**POLICIES**

**POLICY:** Policies check identities for certain conditions that are unwanted of even considered dangerous. Such a condition can be a set of roles that should not be combined in a single identity (e.g. “payment preparation” and “payment approval”), two conflicting values of a multi-valued attribute.

Types of policies are:

1.Role SOD Policy

2.Entitlement SOD Policy

3.Effective Entitlement SOD Policy

4.Activity Policy

5.Account Policy

6.Risk Policy

7.Advanced Policy

**Role SOD Policy**: This policy type checks for any conflicting roles that an identity could have. The policy rules define two lists (“left” and “right”), where any rule from the “left side” list cannot be combined with any rule from the “right side” list.

**Entitlement SOD Policy**: This policy type checks for conflicting entitlements within an application or across applications. This is quite similar to the Role SOD Policy, but for values of application attributes marked as entitlement in the application schema

**Activity Policy: An** activity policy scans activity data for specific events, with the option to select time frames, source and target applications. We can specify list of filters those filters enables us to identify the types of identities that should be considered when scanning activities for violations.

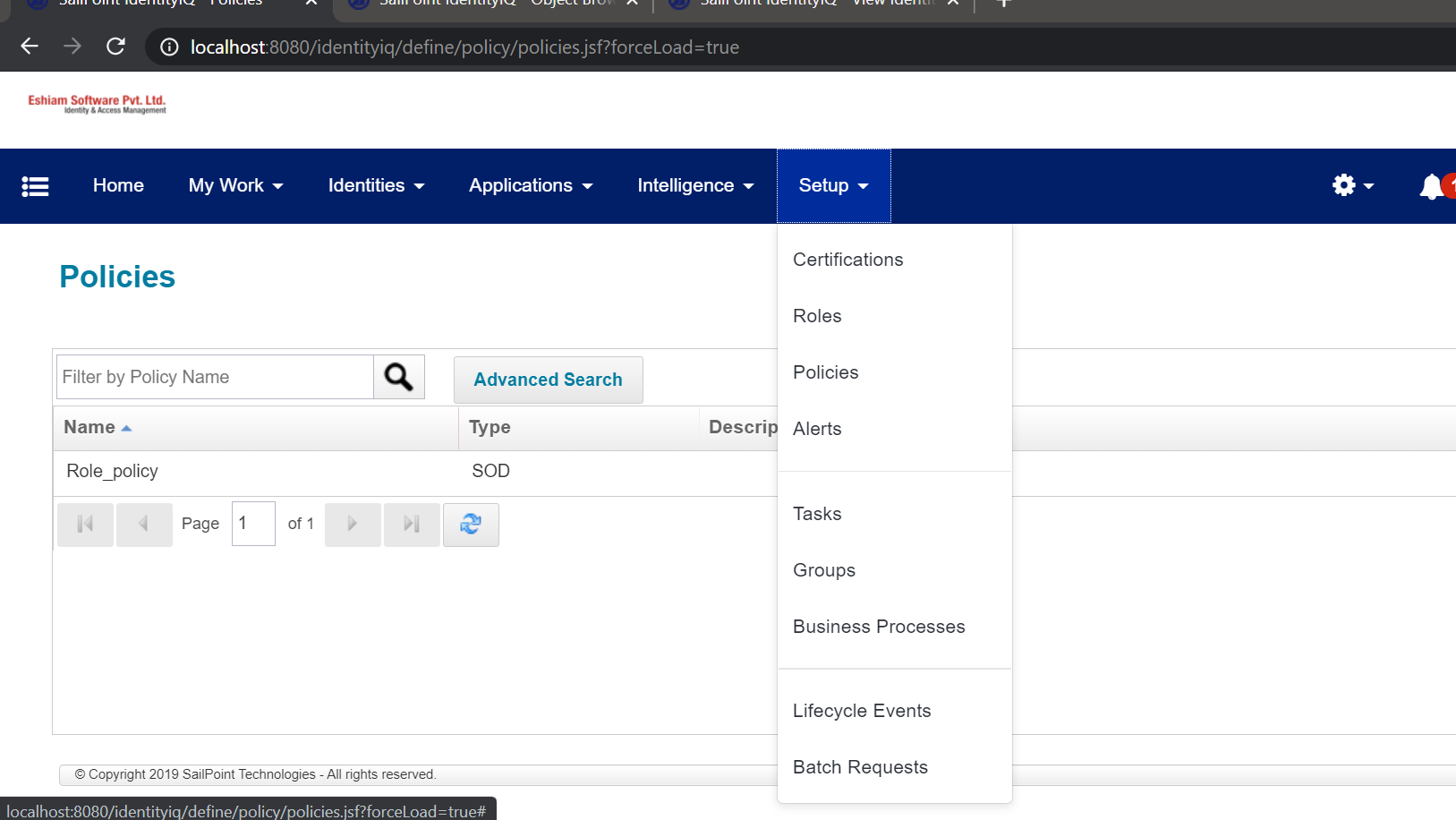
**Account policy:** Account policies only have a single policy rule: they simply check whether an identity has multiple accounts on an application.

**Advanced Policy:**An advanced policy handles situation where the other types do not sufficient. The advanced policy can contain multiple types of rules which allows for greater flexibility.

Here we r concentrating on Entitlement SOD Policy.

**Example of Entitlement SOD Policy:**

**On home page click on setup-->policies.**



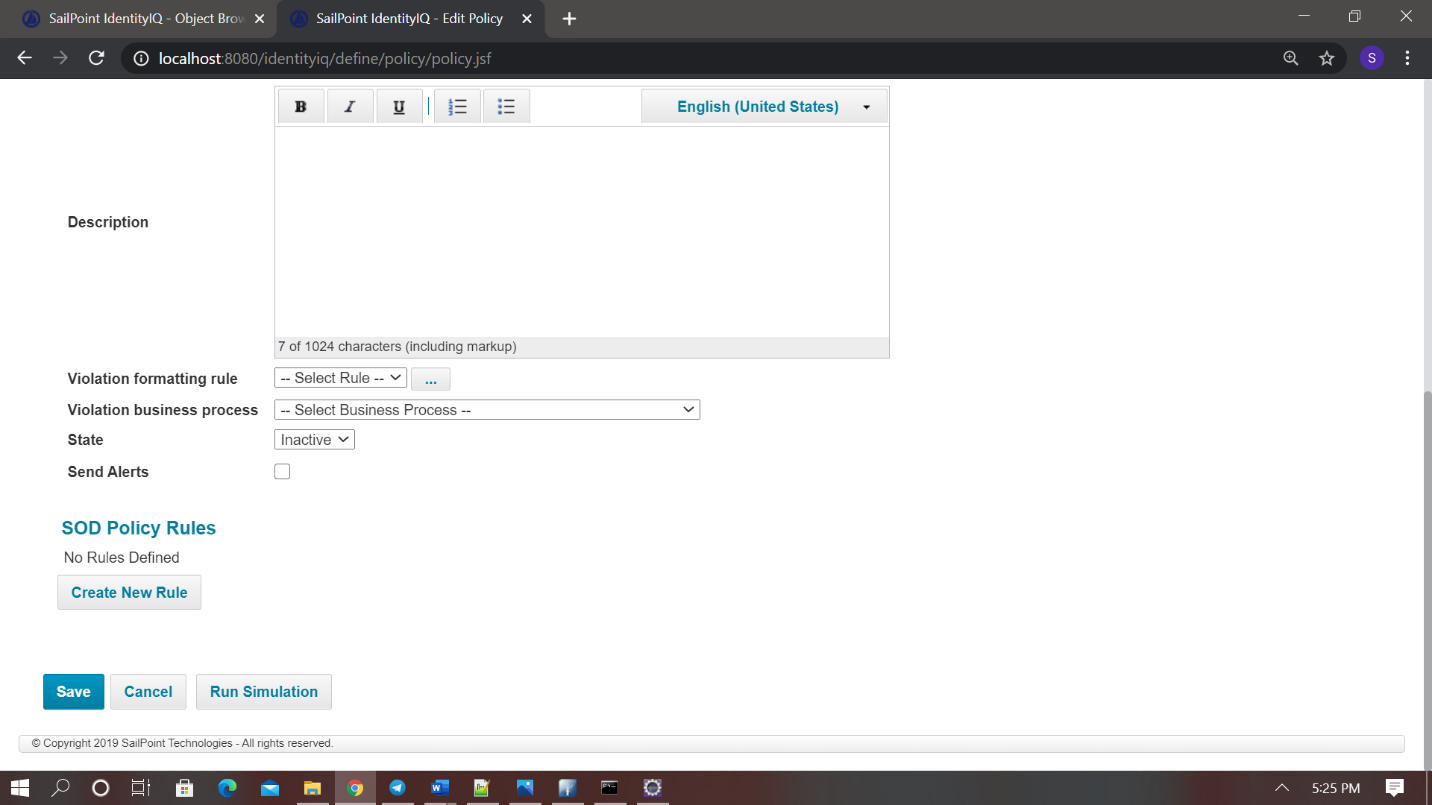
Click on New Policy-->Entitlement SOD Policy

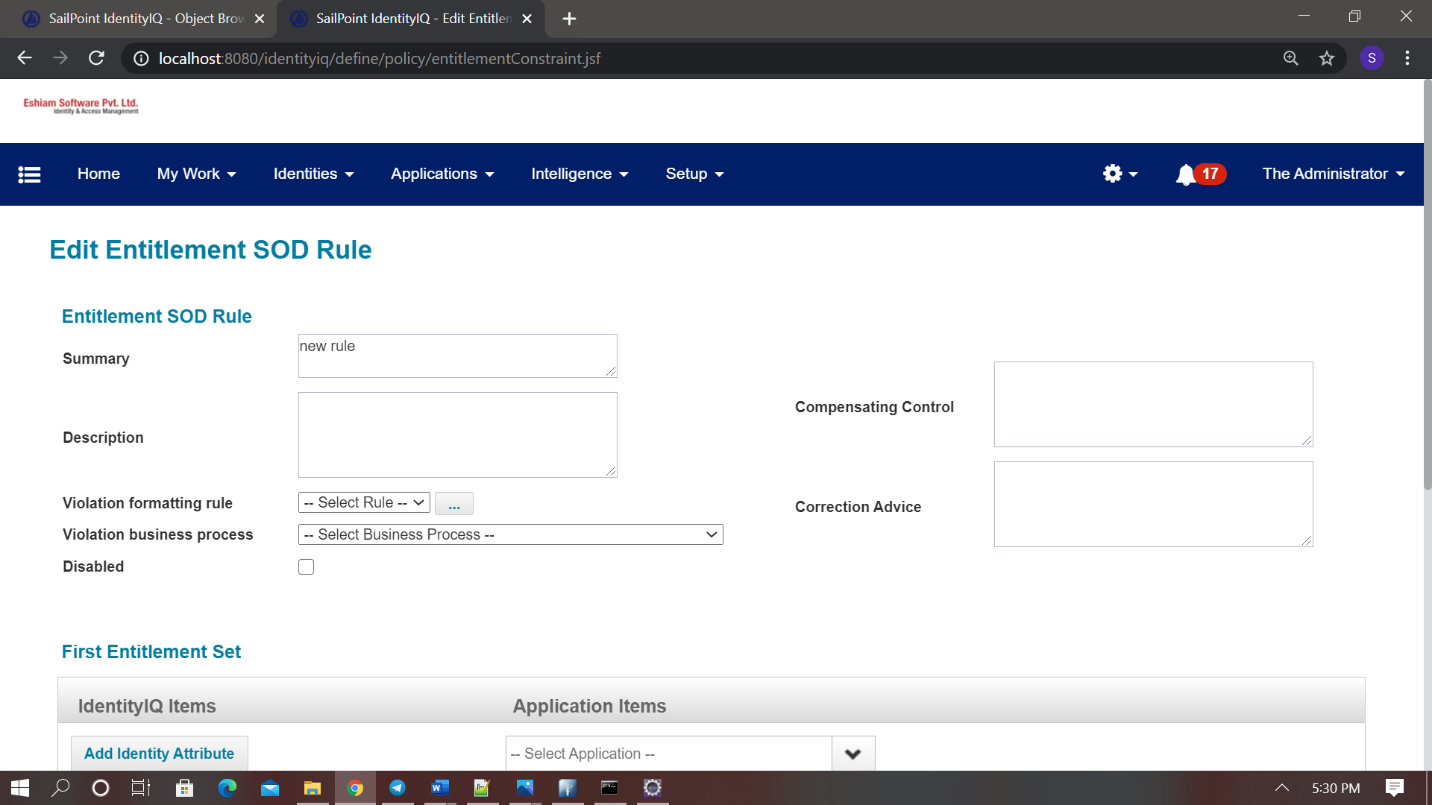
Give any name to the Policy.

Here Status should be **ACTIVE.**

**In SOD policy Rules click on create new rule.**

We will get another page.





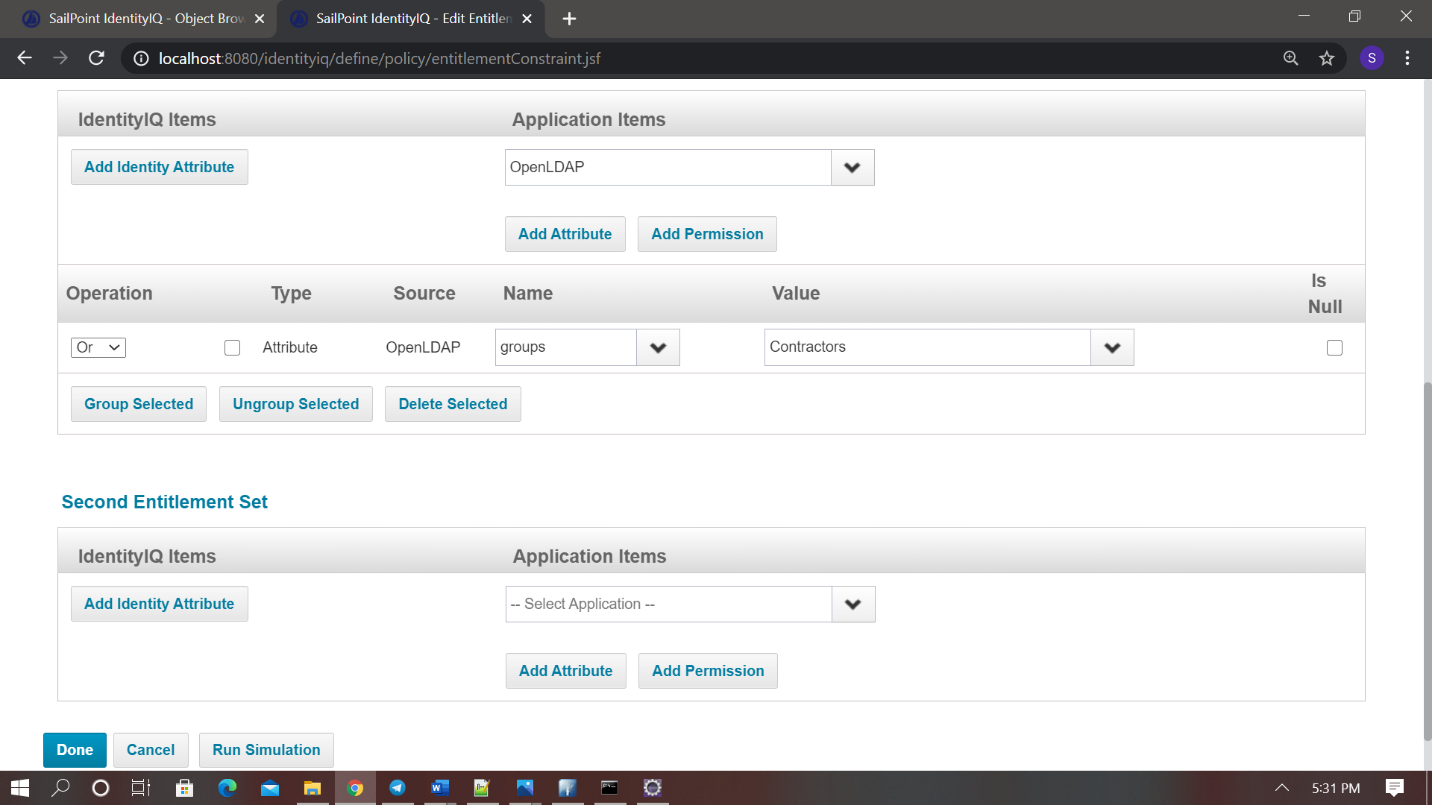
In First Entitlement Set select Application in Application Item.

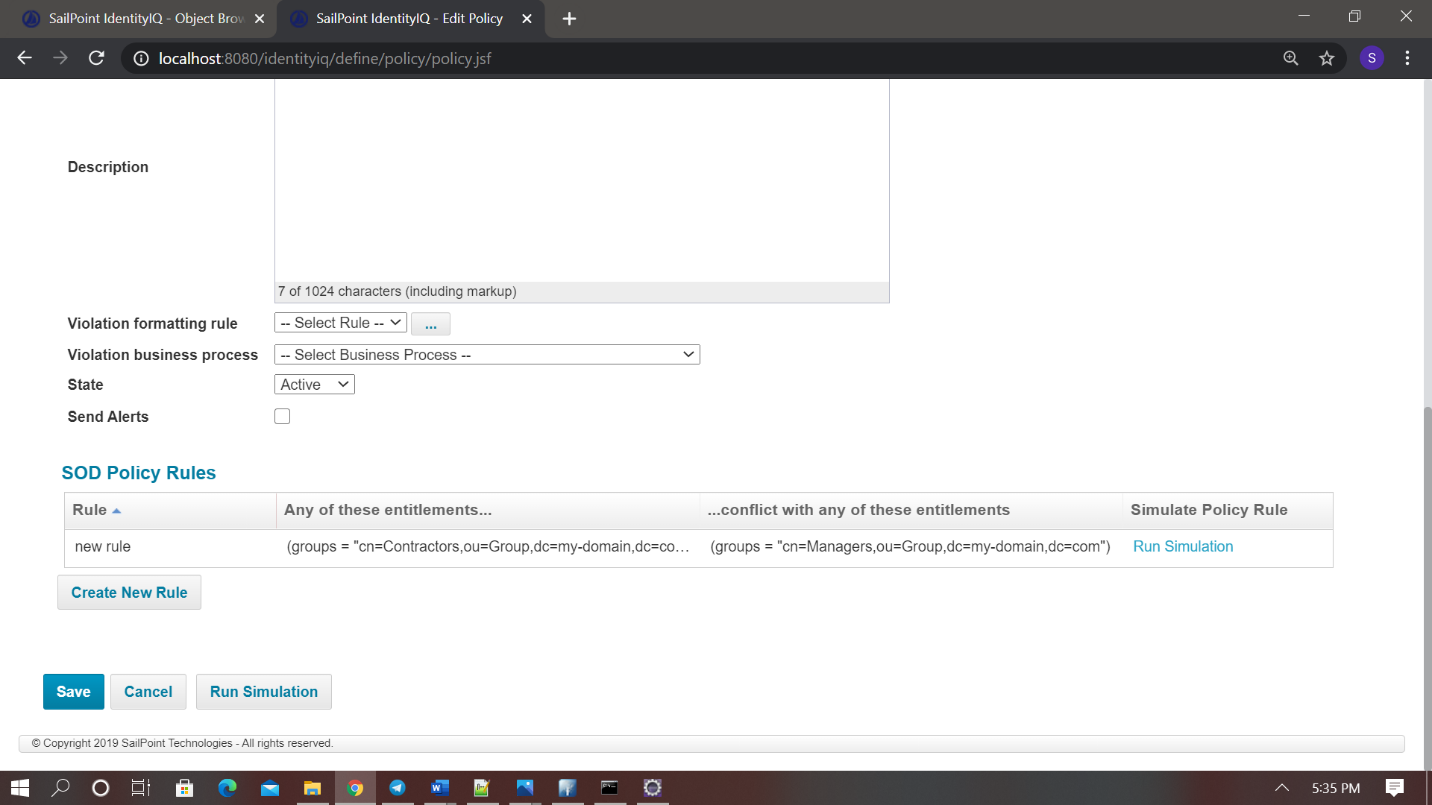
Click on Add Attribute like below.

Then in Second Entitlement Set select Application in Application Item.

Select attributes like above set.

Then click on done.

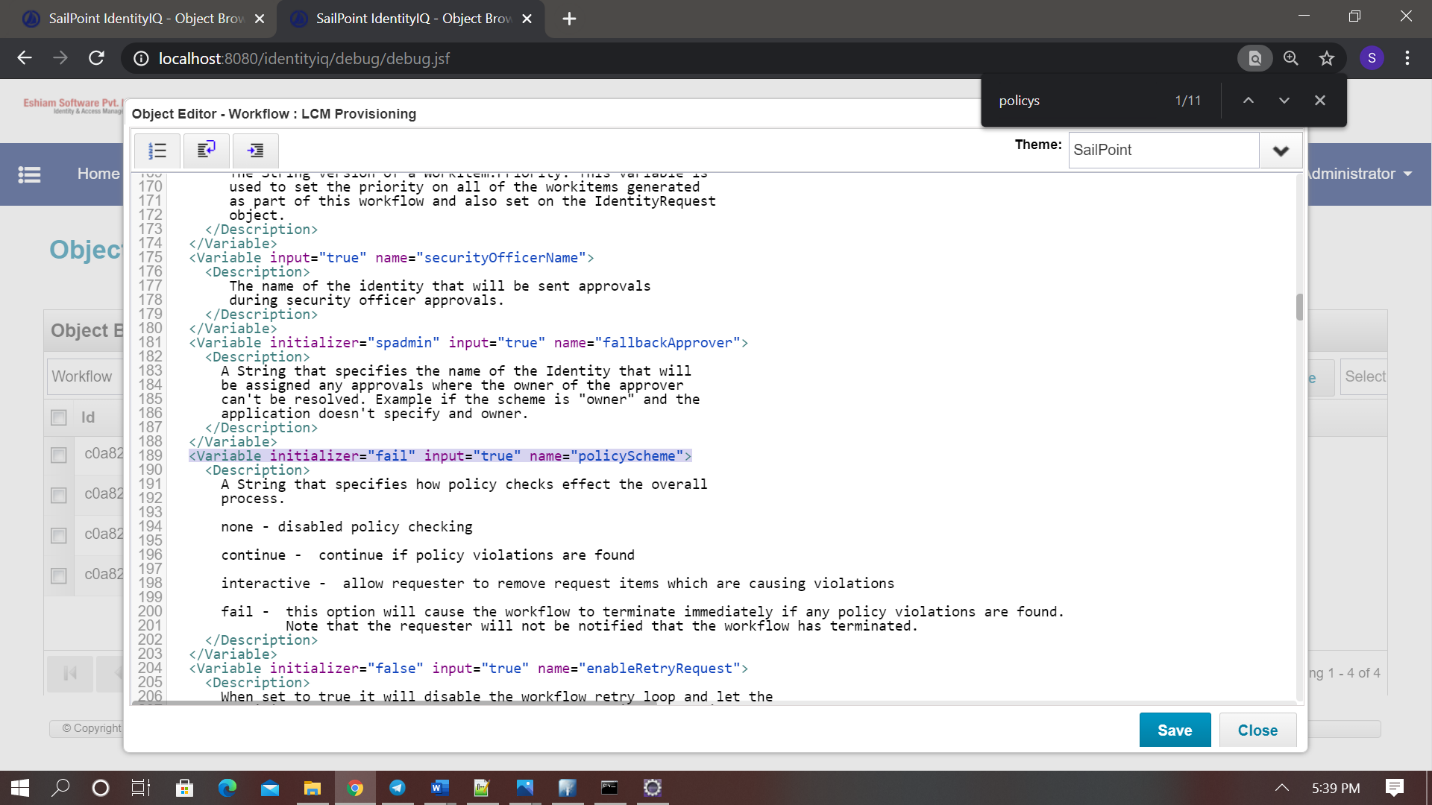




Just like above picture.

Then save.

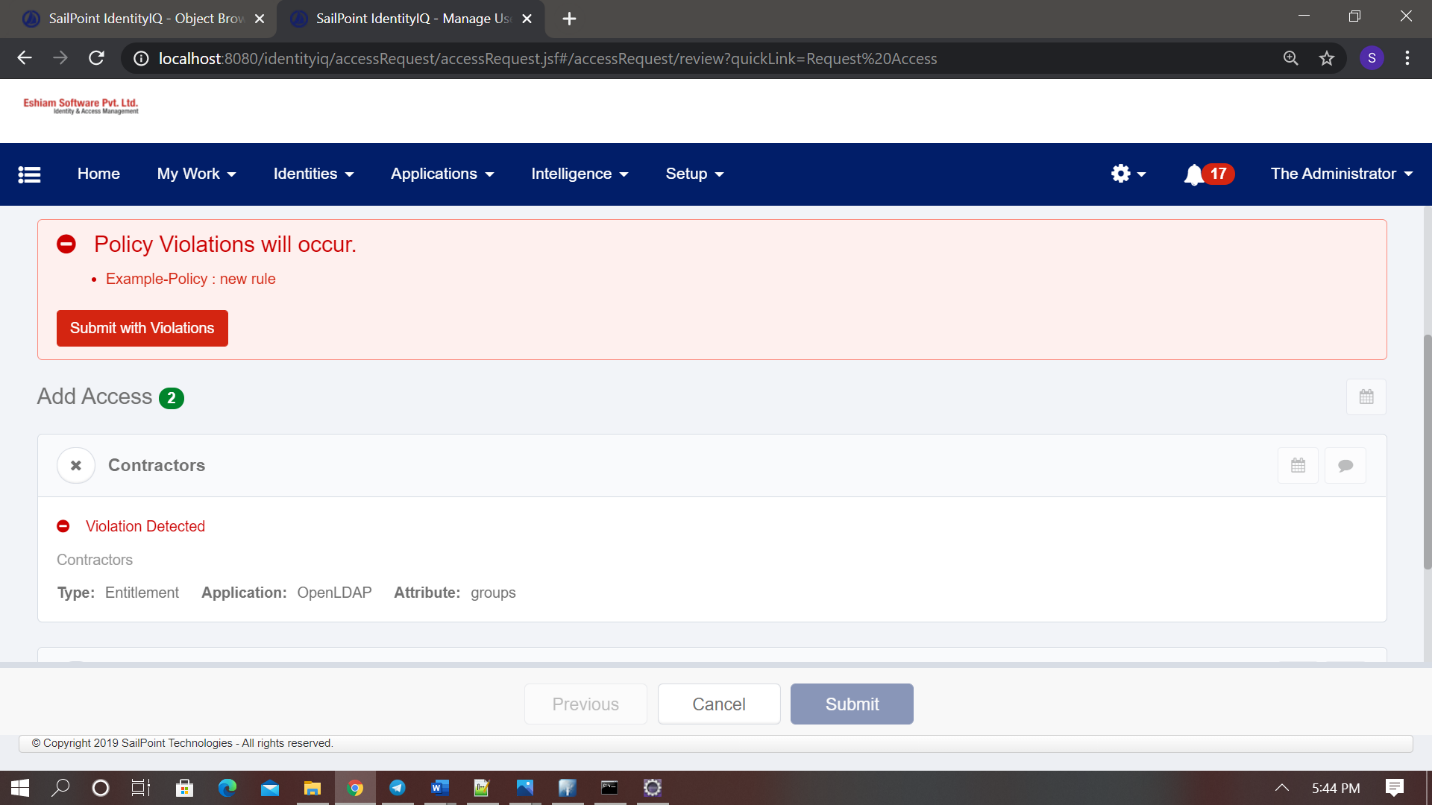
Go to debug-->open LCM Provisioning workflow.



<Variable initializer="fail" input="true" name="policyScheme">

We are created Policy. To check whether it is working or not. Go to Manage User Access select any User. Then add the entitlements which are in the Policy. The User will not be added to the Entitlements. You

Will get an error message like below.



**Thank You**