Integration Guide | PUBLIC
2022-07-06

Switzerland eInvoice Integration Guide (SAP ERP, SAP S4HANA) Neo environment

THE BEST RUN SAP

Content

1 Disclaimer. 3

2 Introduction. 4

3 Prerequisites 5

4 Connectivity Steps. 6

4.1 Set Up a Secure Connection. 6

Retrieve and Save Public Certificates. 7

Upload the Certificates. 7

Authenticate Integration Flows. 8

4.2 Registration at the Service Provider. 9

Deploying Key Pairs, Certificates and Credentials. 9

5 Configuration Steps in SAP Integration Suite. 11

5.1 General Information 11

5.2 Copying Integration Flows. 12

5.3 Configuring Integration Flows. 12

Configuring Value Mappings. 14

6 Configuration Steps in Back-End Systems. 16

6.1 Creating Logical Ports in SOAMANAGER. 16

7 Testing the Integration. 23

1 Disclaimer

This documentation refers to links to Web sites that are not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

- The correctness of the external URLs is the responsibility of the host of the Web site. Please check the validity of the URLs on the corresponding Web sites.
- 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.

2 Introduction

You use SAP Integration Suite 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 Integration Suite tenant so that the integration between the systems works.

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

3 Prerequisites

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

1. You have installed in the test and productive systems all necessary SAP Notes for the Document and Reporting Compliance Solution.
2. You have set up your tenant as follows:
    - Document and Reporting Compliance: All relevant notes are installed in the test and/or productive systems.
    - SAP Cloud Integration test/productive tenants are live.
    - You have configured the connection from SAP back-end system to SAP Cloud Integration.

4 Connectivity Steps

4.1 Set Up a Secure Connection

You establish a trustworthy SSL connection to set up a connection between the SAP back-end systems and the SAP Integration Suite.

Inbound HTTP connections are not required for Switzerland. Outbound HTTP connections are required, and are supported with specific, public certificates.

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, see Operating and Monitoring Cloud Integration

> **i Note**
>
> If you encounter any issues in the information provided in the SAP Integration Suite 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.

4.1.1 Retrieve and Save Public Certificates

Context

Find and save the public certificates from your SAP Integration Suite 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. Use the tenant URL you created as defined in the prerequisites of this document. The URL has the following format: **`https://<tenant>.cfapps.<data center>.hana.ondemand.com`**, where <tenant> corresponds to the dynamic part and is unique for each subaccount and <data center> corresponds to the data center you are using.
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.

4.1.2 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 Integration Suite.

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.

4.1.3 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`).

4.2 Registration at the Service Provider

To send and receive invoices through the Exchange System of the service provider in Switzerland, new customers must register directly on their website.

4.2.1 Deploying Key Pairs, Certificates and Credentials

Context

When registration with the Exchange System (Service Provider) is successful, additional steps are required for communication security. This involves deploying the key pairs, certificates and the credentials to the SAP Integration Suite tenants.

Create Aliases and their Credentials

Context

Aliases (and their credentials) are required for each Biller ID within your test or productive tenant. The service provider supports two types of authentication (user name and password and certificate based). Create the alias for the key pair and user credentials according to the following naming convention: **`edoc_switzerland_<Biller Id>`***.

> **i** Note
>
> If the certificate-based authentication is not needed, the creation of the key pair can be skipped.

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. Use the tenant URL you created as defined in the prerequisites of this document. The URL has the following format: **`https://<tenant>.cfapps.<data center>.hana.ondemand.com`**, where <tenant> corresponds to the dynamic part and is unique for each subaccount and <data center> corresponds to the data center you are using.
4. Navigate to the *Manage Security* section, and choose *Security Material*.
5. Select *Create* and choose *User Credentials*:

Field	Entry
Name	**`Edoc_switzerland_<Biller Id>`**, where **`<Biller Id>`** is the company's Biller Id number
Type	Choose the type of user credentials.
User	Enter the user name provided by the service provider for a specific Biller Id.
Password	Enter the password for the user above.

6. Choose *Deploy* to save the changes.
7. Repeat the steps for each Biller Id alias.
8. Navigate to the *Manage Security* section, and choose *Keystore*.
9. Select *Add* and choose *Keypair*:

Field	Entry
Alias	**`Edoc_switzerland_<Biller Id>`**, where **`<Biller Id>`** is the company's Biller Id number
File	Choose the file with keypair in p12 format which is signed by CA authority that is trusted by the service provider
Password	Enter the password for the key pair.

10. Choose *Deploy* to save the changes.
11. Repeat the steps for each Biller Id alias.
12. Deploy the public certificates and the root certificates of the Exchange System in the keystore. You download them from the Exchange System website.

5 Configuration Steps in SAP Integration Suite

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

5.1 General Information

The package **SAP Document and Reporting Compliance: Electronic Invoice for Switzerland** contains the following integration flows:

Integration flows for eDocument for Switzerland

Integration Flow Name in WebUI	Project Name/Artifact Name
Switzerland Execute Ping	com.sap.GS.Switzerland.ExecutePing
Switzerland Get Status	com.sap.GS.Switzerland.GetStatus
Switzerland Receive Document	com.sap.GS.Switzerland.ReceiveDocument
Switzerland Receive Statuses	com.sap.GS.Switzerland.ReceiveStatuses
Switzerland Send Document	com.sap.GS.Switzerland.SendDocument

Value mappings for eDocument for Switzerland

Value Mapping Name in WebUI
Switzerland Biller Id
Switzerland Payer Id
Switzerland Payer id to Biller Id

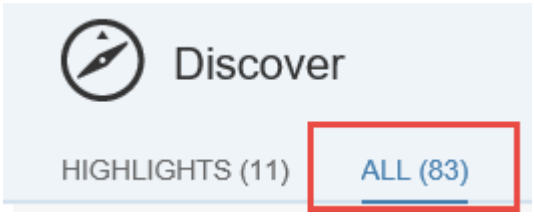
5.2 Copying Integration Flows

Context

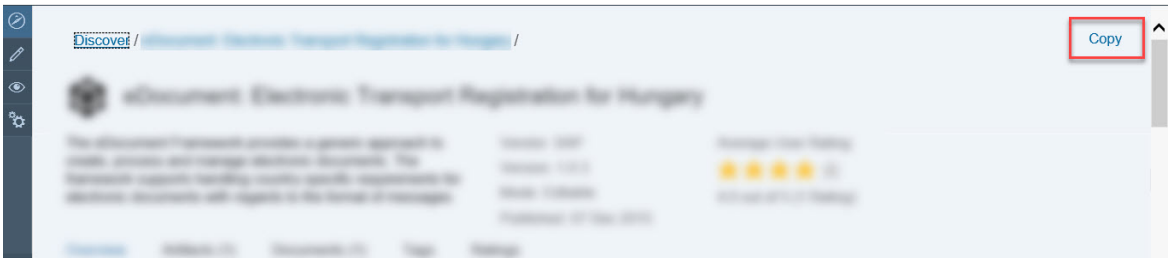
Copy all integration flows in the package SAP Document and Reporting Compliance: Electronic Invoicing for Switzerland to the target tenant as follows:

Procedure

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



3. Search for **SAP Document and Reporting Compliance: Electronic Invoicing for Switzerland**.
4. Select the Package and choose *Copy*.



5.3 Configuring Integration Flows

Context

You configure the package that you have copied as described in .

Procedure

1. There are 5 *Artifacts* in the integration package SAP Document and Reporting Compliance: Electronic Invoicing for Switzerland:
   - Switzerland Execute Ping
   - Switzerland Get Status
   - Switzerland Receive Document
   - Switzerland Receive Statuses
   - Switzerland Send Document
2. Choose *Actions* > *Configure* for the artifact you are configuring.

   > **i Note**
   >
   > Not all external parameters exist for each integration flow. Configure only the ones which are available.

3. Choose *Configure* > *More* tab (in some versions it may be *Externalized Parameters*)
   - Use the `Mode` parameter to set up the integration package usage mode:

Value	Description
TEST	To use the test system of the service provider.
PROD	To use the productive (that is, legally binding) system of the service provider.

   - Use the `Certificate_Authentication` parameter to configure whether you want invoices to be signed or not:

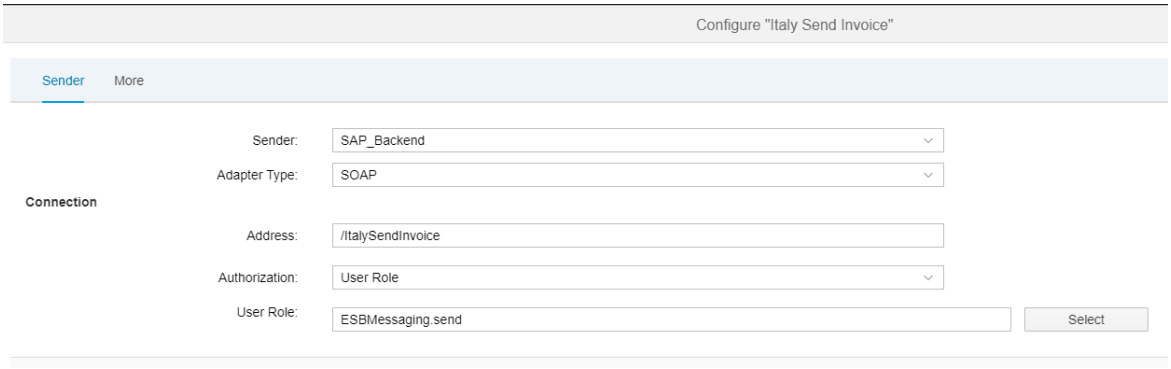
Value	Description
TRUE	The system signs the document using the key pair.
FALSE	The system send document using basic authentication type.

4. Choose *Configure* > *Sender* tab.
   - Use the `Address` parameter to set up the integration package address. Normally you don't have to change this field. In case you change the field, make sure to use the same address when configuring the logical ports in the next chapter.
   - Use the `Authorization` parameter to configure the authorization type.

Value	Description
User Role	You want to use basic authentication (user/password).

Value	Description
Client Certificate	You want to use client certificate authentication.

- Use the `User Role` parameter to configure the role based on which the inbound authorization is checked. Choose *Select* to get a list of all available roles.
  The role `ESBMessaging.send` is provided by default.



5. Choose *Save* and *Deploy* to deploy it actively to server. Note down the URLs of the endpoints for each service.

> **i Note**
>
> Depending on the version of your tenant, after pressing these buttons, a warning messages can appear. You can ignore these messages by choosing *Close*. The first two warnings are related to the payload attachments; currently the invoice registration process does not support or require message attachments (for example, scanned copies of invoices) in any stage of processing and communication.

5.3.1 Configuring Value Mappings

Context

There are 3 Value Mapping in the integration package SAP Document and Reporting Compliance: Electronic Invoice for Switzerland:

- Switzerland Biller Id
- Switzerland Payer Id
- Switzerland Payer Id to Biller Id

Procedure

1. Open *Switzerland Biller Id Value Mapping* artefact and click on *Edit* > *Add*.

Provide the list of all Biller Ids that will be used for communication in following format:

Id, name	Biller Id, name
1	Biller Id must comply with the format <12345678912345678>
2	Biller Id must comply with the format <12345678912345678>

> **i** Note
>
> Numeration of biller Ids should begin from number 1 and up to the number of billers used for communication.

2. Open *Switzerland Payer Id Value Mapping* artefact and click on *Edit* > *Add*.
3. Provide the list of all Payer Ids that will be used for communication in the same way as Biller Ids.
4. Open *Switzerland Switzerland Payer Id to Biller Id Value Mapping* artefact and click on *Edit* > *Add*.

   Provide the list of all Payer Ids related to Biller Ids in following format:

Payer Id, name	Biller Id, name
Payer Id must comply with the format <12345678912345678>	Biller Id must comply with the format <12345678912345678>
Payer Id must comply with the format <12345678912345678>	Biller Id must comply with the format <12345678912345678>

> **i** Note
>
> The list of entries should contain all Biller Ids and Payer Ids from two previous value mappings.

6 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 Integration Suite.

6.1 Creating Logical Ports in SOAMANAGER

Required step for configuring the Integration Package for eDocument and SAP Integration Suite.

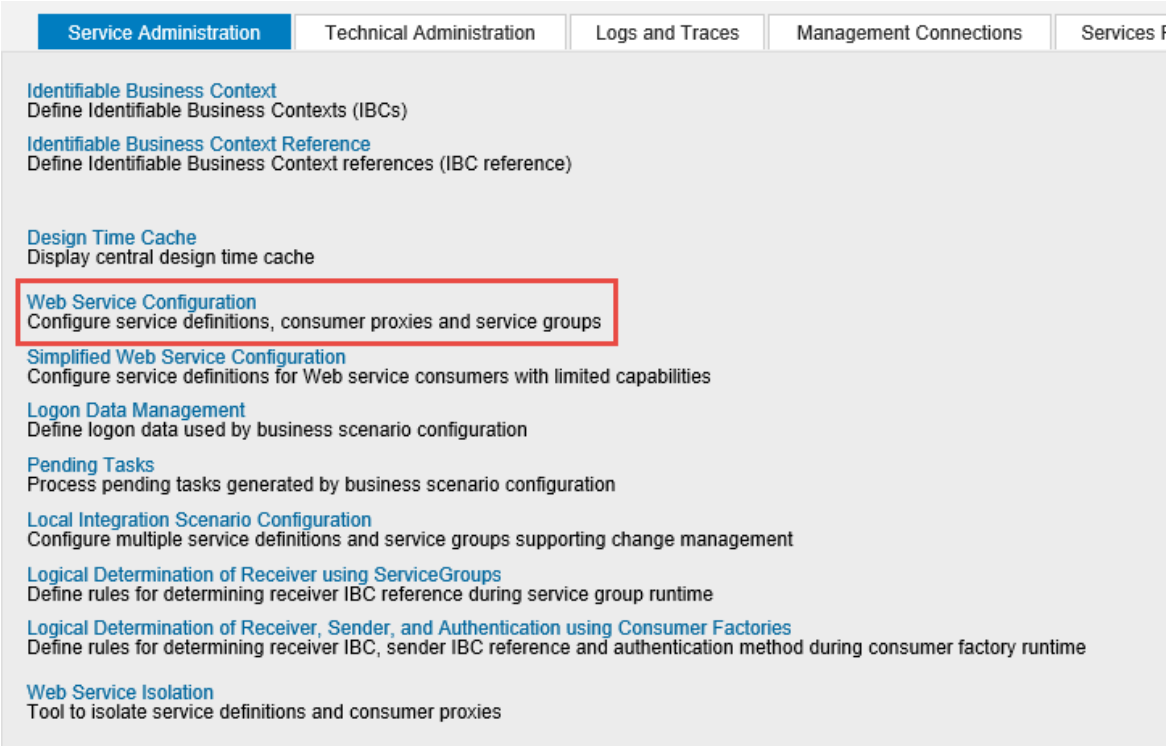
Context

You configure proxies that are needed to connect to the SAP Integration Suite tenant via logical ports. In test back-end systems, the logical ports are configured to connect to the test tenant. In productive back-end systems, the logical ports are configured to connect to the productive SAP Integration Suite tenant.

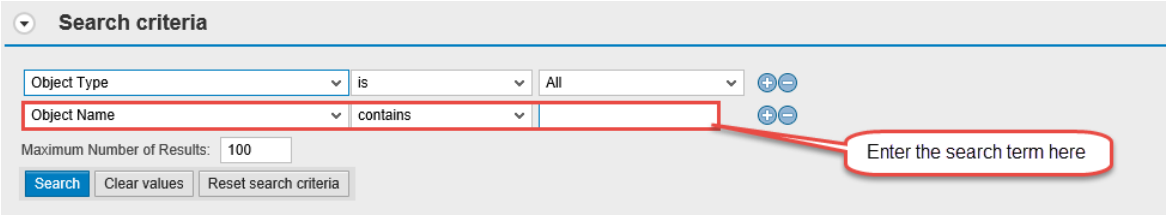
> **i** Note
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

Procedure

1. In your back-end system, go to the `SOAMANAGER` transaction and search for *Web Service Configuration* .



2. Find the proxies for *SAP Document and Reporting Compliance for Switzerland* with search term **`CO_EDO_CH*`**.



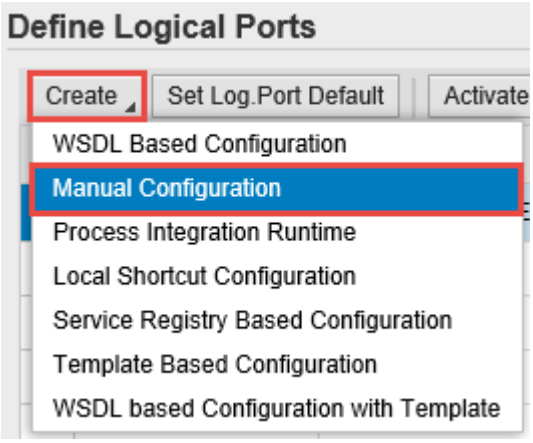
The following table lists the proxies and the logical port name, description and path for each proxy.

List of Proxies, Logical Port Names, and Paths

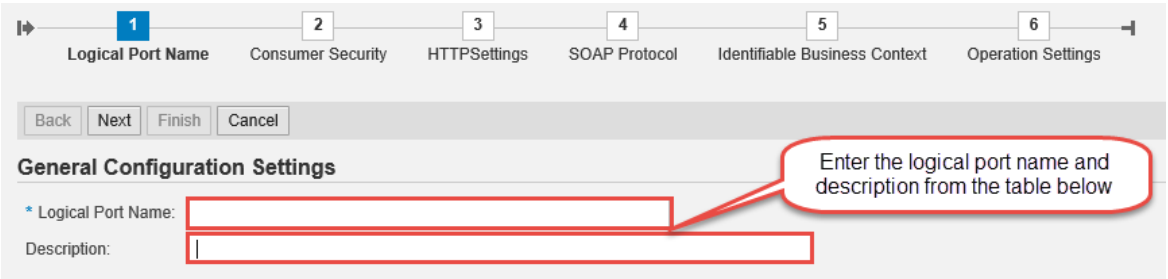
Proxy Name	Logical Port Name	Description	Path
CO_EDO_CH_GET_STATUS	EDO_CH_GET_STATUS	eDocument Switzerland – Get Status	/cxf/SwitzerlandGetStatus
CO_EDO_CH_GET_STATUS	EDO_CH_PULL_STATUS	eDocument Switzerland – Pull Status	/cxf/SwitzerlandPullStatus
CO_EDO_CH_GET_STATUS	EDO_CH_DELETE_STATUS	eDocument Switzerland – Delete Status	/cxf/SwitzerlandDeleteStatus
CO_EDO_CH_INVOICE_TRANS_SERV	EDO_CH_SEND_INVOICE	eDocument Switzerland – Send Invoice	/cxf/SwitzerlandSendDocument

Proxy Name	Logical Port Name	Description	Path
CO_EDO_CH_RECEIVE_IN-VOICE	EDO_CH_RECEIVE_IN-VOICE	eDocument Switzerland – Receive Invoice	/cxf/SwitzerlandPullDocu-ment
CO_EDO_CH_RECEIVE_IN-VOICE	EDO_CH_DELETE_INVOICE	eDocument Switzerland – Delete Invoice	/cxf/SwitzerlandDeleteDo-cument

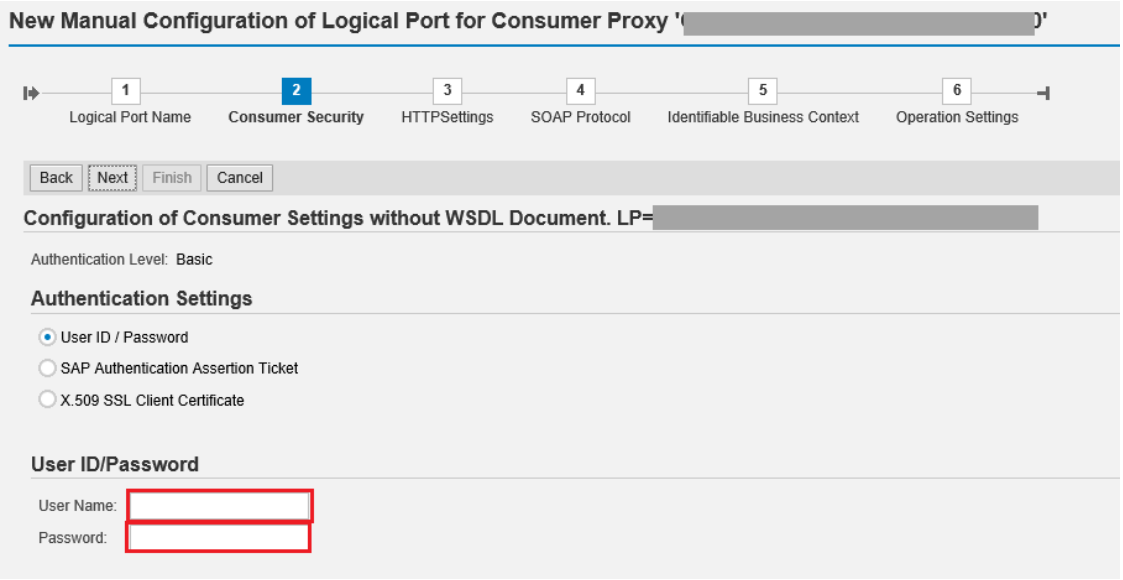
3. In the *Result List*, select a proxy and create a logical port for each proxy. Choose *Create* > *Manual Configuration*.



4. Enter the logical port name and a 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.
   a. If you use the basic authentication, select the *User ID / Password* and enter *User Name* and *Password*.



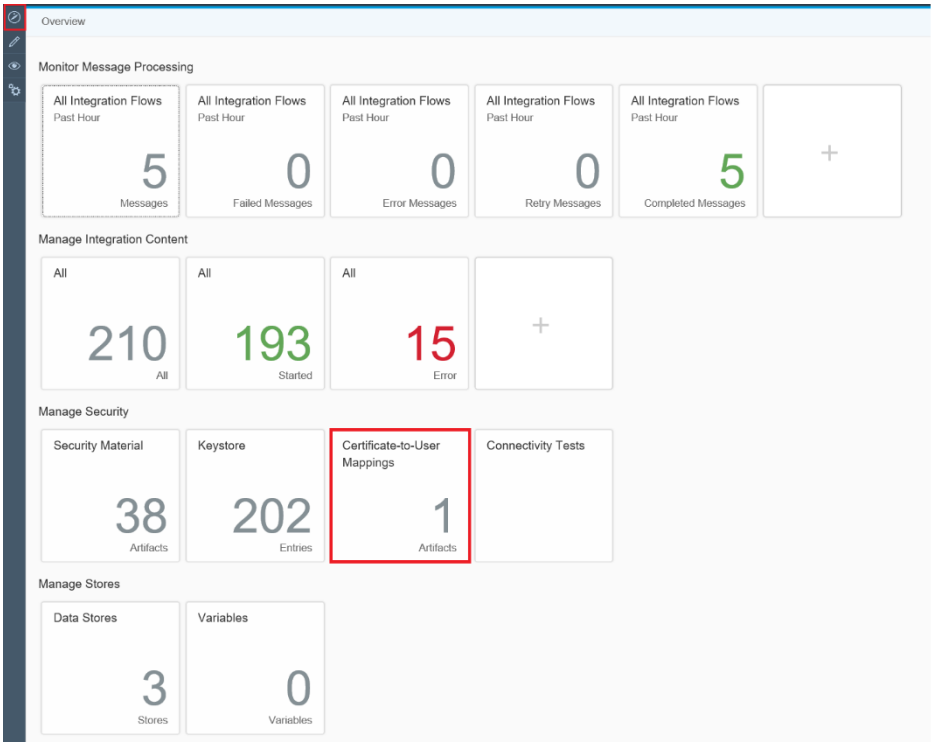
b. If you use certificate-based authentication, select *X.509 SSL Client Certification*. Ensure that the required certificates are available in the `STRUST` transaction.

   Note: If you do not see this option or cannot select it, check the SAP Notes 2368112 and 510007

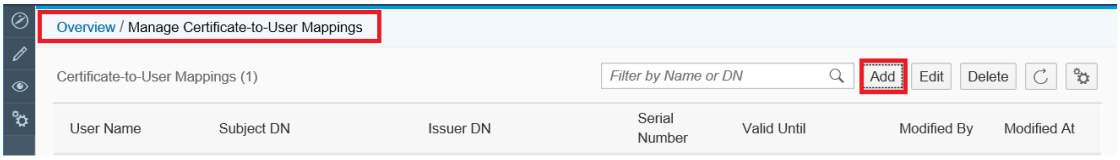
   Additionally, you map the certificate to a user of your tenant with the `ESBMessaging.send` role. First, you export the certifcate from the `STRUST` transaction. Save it locally and upload it to SAP Cloud Integration in the `Certificate-to-User Mappings`

a. Export the SSL Client PSE of the `STRUST` transaction.

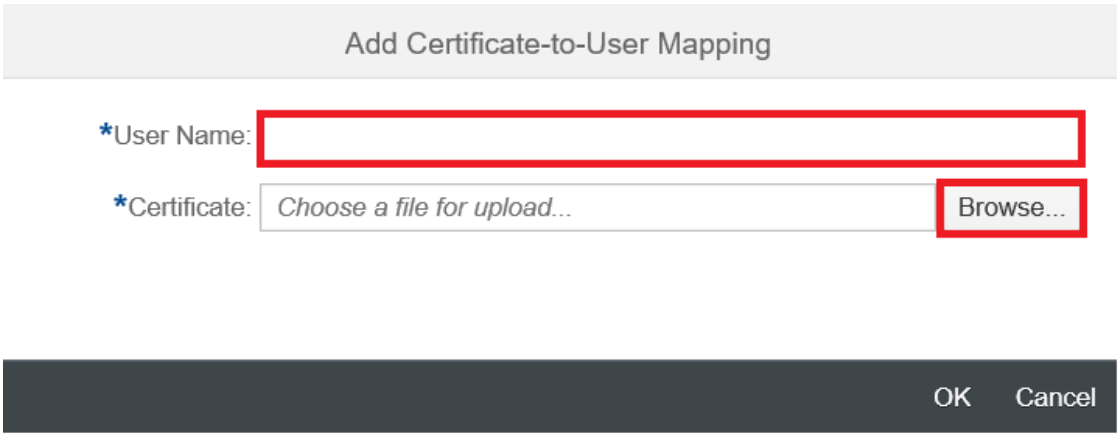
b. Got to SAP Cloud Integration under *Overview* > *Certificate-to-User Mappings*



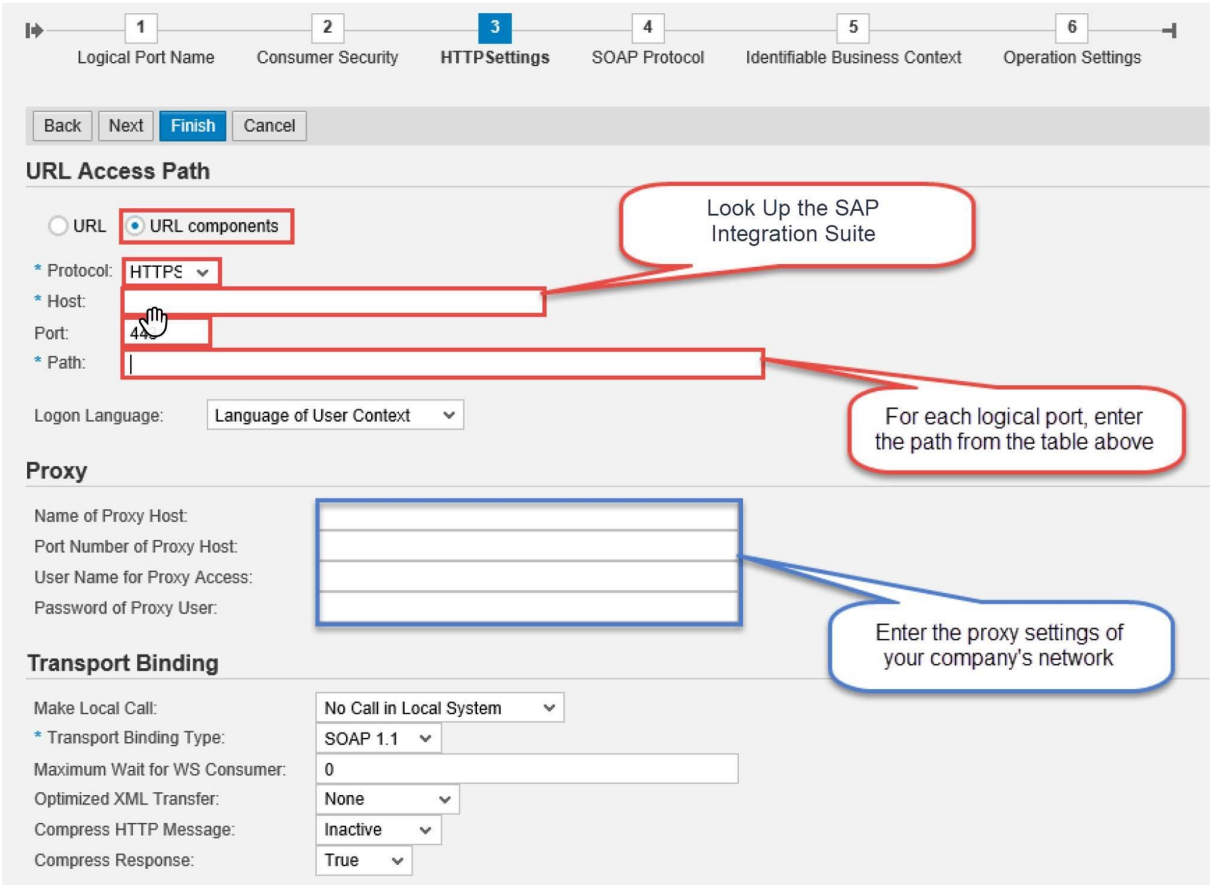
a. Choose *Add*.



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

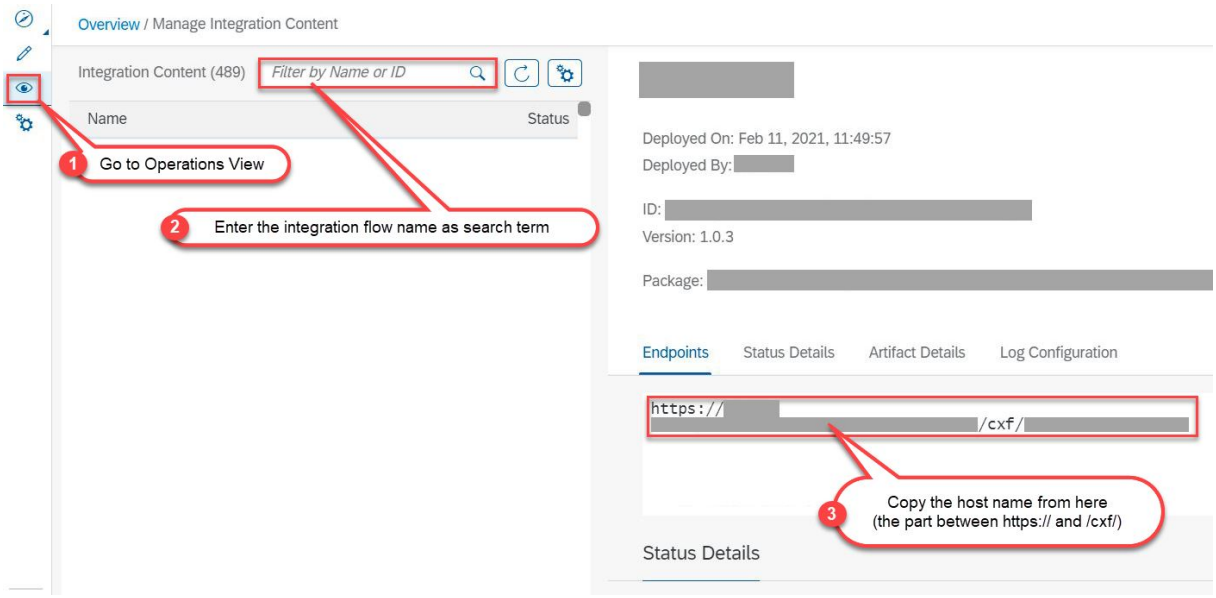


6. On the *HTTP Settings* tab, make the following entries:



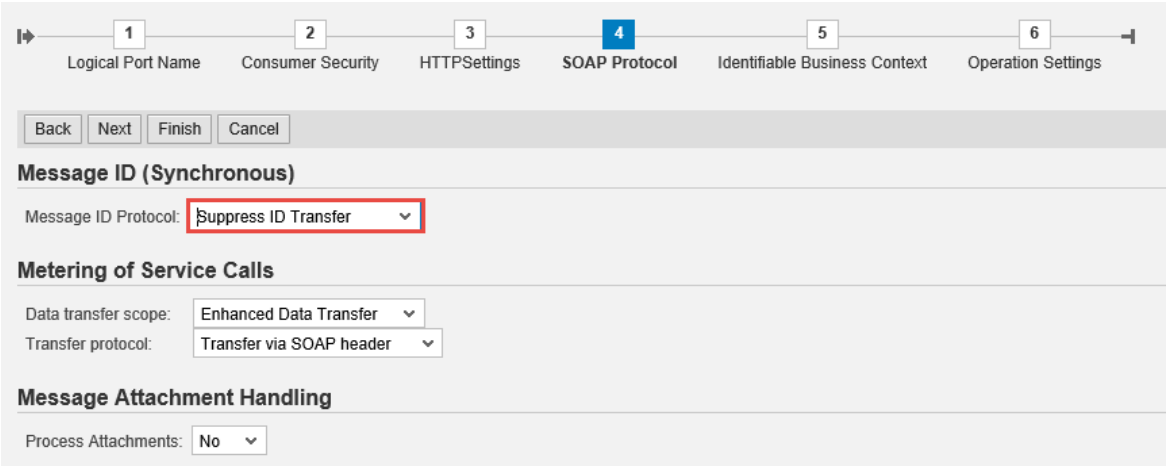
Port 443 is the standard port for the HTTPS protocol.

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



> ### i Note
>
> 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.

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



8. No settings are required in the *Identifiable Business Context* and *Operation Settings* tabs. Just select *Next* > *Finish*.

   SAP Integration Suite does not support WebService Ping for testing your configuration.

   You can set up a HTTP connection in the `SM59` transaction. Maintain a host and a port of SAP Integration Suite service and execute a connection test. In case of a successful connection, you receive an error with HTTP return code 500.

9. Remember to create logical port(s) for each proxy and to execute the following steps in the back-end systems, see SAP Note 2683318 for more information.

- Define the 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 you created before to an interface ID in `EDOINTV` view.

7 Testing the Integration

Describes the steps to test the integration of SAP Document and Reporting Compliance (eDocument) with the integration scenario from SAP Integration Suite.

Context

The best way to test if the integration works is to create and submit an eDocument from SAP backend system and see if that reaches the destination system, typically the service provider's system.

Procedure

1. In the back-end system, go to the *eDocument Cockpit* (EDOC_COCKPIT) transaction, in the relevant process.
2. Select an eDocument and check the status of the eDocument in the Cockpit and perform the following actions, accordingly:
    - If the status of the eDocument is `Created`, the eDocument was created but not submitted yet. In this case, select it and choose *Submit*. This action triggers the creation of the XML and the subsequent communication with SAP Integration Suite.
    - If the status is green or yellow, but not `Created`, the communication with SAP Integration Suite was triggered and was probably successful. You can double-check if the message went through on the SAP Integration Suite tenant. Alternatively, you can use a trace from the `SRT_UTIL` transaction to look at the XMLs transmitted via web services from the SAP back-end systems.
    - If the status is red, an error happened during the submission of the eDocument. Select the *Interface Field* to be directed to the SAP Application Interface Platform where you can check the log. Any communication errors 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