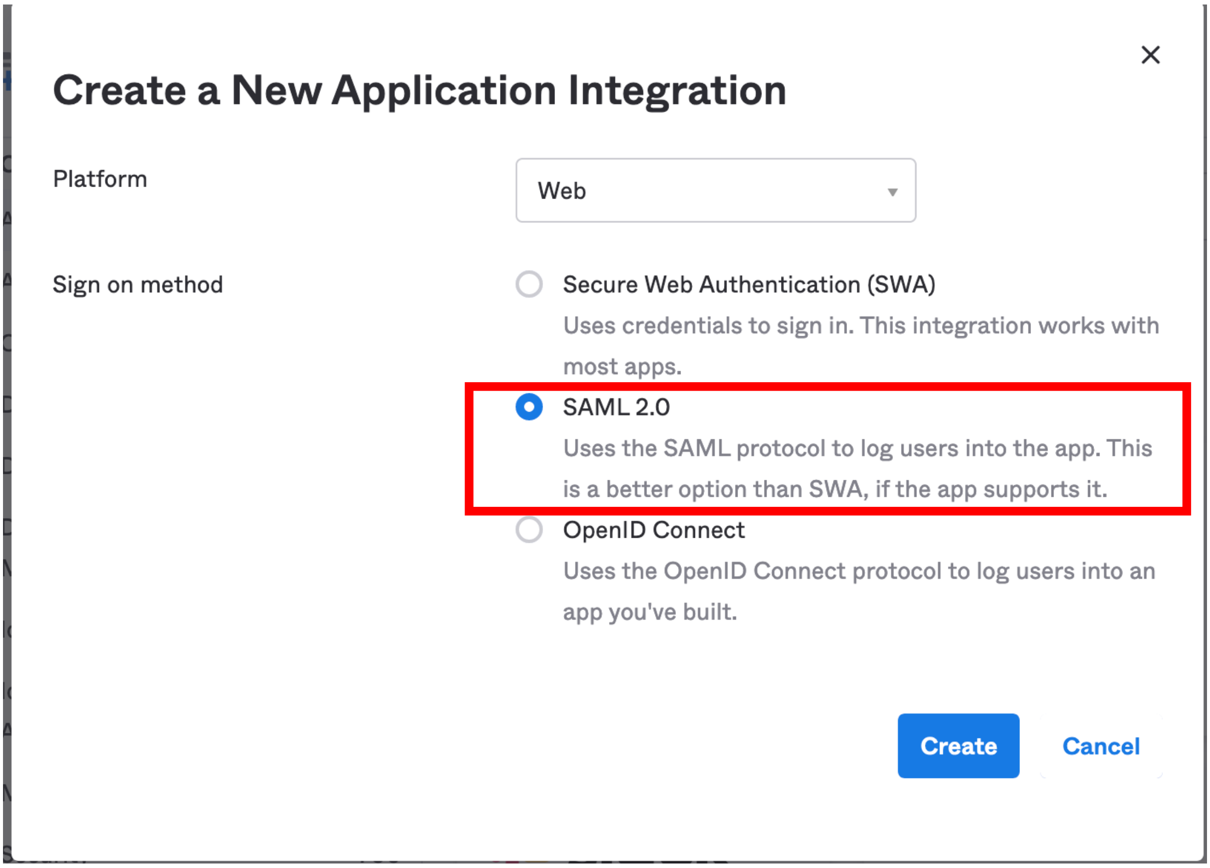
Okta/Cognito Integration in data.all

Okta Actions

1- Create a SAML app in Okta

1. Open the Okta Developer Console. For more information about the console, see The Okta Developer Console: All new, All you on the Okta Developer Blog.
2. In the top left corner, pause on **Developer Console**, and then choose **Classic UI**. This opens the Admin Console. For more information, see Administrator Console on the **Okta Organizations** page of the Okta Developer website.
   Important: You must be in the Admin Console (Classic UI) to create a SAML app.
3. Under **Shortcuts**, choose **Add Applications**.
   --or-- Choose **Applications**, and then choose **Add Application**.
4. On the **Add Application** page, choose **Create New App**.
5. In the **Create a New Application Integration** dialog, confirm that **Platform** is set to **Web**.
6. For **Sign on method**, choose **SAML 2.0**.
7. Choose **Create**.



Create a New Application Integration

Platform: Web

Sign on method

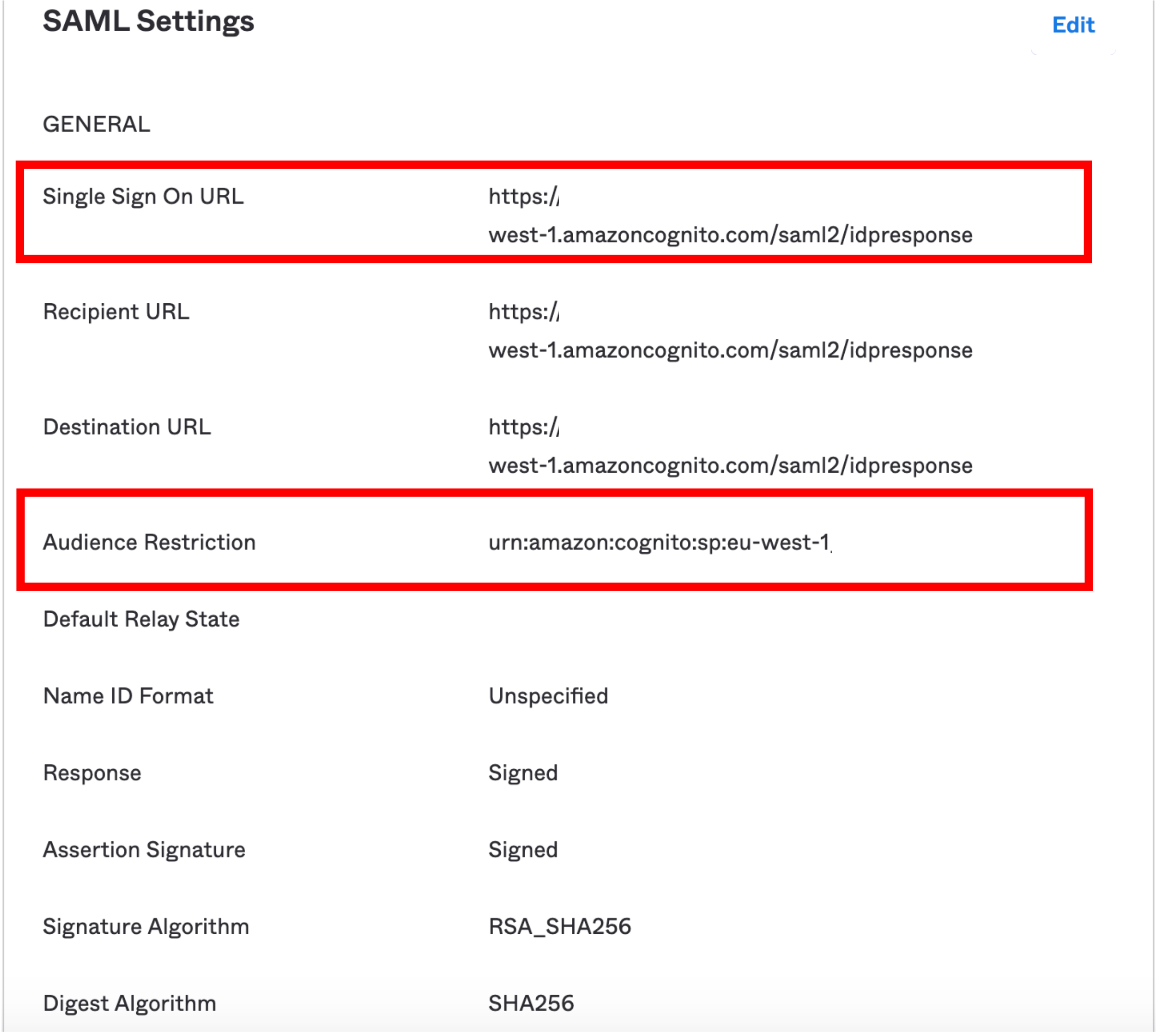
○ Secure Web Authentication (SWA)
Uses credentials to sign in. This integration works with most apps.

● SAML 2.0
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.

○ OpenID Connect
Uses the OpenID Connect protocol to log users into an app you've built.

2- Configure SAML integration for your Okta app

1. On the **Create SAML Integration** page, under **General Settings**, enter a name for your app.
2. (Optional) Upload a logo and choose the visibility settings for your app.
3. Choose **Next**.
4. Under **GENERAL**, for **Single sign on URL**, enter **https://yourDomainPrefix.auth.region.amazoncognito.com/saml2/idpresponse**
Note: Replace **yourDomainPrefix** and **region** with the values for your user pool. You can find these values in the Amazon Cognito console on the **Domain name** page for your user pool.
5. For **Audience URI (SP Entity ID)**, enter **urn:amazon:cognito:sp:yourUserPoolId**.
Note: Replace **yourUserPoolId** with your Amazon Cognito user pool ID. You can find this value in the Amazon Cognito console on the **General settings** page for your user pool.

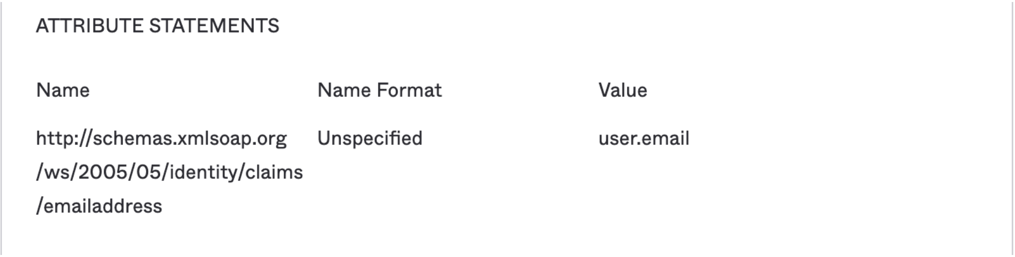


SAML Settings

GENERAL

Single Sign On URL	https:/ west-1.amazoncognito.com/saml2/idpresponse
Recipient URL	https:/ west-1.amazoncognito.com/saml2/idpresponse
Destination URL	https:/ west-1.amazoncognito.com/saml2/idpresponse
Audience Restriction	urn:amazon:cognito:sp:eu-west-1
Default Relay State	
Name ID Format	Unspecified
Response	Signed
Assertion Signature	Signed
Signature Algorithm	RSA_SHA256
Digest Algorithm	SHA256

6. Under **ATTRIBUTE STATEMENTS (OPTIONAL)**, add a statement with the following information:
   For **Name**, enter the SAML attribute name **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress**.
   For **Value**, enter **user.email**.



ATTRIBUTE STATEMENTS

Name	Name Format	Value
http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Unspecified	user.email

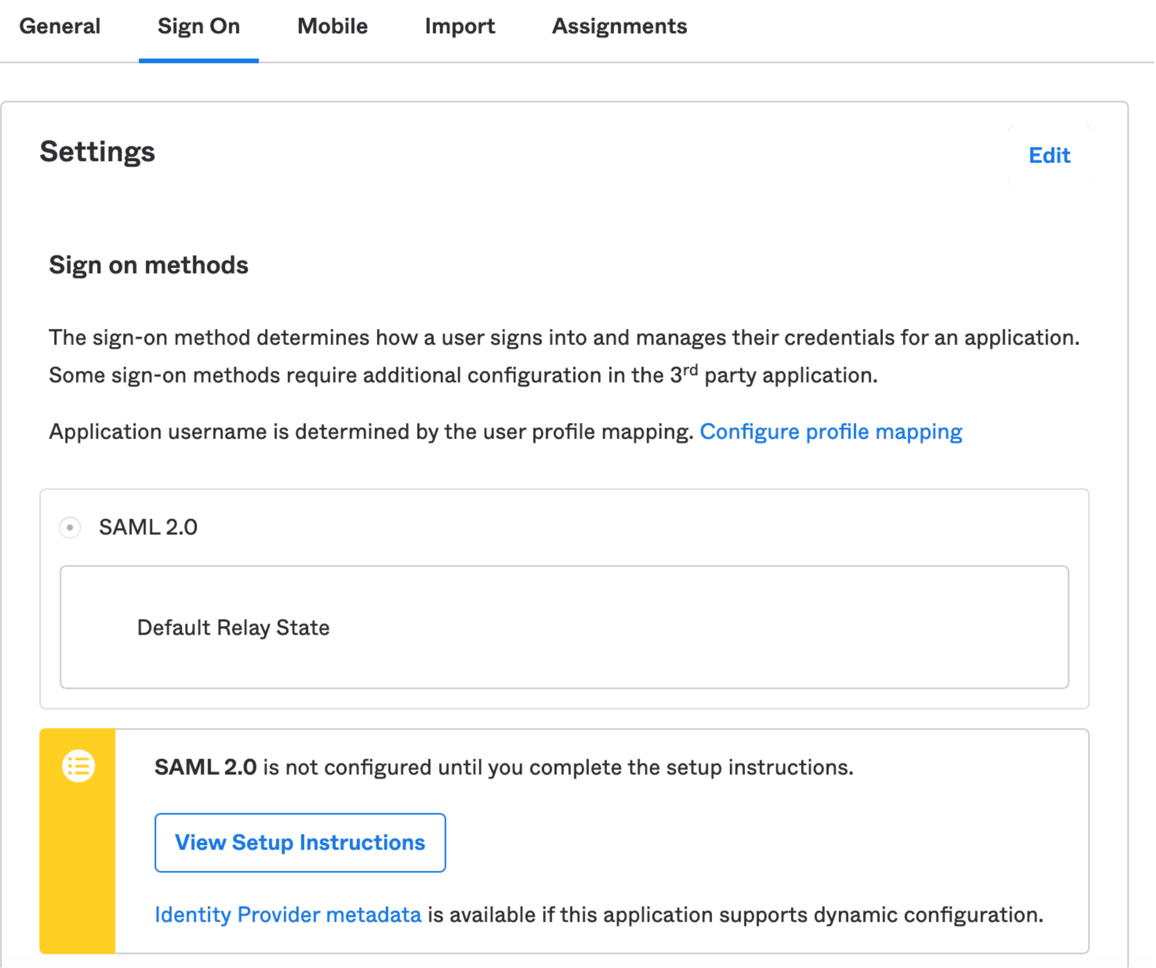
7. For all other settings on the page, leave them as their default values or set them according to your preferences.
8. Choose **Next**.
9. Choose a feedback response for Okta Support.
10. Choose **Finish**.

3- Assign a user to your Okta application

11. On the Assignments tab for your Okta app, for Assign, choose Assign to People.
12. Choose **Assign** next to the user that you want to assign. **Note:** If this is a new account, the only option available is to choose yourself (the admin) as the user.
13. (Optional) For **User Name**, enter a user name, or leave it as the user's email address, if you want.
14. Choose **Save and Go Back**. Your user is assigned.
15. Choose **Done**.

4- Get the IdP metadata for your Okta application

16. On the Sign On tab for your Okta app, find the **Identity Provider metadata** hyperlink. Right-click the hyperlink, and then **copy the URL**.



Settings

Sign on methods

The sign-on method determines how a user signs into and manages their credentials for an application. Some sign-on methods require additional configuration in the 3rd party application.

Application username is determined by the user profile mapping. Configure profile mapping

● SAML 2.0

Default Relay State

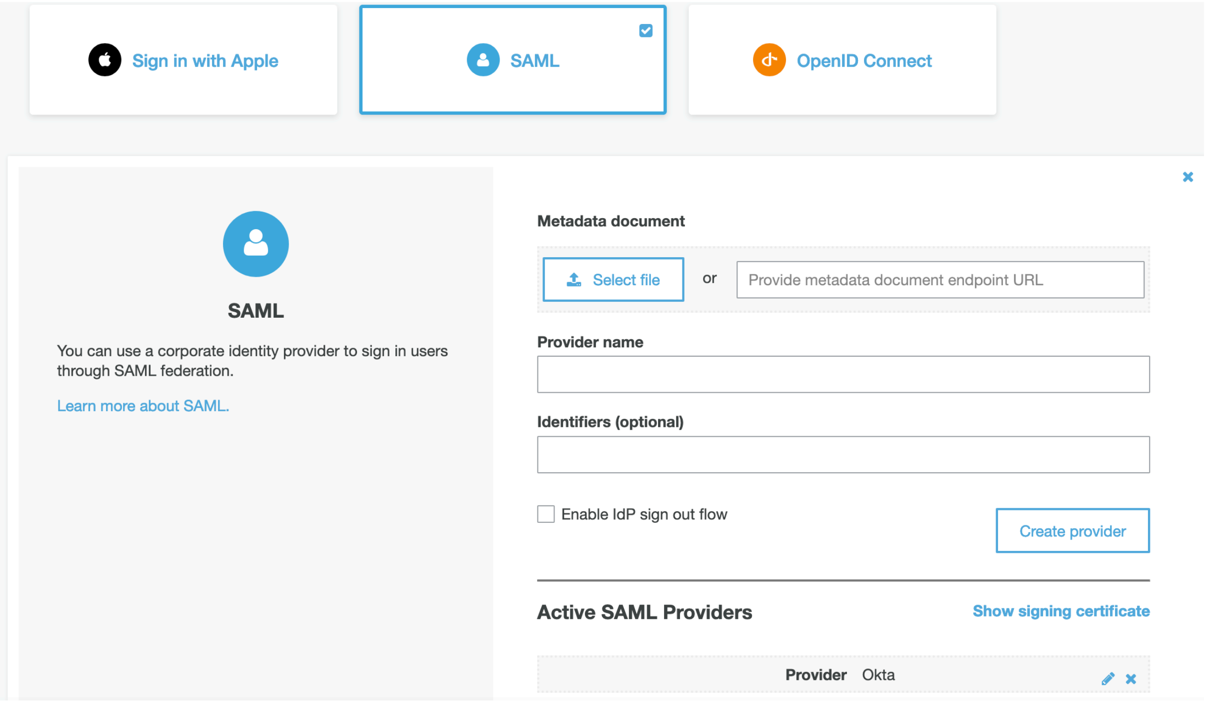
SAML 2.0 is not configured until you complete the setup instructions.

Identity Provider metadata is available if this application supports dynamic configuration.

Cognito (data.all) Actions

5- Configure Okta as a SAML IdP in your user pool

1. In the [Amazon Cognito console](), choose **Manage user pools**, and then choose your user pool.
2. In the left navigation pane, under **Federation**, choose **Identity providers**.
3. Choose **SAML**.
4. Under **Metadata document**, paste the **Identity Provider metadata** URL that you copied.
5. For **Provider name**, enter **Okta**. For more information, see [Choosing SAML Identity Provider Names]().
6. (Optional) Enter any SAML identifiers (**Identifiers (Optional)**) and enable sign-out from the IdP (Okta) when your users sign out from your user pool (**Enable IdP sign out flow**).
7. Choose **Create provider**.



SAML

You can use a corporate identity provider to sign in users through SAML federation.

Learn more about SAML.

Metadata document

Select file or Provide metadata document endpoint URL

Provider name

Identifiers (optional)

□ Enable IdP sign out flow

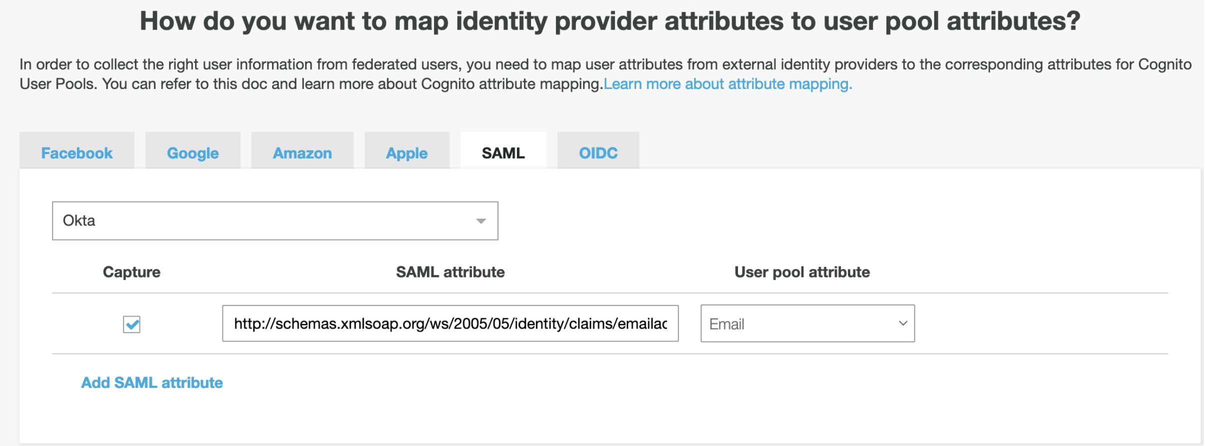
Active SAML Providers

Provider Okta

For more information, see [Creating and managing a SAML identity provider for a user pool (AWS Management Console)]().

6- Map email address from IdP attribute to user pool attribute

1. In the [Amazon Cognito console](), choose **Manage user pools**, and then choose your user pool.
2. In the left navigation pane, under **Federation**, choose **Attribute mapping**.
3. On the attribute mapping page, choose the **SAML** tab.
4. Choose **Add SAML attribute**.
5. For **SAML attribute**, enter the SAML attribute name **http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress**.
6. For **User pool attribute**, choose **Email** from the list.



How do you want to map identity provider attributes to user pool attributes?

In order to collect the right user information from federated users, you need to map user attributes from external identity providers to the corresponding attributes for Cognito User Pools. You can refer to this doc and learn more about Cognito attribute mapping.Learn more about attribute mapping.

Okta

Capture	SAML attribute	User pool attribute
☑	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailac	Email

Reference

[1] https://aws.amazon.com/premiumsupport/knowledge-center/cognito-okta-saml-identity-provider/