Integration of Sonarqube with Key Cloak for SSO

|  |  |  |  |
| --- | --- | --- | --- |
| Documents Name | Version | Prepared By | Reviewed By |
| Integration of Sonarqube with Key Cloak | v.01 | Abhishek |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Contents

[1 Keycloak as a SAML Identity Provider 3](#_Toc61709711)

[1.1 Step 1 : In the Keycloak server, create a new SAML client 3](#_Toc61709712)

[1.2 Step 2 : Configure the new client 3](#_Toc61709713)

[1.3 Step 3 : In SonarQube, Configure SAML authentication 7](#_Toc61709714)

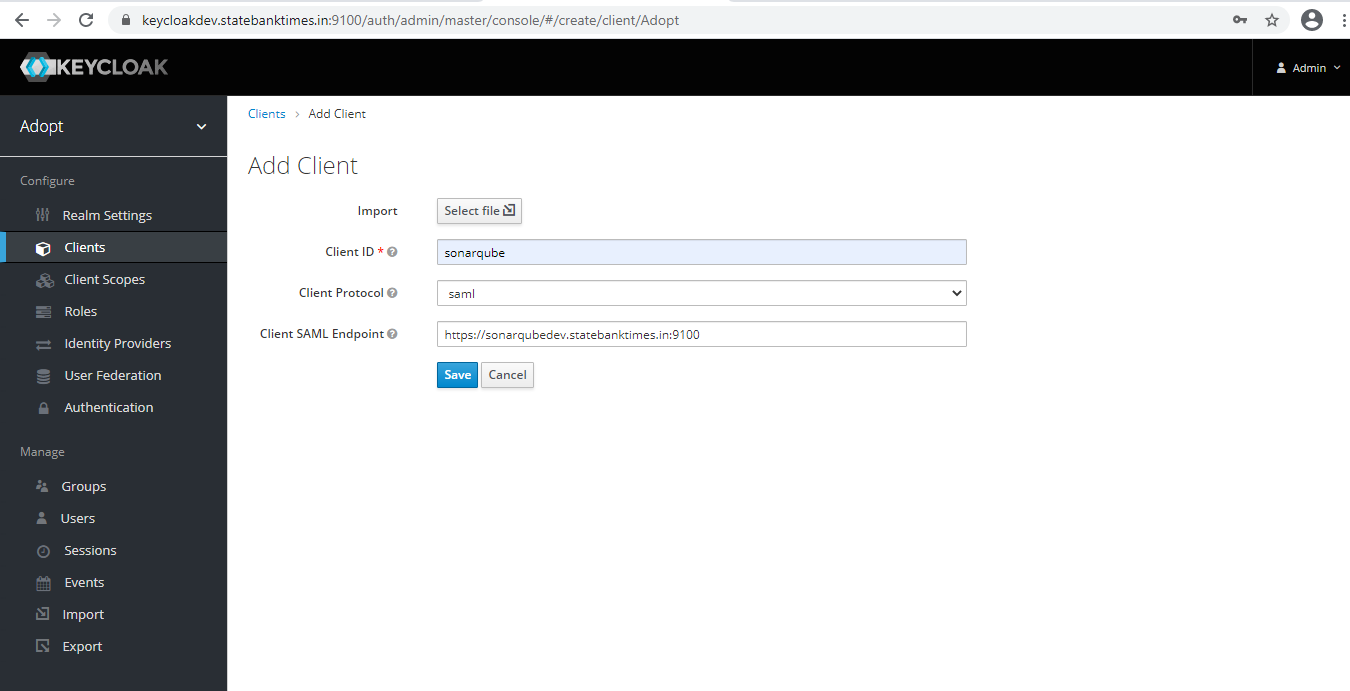
[1.4 Step 4 : In SonarQube, Configure General Setting 9](#_Toc61709715)

# Keycloak as a SAML Identity Provider

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

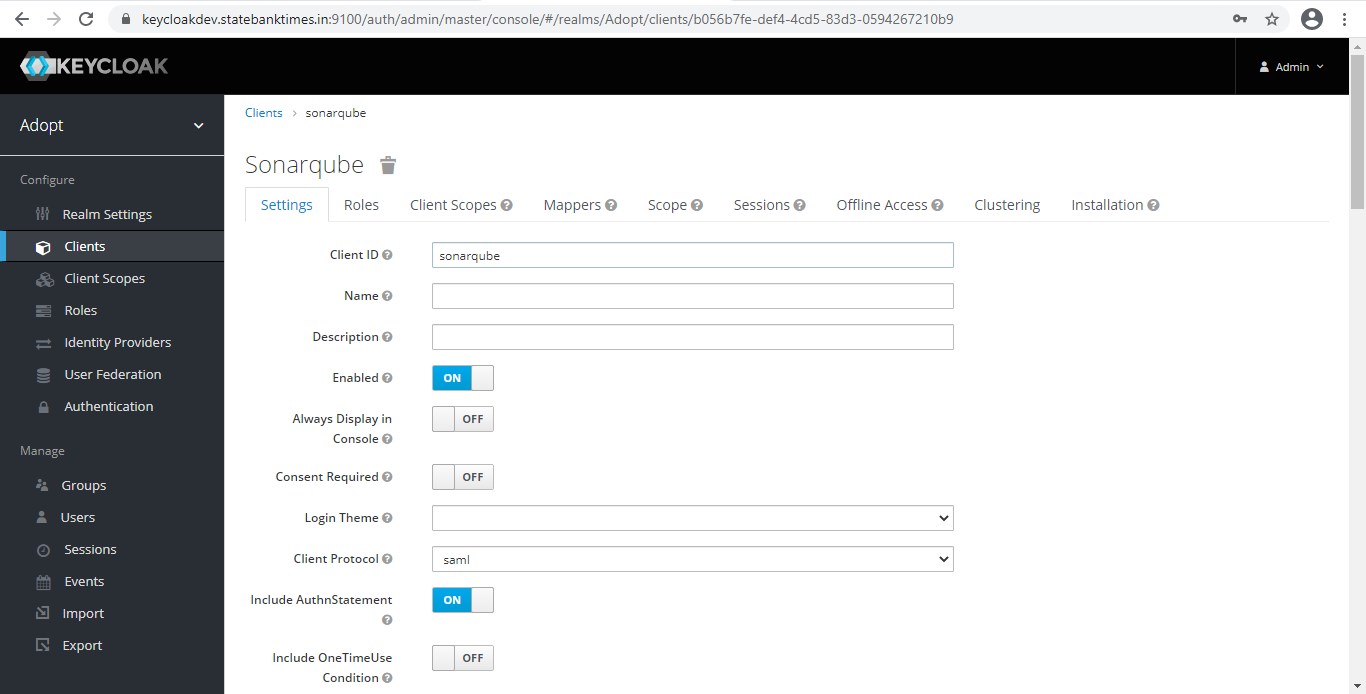
## Step 1 : [In the Keycloak server, create a new SAML client](https://docs.sonarqube.org/latest/instance-administration/delegated-auth/)

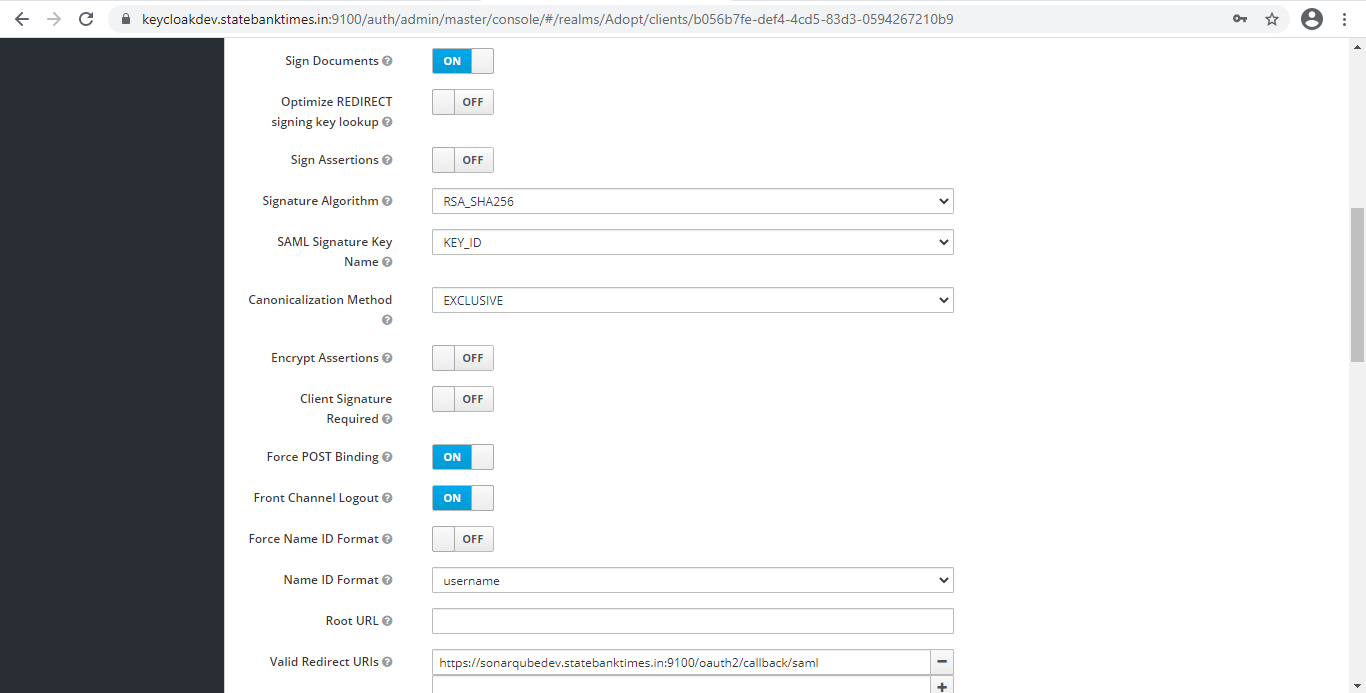
1. "Client ID" is something like "sonarqube"
2. "Client Protocol" must be set to "saml"
3. "Client SAML Endpoint" can be left empty

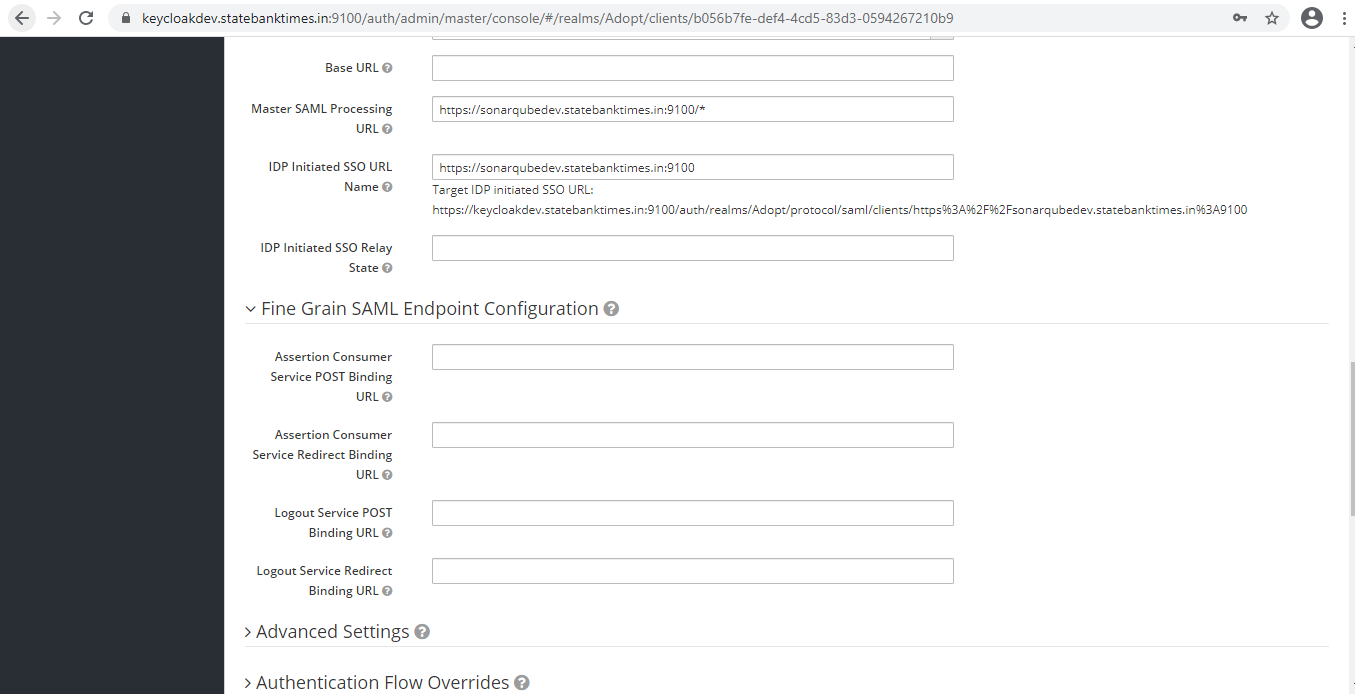


## Step 2 : Configure the new client

1. In Settings
   1. Set"Client Signature Required" to OFF
   2. Set "Valid Redirect URIs" to eg. <https://sonarqubedev.statebanktimes.in:9100/oauth2/callback/saml>



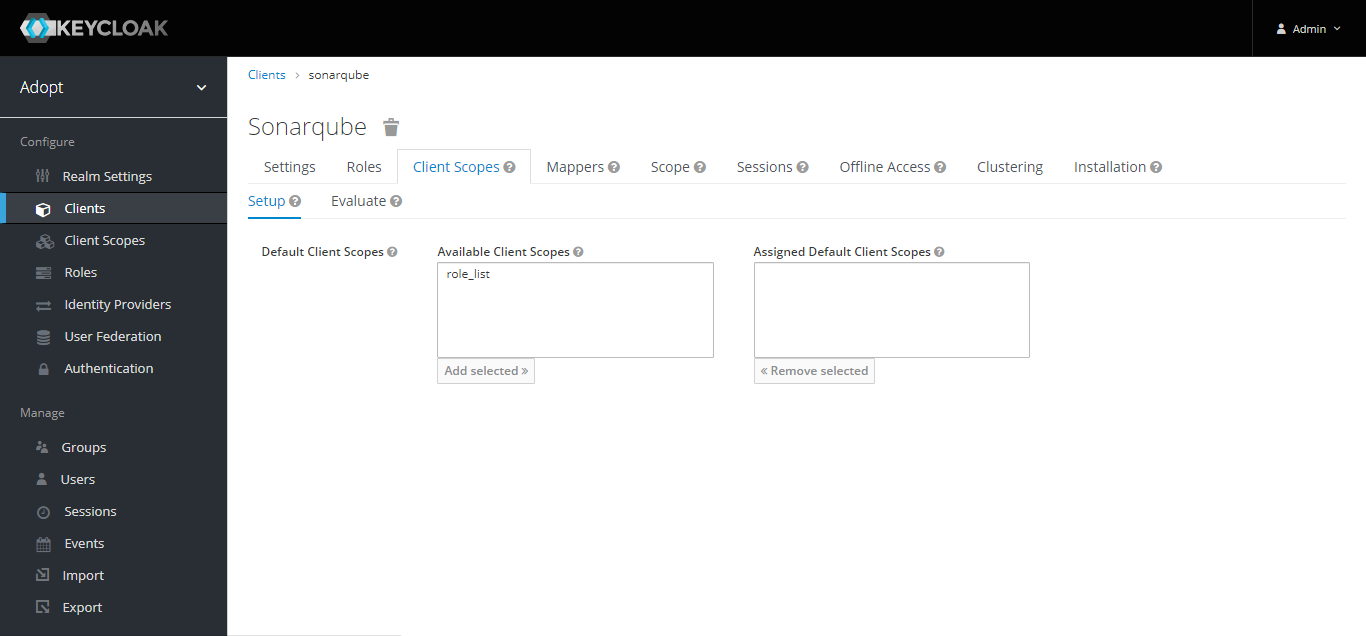




1. In Client Scopes

Default Client Scopes , remove "role\_list" from "Assigned Default Client Scopes"

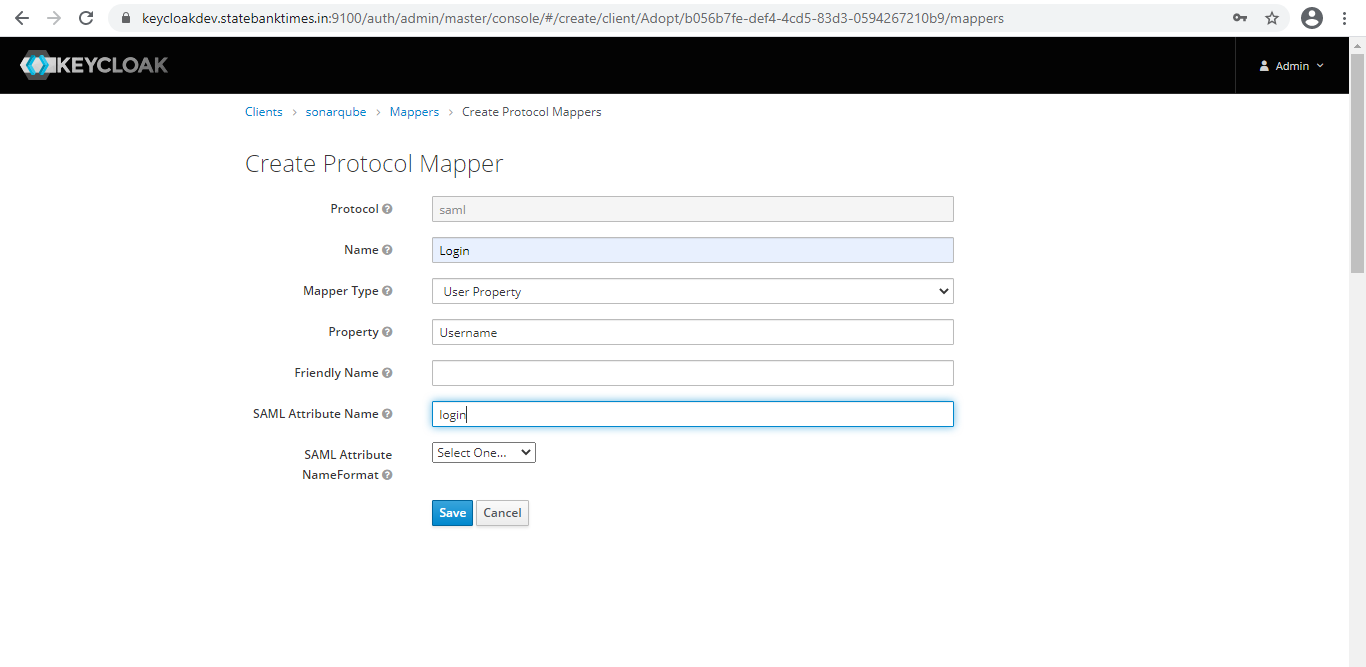
(to prevent the error com.onelogin.saml2.exception.ValidationError: Found an Attribute element with duplicated Name during authentication)

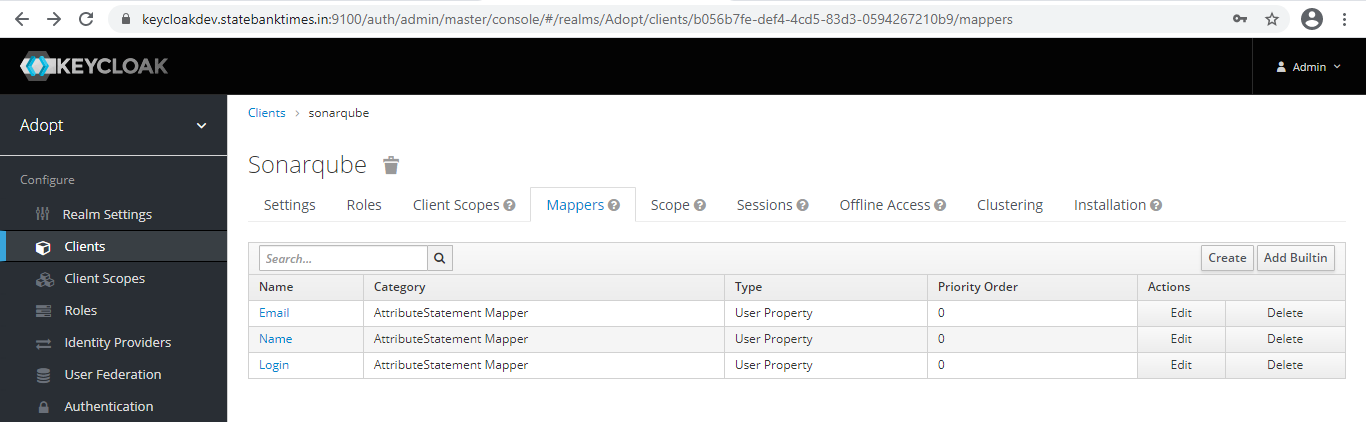


1. In Mappers

create a mapper for each user attribute

(Note that values provided below for Name, SAML Attribute Name, Role Attribute Name are only example values):



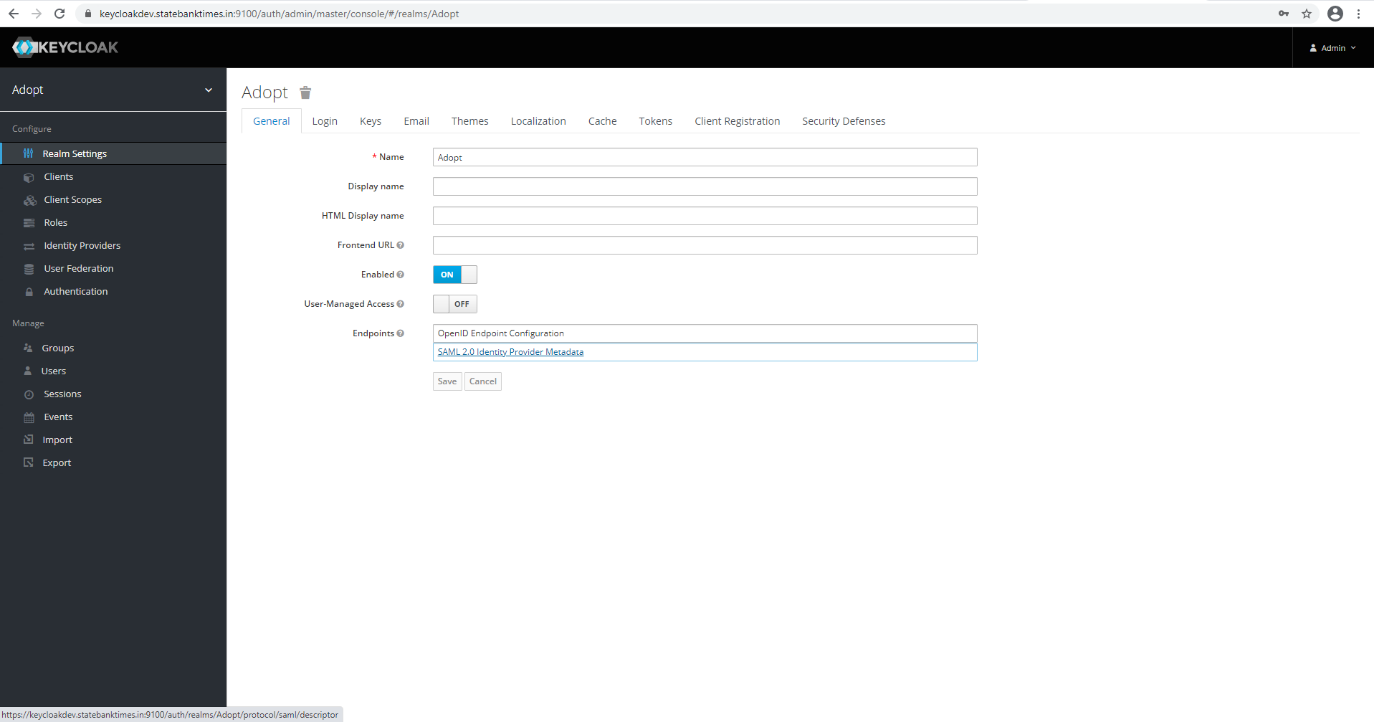


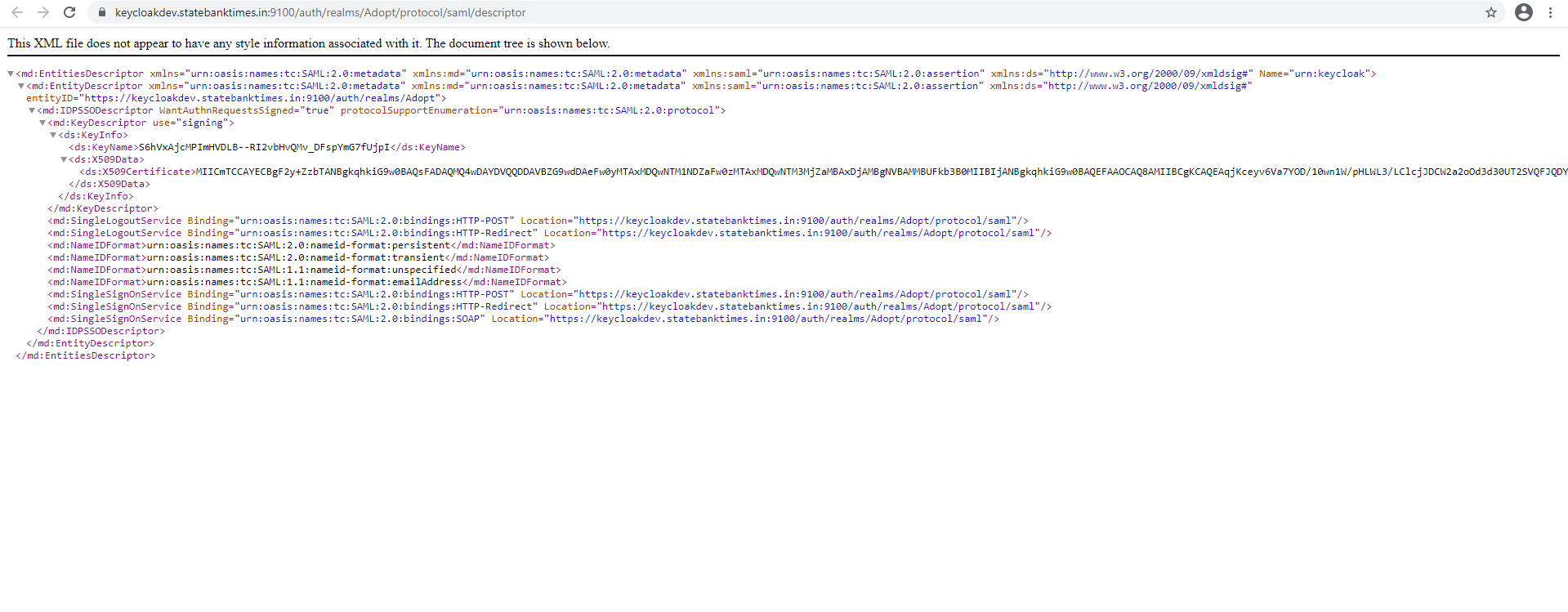
* 1. Create a mapper for the login:
* Name: Login
* Mapper Type: User Property
* Property: Username

(Note that the login should not contain any special characters other than .-\_@ to meet SonarQube restrictions.)

* SAML Attribute Name: login
  1. Create a mapper for the name:
* Name: Name
* Mapper Type: User Property
* User Attribute: Username (It can also be another attribute you would previously have specified for the users)
* SAML Attribute Name: name
  1. (Optional) Create a mapper for the email:
* Name: Email
* Mapper Type: User Property
* Property: Email
* SAML Attribute Name: email
  1. (Optional) Create a mapper for the groups (If you rely on a list of roles defined in "Roles" of the Realm (not in "Roles" of the client)):
* Name: Groups
* Mapper Type: Role list
* Role Attribute Name: groups
* Single Role Attribute: ON
  1. If you rely on a list of groups defined in "Groups":
* Name: Groups
* Mapper Type: Group list
* Role Attribute Name: groups
* Single Role Attribute: ON
* Full Group Path: OFF

1. Download the XML configuration file from Keycloak.



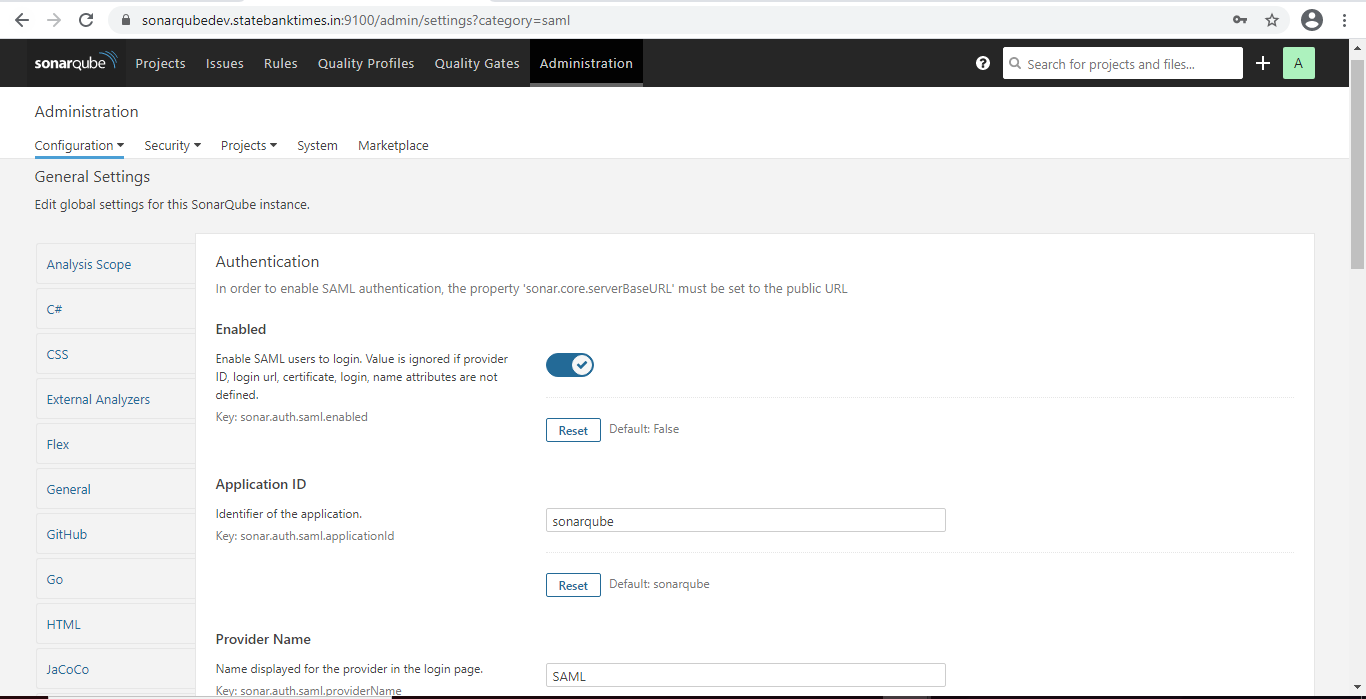


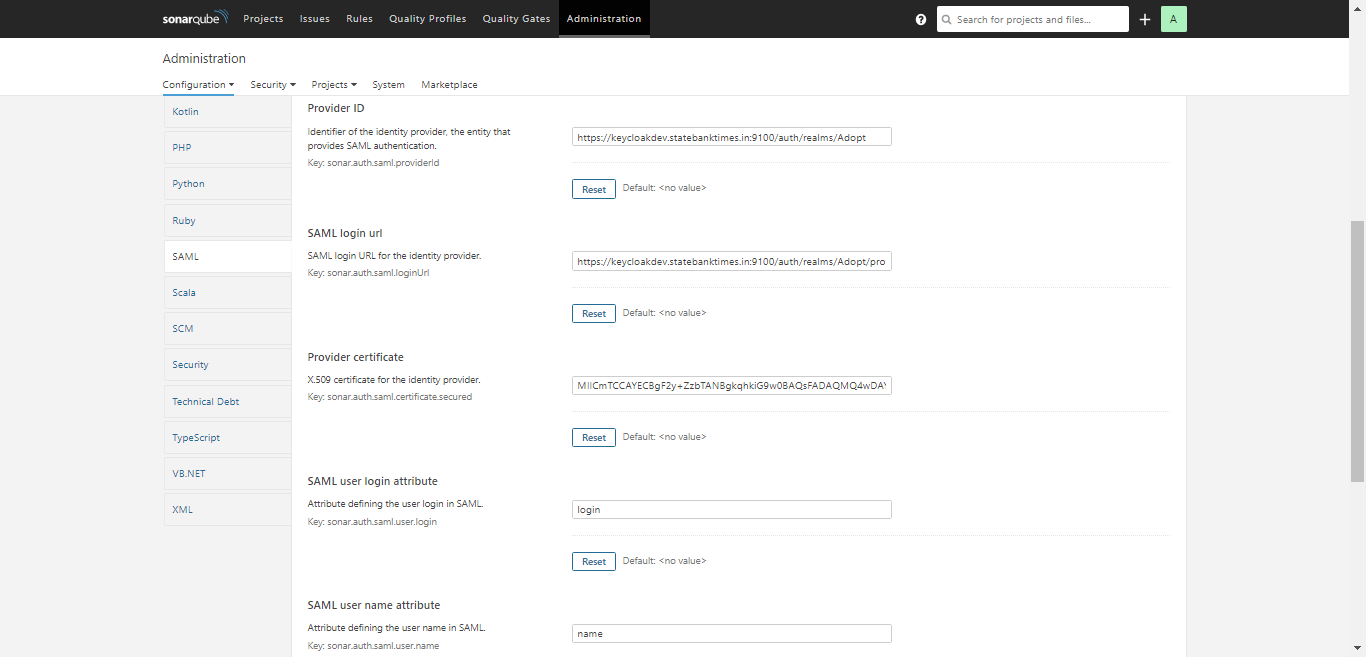
## Step 3 : [In SonarQube, Configure SAML authentication](https://docs.sonarqube.org/latest/instance-administration/delegated-auth/)

* 1. Go to Administration > Configuration > General Settings > Security > SAML
  2. Enabled should be set to true
  3. Application ID is the value of the "Client ID" you set in Keycloak (for example "sonarqube")
  4. Provider ID is the value of the "EntityDescriptor" > "entityID" attribute in the XML configuration file (e.g :"https://keycloakdev.statebanktimes.in:9100/auth/realms/Adopt" where Adopt is the name of the realm)
  5. SAML login url is the value of "SingleSignOnService" > "Location" attribute in the XML configuration file

(e.g :"[https://keycloakdev.statebanktimes.in:9100/auth/realms/Adopt/protocol/saml"](https://keycloakdev.statebanktimes.in:9100/auth/realms/Adopt/protocol/saml%22))

* 1. Provider certificate is the value you get from Reaml Settings -> Keys -> click on the Certificate button
  2. SAML user login attribute is the value set in the login mapper in "SAML Attribute Name"
  3. SAML user name attribute is the value set in the name mapper in "SAML Attribute Name"
  4. (Optional) SAML user email attribute is the value set in the email mapper in "SAML Attribute Name"
  5. (Optional) SAML group attribute is the value set in the groups mapper in "Role/Group Attribute Name"





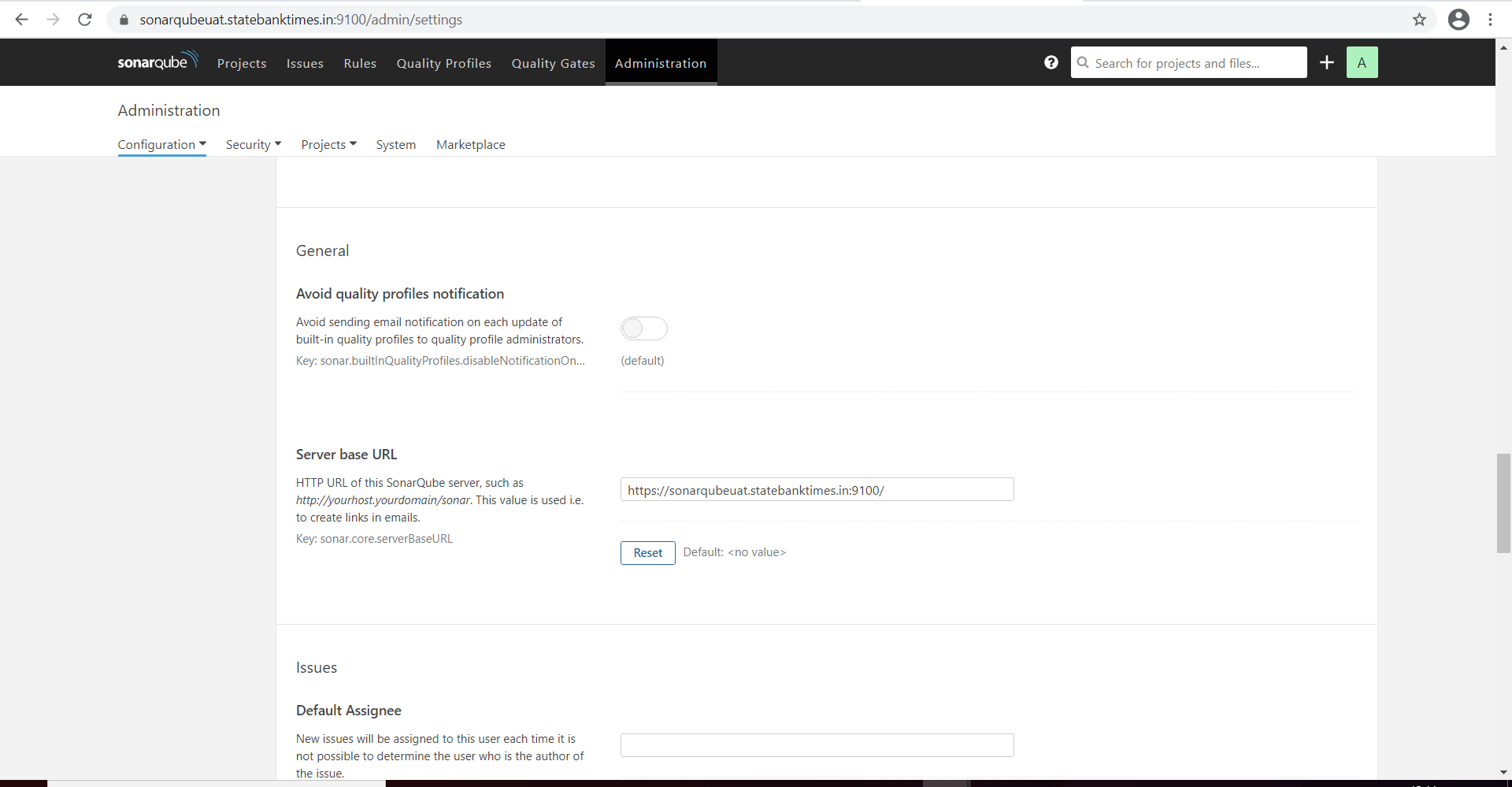
In the login form, the new button "Log in with SAML" allows users to connect with their SAML account.

* SAML and reverse proxy configuration

When using SAML, make sure your reverse proxy is properly configured.

## Step 4 : [In SonarQube, Configure](https://docs.sonarqube.org/latest/instance-administration/delegated-auth/) General Setting

Need to set Server Base URL

Go to Administration > Configuration > General Settings >

Limitations:

SAML requests are not signed. Client signature validation should be disabled in the Identity Provider.

SAML encrypted responses are not supported. SAML encryption should be disabled in the Identity Provider.