

# Authentication and authorization options in legacy Video Portal

Last Modified on 06/04/2026 9:15 am IDT

 This article is designated for administrators.

## About

This article introduces the authentication and authorization options available for the legacy 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 legacy 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 legacy 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 legacy Video Portal](#).

## Available methods

### Single Sign-On (SSO) Gateway

Kaltura's SSO Gateway connects the legacy 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 legacy Video Portal.

Function	Description
<b>Authentication</b>	Uses your organization's existing user management and authentication method.

Function	Description
<b>Authorization</b>	Passes user roles to the legacy Video Portal as part of the organization's login process.
<b>Advantages</b>	<ul style="list-style-type: none"> <li>• Provides a true single sign-on experience</li> <li>• Uses existing systems and credentials</li> <li>• Flexible user data mapping</li> <li>• Login page can appear on your organization's site</li> </ul>
<b>Limitations</b>	<ul style="list-style-type: none"> <li>• Requires minor login page coding</li> <li>• Authorization can only be used with SSO Gateway authentication</li> </ul>
<b>Licensing</b>	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
<b>Authentication</b>	Users log in using credentials stored in Kaltura.
<b>Authorization</b>	Roles and permissions are managed directly in Kaltura.
<b>Advantages</b>	<ul style="list-style-type: none"> <li>• Built-in user management</li> <li>• No integration required</li> </ul>
<b>Limitations</b>	<ul style="list-style-type: none"> <li>• Users must be managed separately from your organization's directory</li> </ul>
<b>Licensing</b>	Included with user-based licensing. Other licensing models available - contact your Kaltura Representative.

## LDAP (Lightweight Directory Access Protocol)

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

Function	Description
<b>Authentication</b>	Users log in using organizational credentials from LDAP or Active Directory.
<b>Authorization</b>	Roles are assigned based on LDAP group membership.
<b>Advantages</b>	<ul style="list-style-type: none"> <li>• Uses existing organizational credentials</li> <li>• Integrates easily with existing systems</li> <li>• Flexible mapping of user information</li> </ul>

Function	Description
<b>Limitations</b>	<ul style="list-style-type: none"> <li>• Not a full single sign-on experience</li> <li>• Configuration depends on your LDAP server setup</li> </ul>
<b>Licensing</b>	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 legacy Video Portal.

Function	Description
<b>Authentication</b>	Users log in automatically through a trusted HTTP header added by your network or infrastructure.
<b>Authorization</b>	Not applicable - you'll need to configure a separate authorization method (for example, Kaltura or LDAP).
<b>Advantages</b>	<ul style="list-style-type: none"> <li>• Seamless single sign-on experience</li> <li>• Minimal configuration effort</li> </ul>
<b>Limitations</b>	<ul style="list-style-type: none"> <li>• Requires another method for authorization</li> </ul>
<b>Licensing</b>	Included with user-based licensing.