PUBLIC
2020-06-26

Spain SII: Setting Up SAP Cloud Platform Integration (SAP ERP, SAP S/4HANA) - Cloud Foundry

THE BEST RUN SAP

Content

1 Introduction

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

The setup steps are typically done by an SAP Cloud Platform Integration consulting team, which is responsible for configuring the SAP back-end systems and the connection with SAP Cloud Platform Integration. This team may be also responsible for maintaining the integration content and certificates/credentials on the SAP Cloud Platform 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 Platform 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. You have installed in the test and productive systems all necessary SAP Notes for the eDocument Solution.
2. You have performed all initial setup steps described in Initial Setup of SAP Cloud Platform Integration in Cloud Foundry Environment . After completing the Provisioning the Tenant step, you have created your own tenant URL. This is the URL needed to complete the steps described in the Configuration Steps section of this guide.

2.1 Deploy Certificates for SAP Cloud Platform Integration with Tax Agency Communication

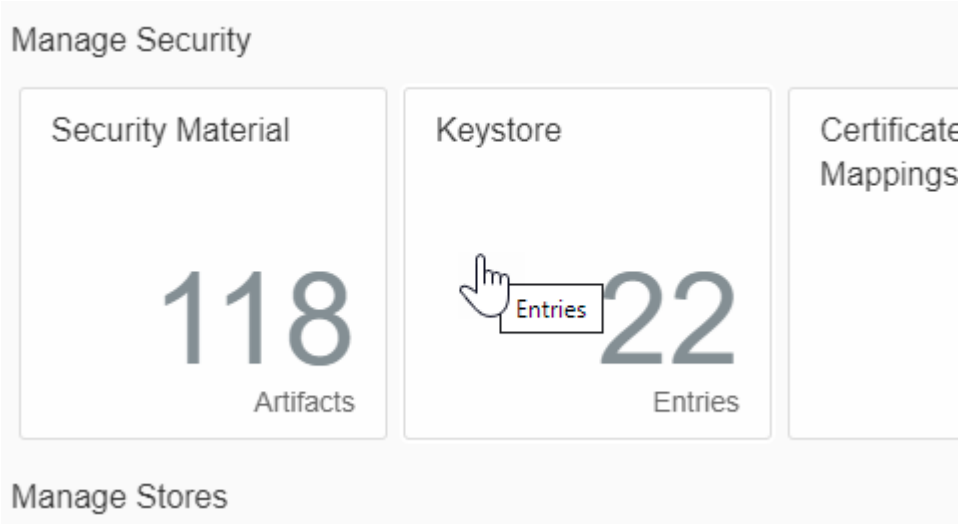
To establish a connection between the SAP Cloud Integration and tax agency servers, you must obtain several certificates, and then deploy these to the SAP Cloud Platform Integration tenant. For more information about certificate deployment in SAP Cloud Platform Integration, see SAP Note 2469460.

2.2 Add Certificate for Client Certificate Authentication

SAP Cloud Platform Integration uses a client certificate to authenticate the communication with external systems. For the SII scenario, you must include certificates that are recognized by the relevant tax agency (AEAT or regional tax agency). Optionally, the tax agency also supports certificates for the electronic seal ("certificado de sello"). This certificate is specific to your company's Fiscal Identity Number (NIF) and/or Tax Identity Number.

To add the certificate, proceed as follows:

1. Collect the key pair from the regional tax office. This key pair is tax ID-specific.
2. 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.
3. In the *Operations* view, choose *Keystore* under *Manage Security*.



4. Choose *Create* > *Key Pair* and create the key pair that you collected from the tax office.

> **Note**
>
> - We recommend that you use private key alias in form of **spainsiixxxx**, where **xxxx** is the company code.
> - From version 3.0.0 onwards, the dynamic private key Alias is available, that is, you can choose to use an alias in form of **spainsiiprivtekey_xxxxx**, where **spainsiiprivtekey** will be the suffix, and **xxxxx** will be you company NIF. If you choose to use the dynamic private key Alias, the system will concatenate the suffix and will extract your company NIF from the header of XML document.

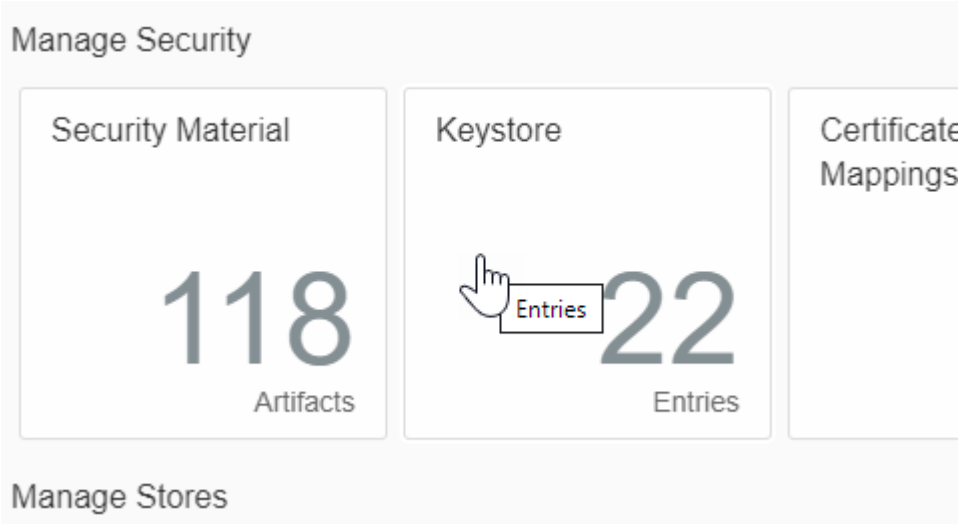
2.3 Add Public Certificates of Relevant Tax Agency

To establish an SSL connection to the tax agency server, the SAP Cloud Platform Integration needs to trust the SSL certificate from the relevant tax agency servers. To achieve this, you must download the entire certificate chain from the relevant server and upload it to the SAP Cloud Platform Integration tenant. Please refer to the relevant tax agencies' sites or the relevant governmental SII support teams to obtain relevant certificate chains.

Another option is to use third-party software, which has the capability of examining and downloading site certificates like browsers or key store explorers. The exact procedure of downloading the SSL certificate depends on third-party software and the operating system that you use.

To add the certificate, proceed as follows:

1. Refer to the regional tax authority guide to get the URL to the tax authority.
2. 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.
3. In the *Operations* view, choose *Keystore* under *Manage Security*.



4. Choose *Add* > *Certificate* to add the certificate.

> **Note**
>
> You can find the list of servers of the regional tax authorities in the document *Regional Support Guide*, included in this integration package.

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 Platform Integration. For more information, refer to the documentation of the SAP Cloud Platform 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 iFlow 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 Operations guide for SAP Cloud Platform Integration

> **i Note**
>
> If you encounter any issues in the information provided in the SAP Cloud Platform 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 iFlow [page 9].

3.1.1 Retrieve and Save Public Certificates

Context

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

Procedure

1. Access the SAP Cloud Platform 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 (iFlows) available.
5. Select an iFlow 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.

3.1.2 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 Cloud Platform 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.

3.1.3 Authenticate iFlow

Create an own certificate and get it signed by a trusted certificate authority (CA) to support iFlow 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 Cloud Platform Integration

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

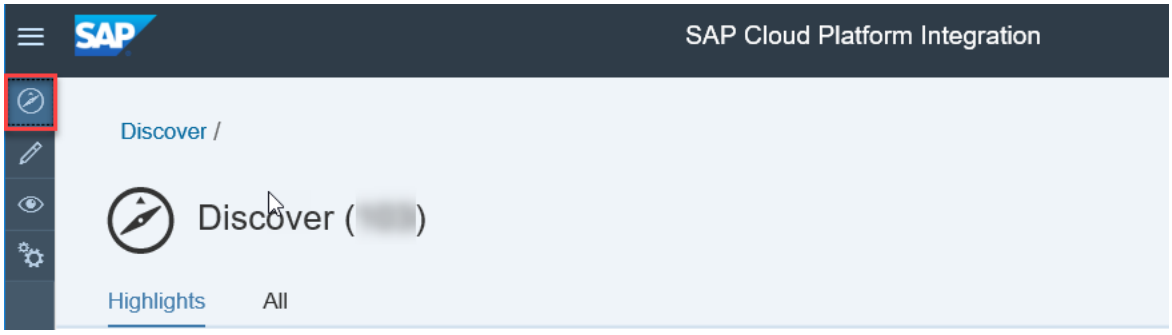
4.1 Copy Published Package

Context

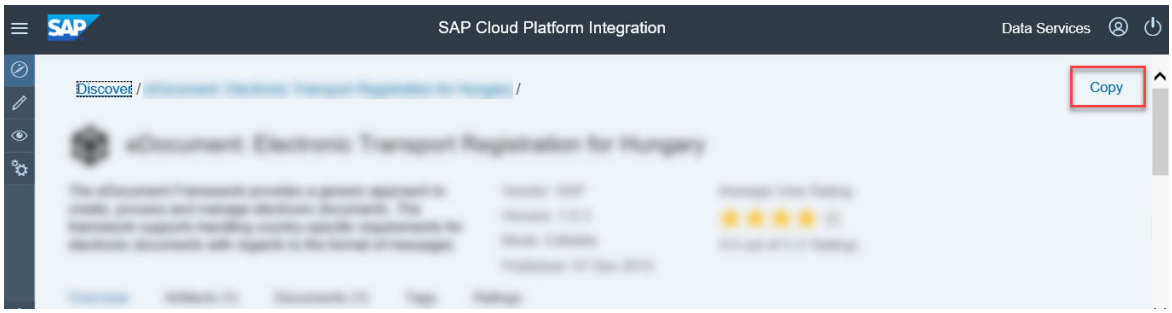
Copy all iFlows in the package *SAP Document Compliance: Tax Register Books for Spain* to the target tenant as follows:

Procedure

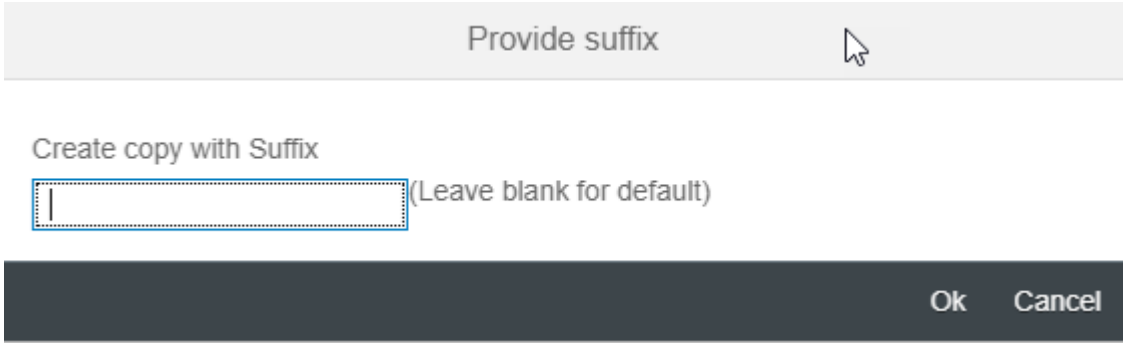
1. In the *Discover* section of your tenant, select the package *SAP Document Compliance: Tax Register Books for Spain*.



2. Select the package and choose *Copy*.



3. In the *Provide suffix* dialog box, leave the field blank and choose *Ok*.



4.2 Configure Integration Flow

4.2.1 Configure Integration Flow - Communicate to SII

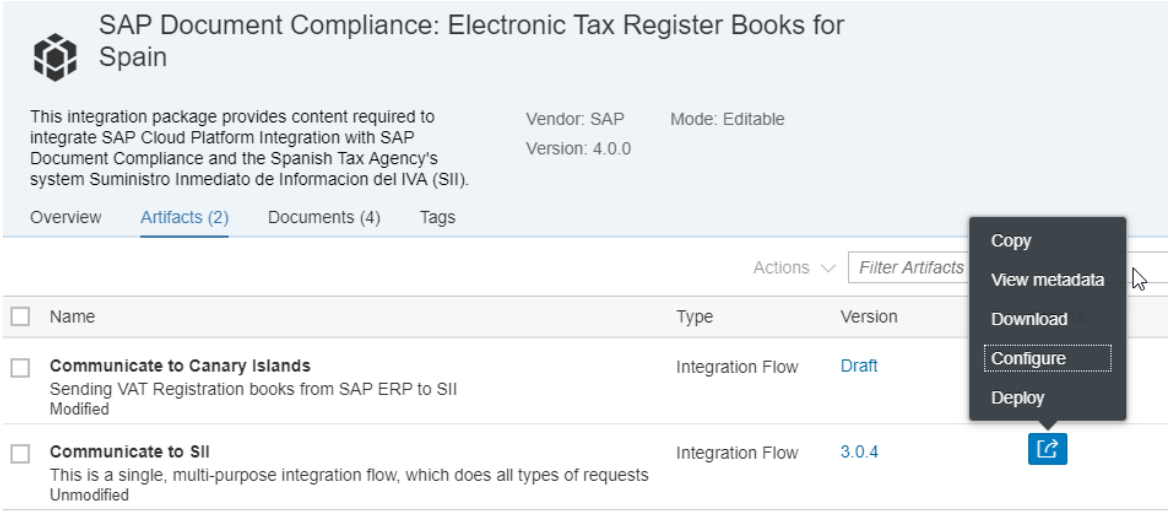
To set up communication with the tax authorities in Spain, you must configure the integration flow “Communicate to SII” as described in this section.

Context

You must repeat the steps below for every package that you copied as described in section Copy Published Package [page 11].

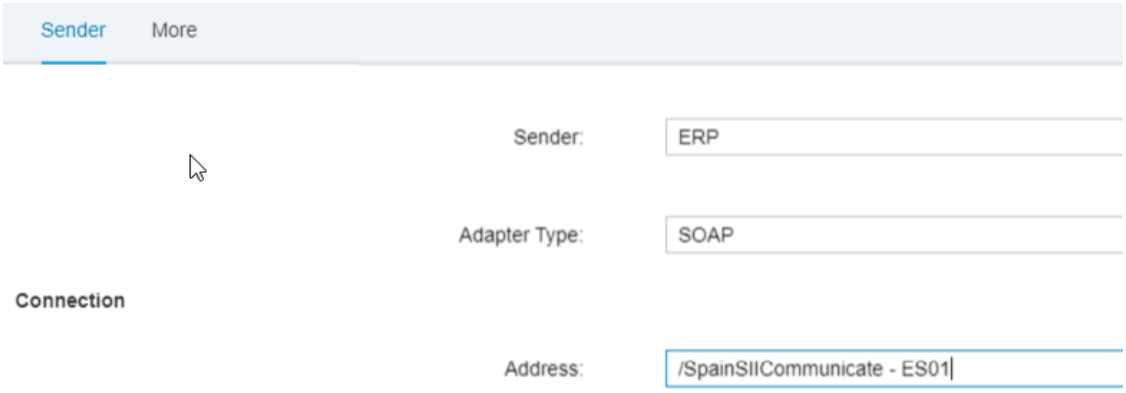
Procedure

1. Choose *Design* from the upper left corner of the page.
2. Click on the package that you copied from the original *Document Compliance: Tax Register Books for Spain* package.
3. Go to the *Artifacts* tab page.
4. Choose *Actions* > *Configure* for the *Communicate to SII* ingegration flow.



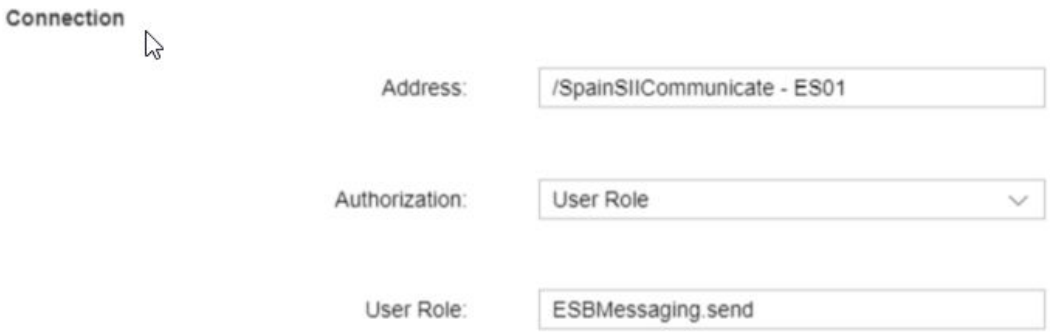
> **Note**
>
> The version of your artifact may differ from the one shown on the figure above.

5. Choose the *Sender* tab and make settings as follows:
   - Update the connection address to a name that can be linked easily to the company code that uses it (for example, **`/SpainSIICommunicate-ES01`** for the company code ES01):



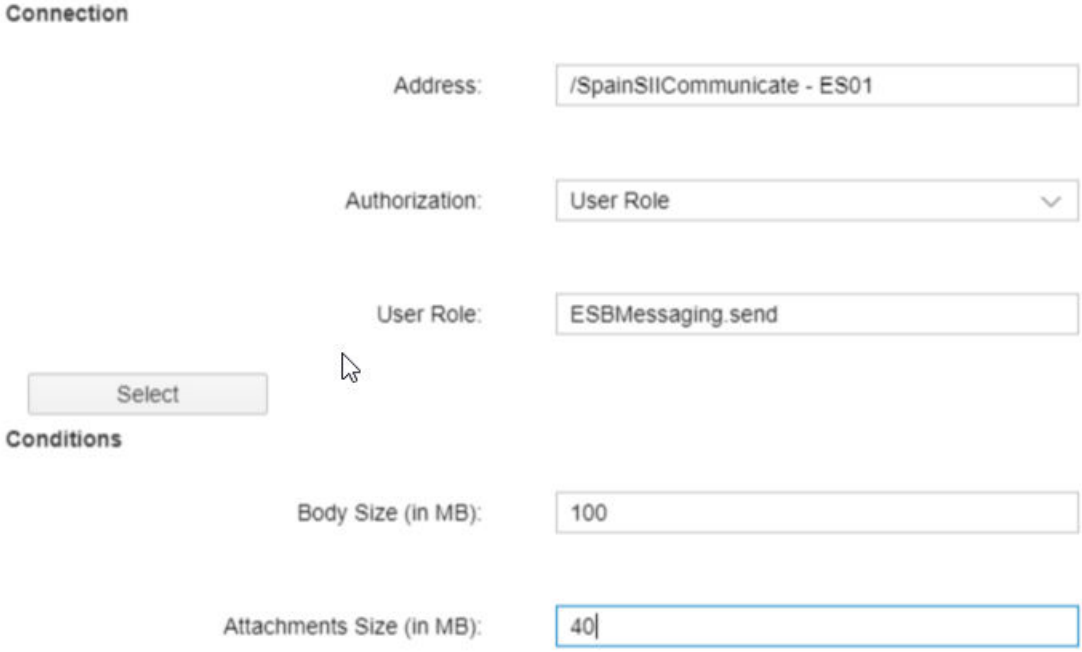
   - *Authorization* field: Select the required authorization (**`User Role`** or **`Client Certificate`**) that has been configured for the connection between the system and the tenant.

- For the *User Role* authorization, select the relevant user role (for example, **`ESBMessaging.send`**):



- For the *Client Certificate* authorization, provide the certificate credentials, for example:

- If required, increase the body size (that is, the maximum XML file size) to the appropriate value:



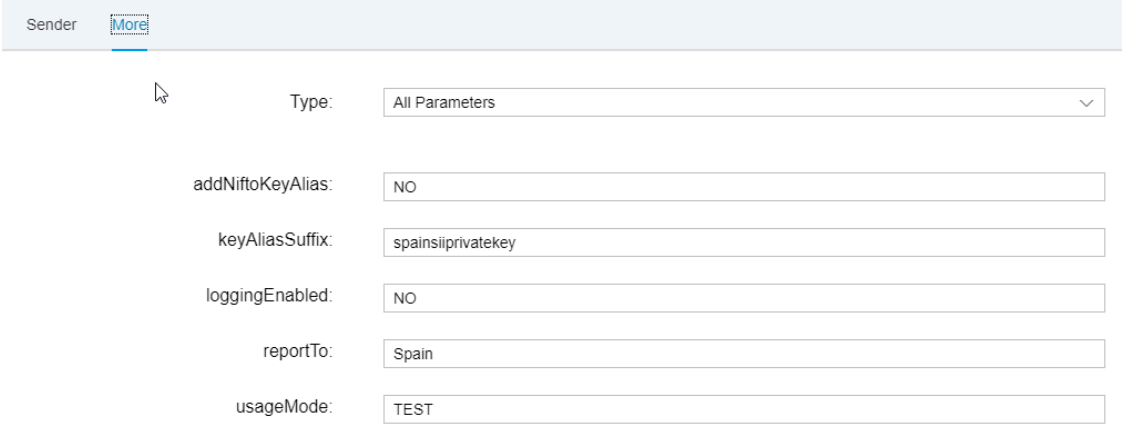
6. Choose the *More* tab and make settings as follows:

> **Note**
>
> - In some versions, this tab may have the title *Parameters*.
> - The layout under this menu tab may differ from the screenshot provided.

- In the *Private Key Alias* field, update the name to match the name that you have defined in section .

  > **Note**
  >
  > From version 3.0.0 onwards, the dynamic private key alias is available.

- In the *addNifftoKeyAlias* 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 .
  The system will concatenate the *keyAliasSuffix* field with the NIF of your company automatically.
  By default, the *addNifftoKeyAlias* field is set to **NO**. In that case, you must also update the *keyAliasSuffix* field with the name that matches the name that you have defined in section .



- Use the *usageMode* field to set up the integration package usage mode:

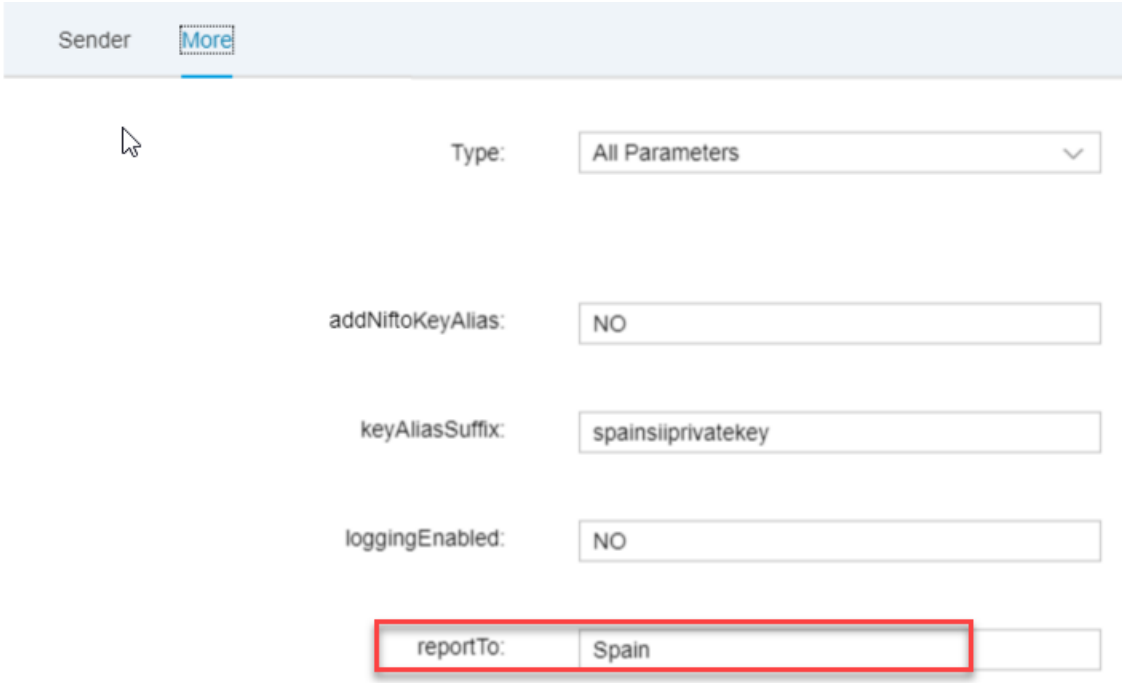
Value	Acceptable aliases	Description
TEST		Uses the test system of the tax agency
PROD	PRODUCTIVE, PRODUCTION	Uses the productive (that is, legally binding) system of the tax agency
ESEAL	E-SEAL, PROD-SEAL	Uses the productive system that accepts certificate of the electronic seal

> **Note**
>
> Submitting documents with an SII Version below 1.0 to productive servers will cause an error. For SII Versions below 1.0, only test services are provided.

- Use the *loggingEnabled* field for switching logging on and off:

Value	Description
YES	Enable logging of the request and response messages
NO	Disable logging of the request and response messages

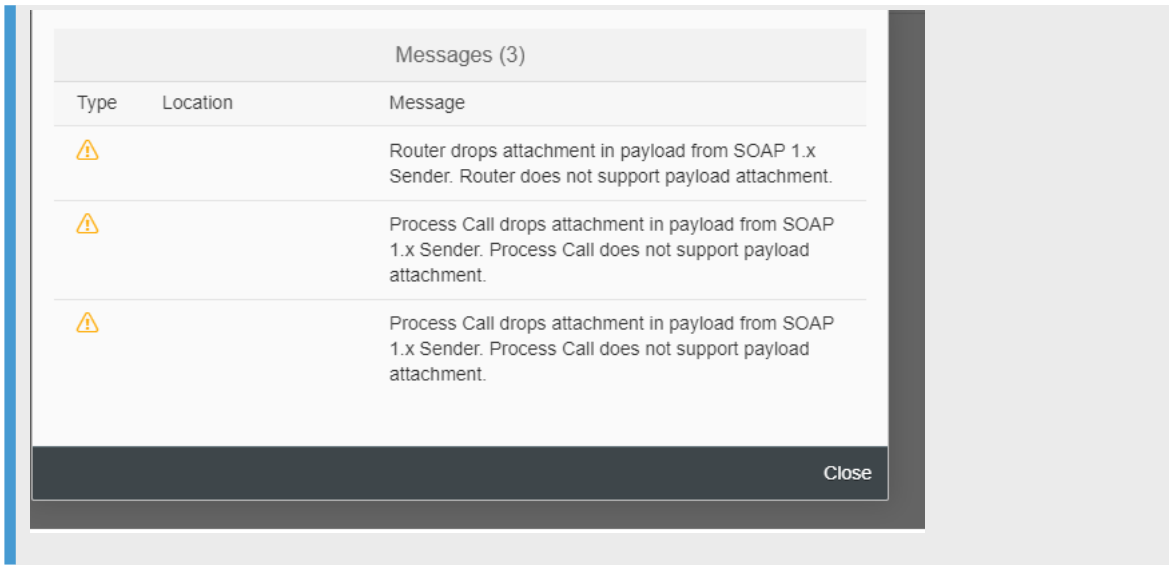
- Use the *reportTo* field to define the regional tax authority to which you want to submit your reports.



> **i Note**
>
> By default, the reports are submitted to the central tax authority (Agencia Estatal de Administración Tributaria). For the list of the values for the regional tax authorities and supported functions, refer to the document "Submitting to the regional tax authorities" included in this package.

7. Select *Save* and *Deploy* to save your configuration and to deploy it actively to server, respectively.

> **i Note**
>
> On some tenants, depending on their version, after pressing these buttons, a screen with warning messages may occur, similar to the one below. Ignore these messages, and press the *Close* button, as they are related to the payload attachments; currently the SII process either does not support or require message attachments (for example, scanned copies of invoices) in any stage of processing and communication.



4.2.2 Configure Integration Flow - Communicate to Canary Islands

To set up communication with the tax authorities in the Canary Islands, you must configure the integration flow “Communicate to Canary Islands” as described in this section.

Repeat the steps described in section Configure Integration Flow - Communicate to SII [page 12] for the *Communicate to Canary Islands* artifact as all the steps are the same for the Canary Islands.

> **i** Note
>
> For the Canary Islands, you must also choose **`Spain`** in the *Report to* field under the *More* tab.

4.3 Parameter Delegation

You can delegate the setup for several parameters back to the back-end system.

To do so, use the value **`ByRequest`** for any parameters listed below instead of the values from the section Configure Integration Flow [page 12] during integration flow configuration.

The following parameters are supported:

Parameter	Comment
`usageMode`	No default value. In case of empty value, an error will be generated.

Parameter	Comment
`loggingEnabled`	Default value is “NO”, that is, request and response bodies will not be logged
`reportTo`	Default value is “Spain”, that is, reporting to Central Tax Authority

To provide the parameter for the integration flow, add it as a query parameter of the same name (for example, usageMode=TEST or loggingEnabled=YES) to the integration flow URL in your source system. If you are adding more than one query parameter, separate them with the ampersand sign (&). The first query parameter must be prepended by the question mark (?), for example:

```
cxf/SpainSIICommunicateES01?usageMode=TEST&loggingEnabled=NO&reportTo=Spain
```

> **i Note**
>
> - Take into account that the parameter setup is only delegated if its value is explicitly set to **`ByRequest`** in Integration Flow configuration, otherwise query parameters will have no effect.
> - The main advantages of such a delegation are the following:
>   - It is possible to change those parameters without reconfiguring and restarting integration flow.
>   - The user can easily see in the source system which parameters are used to access the SAP Cloud Platform Integration content.
> - It is not recommended to use this approach when it is not appropriate to grant integration content configuration rights to the people responsible for the back-end system setup.

5 Configuration Steps in SAP Backend Systems

5.1 Create Logical Ports in SOAMANAGER

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

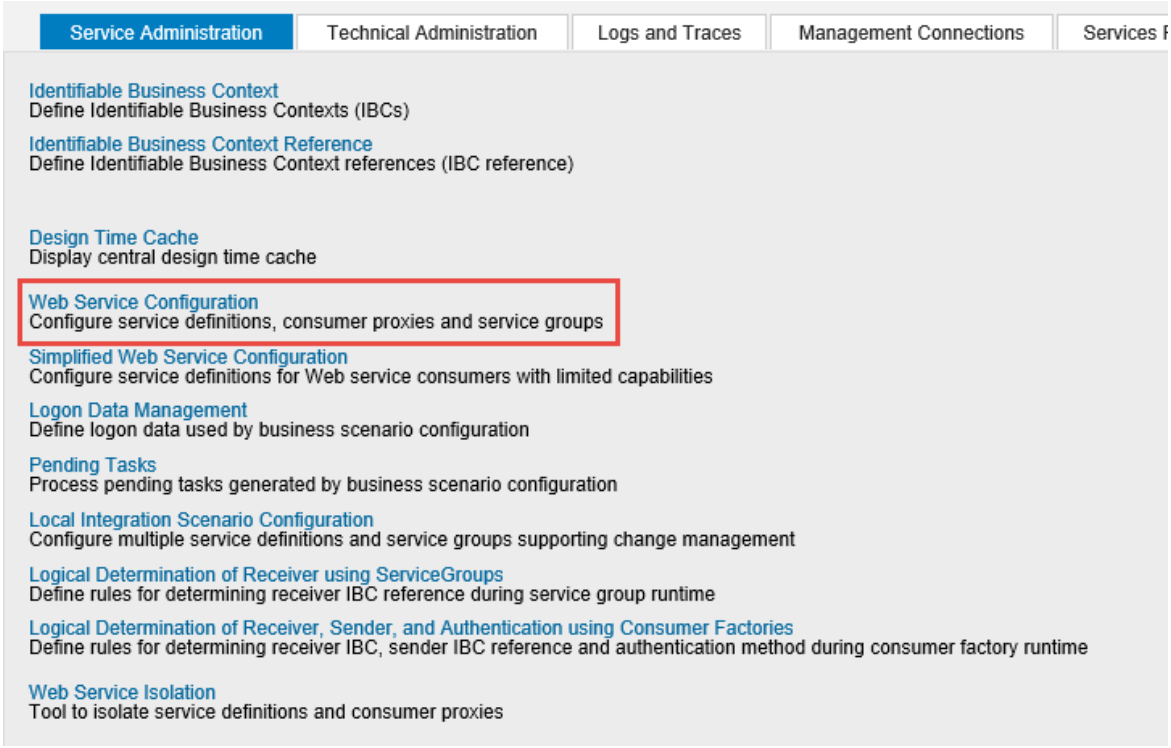
Context

You configure proxies which are needed to connect to the SAP Cloud Platform 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 Platform Integration tenant.

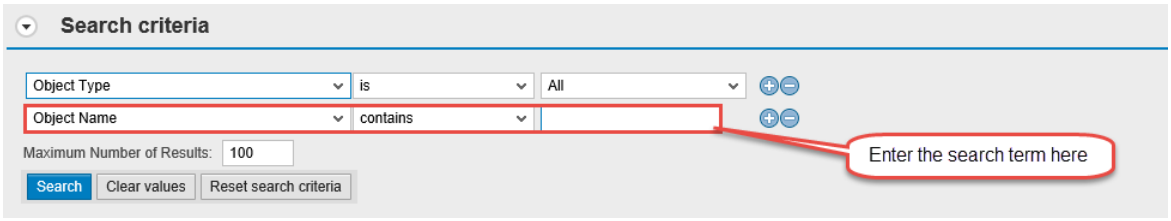
> **i** Note
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

Procedure

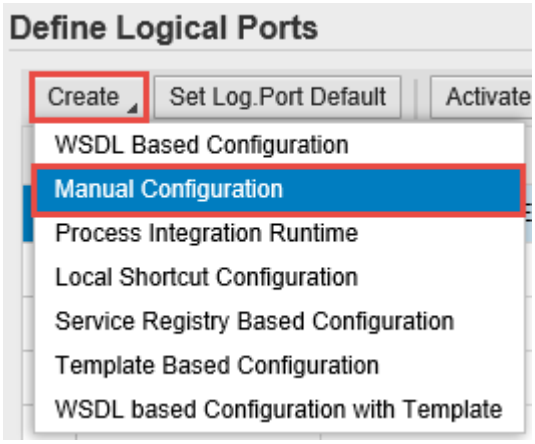
1. In your SAP back-end system, go to the `SOAMANAGER` transaction and search for *Web Service Configuration* .



2. Find the proxies for Spain SII with search term CO_ESSII*. For proxies for Canary Islands, use the search term *EDO_ES_CAN_*.



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



The number of logical ports that you need to configure for each proxy depends on the number of AEAT certificates or integration flows that you are configuring.

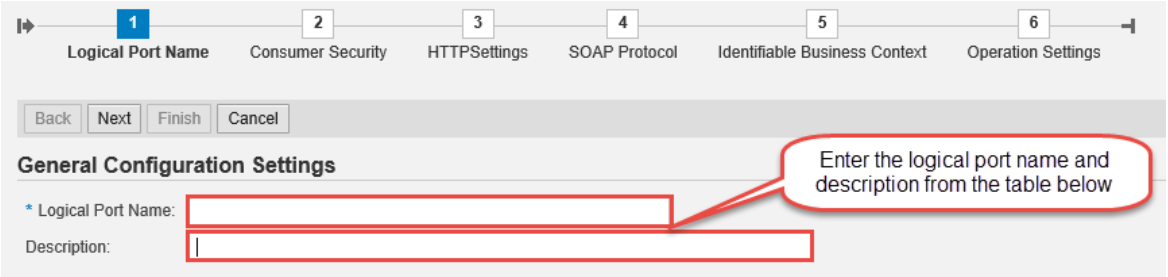
For example, if you're configuring for two company codes (ES01 and ES02):

Proxy Name	Logical Port Name	Path
CO_ESSII_001_INCOMING_INVOICE	ESSII_PORT_ES01	cxf/SpainSIICommunicateES01
CO_ESSII_001_INCOMING_INVOICE	ESSII_PORT_ES02	cxf/SpainSIICommunicateES02
CO_ESSII_001_OUTGOING_INVOICE	ESSII_PORT_ES01	cxf/SpainSIICommunicateES01
CO_ESSII_001_OUTGOING_INVOICE	ESSII_PORT_ES02	cxf/SpainSIICommunicateES02
CO_ESSII_001_OUT_PAY_VOC_EN	ESSII_PORT_ES01	cxf/SpainSIICommunicateES01
CO_ESSII_001_OUT_PAY_VOC_EN	ESSII_PORT_ES02	cxf/SpainSIICommunicateES02
CO_ESSII_001_INC_CASH_PAYMENT	ESSII_PORT_ES01	cxf/SpainSIICommunicateES01
CO_ESSII_001_INC_CASH_PAYMENT	ESSII_PORT_ES02	cxf/SpainSIICommunicateES02

An example for Canary Islands:

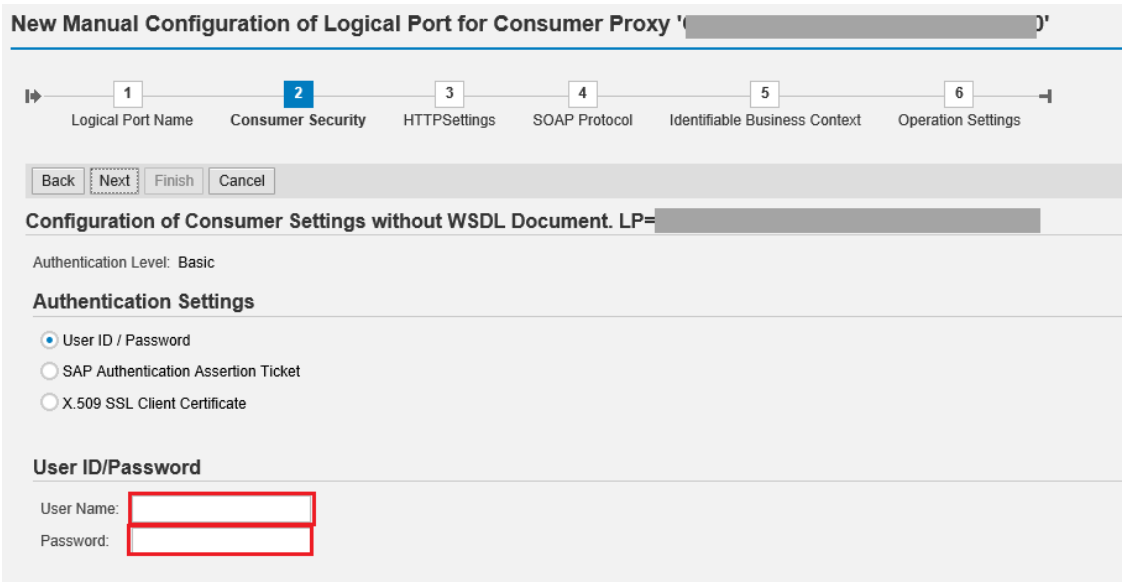
Proxy Name	Logical Port Name	Path
CO_EDO_ES_CAN_INCOMING_IN-VOICE	LP_EDO_ESCAN_ES01	cxf/SpainSIICanaryzommunica-teES01
CO_EDO_ES_CAN_INCOMING_IN-VOICE	LP_EDO_ESCAN_ES02	cxf/SpainSIICanaryCommunica-teES02
CO_EDO_ES_CAN_INC_CASH_PAY-MENT	LP_EDO_ESCAN_ES01	cxf/SpainSIICanaryzommunica-teES01
CO_EDO_ES_CAN_INC_CASH_PAY-MENT	LP_EDO_ESCAN_ES02	cxf/SpainSIICanaryCommunica-teES02
CO_EDO_ES_CAN_OUTGOING_IN-VOICE	LP_EDO_ESCAN_ES01	cxf/SpainSIICanaryzommunica-teES01
CO_EDO_ES_CAN_OUTGOING_IN-VOICE	LP_EDO_ESCAN_ES02	cxf/SpainSIICanaryCommunica-teES02
CO_EDO_ES_CAN_OUTGOING_IN-VOICE	LP_EDO_ESCAN_ES01	cxf/SpainSIICanaryzommunica-teES01
CO_EDO_ES_CAN_OUTGOING_IN-VOICE	LP_EDO_ESCAN_ES02	cxf/SpainSIICanaryCommunica-teES02

4. Enter the logical port name and a description.

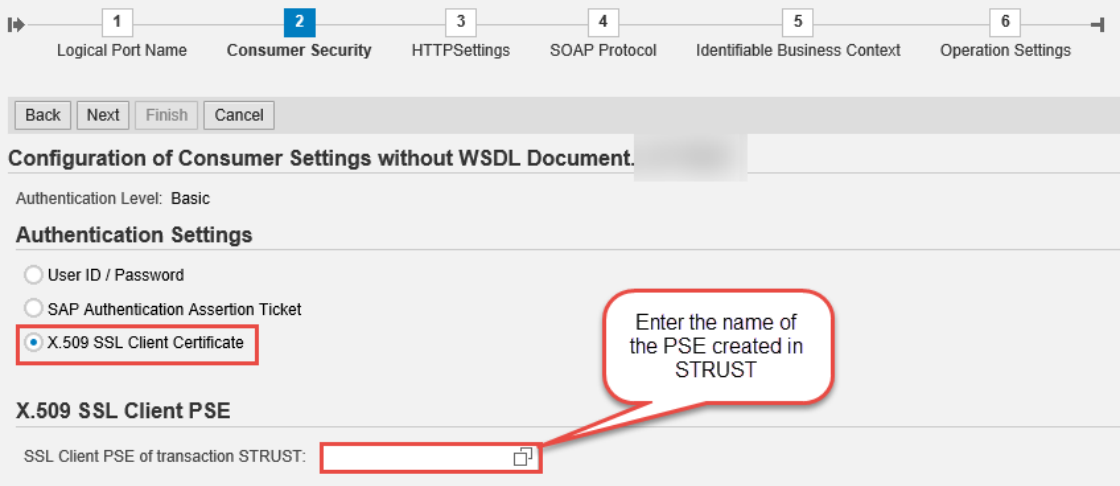


> ### i Note
>
> You can choose to use the dynamic private key alias. You must configure your certificates with a common suffix to concatenate it with the company NIF. In this case, you do not need to make several logical ports, the system will search for the suffix plus company NIF on the certificates.

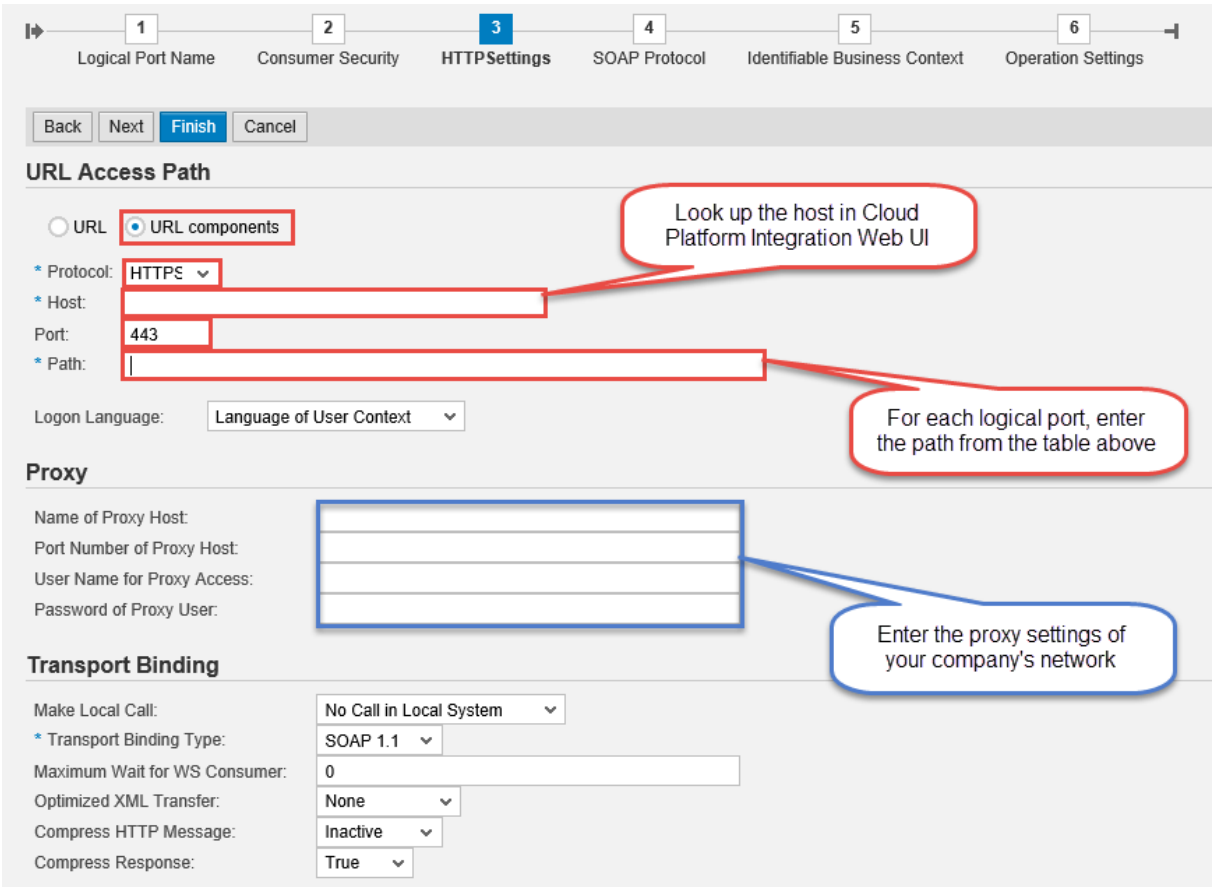
5. The configuration you do in the *Consumer Security* tab in the *Configuration* screen depends on the security being used in the communication between the back-end system and SAP Cloud Platform Integration.
   - If you use the basic authentication for *User Name*, enter the value for the **clientid** and for *Password*, enter the value for **clientsecret**. You have created these values for your service instance in SAP Cloud Platform Integration. See Creating Service Instances.



   - If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have updloaded to `STRUST`. You must configure this certificate in SAP Cloud Platform Integration too. For that you create a service instance using the required grant_type. You create the service key using the certificate uploaded to the `STRUST`. For more information, see Defining a Service Key for the Instance in the Cloud Foundry Environment

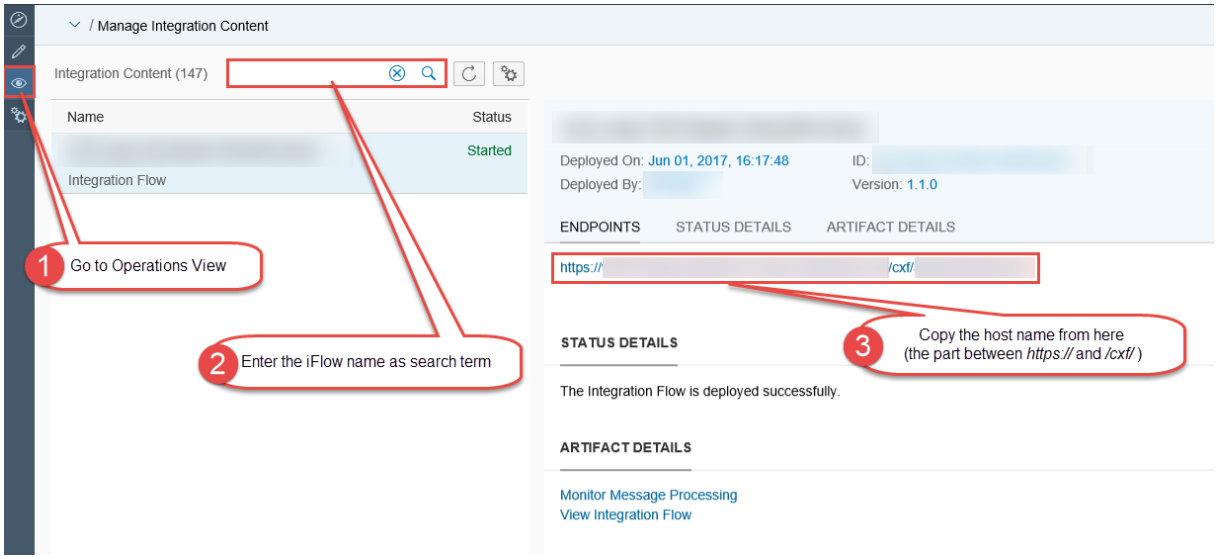


6. On the *HTTP Settings* tab, make the following entries:



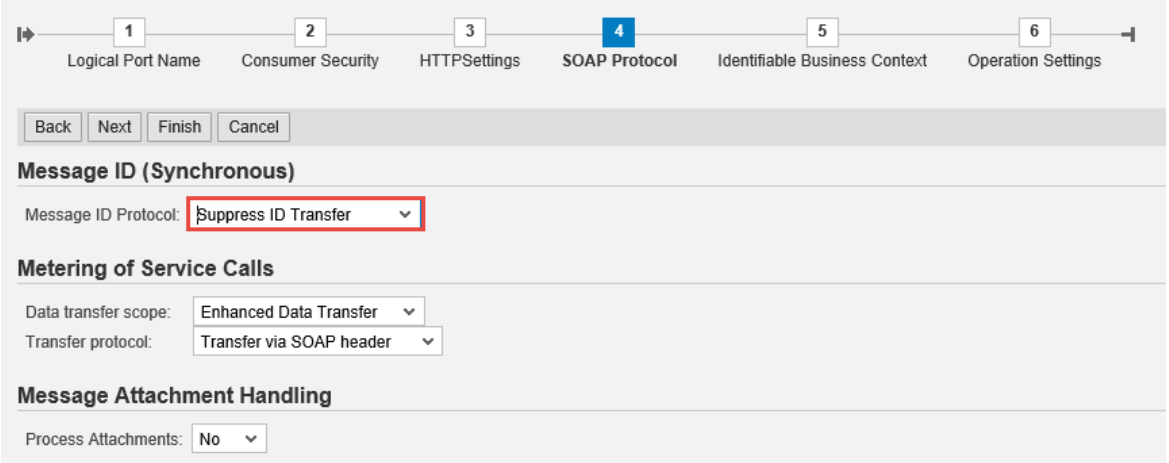
Port 443 is the standard port for the HTTPS protocol.

To find the Host, go to SAP Cloud Platform 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:



> ### 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 Platform 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 Platform Integration service (for example, for path /cxf/SpainSIICommunicateES01) 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 2636341 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

5.2 Define SOA Services for Communication

In Customizing for *Cross-Application Components*, choose *General Application Functions* > *eDocument* > *General Settings* > *Define SOA Services for Communication* (`EDOSOASERV` view).

In this Customizing activity, you define SOA service names and assign the logical ports to the combination of a SOA service name and a company code as follows:

1. Define the name for the following 5 SOA services:
   - Registration of Incoming Invoices: For example, ES_SII_REGIS_INC_INV
   - Registration of Outgoing Invoices: For example, ES_SII_REGIS_OUT_INV
   - Deregistration of Incoming Invoices: For example, ES_SII_DEREG_INC_INV
   - Deregistration of Outgoing Invoices: For example, ES_SII_DEREG_OUT_INV
   - Registration of Outgoing Payments: For example, ES_SII_REGIS_OUT_PAY
   - Registration of Incoming Cash Payments: For example, ES_SII_REGIS_INC_PAY
   - Deregistration of Incoming Cash Payments: For example, ES_SII_DEREG_INC_PAY

   > **i Note**
   >
   > In case you are configuring for several company codes, the SOA service name must not be multiplied, that is, each company code uses the same SOA service name but different logical ports. The logical port is the one you configured in section .

2. Maintain the entries in the Customizing activity.
   For example, following the example shown in section :

SOA Service Name	Company Code	Logical Port	SOA Service Description
ES_SII_DEREG_INC_INV	ES01	ESSII_PORT_ES01	Incoming Invoice Deregistration
ES_SII_DEREG_INC_INV	ES02	ESSII_PORT_ES02	Incoming Invoice Deregistration
ES_SII_DEREG_OUT_INV	ES01	ESSII_PORT_ES01	Outgoing Invoice Deregistration
ES_SII_DEREG_OUT_INV	ES02	ESSII_PORT_ES02	Outgoing Invoice Deregistration
ES_SII_REGIS_INC_INV	ES01	ESSII_PORT_ES01	Incoming Invoice Registration
ES_SII_REGIS_INC_INV	ES02	ESSII_PORT_ES02	Incoming Invoice Registration
ES_SII_REGIS_OUT_INV	ES01	ESSII_PORT_ES01	Outgoing Invoice Registration
ES_SII_REGIS_OUT_INV	ES02	ESSII_PORT_ES02	Outgoing Invoice Registration
ES_SII_REGIS_OUT_PAY	ES01	ESSII_PORT_ES01	Outgoing Payments Registration

SOA Service Name	Company Code	Logical Port	SOA Service Description
ES_SII_REGIS_OUT_PAY	ES02	ESSII_PORT_ES02	Outgoing Payments Registration
ES_SII_REGIS_INC_PAY	ES01	ESSII_PORT_ES01	Incoming Cash Payment Registration
ES_SII_REGIS_INC_PAY	ES02	ESSII_PORT_ES02	Incoming Cash Payment Registration
ES_SII_DEREG_INC_PAY	ES01	ESSII_PORT_ES01	Incoming Cash Payment Deregistration
ES_SII_DEREG_INC_PAY	ES02	ESSII_PORT_ES02	Incoming Cash Payment Deregistration

Example for the Canary Islands:

SOA Service Name	Company Code	Logical Port	SOA Service Description
ES_CAN_DEREG_INC_INV	ES01	LP_EDO_ESCAN_ES01	Incoming Invoice Deregistration
ES_CAN_DEREG_INC_INV	ES02	LP_EDO_ESCAN_ES02	Incoming Invoice Deregistration
ES_CAN_DEREG_INC_PAY	ES01	LP_EDO_ESCAN_ES01	Incoming Cash Payment Deregistration
ES_CAN_DEREG_INC_PAY	ES02	LP_EDO_ESCAN_ES02	Incoming Cash Payment Deregistration
ES_CAN_DEREG_OUT_INV	ES01	LP_EDO_ESCAN_ES01	Outgoing Invoice Deregistration
ES_CAN_DEREG_OUT_INV	ES02	LP_EDO_ESCAN_ES02	Outgoing Invoice Deregistration
ES_CAN_REGIS_INC_INV	ES01	LP_EDO_ESCAN_ES01	Incoming Invoice Registration/Modification
ES_CAN_REGIS_INC_INV	ES02	LP_EDO_ESCAN_ES02	Incoming Invoice Registration/Modification
ES_CAN_REGIS_INC_PAY	ES01	LP_EDO_ESCAN_ES01	Incoming Cash Payment Registration/Modification
ES_CAN_REGIS_INC_PAY	ES02	LP_EDO_ESCAN_ES02	Incoming Cash Payment Registration/Modification
ES_CAN_REGIS_OUT_INV	ES01	LP_EDO_ESCAN_ES01	Outgoing Invoice Registration/Modification
ES_CAN_REGIS_OUT_INV	ES02	LP_EDO_ESCAN_ES02	Outgoing Invoice Registration/Modification
ES_CAN_REGIS_OUT_PAY	ES01	LP_EDO_ESCAN_ES01	Outgoing Payment Registration VOC Vendor
ES_CAN_REGIS_OUT_PAY	ES02	LP_EDO_ESCAN_ES02	Outgoing Payment Registration VOC Vendor

5.3 Assign SOA Services to eDocument Interfaces

In Customizing for *Cross-Application Components*, choose *General Application Functions* > *eDocument* > *General Settings* > *Assign SOA Services to eDocument Interfaces* (`EDOINTV` view).

In this Customizing activity, you must assign the SOA service names you created before to an interface ID. The interface IDs are delivered by SAP as part of the Electronic Tax Register Books with SII solution and their names begin with ES_SII, for example:

Interface ID	SOA Service Name	Direction
ES_SII_DEREGI_IN_INV_REQUEST	ES_SII_DEREG_INC_INV	Outbound
ES_SII_DEREGI_IN_INV_RESPONSE	ES_SII_DEREG_INC_INV	Inbound
ES_SII_DEREGI_OUT_INV_REQUEST	ES_SII_DEREG_OUT_INV	Outbound
ES_SII_DEREGI_OUT_INV_RESPONSE	ES_SII_DEREG_OUT_INV	Inbound
ES_SII_REGIST_IN_INV_REQUEST	ES_SII_REGIS_INC_INV	Outbound
ES_SII_REGIST_IN_INV_RESPONSE	ES_SII_REGIS_INC_INV	Inbound
ES_SII_REGIST_OUT_INV_REQUEST	ES_SII_REGIS_OUT_INV	Outbound
ES_SII_REGIST_OUT_INV_RESPONSE	ES_SII_REGIS_OUT_INV	Inbound
ES_SII_REGIST_OUT_PAY_REQUEST	ES_SII_REGIS_OUT_PAY	Outbound
ES_SII_REGIST_OUT_PAY_RESPONSE	ES_SII_REGIS_OUT_PAY	Inbound
ES_SII_REGIST_IN_PAY_REQUEST	ES_SII_REGIS_INC_PAY	Outbound
ES_SII_REGIST_IN_PAY_RESPONSE	ES_SII_REGIS_INC_PAY	Inbound
ES_SII_DEREGI_IN_PAY_REQUEST	ES_SII_DEREG_INC_PAY	Outbound
ES_SII_DEREGI_IN_PAY_RESPONSE	ES_SII_DEREG_INC_PAY	Inbound

For Canary Islands:

Interface ID	SOA Service Name	Direction
ES_CAN_DEREGI_IN_EXT_REQUEST	ES_CAN_EX_DE_INC_INV	Outbound
ES_CAN_DEREGI_IN_EXT_RESPONSE	ES_CAN_EX_DE_INC_INV	Inbound
ES_CAN_DEREGI_IN_INV_REQUEST	ES_CAN_DEREG_INC_INV	Outbound
ES_CAN_DEREGI_IN_INV_RESPONSE	ES_CAN_DEREG_INC_INV	Inbound
ES_CAN_DEREGI_IN_PAY_REQUEST	ES_CAN_DEREG_INC_PAY	Outbound
ES_CAN_DEREGI_IN_PAY_RESPONSE	ES_CAN_DEREG_INC_PAY	Inbound
ES_CAN_REGIST_IN_INV_REQUEST	ES_CAN_REGIS_INC_INV	Outbound
ES_CAN_REGIST_IN_INV_RESPONSE	ES_CAN_REGIS_INC_INV	Inbound
ES_CAN_REGIST_IN_PAY_REQUEST	ES_CAN_REGIS_INC_PAY	Outbound
ES_CAN_REGIST_IN_PAY_RESPONSE	ES_CAN_REGIS_INC_PAY	Inbound

Interface ID	SOA Service Name	Direction
ES_CAN_REGIST_OUT_EXT_REQUEST	ES_CAN_EX_RE_OUT_INV	Outbound
ES_CAN_REGIST_OUT_EXT_RE-SPONSE	ES_CAN_EX_RE_OUT_INV	Inbound
ES_CAN_REGIST_OUT_INV_REQUEST	ES_CAN_REGIS_OUT_INV	Outbound
ES_CAN_REGIST_OUT_INV_RE-SPONSE	ES_CAN_REGIS_OUT_INV	Inbound

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.

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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

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.

www.sap.com/contactsap

THE BEST RUN SAP