# How to Configure Single Sign-On with SAP HANA using SAML and SAP BusinessObjects BI Platform 4.1

**Applicable Releases:**

**SAP HANA SPS10 and above**
**SAP BusinessObjects BI Platform 4.1 SP6 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. The steps appear will work with |

# 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 BI Platform 4.1 (BI Platform) 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

# 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.

# 5 STEP-BY-STEP CONFIGURATION

## 5.1 Overview

To setup SAML authentication, 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:

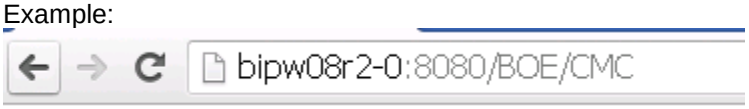
1. Import the certificate into the HANA Security
2. Configure a SAML user with an external identity user
3. Test the connection

## 5.2 Generate a Certificate from BI Platform

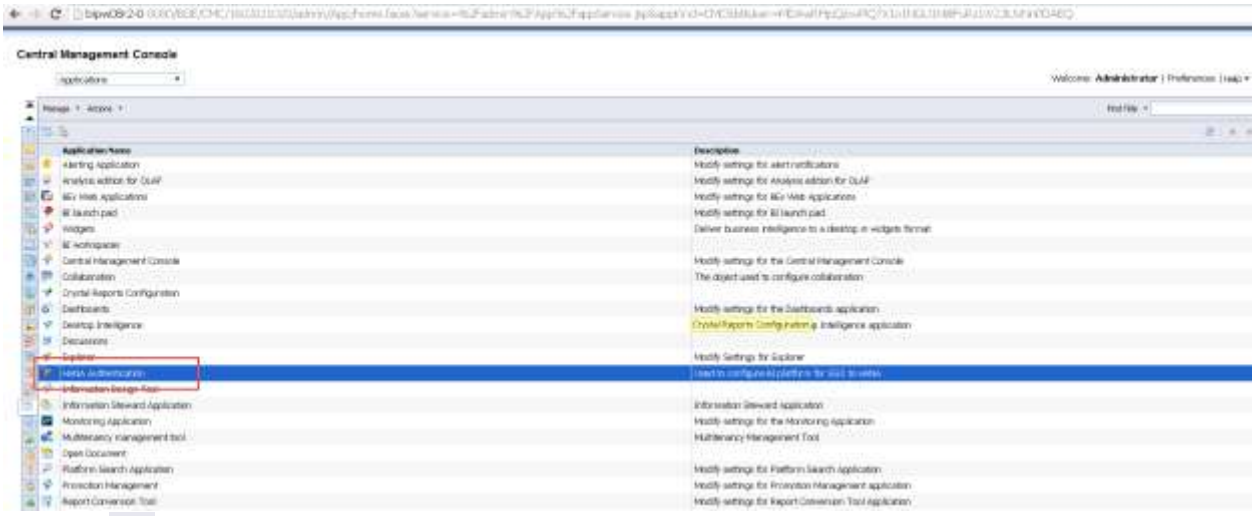
Generating a HANA certificate is performed through the BI Platform Central Management Console (CMC).

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

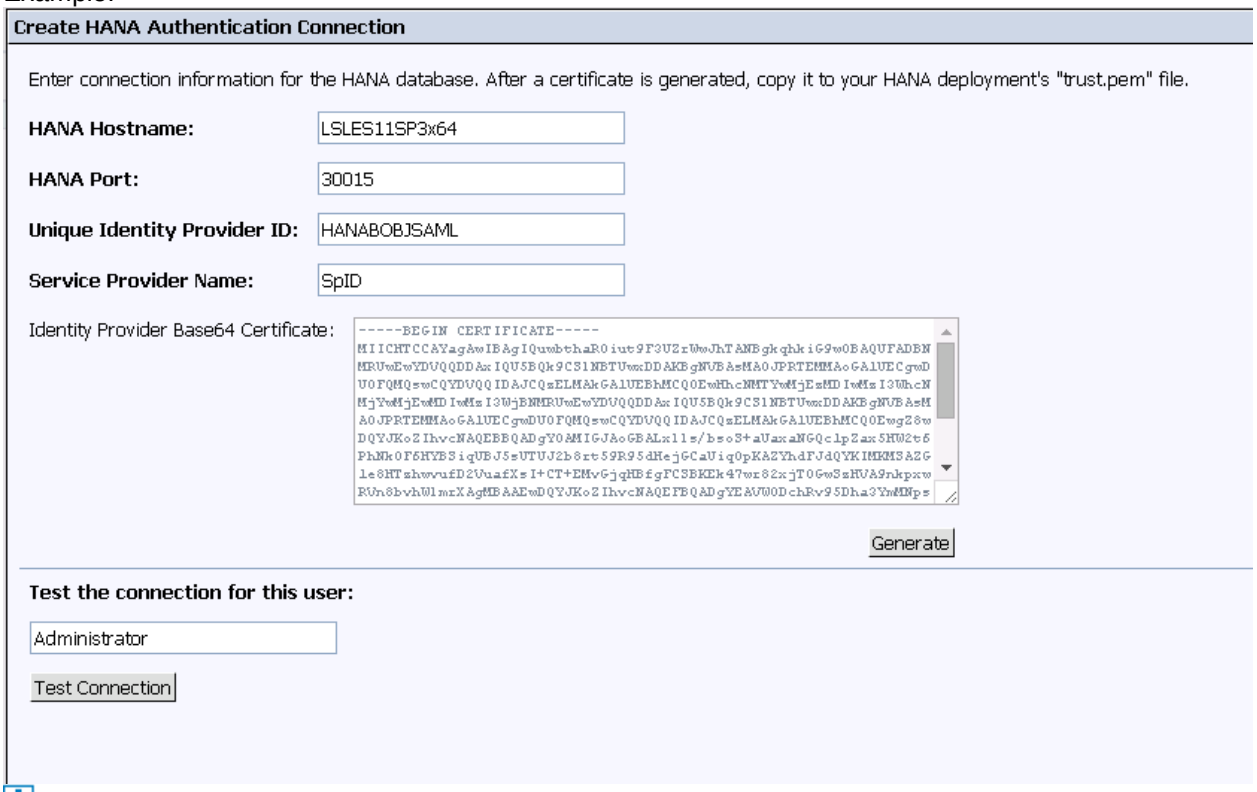



3. Select the  icon to create a new connection
4. Input the HANA details:

| | |
|---|---|
| HANA Hostname | Hostname of the SAP HANA Database system |

| | |
|---|---|
| HANA Port | SQL Port for the HANA indexserver. HANA Studio > Administration |
| Unique Identifier Provider ID: | Unique Name of the certificate |
| Service Provider Name: | Configuration setting (default is SpID).<br><br>This should match the parameter<br>indexserver.ini > [authentication] > saml_service_provider_name<br><br>Service Provider Name mismatch? |

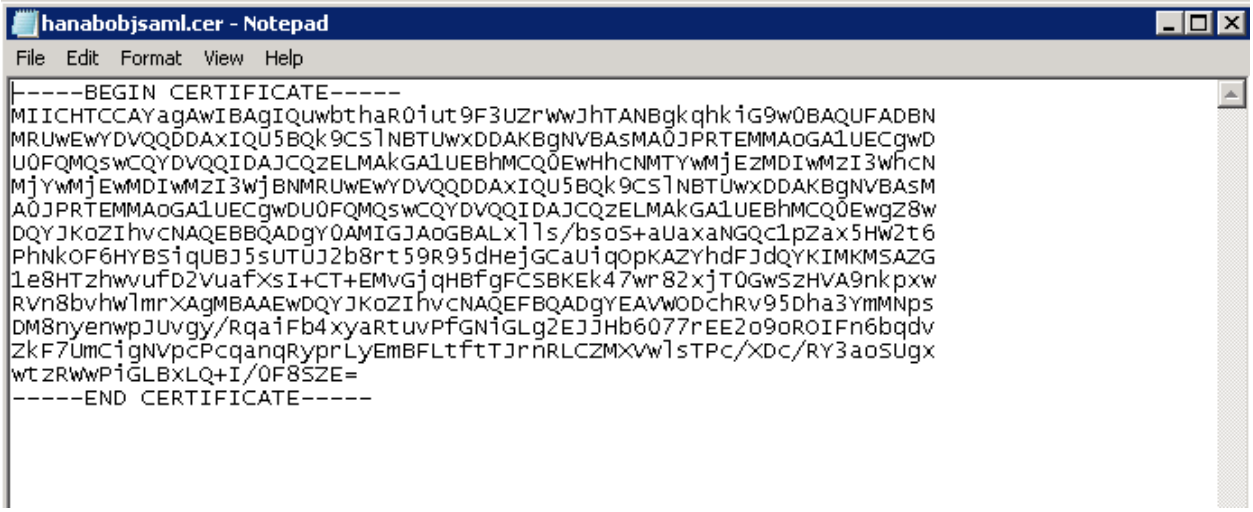
Example:




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.

5. Select Generate and 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.

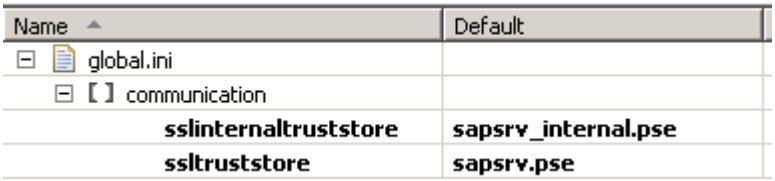
Example:




1. This section is now complete

### 5.3 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

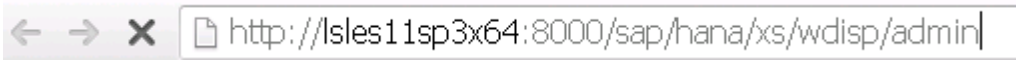
There are two methods of importing the certificate into the trust store:

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

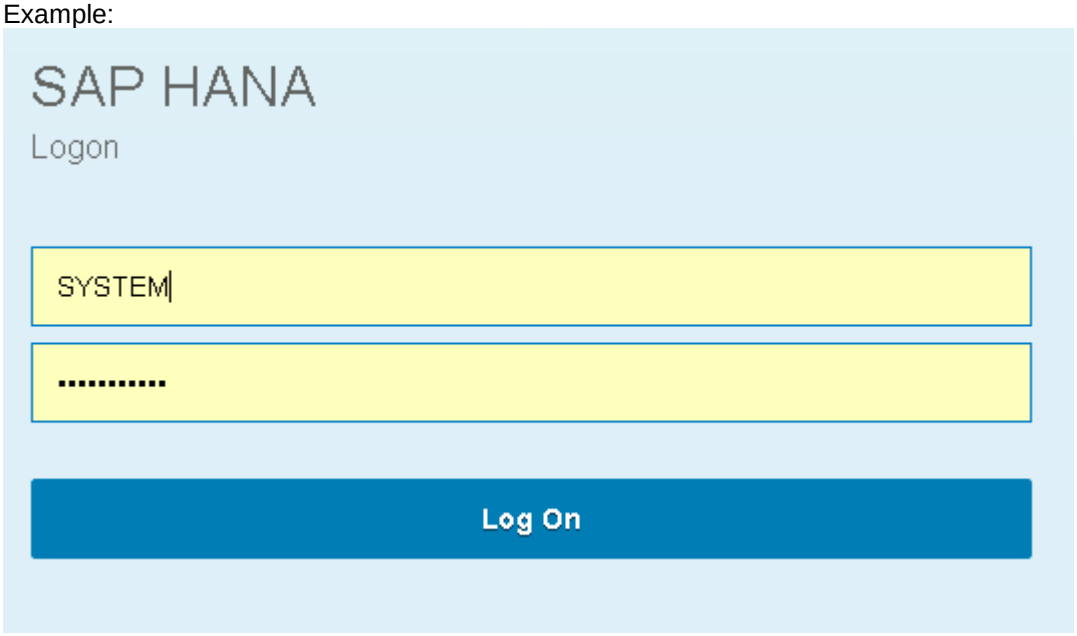
1. Access the Web Dispatcher Administration page by going to this location:

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



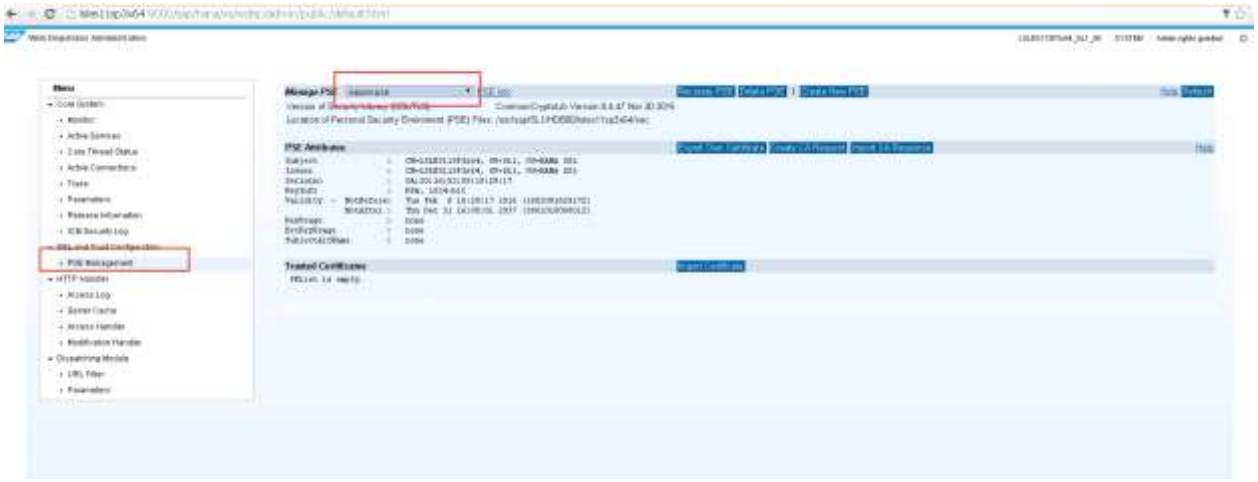
2. Login with a HANA user (In this case, the SYSTEM user)

Example:

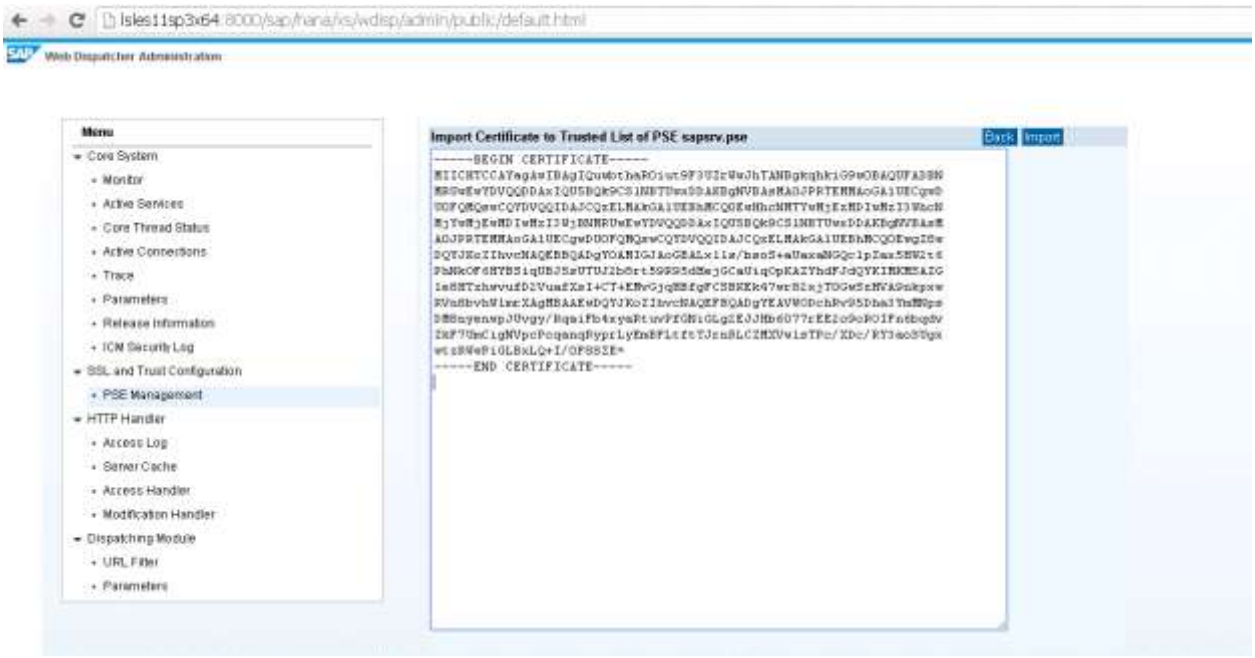



403 Forbidden Error?

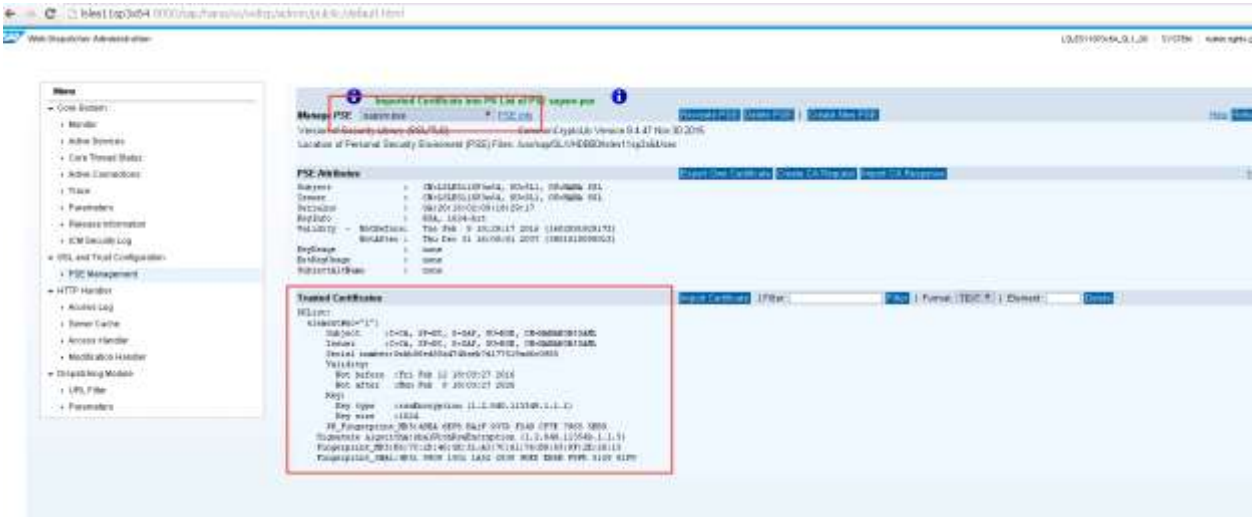
3. Select PSE Management on the left hand side
4. From the Manage PSE drop down menu, select sapsrv.pse



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

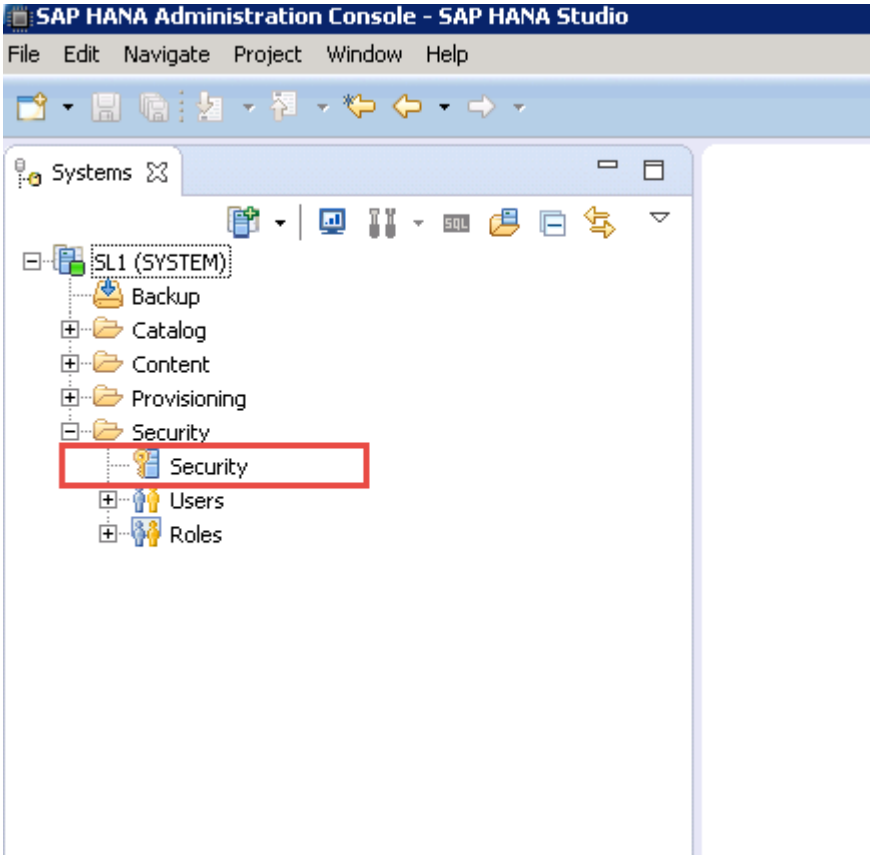


9. Restart the HANA system for these changes to take effect
10. This section is now complete.

### 5.4 Import Certificate into HANA Security

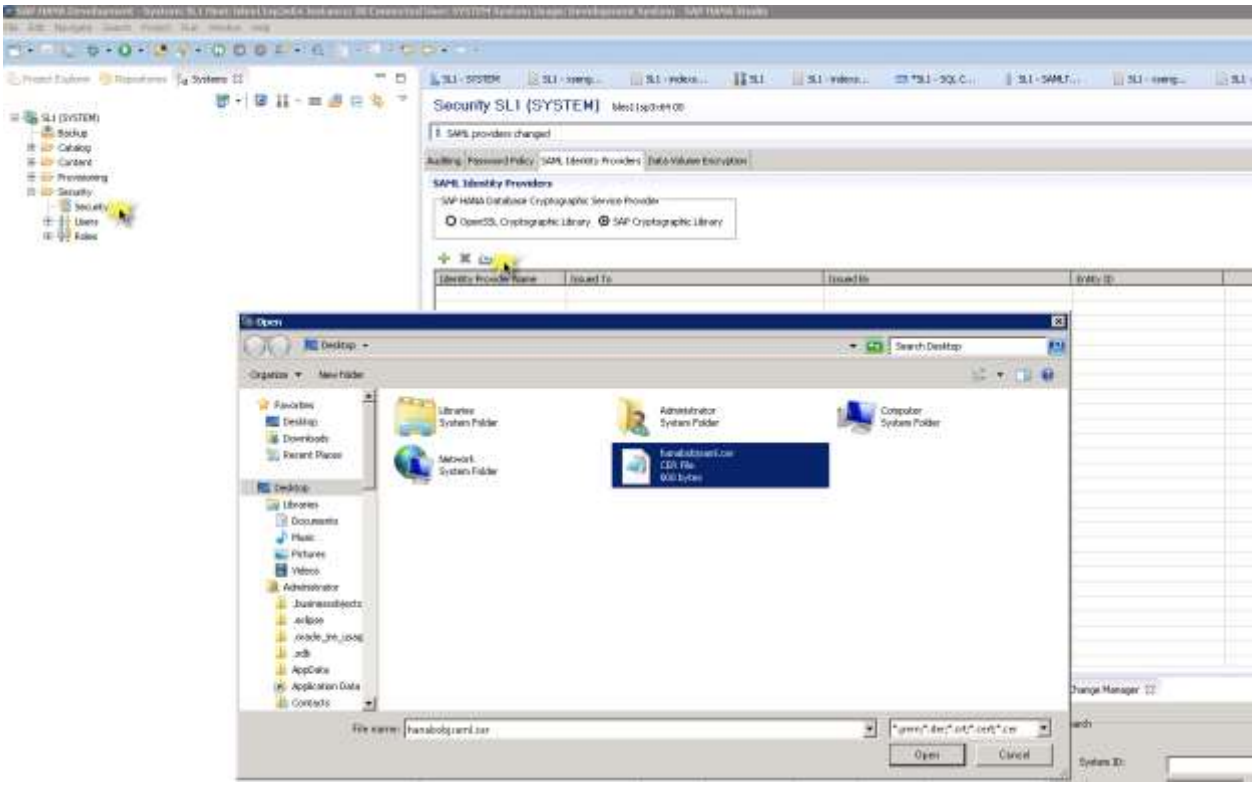
The next step is to import the same certificate into HANA Security. This step is needed to create the SAML Identity Provider (IdP).

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




3. Select the SAML Identity Providers tab and select the Import button 

4. Locate the certificate file that was created earlier



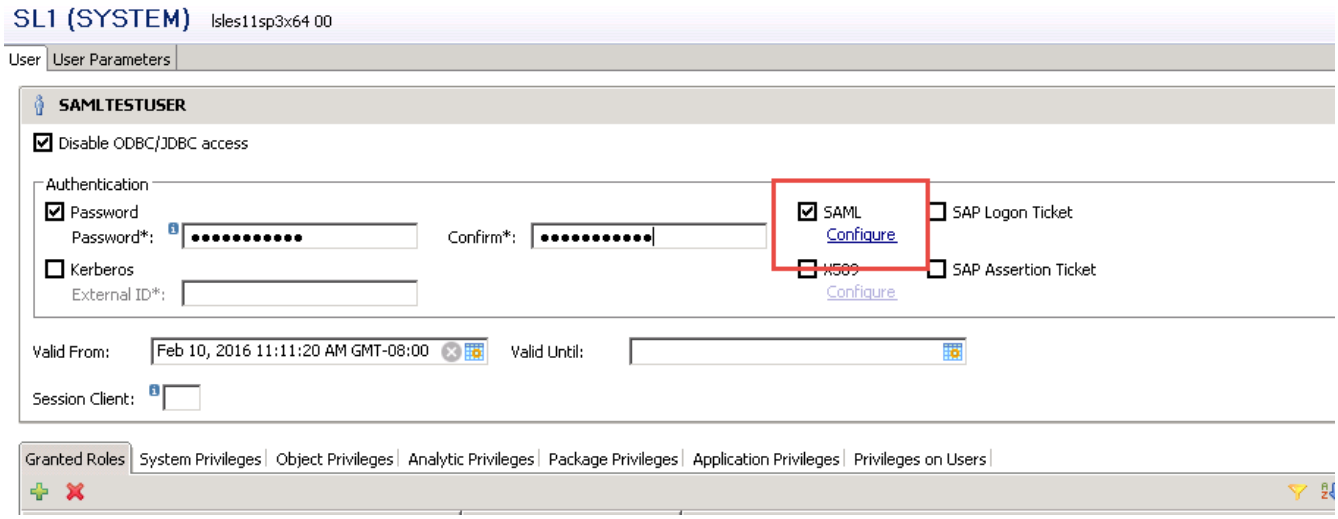

5. Fill in the Identity Provider Name. This can be any name and does not have to match the CN name. The Entity ID is optional as well.


6. This section is now complete.

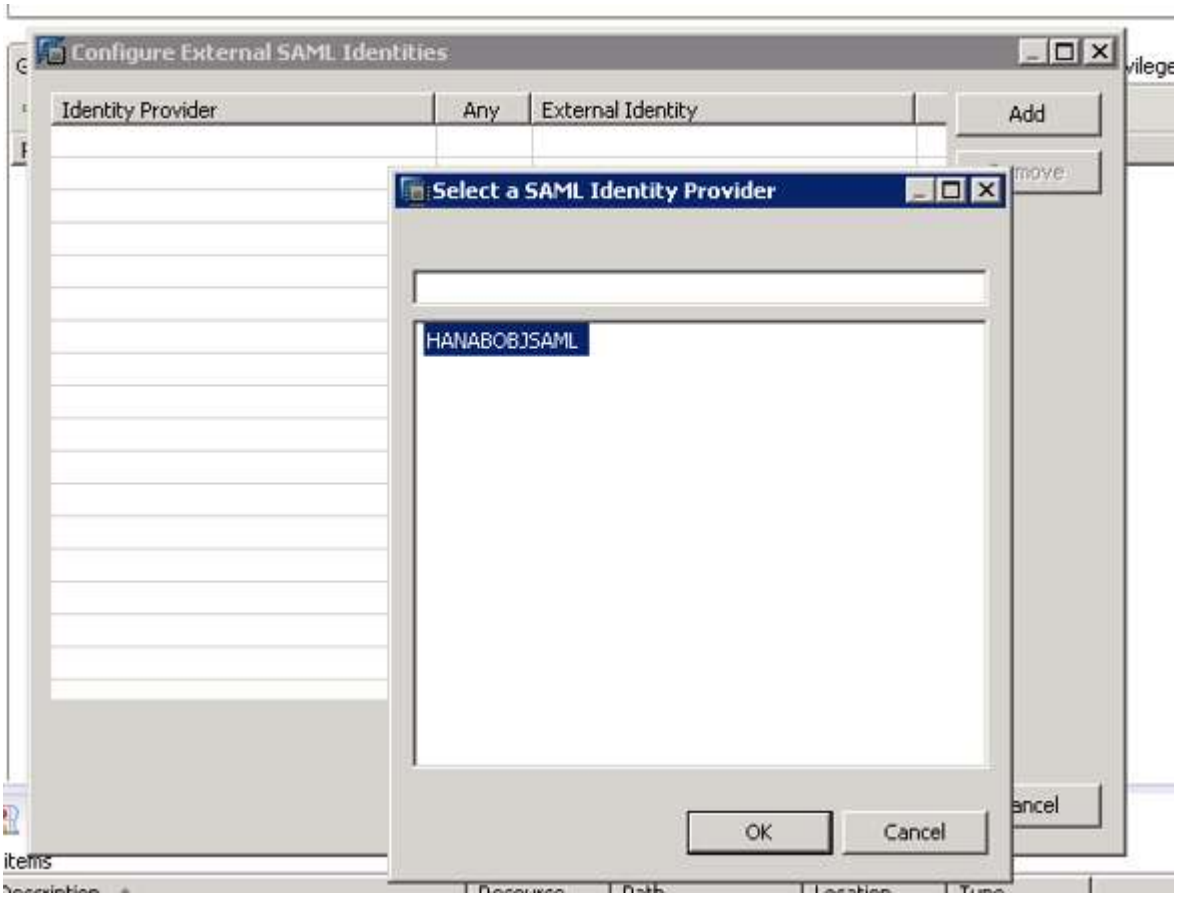
### 5.5 Create a HANA user with SAML

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 right click Users and select New User
3. Specify a username and a password.
4. Select the check box SAML and select Configure.



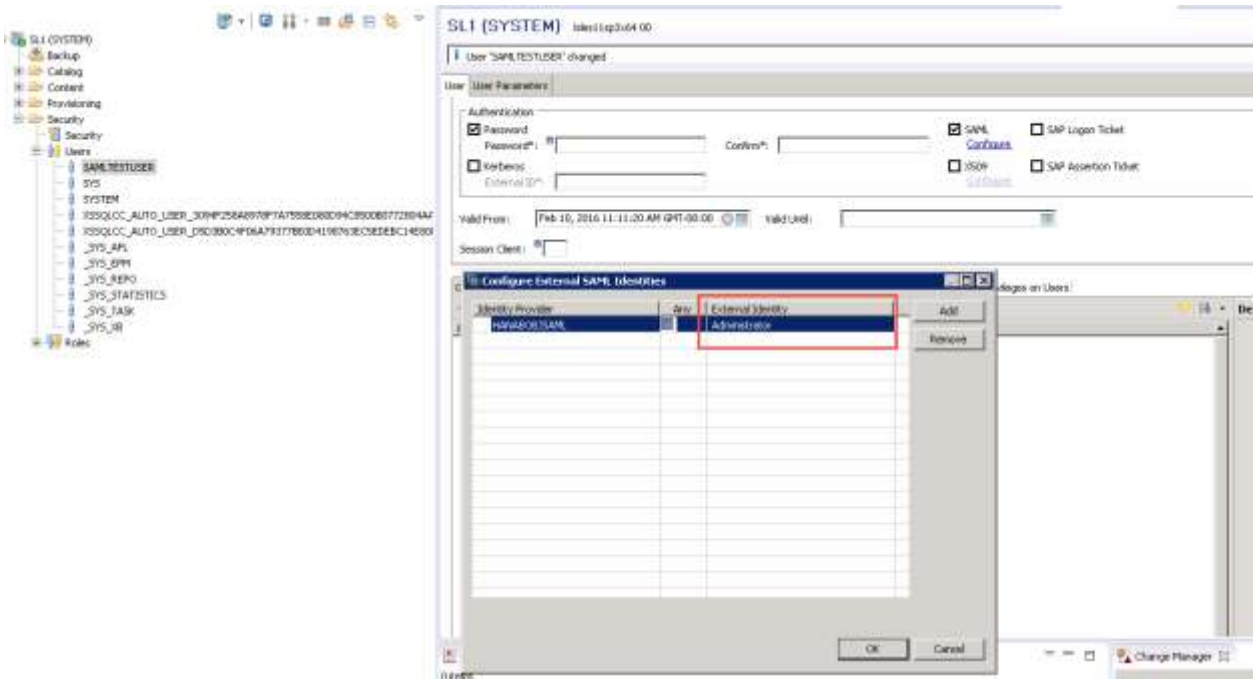

5. Select Add and there should be the SAML Identity Provider in the list.




6. Add an External Identity.

    - The External Identity is the username from the BI Platform system
    - This name is case sensitive

    In this example, Administrator is used.

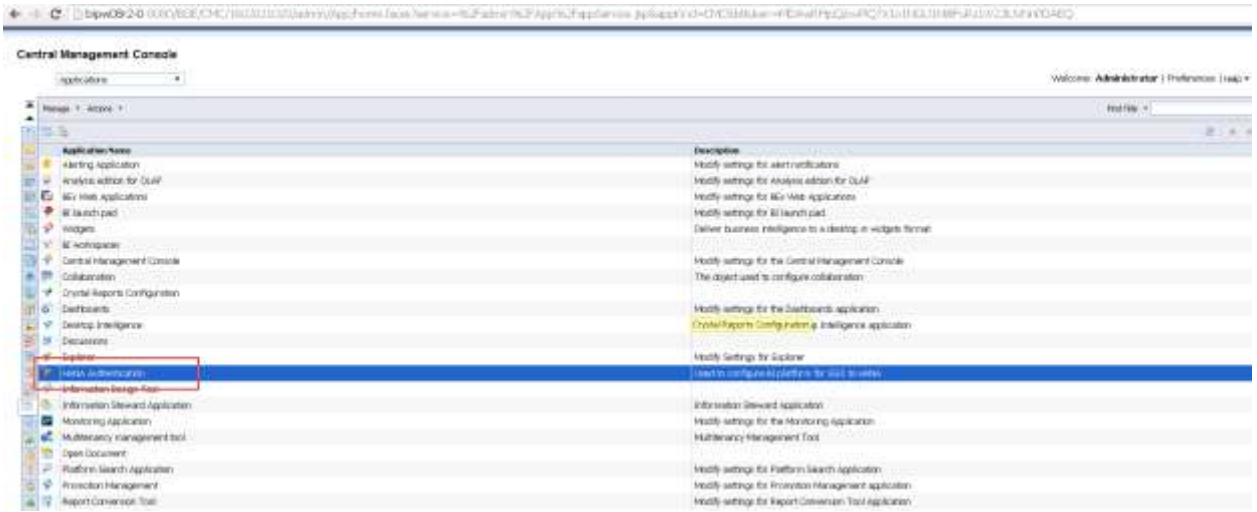



7. This section is now complete

### 5.6 Validation

The next section outlines the steps to validate that the SSO is working.

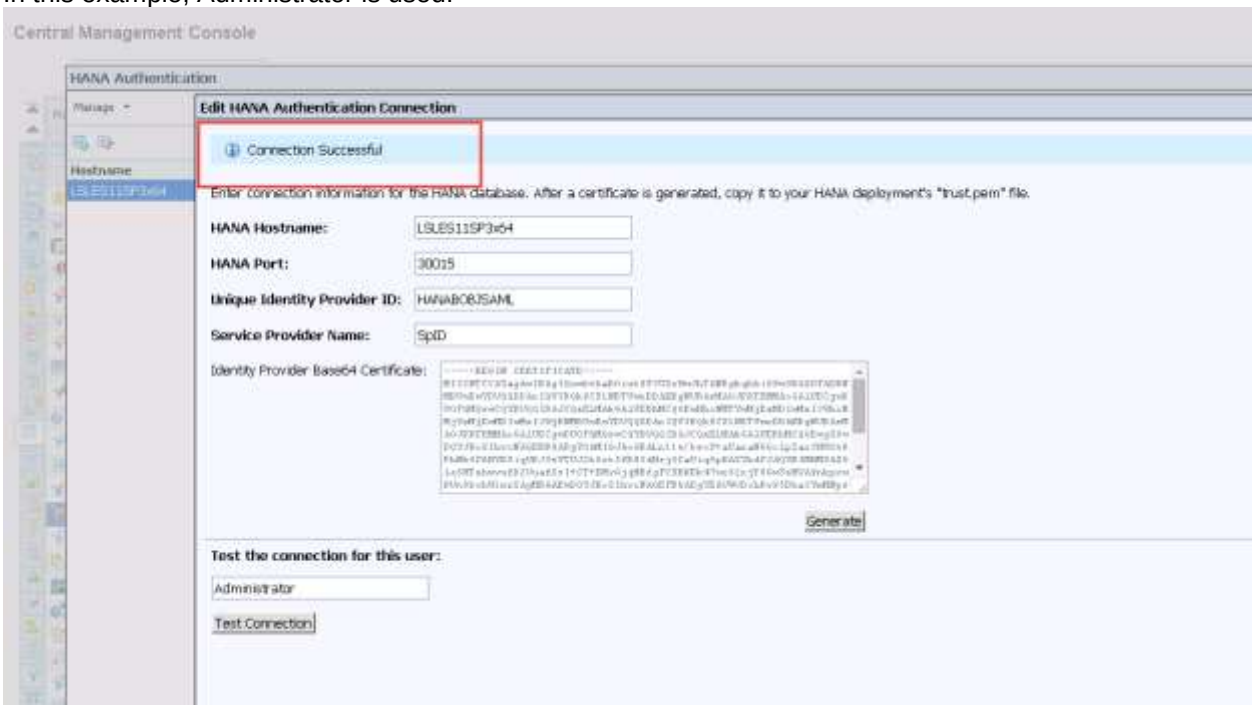
1. Open a browser and go to http://< Web Application Server >:< Web Application Server Port >/BOE/CMC
2. Go to CMC Home > Applications > HANA Authentication




3. Open the existing connection that was created earlier

4. Specify the username to test.

   This user must match the External Identity user that was configured earlier.
   In this example, Administrator is used.

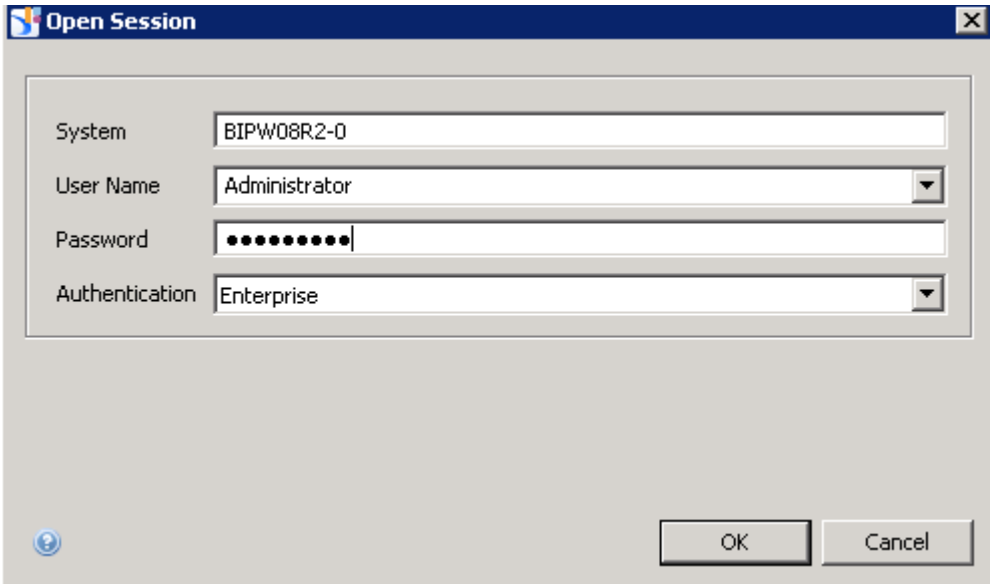



5. If SSO is configured correctly, the message “Connection Successful” will be shown.

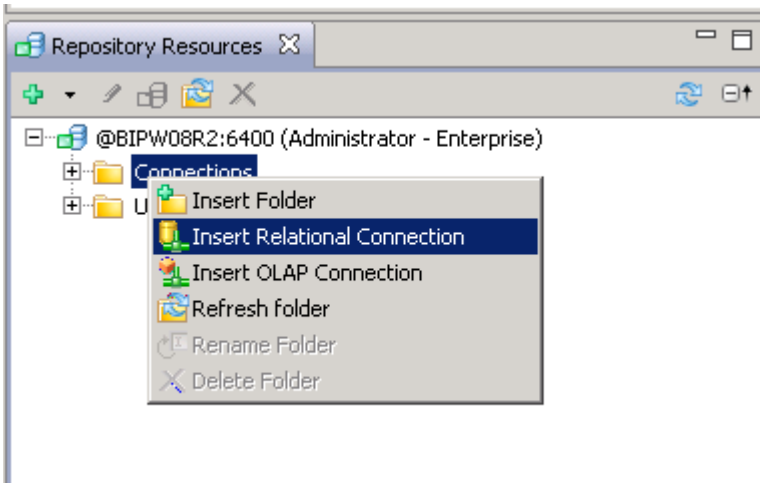
   Connection Failed error?

The next test will validate the BI Platform client tools.

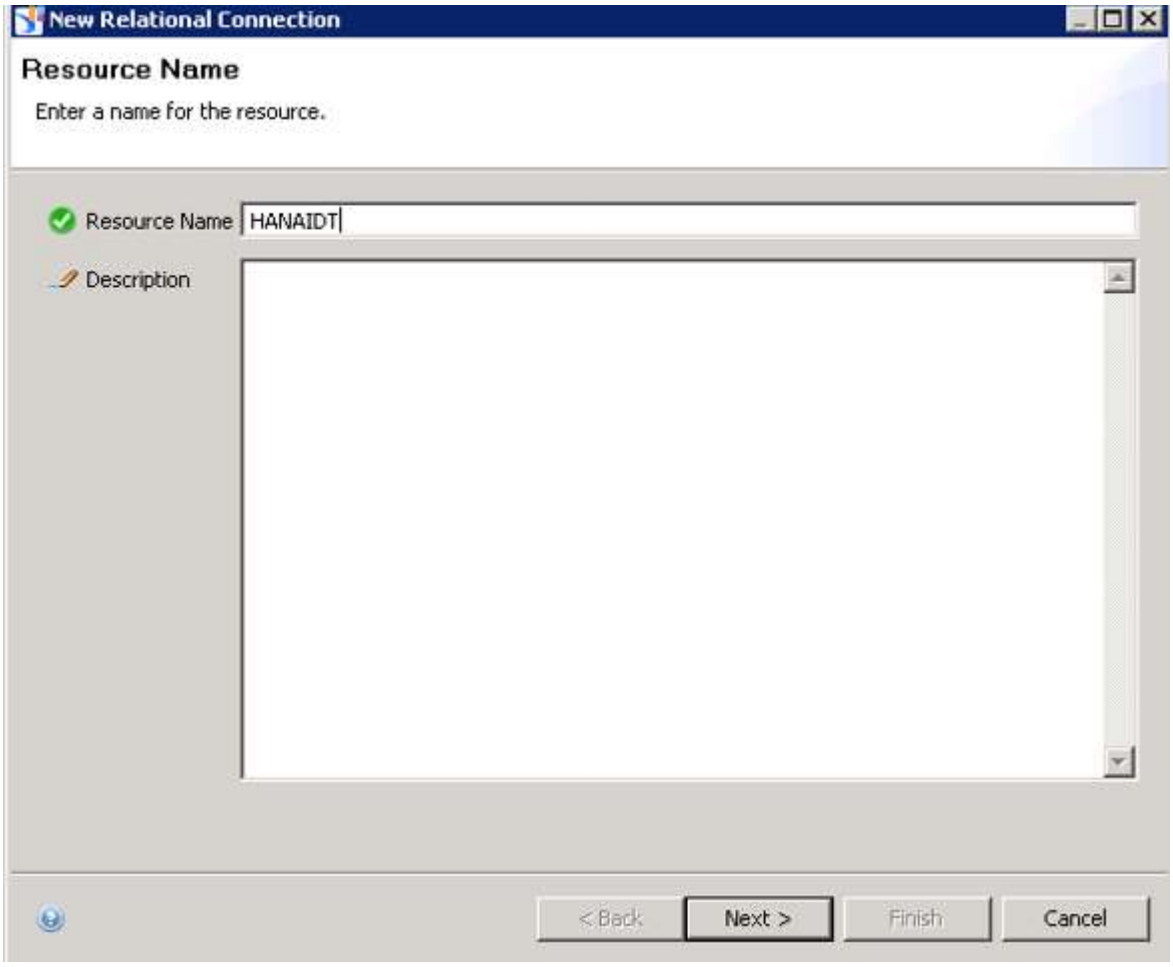
1. Start Information Design Tool (IDT)
2. In the Repository Resources section on the left bottom corner, Select the plus icon and select Insert Session.
3. When prompted to login to BI Platform. Input the username that was specified as the SAML External Identity



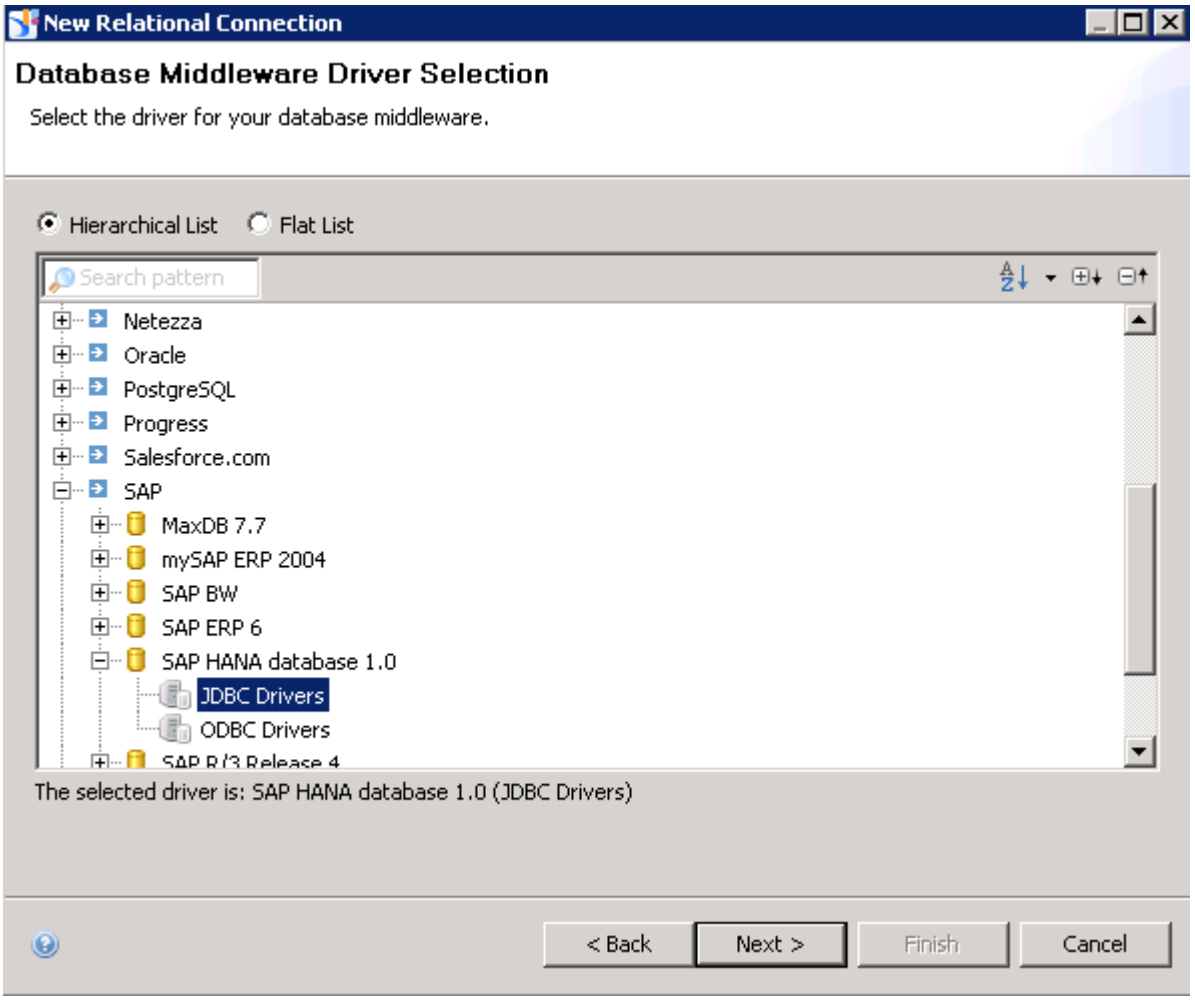

4. Right click connections and select Insert Relational Connection



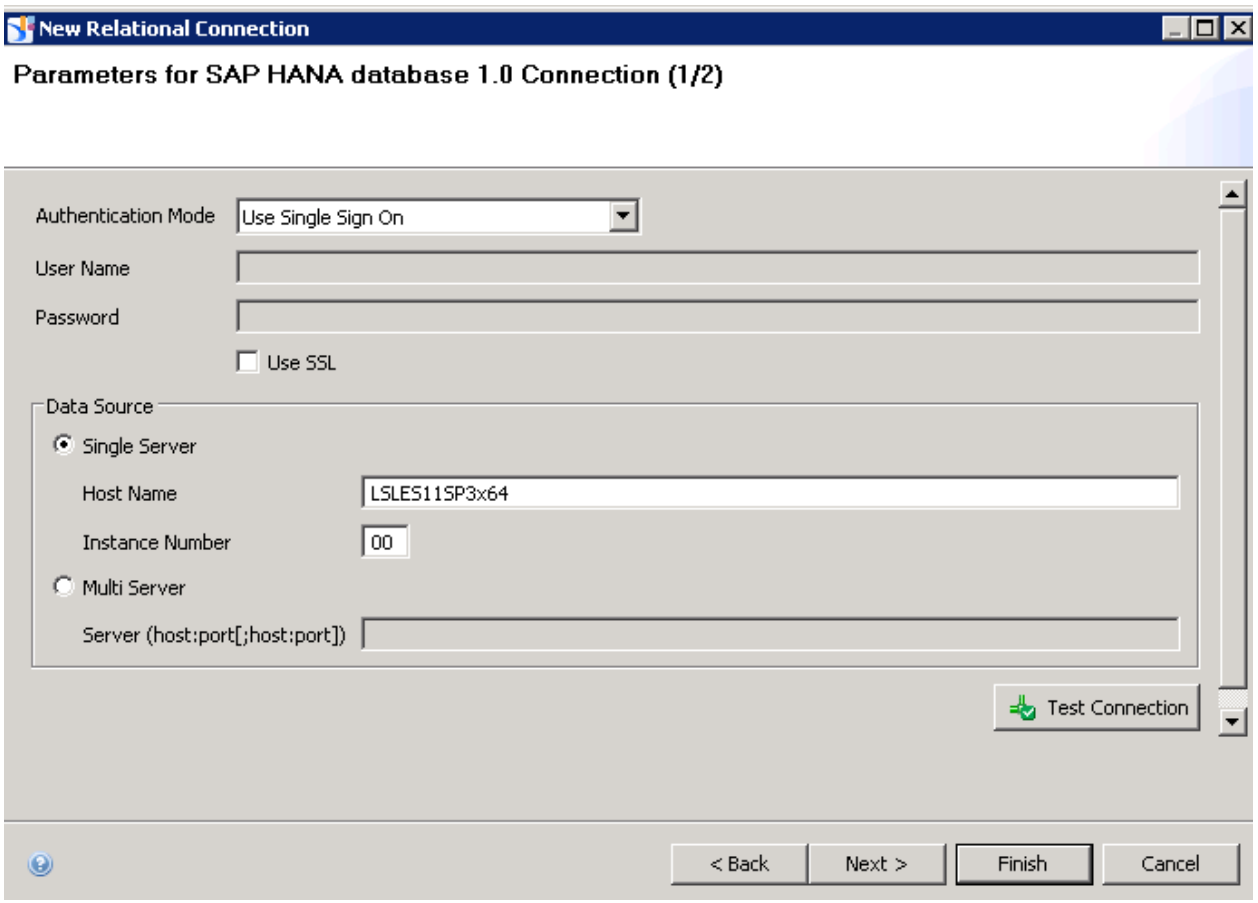

5. Specify a Resource Name



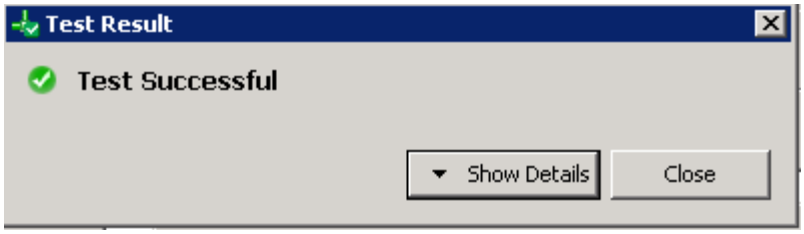

6. Expand SAP > SAP HANA Database 1.0 > JDBC Drivers




7. Select Use Single Sign On from the Authentication Mode drop down. This will grey out the username and password
8. Specify the hostname of the HANA system and the instance number




9. Select Test connection. If the test is successful, the following popup will appear




Test Failed error?

10. This section is now complete

# 6 APPENDIX

## 6.1 Tracing and Troubleshooting

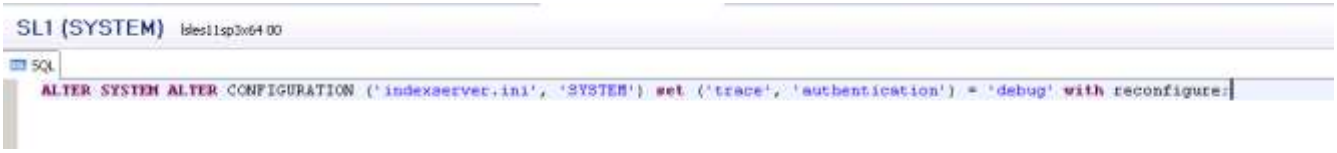
### *6.1.1 Debug Tracing*

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

To enable debug tracing, follow the steps:

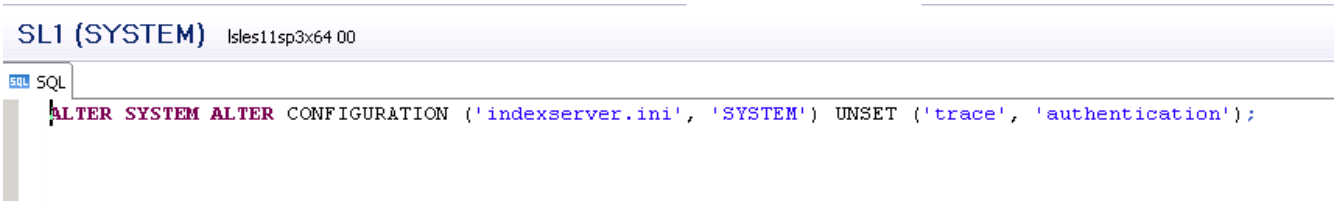
1. Open HANA Studio and Login using the SYSTEM user
2. Open SQL Editor and execute the command:

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



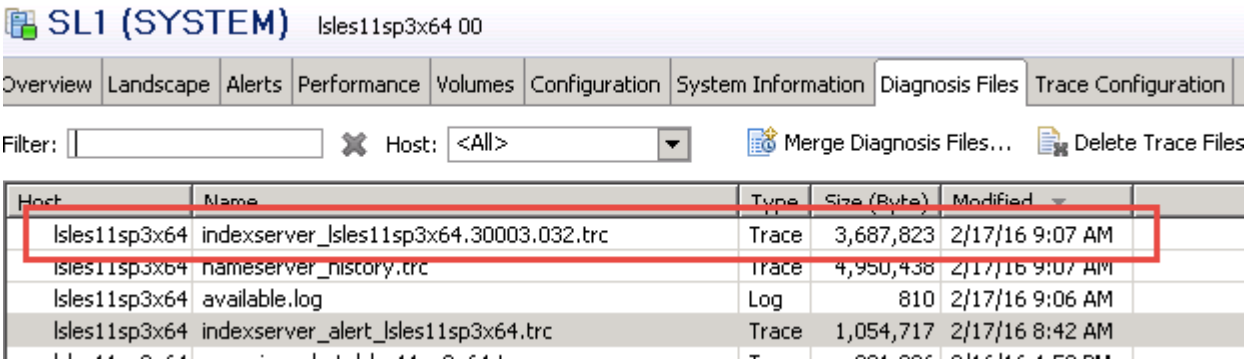

3. Reproduce the error and disable the trace by running the command:

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




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

5. There should be an updated indexserver trace file. For example:



6. Open the indexserver trace file and search for the line:

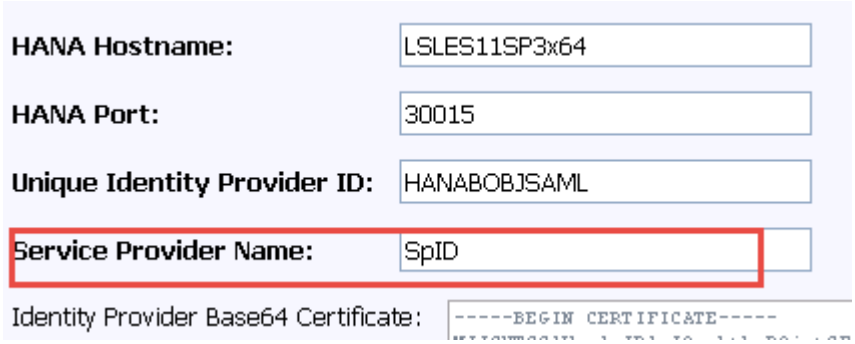
   ALTER SYSTEM ALTER CONFIGURATION ('indexserver.ini', 'SYSTEM') set ('trace', 'authentication') = 'debug' with reconfigure

   This is where the trace analysis should begin.

## 6.2 Common Errors

### *6.2.1 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:

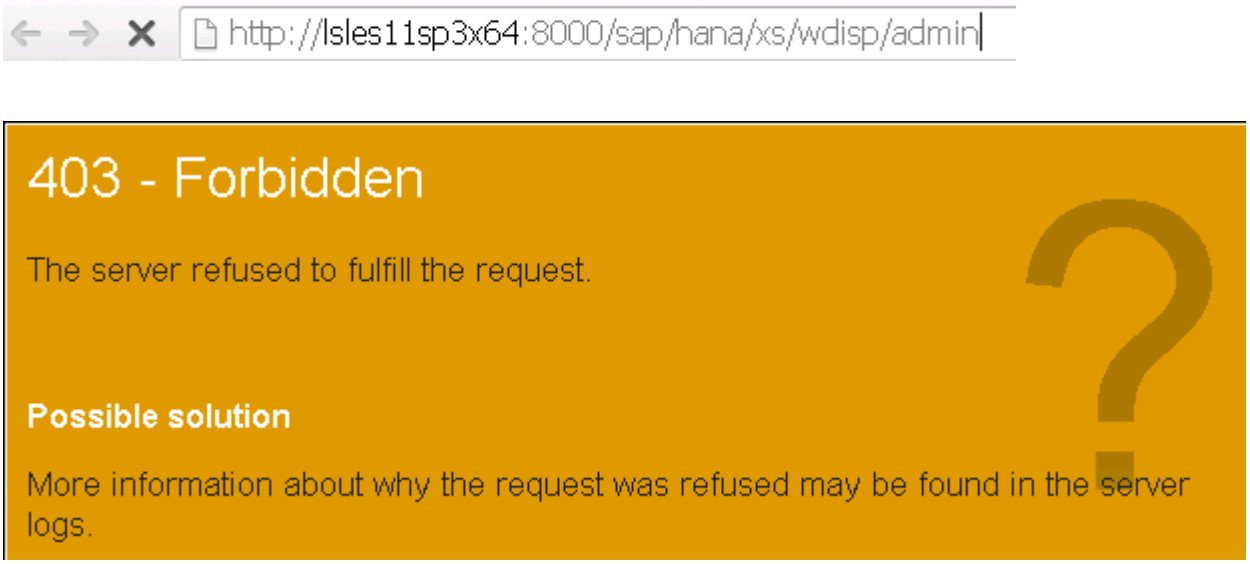

Solution: These two Service Provider names need to match. Change the saml_service_provider_name to match the certificate.

For example:


### *6.2.2 Error 403 – Forbidden error*

After logging into the Web Dispatcher Administration console, a 403 Forbidden error appears.

For example:




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

### *6.2.3 Test Connection fails in the CMC*

When testing the HANA Authentication connection in the CMC > Applications > HANA Authorization, an error occurs.

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)

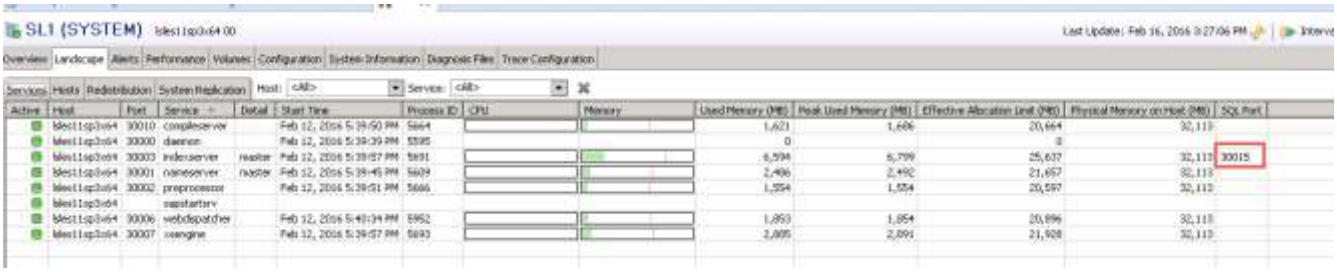
Solution:

- 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.
- Ensure that the Service Provider Name matches the saml_service_provider_name. See Service Provider Name Common Errors

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:

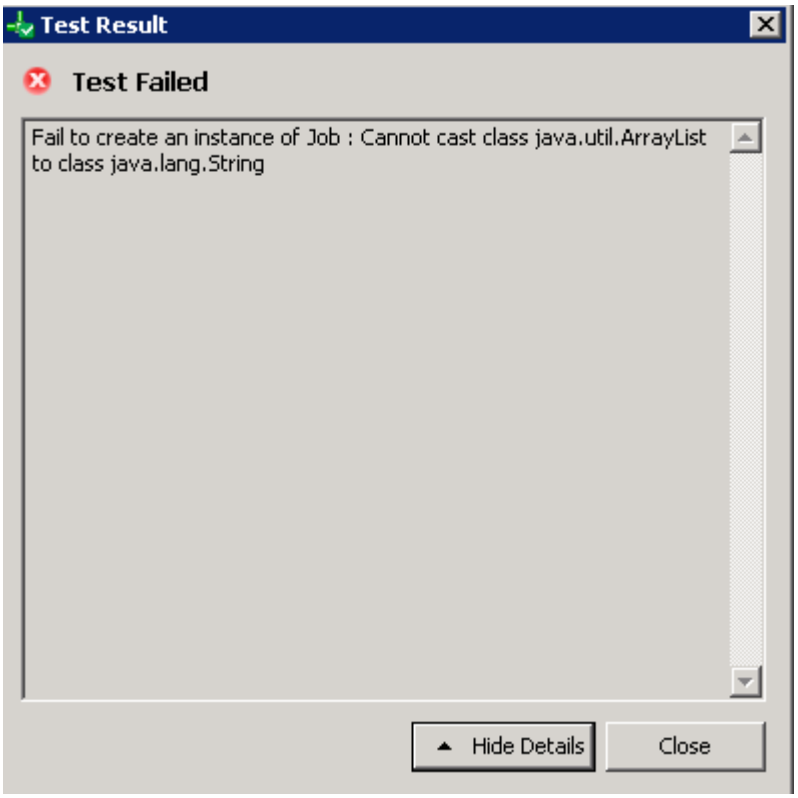
- Check if the firewall is blocking the connectity between BI Platform and SAP HANA System.
- Make sure the HANA port is the correct port. This is especially important when configuring SAML with a mult-tenant HANA system.



### *6.2.4 IDT Test Connection fails*

Selecting Test Connection in IDT fails with error:

Fail to create an instance of Job : Cannot cast class java.util.ArrayList to class java.lang.String




Solution: The connection test has failed. Most likely, this error appears when the CMC connection test also fails. Click here to go to that section.

## 6.3 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 |