

## How to Configure Okta for Authentication

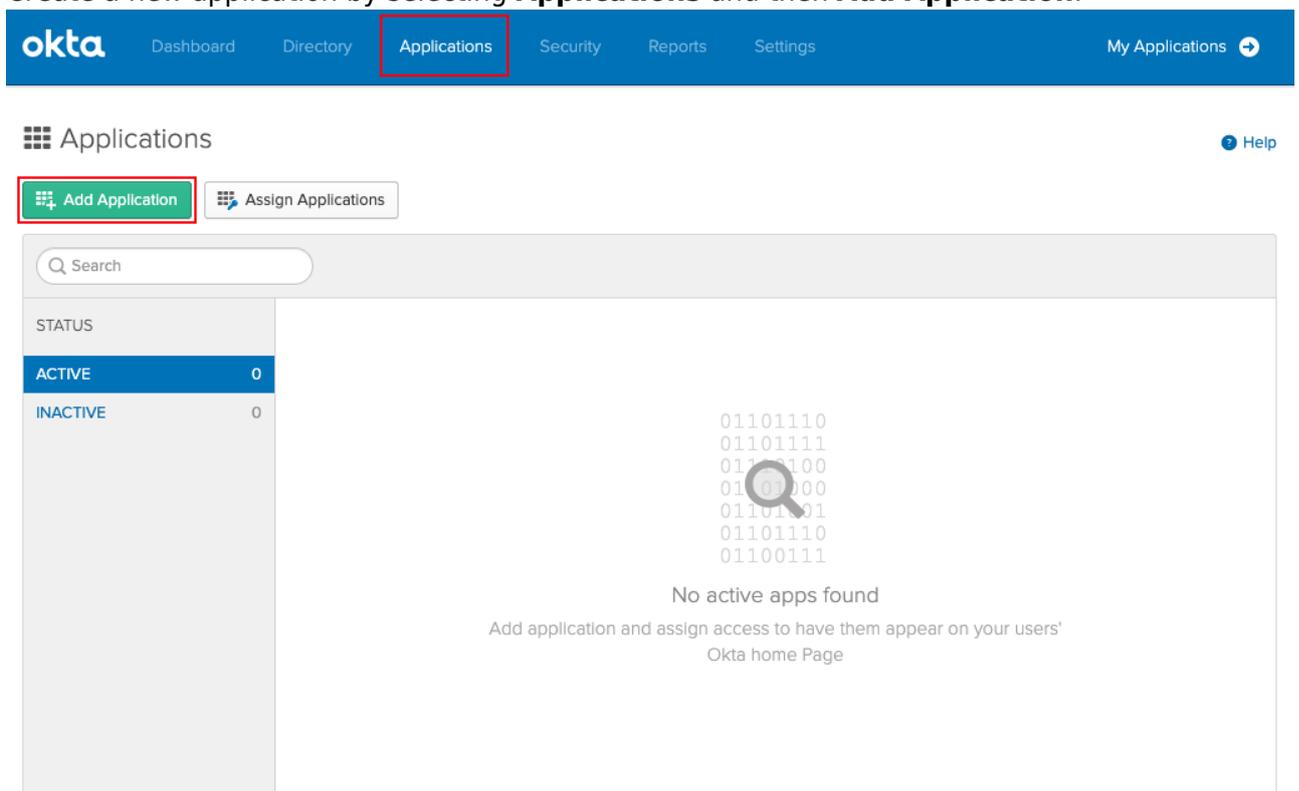
<https://campus.barracuda.com/doc/93201541/>

Use the following steps to create an Okta SAML application to use with CloudGen Access Enterprise Console.

- These steps are also found in [this Okta tutorial](#).
- This tutorial was created with **Okta Version 2019.03.2**

### Configure SAML

1. Log into your Okta organization as a user with administrative privileges.
2. Create a new application by selecting **Applications** and then **Add Application**.



okta Dashboard Directory **Applications** Security Reports Settings My Applications →

Applications Help

**Add Application** Assign Applications

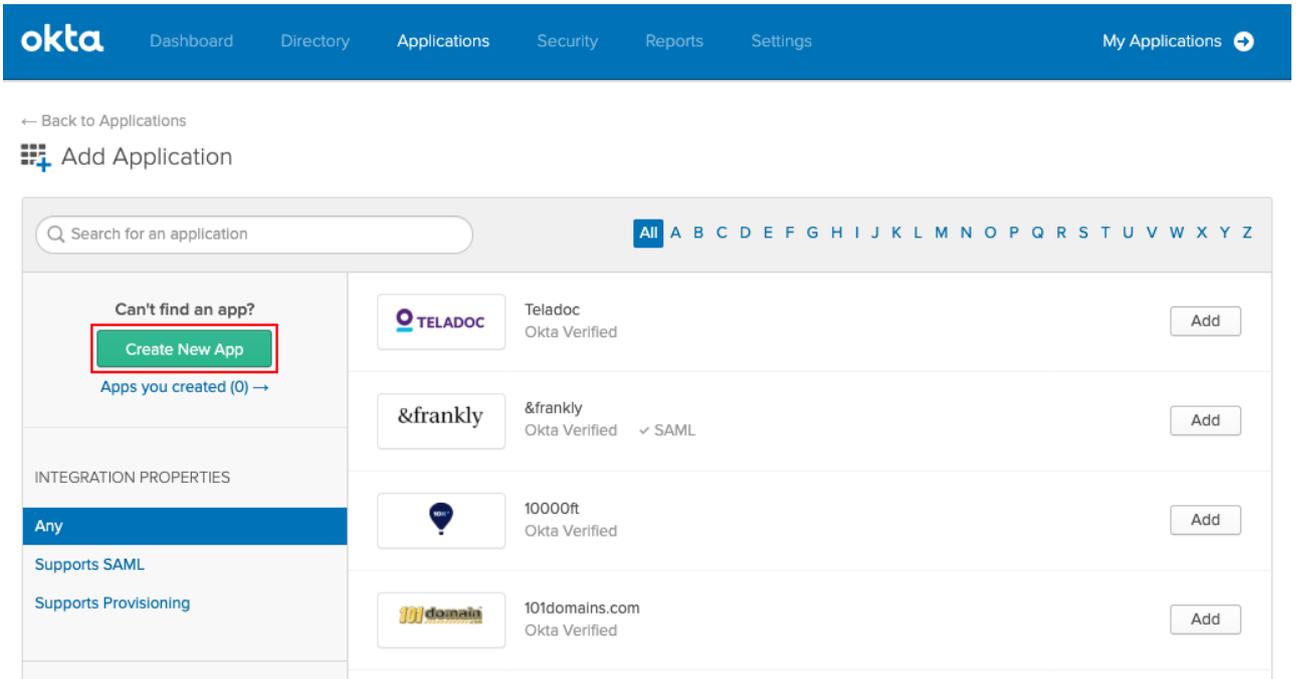
Q Search

STATUS	
ACTIVE	0
INACTIVE	0

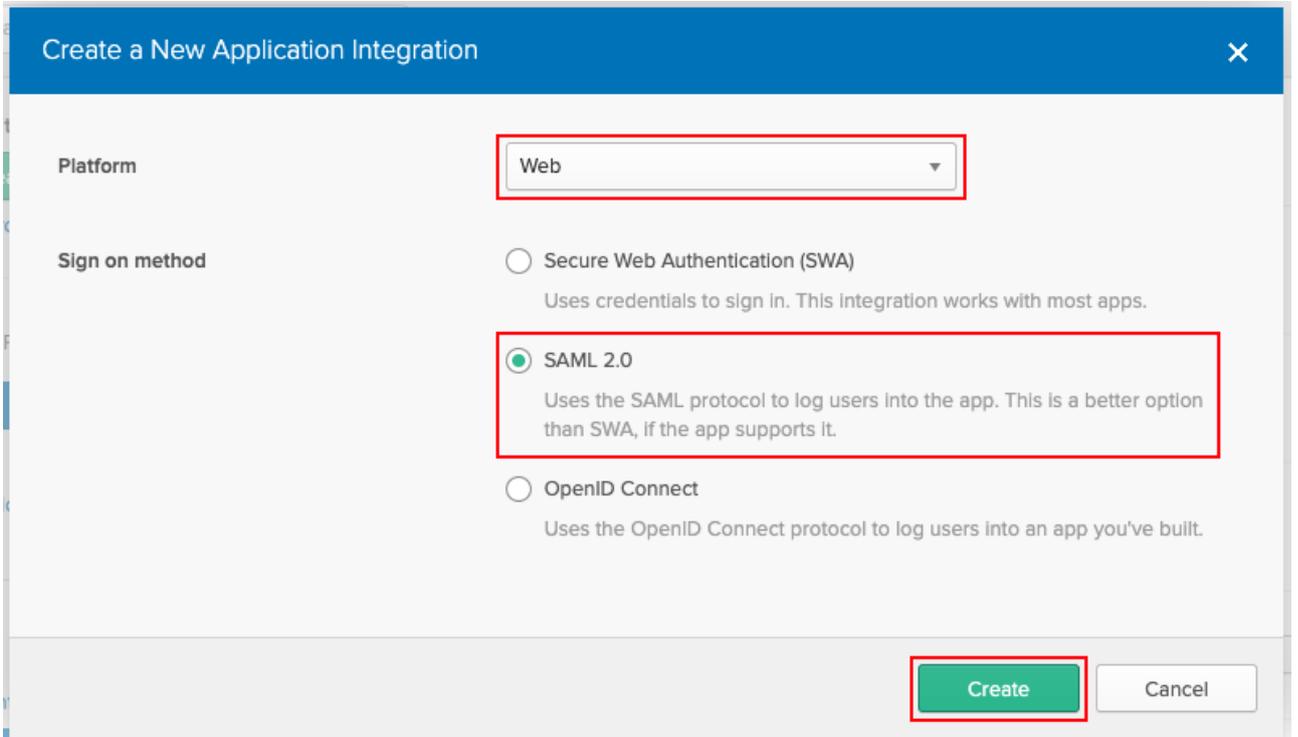
01101110  
01101111  
01101100  
01101100  
01101101  
01101110  
01100111

No active apps found  
Add application and assign access to have them appear on your users'  
Okta home Page

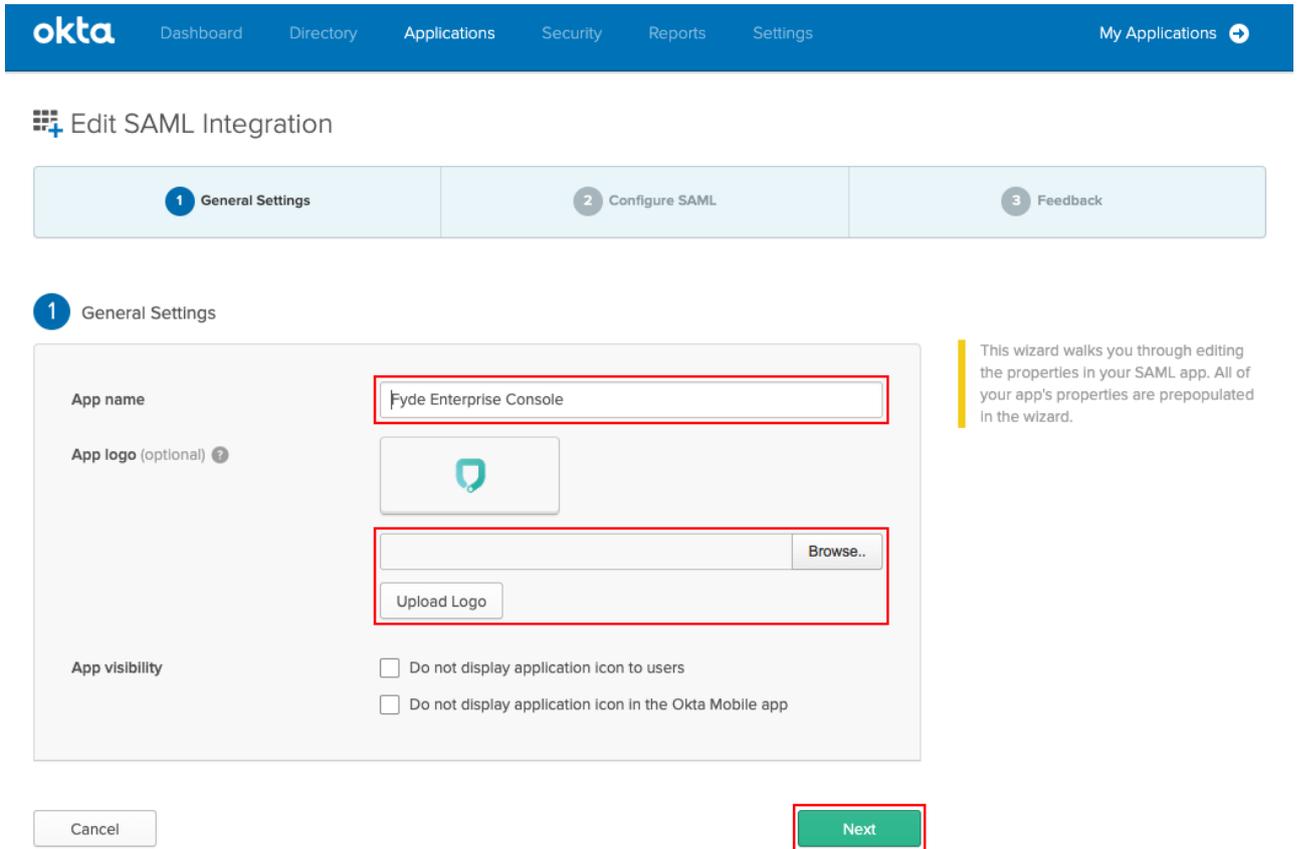
3. Select **Create New App**.



- 4. Configure custom application type:
  - 1. Select **Platform Web**.
  - 2. Select **Sign on method SAML 2.0**.
- 5. Click **Create** to continue.



- 6. Configure custom application type:
  - Insert the desired **App name** (for example: Enterprise Console).
- 7. Select **Next** to continue.



okta Dashboard Directory Applications Security Reports Settings My Applications

### Edit SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

1 General Settings

App name: Fyde Enterprise Console

App logo (optional): [Placeholder icon] [Browse...]

Upload Logo

App visibility:

- Do not display application icon to users
- Do not display application icon in the Okta Mobile app

Cancel Next

This wizard walks you through editing the properties in your SAML app. All of your app's properties are prepopulated in the wizard.

8. In this menu, the values will be used that were obtained from Step 2 in [How to Configure SAML 2.0 Configuration](#):

Fill in the following:

- **Single sign on URL** (Assertion Consumer Service URL)
- Ensure the **Use this Recipient URL and Destination URL** check box is selected.
- **Audience URI** (SP Entity ID)
- Ensure Application username is set to **Email**.
- Leave the remaining fields to defaults (as shown).

9. Select **Show Advanced Settings** to continue.

okta Dashboard Directory Applications Security Reports Settings My Applications

### Edit SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

#### A SAML Settings

**GENERAL**

Single sign on URL   
 Use this for Recipient URL and Destination URL  
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID)

Default RelayState   
If no value is set, a blank RelayState is sent

Name ID format

Application username

Update application username on

[Show Advanced Settings](#)

#### What does this form do?

This form generates the XML needed for the app's SAML request.

#### Where do I find the info this form needs?

The app you're trying to integrate with should have its own documentation on using SAML. You'll need to find that doc, and it should outline what information you need to specify in this form.

#### Okta Certificate

Import the Okta certificate to your Identity Provider if required.

[Download Okta Certificate](#)

10. In the **Advanced Settings** section, ensure that all the values are set as below.

[Hide Advanced Settings](#)

Response

Assertion Signature

Signature Algorithm

Digest Algorithm

Assertion Encryption

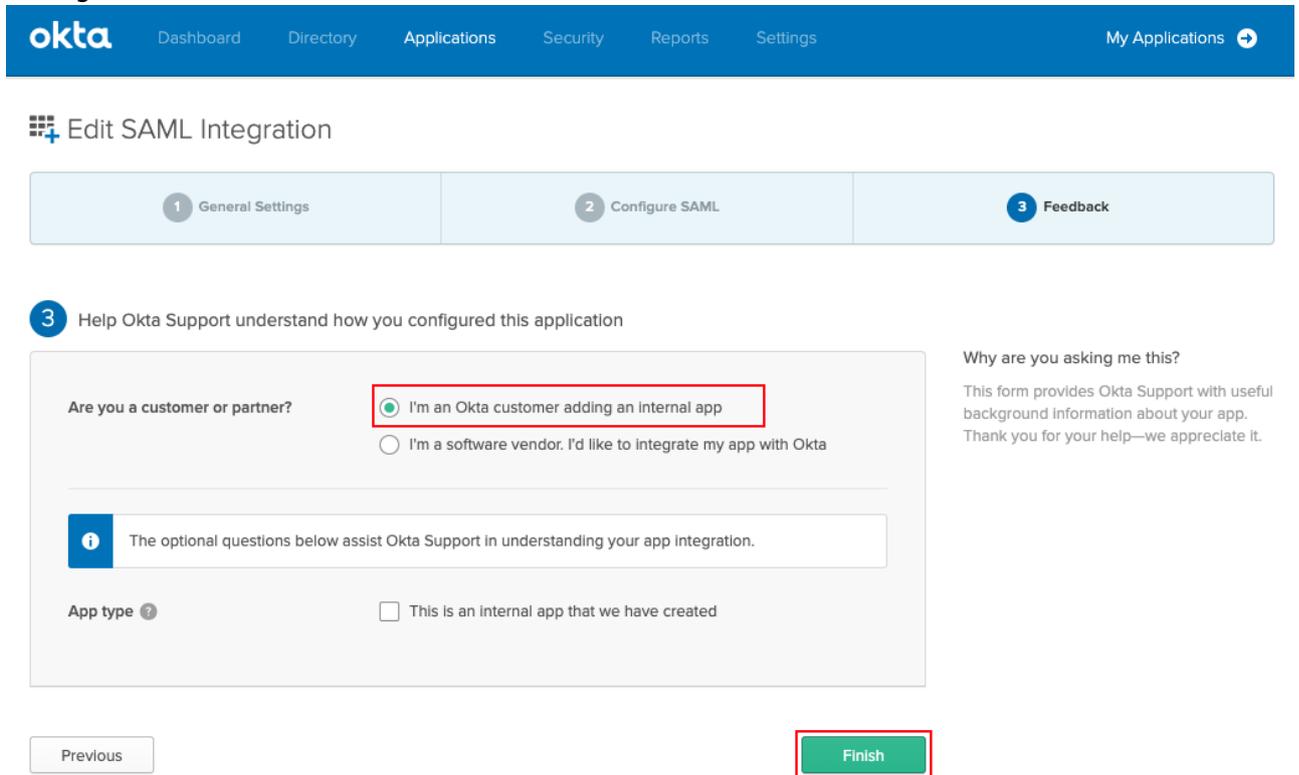
Enable Single Logout  Allow application to initiate Single Logout

Authentication context class

Honor Force Authentication

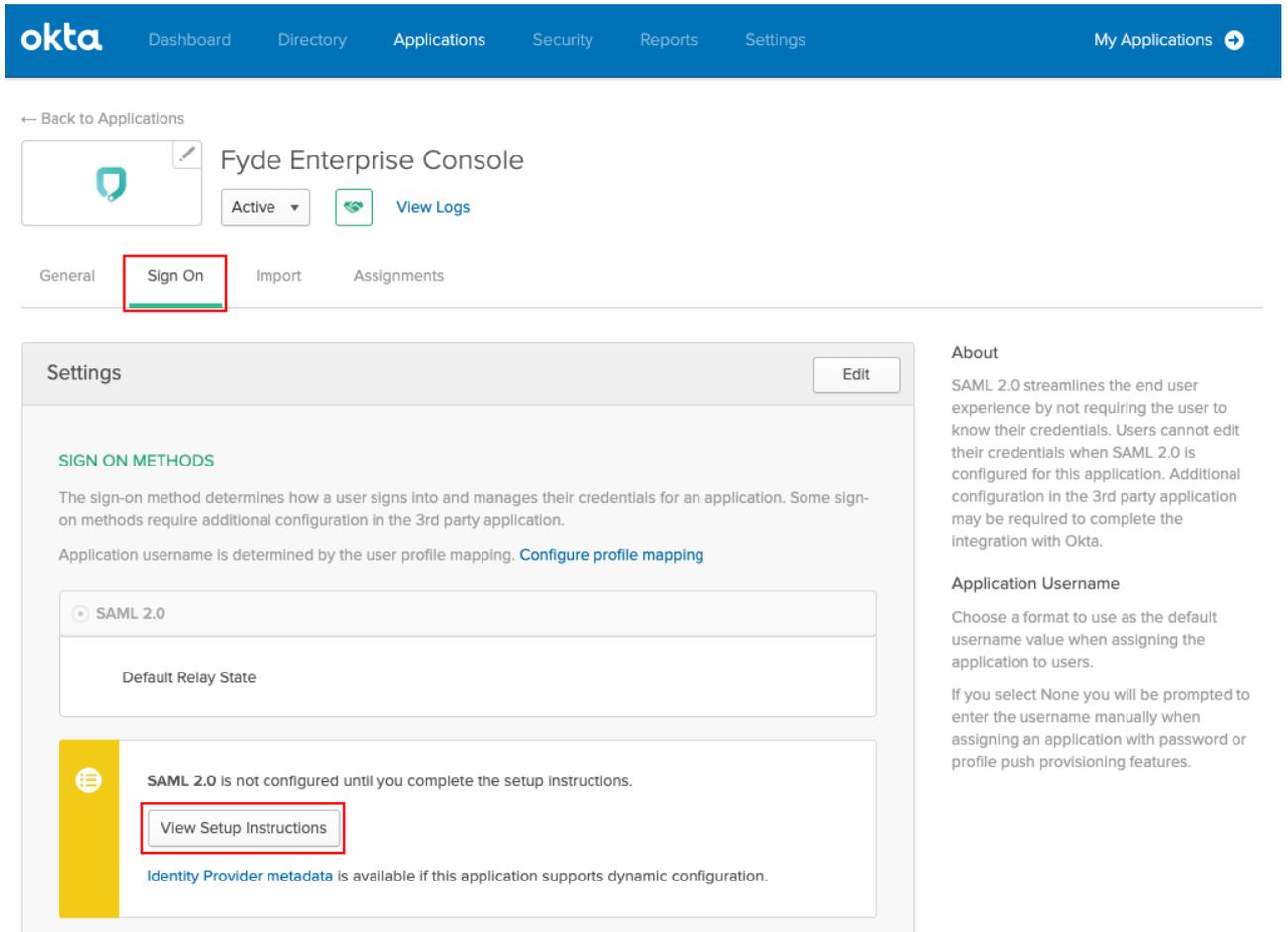
SAML Issuer ID

11. Click **Next** to continue.
12. Configure feedback and click **Finish**.



The screenshot shows the Okta 'Edit SAML Integration' page. The navigation bar at the top includes 'okta', 'Dashboard', 'Directory', 'Applications', 'Security', 'Reports', 'Settings', and 'My Applications'. The main heading is 'Edit SAML Integration'. Below it is a progress bar with three steps: '1 General Settings', '2 Configure SAML', and '3 Feedback'. The '3 Feedback' step is active. The main content area is titled '3 Help Okta Support understand how you configured this application'. It contains a form with the question 'Are you a customer or partner?' and two radio button options: 'I'm an Okta customer adding an internal app' (which is selected and highlighted with a red box) and 'I'm a software vendor. I'd like to integrate my app with Okta'. Below this is an information box with a blue 'i' icon and the text 'The optional questions below assist Okta Support in understanding your app integration.' Underneath is the 'App type' section with a checkbox for 'This is an internal app that we have created'. At the bottom of the form are two buttons: 'Previous' and 'Finish' (which is highlighted with a red box).

13. Get provider definitions by selecting **Sign On** and **View Setup Instructions**.
  - o Use the values obtained to continue the Step 3 configuration in [How to Configure SAML 2.0 Configuration](#):
  - o **Identity Provider Issuer - Entity ID**
  - o **Identity Provider Single Sign-On URL - SSO URL**
  - o **X.509 Certificate - Certificate**



The screenshot shows the Okta management interface. At the top is a blue navigation bar with the Okta logo and menu items: Dashboard, Directory, Applications, Security, Reports, Settings, and My Applications. Below this is a breadcrumb trail: ← Back to Applications. The main content area is for the 'Fyde Enterprise Console' application, which is currently 'Active'. There are tabs for General, Sign On (highlighted with a red box), Import, and Assignments. The 'Sign On' tab is open, showing a 'Settings' panel with an 'Edit' button. Under 'SIGN ON METHODS', there is a section for 'SAML 2.0' with a 'Default Relay State' field. A yellow warning box indicates 'SAML 2.0 is not configured until you complete the setup instructions.' and contains a 'View Setup Instructions' button (highlighted with a red box). Below the warning, it notes that 'Identity Provider metadata' is available if the application supports dynamic configuration. To the right of the settings panel is an 'About' section explaining SAML 2.0 and an 'Application Username' section with instructions on how to choose a format.

- 14. This app must be assigned to users:  
Ensure that you configure the desired assignments.

**okta**   Dashboard   Directory   Applications   Security   Reports   Settings   My Applications →

← Back to Applications

 **Fyde Enterprise Console**  
Active ▾    View Logs

General   Sign On   Import   **Assignments**

Assign ▾    Convert Assignments      People ▾

FILTERS	Person	Type
<b>People</b>	 <p>No users found</p>	
Groups		

**SELF SERVICE**

You need to enable self service for org managed apps before you can use self service for this app.  
[Go to self service settings](#)

**Requests**   Disabled

**Approval**   -

## Figures

1. ec-saml-okta-new-application.png
2. ec-saml-okta-create-new-app.png
3. ec-saml-okta-new-app-type.png
4. ec-saml-okta-general-settings.png
5. ec-saml-okta-settings.png
6. ec-saml-okta-settings-advanced.png
7. ec-saml-okta-feedback.png
8. ec-saml-okta-provider.png
9. ec-saml-okta-assign.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.