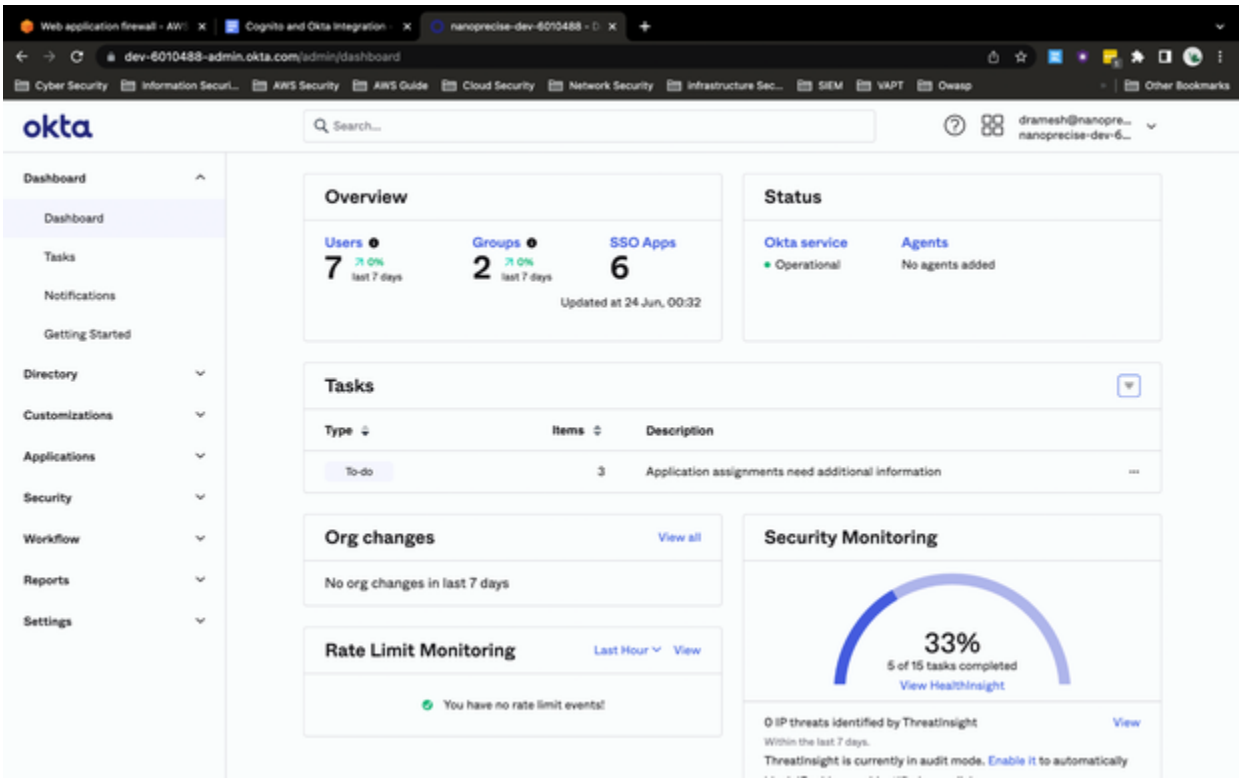
Cognito and Okta Integration

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

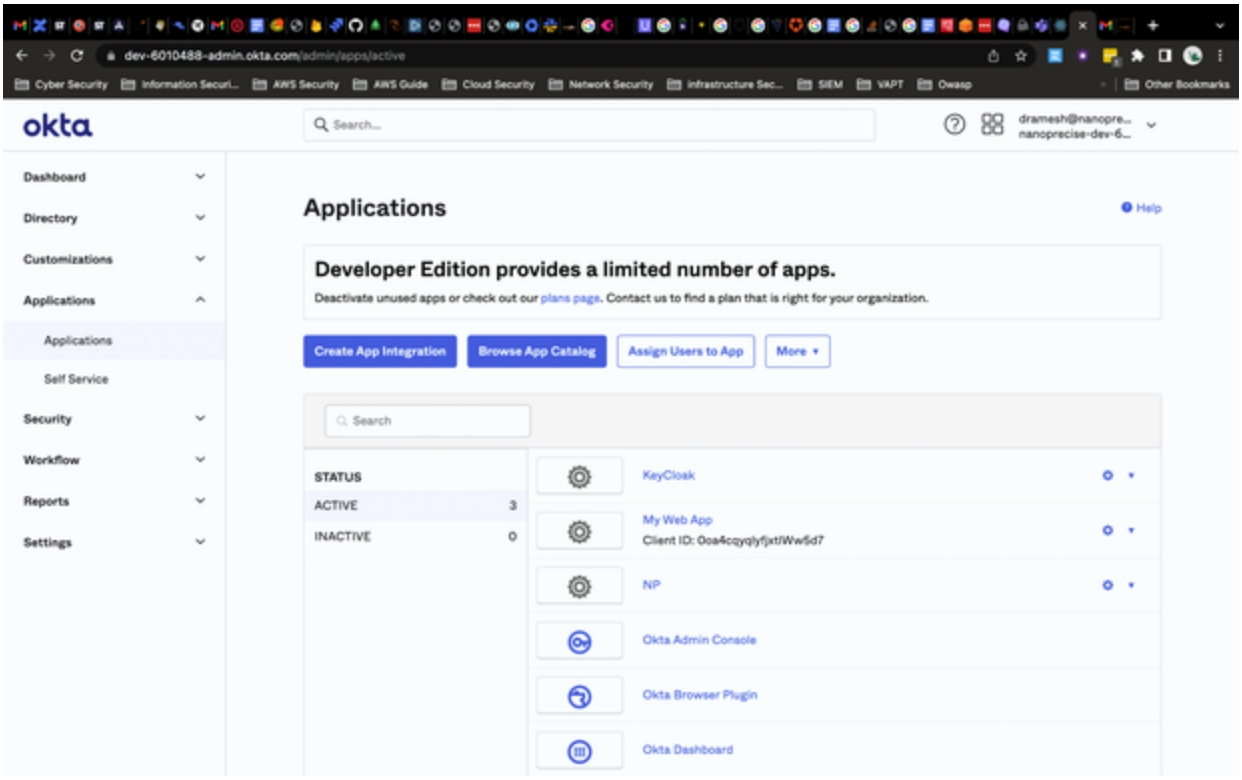
Step 1:

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



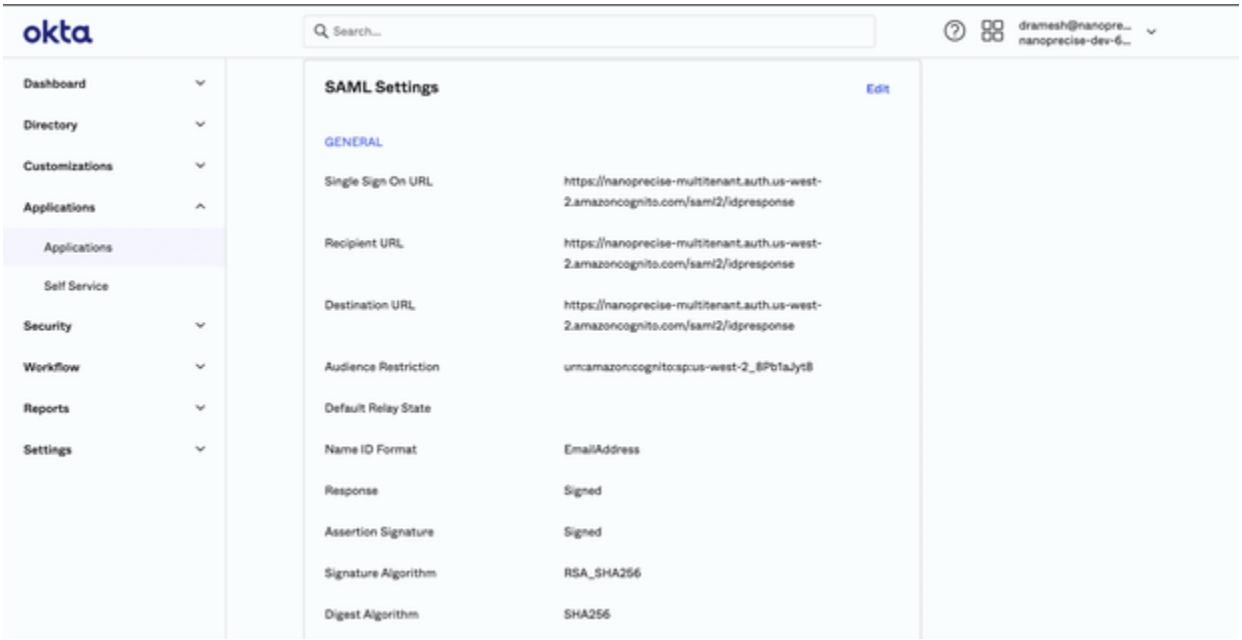
Step 2:

Create an APP Integration under application menu

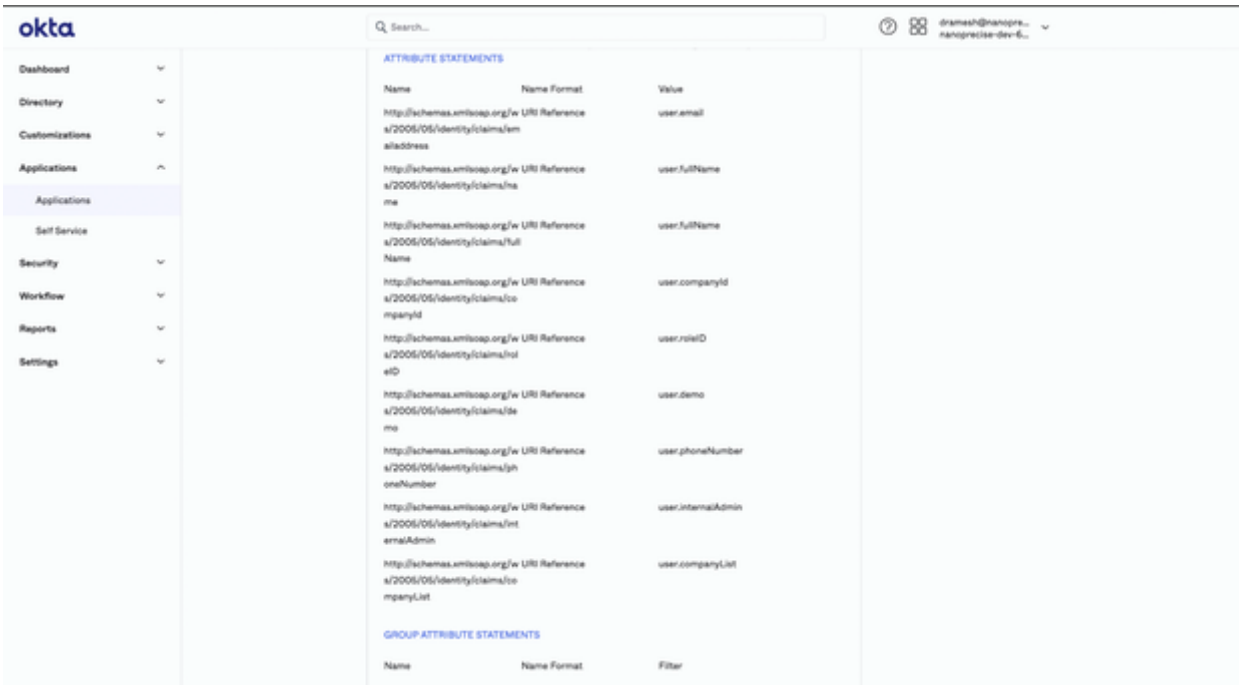


Step 3:

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

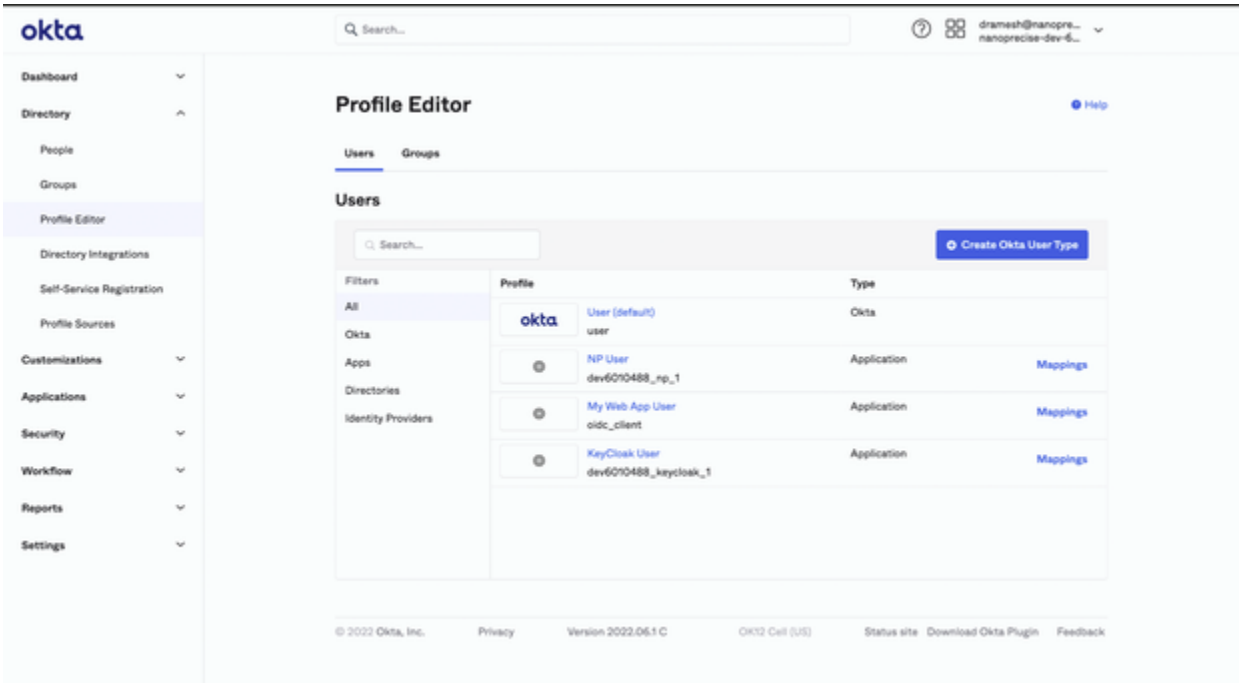


Step 5: Attributes that need to be added and passed as a value from IDP to SP needs to be created and mapped first we will look into creation

Goto >> Directory >> Profile editor

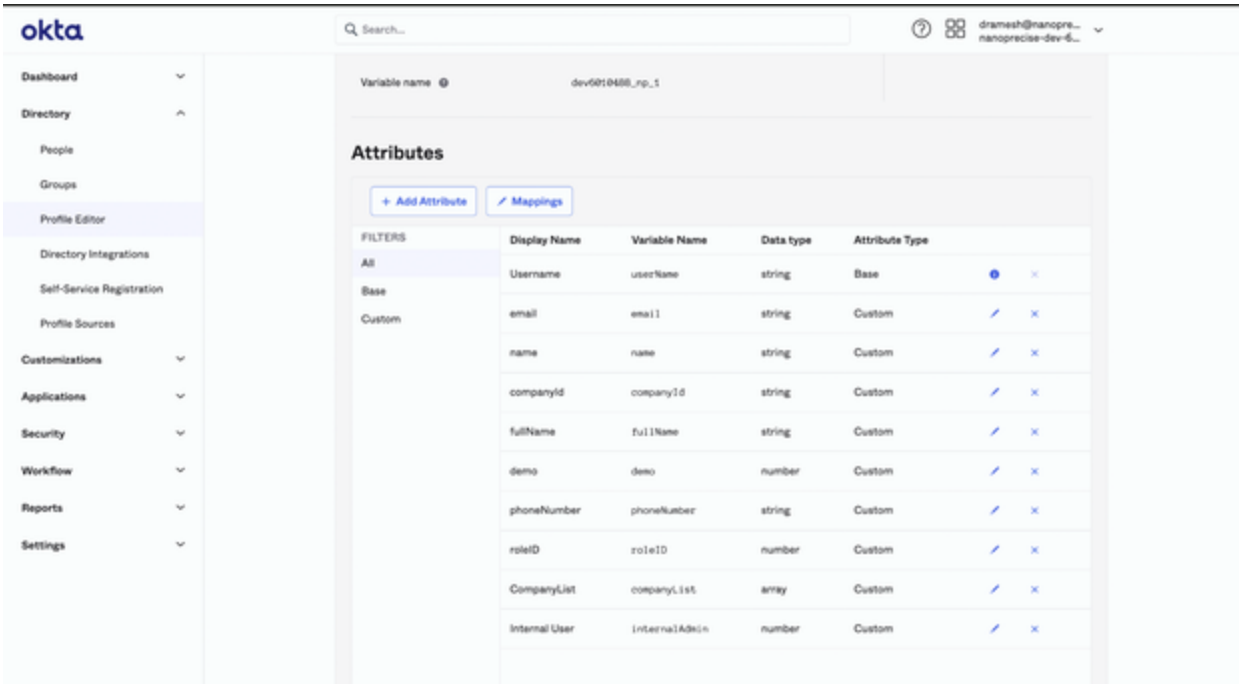
Under profile editor you will see something like this below.

- 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)”



Step 6:

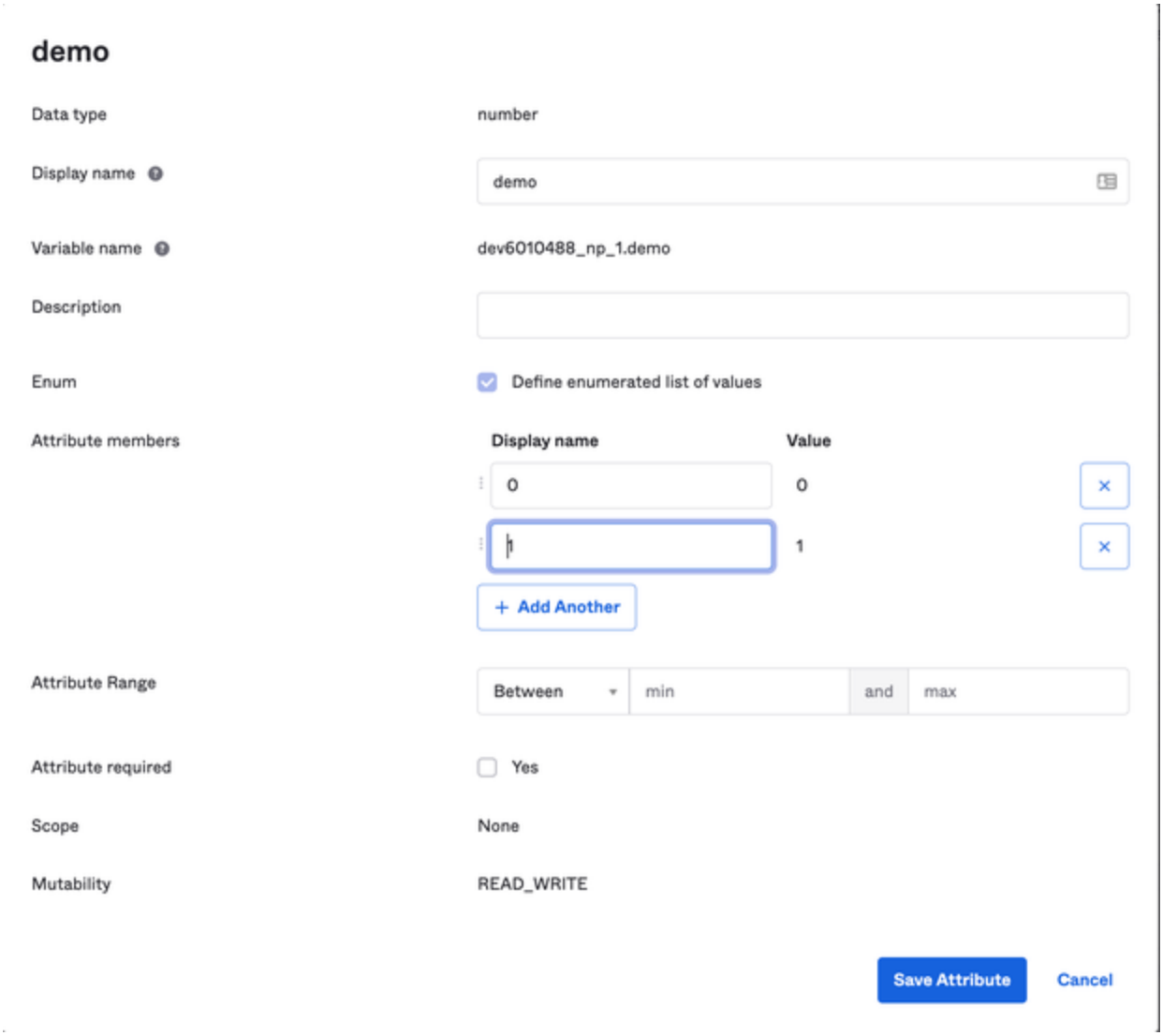
How to create the custom attributes with internal data types and enumeration. Below is the attribute created for “NP User”



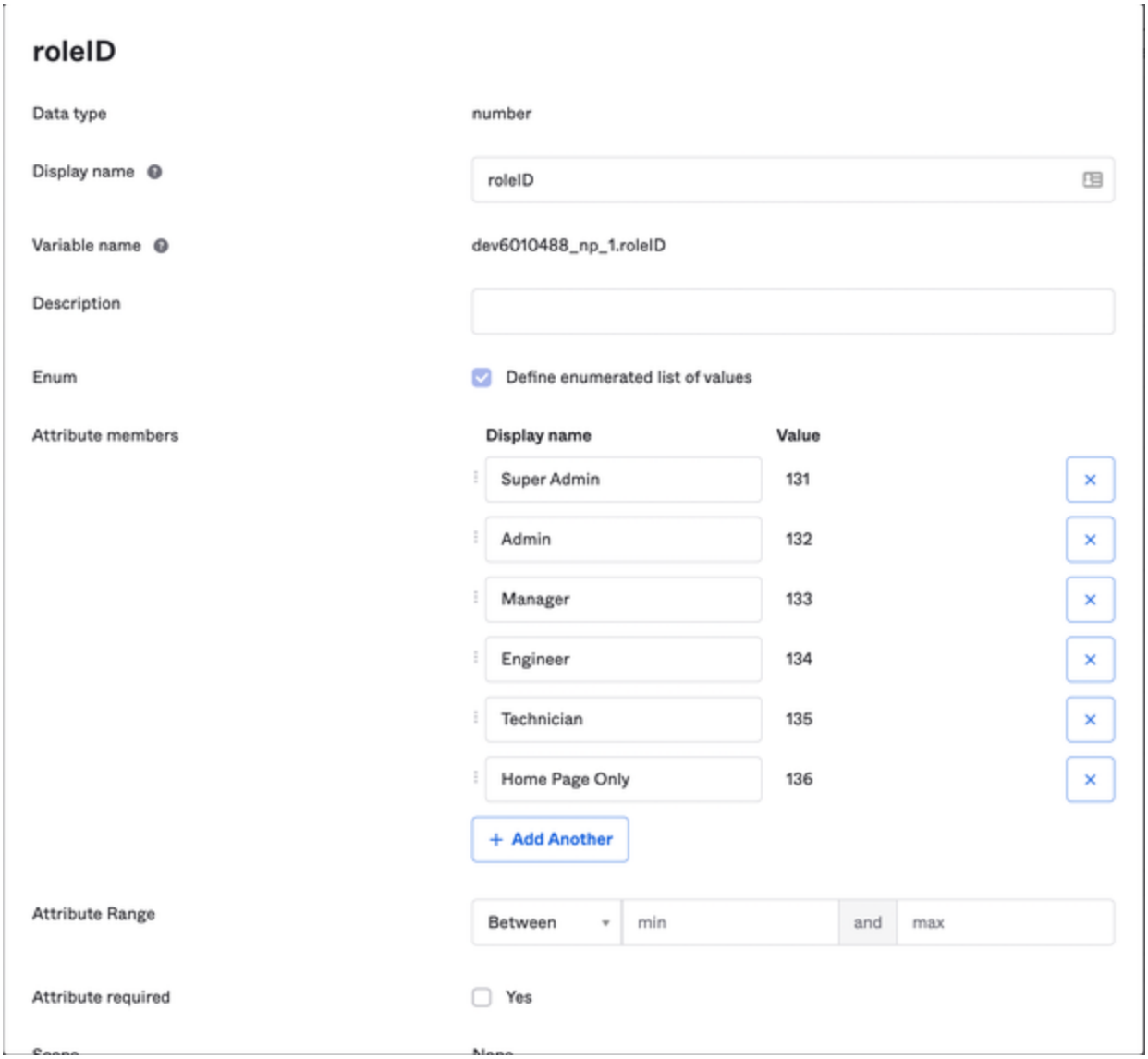
- To avoid confusion please keep the Display Name and Variable Name as same
- All the attributes are case sensitive please do not change anything and replicate the same
- Once the data type is Declared it cannot be changed later until and unless you delete the attribute and recreate again so please be 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
0
0
1
1
+ Add Another
Attribute Range
Between
min
and
max
Attribute required
Yes
Scope
None
Mutability
READ_WRITE
Save Attribute
Cancel

roleID



companyList

CompanyList

companies accesible by user

Data type	string array
Display name	CompanyList
Variable name	dev6010488_np_1.companyList
Description	companies accesible by user
Enum	Define enumerated list of values

Attribute members

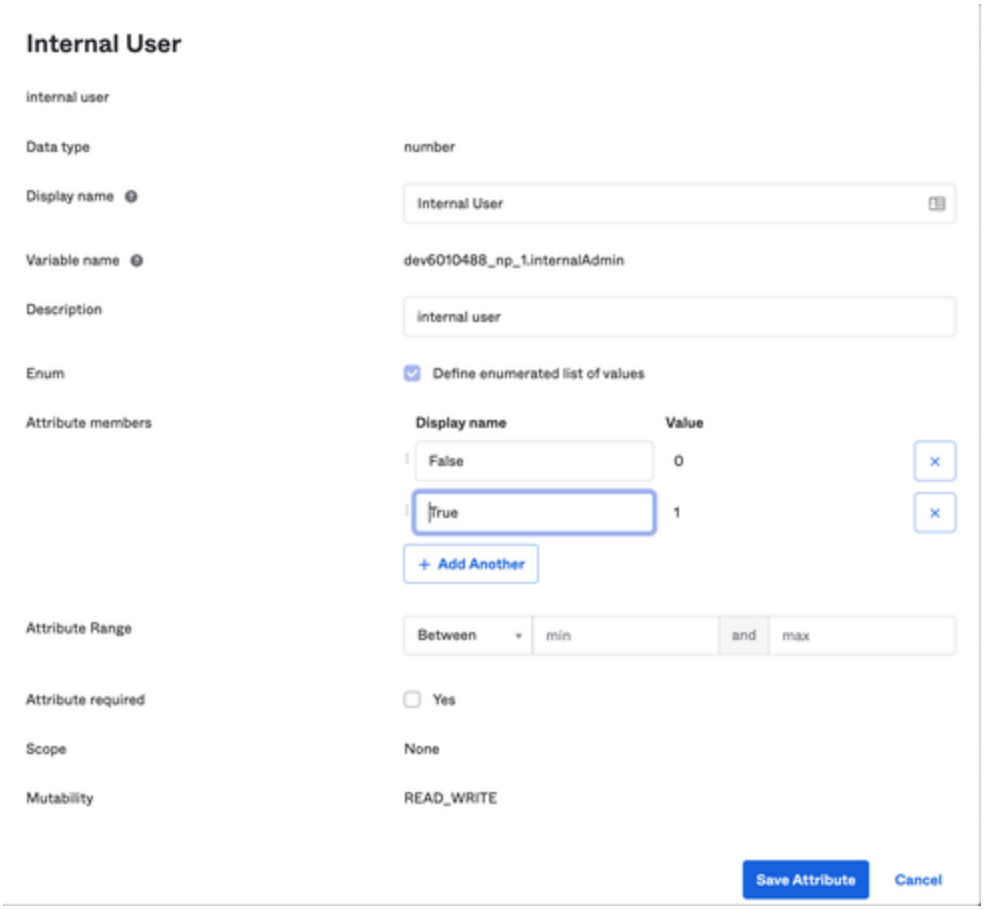
Display name	Value
KENMEX	CAHK
GREENWD	CAHG
29DELAND	CAHD
CHICOPEE	CAHC
62AUGUST	CAHA
CMSCR	CAHR

+ Add Another

Attribute required	Yes
Scope	None

internalAdmin

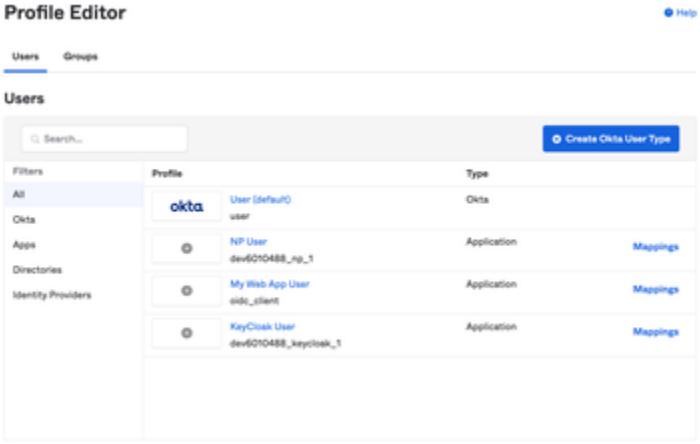
Please make sure all the enumeration list has the “Read Write” access



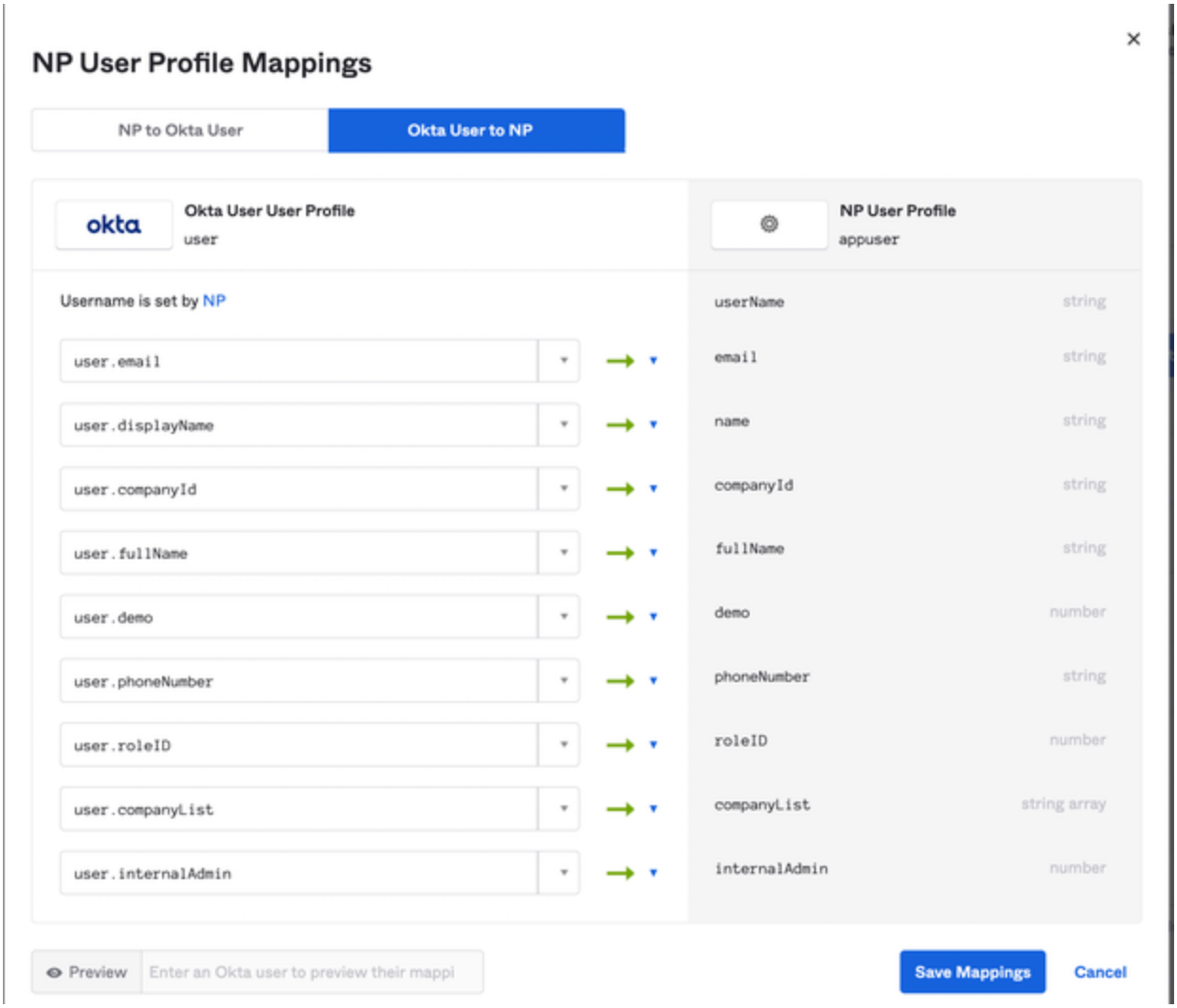
Mapping

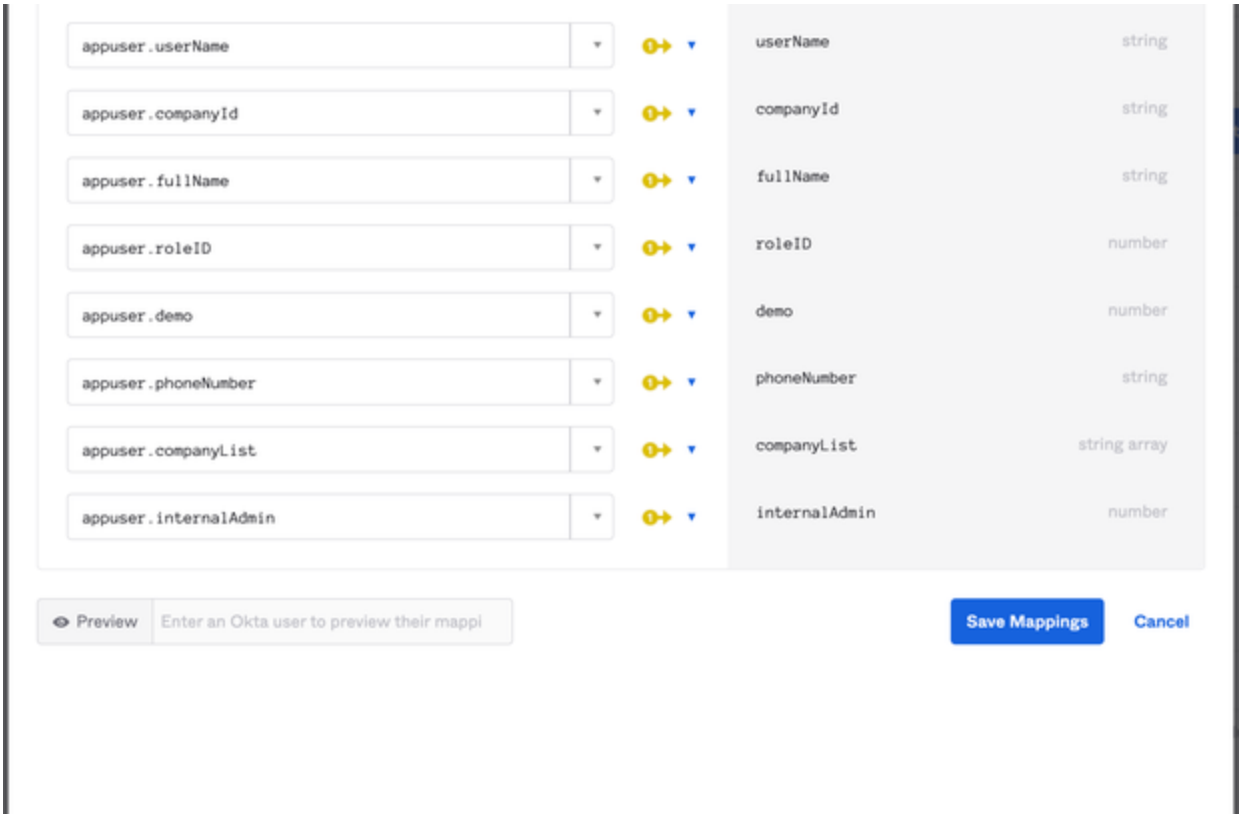
Please do replicate same as above on Okta “User (default)” as well so that we could do mapping

You will find the profile mapping under the Profile editing section

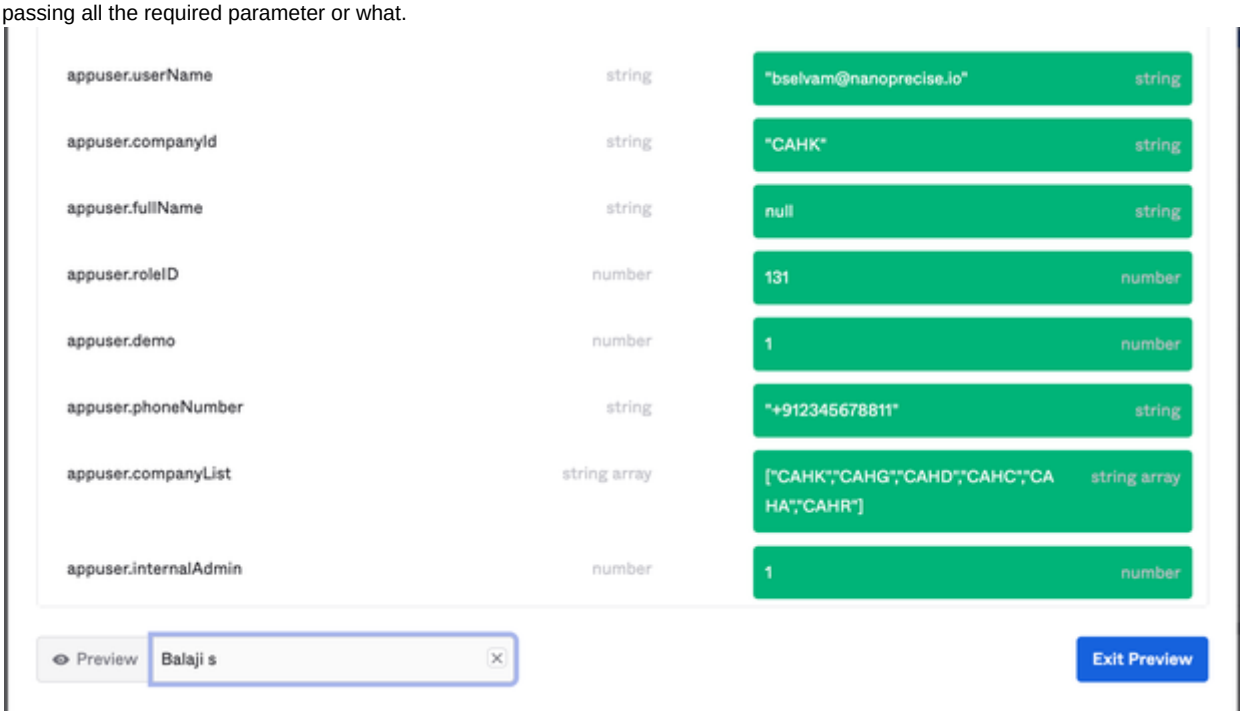


Do a mapping and turn the arrow mark into green below is Okta User to NP same way we should mapp it for NP to Okta User


NP User Profile Mappings
NP to Okta User
Okta User to NP
okta
Okta User User Profile
user
NP User Profile
appuser
Username is set by NP
user.email
email
string
user.displayName
name
string
user.companyId
companyId
string
user.fullName
fullName
string
user.demo
demo
number
user.phoneNumber
phoneNumber
string
user.roleID
roleID
number
user.companyList
companyList
string array
user.internalAdmin
internalAdmin
number
userName
string
Preview
Enter an Okta user to preview their mappi
Save Mappings
Cancel



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.



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