Integration Guide | PUBLIC
2022-07-04

Colombia eInvoice: Setting up SAP Integration Suite (SAP ERP, SAP S/4HANA) - Cloud Foundry Environment

THE BEST RUN

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 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.

3 Prerequisites

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

1. You have installed in the test and productive systems all necessary SAP Notes for the Document and Reporting Compliance Solution.
2. You have set up your tenant as follows:
   - 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**.

3.1 Registration at Tax Authorities' System

You have completed the registration at the Colombian Tax Authorities, DIAN, and the following data is available:

- Certificate for digital signature (Private Key and Password)
- Approved ranger number
- User ID and Password to connect to DIAN's portal
- You find information about the authentication data at DIAN's web page under factura electronica:
  - Documentación y Normatividad tab: Official documents and regulations
  - Manuales y video tab: User guides

.

> i Note
>
> The information above mentioned is of responsibility of DIAN. SAP cannot be made liable for its correctness and accuracy.

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 Integration Suite. 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, 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 8].

4.1.1 Retrieve and Save Public Certificates

Context

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

Procedure

1. Access the SAP BTP cockpit, and navigate to your subaccount (tenant) page.
2. Click the subscriptions link to display the subscriptions for your subaccount.
3. Use the tenant URL you created as defined in the prerequisites of this document. The URL has the following format: `https://<tenant>.cfapps.<data center>.hana.ondemand.com`, where <tenant> corresponds to the dynamic part and is unique for each subaccount and <data center> corresponds to the data center you are using.
4. In the *Operations* view, choose *Manage Integration Content* and select *All* to display the integration flows available.
5. Select an integration flow to display its details.
6. Copy the URL listed within the *Endpoints* tab, and paste the URL into your web browser.
7. When prompted by the *Website Identification* window, choose *View certificate*.
8. Select the root certificate, and then choose *Export to file* to save the certificate locally.
9. Repeat these steps for each unique root, intermediate and leaf certificate, and repeat for both your test and production tenants.

4.1.2 Upload the Certificates

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

Context

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

Procedure

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

4.1.3 Authenticate Integration Flows

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

Context

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

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

Procedure

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

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

   The CA may have specific requirements and request company-specific data, they may also require time to analyze your company before issuing a signed certicate. When signed, the CA provides the certificate for import.
5. Navigate to the PSE for **SSL Client Standard** and open it by double-clicking the PSE.
6. Switch to edit mode.
7. Choose the *Import certificate* button.

8. In the *Import Certificate* dialog box, enter or select the path to the CA-signed certificate and choose *Enter*. The certificate is displayed in the *Certificate* area.
9. Choose *Add to Certificate List* to add the signed certificate to the *Certificate List*.

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

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

5 Configuration Steps in SAP Integration Suite

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

5.1 General Information

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

Integration flows for Document and Reporting Compliance for Colombia

Integration Flow Name in WebUI	Project Name/Artifact Name
Send Invoice	com.sap.GS.Colombia.GenericInvoice
Get Status	com.sap.GS.Colombia.GetStatus
Query Ranges	com.sap.GS.Colombia.GetRanges
Attached Document	com.sap.GS.Colombia.Attachment
Subsequent Document	com.sap.GS.Colombia.SubSqntDoc

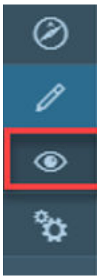
5.2 Deploying Key Pairs

Context

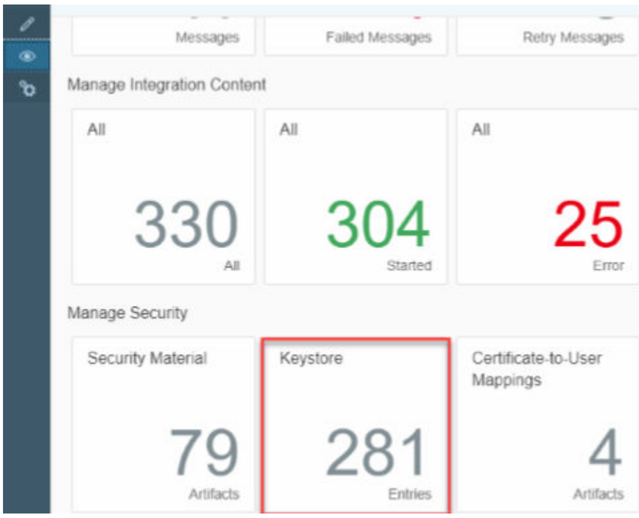
You deploy the key pairs to the SAP Integration Suite tenants.

Procedure

1. Go to overview tab by clicking on the following button.



2. Open Keystore as shown as follows.

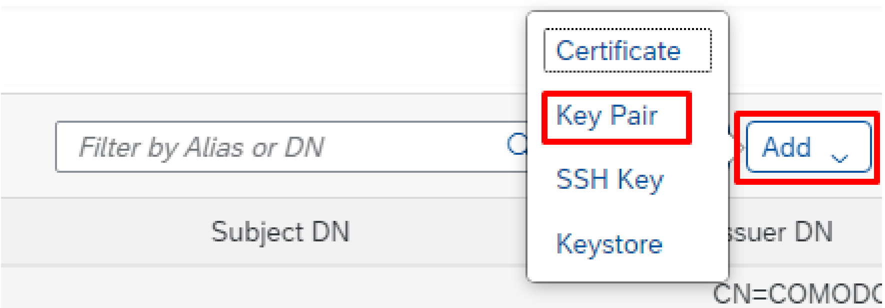


3. Deploy the Key Pair (as private key with alias) in the tenants JAVA_KEYSTORE.

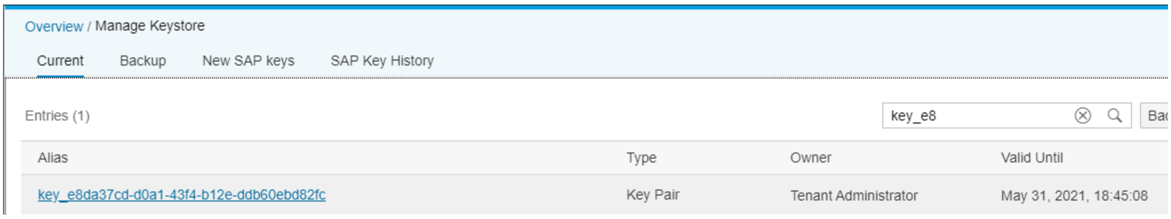
   To allow the integration flows to be updated with minimal adaptation effort, use the alias for the private key as follows: Private Key alias (relevant only for all integration flows): key_(SoftwareID of company that created electronic document). Example: key_e8da37cd-d0a1-43f4-b12e-ddu60ehd82fc

   > **i Note**
   >
   > Private key alias should be created for all unique software ID's used in customer's back-end system.

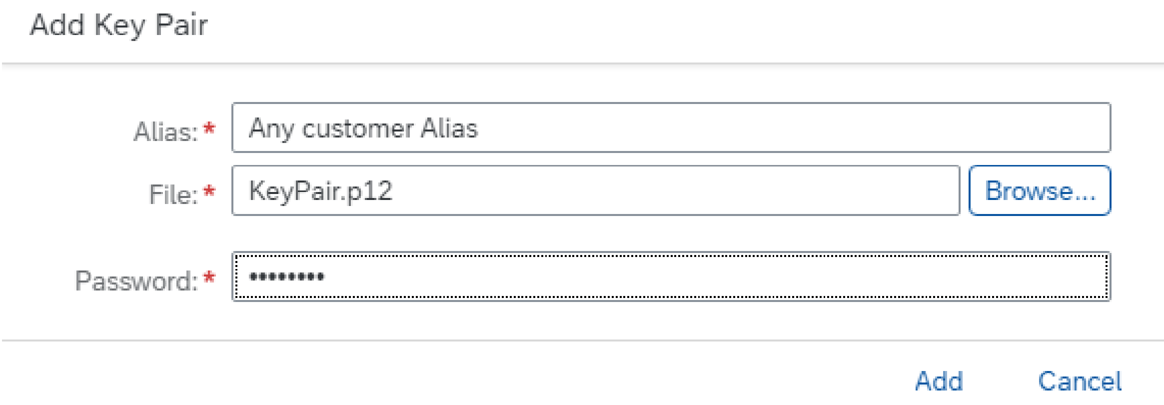
4. Deploy the key pair which is generated in the step above.
5. Go to *Add* > *Key Pair* to add the new Key Pair to the list.



6. Enter the Alias, File and key pair and password to connect to DIAN.



Complete the information related to your key pairs provided by DIAN:



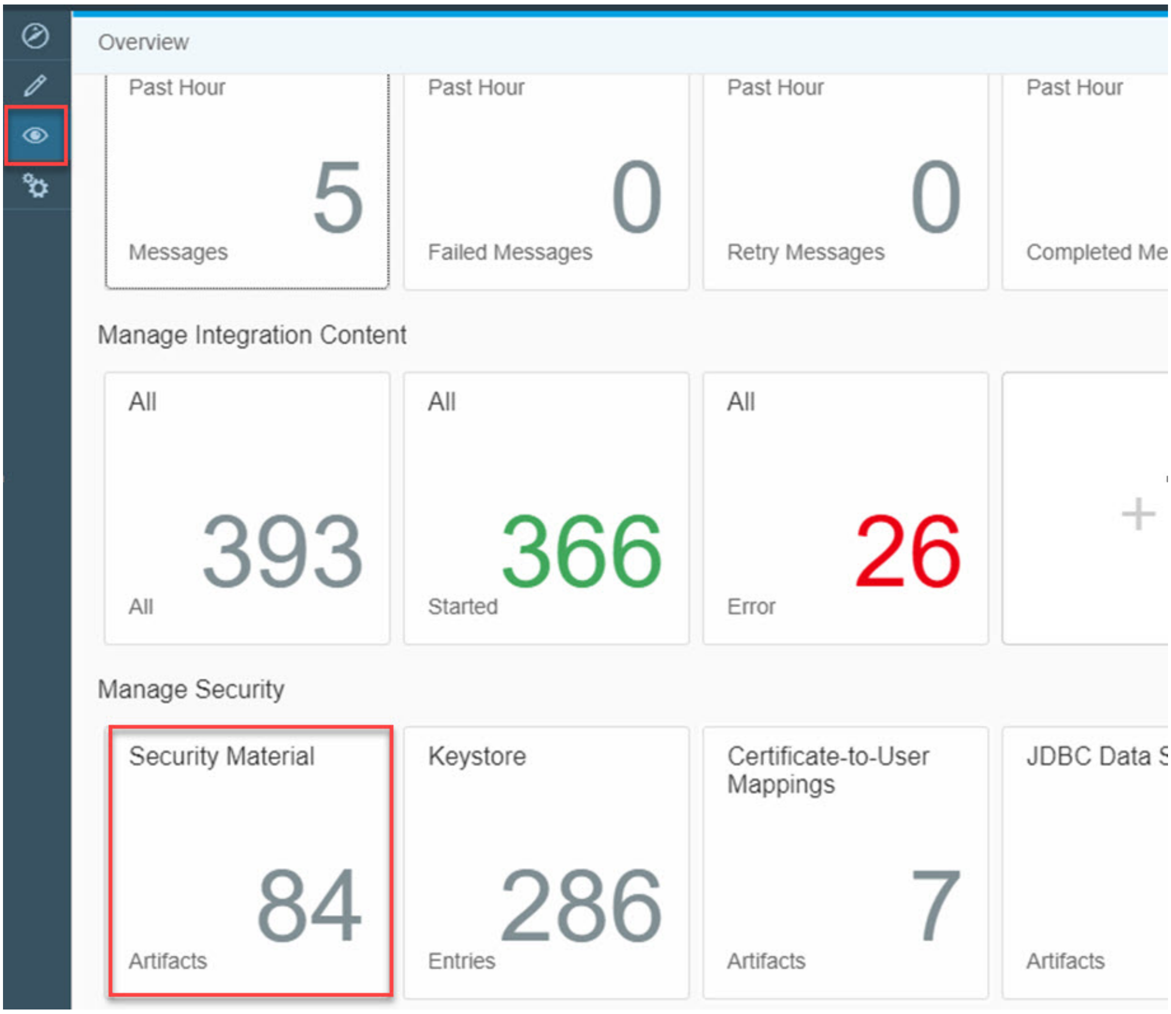
5.3 Deploying Secure Parameters

Context

You deploy the secure parameters to the SAP Integration Suite tenants.

Procedure

1. In the *Overview* tab, choose *Security Material*.

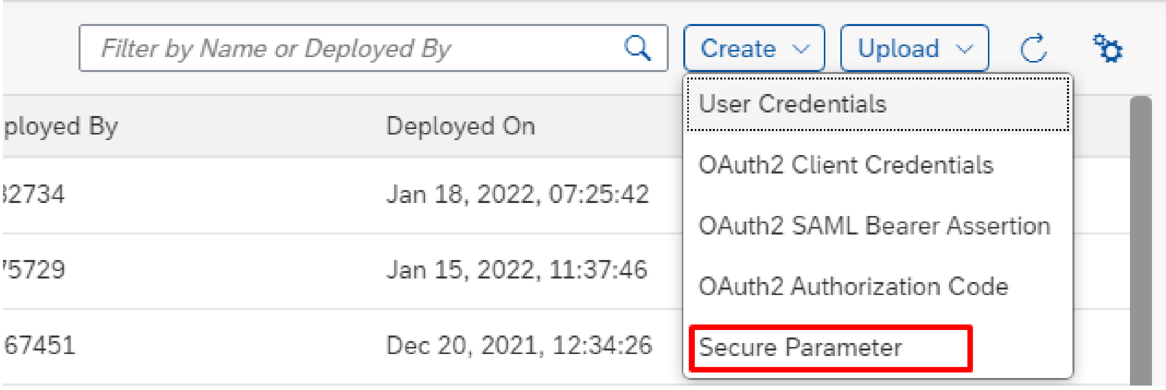


2. Deploy the Secure Parameter in the tenants JAVA_KEYSTORE.

   To allow the integration flows to be updated with minimal adaptation effort, use the alias for the secure parameter as follows: Secure Parameter alias (relevant only for Generic invoice): edoc_co_setid_(SoftwareID of company that created electronic document). Example: edoc_co_setid_e8da37cd-d0a1-43f4-b12e-ddu60ehd82fc

   > **i Note**
   >
   > Secure Parameter alias should be created for all unique software ID's used in customer's back-end system.

3. Deploy the Secure Parameter which is generated in the step above.
4. Go to Add Secure Parameter to add the new secure parameter to the list.



5. Enter the name of Secure Parameter as provided in example, and fill Secure Parameter field with the test Set ID provided by DIAN for habilitation mode.

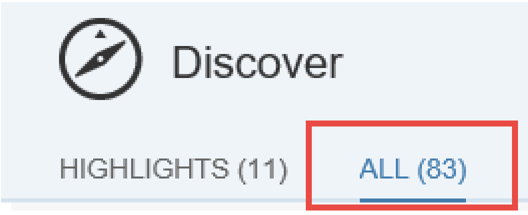
5.4 Copying Integration Flows

Context

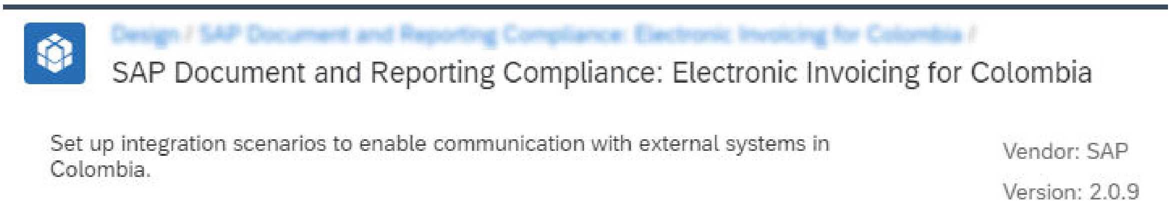
Copy all integration flows in the package SAP Document and Reporting Compliance: Electronic Invoicing for Colombia to the target tenant as follows:

Procedure

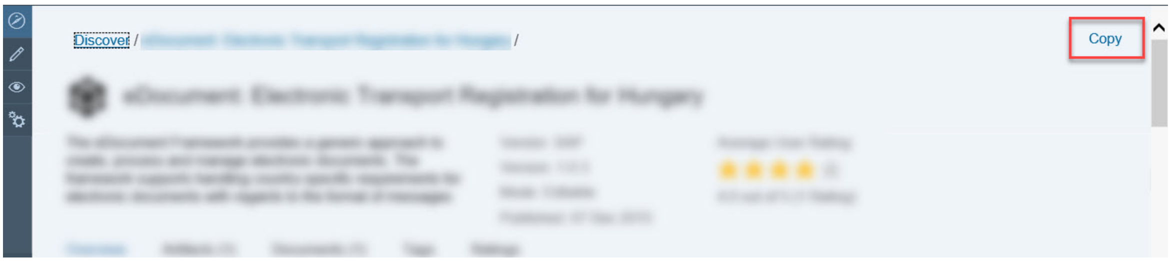
1. In your browser, go to the WebUI of the tenant (URL: <Tenant URL>/itspaces/#shell/discover).
2. Choose *Discover* > *All* > . .



3. Search for **SAP Document and Reporting Compliance: Electronic Invoicing for Colombia**.



4. Select the Package and choose *Copy*.



5.5 Configuring Integration Flows

Context

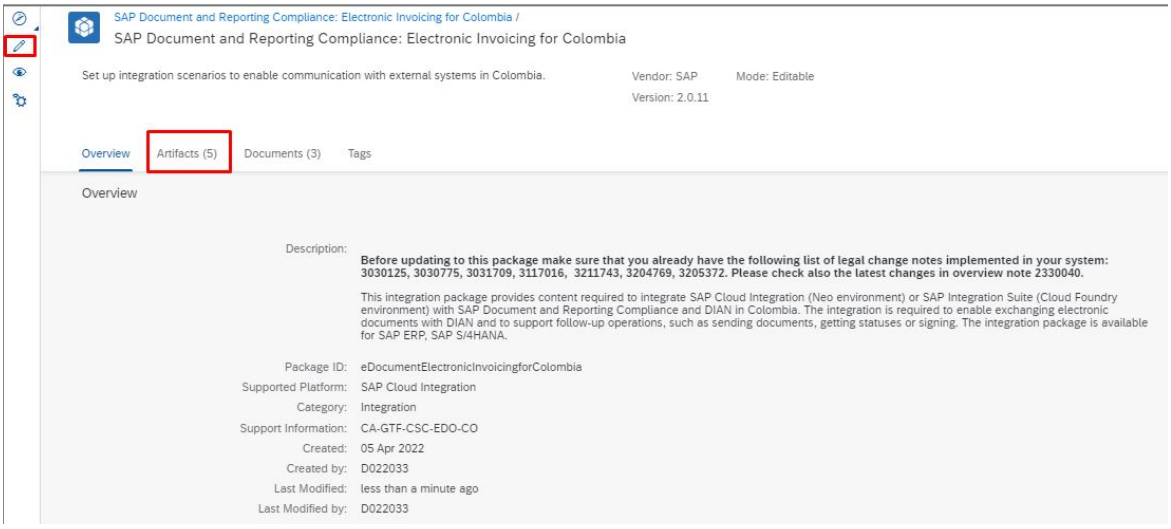
You configure the package that you have copied as described in .

Procedure

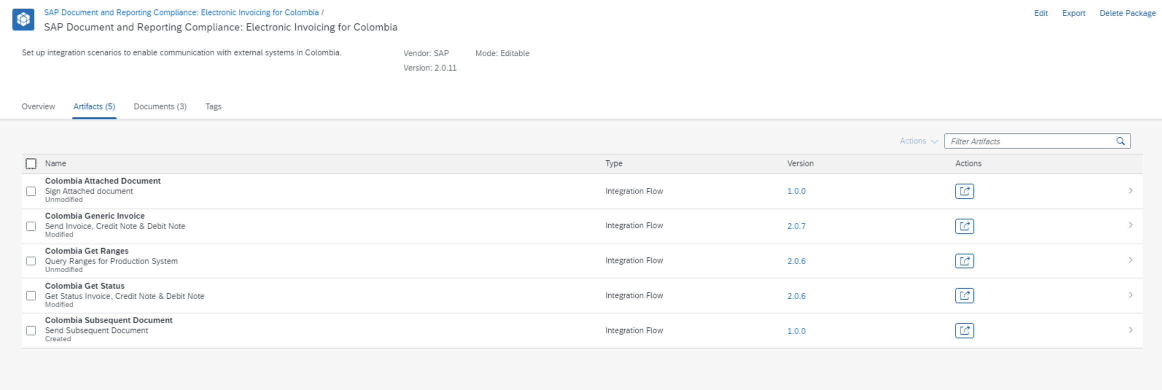
1. There are 5 *Artifacts* in the integration package SAP Document and Reporting Compliance: Electronic Invoicing for Colombia:
    - Attached Document
    - Generic Invoice
    - Get Ranges
    - Get Status

- Subsequent Document

2. Go to the previously imported package on the Design tab and open *Artifacts*.



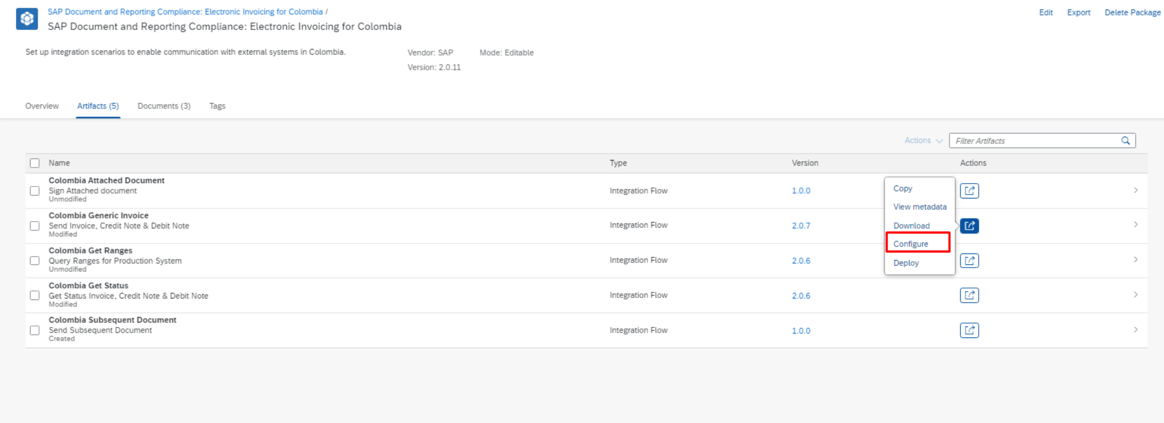
3. Choose either *Actions* > *Generic Invoice*, *Actions* > *Get Status*, or *Actions* > *Subsequent Document*, depending on which artifact you are configuring.



i Note

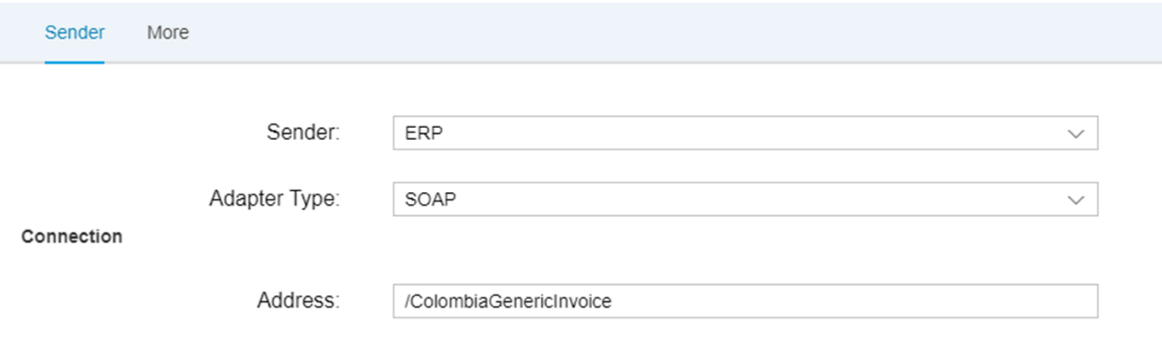
The version of the integration on the screenshot may differ from the one in your tenant.

4. When you configure Generic Invoice integration flow, choose *Actions* > *Configure* to open configuration for it.

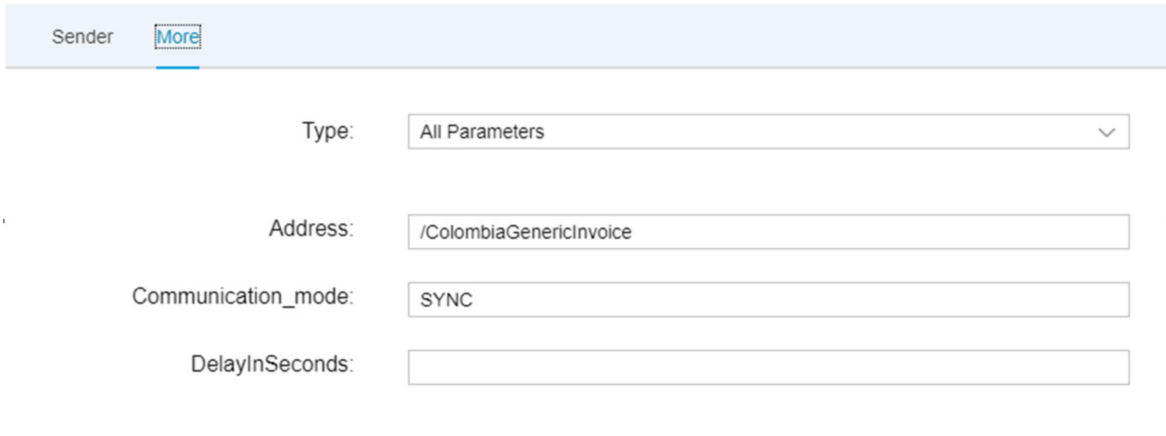


5. Choose *Configure* > *Sender* tab.

   Use the Address parameter to set up the integration package address.



6. Choose *Configure* > *More* tab. You maintain the value from your Keystore, that was previously created as alias for you Key Pair to the *Private_key* field.



7. Define the value in the following fields as required.

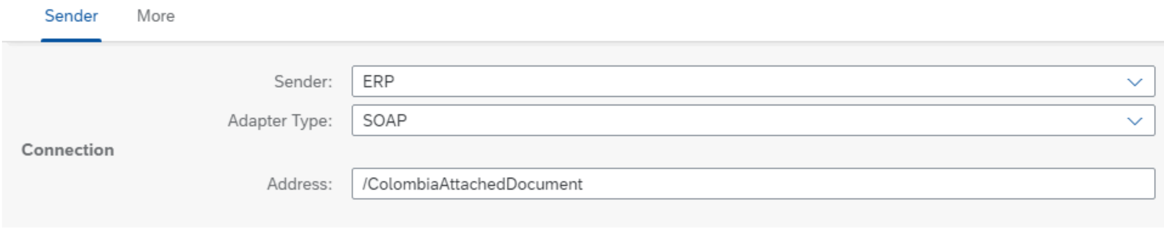
Field	Explanation
Communication_mode	Define the mode of communication with the tax authority. Possible values are SYNC, ASYNC, or HABILITATION.

Field	Explanation
DelayInSeconds	Define the delay in seconds after the signature is performed.
Usage_Mode	**i Note** Required only for the Get Status artifact. Possible values are TEST or PROD.

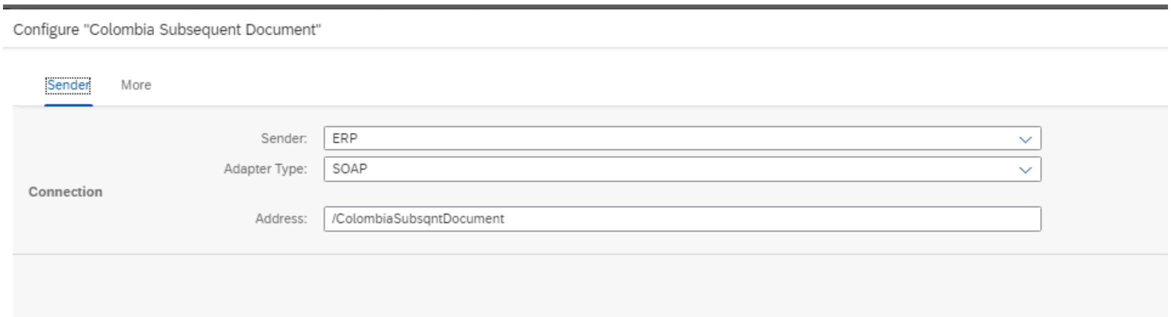
> **i Note**
>
> These values of *Communication_mode* have their own functionality as shown in the table below.
>
> Functionality of Three Communication_mode
>
> | Communication_mode | Description |
> |---|---|
> | SYNC | You submit documents and get responses immediately in one call (approval, rejection, etc). |
> | ASYNC | You submit the edocument and get trackid for it. (Later you can perform get status and get approval, rejection, etc.) |
> | HABILITATION | When customer is ready with tests, it is possible to switch to habilitation mode in order to submit 100 documents successfully and later go to production. |

8. When you configure Get Status integration flow, choose *Actions* > *Configure*. The same steps of configuration with Generic Invoice integration flow should be done to Get Status integration flow with only one difference in the *Address* field:

9. When you configure Get Status integration flow, choose *Actions* > *Configure*. The same steps of configuration with Get Status integration flow should be done to Attached Document integration flow with only one difference in the *Address* field:



10. When you configure Subsequent Document integration flow, choose *Actions* > *Configure*. The same steps of configuration with Get Status integration flow should be done to Subsequent Document integration flow with only one difference in the *Address* field:



5.6 Deploying Integration Flows

Shows you how to deploy the integration flows.

Context

Procedure

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

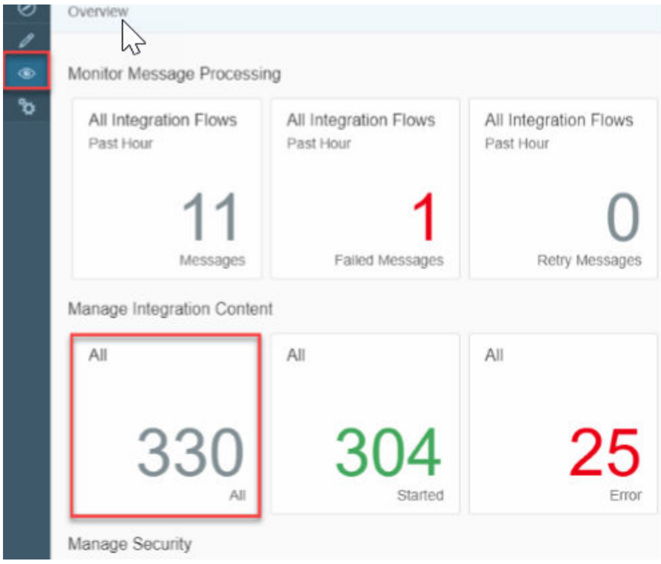
> **i Note**
>
> Depending on the version of your tenant, after pressing these buttons, a warning messages can appear. You can ignore these messages by choosing *Close* . The first two warnings are related to the payload attachments; currently the invoice registration process does not support or require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

5.7 Copying Addresses for SOAMANAGER

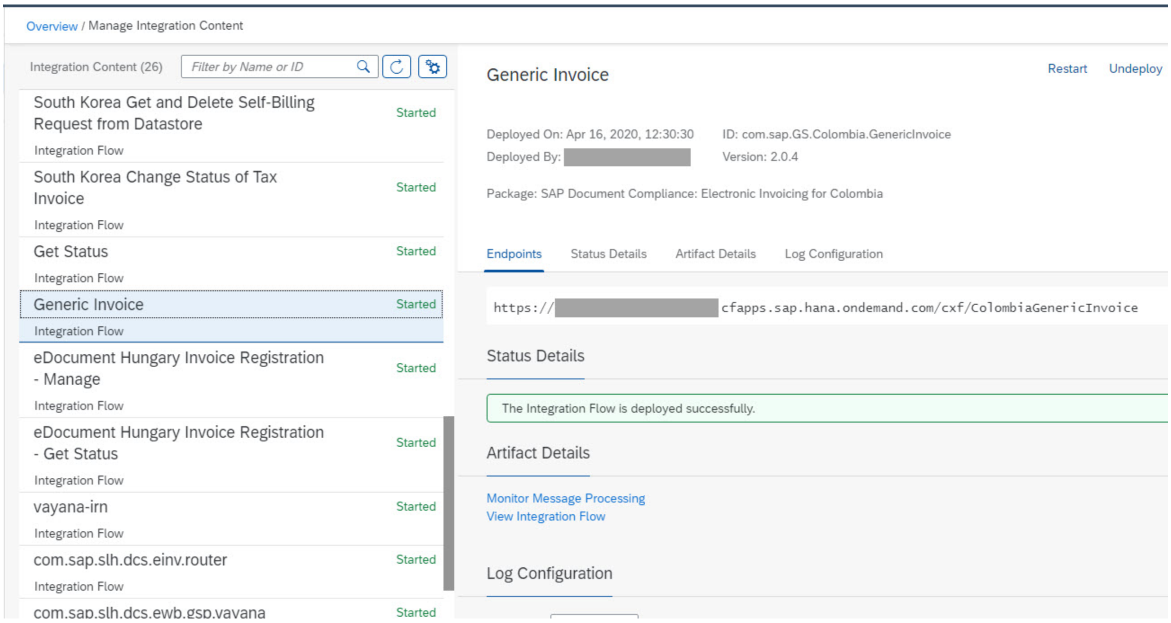
You copy addresses for integration flows for the preparation for the configuration for SOAMANAGER.

Procedure

1. Go to SAP Integration Suite content.



2. Copy address for generic invoice integration flow, get status integration flow, and subsequent document integration flow. Later you can use these addresses in the configuration for SOAMANAGER.



6 Configuration Steps in Back-End Systems

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

6.1 Creating Logical Ports in SOAMANAGER

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

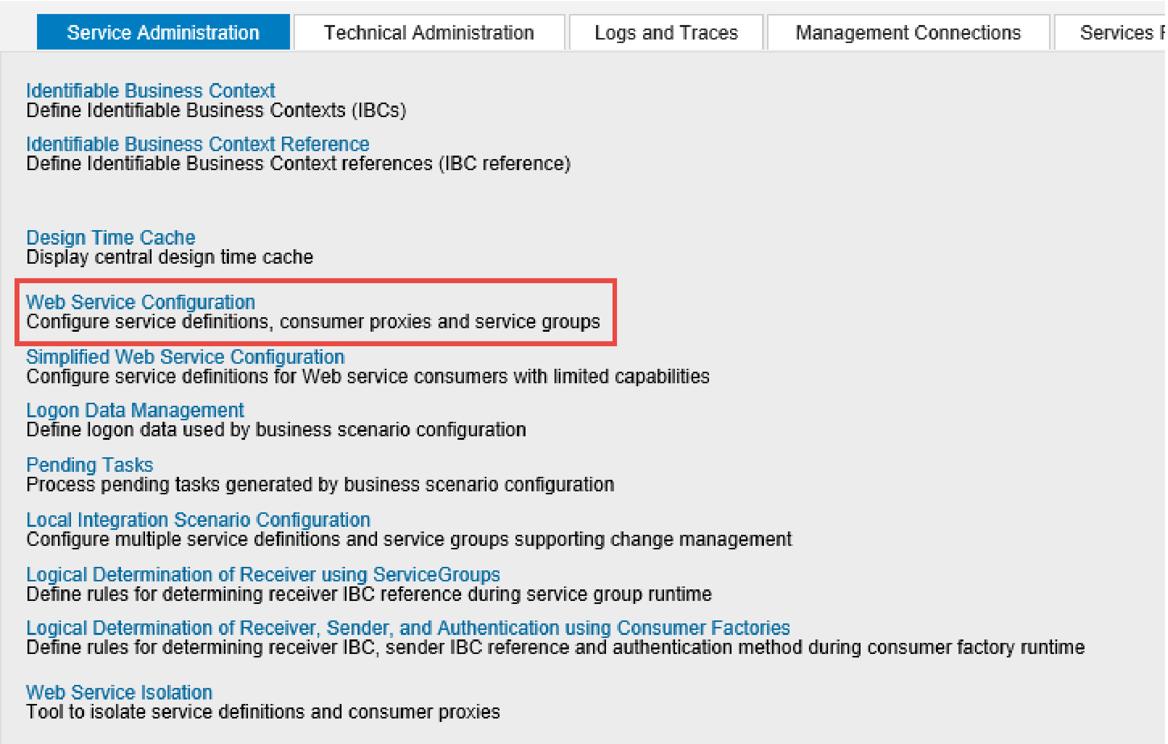
Context

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

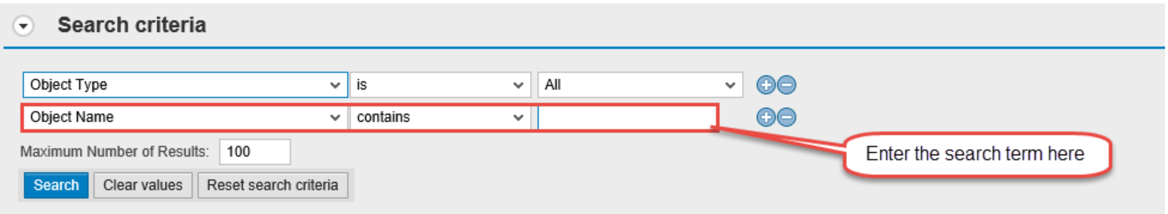
> **i Note**
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

Procedure

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



2. Find the proxies for eDocument for Colombia with search term `CO_EDO_CO*`.



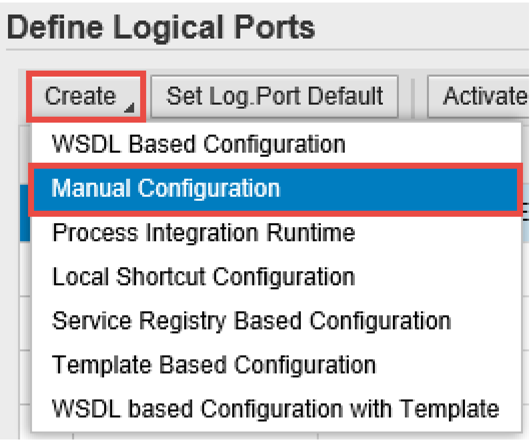
The following table lists the proxies and the logical port name, description and path for each proxy.

List of Proxies, Logical Port Names, and Paths

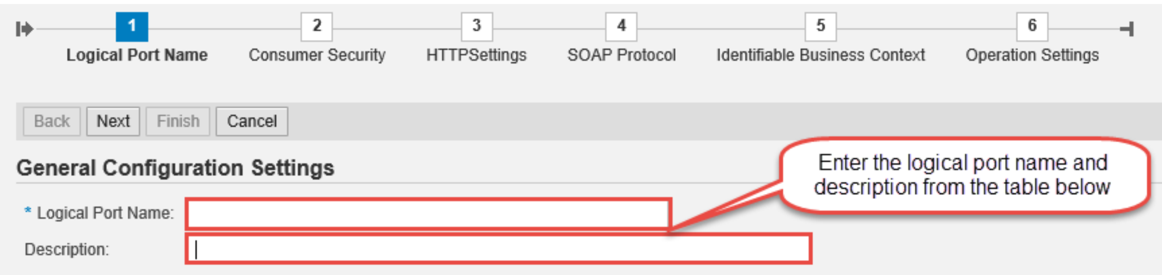
Proxy Name	Logical Port Name	Description	Path
CO_EDO_CO21_INVOICE_V2_0	EDO_CO_INVOICE_V2_TRANSM_SERV_PORT	Colombia eDocument - Invoice Transmission Service	/cxf/ColombiaGenericInvoice
CO_EDO_CO21_DEBIT_NOTE_V2_0	EDO_CO_DE_NOTE_V2_TRANSM_SERV_PORT	Colombia eDocument – Debit Note Transmission Service	/cxf/ColombiaGenericInvoice
CO_EDO_CO21_CREDIT_NOTE_V2_0	EDO_CO_CRE_NOTE_V2_TRANSM_SERV_PORT	Colombia eDocument – Credit Note Transmission Service	/cxf/ColombiaGenericInvoice

Proxy Name	Logical Port Name	Description	Path
CO_EDO_CO21_GET_STATUS_V2_0	EDO_CO_GET_STATUS_V2_PORT	Colombia eDocument - Query Transaction Get Status	/cxf/ColombiaGetStatus
CO_EDO_CO21_QUERY_RANGES_V2_0	EDO_CO_QUERY_RANGES_V2_PORT	Colombia eDocument - Query Ranges	/cxf/ColombiaQueryRanges
CO_EDO_CO21_ATTACHMENT_V2_0	EDO_CO_ATTACHMENT_V2_PORT	Colombia eDocument - Sign Attached Document	/cxf/ColombiaAttachedDocument
CO_EDO_CO21_SUBSQNTDOC_V1_0	EDO_CO_SUBSQNT_V_1_0	Colombia eDocument – Subsequent Documents	/cxf/ColombiaSubsqntDocument

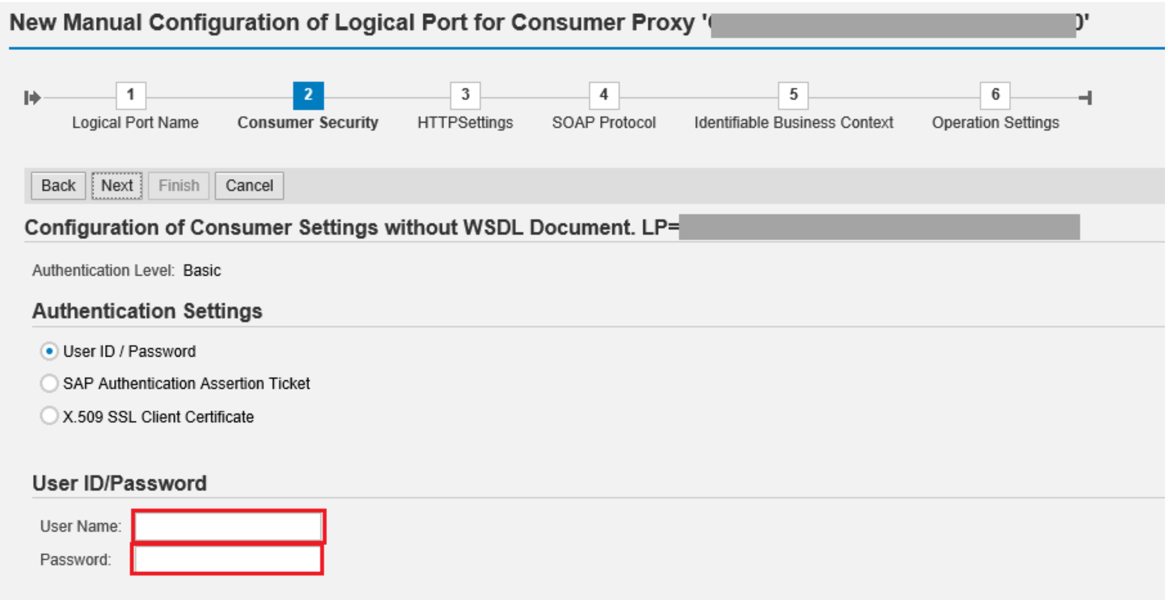
3. In the *Result List*, select a proxy and create a logical port for each proxy. Choose *Create* > *Manual Configuration*.



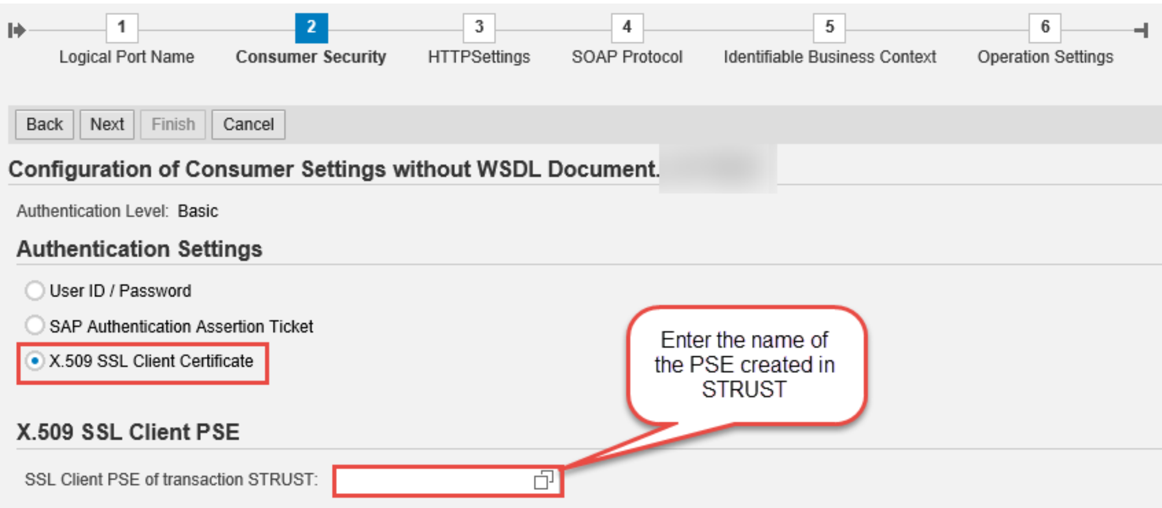
4. Enter the logical port name and a description.



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 back-end system and SAP Integration Suite.

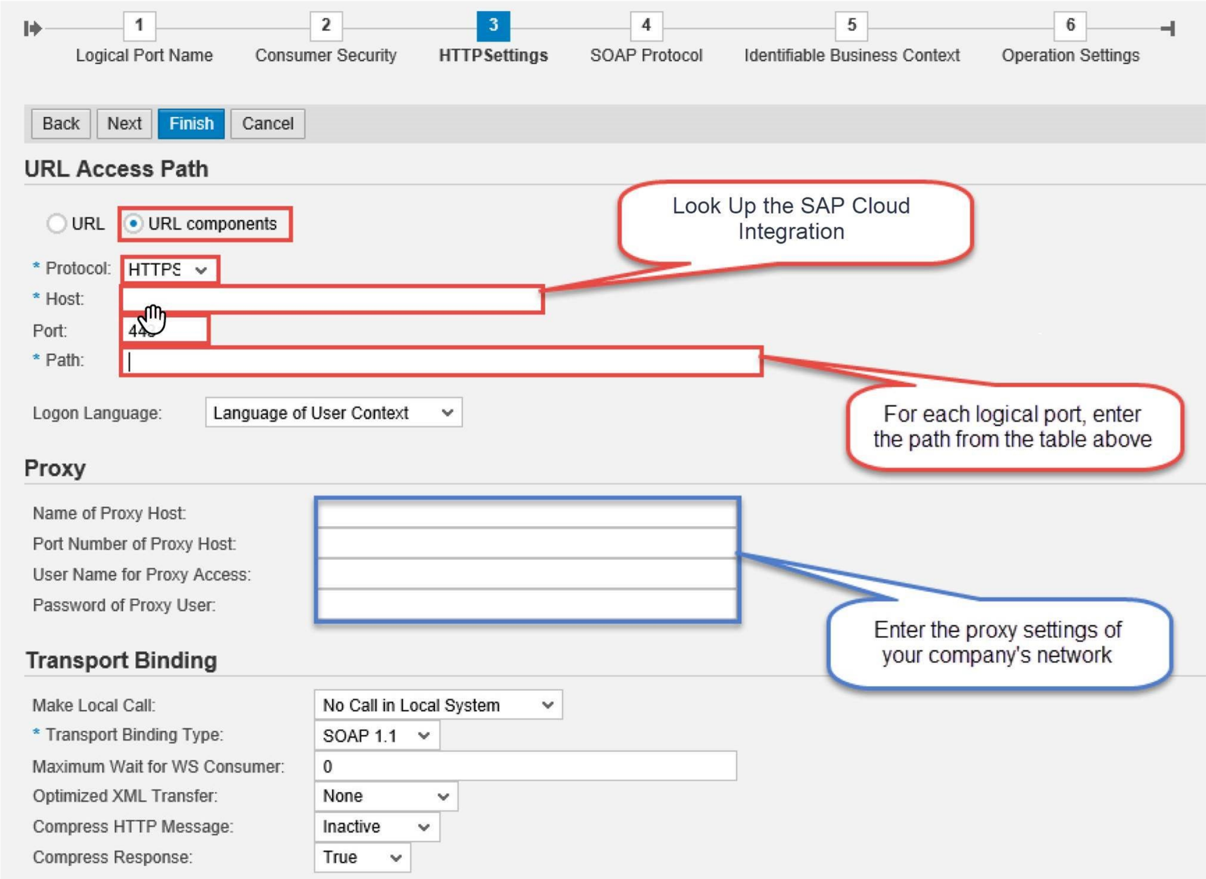


- If you use the basic authentication for *User Name*, enter the value for the **clientid** and for *Password*, enter the value for **clientsecret**. You have created these values for your service instance in SAP Integration Suite. See Creating Service Instances.



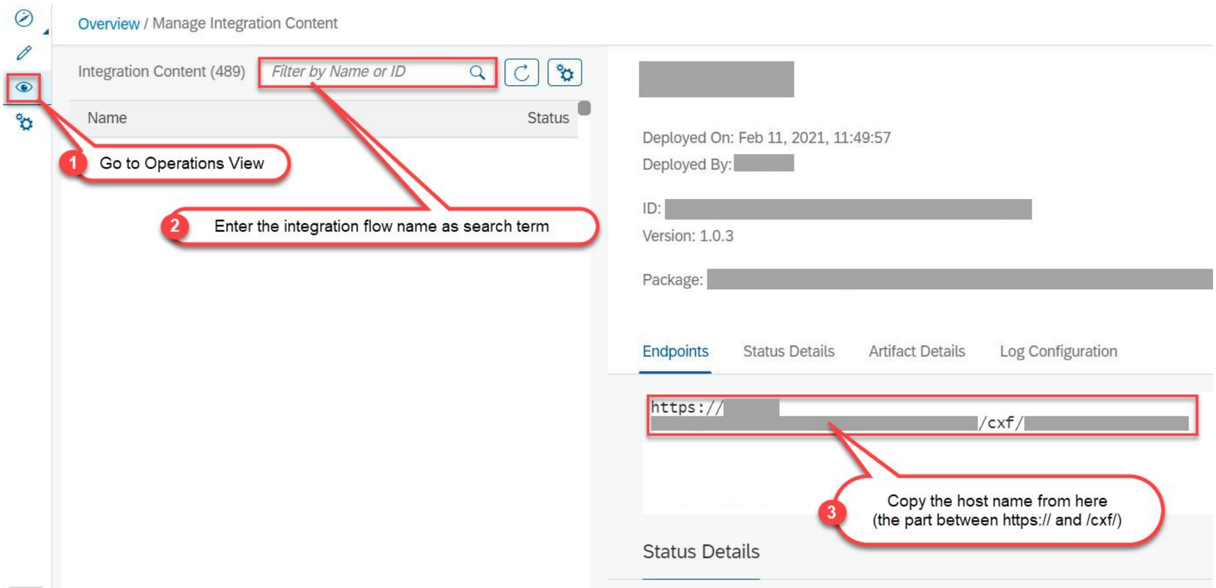
- If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have updloaded to `STRUST`. You must configure this certificate in SAP Integration Suite too. For that you create a service instance using the required grant_type. You create the service 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.

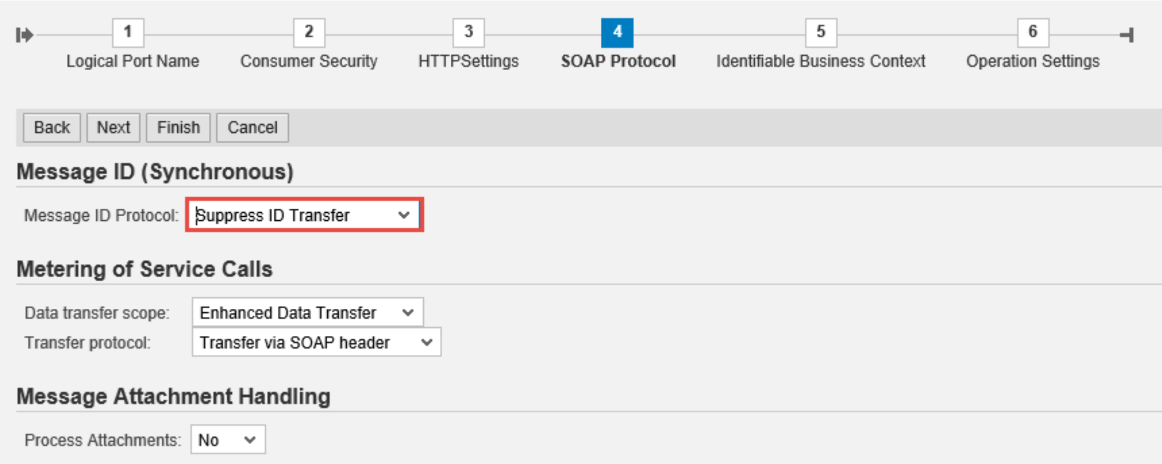
To find the Host, go to SAP Integration Suite Web UI and under Managed Integration Content, go to *Monitor* *All* . Use the search to find your integration flow as in the screenshot below:



i Note

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

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



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

SAP Integration Suite does not support WebService 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 2476827 for more information.

- Define the SOA service names and assign the logical ports to the combination of a SOA service name and a company code in `EDOSOASERV` view.
- Assign the SOA service names you created before to an interface ID in `EDOINTV` view

7 Testing the Integration

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

Context

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

www.sap.com/contactsap

THE BEST RUN