C H A P T E R 41

Integrating Cisco Unity Connection 8.x with an LDAP Directory

⚠️ **Caution** Information in this chapter is applicable in a Cisco Unity Connection configuration only. For information on integrating Cisco Unified Communications Manager Business Edition (CMBE) with an LDAP directory, see the following documentation available at http://www.cisco.com/en/US/products/ps7273/prod_maintenance_guides_list.html:
– The "Understanding the Directory" chapter of the *Cisco Unified Communications Manager System Guide for Cisco Unified Communications Manager Business Edition.*
– The "End User Configuration" chapter of the *Cisco Unified Communications Manager Administration Guide for Cisco Unified Communications Manager Business Edition.*

If you are using a supported LDAP-compliant directory as your corporate directory and if you do not want to separately maintain basic user information in Cisco Unity Connection, you can:

- Create Connection users by importing user data from the LDAP directory, and

- Configure Connection to periodically resynchronize Connection data with data in the LDAP directory.

For a list of the LDAP directories that are supported for use with Connection, see the "Requirements for an LDAP Directory Integration" section in *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:

Integrating Cisco Unified Communications Manager and Cisco Unity Connection 8.x with an LDAP Directory

Added November 16, 2010

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

For information on integrating Cisco Unified CM with an LDAP directory, start with the "LDAP System Configuration" chapter in the "System Configuration" section of the applicable *Cisco Unified Communications Manager Administration Guide* at
http://www.cisco.com/en/US/products/sw/voicesw/ps556/prod_maintenance_guides_list.html.

For information on integrating Connection with an LDAP directory, start with the "Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 8.x Users with LDAP Users" section on page 41-2.

Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Cisco Unity Connection 8.x Users with LDAP Users

Revised November 16, 2010

To configure LDAP and to create users by importing user data from the LDAP directory, do the following tasks:

1. Turn on the Cisco DirSync service. See the "Activating the Cisco DirSync Service in Cisco Unity Connection 8.x" section on page 41-4.

2. Enable LDAP synchronization. See the "Enabling LDAP Synchronization in Cisco Unity Connection 8.x" section on page 41-4.

   If you are using LDAP authentication to authenticate user access to Connection web applications or IMAP access to Connection voice messages, you must enable LDAP synchronization.

3. *(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 Connection, specify a filter that converts phone numbers into extensions when you import LDAP data into Connection. See the applicable section:

– Converting Phone Numbers into Extensions (Cisco Unity Connection 8.5 and Later Only), page 41-5

– Converting Phone Numbers into Extensions (Cisco Unity Connection 8.0), page 41-7

If you use the Bulk Administration Tool (BAT) to create users, you may be able to achieve the same or better results than you could by specifying a filter in this step. In Task 9., if you use BAT, you export 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 that you can specify for the filter discussed in the "Converting Phone Numbers into Extensions (Cisco Unity Connection 8.0)" section on page 41-7.

4. *(Optional)* If you want to use SSL to encrypt the usernames and passwords that are sent to the LDAP server for authentication and/or you want to use SSL to encrypt the data that is passed from the LDAP server to the Connection server during synchronization, export an SSL certificate from the applicable LDAP servers and upload the certificates on all Connection servers. See the "Uploading SSL Certificates on the Cisco Unity Connection 8.x Server" section on page 41-8.

5. *(Optional)* If you want Connection users who access a Connection web application or who access Connection voice messages by using an IMAP email application to authenticate their username and password against the LDAP directory, configure LDAP authentication. See the "Configuring LDAP Authentication in Cisco Unity Connection 8.x" section on page 41-9.

6. Select the user search bases that you will specify when you create LDAP directory configurations in Task 8. See the "Selecting the LDAP Users to Import into Cisco Unity Connection 8.x" section on page 41-12.

7. *(Required if the number of users in all user search bases is greater than 60,000, optional otherwise)* If the user search bases that you selected in Task 6. do not give you enough control over which LDAP users are synchronized with Connection users, you may want to specify one or more LDAP filters. See the "Filtering LDAP Users in Cisco Unity Connection 8.x" section on page 41-13.

8. Add one or more LDAP directory configurations, which define the LDAP directory and user search bases in which Connection accesses data, and import data from the LDAP directory into a hidden Cisco Unified CM database on the Connection server. When you create Connection users that are linked to LDAP users or you convert existing Connection users to users who are integrated with an LDAP directory, the data on the LDAP users is taken from the Cisco Unified CM database on the Connection server. See the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 8.x" section on page 41-15.

9. If you are synchronizing existing Connection users with users in an LDAP directory, see the applicable section in the "Creating User Accounts from LDAP User Data or Changing LDAP Integration Status for Existing Users in Cisco Unity Connection 8.x" 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.

   – *(Connection 8.5 and later)* See the "Changing the LDAP Integration Status of Connection Users (Connection 8.5 or Later)" section.

   – *(Connection 8.0)* See the "Integrating Existing Cisco Unity Connection 8.0 User Accounts with LDAP User Accounts" section.

If you are creating new Connection users who are synchronized with users in an LDAP directory, use one of the following methods:

   – If you are creating a small number of users (a few hundred or fewer) and if you were able to create a regular expression to convert LDAP phone numbers into Connection extensions, you can use the Import Users tool.

–   If you are creating a larger number of users or if you were not able to create a regular expression to convert LDAP phone numbers into Connection extensions, export user data to a CSV file by using the Bulk Administration Tool, reformat the data by using a spreadsheet application (if necessary), and import the data by using the Bulk Administration tool.

Activating the Cisco DirSync Service in Cisco Unity Connection 8.x

The Cisco DirSync service must be turned on for Connection to access an LDAP directory. Do the following procedure.

To Turn On the Cisco DirSync Service

Step 1   Sign in to Cisco Unified Serviceability as a user that has the System Administrator role.

Step 2   On the Tools menu, select **Service Activation**.

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

Step 4   Select **Save**, and select **OK** to confirm.

Enabling LDAP Synchronization in Cisco Unity Connection 8.x

Revised November 16, 2010
LDAP synchronization must be enabled for Connection to access an LDAP directory. Do the following procedure.

To Enable LDAP Synchronization

Step 1   Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

Step 2   Expand **System Settings > LDAP**, then select **LDAP Setup**.

Step 3   On the LDAP Setup page, check the **Enable Synchronizing from LDAP Server** check box.

Step 4   In the LDAP Server Type list, select the type of LDAP server that you want to access.

When you are configuring Connection for Microsoft Active Directory 2008 Lightweight Directory Services, select **Microsoft Active Directory Application Mode**.

Step 5   In the LDAP Attribute for User ID list, select the field in the LDAP directory whose data you want to appear in the Alias field in Connection. Note the following requirements:

   •   The field that you select must have a value for every user in the LDAP directory.

   •   Every value for that field must be unique.

⚠

Caution   If you select a field other than sAMAccountName, when users sign in to the Cisco PCA or an IMAP client (Connection 8.x) or sign in to the Web Inbox (Connection 8.5 only), they must enter their Connection alias and their LDAP password.

⚠

Caution   If you later need to change the field that you select now, and if you have already created LDAP directory configurations on the LDAP Directory page, you must delete all LDAP directory configurations, change the value here, and recreate all LDAP directory configurations. For more information, see the "Changing Which LDAP Field Is Mapped to the Alias Field in Connection" section on page 41-17.

Step 6   Select **Save**.

Disabling LDAP Synchronization in Cisco Unity Connection 8.x

If you want to temporarily disable LDAP synchronization, do the following procedure.

To Disable LDAP Synchronization

Step 1   Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

Step 2   Expand **System Settings > LDAP**, then select **LDAP Setup**.

Step 3   On the LDAP Setup page, uncheck the **Enable Synchronizing from LDAP Server** check box.

Step 4   Select **Save**.

Converting Phone Numbers into Extensions (Cisco Unity Connection 8.5 and Later Only)

Added November 16, 2010
If you want to map phone numbers in the LDAP directory to extensions in Connection but the phone numbers do not match the extensions, you can add a regular expression and a replacement pattern that together convert the phone numbers into extensions:

- The regular expression determines which phone numbers to operate on (for example, phone numbers that are 10 digits long) and the portion of the phone numbers to use as a basis for the extensions (for example, the last four digits).

- The replacement pattern specifies either to use the values selected by the regular expression or to perform additional operations (for example, prepend an 8).

Connection uses the regular expression package of the Java library. Table 41-1 lists some examples of the conversions that are possible with the expanded functionality. For more information, refer to a reference on regular expressions; several are available in print and online; do a web search on "regular expression."

Note the following:

- Connection automatically removes non-numeric characters from the phone number, so the regular expression does not need to account for non-numeric characters.

- If a phone number in the LDAP directory does not match the regular expression, the corresponding Connection Extension field will contain the numeric portion of the LDAP phone number. For example, if a phone number begins with 425 and the regular expression gets the last four digits of the LDAP phone number as the Connection extension, but only if the LDAP phone number starts with 206, the Extension field for that Connection user will contain the entire LDAP phone number minus any non-numeric characters.

- 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 synchronizes data with the LDAP directory.

- You can often write more than one combination of regular expression and replacement pattern that produces the same result.

Table 41-1   Example Phone Number Conversions for Connection 8.5

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

If the expanded support for regular expressions cannot convert phone numbers in your LDAP directory into Connection extensions, you may want to explore whether a formula in a spreadsheet application is able to produce the results that you want. If so, when you create new Connection users from LDAP data or synchronize existing Connection users with LDAP users, you can manipulate phone number data in the CSV file using a spreadsheet application before you import the data back into Connection. See either

the "Creating Cisco Unity Connection 8.x Users from LDAP Data by Using the Bulk Administration Tool" section or the ""Integrating Existing Connection User Accounts with LDAP User Accounts Using Bulk Administration Tool (Cisco Unity Connection 8.5)" section, as applicable, in the "Creating User Accounts from LDAP User Data or Changing LDAP Integration Status for Existing Users in Cisco Unity Connection 8.x" 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.

To Add a Regular Expression and Replacement Pattern That Convert LDAP Phone Numbers into Cisco Unity Connection 8.5 Extensions

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

Step 2   In the Regular Expression for LDAP Phone Number Pattern field, enter a regular expression that identifies:

- Which phone numbers in the LDAP directory you want to convert to extensions (for example, 10-digit phone numbers that begin with 206).

- The portion of the phone numbers to use as a basis for the extensions (for example, the last four digits).

Step 3   In the Replacement Pattern field, enter a value that specifies either to use the values selected by the regular expression or to perform additional operations (for example, prepend an 8).

> ⚠
>
> **Caution**   Connection validates the syntax of the regular expression but does not validate the replacement pattern, and also cannot validate the result of the regular expression and the replacement pattern. We recommend that you verify the results on the Import Users page of Connection Administration before you create Connection subscribers.

Step 4   Select **Save**.

Converting Phone Numbers into Extensions (Cisco Unity Connection 8.0)

If you want to map phone numbers in the LDAP directory to extensions in Connection but the phone numbers do not match the extensions, you can add a regular expression that converts the phone numbers into extensions. Current support for regular expressions is limited: you can use regular expressions to create the Connection extension only by removing digits from the phone number in the LDAP directory. You cannot use regular expressions to prepend, append, or substitute digits.

If a regular expression cannot convert phone numbers in your LDAP directory into Connection extensions, you may want to explore whether a formula in a spreadsheet application is able to produce the results that you want. If so, when you create new Connection users from LDAP data or synchronize existing Connection users with LDAP users, you can manipulate phone number data in the CSV file using a spreadsheet application before you import the data back into Connection. See either the "Creating Cisco Unity Connection 8.x Users from LDAP Data by Using the Bulk Administration Tool" section or the "Integrating Existing Connection User Accounts with LDAP User Accounts (Cisco Unity Connection 8.0)" section, as applicable, in the "Creating User Accounts from LDAP User Data or

Changing LDAP Integration Status for Existing Users in Cisco Unity Connection 8.x" 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 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 synchronizes data with the LDAP directory.

To Add a Filter That Converts LDAP Phone Numbers into Cisco Unity Connection 8.0 Extensions

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

Step 2 In the Filter to Convert LDAP Phone Numbers into Connection Extensions field, enter a regular expression to convert the phone number that is imported from the LDAP directory into an extension for use in Connection. For example:

- To use the phone number as the extension, without punctuation, if any, enter:

  [0-9]+

- To use the last four digits of the phone number as the extension, enter:

  [0-9][0-9][0-9][0-9]$

- To use the first four digits of the phone number as the extension, enter:

  ^[0-9][0-9][0-9][0-9]

For more information on regular expressions, do a web search on "regular expression."

Step 3 Select **Save**.

Uploading SSL Certificates on the Cisco Unity Connection 8.x Server

If you want to use SSL to encrypt data that is transmitted between the LDAP server and the Connection server, do the following procedure.

Note You must also specify servers by host name instead of by IP address, and check the "Use SSL" check box for each LDAP server that you configure for synchronization (see the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 8.x" section on page 41-15), or for authentication (see the "Configuring LDAP Authentication in Cisco Unity Connection 8.x" section on page 41-9).

To Upload SSL Certificates from the LDAP Directory Servers

Step 1   Export the SSL certificate from the LDAP server with which you want Connection to synchronize data and from the LDAP server that you want Connection to access when authenticating user sign-ins, if any.

Ifyou want to configure redundant LDAP servers for synchronization and/or for authentication, export an SSL certificate from each LDAP server with which you want Connection to synchronize or authenticate.

Step 2   On the Connection server, sign in to Cisco Unified Operating System Administration.

Step 3   On the Security menu, select **Certificate Management**.

Step 4   Upload the directory certificate trust that you exported in Step 1:

- For Connection 8.0(1) and 8.0(2), upload the directory certificate trust to directory-trust.

- For Connection 8.0(3) and later, upload the directory certificate trust to tomcat-trust.

If you want this Connection server to synchronize with more than one LDAP server or to authenticate with more than one LDAP server, upload the directory certificate trusts from all of the LDAP servers.

For more information on uploading directory certificate trusts and on restarting the Cisco Dirsync and Cisco Tomcat services, on the Help menu, select **This Page**.

⚠️

Caution   You must restart the Cisco DirSync and Cisco Tomcat services, or LDAP synchronization and authentication will fail.

Step 5   If you are configuring Connection clustering, or if you are configuring a Digital Network, repeat Step 2 through Step 4 on the other Connection servers.

Configuring LDAP Authentication in Cisco Unity Connection 8.x

Revised November 03, 2011

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 in *Design Guide for Cisco Unity Connection*.

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.

If you want to use LDAP usernames and passwords to authenticate sign-ins to Cisco Unity Connection web applications or IMAP access to Connection voice messages, do the following procedure to configure LDAP authentication.

> **Note**   You cannot use LDAP usernames and passwords to authenticate sign-ins for the administrator account that you created during installation. The administrator account is used to sign on to Cisco Unified Operating System Administration, the Disaster Recovery System, and the command line interface.

To Configure LDAP Authentication

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

Step 2   Check the Use LDAP Authentication for End Users check box.

Step 3   Enter other values as applicable. For more information, on the Help menu, select **This Page**.

If you change the value of the Host Name or IP Address for Server field, and if IMAP clients are accessing Connection, restart the Connection IMAP Server service. If other web applications are accessing Connection (for example, Cisco Personal Communications Assistant), restart the server.

If you uploaded SSL certificates to the Connection server in the "To Upload SSL Certificates from the LDAP Directory Servers" procedure on page 41-9:

- Check the **Use SSL** check box for every LDAP server that you specify in the Host Name or IP Address for Server field.

- In the Host Name or IP Address for Server field, specify the host name of the server, or authentication will probably fail for IMAP clients. If you specify an IP address and the SSL certificate identifies the LDAP server only by host name (which is common—certificates rarely include the IP address of a server), Connection cannot verify the identity of the LDAP server.

> **Note**   With some supported LDAP directories, you cannot specify redundant LDAP servers. For information on the LDAP directories with which Connection allows you to specify redundant servers, see the "Requirements for an LDAP Directory Integration" section in *System Requirements for Cisco Unity Connection Release 8.x*.

Step 4   Select **Save**.

Disabling LDAP Authentication

Added November 16, 2010

If you permanently disable LDAP authentication, users sign in to Connection web applications by using their Connection web application password instead of their LDAP directory password. If Connection users were integrated with an LDAP directory when Connection was first installed or if they have been integrated with an LDAP directory for a while, they either do not have Connection web application

passwords or they do not remember their Connection web application password. Do the following procedure to force users to change their Connection web application password the next time they sign in to a Connection web application and to disable LDAP authentication.

You can use Bulk Edit to change passwords for users who have a mailbox, but you must individually change passwords for users who not have a mailbox (meaning administrators).

If you temporarily disable LDAP authentication, for example, because you are changing which field is mapped to the Alias field in Connection, you do not have to change password settings for Connection users.

To Disable LDAP Authentication

Step 1   Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

Step 2   In Cisco Unity Connection Administration, expand **System Settings > LDAP**, and select **LDAP Authentication**.

Step 3   Uncheck the **Use LDAP Authentication for End Users** check box.

Step 4   Select **Save**.

Step 5   If you are only temporarily disabling LDAP authentication, skip the rest of this procedure. Do not change password settings.

Step 6   To change the password setting for users who have a mailbox:

    a.   In Cisco Unity Connection Administration, expand **Users** and select **Users**.

    b.   If all Connection users are integrated with LDAP directory users, select all users. Otherwise, select the users who are integrated with an LDAP directory.

    c.   Select **Bulk Edit**.

    d.   On the **Edit** menu, select **Password Settings**.

    e.   In the Choose Password list, choose **Web Application**.

    f.   For **User Must Change at Next Sign-In**, check both check boxes.

    g.   If you want to schedule when Connection changes the setting for the selected users, under Bulk Edit Task Scheduling, choose **Run Later** and specify a date and time.

    h.   Select **Submit**.

Step 7   To change the password setting for users who do not have a mailbox:

    a.   In Cisco Unity Connection Administration, expand **Users** and select **Users**.

    b.   Select the first user.

    c.   On the **Edit** menu, select **Password Settings**.

    d.   In the Choose Password list, choose **Web Application**.

    e.   Check the **User Must Change at Next Sign-In** check box.

    f.   Select **Save**.

    g.   Repeat Step a. through Step f. for the remaining users who do not have a mailbox.

Selecting the LDAP Users to Import into Cisco Unity Connection 8.x

Later in this chapter, you create up to five Cisco Unity Connection LDAP directory configurations that specify which users in the LDAP directory you want to import into Connection. For each LDAP directory configuration, you specify a user search base, which 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.

After you create the LDAP directory configurations, you synchronize Connection data with data in the LDAP directory, which imports LDAP data into a hidden Cisco Unified Communications Manager database on the Connection server. There is a practical limit of 60,000 users that can be imported into the Cisco Unified CM database. The limit is not enforced by the synchronization process, but 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.

> ⚠
> **Caution**   Do not specify user search bases that will cause more than 60,000 users to be imported into the Cisco Unified CM database during synchronization, or Connection performance will be adversely affected.

We recommend that you analyze the structure of your LDAP directory and determine whether you can specify five or fewer user search bases that:

- Include the LDAP users that you want to import into Connection.
- Exclude the LDAP users that you do not want to import into Connection.
- Will cause fewer than 60,000 users to be imported into the Cisco Unified CM database.

If you cannot specify five or fewer search bases that meet all three of these criteria, we recommend that you create one or more LDAP filters to filter out the unwanted users specified by the search bases. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 8.x" section on page 41-13.

Directories Other than Active Directory

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), 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 an LDAP search filter. For more information, see the "Filtering LDAP Users in Cisco Unity Connection 8.x" section on page 41-13.

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.

Active Directory

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.

Cisco Unity Connection Intrasite and Intersite Networking

Revised November 16, 2010

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

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

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

Filtering LDAP Users in Cisco Unity Connection 8.x

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.

- The LDAP directory includes more than 60,000 users. When you create Connection users by importing LDAP users, there is a practical limit of 60,000 users that can be imported into the Cisco Unified Communications Manager database on the Connection server. The limit is not enforced by the synchronization process, but importing large numbers of LDAP users who will not become Connection users slows database performance and causes upgrades to take longer.

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

- You cannot create LDAP filters for Cisco Unified Communications Manager Business Edition.

- 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 specified by the new or updated filter to be accessible to Connection:

  1. Turn off and turn on again the Cisco DirSync service. In Cisco Unified Serviceability, select **Tools > Service Activation**. Uncheck the check box next to **Cisco DirSync**, and select **Save** to turn off the service. Then check the check box next to **Cisco DirSync**, and select **Save** to turn on 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.

Do the following procedure to add an LDAP filter.

To Add an LDAP Filter

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

Step 2   Select **Add New**.

Step 3   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 4   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 5   Select **Save**.

Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 8.x

Revised November 16, 2010

✎

Note   *Connection 8.5 and later only:* If you are configuring unified messaging with Exchange, you must enter the Exchange email address for each Connection user. On the Unified Messaging Account page in Connection Administration, each user can be configured to use either of the following values:

– The Corporate Email Address specified on the User Basics page
– The email address specified on the Unified Messaging Account page

As you add LDAP directory configurations, we recommend that you choose the option to synchronize the Mail ID field in Cisco Unified Communications Manager with the mail field in the LDAP directory. This causes values in the LDAP mail field to appear in the Corporate Email Address field in Connection. Automatically populating the Corporate Email Address field with the value of the LDAP mail field is easier than populating the email address field on the Unified Messaging Account page by using Connection Administration or the Bulk Administration Tool.

Do the following procedure once for each user search base in the LDAP directory from which you want to import user data into Cisco Unity Connection.

To Add an LDAP Directory Configuration

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

Step 2   In the LDAP Configuration Name field, enter a name for this LDAP directory configuration. If you are adding more than one LDAP directory configuration with different LDAP user search bases, enter a name that identifies the users in the current search base.

Step 3   Enter other values as applicable. For more information, on the Help menu, select **This Page**.

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

If you uploaded SSL certificates to the Connection server in the "To Upload SSL Certificates from the LDAP Directory Servers" procedure on page 41-9, check the **Use SSL** check box for every LDAP server that you specify in the **Host Name or IP Address for Server** field.

✎

Note   With some supported LDAP directories, you cannot specify redundant LDAP servers. For information on the LDAP directories with which Connection allows you to specify redundant servers, see the "Requirements for an LDAP Directory Integration" section in *System Requirements for Cisco Unity Connection Release 8.x*.

Step 4   Select **Save**.

Step 5   Select **Perform Full Sync Now**.

Step 6   To add another LDAP directory configuration for another user search base, select **Add New**, and repeat Step 2 through Step 5.

Changing LDAP Directory Configurations in Cisco Unity Connection 8.x

Added November 16, 2010

If you want to change an LDAP directory configuration, for example, by changing which LDAP user fields are imported into Connection, you must delete the existing directory configuration and recreate it.

> ⚠ **Caution**   You must recreate the directory configuration within 24 hours, or the Connection users that are integrated with LDAP users will be converted to standalone Connection users.

To Change LDAP Directory Configurations

Step 1   Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

Step 2   Expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

Step 3   If you do not have a record of the existing settings, select the configuration that you want to change, and write down the existing settings.

Step 4   On the Find and List LDAP Directory Configurations page, check the check box next to the directory configuration that you want to change.

> ✎ **Note**   If the directory configuration does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

Step 5   Select **Delete Selected**.

Step 6   In the dialog box that opens, asking you to confirm the deletion, select **OK**.

Step 7   Under **System Settings > LDAP**, select **LDAP Setup**.

Step 8   On the LDAP Setup page, uncheck the **Enable Synchronizing from LDAP Server** check box.

Step 9   Select **Save**.

Step 10   Recheck the **Enable Synchronizing from LDAP Server** check box.

Step 11   Select **Save** again.

Step 12   Recreate the directory configuration, and perform a full synchronization for the recreated directory configuration. See the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 8.x" section on page 41-15.

Step 13   Repeat Step 2 through Step 12 for other directory configurations that you want to change, if any.

Deleting LDAP Directory Configurations in Cisco Unity Connection 8.x

Added November 16, 2010

If you want to delete an LDAP directory configuration, for example, because you no longer want Connection users to be integrated with an LDAP directory, do the following procedure.

⚠
Caution   When you delete a directory configuration, Connection users that are integrated with LDAP users are converted to standalone Connection users in 24 hours.

To Delete LDAP Directory Configurations

Step 1   Sign in to Cisco Unity Connection Administration as a user that has the System Administrator role.

Step 2   Expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

Step 3   On the Find and List LDAP Directory Configurations page, check the check boxes next to the directory configurations that you want to delete.

✎
Note   If a directory configuration does not appear in the search results table, set the applicable parameters in the search fields at the top of the page, and select **Find**.

Step 4   Select **Delete Selected**.

Step 5   In the dialog box that opens, asking you to confirm the deletion, select **OK**.

Step 6   Under **System Settings > LDAP**, select **LDAP Setup**.

Step 7   On the LDAP Setup page, uncheck the **Enable Synchronizing from LDAP Server** check box.

Step 8   Select **Save**.

Step 9   Recheck the **Enable Synchronizing from LDAP Server** check box.

Step 10   Select **Save** again.

Changing Which LDAP Field Is Mapped to the Alias Field in Connection

Added November 16, 2010
If you need to change which field in the LDAP directory is mapped to the Alias field in Connection, do the following procedure.

⚠
Caution   You must complete this entire procedure within 24 hours, or Connection will convert all of the users who are integrated with the LDAP directory to standalone Connection users.

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

To Change the LDAP Field that Is Mapped to the Alias Field in Connection

Step 1   Disable the DirSync service:

   a.   Sign in to Cisco Unified Serviceability as a user that has the System Administrator role.

b. On the Tools menu, select **Service Activation**.

c. Under Directory Services, uncheck the **Cisco DirSync Service** check box.

d. Select **Save**, and select **OK** to confirm.

Step 2 Disable LDAP authentication. See the "Disabling LDAP Authentication" section on page 41-10.

Step 3 Delete all LDAP directory configurations:

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

b. Expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

c. If necessary, write down the specifications for the existing LDAP directory configurations so you can reproduce them later in this procedure.

d. On the Find and List LDAP Directory Configurations page, select all directory configurations.

e. Select **Delete Selected**.

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

a. In Connection Administration, expand **System Settings > LDAP**, then select **LDAP Setup**.

b. In the LDAP Attribute for User ID list, select the field in the LDAP directory whose data you want to appear in the Alias field in Connection. Note the following requirements:

   – The field that you select must have a value for every user in the LDAP directory.

   – Every value for that field must be unique.

⚠

Caution   If you select a field other than sAMAccountName, when users sign in to the Cisco PCA or an IMAP client (Connection 8.x) or sign in to the Web Inbox (Connection 8.5 only), they must enter their Connection alias and their LDAP password.

c. Select **Save**.

Step 5 Re-enable LDAP authentication. For more information, see the "Configuring LDAP Authentication in Cisco Unity Connection 8.x" section on page 41-9.

Step 6 Re-add LDAP configurations, but do not synchronize Connection and LDAP data. The synchronization will not work until after you re-enable the DirSync service in the next step.

For more information, see the "Adding LDAP Directory Configurations and Importing LDAP Data in Cisco Unity Connection 8.x" section on page 41-15.

Step 7 Re-enable the DirSync service:

a. Sign in to Cisco Unified Serviceability as a user that has the System Administrator role.

b. On the Tools menu, select **Service Activation**.

c. Under Directory Services, check the **Cisco DirSync Service** check box.

d. Select **Save**, and select **OK** to confirm.

Step 8 Synchronize Connection data with LDAP data:

a. In Connection Administration, expand **System Settings > LDAP**, then select **LDAP Directory Configuration**.

b. Select **Find** to display a list of all directory configurations.

c. Display the first directory configuration, and select **Perform Full Sync Now**.

d. Repeat Step a. through Step c. for the remaining directory configurations.