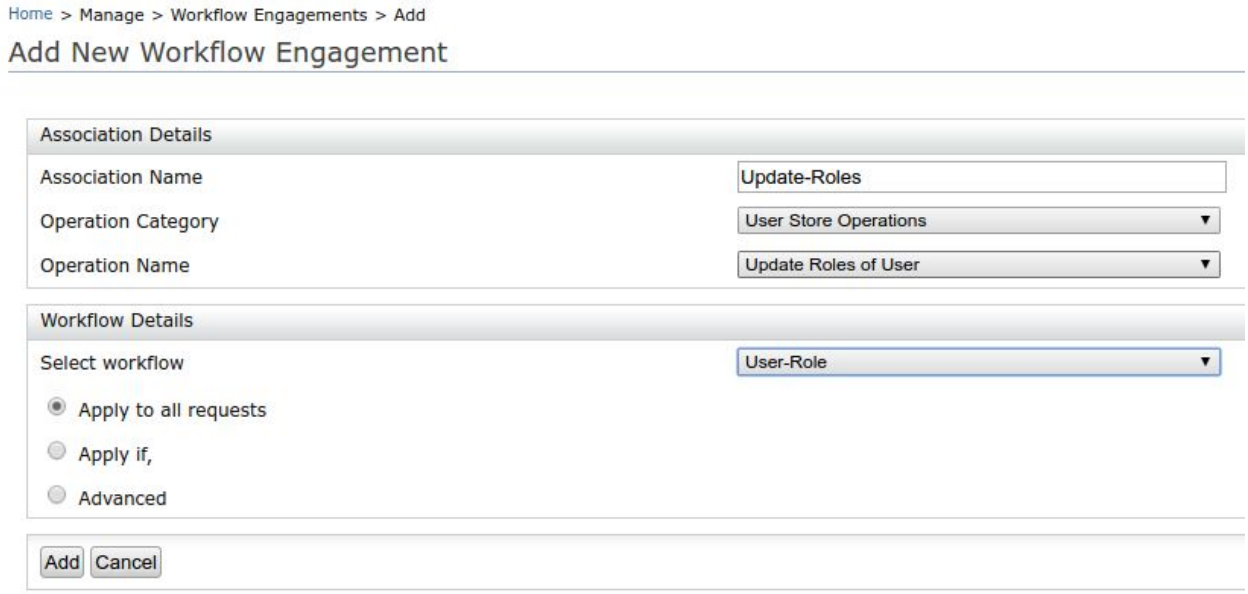
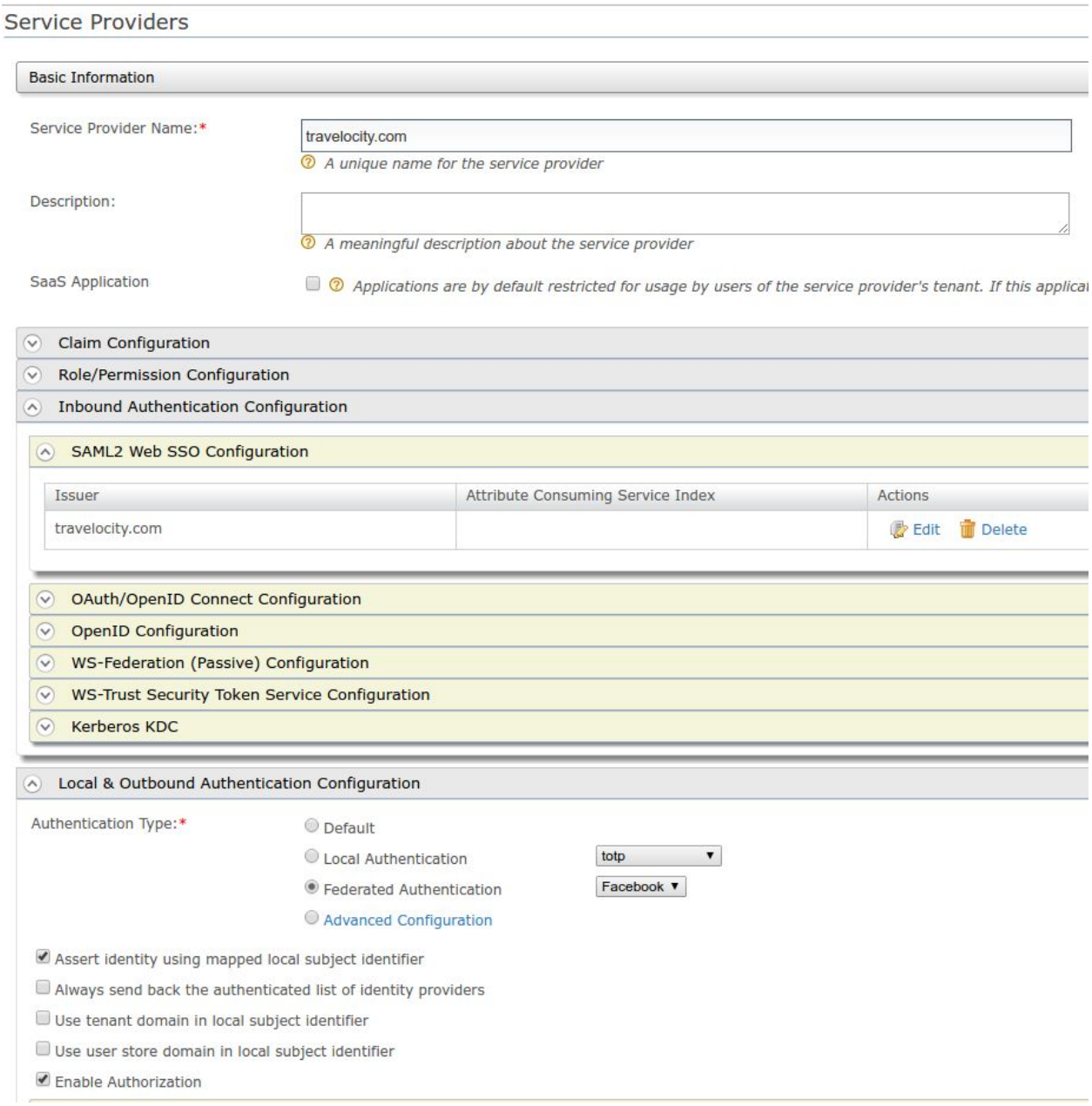
- Use the source from here. Use Maven 3 and Java 7 to build the source code and copy custom-identity-mgt/components/custom-identity-mgt/target/custom-identity-mgt-1.0.0.jar to <CARBON_HOME>/repository/components/dropins/ directory.
- Add secondary userstore with domain name ACME.COM and create two roles with names admin and travelocity.com

UC1: Add external users through JIT

- Add workflow definition as described here
- Add workflow engagement like below.



- Add facebook Identity provider as described here or any other identity provider as described here
- Add service provider with name travelocity.com. Enable authorization and Enable Assert identity using mapped local subject identifier



- Go to *Entitlement -> PAP -> Policy Administration -> Add New Entitlement Policy -> Write Policy in XML* to add new XACML policy. Use below XACML policy.

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17" PolicyId="travelocity.com-auth-by-application-role-policy" RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable" Version="1.0">

<Description>This is a reference policy for service provider authorization by role. This will only allow users in ACME.COM/travelocity.com role to login to travelocity.com SP and anyone else will be denied.</Description>
<Target>
<AnyOf>
<AllOf>
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">travelocity.com</AttributeValue>
<AttributeDesignator AttributeId="http://wso2.org/identity/sp/sp-name" Category="http://wso2.org/identity/sp" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
</Match>
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">authenticate</AttributeValue>
<AttributeDesignator AttributeId="http://wso2.org/identity/identity-action/action-name" Category="http://wso2.org/identity/identity-action" DataType="http://www.w3.org/2001/XMLSchema#string" MustBePresent="true"></AttributeDesignator>
</Match>
</AllOf>
</AnyOf>
</Target>
<Rule Effect="Permit" RuleId="allow-if-in-admin">
<Condition>
<Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-in">
<AttributeValue DataType="http://www.w3.org/2001/XMLSchema#string">ACME.COM/travelocity.com</AttributeValue>
<AttributeDesignator AttributeId="http://wso2.org/claims/role" Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"

DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
</Apply>
</Condition>
</Rule>
<Rule Effect="Deny" RuleId="deny-all-others"></Rule>
</Policy>

- Publish the created policy to PDP
- Change *StepBasedSequenceHandler* in *<CARBON_HOME>/repository/conf/identity/application-authentication.xml* to *com.custom.listener.handler.provisioning.ExtendedStepBasedSequenceHandler* and *ProvisioningHandler* to *com.custom.listener.handler.provisioning.ExtendedProvisioningHandler*

UC2: Restricted ability to change user details

- Add below XACML policy as described above

<Policy xmlns="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
PolicyId="update-claims-auth-by-role-policy"
RuleCombiningAlgId="urn:oasis:names:tc:xacml:1.0:rule-combining-algorithm:first-applicable"
Version="1.0">
<Description>This is a reference policy for authorization to update user profile by role. This will only allow users in admin role of the userstore to update the user profiles in that particular user store and anyone else will be denied.</Description>
<Target>
<AnyOf>
<AllOf>
<Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
<AttributeValue
*DataType="http://www.w3.org/2001/XMLSchema#string">*ACME.*COM</AttributeValue>*
<AttributeDesignator AttributeId="http://wso2.org/identity/user/user-store-domain"
Category="http://wso2.org/identity/user"

```
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
          </Match>
          <Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
            <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">update-claims</AttributeValue>
            <AttributeDesignator AttributeId="http://wso2.org/identity/identity-action/action-name"
Category="http://wso2.org/identity/identity-action"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
          </Match>
        </AllOf>
      </AnyOf>
    </Target>
    <Rule Effect="Permit" RuleId="allow-if-in-admin">
      <Condition>
        <Apply FunctionId="urn:oasis:names:tc:xacml:1.0:function:string-is-in">
          <AttributeValue
DataType="http://www.w3.org/2001/XMLSchema#string">ACME.COM/admin</AttributeValue>
          <AttributeDesignator AttributeId="http://wso2.org/claims/role"
Category="urn:oasis:names:tc:xacml:1.0:subject-category:access-subject"
DataType="http://www.w3.org/2001/XMLSchema#string"
MustBePresent="true"></AttributeDesignator>
        </Apply>
      </Condition>
    </Rule>
    <Rule Effect="Deny" RuleId="deny-all-others"></Rule>
</Policy>
```

UC4: Audit Trail

- To disable the default user operation audit logger add below configuration inside *<EventListeners>* to *<CARBON_HOME>/repository/conf/identity/identity.xml*

<EventListener type="org.wso2.carbon.user.core.listener.UserOperationEventListener"
name="org.wso2.carbon.user.mgt.listeners.UserMgtAuditLogger"
orderId="9" enable="false"/>

UC5: Show / Hide claim details

- Edit the claim needed to hide in http://wso2.org/claims dialect and add mapped attribute as NA for ACME.COM user store domain.