Integration Guide | PUBLIC
2022-07-15

Hungary Transport Registration: Setting Up SAP Cloud Integration (SAP ERP, SAP S/4HANA) - Neo Environment

THE BEST RUN SAP

Content

1 Introduction

You use SAP Cloud Integration to establish the communication with external systems with whom you want to exchange electronic documents created with *SAP Document and Reporting Compliance*. This document lists the required setup steps you perform in the SAP ERP or SAP S/4HANA system* and the SAP Cloud Integration tenant so that the integration between the systems works.

The setup steps are typically done by an SAP Cloud Integration consulting team, which is responsible for configuring the SAP back-end systems and the connection with SAP Cloud Integration. This team may be also responsible for maintaining the integration content and certificates/credentials on the SAP Cloud Integration tenant.

> **i** Note
>
> This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Cloud Integration tenant. It may happen, however, that in the SAP back-end systems the access to such functionality is only partially implemented. Additionally, it may also happen that the tax authority servers do not provide all services that are described in this document. Please refer to the relevant SAP back-end systems documentation and to the relevant tax authority information, respectively.

For the sake of simplicity in this guide, we mention SAP back-end systems when something refers to both SAP ERP or SAP S/4HANA.

2 Prerequisites

Before you start with the activities described in this document, ensure that the following prerequisites are met.

1. Electronic documents for Hungary: All relevant notes are installed in the test and/or productive systems (see SAP Note 2227052 for an overview of which notes are required).
2. Registration at NAV is completed and the following data is available:
   - User name
   - Secret signature key
3. SAP Cloud Integration test/productive tenants are live.
4. You have configured the connection from SAP back-end system to SAP Cloud Integration. Please refer to the following document: http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/4037b5a5-47a5-3110-e891-f3d9dbafbe86.

3 Connectivity Steps

3.1 Setup of Secure Connection

You establish a trustworthy SSL connection to set up a connection between the SAP back-end systems and the SAP Cloud Integration. For more information, see Connecting a Customer System to Cloud Integration.

You use SAP ERP Trust Manager (transaction `STRUST`) to manage the certificates required for a trustworthy SSL connection. The certificates include public certificates to support outbound connections, as well as trusted certificate authority (CA) certificates to support integration flow authentication.

Refer to the system documentation for more information regarding the certificate deployment to SAP back-end systems. In case of issues, refer to the following SAP notes:

- 2368112 Outgoing HTTPS connection does not work in AS ABAP
- 510007 Setting up SSL on Application Server ABAP

For more information, refer to Operating and Monitoring Cloud Integration

> **i Note**
>
> If you encounter any issues in the information provided in the SAP Cloud Integration product page, open a customer incident against the `LOD-HCI-PI-OPS` component.

Client Certificate

If you are using a client certificate, this must be signed by one of the root certificates supported by the load balancer. A self-signed certificate is not suitable. For more information see Load Balancer Root Certificates Supported by SAP.

For information about creating your own certificate and get it signed by a trusted certificate authority (CA), see Authenticate Integration Flows [page 7].

3.1.1 Set Up SAP Cloud Integration Tenants

Ensure that your SAP Cloud Integration test and production tenants are live, and users in the tenants have the rights to copy the integration package and to configure and deploy the integration flows.

When your tenants are provisioned, you receive an email with a Tenant Management (TMN) URL. You need this URL when configuring on your SAP S/4HANA Cloud tenant the communication with the SAP Cloud Integration tenant.

To be able to deploy the security content you must be assigned the `AuthGroup.Administrator` role.

If you are a first-time user, you must first set up your users (members) and their authorizations in the SAP BTP cockpit.

3.1.2 Retrieve and Save Public Certificates

You perform this action in the back-end systems only if you are using certificate-based authentification. Not required for basic authentification.

Context

Find and save the public certificates from your SAP Cloud Integration runtime.

Procedure

1. Access the SAP BTP cockpit, and navigate to your subaccount (tenant) page.
2. Click the subscriptions link to display the subscriptions for your subaccount.
3. Select the subscription with suffix **`iflmap`** as this corresponds to your worker node within SAP Cloud Integration.

   Alternatively, use the URL emailed to you with your SAP Cloud Integration subscription details. The URL has the following format **`https://xxxxx.hana.ondemand.com/itspaces`**.
4. In the *Operations* view, choose *Manage Integration Content* and select *All* to display the integration flows available.
5. Select an integration flow to display its details.
6. Copy the URL listed within the *Endpoints* tab, and paste the URL into your web browser.
7. When prompted by the *Website Identification* window, choose *View certificate*.
8. Select the root certificate, and then choose *Export to file* to save the certificate locally.
9. Repeat these steps for each unique root, intermediate and leaf certificate, and repeat for both your test and production tenants.

3.1.3 Upload the Certificates

Store the public certificates used for your productive and test tenants.

Context

You use the SAP ERP Trust Manager (transaction `STRUST`) to store and manage the certificates required to support connectivity between SAP back-end systems and SAP Cloud Integration.

Procedure

1. Access transaction `STRUST`.
2. Navigate to the PSE for **SSL Client (Anonymous)** and open it by double-clicking the PSE.
3. Switch to edit mode.
4. Choose the *Import certificate* button.
5. In the *Import Certificate* dialog box, enter or select the path to the required certificates and choose *Enter*. The certificates are displayed in the *Certificate* area.
6. Choose *Add to Certificate List* to add the certificates to the *Certificate List*.
7. Save your entries.

3.1.4 Authenticate Integration Flows

Create an own certificate and get it signed by a trusted certificate authority (CA) to support integration flow authentication.

Context

You use the SAP ERP Trust Manager (transaction `STRUST`) for this purpose.

This process is required only if you use certificate-based authentication (that is, you choose the **`X.509 SSL Client Certification`** option in your settings for SOAMANAGER).

Procedure

1. Access transaction `STRUST`.

2. Create your own PSE (for example, Client SSL Standard) and then generate a certificate sign request.
3. Export the certificate sign request as a `*.csr` file.
4. Arrange for the certificate to be signed by a trusted certificate authority (CA).

   If you are using a client certificate, this must be signed by one of the root certificates supported by the load balancer. A self-signed certificate is not suitable. For more information, see Load Balancer Root Certificates Supported by SAP.

   The CA may have specific requirements and request company-specific data, they may also require time to analyze your company before issuing a signed certicate. When signed, the CA provides the certificate for import.
5. Navigate to the PSE for **SSL Client Standard** and open it by double-clicking the PSE.
6. Switch to edit mode.
7. Choose the *Import certificate* button.
8. In the *Import Certificate* dialog box, enter or select the path to the CA-signed certificate and choose *Enter*. The certificate is displayed in the *Certificate* area.
9. Choose *Add to Certificate List* to add the signed certificate to the *Certificate List*.

   Ensure that you import the CA root and intermediate certificates to complete the import.
10. Save your entries.

    The certificates can now be used in the SOA Manager (transaction `SOAMANAGER`).

4 Configuration Steps in SAP Integration Suite

The following sections tell you the necessary configuration you do in SAP Integration Suite.

4.1 General Information

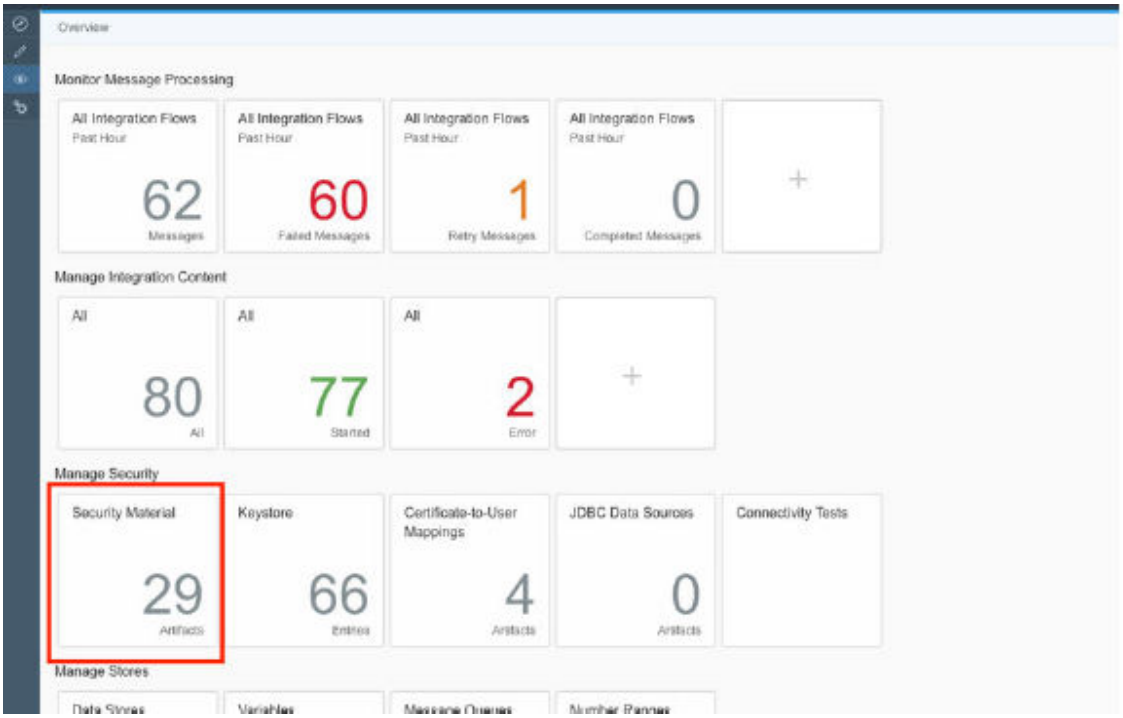
The package *SAP Document and Reporting Compliance: Transport Registration for Hungary* contains the following integration flow:

Integration Flow Name in WebUI	Project Names / Artifact Names
com.sap.GS.Hungary.ManageTradeCard	com.sap.GS.Hungary.ManageTradeCard

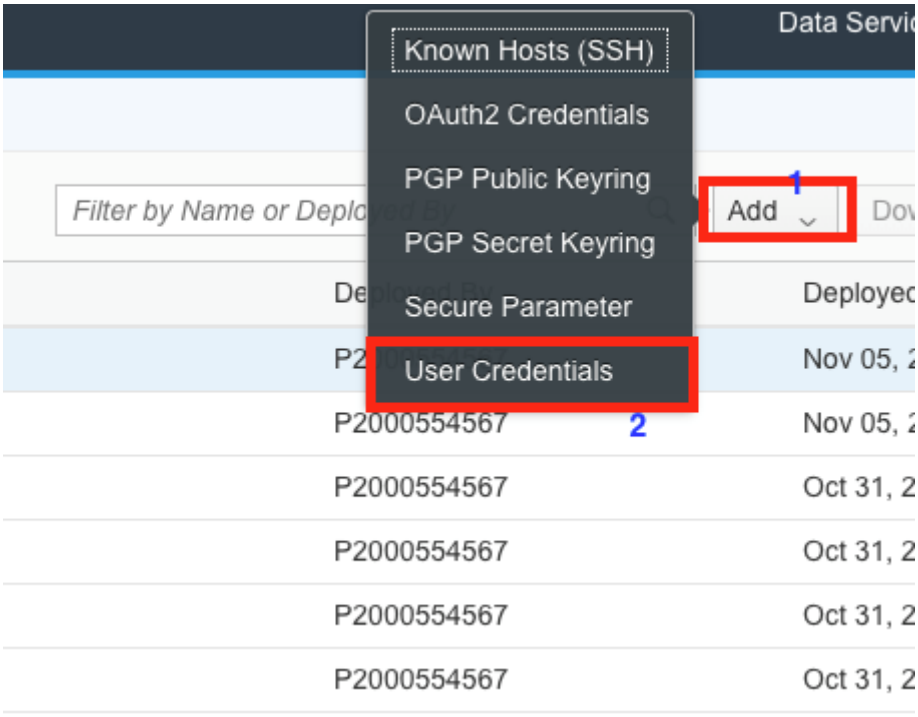
4.2 Deploying Certificates and Credentials to SAP Cloud Integration Tenants

Procedure

1. Open a ticket against LOD-HCI-PI-OPS at SAP Cloud Integration and ask the operation team to import the root certificate of the URL of the Transport Registration Web Service – NetLock Gold (Class Gold) Root Certificate. You can download the certificate from the website of NetLock at https://www.netlock.hu/index.cgi?ca=gold&lang=EN&tem=ANONYMOUS/kulcsjegyzok/adatok.tem and send the certificate that you have downloaded to SAP Cloud Integration.
2. Deploy the user name and secret signature key that you have got at registration from the tax authority (NAV) to your SAP Cloud Integration tenant.
   a. In your browser, go to the *Overview* tab and choose *Security Material*.



b. Choose *Add* on the right corner and choose *User Credentials*.



c. Enter the name, username and password, and deploy them.
   - Name: **`gshungarycredentials`**.
   - Username and password are the username and the secret signature key that are registered at NAV.

> **Note**
>
> The secret signature key consists of a password and a secret key which are separated by a space. For example, `zuhuTD L7fuxgg8Mb`.

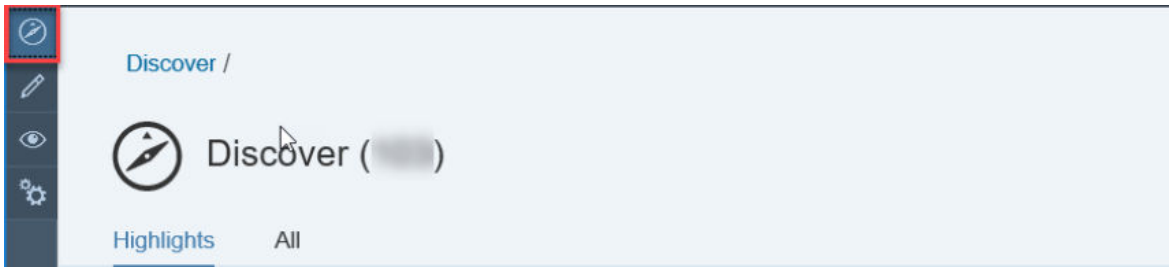
4.3 Copying Published Package

Context

You download the integration flow in the package *SAP Document and Reporting Compliance: Transport Registration for Hungary* to the target tenant as follows:

Procedure

1. In your browser, go to the WebUI of the tenant (URL: <Tenant URL>/itspaces/#shell/catalog).
2. Choose *Discover*.



3. Choose *SAP Document and Reporting Compliance: Transport Registration for Hungary* package.
4. Choose *Copy*.

4.4 Configuring Integration Flows

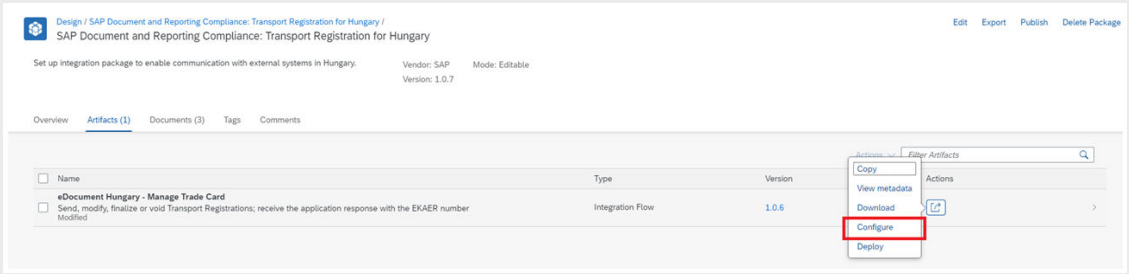
Context

You configure the package that you have copied as described in Copying Published Package [page 11].

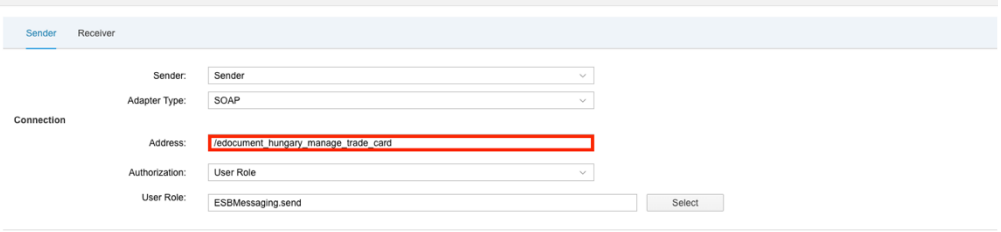
Procedure

1. Go to the integration package that was copied from the original *SAP Document and Reporting Compliance: Transport Registration for Hungary*.
2. Choose *Artifacts* tab.
3. Choose *Actions* that corresponds to integration flows *eDocument Hungary – Manage Trade Card*.
4. Choose *Configure* and maintain the following configuration parameters:

> **i Note**
>
> The version of the integration on the screenshot may differ from the current one.

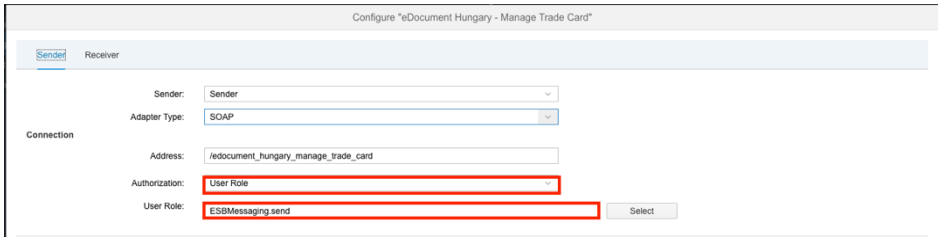


- *Sender* tab
  - Use the *Address* parameter if you would like to follow your own naming convention.

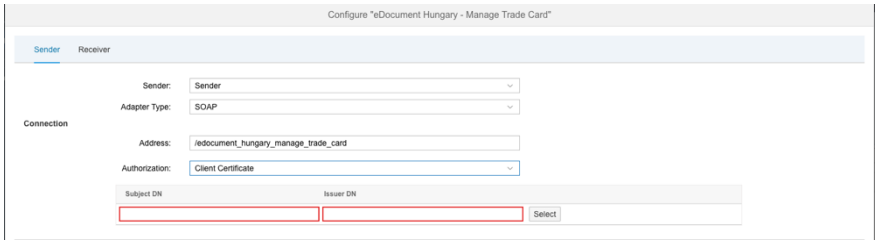


> **i Note**
>
> The connection address has to be unique within a tenant.

  - Select the required authorization (*User Role* or *Client Certificate*) that has been configured for the connection between your back-end system and the tenant:
    1. For *User Role* authorization, please select relevant user role. For example, `ESBMessaging.send`.



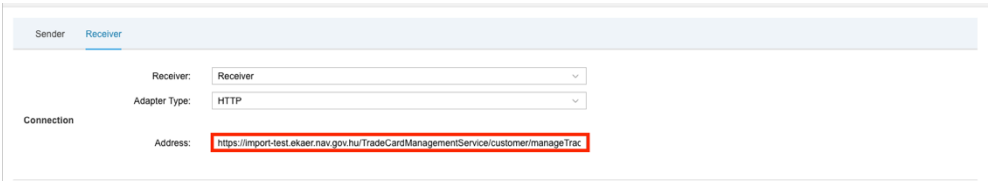
    2. For *Client Certificate* authorization, please provide certificate credentials.



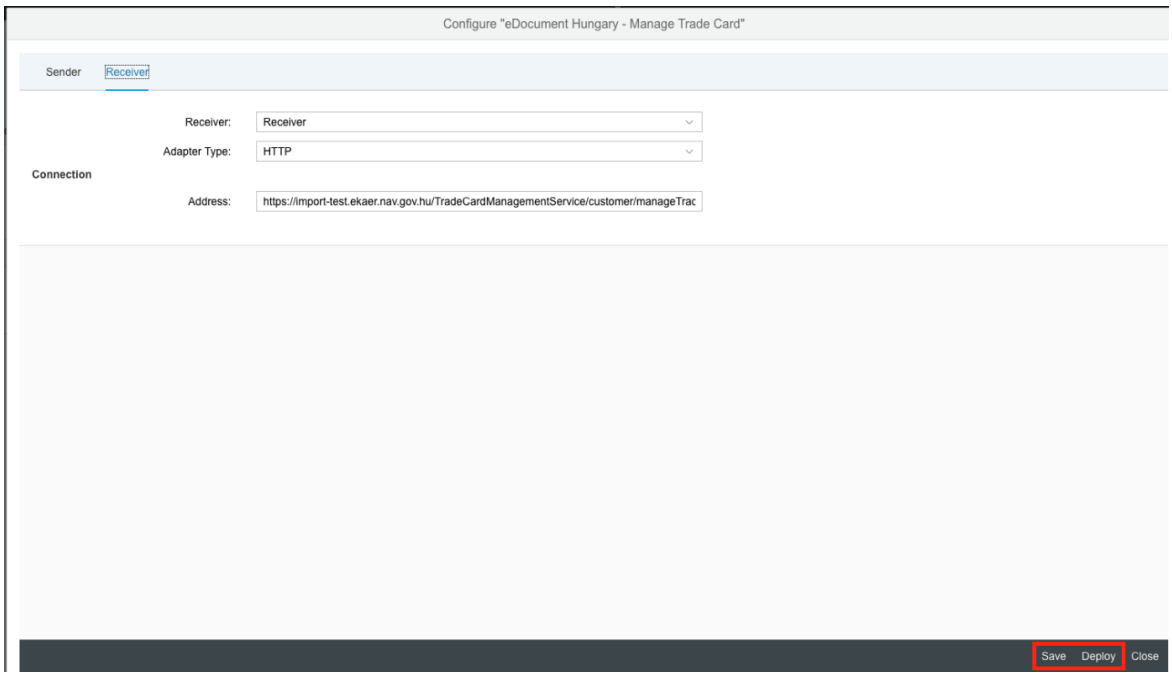
> ### Note
>
> The layout under this menu tab may differ from the screenshot provided.

- *Receiver* tab
  Maintain the receiver URL in the address field.

Environment	URL
Test	https://import-test.ekaer.nav.gov.hu/TradeCardManagementService/customer/manageTradeCards
Production	https://import.ekaer.nav.gov.hu/TradeCardManagementService/customer/manageTradeCards



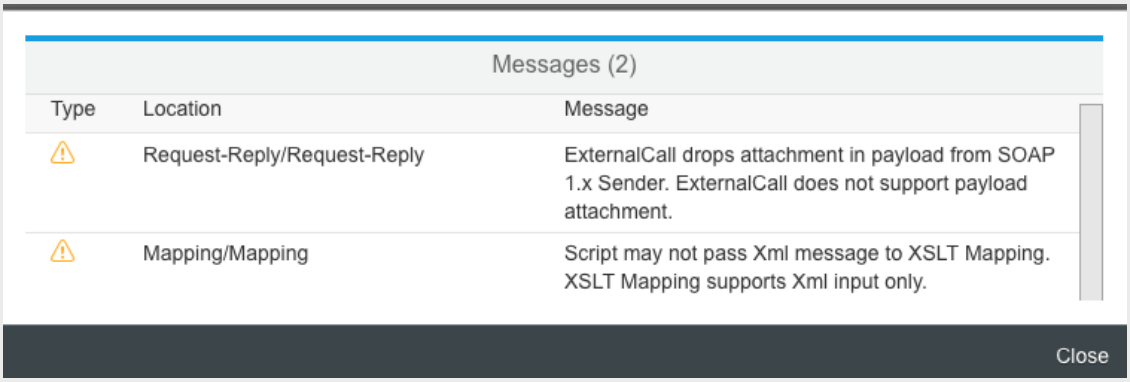
5. Choose *Save* and *Deploy* to deploy the integration flow actively to server.



A message will appear to inform the integration flow is deployed successfully.

Note

Probably some warning information will appear when you choose *Save*. Warning information like the following can be ignored.



5 Configuration Steps in Back-End Systems

The following sections tell you the necessary configuration you do in SAP back-end systems to connect with SAP Cloud Integration.

5.1 Creating Logical Ports in SOAMANAGER

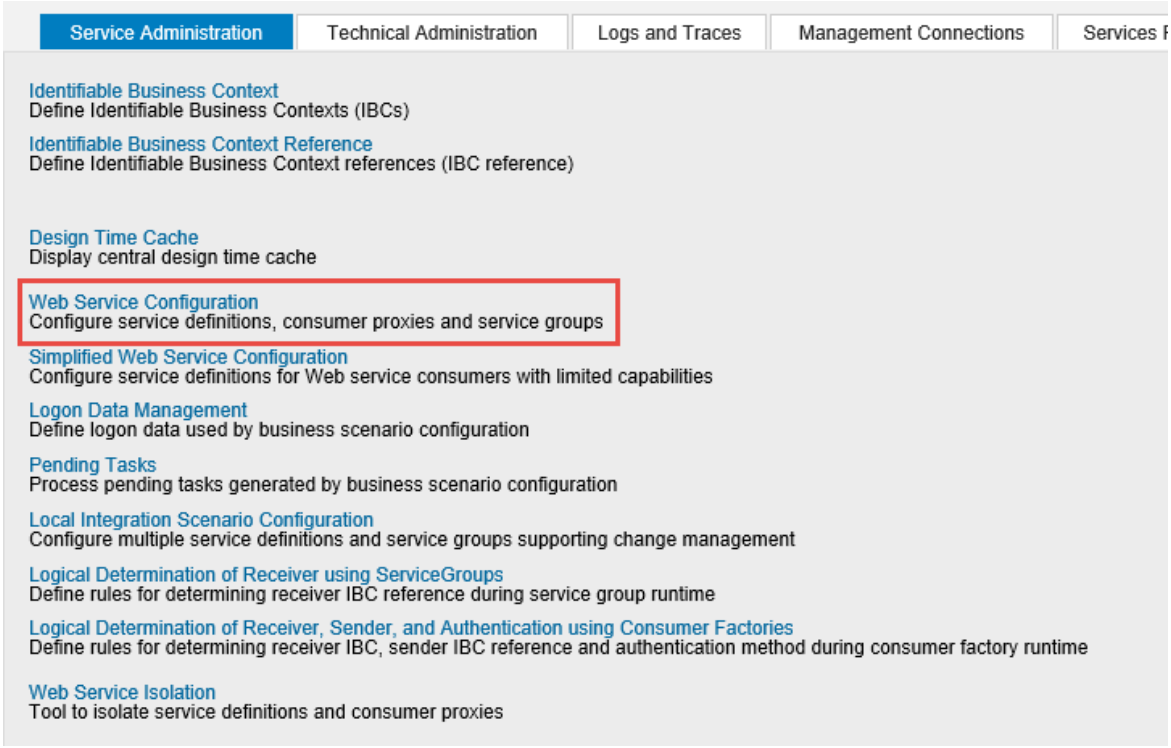
Context

The proxies have to be connected to the SAP Cloud Integration tenant via logical ports. In test SAP backend system, the logical ports are configured to connect to the test tenant. In the productive SAP backend system, the logical ports are configured to connect to the productive SAP Cloud Integration tenant.

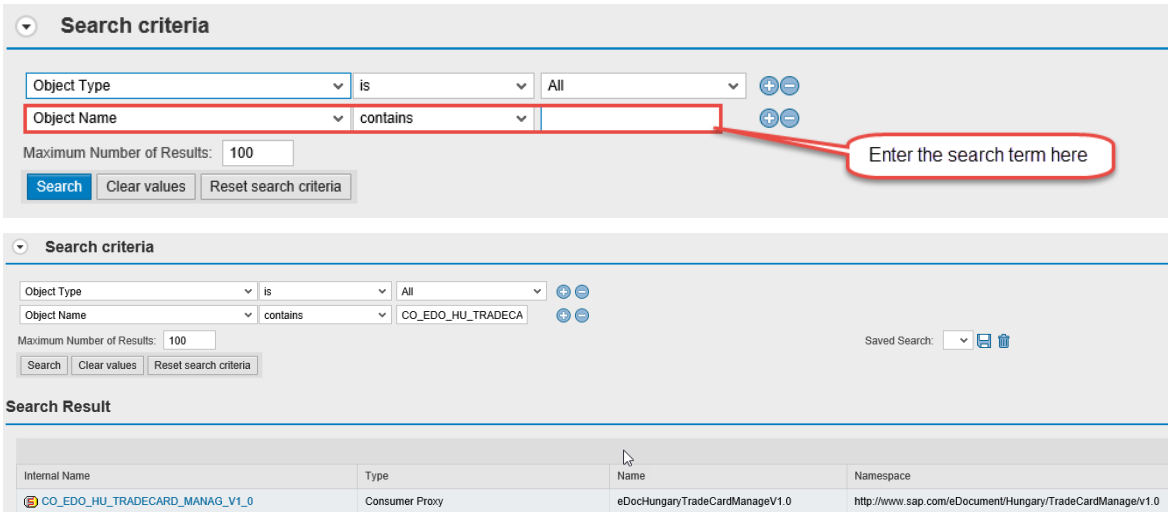
> **i** Note
>
> The screens in your system may differ from the screenshot below, depending on your release.

Procedure

1. In your SAP backend system, go to transaction `SOAMANAGER`.



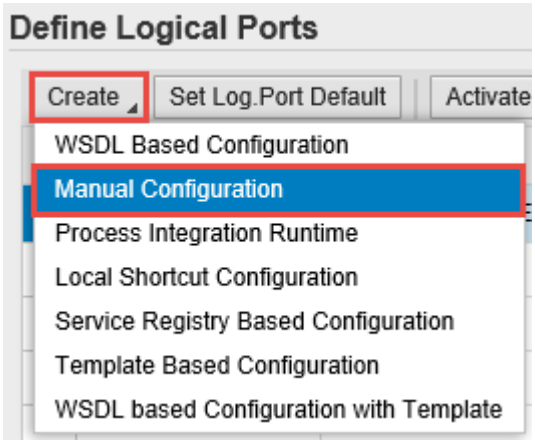
2. Select *Web Service Configuration* and find the proxies for Hungary Invoice Registration with search term **`CO_EDO_HU_TRADECARD*`**.



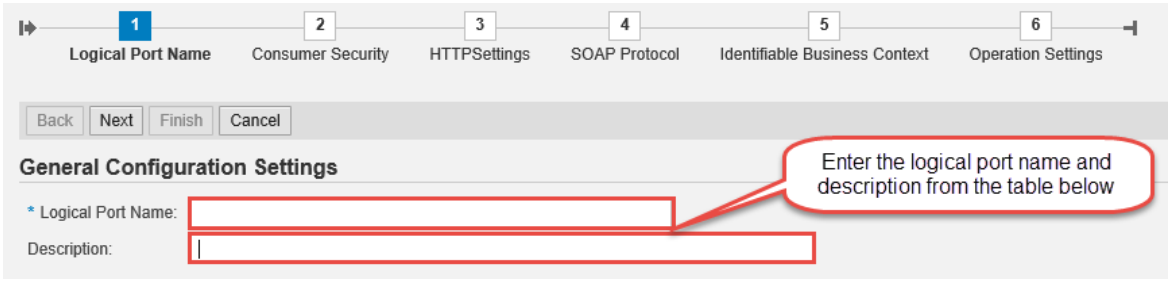
The following table lists the proxies and the logical port name, description and path for each proxy.

Proxy Name	Logical Port Name	Description	Path
CO_EDO_HU_TRADE-CARD_MANAG_V1_0	EDO_HU_MANAGE_TRADE-CARD_SERV_PORT	Hungary eDocument – Transport Registration Port	/cxf/edocu-ment_hungary_man-age_trade_card

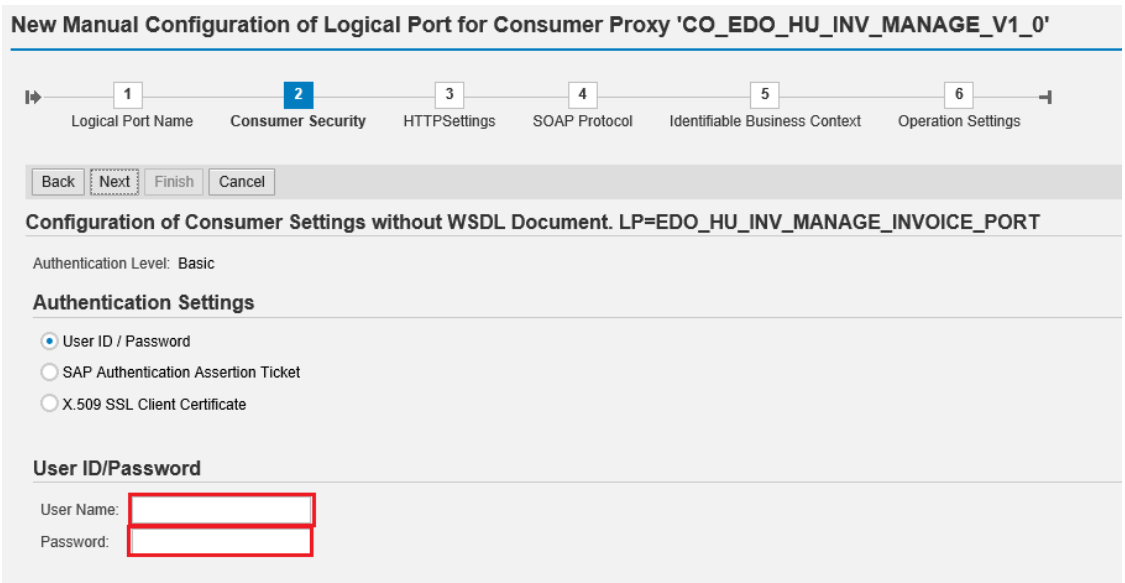
3. In the result list, select a proxy and create logical port(s) for each proxy. Choose *Create* > *Manual Configuration*.



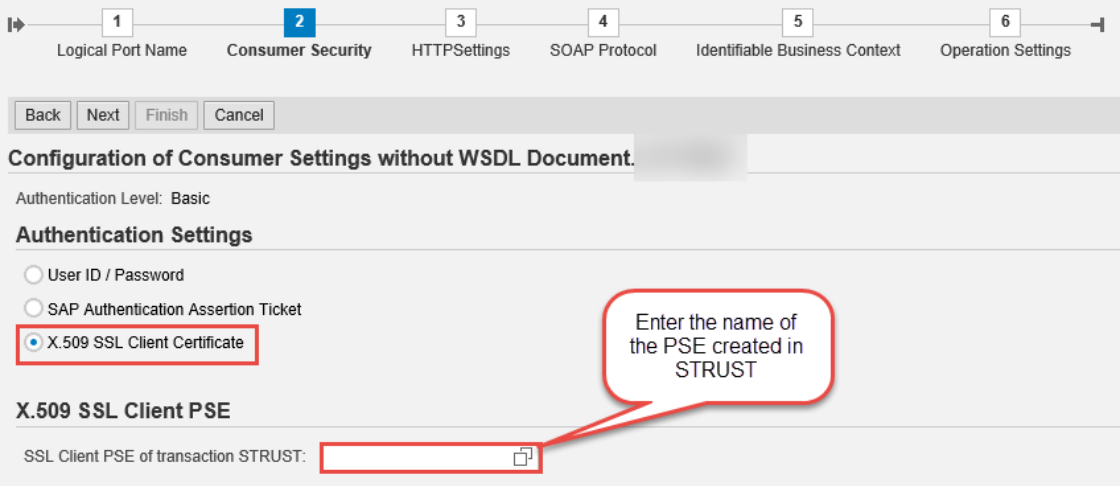
4. Enter logical port name and description.



5. The configuration you do in the *Consumer Security* tab in the *Configuration* screen depends on the security being used in the communication between the SAP back-end system and SAP Cloud Integration.
   - If you use basic authentication, select *User ID / Password* and enter user name and password.



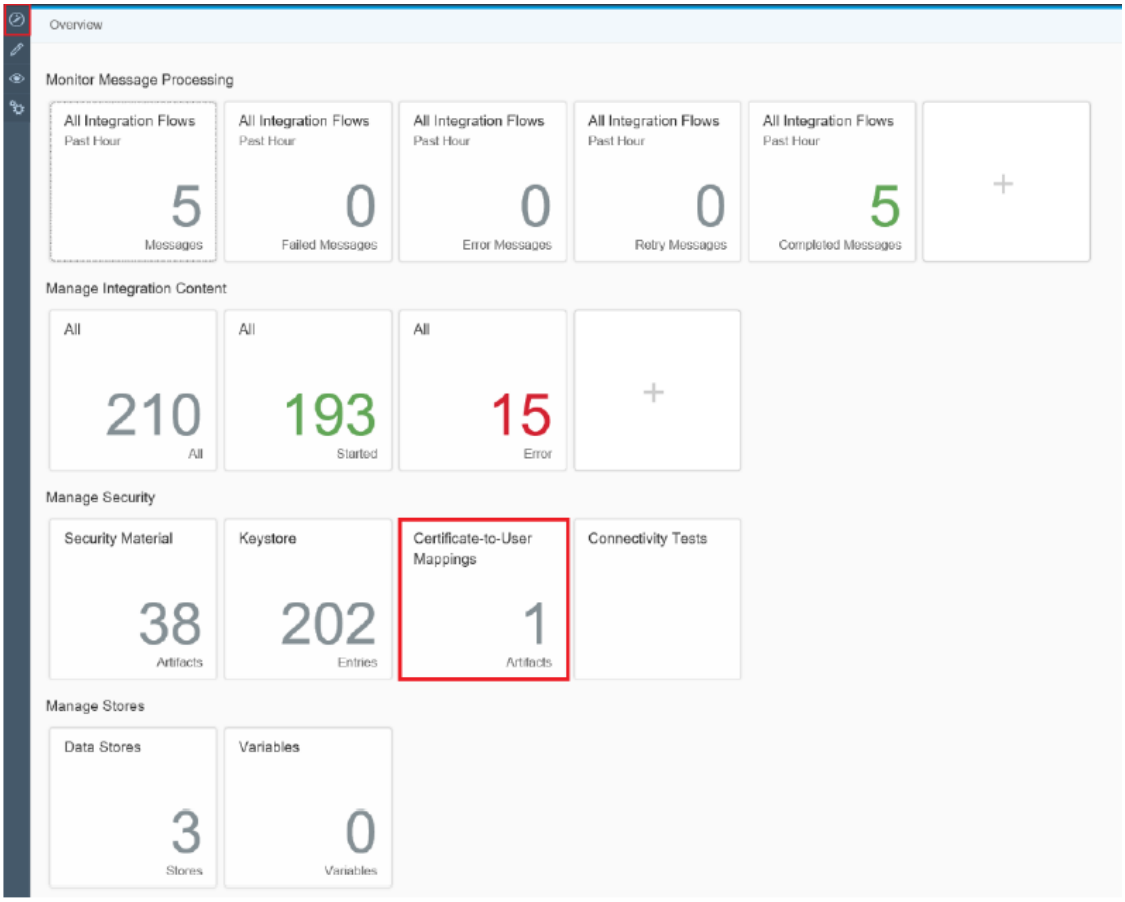
   - If you use certificate-based authentication, select *X.509 SSL Client Certificate* and ensure that the required certificates are available in transaction `STRUST`.



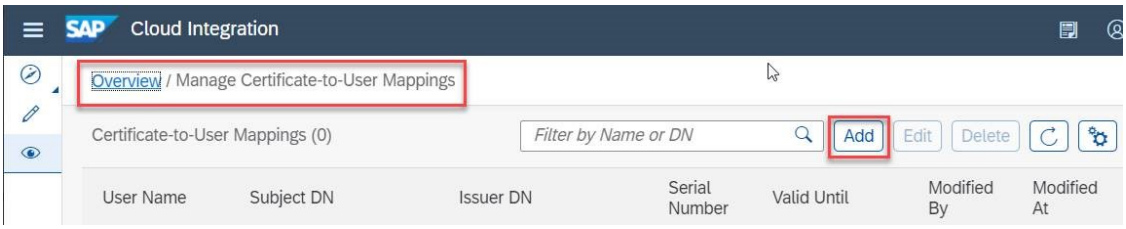
> ### i Note
>
> If you do not see this radio button or cannot select it, please refer to SAP Note 2368112 Outgoing HTTPS connection does not work in AS ABAP and SAP Note 510007 Setting up SSL on Application Server ABAP.

Additionally, if you have selected *User Role authorization* as describe in Sender tab, step 4 of Configuring Integration Flows [page 11], you need to map the certificate to a user of your tenant with the `ESBMessaging.send` role. Firstly, you need to export the certificate from transaction `STRUST`. Save it locally and upload it to SAP Cloud Integration, *Certificate-to-User Mappings*.

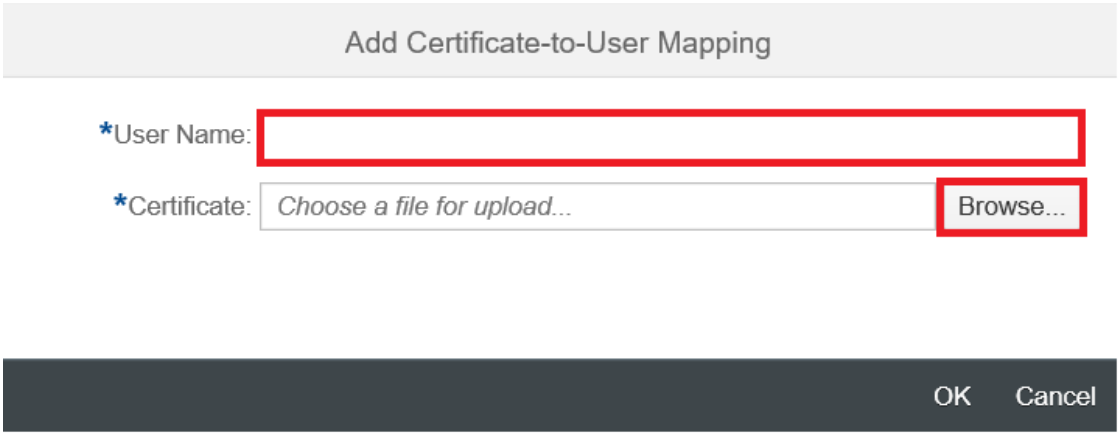
1. Export the SSL Client PSE of transaction `STRUST`.
2. Choose *OverviewCertificate-to-User Mappings*.



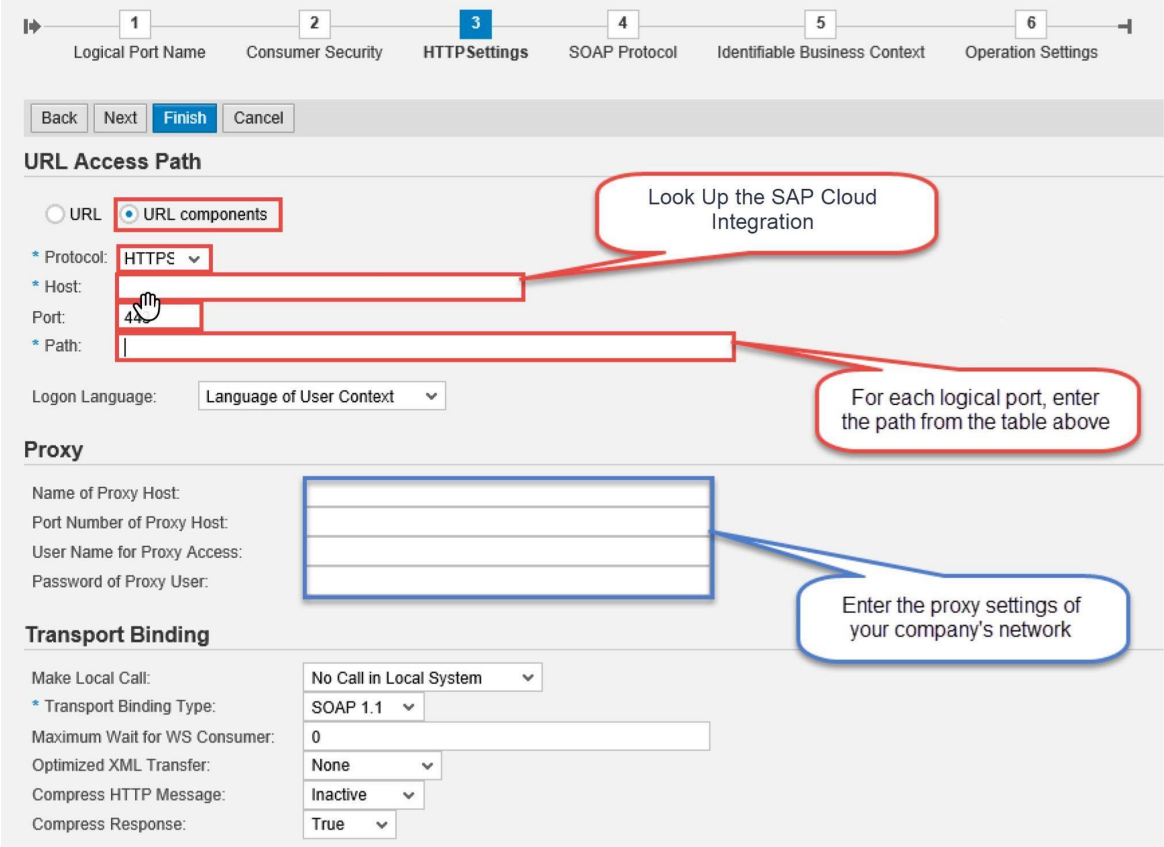
3. Choose *Add*.



4. Enter a user name with `ESBMessaging.send` role, upload the SSL Client PSE of transaction `STRUST` and choose *OK*.



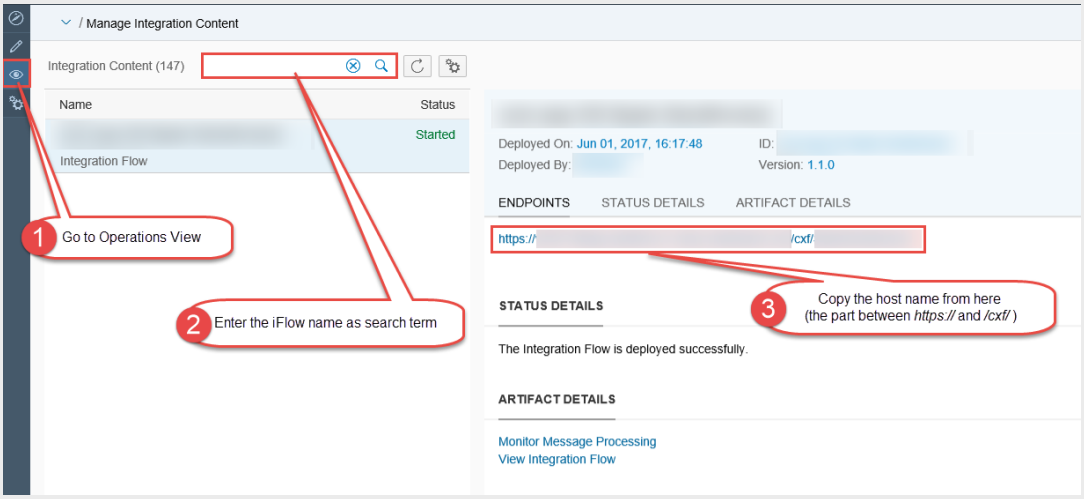
6. On *HTTP Settings* tab, make the following entries:



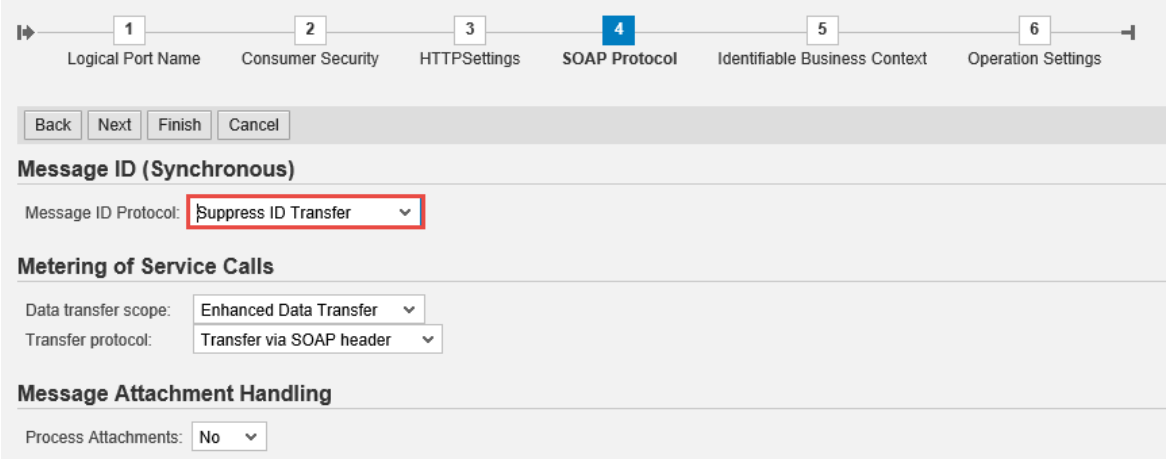
Note that the entries for the *Proxy* fields depend on your company's network settings. The proxy server is needed to enable the connection to the internet through the firewall.

> **i Note**
>
> 1. The screenshots may look slightly different in your system depending on the release, but all the required fields should be available.
> 2. Port 443 is the standard port for the HTTPS protocol.

3. To find the Host, go to SAP Cloud Integration Web UI and under *Managed Integration Content*, choose *Monitor* > *All*. Use search to find your integration flow as in the screenshot below:



7. On the SOAP Protocol tab page, set *Message ID Protocol* to *Suppress ID Transfer*.



8. No settings are required in the *Identifiable Business Context* tab, choose *Next*.
9. No settings are required in the *Operation Settings* tab, choose *Finish*.

> ### i Note
>
> To check if the connection works, choose *Ping Web Service*. If the connection works, the system will show the following result (HTTP 405 Service Ping ERROR: Method Not Allowed).
>
> You can set up a HTTP connection in the `SM59` transaction. Maintain a host and a port of SAP Cloud Integration service and execute a connection test. In case of a successful connection, you receive an error with HTTP return code 500
>
> Remember to create logical port(s) for each proxy.
>
> Execute the following steps in the SAP backend systems, see SAP Note 2636341 for more information.
>
> - Define SOA service names and assign the logical ports to the combination of a SOA service name and a company code in `EDOSOASERV` view.

- Assign the SOA service names that you have created before to an interface ID in `EDOINTV` view.

6 Test Steps for Communication

Context

To test the communication, the recommended practice is to create and send an electronic document from SAP back-end system. The steps depend on how the system is configured to generate and send electronic documents.

Procedure

1. Check if all the notes relevant to the solution for Hungary are installed and all the manual configuration steps were performed.
2. Create a relevant document for electronic document processing for Hungary (for example an Outbound Delivery).

   > **i Note**
   >
   > If the system is configured to generate an electronic document for the selected document type, an instance of the eDocument will be created as soon as the document is posted (for example when you post a Goods Issue for the delivery).

3. Go to the *eDocument Cockpit* by running the transaction `EDOC_COCKPIT`.
4. Enter the company code for the document that was posted. If necessary, enter additional selection parameters. When the selection is complete, run the report.

   > **i Note**
   >
   > Based on your selection, a list of electronic documents is displayed. Find the one that you have just created and check the following:
   >
   > - If the *eDocument GUID* field of your entry is yellow, the electronic document was created but not submitted yet. In this case, select it and choose *Submit* to trigger the communication with SAP Cloud Integration.
   > - If the *eDocument GUID* field is green, the communication with SAP Cloud Integration was triggered and was successful. You can double-check if the message went through on the SAP Cloud Integration tenant; or you can use a trace from transaction `SRT_UTIL` to look at the XMLs transmitted via web services from SAP back-end systems. Note that the trace must be activated before you start the `EDOC_COCKPIT` transaction.
   > - Double-click on the Interface *Message GUID* field to navigate to *AIF* and look at the log. Communication errors, if any, are displayed there.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering a SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP