

Kaltura MediaSpace™ SAML Integration Guide

Version: 5.0

Kaltura Business Headquarters

200 Park Avenue South, New York, NY. 10003, USA

Tel.: +1 800 871 5224

Copyright © 2014 Kaltura Inc. All Rights Reserved. Designated trademarks and brands are the property of their respective owners.

Use of this document constitutes acceptance of the Kaltura Terms of Use and Privacy Policy.

Contents

Preface	4
About this Guide	4
Audience	4
Document Conventions.....	4
Related Documentation	5
Section 1 Understanding SAML Implementation in Kaltura MediaSpace.....	6
Understanding SAML Authorization in MediaSpace.....	6
Understanding the SAML Authentication Flow	6
Service Provider Initiated Authentication	6
Identity Provider (IdP) Initiated Authentication	7
Understanding the SAML Authorization Flow	8
Section 2 Configuring SAML in MediaSpace	9
Identity Provider (IdP) Metadata Details	9
SAML Authentication Configuration Steps.....	11
Generating a Certificate Workflow	15
SAML Response Example	15

Preface

This preface contains the following topics:

- [About this Guide](#)
- [Audience](#)
- [Document Conventions](#)
- [Related Documentation](#)

About this Guide

This guide describes how to configure the [Security Assertion Markup Language \(SAML\)](#) module in Kaltura MediaSpace™ (KMS) Version 4.x and 5.x.



NOTE: Please refer to the official and latest product release notes for last-minute updates. Technical support may be obtained directly from: [Kaltura Customer Care](#).

Contact Us:

Please send your documentation-related comments and feedback or report mistakes to knowledge@kaltura.com.

We are committed to improving our documentation and your feedback is important to us.

Audience

This guide is intended for Kaltura partners, community members, and customers who want to understand and configure SAML authentication and authorization in MediaSpace.

To understand this information, you need to be familiar with SAML, authentication and authorization terminology.

Document Conventions

Kaltura uses the following admonitions:

- Note
- Workflow



NOTE: Identifies important information that contains helpful suggestions.



Workflow: Provides workflow information.

1. Step 1
2. Step 2

Related Documentation

In addition to this guide, the following product documentation is available:

- [Kaltura MediaSpace](#)
- [Kaltura MediaSpace Setup Guide](#)
- [Kaltura MediaSpace: Introduction to Authentication and Authorization Solutions](#)



NOTE: Please remember to review all product [release notes](#) for known issues and limitations.

Understanding SAML Implementation in Kaltura MediaSpace

SAML authentication in MediaSpace enables users to log into MediaSpace using their credentials from an organizational SAML based Identity Provider. A user does not require an additional set of credentials for MediaSpace.

When MediaSpace is configured to authenticate using SAML, other authentication methods are disabled.



NOTE: The MediaSpace SAML module supports SAML 2.0. Older Identity Providers that work with SAML 1.0 or SAML 1.1 are not supported by this module.

Understanding SAML Authorization in MediaSpace

A user's *application role* determines the MediaSpace actions that the user is authorized to do. When SAML is used for authorization in MediaSpace, the user's application role is based on membership in organizational groups and specific attribute in the [SAML response](#). The organizational groups are managed in the organization's Identity Provider.

To learn more about the MediaSpace application role, refer to Understanding Application Roles in the [Kaltura MediaSpace Setup Guide](#).

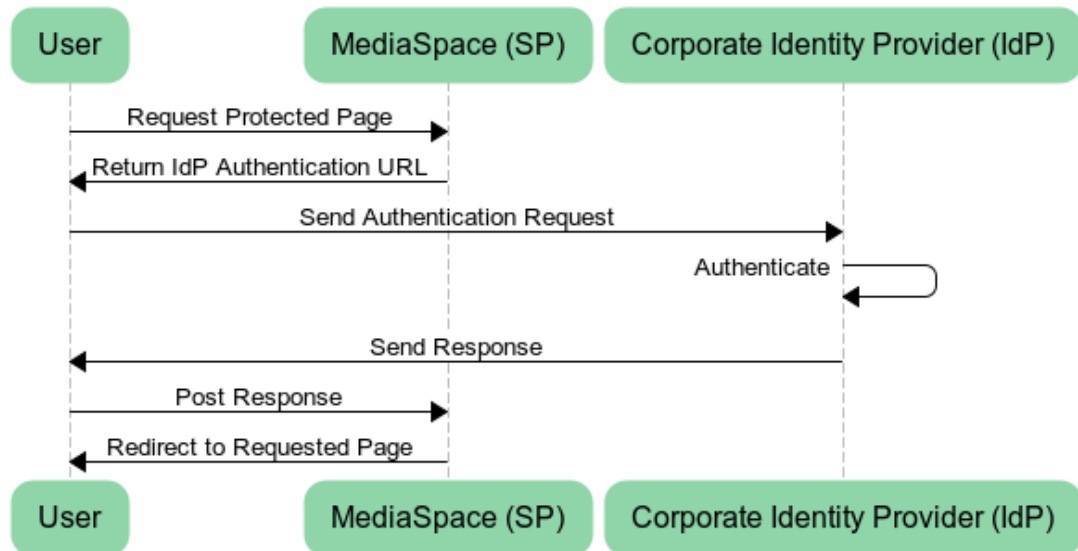
Understanding the SAML Authentication Flow

There are two types of SAML authentication:

- [Service Provider Initiated Authentication](#)
- [Identity Provider \(IdP\) Initiated Authentication](#)

Service Provider Initiated Authentication

In this workflow the user attempts to access a resource on MediaSpace that requires authentication. MediaSpace, the Service Provider ("SP") sends an authentication request to the Identity Provider ("IdP"). Both the request and the response are sent through the users' browser via HTTP Get.

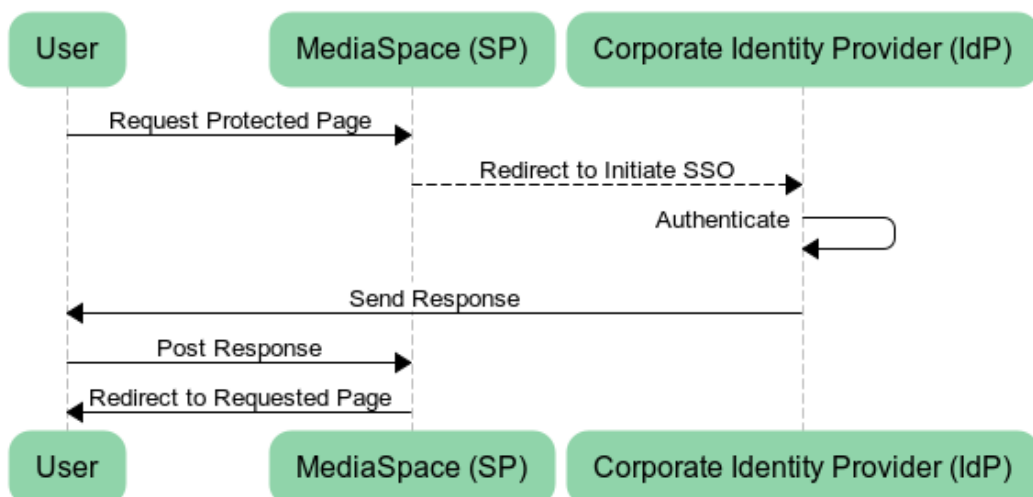


Processing Steps:

1. The user requests access to a MediaSpace page that requires authentication.
2. MediaSpace builds a request and the user's browser sends it to the IdP to handle the authentication.
3. On a successful authentication, The IDP returns an HTML form to the browser with a [SAML response](#). The browser automatically posts the HTML form back to MediaSpace.
4. MediaSpace redirects the user to the requested page.

Identity Provider (IdP) Initiated Authentication

In this workflow the entries process is handled by the Identity Provider. MediaSpace will redirect the user to an external URL that handles the authentication and redirects the user back to MediaSpace.





Processing Steps:

1. The user requests access to a MediaSpace page that requires authentication.
2. MediaSpace redirects the user to a URL on the IdP to handle authentication.
3. On a successful authentication, the IDP returns an HTML form to the browser with a [SAML response](#). The browser automatically posts the HTML form back to MediaSpace
4. MediaSpace redirects the user to the requested page

Understanding the SAML Authorization Flow

Depending on your [MediaSpace SAML configuration](#), MediaSpace queries attributes in the SAML response to determine the MediaSpace application role of the authenticated user. You can define a default role for authenticated users and map specific attributes and values to a MediaSpace role in the SAML module configuration.

Configuring SAML in MediaSpace

This section describes the IdP Metadata Details and provides information on how to set up the SAML module for SP initiated and IdP initiated configurations.

Identity Provider (IdP) Metadata Details

The following information about the Identity Provider is required to be able to configure the MediaSpace SAML module:

SAML Authentication Mode Select one	<input type="checkbox"/> IdP Initiated <input type="checkbox"/> SP Initiated
If IdP Initiated is used: What is the query string key for the <i>RelayState</i> Parameter?	
Login URL	
Logout URL	
Host Name of IdP	
IdP Issuer Name	
IdP Name	
IdP Certificate	
Is SAML response encryption required?	
Example of SAML XML Response	
Metadata XML (Optional)	
SAML2 Attribute name where the <i>User ID</i> is taken from Note: A persistent and unique user ID for each authenticated user is required. This user ID is used when the user uploads media, comments on media etc. Without this, the user will not be identified properly in MediaSpace.	
SAML2 Attribute name where the <i>First Name</i> is taken from Note: If this information cannot be provided, the display name will be built from the User ID.	
SAML2 Attribute name where the <i>Last Name</i> is taken from Note: If this information cannot be provided, the display name will be built from the User ID	
SAML2 Attribute name where the <i>Email</i> is taken from	

<p>Note: If this information cannot be provided you will not be able to use email notification functionality in MediaSpace.</p>	
<p>Default MediaSpace role for authenticated users</p> <p>Select one:</p>	<p><input type="checkbox"/> viewerRole – User can browse public galleries, is not authorized to upload new content, and does not have a My Media page.</p> <p><input type="checkbox"/> privateOnlyRole – User can upload content to My Media, cannot publish to galleries, and can add media to channels according to entitlements.</p> <p><input type="checkbox"/> adminRole - User can upload content and publish to all galleries.</p> <p><input type="checkbox"/> unmoderatedAdminRole – User can upload content and bypass moderation (when moderation is enabled for an account)</p>
<p>If you can map MediaSpace roles to groups / attributes in the IdP, provide for each group / role the following</p>	<p>SAML2 Attribute Name:</p> <p>SAML Attribute Value:</p> <p>MediaSpace Role:</p>
<p>Provide credentials that can be used to test the configuration. It is best to provide one credential per role.</p> <p>If credentials are not provided we will not be able to test the configuration and authentication.</p>	

The following is an **example** of the metadata provided by the IdP with the information that should be used:

SAML 2.0 IdP Metadata

Here is the metadata that simpleSAMLphp has generated for you. You may send this metadata document to trusted partners to setup a trusted federation.

You can get the metadata xml on a dedicated URL:

<https://openidp.feide.no/simplesaml/saml2/idp/metadata.php>

Metadata

In SAML 2.0 Metadata XML format:

```
<?xml version="1.0"?>
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:ds="http://www.w3.org/2000/09/xmldsig#" entityID="https://openidp.feide.no">
  <md:IDPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
    <md:KeyDescriptor use="signing">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAKGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVUVEOMAwGA1UECjA=
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:KeyDescriptor use="encryption">
      <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        <ds:X509Data>
          <ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAKGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVUVEOMAwGA1UECjA=
        </ds:X509Data>
      </ds:KeyInfo>
    </md:KeyDescriptor>
    <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://openidp.feide.no/simplesaml/saml2/idp/SingleLogoutService.php">
      <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</md:NameIDFormat>
    </md:SingleLogoutService>
    <md:SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://openidp.feide.no/simplesaml/saml2/idp/SSOService.php">
      <md:IDPSSODescriptor>
        <md:ContactPerson contactType="technical">
          <md:GivenName>Feide</md:GivenName>
          <md:SurName>support</md:SurName>
          <md:EmailAddress>support@feide.no</md:EmailAddress>
        </md:ContactPerson>
      </md:IDPSSODescriptor>
    </md:SingleSignOnService>
  </md:EntityDescriptor>
```

In simpleSAMLphp flat file format - use this if you are using a simpleSAMLphp entity on the other side:

```
$metadata['https://openidp.feide.no'] = array (
  'metadata-set' => 'saml20-idp-remote',
  'entityid' => 'https://openidp.feide.no',
  'SingleSignOnService' =>
    array (
      0 =>
        array (
          'Binding' => 'urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect',
          'Location' => 'https://openidp.feide.no/simplesaml/saml2/idp/SSOService.php',
        ),
      'SingleLogoutService' => 'https://openidp.feide.no/simplesaml/saml2/idp/SingleLogoutService.php',
      'certData' => 'MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAKGA1UEBhMCTk8xEjAQBgNVBAgTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVUVEOMAwGA1UECjA=MFRRMjZGUxGTp',
      'NameIDFormat' => 'urn:oasis:names:tc:SAML:2.0:nameid-format:transient',
    );
```

Certificates

Download the X509 certificates as PEM-encoded files.

- idp.crt

SAML Authentication Configuration Steps

Perform the following steps to setup the SAML module both for SP initiated and IdP initiated configurations. Parameters that are relevant or different between methods are noted as such.

Before you begin:

To setup the SAML module for SP initiated and IdP initiated configurations.

Before you begin:

Make sure that the *Forcehttps* is enabled and configured on the MediaSpace instance. SAML authentication will not work if MediaSpace is working over HTTP.

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

Parameter	Description
loginRedirectUrl	<p>The URL where the user will be redirected when authentication is required. 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.</p> <ul style="list-style-type: none"> • SP Initiated Example: https://idp.example.com/identity

Parameter	Description
	<ul style="list-style-type: none"> IdP Initiated Example: https://idp.example.com/identity/UnsolicitedSSO?entityID=mediaspaceentityID
logoutRedirectUrl	<p>The URL where the user will be redirected when logging out from MediaSpace.</p> <p>NOTE: On logout, MediaSpace will always expire the MediaSpace session and then optionally redirect the user to this URL. MediaSpace does not expire login session from the identity provider.</p>
relayStateUrlParam	<p>The parameter <u>name</u> 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 <i>TARGET</i>. For other SAML providers it is typically <i>RelayState</i>.</p>
enableMetadataEndPoint	<p>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: <code>http://[MediaSpace Server]/saml/index/sp-metadata</code></p>
useInternalLogoutPage	<p>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:</p> <div style="background-color: #ffffcc; padding: 5px; border: 1px solid #ccc;"> <p>You have signed out from MediaSpace. For improved security, we recommend that you close all browser windows at the end of your online session.</p> </div>
logoutText	<p>If useInternalLogoutPage is set to Yes you can define a custom message to users. You can use HTML tags to display a message.</p>

3. Complete the following values in the *spMetadata* section:

Parameter	Description
name	<p>The entity ID of the service provider (MediaSpace) as it was configured in your Identity Provider. For example: https://partner_id.mediaspace.kaltura.com </p>
host	<p>The host of the MediaSpace instance. For example: partner_id.mediaspace.kaltura.com. </p> <p>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: <code>video.company.com</code>) you should use that alias.</p>
relayState	<p>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 “TARGET”.</p>
certificate – (optional)	<p>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.</p> <p>NOTE: You should paste the content without the 2 comment lines (----BEGIN... and ----END...)</p> <p>All text should be in a single line with no spaces, so remove all the breaklines in the generated file</p> <p>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:</p>

Parameter	Description
	<pre> -----BEGIN CERTIFICATE----- MIICsDCCAhmgAwIBAgIJALM+uZK9gWbQMA0GCSqGSIb3DQEBAQUAMEUxCzAJBgNV BAYTAkFVMRMwEQYDVQQIEWpTb211LVN0YXRlMSEwHwYDVQQKEWhJbnRlcm5ldCBX aWRnaXRzIFB0eSBMdGQwHhcNMjMwNDI0MDgzOTU1WhcNMjMwNDI0MDgzOTU1WjBF MQswCQYDVQQGEwJBVTETMBEGA1UECBMKU29tZS1TdGF0ZTEhMB8GA1UEChMYSW50 ZXJuzXQgV2lkZ210cyBqdHkgTHRkMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB gQCC3Pkd3p+a9Yy0TFHuwy6trDlxhKwa0FAwrG1BnJCw4V+Xg15JaymRqICo1Vrk3 MEXFD1hf5GuG17Sm1CXA02XAdzJMemr8RcLjq5dqAPP+6ZZ+3JM9owjvylLRhMMP wCUBDeCI3WNvmNDCpnoJp+mBIgyZpr87ecgaCt2626CRKQIDAQABo4GnMIGkMB0G A1UdDgQWBBTODBaXbjmbJUJ1+gnD7CFKECmp9jB1BgNVHSMbjBsgBTODBaXbjmb JUJ1+gnD7CFKECmp9jB1BgNVHSMbjBsgBTODBaXbjmbJUJ1+gnD7CFKECmp9jB1Bg NVHSMbjBsgBTODBaXbjmbJUJ1+gnD7CFKECmp9jB1BgNVHSMbjBsgBTODBaXbjmb U3RhZGUxITAFBgNVBAoTGEIudGVybmV0IFdpZGdpdHMgUHR5IEx0ZiIjALM+uZK9 gWbQMAwGA1UdEwQFMAMBAF8wDQYJKoZIhvcNAQEFBQADgYEAo6LDQVKjODx0L7N/ CXTDMdnZ74gXLnZfOWh4RSQZzg/N5JpHt7RH4KTKpc/uWf0cUVRhUED4Vx3K/h1O rr8I7ylh6hpD2T8Ecmimx8oXieGrVU5ZuIsMaFxDJFeIvzq6+KtYz+ZaIx2wc6tJ Rce3NZLDKW3Wvwgjkdy+YyOkaTs= -----END CERTIFICATE----- </pre>
privateKey – (optional)	<p>Copy paste the pem file as is. The privateKey value is used to decrypt the response provided by the IdP.</p> <pre> -----BEGIN RSA PRIVATE KEY----- MIICXQIBAAKBgQC3Pkd3p+a9Yy0TFHuwy6trDlxhKwa0FAwrG1BnJCw4V+Xg15Ja ymRqICo1Vrk3MEXFD1hf5GuG17Sm1CXA02XAdzJMemr8RcLjq5dqAPP+6ZZ+3JM9 owjvylLRhMMPwCUBDeCI3WNvmNDCpnoJp+mBIgyZpr87ecgaCt2626CRKQIDAQAB AoGAURW1+jTJ3bQtFexSb4EwcUcBid3IMZdNayVRvtI63xPGHNXWJUy58lwZUVD2 1Hz/4ptPt98T1a9NuSTXL+RbeXaOFI5nPXQvIV62IsOVrg111SkKedkWKm3EPesx iACqtC3xOaV+kjDS1R7x5MNXroMHM/tOKg9xfjmlmckisyECQQDWRh0NSTNGKHEA gNA6TqQ3X4G9VkyWE1/KT9MQyc2k41LrKLXD9nd39kgHb7lkozq5r+KmVNo2nki3 mqijZ0aTAkEawzyYQik8pRkF1BH/UDYLJ96wuGrqYjvQO+94WWzWCZPXBpB1OY5g KG+15WMfIpvHwsbd0iPaZeCax0INW6LC0wJATRNaUwVvxFiuvymTlEdpXImrTTi sKwwWza2DzmdFRqy+6qIfd8w3bOMMY5+WzEdYn1wbEj14wVtcDBVjm1PrwJBALu/ VrAxFaeyS0GcOQI6n+m8ZfdCoZjL6kjo1bQxTHczW4/dWYqK1v+rtj4sHvHaGrS9 Ju2BGvHjlxRM+amIkI8CQQCHQNWiyVzMvJxn1HGO0Sz04vKPs4xSVegYmOL3JPOT Rr7FMzBMRp46CSa6p38k4ZnAqP7LvoWWci/AvKvjz/xE -----END RSA PRIVATE KEY----- </pre>

4. Complete the following values in the *idpMetadata* section:

Parameter	Description
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.

5. Complete the following values in the attributes section:

MediaSpace Attribute	Recommended SAML Attribute Name	Required?
userIdAttribute	SAML 2.0 Persistent NameID or urn:oid:1.3.6.1.4.1.5923.1.1.1.6	Yes
firstNameAttribute	urn:oid:2.5.4.42	No
lastNameAttribute	urn:oid:2.5.4.4	No

emailAttribute	urn:oid:0.9.2342.19200300.100.1.3	No
----------------	-----------------------------------	----

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



NOTE: You can configure the option to retrieve the role of the user from the Identity Provider through the *Auth* → *refreshRoleOnLogin* 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.

7. In the **roleAttributes** section, map individual groups and values that are returned in the SAML response to a MediaSpace role. For example:

roleAttributes

Map attribute values to KMS roles.

* **DELETE**

attribute	<input type="text" value="group"/>	SAML attribute Name
value	<input type="text" value="student"/>	SAML attribute value
role	<input type="text" value="privateOnlyRole"/>	Mapped KMS role

In the above 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*.



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.

8. Click on **Save** to apply the settings.
9. From the MediaSpace Configuration Management, Go to the *Auth* module.
- For SP Initiated configuration enter:
- *Saml_Model_SplInitiated* in the *authNAdapter* text box and click **Add custom value**
 - *Saml_Model_SplInitiated* in the *authZAdapter* text box and click **Add custom value**

Auth

demoMode

authNAdapter

authZAdapter

For IdP Initiated configuration enter:

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

10. Click on **Save** to save the settings.

The Identity Provider should be configured accordingly to support authentication requests from MediaSpace.

Example Configuration Using TestIDP (SimpleSAMLphp)

The following example shows a configuration using TestIDP (SimpleSAMLphp)

<https://openidp.feide.no>:

Metadata Editor

Name and description	SAML 2.0
EntityID	damian.mediaspace.kaltura.com
Name of service	http://damian.mediaspace.kaltura.com/
Description of service	Damian's Kaltura MediaSpace
Owner	drochman@rnd.feide.no
Last updated	8. April 2013, 16:37
Expire	Not set

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

Metadata Editor

Name and description	SAML 2.0
AssertionConsumerService endpoint	http://damian.mediaspace.kaltura.com/user/authenticate
SingleLogoutService endpoint	http://damian.mediaspace.kaltura.com/user/logout

Generating a Certificate Workflow



1. From a Linux or a Mac Terminal window execute the following command:

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

2. From Windows, you can 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.

SAML Response Example

```
<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="_8d32fa51f5ef2b70fe6d619000c5aadb143bfb937c">
  <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" />
```

Configuring SAML in MediaSpace

```
<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/LRxATMmedlzag=</ds:DigestValue>
</ds:Reference>
</ds:SignedInfo>

<ds:SignatureValue>iN+urKe/LFlwPyRCgvAY85QvDDSub43vx8Rk7UpSKO/mGdcoJJNkc/GUBpUtEopqBDbCFE4HQX5
Gr8rMWdEgLV9oTyYLMCKrRSyIewsx8f1L/w6swcCKTVWph1lnLGgqXOr7DSTpj0TvsQQPygifovbvc9rh6g72ONJPEj84g
sQ=</ds:SignatureValue>

<ds:KeyInfo>
<ds:X509Data>

<ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBg
NVBAGTCVRyb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDU0MAwGA1UECzMFRmVpZGUXGTAXBgNVBAMTEG9wZW5pZHAuZmVp
ZGUubm8xKTANBgkqhkiG9w0BCQEWGmFuZG9wYXVzOjB1bm1uZXR0Lm5vMB4XDTA4MDUwODA5MjI0OFOxDTM1MD
kyMzA5MjI0OFOwYkxCzAJBgNVBAYTAk5PMRIwEAYDVQQIEWlUcm9uZGhlaW0xEDAOBgNVBAoTB1VOSU5FVFQxZjAMBGNV
BAsTBUZlaWRlMRkwFwYDVQQDExBvcGVuaWRwLmZlaWRlLm5vMSkwJwYJKoZIhvcNAQkBFhphbmRyZWZzLnNvbGJlcmdAdW
5pbmV0dC5ubzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwGykCgYEAt8jLoqI1VtLxAZ2axiDIThWcAOXdu8KkVUWaN/SooO9O
0QQ7KRujSGKN9JK65AFRDxQkWPau4HlnO4noYlFSLnYyDxI66LCr71x4lgFJjqLeAvB/GqBqFfIZ3YK/NrhnUqFwZu63nL
rZjCuzxNaPjOOSRSDaXpvlkb5k3jOiSGECAwEATANBgkqhkiG9w0BAQUFAAOBgQBQYj4cAafWaYfjBU2zi1ElwStIaJ5n
yp/s/8B8SAPK2T79McMyccP3wSW13LHkmM1jwKe3ACFXBvqQQN0IbcH49hu0FKhYFM/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="_37b2602c8e0327a7896367288c195e0982feale511"
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="#_37b2602c8e0327a7896367288c195e0982feale511">
<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>NCKBpIuggEjdNm7QL16oOrKXUmZQ2eaQbAntyIVqrRs67tUnExRcac3Vrqiso4H/4FQRGdWdS1f
6Yh2uo0psItwzTuPkDrv2QotuWSiAFo54bABDj9Q+wVKBqk1ShgiQ7RCBoJDK1V1k/A7dm7CMCGW2GNYZ18q35tgKccJzv
7o=</ds:SignatureValue>
<ds:KeyInfo>
<ds:X509Data>
```



```
<ds:X509Certificate>MIICizCCAfQCCQCY8tKaMc0BMjANBgkqhkiG9w0BAQUFADCBiTELMAkGA1UEBhMCTk8xEjAQBg
NVBAGTCVRYb25kaGVpbTEQMA4GA1UEChMHVU5JTkVUVDIOMAwGA1UECmFMRmVpZGUXGTAXBgNVBAMTEG9wZW5pZHAuZmVp
ZGUubm8xKTANBgkqhkiG9w0BCQEWGmFuZlYXNjYXN5Y29sYmVpZ0B1bm1uZXR0Lm5vMB4XDTA4MDUwODA5MjI0OFoXDTMlMD
kyMzA5MjI0OFowYkxCzAJBGNVBAYTAk5PMRIWEAYDVQqIEwluUcm9uZGhlaW0xEDA0BgNVBAoTB1VOSU5FVFQxDjAMBgNV
BAsTBUZlaWRlMRkwFwYDVQqDExBvcGVuaWRmLmZlaWRlLm5vMSkwJWYJKoZIhvcNAQkBFhphbmRyZWZzLnNvbGJlcmdAdW
5pbmV0dC5ubzCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEAt8jLoqI1VtLxAZ2axiDiThWcAOXdu8KkVUWaN/SooO9O
0QQ7KRujSGKN9JK65AFRDxQkWPau4Hln04noYlFSLnYyDxI66LCr71x4lgFJjqLeAvB/GqBqFfI23YK/NrhnUqFwZu63nL
rZjcUZxNaPjOOSRSDaXpvlkb5k3jOISGECaWEAATANBgkqhkiG9w0BAQUFAAOBgQBQYj4cAafWafYfjBU2ziElwStIaJ5n
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:nameid-
    format: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"
```

Configuring SAML in MediaSpace

```
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:attrname-
format: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>
                                </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:attrname-
format: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:attrname-
format: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:attrname-
format:uri">
                                <saml:AttributeValue
xsi:type="xs:string">bdb1871794ce63c792caa42adc93f233df652e01</saml:AttributeValue>
                                </saml:Attribute>
                                </saml:AttributeStatement>
                        </saml:Assertion>
</samlp:Response>
```