

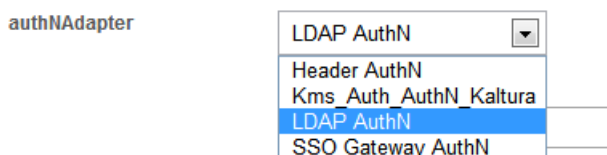
Configuring LDAP Authentication and Authorization

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

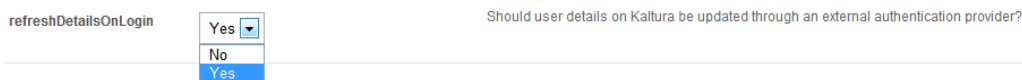
To learn more about integrating your LDAP server for authenticating users and authorizing user access to MediaSpace with a specific application role, refer to [Kaltura MediaSpace Authentication and Authorization Solutions – Overview](#) and [Kaltura MediaSpace LDAP Integration Guide](#).

To configure user authentication through your LDAP server

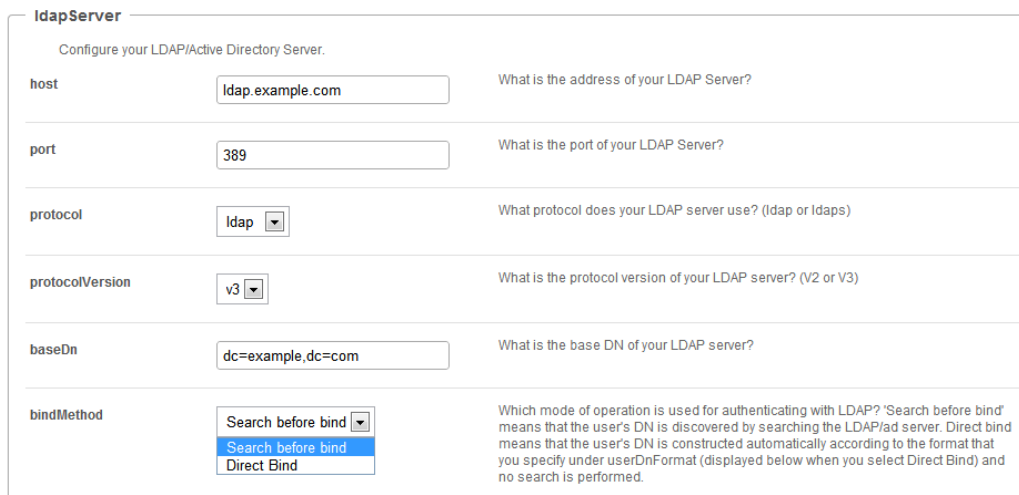
1. On the Configuration Management panel of the Kaltura MediaSpace Administration Area, open the [Auth](#) tab.
After you complete and verify the following steps, click **Save**.
2. Under [authNAdapter](#), select **LDAP AuthN**.



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.



5. Under [IdapServer](#):
 - a. Select the LDAP Server access and bind settings.
Your [bindMethod](#) selection will affect the information you need to provide for authenticating the user.



LDAP Server Configuration – bindMethod selection

bindMethod	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.
<div>directBind</div> <div> userDnFormat cn=@@USERNAME@@,dc=exar </div> <p>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')</p>		

LDAP Server Configuration - Direct Bind options

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.
<div>searchUser</div> <div> username </div> <p>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.</p> <div> password </div> <p>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.</p> <div> userSearchQueryPattern (&(objectClass=person)(uid=@@U </div> <p>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.</p>		

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		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.

LDAP Server Configuration - Email options

6. 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

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 **authZAdapter**, select **LDAP AuthZ**.

authZAdapter

LDAP AuthZ

Kms_Auth_AuthZ_Kaltura

LDAP AuthZ

SSO Gateway AuthZ

Add custom value

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

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

refreshRoleOnLogin

Yes

No

Yes

Should the user role on Kaltura be updated through an external authorization provider? Select 'No' to allow overriding a role through Kaltura user management.

4. 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.

ldapOptions

Configure the LDAP options for group searches.

groupSearch

Get groups from user

Get user from groups

Get groups from user

byUser

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=@@U

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

unmoderatedAdminRole,adminRole

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

Get user from groups
Get user from groups
Get groups from user

byGroup

groupSearchQueryPattern

(&(objectclass=group)(|@GROU

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

(cn=@@GROUPNAME@@)

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

member

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

groupsMatchingOrder

unmoderatedAdminRole,adminRole

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

mediaSpaceFaculty X
mediaSpaceAdmin X

Enter LDAP group names that match the MediaSpace adminRole.

+ Add "adminRole"

viewerRole

mediaSpaceStudent X
mediaSpaceUser X

Enter LDAP group names that match the MediaSpace viewerRole.

+ Add "viewerRole"

privateOnlyRole

mediaSpacePrivateOnly X

Enter LDAP group names that match the MediaSpace privateOnlyRole.

+ Add "privateOnlyRole"

unmoderatedAdminRole

mediaSpaceSuperAdmin X

Enter LDAP group names that match the MediaSpace unmoderatedAdminRole.

+ Add "unmoderatedAdminRole"

matchByPrimaryGroupid

Match by primary group Id

+ Add "matchByPrimaryGroupid"