

Authentication and authorization options in Video Portal

Last Modified on 11/14/2025 10:55 am IST



This article is designated for administrators.

About

This article introduces the authentication and authorization options available for the Video Portal. It explains how each method works and how they can be combined to manage user access and roles.

These options let you:

- Use your organization's existing login systems
- Control who can access the Video Portal
- Define what each user can do after logging in

All authentication and authorization settings are configured in the Auth module of the Configuration Management console.

How authentication and authorization work

- Authentication controls who can log in to the Video Portal.
- Authorization controls what each user can do after logging in (their application role).

For more about roles, see User roles and permissions in Video Portal.

Available methods

Single Sign-On (SSO) Gateway

Kaltura's SSO Gateway connects the Video Portal to your organization's existing login system, such as LDAP, CAS, or another identity provider. This lets users sign in once and access both your organization's site and the Video Portal.



Function	Description
Authentication	Uses your organization's existing user management and authentication method.
Authorization	Passes user roles to the Video Portal as part of the organization's login process.
Advantages	 Provides a true single sign-on experience Uses existing systems and credentials Flexible user data mapping Login page can appear on your organization's site
Limitations	• Requires minor login page coding • Authorization can only be used with SSO Gateway authentication
Licensing	Included with user-based licensing. Professional Services available for implementation support.

Kaltura authentication and authorization

This built-in method uses Kaltura's internal user management system. It's simple to configure and doesn't require integration with external systems.

Function	Description
Authentication	Users log in using credentials stored in Kaltura.
Authorization	Roles and permissions are managed directly in Kaltura.
Advantages	Built-in user management No integration required
Limitations	Users must be managed separately from your organization's directory
Licensing	Included with user-based licensing. Other licensing models available - contact your Kaltura Representative.

LDAP (Lightweight Directory Access Protocol)

LDAP integration connects the Video Portal to your organization's LDAP or Active Directory server for login and role assignment.



Function	Description
Authentication	Users log in using organizational credentials from LDAP or Active Directory.
Authorization	Roles are assigned based on LDAP group membership.
Advantages	 Uses existing organizational credentials Integrates easily with existing systems Flexible mapping of user information
Limitations	Not a full single sign-on experienceConfiguration depends on your LDAP server setup
Licensing	Included with user-based licensing. Works out of the box with standard LDAP configurations.

Header authentication

Header authentication provides a seamless login experience by relying on network components (for example, a load balancer) that add an authenticated HTTP header when a user opens the Video Portal.

Function	Description	
Authentication	Users log in automatically through a trusted HTTP header added by your network or	
	infrastructure.	
Authorization	Not applicable - you'll need to configure a separate authorization method (for example,	
	Kaltura or LDAP).	
Advantages	Seamless single sign-on experience	
	Minimal configuration effort	
Limitations	Requires another method for authorization	
Licensing	Included with user-based licensing.	
•		