# SAML

Last Modified on 12/28/2020 10:23 pm IST

Please see the Kaltura MediaSpace™ SAML Integration Guide (https://knowledge.kaltura.com/help/kaltura-mediaspace-saml-integration-guide) for the setup configuration.

This module allows you to allow users to Authenticate into MediaSpace using the SAML 2.0 standard.

1. In the SAML module configuration, select Yes to enable the SAML module.
2. Enter values for the following:

| Parameter | Description |
|---|---|
| metadataMode | Select Manual or Automatic. |
| enableMultiIdp | Enable using multiple IDPs (requires MultiAuth to be enabled) |
| loginRedirectUrl | The URL to redirect the user when authentication is required (relevant only if metadata mode is set to Manual). |
| logoutRedirectUrl | The URL to redirect the user after logo.<br><br>NOTE: This field is only applicable if useInternalLogoutPage is set to "No" and metadataMode is set to "Manual". When the MediaSpace session expires, the user is redirected to this URL, along with a SAML logout request. This request is made via POST request.<br><br>MediaSpace does not expire login session from the identity provider. For the logout request, MediaSpace uses the value that was provided in the NameID element in the SAML login request. |
| relayStateUrlParam | The parameter name that the IdP uses to pass the URL to redirect the user back after a successful login. This defines the default place to redirect the user to in case it is not passed as part of request. For example for PingFederate it would be TARGET. For other SAML providers it is typically RelayState. |
| enableMetadataEndPoint | Customers that require a standard XML response that exposes the metadata configured on the Service Provider side, can use this configuration. This will expose the configured parameters of the SAML module through the following URL: http://[MediaSpace Server]/saml/index/sp-metadata |
| useInternalLogoutPage | If set to “Yes” logout will expire the MediaSpace session and display message to user but will not redirect to IdP logout page. For example:<br>  <br> |
| allowKeepAlive | When Yes, session will be extended upon user's interaction. Default is No. |
| | If useInternalLogoutPage is set to Yes you can define a custom message to users. |

| Parameter | Description |
| --- | --- |
| logoutText | You can use HTML tags to display a message. |
| shouldNestRelayState | Select whether to concatenate the relay state as query-string or as URL-encoded query string. |
| shouldPost | When set to Yes, the SAML request will be posted instead of using get. Default is No. |
| shouldDecodeRelayState | When set to Yes, RelayState will be decoded before redirect.. |
| name | The entity ID of the service provider (MediaSpace) 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 | The host of the MediaSpace instance. For example: partner_id.mediaspace.kaltura.com.<br><br>NOTE: The host may be configured only with a single URL per KMS instance. If you are using your own alias for MediaSpace (for example: video.company.com) you should use that alias. |
| relayState | 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 | Transient<br>This field is used for SP initiated mode only and will not work if the NameID is not released.<br>• Transient - Recommended for Shibboleth setup<br>• Persistent - Preferred setup.<br>• None - set to remove the NameIDPolicy element from the SAML request. |
| certificate - (optional) | When encryption is required for the SAML response, enter the certificate information. Paste the content of the crt file without the comments line. See Generating a Certificate Workflow (https://knowledge.kaltura.com/help/kaltura-mediaspace-saml-integration-guide#generating-a-certificate-workflow).<br><br>NOTE: You should paste the content without the 2 comment lines:<br><br>(----*BEGIN*… and -----*END*…)<br><br>All text should be in a single line with no spaces, so remove all the breaklines in the generated file<br><br>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: |

| | |
|---|---|
| | <pre>-----BEGIN CERTIFICATE-----<br>MIICsDCCAhmgAwIBAgIJALM+uZK9gWbQMA0GCSqGSIb3DQEBBQUAMEUxCzAJBgNV<br>BAYTAkFVMRMwEQYDVQQIEwpTb21lLVN0YXRlMSEwHwYDVQQKExhJbnRlcm5ldCBX<br>aWRnaXRzIFB0eSBMdGQwHhcNMTMwNDI0MDgzOTU1WhcNMjMwNDI0MDgzOTU1WjBF<br>MQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50<br>ZXJuZXQgV2lkZ2l0cyBQdHkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB<br>gQC3Pkd3p+a9Yy0TFHuwy6trDlxhKwa0FAwrGlBnJCw4V+XgL5JaymRqICo1Vrk3<br>MEXFD1hf5GuG17Sm1CXA02XAdzJMemr8RcLjq5dqAPP+6ZZ+3JM9owjvy1LRhMMP<br>wCUBDeCI3WNvmNDCpnoJp+mBIgyZpr87ecgaCt2626CRKQIDAQABo4GnMIGkMB0G<br>A1UdDgQWBBTODBaXbjmbJUJ1+gnD7CFKECmp9jB1BgNVHSMEbjBsgBTODBaXbjmb<br>JUJ1+gnD7CFKECmp9qFJpEcwRTELMAkGA1UEBhMCQVUxEzARBgNVBAgTClNvbWUt<br>U3RhdGUxITAfBgNVBAoTGEludGVybmV0IFdpZGdpdHMgUHR5IEx0ZIIJALM+uZK9<br>gWbQMAwGA1UdEwQFMAMBAf8wDQYJKoZIhvcNAQEFBQADgYEAo6LDQVKjODxoL7N/<br>CXTDMDnZ74gXLnZfOWh4RSQZzg/N5JpHt7RH4KTKpc/uWf0cUVRhUED4Vx3K/hlO<br>rr8I7ylh6hpD2T8Ecmimx8oXieGrVU5ZuIsMaFxDJFeIvzq6+KtYz+ZaIx2wc6tJ<br>RCe3NZLDKW3WvwgjKdY+YyOkaTs=<br>-----END CERTIFICATE-----</pre> |
| privateKey - (optional) | (Optional) SP Private Key PEM format. The privateKey value is used to decrypt the response provided by the IdP.<br><br><pre>-----BEGIN RSA PRIVATE KEY-----<br>MIICXQIBAAKBgQC3Pkd3p+a9Yy0TFHuwy6trDlxhKwa0FAwrGlBnJCw4V+XgL5Ja<br>ymRqICo1Vrk3MEXFD1hf5GuG17Sm1CXA02XAdzJMemr8RcLjq5dqAPP+6ZZ+3JM9<br>owjvy1LRhMMPwCUBDeCI3WNvmNDCpnoJp+mBIgyZpr87ecgaCt2626CRKQIDAQAB<br>AoGAURW1+jTJ3bQtFexSb4EwcUcBid3IMZdNayVRvtI63xPGHNXwJUy58lwZUVD2<br>1Hz/4ptPt98T1a9NuSTXL+RbeXaOFI5nPXQvIV62IsOVrg1l1SkKedkWKM3EPesx<br>iACqtC3xOaV+kjDS1R7x5MNXroMHM/tOKg9xfjmlmckisyECQQDwRh0NSTNGKHEA<br>gNA6TqO3X4G9VkYWE1/KT9MQyc2k41LrKLXD9nd39kgHb7lkozq5r+KmVNo2nki3<br>mqijZ0aTAkEAwzyYQik8pRkFlBH/UDYLJ96wuGrqYjvQO+94WWzWCZPXBPBlOY5g<br>KG+l5WMfIpvHwsbd0iPaZeCax0INW6LC0wJATRNAuIVVxFiuvymTIlEdpXImrTTi<br>sKwwWza2DzmdFRqy+6qIfD8w3bOMMY5+WzEdYnlwbEjl4wVtcDBVjm1PrwJBALu/<br>VrAxFaeys0GcOQi6n+m8ZfdCoZjL6kjo1bQxTHczW4/dWYqK1v+rtj4sHvHaGrS9<br>Ju2BGvHjlxRM+amIkI8CQQCHQNwIyVzMvJxnlHGO0Sz04vKPs4xSVegYmOL3JPOt<br>Rr7FMzBMRp46CSa6p38k4ZnAqP7LvoWWci/AvKvjz/xE<br>-----END RSA PRIVATE KEY-----</pre> |
| host | The entity ID of the identity provider. For example: https://openidp.feide.no |
| issuer | The entity ID of the identity provider. For example: https://openidp.feide.no |
| name | Friendly display name for the Identity |
| certFilePath | Provider (only for self-hosted MediaSpace) The absolute file system path of the crt file provided by Identity Provider. |
| certFileContent | The content of the certification file provided by Identity Provider that is used to validate the signature of the response. |

Complete the following values in the attributes section:

| Parameter | Description |
|---|---|
| userIdAttribute | The SAML attribute containing the user ID. When blank, NameID element will be used. |
| firstNameAttribute | The SAML attribute containing the first name. |
| lastNameAttribute | The SAML attribute containing the last name. |
| emailAttribute | The SAML attribute containing the email. |
| logoutUrlAttribute | The SAML attribute containing the logout URL. When configured, if useInternalLogoutPage is set to No, the value passed in the attribute will be used instead of the value set in logoutRedirectUrl. |

Complete the following values in the defaultRole section:

| Parameter | Description |
|---|---|
| defaultRole | The default role for authenticated SAML user. |
| allowDefaultRole | Select Yes or No. |
| role | Select the default role that should be assigned to each user that is authenticated. |

Complete the following values in the roleAttributes  section:

| Parameter | Description |
|---|---|
| roleAttributes | Map attribute values to KMS roles. |
| attribute | The SAML attribute name. |
| value | The SAML attribute value |
| role | Mapped KMS role. |

**NOTE:** 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.

Complete the following values in the roleAttributesCsv section:

| Parameter | Description |
|---|---|
| | |

| Parameter | Description |
|---|---|
| roleAttributesCsv | Map attribute values to KMS roles. Each CSV row should contain 3 values: attributeName,attributeValue,mediaSpaceRole. Invalid MediaSpace roles would not be saved. |
| Load new CSV | Click to upload a CSV with role attributes. |
| storageDataEntryId | Data entry ID that stores the parsed csv data |

In the blockAuthorizationAttributes (optional) map individual groups and values that are returned in the SAML response and should lead to unauthorizing an authenticated user from using MediaSpace. Complete the following values in the blockAuthorizationAttributes section: (Optional)

| Parameter | Description |
|---|---|
| blockAuthorizationAttributes | Mapping of attributes and values that blocks authorization |
| attribute | The SAML attribute name. |
| value | The SAML attribute value |

The unauthorizedBehavior is applicable only if the blockAuthorizationAttributes is used. If 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 in the unauthorizedBehavior section: (Optional)

| Parameter | Description |
|---|---|
| unauthorizedBehavior | Mapping of attributes and values that blocks authorization |
| useInternalUnauthorizedPage | 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) Text to be shown in the internal unauthorized page, leave empty to use the default text. |

From the MediaSpace Configuration Management, Go to the Auth (https://knowledge.kaltura.com/help/auth) module.

For SP Initiated configuration enter:

- Saml_Model_SpInitiated in the authNAdapter text box and click Add custom value
- Saml_Model_SpInitiated in the authZAdapter text box and click Add custom value

For IdP Initiated configuration enter:

- Saml_Model_IdpInitiated in the authNAdapter text box and click Add custom value
- Saml_Model_IdpInitiated in the authZAdapter text box and click Add custom value