

**Main page:** [Cisco Unified MeetingPlace, Release 8.0](#)

**Up one level:** [Configuration](#)

- [About Directory Service](#)
- [Restrictions for Directory Service](#)
- [How to Configure Cisco Unified Communications Manager for Directory Service](#)
- [How to Configure Cisco Unified MeetingPlace for Directory Service](#)

## Contents

- [1 About Directory Service](#)
  - ◆ [1.1 Directory Service](#)
    - ◇ [1.1.1 Related Topics](#)
  - ◆ [1.2 Directory Service User Profile Configuration](#)
    - ◇ [1.2.1 Table: User Profile Field Configuration Through Directory Service](#)
    - ◇ [1.2.2 Related Topics](#)
  - ◆ [1.3 Directory Service User Profile Deletion](#)
    - ◇ [1.3.1 Related Topics](#)
  - ◆ [1.4 Directory Service isLocalUser Setting In User Profiles](#)
    - ◇ [1.4.1 Related Topics](#)
  - ◆ [1.5 External AXL Authentication for Directory Service Users](#)
    - ◇ [1.5.1 Table: Directory Service User Authentication](#)
    - ◇ [1.5.2 Related Topics](#)
- [2 Restrictions for Directory Service](#)
  - ◆ [2.1 Table: Maximum Length of Directory Service User Fields](#)
  - ◆ [2.2 Related Topics](#)
- [3 How to Configure Cisco Unified Communications Manager for Directory Service](#)
  - ◆ [3.1 Enabling Cisco AXL Web Services and Cisco DirSync on Cisco Unified Communications Manager](#)
    - ◇ [3.1.1 Before You Begin](#)
    - ◇ [3.1.2 Procedure](#)
    - ◇ [3.1.3 What to Do Next](#)
  - ◆ [3.2 How to Configure LDAP Integration on Cisco Unified Communications Manager](#)
    - ◇ [3.2.1 Prerequisites for Configuring LDAP Integration on Cisco Unified Communications Manager](#)
      - [3.2.1.1 Related Topics](#)
    - ◇ [3.2.2 Enabling LDAP Synchronization on Cisco Unified Communications Manager](#)
      - [3.2.2.1 Before You Begin](#)
      - [3.2.2.2 Procedure](#)
      - [3.2.2.3 What to Do Next](#)
    - ◇ [3.2.3 Adding an LDAP Directory to Cisco Unified Communications Manager](#)
      - [3.2.3.1 Before You Begin](#)
      - [3.2.3.2 Procedure](#)
      - [3.2.3.3 What to Do Next](#)
    - ◇ [3.2.4 Synchronizing Cisco Unified Communications Manager with the LDAP Directory](#)
      - [3.2.4.1 Before You Begin](#)

- [3.2.4.2 Procedure](#)
        - [3.2.4.3 What to Do Next](#)
    - ◆ [3.3 Configuring LDAP Authentication for a Single Active Directory Domain in Cisco Unified Communications Manager](#)
      - ◇ [3.3.1 Before You Begin](#)
      - ◇ [3.3.2 Procedure](#)
      - ◇ [3.3.3 What to Do Next](#)
    - ◆ [3.4 Configuring LDAP Authentication for Multiple Active Directory Domains in Cisco Unified Communications Manager](#)
      - ◇ [3.4.1 Before You Begin](#)
      - ◇ [3.4.2 Procedure](#)
      - ◇ [3.4.3 What to Do Next](#)
    - ◆ [3.5 Creating an Application User in Cisco Unified Communications Manager](#)
      - ◇ [3.5.1 Before You Begin](#)
      - ◇ [3.5.2 Procedure](#)
      - ◇ [3.5.3 What to Do Next](#)
    - ◆ [3.6 How to Configure the User PIN in Cisco Unified Communications Manager](#)
      - ◇ [3.6.1 Configuring the Credential Policy Default in Cisco Unified Communications Manager Release 6.x](#)
        - [3.6.1.1 Before You Begin](#)
        - [3.6.1.2 Procedure](#)
        - [3.6.1.3 What to Do Next](#)
      - ◇ [3.6.2 Configuring the User PIN in Cisco Unified Communications Manager](#)
        - [3.6.2.1 Before You Begin](#)
        - [3.6.2.2 Procedure](#)
        - [3.6.2.3 What to Do Next](#)
    - ◆ [3.7 Viewing Department Information for Users in Cisco Unified Communications Manager](#)
      - ◇ [3.7.1 Before You Begin](#)
      - ◇ [3.7.2 Restrictions](#)
      - ◇ [3.7.3 Procedure](#)
      - ◇ [3.7.4 What To Do Next](#)
  - [4 How to Configure Cisco Unified MeetingPlace for Directory Service](#)
    - ◆ [4.1 Saving and Then Clearing the User and Meeting Data on One Application Server](#)
      - ◇ [4.1.1 Before You Begin](#)
      - ◇ [4.1.2 Procedure](#)
      - ◇ [4.1.3 Related Topics](#)
      - ◇ [4.1.4 What To Do Next](#)
    - ◆ [4.2 Configuring User Database Replication for Two Sites](#)
      - ◇ [4.2.1 Before You Begin](#)
      - ◇ [4.2.2 Restrictions](#)
      - ◇ [4.2.3 Procedure](#)
      - ◇ [4.2.4 Related Topics](#)
      - ◇ [4.2.5 What to Do Next](#)
    - ◆ [4.3 Restoring User and Meeting Data on Application Servers](#)
      - ◇ [4.3.1 Before You Begin](#)
      - ◇ [4.3.2 Procedure](#)
      - ◇ [4.3.3 Related Topics](#)
      - ◇ [4.3.4 What To Do Next](#)
    - ◆ [4.4 How to Configure User Profiles for Directory Service Users](#)
      - ◇ [4.4.1 Assigning User Groups for Directory Service Users](#)
        - [4.4.1.1 Before You Begin](#)
        - [4.4.1.2 Procedure](#)
        - [4.4.1.3 Related Topics](#)

- [4.4.1.4 What To Do Next](#)
- ◇ [4.4.2 Configuring Directory Service Filters for User Groups](#)
  - [4.4.2.1 Before You Begin](#)
  - [4.4.2.2 Restrictions](#)
  - [4.4.2.3 Procedure](#)
  - [4.4.2.4 Table: Field Reference: Add Group Filter Page and Edit Group Filter Page](#)
  - [4.4.2.5 Related Topics](#)
  - [4.4.2.6 What To Do Next](#)
- ◇ [4.4.3 Assigning Time Zones to Directory Service Users](#)
  - [4.4.3.1 Before You Begin](#)
  - [4.4.3.2 Procedure](#)
  - [4.4.3.3 Related Topics](#)
  - [4.4.3.4 What To Do Next](#)
- ◇ [4.4.4 Configuring Directory Service Filters for Time Zones](#)
  - [4.4.4.1 Table: Examples of Phone Prefix Matching for Time Zone Filters](#)
  - [4.4.4.2 Before You Begin](#)
  - [4.4.4.3 Restrictions](#)
  - [4.4.4.4 Procedure](#)
  - [4.4.4.5 Table: Field Reference: Add Time Zone Filter Page, Edit Time Zone Filter Page, and View Time Zone Filter Page](#)
  - [4.4.4.6 Related Topics](#)
  - [4.4.4.7 What To Do Next](#)
- ◇ [4.4.5 Modifying Directory Service Filters and Applying the Filters to Previously Imported Directory Service User Profiles](#)
  - [4.4.5.1 Procedure](#)
  - [4.4.5.2 What To Do Next](#)
- ◇ [4.4.6 Assigning Profile Numbers to Directory Service Users](#)
  - [4.4.6.1 Before You Begin](#)
  - [4.4.6.2 Procedure](#)
  - [4.4.6.3 Related Topics](#)
  - [4.4.6.4 What To Do Next](#)
- ◆ [4.5 Configuring Directory Service in Cisco Unified MeetingPlace](#)
  - ◇ [4.5.1 Before You Begin](#)
  - ◇ [4.5.2 Procedure](#)
  - ◇ [4.5.3 Related Topics](#)
  - ◇ [4.5.4 What To Do Next](#)

## About Directory Service

- [Directory Service](#)
- [Directory Service User Profile Configuration](#)
- [Directory Service User Profile Deletion](#)
- [Directory Service isLocalUser Setting In User Profiles](#)
- [External AXL Authentication for Directory Service Users](#)

## 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.

**Note:** For information about LDAP integration, see 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](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.html).

Specifically, Directory Service simplifies user profile administration in these ways:

- 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](#)
- [Directory Service User Profile Deletion](#)
- [Directory Service isLocalUser Setting In User Profiles](#)
- [External AXL Authentication for Directory Service Users](#)
- [Configuring Cisco Unified MeetingPlace Directory Service](#)

## Directory Service User Profile Configuration

During the initial Directory Service import of a user profile, the fields are configured as described in [Table: User Profile Field Configuration Through Directory Service](#). If the corresponding Cisco Unified Communications Manager user profile is modified, the next Directory Service user profile update or full synchronization reconfigures the Cisco Unified MeetingPlace user profile fields as specified in [Table: User Profile Field Configuration Through Directory Service](#).

**Note:** To change any of the User Profile Fields in [Table: User Profile Field Configuration Through Directory Service](#), you must configure the corresponding Source.

**Table: User Profile Field Configuration Through Directory Service**

Source	User Profile Fields
Directory Service import process	isLocalUser-This is always set to No in each Directory Service user profile.

Cisco Unified Communications Manager user database	<p>Unless otherwise specified, if the corresponding field in Cisco Unified Communications Manager is empty, the field is left blank in the Cisco Unified MeetingPlace user profile.</p> <ul style="list-style-type: none"> <li>• <u>First name</u></li> <li>• <u>Last name</u></li> <li>• <u>User ID</u></li> <li>• <u>Profile number</u></li> </ul> <p>See the <u>Assigning Profile Numbers to Directory Service Users</u>.</p> <ul style="list-style-type: none"> <li>• <u>User status</u></li> <li>• <u>Email address</u></li> <li>• <u>Main phone number</u></li> </ul>
User group filters or <u>Group name</u> in user profile	<u>Group name</u> -See the <u>Assigning User Groups for Directory Service Users</u> .
Time zone filters or <u>Time zone</u> in user group or user profile	<u>Time zone</u> -See the <u>Assigning Time Zones to Directory Service Users</u> .
Guest Profile (first import only)	<p>All user profile fields <i>not</i> mentioned previously in this table are initially populated with the values configured in the <u>Guest Profile</u>. You can then modify the individual user profile fields through the Administration Center. The values will <i>not</i> be overwritten by Directory Service user profile updates or full synchronizations.</p> <p>Restrictions:</p> <ul style="list-style-type: none"> <li>• Remember that all user profile fields set to "Group default" inherit their value from the user group. If the <u>Group name</u> is modified through Directory Service filters or department changes, the user profile fields will be modified accordingly.</li> <li>• The following fields are not populated at all through Directory Service. Because Directory Service users are <i>not</i> authenticated by Cisco Unified MeetingPlace, these password fields are not imported and cannot be modified through Cisco Unified MeetingPlace: <ul style="list-style-type: none"> <li>◆ <u>User password</u> and <u>User password confirm</u></li> <li>◆ <u>Profile PIN</u> and <u>Profile PIN confirm</u></li> </ul> </li> </ul>

#### Related Topics

- [Directory Service isLocalUser Setting In User Profiles](#)
- [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](#)
- [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.

<b>isLocalUserSetting</b>	<b>Description</b>
Yes	<ul style="list-style-type: none"> <li>• User is authenticated locally against the Cisco Unified MeetingPlace database.</li> <li>• User profile settings can be modified through Cisco Unified MeetingPlace user interfaces. (1)</li> <li>• Yes is the default value for user profiles that are manually imported or created through the Administration Center.</li> </ul>
No	<ul style="list-style-type: none"> <li>• Identifies a Directory Service user.</li> <li>• User is authenticated externally through AXL authentication. See the <a href="#">External AXL Authentication for Directory Service Users</a>.</li> <li>• User profile changes that are made through Cisco Unified MeetingPlace user interfaces (1) can be overwritten by the next Directory Service user profile update. See the <a href="#">Directory Service User Profile Configuration</a>.</li> <li>• No is the default value for user profiles that are imported through Directory Service.</li> </ul>

Footnote 1: Cisco Unified MeetingPlace user interfaces include the web user portal on the Web Server, the Cisco WebEx integration end-user interface on the Application Server, and the Administration Center (both the [User Profiles Page](#) and the [Import User Profiles Page](#)).

**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 might 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](#).

#### Related Topics

- [About Directory Service](#)
- [Adding or Editing User Profiles by Import](#) in the [Importing Data into Cisco Unified MeetingPlace](#) module
- [Methods for Adding User Profiles](#) in the [Configuring User Profiles and User Groups for Cisco Unified MeetingPlace](#) module

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

**Table: Directory Service User Authentication**

Directory Service User Login Method	Device Used to Authenticate the Directory Service User (With LDAP Integration)	Device Used to Authenticate the Directory Service User (Without LDAP Integration)
Phone	Cisco Unified Communications Manager	Cisco Unified Communications Manager
Web	LDAP directory	Cisco Unified Communications Manager

### Related Topics

- [Directory Service isLocalUser Setting In User Profiles](#)
- [User Authentication for Cisco Unified MeetingPlace module](#)
- [Configuring Cisco Unified MeetingPlace Directory Service module](#)

## Restrictions for Directory Service

- Cisco Unified Communications Manager Release 4.x and earlier releases are not supported.
- (Cisco WebEx integration) Do not configure Directory Service if your system is or will be integrated with a Cisco WebEx site that is provisioned to *not* use [Directory Integration](#).
  - ◆ iPhone and Blackberry Smartphone Click-to-Join WebEx Meetings are not currently supported with Directory Service and SSO to Cisco WebEx. We do, however, recommend that you have your Cisco WebEx site provisioned for directory integration, which requires that you configure Directory Service.
- 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 PIN 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 PIN, Minimum user password length, Change user password (days, and Maximum profile sign-in 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 sign in to Cisco Unified MeetingPlace.



If Cisco Unified Communications Manager fails, 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 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: Maximum Length of Directory Service User Fields](#).

**Table: Maximum Length of Directory Service User Fields**

Cisco Unified MeetingPlace Field	Cisco Unified Communications Manager Field	Maximum Number of Characters
<a href="#">First name</a>	First name (FirstName)	64
<a href="#">Last name</a>	Last name (LastName)	64
<a href="#">User ID</a>	User ID (UserId)	120
<a href="#">Email address</a>	Mail ID (EmailAddress)	128
<a href="#">Main phone number</a>	Telephone Number (PhoneNumber)	32

- 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 disable 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

- [Integrating Cisco Unified MeetingPlace with Cisco WebEx module](#)
- [Directory Service isLocalUser Setting In User Profiles](#)
- [External AXL Authentication for Directory Service Users](#)
- [Directory Service User Profile Configuration](#)
- [How to Configure Cisco Unified Communications Manager for Directory Service](#)
- [Configuring Application Server Failover for Cisco Unified MeetingPlace module](#)

## How to Configure Cisco Unified Communications Manager for Directory Service

- [Enabling Cisco AXL Web Services and Cisco DirSync on Cisco Unified Communications Manager](#)
- [How to Configure LDAP Integration on Cisco Unified Communications Manager](#)
- [Configuring LDAP Authentication for a Single Active Directory Domain in Cisco Unified Communications Manager](#)
- [Configuring LDAP Authentication for Multiple Active Directory Domains in Cisco Unified Communications Manager](#)
- [Creating an Application User in Cisco Unified Communications Manager](#)
- [How to Configure the User PIN in Cisco Unified Communications Manager](#)
- [Viewing Department Information for Users in Cisco Unified Communications Manager](#)

## Enabling 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

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **Cisco Unified Serviceability** in the Navigation window then select **Go**.
4. Select **Tools > Service Activation**.
5. Check **Cisco AXL Web Service** (if not already checked).
6. Check **Cisco DirSync** if you are using LDAP integration.
7. Select **Save**.

## What to Do Next

If you are using LDAP integration, proceed to the [How to Configure LDAP Integration on Cisco Unified Communications Manager](#).

Otherwise, proceed to the [Creating an Application User in Cisco Unified Communications Manager](#).

## How to Configure LDAP Integration on Cisco Unified Communications Manager

- [Prerequisites for Configuring LDAP Integration on Cisco Unified Communications Manager](#)
- [Enabling LDAP Synchronization on Cisco Unified Communications Manager](#)
- [Adding an LDAP Directory to Cisco Unified Communications Manager](#)
- [Synchronizing Cisco Unified Communications Manager with the LDAP Directory](#)

## Prerequisites for Configuring LDAP Integration on Cisco Unified Communications Manager

- Complete the [Enabling Cisco AXL Web Services and Cisco DirSync on Cisco Unified Communications Manager](#)
- If LDAP integration is already configured for your Cisco Unified Communications Manager, proceed to the [Creating an Application User in Cisco Unified Communications Manager](#).
- Some LDAP directories might require different or more complex configurations than the procedures described in this document. To do the following, check the *System Requirements for Cisco Unified MeetingPlace* at [http://docwiki.cisco.com/wiki/Cisco Unified MeetingPlace Release 8.0 -- System Requirements for Cisco U](http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace_Release_8.0_--_System_Requirements_for_Cisco_U)
  - ◆ 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:
  - ◆ *Cisco Unified Communications Solution Reference Network Design (SRND)* at [http://www.cisco.com/en/US/products/sw/voicesw/ps556/products\\_implementation\\_design\\_guides\\_list.ht](http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_implementation_design_guides_list.ht)
  - ◆ *Cisco Unified Communications Manager Administration Guide* 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)
- You perform these tasks in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you might 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](#)

## Enabling LDAP Synchronization on Cisco Unified Communications Manager

### Before You Begin

Read the [Prerequisites for Configuring LDAP Integration on Cisco Unified Communications Manager](#).

### Procedure

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **System > LDAP > LDAP System**.
4. Check **Enable Synchronizing from LDAP Server**.
5. Select the appropriate server type and user ID attribute.  
You can select **Help > This Page** at any time to find detailed information.
6. Select **Save**.

### What to Do Next

Proceed to the [Adding an LDAP Directory to Cisco Unified Communications Manager](#).

## Adding an LDAP Directory to Cisco Unified Communications Manager

### Before You Begin

Complete the [Enabling LDAP Synchronization on Cisco Unified Communications Manager](#).

If you are configuring LDAP authentication for multiple Active Directory domains, make sure that you add an LDAP directory for each domain on Cisco Unified Communications Manager.

### Procedure

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **System > LDAP > LDAP Directory**.
4. Select **Add New**.
5. Configure the fields on the LDAP Directory page.  
You can select **Help > This Page** at any time to find detailed information.
6. Select **Save**.

#### What to Do Next

Proceed to the [Synchronizing Cisco Unified Communications Manager with the LDAP Directory](#).

### Synchronizing Cisco Unified Communications Manager with the LDAP Directory

#### Before You Begin

Complete the [Adding an LDAP Directory to Cisco Unified Communications Manager](#).

#### Procedure

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **System > LDAP > LDAP Directory**.
4. Select **Find**.
5. Select the name of your LDAP configuration entry.
6. Select **Perform Full Sync Now**.

#### What to Do Next

Proceed to the [Configuring LDAP Authentication for a Single Active Directory Domain in Cisco Unified Communications Manager](#).

### Configuring LDAP Authentication for a Single Active Directory Domain in Cisco Unified Communications Manager

#### Before You Begin

Complete the tasks in the [How to Configure LDAP Integration on Cisco Unified Communications Manager](#).

#### Procedure

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **System > LDAP > LDAP Authentication**.
4. Configure the fields on the LDAP Authentication page.  
You can select **Help > This Page** at any time to find detailed information.
5. Make sure that you check **Use LDAP Authentication for End Users**.
6. Select **Save**.

#### What to Do Next

Proceed to the [Creating an Application User in Cisco Unified Communications Manager](#).

## Configuring LDAP Authentication for Multiple Active Directory Domains in Cisco Unified Communications Manager

If you have users in two active directory domains, for example, a parent domain (company.com) and a child domain (marketing.company.com), you must ensure that the system authenticates all users so that they can sign in to Cisco Unified MeetingPlace.

#### Before You Begin

Complete the tasks in the [How to Configure LDAP Integration on Cisco Unified Communications Manager](#). Make sure that you add an LDAP directory for each domain on Cisco Unified Communications Manager.

#### Procedure

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **System > LDAP > LDAP Authentication**.
4. Configure the fields on the LDAP Authentication page.
  - You can select **Help > This Page** at any time to find detailed information.
  - 1. Check **Use LDAP Authentication for End Users**.
  - 2. For LDAP Manager Distinguished Name, enter the distinguished name of the administrator of the parent domain.
  - 3. For LDAP Password, enter the password of the administrator of the parent domain.
  - 4. Confirm the password.
  - 5. For LDAP User Search Base, enter dc=company;dc=com (all parent domain information).
  - 6. For Host Name or IP Address for Server, enter the name or IP address of the parent domain.
  - 7. For LDAP Port, enter **3268**.
5. Select **Save**.

#### What to Do Next

Proceed to the [Creating an Application User in Cisco Unified Communications Manager](#).

## 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, skip this task and proceed to the [How to Configure the User PIN in Cisco Unified Communications Manager](#):
  - ◆ 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, you must update the [AXL user ID](#) 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 a Single Active Directory Domain in Cisco Unified Communications Manager](#).
- 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/ccmadmin/>, where ccm-server is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **User Management > Application User**.
4. Select **Add New**.
5. Configure a **User ID**, such as mpdsaxl.
6. Configure the **Password** and **Confirm Password** fields.
7. Select **Add to User Group**.
8. Find the **Standard CCM Super Users** group.
9. Check the Standard CCM Super Users group.
10. Select **Add Selected**.
11. Select **Save**.

## What to Do Next

Proceed to the [How to Configure the User PIN in Cisco Unified Communications Manager](#).

## How to Configure the User PIN in Cisco Unified Communications Manager

The user PIN in Cisco Unified Communications Manager is equivalent to the [Profile PIN](#) in Cisco Unified MeetingPlace.

Directory Service users cannot sign in to Cisco Unified MeetingPlace over the phone until the user PIN is changed through the Cisco Unified Communications Manager user page.

- [Configuring the Credential Policy Default in Cisco Unified Communications Manager Release 6.x](#)
- [Configuring the User PIN in Cisco Unified Communications Manager](#)

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

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

#### Before You Begin

- This task applies only to Cisco Unified Communications Manager Release 6.x (or later). If you are using Cisco Unified Communications Manager Release 5.x, you must configure the user PINs individually. See the [Configuring the User PIN in Cisco Unified Communications Manager](#).
- Complete the [Creating an Application User in Cisco Unified Communications Manager](#).
- 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

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **User Management > Credential Policy Default**.
4. Select **Default Credential Policy** for the End User PIN.
5. Enter the default PIN in the **Change Credential** and **Confirm Credential** fields.
6. (Recommended) Check **User Must Change at Next Login** to prevent toll fraud.
7. Select **Save**.

#### What to Do Next

If you want to configure individual user PINs, proceed to the [Configuring the User PIN in Cisco Unified Communications Manager](#).

Otherwise, proceed to the [How to Configure Cisco Unified MeetingPlace for Directory Service](#).



## Configuring the User PIN in Cisco Unified Communications Manager

This task enables Directory Service users to sign 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](#)
- If you are using Cisco Unified Communications Manager Release 6.x, complete the [Configuring the Credential Policy Default in Cisco Unified Communications Manager Release 6.x](#).
- 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

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **User Management > End User**.
4. Select **Find**.
5. Select the User ID.
6. Configure the **PIN** and **Confirm PIN** fields.
7. If you configured a PIN that might be accessed or guessed by someone other than the intended user, we recommend completing these steps to prevent toll fraud:
  1. Select **Edit Credential**.
  2. Check **User Must Change at Next Login**.
  3. Select **Save**.
8. Select **Save**.
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](#).

## Viewing Department Information for Users in Cisco Unified Communications Manager

If you plan to configure Directory Service filters to user groups, perform this task to obtain the department information (name or number) 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, you cannot modify the department information for users in Cisco Unified Communications Manager.

### Procedure

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.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **User Management > End User**.
4. Select **Find**.
5. (Optional) Select the **Department** column title to sort user entries by department.
6. (Optional) In the **Rows per Page** field, select a larger number of entries to display.
7. 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](#).

## How to Configure Cisco Unified MeetingPlace for Directory Service

- [Saving and Then Clearing the User and Meeting Data on One Application Server](#)
- [Configuring User Database Replication for Two Sites](#)
- [Restoring User and Meeting Data on Application Servers](#)
- [How to Configure User Profiles for Directory Service Users](#)
- [Configuring Directory Service in Cisco Unified MeetingPlace](#)

### 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 By Using the CLI on the Application Server](#) 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

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](#)
2. Sign in to the Application Server CLI as the `[[Cisco Unified MeetingPlace Release 8.0 -- Using the Command-Line Interface (CLI) on the Cisco Unified MeetingPlace Application Server#rootroot]]` user.
3. Save user and meeting recordings by entering these commands:
  1. `cd /mpx-record`
  2. `tar cvf user-recordings.tar $MP_HOME/afs/custom/userprofile`
  3. `tar cvf conf-recordings.tar /mpx-record/conf`
4. Enter the `cleardb` command to delete user profiles, user groups, meetings, and recordings from the database.

### Related Topics

- [Running Reports and Exporting Data from Cisco Unified MeetingPlace](#) module

### What To Do Next

Proceed to the [Configuring User Database Replication for Two Sites](#).

## 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

- Time must be synchronized between the Application Servers.
- 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, designate one site as "Site 1," and complete the [Saving and Then Clearing the User and Meeting Data on One Application Server](#) 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 By Using the CLI on the Application Server](#)

## Restrictions

User database replication for two sites is not supported with [Application Server Failover](#).

## Procedure

1. Sign in to the CLI of the Application Server in Site 2.
2. Enter `su` to get root privileges.
3. Enter the following command using the hostname of the Application Server in Site 1:  
**`mp_replication init -s 2 -n 1 -r hostname-site1 -m`**
4. Sign in to the CLI of the Application Server in Site 1.
5. Enter `su` to get root privileges.
6. Enter the following commands using the hostname of the Application Server in the specified site:  
**`mp_replication init -s 1 -n 1 -r hostname-site2 -m`**  
**`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.

**Note:** After setting up replication, if you stop the remote server, the changes made in the local server will be queued and be applied on the remote server when it comes up. If the remote server is down for a long time (for days or weeks, depending on the amount of the configuration changes), this queue can become full and cause a restart of the local server. To avoid this, you should disable replication if the remote server is going to be down for a long time.

## Related Topics

- [Using the Command-Line Interface \(CLI\) on the Cisco Unified MeetingPlace Application Server module](#)

## What to Do Next

If you need to restore user and meeting data from the second Application Server, proceed to the [Restoring User and Meeting Data on Application Servers](#).

If you are configuring [RSNA](#) without Directory Service, 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](#).

## 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](#).
- Complete the [Configuring User Database Replication for Two Sites](#).
- Perform the following procedure on only one Application Server.

### Procedure

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](#)
2. Sign in to the Application Server CLI as the **mpxadmin** user.
3. Restore user and meeting recordings by entering these commands:
  1. **cd /mpx-record**
  2. **tar xvf user-recordings.tar**
  3. **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, 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](#).

## 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](#).

- [Assigning User Groups for Directory Service Users](#)
- [Configuring Directory Service Filters for User Groups](#)
- [Assigning Time Zones to Directory Service Users](#)
- [Configuring Directory Service Filters for Time Zones](#)
- [Modifying Directory Service Filters and Applying the Filters to Previously Imported Directory Service User Profiles](#)
- [Assigning Profile Numbers to Directory Service Users](#)

### 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

1. Sign in to the Cisco Unified MeetingPlace Administration Center.
2. Select **User Configuration > Directory Service > Directory Service Configuration**.
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 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.

4. Select **Save**.

#### Related Topics

- [Table: Field Reference: Directory Service Configuration Page](#) in the [Cisco Unified MeetingPlace Release 8.0 -- Administration Center Page References for Cisco Unified MeetingPlace \(D - G pages\)](#)
- [Directory Service User Profile Configuration](#)

#### What To Do Next

Proceed to the [Configuring Directory Service Filters for User Groups](#) if you set the User groups for imported users field to Use filters.

Otherwise, proceed to the [Assigning Time Zones to Directory Service Users](#).

### 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](#).
- Configure user groups. See [Configuring User Profiles and User Groups for Cisco Unified MeetingPlace](#) module.
- Obtain department information (name or number) for users. See the [Viewing Department Information for Users in Cisco Unified Communications Manager](#).

#### 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](#).

**Procedure**

1. Sign in to the Cisco Unified MeetingPlace Administration Center.
2. Select **User Configuration > Directory Service > Directory Service Filters for Groups**.
3. Select **Add New** or **Edit**.
4. Configure the fields described in [Table: Field Reference: Add Group Filter Page and Edit Group Filter Page](#).

**Table: Field Reference: Add Group Filter Page and Edit Group Filter Page**

Field	Description
Department	The system applies this filter when this field matches the department information (name or number) of the imported user.
Group	User group to assign to imported user profiles which match the <a href="#">Department</a> .

5. Select **Save**.

**Related Topics**

- [Directory Service User Profile Configuration](#)

**What To Do Next**

Proceed to the [Assigning Time Zones to Directory Service Users](#).

**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**

1. Sign in to the Cisco Unified MeetingPlace Administration Center.
2. Select **User Configuration > Directory Service > Directory Service Configuration**.
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, then 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.
4. 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.
5. Select **Save**.

**Related Topics**

- [Table: Field Reference: Directory Service Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace \(D - G pages\)](#)
- [Directory Service User Profile Configuration](#)

**What To Do Next**

If you configured the **Time zones for imported users** field to apply custom time zone filters, proceed to the [Configuring Directory Service Filters for Time Zones](#).

Otherwise, proceed to the [Assigning Profile Numbers to Directory Service Users](#).

**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: Examples of Phone Prefix Matching for Time Zone Filters](#). 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: Examples of Phone Prefix Matching for Time Zone Filters**

Sample Phone Number in Cisco Unified Communications Manager	<u>Phone prefix</u> Used to Match a Time Zone Filter
---	--

+12 34 555-0123	+12 34
12-345-555-0123	12
(1234)555-0123	1234
123-555-0123	123
1235550123	123

**Before You Begin**

- Enable the use of *custom* filters. See the [Assigning Time Zones to Directory Service Users](#).
- If the system does not find a matching phone prefix, the system assigns the local time of the Application Server.
- If you have multiple Application Servers for multiple sites or for [Application Server Failover](#), 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, 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](#).

**Procedure**

1. Sign in to the Cisco Unified MeetingPlace Administration Center.
2. Select **User Configuration > Directory Service > Directory Service Filters for Time Zones**.
3. Select **Add New** or **Edit**.
4. Configure the fields described in [Table: Field Reference: Add Time Zone Filter Page](#), [Edit Time Zone Filter Page](#), and [View Time Zone Filter Page](#).

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

Field	Description
Phone prefix	The system applies this filter when this value matches the first digits of the telephone number of the imported user.
Region	Determines which options become available in the Time zone field.
Time zone	<a href="#">Time zone</a> assigned to imported user profiles that match the <a href="#">Phone prefix</a> .

5. Select **Save**.

**Related Topics**

- [Directory Service User Profile Configuration](#)

**What To Do Next**

Proceed to the [Assigning Profile Numbers to Directory Service Users](#).

**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**

High-Level Task		Details
1	Delete the user profiles from Cisco Unified MeetingPlace.	Complete one of the following tasks: <ul style="list-style-type: none"> <li>• <a href="#">Deleting a User Profile in the Configuring User Profiles and User Groups for Cisco Unified MeetingPlace</a> module</li> <li>• <a href="#">Deleting User Profiles by Import</a> in the <a href="#">Importing Data into Cisco Unified MeetingPlace</a> module</li> </ul>
2	Configure the Directory Service filters for user groups.	Complete one or both of the following tasks: <ul style="list-style-type: none"> <li>• <a href="#">Configuring Directory Service Filters for User Groups</a></li> <li>• <a href="#">Configuring Directory Service Filters for Time Zones</a></li> </ul>
3	Import the user profiles from Cisco Unified Communications Manager.	<ol style="list-style-type: none"> <li>1. Go to the <a href="#">Directory Service Configuration Page</a>.</li> <li>2. Check <a href="#">Update Now</a>.</li> <li>3. Check <a href="#">Perform full sync with Cisco Unified Communications Manager</a>.</li> <li>4. Select <a href="#">Save</a>.</li> </ol>

**What To Do Next**

Proceed to the [Configuring Directory Service in Cisco Unified MeetingPlace](#).

**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

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

## Procedure

1. Sign in to the Cisco Unified MeetingPlace Administration Center.
2. Select **User Configuration > Directory Service > Directory Service Configuration**.
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.
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, the Telephone Number will be used *as is* as the Profile number.
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.
6. Select **Save**.

## Related Topics

- [Table: Field Reference: Directory Service Configuration Page](#) in the [Administration Center Page References for Cisco Unified MeetingPlace](#)
- [Directory Service User Profile Configuration](#)

## What To Do Next

Proceed to the [Configuring Directory Service in Cisco Unified MeetingPlace](#).

## Configuring Directory Service in Cisco Unified MeetingPlace

## Before You Begin

- Read the [Restrictions for Directory Service](#).
- Complete these tasks:
  - ◆ [Creating an Application User in Cisco Unified Communications Manager](#)
  - ◆ [How to Configure User Profiles for Directory Service Users](#)
- 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](#).

## Procedure

1. Sign in to the Cisco Unified MeetingPlace Administration Center.
2. Select **User Configuration > Directory Service > Directory Service Configuration**.
3. Configure the [AXL user ID](#) and [AXL password](#) fields:
  - ◆ If you created an application user in Cisco Unified Communications Manager, enter the user ID and password for that application user.
  - ◆ If you did not create an application user, enter the user ID 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, you must update the AXL user ID or AXL password in Cisco Unified MeetingPlace whenever the Cisco Unified Communications Manager administrator user ID or password is modified.
4. In the [AXL URL](#) field, enter **https://ip-address:8443/axl/** using the Cisco Unified Communications Manager IP address.
5. Check [Update Now](#).
6. Enter the Application Server hostname in the [Hostname for Active Directory Service](#) field.
7. (Optional) To modify the frequency and other settings of user profile synchronization, configure the remaining fields on the [Directory Service Configuration Page](#).
8. Select **Save**.

## Related Topics

- [Table: Field Reference: Directory Service Configuration Page](#) in the [Administration Center Page References for Cisco Unified MeetingPlace](#)
- [About Directory Service](#)

## What To Do Next

If you are configuring RSNA, return to [How to Configure User Profiles for RSNA](#) in the [Configuring Reservationless Single Number Access \(RSNA\) for Cisco Unified MeetingPlace](#) module.