This authentication mode attempts to authenticate users against two directories if the need arises. When users first log in, they are authenticated against the LDAP directory. If this authentication fails, the login information is sent to the Cisco Unified MeetingPlace Audio Server for a possible match. This behavior allows a company to give non-LDAP users, such as guests or contractors, access to Cisco Unified MeetingPlace.

Before configuring this authentication mode, keep the following points in mind:

- 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).
- If a match is made in the LDAP database, the user must provide the proper LDAP password. Three attempts with the incorrect password will lock the LDAP profile of the user.
- Only users who are not found in the LDAP directory are eligible for authentication through the Cisco Unified MeetingPlace directory.
- User IDs in the Cisco Unified MeetingPlace profile database are case sensitive.

See the following procedures:

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

See also:

- Troubleshooting Problems with LDAP Authentication

#### To Configure the LDAP Then MeetingPlace 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, then MeetingPlace** .
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:** All users in the LDAP server directory must be in one container rather than broken into multiple containers each representing a child OU.
**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 types 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 want to verify your Web Page Form configuration, continue with the To Verify the LDAP Then MeetingPlace Authentication Configuration by Using the Web Page Form.
11. (Optional) If you want to verify you HTTP form configuration, continue with the To Verify the LDAP Then MeetingPlace Authentication Configuration by Using the HTTP Form.

#### To Verify the LDAP Then MeetingPlace 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:
   - You can log in with your LDAP password.
   - You cannot log in without a password.
   - If you have a Cisco Unified MeetingPlace profile, you can log in and schedule meetings.
   - If you do not have a Cisco Unified MeetingPlace profile, you can only attend and search public meetings.

#### To Verify the LDAP Then MeetingPlace 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:
   - You can log in with your LDAP password.
   - You cannot log in without a password.
   - If you have a Cisco Unified MeetingPlace profile, you can log in and schedule meetings.

- This option does not allow you to log in to Cisco Unified MeetingPlace as a guest, that is, without a Cisco Unified MeetingPlace profile.