Set up LDAP login and user roles in Content Hubs

Content updated: 05/26/2020

This article is designated for administrators.

About

This article explains how to connect your Content Hubs or legacy Video Portal to your organization's **LDAP** or **Active Directory** (AD) server.

This lets users log in with their existing organizational credentials and (optionally) assigns legacy Video Portal roles based on LDAP groups.

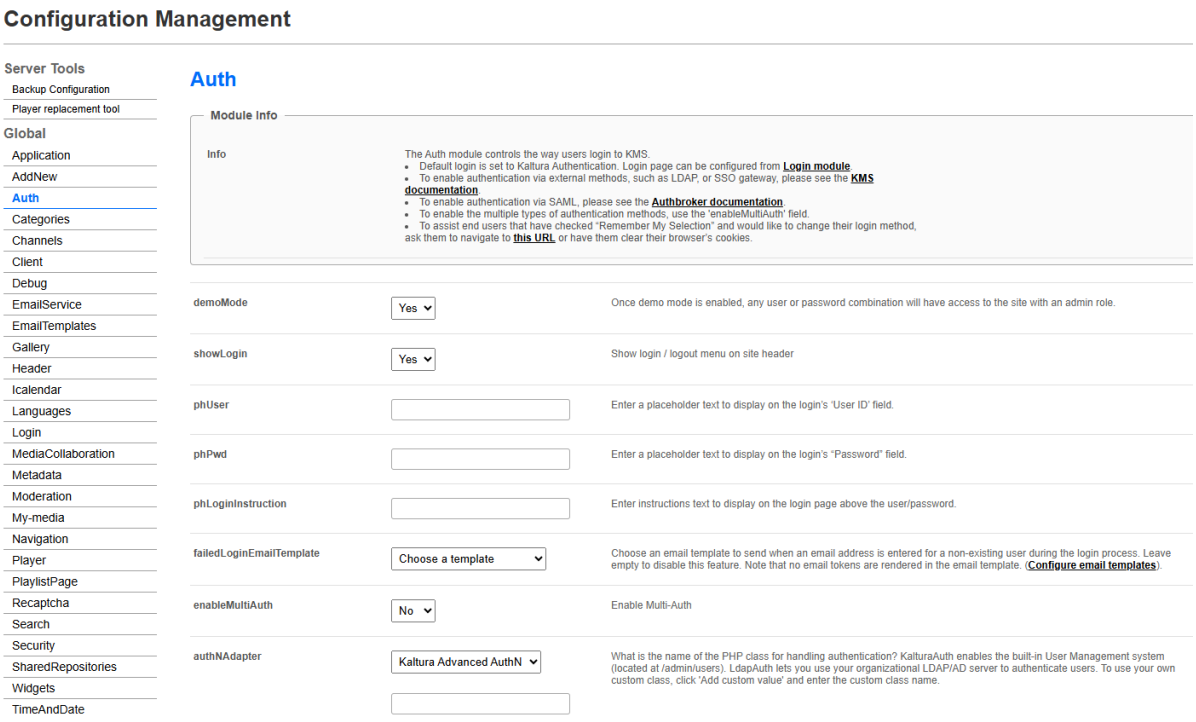
If you're deciding which method to use, see Authentication and authorization options in Content Hubs.

Set up LDAP login

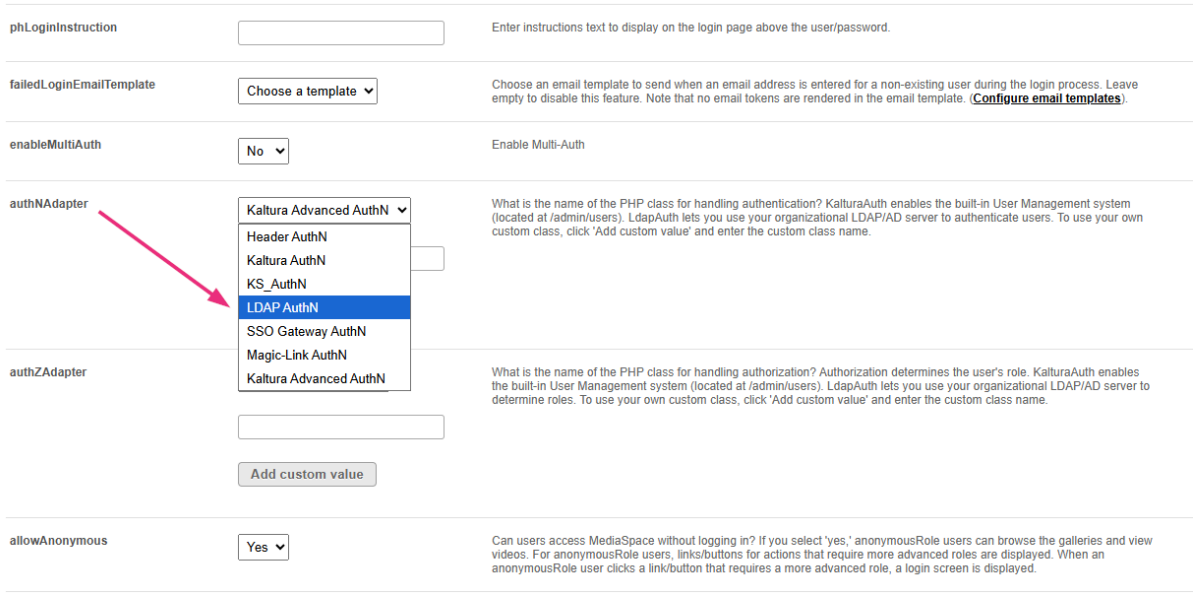
1. Go to your **Configuration Management** console, locate the **Auth module** in the left panel, then select it. You can also navigate directly: `https://{your_site_URL}/admin/config/tab/auth`.

The Auth page displays.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.



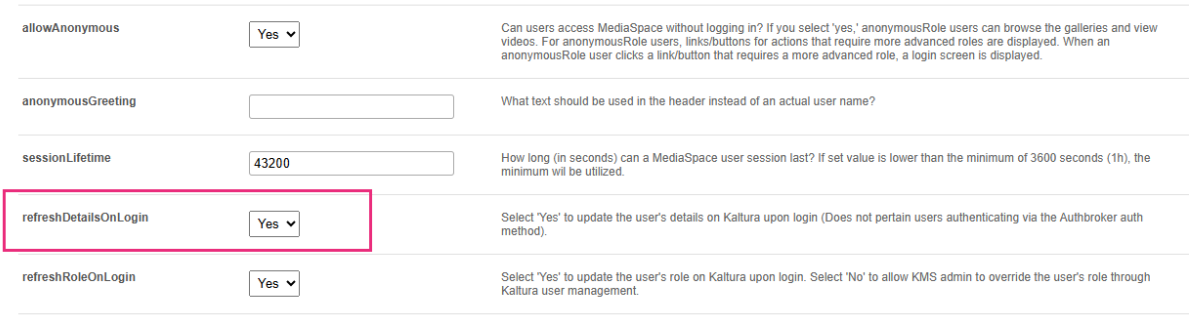
2. Scroll down to the **authNAdapter** field and select **LDAP AuthN** from the drop-down menu. This enables LDAP as the login method.



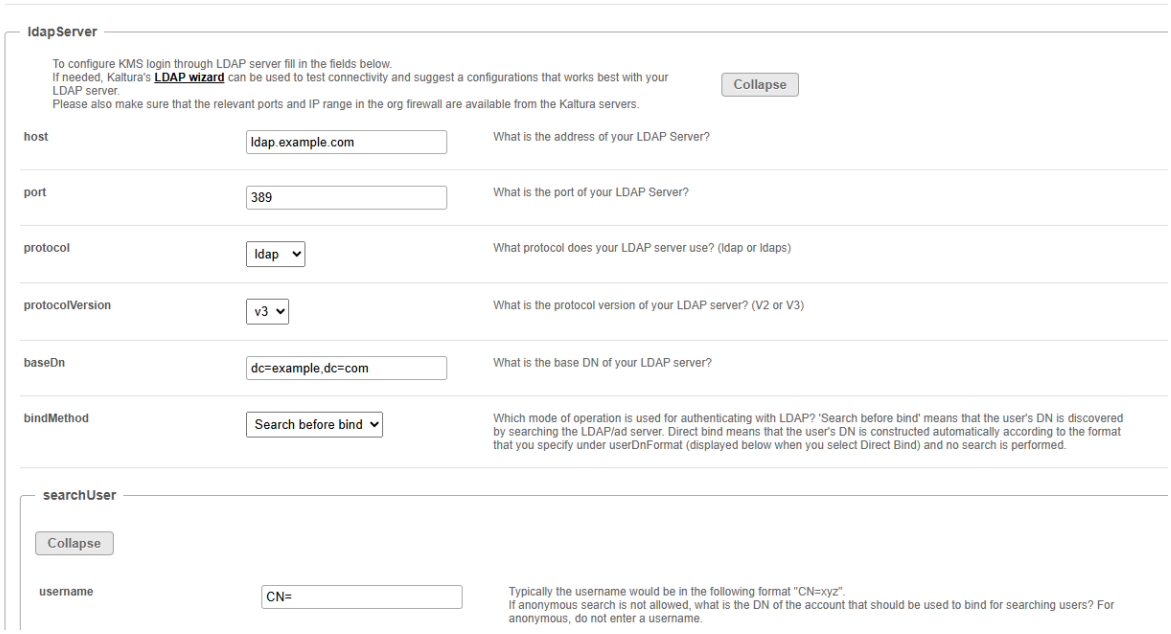
3. Scroll down to **refreshDetailsOnLogin**, select whether user details should be updated from LDAP every time the user logs in.

- **Yes** – Sync first name, last name, and email from LDAP
- **No** – Keep the details already stored in Kaltura

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.



4. Scroll to the **ldapServer** section. These settings define how the site connects to your LDAP/AD environment.



5. Enter the connection information for your LDAP or AD server:

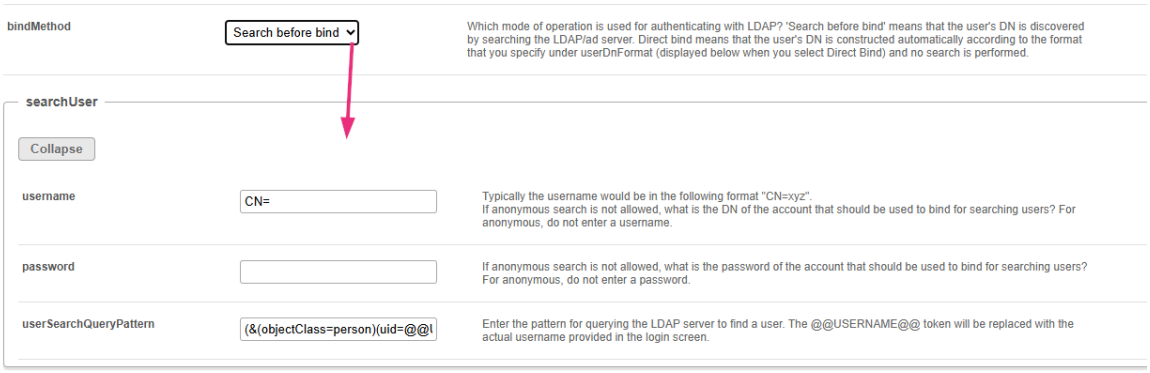
- **host** – Your LDAP/AD server address
- **port** – Usually 389 (LDAP) or 636 (LDAPS)
- **protocol** – ldap or ldaps
- **protocolVersion** – Usually v3
- **baseDn** – The base DN where user records are stored
- **bindmethod** (see below)

6. Choose your bind method:

Search before bind (default)

Use this option when the site needs to search your LDAP server to find the user's DN before attempting to authenticate them. When this method is selected, you'll see the following **searchUser** section.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.



username - Enter the full path of the LDAP account the site should use to search for users. The field starts with **CN=** as a placeholder. Replace it with the full value your LDAP team uses for this account.

Example: `CN=SearchUser,OU=Accounts,DC=example,DC=com`

If your LDAP server allows anonymous search, leave this field empty.

password - Enter the password for the account listed in the username field.

If your LDAP server allows anonymous searches, leave this field empty.

userSearchQueryPattern - Enter the LDAP search filter your site should use to find the user record. The token `@@USERNAME@@` is replaced automatically with the username the user enters at login.

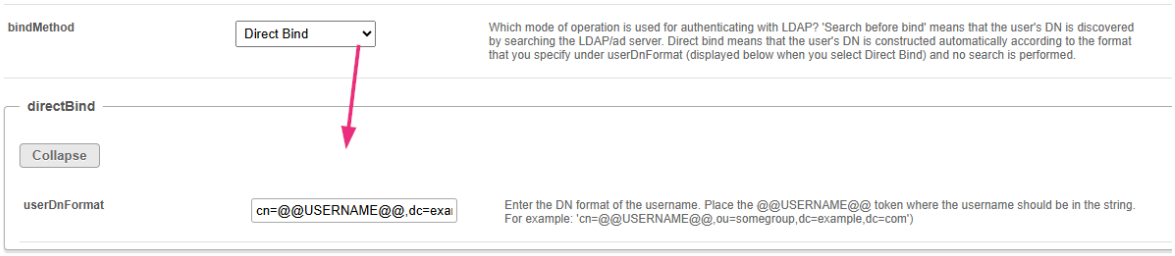
Example default: `(&(objectClass=person)(uid=@@USERNAME@@))`

If your directory uses a different attribute for usernames (such as sAMAccountName or mail), update this filter accordingly.

Direct bind

If you choose Direct bind, your site does not search LDAP for the user. Instead, it builds the user's full LDAP path using a format you provide, then tries to log in with the username and password the user enters.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.



When this method is selected, complete the following:

userDnFormat - Enter the full path format of your users in LDAP. Use the token `@@USERNAME@@` where the username should appear. Example: `cn=@@USERNAME@@,dc=example,dc=com`

When someone logs in, the legacy Video Portal replaces `@@USERNAME@@` with the name they typed. It uses the resulting full path to authenticate the user. If your organization stores users in different OUs, make sure the format you enter matches exactly where the accounts live.

7. Configure optional user-attribute fields:

emailAttribute – Enter the LDAP attribute that contains the user's email address. Leave this empty if you don't want email synced to Kaltura.

firstNameAttribute – Enter the LDAP attribute that contains the user's first name. Leave empty if you don't want to sync first names.

lastNameAttribute – Enter the LDAP attribute that contains the user's last name. Leave empty if you don't want to sync last names.

tlsCipherSuite (advanced) - This field is for advanced environments that require a specific TLS cipher for LDAP connections. Use only if required by your IT/security team.

8. Click **Save** to save your changes

If you only need LDAP login, you are done. If you want your site to assign user roles based on LDAP groups, complete the next section.

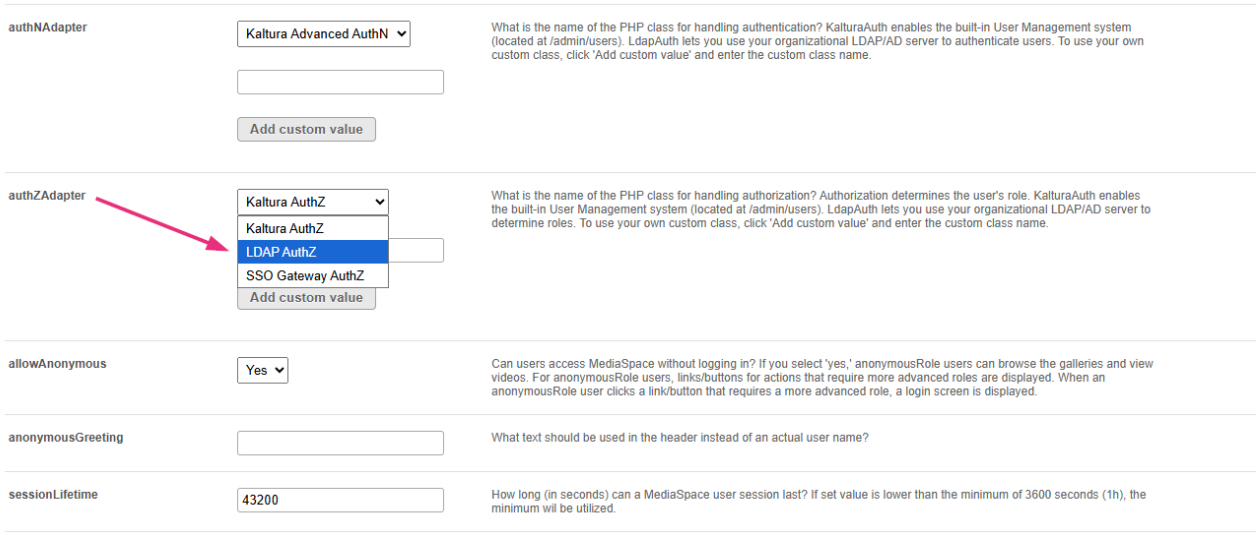
Set up LDAP user roles (optional)

This step lets you assign roles (viewer, contributor, admin, etc.) using LDAP group membership.

Select LDAP for authorization

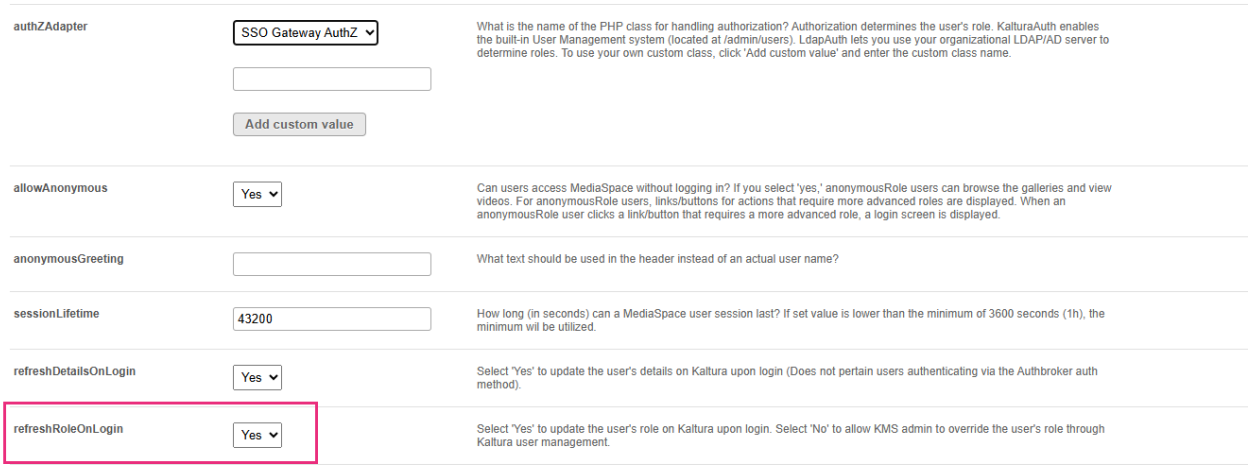
1. In the Auth module, find the **authZAdapter** field and select **LDap AuthZ** from the drop-down menu.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.



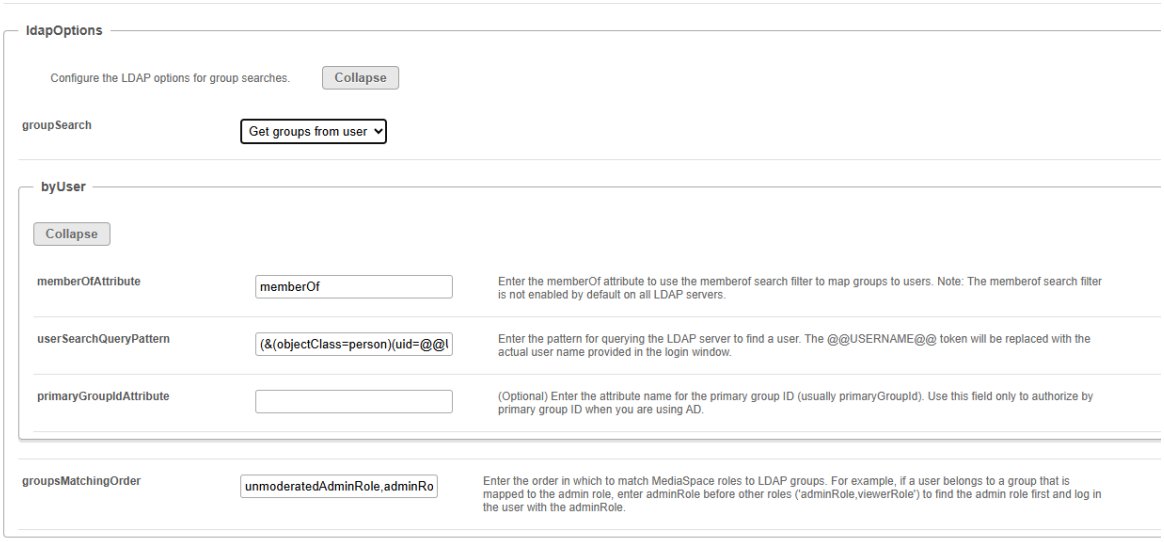
2. Under **refreshRoleOnLogin**, choose whether to update a user's role from your authentication system each time they log in.

- 'Yes' – Always update the user's role using LDAP groups
- 'No' – Keep the existing role stored in Kaltura



3. Scroll to the **ldapOptions** section.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

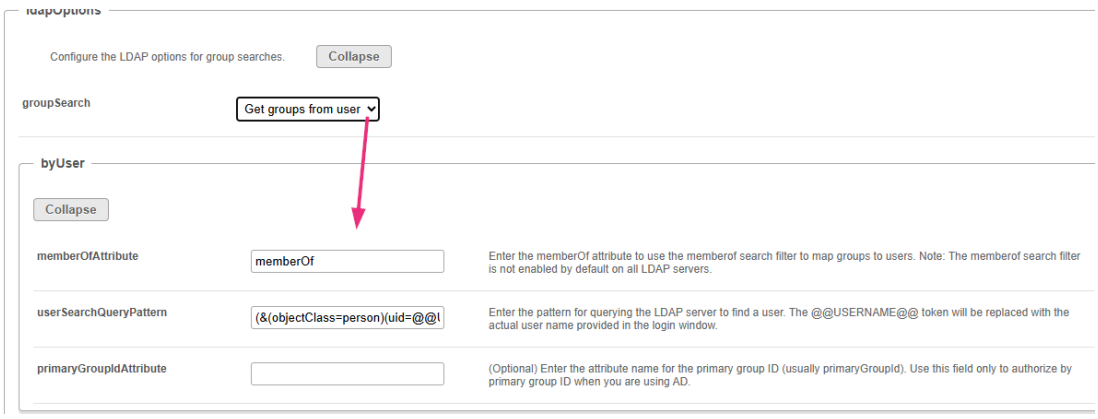


4. Configure the following:

groupsearch - Choose an option from the drop-down menu:

Get groups from user

(recommended for AD) This option reads the user's LDAP record and uses the **memberOf** attribute to find their groups.



When you select **Get groups from user**, a subsection called **byUser** appears. Configure these fields:

memberOfAttribute – Enter the LDAP attribute that lists a user's groups. Default: memberOf

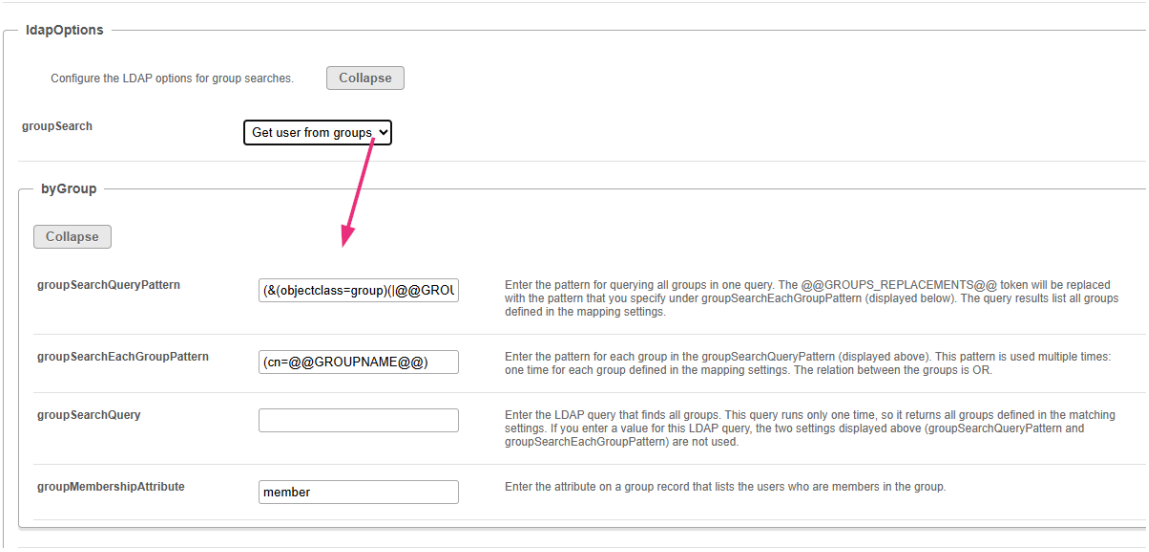
userSearchQueryPattern – The LDAP query used to retrieve the user record. The `@@USERNAME@@` token is replaced automatically with the username entered at login.

primaryGroupIdAttribute (optional) – Used only when working with AD and you want to authorize based on an AD primary group ID.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

Get users from groups

Choose this option when your LDAP or AD server does not support the 'memberOf' attribute, or when your group structure requires checking each group’s membership list.



When you select this option, a **byGroup** section appears. Configure the following fields:

groupSearchQueryPattern - Enter the LDAP query pattern that retrieves all relevant groups in one search. The @@GROUPS_REPLACEMENTS@@ token is replaced with individual group filters defined under groupSearchEachGroupPattern. This query runs once for all groups.

groupSearchEachGroupPattern - Enter the pattern for identifying each group. This pattern runs once per group configured in your role-mapping settings. Example: (cn=@@GROUPNAME@@)

@@GROUPNAME@@ is replaced with the CN of each group you mapped under **ldapGroups**.

groupSearchQuery (optional) - Enter a complete LDAP query that returns all groups in a single search. If you fill in this field, it overrides both: groupSearchQueryPattern and groupSearchEachGroupPattern. Use this only if your LDAP team provides a single, complete query.

groupMembershipAttribute - Enter the attribute on each group object that lists its members, for example: *member*. This is where LDAP stores the DNs of users who belong to that group.

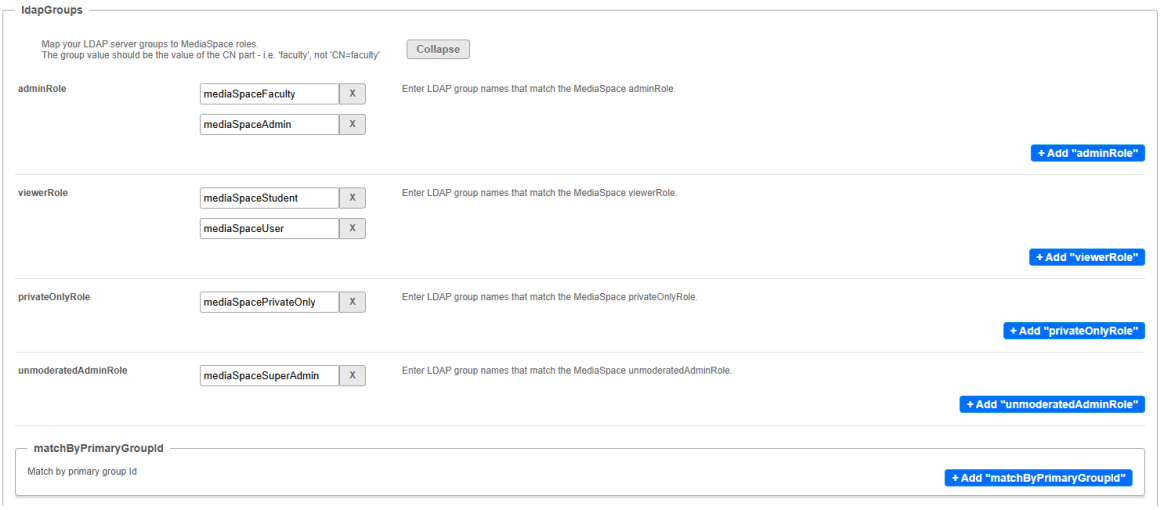
Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

groupsMatchingOrder - Enter the order in which the site should match LDAP groups to roles.

The field is small, but it accepts long values. To avoid typos, prepare the list in a text editor and then paste it into the field exactly as shown (comma-separated, no spaces).

Map LDAP groups to legacy Video Portal roles

Scroll to the **ldapGroups** section. Here, you'll map the LDAP groups from your directory to the legacy Video Portal's application roles. This determines which users become admins, viewers, contributors, and other roles.



How to enter group names

- Enter only the group name (the CN value), for example: *faculty*
- You can add multiple LDAP groups to each role
- The role assigned at login follows your groupsMatchingOrder setting

Configure the following role fields:

adminRole - Click **+ Add "adminRole"** to enter the LDAP group names that should map to the admin role, for example:

- *mediaSpaceFaculty*
- *mediaSpaceAdmin*

Users who belong to any of these groups are treated as administrators (unless another

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

role takes priority based on the matching order).

viewerRole - This is the most common role for general users. Click **+ Add "viewerRole"** to enter the LDAP groups that should map to the viewer role, for example:

- *mediaSpaceStudent*
- *mediaSpaceUser*

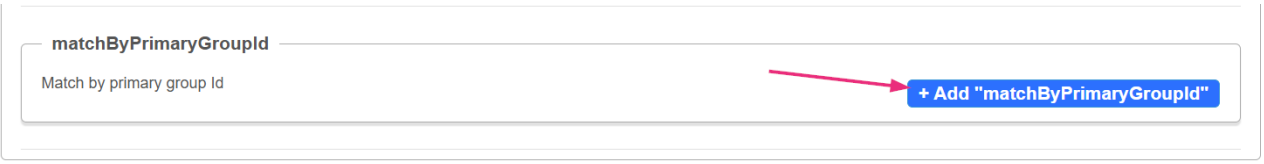
privateOnlyRole - Users with this role can only view content they own or content shared directly with them. Click **+ Add "privateOnlyRole"** to enter the groups that should map to private only role, for example: *mediaSpacePrivateOnly*

unmoderatedAdminRole - This role grants full administrative access without moderation restrictions. Click **+ Add "unmoderatedAdminRole"** to enter the groups that should map to the unmoderated admin role, for example: *mediaSpaceSuperAdmin.*

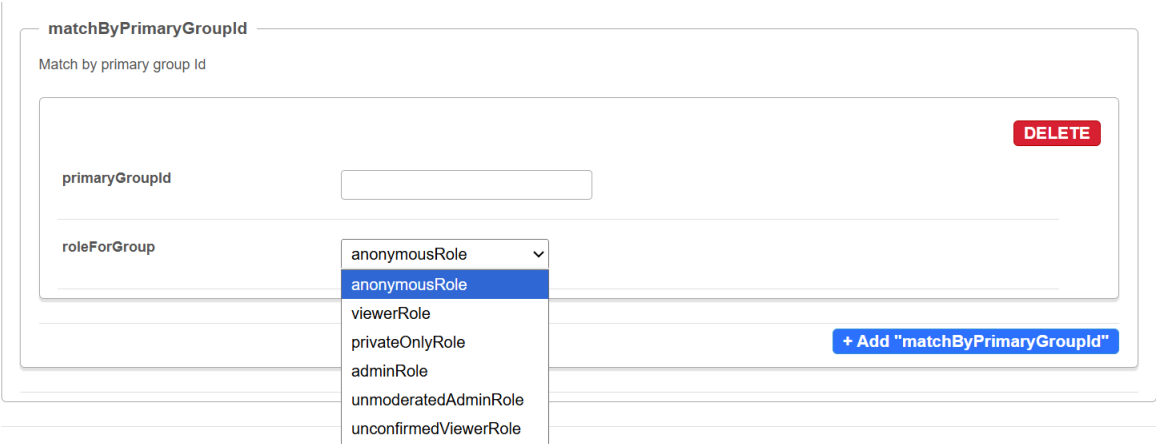
matchByPrimaryGroupId (optional) - Use this only in AD environments that rely on `primaryGroupId` instead of normal group membership.

To configure:

1. Click **+Add "matchByPrimaryGroupId"**.



A new section opens.



2. Enter the **primary group ID** value to match.

3. From the **roleForGroup** drop-down menu, choose the legacy Video Portal role to

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

assign to users with this primary group ID.

This option is typically used only in older or highly customized AD environments. Most environments do not need this field.

4. Click **Save** to save your changes.

Copyright © 2025 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners. Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.