

Live Data Connection to SAP HANA and SAP Cloud Platform

Live data connections allow you to connect your data sources with SAP Analytics Cloud. Any changes made to your data in the source system are reflected immediately.

The benefit of connecting to data this way is that the data stays in the source system so large amounts of data do not need to be transferred. The existing models in the source system can also be used directly by SAP Analytics Cloud to build story and visualization on that model and perform online analysis without data replication.

For a list of supported system types and limitations, please see [System Requirements and Technical Prerequisites](#) and [Limitations to SAP HANA and SAP Cloud Platform](#).

1. Live Data Connection to SAP HANA and SAP Cloud Platform

You can create a Live Data Connection to SAP HANA using several connection types:

- Direct
- Path
- SAP Cloud Platform

The **Direct connection** type is recommended in the following instances:

- You don't want to set up a reverse proxy on your local network and put SAP Analytics Cloud behind it
- You are not connecting to an SAP Cloud Platform system
- You are okay to connect to your HANA instance from your company network

To use this connection type, you must configure Cross-Origin Resource Sharing (CORS) support on your SAP HANA system.

The **Path connection** type is recommended in the following instances:

- You already have a reverse proxy set up on your local network and must access SAP Analytics Cloud through it
- You do not want to enable CORS support on your SAP HANA system
- You want to add multiple remote HANA systems as paths instead of enabling CORS on every system
- You are not connecting to an SAP Cloud Platform system

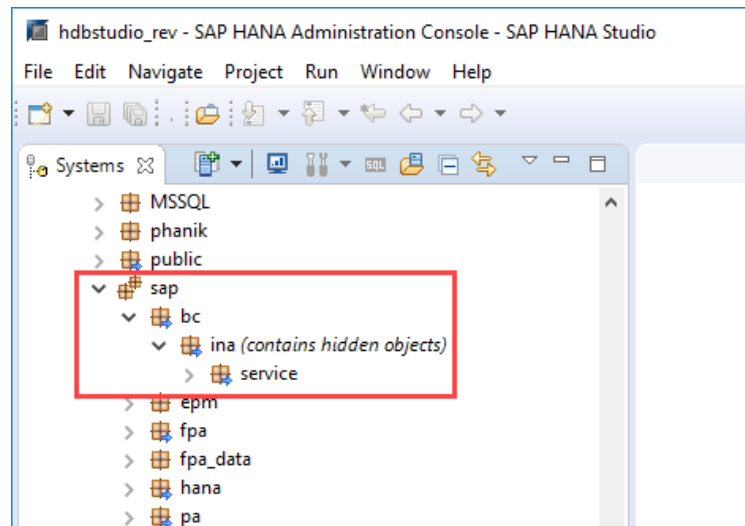
To use this connection type, you must set up a reverse-proxy server. Supported servers are Apache HTTP Server and SAP Web Dispatcher.

Use **SAP Cloud Platform** connection type if you want to connect to data on an SAP Cloud Platform system. A connection being made to SAPCP by specifying the SAPCP account and database name of the remote HANA system.

Direct Connection

General Prerequisites for Direct Connection

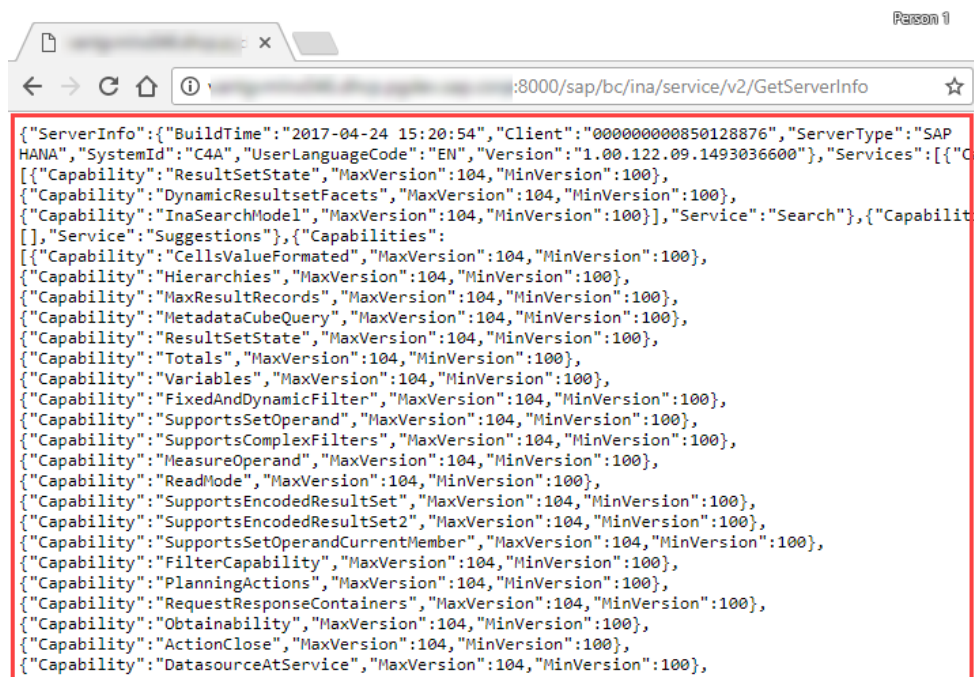
1. Set up and activate the SAP HANA Info Access Service (InA), version 4.10.0 or above, on your SAP HANA system
 - a. Check if the HCO_INA_SERVICE is deployed on your HANA system in SAP HANA Studio. If you see the package in **Content\sap\bc\ina\service InA** Service is deployed:



- b. Ensure that the SAP Information Access (InA) service (/sap/bc/ina/service/v2) on your SAP HANA server is exposed either directly, or via a reverse-proxy to browser users.

Navigate to:

[http://\[HANA XS HOST\]:80\[INSTANCE NUMBER\]/sap/bc/ina/service/v2/GetServerInfo](http://[HANA XS HOST]:80[INSTANCE NUMBER]/sap/bc/ina/service/v2/GetServerInfo) to see the JSON response:

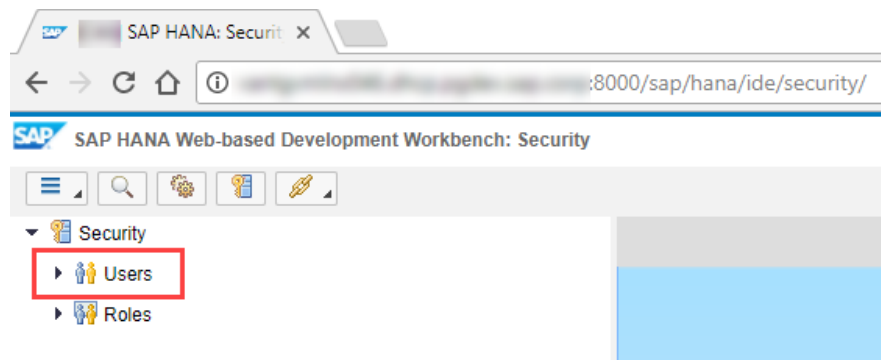


NOTE: If you can't see the response or the package the InA service might be not deployed. Follow the steps how to deploy [Importing the info access service](#).

2. Ensure the sap.bc.ina.service.v2.userRole::INA_USER role is assigned to all users who will use the live connection.

NOTE: You can perform this action in SAP Hana Studio or using the Web-Based Workbench as well.

- a. Using Web-Based Workbench
 - i. Navigate to:
[http://\[HANA XS HOST\]:80\[INSTANCE NUMBER\]/sap/hana/ide/security/](http://[HANA XS HOST]:80[INSTANCE NUMBER]/sap/hana/ide/security/)
 - ii. Expand the list of users



- iii. Locate the user and make sure the user has the required role assigned

The screenshot shows the SAP Analytics Cloud user configuration interface. The 'User' tab is active, displaying authentication settings and a table of granted roles.

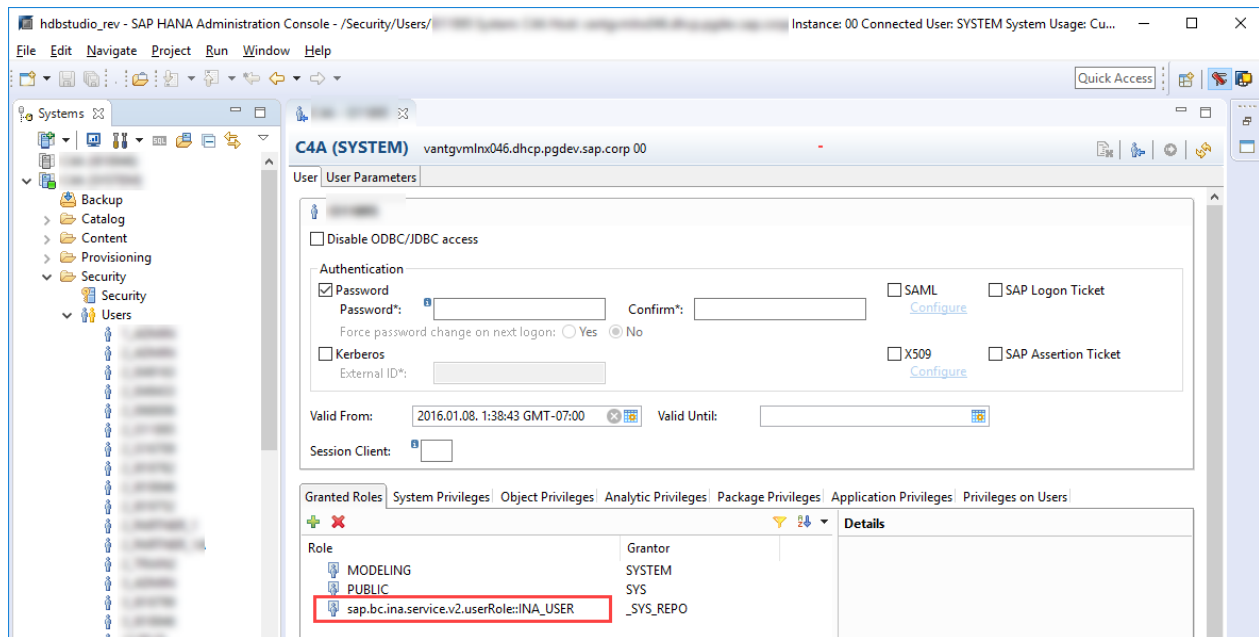
Authentication Settings:

- ☒ Password: [Password field] Confirm*: [Confirm field]
- ☐ Kerberos: [External ID field]
- ☐ SAML: [Configure](#)
- ☐ SAP Logon Ticket
- ☐ X509: [Configure](#)
- ☐ SAP Assertion Ticket
- Valid From: Jan 8, 2016 2:38:43 AM UTC-07:00
- Valid Until: [hh:mm:ss]
- Session Client: [Field]

Granted Roles Table:

| Role | Grantor |
|--|-----------|
| MODELING | SYSTEM |
| PUBLIC | SYS |
| sap.bc.ina.service.v2.userRole::INA_USER | _SYS_REPO |

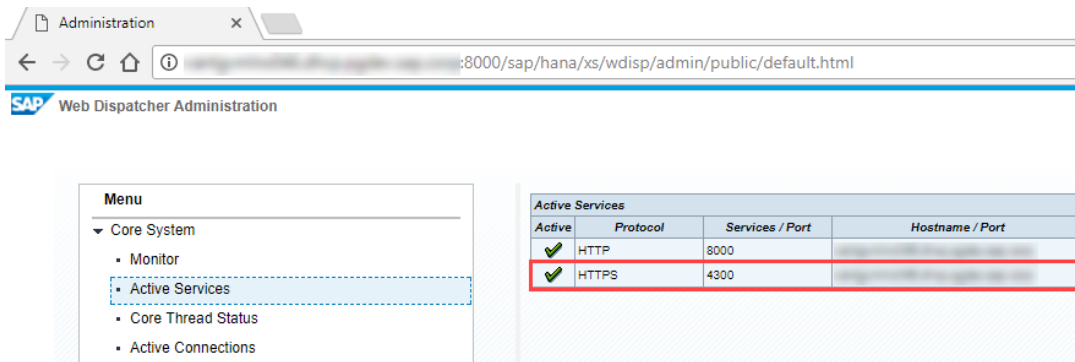
- iv. Add the role using the green + icon in case it hasn't been assigned
- b. Using SAP Hana Studio
 - i. Go to **Security > Users** list
 - ii. Locate the user and make sure the user has the required role assigned



- iii. Add the role using the green + icon in case it hasn't been assigned
3. Ensure that your SAP HANA XS server is configured for HTTPS (SSL) with a signed certificate, and that you know which port it is using for HTTPS requests

NOTE: You can perform this action in SAP Hana Studio or using the XS Admin page as well.

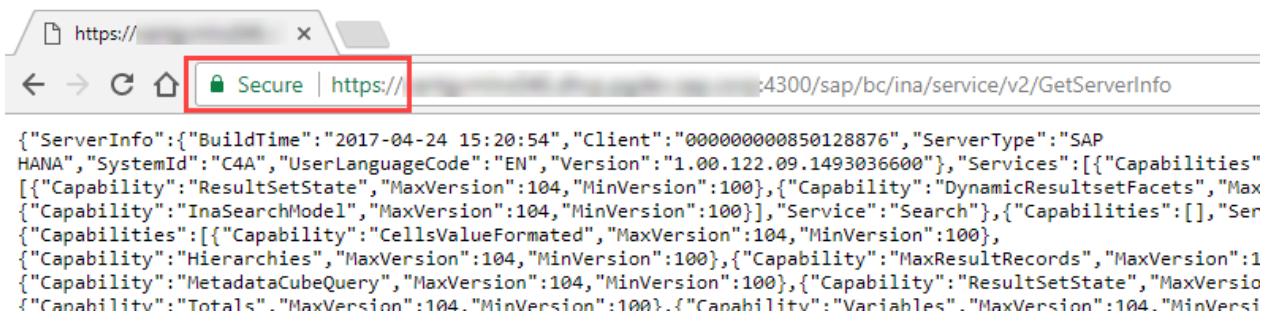
- a. Navigate to:
[https://\[HANA XS HOST\]:\[HTTPS PORT\]/sap/hana/xs/wdisp/admin/public/default.html](https://[HANA XS HOST]:[HTTPS PORT]/sap/hana/xs/wdisp/admin/public/default.html)
- b. Go to **Core System > Active Services** and confirm that you have HTTPS port configured



- c. Note the HTTPS service port and navigate to the URL to test the HTTPS service and the JSON response:

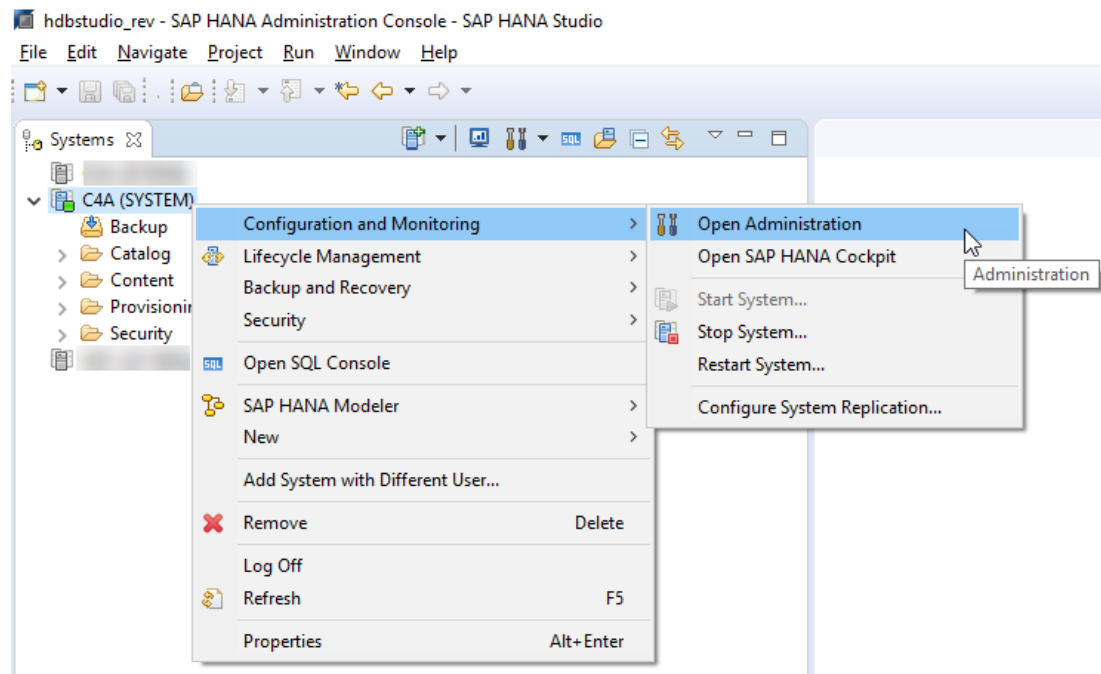
[https://\[HANA XS HOST\]:\[HTTPS Port\]/sap/bc/ina/service/v2/GetServerInfo](https://[HANA XS HOST]:[HTTPS Port]/sap/bc/ina/service/v2/GetServerInfo)

NOTE: If you see the sign **Secure** in green next to the “https://”, then your server is configured for HTTPS with secured/signed SSL certificate. However, if your server doesn't respond to the HTTPS port, or the site is not secured by SSL certificate, verify that you completed the SSL configuration correctly as indicated in [SAP KBA 2502174](#).

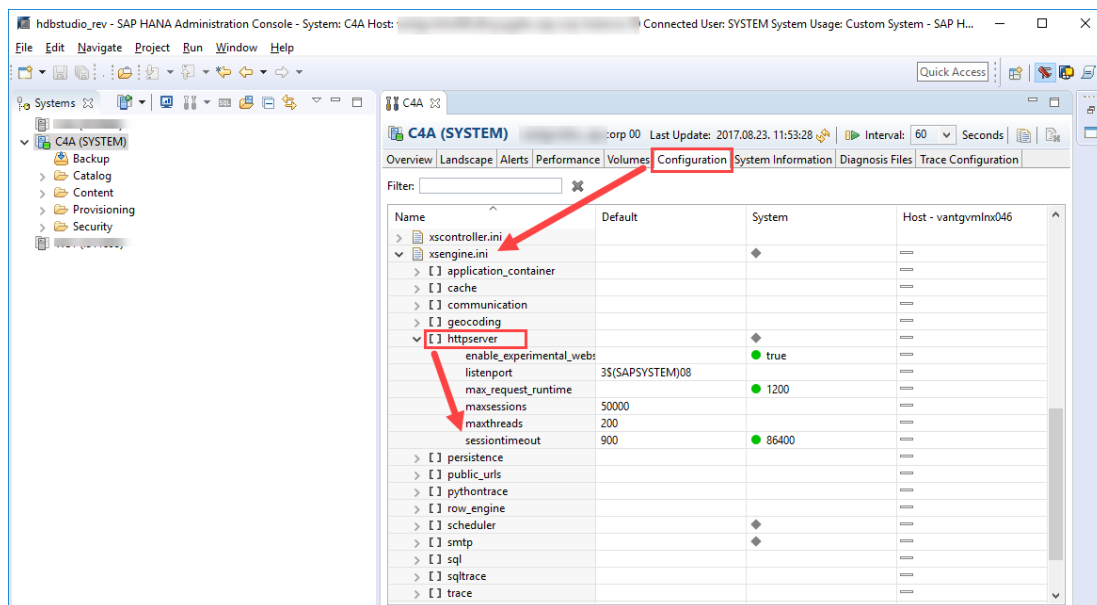


- For SAP HANA version 1.00.112.04 and above, users require both the INA_USER role, and additional object rights. The SAP HANA administrator must grant users SELECT privileges on all view items in the _SYS_BIC schema that users should have access to. For more information, see SAP Knowledge Base Article [2353833](#)
- Increase the session timeout configuration parameters in SAP HANA XS server

- a. Open the Administration page of the HANA instance in SAP HANA Studio



- b. Switch to the **Configuration** tab
- c. Here you will need to increase the `sessiontimeout` parameter in the `httpserver` section of the `xsengine.ini` file

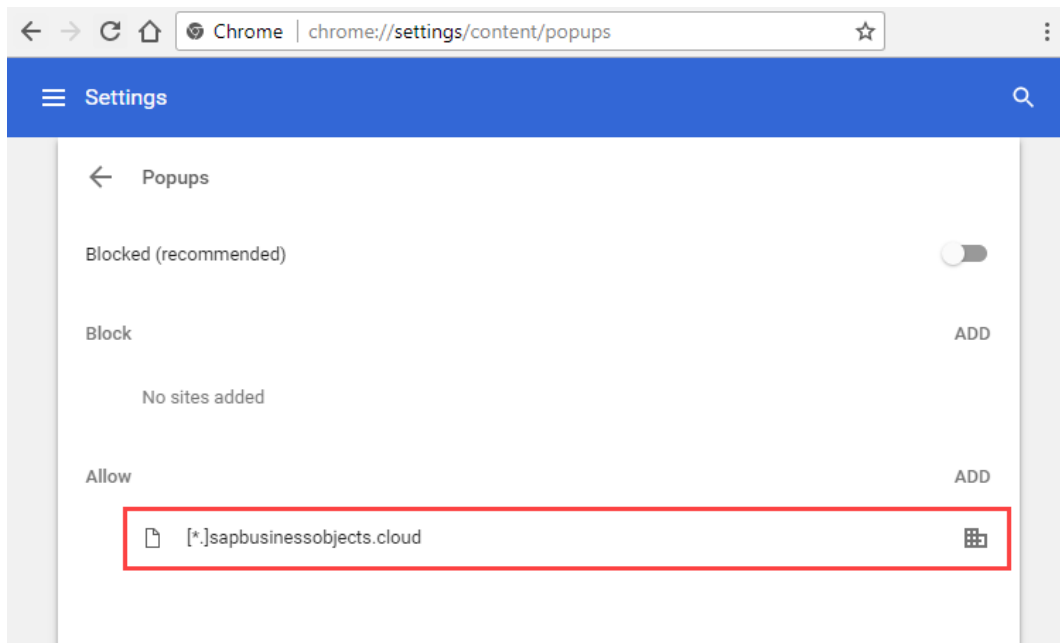


Example: if you change the parameter to 86400, the session will be active for 24 hours

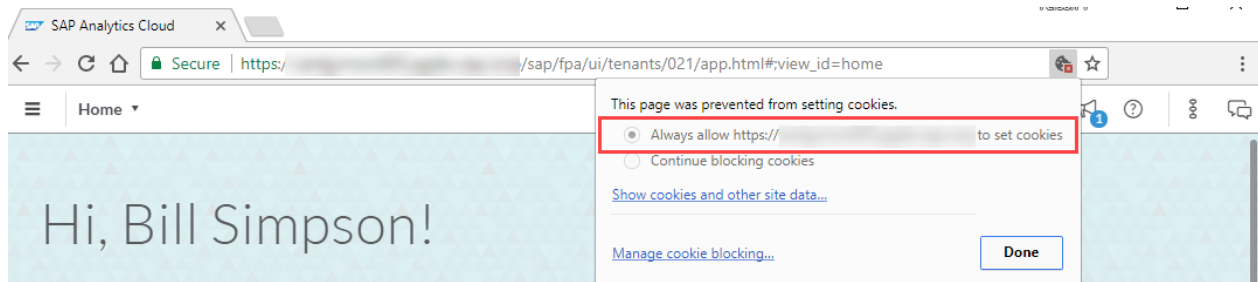
Live Data Connection to SAP HANA using a Direct Connection and SSO

Prerequisites for SAML SSO

1. Allow popup windows from your SAP Analytics Cloud Domain
 - a. Using Google Chrome go to <chrome://settings/content/popup>
 - b. Make sure to add the domain of your SAC URL



2. If you have Reverse Proxy configured, you must not block 3rd party cookies from the reverse proxy domain (this is the reverse proxy with the remote system behind). When navigating to SAC using your Reverse Proxy URL in your browser, you need to allow the reverse proxy domain always to set cookies.

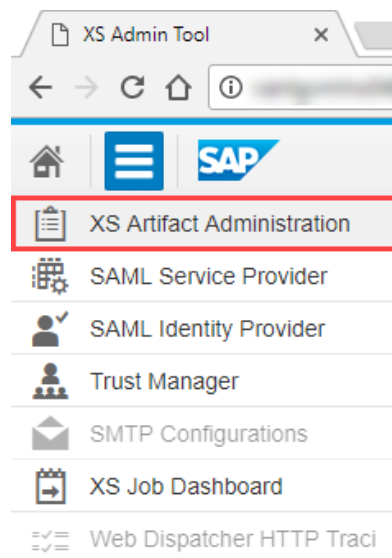


3. Ensure that the InA package (/sap/bc/ina/service/v2) or a higher-level package is configured for SAML authentication using the same identity provider URL as your SAP Analytics Cloud tenant.

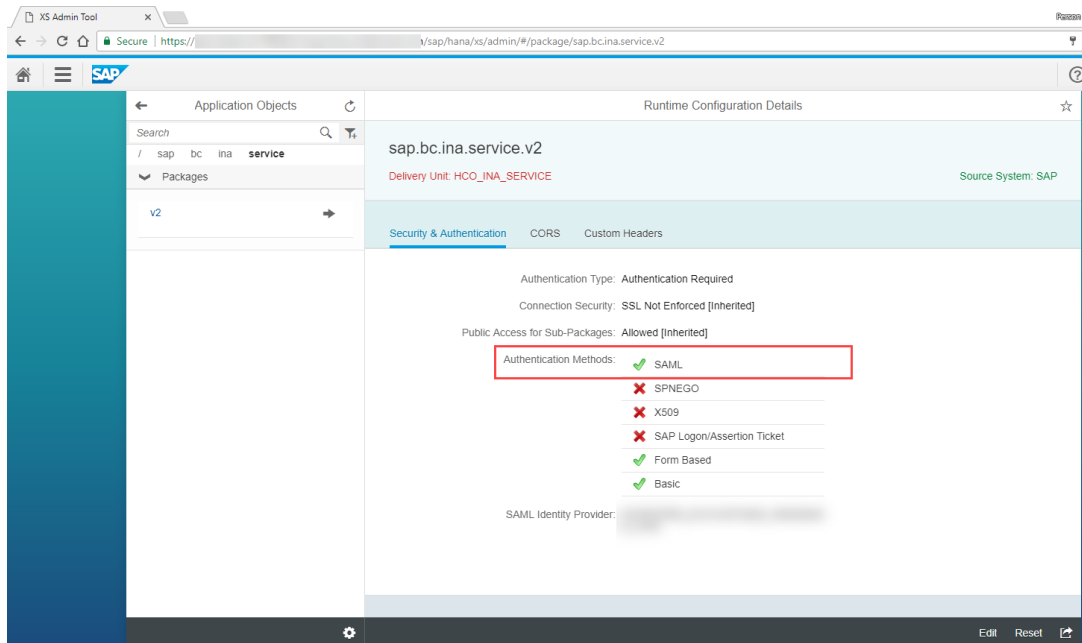
- a. Login using the following URL

http://<HANA XS HOST>:80<INSTANCE_NUMBER>/sap/hana/xs/admin/

- b. Click on **Menu > XS Artifact Administration**



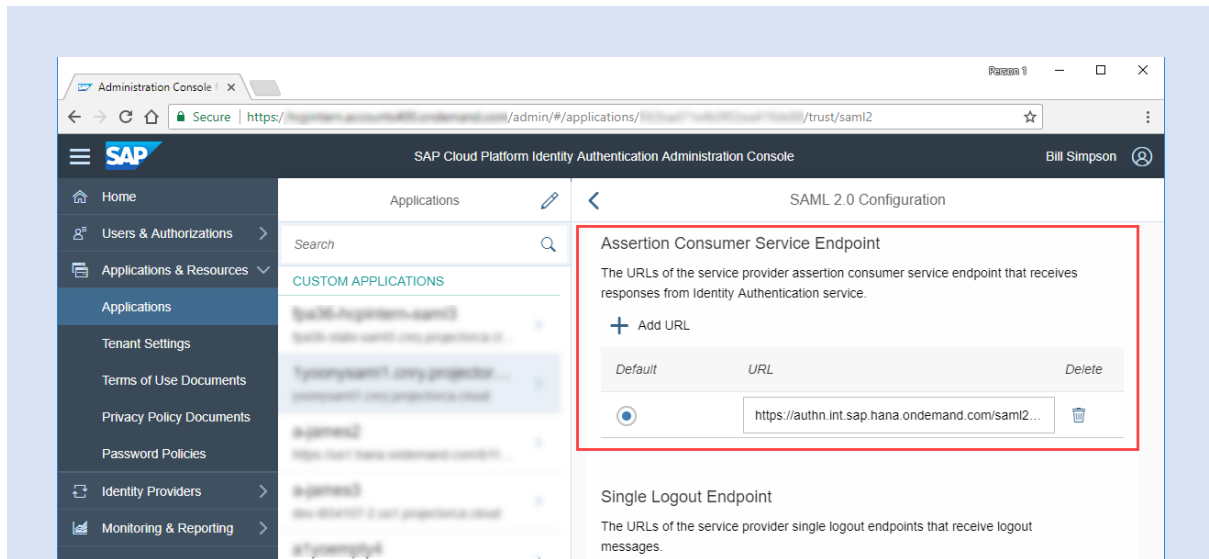
- c. In the left navigation pane go to the package **sap > bc > ina > service > v2**
 - d. Make sure that the “SAML” authentication is checked



For more details, see the [SAP HANA XS documentation](#).

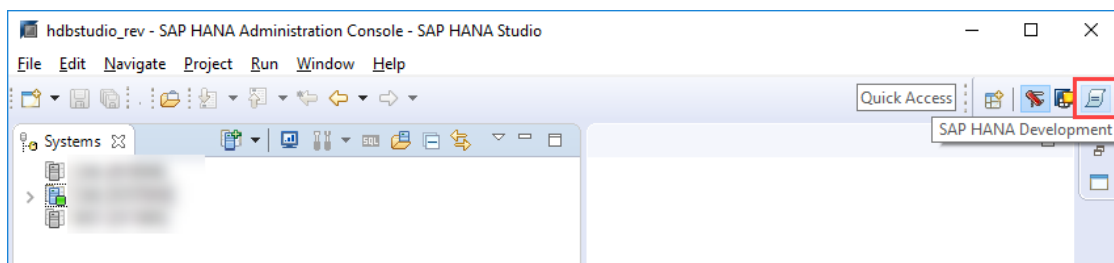
4. If your SAP HANA server is exposed to internet users via a reverse proxy, in your SAML identity provider configuration, ensure that the Assertion Consumer Service (ACS) endpoint URL for the SAP HANA service provider is set to the SAP HANA server's reverse proxy URL.

NOTE: If you are using SAP Cloud Platform ID authentication, go to your SAML 2.0 application and click Add URL under "Assertion Consumer Service Endpoint". Specify the URL to the reverse proxy pass to the remote HANA system with the appropriate path, for example, <https://<reverse-proxy-host>/sap/hana/xs/saml/login.xscfunc>

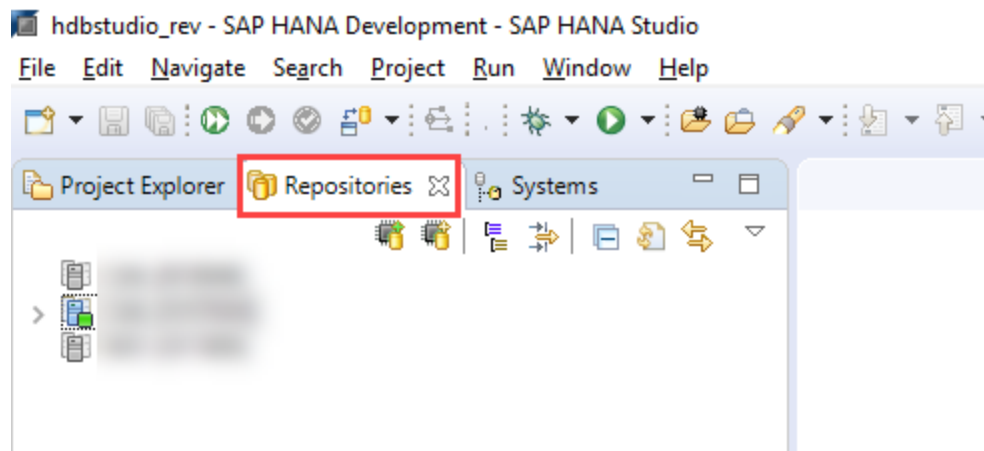


Setup

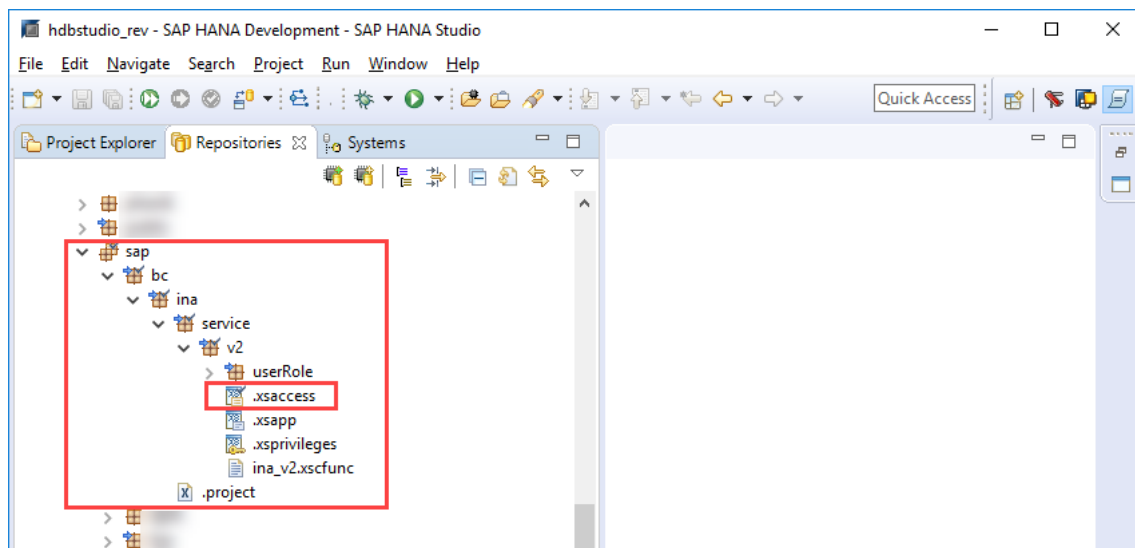
1. Enable CORS support for the InA package directly on the SAP HANA system:
 - a. Login to SAP HANA Studio as the System user or with other admin/developer credentials
 - b. Switch to the **SAP HANA Development** perspective



- c. Choose the *Repositories* tab



d. Navigate to **sap.bc.ina.service.v2.** and open the **.xsaccess** file



e. Replace its contents with the following text. Please ensure that the `allowOrigin` value matches the host of your SAP Analytics Cloud tenant:

```
{
  "exposed" : true,
  "prevent_xsrf" : true,
  "authentication": [
    {
      "method" : "Basic"
    }
  ],
}
```

```

    "rewrite_rules": [
      {
        "source":
"(GetResponse|Perspectives|GetVersion|GetServerInfo|Analytics|Metad
ata|Planning).*",
        "target": "ina_v2.xscfunc?service=$0"
      }
    ],

    "authorization" : [
      "sap.bc.ina.service.v2::Execute"
    ],

    "cors": {
      "enabled": true,
      "allowMethods": ["GET","POST","HEAD","OPTIONS"],
      "allowOrigin": ["https://<customer-prefix>.<data-
center>.sapbusinessobjects.cloud"],
      "maxAge": 3600,
      "allowHeaders": ["x-csrf-token","accept","authorization","x-
request-with","content-type","x-sap-cid"],
      "exposeHeaders":["x-csrf-token","accept","authorization","x-
request-with","content-type","x-sap-cid"]
    },
    "cache_control" : "no-cache, no-store",
    "headers": {
      "enabled": true,
      "customHeaders": [ { "name":"Access-Control-Allow-
Credentials","value":"true"} ]
    }
  }

```

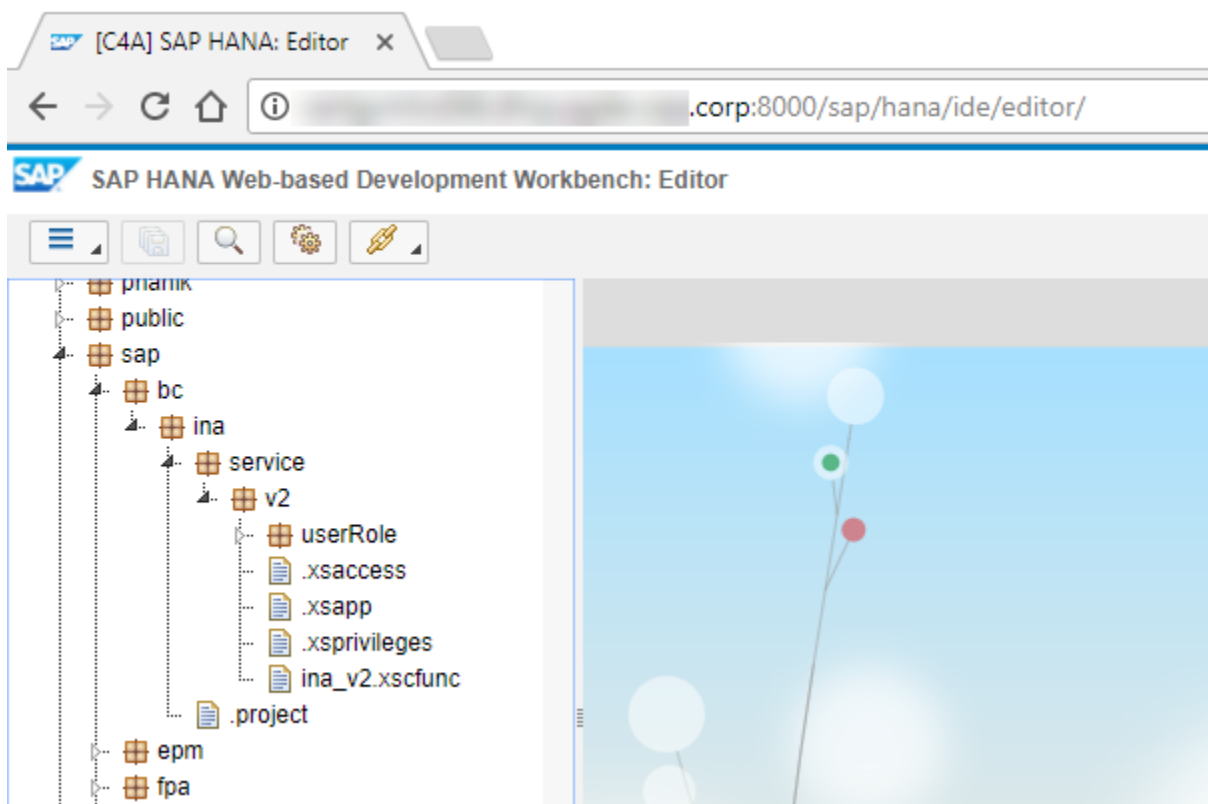
NOTE: The `allowOrigin` variable should match your SAP Analytics Cloud tenant URL. More than one URL can be added to the `allowOrigin` variable. For more information on CORS options, see [Application-Access File Keyword Options](#).

2. Deploy the custom web content to your SAP HANA server

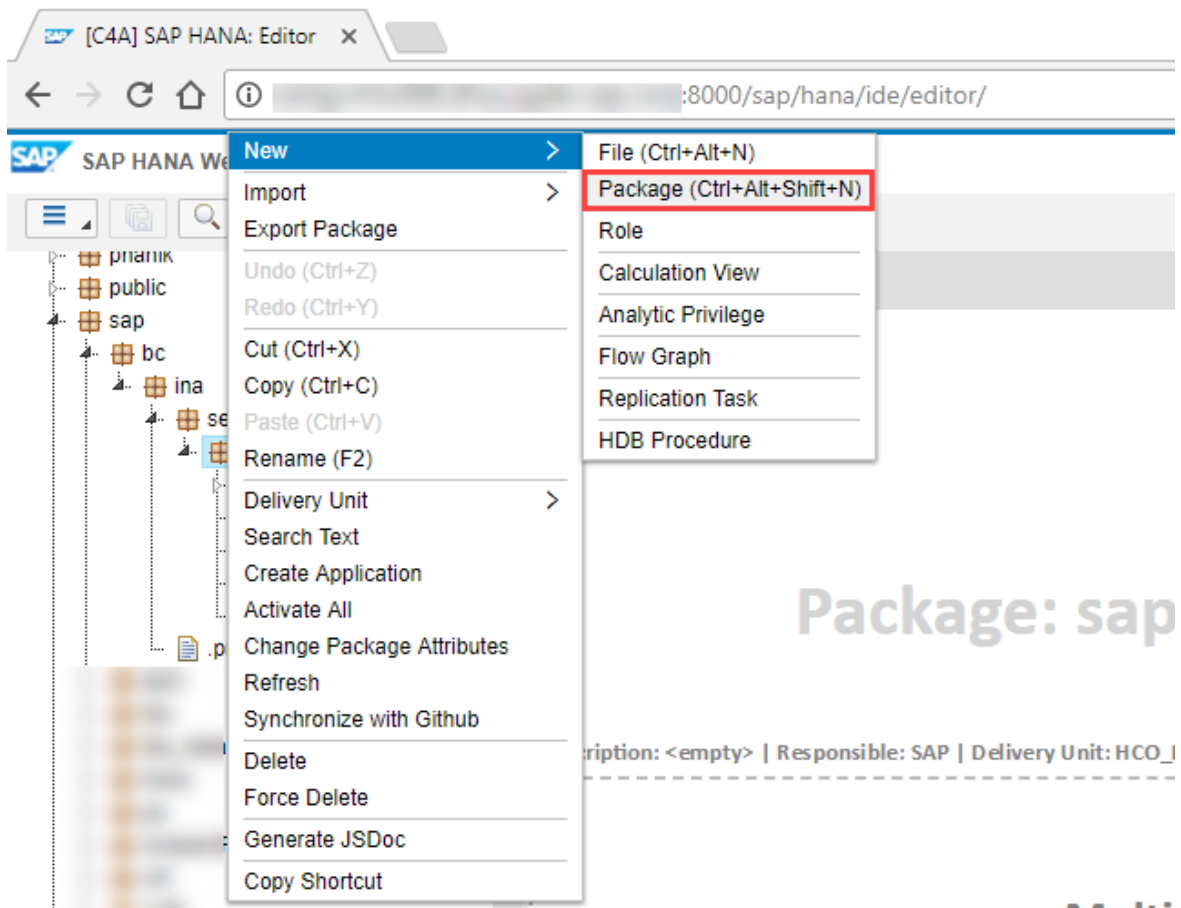
To enable SSO for the direct connectivity type, you must deploy some custom web content to your SAP HANA server. This web content is what will appear briefly to users once per session when they first create a live data connection to your SAP HANA system, or when they refresh charts or tables against that live data connection.

NOTE: You can perform this action in SAP Hana Studio as well as using the Web IDE.

- a. Login to your SAP HANA server's Web IDE
at: https://<HANA_XS_HOST>:80<INSTANCE_NUMBER>/sap/hana/ide/editor/ with the system user credentials
- b. Navigate to sap.bc.ina.service.v2



- c. Right-click on the v2 package, and select **New > Package**



d. In Package Name enter cors and click Create

Create Package [X]

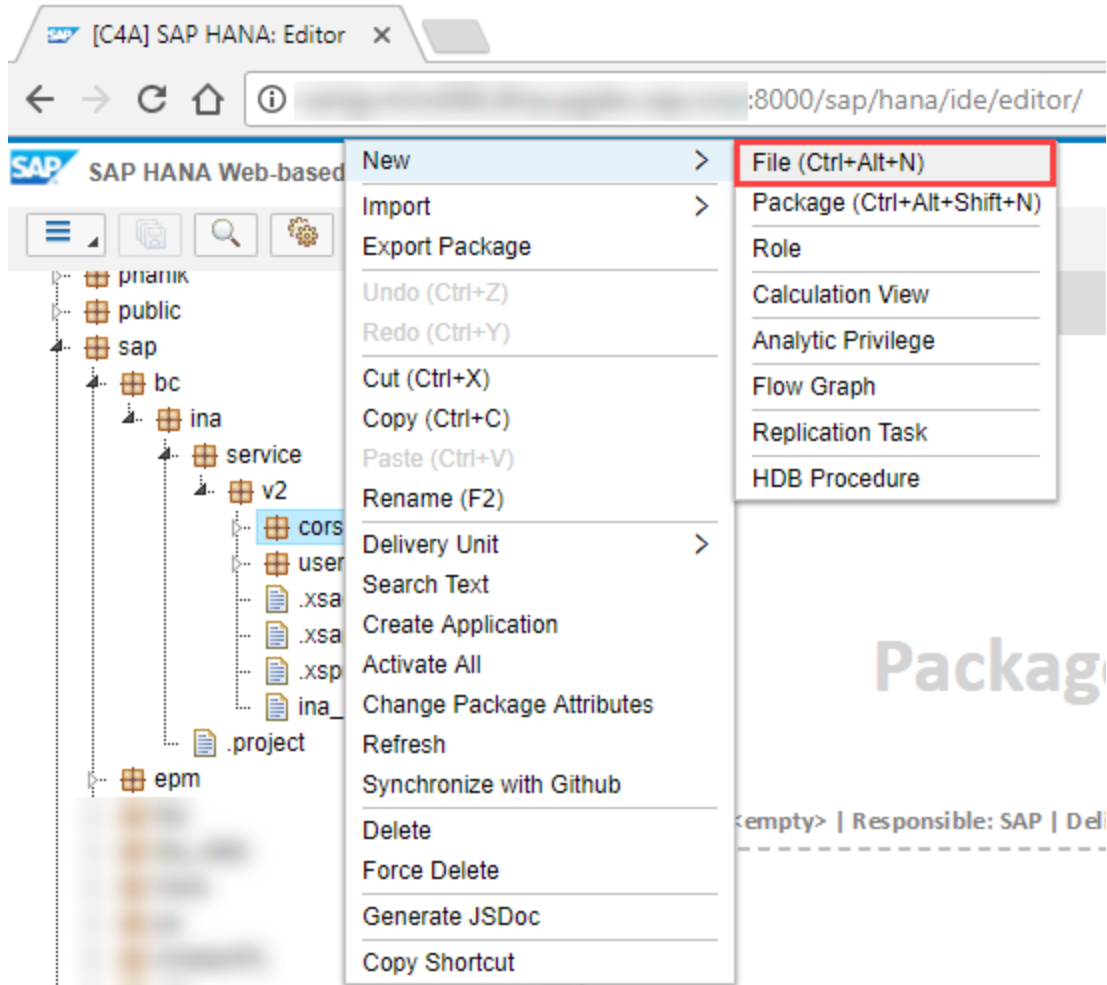
Package name:

Description:

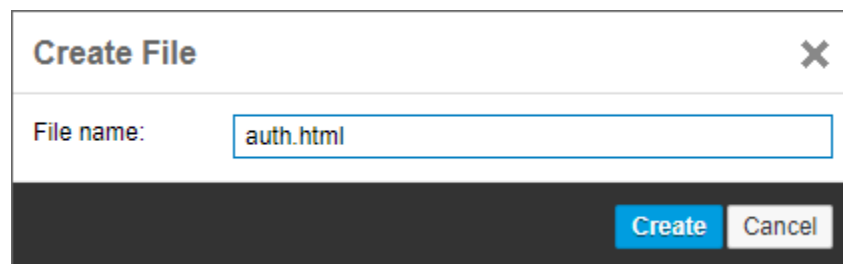
Responsible:

Original Language:

- e. Right-click the cors package and select **New > File**



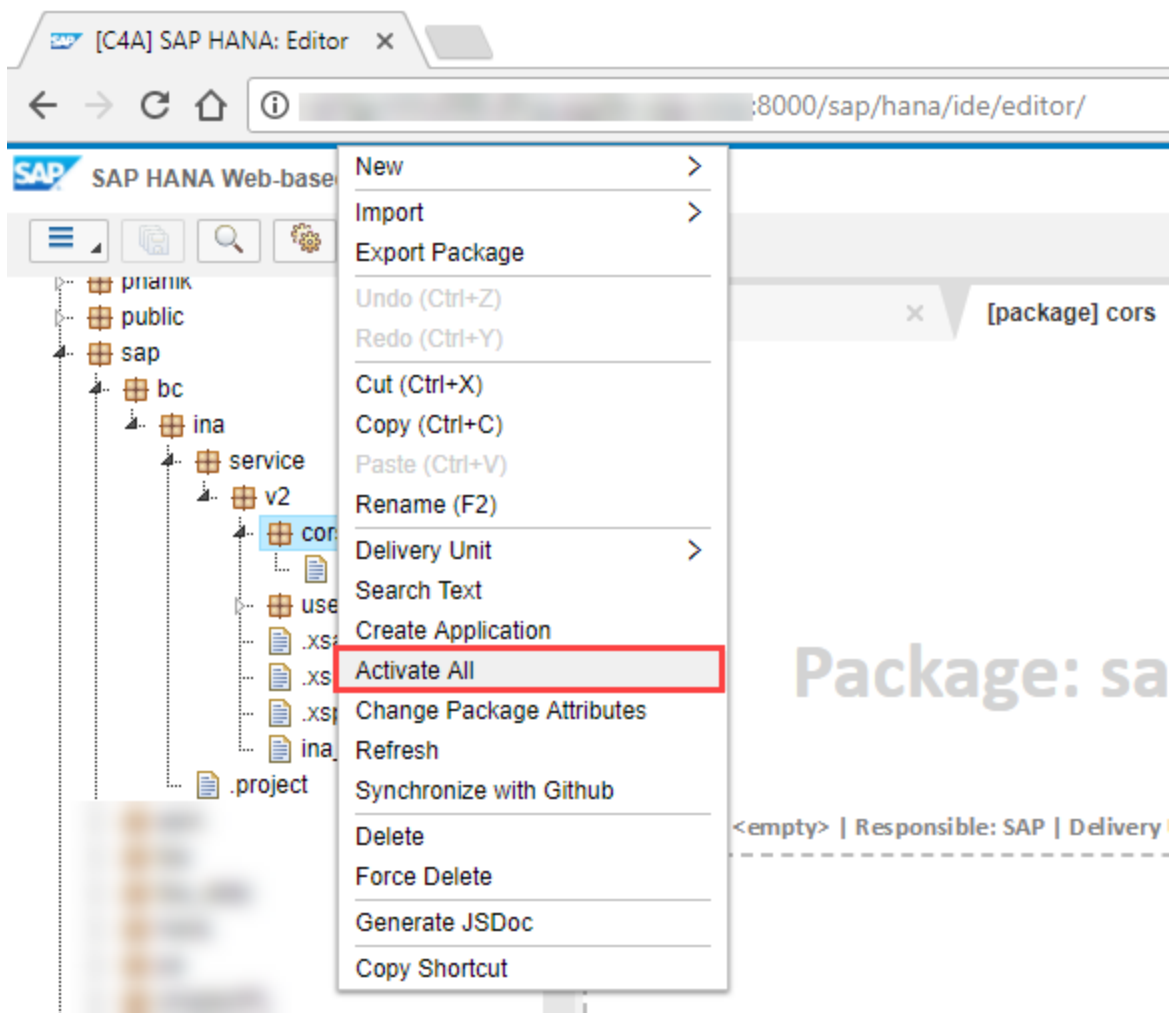
- f. Enter **auth.html** and click Create



- g. Open the recently created auth.html file, and add the following code:

```
<html>
  <script type="text/javascript">
    window.close();
  </script>
</html>
```

- h. Save the auth.html file
- i. Right-click the **cors** package, and click **Activate**



- j. In a new browser tab, go to the following URL:
[https://\[HANA XS HOST\]:\[HTTPS Port\]/sap/bc/ina/service/v2/cors/auth.html](https://[HANA XS HOST]:[HTTPS Port]/sap/bc/ina/service/v2/cors/auth.html)

If the html page is configured correctly, the page will load and close automatically

3. Create a Live Data Connection to SAP HANA in SAP Analytics Cloud:
 - a. Login to SAP Analytics Cloud and go to **Main Menu > Connection > Connections > + (Add Connection) > Live Data Connection > SAP HANA**
 - b. In the dialog, enter a name for your new connection

NOTE: The connection name cannot be changed later.

- c. Set the connection type to **Direct**
- d. Add your SAP HANA host name, and HTTPS port
- e. Under **Authentication Method** select **SAML Single Sign On**

New HANA Live Connection

Name *

SAP HANA Direct Connection with SSO

Description

My direct SSO connection to HANA using CORS

Datasource Configuration

Additional components or configuration may be required for this connection type. See our [Help Center](#) to find out what's required.

Connection Details

Connection Type

Direct

Host *

<HANA_XS_ENGINE_HOST>

HTTPS Port

<HANA_XS_ENGINE_HTTPS_PORT>

Credentials

Authentication Method

SAML Single Sign On

Follow these steps to [setup Single Sign On](#) with your datasource.

OK

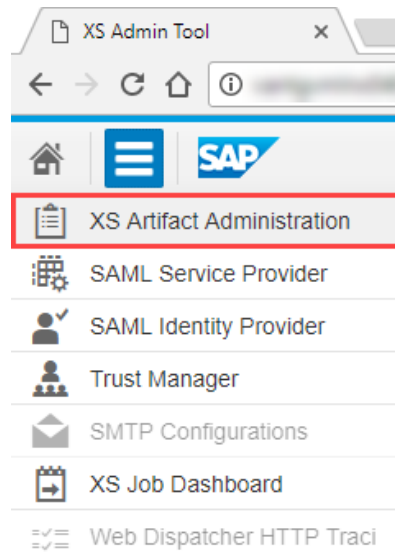
Cancel

f. Select **OK**

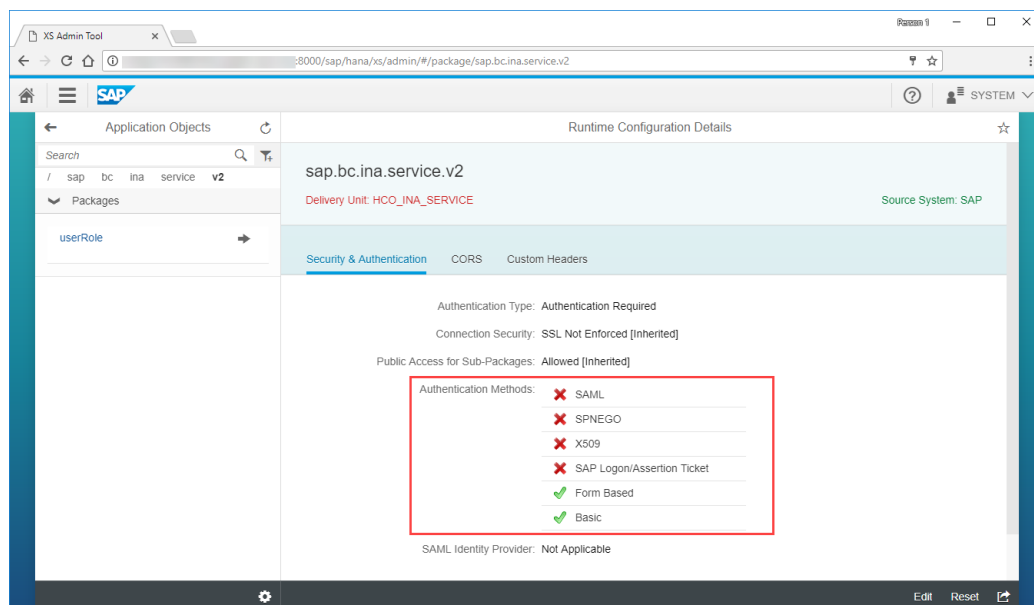
Live Data Connection to SAP HANA using a Direct Connection with User Name and Password Authentication

Prerequisites for User Name and Password Authentication

1. Ensure that the InA package (/sap/bc/ina/service/v2) or a higher-level package is configured for basic authentication:
 - a. Login using the following URL and [http://\[HANA_XS_HOST\]:80\[INSTANCE_NUMBER\]/sap/hana/xs/admin/](http://[HANA_XS_HOST]:80[INSTANCE_NUMBER]/sap/hana/xs/admin/)
 - b. Click on **Menu > XS Artifact Administration**



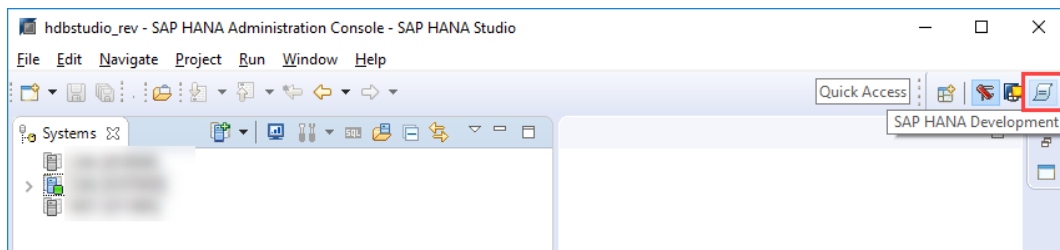
- c. In the left navigation pane go to the package **sap > bc > ina > service > v2**
- d. Make sure that the “Basic” authentication is checked



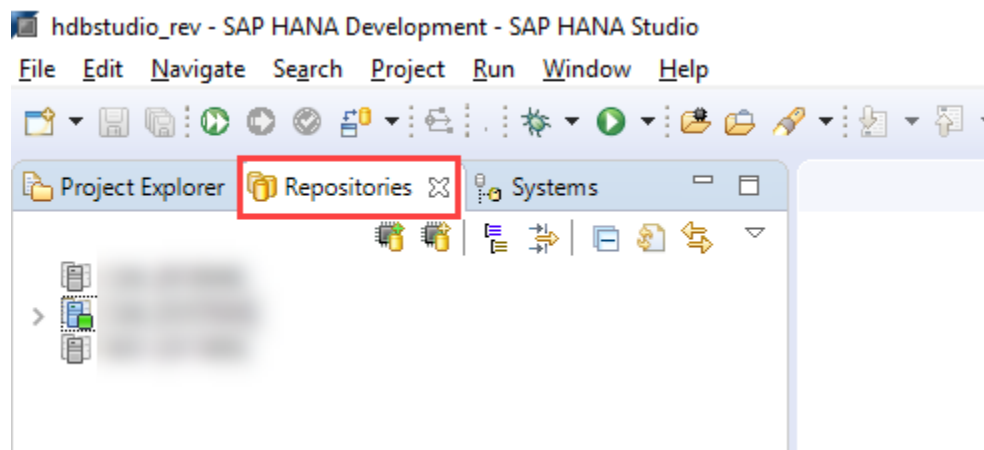
- e. In case it is not, Select **Edit**
- f. Select the Basic Authentication checkbox and **Save**

Setup

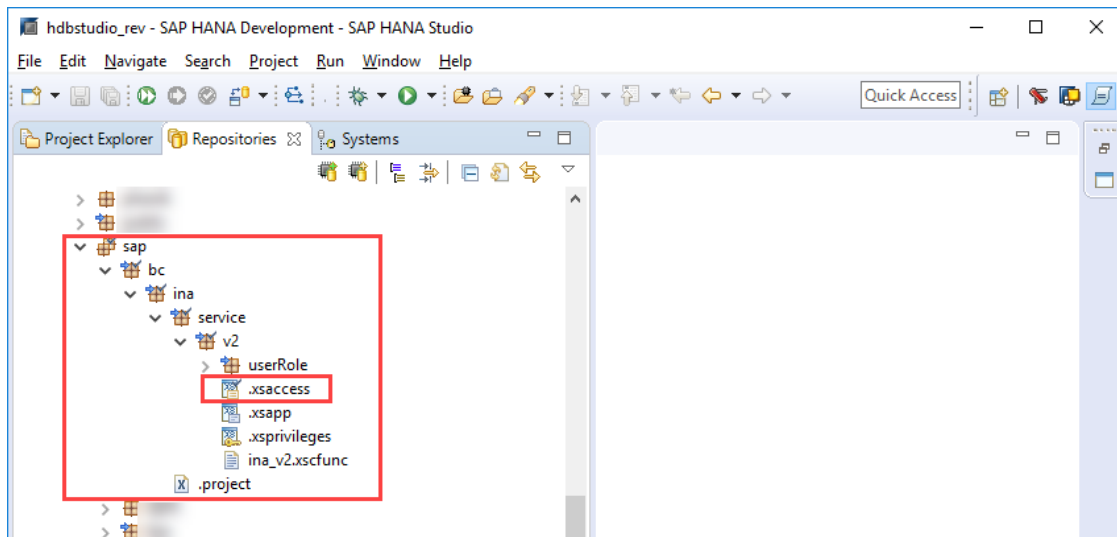
1. Enable CORS support for the InA package directly on the SAP HANA system.
CORS headers must be supported by the remote HANA system.
 - a. Login to SAP HANA Studio as the System user or with other admin/developer credentials
 - b. Switch to the **SAP HANA Development** perspective



- c. Choose the *Repositories* tab



- d. Navigate to **sap.bc.ina.service.v2** package and open the `.xsaccess` file



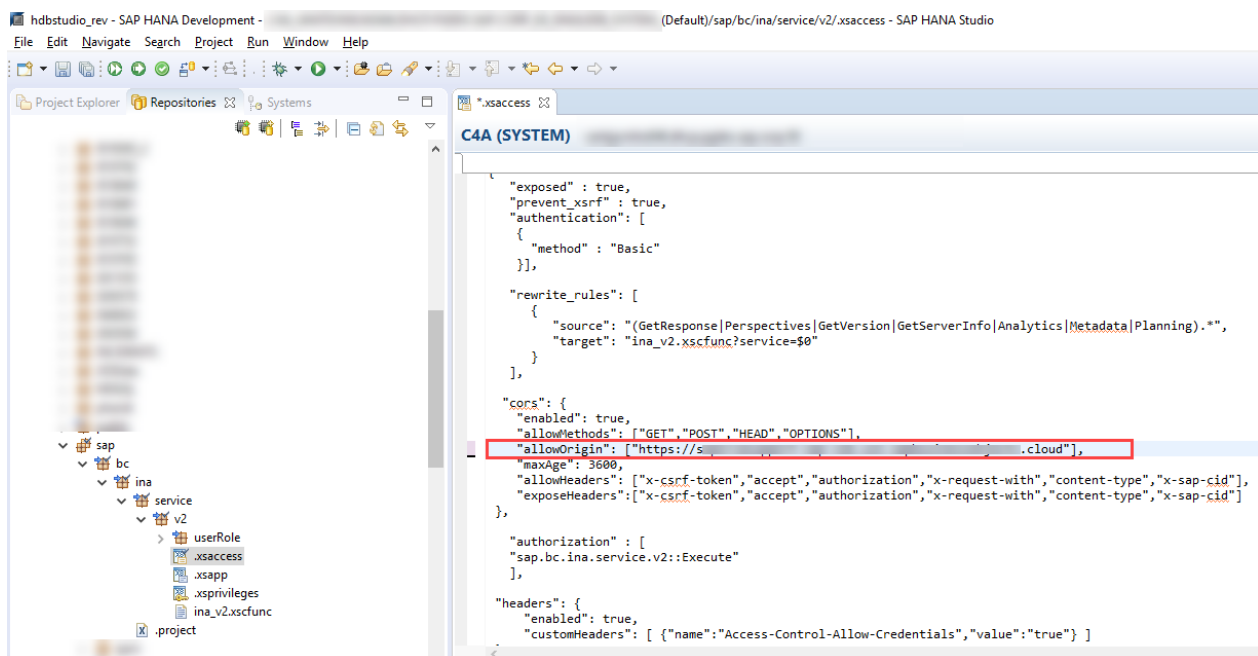
- e. Replace its content with the following text. Please ensure that the allowOrigin value matches the host of your SAP Analytics Cloud tenant:

```
{
  "exposed" : true,
  "prevent_xsrp" : true,
  "authentication": [
    {
      "method" : "Basic"
    }
  ],
  "rewrite_rules": [
    {
      "source":
"(GetResponse|Perspectives|GetVersion|GetServerInfo|Analytics|Metad
ata|Planning).*",
      "target": "ina_v2.xscfunc?service=$0"
    }
  ],
  "authorization" : [
    "sap.bc.ina.service.v2::Execute"
  ],
  "cors": {
    "enabled": true,
    "allowMethods": ["GET", "POST", "HEAD", "OPTIONS"],
```

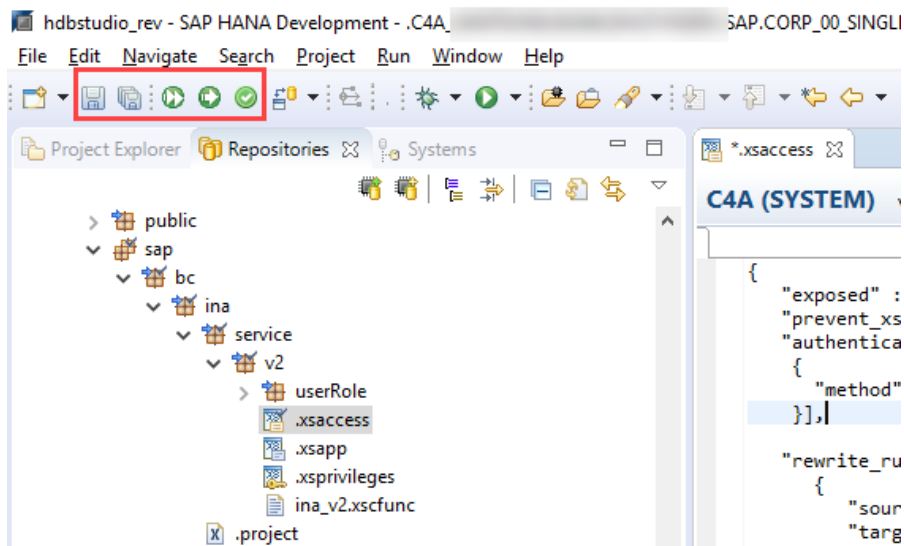
```

    "allowOrigin": ["https://<customer-prefix>.<data-
center>.sapbusinessobjects.cloud"],
    "maxAge": 3600,
    "allowHeaders": ["x-csrf-token", "accept", "authorization", "x-
request-with", "content-type", "x-sap-cid"],
    "exposeHeaders": ["x-csrf-token", "accept", "authorization", "x-
request-with", "content-type", "x-sap-cid"]
  },
  "headers": {
    "enabled": true,
    "customHeaders": [ { "name": "Access-Control-Allow-
Credentials", "value": "true" } ]
  }
}

```



f. Save the changes in the .xsaccess file and activate the file



NOTE: If the remote system does not allow CORS configuration, or you are reaching SAC via reverse proxy, then you can perform the CORS configuration by editing the apache reverse proxy config file. More information about configuring CORS on Reverse Proxy in the [SAP Analytics Cloud Documentation](#).

2. Add a remote system to SAP Analytics Cloud:

- a. Log onto of SAP Analytics Cloud and go to **Main Menu > Connection > Connections > + (Add Connection) > Live Data Connection > SAP HANA**

- b. In the dialog, enter a name for your new connection

NOTE: The connection name cannot be changed later.

- c. Set the connection type to **Direct**
- d. Add your SAP HANA host name, and HTTPS port
- e. Under **Authentication Method** select **User Name and Password**
- f. Enter an SAP HANA user name and password

New HANA Live Connection

Name *
SAP HANA Direct Connection

Description
My direct connection to HANA using CORS

Datasource Configuration

① Additional components or configuration may be required for this connection type. See our [Help Center](#) to find out what's required.

Connection Details

Connection Type
Direct

Host *
<HANA_XS_ENGINE_HOST>

HTTPS Port
<HANA_XS_ENGINE_HTTPS_PORT>

Credentials

Authentication Method
User Name and Password

① Follow these steps to [Set up a connection](#) with your datasource.

User Name *

Password *

OK Cancel

g. Then select **OK**

Path Connection

General Prerequisites for Path Connection

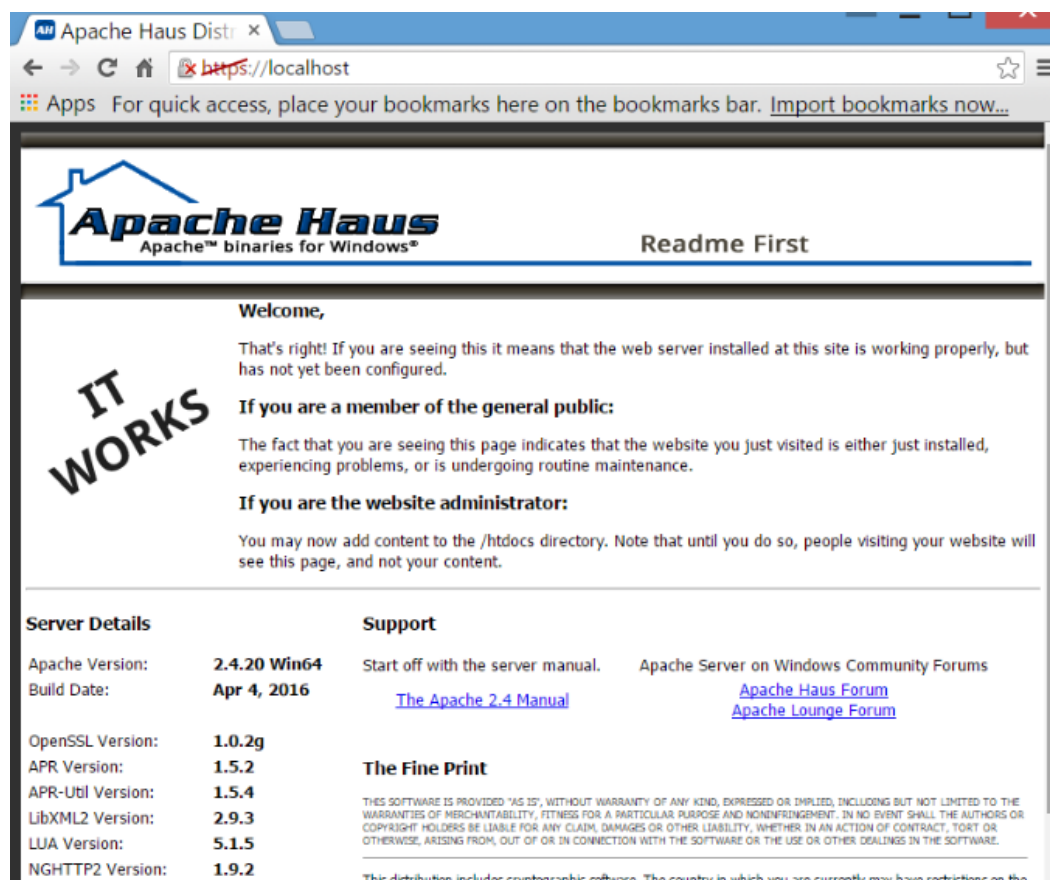
- Set up and activate the SAP HANA Info Access Service (InA), version 4.10.0 or above, on your SAP HANA system.
- Create an SAP HANA info access user and assigned the sap.bc.ina.service.v2.userRole::INA_USER role to all users who will use the live connection.
- SAP HANA version 1.00.112.04 and above, users require both the INA_USER role, and additional object rights. The SAP HANA administrator must grant users SELECT privileges on all.

Live Data Connection setup to SAP HANA via Apache HTTP Server

Prerequisites for Apache HTTPServer setup

- You have installed and configured an HTTP server of your choice on port 443 in the same network as your on-premise system.

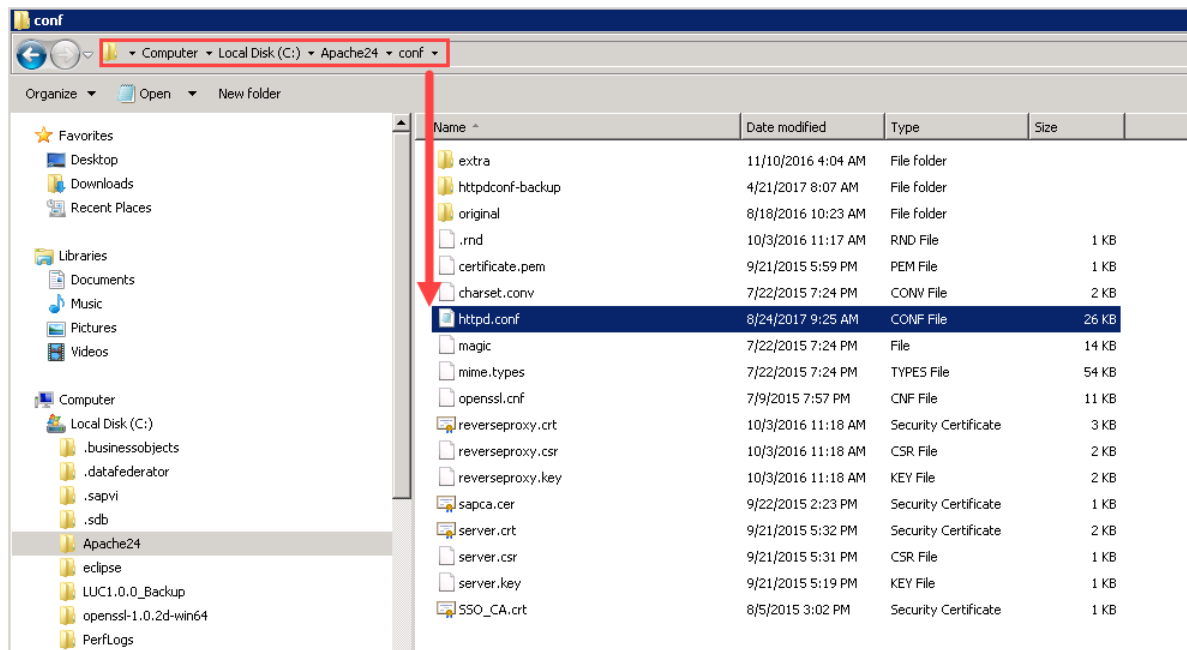
Launch a web browser on the machine where Apache HTTP server is installed and test the server with this URL: <https://localhost>. Ignore the browser warning about certificate error, and you should see the web page like the screenshot.



NOTE: If you are facing difficulties reaching your Apache host, you may need to reconfigure Apache Reverse proxy. Please refer to these documents to help install Apache — [Windows Server](#) and for [Linux](#).

Setup

1. Apache HTTP Server configuration steps
 - a. Configure the Apache HTTP Server by opening Apache24\conf\httpd.conf file in Notepad



- b. Add the following rules at the end of the file:

```
#Configure SSL on the default HTTPS port 443
LoadModule ssl_module modules/mod_ssl.so
Listen 443
```

```
SSLEngine On
SSLCertificateFile "/path/to/ssl.cert"
SSLCertificateKeyFile "/path/to/ssl.key"
```

```
SSLProxyEngine on
SSLProxyCheckPeerCN Off
SSLProxyCheckPeerName Off
```

NOTE: You may need to specify the ssl.cert certificate and ssl.key keyfile certified by your Certificate Authority in order to run Apache HTTPS Server.

```
#Specify the required modules
LoadModule proxy_module modules/mod_proxy.so
LoadModule proxy_http_module modules/mod_proxy_http.so
```

```
LoadModule headers_module modules/mod_headers.so
LoadModule xml2enc_module modules/mod_xml2enc.so

#Define the qualified domain name of the SAP Analytics Cloud URL
Define SAP_ANALYTICS_CLOUD <SAP Analytics Cloud URL>

ProxyRequests off
ProxyPreserveHost on

RequestHeader append X-Custom-Host ${SAP_ANALYTICS_CLOUD}
```

NOTE: Fill the squared brackets with the domain name of your SAP Analytics Cloud URL. For example if the URL is <https://mytenant.eu1.sapbusinessobjects.cloud>, then:
Define SAP_ANALYTICS_CLOUD <mytenant.eu1.sapbusinessobjects.cloud>

```
#Configure pass rules for remote HANA system(s)
ProxyPass /<PATH>/ http(s)://<Remote SAP HANA System Host>:<Port>/
ProxyPassReverse /<PATH>/ http(s)://<Remote SAP HANA System Host>:<Port>/
```

NOTE: Fill the squared brackets by specifying a preferable path of your HANA Instance and the XS Host of your HANA database. This could be HTTP or HTTPS as well. For example, when navigating to <http://yourHANAXSHost.domain.com:8000/> to see “XSEngine is up and running” response:



If you get the response, then:

```
ProxyPass /SID/ http://yourHANAXSHost.domain.com:8000/
ProxyPassReverse /SID/ http://yourHANAXSHost.domain.com:8000/
```

- c. Add the following rule if you're using basic authentication to suppress the browser's default authentication dialog when a user enters incorrect credentials:

```
#Role to suppress the browser's default authentication dialog
<Location /<PATH>/>
    Header unset www-authenticate
</Location>
```

- d. Test if the dispatcher rules for the remote system work properly. By opening the following URL you'll see the JSON response:

```
https://<Apache Web Host>/<PATH>/sap/bc/ina/service/v2/GetServerInfo
```

- e. Add the following lines after all pass rules for remote systems:

```
#Pass Rules for SAP Analytics Cloud
ProxyPass / https://${SAP_ANALYTICS_CLOUD}/
ProxyPassReverse / https://${SAP_ANALYTICS_CLOUD}/
```

- f. Restart the Apache service to make your changes effective.
- g. You can test if the rules are set up correctly. By opening the following URL SAP Analytics Cloud login page should open: `https://<Apache Web Host>/`
2. Configure Route rules for SAML SSO (optional). If you want to use saml sso, you have to configure them for the same idp. Remote system and SAC are using same SAML ID Provider to authenticate.

- a. Configure rules for the central SAPCP SAML Redirect Node

```
ProxyPass /authn/ https://authn.<region>.hana.ondemand.com/
ProxyPassReverse /authn/ https://authn.<region>.hana.ondemand.com /
<Location /authn/>
    ProxyHTMLEnable on
    SetOutputFilter proxy-html
    ProxyHTMLCharsetOut *
    RequestHeader unset Accept-Encoding
    ProxyHTMLURLMap https://<Your SAML Provider>/ /<Your SAML
Provider Path>/
    ProxyHTMLURLMap https://${SAP_ANALYTICS_CLOUD}/ /
    ProxyPassReverseCookiePath / /authn/
</Location> ProxyHTMLEnable
```

NOTE: You can find the <region> value in your SAP Analytics Cloud URL. If your region is eu1, you should omit the <region> value in this rewrite rule. For example, `https://authn.hana.ondemand.com`.

- b. Configure SAML Rules for remote HANA System

```
ProxyPass /<PATH>/ https://<Remote SAP HANA System Host>:<Port>/
ProxyPassReverse /<PATH>/ https://<Remote SAP HANA System
Host>:<Port>/
<Location /<PATH>/>
```

```
ProxyPassReverse /
ProxyPassReverseCookiePath /sap/hana/xs/saml
/<PATH>/sap/hana/xs/saml
</Location>
```

NOTE: Fill the squared brackets by specifying a path of your HANA Instance and the XS Host of your HANA database. This must be HTTPS only.

- c. Add rules for SAML Identity Providers
 - i. If you use the SAP Cloud Platform Identity Authentication service (IAS), add the following

```
#SAML rules for Cloud Platform IDP (IAS)
ProxyAddHeaders off
ProxyPassReverseCookieDomain <IAS Server> <Your Reversed Proxy Host Name>

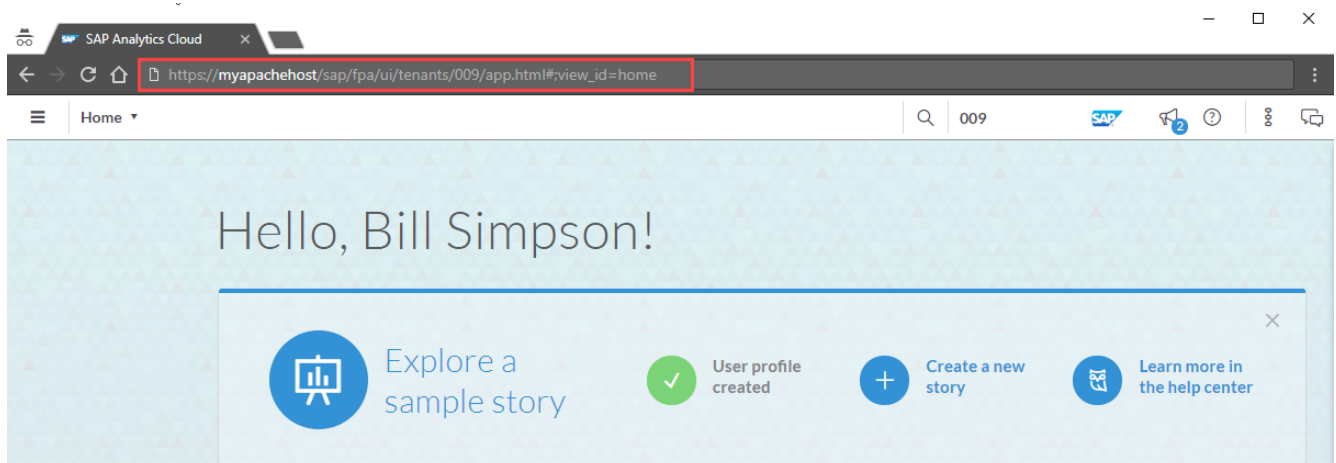
ProxyPass /saml2/ https://<IAS Server>:443/saml2/
ProxyPassReverse /saml2/ https://<IAS Server>:443/saml2/
<Location /saml2/>
  ProxyHTMLEnable on
  SetOutputFilter proxy-html
  ProxyHTMLCharsetOut *
  RequestHeader unset Accept-Encoding
  ProxyHTMLURLMap https://<SAP Analytics Cloud Server>:<Port>/sap
/sap
  ProxyHTMLURLMap https://authn.<region>.hana.ondemand.com/
/authn/
  ProxyHTMLURLMap https://<Remote SAP HANA System Host>:<Port>
/<PATH>
</Location>
ProxyPass /universalui/ https://<IAS Server>:443/universalui/
ProxyPassReverse /universalui/ https://<IAS
Server>:443/universalui/
```

- ii. If you use SAP NetWeaver or ADFS as an identity provider, please follow our users guide explaining how to configure the rules under [Live Data Connection to SAP HANA via HTTP Server](#)
- d. At the end of the file, after the pass rules for SAP Analytics Cloud, add the following

```
ProxyPass / https://${SAP_ANALYTICS_CLOUD}/
ProxyPassReverse / https://${SAP_ANALYTICS_CLOUD}/
<LocationMatch "^/$|^/sap/fpa/ui/tenants/.*/^/logout.*">
```

```
ProxyHTMLEnable on
ProxyHTMLDocType "<!DOCTYPE html>" XML
SetOutputFilter proxy-html
RequestHeader append X-Custom-Host ${SAP_ANALYTICS_CLOUD}
ProxyHTMLCharsetOut *
RequestHeader unset Accept-Encoding
ProxyHTMLURLMap https://authn.<region>.hana.ondemand.com/
/authn/
</LocationMatch>
```

- e. Restart Apache to apply your changes
3. After Apache restarted you can test if the setup has been performed successfully
 - a. Access SAP Analytics Cloud via the Apache HTTP server URL and the port you configured. For example, <https://myapachehost:443>
 - i. If you configured SAML SSO you should verify that the Apache HTTP server URL redirects within the same domain as the HTTP server you configured. This means if navigating to the <https://myapachehost> site the login URL should contain the IdP system information you setup like:
<https://myapachehost/idp/saml2/idp/sso/myidentityprovider>
 - ii. If you haven't configured SAML SSO, log on with your IDP credentials
 - iii. Verify that you are redirected back to SAP Analytics Cloud and that the domain is still the reverse proxy



4. Create a Live Data Connection to SAP HANA in SAP Analytics Cloud:

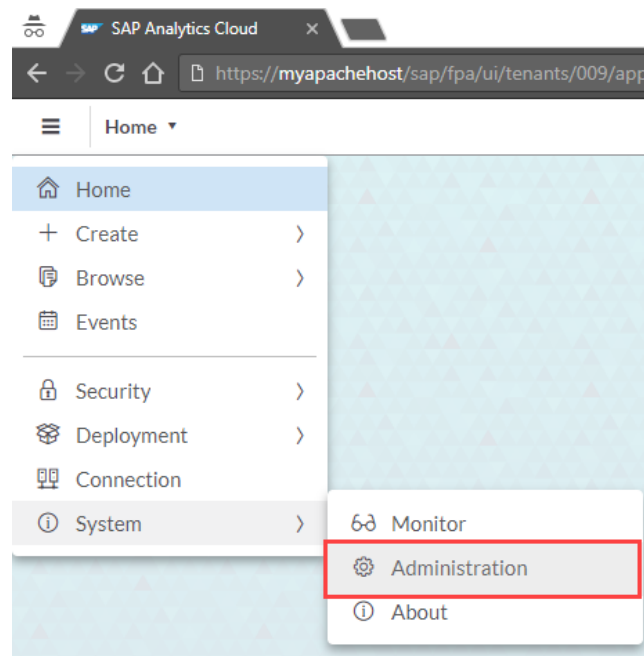
- a. Log onto of SAP Analytics Cloud and go to **Main Menu > Connection > Connections > + (Add Connection) > Live Data Connection > SAP HANA**
- b. In the dialog, enter a name for your new connection

NOTE: The connection name cannot be changed later.

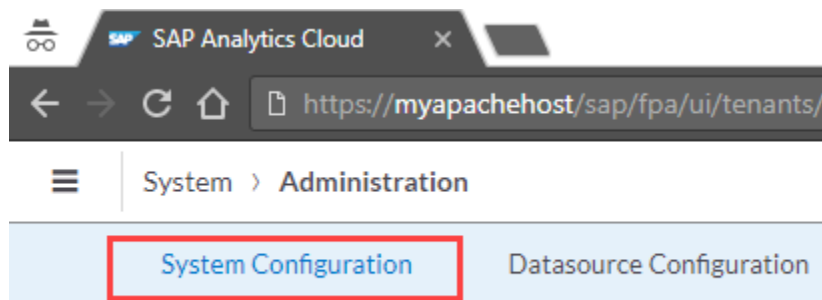
- c. Set the connection type to **Path**
- d. In the **Path Prefix** field, enter the /<PATH> value defined above
In our example above: **/SID**
- e. Select an **Authentication Method** and set the required information
 - i. Select **SAML Single Sign-On** if you're using SAML SSO

NOTE: If you want to use SAML Single Sign-On (SSO) you need to enable it by following the steps under [Enabling Single Sign-On \(SSO\)](#) under Administration.

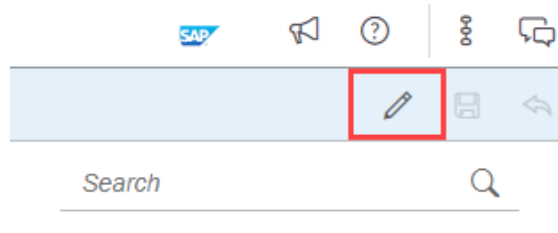
- ii. Choose **User Name and Password** if you use basic authentication to login to HANA and enter your credentials for the remote system
 - iii. If you select **None**, your SAP HANA administrator must expose the InA service on the SAP HANA XS server without any authentication requirement, or configured SAP HANA to authenticate you via other means, for example via X.509 client certificate or Kerberos. In such cases, the authentication if necessary should be achieved via your SAP HANA configuration
- f. Then select **OK**
5. Define the reverse proxy hostname in SAP Analytics Cloud under Administration. By performing this action your reverse proxy hostname will replace the URL of your SAP Analytics Cloud system included in e-mail notifications sent to users
 - a. Go to **System > Administration**



b. Choose **System Configuration** tab



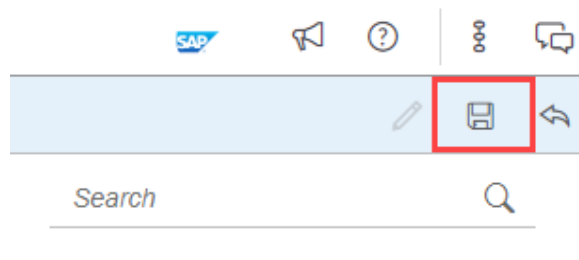
c. Click on the pencil icon to edit the settings



d. Enter the reverse proxy host name in **Reverse Proxy Host** option

| | |
|------------------------------------|--|
| Enable embedding inside an iframe | <input checked="" type="checkbox"/> ON |
| Enable Progressive Chart Rendering | <input type="checkbox"/> OFF |
| Remote Session Timeout | 30 |
| Reverse Proxy Host | myapachehost |

e. Click on **Save**



Live Data Connection setup to SAP HANA via SAP Web Dispatcher

SAP Cloud Platform (SAPCP) Connection

General Prerequisites for SAPCP Connection

- You have set up and activate the SAP HANA Info Access Service (InA), version 4.10.0 or above, on your SAP HANA system
- Create an SAP HANA info access user and assigned the `sap.bc.ina.service.v2.userRole::INA_USER` role to all users who will use the live connection
- SAP HANA version 1.00.112.04 and above, users require both the `INA_USER` role, and additional object rights. The SAP HANA administrator must grant users `SELECT` privileges on all

Live Data Connection setup to SAPCP with SSO

Prerequisites for SSO

To perform these steps, you must use an SAP HANA administrator account that is assigned to the following application roles:

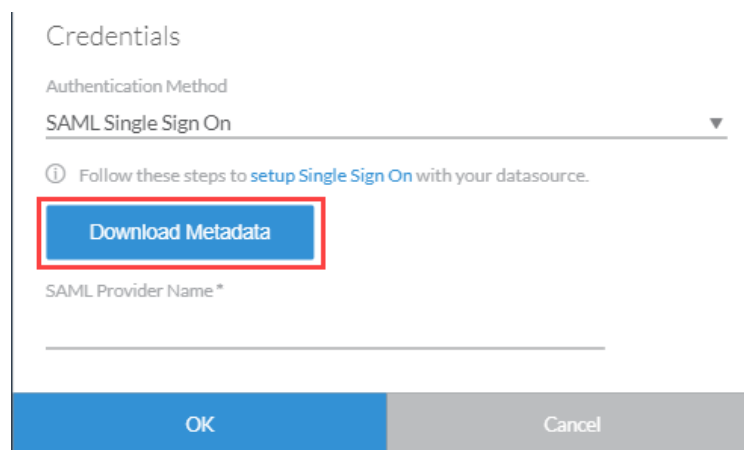
- sap.hana.xs.admin.roles::SAMLAdministrator
- sap.hana.xs.admin.roles::RuntimeConfAdministrator
- sap.hana.ide.roles::CatalogDeveloper
- sap.hana.ide.roles::SecurityAdmin

To make sure you have these roles you need to go to XS Security page of your HANA Database: <https://<yourhanadbinstance>/sap/hana/ide/security/>

You can find more info about authorizations and roles in the [Official HANA Security Guide](#).

Setup

1. Setup SAML trust relationship between the SAC tenant and the HANA database
 - a. Retrieve the SAML metadata from the SAP Analytics Cloud system
 - i. Log onto of SAP Analytics Cloud and go to **Main Menu > Connection > Connections > + (Add Connection) > Live Data Connection > SAP HANA**
 - ii. Set the connection type to **SAP Cloud Platform**
 - iii. Under **Credentials**, select **SAML Single Sign-On**
 - iv. Click on “**Download Metadata**” button



The current SSO metadata file is being downloaded on your machine.

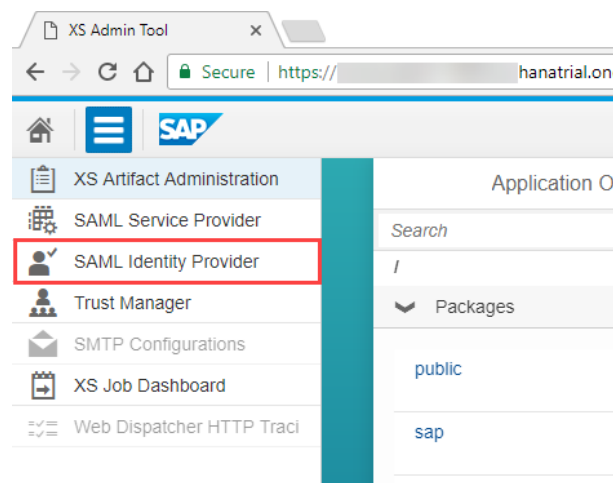
- b. Upload the SAC tenant metadata to the HANA database through XS Admin

- i. Go to the the XS Admin page of your SAP HANA system. You can access the XS Admin page at the following URL:

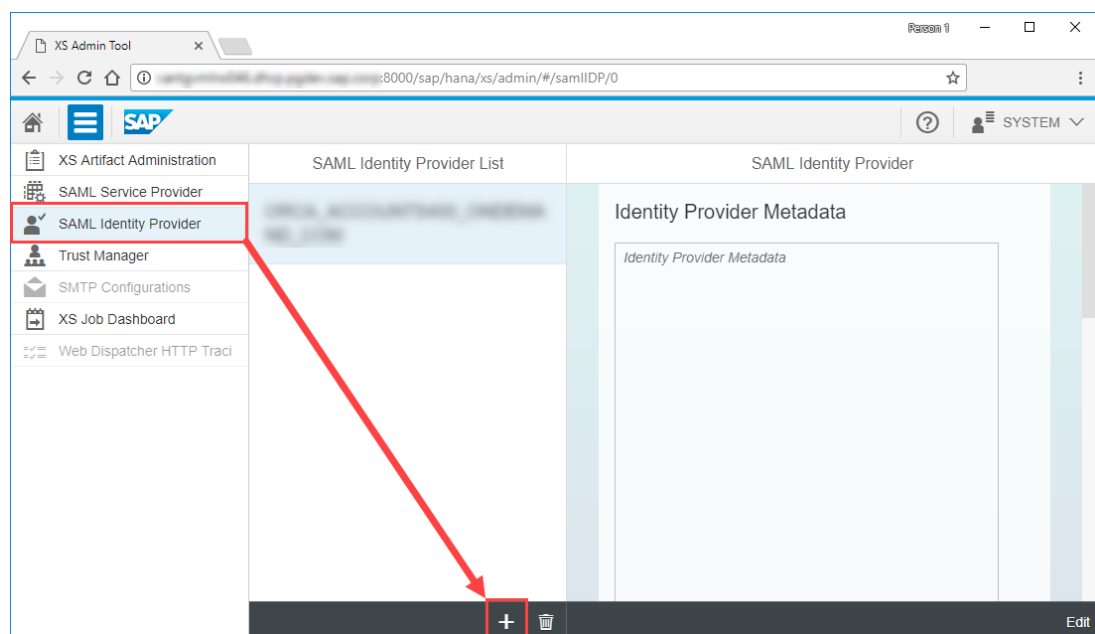
<https://<yourhanadbinstance>/sap/hana/xs/admin>

NOTE: If you are having problem accessing this site, please get in touch with your HANA Administrator as you may have roles missing.

- ii. Select “SAML Identity Provider” from the main menu



- iii. Add a new identity provider to the list by pressing the + button



- iv. Copy and paste the content from the previously downloaded metadata file into the **Metadata** textbox on the right.
- v. Click outside of the field to populate the other tabs.
- vi. Enter dummy values into the two SingleSignOn URL fields (i.e. “/saml2/sso”)
- vii. Click **Save**

Add Identity Provider Info

<ns3:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" Location="https://authn.eu1.hana.ondemand.com/saml2/sp/slo/a2548db54/a2548db54"/>
 <ns3:AssertionConsumerService index="0" isDefault="true" Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Location="https://authn.eu1.hana.ondemand.com/saml2/sp/acs/a2548db54/a2548db54"/>
 </ns3:SPSSODescriptor>
 </ns3:EntityDescriptor>

General Data

Name:

*Subject: CN= =HANA Cloud, O=SAP AG, C=DE

*Issuer: CN= =HANA Cloud, O=SAP AG, C=DE

*Entity ID:

Dynamic User Creation: ☐

Destination

*Base URL:

*SingleSignOn URL (RedirectBinding):

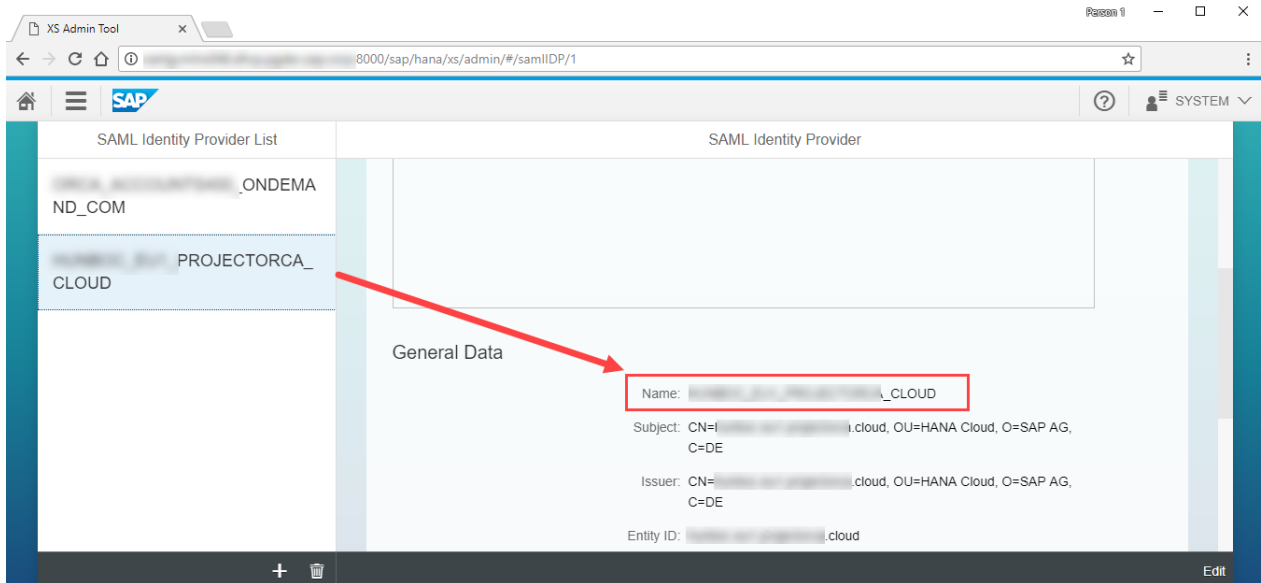
*SingleSignOn URL (PostBinding):

*SingleLogout URL (RedirectBinding):

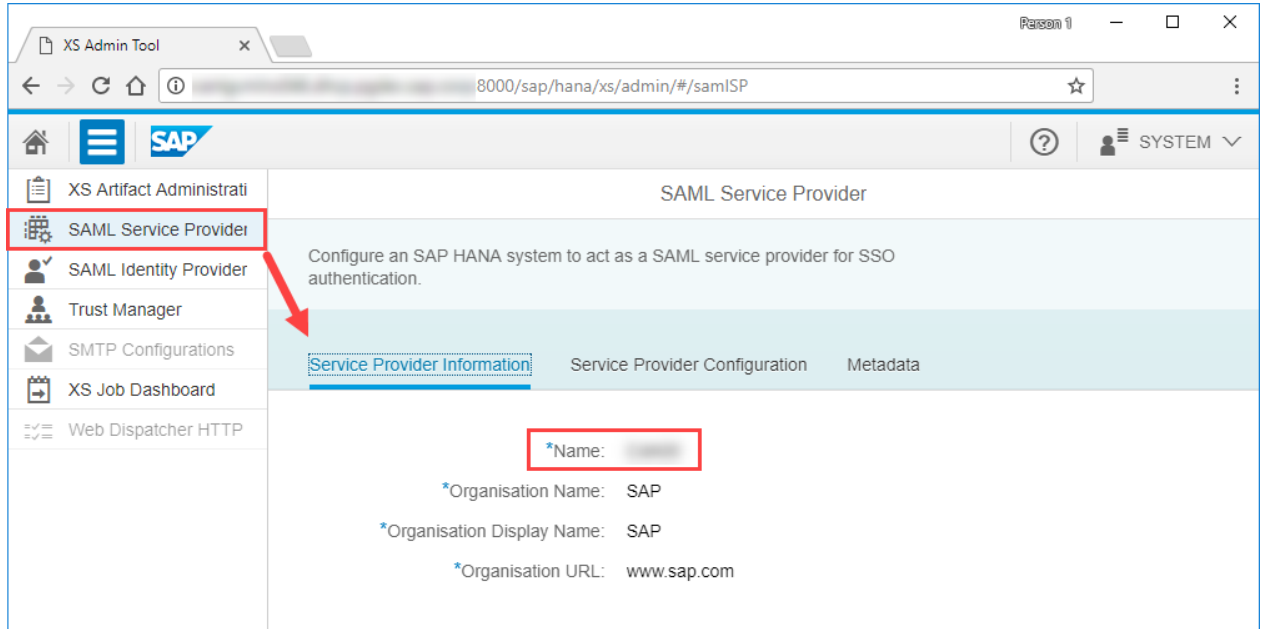
*SingleLogout URL (PostBinding):

Save **Cancel**

- viii. Take note of the “Name” value as the **SAML Identity Provider Name** for this newly created (SAC tenant) identity provider, to be used later on



- ix. Also, click on the SAML Service Provider and note of the name of the XS service provider as the **SAML Service Provider Name**

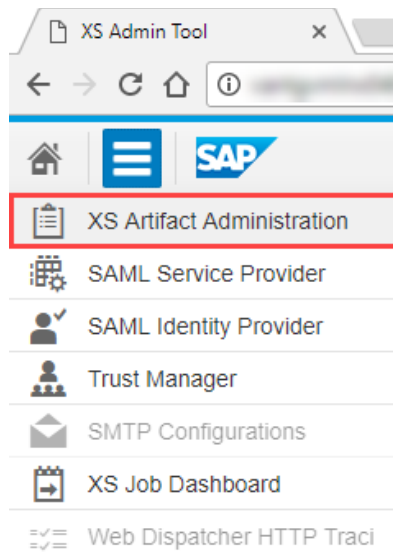


2. Enable SAML on the HANA system

- a. Login using the following URL and

[http://\[HANA_XS_HOST\]:80\[INSTANCE_NUMBER\]/sap/hana/xs/admin/](http://[HANA_XS_HOST]:80[INSTANCE_NUMBER]/sap/hana/xs/admin/)

- b. Click on **Menu > XS Artifact Administration**



- c. In the left navigation pane go to the package **sap > bc > ina > service > v2**
- d. Select the SAML checkbox if the checkbox is not already enabled
- i. Click on **Edit**
 - ii. Choose a SAML Identity Provider if an IdP is not already selected
 - iii. Select the the **SAML Identity Provider Name** noted earlier
 - iv. **Save**

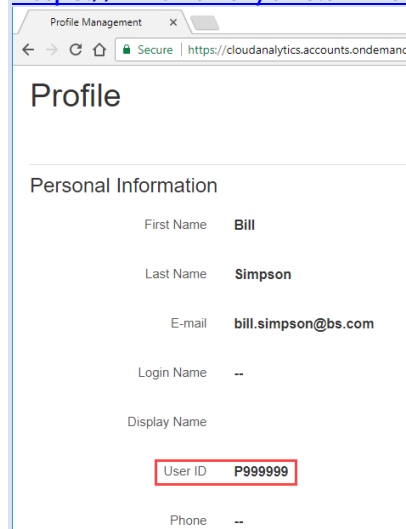
3. Manual user mapping of the users:

NOTE: If you do not map users, they will not have access to the SAP HANA database.

- a. Login to the HANA database using HANA Studio or the Web IDE as an administrator user to create users
- b. For each SAC user that requires access, create a new HANA database user
- c. Uncheck the “**Password**” checkbox, as this user should not be required to login to the database
- d. Check the “**SAML**” checkbox and click “**Configure**” to open the SAML dialog
- e. Click on Add and select the SAC tenant identity provider (noted earlier) as the “**SAML Identity Provider Name**”

- f. Enter the user ID as the “External Identity” and click OK

NOTE: To find out your User ID you will need to log in to your IdP. If you’re using SAP Cloud Identity you should be able to log in using <https://cloudanalytics.accounts.ondemand.com> website and your SAC credentials.



The screenshot shows a web browser window with the URL <https://cloudanalytics.accounts.ondemand.com>. The page title is "Profile Management" and the main heading is "Profile". Under the "Personal Information" section, the following details are listed:

- First Name: Bill
- Last Name: Simpson
- E-mail: bill.simpson@bs.com
- Login Name: --
- Display Name: --
- User ID: P999999 (highlighted with a red box)
- Phone: --

- g. Add a Granted Role:
 - i. sap.bc.ina.service.v2.userRole::INA_USER
- h. Add an Object Privilege:
 - i. _SYS_BIC with SELECT privileges

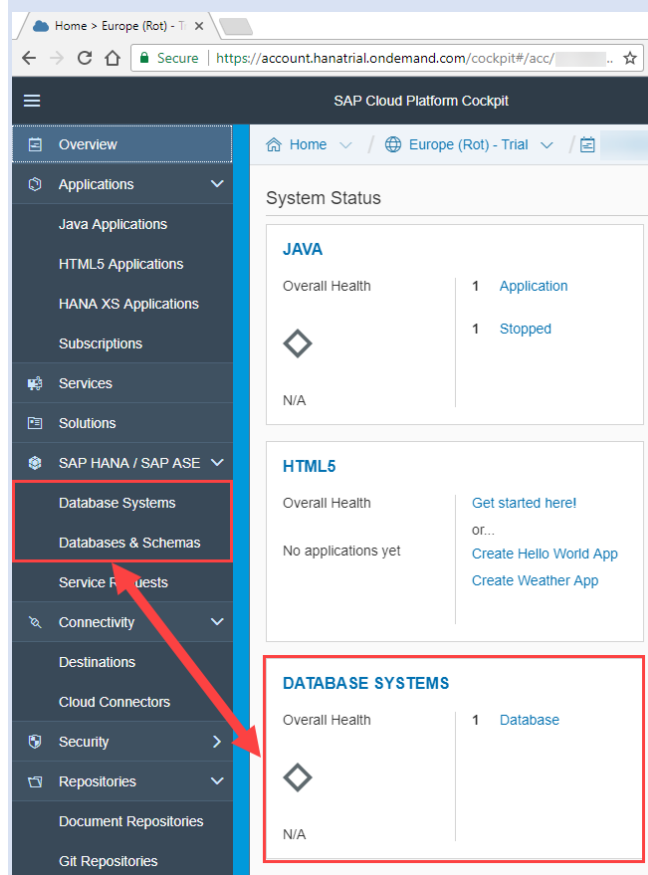
NOTE: You can select one or more views (i.e. with _SYS_BIC in the name) if more precision is desired.

- i. Save the user
4. Create a Live Data Connection to the SAP HANA Cloud Platform database in SAC
 - a. Login to SAC with one of the users that now has a database user mapped
 - b. Go to **Main Menu > Connection > Connections > + (Add Connection) > Live Data Connection > SAP HANA**
 - c. In the dialog, enter a name for your new connection

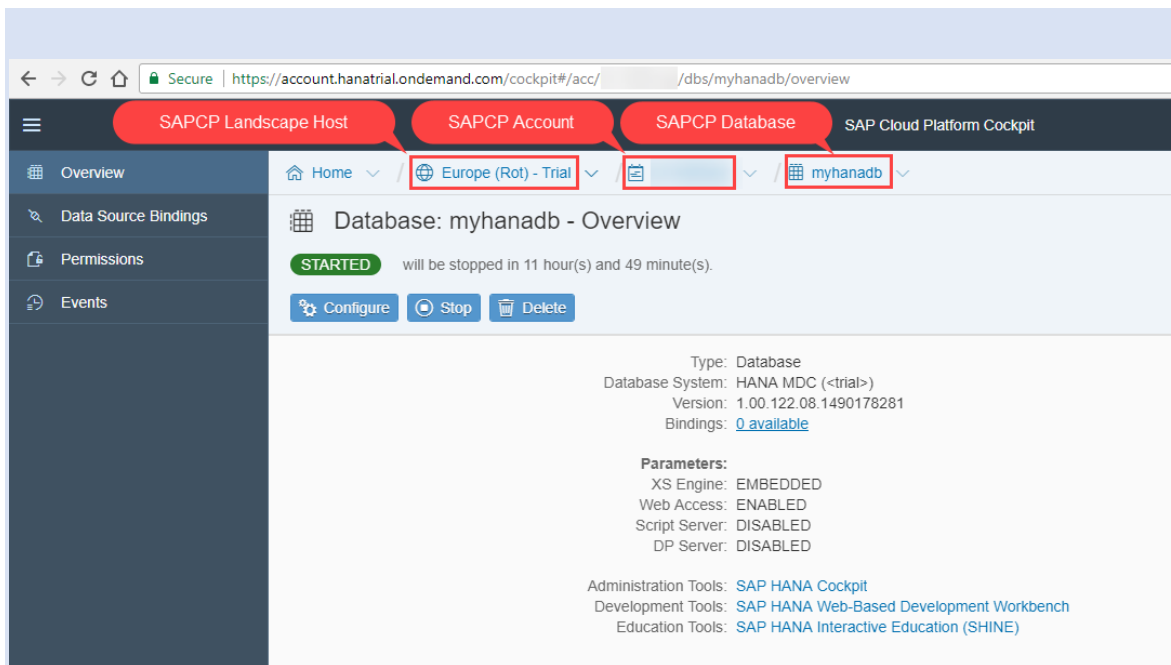
NOTE: The connection name cannot be changed later.

- d. Set the connection type to **SAP Cloud Platform**
- e. Add your SAP Cloud Platform (SAPCP) account name, database name, and landscape host

NOTE: To find out yours navigate to your database system or database schema in the SAP Cloud Platform Cockpit.



Then choose the database you want to connect to. The required information can be obtained from the SAP Cloud Platform Cockpit – Overview screen.



- f. Under **Credentials**, select **SAML Single Sign-On**
- g. SAML Provider Name:
 - i. Enter the SAML Provider Name (noted earlier as the **SAML Service Provider name**)

New HANA Live Connection

Name *

Description

Datasource Configuration

① Additional components or configuration may be required for this connection type. See our [Help Center](#) to find out what's required.

Connection Details

Connection Type

SAP Cloud Platform Account *

Database Name *

Landscape Host *

Credentials

Authentication Method

① Follow these steps to [setup Single Sign On](#) with your datasource.

Download Metadata

SAML Provider Name *

OK

Cancel

h. Click on **OK**.

Live Data Connection setup to SAPCP with User Name and Password Authentication

Prerequisites for Basic authentication

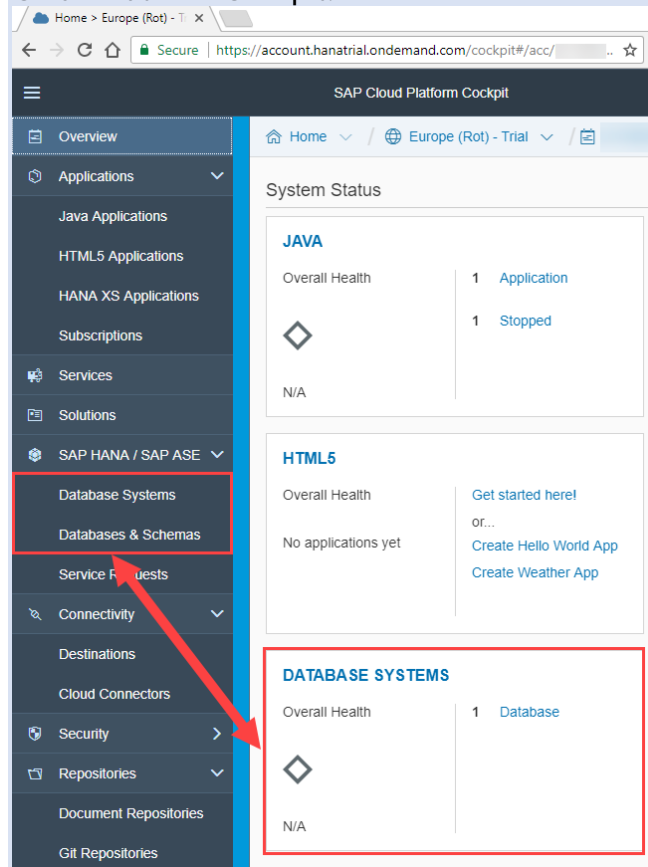
1. Ensure that the InA package (/sap/bc/ina/service/v2) or a higher-level package is configured for basic authentication

Setup

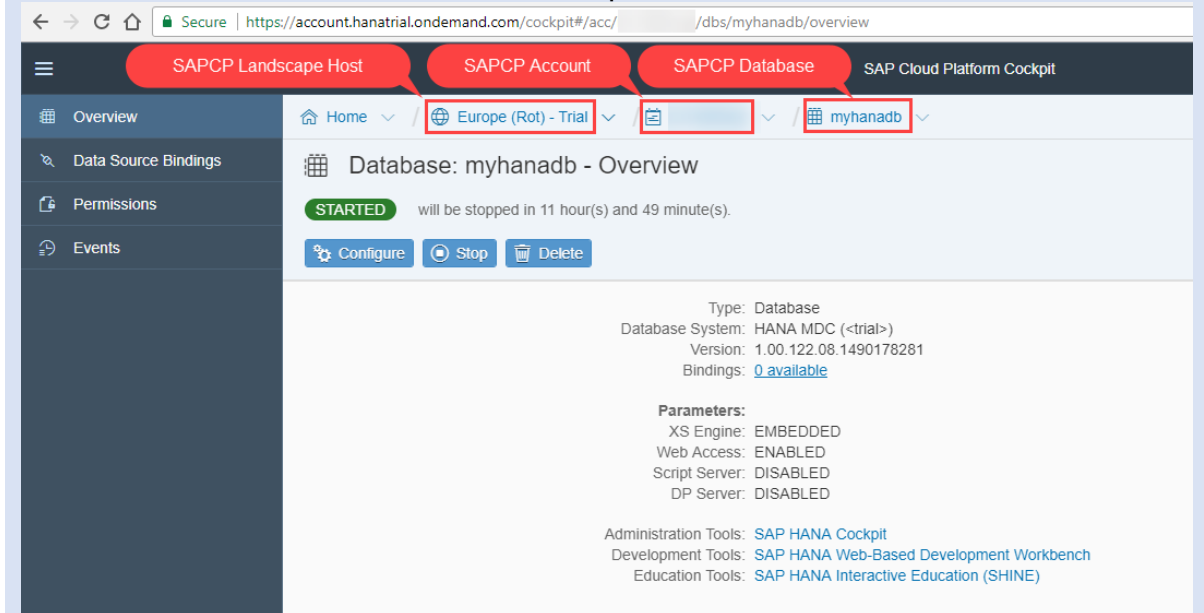
1. Create a Live Data Connection to the SAP HANA Cloud Platform database in SAC

- Login to SAC and go to **Main Menu > Connection > Connections > + (Add Connection) > Live Data Connection > SAP HANA**
 - In the dialog, enter a name for your new connection
- NOTE:** The connection name cannot be changed later.
- Set the connection type to **SAP Cloud Platform**
 - Add your SAP Cloud Platform (SAPCP) account name, database name, and landscape host

NOTE: To find out yours navigate to your database system or database schema in the SAP Cloud Platform Cockpit.



Then choose the database you want to connect to. The required information can be obtained from the SAP Cloud Platform Cockpit – Overview screen.



- e. Choose a **Default Language** from the list optionally.

NOTE: This language will always be used for this connection. It cannot be changed by users without administrator privileges. Please make sure you have installed a language on your SAPCP system before adding a language code otherwise SAC will default to the language specified by your system metadata.

- f. Under **Credentials**, select **User Name and Password** for Authentication Method
- g. Enter an SAP HANA user name and password having the `sap.bc.ina.service.v2.userRole::INA_USER` role assigned.
- h. Optionally select **Save this credential for all users on this system**

NOTE: If this option is selected, all users with Read or Maintain privileges on the Connection permission will be able to view all models or stories created from this

connection that the user entered in Step 7 has access to. For more information, see [Permissions](#).

- i. Click on **OK**