Integration of Keycloak with SBI SSO

**Version History**

|  |  |  |  |
| --- | --- | --- | --- |
| **Versions** | **Developed by** | **Reviewer-01** | **Reviewer-02** |
| v01 | Komal Ghonge | Sumit Malhotra | Nilesh Rane |
|  |  |  |  |
|  |  |  |  |

Table of Contents

[Setup Keycloak sever: 1](#_Toc61369855)

[Setup keycloak for incoming HTTPS connections. 1](#_Toc61369856)

[Step1: Configuration in ssl.conf 1](#_Toc61369857)

[Step 2: Configuration in standalone.xml file 2](#_Toc61369858)

[Setup identity provider in Keycloak: 2](#_Toc61369859)

[Setup basic properties of brokered identity provider. 2](#_Toc61369860)

[Setup Mappers. 4](#_Toc61369861)

[Obtain information for the ADFS configuration. 4](#_Toc61369862)

# Setup Keycloak sever:

## Setup keycloak for incoming HTTPS connections.

Step1: Configuration in ssl.conf

Go to below path and do some configuration in the given file.

vim /etc/httpd/conf.d/ssl.conf



<VirtualHost keyclockduat.statebanktimes.in:6565>

SSLEngine on

SSLProtocol all -SSLv2 -SSLv3

SSLCipherSuite HIGH:3DES:!aNULL:!MD5:!SEED:!IDEA

ProxyRequests Off

AllowEncodedSlashes NoDecode

ProxyPreserveHost On

ProxyPass / http://10.191.159.51:6565/ nocanon

ProxyPassReverse / http://10.191.159.51:6565/

SSLCertificateFile /opt/ssl\_cert/29122020/uatopsuat.statebanktimes.in.crt

SSLCertificateKeyFile /opt/ssl\_cert/29122020/uatopsuat.statebanktimes.in.key

RequestHeader set X-Forwarded-Proto "https"

</VirtualHost

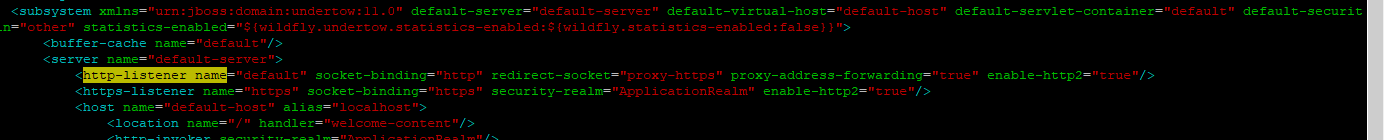
Step 2: Configuration in standalone.xml file

Get to below path and do change in standalone.xml file:

vim /opt/keycloak-12.0.1/standalone/configuration/standalone.xml

<http-listener name="default" socket-binding="http" redirect-socket="https" enable-http2="true"/>

<https-listener name="https" socket-binding="https" security-realm="ApplicationRealm" enable-http2="true"/>



After that start the apache web server

Systemctl start httpd

# Setup identity provider in Keycloak:

## Setup basic properties of brokered identity provider.

In the identity providers, create a new SAMl v2.0 identity provider, the identity provider will be known under alias adfs-idp-alias.

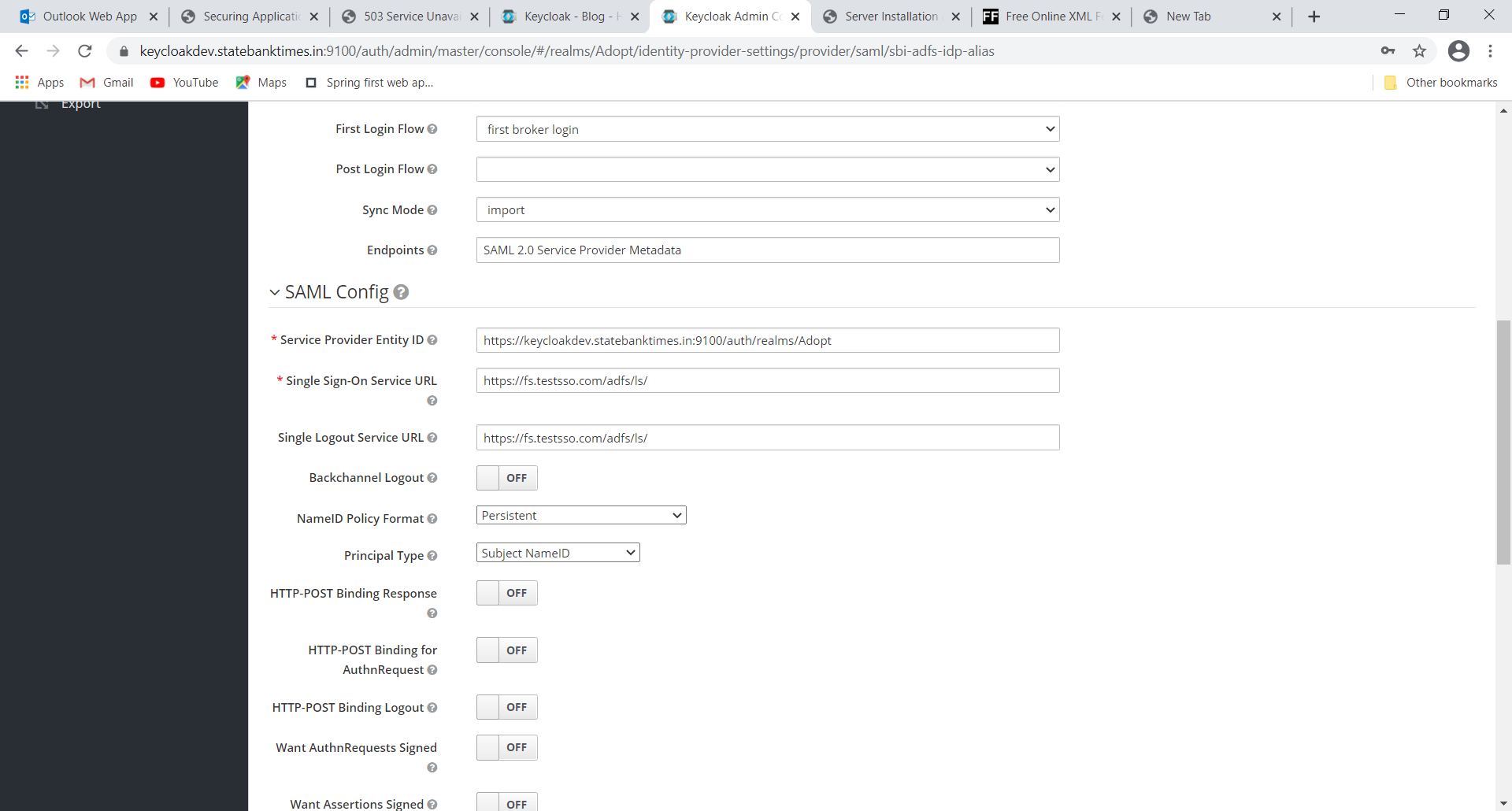
Scroll to the bottom and enter the AD FS descriptor URL into Import from URL field. For AD FS 3.0, this URL is https://fs.domain.name/FederationMetadata/2007-06/FederationMetadata.xml. Once you click “Import”, check the settings.

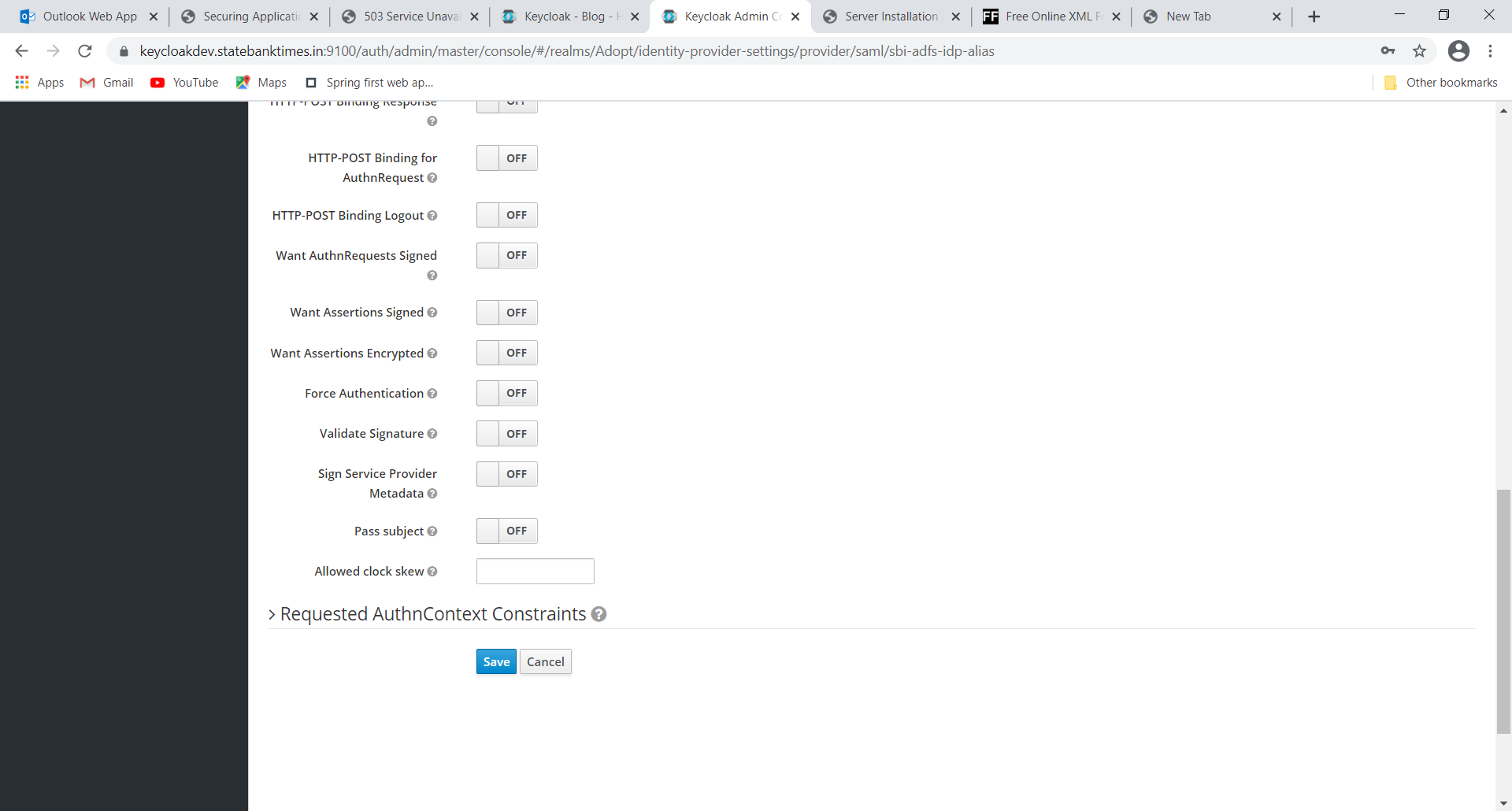
In our case, the URL was

<https://fs.testsso.com/FederationMetadata/2007-06/FederationMetadata.xml>

Once you click “Import”, check the settings.

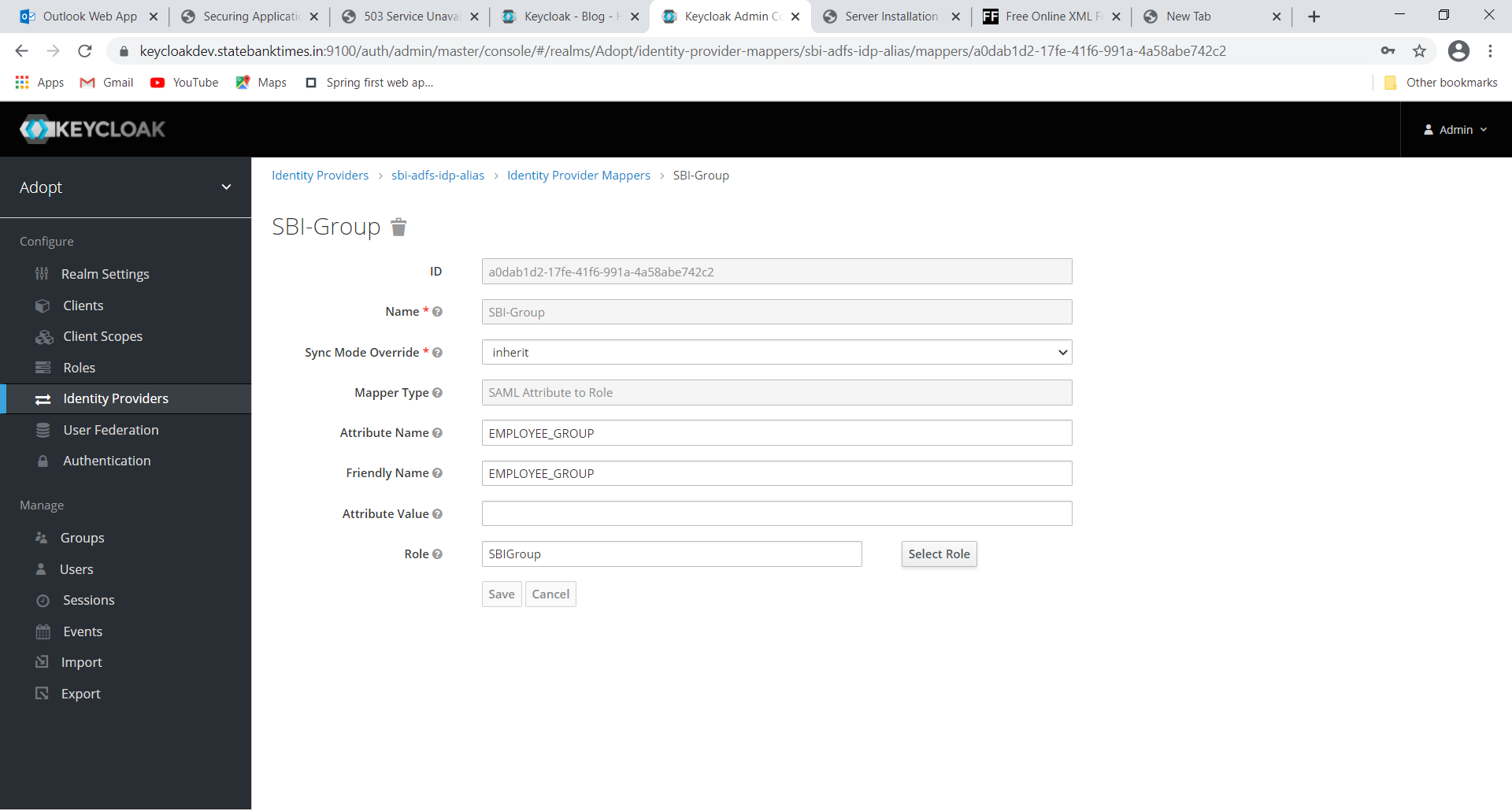
Please find the screenshot below.

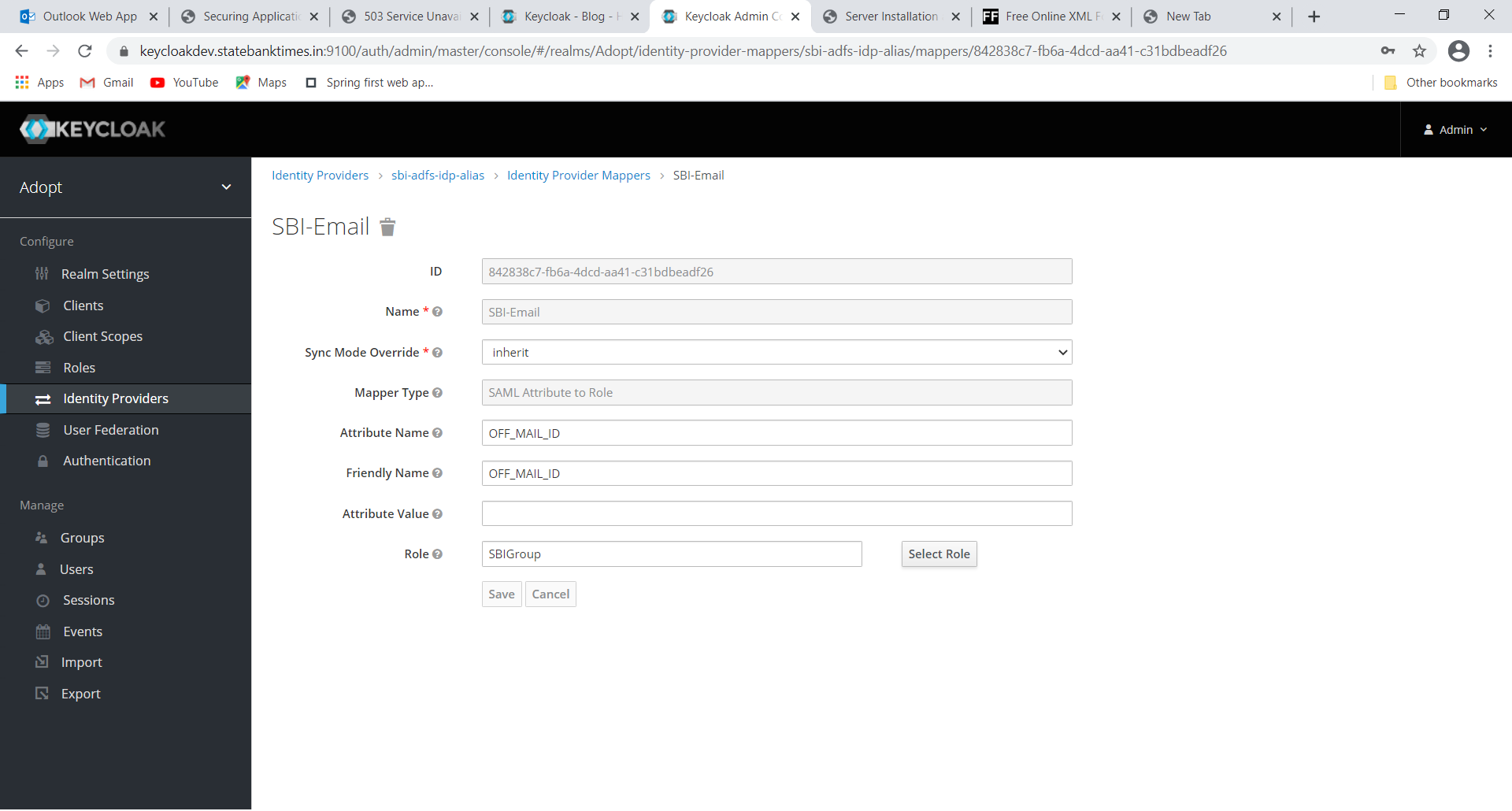




## Setup Mappers.

Please find the screenshot below.





## Obtain information for the ADFS configuration.

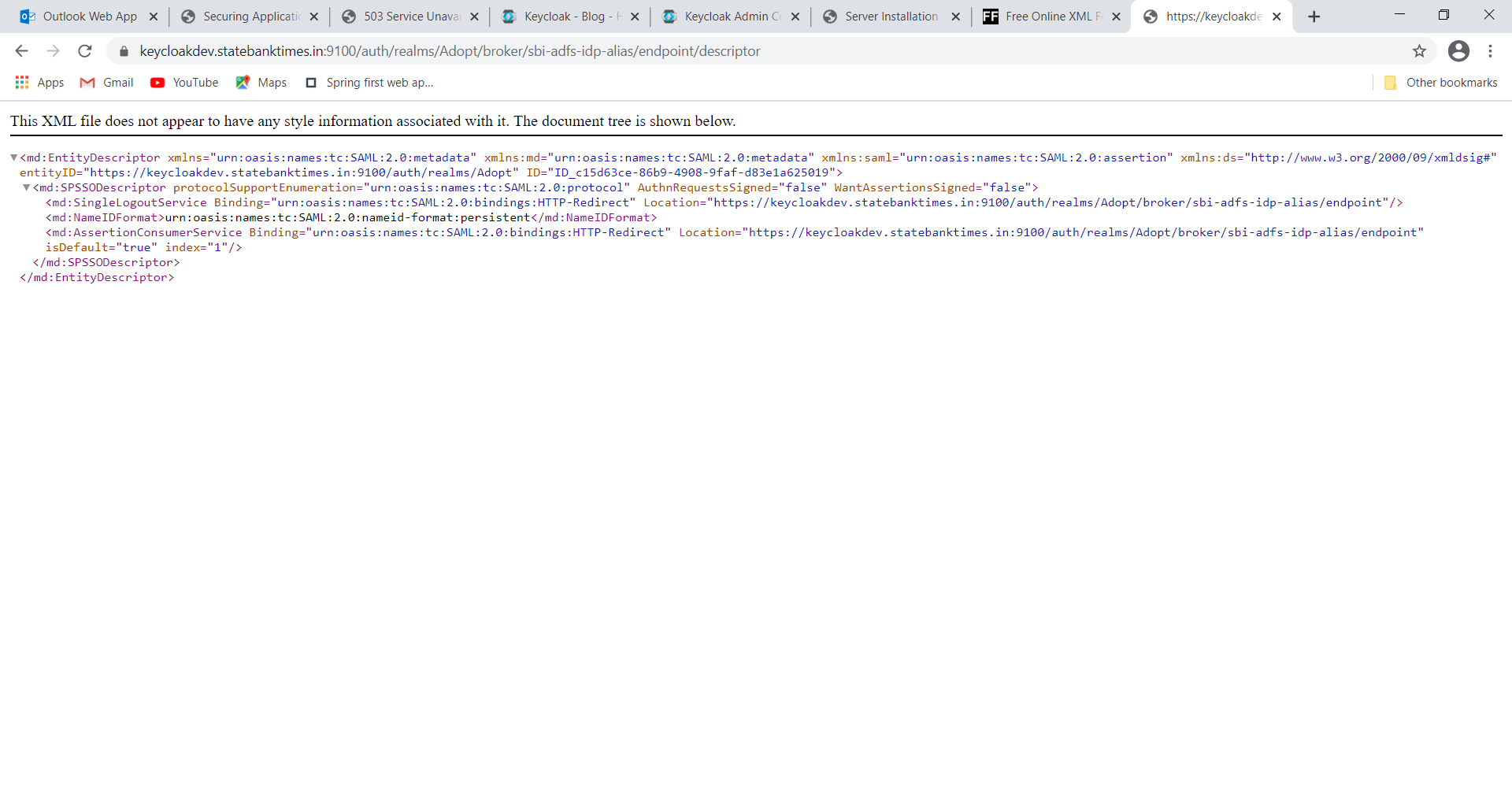
Now we determine SAML service provider descriptor URI that will be used in AD FS setup from the Redirect URI field in the identity provider detail by adding “/descriptor” to the URI in this field. The URI will be similar to <https://kc.domain.name:8443/auth/realms/master/broker/adfs-idp-alias/endpoint/descriptor>.

In our case the URI is

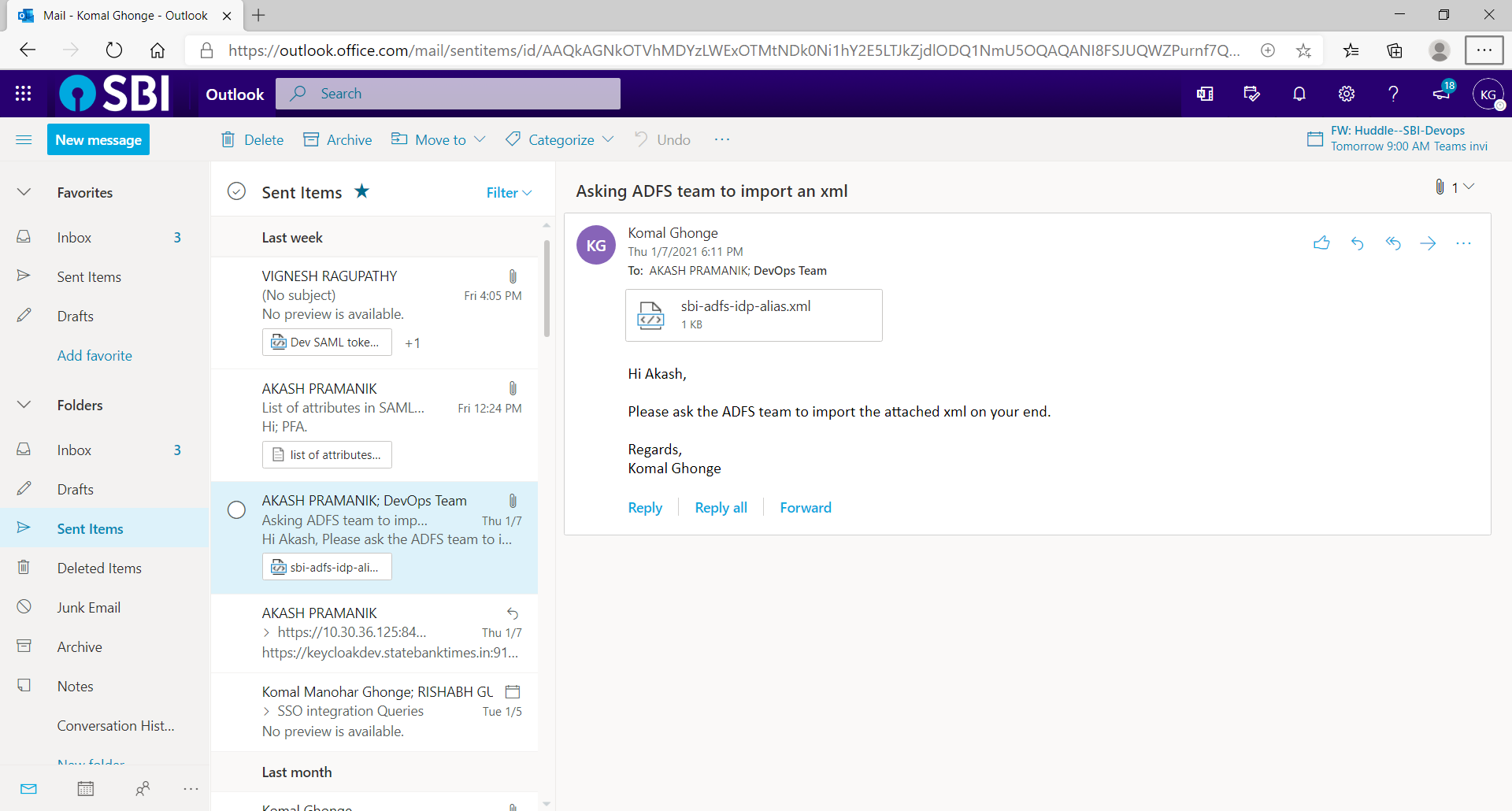
https://keycloakdev.statebanktimes.in:9100/auth/realms/Adopt/broker/sbi-adfs-idp-alias/endpoint

You can check whether you got the URI right by entering the URI into the browser - you should receive a SAML service provider XML descriptor.

Please find the screenshot below.



This xml file is named as sbi-adfs-idp-alias. Send this file to ADFS team to get it imported from their end.



**Note**: We had asked SSO team to register the URLs below.

<https://keycloakdev.statebanktimes.in:9100/> (Keycloak’s URL on DEV environment)

<https://devopsdev.statebanktimes.in:9090> (ADOPT’s URL on DEV environment)