How to Configure Single Sign-On with SAP HANA using SAML and SAP BusinessObjects Analysis for Office 2.2

Applicable Releases:

SAP HANA SPS10 and above
SAP BusinessObjects BI Platform 4.1 SP6 and above
SAP BusinessObjects Analysis for Office 2.1 and above

Topic Area:
Installation, Configuration, Security, Troubleshooting

Capability:
SAP HANA Database, Single Sign-On, SSO, SAML, IDP

Version 1.0.0

February 2016

Document History

Document Version	Description
1.0.0	• First Release of this guide
1.0.1	• Updated Applicable Releases. • Added an additional Single Sign On failure - Common Issues section

Typographical Conventions

Type Style	Description
Example Text	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Cross-references to other documentation.
Example text	Emphasized words or phrases in body text, graphic titles, and table titles.
`Example text`	File and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example text`	User entry texts. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example text>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE TEXT`	Keys on the keyboard, for example, `F2` or `ENTER`.

Icons

Icon	Description
	Note
	SAP Knowledge Base Article
	Recommendation
	Go to Common Errors on this topic

TABLE OF CONTENTS

1 BUSINESS SCENARIO

The objective of this document is to provide step-by-step instructions on how to configure Single Sign-On (SSO) using Security Assertion Markup Language (SAML) between SAP BusinessObjects Analysis for Office (AO) and SAP HANA Database SPS10 (HANA).

2 PREREQUISITES

This guide is geared towards HANA Database Administrators or SAP BusinessObjects BI Platform Administrators.

This guide will assume there is basic knowledge of:

- SAP HANA Configuration Files such as indexserver.ini and global.ini
- SAP HANA Studio
- SAP BusinessObjects BI Platform Central Management Console
- SAP BusinessObjects Analysis for Office

3 BACKGROUND INFORMATION

3.1 Single Sign-On

Single Sign-On (SSO) allows a user to log on once and gain access to multiple systems and services without being asked to produce credentials again.

Security Assertion Markup Language (SAML) Kerberos is one of many ways for realizing SSO (other examples are Kerberos, SAP Logon Ticket or X.509 certificates).

Depending on how SSO has been setup, it could permit the user logon to just a front end application or it can enable SSO all the way down to the database in what's known as SSO to database (SSO2DB).

> *Example*
> *An example of SSO that is relevant to many office workers day-to-day is the use of Microsoft Outlook and the absence of a login and password to access your email and address book. When a user logs into a workstation, they enter a username and password. Shortly afterwards the desktop appears. If you start Outlook, you are not prompted for the login and password you just entered. The mechanisms of this are described in detail later in this document.*

3.2 Definitions

There will be several references to specific HANA and BI Platform systems in the guide and also in the screenshots. The following systems are used:

- SAP HANA Database Server
  - Hostname: LSLES11SP3x64
  - Instance: 00
  - System ID (SID): SL1

  - Revision: 102.4
  - Operating System: SUSE Linux 11.3
  - Web Dispatcher: Internal
  - Crypto Provider: CommonCrypto

- SAP BusinessObjects BI Platform
  - Hostname: BIPW08R2-0
  - Version: 4.1 SP 7 Patch 1
  - Operating System: Windows Server 2008 R2
  - Web Application Server: Apache Tomcat for BI 4 (residing on the same system)

This guide will reference the placeholders identified in the following table:

Placeholder	Description
<HANA System>	Hostname of the SAP HANA Database system
<HANA Instance>	Instance number of the SAP HANA Database system
<WDisp Port>	Web Dispatcher port number
<BI System>	Hostname of the SAP BusinessObjects BI Platform system.
<Web Application Server>	Hostname of the Web Application Server hosting the BI Platform system.
<Web Application Server Port>	Port number of the Web Application Server hosting the BI Platform system.

4 PREREQUISITES

4.1 Network Requirements

Hostname resolution must be possible between the HANA system and the BI Platform System (ping <BI System> and ping <HANA System>)

4.2 Software Requirements

SAP HANA SPS10 and higher
SAP BusinessObjects BI Platform 4.0 and higher.
SAP BusinessObjects Analysis for Office 2.2 and higher

5 STEP-BY-STEP CONFIGURATION

5.1 Overview

There are some initial configuration steps:

1. Enable HANA http connections for the MDAS server.

After that is set up, a trust must be established between the HANA and BI Platform System. At a high level, the steps include:

1. Generate a certificate from BI Platform
2. Import the certificate into the HANA Trust Store

After that trust has been estabilished, the last step is to setup the security on the HANA system:

1. Import the certificate into the HANA Security
2. Configure a SAML user with an external identity user
3. Test the connection

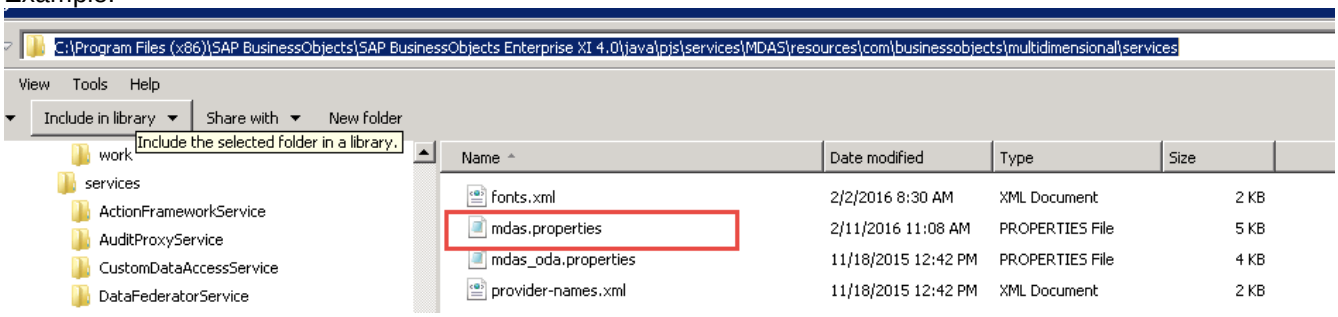
5.2 Enable HANA http connection for the Multi-Dimensional Analysis Service (MDAS)

The Multi-Dimension Analysis Service (MDAS) is a BI Platform service that handles the OLAP connections for Analysis for Office. By default, the MDAS service does not handle HANA http InA connections.

To enable HANA http InA connections

1. Locate the mdas.properties in the BI Platform system.

   Example:



2. Edit the mdas.properties file in Notepad and then change multidimensional.services.enable.hana.http.connections=false to true.

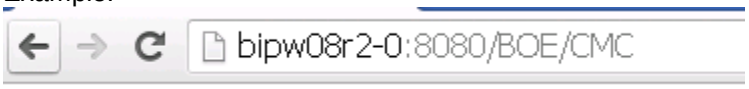
3. Restart SAP BusinessObjects BI Platform for these changes to take effect
4. This section is now complete.

5.3 Generate a Certificate from BI Platform

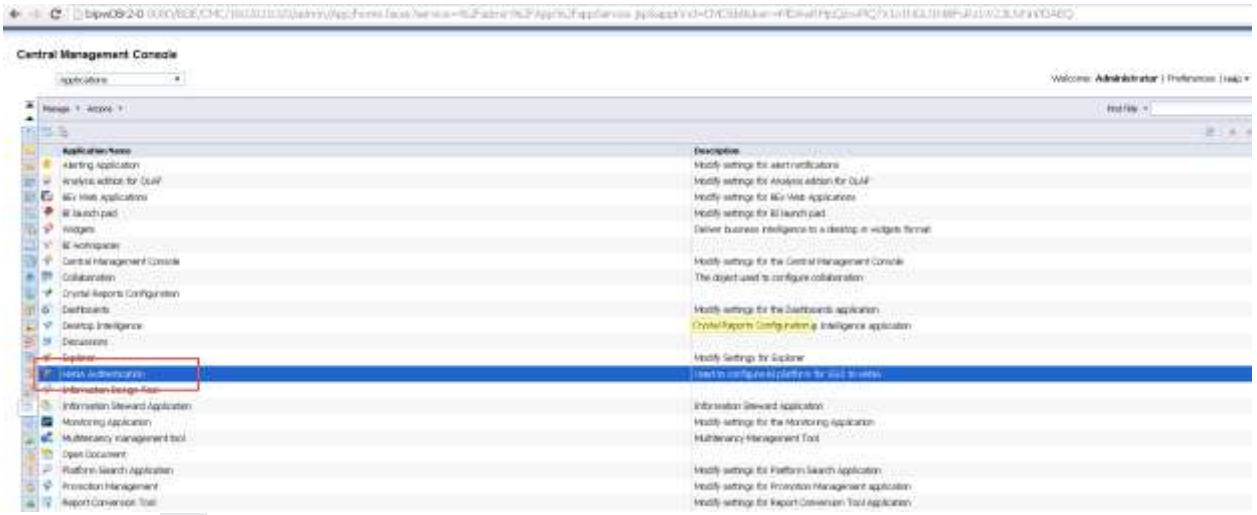
Generating a HANA certificate is performed through the BI Platform Central Management Console (CMC). This certificate will be specific to the HANA HTTP connection.

1. Open a browser and go to http://< Web Application Server >:< Web Application Server Port >/BOE/CMC

   Example:



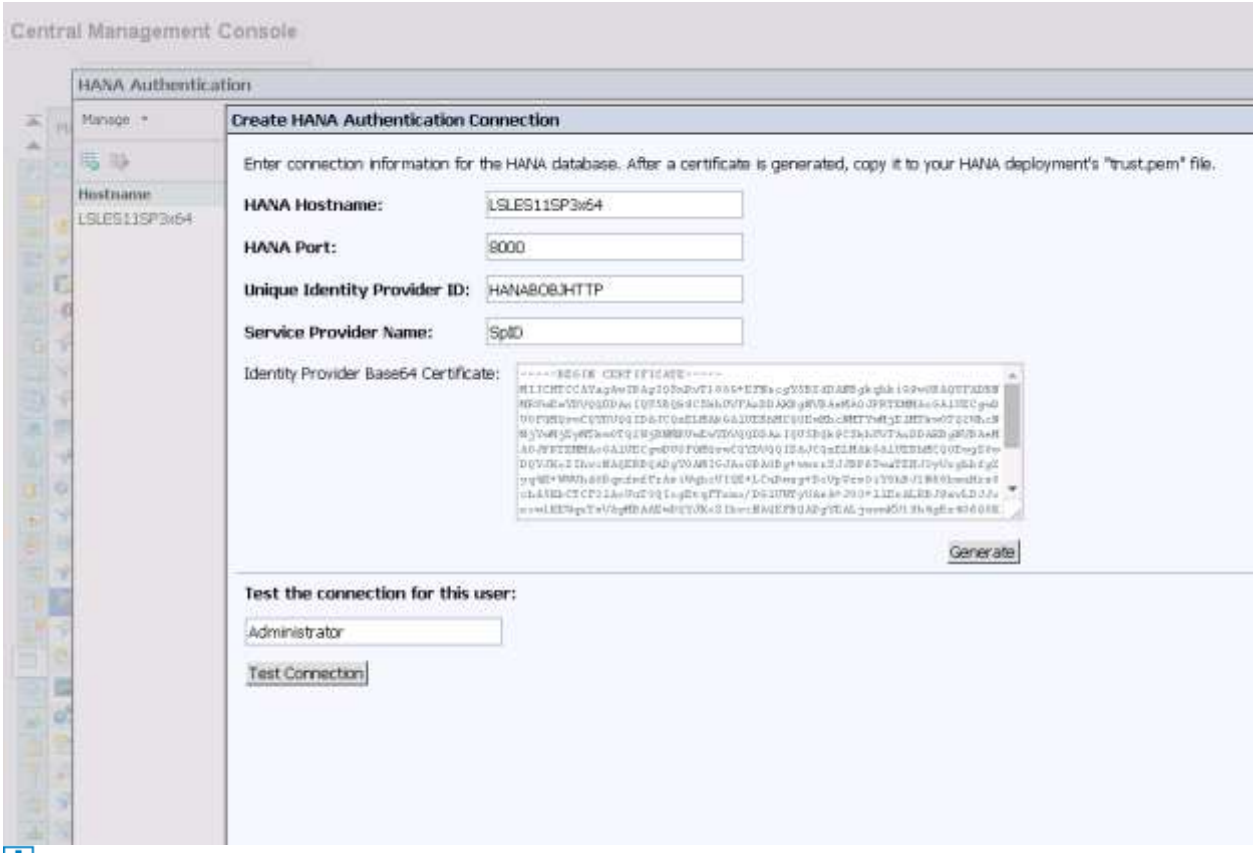
2. Go to CMC Home > Applications > HANA Authentication



3. Select the add  icon to create a new connection
4. Input the HANA details:

HANA Hostname	Hostname of the SAP HANA Database system
Web Dispatcher Port	The port the Web Dispatcher is listening on (default is 80<HANA Instance>)
Unique Identifier Provider ID:	Unique Name of the certificate
Service Provider Name:	Configuration setting (default is SpID). This should match the parameter indexserver.ini > [authentication] > saml_service_provider_name Service Provider Name mismatch?

Example:

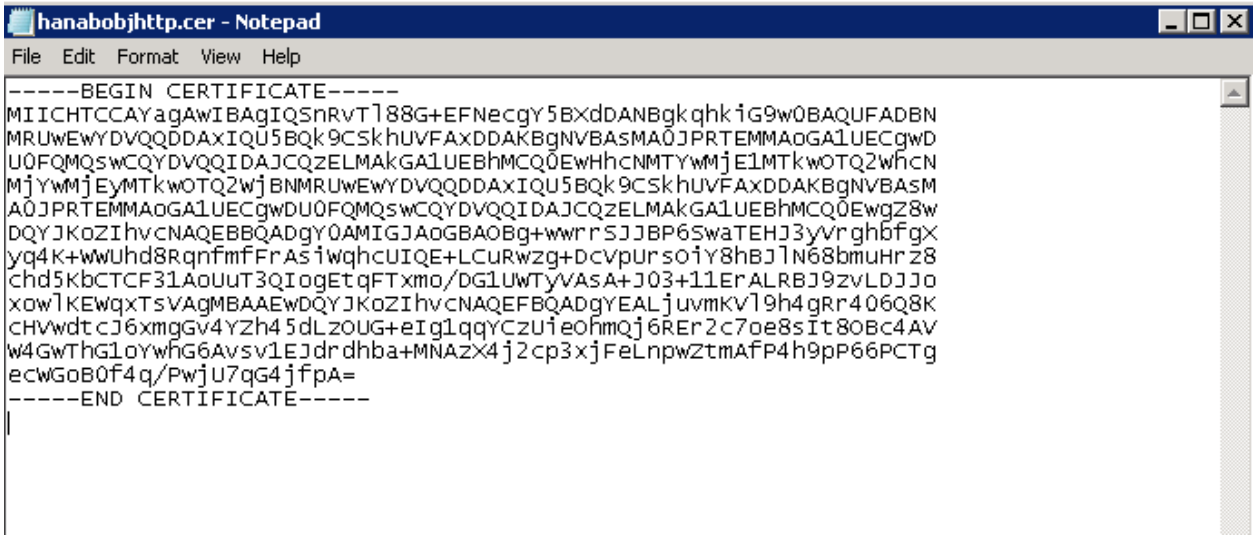


The text “After the certificate is generated, copy it to your HANA deployment’s “trust.pem” file” is not applicable in this case because CommonCrypto is used. A trust.pem is used for OpenSSL.

Connection Error?

5. Select Generate and then copy the entire certificate into the clipboard.
6. Select OK to save the connection
7. Create a new certificate file by pasting the certificate into a text editor.
8. Save the file as a .cer extension.

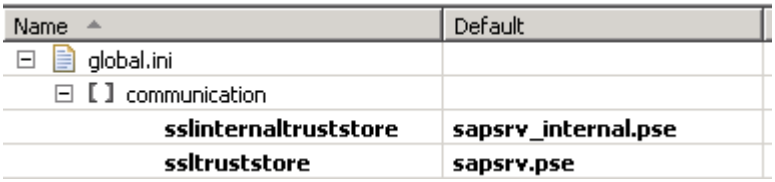
Example:



9. This section is now complete

5.4 Import the Certificate into the HANA Trust Store

To find out which trust store is used by HANA, check the configuration setting global.ini > [communication] > ssltruststore.



By default, the value is sapsrv.pse. This means the sapsrv.pse is located in the $SECUDIR/sapsrv.pse

There are two methods of importing the certificate into the trust store:

1. On the HANA O/S directly using sapgepse commands.
2. Using the internal Web Dispatcher Administration console.

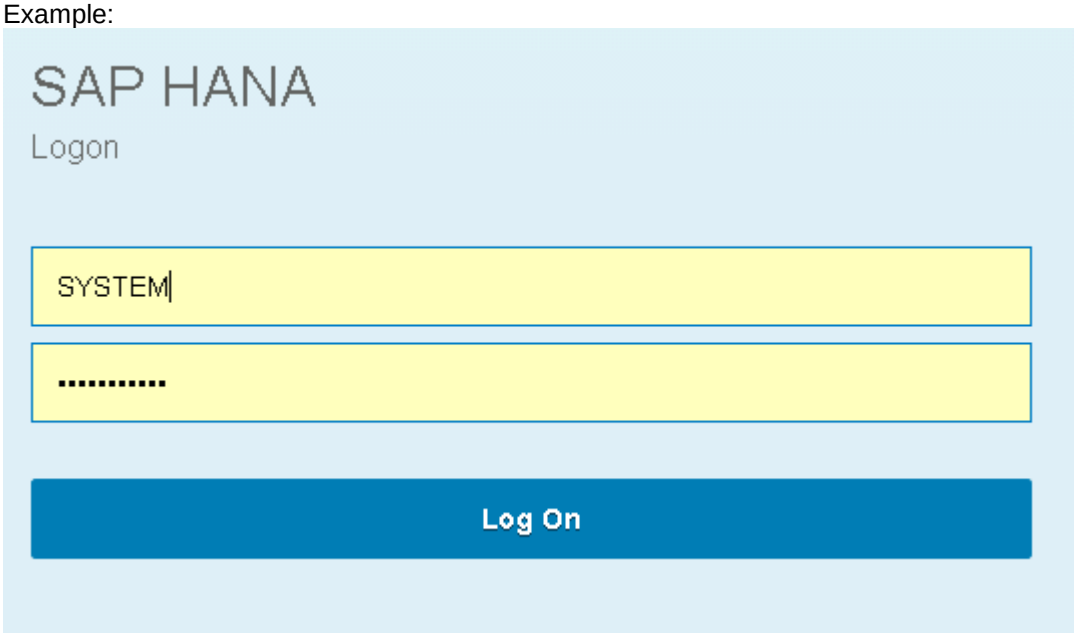
The following steps will be performed using the Web Dispatcher Adminstration console

1. Access the Web Dispatcher Administration page by going to this location:

   http://<HANA System>:<WDisp Port>/sap/hana/xs/wdisp/admin/public/default.html

2. Login with a HANA user (In this case, the SYSTEM user)

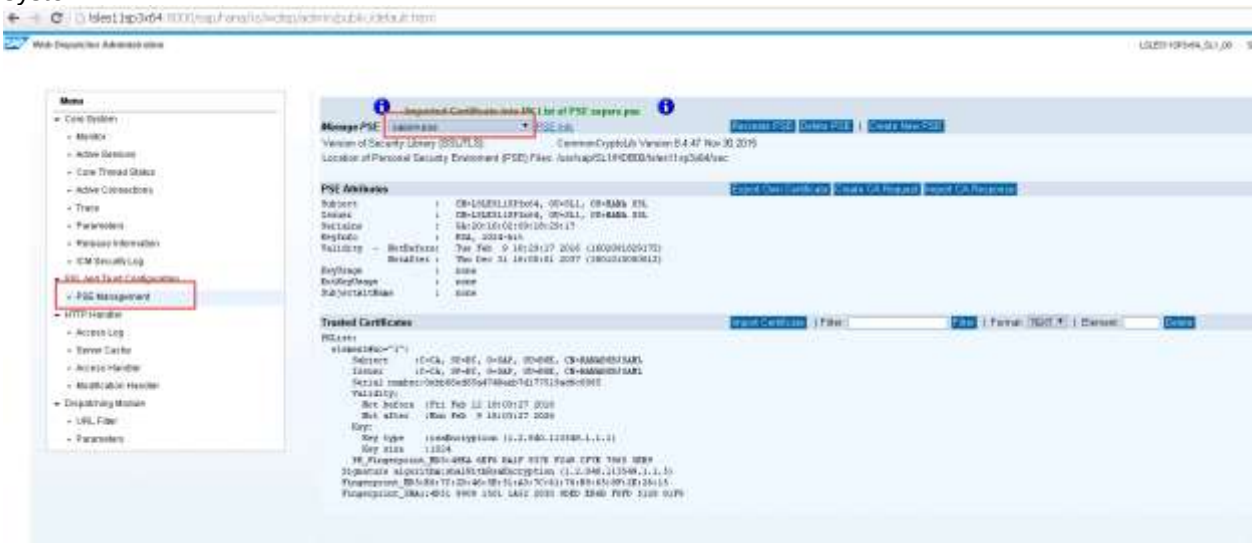
Example:



403 Forbidden Error?

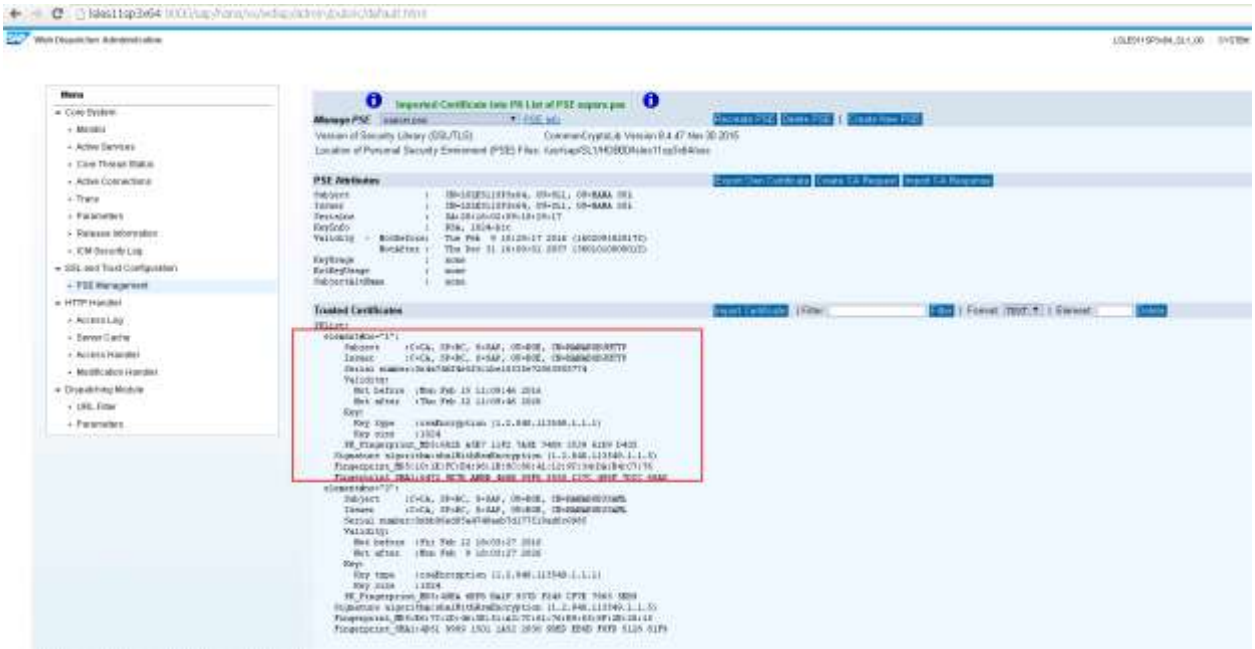
3. Select PSE Management on the left hand side
4. From the Manage PSE drop down menu, select sapsrv.pse

In the example screenshot, the sapsrv.pse already contains an existing certificate for the BI Platform system.



5. Select Import Certificate from the Trusted Certificates
6. Copy the certificate text from the certificate generated from the BI Platform CMC. Make sure to include the -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----

7. Select Import
8. The certificate should appear in the Trusted Certificates section

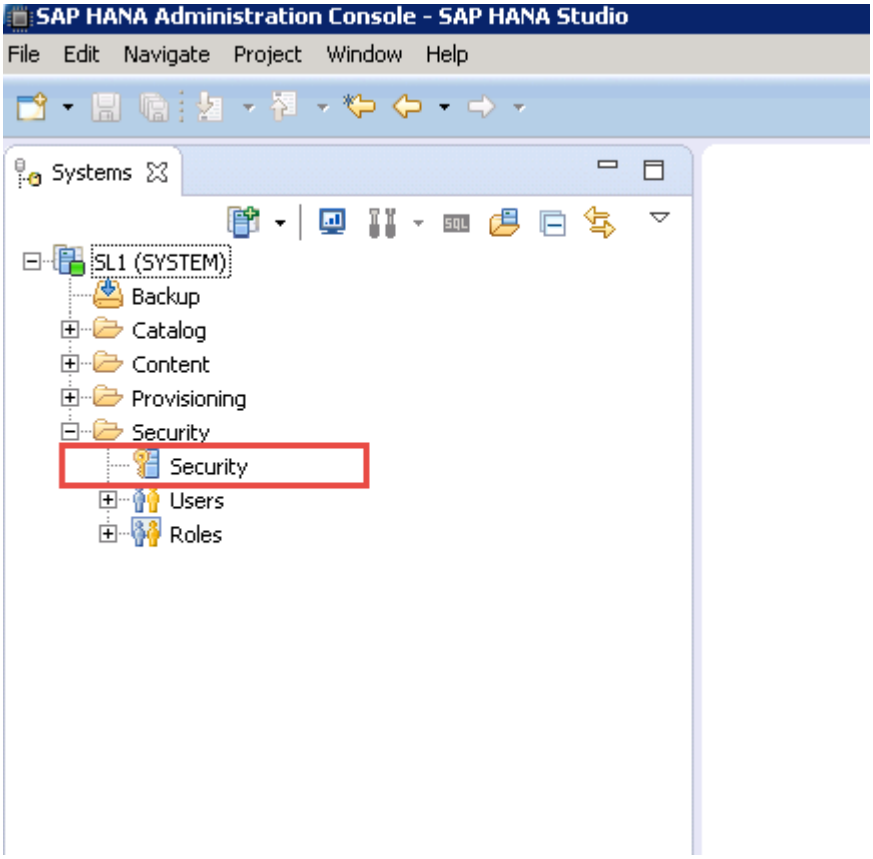


9. Restart the HANA system for these changes to take effect
10. This section is now complete.

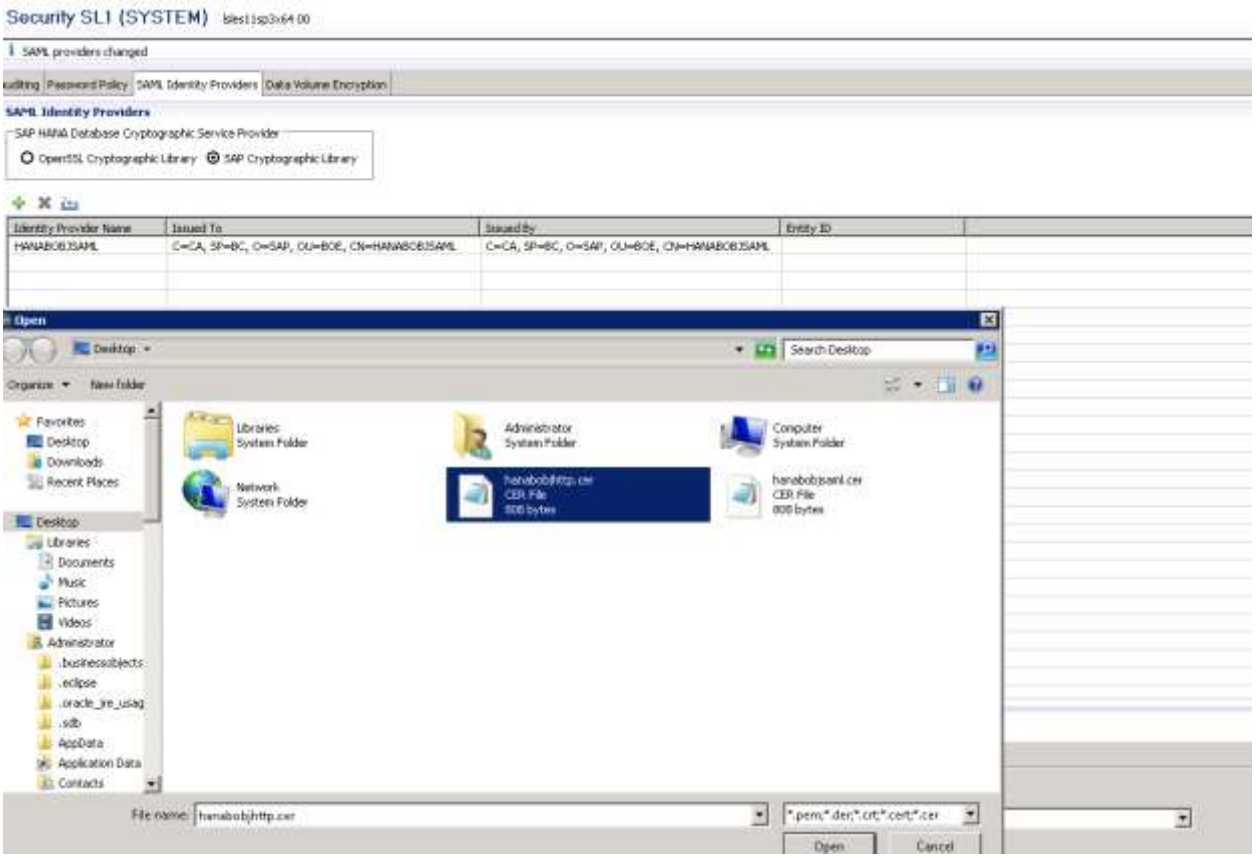
5.5 Import Certificate into HANA Security

The next step is to import the same certificate into HANA Security. This step is needed to create the SAML Identity Provider (IdP).

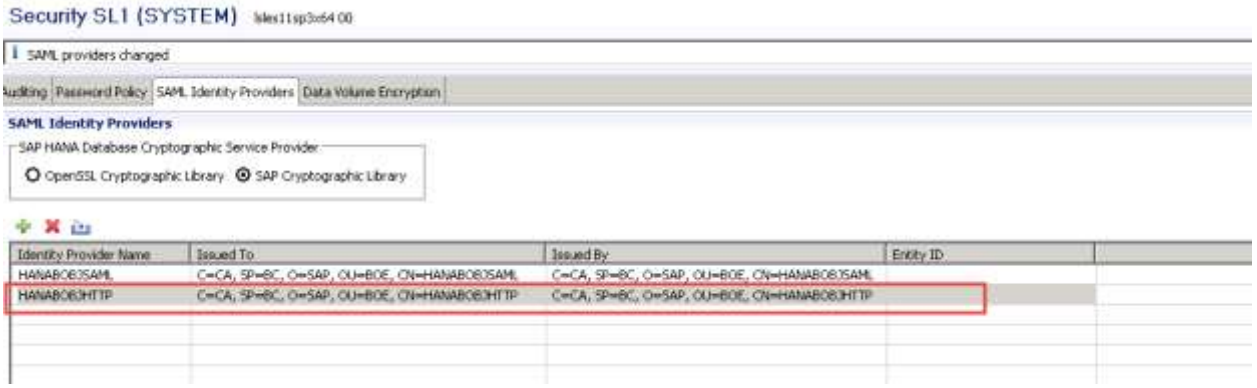
1. Open HANA Studio and Login to the HANA System using the SYSTEM user (or an equivalent user)
2. Expand Security Folder and then double click on Security



3. Select SAML Identity Providers tab and then select the Import button 
4. Locate the certificate file that was created earlier



5. Fill in the Identity Provider Name. This can be any name and does not have to match the CN name. The Entity ID is optional as well.

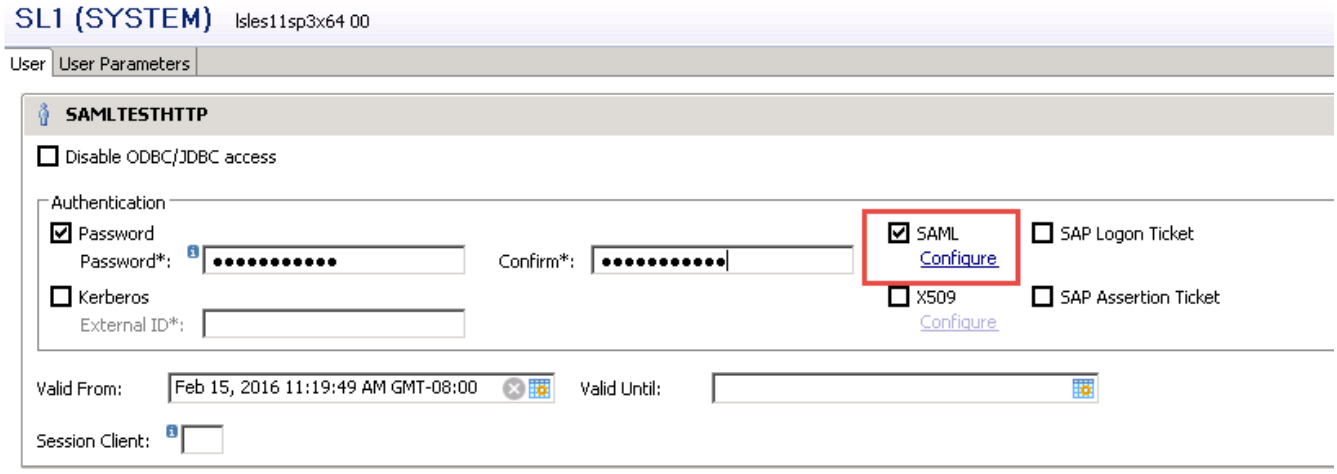


6. This section is now complete.

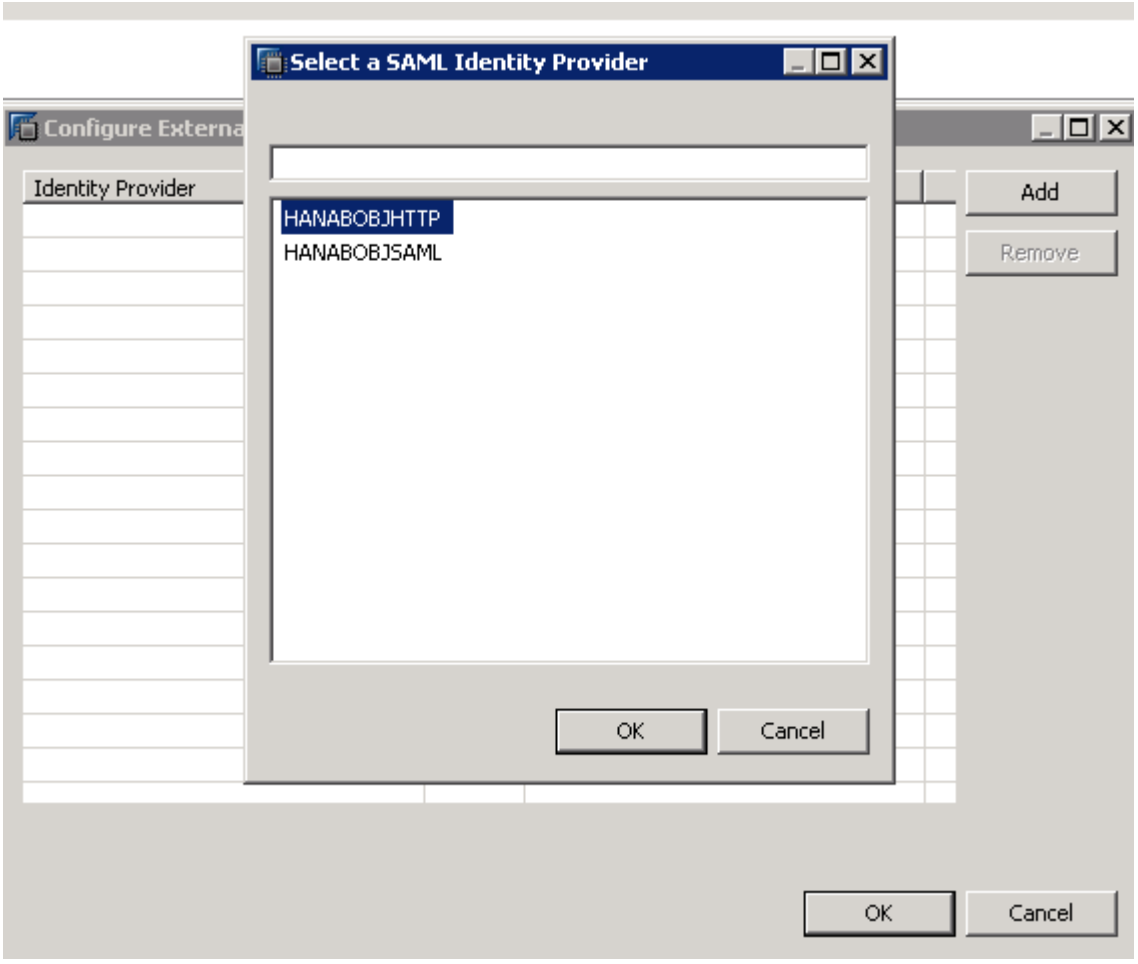
5.6 Create a HANA user with SAML

The certificate has been generated and imported into the truststore and also into HANA Security. The next step is to assign a HANA user to a BI Platform user.

1. Open HANA Studio and Login to the HANA System using the SYSTEM user (or an equivalent user)
2. Expand the Security folder and then right click Users and select New User
3. Specify a username and a password.
4. Select the check box SAML and then select on Configure.



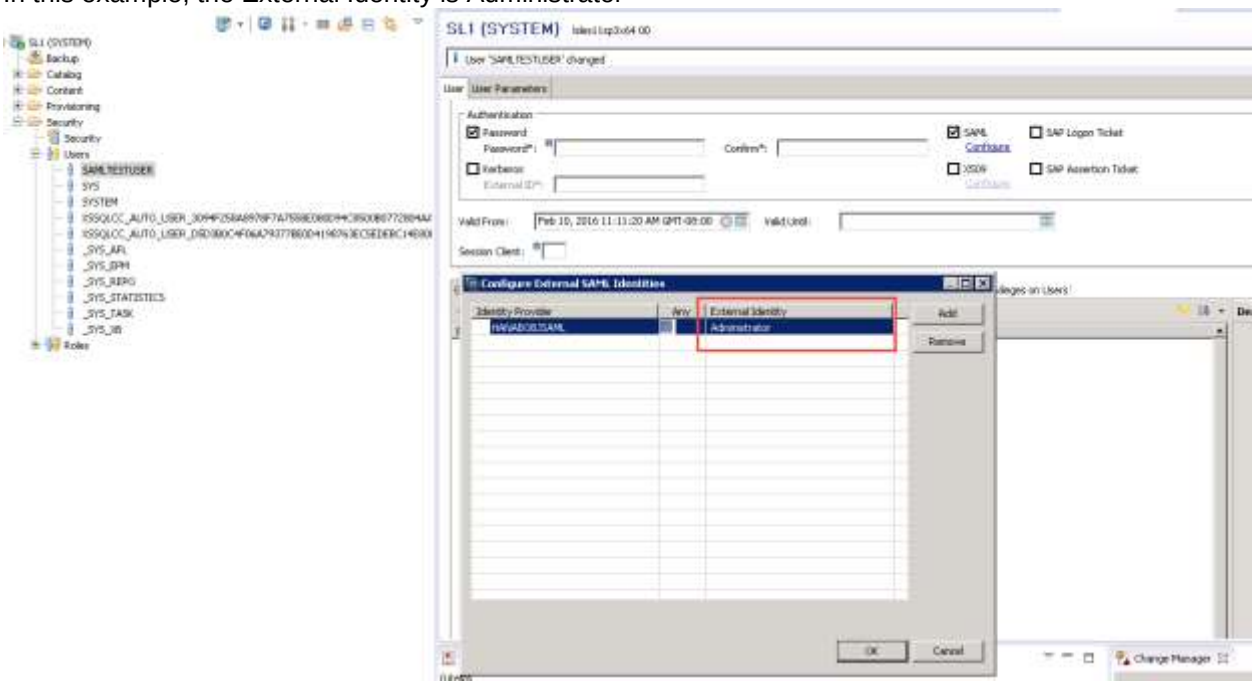
5. Select Add and there should be a list of SAML Identity Providers. Add the one which was created earlier and then select on OK.



6. There needs to be a BI Platform user hardcoded as the External Identity. In this example, Administrator is used but any BI Platform user could be used.

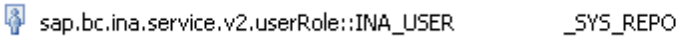
   Be aware the External Identity is case-sensitive.

In this example, the External Identity is Administrator



7. This user also needs the sap.bc.ina.service.v2.userRole::INA_USER role to access the HANA InA service.

   To add the role, in the Granted Roles tab, select the plus icon  and then add the role sap.bc.ina.service.v2.userRole::INA_USER

   Role doesn't exist?

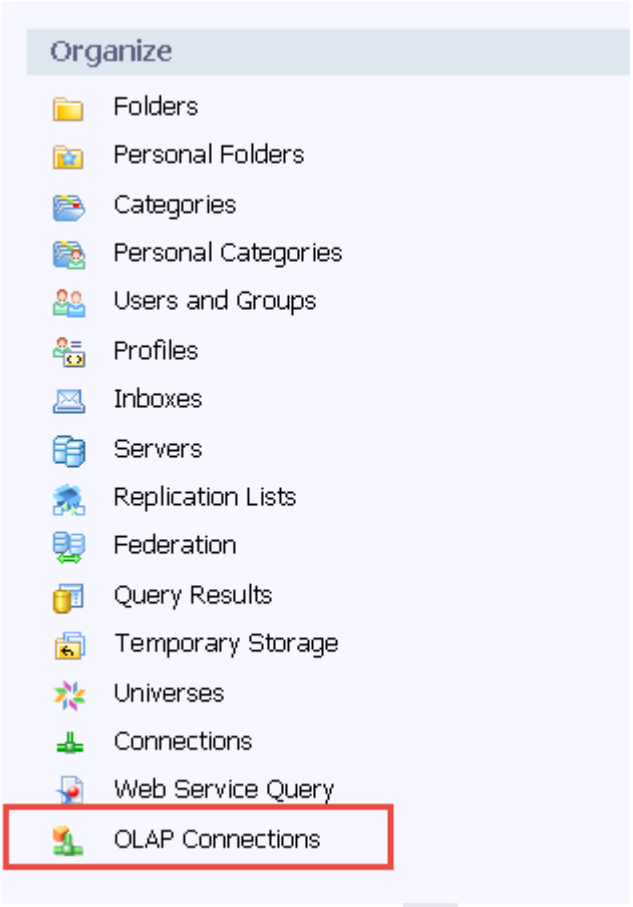
8. This section is now complete

5.7 Create OLAP Connection

The next section outlines the steps to create the OLAP connection

1. Open a browser and go to http://< Web Application Server >:< Web Application Server Port >/BOE/CMC

2. Go to CMC Home > OLAP Connections



3. Select on the New Connection icon 
4. A prompt appears for the connection details.

Input the following details and then save.

Name:	Name of the connection. Must be unique.
Description (Optional):	Optional
Provider	SAP HANA http to use the InA service.
Server Information:	http://<HANA System>:<Wdisp port> or https URL.
Connect to server to choose a cube:	Optional
Authentication	SSO
Associated Universe:	Optional

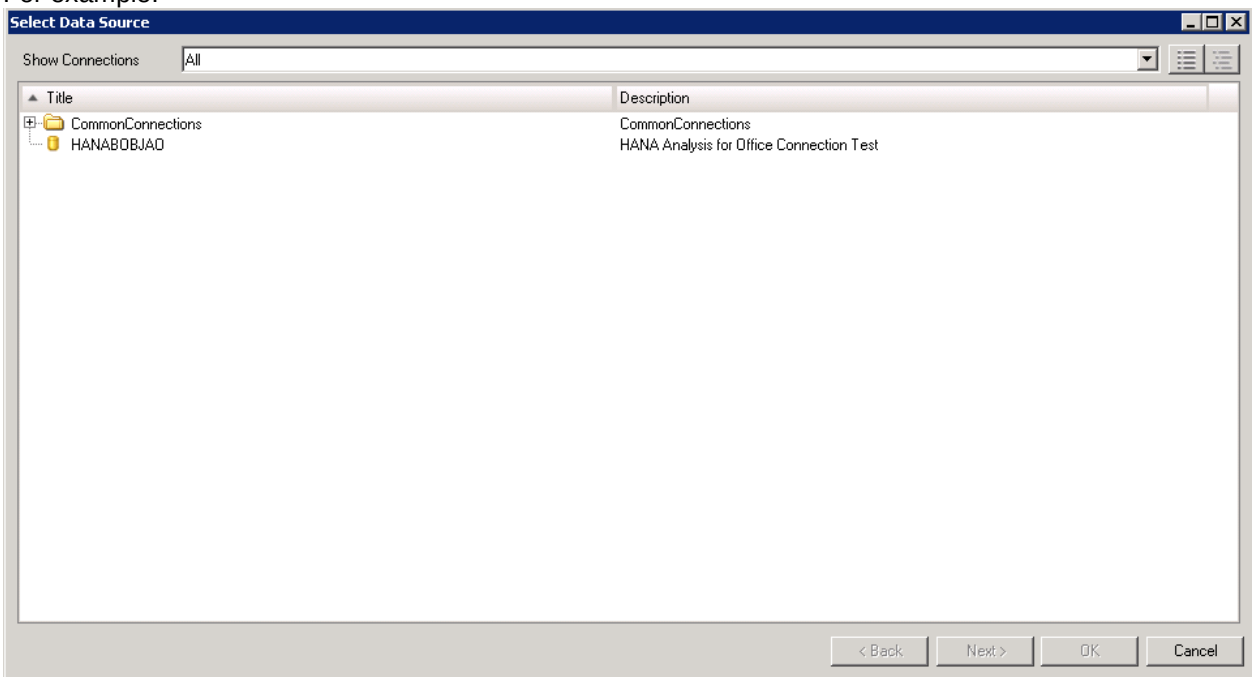
5. This section is now complete

5.8 Validation

The next step is to test the SSO through Analysis for Office 2.2.

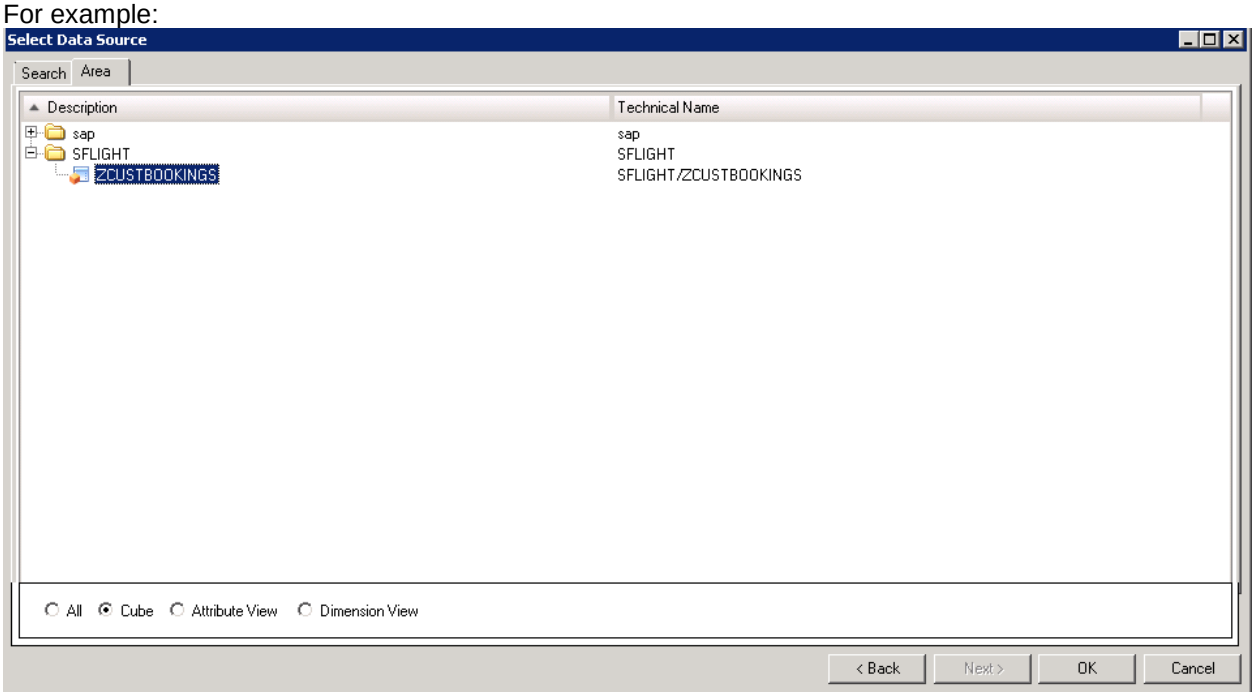
1. Start Analysis for Microsoft Excel
2. Select the Analysis tab
3. Select Insert Data Source and then from the drop down Select Data Source
4. When prompt to login to BI Platform. Input the username that was specified as the External Identity.
5. A list of OLAP connections will appear. Select the connection that was created earlier.

For example:



6. If SSO was setup correctly, the next window will appear with the tabs Search and Area. Open the Area tab and the HANA Content catalog will be displayed.

For example:



7. This section is now complete.

6 APPENDIX

6.1 Tracing

Debug tracing can be enabled to get more information on potential errors. Use this if there is an error not mentioned in this guide.

This tracing is more enhanced than the previous authentication tracing because the Analysis for Office 2.2 system will use the InA service which resides on the XS engine.

To enable debug tracing, follow the steps:

1. Open HANA Studio and Login using the SYSTEM user
2. Open SQL Editor and execute the command:

```
ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') set ('trace',
'authentication') = 'debug' with reconfigure;

ALTER SYSTEM ALTER CONFIGURATION ('xsengine.ini', 'SYSTEM') set ('trace',
'authentication') = 'debug' with reconfigure;

ALTER SYSTEM ALTER CONFIGURATION ('xsengine.ini', 'SYSTEM') set ('trace',
'xssession') = 'debug' with reconfigure;

ALTER SYSTEM ALTER CONFIGURATION ('xsengine.ini', 'SYSTEM') set ('trace',
'xsauthentication') = 'debug' with reconfigure;
```

3. Reproduce the error and then disable the trace by running the command:

```
ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') UNSET
('trace', 'authentication');

ALTER SYSTEM ALTER CONFIGURATION ('xsengine.ini', 'SYSTEM') UNSET ('trace',
'authentication');

ALTER SYSTEM ALTER CONFIGURATION ('xsengine.ini', 'SYSTEM') UNSET ('trace',
'xssession');

ALTER SYSTEM ALTER CONFIGURATION ('xsengine.ini', 'SYSTEM') UNSET ('trace',
'xsauthentication');
```

4. Go to the Administration tab in HANA Studio and select on Diagnosis Files.

5. There should be an updated indexserver trace file and an xsengine trace file. Both of these files are needed to troubleshoot this issue further.

6.2 Troubleshooting

6.2.1 Analyzing Traces

If the solution of an issue cannot be located, HANA debug traces are required (click here on how to enable the traces)

Specifically for SAML connections using the InA service, the traces are contained in the xsengine trace file. This is because the InA service is an xsengine application.

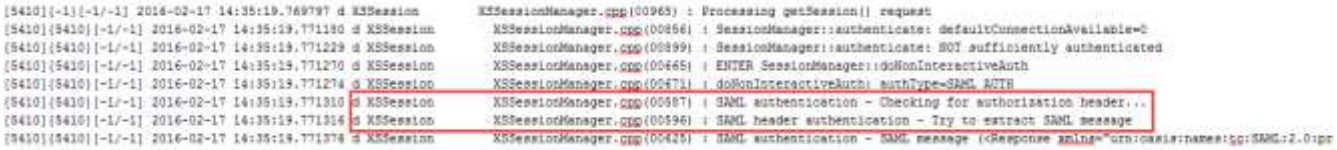
If the xsengine is in embedded mode (xsengine.ini > httpserver > embedded = true)

Here is an example of xsengine trace file analysis.

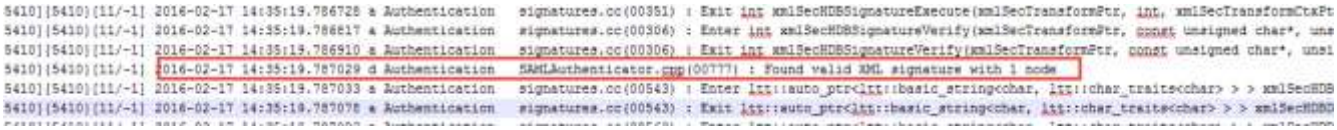
1) Open the indexserver trace file
2) To determine the exact time tracing was enabled search for “ALTER SYSTEM ALTER CONFIGURATION”.
   In this example, the tracing was enabled at roughly 2016-02-17 14:35:36

3) Open the xsengine trace file and only focus on the after this start time
4) Search for XSSession

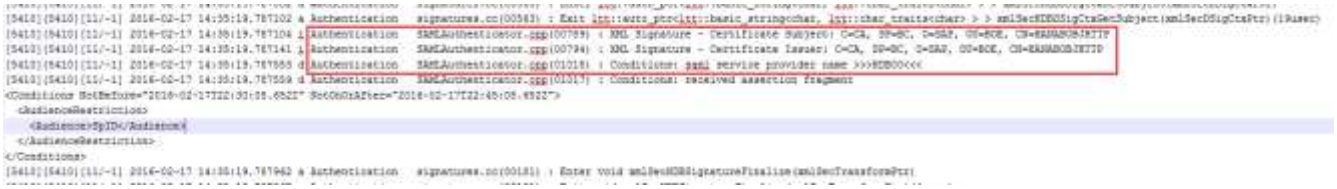
   In this example, the SAML assertion is being extracted from the header.



5) The header is extracted and then HANA will look for a matching certificate in the HANA Trust Store.



6) The HANA Trust Store certificate and saml service provider name is extracted.



7) The saml service provider name is compared to the incoming certificate (audience restriction)

```
[5410][5410][11/-1] 2016-02-17 14:35:19.787553 d Authentication   SAMLAuthenticator.cpp(01015) : Conditions: saml service provider name >>>HDB00<<<
[5410][5410][11/-1] 2016-02-17 14:35:19.787559 d Authentication   SAMLAuthenticator.cpp(01017) : Conditions: received assertion fragment
<Conditions NotBefore="2016-02-17T22:30:08.652Z" NotOnOrAfter="2016-02-17T22:45:08.652Z">
  <AudienceRestriction>
    <Audience>SpID</Audience>
  </AudienceRestriction>
</Conditions>
[5410][5410][11/-1] 2016-02-17 14:35:19.787962 a Authentication   signatures.cc(00181) : Enter void xmlSecHDBSignatureFinalize(xmlSecTransformPtr)
[5410][5410][11/-1] 2016-02-17 14:35:19.787967 a Authentication   signatures.cc(00181) : Exit void xmlSecHDBSignatureFinalize(xmlSecTransformPtr)(4usec
```

8) Authentication fails because of error “Assertion is not intended for this service provider”

9) The cause of the error is a SAML Service Provider Name mismatch

6.2.2 Restarting HANA

A restart of HANA is sometimes required after updating certificates and also if changes are made to the HANA configuration.

6.3 Common Errors

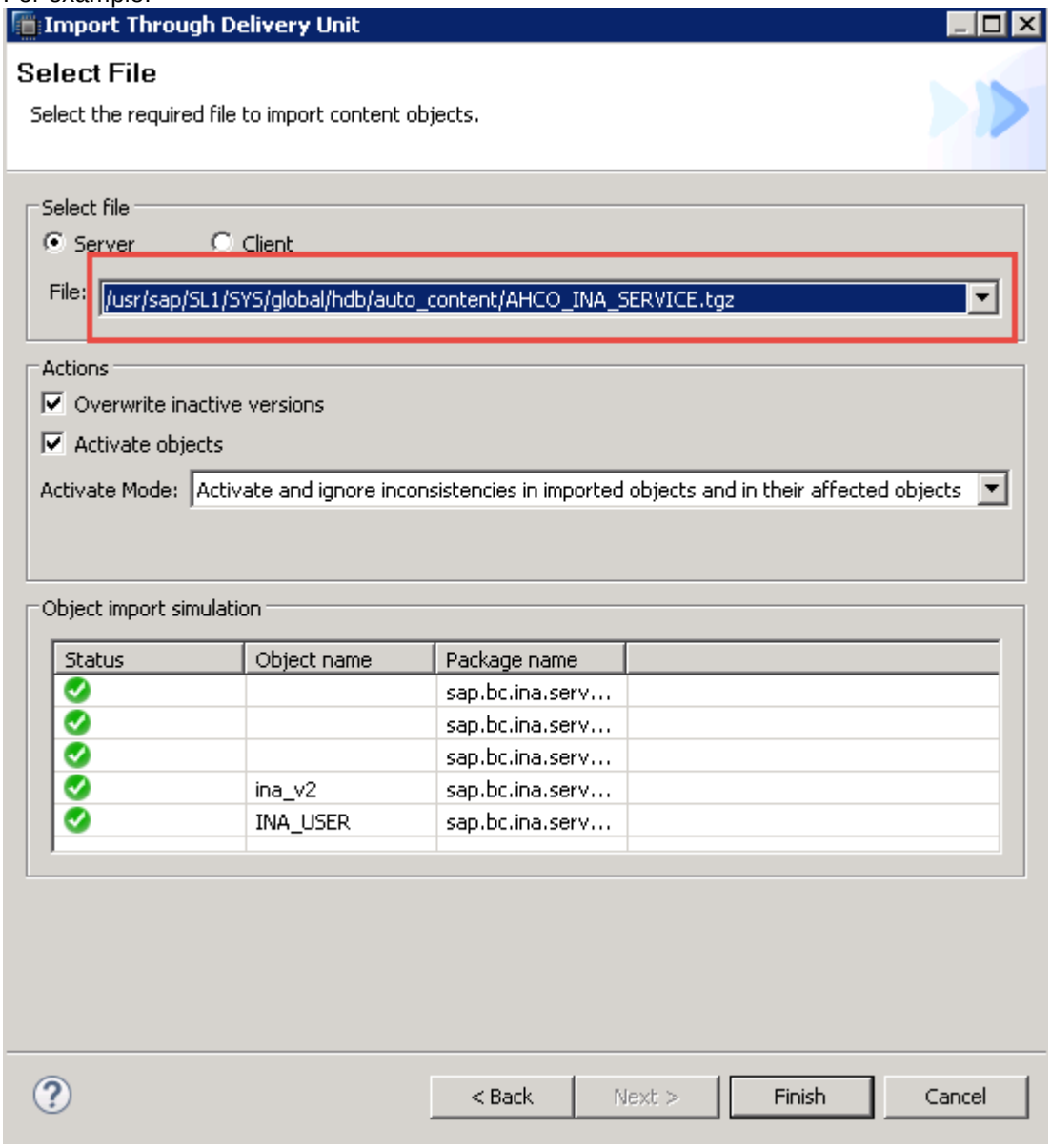
6.3.1 sap.bc.ina.service.v2.userRole::INA_USER does not exist.

The sap.bc.ina.service.v2.userRole::INA_USER role does not exist

Solution: The missing role is contained within a delivery unit. This delivery unit can be reimported again through these steps:

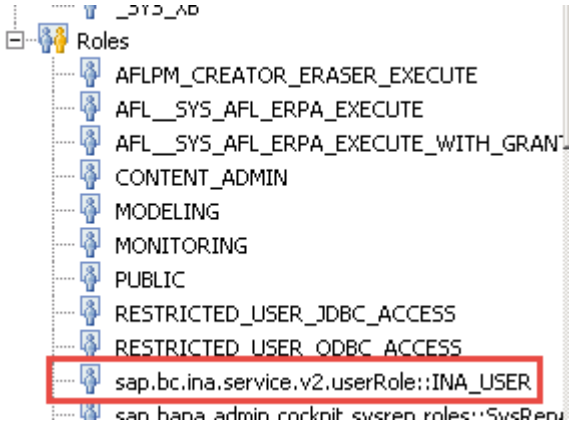
1. Go to HANA Studio and login using SYSTEM
2. Go to File > Import > Delivery Unit
3. Select the HANA System
4. Select the Server radio box and then from the drop down list, select xHCO_INA_SERVICE.tgz (The name of the delivery unit may be prefixed by another letter)

For example:



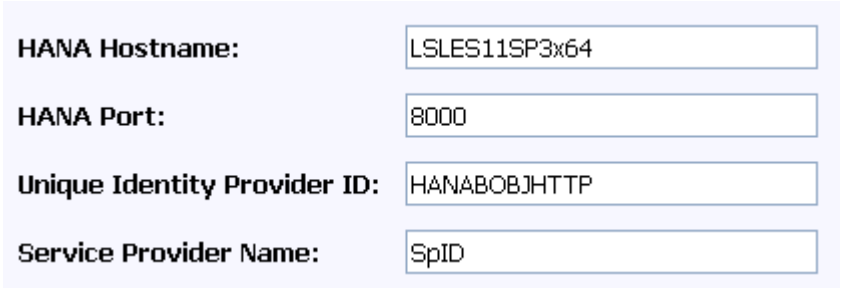
5. Select Finish

6. The role should now appear in Security > Roles



6.3.2 SAML Service Provider Name mismatch

During the step of creating a HANA certificate from the CMC. The value for Service Provider Name is not the same.



Does not match:

Solution: These two Service Provider names need to match. Change the saml_service_provider_name to match the certificate.

For example:

6.3.3 Error 403 Forbidden

When trying to access Web Dispatcher Admin Console, a 403 Forbidden error appears.

Solution: Grant the role sap.hana.xs.wdisp.admin::WebDispatcherAdmin role to the user trying to login.

6.3.4 Test Connection fails in the CMC

Connection Failed: The test of the HANA SSO ticket used to log onto the HANA DB has failed due to: [10]: authentication failed. (FWM 02133)

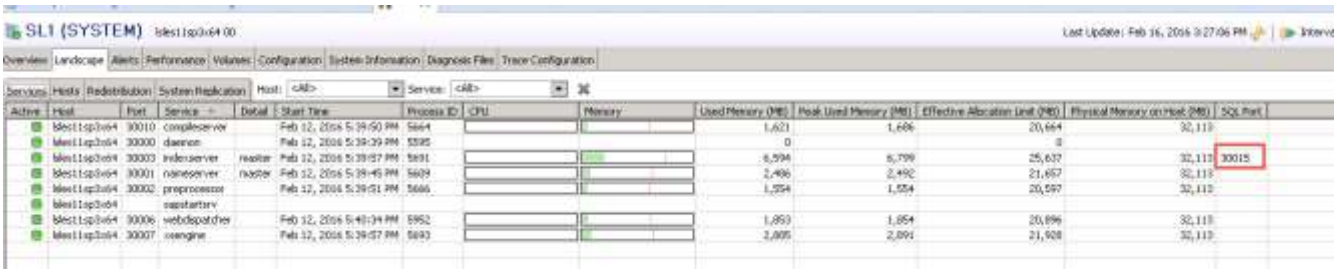
Solution:

- Make sure the case sensitivity is correct for the “External Identity” and the BI Platform user.
- After importing the certificate from SAP Web Dispatcher, the HANA system is restarted.

Connection Failed: The test of the HANA SSO ticket used to log onto the HANA DB has failed due to: SAP DBTech JDBC: Cannot connect to jdbc:sap://LSLES11SP3x64:30011/ [Cannot connect to host LSLES11SP3x64:30011 [Connection refused: connect], -813.].. (FWM 02133)

Solution: The BI Platform system cannot reach the HANA system. Make sure to check the following:

- Check if the firewall is blocking the connectity between BI Platform and SAP HANA System.
- Make sure the HANA port is the correct port. This is especially important when configuring SAML with a mult-tenant HANA system.



Connection Failed: All the servers with CMS BIPW08R2:6400, cluster @BIPW08R2:6400, kind pjs which host service null, are down or disabled

Solution: Do not use this test for HTTP/HTTPS connections. This will fail regardless of if SSO is setup correctly or not.
The test to validate if SSO is setup correctly is through Analysis for Office 2.2

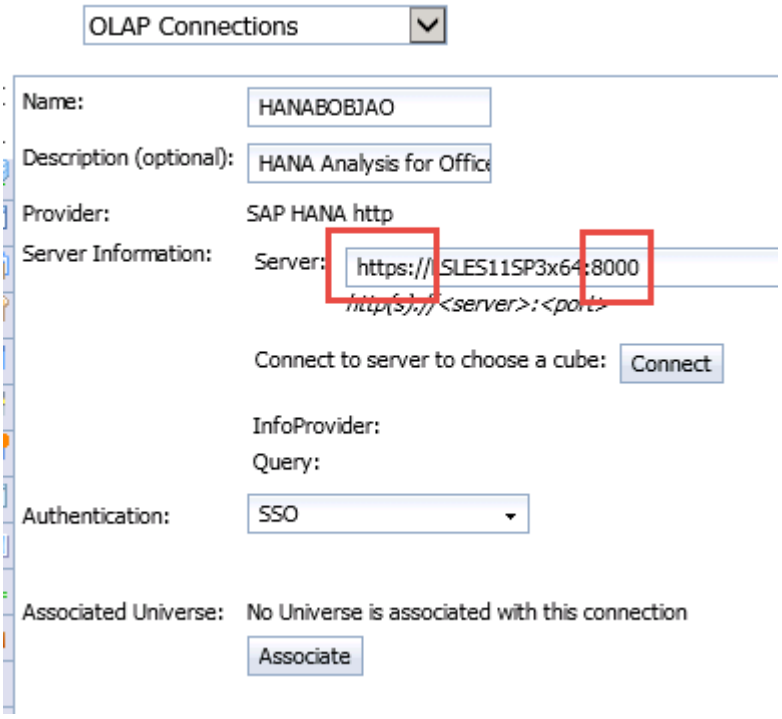
6.3.5 Single Sign On failed

When trying to SSO into the OLAP Connection, the following error “Single Sign On failed. Log on manually”.

Common Configuration Mistakes

- The HANA server URL is incorrect.
  The format of the URL should be: http(s)://<server>:<port>

  In the below example, the URL has https but the port is http port.



To validate that the URL is correct, open it in a browser and the following page should appear.

6.4 References and Notes

Referenced Document	Description
http://scn.sap.com/community/hana-in-memory/blog/2012/05/30/ssl-with-hana-and-bi4-feature-pack-3	Configuring openssl with HANA and BI 4
http://scn.sap.com/community/hana-in-memory/blog/2013/08/01/configuring-saml-with-sap-hana-and-sap-businessobjects-41--part-1	Configuring SAML SSO with HANA and BI 4.1
http://scn.sap.com/community/hana-in-memory/blog/2014/10/24/setup-saml-sso-from-bi-to-hana-using-sap-crypto-libraries	Configuring SAML with CommonCrypto and BI 4.1
1718944 - SAP HANA DB: Securing External SQL Communication (CommonCryptoLib)	Setup SSL on a HANA system.
2087537 - How to Configure SAML SSO Between HANA DB and Business Intelligence using CommonCrypto	Configuration Steps of HANA and BI
1900023 - How to setup SAML SSO to HANA from BI	Known issues and setup guide for HANA and BI with SAML SSO