

AICC - Admin Guide

Last Modified on 09/11/2024 6:51 pm IDT

 This article is designated for administrators.

About

The AICC Communication Protocol supports communication between a Learning Management System (LMS) and existing course content. Enabling the AICC module in the video portal allows a customer to securely share Kaltura media content within their course. Each authenticated user has a seamless experience when consuming Kaltura-uploaded content.

Kaltura recently performed such integration for Siam Commercial Bank (SCB). Following is a brief overview of how integration was accomplished in this design use case:

SCB employs an LMS that uses the AICC protocol - Saba. Media is created and uploaded to a video portal channel, then embedded into Saba. An SCB user opens Saba and attempts to play said media. Saba sends a request to the video portal providing the Saba session ID and the video portal channel ID. The video portal sends a request to Saba for additional information about the user. Playback is granted to the authenticated user and video portal analytics are tracked in the player, which are then sent through the video portal backend to Saba.

This guide explains how to enable and configure the AICC module in the Configuration Management console.

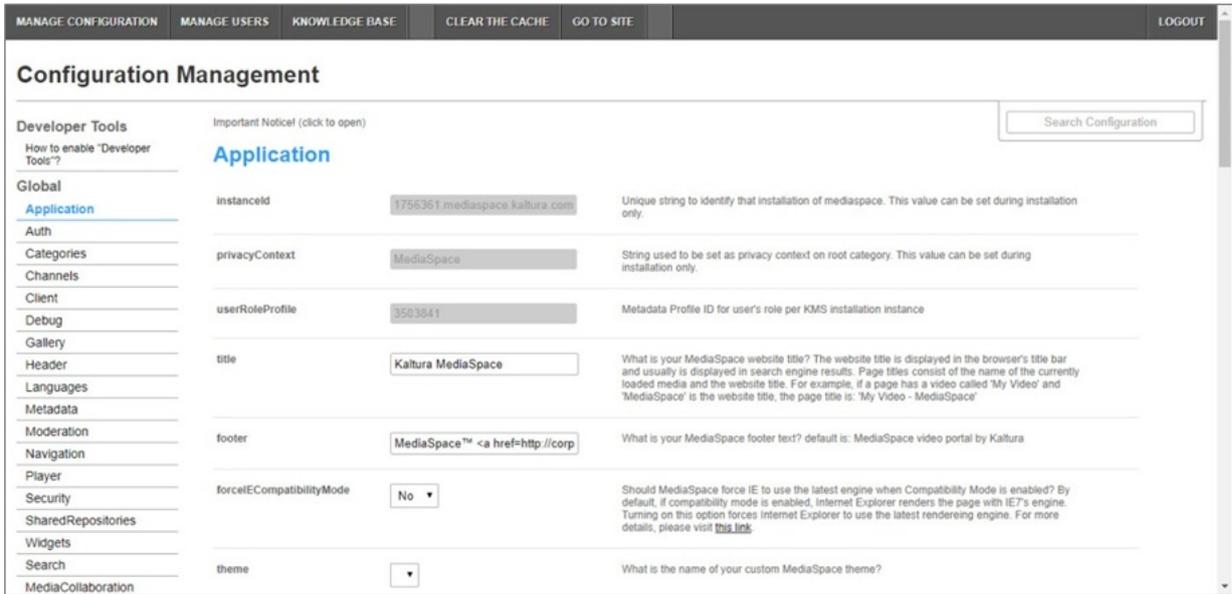
 This module is for non-Theming users.

 For technical support, contact Kaltura Customer Care. For all other inquiries, reach out to your Customer Success Manager.

Configure

1. Log into the Configuration Management console by going to your video portal URL and adding `/admin` at the end.
2. Enter your Kaltura user ID and password.
3. Click **Sign In**.

The **Configuration Management** console displays.



Configuration Management

Developer Tools
How to enable "Developer Tools"?

Global
Application
Auth
Categories
Channels
Client
Debug
Gallery
Header
Languages
Metadata
Moderation
Navigation
Player
Security
SharedRepositories
Widgets
Search
MediaCollaboration

Important Notice! (click to open)

Application

Search Configuration

instanceId: 1756361.mediaspace.kaltura.com
Unique string to identify that installation of mediaspace. This value can be set during installation only.

privacyContext: MediaSpace
String used to be set as privacy context on root category. This value can be set during installation only.

userRoleProfile: 3503841
Metadata Profile ID for user's role per KMS installation instance

title: Kaltura MediaSpace
What is your MediaSpace website title? The website title is displayed in the browser's title bar and usually is displayed in search engine results. Page titles consist of the name of the currently loaded media and the website title. For example, if a page has a video called 'My Video' and 'MediaSpace' is the website title, the page title is: 'My Video - MediaSpace'

footer: MediaSpace™ <a href=http://corp
What is your MediaSpace footer text? default is: MediaSpace video portal by Kaltura

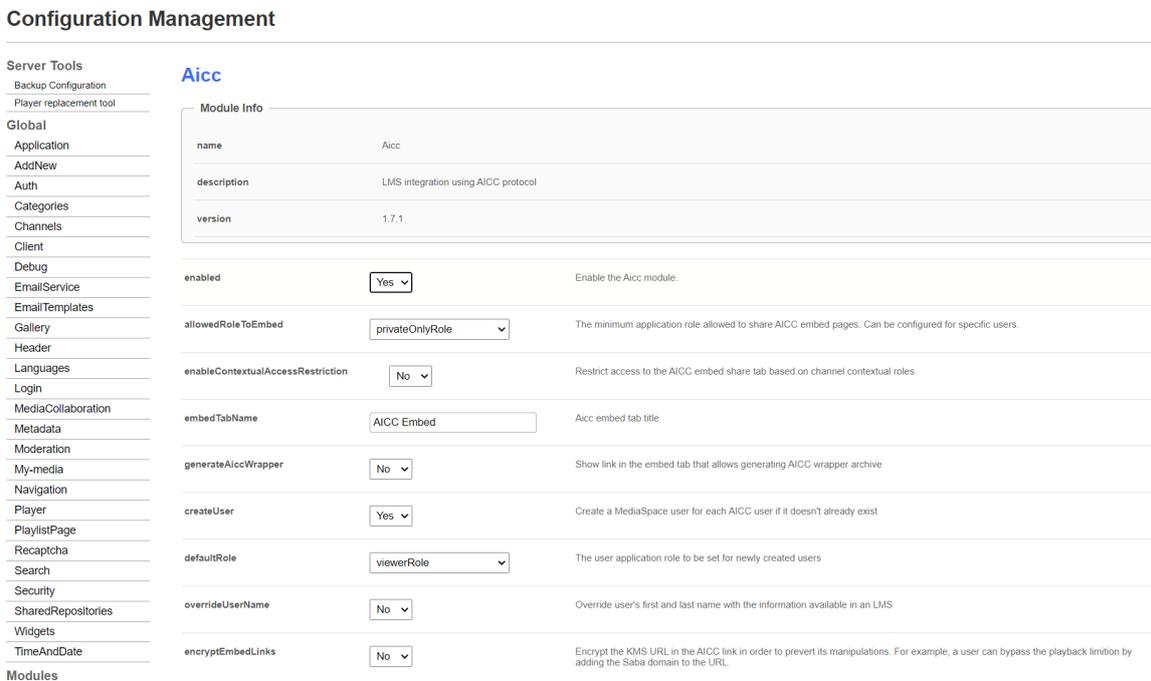
forceIECompatibilityMode: No
Should MediaSpace force IE to use the latest engine when Compatibility Mode is enabled? By default, if compatibility mode is enabled, Internet Explorer renders the page with IE7's engine. Turning on this option forces Internet Explorer to use the latest rendering engine. For more details, please visit [this link](#).

theme:
What is the name of your custom MediaSpace theme?

4. In the list of configurable items on the left of your screen, locate and click on **Aicc**. (The item will be crossed out because it's disabled by default.)

⚠ If this module is not in your KMS application, please get in touch with your Kaltura representative to inquire about adding it.

5. The AICC window displays.



Configuration Management

Server Tools
Backup Configuration
Player replacement tool

Global
Aicc
AddNew
Auth
Categories
Channels
Client
Debug
EmailService
EmailTemplates
Gallery
Header
Languages
Login
MediaCollaboration
Metadata
Moderation
My-media
Navigation
Player
PlaylistPage
Recaptcha
Search
Security
SharedRepositories
Widgets
TimeAndDate
Modules

Aicc

Module Info

name: Aicc
description: LMS integration using AICC protocol
version: 1.7.1

enabled: Yes
Enable the Aicc module.

allowedRoleToEmbed: privateOnlyRole
The minimum application role allowed to share AICC embed pages. Can be configured for specific users.

enableContextualAccessRestriction: No
Restrict access to the AICC embed share tab based on channel contextual roles

embedTabName: AICC Embed
Aicc embed tab title

generateAiccWrapper: No
Show link in the embed tab that allows generating AICC wrapper archive

createUser: Yes
Create a MediaSpace user for each AICC user if it doesn't already exist

defaultRole: viewerRole
The user application role to be set for newly created users

overrideUserName: No
Override user's first and last name with the information available in an LMS

encryptEmbedLinks: No
Encrypt the KMS URL in the AICC link in order to prevent its manipulations. For example, a user can bypass the playback limitation by adding the Saba domain to the URL.

The **Module Info** box displays the module name, description (what enabling this module allows users to do), and version number.

6. Configure the following:

enabled - Set to 'Yes' to enable the module.

allowedRoleToEmbed - Choose the minimum applicative role that is allowed to share AICC embed pages. This can be configured for specific users. The options are as follows:

- Owner Only
- Specific Users
- ViewerRole
- PrivateOnlyRole
- AdminRole
- UnmoderatedAdminRole

✔ For more information about contextual roles, visit our article [Video Portal and KAF roles and permissions](#).

enableContextualAccess Restriction - This setting is applicable to a user who browses the site, accesses a certain channel, and accesses a media entry within that channel. Set to 'Yes' to make access to the AICC embed tab only possible within the context of a channel.

If set to 'No', access to the AICC embed tab will not be restricted and the tab will be present across the video portal. In other words, any user can access the AICC embed tab with any contextual role. In fact, the media does not even need to be published and can be privately owned.

If you set to 'Yes', additional configuration options display:

allowedChannelMembership	Contributor ▼	The minimum contextual role in a channel allowed to share AICC embed pages
allowedChannelTypes	<input type="checkbox"/> Open <input type="checkbox"/> Restricted <input type="checkbox"/> Private <input type="checkbox"/> Shared Repository <input type="checkbox"/> Public	The channel type allowed to embed. The embed option will be possible only from the selected options. Please select at least 1.
createGroupUser	Yes ▼	Automatically create a group user for the allowed channel types. AICC content consumers will be automatically added to this group user and inherit its role.
groupUserMembership	Member ▼	The contextual role allowed assigned to the automatically created group user. Changing this value will not affect the roles of existing group users.

allowedChannelTypes - Enter the minimum contextual role in a channel allowed to share AICC embed pages. The options are as follows:

- Manager
- Moderator
- Contributor
- Member

✔ For more information about contextual roles, visit our article [Video Portal and KAF roles and permissions](#).

createGroupUser - Automatically create a group user for the allowed channel types. AICC content consumers will be automatically added to this group user and inherit its role. This is set to 'Yes' by default.

groupUserMembership - Select the contextual role assigned to the automatically created group user. Changing this value will not affect the roles of existing group users. The options are as follows:

- Manager
- Moderator
- Contributor
- Member

embedTabName - Type a name for the embed tab that displays the AICC embed (see [example below](#)).

generateAiccWrapper - Set to 'Yes' to show link in the embed tab that allows generating AICC wrapper archive. If set to 'Yes', an additional configuration option displays:

aiccWrapperLinkText

The text of the AICC wrapper generation link

aiccWrapperLinkText - Enter text of the AICC wrapper generation link.

createUser - Set to 'Yes' to create a video portal user for each AICC user if it does not already exist. For example, in the design use case for SCB, when a user attempts to watch content that was embedded in Saba, the video portal requests to query Saba for additional information on that user's ID. If 'Yes' is selected, a video portal user will be created and listed in the User ID column of the User Management Window in the Configuration Management Section of the video portal based on the Saba's user ID information.

If 'No' is selected, the playback will only work if the user already exists and is entitled to watch the content or if the content itself is publicly accessible to all end users, including unauthenticated users.

If you select 'Yes', an additional configuration option displays:

defaultRole

The user application role to be set for newly created users

defaultRole - Choose the user applicative role for newly created users. In other words, what is the default role that this new video portal user will be assigned? The options are as follows:

- ViewerRole
- PrivateOnlyRole
- AdminRole
- UnmoderatedAdminRole

✓ For more information about contextual roles, visit our article [Video Portal and KAF roles and permissions](#).

overrideUserName - Set to 'Yes' to override the user's first and last name with the information available in the LMS. If the user exists in the video portal, this setting allows their name to be overridden – regardless of whether or not they are a video portal user or regular user. If set to 'No', the user's first and last name will not be overridden.

encryptEmbedLinks - Set to 'Yes' to encrypt the video portal URL in the AICC link in order to prevent its manipulation. This is a security configuration regarding whether or not to obfuscate the parameters in the URL.

When encrypted, the video portal will be able to decrypt those parameters, but any other entity seeking to manipulate them will not be able to create URLs in this structure. The video portal will not process the request when a request is being made with a manipulated URL.

For example, in the design use case for SCB, the video portal will process requests made only from the Saba domain. When the video portal edits the URL to that domain, it is encrypted. If another user attempts to add the Saba domain, exposed in the URL, the video portal will not process the request.

verifyDomain - Set to 'Yes' to limit the playback of the video portal URL only within the context of an LMS domain. This setting allows the administrator to add a whitelist. If 'No', the system will process requests from any domain.

7. Click **Save**.

You receive a notice that your configuration for AICC was saved and the cache was cleared.

The example below shows the embed tab (named "AICC Embed" by the administrator) on the **Share** tab of the media page.

Copy link to share

[Download AICC wrapper](#)

✓ This document is maintained by Kaltura's Professional Services team. Please send comments or corrections to your Customer Success Manager. Ask them to forward it to the Professional Services team. We are committed to improving our documentation and your feedback is appreciated.