

Okta SSO Configuration Guide

This document guides an Okta administrator through the steps necessary to set up Single Sign On (SSO) functionality via Okta with Brivo. For information and support using Okta with Brivo outside the scope detailed in this guide, please contact Okta.



Configuration

- Configuring Okta for Single Sign On..... 2
- Configuring General Settings 5
- Configuring SAML Settings 6
- Configuring Feedback..... 8

Configuration

When configuration is complete, Brivo will need the following information to establish the Okta SSO connection:

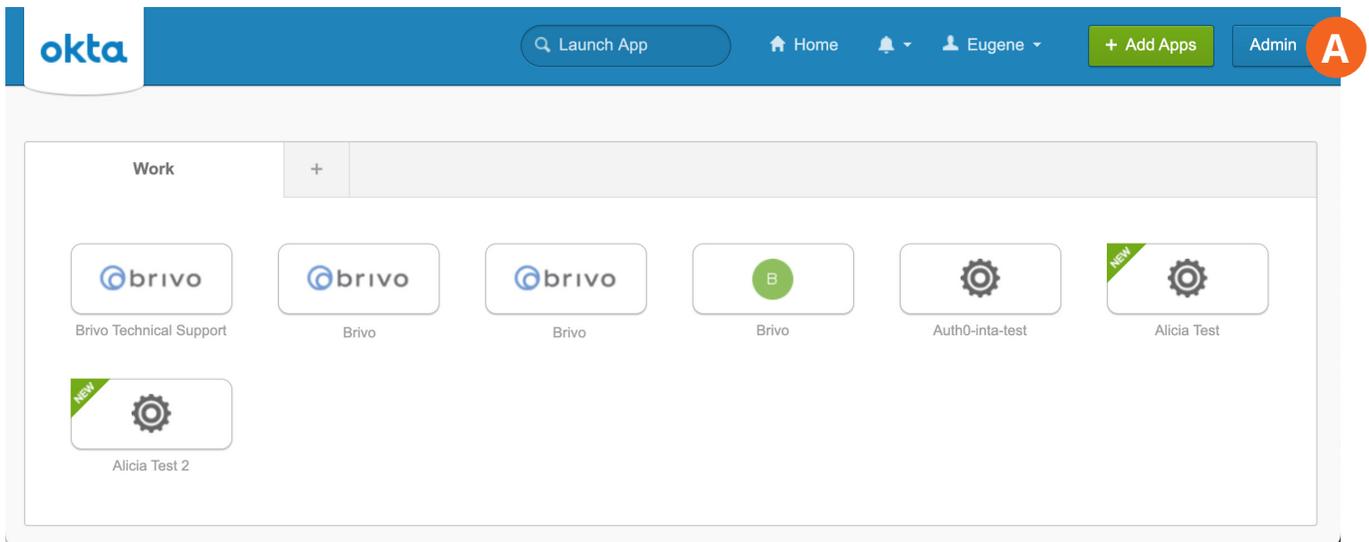
connectionName - See page 6 of this guide

Identity Provider Single Sign-On URL - See page 11 of this guide

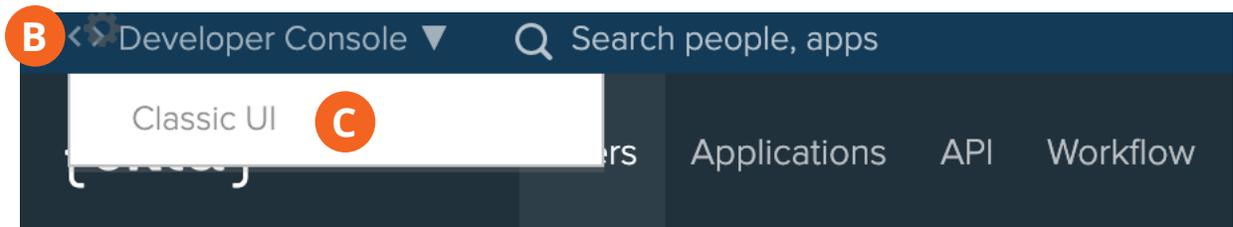
X.509 Certificate - See page 11 of this guide

Configuring Okta for Single Sign On (SSO)

1. Login to the Okta Admin Console using your Okta account sandbox link.
2. Verify that you are using the Admin Console (A). If you are using the Developer Console, you will need to switch over to the Admin Console.



3. If you see <> Developer Console (B) in the top left corner of your console, click on it and select Classic UI (C) from the dropdown menu.



- In the Admin Console, click on the Applications (A) link.

Dashboard

- The Applications page will display. Click on the Add Application (B) button.

Applications

- Click on the Create New App (C) button on the upper right side of the page.

← Back to Applications

Add Application

Create New App



CATEGORIES	
Featured	
API Management	6
Apps	6114
Apps for Good	9
CASB	3
Directories and HR Systems	13
Security Applications	662
Okta Applications	11

7. To create a SAML integration, select Web (A) as the Platform and SAML 2.0 (B) for the Sign on method, and click on the Create (C) button to complete the process.

Create a New Application Integration ✕

Platform A

Sign on method

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

B 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.

C

Configuring General Settings

1. On the General Settings page, specify a name for your application in the App Name (A) field.

NOTE: In order to prevent problems with accounts with similar names, Brivo recommends that you use your Brivo account name and account number for the App Name entry. This will be unique and should avoid any problems.

2. Optionally, you may click on the Upload Logo button (B) and upload a logo image (.png, .jpg, or .gif only) with a maximum image size of 1400 by 400 pixels and a file size of less than 100kb. Be sure to check both checkboxes (C) for App Visibility. When complete, click Next (D)

1 General Settings

App name **A**

App logo (optional) **B**

App visibility **C** Do not display application icon to users
 Do not display application icon in the Okta Mobile app

D

Configuring SAML Settings

A SAML 2.0 configuration requires a combination of information from both your organization and the target application. For help completing each field, use your app-specific documentation and the Okta tool tips.

The single sign on URL is the location where the SAML assertion is sent with a POST operation. This URL is required and serves as the default ACS URL value for the Service Provider (SP). This URL is always used for IdP-imitated sign-on requests.

1. Enter your single sign on URL (A) in the field provided. The single sign on URL is provided by Brivo with the connection name provided by the end-user.

`https://login.brivo.com/login/callback?connection=(user provided connection name)`

2. Check the **Use this for Recipient URL and Destination URL** checkbox (B).

3. Enter your audience URI (SP Entity ID) (C) in the field provided. This is the intended audience of the SAML assertion. This is usually the Entity ID of your application.

`urn:auth0:brivo:(user provided connection name)`

Note: It is suggested that you use your domain name for the user provided connection name. For instance, in the example below, we have used **ezstor** for the connection name.

A SAML Settings

GENERAL

Single sign on URL ? **A**

B Use this for Recipient URL and Destination URL
 Allow this app to request other SSO URLs

Audience URI (SP Entity ID) ? **C**

Default RelayState ?

If no value is set, a blank RelayState is sent

Name ID format ?

Application username ?

Update application username on

[Show Advanced Settings](#)

When you create a new SAML integration, or modify an existing one, you may define custom attribute statements. These statements are inserted into the SAML assertions shared with your application.

- In the Attribute Statements section, enter **email** in the name field (A), select **Unspecified** (B) from the Name format dropdown menu, and enter **user.email** in the Value (C) field.

Name	Name format	Value
email A	Unspecified B	user.email C

[Add Another](#)

- When finished, click on the green Next button at the bottom of the page.

Configuring Feedback

- As an Okta customer adding an integration that is intended for internal use only, select the **I'm an Okta customer adding an internal app** (A) button. When selected, an additional set of optional questions appear and may be completed by the end user at your discretion.

- Help Okta Support understand how you configured this application

Are you a customer or partner?

A I'm an Okta customer adding an internal app

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

- Click the green Finish button at the bottom of the page and you are returned to the Application Description Page.
- Click on the Assignments (B) tab. By clicking on the green Assign (C) button on the left side of the page, you may Assign to People (D) or Assign to Groups (E) the ability to use Okta Single Sign On.

← Back to Applications



EZ Storage Single Sign On

Active ▾
 View Logs

General
Sign On
Mobile
Import
Assignments **B**

C Assign ▾
 Convert Assignments

Q Search...

People ▾

	Type
Assign to People D	
Assign to Groups E	

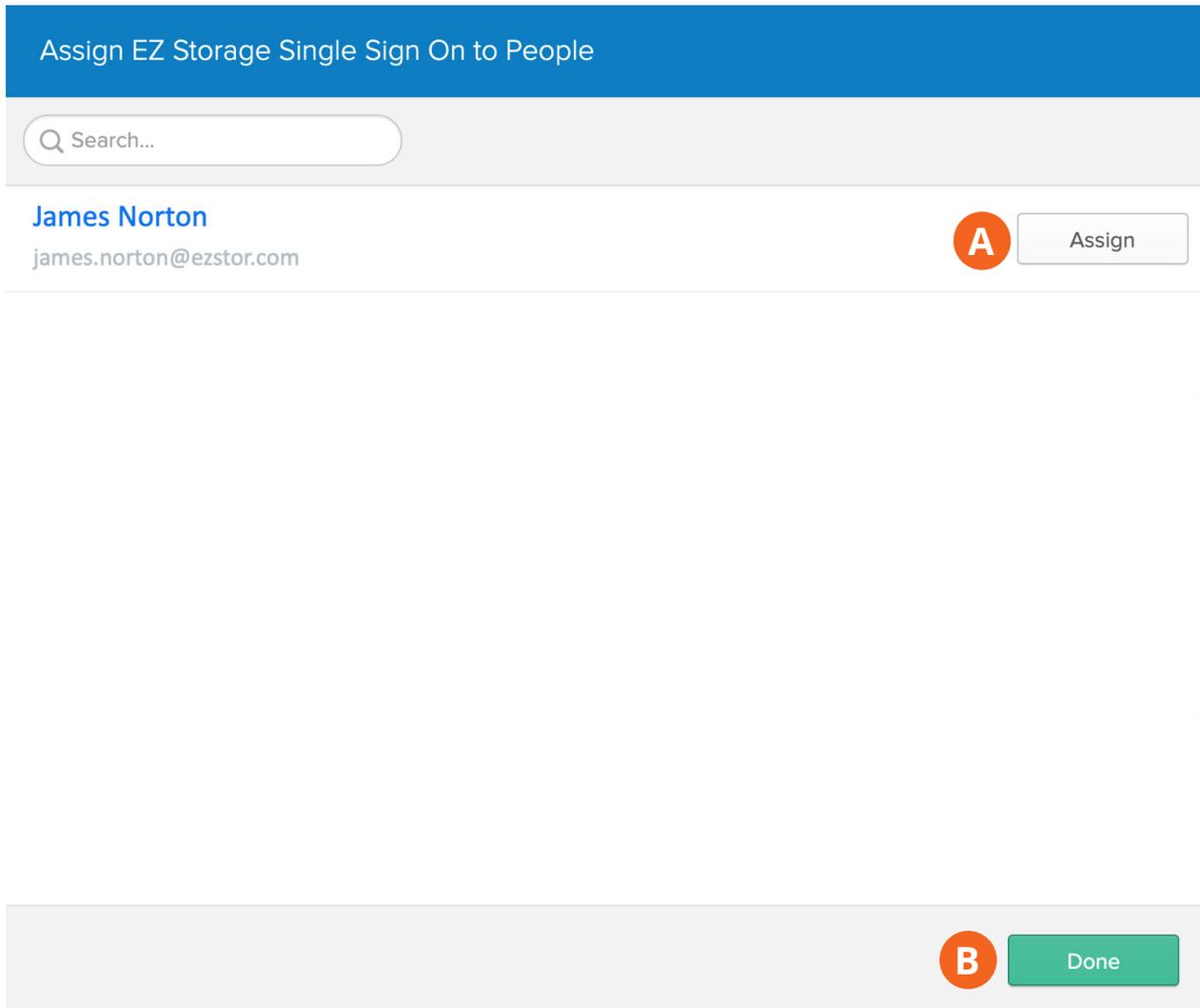
Groups

01101110
01101111
01110100
01001000
01101001
01101110
01100111



No users found

4. For the purposes of this guide, we will assign a person. When the Assignment pop-up window appears, click on the Assign (A) button next to the people you wish and click Done (B) when finished.



Assign EZ Storage Single Sign On to People

Q Search...

James Norton
james.norton@ezstor.com

A Assign

B Done

5. You are returned to the Application Description Page.

6. Click on the Sign On tab (A) and then click on the View Setup Instructions (B) button.

EZ Storage Single Sign On

Active ▾

View Logs

A

Sign On

Mobile

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

B

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

CREDENTIALS DETAILS

Application username format

Update application username on

Password reveal

Okta username

Create and update

Allow users to securely see their password (Recommended)

Update Now

© 2022 Brivo Systems LLC. All rights reserved.

10

PUB-Okta SSO Configuration Guide v1.5

- The How to Configure SAML 2.0 for Your Application page displays.
- The Identity Provider Single Sign-On URL (A) and the X.509 Certificate (B) should be copied and provided to Brivo in the following steps.

How to Configure SAML 2.0 for EZ Storage Single Sign On Application

The following is needed to configure EZ Storage Single Sign On

1 Identity Provider Single Sign-On URL:

`https://dev-567529.oktapreview.com/app/brivodev567529_ezstoragesinglesignon_1/exks2uvrgj0xSU4110h7/sso/saml` **A**

2 Identity Provider Issuer:

`http://www.okta.com/exks2uvrgj0xSU4110h7`

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDpDCCAoygAwIBAgIGAWOC/VDVMA0GCSqGSIb3DQEBCwUAMIGSMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcml5TEWMBQGA1UEBwwNU2FuIEZyYW55LjAeXjAzbzENMAsGA1UECgwET2t0YTEU
MBIGA1UECmlwLlNPUHJvdmlkZXIxEzARBgNVBAMMcmR1di01Njc1MjkxHDAaBgkqhkiG9w0BCQEW
DW1uZm9Ab2t0YS55LjB20wHhcNMjgwNTIxMTM1NjA5WhcNMjgwNTIxMTM1NzA5WjCBKjELMAkGA1UE
BhMCMV9MxZzARBgNVBAGMCKNhG1mb3JuaWExFjAUBgNVBACMDVNhbiBGcmFuY21zY28xDTALBgNV
BAoMBE9rdGEzFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRMwEQYDVQQDDApkZXZlbnV3NTI1I5MRwwGgYJ
KoZlhcNAQkBFg1pbmZvQ99rdGEuY29tMIIIBjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
hKx4cBPdNLqGPOq1I1+WbtGUfHQuq1ci1BiUiX69JdaOKKndb85euTMsCQ2F6BL2nd04SP+c/mbn
xMGR0Lfd86tDQeXwPXJCIFEWV5FF/LGd8dyBsSu8ac9Cz2jIq27bxKsOXkkIFJ2ae2g9mR/QWqIQ
9xqiVevgS8uSs680JK/eC94YZ77qKQLBM1vYpVzJdndRtjI1CKu9x2ZnahvrEaaRtpKFceawvS2t
gPjfh1NGRS2oVKgfhGnbGt2tYJRXY8EJkEG6G9Kfv0FgYqoCLCrI5XKfXRgruT3vuH2gChu2x
Su6QT06q7rJrIY+9jHX2+fPLtr9CAs+RMWgVHQIDAQABMA0GCSqGSIb3DQEBCwUAA4IBAQAcbjqc
kkdth91bj7Gz01Gwi40Gv1F25NiDD+nXw98KQYPSYI0DQE6m43pBBRw6xOWIVsg3h6d6YRjwArJY
XnIQhEJQk16cFaSOU07yglcZYD30CIx/LjLHG4txiA5Qg/Es5uqrEUXnaRDnv/hmptYxCE/VTIq
AnbMD1a1SXWM5iQn2ocNObJbuTOFjbWPb81BGG2uvPWkb7EfeXciU2kiDUgV8i9sumGKm1YR88gc
KXqQ8XCOGCTV2n1GU+hwjvJk7FGSn4KQs0wJWnghok+KuumoXHOXVghfKggvcm1y7uDvt/PeEjK
x0A43N487kUFu0H6F89nmkEmXWTUKEwv
-----END CERTIFICATE-----
```

[Download certificate](#)

9. Open a browser window and go to <https://forms.gle/qCbShAPGmhHTzyreA> (an online fillable form).
10. Enter your email address (A), your Brivo account number (B), select Okta (C), select Local Auth enabled or disabled (D), and click Next (E).

Important Note: If Local Auth is disabled, all administrators MUST use the SSO integration to authenticate into their Brivo account. They will no longer be able to log in with their email address and password via the Brivo login screen. Additionally, administrators on this account will not be able to use Brivo Access app as SSO is not yet available with our mobile application.

SSO Configuration Form

* Required

Email address *

Your email A

What is your Account Number? *

Your answer B

Which SSO provider are you using? *

Azure

Okta C

Do you want to disable local authentication? *

Important Note: If local authentication is disabled, all admins MUST use the SSO integration to authenticate into their Brivo account. They will no longer be able to log in with their email address and password via the Brivo login screen. Additionally, admins on this account will not be able to use BOMA, as SSO is not yet available with our mobile application.

Yes, disable local authentication D

No, keep local authentication enabled

Next E

Page 1 of 3

11. Enter the User Provided Connection Name from page 6 in the Connection Name (A) field, the X.509 Certificate information from page 11 in the X.509 Certificate (B) field, and the Identity Provider Single Sign-On URL from page 11 in the Identity Provider Single Sign-On URL (C) field. If you wish to have a copy of these responses sent to your email address, switch the Send me a copy of my responses toggle (D) and then click Submit (E).

12. All other steps concerning Okta SSO Configuration are handled by Brivo directly.

Revision List

Date	Version	Description
June 11, 2020	1.0	Initial Draft
June 22, 2020	1.1	Corrections and additions to instructions on pages 5 and 6
July 10, 2020	1.2	Addition of the SSO Configuration Form
July 31, 2020	1.3	Updated Google Form information on page 12
April 26, 2021	1.4	Updated content
August 25, 2022	1.5	Removed Onair references