

# Set up LDAP login and user roles in Video Portal

Last Modified on 11/13/2025 7:48 pm IST

 This article is designated for administrators.

## About

This article explains how to connect your 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 Video Portal roles based on LDAP groups.

All LDAP settings are configured in the [Auth module](#) of the Configuration Management console.



If you're deciding which method to use, see [Video Portal authentication and authorization options](#).

## Set up LDAP login

1. Go to your Configuration Management console, and navigate to the **Auth** module. You can also navigate directly: `https://{your_KMS_URL}/admin/config/tab/auth`.

### Global

Application

AddNew

**Auth** 

Categories

Channels

The Auth page displays.

## Configuration Management

### Server Tools

Backup Configuration  
Player replacement tool

### Global

Application  
AddNew

### Auth

### Categories

### Channels

### Client

### Debug

### EmailService

### EmailTemplates

### Gallery

### Header

### Icalendar

### Languages

### Login

### MediaCollaboration

### Metadata

### Moderation

### My-media

### Navigation

### Player

### PlaylistPage

### Recaptcha

### Search

### Security

### SharedRepositories

### Widgets

### TimeAndDate

## Auth

### Module Info

#### Info

The Auth module controls the way users login to KMS.

- Default login is set to Kaltura Authentication. Login page can be configured from [Login module](#).
- To enable authentication via external methods, such as LDAP, or SSO gateway, please see the [KMS documentation](#).
- To enable authentication via SAML, please see the [Authbroker documentation](#).
- To enable the multiple types of authentication methods, use the 'enableMultiAuth' field.
- To assist end users that have checked "Remember My Selection" and would like to change their login method, ask them to navigate to [this URL](#), or have them clear their browser's cookies.

demoMode	<input type="button" value="Yes"/>	Once demo mode is enabled, any user or password combination will have access to the site with an admin role.
showLogin	<input type="button" value="Yes"/>	Show login / logout menu on site header
phUser	<input type="text"/>	Enter a placeholder text to display on the login's 'User ID' field.
phPwd	<input type="text"/>	Enter a placeholder text to display on the login's 'Password' field.
phLoginInstruction	<input type="text"/>	Enter instructions text to display on the login page above the user/password.
failedLoginEmailTemplate	<input type="button" value="Choose a template"/>	Choose an email template to send when an email address is entered for a non-existing user during the login process. Leave empty to disable this feature. Note that no email tokens are rendered in the email template. ( <a href="#">Configure email templates</a> ).
enableMultiAuth	<input type="button" value="No"/>	Enable Multi-Auth
authNAdapter	<input type="button" value="Kaltura Advanced AuthN"/>	What is the name of the PHP class for handling authentication? KalturaAuth enables the built-in User Management system (located at /admin/users). LdapAuth lets you use your organizational LDAP/AD server to authenticate users. To use your own custom class, click 'Add custom value' and enter the custom class name.

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

phLoginInstruction	<input type="text"/>	Enter instructions text to display on the login page above the user/password.
failedLoginEmailTemplate	<input type="button" value="Choose a template"/>	Choose an email template to send when an email address is entered for a non-existing user during the login process. Leave empty to disable this feature. Note that no email tokens are rendered in the email template. ( <a href="#">Configure email templates</a> ).
enableMultiAuth	<input type="button" value="No"/>	Enable Multi-Auth
authNAdapter	<div> <input type="button" value="Kaltura Advanced AuthN"/> <div> Header AuthN Kaltura AuthN KS_AuthN <b>LDAP AuthN</b> SSO Gateway AuthN Magic-Link AuthN Kaltura Advanced AuthN </div> </div>	What is the name of the PHP class for handling authentication? KalturaAuth enables the built-in User Management system (located at /admin/users). LdapAuth lets you use your organizational LDAP/AD server to authenticate users. To use your own custom class, click 'Add custom value' and enter the custom class name.
authZAdapter	<input type="text"/> <input type="button" value="Add custom value"/>	What is the name of the PHP class for handling authorization? Authorization determines the user's role. KalturaAuth enables the built-in User Management system (located at /admin/users). LdapAuth lets you use your organizational LDAP/AD server to determine roles. To use your own custom class, click 'Add custom value' and enter the custom class name.
allowAnonymous	<input type="button" value="Yes"/>	Can users access MediaSpace without logging in? If you select 'yes,' anonymousRole users can browse the galleries and view videos. For anonymousRole users, links/buttons for actions that require more advanced roles are displayed. When an anonymousRole user clicks a link/button that requires a more advanced role, a login screen is displayed.

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

allowAnonymous	Yes ▼	Can users access MediaSpace without logging in? If you select 'yes,' anonymousRole users can browse the galleries and view videos. For anonymousRole users, links/buttons for actions that require more advanced roles are displayed. When an anonymousRole user clicks a link/button that requires a more advanced role, a login screen is displayed.
anonymousGreeting		What text should be used in the header instead of an actual user name?
sessionLifetime	43200	How long (in seconds) can a MediaSpace user session last? If set value is lower than the minimum of 3600 seconds (1h), the minimum will be utilized.
refreshDetailsOnLogin	Yes ▼	Select 'Yes' to update the user's details on Kaltura upon login (Does not pertain users authenticating via the Authbroker auth method).
refreshRoleOnLogin	Yes ▼	Select 'Yes' to update the user's role on Kaltura upon login. Select 'No' to allow KMS admin to override the user's role through Kaltura user management.

4. Scroll to the **IdapServer** section. These settings define how the Video Portal connects to your LDAP/AD environment.

**IdapServer**

To configure KMS login through LDAP server fill in the fields below.  
If needed, Kaltura's **LDAP wizard** can be used to test connectivity and suggest a configurations that works best with your LDAP server.  
Please also make sure that the relevant ports and IP range in the org firewall are available from the Kaltura servers.

Collapse

host	ldap.example.com	What is the address of your LDAP Server?
port	389	What is the port of your LDAP Server?
protocol	ldap ▼	What protocol does your LDAP server use? (ldap or ldaps)
protocolVersion	v3 ▼	What is the protocol version of your LDAP server? (V2 or V3)
baseDn	dc=example,dc=com	What is the base DN of your LDAP server?
bindMethod	Search before bind ▼	Which mode of operation is used for authenticating with LDAP? 'Search before bind' means that the user's DN is discovered by searching the LDAP/ad server. Direct bind means that the user's DN is constructed automatically according to the format that you specify under userDnFormat (displayed below when you select Direct Bind) and no search is performed.

**searchUser**

Collapse

username	CN=	Typically the username would be in the following format "CN=xyz". If anonymous search is not allowed, what is the DN of the account that should be used to bind for searching users? For anonymous, do not enter a username.
----------	-----	---

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 Video Portal 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.

bindMethod

Search before bind

Which mode of operation is used for authenticating with LDAP? 'Search before bind' means that the user's DN is discovered by searching the LDAP/ad server. Direct bind means that the user's DN is constructed automatically according to the format that you specify under userDnFormat (displayed below when you select Direct Bind) and no search is performed.

searchUser

Collapse

username

CN=

Typically the username would be in the following format "CN=xyz". If anonymous search is not allowed, what is the DN of the account that should be used to bind for searching users? For anonymous, do not enter a username.

password

If anonymous search is not allowed, what is the password of the account that should be used to bind for searching users? For anonymous, do not enter a password.

userSearchQueryPattern

(&(objectClass=person)(uid=@@!))

Enter the pattern for querying the LDAP server to find a user. The @@USERNAME@@ token will be replaced with the actual username provided in the login screen.

**username** - Enter the full path of the LDAP account the Video Portal 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 the Video Portal should use to find the user record. The token **@@USERNAME@@** is replaced automatically with the username the user enters at login.

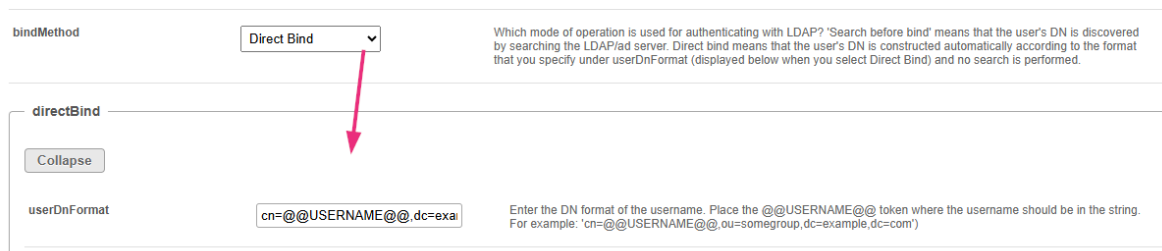
Example default: (&(objectClass=person)(uid=@@USERNAME@@))



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, the Video Portal 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.



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 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 the Video Portal to assign user roles based on LDAP groups, complete the next section.

## Set up LDAP user roles (optional)

This step lets you assign Video Portal 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.

authNAdapter	Kaltura Advanced AuthN	What is the name of the PHP class for handling authentication? KalturaAuth enables the built-in User Management system (located at /admin/users). LdapAuth lets you use your organizational LDAP/AD server to authenticate users. To use your own custom class, click 'Add custom value' and enter the custom class name.
	Add custom value	
authZAdapter	<div> <div>Kaltura AuthZ</div> <div>Kaltura AuthZ</div> <div>LDAP AuthZ</div> <div>SSO Gateway AuthZ</div> <div>Add custom value</div> </div>	What is the name of the PHP class for handling authorization? Authorization determines the user's role. KalturaAuth enables the built-in User Management system (located at /admin/users). LdapAuth lets you use your organizational LDAP/AD server to determine roles. To use your own custom class, click 'Add custom value' and enter the custom class name.
allowAnonymous	Yes	Can users access MediaSpace without logging in? If you select 'yes,' anonymousRole users can browse the galleries and view videos. For anonymousRole users, links/buttons for actions that require more advanced roles are displayed. When an anonymousRole user clicks a link/button that requires a more advanced role, a login screen is displayed.
anonymousGreeting		What text should be used in the header instead of an actual user name?
sessionLifetime	43200	How long (in seconds) can a MediaSpace user session last? If set value is lower than the minimum of 3600 seconds (1h), the minimum will be utilized.

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

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

authZAdapter	SSO Gateway AuthZ	What is the name of the PHP class for handling authorization? Authorization determines the user's role. KalturaAuth enables the built-in User Management system (located at /admin/users). LdapAuth lets you use your organizational LDAP/AD server to determine roles. To use your own custom class, click 'Add custom value' and enter the custom class name.
	Add custom value	
allowAnonymous	Yes	Can users access MediaSpace without logging in? If you select 'yes,' anonymousRole users can browse the galleries and view videos. For anonymousRole users, links/buttons for actions that require more advanced roles are displayed. When an anonymousRole user clicks a link/button that requires a more advanced role, a login screen is displayed.
anonymousGreeting		What text should be used in the header instead of an actual user name?
sessionLifetime	43200	How long (in seconds) can a MediaSpace user session last? If set value is lower than the minimum of 3600 seconds (1h), the minimum will be utilized.
refreshDetailsOnLogin	Yes	Select 'Yes' to update the user's details on Kaltura upon login (Does not pertain users authenticating via the Authbroker auth method).
refreshRoleOnLogin	Yes	Select 'Yes' to update the user's role on Kaltura upon login. Select 'No' to allow KMS admin to override the user's role through Kaltura user management.

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

IdapOptions

Configure the LDAP options for group searches.

Collapse

groupSearch

Get groups from user

byUser

Collapse

memberOfAttribute

memberOf

Enter the memberOf attribute to use the memberof search filter to map groups to users. Note: The memberof search filter is not enabled by default on all LDAP servers.

userSearchQueryPattern

(&(objectClass=person)(uid=@@@))

Enter the pattern for querying the LDAP server to find a user. The @@@ token will be replaced with the actual user name provided in the login window.

primaryGroupIdAttribute

(Optional) Enter the attribute name for the primary group ID (usually primaryGroupid). Use this field only to authorize by primary group ID when you are using AD.

groupsMatchingOrder

unmoderatedAdminRole,adminRo

Enter the order in which to match MediaSpace roles to LDAP groups. For example, if a user belongs to a group that is mapped to the admin role, enter adminRole before other roles ('adminRole,viewerRole') to find the admin role first and log in the user with the adminRole.

#### 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.

IdapOptions

Configure the LDAP options for group searches.

Collapse

groupSearch

Get groups from user

byUser

Collapse

memberOfAttribute

memberOf

Enter the memberOf attribute to use the memberof search filter to map groups to users. Note: The memberof search filter is not enabled by default on all LDAP servers.

userSearchQueryPattern

(&(objectClass=person)(uid=@@@))

Enter the pattern for querying the LDAP server to find a user. The @@@ token will be replaced with the actual user name provided in the login window.

primaryGroupIdAttribute

(Optional) Enter the attribute name for the primary group ID (usually primaryGroupid). Use this field only to authorize by primary group ID when you are using AD.

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

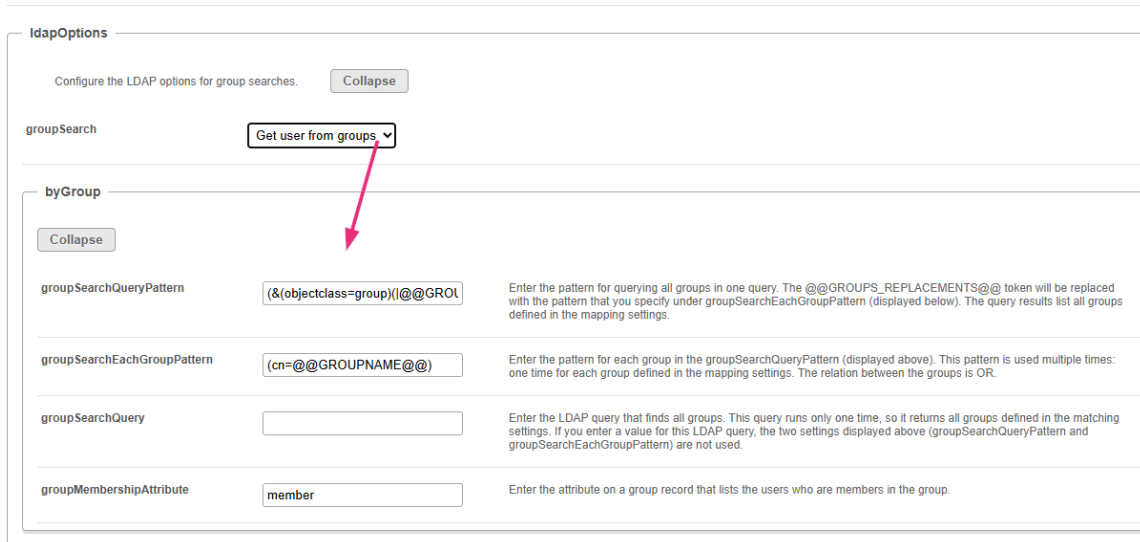
**memberOfAttribute** - Enter the LDAP attribute that lists a user's groups. Default: **memberOf**

**userSearchQueryPattern** - The LDAP query used to retrieve the user record. The **@@@** 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.

## 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.



**IdapOptions**

Configure the LDAP options for group searches. [Collapse](#)

**groupSearch** Get user from groups ▼

**byGroup** [Collapse](#)

**groupSearchQueryPattern**  Enter the pattern for querying all groups in one query. The @@GROUPS\_REPLACEMENTS@@ token will be replaced with the pattern that you specify under groupSearchEachGroupPattern (displayed below). The query results list all groups defined in the mapping settings.

**groupSearchEachGroupPattern**  Enter the pattern for each group in the groupSearchQueryPattern (displayed above). This pattern is used multiple times: one time for each group defined in the mapping settings. The relation between the groups is OR.

**groupSearchQuery**  Enter the LDAP query that finds all groups. This query runs only one time, so it returns all groups defined in the matching settings. If you enter a value for this LDAP query, the two settings displayed above (groupSearchQueryPattern and groupSearchEachGroupPattern) are not used.

**groupMembershipAttribute**  Enter the attribute on a group record that lists the users who are members in the group.

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 **IdapGroups**.

**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.



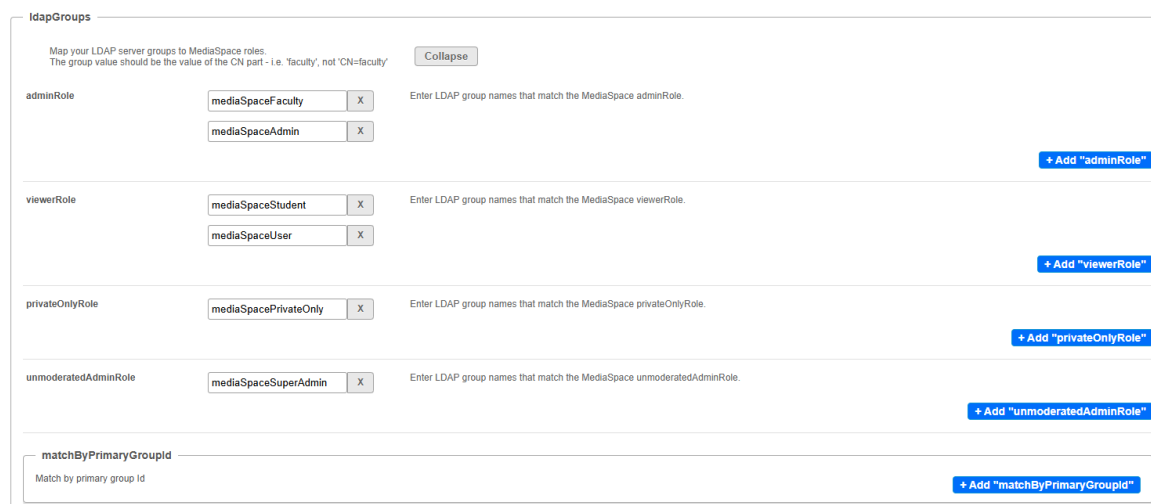
**groupsMatchingOrder** - Enter the order in which the Video Portal should match LDAP groups to Video Portal roles.



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 Video Portal roles

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



**ldapGroups**

Map your LDAP server groups to MediaSpace roles.  
The group value should be the value of the CN part - i.e. 'faculty', not 'CN=faculty'

**adminRole**    Enter LDAP group names that match the MediaSpace adminRole.

**viewerRole**     Enter LDAP group names that match the MediaSpace viewerRole.

**privateOnlyRole**    Enter LDAP group names that match the MediaSpace privateOnlyRole.

**unmoderatedAdminRole**    Enter LDAP group names that match the MediaSpace unmoderatedAdminRole.

**matchByPrimaryGroupid**



### 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 Video Portal admin role, for example:

- *mediaSpaceFaculty*
- *mediaSpaceAdmin*

Users who belong to any of these groups are treated as Video Portal administrators

(unless another 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*

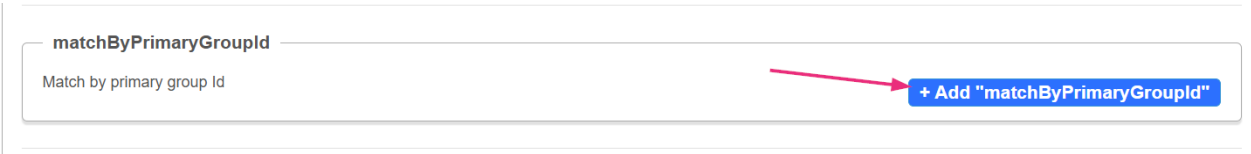
**privateOnlyRole** - Users with this role can only view content they own or content shared directly with them. Click **+ Add** "**privateOnlyRole**" to enter the groups that should map to private only role, for example: *mediaSpacePrivateOnly*

**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*.

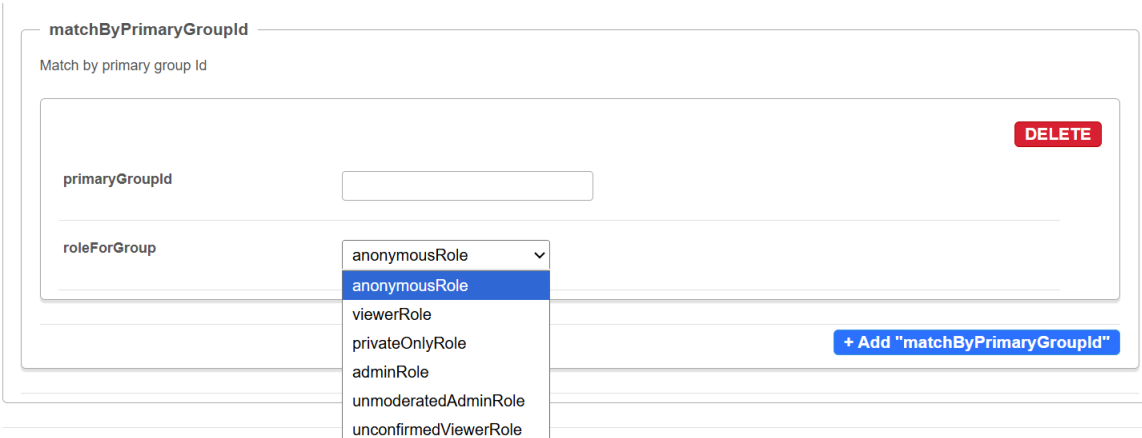
**matchByPrimaryGroupId** (optional) - Use this only in AD environments that rely on `primaryGroupId` instead of normal group membership.

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 Video Portal role to 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.

---