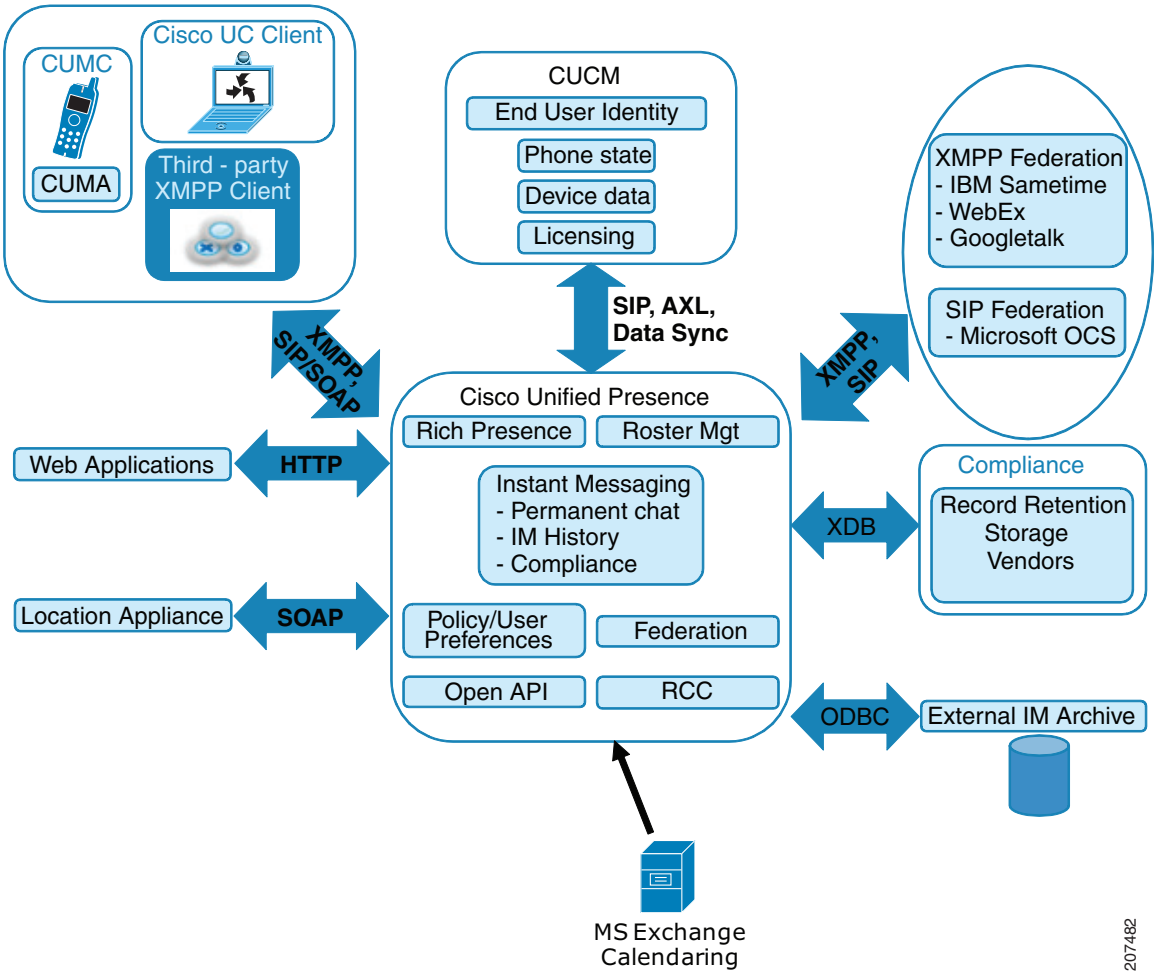
LDAP Directory Integration

July 2, 2014

Figure 9-1 LDAP Interface



LDAP Directory Integration with Cisco Unified Communications Manager

Related Topics

- *Release Notes for Cisco Unified Personal Communicator*:
  http://www.cisco.com/en/US/products/ps6844/prod_release_notes_list.html
- *Cisco Unified Communications Manager System Guide:*
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

Secure Connection between Cisco Unified Communications Manager and the LDAP Directory

You can secure the connection between the Cisco Unified Communications Manager server and the LDAP directory server by enabling a Secure Socket Layer (SSL) connection for the LDAP server on Cisco Unified Communications Manager, and uploading the SSL certificate to Cisco Unified Communications Manager. You must upload the LDAP SSL certificate as a directory-trust certificate on Cisco Unified Communications Manager Release 7.x and earlier, and as a tomcat-trust certificate on Cisco Unified Communications Manager Release 8.x and later.

After you upload the LDAP SSL certificate, you need to restart the following services on Cisco Unified Communications Manager:

- Directory service
- Tomcat service

Related Topics

- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6
- *Cisco Unified Operating System Maintenance Guide for Cisco Unified Presence*

Configure the LDAP Synchronization for User Provisioning

LDAP synchronization uses the Cisco Directory Synchronization (DirSync) tool on Cisco Unified Communications Manager to synchronize information (either manually or periodically) from a corporate LDAP directory. When you enable the DirSync service, Cisco Unified Communications Manager automatically provisions users from the corporate directory. Cisco Unified Communications Manager still uses its local database, but disables its facility to allow you to create user accounts. You use the LDAP directory interface to create and manage user accounts.

Before You Begin

- Make sure that you install the LDAP server before you attempt the LDAP-specific configuration on Cisco Unified Communications Manager.
- Activate the Cisco DirSync service on Cisco Unified Communications Manager.

Restrictions

LDAP synchronization does not apply to application users on Cisco Unified Communications Manager. You must manually provision application users in the Cisco Unified CM Administration interface.

Procedure

Step 1 Choose **Cisco Unified Communications Manager Administration > System > LDAP > LDAP System.**

Step 2 Click **Add New**.

Step 3 Configure the LDAP server type and attribute.

Step 4 Click **Enable Synchronizing from LDAP Server**.

Step 5 Choose **Cisco Unified Communications Manager Administration > System > LDAP > LDAP Directory**

Step 6 Configure the following items:

- LDAP directory account settings
- User attributes to be synchronized
- Synchronization schedule
- LDAP server hostname or IP address, and port number

Step 7 Check **Use SSL** if you want to use Secure Socket Layer (SSL) to communicate with the LDAP directory.

Note If you configure LDAP over SSL, upload the LDAP directory certificate onto Cisco Unified Communications Manager.

Related Topics

- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6
- *Cisco Unified Communication SRND*:
  http://www.cisco.com/go/designzone
- *Cisco Unified Communications Manager Administration Guide*:
  http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html

What To Do Next

Upload LDAP Authentication Server Certificates, page 9-4

Upload LDAP Authentication Server Certificates

When Cisco Unified Communications Manager LDAP authentication is configured for secure mode (port 636 or 3269), LDAP authentication server certificates, such as Certificate Authority (CA) root and all other Intermediate certificates, must be individually uploaded as “tomcat-trust” to the Cisco Unified Presence server.

Procedure

Step 1 Choose **Cisco Unified OS Administration > Security > Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 Choose **tomcat-trust** from the **Certificate Name** menu.

Step 4 Browse and choose the LDAP server root certificate from your local computer.

Step 5 Click **Upload File**.

Step 6 Repeat the above steps for all other intermediate certificates.

Related Topic

Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

What To Do Next

Configure LDAP Authentication, page 9-5

Configure LDAP Authentication

The LDAP authentication feature enables Cisco Unified Communications Manager to authenticate user passwords against the corporate LDAP directory.

Before You Begin

Enable LDAP synchronization on Cisco Unified Communications Manager.

Restrictions

LDAP authentication does not apply to the passwords of application users; Cisco Unified Communications Manager authenticates application users in its internal database.

Procedure

Step 1 Choose **Cisco Unified Communications Manager Administration > System > LDAP > LDAP Authentication**.

Step 2 Enable LDAP authentication for users.

Step 3 Configure the LDAP authentication settings.

Step 4 Configure the LDAP server hostname or IP address, and port number

Note To use Secure Socket Layer (SSL) to communicate with the LDAP directory, check **Use SSL**. If you configure LDAP over SSL, upload the LDAP directory certificate to Cisco Unified Communications Manager.

Related Topics

- Configuring the LDAP Synchronization for User Provisioning, page 9-3
- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

What To Do Next

Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory

This topic is only applicable if you configure a secure connection between Cisco Unified Communications Manager and the LDAP directory.

Note Perform this procedure on all Cisco Unified Presence nodes in the cluster.

Before You Begin

Enable SSL for LDAP on Cisco Unified Communications Manager, and upload the LDAP directory certificate to Cisco Unified Communications Manager.

Procedure

Step 1 Choose **Cisco Unified OS Administration > Security > Certificate Management**.

Step 2 Click **Upload Certificate**.

Step 3 Choose **tomcat-trust** from the Certificate Name menu.

Step 4 Browse and choose the LDAP server certificate from your local computer.

Step 5 Click **Upload File**.

Step 6 Restart the Tomcat service from the CLI using this command:

utils service restart Cisco Tomcat

Related Topic

Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

What To Do Next

LDAP Directory Integration with Cisco Unified Personal Communicator, page 9-6

LDAP Directory Integration with Cisco Unified Personal Communicator

These topics describe how to configure the LDAP settings on Cisco Unified Presence to allow Cisco Unified Personal Communicator users to search and add contacts from the LDAP directory.

Before you perform this configuration, fully integrate the Cisco Unified Personal Communicator client with Cisco Unified Communications Manager and Cisco Unified Presence.

- Configure LDAP Server Names and Addresses for Cisco Unified Personal Communicator, page 9-9
- Create LDAP Profiles and Add Cisco Unified Personal Communicator Users to the Profile, page 9-10

Rules for a Displayed Contact Name

When you configure the user fields in the LDAP attribute map, note the following rules that determine how Cisco Unified Personal Communicator displays contact names:

- If the user edits a contact name in Cisco Unified Personal Communicator, display this name. This is the Nickname LDAP attribute in Cisco Unified Presence.
- If you configure an LDAP user field for DisplayName, display this name.
- If you configure an LDAP user field for Nickname, display this name with the last name.
- Otherwise, display the configured LDAP user fields for the first and last names in the Contact pane. If there is a first name but no last name, display the first name. If there is a last name but no first name, display the last name.
- If you do not configure LDAP user fields for the FirstName and LastName, display the LDAP UserID or the Cisco Unified Presence user ID in the Contact pane.
- If a user adds a non-LDAP contact, the contact details in Cisco Unified Personal Communicator allow the user to edit the Display As name, the first name, and the last name.

Related Topics

- (Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server, page 9-7
- Configure the LDAP Attribute Map for Cisco Unified Personal Communicator, page 9-8

(Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server

You can configure a parameterized URL string in the Photo field in the LDAP attribute map so that Cisco Unified Personal Communicator can fetch pictures from a web server instead of from the LDAP server. The URL string must contain an LDAP attribute with a query value containing a piece of data that uniquely identifies the photo of the user. Cisco recommends that you use the User ID attribute. However, you can use any LDAP attribute whose query value contains a piece of data that uniquely identifies the photo of the user.

Cisco recommends that you use %%<*userID*>%% as the substitution string, for example:

- http://mycompany.cisco.com/photo/std/%%uid%%.jpg
- http://mycompany.cisco.com/photo/std/%%sAMAccountName%%.jpg

You must include the double percent symbols in this string, and they must enclose the name of the LDAP attribute to substitute. Cisco Unified Personal Communicator removes the percent symbols and replaces the parameter inside with the results of an LDAP query for the user whose photo it resolves.

For example, if a query result contains the attribute “uid” with a value of “johndoe,” then a template such as http://mycompany.com/photos/%%uid%%.jpg creates the URL http://mycompany.com/photos/johndoe.jpg. Cisco Unified Personal Communicator attempts to fetch the photo.

This substitution technique works only if Cisco Unified Personal Communicator can use the results of the query and can insert it into the template you specify above to construct a working URL that fetches a JPG photo. If the web server that hosts the photos in a company requires a POST (for example, the name of the user is not in the URL) or uses some other cookie name for the photo instead of the username, this technique does not work.

Note

- The URL length is limited to 50 characters.
- Cisco Unified Personal Communicator does not support authentication for this query; the photo must be retrievable from the web server without credentials.

Related Topics

- Rules for a Displayed Contact Name, page 9-7
- Configure the LDAP Attribute Map for Cisco Unified Personal Communicator, page 9-8

Configure the LDAP Attribute Map for Cisco Unified Personal Communicator

Note The information about fetching a photo from Active Directory in this topic relates only to Cisco Unified Personal Communicator Release 7.1.

You must configure the LDAP attribute map on Cisco Unified Presence where you enter LDAP attributes for your environment and map them to the given Cisco Unified Personal Communicator attributes.

If you want to use LDAP to store your employee profile photos, you must either use a third-party extension to upload the photo files to the LDAP server, or extend the LDAP directory server schema by other means to create an attribute that the LDAP server can associate with an image. For Cisco Unified Personal Communicator to display the profile photo, in the LDAP attribute map, you must map the Cisco Unified Personal Communicator "Photo" value to the appropriate LDAP attribute. By default, Cisco Unified Personal Communicator uses the jpegPhoto LDAP attribute to display the user photo, which is present in the Windows 2003 and 2007 Active Directory schema. Note that Windows 2000 Active Directory uses the thumbnailPhoto attribute.

Before You Begin

- Make sure that you install and set up the LDAP server before you configure the LDAP attribute map on Cisco Unified Presence.
- By default, Cisco Unified Personal Communicator uses the *jpegPhoto* LDAP attribute, which is present in the Windows 2003 Active Directory schema. By contrast, the Windows 2000 Active Directory uses the *thumbnailPhoto* attribute.

Restrictions

- The UPC UserID setting in the LDAP attribute map must match the Cisco Unified Communications Manager user ID. This mapping allows a user to add a contact from LDAP to the Contact list in Cisco Unified Personal Communicator. This field associates the LDAP user with the associated user on Cisco Unified Communications Manager and Cisco Unified Presence.
- You can map an LDAP field to only one Cisco Unified Personal Communicator field.

Procedure

Step 1 Choose **Cisco Unified Presence Administration > Application > Cisco Jabber > Settings**

Step 2 Choose a supported LDAP server from Directory Server Type.

The LDAP server populates the LDAP attribute map with Cisco Unified Personal Communicator user fields and LDAP user fields.

Step 3 If necessary, make modifications to the LDAP field to match your specific LDAP directory. The values are common to all LDAP server hosts. Note the following LDAP directory product mappings:

Product	LastName Mapping	UserID Mapping
Microsoft Active Directory	SN	sAMAccountName
iPlanet, Sun ONE or OpenLDAP	SN	uid

Step 4 Click **Save**.

Related Topics

- Rules for a Displayed Contact Name, page 9-7
- (Cisco Unified Personal Communicator Release 8.0) Fetch Contact Pictures from a Web Server, page 9-7

What To Do Next

Configure LDAP Server Names and Addresses for Cisco Unified Personal Communicator, page 9-9

Configure LDAP Server Names and Addresses for Cisco Unified Personal Communicator

Before You Begin

- Configure the LDAP attribute map.
- Obtain the hostnames or IP addresses of the LDAP directories.

Procedure

Step 1 Choose **Cisco Unified Presence Administration > Application > Cisco Jabber > LDAP Server**.

Step 2 Click **Add New**.

Step 3 Enter the LDAP server name.

Step 4 Enter an IP address or an FQDN (Fully Qualified Domain Name) of the LDAP server.

Step 5 Specify the port number used by the LDAP server. The defaults are:

- TCP - **389**
- TLS - **636**

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

Note If you integrate with Microsoft Active Directory and if the server is Global Catalog, configure **3268** as the port number.

Step 6 Choose **TCP** or **TLS** for the protocol type.

Note If you integrate with Microsoft Active Directory and if the server is Global Catalog, choose **TCP** as the protocol type.

Step 7 Click **Save**.

Troubleshooting Tips

- The jpegPhoto attribute is not available in Microsoft Active Directory Global Catalog server, and it is not indexed (http://msdn2.microsoft.com/en-us/library/ms676813.aspx). If your LDAP configuration uses Global Catalog port 3268, Cisco Unified Personal Communicator cannot retrieve the jpegPhoto. Instead, change the LDAP directory configuration to TCP and port 389. Cisco Unified Personal Communicator retrieves the photo when you sign in again.
- If you configure an application dial rule, create proper directory lookup dialing rules in Cisco Unified Communications Manager to make sure that a picture displays both when you place a call to a contact and in the contact details. When you add a contact in Cisco Unified Personal Communicator, the directory lookup returns a 10-digit number (for example, 1234567890). If the user places the call by dialing only four digits (for example, 7890), the picture does not display because 7890 is not a match for 1234567890. Create the following rules to fix this problem:
  - Outbound rule to remove the area code. The picture displays in the contact details.
  - Inbound rule for directory lookup to prefix the area code (translate the 4-digit extension number into the 10-digit DID number stored in AD). The picture displays when you place a call.

Related Topic

Configure the LDAP Attribute Map for Cisco Unified Personal Communicator, page 9-8

What To Do Next

Create LDAP Profiles and Add Cisco Unified Personal Communicator Users to the Profile, page 9-10

Create LDAP Profiles and Add Cisco Unified Personal Communicator Users to the Profile

Cisco Unified Personal Communicator connects to an LDAP server on a per-search basis. If the connection to the primary server fails, Cisco Unified Personal Communicator attempts the first backup LDAP server, and if it is not available, it then attempts to connect to the second backup server. Cisco Unified Personal Communicator also periodically attempts to return to the primary LDAP server. If an LDAP query is in process when the system fails over, the next available server completes this LDAP query.

You can see LDAP server information in the server health window in Cisco Unified Personal Communicator (**Help > Show Server Health** on Windows and **Help > Show System Diagnostics** on Mac OS).If Cisco Unified Personal Communicator cannot connect to any of the LDAP servers, it reports the failure in the System Diagnostics window.

Before You Begin

- Specify the LDAP server names and addresses.
- You must create the LDAP profile before you can add Cisco Unified Personal Communicator licensed users to the profile.

Procedure

Step 1 Choose **Cisco Unified Presence Administration > Application > Cisco Jabber > LDAP Profile**.

Step 2 Click **Add New**.

Step 3 Enter information into the fields.

Table 9-1

Field	Setting
Name	Enter the profile name limited to 128 characters.
Description	(Optional) Enter a description limited to 128 characters.
Bind Distinguished Name	(Optional) Enter the administrator-level account information limited to 128 characters. This is the distinguished name with which you bind for authenticated bind. The syntax for this field depends on the type of LDAP server that you deploy. For details, see the LDAP server documentation.
Anonymous Bind	(Optional) Uncheck this option to use the user credentials to sign in to this LDAP server. For non-anonymous bind operations, Cisco Unified Personal Communicator receives one set of credentials. If configured, these credentials must be valid on the backup LDAP servers. **Note** If you check Anonymous Bind, users can sign in anonymously to the LDAP server with read-only access. Anonymous access might be possible on your directory server, but we do not recommend it. Instead, create a user with read-only privileges on the same directory where the users to be searched are located. Specify the directory number and password in Cisco Unified Presence for Cisco Unified Personal Communicator to use.
Password	(Optional) Enter the LDAP bind password limited to 128 characters. This is the password for the administrator-level account that you provided in the Bind Distinguished Name string to allow users to access this LDAP server.
Confirm Password	Reenter the same password as the password you entered in the Password field. (Optional) After configuring Cisco Unified Presence for authenticated bind with the LDAP server, configure the LDAP server for anonymous permissions and anonymous login so that all directory information (name, number, mail, fax, home number, and so forth) is passed to the Cisco Unified Personal Communicator client.

Table 9-1

Field	Setting
Search Context	(Optional) Enter the location where you configured all the LDAP users. This location is a container or directory. The name is limited to 256 characters. Only use a single OU/LDAP search context. **Note** If you integrate with Microsoft Active Directory: • Set O and OU (OU must contain users; for example, ou=users,dc=cisco,dc=com). For example, cn=users,DC=EFT-LA,DC=cisco,DC=com • The search base should include all users of Cisco Unified Personal Communicator.
Recursive Search	(Optional) Check to perform a recursive search of the directory starting at the search base.
Primary LDAP Server and Backup LDAP Server	Choose the primary LDAP server and optional backup servers.
Make this the Default LDAP Profile for the System	(Optional) Check to add any new users to the system into this default profile. If you turn on this setting, Cisco Unified Presence adds any users that it synchronizes from Cisco Unified Communications Manager to this default profile. Cisco Unified Presence only adds users to this default profile after you choose the default profile (and you turn on the Sync Agent). Cisco Unified Presence does not change any existing profile configuration. Therefore, Cisco recommends that you choose and configure the default profile before you turn on the Sync Agent.
Add Users to Profile	Click the button to open the Find and List Users window. Click **Find** to populate the search results fields. Alternatively, search for a specific users and click **Find**. To add users to this profile, choose the users, and click **Add Selected**.

Step 4 Click **Save**.

Related Topic

Section “How to Update User Configuration After Deploying Cisco Unified Personal Communicator” in the *Cisco Unified Personal Communicator Administration Guide for Cisco Unified Presence Release 8.6*

LDAP Directory Integration for Contact Searches on XMPP Clients

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

The JDS component on Cisco Unified Presence handles the third-party XMPP client communication with the LDAP directory. Third-party XMPP clients send queries to the JDS component on Cisco Unified Presence. 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 Cisco Unified Presence. See chapter Third-party XMPP Client Application Configuration on Cisco Unified Presence, page 10-1.

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 Cisco Unified Presence, 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 Cisco Unified Presence), 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 SSL, configure a secure connection between the LDAP server and Cisco Unified Presence. Upload the root CA certificate to Cisco Unified Presence as an xmpp-trust-certificate, following the certificate upload procedure described in this module. The subject CN in the certificate must match the FQDN of the LDAP server.

Note 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, you just import the CA certificate, not the certificate for the LDAP server.

Before You Begin

Obtain the hostnames or IP addresses of the LDAP directories.

Procedure

Step 1 Choose **Cisco Unified 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 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 Secure Socket Layer (SSL) to communicate with the LDAP server.

Note 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 Cisco Unified Presence 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.

Step 8 Click **Save**.

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

Step 10 If you make an update to the LDAP server configuration for third-party XMPP clients, restart the Cisco UP XCP Directory Service. Choose **Cisco Unified Serviceability > Tools > Control Center - Feature Services** to restart this service.

Related Topics

- LDAP Account Lock Issue, page 9-13
- Secure Connection Between Cisco Unified Communications Manager and the LDAP Directory, page 9-3
- Configure a Secure Connection between Cisco Unified Presence and the LDAP Directory, page 9-6

What To Do Next

Configure the LDAP Search Settings for XMPP Clients, page 9-14

Configure the LDAP Search Settings for XMPP Clients

You must specify the LDAP search settings that will allow Cisco Unified Presence 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:

- Cisco Unified Presence 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 Cisco Unified Presence database.

- Clients can set or modify their own vCard.

Before You Begin

Specify the LDAP server names and addresses for XMPP clients.

Procedure

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

Step 2 Enter information into the fields.

Table 9-2

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).
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.
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.

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 Cisco Unified Presence 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, Cisco Unified Presence populates the default attribute values in the table.

Step 6 Click **Save**.

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

Step 8 Restart the Cisco XCP Directory service.

Related Topic

Configure LDAP Server Names and Addresses for XMPP Clients, page 9-13

What To Do Next

Turn on the Cisco UP XCP Directory Service, page 9-16

Turn on the Cisco UP XCP Directory Service

You must turn on the Cisco UP 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 UP XCP Directory Service on all nodes in the cluster.

Note Do not turn on the Cisco UP XCP Directory Service until you configure the LDAP server, and LDAP search settings for third-party XMPP clients. If you turn on the Cisco UP 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 Serviceability > Tools > Service Activation**.

Step 2 Choose the Cisco Unified Presence server from the Server menu.

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

Step 4 Click **Save**.

Related Topics

- Configure LDAP Server Names and Addresses for XMPP Clients, page 9-13
- Configure the LDAP Search Settings for XMPP Clients, page 9-14