



CISCO Configure LDAP Synchronization User Guide

[Home](#) » [Cisco](#) » CISCO Configure LDAP Synchronization User Guide 

CISCO Configure LDAP Synchronization



Contents

- [1 LDAP Synchronization Overview](#)
- [2 LDAP Synchronization Prerequisites](#)
- [3 LDAP Synchronization Configuration Task Flow](#)
- [4 Activate the Cisco DirSync Service](#)
- [5 Enable LDAP Directory Synchronization](#)
- [6 Create an LDAP Filter](#)
- [7 Configure LDAP Directory Sync](#)
- [8 Configure Enterprise Directory User Search](#)
- [9 Configure LDAP Authentication](#)
- [10 Customize LDAP Agreement Service Parameters](#)
- [11 Documents / Resources](#)
- [12 Related Posts](#)

LDAP Synchronization Overview

Lightweight Directory Access Protocol (LDAP) synchronization helps you to provision and configure end users for your system. During LDAP synchronization, the system imports a list of users and associated user data from an external LDAP directory into the Unified Communications Manager database. You can also configure your end users while the import occurs.



Note Unified Communications Manager supports LDAPS (LDAP with SSL) but does not support LDAP with StartTLS. Ensure that you upload the LDAP server certificate to Unified Communications Manager as a Tomcat-Trust.

See the Compatibility Matrix for Cisco Unified Communications Manager and the IM and Presence Service for information on the supported LDAP directories.

LDAP synchronization advertises the following functionalities:

- **Importing End Users—You** can use LDAP synchronization during the initial system setup to import your user list from a company LDAP directory into the Unified Communications Manager database. If you've preconfigured items such as feature group templates, user profiles, service profiles, universal device and line templates, you can apply configurations to your users, and assign configured directory numbers and directory URIs during the sync process. The LDAP synchronization process imports the list of users and user-specific data and applies the configuration templates that you've set up.



Note You cannot make edits to an LDAP synchronization once the initial synchronization has occurred already.

- **Scheduled Updates—You** can configure Unified Communications Manager to synchronize with multiple LDAP directories at scheduled intervals to ensure that the database is updated regularly and user data is up-to-date.
- **Authenticate End Users—You** can configure your system to authenticate end user passwords against the LDAP directory rather than the Cisco Unified Communications Manager database. LDAP authentication provides companies with the ability to assign a single password to end users for all company applications. This functionality does not apply to PINs or application user passwords.
- **Directory Server User Search for Cisco Mobile and Remote Access Clients and Endpoints—You** can search a corporate directory server even when operating outside the enterprise firewall. When this feature is enabled, the User Data Service (UDS) acts as a proxy and sends the user search request to the corporate directory instead of sending it to the Unified Communications Manager database.

LDAP Synchronization Prerequisites

Prerequisite Tasks

Before you import end users from an LDAP directory, complete the following tasks:

- **Configure User Access.** Decide which access control groups you want to assign to your users. For many deployments, the default groups are sufficient. If you need to customize your roles and groups, refer to the 'Manage User Access' chapter of the Administration Guide.
- **Configure Default credentials** for a credential policy that is applied by default to newly provisioned users.
- **If you are syncing users from an LDAP directory,** make sure that you have a Feature Group Template set up that includes the User Profiles, Service Profiles, and Universal Line and Device Template settings that you want to assign to your users phones and phone extensions.



Note For users whose data you want to synchronize to your system, ensure that their email ID fields on the Active Directory server are unique entries or left blank.

LDAP Synchronization Configuration Task Flow

Use the following tasks to pull a user list from the external LDAP directory and import it into the Unified



Note If you have already synced the LDAP directory once, you can still sync new items from your external LDAP directory, but you cannot add new configurations Unified Communications Manager to the LDAP directory sync. In this case, you can use the Bulk Administration Tool and menus such as Update Users or Insert Users. Refer to the Bulk Administration Guide for Cisco Unified Communications Manager.

Procedure

	Command or Action	Purpose
Step 1	Activate the Cisco DirSync Service, on page 3	Log in to Cisco Unified Serviceability and activate the Cisco DirSync service.
Step 2	Enable LDAP Directory Synchronization, on page 4	Enable LDAP directory synchronization in Unified Communications Manager.
Step 3	Create an LDAP Filter, on page 4	Optional. Create an LDAP filter if you want Unified Communications Manager to synchronize only a subset of users from your corporate LDAP directory.
Step 4	Configure LDAP Directory Sync, on page 5	Configure settings for the LDAP directory sync such as field settings, LDAP server locations, synchronization schedules, and assignments for access control groups, feature group templates, and primary extensions.

Step 5	Configure Enterprise Directory User Search, on page 7	Optional. Configure the system for enterprise directory server user searches. Follow this procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.
Step 6	Configure LDAP Authentication, on page 7	Optional. If you want to use the LDAP directory for end user password authentication, configure LDAP authentication settings.
Step 7	Customize LDAP Agreement Service Parameters, on page 8	Optional. Configure the optional LDAP Synchronization service parameters. For most deployments, the default values are sufficient.

Activate the Cisco DirSync Service

Perform this procedure to activate the Cisco DirSync Service in Cisco Unified Serviceability. You must activate this service if you want to synchronize end user settings from a corporate LDAP directory.

Procedure

- **Step 1** From Cisco Unified Serviceability, choose Tools > Service Activation.
- **Step 2** From the Server drop-down list, choose the publisher node.
- **Step 3** Under Directory Services, click the Cisco DirSync radio button.
- **Step 4** Click Save.

Enable LDAP Directory Synchronization

Perform this procedure if you want to configure Unified Communications Manager to synchronize end user settings from a corporate LDAP directory.



Note If you have already synced the LDAP directory once, you can still sync new users from your external LDAP directory, but you cannot add new configurations in Unified Communications Manager to the LDAP directory sync. You also cannot add edits to underlying configuration items such as the feature group template or user profile. If you have already completed one LDAP sync, and want to add users with different settings, you can use Bulk Administration menus such as Update Users or Insert Users.

Procedure

- Step 1 From Cisco Unified CM Administration, choose System > LDAP > LDAP System.
- Step 2 If you want Unified Communications Manager to import users from your LDAP directory, check the Enable Synchronizing from LDAP Server check box.
- Step 3 From the LDAP Server Type drop-down list, choose the type of LDAP directory server that your company uses.
- Step 4 From the LDAP Attribute for User ID drop-down list, choose the attribute from your corporate LDAP directory that you want Unified Communications Manager to synchronize with for the User ID field in the End User Configuration window.
- Step 5 Click Save.

Create an LDAP Filter

You can create an LDAP filter to limit your LDAP synchronization to a subset of users from your LDAP directory. When you apply the LDAP filter to your LDAP directory, Unified Communications Manager imports only those users from the LDAP directory who match the filter.



Note Any LDAP filter that you configure must comply with the LDAP search filter standards that are specified in RFC4515.

Procedure

- Step 1 In Cisco Unified CM Administration, choose System > LDAP > LDAP Filter.
- Step 2 Click Add New to create a new LDAP filter.
- Step 3 In the Filter Name text box, enter a name for your LDAP filter.
- Step 4 In the Filter text box, enter a filter. The filter can contain a maximum of 1024 UTF-8 characters and must be enclosed in parentheses ().
- Step 5 Click Save.

Configure LDAP Directory Sync

Use this procedure to configure Unified Communications Manager to synchronize with an LDAP directory.

LDAP directory synchronization allows you to import end user data from an external LDAP directory into the Unified Communications Manager database such that it displays in End User Configuration window. If you have setup feature group templates with universal line and device templates, you can assign settings to newly provisioned users and their extensions automatically



Tip If you are assigning access control groups or feature group templates, you can use an LDAP filter to limit the import to the group of users with the same configuration requirements.

Procedure

- Step 1 From Cisco Unified CM Administration, choose System > LDAP > LDAP Directory.

- Step 2 Perform one of the following steps:
 - Click Find and select an existing LDAP directory.
 - Click Add New to create a new LDAP directory.
- Step 3 In the LDAP Directory Configuration window, enter the following:
 - a) In the LDAP Configuration Name field, assign a unique name to the LDAP directory.
 - b) In the LDAP Manager Distinguished Name field, enter a user ID with access to the LDAP directory server.
 - c) Enter and confirm the password details.
 - d) In the LDAP User Search Space field, enter the search space details.
 - e) In the LDAP Custom Filter for UsersSynchronize field,select either Users Only or Users and Groups.
 - f) (Optional). If you want to limit the import to only a subset of users who meet a specific profile, from the LDAP Custom Filter for Groups drop-down list, select an LDAP filter.
- Step 4 In the LDAP Directory Synchronization Schedule fields, create a schedule that Unified Communications Manager uses to synchronize data with the external LDAP directory.
- Step 5 Complete the Standard User Fields to be Synchronized section. For each End User field, choose an LDAP attribute. The synchronization process assigns the value of the LDAP attribute to the end user field in Unified Communications Manager.
- Step 6 If you are deploying URI dialing, make sure to assign the LDAP attribute that will be used for the user's primary directory URI address.
- Step 7 In the Custom User Fields To Be Synchronized section, enter custom user field name with the required LDAP attribute.
- Step 8 To assign the imported end users to an access control group that is common to all the imported end users, do the following
 - a) Click Add to Access Control Group.
 - b) In the pop-up window, click the corresponding check box for each access control group that you want to assign to the imported end users.
 - c) Click Add Selected.
- Step 9 If you want to assign a feature group template, select the template from the Feature Group Template drop-down list.



Note The end users are synced with the assigned Feature Group Template only for the first time when the users are not present. If an existing Feature Group Template is modified and a full sync is performed for the associated LDAP, the modifications will not get updated.

- Step 10 If you want to assign primary extension by applying a mask to imported telephone numbers, do the following:
 - a) Check the Apply mask to synced telephone numbers to create a new line for inserted users check box.
 - b) Enter a Mask.For example, a mask of 11XX creates a primary extension of 1145 if the imported telephone number is 8889945.
- Step 11 If you want to assign primary extensions from a pool of directory numbers, do the following:
 - a) Check the Assignnew line from thepoollist if one wasnot createdbasedona synced LDAP telephone number check box.
 - b) In the DN Pool Start and DN Pool End text boxes, enter the range of directory numbers from which to select primary extensions.
- Step 12 In the LDAP Server Information section, enter the hostname or IP address of the LDAP server.
- Step 13 If you want to use TLS to create a secure connection to the LDAP server, check the Use TLS check

box.

- Step 14 Click Save.
- Step 15 To complete an LDAP sync, click Perform Full Sync Now. Otherwise, you can wait for the scheduled sync.



Note

When users are deleted in LDAP, they will automatically be removed from Unified Communications Manager after 24 hours. Also, if the deleted user is configured as a mobility user for any of the following devices, these inactive devices will also be automatically deleted:

- Remote Destination Profile
- Remote Destination Profile Template
- Mobile Smart Client
- CTI Remote Device
- Spark Remote Device
- Nokia S60
- Cisco Dual Mode for iPhone
- IMS-integrated Mobile (Basic)
- Carrier-integrated Mobile
- Cisco Dual Mode for Android

Configure Enterprise Directory User Search

Use this procedure to configure phones and clients in your system to perform user searches against an enterprise directory server instead of the database.

Before you begin

- Ensure that the primary, secondary, and tertiary servers, which you choose for LDAP user search, are network reachable to the Unified Communications Manager subscriber nodes.
- From System > LDAP > LDAP System, configure the type of LDAP server from the LDAP Server Type drop-down list in the LDAP System Configuration window.

Procedure

- Step 1 In Cisco Unified CM Administration, choose System > LDAP > LDAP Search.
- Step 2 To enable user searches to be performed using an enterprise LDAP directory server, check the Enable user search to Enterprise Directory Server check box.
- Step 3 Configure the fields in the LDAP Search Configuration window. See the online help for more information about the fields and their configuration options.
- Step 4 Click Save.



Note To search conference rooms represented as Room objects in OpenLDAP Server, configure the custom filter as `(|(objectClass=intOrgPerson)(objectClass=rooms))`. This allows Cisco Jabber client to search

conference rooms by their name and dial the number associated with the room.

Conference rooms are searchable provided givenName or sn or mail or displayName or telephonenumber attribute is configured in the OpenLDAP server for a room object.

Configure LDAP Authentication

Perform this procedure if you want to enable LDAP authentication so that end user passwords are authenticated against the password that is assigned in the company LDAP directory. This configuration applies to end user passwords only and does not apply to end user PINs or application user passwords.

Procedure

- Step 1 In Cisco Unified CM Administration, choose System > LDAP > LDAP Authentication.
- Step 2 Check the Use LDAP Authentication for End Users check box to use your LDAP directory for user authentication.
- Step 3 In the LDAP Manager Distinguished Name field, enter the user ID of the LDAP Manager who has access rights to the LDAP directory.
- Step 4 In the Confirm Password field, enter the password for the LDAP manager.
- Step 5 In the LDAP User Search Base field, enter the search criteria.
- Step 6 In the LDAP Server Information section, enter the hostname or IP address of the LDAP server.
- Step 7 If you want to use TLS to create a secure connection to the LDAP server, check the Use TLS check box.
- Step 8 Click Save.

What to do next

Customize LDAP Agreement Service Parameters, on page 8

Customize LDAP Agreement Service Parameters

Perform this procedure to configure the optional service parameters that customize the system-level settings for LDAP agreements. If you do not configure these service parameters, Unified Communications Manager applies the default settings for LDAP directory integration. For parameter descriptions, click the parameter name in the user interface.


You can use service parameters to customize the below settings:

- Maximum Number of Agreements—Default value is 20.
- Maximum Number of Hosts—Default value is 3.
- Retry Delay On Host Failure (secs)—Default value for host failure is 5.
- Retry Delay On HotList failure (mins)—Default value for hostlist failure is 10.
- LDAP Connection Timeouts (secs)—Default value is 5.
- Delayed Sync Start time (mins)—Default value is 5.
- User Customer Map Audit Time

Procedure

- Step 1 From Cisco Unified CM Administration, choose System > Service Parameters.
- Step 2 From the Server drop-down list box, choose the publisher node.
- Step 3 From the Service drop-down list box, choose Cisco DirSync.
- Step 4 Configure values for the Cisco DirSync service parameters.
- Step 5 Click Save.

Documents / Resources

 <p>Configure LDAP Synchronization</p> <p>LDAP Synchronization Overview</p> <p>The LDAP Synchronization Overview section provides a high-level overview of the LDAP Synchronization process, including the components involved and the steps to configure and manage the synchronization.</p> <p>1. Overview</p> <p>2. Components</p> <p>3. Steps to Configure and Manage the Synchronization</p> <p>4. Troubleshooting</p> <p>5. Appendix</p>	<p>CISCO Configure LDAP Synchronization [pdf] User Guide</p> <p>Configure LDAP Synchronization, LDAP Synchronization, Synchronization</p>
--	---

Manuals+.