Create and manage SAML profiles in KMC

Last Modified on 02/25/2025 11:46 pm IST

This article is designated for administrators.

About

This article describes how to view a full list of Security Assertion Markup Language (SAML) profiles, create new SAML profiles, edit, and delete SAML profiles in the Kaltura Management Console (KMC).

SAML profiles facilitate authentication between service providers and their configured IdPs. Once authenticated, you may connect the KMC to Auth Broker (a "gateway" that sits on the partner (account) level and manages authentication to Kaltura via external Identity providers (IdP)). Auth Broker works with the Security Assertion Markup Language (SAML) and Open Authorization (OAuth 2.0) protocols. Auth Broker users are "shared users" (users who are shared between applications/instances in the partner).

To learn more about Auth Broker, please see Auth Broker.

Currently, only SAML is supported for self-serve setup.

Prerequisites

To create and manage SAML profiles, you must:

- Either be an IdP Admin or have access to IdP configurations.
- Be logged into the KMC. For instructions on logging into the KMC, see Log into the KMC.

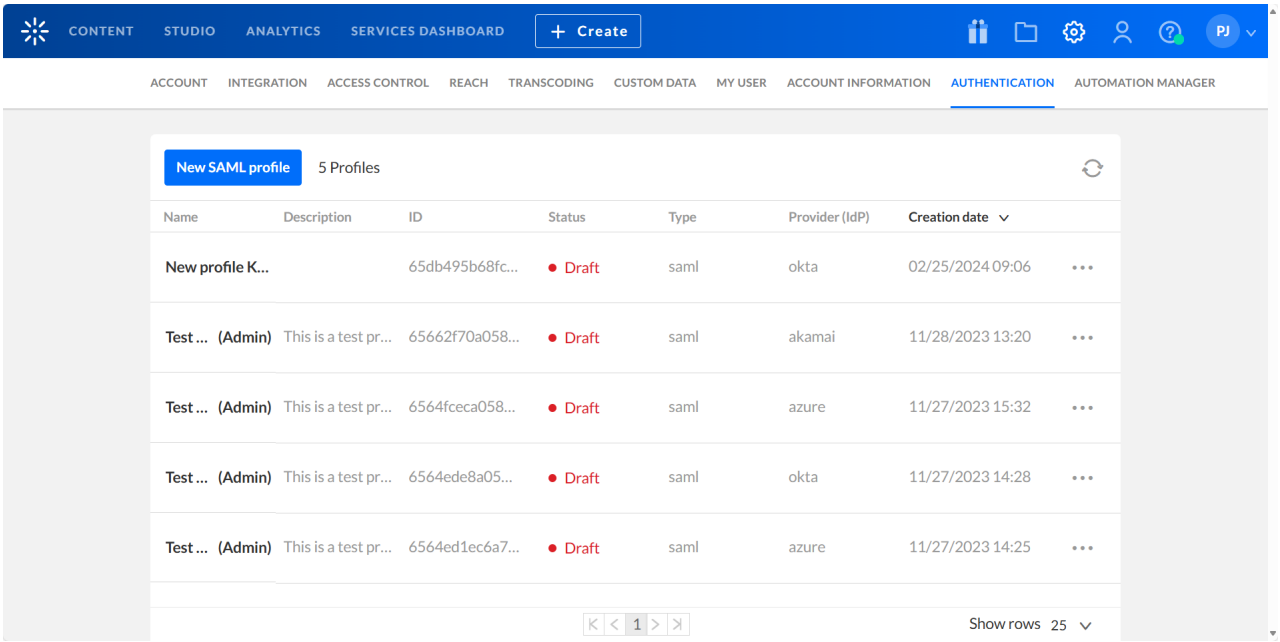
  Event customers - Please use the same credentials to log into the KMC that you use to log into Kaltura Events.

- Have the AUTHENTICATION tab enabled in the KMC. All the functionality described herein takes place on the AUTHENTICATION tab of the KMC.

If the AUTHENTICATION tab is unavailable as part of your account, please contact your Kaltura representative about adding it.

View your SAML profiles

Navigate to the AUTHENTICATION tab of the KMC; either use this direct link to the AUTHENTICATION tab or click the settings (gear icon) button in the upper right area of the KMC then click the AUTHENTICATION tab.
The full list of SAML profiles is displayed.



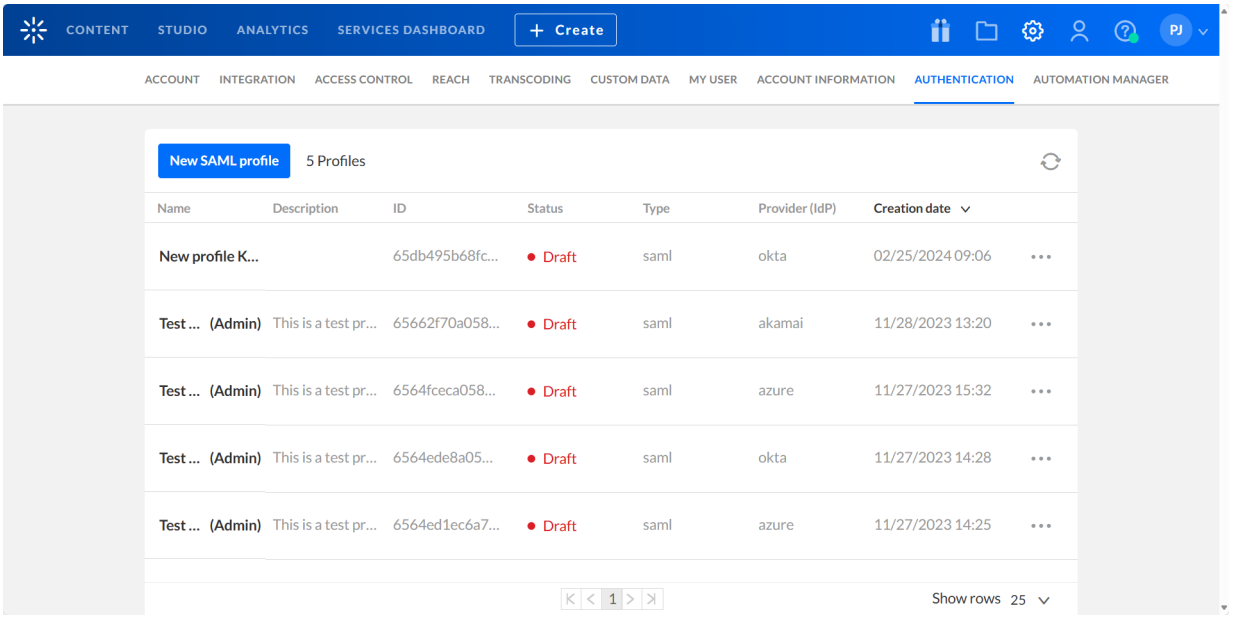
Following is a description of each field in the AUTHENTICATION tab:

Field	Description
Name	The name given to the SAML profile.
Description	The description given to the SAML profile.
ID	ID automatically generated when the SAML profile was created.
Status	*Draft* or *Ready*, depending on population of required fields marked by "*". Please see note in blue below.
Type	Authentication type
Provider (IdP)	The provider chosen for the SAML profile.
Creation date	Date the SAML profile was created. You may sort by this field.

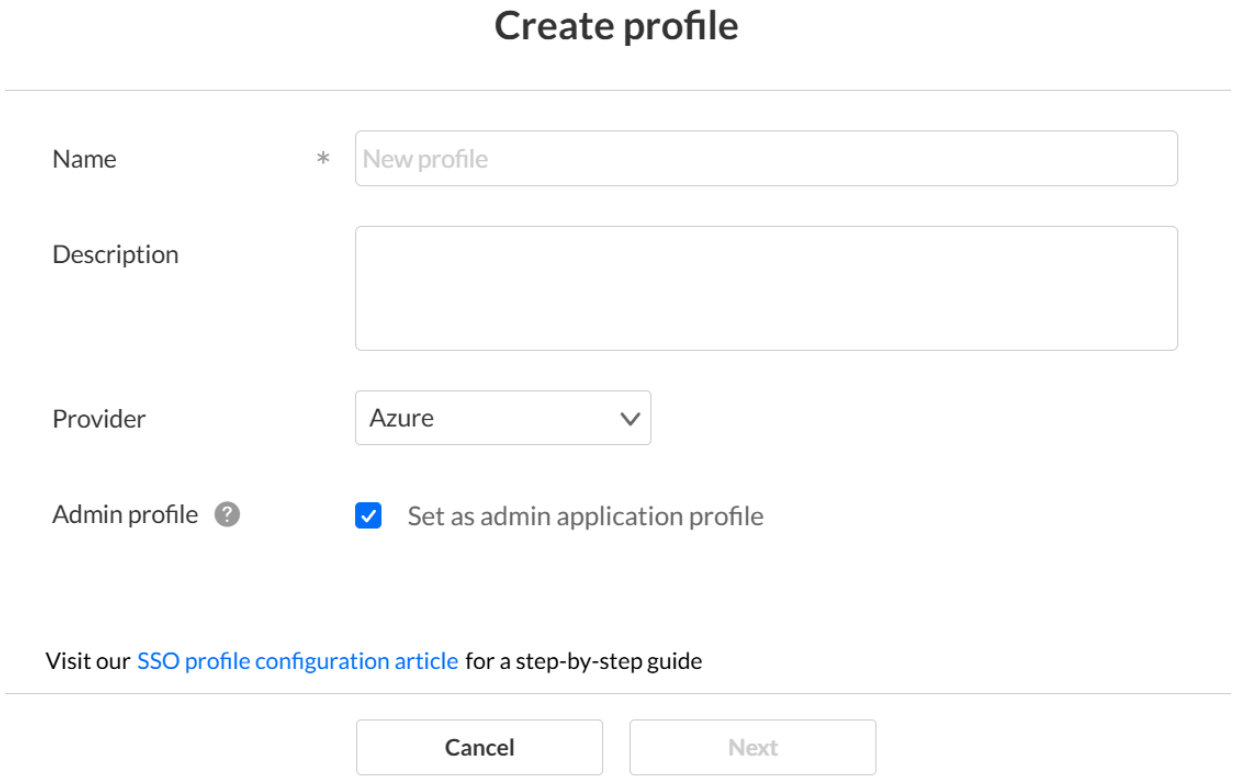
Required fields include Name, Entity ID, Login URL, IdP certificate and the attribute name mapped to Core_User_Email. When creating a SAML profile, if you click **Save** and all the required fields are populated, your SAML profile will be marked "Ready" in the Status column. If any required fields are not populated, your SAML profile will be marked "Draft" in the Status column. Please note - "Ready" in the Status column does not signify *technically accurate*. If fields are populated with erroneous data, the SAML profile will be invalid.

Create a SAML profile

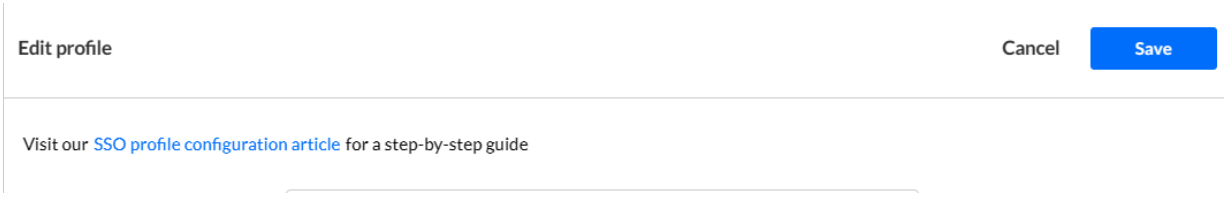
1. Navigate to the AUTHENTICATION tab of the KMC; either use this direct link to the AUTHENTICATION tab or click the settings (gear icon) button in the upper right area of the KMC then click the AUTHENTICATION tab.
   The full list of SAML profiles is displayed.

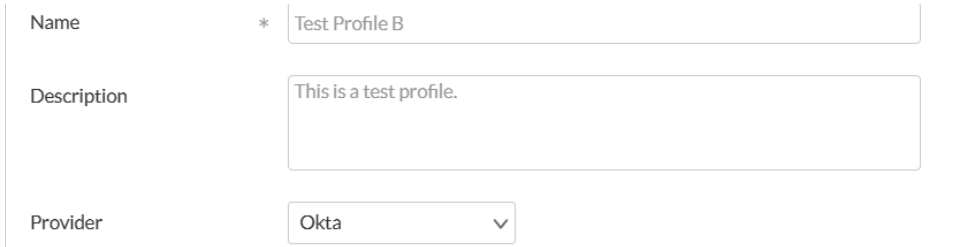


   If no profiles exist, the list is empty and reads "No Results".
2. Click **New SAML profile**. The Create profile screen displays.



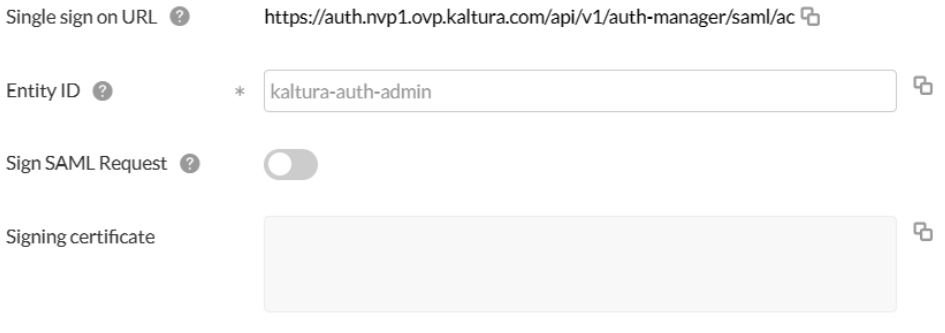
3. Enter the following information:
   - **Name** (Required) - Type a name for your new SAML profile (max 255 chars).
   - **Description** - Type a description for your new SAML profile (max 512 chars).
   - **Provider** - Choose the appropriate provider from the dropdown list. You may choose from Azure, Okta, AWS, Akamai, or Other.
   - **Admin profile*** - Check this box to use this SAML profile to sign into KMS/KAF administration pages. All KMS/KAF accounts in the application will automatically subscribe to profiles in which this box is checked, allowing access to the administration page using this SAML profile. Applications can still manually subscribe to this profile. Please note - once the SAML profile is saved, you may not edit this selection.
4. Click **Next** to create the new SAML profile and continue entering profile settings. You may also click **Cancel** to cancel the action. Note - The **Next** button is greyed out until all required fields are populated.
   If you clicked **Next**, you are re-directed to the Edit profile page of the newly created SAML profile.

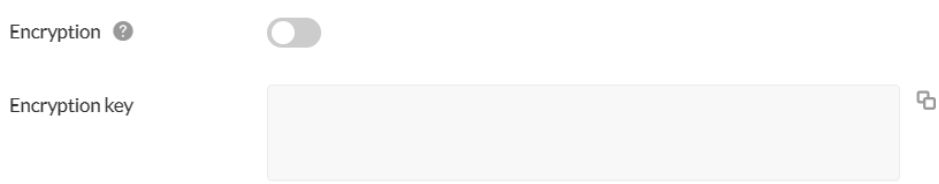




Service provider settings

Click here to download SP metadata via XML file or URL





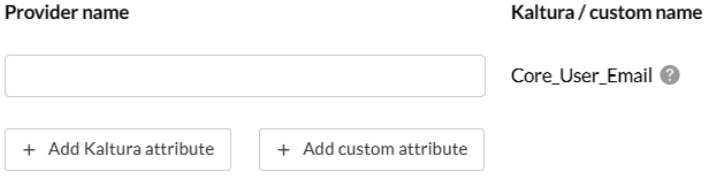
Identity provider settings

Copy the following from the IdP and paste in the text boxes below:

Attribute statements

Type in the attribute name, as it appears in the SAML assertion, into the provider name text-box. Map it to the Kaltura attribute statements by selecting a Kaltura attribute statement from the dropdown menu.

For custom attributes, type in both the provider custom name, and Kaltura custom name.



Show advanced settings

5. **Service provider settings -** This section contains information you will copy from Kaltura and provide to your IdP.
   - The **SSO URL** is the Assertion Consumer Service (ACS). It tells the IdP where to redirect an authenticated user after sign-in. The SAML response is posted to this URL. You may copy the SSO URL by clicking the **Copy** button to the right of the URL and pasting this information into the IdP.
   - The **Entity ID** (Required) is already populated with a default value. This is the unique identifier of the service provider. You may change this value. The Entity ID must be unique per profile, for example, if you need to add multiple Kaltura SSO profiles to your IdP. Copy the Entity ID by clicking the **Copy** button to the right of the ID and pasting this information into the IdP.
   - **Sign SAML Request** - If enabled, SAML requests will be signed. A confirmation displays letting you know this action will save the profile. Verify your action by clicking **Yes** or cancel your action by clicking **No**. If enabled, this generates a signed authentication request. The request will be signed and the IdP can validate the request against the public key that was provided in the metadata (see next field).
   - **Signing certificate** - If Sign SAML Request is enabled, the Signing certificate is displayed. This is a public key against which to validate the SAML request. You may copy the Signing certificate by clicking the **Copy** button to the right of the certificate and pasting this information into the IdP.
   - **Encryption** - Choose whether to enable encryption of the SAML response. Click toggle switch to right to enable. A confirmation displays letting you know this action will save the profile. Verify your action by clicking **Yes** or cancel your action by clicking **No**. Encrypt the SAML assertions with the public key provided in the Encryption key field.
   - **Encryption key** - If Encryption is enabled, the Encryption key is displayed as read only. This is a public key against which SAML assertions are encrypted. You may copy the Encryption key by clicking the **Copy** button to the right of the key and pasting this information into the IdP.

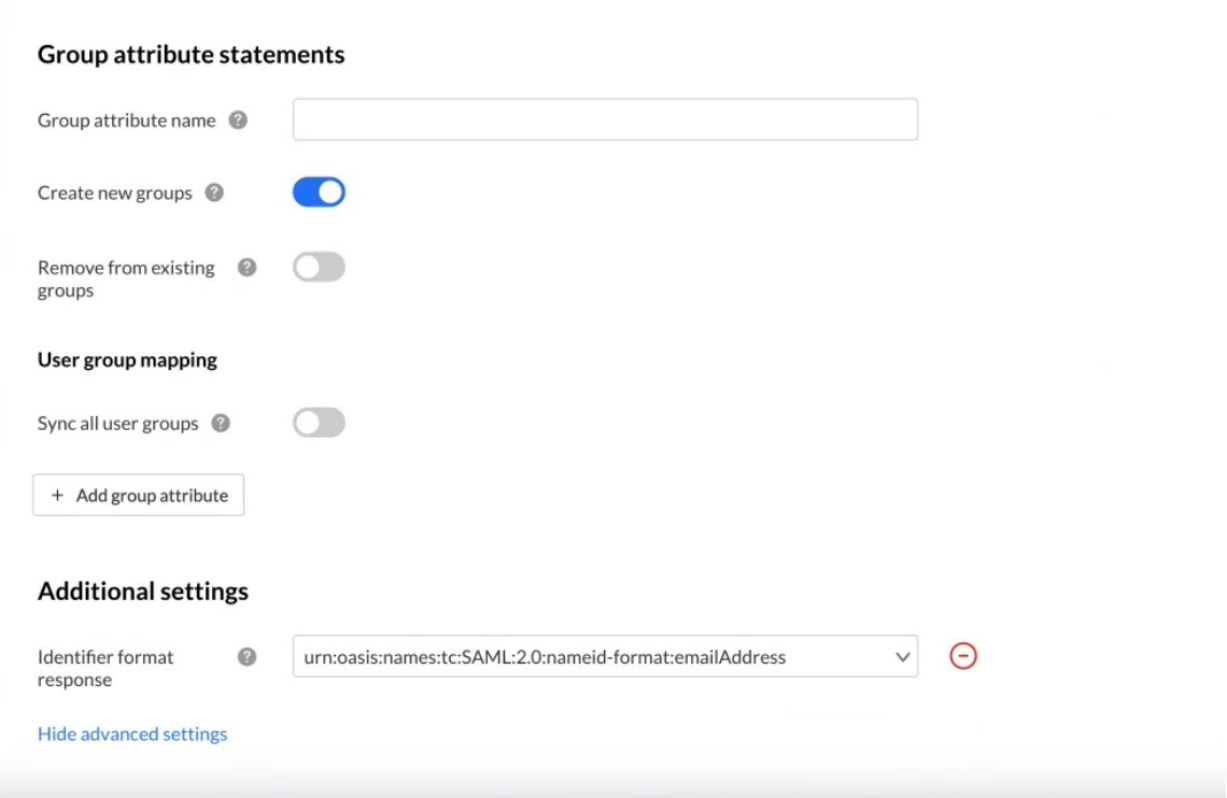
     In addition to using the **Copy** button to copy each service provider setting (as outlined above), Kaltura also provides the metadata as a URL or downloadable XML file. Click on the respective button (URL or File) to get the

metadata and upload it directly to your IdP.

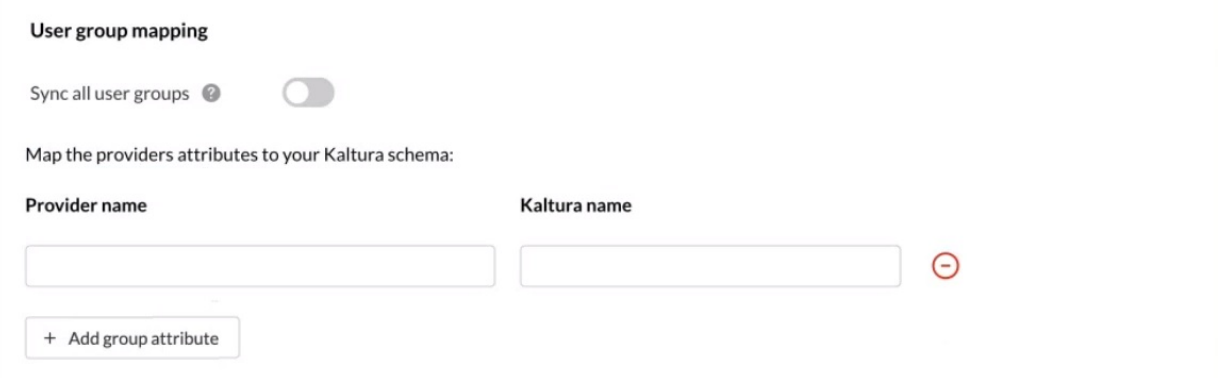
6. **Identity provider settings -** This section contains information you will copy from your IdP and provide to Kaltura. Enter the following information:
   - **Login URL** (Required) - Type the URL which is obtained from the IdP metadata. Typically, this URL will appear as <SingleSignOnService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"...../>
   - **Logout URL** - Type the URL Which is obtained from the IdP metadata. Typically, this will appear as <SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"…/>
   - **IdP certificate** (Required) - Copy/paste the certificate used by the IdP to sign the SAML response. This is obtained from the IdP metadata.

     ⚠ When pasting the certificate, remove the comment lines and spaces (e.g., -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----) to ensure it is a single, continuous line without any breaks.

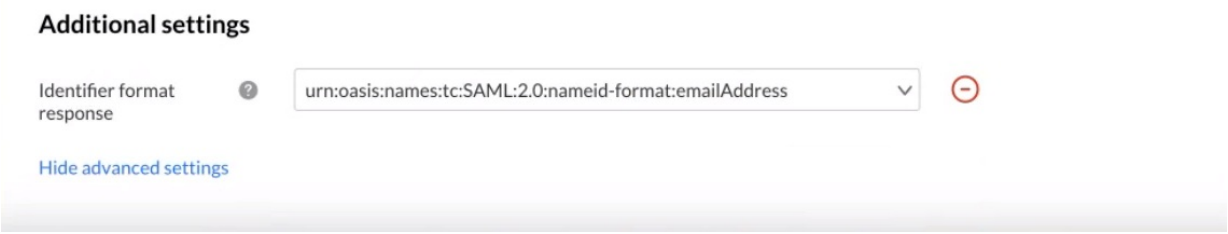
   - **Metadata URL** (Optional) - Type the metadata URL if you would like Kaltura to update the IdP signing certificate automatically before the certificate expires.
7. Under **Attribute statements**, type the **Provider name** and map it to the Kaltura or custom attribute name.
   The Core_User_Email attribute is mandatory. Type the provider name value that should be mapped to the Core_User_Email attribute. To add additional attributes, click **+ Add Kaltura attribute,** type the name of the attribute as it would appear in the SAML assertion into the first text box, and map them to the Kaltura attribute statements by selecting a Kaltura attribute statement from the dropdown list. To add custom attributes, click **+ Add custom attribute,** type the name of the attribute as it would appear in the SAML assertion into the first text box, and then map them to the Kaltura attribute statements by typing the name of the attribute as it will be saved in Kaltura. Once an attribute statement is added, it can always be removed by clicking the **Remove** button next to the appropriate attribute statement.
8. Click **Show advanced settings.** Additional configuration options are displayed.



9. Under Group attribute statements, enter the following information:
   - **Group attribute name** - Type the name of the custom attribute to which the SAML assertion groups were mapped in the **Attribute statements** section. Note - The SAML assertion groups must first be mapped to that custom attribute as shown above in Step 9.
   - **Create new groups** - Choose whether to enable the creation of new groups in Kaltura that exist in the IdP and do not exist in Kaltura during the sync.
   - **Remove from existing groups** - Choose whether to enable the removal of users that were removed from the IdP group from the Kaltura group during the sync.
10. Under User group mapping, if the **Sync all user groups** toggle is enabled, mapping is disabled because all IdP user groups are automatically synced up to Kaltura user groups. Group names in Kaltura will be identical to the ones in the SAML assertion. If the **Sync all user groups** toggle is disabled, you may add group attributes by clicking the **+ Add group attribute** button, typing a Provider name and Kaltura name in the respective fields. You may also remove additional attributes by clicking the **Remove** button next to the appropriate attribute.



11. Under Additional settings, choose an identifier format response from the Identifier format response pull-down menu. You may also remove the Identifier format response by clicking the **Remove** button next to the right of the field.

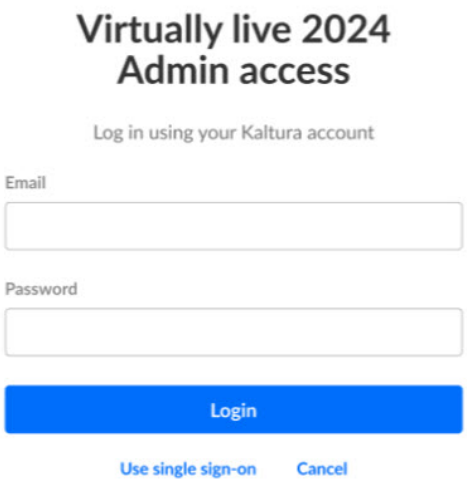


12. Once you are finished entering your information, click **Save**. You may click **Cancel** at any time but be aware you will lose any unsaved changes.

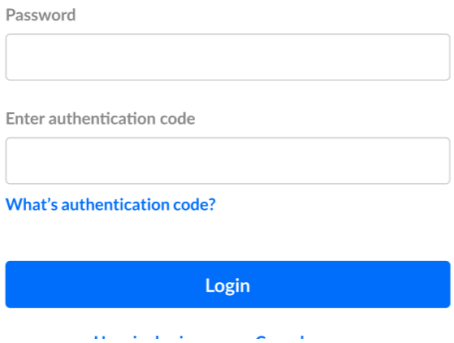
To learn more about subscribing applications to your newly created SAML profile, see Subscribe KMC and Event accounts to Auth Broker profiles.

***Notes about SAML profiles set as admin application profiles:**

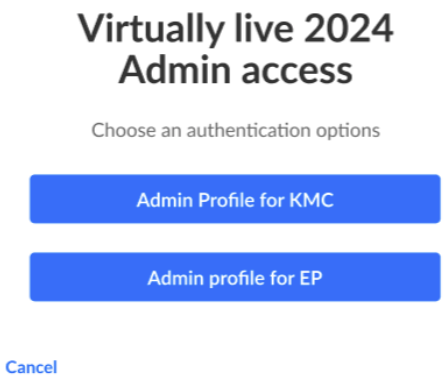
- Once a new SAML profile is set as an "Admin profile", the KMS/KAF admin automatically finds it and allows access to the admin pages using that profile.



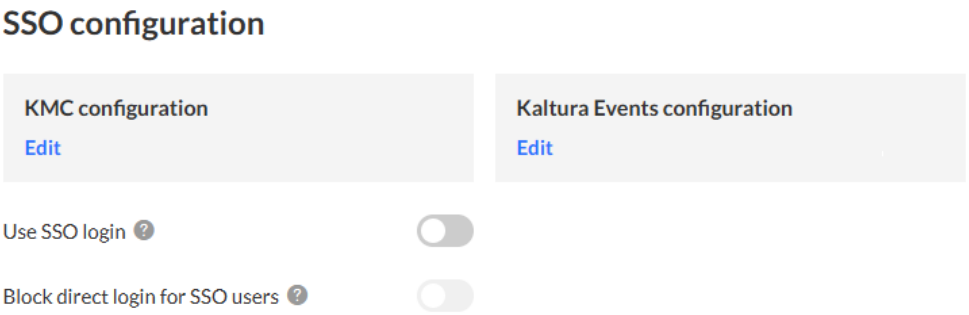
- SAML profiles set as admin are presented with Two Factor Authentication for the KMS admin page if it is enabled at the account level.



- If more than one SAML profile is set as an admin application profile, after clicking **Use single sign-on**, the admin is prompted to choose an authentication option.



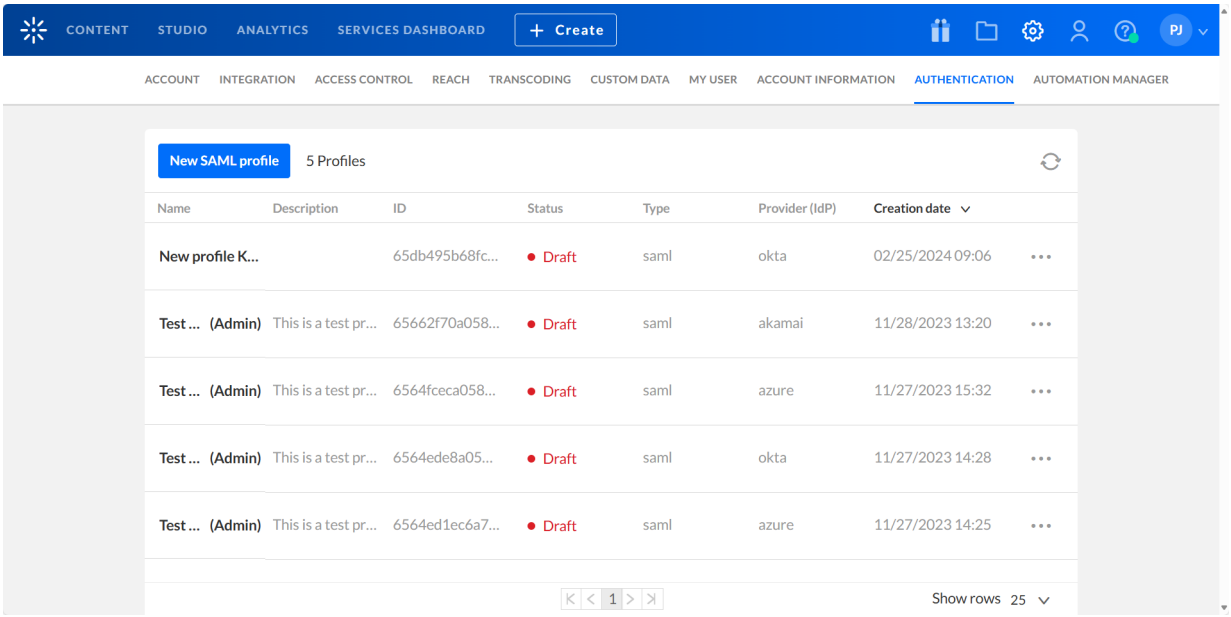
- You may block direct login for SSO users into the KMS admin pages via the KMC "Block direct login for SSO users" toggle.



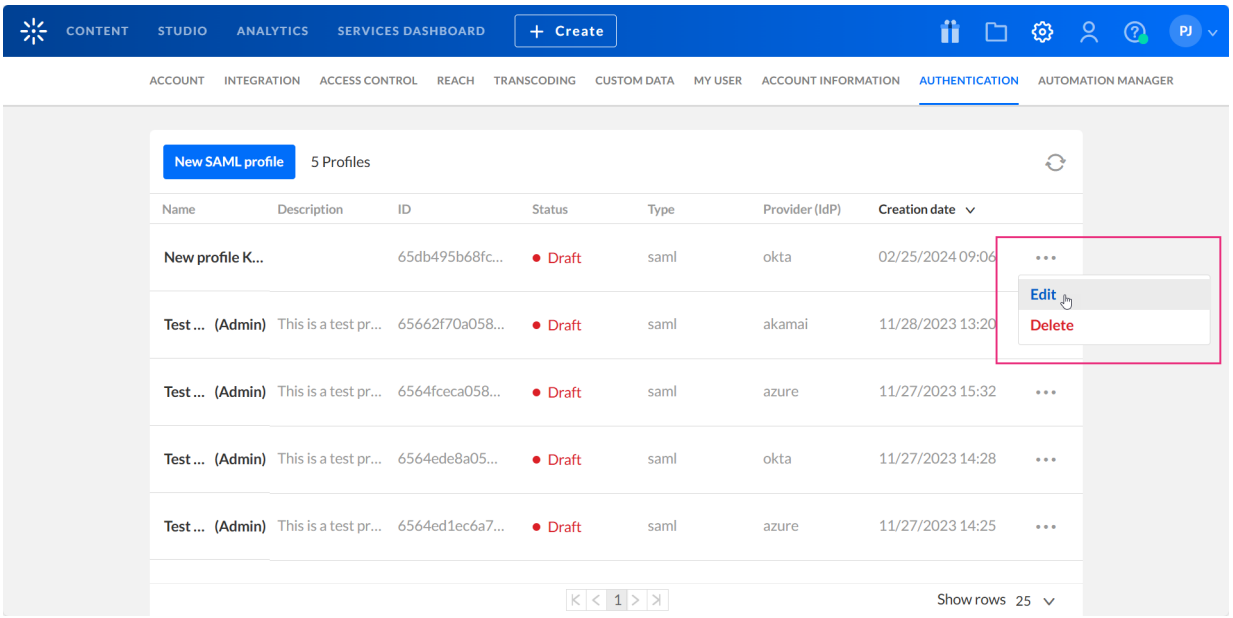
Edit a SAML profile

1. Navigate to the AUTHENTICATION tab of the KMC; either use this direct link to the AUTHENTICATION tab or click the settings (gear icon) button in the upper right area of the KMC then click the AUTHENTICATION tab.

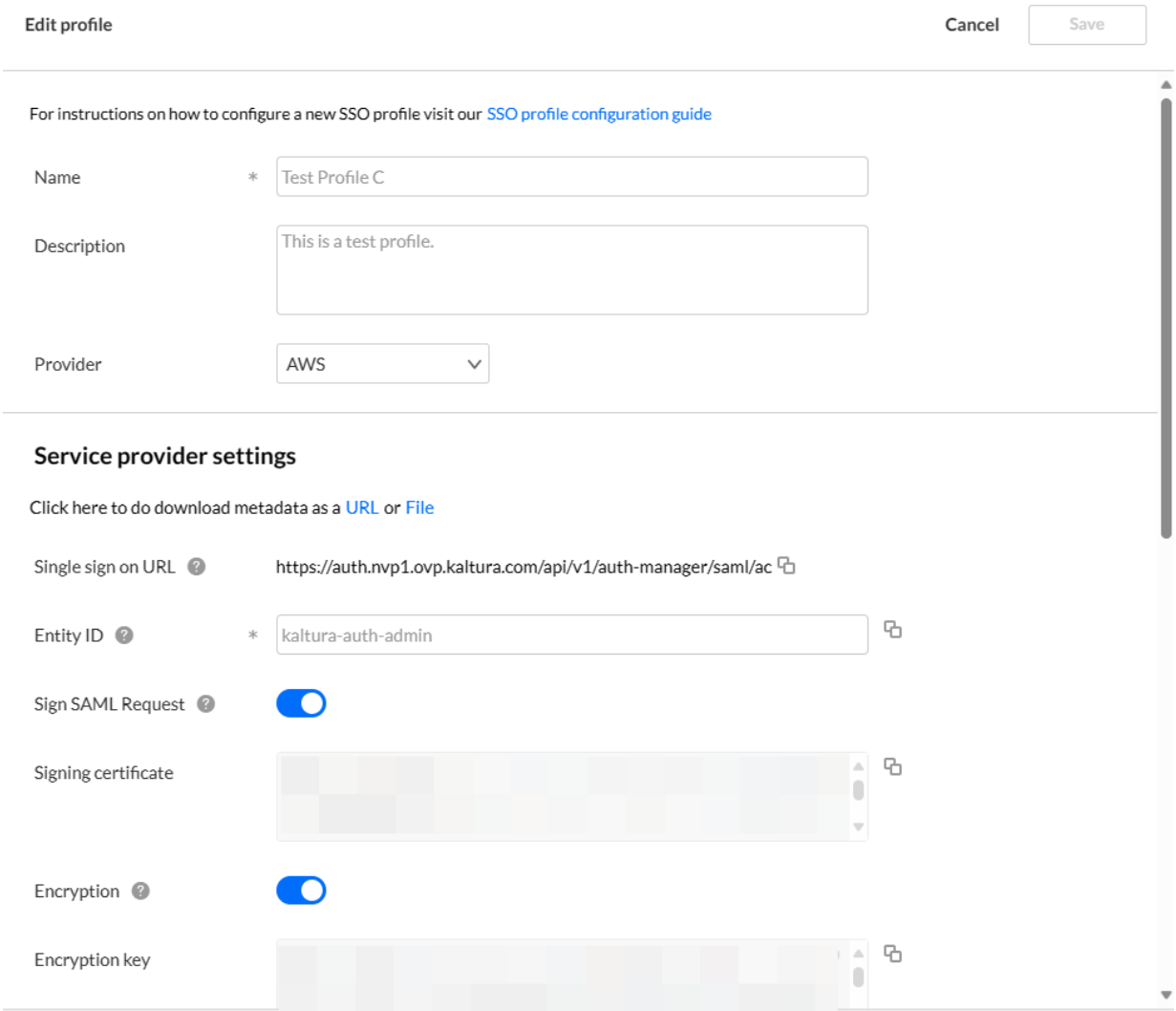
The full list of SAML profiles is displayed.



2. Click the three dots to the right of the appropriate SAML profile and choose Edit.



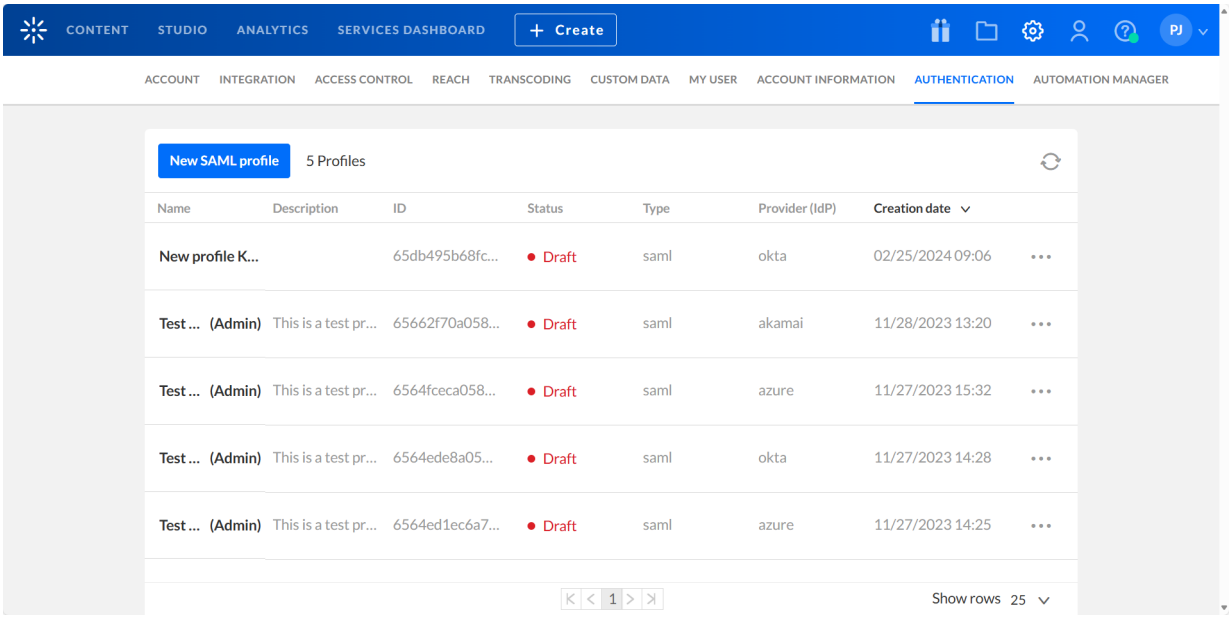
The Edit profile page displays.



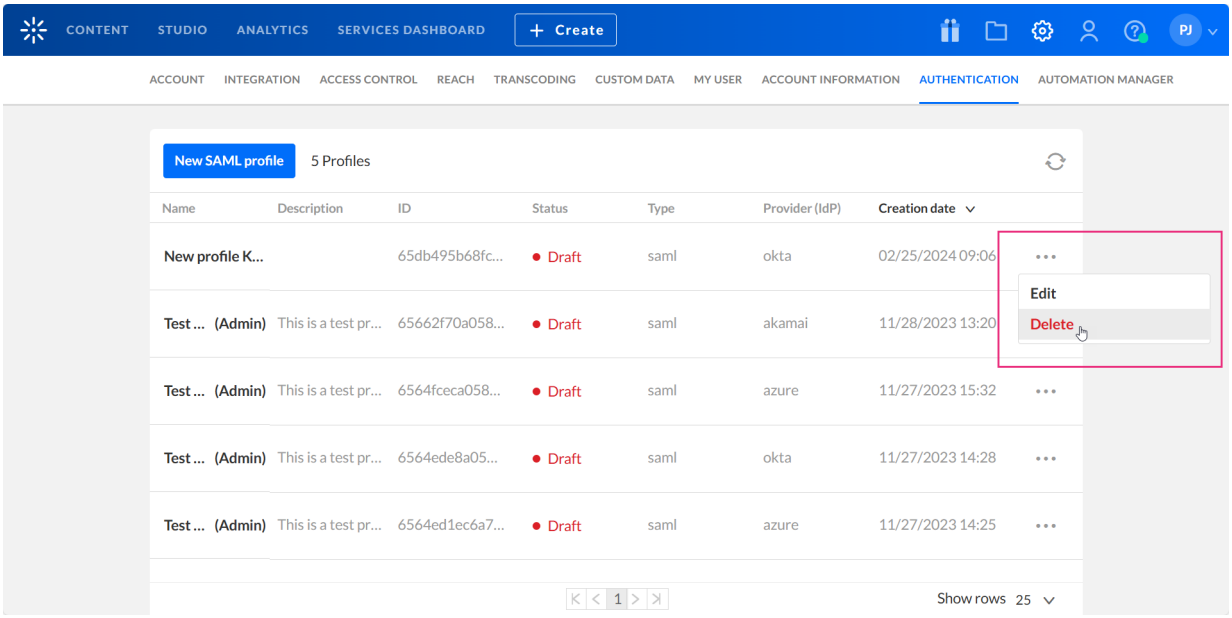
3. Edit the information as desired and click **Save** when finished.

Delete a SAML profile

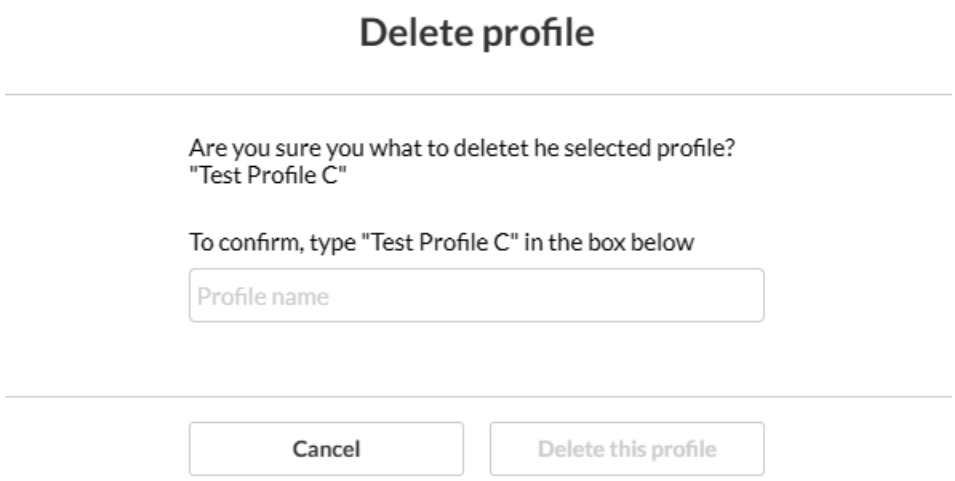
1. Navigate to the AUTHENTICATION tab of the KMC; either use this direct link to the AUTHENTICATION tab or click the settings (gear icon) button in the upper right area of the KMC then click the AUTHENTICATION tab.
   The full list of SAML profiles is displayed.



2. Click the three dots to the right of the appropriate SAML profile and choose Delete.



A confirmation message displays asking you to confirm your action.



3. To confirm, type the profile name in the Profile name field. Note - the name must be typed exactly as it is shown in the KMC. Only then will the **Delete this profile** button be enabled.
4. Click **Delete this profile**. The profile is deleted from the KMC.