SAML module

Last Modified on 10/12/2024 10:52 am IDT

This article is designated for administrators.

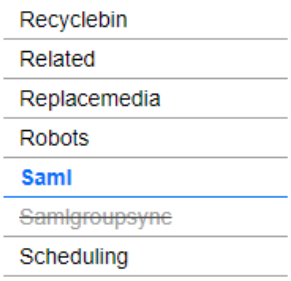
About

This module enables admins to set up SSO authentication for their video portal using the SAML 2.0 standard. For detailed setup instructions and error log documentation, visit our article Kaltura Video Portal SAML integration guide.

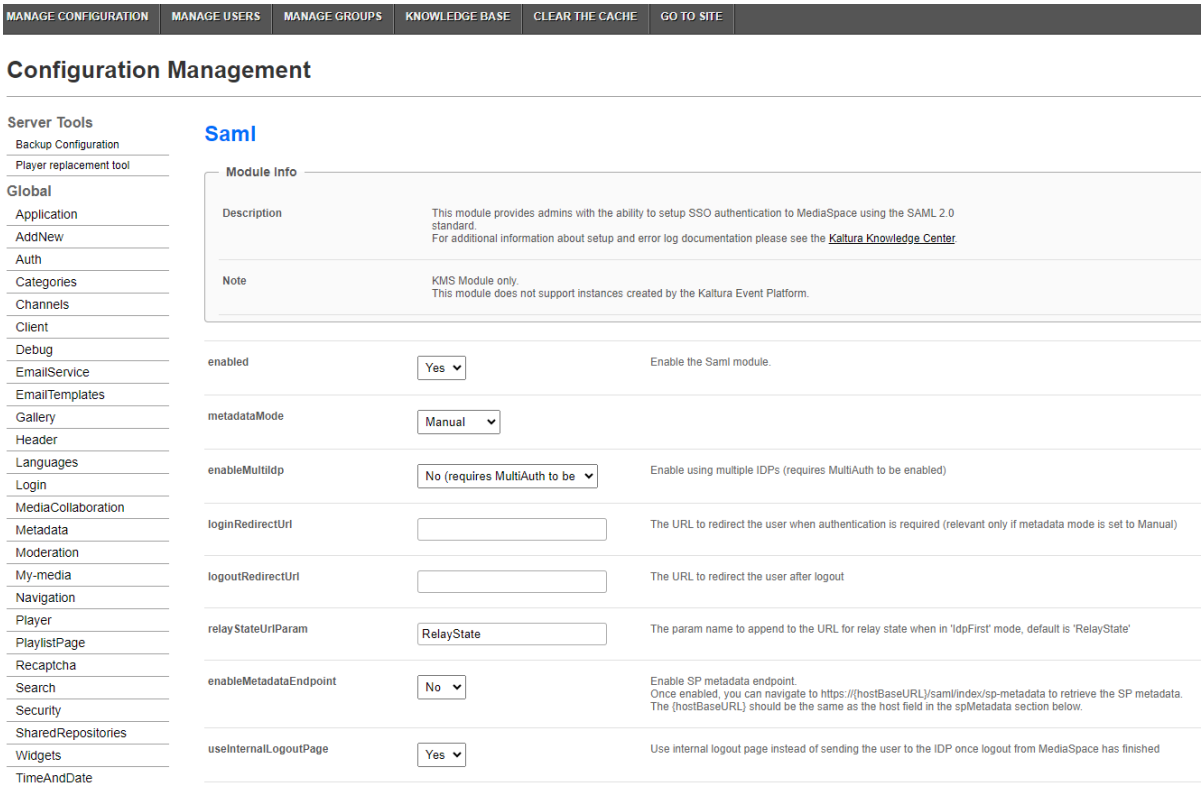
This module is for the video portal only and does not support instances created by Kaltura Events.

Configure

1. Go to your Configuration Management console and click on the **Saml** module. You can also navigate to it directly using a link: https://{your_videoportal_URL}/admin/config/tab/saml.



The Saml page displays.



2. Configure the following:

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

metadataMode - Select Manual or Automatic.

enableMultiIdp - Enable using multiple IDPs (requires MultiAuth to be enabled)

loginRedirectUrl - Enter the URL to redirect the user when authentication is required (relevant only if metadata mode is set to Manual). For SP initiated it would be a URL where the request is posted. For IdP initiated a URL with the entity ID as a parameter.

SP Initiated Example: `https://idp.example.com/identity`

IdP Initiated Example: `https://idp.example.com/identity/UnsolicitedSSO?entityID=mediaspaceentityID`

logoutRedirectUrl - Enter the URL to redirect the user after logout.

This field is only applicable if useInternalLogoutPage is set to "No" and metadataMode is set to "Manual". When the video portal session expires, the user is redirected to this URL, along with a SAML logout request. This request is made via POST request.

The video portal does not expire login session from the identity provider. For the logout request, video portal uses the value that was provided in the NameID element in the SAML login request.

relayStateUrlParam - Enter the parameter name used by the IdP to specify the redirect URL for relay state when in 'IdpFirst' mode. This defines the default redirect location if it’s not included in the request. For example, in PingFederate, this would be TARGET, while for most other SAML providers, it defaults to RelayState.

enableMetadataEndpoint - Enable the SP metadata endpoint to retrieve SP metadata. Once enabled, you can access the SP metadata at `https://{hostBaseURL}/saml/index/sp-metadata.` Make sure to replace `{hostBaseURL}` with the value specified in the **host** field of the **spMetadata** section below.

useInternalLogoutPage - If set to 'Yes', logging out will terminate the video portal session, and use the internal logout page instead of redirecting to the IdP logout page, accompanied by a message such as the following: *You have signed out of MediaSpace. For improved security, we recommend closing all browser windows at the end of your online sessions.*

allowKeepAlive - When set to 'Yes', session will be extended upon user's interaction. Default is 'No'.

logoutText - If useInternalLogoutPage is set to 'Yes', you can define a custom message to users. You can use HTML tags to display a message.

shouldNestRelayState - Choose whether to append the relay state as a regular query string or as a URL-encoded query string.

shouldPost - When set to 'Yes', the SAML request will be posted instead of using get. Default is 'No'.

shouldSignLogoutRequest - When set to 'Yes', the SP SAML logout request will be signed. Default is 'No'.

shouldDecodeRelayState - When set to 'Yes', RelayState will be decoded before redirect.

spMetadata

Configure the settings of this Service Provider (SP) as defined in the Identity Provider (IdP).

name - Enter the entity ID of the service provider (video portal) as it was configured in your Identity Provider. For example: `https://partner_id.mediaspace.kaltura.com` (this will be used as the SP entity ID).

host - Enter the desired video portal alias URN (no `https://` needed). Please note that only one video portal alias can be used with the SAML module. This is the host of your video portal instance (for example, `partner_id.mediaspace.kaltura.com`).

The host can only be configured with a single URL per video portal instance. If you are using a custom alias for your video portal (for example, video.company.com), use that alias instead.

relayState - Enter the value for the relative URL to redirect the user after login if a relay state is not passed as part of the authentication request. The default is /.

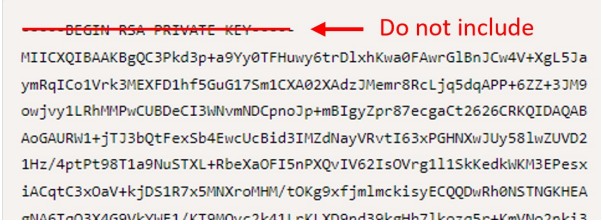
nameIdFormat - This field is only applicable for SP-initiated mode and will not function if the NameID is not released. Select from the following options:

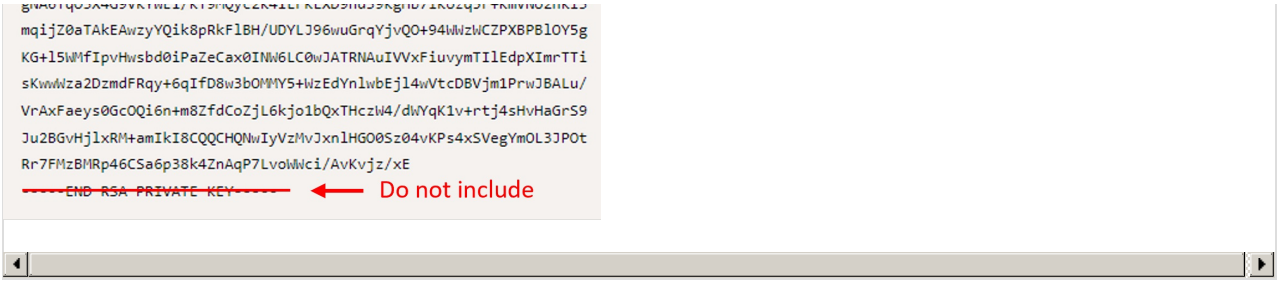
- **Transient**: Recommended for Shibboleth setup.
- **Persistent**: Preferred setup.
- **None**: Removes the NameIDPolicy element from the SAML request.

certificate - (Optional) Enter the certificate information for encryption of the SAML response. Paste the content of the .crt file without the comment lines (for example, **do not paste in**: -----BEGIN CERTIFICATE----- **and** -----END CERTIFICATE-----). Make sure all text is in a single line with no spaces or line breaks. See Generating a Certificate Workflow.

The certificate value is used to encrypt the response provided by the IdP. The following example shows how the crt file would look including the comment lines and the extra line breaks that should be removed:

privateKey - (optional) SP Private Key PEM format. The privateKey value is used to decrypt the response provided by the IdP.





idpMetadata

Configure the settings for the Identity Provider (IdP) as follows:

host - IdP Host Name. Enter the Identity Provider's entity ID (for example, `https://openidp.feide.no`).

issuer - IdP Issuer: The entity ID of the Identity Provider as it appears in the SAML response (for example, `https://openidp.feide.no`).

name - Enter a user-friendly display name for the IdP (in English).

certFilePath - Enter the full path on the video portal server where the SAML certificate is stored, including the file name. Make sure the certificate file does not contain comment lines like `-----BEGIN CERTIFICATE-----` or `-----END CERTIFICATE-----`.

certFileContent - Use this field as an alternative to `certFilePath`. Paste the content of the `.crt` file without the comment lines (for example, **do not paste in**: `-----BEGIN CERTIFICATE-----` **and** `-----END CERTIFICATE-----`). Ensure all text is in a single line, and leave `certFilePath` empty if using this field.

attributes

userIdAttribute - (Optional) The SAML attribute containing the user id. When blank, NameID element will be used. Example: urn:oid:1.3.6.1.4.1.5923.1.1.1.6

firstNameAttribute - (Optional) The SAML attribute containing the first name. Example: urn:oid:2.5.4.42

lastNameAttribute - (Optional) The SAML attribute containing the last name. Example: urn:oid:2.5.4.4

emailAttribute - (Optional) The SAML attribute containing the email. Example: urn:oid:0.9.2342.19200300.100.1.3

logoutUrlAttribute - (Optional) The SAML attribute containing the logout URL. Example: urn:oid:0.9.2342.19200300.100.1.3 When configured, if useInternalLogoutPage is set to No, the value passed in the attribute will be used instead of the value set in logoutRedirectUrl.

defaultRole

In the defaultRole section, select the default role that should be assigned to each user that is authenticated.

You can configure the option to retrieve the role of the user from the Identity Provider through the Auth module **refreshRoleOnLogin** setting every time a user logs in. This option allows you also, to define a default role for all users and then manually override the role through the MediaSpace user management section.

allowDefaultRole - Set to 'Yes' or 'No'.

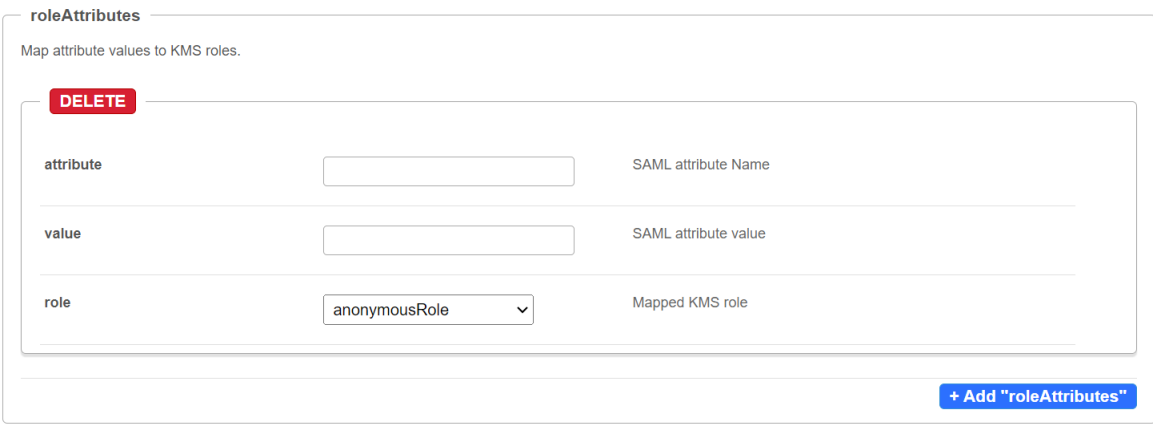
role - Select the default role that should be assigned to each user that is authenticated. Choose from the following options:

- viewerRole
- privateonlyRole
- adminRole
- unmoderatedAdminRole

roleAttributes

Click **+Add "roleAttributes** to map attribute values to video portal roles.

An additional section displays:



Configure the following:

attribute - Enter the SAML attribute name.

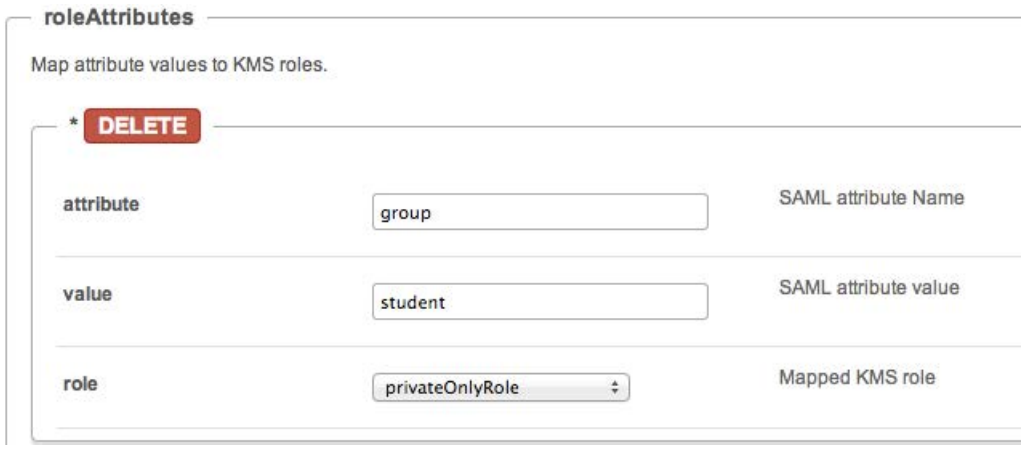
value - Enter the SAML attribute value.

role - Choose the mapped video portal role from the following options:

- anonymousRole
- viewerRole
- privateonlyRole
- adminRole
- unmoderatedAdminRole
- emptyRole
- partnerRole

If more than one attribute value is found (a user belongs to multiple groups) the user will be mapped to the role that was defined in the last roleAttribute found.

In the following example the SAML response will be parsed to find an attribute named group. If the attribute is found in the assertion and its value is student, the user will get the privateOnlyRole.



roleAttributesCsv

Complete the following values:

roleAttributesCsv - Map attribute values to video portal roles. Each CSV row should include three values: attributeName, attributeValue, and videoportalRole. Invalid video portal roles would not be saved.

Click **Load a new CSV** to upload a CSV with role attributes.

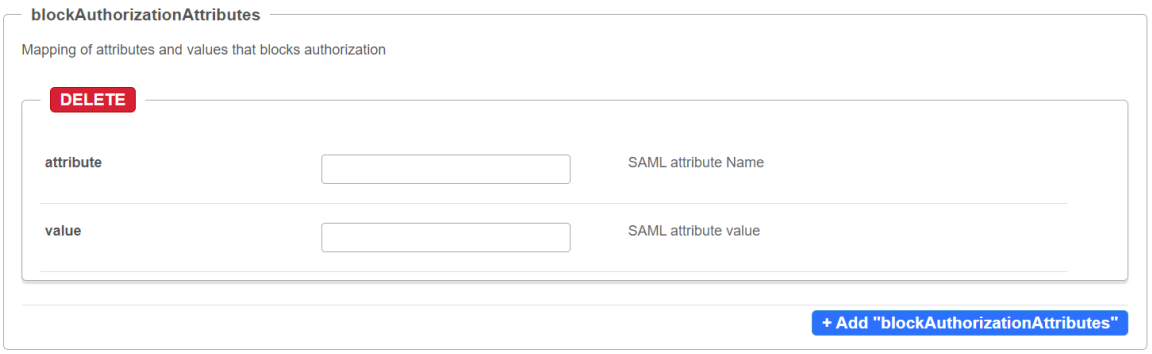
storageDataEntryId - Enter the data entry ID that stores the parsed csv data

blockAuthorizationAttributes

In the blockAuthorizationAttributes (optional), you can map individual groups and values that are returned in the SAML response and should lead to unauthorizing an authenticated user from using the video portal.

Click **+Add "blockAuthorizationAttributes"**.

A new section displays:



Complete the following:

attribute - Enter the SAML attribute name.

value - Enter the SAML attribute name.

unauthorizedBehavior

The **unauthorizedBehavior** (optional) is applicable only if the **blockAuthorizationAttributes** is used. If the field **usersuseInternalUnauthorizedPage** is in use (set to ‘Yes’), you can optionally set the text to be presented to the unauthorized user. If **usersuseInternalUnauthorizedPage** is not used, you can specify the URL where the user will be redirected to.

Complete the following values:

usersuseInternalUnauthorizedPage - Default is 'Yes'. If set to 'No', **unauthorizedRedirectUrl** will be used.

unauthorizedRedirectUrl - (Optional) The URL to redirect the authenticated, but unauthorized users. Should be used only in cases where the customer wants authenticated users to be redirected to his self hosted page.

unauthorizedText - (Optional) Enter the text to be shown in the internal unauthorized page. Leave empty to use the default text.

nameIdStructureAsArray - Specify whether to construct the Name ID attribute as an array when building a SAML Logout Request (leave empty to use as a string).

3. Click **Save**.