# SAML integration guide

Last Modified on 10/12/2024 9:48 am IDT

This article is designated for administrators.

## About

This guide explains how to configure the SAML module in the video portal for authentication and authorization. It's designed for Kaltura partners, community members, and customers familiar with SAML and authentication terminology.

## What is SAML in Kaltura's Video Portal?

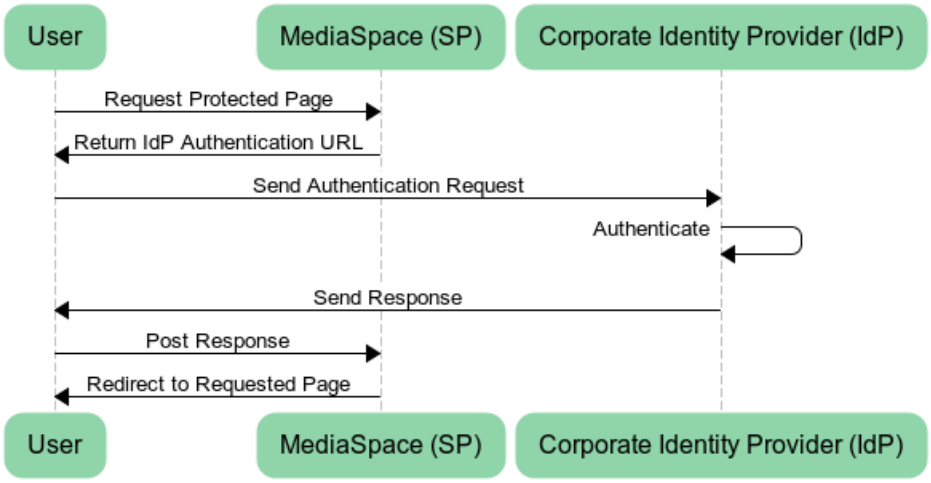
SAML authentication in Kaltura's video portal platform allows users to log in using their organization's SAML-based Identity Provider (IdP) credentials. This means users don't need separate credentials for the video portal. When SAML is enabled, other authentication methods are disabled.

The video portal's SAML module supports SAML 2.0 only. Older Identity Providers that use SAML 1.0 or 1.1 are not compatible.

A user's role in the video portal is determined by their membership in organizational groups and specific attributes defined in the SAML response from the IdP. Roles can be configured and mapped in the SAML module settings. For information about video portal roles, please see our article Video Portal and KAF roles and permissions.

## SP initiated authentication

Below are the steps involved in the Service Provider-initiated SAML authentication flow.

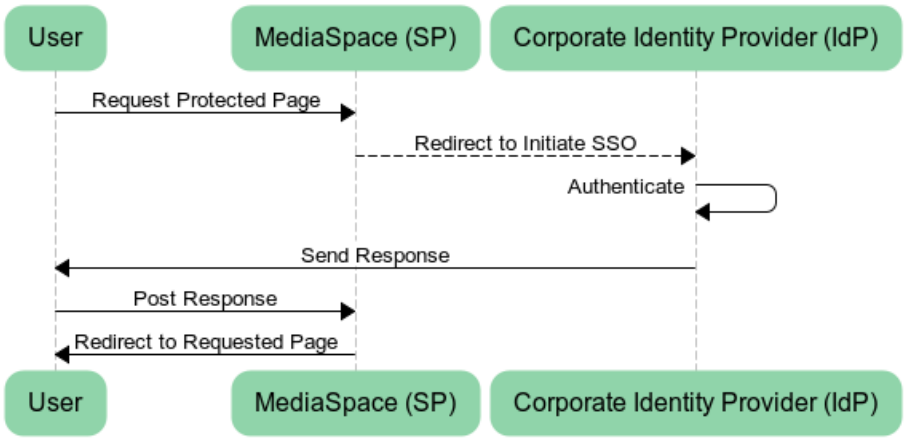


### Processing steps

1. The user requests access to a video portal page that requires authentication.
2. The video portal builds an authentication request and the user's browser sends it to the IdP.
3. On a successful authentication, the IdP returns an HTML form to the browser with a SAML response.
4. The browser automatically posts the HTML form back to the video portal.
5. The video portal processes the response and redirects the user to the requested page.

## IdP initiated authentication

The following outlines the steps in the Identity Provider-initiated SAML authentication flow.




### Processing steps

1. The user requests access to a video portal page that requires authentication.
2. The video portal redirects the user to a URL on the IdP for authentication.
3. Upon successful authentication, the IdP returns an HTML form to the browser with a SAML response.
4. The browser automatically posts the HTML form back to the video portal.
5. The video portal processes the response and redirects the user to the requested page.

## SAML authorization in the video portal

A user's role in the video portal is determined by their membership in organizational groups and specific attributes defined in the SAML response from the IdP. Roles can be configured and mapped in the SAML module settings.

## Configuring SAML in the video portal

Follow the steps below to set up authentication in your video portal.

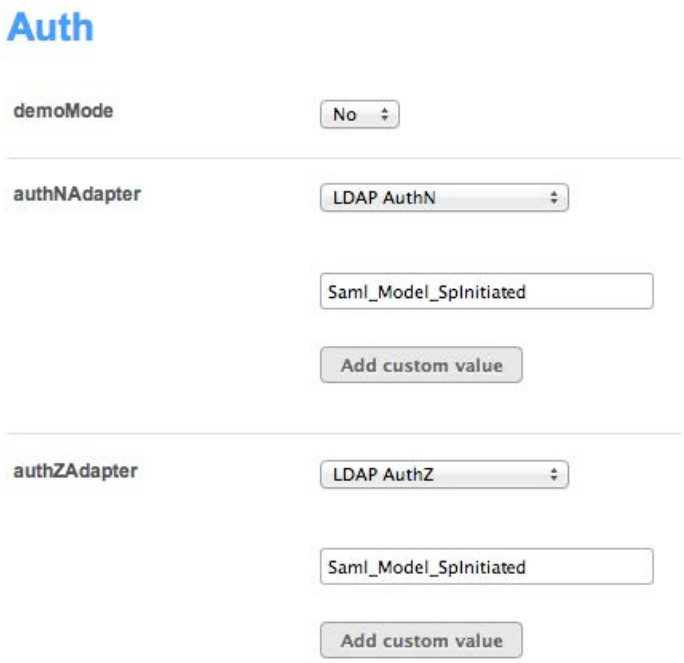
### Step 1: Configure the Saml module

Please visit our article Saml module for directions.

### Step 2: Configure the 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**.

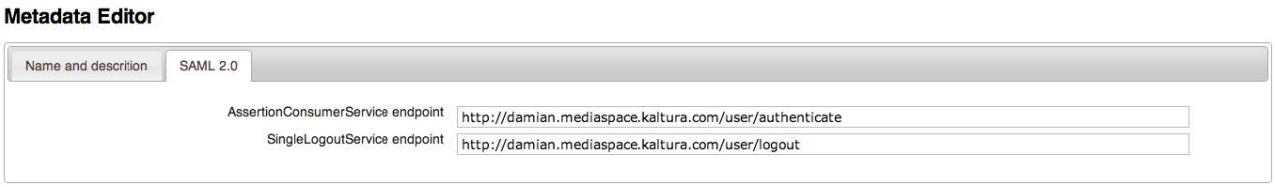
The Identity Provider should be configured accordingly to support authentication requests from the video portal.

Please visit our article Auth module for more information.

## Example configuration using TestIDP (SimpleSAMLphp)

The following example shows a configuration using TestIDP (SimpleSAMLphp) https://openidp.feide.no:


The following shows the URLs that should be configured for authentication and logout:




## Generating a certificate workflow

You can generate a certificate for SAML authentication using the following steps:

### From Linux / Mac

1. Open a terminal window and execute the following command:

```
openssl req -new -x509 -days 3652 -nodes -out example.org.crt -newkey rsa:2048 -keyout example.org.pem
```

2. Follow the command line prompts to enter additional data. When prompted for **Common Name**, enter the name used to generate the key (for example, `example.org`).

```
>openssl req -new -x509 -days 3652 -nodes -out example.org.crt -newkey rsa:2048 -keyout example.org.pem
Generating a 2048 bit RSA private key
.....................................+++
.............+++
writing new private key to 'example.org.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:New York
Locality Name (eg, city) []:New York
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Kaltura
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:example.org
Email Address []:
```

3. The following files will be generated:

**example.org.crt**: The certificate containing the public key.

**example.org.pem**: The private key file.

When copying the content of the .crt or .pem files into the SAML module, **do not include the comment lines**:
-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----

### From Windows

Use OpenSSL. After downloading and extracting the package, execute the following from a command line in the extracted folder:

```
req –new –x509 –days 3652 –nodes –config
c:\openssl\openssl.cnf –out
example.org.crt –keyout example.org.pem
```

Both suggested options will generate two files:

- example.org.crt – This is the certificate containing the public key.
- example.org.pem – This is the private key. Please note that this file must be protected.

When copying the content of the .crt or .pem files into the SAML module, **do not include the comment lines**:
-----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----
-----BEGIN RSA PRIVATE KEY----- and -----END RSA PRIVATE KEY-----

## SAML response example

The certificate and key content in this SAML response are for illustration purposes only. When using your own certificate or private key, **do not include the following comment lines**:

-----BEGIN CERTIFICATE-----

-----END CERTIFICATE-----

-----BEGIN RSA PRIVATE KEY-----

-----END RSA PRIVATE KEY-----

These comment lines are automatically added by OpenSSL when generating the files but should be removed before pasting the content into the SAML module.

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
ID="_3ab056b68b199b976b49198cfa6b9e28b0317c4c6a" Version="2.0" IssueInstant="2013-04-
24T08:51:16Z" Destination="http://damian.mediaspace.kaltura.com/user/authenticate"
InResponseTo="_8d32fa51f5ef2b70fe6d619000c5aedb143bfb937c">
<saml:Issuer>https://openidp.feide.no</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference
URI="#_3ab056b68b199b976b49198cfa6b9e28b0317c4c6a">
<ds:Transforms>
<ds:Transform
Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>pTsLnZhfAW6Zn/LRxATMmed1zag=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>iN+urKe/LFlwPyRCgvAY85QvDDSUb43vx8Rk7UpSKO/mGdcoJJNkc/GUBpUtEopqBDbCFE4HQX5
Gr8rMWdEgLV9oTyYLmCKrRSyIewsx8flL/w6swcCKTVWph1lnLGgqXOr7DSTpj0TvsQQPygifovbvc9rh6g72ONJPEj84g
sQ=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBg
NVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECxMFRmVpZGUxGTAXBgNVBAMTEG9wZW5p
ZHAuZmVp
ZGUubm8xKTAnBgkqhkiG9w0BCQEWGmFuZHJlYXMuc29sYmVyZ0B1bmluZXR0Lm5vMB4XDTA4MDUwODA5MjI0OFoXD
TM1MD
kyMzA5MjI0OFowgYkxCzAJBgNVBAYTAk5PMRIwEAYDVQQIEwlUcm9uZGhlaW0xEDAOBgNVBAoTB1VOSU5FVFQxDjAMBg
NV
BAsTBUZlaWRlMRkwFwYDVQQDExBvcGVuaWRwLmZlaWRlLm5vMSkwJwYJKoZIhvcNAQkBFhphbmRyZWFzLnNvbGJlcmd
AdW
5pbmV0dC5ubzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8jLoqI1VTlxAZ2axiDIThWcAOXdu8KkVUWaN/SooO9O
0QQ7KRUjSGKN9JK65AFRDXQkWPAu4HlnO4noYlFSLnYyDxI66LCr71x4lgFJjqLeAvB/GqBqFfIZ3YK/NrhnUqFwZu63nL
rZjcUZxNaPjOOSRSDaXpv1kb5k3jOiSGECAwEAATANBgkqhkiG9w0BAQUFAAOBgQBQYj4cAafWaYfjBU2zi1ElwStIaJ5n
yp/s/8B8SAPK2T79McMyccP3wSW13LHkmM1jwKe3ACFXBvqGQN0IbcH49hu0FKhYFM/GPDJcIHFBsiyMBXChpye9vBaTNE
BCtU3KjjyG0hRT2mAQ9h+bkPmOvlEo/aH0xR68Z9hw4PF13w==</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
```

<samlp:Status>
<samlp:StatusCode
Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<saml:Assertion xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xs="http://www.w3.org/2001/XMLSchema" ID="_37b2602c8e0327a7896367288c195e0982fea1e511"
Version="2.0" IssueInstant="2013-04-24T08:51:16Z">
<saml:Issuer>https://openidp.feide.no</saml:Issuer>
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
<ds:SignedInfo>
<ds:CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
<ds:SignatureMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
<ds:Reference
URI="#_37b2602c8e0327a7896367288c195e0982fea1e511">
<ds:Transforms>
<ds:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
<ds:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
</ds:Transforms>
<ds:DigestMethod
Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
<ds:DigestValue>jVKo/6IZjEllyA5lYjgXxJQ3YmQ=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>
<ds:SignatureValue>NCKBpluggEjdNm7QL16oOrKXUmZQ2eaQbANtyIVqrRs67tUnExRcac3Vrqiso4H/4FQRGdWdS1f
6Yh2uo0psItwzTuPkDrv2QotuWSiAFo54bABDj9Q+wVKBqk1ShgiQ7RCBoJDK1V1k/A7dm7CMCGW2GNYZl8q35tgKccJzv
7o=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
<ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBg
NVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDEOMAwGA1UECxMFRmVpZGUxGTAXBgNVBAMTEG9wZW5p
ZHAuZmVp
ZGUubm8xKTAnBgkqhkiG9w0BCQEWGmFuZHJlYXMuc29sYmVyZ0B1bmluZXR0Lm5vMB4XDTA4MDUwODA5MjI0OFoXD
TM1MD
kyMzA5MjI0OFowgYkxCzAJBgNVBAYTAk5PMRIwEAYDVQQIEwlUcm9uZGhlaW0xEDAOBgNVBAoTB1VOSU5FVFQxDjAMBg
NV
BAsTBUZlaWRlMRkwFwYDVQQDExBvcGVuaWRwLmZlaWRlLm5vMSkwJwYJKoZIhvcNAQkBFhphbmRyZWFzLnNvbGJlcmd
AdW
5pbmV0dC5ubzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8jLoqI1VTlxAZ2axiDIThWcAOXdu8KkVUWaN/SooO9O
0QQ7KRUjSGKN9JK65AFRDXQkWPAu4HlnO4noYlFSLnYyDxI66LCr71x4lgFJjqLeAvB/GqBqFflZ3YK/NrhnUqFwZu63nL
rZjcUZxNaPjOOSRSDaXpv1kb5k3jOiSGECAwEAATANBgkqhkiG9w0BAQUFAAOBgQBQYj4cAafWaYfjBU2zi1ElwStIaJ5n
yp/s/8B8SAPK2T79McMyccP3wSW13LHkmM1jwKe3ACFXBvqGQN0IbcH49hu0FKhYFM/GPDJcIHFBsiyMBXChpye9vBaTNE
BCtU3KjjyG0hRT2mAQ9h+bkPmOvlEo/aH0xR68Z9hw4PF13w==</ds:X509Certificate>
</ds:X509Data>
</ds:KeyInfo>
</ds:Signature>
<saml:Subject>
<saml:NameID
SPNameQualifier="damian.mediaspace.kaltura.com" Format="urn:oasis:names:tc:SAML:2.0:nameidformat:
transient">_18d5ad80174e8498d0703c9f5b1976566a50704f9f</saml:NameID>
<saml:SubjectConfirmation
Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
<saml:SubjectConfirmationData
NotOnOrAfter="2013-04-24T08:56:16Z"
Recipient="http://damian.mediaspace.kaltura.com/user/authenticate"
InResponseTo="_8d32fa51f5ef2b70fe6d619000c5aedb143bfb937c"/>
</saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2013-04-24T08:50:46Z"
NotOnOrAfter="2013-04-24T08:56:16Z">
<saml:AudienceRestriction>

<saml:Audience>damian.mediaspace.kaltura.com</saml:Audience>
</saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2013-04-24T08:51:16Z"
SessionNotOnOrAfter="2013-04-24T16:51:16Z"
SessionIndex="_2b2053d785ab116b42ca5e57a9e9a7a40ff1673895">
<saml:AuthnContext>
<saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnContextC
lassRef>
</saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement>
<saml:Attribute Name="uid"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">roman-kreichman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="givenName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">Roman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="sn"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">Kreichman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="cn"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">Roman Kreichman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="mail"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">roman.kreichman@kaltura.com</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="eduPersonPrincipalName"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">roman-kreichman@rnd.feide.no</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="eduPersonTargetedID"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">bdb1871794ce63c792caa42adc93f233df652e01</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
Name="urn:oid:0.9.2342.19200300.100.1.1" NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
uri">
<saml:AttributeValue
xsi:type="xs:string">roman-kreichman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:oid:2.5.4.42"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">Roman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:oid:2.5.4.4"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">Kreichman</saml:AttributeValue>

```
xsi:type="xs:string">Kreichman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:oid:2.5.4.3"
NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri">
<saml:AttributeValue
xsi:type="xs:string">Roman Kreichman</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
Name="urn:oid:0.9.2342.19200300.100.1.3" NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
uri">
<saml:AttributeValue
xsi:type="xs:string">roman.kreichman@kaltura.com</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.6" NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
uri">
<saml:AttributeValue
xsi:type="xs:string">roman-kreichman@rnd.feide.no</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute
Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.10" NameFormat="urn:oasis:names:tc:SAML:2.0:attrnameformat:
uri">
<saml:AttributeValue
xsi:type="xs:string">bdb1871794ce63c792caa42adc93f233df652e01</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</samlp:Response>
```


[template("cat-subscribe")]