—User cannot schedule meetings, regardless of start time.</td>
</tr>
<tr>
<td></td>
<td>• <strong>Numeric value</strong>—Maximum number of meetings that the user may schedule to begin within six hours after the time of scheduling.</td>
</tr>
<tr>
<td></td>
<td>Each time the user attempts to schedule a meeting, the system counts the number of meetings owned by the user that are scheduled to begin within the next six hours. If this number is greater than the field value, then the user cannot schedule any more meetings to begin within the next six hours. Note that the user may still schedule an unlimited number of meetings to begin more than six hours after the time of scheduling.</td>
</tr>
<tr>
<td>Default: Group default (Unrestricted)</td>
<td></td>
</tr>
<tr>
<td>Maximum number of attachments</td>
<td>Maximum number of attachments the user may upload per meeting.</td>
</tr>
<tr>
<td>Default: Group default (10)</td>
<td></td>
</tr>
<tr>
<td>Can change meeting ID via phone</td>
<td>Whether the user can change the meeting ID over the phone for meetings owned by the user.</td>
</tr>
<tr>
<td>Default: Group default (Yes)</td>
<td></td>
</tr>
</tbody>
</table>
Table 7  **Field Reference: Add User Profile Page and Edit User Profile Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Video usage | Whether the user can attend, host, or reserve video ports for video meetings.  
  - Can attend video meetings  
    - User can attend video-enabled meetings as a video participant.  
    - User *cannot* schedule meetings that allow video participants.  
  - Can attend + host video meetings  
    - User can attend video-enabled meetings as a video participant.  
    - User schedules video-enabled meetings, which means that video participants may attend.  
  - Can attend + host video meetings + reserve video ports  
    - User can attend video-enabled meetings as a video participant.  
    - User schedules video-enabled meetings, which means that video participants may attend.  
    - While scheduling meetings, the user can reserve video resources and invite video terminals.  
| Default: Group default (Can attend video meetings) |
| Can dial out (does not apply to Cisco WebEx meetings) | Whether dial-out privileges are enabled for this user.  
  The value of this field in the guest profile is applied to guest users.  
  Restriction: *Anyone* may dial out from Cisco WebEx web meetings, regardless of the user profile settings.  
| Default: Group default (Yes) |
| Maximum TUI outdial attempts per meeting | Maximum number of TUI (#31) dial-out calls that this user may attempt from within a meeting.  
  - Failed dial-out attempts from the TUI count against this number.  
  - Dial-out attempts from the web meeting room *do not* count against this number.  
  A value of 0 means that the user cannot press #3 to dial out from within a meeting.  
| Default: Group default (Unrestricted) |
| Can send notifications | Whether notifications are sent for meetings scheduled by the user.  
  Restriction: Notifications are never sent for reservationless meetings.  
  Recommendations: Use a consistent setting across your user base. Also, avoid changing this setting once Cisco Unified MeetingPlace is in use, because users might expect and rely on the current e-mail notification behavior.  
| Default: Group default (Yes) |
| Can receive notifications | Whether to send e-mail notifications to the user.  
  Recommendations: Use a consistent setting across your user base. Also, avoid changing this setting once Cisco Unified MeetingPlace is in use, because users might expect and rely on the current e-mail notification behavior.  
| Default: Group default (Yes) |
Table 7  **Field Reference: Add User Profile Page and Edit User Profile Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Auto attend mode             | Enables or disables the auto attend feature for the user. When enabled, you specify whether the caller automatically joins meetings or is only authenticated.  
For details, see the Configuring the Auto Attend Feature for Cisco Unified MeetingPlace module.  
Default: Group default (None) |
| Auto attend requires profile password | When the auto attend feature is enabled, this field specifies whether the user must enter the Profile password before being automatically authenticated or placed into meetings.  
Default: Group default (Yes) |
| Meeting password required    | Whether scheduled and reservationless meetings owned by this user require a meeting password. Restrictions:  
  - This field is ignored if the Minimum meeting password length field on the Meeting Configuration Page is set to 0.  
  - In reservationless meetings, meeting passwords are not required to join the web meeting room.  
Default: Group default (No) |
| Can record meetings          | Whether this user has recording privileges, specifically:  
  - Whether this user can start and stop the recording of any meeting from the TUI, regardless of who scheduled the meeting.  
  - For meetings owned by this user, whether moderators can start and stop recording from the web meeting room.  
  - Whether this user can configure the following options after selecting More Options from the New Meeting scheduling page:  
    - Reserve a recording resource (if any are available for the meeting time)  
    - Automatically start recording the meeting  
Restriction (guest profile only): When set to Yes, this field enables guest users to start and stop meeting recordings:  
  - From the TUI only (not from the web meeting room).  
  - Only if the Guests can lock and record meetings field on the Usage Configuration Page is also set to Yes.  
Default: Group default (No) |

**Recordings and Attachments**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Who can access | Who can access attachments and listen to recordings for scheduled meetings owned by this user.  
Restriction: This field does not apply to reservationless meetings. Anyone can access reservationless meeting recordings and attachments.  
Default: Group default (Anyone) |
Auto-start recording | When set to No, the system never automatically starts recording meetings that are owned by this user. Instead, a meeting participant (with recording privileges) must start the recording. When set to Yes, recording begins when the first user enters the audio component of a Collaborative or Presentation meeting, or when the moderator joins a Webinar meeting. For information about these meeting templates, see the User Guide for Cisco Unified MeetingPlace at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_user_guide_list.html. See “Options for Starting Meeting Recordings” in the Configuring Recordings for Cisco Unified MeetingPlace module. Restriction: This field is always set to No when the Can record meetings field is set to No. Default: Group default (No)

Outdial Meeting Defaults

Ask for profile password | Whether a dialed-out participant must provide a profile password before being admitted into the meeting. Default: Group default (Yes)

Meeting Preferences

Entry announcement | Announcement played when callers join meetings scheduled by this user. Default: Group default (Beep + name)

Departure announcement | Announcement played when callers leave meetings scheduled by this user. Default: Group default (Beep + name)

Meeting entry mode | Whether participants hear one, both, or none of the following items when they join meetings scheduled by this user:
- Meeting ID confirmation
- Name recording option
Restriction: Participants who automatically join a meeting through the Auto Attend Feature will hear the meeting ID confirmation, even if the Meeting entry mode for the meeting is configured to skip the meeting ID. Default: Group default (Skip ID repeat)

Who may skip password | Specifies who may join a meeting scheduled by this user without entering a meeting password. Default: Group default (Nobody)

Who can attend | Specifies who may attend meetings scheduled by this user.
Restrictions:
- This field is ignored for reservationless meetings, which anyone may attend.
- If meeting attendance is restricted to profiled users, then:
  - Unprofiled external users (such as your customers or business partners) and users with locked profiles cannot attend meetings, even if they are invited.
  - Only those who successfully authenticate to Cisco Unified MeetingPlace may attend these meetings.
Default: Group default (Anyone)
Table 7  Field Reference: Add User Profile Page and Edit User Profile Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show meetings in public listing</td>
<td>Whether to publicly list the meetings scheduled by this user in the end-user web interface. Unless you hide the field on the end-user web interface, meeting schedulers can override this setting. Default: Group default (No)</td>
</tr>
<tr>
<td>Show reservationless meetings in public listing</td>
<td>Whether to publicly display reservationless meetings owned by this user in the end-user web interface. Default: Group default (Yes)</td>
</tr>
</tbody>
</table>
| Host web meetings with                     | Whether web ports are reserved when users in this group set up meetings:  
  - Full meeting room—Reserves web ports, if available.  
  - Participant list only—Does not reserve web ports. Web meeting participants see the lite web meeting room.  

  Note You cannot use the Participant list only option if you are using Cisco WebEx as your web meeting provider. For information about the features available in the full web meeting room and the lite web meeting room, see the User Guide for Cisco Unified MeetingPlace at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_user_guide_list.html.  

  Note This field applies to both scheduled and reservationless meetings.  

  Restriction: If the user is logged in when this field is modified, then the previous setting applies until the user logs out and logs back in.  

  Recommendation: If your system has fewer web ports than voice ports available for scheduled and reservationless meetings, then set this field to Participant list only (no licenses required) for most users. This configuration helps to keep web ports available for the users who need the full web meeting room to share files or applications. If you want all or most users to be able to schedule full web meetings, then make sure that an equal number of web ports and voice parts are available on your system for scheduled and reservationless meetings. See the Installing and Managing Licenses for Cisco Unified MeetingPlace module. Default: Group default (Full meeting room (licenses required)) |
| End of meeting announcement                | Whether the end-of-meeting announcement is played in meetings scheduled by this user. Default: Group default (No)                                                                                                                                                                                                                                                                                                                                                      |
| Meeting extension announcement             | Whether meeting-extension announcements are played in meetings scheduled by this user. Default: Group default (No)                                                                                                                                                                                                                                                                                                                                                       |
| Screened entry                             | Whether screened entry is enabled in meetings scheduled by this user. Default: Group default (No)                                                                                                                                                                                                                                                                                                                                                                           |
| Disable roll call                          | Whether to disable roll call in meetings scheduled by this user. Default: Group default (No)                                                                                                                                                                                                                                                                                                                                                                               |
### Allow Internet access

Whether, by default, this user’s meetings will be scheduled on a Web Server in the DMZ.

- **Yes**—By default, meetings scheduled by this user are held on the Web Server in the DMZ, and are accessible by anyone on the Internet or intranet. By default, meetings scheduled by this user are held on the Web Server in the intranet, and are accessible by anyone on the intranet only.
- **No**—User can schedule web meetings for users on the intranet only.

**Note** Users can change this value at schedule time and schedule web meetings on the Internet or intranet.

Default: Group default (No)

### Reservationless allow Internet access

Whether this user can host reservationless meetings on a Web Server in the DMZ.

- **Yes**—User can host reservationless web meetings that are accessible by anyone on the Internet or intranet.
- **No**—User can host reservationless web meetings for users on the intranet only.

**Note** Users can change this value at schedule time and schedule web meetings on the Internet or intranet.

Default: Group default (Yes)

### Lecture meeting attend settings

How listen-only participants attend lecture-style meetings scheduled by this user:

- **Admit as listeners**
  
  Automatically enter the meeting through the meeting room with their speaking ability turned off. Video participants receive video even when their speaking ability is turned off. Meeting controllers can “Open the floor” at any time to allow for general discussion.

- **Start callers in waiting room**
  
  Automatically enter the meeting through the waiting room where they can listen to on-hold music plus any meeting announcements the moderator may have recorded. This option allows speakers to converse in private in the main meeting room before beginning the meeting. Video is blocked for video participants. However, the web portion of the meeting is visible to all web participants.

  When the moderators are ready to start the audio and video portion of the meeting, they can “Call the meeting to order” and bring all the waiting room participants into the meeting. Participants automatically have their speaking ability turned off until the moderator chooses to “Open the floor.” Video participants receive video.

- **Start meeting with floor open**
  
  Automatically enter the meeting through the meeting room with their speaking ability turned on. When the meeting is set to begin, the meeting controller can “Close the floor” and turn off the speaking ability of participants. Video participants receive video throughout.

Default: Group default (Admit as listeners)
### Table 7  
**Field Reference: Add User Profile Page and Edit User Profile Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hide web conference provider</td>
<td>Whether the user sees the web conferencing provider field while scheduling meetings. Restriction: This field appears only when Cisco Unified MeetingPlace is integrated with Cisco WebEx, specifically when the Web conference scheduling field on the Cisco WebEx Site and Server Page is set to Unified MP schedule, Cisco WebEx meeting. Default: Group default (Yes)</td>
</tr>
<tr>
<td>Default web conference provider</td>
<td>Choose between Cisco Unified MeetingPlace or Cisco WebEx. Restriction: This field appears only when Cisco Unified MeetingPlace is integrated with Cisco WebEx, specifically when the Web conference scheduling field on the Cisco WebEx Site and Server Page is set to Unified MP schedule, Cisco WebEx meeting. Default: Group default (Cisco Unified MeetingPlace)</td>
</tr>
</tbody>
</table>

### Notifications

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Priority</td>
<td>Priority of e-mail notifications for meetings scheduled by the user. Default: Group default (Normal)</td>
</tr>
</tbody>
</table>
| Send if meeting changes      | Whether e-mail notifications are sent when the following parameters change for meetings scheduled by the user:  
  - Date or time  
  - Password  
  - Meeting ID  
  - List of invitees  
  Recommendations: Use a consistent setting across your user base. Also, avoid changing this setting once Cisco Unified MeetingPlace is in use, because users might expect and rely on the current e-mail notification behavior. Default: Group default (Yes) |
| Include invitee list when scheduled from web | Whether to include a list of invitees in e-mail notifications for meetings that the user schedules from the Cisco Unified MeetingPlace end-user web interface. Note that a list of meeting invitees is not included in e-mail notifications for meetings that are scheduled from IBM Lotus Notes or the Microsoft Outlook calendar. Users can view the list of invitees through the Microsoft Outlook Scheduling tab. Default: Group default (Yes) |
| Include password             | Whether the meeting password (if any) is included in e-mail notifications for meetings scheduled by the user. Default: Group default (No)                                                                                                                                                                                                                       |
| Send attachments            | Whether to include attachments in e-mail notifications for meetings scheduled by the user. Default: Group default (No)                                                                                                                                                                                                                                           |
| Receive attachments         | Whether to include attachments in e-mail notifications sent to this user. Default: Group default (No)                                                                                                                                                                                                                                                            |
Table 7  Field Reference: Add User Profile Page and Edit User Profile Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Q&amp;A Meetings</td>
<td></td>
</tr>
<tr>
<td>Off at meeting startup</td>
<td>Whether Cisco Unified MeetingPlace disables the Q&amp;A feature at the start of lecture-style meetings scheduled by this user. If Q&amp;A is disabled at the start, the moderator can enable the Q&amp;A feature during the meeting by pressing #7. Default: Group default (No)</td>
</tr>
<tr>
<td>Notify attendees about Q&amp;A</td>
<td>Whether to play an instructional Q&amp;A prompt as people join lecture-style meetings scheduled by this user. Default: Group default (No)</td>
</tr>
<tr>
<td>Q&amp;A introduction</td>
<td>Whether to announce to everyone when a participant is given the floor in lecture-style meetings scheduled by this user. Default: Group default (Beep + name)</td>
</tr>
<tr>
<td>Q&amp;A departure</td>
<td>Whether to announce to everyone when a participant leaves the floor in lecture-style meetings scheduled by this user. Default: Group default (Beep + name)</td>
</tr>
<tr>
<td>Automatically ask next question</td>
<td>In lecture-style meetings scheduled by this user, whether participants in line to ask a question are automatically granted speaking ability at their turn. Default: Group default (No)</td>
</tr>
<tr>
<td>More than one question per site</td>
<td>In lecture-style meetings scheduled by this user, whether any participant may occupy multiple positions in the queue to ask a question. This field does not limit the number of questions a participant can ask, but it does limit the number of times they can be listed in the queue to ask a question. Default: Group default (Yes)</td>
</tr>
<tr>
<td>Tell my position in line</td>
<td>While attending a lecture-style meeting, whether this user is informed about the position in the queue to ask a question. Default: Group default (Yes)</td>
</tr>
<tr>
<td>Disable floor warning prompt</td>
<td>While attending a lecture-style meeting, whether this user is warned about being next in line to be given the floor. Default: Group default (Yes)</td>
</tr>
</tbody>
</table>

Flex Fields

If profile flex fields are configured, then they appear in this area.
See the Configuring Flex Fields for Cisco Unified MeetingPlace module.

1. The required format for phone numbers is determined by the call-control device for your IP telephony network. Therefore, enter phone numbers in the same format used to dial similar numbers from a phone on the same IP telephony network as Cisco Unified MeetingPlace. For example, if calls within your company are made by dialing the last four digits of a phone number, then enter only the last four digits in Cisco Unified MeetingPlace for internal phone numbers. If, however, you want Cisco Unified MeetingPlace to call a phone in a different area code, then you may need to include a 9 and the complete telephone number including the area code.

Related Topics
- Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Configuring Meetings for Cisco Unified MeetingPlace module
- Configuring Recordings for Cisco Unified MeetingPlace module
• Integrating Cisco Unified MeetingPlace with Cisco WebEx module
• Securing the Cisco Unified MeetingPlace System module
• Configuring Dial-Out Features for Cisco Unified MeetingPlace module
• Configuring Flex Fields for Cisco Unified MeetingPlace module
• Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module
• How to Moderate a Question and Answer Session in the Using MeetingPlace Conference Manager module

Reference Information about User Profile Fields

• About User Types, page 21
• About Time Zones, page 22

About User Types

The **Type of user** field in each user profile determines the user privileges and capabilities in Cisco Unified MeetingPlace. See Table 8.

<table>
<thead>
<tr>
<th>Table 8</th>
<th>Types of Users</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type of user</strong></td>
<td><strong>Description</strong></td>
</tr>
</tbody>
</table>
| End user | • Can schedule and control meetings, attend meetings to which they have been invited, attend any publicly listed meeting, and modify preferences in their own user profiles.  
• Cannot access the Administration Center or MeetingPlace Conference Manager. |
| Delegate | • Can view, reschedule, end, or delete meetings on behalf of end users whose user profiles specify that delegate in the **User ID of delegate** field.  
• Cannot schedule meetings on behalf of other users, even those whose user profiles specify that delegate in the **User ID of delegate** field.  
• Cannot access the Administration Center or MeetingPlace Conference Manager.  
• Cannot change user permissions before or during the meeting.  
Restrictions:  
• Microsoft Outlook delegates are completely separate from Cisco Unified MeetingPlace delegates. The **Type of user** and **User ID of delegate** fields in Cisco Unified MeetingPlace user profiles do not affect the privileges and capabilities of Microsoft Outlook delegates.  
• Delegates are not supported with the Microsoft Outlook integration when you enable Single Sign-On (SSO) based on Windows Active Directory credentials. |
Each user profile has a Time zone setting. Things you should know about time zones in Cisco Unified MeetingPlace:

- For each meeting, Cisco Unified MeetingPlace accepts and reports the start time in the time zone of the meeting scheduler.
- All e-mail notifications use the time zone of the meeting scheduler, even those that are sent to invitees in different time zones.
- On the Find Meeting and Meeting Details pages in the end-user web interface, the meeting times appear in the time zone of the user who is logged into the end-user web interface.
- All instances of recurring meetings take place at the same time of day in the time zone configured in the user profile of the meeting scheduler. Meeting invitees must adjust for time zone differences. Remember that some locations, such as Arizona, do not use daylight savings time.
- Cisco Unified MeetingPlace schedules meetings using Greenwich Mean Time (GMT). At the time each meeting is scheduled, the system converts the meeting time to GMT from the time zone that is defined in the user profile of the meeting scheduler. If the time zone setting is changed in the user profile after a meeting is scheduled, the scheduled time of that meeting does not change to reflect the new time zone. Meetings must be rescheduled to reflect the new time zone.
Add Video Terminal Profile Page

To find this page, select User Configuration > Video Terminal Profiles > Add New.

Note

In this table, VTP stands for video terminal profile.

Table 9  Field Reference: Add Video Terminal Profile Page and Edit Video Terminal Profile Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Identification         | Name used in meeting participant lists and reports. For example, enter the name or location of the conference room that contains the video terminal.  
Recommendation: Consider adding text that reflects the Method of attending field value, so that meeting schedulers can perform the following actions:  
- If multiple video terminals are required for a meeting, the meeting scheduler may want to invite video terminals that have the same Method of attending.  
- If the Method of attending is set to Have terminal call in, then the meeting scheduler may want to invite only video terminals and no users. Any users who are invited will also be dialed out when a meeting participant (with dial-out privileges) enters #33 in the TUI.  
Restriction: At most, only the first 60 characters of the Video terminal name will appear on the scheduling page. Depending on the specific web browser and window size, even a smaller number of characters may appear. Therefore, make sure that you use concise video terminal names. |
| Endpoint E.164 number   | Phone number for the system to dial out to the video endpoint.  
Restriction: Only the following characters are allowed: (),.- and 0-9. |
| Group name              | Name of user group to which this VTP belongs.  
Default: System |
| E-mail address          | Where to send e-mail notifications when this video terminal is invited to a meeting. Typically, you configure this field with the address of help desk staff or whoever is in charge of reserving the video terminal and conference room.  
(Microsoft Outlook integration only) See “Requirements for Inviting Video Terminal Profiles from Microsoft Outlook” in the Configuring Endpoints for Cisco Unified MeetingPlace module.  
For format requirements, see the E-mail address user profile field. |
| Region                  | See the Region user profile field.  
Default: Other |
| Time zone               | See the Time zone user profile field.  
Default: Group default (Local time of Cisco Unified MeetingPlace server) |
Table 9  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Skip meeting entry voice prompts on outdial | Whether this video terminal joins meetings directly without hearing voice prompts to record a name or enter a password.  
Restriction: This field applies only when the Method of attending field is set to Outdial to terminal.  
Recommendation: Select Yes if any of the following statements are true:  
• You want to configure the VTP for Direct-to-Meeting Mode for Invited Terminals.  
• The video terminal is incapable of using the TUI.  
• Your users are not proficient with this video terminal.  
Default: Yes |
| Method of attending | The method by which this video terminal joins meetings:  
• (Recommended) Outdial to terminal—System dials out to the video terminal at meeting start. Use this setting for Direct-to-Meeting Mode for Invited Terminals.  
• Have terminal call in—Video terminal can join meetings in any of the following ways:  
  – (Recommended) Meeting owner dials out to all missing invitees by entering #33 in the TUI. Only meeting participants with dial-out privileges may perform this task. This is the Alternative to Direct-to-Meeting Mode for Invited Terminals.  
  – User calls into the meeting from this video terminal.  
  – Meeting participant dials out to the phone number (Endpoint E.164 number) of the video terminal. This can be performed from the web meeting room or by entering #31 in the TUI. Only meeting participants with dial-out privileges may perform this task.  
Restriction: Some video terminals may not successfully negotiate video unless one of the recommended options are used.  
Default: Have user call in |
| Preferred codec | Which codec to use when the video terminal dials directly in to Cisco Unified MeetingPlace, or when the system dials directly out to the video terminal. Choose from the following options:  
• H.261  
• H.263  
• H.264  
• Use default (H.264)  
Restrictions:  
• The selected codec is not applied to calls that are transferred to Cisco Unified MeetingPlace from another phone. For transferred calls, Cisco Unified MeetingPlace uses the Preferred codec in the VTP associated with the originally connected phone or terminal, not the terminal that is transferred.  
• H.261 works only when the Global video mode field on the Meeting Configuration Page is set to High rate. If the Global video mode field is set to Standard rate, then any video terminals whose profiles are configured to use H.261 will use H.263 instead.  
Default: H.264 |
Use this page to display the Alarm Table and clear alarms. To find this page, select Services > Alarms.

Table 10  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity</td>
<td>Magnitude of the alarm. Can be major or minor.</td>
</tr>
<tr>
<td>Code</td>
<td>Exception code.</td>
</tr>
<tr>
<td>Count</td>
<td>Number of alarms that were combined into the one table entry.</td>
</tr>
<tr>
<td>First Time</td>
<td>When the alarm was first added to the Alarm Table, not including any alarms that were previously cleared.</td>
</tr>
<tr>
<td>Last Time</td>
<td>When the most recent alarm occurred for this table entry.</td>
</tr>
<tr>
<td>Unit</td>
<td>Unit number reporting the alarm.</td>
</tr>
<tr>
<td></td>
<td>• This is always 0 for alarms generated within the Application Server.</td>
</tr>
<tr>
<td></td>
<td>• For alarms that are reported through the Cisco Unified MeetingPlace Gateway System Integrity Manager (Gateway SIM), this is the unit number used by Gateway SIM to identify the device.</td>
</tr>
<tr>
<td>Software Module</td>
<td>Number that identifies a specific software module.</td>
</tr>
</tbody>
</table>

Related Topics

- Video Terminal Profiles Page, page 89
- Adding or Editing a Video Terminal Profile in the Configuring Endpoints for Cisco Unified MeetingPlace module

Alarms Page

Table 9  

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notifications</td>
<td>Whether to send e-mail notifications to the E-mail address in this VTP.</td>
</tr>
<tr>
<td></td>
<td>Recommendations: Avoid changing this setting once Cisco Unified MeetingPlace is in use, because users might expect and rely on the current e-mail notification behavior. Default: Group default (Yes)</td>
</tr>
<tr>
<td>Receive attachments</td>
<td>Whether to include attachments in e-mail notifications sent to the E-mail address in this VTP. Default: Group default (No)</td>
</tr>
</tbody>
</table>

1. The required format for phone numbers is determined by the call-control device for your IP telephony network. Therefore, enter phone numbers in the same format used to dial similar numbers from a phone on the same IP telephony network as Cisco Unified MeetingPlace. For example, if calls within your company are made by dialing the last four digits of a phone number, then enter only the last four digits in Cisco Unified MeetingPlace for internal phone numbers. If, however, you want Cisco Unified MeetingPlace to call a phone in a different area code, then you may need to include a 9 and the complete telephone number including the area code.

2. VTP = video terminal profile
The brief description for the Alarm Table entry may contain values that are specific to one alarm occurrence, such as an IP address. These values may differ in all alarms that are combined into one table entry, but only the values for the first alarm are displayed. To see the individual alarms, view the Exception Log.

Related Topics
- Using Alarms and Logs on Cisco Unified MeetingPlace module
- Module Numbers in the Using Alarms and Logs on Cisco Unified MeetingPlace module

## Auto Attend Translation Configuration Page

Use this page to define Automatic Number Identification (ANI) translation rules for the auto attend feature. These translation rules enable the system to match different ANI formats to the phone numbers in user profiles.

To find this page, select System Configuration > Call Configuration > Auto Attend Translation Configuration.

### Table 11 Navigation Reference: Auto Attend Translation Configuration Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort by number of digits to match, string to match, or string to replace with</td>
<td>Select the Digits to match, Match string, or Replace by column heading.</td>
</tr>
<tr>
<td>Change the alphanumeric sort order to ascending or descending</td>
<td>Select the column heading to change the arrow direction:</td>
</tr>
<tr>
<td></td>
<td>• Down arrow—ascending sort</td>
</tr>
<tr>
<td></td>
<td>• Up arrow—descending sort</td>
</tr>
<tr>
<td>Display a shorter or longer list of auto attend translation rules in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the number of entries to display.</td>
</tr>
<tr>
<td>Display a different page of auto attend translation rules</td>
<td>At the bottom of the page, perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• In the Go field, enter the page number to display, and select Go.</td>
</tr>
<tr>
<td></td>
<td>• Click the arrows to page through the list.</td>
</tr>
<tr>
<td>Edit an existing auto attend translation rule</td>
<td>Select edit in the same row as the auto attend translation rule.</td>
</tr>
<tr>
<td>Create a new auto attend translation rule</td>
<td>Select Add New.</td>
</tr>
<tr>
<td>Delete one or more auto attend translation rule</td>
<td>Check the appropriate check boxes in the far left column, then select Delete Selected.</td>
</tr>
</tbody>
</table>

Restriction: You cannot delete the preconfigured translation rule, in which the Digits to match field is set to 0. The check box is dimmed for the preconfigured auto attend translation rule.

Related Topics
- Configuring the Auto Attend Feature for Cisco Unified MeetingPlace module
• Add Translation Rule Page, page 4

Backup and Archive Page

Use this page to configure automatic system backups and archiving. To find this page, select Maintenance > Backup and Archive.

Table 12  Field Reference: Backup and Archive Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable automatic backup</td>
<td>Default: Yes</td>
</tr>
<tr>
<td>Enable automatic archiving</td>
<td>Whether to automatically archive the database after a backup. Default: No</td>
</tr>
<tr>
<td>Archiving method</td>
<td>Whether to enable archiving via FTP or SSH/rsync. Default: Remote (SSH/rsync)</td>
</tr>
<tr>
<td>Pathname location of archive</td>
<td>Directory in which the archived database is saved. Requirement: Include a leading slash before the directory name. Example: /folder_name</td>
</tr>
<tr>
<td>Remote archive host</td>
<td>Host name or IP address of the remote server to which the files are archived.</td>
</tr>
<tr>
<td>Remote host username</td>
<td>Username and password to authenticate to the remote server.</td>
</tr>
<tr>
<td>Remote host password</td>
<td>Requirement: Use an account that has the privileges to create, access, and write to directories.</td>
</tr>
<tr>
<td>Notification e-mail</td>
<td>E-mail address to which the system sends archive execution status.</td>
</tr>
</tbody>
</table>

Related Topics
• Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server module

Billing Report Page

The Billing Report page provides billing information for all meetings held in the specified date range. To find this page, select Reports > Billing Report.

Table 13  Field Reference and Output Field Reference: Billing Report Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report type</td>
<td>Output format, either text or HTML.</td>
</tr>
<tr>
<td>Destination</td>
<td>Output destination. For restrictions and recommendations for each option, see “Reports and Exported Data” in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td>Billing code</td>
<td>See Billing code.</td>
</tr>
<tr>
<td>Start date</td>
<td>Default: yesterday (mm/dd/yyyy)</td>
</tr>
</tbody>
</table>
Table 13   
Field Reference and Output Field Reference: Billing Report Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End date</td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
<tr>
<td>Billing rate (voice)</td>
<td>Billing rate, in cents, used to calculate the usage cost for voice meetings.</td>
</tr>
<tr>
<td></td>
<td>Default: 20</td>
</tr>
<tr>
<td>Billing rate (full web)</td>
<td>Billing rate, in cents, used to calculate the usage cost for full web meetings.</td>
</tr>
<tr>
<td></td>
<td>Default: 20</td>
</tr>
<tr>
<td>Billing rate (lite web)</td>
<td>Billing rate, in cents, used to calculate the usage cost for lite web meetings.</td>
</tr>
<tr>
<td></td>
<td>Default: 20</td>
</tr>
<tr>
<td>Billing rate (video)</td>
<td>Billing rate, in cents, used to calculate the usage cost for video meetings.</td>
</tr>
<tr>
<td></td>
<td>Default: 20</td>
</tr>
</tbody>
</table>

Check Boxes and Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Show all fields</td>
<td>Displays all fields in the report output. Unchecking this clears all check boxes, except Billing code, Owner ID, and Meeting ID.</td>
</tr>
<tr>
<td>Billing code</td>
<td>Display only. See Billing code.</td>
</tr>
<tr>
<td>Owner ID</td>
<td>Display only. User ID of the meeting owner.</td>
</tr>
<tr>
<td>Owner name</td>
<td>Last name and First name of the meeting owner.</td>
</tr>
<tr>
<td>Date/time</td>
<td>Date and time the meeting started.</td>
</tr>
<tr>
<td>Meeting ID</td>
<td>Display only. Meeting ID, which uniquely identifies the meeting.</td>
</tr>
<tr>
<td>Voice minutes</td>
<td>Number of minutes used for all voice meetings.</td>
</tr>
<tr>
<td>Voice cost</td>
<td>Cost of all voice meetings. Calculated by multiplying the Voice minutes output field by the value configured in the Billing rate (voice) field.</td>
</tr>
<tr>
<td>Full web minutes</td>
<td>Number of minutes used for all full-web meetings.</td>
</tr>
<tr>
<td>Full web cost</td>
<td>Cost of all full-web meetings. Calculated by multiplying the Full web minutes output field by the value configured in the Billing rate (full web) field.</td>
</tr>
<tr>
<td>Lite web minutes</td>
<td>Number of minutes used for all lite web meetings.</td>
</tr>
<tr>
<td>Lite web cost</td>
<td>Cost of all lite web meetings. Calculated by multiplying the Lite web minutes output field by the value configured in the Billing rate (lite web) field.</td>
</tr>
<tr>
<td>Video minutes</td>
<td>Number of minutes used for all video meetings.</td>
</tr>
<tr>
<td>Video cost</td>
<td>Cost of all video meetings. Calculated by multiplying the Video minutes output field by the value configured in the Billing rate (video) field.</td>
</tr>
<tr>
<td>Total cost</td>
<td>Sum of the Voice cost, Full web cost, Lite web cost, and Video cost.</td>
</tr>
</tbody>
</table>
Table 13  Field Reference and Output Field Reference: Billing Report Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional Output Fields</td>
<td></td>
</tr>
</tbody>
</table>
| Total Meeting Stats User <User ID> | Total sum of the following fields for the specified end user:  
  - Voice minutes  
  - Voice cost  
  - Full web minutes  
  - Full web cost  
  - Lite web minutes  
  - Lite web cost  
  - Video minutes  
  - Video cost  
  - Total cost |
| Total Meetings for User <User ID> | Total number of meetings billed to the specified end user. |
| Total Meeting Stats for Bill Code <Billing Code> | Sum of the following fields for all end users assigned to the specified billing code:  
  - Voice minutes  
  - Voice cost  
  - Full web minutes  
  - Full web cost  
  - Lite web minutes  
  - Lite web cost  
  - Video minutes  
  - Video cost  
  - Total cost |
| Total Meetings for Bill Code <Billing Code> | Total number of meetings billed to this billing code. |

Related Topics
- Running Reports and Exporting Data from Cisco Unified MeetingPlace module

Call Configuration Page

Use this page to perform the following tasks:
- Configuring Call Control for Cisco Unified MeetingPlace
- Configuring Parameters that Affect Sound and Video Quality
- Configuring the Auto Attend Feature for Cisco Unified MeetingPlace
Cisco WebEx Certificate Page

Use this page to create a certificate and upload it to the Cisco WebEx Site Administration. To find this page, select System Configuration > Cisco WebEx Configuration > Cisco WebEx Certificate.

Table 14 Field Reference: Cisco WebEx Certificate

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate location</td>
<td>Go to this directory to save a local copy of the certificate.</td>
</tr>
<tr>
<td>Cisco WebEx Site Administration URL</td>
<td>Use this URL to upload the certificate to the Cisco WebEx Site Administration.</td>
</tr>
<tr>
<td></td>
<td>If no link appears, then you first need to configure the fields on the Cisco WebEx Site and Server Page.</td>
</tr>
<tr>
<td>Create Certificate</td>
<td>Creates a new certificate and saves it to the stated Certificate location.</td>
</tr>
<tr>
<td></td>
<td>Restriction: If you create a certificate when one is already in place, then you will block further user access to Cisco WebEx through Cisco Unified MeetingPlace. You must upload the new certificate to the Cisco WebEx Site Administration to re-enable user access.</td>
</tr>
</tbody>
</table>

Related Topics

- Creating and Uploading the Cisco WebEx Certificate in the Administration Center Page References for Cisco Unified MeetingPlace module
## Cisco WebEx Site and Server Page

To find this page, select **System Configuration > Cisco WebEx Configuration > Cisco WebEx Site and Server**.

### Table 15  
**Field Reference: Cisco WebEx Site and Server Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Web conference scheduling</strong></td>
<td>Configures Cisco WebEx integration:</td>
</tr>
<tr>
<td></td>
<td>• Unified MP schedule, Unified MP meeting—Cisco WebEx integration is disabled.</td>
</tr>
<tr>
<td></td>
<td>• Unified MP schedule, Cisco WebEx meeting—Specifies About Cisco WebEx Integration Option 1.</td>
</tr>
<tr>
<td></td>
<td>• Cisco WebEx schedule, Cisco WebEx meeting—Specifies About Cisco WebEx Integration Option 2.</td>
</tr>
<tr>
<td></td>
<td>The value of this field also determines which other fields appear on this page. Restriction: Changes to this field take effect only after you do the following:</td>
</tr>
<tr>
<td></td>
<td>1. Select <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>2. Select the <strong>Restart Cisco WebEx Adapter</strong> or <strong>Reset TSP Connection</strong> button.</td>
</tr>
<tr>
<td></td>
<td>3. Wait 10 minutes for the system to transfer the configuration to the Web Server.</td>
</tr>
<tr>
<td></td>
<td>4. Restart the Cisco Unified MeetingPlace Web Conferencing service on the Web Server. See “Restarting All Web Conferencing Services” in the <strong>Managing Cisco Unified MeetingPlace Web Conferencing Services</strong> module.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>When you restart the Web Server, all manual changes made to the registry are lost.</td>
</tr>
<tr>
<td></td>
<td>Default: Unified MP schedule, Unified MP meeting (which hides all other fields on the page)</td>
</tr>
<tr>
<td><strong>Web conference meeting template</strong></td>
<td>Which Cisco WebEx meeting template options to offer meeting schedulers. Restriction: This field appears only when you have configured the <strong>Web conference scheduling</strong> field to schedule Cisco WebEx meetings from Cisco Unified MeetingPlace user interfaces.</td>
</tr>
<tr>
<td><strong>Cisco WebEx site ID</strong></td>
<td>Cisco WebEx site parameters provided by your Cisco WebEx administrator.</td>
</tr>
<tr>
<td><strong>Cisco WebEx site name</strong></td>
<td>The <strong>Cisco WebEx site name</strong> identifies your organization and becomes part of the URL for your Cisco WebEx site.</td>
</tr>
<tr>
<td><strong>Cisco WebEx partner ID</strong></td>
<td></td>
</tr>
</tbody>
</table>
Table 15  Field Reference: Cisco WebEx Site and Server Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco WebEx site administration password</td>
<td>Password provided by your Cisco WebEx administrator for accessing the Cisco WebEx Site Administration. Cisco Unified MeetingPlace always uses the user ID of &quot;admin&quot; profile for Cisco WebEx integrations and this cannot be changed. Only the password can be modified and must be modified in both the Cisco Unified MeetingPlace &quot;admin&quot; profile and in the Cisco WebEx Site Administration &quot;admin&quot; host ID. Combined with your system administrator User ID, the system uses this password to automatically log you in to the Cisco WebEx Site Administration when you select the Cisco WebEx Site Administration URL in the Administration Center. If this password is not configured correctly, or if your User ID was modified after logging in to the Cisco WebEx Site Administration even once, then you will be prompted to enter a username and password when you select one of the Administration Center links for the Cisco WebEx Site Administration URL.</td>
</tr>
<tr>
<td>Cisco WebEx site version</td>
<td>Display only. Cisco WebEx release number.</td>
</tr>
<tr>
<td>Proxy configuration required</td>
<td>Provided by your network administrator.</td>
</tr>
<tr>
<td>Proxy server hostname</td>
<td>Proxy servers are often used with firewalls.</td>
</tr>
<tr>
<td>Proxy server port</td>
<td>Requirement: If you modify these fields after the connection with Cisco WebEx is already established, then you must select the Restart Cisco WebEx Adapter button.</td>
</tr>
<tr>
<td>Caution</td>
<td>This button causes the system to drop all Cisco WebEx meetings that are in session.</td>
</tr>
<tr>
<td>Cisco WebEx adapter status</td>
<td>Display only. Whether or not the adapter process is running.</td>
</tr>
<tr>
<td>Reset TSP Connection</td>
<td>Establishes or resets the telephony connection between Cisco Unified MeetingPlace and Cisco WebEx.</td>
</tr>
<tr>
<td></td>
<td>Updates the TSP primary host and TSP secondary host configuration from the Cisco WebEx site and then restarts the adapter.</td>
</tr>
<tr>
<td>Caution</td>
<td>This button causes the system to drop all Cisco WebEx meetings that are in session.</td>
</tr>
</tbody>
</table>
**Community Strings Page**

To find this page, select Maintenance > SNMP > Community Strings.

### Table 16  Fields Reference: Community Strings Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Community string name</td>
<td>The name of the SNMP community string. Select the underlined name of the SNMP community string to edit it.</td>
</tr>
<tr>
<td>Access privileges</td>
<td>The level of access for this SNMP community string. Access privileges provide security by restricting the ability to alter the Cisco Unified MeetingPlace system. Allowable access privileges for the community strings are:</td>
</tr>
<tr>
<td></td>
<td>- Read only</td>
</tr>
<tr>
<td></td>
<td>- Read write</td>
</tr>
<tr>
<td></td>
<td>- Read write notify</td>
</tr>
<tr>
<td></td>
<td>- Notify only</td>
</tr>
<tr>
<td></td>
<td>- None</td>
</tr>
</tbody>
</table>

**Related Topics**
- Adding or Editing SNMP Community Strings in the Configuring SNMP on Cisco Unified MeetingPlace module
- Displaying or Deleting SNMP Community Strings in the Configuring SNMP on Cisco Unified MeetingPlace module
Custom Prompts Page

Use this page to add custom voice prompts to the Cisco Unified MeetingPlace database. To find this page, select Maintenance > Custom Prompts.

- Field Reference: Custom Prompts Page
- Navigation Reference: Custom Prompts Page

**Table 17  Field Reference: Custom Prompts Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disable music</td>
<td>Select Yes to disable (or No to enable) music, and then select Save. Default: No</td>
</tr>
<tr>
<td>Language</td>
<td>Select the language of the custom prompt that you will upload. Default: English (US)</td>
</tr>
<tr>
<td>File to upload</td>
<td>Browse to the custom voice prompt file that you want to add.</td>
</tr>
<tr>
<td>Upload File</td>
<td>Select this button after you specify the language and voice prompt file.</td>
</tr>
</tbody>
</table>

**Table 18  Navigation Reference: Custom Prompts Page**

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display a shorter or longer list of entries in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the number of entries to display.</td>
</tr>
</tbody>
</table>
| Change the alphanumeric sort order to ascending or descending | Select the column heading to change the arrow direction:  
  - Down arrow—ascending sort  
  - Up arrow—descending sort |
| Display a different page of entries     | At the bottom of the page, perform one of the following actions:  
  - In the Go field, enter the page number to display, and select Go.  
  - Click the arrows to page through the list. |
| Delete entries                          | Check the appropriate check boxes in the far left column, then select Delete Selected. |

**Related Topics**
- Customizing Music and Voice Prompts for Cisco Unified MeetingPlace module

Customize Outlook Interface

To find this Administration Center page, select System Configuration > Customize Outlook Interface.

**Note**
This page appears only when the msft_int license is installed.
**Table 19**  
*Field Reference: Customize Outlook Interface*

<table>
<thead>
<tr>
<th>Field</th>
<th>Definition</th>
</tr>
</thead>
</table>
| Language       | Specifies which scheduling form to modify. The system has a separate scheduling form for each language.  
|                | Recommendation: Use consistent customizations for all languages on your system.  
|                | Default: Value of the Language 1 field on the Usage Configuration Page.     |
| Field Name     | Default field label for scheduling form.                                    |
| Custom Label   | Customized field label for scheduling form.                                 |
| Enabled        | Whether to show (Yes) or hide (No) the field on the scheduling form.        |
| Default Enabled| Default value of the Enabled field.                                         |
| Save           | Saves the settings for the scheduling form specific to the selected Language.  
|                | Recommendation: Use consistent customizations for all languages on your system by making similar changes for each Language option. |

**Related Topics**
- Customizing the Cisco Unified MeetingPlace Scheduling Form for Microsoft Outlook in the Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module

---

**Directory Service Configuration Page**

To find this page, select User Configuration > Directory Service > Directory Service Configuration.

**Table 20**  
*Field Reference: Directory Service Configuration Page*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| AXL username           | Username and password for Cisco Unified MeetingPlace to access the Cisco Unified Communications Manager AXL database for user authentication.  
| AXL password           | If you created an application user in Cisco Unified Communications Manager, then enter the user ID and password for that application user.  
| AXL confirm password   | For information about creating an application user, see “Creating an Application User in Cisco Unified Communications Manager” in the Configuring Cisco Unified MeetingPlace Directory Service module.  
|                        | If you did not create an application user, then enter the username and password for the default administrator user that was configured during the installation of Cisco Unified Communications Manager.  
|                        | If you choose to use the default administrator user, then you will need to update the AXL username or AXL password in Cisco Unified MeetingPlace whenever the Cisco Unified Communications Manager administrator username or password gets modified. |
**Table 20  Field Reference: Directory Service Configuration Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>AXL URL</td>
<td>Enter <code>https://ip-address:8443/axl/</code>, using the Cisco Unified Communications Manager IP address.</td>
</tr>
<tr>
<td></td>
<td>When you configure this field for the initial Directory Service configuration, make sure that you also check the <strong>Update Now</strong> and <strong>Perform full sync with Cisco Unified Communications Manager</strong> check boxes.</td>
</tr>
<tr>
<td></td>
<td>If Cisco Unified Communications Manager fails, then you can modify this field to use a redundant Cisco Unified Communications Manager for authentication only. You must avoid updating or importing user profiles from the redundant Cisco Unified Communications Manager by setting the <strong>Update users interval</strong> field to the largest available value. When you switch the AXL URL field back to the primary Cisco Unified Communications Manager, you need to set the <strong>Update users interval</strong> field to the previous value to re-enable user profile synchronization between Cisco Unified MeetingPlace and the primary Cisco Unified Communications Manager.</td>
</tr>
</tbody>
</table>
| Update users interval | How frequently to update the **Directory Service** user profiles.  
Default: 6 hours                                                                                   |
| Update Now     | If this is checked when you select **Save**, then an immediate Directory Service user profile update occurs. Specifically:  
• New users are imported from Cisco Unified Communications Manager.  
• Existing user profiles in Cisco Unified MeetingPlace are updated.  
Check this whenever you change the **AXL URL**, unless you are configuring RSNA without Directory Service.  
For details about how the user profiles are configured, see **Directory Service User Profile Configuration** in the **Configuring Cisco Unified MeetingPlace Directory Service** module. |
Table 20  Field Reference: Directory Service Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Perform full sync with Cisco Unified Communications Manager | Determines how the system performs Directory Service user profile updates, both at scheduled intervals and when triggered by checking Update Now and selecting Save:  
- When this is unchecked, Cisco Unified MeetingPlace updates only the user profiles that were updated in Cisco Unified Communications Manager after the most recent Directory Service user profile update.  
- When this is checked, Cisco Unified MeetingPlace updates all Directory Service user profiles, whether or not they were recently updated in Cisco Unified Communications Manager.  
- Whether or not this is checked, new users in Cisco Unified Communications Manager are always imported to Cisco Unified MeetingPlace as part of the Directory Service user profile update.  
Restriction: Because of the large amount of user data being transferred, full synchronizations may impact system performance. Therefore, use this check box only in the following situations:  
- You are performing the first Directory Service import of user profiles.  
- You migrated non-local users from a Cisco Unified MeetingPlace Release 6.0 system to a Release 7.1 system.  
- You modify the AXL URL.  
- You accidentally delete Directory Service user profiles through the User Profiles Page or Import User Profiles Page of the Administration Center.  
For details about how the user profiles are configured, see Directory Service User Profile Configuration in the Configuring Cisco Unified MeetingPlace Directory Service module. |
| Set Unified CM sync schedule to match update users interval | Configures the Cisco Unified Communications Manager LDAP directory synchronization schedule to match the value configured in the Update users interval field. |
| User groups for imported users | Determines how the Group name user profile field is configured for each Directory Service user.  
| Time zones for imported users | Determines how the Time zone user profile field is configured for each Directory Service user.  
| Custom TZ pattern length | Number of digits to match between the telephone number of the user and a time zone filter.  
You do not need to modify this field if the Telephone Number field in Cisco Unified Communications Manager contains the punctuation or spacing required for the system to match the phone number to a time zone field. For details, see “Configuring Directory Service Filters for Time Zones” in the Configuring Cisco Unified MeetingPlace Directory Service module.  
Default: 3 |
### Hostname for Active Directory Service

Enter the hostname of the Application Server.

In an Application Server Failover deployment, enter the shared hostname that you configured on the eth0 interface of both Application Servers.

In an RSNA deployment:
- On the RSNA system that is configured for Directory Service, enter the hostname of the Application Server.
- On the RSNA system that is not configured for Directory Service, if this field is blank, then leave it blank. The field will automatically be populated with the value from the Directory Service–configured system.

### Profile Number Configuration

- **Generate profile number using**
  
  Determines how the Profile number field is configured for each Directory Service user.
  
  For details, see “Assigning Profile Numbers to Directory Service Users” in the Configuring Cisco Unified MeetingPlace Directory Service module.
  
  Default: Use phone number as profile number

- **Number of digits**
  
  Determines how many digits of the phone number are used to create the Profile number.
  
  This field is applicable only when the Generate profile number using field is set to Use last ‘n’ digits of phone number as profile number.
  
  Default: 6

- **Apply to**
  
  Determines whether to apply the Profile Number Configuration settings:
  
  - To new users only.
  - To each user whose profile gets imported or updated during Directory Service user profile updates or full synchronizations.
  
  Default: New users only

- **Save**
  
  Recommendation: After you select Save, make sure that Perform full sync with Cisco Unified Communications Manager is unchecked.

---

### Table 20  Field Reference: Directory Service Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname for Active Directory Service</td>
<td>Enter the hostname of the Application Server.</td>
</tr>
<tr>
<td></td>
<td>In an Application Server Failover deployment, enter the shared hostname that you configured on the eth0 interface of both Application Servers.</td>
</tr>
<tr>
<td></td>
<td>In an RSNA deployment:</td>
</tr>
<tr>
<td></td>
<td>- On the RSNA system that is configured for Directory Service, enter the hostname of the Application Server.</td>
</tr>
<tr>
<td></td>
<td>- On the RSNA system that is not configured for Directory Service, if this field is blank, then leave it blank. The field will automatically be populated with the value from the Directory Service–configured system.</td>
</tr>
<tr>
<td>Generate profile number using</td>
<td>Determines how the Profile number field is configured for each Directory Service user.</td>
</tr>
<tr>
<td></td>
<td>For details, see “Assigning Profile Numbers to Directory Service Users” in the Configuring Cisco Unified MeetingPlace Directory Service module.</td>
</tr>
<tr>
<td></td>
<td>Default: Use phone number as profile number.</td>
</tr>
<tr>
<td>Number of digits</td>
<td>Determines how many digits of the phone number are used to create the Profile number.</td>
</tr>
<tr>
<td></td>
<td>This field is applicable only when the Generate profile number using field is set to Use last ‘n’ digits of phone number as profile number.</td>
</tr>
<tr>
<td></td>
<td>Default: 6</td>
</tr>
<tr>
<td>Apply to</td>
<td>Determines whether to apply the Profile Number Configuration settings:</td>
</tr>
<tr>
<td></td>
<td>- To new users only.</td>
</tr>
<tr>
<td></td>
<td>- To each user whose profile gets imported or updated during Directory Service user profile updates or full synchronizations.</td>
</tr>
<tr>
<td></td>
<td>Default: New users only</td>
</tr>
<tr>
<td>Save</td>
<td>Recommendation: After you select Save, make sure that Perform full sync with Cisco Unified Communications Manager is unchecked.</td>
</tr>
</tbody>
</table>

---

1. RSNA = Reservationless Single Number Access

**Related Topics**

- Configuring Cisco Unified MeetingPlace Directory Service module
- Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module
Directory Service Filters for User Groups Page

To find this page, select User Configuration > Directory Service > Directory Service Filters for Groups. By default, this page displays user group filters sorted by department number in ascending order.

Table 21 Navigation Reference: Directory Service Filters for User Groups Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort by department number or user group</td>
<td>Select the relevant column heading.</td>
</tr>
<tr>
<td>Change the sort order to ascending or descending</td>
<td>Select the column heading to display an arrow. Select the arrow to toggle between a down arrow (ascending sort) and an up arrow (descending sort).</td>
</tr>
<tr>
<td>Display a shorter or longer list of entries in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the number of entries to display.</td>
</tr>
<tr>
<td>Display a different page of entries</td>
<td>At the bottom of the page, perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• In the Go field, enter the page number to display, and select Go.</td>
</tr>
<tr>
<td></td>
<td>• Click the arrows to page through the list.</td>
</tr>
<tr>
<td>Create a user group filter</td>
<td>Select Add New.</td>
</tr>
<tr>
<td>Edit a user group filter</td>
<td>Select Edit.</td>
</tr>
<tr>
<td>Delete entries</td>
<td>Check the appropriate check boxes in the far left column, then select Delete Selected.</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring Cisco Unified MeetingPlace Directory Service module

Directory Service Filters for Time Zones Page

To find this page, select User Configuration > Directory Service > Directory Service Filters for Time Zones. By default, this page displays time zone filters sorted by phone prefix in ascending order.

Table 22 Navigation Reference: Directory Service Filters for Time Zones Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort by region and time zone or by phone prefix</td>
<td>Select the relevant column heading.</td>
</tr>
<tr>
<td>Change the sort order to ascending or descending</td>
<td>Select the column heading to display an arrow. Select the arrow to toggle between a down arrow (ascending sort) and an up arrow (descending sort).</td>
</tr>
<tr>
<td>Display a shorter or longer list of entries in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the number of entries to display.</td>
</tr>
<tr>
<td>Display a different page of entries</td>
<td>At the bottom of the page, perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• In the Go field, enter the page number to display, and select Go.</td>
</tr>
<tr>
<td></td>
<td>• Click the arrows to page through the list.</td>
</tr>
<tr>
<td>Create a custom time zone filter</td>
<td>Select Add New.</td>
</tr>
</tbody>
</table>
To find this page, select System Configuration > Flex Fields Configuration, and then select one of the flex field entries.

### Edit Flex Fields Page

To activate this field, set the Type field to Text.

### Table 22 Navigation Reference: Directory Service Filters for Time Zones Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit a custom time zone filter</td>
<td>Select Edit.</td>
</tr>
<tr>
<td>View detailed time zone information for a preconfigured entry</td>
<td>Select View.</td>
</tr>
<tr>
<td>Delete entries</td>
<td>Check the appropriate check boxes in the far left column, then select Delete Selected.</td>
</tr>
</tbody>
</table>

### Related Topics
- Configuring Cisco Unified MeetingPlace Directory Service module

### Table 23 Field Reference: Edit Flex Fields Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Active</td>
<td>Whether the flex field appears in the end-user web interface and in reports and exported data.</td>
</tr>
<tr>
<td>Title</td>
<td>Field title that appears in user profiles, user groups, or meetings.</td>
</tr>
<tr>
<td>Type</td>
<td>Information type that determines the format in which the flex field value is stored and interpreted. Restriction: If you modify the Type of an existing flex field, then the corresponding flex field value in existing user groups, user profiles, and meeting records will be replaced by the default value applicable to the newly specified Type. See “Default Flex Field Values” in the Configuring Flex Fields for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td>Import title</td>
<td>Header field to use in import and export files.</td>
</tr>
<tr>
<td>Protection level</td>
<td>Controls user access to this flex field from the end-user web interface:</td>
</tr>
<tr>
<td>Use custom drop-down list</td>
<td>Whether users enter text or choose from a drop-down list that you create. To activate this field, set the Type field to Text.</td>
</tr>
</tbody>
</table>
Use this page to modify the content and appearance of e-mail notifications. To find this page, select System Configuration > E-Mail Notifications > E-Mail Notification Templates > Edit Templates (Advanced).

**Note**

Make sure you read the Restrictions for Editing Templates for E-Mail Notifications in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module.

- Field Reference: Edit Templates (Advanced) Page
- Editing Areas of the Edit Templates (Advanced) Page

### Table 23  
Field Reference: Edit Flex Fields Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>New drop-down list item</td>
<td>Use these fields to view and define a drop-down list of options for the flex field.</td>
</tr>
<tr>
<td>Drop-down list</td>
<td>To activate this field, set the Use custom drop-down list field to Yes.</td>
</tr>
<tr>
<td></td>
<td>Restrictions:</td>
</tr>
<tr>
<td></td>
<td>- Do not include any commas (,) when you add a drop-down list item.</td>
</tr>
<tr>
<td></td>
<td>- The combined length of all drop-down list items cannot exceed 300 – n characters, where n is the number of drop-down list items you defined.</td>
</tr>
<tr>
<td>Required field</td>
<td>Whether the flex field is a required field:</td>
</tr>
<tr>
<td></td>
<td>- Yes—If a user tries to schedule a meeting or save a user profile that includes an empty required field, then an error message appears.</td>
</tr>
<tr>
<td></td>
<td>- No—Default value.</td>
</tr>
</tbody>
</table>

**Related Topics**

- Configuring Flex Fields for Cisco Unified MeetingPlace module

### Edit Templates (Advanced) Page

Use this page to modify the content and appearance of e-mail notifications. To find this page, select System Configuration > E-Mail Notifications > E-Mail Notification Templates > Edit Templates (Advanced).

**Note**

Make sure you read the Restrictions for Editing Templates for E-Mail Notifications in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module.

- Field Reference: Edit Templates (Advanced) Page
- Editing Areas of the Edit Templates (Advanced) Page

### Table 24  
Field Reference: Edit Templates (Advanced) Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Which template to view or edit.</td>
</tr>
<tr>
<td></td>
<td>For template descriptions, see “E-Mail Notification Templates” in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>For templates that have both SMTP and non-SMTP versions, you must modify both versions to keep them consistent with each other. Otherwise, users may receive different information about the same meeting, depending on the E-mail type and format setting in each user profile.</td>
</tr>
</tbody>
</table>
Editing Areas of the Edit Templates (Advanced) Page

- **Left**—Use the editing area on the left side of the page to modify the appearance of e-mail notifications.
  - For the HTML format, you can modify the font, size, color, and alignment of the text. You can also insert horizontal lines and hypertext links and modify the location of the graphics.
  - The tags ($notify_xxxx) are defined in language property files, one of which appears on the right side of the page.
- **Right**—Use the editing area on the right side of the page to modify language property files, which define the language translations of the tags used in the templates.
  - Because the same tags are used in multiple templates, you should preview all templates after editing a language property file.
  - To view or edit a different language property file, modify the Language field at the top of the page.

**Note**

The following notes apply to the graphics in e-mail notifications:

- The HTML templates display only the size and location of each graphic.
- Graphics cannot be previewed through the Administration Center and are displayed only in actual e-mail notifications.
- E-mail notification graphics cannot be modified or replaced.
- New graphics cannot be added to e-mail notifications.

**Related Topics**

- Editing Templates for E-Mail Notifications in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module
- About E-Mail Notification Templates and Language Property Files in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module
Edit Templates (Basic) Page

Use this page to modify the content and appearance of e-mail notifications. To find this page, select System Configuration > E-Mail Notifications > E-Mail Notification Templates > Edit Templates (Basic).

Note
Make sure you read the Restrictions for Editing Templates for E-Mail Notifications in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module.

- Field Reference: Edit Templates (Basic)
- Editing Area of the Edit Templates (Basic) Page

Table 25 Field Reference: Edit Templates (Basic)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Template</td>
<td>Which template to view or edit. For template descriptions, see “E-Mail Notification Templates” in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module. Note: For templates that have both SMTP and non-SMTP versions, you must modify both versions to keep them consistent with each other. Otherwise, users may receive different information about the same meeting, depending on the E-mail type and format setting in each user profile.</td>
</tr>
<tr>
<td>Format</td>
<td>Select either the HTML or text version. Note: If you modify an e-mail notification template, you must modify both the HTML and plain text formats to keep them consistent with each other. Otherwise, users may receive different information about the same meeting, depending on the E-mail type and format setting in each user profile. Default: html</td>
</tr>
</tbody>
</table>

Editing Area of the Edit Templates (Basic) Page

Use the editing area to modify the appearance of e-mail notifications.

- For the HTML format, you can modify the font, size, color, and alignment of the text. You can also insert horizontal lines and hypertext links and modify the location of the graphics.
- The tags ($notify_xxxx) are defined in language property files.

Note
The following notes apply to the graphics in e-mail notifications:

- The HTML templates display only the size and location of each graphic.
- Graphics cannot be previewed through the Administration Center and are displayed only in actual e-mail notifications.
- E-mail notification graphics cannot be modified or replaced.
- New graphics cannot be added to e-mail notifications.
Related Topics

- Editing Templates for E-Mail Notifications in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module
- About E-Mail Notification Templates and Language Property Files in the Customizing E-Mail Notifications for Cisco Unified MeetingPlace module

Edit Web Server Page

To find this page, select System Configuration > Web Servers, and then select one of the entries.

Table 26  Field Reference: Edit Web Server Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>FQDN</td>
<td>Fully-qualified domain name of the Web Server.</td>
</tr>
<tr>
<td>Hostname</td>
<td>Hostname of the Web Server. This may or may not be the same as the FQDN.</td>
</tr>
<tr>
<td></td>
<td>When Enabled is set to Yes, this text appears in the drop-down menu of links</td>
</tr>
<tr>
<td></td>
<td>at the top of each Administration Center page.</td>
</tr>
<tr>
<td></td>
<td>See “Changing the Web Server Hostname From an IP Address to a Hostname” in</td>
</tr>
<tr>
<td></td>
<td>the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features</td>
</tr>
<tr>
<td></td>
<td>module.</td>
</tr>
<tr>
<td>Unit number</td>
<td>Display only. Identifies the Web Server associated with this entry. This</td>
</tr>
<tr>
<td></td>
<td>number matches the “Unit” value on the Gateway SIM tab in the MeetingPlace</td>
</tr>
<tr>
<td></td>
<td>Gateways Configuration Utility on the Web Server.</td>
</tr>
<tr>
<td></td>
<td>See “Opening the MeetingPlace Gateways Configuration Utility” in the</td>
</tr>
<tr>
<td></td>
<td>Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager</td>
</tr>
<tr>
<td>Installation key</td>
<td>These fields are required to support a “reverse connection” between the</td>
</tr>
<tr>
<td>IP address</td>
<td>Application Server and the Gateway SIM on the Web Server.</td>
</tr>
<tr>
<td></td>
<td>Obtain the “Installation Key” and “Local IP Address” values from the</td>
</tr>
<tr>
<td></td>
<td>Gateway SIM tab in the MeetingPlace Gateways Configuration Utility on the</td>
</tr>
<tr>
<td></td>
<td>Web Server.</td>
</tr>
<tr>
<td></td>
<td>See “Opening the MeetingPlace Gateways Configuration Utility” in the</td>
</tr>
<tr>
<td></td>
<td>Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager</td>
</tr>
<tr>
<td>Enabled</td>
<td>Whether to enable the following:</td>
</tr>
<tr>
<td></td>
<td>• Gateway SIM “reverse connection” between the Application Server and the</td>
</tr>
<tr>
<td></td>
<td>Web Server.</td>
</tr>
<tr>
<td></td>
<td>• Link to the Web Server from the Administration Center.</td>
</tr>
</tbody>
</table>

Related Topics

- Connecting the Cisco Unified MeetingPlace Application Server to a Web Server module
- Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module
E-Mail Notifications Page

Use this page to perform the following tasks:

- Configuring E-Mail Notification Retries in the Configuring E-Mail Notification Retries module
- Configuring the SMTP Servers in the Configuring E-Mail Notification Retries module
- Customizing E-Mail Notifications for Cisco Unified MeetingPlace module

Enable SSL Page

To find this page, select Certificate Management > Enable SSL.

<table>
<thead>
<tr>
<th>Table 27</th>
<th>Field Reference: Enable SSL Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field</td>
<td>Description</td>
</tr>
<tr>
<td>Certificate file</td>
<td>Restriction: The certificate must be in one of these formats:</td>
</tr>
<tr>
<td></td>
<td>• Privacy enhanced mail (PEM)</td>
</tr>
<tr>
<td></td>
<td>• Distinguished Encoding Rules (DER)</td>
</tr>
<tr>
<td>Private key file</td>
<td>Leave these fields blank if you used the Generate Certificate Signing Request (CSR) Page to obtain a certificate file from a CA. On that page, selecting Generate CSR also causes the system to generate and store the private key file and password for the CA-provided certificate.</td>
</tr>
<tr>
<td>Password</td>
<td>If you use a different tool to obtain a certificate, private key file, and password, then enter values in these fields.</td>
</tr>
<tr>
<td></td>
<td>Also, in the unlikely case that you need to replace your Application Server, you can transfer the certificate file, private key file, and password information to the new Application Server by entering the values in these fields.</td>
</tr>
<tr>
<td>Upload Certificate</td>
<td>This button submits the entered information and enables SSL.</td>
</tr>
</tbody>
</table>

Related Topics

- Uploading the Certificate File and Enabling SSL in the Configuring SSL for the Cisco Unified MeetingPlace Application Server module
- Troubleshooting the Cisco Unified MeetingPlace Application Server module
- Generate Certificate Signing Request (CSR) Page, page 47
Exchange Server Configuration Page

Use this page when configuring your Microsoft Exchange Servers to send Exchange calendar notifications. Changes to this page impact Cisco Unified MeetingPlace users who have E-Mail Type set to Exchange.

To find this page, select System Configuration > E-Mail Notifications > Exchange Server Configuration.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exchange Server</td>
<td></td>
</tr>
<tr>
<td>Hostname (SMTP)</td>
<td>Hostname or IP address of the Microsoft Exchange Server running the SMTP service. This service is required for sending calendar notifications.</td>
</tr>
<tr>
<td>Hostname (WebDAV/EWS)</td>
<td>Hostname or IP address of the Microsoft Exchange Server running the WebDAV/EWS service.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This field is optional. If your Exchange server runs both the email transmission and WebDAV/EWS extension services, leave this field blank. The system will automatically populate it with the information you provided for Hostname (SMTP).</td>
</tr>
<tr>
<td>Language</td>
<td>Used to support localized Exchange servers. Default: en_US.</td>
</tr>
<tr>
<td>TLS enabled</td>
<td>If the Microsoft Exchange Server is configured to use TLS(^1) encryption, then set this to true. Default: false</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> TLS is enabled by default on Exchange 2010. If you are deploying Cisco Unified MeetingPlace in an environment that uses Exchange 2010, set TLS enabled to true.</td>
</tr>
<tr>
<td>MeetingPlace Mailbox Account</td>
<td></td>
</tr>
<tr>
<td>Windows domain</td>
<td>Microsoft Windows domain. Obtain this value from your Microsoft Exchange Server administrator.</td>
</tr>
<tr>
<td>Username</td>
<td>Username for the Cisco Unified MeetingPlace–dedicated e-mail account on the Microsoft Exchange Server. Example: MeetingPlace</td>
</tr>
<tr>
<td>Password</td>
<td>Password for the Cisco Unified MeetingPlace–dedicated e-mail account on the Microsoft Exchange Server.</td>
</tr>
<tr>
<td>Password confirm</td>
<td></td>
</tr>
<tr>
<td>E-mail address</td>
<td>E-mail address of the Cisco Unified MeetingPlace–dedicated e-mail account on the Microsoft Exchange Server. Example: <a href="mailto:MeetingPlace@example.com">MeetingPlace@example.com</a></td>
</tr>
</tbody>
</table>
Table 28  Field Reference: Exchange Server Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox maintenance interval (days)</td>
<td>How often the Microsoft Exchange Server cleans up the mailbox for the Cisco Unified MeetingPlace–dedicated e-mail account on the Microsoft Exchange Server. A value of 0 disables this purge. After you select Save on the Exchange Server Configuration Page, the first purge occurs the following Sunday at 12:00 a.m. (local server time). Default: 7</td>
</tr>
<tr>
<td>Mailbox maintenance cutover (days)</td>
<td>Number of days that notifications are stored in the mailbox for the Cisco Unified MeetingPlace–dedicated e-mail account on the Microsoft Exchange Server. Default: 14</td>
</tr>
<tr>
<td>Test</td>
<td>Use this button to verify the connection between Cisco Unified MeetingPlace and the Microsoft Exchange Server.</td>
</tr>
</tbody>
</table>

1. TLS = Transport Layer Security

Related Topics
- Enabling Microsoft Outlook Calendar Notifications for Meetings Scheduled from the Cisco Unified MeetingPlace End-User Web Interface module

Generate Certificate Signing Request (CSR) Page

Use this page to generate a CSR that you then send to an authorized Certificate Authority (CA) to apply for a digital identity certificate.

Caution
If you already installed a valid SSL certificate, then generating a new CSR will make the existing certificate invalid. Proceed only if you are installing the certificate for the first time, if you are replacing an expired certificate, or if you change the hostname of your Application Server.

Table 29  Field Reference: Generate Certificate Signing Requests (CSRs) Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization unit</td>
<td>The name of your group within your organization. Restriction: If you want to use any special (non-alphanumeric) characters, ask your CA for character restrictions.</td>
</tr>
<tr>
<td>Organization</td>
<td>The name of your organization. Restriction: If you want to use any special (non-alphanumeric) characters, ask your CA for character restrictions.</td>
</tr>
<tr>
<td>City</td>
<td>The city in which you are located.</td>
</tr>
<tr>
<td>State</td>
<td>The state in which you are located. Restriction: Some CAs do not recognize two-letter state abbreviations, so use the full state name.</td>
</tr>
</tbody>
</table>
Import Meetings Page

Use this page to schedule or cancel meetings by import. To find this page, select Maintenance > Import Data > Import Meetings.

Table 29  Field Reference: Generate Certificate Signing Requests (CSRs) Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Country</td>
<td>Two-letter country code that identifies the country in which you are located.</td>
</tr>
</tbody>
</table>

Generate CSR

Creates the following:

- CSR that you download and then send to the CA in return for a certificate file.
- Private key file and password that are stored on the system.

When you later upload the certificate file, the system binds the certificate file with the generated private key file and password to enable SSL.

**Caution**

Do not select this button more than once. Specifically, do not select this button again after downloading the CSR, because the resulting certificate will not work with the private key file and password.

Related Topics

- [Generating a Certificate Signing Request and Obtaining the Certificate](#) in the Configuring SSL for the Cisco Unified MeetingPlace Application Server module
- [Troubleshooting the Cisco Unified MeetingPlace Application Server](#) module
- [Enable SSL Page, page 45](#)

Import Meetings Page

Use this page to schedule or cancel meetings by import. To find this page, select Maintenance > Import Data > Import Meetings.

Table 30  Field Reference: Import Meetings Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to perform</td>
<td>Whether to schedule or cancel meetings. Default: Schedule meetings</td>
</tr>
<tr>
<td>Data file to use</td>
<td>Directory path and filename of the import file that contains the user profile information.</td>
</tr>
<tr>
<td>Scheduler user ID</td>
<td>Username to enter as the owner of meetings with blank SchedulerUid fields in the import file. Default: your username</td>
</tr>
</tbody>
</table>
Import User Groups Page

Use this page to import user groups that are specified in a comma-separated values (CSV) file. To find this page, select Maintenance > Import Data > Import User Groups.

### Table 31 Field Reference: Import User Groups Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to perform</td>
<td>Whether to add or delete user groups from the database.</td>
</tr>
<tr>
<td></td>
<td>Default: Add groups to system</td>
</tr>
<tr>
<td>Data file to use</td>
<td>Directory path and filename of the import file that contains the user group information.</td>
</tr>
<tr>
<td></td>
<td>Default: All existing user groups in the database skipped and remain as is.</td>
</tr>
<tr>
<td>Overwrite duplicate information</td>
<td>Whether to overwrite data that is duplicated in the target file as a result of importing.</td>
</tr>
<tr>
<td></td>
<td>- <strong>No</strong>—All existing user groups in the database are skipped and remain as is.</td>
</tr>
<tr>
<td></td>
<td>- <strong>Yes</strong>—Existing user groups in the database are overwritten by any imported user groups that have identical user group <strong>Numbers</strong>. Note that the group <strong>Name</strong> is not overwritten.</td>
</tr>
<tr>
<td></td>
<td>Restriction: This field is ignored when you select “Delete groups from system” in the <strong>Action to perform</strong> field.</td>
</tr>
<tr>
<td></td>
<td>Default: No</td>
</tr>
</tbody>
</table>
Import User Profiles Page

Use this page to import user profile information that is specified in a comma-separated values (CSV) file. To find this page, select Maintenance > Import Data > Import User Profiles.

### Table 31 Field Reference: Import User Groups Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Send log info to</td>
<td>Choose screen or file.</td>
</tr>
<tr>
<td></td>
<td>Default: Screen</td>
</tr>
<tr>
<td>Error threshold</td>
<td>If the number of errors that occur while importing groups is greater than this error threshold, the system aborts the import.</td>
</tr>
<tr>
<td></td>
<td>To estimate the error threshold, determine the number of groups in the import file and add 10.</td>
</tr>
<tr>
<td></td>
<td>Default: 5000</td>
</tr>
</tbody>
</table>

### Related Topics
- [Import and Export Data Specifications for User Groups](#) in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module
- [Importing Data into Cisco Unified MeetingPlace](#) module

### Import User Profiles Page

Use this page to import user profile information that is specified in a comma-separated values (CSV) file. To find this page, select Maintenance > Import Data > Import User Profiles.

### Table 32 Field Reference: Import User Profiles Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to perform</td>
<td>Whether to add or delete user profiles from the database.</td>
</tr>
<tr>
<td></td>
<td>Default: Add profiles to system</td>
</tr>
<tr>
<td>Data file to use</td>
<td>Directory path and filename of the import file.</td>
</tr>
<tr>
<td>Overwrite duplicate information</td>
<td>When set to No, existing user profiles in the database are not modified by the import process. When set to Yes, the system overwrites each existing user profile in the database that matches both the Profile number and User ID of an imported user profile. Exceptions:</td>
</tr>
<tr>
<td></td>
<td>• In the preconfigured Admin profile, the User status and Type of user fields are not updated with imported values.</td>
</tr>
<tr>
<td></td>
<td>• In the preconfigured Guest profile, the Profile password and Type of user fields are not updated with imported values.</td>
</tr>
<tr>
<td></td>
<td>Restriction: The system does not import any user profile that matches only one (not both) of the Profile number and User ID fields of an existing user profile in the database. Instead, the system reports an error and treats this as an attempt to add a new user profile whose Profile number or User ID (both of which must be unique) conflicts with an existing user profile in the database.</td>
</tr>
<tr>
<td></td>
<td>Default: No</td>
</tr>
</tbody>
</table>

[1] Import and Export Data Specifications for User Groups in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module
[2] Importing Data into Cisco Unified MeetingPlace module
Use this page to import video terminal profile (VTP) information that is specified in a comma-separated values (CSV) file. To find this page, select Maintenance > Import Data > Import Video Terminal Profiles.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action to perform</td>
<td>Whether to add or delete VTPs from the database. Default: Add video terminal profiles to system</td>
</tr>
<tr>
<td>Data file to use</td>
<td>Directory path and filename of the import file.</td>
</tr>
<tr>
<td>Overwrite duplicate</td>
<td>When set to No, existing VTPs in the database are not modified by the import process. When set to Yes, the system overwrites each existing VTP in the database that matches one or both of the following fields in an imported VTP:</td>
</tr>
<tr>
<td>information</td>
<td>• Video terminal name</td>
</tr>
<tr>
<td></td>
<td>• Endpoint E.164 number</td>
</tr>
<tr>
<td>Send log information to</td>
<td>Choose screen or file. Default: Screen</td>
</tr>
<tr>
<td>Error threshold</td>
<td>If the number of errors that occur while importing user profiles is greater than this error threshold, the system aborts the import. To estimate the error threshold, determine the number of users in the import file and add 10. Default: 5000</td>
</tr>
</tbody>
</table>
Related Topics

- Import and Export Data Specifications for Video Terminal Profiles in the Raw Data Export and Import Specifications for Cisco Unified MeetingPlace module

Topics in the Importing Data into Cisco Unified MeetingPlace module:

- Requirements for Importing Data
- Adding or Editing Video Terminal Profiles by Import
- Deleting Video Terminal Profiles by Import
- Examples of Import Files

Install Licenses Page

To find this page, select **Maintenance > Licenses > Install Licenses**.

**Table 34 Field Reference: Install Licenses Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Upload new license file</td>
<td>Specifies to delete all previously installed licenses before installing the license file. Restriction: Select this option only when uploading licenses to your system for the first time, or in the unlikely event that you must install an entirely new set of licenses.</td>
</tr>
<tr>
<td>Append incremental license file</td>
<td>Specifies to keep all the previously installed licenses and to add additional licenses from the license file.</td>
</tr>
<tr>
<td>Host ID (MAC address)</td>
<td><em>Display only.</em> MAC address of the Application Server. You need this address to obtain licenses.</td>
</tr>
<tr>
<td>License file to use</td>
<td>Directory path and filename of the license file.</td>
</tr>
<tr>
<td>Install License</td>
<td>Installs the file specified in the License file to use field.</td>
</tr>
<tr>
<td>Restart License Manager</td>
<td>Use this button to start or restart the license manager.</td>
</tr>
<tr>
<td>Download License</td>
<td>Use this button to save a copy of the license file.</td>
</tr>
</tbody>
</table>

Related Topics

- Installing and Managing Licenses for Cisco Unified MeetingPlace module
- Planning the Capacity of your Cisco Unified MeetingPlace System module in the Planning Guide for Cisco Unified MeetingPlace

Licenses Summary Page

Use this page to display and download licenses for the Cisco Unified MeetingPlace system. To find this page, select **Maintenance > Licenses > Licenses Summary**.
Use this page to perform the following tasks:

- Importing Data into Cisco Unified MeetingPlace
- Running Reports and Exporting Data from Cisco Unified MeetingPlace
- Configuring SNMP on Cisco Unified MeetingPlace
- Installing and Managing Licenses for Cisco Unified MeetingPlace
- Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server
- Sending E-Mail Blasts from Cisco Unified MeetingPlace
- Customizing Music and Voice Prompts for Cisco Unified MeetingPlace

**Media Parameters Page**

Use this page to modify audio and video settings. To find this page, select System Configuration > Call Configuration > Media Parameters.
<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Audio RTP starting port**  | The Media Server assigns RTP/UDP ports starting from the specified value up to that value plus 1024. Modify this field only if required to conform with local firewall rules.  
This field applies only to audio ports. Video ports always start at 20000 and are not configurable.  
Default: 16384 |
| **TTL**                      | Time-to-live value in the IP header of transmitted voice packets. Determines how many hops an IP packet can travel through the network before it is discarded.  
Recommendation: Set the value at least high enough to match the number of router hops between Cisco Unified MeetingPlace and the furthest user endpoint. Using a relatively low number can help reduce the quantity of stray packets on the network.  
Default: 64 |
| **QoS**                      | Differentiated Services (DiffServ) code point (DSCP) settings that determine the QoS for the audio and video media signaling, as defined in RFC 2475.  
Recommendation: Keep the default value. The other values are available for the rare instances when the network requires a different DSCP setting.  
For more information, see the “Network Infrastructure” chapter of the Cisco Unified Communications Solution Reference Network Design (SRND) that applies to your version of Cisco Unified Communications Manager at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html.  
Defaults:  
- Audio media: EF DSCP (101110)  
- Video media: AF41 DSCP (100010)  
- Signaling: CS3 (precedence 3) DSCP (011000) |
| **Echo Canceller**           | Range of echo return delay that the LEC will attempt to cancel.  
Default: 128 |
| **Enable non-linear processing (NLP)** | NLP removes the small amount of residual uncanceled echo that inevitably passes through the echo canceller and may be useful for removing residual echo from acoustic or low-bandwidth voice codec (for example, ITU-T G.729) endpoints.  
Set this field to No:  
- If you do not want to suppress the residual echo.  
- If you notice subtle voice quality issues, such as variations in background noise levels while NLP is enabled.  
Default: Yes |
### Table 36  Field Reference: Media Parameters Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable comfort noise in NLP</td>
<td>To help make the overall background noise level continuous, the NLP generates comfort noise. Set this field to No if you prefer silence instead of comfort noise whenever NLP is actively removing residual echo. Note, however, that disabling comfort noise may result in undesirable variations of background noise levels between silence and noise. Default: Yes</td>
</tr>
</tbody>
</table>
| Enable LEC w. G.729?         | Whether to enable LEC when G.729 is in use. Restrictions:  
  - You must set this field to No if you select the higher capacity option in the Global audio mode field on the Meeting Configuration Page. Otherwise, the G.729 codec will be disabled.  
  - Changes to this field take effect only after restarting the system. Default: Yes |
| Minimum echo return loss (ERL) (dB) | A lower ERL setting may help the LEC cancel loud echoes, but it increases the risk of distortion caused by clipping or squelching of the signal. Default: 6 |
| Bulk delay (milliseconds)     | This value is added to the Window size (milliseconds), so that the cancelled echo return delays will range from Bulk delay (milliseconds) to Bulk delay (milliseconds) + Window size (milliseconds). This allows the LEC to work on echoes that are outside the normal range in exchange for not canceling short-return-delay echoes. Default: 0 |
| Gain Control 6                | AGC causes Cisco Unified MeetingPlace to dynamically adjust the input gain so the average energy matches a specific level. This is useful when various phones, or people in a conference room, produce different volume levels. Nevertheless, AGC can be problematic in cases where noise may be mistaken for voice. When AGC is disabled, the specified Fixed gain (dB) is applied to all inputs. Default: No |
| AGC target level (dBm)        | The target energy level for the AGC algorithm is applied to all inputs. Make this number less negative to increase the average volume level. The default value of -18 is a typical level for telephony circuits. Restriction: This field applies only when the Enable automatic gain control (AGC) field is set to Yes. Default: -18 |
| Fixed gain (dB)               | The fixed input gain is applied to all inputs. Use positive numbers to increase the volume, and use negative numbers to decrease the volume. The default value of 0 leaves the input level alone. Restriction: This field applies only when the Enable automatic gain control (AGC) field is set to No. Default: 0 |
Enable RFC 2833 detection

There are three DTMP methods:

1. RFC-2833, which is negotiated and can be disabled.
2. KPML, which is negotiated and cannot be disabled.
3. In-band DTMF tones, which is not negotiated but can be disabled (see "Enable in-band DTMF detection" setting).

RFC 2833 is a standard mechanism for transmitting keypad digits in-band in VoIP media packets. It is commonly used as an adjunct to SIP signaling. Most calls will negotiate either RFC 2833 (in band) or KPML\(^8\) (out of band) depending on the capabilities of the user endpoint.

If both RFC-2833 and KPML are negotiated (implying that RFC-2833 was enabled), Cisco Unified MeetingPlace will listen for RFC-2833 and not KPML. You can force the use of KPML by disabling RFC 2833 if you are trying to validate KPML. Otherwise, disabling RFC-2833 is typically not necessary as most calls will not notice a difference.

If you do notice a difference it may be due to Cisco Unified Communications Manager inserting a MTP to translate RFC-2833 to KPML. This happens if a trunk or endpoint does not support out-of-band signaling. Depending on the setup, MTP insertion may result in loss of video or, if you run out of MTP resources, call failure.

Default: Yes

Enable in-band DTMF detection

Whether to turn on the signal processing which looks for in-band acoustic DTMF\(^9\) tones in the input audio media stream. Note that DTMF works well only with the G.711 codec.

Recommendation: Enter Yes to support terminals that lack another signaling mechanism, including RFC 2833, KPML, or H.245. Enter No if you find that Cisco Unified MeetingPlace responds to voices as if they were keypad inputs (talk off).

Default: Yes

Jitter Buffer

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Maximum size (milliseconds)</td>
<td>Maximum and minimum lengths of time, in milliseconds, that the jitter buffer holds voice packets. A large jitter buffer helps the system accurately reassemble the media stream, but it adds to perceived latency. Jitter refers to the variation in the delay of received packets. When voice data is sent across the network, the packets are sent in a continuous stream with the packets spaced evenly apart. Due to network congestion, improper queuing, or configuration errors, the delay between each received packet can vary instead of remaining constant. Some packets may even arrive out of order or not arrive at all. A higher Maximum size (milliseconds) helps the system adapt to poor conditions. A lower value may be better for interactive conversations, where an occasional dropped packet may be preferable to long latency. The Minimum size (milliseconds) is the starting jitter buffer size. The closer this value is to the typical jitter on the network, the quicker the system adapts, but this adds directly to latency.</td>
</tr>
<tr>
<td>Minimum size (milliseconds)</td>
<td>Maximum size (milliseconds) default: 250 Minimum size (milliseconds) default: 30</td>
</tr>
</tbody>
</table>
### Meeting Cancellation Report Page

This page provides information about each meeting that was cancelled during a specified range of dates. To find this page, select **Reports > Meeting Cancellation Report**.

#### Table 37  Field Reference: Meeting Cancellation Report Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Report type</strong></td>
<td>Output format, either text or HTML. Restriction: If you select txt, all fields are displayed in the report output. The check boxes for selecting fields become dimmed.</td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td>Output destination. For restrictions and recommendations for each option, see “Reports and Exported Data” in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td><strong>Sort by</strong></td>
<td>Whether you want the report data sorted by scheduler ID, meeting ID, or date. Default: Meeting ID</td>
</tr>
<tr>
<td><strong>Start date</strong></td>
<td>Default: yesterday (mm/dd/yyyy)</td>
</tr>
<tr>
<td><strong>End date</strong></td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
<tr>
<td><strong>Check Boxes and Output Fields</strong></td>
<td>Displays all fields in the report output. Unchecking this clears all check boxes, except Scheduler ID and Meeting ID.</td>
</tr>
</tbody>
</table>

### Related Topics

- Configuring Parameters that Affect Sound and Video Quality in the Configuring Meetings for Cisco Unified MeetingPlace module
Meeting Categories Page

To find this page, select System Configuration > Meeting Categories.

Table 38  Navigation Reference: Meeting Categories Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort by owner, last modifier, or last modification time</td>
<td>Select the Owner, Last Modified By, or Last Modified Time column heading.</td>
</tr>
<tr>
<td>Change the sort order to ascending or descending</td>
<td>Select the column heading to display an arrow. Select the heading again to toggle between a down arrow (ascending sort) and an up arrow (descending sort).</td>
</tr>
<tr>
<td>Display a shorter or longer list in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the number of entries to display.</td>
</tr>
<tr>
<td>Display a different page of entries</td>
<td>At the bottom of the page, perform one of the following actions:</td>
</tr>
<tr>
<td>Search by name</td>
<td>• In the Go field, enter the page number to display, and select Go.</td>
</tr>
<tr>
<td>Edit an existing entry</td>
<td>• Click the arrows to page through the list.</td>
</tr>
<tr>
<td>Create a new meeting category</td>
<td>Select Add New.</td>
</tr>
<tr>
<td>Delete one or more meeting categories</td>
<td>Check the appropriate check boxes in the far left column, then select Delete Selected.</td>
</tr>
<tr>
<td></td>
<td>Restriction: You cannot delete the preconfigured Standard meeting category.</td>
</tr>
</tbody>
</table>
Meeting Configuration Page

Use this page to configure system-wide meeting parameters. To find this page, select **System Configuration > Meeting Configuration**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Audio Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Audio licensed ports | *Display only.* Number of voice licenses installed on the system, determined by the installed videoconf and maxvoice licenses. To view installed licenses, see “Displaying Licenses” in the Installing and Managing Licenses for Cisco Unified MeetingPlace module.  
Voice ports are also used by meeting recordings. See “Recording Resources and Port Usage” in the Configuring Recordings for Cisco Unified MeetingPlace module.  
The displayed value determines the maximum possible number of simultaneous voice meeting connections to Cisco Unified MeetingPlace. |
| Audio available ports | *Display only.* Number of voice ports for scheduled and reservationless meetings on the system, determined by either the Audio licensed ports field or the Audio capacity override (ports) field. This number is also affected by the Global audio mode field setting.  
Voice ports are also used by meeting recordings. See “Recording Resources and Port Usage” in the Configuring Recordings for Cisco Unified MeetingPlace module.  
The displayed value determines the maximum possible number of simultaneous voice meeting connections to Cisco Unified MeetingPlace. |
| Audio floater ports | Number of voice ports that are reserved as floater ports. Floater ports can be used by any meeting to accommodate unanticipated additional attendees. Configuring voice floater ports reduces the number of ports that are available for scheduling meetings.  
Voice floater ports are also used by meeting recordings. See “Recording Resources and Port Usage” in the Configuring Recordings for Cisco Unified MeetingPlace module.  
Restrictions:  
• This number cannot exceed the value of the Audio available ports field.  
• Changing the licenses may affect the upper and lower limits for this parameter.  
Default: 2 |
| Audio overbook ports | Number of voice ports to allow for scheduling meetings that exceed the number of available voice ports on the system. Configuring voice overbook ports increases the risk of users being unable to attend scheduled meetings.  
If you use this feature, you assume that users who are scheduled to attend meetings do not always attend, leaving their reserved voice ports unused. Once all voice ports are in use, other users who try to attend a voice meeting will not be able to get through.  
Restrictions:  
• This number cannot exceed twice the value of the Audio available ports field.  
• Changing the licenses may affect the upper and lower limits for this parameter.  
Default: 0 |
Table 39  **Field Reference: Meeting Configuration Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Video Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Video licensed ports</td>
<td><em>Display only.</em> Number of video licenses on the system, determined by the installed videoconf and maxvideo licenses. To view installed and enabled licenses, see “Displaying Licenses” in the Installing and Managing Licenses for Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td>Video available ports</td>
<td><em>Display only.</em> Number of video ports for scheduled and reservationless meetings on the system, determined by either the Video licensed ports field or the Video capacity override (ports) field. This number is also affected by the Global video mode field setting. Video ports can also be used by meeting recordings. See “Recording Resources and Port Usage” in the Configuring Recordings for Cisco Unified MeetingPlace module. The displayed value determines the maximum possible number of simultaneous video connections to Cisco Unified MeetingPlace.</td>
</tr>
</tbody>
</table>
| Video floater ports | Number of video ports that are reserved as floater ports. Floater ports can be used by any meeting to accommodate unanticipated additional attendees. Video floater ports can also be used by meeting recordings. See “Recording Resources and Port Usage” in the Configuring Recordings for Cisco Unified MeetingPlace module. Restrictions:  
  - This number cannot exceed the value of the Video available ports field.  
  - Changing the licenses may affect the upper and lower limits for this parameter.  
See “Recommendations for Determining the Number of Floater Ports” in the Planning the Capacity of your Cisco Unified MeetingPlace System module. Default: 0 |
| Video overbook ports | Number of video ports to allow for scheduling meetings that exceed the number of available video ports on the system.  
If you use this feature, you assume that users who are scheduled to attend meetings do not always attend or use video, leaving their reserved video ports unused. Once all video ports are in use, any other video users who try to attend a meeting will join audio-only; if no voice ports are available at that time, then those users will not be able to attend. Restrictions:  
  - This number cannot exceed twice the value of the Video available ports field.  
  - Changing the licenses may affect the upper and lower limits for this parameter. Default: 0 |
| **Web Settings**   |                                                                                                                                               |
| Web licensed ports | *Display only.* Number of web ports for scheduled and reservationless meetings on the system, determined by the installed webconf and maxweb licenses. To view installed and enabled licenses, see the “Displaying Licenses” section on page 4. The value determines the maximum number of possible simultaneous connections to Cisco Unified MeetingPlace using the full web meeting room. Web ports are allocated on an ad-hoc basis and are never reserved for meetings.  
**Note**  
Cisco Unified MeetingPlace web ports are not used by Cisco WebEx web meetings. |
### Table 39  Field Reference: Meeting Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Override System Capacity</strong></td>
<td></td>
</tr>
<tr>
<td>Use licensed audio capacity</td>
<td>Whether the Audio available ports field value is determined by the Audio licensed ports field or the Audio capacity override (ports) field. Recommendation: Set this to No when the licensed capacity is greater than the physical capacity of your system. See “Limitations for Cisco Unified MeetingPlace Licenses” in the Planning the Capacity of your Cisco Unified MeetingPlace System module. Default: Yes</td>
</tr>
<tr>
<td>Audio capacity override (ports)</td>
<td>Number of voice ports for scheduled and reservationless meetings on the system. This field can be modified only when the Use licensed audio capacity field is set to No. Recommendation: Enter the number of audio ports that are supported by your Media Server. See “Limitations for Cisco Unified MeetingPlace Licenses” in the Planning the Capacity of your Cisco Unified MeetingPlace System module.</td>
</tr>
<tr>
<td>Use licensed video capacity</td>
<td>Whether the Video available ports field value is determined by the Video licensed ports field or the Video capacity override (ports) field. Recommendation: Set this to No when the licensed capacity is greater than the physical capacity of your system. See “Limitations for Cisco Unified MeetingPlace Licenses” in the Planning the Capacity of your Cisco Unified MeetingPlace System module. Default: Yes</td>
</tr>
<tr>
<td>Video capacity override (ports)</td>
<td>Configurable number of video ports for scheduled and reservationless meetings on the system. This field is configurable only when the Use licensed video capacity field is set to No. Recommendation: Enter the number of video ports that are supported by your Media Server. See “Limitations for Cisco Unified MeetingPlace Licenses” in the Planning the Capacity of your Cisco Unified MeetingPlace System module.</td>
</tr>
<tr>
<td><strong>Global Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Global video mode</td>
<td>Limits the bandwidth of video calls: • Standard rate—384 kbps maximum • High rate—2 Mbps maximum Restriction: The maximum bandwidth of video calls may also be limited by the following settings, the lowest of which is enforced: • Video Call Bandwidth region parameter in Cisco Unified Communications Manager. See “Configuring the Maximum Video Call Bandwidth in Cisco Unified Communications Manager” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module. • Bandwidth capabilities and configurations of the video endpoints. Default: High rate</td>
</tr>
<tr>
<td>Global audio mode</td>
<td>Choose between the higher capacity and higher quality options.</td>
</tr>
</tbody>
</table>
### Table 39  Field Reference: Meeting Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Meeting Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Maximum ports per reservationless meeting</td>
<td>Maximum number of voice, web, or video ports that can be used in a meeting. These fields restrict both of the following:</td>
</tr>
<tr>
<td></td>
<td>• Maximum number of ports that can be reserved when a meeting is scheduled.</td>
</tr>
<tr>
<td></td>
<td>• Maximum size that a meeting can grow to, even when ports are still available.</td>
</tr>
<tr>
<td></td>
<td>Restrictions:</td>
</tr>
<tr>
<td></td>
<td>• This number cannot exceed the value of either the Audio available ports field or the Web licensed ports field.</td>
</tr>
<tr>
<td></td>
<td>• The upper and lower limits for this field also depend on the Global video mode and Global audio mode field values.</td>
</tr>
<tr>
<td></td>
<td>• This number cannot exceed 1000.</td>
</tr>
<tr>
<td></td>
<td>Default: 6</td>
</tr>
<tr>
<td>Maximum ports per scheduled meeting</td>
<td>Maximum reserved ports per scheduled meeting (MR2 only) restricts the maximum number of ports that can be reserved when a meeting is scheduled.</td>
</tr>
<tr>
<td></td>
<td>• The upper limit for this field is Maximum ports per scheduled meeting</td>
</tr>
<tr>
<td></td>
<td>• The lower limit for this field is 2.</td>
</tr>
<tr>
<td>Maximum reserved ports per scheduled meeting (MR2 only)</td>
<td></td>
</tr>
<tr>
<td>Default number of ports per audio meeting</td>
<td>Default number of voice ports to reserve for meetings. This value is used in the Number of Participants field when scheduling meetings. This field also applies to reservationless meetings.</td>
</tr>
<tr>
<td></td>
<td>Restriction: This number cannot exceed the Audio available ports field.</td>
</tr>
<tr>
<td></td>
<td>Default: 4</td>
</tr>
<tr>
<td>Default meeting length (minutes)</td>
<td>Default length of meetings, in minutes. This value is used in the Duration field when scheduling meetings. This field also applies to reservationless meetings.</td>
</tr>
<tr>
<td></td>
<td>Restrictions:</td>
</tr>
<tr>
<td></td>
<td>• This number cannot exceed the value entered in the Maximum meeting length (minutes) field.</td>
</tr>
<tr>
<td></td>
<td>• This field does not apply to meetings that are scheduled from Microsoft Outlook.</td>
</tr>
<tr>
<td></td>
<td>Default: 30</td>
</tr>
<tr>
<td>Maximum meeting length (minutes)</td>
<td>User cannot schedule meetings longer than this number of minutes. Also, reservationless meetings end after this number of minutes.</td>
</tr>
<tr>
<td></td>
<td>Restriction: If this value differs from the following, then the lowest value is used:</td>
</tr>
<tr>
<td></td>
<td>• Maximum meeting length (minutes) field in the user profile of the meeting owner.</td>
</tr>
<tr>
<td></td>
<td>• Maximum Call Duration Timer service parameter in Cisco Unified Communications Manager.</td>
</tr>
<tr>
<td></td>
<td>See “Configuring the Maximum Call Duration in Cisco Unified Communications Manager” in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.</td>
</tr>
<tr>
<td></td>
<td>Default: 240</td>
</tr>
</tbody>
</table>
Table 39  **Field Reference: Meeting Configuration Page (continued)**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Meeting ID start guard time (minutes)</td>
<td>Number of minutes before the requested meeting start time that the meeting ID is reserved. This field and the Meeting ID end guard time (minutes) field control when meeting IDs are available for reuse and when the system recognizes a meeting ID. Before the meeting ID start guard time, users who try to attend the meeting hear or see on the screen: “This is not a recognized meeting ID number.” During the meeting ID start guard time period, users hear: “The meeting has not started.” Meeting ID start guard times are not applied to reservationless meetings or meetings that begin immediately. Recommendation: 30. To ensure that meeting IDs are available for reuse, decrease this value if the number of simultaneous meetings to be held on your system is about the same as the number of available meeting IDs. Default: 30</td>
</tr>
<tr>
<td>Meeting ID end guard time (minutes)</td>
<td>Number of minutes after a meeting that the meeting ID is reserved. This field and the Meeting ID start guard time (minutes) field control when meeting IDs are available for reuse and when the system recognizes a meeting ID. During the meeting ID end guard time, users who try to attend the meeting hear or see on the screen: “The meeting has ended.” After the meeting ID end guard time period, users hear: “This is not a recognized meeting ID number.” Meeting ID end guard times are not applied to reservationless meetings or meetings that are user-terminated before the scheduled end time. Recommendation: 15. To ensure that meeting IDs are available for reuse, decrease this value if the number of simultaneous meetings to be held on your system is about the same as the number of available meeting IDs. Default: 30</td>
</tr>
<tr>
<td>Extend meeting (minutes)</td>
<td>Whether to extend meetings if they run over the requested duration and if ports are available. Meetings may continue to be extended as long as ports are available, up to the Maximum meeting length (minutes) field value. Specifically for web meeting rooms: • For meetings scheduled with zero locations, the web meeting is extended as long as there is at least one participant in the web meeting room. • For meetings scheduled with at least one location, the web meeting is extended only if there are at least two voice meeting participants. If you select Yes, then also enter the number of minutes to extend meetings. If you select No, or if ports are not available at the end of the meeting, callers receive a warning that the meeting will end. The warning time is determined by the Last warning time (minutes) field. <strong>Note</strong> If you have two consecutive meetings with the same meeting ID, the first occurrence of the meeting (Meeting 1) will be extended if the second occurrence (Meeting 2) complies with the following condition: Extend Meeting time is less than (Meeting2StartTime - StartGuardTime) - (Meeting1EndTime + EndGuardTime) Default: Yes, 15</td>
</tr>
</tbody>
</table>
### Table 39 Field Reference: Meeting Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Early meeting start (minutes)</td>
<td>Maximum time, in minutes, before the scheduled meeting start that participants may enter the meeting. This field does not apply to reservationless meetings.</td>
</tr>
<tr>
<td></td>
<td>Restriction: This number cannot exceed the value entered in the Meeting ID start guard time (minutes) field.</td>
</tr>
<tr>
<td></td>
<td>Recommendation: 10. If you plan to permit consecutive meetings with the same meetingID, make sure that you set the Early meeting start parameter so that it is less than or equal to the meeting ID start guard time.</td>
</tr>
<tr>
<td></td>
<td>Default: 10</td>
</tr>
<tr>
<td>Last warning time (minutes)</td>
<td>Number of minutes before the end of a meeting when the system issues a warning.</td>
</tr>
<tr>
<td></td>
<td>Default: 2</td>
</tr>
<tr>
<td>Minimum meeting password length</td>
<td>Minimum number of characters required in meeting passwords.</td>
</tr>
<tr>
<td></td>
<td>A value of 0 means that meeting passwords are never required, even for meetings that are scheduled by users whose user profile Meeting password required field is set to Yes.</td>
</tr>
<tr>
<td></td>
<td>Recommendation: Follow your company guidelines for similar telecommunications systems.</td>
</tr>
<tr>
<td></td>
<td>Default: 0</td>
</tr>
<tr>
<td>Maximum advance days to schedule</td>
<td>How many days in advance users can schedule meetings.</td>
</tr>
<tr>
<td></td>
<td>Default: 300</td>
</tr>
<tr>
<td>Days until meeting statistics purged</td>
<td>Minimum number of days that meeting data is stored on the Application Server and Web Server. To determine the actual date when the meeting data will be purged:</td>
</tr>
<tr>
<td></td>
<td>• If you enter a value less than 7, then the system purges the meeting data after the specified number plus 7 days. For example, if you enter 5, then the meeting data is purged after 5 + 7 = 12 days.</td>
</tr>
<tr>
<td></td>
<td>• If you enter a value equal to or greater than 7 days, then the system purges the meeting data after the specified number of days. For example, if you enter 7, then the meeting data is purged after 7 days.</td>
</tr>
<tr>
<td></td>
<td>Restriction: Seven days after a meeting was scheduled to occur, the system applies the value that you configure in this field. For example, if you set this field to “7,” the system purges meeting statistics immediately after it applies the field value to the meeting. If you set this field to “3,” the system purges meeting statistics three days later.</td>
</tr>
<tr>
<td></td>
<td>This field also affects Cisco Unified MeetingPlace report data. When meetings are purged, they are no longer available for reporting purposes.</td>
</tr>
<tr>
<td></td>
<td>Default: 38</td>
</tr>
<tr>
<td>Allow vanity meeting IDs</td>
<td>Whether users may request a specific meeting ID when scheduling a meeting. If a user requests a meeting ID that is already reserved for another meeting, the system prompts the user to select another meeting ID.</td>
</tr>
<tr>
<td></td>
<td>If you select No, the system generates a unique, randomly generated ID for every scheduled meeting. Users cannot change the assigned meeting IDs.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
</tbody>
</table>
Table 39  Field Reference: Meeting Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum scheduled meeting ID length</td>
<td>Minimum number of characters in meeting IDs. Note that longer meeting IDs are more secure, because they are more difficult to guess. Restriction: If this value is set to 3 and the scheduler does not enter a vanity meeting ID, the system assigns a four-digit meeting ID to all new meetings. Default: 4</td>
</tr>
<tr>
<td>Enable rescheduled recurring meetings</td>
<td>Whether to enable users to reschedule recurring meetings. Default: Yes</td>
</tr>
<tr>
<td>Disconnect empty port (minutes)</td>
<td>Number of minutes after the scheduled start time that ports are held after all participants leave, even when the scheduled meeting time is not over. This time accounts for longer meetings when people break and return to the meeting. This time also applies if no one comes to the meeting. For meetings that were scheduled with the “Number of Participants” set to 0, this field applies only when one person remains in the web meeting. This parameter does not apply to reservationless meetings. Default: 30</td>
</tr>
<tr>
<td>Early meeting port release (minutes)</td>
<td>Number of minutes before the scheduled end of a meeting that ports are released if no ports are in use for that meeting. For meetings that were scheduled with the “Number of Participants” set to 0, this field applies only when one person remains on the web conference. Default: 5</td>
</tr>
</tbody>
</table>

Auto-Answer Devices

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Meeting controls device | Determines whether the meeting owner or the meeting itself controls when auto-answer devices are disconnected from each meeting:  
  • No—When the meeting owner leaves the meeting, all auto-answer devices are disconnected from the meeting.  
    If the meeting owner never joins the meeting, then auto-answer devices are disconnected from the meeting when ports are disconnected or released due to the Disconnect empty port (minutes) and Early meeting port release (minutes) settings on the Meeting Configuration Page, whichever field is enforced first.  
  • Yes—The Connected until meeting ends field is enforced.  
  Restriction: You must select Yes if your Cisco Unified MeetingPlace system is integrated with Cisco WebEx. Otherwise, the Cisco WebEx audio recorder will not work. Default: No |
### Field Reference: Meeting Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Connected until meeting ends           | Determines how meeting-controlled auto-answer devices are disconnected from meetings:  
- No—All auto-answer devices are disconnected from the meeting when all non-auto-answer participants leave the meeting.  
- Yes—Auto-answer devices are disconnected from the meeting when ports are disconnected or released due to the Disconnect empty port (minutes) and Early meeting port release (minutes) settings on the Meeting Configuration Page, whichever field is enforced first.  
Restriction: This field is ignored when the Meeting controls device field is set to No.  
Default: No                                                                               |
| Disconnect when all continuous meeting parties leave | Whether to disconnect auto-answer devices from continuous meetings when all non-auto-answer participants leave the meeting.  
Recommendation: Set this field to Yes if both the Meeting controls device and Connected until meeting ends fields are also set to Yes. Otherwise, the system will never automatically disconnect auto-answer devices from continuous meetings.  
Default: No                                                                               |

#### Recordings

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Maximum meeting message length (minutes) | Maximum length of each recorded meeting message.  
Default: 60                                                                                                                                                                                                 |
| Maximum meeting name length (seconds)   | Maximum length of recorded meeting names.  
Default: 4                                                                                                                                                                                                |
| Maximum participant name length (seconds) | Maximum length of recorded meeting participant names.  
Default: 4                                                                                                                                                                                               |

### Related Topics

- Configuring Meetings for Cisco Unified MeetingPlace module
- How to Configure Auto-Answer Devices in the Configuring Endpoints for Cisco Unified MeetingPlace module
- Configuring Recordings for Cisco Unified MeetingPlace module
- “Planning the Capacity of your Cisco Unified MeetingPlace System” module in the Planning Guide for Cisco Unified MeetingPlace.
Meeting Information Report Page

This report provides information about meetings that occur in the specified date range. The output is grouped by User ID of the meeting owner. To find this page, select Reports > Meeting Information Report.

Table 40  Field Reference and Output Field Reference: Meeting Information Report Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Report type</td>
<td>Output format, either text or HTML.</td>
</tr>
<tr>
<td>Destination</td>
<td>Output destination. For restrictions and recommendations for each option, see “Reports and Exported Data” in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td>Start date</td>
<td>Default: yesterday (mm/dd/yyyy)</td>
</tr>
<tr>
<td>End date</td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
</tbody>
</table>

Check Boxes and Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Owner ID</td>
<td>User ID of the meeting owner.</td>
</tr>
<tr>
<td>Date held</td>
<td>Date and time that this meeting took place.</td>
</tr>
<tr>
<td>Billing code</td>
<td>Billing code for the meeting.</td>
</tr>
<tr>
<td>Disk space purge date</td>
<td>Date and time when recordings for the meeting will be deleted from the Application Server. This purge date cannot be changed, and it is set to 7 days after the meeting ends.</td>
</tr>
<tr>
<td>Scheduled length</td>
<td>Length of time scheduled for the meeting.</td>
</tr>
<tr>
<td>Actual length</td>
<td>Actual meeting length, from when the first meeting participant joined to when the last meeting participant left. If the meeting is not attended, the length is 1+ the disconnect empty port (minutes).</td>
</tr>
<tr>
<td>Roll call</td>
<td>Number of minutes used to record the participant names or locations.</td>
</tr>
</tbody>
</table>

Additional Output Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total for &lt;User ID&gt;</td>
<td>Sums of the following items for the user:</td>
</tr>
<tr>
<td></td>
<td>• Scheduled length</td>
</tr>
<tr>
<td></td>
<td>• Actual length</td>
</tr>
<tr>
<td></td>
<td>• Roll call</td>
</tr>
<tr>
<td>Number of Meetings</td>
<td>Number of meetings in this report that were owned by the user.</td>
</tr>
</tbody>
</table>

Related Topics

- Running Reports and Exporting Data from Cisco Unified MeetingPlace module
Migration Import Tool

Use this file to migrate user groups, user profiles, and meetings from an existing Cisco Unified MeetingPlace system of a previous release.

To find this page, select Maintenance > Migration Import Tool.

Caution

Once you execute a migration, do not make any changes in the Administration Center until the migration is complete.

Table 41  Field Reference: Migration Import Tool Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data file to use</td>
<td>Selects the data migration file.</td>
</tr>
<tr>
<td>Send log information to</td>
<td>Whether to display the migration log information on the screen or save the log information to a file.</td>
</tr>
<tr>
<td>Error threshold</td>
<td>If the number of errors that occur while importing the migration file is greater than this error threshold, then the system aborts the import. Default: 50</td>
</tr>
<tr>
<td>Exclude meetings started before</td>
<td>Use to specify a date range for the migration log. Any data prior to the specified date is excluded from the log.</td>
</tr>
</tbody>
</table>

Related Topics


Notification Configuration Page

To find this page, select System Configuration > E-Mail Notifications > Notification Configuration.

Table 42  Field Reference: Notification Configuration Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>If notification fails retry (times)</td>
<td>Default: 3</td>
</tr>
<tr>
<td>Delay between retries (seconds)</td>
<td>Default: 10</td>
</tr>
<tr>
<td>If still fails wait before trying again (hours)</td>
<td>Default: 4</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring E-Mail Notification Retries in the Configuring E-Mail Notifications for Cisco Unified MeetingPlace module
Notification Destinations Page

To find this page, select Maintenance > SNMP > Notification Destinations.

Table 43  Field Reference: Notification Destinations Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination IP address</td>
<td>Click to edit this notification destination.</td>
</tr>
<tr>
<td>Port number</td>
<td>Port number of this notification destination.</td>
</tr>
<tr>
<td>SNMP version</td>
<td>Either SNMP version 1 or version 2c.</td>
</tr>
<tr>
<td>Community string name</td>
<td>Community string associated with this notification destination.</td>
</tr>
<tr>
<td>Notification type</td>
<td>Either trap or inform.</td>
</tr>
</tbody>
</table>

Related Topics
- Adding or Editing SNMP Notification Destinations in the Configuring SNMP on Cisco Unified MeetingPlace module
- Displaying or Deleting SNMP Notification Destinations in the Configuring SNMP on Cisco Unified MeetingPlace module

Outlook Authentication Configuration Page

To find this page, select System Configuration > Outlook Authentication Configuration.

Note
This page appears only when the msft_int license is installed.

Use this page to configure the default authentication method for users who schedule Cisco Unified MeetingPlace meetings from Microsoft Outlook.

If you select the Single Sign-On authentication method, then the following options become available:
- To add a domain, select Add New.
- To edit an existing entry, select the name of that entry.
- To delete an entry, check the item and select Delete Selected.
Outlook Plug-In Configuration Page

Use this page to configure which Cisco Unified MeetingPlace servers become available in the client PC Microsoft Outlook options after the plug-in is installed.

- To add a server, select Add New.
- To edit an existing entry, select the name of that entry.
- To delete an entry, check the item and select Delete Selected.

To find this page, select System Configuration > Outlook Plug-In Configuration.
Note

This page appears only when the msft_int license is installed.

Table 45  Field Reference: Outlook Plug-In Configuration Page, Add Cisco Unified MeetingPlace Server Page, and Edit Cisco Unified MeetingPlace Server Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Make Cisco Unified MeetingPlace form the default appointment form</td>
<td>Whether to use the Cisco Unified MeetingPlace scheduling form by default for all new Microsoft Outlook appointments and meetings. The user can override this setting from Microsoft Outlook by selecting <strong>Tools &gt; Options</strong> and selecting the <strong>MeetingPlace</strong> tab. Default: Yes</td>
</tr>
<tr>
<td>Name</td>
<td>Unique name to appear in the list of available Cisco Unified MeetingPlace systems in the Microsoft Outlook options on the end-user PC. Restriction: This field cannot contain any spaces. You may, however, use an underscore character (_), for example, “my_mpox_server.”</td>
</tr>
<tr>
<td>URL</td>
<td>URL of the Cisco Unified MeetingPlace server to associate with the entered Name. If SSL is enabled, be sure that the URL starts with “https” and not “http”. Required format: <a href="http://hostname/outlook/mpe">http://hostname/outlook/mpe</a></td>
</tr>
</tbody>
</table>

Related Topics

- Adding Cisco Unified MeetingPlace Systems to the Plug-In for Microsoft Outlook in the Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module

Port Utilization Report Page

To find this page, select **Reports > Port Utilization Report**.

Use this page to compare the number of ports scheduled to the number of ports actually used during a specified period of time. This information can help you determine the peak and off-peak times for your system and compare resource usage with available capacity.

- Field Reference: Port Utilization Report Page
- Output Reference: Port Utilization Report

Table 46  Field Reference: Port Utilization Report Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
<tr>
<td>Start time</td>
<td>The hour you want the port utilization report data to begin. Default: 8:00 AM</td>
</tr>
</tbody>
</table>
Output Reference: Port Utilization Report

The port utilization report output is a chart that shows the following information:

- Date and times represented by the report.
- Number of licensed ports on the system for the selected Conference type.
- (Red data) Percentage of licensed ports that were scheduled for meetings of the selected Conference type.
- (Blue data) Percentage of licensed ports that were actually used to attend meetings of the selected Conference type.

Related Topics

- Running Reports and Exporting Data from Cisco Unified MeetingPlace module

Remote Server Configuration Page

To find this page, select System Configuration > Remote Server Configuration.

Table 46 Field Reference: Port Utilization Report Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>End time</td>
<td>The hour you want the port utilization report data to end. Default: 5:00 PM</td>
</tr>
<tr>
<td>Conference type</td>
<td>Whether you want report data about voice, web, or video meetings. Default: Voice</td>
</tr>
</tbody>
</table>

Remote Server Configuration

See “Configuring the Remote Servers” in the Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module.

Auto Answer Parameters

The Auto-Answer Devices fields were moved to the Meeting Configuration Page in Release 7.0.2.

Reservationless Single Number Access

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable RSNA</td>
<td>Whether or not the Reservationless Single Number Access (RSNA) feature is enabled.</td>
</tr>
<tr>
<td>Dial prefix</td>
<td>Reserved for a future release.</td>
</tr>
</tbody>
</table>

Related Topics

- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module
- How to Configure Auto-Answer Devices in the Configuring Endpoints for Cisco Unified MeetingPlace module
- Field Reference: Add Server Configuration Page and Edit Server Configuration Page
**Sametime Configuration Page**

To find this page, select **System Configuration > Sametime Configuration**. Use this page to:

- Connect Cisco Unified MeetingPlace to an IBM Lotus Sametime server.
- Download the installer for Cisco Unified MeetingPlace for IBM Lotus Sametime Web Conferencing.

**Related Topics**

- **Sametime Servers Page**, page 73
- *Integration Note for Installing and Configuring IBM Lotus Sametime Web Conference with Cisco Unified MeetingPlace*
  

**Sametime Servers Page**

To find this page, select **System Configuration > Sametime Configuration > Sametime Servers**.

**Table 48 Navigation Reference: Sametime Servers Page**

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edit an existing server entry</td>
<td>Select <strong>Edit</strong> in the same row as the server hostname.</td>
</tr>
<tr>
<td>Create a new server entry</td>
<td>Select <strong>Add New</strong>, enter the hostname, and select <strong>Save</strong>.</td>
</tr>
<tr>
<td>Delete one or more server entries</td>
<td>Check the appropriate check boxes in the far left column, then select <strong>Delete Selected</strong>.</td>
</tr>
</tbody>
</table>

**Related Topics**

- *Integration Note for Installing and Configuring IBM Lotus Sametime Web Conference with Cisco Unified MeetingPlace*
  

**SIP Configuration Page**

To find this page, select **System Configuration > Call Configuration > SIP Configuration**.

**Table 49 Field Reference: SIP Configuration Page**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Display name</td>
<td>Name that appears on Cisco Unified IP Phone screens during calls placed by Cisco Unified MeetingPlace. Default: Cisco Unified MeetingPlace</td>
</tr>
<tr>
<td>Username</td>
<td>Enter the same value that is in the <strong>Access phone number 1</strong> field on the <strong>Usage Configuration Page</strong>. The system uses this value in the “From” address for outgoing calls. Default: 0000</td>
</tr>
</tbody>
</table>
Table 49  Field Reference: SIP Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Only accept incoming calls from proxies</td>
<td>Whether to accept incoming calls from only the SIP proxy servers that are configured on the SIP Configuration Page. If you select Yes, then make sure that the configured SIP proxy servers include all Cisco Unified Communications Manager subscriber nodes that might send calls directly to this Cisco Unified MeetingPlace server. Default: No</td>
</tr>
<tr>
<td>SIP domain name</td>
<td>Domain name that is used in the “To” address for outgoing calls. If left blank, then the Application Server IP address is used instead. Typically, this field is left blank when the SIP Proxy Server fields are populated with Cisco Unified Communications Manager information. If you enter a value that does not match the domain used by the SIP proxy servers, then Cisco Unified MeetingPlace will fail to dial out.</td>
</tr>
<tr>
<td>Caution</td>
<td>If outgoing calls fail, then configure this field to match the SIP domain used by the SIP Proxy Server or your local Cisco Unified Communications Manager node. In Cisco Unified Communications Manager, the SIP domain is specified under System &gt; Enterprise Parameters in the Organization Top Level Domain field.</td>
</tr>
<tr>
<td>Note</td>
<td>For details about any field in Cisco Unified Communications Manager, select the field name, or select Help &gt; This Page.</td>
</tr>
<tr>
<td>Example: cisco.com</td>
<td></td>
</tr>
<tr>
<td>SIP Proxy Server</td>
<td>Outgoing SIP calls are directed to these proxies. These proxies are also used to filter incoming calls if the Only accept incoming calls from proxies field is set to Yes. Note: At least one SIP proxy server must be configured to enable dial-out calls. If multiple proxy servers are configured when placing a call, Cisco Unified MeetingPlace tries each one successively until it finds one that accepts the call. Note, however, that if a proxy does not respond at all (as opposed to rejecting the invite), the call attempt will probably time out before the next proxy is tried.</td>
</tr>
<tr>
<td>Hostname or IP address</td>
<td>Hostname or IP address of the SIP proxy server.</td>
</tr>
<tr>
<td></td>
<td>In a Cisco Unified Communications Manager environment, the SIP proxy server should be the IP address of a Cisco Unified Communications Manager node. Enter the FQDN (or IP address) if the domain of the SIP proxy server differs from the domain that you configured in DNS when you installed Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td>Port</td>
<td>TCP or UDP port on which the proxy listens for SIP calls. Default: 5060</td>
</tr>
<tr>
<td>Transport</td>
<td>Whether the port is TCP or UDP. Recommendation: Use TCP for the SIP signaling between Cisco Unified MeetingPlace and Cisco Unified Communications Manager. This is already the default on the Cisco Unified Communications Manager side. Default: UDP</td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>
1. FQDN = fully-qualified domain name

Related Topics
- Configuring Call Control for Cisco Unified MeetingPlace module

SMTP Server Configuration Page

Use this page to configure your servers to send plain SMTP notifications. This impacts those Cisco Unified MeetingPlace users who have E-Mail Type set to SMTP.

To find this page, select System Configuration > E-Mail Notifications > SMTP Server Configuration.

Table 50  Field Reference: SMTP Server Configuration Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Primary SMTP Server</td>
<td></td>
</tr>
<tr>
<td>Primary SMTP server</td>
<td>Hostname or IP address of the primary SMTP server. Example: mail1.example.com</td>
</tr>
<tr>
<td>Primary SMTP server authentication</td>
<td>Whether the primary SMTP server requires authentication for Cisco Unified MeetingPlace. Default: false</td>
</tr>
<tr>
<td>Primary SMTP server username</td>
<td>SMTP server username to use for authentication for the primary SMTP server.</td>
</tr>
<tr>
<td>Primary SMTP server password</td>
<td>SMTP server password to use for authentication for the primary SMTP server. confirm</td>
</tr>
<tr>
<td>Secondary SMTP Server</td>
<td></td>
</tr>
<tr>
<td>Secondary SMTP server</td>
<td>Hostname or IP address of the secondary SMTP server. Example: mail2.example.com</td>
</tr>
<tr>
<td>Secondary SMTP server authentication</td>
<td>Whether the secondary SMTP server requires authentication for Cisco Unified MeetingPlace. Default: false</td>
</tr>
<tr>
<td>Secondary SMTP server username</td>
<td>SMTP server username to use for authentication for the secondary SMTP server.</td>
</tr>
<tr>
<td>Secondary SMTP server password</td>
<td>SMTP server password to use for authentication for the secondary SMTP server. confirm</td>
</tr>
</tbody>
</table>

Related Topics
- Configuring E-Mail Notifications for Cisco Unified MeetingPlace module
System Configuration Page

Use this page to perform the following tasks:

- Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace module
- Configuring Meetings for Cisco Unified MeetingPlace module
- Configuring Languages for Cisco Unified MeetingPlace module
- Configuring Call Control for Cisco Unified MeetingPlace module
- Configuring E-Mail Notifications for Cisco Unified MeetingPlace module
- Configuring Attendant Settings for Cisco Unified MeetingPlace module
- Configuring the Auto Attend Feature for Cisco Unified MeetingPlace module
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace module
- Integrating Cisco Unified MeetingPlace with Cisco WebEx module
- Enabling Cisco Unified MeetingPlace Scheduling from Microsoft Outlook module
- Securing the Cisco Unified MeetingPlace System module

System Information Capture Page

Running this log generates a very large zip file that you can send to Cisco TAC for troubleshooting. To find this page, select Services > Logs > System Information Capture.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Start date and time</td>
<td>Specify the time period during which you want to capture the system information. Defaults:</td>
</tr>
<tr>
<td>End date and time</td>
<td></td>
</tr>
<tr>
<td>Your name</td>
<td>Contact information that Cisco TAC can use to reach you.</td>
</tr>
<tr>
<td>Your phone number</td>
<td></td>
</tr>
<tr>
<td>Your e-mail address</td>
<td></td>
</tr>
<tr>
<td>Event scenario</td>
<td>Information to help Cisco TAC understand and troubleshoot the problem.</td>
</tr>
<tr>
<td>Observed results</td>
<td></td>
</tr>
<tr>
<td>Expected results</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics

- Obtaining and Viewing the System Information Capture (Infocap) Log in the Using Alarms and Logs on Cisco Unified MeetingPlace module
System Logs Page

To find this page, select Services > Logs > View System Logs, and select View Logs.

Note These fields appear only when your system has data for the parameters you entered.

Table 52 Field Reference: System Logs Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Date</td>
<td>The date on which the event occurred.</td>
</tr>
<tr>
<td>Time</td>
<td>The time at which the event occurred.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity of the event. Can be INFO, WARN, MIN, or MAJ.</td>
</tr>
<tr>
<td>Ex</td>
<td>Exception code.</td>
</tr>
<tr>
<td>Note</td>
<td>A value of 0 means that no exception code is defined for this event.</td>
</tr>
<tr>
<td>File</td>
<td>The name of the file in which the event occurred.</td>
</tr>
<tr>
<td>Line</td>
<td>The line in the file on which the event occurred.</td>
</tr>
<tr>
<td>SCodes</td>
<td>Context-specific values that are reported along with the exception code.</td>
</tr>
<tr>
<td>Note</td>
<td>For events with undefined exception codes, these values are used as the description.</td>
</tr>
<tr>
<td>Description</td>
<td>Description of the event.</td>
</tr>
</tbody>
</table>

Related Topics

- Viewing the System Log in the Using Alarms and Logs on Cisco Unified MeetingPlace module
- View System Logs Page, page 91

System Status Details Page

To find this page, select Services > System Status, and select View Status.

Table 53 Field Reference: System Status Details Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>General</td>
<td>The current loading status of the Cisco Unified MeetingPlace software. One of the following: up, down, shutting down, loading, coming up, and unloaded.</td>
</tr>
<tr>
<td>System mode</td>
<td>The current loading status of the Cisco Unified MeetingPlace software. One of the following: up, down, shutting down, loading, coming up, and unloaded.</td>
</tr>
<tr>
<td>Temperature</td>
<td>The temperature (in degrees Celsius) as measured on the MSC card inside the cabinet.</td>
</tr>
<tr>
<td>Note</td>
<td>Until the Cisco Unified MeetingPlace system is up, the temperature reads “Unknown.” Once the system is up, the temperature reads correctly.</td>
</tr>
<tr>
<td>Power supply</td>
<td>Displays either “OK” or displays a count of the times the voltage was out of tolerance.</td>
</tr>
</tbody>
</table>
Table 53  Field Reference: System Status Details Page (continued)

<table>
<thead>
<tr>
<th>Field Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server name</td>
<td>The name of the server.</td>
</tr>
<tr>
<td>Unit</td>
<td>Always set to 0 to identify the Application Server.</td>
</tr>
<tr>
<td>Class</td>
<td>The class name.</td>
</tr>
<tr>
<td>Mailbox</td>
<td>The number of the mailbox. This is a hexadecimal number.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Mailbox Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mailbox name</td>
<td>The name of the mailbox.</td>
</tr>
<tr>
<td>Unit</td>
<td>This is always set to 0.</td>
</tr>
<tr>
<td>Mailbox</td>
<td>The number of the mailbox. This is a hexadecimal number.</td>
</tr>
<tr>
<td>Messages</td>
<td><em>For internal use only.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Connection Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Conn ID</td>
<td><em>For internal use only.</em></td>
</tr>
<tr>
<td>Unit</td>
<td>This is always set to 0.</td>
</tr>
<tr>
<td>Creator MB</td>
<td><em>For internal use only.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Module Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Module name</td>
<td>The name of the software module.</td>
</tr>
<tr>
<td>CLS</td>
<td>The number of the software module. See “Module Numbers” in the Using Alarms and Logs on Cisco Unified MeetingPlace module.</td>
</tr>
<tr>
<td>Status</td>
<td>Status of the module. One of the following: up, down, starting, going down, exiting, or gone.</td>
</tr>
<tr>
<td>PID</td>
<td><em>For internal use only.</em></td>
</tr>
<tr>
<td>UID</td>
<td>Username used to log in to Cisco Unified MeetingPlace from a workstation (not from a phone).</td>
</tr>
<tr>
<td>Exit</td>
<td><em>For internal use only.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Unit Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unit</td>
<td><em>For internal use only.</em></td>
</tr>
<tr>
<td>Site</td>
<td><em>For internal use only.</em></td>
</tr>
<tr>
<td>Status</td>
<td><em>For internal use only.</em></td>
</tr>
<tr>
<td>Run level</td>
<td><em>For internal use only.</em></td>
</tr>
<tr>
<td>Unit kind</td>
<td><em>For internal use only.</em></td>
</tr>
<tr>
<td>Last attach</td>
<td><em>For internal use only.</em></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CPU Information</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CPU usage</td>
<td><em>For internal use only.</em></td>
</tr>
</tbody>
</table>

Related Topics
- Viewing the Current Status of the System in the Administration Center in the Using Alarms and Logs on Cisco Unified MeetingPlace module
Unattended Ports Report Page

Use this report to see what percentage of scheduled ports were not used during a specified time range. The output can help you determine the appropriate settings for your overbook and floater ports.

- Field Reference: Unattended Ports Report Page
- Output Reference: Unattended Ports Report

To find this page, select Reports > Unattended Ports Report.

Table 54  Field Reference: Unattended Ports Report Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>Select an output option. The File option uses the Portable Network Graphics (PNG) format. Default: Screen</td>
</tr>
<tr>
<td>Date</td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
<tr>
<td>Start time</td>
<td>The hour you want the port utilization report data to begin. Default: 8:00 AM</td>
</tr>
<tr>
<td>End time</td>
<td>The hour you want the port utilization report data to end. Default: 5:00 PM</td>
</tr>
<tr>
<td>Conference type</td>
<td>Whether you want report data about voice, web, or video meetings. Default: Voice</td>
</tr>
</tbody>
</table>

Output Reference: Unattended Ports Report

The report output is a chart that shows the following information:

- Date and times represented by the report.
- Number of licensed ports on the system for the selected Conference type.
- Unattended Ports (red data)—Percentage of scheduled ports that exceeded the actual number of meeting participants.
- No Show Ports (blue data)—Percentage of scheduled ports for meetings that never took place
- Average percentage of unused scheduled ports during the specified time range.

Related Topics
- Running Reports and Exporting Data from Cisco Unified MeetingPlace module
# Usage Configuration Page

To find this page, select **System Configuration > Usage Configuration**.

## Table 55  Field Reference: Usage Configuration Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Usage Configuration</strong></td>
<td><strong>Description</strong></td>
</tr>
<tr>
<td>Attendant phone</td>
<td>Phone number that callers are routed to if they do not press a number at a voice prompt or press 0 for operator assistance. †</td>
</tr>
<tr>
<td></td>
<td><strong>Tip</strong> Make sure that the people at this phone number are available and trained to provide assistance for Cisco Unified MeetingPlace.</td>
</tr>
<tr>
<td></td>
<td><strong>Restriction:</strong> The + character is allowed only as the first character in the field.</td>
</tr>
<tr>
<td>24-hour time</td>
<td>Whether to show meeting times by a 24-hour clock.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> No</td>
</tr>
<tr>
<td>Dial attendant on timeout</td>
<td>Whether callers are transferred to the attendant in the following situations:</td>
</tr>
<tr>
<td></td>
<td>• Caller dials 0 for operator assistance.</td>
</tr>
<tr>
<td></td>
<td>• Caller does not enter a number at a voice prompt.</td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> No</td>
</tr>
<tr>
<td>Language 1</td>
<td>Enabled languages. The Language 1 field sets the default system-wide language.</td>
</tr>
<tr>
<td>Language 2</td>
<td>• If the languages license is installed, then the number of active language fields (up to four fields) is determined by the number of installed languages.</td>
</tr>
<tr>
<td>Language 3</td>
<td>• If the languages license is not installed, then only the Language 1 field appears.</td>
</tr>
<tr>
<td>Language 4</td>
<td><strong>Default:</strong> English (US)</td>
</tr>
<tr>
<td>Guests can lock and record meetings</td>
<td>If set to No, then guest users cannot lock or record meetings.</td>
</tr>
<tr>
<td></td>
<td>If set to Yes:</td>
</tr>
<tr>
<td></td>
<td>• Guests can lock meetings.</td>
</tr>
<tr>
<td></td>
<td>• If the Can record meetings field in the preconfigured Guest Profile is also set to Yes, then guests can use the TUI to start and stop the meeting recording. Guests cannot start and stop recordings from the web meeting room, because only meeting moderators may do so.</td>
</tr>
<tr>
<td>Route calls to meeting ID that matches DID</td>
<td>Whether to enable the DID² feature, which routes incoming calls directly to meetings based on DID and DNIS³. When the DID feature is enabled, the caller is routed to the meeting ID that is equal to the DID phone number.</td>
</tr>
<tr>
<td></td>
<td><strong>See the Configuring Direct Inward Dial for Cisco Unified MeetingPlace module.</strong></td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td><strong>Number of numeric characters required in the Profile password for each user.</strong></td>
</tr>
<tr>
<td>Minimum profile password length</td>
<td><strong>Restriction:</strong> This field does not apply to Directory Service users. <strong>See the Configuring Cisco Unified MeetingPlace Directory Service module.</strong></td>
</tr>
<tr>
<td></td>
<td><strong>Default:</strong> 5</td>
</tr>
</tbody>
</table>
### Table 55: Field Reference: Usage Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Change profile password (days)</td>
<td>Frequency, in days, at which the Profile password must be changed in each user profile. A value of 0 means that the Profile password never needs to change. Restriction: This field does not apply to Directory Service users. See the Configuring Cisco Unified MeetingPlace Directory Service module. Default: 90</td>
</tr>
<tr>
<td>Minimum user password length</td>
<td>Number of alphanumeric characters required in the User password for each user. Restriction: This field does not apply to Directory Service users. See the Configuring Cisco Unified MeetingPlace Directory Service module. Default: 5</td>
</tr>
<tr>
<td>Change user password (days)</td>
<td>Frequency, in days, at which the User password must be changed in each user profile. A value of 0 means that the User password never needs to change. Restriction: This field does not apply to Directory Service users. See the Configuring Cisco Unified MeetingPlace Directory Service module. Default: 90</td>
</tr>
<tr>
<td>Maximum profile login attempts</td>
<td>Number of times that a user may try to: • Sign in to Cisco Unified MeetingPlace before the user profile is locked. • Enter a meeting password before the call is transferred to the attendant. If no attendant is available, then the call is disconnected. • Enter a Profile PIN to start a reservationless meeting from the TUI before the user profile is locked. A value of 0 means that there is no limit to the number of attempts. Before reaching the maximum number of login attempts, the user may restart the counter by taking one of the following actions: • Close the browser and open a new one. • End the call to Cisco Unified MeetingPlace and begin a new call. Restriction: Preconfigured user profiles cannot be locked. Default: 3</td>
</tr>
<tr>
<td>User locked interval</td>
<td>The amount of time for which a user profile stays locked. A value of 0 means the user profile stays locked until the System administrator unlocks it. Default: 0</td>
</tr>
</tbody>
</table>

### Click-to-Attend Link Configuration

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>External web server hostname</td>
<td>FQDN(^4) of the Web Server in the DMZ(^5). Example: meetings.example.com</td>
</tr>
<tr>
<td>Internal web server hostname</td>
<td>FQDN of the Web Server on the intranet. Example: meetingsint.example.com</td>
</tr>
</tbody>
</table>
### SSL enabled on external web server
Determines whether the click-to-attend URLs begin with “https” or “http”.
For information about configuring SSL on the Web Servers, see the Configuring Cisco Unified MeetingPlace Web Conferencing Security Features module.

### SSL enabled on internal web server

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Label for access phone number 1 | Text used to describe the first meeting access phone number that is displayed in the following places:  
  - E-mail notifications  
  - Telephone pop-up notification box in the full web meeting room  
  - Cisco Unified IP Phone screens (only when subscribed to the Cisco Unified MeetingPlace service for the PhoneView.)  
  Example: “Dial-In”  
  Restrictions:  
  - Changes to this field take effect only after restarting the system.  
  - (For full web meeting rooms only) See “Restrictions for Access Phone Numbers and Notification Labels” in the Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace module. |
| Access phone number 1         | First meeting access phone number.  
  Restrictions:  
  - Changes to this field take effect only after restarting the system.  
  - (For Find Me feature with pagers only) Only the characters 0-9, #, and * are processed and sent to pagers at the start of a meeting. See the “About the Find Me Feature” section on page 2.  
  - The + character is allowed only as the first character in the field. |
| Label for access phone number 2 | Text used to describe the second meeting access phone number.  
  Example: “Toll-Free”  
  Restrictions:  
  - Changes to this field take effect only after restarting the system.  
  - (For full web meeting rooms only) See “Restrictions for Access Phone Numbers and Notification Labels” in the Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace module. |
| Access phone number 2         | Second meeting access phone number.  
  Restrictions:  
  - Changes to this field take effect only after restarting the system.  
  - The + character is allowed only as the first character in the field. |
### Table 55  Field Reference: Usage Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Label for access phone number 3            | Text used to describe the third meeting access phone number. Example: “Internal” Restrictions:  
  • Changes to this field take effect only after restarting the system.  
  • (For full web meeting rooms only) See “Restrictions for Access Phone Numbers and Notification Labels” in the Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace module. |
| Access phone number 3                      | Third meeting access phone number. Restrictions:  
  • Changes to this field take effect only after restarting the system.  
  • The + character is allowed only as the first character in the field. |
| Label for access phone number 4            | Text used to describe the fourth meeting access phone number. Example: “International” Restrictions:  
  • Changes to this field take effect only after restarting the system.  
  • (For full web meeting rooms only) See “Restrictions for Access Phone Numbers and Notification Labels” in the Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace module. |
| Access phone number 4                      | Fourth meeting access phone number. Restrictions:  
  • Changes to this field take effect only after restarting the system.  
  • The + character is allowed only as the first character in the field. |

**Reservationless Meetings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enable reservationless meetings</td>
<td>Whether reservationless meetings are enabled on the system. Default: Yes</td>
</tr>
</tbody>
</table>
| Allow any profiled user to initiate        | Whether any profiled user can start a reservationless meeting from the TUI before the meeting owner joins:  
  • No—Profiled users cannot start a reservationless meeting before the meeting owner joins.  
  • Yes, by pressing 3—Profiled users can start a reservationless meeting from the TUI by pressing 3.  
  • Yes, by joining—Profiled users can start a reservationless meeting by joining the meeting. Default: Yes, by pressing 3 |
### Field Reference: Usage Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Bill initiator</td>
<td>Who gets billed for each reservationless meeting:</td>
</tr>
<tr>
<td></td>
<td>• Yes—Bill the user who starts the meeting.</td>
</tr>
<tr>
<td></td>
<td>• No—Bill the meeting owner.</td>
</tr>
<tr>
<td></td>
<td>Restriction: This field is always set to No when the Allow any profiled user to initiate field is set to No.</td>
</tr>
<tr>
<td></td>
<td>Default: Yes</td>
</tr>
<tr>
<td>TUI menu is reservationless only</td>
<td>Whether users can schedule meetings or only start reservationless meetings from the TUI.</td>
</tr>
<tr>
<td></td>
<td>Default: No</td>
</tr>
<tr>
<td>Owner can press 2 in TUI to initiate</td>
<td>Whether meeting owners can initiate reservationless meetings more quickly by skipping the Profile number entry.</td>
</tr>
<tr>
<td></td>
<td>• Yes—Meeting owner can start a reservationless meeting from the TUI waiting room by pressing 2 and entering the Profile password.</td>
</tr>
<tr>
<td></td>
<td>• No—Meeting owner starts the reservationless meeting from the TUI waiting room by pressing 3 and entering both the Profile number and Profile password.</td>
</tr>
<tr>
<td></td>
<td>If the Allow any profiled user to initiate field is set to Yes, then any profiled user may press 3 to start the reservationless meeting with both the Profile number and Profile password.</td>
</tr>
<tr>
<td></td>
<td>Default: No</td>
</tr>
</tbody>
</table>

#### Alarms

| Call capacity MINOR alarm (in percentage) | Specify the percentage of call capacity that triggers a minor and major alarm. |
| Call capacity MAJOR alarm (in percentage) | You can configure minor alarms to be triggered when call capacity is 30–100 percent. You can configure major alarms to be triggered when call capacity is 91–100 percent. The call capacity percentage for a major alarm must be greater than the percentage for a minor alarm. |
| Call out on major alarm                  | Whether the system places a call to the specified phone number if an error condition affects system operation. |
| Phone number to call on alarm            | Recommendation: Yes                                                         |
|                                        | Restriction: The + character is allowed only as the first character in the field. |
|                                        | Default: No                                                                 |

#### Outdial Meetings

<table>
<thead>
<tr>
<th>Number of retry attempts</th>
<th>Number of times the system tries to call each person, when dial out is enabled for a meeting. This setting also determines the number of times the system goes through the Find Me sequence for each user.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Default: 2</td>
</tr>
<tr>
<td>Delay between retries (sec)</td>
<td>Number of seconds between dial-out retries. This setting also determines the number of seconds between each set of Find Me calls. Restriction: The actual time between dial-out attempts may be longer due to network delays.</td>
</tr>
<tr>
<td></td>
<td>Default: 300</td>
</tr>
</tbody>
</table>
### Table 55  Field Reference: Usage Configuration Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Pager Settings</strong></td>
<td></td>
</tr>
</tbody>
</table>
| Prefix string                              | Number string required by certain paging services in some counties. Cisco Unified MeetingPlace adds this string at beginning of all pages.  
Keep this field blank if users' paging services do not require prefix string.  
Supported characters: 0, 1, 2, 3, #, and *                                                                                                                                                                                                                                  |
| Suffix string                              | Number string required by certain paging services in some counties. Cisco Unified MeetingPlace adds this string at the end of all pages.  
Keep this field blank if users' paging services do not require suffix string.  
Supported characters: 0, 1, 2, 3, #, and *                                                                                                                                                                                                                                  |
| **Attendant Privileges**                   |                                                                                                                                                                                                                                                                                                                                          |
| Create user profiles and user groups       | Whether attendants can create, delete, edit, lock, and unlock user profiles and user groups from the Administration Center and MeetingPlace Conference Manager.  
Default: Yes                                                                                                                                                                                                                                                                 |
| Delete user profiles and user groups       |                                                                                                                                                                                                                                                                                                                                          |
| Modify user profiles and user groups       |                                                                                                                                                                                                                                                                                                                                          |
| Lock and unlock user profiles              |                                                                                                                                                                                                                                                                                                                                          |
| Run reports                                | Whether attendants can run and view formatted reports in the Administration Center.  
Default: No                                                                                                                                                                                                                                                                                                                      |
| View alarms                                | Whether attendants can view alarms from the Administration Center.  
Default: No                                                                                                                                                                                                                                                                                                                      |
| End meetings                               | Whether attendants can end meetings from MeetingPlace Conference Manager and the Cisco Unified MeetingPlace end-user web interface.  
Default: Yes                                                                                                                                                                                                                                                                                                                      |
| **Password Complexity Checks**             |                                                                                                                                                                                                                                                                                                                                          |
| Password contains characters from at least three classes | Whether each new or modified User password must contain characters from at least three of the following character classes:  
- lowercase letters  
- uppercase letters  
- digits  
- special characters  
Default: No                                                                                                                                                                                                                                                                                   |
| No character in the new password repeated more than three times | Whether each new or modified User password is restricted from containing a character that is repeated more than three times consecutively.  
Default: No                                                                                                                                                                                                                                                                             |
| Password does not repeat or reverse the user name | Whether each new or modified User password is restricted from being a repeat or the reverse of the User ID.  
Default: No                                                                                                                                                                                                                                                                                     |
### Related Topics

- Configuring Access Phone Numbers and Notification Labels for Cisco Unified MeetingPlace module
- Configuring Languages for Cisco Unified MeetingPlace module
- Configuring Meetings for Cisco Unified MeetingPlace module
- Configuring Recordings for Cisco Unified MeetingPlace module
- Configuring E-Mail Notifications for Cisco Unified MeetingPlace module
- Configuring Attendant Settings for Cisco Unified MeetingPlace module
- Configuring Call Control for Cisco Unified MeetingPlace module
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace module
- Securing the Cisco Unified MeetingPlace System module

### User Configuration Page

Use this page to perform the following tasks:

- Configuring User Profiles and User Groups for Cisco Unified MeetingPlace module
- Adding or Editing a Video Terminal Profile in the Configuring Endpoints for Cisco Unified MeetingPlace module
- Changing the User Status in Cisco Unified MeetingPlace User Profiles module
- Configuring Cisco Unified MeetingPlace Directory Service module
# User Groups Page

To find this page, select **User Configuration > User Groups**. By default, this page displays user groups sorted by group name in ascending order.

## Table 56  
**Navigation Reference: User Groups Page**

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort by group name, group number, or active status</td>
<td>Select the relevant column heading.</td>
</tr>
<tr>
<td></td>
<td>Restriction: The system sorts entries as text strings. For example, if you sort by number, the system lists 10 as a lower number than 2.</td>
</tr>
<tr>
<td>Change the sort order to ascending or descending</td>
<td>Select the column heading to display an arrow. Select the arrow to toggle between a down arrow (ascending sort) and an up arrow (descending sort).</td>
</tr>
<tr>
<td></td>
<td>Restriction: The system sorts entries as text strings. For example, if you sort by number, the system lists 10 as a lower number than 2.</td>
</tr>
<tr>
<td>Display a shorter or longer list of user groups in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the number of user groups to display.</td>
</tr>
<tr>
<td>Display a different page of user groups</td>
<td>At the bottom of the page, perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• In the Go field, enter the page number to display, and select <strong>Go</strong>.</td>
</tr>
<tr>
<td></td>
<td>• Click the arrows to page through the list.</td>
</tr>
<tr>
<td>Create a new user group</td>
<td>Select <strong>Add New</strong>.</td>
</tr>
<tr>
<td>Delete user groups</td>
<td>Check the appropriate check boxes in the far left column, then select <strong>Delete Selected</strong>.</td>
</tr>
<tr>
<td></td>
<td>Restriction: The preconfigured System user group cannot be deleted.</td>
</tr>
</tbody>
</table>

## Related Topics
- [Configuring User Profiles and User Groups for Cisco Unified MeetingPlace](#) module
- [Add User Group Page](#) page 4
User Profiles Page

To find this page, select **User Configuration > User Profiles**. By default, this page displays user profiles sorted by username in ascending order.

### Table 57 Navigation Reference: User Profiles Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
</table>
| Sort by username, profile number, or name | Select the relevant column heading.  
Restriction: The system sorts entries as text strings. For example, if you sort by number, the system lists 10 as a lower number than 2. |
| Change the sort order to ascending or descending | Select the column heading to display an arrow. Select the arrow to toggle between a down arrow (ascending sort) and an up arrow (descending sort).  
Restriction: The system sorts entries as text strings. For example, if you sort by number, the system lists 10 as a lower number than 2. |
| Display a shorter or longer list of user profiles in one view | At the bottom of the page, in the Rows per page field, select the number of user profiles to display. |
| Display a different page of user profiles | At the bottom of the page, perform one of the following actions:  
- In the Go field, enter the page number to display, and select **Go**.  
- Click the arrows to page through the list. |
| Search by username | Select the **User ID** radio button, enter the first characters of the username, and select **Search**. |
| Search by first or last name | Select the **Name** radio button, enter at least the first character of the first name or last name, and select **Search**. |
| Edit an existing user profile | Select **Edit** in the same row as the user profile. |
| Create a new user profile | Select **Add New**. |
| Delete one or more user profiles | Check the appropriate check boxes in the far left column, then select **Delete Selected**.  
Restriction: The preconfigured admin and guest profiles cannot be deleted. |

**Related Topics**
- **Configuring User Profiles and User Groups for Cisco Unified MeetingPlace** module  
- **Add User Profile Page**, page 6
# Video Terminal Profiles Page

To find this page, select User Configuration > Video Terminal Profiles. By default, this page displays video terminal profiles (VTPs) sorted by VTP name in ascending order.

## Table 58: Navigation Reference: Video Terminal Profiles Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sort by VTP name or endpoint E.164 number.</td>
<td>Select the column heading.</td>
</tr>
<tr>
<td></td>
<td>Restriction: The system sorts entries as text strings. For example, if</td>
</tr>
<tr>
<td></td>
<td>you sort by number, the system lists 10 as a lower number than 2.</td>
</tr>
<tr>
<td>Change the sort order to ascending or descending</td>
<td>Select the column heading to display an arrow. Select the arrow to</td>
</tr>
<tr>
<td></td>
<td>toggle between a down arrow (ascending sort) and an up arrow (descending</td>
</tr>
<tr>
<td></td>
<td>sort).</td>
</tr>
<tr>
<td></td>
<td>Restriction: The system sorts entries as text strings. For example, if</td>
</tr>
<tr>
<td></td>
<td>you sort by number, the system lists 10 as a lower number than 2.</td>
</tr>
<tr>
<td>Display a shorter or longer list of entries in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the</td>
</tr>
<tr>
<td></td>
<td>number of user profiles to display.</td>
</tr>
<tr>
<td>Display a different page</td>
<td>At the bottom of the page, perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• In the Go field, enter the page number to display, and select Go.</td>
</tr>
<tr>
<td></td>
<td>• Click the arrows to page through the list.</td>
</tr>
<tr>
<td>Search by VTP name</td>
<td>Select the VTP Name radio button, enter the first characters of the</td>
</tr>
<tr>
<td></td>
<td>name, and select Search.</td>
</tr>
<tr>
<td>Search by E.164 number</td>
<td>Select the Endpoint E.164 number radio button, enter digits, and select</td>
</tr>
<tr>
<td></td>
<td>Search.</td>
</tr>
<tr>
<td>Edit an existing VTP</td>
<td>Select Edit in the same row as the VTP.</td>
</tr>
<tr>
<td>Create a new VTP</td>
<td>Select Add New.</td>
</tr>
<tr>
<td>Delete one or more VTP</td>
<td>Check the appropriate check boxes in the far left column, then select</td>
</tr>
<tr>
<td></td>
<td>Delete Selected.</td>
</tr>
</tbody>
</table>

## Related Topics

- Adding or Editing a Video Terminal Profile in the Configuring Endpoints for Cisco Unified MeetingPlace module
- Add Video Terminal Profile Page, page 23
View Locked Profiles Page

This page displays the user profiles that are locked. For locked user profiles that belong to user groups, the group defaults for active and inactive status are also displayed. To find this page, select User Configuration > Locked Profiles.

Table 59  Navigation Reference: View Locked Profiles Page

<table>
<thead>
<tr>
<th>To</th>
<th>Do This</th>
</tr>
</thead>
<tbody>
<tr>
<td>Set locked user profiles to active state</td>
<td>Check the appropriate check boxes in the far left column, then select Set Selected to Active.</td>
</tr>
<tr>
<td>Set locked user profiles to inactive state</td>
<td>Check the appropriate check boxes in the far left column, then select Set Selected to Inactive.</td>
</tr>
<tr>
<td>Display a shorter or longer list of locked user profiles in one view</td>
<td>At the bottom of the page, in the Rows per page field, select the number of user profiles to display.</td>
</tr>
<tr>
<td>Display a different page of locked user profiles</td>
<td>At the bottom of the page, perform one of the following actions:</td>
</tr>
<tr>
<td></td>
<td>• In the Go field, enter the page number to display, and select Go.</td>
</tr>
<tr>
<td></td>
<td>• Click the arrows to page through the list.</td>
</tr>
</tbody>
</table>

Related Topics

- Changing the User Status in Cisco Unified MeetingPlace User Profiles module

View System Information Capture Page

Note  This information applies only to Release 7.0.1. In Release 7.0.2 and later, this page was replaced by the System Information Capture Page.

Running this log generates a very large zip file that you can send to Cisco TAC for troubleshooting. To find this page, select Services > Logs > View System Information Capture.

Table 60  Field Reference: View System Information Capture Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event date</td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
<tr>
<td>Approximate event time</td>
<td>The approximate hour and minute of the event for which you want system information. Default: current time</td>
</tr>
<tr>
<td>Log capture window</td>
<td>The number of minutes before and after the approximate event time for which you want system information. Default: 60</td>
</tr>
</tbody>
</table>
Table 60  Field Reference: View System Information Capture Page (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name of person to contact</td>
<td>Contact information that Cisco TAC can use to reach you.</td>
</tr>
<tr>
<td>Phone number of person to contact</td>
<td></td>
</tr>
<tr>
<td>E-mail address of person to contact</td>
<td></td>
</tr>
<tr>
<td>Event scenario</td>
<td>Information to help Cisco TAC understand and troubleshoot the problem.</td>
</tr>
<tr>
<td>Observed results</td>
<td></td>
</tr>
<tr>
<td>Expected results</td>
<td></td>
</tr>
</tbody>
</table>

Related Topics
- Obtaining and Viewing the System Information Capture (Infocap) Log in the Using Alarms and Logs on Cisco Unified MeetingPlace module

View System Logs Page

To find this page, select Services > Logs > View System Logs. The output is displayed on the System Logs Page.

Table 61  Field Reference: View System Logs Page

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Severity level</td>
<td>For normal operations, select minor, which provides a list of all log entries, or information, which lists everything. Default: major</td>
</tr>
<tr>
<td>Sort by date</td>
<td>Whether to list the oldest or newest messages first.</td>
</tr>
<tr>
<td>Note</td>
<td>The system sorts messages by using the date and time that each message was added to the log file. If time is not synchronized across all Cisco Unified MeetingPlace servers, then the time used for sorting may differ from the displayed time stamps, and the log messages may seem to appear out of order. The time stamp for each message is used by the system to filter out messages that are outside the specified start and end dates. Default: Sort by date descending</td>
</tr>
<tr>
<td>Start date</td>
<td>Default: yesterday (mm/dd/yyyy)</td>
</tr>
<tr>
<td>End date</td>
<td>Default: today (mm/dd/yyyy)</td>
</tr>
<tr>
<td>Module</td>
<td>The number of the software module whose log messages you want to see. See “Module Numbers” in the Using Alarms and Logs on Cisco Unified MeetingPlace module. Default: 0</td>
</tr>
<tr>
<td>Unit</td>
<td>Number used by the Cisco Unified MeetingPlace Gateway System Integrity Manager (Gateway SIM) to identify the server. Default: 0 (Application Server)</td>
</tr>
<tr>
<td>Rows per page</td>
<td>Default: 20</td>
</tr>
</tbody>
</table>
Related Topics
- Viewing the System Log in the Using Alarms and Logs on Cisco Unified MeetingPlace module
- System Logs Page, page 77
- Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module

Web Servers Page

To find this page, select System Configuration > Web Servers. Use this page to:
- Configure the Gateway SIM connections between the Application Server and the Web Servers.
- Add links to the Web Server from the Administration Center. The links appear in a drop-down menu at the top of each Administration Center page.

This page is automatically populated with Web Servers that were successfully registered to the Application Server by Gateway SIM. To add or edit an entry, select the text in any entry row.

Related Topics
- Edit Web Server Page, page 44
- Connecting the Cisco Unified MeetingPlace Application Server to a Web Server module
- Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module
Field Reference: Web Server Specific Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Server Name</td>
<td>The name assigned to this Web Server.</td>
</tr>
<tr>
<td></td>
<td>This field was populated during the Cisco Unified MeetingPlace Web Conferencing installation.</td>
</tr>
<tr>
<td>Hostname [Home Page]</td>
<td>A unique hostname, FQDN, or IP address used to connect to the Cisco Unified MeetingPlace home page.</td>
</tr>
<tr>
<td></td>
<td>This field was populated during the Cisco Unified MeetingPlace Web Conferencing installation with the first IP address assigned in the Operating System.</td>
</tr>
<tr>
<td></td>
<td>- If this field contains just the hostname of your web server, we recommend that you change it to the FQDN, that is, hostname.domain.com. If your web server is not in a Domain Name System (DNS), insert the IP address instead.</td>
</tr>
<tr>
<td></td>
<td>- Do not set this parameter to the same value as the Hostname [Web Conferencing].</td>
</tr>
<tr>
<td></td>
<td>- To use SSL, you must change this value from the default IP address to either hostname or FQDN.</td>
</tr>
<tr>
<td></td>
<td>- Verify that intended users can resolve this hostname or IP address.</td>
</tr>
<tr>
<td></td>
<td>- Make sure that you can resolve the hostnames for Home Page and Web Conferencing on the Web Server computer. If the hostnames cannot be resolved by the DNS Server, these entries should be added to the local hosts file. Otherwise, users may experience trouble when trying to share attachments in the meeting room.</td>
</tr>
</tbody>
</table>
**Field Reference: Web Server Specific Fields**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hostname [Web Conferencing]</td>
<td>A unique hostname, FQDN, or IP address used to connect Flash clients to the Cisco Unified MeetingPlace meeting console. If this field contains just the hostname of your web server, we recommend that you change it to the FQDN, that is, hostname.domain.com. If your web server is not in a Domain Name System (DNS), insert the IP address instead. Do not set this parameter to the same value as the Hostname [Home Page]. To use SSL, you must change this value from the default IP address to either hostname or FQDN. Verify that intended users can resolve this hostname or IP address. Make sure that you can resolve the hostnames for Home Page and Web Conferencing on the web server computer. If the hostnames cannot be resolved by the DNS Server, these entries should be added to the local hosts file. Otherwise, users may experience trouble when trying to share attachments in the meeting room. Note You must restart the Cisco Unified MeetingPlace Web Conferencing services for changes to this field to take effect. Note When you restart the Web Server, all manual changes made to the registry are lost.</td>
</tr>
<tr>
<td>Require SSL</td>
<td>Whether this Web Server is configured for Secure Socket Layer (SSL) connections.</td>
</tr>
<tr>
<td>Trust Web Server Authentication</td>
<td>Whether this Web Server accepts authenticated Windows login information to automatically log in to Cisco Unified MeetingPlace.</td>
</tr>
</tbody>
</table>
Troubleshooting Tips

Entering an IP address for Hostname will prevent proper functionality of the Windows authentication feature. For further information about this issue and workarounds, see “How to Resolve Authentication Problems” in the Troubleshooting Cisco Unified MeetingPlace Web Conferencing module.

Related Topics
- Restarting All Web Conferencing Services in the Managing Cisco Unified MeetingPlace Web Conferencing Services module

Field Reference: Web Server Customization Values

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| Performance Tuning                        | Allows you to optimize your Web Server based on the number of potential concurrent web conferencing users (versus users who may not be using the conferencing portion, such as administrators who only schedule meetings).
| Note                                       | Setting this parameter to the highest level on a computer with inadequate hardware results in poor user performance.                                                                                          |
| Verbose Logging                            | Determines whether detailed entries will be logged to the Gateway SIM log.-------------------------------------------------------------------------------------------------------------------------------------|
|                                            | **Recommended** Select No to enhance performance. This is the default setting.                                                                                                                            |

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verbose Logging</td>
<td>Determines whether detailed entries will be logged to the Gateway SIM log.-------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td></td>
<td><strong>Recommended</strong> Select No to enhance performance. This is the default setting.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>--------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Allow Profile Access</td>
<td>Determines whether users see the Account link on the Cisco Unified MeetingPlace Web Conferencing home page. The Account link provides users with access to their profile information.</td>
</tr>
<tr>
<td>Allow Admission of External Participants</td>
<td>Determines whether this Web Server allows users with appropriate meeting console permissions to escalate a meeting in progress from the internal Web Server to an external Web Server to allow external participants to join.</td>
</tr>
<tr>
<td>Allow Chat In Meeting Console</td>
<td>Determines whether the chat window is available in the meeting console.</td>
</tr>
<tr>
<td>Allow Show Moderator Cursors</td>
<td>Determines whether users will see cursors when moderators move their mouse during a meeting.</td>
</tr>
<tr>
<td>Allow Public Meetings in Find Meeting List</td>
<td>Determines whether public meetings are listed when users use the Find Meetings search engine. If you select No, the search engine displays only the meetings scheduled by the searcher or meetings that the searcher has been invited to by profile.</td>
</tr>
<tr>
<td></td>
<td><strong>Default</strong> Yes.</td>
</tr>
<tr>
<td>Allow Guest Access to Find Meetings Page</td>
<td>Determines whether guest users (that is, users who do not have Cisco Unified MeetingPlace profiles) have access to the Find Meetings page.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> To make sure that guest users can use the Find Meetings feature, set both the Allow Public Meetings in Find Meeting List and Allow Guest Access to Find Meetings Page parameters to Yes.</td>
</tr>
</tbody>
</table>
### Field Reference: Site Configuration Page

**Note**  
WebConnect is not supported in this release of Cisco Unified MeetingPlace.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Allow Remember Me</strong></td>
<td>Determines whether the Remember Me check box displays on the Cisco Unified MeetingPlace Sign In page. Remember Me stores user passwords as a cookie for future web conferencing sessions.</td>
</tr>
<tr>
<td><strong>Remember Me Expiration Interval (Days)</strong></td>
<td>Specifies the number of days Remember Me is valid. If you enter 0, Remember Me never expires. Default 90</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Site Name</strong></td>
<td>The name of the chosen site.</td>
</tr>
<tr>
<td><strong>Dedicated External</strong></td>
<td>Whether this site is a Hosted Service.</td>
</tr>
<tr>
<td><strong>Primary Web Server</strong></td>
<td>This feature is part of WebConnect and is not supported in this release.</td>
</tr>
<tr>
<td><strong>Contact Phone Number</strong></td>
<td>The phone number assigned for this site. If this field is blank, enter the phone number.</td>
</tr>
<tr>
<td><strong>Warn before Rolling onto Site</strong></td>
<td>This feature is part of WebConnect and is not supported in this release.</td>
</tr>
<tr>
<td><strong>Site Included in Image</strong></td>
<td>This feature is part of WebConnect and is not supported in this release.</td>
</tr>
<tr>
<td><strong>Roll on Meeting ID Conflict</strong></td>
<td>This feature is part of WebConnect and is not supported in this release.</td>
</tr>
<tr>
<td><strong>DMZ Web Server</strong></td>
<td>Indicates the external Web Server assigned to this site. If there is not an external Web Server assigned to this site, this field is blank.</td>
</tr>
<tr>
<td><strong>Internal Web Server</strong></td>
<td>Indicates which Web Server in this site is designated as the entry point for all dedicated internal rollover traffic.</td>
</tr>
<tr>
<td><strong>Load Stats Poll Period (Seconds)</strong></td>
<td>Indicates how often the Web Server is polled for its current load index.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>The default is 60 seconds.</td>
</tr>
</tbody>
</table>
## Counters Available in the Cisco Unified MeetingPlace Performance Object

For more information about how to save or record performance graphs, see the Microsoft website.

<table>
<thead>
<tr>
<th>Counter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>MPAgent: Total client connections in MPAgent</td>
<td>The number of client connections in the Cisco MeetingPlace Agent Service.</td>
</tr>
<tr>
<td>MPAudio: Total audio attachments converted by the audio service</td>
<td>The number of audio attachments converted by the audio service.</td>
</tr>
<tr>
<td>MPAudio: Total MP3 files converted by the audio service</td>
<td>The number of MP3 files converted by the audio service.</td>
</tr>
<tr>
<td>MPAudio: Total windows media files converted by the audio service</td>
<td>The number of Windows Media files converted by the audio service.</td>
</tr>
<tr>
<td>MPDatSvc: Total users pulled by the replication service</td>
<td>The number of users replicated to the SQL database.</td>
</tr>
<tr>
<td>MPDatSvc: Total groups pulled by the replication service</td>
<td>The number of user groups replicated to the SQL database.</td>
</tr>
<tr>
<td>MPDatSvc: Total meetings pulled by the replication service</td>
<td>The number of meetings replicated to the SQL database.</td>
</tr>
<tr>
<td>MPDatSvc: Total attachments pulled by the replication service</td>
<td>The number of attachments replicated to the SQL database.</td>
</tr>
<tr>
<td>MPDatSvc: Total confparts pulled by the replication service</td>
<td>The number of conference attendees replicated to the SQL database.</td>
</tr>
<tr>
<td>MPDatSvc: Total meeting categories pulled by the replication service</td>
<td>The number of meeting categories replicated to the SQL database.</td>
</tr>
<tr>
<td>MPDatSvc: Total size of attachments (KB) pulled by the replication service</td>
<td>The total size of attachments in KB replicated to the SQL database.</td>
</tr>
<tr>
<td>MPX: Active MPX Threads</td>
<td>The number of active threads in MPX, the ISAPI entry point.</td>
</tr>
<tr>
<td>MPX: Total queries to MPX</td>
<td>The total number of queries processed by MPX.</td>
</tr>
<tr>
<td>MPX: Total schedules</td>
<td>The total number of scheduling attempts made through MPX.</td>
</tr>
<tr>
<td>MPX: Total successful schedules</td>
<td>The total number of successful scheduling attempts made through MPX.</td>
</tr>
<tr>
<td>MPX: Total attends</td>
<td>The total number of attend attempts made through MPX.</td>
</tr>
<tr>
<td>MPX: Total successful attends</td>
<td>The total number of successful attends made through MPX.</td>
</tr>
<tr>
<td>MPX: Total 1st MtgStatusGetQS queries</td>
<td>The total number of times the meeting console loaded successfully.</td>
</tr>
<tr>
<td>MPX: Total rollover schedules</td>
<td>The total number of meeting rollover attempts.</td>
</tr>
<tr>
<td>MPX: Total successful rollover schedules</td>
<td>The total number of successful meeting rollovers.</td>
</tr>
<tr>
<td>MPX: Total server busy messages</td>
<td>The total number of server busy messages MPX returned to users.</td>
</tr>
<tr>
<td>Various FormType counters</td>
<td>FormType counters are web service API calls that facilitate internal tracking.</td>
</tr>
</tbody>
</table>
Related Topics

- Running the Windows Performance Monitoring Tool in the Monitoring and Maintaining Cisco Unified MeetingPlace Web Conferencing module
## Field Reference: Meeting Scheduling Page

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Subject</td>
<td>A short description that distinguishes your meeting in Search results and meeting confirmation pages for users. If no subject is specified, the last name of the meeting scheduler is used to populate this field.</td>
</tr>
</tbody>
</table>
| Meeting ID       | A number that allows the system to uniquely identify a meeting that is occurring at any particular time. The system can automatically assign meeting IDs, or you can assign a custom ID.  

**Note**

If you are scheduling two consecutive meetings with the same meeting ID, note that the second occurrence of the meeting (Meeting2) must be scheduled as follows: `Meeting2StartTime >= EndTimeMeeting1 + EndGuardTime + StartGuardTime`  

For information about guard times, see [here](#). |
| Start Time       | The time you want your meeting to start. This is based on your time zone setting.                                                             |
| Duration         | The duration of your meeting in minutes. The default maximum meeting length is 24 hours for voice meetings and 12 hours for web meetings. The minimum meeting length is 2 minutes. |
| On behalf of user| The user ID of the person for whom you are scheduling a meeting.  

**Note**

This field is available only to users who have Attendant or System Manager privileges. |
| Public           | When checked, this meeting will appear in the list of results when users use the Find Meeting feature on the end-user web interface. |
Field Reference: Meeting Recurrence Options

Parameter | Description
--- | ---
**Type** | Your meeting type.
  - Personal—A meeting associated with your profile number that you can start right away. In Cisco Unified MeetingPlace, this is also referred to as a reservationless meeting.
  - Regular—The default meeting type set by your system administrator.
  - Lecture-style—A meeting in which there is one or more Speakers. The majority of participants are Listeners and are only granted speaking privileges by the meeting moderator. This meeting type is usually meant for one-to-many meetings.
  - Reserve all ports—A meeting that reserves all ports so that a system administrator can schedule a maintenance window.
  
  **Note** (Cisco WebEx integration only) If you select Cisco WebEx as the Web conference provider, then you can only schedule Personal and Regular meetings.

**Category** | An optional parameter that allows you to set your meeting within a specified category of meetings (for example, all Sales meetings or Crisis meetings).
  
  **Note** This field is available only if your system administrator configured meeting categories.

**Password** | An optional password that you are setting for your meeting.
  
  If you choose to protect a meeting with a password, all invitees must enter this password to access your meeting. If you do not require password protection, leave this field blank.

**Billing code** | If your company uses bill-backs, this field contains the number that is used to identify the group or department that should be billed for this meeting.

**Audio ports** | The number of audio ports to reserve for the meeting.

**Enable video** | When checked, video is enabled for the meeting.

**Reserve video** | When checked, video ports (the same number as you specified in the Audio ports field) are reserved for the meeting.

**Recurrence** | Select the button to change the recurrence pattern.

**Web conference provider** | Choose between Cisco WebEx and Cisco Unified MeetingPlace Web Conferencing.
  
  **Note** This field appears only when Cisco Unified MeetingPlace is integrated with Cisco WebEx.

Field Reference: Meeting Recurrence Options

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Once</td>
<td>This is not a recurring meeting.</td>
</tr>
<tr>
<td>Daily</td>
<td>This meeting occurs at the same time every day, for a maximum of 200 days.</td>
</tr>
<tr>
<td>Weekly</td>
<td>This meeting occurs once per week at the same time and day of the week.</td>
</tr>
</tbody>
</table>
MeetingPlace Conference Manager References

Field Reference: Advanced Options

<table>
<thead>
<tr>
<th>Frequency</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monthly</td>
<td>This meeting occurs once per month on a particular date or day of the week.</td>
</tr>
<tr>
<td>Continuous</td>
<td>This meeting is always available. It has no end time or date. However, each instance of a continuous meeting is limited to 24 hours.</td>
</tr>
</tbody>
</table>

This field is available only for users with System Manager privileges.

**Note** You cannot invite video terminals to a continuous meeting. The system will return an error if you attempt to schedule a continuous meeting with invited video terminals. Video endpoints can attend continuous meetings, but only if unreserved ports are available.

**Field Reference: Advanced Options**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who can attend</td>
<td>Choose an option from the list to indicate who can attend the meeting:</td>
</tr>
<tr>
<td></td>
<td>• Anyone—The meeting is unrestricted. Both profiled users and guest users can attend.</td>
</tr>
<tr>
<td></td>
<td>• MeetingPlace Profile Users—All components of the meeting (audio, web, and video) are restricted to profile users who sign in by using their Cisco Unified MeetingPlace user ID and password.</td>
</tr>
<tr>
<td></td>
<td>• Invited Profile Users—All components of the meeting (audio, web, and video) are restricted to profile users who were invited to attend. All invited users must sign in by using their Cisco Unified MeetingPlace user ID and password.</td>
</tr>
<tr>
<td>Outdial on first join</td>
<td>Select to have the system dial out to all invitees after the first person joins the meeting.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> This feature is only available for system administrators who schedule continuous meetings.</td>
</tr>
<tr>
<td>Meeting entry mode</td>
<td>Choose what users will hear when they try to join the audio portion of your meetings.</td>
</tr>
<tr>
<td></td>
<td>• Echo meeting ID—The system repeats the meeting ID so that users can confirm their choice. When users first enter the meeting ID, their ID is repeated for confirmation. After users confirm the meeting ID, they are asked to record their names then placed in the meeting.</td>
</tr>
<tr>
<td></td>
<td>• Skip echo—The system skips the repeat of the meeting ID. When users first enter the meeting, users are asked to record their names then are placed in the meeting.</td>
</tr>
<tr>
<td></td>
<td>• Skip echo and name—The system skips the repeat of the meeting ID and recording. When users first enter the meeting ID, they are placed directly in the meeting without recording their names.</td>
</tr>
<tr>
<td>Entry announcement</td>
<td>Choose what users will hear when a new participant joins the meeting.</td>
</tr>
<tr>
<td></td>
<td>• Beep Only—A short beep is emitted during the meeting to indicate that someone has entered the meeting.</td>
</tr>
<tr>
<td></td>
<td>• Beep + Name—After a short beep, the recorded name of the participant is announced.</td>
</tr>
<tr>
<td></td>
<td>If you do not hear the name of a participant upon entry, the participant probably did not record a name before entering the meeting. Identify the participant before the meeting begins.</td>
</tr>
<tr>
<td></td>
<td>• None—There is no indication that someone has entered the meeting.</td>
</tr>
</tbody>
</table>
### Field Reference: Advanced Options

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exit announcement</td>
<td>Choose what users will hear when a participant leaves the meeting.</td>
</tr>
<tr>
<td></td>
<td>• Beep Only—A short beep is emitted during the meeting to indicate that someone has departed the meeting.</td>
</tr>
<tr>
<td></td>
<td>• Beep+ Name—After a short beep, the recorded name of the participant is announced.</td>
</tr>
<tr>
<td></td>
<td>If you do not hear the name of a participant upon departure, the participant probably did not record a name before entering the meeting.</td>
</tr>
<tr>
<td></td>
<td>• None—There is no indication that someone has departed the meeting.</td>
</tr>
<tr>
<td>Auto record</td>
<td>Indicates whether you want your meeting to be automatically recorded when the meeting starts.</td>
</tr>
<tr>
<td></td>
<td>Choose No if you want the option to manually start recording the meeting from the meeting room or from the telephone.</td>
</tr>
<tr>
<td><strong>Tip</strong></td>
<td>You can also press #61 on your phone to manually start recording during a meeting.</td>
</tr>
<tr>
<td>Send notifications</td>
<td>Check this option to have the system send notifications for the meeting.</td>
</tr>
<tr>
<td>Include attachments in</td>
<td>Check this option to include attachments with notifications.</td>
</tr>
<tr>
<td>notifications</td>
<td></td>
</tr>
<tr>
<td>Meeting change</td>
<td>Check this option to have the system send notifications if the meeting is updated or rescheduled.</td>
</tr>
<tr>
<td>notification</td>
<td></td>
</tr>
<tr>
<td>Include invitees in</td>
<td>Check this option to include invitee names in notifications.</td>
</tr>
<tr>
<td>notification</td>
<td></td>
</tr>
</tbody>
</table>
Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace

Release 7.1
Revised: April 5, 2011 2:49 pm

You can use the Command-Line Interface (CLI) to perform functions that cannot be performed in the Administration Center.

- CLI User Level Options, page 1
- Restrictions for the CLI, page 2
- How to Log in to the CLI, page 2
- Command Reference, page 4

## CLI User Level Options

<table>
<thead>
<tr>
<th>CLI User Level</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mpxadmin</td>
<td>We recommend that you use this user level whenever possible.</td>
</tr>
<tr>
<td>root</td>
<td>Highest authority, enabling you to do the following:</td>
</tr>
<tr>
<td></td>
<td>• Enter Operating System Commands, though pseudo (sudo) root access may also be used.</td>
</tr>
<tr>
<td></td>
<td>• Enter Database Replication Commands or Failover Commands.</td>
</tr>
<tr>
<td></td>
<td>• Reset the root or mpxadmin user passwords.</td>
</tr>
<tr>
<td></td>
<td>• Uninstall the system.</td>
</tr>
</tbody>
</table>

To get to the root user level, do one of the following:

- Log in as the mpxadmin user, and enter `su` at the command line.
- Log in directly as the root user—this is possibly only by Logging in to the CLI Using the Console.

⚠️ Caution ⚠️ For security reasons, we do not recommend logging in directly as the root user, unless you need to reset the root user or mpxadmin user passwords or uninstall the system.
Restrictions for the CLI

- The CLI and its commands are available only in English.
- The CLI accepts only the standard 128 ASCII characters.
- Many commands you enter may prompt you for information. If the Backspace key does not delete characters in this interactive mode, then use one of the following options:
  - Press the Delete key to delete the previous character.
  - Press Ctrl-W to delete the previous word.
  - Press Ctrl-U to delete the entire line.

How to Log in to the CLI

- Logging in to the CLI Using the Console, page 2
- Logging in to the CLI Using SSH, page 3

Logging in to the CLI Using the Console

You can log in to the CLI from the console using either the mpxadmin or root user IDs. This is the only way you can log in directly as the root user. You can enter operating system commands here.

Procedure

**Step 1**
Connect the monitor, keyboard, and mouse to the Application Server.
The Cisco Unified MeetingPlace operating system login page is displayed.

**Step 2**
For the username, enter mpxadmin.

**Step 3**
Enter the password for the mpxadmin user.
This was established during installation.

**Step 4**
Right-click the desktop and select Open Terminal.
A command window appears. You can start entering commands. This is a Linux operating system so all commands should be either Linux commands or Cisco Unified MeetingPlace operating system commands. See the “Operating System Commands” section on page 13 for information about the operating system commands.
Step 5  When you are finished with the command window, either enter `exit` or select the X in the top right corner.

Note Always log out of the Cisco Unified MeetingPlace operating system when you are finished.

Related Topics
• Logging in to the CLI Using SSH, page 3
• Command Reference, page 4

Logging in to the CLI Using SSH

This section provides one method of logging in to the CLI using SSH. Other methods may be available for you.

Restriction
Only the `mpxadmin` user can log in to the CLI remotely using SSH. If needed, you can later switch to the `root` user by entering `su`.

Before You Begin
You need a remote connection with a non-configurable terminal emulation program, such as the Windows SSH client, to log in to the CLI remotely using SSH.

Procedure

Step 1  From your computer, go to Start > Programs > SSH Secure Shell > Secure Shell Client.
Step 2  Select Quick Connect.
Step 3  In the Connect to Remote Host dialog box, enter the following values:

<table>
<thead>
<tr>
<th>Field</th>
<th>Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Host Name</td>
<td>IP address of your Cisco Unified MeetingPlace system</td>
</tr>
<tr>
<td>User Name</td>
<td>mpxadmin</td>
</tr>
<tr>
<td>Port Number</td>
<td>22</td>
</tr>
<tr>
<td>Authentication Method</td>
<td>leave as &lt;Profile Settings&gt;</td>
</tr>
</tbody>
</table>

Step 4  Select Connect.
Step 5  In the Enter Password dialog box, enter the password for the mpxadmin user.
This was established during installation.
Step 6  Select OK.
The system displays the command line and you can now enter commands.
Related Topics

- Logging in to the CLI Using the Console, page 2
- Command Reference, page 4

Command Reference

- Command Syntax Conventions, page 4
- Application Commands, page 5
- Operating System Commands, page 13
- Database Replication Commands, page 15
- Failover Commands, page 16

Command Syntax Conventions

This document uses these command syntax conventions.

<table>
<thead>
<tr>
<th>Convention</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>bold</strong></td>
<td>Bold text indicates commands and parameters that you enter as shown.</td>
</tr>
<tr>
<td><em>italic</em></td>
<td>Italic text indicates parameters for which you supply values.</td>
</tr>
<tr>
<td><code>&lt;x&gt;</code></td>
<td>Angle brackets enclose a parameter for which you supply values. This is typically used instead of italic text when there is no space between adjacent parameters.</td>
</tr>
<tr>
<td><code>[x]</code></td>
<td>Square brackets enclose an optional parameter.</td>
</tr>
<tr>
<td>`</td>
<td>`</td>
</tr>
<tr>
<td><code>[x y]</code></td>
<td>Square brackets enclosing parameters separated by a pipe indicate an optional choice.</td>
</tr>
<tr>
<td>`{x</td>
<td>y}`</td>
</tr>
<tr>
<td>`[x {y</td>
<td>z}]`</td>
</tr>
</tbody>
</table>
## Application Commands

### Table 1  Command Reference: Application Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| activity | Displays a quick, verbose, or complete status of all ports or a range of ports. Allows you to make a test call and show all meetings.  
Syntax: `activity` |
| alarm    | Displays the Alarm Table:  
- REFNO—Reference number used with the clearalarm command to clear a specific alarm table entry.  
- SEV—Severity, either major (MAJ) or minor (MIN). See “Alarm Severity Levels” in the Using Alarms and Logs on Cisco Unified MeetingPlace module.  
- CODE—See Code.  
- COUNT—See Count.  
- FIRST—See First Time.  
- LAST—See Last Time.  
- UNIT—See Unit.  
- SW MODULE—See Software Module.  
**Note** The brief description in the alarm table entry may contain values that are specific to one alarm occurrence, such as an IP address. These values may differ in all alarms that are combined into one table entry, but only the values for the first alarm are displayed. To see the individual alarms, use the errorlog command or the viewexlog command.  
Syntax: `alarm` |
| checklic | Shows the type and number of licenses installed.  
**Note** The system may take up to 15 seconds to process this information.  
Syntax: `checklic` |
| clearalarm | Clears either all the alarms in the alarm table or just the alarm specified.  
If there are any major alarms in the alarm table, the system can be configured to call the system administrator after every restart until all major alarms are deleted from the alarm table. See “Configuring the System to Call You if There is a Major Alarm” in the Using Alarms and Logs on Cisco Unified MeetingPlace module.  
Running this command stops the system from calling the system administrator (if it has been configured to do so).  
Syntax: `clearalarm` {reference-number | all}` |
cleardb Clears the following Application Server data:
- All user profiles except the admin and guest user profiles
- All user groups except the System group
- All user recordings
- All conference recordings

You must be signed in to the Application Server CLI as the root user to enter this command.

Use this command for specific situations; as instructed in the documentation or as recommended by Cisco TAC. It first clears the database, then restarts all Cisco Unified MeetingPlace services. Upon restarting, ConfSchd service executes a ConfSchd db table rebuild to clean up other dependent tables. When the ConfSchd db table rebuild is completed and all other MeetingPlace services are up, then the prompt returns.

Note: If the Application Server is in a failover or in a RSNA deployment, then turn off replication before running this command. Be sure that the Application Server is in active mode before running this command.

Syntax: cleardb

cpstatus Displays information about each active call, including the associated meeting ID, whether the system dialed out to the endpoint, and whether the call uses video.

Syntax: cpstatus

cptrace Lists selected portions of the call processing trace log.

Syntax: cptrace

date Displays the time and date for the Application Server.

If you are logged in as a root user, then you can also set the date and time based on the local time zone.

Syntax: date [MMDDhhmmYYYY][.ss]

Parameters (available only to root users):
- **MM**—month, specified by two digits
- **DD**—day, specified by two digits
- **hh**—hour, specified by two digits in 24-hour format
- **mm**—minute, specified by two digits
- **YYYY**—calendar year, specified by four digits
- **.ss**—second, specified by two digits and a preceding period (.)
Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace

Command Reference

---

**dbupdate** Deletes all entries in the Cisco Unified MeetingPlace database, so that the database is the equivalent of that in a newly installed Cisco Unified MeetingPlace system. This means that all user groups, user profiles, video terminal profiles, remote servers, meeting categories, and all meeting records are deleted from the system except the standard, preconfigured items, such as the System user group.

**Caution** Deleting all database entries is an irreversible operation. Before you run the `dbupdate` command, consider backing up and archiving the database. See the [Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server](#) module.

Use this command only in the following situations:

- Cisco TAC instructs you to do so.
- You configured Directory Service on your system, and you need to change the LDAP directory with which Cisco Unified Communications Manager is integrated. If you do not clear the database before switching from one LDAP directory to another, then all the user profiles from the first LDAP directory will remain in the Cisco Unified MeetingPlace database until you manually delete them.

The automatic Directory Service deletion of user profiles does not apply when you change the LDAP directory. For details about when and how the system automatically deletes Directory Service user profiles, see “Directory Service User Profile Deletion” in the [Configuring Cisco Unified MeetingPlace Directory Service](#) module.

---

**errorlog** Displays the Exception Log output one screen at a time:

- Date of the event
- Time of the event
- Severity (major, minor, informational, or warning)
- Exception code
- Brief description

In contrast, the `viewexlog` command provides the entire Exception Log output all at once.

**Syntax:** `errorlog`

---

### Table 1  Command Reference: Application Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>dbupdate</td>
<td>Deletes all entries in the Cisco Unified MeetingPlace database, so that the database is the equivalent of that in a newly installed Cisco Unified MeetingPlace system. This means that all user groups, user profiles, video terminal profiles, remote servers, meeting categories, and all meeting records are deleted from the system except the standard, preconfigured items, such as the System user group.</td>
</tr>
</tbody>
</table>

**Caution** Deleting all database entries is an irreversible operation. Before you run the `dbupdate` command, consider backing up and archiving the database. See the [Backing Up, Archiving, and Restoring Data on the Cisco Unified MeetingPlace Application Server](#) module.

Use this command only in the following situations:

- Cisco TAC instructs you to do so.
- You configured Directory Service on your system, and you need to change the LDAP directory with which Cisco Unified Communications Manager is integrated. If you do not clear the database before switching from one LDAP directory to another, then all the user profiles from the first LDAP directory will remain in the Cisco Unified MeetingPlace database until you manually delete them.

The automatic Directory Service deletion of user profiles does not apply when you change the LDAP directory. For details about when and how the system automatically deletes Directory Service user profiles, see “Directory Service User Profile Deletion” in the [Configuring Cisco Unified MeetingPlace Directory Service](#) module.

<table>
<thead>
<tr>
<th>errorlog</th>
<th>Displays the Exception Log output one screen at a time:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Date of the event</td>
</tr>
<tr>
<td></td>
<td>Time of the event</td>
</tr>
<tr>
<td></td>
<td>Severity (major, minor, informational, or warning)</td>
</tr>
<tr>
<td></td>
<td>Exception code</td>
</tr>
<tr>
<td></td>
<td>Brief description</td>
</tr>
</tbody>
</table>

In contrast, the `viewexlog` command provides the entire Exception Log output all at once.

**Syntax:** `errorlog`
Table 1  Command Reference: Application Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| eventlog | Displays the system event log. **Note** This command has many parameter options; only the most commonly used parameters are listed below. Syntax: `eventlog [-b [YY][MMDD]hhmm] [-e [YY][MMDD]hhmm] [-G | -C ] [-t ] [more]` Parameters:  
  - `-b`—Specifies a start time for the log events to include in the output.  
  - `-e`—Specifies an end time for the log events to include in the output.  
  - `YY`—Calendar year, specified by two digits. Typically, this parameter is included only when troubleshooting issues around the start of a new calendar year.  
  - `MM`—month, specified by two digits  
  - `DD`—day, specified by two digits  
  - `hh`—hour, specified by two digits in 24-hour format  
  - `mm`—minute, specified by two digits  
  - `-G`—Shows the telephony and conference events and control messages from the Call Processing–Media Control Protocol (CPMCP) component, which is a proxy for the Media Server.  
  - `-C`—Limits log output to events for the conference scheduler (ConfSchd) component.  
  - `-t`—Displays the log output in real time. This option is useful for troubleshooting issues in real time. For example, you can enter `eventlog -G -t` and then place a test call to the system to see how the system responds to the incoming call and to any subsequent user input.  
  - `more`—Displays the log output one screen at a time.  

| exc | Displays the meaning of an exception code that was listed in the errorlog or viewexlog command output. Syntax: `exc [-v] exception-code` |
| hostname | Displays the hostname of the Application Server. Syntax: `hostname` |
| infocap | Captures configuration details and logs from the system for a particular time period. The output file is a zip file that is stored in the /tmp directory. The system gives the exact location after compiling the information. **Restrictions:**  
  - You must be logged in as the root user to run this command.  
  - You can also get this information by completing “Obtaining and Viewing the System Information Capture (Infocap) Log” in the Using Alarms and Logs on Cisco Unified MeetingPlace module. Use this command only if you are unable to get the information from the Cisco Unified MeetingPlace Administration Center.  
  - The begin and end dates and times must be in the format [YY]MMDDhhmm. The YY is optional and if not specified, the system uses the current year. For format details, see the parameters for the date command. Syntax: `infocap -b begin-date-and-time -e end-date-and-time` |
Table 1  Command Reference: Application Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| langinfo | Displays information about all installed locales including the following:  
- Locale ID  
- Language code  
- Locale order  
- Locale name  
- Country code  
- Locale version number  
Syntax: `langinfo` |

| mtginfo | Displays information about a specific meeting. Searches for a meeting based on any of these:  
- Unique conference ID (such as 125). (This number is output by certain commands such as `cptrace -C` and `errorlog`. It uniquely identifies a meeting.)  
- Meeting ID (such as 1278). Can optionally use any of the time arguments.  
- Unique user ID (such as 0x65). (This number is output by certain commands such as `userinfo`. It uniquely identifies a user.) Searches for all meetings that a user has attended or been invited to.  
- Activity. Searches only for active meetings.  
- Time. Searches for all meetings valid at a certain time with the -t argument or between two times when the -s and -e arguments are used together.  
Syntax: `mtginfo -a time -c unique-conf-id -e end-time -m meeting-id -s start-time -t time -u unique-user-id`  
**Note** The start and end times must be in the format YYMMDDhhmm. All parameters are optional. If they are not all present, the system starts processing from the right. For format details, see the parameters for the `date` command.  
**Note** Start and end times in the command output are adjusted for the Meeting ID start guard time (minutes) and Meeting ID end guard time (minutes) fields on the Meeting Configuration Page. |

Examples:  
- `mtginfo -m 1234` Looks for the meeting with the ID of 1234 at the current time  
- `mtginfo -m 1234 -t 11` Looks for meeting with the ID of 1234 at 11 minutes after the current hour  
- `mtginfo -m 1234 -t 1111111111` Looks for meeting with the ID of 1234 at 11:11am on Nov 11, 2011  
- `mtginfo -a 1430` Looks for meetings that are active at 2:30pm today  
- `mtginfo -s 1430 -e 1530` Looks for meetings that started or ended between 2:30 and 3:30pm today  
- `mtginfo -c 123` Looks for meeting with the unique conference ID of 123  
- `mtginfo -u 123 -t 1111 -e 1211` Looks for meetings that the user with the unique user ID of 123 is invited to between 11:11 and 12:11 today |
Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace

Command Reference

**Table 1 Command Reference: Application Commands (continued)**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| net     | Lists the current network configuration settings and allows you to change them after the system has been installed. Most changes take affect after restarting the system.  

**Caution** A system restart terminates all existing call connections. Proceed only during a scheduled maintenance period or during a period of extremely low usage. **Note:** When you restart the Web Server, all manual changes made to the registry are lost.  

Use the *net* command to set the following:  

- Port configuration parameters, including:  
  - Application Server (eth0) hostname, IP address, subnet mask, and default gateway  
  - Virtual (eth0:0) hostname, IP address, subnet mask, and default gateway—the eth0:0 virtual interface is used in Application Server Failover deployments  
  - MTU and link parameters (auto-negotiation, speed, duplex).  
- Domain name  
- DNS servers  
- NTP servers  

**Note** If you change the Application Server hostname (for eth0), then you must also perform the following actions:  

- Configure the DNS¹ server to point the old hostname to the new hostname.  
- Restart the application by entering either the *mpx_sys restart* operating system command or the *reboot* Linux command.  
- If you enabled SSL for the Application Server, then complete the “Generating a Certificate Signing Request and Obtaining the Certificate” and “Uploading the Certificate File and Enabling SSL” sections in the Configuring SSL for the Cisco Unified MeetingPlace Application Server module.  
- If you installed MeetingPlace Conference Manager, then complete the “Editing an Existing Server” section in the Using MeetingPlace Conference Manager module.  
- If your system includes a Web Server, then complete the “Changing the Cisco Unified MeetingPlace Application Server Connection Configured in the Gateway SIM” section in the Configuring the Cisco Unified MeetingPlace Gateway System Integrity Manager module.  
- If you integrated the system with Cisco WebEx, then notify the Cisco WebEx administrator to update the Cisco Unified MeetingPlace hostname that is configured in the Cisco WebEx license manager.  

**Syntax:** *net*  

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| ntpdate | Sets the Application Server date and time to match the time obtained by polling an NTP² server.  

**Syntax:** *ntpdate [-u] ntp-server*  

**Parameters:**  

- *-u*—Specifies to send packets through an unprivileged port to communicate with the NTP server. Use this option when you want to reach an NTP server that is beyond a firewall.  
- *ntp-server*—Hostname or IP address of the NTP server.
Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace

Command Reference

**Table 1** Command Reference: Application Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| swstatus | Displays information about Cisco Unified MeetingPlace, including the following:  
- Version number  
- System mode  
- Status of the power supplies  
- List of software modules loaded into memory, their version number, and their status  
Syntax: `swstatus` |
| techui | Displays statistics for the Media Server, ports, and conferences.  
This technician user interface helps to diagnose and troubleshoot media and voice quality issues of active calls.  
Syntax: `techui` |
| userinfo | Displays information about a specific user. Searches for a user based on any of these:  
- User ID  
- Profile number  
- Unique user ID (such as 0x65). The unique user ID is output by certain commands. It uniquely identifies a user but does not display the name of the user.  
Syntax: `userinfo {user-id | profile-number | unique-user-id}` |
Command Reference: Application Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| userutil | Performs administrative functions for any user profile.  
Restriction: You cannot set the admin user to inactive, locked, or the group default.  
Syntax: userutil [-q | [-p | -P] [-n | -N] [-a | -i | -l | -g]] userid [password]  
Parameters:  
- `-q`—Displays user profile information and status.  
- `-p`—Reset the User password. Requires a password entry.  
- `-P`—Reset the User password and force it to expire. Requires a password entry.  
- `-n`—Reset the Profile password (PIN for authentication over the phone). Requires a password entry.  
- `-N`—Reset the Profile password and force it to expire. Requires a password entry.  
- `-a`—Set User status to active.  
- `-i`—Set User status to inactive.  
- `-l`—Set User status to locked.  
- `-g`—Set User status to group default setting.  
- `userid`—User ID.  
- `password`—New User password or Profile password. Required if you enter `-p`, `-P`, `-n`, or `-N`. |
| viewexlog | Provides the entire Exception Log output all at once:  
- Date of the event  
- Time of the event  
- Severity (major, minor, informational, or warning)  
- Exception code  
- Brief description  
In contrast, the errorlog command displays the Exception Log output one screen at a time:  
Syntax: viewexlog |

1. DNS = Domain Name System  
2. NTP = Network Time Protocol

Related Topics  
- Using Alarms and Logs on Cisco Unified MeetingPlace module
Operating System Commands

In addition to the Cisco Unified MeetingPlace commands listed in Table 2, the CLI supports the standard Linux operating system commands. You can use the `vim` command to view or modify text files if necessary.

Note the following requirements and restrictions for operating system commands:

- With the exception of the `mpx_sys` command, use the operating system commands to start or stop services only when you have been explicitly told to do so by Cisco TAC. Use of these commands may cause unpredictable results.
- If you are not logged in as the `root` user, then you must enter `sudo` before you can run any of these commands. For example, to stop all application services, go to the command line and enter the following:

  ```
  sudo /mpx_app stop
  ```

  The preceding example assumes that you are already in the `/etc/init.d` directory. If you are not in that directory, then you instead enter the following:

  ```
  sudo /etc/init.d/mpx_app stop
  ```

- Existing call connections will not be terminated by stopping services on the Application Server. However, starting or restarting services will terminate those calls. This behavior applies:
  - To the `mpx_app`, `mpx_sys`, and `mpx_va` commands.
  - If the Application Server crashes and is reloaded.
  - If you enter the `shutdown` or `reboot` Linux command on the Application Server.

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><code>mpx_app</code></td>
<td>Starts, stops, or restarts all Cisco Unified MeetingPlace application services. Note: When you restart the Web Server, all manual changes made to the registry are lost. Syntax: `mpx_app {start</td>
</tr>
<tr>
<td><code>mpx_axlds</code></td>
<td>Starts, stops, or restarts Directory Service and external AXL authentication through Cisco Unified Communications Manager. Syntax: `mpx_axlds {start</td>
</tr>
<tr>
<td><code>mpx_db</code></td>
<td>Starts, stops, or restarts Cisco Unified MeetingPlace database services. Syntax: `mpx_db {start</td>
</tr>
<tr>
<td><code>mpx_lm</code></td>
<td>Starts, stops, or restarts Cisco Unified MeetingPlace license manager services. Syntax: `mpx_lm {start</td>
</tr>
<tr>
<td><code>mpx_rmi</code></td>
<td>Starts, stops, or restarts messaging integration services for Cisco Unified MeetingPlace Click-to-Conference for IBM Lotus Sametime Instant Messaging. Syntax: `mpx_rmi {start</td>
</tr>
<tr>
<td><code>mpx_rssctrl</code></td>
<td>Starts, stops, or restarts the Cisco Unified MeetingPlace recording and streaming service. Syntax: `mpx_rssctrl {start</td>
</tr>
<tr>
<td><code>mpx_sipserver</code></td>
<td>Starts, stops, or restarts the SIP B2BUA on the Application Server. Syntax: `mpx_sipserver {start</td>
</tr>
</tbody>
</table>
mpx_snmp Starts, stops, or restarts SNMP services.
Syntax: `mpx_snmp { start | stop | restart | status } [-v]`

Caution
A system restart terminates all existing call connections. Proceed only during a scheduled maintenance period or during a period of extremely low usage.

Note
If the restart process is interrupted, then you will have to reenter the `mpx_sys restart` command. For example, the restart process may be interrupted by a power outage, by closing the SSH connection, or by another restart process that is initiated from a different terminal.

Syntax: `mpx_sys { stop | restart | status } [-v]`

mpx_sys Starts, stops, or restarts all Cisco Unified MeetingPlace services.

mpx_tomcat Starts, stops, or restarts Apache Tomcat services.
Syntax: `mpx_tomcat { start | stop | restart | status } [-v]`

mpx_tomcatmon Starts, stops, or restarts Apache Tomcat monitoring services.
Syntax: `mpx_tomcatmon { start | stop | restart | status } [-v]`

mpx_va Starts, stops, or restarts Media Server services on the Application Server.
If all other Cisco Unified MeetingPlace services continue running, then entering this command does not interrupt meetings that are in session.
Syntax: `mpx_va { start | stop | restart | status } [-v]`

mpx_version Lists all installed versions of Cisco Unified MeetingPlace.
Syntax: `mpx_version`

mpx_webx Starts, stops, or restarts all Cisco WebEx integration services on the Application Server.
Syntax: `mpx_webx { start | stop | restart | status } [-v]`

resetmsapassword Resets the Media Server Administration password to “cisco”.
Syntax: `resetmsapassword`

shutdown Shuts down the Application Server.
For a graceful shutdown, we recommend that you enter the command using the syntax below. You can see which other options are available by entering `shutdown` without any parameters.
Syntax: `shutdown -h now`


Related Topics
- Configuring Application Server Failover for Cisco Unified MeetingPlace module
- “Changing the Media Server Administration Password” in the Changing Values for the Media Server module of the Installation, Upgrade, and Migration Guide for Cisco Unified MeetingPlace
Database Replication Commands

**Note** To enter the database replication commands in Table 3:

- The MeetingPlace Database services must be running on the Application Server.
- You must be logged in to the CLI as the root user.

The output messages from each command execution are displayed on the screen and stored in a log file under the directory $MP_LOGDIR/database/replication/logs. The log file names have the format mp_replication_log.<YYYY-MM-DD_hh-mm-ss>.

**Table 3 Command Reference: Database Replication Commands**

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mp_replication init</td>
<td>Makes necessary changes in configuration files and database to enable the Application Server to use database replication. Run this command on each node involved in replication. Syntax: `mp_replication init -n node {1</td>
</tr>
<tr>
<td></td>
<td>- <code>-n node</code>—Specifies the node (within the specified site) on which you run the command. Valid values for <code>node</code> are 1 and 2.</td>
</tr>
<tr>
<td></td>
<td>- <code>-r remote-server</code>—Specifies the hostname or IP address of the other Application Server with which to establish replication.</td>
</tr>
<tr>
<td></td>
<td>- <code>-v</code>—Specifies verbose output.</td>
</tr>
<tr>
<td>mp_replication switchON</td>
<td>Starts replication between two Application Servers.</td>
</tr>
<tr>
<td></td>
<td>- Run this command on node 1 only.</td>
</tr>
<tr>
<td></td>
<td>- Run this command only after running the <code>mp_replication init</code> command on each node involved in replication.</td>
</tr>
<tr>
<td></td>
<td>Syntax: <code>mp_replication switchON [-S -F from-sync] [-v]</code> Parameters:</td>
</tr>
<tr>
<td></td>
<td>- <code>-S -F from-sync</code>—Indicates data synchronization between the two Application Servers.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> Both Application Servers must be in standby mode when the <code>-S -F</code> options are used.</td>
</tr>
</tbody>
</table>
|                          | For intra-site replication, which is used for Application Server Failover, specify the hostname or IP address of the virtual network interface eth0:0.  
- `-v`—Specifies verbose output.                                                                                                                                                                                                 |
| mp_replication status    | Displays the status of replication between the specified servers.                                                                                                                                                                   |
### Table 3: Command Reference: Database Replication Commands (continued)

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>mp_replication switchOFF</td>
<td>Stops replication, but does not restore configuration changes.</td>
</tr>
<tr>
<td></td>
<td>• Run this command on node 1 only.</td>
</tr>
<tr>
<td></td>
<td>• To restart replication, use the mp_replication switchON command.</td>
</tr>
<tr>
<td></td>
<td>• To restore the configuration changes done by the mp_replication init command, use the mp_replication teardown command.</td>
</tr>
<tr>
<td>Syntax:</td>
<td><strong>mp_replication switchOFF</strong> [-v]</td>
</tr>
<tr>
<td>Parameters:</td>
<td>See the mp_replication init command.</td>
</tr>
<tr>
<td>mp_replication teardown</td>
<td>Removes configuration changes made on the local server for replication with the specified remote server. Run this command on each node involved in replication to undo the configuration changes.</td>
</tr>
<tr>
<td>Syntax:</td>
<td><strong>mp_replication teardown</strong> [-v]</td>
</tr>
<tr>
<td>Parameters:</td>
<td>See the mp_replication init command.</td>
</tr>
</tbody>
</table>

### Failover Commands

**Note** You must be logged in to the CLI as the root user to enter the failover commands in Table 4.
### Table 4  Command Reference: Failover Commands

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| failoverUtil copyConfigFiles | Transfers configuration files from one Application Server to the other, specifically:

1. Compresses the configuration files and user prompts on the local server.
2. Transfers the compressed files to the remote server.

After you enter this command on the local server, you need to enter the `failoverUtil restoreConfigFiles` on the remote server.

The following files and directories are transferred by this command:

- **Directory Service:**
  - `/opt/cisco/meetingplace/axlds/current/etc/config.properties`

- **Recorded user names and custom voice prompts:**
  - Everything under `/opt/cisco/meetingplace/afs/custom`

- **Microsoft Outlook integration files:**
  - Everything under `/opt/cisco/meetingplace/var/outlook`
  - `/opt/cisco/meetingplace/var/admin/outlook.config`
  - Everything under `/opt/cisco/meetingplace/var/mail`

- **Cisco WebEx integration files:**
  - `/opt/cisco/meetingplace/web/current/etc/conf/keyinfo.properties`
  - `/opt/cisco/meetingplace/web/current/etc/conf/keystore.jks`
  - `/opt/cisco/meetingplace/web/current/etc/conf/cert.cer`

- **Cisco Unified MeetingPlace application server certificate files used for SSL in the Tomcat-based web applications:**
  - `/usr/local/enrollment`

The script pauses to request your credentials. You must provide the following:

- The remote machine's hostname or IP address
- The administrator's username on the remote machine (the mpxadmin username)
- The mpxadmin password

Syntax: `failoverUtil copyConfigFiles`

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Description</th>
</tr>
</thead>
</table>
| failoverUtil restoreConfigFiles | Completes the transfer of configuration files from one Application Server to the other, specifically:

1. Decompresses the configuration files and user prompts that were transferred from the remote server.
2. Places the transferred files into the correct directories, overwriting any existing local files with those from the remote server.

**Note** The `failoverUtil copyConfigFiles` and `failoverUtil restoreConfigFiles` commands are entered on separate Application Servers.

Syntax: `failoverUtil restoreConfigFiles`
Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace

Related Topics

- Configuring Application Server Failover for Cisco Unified MeetingPlace module
Raw Data Export and Import Specifications for Cisco Unified MeetingPlace

Release 7.1
Revised: April 3, 2011 8:31 pm

Use these specifications when importing data to Cisco Unified MeetingPlace or exporting data from Cisco Unified MeetingPlace to a spreadsheet or database program:

- User Groups—Raw Data Export and Import Specifications, page 2
- User Profiles—Raw Data Export and Import Specifications, page 7
- Video Terminal Profiles—Raw Data Export and Import Specifications, page 18
- Meetings—Raw Data Export and Import Specifications, page 27
- Outgoing Calls Information—Raw Data Export Specifications, page 33
- Meeting Participant Information—Raw Data Export Specifications, page 34
- Meeting Participant Join Leave Information—Raw Data Export Specifications, page 36
- Scheduling Failures Information—Raw Data Export Specifications, page 37
- Scheduling Statistics Information—Raw Data Export Specifications, page 38
- Scheduling Activity By User Information—Raw Data Export Specifications, page 39
- Continuous Meetings Information—Raw Data Export Specifications, page 39
# User Groups—Raw Data Export and Import Specifications

**Note** The first line in the export file specifies the Cisco Unified MeetingPlace version. If you want to import this file or use this file as a template for importing data, then you must *not* modify this line.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ContactID</td>
<td>See User ID of delegate.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>tzcode</td>
<td>See Time zone.</td>
<td>0 to 17 ASCII text characters</td>
</tr>
<tr>
<td>Import requirements:</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>The integer value in the import file must match a value defined by Cisco Unified MeetingPlace. Make sure you use a previously exported value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If the import file contains the tzcode header field, then all user groups in the import file must have a valid entry for the field. For any invalid or blank tzcode values, the associated user group is not imported, and an error is logged.</td>
<td></td>
</tr>
<tr>
<td>BillCode</td>
<td>See Billing code.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>grpnum</td>
<td>See Number.</td>
<td>1 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>Import requirement: This field is required in the import file whether you are adding or deleting user groups by import.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>See Name.</td>
<td>1 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>Import requirement: This field is required in the import file whether you are adding or deleting user groups by import.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IsActive</td>
<td>See User status.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>IsAdvancedPrompts</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>CanOutdial</td>
<td>See Can dial out (does not apply to Cisco WebEx meetings).</td>
<td>Yes/No</td>
</tr>
<tr>
<td>NamedDisconnect</td>
<td>See Departure announcement.</td>
<td>Beep only/Beep + name/Silent</td>
</tr>
<tr>
<td>NamedIntroduction</td>
<td>See Entry announcement.</td>
<td>Beep only/Beep + name/Silent</td>
</tr>
<tr>
<td>PasswordRequired</td>
<td>See Meeting password required.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>ScreenedIntroduction</td>
<td>See Screened entry.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>RecordMeetings</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>QuickMtgEntryAllowed</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
</tbody>
</table>
Table 1  Import and Export Data Specifications for User Groups (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PasswordRequiredOnOD</td>
<td>See Ask for profile password.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>MeetingRestriction</td>
<td>See Who can attend.</td>
<td>Anyone/Users/Invited Users/None</td>
</tr>
<tr>
<td>CanRecordMeetings</td>
<td>See Can record meetings.</td>
<td>Yes/No</td>
</tr>
<tr>
<td></td>
<td>Import restriction: If you set this to No, then the autostrtrcrd</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(Auto-start recording) field is set to No during the import</td>
<td></td>
</tr>
<tr>
<td></td>
<td>process.</td>
<td></td>
</tr>
<tr>
<td>MtgNoteRestriction</td>
<td>See Who can access.</td>
<td>Anyone/Users/Invited Users/None</td>
</tr>
<tr>
<td>ODXLabTableNum</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exported value. If you import a new group, enter 0.</td>
<td></td>
</tr>
<tr>
<td>MaxImmedMtgPerDay</td>
<td>See Scheduling restriction (meetings to start within 6 hours</td>
<td>Numeric—range is 0 to 50</td>
</tr>
<tr>
<td></td>
<td>of scheduling).</td>
<td>• 10000—Unrestricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10001—Cannot schedule</td>
</tr>
<tr>
<td>MaximumMeetingLength</td>
<td>See Maximum meeting length (minutes).</td>
<td>Numeric—range is 0 to 1440</td>
</tr>
<tr>
<td></td>
<td>Import restriction: This cannot exceed the value of the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Maximum meeting length (minutes) field on the Meeting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Configuration Page.</td>
<td></td>
</tr>
<tr>
<td>MaxVUIODsPerMtg</td>
<td>See Maximum TUI outdial attempts per meeting.</td>
<td>• Numeric—range is 0 to 500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10000 (unrestricted)</td>
</tr>
<tr>
<td>nondidpgrnum</td>
<td>See Phone number for non-direct-dial pagers.</td>
<td>0 to 32 characters of the</td>
</tr>
<tr>
<td></td>
<td></td>
<td>following types:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• numeric</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• ()</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• space ( )</td>
</tr>
<tr>
<td>faxnum</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>exported value. If you import a new group, leave this field blank.</td>
<td></td>
</tr>
<tr>
<td>maxattsprmtg</td>
<td>See Maximum number of attachments</td>
<td>Numeric—range is 0 to 30</td>
</tr>
<tr>
<td>rcvnotifs</td>
<td>See Can receive notifications.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>site</td>
<td>Not supported.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 1 Import and Export Data Specifications for User Groups (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>preferredunit</td>
<td>See Schedule home server. Import restriction: Cisco Unified MeetingPlace Release 7.1 supports a smaller range of values than earlier releases. If you import user groups that were originally configured for an earlier release system, then make sure that you adjust this value accordingly.</td>
<td>Numeric—range is 0 to 999</td>
</tr>
<tr>
<td>attndprf</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter UserCallsIn.</td>
<td>—</td>
</tr>
<tr>
<td>prmrynifprf</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter EMail.</td>
<td>—</td>
</tr>
<tr>
<td>altnotifprf</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter Unknown_NotPref_Type.</td>
<td>—</td>
</tr>
<tr>
<td>pgrtype</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter DIDPager.</td>
<td>—</td>
</tr>
<tr>
<td>emailtype</td>
<td>See E-mail type and format, which combines the emailtype and EmailFormat fields. <em>Note</em> The emailtype value determines which options are supported in the EmailFormat field.</td>
<td>SMTP/Exchange/LotusNotes</td>
</tr>
<tr>
<td>faxxlattablenum</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter 0.</td>
<td>—</td>
</tr>
<tr>
<td>sndnotifs</td>
<td>See Can send notifications.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>autodistatts</td>
<td>See Send attachments.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>dfltnotifprio</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter Normal.</td>
<td>Low/Normal/Urgent</td>
</tr>
<tr>
<td>sndnotifonmtch</td>
<td>See Send if meeting changes.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>sndinvlstwnotif</td>
<td>See Include invitee list when scheduled from web.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>sndmtgpwdwnotif</td>
<td>See Include password.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>rcvattswnotif</td>
<td>See Receive attachments.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>playattlstfifo</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter Yes.</td>
<td>—</td>
</tr>
</tbody>
</table>
### Table 1 Import and Export Data Specifications for User Groups (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>schedprefunitonly</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>No</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>autostrtrcrd</td>
<td>See Auto-start recording.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>disablerolcall</td>
<td>See Disable roll call.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>schedhomesiteonly</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>Yes</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>concurrentquestions</td>
<td>See More than one question per site.</td>
<td>• 0—No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—Yes</td>
</tr>
<tr>
<td>announceqarr</td>
<td>See Q&amp;A introduction.</td>
<td>Beep only/Beep + name/Silent</td>
</tr>
<tr>
<td>announceqdep</td>
<td>See Q&amp;A departure.</td>
<td>Beep only/Beep + name/Silent</td>
</tr>
<tr>
<td>fqnadisabled</td>
<td>See Off at meeting startup.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>ftellpartpos</td>
<td>See Tell my position in line.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fadvanceinfo</td>
<td>See Disable floor warning prompt.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fautoproenabled</td>
<td>See Automatically ask next question.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fstartpeopleinwr</td>
<td>See Lecture meeting attend settings.</td>
<td>admitaslisteners/ startinwaitingrm/ starmtgwithflooropen</td>
</tr>
<tr>
<td>publiculallowed</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>10</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>groupulallowed</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>0</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>privateulallowed</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>0</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>meetingcategory</td>
<td>See Default meeting category.</td>
<td>Up to 20 alphanumeric characters</td>
</tr>
<tr>
<td>numdataparts</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>0</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>chatclienttype</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>0</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>allowdataconf</td>
<td>See Hide web conference provider.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fchatsession</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>0</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>fismtgseminartype</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>0</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>fallowguestview</td>
<td>See Show meetings in public listing.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>qnanotify</td>
<td>See Notify attendees about Q&amp;A.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td>Size and Type of Value</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>fCanInviteRemoteServers</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>canallowguestoutdial</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>No</strong>.</td>
<td></td>
</tr>
<tr>
<td>allowguestoutdial</td>
<td></td>
<td></td>
</tr>
<tr>
<td>VLanguage</td>
<td>See <strong>Language</strong>.</td>
<td>0 to 128 alphanumeric characters</td>
</tr>
<tr>
<td>fEndMtgWarn</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fMtgExtendPrompts</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>No</strong>.</td>
<td></td>
</tr>
<tr>
<td>SSI_SystemID</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>SSI_RollMapID</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>0</strong>.</td>
<td></td>
</tr>
<tr>
<td>SSI_SiteID</td>
<td></td>
<td></td>
</tr>
<tr>
<td>CanChangeMtgID</td>
<td>See <strong>Can change meeting ID via phone</strong>.</td>
<td><strong>Yes/No</strong></td>
</tr>
<tr>
<td>RsvnlessCnfg</td>
<td>See <strong>Use reservationless</strong>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 0—Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—No</td>
</tr>
<tr>
<td>AllowVideoSched</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>No</strong>.</td>
<td></td>
</tr>
<tr>
<td>AllowInternetAccess</td>
<td>See <strong>Allow Internet access</strong>.</td>
<td><strong>Yes/No</strong></td>
</tr>
<tr>
<td>VideoEndPtBandwidth</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>384K</strong>.</td>
<td></td>
</tr>
<tr>
<td>EmailFormat</td>
<td>See <strong>E-mail type and format</strong>, which combines the <code>emailtype</code> and <code>EmailFormat</code> fields. Restriction: Only the following combinations of <code>emailtype</code> and <code>EmailFormat</code> fields are supported:</td>
<td><strong>txt/html/RTF</strong></td>
</tr>
<tr>
<td></td>
<td>• SMTP/html</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SMTP/txt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LotusNotes/txt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Exchange/html</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Exchange/txt</td>
<td></td>
</tr>
<tr>
<td>ReserveVoiceLicenses</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>Yes</strong>.</td>
<td></td>
</tr>
<tr>
<td>Can Reserve Video Ports</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new group, enter <strong>No</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
Table 1 Import and Export Data Specifications for User Groups (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreferVideo</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter Yes.</td>
<td>—</td>
</tr>
<tr>
<td>FRsvnAllowGuestView</td>
<td>See Show reservationless meetings in public listing.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>attendMode</td>
<td>See Auto attend mode.</td>
<td>—</td>
</tr>
<tr>
<td>attendPasswdRequired</td>
<td>See Auto attend requires profile password.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>FRsvnlessAllowInternetAcc</td>
<td>See Reservationless allow Internet access.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>videoTypes</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new group, enter 0.</td>
<td>—</td>
</tr>
<tr>
<td>mtgEntryMode</td>
<td>See Meeting entry mode.</td>
<td>—</td>
</tr>
<tr>
<td>dataConfClientType</td>
<td>See Default web conference provider.</td>
<td>MP/WEBEX</td>
</tr>
</tbody>
</table>

Related Topics

- Exporting User Groups in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
- Adding or Editing User Groups by Import in the Importing Data into Cisco Unified MeetingPlace module
- Deleting User Groups by Import in the Importing Data into Cisco Unified MeetingPlace module

User Profiles—Raw Data Export and Import Specifications

**Note**

The first line in the export file specifies the Cisco Unified MeetingPlace version. If you want to import this file or use this file as a template for importing data, then you must *not* modify this line.

Table 2 Import and Export Data Specifications for User Profiles

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>fnm</td>
<td>See First name.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
<tr>
<td>lnm</td>
<td>See Last name.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td>Size and Type of Value</td>
</tr>
<tr>
<td>------------</td>
<td>-------------</td>
<td>-----------------------</td>
</tr>
<tr>
<td>uid</td>
<td>See User ID. Import requirement: This field is required whether you are adding or deleting user profiles by import.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>prfnum</td>
<td>See Profile number. Import requirement: This field is required whether you are adding or deleting user profiles by import.</td>
<td>1 to 32 numeric characters</td>
</tr>
<tr>
<td>phnum</td>
<td>See Main phone number.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
<tr>
<td>ctctuid</td>
<td>See User ID of delegate. Import requirement: If not set to gd, then the value must match one of the following: • User ID in the Cisco Unified MeetingPlace database • uid in the import file Restriction: The specified user must be of type Delegate.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>grpnme</td>
<td>See Group name. Import requirement: If the import file contains the grpnme header field, then all user profiles in the import file must have a valid entry for this field. For details, see “Adding or Editing User Profiles by Import” in the Importing Data into Cisco Unified MeetingPlace module.</td>
<td>1 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>grpnum</td>
<td>See Number. Import requirement: If the import file contains the grpnum header field, then all user profiles in the import file must have a valid entry for this field. For details, see “Adding or Editing User Profiles by Import” in the Importing Data into Cisco Unified MeetingPlace module.</td>
<td>0 to 17 numeric characters</td>
</tr>
<tr>
<td>tzcode</td>
<td>See Time zone. Import requirements: • The integer value in the import file must match a value defined by Cisco Unified MeetingPlace. Make sure you use a previously exported value. • If the import file contains the tzcode header field, then all user profiles in the import file must have a valid entry for the field. For any invalid or blank tzcode values, the associated user profile is not imported, and an error is logged.</td>
<td>0 to 17 ASCII text characters</td>
</tr>
<tr>
<td>abbprmpts</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>anndpart</td>
<td>See Departure announcement.</td>
<td>Beep+ name/Beep only/Silent/gd</td>
</tr>
</tbody>
</table>
### Table 2 Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>annentry</td>
<td>See Entry announcement.</td>
<td>Beep+ name/Beep only/ Silent/gd</td>
</tr>
<tr>
<td>pwdreq</td>
<td>See Meeting password required.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>screntry</td>
<td>See Screened entry.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>bcode</td>
<td>See Billing code.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>uactive</td>
<td>See User status.</td>
<td>Yes/No/gd/Locked</td>
</tr>
<tr>
<td>utype</td>
<td>See Type of user.</td>
<td>EndUser/Delegate/Attendant/SysMgr</td>
</tr>
<tr>
<td>cndial</td>
<td>See Can dial out (does not apply to Cisco WebEx meetings).</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>shrtmnus</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>pwdonoutdial</td>
<td>See Ask for profile password.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>whocanattnd</td>
<td>See Who can attend.</td>
<td>Anyone/Users/Invited Users/None</td>
</tr>
<tr>
<td>whocanlstn</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>canrecord</td>
<td>See Can record meetings.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>recordmtgs</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>WFPasswordLastChanged</td>
<td>Display only. When the User password was last changed.</td>
<td>MM/DD/YYYY hh:mm</td>
</tr>
<tr>
<td>VUPasswordLastChanged</td>
<td>Display only. When the Profile password was last changed.</td>
<td>MM/DD/YYYY hh:mm</td>
</tr>
<tr>
<td>ODXLatTableNum</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
</tbody>
</table>
| MaxImmedMtgsPerDay          | See Scheduling restriction (meetings to start within 6 hours of scheduling). | • Numeric—range is 0 to 50  
• 10000—Unrestricted  
• 10001—Cannot schedule  
• gd |
| DayOfLastImmedMtg           | Display only. The date and time of the last immediate meeting that this user scheduled. | MM/DD/YYYY hh:mm       |
| NumImmedMtgsOnThatDay       | Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter 0. | —                      |
| MaximumMeetingLength        | See Maximum meeting length (minutes). Import restriction: This cannot exceed the value of the Maximum meeting length (minutes) field on the Meeting Configuration Page. | gd/Numeric—range is 0 to 1440 |
### Table 2  Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MaxVUIDsPerMtg</td>
<td>See Maximum TUI outdial attempts per meeting.</td>
<td>• Numeric—range is 0 to 500</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 10000—Unrestricted</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• gd</td>
</tr>
<tr>
<td>faxnum</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you import a new profile, leave this field blank.</td>
<td></td>
</tr>
<tr>
<td>pgrnum</td>
<td>See Pager number.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
<tr>
<td>mxattsprmtg</td>
<td>See Maximum number of attachments.</td>
<td>Numeric—range is 0 to 30/gd</td>
</tr>
<tr>
<td>rcvnotifs</td>
<td>See Can receive notifications.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>atndprf</td>
<td>See Method of attending.</td>
<td>UserCallsIn/SysFindsUser</td>
</tr>
<tr>
<td>prmrynotifprf</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>altnotifprf</td>
<td>Import requirement: Do not modify this field from the exported value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you import a new profile, enter gd.</td>
<td></td>
</tr>
<tr>
<td>pgrtype</td>
<td>See Pager type.</td>
<td>DIDPager/NonDIDPager</td>
</tr>
<tr>
<td>emailtype</td>
<td>See E-mail type and format, which combines the emailltype and EmailFormat</td>
<td>SMTP/Exchange/LotusNotes/gd</td>
</tr>
<tr>
<td></td>
<td>fields.</td>
<td></td>
</tr>
<tr>
<td>site</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>preferredunit</td>
<td>See Schedule home server.</td>
<td>Numeric—range is 0 to 999/gd</td>
</tr>
<tr>
<td>emailaddr</td>
<td>See E-mail address.</td>
<td>0 to 128 alphanumeric characters</td>
</tr>
<tr>
<td>faxxlattblnum</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you import a new profile, enter gd.</td>
<td></td>
</tr>
<tr>
<td>sndnotifs</td>
<td>See Can send notifications.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>autodistatts</td>
<td>See Send attachments.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>dfllnotifprio</td>
<td>See Priority.</td>
<td>Low/Normal/Urgent/gd</td>
</tr>
<tr>
<td>sndnotifonmtgch</td>
<td>See Send if meeting changes.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>sndinvlstwnotif</td>
<td>See Include invitee list when scheduled from web.</td>
<td>Yes/No/gd</td>
</tr>
</tbody>
</table>
### Table 2 Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>sndmtgpwdwnotif</td>
<td>See Include password.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>rcvattswnotif</td>
<td>See Receive attachments.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>playattlstfifo</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>schedprefunitonly</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td></td>
</tr>
<tr>
<td>autostrtrcrd</td>
<td>See Auto-start recording.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>disablerolcall</td>
<td>See Disable roll call.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>schedhomesiteonly</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>concurrentquestions</td>
<td>See More than one question per site.</td>
<td>• 0—No</td>
</tr>
<tr>
<td>announceqarr</td>
<td>See Q&amp;A introduction.</td>
<td>• 1—Yes</td>
</tr>
<tr>
<td>announceqdep</td>
<td>See Q&amp;A departure.</td>
<td>• gd</td>
</tr>
<tr>
<td>fqnadisabled</td>
<td>See Off at meeting startup.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>ftellpartpos</td>
<td>See Tell my position in line.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>fadvanceinfo</td>
<td>See Disable floor warning prompt.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>fautoproenabled</td>
<td>See Automatically ask next question.</td>
<td>Yes/No/gd</td>
</tr>
</tbody>
</table>

This field provides the same data, but in text format, as the announceQArr field, which provides data in numeric format:
- 0—Beep only
- 1—Beep+Name
- 2—Silent

Import restriction: If the import file includes both the announceqarr and announceQArr fields, then the system imports only the announceQArr values and ignores the announceqarr values.
### Table 2 Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>fstartpeopleinwr</td>
<td>See Lecture meeting attend settings. This field provides the same data, but in text format, as the FStartPeopleInWR field, which provides data in numeric format: 0—admitaslisteners 1—startinwaitingrm 2—startmtgwithflooropen</td>
<td>admitslisteners/startinwaitingrm/startmtgwithflooropen/gd</td>
</tr>
<tr>
<td>publicallowed</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>groupallowed</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>privateallowed</td>
<td>—</td>
<td>—</td>
</tr>
<tr>
<td>meetingcategory</td>
<td>See Default meeting category.</td>
<td>0 to 20 alphanumeric characters/gd</td>
</tr>
<tr>
<td>numdataparts</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>chatclienttype</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>fallowdataconf</td>
<td>See Hide web conference provider.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>fchatsession</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>fismtgseminartype</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>fallowguestview</td>
<td>See Show meetings in public listing.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>qnanotify</td>
<td>See Notify attendees about Q&amp;A.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>InternetEmailAddr</td>
<td>Not supported.</td>
<td>—</td>
</tr>
</tbody>
</table>
EncryptedUserPWD or upwd

The exported EncryptedUserPWD field is the encrypted User password.

When importing a user profile:
- Use the EncryptedUserPWD field to import a previously encrypted user password.
- Use the import-only upwd field to import an unencrypted user password.

Import requirements:
- The import file must contain the EncryptedUserPWD field or the upwd field. If both fields are included in the import file, then one must be left blank in each user profile.
- If the isLocalUser field is set to No, then both the EncryptedUserPWD and upwd fields must be left blank.

Import restrictions:
- Unicode is not supported.
- If the user is authenticated by an external directory, you cannot modify the User password through Cisco Unified MeetingPlace.

The exported EncryptedProfilePWD field is the encrypted Profile password.

When importing a user profile:
- Use the EncryptedProfilePWD field to specify a previously exported profile password for a locally authenticated user.
- Use the import-only prfpwd field to specify an unencrypted profile password for a locally authenticated user.
- Use the import-only numeric ProfilePWD field for an externally authenticated user. This value is not actually saved or used by the system, but it is required to successfully import externally authenticated users.

Import requirements:
- If the isLocalUser field is set to No, then enter a numeric-only value (such as "12345") for the ProfilePWD field, and make sure that the import file does NOT include the EncryptedProfilePWD field and the prfpwd field.
- If the isLocalUser field is set to Yes, then the import file must contain the EncryptedProfilePWD field or the prfpwd field. If both fields are included in the import file, then one must be left blank in each user profile.

Import restrictions:
- This field cannot be modified in the preconfigured Guest Profile.
- If the user is authenticated by an external directory, you cannot modify the Profile password through Cisco Unified MeetingPlace.


<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>EncryptedProfilePWD</td>
<td>The exported EncryptedProfilePWD field is the encrypted Profile password.</td>
<td>5 to 45 alphanumeric characters</td>
</tr>
<tr>
<td>or prfpwd</td>
<td>When importing a user profile:</td>
<td></td>
</tr>
<tr>
<td>or ProfilePWD</td>
<td>• Use the EncryptedProfilePWD field to specify a previously exported profile password for a locally authenticated user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use the import-only prfpwd field to specify an unencrypted profile password for a locally authenticated user.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Use the import-only numeric ProfilePWD field for an externally authenticated user. This value is not actually saved or used by the system, but it is required to successfully import externally authenticated users.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirements:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the isLocalUser field is set to No, then enter a numeric-only value (such as &quot;12345&quot;) for the ProfilePWD field, and make sure that the import file does NOT include the EncryptedProfilePWD field and the prfpwd field.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the isLocalUser field is set to Yes, then the import file must contain the EncryptedProfilePWD field or the prfpwd field. If both fields are included in the import file, then one must be left blank in each user profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import restrictions:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• This field cannot be modified in the preconfigured Guest Profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the user is authenticated by an external directory, you cannot modify the Profile password through Cisco Unified MeetingPlace.</td>
<td></td>
</tr>
<tr>
<td>fCanInviteRemoteServers</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If you import a new profile, enter gd.</td>
<td></td>
</tr>
<tr>
<td>alphnum</td>
<td>See Alternate phone number.</td>
<td>0 to 32 characters of the following types:</td>
</tr>
<tr>
<td></td>
<td>• numeric</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• ().-.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• space ( )</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2 Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1stSearch</td>
<td>See Search order for find me.</td>
<td>Main phone/Alternate phone/Pager</td>
</tr>
<tr>
<td>2ndSearch</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>3rdSearch</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>canallowguestoutdial</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td>—</td>
</tr>
<tr>
<td>allowguestoutdial</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td>—</td>
</tr>
<tr>
<td>VLanguage</td>
<td>See Language.</td>
<td>0 to 128 alphanumeric characters/gd</td>
</tr>
<tr>
<td>fEndMtgWarn</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>fMtgExtendPrompts</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td>—</td>
</tr>
<tr>
<td>SSI_SystemID</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>SSI_RollMapID</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>SSI_SiteID</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>CanChangeMtgID</td>
<td>See Can change meeting ID via phone.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>RsvnlessCnfg</td>
<td>In effect when RsvnlessCnfgGD is set to 254. See Use reservationless.</td>
<td>• 0—Yes  • 1—No</td>
</tr>
<tr>
<td>RsvnlessCnfgGD</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <code>255</code> for Group Default, or <code>254</code> for custom value defined in RsvnlessCnfg.</td>
<td>—</td>
</tr>
<tr>
<td>AllowVideoSched</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>AllowInternetAccess</td>
<td>See Allow Internet access.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>VideoEndPtBandwidth</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>bountyUser</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <code>TRUE</code>.</td>
<td>—</td>
</tr>
</tbody>
</table>
### Table 2 Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>isLocalUser</td>
<td>Whether the user profile is for a Directory Service user. Also determines the user authentication method:</td>
<td>Yes/No</td>
</tr>
<tr>
<td></td>
<td>• Yes—Local authentication against the Cisco Unified MeetingPlace database.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• No—Directory Service user; External AXL authentication.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>See “Directory Service isLocalUser Setting In User Profiles” in the Configuring Cisco Unified MeetingPlace Directory Service module.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restriction: This field does not appear in the Administration Center. You can view this setting only by exporting user profiles, and you can modify this field only through a manual import process.</td>
<td></td>
</tr>
<tr>
<td>EmailFormat</td>
<td>See E-mail type and format, which combines the emailltype and EmailFormat fields.</td>
<td>txt/html/RTF/gd</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong> If you use the gd value, then make sure that the EmailFormat field in the assigned user group is compatible with the emailltype field in the user profile.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restriction: Only the following combinations of emailltype and EmailFormat fields are supported:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SMTP/html</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SMTP/txt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• LotusNotes/txt</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Exchange/html</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Exchange/txt</td>
<td></td>
</tr>
<tr>
<td>ReserveVoiceLicenses</td>
<td><strong>Not supported.</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td></td>
</tr>
<tr>
<td>LockedProfileTime</td>
<td>Time when profile was locked, in seconds, from 1/1/1970 00:00:00 GMT.</td>
<td>Integer—range is 0 to $2^{31} - 1$</td>
</tr>
<tr>
<td></td>
<td>A value of 0 means that the profile is not currently locked.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, then enter 0 for this field.</td>
<td></td>
</tr>
<tr>
<td>CanReserveVideoPorts</td>
<td><strong>Not supported.</strong></td>
<td></td>
</tr>
<tr>
<td>PreferVideo</td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 2  Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PreferDataConf</td>
<td>Not supported. Do not modify this field from the exported value. If you import a new profile, enter Yes.</td>
<td>—</td>
</tr>
<tr>
<td>FRsvnlessAllowInternetAcc</td>
<td>See Reservationless allow Internet access.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>FStartPeopleInWR</td>
<td>See Lecture meeting attend settings. This field provides the same data, but in numeric format, as the fstartpeopleinwr field, which provides data in text format: 0—admitaslisteners 1—startinwaitingrm 2—startmtgwithflooropen Import restriction: If the import file includes both the fstartpeopleinwr and FStartPeopleInWR fields, then the system imports only the FStartPeopleInWR values and ignores the fstartpeopleinwr values.</td>
<td>0/1/2/gd</td>
</tr>
<tr>
<td>attendMode</td>
<td>See Auto attend mode.</td>
<td>• 0—None</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—Automatically join meeting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 2—Automatically log in</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• gd</td>
</tr>
<tr>
<td>attendPasswdRequired</td>
<td>See Auto attend requires profile password.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>announceQArr</td>
<td>See Q&amp;A introduction.</td>
<td>0/1/2/gd</td>
</tr>
<tr>
<td></td>
<td>This field provides the same data, but in numeric format, as the announceqarr field, which provides data in text format: 0—Beep only 1—Beep+Name 2—Silent Import restriction: If the import file includes both the announceqarr and announceQArr fields, then the system imports only the announceQArr values and ignores the announceqarr values.</td>
<td></td>
</tr>
<tr>
<td>videoTypes</td>
<td>Not supported. Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>mtgEntryMode</td>
<td>see Meeting entry mode.</td>
<td>• 0—Echo meeting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—Skip ID repeat</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 3—Skip ID repeat and skip names</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• gd</td>
</tr>
</tbody>
</table>
Table 2  Import and Export Data Specifications for User Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dataConfClientType</td>
<td>See Default web conference provider.</td>
<td>MP/WEBEX/gd</td>
</tr>
<tr>
<td>CCMpkid</td>
<td>This field determines whether the user profile will be affected by the next Directory Service user profile update. Import requirement: Do not modify this field from the exported value. If you import a new profile, leave this field blank.</td>
<td>Up to 40 characters</td>
</tr>
</tbody>
</table>

1.  gd = group default
2.  GMT = Greenwich Mean Time

Related Topics
- Exporting User Profiles in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
- Adding or Editing User Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module
- Deleting User Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module

Video Terminal Profiles—Raw Data Export and Import Specifications

Table 3 contains two categories:
- Fields Exported in All Releases
- Fields Exported Only in Release 7.0.1

Table 3  Import and Export Data Specifications for Video Terminal Profiles

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>videoTermName</td>
<td>See Video terminal name.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
<tr>
<td></td>
<td>Import requirement: This field is required when you add VTPs by import.</td>
<td></td>
</tr>
</tbody>
</table>
Table 3  **Import and Export Data Specifications for Video Terminal Profiles (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>videoTermId</td>
<td>Unique value that identifies the VTP in report and export output.</td>
<td>1 to 30 numeric characters</td>
</tr>
<tr>
<td></td>
<td>(Release 7.0.1 only) The values for the following fields are identical in each VTP:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• uid</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• prfnum</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• videoTermId</td>
<td></td>
</tr>
<tr>
<td></td>
<td>For VTPs that you manually add through the Administration Center, this value is automatically generated by the system.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Import requirements:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• This field is required whether you are adding or deleting VTPs by import.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do not modify this field from the exported value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Release 7.0.1 only) If you import a new VTP, you must enter a unique value that exactly matches what you enter in the uid and prfnum fields.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• (Release 7.0.1 only) Make sure that this field contains only numeric characters.</td>
<td></td>
</tr>
<tr>
<td>videoEndPtAddStr</td>
<td>See Endpoint E.164 number.</td>
<td>Up to 32 characters</td>
</tr>
<tr>
<td></td>
<td>Import requirement: This field is required when you add VTPs by import.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restriction: Only the following characters are allowed: (),.-, and 0-9.</td>
<td></td>
</tr>
<tr>
<td>grpnme</td>
<td>See Group name.</td>
<td>1 to 17 alphanumeric characters</td>
</tr>
<tr>
<td></td>
<td>Import requirements:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• This field is required whether you are adding or deleting user profiles by import.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Do not modify this field from the exported value. If you import a new VTP, enter System.</td>
<td></td>
</tr>
<tr>
<td>grpnum</td>
<td>Number of user group.</td>
<td>0 to 17 numeric characters</td>
</tr>
<tr>
<td></td>
<td>Import requirement: Do not modify this field from the exported value. If you import a new VTP, enter 0 to indicate the System User Group.</td>
<td></td>
</tr>
<tr>
<td>emailaddr</td>
<td>See E-mail address.</td>
<td>0 to 128 alphanumeric characters</td>
</tr>
</tbody>
</table>
Table 3 Import and Export Data Specifications for Video Terminal Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>tzcode</td>
<td>Time zone of the video terminal. Import requirements:</td>
<td>0 to 17 ASCII text characters</td>
</tr>
<tr>
<td></td>
<td>• The integer value in the import file must match a value defined by Cisco Unified MeetingPlace. Make sure you use a previously exported value.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• If the import file contains the tzcode header field, then all user groups in the import file must have a valid entry for the field. For any invalid or blank tzcode values, the associated user group is not imported, and an error is logged.</td>
<td></td>
</tr>
<tr>
<td>supportSIPReInvite</td>
<td>See Skip meeting entry voice prompts on outdial.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>attnDpf</td>
<td>See Method of attending.</td>
<td>UserCallsIn/SysFindsUser</td>
</tr>
<tr>
<td>rcvnotifs</td>
<td>See Can receive notifications.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>rcvattswnotif</td>
<td>See Receive attachments.</td>
<td>Yes/No/gd</td>
</tr>
<tr>
<td>preferedCodec</td>
<td>See Preferred codec.</td>
<td>1/2/5/6</td>
</tr>
<tr>
<td></td>
<td>• 1—H.261</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 2—H.263</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 5—H.264</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 6—Use default (H.264)</td>
<td></td>
</tr>
<tr>
<td>fnm</td>
<td>Video terminal name that appears in the participant list and in reports. The system copies this value from the videoTermName field. Import requirement: Do not modify this field from the exported value. If you import a new VTP, enter the same text that you enter in the videoTermName field.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
</tbody>
</table>
### Table 3 Import and Export Data Specifications for Video Terminal Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>uid</td>
<td>Unique value that identifies the VTP in report and export output. The values for the following fields are identical in each VTP: • uid • prfnum • videoTermId For VTPs that you manually add through the Administration Center, this value is automatically generated by the system. Import requirements: • This field is required whether you are adding or deleting VTPs by import. • Do not modify this field from the exported value. If you import a new VTP, you must enter a unique value that exactly matches what you enter in the prfnum and videoTermId fields.</td>
<td>1 to 30 numeric characters</td>
</tr>
<tr>
<td>phnum</td>
<td>See Endpoint E.164 number.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
<tr>
<td>abbprmpts</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>anndpart</td>
<td>See Departure announcement. Import requirement: Do not modify this field from the exported value. If you import a new VTP, enter gd.</td>
<td>Beep+ name/Beep only/ Silent/gd</td>
</tr>
<tr>
<td>annentry</td>
<td>See Entry announcement. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter Beep only.</td>
<td>Beep+ name/Beep only/ Silent/gd</td>
</tr>
<tr>
<td>pwdreq</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new VTP, enter No.</td>
<td>—</td>
</tr>
<tr>
<td>screntry</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter Yes.</td>
<td>—</td>
</tr>
<tr>
<td>uactive</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter EndUser.</td>
<td>—</td>
</tr>
<tr>
<td>utype</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter No.</td>
<td>—</td>
</tr>
<tr>
<td>cndial</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter No.</td>
<td>—</td>
</tr>
</tbody>
</table>
### Table 3 Import and Export Data Specifications for Video Terminal Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>shrtmnus</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td></td>
</tr>
<tr>
<td>pwdonoutdial</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>No</code>.</td>
<td></td>
</tr>
<tr>
<td>whocanattnd</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td></td>
</tr>
<tr>
<td>whocanlstn</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>Anyone</code>.</td>
<td></td>
</tr>
<tr>
<td>canrecord</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>No</code>.</td>
<td></td>
</tr>
<tr>
<td>recordmtgs</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>No</code>.</td>
<td></td>
</tr>
<tr>
<td>ODXLatTableNum</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td></td>
</tr>
<tr>
<td>MaxImmedMtgsPerDay</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td></td>
</tr>
<tr>
<td>DayOfLastImmedMtg</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, leave this field blank.</td>
<td></td>
</tr>
<tr>
<td>NumImmedMtgsOnThatDay</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>0</code>.</td>
<td></td>
</tr>
<tr>
<td>site</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>0</code>.</td>
<td></td>
</tr>
<tr>
<td>sndnotifs</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>No</code>.</td>
<td></td>
</tr>
<tr>
<td>autodistatts</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>No</code>.</td>
<td></td>
</tr>
<tr>
<td>dfltnotifprio</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td></td>
</tr>
<tr>
<td>sndnotifonmtgch</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td></td>
</tr>
<tr>
<td>sndinvlstwnotif</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>gd</code>.</td>
<td></td>
</tr>
<tr>
<td>sndmtgpwdwnotif</td>
<td>Not supported.IMP: Do not modify this field from the exported value. If you import a new profile, enter <code>No</code>.</td>
<td></td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td>Size and Type of Value</td>
</tr>
<tr>
<td>--------------------------</td>
<td>------------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>playattlstfifo</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>schedprefuninitonly</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{Yes}.</td>
<td>—</td>
</tr>
<tr>
<td>autostrtrcdr</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{No}.</td>
<td>—</td>
</tr>
<tr>
<td>disbablerollcall</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{Yes}.</td>
<td>—</td>
</tr>
<tr>
<td>concurrentquestions</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>announceqarr</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>announceqdep</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fqnadisabled</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>ftellpartpos</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fadvanceinfo</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fautoproenabled</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fstartpeopleinwr</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>groupulallowed</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>privateulallowed</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>meetingcategory</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>numdataparts</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>chatclienttype</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fallowdataconf</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fchatsession</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fismtgseminartype</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fallowguestview</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>qnanotify</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
<tr>
<td>fCanInviteRemoteServers</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter \textbf{gd}.</td>
<td>—</td>
</tr>
</tbody>
</table>
### Import and Export Data Specifications for Video Terminal Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>1stSearch</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>Main phone</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>2ndSearch</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>Alternate phone</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>3rdSearch</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>Pager</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>canallowguestoutdial</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>allowguestoutdial</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>VLanguage</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>English (US)</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>fEndMtgWarn</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>fMtgExtendPrompts</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>CanChangeMtgID</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>No</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>RsvnlessCnfg</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>0</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>RsvnlessCnfgGD</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>254</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>AllowVideoSched</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>AllowInternetAccess</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>No</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>VideoEndPtBandwidth</td>
<td><em>Not supported.</em> Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td>—</td>
</tr>
<tr>
<td>Field Name</td>
<td>Description</td>
<td>Size and Type of Value</td>
</tr>
<tr>
<td>-----------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>------------------------</td>
</tr>
<tr>
<td>bountyUser</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>TRUE</strong>.</td>
<td></td>
</tr>
<tr>
<td>isLocalUser</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>Yes</strong>.</td>
<td></td>
</tr>
<tr>
<td>EmailFormat</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>txt</strong>.</td>
<td></td>
</tr>
<tr>
<td>ReserveVoiceLicenses</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>LockedProfileTime</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>0</strong>.</td>
<td></td>
</tr>
<tr>
<td>CanReserveVideoPorts</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>PreferVideo</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>PreferDataConf</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>Yes</strong>.</td>
<td></td>
</tr>
<tr>
<td>FRsvnlessAllowInternetAcc</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>Yes</strong>.</td>
<td></td>
</tr>
<tr>
<td>FStartPeopleInWR</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>No</strong>.</td>
<td></td>
</tr>
<tr>
<td>attendMode</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>attendPasswdRequired</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>No</strong>.</td>
<td></td>
</tr>
<tr>
<td>announceQArr</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>videoTypes</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>mtgEntryMode</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>dataConfClientType</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
<tr>
<td>allowVideoSched</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter <strong>gd</strong>.</td>
<td></td>
</tr>
</tbody>
</table>
### Import and Export Data Specifications for Video Terminal Profiles (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>endpointType</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter 4.</td>
<td>—</td>
</tr>
<tr>
<td>FVideoMCUOnly</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value.</td>
<td>—</td>
</tr>
<tr>
<td>videoAttPref</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter gd.</td>
<td>—</td>
</tr>
<tr>
<td>videoTermClass</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, leave this field blank.</td>
<td>—</td>
</tr>
<tr>
<td>attPref</td>
<td>Not supported. Import requirement: Do not modify this field from the exported value. If you import a new profile, enter 1.</td>
<td>—</td>
</tr>
<tr>
<td>rcvNMaskEn</td>
<td>See Can receive notifications.</td>
<td>• 0—No</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• 1—Yes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>• gd</td>
</tr>
</tbody>
</table>

1. gd = group default
2. VTP = video terminal profile

**Related Topics**

- Exporting Video Terminal Profiles in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
- Adding or Editing Video Terminal Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module
- Deleting Video Terminal Profiles by Import in the Importing Data into Cisco Unified MeetingPlace module
Meetings—Raw Data Export and Import Specifications

Note

The first line in the export file specifies the Cisco Unified MeetingPlace version. If you want to import this file or use this file as a template for importing data, then you must not modify this line.

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>ConfNum</td>
<td>Unique conference number assigned to this meeting after it was successfully scheduled. Import requirement: Must be a unique value.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>StartDateTimeOfConf</td>
<td>The date and time for which this meeting is scheduled.</td>
<td>MM/DD/YYYY HH:MM</td>
</tr>
<tr>
<td>SchedulerUid</td>
<td>User ID of the meeting owner. Import requirement: Must be a valid User ID.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>ContactUid</td>
<td>User ID of delegate of the meeting owner. Import requirement: Must be a valid User ID.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>DialableConfID</td>
<td>Meeting ID.</td>
<td>0 to 9 ASCII text characters</td>
</tr>
<tr>
<td>LastModified</td>
<td>Date and time when the meeting information was last modified.</td>
<td>MM/DD/YYYY HH:MM</td>
</tr>
<tr>
<td>OriginallyScheduled</td>
<td>Date and time when this meeting was originally scheduled.</td>
<td>MM/DD/YYYY HH:MM</td>
</tr>
<tr>
<td>PartRecordTimeUsed</td>
<td>Amount of time, in seconds, of participant name recordings.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>NameRecordTimeUsed</td>
<td>Amount of time, in seconds, of the recorded meeting name.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>AgendaRecordTimeUsed</td>
<td>Amount of time, in seconds, of the meeting agenda recording.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>VRecordRecordTimeUsed</td>
<td>Amount of time, in seconds, of the meeting recording.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>VIntroTimeUsedSecs</td>
<td>Amount of time, in seconds, of the meeting introduction recording.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>TName</td>
<td>Meeting subject.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>SchedulerTimeZone</td>
<td>Time zone of the meeting scheduler. Import requirement: The integer value in the import file must match a value defined by Cisco Unified MeetingPlace. Make sure you use a previously exported value.</td>
<td>0 to 17 ASCII text characters</td>
</tr>
<tr>
<td>TAheada</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>VName</td>
<td>Whether the meeting name was recorded.</td>
<td>Recorded/Not Recorded</td>
</tr>
<tr>
<td>VAgenda</td>
<td>Whether the meeting agenda was recorded.</td>
<td>Recorded/Not Recorded</td>
</tr>
<tr>
<td>VRecord</td>
<td>Whether the meeting was recorded.</td>
<td>Recorded/Not Recorded</td>
</tr>
</tbody>
</table>
### Table 4  Import and Export Data Specifications for Meetings (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>VMeeetingIntro</td>
<td>Whether the meeting introduction was recorded.</td>
<td>Recorded/Not Recorded</td>
</tr>
<tr>
<td>VoiceStorageEndTime</td>
<td>When the following items for this meeting will be deleted from the Application Server:</td>
<td>MM/DD/YYYY HH:MM</td>
</tr>
<tr>
<td></td>
<td>• Voice agenda</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Conference name</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Meeting introduction</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Voice recording</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Attachment records</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Recorded participant names</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Voice storage reservation</td>
<td></td>
</tr>
<tr>
<td></td>
<td>This date cannot be changed, and it is set to 7 days after the meeting ends.</td>
<td></td>
</tr>
<tr>
<td>ActSrtTimeOfConf</td>
<td>When the meeting started.</td>
<td>MM/DD/YYYY HH:MM</td>
</tr>
<tr>
<td></td>
<td>Note</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If meeting was not attended, field displays time zero</td>
<td></td>
</tr>
<tr>
<td></td>
<td>(midnight January 1, 1970 converted to server's time zone).</td>
<td></td>
</tr>
<tr>
<td>TotConfPortSec</td>
<td>Accumulated number of seconds for all voice ports that were in the meeting.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td></td>
<td>For example, if three ports were in the meeting for 5, 6, and 7 seconds,</td>
<td></td>
</tr>
<tr>
<td></td>
<td>respectively, then</td>
<td></td>
</tr>
<tr>
<td></td>
<td>TotConfPortSec = 5 + 6 + 7 = 18.</td>
<td></td>
</tr>
<tr>
<td>ActLenOfConf</td>
<td>Actual length of the meeting, in minutes.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>nPartRegistered</td>
<td>Number of users that were either invited to or joined the meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>ActnParticipants</td>
<td>Number of users who attended this meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>PeakNumberOfParticipants</td>
<td>Peak number of participants in this meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>PeakNumberOfPorts</td>
<td>Peak number of voice ports used during this meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>OrigNumberOfPorts</td>
<td>Number of voice ports planned for this meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>nPartAttemptsAfterConfLocked</td>
<td>The number of participants that tried to join the meeting after it was</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td></td>
<td>locked.</td>
<td></td>
</tr>
<tr>
<td>ReqLengthOfConf</td>
<td>The requested number of minutes for this meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>nPortsRequired</td>
<td>The number of voice ports required for this meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>nPartsRequested</td>
<td>The number of participants invited to the meeting.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>MaxDaysReOccuring</td>
<td>Number of instances of reoccurrence.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td></td>
<td>For example, a meeting that occurs monthly for 2 years will have a value of</td>
<td></td>
</tr>
<tr>
<td></td>
<td>12.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4  Import and Export Data Specifications for Meetings (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>MeetingJoinRestriction</td>
<td>Who can join the meeting.</td>
<td>Anyone/Users/Invited Users/None</td>
</tr>
<tr>
<td>DefaultAbility</td>
<td>The default speaking ability of uninvited participants in the meeting.</td>
<td>SPEAKERPLUS/ MUTED SPEAKERPLUS/ SPEAKER/ MUTED SPEAKER/ LISTENER</td>
</tr>
<tr>
<td></td>
<td>See the <strong>SpeakingAbility</strong> meeting participant information field.</td>
<td></td>
</tr>
<tr>
<td>ReOccuringConference</td>
<td>Frequency of meeting recurrence.</td>
<td>ONCE/DAILY/WEEKLY/ MONTHLY/WEEKDAYS/ PERMANENT/BIWEEKLY/ MONTHLYBYDAYOFWEEK1/ MONTHLYBYDAYOFWEEK2/ MONTHLYBYDAYOFWEEK3/ MONTHLYBYDAYOFWEEK4/ MONTHLYBYDAYOFWEEKLAST/ SPECIFIEDWEEKDAYS</td>
</tr>
<tr>
<td>MtgNoteRestriction</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>fPasswordRequired</td>
<td>Whether the meeting requires a password.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fNamedIntroduction</td>
<td>Announcement played when participants join the meeting.</td>
<td>Beep/BeepName/None</td>
</tr>
<tr>
<td>fNamedDisconnect</td>
<td>Announcement played when participants leave the meeting.</td>
<td>Beep/BeepName/None</td>
</tr>
<tr>
<td>fScreenedIntroduction</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>fRecordConference</td>
<td>Whether this meeting is recorded.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fPosted</td>
<td>Whether the recording of this meeting is posted.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fQuickMtgEntryAllowed</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>fPasswordRequiredOnOD</td>
<td>Whether dial-out participants must enter <strong>Profile passwords</strong> before being admitted into the voice meeting.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>nUserVUIMtgNotesAccesses</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>nUserGUIMtgNotesAccesses</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>nGuestMtgNotesAccesses</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>SchedulingClient</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>CurAttRefID</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>CurNumDataAtt</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>CurNumVoiceAtt</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>CurVoiceAttSpace</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>CurDataAttSpace</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>nVoiceAttAdded</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>nDataAttAdded</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
<tr>
<td>PeaknVoiceAtt</td>
<td><em>Not supported.</em></td>
<td></td>
</tr>
</tbody>
</table>
### Table 4  Import and Export Data Specifications for Meetings (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PeaknDataAtt</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>PeakAttVoiceSpace</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>PeakAttDataSpace</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>CurAttNameHeaderSpace</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>MaxAttachments</td>
<td>Maximum number of attachments for this meeting. 1 to 9 numeric characters</td>
<td></td>
</tr>
<tr>
<td>fBAgendaAttAvail</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fAutoStartRecord</td>
<td>Whether the system automatically starts recording the meeting. Yes/No</td>
<td></td>
</tr>
<tr>
<td>fDisableRollCall</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>SendNotAboutMtgs</td>
<td>Whether an e-mail notification was sent when this meeting was scheduled.</td>
<td>Yes/No</td>
</tr>
<tr>
<td></td>
<td>Notifications are never sent for reservationless meetings.</td>
<td></td>
</tr>
<tr>
<td>AutoDistributeAtt</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>DefNotPriority</td>
<td>Priority given to the e-mail notifications sent when this meeting is scheduled. Low/Normal/Urgent</td>
<td></td>
</tr>
<tr>
<td>SendNotAboutMtgChngs</td>
<td>Whether e-mail notifications are sent when the following meeting parameters change: Yes/No</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Date or time</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Password</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Meeting ID</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• List of invitees</td>
<td></td>
</tr>
<tr>
<td>SendInviteListWithNot</td>
<td>Whether to include a list of meeting invitees in e-mail notifications for this meeting. Yes/No</td>
<td></td>
</tr>
<tr>
<td>SendMtgPwdWithNot</td>
<td>Whether to include the meeting password in e-mail notifications for this meeting. Yes/No</td>
<td></td>
</tr>
<tr>
<td>fUsedBlastOutdial</td>
<td>Whether the system dials out to all meeting invitees. Yes/No</td>
<td></td>
</tr>
<tr>
<td>BillCode</td>
<td>Billing code applied to this meeting. 0 to 18 alphanumeric characters</td>
<td></td>
</tr>
<tr>
<td>fTAgendaAttAvail</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fVAgendaAttAvail</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>PriUnitNum</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>PriSiteNum</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>concurrentquestions</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>announceqarr</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>announceqdep</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fqnadisabled</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fautoproenabled</td>
<td>Not supported.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4: Import and Export Data Specifications for Meetings (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>fstartpeopleinwr</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>numdataparts</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fchatsession</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fismsgseminartype</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>fallowguestview</td>
<td>Whether this meeting is publicly listed in the end-user web interface.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>tottimesfgiven</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>qnanotify</td>
<td>Whether to play an instructional Q&amp;A prompt as people join this meeting.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>PeakVRecordTimeUsed</td>
<td>Peak number of recording seconds used by a meeting over its lifetime. A historical statistic used for billing purposes.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>MPConnectionType</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>nRemoteServersRegistered</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>TotnRSsInvited</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>ActnRSs</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>PeakNumberOfRSs</td>
<td>Not supported.</td>
<td></td>
</tr>
<tr>
<td>allowguestoutdial</td>
<td>Whether guest users can dial out from this meeting.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>TotDCConfPortSec</td>
<td>Total number of seconds that the web meeting room was used by this meeting.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>VLanguage</td>
<td>Meeting language, which is used for voice prompts that are heard by all meeting participants.</td>
<td>0 to 128 alphanumeric characters</td>
</tr>
<tr>
<td>EncryptedConfPwd</td>
<td>Encrypted meeting password.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>StartDateTimeOfConfGMT</td>
<td>Date on which the meeting is scheduled to occur.</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>fEndMtgWarn</td>
<td>Whether the end-of-meeting announcement is played in this meeting.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fMtgExtendPrompts</td>
<td>Whether meeting-extension announcements are played in this meeting.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>ActSrtTimeOfDataConf</td>
<td>Date and time at which the web meeting room meeting started.</td>
<td>MM/DD/YYYY HH:MM</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>If this is a voice-only meeting (no web meeting room), this field displays a dummy value.</td>
<td></td>
</tr>
<tr>
<td>ActLenOfDataConf</td>
<td>The actual length of the web meeting, in minutes.</td>
<td>1 to 9 numeric characters</td>
</tr>
</tbody>
</table>
| ConfExtensionFailCode | Failure code that indicates why an attempted meeting extension failed. See Table 9.  
If there were no attempts to extend the meeting, then this value is 0. | 1 to 6 numeric characters |
### Field Name | Description | Size and Type of Value
--- | --- | ---
NumSuccConfExtensions | Number of times that the meeting was successfully extended. | 1 to 9 numeric characters
MeetingType | Descriptor for meetings.  
- 0—Scheduled non-lecture-style  
- 1—Reservationless  
- 2—Reserve All Ports (RAP)  
- 3—Scheduled lecture-style  
- 4—Web only | Numeric—range is 0 to 4
RsvnlessStartID | User ID of the person who initiates the reservationless meeting.  
This field applies only to reservationless meetings. | 0 to 17 alphanumeric characters
OutdialFirstCall | Whether the system dials out to all invitees after the first person joins the meeting.  
This field applies only to continuous meetings, which can be scheduled only by system administrators. | Yes/No
nVideoPortsReq | The number of video ports required for this meeting.  
Import restriction: This value cannot exceed the number of licensed ports. | 1 to 4 numeric characters
ActNumVideoPorts | Number of video participants in this meeting. | 1 to 4 numeric characters
TotVideoPortSecs | Total number of seconds that video endpoints were in the meeting.  
For example, if three video endpoints attended the meeting for 5, 6, and 7 seconds, respectively, then \( \text{TotVideoPortSec} = 5 + 6 + 7 = 18. \) | 1 to 9 numeric characters
AllowInternetAccess | Whether the meeting is accessible by anyone on the Internet and appears on the external Web Server. | Yes/No
nDCPortsRequired | Number of web ports required for this meeting to be scheduled.  
Import restriction: This value cannot exceed the number of licensed ports. | 1 to 4 numeric characters
meetingInvitees | List of User IDs or e-mail addresses of meeting invitees, separated by a semicolon (;).  
Example: user1;user2@example.com;user3;user4  
Import restriction: The number of invitees cannot exceed the value in the Maximum ports per scheduled meeting field on the Meeting Configuration Page. | Alphanumeric characters
allowVideoConf | Whether video is enabled for this meeting. | Yes/No
Table 4  Import and Export Data Specifications for Meetings (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>external</td>
<td>Identical to AllowInternetAccess.</td>
<td>Yes/No</td>
</tr>
<tr>
<td>videoTypeId</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>videoTypeName</td>
<td></td>
<td></td>
</tr>
<tr>
<td>videoMinBitRate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>videoMaxBitRate</td>
<td></td>
<td></td>
</tr>
<tr>
<td>videoCodec</td>
<td></td>
<td></td>
</tr>
<tr>
<td>OrigNvideoPorts</td>
<td>Number of originally scheduled video ports.</td>
<td>1 to 4 numeric characters</td>
</tr>
<tr>
<td>fMeetingTemplateID</td>
<td>Number that identifies the meeting template used for this meeting. The meeting template specifies the web meeting room layout.</td>
<td>Any numeric value up to 9 characters</td>
</tr>
<tr>
<td>fWebOnly</td>
<td>Whether participants are allowed to enter only the web meeting room (no audio participants).</td>
<td>Yes/No</td>
</tr>
<tr>
<td>fAllowAnyoneToView</td>
<td>Whether anyone can search to find this meeting through the end-user web interface. If set to No, then even system administrators will not be able to see the meeting.</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>

Related Topics

- Exporting Meetings in the Running Reports and Exporting Data from Cisco Unified MeetingPlace module
- Scheduling Meetings by Import in the Importing Data into Cisco Unified MeetingPlace module
- Canceling Meetings by Import in the Importing Data into Cisco Unified MeetingPlace module

Outgoing Calls Information—Raw Data Export Specifications

Table 5  Export Data Specifications—Outgoing Calls Information

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>StartTimeOfCall</td>
<td>Date and time when the system placed the call.</td>
<td>MM/DD/YYYY HH:MM</td>
</tr>
<tr>
<td>uid</td>
<td>User ID of the person who initiated the dial-out call.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>ConfNum</td>
<td>See ConfNum.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>nSeconds</td>
<td>Duration of the outgoing call, in seconds.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>CalledDest</td>
<td>Telephone number that was dialed.</td>
<td>No more than 32 ASCII digits</td>
</tr>
<tr>
<td>fBlastOutdial</td>
<td>Whether this was a blast dial-out call.</td>
<td>Yes/No</td>
</tr>
</tbody>
</table>
Meeting Participant Information—Raw Data Export Specifications

### Table 5  Export Data Specifications—Outgoing Calls Information (continued)

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>UpdateTime</td>
<td>When this record was most recently updated.</td>
<td>MM/DD/YY HH:MM</td>
</tr>
<tr>
<td>PartID</td>
<td>Unique number that identifies each meeting participant. The meeting owner</td>
<td>0 to 17 ASCII text characters</td>
</tr>
<tr>
<td></td>
<td>is assigned the number 0. The first non-owner participant is assigned the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>number 1. As each participant joins, the next incremental number is assigned.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If a profiled user leaves and rejoins a meeting, the same PartID is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>If a guest user leaves and rejoins a meeting, a new PartID is used.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>A PartID of -851969 indicates that the user did not actually join the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>meeting.</td>
<td></td>
</tr>
</tbody>
</table>

### Related Topics
- Running Reports and Exporting Data from Cisco Unified MeetingPlace module

### Meeting Participant Information—Raw Data Export Specifications

### Table 6  Export Data Specifications—Meeting Participant Information

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PartId</td>
<td>See PartID.</td>
<td>0 to 17 ASCII text characters</td>
</tr>
<tr>
<td>ConfNum</td>
<td>See ConfNum.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>uid</td>
<td>User ID of the meeting participant.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>MeetingId</td>
<td>Meeting ID.</td>
<td>Numeric characters</td>
</tr>
<tr>
<td>StartTimeOfConf</td>
<td>Date and time when the meeting started.</td>
<td>MM/DD/YYYY hh:mm</td>
</tr>
<tr>
<td>nVSecInConf</td>
<td>Amount of time, in seconds, that the participant spent in the voice portion</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td></td>
<td>of the meeting.</td>
<td></td>
</tr>
<tr>
<td>nWFSecInConf</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>nSecsOutboundCalls</td>
<td>Amount of time, in seconds, that the participant spent in a call that was</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td></td>
<td>dialed out by the system.</td>
<td></td>
</tr>
<tr>
<td>VNameHeader</td>
<td>Whether the name of the participant was recorded.</td>
<td>Recorded/Not_Recorded</td>
</tr>
<tr>
<td>nOutboundCalls</td>
<td>Number of dial-out calls initiated by this participant</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>nRetries</td>
<td>Number of dial-out retries initiated by this participant</td>
<td>An unsigned integer</td>
</tr>
</tbody>
</table>
### Table 6  
**Export Data Specifications — Meeting Participant Information (continued)**

<table>
<thead>
<tr>
<th>Field Name</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>TNameHeader</td>
<td><strong>First name</strong> and <strong>Last name</strong> of the meeting participant. For unprofiled</td>
<td>0 to 64 alphanumeric</td>
</tr>
<tr>
<td></td>
<td>participants, this displays one of the following:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Name the guest user enters to join the meeting from the end-user web</td>
<td></td>
</tr>
<tr>
<td></td>
<td>interface.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• “Guest User” followed by the phone number or extension from which the</td>
<td></td>
</tr>
<tr>
<td></td>
<td>user dials in.</td>
<td></td>
</tr>
<tr>
<td>SpeakingAbility</td>
<td>Speaking ability of the participant upon leaving the meeting. Upon</td>
<td>• LISTENER</td>
</tr>
<tr>
<td></td>
<td>entering the meeting, the participant has one of the following speaking</td>
<td>• SPEAKER</td>
</tr>
<tr>
<td></td>
<td>abilities:</td>
<td>• SPEAKERPLUS</td>
</tr>
<tr>
<td></td>
<td>• LISTENER—Audience/Listener</td>
<td>• MUTED_SPEAKERPLUS</td>
</tr>
<tr>
<td></td>
<td>• SPEAKER—Audience/Speaker or Presenter/Speaker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SPEAKERPLUS—Moderator/Speaker</td>
<td></td>
</tr>
<tr>
<td></td>
<td>In collaborative meetings, all participants are speakers. The moderator</td>
<td></td>
</tr>
<tr>
<td></td>
<td>may change the speaking abilities of participants via lecture-style</td>
<td></td>
</tr>
<tr>
<td></td>
<td>meeting controls, for example:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Opening the floor converts all listeners to speakers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Closing the floor converts all speakers to listeners.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Moderators are always speakers.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Note, however, that the mute state is controlled by the individual</td>
<td></td>
</tr>
<tr>
<td></td>
<td>participant, not the moderator.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Each speaker chooses whether or not to be muted. Listeners cannot mute</td>
<td></td>
</tr>
<tr>
<td></td>
<td>or unmute themselves.</td>
<td></td>
</tr>
<tr>
<td>nVUIODsMade</td>
<td>Number of dial-out calls that this participant initiated from the</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td></td>
<td>TUI¹.</td>
<td></td>
</tr>
<tr>
<td>nTimesQAAsked</td>
<td>Number of times a question was asked by the participant.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>nTimesFGiven</td>
<td>Number of times the floor was given to the participant.</td>
<td>Integer</td>
</tr>
<tr>
<td>UpdateTime</td>
<td>When this record was most recently updated.</td>
<td>MM/DD/YYYY hh:mm</td>
</tr>
<tr>
<td>nDCSecInConf</td>
<td>Amount of time, in seconds, that the user spent in the web meeting room.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>nSecInMTGNotes</td>
<td>Amount of time, in seconds, that the user spent listening to recordings</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td></td>
<td>and other notes for this meeting.</td>
<td></td>
</tr>
</tbody>
</table>

1. TUI = telephone user interface

**Related Topics**
- Running Reports and Exporting Data from Cisco Unified MeetingPlace module
Meeting Participant Join Leave Information—Raw Data Export Specifications

Note
This report provides a separate entry for each Device used by a meeting participant.

Table 7  
Export Data Specifications—Meeting Participant Join Leave Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>PartID</td>
<td>See PartID.</td>
<td>0 to 17 ASCII text characters</td>
</tr>
<tr>
<td>UserID</td>
<td>User ID of the meeting participant.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>ConfNum</td>
<td>See ConfNum.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>MeetingID</td>
<td>Meeting ID.</td>
<td></td>
</tr>
<tr>
<td>gmStartDate</td>
<td>Date on which the user joined the meeting.</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>gmStartTime</td>
<td>Time at which the user joined the meeting.</td>
<td>HH:MM:SS AM/PM</td>
</tr>
<tr>
<td>gmEndDate</td>
<td>Date on which the user left the meeting.</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>gmEndTime</td>
<td>Time at which the user left the meeting.</td>
<td>HH:MM:SS AM/PM</td>
</tr>
<tr>
<td>Device</td>
<td>Device identifier or port number:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 0 to 1151—voice port</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4080—MeetingPlace Conference Manager</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4081—Cisco Unified MeetingPlace Web Conferencing</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4082—Share pod in web meeting</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• 4084—Cisco Unified MeetingPlace Video</td>
<td></td>
</tr>
<tr>
<td>nIncDigits</td>
<td>Number of DNIS digits that were received from the PBX.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>IncDigits</td>
<td>String of DNIS digits received from the PBX.</td>
<td>Numerical string of up to 24 digits</td>
</tr>
<tr>
<td>AttachmentID</td>
<td>Not supported.</td>
<td>Not supported.</td>
</tr>
<tr>
<td>nANIDigits</td>
<td>Number of alpha-numeric characters in the display name, or the number of ANI digits that were received from the PBX. The display name takes precedence; if not present, the ANI value is used.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>ANIDigits</td>
<td>Alpha-numeric characters in the display name, or the string of ANI digits received from the PBX. The display name takes precedence; if not present, the ANI value is used.</td>
<td>Alpha-numeric string of up to 24 digits</td>
</tr>
</tbody>
</table>

Related Topics
- Running Reports and Exporting Data from Cisco Unified MeetingPlace module
Scheduling Failures Information—Raw Data Export Specifications

- Export Data Specifications—Scheduling Failures Information
- Failure Code Reference: Scheduling Failures Information

Table 8  
Export Data Specifications—Scheduling Failures Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>SchedulerUid</td>
<td>User ID of the meeting owner.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>SchedulingTime</td>
<td>Date and time when the user tried to schedule the meeting.</td>
<td>MM/DD/YYYY hh:mm</td>
</tr>
<tr>
<td>MtgStartTime</td>
<td>Date and time that the user requested for the meeting to begin.</td>
<td>MM/DD/YYYY hh:mm</td>
</tr>
<tr>
<td>DialableConfID</td>
<td>Meeting ID.</td>
<td>0 to 9 ASCII text characters</td>
</tr>
<tr>
<td>NumOfPortsRqsted</td>
<td>Number of voice ports requested for the failed meeting.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>MtgLenthInMin</td>
<td>Number of minutes that the user requested for the meeting length.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>FailCode</td>
<td>Failure code that describes why the meeting could not be scheduled. See Table 9.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>ErrorString</td>
<td>A text string message that is displayed to the user. This message corresponds to the FailCode.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>FailSeqNum</td>
<td>Tracks multiple failure attempts for the same meeting.</td>
<td>An unsigned integer</td>
</tr>
<tr>
<td>UniqueConfNum</td>
<td>Unique conference number assigned to this meeting after it was successfully scheduled. This is 0 for meetings that are not scheduled successfully.</td>
<td>An unsigned integer</td>
</tr>
</tbody>
</table>

Table 9  
Failure Code Reference: Scheduling Failures Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>5122</td>
<td>Generic code for any error found from internal reservation mechanism.</td>
<td></td>
</tr>
<tr>
<td>5129</td>
<td>Original resource reservation cannot be found.</td>
<td></td>
</tr>
<tr>
<td>5154</td>
<td>The server cannot commit the extensions because of a failure to save the extension record to the database.</td>
<td></td>
</tr>
<tr>
<td>5155</td>
<td>Server did not extend meeting because of one of these reasons:</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Less than two participants were in the voice and web conferencing sessions.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The meeting was extended to more than 24 hours.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• The Extend Meeting parameter was set to 0 minutes.</td>
<td></td>
</tr>
<tr>
<td>5190</td>
<td>The Meeting ID conflicts with an existing meeting.</td>
<td></td>
</tr>
<tr>
<td>5209</td>
<td>The meeting was terminated.</td>
<td></td>
</tr>
<tr>
<td>5291</td>
<td>There were not enough video resources.</td>
<td></td>
</tr>
<tr>
<td>5295</td>
<td>Not enough ports are available.</td>
<td></td>
</tr>
<tr>
<td>5318</td>
<td>The meeting could not be scheduled because the recording would have been too long.</td>
<td></td>
</tr>
</tbody>
</table>
Table 9  
Failure Code Reference: Scheduling Failures Information (continued)

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>131158</td>
<td>One person remains in the meeting.</td>
</tr>
<tr>
<td>131159</td>
<td>Meeting was extended more than 24 hours.</td>
</tr>
<tr>
<td>131262</td>
<td>Failed to extend because of meeting ID conflict.</td>
</tr>
<tr>
<td>131198</td>
<td>Failed to extend because of lack of voice ports.</td>
</tr>
<tr>
<td>131199</td>
<td>Failed to extend because of lack of recording space.</td>
</tr>
</tbody>
</table>

Related Topics
- [Running Reports and Exporting Data from Cisco Unified MeetingPlace](#) module

Scheduling Statistics Information—Raw Data Export Specifications

Table 10  
Export Data Specifications—Scheduling Statistics Information

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>fNumSchedSuccesses</td>
<td>Number of scheduling operations that were successful. For example, suppose that a user successfully schedules a recurring meeting with 100 instances from the end-user web interface. This would add 1 to fNumSchedSuccesses and 100 to fNumSchedWeb.</td>
<td>Up to 16 numeric integers</td>
</tr>
<tr>
<td>fNumSchedWindows</td>
<td>Number of meetings scheduled from Microsoft Windows computers.</td>
<td>Up to 16 numeric integers</td>
</tr>
<tr>
<td>fNumSchedMac</td>
<td>Number of meetings scheduled from Macintosh computers.</td>
<td>Up to 16 numeric integers</td>
</tr>
<tr>
<td>fNumSchedNotes</td>
<td>Number of meeting scheduled from IBM Lotus Notes.</td>
<td>Up to 16 numeric integers</td>
</tr>
<tr>
<td>fNumSchedVUI</td>
<td>Number of meetings scheduled from the TUI.</td>
<td>Up to 16 numeric integers</td>
</tr>
<tr>
<td>fNumSchedWeb</td>
<td>Number of meetings scheduled from the end-user web interface.</td>
<td>Up to 16 numeric integers</td>
</tr>
<tr>
<td>fSumSchedClients</td>
<td>Total number of meetings that were successfully scheduled, specifically, the sum of these values: fNumSchedWindows, fNumSchedMac, fNumSchedNotes, fNumSchedVUI, and fNumSchedWeb.</td>
<td>Up to 16 numeric integers</td>
</tr>
</tbody>
</table>

Related Topics
- [Running Reports and Exporting Data from Cisco Unified MeetingPlace](#) module
Scheduling Activity By User Information—Raw Data Export Specifications

Table 11  Export Data Specifications—Scheduling Activity By User Information

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>dialableConfId</td>
<td>Meeting ID.</td>
<td>0 to 9 ASCII text characters</td>
</tr>
<tr>
<td>confname</td>
<td>Meeting subject.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>schedulerName</td>
<td>First name and Last name of the meeting scheduler.</td>
<td>0 to 64 alphanumeric characters</td>
</tr>
<tr>
<td>dateScheduled</td>
<td>Date when the user scheduled the meeting.</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>timeScheduled</td>
<td>Time when the user scheduled the meeting.</td>
<td>hh:mm</td>
</tr>
<tr>
<td>conflength</td>
<td>Requested number of minutes for this meeting.</td>
<td>Numeric</td>
</tr>
<tr>
<td>nPortsRequired</td>
<td>Number of voice ports required for this meeting.</td>
<td>Numeric</td>
</tr>
<tr>
<td>groupIdNumber</td>
<td>Number of user group to which this user belongs.</td>
<td>1 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>groupName</td>
<td>Name of user group to which this user belongs.</td>
<td>1 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>userID</td>
<td>User ID of this user.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
</tbody>
</table>

Related Topics
- Running Reports and Exporting Data from Cisco Unified MeetingPlace module

Continuous Meetings Information—Raw Data Export Specifications

Table 12  Export Data Specifications—Continuous Meetings Information

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>confnum</td>
<td>Unique conference number assigned to this meeting after it was successfully scheduled.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>DialableConfID</td>
<td>Meeting ID.</td>
<td>0 to 9 ASCII text characters</td>
</tr>
<tr>
<td>ConfName</td>
<td>Meeting subject.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>organizerName</td>
<td>First name and Last name of the meeting owner.</td>
<td>0 to 64 alphanumeric characters</td>
</tr>
</tbody>
</table>
### Table 12 Export Data Specifications—Continuous Meetings Information (continued)

<table>
<thead>
<tr>
<th>Header Field</th>
<th>Description</th>
<th>Size and Type of Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>contactName</td>
<td>User ID of delegate that is assigned to the meeting owner.</td>
<td>1 to 30 alphanumeric characters</td>
</tr>
<tr>
<td>billCode</td>
<td>See Billing code.</td>
<td>0 to 17 alphanumeric characters</td>
</tr>
<tr>
<td>meetingType</td>
<td>See MeetingType.</td>
<td>Numeric—range is 0 to 4</td>
</tr>
<tr>
<td>startdatesched</td>
<td>Date on which the meeting is scheduled to begin.</td>
<td>MM/DD/YYYY</td>
</tr>
<tr>
<td>starttimesched</td>
<td>Time at which the meeting is scheduled to begin.</td>
<td>hh:mm</td>
</tr>
<tr>
<td>actnParticipants</td>
<td>The number of users who have attended this meeting.</td>
<td>Any numeric value</td>
</tr>
<tr>
<td>actlenofconf</td>
<td>Total number of seconds for which the continuous meeting had at least one participant.</td>
<td>1 to 9 numeric characters</td>
</tr>
<tr>
<td>recmins</td>
<td>Not supported.</td>
<td>—</td>
</tr>
<tr>
<td>peaknparticipants</td>
<td>Peak number of participants in this meeting.</td>
<td>Any numeric value</td>
</tr>
<tr>
<td>nUserVUIMtgNotesAccesses</td>
<td>Number of times that the meeting recordings and attachments have been accessed from the TUI.</td>
<td>Any numeric value</td>
</tr>
<tr>
<td>nGuestMtgNotesAccesses</td>
<td>Number of times that the meeting recordings and attachments have been accessed by guest users.</td>
<td>Any numeric value</td>
</tr>
<tr>
<td>nUserGUIMtgNotesAccesses</td>
<td>Number of times that the meeting recordings and attachments have been accessed from the end-user web interface.</td>
<td>Any numeric value</td>
</tr>
<tr>
<td>fconfportmins</td>
<td>Number of voice ports per minute used by the meeting.</td>
<td>Any numeric value</td>
</tr>
<tr>
<td>fdconfportmins</td>
<td>Number of web ports per minute used by the meeting.</td>
<td>Any numeric value</td>
</tr>
<tr>
<td>schedulerLastName</td>
<td>Last name of the meeting scheduler.</td>
<td>0 to 32 alphanumeric characters</td>
</tr>
</tbody>
</table>

**Related Topics**

- Running Reports and Exporting Data from Cisco Unified MeetingPlace module
# Time Zone Mapping Between Cisco WebEx and Cisco Unified MeetingPlace

**Release 7.1**  
**Revised: April 3, 2011 8:31 pm**

Use this information with the Integrating Cisco Unified MeetingPlace with Cisco WebEx module.

## Table 1  Time Zone Mapping Between Cisco Unified MeetingPlace and Cisco WebEx

<table>
<thead>
<tr>
<th>Cisco Unified MeetingPlace Time Zone</th>
<th>Cisco WebEx Time Zone</th>
<th>ID</th>
<th>GMT Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeZoneName_Africa/Abidjan=West Africa (GMT/WET)</td>
<td></td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Africa/Windhoek=Namibia</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Africa/Ceuta=Spanish Morocco</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Africa/Tunis=Tunisia</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Africa/Bangui=West Central Africa (GMT+1/CET)</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Africa/Blantyre=Central Africa (GMT+2/EET)</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Africa/Cairo=Egypt</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Africa/Johannesburg=South Africa, Lesotho &amp; Swaziland</td>
<td></td>
<td>29</td>
<td>2</td>
</tr>
<tr>
<td>timeZoneName_Africa/Addis_Ababa=East Africa (GMT+3)</td>
<td></td>
<td>3</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Jerusalem=Israel</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Amman=Jordan</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Beirut=Lebanon</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Gaza=Palestine</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Damascus=Syria</td>
<td></td>
<td>2</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Istanbul=Turkey</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Tbilisi=Georgia</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Baghdad=Iraq</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Asia/Aden=Saudi Arabia, Bahrain, Kuwait, Quatar &amp; Yemen</td>
<td></td>
<td>32</td>
<td>3</td>
</tr>
<tr>
<td>timeZoneName_Asia/Tehran=Iran</td>
<td></td>
<td>35</td>
<td>3.3</td>
</tr>
</tbody>
</table>
### Table 1: Time Zone Mapping Between Cisco Unified MeetingPlace and Cisco WebEx (continued)

<table>
<thead>
<tr>
<th>Cisco Unified MeetingPlace Time Zone</th>
<th>Cisco WebEx Time Zone Locations</th>
<th>ID</th>
<th>GMT(^1) Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeZoneName_Asia/Yerevan=Armenia</td>
<td>Arabian</td>
<td>Abu Dhabi, Muscat4</td>
<td>36</td>
</tr>
<tr>
<td>timeZoneName_Asia/Baku=Azerbaijan</td>
<td>Bakul</td>
<td>Bakul4</td>
<td>37</td>
</tr>
<tr>
<td>timeZoneName_Asia/Dubai=Dubai &amp; Oman</td>
<td>Arabian</td>
<td>Abu Dhabi, Muscat4</td>
<td>36</td>
</tr>
<tr>
<td>timeZoneName_Asia/Kabul=Afghanistan</td>
<td>Afghanistan</td>
<td>Kabul4.5</td>
<td>38</td>
</tr>
<tr>
<td>timeZoneName_Asia/Karachi=Pakistan, Tajikistan, Turkmenistan, Uzbekistan &amp; Western Kazakhstan</td>
<td>West Asia</td>
<td>Islamabad5</td>
<td>40</td>
</tr>
<tr>
<td>timeZoneName_Asia/Bishkek=Russia: Kyrgyzstan &amp; Yekaterinburg</td>
<td>West Asia</td>
<td>Ekaterinburg5.5</td>
<td>39</td>
</tr>
<tr>
<td>timeZoneName_Asia/Calcutta=India</td>
<td>India</td>
<td>Bombay5.5</td>
<td>41</td>
</tr>
<tr>
<td>timeZoneName_Asia/Katmandu=Nepal</td>
<td>India</td>
<td>Kabul4.5</td>
<td>38</td>
</tr>
<tr>
<td>timeZoneName_Asia/Novosibirsk=Russia: Novosibirsk, Omsk</td>
<td>Russia</td>
<td>Novosibirsk, Omsk</td>
<td>6</td>
</tr>
<tr>
<td>timeZoneName_Asia/Rangoon=Myanmar</td>
<td>Russia</td>
<td>Rangoon4</td>
<td>6.3</td>
</tr>
<tr>
<td>timeZoneName_Asia/Jakarta=Indonesia: Jakarta</td>
<td>Indonesia</td>
<td>Jakarta7</td>
<td>4</td>
</tr>
<tr>
<td>timeZoneName_Asia/Hovd=Mongolia: Hovd</td>
<td>Mongolia</td>
<td>Hovd7</td>
<td>7</td>
</tr>
<tr>
<td>timeZoneName_Asia/Krasnoyarsk=Russia: Krasnoyarsk</td>
<td>Russia</td>
<td>Krasnoyarsk7</td>
<td>7</td>
</tr>
<tr>
<td>timeZoneName_Asia/Bangkok=Thailand, Cambodia, Vietnam &amp; Laos</td>
<td>Thailand</td>
<td>Bangkok7</td>
<td>44</td>
</tr>
<tr>
<td>timeZoneName_Asia/Chongqing=China</td>
<td>China</td>
<td>Beijing8</td>
<td>45</td>
</tr>
<tr>
<td>timeZoneName_Asia/Kuala_Lumpur=Malaysia &amp; Philippines</td>
<td>Malaysia</td>
<td>Kuala Lumpur8</td>
<td>8</td>
</tr>
<tr>
<td>timeZoneName_Asia/Ulaanbaatar=Mongolia: Ulaanbaatar</td>
<td>Mongolia</td>
<td>Ulaanbaatar8</td>
<td>8</td>
</tr>
<tr>
<td>timeZoneName_Asia/Irkutsk=Russia: Irkutsk</td>
<td>Russia</td>
<td>Irkutsk8</td>
<td>8</td>
</tr>
<tr>
<td>timeZoneName_Asia/Singapore=Singapore, Taiwan &amp; Hong Kong</td>
<td>Singapore</td>
<td>Singapore8</td>
<td>47</td>
</tr>
<tr>
<td>timeZoneName_Asia/Tokyo=Japan</td>
<td>Japan</td>
<td>Tokyo9</td>
<td>49</td>
</tr>
<tr>
<td>timeZoneName_Asia/Pyongyang=Korea</td>
<td>Korea</td>
<td>Seoul9</td>
<td>50</td>
</tr>
<tr>
<td>timeZoneName_Asia/Choibalsan=Mongolia: Choibalsan</td>
<td>Mongolia</td>
<td>Choibalsan8</td>
<td>8</td>
</tr>
<tr>
<td>timeZoneName_Asia/Yakutsk=Russia: Yakutsk</td>
<td>Russia</td>
<td>Yakutsk9</td>
<td>51</td>
</tr>
<tr>
<td>timeZoneName_Asia/Sakhalin=Russia: Sakhalin &amp; Vladivostok</td>
<td>Russia</td>
<td>Sakhalin10</td>
<td>58</td>
</tr>
<tr>
<td>timeZoneName_Asia/Magadan=Russia: Magadan</td>
<td>Russia</td>
<td>Magadan11</td>
<td>11</td>
</tr>
<tr>
<td>timeZoneName_Asia/Anadyr=Russia: Chukotskij &amp; Kamchatka</td>
<td>Russia</td>
<td>Anadyr12</td>
<td>12</td>
</tr>
<tr>
<td>timeZoneName_Atlantic/Bermuda=Bermuda</td>
<td>Russia</td>
<td>Benguerra-1</td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_America/Godthab=Greenland: West (Godthab)</td>
<td>Greenland</td>
<td>Godthab-1</td>
<td>-1</td>
</tr>
<tr>
<td>timeZoneName_America/Scoresbysund=Greenland: East (Scoresbysund)</td>
<td>Greenland</td>
<td>Scoresbysund0</td>
<td>0</td>
</tr>
<tr>
<td>timeZoneName_Australia/Perth=Western Australia</td>
<td>Australia</td>
<td>Perth8</td>
<td>46</td>
</tr>
<tr>
<td>timeZoneName_Australia/Darwin=Northern Territory</td>
<td>Australia</td>
<td>Darwin9.5</td>
<td>53</td>
</tr>
<tr>
<td>Cisco Unified MeetingPlace Time Zone</td>
<td>Cisco WebEx Time Zone</td>
<td>ID</td>
<td>GMT¹ Offset</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------</td>
<td>----</td>
<td>-------------</td>
</tr>
<tr>
<td>TimeZoneName_Australia/Adelaide=South Australia &amp; Broken Hill</td>
<td>Australia CentralAdelaide</td>
<td>52</td>
<td>9.3</td>
</tr>
<tr>
<td>TimeZoneName_Australia/Melbourne=NSW, Victoria &amp; Tasmania</td>
<td>TasmaniaHobart</td>
<td>57</td>
<td>10</td>
</tr>
<tr>
<td>TimeZoneName_Australia/Brisbane=Queensland</td>
<td>Australia EasternBrisbane</td>
<td>54</td>
<td>10</td>
</tr>
<tr>
<td>TimeZoneName_Australia/Brisbane=Queensland</td>
<td>Australia EasternSydney</td>
<td>55</td>
<td>10</td>
</tr>
<tr>
<td>TimeZoneName_Australia/Lord_Howe=Lord Howe Island</td>
<td>10.3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/Casey=Antarctica/Casey</td>
<td>8</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/Davis=Antarctica/Davis</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/DumontDUrville=Antarctica/DumontDUrville</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/Mawson=Antarctica/Mawson</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/McMurdo=Antarctica/McMurdo</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/Palmer=Antarctica/Palmer</td>
<td>-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/Rothera=Antarctica/Rothera</td>
<td>-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/South_Pole=Antarctica/South_Pole</td>
<td>12</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/Syowa=Antarctica/Syowa</td>
<td>3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Antarctica/Vostok=Antarctica/Vostok</td>
<td>6</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_America/Belize=Central America (CST)</td>
<td>CentralSaskatchewan</td>
<td>-6</td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_America/Panama=Panama</td>
<td>-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_America/Cayman=Cayman Is., Haiti &amp; Jamaica (EST)</td>
<td>-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_America/Havana=Cuba</td>
<td>-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_America/Grand_Turk=Turks &amp; Caicos</td>
<td>-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_America/Anguilla=Caribbean (AST) rename to Windward or Leeward Islands (eastern islands)</td>
<td>-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_America/Nassau=Bahamas</td>
<td>-5</td>
<td></td>
<td></td>
</tr>
<tr>
<td>TimeZoneName_Atlantic/Azores=Azores</td>
<td>AzoreslAzoresl</td>
<td>19</td>
<td>-1</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Lisbon=EU: West (WET/WEST)</td>
<td>GMTILondon</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>TimeZoneName_Europe/London=United Kingdom</td>
<td>GMTILondon0</td>
<td>21</td>
<td>0</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Brussels=EU: Central (CET/CEST)</td>
<td>EuropeAmsterdaml</td>
<td>22</td>
<td>1</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Brussels=EU: Central (CET/CEST)</td>
<td>EuropeParisl</td>
<td>23</td>
<td>1</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Brussels=EU: Central (CET/CEST)</td>
<td>EuropePrague1</td>
<td>24</td>
<td>1</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Brussels=EU: Central (CET/CEST)</td>
<td>EuropeBerlin1</td>
<td>25</td>
<td>1</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Athens=EU: East (EET/EEST)</td>
<td>EasternEuropeBucharest2</td>
<td>27</td>
<td>2</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Athens=EU: East (EET/EEST)</td>
<td>GreeceAthens2</td>
<td>26</td>
<td>2</td>
</tr>
<tr>
<td>TimeZoneName_Europe/Athens=EU: East (EET/EEST)</td>
<td>NorthernEuropeHelsinki2</td>
<td>30</td>
<td>2</td>
</tr>
<tr>
<td>Cisco Unified MeetingPlace Time Zone</td>
<td>Cisco WebEx Time Zone</td>
<td>Locations</td>
<td>ID</td>
</tr>
<tr>
<td>-------------------------------------</td>
<td>-----------------------</td>
<td>-----------</td>
<td>----</td>
</tr>
<tr>
<td>timeZoneName_Europe/Kaliningrad=Russia: Kaliningrad, Minsk</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Europe/Moscow=Russia: Moscow</td>
<td></td>
<td>Russian</td>
<td>Moscow</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+12=GMT-12</td>
<td></td>
<td>Dateline</td>
<td>Marshall Islands</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+11=GMT-11</td>
<td></td>
<td>Samoal</td>
<td>Samoal-11</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+10=GMT-10</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+9=GMT-9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+8=GMT-8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+7=GMT-7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+6=GMT-6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+5=GMT-5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+4=GMT-4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+3=GMT-3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+2=GMT-2</td>
<td></td>
<td>Mid-Atlantic</td>
<td>Mid-Atlantic</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT+1=GMT</td>
<td></td>
<td>Greenwich</td>
<td>Casablanca</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-1=GMT+1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-2=GMT+2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-3=GMT+3</td>
<td></td>
<td>Nairobi</td>
<td>Nairobi</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-4=GMT+4</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-5=GMT+5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-6=GMT+6</td>
<td></td>
<td>Central Asia</td>
<td>Almaty</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-7=GMT+7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-8=GMT+8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-9=GMT+9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-10=GMT+10</td>
<td></td>
<td>West Pacific</td>
<td>Guam</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-11=GMT+11</td>
<td></td>
<td>Central Pacific</td>
<td>Solomon Isl</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-12=GMT+12</td>
<td></td>
<td>Fiji</td>
<td>Fiji</td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-13=GMT+13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Etc/GMT-14=GMT+14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_America/Adak=US: Aleutian Islands (HAST/HADT)</td>
<td></td>
<td>Alaska</td>
<td>Anchorage</td>
</tr>
<tr>
<td>timeZoneName_America/Anchorage=US: Alaska (AKST/AKDT)</td>
<td></td>
<td>Alaska</td>
<td>Anchorage</td>
</tr>
<tr>
<td>timeZoneName_America/Vancouver=Canada: Pacific (PST/PDT)</td>
<td></td>
<td>Pacific</td>
<td>San Francisco</td>
</tr>
<tr>
<td>timeZoneName_America/Tijuana=Mexico: Pacific (PST/PDT)</td>
<td></td>
<td>Pacific</td>
<td>San Francisco</td>
</tr>
</tbody>
</table>
### Table 1  Time Zone Mapping Between Cisco Unified MeetingPlace and Cisco WebEx (continued)

<table>
<thead>
<tr>
<th>Cisco Unified MeetingPlace Time Zone</th>
<th>Cisco WebEx Time Zone</th>
<th>ID</th>
<th>GMT Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeZoneName_America/Los_Angeles=US: Pacific (PST/PDT)</td>
<td>Pacific/San Francisco=US: Pacific (PST/PDT)</td>
<td>4</td>
<td>-8</td>
</tr>
<tr>
<td>timeZoneName_America/Dawson_Creek=Canada: Dawson Creek (MST)</td>
<td>Mountain/Denver=US: Mountain (MST/MDT)</td>
<td>6</td>
<td>-7</td>
</tr>
<tr>
<td>timeZoneName_America/Edmonton=Canada: Mountain (MST/MDT)</td>
<td>Mountain/Denver=US: Mountain (MST/MDT)</td>
<td>6</td>
<td>-7</td>
</tr>
<tr>
<td>timeZoneName_America/Chihuahua=Mexico: Mountain (MST/MDT)</td>
<td>Mountain/Denver=US: Mountain (MST/MDT)</td>
<td>6</td>
<td>-7</td>
</tr>
<tr>
<td>timeZoneName_America/Hermosillo=Mexico: Sonora (MST)</td>
<td>Mountain/Arizona=US: Arizona (MST)</td>
<td>5</td>
<td>-7</td>
</tr>
<tr>
<td>timeZoneName_America/Phoenix=US: Arizona (MST)</td>
<td>Mountain/Arizona=US: Arizona (MST)</td>
<td>5</td>
<td>-7</td>
</tr>
<tr>
<td>timeZoneName_America/Denver=US: Mountain (MST/MDT)</td>
<td>Mountain/Denver=US: Mountain (MST/MDT)</td>
<td>6</td>
<td>-7</td>
</tr>
<tr>
<td>timeZoneName_America/Winnipeg=Canada: Central (CST/CDT)</td>
<td>Central/Chicago=US: Central (CST/CDT)</td>
<td>7</td>
<td>-6</td>
</tr>
<tr>
<td>timeZoneName_America/Regina=Canada: Saskatchewan (CST)</td>
<td>Central/Saskatchewan=Canada: Saskatchewan (CST)</td>
<td>9</td>
<td>-6</td>
</tr>
<tr>
<td>timeZoneName_America/Cancun=Mexico: Central (CST/CDT)</td>
<td>Mexico/Mexico City=US: Central Mexico (CST)</td>
<td>8</td>
<td>-6</td>
</tr>
<tr>
<td>timeZoneName_America/Chicago=US: Central (CST/CDT)</td>
<td>Central/Chicago=US: Central (CST/CDT)</td>
<td>7</td>
<td>-6</td>
</tr>
<tr>
<td>timeZoneName_America/Toronto=Canada: Eastern (EST/EDT)</td>
<td>Eastern/New York=US: Eastern (EST/EDT)</td>
<td>11</td>
<td>-5</td>
</tr>
<tr>
<td>timeZoneName_America/New_York=US: Eastern (EST/EDT)</td>
<td>Eastern/New York=US: Eastern (EST/EDT)</td>
<td>11</td>
<td>-5</td>
</tr>
<tr>
<td>timeZoneName_America/Indiana/Indianapolis=US: Indiana</td>
<td>Eastern/Indiana=US: Indiana (EST/EDT)</td>
<td>12</td>
<td>-5</td>
</tr>
<tr>
<td>timeZoneName_America/Halifax=Canada: Atlantic Time (AST/ADT)</td>
<td>Atlantic/Halifax=Canada: Atlantic Time (AST/ADT)</td>
<td>13</td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_America/St_Johns=Canada: Newfoundland (NST/NDT)</td>
<td>Newfoundland/Newfoundland=Canada: Atlantic Time (AST/ADT)</td>
<td>15</td>
<td>-3.5</td>
</tr>
<tr>
<td>timeZoneName_America/Miquelon=Canada: St. Pierre &amp; Miquelon (PMST/PMDT)</td>
<td>-3</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Pacific/Honolulu=US: Hawaii (HST)</td>
<td>Hawaii/Honolulu=US: Hawaii (HST)</td>
<td>2</td>
<td>-10</td>
</tr>
<tr>
<td>timeZoneName_Pacific/Marquesas=French Polynesia: Marquesas (GMT-9:30)</td>
<td>Marquesas/Marquesas=French Polynesia: Marquesas (GMT-9:30)</td>
<td>-9.3</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Pacific/Easter=Easter Island</td>
<td>Easter Island/Easter Island</td>
<td>-6</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Pacific/Norfolk=Norfolk (GMT+11:30)</td>
<td>Norfolk/Norfolk=US: Hawaii (HST)</td>
<td>11.3</td>
<td></td>
</tr>
<tr>
<td>timeZoneName_Pacific/Auckland=New Zealand (NZST/NZDT)</td>
<td>New Zealand/New Zealand=New Zealand (NZST/NZDT)</td>
<td>60</td>
<td>12</td>
</tr>
<tr>
<td>timeZoneName_Pacific/Chatham=New Zealand</td>
<td>New Zealand/New Zealand=New Zealand (NZST/NZDT)</td>
<td>60</td>
<td>12</td>
</tr>
<tr>
<td>timeZoneName_America/Eirunepe=Brazil: Northwest (ACT)</td>
<td>-4</td>
<td></td>
<td></td>
</tr>
<tr>
<td>timeZoneName_America/Bogota=Colombia, Ecuador &amp; Peru</td>
<td>10S. America/Pacific/Bogota=10S. America/Pacific/Bogota</td>
<td>10</td>
<td>-5</td>
</tr>
<tr>
<td>timeZoneName_America/Cuiaba=Brazil: Mato Grosso (AMT/AMST)</td>
<td>4S. America/Western/Caracas=4S. America/Western/Caracas</td>
<td>14</td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_America/Boa_Vista=Brazil: Northeast (AMT)</td>
<td>4S. America/Western/Caracas=4S. America/Western/Caracas</td>
<td>14</td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_America/Santiago=Chile</td>
<td>4S. America/Western/Caracas=4S. America/Western/Caracas</td>
<td>14</td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_Atlantic/Stanley=Falkland Islands</td>
<td>-4</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
### Table 1: Time Zone Mapping Between Cisco Unified MeetingPlace and Cisco WebEx (continued)

<table>
<thead>
<tr>
<th>Cisco Unified MeetingPlace Time Zone</th>
<th>Cisco WebEx Time Zone</th>
<th>Locations</th>
<th>ID</th>
<th>GMT Offset</th>
</tr>
</thead>
<tbody>
<tr>
<td>timeZoneName_America/Asuncion=Paraguay</td>
<td>timeZoneName_America/Caracas=Venezuela, Guyana &amp; Bolivia</td>
<td>S. America Western</td>
<td>Caracas</td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_America/Argentina/Buenos Aires=Argentina</td>
<td></td>
<td>S. America Western</td>
<td>Caracas</td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_America/Sao_Paulo=Brazil (BRT/BRST)</td>
<td>timeZoneName_America/Sao_Paulo=Brazil (BRT/BRST)</td>
<td>S. America Eastern</td>
<td>Buenos Aires</td>
<td>-3</td>
</tr>
<tr>
<td>timeZoneName_America/Belem=Brazil: Northern States (BRT)</td>
<td></td>
<td></td>
<td></td>
<td>-4</td>
</tr>
<tr>
<td>timeZoneName_America/Cayenne=French Guiana &amp; Suriname</td>
<td></td>
<td>S. America Eastern</td>
<td>Buenos Aires</td>
<td>-3</td>
</tr>
<tr>
<td>timeZoneName_America/Montevideo=Uruguay</td>
<td></td>
<td>S. America Eastern</td>
<td>Buenos Aires</td>
<td>-3</td>
</tr>
<tr>
<td>timeZoneName_America/Noronha=Brazil: Fernando do Noronha (FNT)</td>
<td></td>
<td>Columbo</td>
<td>Columbo</td>
<td>5.5</td>
</tr>
</tbody>
</table>

1. GMT = Greenwich Mean Time
# Application Server File Locations for Cisco Unified MeetingPlace

## Release 7.1
Revised: April 3, 2011 8:31 pm

<table>
<thead>
<tr>
<th>Location</th>
<th>Files</th>
</tr>
</thead>
<tbody>
<tr>
<td>/var/mp</td>
<td>Application log files</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/application</td>
<td>Cisco Unified MeetingPlace application code</td>
</tr>
<tr>
<td>/lat/bin</td>
<td>Shortcut to many application code binaries</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/licenses</td>
<td>License file</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/uninstaller</td>
<td>Application uninstaller</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/database/db-maintenance</td>
<td>Database maintenance scripts and utilities</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/afs/conf</td>
<td>Conference-specific recordings and attachments</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/afs/prompts</td>
<td>Factory audio prompt files</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/afs/custom</td>
<td>Custom audio prompts and user name recordings</td>
</tr>
<tr>
<td>/opt/cisco/meetingplace/afs/runprompt</td>
<td>Currently active prompt files</td>
</tr>
</tbody>
</table>

**Related Topics**

- [Music Prompt Numbers and Durations](#) in the [Customizing Music and Voice Prompts for Cisco Unified MeetingPlace](#) module
- [failoverUtil copyConfigFiles](#) in the [Using the Command-Line Interface (CLI) in Cisco Unified MeetingPlace](#) module