

Configuring LDAP Authentication and Authorization

Last Modified on 05/26/2020 10:22 pm IDT

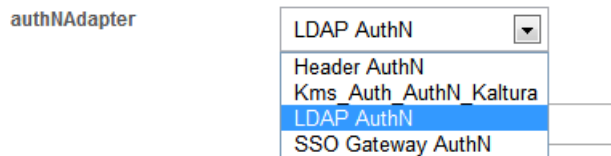
To learn more about integrating your LDAP server for authenticating users and authorizing user access to MediaSpace with a specific application role, refer to [Kaltura MediaSpace Authentication and Authorization Solutions – Overview](#) and [Kaltura MediaSpace LDAP Integration Guide](#).

To configure user authentication through your LDAP server

1. On the Configuration Management panel of the Kaltura MediaSpace Administration Area, open the [Auth](#) tab.

After you complete and verify the following steps, click **Save**.

2. Under [authNAdapter](#), select **LDAP AuthN**.

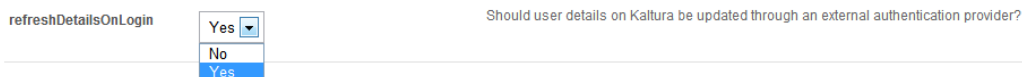


The screenshot shows a configuration field labeled "authNAdapter". A dropdown menu is open, displaying the following options: "LDAP AuthN", "Header AuthN", "Kms_Auth_AuthN_Kaltura", "LDAP AuthN", and "SSO Gateway AuthN". The "LDAP AuthN" option is currently selected and highlighted in blue.

3. Select your preferences for the [common login options](#).

4. Under [refreshDetailsOnLogin](#), select your preference.

This option affects the updating of the user's first name, last name, and email address (when provided) from your LDAP system upon every login.



The screenshot shows a configuration field labeled "refreshDetailsOnLogin". A dropdown menu is open, displaying the options "Yes", "No", and "Yes". The "Yes" option is currently selected and highlighted in blue. To the right of the dropdown, the text reads: "Should user details on Kaltura be updated through an external authentication provider?"

5. Under [ldapServer](#):

- a. Select the LDAP Server access and bind settings.

Your **bindMethod** selection will affect the information you need to provide for authenticating the user.

ldapServer

Configure your LDAP/Active Directory Server.

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

LDAP Server Configuration – bindMethod selection

bindMethod	<input type="text" value="Direct 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.
-------------------	------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

directBind

userDnFormat

Enter the DN format of the username. Place the @@USERNAME@@ token where the username should be in the string. For example:
'cn=@@USERNAME@@,ou=somegroup,dc=example,dc=com')

LDAP Server Configuration - Direct Bind options

bindMethod	<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.
-------------------	-------------------------------------------------	--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

searchUser

username

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.

LDAP Server Configuration - Search before Bind options

- b. Select the LDAP attributes for first name, last name and email address.

Populating the user's first and last name is used for several MediaSpace options that require the user name.

The email address is optional. This field is useful for user management and for future features (such as email notifications).

emailAttribute	<input type="text"/>	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	<input type="text"/>	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	<input type="text"/>	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.

LDAP Server Configuration - Email options

- If you are using your LDAP server to authorize user access to MediaSpace with a specific application role, continue with the next procedure. If not, select a different authorization method.

To configure user authorization through your LDAP server

- On the Configuration Management panel of the Kaltura MediaSpace Administration Area, open the [Auth](#) tab.

After you complete and verify the following steps, click **Save**.

- Under [authZAdapter](#), select **LDAP AuthZ**.

authZAdapter

LDAP AuthZ

▼

Kms_Auth_AuthZ_Kaltura

LDAP AuthZ

SSO Gateway AuthZ

- Under [refreshRoleOnLogin](#), select your preference.

This option affects the updating of the user's role from your LDAP system upon every login.

refreshRoleOnLogin	<div style="border: 1px solid #ccc; padding: 2px;"> <div style="display: flex; align-items: center;"> <div style="border: 1px solid #ccc; padding: 2px 5px;">Yes</div> <div style="margin-left: 5px;">▼</div> </div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-top: 2px;">No</div> <div style="border: 1px solid #ccc; padding: 2px 5px; margin-top: 2px; background-color: #e0e0e0;">Yes</div> </div>	Should the user role on Kaltura be updated through an external authorization provider? Select 'No' to allow overriding a role through Kaltura user management.
--------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	----------------------------------------------------------------------------------------------------------------------------------------------------------------

- Under [ldapOptions](#), select your preferences for getting the list of groups in which the user is a member.

This option is used to determine the user's MediaSpace Application Role.

Under [groupsMatchingOrder](#), enter the order for matching MediaSpace roles to LDAP groups. The order determines whether the strongest or weakest role is mapped first.

Your **groupSearch** selection will affect the information you need to provide.

IdapOptions

Configure the LDAP options for group searches.

groupSearch

byUser

memberOfAttribute

userSearchQueryPattern

primaryGroupIdAttribute

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.

LDAP Authorization Options - Get Groups from User

Configure the LDAP options for group searches.

groupSearch

byGroup

groupSearchQueryPattern

groupSearchEachGroupPattern

groupSearchQuery

groupMembershipAttribute

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.

LDAP Authorization Options - Get User from Groups

- Under **IdapGroups**, select your preferences to define the mappings between the groups defined in your LDAP server and the MediaSpace Application Roles.

IdapGroups

Map your LDAP server groups to MediaSpace groups.

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