Steps for SAML integration with IBemsServer

The following are requirement for SAML integration

1. samlKeystore.jks file
2. keystore.p12 file
3. metadafile
4. ldap configuration file

Step 1: Go to

C:\Program Files\Java\jdk1.8.0\_25\bin and open commond cmd

1. And put the following command for creation for samlKeystore.jks file

**keytool -genkey -alias tomcat** **-keyalg RSA -keystore E:\samlKeystore.jks**

**it looks like**

C:\Program Files\Java\jdk1.8.0\_25\bin>keytool -genkey -alias tomcat -keyalg RSA

-keystore E:\samlKeystore.jks

Enter keystore password:123456

What is your first and last name?

[Unknown]: AAA

What is the name of your organizational unit?

[Unknown]: AAA

What is the name of your organization?

[Unknown]: AAA

What is the name of your City or Locality?

[Unknown]: AAA

What is the name of your State or Province?

[Unknown]: AAA

What is the two-letter country code for this unit?

[Unknown]: AAA

Is CN=AAA, OU=AAA, O=AAA, L=AAA, ST=AAA, C=AAA correct?

[no]: yes

Enter key password for <tomcat>

(RETURN if same as keystore password):123456

Re-enter new password:123456

And now E:\samlKeystore.jks file generated now

Step 2: Genarate the keystore.p12 file

Use the following commond

keytool -importkeystore -srckeystore E:\samlKeystore.jks -destkeystore E:\keystore.p12

-srcstoretype JKS -deststoretype PKCS12 -deststorepass 123456

-srcalias tomcat -destalias tomcat

**it looks like**

C:\Program Files\Java\jdk1.8.0\_25\bin>keytool -importkeystore -srckeystore E:\sa

mlKeystore.jks -destkeystore E:\keystore.p12

Enter destination keystore password:123456

Re-enter new password: 123456

Enter destination keystore password: 123456

Re-enter new password: 123456

Enter source keystore password: 123456

Entry for alias apollo successfully imported.

Entry for alias tomcat successfully imported.

Import command completed: 2 entries successfully imported, 0 entries failed or

cancelled

and now E:\keystore.p12 file is created

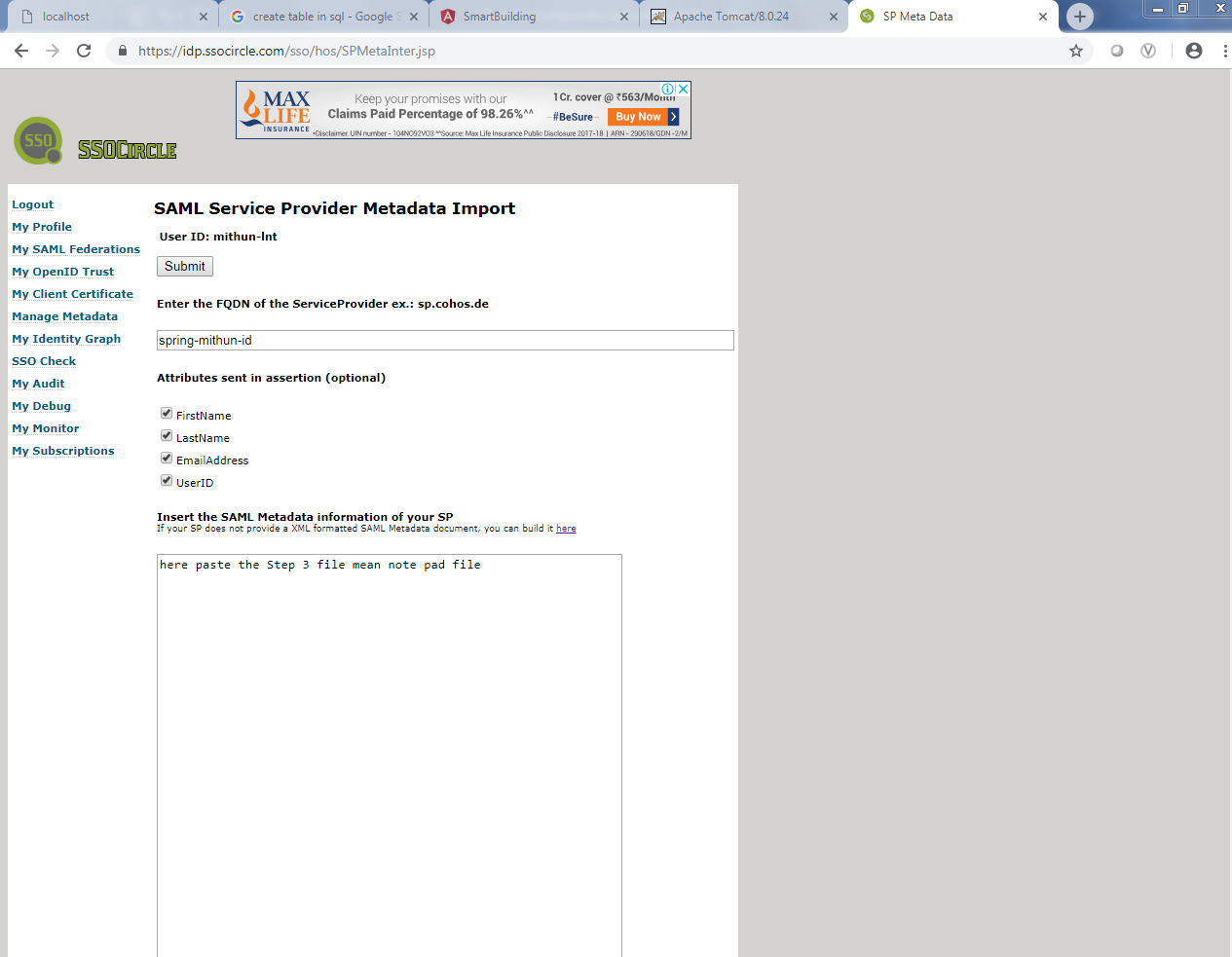
Now Go to <https://idp.ssocircle.com/sso/UI/Login?gx_charset=UTF-8>

Create user and login

After login do the following process

Step 3: create LDP

Go to >>> Manage your Service Provider Metadata>> [Add new Service Provider](https://idp.ssocircle.com/sso/hos/SPMetaInter.jsp) . here create



**Enter the FQDN of the ServiceProvider ex.: sp.cohos.de**

spring.lnt.saml.sp.mithun2.id

Put this in **Insert the SAML Metadata information of your SP**

<?xml version="1.0" encoding="UTF-8" standalone="yes"?><EntityDescriptor entityID="spring.lnt.saml.sp.mithun2.id" xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><SPSSODescriptor AuthnRequestsSigned="false" WantAssertionsSigned="true" protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"><NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified</NameIDFormat><AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://idp.ssocircle.com:443/sso/ArtifactResolver/metaAlias/publicidp"/></SPSSODescriptor></EntityDescriptor>

Click on the submit button :

Step 4: create LDP

Go to >>> Manage your Service Provider Metadata>> [SSOCircle Public IDP Metadata](https://idp.ssocircle.com/meta-idp.xml) . here take the entire file and save it as MY\_Meta.xml file

So this your metada file

Step 5: Go to tomcat server file

F:\SRR4\Eclipse\_Workspace\tomcatserver\apache-tomcat-8.0.24\webapps

Create metada folder and put your MY\_Meta.xml here and change the server port number to 8082 and after that start your server and check after your server is starting

<http://10.20.200.164:8082/metadata/My_META.xml>

and now in import the project in to eclipse

**spring-boot-security-saml-sample**

and do some changes here in following classes

com.lnt.spring.boot.security.saml.web.config>> WebSecurityConfig

@Bean

@Qualifier("idp-ssocircle")

public ExtendedMetadataDelegate ssoCircleExtendedMetadataProvider()

throws MetadataProviderException {

// Can be converted to FilesystemMetadataProvider instead of HTTPMetadataProvider

// https://www.programcreek.com/java-api-examples/?api=org.opensaml.saml2.metadata.provider.FilesystemMetadataProvider

String idpSSOCircleMetadataURL = "http://10.20.200.164:8082/metadata/My\_META.xml";

HTTPMetadataProvider httpMetadataProvider = new HTTPMetadataProvider(

this.backgroundTaskTimer, httpClient(), idpSSOCircleMetadataURL);

httpMetadataProvider.setParserPool(parserPool());

ExtendedMetadataDelegate extendedMetadataDelegate =

new ExtendedMetadataDelegate(httpMetadataProvider, extendedMetadata());

extendedMetadataDelegate.setMetadataTrustCheck(true);

extendedMetadataDelegate.setMetadataRequireSignature(false);

backgroundTaskTimer.purge();

return extendedMetadataDelegate;

}

@Bean

public MetadataGenerator metadataGenerator() {

MetadataGenerator metadataGenerator = new MetadataGenerator();

//metadataGenerator.setEntityId("com:vdenotaris:spring:sp");

metadataGenerator.setEntityId("spring.lnt.saml.sp.mithun2.id");

metadataGenerator.setExtendedMetadata(extendedMetadata());

metadataGenerator.setIncludeDiscoveryExtension(false);

metadataGenerator.setKeyManager(keyManager());

return metadataGenerator;

}

And run this application Application.java

And after that successfully run

Open browser and run

<http://localhost:8080>

then you you get UI is Like