SAP BUSINESS TECHNOLOGY PLATFORM | EXTERNAL

Replication of Material Classifications Configuration Guide

SAP Responsible Design and Production Integration with SAP ERP

THE BEST RUN SAP

Table of Contents

Prerequisites

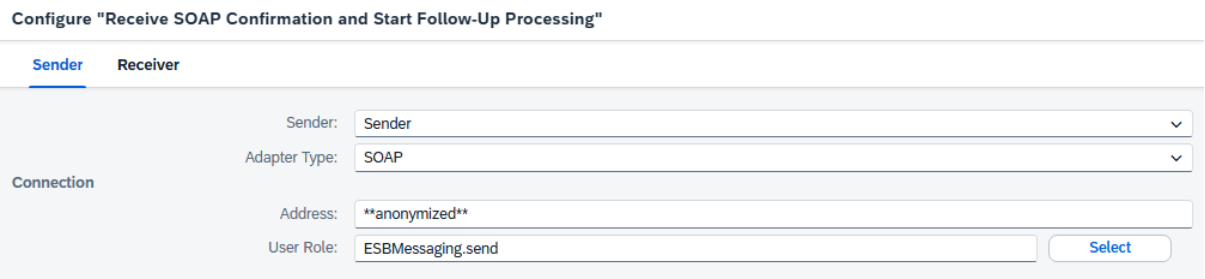
Obtain Client Certificate for authentication with Integration Flows

Follow SAP Help Portal guide: Client Certificate Authentication for Integration Flow Processing

NOTE: SAP certificates created in BTP have a maximum validity period of 1 year, external certificate may be provided to avoid this limitation. The certificate should later be imported in the S/4HANA Private Cloud instance to establish trust between BTP and the system (see Authentication section).

Configuration and Deployment of SOAP Confirmation Flow in Cloud Integration

In Cloud Integration, configure integration flow “Receive SOAP Confirmation and Start Follow-Up Processing”.
Decide on a path to the API and enter it in the Address field, e.g.: /confirmation

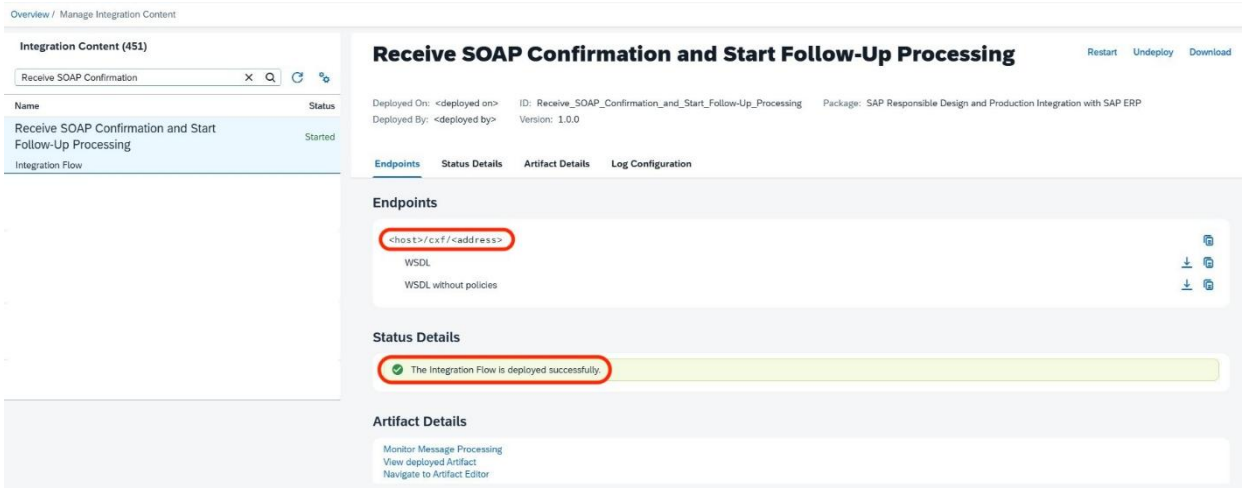


Make sure to configure the Receiver as well, it’s Address should point either to:

- Flow “Send Pricing Condition Records to S4HANA Public Cloud” if integration with S/4HANA Public Cloud is desired
- Flow “Send Records to SAP ERP Systems” if integration with S/4HANA Private Cloud or On-Premise is desired

Deploy the integration flow “Receive SOAP Confirmation and Start Follow-Up Processing” and check its deployment status.
If deployment is successful an endpoint should be listed with the path specified during configuration. Take note of this URL as it will be used later.

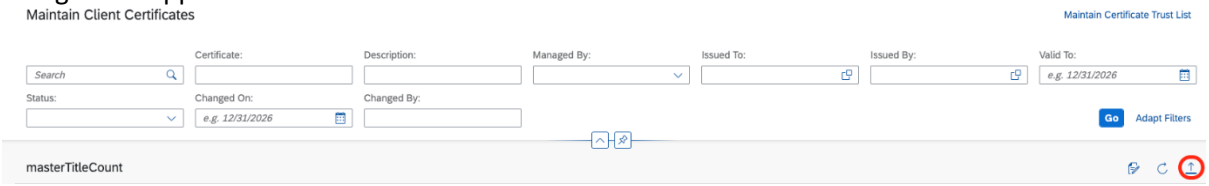
Note: It may take a few minutes for an endpoint to appear after the first deployment, a page reload may be required to appear as seen in the screenshot.


Overview / Manage Integration Content
Integration Content (451)
Receive SOAP Confirmation
Name
Status
Receive SOAP Confirmation and Start Follow-Up Processing
Started
Integration Flow
Receive SOAP Confirmation and Start Follow-Up Processing
Restart
Undeploy
Download
Deployed On: <deployed on>
ID: Receive_SOAP_Confirmation_and_Start_Follow-Up_Processing
Package: SAP Responsible Design and Production Integration with SAP ERP
Deployed By: <deployed by>
Version: 1.0.0
Endpoints
Status Details
Artifact Details
Log Configuration
Endpoints
<host>/cxf/<address>
WSDL
WSDL without policies
Status Details
The Integration Flow is deployed successfully.
Artifact Details
Monitor Message Processing
View deployed Artifact
Navigate to Artifact Editor

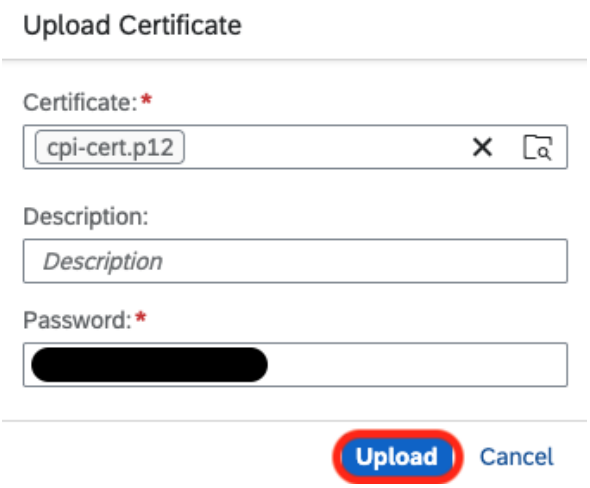
S/4HANA Public Cloud

Authentication

Navigate to App: Maintain Client Certificates



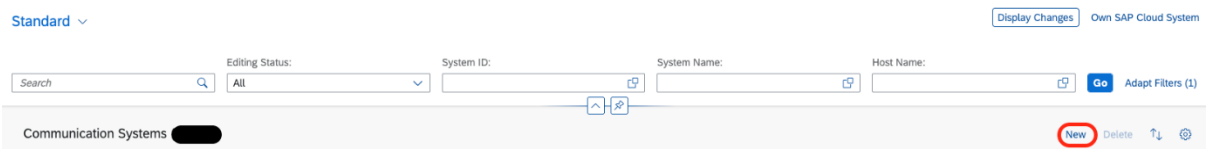
Upload Certificate



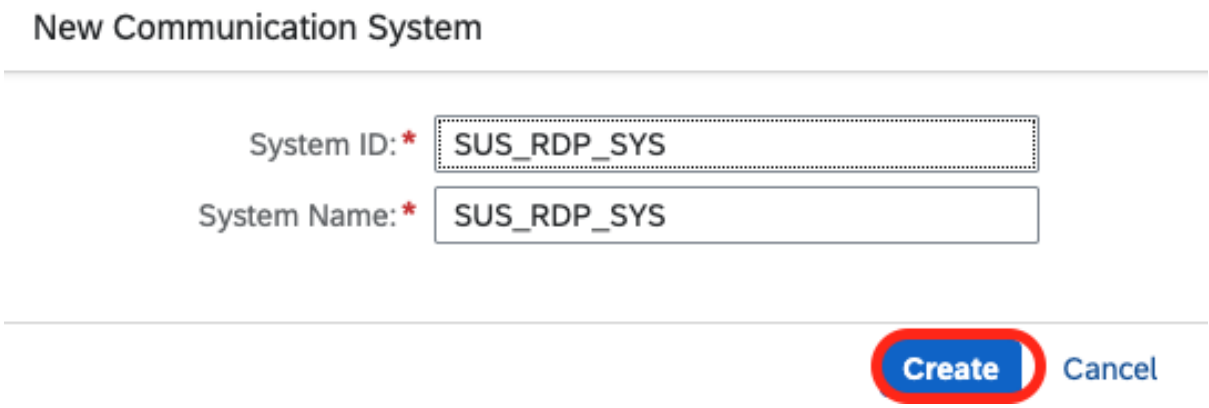
Communication System

Note down the generated name for the certificate

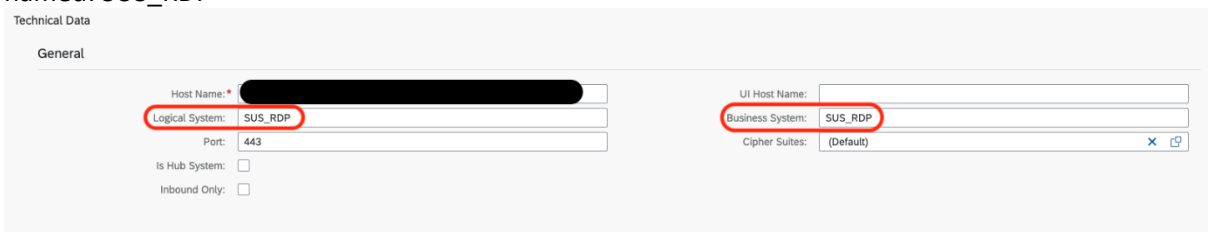
Navigate to App: Communication System and click New:



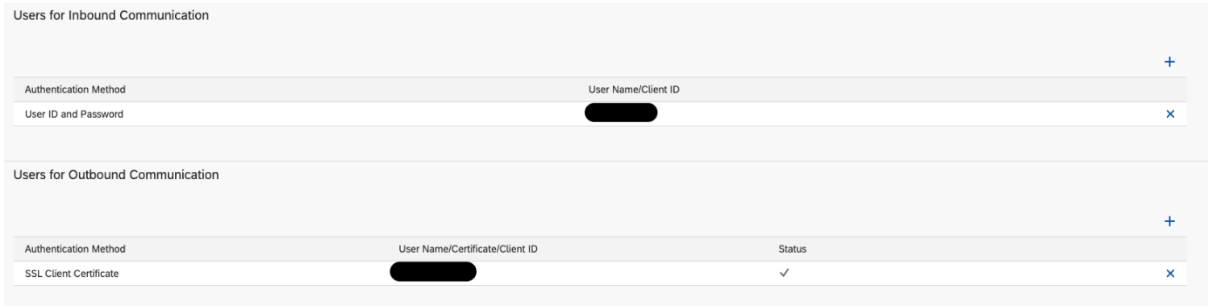
The system name does not matter, in this example it is named: SUS_RDP_SYS



Decide on a name for the system to identify the scenario and note it down, in this example it is named: SUS_RDP



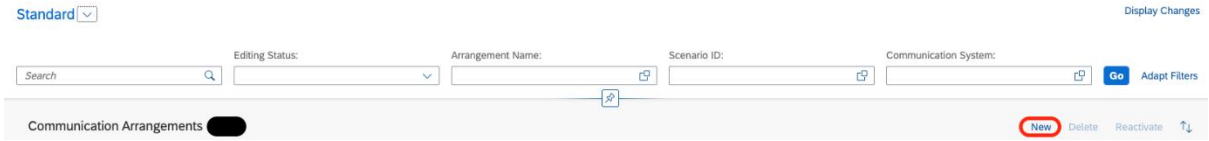
Configure authentication methods for Inbound and Outbound authentication.
In this example User ID and Password are used for Inbound communication (credentials for the S/4 system) and the CPI certificate uploaded in the previous steps is used for Outbound communication.



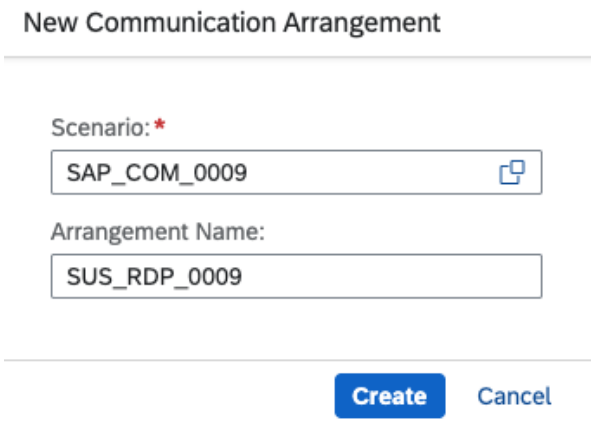
Click save:

Communication Arrangement

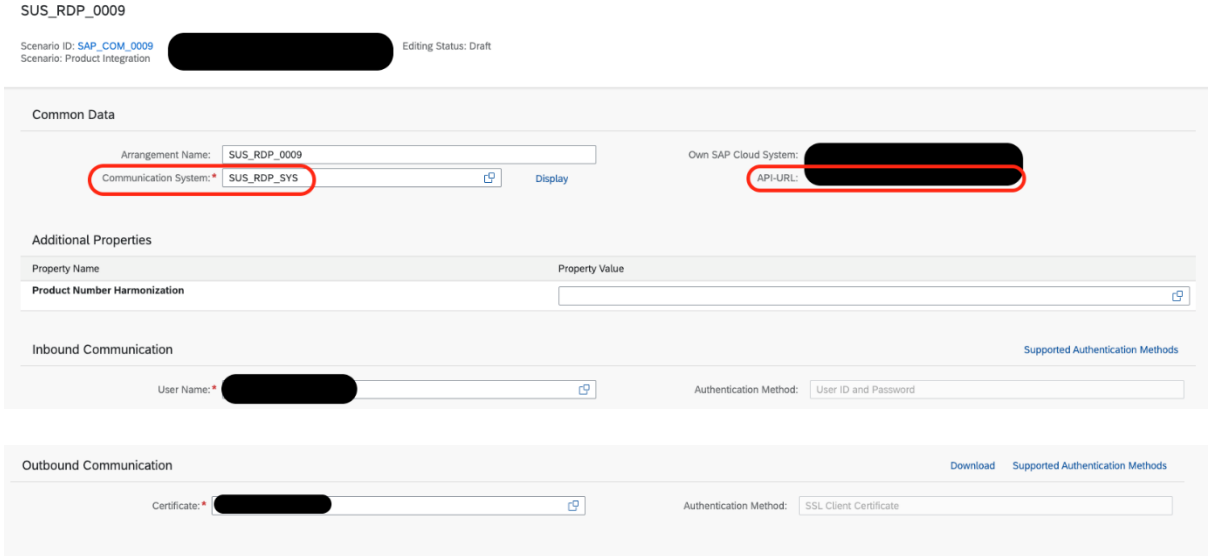
Navigate to Application: Communication Arrangements and click New



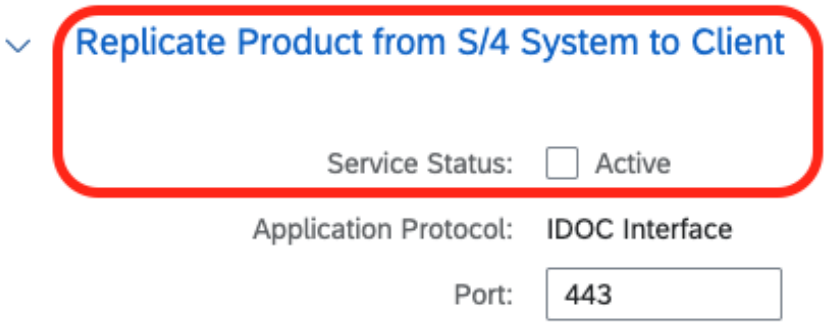
For Scenario, select SAP_COM_0009, Arrange Name can be anything, in this example it is named: SUS_RDP_0009
Click Create

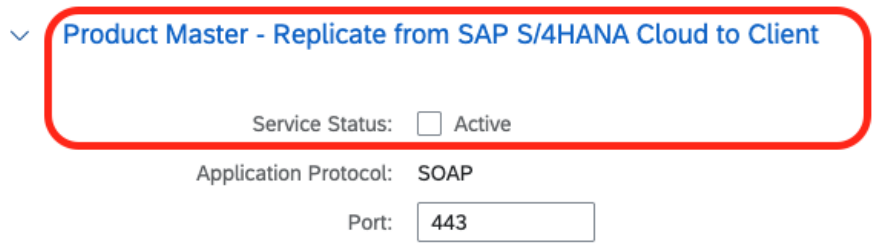


Select the previously created Communication System and ensure the correct authentication credentials are selected for Inbound and Outbound communication.
You may also take note of the API URL which will be used in the CPI Integration Flow.

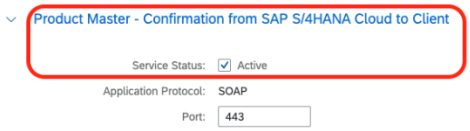


Deactivate the Outbound Services: “Product Master - Replicate from SAP S/4HANA Cloud to Client” and “Replicate Product from S/4 System to Client” as they are not needed



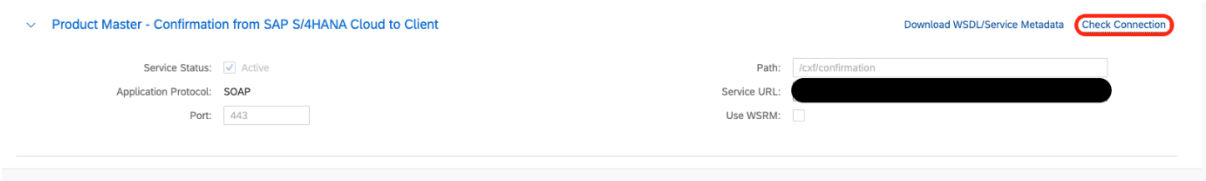


For Outbound service “Product Master - Confirmation from SAP S/4HANA Cloud to Client” make sure it is Active and adapt the Path to the one in CPI. The Service URL should equal the complete URL pointing to the “Receive SOAP Confirmation and Start Follow-Up Processing” integration flow deployed in Cloud Integration.

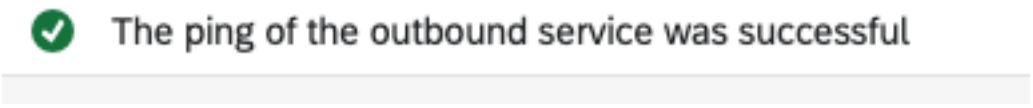


Click save:

After the arrangement is created, check connection for Outbound service ““Product Master - Confirmation from SAP S/4HANA Cloud to Client”.



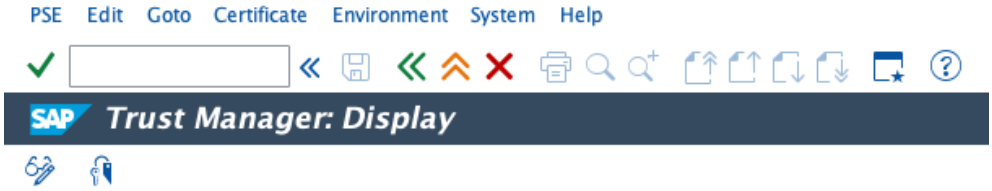
If everything is correct, the following message should appear and the configuration is complete.



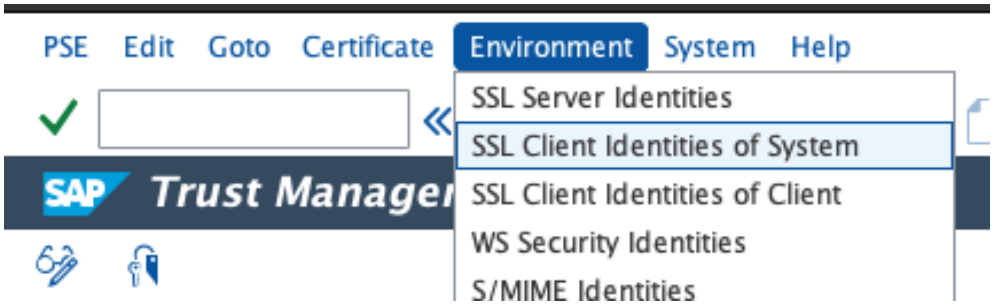
S/4HANA Private Cloud / On-Premise

Authentication

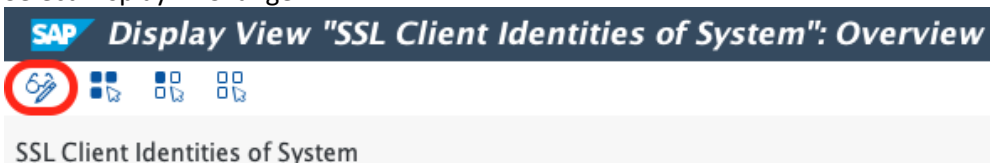
Enter transaction: STRUST



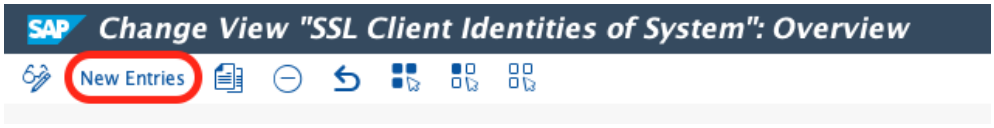
Select Environment -> SSL Client Identities of System



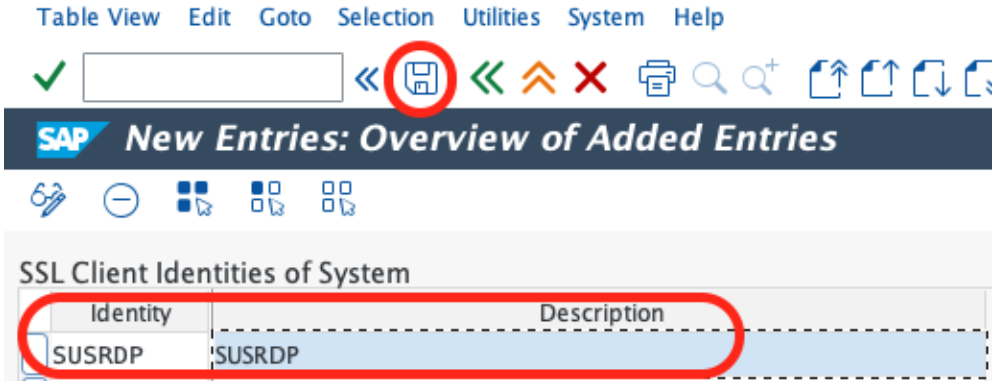
Select Display -> Change



Select New Entries



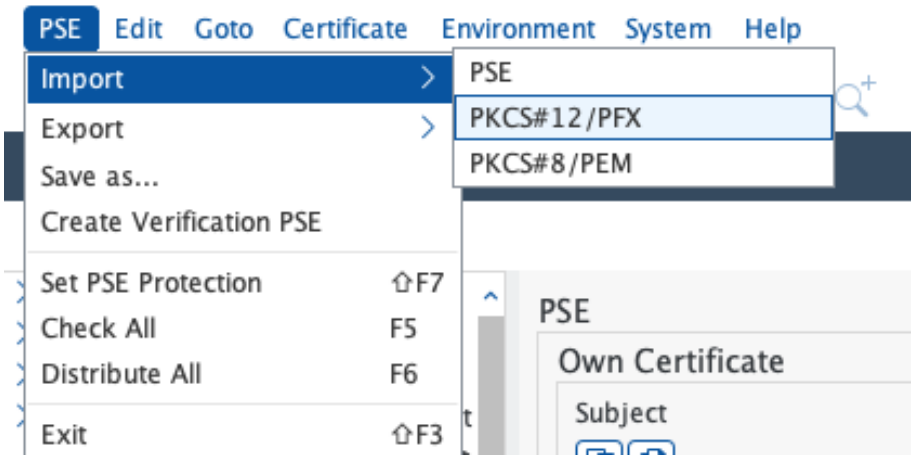
Enter a desired Identity and Description then click on the Save icon.



Go back to the main page of STRUST, the following entry should now be present:

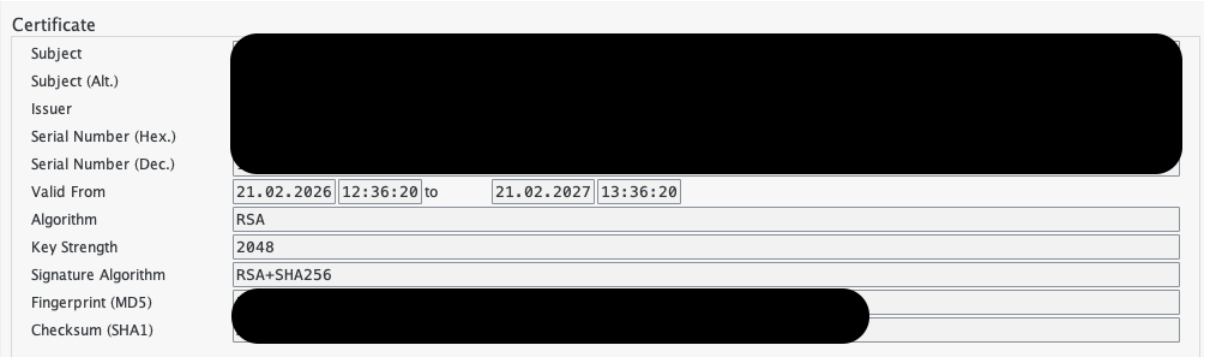
Select Display -> Change.
If you are missing permissions.
Access your user using transaction SU01 and make sure your user has the following role:
SAP_BC_SEC_AUTH_ADMIN

Select PSE -> Import -> PKCS# 12/PFX

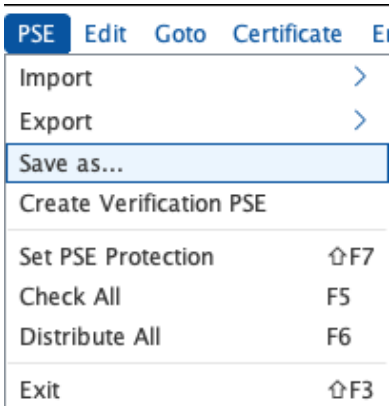


After selecting the certificate from the File upload menu the following should be visible.
Double click on the subject field maked in red.

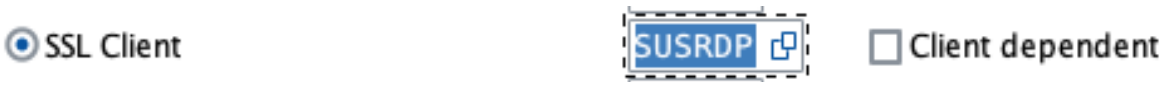
Details of the certificate should now appear:



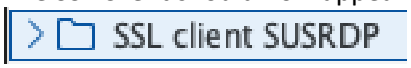
After this select PSE -> Save as…



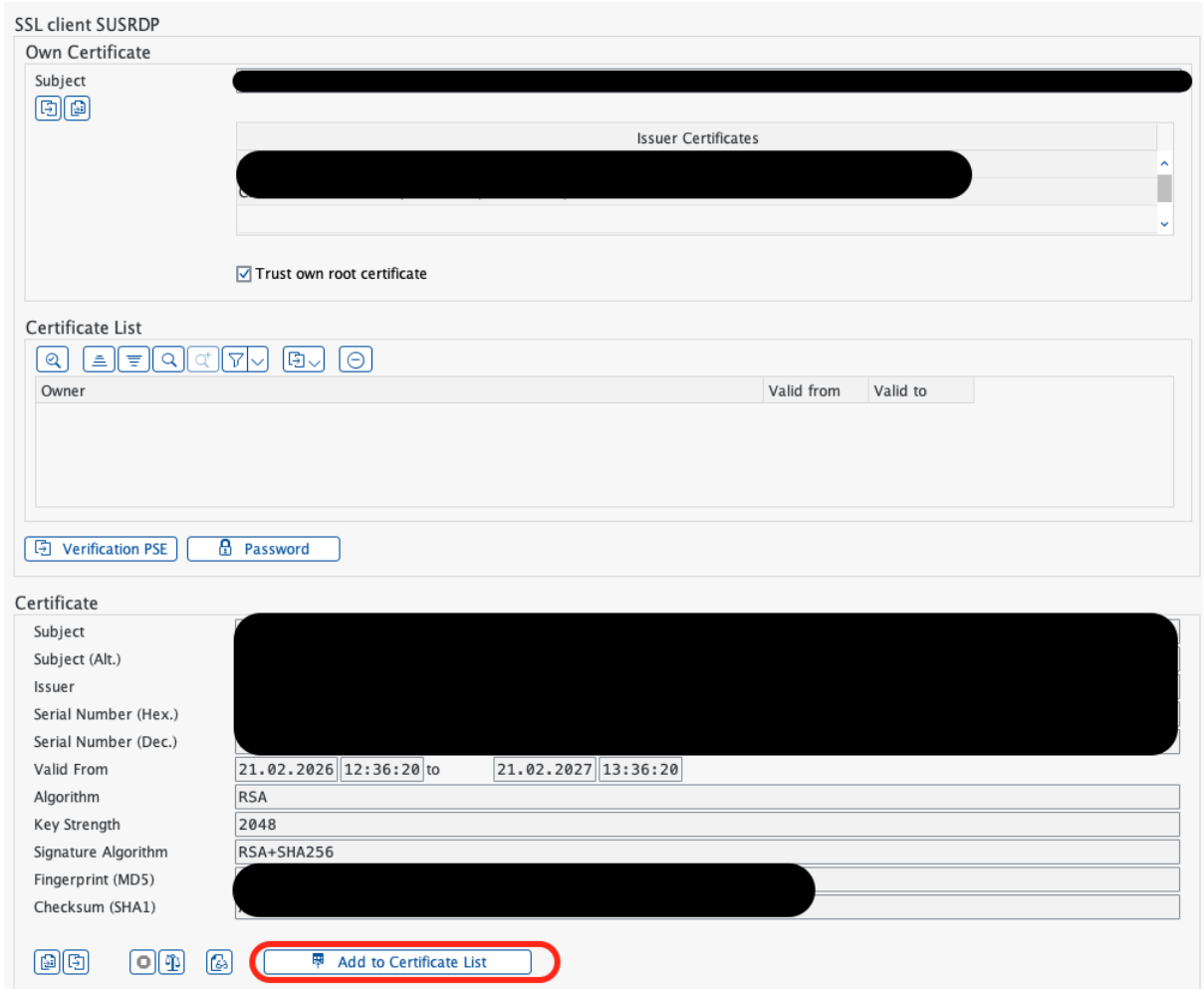
Select SSL Client, make sure to choose the newly created PSE, then confirm.



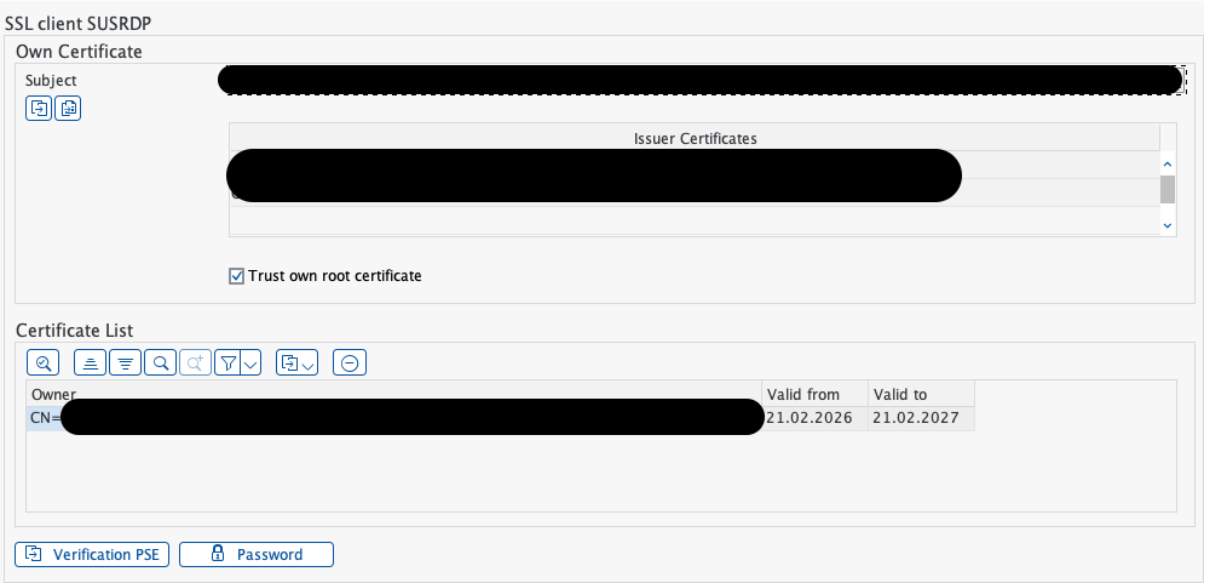
The SSL Client should now appear as a folder instead of having an X.



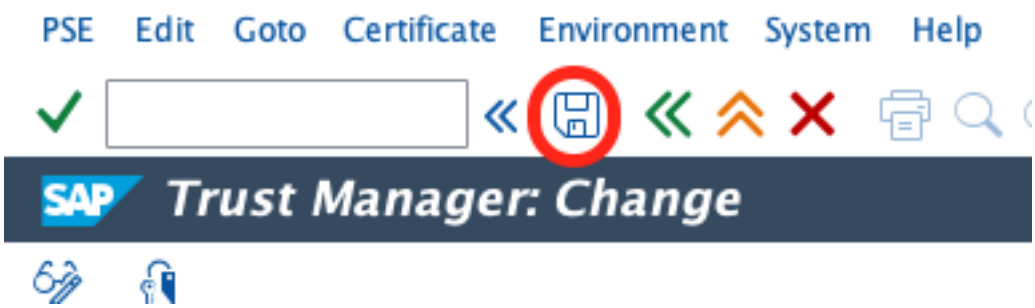
Double click on the folder the SSL client should be selected as well as the certificate.
Next click on Add to Certificate List



The certificate should now be present in the list.

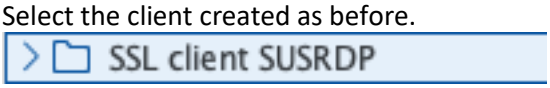


Make sure to save by pressing the Disk button.



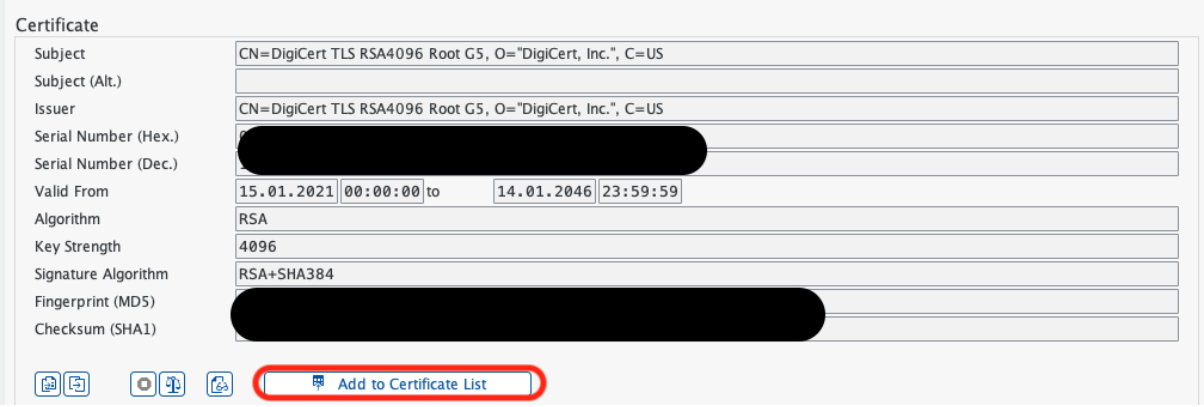
A root certificate is also required to complete the chain.
The correct certificate can be found in the CPI Instance.
Go to Monitor -> Integrations and APIs -> Manage Security -> Keystore.
It should be named sap_digicert_tls_rsa4096_root_g5 or something similar and should be maintained by SAP which is indicated by the lock icon.
Next, click on the three dots, then Download.

Go back to the S/4 sytem, and use transaction STRUST.
Select the client created as before.

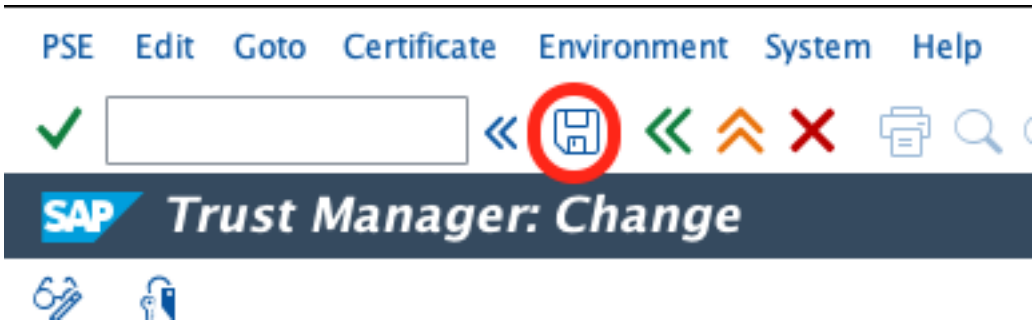


Click the Import certificate button.

With the root certificate loaded, click Add to Certificate List.



Make sure to save the changes.



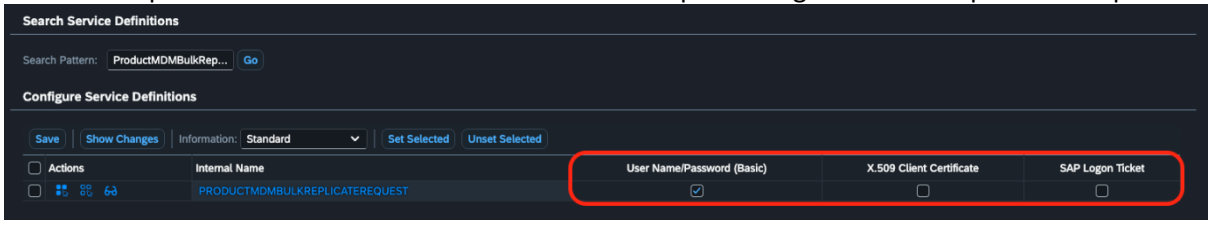
The final certificate list should look like this with both the BTP and root certificates added:

Inbound Product Request

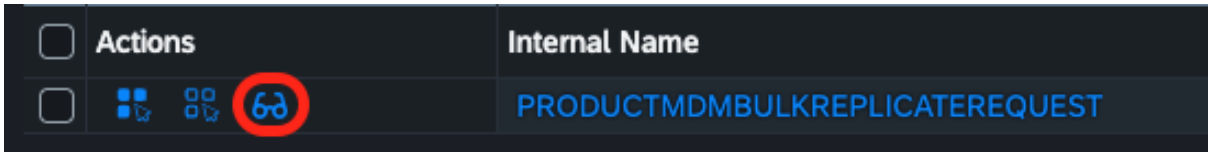
Enable the processing for service “ProductMDMBulkReplicateRequest_In” by following the procedure described in this SAP Help Portal guide: [Configuring a Service Provider (Simplified)]

Stop after Step 9 of the Procedure.
The result should look something like this, at least one authentication method should be selected.

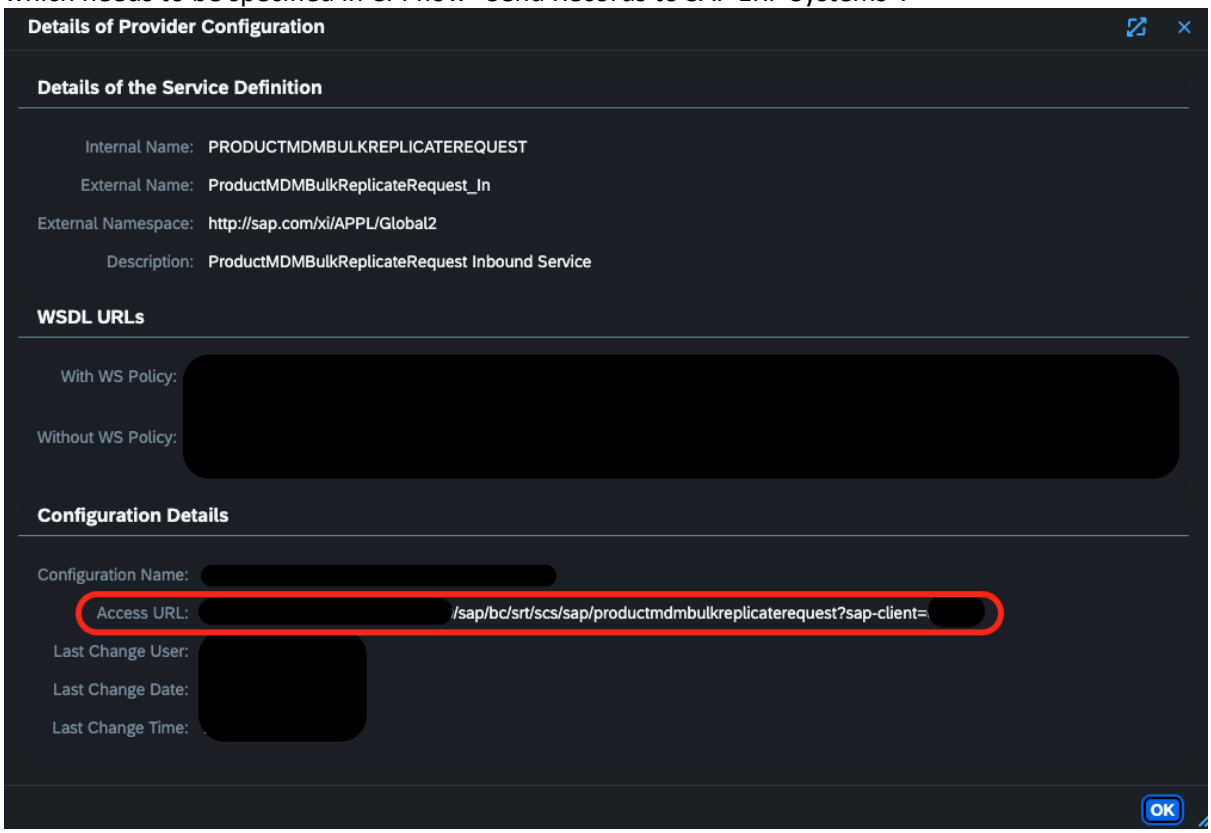
In this example Basic Authentication is used for Inbound processing of Product replication requests.



Next click on the display button:



Details should be available for the enabled service. Take note of the Access URL, this will be the URL which needs to be specified in CPI flow “Send Records to SAP ERP Systems”.

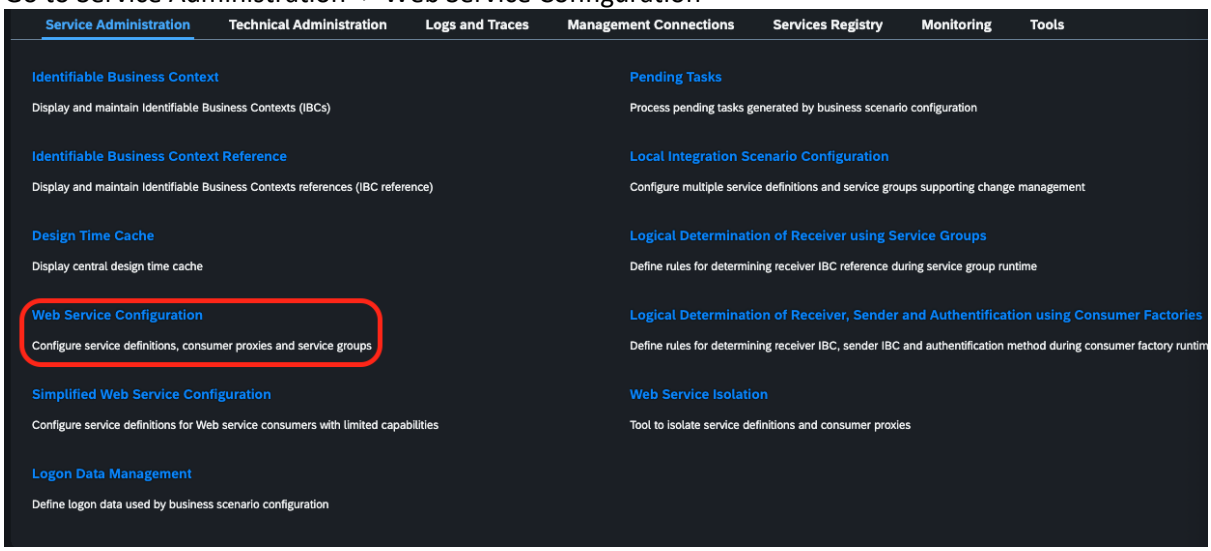


Outbound Product Confirmation

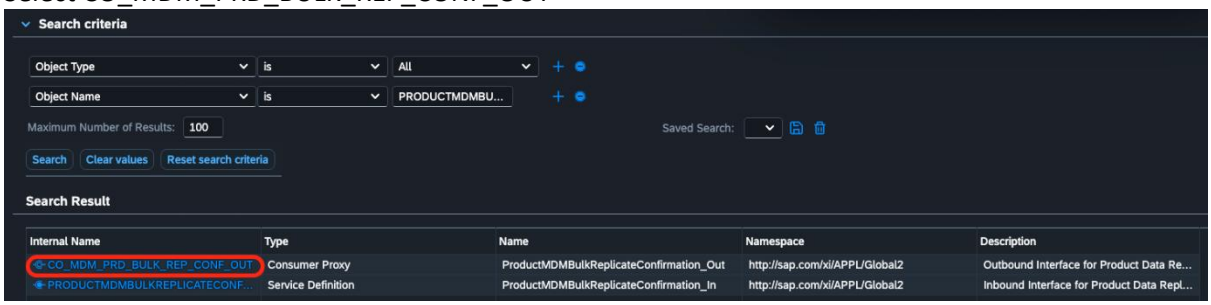
Create the Logical System in DRF by following SAP Help Portal guide: Create Logical Systems
In the guide, SUS_RDP is used as an example.

In the S/4 system, navigate to SOA Management using transaction SOAMANAGER.

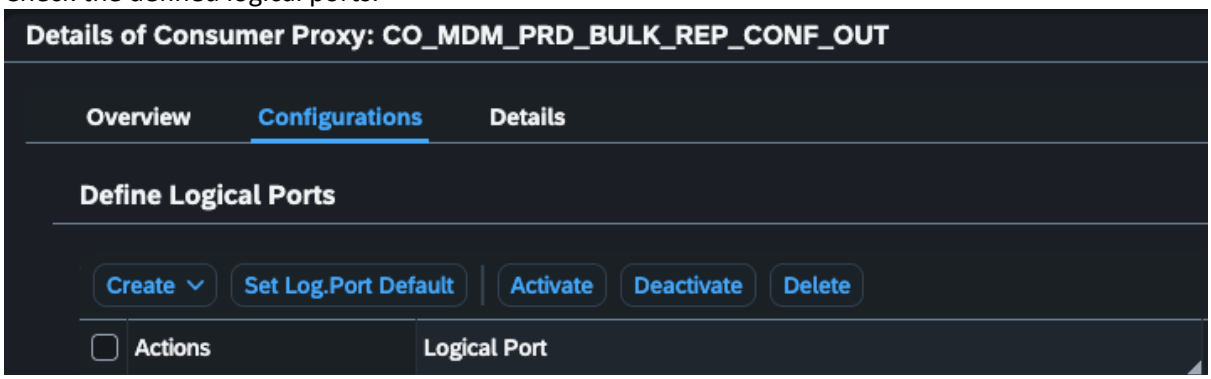
Go to Service Administration -> Web Service Configuration



Search using: Object Name is ProductMDMBulkReplicateConfirmation_Out
Select CO_MDM_PRD_BULK_REP_CONF_OUT



Check the defined logical ports.



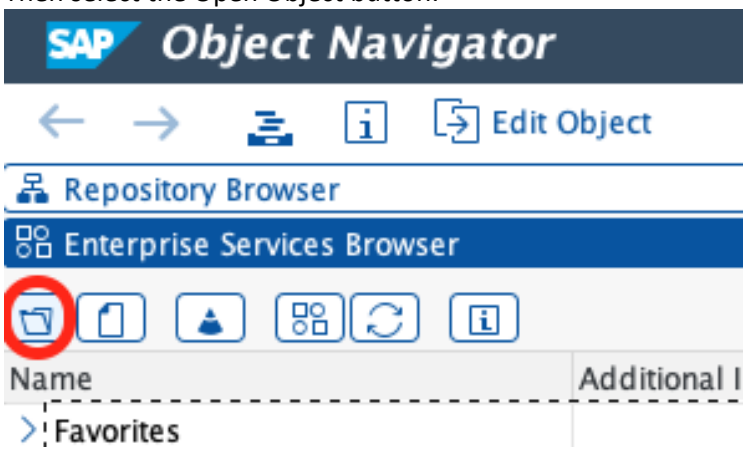
If there are no ports listed or none of them have the option Logical Port is Default set to true, then both **Setup with Default Logical Port** or **Setup without Default Logical Port** may be used. However, if that is not the case, **Setup without Default Logical Port** must be used.

Outbound Confirmation without Default Logical Port (Recommended)

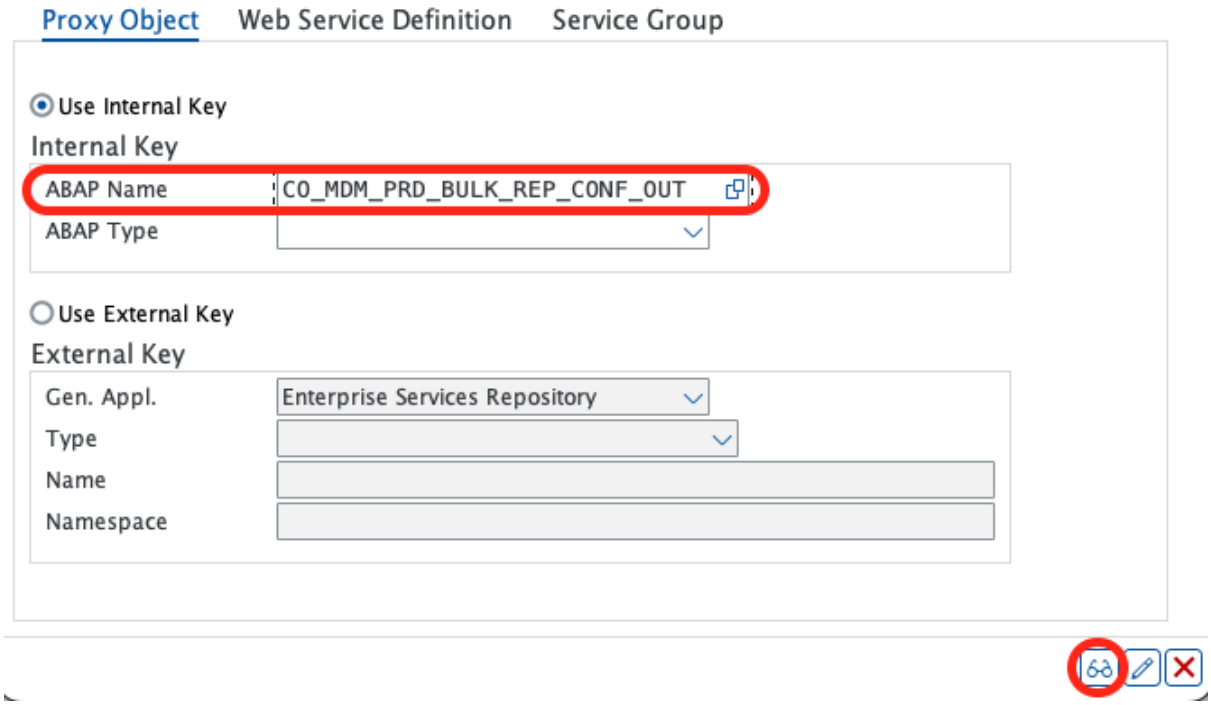
This approach involves autogenerating a proxy for the CPI Instance. It involves more steps in order to configure than the approach with Default Logical Port since CPI is considered a Third-Party System. However it is a more flexible approach and lacks the drawbacks of the setup with Default Logical Port, hence this is the recommended approach.

Upload an external WSDL

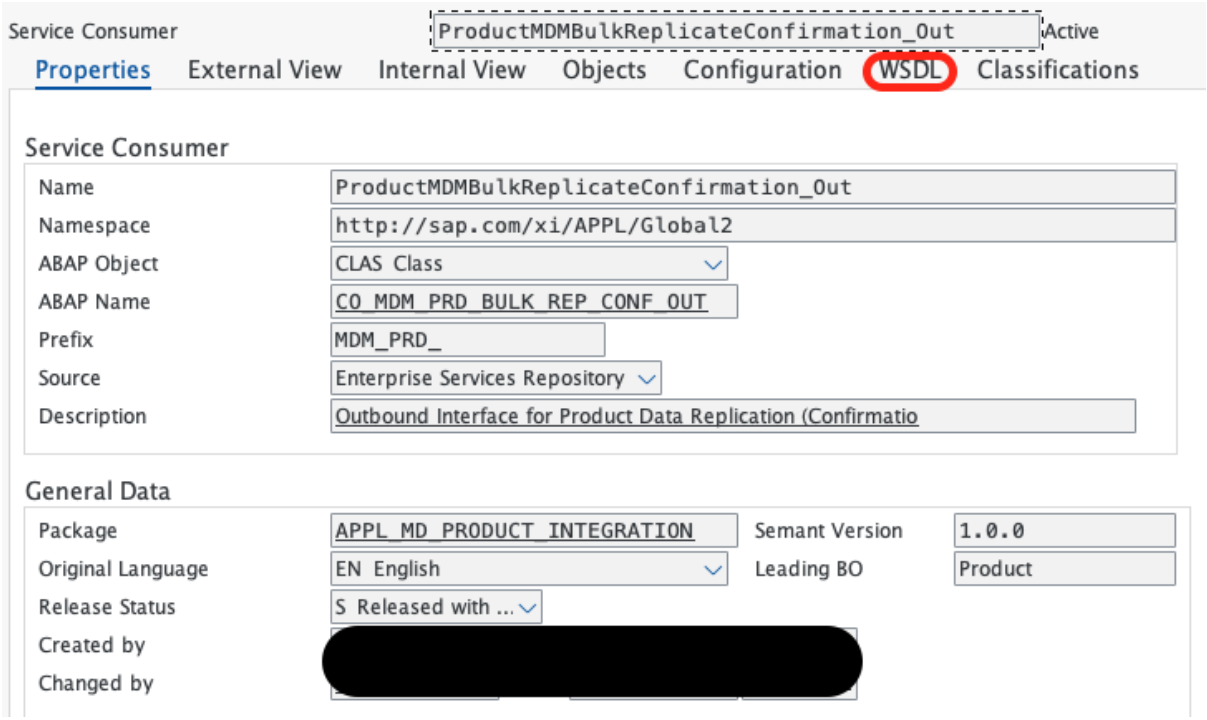
To start, in S/4HANA, enter the Object Navigator using transaction SPROXY.
Then select the Open Object button.



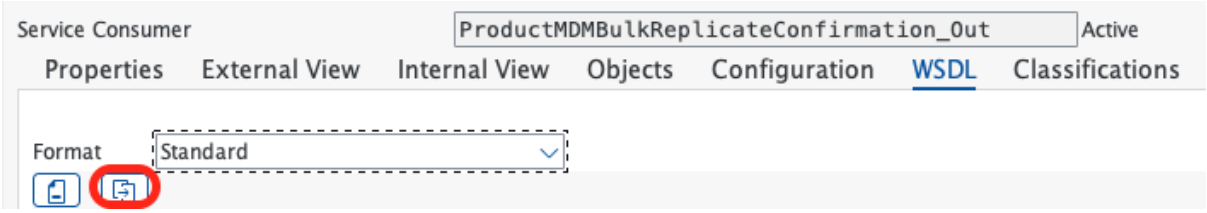
In the ABAP Name field enter: CO_MDM_PRD_BULK_REP_CONF_OUT
Then click the Display button.



The following section object should appear.
Select the WSDL tab.



Click on the Save to file… button and store the file where convenient.



Open the downloaded .wsdl file in an editor of choice and add the following sections to the WSDL at the bottom just before the closing `</wsdl:definitions>` tag.

```
<wsp:Policy wsu:Id="BN__CLIENT_CERTIFICATE">
  <wsp:ExactlyOne>
    <wsp:All>
      <sapattahnd:Enabled
xmlns:sapattahnd="http://www.sap.com/710/features/attachment/">true</sapattahnd:Enabled>
      <saptrnbnd:OptimizedMimeSerialization

xmlns:saptrnbnd="http://schemas.xmlsoap.org/ws/2004/09/policy/optimizedmimeserialization"
        wsp:Optional="true" />
      <wsrmp:RMAssertion xmlns:wsrmp="http://docs.oasis-open.org/ws-rx/wsrmp/200702">
        <wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" />
      </wsrmp:RMAssertion>
      <wsaw:UsingAddressing xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" />
      <wsp:All xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <sp:TransportBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702"
          xmlns:sapsp="http://www.sap.com/webas/630/soap/features/security/policy"
          xmlns:wsa="http://www.w3.org/2005/08/addressing"
          xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
          xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
          xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken>
                  <wsp:Policy>
                    <sp:RequireClientCertificate />
                  </wsp:Policy>
                </sp:HttpsToken>
              </wsp:Policy>
```

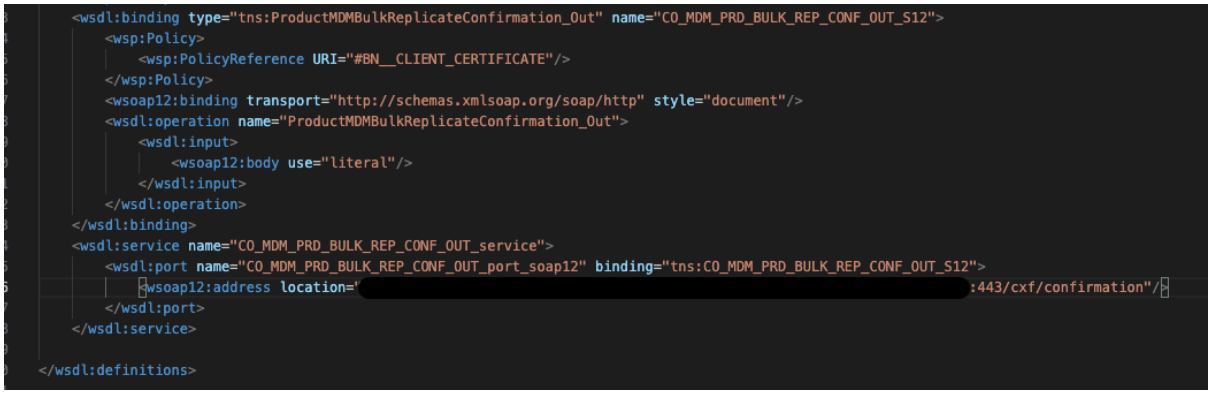
```
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic128Rsa15 />
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict />
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
      </wsp:All>
    </wsp:All>
    <wsp:All>
      <sapattahnd:Enabled
xmlns:sapattahnd="http://www.sap.com/710/features/attachment/">true</sapattahnd:Enabled>
      <saptrnbnd:OptimizedMimeSerialization

xmlns:saptrnbnd="http://schemas.xmlsoap.org/ws/2004/09/policy/optimizedmimeserialization"
        wsp:Optional="true" />
      <wsrm:RMAssertion xmlns:wsrm="http://schemas.xmlsoap.org/ws/2005/02/rm/policy" />
      <wsaw:UsingAddressing xmlns:wsaw="http://schemas.xmlsoap.org/ws/2004/08/addressing"
/>
      <wsp:All xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <sp:TransportBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702"
          xmlns:sapsp="http://www.sap.com/webas/630/soap/features/security/policy"
          xmlns:wsa="http://www.w3.org/2005/08/addressing"
          xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
          xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
          xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken>
                  <wsp:Policy>
                    <sp:RequireClientCertificate />
                  </wsp:Policy>
                </sp:HttpsToken>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic128Rsa15 />
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict />
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
      </wsp:All>
    </wsp:All>
    <wsp:All>
      <sapattahnd:Enabled
xmlns:sapattahnd="http://www.sap.com/710/features/attachment/">true</sapattahnd:Enabled>
      <saptrnbnd:OptimizedXMLTransfer uri="http://xml.sap.com/2006/11/esi/esp/binxml"
        xmlns:saptrnbnd="http://www.sap.com/webas/710/soap/features/transportbinding/"
        wsp:Optional="true" />
      <wsrmp:RMAssertion xmlns:wsrmp="http://docs.oasis-open.org/ws-rx/wsrmp/200702">
        <wsp:Policy xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy" />
      </wsrmp:RMAssertion>
      <wsaw:UsingAddressing xmlns:wsaw="http://www.w3.org/2006/05/addressing/wsdl" />
      <wsp:All xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <sp:TransportBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702"
          xmlns:sapsp="http://www.sap.com/webas/630/soap/features/security/policy"
          xmlns:wsa="http://www.w3.org/2005/08/addressing"
          xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
          xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
          xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex">
          <wsp:Policy>
            <sp:TransportToken>
```

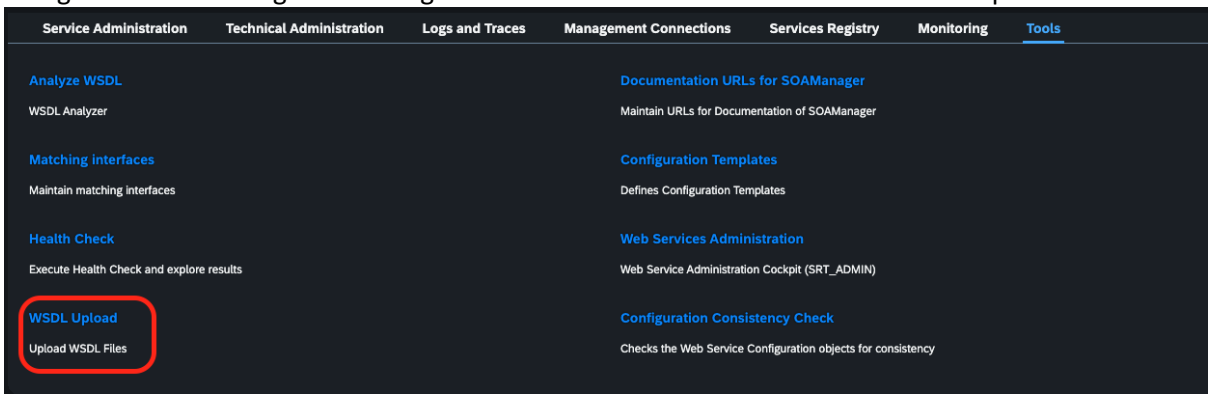
```
              <wsp:Policy>
                <sp:HttpsToken>
                  <wsp:Policy>
                    <sp:RequireClientCertificate />
                  </wsp:Policy>
                </sp:HttpsToken>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic128Rsa15 />
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict />
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
      </wsp:All>
    </wsp:All>
    <wsp:All>
      <sapattahnd:Enabled
xmlns:sapattahnd="http://www.sap.com/710/features/attachment/">true</sapattahnd:Enabled>
      <saptrnbnd:OptimizedXMLTransfer uri="http://xml.sap.com/2006/11/esi/esp/binxml"
        xmlns:saptrnbnd="http://www.sap.com/webas/710/soap/features/transportbinding/"
        wsp:Optional="true" />
      <wsrm:RMAssertion xmlns:wsrm="http://schemas.xmlsoap.org/ws/2005/02/rm/policy" />
      <wsaw:UsingAddressing xmlns:wsaw="http://schemas.xmlsoap.org/ws/2004/08/addressing"
/>
      <wsp:All xmlns:wsp="http://schemas.xmlsoap.org/ws/2004/09/policy">
        <sp:TransportBinding xmlns:sp="http://docs.oasis-open.org/ws-sx/ws-
securitypolicy/200702"
          xmlns:sapsp="http://www.sap.com/webas/630/soap/features/security/policy"
          xmlns:wsa="http://www.w3.org/2005/08/addressing"
          xmlns:wst="http://docs.oasis-open.org/ws-sx/ws-trust/200512"
          xmlns:wsu="http://schemas.xmlsoap.org/ws/2002/07/utility"
          xmlns:wsx="http://schemas.xmlsoap.org/ws/2004/09/mex">
          <wsp:Policy>
            <sp:TransportToken>
              <wsp:Policy>
                <sp:HttpsToken>
                  <wsp:Policy>
                    <sp:RequireClientCertificate />
                  </wsp:Policy>
                </sp:HttpsToken>
              </wsp:Policy>
            </sp:TransportToken>
            <sp:AlgorithmSuite>
              <wsp:Policy>
                <sp:Basic128Rsa15 />
              </wsp:Policy>
            </sp:AlgorithmSuite>
            <sp:Layout>
              <wsp:Policy>
                <sp:Strict />
              </wsp:Policy>
            </sp:Layout>
          </wsp:Policy>
        </sp:TransportBinding>
      </wsp:All>
    </wsp:All>
  </wsp:ExactlyOne>
</wsp:Policy>
<wsdl:binding type="tns:ProductMDMBulkReplicateConfirmation_Out"
  name="CO_MDM_PRD_BULK_REP_CONF_OUT_S12">
  <wsp:Policy>
    <wsp:PolicyReference URI="#BN__CLIENT_CERTIFICATE" />
  </wsp:Policy>
  <wsoap12:binding transport="http://schemas.xmlsoap.org/soap/http" style="document" />
  <wsdl:operation name="ProductMDMBulkReplicateConfirmation_Out">
    <wsdl:input>
      <wsoap12:body use="literal" />
    </wsdl:input>
  </wsdl:operation>
</wsdl:binding>
```

```
<wsdl:service name="CO_MDM_PRD_BULK_REP_CONF_OUT_service">
  <wsdl:port name="CO_MDM_PRD_BULK_REP_CONF_OUT_port_soap12"
    binding="tns:CO_MDM_PRD_BULK_REP_CONF_OUT_S12">
    <wsoap12:address location="<URL_TO_SOAP_API>" />
  </wsdl:port>
</wsdl:service>
```

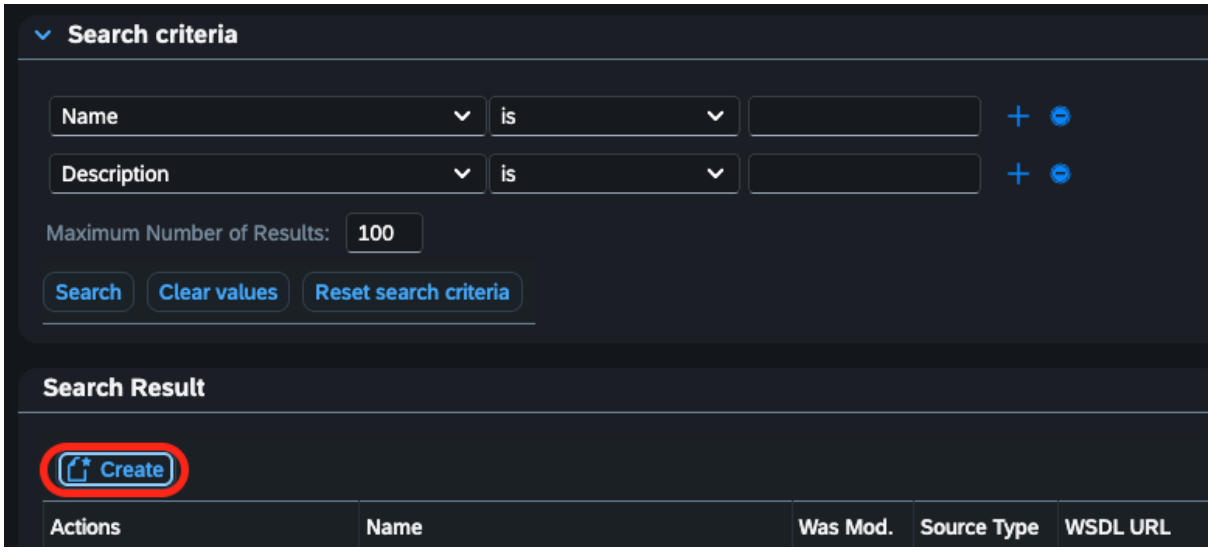
Replace <URL_TO_SOAP_API> placeholder with the actual address pointing to the “Receive SOAP Confirmation and Start Follow-Up Processing” integration flow in Cloud Integration. Make sure to include the port :443 after the host as shown in the screenshot below.



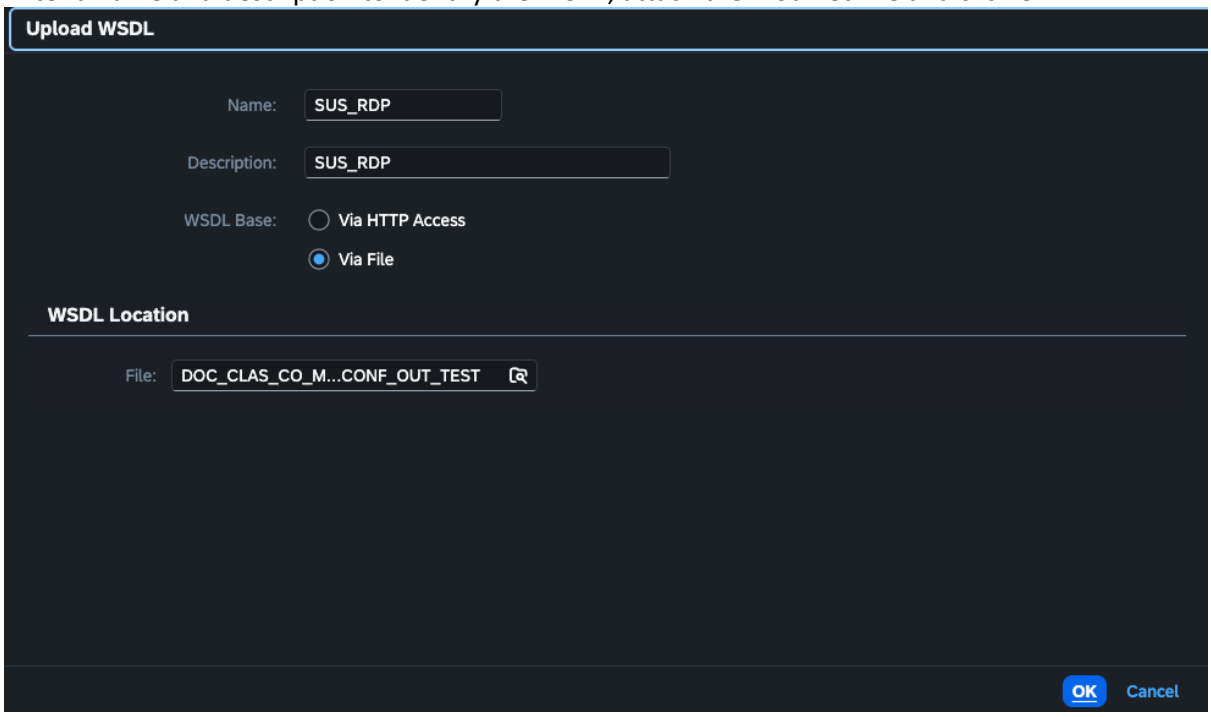
Navigate to SOA Management using transaction SOAMANAGER -> Tools -> WSDL Upload



Then click the Create button.



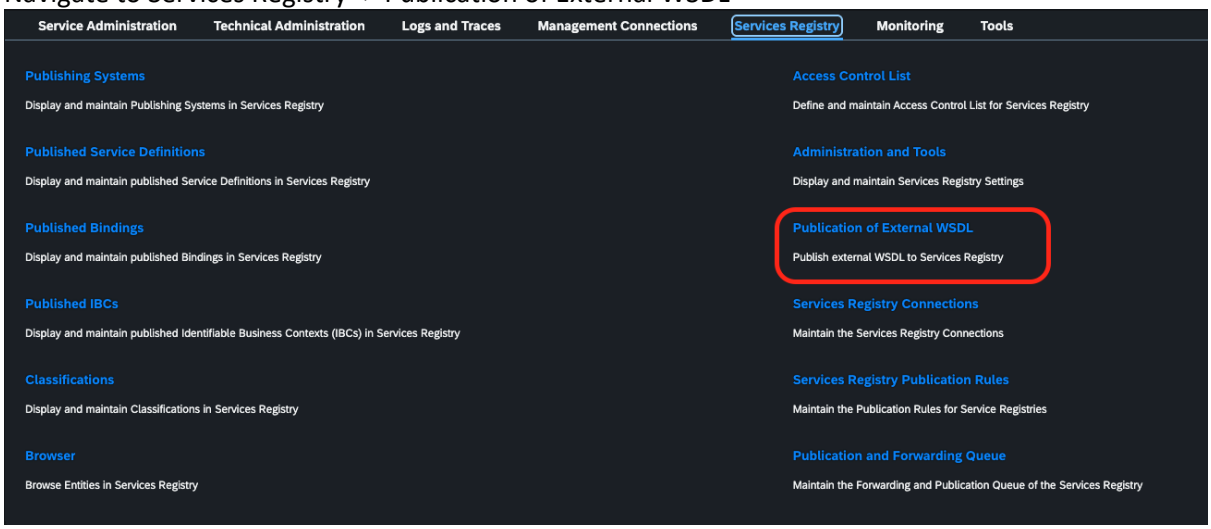
Enter a name and description to identify the WSDL, attach the modified file and click OK.



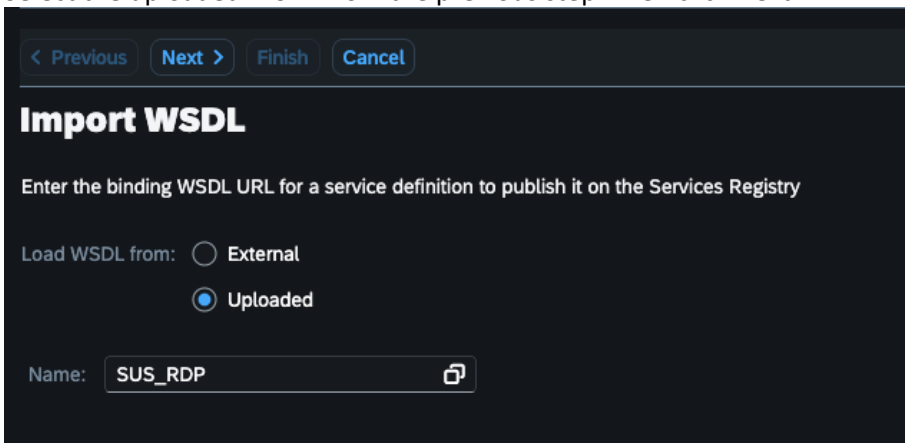
A new file should now be visible in the list.

Publish WSDL

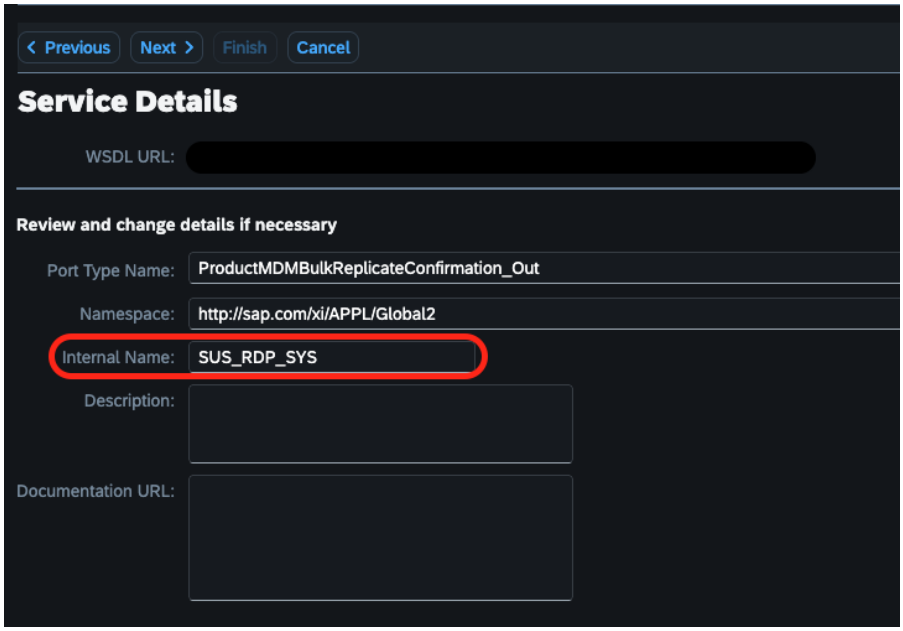
Navigate to Services Registry -> Publication of External WSDL



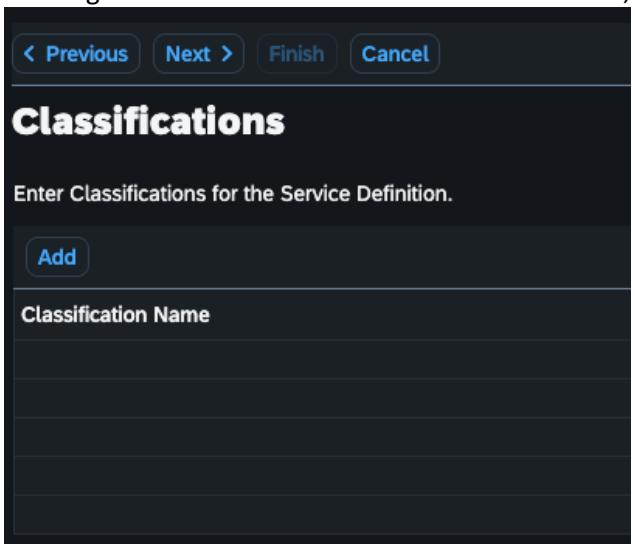
Choose Load WSDL from: Uploaded
Select the uploaded WSDL from the previous step. Then click Next.



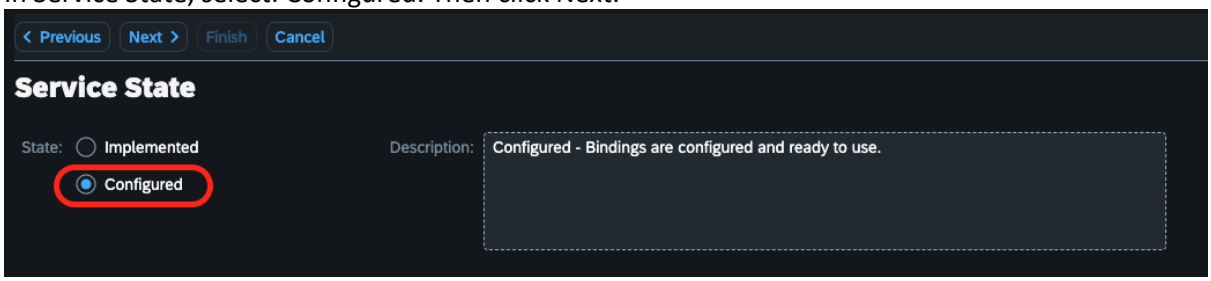
Enter an Internal Name of choice. Then click Next.



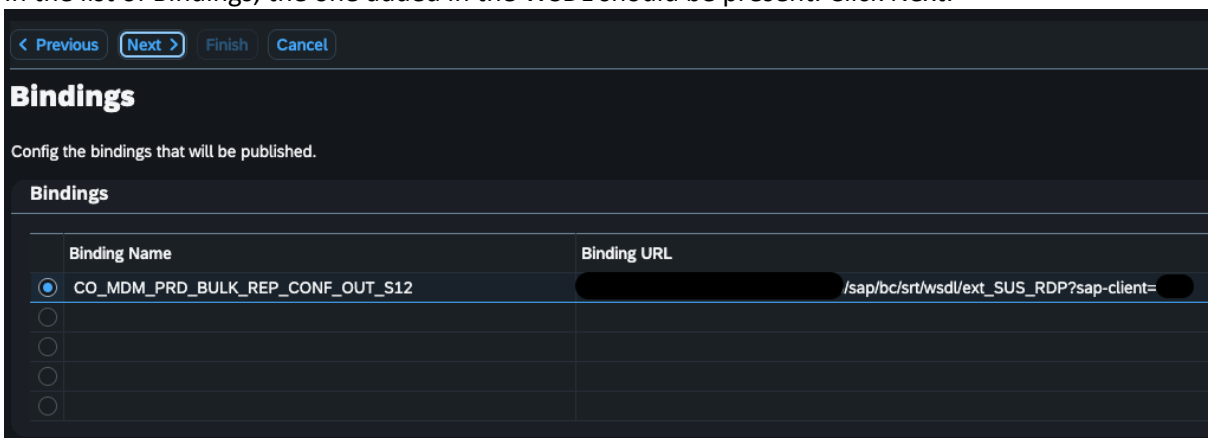
Nothing needs to be added in Classifications section, click Next.



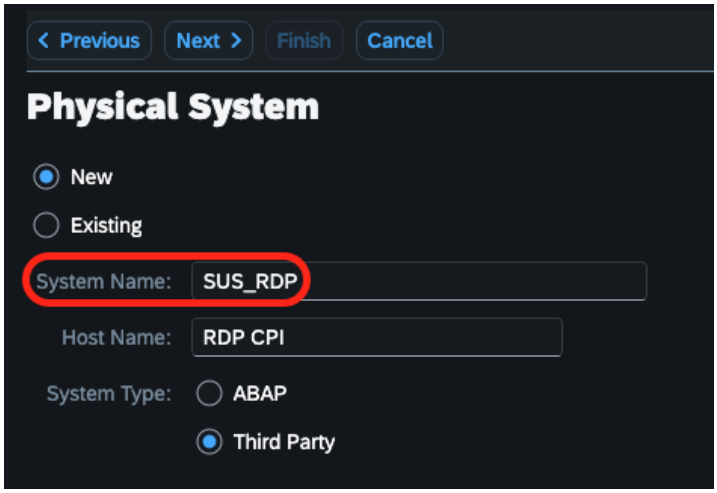
In Service State, select: Configured. Then click Next.



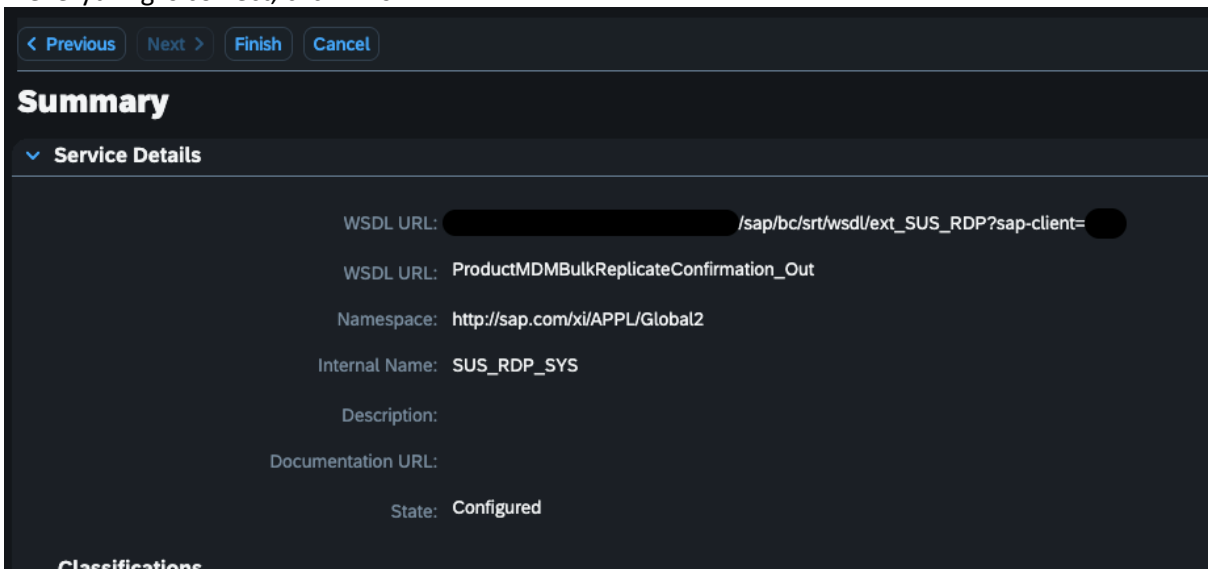
In the list of Bindings, the one added in the WSDL should be present. Click Next.



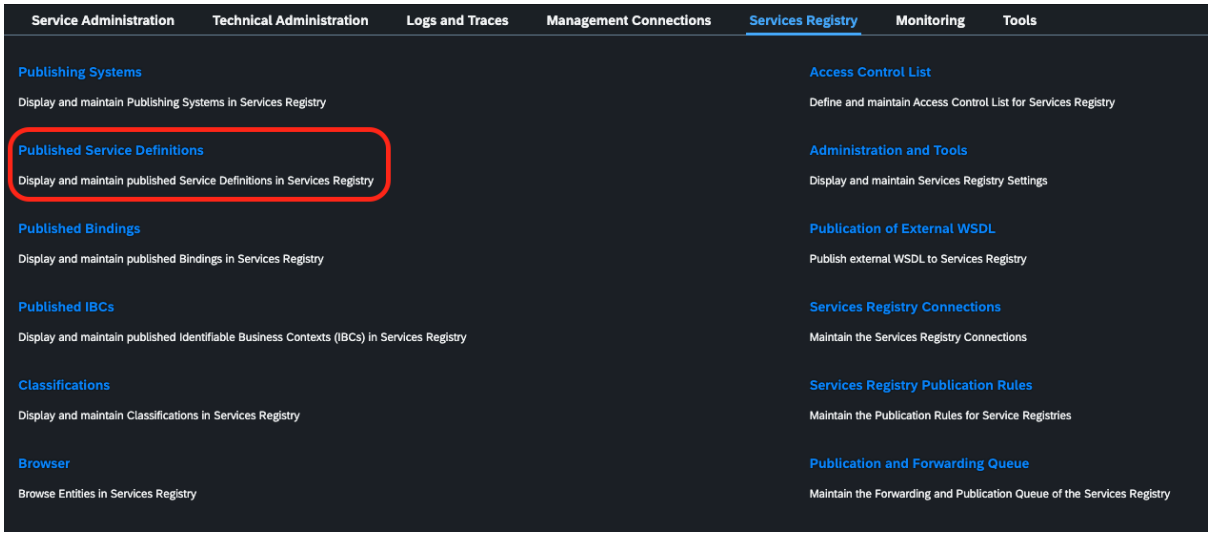
Select New.
System Name - The RDP CPI system ID used in DRF IMG (**This is important**, otherwise the integration will not work.)
Host Name – Any meaningful name
System Type - Third Party.
Then click Next.

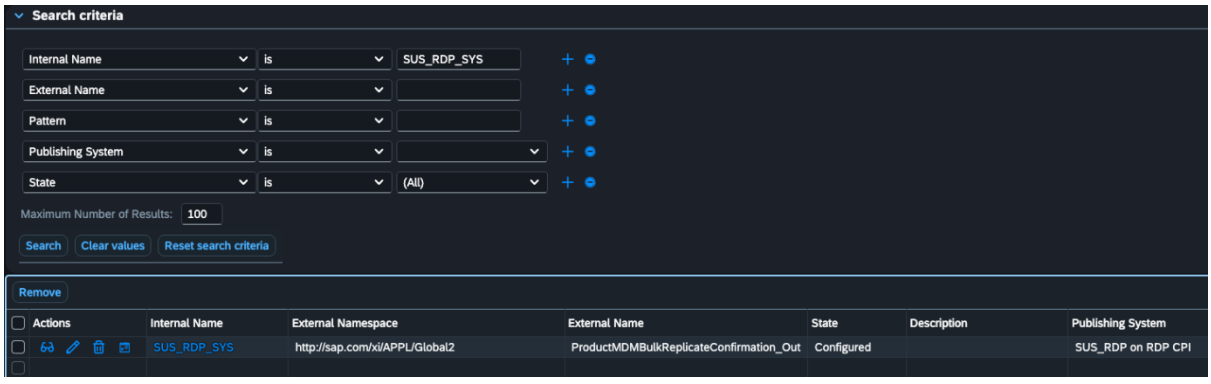


View the Summary and check the configurations again.
If everything is correct, click finish.



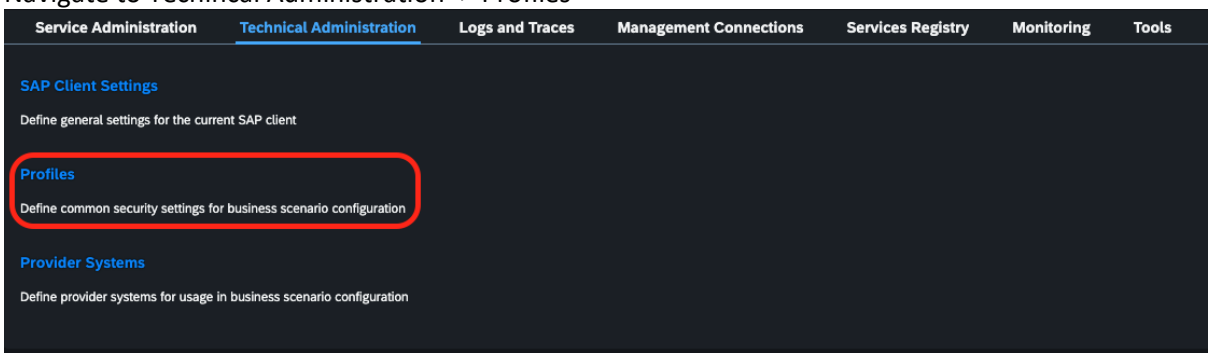
The newly created definition should now be available in Services Registry -> Published Service Definitions



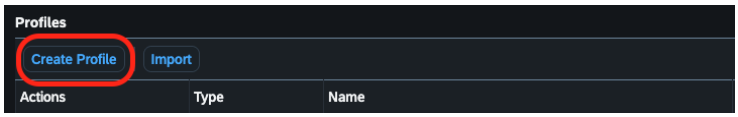


Create Profile

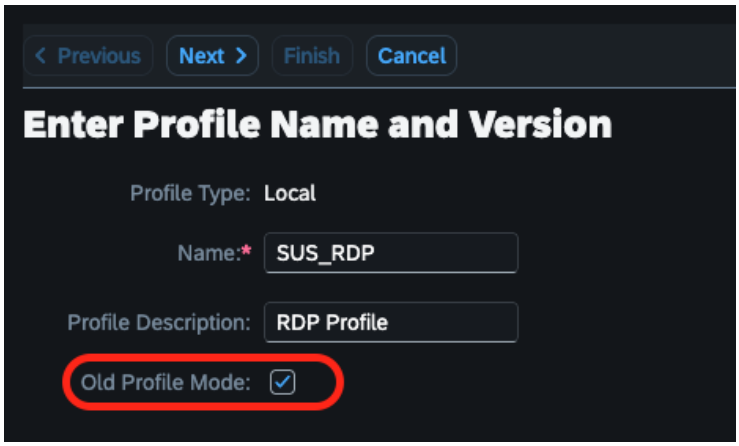
Navigate to Techincal Administration -> Profiles



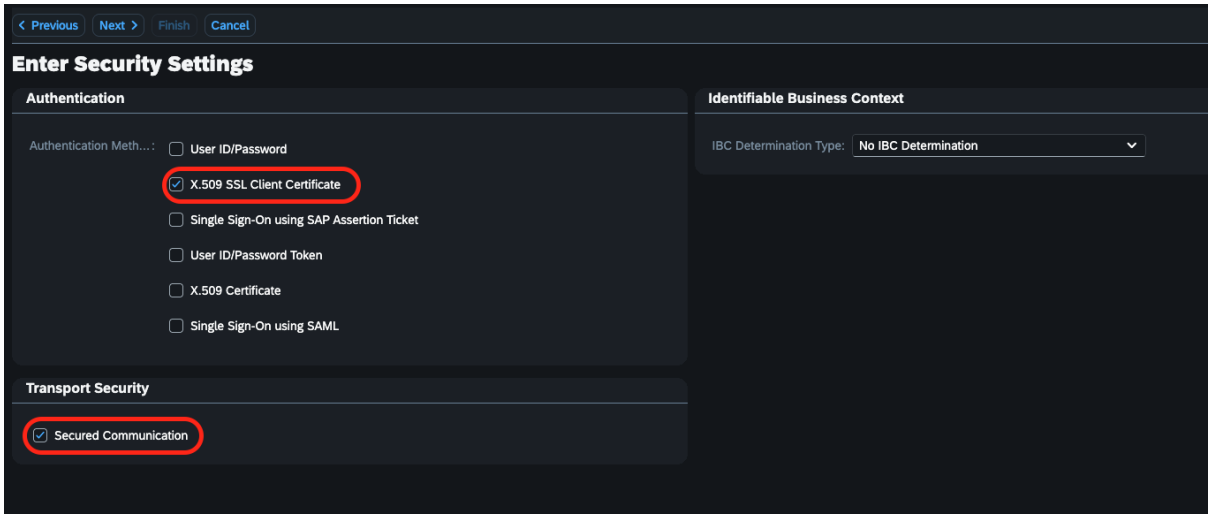
Click Create Profile



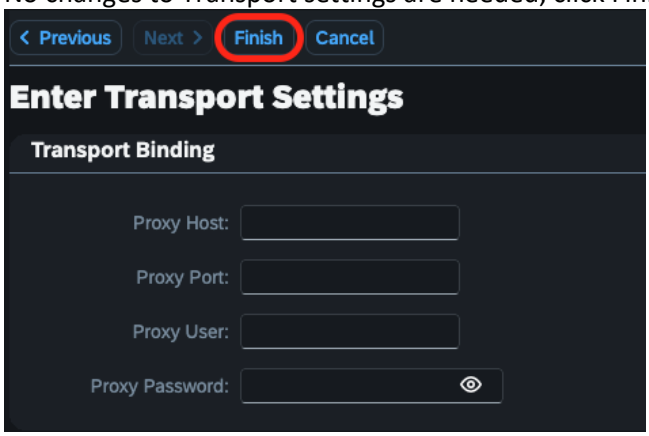
Enter a name and description for the profile and make sure to check “Old Profile Mode”.
Then click Next.



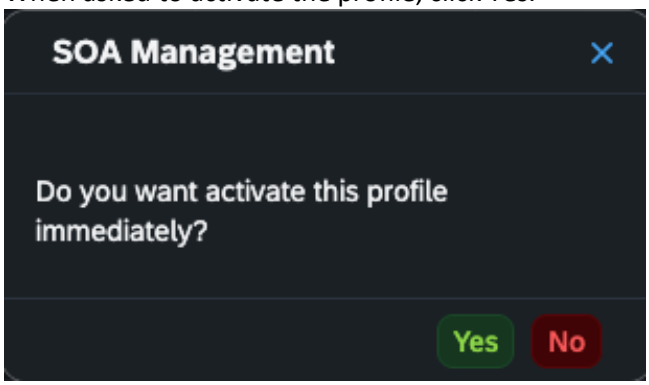
For authentication method, select X.509 SSL Client Certificate.
If CPI is accessible through HTTPS (most likely the case) check Secured Communication.
Then click Next.



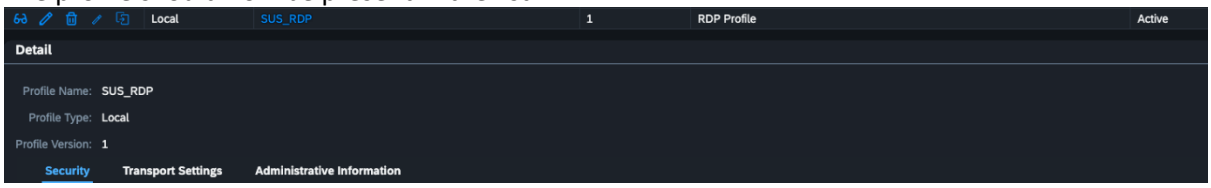
No changes to Transport settings are needed, click Finish.



When asked to activate the profile, click Yes.

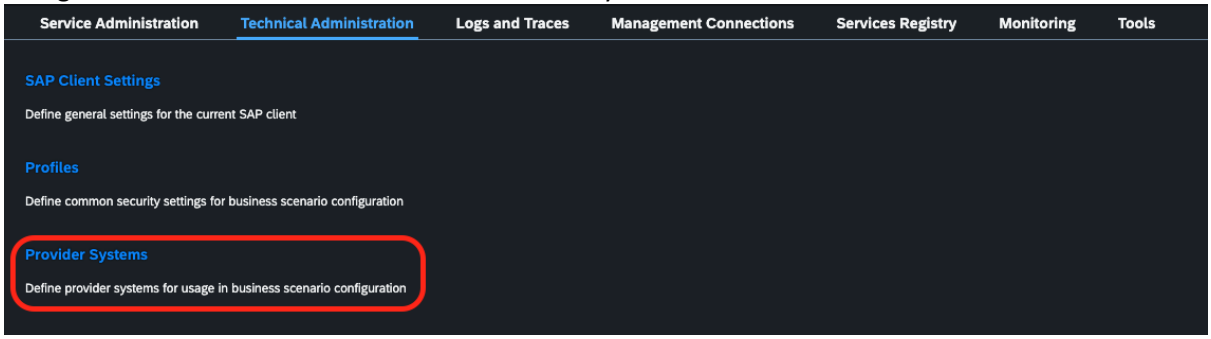


The profile should now be present in the list.

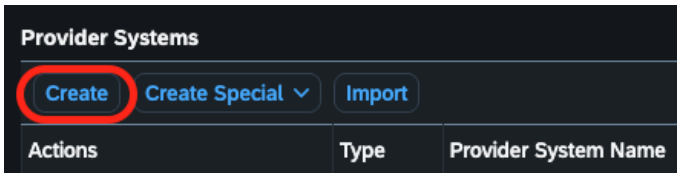


Create Provider System

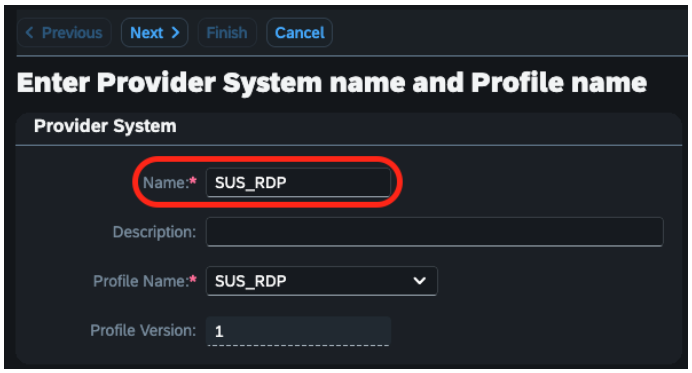
Navigate to Techincal Administration -> Provider Systems



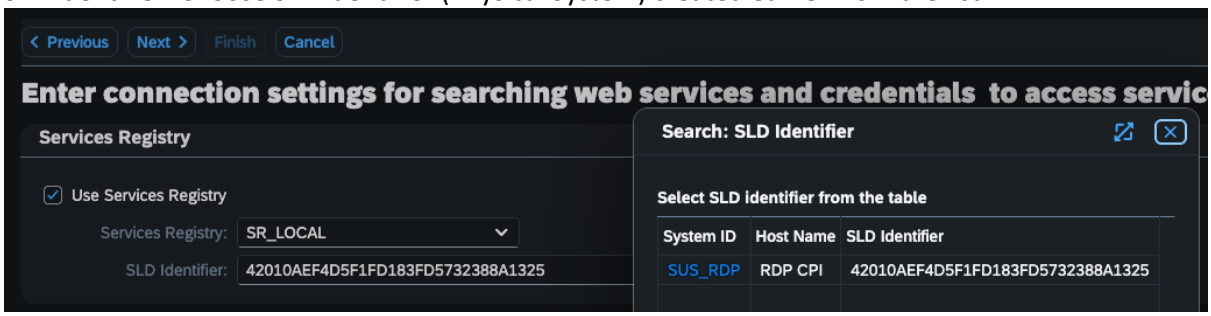
Click Create.



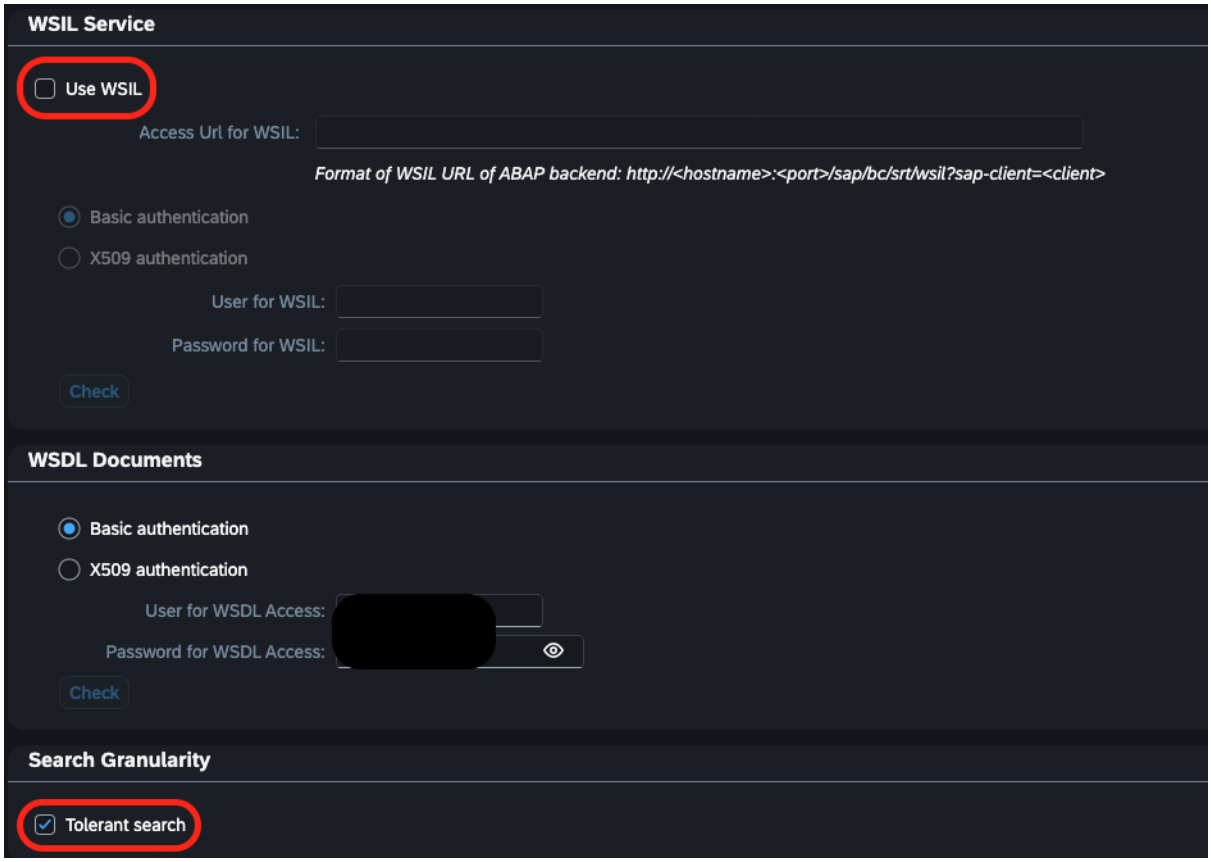
Name: RDP CPI system ID used in DRF IMG (**This is important**, otherwise the integration will not work.)
Description – Any meaningful description
Profile Name – Choose the Profile created earlier from the dropdown menu



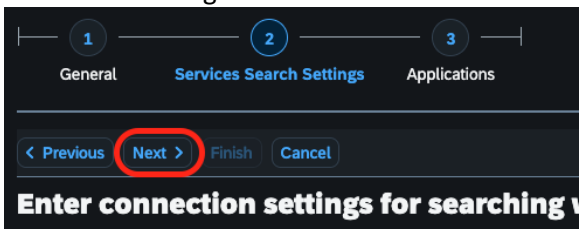
Select “Use Services Registry”
Services Registry: Choose SR_LOCAL from dropdown
SLD Identifier: Choose SLD Identifier (Physical System) created earlier from the list.



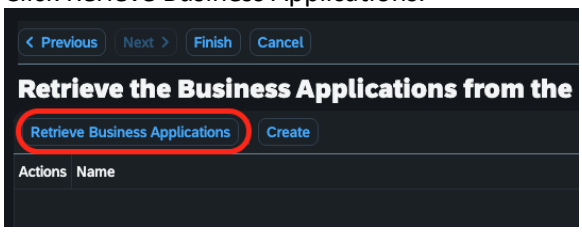
Deselect “Use WSIL”
WSDL Document Access: provide a user who can access the WSDL files and is assigned to role SAP_BC_WEBSERVICE_CONFIGURATOR; in SAP test systems, typically the WSAPPLUSER has sufficient authorizations
Search Granularity: select “Tolerant Search”



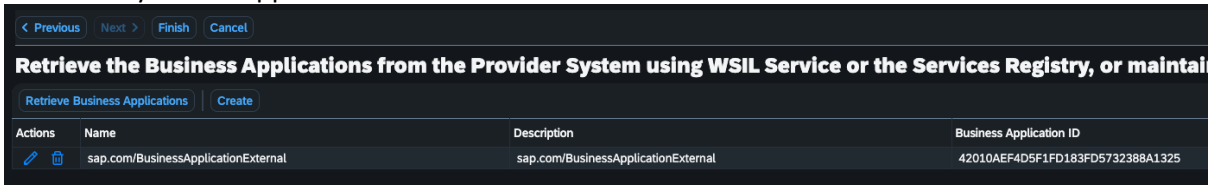
After these configurations click Next.



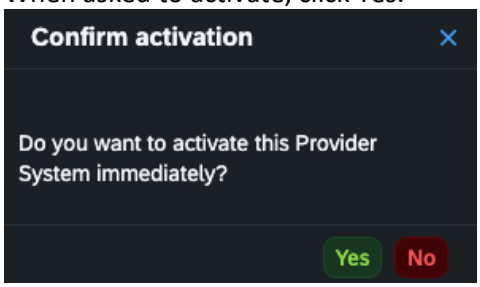
Click Rerieve Business Applications.



A new entry should appear. After this click Finish.



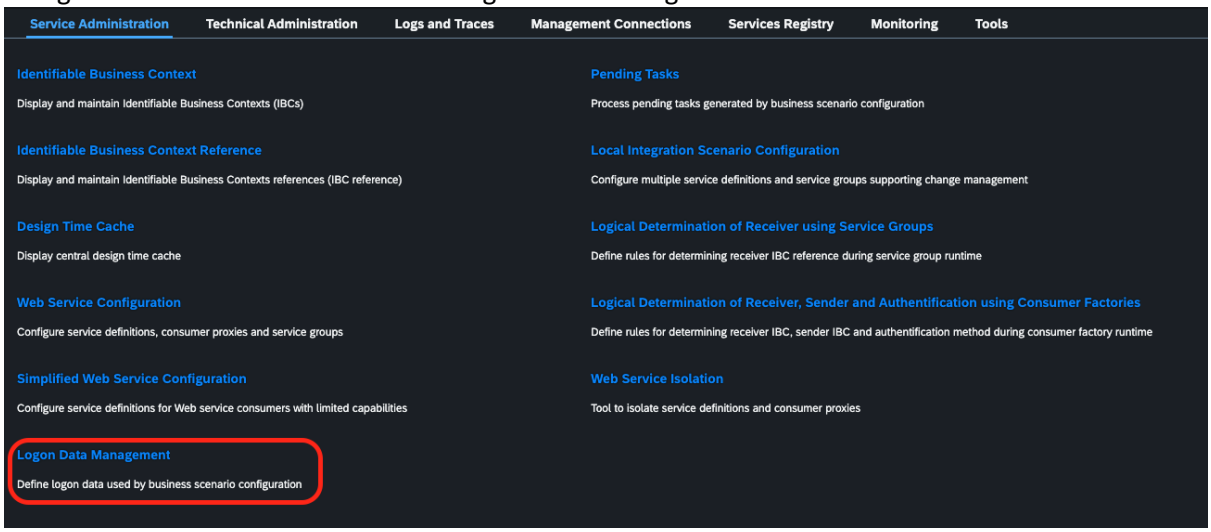
When asked to activate, click Yes.



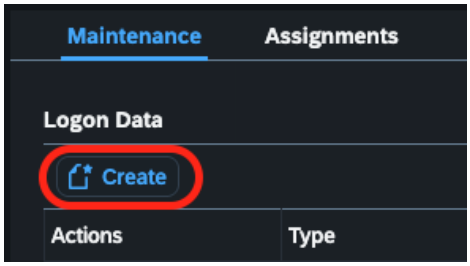
A new Entry should be visible in the Provider System list.

Create Logon Data

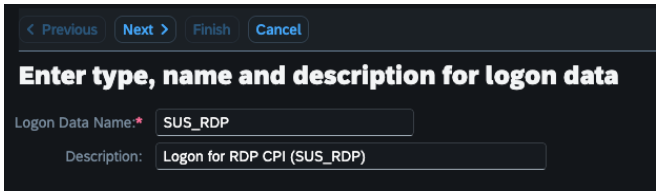
Navigate to Service Administration -> Logon Data Management



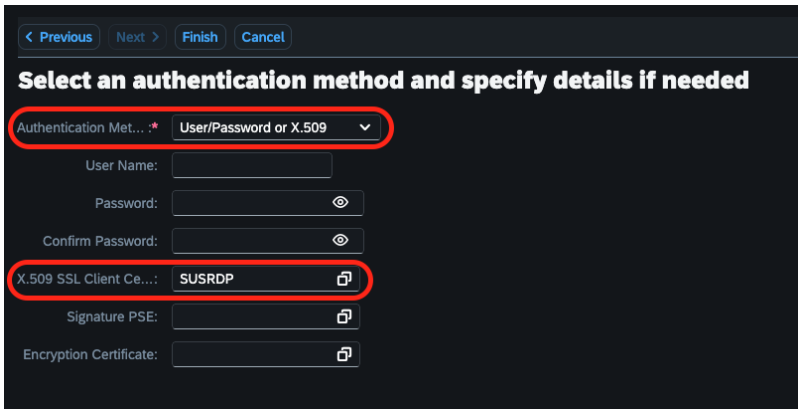
Click on Create.



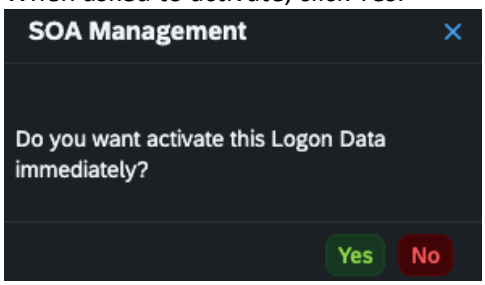
Provide a meaningful Logon Data Name and Description.
Then click Next.



Authentication Method: User/Password or X.509
X.509 SSL Client Certificate: Choose the created one from the dropdown.
Then click Finish.



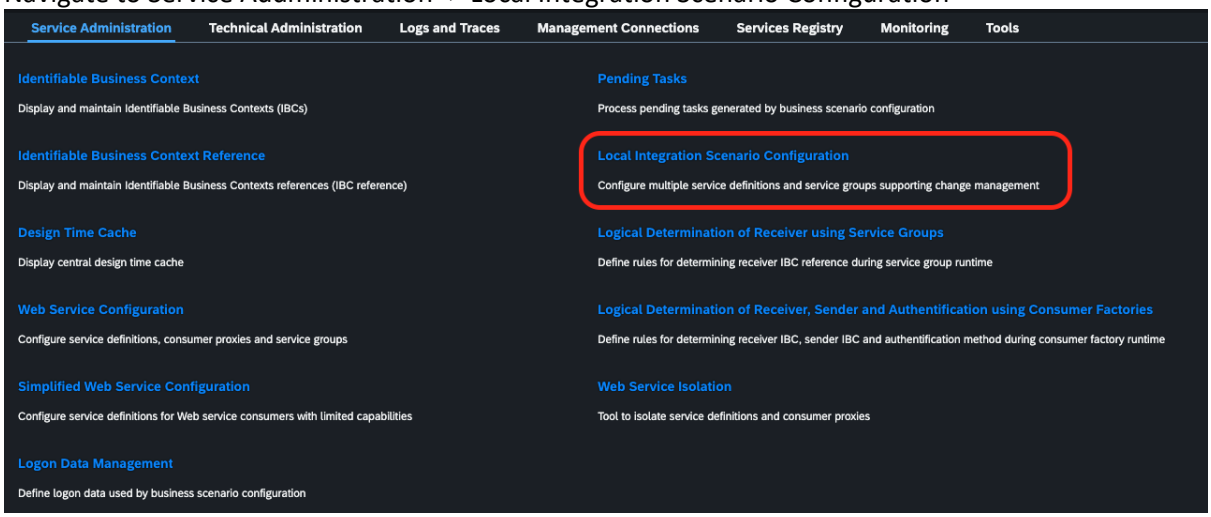
When asked to activate, click Yes.



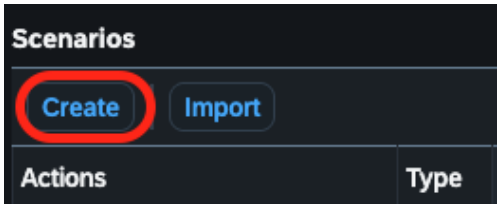
A new entry should appear in the Logon Data list.

Create Local Integration Scenario Configuration

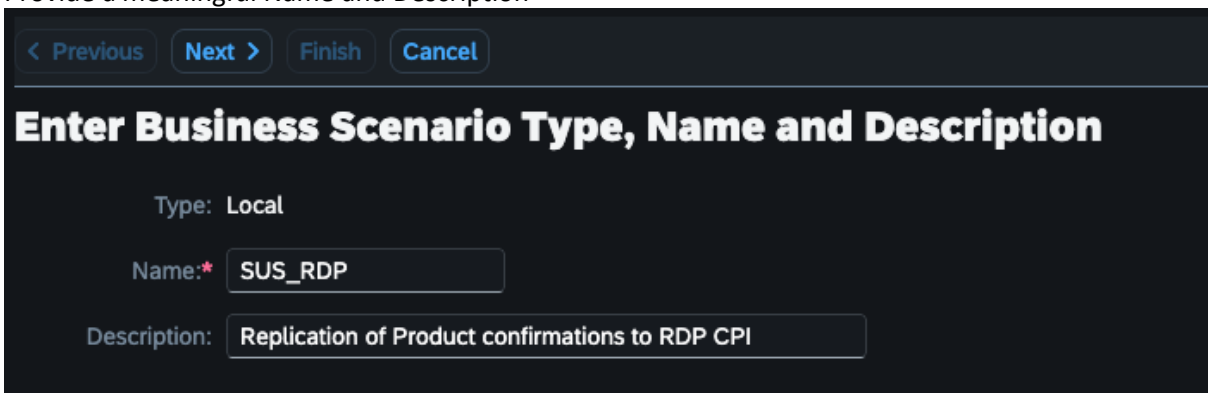
Navigate to Service Addministration -> Local Integration Scenario Configuration



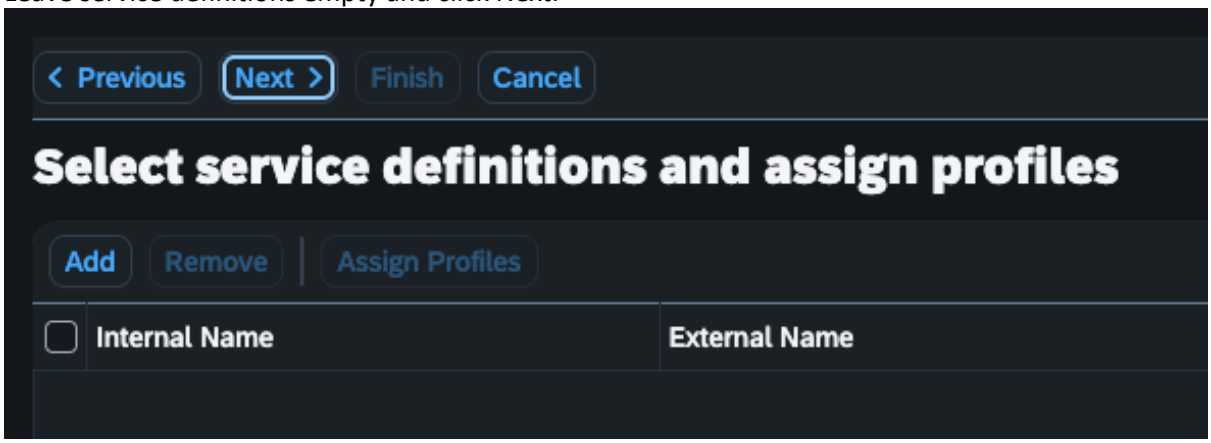
Click Create.



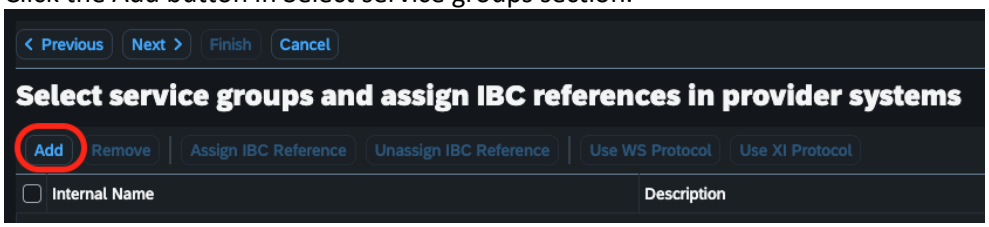
Provide a meaningful Name and Description



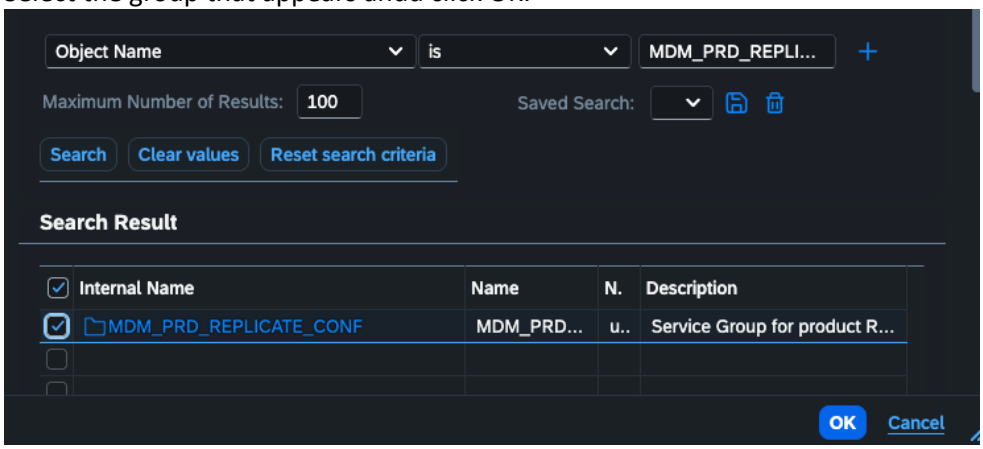
Leave service definitions empty and click Next.



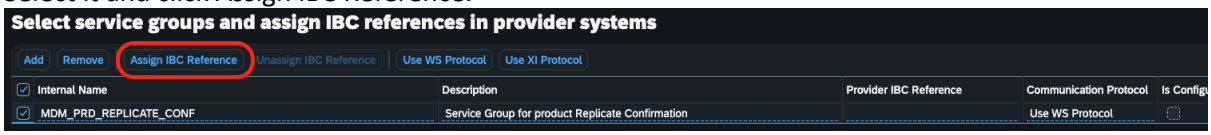
Click the Add button in Select service groups section.



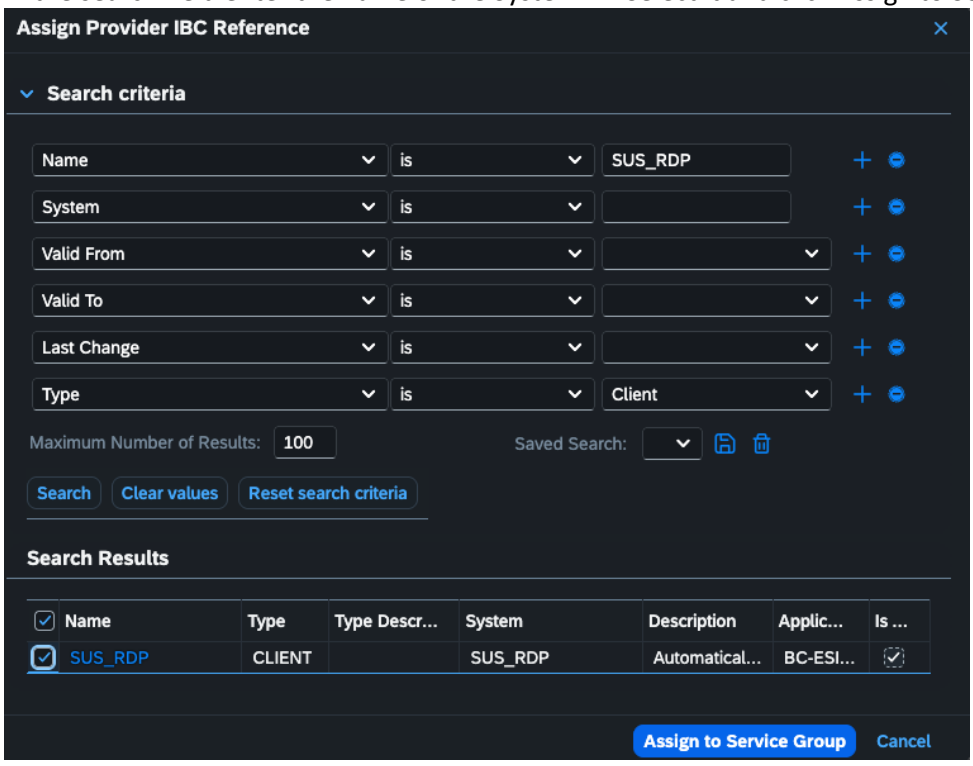
Search for Object Name is **MDM_PRD_REPLICATE_CONF**
Select the group that appears andd click OK.



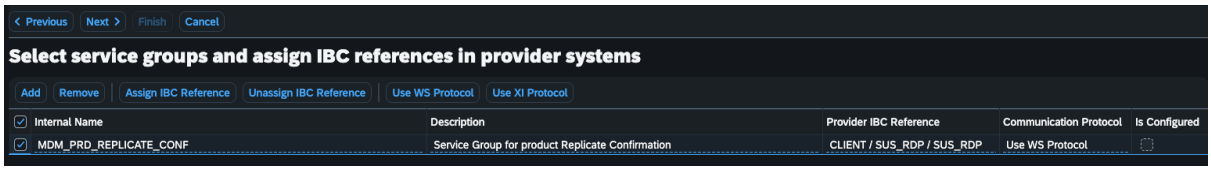
A new entry should appear in the list of service groups.
Select it and click Assign IBC Reference.



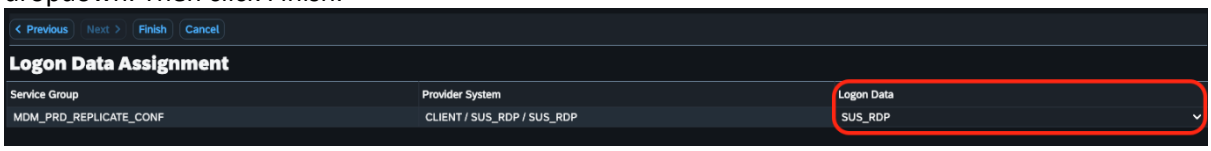
In the search field enter the name of the System ID. Select it and click Assign to Service Group.



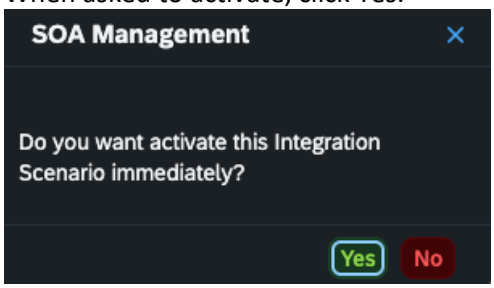
The Provider IBC Reference should now be set. Click Next.



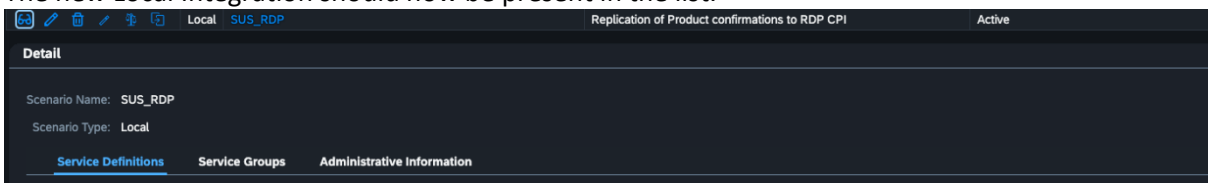
In the Logon Data Assignment, select the Logon Data created from the previous step in the dropdown. Then click Finish.



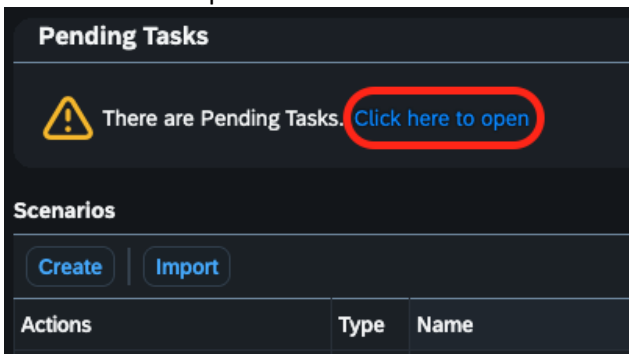
When asked to activate, click Yes.



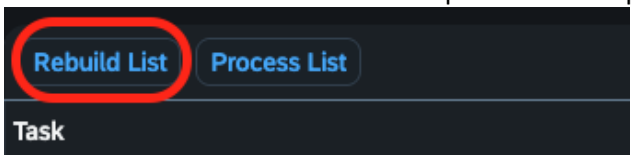
The new Local Integration should now be present in the list.



At the top above the list, there should be a message stating that “There are Pensing Tasks”. Click the link to open.

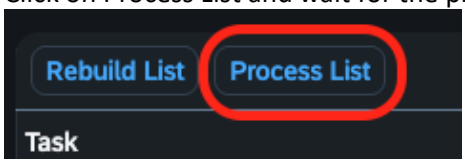


Click on Rebuild List and wait for the process to complete.



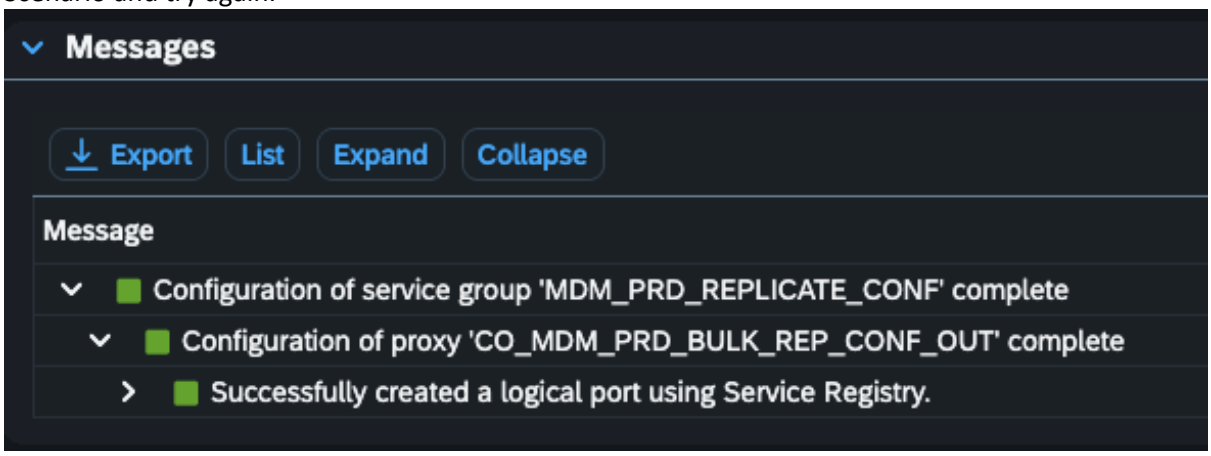
A task similar to this should now be present in the list.

Click on Process List and wait for the process to finish.



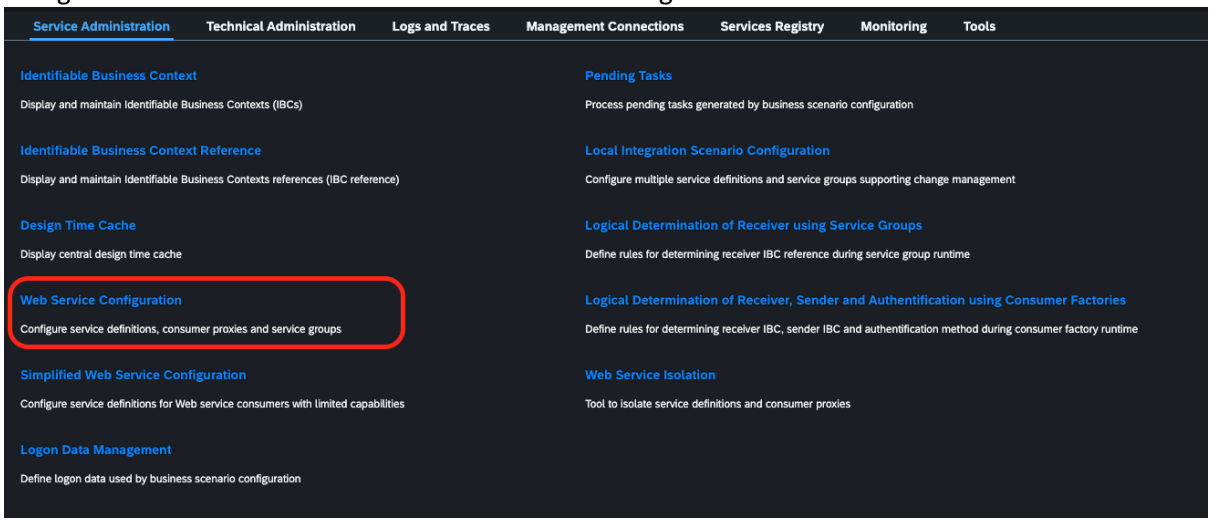
If everything is configured correctly, you should see the following message.
Important: This step MUST succeed so you can proceed!

Troubleshooting: If there are issues, retrace your steps, most likely issue would be with the uploaded WSDL. Correct the issue, reupload the WSDL, recreate the Provider System and Integration Scenario and try again.

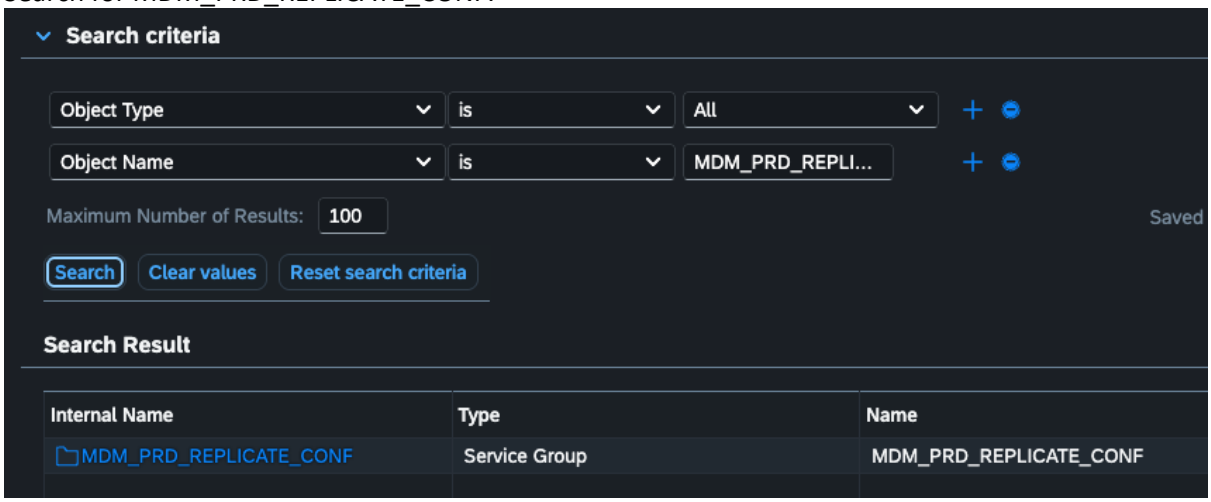


Create Fallback Logical Port

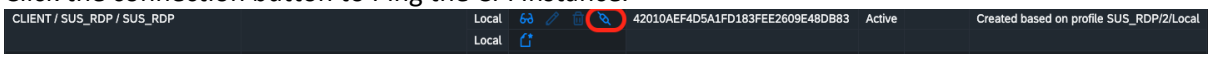
Navigate to Servie Administration -> Web Service Configuration



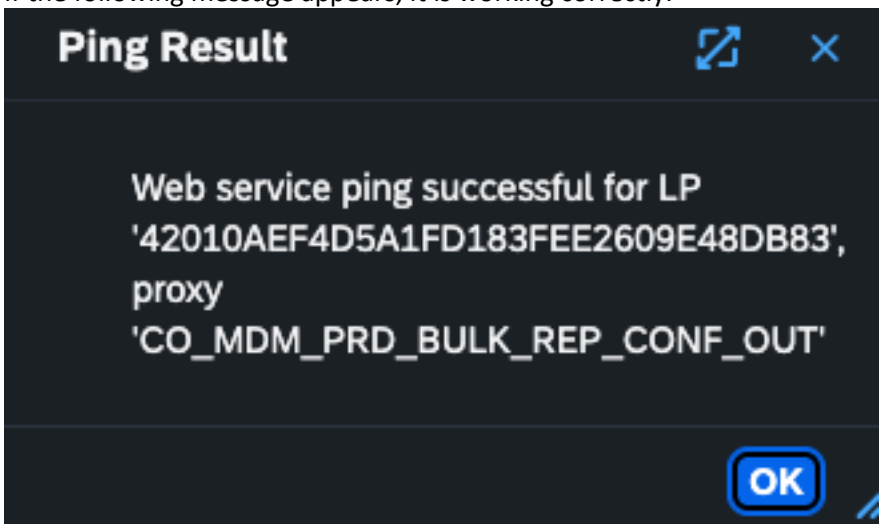
Search for MDM_PRD_REPLICATE_CONF.



The following Port should have been generated.
Click the connection button to Ping the CPI Instance.

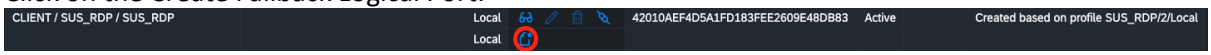


If the following message appears, it is working correctly.

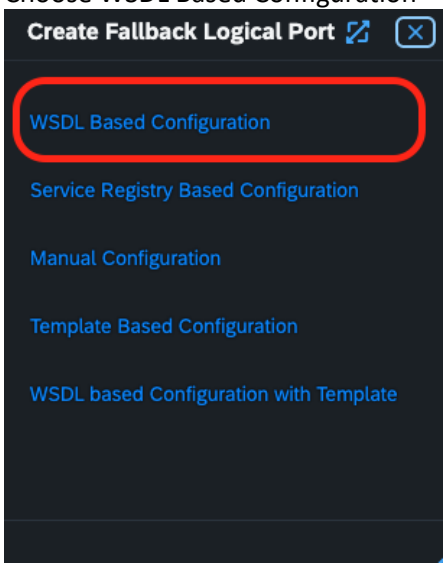


At this point, routing to the Cloud Integration Instance based on the System ID, should happen correctly. However the confirmation will probably be sent in the wrong format and there will be errors in the Integration Flow.

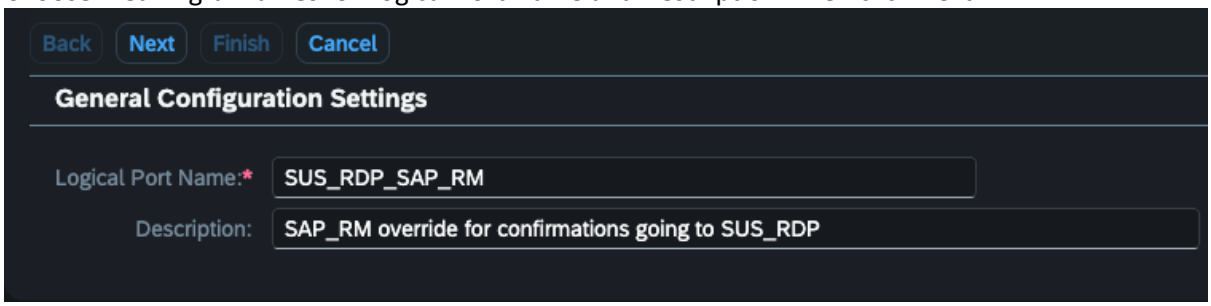
To fix this do the following.
Click on the Create Fallback Logical Port.



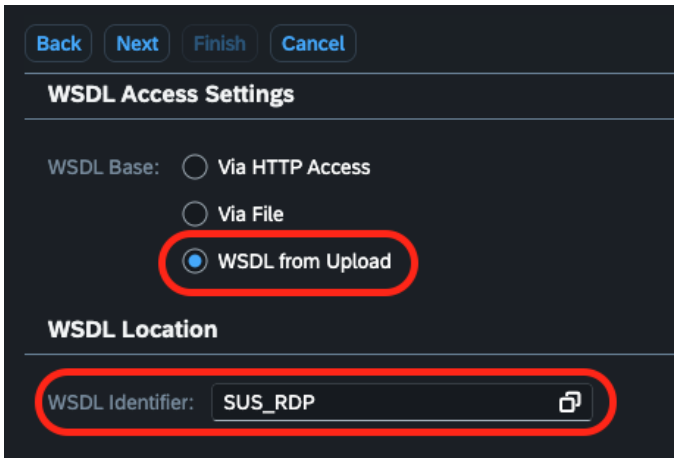
Choose WSDL Based Configuration



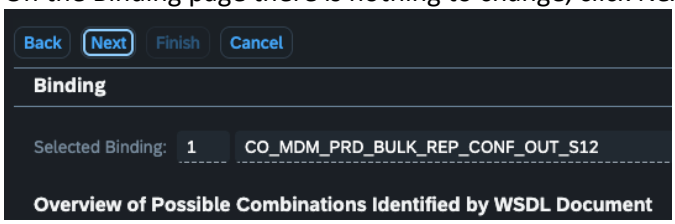
Choose meaningful names for Logical Port Name and Description. Then click Next.



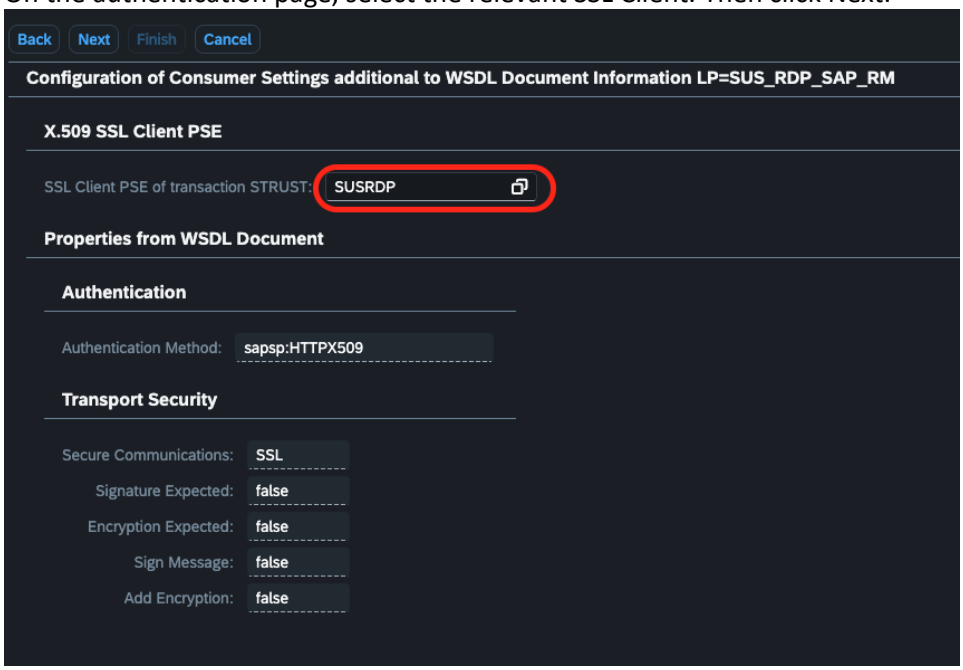
For WSDL Base: Select WSDL from Upload
WSDL Identifier: Identifier of the uploaded WSDL.
Click Next.



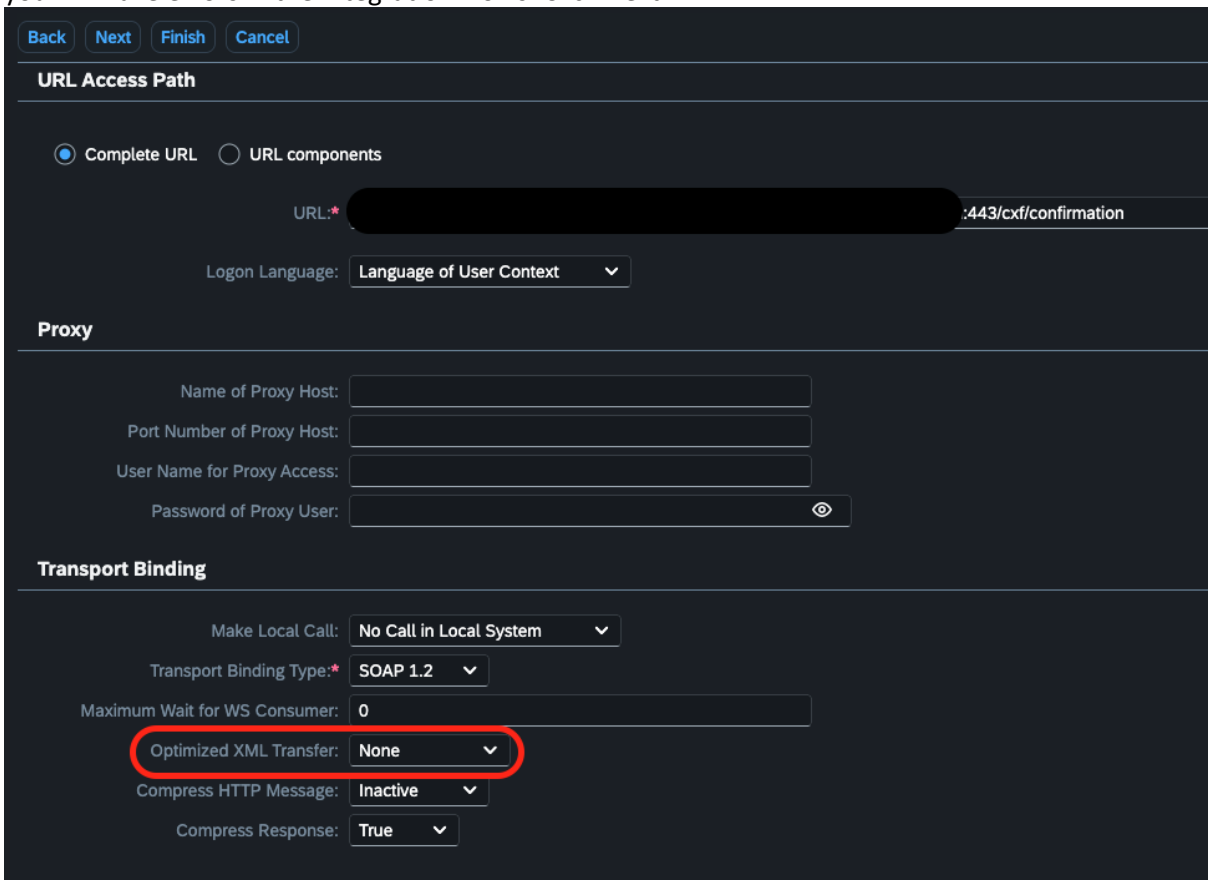
On the Binding page there is nothing to change, click Next.



On the authentication page, select the relevant SSL Client. Then click Next.

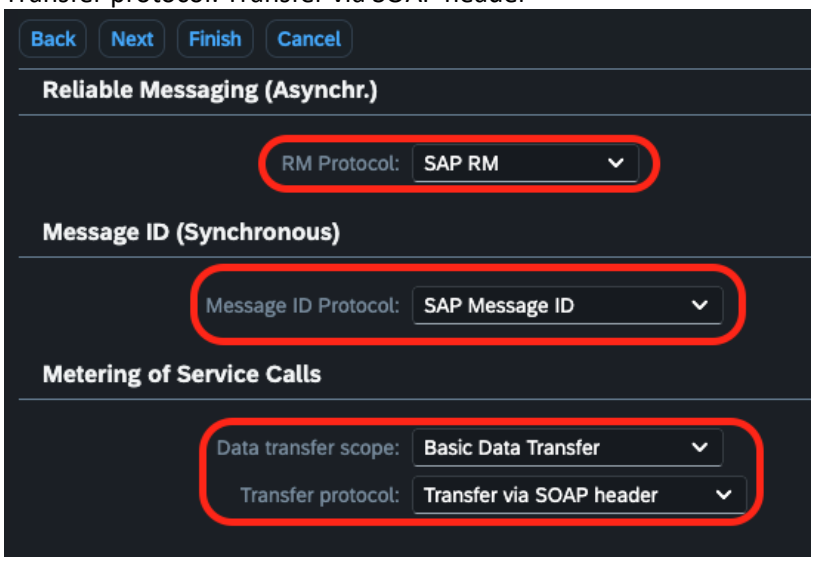


Important: In the HTTP Settings page make sure to set Optimized XML Transfer to None, otherwise you will have errors in the Integration Flows. Click Next.

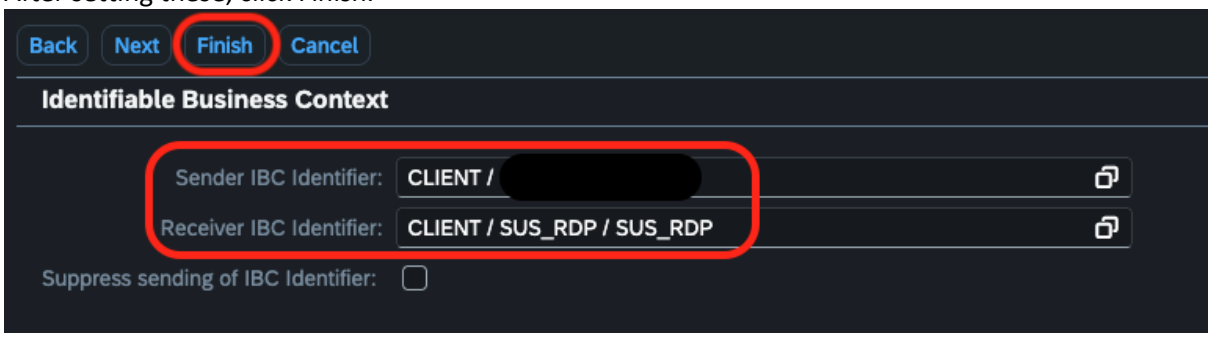


In the SOAP Protocol page, make sure to set:
RM Protocol: SAP RM
Message ID Protocol: SAP Message ID
Data transfer scope: Basic Data Transfer

Transfer protocol: Transfer via SOAP header

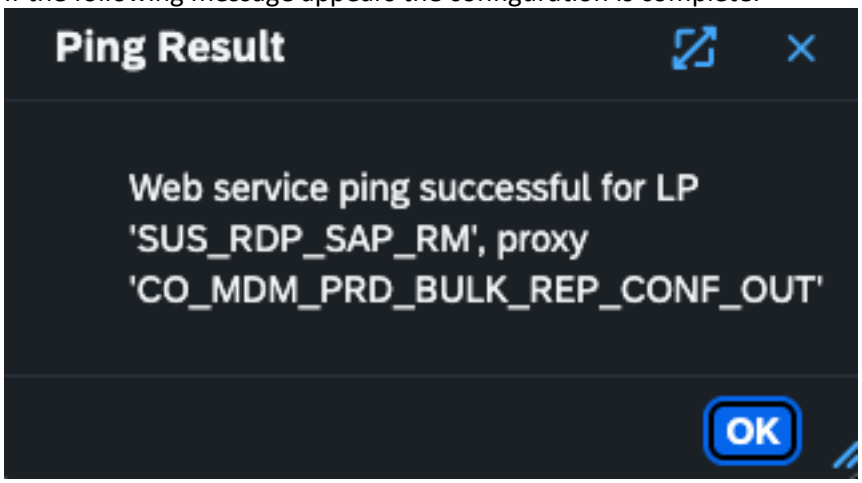


For Identifiable Business Context:
Sender IBC Identifier: The S/4 system IBC
Receiver IBC Identifier: System ID pointing to the CPI Instance
After setting these, click Finish.



The result should look similar to this.
Press the connection icon on the second entry to ensure the system is still accessible.

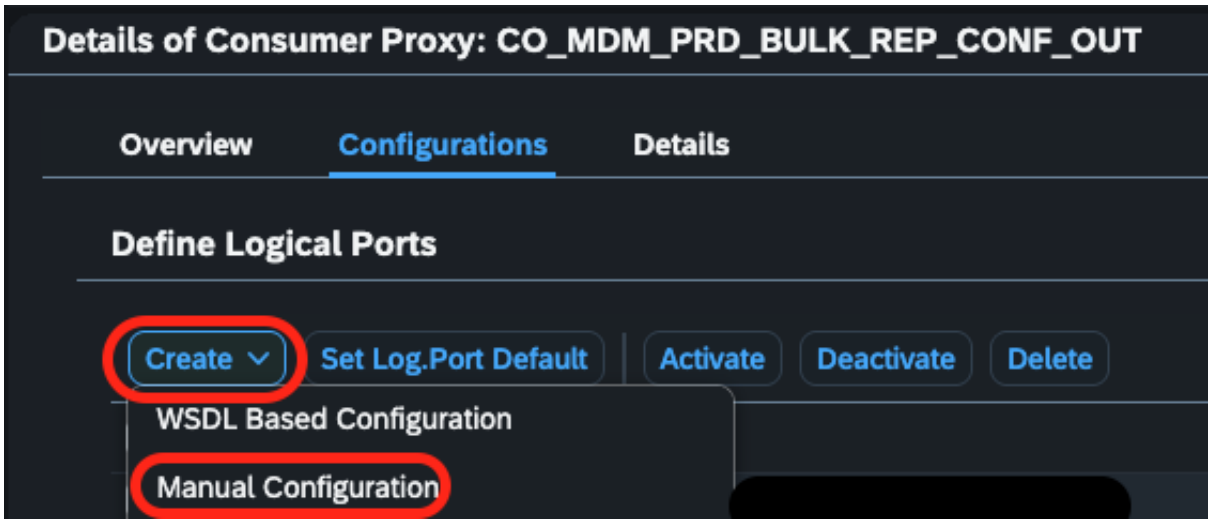
If the following message appears the configuration is complete.



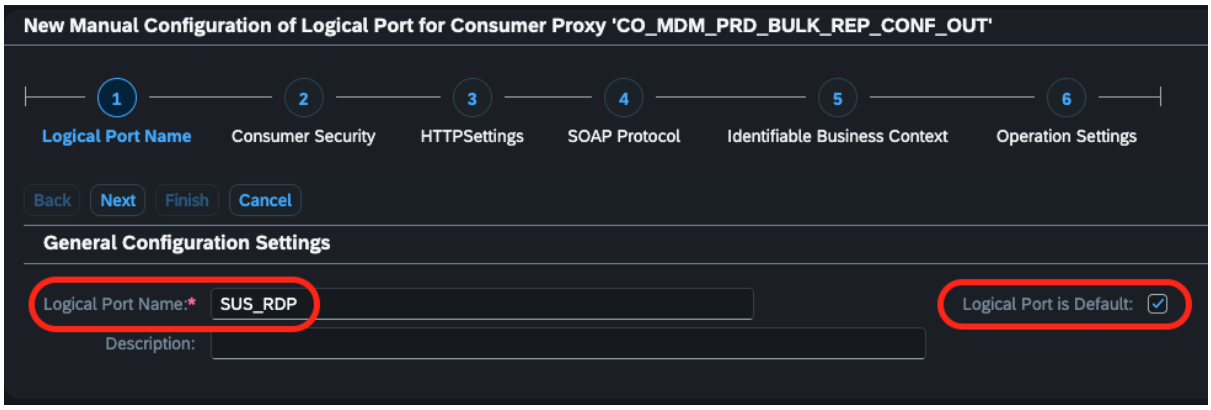
Outbound Confirmation with Default Logical Port (NOT Recommended)

This approach involves fewer steps in order to configure, however it has drawbacks which are described in the following SAP Note: https://me.sap.com/notes/0003237511

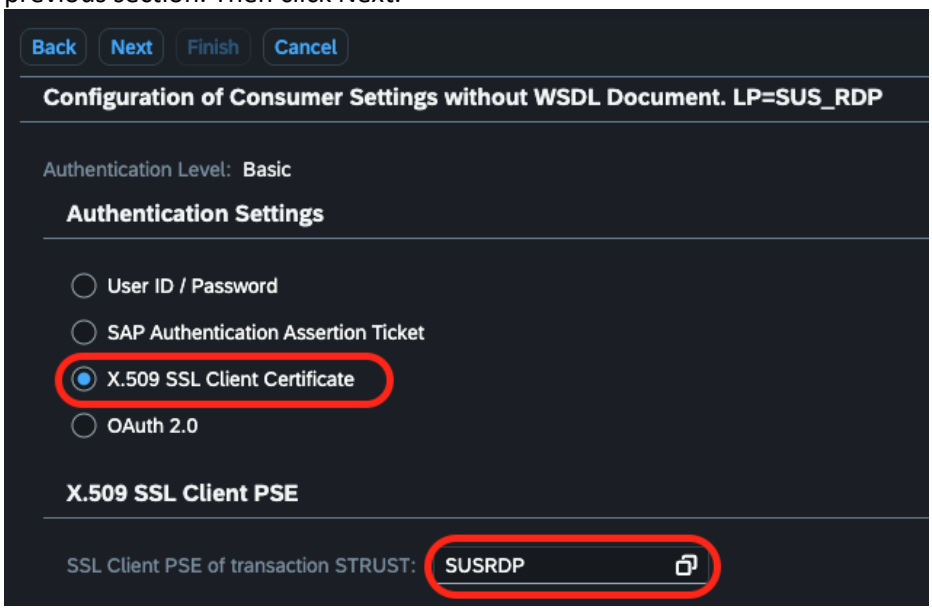
In the S/4 system, navigate to SOA Management using transaction SOAMANAGER.
Go to Service Administration -> Web Service Configuration -> Object Name is ProductMDMBulkReplicateConfirmation_Out
Select CO_MDM_PRD_BULK_REP_CONF_OUT.
Click Create -> Manual Configuration.



Enter a name of choice for the Logical Port and make sure to enable “Logical Port is Default”.
Then click Next.



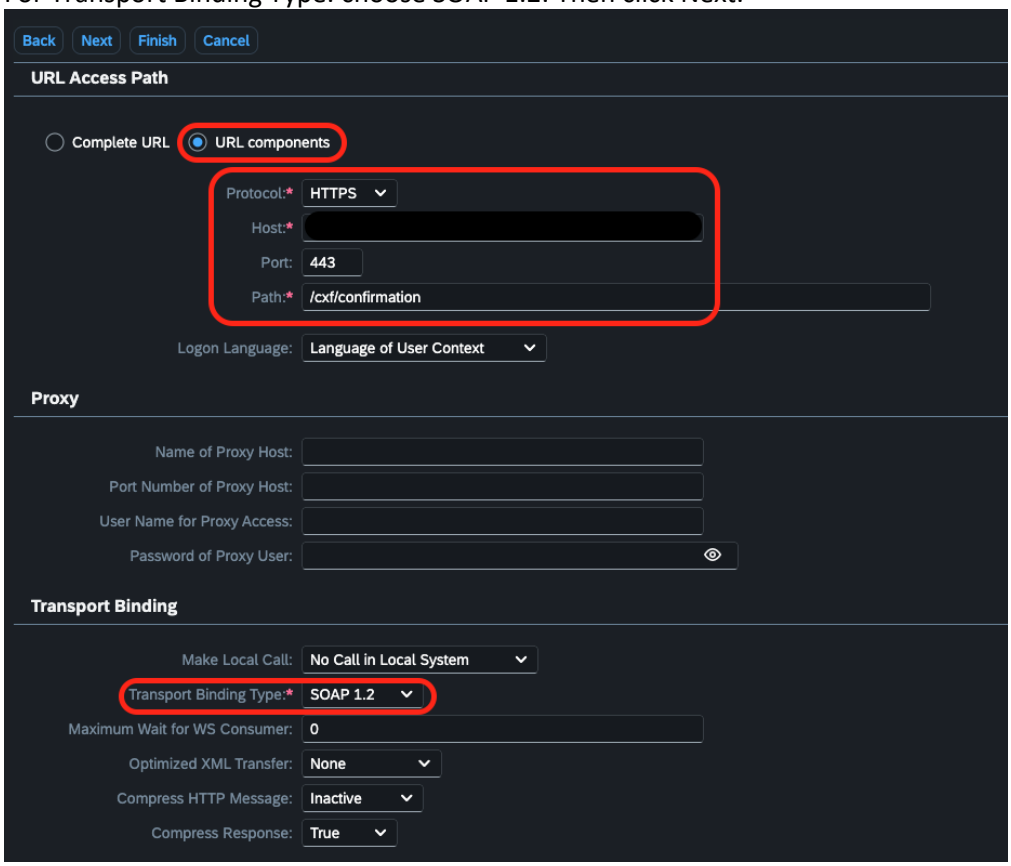
For authentication, choose X.509 SSL Client Certificate and select the SSL Client PSE created in the previous section. Then click Next.



Select URL components, then enter:

- Protocol: HTTPS
- Host: <Host of the CPI Instance>
- Port: 443
- Path: <Path to integration flow Receive SOAP Confirmation and Start Follow-Up Processing>

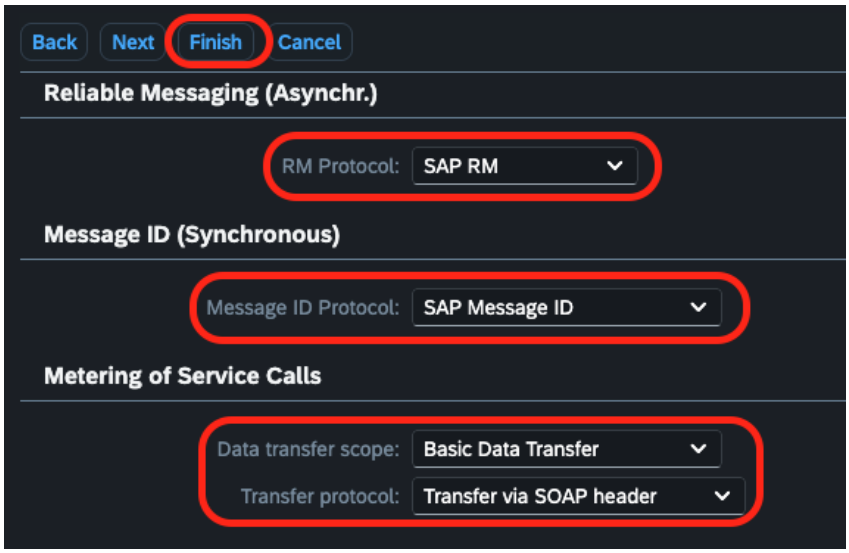
For Transport Binding Type: choose SOAP 1.2. Then click Next.



For SOAP Protocol, set the following:

- RM Protocol: SAP RM
- Message ID Protocol: SAP Message ID
- Data transfer scope: Basic Data Transfer
- Transfer protocol: Transfer via SOAP Header

Then click Finish.



After creation, the following entry should appear.
The state should be Active and the “Logical Port is Default” should be set as true.
Click on the connection icon to verify that the SOAP connection to “Receive SOAP Confirmation and Start Follow-Up Processing” integration flow in Cloud Integration is accessible.

If everything is configured correctly the following message should appear and the configuration is complete.