Enabling single sign-on authentication (SSO) for Okta

Background Info

This feature is available in Lucy 4.6 or newer version.

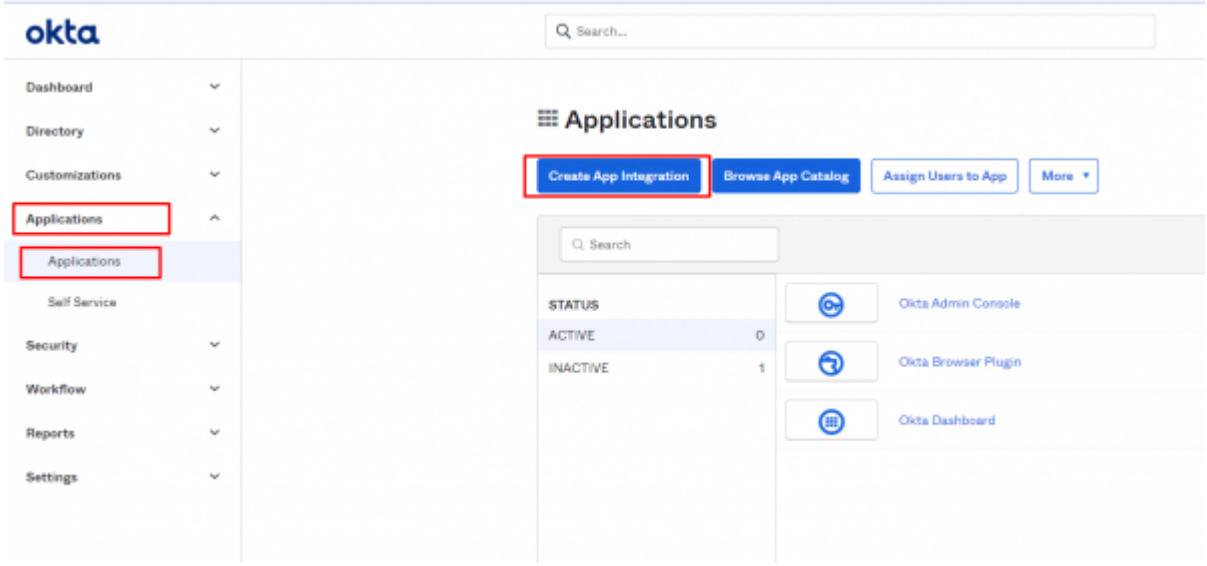
This article describes the basic settings for integrating Okta into Lucy. More information can be found on the Okta website at https://www.okta.com/products/single-sign-on

Additional information about what SSO in Lucy is designed for can be found here.

What preparations need to be done before connecting to Okta?

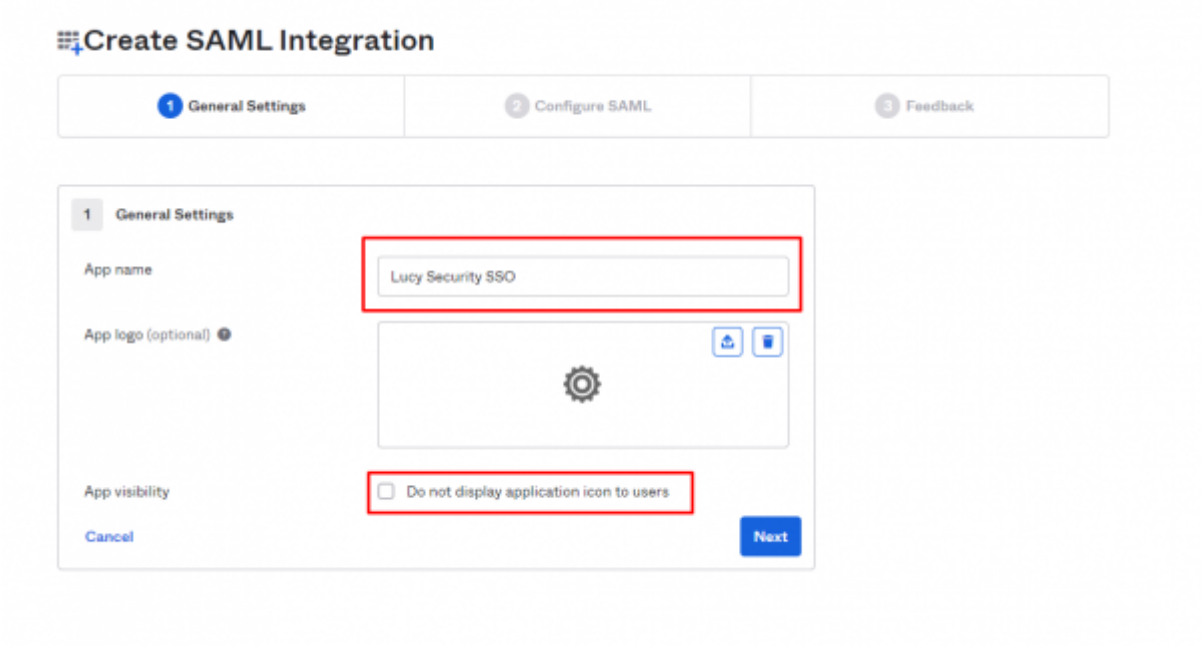
1. Register an account with Okta and login to Admin portal

2. Go to the **Applications** > click "Create App Integration"

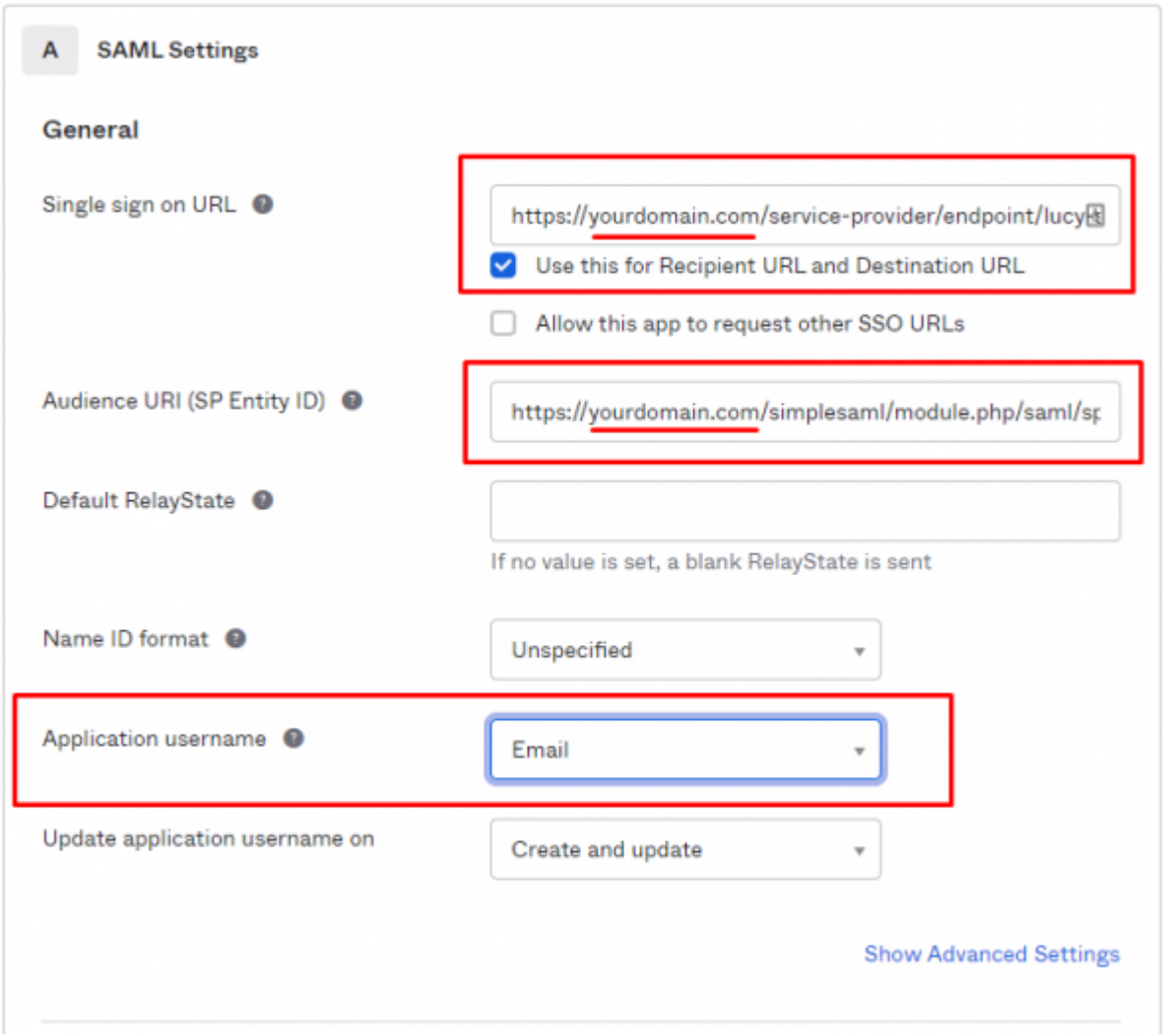


3. Add a new application with the following settings:

- Sign on method: **SAML 2.0**
- App name: **Lucy Security SSO**
- App visibility: leave unchecked

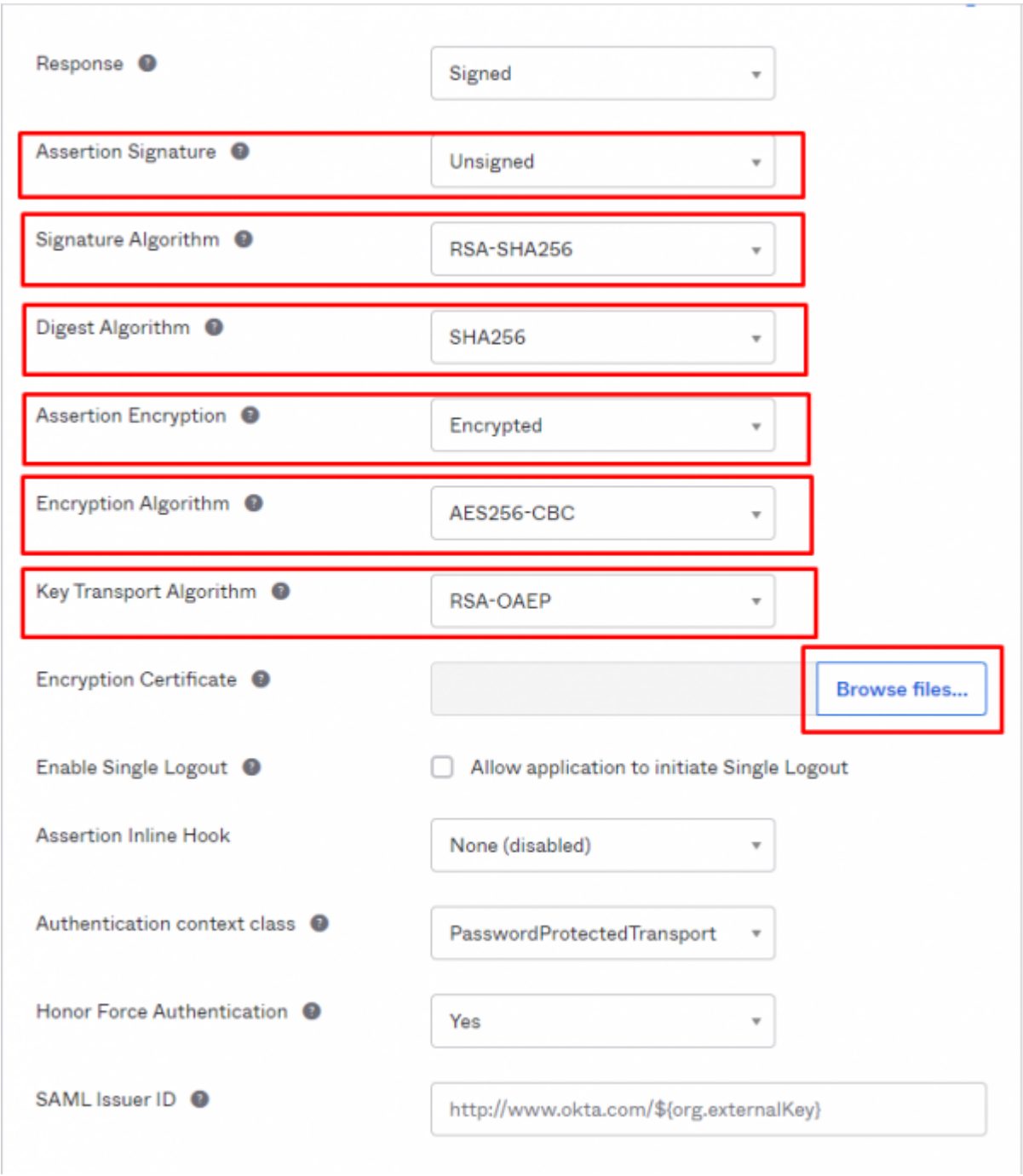


- Single sign on URL: https://yourdomain.com/service-provider/endpoint/lucy-sp
- Audience URI (SP Entity ID): https://yourdomain.com/simplesaml/module.php/saml/sp/metadata.php/lucy-sp
  where 'yourdomain.com' is your Lucy's admin domain name
- Application username: **Email**



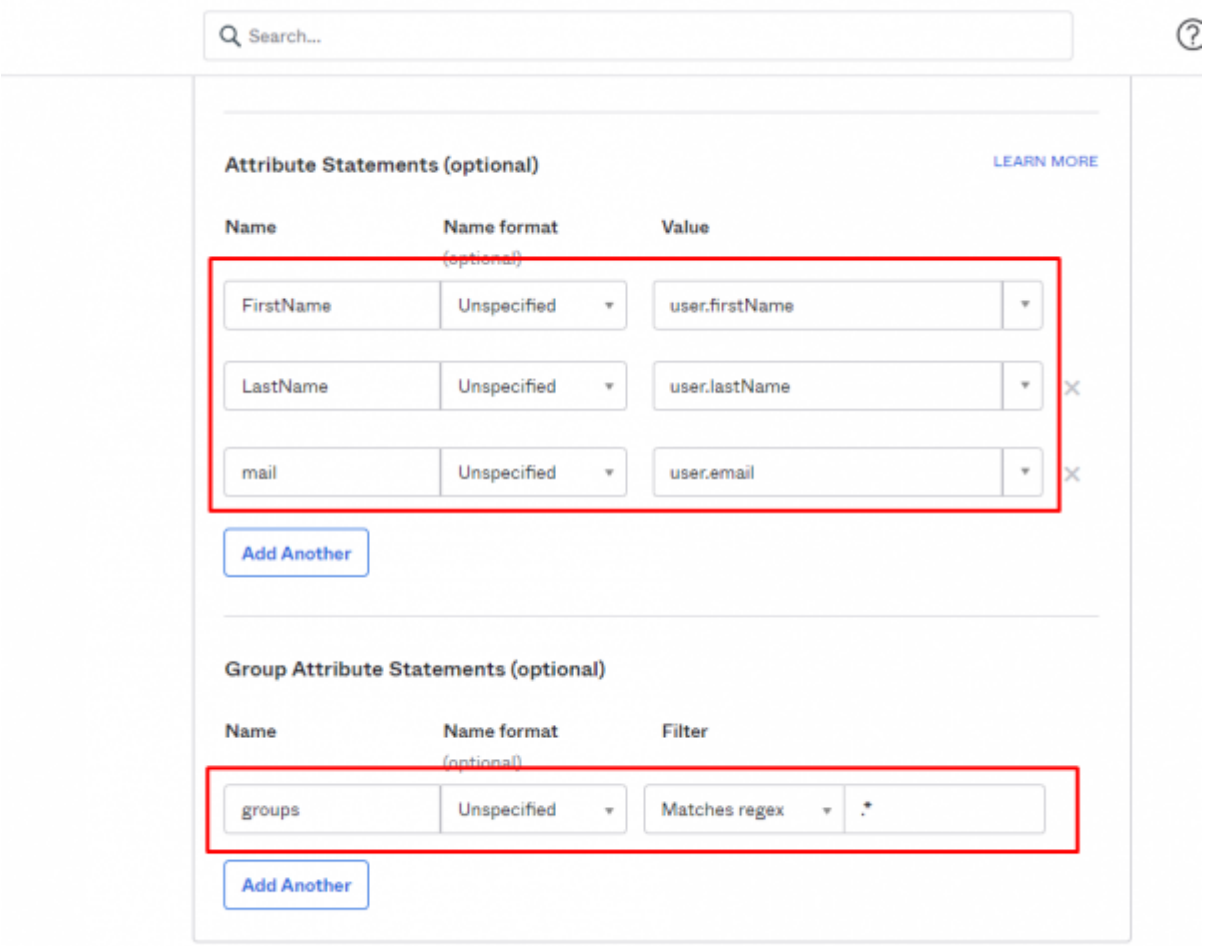
4. Click "Show Advanced Settings" and add the following settings:

- Assertion Signature: **Unsigned**
- Signature Algorithm: **RSA_SHA256**
- Digest Algorithm: **SHA256**
- Assertion Encryption: **Encrypted**
- Encryption Algorithm: **AES256_CBC**
- Key Transport Algorithm: **RSA_OAEP**
- Encryption Certificate: use the certificate from Lucy's *Settings* page > *SSO Configuration* > *Download Certificate*

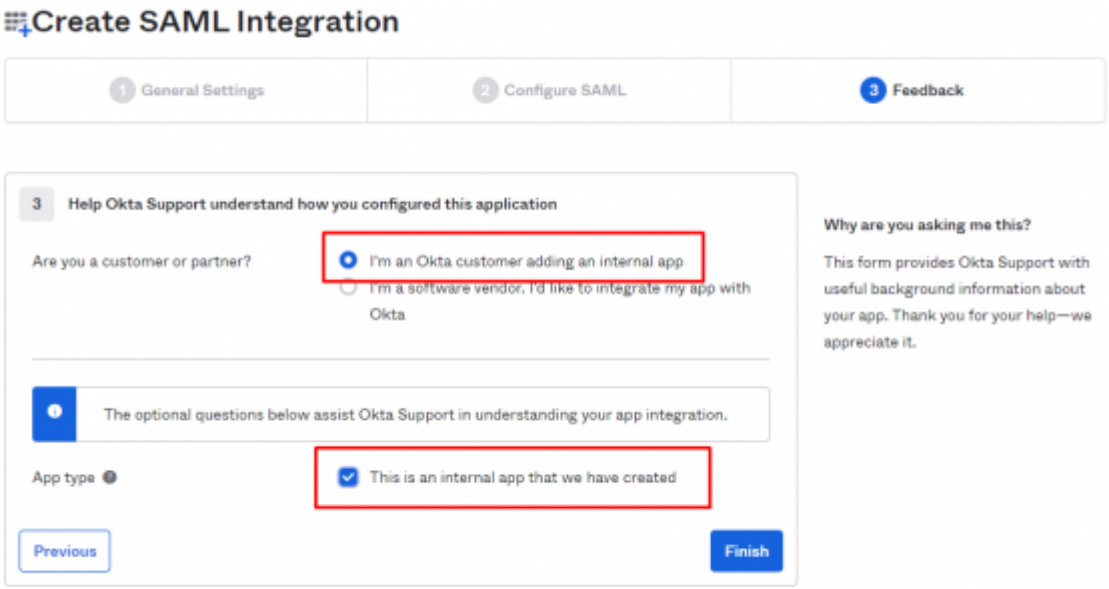


- Attribute Statements:
  - Name: **FirstName** Value: **user.firstName**
  - Name: **LastName** Value: **user.lastName**
  - Name: **mail** Value: **user.email**

- Group Attribute Statements:
  - Name: **groups** Filter: **Matches regex: .***

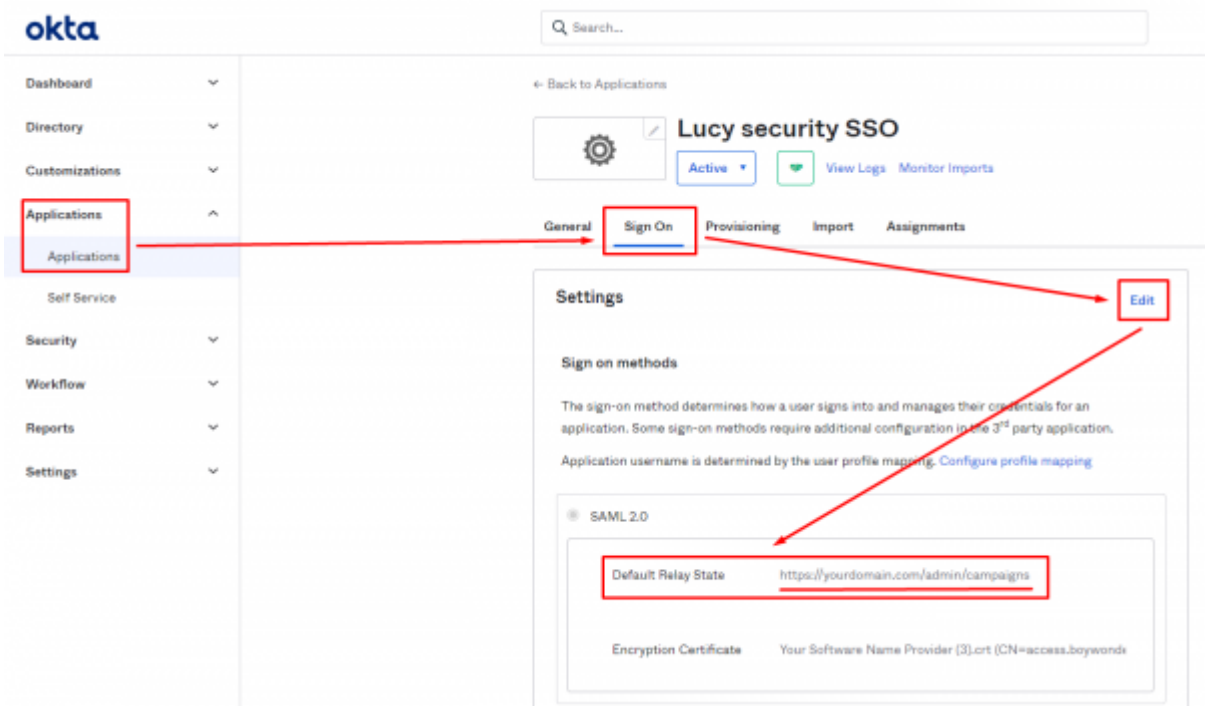


- Feedback page:
  - Are you a customer or partner? **I'm an Okta customer adding an internal app**
  - App type: **This is an internal app that we have created**

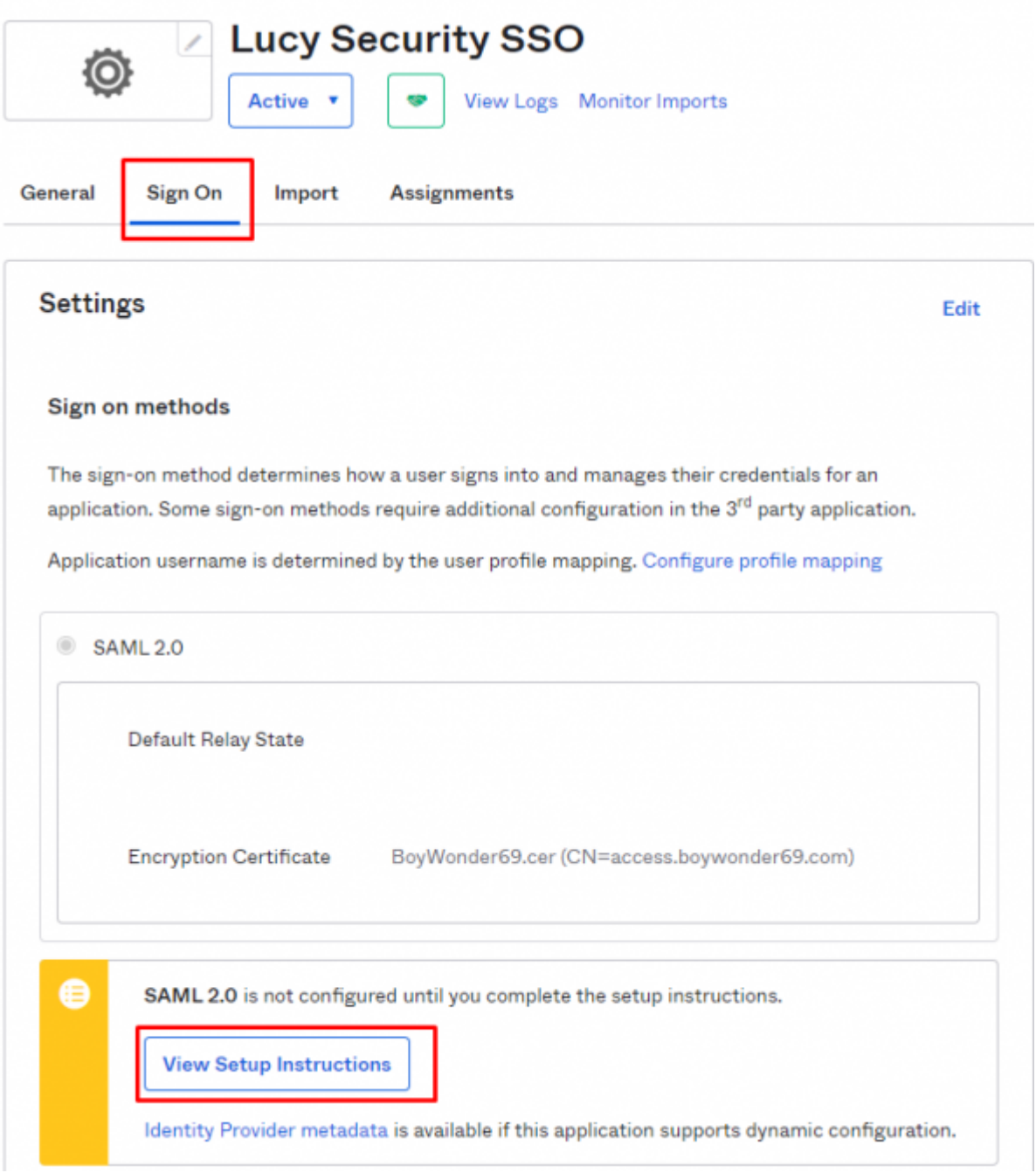


5. Once the initial configuration is finished, go to the **Sign On** tab, click the **Edit** button in “**Settings**” and in the **Default Relay State** add “https://yourdomain.com/admin/campaigns“(without the quotes).

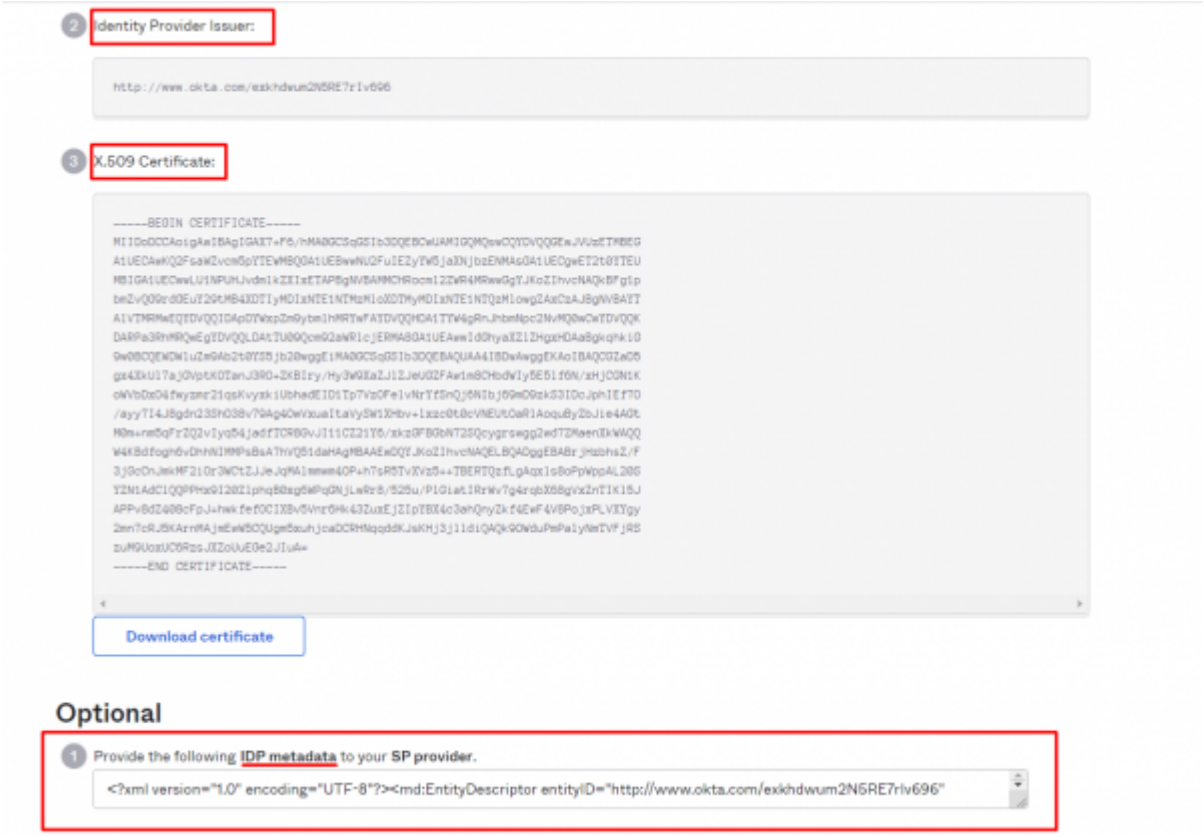
where 'yourdomain.com' is your Lucy's admin domain name
Then click **Save**.



6. On the **Sign On** tab click the "**View Setup Instructions**" button.



To enable Single sign-on in Lucy you will need **Identity Provider Issuer**, **X.509 Certificate** and **IDP**



metadata.

Enable Single sign-on in Lucy

1. Open Lucy Admin console

2. Navigate to the **SSO Configuration** page (Settings > SSO Configuration)

3. Click the option "**Enabled**"

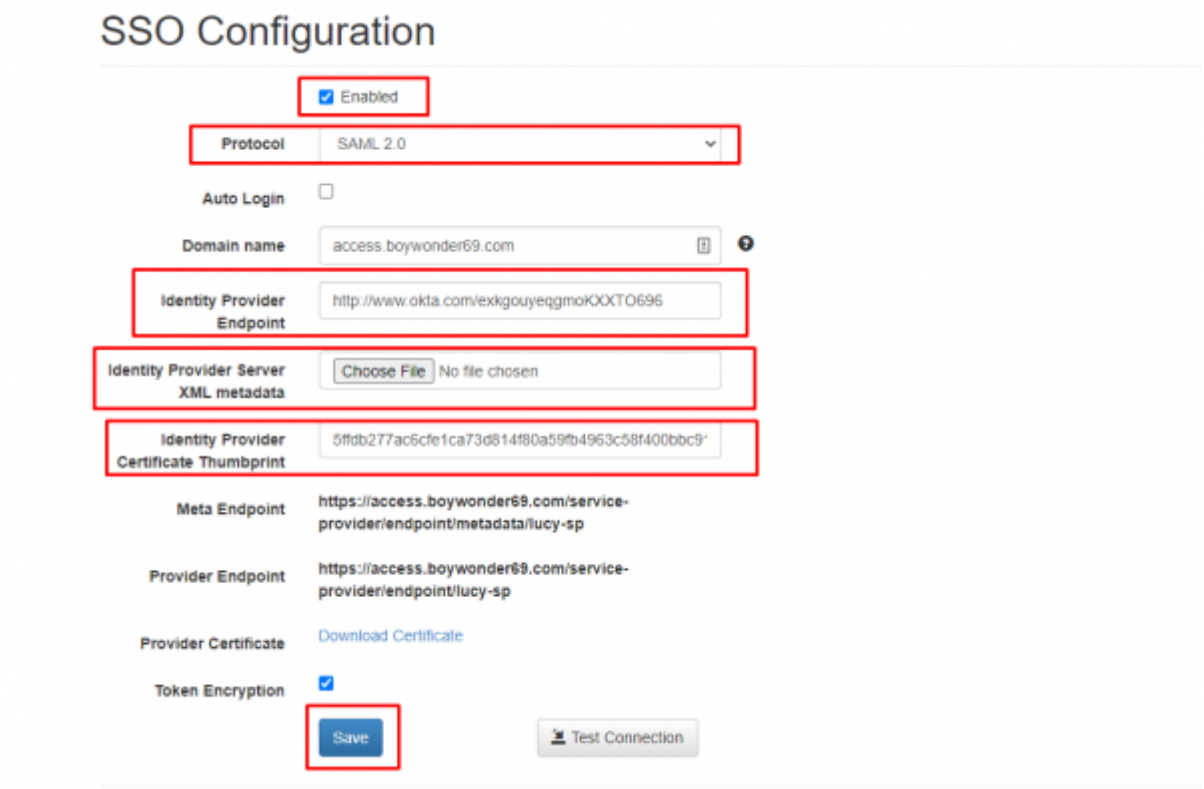
4. Chose **Protocol**: "SAML 2.0"

5. Fill in "**Identity Provider Endpoint**" with the **Identity Provider Issuer** provided by Okta (e.g. http://www.okta.com/<unique_id>)

6. Download **X.509 Certificate** file provided by Okta, copy Thumbprint data from the certificate and paste it into **Identity Provider Certificate Thumbprint** field

7. Save the IDP metadata provided by Okta to an XML file and upload it into Lucy's **Identity Provider Server XML metadata** field

8. **Save** the settings

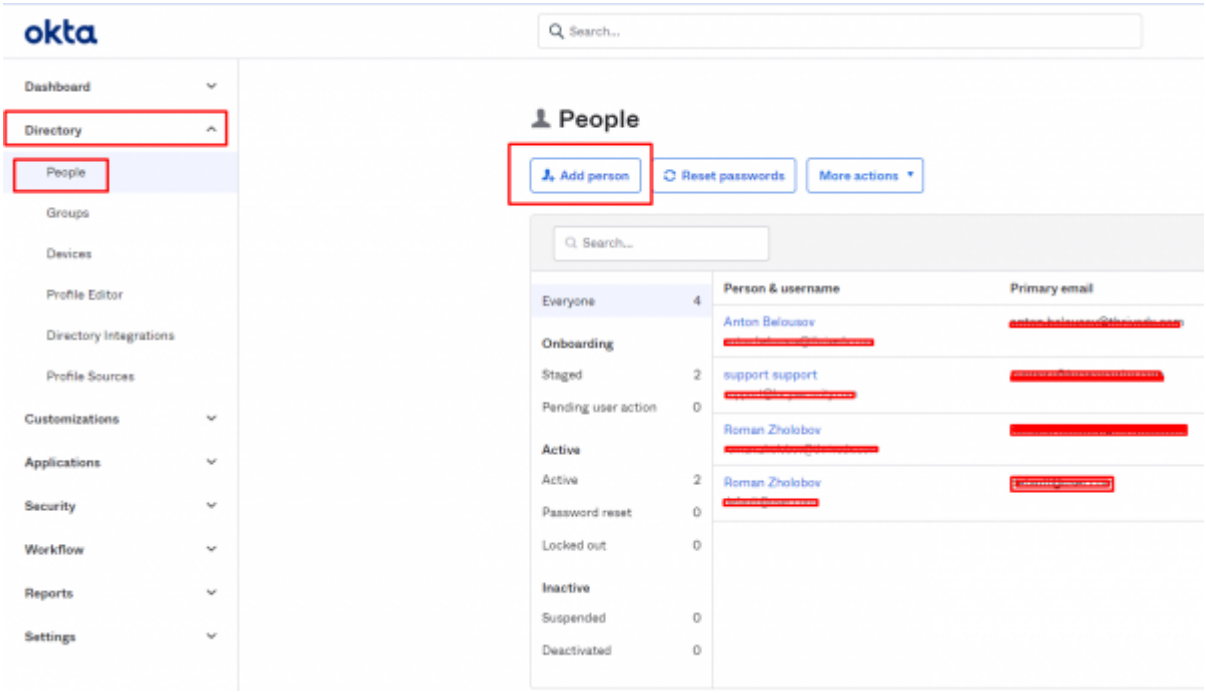


Testing Authentication

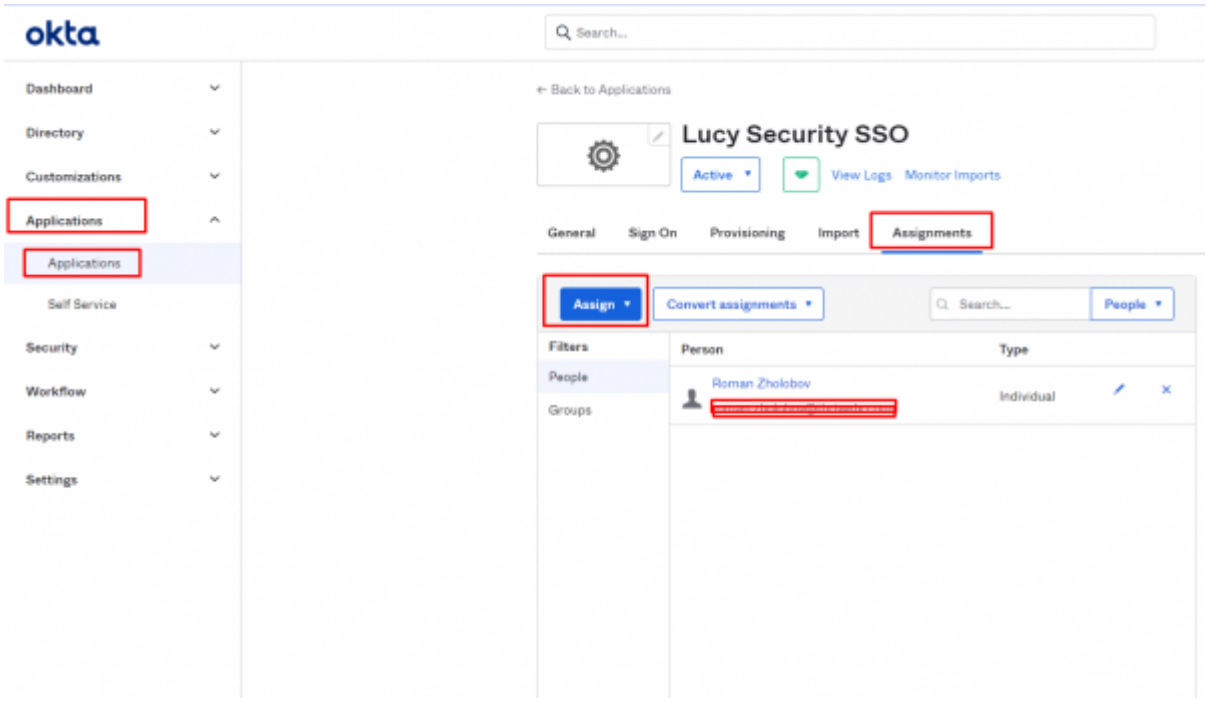
1. Go to Okta Admin portal

2. Navigate to the Directory > People page

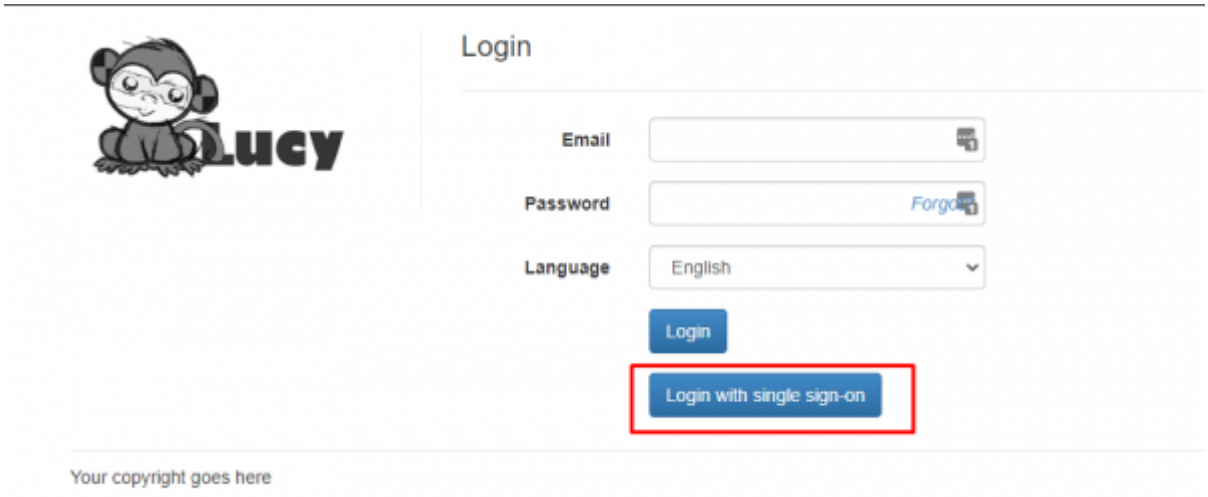
3. Add at least one person corresponding to the Administrator account in Lucy (must be the same e-mail address)



4. Assign the recently added application to the user



5. Use "Login with single sign-on" button on the Lucy's Login page to login using Okta



From:
https://wiki.lucysecurity.com/ - **LUCY**

Permanent link:
https://wiki.lucysecurity.com/doku.php?id=sso_okta

Last update: **2022/03/04 21:06**