**Scenario 01: Single Sign On between multiple heterogeneous identity federation protocols**

### **Problem:**

* The business users need to access multiple service providers supporting multiple heterogeneous identity federation protocols.
* Some service providers are on-premise while others are in the cloud. For example Google Apps (SAML 2.0), Salesforce (SAML 2.0), Office 365 (WS-Federation) are cloud based while JIRA, Drupal, Redmine are on-premise service providers.
* A user logs into any of the service providers should be automatically logged into the rest.

### **Test Cases:**

|  |  |
| --- | --- |
| Test cases | Script |
| IAMST-5 : User can log out after successful SSO authentication | Single sign on value set 01 |
| IAMST-8 : Validate user can login again after successful logout -SSO | Single sign on value set 01 |
| IAM ST-9 : Validate single logout -SSO | Single sign on value set 01 |
| IAMST-11 : User can successful Multi option authentication -SSO | Single sign on value set 02 |
| IAMST-12 : Validate user can SSO authenticate with WS-Trust/SAML/OpenId | Single sign on value set 01 |
| IAMST-22 : SP configuration with enable Attribute Profile -SS | Single sign on value set 01 |
| IAMST-25 : SP configuration with saas enable -SSO | Single sign on value set 04 |
| IAMST-28 : SP configuration with metadata file - SSO authentication |  |
| IAMST-31 : SP configuration with urls configurations - SSO authentication | Single sign on value set 03 |

For more scenario detail please refer Testlink [2] IAMST: Identity-test-Integration

**Products:**

WSO2 Identity Server 5.5.0

### **Preconditions**

General:

* User needs to deploy travelocity, playground and passiveSTS webapps in tomcat server.Check [1] on how to build webapps from repository.

IAMST-25 : SP configuration with saas enable -SSO

* change travelocity property file #Additional request parameters #QueryParams=tenantDomain=tenant\_a.com

(before test and after test 2 bash files)

* IAMST-28 : SP configuration with metadata file - SSO authentication
* Deployed metadata file in the tomcat

IAMST-31 : SP configuration with urls configurations - SSO authentication

* Add <Identity test integration home>/CommonValueSets/spMetadat/metadataTravApp.xml file in to the <tomcat home>/webapp

### **Configurations**

1.Go to user.properties file and change the values of configurations as below.

#### **IS Server**

serverHost=< HOST NAME OF IS SERVER >

serverPort=< PORT OF THE IS SERVER >

scenarioName=< Scenario Name >

#### **User Management**

adminusername=< ADMIN USER NAME >

adminpassword=< ADMIN PASSWORD >

adminCredentials=< BASE64 Encoded ADMIN USERNAME:ADMIN PASSWORD >

rolename= < NEW ADMIN ROLE NAME >

usernamePrefix=< NEW ADMIN USERNAME >

noOfUsers= < NUMBER OF USERS TO CREATE >

noUsername=< NEW NON EXISTING USER'S USERNAME >

noPassword=< NEW NON EXISTING USER'S PASSWORD >

permission=< PERMISSION FOR ADMIN ROLE >

userEmailAddress=<USER EMAIL ADDRESS>

#### **SP**

spname=< SP NAME >

spdescription=< SP DESCRIPTION >

carbonServer=< ISSUER NAME >

## **Travelocity**

travelocityAppName=travelocity.com spName=< SP NAME OF TRAVELOCITY >

spDescription=< SP DESCRIPTION OF TRAVELOCITY >

## **Playground**

playgroundHost=< HOST NAME FOR PLAYGROUND APP >

spName2=< SP NAME OF PLAYGROUND >

spDescription2=< SP DESCRIPTION OF PLAYGROUND >

## **PssiveSTS**

spName3=< SP NAME OF passiveSTS >

spDescription3=< SP DESCRIPTION OF passiveSTS >

**Connectors**

LinkedinUserName=<LINKEDIN USER NAME>

LinkedinPassword=<LINKEDIN PASSWORD>

IdentityProviderName=<LINKEDIN IDP NAME>

linkedinClientId=<LINKEDIN CLIENT ID>

linkedinClientSecret=<LINKEDIN CLIENT SESCRET>

**Facebook**

FbClientId=<FACEBOOK CLIENT ID>

FbSecret=<FACEBOOK SECRET ID>

FbScope=<FEACEBOOK EMAIL>

FbUserInfoFields= <FACEBOOK FIELDS>

FacebookPassword=<FACEBOOK PASSWORD>

FaceboookUserName=<FACEBOOK USER NAME>

**Tenant**

adminusernameTa=<TENANT ‘A’ ADIMIN USER>

adminpsswordTa=<TENANT ‘A’ ADMIN PASSWORD>

emailAddressTa=<TENANT ‘A’ EMAIL ADDRESS>

fNameTa=<TENANT ‘A’ FIRST NAME>

lNameTa=<TENANT ‘A’ LAST NAME>

domainTa=<TENANT ‘A’ DOMAIN NAME>

adminusernameTb=<TENANT ‘B’ ADIMIN USER>

adminpsswordTb=<TENANT ‘B’ ADMIN PASSWORD>

emailAddressTb=<TENANT ‘B’ EMAIL ADDRESS>

fNameTb=<TENANT ‘B’ FIRST NAME>

lNameTb=<TENANT ‘B’ LAST NAME>

domainTb=<TENANT ‘B’ DOMAIN NAME>

adminusernameLoginTa=<TENANT ‘A’ LOGIN NAME>

adminusernameLoginTb=<TENANT ‘B’ LOGIN NAME>

## **Tomcat**

tomcatHost=< HOST NAME OF TOMCAT SERVER >

tomcatPort=< PORT OF THE TOMCAT SERVER >

## **Metadata file path**

metadataFilePath=<METADATA FILE PATH>

managmentConsole=<MANAGMENT CONSOLE>

spListUrlCarbon=<LIST SERVICE PROVIDER JSP>

loadSpUrlCarbon=<LOAD SP PROVIDER JSP>

addSamlSpUrlCarbon=<ADD SERVICE PROVIDER JSP>

[1]<https://docs.wso2.com/display/IS541/Downloading+a+Sample>

[2] <https://testlink.wso2.com/>

**Scenario 02: Multiple login options by service provider**

**Problem:**

* The business users need to access multiple service providers, where each service provider requires different login options. For example login to Google Apps with username/password, while login to Drupal either with username/password or Facebook
* Enable multi-factor authentication for some service providers. For example login to Salesforce require username/password + FIDO

For more scenario detail please refer Testlink [2] IAMST: Identity-test-Integration

**Products:**

WSO2 Identity Server 5.5.0

### **Test cases:**

|  |  |
| --- | --- |
| Test cases | Script |
| Travelocity logout -MFA with (linkedin) | MFA value set 01 |
| Travelocity logout -MFA with (Facebook) | MFA value set 02 |
| IAMST-24 : SP configuration with enable Attribute Profile - MFA authentication | MFA value set 03 |
| IAMST-27 : SP configuration with saas enable - MFA authentication | MFA value set 04 |
| IAMST-33 : SP configuration with urls configurations - MFA authentication | MFA value set 05 |

### **Preconditions**

General:

* User needs to deploy travelocity webapp in tomcat server.Check [1] on how to build webapps from repository.

IAMST-27 : SP configuration with saas enable - MFA authentication

* change travelocity property file #Additional request parameters #QueryParams=tenantDomain=tenant\_a.com

(before test and after test 2 bash files)

Travelocity logout -MFA with (linkedin)

* Linkedin connector download [3] and place in <IS home>/ repository/components/dropins

Travelocity logout -MFA with (Facebook)

* Facebook connector download [4] and place in <IS home>/ repository/components/dropins

IAMST-33 : SP configuration with urls configurations - MFA authentication

* Add <Identity test integration home>/CommonValueSets/spMetadat/metadataTravApp.xml file in to the <tomcat home>/webapp

[1]<https://docs.wso2.com/display/IS541/Downloading+a+Sample>

[2] <https://testlink.wso2.com/>

[3][https://store.wso2.com/store/assets/isconnector/list?q=%22\_default%22%3A%22linkedin%22](https://store.wso2.com/store/assets/isconnector/list?q="_default"%3A"linkedin")

[4]<https://store.wso2.com/store/assets/isconnector/details/9edb106b-05ee-4810-8d47-81d0639f8c2b>

### **Configurations**

Go to user.properties file and change the values of configurations as below.

#### **IS Server**

serverHost=< HOST NAME OF IS SERVER >

serverPort=< PORT OF THE IS SERVER >

scenarioName=< Scenario Name >

#### **User Management**

adminusername=< ADMIN USER NAME >

adminpassword=< ADMIN PASSWORD >

adminCredentials=< BASE64 Encoded ADMIN USERNAME:ADMIN PASSWORD >

rolename= < NEW ADMIN ROLE NAME >

usernamePrefix=< NEW ADMIN USERNAME >

noOfUsers= < NUMBER OF USERS TO CREATE >

noUsername=< NEW NON EXISTING USER'S USERNAME >

noPassword=< NEW NON EXISTING USER'S PASSWORD >

permission=< PERMISSION FOR ADMIN ROLE >

userEmailAddress=<USER EMAIL ADDRESS>

#### **SP**

spname=< SP NAME >

spdescription=< SP DESCRIPTION >

carbonServer=< ISSUER NAME >

## **Travelocity**

travelocityAppName=travelocity.com spName=< SP NAME OF TRAVELOCITY >

spDescription=< SP DESCRIPTION OF TRAVELOCITY >

## **Playground**

playgroundHost=< HOST NAME FOR PLAYGROUND APP >

spName2=< SP NAME OF PLAYGROUND >

spDescription2=< SP DESCRIPTION OF PLAYGROUND >

## **PssiveSTS**

spName3=< SP NAME OF passiveSTS >

spDescription3=< SP DESCRIPTION OF passiveSTS >

**Connectors**

LinkedinUserName=<LINKEDIN USER NAME>

LinkedinPassword=<LINKEDIN PASSWORD>

IdentityProviderName=<LINKEDIN IDP NAME>

linkedinClientId=<LINKEDIN CLIENT ID>

linkedinClientSecret=<LINKEDIN CLIENT SESCRET>

**Facebook**

FbClientId=<FACEBOOK CLIENT ID>

FbSecret=<FACEBOOK SECRET ID>

FbScope=<FEACEBOOK EMAIL>

FbUserInfoFields= <FACEBOOK FIELDS>

FacebookPassword=<FACEBOOK PASSWORD>

FaceboookUserName=<FACEBOOK USER NAME>

**Tenant**

adminusernameTa=<TENANT ‘A’ ADIMIN USER>

adminpsswordTa=<TENANT ‘A’ ADMIN PASSWORD>

emailAddressTa=<TENANT ‘A’ EMAIL ADDRESS>

fNameTa=<TENANT ‘A’ FIRST NAME>

lNameTa=<TENANT ‘A’ LAST NAME>

domainTa=<TENANT ‘A’ DOMAIN NAME>

adminusernameTb=<TENANT ‘B’ ADIMIN USER>

adminpsswordTb=<TENANT ‘B’ ADMIN PASSWORD>

emailAddressTb=<TENANT ‘B’ EMAIL ADDRESS>

fNameTb=<TENANT ‘B’ FIRST NAME>

lNameTb=<TENANT ‘B’ LAST NAME>

domainTb=<TENANT ‘B’ DOMAIN NAME>

adminusernameLoginTa=<TENANT ‘A’ LOGIN NAME>

adminusernameLoginTb=<TENANT ‘B’ LOGIN NAME>

## **Tomcat**

tomcatHost=< HOST NAME OF TOMCAT SERVER >

tomcatPort=< PORT OF THE TOMCAT SERVER >

## **Metadata file path**

metadataFilePath=<METADATA FILE PATH>

managmentConsole=<MANAGMENT CONSOLE>

spListUrlCarbon=<LIST SERVICE PROVIDER JSP>

loadSpUrlCarbon=<LOAD SP PROVIDER JSP>

addSamlSpUrlCarbon=<ADD SERVICE PROVIDER JSP>

**Scenario 09:User Management upon multi-layer approval**

**Problem:**

All the user management operations must be approved by multiple administrators in the enterprise in a hierarchical manner.

### **Test Cases:**

|  |  |
| --- | --- |
| Test cases | Script |
| IAMST-17 : Validate workflow trigger only it's condition is satisfied | Multilayer approval value set 01 |
| IAMST-19 : Validate approval rejection from one or more than one approver | Multilayer approval value set 01 |
| IAMST-20 : Ensure user can not approve by violating the approval step order | Multilayer approval value set 01 |

For more scenario detail please refer Testlink [1] IAMST: Identity-test-Integration

**Products:**

WSO2 Identity Server 5.5.0

### **Preconditions:**

IS should up and running

[1] <https://testlink.wso2.com/>

### **Configurations**

Go to user.properties file and change the values of configurations as below.

**IS**

serverHost= <SERVER HOST>

serverPort=<SERVER PORT>

**User Management**

adminUsername=<ADMIN USER NAME>

adminPassword=<ADMIN PASSWORD>

**Workflow**

authorityUser1=<AUTHORITY USER 01>

authorityUser2=<AUTHORITY USER 02>

authorityUser1Password=<AUTHORITY USER 01 PASSWORD>

authorityUser2Password=<AUTHORITY USER 02 PASSWORD>

authorityRole1=<AUTHORITY ROLE 01>

authorityRole2=<AUTHORITY ROLE 02>

workflowUser=<WORKFLOW USER>

workflowRole=<WORKFLOW ROLE>

workflowUserPassword=<WORKFLOW USER PASSWORD>

workFlowName= <WORKFLOW NAME>

workFlowId=<WORKFLOW ID>

workFlowAssociationName=<WORKFLOW ASSOCIATION NAME>

wAEventID=<WORKFLOW EVENT ID>

wACondition=<WORKFLOW CONDITION>

workflowUserEmail=<WORKFLOW USER EMAIL>

authorityUser2Email=<AUTHORITY 02 USER EMAIL>

authorityUser1Email=<AUTHORITY 01 USER EMAIL>

constantTimer=<CONSTANT TIME>

**Scenario 05: Multi-factor authentication for WSO2 Identity Server management console**

**Problem:**

Enable MFA for the WSO2 Identity Server Management Console. -In other words, the Identity Server’s Management Console itself must be protected with MFA.

### **Test Cases:**

|  |  |
| --- | --- |
| Test cases | Script |
| Validate IS enable MFA authentication and Sp caretion from metadata url upload | MFA for IS itself value set 01 |

For more scenario detail please refer Testlink [1] IAMST: Identity-test-Integration

**Products:**

WSO2 Identity Server 5.5.0

### **Script execution order**

1. Script: MFAForISItSelf\_Datacreation

### **Preconditions:**

* IS server up and running
* Twitter connector download [2] and place in <IS home>/ repository/components/dropins

1. Script: ISAuthenticationWithMFA

### **Preconditions:**

* Change <isHome>/repository/conf/security/authenticators.xml file,  following tags as below.

<Authenticator name="SAML2SSOAuthenticator" disabled="false">

   <Priority>1</Priority>

* Restart the carbon server
* Deployed metadata file (metadataIsItselfAsSp.xml) in the tomcat

1. Script: Cleaning
   * Change <isHome>/repository/conf/security/authenticators.xml file,  following tags as below.

<Authenticator name="SAML2SSOAuthenticator" disabled="true">

   <Priority>10</Priority>

* + Restart the carbon server

[1] <https://testlink.wso2.com/>

[2] [https://store.wso2.com/store/assets/isconnector/list?q=%22\_default%22%3A%22twitter%22](https://store.wso2.com/store/assets/isconnector/list?q="_default"%3A"twitter")

### **Configurations**

**IS**

serverHost= <SERVER HOST>

serverPort=<SERVER PORT>

**User Management**

adminUsername=<ADMIN USER NAME>

adminPassword=<ADMIN PASSWORD>

**IDP**

idpname=<Idp Name>

idpdescription=<IDP DESCRIPTION>

TwitterClientId=<IDP CLIENT ID>

TwitterSecret=<IDP SECREAT>

twitterUserName=<IDP USER NAME>

twitterPassword=<IDP PASSWORD>

**SP**

spname=<SP NAME>

spdescription=<SP DECRIPTION>

## **Metadata file path**

metadataFilePath=<METADATA FILE PATH>

managmentConsole=<MANAGMENT CONSOLE>

spListUrlCarbon=<LIST SERVICE PROVIDER JSP>

loadSpUrlCarbon=<LOAD SP PROVIDER JSP>

addSamlSpUrlCarbon=<ADD SERVICE PROVIDER JSP>