LDAP Authentication Setup

This chapter provides information to configure LDAP directory, authentication, and custom filters using Cisco Unified Communications Manager. The LDAP directory configuration takes place in the following windows:

- LDAP System Configuration
- LDAP Directory
- LDAP Authentication
- LDAP Filter Configuration

You can make changes to LDAP directory information and LDAP authentication settings only if synchronization with the customer LDAP directory is enabled in the Cisco Unified Communications Manager Administration LDAP System Configuration window.

For additional information, see topics related to the directory, application users, and end users in the *Cisco Unified Communications Manager System Guide*.

About LDAP Authentication Setup

In Cisco Unified Communications Manager Administration, use the **System** > **LDAP** > **LDAP Authentication** menu path to configure LDAP authentication.

The authentication process verifies the identity of the user by validating the user ID and password/PIN before granting access to the system. Verification takes place against the Cisco Unified Communications Manager database or the LDAP corporate directory.

You can only configure LDAP authentication if you enable LDAP synchronization in the LDAP System Configuration window.

Note User accounts must be synchronized with Cisco Unified Communications Manager to use LDAP authentication. Administrators must enable LDAP synchronization and configure LDAP directory instance(s) to use the LDAP authentication mechanism.

When both synchronization and LDAP authentication are enabled, the system always authenticates application users and end user PINs against the Cisco Unified Communications Manager database. End user passwords get authenticated against the corporate directory; thus, end users need to use their corporate directory password.

When only synchronization is enabled (and LDAP authentication is not enabled), end users get authenticated against the Cisco Unified Communications Manager database. In this case, the administrator can configure a password in the End User Configuration window in Cisco Unified Communications Manager Administration.

Note When you are using the sAMAccountName value for the **LDAP Attribute for User ID** field, you can only authenticate with one LDAP Domain. To authenticate with multiple domains, you need to use the Active Directory Lightweight Directory Service (AD LDS).

Update LDAP Authentication

The setting of the Enable Synchronizing from LDAP Server check box in the LDAP System Configuration window affects your ability to modify LDAP authentication settings. If synchronization with the LDAP server is enabled, you cannot modify LDAP directory information and LDAP authentication settings. See topics related to understanding the directory in the Cisco Unified Communications Manager System Guide for more information about LDAP synchronization.

Conversely, if you want to enable administrators to modify LDAP directory information and LDAP authentication settings, you must disable synchronization with the LDAP server.

LDAP Authentication Settings

The following table describes the LDAP authentication settings.

Table 1: LDAP Authentication Settings

Field	Description
LDAP Authentication for End Users	
Use LDAP Authentication for End Users	Click this check box to require authentication of end users from the LDAP directory. If the check box is left unchecked, authentication gets performed against the database. **Note** You can only access this field if LDAP synchronization is enabled in the LDAP System Configuration window.
LDAP Manager Distinguished Name	Enter the user ID of the LDAP Manager who is an administrative user that has access rights to the LDAP directory in question. **Note** You can only access this field if LDAP authentication for end users is enabled.

Field	Description
LDAP Password	Enter a password for the LDAP Manager. **Note** You can only access this field if LDAP authentication for end users is enabled.
Confirm Password	Reenter the password that you provided in the LDAP Password field. **Note** You can only access this field if LDAP authentication for end users is enabled.
LDAP User Search Base	Enter the user search base. Cisco Unified Communications Manager searches for users under this base. **Note** You can only access this field if LDAP authentication for end users is enabled.
LDAP Server Information	
Host Name or IP Address for Server	Enter the host name or IP address where you installed the corporate directory. **Note** You can only access this field if LDAP authentication for end users is enabled.

Field	Description
LDAP Port	Enter the port number on which the corporate directory receives the LDAP requests. You can only access this field if LDAP authentication for end users is enabled. The default LDAP port for Microsoft Active Directory and for Netscape Directory specifies 389. The default LDAP port for Secured Sockets Layer (SSL) specifies 636. How your corporate directory is configured determines which port number to enter in this field. For example, before you configure the LDAP Port field, determine whether your LDAP server acts as a Global Catalog server and whether your configuration requires LDAP over SSL. Consider entering one of the following port numbers: LDAP port when LDAP server is not a Global Catalog server: • 389—When SSL is not required. (This port number specifies the default that displays in the LDAP Port field.) • 636—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) LDAP port when LDAP server is a Global Catalog server: • 3268—When SSL is not required. • 3269—When SSL is required. (If you enter this port number, make sure that you check the Use SSL check box.) **Tip** Your configuration may require that you enter a different port number than the options that are listed in the preceding bullets. Before you configure the LDAP Port field, contact the administrator of your directory server to determine the correct port number to enter.

Field	Description
Use SSL	Check this check box to use SSL encryption for security purposes. **Note** • If LDAP over SSL is required, the corporate directory SSL certificate must be loaded into Cisco Unified Communications Manager. The *Cisco Unified Communications Operating System Administration Guide* describes the certificate upload procedure. • You can do LDAP User Authentication using the IP address or the hostname. When IP address is used while configuring the LDAP Authentication, LDAP configuration needs to be made the IP address using the command `utils ldap config ipaddr`. When hostname is used while configuring the LDAP Authentication, DNS needs to be configured to resolve that LDAP hostname. If you check the Use SSL check box, enter the IP address or the hostname that exists in the corporate directory SSL certificate in the Host Name or IP Address for Server field in the LDAP Authentication Configuration window. If the certificate contains an IP address, enter the IP address. If the certificate contains the hostname, enter the hostname. If you do not enter the IP address or hostname exactly as it exists in the certificate, problems may occur for some applications; for example, applications that use CTIManager.
Add Another Redundant LDAP Server	Click this button to add another row for entry of information about an additional server. **Note** You can only access this button if LDAP authentication for end users is enabled.