LDAP

Overview

When you are using an LDAP compliant directory as your corporate directory and do not want to separately maintain basic user information in Cisco Unity Connection, you can use the LDAP integration feature.

The LDAP integration in Unity Connection involves:

- Creating Unity Connection users by importing user data from an LDAP directory.
- Configuring Unity Connection to periodically synchronize the users with the user data in an LDAP directory.
- Authenticating Unity Connection users against the user data in an LDAP directory. An LDAP authenticated user uses the LDAP password as the web application password to log in to Unity Connection web applications.

For a list of the LDAP directories that are supported for use with Unity Connection, see the "Requirements for an LDAP Directory Integration" section in System Requirements for Cisco Unity Connection *Release 15* available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html.

Integrating Unity Connection with an LDAP Directory

If a Unity Connection server is integrated with a Cisco Unified CM phone system and you want to integrate both the servers with an LDAP directory, you must separately integrate each server with the LDAP directory. Integrating only one of the servers with an LDAP directory is not sufficient to allow the other server to synchronize or authenticate to the LDAP directory.

See the related links:

- For information on integrating Cisco Unified CM with an LDAP directory, see the "LDAP System Setup" chapter of the Cisco Unified Communications Manager Administration Guide for the required release, available at http://www.cisco.com/c/en/us/support/unified-communications/unified-communications-manager-callmanager/products-maintenance-guides-list.html.
- For information on integrating Unity Connection with an LDAP directory, see the Task List for Configuring LDAP section.

Task List for Configuring LDAP

This section contains a list of tasks that you must follow to ensure successful LDAP integration in a Unity Connection server:

Note In case of a cluster, you perform all the LDAP configuration tasks only on the publisher server.

1. Activate the Cisco DirSync service in Unity Connection to access an LDAP directory. See the Activating Cisco DirSync Service section.
2. Enable LDAP synchronization. See the Enabling LDAP Synchronization section.
3. Add one or more LDAP directory configurations that define the LDAP directory and user search bases in which Unity Connection accesses data, and import data from the LDAP directory in to a Unity Connection server. See the Configuring LDAP Directory Configurations section.
4. *(Optional)* If the phone numbers stored in the LDAP directory are not in the same format as the extensions that you want to use in Unity Connection, specify a regular expression that converts phone numbers into extensions when you import LDAP data into Unity Connection. See the Converting Phone Numbers into Extensions section.
5. *(Optional)* If you want to use SSL to encrypt the usernames and passwords that are sent to the LDAP server for authentication, export an SSL certificate from the applicable LDAP servers, and upload the certificates on the Unity Connection server. See the Uploading SSL Certificates on the Cisco Unity Connection 9.x Server section.
6. *(Optional)* Configure LDAP authentication if you want to authenticate the username and web application password of a Unity Connection user. See the Configuring LDAP Authentication in Unity Connection section.
7. You can add new Unity Connection users linked to the user data in LDAP directory or integrate existing Unity Connection users with the LDAP user data. Do the following steps:

   Select the user search bases that you specify when you create LDAP directory configurations. See the Selecting the LDAP Users to Import into Unity Connection section.

   If you need to determine whether a Unity Connection user is integrated with an LDAP directory, see the Determining if a Unity Connection User is Integrated with an LDAP Directory section.

   (Optional) You need to specify one or more LDAP filters if the user search bases are not sufficient enough to control the LDAP users that are synchronized with Unity Connection users. See the Filtering LDAP Users section.

   You can use either of the following tools to import user data from an LDAP directory:

   The Bulk Administration Tool is used to add new Unity Connection users by importing the LDAP user data information into a comma separated value (CSV) file. Importing from a CSV file can be useful for transferring information from an LDAP directory to Unity Connection. For more information, see the Changing LDAP Integration Status and the Integrating Existing Unity Connection User Accounts with LDAP User Accounts Using Bulk Administration Tool sections.

   The Import Users tool is used to add new Unity Connection users by importing the user data from an LDAP directory. For more information, see the Creating Unity Connection Users from LDAP Data Using the Import Users Tool section.

Activating Cisco DirSync Service

Step 1 In Cisco Unified Serviceability, expand Tools and select **Service Activation**.

Step 2 On the Service Activation page, select the Unity Connection server in the Server drop-down field.

Step 3 In the Directory Services list, check the **Cisco DirSync Service** check box.

Step 4 Select **Save** and **OK** to confirm the activation of this service.

Enabling LDAP Synchronization

Enable LDAP synchronization to specify the LDAP directory with which Unity Connection integrates to get basic information from the LDAP directory.

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **LDAP** and select **LDAP Setup**.

Step 2 To configure LDAP synchronization, do the following steps on the LDAP Setup page (For information on each field, see Help> This Page):

a) Check the **Enable Synchronizing from LDAP Server** check box.

b) Select the LDAP server type in the LDAP Server Type list.

c) In the LDAP Attribute for User ID list, select the attribute in the LDAP directory from which you want the data to appear in the Alias field in Unity Connection.

Caution If you select an attribute other than sAMAccountName, when users sign in to Cisco PCA, an IMAP client, or Web Inbox, they must enter the Unity Connection alias and LDAP password.

Caution If you later need to change the attribute in LDAP Attribute for User ID list after creating LDAP directory configurations on the LDAP Directory page, you must delete all LDAP directory configurations, change the value, and re-create all the LDAP directory configurations. For more information, see the Changing the LDAP Field Mapped to the Alias Field section.

Step 3 Select **Save**.

Note *(Applicable to Cisco Unity Connection 12.5SU7 and later releases)* If you choose **LDAP Attribute for User ID**, mail as Alias field then the relay address will be selected as %Email%@ldap.com in **User Templates** > **Message Actions** by default. If Alias field contains @ldap.com then it will be truncated so that the valid email address is saved in database while creating users.

Configuring LDAP Directory Configurations

If you want to import the user data from LDAP directory into Unity Connection, do the following steps for each user search base in the LDAP directory.

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **LDAP** > **and** select **LDAP Directory Configuration**.

Step 2 On the Find and List LDAP Directory Configurations page, select Add New to add a new LDAP directory configuration.

Step 3 To configure the LDAP Directory Configuration, do the following steps on the LDAP Directory Configuration page (For more information on each field, see Help> This Page):

a) Enter the values in all the required fields.

b) If you specify an LDAP filter, LDAP filter syntax is checked. If the syntax is invalid, an error message appears.

c) If you uploaded SSL certificates to the Unity Connection server in the Uploading SSL Certificates on the Cisco Unity Connection 9.x Server section, check the **Use SSL** check box for every LDAP server that you specify in the **Host Name or IP Address for Server** field.

Step 4 Select **Save** and select **Perform Full Sync Now**.

Step 5 To add another LDAP directory configuration for another user search base, select **Add New**, and repeat Step 2 through Step 4

Note When importing users from LDAP, the user gets successfully imported into the end user table. However, when the user is imported into the tbl_user from end user table, the synchronization fails if the middlename has value more than 12 bytes.

Converting Phone Numbers into Extensions

If the phone numbers in LDAP directory do not match the Extension field in Unity Connection, you need to add a regular expression and a replacement pattern that converts the phone numbers into extensions. If you use the Bulk Administration Tool to add users by exporting the user data to a CSV file, edit the CSV file, and import the edited file. During this process, you can open the CSV file in a spreadsheet application and possibly create a formula that is more effective than the regular expression.

Consider the following points when converting phone numbers in LDAP directory into extensions in Unity Connection:

- Phone numbers are converted to extensions only at the time when you first synchronize Unity Connection data with LDAP data. Later on, during the scheduled LDAP synchronizations, the extension is not overwritten by any changes in the phone number.
- Unity Connection automatically removes non-numeric characters from a phone number, therefore it is not required to add a regular expression for non-numeric characters.
- You can often specify more than one combination of regular expression and replacement pattern that produces the same result. Unity Connection uses the regular expression package of the Java library. Table 1: Examples for Converting LDAP Phone Numbers to Unity Connection Extensions lists some examples of the conversions that are possible with the expanded functionality.

Table 1: Examples for Converting LDAP Phone Numbers to Unity Connection Extensions

Example Conversion Operation	Regular Expression for LDAP Phone Number Pattern	Replaceme
Use LDAP phone number as Unity Connection extension	(.*)	$1
Use the last four digits of LDAP phone number as Unity Connection extension	.*(\d{4})	$1

Example Conversion Operation	Regular Expression for LDAP Phone Number Pattern	Replacement
Use the first four digits of LDAP phone number as Unity Connection extension.	(\d{4}).*	$1
Append 8 to the end of LDAP phone number	^(.*)	$18
Append 9 to the left of the last four digits of LDAP phone number	.*(\d{4})	9$1
Append 88 to the end of LDAP phone number	(.*)	$18
Use the digits 555 between the first three digits and the last four digits of LDAP phone number	(\d{3}).*(\d{4})	$1555$2
Use the last four digits of LDAP phone number as Unity Connection extension if LDAP phone number is between seven and ten digits long	\d{3,6}(\d{4})	$1
Use the last four digits of LDAP phone number as Unity Connection extension if LDAP phone number starts with 206	206.*(\d{4})	$1
Prepend +9 to the left of the LDAP phone number	(.+)	+9$1
Prepend 85 to the left of the rightmost 5 digits of LDAP phone number if LDAP phone number is 10-digit long	\d{5}(\d{5})	85$1
Remove the leftmost three digits of LDAP phone number if LDAP phone number is 13 digits long and the first three digits are 011	011(\d{10})	$1
Remove the leftmost six digits of LDAP phone number and then prepend 52 to the remaining digits if LDAP phone number is 10 digits long and the first three digits are 206	206\d{3}(\d{4})	52$1

Adding a Regular Expression and Replacement Pattern

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **LDAP** and select **Phone Number Conversion**.

Step 2 On the Phone Number Conversion page, enter the values in the required fields. (For information on each field, see Help> This Page).

Step 3 Select **Save**.

Uploading SSL Certificates on the Cisco Unity Connection 9.x Server

If you want to use SSL to encrypt data transmitted between the LDAP server and the Unity Connection server, check the Use SSL check box for each LDAP server that you configure for synchronization. To upload SSL certificates, do the following procedure.

Step 1 Export the SSL certificates from the following LDAP servers:

- Each LDAP server with which Unity Connection should synchronize data.
- Each LDAP server that Unity Connection user should access to authenticate user sign-ins.
- Each redundant LDAP server which you want Unity Connection to synchronize or authenticate.

Step 2 In Cisco Unified Operating System Administration, expand Security and select **Certificate Management** > **.**

Step 3 To upload the SSL certificate you exported in Step 1, do the following steps:

- Select the Upload Certificate/ Certificate chain option.
- Select tomcat-trust from the Certificate Purpose drop-down list.
- Select Browse in the Upload File field to upload the SSL certificate.
- Restart the Cisco DirSync and Cisco Tomcat services to avoid failures in LDAP synchronization and authentication.

Step 4 To restart Cisco DirSync service, do the following steps:

- In Cisco Unified Serviceability, expand Tools and select Service Activation.
- On the Service Activation page, uncheck the Cisco DirSync service field and select Save.
- Check the Cisco DirSync service field and select Save.

To restart the Cisco Tomcat service, run the CLI command utils service restart Cisco Tomcat.

Configuring LDAP Authentication in Unity Connection

The LDAP directories supported for LDAP synchronization are also supported for LDAP authentication. LDAP authentication authenticates Unity Connection user data against the user data in the LDAP directory, so that:

- Passwords that allow Unity Connection users gain single sign-on access on Unity Connection web applications, such as Cisco Unity Connection Administration and Cisco PCA.
- Passwords that are required to sign in to IMAP email applications to access Unity Connection voicemails.

If LDAP authentication is enabled, the web application password field does not appear in Cisco Unity Connection Administration and can only be managed from the LDAP directory.

The voicemail passwords used to access Unity Connection voicemails from telephone user interface (TUI) are authenticated against the Unity Connection database. The passwords or PINs can be managed using phone interface or Messaging Assistant web tool.

Note The administrator account that is used to sign in to Cisco Unified Operating System Administration, Disaster Recovery System, and the command line interface cannot be configured for LDAP integration.

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **LDAP** and select **LDAP Authentication**.

Step 2 On the LDAP Authentication page, do the following steps (For information on each field, see Help> This Page):

a) Check the Use LDAP Authentication for End Users check box.

b) Enter the values in all other fields.

c) If you change the value of the Host Name or IP Address for Server field and if the IMAP clients are accessing Unity Connection, you need to restart the Unity Connection IMAP Server service. If other web applications are accessing Unity Connection, restart the server.

d) If you uploaded SSL certificates to the Unity Connection server in the Uploading SSL Certificates on the Cisco Unity Connection 9.x Server section, check the **Use SSL** check box.

Step 3 Select **Save**.

Selecting the LDAP Users to Import into Unity Connection

Consider the following points when importing LDAP user accounts into Unity Connection:

- Before importing users into Unity Connection, check the LDAP directory that integrates with Unity Connection.
- You can create up to 20 LDAP directory configurations to specify the users in the LDAP directory you want to import into Unity Connection. For each LDAP directory configuration, specify a user search base in which Unity Connection should search for user accounts.
- Unity Connection imports all users that belong to the specified user search base, such as domain or Organization Unit in an LDAP directory tree. 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.
- After creating the LDAP directory configurations, synchronize Unity Connection data with data in the LDAP directory to import the LDAP data in to the Unity Connection server. The practical limit of users that can be imported into the Cisco Unified CM database is 120,000. The limit is not enforced by the synchronization process but importing a large numbers of LDAP users who do not become Unity Connection users. This reduces the amount of disk space available for messages and slows down the database performance causing the upgrades to take longer.

Caution Do not specify user search bases that causes more than 120,000 users to be imported into the Cisco Unified CM database during synchronization to avoid impact on Unity Connection performance.

You can synchronize the data of 160,000 users with LDAP directory.

- Analyze the structure of your LDAP directory and determine whether you can specify five or less than five user search bases that:
  - Include the LDAP users that you want to import into Unity Connection.
  - Exclude the LDAP users that you do not want to import into Unity Connection.
  - Causes less than 60,000 users to be imported into the Cisco Unified CM database.

Directories Other than Active Directory

If you are using an LDAP directory other than Microsoft Active Directory, you should specify one or more user search bases that include the smallest possible number of users to enhance the speed of synchronization, even when that means creating multiple configurations.

If the root directory contains subtrees that you do not want Unity Connection to access (for example, a subtree for service accounts), do either of the following tasks:

- Create two or more LDAP directory configurations and specify the search bases that you do not want Unity Connection to access.
- Create an LDAP search filter. For more information, see the "Filtering LDAP Users" section of the "LDAP Directory Integration with Cisco Unity Connection" chapter of the Design Guide for Cisco Unity Connection Release 15, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/guide/b_15cucdg.html.

Active Directory

You must create a separate LDAP directory configuration when using Active Directory or when the LDAP directory domain has several child domains. Unity Connection do not follow Active Directory referrals during synchronization. In this type of LDAP configuration, you must map the UserPrincipalName (UPN) attribute to the Unity Connection Alias field because UPN is unique across the forest in Active Directory.

Unity Connection Intrasite and Intersite Networking

Intrasite or intersite networking allows to network two or more Unity Connection servers that may be each integrated with an LDAP directory. When you are using intrasite or intersite networking, you may specify a user search base on one Unity Connection server that overlaps a user search base on another Unity Connection server. Be careful not to accidentally create duplicate Unity Connection users on different Unity Connection servers by importing the same LDAP user more than once.

Note Regardless of how you create users, Unity Connection prevents you from creating two users with the same alias on the same Unity Connection server but does not prevent you from creating two users with the same alias on different Unity Connection servers in the same site or organization.

In some cases, you may find it useful to create multiple Unity Connection users from the same LDAP user. For example, if you import the some of the LDAP administrator accounts into every Unity Connection server as Unity Connection users without voice mailboxes and use them as administrator accounts. This allows you to use LDAP synchronization and authentication for Unity Connection administrator accounts without creating one or more LDAP users for every Unity Connection server.

Filtering LDAP Users

For more information, see the "Filtering LDAP Users" section of the "LDAP Directory Integration with Cisco Unity Connection" chapter of the Design Guide for Cisco Unity Connection Release 15, available at https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/design/guide/b_15cucdg.html.

Adding an LDAP Filter

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **LDAP**, then select **LDAP Custom Filter**.

Step 2 The Find and List LDAP Filters page appears displaying the currently configured LDAP filters.

Step 3 Select **Add New.**

Step 4 In the Filter Name field, enter a name for this LDAP filter. If you are adding more than one LDAP filter configuration, enter a name that identifies the LDAP users included in the current filter, for example, "Engineering."

Step 5 In the Filter field, enter a filter that adheres to the LDAP filter syntax specified in RFC 2254, "The String Representation of LDAP Search Filters." You must enclose the filter text in parentheses.

Step 6 Select **Save**.

Creating Unity Connection Users from LDAP Data Using the Import Users Tool

The LDAP Integration process imports the LDAP data into a hidden Cisco Unified CM database on the Unity Connection server. You can create new Unity Connection users by importing the user data from an LDAP directory using the Bulk Administration Tool or Import Users tool. You can also use BAT tool to update the existing Unity Connection users with the users in an LDAP directory.

Step 1 In Cisco Unity Connection Administration, expand Users and select Import Users.

Step 2 On the Import Users page, import the LDAP user accounts to create Unity Connection users (For more information on each field, see Help> This Page):

a) Select LDAP Directory in Find End Users In field.
b) Select the template on which the new user is based.
c) Specify the Alias, First Name, or Last Name of the LDAP user accounts that you want to import.
d) Check the check boxes against the LDAP user accounts that you want to import and select Import Selected.

Creating Unity Connection Users from LDAP Data Using Bulk Administration Tool

Step 1 In Cisco Unity Connection Administration, expand Tools and select Bulk Administration Tool.

Step 2 To add Unity Connection users, do the following steps on the Bulk Administration Tool page (For more information on each field, see Help> This Page):

a) From Select Operation, select Export.
b) From Select Object Type, select Users from LDAP Directory.
c) Enter the values in all the required fields.
d) Select Submit.

This creates a CSV file with the LDAP user data. Open the CSV file in a spreadsheet application or in a text editor and edit the data as applicable. Now, import the data from the CSV file:

e) From Select Operation, select Create.
f) From Select Object Type, select Users with Mailbox.
g) Enter the values in all the required fields.
h) Select Submit.

Step 3 When the import is complete, review the file that you specified in the Failed Objects Filename field to verify that all users are created successfully.

Editing LDAP Directory Configuration

Changing or Deleting LDAP Directory Configuration

To make any changes to the existing LDAP directory configuration, you must delete the existing LDAP integration and re-create it to change the LDAP user fields that are imported into Unity Connection.

Caution You must re-create the directory configuration within 24 hours else the LDAP integrated Unity Connection users are converted to standalone Unity Connection users.

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **, select** > **LDAP**, and then select **LDAP Directory Configuration**.

Note If you do not have a record of the existing settings, you must write it down before deleting the LDAP directory configuration.

Step 2 On the Find and List LDAP Directory Configurations page, check the check box next to the LDAP directory configuration that you want to change or delete.

Step 3 Select **Delete Selected** and select OK to confirm deletion.

Step 4 Expand **System Settings** > **, select** > **LDAP**, and then select **LDAP Setup**.

Step 5 On the LDAP Setup page, uncheck the **Enable Synchronizing from LDAP Server** check box and select **Save**.

Step 6 Recheck the **Enable Synchronizing from LDAP Server** check box and select **Save** again.

This confirms the deletion of LDAP directory configuration. However, if you want to change the existing LDAP directory configuration, then follow the next step to re-create a new LDAP directory configuration after deleting the existing LDAP configuration.

Step 7 Re-create the directory configuration, and perform a full synchronization for the re-created directory configuration. See the Configuring LDAP Directory Configurations section.

Note If you need to create an IMAP account for a user after changing the LDAP directory synchronization, make sure to restart Unity Connection before creating the accounts.

Disabling LDAP Authentication

If you permanently disable LDAP authentication, users sign in to Unity Connection web applications using the Unity Connection web application password instead of the LDAP directory password. As LDAP integrated users do not have separate web application passwords, they manage the Unity Connection web applications using LDAP directory passwords. All the users with mailbox must change the web application password the next time they sign in to a Unity Connection web application.

However, if you temporarily disable LDAP authentication, for example, when you are changing the LDAP field mapped to the user Alias field in Unity Connection, you do not have to change password settings for Unity Connection users.

You can use Bulk Edit to change the passwords for all the users who have mailboxes but you must individually change passwords for users who not have mailboxes (meaning administrators).

Step 1 In Cisco Unity Connection Administration, expand **System Settings** > **LDAP** and select **LDAP Authentication**.

Step 2 On the LDAP Authentication page, uncheck the **Use LDAP Authentication for End Users** check box and select **Save**.

If you are temporarily disabling LDAP authentication, skip the rest of this procedure. Do not change password settings of users with mailbox.

Step 3 To change the password settings for all LDAP integrated users, do the following steps:

a) In Cisco Unity Connection Administration, expand **Users** and select **Users**.
b) On the Search Users page, select the LDAP users and select **Bulk Edit**.
c) From the **Edit** menu, select **Password Settings**.
d) For **Web Application** password, check the **User Must Change at Next Sign-In check box.**
e) If you want to schedule when Unity Connection changes the setting for the selected users, from the Bulk Edit Task Scheduling menu, select **Run Later** and specify a date and time.
f) Select **Submit**.

Changing the LDAP Field Mapped to the Alias Field

To change the field in LDAP directory that is mapped to the Alias field in Unity Connection, do the following steps.

Caution If you are using LDAP authentication, after you complete this procedure, users have to sign in to Unity Connection web interfaces using the new value of the Alias field in Unity Connection.

Step 1 Deactivate the Cisco DirSync service:

a) In Cisco Unified Serviceability, expand the Tools menu and select **Service Activation**.
b) On the Service Activation page, in the Directory Services list, uncheck the **Cisco DirSync Service** check box and select **Save**.

Step 2 Disable LDAP authentication. See the Disabling LDAP Authentication section.

Step 3 Delete all the LDAP directory configurations. See the Changing or Deleting LDAP Directory Configuration section.

Step 4 Change the field that is mapped to the Unity Connection Alias field:

a) In Cisco Unity Connection Administration, expand **System Settings > LDAP** and select **LDAP Setup**.

b) On the LDAP Setup page, change the values in the required fields and select Save. (For more information on each field, see Help> This Page).

If you select a field other than sAMAccountName, when the users sign in to the Cisco PCA or an IMAP client or sign in to the Web Inbox, they must enter the Unity Connection alias and the LDAP password.

Step 5 Re-enable LDAP authentication. For more information, see the Configuring LDAP Authentication in Unity Connection section.

Step 6 Re-add LDAP configurations but do not synchronize Unity Connection and LDAP data. The synchronization do not work until you re-enable the DirSync service. For more information, see the Configuring LDAP Directory Configurations section.

Step 7 Activate the DirSync service. See the Activating Cisco DirSync Service section.

Step 8 Synchronize Unity Connection data with LDAP data:

a) In Cisco Unity Connection Administration, expand **System Settings > LDAP** and select **LDAP Directory Configuration**.

b) On the Find and List LDAP Directory Configurations page, select the necessary directory configuration.

c) On the LDAP Directory Configuration page, select **Perform Full Sync Now**.

Determining if a Unity Connection User is Integrated with an LDAP Directory

If you integrate Unity Connection user accounts with LDAP user accounts, you are not required to integrate every Unity Connection account with an LDAP account. In addition, you can create new Unity Connection accounts that are not integrated with LDAP accounts.

Step 1 In Cisco Unity Connection Administration, expand Users and select Users.

Step 2 The Search Users page appears displaying the default and currently configured users.

Step 3 Select the user that you want to determine if it is integrated with LDAP directory.

Step 4 On the Edit User Basics page, if the user is integrated with an LDAP user account, the Status area contains one of the following messages:

- Active User Imported from LDAP Directory
- Inactive User Imported from LDAP Directory

If neither of these messages appears in the Status area, the user is not integrated with an LDAP user account.

Changing LDAP Integration Status

To change the LDAP integration status of a Unity Connection user, you use one of the following methods, depending on your situation:

- To change the LDAP integration status of an individual Unity Connection user who was not created by importing from Cisco Unified Communications Manager, see the Changing the LDAP Integration Status of an Individual Unity Connection User.
- To change the LDAP integration status of multiple Unity Connection users who were not created by importing from Cisco Unified Communications Manager, see the Changing the LDAP Integration Status of Multiple Unity Connection User Accounts in Bulk Edit Mode.
- To change the LDAP integration status of Unity Connection users who were created by importing from Cisco Unified Communications Manager, see the Integrating Existing Unity Connection User Accounts with LDAP User Accounts Using Bulk Administration Tool.

Regardless of the method you select, note the following considerations which apply to all cases:

If you are integrating a Unity Connection user account with an LDAP user account, note the following:

- If any users in the LDAP directory were missing values in the field that you specified on the LDAP Setup page in the LDAP Attribute for User ID list, you must add the missing values in the LDAP directory and resynchronize the Unity Connection database with the LDAP directory.
- During the next scheduled synchronization of the Connection database with the LDAP directory, existing values for certain fields are overwritten with values from the LDAP directory.
- If you have configured Unity Connection to periodically resynchronize Unity Connection data with LDAP data, new values in the LDAP directory are automatically imported into the Unity Connection database during the next automatic resynchronization. However, if new users have been added to the LDAP directory, this resynchronization does not create new Unity Connection users. You must manually create new Unity Connection users using either the Import Users tool or the Bulk Administration Tool.

If you are breaking the association between a Unity Connection user account and an LDAP directory user account, note the following:

- If Unity Connection is configured to authenticate passwords for web applications against the LDAP directory, the Unity Connection user is no longer authenticate against the LDAP password for the corresponding user. To enable the user to log on to Unity Connection web applications, you must enter a new password on the Edit > Change Password page.
- If Unity Connection is configured to periodically synchronize with the LDAP directory, selected data for the Unity Connection user is no longer be updated when the corresponding data in the LDAP directory is updated.

Changing the LDAP Integration Status of an Individual Unity Connection User

Step 1 In Cisco Unity Connection Administration, click **Users**.

Step 2 On the Search Users page, click the alias of the user account.

Note If the user does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and click **Find**.

Step 3 On the Edit User Basics page, in LDAP Integration Status section, select the desired radio button:

- Integrate with LDAP Directory—To integrate a Unity Connection user account with an LDAP user account, select this option. The Unity Connection alias must match the corresponding value in the LDAP directory. (On the System

Settings > LDAP > LDAP Setup page, the LDAP Attribute for User ID list identifies the field in the LDAP directory for which the value must match the value of the Alias field in Unity Connection.)

- Do Not Integrate with LDAP Directory—To break the association between a Unity Connection user account and an LDAP directory user account, select this option.

If the user was created by importing from Cisco Unified Communications Manager, the LDAP Integration Status field is grayed out and you must use Bulk Administration Tool to integrate them with an LDAP user account. See Integrating Existing Unity Connection User Accounts with LDAP User Accounts Using Bulk Administration Tool.

Step 4 Click **Save**.

Changing the LDAP Integration Status of Multiple Unity Connection User Accounts in Bulk Edit Mode

Step 1 In Cisco Unity Connection Administration, on the Search Users page, check the applicable user check boxes, and select Bulk Edit.

If the user accounts that you want to edit in bulk do not all appear on one Search page, check all applicable check boxes on the first page, then go to the next page and check all applicable check boxes, and so on, until you have selected all applicable users. Then select Bulk Edit.

Step 2 On the User Basics page, in LDAP Integration Status section, select the desired radio button:

- Integrate with LDAP Directory—To integrate a Unity Connection user account with an LDAP user account, select this option. The Unity Connection alias must match the corresponding value in the LDAP directory. (On the System Settings > LDAP > LDAP Setup page, the LDAP Attribute for User ID list identifies the field in the LDAP directory for which the value must match the value of the Alias field in Unity Connection.)
- Do Not Integrate with LDAP Directory—To break the association between a Unity Connection user account and an LDAP directory user account, select this option.
- If applicable, set the Bulk Edit Task Scheduling Fields to schedule the Bulk Edit operation for a later date and/or time.
- Select Submit.

If any of the users were created by importing from Cisco Unified Communications Manager, Bulk Edit logs an error indicating that you must use the Bulk Administration Tool to integrate them with an LDAP user account. See Integrating Existing Unity Connection User Accounts with LDAP User Accounts Using Bulk Administration Tool.

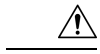
Integrating Existing Unity Connection User Accounts with LDAP User Accounts Using Bulk Administration Tool

The Bulk Administration Tool can be used to integrate existing Unity Connection users with LDAP user accounts, but it cannot be used to break the association between a Unity Connection user account and an LDAP directory user account.

That process invisibly imported the LDAP data into a hidden Cisco Unified Communications Manager database on the Unity Connection server.

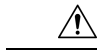
When you use the Bulk Administration Tool to integrate existing Unity Connection users with LDAP users, you do the following tasks, which update each Unity Connection user account with the LDAP user ID for the corresponding LDAP user account:

- Export the data from the Cisco Unified CM database into a CSV file.
- Update the CSV file to remove LDAP users who don't have Unity Connection accounts and to remove Cisco Unified CM IDs, if applicable.



Caution If any users in the LDAP directory were missing values in the field that you specified on the LDAP Setup page in the LDAP Attribute for User ID list, you must add the missing values in the LDAP directory and resynchronize the Unity Connection database with the LDAP directory. Do not enter the values in the CSV file and then import the CSV file; Unity Connection is not able to locate those users in the LDAP directory.

- Import the updated CSV file into the Unity Connection database.



Caution When you import LDAP user data into the Unity Connection database, existing values for the fields being imported are overwritten with values from the LDAP directory.

Step 1 For every Cisco Unity Connection user that you want to integrate with an LDAP user, if the value of the Unity Connection Alias field does not match the value of the LDAP user ID, use Cisco Unity Connection Administration to update the Unity Connection alias so that they do match.

Step 2 Sign in to Unity Connection Administration as a user that has the System Administrator role.

Step 3 Expand **Tools** and select **Bulk Administration Tool**.

Step 4 Export to a CSV file the LDAP user data that is currently in the cache on the Connection server:

a) Under Select Operation, select **Export**.
b) Under Select Object Type, select **Users from LDAP Directory**.
c) In the **CSV File** field, enter the name of the file in which you want to save exported data.
d) Select **Submit**.

Step 5 Download and edit the CSV file that you created in Step 4:

- Remove any Unity Connection users who you do not want to synchronize with users in the LDAP directory.
- For Unity Connection users who were originally created by importing data from Cisco Unified CM, enter %null% in the CcmId field.
- Confirm that the LdapCcmUserId field contains the correct LDAP alias for each user.

Step 6 Import the data that you edited in Step 5:

- **a.** In Cisco Unity Connection Administration, expand **Tools** and select **Bulk Administration Tool**.
- **b.** Under Select Operation, select **Update**.
- **c.** Under Select Object Type, select **Users with Mailbox**.

d. In the **CSV File** field, enter the full path to the file from which you want to import data.

e. In the Failed Objects Filename field, enter the name of the file to which you want Unity Connection to write error messages about users who could not be created.

f. Select **Submit**.

Step 7 When the import is complete, review the file that you specified in the Failed Objects Filename field to verify that all Unity Connection users were successfully integrated with the corresponding LDAP users.