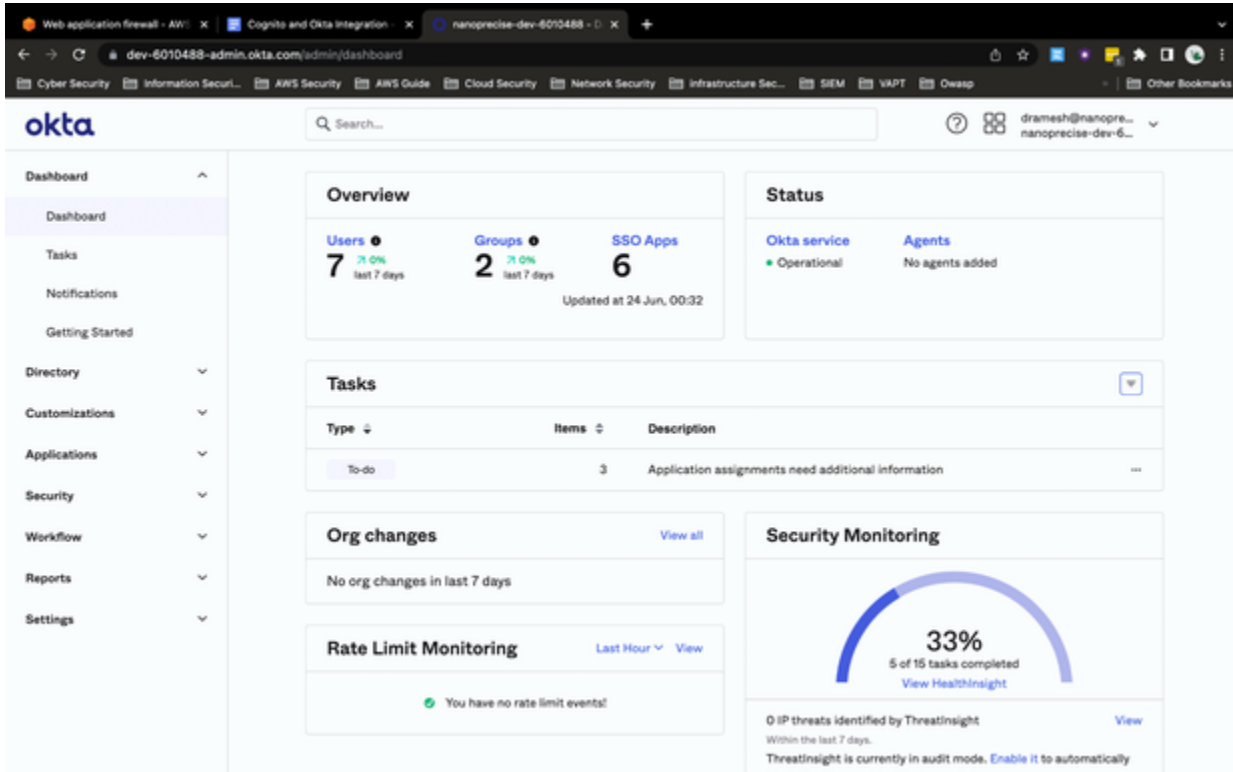


Cognito and Okta Integration

This Document will give you the entire steps and methodology to build and configure SAML app inside OKTA to connect to any SP in our case we are using COGNITO as our SP

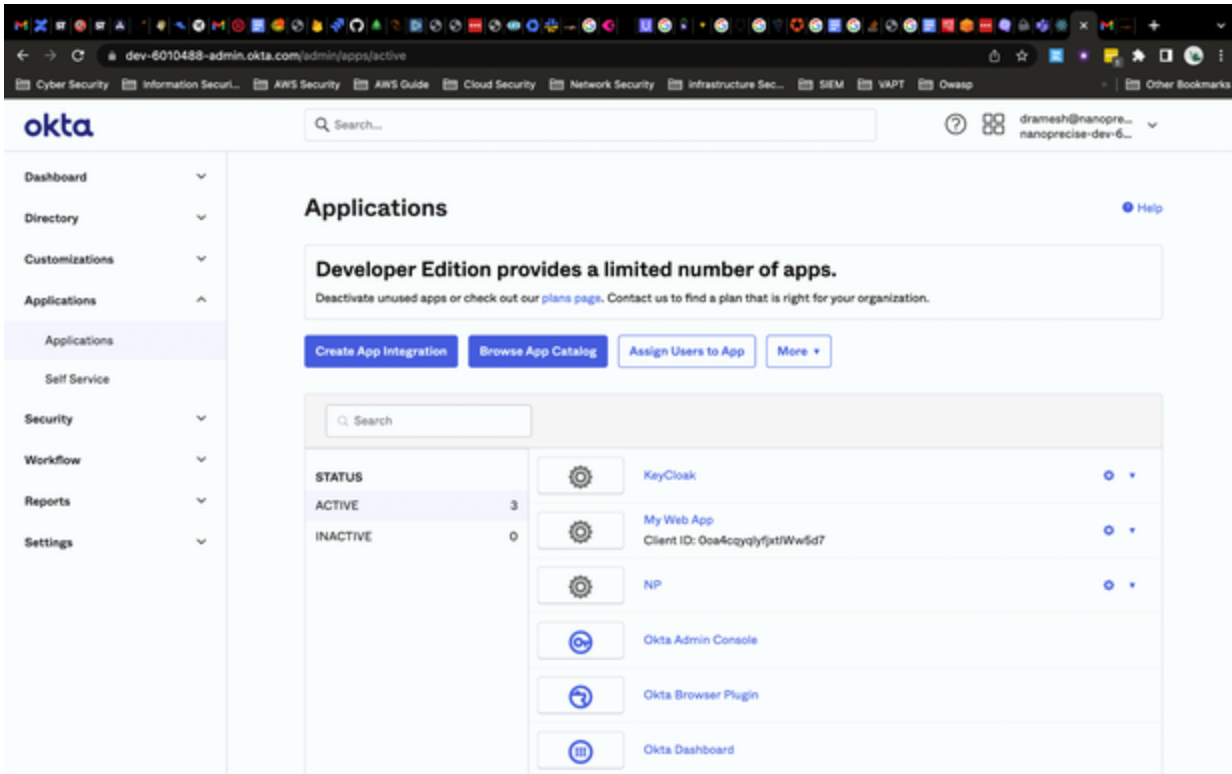
Step 1:

Get into okta app and redirect you to the dashboard to have the overview below is the display SS of generic OKTA dashboard



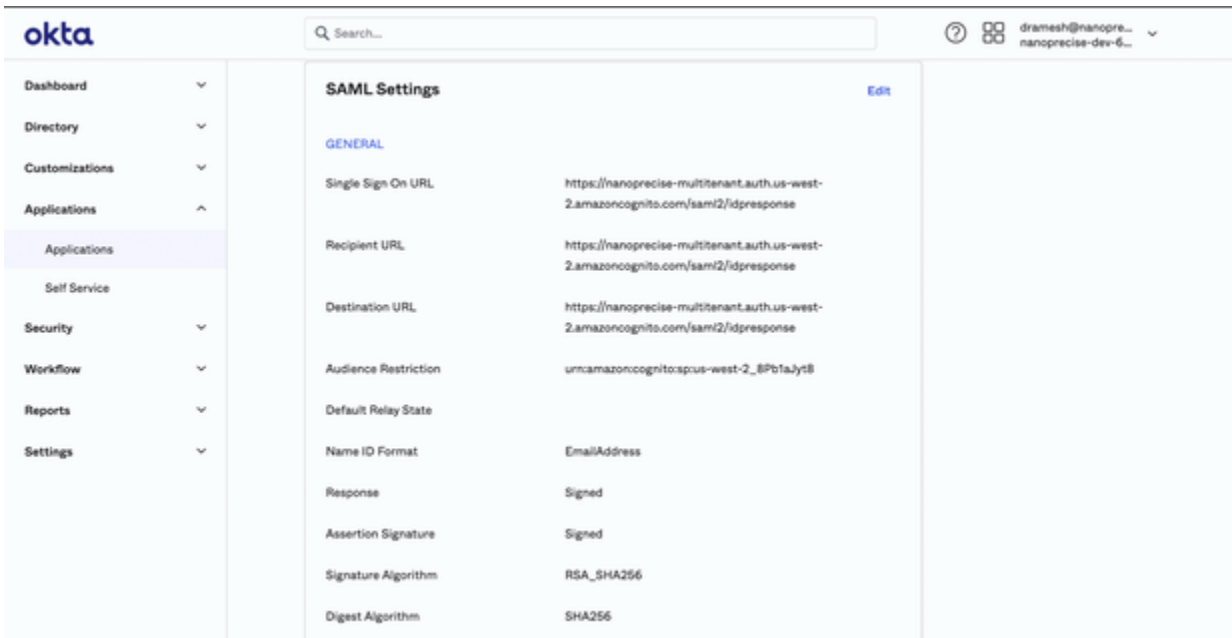
Step 2:

Create an APP Integration under application menu



Step 3:

Basic Configuration to be followed , In case of client end Nanoprecise will be providing all these Metadata to get the app integration configuration done.



Step 4: App Attribute statements we are going to map the attributes to XML metadata via some URI reference. This is for SAML integration. Attaching the mapping elements below as a screenshot

ATTRIBUTE STATEMENTS		
Name	Name Format	Value
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/emailaddress	URI Reference	user.email
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/firstme	URI Reference	user.fullName
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/fullme	URI Reference	user.fullName
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/companyid	URI Reference	user.companyId
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/roleid	URI Reference	user.roleID
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/roleid	URI Reference	user.demo
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/phoneNumber	URI Reference	user.phoneNumber
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/internalAdmin	URI Reference	user.internalAdmin
http://schemas.xmlsoap.org/ws/ URI Reference s/2005/05/identity/claims/companyList	URI Reference	user.companyList
GROUP ATTRIBUTE STATEMENTS		
Name	Name Format	Filter

Step 5: Attributes that need to be added and passed as a value from IDP to SP needs to be created and mapped first we will look into creation

Goto >> Directory >> Profile editor

Under profile editor you will see something like this below.

- Consider "NP" is your app name the attributes and the user values that need to be passed can be created under "NP User"
- Creating there alone will not suffice your requirement it should be both the ways please do create it under "Okta User" also since it is the SP facing entity
- It will be displayed as "User (default)"

Profile Editor

Users Groups

Users

Filters	Profile	Type	
All	okta User (default)	Okta	
Okta	NP User	Application	Mappings
Apps	dev600488_np_1	Application	Mappings
Directories	My Web App User	Application	Mappings
Identity Providers	oidc_client	Application	Mappings
	Keycloak User	Application	Mappings
	dev600488_keycloak_1		

© 2022 Okta, Inc. Privacy Version 2022.06.1 C OK12 Call (US) Status site Download Okta Plugin Feedback

Step 6:

How to create the custom attributes with internal data types and enumeration. Below is the attribute created for "NP User"

Variable name: dev0010488_np_1

Attributes

+ Add Attribute | Mappings

FILTERS	Display Name	Variable Name	Data type	Attribute Type
All	Username	userName	string	Base
Base	email	email	string	Custom
Custom	name	name	string	Custom
	companyId	companyId	string	Custom
	fullName	fullName	string	Custom
	demo	demo	number	Custom
	phoneNumber	phoneNumber	string	Custom
	roleID	roleID	number	Custom
	CompanyList	companyList	array	Custom
	Internal User	InternalAdmin	number	Custom

- To avoid confusion please keep the Display Name and Variable Name as same
- All the attributes are case sensitive please do not change anything and replicate the same
- Once the data type is Declared it cannot be changed later until and unless you delete the attribute and recreate again so please be cautious on creating the data type
- Inside demo, roleID, companyList and internal admin we have enumeration adding the screenshot below for that


References :

Demo


demo

Data type

number

Display name 

demo 

Variable name 

dev6010488_np_1.demo

Description

Enum

Define enumerated list of values

Attribute members

Display name	Value	
<input type="text" value="0"/>	0	<input type="button" value="x"/>
<input type="text" value="1"/>	1	<input type="button" value="x"/>

Attribute Range

Between min and max

Attribute required

Yes

Scope

None

Mutability


READ_WRITE

roleID

roleID

Data type

number

Display name 

roleID 

Variable name 

dev6010488_np_1.roleID

Description


Enum

Define enumerated list of values

Attribute members

Display name	Value	
<input type="text" value="Super Admin"/>	131	<input type="button" value="x"/>
<input type="text" value="Admin"/>	132	<input type="button" value="x"/>
<input type="text" value="Manager"/>	133	<input type="button" value="x"/>
<input type="text" value="Engineer"/>	134	<input type="button" value="x"/>
<input type="text" value="Technician"/>	135	<input type="button" value="x"/>
<input type="text" value="Home Page Only"/>	136	<input type="button" value="x"/>

Attribute Range

Between  min and max

Attribute required

Yes


companyList

CompanyList

companies accessible by user

Data type

string array

Display name 

CompanyList 

Variable name 

dev6010488_np_1.companyList

Description

companies accessible by user

Enum

Define enumerated list of values

Attribute members

Display name	Value	
<input type="text" value="KENMEX"/>	CAHK	<input type="button" value="x"/>
<input type="text" value="GREENWD"/>	CAHG	<input type="button" value="x"/>
<input type="text" value="29DELAND"/>	CAHD	<input type="button" value="x"/>
<input type="text" value="CHICOPEE"/>	CAHC	<input type="button" value="x"/>
<input type="text" value="62AUGUST"/>	CAHA	<input type="button" value="x"/>
<input type="text" value="CMSCR"/>	CAHR	<input type="button" value="x"/>

Attribute required

Yes

Scope

None

internalAdmin

Please make sure all the enumeration list has the "Read Write" access

Internal User

internal user

Data type

number

Display name

Internal User

Variable name

dev6010488_np_1.internalAdmin

Description

internal user

Enum

Define enumerated list of values

Attribute members

Display name

Value

False

0

True

1

+ Add Another

Attribute Range

Between min and max

Attribute required

Yes

Scope

None

Mutability

READ_WRITE

Save Attribute

Cancel

Mapping

Please do replicate same as above on Okta "User (default)" as well so that we could do mapping





You will find the profile mapping under the Profile editing section

Profile Editor

Help

Users Groups

Users

Filters	Profile	Type
All	 User (default) user	Okta
Okta	 NP User dev6010488_np_1	Application Mappings
Apps	 My Web App User web_client	Application Mappings
Directories	 Keycloak User dev6010488_keycloak_1	Application Mappings
Identity Providers		

Do a mapping and turn the arrow mark into green below is **Okta User** to **NP** same way we should mapp it for **NP** to **Okta User**

NP User Profile Mappings

X

NP to Okta User

Okta User to NP



Okta User User Profile
user



NP User Profile
appuser

Username is set by NP

user.email	▼	→	▼
user.displayName	▼	→	▼
user.companyId	▼	→	▼
user.fullName	▼	→	▼
user.demo	▼	→	▼
user.phoneNumber	▼	→	▼
user.roleID	▼	→	▼
user.companyList	▼	→	▼
user.internalAdmin	▼	→	▼

userName	string
email	string
name	string
companyId	string
fullName	string
demo	number
phoneNumber	string
roleID	number
companyList	string array
internalAdmin	number

Preview

Enter an Okta user to preview their mappi

Save Mappings

Cancel

appuser.userName	→	userName	string
appuser.companyId	→	companyId	string
appuser.fullName	→	fullName	string
appuser.roleID	→	roleID	number
appuser.demo	→	demo	number
appuser.phoneNumber	→	phoneNumber	string
appuser.companyList	→	companyList	string array
appuser.internalAdmin	→	internalAdmin	number

Enter an Okta user to preview their mappi

You could always preview the user by entering his name in preview option to check if the mapping is done properly and whether the user is passing all the required parameter or what.

appuser.userName	string	"bseivam@nanoprecise.io"	string
appuser.companyId	string	"CAHK"	string
appuser.fullName	string	null	string
appuser.roleID	number	131	number
appuser.demo	number	1	number
appuser.phoneNumber	string	"+912345678811"	string
appuser.companyList	string array	["CAHK","CAHG","CAHD","CAHC","CAHA","CAHR"]	string array
appuser.internalAdmin	number	1	number

Balaji s

Conclusion All set to use the OKTA and configuration if this is done on OKTA end