CHAPTER 43

Integrating Cisco Unity Connection with an LDAP Directory

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 7.x* at http://www.cisco.com/en/US/docs/voice_ip_comm/connection/7x/requirements/7xcucsysreqs.html.

Note that you can only use the information in this chapter to integrate Cisco Unity Connection with an LDAP directory. For information on integrating Cisco Unified Communications Manager Business Edition 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*.

See the following sections:

Task List for Configuring LDAP and for Creating New Users or Synchronizing Existing Connection Users with LDAP Users

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

1. Activate the Cisco DirSync service. See the "Activating the Cisco DirSync Service" section on page 43-3.
2. Enable LDAP synchronization. See the "Enabling LDAP Synchronization" section on page 43-3.

   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 "Converting Phone Numbers into Extensions" section on page 43-4.

   (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 8., 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" section on page 43-4.)

Note To integrate existing Connection users with LDAP users, you must use BAT.

4. *(Optional)* If you want to use SSL to encrypt the user names 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 Connection Server" section on page 43-4.
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 user name and password against the LDAP directory, configure LDAP authentication. See the "Configuring LDAP Authentication" section on page 43-5.
6. *(Optional)* If user search bases do not give you enough control over which LDAP users are synchronized with Connection users, you may want to specify an LDAP filter. See the "Filtering LDAP Users" section on page 43-6.
7. Add one or more LDAP configurations, which define the LDAP directory and user search bases in which Connection accesses data, and synchronize the Cisco Unified Communications Manager directory with the LDAP directory. See the "Adding LDAP Configurations and Synchronizing Data" section on page 43-7.
8. If you are synchronizing existing Connection users with users in an LDAP directory, do the procedure in the "Integrating Existing Cisco Unity Connection User Accounts with LDAP User Accounts" section in the "Creating User Accounts from LDAP User Data" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

   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

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

To Activate the Cisco DirSync Service

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

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

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

Step 4 Click **Save**, and click **OK** to confirm.

Enabling LDAP Synchronization

LDAP synchronization must be enabled for Connection to access an LDAP directory. Do the following procedure.

To Enable LDAP Synchronization

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

Step 2 Expand **System Settings > LDAP**, then click **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, choose the type of LDAP server that you want to access.

Step 5 In the LDAP Attribute for User ID list, choose the field in the LDAP directory whose data you want to appear in the Alias field in Connection. The field that you choose must have a value for every user in the LDAP directory. In addition, every value for that field must be unique.

Caution If you later need to change the field that you choose now, and if you have already created LDAP configurations on the LDAP Directory page, you must delete all LDAP configurations, change the value here, and recreate all LDAP configurations.

Step 6 Click **Save**.

Converting Phone Numbers into Extensions

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.

Note A regular expression may not be sufficient to convert phone numbers in your LDAP directory into Connection extensions. In that case, 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 by using the Bulk Administration Tool or synchronize existing Connection users with LDAP users, also by using the Bulk Administration Tool, 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 Users from LDAP Data by Using the Bulk Administration Tool" or the "Integrating Existing Cisco Unity Connection User Accounts with LDAP User Accounts" section, as applicable, in the "Creating User Accounts from LDAP User Data" chapter of the *User Moves, Adds, and Changes Guide for Cisco Unity Connection*.

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

Step 1 In Cisco Unity Connection Administration, expand **System Settings > LDAP**, then click **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 Click **Save**.

Uploading SSL Certificates on the Connection Server

Added May 2009

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 Configurations and Synchronizing Data" section on page 43-7), or for authentication (see the "Configuring LDAP Authentication" section on page 43-5).

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 logons, if any.

If you 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, log on to Cisco Unified Operating System Administration.

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

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

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, click **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

Revised May 2009

If you want to use LDAP user names and passwords to authenticate logons to Cisco Unity Connection web applications or IMAP access to Connection voice messages, do the following procedure to configure LDAP authentication.

To Configure LDAP Authentication

Step 1 In Cisco Unity Connection Administration, expand **System Settings > LDAP**, and click **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, click **This Page**.

If you uploaded SSL certificates to the Connection server in the "To Upload SSL Certificates from the LDAP Directory Servers" procedure on page 43-5:

- 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 7.x*.

Step 4 Click **Save**.

Filtering LDAP Users

Added May 2009

Note This feature was added for Cisco Unity Connection 7.0(2).

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 the "set cuc ldapfilter" CLI command to provide additional control over user search bases. Note the following:

- The "set cuc ldapfilter" CLI command cannot be used with Cisco Unified Communications Manager Business Edition.
- You can only create one filter per Connection server or Connection cluster pair, so the LDAP filter must specify all of the users that you want to synchronize with Connection users.
- When you configure LDAP synchronization in Connection, you can further filter the LDAP users by your choice of user search bases.
- The filter must adhere to the LDAP filter syntax specified in RFC 2254, "The String Representation of LDAP Search Filters."

- The filter syntax is not verified, and no error message is returned. We recommend that you verify the LDAP filter syntax before you include it in this command.
- After you run this command, you must do the following steps for the LDAP users specified by the filter to be accessible to Connection:
  1. Deactivate and reactivate the Cisco DirSync service. In Cisco Unified Serviceability, click Tools > Service Activation. Uncheck the check box next to Cisco DirSync, and click Save to deactivate the service. Then check the check box next to Cisco DirSync, and click Save to reactivate the service.
  2. Perform a full synchronization in Connection Administration.
- If you re-run this command and specify a filter that excludes some of the users who were accessible with the previous filter, 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 log on 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 log on 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.

Adding LDAP Configurations and Synchronizing Data

Revised May 2010

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.

Note 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.

To Add an LDAP Configuration

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

Step 2 In the LDAP Configuration Name field, enter a name for this LDAP configuration. If you are adding several LDAP configurations 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, see the "LDAP Directory Configuration" section in the "System Settings" chapter of the *Interface Reference Guide for Cisco Unity Connection Administration Release 7.x*.

If you uploaded SSL certificates to the Connection server in the "To Upload SSL Certificates from the LDAP Directory Servers" procedure on page 43-5, 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 7.x*.

Step 4 Click **Save**.

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

When you have added the last LDAP configuration, continue with Step 6.

Step 6 Click **Perform Full Sync Now**.