

# Replication of Material Classifications Configuration Guide

SAP Responsible Design and Production Integration with SAP ERP

## Table of Contents

PREREQUISITES .....	3
OBTAIN CLIENT CERTIFICATE FOR AUTHENTICATION WITH INTEGRATION FLOWS .....	3
CONFIGURATION AND DEPLOYMENT OF SOAP CONFIRMATION FLOW IN CLOUD INTEGRATION .....	3
S/4HANA PUBLIC CLOUD .....	5
AUTHENTICATION .....	5
COMMUNICATION SYSTEM .....	5
COMMUNICATION ARRANGEMENT .....	6
S/4HANA PRIVATE CLOUD / ON-PREMISE .....	9
AUTHENTICATION .....	9
INBOUND PRODUCT REQUEST .....	13
OUTBOUND PRODUCT CONFIRMATION .....	14
<i>Outbound Confirmation without Default Logical Port (Recommended)</i> .....	15
Upload an external WSDL .....	16
Publish WSDL .....	21
Create Profile .....	25
Create Provider System .....	26
Create Logon Data .....	29
Create Local Integration Scenario Configuration .....	31
Create Fallback Logical Port .....	34
<i>Outbound Confirmation with Default Logical Port (NOT Recommended)</i> .....	39

# 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

Configure "Receive SOAP Confirmation and Start Follow-Up Processing"

Sender Receiver

Connection

Sender: Sender

Adapter Type: SOAP

Address: \*\*anonymized\*\*

User Role: ESBMessaging\_send Select

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

Configure "Receive SOAP Confirmation and Start Follow-Up Processing"

Sender Receiver

Connection

Receiver: Process\_Flow

Adapter Type: ProcessDirect

Address: \*\*anonymized\*\*

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.*

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

Maintain Client Certificates Maintain Certificate Trust List

Search  Certificate:  Description:  Managed By:  Issued To:  Issued By:  Valid To:

Status:  Changed On:  Changed By:

Adapt Filters

masterTitleCount 🔄 🔄 🗑️

Upload Certificate

Upload Certificate

Certificate: \*

Description:

Password: \*

## Communication System

Note down the generated name for the certificate

Certificate	Description	Managed By	Issued To	Issued By	Valid To
<input type="text"/>		Customer	<input type="text"/>	SAP Cloud Platform Client CA	02/21/2027

Navigate to App: Communication System and click New:

Standard  Own SAP Cloud System

Search  Editing Status:  System ID:  System Name:  Host Name:

Adapt Filters (1)

Communication Systems   Delete

The system name does not matter, in this example it is named: SUS\_RDP\_SYS

## New Communication System

System ID: \*

System Name: \*



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

Technical Data

General

Host Name: \*

Logical System:

Port:

Is Hub System:

Inbound Only:

UI Host Name:

Business System:

Cipher Suites: (Default)

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.

Users for Inbound Communication

Authentication Method	User Name/Client ID
User ID and Password	<input type="text"/>

Users for Outbound Communication

Authentication Method	User Name/Certificate/Client ID	Status
SSL Client Certificate	<input type="text"/>	✓

Click save:



## Communication Arrangement

Navigate to Application: Communication Arrangements and click New

Standard

Search  Editing Status:  Arrangement Name:  Scenario ID:  Communication System:

Communication Arrangements

For Scenario, select SAP\_COM\_0009, Arrange Name can be anything, in this example it is named: SUS\_RDP\_0009  
Click Create

### New Communication Arrangement

Scenario: \*

SAP\_COM\_0009

Arrangement Name:

SUS\_RDP\_0009

Create Cancel

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.

SUS\_RDP\_0009

Scenario ID: SAP\_COM\_0009 Editing Status: Draft  
Scenario: Product Integration

Common Data

Arrangement Name: SUS\_RDP\_0009 Own SAP Cloud System: [Redacted]

Communication System: \* SUS\_RDP\_SYS API-URL: [Redacted]

Additional Properties

Property Name	Property Value
Product Number Harmonization	

Inbound Communication Supported Authentication Methods

User Name: \* [Redacted] Authentication Method: User ID and Password

Outbound Communication Download Supported Authentication Methods

Certificate: \* [Redacted] Authentication Method: SSL Client Certificate

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

Replicate Product from S/4 System to Client

Service Status:  Active

Application Protocol: IDOC Interface

Port: 443

✓ **Product Master - Replicate from SAP S/4HANA Cloud to Client**

Service Status:  Active

Application Protocol: SOAP

Port:

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.

✓ **Product Master - Confirmation from SAP S/4HANA Cloud to Client**

Service Status:  Active

Application Protocol: SOAP

Port:

Path:

Service URL:

Use WSRM:

Click save:



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

✓ **Product Master - Confirmation from SAP S/4HANA Cloud to Client**

Download WSDL/Service Metadata  Check Connection

Service Status:  Active

Application Protocol: SOAP

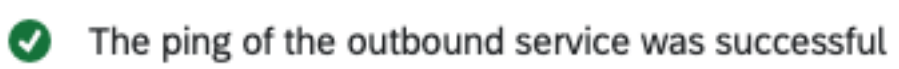
Port:

Path:

Service URL:

Use WSRM:

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



# S/4HANA Private Cloud / On-Premise

## Authentication

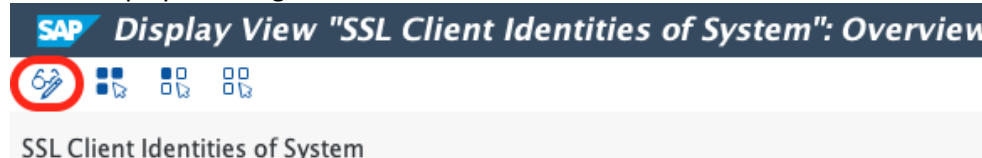
Enter transaction: STRUST



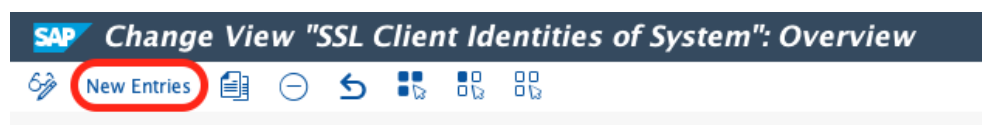
Select Environment -> SSL Client Identities of System



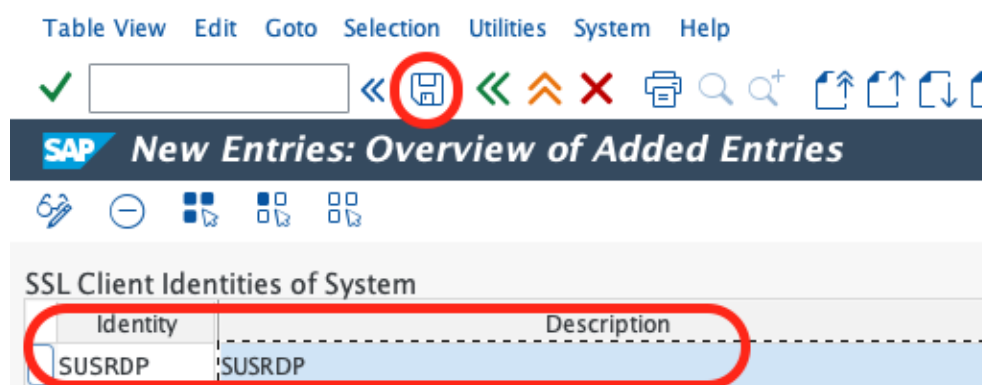
Select Display -> Change



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:

## ✗ SSL client SUSRDP

Select Display -> Change.

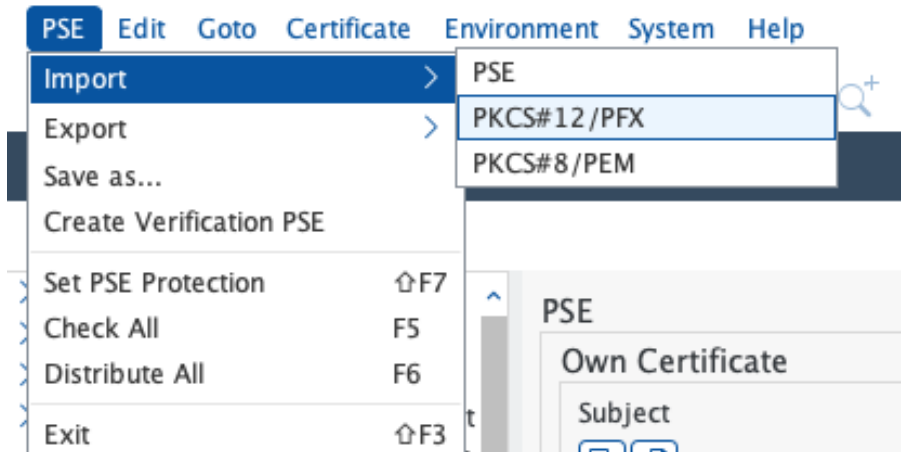
If you are missing permissions.

Access your user using transaction SU01 and make sure your user has the following role:

SAP\_BC\_SEC\_AUTH\_ADMIN

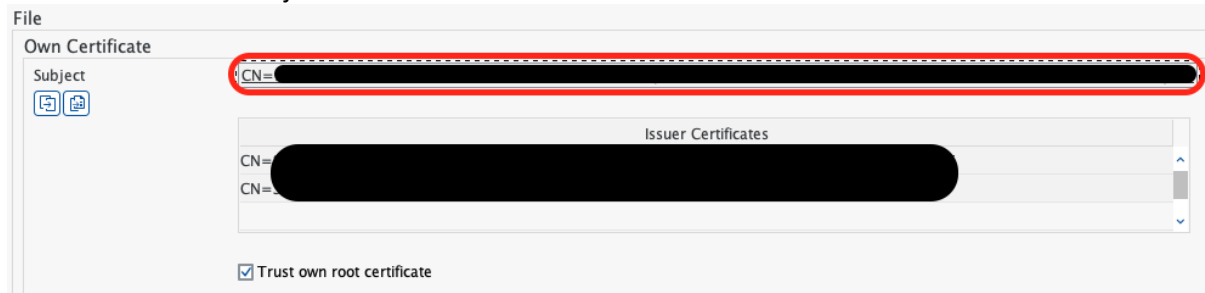


Select PSE -> Import -> PKCS# 12/PFX

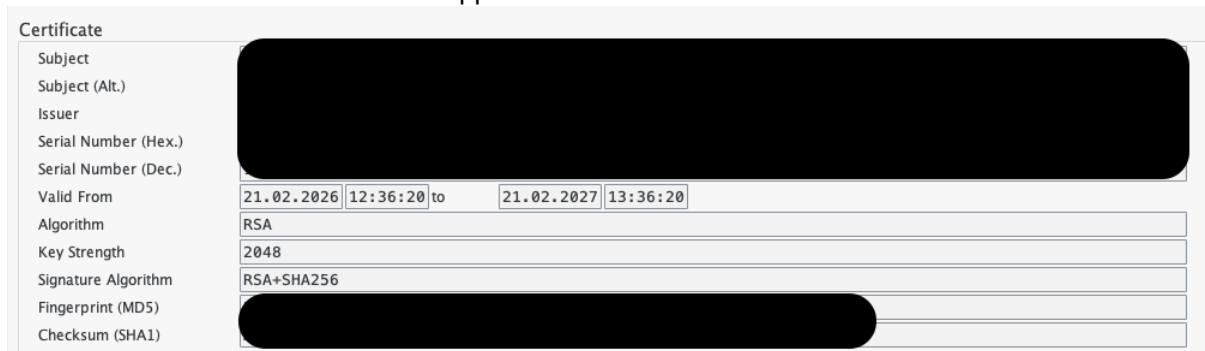


After selecting the certificate from the File upload menu the following should be visible.

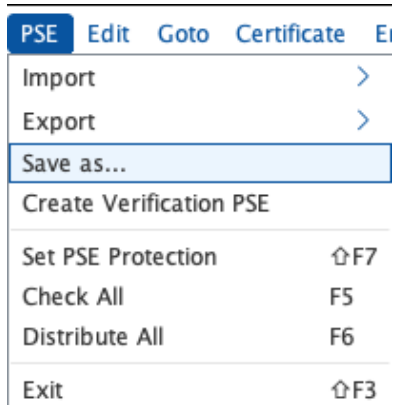
Double click on the subject field marked in red.



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.

SSL Client

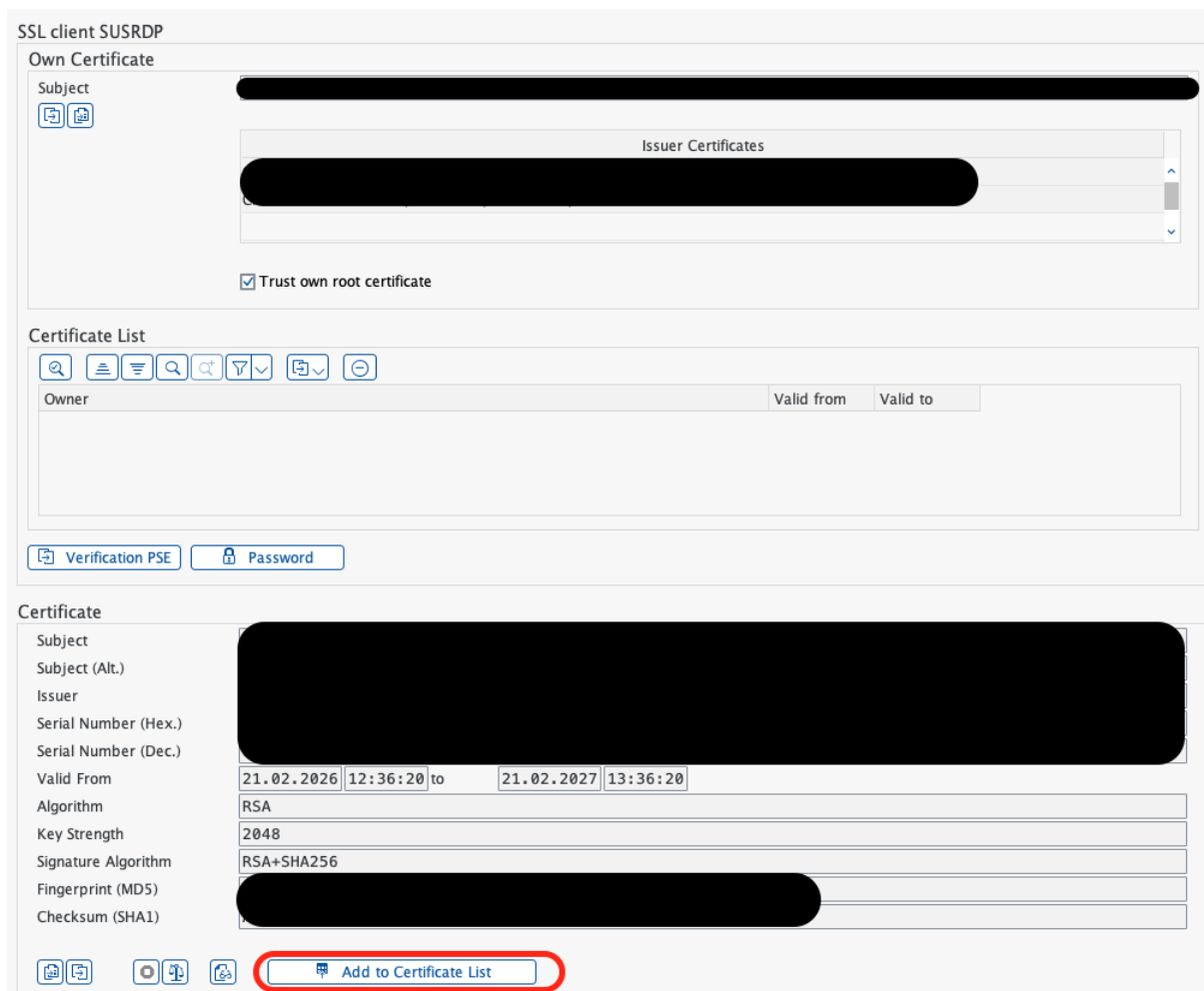


Client dependent

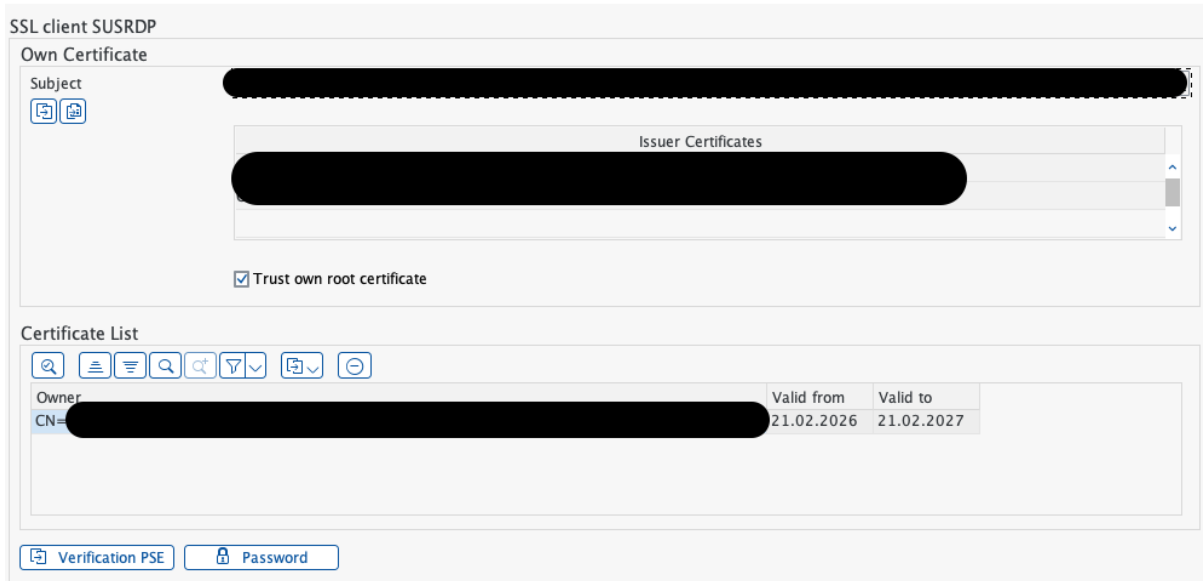
The SSL Client should now appear as a folder instead of having an X.



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.



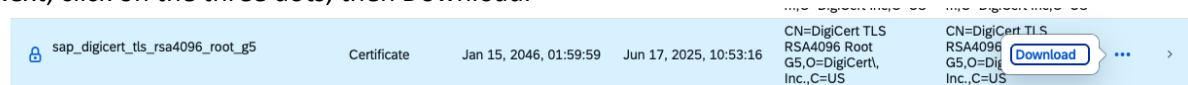
A root certificate is also required to complete the chain.

The correct certificate can be found in the CPI Instance.

Go to Monitor -> Integrations and APIs -> Manage Security -> Keystore.

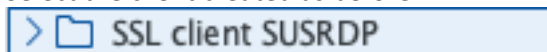
It should be named sap\_digicert\_tls\_rsa4096\_root\_g5 or something similar and should be maintained by SAP which is indicated by the lock icon.

Next, click on the three dots, then Download.



Go back to the S/4 system, 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.

**Certificate**

Subject	CN=DigiCert TLS RSA4096 Root G5, O="DigiCert, Inc.", C=US
Subject (Alt.)	
Issuer	CN=DigiCert TLS RSA4096 Root G5, O="DigiCert, Inc.", C=US
Serial Number (Hex.)	[REDACTED]
Serial Number (Dec.)	[REDACTED]
Valid From	15.01.2021 00:00:00 to 14.01.2046 23:59:59
Algorithm	RSA
Key Strength	4096
Signature Algorithm	RSA+SHA384
Fingerprint (MD5)	[REDACTED]
Checksum (SHA1)	[REDACTED]



Make sure to save the changes.



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

**Certificate List**

Owner	Valid from	Valid to
CN=[REDACTED]	21.02.2026	21.02.2027
CN=DigiCert TLS RSA4096 Root G5, O="DigiCert, Inc.", C=US	15.01.2021	14.01.2046

## 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.

**Search Service Definitions**

Search Pattern: ProductMDMBulkRep... Go

**Configure Service Definitions**

Save Show Changes Information: Standard Set Selected Unset Selected

Actions	Internal Name	User Name/Password (Basic)	X.509 Client Certificate	SAP Logon Ticket
	PRODUCTMDMBULKREPLICATEREQUEST	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Next click on the display button:

Actions	Internal Name
<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	PRODUCTMDMBULKREPLICATEREQUEST

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".

**Details of Provider Configuration** ✖

---

**Details of the Service Definition**

Internal Name: PRODUCTMDMBULKREPLICATEREQUEST  
 External Name: ProductMDMBulkReplicateRequest\_In  
 External Namespace: http://sap.com/xi/APPL/Global2  
 Description: ProductMDMBulkReplicateRequest Inbound Service

---

**WSDL URLs**

With WS Policy: [REDACTED]  
 Without WS Policy: [REDACTED]

---

**Configuration Details**

Configuration Name: [REDACTED]  
 Access URL: /sap/bc/srt/scs/sap/productmdmbulkreplicaterequest?sap-client=  
 Last Change User: [REDACTED]  
 Last Change Date: [REDACTED]  
 Last Change Time: [REDACTED]

OK

## 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

The screenshot shows the SAP Service Administration navigation menu. The 'Web Service Configuration' option is highlighted with a red box. The menu includes the following items:

- Service Administration** (selected)
- Technical Administration
- Logs and Traces
- Management Connections
- Services Registry
- Monitoring
- Tools

Under 'Service Administration', the following options are listed:

- Identifiable Business Context**: Display and maintain Identifiable Business Contexts (IBCs)
- Identifiable Business Context Reference**: Display and maintain Identifiable Business Contexts references (IBC reference)
- Design Time Cache**: Display central design time cache
- Web Service Configuration** (highlighted): Configure service definitions, consumer proxies and service groups
- Simplified Web Service Configuration**: Configure service definitions for Web service consumers with limited capabilities
- Logon Data Management**: Define logon data used by business scenario configuration
- Pending Tasks**: Process pending tasks generated by business scenario configuration
- Local Integration Scenario Configuration**: Configure multiple service definitions and service groups supporting change management
- Logical Determination of Receiver using Service Groups**: Define rules for determining receiver IBC reference during service group runtime
- Logical Determination of Receiver, Sender and Authentication using Consumer Factories**: Define rules for determining receiver IBC, sender IBC and authentication method during consumer factory runtime
- Web Service Isolation**: Tool to isolate service definitions and consumer proxies

Search using: Object Name is ProductMDMBulkReplicateConfirmation\_Out  
 Select CO\_MDM\_PRD\_BULK\_REP\_CONF\_OUT

The screenshot shows the search results for 'CO\_MDM\_PRD\_BULK\_REP\_CONF\_OUT'. The search criteria are: Object Type is All, Object Name is PRODUCTMDMBU... The search results table is as follows:

Internal Name	Type	Name	Namespace	Description
CO_MDM_PRD_BULK_REP_CONF_OUT	Consumer Proxy	ProductMDMBulkReplicateConfirmation_Out	http://sap.com/xi/APPL/Global2	Outbound Interface for Product Data Re...
PRODUCTMDMBULKREPLICATECONF...	Service Definition	ProductMDMBulkReplicateConfirmation_In	http://sap.com/xi/APPL/Global2	Inbound Interface for Product Data Repl...

Check the defined logical ports.

The screenshot shows the 'Details of Consumer Proxy: CO\_MDM\_PRD\_BULK\_REP\_CONF\_OUT' page. The 'Configurations' tab is selected. The 'Define Logical Ports' section is visible, showing a table with columns for 'Actions' and 'Logical Port'. The 'Actions' column contains buttons for 'Create', 'Set Log.Port Default', 'Activate', 'Deactivate', and 'Delete'. The 'Logical Port' column is currently empty.

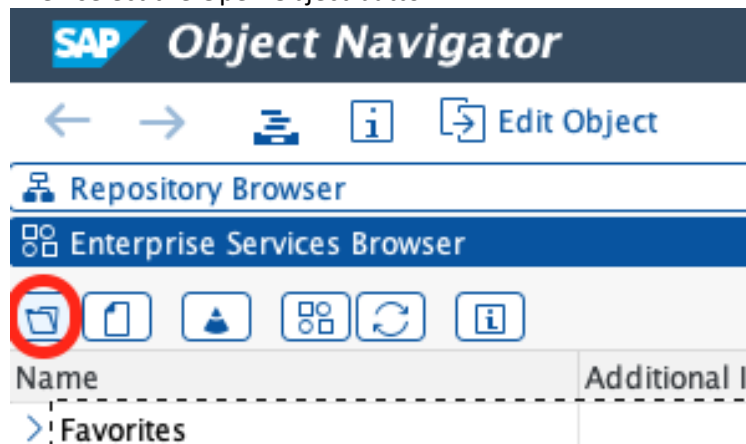
If there are no ports listed or none of them have the option Logical Port is Default set to true, then both **Setup with Default Logical Port** or **Setup without Default Logical Port** may be used. However, if that is not the case, **Setup without Default Logical Port** must be used.

## Outbound Confirmation without Default Logical Port (Recommended)

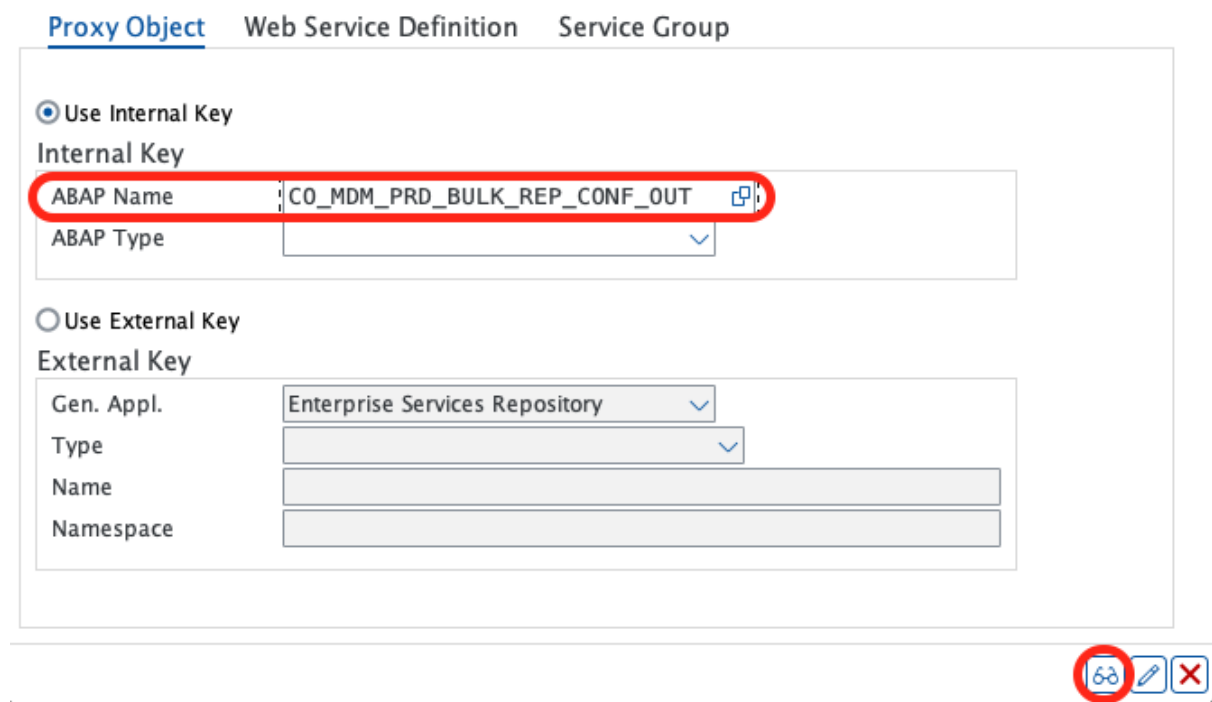
This approach involves autogenerating a proxy for the CPI Instance. It involves more steps in order to configure than the approach with Default Logical Port since CPI is considered a Third-Party System. However it is a more flexible approach and lacks the drawbacks of the setup with Default Logical Port,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

Service Consumer **ProductMDMBulkReplicateConfirmation\_Out** Active

Properties External View Internal View Objects Configuration **WSDL** Classifications

### Service Consumer

Name	ProductMDMBulkReplicateConfirmation_Out		
Namespace	http://sap.com/xi/APPL/Global2		
ABAP Object	CLAS Class		
ABAP Name	CO_MDM_PRD_BULK_REP_CONF_OUT		
Prefix	MDM_PRD_		
Source	Enterprise Services Repository		
Description	Outbound Interface for Product Data Replication (Confirmatio		

### General Data

Package	APPL_MD_PRODUCT_INTEGRATION	Semant Version	1.0.0
Original Language	EN English	Leading BO	Product
Release Status	S Released with ...		
Created by	[REDACTED]		
Changed by	[REDACTED]		

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

Service Consumer **ProductMDMBulkReplicateConfirmation\_Out** Active

Properties External View Internal View Objects Configuration **WSDL** Classifications

Format **Standard**

[Save to file] [Save]

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>
          </wsp:Policy>
        </wsp>All>
      </wsp:Policy>
    </wsp:ExactlyOne>
  </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/wsd1" />
  <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>
  <sapattachnd:Enabled
xmlns:sapattachnd="http://www.sap.com/710/features/attachment/">true</sapattachnd: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">
    <wssoap12:address location="<URL_TO_SOAP_API>" />
  </wsdl:port>
</wsdl:service>

```

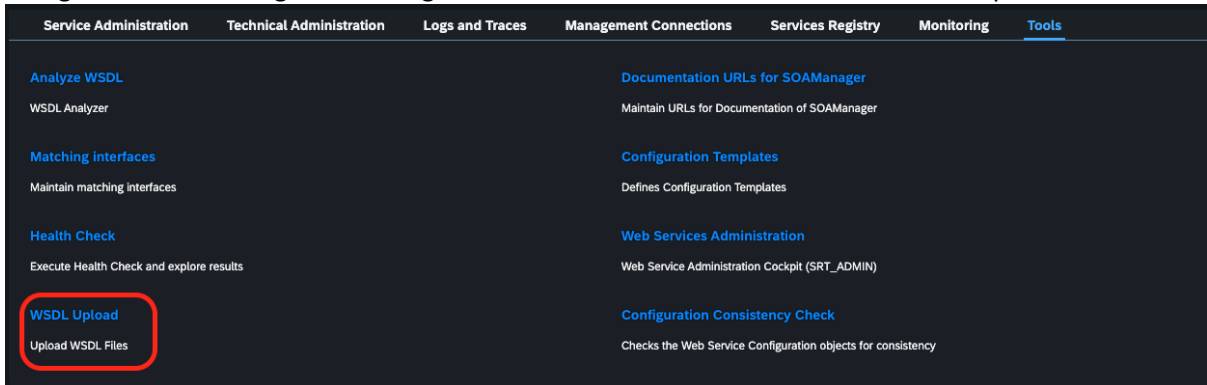
Replace <URL\_TO\_SOAP\_API> placeholder with the actual address pointing to the “Receive SOAP Confirmation and Start Follow-Up Processing” integration flow in Cloud Integration. Make sure to include the port :443 after the host as shown in the screenshot below.

```

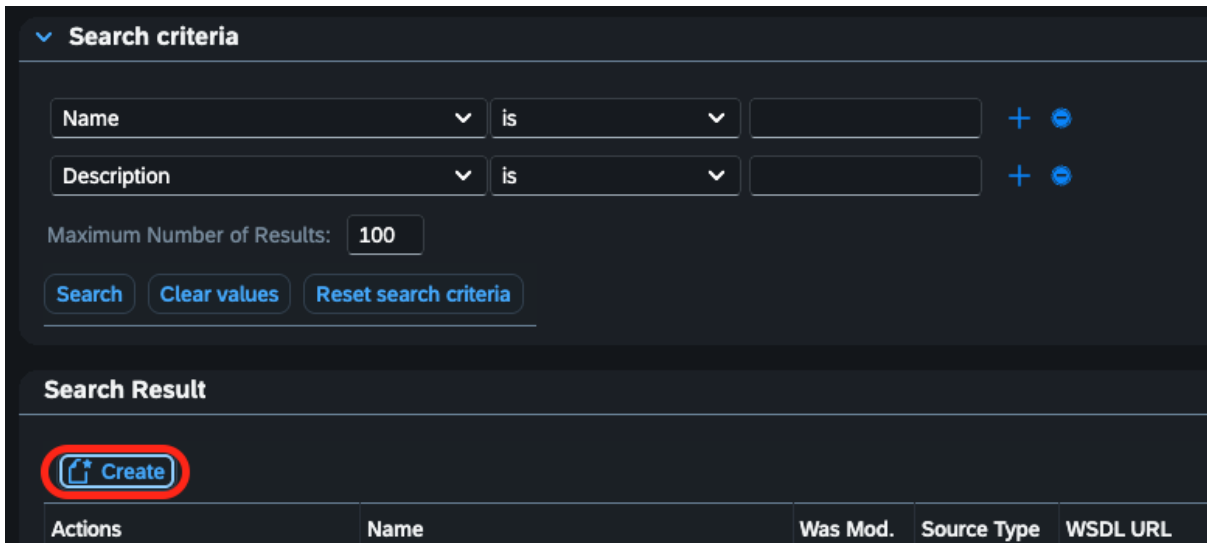
<wsdl:binding type="tns:ProductMDMBulkReplicateConfirmation_Out" name="CO_MDM_PRD_BULK_REP_CONF_OUT_S12">
  <wsp:Policy>
    <wsp:PolicyReference URI="#BN_CLIENT_CERTIFICATE"/>
  </wsp:Policy>
  <wssoap12:binding transport="http://schemas.xmlsoap.org/soap/http" style="document"/>
  <wsdl:operation name="ProductMDMBulkReplicateConfirmation_Out">
    <wsdl:input>
      <wssoap12: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">
    <wssoap12:address location="https://...:443/cxf/confirmation"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>

```

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.

**Upload WSDL**

Name:

Description:

WSDL Base:  Via HTTP Access  
 Via File

**WSDL Location**

File:

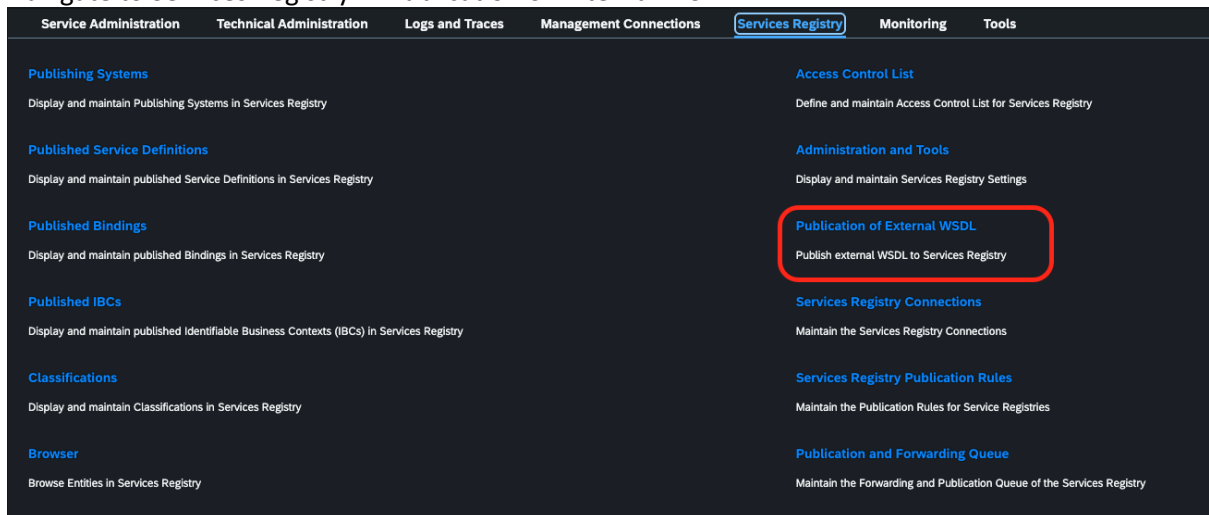
**OK** Cancel

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.

< Previous **Next >** Finish Cancel

### Import WSDL

Enter the binding WSDL URL for a service definition to publish it on the Services Registry

Load WSDL from:  External  
 Uploaded

Name:

Enter an Internal Name of choice. Then click Next.

< Previous **Next >** Finish Cancel

### Service Details

WSDL URL:

Review and change details if necessary

Port Type Name:

Namespace:

**Internal Name:**

Description:

Documentation URL:

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

< Previous **Next >** Finish Cancel

### Classifications

Enter Classifications for the Service Definition.

**Add**

Classification Name

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

< Previous Next > Finish Cancel

### Service State

State:  Implemented  **Configured**

Description: Configured - Bindings are configured and ready to use.

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

< Previous Next > Finish Cancel

### Bindings

Config the bindings that will be published.

**Bindings**

Binding Name	Binding URL
<input checked="" type="radio"/> CO_MDM_PRD_BULK_REP_CONF_OUT_S12	/sap/bc/srt/wsdll/ext_SUS_RDP?sap-client=
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	
<input type="radio"/>	

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.

< Previous Next > Finish Cancel

### Physical System

New  Existing

**System Name:**

**Host Name:**

System Type:  ABAP  Third Party

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

[< Previous](#)
[Next >](#)
[Finish](#)
[Cancel](#)

## Summary

[Service Details](#)

WSDL URL:

WSDL URL: ProductMDMBulkReplicateConfirmation\_Out

Namespace: http://sap.com/xi/APPL/Global2

Internal Name: SUS\_RDP\_SYS

Description:

Documentation URL:

State: Configured

[Classifications](#)

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

[Service Administration](#)
[Technical Administration](#)
[Logs and Traces](#)
[Management Connections](#)
[Services Registry](#)
[Monitoring](#)
[Tools](#)

[Publishing Systems](#)  
 Display and maintain Publishing Systems in Services Registry

[Published Service Definitions](#)  
 Display and maintain published Service Definitions in Services Registry

[Published Bindings](#)  
 Display and maintain published Bindings in Services Registry

[Published IBCs](#)  
 Display and maintain published Identifiable Business Contexts (IBCs) in Services Registry

[Classifications](#)  
 Display and maintain Classifications in Services Registry

[Browser](#)  
 Browse Entities in Services Registry

[Access Control List](#)  
 Define and maintain Access Control List for Services Registry

[Administration and Tools](#)  
 Display and maintain Services Registry Settings

[Publication of External WSDL](#)  
 Publish external WSDL to Services Registry

[Services Registry Connections](#)  
 Maintain the Services Registry Connections

[Services Registry Publication Rules](#)  
 Maintain the Publication Rules for Service Registries

[Publication and Forwarding Queue](#)  
 Maintain the Forwarding and Publication Queue of the Services Registry

[Search criteria](#)

Internal Name   +

External Name   +

Pattern   +

Publishing System   +

State   +

Maximum Number of Results:

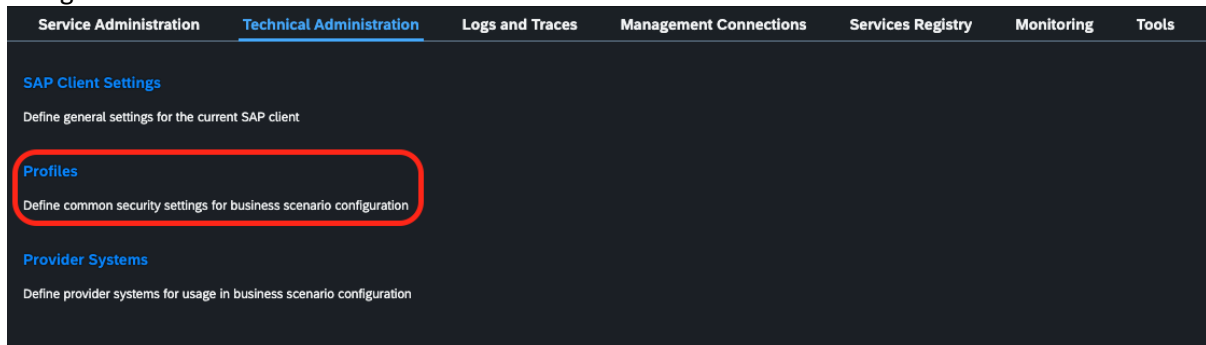
[Search](#)
[Clear values](#)
[Reset search criteria](#)

[Remove](#)

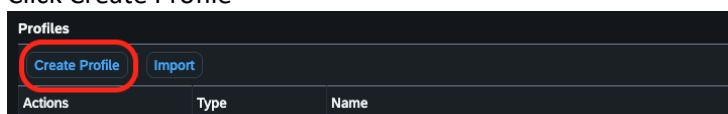
Actions	Internal Name	External Namespace	External Name	State	Description	Publishing System
<input type="checkbox"/>	SUS_RDP_SYS	http://sap.com/xi/APPL/Global2	ProductMDMBulkReplicateConfirmation_Out	Configured		SUS_RDP on RDP CPI

## Create Profile

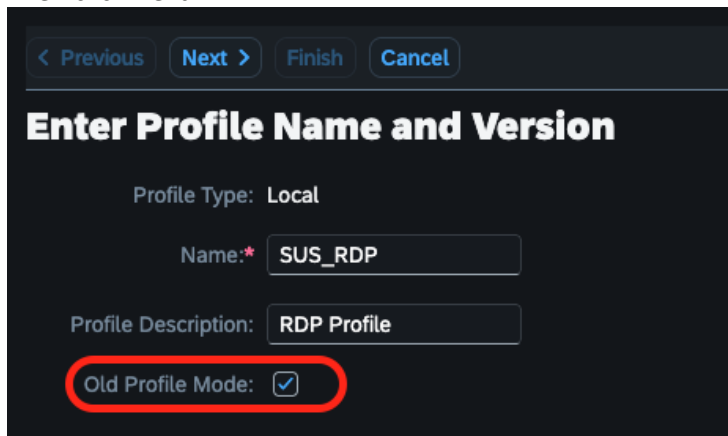
Navigate to Technical Administration -> Profiles



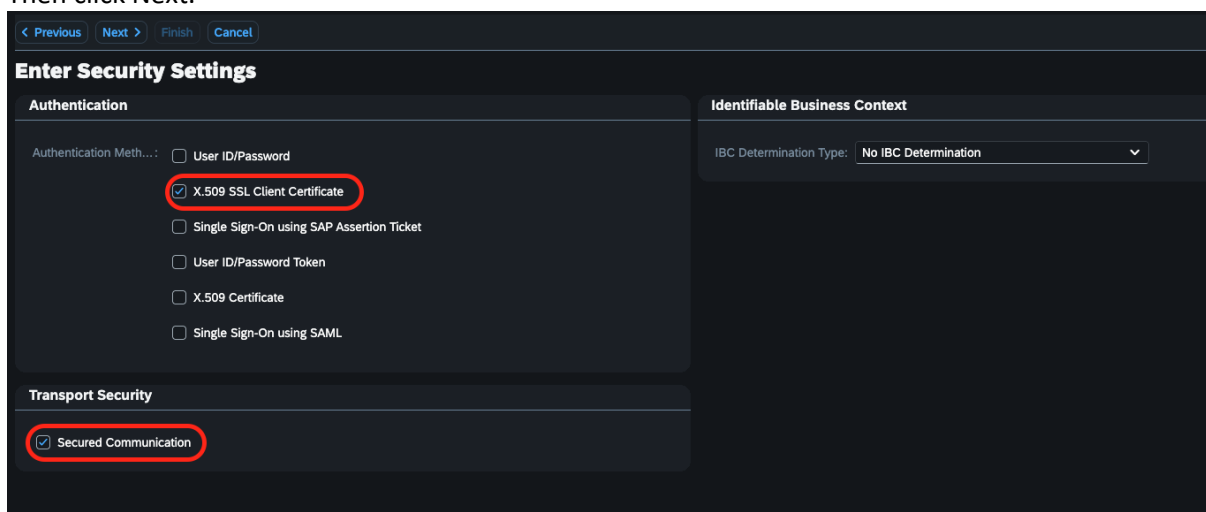
Click Create Profile



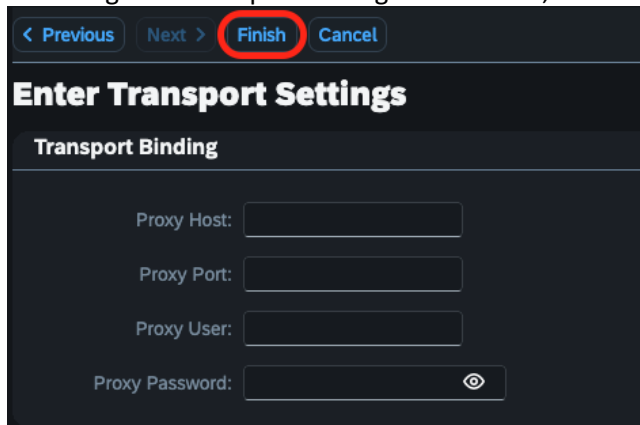
Enter a name and description for the profile and make sure to check "Old Profile Mode". Then click Next.



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.

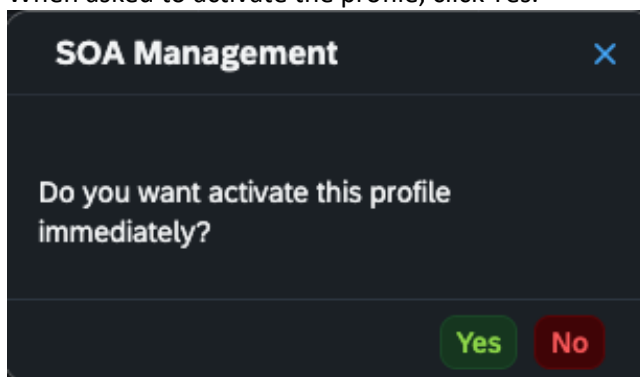


No changes to Transport settings are needed, click Finish.



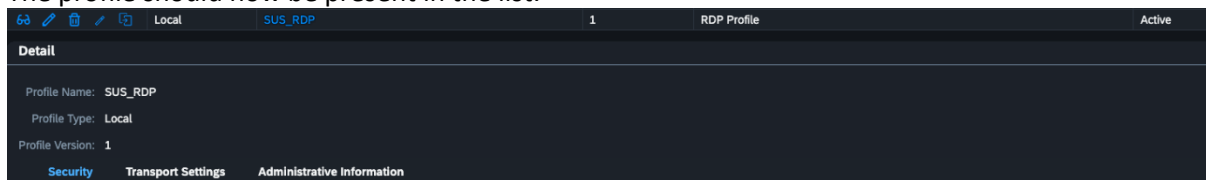
The screenshot shows a dark-themed dialog box titled "Enter Transport Settings". At the top, there are four buttons: "< Previous", "Next >", "Finish", and "Cancel". The "Finish" button is highlighted with a red circle. Below the buttons is a section titled "Transport Binding" with four input fields: "Proxy Host:", "Proxy Port:", "Proxy User:", and "Proxy Password:". The "Proxy Password:" field includes a small eye icon for toggling visibility.

When asked to activate the profile, click Yes.



The screenshot shows a dark-themed dialog box titled "SOA Management" with a close button (X) in the top right corner. The main text asks, "Do you want activate this profile immediately?". At the bottom, there are two buttons: a green "Yes" button and a red "No" button.

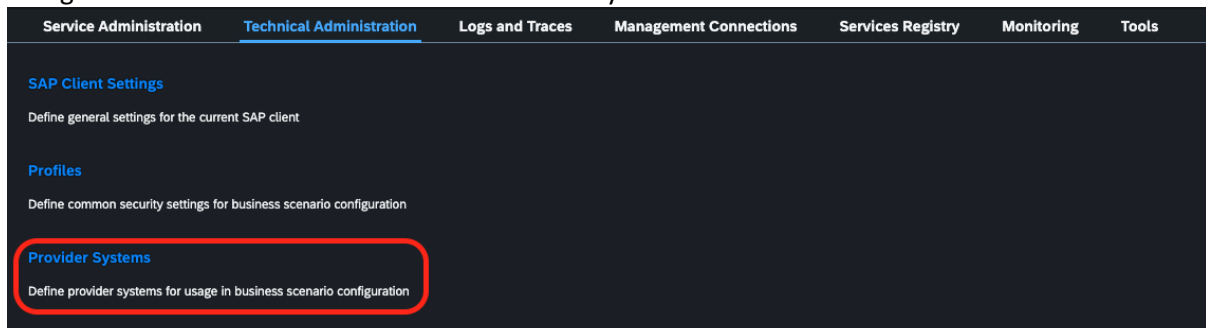
The profile should now be present in the list.



The screenshot shows a table of profiles. The first row is highlighted and contains the following information: "Local" (Location), "SUS\_RDP" (Profile Name), "1" (Profile Version), "RDP Profile" (Profile Type), and "Active" (Status). Below the table, there are tabs for "Security", "Transport Settings", and "Administrative Information".

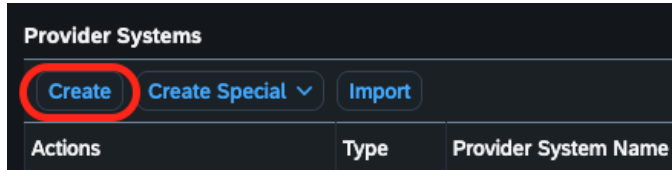
## Create Provider System

Navigate to Technical Administration -> Provider Systems



The screenshot shows a navigation menu at the top with the following items: "Service Administration", "Technical Administration" (which is underlined and highlighted), "Logs and Traces", "Management Connections", "Services Registry", "Monitoring", and "Tools". Below the menu, there are three sections: "SAP Client Settings" (with a sub-description "Define general settings for the current SAP client"), "Profiles" (with a sub-description "Define common security settings for business scenario configuration"), and "Provider Systems" (with a sub-description "Define provider systems for usage in business scenario configuration"). The "Provider Systems" section is highlighted with a red rounded rectangle.

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

The screenshot shows a form titled 'Enter Provider System name and Profile name'. It has navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The form fields are: 'Name:\*' with 'SUS\_RDP' entered, 'Description:' (empty), 'Profile Name:\*' with 'SUS\_RDP' selected in a dropdown, and 'Profile Version:' with '1' entered.

Select “Use Services Registry”

Services Registry: Choose SR\_LOCAL from dropdown

SLD Identifier: Choose SLD Identifier (Physical System) created earlier from the list.

The screenshot shows a form titled 'Enter connection settings for searching web services and credentials to access service'. It has navigation buttons: '< Previous', 'Next >', 'Finish', and 'Cancel'. The form fields are: 'Use Services Registry' checked, 'Services Registry:' with 'SR\_LOCAL' selected, and 'SLD Identifier:' with '42010AEF4D5F1FD183FD5732388A1325' entered. A search results table is shown on the right:

Search: SLD Identifier		
Select SLD Identifier from the table		
System ID	Host Name	SLD Identifier
SUS_RDP	RDP CPI	42010AEF4D5F1FD183FD5732388A1325

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”

**WSIL Service**

Use WSIL

Access Url for WSIL:

Format of WSIL URL of ABAP backend: `http://<hostname>:<port>/sap/bc/srt/wsil?sap-client=<client>`

Basic authentication

X509 authentication

User for WSIL:

Password for WSIL:

[Check](#)

---

**WSDL Documents**

Basic authentication

X509 authentication

User for WSDL Access:

Password for WSDL Access:

[Check](#)

---

**Search Granularity**

Tolerant search

After these configurations click Next.

1 — 2 — 3

General **Services Search Settings** Applications

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

**Enter connection settings for searching v**

Click Retrieve Business Applications.

[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

**Retrieve the Business Applications from the**

[Retrieve Business Applications](#) [Create](#)

Actions	Name
<input type="checkbox"/>	

A new entry should appear. After this click Finish.

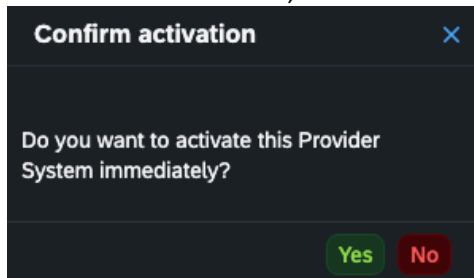
[< Previous](#) [Next >](#) [Finish](#) [Cancel](#)

**Retrieve the Business Applications from the Provider System using WSIL Service or the Services Registry, or maintai**

[Retrieve Business Applications](#) [Create](#)

Actions	Name	Description	Business Application ID
<input type="checkbox"/>	sap.com/BusinessApplicationExternal	sap.com/BusinessApplicationExternal	42010AEF4D5F1FD183FD5732388A1325

When asked to activate, click Yes.

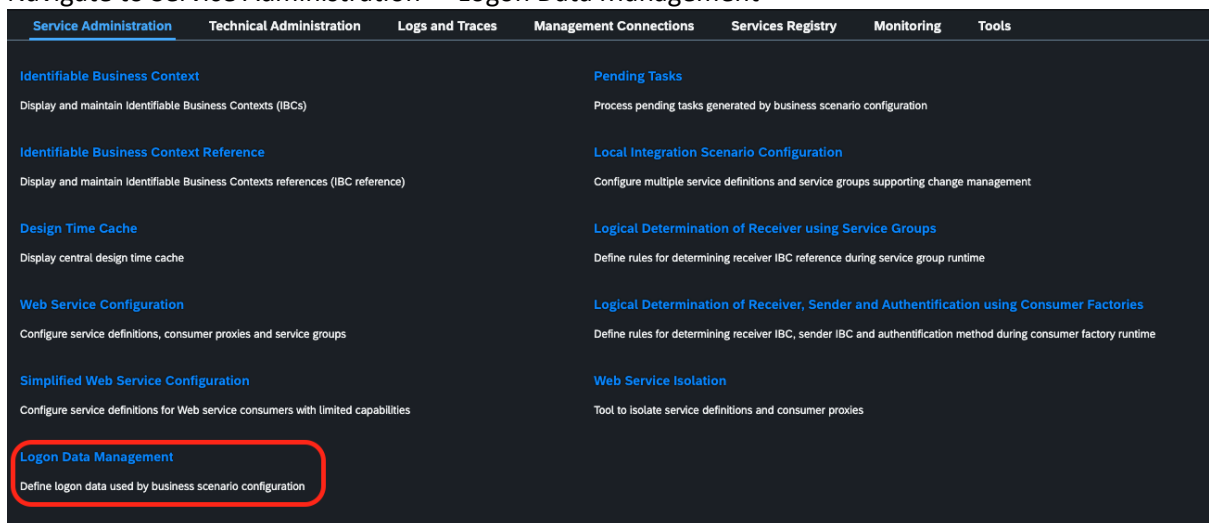


A new Entry should be visible in the Provider System list.

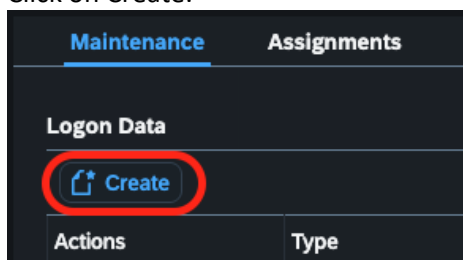


## Create Logon Data

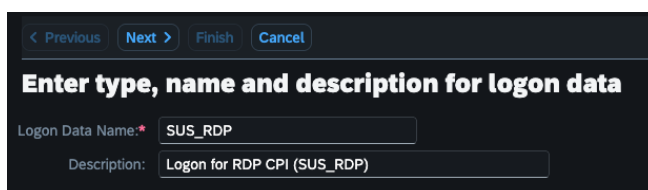
Navigate to Service Administration -> Logon Data Management



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.

< Previous   Next >   Finish   Cancel

### Select an authentication method and specify details if needed

Authentication Met...: \* User/Password or X.509

User Name:

Password:

Confirm Password:

X.509 SSL Client Ce...: SUSRDP

Signature PSE:

Encryption Certificate:

When asked to activate, click Yes.

**SOA Management** ✕

Do you want activate this Logon Data immediately?

Yes No

A new entry should appear in the Logon Data list.

Local   SUS\_RDP   Logon for RDP CPI (SUS\_RDP)   User/Password or X.509   Active

#### Logon Data Detail for 'SUS\_RDP'

**Credentials**   Administrative Information

Authentication Met...: \* User/Password or X.509

User Name:

Password:

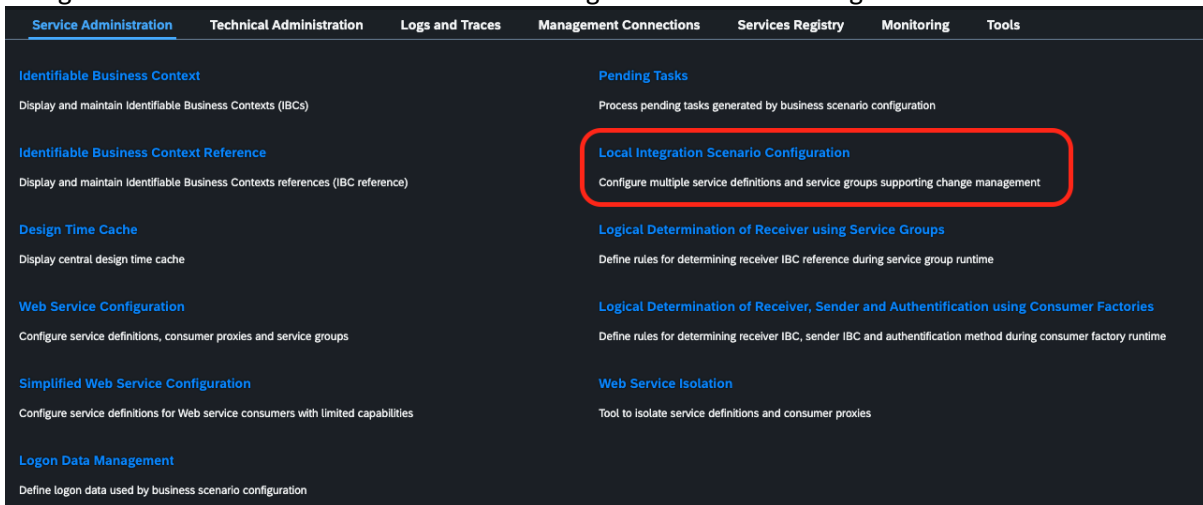
X.509 SSL Client Ce...: SUSRDP

Signature PSE:

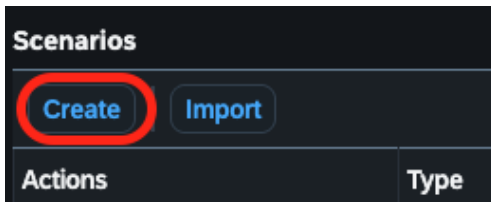
Encryption Certificate:

# Create Local Integration Scenario Configuration

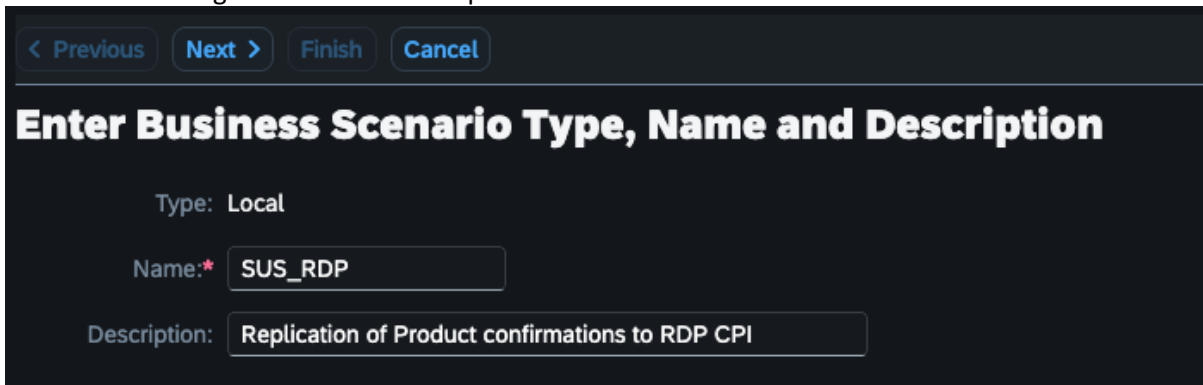
Navigate to Service Administration -> Local Integration Scenario Configuration



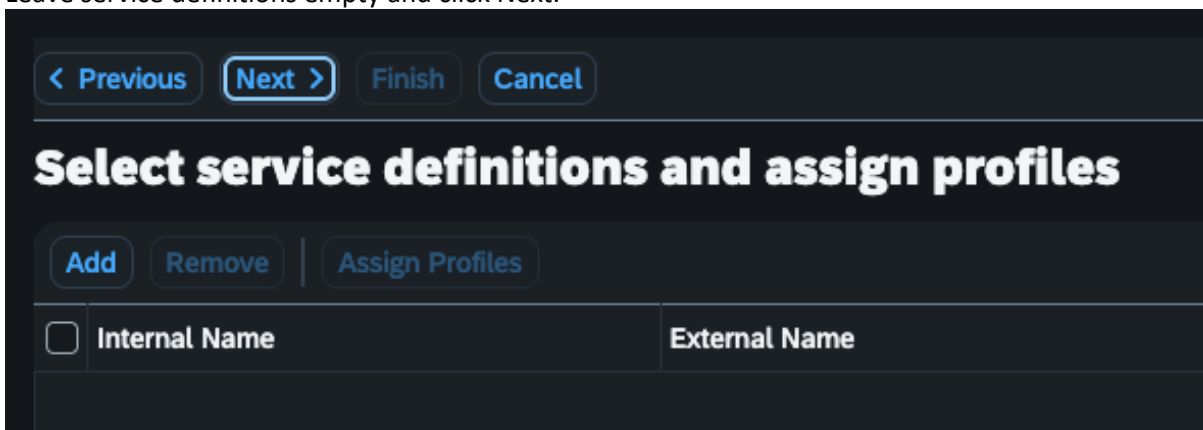
Click Create.



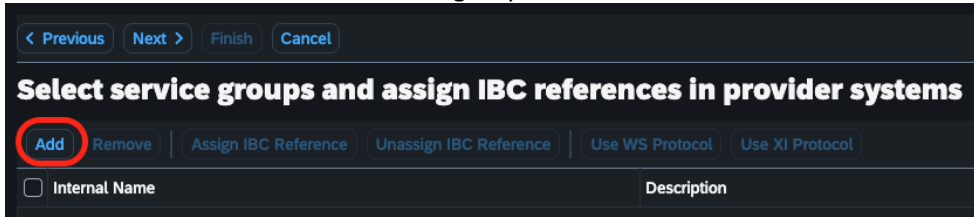
Provide a meaningful Name and Description



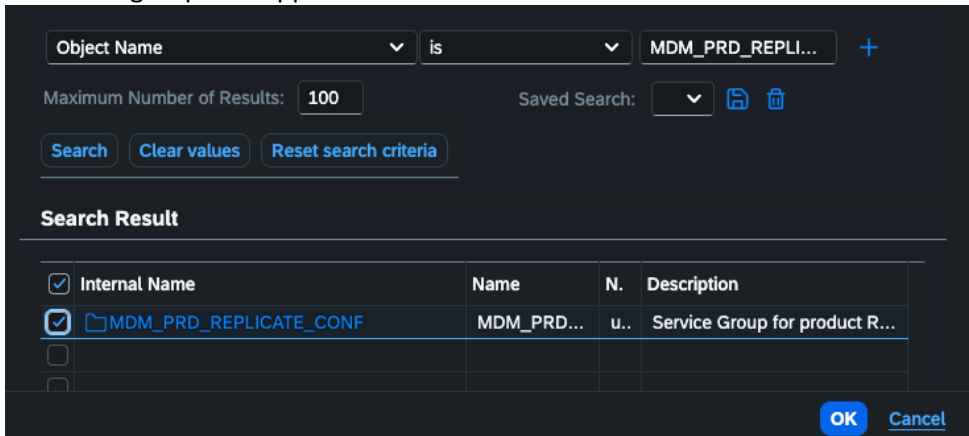
Leave service definitions empty and click Next.



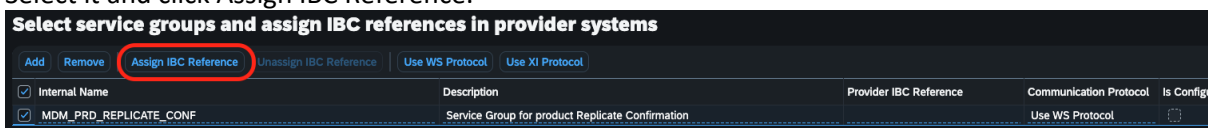
Click the Add button in Select service groups section.



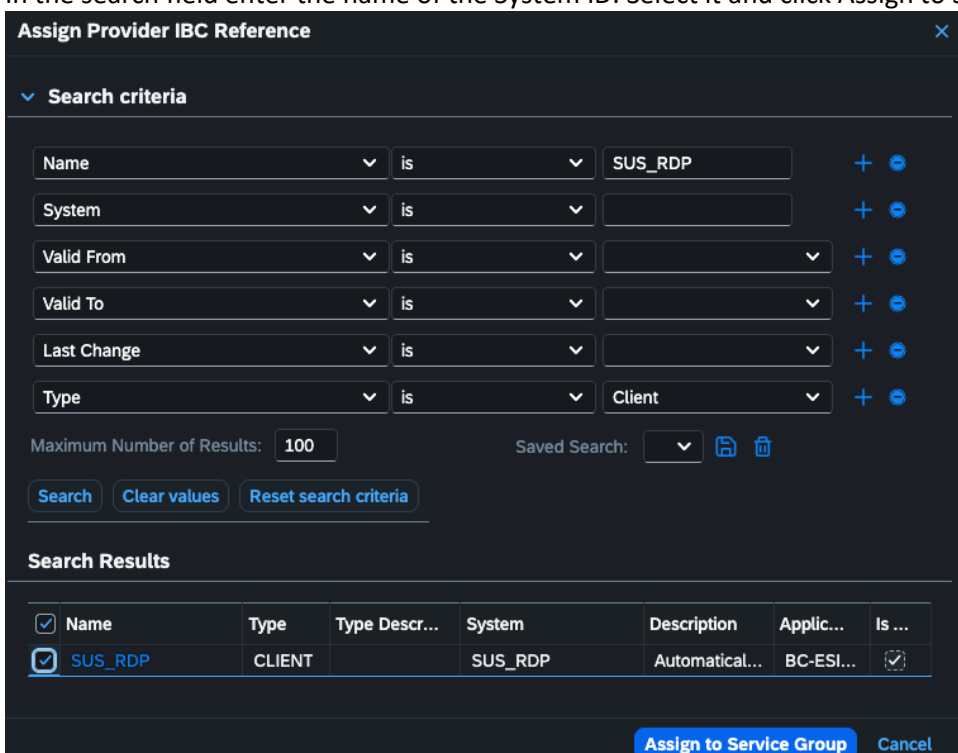
Search for Object Name is **MDM\_PRD\_REPLICATE\_CONF**  
 Select the group that appears and click OK.



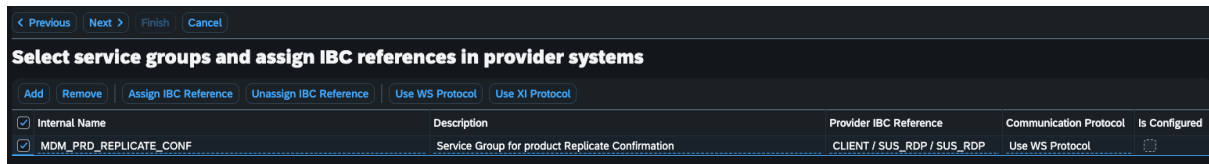
A new entry should appear in the list of service groups.  
 Select it and click Assign IBC Reference.



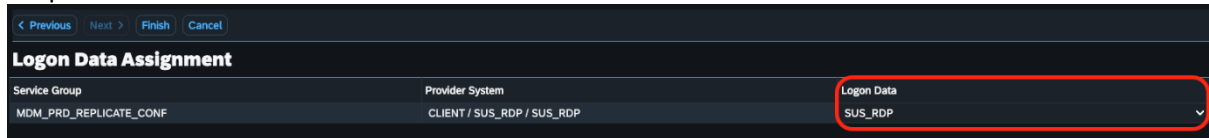
In the search field enter the name of the System ID. Select it and click Assign to Service Group.



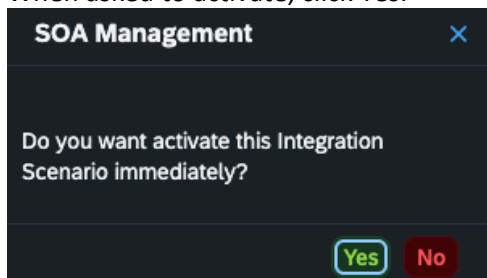
The Provider IBC Reference should now be set. Click Next.



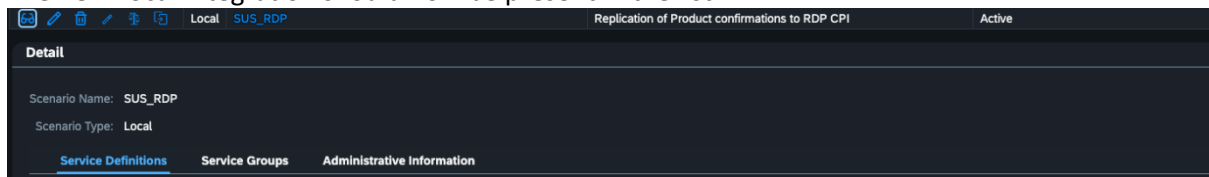
In the Logon Data Assignment, select the Logon Data created from the previous step in the dropdown. Then click Finish.



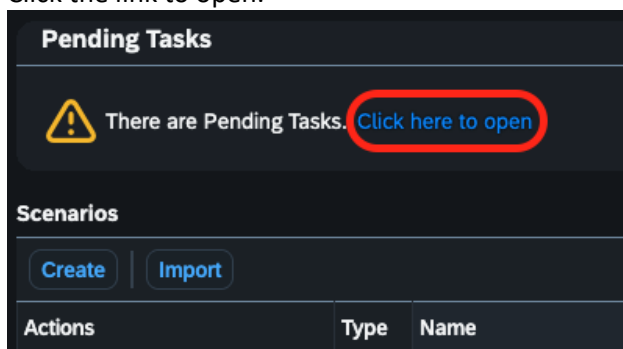
When asked to activate, click Yes.



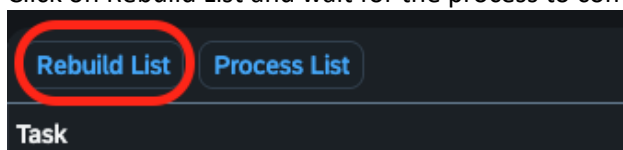
The new Local Integration should now be present in the list.



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



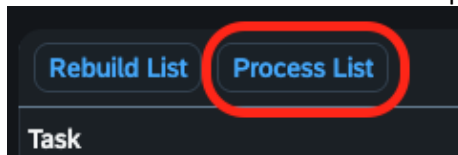
Click on Rebuild List and wait for the process to complete.



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



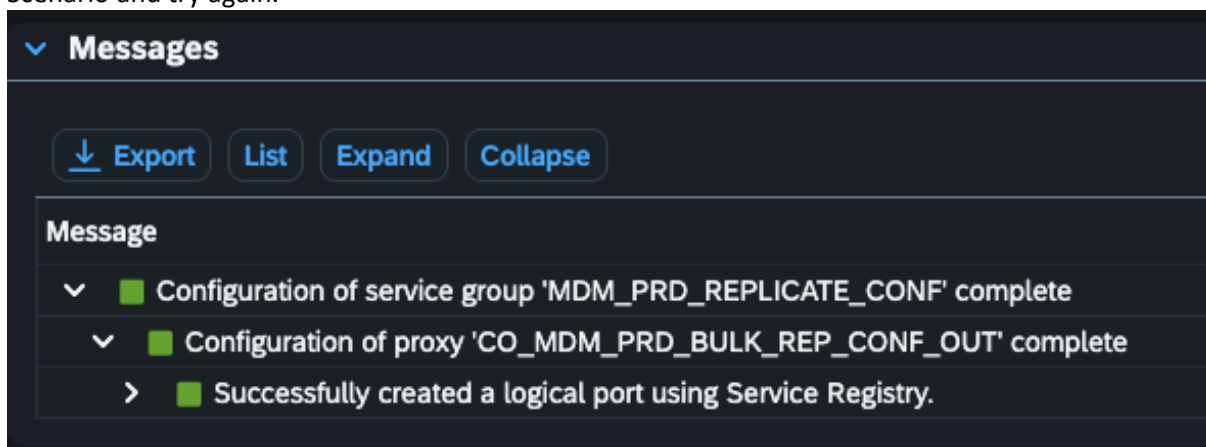
Click on Process List and wait for the process to finish.



If everything is configured correctly, you should see the following message.

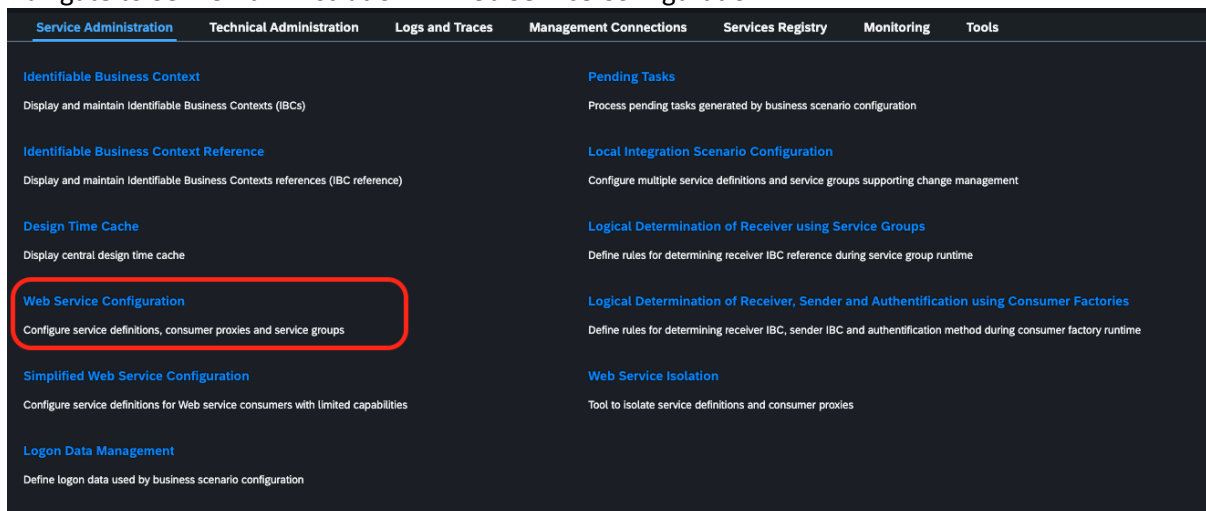
**Important:** This step MUST succeed so you can proceed!

**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.

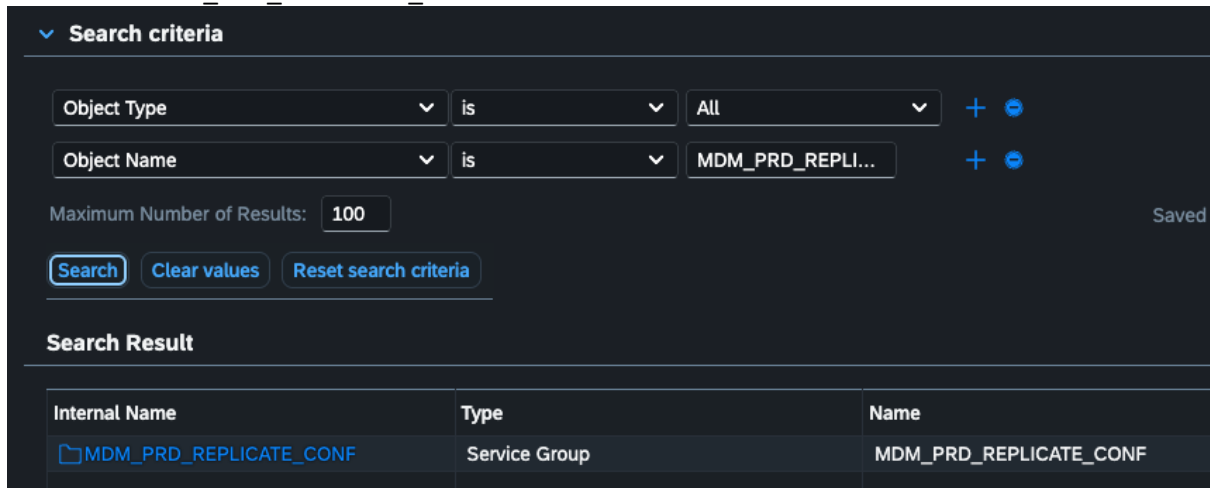


## Create Fallback Logical Port

Navigate to Service Administration -> Web Service Configuration



Search for MDM\_PRD\_REPLICATE\_CONF.



The screenshot shows a search interface with the following details:

- Search criteria:**
  - Object Type: [dropdown]
  - Operator: is
  - Value: All
  - Object Name: [dropdown]
  - Operator: is
  - Value: MDM\_PRD\_REPLI...
- Maximum Number of Results: 100
- Buttons: Search, Clear values, Reset search criteria
- Search Result table:

Internal Name	Type	Name
MDM_PRD_REPLICATE_CONF	Service Group	MDM_PRD_REPLICATE_CONF

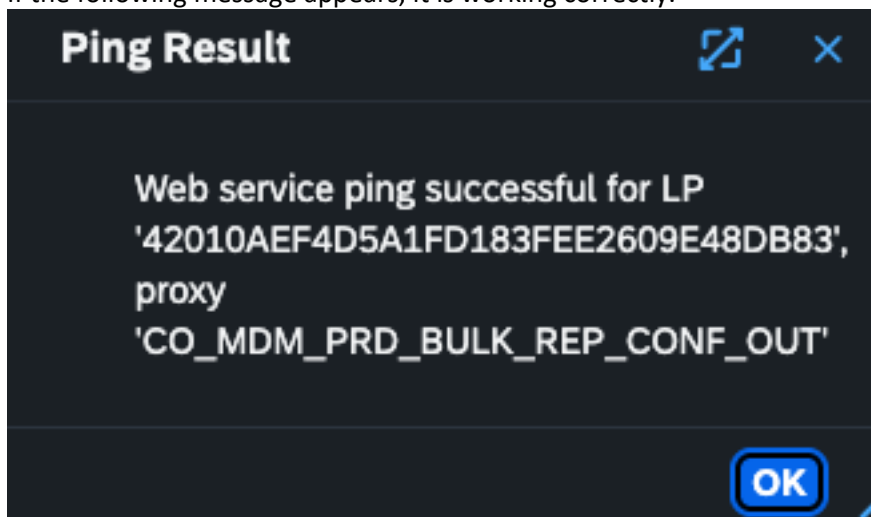
The following Port should have been generated.  
Click the connection button to Ping the CPI Instance.



The screenshot shows a table with port configuration details:

CLIENT / SUS_RDP / SUS_RDP	Local	Local	42010AEF4D5A1FD183FEE2609E48DB83	Active	Created based on profile SUS_RDP/2/Local
----------------------------	-------	-------	----------------------------------	--------	--

If the following message appears, it is working correctly.



The screenshot shows a dialog box titled "Ping Result" with the following text:

Web service ping successful for LP  
'42010AEF4D5A1FD183FEE2609E48DB83',  
proxy  
'CO\_MDM\_PRD\_BULK\_REP\_CONF\_OUT'

An "OK" button is visible at the bottom right of the dialog.

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.

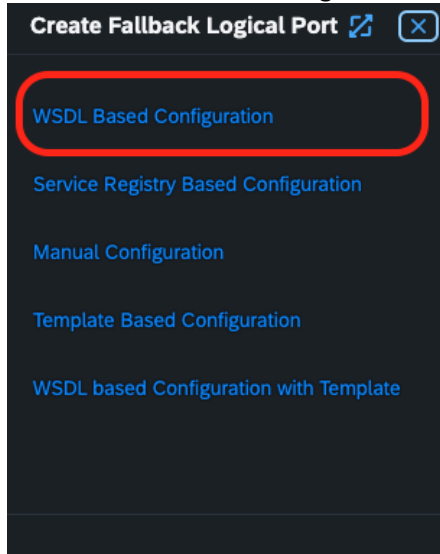
To fix this do the following.  
Click on the Create Fallback Logical Port.



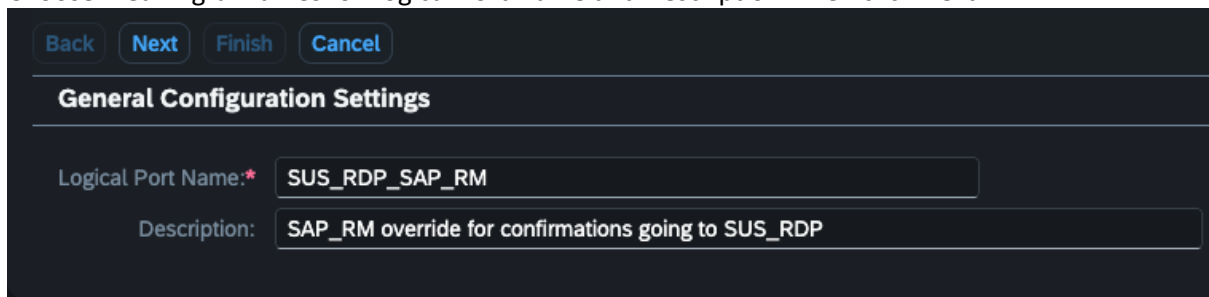
The screenshot shows a table with port configuration details:

CLIENT / SUS_RDP / SUS_RDP	Local	Local	42010AEF4D5A1FD183FEE2609E48DB83	Active	Created based on profile SUS_RDP/2/Local
----------------------------	-------	-------	----------------------------------	--------	--

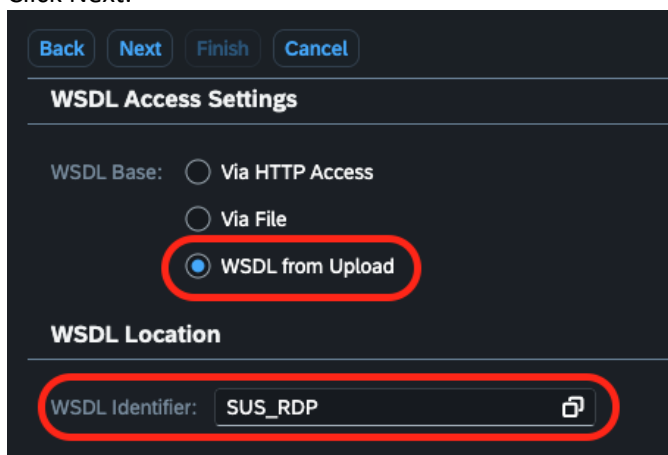
### Choose WSDL Based Configuration



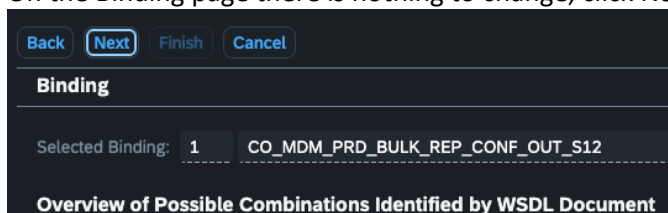
Choose meaningful names for Logical Port Name and Description. Then click Next.



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.

Back Next Finish Cancel

Configuration of Consumer Settings additional to WSDL Document Information LP=SUS\_RDP\_SAP\_RM

**X.509 SSL Client PSE**

SSL Client PSE of transaction STRUST: **SUSRDP**

**Properties from WSDL Document**

**Authentication**

Authentication Method: saps:HTTP509

**Transport Security**

Secure Communications: SSL

Signature Expected: false

Encryption Expected: false

Sign Message: false

Add Encryption: false

**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.

Back Next Finish Cancel

**URL Access Path**

Complete URL  URL components

URL: [REDACTED] :443/cxf/confirmation

Logon Language: Language of User Context

**Proxy**

Name of Proxy Host: [REDACTED]

Port Number of Proxy Host: [REDACTED]

User Name for Proxy Access: [REDACTED]

Password of Proxy User: [REDACTED]

**Transport Binding**

Make Local Call: No Call in Local System

Transport Binding Type: SOAP 1.2

Maximum Wait for WS Consumer: 0

**Optimized XML Transfer: None**

Compress HTTP Message: Inactive

Compress Response: True

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

The screenshot shows a configuration window with three sections: **Reliable Messaging (Asynchr.)**, **Message ID (Synchronous)**, and **Metering of Service Calls**. In the first section, the 'RM Protocol' dropdown is set to 'SAP RM'. In the second section, the 'Message ID Protocol' dropdown is set to 'SAP Message ID'. In the third section, the 'Data transfer scope' dropdown is set to 'Basic Data Transfer' and the 'Transfer protocol' dropdown is set to 'Transfer via SOAP header'. All three dropdown menus are highlighted with red circles.

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.

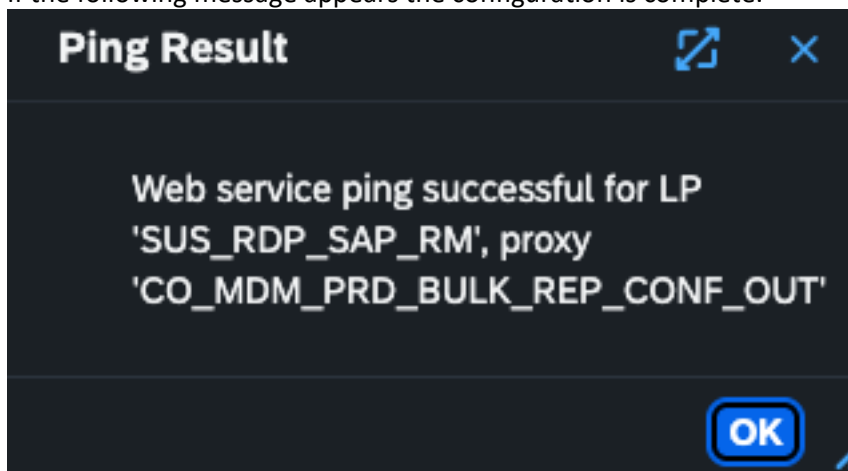
The screenshot shows the 'Identifiable Business Context' configuration window. The 'Finish' button is highlighted with a red circle. Below it, the 'Sender IBC Identifier' field is set to 'CLIENT / [redacted]' and the 'Receiver IBC Identifier' field is set to 'CLIENT / SUS\_RDP / SUS\_RDP'. Both fields have a copy icon to their right. A 'Suppress sending of IBC Identifier' checkbox is present and unchecked.

The result should look similar to this.

Press the connection icon on the second entry to ensure the system is still accessible.

CLIENT / SUS_RDP / SUS_RDP	Local	63		42010AEF4D5A1FD183FEE2609E48DB83	Active	Created based on profile SUS_RDP/2/Local
	Local	63		SUS_RDP_SAP_RM	Active	Manually created

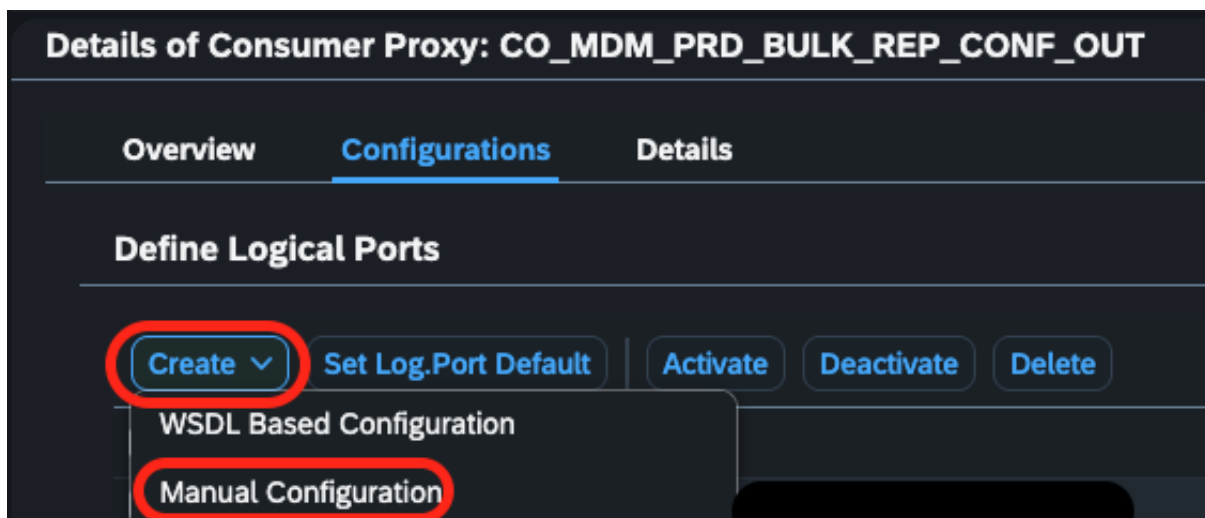
If the following message appears the configuration is complete.



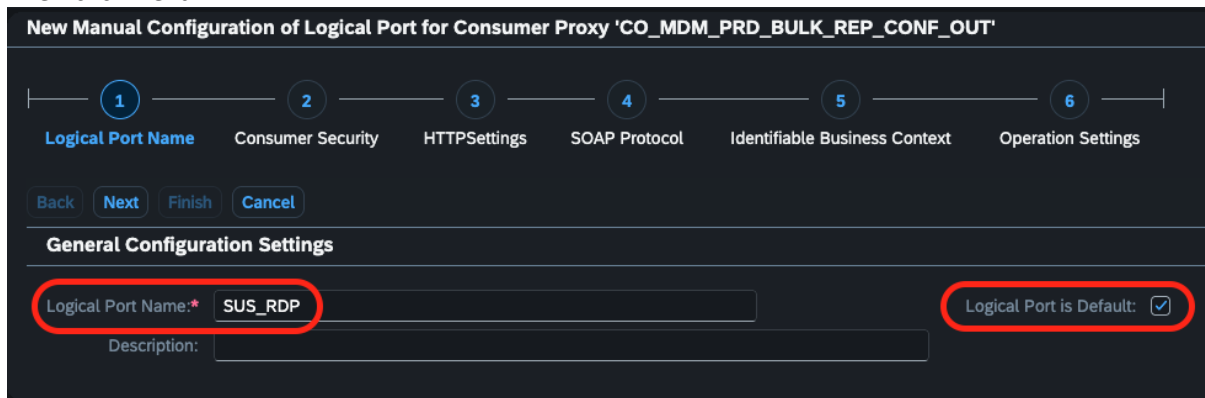
## Outbound Confirmation with Default Logical Port (NOT Recommended)

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.

Configuration of Consumer Settings without WSDL Document. LP=SUS\_RDP

Authentication Level: Basic

**Authentication Settings**

User ID / Password

SAP Authentication Assertion Ticket

X.509 SSL Client Certificate

OAuth 2.0

**X.509 SSL Client PSE**

SSL Client PSE of transaction STRUST:

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.

URL Access Path

Complete URL  URL components

Protocol:\*

Host:\*

Port:

Path:\*

Logon Language:

**Proxy**

Name of Proxy Host:

Port Number of Proxy Host:

User Name for Proxy Access:

Password of Proxy User:

**Transport Binding**

Make Local Call:

Transport Binding Type:\*

Maximum Wait for WS Consumer:

Optimized XML Transfer:

Compress HTTP Message:

Compress Response:

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.

Back Next **Finish** Cancel

**Reliable Messaging (Asynchr.)**

RM Protocol: SAP RM

**Message ID (Synchronous)**

Message ID Protocol: SAP Message ID

**Metering of Service Calls**

Data transfer scope: Basic Data Transfer

Transfer protocol: Transfer via SOAP header

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.

<input checked="" type="checkbox"/>					SUS_RDP	Active	true
<input type="checkbox"/>							

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

