LDAP authentication compares user login information against the profile database on an LDAPv2-compliant directory server. After users are authenticated by the LDAP server, they are automatically logged in to Cisco Unified MeetingPlace as long as their LDAP user IDs also exist in Cisco Unified MeetingPlace. With LDAP authentication, the following restrictions apply:

- Cisco Unified MeetingPlace Web Conferencing supports only unencrypted LDAP, that is, queries to the LDAP server are in clear text.
- Users cannot log in with their Cisco Unified MeetingPlace passwords for their same LDAP user names.
- LDAP profiles are used for authentication; Cisco Unified MeetingPlace profiles are ignored.

Note: To authenticate Cisco Unified MeetingPlace Web Conferencing against the LDAP server, make sure that the LDAP server directory is designed to have all users in one container rather than broken into multiple containers (each representing a child OU).

See the following procedures:

- To Configure LDAP Authentication
- To Verify the LDAP Authentication Configuration by Using the Web Page Form
- To Verify the LDAP Authentication Configuration by Using the HTTP Form

See also:

- Troubleshooting Problems with LDAP Authentication

To Configure LDAP Authentication

If you are also using Cisco Unified MeetingPlace for Outlook, complete the Allowing Cisco Unified MeetingPlace for Outlook Authentication before beginning this procedure.

1. Sign in to Cisco Unified MeetingPlace Web Conferencing.
2. From the Welcome page, click **Admin** , then click **Web Server** .
3. From the "View" section of the page, click the name of the web server that you want to configure.
4. Scroll to the Web Authentication section.
5. For "Step 1: Directory," choose **LDAP** .
6. For "LDAP Hostname," enter the LDAP hostname, for example *ldap.domain.com* .
7. For "LDAP Distinguished Name (DN)," enter the DN information for your directory. Note the following considerations for properly configuring the DN:
    - Cisco Unified MeetingPlace user profile login names are limited to 17 characters; therefore, the LDAP match be 17 characters or less.

- You can only enter one value for the LDAP Distinguished Name (DN) field in the Web Conferencing directory configuration. If your users are segregated into multiple organizational units (OUs), you can work around this issue by using either the DOMAIN\USER or user@ou.domain.com format for the DN. When configuring the LDAP Distinguished Name field in Web Conferencing, enter just %USERNAME%, without specifying an OU, DC, or other parameter.
- Instead of entering %USERNAME%, leave the DN field blank if you are authenticating against a multiple LDAP forest configuration.
  Example
  CN= *%USERNAME%* , OU=People, DC=mydomain, DC=com
- If the LDAP server that is being used is the LDAP interface on a Microsoft Active Directory server, leave the DN field blank (empty) for authentication to work. When configured in this manner, the format of the usernames that the user enters must be DOMAIN\USER or user@ou.domain.com.
- *%USERNAME%* is the username that the user enters when logging in.
- Before sending the request to the LDAP server *%USERNAME%* is replaced with the username that the user enters in the login username field. No additional modifications are made to the DN value.
- *%USERNAME%* is case-sensitive, that is, all upper case.
- Consult your LDAP expert for your DN information.

8. For "Step 2: Login Method," choose one of the following:
   - To see an HTML-based Cisco Unified MeetingPlace login window, choose **Web Page Form** .
   - To see a login window rendered by your web browser, choose **HTTP Basic Authentication** .
     Note: If you choose HTTP Basic Authentication, users cannot log in to Cisco Unified MeetingPlace as guests.
9. Click **Submit** and wait five minutes for the new configuration to take effect.
10. (Optional) If you chose Web Page Form and want to verify your configuration, continue with the To Verify the LDAP Authentication Configuration by Using the Web Page Form.
11. (Optional) If you chose HTTP Basic Authentication and want to verify your configuration, continue with the To Verify the LDAP Authentication Configuration by Using the HTTP Form.

To Verify the LDAP Authentication Configuration by Using the Web Page Form

Use a Cisco Unified MeetingPlace end user profile when completing this procedure.

1. Open a web browser and navigate to Cisco Unified MeetingPlace Web Conferencing.
2. Verify the following end-user behaviors:
   - If you have a Cisco Unified MeetingPlace profile, you can log in with your LDAP password.
   - You cannot log in as a profile user without a password.

To Verify the LDAP Authentication Configuration by Using the HTTP Form

Use a Cisco Unified MeetingPlace end user profile when completing this procedure.

1. Open a web browser and navigate to Cisco Unified MeetingPlace Web Conferencing.
2. Verify the following end-user behaviors:

- When you access the Cisco Unified MeetingPlace home page, you see an Enter Network Password window.
- After you enter your LDAP profile user ID and password, you are authenticated to the Audio Server.
- The Welcome page displays your name in firstname, lastname order.
- Sign In and Sign Out links do not display.