User Guide | PUBLIC
2022-03-18

Spain Electronic Invoicing: Setting Up SAP Cloud Integration (SAP ERP, SAP S4HANA)- Neo environment

THE BEST RUN SAP

Content

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 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.

3 Prerequisites

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

1. Document and Reporting Compliance: All relevant notes are installed in the test and/or productive systems.
2. SAP Cloud Integration test/productive tenants are live.
3. You have configured the connection from SAP back-end system to SAP Cloud Integration.

3.1 Installation of eDocuments Solution for Spain Electronic Invoicing

You must install and configure the SAP Document and Reporting Compliance solution for Spain Electronic Invoicing of Public Entities in your test and productive systems. If you did not install the latest support package for your system, see the SAP Note 2070409 (for SAP ERP) or SAP Note 2735302 (for SAP S/4HANA) for the list of SAP Notes to be installed. For generic information about the installation of the eDocument Framework, refer to the SAP Note 2134248 (for SAP ERP) or SAP Note 2343822 (for SAP S/4HANA) for the installation guide of SAP Notes.

Application Help for eDocument

For more information about features and country availability of each solution, see the application help in the product page for eDocuments. https://help.sap.com/viewer/p/SAP_E_DOCUMENT. To find the latest published documentation for eDocument for your country, follow the steps below:

1. Choose from *Version* the release you are interested in.
2. To get to the documentation for a given country, under *Application Help* choose *View All* and select your country.

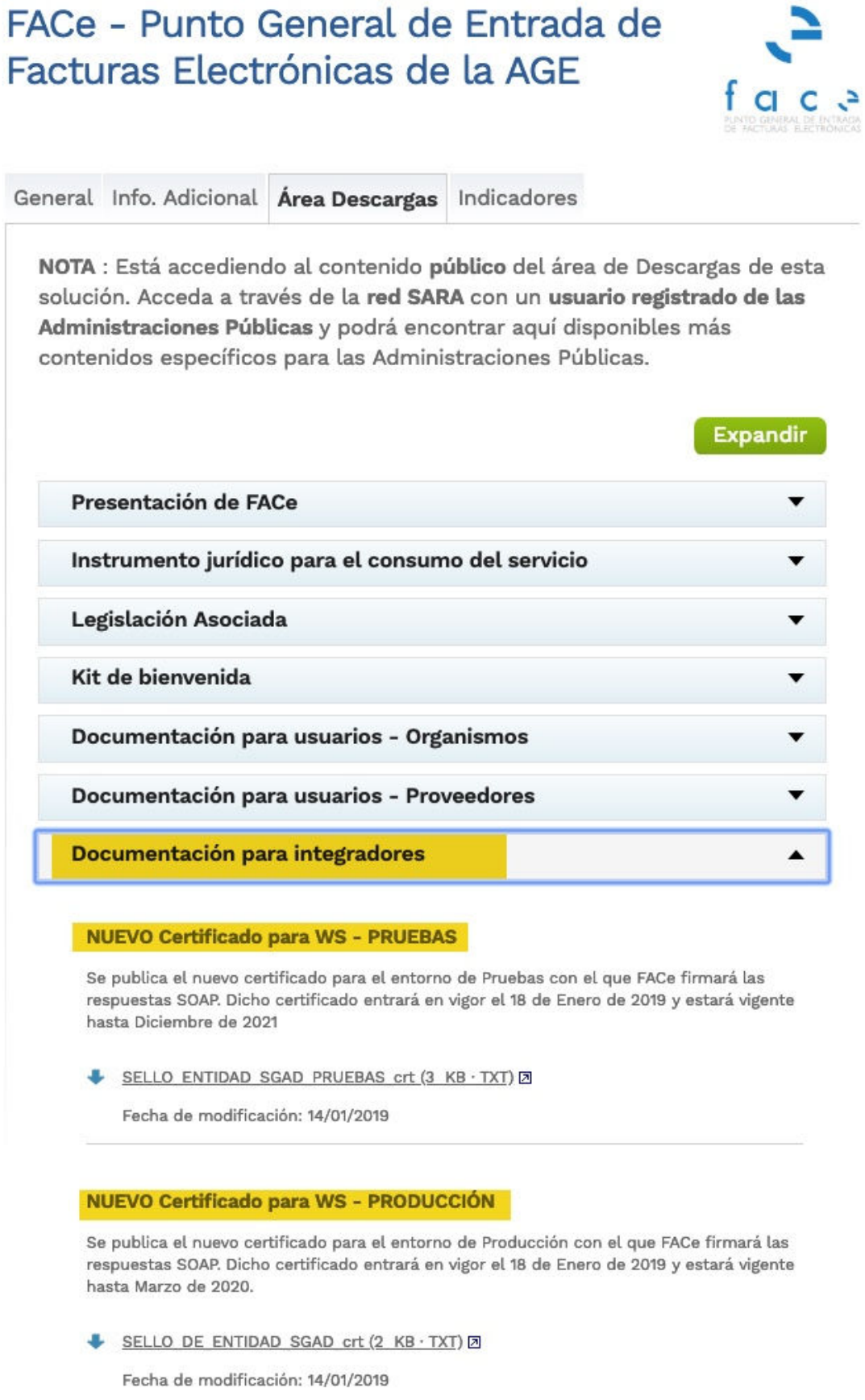
3.2 Registration at FACe

You must complete the registration at the General Point of Entry of Electronic Invoices of the General State Administration (FACe) and the following data must be available:

- Certificate used for digital signature (private key and password)

- Public certificate to verify the SOAP response deployed on SAP Cloud Integration tenant's keystore. Follow the steps below to generate the public certificate:
    1. Download the appropriate certificate from the FACe Portal.
       At the time of publishing this document, the relevant link is http://administracionelectronica.gob.es/ctt/face/descargas#.VOsMYvmG-4I

2. Search for the certificate NUEVO Certificado para WS as shown in the example below:



> **i Note**
>
> The screenshot is from June, 2020. SAP cannot guarantee that the layout of the page and the name of the certificate remain constant. SAP is not responsible for the content of external web pages.

3. Copy the content of the certificate into a text file and save it with **.cer** extension.

> **i Note**
>
> The screenshot is from June, 2020. SAP cannot guarantee that the layout of the page and the name of the certificate remain constant. SAP is not responsible for the content of external web pages.

- Public certificate "*.redsara.es" to communicate with FACe.
  These certificates can be obtained from the respective contacts from FACe.

4 Connectivity Steps

4.1 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 11].

4.1.1 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.

4.1.2 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.

4.1.3 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.

4.1.4 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`).

5 Configuration Steps in SAP Cloud Integration

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

5.1 General Information

The package *SAP Document and Reporting Compliance: Electronic Invoicing of Public Entities for Spain* contains the following integration flows:

Integration Flows for Spain Electronic Invoicing

Integration Flow Name in WebUI	Project Name/Artifact Name
Spain Electronic Invoicing of Public Entities - Send Invoice	com.sap.GS.Spain.SendInvoice
Spain Electronic Invoicing of Public Entities - Get Status	com.sap.GS.Spain.GetStatus
Spain Electronic Invoicing of Public Entities - Cancel Invoice	com.sap.GS.Spain.CancelInvoice

5.2 Deploy Certificates and Credentials

You deploy the certificates and the credentials to the SAP Cloud Integration tenants.

1. Deploy the certificate (as private key with alias) in the tenants JAVA_KEYSTORE.
   To allow the integration flows to be updated with minimal adaptation effort, use the following alias for the private key:
   Private key alias: **spainsignaturekey**

   > **i** Note
   >
   > - If you deploy the private key with another alias, you must configure the alias name in the integration flow parameters. For information about how to configure the alias name, see Configure and Deploy Integration Flows [page 15].
   > - From version 1.1.8 onwards, the dynamic private key *Alias* is available, that is, you can choose to use an alias in the form of **`spainsignaturekey_xxxxx`**, where **`spainsignaturekey`** will be the suffix, and **`xxxxx`** will be you company tax ID. If you choose to use the dynamic private key *Alias*, the system will concatenate the suffix and will extract your company tax ID from the header of the XML document.

2. Deploy the public certificate that you generated in the Registration at FACe [page 5] section into the tenants JAVA_KEYSTORE. Deploy the public certificate for staging in the TEST tenants JAVA_KEYSTORE and the public certificate for production in the PRODUCTION tenants JAVA_KEYSTORE.

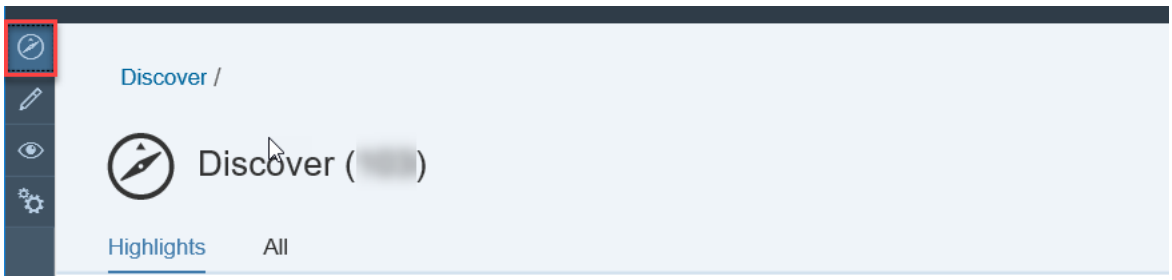
5.3 Copy Published Package

Context

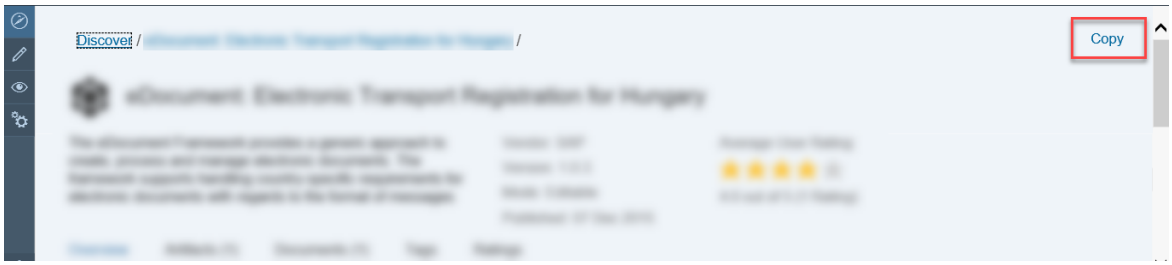
Copy all integration flows in the package *SAP Document and Reporting Compliance: Electronic Invoicing of Public Entities for Spain* to the target tenant as follows:

Procedure

1. In your browser, go to the WebUI of the tenant (URL: <Tenant URL>/itspaces/#shell/catalog).
2. In the *Discover* section of your tenant, select the package *SAP Document and Reporting Compliance: Electronic Invoicing of Public Entities for Spain*.



3. Select the package and choose *Copy*.



5.4 Configure and Deploy Integration Flows

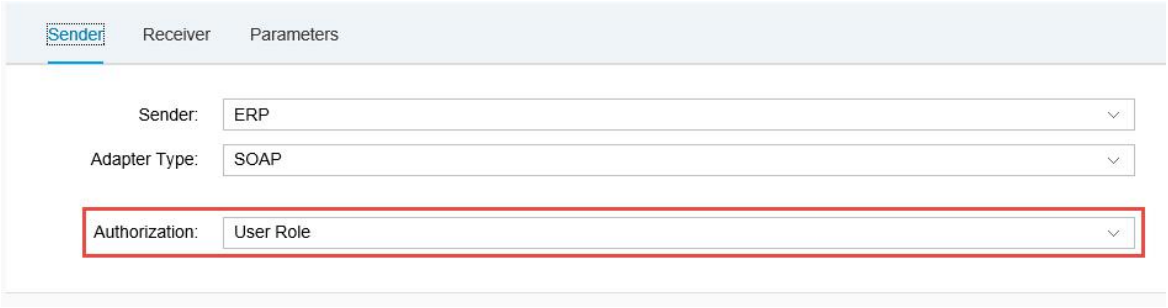
Context

You configure the package that you have copied as described in Copy Published Package [page 14]. For each integration flow, you must maintain several parameters as described below.

Procedure

1. Choose *Design* from the upper left corner of the page.
2. Click on the *SAP Document and Reporting Compliance: Electronic Invoicing of Public Entities for Spain* package.
3. Go to the *Artifacts* tab page.
4. Choose *Actions* > *Configure* for the artifact you are configuring.
5. Choose the *Sender* tab and make settings as follows:
   - *Authorization* field: Select `User Role` or `Client Certificate`
   - *Client Certificate* only: Upload your client certificates. *Subject DN* and *Issuer DN* are filled from the certificate information.

   See the following example:

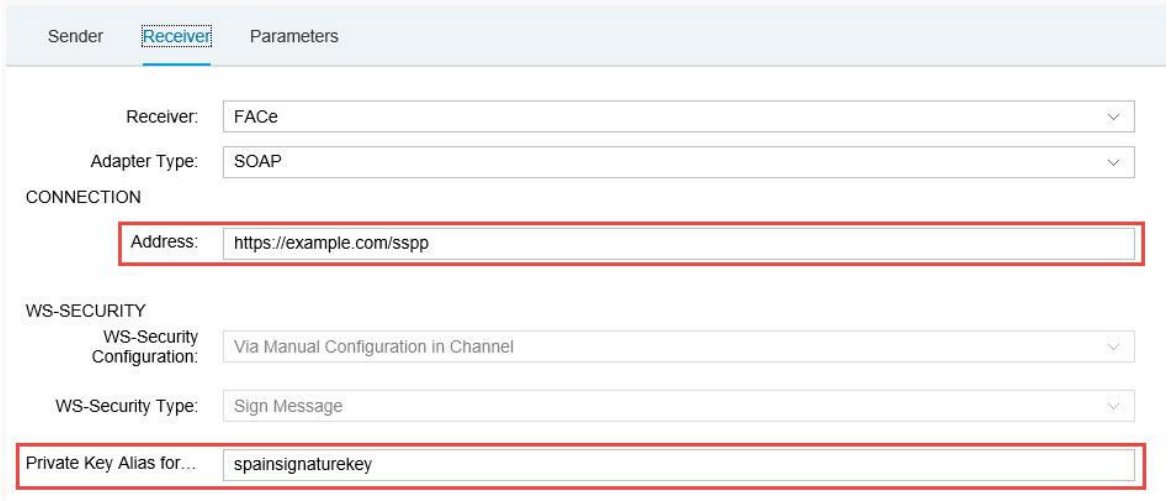


6. Choose the *Receiver* tab and make settings as follows:
   - Maintain the receiver URL in the *Address* field:

Environment	URL
TEST	https://se-face-webservice.redsara.es/facturasspp
PRODUCTION	https://webservice.face.gob.es/facturasspp

   - *Private Key Alias for Signing* field: The default alias for the private key is `spainsignaturekey`. If you deployed the private key with a different alias, defint it here.

See the following example:



7. Choose the *Parameters* tab and make settings as follows:

> **i Note**
>
> The integration flows *Get Status* and *Cancel Invoice* do not have the *Parameters* tab page. You make the settings in this step only for the *Send Invoice* integration flow.

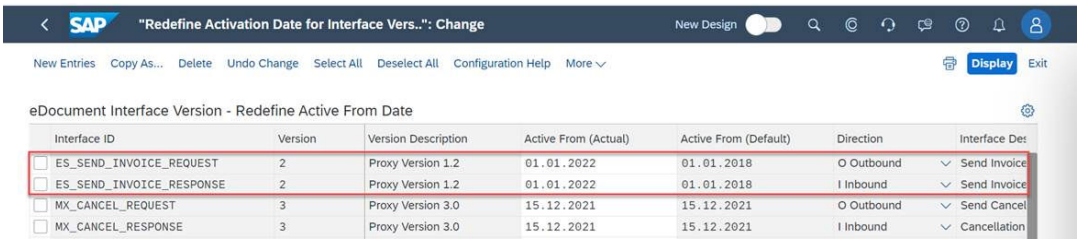
- *Correo* field: Enter the e-mail ID for all communications with FACe.
- The *Send Invoice* integration flow supports both the 3.2 and 3.2.2 version of the XML file, depending on which version you use, enter data in the fields below as follows:

Field	Value for 3.2 Version	Value for 3.2.2 Version
responseNamespace	http://www.sap.com/eDocument/Spain/SendInvoice/v1.1	http://www.sap.com/eDocument/Spain/SendInvoice/v1.2
Signing_Namespace	http://www.facturae.es/Facturae/2009/v3.2/Facturae	**`http://www.facturae.gob.es/formato/Versiones/Facturaev3_2_2.xml`**

To switch from Facturae v3.2 (default version) to v3.2.2, make settings as follows:

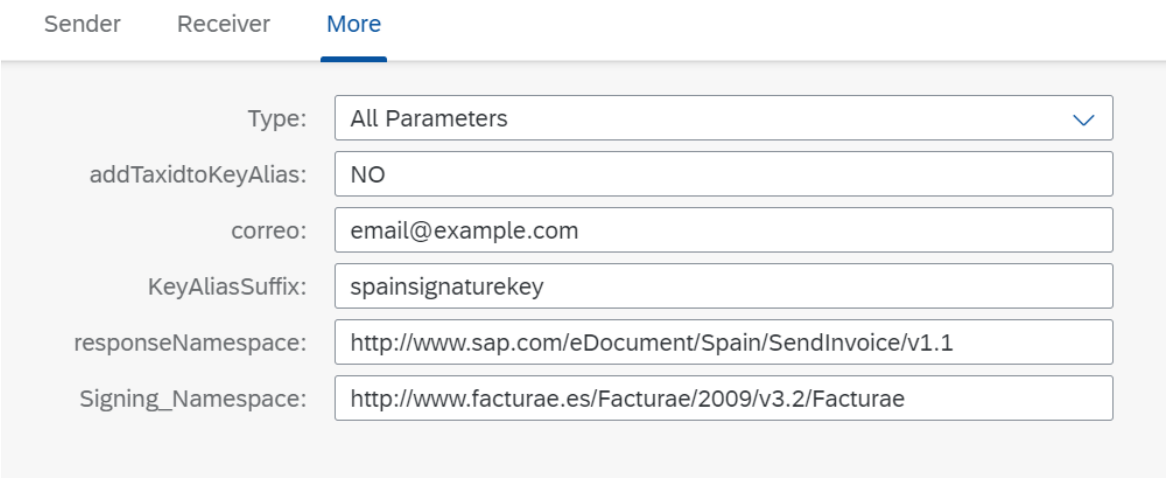
1. Click on the *Manage Your Solution* tile in the Business Process Configuration and ensure that the local version is set to *Spain*.
2. Click on *Configure Your Solution*.
3. In the Application section, choose *Application Platform and Infrastructure* and in the Sub Application section, choose *General Settings for eDocuments* under Item Name.
4. Configure Step Name *Redefine Activation Date for Interface Version* with SSCUI ID 103657 (view `EDOINTVERSCUSTV`).
5. Enter the date of activation in *Active From (Actual)* for the *Interface IDs* of **`ES_SEND_INVOICE_REQUEST`** and **`ES_SEND_INVOICE_RESPONSE`** with **`Proxy Version 1.2`**.

See the following example:



6. If you want to disable Facturae v3.2.2, edit *Active From (Actual)* to **`12/31/9999`**.

- In the *addTaxidtoKeyAlias* field, enter **`YES`** if you want to use the dynamic private key alias, then update the *keyAliasSuffix* field with the name that matches the name that you have defined in section Deploy Certificates and Credentials [page 13]. The system will concatenate the *keyAliasSuffix* field with the tax ID of your company automatically. By default, the *keyAliasSuffix* field is set to **`NO`**.



8. Choose *Save* and *Deploy* to deploy it actively to server. Note down the URLs of the endpoints for each service. Provide the endpoint URLs for FACe in the externalized parameters of the integration flows for the test and productive tenants.

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 Cloud Integration.

6.1 Create Logical Ports in SOAMANAGER

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

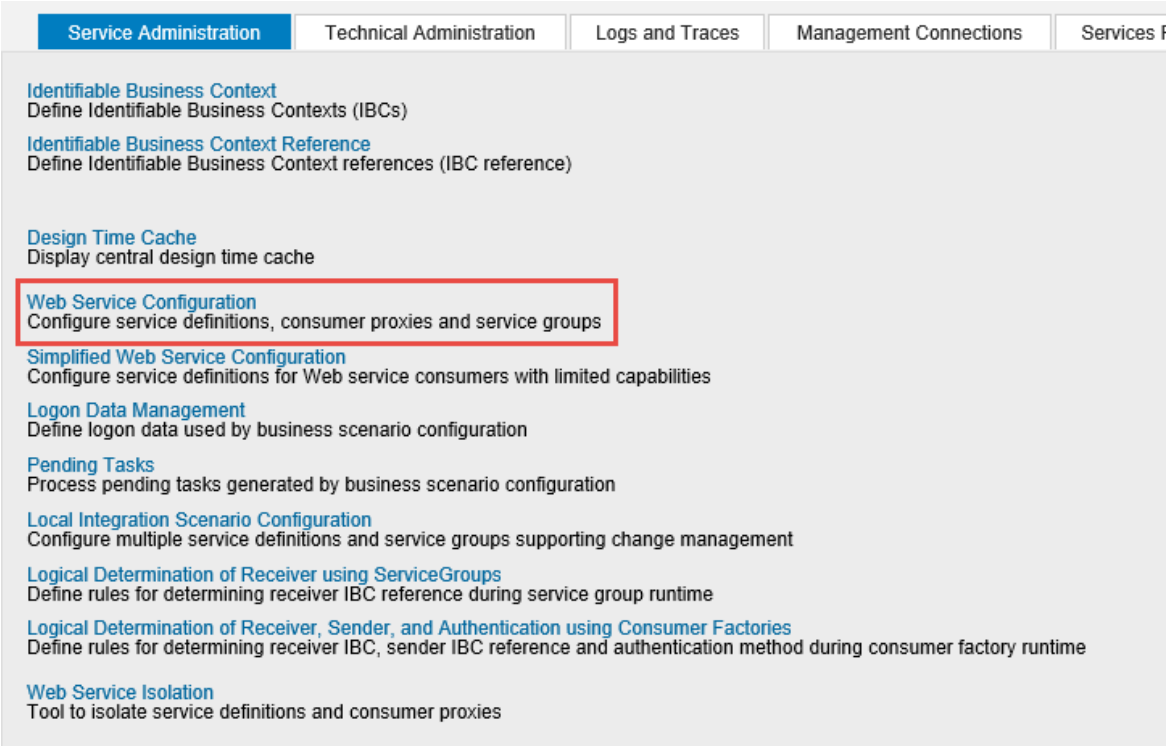
Context

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

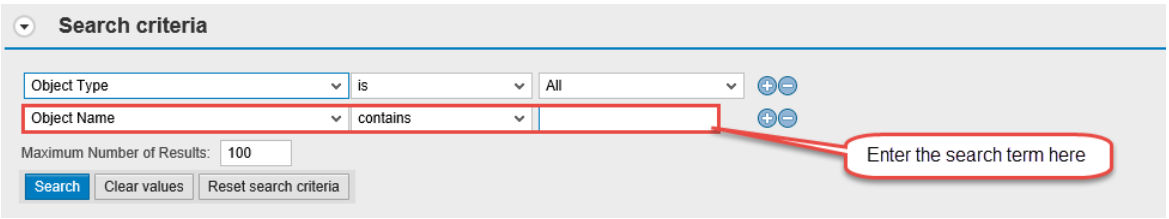
> **i** Note
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

Procedure

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



2. Find the proxies for Spain electronic invoicing with search term CO_EDO_ES_*V1_1.

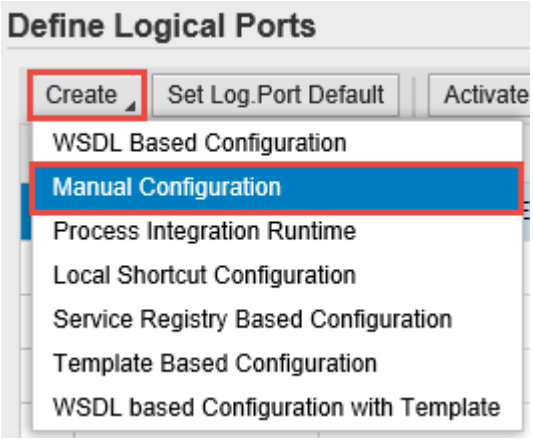


The following table lists the proxies and the logical port name, description and path for each proxy.

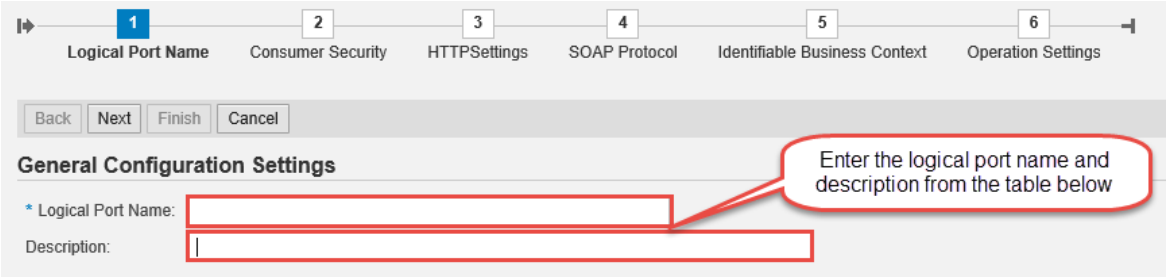
List of Proxies, Logical Port Names, and Paths

Proxy Name	Logical Port Name	Description	Path
CO_EDO_ES_SEND_IN-VOICE_V1_1	EDO_ES_IN-VOICE_TRANSMI_SERV_PORT	Spain eDocument – Send Invoice Service	/cxf/SpainSendInvoice
CO_EDO_ES_GET_STA-TUS_V1_1	EDO_ES_GET_STA-TUS_SERV_PORT	Spain eDocument – Get Status Service	/cxf/SpainGetStatus
CO_EDO_ES_CANCEL_IN-VOICE_V1_1	EDO_ES_CANCEL_IN-VOICE_SERV_PORT	Spain eDocument – Cancel Invoice Service	/cxf/SpainCancelInvoice

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

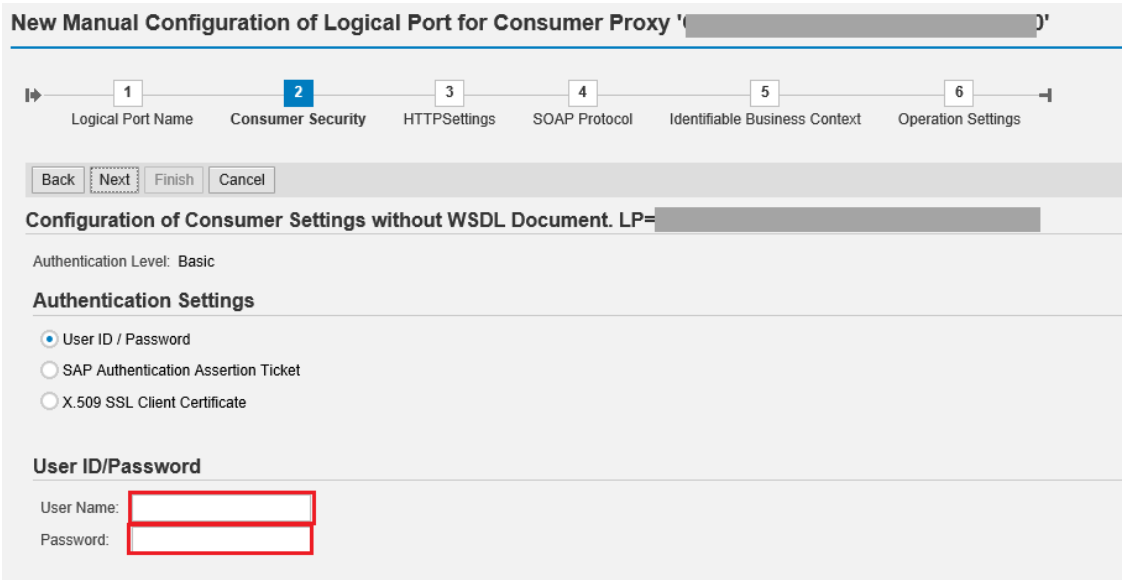


4. Enter the logical port name and a description.



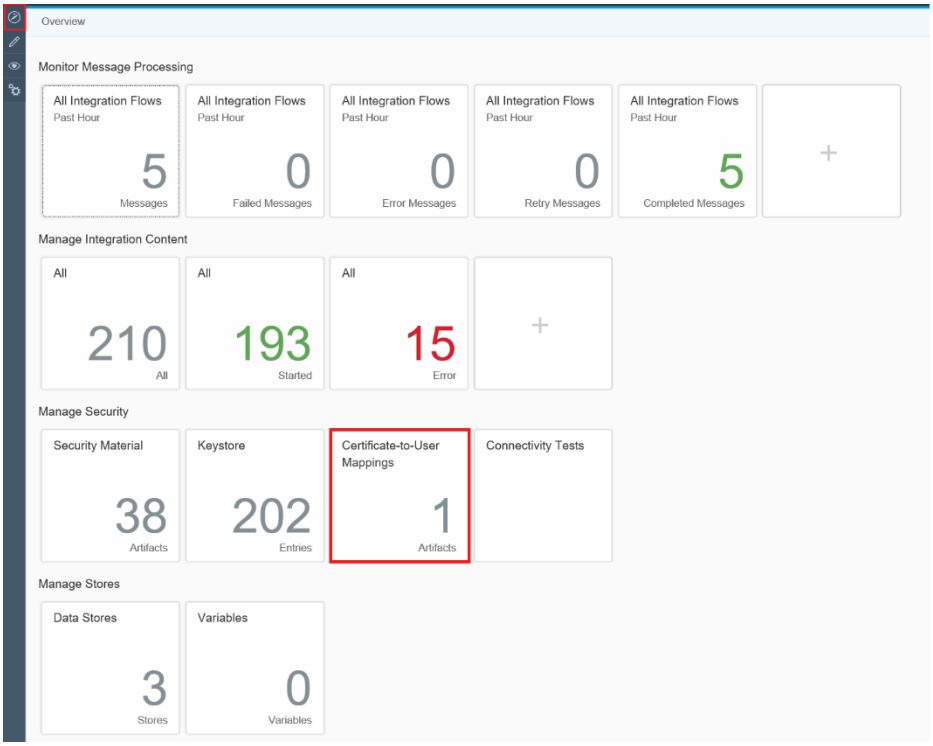
5. The configuration you do in the *Consumer Security* tab in the *Configuration* screen depends on the security being used in the communication between the SAP back-end system and SAP Cloud Integration.
   - If you use the basic authentication, select the *User ID / Password* and enter *User Name* and *Password*.
   - If you use certificate-based authentication, select *X.509 SSL Client Certification*. Ensure that the required certificates are available in the `STRUST` transaction.

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

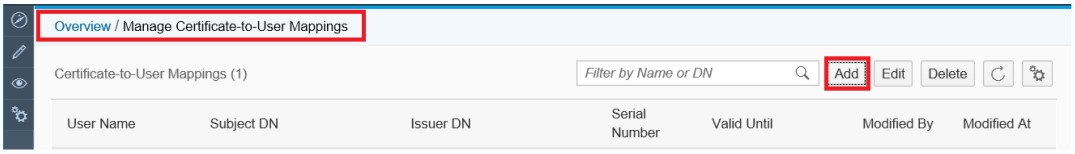


Additionally, you map the certificate to a user of your tenant with the `ESBMessaging.send` role. First, you export the certificate from the `STRUST` transaction. Save it locally and upload it to SAP Cloud Integration in the `Certificate-to-User Mappings`

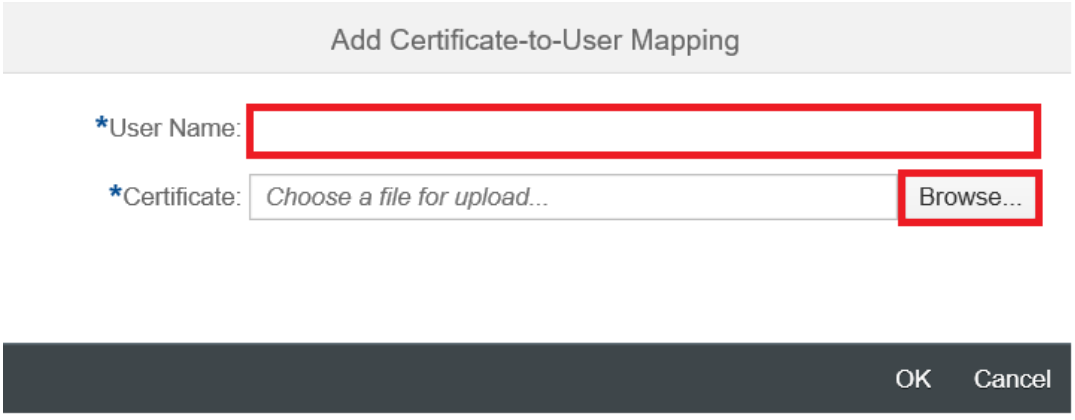
1. Export the SSL Client PSE of the `STRUST` transaction.
2. Go to SAP Cloud Integration under *Overview* > *Certificate-to-User Mappings*



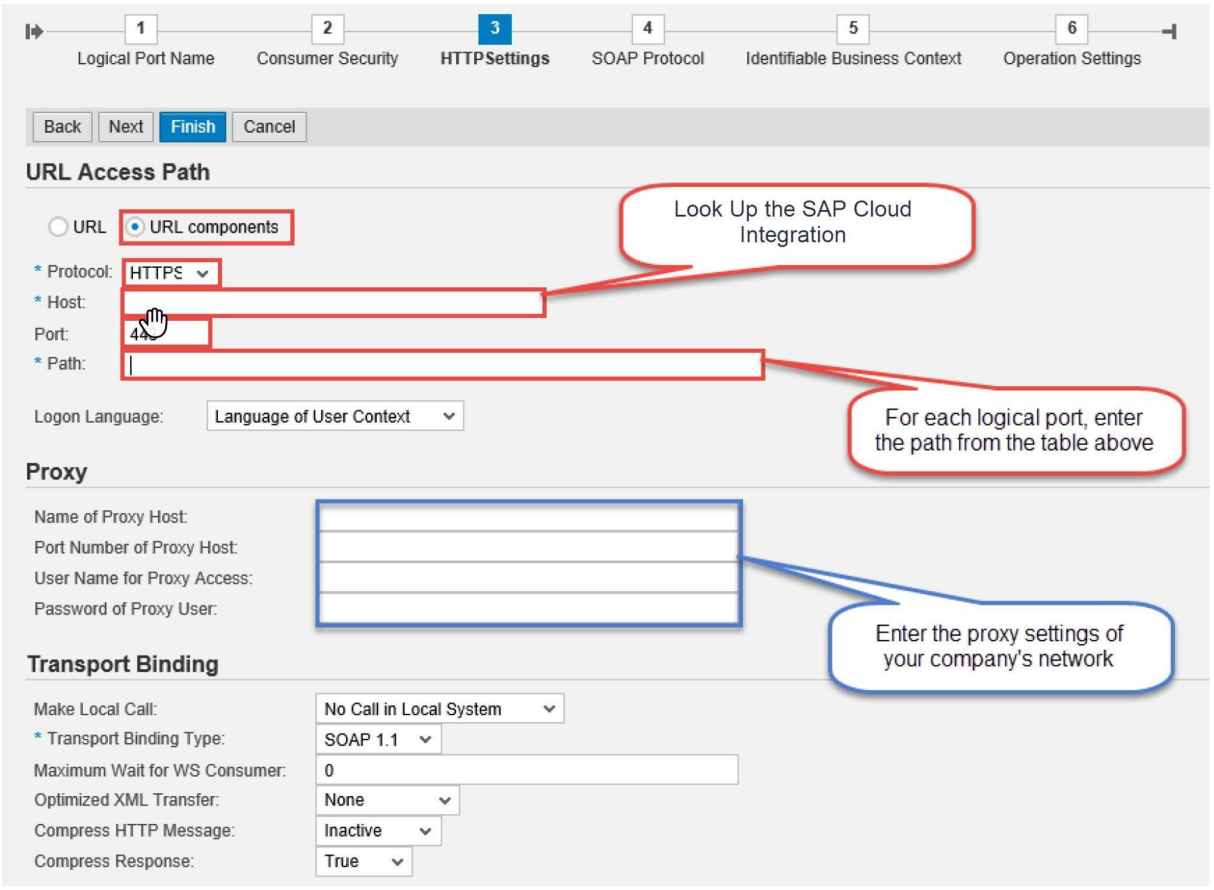
3. Choose *Add*.



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

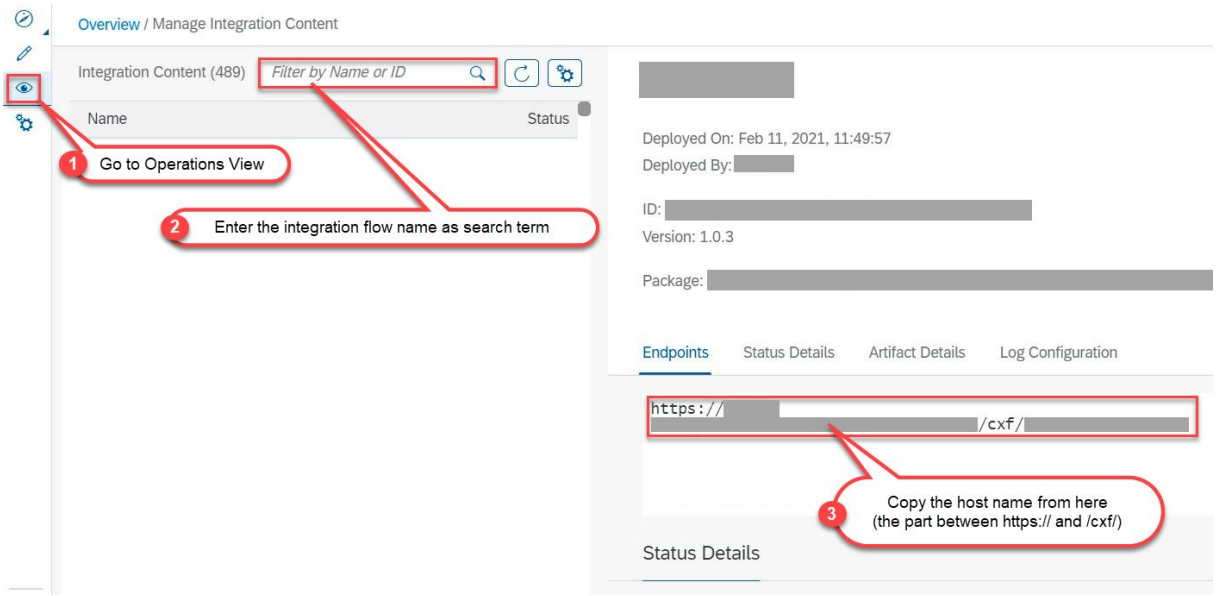


6. On the *HTTP Settings* tab, make the following entries:



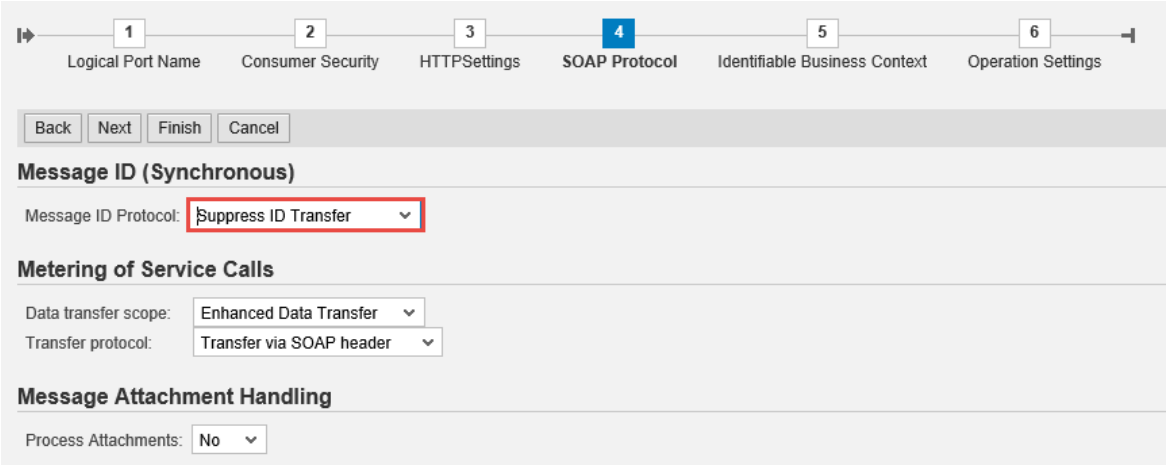
Port 443 is the standard port for the HTTPS protocol.

To find the Host, go to SAP Cloud Integration 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 Cloud Integration does not support WebService Pin for testing your configuration.

   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.

9. Remember to create logical ports for each proxy and to execute the following steps in the SAP back-end systems. For more information, see SAP Note 2095919.

   - 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 the `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 Cloud Integration.

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 tax authority'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 Cloud Integration.
    - If the status is green or yellow, but not `Created`, the communication with SAP Cloud Integration was triggered and was probably successful. You can double-check if the message went through on the SAP Cloud Integration 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 Application Interface Platform (AIF) 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