

## Auth module

Last Modified on 06/17/2024 3:25 pm IDT

 This article is designated for administrators.

### About

The Auth module manages user logins for the video portal. By default, it uses Kaltura Authentication. Please note:

- To switch to SAML authentication, check out the SAML module.
- For multiple authentication methods, use the 'enableMultiAuth' setting.
- To help users change their login method after selecting "Remember My Selection," they can visit: <https://<partnerId>.mediaspace.kaltura.com/user/clear-login-selection> or clear their browser cookies."

### Authbroker

AuthBroker is a "gateway" that sits on the partner (account) level and manages authentication to Kaltura via external Identity providers (IdP). AuthBroker works with the Security Assertion Markup Language (SAML) and Open Authorization (OAuth 2.0) protocols. AuthBroker users are "shared users" (users who are shared between applications / instances in the partner).

AuthBroker works with a higher version of SAML and you no longer need to set up a new profile for each new account. You can set up profile(s) just once and easily use them in multiple applications/instances.

### Configure

Go to your Configuration Management console, and navigate to the **Auth** module. Your link should look like this: [https://{your\\_KMS\\_URL}/admin/config/tab/auth](https://{your_KMS_URL}/admin/config/tab/auth).

#### Global

Application

AddNew

**Auth** 

Categories

Channels

In the Auth module window, configure the following:

**demoMode** - Set to 'Yes' if you want to enable the demo login mode. After entering any user or password combination, the user has an admin role.

**showLogin** - Set to 'Yes' if you want to show login / logout menu on site header.

**phUser** - user ID alternate field placeholder

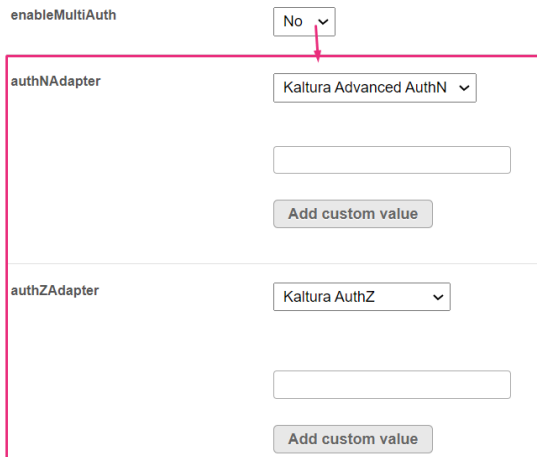
**phPwd** - password alternate field placeholder

**phLoginInstruction** - login instructions


enableMultiAuth

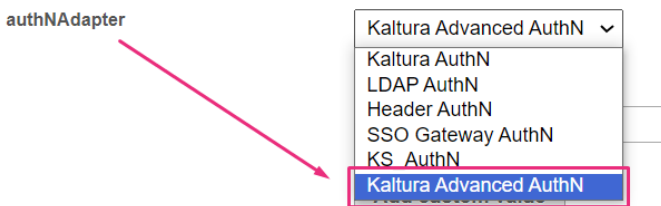
### enableMultiAuth set to 'No'

**enableMultiAuth** - Enable Multi-Authentication Methods configuration. If you leave the setting on 'No', complete the authNAdapter and authZAdapter fields below. If you select 'Yes', [skip to the next section](#).



**authNAdapter** - What is the name of the PHP class for handling authentication? KalturaAuth enables the built-in User Management system (located at /admin/users).

 When [Theming](#) is enabled, authNAdapter should be set to Kaltura Advanced AuthN.



LdapAuth lets you use your organizational LDAP/AD server to authenticate users. To

use your own custom class, enter the custom class name, then click 'Add custom value'.

authNAdapter

The value is added to the menu.

authNAdapter

- Kaltura AuthN
- LDAP AuthN
- Header AuthN
- SSO Gateway AuthN
- KS\_AuthN
- Kaltura Advanced AuthN
- Example**

**authZAdapter** - 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, enter the custom class name, then click 'Add custom value'.

authZAdapter

The value is added to the menu.

authZAdapter

- Kaltura AuthZ
- LDAP AuthZ
- SSO Gateway AuthZ
- Example**

### **enableMultiAuth set to 'Yes'**

**enableMultiAuth** - If you select 'Yes', a new section displays with **multiAuthWelcome** and **multiAuthselect** fields, and a section for each

authentication method you choose to configure.

enableMultiAuth	<input type="text" value="Yes"/>	Enable Multi-Auth
multiAuthWelcome	<input type="text" value="Welcome to MediaSpace"/>	welcome text to show on login selection page
multiAuthSelect	<input type="text" value="Please choose one of the login op"/>	text to show on login selection page
authMethods	Select authentication methods <span style="float: right;">+ Add "authMethods"</span>	

**multiAuthWelcome** - Enter welcome text to show on login selection page.

**multiAuthSelect** - Enter the text to show on login selection page.

### authMethods

Click **+Add "authMethods"**.

A new section displays.

**authMethods**

Select authentication methods

\* DELETE

<b>method</b>	<input type="text" value="Kaltura AuthN"/>	authentication method
<b>friendlyName</b>	<input type="text"/>	text to show the user on the login selection page, leave empty to use default
<b>helpText</b>	<input type="text"/>	Fill in explanation text on the auth method in the Login Selection page. The text will show in a tool tip for users in a question mark. Leave empty to hide the tool tip.
<b>authSlug</b>	<input type="text"/>	Fill in the URL ending to allow a direct link for users to login via this auth method. The new URL will be <code>https://4834032.mediaspace.kaltura.com/auth/SLUG</code> . Note: Only alphanumeric characters are allowed.

**method** - Choose an authentication method from the drop-down menu.

**friendlyName** - Enter the text to show the user on the login selection page, leave empty to use default.

**helpText** - Enter the text to show when hovering over the question mark on the login selection page, leave empty to use default.

**authSlug** - Fill in the URL ending to allow a direct link for users to login via this auth method. The new URL will be `https://<my_mediaspace_instance>.kaltura.com/auth/SLUG`.

Only alphanumeric characters are allowed.

**allowAnonymous** - 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** - Set how long (in seconds) a MediaSpace user session can last. If set value is lower than the minimum of 3600 seconds (1h), the minimum will be utilized.

**refreshDetailsOnLogin** - Select 'Yes' to update the user's details on Kaltura upon login (recommended).

**refreshRoleOnLogin** - 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.

## IdapServer

Click **Expand** to display the LDAP server options.

**IdapServer**
Collapse

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.

<b>host</b>	<input type="text" value="ldap.example.com"/>	What is the address of your LDAP Server?
<b>port</b>	<input type="text" value="389"/>	What is the port of your LDAP Server?
<b>protocol</b>	<input type="text" value="ldap"/>	What protocol does your LDAP server use? (ldap or ldaps)
<b>protocolVersion</b>	<input type="text" value="v3"/>	What is the protocol version of your LDAP server? (V2 or V3)
<b>baseDn</b>	<input type="text" value="dc=example,dc=com"/>	What is the base DN of your LDAP server?
<b>bindMethod</b>	<input type="text" value="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.

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.

**host** - Enter the address of your LDAP Server.

**port** - Enter the port of your LDAP Server.

**protocol** - Enter the protocol your LDAP server uses (ldap or ldaps).

**Protocolversion** - Enter the protocol version of your LDAP server (V2 or V3).

**baseDn** - Enter the base DN of your LDAP server.

**bindMethod** - Select the mode of operation used for authenticating with LDAP.

**bindMethod**

Search before bind ▾
Search before bind
Direct Bind

- **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

Click **Expand** to display the options.

searchUser
Collapse

<b>username</b>	<input data-bbox="496 622 743 651" style="width: 90%;" type="text" value="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.
<b>password</b>	<input data-bbox="496 712 743 741" style="width: 90%;" type="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.
<b>userSearchQueryPattern</b>	<input data-bbox="496 786 743 815" style="width: 90%;" type="text" value="(&amp;(objectClass=person)(uid=@@l"/>	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** - 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** - 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.

**emailAttribute** - What is the name of the attribute on the user record that contains the user ID? If you do not want to sync email with Kaltura, do not enter an emailAttribute.

**firstNameAttribute** - What is the name of the attribute on the user record that contains the user's first name? If you do not want to sync the first name with Kaltura, do not enter a firstNameAttribute.

**lastNameAttribute** - What is the name of the attribute on the user record that contains the user's last name? If you do not want to sync the last name with Kaltura, do not enter a lastNameAttribute.

**tlsCipherSuite - Advanced:** Control the value of LDAPTLS\_CIPHER\_SUITE environment variable. **Use with extra care!**

## IdapOptions

Click **Expand** to display the LDAP Options for group searches.

**IdapOptions** Collapse

Configure the LDAP options for group searches.

**groupSearch** Get groups from user ▾

---

**byUser** Collapse

<b>memberOfAttribute</b>	<input type="text" value="memberOf"/>	<small>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.</small>
<b>userSearchQueryPattern</b>	<input type="text" value="(&amp;(objectClass=person)(uid=@@l)"/>	<small>Enter the pattern for querying the LDAP server to find a user. The @@USERNAME@@ token will be replaced with the actual user name provided in the login window.</small>
<b>primaryGroupIdAttribute</b>	<input type="text"/>	<small>(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.</small>

---

**groupsMatchingOrder**

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.

Configure the LDAP options for group searches.

**groupSearch** - Select the option from the drop-down menu: Get user from groups or Get groups from user

**groupSearch** Get groups from user ▾

Get user from groups

Get groups from user

Get user from groups

If you select **Get user from groups**, complete the **byGroup** section that follows:

**byGroup** Collapse

**groupSearchQueryPattern**

---

**groupSearchEachGroupPattern**

---

**groupSearchQuery**

---

**groupMembershipAttribute**



groupMembershipAttribute

member

**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.

Get groups from user

If you select **Get groups from user**, complete the **byUser** section that follows:

byUser
Collapse

memberOfAttribute	<input style="width: 90%;" type="text" value="memberOf"/>
userSearchQueryPattern	<input style="width: 90%;" type="text" value="{&amp;(objectClass=person)(uid=@@!"/>
primaryGroupIdAttribute	<input style="width: 90%;" type="text"/>

**memberOfAttribute** - 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** - Enter the pattern for querying the LDAP server to find a user. The @@USERNAME@@ 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** - 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.

## IdapGroups

Click **Expand** to 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'

**IdapGroups** Collapse

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'

<b>adminRole</b>	<input type="text" value="mediaSpaceFaculty"/> <span>X</span> <input type="text" value="mediaSpaceAdmin"/> <span>X</span>	Enter LDAP group names that match the MediaSpace adminRole.
		<a href="#">+ Add "adminRole"</a>
<b>viewerRole</b>	<input type="text" value="mediaSpaceStudent"/> <span>X</span> <input type="text" value="mediaSpaceUser"/> <span>X</span>	Enter LDAP group names that match the MediaSpace viewerRole.
		<a href="#">+ Add "viewerRole"</a>
<b>privateOnlyRole</b>	<input type="text" value="mediaSpacePrivateOnly"/> <span>X</span>	Enter LDAP group names that match the MediaSpace privateOnlyRole.
		<a href="#">+ Add "privateOnlyRole"</a>
<b>unmoderatedAdminRole</b>	<input type="text" value="mediaSpaceSuperAdmin"/> <span>X</span>	Enter LDAP group names that match the MediaSpace unmoderatedAdminRole.
		<a href="#">+ Add "unmoderatedAdminRole"</a>
<b>matchByPrimaryGroupId</b>	<input type="text" value="Match by primary group id"/>	
		<a href="#">+ Add "matchByPrimaryGroupId"</a>

**adminRole** - Enter LDAP group names that match the MediaSpace adminRole. Click **+Add "adminRole"** to add another role.

**viewerRole** - Enter LDAP group names that match the MediaSpace viewerRole. Click **+Add "viewerRole"** to add another role.

**privateOnlyRole** - Enter LDAP group names that match the MediaSpace privateOnlyRole. Click **+Add "privateOnlyRole"** to add another role.

**unmoderatedAdminRole** - Enter LDAP group names that match the MediaSpace unmoderatedAdminRole. Click **+Add "unmoderatedAdminRole"** to add another role.

### **matchByPrimaryGroupId**

To match by primary group ID, click **+Add "matchByPrimaryGroupId"**.

A new section displays.

\* **DELETE**

**primaryGroupId**

**roleForGroup**

**primaryGroupId** - Enter ID.

**roleForGroup** - Select the desired role from the drop-down menu.

**roleForGroup**

anonymousRole ▾

**anonymousRole**

viewerRole

privateOnlyRole

adminRole

unmoderatedAdminRole

## SSO

Click **Expand** to configure the video portal login through SSO gateway.

SSO
**Collapse**

To configure KMS login through SSO gateway fill in the fields below.

**secret**  Enter a custom secret, or enter 'default' to use the Kaltura Admin Secret associated with your Kaltura account.

**loginUrl**  What is the URL for the SSO gateway login page? Note: The 'ref' parameter is added automatically.

**logoutUrl**  What is the URL to which a user is redirected after logging out of MediaSpace? Usually, you enter your organization's login page.

**hashAlgorithm**  Choose the hash algorithm you use to generate the session key.

**secret** - Enter a custom secret, or enter 'default' to use the Kaltura Admin Secret associated with your Kaltura account.

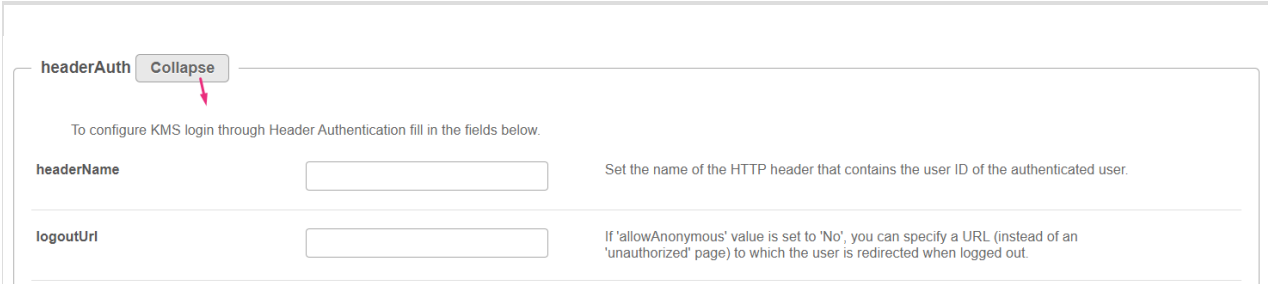
**loginUrl** - What is the URL for the SSO gateway login page? Note: The 'ref' parameter is added automatically.

**logoutUrl** - What is the URL to which a user is redirected after logging out of MediaSpace? Usually, you enter your organization's login page.

**hashAlgorithm** - Choose the hash algorithm used to generate the session key - either 'SHA1' or 'SHA256'.

## headerAuth

Click **Expand** to configure KMS login through Header Authentication.



headerAuth **Collapse**

To configure KMS login through Header Authentication fill in the fields below.

<b>headerName</b>	<input type="text"/>	Set the name of the HTTP header that contains the user ID of the authenticated user.
<b>logoutUri</b>	<input type="text"/>	If 'allowAnonymous' value is set to 'No', you can specify a URL (instead of an 'unauthorized' page) to which the user is redirected when logged out.

**headerName** - Set the name of the HTTP header that contains the user ID of the authenticated user.

**logoutURL** - If 'allowAnonymous' value is set to 'No', you can specify a URL (instead of an 'unauthorized' page) to which the user is redirected when logged out.

## forgotPassword

Click **Expand** to define the values for the **Forgot Password** options.

**forgotPassword** Collapse

Define the values for the 'Forgot Password' options.

<b>link</b>	<input type="text" value="mailto:admin@example.com"/>	The 'link' options are: [1] Empty the value if you do not want a 'Forgot Password' link to be displayed. [2] Enter an email address preceded by 'mailto:' (without quotes). The user's local email client opens an email with the subject and body populated with the texts defined in the 'emailSubject' and 'emailBody' fields. [3] Enter a URL for a page that you define (for example, a mechanism for reminding users of their login credentials). Note: Do not enter 'true.'
<b>emailSubject</b>	<input type="text" value="This is email subject"/>	If you enter an email address in the 'link' field, enter the text to populate the subject field of the email. If you do not want to populate the subject field, enter an empty string ('').
<b>emailBody</b>	<input type="text" value="I forgot my password"/>	If you enter an email address in the 'link' field, enter the text to populate the body of the email. If you do not want to populate the body, enter an empty string (''). For KalturaAuth's User Management send new password feature: (If authClass is set to KalturaAuth, MediaSpace exposes a user management system. This system's admin can click on a user's email to open the admin's local email client to email the new password to the user.)
<b>reminderSubject</b>	<input type="text" value="New MediaSpace Password"/>	Enter the text to populate the subject field of the 'new password' email. If you do not want to populate the subject field, enter an empty string ('').
<b>reminderBody</b>	<input "="" type="text" value="Your new password is:"/>	Enter the text to populate the body of the 'new password' email. The password will be inserted automatically at the end of the body text. If you do not want to populate the body, enter an empty string ('').

### link - The 'link' options are:

- [1] Empty the value if you do not want a 'Forgot Password' link to be displayed.
- [2] Enter an email address preceded by 'mailto:' (without quotes). The user's local email client opens an email with the subject and body populated with the texts defined in the 'emailSubject' and 'emailBody' fields.
- [3] Enter a URL for a page that you define (for example, a mechanism for reminding users of their login credentials). Note: Do not enter 'true.'

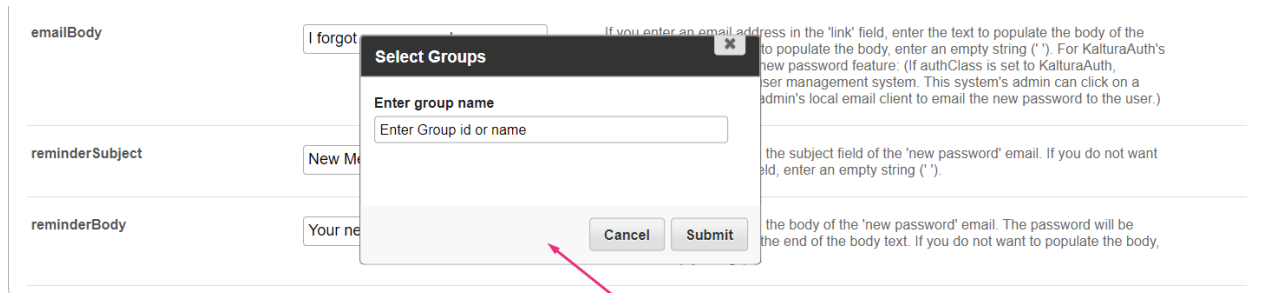
**emailSubject** - If you enter an email address in the 'link' field, enter the text to populate the subject field of the email. If you do not want to populate the subject field, enter an empty string ('').

**emailBody** - If you enter an email address in the 'link' field, enter the text to populate the body of the email. If you do not want to populate the body, enter an empty string (''). For KalturaAuth's User Management send new password feature: (If authClass is set to KalturaAuth, MediaSpace exposes a user management system. This system's admin can click on a user's email to open the admin's local email client to email the new password to the user.)

**reminderSubject** - Enter the text to populate the subject field of the 'new password' email. If you do not want to populate the subject field, enter an empty string ('').

**reminderBody** - Enter the text to populate the body of the 'new password' email. The password will be inserted automatically at the end of the body text. If you do not want to populate the body, enter an empty string ('').

**adminsGroup** - Enter a group ID to which any KMC or EP users will be added upon login to the site.



The screenshot shows a configuration form with fields for emailBody, reminderSubject, and reminderBody. A modal dialog titled "Select Groups" is open, containing a text input field labeled "Enter group name" with the placeholder text "Enter Group id or name". Below the input field are "Cancel" and "Submit" buttons. A red arrow points from the "Select Groups" button in the form below to the "Submit" button in the modal.

**adminsGroup**  **Select Groups** Enter a group ID to which any KMC or EP users will be added upon login to the site.

Click **Save**.