Integration of Gitlab with Key Cloak for SSO

|  |  |  |  |
| --- | --- | --- | --- |
| Documents Name | Version | Prepared By | Reviewed By |
| Integration of Gitlab with Key Cloak | v.01 | Vikat Patil |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Keycloak as a SAML Identity Provider 3](#_Toc61710024)

[1.1 Step 1 : In the Keycloak server, create a new SAML client 3](#_Toc61710025)

[1.2 Step 2 : Configure newly created SAML Client in Keycloak for Gitlab. 3](#_Toc61710026)

[1.3 Step 3: Copy Certificate from Realm. 7](#_Toc61710027)

[1.4 Step 4: Setup Gitlab. 8](#_Toc61710028)

[1.5 Step 5: Reconfigure the Gitlab. 9](#_Toc61710029)

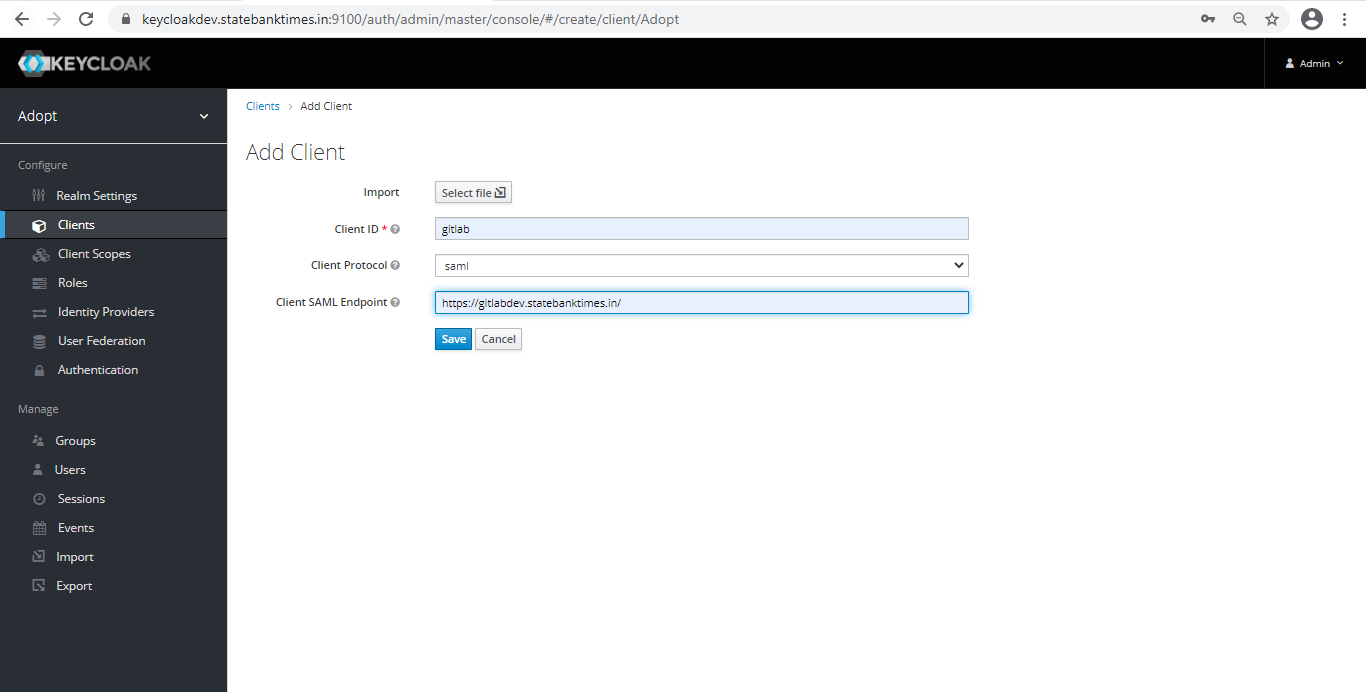
# Keycloak as a SAML Identity Provider

The following example may be useful if you're using Keycloak as a SAML Identity Provider.

## Step 1 : [In the Keycloak server, create a new SAML client](https://docs.sonarqube.org/latest/instance-administration/delegated-auth/)

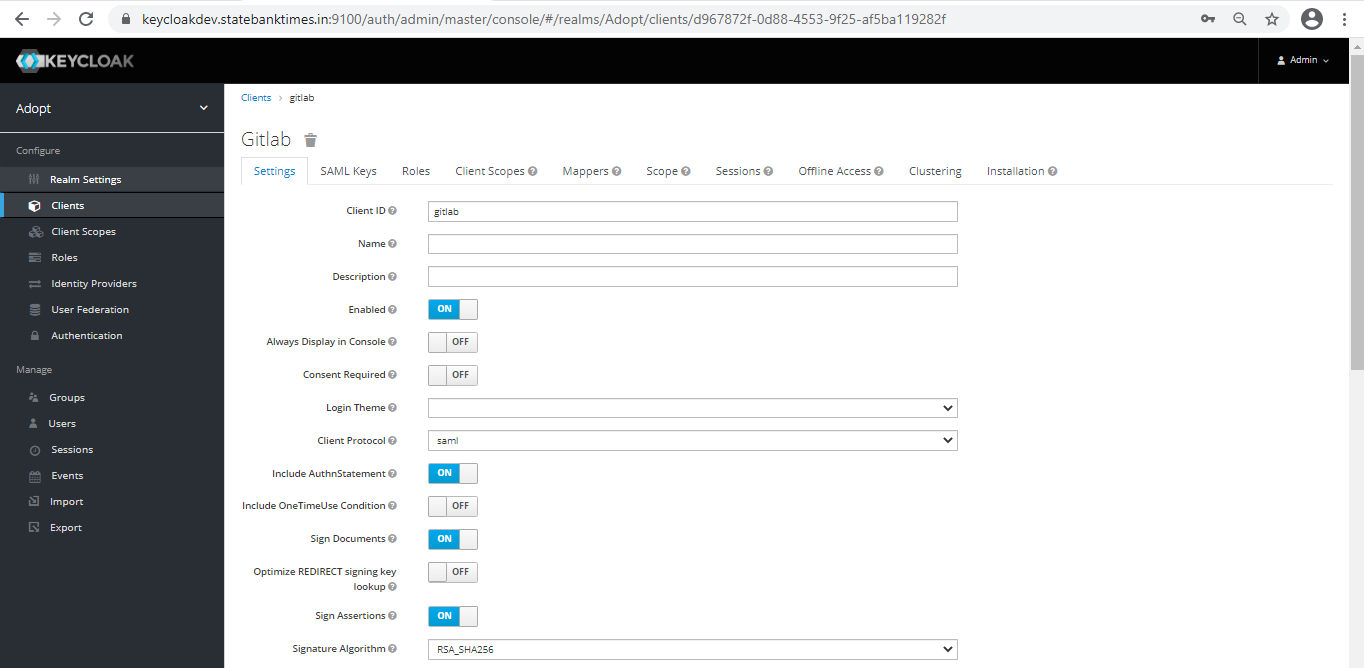
Our realm name is Adopt. Yours can be different. So change Adopt with your own realm name wherever possible.  
  
NOTE Replace https://gitlabdev.statebanktimes.in with your actual GitLab hostname, example gitlabdev.statebanktimes.in.  
  
Go to the Clients page and click the Create button in the right upper corner.

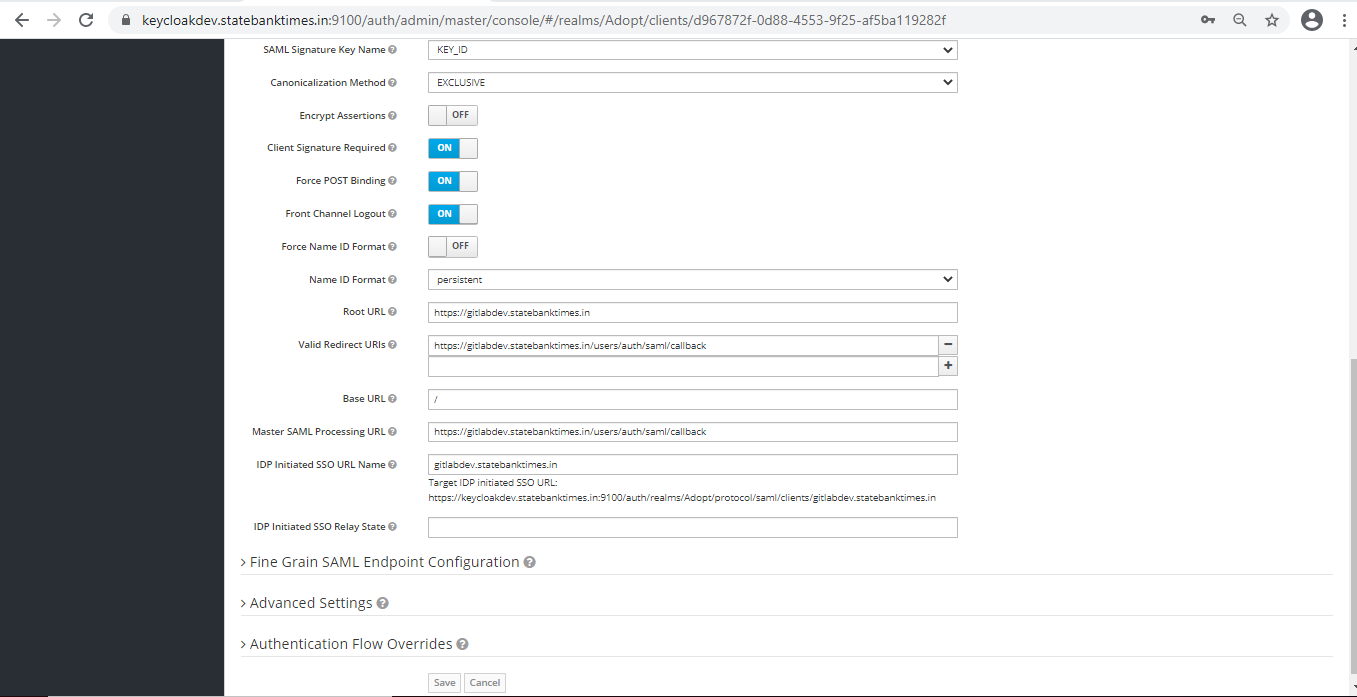
1. "Client ID" is something like "sonarqube"
2. "Client Protocol" must be set to "saml"
3. "Client SAML Endpoint" can be left empty



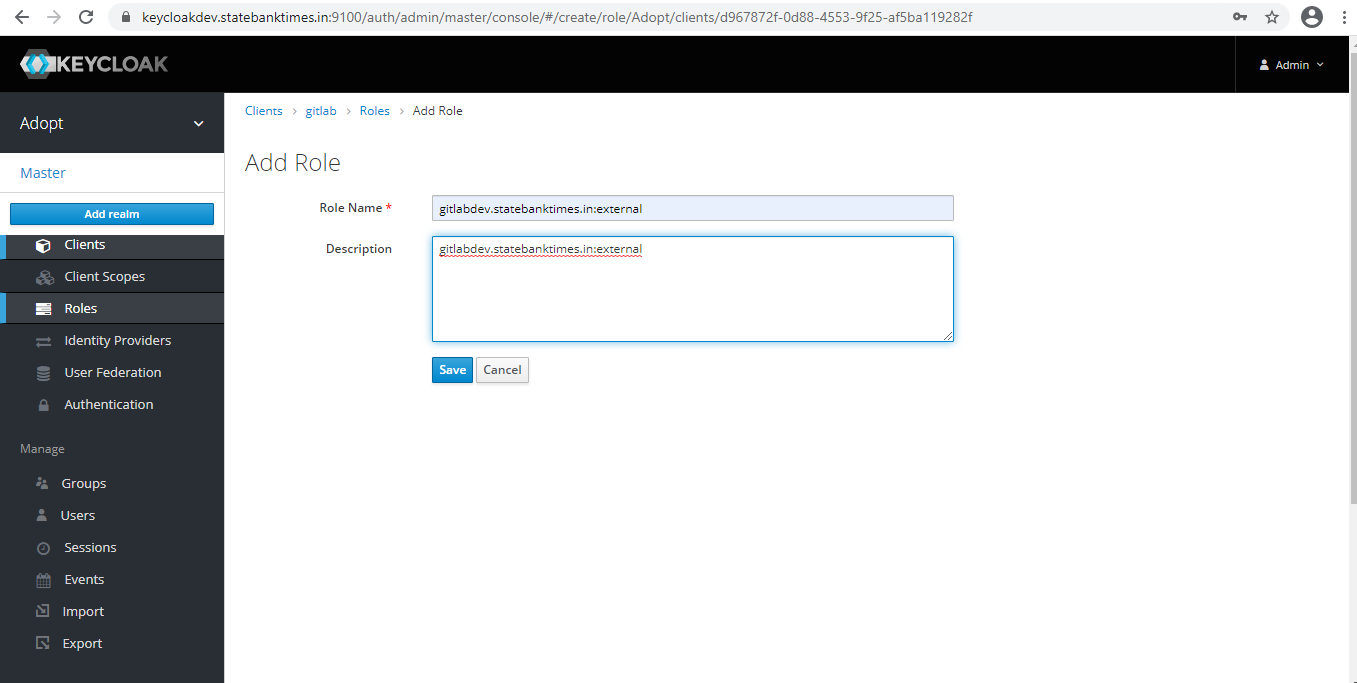
## Step 2 : Configure newly created SAML Client in Keycloak for Gitlab.

1. In Settings





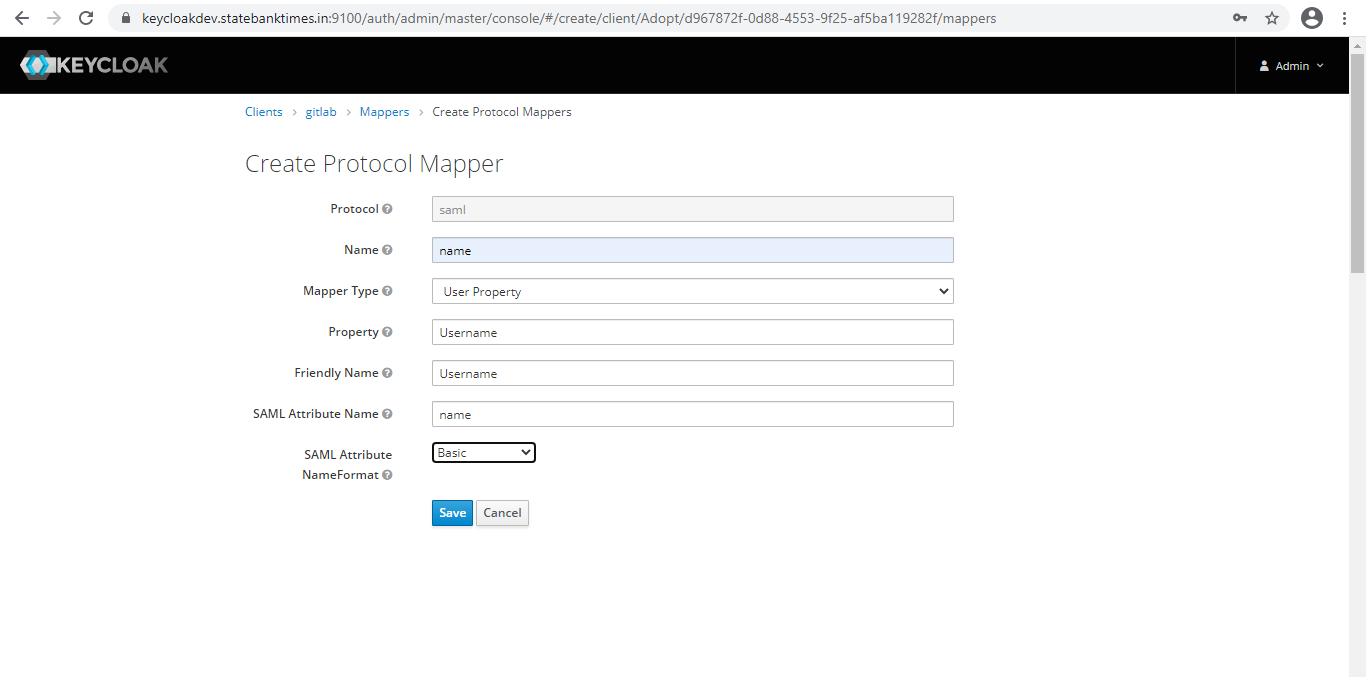
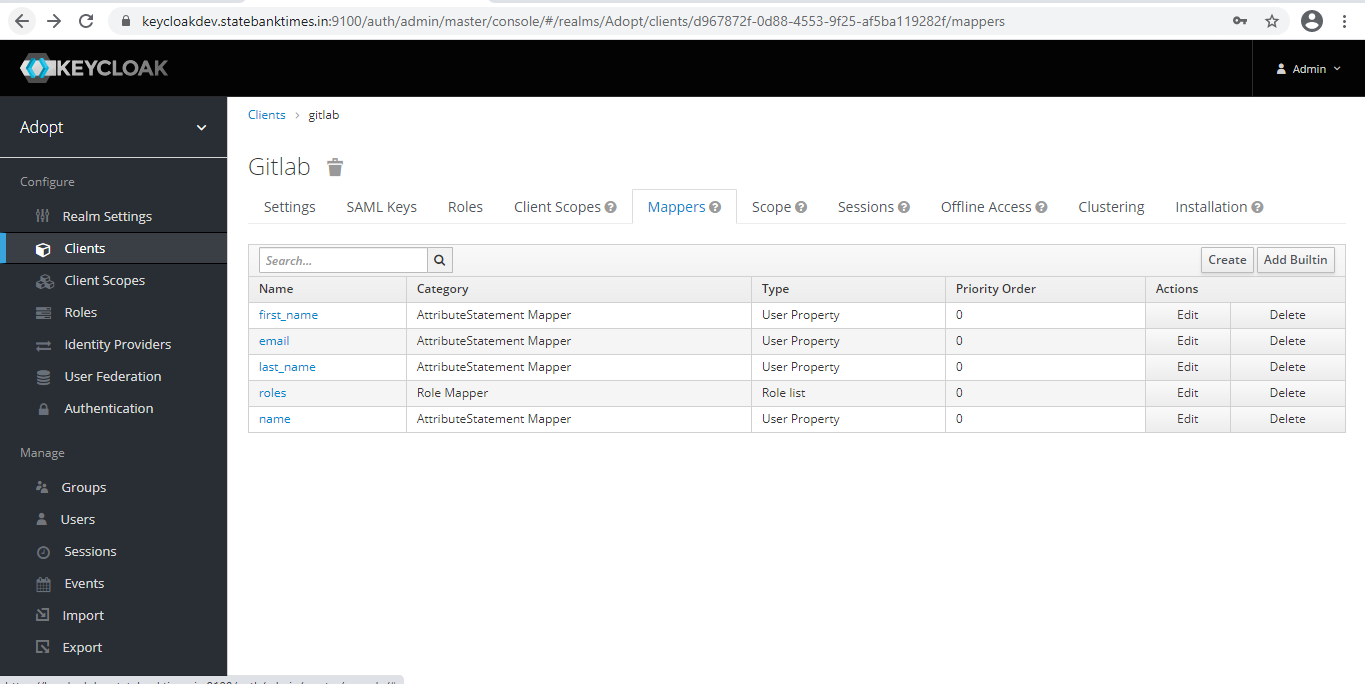
1. Roles Tab.



Gitlab CE users has limited functionality available with keycloak. We will create a group name external

in Keycloak for Gitlab.

1. Mappers Tab  
     
   Mappers allows you to map user information to parameters in the SAML 2.0 request for GitLab. For example a name mapper will be used to map the Username into the request for GitLab.  
     
   We will create few mappers for Gitlab in Keycloak.

Start with Name mapper.

Repeat the same process and create other mappers for email, first\_name, last\_name and roles as suggested below.

* 1. Name: name

Mapper Type: User Property

Property: Username

Friendly Name: Username

SAML Attribute Name: name

SAML Attribute Name Format: Basic

* 1. Name: email

Mapper Type: User Property

Property: Email

Friendly Name: Email

SAML Attribute Name: email

SAML Attribute Name Format: Basic

* 1. Name: first\_name

Mapper Type: User Property

Property: FirstName

Friendly Name: First Name

SAML Attribute Name: first\_name

SAML Attribute Name Format: Basic

* 1. Name: last\_name

Mapper Type: User Property

Property: LastName

Friendly Name: Last Name

SAML Attribute Name: name

SAML Attribute Name Format: Basic

* 1. Name: roles

Mapper Type: Role list

Role attribute name: roles

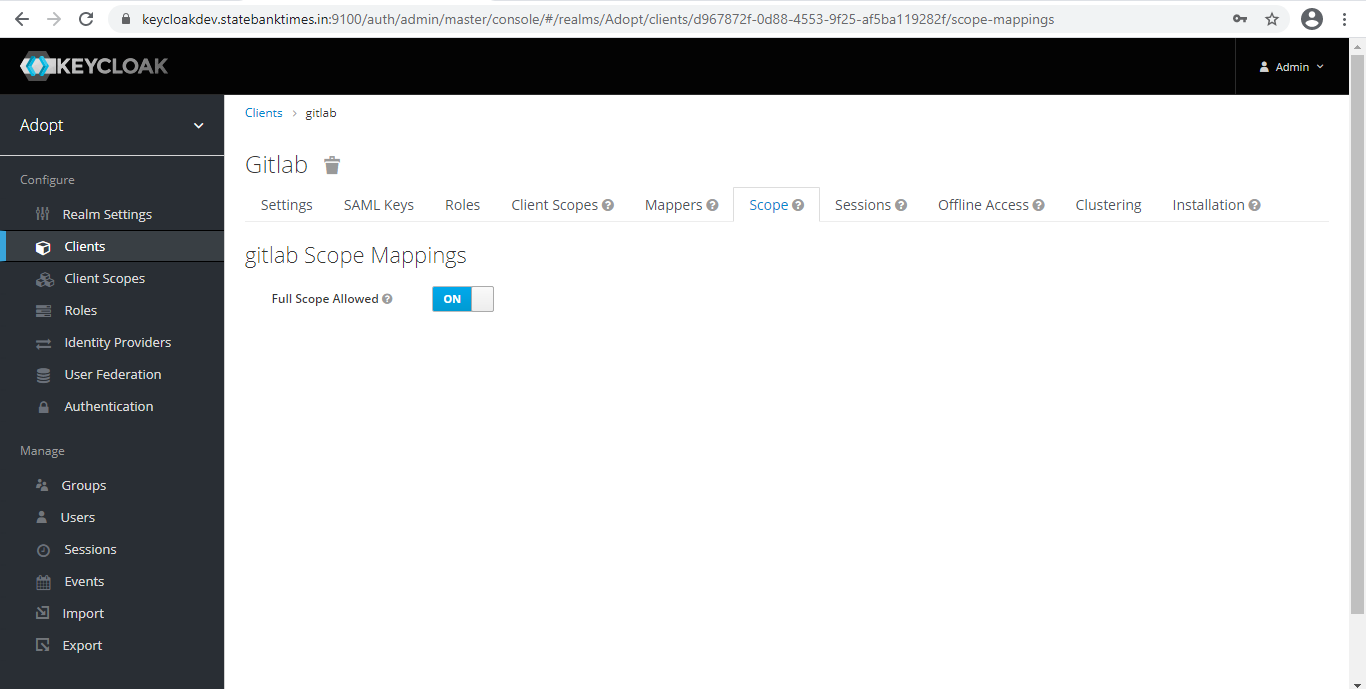
Friendly Name: Roles

SAML Attribute Name Format: Basic

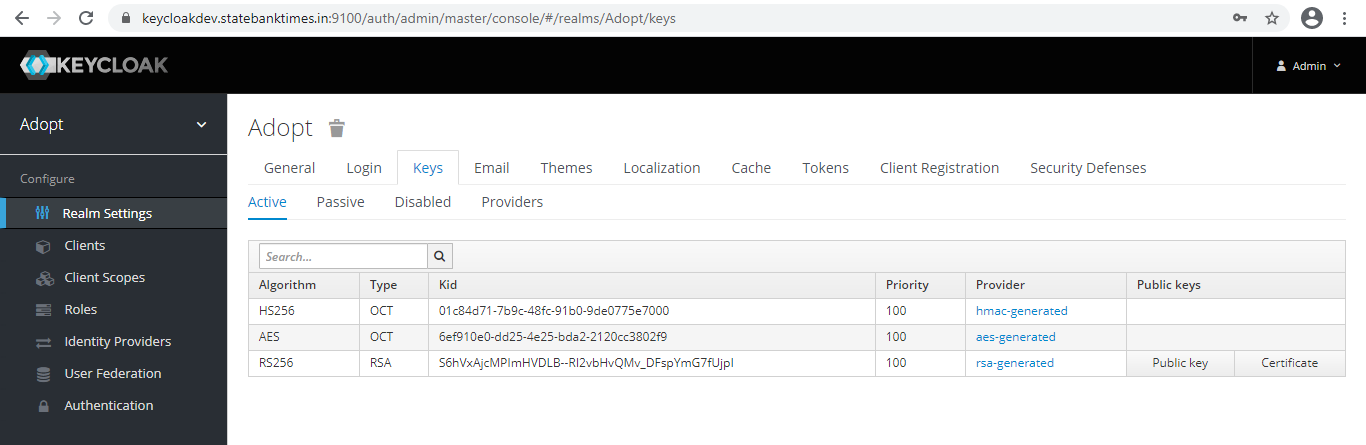
Single Role Attribute: On

All of the mappers have “Consent Required” set to Off.

End result should be like this.

1. Scope Tab.  
     
   Set full Scope Allowed to ON.  
   

## Step 3: Copy Certificate from Realm.

Go to Realm -> Keys and Download the public certificate.  


## Step 4: Setup Gitlab.

SSH into the gitlab server and take backup of gitlab.rb.  
cd /etc/gitlab/  
cp -a gitlab.rb{,.bak-working-$(date +%F)}  
  
Now open the gitlab.rb in vim or nano and paste the following lines at the end of file.  
  
gitlab\_rails['omniauth\_enabled'] = true

gitlab\_rails['omniauth\_allow\_single\_sign\_on'] = ['saml']

#gitlab\_rails['omniauth\_auto\_sign\_in\_with\_provider'] = 'saml'

gitlab\_rails['omniauth\_block\_auto\_created\_users'] = false

# gitlab\_rails['omniauth\_auto\_link\_ldap\_user'] = false

gitlab\_rails['omniauth\_auto\_link\_saml\_user'] = true

gitlab\_rails['omniauth\_providers'] = [

{

name: 'saml',

args: {

assertion\_consumer\_service\_url: 'https://gitlabdev.statebanktimes.in/users/auth/saml/callback',

idp\_cert: "",

idp\_sso\_target\_url: 'https://keycloakdev.statebanktimes.in:9100/auth/realms/Adopt/protocol/saml/clients/gitlabdev.statebanktimes.in',

issuer: 'gitlab',

name\_identifier\_format: 'urn:oasis:names:tc:SAML:2.0:nameid-format:persistent',

allowed\_clock\_drift: 180

},

label: 'Keycloak Login'

}

]

## Step 5: Reconfigure the Gitlab.

gitlab-ctl reconfigure  
After that you can go to your Gitlab server and just below the sing in tab you will have another option of  
  
Sign in with  
That’s all. We have properly configure gitlab with Keycloak. Thanks