

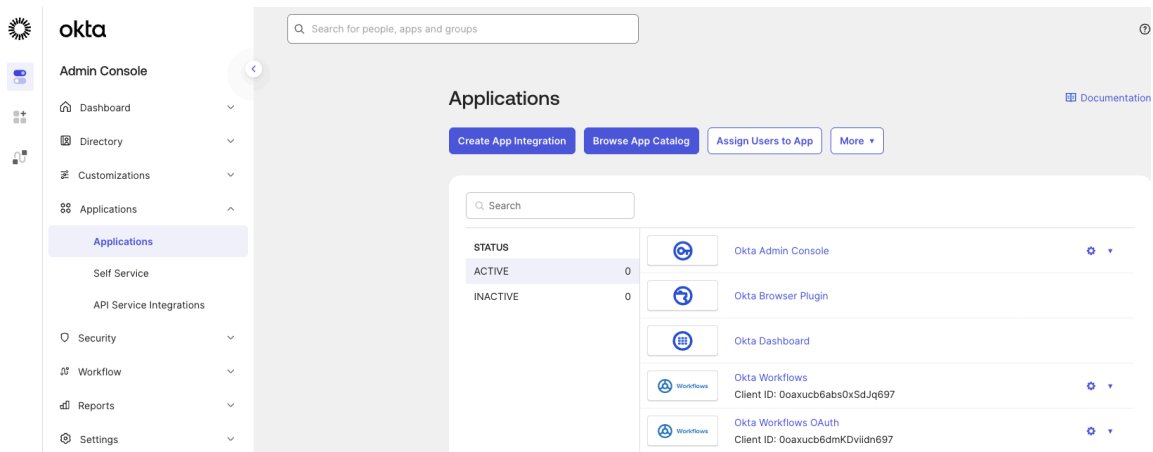
OKTA SSO Setup for Gainsight Integration

Follow these steps to configure Single Sign-On (SSO) between Okta and Gainsight.

Stage 1: Create an Application in Okta

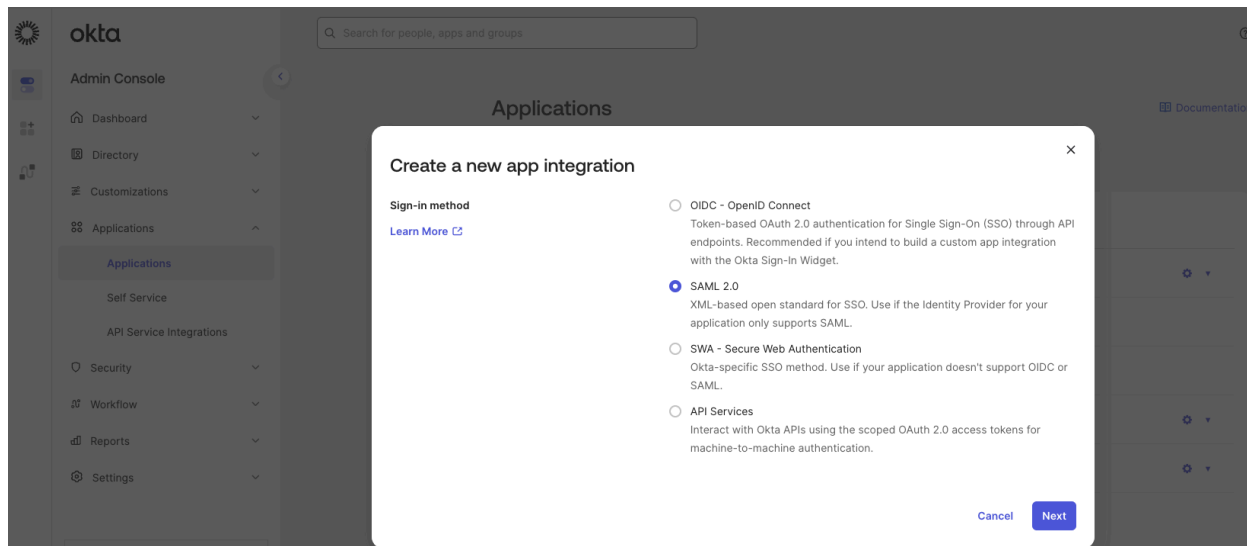
1. Log in to Okta Admin Console

Navigate to **Applications > Create App Integration**.



2. Select the SAML 2.0 Option

Choose **SAML 2.0** and click **Next**.



3. Configure the Application

App Name: Enter a name for the app, e.g., "Gainsight" and Click **Next**

The screenshot shows the Okta Admin Console interface. On the left is a sidebar with the 'Admin Console' menu and various navigation options like Dashboard, Directory, Customizations, Applications, Security, Workflow, Reports, and Settings. The main content area is titled 'Create SAML Integration' and has three steps: 1. General Settings (active), 2. Configure SAML, and 3. Feedback. In the 'General Settings' step, there are three main sections: 'App name' with a text input field, 'App logo (optional)' with a large image upload area containing a gear icon and buttons for upload and delete, and 'App visibility' with a checkbox labeled 'Do not display application icon to users'. At the bottom of the form are 'Cancel' and 'Next' buttons.

4. Enter a Dummy SSO URL and Audience URI

- **Single Sign-On URL:** <https://trial-9582957-admin.Test.com/> (Replace with your own URL)
- **Audience URI (SP Entity ID):** [abc](#) (Replace with your own value)
- Click **Next** to proceed.

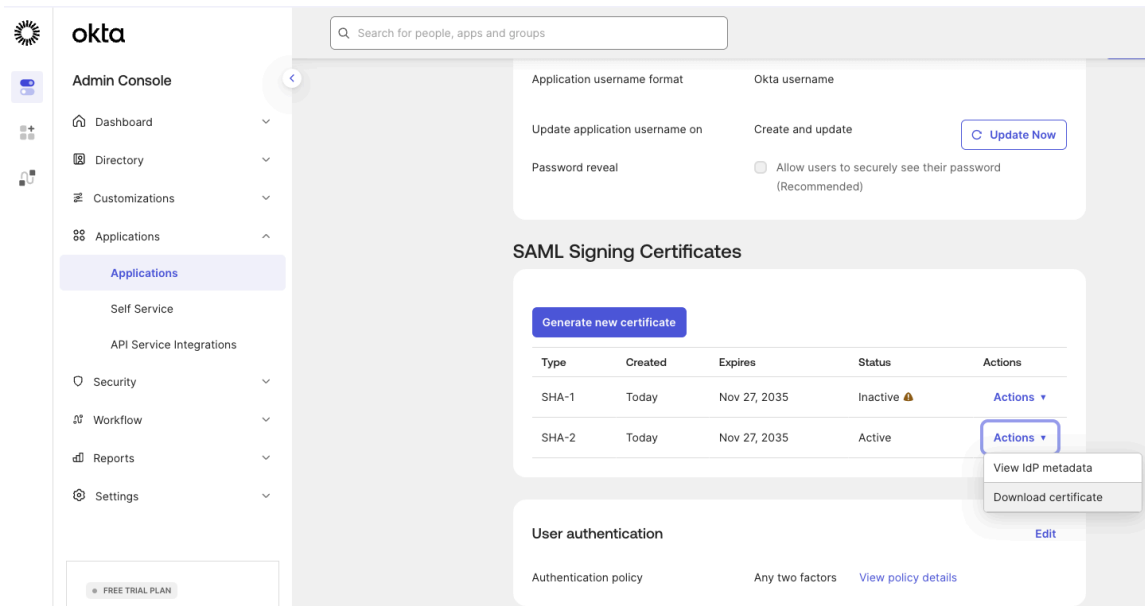
The screenshot shows the 'Configure SAML' step of the 'Create SAML Integration' process. The sidebar is the same as in the previous screenshot. The main content area has three steps: 1. General Settings, 2. Configure SAML (active), and 3. Feedback. The 'SAML Settings' form is divided into a 'General' section and a 'Where do I find the info this form needs?' section. The 'General' section includes: 'Single sign-on URL' with a text input containing 'https://trial-9582957-admin.Test.com/' and a checked checkbox 'Use this for Recipient URL and Destination URL'; 'Audience URI (SP Entity ID)' with a text input containing 'abc'; 'Default RelayState' with a text input and a note 'If no value is set, a blank RelayState is sent'; 'Name ID format' with a dropdown menu set to 'Unspecified'; 'Application username' with a dropdown menu set to 'Okta username'; and 'Update application username on' with a dropdown menu set to 'Create and update'. A 'Show Advanced Settings' link is at the bottom right of the form. The 'Where do I find the info this form needs?' section contains explanatory text about the XML generation and the need for documentation.

5. Finish the App Creation

Click **Finish** to complete the app setup.

6. Download the Certificate

Go to **Applications** > [Your Gainsight App Name] > **Sign On** tab, and download the **SHA-2 Certificate**.



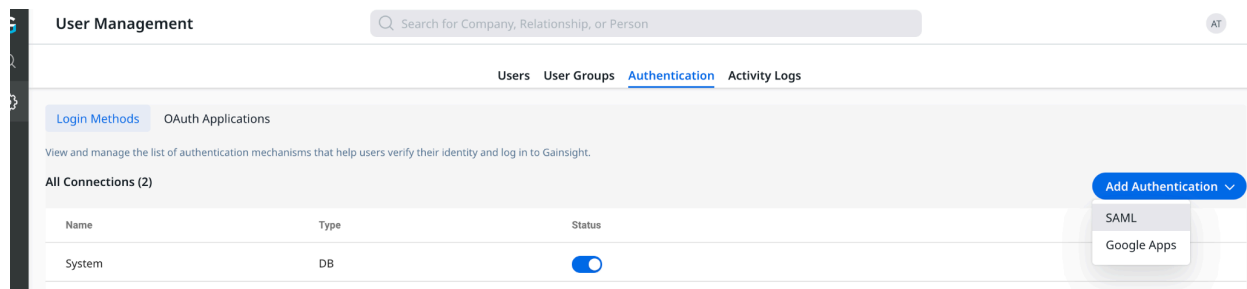
Stage 2: Set Up SAML Authentication in Gainsight

1. Navigate to Gainsight Administration

Go to **Administration** > **User Management** > **Authentication**.

2. Add SAML Authentication

Click **Add Authentication** and select **SAML**.



3. Enter the SAML Details

- **Name:** Choose a name (e.g., "Okta SSO").
- **Email Domain:** Enter your domain, e.g., [yourdomain.com](#).
- **Sign-In URL:** Enter the Dummy URL you created in Okta (e.g., <https://trial-9582957-admin.Test.com/>).
- **Certificate:** Upload the SHA-2 Certificate you downloaded from Okta in Stage 1.

4. Save the Configuration

Click Save to complete the setup in Gainsight.

Users

User Groups

Authentication

Activity Logs

SAML Mechanism

✕

Name *

OKTA

Enter a unique connection name for authentication

Email Domain *

yourdomain.com

Enter the domain name for SAML authentication

Sign In URL *

https://trial-9582957-admin.Test.com


Enter SAML login URL for authentication

Sign Out URL

Enter Sign Out URL

Enter SAML logout URL to exit from authentication

Certificate *

 NewOkta.cert

Field Mapping

Source Field

Username

Target Field

Username

Enter the name of the claim containing User attributes from the source to be mapped to the Username.

Cancel

Save

Stage 3: Update the SSO URL and Entity ID

1. Download the XML File from Gainsight

- Go back to **Administration > User Management > Authentication**.
- Click **Edit** on the SAML configuration you created in Stage 2.

- Click the **Download** button to get the XML file.

The image shows a 'SAML Mechanism' configuration dialog box with a close button (X) in the top right corner. The dialog contains several input fields and sections:

- Name ***: A text input field containing 'OKTA'. Below it is the instruction: 'Enter a unique connection name for authentication'.
- Email Domain ***: A text input field containing 'yourdomain.com'. Below it is the instruction: 'Enter the domain name for SAML authentication'.
- Sign In URL ***: A text input field containing 'https://trial-9582957-admin.Test.com'. Below it is the instruction: 'Enter SAML login URL for authentication'.
- Sign Out URL**: A text input field containing the placeholder 'Enter Sign Out URL'. Below it is the instruction: 'Enter SAML logout URL to exit from authentication'.
- Certificate ***: A section with a file upload icon and the text 'Drag and drop file here or [Browse](#)'.
- Field Mapping**: A section with two input fields:
 - Source Field**: A text input field containing 'Username'.
 - Target Field**: A text input field containing 'Username'.Below these fields is the instruction: 'Enter the name of the claim containing User attributes from the source to be mapped to the Username.'

At the bottom of the dialog, there is a blue 'Download' button with a cloud icon, and 'Cancel' and 'Save' buttons.

2. Extract the SSO URL and Audience URI

- Open the XML file and locate the following:
- a. **Single Sign on URL.** Towards the bottom of the file. It would be the blurred out section from below image. This would need to be copied.

```
23 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat>
24 <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress</NameIDFormat>
25 <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:persistent</NameIDFormat>
26 <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
27 <AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location=""
28   index="0" isDefault="true"/>
29 </SPSSODescriptor>
30 </EntityDescriptor>
```

- b. **Audience URI (SP Entity ID).** Towards the top of the file.. It would be the blurred out section from below image. This would need to be copied.

```
1 <EntityDescriptor entityID="" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
2   <SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
3     <keyDescriptor use="signing">
```

3. Update Gainsight Authentication

- Go to Administration > User Management > Authentication in Gainsight.

- Edit the configuration, and paste the Single Sign-On URL value from the XML file

The screenshot shows the 'SAML Mechanism' configuration dialog. It includes fields for Name (OKTA), Email Domain, Sign In URL (highlighted with a red arrow), Sign Out URL, Certificate, and Field Mapping. The Field Mapping section shows 'Username' mapped to 'Username'. At the bottom are 'Download', 'Cancel', and 'Save' buttons.

SAML Mechanism

Name *

OKTA

Enter a unique connection name for authentication

Email Domain *

Enter the domain name for SAML authentication

Sign In URL *

Enter SAML login URL for authentication

Sign Out URL

Enter Sign Out URL

Enter SAML logout URL to exit from authentication

Certificate *

Drag and drop file here or [Browse](#)

Field Mapping

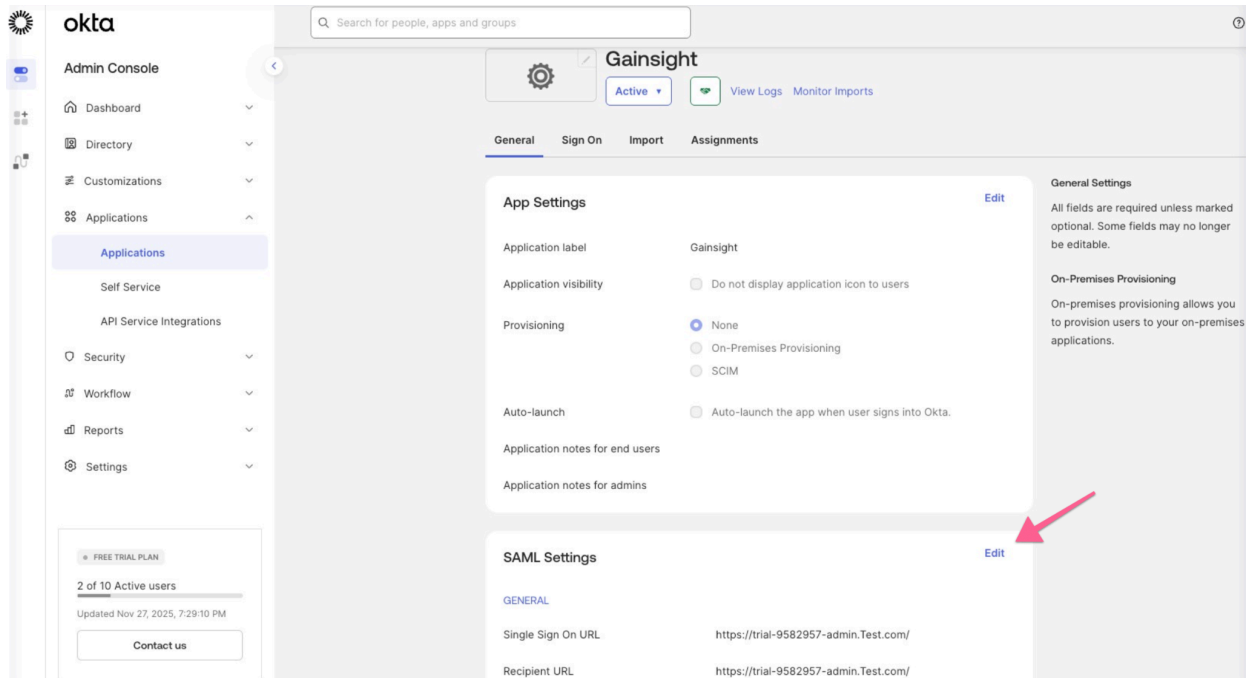
Source Field	Target Field
Username	Username

Enter the name of the claim containing User attributes from the source to be mapped to the Username.

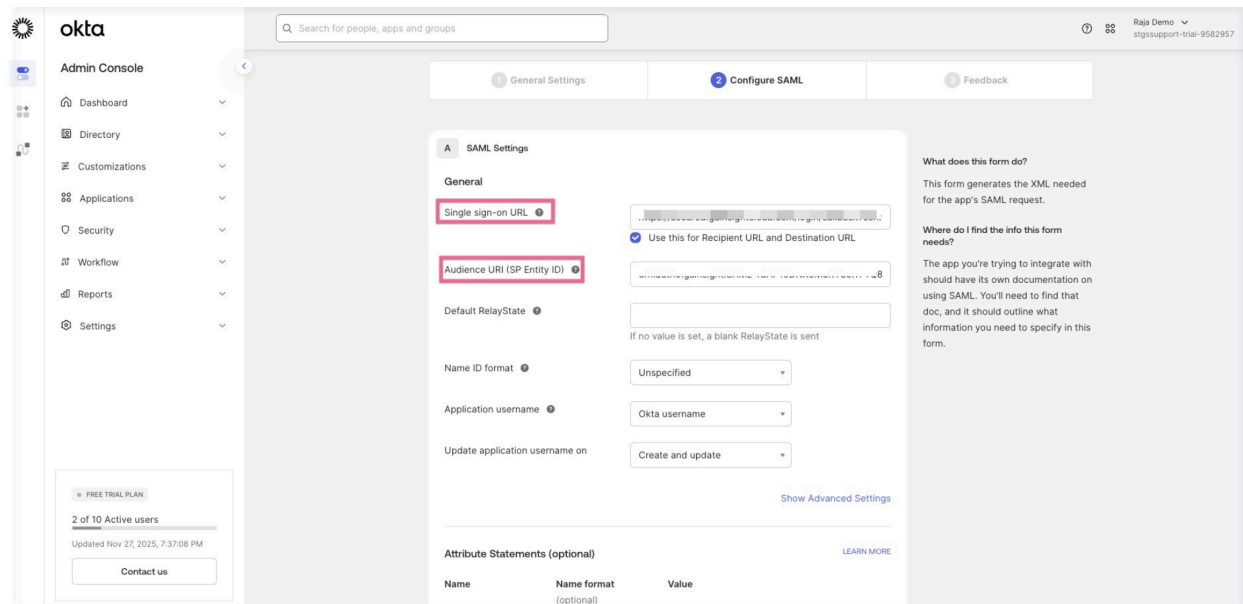
[Download](#) [Cancel](#) [Save](#)

4. Update Okta with the New SSO Information

- In Okta Admin Console, navigate to the General tab of your Gainsight app.
- Click SAML Settings and then click Edit.



- Update the Single Sign-On URL and Audience URI (SP Entity ID) with the values you obtained from the XML file.



Final Steps: Create Attributes and Assign Users in Okta

1. **Create an Email Attribute**

In the Okta **Configure SAML** settings, add an attribute for **Email** and map it to the Okta email value.

2. **Complete the App Configuration**

Click **Next** to proceed, and then **Finish** to complete the app update.

Attribute Statements (optional)

[LEARN MORE](#)

Name	Name format (optional)	Value
email	Unspecified ▼	user.email ▼

[Add Another](#)

Now, the Okta integration setup is now complete. The admin needs to assign the app to the appropriate users or teams.