



Integration Guide | INTERNAL
2022-07-12

Portugal eInvoice: Setting Up SAP Integration Suite (SAP ERP, SAP S/4HANA) - Cloud Foundry

Content

- 1 Introduction. 3**
- 2 Prerequisites 4**
- 3 Connectivity Steps. 5**
 - 3.1 Setup of Secure Connection. 5
 - Retrieve and Save Public Certificates. 6
 - Upload the Certificates. 6
 - Authenticate Integration Flows. 7
 - 3.2 Set Up SAP Integration Suite Tenants. 8
- 4 Configuration Steps in SAP Integration Suite. 9**
 - 4.1 General Information 9
 - 4.2 Copying Integration Flows. 9
 - 4.3 Configuring Integration Flows. 10
 - Configuring Portugal: Send Invoice. 10
 - Configuring Portugal: Receive Message. 12
 - 4.4 Service Provider. 12
 - Creating a Custom Role 13
 - Sharing Details with the Service Provider. 13
 - Creating Credentials. 14
- 5 Configuration Steps in Back-End Systems. 16**
 - 5.1 Creating Logical Ports in SOAMANAGER. 16
- 6 Testing the Integration. 22**

1 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

Although the service name **SAP Integration Suite** is used in the guide title and throughout the guide, this guide **also applies to SAP Cloud Integration running in the Cloud Foundry environment**. If you were onboarded before July 2020, the service you use is SAP Cloud Integration. The initial setup steps for the two services are different, while the integration flow settings and configuration steps in your back-end system are the same. See the **Prerequisites** section for their respective initial setup steps.

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 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 Document and Reporting Compliance Solution.
2. You have set up your tenant as follows:
 - If you have subscribed to Process Integration, perform all the initial setup steps described in [Initial Setup of SAP Cloud Integration in Cloud Foundry Environment](#).
 - If you have subscribed to Integration Suite, perform all the initial setup steps described in [Initial Setup](#).

i Note

SAP Document and Reporting Compliance requires the **Cloud Integration capability**. You need to activate this capability in the step **Provisioning the Capabilities**.

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 Integration Suite. For more information, see [Connecting a Customer System to Cloud Integration](#).

Inbound HTTP connections are not required for Portugal. 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](#).

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

3.1.1 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.

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 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.

3.1.3 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 certificate. 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`).

3.2 Set Up SAP Integration Suite Tenants

SAP Integration Suite 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.

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 Configuration Steps in SAP Integration Suite

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

4.1 General Information

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

Integration Flows for eDocument for Portugal

Integration Flow Name in WebUI	Project Name/Artifact Name
Portugal Send Invoice	com.sap.GS.Portugal.SendInvoice
Portugal Receive Message	com.sap.GS.Portugal.ReceiveMessage

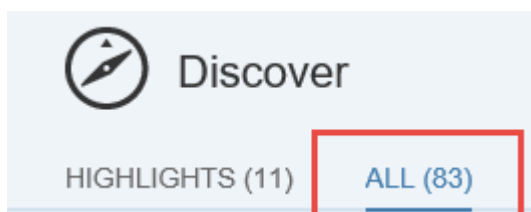
4.2 Copying Integration Flows

Context

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

Procedure

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 Portugal**.
4. Select the Package and choose [Copy](#).

4.3 Configuring Integration Flows

Provides instructions for configuring integration flows.

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

There are 2 [Artifacts](#) in the integration package SAP Document and Reporting Compliance: Electronic Invoicing for Portugal:

- Portugal: Send Invoice
- Portugal: Receive Message

i Note

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

4.3.1 Configuring Portugal: Send Invoice

Provides instructions for configuring integration flow for Portugal: Send Invoice.

Procedure

1. Choose **Actions > 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 `Enable Logging` parameter to configure whether you want to activate logging functionally for all the messages:

Value	Description
true	The system adds log files to a message.
false	Logging disabled.

- Use the `PROD_API_URL` and `TEST_API_URL` parameters to configure the URL address of the service provider API endpoint for productive and test system respectively.

Configure "Portugal Send Invoice"

Sender **More**

Type: All Parameters

Enable Logging: true

Mode: TEST

PROD_API_URL: https://

TEST_API_URL: https://

2. Choose the *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.

Configure "Portugal Send Invoice"

Sender More

Sender: Sender

Adapter Type: SOAP

Connection

Address: /PortugalSendInvoice

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

4.3.2 Configuring Portugal: Receive Message

Provides instructions for configuring integration flow for Portugal: Receive Message.

Procedure

1. Choose **Actions > Configure > More** tab (in some versions it may be *Externalized Parameters*)
 - o Select *Partner_PushMessage* as sender.
 - o Under Connections, use *DCPortugal.ReceiveMessage* as user role.

Note

If you choose a user role other than *DCPortugal.ReceiveMessage*, then ensure that you use the same role name when you create a custom role.

The screenshot shows a configuration form with the following fields:

- Sender:** Partner_PushMessage
- Adapter Type:** HTTPS
- Address:** /PortugalReceiveMessages
- Authorization:** User Role
- User Role:** DCPortugal.ReceiveMessage (highlighted with a red box)

A "Select" button is located to the right of the User Role field.

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

4.4 Service Provider

Provides a description of the service provider.

Saphety is one of the registered service providers for signing elinvoices in Portugal. SAP establishes communication with Saphety.

eSPAP (Entidade de Servicos Partihados da Administracao Publica, I.P.) is the Portuguese government organization responsible for elInvoice. It provides the formats of elInvoice for Portugal.

A customer is an organization with tax identification. A customer is identified in Saphety's network by its country code and tax identification, for example: PT123456789. Handling multiple tax identifications is possible. Each tax identification is a different customer.

Each customer requires a provisioning process.

4.4.1 Creating a Custom Role

The integration package requires that you create a custom role for the authentication in SAP Integration Suite

Prerequisites

- You must have created a subaccount as described in [Creating a Subaccount and Enabling Cloud Foundry](#) and you did not assign the standard user role.

Procedure

- Go to the tenant URL <https://<tenant>.cfapps.<data center>.hana.ondemand.com/itspaces>.
- In the *Operations* view, click the *User Roles* tile.
- Choose *Add* and enter a role name (such as **DCPortugal.ReceiveMessage**) and a role description and click *Add*.

For more information, see [Managing Custom Roles in the Cloud Foundry Environment](#).

- To assign the custom role to the integration, go to *SAP BTP cockpit*, choose your subaccount and create an instance as described in this topic [Creating Service Instances](#).

i Note

In step 3.e, enter the user role you created in step 3 as described in this document. To do so, go back to the *Operations* view, choose the user role you created and choose *Download JSON* to get the user role in JASON format. Enter the code in the text field and choose *Next*.

- Proceed with the steps to create a service key as described in [Creating Service Instances](#).

You generate a service key that holds the authentication information with the custom role.

4.4.2 Sharing Details with the Service Provider

Provides a description of how to share details with the service provider.

In SAP Integration Suite, go to **Operations** > *Manage Integration Content* > *All* and search for *Portugal Receive Message*.

Share the following details with the service provider: Service URL (see highlighted part in screenshot), Technical User ID, Password.

Portugal Receive Message

[Restart](#) [Undeploy](#) [Download](#)

Deployed On: [REDACTED] ID: com.sap.GS.Portugal.ReceiveMessage

Deployed By: [REDACTED] Version: 1.0.0

Package: SAP Document Compliance: Electronic Invoicing for Portugal

[Endpoints](#) [Status Details](#) [Artifact Details](#) [Log Configuration](#)

https://[REDACTED]hana.ondemand.com/cxf/PortugalDeleteMessages	
WSDL	
WSDL without policies	
https://[REDACTED]hana.ondemand.com/http/PortugalReceiveMessages	
https://[REDACTED]hana.ondemand.com/cxf/PortugalPullMessages	
WSDL	
WSDL without policies	

⚠ Caution

- If the service provider informs you with the error code “404”, check if the integration flow was successfully deployed and the URL is available to receive the messages
- If the service provider informs with the error code “403”, check the following details:
 - The technical user is assigned with an appropriate role (DCPortugal.ReceiveMessage)
 - The user credentials are correct.

4.4.3 Creating Credentials

Provides a description of how to enter the credentials from the service provider in SAP Integration Suite

Context

To get access to the webservice provided by the service provider, the credentials received from the service provider are entered in SAP Integration Suite.

Procedure

1. Access the SAP BTP cockpit and navigate to your subaccount (tenant).

2. Choose the [Subscriptions](#) link to display the subscriptions for your account
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/itspaces>, 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. Choose [Add User Credentials](#) and enter the following data and choose [Deploy](#) to save the changes.

Option	Description
Name	<p><VAT_code>_<SystemType></p> <p>where <VAT_code> is the company's VAT in the SAP system</p> <p><SystemType> is TEST or PROD depending on the type of your tenant</p> <p>Example: PT123456789_TEST</p>
Description	Enter the name of the company.
User	Enter the username from the service provider.
Password	Enter the password received from the service provider.

6. Choose [Deploy](#) to save the changes.

5 Configuration Steps in Back-End Systems

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

5.1 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](#) .

Service Administration | Technical Administration | Logs and Traces | Management Connections | Services

Identifiable Business Context
Define Identifiable Business Contexts (IBCs)

Identifiable Business Context Reference
Define Identifiable Business Context references (IBC reference)

Design Time Cache
Display central design time cache

Web Service Configuration
Configure service definitions, consumer proxies and service groups

Simplified Web Service Configuration
Configure service definitions for Web service consumers with limited capabilities

Logon Data Management
Define logon data used by business scenario configuration

Pending Tasks
Process pending tasks generated by business scenario configuration

Local Integration Scenario Configuration
Configure multiple service definitions and service groups supporting change management

Logical Determination of Receiver using ServiceGroups
Define rules for determining receiver IBC reference during service group runtime

Logical Determination of Receiver, Sender, and Authentication using Consumer Factories
Define rules for determining receiver IBC, sender IBC reference and authentication method during consumer factory runtime

Web Service Isolation
Tool to isolate service definitions and consumer proxies

- Find the proxies for SAP Document and Reporting Compliance for Portugal with search term `CO_EDO_PT*`.

Search criteria

Object Type is All

Object Name contains

Maximum Number of Results: 100

Search Clear values Reset search criteria

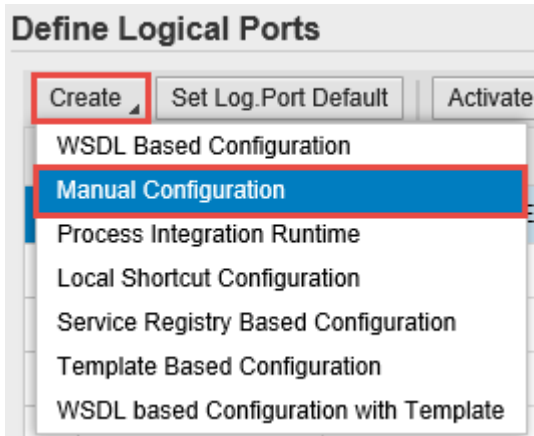
Enter the search term here

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

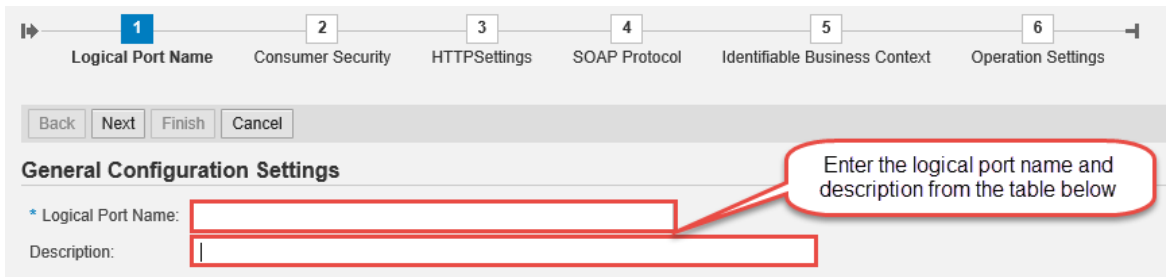
List of Proxies, Logical Port Names, and Paths

Proxy Name	Logical Port Name	Description	Path
CO_EDO_PT_SEND_IN-VOICE_V1_0	EDO_PT_SEND_INVOICE	eDocument Portugal - Send Invoice	/cxf/PortugalSendInvoice
CO_EDO_PT_SEND_CREDITNOTE_V1_0	EDO_PT_SEND_CREDITNOTE	eDocument Portugal – Send Credit Note	/cxf/PortugalSendInvoice
CO_EDO_PT_RECEIVE_MESSAGE_V1_0	EDO_PT_PULL_MESSAGE	eDocument Portugal – Pull Message	/cxf/PortugalPullMessages
CO_EDO_PT_RECEIVE_MESSAGE_V1_0	EDO_PT_DELETE_MESSAGE	eDocument Portugal – Delete Message	/cxf/PortugalDeleteMessages

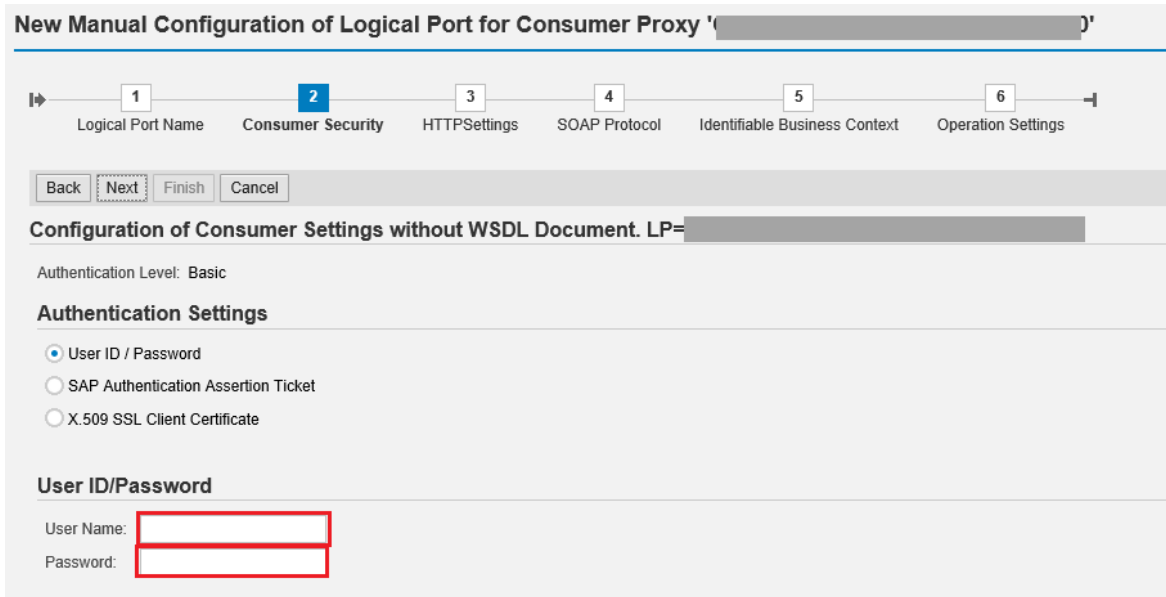
- In the *Result List*, select a proxy and create a logical port for each proxy. Choose **Create** **Manual Configuration**.



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 back-end system and SAP Integration Suite.



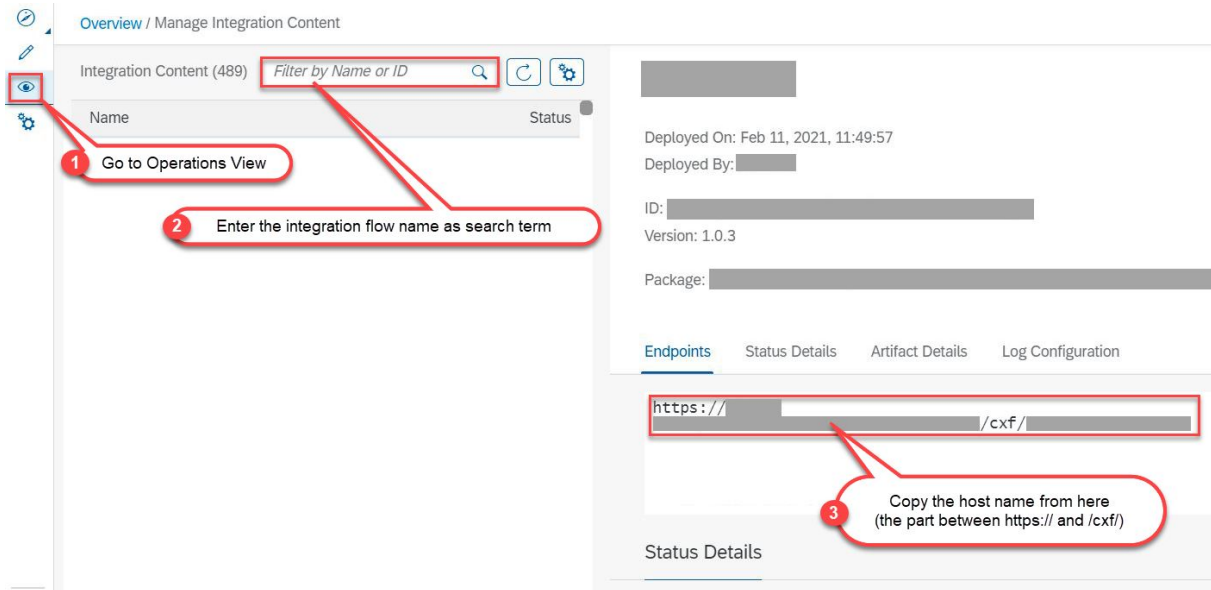
- If you use the basic authentication for *User Name*, enter the value for the **clientid** and for *Password*, enter the value for **clientsecret**. You have created these values for your service instance in SAP Integration Suite. See [Creating Service Instances](#).

- If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have uploaded to *STRUST*. Export the SSL Client PSE of the *STRUST* transaction. You must configure this certificate in SAP Integration Suite too. For that you create a service instance using the required *grant_type* as explained in [Creating a Service Instance in the Cloud Foundry Environment](#). After the instance creation, you create the service key using the certificate exported from *STRUST* as explained in [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.

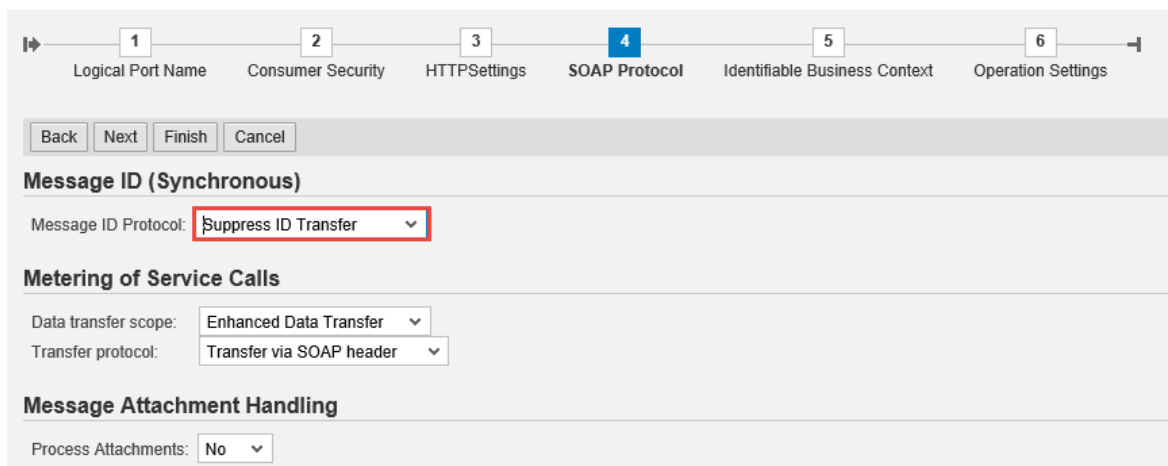
To find the Host, go to SAP Integration Suite Web UI and under Managed Integration Content, go to **Monitor** **All**. Use the search to find your integration flow as in the screenshot below:



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.

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



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

SAP Integration Suite 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 Integration Suite service and execute a connection test. In case of a successful connection, you receive an error with HTTP return code 500.

Remember to create logical port(s) for each proxy 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

6 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 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 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.

© 2022 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.