CHAPTER 9

LDAP Directory Integration with Cisco Unity Connection 8.x

Revised November 16, 2010

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.

Integrating Connection with an LDAP directory provides several benefits:

- **User creation**—Connection users can be created by importing data from the LDAP directory.
- **Data synchronization**—Connection can be configured to automatically synchronize user data in the Connection database with data in the LDAP directory.
- **Single sign-on**—Optionally, you can configure Connection to authenticate user names and passwords for 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 Connection database.)

Connection uses standard LDAPv3 for accessing data in an LDAP directory. For a list of the LDAP directories that are supported by Connection for synchronization, see the "Requirements for an LDAP Directory Integration" section in the *System Requirements for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/requirements/8xcucsysreqs.html.

This chapter covers the main design issues of integrating Cisco Unity Connection 8.x with a corporate LDAP directory. See the following sections:

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 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 Connection and data in the LDAP directory. See the "Configuring LDAP Synchronization" section on page 9-82.
2. Create new Connection users by importing data from the LDAP directory and/or linking data on existing Connection users with data in the LDAP directory. See the "Creating Cisco Unity Connection Users" section on page 9-85.

   For additional control over which LDAP users are imported into Connection, you can create one or more LDAP filters before you create Connection users. See the "Filtering LDAP Users" section on page 9-86.

Configuring LDAP Synchronization

When you configure LDAP directory synchronization, you can create up to five 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 Connection networking site also supports up to five LDAP directory configurations for each 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 50 domains. Or if you have a Cisco Voicemail Organization of two sites with ten servers each, you can import users from up to 100 domains.

In each LDAP directory configuration, you specify:

- **The user search base that the configuration will access.** A user search base is the position in the LDAP directory tree where Connection begins its search for user accounts. Connection imports all users in the tree or subtree (domain or OU) specified by the search base. A 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 In Cisco Unity Connection 8.5(1) and earlier, the user search bases that are specified in the LDAP directory configurations on a Connection server must include no more than a total of 60,000 LDAP users. In Cisco Unity Connection 8.6(1) and later, the user search bases that are specified in the LDAP directory configurations on a Connection server must include no more than a total of 80,000 LDAP users. Importing large numbers of LDAP users who will not become 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 Connection LDAP directory configuration that specifies the root of the directory as the user search base, Connection will import data for every user in the directory. If the root of the directory contains subtrees that you do not want Connection to access (for example, a subtree for service accounts), you should do one of the following:

- Create two or more Connection LDAP directory configurations, and specify search bases that omit the users that you do not want Connection to access.

  - Create one or more LDAP search filters. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 8.x" section in the "Integrating Cisco Unity Connection 8.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.

For directories other than Active Directory, we recommend that you 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; 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 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" section on page 9-89.

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

Note You can eliminate the potential for duplicate users by creating LDAP filters on one or more Connection servers. See the "Filtering LDAP Users in Cisco Unity Connection 8.x" section in the "Integrating Cisco Unity Connection 8.x with an LDAP Directory" chapter of the *System Administration Guide for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/administration/guide/8xcucsagx.html.

- **The administrator account in the LDAP directory that Connection will use to access the subtree specified in the user search base.** Connection performs a bind to the directory and authenticates by using this account. We recommend that you use an account dedicated to 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, Connection must be reconfigured with the new password.)

  If you create more than one configuration, we recommend that you 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 Connection automatically resynchronizes the 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). We recommend that you 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 Connection uses to access LDAP data.**
- **Optionally, whether to use SSL to encrypt data that is transmitted between the LDAP server and the Connection server.**

- **One or more LDAP servers.** For some LDAP directories, you can specify up to three LDAP directory servers that Connection uses when attempting to synchronize. Connection tries to contact the servers in the order that you specify. If none of the directory servers responds, synchronization fails; 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 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 Integration" section in the *System Requirements for Cisco Unity Connection Release 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/requirements/8xcucsysreqs.html.

- **The mapping of LDAP directory attributes to Connection fields, as listed in Table 9-1.** Note that the mapping to the Connection Alias field must be the same for all configurations. As you choose an LDAP attribute to map to the Connection Alias field:
  - Confirm that every user that you want to import from the LDAP directory into Connection has a unique value for that attribute.
  - If there are already users in the 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 Connection user.

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

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

  Note that no passwords or PINs are copied from the LDAP directory to the Connection database. If you want Connection users to authenticate against the LDAP directory, see the "LDAP Authentication" section on page 9-87.

Table 9-1 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

Table 9-1 Mapping of LDAP Directory Attributes to Cisco Unity Connection User Fields

LDAP Directory Attribute	Cisco Unity Connection User Field
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 Connection Administration)
mobile	Mobile (imported but not currently used, and not visible in Connection Administration)
pager	Pager (imported but not currently used, and not visible in Connection Administration)

When clustering (active/active high availability) is configured, all user data, including data imported from the LDAP directory, is automatically replicated from the 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 will not be overwritten the next time that Connection synchronizes data with the LDAP directory.

Creating Cisco Unity Connection Users

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

- When you create Connection users by importing LDAP data, Connection takes the values specified in Table 9-1 from the LDAP directory and fills in the remaining information from the Connection user template that you specify.
- When you convert existing users, existing values in the fields in Table 9-1 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 Connection Alias field cannot match the value in the Connection Alias field for any 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 Connection with the LDAP directory, you can continue to add Connection users who are not integrated with the LDAP directory. You can also continue to add Connection users by importing users from Cisco Unified Communications Manager via an AXL Server.
- After you have synchronized Connection with the LDAP directory, new LDAP directory users are not automatically imported into 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, 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 Connection users.
- The LDAP directory structure does not match the way you want to import users into Connection. For example:
  - If organizational units are set up according to an organizational hierarchy but users are mapped to 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 Connection server, you need to do something to prevent users from having mailboxes on more than one Connection server.

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

- You cannot create LDAP filters for Cisco Unified CMBE.
- You can create as many LDAP filters as you want, but you can only have one active filter per Connection directory configuration, up to five per server or cluster.
- When you create LDAP directory configurations in 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 will specify for the maximum of five 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 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 Connection users who are synchronized with the now-inaccessible LDAP users will be converted to standalone Connection users over the next two scheduled synchronizations or within 24 hours, whichever is greater. The users will still be able to sign in to Connection by phone, callers can still leave messages for them, and their messages will not be deleted. However, they will not be able to sign in to Connection web applications while Connection is breaking synchronization for these users. After the synchronization has been broken, their web-application passwords will be the passwords that were assigned when their Connection accounts were created.

Cisco Unity Connection Multi-Forest LDAP Synchronization

Added June 9, 2011

A Connection deployment using a multi-forest LDAP infrastructure can be supported by 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_example09186a0080b2b103.shtml.

LDAP Authentication

Some companies want the convenience of single sign-on credentials for their applications. To authenticate sign-ins to Connection web applications against user credentials in an LDAP directory, you must synchronize Connection user data with user data in the LDAP directory as described in the "LDAP Synchronization" section on page 9-82.

Only passwords for 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 Connection voice messages, are authenticated against the corporate directory. You manage these passwords by 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 Connection voice messages, numeric passwords (PINs) are still authenticated against the Connection database. You manage these passwords in Connection Administration; users manage PINs by 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 8.x*, at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/requirements/8xcucsysreqs.html.

See the following sections for additional details:

- Configuring LDAP Authentication, page 9-88
- How LDAP Authentication Works, page 9-88
- .Additional Considerations for Authentication and Microsoft Active Directory, page 9-89

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 Cisco Unity Connection will use to access the search base.** We recommend that you use an account dedicated to 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, 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 Connection uses when attempting to authenticate. 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.

How LDAP Authentication Works

Revised September 24, 2013

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. Connection issues an LDAP query for the alias jsmith. For the scope for the query, 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. Connection attempts an LDAP bind by using this full DN and the password provided by the user.
5. If the LDAP bind is successful, Connection allows the user to proceed to the Cisco PCA.

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

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

1. Initially, when Connection users try to sign in to a Connection web application, LDAP authentication fails because 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 Connection web applications.

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

   Attempts to sign in to 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 Connection users whose accounts were associated with LDAP accounts are converted to Connection standalone users.

   For each Connection user, the password for Connection web applications and for IMAP email access to Connection voice messages becomes the password that was stored in the Connection database when the user account was created. (This is usually the password in the user template that was used to create the user.) 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 Connection users whose LDAP user accounts were disabled or deleted, or who were synchronized via an LDAP directory configuration that was deleted from Connection:

- The users can continue to sign in to Connection by phone during the period in which 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 Connection users.

Note LDAP phone numbers are converted to Connection extensions only once, when you first synchronize 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 will not be overwritten the next time that Connection

.Additional Considerations for Authentication and Microsoft Active Directory

When you enable LDAP authentication with Active Directory, we recommend that you configure Cisco Unity Connection to query an Active Directory global catalog server for faster response times. To enable queries against a global catalog server, in 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 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 Connection can authenticate users immediately without having to follow referrals. For these cases, configure 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, Connection must use a different mechanism to authenticate users. In this configuration, you must map the LDAP userPrincipalName (UPN) attribute to the 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, Connection users cannot authenticate against the entire Active Directory forest. However, you can map a different LDAP attribute to the 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. 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. Connection performs an LDAP query against an Active Directory global catalog server by 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 Connection with the full Distinguished Name for this user.
5. Connection attempts an LDAP bind by using the Distinguished Name and the password initially entered by the user.
6. If the LDAP bind is successful, Connection allows the user to proceed to the Cisco PCA.

Comparison of Integrating Connection 8.x with an LDAP Directory and Creating Users by Importing Data from Cisco Unified CM

Added November 16, 2010

An alternative to integrating Connection with an LDAP directory is to create users by importing data from Cisco Unified Communications Manager as described in the “Creating Multiple Cisco Unity Connection 8.x User Accounts from Cisco Unified Communications Manager Users” chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection Release 8.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/8x/user_mac/guide/8xcucmacx.html.

Note the following:

- If you import users from Cisco Unified CM and if Cisco Unified CM is integrated with the LDAP directory, Connection does not automatically have access to LDAP synchronization or authentication. If you want Connection users to authenticate against the LDAP directory, you must integrate 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 Connection server, so you must remember to use the Synch Users page in Cisco Unity Connection Administration to manually synchronize Connection user data with Cisco Unified CM user data from time to time. If you integrate Connection with an LDAP directory, you can define a synchronization schedule that specifies when data in the 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 Connection; automatic synchronization only updates the Connection database with new data for existing users, not new data for new users.
- When you integrate Connection with an LDAP directory, you can configure Connection to authenticate passwords for web applications against the LDAP database. When you import data from Cisco Unified CM, you must maintain passwords for Connection web applications in Connection and maintain passwords for Cisco Unified CM web applications in Cisco Unified CM.