



LDAP Directory Setup

This chapter provides information to configure the LDAP directory. The LDAP directory configuration takes place in these related windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

For additional information, see topics related to the directory, application users, and end users in the *Cisco Unified Communications Manager System Guide*.

- [About LDAP Directory Setup](#), on page 1
- [LDAP Directory Settings](#), on page 2

About LDAP Directory Setup

In Cisco Unified Communications Manager, use the **System > LDAP > LDAP Directory** menu path to configure LDAP directories.

In the LDAP Directory window, you specify information about the LDAP directory; for example, the name of the LDAP directory, where the LDAP users exist, how often to synchronize the data, and so on.

When LDAP synchronization happens, users get added to the Cisco Unified Communications Manager and are assigned with extensions. With the introduction of Self-Provisioning, changes to a user's primary telephone number in LDAP are synced to the user. However, the extension that was assigned based upon mask and the old primary number is not updated with the new number. And, deleting the user does not delete the extension, thus retaining the extension on the phone that it was assigned to.



Note

Assuming LDAP data is accurate, during LDAP synchronization, and using the mask, extensions are created based on the desired requirements. If LDAP data is not accurate, it can create undesired extensions and can affect dial plan and routing that can lead to outside dial tones to fail, or be delayed, or some other numbers to not be reachable. Ensure that LDAP data is always accurate to avoid changes in dial plans and routing behavior.

Before You Begin

Before you can synchronize the LDAP directory, you must activate the Cisco DirSync service. For information about how to activate services, see the *Cisco Unified Serviceability Administration Guide*.

LDAP Directory Settings

The following table describes the LDAP directory settings.

Table 1: LDAP Directory Settings

Field	Description
LDAP Directory Information	
LDAP Configuration Name	Enter a unique name (up to 40 characters) for the LDAP directory.
LDAP Manager Distinguished Name	Enter the user ID (up to 128 characters) of the LDAP Manager, who is an administrative user that has access rights to the LDAP directory in question.
LDAP Password	Enter a password (up to 128 characters) for the LDAP Manager.
Confirm Password	Reenter the password that you provided in the LDAP Password field.
LDAP User Search Base	<p>Enter the location (up to 256 characters) where all LDAP users exist. This location acts as a container or a directory. This information varies depending on customer setup.</p> <p>Note This field is mandatory.</p>

Field	Description
LDAP Custom Filter	<p>Select an LDAP custom filter from the drop-down list. The LDAP filter filters the results of LDAP searches. LDAP users that match the filter get imported into the Cisco Unified Communications Manager database, but LDAP users that do not match the filter do not get imported.</p> <p>The default value is <None>. This value applies a default LDAP filter that is specific to the LDAP server type. These are the default LDAP filters:</p> <ul style="list-style-type: none"> • Microsoft Active Directory (AD):(&(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:12840,113556,14803=2))) • iPlanet or Sun One LDAP Server:(objectclass=inetOrgPerson) • OpenLDAP:(objectclass=inetOrgPerson) • Microsoft Active Directory Application Mode (ADAM):(&(objectclass=user)(!(objectclass=Computer))(!(UserAccountControl:12840,113556,14803=2)))
LDAP Directory Synchronization Schedule	
Perform Sync Just Once	<p>If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database only once, check this check box.</p>

Field		Description
Perform a Re-sync Every		<p>If you want to perform synchronization of the data in this LDAP directory with the data in the Cisco Unified Communications Manager database at a regular interval, use these fields.</p> <p>In the left field, enter a number. In the drop-down list box, choose a value:</p> <ul style="list-style-type: none"> • hours • days • weeks • months <p>Cisco Unified Communications Manager can synchronize directory information every 6 hours, which is the minimum value allowed for this field.</p> <p>Note This field remains active only if you do not check the Perform Sync Just Once check box.</p>
Next Re-sync Time (YYYY-MM-DD hh:mm)		Specify a time to perform the next synchronization of Cisco Unified Communications Manager directory data with this LDAP directory. Use a 24-hour clock to specify the time of day. For example, 1:00 pm equals 13:00.
Standard User Fields To Be Synchronized		
Cisco Unified Communications Manager User Fields	LDAP User Fields	
User ID	sAMAccountNameoruid	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p> <p>Note Cisco recommends that you do not use a slash (/) in the User ID field. Cisco User Data Services will not function properly for the user when the User ID contains a slash.</p>

Field		Description
Middle Name	(drop-down list box)	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p> <p>For the LDAP User field, choose one of the following values:</p> <ul style="list-style-type: none"> • middleName • initials
Manager ID	manager	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p>
Work Number	(drop-down list box)	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p> <p>For the LDAP User field, choose one of the following values:</p> <ul style="list-style-type: none"> • telephoneNumber • ipPhone
Title	title	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p>
Mobile Number	mobile	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p>

Field		Description
Directory URI	(drop-down list box)	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p> <p>For the LDAP User field, choose one of the following values:</p> <ul style="list-style-type: none"> • msRTCSIP-primaryuseraddress • mail • None <p>Note The msRTCSIP-primaryuseraddress option is only available if you choose Microsoft Active Directory as the LDAP Server Type in the LDAP System Configuration window.</p> <p>Note By default, the user portion of a directory URI is case-sensitive. Under this setting, whatever case the directory URI has in LDAP will be imported into Cisco Unified Communications Manager. For compatibility with third party call control systems, Cisco recommends that you change this setting by setting the value of the URI Lookup Policy enterprise parameter to case-insensitive.</p>
First Name	givenName	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Last Name	sn	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.

Field		Description
Department	departmentordepart mentnumber	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Mail ID	(drop-down list box)	<p>For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.</p> <p>For the LDAP User field, choose one of the following values:</p> <ul style="list-style-type: none"> • mail • sAMAccountName • uid
Home Number	homePhone	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Pager Number	pager	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Display Name	displayName	For these fields, the Cisco Unified Communications Manager data in the field specified at left gets synchronized with the LDAP user data in the field specified at right.
Custom User Fields To Be Synchronized		

Field	Description
Custom User Field Name	<p>Cisco Unified Communications Manager allows you to synchronize LDAP directory attributes that are not included among the defaults for the Standard User Fields to be Synchronized. Using Custom User Fields, you can synchronize LDAP attributes to a customized field that gets saved in the Cisco Unified Communications Manager database.</p> <p>In the Custom User Field text box, enter a name for the customized field that you want to create. The custom user field can contain up to 64 alphanumeric characters, including spaces. Cisco Unified Communications Manager saves the new customized field in the database.</p> <p>You can create up to five custom user fields. Click the (+) button to add additional rows on which you can create new fields.</p>
LDAP Attribute	<p>In the LDAP attribute field, enter a valid LDAP attribute that exists in your LDAP directory. The maximum field length is 128 characters.</p>
Group Information	

Field	Description
Access Control Groups	<p>Use this option to manage the Access Control Group to configure different levels of access for new users that were synchronized from the LDAP directory.</p> <p>Click the Add to Access Control Group button to open the Find and List Access Control Groups window. From the list, select one or more Access Control Groups for a user. Click the Add Selected button. The Find and List Access Control Groups window closes, and the Update Users Configuration window now shows the selected groups in the list box.</p> <p>To delete an existing Access Control Group, select the relevant Access Control Group from the list box. Click the Remove from Access Control button to complete the process.</p> <p>To add a new Access Control Group to the Find and List Access Control Groups window, use the following menu path: User Management > User Settings > Access Control Group</p>

Field	Description
Feature Group Template	<p>From the drop-down list box, select the Feature Group template to be associated with the new users that are synchronized from the LDAP directory.</p> <p>To create a Feature Group template that includes features such as mobility and IM and Presence, use the following menu path: User Management > User/Phone Add > Feature Group Template</p> <p>If you do not select a feature group template, a warning message displays as mentioned below:</p> <p>Warning If no template is selected, the new line features below will not be active.</p> <p>If you select a custom feature group template with no user profile, a warning message displays as mentioned below:</p> <p>Warning The selected Feature Group Template does not have a Universal Line Template configured. The new line features below will not be active.</p>
Apply mask to synced telephone numbers to create a new line for inserted users	<p>Check the check box to apply mask to the synced telephone number of the user.</p> <p>Enter a mask value in the Mask text box. The Mask can contain one to twenty four characters including numbers (0-9), X, and x. It must include at least one x or X.</p> <p>For example, if you set the mask as 11XX for the user with a telephone number 8889945, after the mask is applied, 1145 becomes the primary extension of the user.</p>
Assign new line from the pool list if one was not created based on a synced LDAP telephone number	<p>Check the check box to assign a new line from the DN pool list.</p>

Field	Description
Next Candidate DN	<p>Displays the next probable DN that will be assigned to the user.</p> <p>The DN from the next DN pool is displayed only after all the DNs from the first DN pool are assigned.</p> <p>Note The Next Candidate DN displays only when you check the Assign new line from the pool list if one was not created based on a synced LDAP telephone number check box.</p>

Field	Description
Add DN Pool	<p>By default, only one DN pool is available. Click this option to add more DN's to the DN pool.</p> <p>The DN Pool Start and DN Pool End values must conform to the following requirements:</p> <ul style="list-style-type: none"> • Must be a number and can contain one to twenty characters • DN Pool End must be greater than DN Pool Start • DN Pool Start and DN Pool End must not be null • DN range must be less than 10,000,000 <p>Note The following error message displays if the DN range is not less than 10,000,000: The DN range must be less than 10,000,000. Also, the Start DN and End DN can only vary in the rightmost seven digits. If the DN's are greater than seven digits long, the additional leftmost digits must be identical.</p> <p>Enter the DN Pool Start and DN Pool End values in the text box. You can reorder the DN pool to prioritize the DN's that you want to assign.</p> <p>If the length of the start and end DN pools are different, an error message displays: The DN's length must be identical.</p> <p>You can create only three DN pools.</p>
LDAP Server Information	

Field	Description
Host Name or IP Address for Server	Enter the host name or IP address of the server where the data for this LDAP directory resides.

Field	Description
LDAP Port	<p>Enter the port number on which the corporate directory receives the LDAP requests. You can only access this field if LDAP authentication for end users is enabled.</p> <p>The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636.</p> <p>How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers:</p> <p>LDAP Port when LDAP server is not a Global Catalog server:</p> <ul style="list-style-type: none"> • 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.) • 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) <p>LDAP Port when LDAP server Is a Global Catalog server:</p> <ul style="list-style-type: none"> • 3268—When SSL is not required. • 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) <p>Tip Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.</p>

Field	Description
Use SSL	<p>Check this check box to use Secured Sockets Layer (SSL) encryption for security purposes.</p> <p>Note If LDAP over SSL is required, the corporate directory SSL certificate must be loaded into Cisco Unified Communications Manager. The <i>Cisco Unified Communications Operating System Administration Guide</i> documents the certificate upload procedure in the Security chapter.</p>
Add Another Redundant LDAP Server	Click this button to add another row for entry of information about an additional server.
Perform Full Sync	Click this button to perform a full directory sync. While the directory is synchronizing, the button name changes to Cancel Full Sync. You can click the Cancel Full Sync button to cancel the sync.

In addition to the user fields that appear in Cisco Unified Communications Manager Administration, the Microsoft Active Directory user fields that are described in the following table also get synchronized.

Table 2: Additional Synchronized Microsoft Active Directory User Fields

Cisco Unified Communications Manager User Fields	LDAP User Fields
UniqueIdentifier	ObjectGUID
OCSPPrimaryUserAddress	msRTCSIP-primaryuseraddress

