GREENORBIT GUIDE

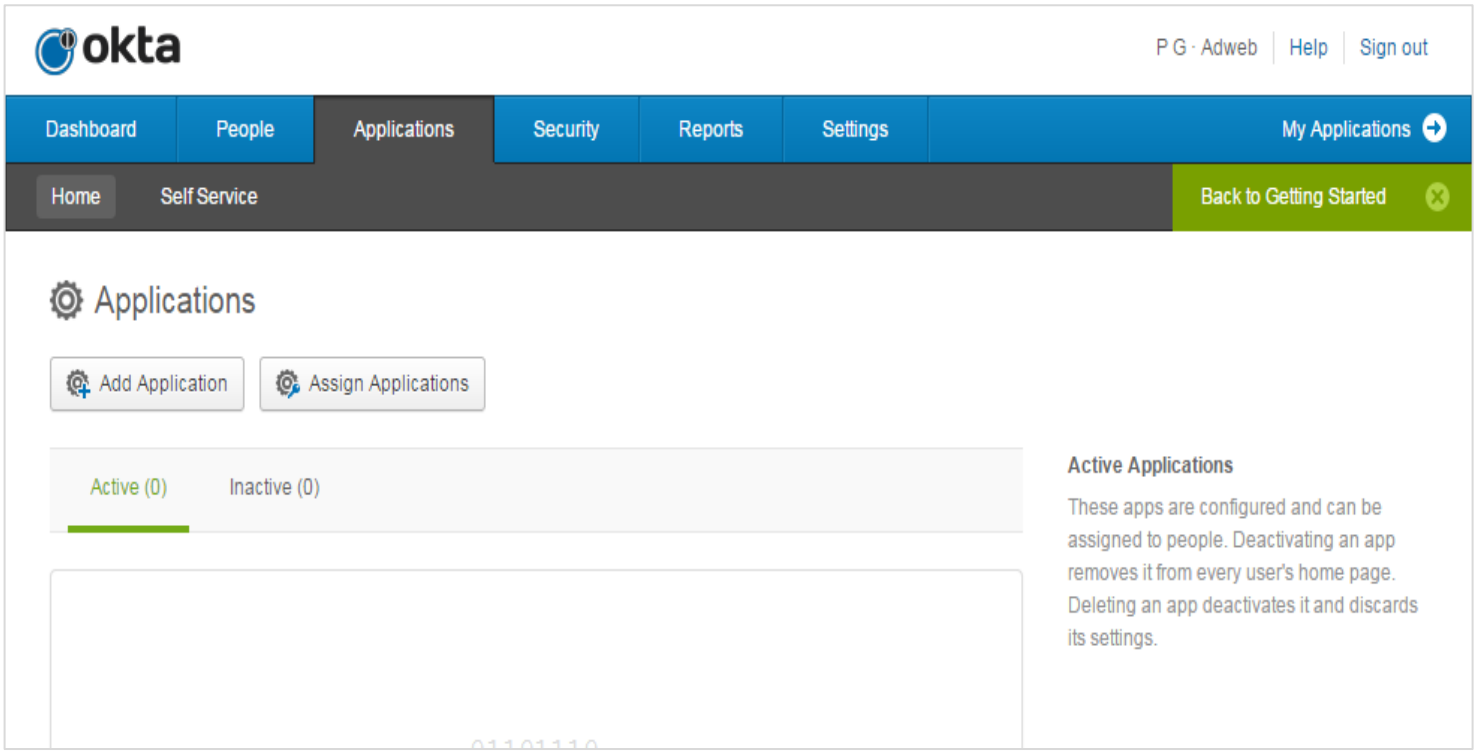
Integrate GreenOrbit with OKTA and OneLogin

INTEGRATE GO WITH OKTA

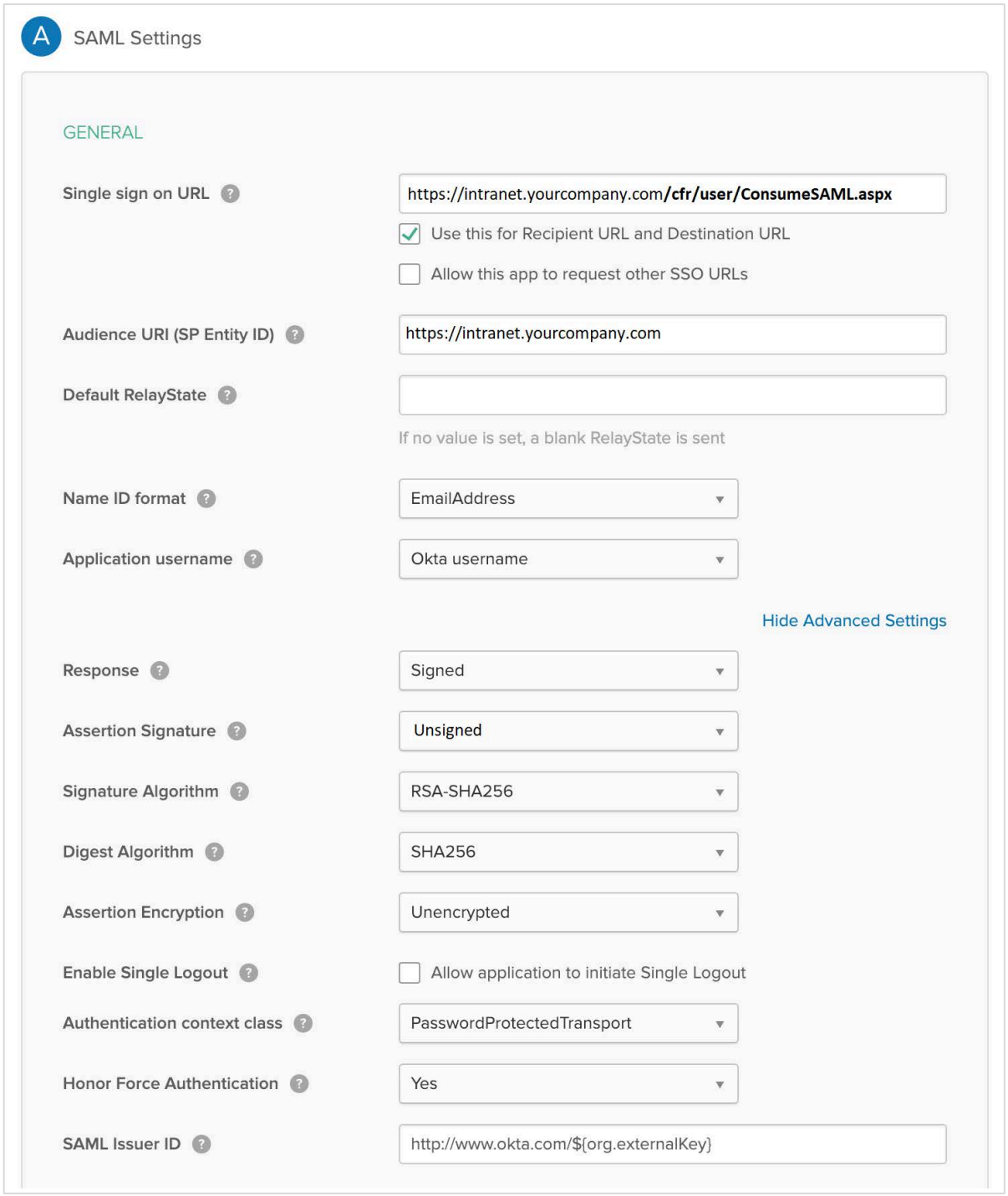
Note: Please always refer to instructions provided by your Identity Provider in the first instance.

Steps to create a SAML application in Okta and how to configure this Intranet DASHBOARD.

1. Create a new account in Okta
2. From the **Applications** tab, **Add Application**
3. **Add Application** titled 'Template SAML 2.0 App'
4. Fill in necessary detail as shown in the extended screen shots below:

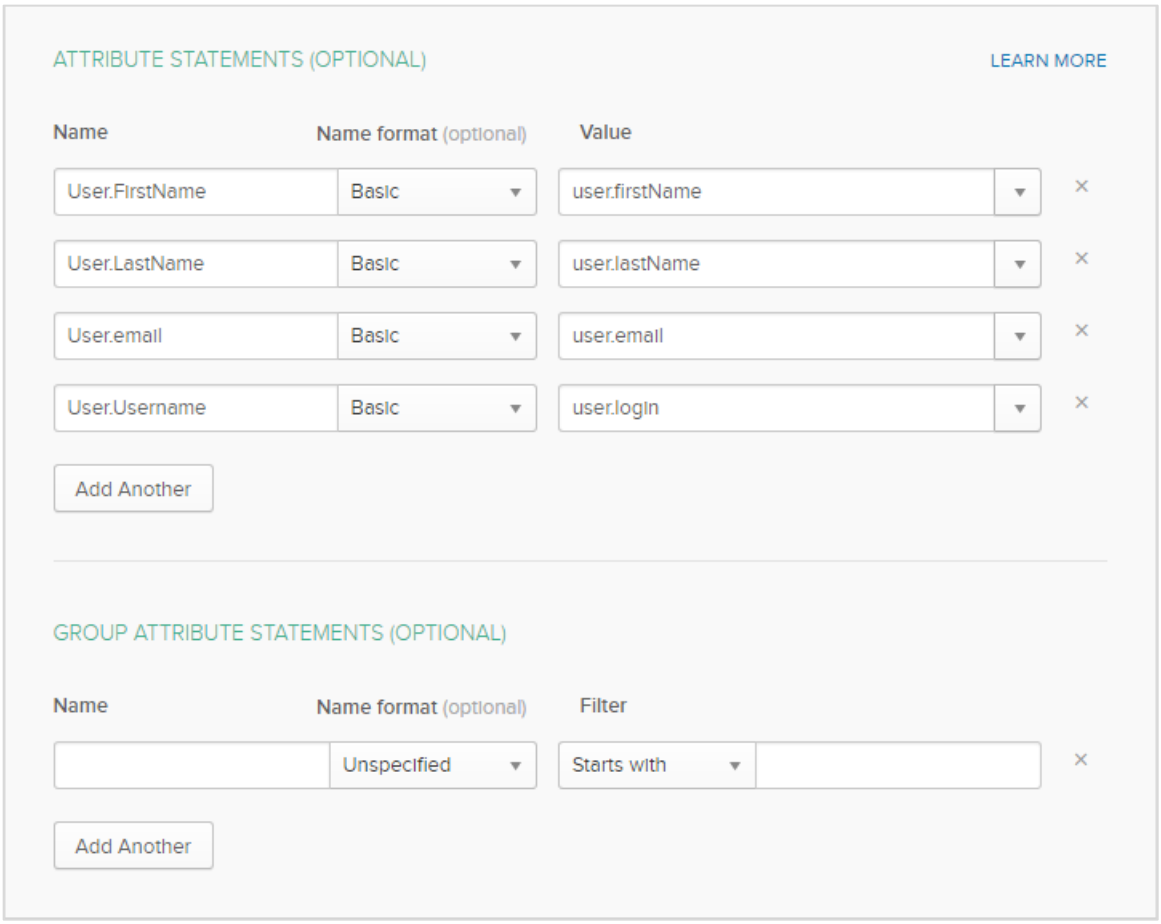


Note: The following details must be entered into your Okta Application:


A
SAML Settings
GENERAL
Single sign on URL
https://intranet.yourcompany.com/cfr/user/ConsumeSAML.aspx
Use this for Recipient URL and Destination URL
Allow this app to request other SSO URLs
Audience URI (SP Entity ID)
https://intranet.yourcompany.com
Default RelayState
If no value is set, a blank RelayState is sent
Name ID format
EmailAddress
Application username
Okta username
Hide Advanced Settings
Response
Signed
Assertion Signature
Unsigned
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}

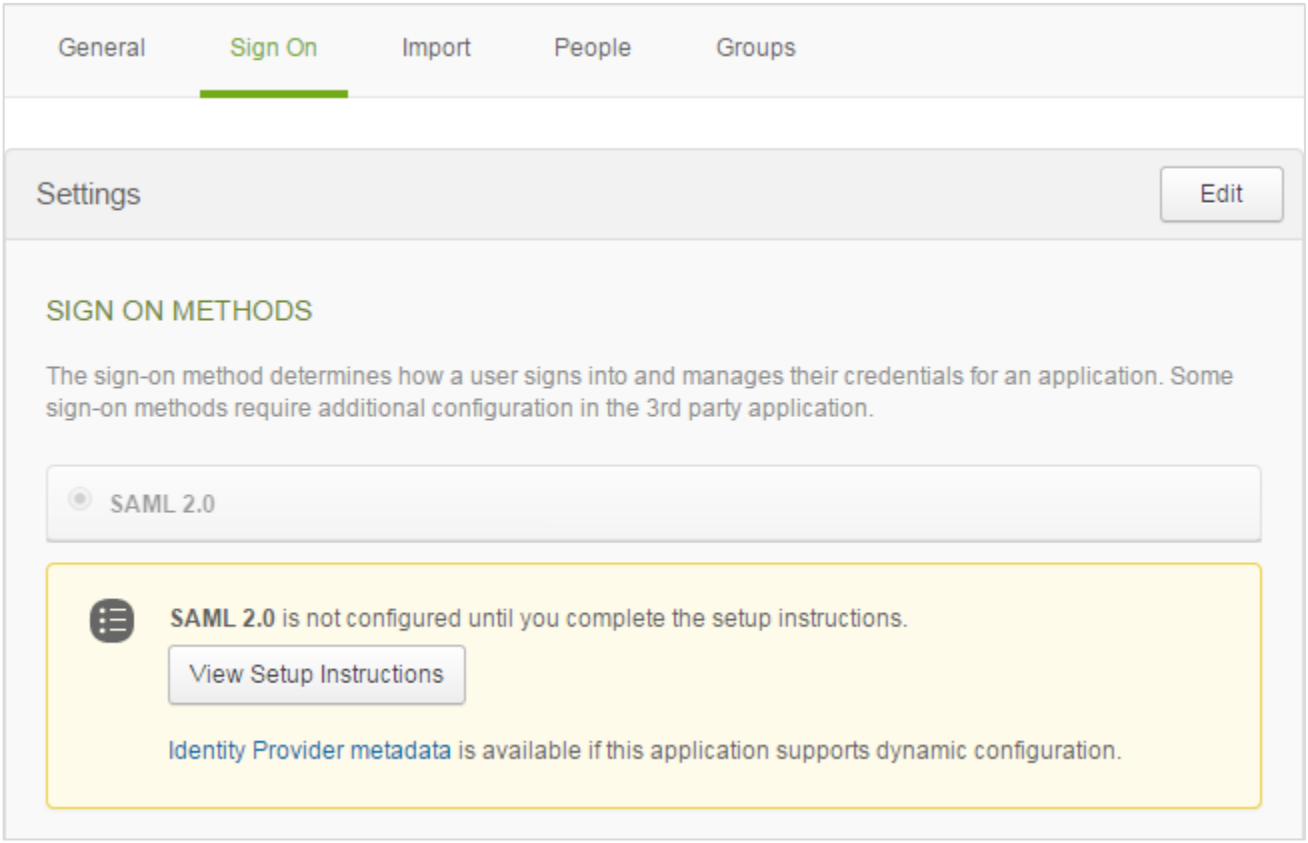
Note: The Attribute Statements should be in the following format:

User.Email|${user.email},User.FirstName|${user.firstName},User.LastName|${user.lastName},User.Username|${user.userName}

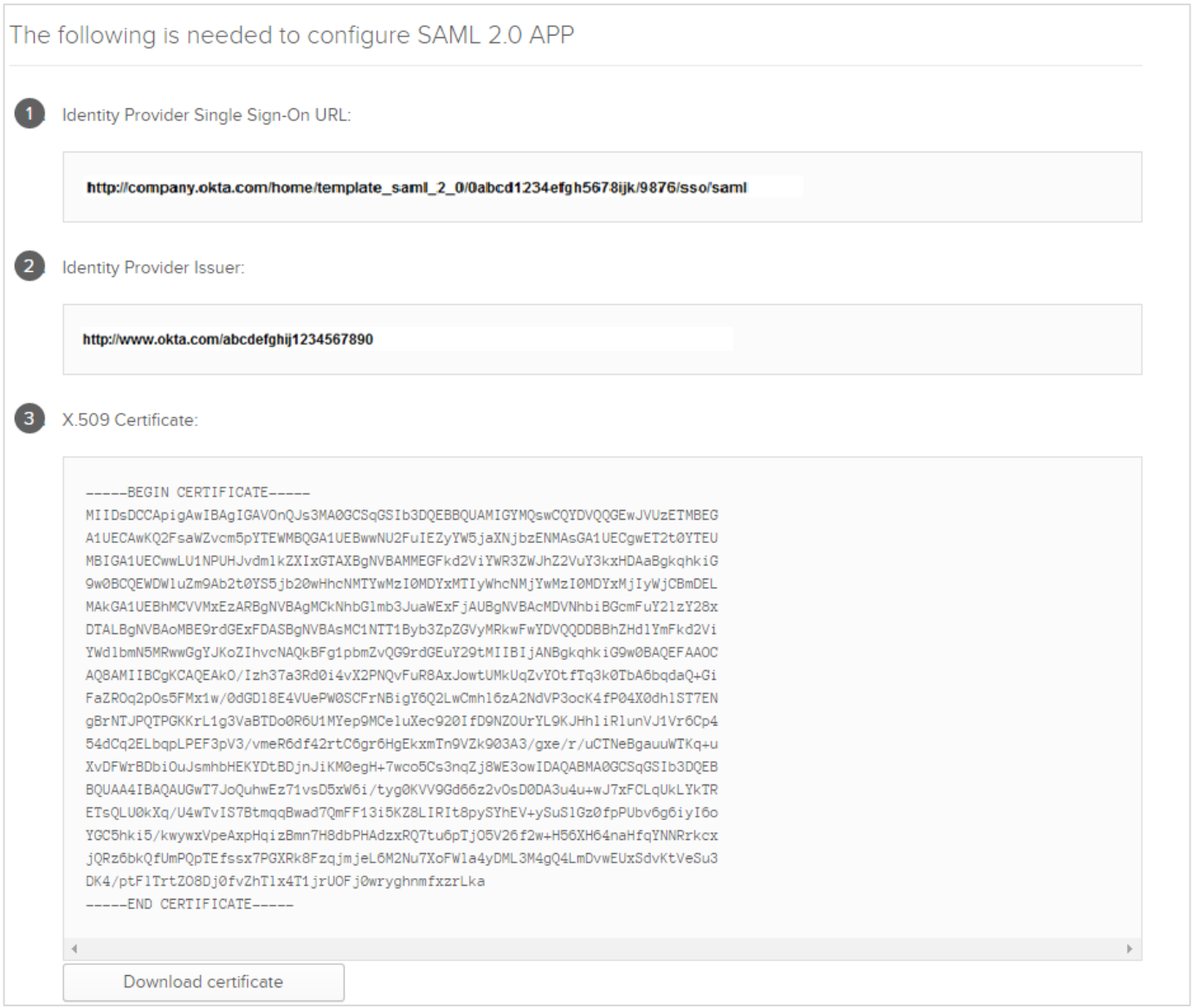


5. In the next step, Assign to People > the Admin can assign multiple users to the SAML application.

6. Once you save the application; under **SignOn** tab there is a **View Setup Instructions** button which redirects the user to Help page.



7. In this Help page, if you scroll right to the end of the page, there is Configuration data available.



The user has to Download certificate, save it and open it in Notepad. Copy the certificate between the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- and paste in Green Orbit as mentioned above.

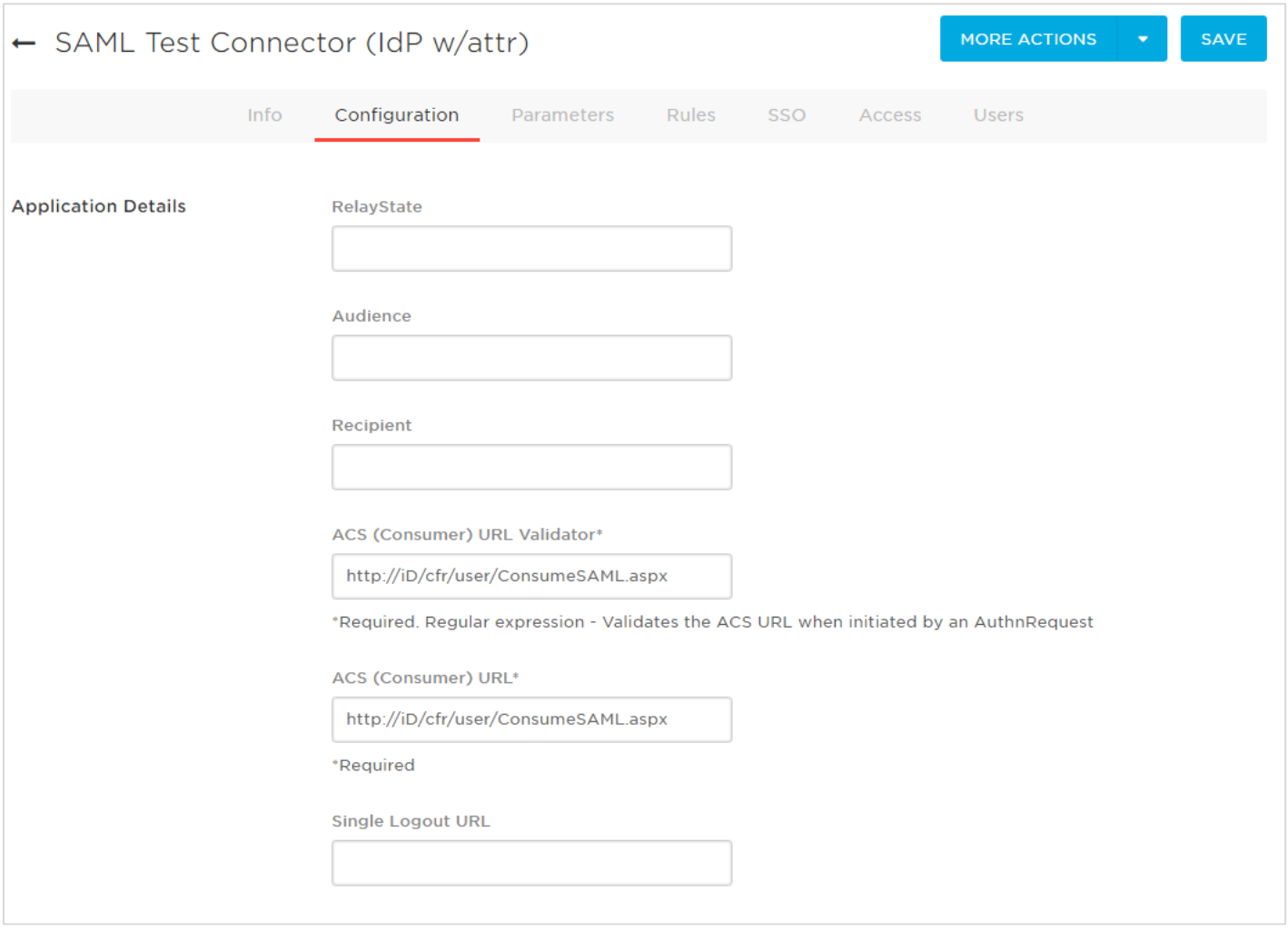
GreenOrbit

Create SAML Account in OneLogin

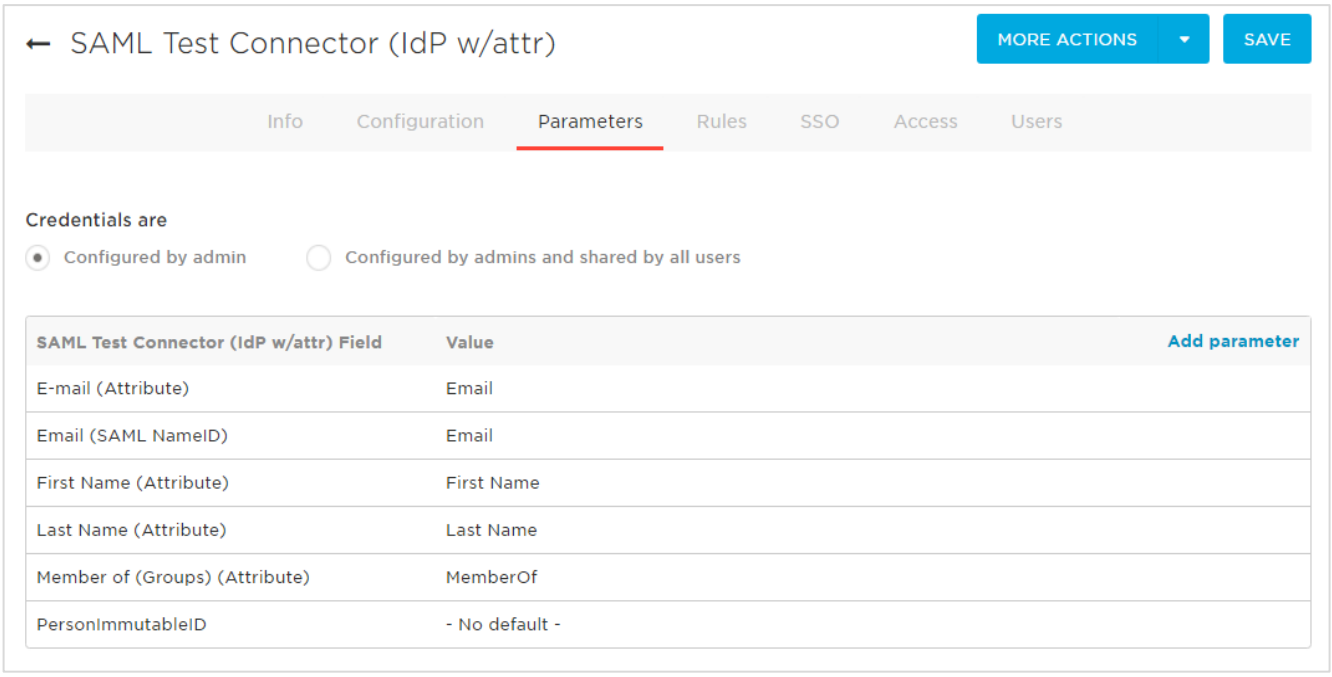
Note: Please always refer to instructions provided by your Identity Provider in the first instance.
Steps to create a SAML application in OneLogin and how to configure this with Green Orbit.

1. Create a new account in OneLogin
2. Add an application under Apps > Add Apps > OneLogin SAML Test (IdP w/attr)

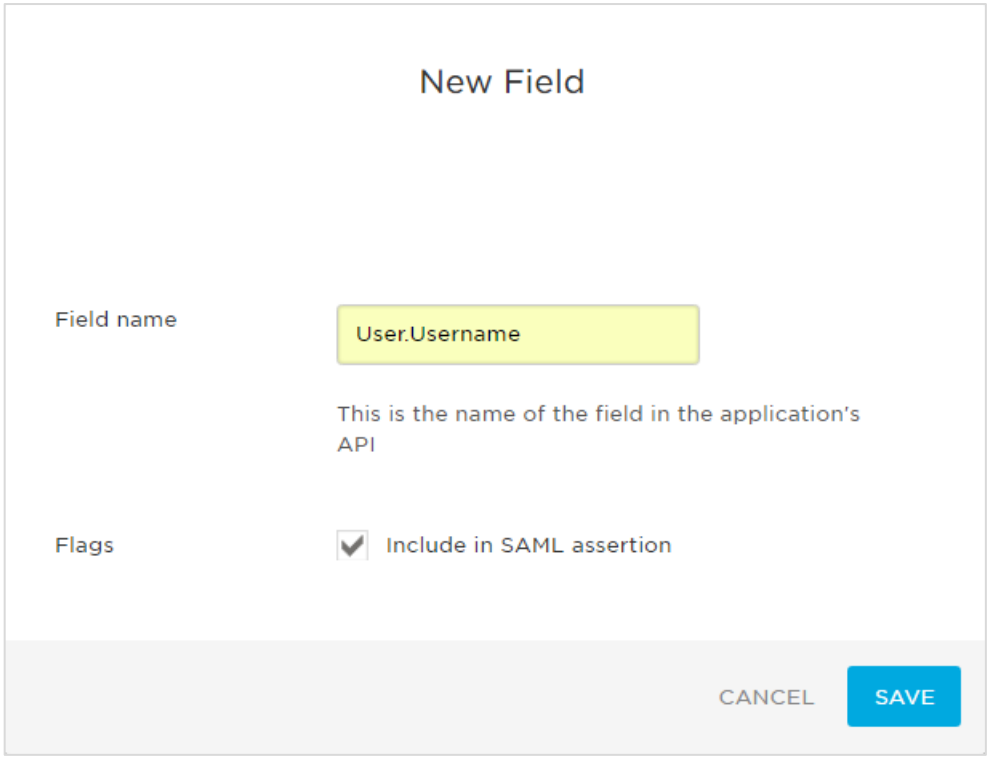
OneLogin SAML Test (IdP w/attr)



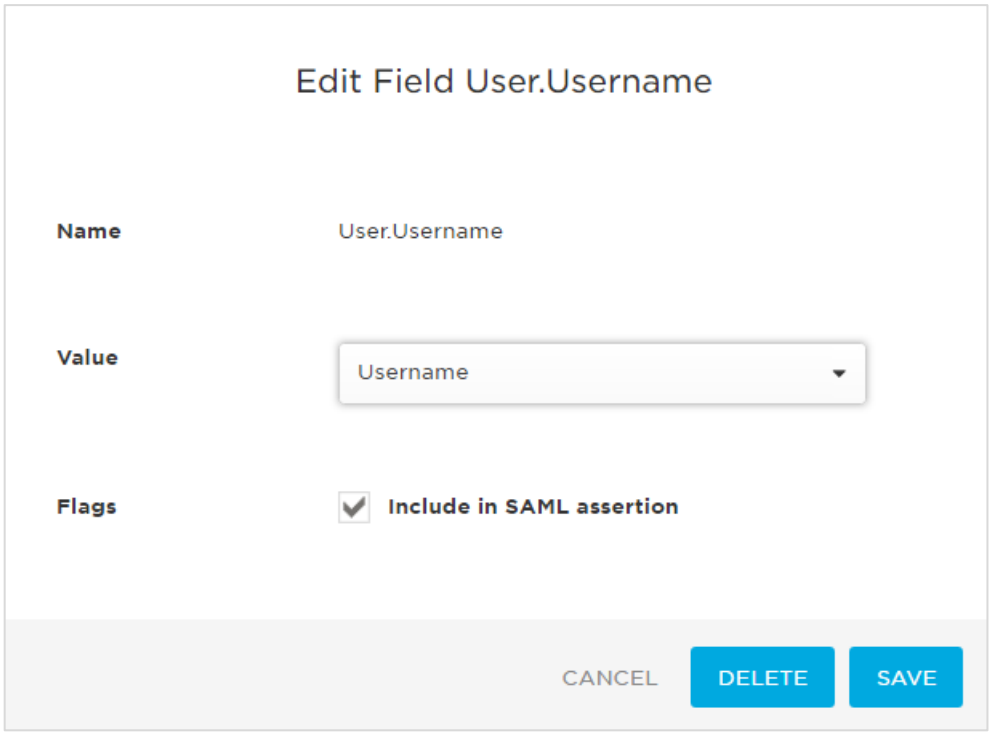
3. Make the settings in OneLogin as shown in the below screenshots.

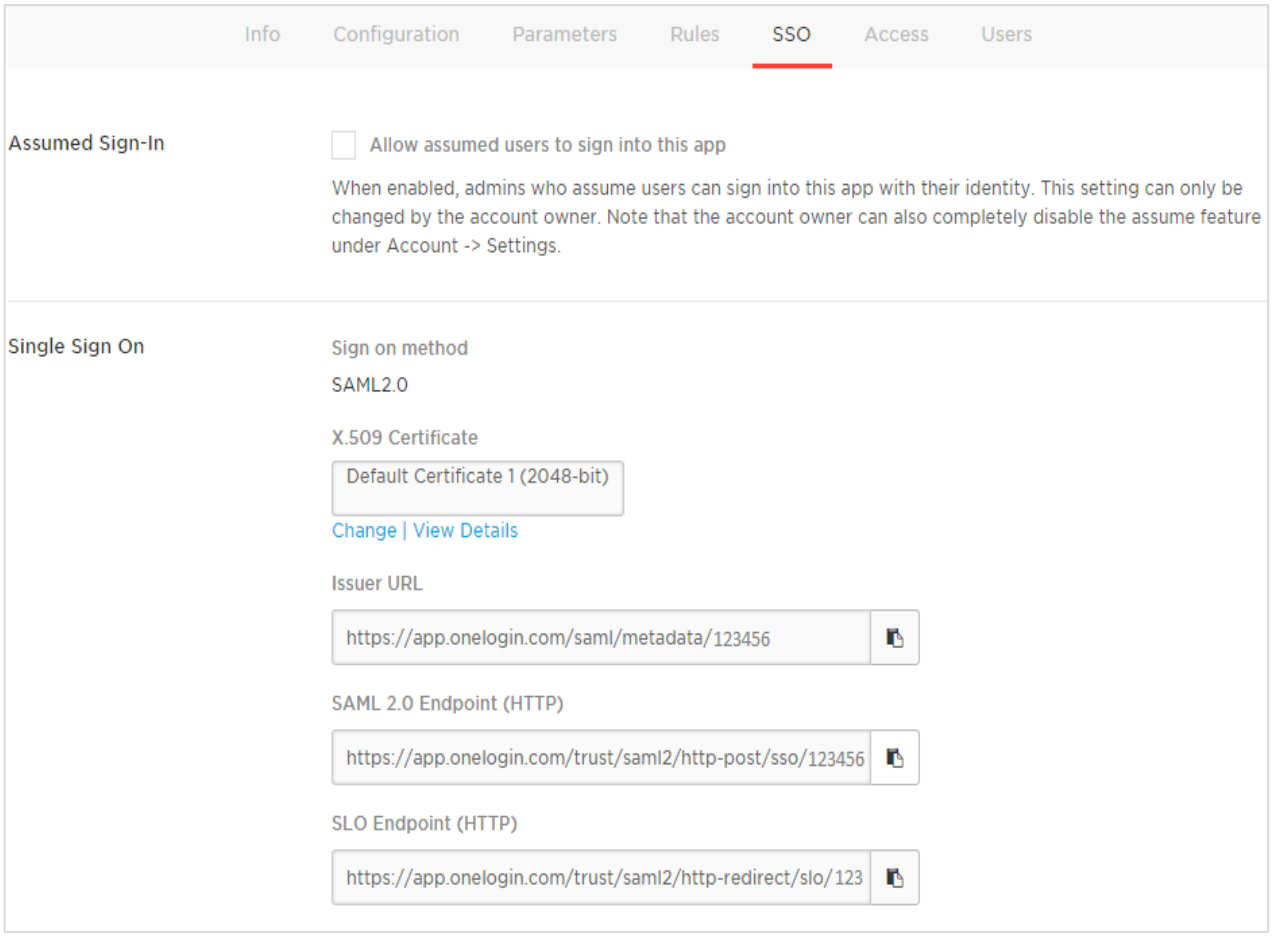


Add Parameter > User.Username as shown below. Click on Save.



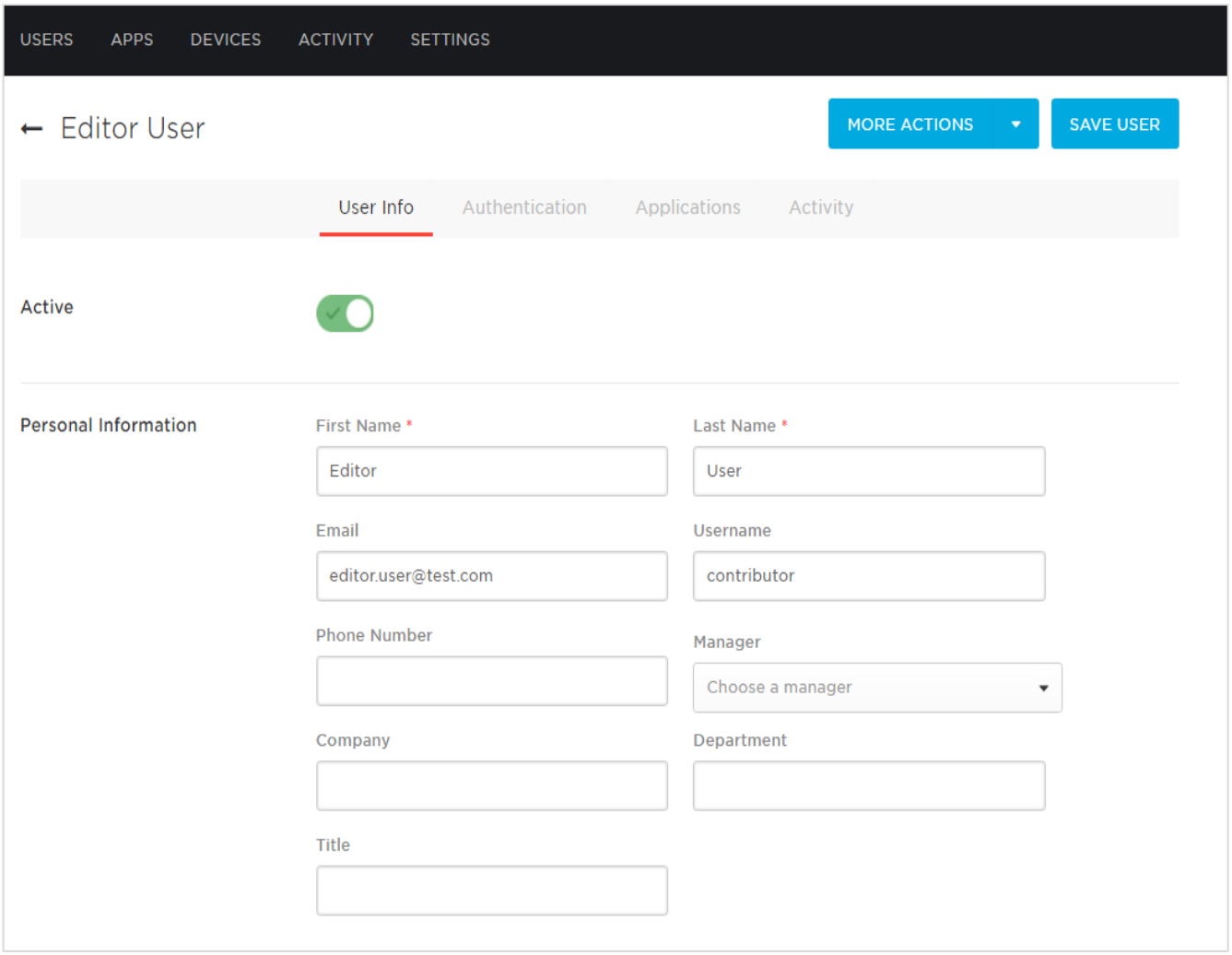
Set the value to Username and click Save.


Edit Field User.Username
Name
User.Username
Value
Username
Flags
Include in SAML assertion
CANCEL
DELETE
SAVE

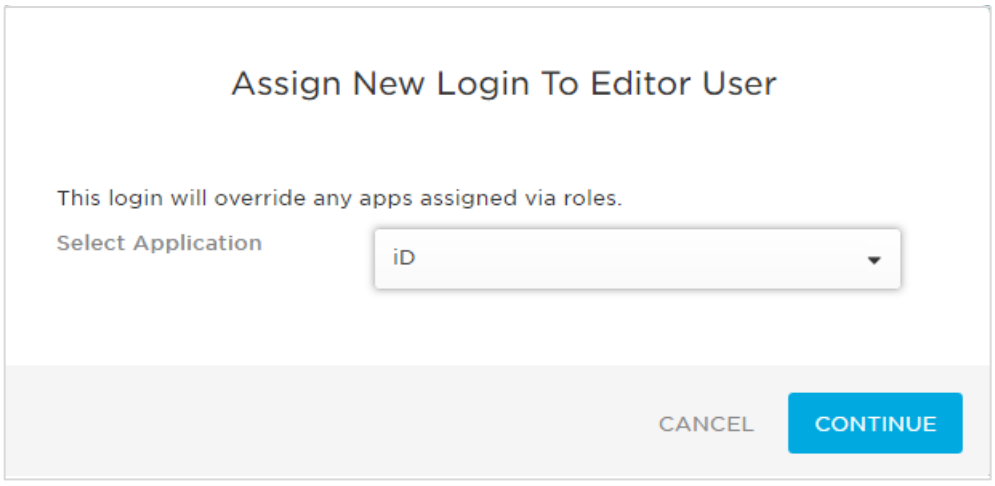


4. Now, go to the Tab titled SSO. Her you will obtain the necessary SAML Endpoint URL and the X.509 Certificate

5. To add more users to the newly created SAML application, go to USERS tab. Add user and assign application to the user.



6. In Application tab, assign the newly created SAML application to the user.



Note: GreenOrbit will be the listed field for the Select Application Option.

ADDITIONAL INFORMATION

If you have been unsuccessful configuring OKTA or OneLogin to act as an SAML Identity Provider for GO, please reach out to our support team at support@greenorbit.com.