LDAP Directory Integration

LDAP Server Name, Address, and Profile Configuration

LDAP server name, address, and profile configuration on IM and Presence Service has moved to Cisco Unified Communications Manager. For more information, see the *Cisco Unified Communications Manager Administration Guide, Release 9.0(1)*.

LDAP Directory Integration with Cisco Unified Communications Manager Task List

The following workflow diagram shows the high-level steps to integrate the LDAP directory with Cisco Unified Communications Manager.

Figure 1: LDAP Directory Integration with Cisco Unified Communications Manager Workflow

The following table lists the tasks to perform to integrate the LDAP directory with Cisco Unified Communications Manager. For detailed instructions, see the related tasks.

Table 1: Task List for LDAP Directory Integration

Task	Description
Secure Cisco Unified Communications Manager and LDAP Directory Connection	Enable a Secure Socket Layer (SSL) connection for the LDAP server on Cisco Unified Communications Manager. **Tip** You must upload the LDAP SSL certificate as a tomcat-trust certificate on Cisco Unified Communications Manager Release 8.x and later.

Task	Description
Configure LDAP Synchronization for User Provisioning	You can enable the Cisco Directory Synchronization (DirSync) tool on Cisco Unified Communications Manager to automatically provision users from the corporate directory, or you can manually synchronize user directory information. **Tip** LDAP synchronization does not apply to application users on Cisco Unified Communications Manager. Manually provision application users using the Cisco Unified CM Administration GUI.
Upload LDAP Server Certificates	When Cisco Unified Communications Manager LDAP authentication is configured for secure mode (port 636 or 3269), you must upload all LDAP authentication server certificates and Intermediate certificates as "tomcat-trust" to the IM and Presence Service node.
Configure LDAP Server Authentication	Enable Cisco Unified Communications Manager to authenticate user passwords against the corporate LDAP directory. **Tip** LDAP authentication does not apply to the passwords of application users.
Configure Secure Connection Between IM and Presence Service and LDAP Directory	Perform this task on all IM and Presence Service nodes in the cluster if you configured a secure connection between Cisco Unified Communications Manager and the LDAP directory.

Secure Connection Between Cisco Unified Communications Manager and LDAP Directory

You can secure the connection between the Cisco Unified Communications Manager node 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 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

See the Cisco Unified Communications Manager documentation for details on uploading a certificate to Cisco Unified Communications Manager.

Configure 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 CM Administration** > **System** > **LDAP** > **LDAP System.**

Step 2 Click **Add New**.

Step 3 Configure the LDAP server type and attribute.

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

Step 5 Choose **Cisco Unified CM Administration** > **System** > **LDAP** > **LDAP Directory**

Step 6 Configure the following items:

a) LDAP directory account settings
b) User attributes to be synchronized
c) Synchronization schedule
d) 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.

Tip
- If you configure LDAP over SSL, upload the LDAP directory certificate onto Cisco Unified Communications Manager.
- See the LDAP directory content in the Cisco Unified Communications Manager SRND for information about the account synchronization mechanism for specific LDAP products, and general best practices for LDAP synchronization.

What to do next

Proceed to upload the LDAP authentication server certificates.

Related Topics

http://www.cisco.com/go/designzone

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 IM and Presence Service node.

Procedure

Step 1 Choose **Cisco Unified IM and Presence 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.

What to do next

Proceed to configure LDAP authentication.

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 CM 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 check the **Use SSL** check box, enter the IP address or hostname or FQDN that matches the Subject CN of the LDAP server's certificate. The Subject CN of the LDAP server's certificate must be either an IP address or hostname or FQDN. If this condition cannot be met, do not check the **Use SSL** check box because it will result in login failures on Cisco Unified CM IM and Presence Administration, Cisco Unified IM and Presence Serviceability, Cisco Unified IM and Presence Reporting, Cisco Jabber login, Third Party XMPP Clients and any other applications on Cisco Unified Communications Manager and IM and Presence Service that connect to LDAP to perform user authentication.

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

What to do next

Configure secure connection between IM and Presence Service and LDAP directory.

Configure Secure Connection Between IM and Presence Service and 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 IM and Presence Service 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 IM and Presence 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`

What to do next

Proceed to integrate the LDAP directory with Cisco Jabber.

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 2: 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.

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 2: 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.

Task	Description
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.

Before you begin

Obtain the hostnames or IP addresses of the LDAP directories.

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.

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.

Related Topics

Secure Connection Between Cisco Unified Communications Manager and LDAP Directory, on page 2
Configure Secure Connection Between IM and Presence Service and LDAP Directory, on page 5

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 3: 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).
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**.