CUCM Configuration for LDAP

Enable LDAP Integration

Follow these steps to enable LDAP integration with Active Directory (AD) or OpenLDAP. Note the following limitations:

- Only one LDAP server can be enabled at each hierarchy node. Attempting to enable more than one causes the transaction to fail.
- Adding the same LDAP server with the same Search Base DN to any of the related hierarchies causes the LDAP server addition transaction to fail.

Procedure

Step 1 Log in as a provider, reseller, or customer administrator.

Step 2 Set the hierarchy node to the desired node where you want the users synchronized.

Step 3 Navigate to **LDAP Management** > **LDAP Server**.

Step 4 Click **Add**.

Step 5 Complete the fields:

Fields	Description
Description	Defaults to the current hierarchy level
Hostname	Hostname or IP address of the LDAP server . This field is required.
Port	Port number for LDAP traffic. Defaults to 389.
User DN	The User Distinguished Name of an administrative user who has access rights to the Base DN on the LDAP server. This field is required.

Fields	Description
Admin Password	Admin password associated with the user. This field is required.
Search Base DN	Base Distinguished Name for LDAP search. This should be a container or directory on the LDAP server where the LDAP users exist (for example, an Organization Unit or OU). This field is required.
Server Type	LDAP server type
AD Sync Mode	Defaults to Direct.
CUCM LDAP Directory Name	The LDAP Directory configured on Cisco Unified Communications Manager that users are considered synced from. Required for users that are synced from this LDAP server to use SSO or LDAP Authentication to login to Cisco Unified CM.
Encryption Method	Choose between No Encryption, Use SSL Encryption (ldaps://), or Use StartTLS Extension.
Server Root Certificate	If Trust All is not checked, the LDAP server's SSL certificate is validated against this root certificate. If no Server Root Certificate is specified, validation is done against any existing trusted CA certificates. Use this option for custom root certificates in .pem format. See the SSO Certificate Management section of *Cisco Unified Communications Domain Manager, Release 10.6(2) Maintain and Operate Guide* for more information.
Trust All	Check to disable certificate validation.

Step 6 Click **Save** to save the LDAP server.

What to Do Next

Perform a test connection to ensure the LDAP server is configured correctly.

Set up LDAP for User Synchronization

Follow these steps to set up an LDAP for user synchronization. This process syncs users from the configured LDAP directory into Cisco Unified CDM. The users then appear at the hierarchy node at which the LDAP User Sync object exists. You can manage the users through User Management menu options (for example, move users to other hierarchies, or push to Cisco Unified Communications Manager).

Procedure

Step 1 Log in as a provider, reseller, or customer administrator.

Step 2 Set the hierarchy path to the node where you have set up the LDAP server you want to sync users from.

Step 3 Select **LDAP Management** > **LDAP User Sync**.

Step 4 Click **Add**.

Step 5 On the Base tab, provide the following information:

Field	Description
LDAP Server	This read-only field displays the LDAP Server you are syncing users from.
User Model Type	The User Model Type identifies which LDAP object, defined in the configured LDAP server, is used to import and authenticate users. If the LDAP server is Active Directory, the default is device/ldap/user. If the LDAP server is OpenLDAP, the default is device/ldap/inetOrgPerson. To identify a non-default User Model Type to use, contact the LDAP administrator for the LDAP server from which you are syncing users.
User Entitlement Profile	Select the User Entitlement Profile that specifies the devices and services to which users synced from the LDAP server are entitled. The selected entitlement profile is assigned to each synced user. It is checked during user provisioning to ensure the user's configuration does not exceed the allowed services and devices specified in the entitlement profile.
User Role	Select the User Role to be assigned to all synchronized users. This value can be changed manually for individual users after synchronization. This field is mandatory
User Move Mode	Indicates whether users are automatically moved to sites based on the filters and filter order defined in **User Management** > **Manage Filters**.
User Delete Mode	Indicates whether users are automatically deleted from Cisco Unified CDM if they are deleted from the LDAP directory. If set to automatic, all subscriber resources associated with the user, such as a phone, are also deleted.
User Purge Mode	Indicates whether users are automatically deleted from Cisco Unified CDM if they are purged from the LDAP device model. An administrator can remove the LDAP user from the device layer even if the user has not been removed from the LDAP directory.

Step 6 Click the **Field Mappings** tab and enter the following required mappings:

- *LDAP Username* (for example, sAMAccountName)
- *Surname*

Step 7 (Optional) Complete other field mappings as desired, for other operations such as pushing users to Cisco Unified Communications Manager or creating move filters.

Step 8 Click **Save**.

An LDAP synchronization is scheduled, but is not activated by default. See Sync Users from LDAP, on page 4.

Sync Users from LDAP

You can synchronize users from LDAP by activating a scheduled synchronization, or by performing a manual synchronization.

Note A synchronization cannot be cancelled, and an LDAP server cannot be deleted while a synchronization is in progress.

Procedure

Step 1 To activate a scheduled LDAP synchronization:

a) Navigate to **LDAP Management** > **LDAP Schedule**.
b) Click an LDAP Schedule.
c) Check the **Active** check box.
d) Click **Save**.

Step 2 To perform a manual LDAP synchronization, see Sync and Purge LDAP Users.

Cisco Unified Communications Domain Manager 10.6(x) attempts to synchronize users from the LDAP server. It may take a few minutes for the users to show up in Cisco Unified Communications Domain Manager 10.6(x).

What to Do Next

Navigate to **User Management** > **Users** and verify that users have been synchronized from LDAP.