

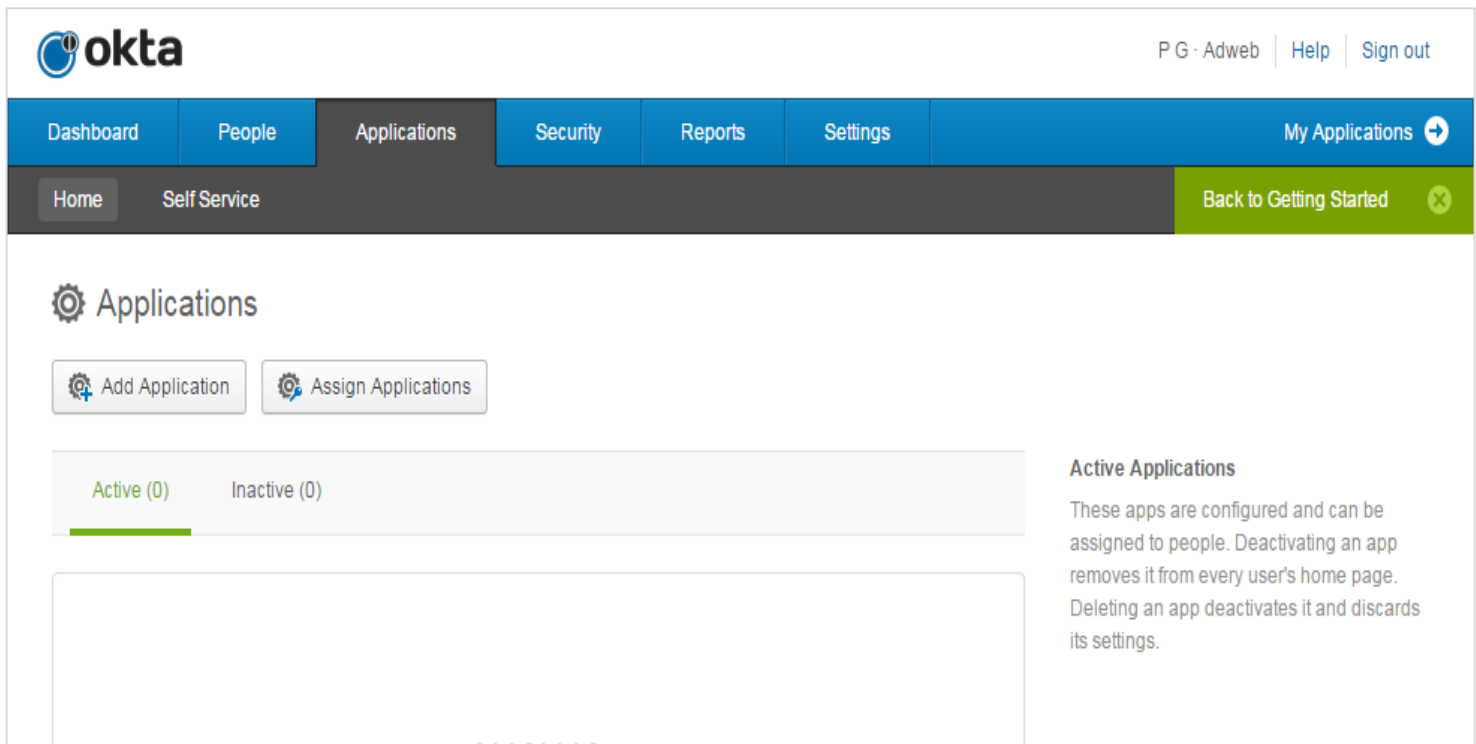
Integrate GreenOrbit with OKTA and OneLogin

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 ?

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 ?

Application username ?

[Hide Advanced Settings](#)

Response ?

Assertion Signature ?

Signature Algorithm ?

Digest Algorithm ?

Assertion Encryption ?

Enable Single Logout ? Allow application to initiate Single Logout

Authentication context class ?

Honor Force Authentication ?

SAML Issuer ID ?

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}

ATTRIBUTE STATEMENTS (OPTIONAL) [LEARN MORE](#)

Name	Name format (optional)	Value	
<input type="text" value="User.FirstName"/>	<input type="text" value="Basic"/>	<input type="text" value="user.firstName"/>	×
<input type="text" value="User.LastName"/>	<input type="text" value="Basic"/>	<input type="text" value="user.lastName"/>	×
<input type="text" value="User.email"/>	<input type="text" value="Basic"/>	<input type="text" value="user.email"/>	×
<input type="text" value="User.Username"/>	<input type="text" value="Basic"/>	<input type="text" value="user.login"/>	×

GROUP ATTRIBUTE STATEMENTS (OPTIONAL)

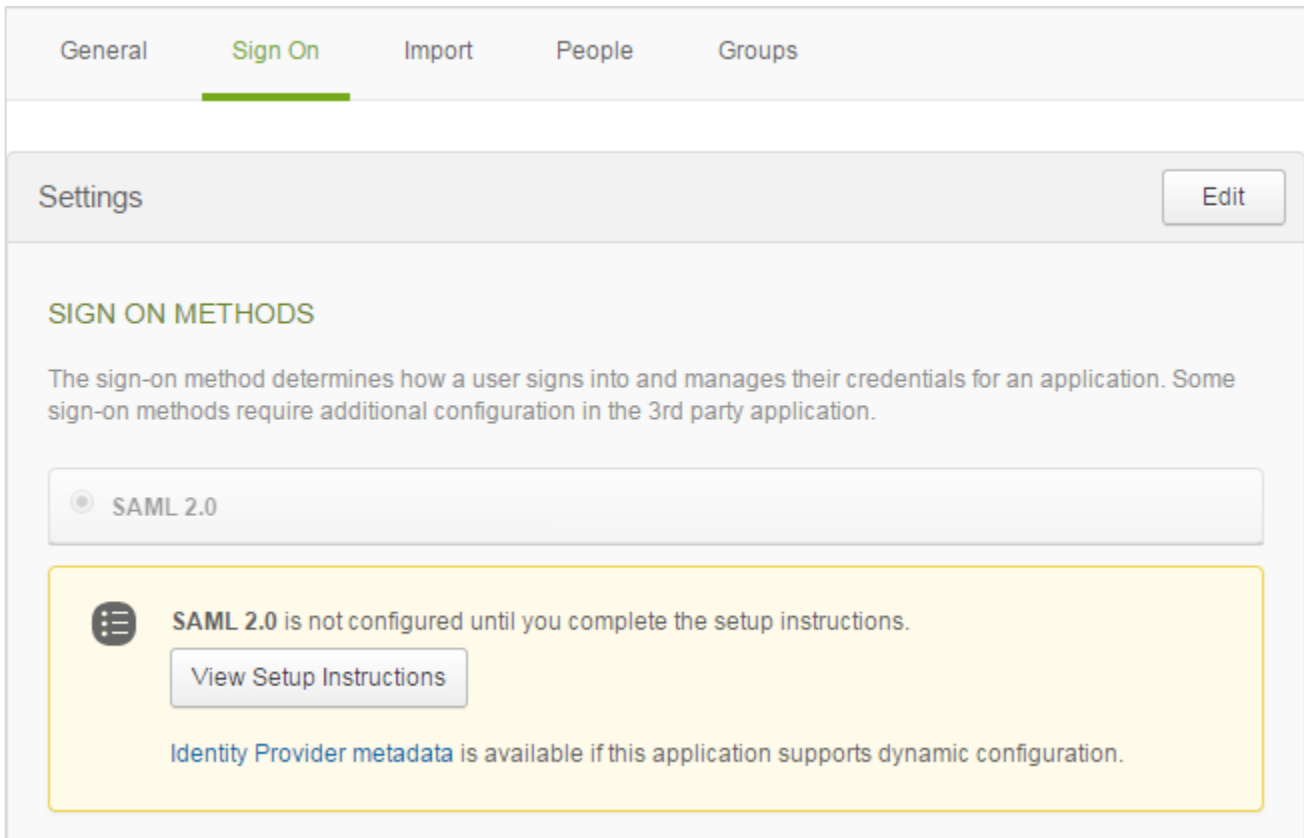
Name	Name format (optional)	Filter	
<input type="text"/>	<input type="text" value="Unspecified"/>	<input type="text" value="Starts with"/> <input type="text"/>	×

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

Assign SAML 2.0 APP to People
×

User Name

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



The screenshot shows the 'Sign On' tab selected in a settings interface. The 'Settings' header has an 'Edit' button. Under 'SIGN ON METHODS', there is a description: '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.' Below this, 'SAML 2.0' is selected with a radio button. A yellow warning box contains a menu icon, the text 'SAML 2.0 is not configured until you complete the setup instructions.', a 'View Setup Instructions' button, and the text 'Identity Provider metadata is available if this application supports dynamic configuration.'

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

The following is needed to configure SAML 2.0 APP

1 Identity Provider Single Sign-On URL:

http://company.okta.com/home/template_saml_2_0/0abcd1234efgh5678ijk9876/sso/saml

2 Identity Provider Issuer:

<http://www.okta.com/abcdefghijkl1234567890>

3 X.509 Certificate:

```
-----BEGIN CERTIFICATE-----
MIIDsDCCApigAwIBAgIGAVOnQJs3MA0GCSqGSIb3DQEBBQUAMIGYMQswCQYDVQQGEwJVUzETMBEG
A1UECAwKQ2FsaWZvcms5YTEWMBQGA1UEBwwNU2FuIEZyYW5jaXNjbzENMAAsGA1UECgwET2t0YTEU
MBIGA1UECwwLU1NPUHJvdmlkZlxiZG90b3R5b20wHhcNMTYwMzI0MDYxMTIyWWhcNMjYwMzI0MDYx
MjIyWjCBMDELMAkGA1UEBhMCVGVhZARBgNVBAgMCKNhbnG1mb3JuaWExFjAUBgNVBAcMDVNBb1BGcmFu
Y21zY28xDTALBgNVBAoMBE9rdGEzFDASBgNVBAsMC1NTT1Byb3ZpZGVyMRkwFwYDVQQDBBhZhd1YmFk
d2ViYw1bmN5MRwwGgYJKoZIhvcNAQkBFg1pbmZvQG9rdGEuY29tMIIIBIjANBgkqhkiG9w0BAQEF
AAOC AQ8AMIIBCgKCAQEAK0/Izh37a3Rd0i4vX2PNQvFuR8AxAJowtUMkUqZvYotfTq3k0TbA6bqdaQ+G1
FaZROq2p0s5FMx1w/0dGD18E4VUePW0SCFrNBIGY6Q2LwCmh16zA2NdVP3ocK4fP04X0dh1ST7EN
g8rNTJPQTPGKKrL1g3VaBTDo0R6U1MYep9MCEluXec920IfD9NZOUrYL9KJHh1iR1unVJ1vr6Cp4
54dCq2ELbqLPEF3pV3/vmeR6d#42rtC6gr6HgEkxmTn9VZk903A3/gxe/r/uCTNeBgauuWTKq+u
XvDFwrBDbi0uJsmhbHEKYDtBDjnJiKM0egH+7wco5Cs3nqZj8WE3owIDAQAAMA0GCSqGSIb3DQEB
BQUAA4IBAQAUGWIT7JoQuhwEz71vsD5xW6i/tyg0KVV9Gd66z2v0sD0DA3u4u+wJ7xFLqUkLYkTR
ETsQLU0kXq/U4wTivIS7BtmqqBwad7QmFF13i5KZ8LIRIt8pySYhEV+ySuS1Gz0fpUubv6g6iyI6o
YGC5hkI5/kwywxVpeAxpHqizBmn7H8dbPHAdzxRQ7tu6pTj05V26f2w+H56XH64naHfqYNNRrkcx
jQRz6bkQfUmPQpTEfsxx7PGXRk8FzqjmjeL6M2Nu7XoFW1a4yDML3M4gQ4LmDvwEUsxdvktVeSu3
DK4/ptF1TrtZ08Dj0fvZht1x4T1jru0Fj0wryghnmfxzrLka
-----END CERTIFICATE-----
```

Download certificate

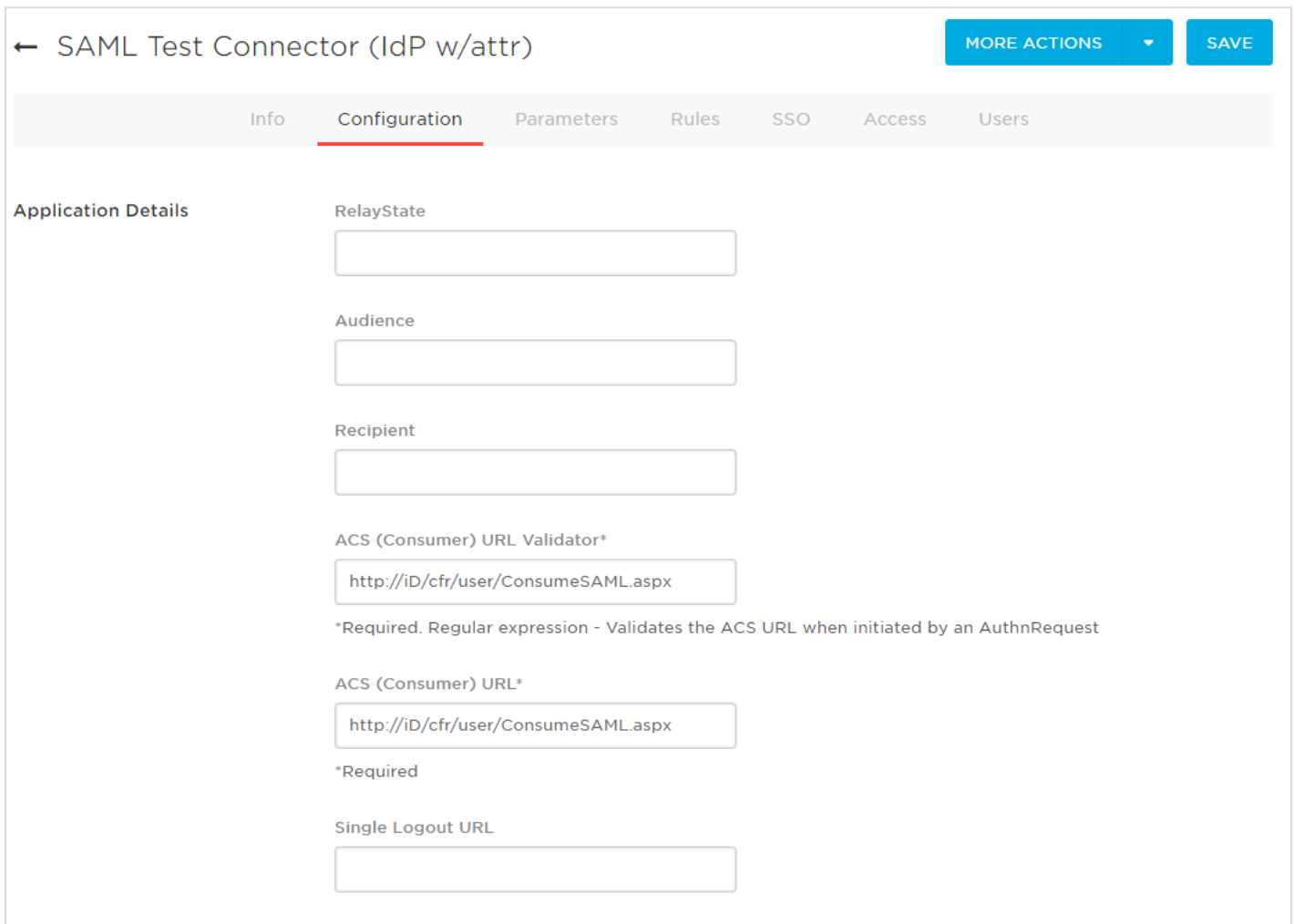
The user has to Download certificate, save it and open it in Notepad. Copy the certificate between the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- and paste in Green Orbit as mentioned above.

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)



The screenshot shows the configuration page for a SAML Test Connector (IdP w/attr) in OneLogin. The page has a breadcrumb trail: ← SAML Test Connector (IdP w/attr). At the top right, there are two buttons: 'MORE ACTIONS' with a dropdown arrow and 'SAVE'. Below the breadcrumb is a navigation bar with tabs: 'Info', 'Configuration' (which is selected and underlined), 'Parameters', 'Rules', 'SSO', 'Access', and 'Users'. The main content area is titled 'Application Details' and contains several input fields:

- RelayState:
- Audience:
- Recipient:
- ACS (Consumer) URL Validator*:
*Required. Regular expression - Validates the ACS URL when initiated by an AuthnRequest
- ACS (Consumer) URL*:
*Required
- Single Logout URL:

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

← SAML Test Connector (IdP w/attr) MORE ACTIONS  SAVE

Info Configuration Parameters Rules SSO Access Users

Credentials are
 Configured by admin Configured by admins and shared by all users

SAML Test Connector (IdP w/attr) Field	Value	Add parameter
E-mail (Attribute)	Email	
Email (SAML NameID)	Email	
First Name (Attribute)	First Name	
Last Name (Attribute)	Last Name	
Member of (Groups) (Attribute)	MemberOf	
PersonImmutableID	- No default -	

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

New Field

Field name

This is the name of the field in the application's API

Flags Include in SAML assertion

CANCEL SAVE

Set the value to Username and click Save.

Edit Field User.Username

Name	User.Username
Value	<input type="text" value="Username"/>
Flags	<input checked="" type="checkbox"/> Include in SAML assertion

[CANCEL](#) [DELETE](#) [SAVE](#)

Info Configuration Parameters Rules **SSO** Access Users


Assumed Sign-In Allow assumed users to sign into this app


When enabled, admins who assume users can sign into this app with their identity. This setting can only be changed by the account owner. Note that the account owner can also completely disable the assume feature under Account -> Settings.


Single Sign On

Sign on method
SAML2.0

X.509 Certificate
Default Certificate 1 (2048-bit)
[Change](#) | [View Details](#)

Issuer URL
 

SAML 2.0 Endpoint (HTTP)
 

SLO Endpoint (HTTP)
 

4. Now, go to the Tab titled SSO. Here 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.

USERS APPS DEVICES ACTIVITY SETTINGS

← Editor User MORE ACTIONS SAVE USER

User Info Authentication Applications Activity

Active

Personal Information

First Name *	<input type="text" value="Editor"/>	Last Name *	<input type="text" value="User"/>
Email	<input type="text" value="editor.user@test.com"/>	Username	<input type="text" value="contributor"/>
Phone Number	<input type="text"/>	Manager	<input type="text" value="Choose a manager"/>
Company	<input type="text"/>	Department	<input type="text"/>
Title	<input type="text"/>		

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

Assign New Login To Editor User

This login will override any apps assigned via roles.

Select Application

CANCEL CONTINUE

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.