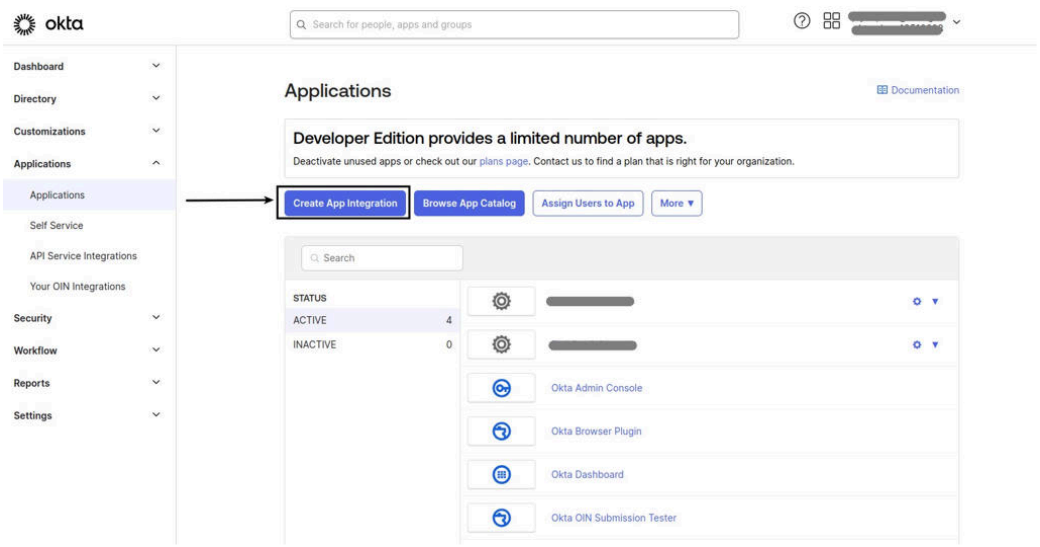
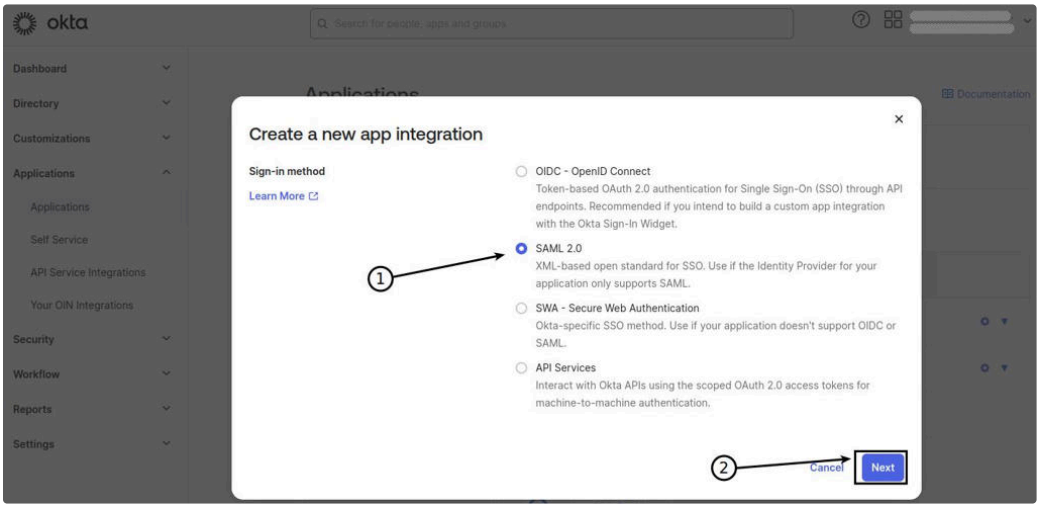
SAML Setup (Okta)

- Login to the **OKTA Admin Dashboard** at Okta Developer
- Navigate to the **Applications** → Click on the **Create App Integration**

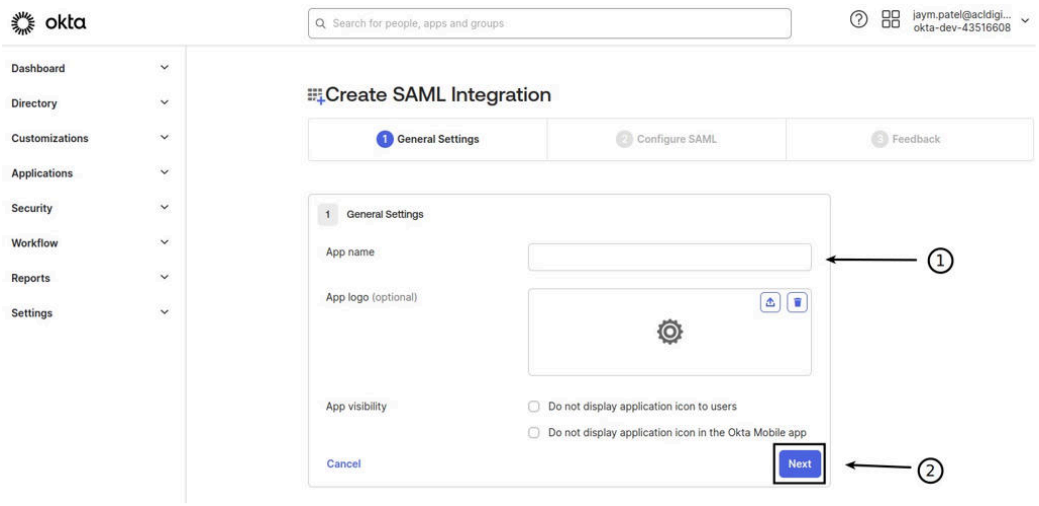


- In Create a new app integration pop-up

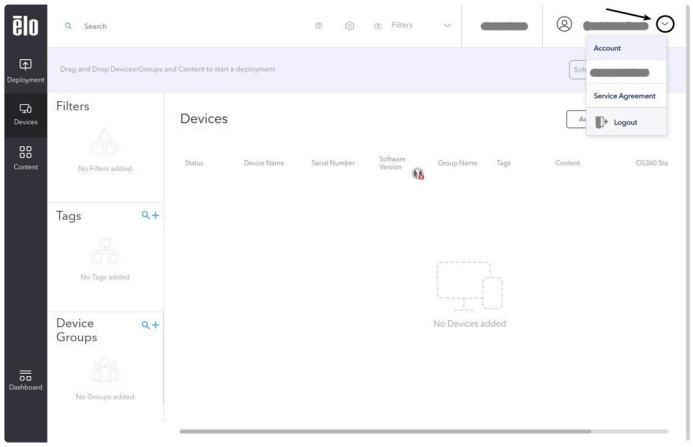
1. IN Sign-in method: Select **SAML 2.0**
2. Click on the **Next button** to proceed further



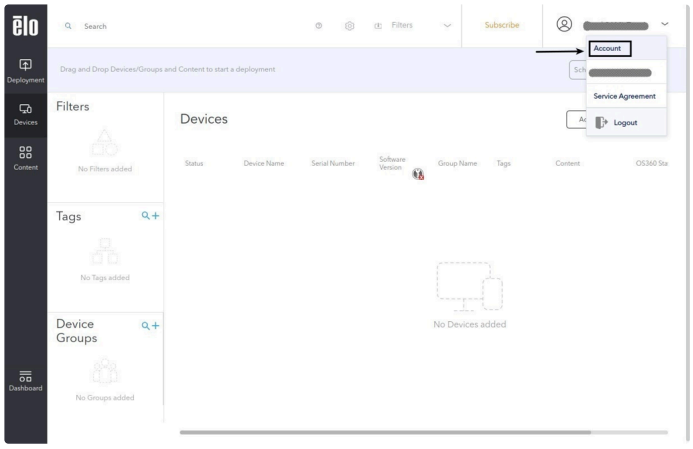
1. Add an appropriate name in the **App name**
2. Click on the **Next Button** to **Configure SAML**



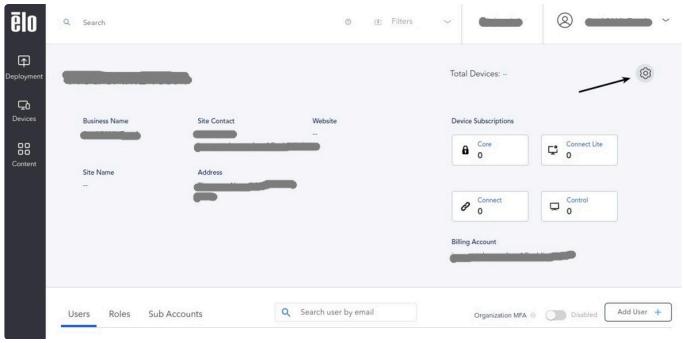
- In a separate tab, Log in to Elo
- Click on the **dropdown beside User Profile.**



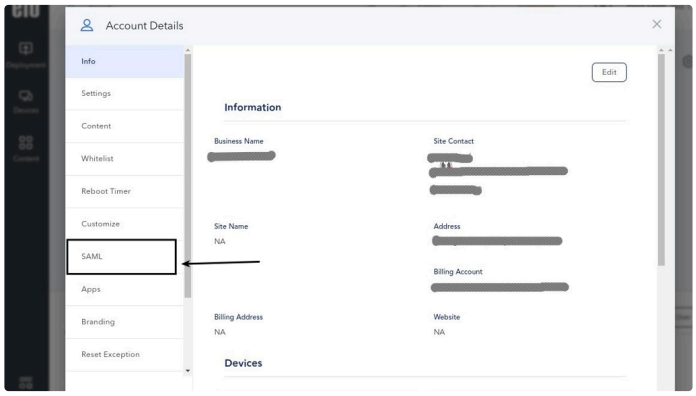
- Navigate to the Account page.



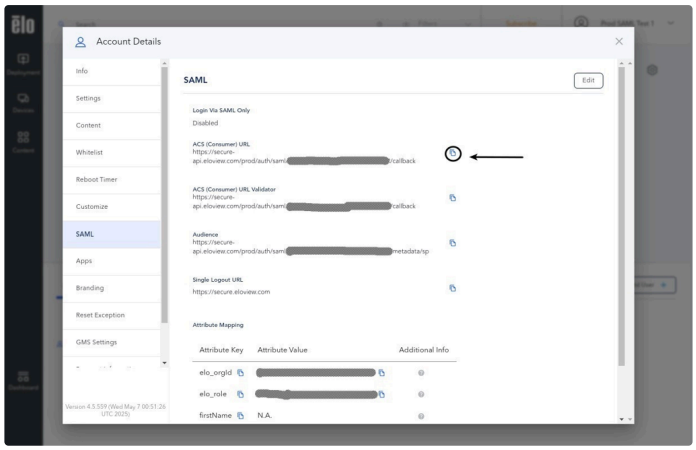
- Click on the **Gear Icon for Account Settings**



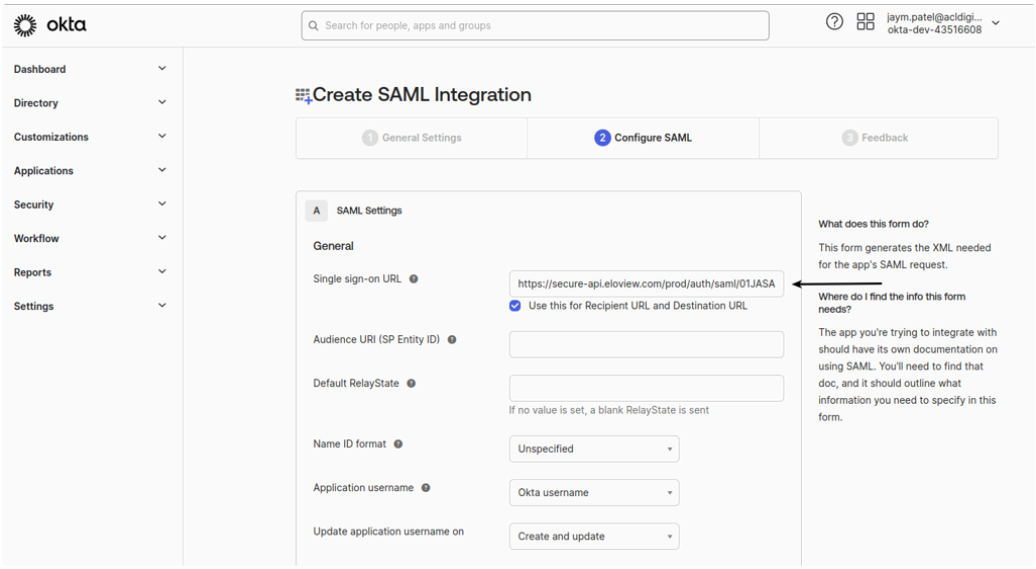
- In the **Account Settings** pop-up, click on the **SAML tab.**



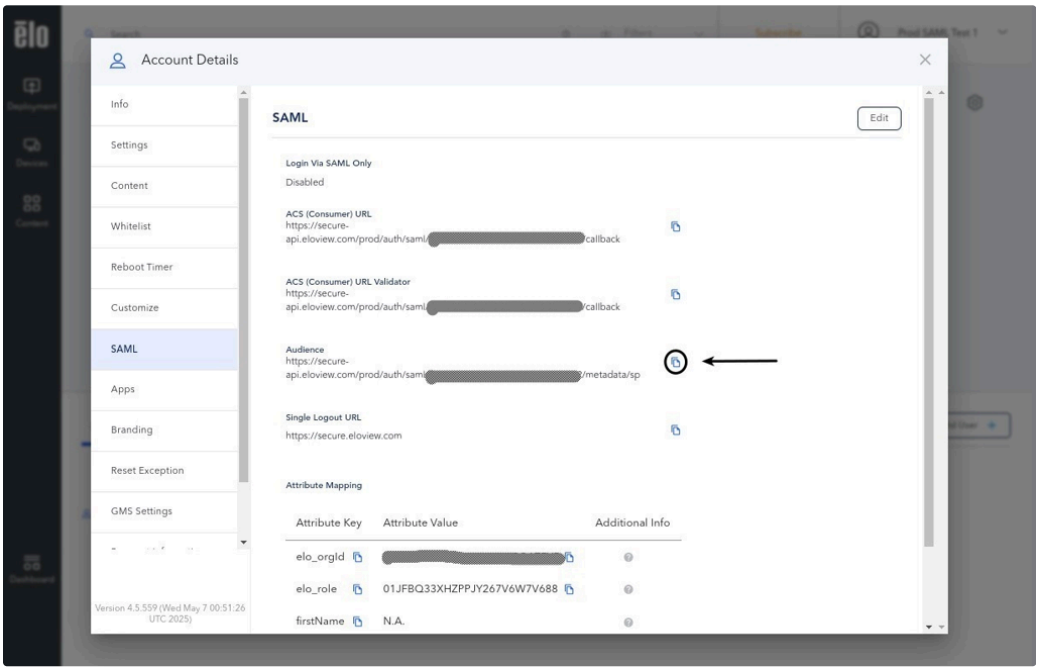
- In the SAML tab, copy the **ACS URL** by clicking the **copy button.**



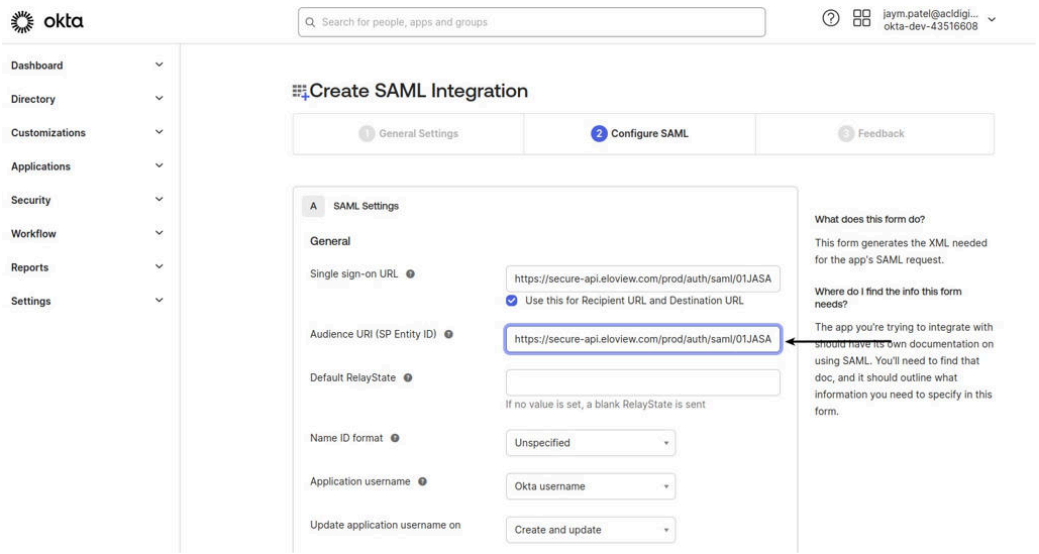
- Paste the copied **ACS URL** in **the Single Sign-On URL as shown below**



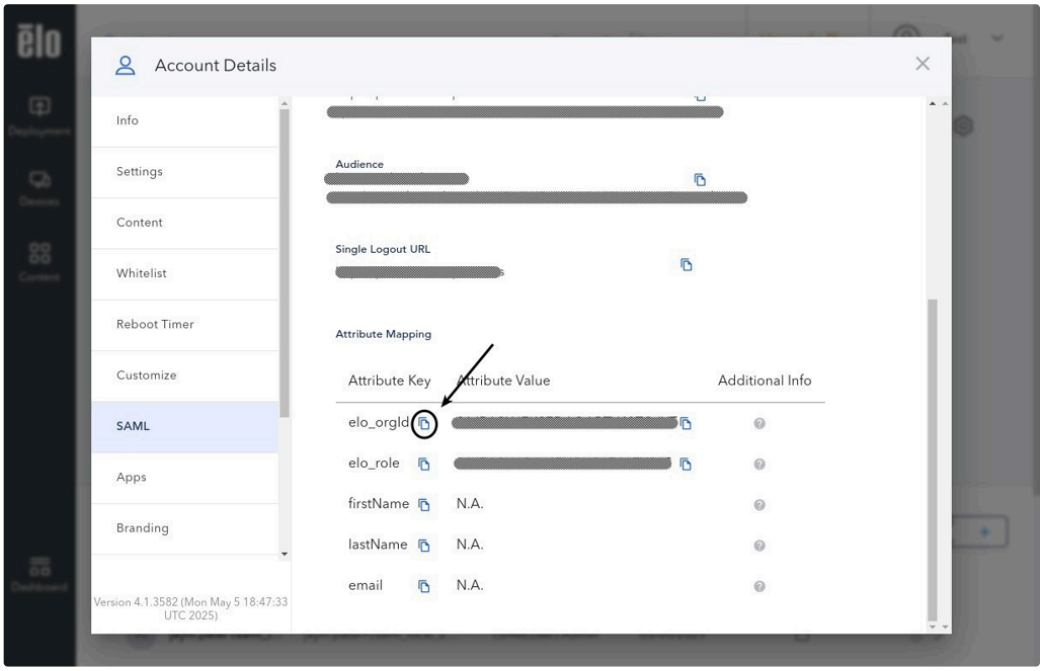
- Go to the EloView4 Account SAML tab, copy the **Audience(Entity ID)** by clicking the **copy button.**



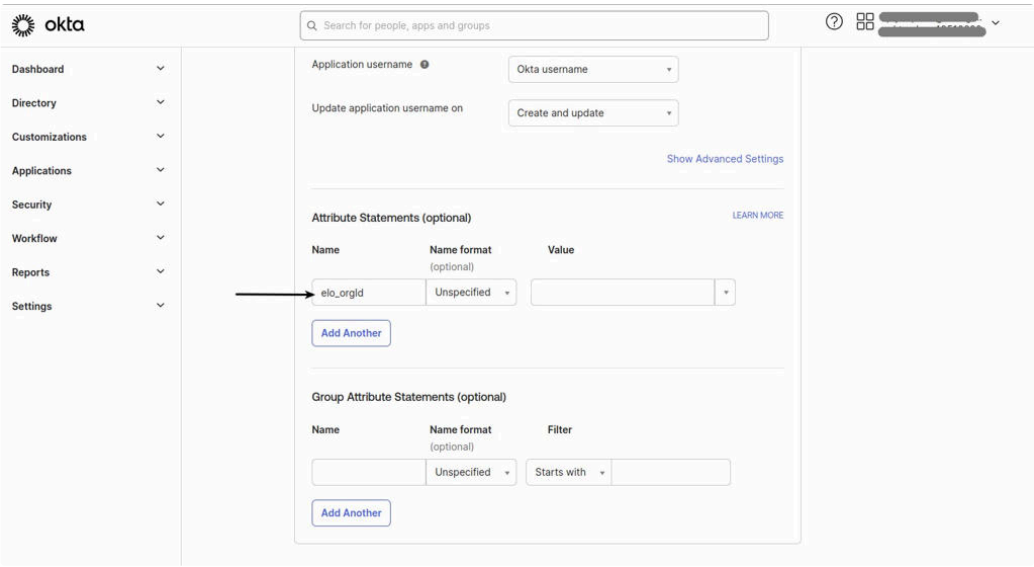
- Paste the copied **Audience(Entity Id)** in **Audience URI as shown below**



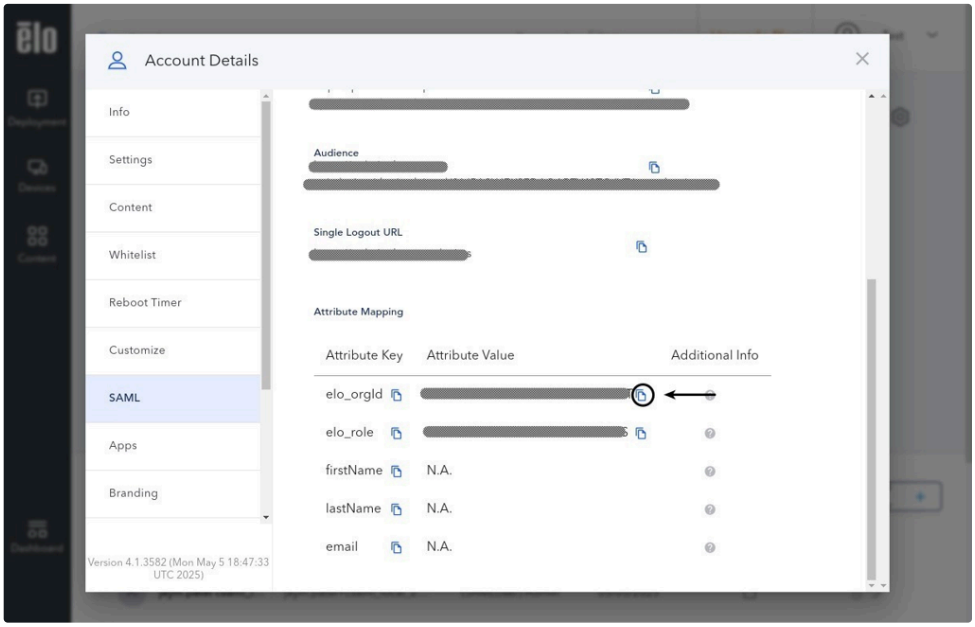
- Now, set up the required **Attribute** in Okta, so scroll down and go to the **Attribute Statements** section on the same screen (SAML Config) -
  - Go to the EloView4 Account's SAML tab, **click the copy icon** next to "elo_orgId" in Attribute Mapping, as shown below.



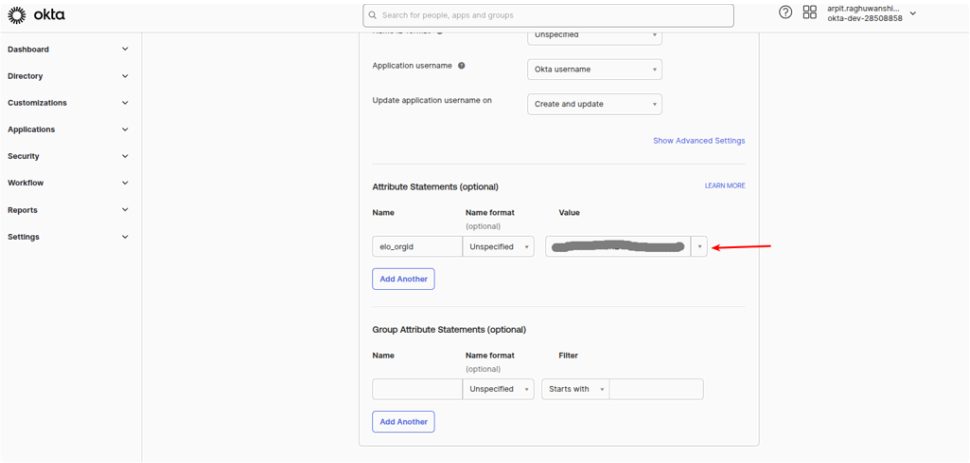
  - In the Okta Application > SAML Config, scroll down and go to the Attribute Statements section, and paste the copied **Attribute key** in the box below **Name,** as shown below -



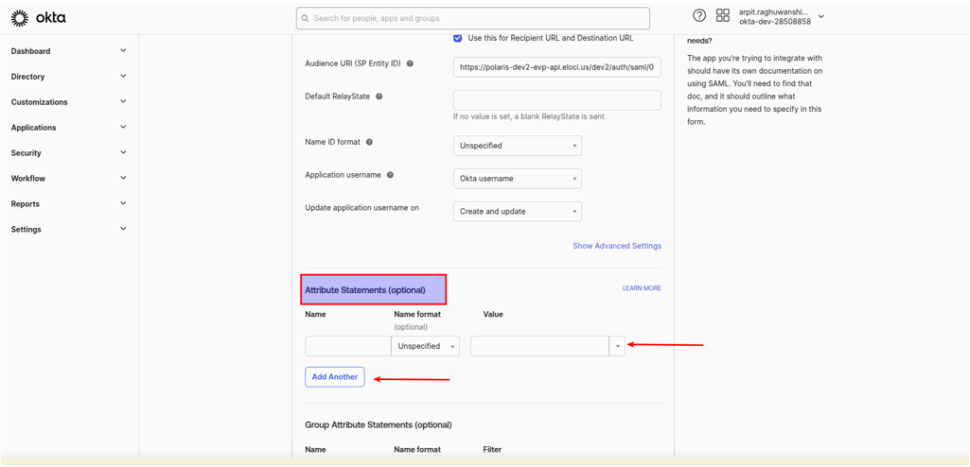
- Switch to the EloView SAML configuration screen and click on the copy icon to copy the value of the **elo_orgId** attribute.



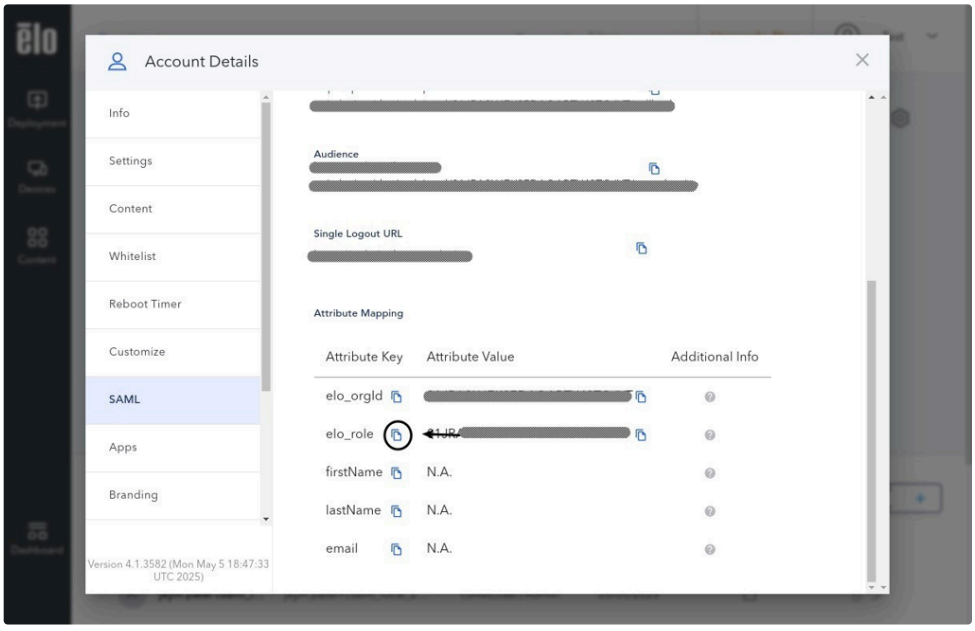
- Paste the copied **value of elo_orgId** from **EloView4** into the **attribute value** field as shown in the image -



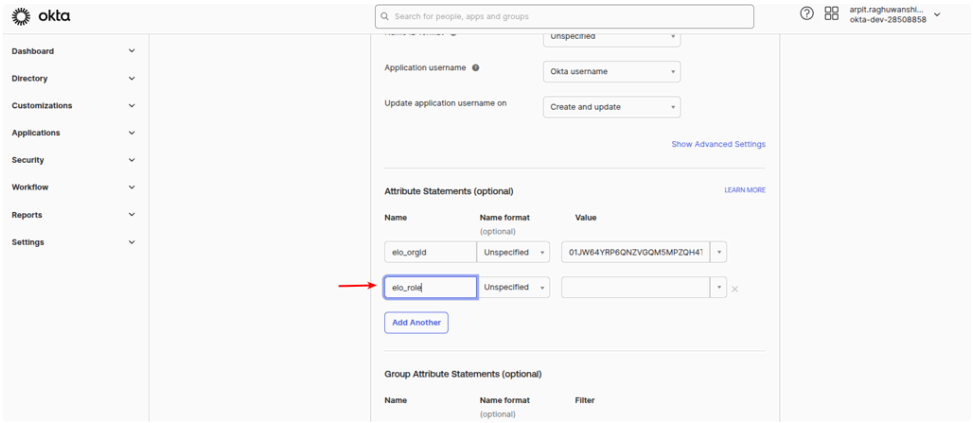
- Click the Add Another button to add more attributes, it will expand the section & provide more fields to add more attributes.



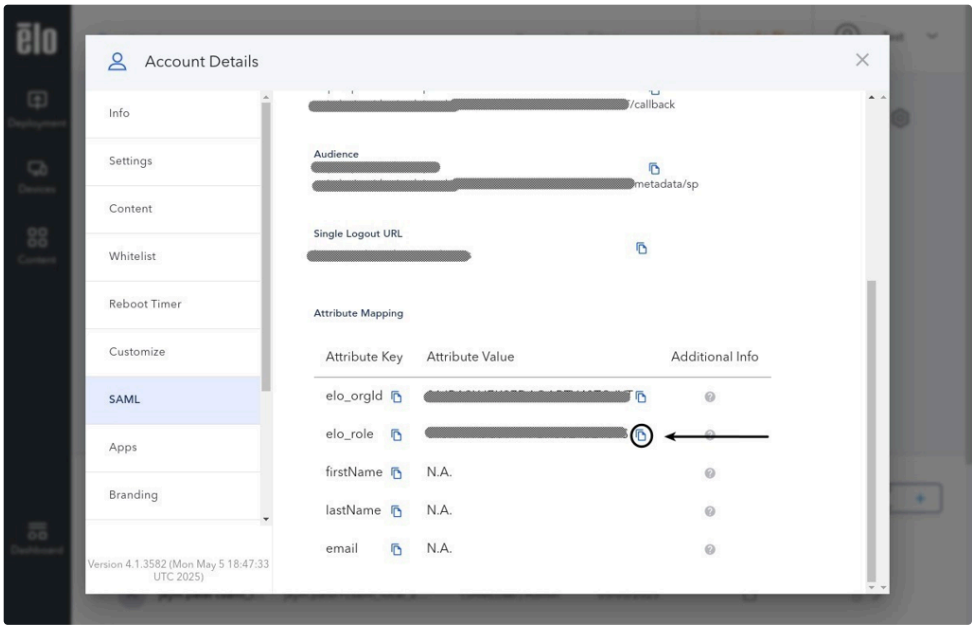
- Switch to the EloView4 tab, **click the copy icon** to copy the "**elo_role**" Attribute Key.



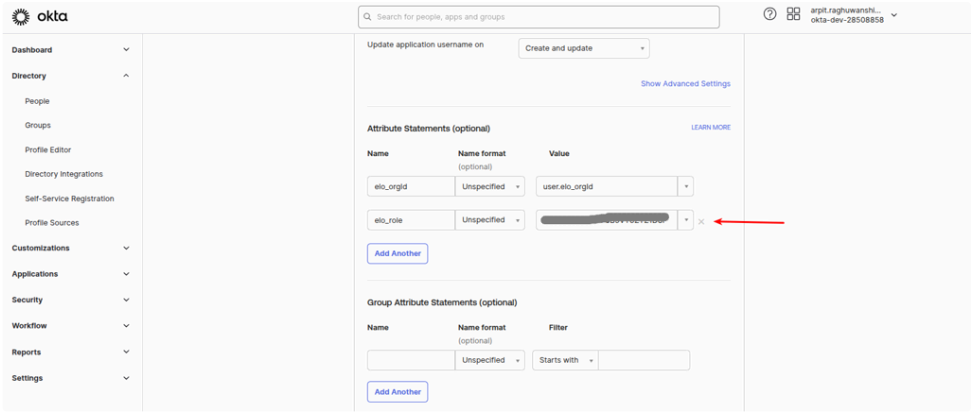
- **In the Okta console**, paste the copied value in the Attributes key field.



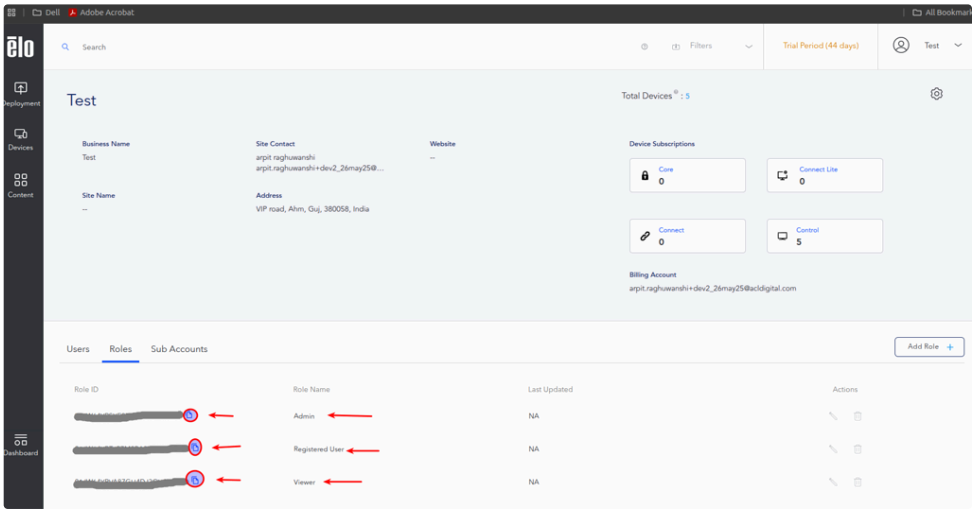
- Go to the EloView screen and click on the copy icon to copy the value of the **elo_role** attribute (this is the EloView Org admin role ID), as shown below -



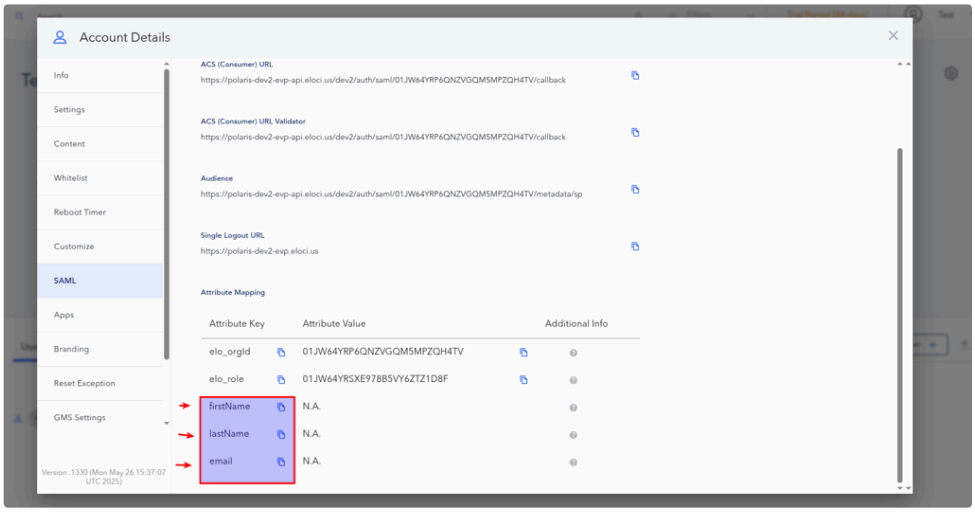
- Paste the copied **value of elo_role** from **EloView4** into the **attribute value** field as shown in the image.



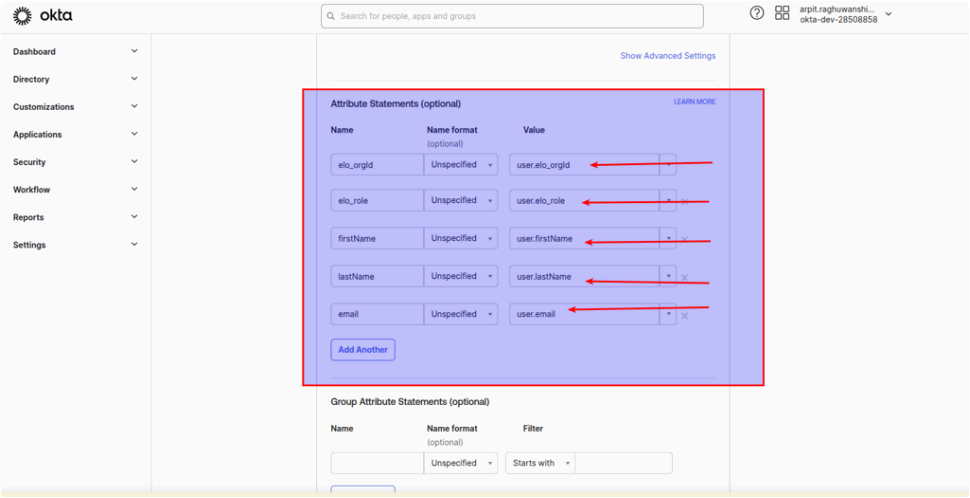
- Value for **elo_role** can be copied as per the **role preference** wanted to set up. EloView role ID can be copied from the Role List for other EloView custom or default roles e.g. Viewer, Registered User, etc -



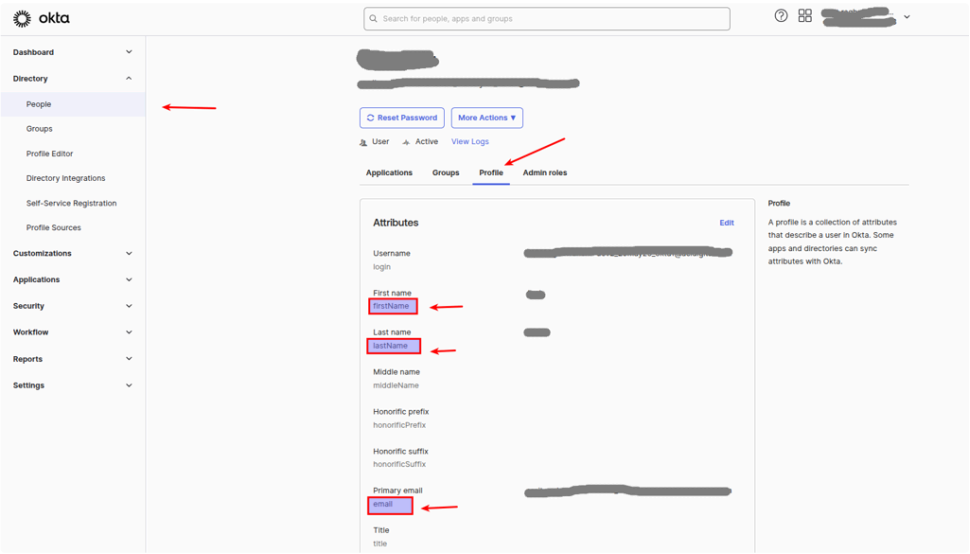
- Similarly, add all other attribute keys available in the EloView Attribute Mapping



- To do so, click on the copy icon, followed by the attribute key, and paste into the Okta Attribute Name field of the Attribute Statements section as we did above for **elo_orgId, elo_role**
- The **value** for other attributes key (i.e., **firstName**, **lastName**, **email**) should be like **attribute key** followed by “**user.”,** as shown below, i.e., **user**.<**attribute_key**>

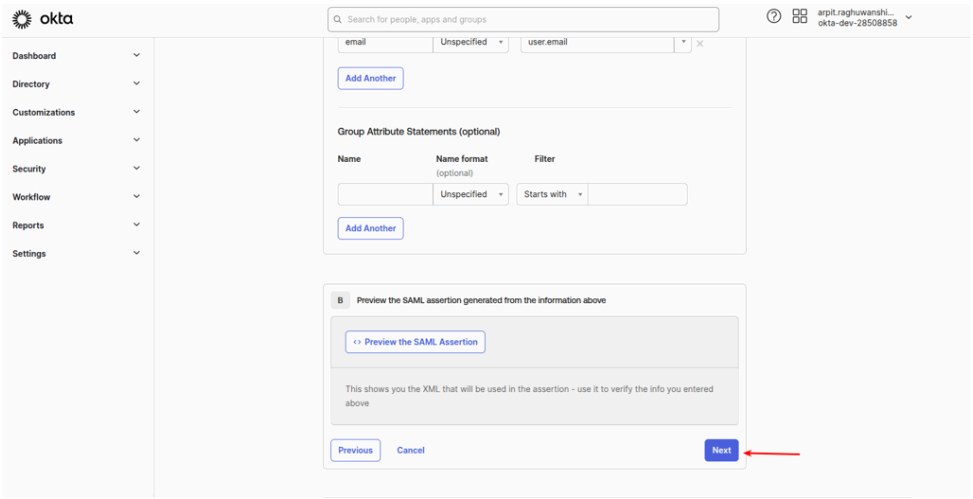


- Verify that the **attribute_key** added in the value for firstName, lastName & email should match with the **profile attributes** of the Okta users, as shown in the below screen -

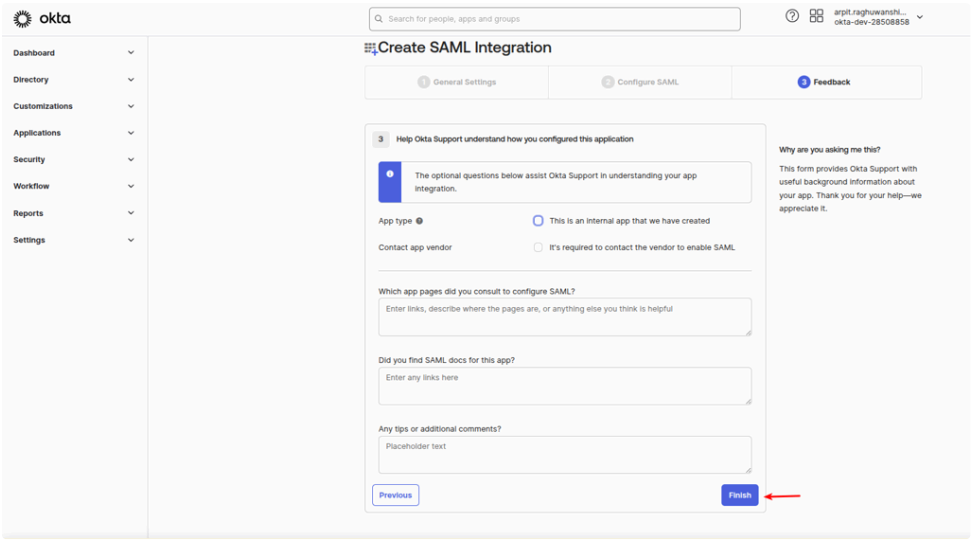


- This way, we have added all the required attributes and the value **user.<attribute_name>** denotes that it will get these values from the users/people configured in **Okta**.

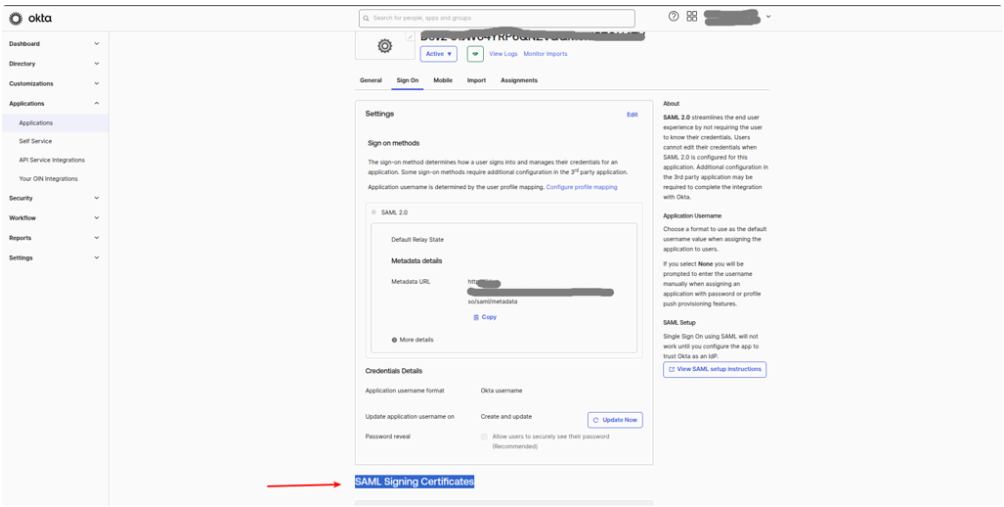
- Next, scroll down and click on the Next button



- Not mandatory to provide any inputs on the feedback tab. Click to **Finish** to complete the **application** setup in **Okta**



- Now, find out the **SAML Signing Certificate** section on the **Sign-On tab** of your Application, as shown below -



- In the SAML Signing Certificate, find the **Active** certificate, then click on the **Actions** drop-down and c**lick** on the **View IdP metadata** button (Image 1). This will open a new tab with SAML metadata (Image 2).

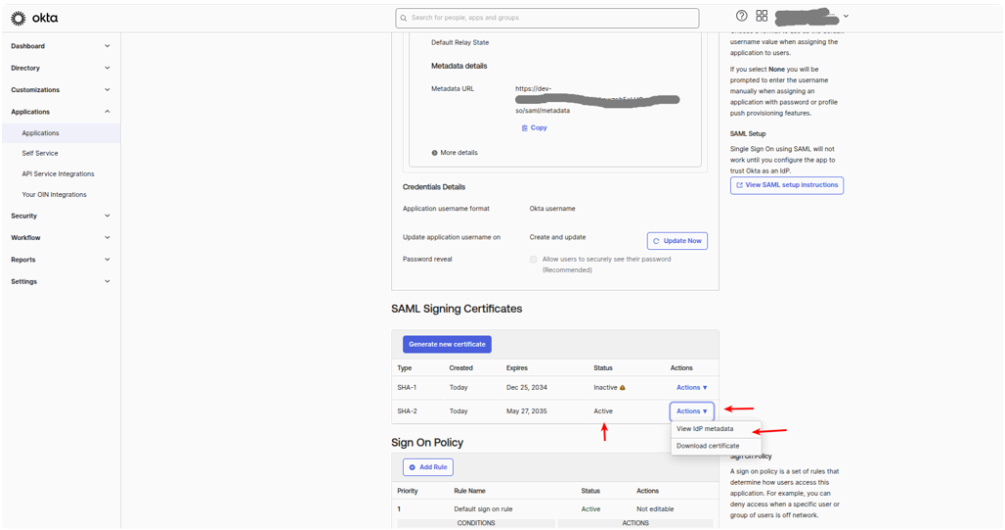


Image 1: View IdP metadata

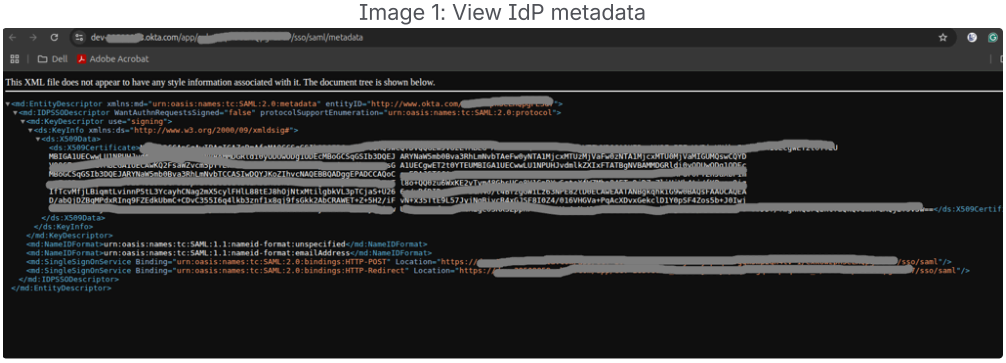
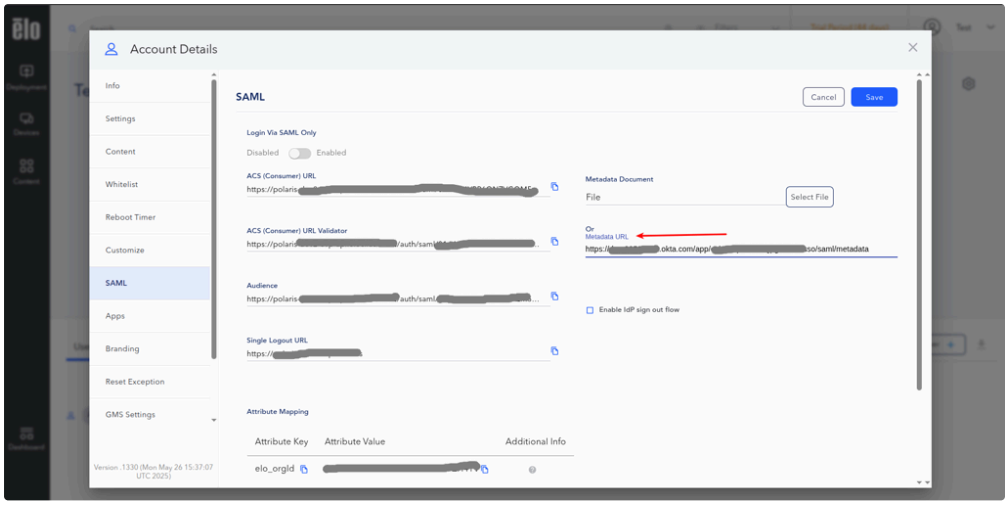
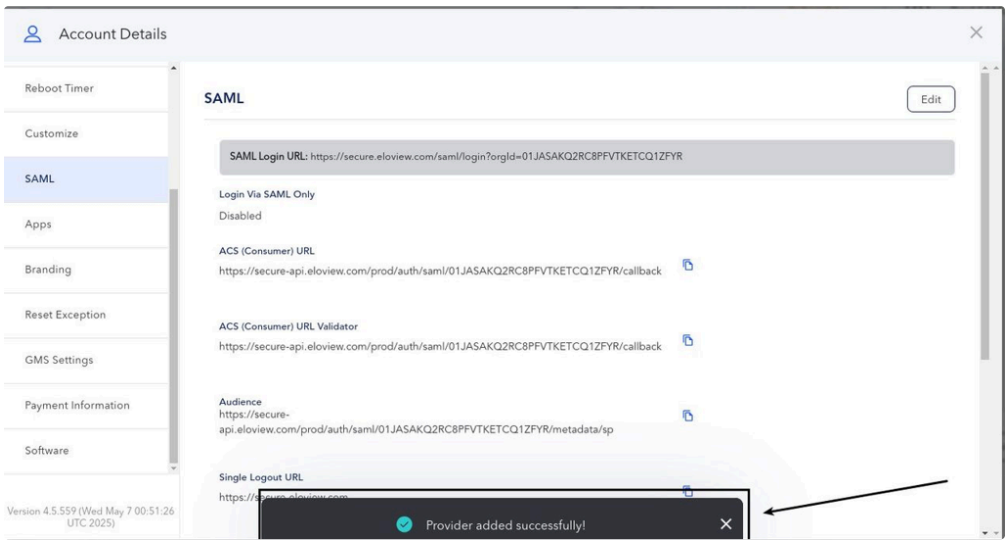


Image 2: IDP metadata in new tab

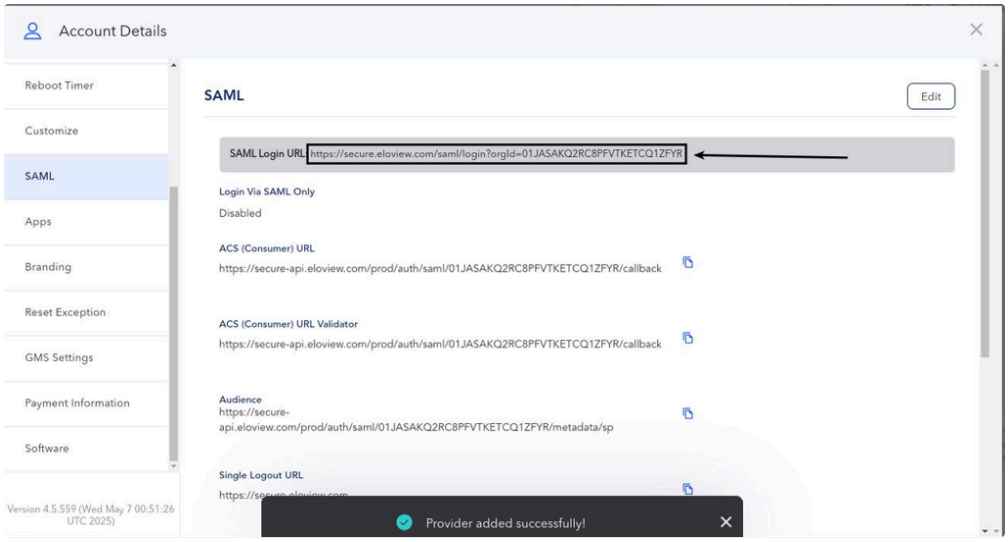
- **Copy the URL(**ending with **/sso/saml/metadata)** from the **newly opened tab** (See above: Image 2 - browser address bar)
- Navigate to the **EloView SAML Configuration tab** from the **Account Details page,** click **Edit**, and paste the copied **Identity Provider Issuer URL (**from the previous step**)** in the **Metadata URL** input field**,** as shown below -



- Check the **Enable IdP sign-out flow** checkbox (**Optional**) if you want to allow a single log-out flow(while logging out from EloView, it will also expire the IDP/Okta session).
- Click on the **Save button** to apply changes**.**
- You should get a successful response to the following -



- Bookmark or use the **SAML Login URL** for future logins



- Here we are **done** with the **Okta application configuration** & **EloView SAML configuration**.

End of Document