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.

I Configuration

Configuration

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

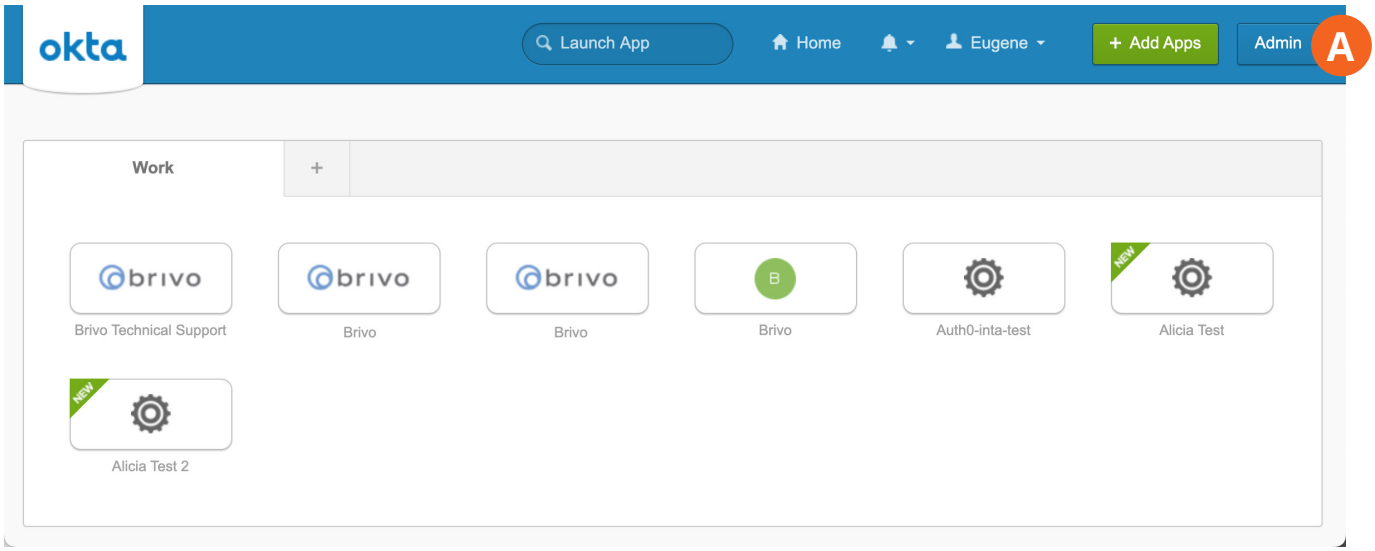
connectionName - See page 6 of this guide

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

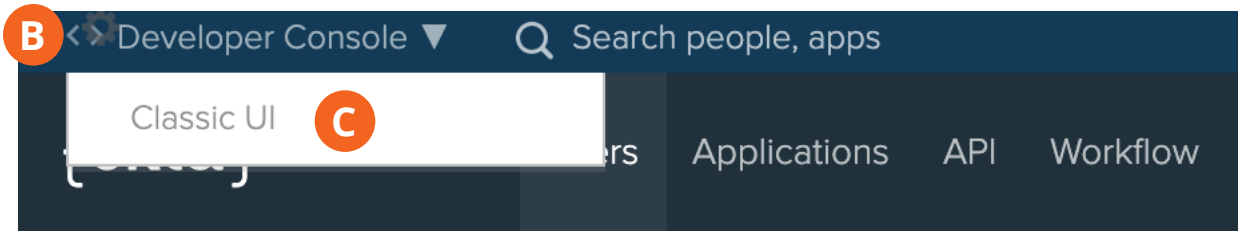
X.509 Certificate - See page 11 of this guide

Configuring Okta for Single Sign On (SSO)

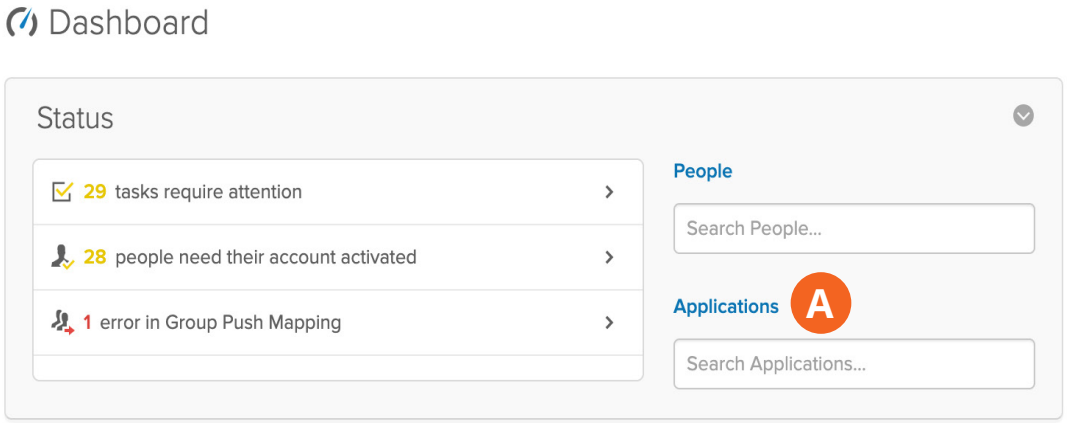
1. Login to the Okta Admin Console using your Okta account sandbox link.
2. Verify that you are using the Admin Console (A). If you are using the Developer Console, you will need to switch over to the Admin Console.



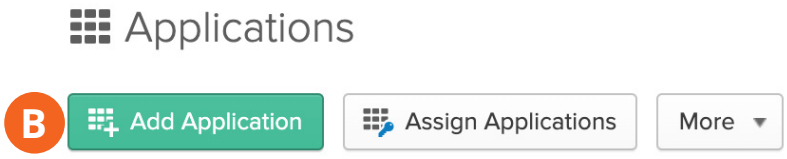
3. If you see <> Developer Console (B) in the top left corner of your console, click on it and select Classic UI (C) from the dropdown menu.



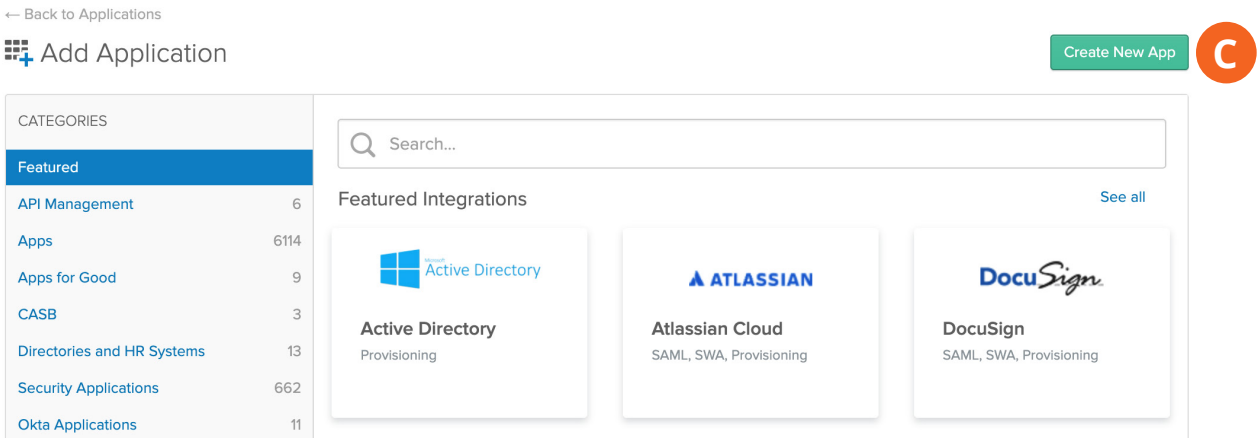
4. In the Admin Console, click on the Applications (A) link.



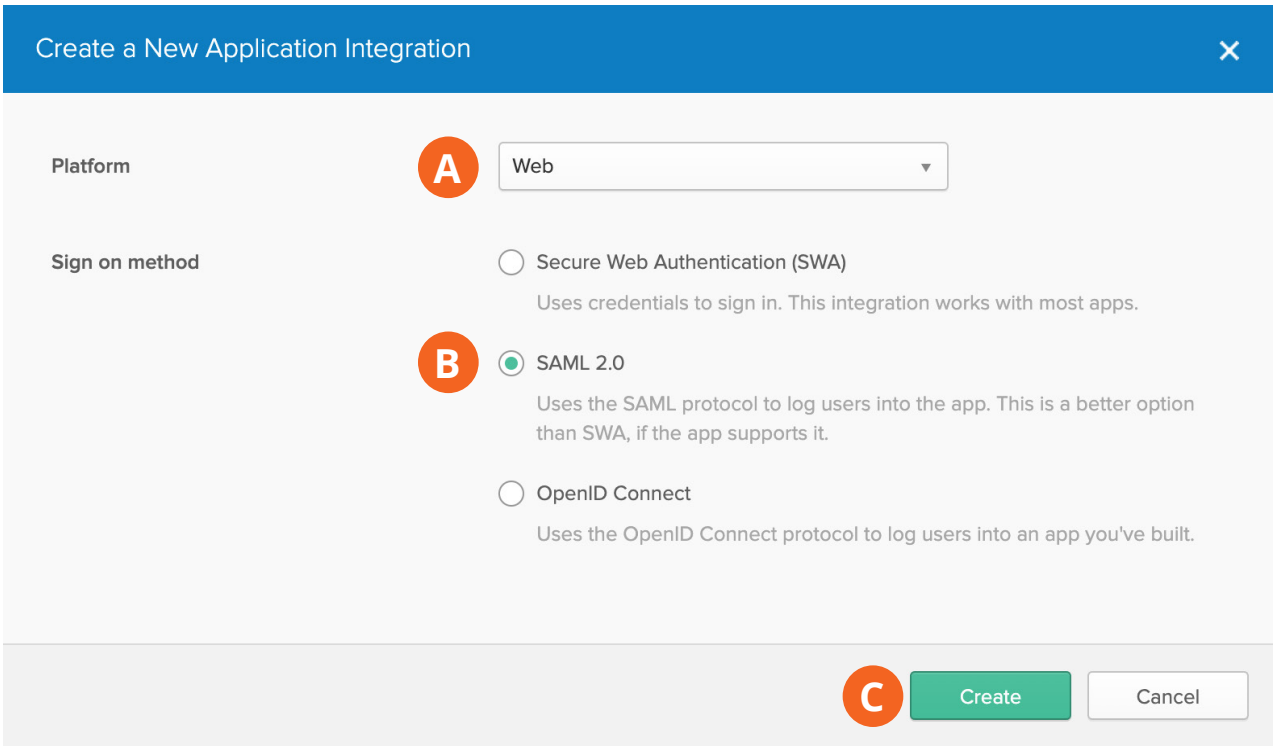
5. The Applications page will display. Click on the Add Application (B) button.



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



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.

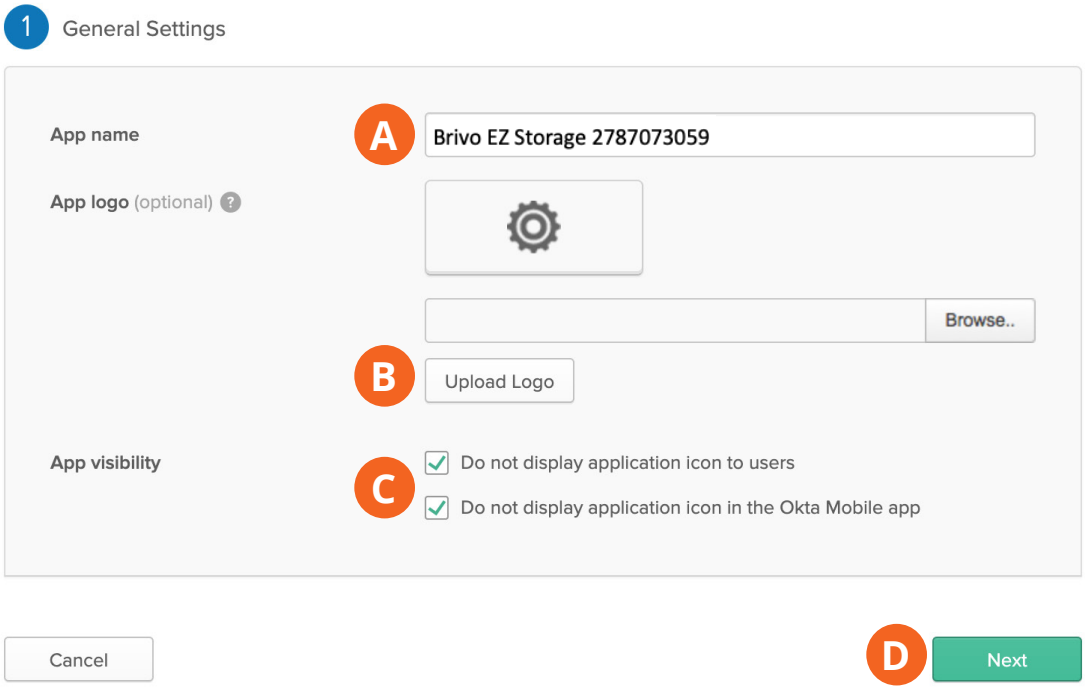


Configuring General Settings

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)



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.

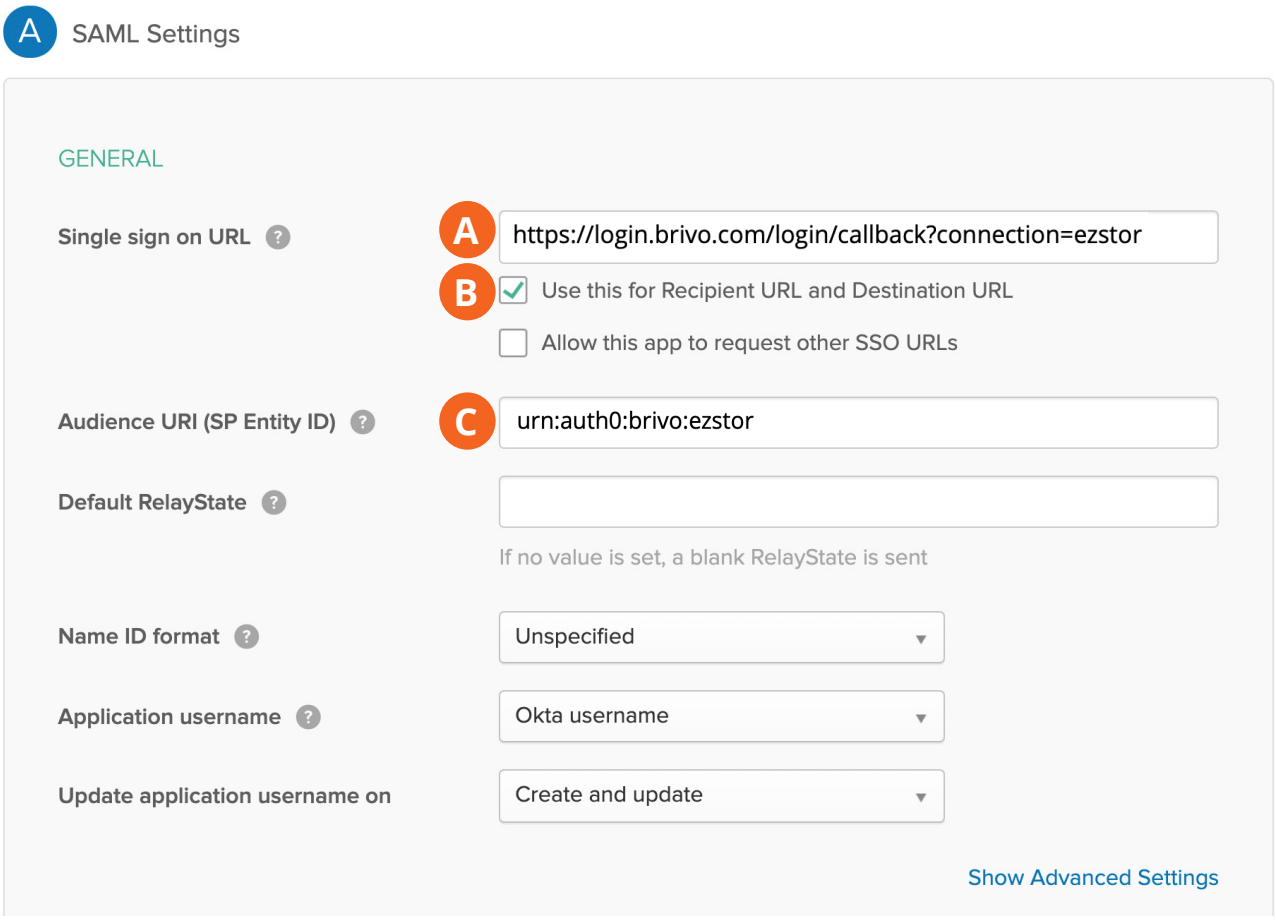
   https://login.brivo.com/login/callback?connection=(user provided connection name)

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.

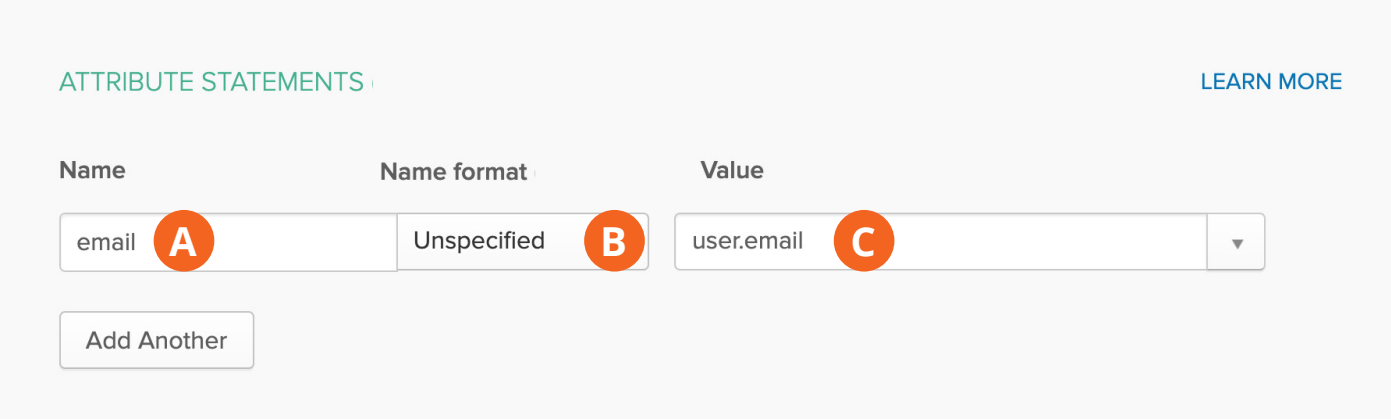
   urn:auth0:brivo:(user provided connection name)

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.



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.

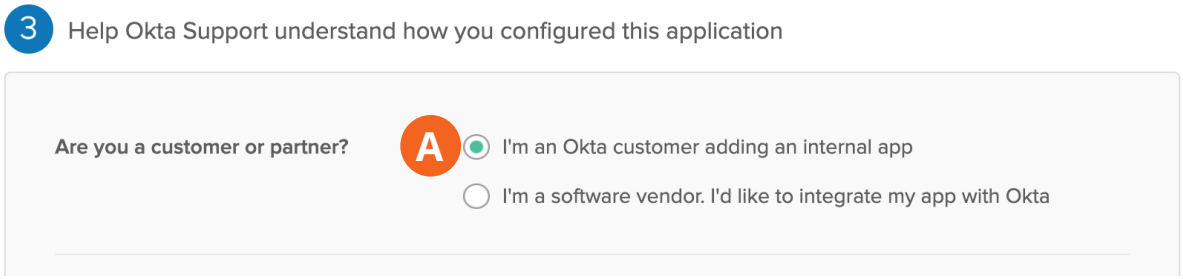
4. In the Attribute Statements section, enter **email** in the name field (A), select **Unspecified** (B) from the Name format dropdown menu, and enter **user.email** in the Value (C) field.



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

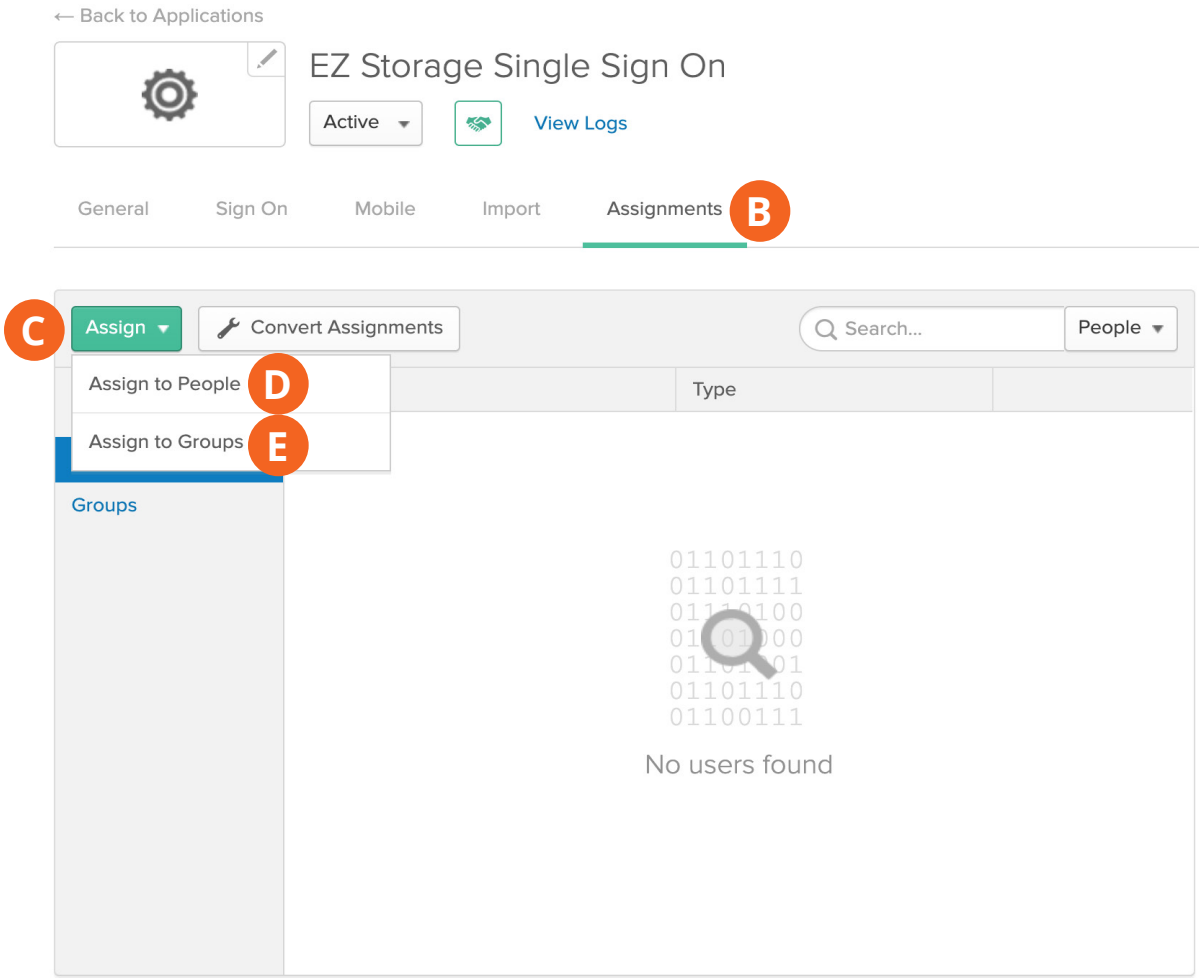
Configuring Feedback

1. 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.

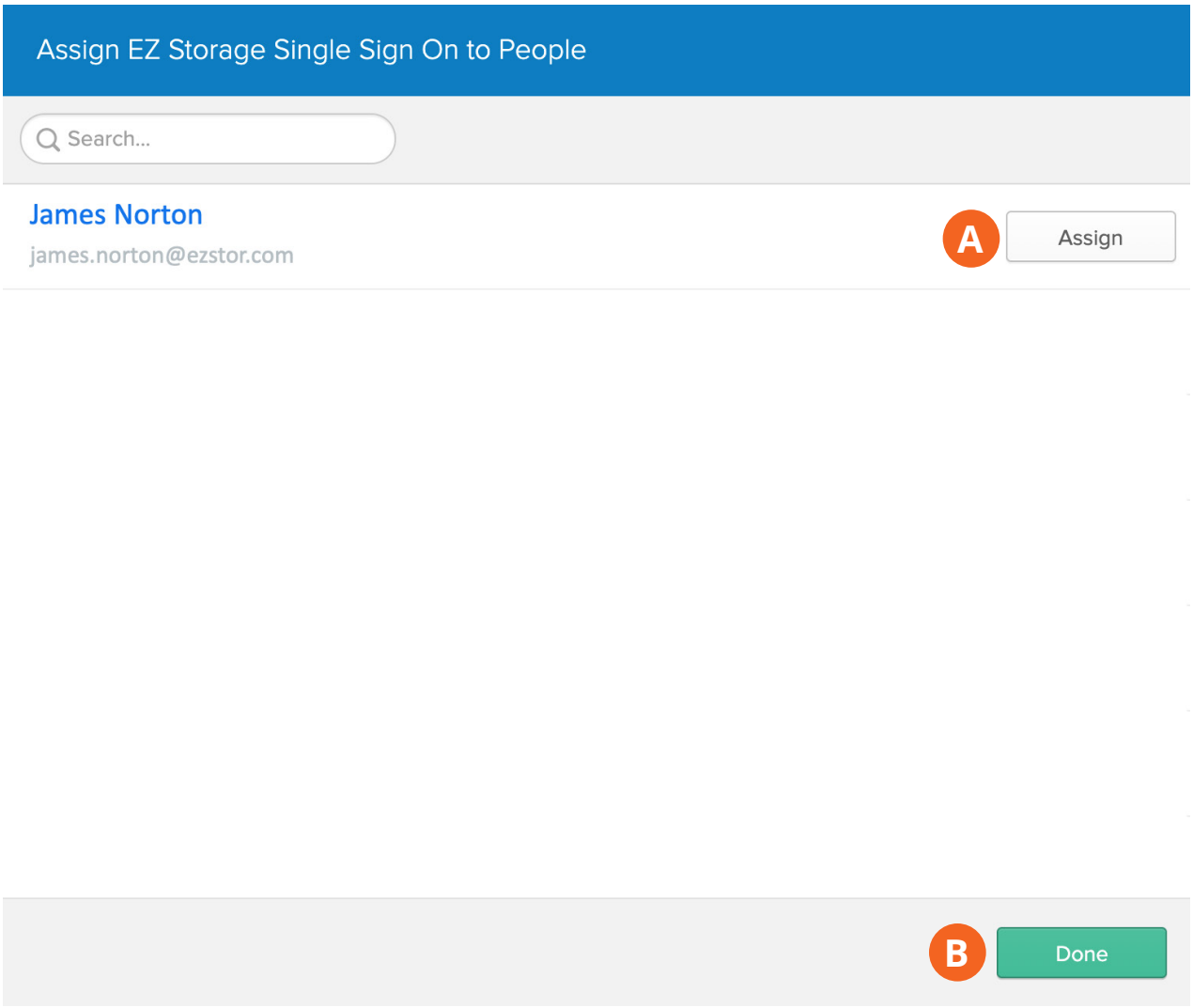


2. Click the green Finish button at the bottom of the page and you are returned to the Application Description Page.

3. 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.

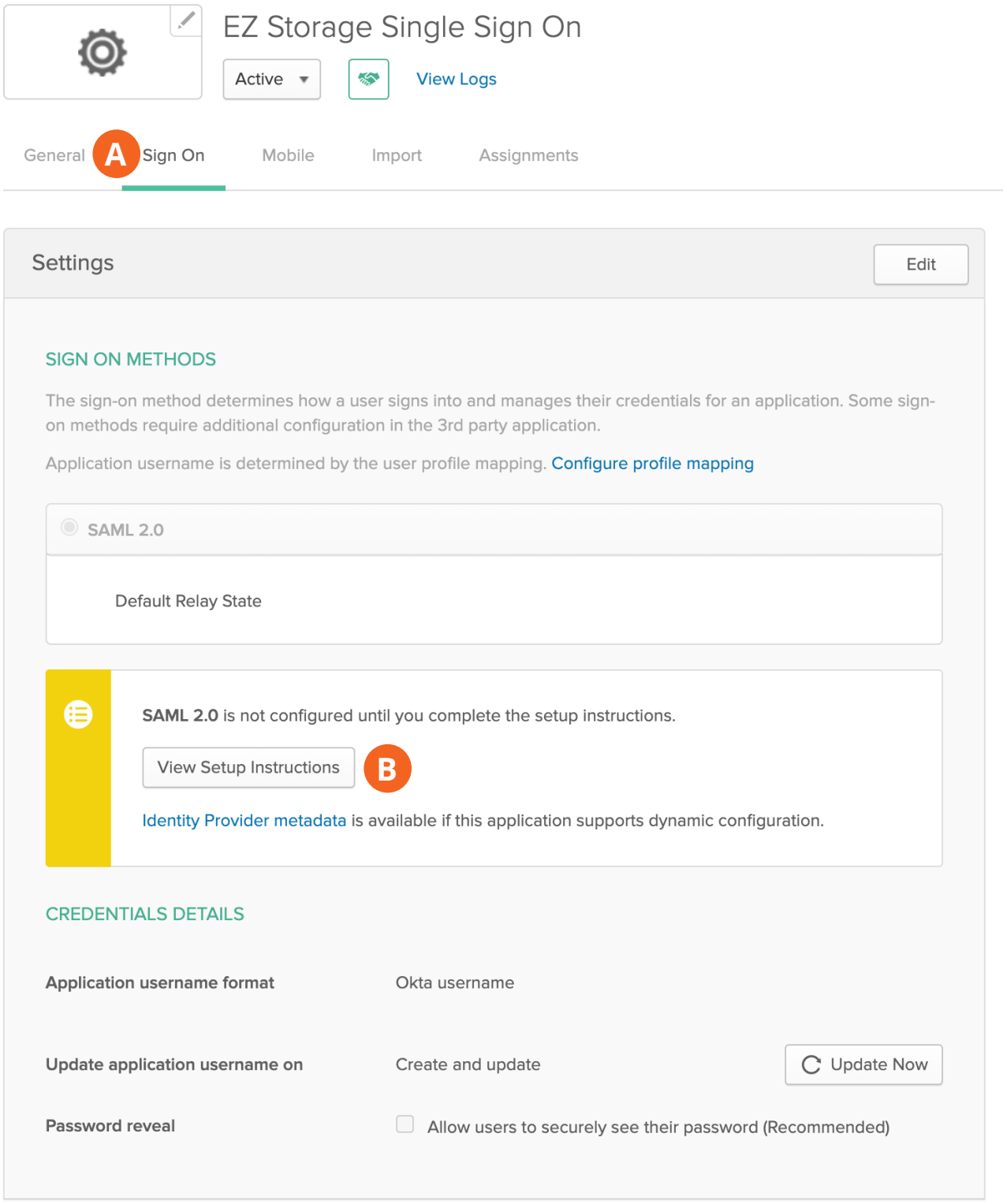


4. For the purposes of this guide, we will assign a person. When the Assignment pop-up window appears, click on the Assign (A) button next to the people you wish and click Done (B) when finished.



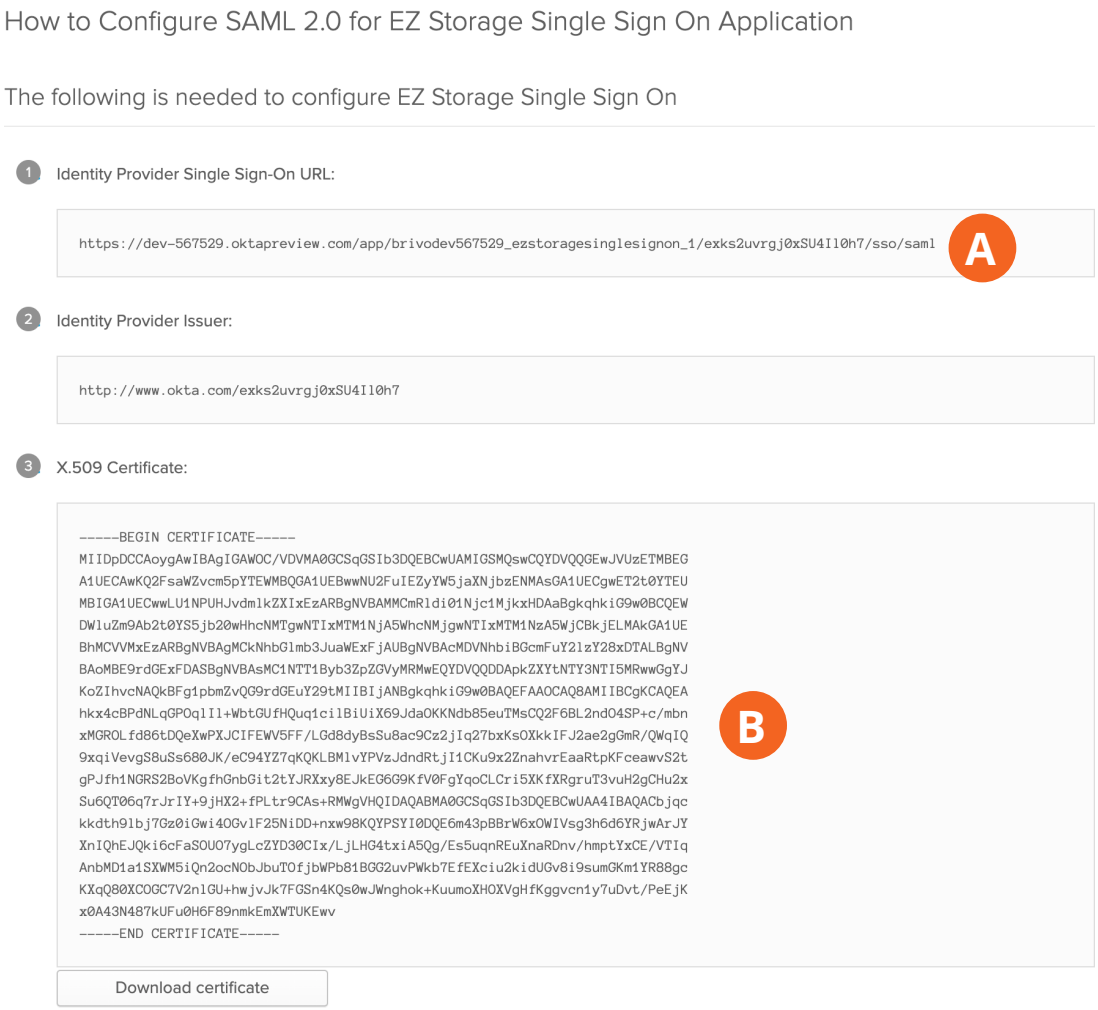
5. You are returned to the Application Description Page.

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



7. The How to Configure SAML 2.0 for Your Application page displays.

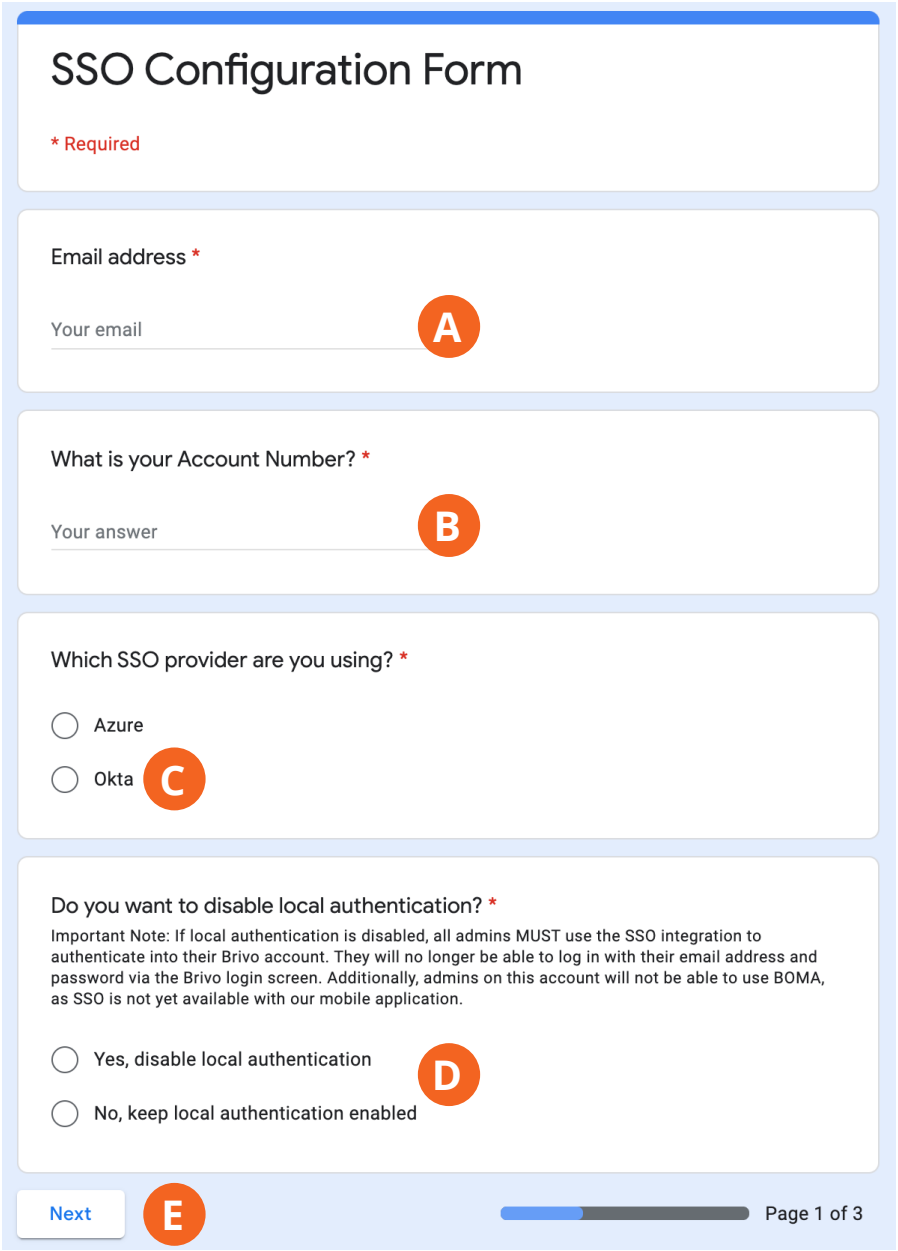
8. The Identity Provider Single Sign-On URL (A) and the X.509 Certificate (B) should be copied and provided to Brivo in the following steps.



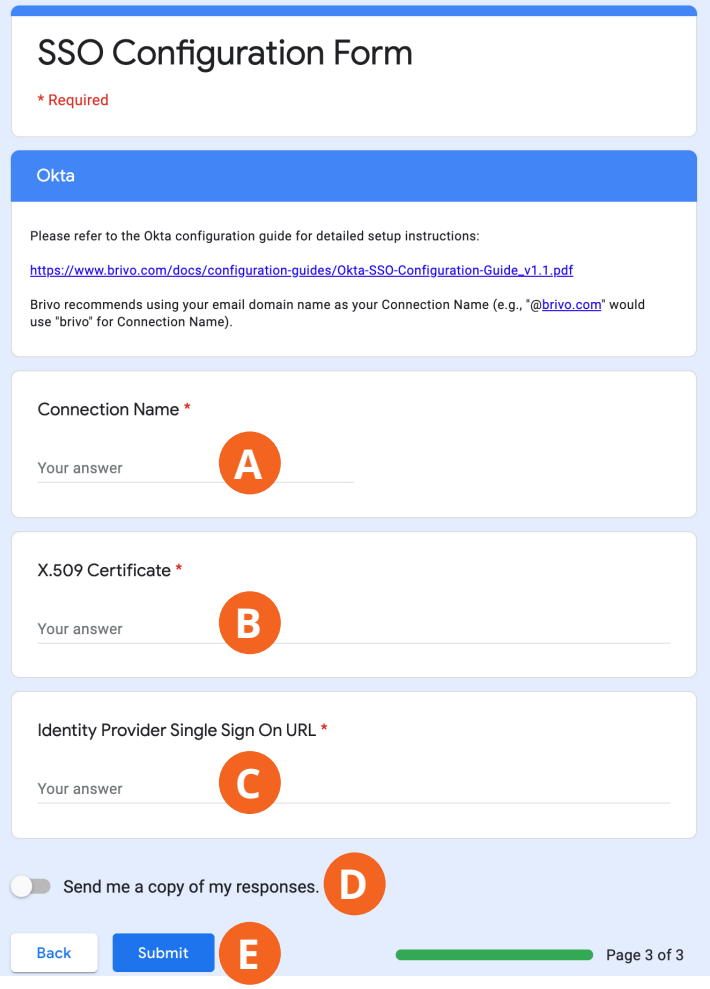
9. Open a browser window and go to https://forms.gle/qCbShAPGmhHTzyreA (an online fillable form).

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.



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