Configure LDAP Directory

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 Authentication for End Users

LDAP synchronization allows you to 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

In previous releases, when a user with a Cisco mobile and remote access client (for example, Cisco Jabber) or endpoint (for example, Cisco DX 80 phone) performed a user search while outside the enterprise firewall, results were based on those user accounts that are saved in the Cisco Unified Communications Manager database. The database contains user accounts which are either configured locally or synchronized from the corporate directory.

With this release, Cisco mobile and remote access clients and endpoints can now 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 Cisco Unified Communications Manager database.

Use this feature to achieve the following results:

- Deliver the same user search results regardless of geographic location—Mobile and remote access clients and endpoints can perform user searches by using the corporate directory; even when they are connected outside the enterprise firewall.
- Reduce the number of user accounts that are configured in the Cisco Unified Communications Manager database—Mobile clients can now search users in the corporate directory. In the previous releases, user search results were based on the users that are configured in the database. Now, administrators no longer need to configure or synchronize user accounts to the database solely for user searches. Administrators need to configure only those user accounts that are served by a cluster. Reducing the total number of user accounts in the database shortens software upgrade time frames while improving overall database performance.

To configure this feature, you must enable the **Enable user search to Enterprise Directory Server** option in the **LDAP Search Configuration** window, and configure the LDAP directory server details. For details, see the Configure Enterprise Directory User Search, on page 8 procedure.

LDAP Synchronization Prerequisites

Prerequisite Tasks

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

- Configure User Access
- Configure Credential Policy
- Configure Feature Group Template

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 Communications Manager database.

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 in 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 4	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 5	**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 8	**Optional**. Configure the system for enterprise directory server user searches. Follow this

	Command or Action	Purpose
		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 9	**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 10	**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 Users Synchronize** 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 a 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 **Assign new line from the pool list if one was not created based on a 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 (Optional) In the Jabber Endpoint Provisioning section, select one of the required Jabber devices for auto provisioning from the following drop-down in case you want to create a Jabber device:

- Cisco Dual Mode for Android (BOT)
- Cisco Dual Mode for iPhone (TCT)
- Cisco Jabber for Tablet (TAB)
- Cisco Unified Client Services Framework (CSF)

Note The **Write back to LDAP** option allows you to write the Primary DN chosen from Unified CM back to the LDAP server. LDAP attributes available for write back are: **telephoneNumber**, **ipPhone**, and **mobile**.

Step 13 In the **LDAP Server Information** section, enter the hostname or IP address of the LDAP server.

Step 14 If you want to use TLS to create a secure connection to the LDAP server, check the **Use TLS** check box.

Note Sometimes, when we try to synchronize users through the secure port after restarting tomcat, the users will not be synchronized. You must restart the Cisco DirSync service for the user synchronization to happen successfully.

Step 15 Click **Save**.

Step 16 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.

LDAP Attributes for UDS Search of Directory Server

The following table lists the LDAP attributes that UDS users search request uses when the **Enable user search to Enterprise Directory Server** option is enabled. For these types of directory requests, UDS acts as a proxy and relays the search request to the corporate directory server.

Note UDS users response tag may be mapped to one of the LDAP attributes. The mapping of the attributes is determined by the option you select from the **LDAP Server Type** drop-down list. Access this drop-down list from **System** > **LDAP** > **LDAP System Configuration** window.

UDS Users Response Tag	LDAP Attribute
userName	• samAccountName • uid
firstName	givenName

UDS Users Response Tag	LDAP Attribute
lastName	sn
middleName	• initials • middleName
nickName	nickName
displayName	displayName
phoneNumber	• telephonenumber • ipPhone
homeNumber	homephone
mobileNumber	mobile
email	mail
directoryUri	• msRTCSIP-primaryuseraddress • mail
department	• department • departmentNumber
manager	manager
title	title
pager	pager

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 10

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**.

LDAP Directory Service Parameters

Service Parameter	Description
Maximum Number Of Agreements	The maximum number of LDAP directories that you can configure. The default setting is 20.

Service Parameter	Description
Maximum Number Of Hosts	The maximum number of LDAP hostnames that you can configure for failover purposes. The default value is 3.
Retry Delay On Host Failure (secs)	After a host failure, the number of seconds that Cisco Unified Communications Manager delays before it retries the connection to the first LDAP server (hostname). The default value is 5.
Retry Delay On HostList Failure (mins)	After a hostlist failure, the number of minutes that Cisco Unified Communications Manager delays before it retries every configured LDAP server (hostnames). The default is 10.
LDAP Connection Timeout (secs)	The number of seconds that Cisco Unified Communications Manager allows for establishing the LDAP connection. The LDAP service provider aborts the connection attempt if a connection cannot be established in the specified amount of time. The default is 5.
Delayed Sync Start time (mins)	The number of minutes that Cisco Unified Communications Manager delays in starting the directory synchronization process after the Cisco DirSync service starts. The default is 5.

Convert LDAP Synchronized User to Local User

When you synchronize your LDAP directory with Cisco Unified Communications Manager, for LDAP-synchronized end users, you cannot edit any of the fields within the **End User Configuration** window unless you convert the LDAP-synchronized user to a local user.

To edit to an LDAP-synchronized field in the **End User Configuration** window, convert the user to a local user. However, if you perform this conversion, the end user will not be updated when Cisco Unified Communications Manager synchronizes with the LDAP directory.

Procedure

Step 1 In Cisco Unified CM Administration, choose **End Users** > **End User Management**.

Step 2 Click **Find** and select the end user.

Step 3 Click the **Convert to Local User** button.

Step 4 Make your updates in the **End User Configuration** window.

Step 5 Click **Save**.

Assign LDAP Synchronized Users to an Access Control Group

Perform this procedure to assign LDAP synchronized users to an access control group.

Before you begin

Cisco Unified Communications Manager must be configured to synchronize end users with an external LDAP directory.

Procedure

Step 1 In Cisco Unified CM Administration, choose **System** > **LDAP** > **LDAP Directory**.

Step 2 Click **Find** and select a configured LDAP Directory.

Step 3 Click the **Add to Access Control Group** button.

Step 4 Select the access control groups that you want to apply to the end users in this LDAP directory.

Step 5 Click **Add Selected**.

Step 6 Click **Save**

Step 7 Click **Perform Full Sync**.
Cisco Unified Communications Manager syncs with the external LDAP directory and synchronized users get inserted into the correct access control group.

Note The synchronized users get inserted into the selected access group only when you add an access control group for the first time. Any subsequent group that you add to LDAP will not be applied to the synchronized users after performing a full sync.

LDAP Directory Integration for Contact Searches on XMPP Clients

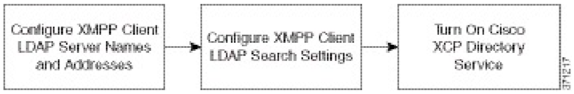
These topics describe how to configure the LDAP settings on IM and Presence Service to allow users of third-party XMPP client to search and add contacts from the LDAP directory.

The JDS component on IM and Presence Service handles the third-party XMPP client communication with the LDAP directory. Third-party XMPP clients send queries to the JDS component on IM and Presence Service. The JDS component sends the LDAP queries to the provisioned LDAP servers, and then sends the results back to the XMPP client.

Before you perform the configuration described here, perform the configuration to integrate the XMPP client with Cisco Unified Communications Manager and IM and Presence Service. See topics related to third party XMPP client application integration.

Figure 1: LDAP Directory Integration for Contact Searches on XMPP Clients Workflow

The following workflow diagram shows the high-level steps to integrate the LDAP directory for contact searches on XMPP clients.


Configure XMPP Client LDAP Server Names and Addresses
Configure XMPP Client LDAP Search Settings
Turn On Cisco XCP Directory Service
371217

The following table lists the tasks to perform to integrate the LDAP directory for contact searches on XMPP clients. For detailed instructions, see the related tasks.

Table 1: Task List for LDAP Directory Integration for Contact Searches on XMPP Clients

Task	Description
Configure XMPP Client LDAP Server Names and Addresses	Upload the root CA certificate to IM and Presence Service as an xmpp-trust-certificate if you enabled SSL and configured a secure connection between the LDAP server and IM and Presence Service. **Tip** The subject CN in the certificate must match the FQDN of the LDAP server.
Configure XMPP Client LDAP Search Settings	You must specify the LDAP search settings that will allow IM and Presence Service to successfully perform contact searches for third-party XMPP clients. You can specify a primary LDAP server and up to two backup LDAP servers. **Tip** Optionally, you can turn on the retrieval of vCards from the LDAP server or allow the vCards to be stored in the local database of IM and Presence Service.
Turn On Cisco XCP Directory Service	You must turn on XCP Directory Service to allow users of a third-party XMPP client to search and add contacts from the LDAP directory. **Tip** Do not turn on the Cisco XCP Directory Service until after you configure the LDAP server and LDAP search settings for third-party XMPP clients; otherwise, the service with stop running.

LDAP Account Lock Issue

If you enter the wrong password for the LDAP server that you configure for third-party XMPP clients, and you restart the XCP services on IM and Presence Service, the JDS component will perform multiple attempts to sign in to the LDAP server with the wrong password. If the LDAP server is configured to lock out an account after a number of failed attempts, then the LDAP server may lock the JDS component out at some point. If the JDS component uses the same credentials as other applications that connect to LDAP (applications that are not necessarily on IM and Presence Service), these applications will also be locked out of LDAP.

To fix this issue, configure a separate user, with the same role and privileges as the existing LDAP user, and allow only JDS to sign in as this second user. If you enter the wrong password for the LDAP server, only the JDS component is locked out from the LDAP server.

Configure LDAP Server Names and Addresses for XMPP Clients

If you choose to enable Secured Sockets Layer (SSL), configure a secure connection between the LDAP server and IM and Presence Service and upload the root Certificate Authority (CA) certificate to IM and Presence Service as an cup-xmpp-trust certificate. The subject common name (CN) in the certificate must match the Fully Qualified Domain Name (FQDN) of the LDAP server.

If you import a certificate chain (more than one certificate from the root node to the trusted node), import all certificates in the chain except the leaf node. For example, if the CA signs the certificate for the LDAP server, import only the CA certificate and not the certificate for the LDAP server.

You can use IPv6 to connect to the LDAP server even though the connection between IM and Presence Service and Cisco Unified Communications Manager is IPv4. If IPv6 gets disabled for either the enterprise parameter or for ETH0 on the IM and Presence Service node, the node can still perform an internal DNS query and connect to the external LDAP server if the hostname of the external LDAP server configured for third-party XMPP clients is a resolvable IPv6 address.

Tip You configure the hostname of the external LDAP server for third-party XMPP clients in the **LDAP Server - Third-Party XMPP Client** window.

Before you begin

Obtain the hostnames or IP addresses of the LDAP directories.

If you use IPv6 to connect to the LDAP server, enable IPv6 on the enterprise parameter and on Eth0 for each IM and Presence Service node in your deployment before you configure the LDAP server.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Third-Party Clients** > **Third-Party LDAP Servers**.

Step 2 Click **Add New**.

Step 3 Enter an ID for the LDAP server.

Step 4 Enter the hostname for the LDAP server.

For IPv6 connections, you can enter the IPv6 address of the LDAP server.

Step 5 Specify the port number on the LDAP server that is listening to the TCP or SSL connection.

The default port is 389. If you enable SSL, specify port 636.

Step 6 Specify the username and the password for the LDAP server. These values must match the credentials you configure on the LDAP server.

See the LDAP directory documentation or the LDAP directory configuration for this information.

Step 7 Check **Enable SSL** if you want to use SSL to communicate with the LDAP server.

Note If SSL is enabled then the **hostname** value which you enter can be either the hostname or the FQDN of the LDAP server. The value that is used must match the value in the security certificate **CN** or **SAN** fields.

If you must use an IP address, then this value must also be used on the certificate for either the **CN** or **SAN** fields.

Step 8 Click **Save**.

Step 9 Start the Cisco XCP Router service on all nodes in the cluster (if this service is not already running).

Tip

- If you enable SSL, the XMPP contact searches may be slower because of the negotiation procedures at SSL connection setup, and data encryption and decryption after IM and Presence Service establishes the SSL connection. As a result, if your users perform XMPP contact searches extensively in your deployment, this could impact the overall system performance.
- You can use the certificate import tool to check the communication with the LDAP server hostname and port value after you upload the certificate for the LDAP server. Choose **Cisco Unified CM IM and Presence Administration** > **System** > **Security** > **Certificate Import Tool**.
- If you make an update to the LDAP server configuration for third-party XMPP clients, restart the Cisco XCP Directory Service. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

What to do next

Proceed to configure LDAP search settings for XMPP clients.

Configure LDAP Search Settings for XMPP Clients

You must specify the LDAP search settings that will allow IM and Presence Service to successfully perform contact search for third-party XMPP clients

Third-party XMPP clients connect to an LDAP server on a per-search basis. If the connection to the primary server fails, the XMPP client tries the first backup LDAP server, and if it is not available, it then tries the second backup server and so on. If an LDAP query is in process when the system fails over, the next available server completes this LDAP query.

Optionally you can turn on the retrieval of vCards from the LDAP server. If you turn on vCard retrieval:

- The corporate LDAP directory stores the vCards.
- When XMPP clients search for their own vCard, or the vCard for a contact, the vCards are retrieved from LDAP via the JDS service.
- Clients cannot set or modify their own vCard as they are not authorized to edit the corporate LDAP directory.

If you turn off the retrieval of vCards from LDAP server:

- IM and Presence Service stores the vCards in the local database.
- When XMPP clients search for their own vCard, or the vCard for a contact, the vCards are retrieved from the local IM and Presence Service database.
- Clients can set or modify their own vCard.

The following table lists the LDAP search settings for XMPP clients.

Table 2: LDAP Search Settings for XMPP Clients

Field	Setting
LDAP Server Type	Choose an LDAP server type from this list: • Microsoft Active Directory • Generic Directory Server - Choose this menu item if you are using any other supported LDAP server type (iPlanet, Sun ONE or OpenLDAP).

Field	Setting
User Object Class	Enter the User Object Class value appropriate to your LDAP server type. This value must match the User Object Class value configured on your LDAP server. If you use Microsoft Active Directory, the default value is ‘user’.
Base Context	Enter the Base Context appropriate to your LDAP server. This value must match a previously configured domain, and/or an organizational structure on your LDAP server.
User Attribute	Enter the User Attribute value appropriate to your LDAP server type. This value must match the User Attribute value configured on your LDAP server. If you use Microsoft Active Directory, the default value is sAMAccountName. If the Directory URI IM address scheme is used and the Directory URI is mapped to either mail or msRTCSIPPrimaryUserAddress, then mail or msRTCSIPPrimaryUserAddress must be specified as the user attribute.
LDAP Server 1	Choose a primary LDAP server.
LDAP Server 2	(Optional) Choose a backup LDAP server.
LDAP Server 3	(Optional) Choose a backup LDAP server.

Before you begin

Specify the LDAP server names and addresses for XMPP clients.

Procedure

Step 1 Choose **Cisco Unified CM IM and Presence Administration** > **Application** > **Third-Party Clients** > **Third-Party LDAP Settings**.

Step 2 Enter information into the fields.

Step 3 Check **Build vCards from LDAP** if you want to enable users to request vCards for their contacts and retrieve the vCard information from the LDAP server. Leave the check box unchecked if you want clients to be able to automatically request vCards for users as users join the contact list. In this case, clients retrieve the vCard information from the local IM and Presence Service database.

Step 4 Enter the LDAP field required to construct the vCard FN field. Clients use the value in the vCard FN field to display the contact's name in the contact list when a user requests a contact's vCard.

Step 5 In the Searchable LDAP Attributes table, map the client user fields to the appropriate LDAP user fields.

If you use Microsoft Active Directory, IM and Presence Service populates the default attribute values in the table.

Step 6 Click **Save**.

Step 7 Start the Cisco XCP Router service (if this service is not already running)

Tip If you make an update to the LDAP search configuration for third-party XMPP clients, restart the Cisco XCP Directory Service. Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Control Center - Feature Services** to restart this service.

What to do next

Proceed to turn on the Cisco XCP directory service.

Turn On Cisco XCP Directory Service

You must turn on the Cisco XCP Directory Service to allow users of a third-party XMPP client to search and add contacts from the LDAP directory. Turn on the Cisco XCP Directory Service on all nodes in the cluster.

Note Do not turn on the Cisco XCP Directory Service until you configure the LDAP server, and LDAP search settings for third-party XMPP clients. If you turn on the Cisco XCP Directory Service, but you do not configure the LDAP server, and LDAP search settings for third-party XMPP clients, the service will start, and then stop again.

Before you begin

Configure the LDAP server, and LDAP search settings for third-party XMPP clients.

Procedure

Step 1 Choose **Cisco Unified IM and Presence Serviceability** > **Tools** > **Service Activation**.

Step 2 Choose the IM and Presence Service node from the Server menu.

Step 3 Choose **Cisco XCP Directory Service**.

Step 4 Click **Save**.