LDAP Directory Integration with Cisco Unity Connection

The Lightweight Directory Access Protocol (LDAP) provides applications like Cisco Unity Connection with a standard method for accessing user information that is stored in the corporate directory. Companies that centralize all user information in a single repository that is available to multiple applications can reduce maintenance costs by eliminating redundant adds, moves, and changes.

- **User creation**—Unity Connection users can be created by importing data from the LDAP directory.
- **Data synchronization**—Unity Connection can be configured to automatically synchronize user data in the Unity Connection database with data in the LDAP directory.
- **Single sign-on**—Optionally, you can configure Unity Connection to authenticate user names and passwords for Unity Connection web applications against the LDAP directory, so that users do not have to maintain multiple application passwords. (Phone passwords are still maintained in the Unity Connection database.)

Unity Connection uses standard LDAPv3 for accessing data in an LDAP directory. For a list of the LDAP directories that are supported by Unity Connection for synchronization, see the "Requirements for an LDAP Directory Integration" section in the System Requirements for Cisco Unity Connection *Release 12.x*, at http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/requirements/b_12xcucsysreqs.html.

- LDAP Synchronization, on page 1
- LDAP Authentication, on page 7

LDAP Synchronization

LDAP synchronization uses an internal tool called Cisco Directory Synchronization (DirSync) to synchronize a small subset of Cisco Unity Connection user data (first name, last name, alias, phone number, and so on) with the corresponding data in the corporate LDAP directory. To synchronize user data in the Unity Connection database with user data in the corporate LDAP directory, do the following tasks:

1. Configure LDAP synchronization, which defines the relationship between data in Unity Connection and data in the LDAP directory. See the Configuring LDAP Synchronization, on page 2section.
2. Create new Unity Connection users by importing data from the LDAP directory and/or linking data on existing Unity Connection users with data in the LDAP directory. See the Creating Unity Connection Users, on page 5 section.

For additional control over which LDAP users are imported into Unity Connection, you can create one or more LDAP filters before you create Unity Connection users. See the Filtering LDAP Users.

Configuring LDAP Synchronization

When you configure LDAP directory synchronization, you can create up to 20 LDAP directory configurations for each Cisco Unity Connection server or cluster. Each LDAP directory configuration can support only one domain or one organizational unit (OU); if you want to import users from five domains or OUs, you must create five LDAP directory configurations.

A Unity Connection networking site also supports up to 20 LDAP directory configurations for each Unity Connection server or cluster joined to the site. For example, if you have a site with ten servers, you can import users from up to 200 domains.

With Unity Connection 12.5(1) SU1 and later, you can synchronize the data of 160,000 users with LDAP directory.

In each LDAP directory configuration, you specify:

- **The user search base that the configuration accesses:** A user search base is the position in the LDAP directory tree where Unity Connection begins its search for user accounts. Unity Connection imports all users in the tree or subtree (domain or OU) specified by the search base. A Unity Connection server or cluster can only import LDAP data from subtrees with the same directory root, for example, from the same Active Directory forest.

  Note The user search bases that are specified in the LDAP directory configurations on a Unity Connection server must include no more than a total of 120,000 LDAP users. Importing large numbers of LDAP users who do not become Unity Connection users reduces the amount of disk space available for messages, slows database performance, and causes upgrades to take longer.

  If you are using an LDAP directory other than Microsoft Active Directory, and if you create a Unity Connection LDAP directory configuration that specifies the root of the directory as the user search base, Unity Connection imports data for every user in the directory. If the root of the directory contains subtrees that you do not want Unity Connection to access (for example, a subtree for service accounts), you should do one of the following:

  - Create two or more Unity Connection LDAP directory configurations, and specify search bases that omit the users that you do not want Unity Connection to access.
  - Create one or more LDAP search filters. For more information, see the " Filtering LDAP Users " section in the "LDAP" chapter of the System Administration Guide for Cisco Unity Connection Release 12.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

  For directories other than Active Directory, you should specify user search bases that include the smallest possible number of users to speed synchronization, even when that means creating multiple configurations.

  If you are using Active Directory and if a domain has child domains, you must create a separate configuration to access each child domain; Unity Connection does not follow Active Directory referrals during synchronization. The same is true for an Active Directory forest that contains multiple trees-you must create at least one configuration to access each tree. In this configuration, you must map the UserPrincipalName (UPN) attribute to the Unity Connection Alias field; the UPN is guaranteed by Active

Directory to be unique across the forest. For additional considerations on the use of the UPN attribute in a multi-tree AD scenario, see the Additional Considerations for Authentication and Microsoft Active Directory, on page 9 section.

If you are using intrasite or intersite networking to network two or more Unity Connection servers that are each integrated with an LDAP directory, do not specify a user search base on one Unity Connection server that overlaps a user search base on another Unity Connection server, or you have user accounts and mailboxes for the same Unity Connection user on more than one Unity Connection server.

Note You can eliminate the potential for duplicate users by creating LDAP filters on one or more Unity Connection servers. See the " Filtering LDAP Users " section in the "LDAP" chapter of the System Administration Guide for Cisco Unity Connection Release 12.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html .

- **The administrator account in the LDAP directory that Unity Connection uses to access the subtree specified in the user search base.**

  Connection performs a bind to the directory and authenticates using this account. You should use an account dedicated to Unity Connection, with minimum permissions set to "read" all user objects in the search base and with a password set never to expire. (If the password for the administrator account changes, Unity Connection must be reconfigured with the new password.)

  If you create more than one configuration, you should create one administrator account for each configuration and give that account permission to read all user objects only within the corresponding subtree. When creating the configuration, you enter the full distinguished name for the administrator account; therefore the account can reside anywhere in the LDAP directory tree.

- **The frequency with which Unity Connection automatically resynchronizes the Unity Connection database with the LDAP directory, if at all.**

  You can specify the date and time of the next resynchronization, whether the resynchronization occurs just once or on a schedule and, if on a schedule, what you want the frequency to be in hours, days, weeks, or months (with a minimum value of six hours). You should stagger synchronization schedules so that multiple agreements are not querying the same LDAP servers simultaneously. Schedule synchronization to occur during nonbusiness hours.

- **The port on the LDAP server that Unity Connection uses to access LDAP data.**
- **Optionally, whether to use SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server.**
- **One or more LDAP servers.**

  For some LDAP directories, you can specify up to three LDAP directory servers that Unity Connection uses when attempting to synchronize. Unity Connection tries to contact the servers in the order that you specify. If none of the directory servers responds, synchronization fails; Unity Connection tries again at the next scheduled synchronization time. You can use IP addresses rather than host names to eliminate dependencies on Domain Name System (DNS) availability.

Note Not all LDAP directories support specifying additional LDAP directory servers to act as backup in case the LDAP directory server that Unity Connection accesses for synchronization becomes unavailable. For information on whether your LDAP directory supports specifying multiple directory servers, see the " Requirements for an LDAP Directory Configuration " section in the System Requirements for Cisco Unity Connection Release 12.x, at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html .

- **The mapping of LDAP directory attributes to Unity Connection fields, as listed in below Table.**

  Note that the mapping to the Unity Connection Alias field must be the same for all configurations. As you choose an LDAP attribute to map to the Unity Connection Alias field:

  - Confirm that every user that you want to import from the LDAP directory into Unity Connection has a unique value for that attribute.
  - If there are already users in the Unity Connection database, confirm that none of the users that you want to import from the directory has a value in that attribute that matches the value in the Alias field for an existing Unity Connection user.

  Note that for every user that you want to import from the LDAP directory into Unity Connection, the LDAP sn attribute must have a value. Any LDAP user for whom the value of the sn attribute is blank is not imported into the Unity Connection database.

  To protect the integrity of data in the LDAP directory, you cannot use Unity Connection tools to change any of the values that you import. Unity Connection-specific user data (for example, greetings, notification devices, conversation preferences) is managed by Unity Connection and stored only in the local Unity Connection database.

  Note that no passwords or PINs are copied from the LDAP directory to the Unity Connection database. If you want Unity Connection users to authenticate against the LDAP directory, see the LDAP Authentication, on page 7

Table 1: Mapping of LDAP Directory Attributes to Cisco Unity Connection User Fields

LDAP Directory Attribute	Cisco Unity Connection User Field
One of the following: • samAccountName • mail • employeeNumber • telephoneNumber • userPrincipleName	Alias
givenName	First Name
One of the following: • middleName • initials	Initials
SN	Last Name

manager	Manager
department	Department
One of the following: • telephoneNumber • ipPhone	Corporate Phone
One of the following: • mail • samAccountName	Corporate Email Address
title	Title
homePhone	Home (imported but not currently used, and not visible in Unity Connection Administration)
mobile	Mobile (imported but not currently used, and not visible in Unity Connection Administration)
pager	Pager (imported but not currently used, and not visible in Unity Connection Administration)
One of the following: • msRTCSIP-primaryuseraddress • mail • none	Directory URI
display name	Display Name

When clustering (active/active high availability) is configured, all user data, including data imported from the LDAP directory, is automatically replicated from the Unity Connection publisher server to the subscriber server. In this configuration, the Cisco DirSync service runs only on the publisher server.

Note Extension field are not updated with changes to the LDAP phone number. As a result, you can change the LDAP phone number as required, including specifying a completely different number, and the extension is not overwritten the next time that Connection synchronizes data with the LDAP directory.

Creating Unity Connection Users

On a Unity Connection system that is integrated with an LDAP directory, you can create Unity Connection users by importing data from the LDAP directory, converting existing Unity Connection users to synchronize with the LDAP directory, or both. Note the following:

- When you create Unity Connection users by importing LDAP data, Unity Connection takes the values specified in Table 10-1 from the LDAP directory and fills in the remaining information from the Unity Connection user template that you specify.
- When you convert existing users, existing values in the fields in Table 10-1 are replaced with the values in the LDAP directory.

- For any user that you want to import from the LDAP directory, the value in the LDAP attribute that maps to the Unity Connection Alias field cannot match the value in the Unity Connection Alias field for any Unity Connection object (standalone users, users already imported from an LDAP directory, users imported from Cisco Unified Communications Manager via AXL, contacts, distribution lists, and so on).
- After you have synchronized Unity Connection with the LDAP directory, you can continue to add Unity Connection users who are not integrated with the LDAP directory. You can also continue to add Unity Connection users by importing users from Cisco Unified Communications Manager via an AXL Server.
- After you have synchronized Unity Connection with the LDAP directory, new LDAP directory users are not automatically imported into Unity Connection, but must be imported manually.
- After a user has been imported from LDAP, the user page in Cisco Unity Connection Administration identifies the user as an "Active User Imported from LDAP Directory."
- Subsequently when changes are made to user data in the corporate directory, Unity Connection fields that are populated from the LDAP directory are updated with the new LDAP values during the next scheduled resynchronization.

Filtering LDAP Users

You may want additional control over which LDAP users you import into Cisco Unity Connection for a variety of reasons. For example:

- The LDAP directory has a flat structure that you cannot control sufficiently by specifying user search bases.
- You only want a subset of LDAP user accounts to become Unity Connection users.
- The LDAP directory structure does not match the way you want to import users into Unity Connection. For example:
  - If organizational units are set up according to an organizational hierarchy but users are mapped to Unity Connection by geographical location, there might be little overlap between the two.
  - If all users in the directory are in one tree or domain but you want to install more than one Unity Connection server, you need to do something to prevent users from having mailboxes on more than one Unity Connection server.

In these cases, you may want to use create filters to provide additional control over user search bases. Note the following:

- You can create as many LDAP filters as you want, but you can only have one active filter per Unity Connection directory configuration, up to 20 per server or cluster.
- When you create LDAP directory configurations in Unity Connection, you specify both a user search base and an LDAP filter. As applicable, create filters that integrate with the user search bases that you specify for the maximum of twenty LDAP directory configurations that you can create.
- Each filter must adhere to the LDAP filter syntax specified in RFC 4515, "Lightweight Directory Access Protocol (LDAP): String Representation of Search Filters."
- The filter syntax is not validated when you create the filter. Instead, it is validated when you specify the filter in an LDAP directory configuration.

- If you add a filter and add it to an LDAP directory configuration that you have already synchronized with the LDAP directory, or if you change a filter that is already in use in an LDAP directory configuration, you must do the following steps for the LDAP users that are specified by the new or updated filter to be accessible to Connection:

  1. Deactivate and reactivate the Cisco DirSync service. In Cisco Unified Serviceability, select **Tools > Service Activation**. Uncheck the check box next to **Cisco DirSync**, and select **Save** to deactivate the service. Then check the check box next to **Cisco DirSync**, and select **Save** to reactivate the service.
  2. In Unity Connection Administration, in the LDAP directory configuration that accesses the filter, perform a full synchronization (select **Perform Full Sync Now**).

- If you change a filter to one that excludes some of the users who were previously accessible, the Unity Connection users who are synchronized with the now-inaccessible LDAP users are converted to standalone Unity Connection users over the next two scheduled synchronizations or within 24 hours, whichever is greater. The users are still able to sign in to Unity Connection by phone, callers can still leave messages for them, and their messages are not deleted. However, they are not able to sign in to Unity Connection web applications while Unity Connection is breaking synchronization for these users. After the synchronization has been broken, their web-application passwords are the passwords that were assigned when their Unity Connection accounts were created.

Unity Connection Multi-Forest LDAP Synchronization

A Unity Connection deployment using a multi-forest LDAP infrastructure can be supported using Active Directory Lightweight Directory Services (AD LDS) as a single forest view integrating with the multiple disparate forests. The integration also requires the use of LDAP filtering. For more information, refer to the document on "How to Configure Unified Communications Manager Integration Directory Integration in a Multi-Forest Environment" available at http://www.cisco.com/en/US/products/sw/voicesw/ps556/products_configuration_example019186a0080b2b103.shtml.

LDAP Authentication

Some companies want the convenience of single sign-on credentials for their applications. To authenticate sign-ins to Unity Connection web applications against user credentials in an LDAP directory, you must synchronize Unity Connection user data with user data in the LDAP directory as described in the LDAP Synchronization.

Only passwords for Unity Connection web applications (Cisco Unity Connection Administration for administration, Cisco Personal Communications Assistant for end users), and for IMAP email applications that are used to access Unity Connection voice messages, are authenticated against the corporate directory. You manage these passwords using the administration application for the LDAP directory. When authentication is enabled, the password field is no longer displayed in Cisco Unity Connection Administration.

For telephone user interface or voice user interface access to Unity Connection voice messages, numeric passwords (PINs) are still authenticated against the Unity Connection database. You manage these passwords in Unity Connection Administration; users manage PINs using the phone interface or the Messaging Assistant web tool.

The LDAP directories that are supported for LDAP authentication are the same as those supported for synchronization. See the "Requirements for an LDAP Directory Integration" section in the System Requirements

for Cisco Unity Connection *Release 12.x*, at
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/requirements/b_12xcucsysreqs.html.

Configuring LDAP Authentication

Configuring LDAP authentication is much simpler than configuring synchronization. You specify only the following:

- **A user search base.** If you created more than one LDAP configuration, when you configure authentication, you must specify a user search base that contains all of the user search bases that you specified in your LDAP configurations.
- **The administrator account in the LDAP directory that Unity Connection uses to access the search base.** You should use an account dedicated to Unity Connection, with minimum permissions set to "read" all user objects in the search base and with a password set never to expire. (If the password for the administrator account changes, Unity Connection must be reconfigured with the new password.) You enter the full distinguished name for the administrator account; therefore the account can reside anywhere in the LDAP directory tree.
- **One or more LDAP servers.** You can specify up to three LDAP directory servers that Unity Connection uses when attempting to authenticate. Unity Connection tries to contact the servers in the order that you specify. If none of the directory servers responds, authentication fails. You can use IP addresses rather than host names to eliminate dependencies on Domain Name System (DNS) availability.

Working of LDAP Authentication

When LDAP synchronization and authentication are configured in Cisco Unity Connection, authenticating the alias and password of a user against the corporate LDAP directory works as follows:

1. A user connects to the Cisco Personal Communications Assistant (PCA) via HTTPS and attempts to authenticate with an alias (for example, jsmith) and password.
2. Unity Connection issues an LDAP query for the alias jsmith. For the scope for the query, Unity Connection uses the LDAP search base that you specified when you configured LDAP synchronization in Cisco Unity Connection Administration. If you chose the SSL option, the information that is transmitted to the LDAP server is encrypted.
3. The corporate directory server replies with the full Distinguished Name (DN) of user jsmith, for example, "cn=jsmith, ou=Users, dc=vse, dc=lab".
4. Unity Connection attempts an LDAP bind using this full DN and the password provided by the user.
5. If the LDAP bind is successful, Unity Connection allows the user to proceed to the Cisco PCA.

If all of the LDAP servers that are identified in a Unity Connection LDAP directory configuration are unavailable, authentication for Unity Connection web applications fails, and users are not allowed to access the applications. However, authentication for the phone and voice user interfaces continue to work, because these PINs are authenticated against the Unity Connection database.

When the LDAP user account for a Unity Connection user is disabled or deleted, or if an LDAP directory configuration is deleted from the Unity Connection system, the following occurs:

1. Initially, when Unity Connection users try to sign in to a Unity Connection web application, LDAP authentication fails because Unity Connection is still trying to authenticate against the LDAP directory.

If you have multiple LDAP directory configurations accessing multiple LDAP user search bases, and if only one configuration was deleted, only the users in the associated user search base are affected. Users in other user search bases are still able to sign in to Unity Connection web applications.

2. At the first scheduled synchronization, users are marked as "LDAP inactive" in Unity Connection.

   Attempts to sign in to Unity Connection web applications continue to fail.

3. At the next scheduled synchronization that occurs at least 24 hours after users are marked as "LDAP inactive," all Unity Connection users whose accounts were associated with LDAP accounts are converted to Unity Connection standalone users.

   For each Unity Connection user, the password for Unity Connection web applications and for IMAP email access to Unity Connection voice messages becomes the password that was stored in the Unity Connection database when the user account was created. (This is usually the password in the user template that was used to create the user.) Unity Connection users do not know this password, so an administrator must reset it.

   The numeric password (PIN) for the telephone user interface and the voice user interface remains unchanged.

Note the following regarding Unity Connection users whose LDAP user accounts were disabled or deleted, or who were synchronized via an LDAP directory configuration that was deleted from Unity Connection:

- The users can continue to sign in to Unity Connection by phone during the period in which Unity Connection is converting them from an LDAP-synchronized user to a standalone user.
- Their messages are not deleted.
- Callers can continue to leave messages for these Unity Connection users.

Note LDAP phone numbers are converted to Unity Connection extensions only once, when you first synchronize Unity Connection data with LDAP data. On subsequent, scheduled synchronizations, values in the Connection Extension field are not updated with changes to the LDAP phone number. As a result, you can change the LDAP phone number as required, including specifying a completely different number, and the extension is not overwritten the next time that Connection

Additional Considerations for Authentication and Microsoft Active Directory

When you enable LDAP authentication with Active Directory, you should configure Unity Connection to query an Active Directory global catalog server for faster response times. To enable queries against a global catalog server, in Unity Connection Administration, specify the IP address or host name of a global catalog server. For the LDAP port, specify either 3268 if you are not using SSL to encrypt data that is transmitted between the LDAP server and the Unity Connection server, or 3269 if you are using SSL.

Using a global catalog server for authentication is even more efficient if the users that are synchronized from Active Directory belong to multiple domains, because Unity Connection can authenticate users immediately without having to follow referrals. For these cases, configure Unity Connection to access a global catalog server, and set the LDAP user search base to the top of the root domain.

A single LDAP user search base cannot include multiple namespaces, so when an Active Directory forest includes multiple trees, Unity Connection must use a different mechanism to authenticate users. In this configuration, you must map the LDAP userPrincipalName (UPN) attribute to the Unity Connection Alias field. Values in the UPN attribute, which look like email addresses (username@companyname.com), must be unique in the forest.

Note When an Active Directory forest contains multiple trees, the UPN suffix (the part of the email address after the @ symbol) for each user must correspond to the root domain of the tree where the user resides. If the UPN suffix does not match the namespace of the tree, Unity Connection users cannot authenticate against the entire Active Directory forest. However, you can map a different LDAP attribute to the Unity Connection Alias field and limit the LDAP integration to a single tree within the forest.

For example, suppose an Active Directory forest contains two trees, avvid.info and vse.lab. Suppose also that each tree includes a user whose samAccountName is jdoe. Unity Connection authenticates a sign-in attempt for jdoe in the avvid.info tree as follows:

1. The user jdoe connects to the Cisco Personal Communications Assistant (PCA) via HTTPS and enters a UPN (jdoe@avvid.info) and password.
2. Unity Connection performs an LDAP query against an Active Directory global catalog server using the UPN. The LDAP search base is derived from the UPN suffix. In this case, the alias is jdoe and the LDAP search base is "dc=avvid, dc=info."
3. Active Directory finds the Distinguished Name corresponding to the alias in the tree that is specified by the LDAP query, in this case, "cn=jdoe, ou=Users, dc=avvid, dc=info."
4. Active Directory responds via LDAP to Unity Connection with the full Distinguished Name for this user.
5. Unity Connection attempts an LDAP bind using the Distinguished Name and the password initially entered by the user.
6. If the LDAP bind is successful, Unity Connection allows the user to proceed to the Cisco PCA.

Comparison LDAP Integrated Users and Users Created by Importing Data from Cisco Unified CM

An alternative to integrating Unity Connection with an LDAP directory is to create users by importing data from Cisco Unified Communications Manager as described in the "Importing Users through AXL" section of the "Users" chapter of the *System Administration Guide for Cisco Unity Connection, Release 12.x*, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/12x/administration/guide/b_12xcucsag.html.

Note the following:

- If you import users from Cisco Unified CM and if Cisco Unified CM is integrated with the LDAP directory, Unity Connection does not automatically have access to LDAP synchronization or authentication. If you want Unity Connection users to authenticate against the LDAP directory, you must integrate Unity Connection with the LDAP directory, too.
- If you import users from Cisco Unified CM, updates to Cisco Unified CM data do not automatically replicate to the Unity Connection server, so you must remember to use the Synch Users page in Cisco Unity

Connection Administration to manually synchronize Unity Connection user data with Cisco Unified CM user data from time to time. If you integrate Unity Connection with an LDAP directory, you can define a synchronization schedule that specifies when data in the Unity Connection database is automatically resynchronized with data in the LDAP directory.

Note that when you add users to the LDAP directory, you still need to manually import them into Unity Connection; automatic synchronization only updates the Unity Connection database with new data for existing users, not new data for new users.

- When you integrate Unity Connection with an LDAP directory, you can configure Unity Connection to authenticate passwords for web applications against the LDAP database. When you import data from Cisco Unified CM, you must maintain passwords for Unity Connection web applications in Unity Connection and maintain passwords for Cisco Unified CM web applications in Cisco Unified CM.