

How to Configure Okta for Authentication

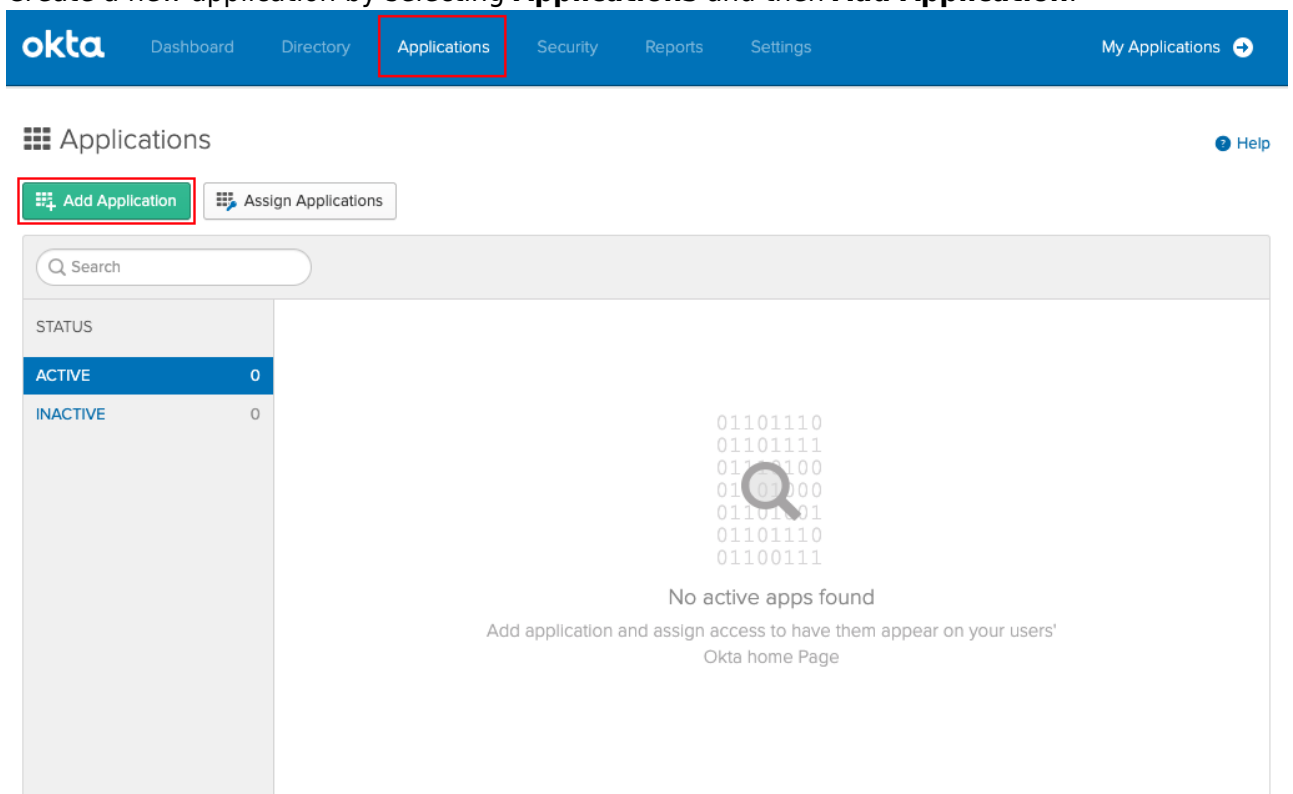
<https://campus.barracuda.com/doc/93201541/>

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

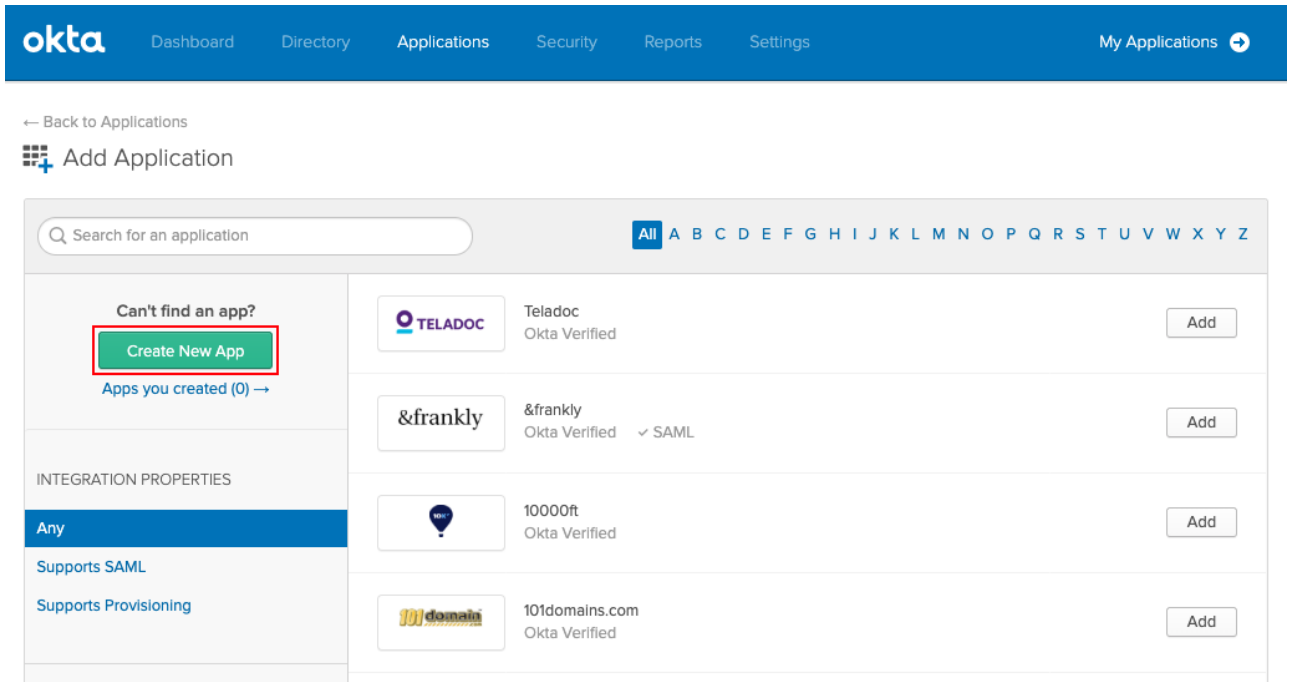
- These steps are also found in [this Okta tutorial](#).
- This tutorial was created with **Okta Version 2019.03.2**

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**.

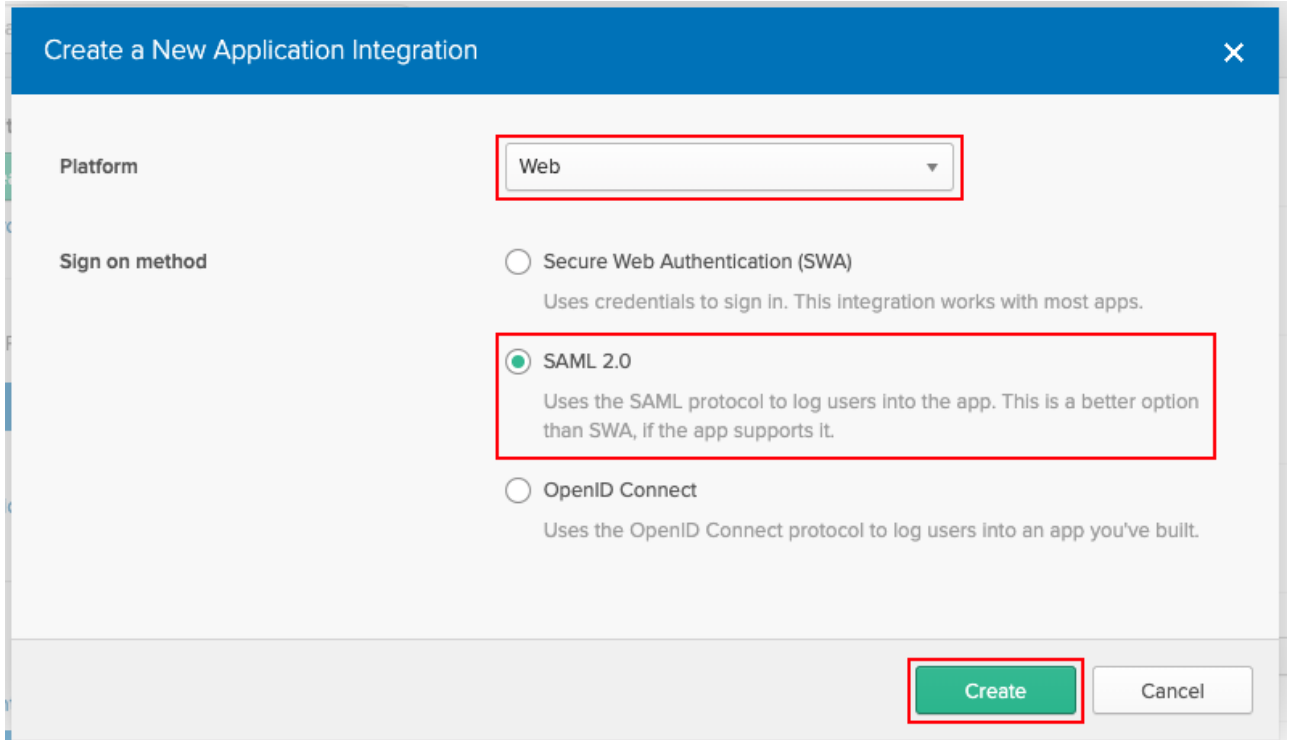


3. Select **Create New App**.



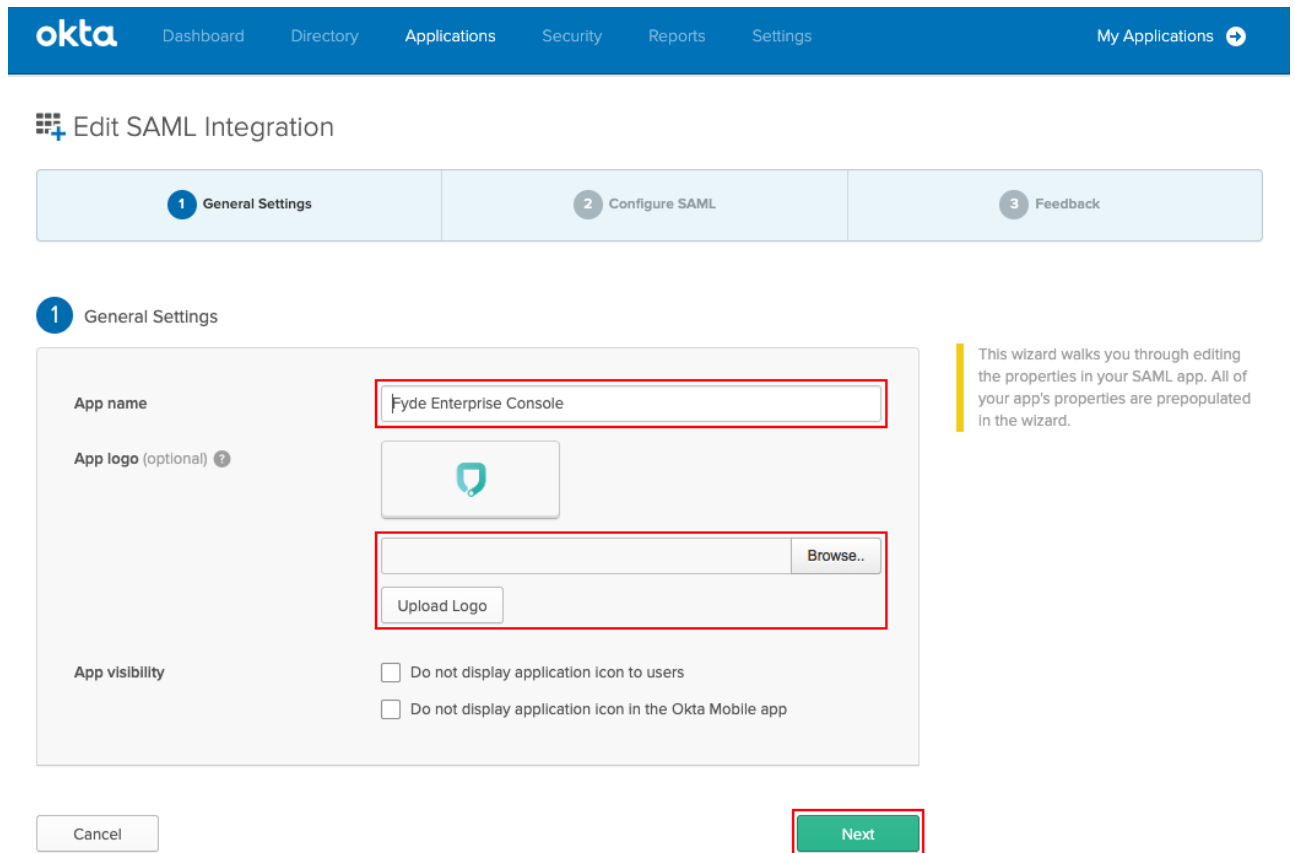
The screenshot shows the Okta Applications page. At the top is a navigation bar with links: Dashboard, Directory, Applications, Security, Reports, Settings, and My Applications. Below the navigation bar is a breadcrumb trail: ← Back to Applications, followed by a '+ Add Application' button. A search bar is present with the text 'Search for an application'. To the left of the application list is a sidebar with a 'Can't find an app?' section containing a 'Create New App' button (highlighted with a red box) and a link 'Apps you created (0) →'. Below this is the 'INTEGRATION PROPERTIES' section with a tab 'Any' and two options: 'Supports SAML' and 'Supports Provisioning'. The main area displays a list of applications: Teladoc, &frankly, 10000ft, and 101domains.com, each with an 'Add' button.

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



The screenshot shows the 'Create a New Application Integration' dialog. It has a blue header with the title and a close button. The 'Platform' dropdown is set to 'Web' (highlighted with a red box). Under 'Sign on method', there are three radio button options: 'Secure Web Authentication (SWA)', 'SAML 2.0' (selected and highlighted with a red box), and 'OpenID Connect'. Each option has a descriptive text below it. At the bottom right, there are 'Create' and 'Cancel' buttons, with 'Create' highlighted by a red box.

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) ?

Upload Logo

Browse...

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 ?

Unspecified

Application username ?

Email

Update application username on

Create and update

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 ?

Signed

Assertion Signature ?

Signed

Signature Algorithm ?

RSA-SHA256

Digest Algorithm ?

SHA256

Assertion Encryption ?

Unencrypted

Enable Single Logout ?
☐ Allow application to initiate Single Logout

Authentication context class ?

PasswordProtectedTransport

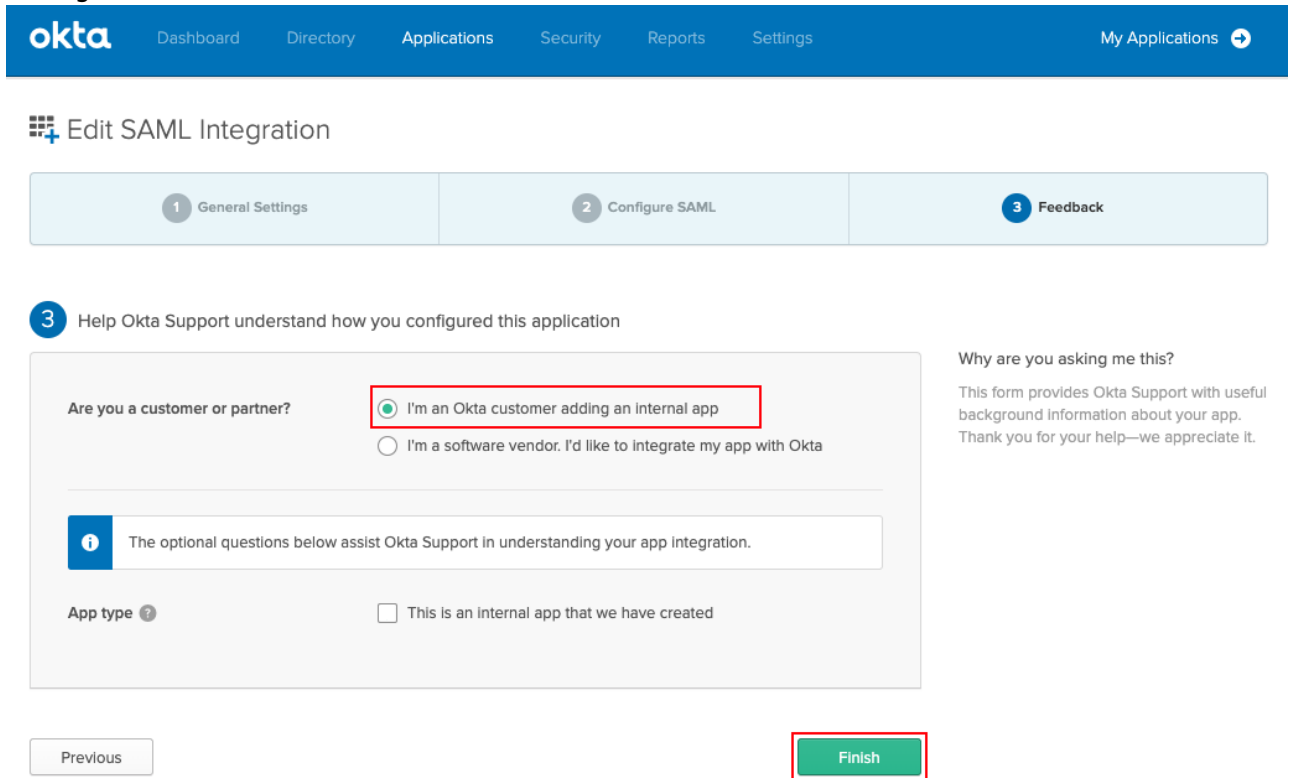
Honor Force Authentication ?

Yes

SAML Issuer ID ?

http://www.okta.com/\${org.externalKey}

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



okta Dashboard Directory Applications Security Reports Settings My Applications →

Edit SAML Integration

1 General Settings 2 Configure SAML 3 Feedback

3 Help Okta Support understand how you configured this application

Are you a customer or partner?

☒ I'm an Okta customer adding an internal app

☐ I'm a software vendor. I'd like to integrate my app with Okta

i The optional questions below assist Okta Support in understanding your app integration.

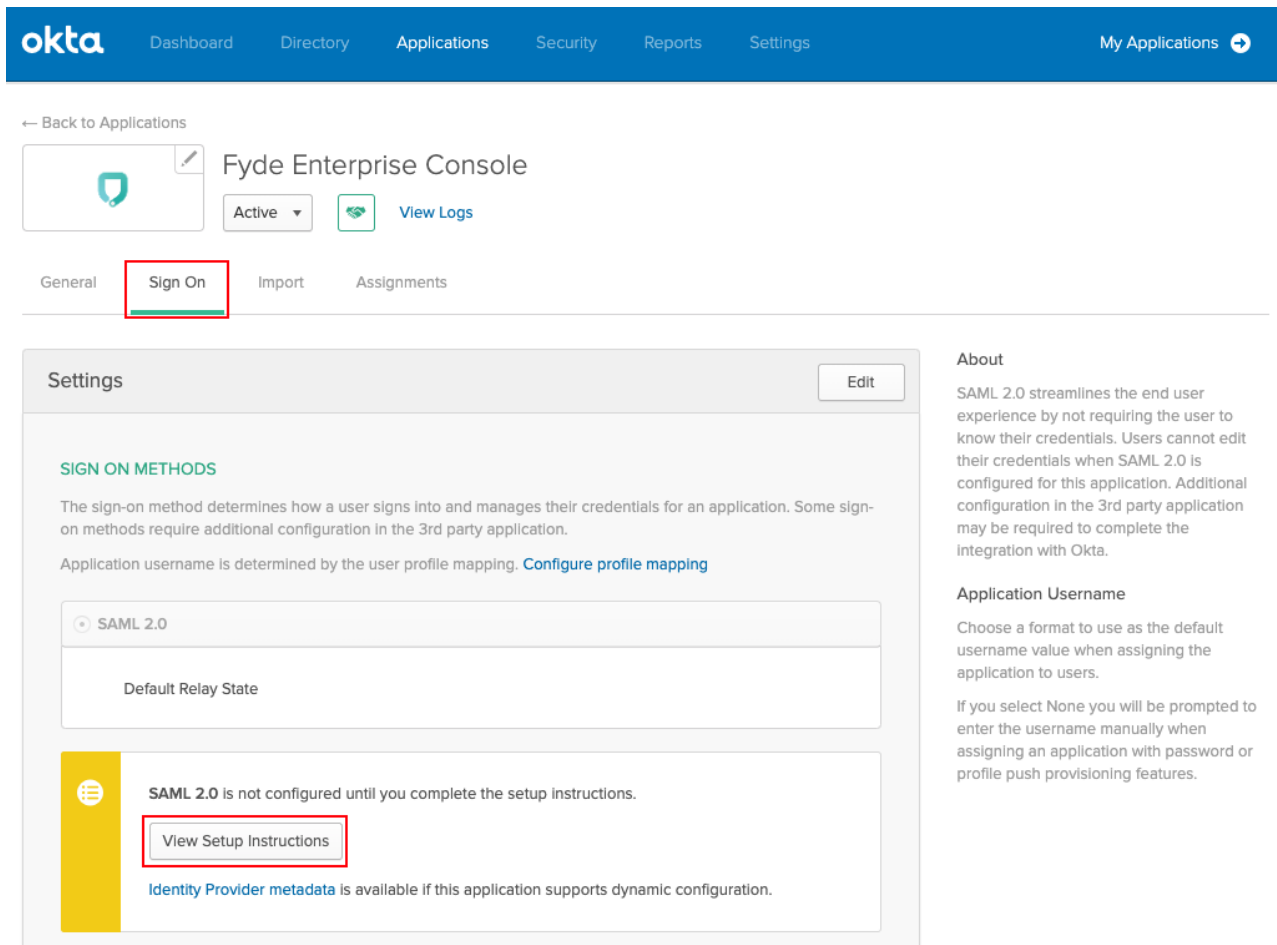
App type ? ☐ This is an internal app that we have created

Previous Finish

Why are you asking me this?

This form provides Okta Support with useful background information about your app. Thank you for your help—we appreciate it.

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



← Back to Applications

okta Dashboard Directory Applications Security Reports Settings My Applications

Fyde Enterprise Console Active View Logs

General **Sign On** Import Assignments

Settings Edit

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.

[View Setup Instructions](#)

[Identity Provider metadata](#) is available if this application supports dynamic configuration.

About

SAML 2.0 streamlines the end user experience by not requiring the user to know their credentials. Users cannot edit their credentials when SAML 2.0 is configured for this application. Additional configuration in the 3rd party application may be required to complete the integration with Okta.



Application Username

Choose a format to use as the default username value when assigning the application to users.


If you select None you will be prompted to enter the username manually when assigning an application with password or profile push provisioning features.

14. This app must be assigned to users:



Ensure that you configure the desired assignments.

 [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
People	<div><p>01101110 01101111 01101100 01101000 01101001 01101110 01100111</p><p>No users found</p></div>	
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	-

Edit

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.