Integration Guide | PUBLIC
2024-09-02

Peru Electronic Documents: Setting Up SAP Integration Suite (SAP ERP, SAP S/4HANA, and SAP S/4HANA Cloud) - Cloud Foundry Environment

THE BEST RUN SAP

Content

1 Disclaimer

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

- The correctness of the external URLs is the responsibility of the host of the Web site. Please check the validity of the URLs on the corresponding Web sites.
- The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
- SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

2 Introduction

You use SAP 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.

> ⓘ 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.

> ⓘ 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.

> ⓘ 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 Installation of eDocuments Solution for Peru

You have installed and configured the eDocument solution in your test and productive systems. If you did not install the latest support package for your system, see the SAP Note 2031941 (for SAP ERP) or SAP Note 2651114 (for SAP S/4HANA) for the list of SAP Notes to be installed for Peru. For generic information about the installation of the eDocument Framework, refer to the SAP Note 2134248 (for SAP ERP) or SAP Note 2343822 (for SAP S/4HANA) for the installation guide of SAP Notes.

Application Help for eDocument

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

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

3.2 Registration at SUNAT/OSE

You have completed registration at SUNAT or, in case you use the services of a designated technology provider, termed Operator of Electronic Services (OSE), at the specific OSE.

In case of registration at SUNAT, you must have the following data available:

- Key pair certificate used for digital signature (Private Key Alias)
- SUNAT Web Server Certificates (for example, **GeoTrust Global CA**) for connecting to the SUNAT web service deployed on the SAP Integration Suite tenants' keystores
- SOL username registered with profile "Envio de documentos electronicos – Grandes emisores"
- Username and password that belong to the SOL username

> ⓘ Note
>
> In case there are any issues with SSL, you can open SUNAT's web service URL in a browser and check the certification path.

In case of registration at OSE, you must have the following data available:

- Key pair certificate used for digital signature (Private Key Alias)
- OSE Web Server Certificates (for example, GeoTrust Global CA) for connecting to the OSE web service deployed on the SAP Integration Suite tenants' keystores
- Username and password to connect to OSE

3.2.1 Generating Credentials

This section is only relevant for delivery notes.

Context

You are required to enroll the application that uses the REST services and generate its credentials (client_id and client_secret) on the tax authority's website.

This step needs to be done only once.

> ⓘ Note
>
> SAP cannot guarantee that the layout or content of the tax authority's page remains constant. SAP is not responsible for the layout and content of external web pages.

Procedure

Perform the following steps to generate your credentials.

1. Choose *Credenciales de API SUNAT* > *Credenciales de API SUNAT* > *Credenciales de API SUNAT* > *Gestión Credenciales de API SUNAT* in the SOL menu.
2. Click the *GRE Emision de Comprobantes/v1/contribuyente/gem* checkbox and select *Desktop* under *Alcance* in the *REGISTRE SU APLICACIÓN* window.
3. Click *Guardar*.

   Your credentials are now generated.

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.

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.

> **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 11].

4.1.1 Retrieve and Save Public Certificates

You perform this action in the back-end systems only if you are using certificate-based authentication. Not required for basic authentication.

Prerequisites

If you do not find any integration flows in your tenant then refer to and .

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 General Information

5.1 Integration Flows for Peru Electronic Invoicing

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

Integration Flow Name in WebUI	Project Names/Artifact Names
Peru Send Invoice And Get Status	com.sap.GS.Peru.GenericInvoiceGetStatus
Peru Get Status of Invoice and Summaries	com.sap.GS.Peru.GetStatusInvoice
Peru Send Summary Documents	com.sap.GS.Peru.SummaryDocuments
Peru Send Tax Certificate	com.sap.GS.Peru.TaxCertificate
Peru Send Voided Documents	com.sap.GS.Peru.VoidedDocuments
Peru Send Delivery Note	com.sap.GS.Peru.DeliveryNote
Peru Get Token	com.sap.GS.Peru.GetToken

5.1.1 Integration Flow Modes

Each integration flow in the package has two different ways of operating, the so-called modes. A mode controls the logic of the integration flow and the endpoint to which the message is sent. For each integration flow, you set up a mode in the externalized parameter called mode.

The following two modes exist:

Integration Flow Mode	Integration Flow Mode Name	Description
PROD	Production	• Intended for use in the productive SAP Integration Suite tenant • Connects to the SUNAT web service/REST APIs for production • Invoice, Credit Note, Debit Note, and Delivery Note: Boletas are only signed, but not sent to SUNAT • Available for all integration flows
TEST	Test	• Intended for use in the SAP Integration Suite test tenant • Connects to the SUNAT web service for testing • Invoice, Credit Note and Debit Note: Boletas are only signed, but not sent to SUNAT Available for all integration flows except Delivery Note

When you import the integration flows to the SAP Integration Suite tenant the first time, the TEST mode is the standard setting. For information about how to change the mode, see Download Integration Flows to Tenant Workspace and Adapt [page 19].

5.2 Value Mappings for Peru Electronic Invoicing

The package *SAP Document and Reporting Compliance: Electronic Documents for Peru* contains two value mapping artifacts: *Peru Configure SUNAT Error Code Mapping* and *Peru Configure SUNAT Error Code Mapping for Delivery Notes*, which includes value mappings for possible error codes from SUNAT. These value mappings is used in the *Peru Send Invoice and Get Status* and *Peru Send Delivery Note* integration flows.

If any error codes are missing, you can configure this artifact as required.

6 Configuration Steps in SAP Integration Suite

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

6.1 Deploy Key Pair, Certificates and Credentials to Tenants

The credentials (username + password) for the WS UsernameToken authentication differ depending on the endpoint of the integration flow which is determined by the mode. The credentials for mode **TEST** differ from the credentials of mode **PROD**.

You must make sure that the security elements (key pair certificate for digital signature + SSL Public Certificate) and the credentials are available.

Deploy the signature certificate (as key pair/key store with an alias) in the SAP Integration Suite tenants' KEYSTORE. Deploy the credentials as a **USER CREDENTIALS** object (with an alias).

To update the integration flows with minimal adaptation effort, the alias used for the private key and for the credential must be as follows:

- *Key pair alias*: **perusignaturekey**

  > ⓘ Note
  >
  > From version 2.0.5 onwards, the dynamic private key *Alias* is available, that is, you can choose to use an alias in the form of **`perusignaturekey_xxxxx`**, where **`perusignaturekey`** will be the suffix, and **`xxxxx`** will be you company tax ID. If you choose to use the dynamic private key *Alias*, the system will concatenate the suffix and will extract your company tax ID from the tag `AccountingSupplierParty/CustomerAssignedAccountID`.

- *PROD Credentials alias*: **peruwstokencredentials_**`<TAX ID OF COMPANY CODE>`
- *TEST Credentials alias*: **peruwstokencredentials_test_**`<TAX ID OF COMPANY CODE>`

The correct format for the username in the *PROD* credentials is **<CompanyTaxCode><SOL Secondary Key Username>**.

For example, the company has Tax Code (RUC) 21544512515; SOL secondary key username is **USER1** and SOL secondary key password is **MYPASS**. The PROD credentials will be:

- Username: **21544512515USER1**
- Password: **MYPASS**

In the *TEST* environment, the credentials are independent from the SOL secondary key. The username is always **<CompanyTaxCode>MODDATOS**. The password is always **MODDATOS**.

For example, the company has Tax Code (RUC) 21544512515. The correct TEST credentials are:

- Username: **21544512515MODDATOS**
- Password: **MODDATOS**

You must maintain a separate pair of credentials for *Peru Delivery Note* with **peruclientcredentials** as the name.

Enter the credentials that you generated in the tax authority's website. For more information, see Generating Credentials [page 7].

For example, you can maintain the credentials as follows:

- Username: **Client ID**
- Password: **Client Secret**

You must also maintain the below pair of credentials to connect to *SUNAT* for *Peru Delivery Note*.

PROD Credentials alias: **peruwstokencredentials_delivery_**`<TAX ID OF COMPANY CODE>`

For example, the company has Tax Code (RUC) 21544512515; SOL secondary key username is **USER1** and SOL secondary key password is **MYPASS**. The PROD credentials will be:

- Username: **21544512515USER1**
- Password: **MYPASS**

> **Note**
>
> The client secret generated by the tax authority's system for **peruclientcredentials** often includes special characters like **+**, **-**, and **==**. To mitigate this, you can use an online URL encoder to convert these special characters in the client secret into their respective URL-encoded representations.

6.1.1 Deploying Credentials

Context

The credentials (username + password) differ for the integration flow and you must ensure to maintain your credentials.

Procedure

Perform the following steps to create your credentials.

1. Click the *Security Material* tile under *Manage Security* section of the *Overview* page.
2. Choose *Create* > *User Credentials* in the *Security Material* window.

3. Enter the credentials as **mentioned in the previous section.**.
4. Click *Deploy*.

   Your credentials have been created.

6.1.2 Create Aliases and Their Credentials

You create aliases for each key pair, and upload the credentials for the company to the productive tenant.

Context

To do that, follow the steps below:

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 URL you created as defined in the *Prerequisites* section of this document. The URL has the following format **`https://xxxxxxx.hana.ondemand.com/itspaces`**.
4. Navigate to the *Manage Security* section, and choose *Select Material*.
5. Choose *Add* > *User Credentials* and enter the following data:.

Field	Entry
Name	• **`Peruwstokencredentials_<TAX ID OF COMPANY CODE>`** for productive system • **`peruwstokencredentials _test_<TAX ID OF COMPANY CODE>`** for test system
Description	Enter a meaningful description.
User	Enter the SUNAT/OSE username of the signatory.
Password	Enter the SUNAT/OSE password.

6. Choose *Deploy* to save the changes.

6.1.3 Upload the Certificates to the Keystore

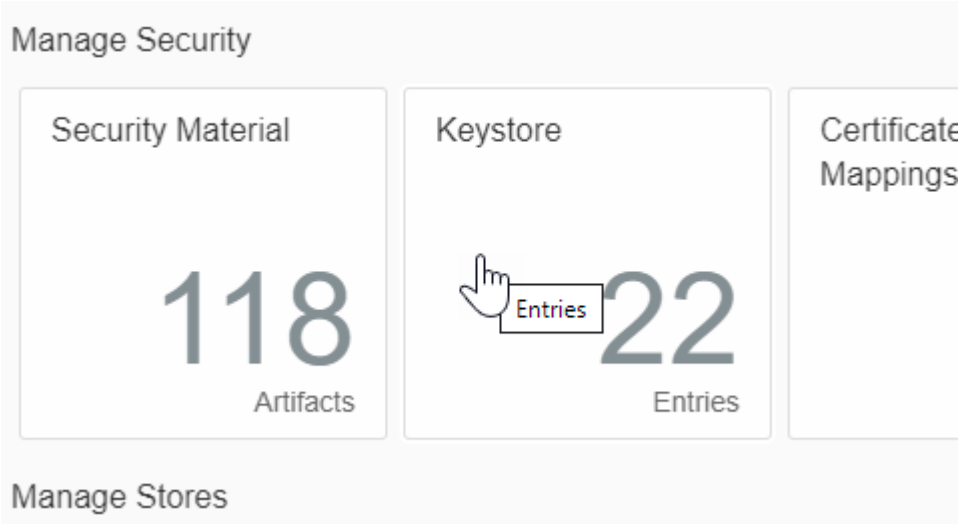
This topic describes how to upload certificates to the SAP Integration Suite tenant.

Context

To establish a connection to the tax agency/OSE server, the SAP Integration Suite needs to trust the certificate from the relevant servers. To achieve this, you must upload the certificate to the SAP Integration Suite tenant.

Procedure

1. Use your tenant URL to access SAP Integration Suite.
2. In the *Operations* view, choose *Keystore* under *Manage Security*.



3. Choose *Add* > *Certificate* to import the certificate.
4. Save your entries.

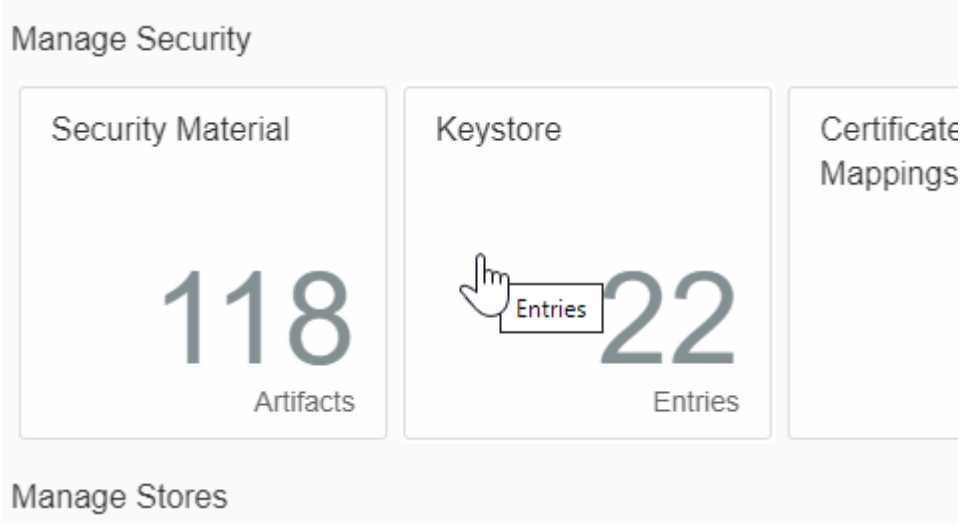
6.1.4 Upload the Key Pair to the Keystore

This topic describes how to upload key pairs to the SAP Integration Suite tenant.

Context

Procedure

1. Use your tenant URL to access SAP Integration Suite.
2. In the *Operations* view, choose *Keystore* under *Manage Security*.



3. Choose *Add* > *Key Pair* to import the key pair. Define the key pair alias as **`perusignaturekey`**.
4. Save your entries.

6.2 Download Integration Flows to Tenant Workspace and Adapt

Download the integration flows and maintain the parameters for each integration flow as described below.

Download Integration Flows

Download all integration flows in the package to the target tenant as follows:

1. In your browser, go to the WebUI of the tenant. The URL has the following format: **`https:\\xxxxx.hana.ondemand.com\itspaces`**.
2. From the menu in the upper left corner, choose *Discover*.
3. Click on the *SAP Document and Reporting Compliance: Electronic Documents for Peru* package.
4. In the lower right corner, choose *Copy*. If the package already exist, overwrite it.

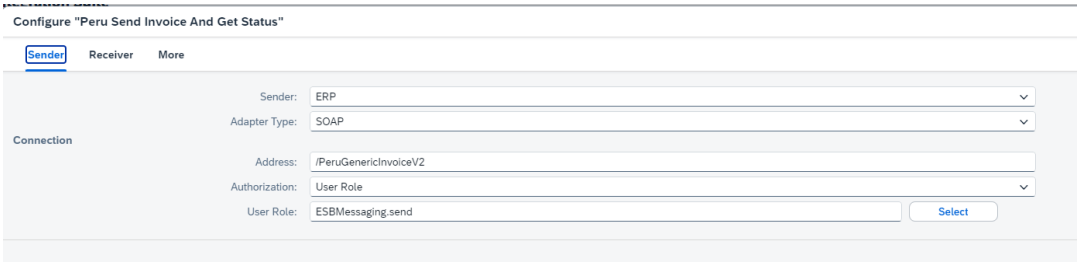
Maintain Parameters

You must maintain are several parameters for each integration flow. To change the parameters in the WebUI, do the following:

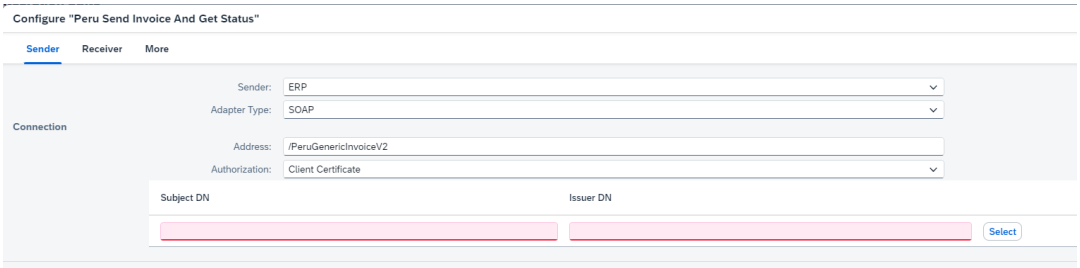
1. From the menu in the upper left corner, choose *Design*.
2. Click on the *SAP Document and Reporting Compliance: Electronic Documents for Peru* package and then on *Package Content*.
3. For the integration flow that you want to change, choose *Actions* > *Configure*.
4. After changing the parameters, choose *Save*.

You must configure the following parameters:

- *Sender* tab
  - *Address*: If you are deploying the same integration flow for multiple company codes, you need to change the address for the second company onwards to generate unique URL for each company code.
  - *Authorization Type*: Select either of the following:
    - **`User Role`**: Select this value if you want to use basic authentication (user/password). In this case, you must configure the role based on which the inbound authorization is checked. Choose *Select* to get a list of all available roles.
      The role *ESBMessaging.send* is provided by default.

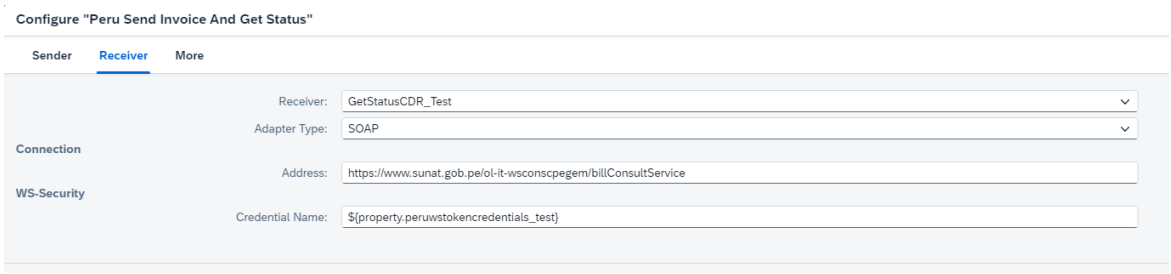


    - **`Client Certificate`**: Select this value if you want to use client certificate authentication. In this case, you must define the **`Subject DN`** and **`Issuer DN`** of client certificates.



- *Receiver* tab

Receiver	*Address*
SUNAT_Production	• **Invoices**: https://e-factura.sunat.gob.pe/ol-ti-itcpfe-gem/billservice • **WTC & tax perception**: https://www.sunat.gob.pe/ol-ti-itemision-otroscpe-gem/billService?wsdl (Retention and Perception Service) • **Get Status**: https://www.sunat.gob.pe/ol-it-wsconscpegem/billConsultService?wsdl (Invoice, Boleta Summary & Void Get Status)
SUNAT_Test	• **Invoices**: https://e-beta.sunat.gob.pe/ol-ti-itcpfe-gem-beta/billService • **WTC and tax perception**: https://e-beta.sunat.gob.pe/ol-ti-itemision-otroscpe-gem-beta/billService?wsdl • **Get Status**: Only available for production



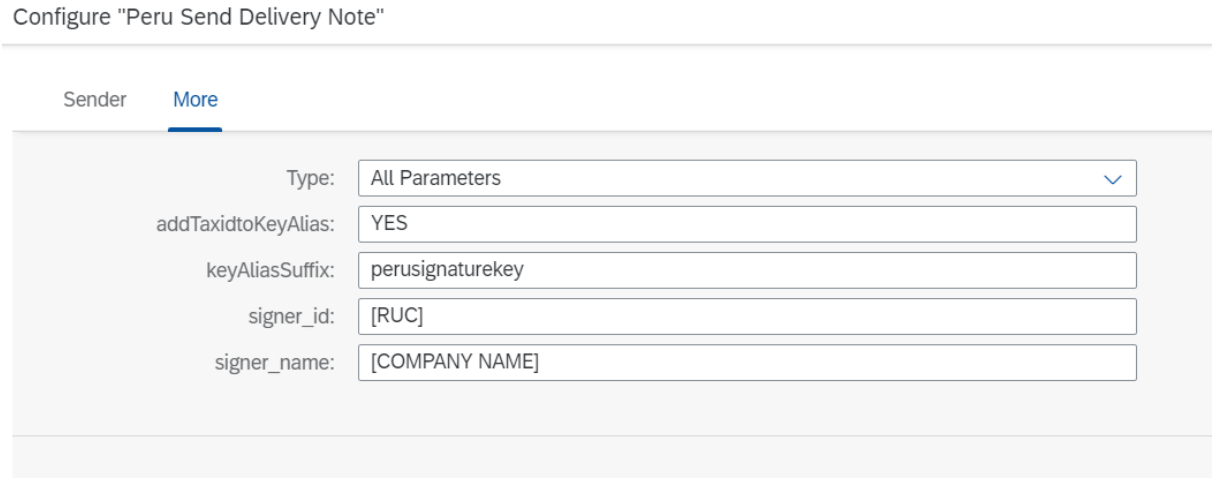
- *More* tab
  - In the *addTaxidtoKeyAlias* field, enter **YES** if you want to use the dynamic private key alias, then update the *KeyAliasSuffix* field with the name that matches the name that you have defined in section Deploy Key Pair, Certificates and Credentials to Tenants [page 15]. The system will concatenate the *KeyAliasSuffix* field with the tax ID of your company automatically. By default, the *KeyAliasSuffix* field is set to **NO**.
  - *mode*: Enter the mode of the integration flow: **< PROD | HMLG | TEST | SIGN >**
  - *signer_id*: **<RUC (Tax Code)>**
  - *signer_name*: **<Name in the certificate used for the digital signature>**
  - *ZIP_Decompress*: Enter **YES** if you receive the following error message:
    `Invalid xpath: /node(). Reason: javax.xml.xpath.XPathExpressionException: Failure converting a node of class javax.xml.transform`
    The default value is set to **NO**.

> ### Note
>
> - The integration flow for *Peru Get Status of Invoice and Summaries* does not have the parameters *signer_id* and *signer_name*.
> - Only the integration flows for *Peru Get Status of Invoice and Summaries*, *Peru Send Tax Certificate*, and *Peru Send Invoice and Get Status* have the parameter *ZIP_Decompress*.

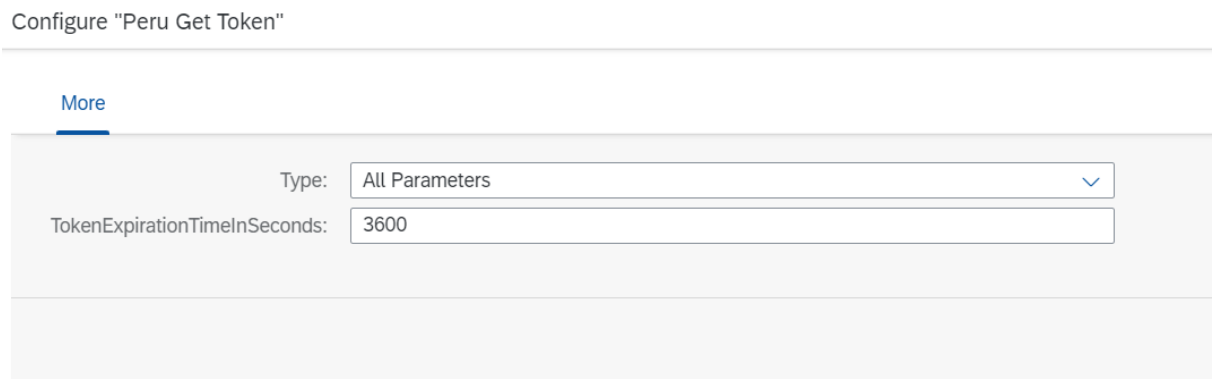
In the integration flow for *Peru Send Delivery Note*, the *Sender* tab must be configured in the same was as *Peru Send Invoice and Get Status*.

The following parameters must be maintained for the *More* tab of *Peru Send Delivery Note*.

- In the *addTaxidtoKeyAlias* field, enter **YES** if you want to use the dynamic private key alias, then update the *KeyAliasSuffix* field with the name that matches the name that you have defined in section Deploy Key Pair, Certificates and Credentials to Tenants [page 15]. The system will concatenate the *KeyAliasSuffix* field with the tax ID of your company automatically. By default, the *KeyAliasSuffix* field is set to **NO**.
- *signer_id*: **<RUC (Tax Code)>**
- *signer_name*: **<Name in the certificate used for the digital signature>**



In *Peru Get Token* iFlow, the parameters have been defaulted as per SUNAT. Hence, no further configuration is required.



6.3 Copy and Adapt Integration Flows for Multiple Companies with Same Tenant

You must follow the steps below if you want to support multiple companies in the same SAP Integration Suite tenant. These settings are optional.

For supporting multiple companies in the same SAP Integration Suite tenant, you must create multiple copies of the integration flows and adapt them to each company.

> **Note**
>
> If you use a dynamic private key alias, you do not need to perform any of the steps described in this section. The dynamic private key alias is available from version 2.0.5 onwards.

6.3.1 Copy the Integration Package with an Alias Name

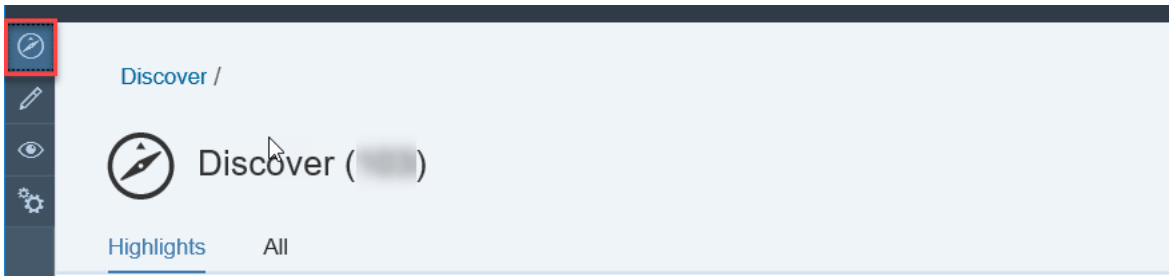
This section describes how to copy an integration package with an alias name.

Context

> **Note**
>
> The steps below are not required if you use a dynamic private key alias.

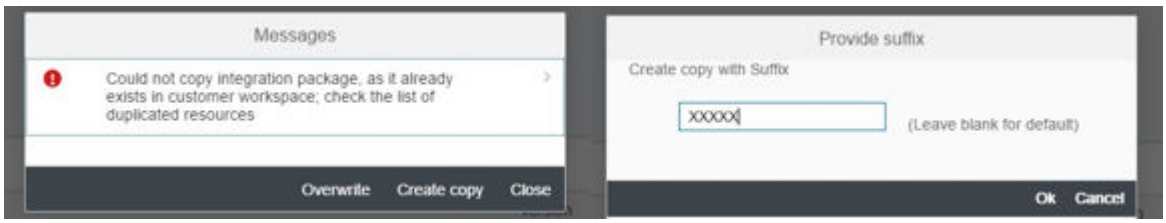
Procedure

1. In your browser, go to the WebUI of the tenant. The URL has the following format: **`https:\\xxxxx.hana.ondemand.com\itspaces`**.
2. From the menu in the upper left corner, choose *Discover*.



3. Click on the *SAP Document and Reporting Compliance: Electronic Documents for Peru* package.
4. When the systems asks whether to overwrite or create a copy, choose the *Create copy* option and enter the company code.

   In the example below, XXXXX stands for the company code:



5. In your browser, go to the WebUI of the tenant. The URL has the following format: **`https:\\xxxxx.hana.ondemand.com\itspaces`**.
6. From the menu in the upper left corner, choose *Design*.
7. Click on the *SAP Document and Reporting Compliance: Electronic Documents for Peru XXXX (copied with alias)* package and then on *Package Content* to see the copied package.

6.3.2 Configure Integration Flows

This topic describes how to configure integration flows for a specific company.

Context

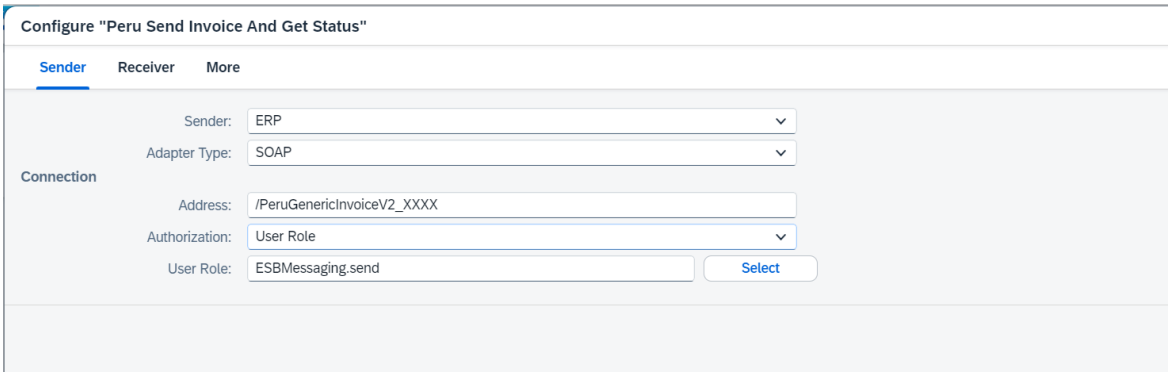
You must repeat the steps below for every integration content copied in the previous section.

> **Note**
>
> The steps below are not required if you use a dynamic private key alias.

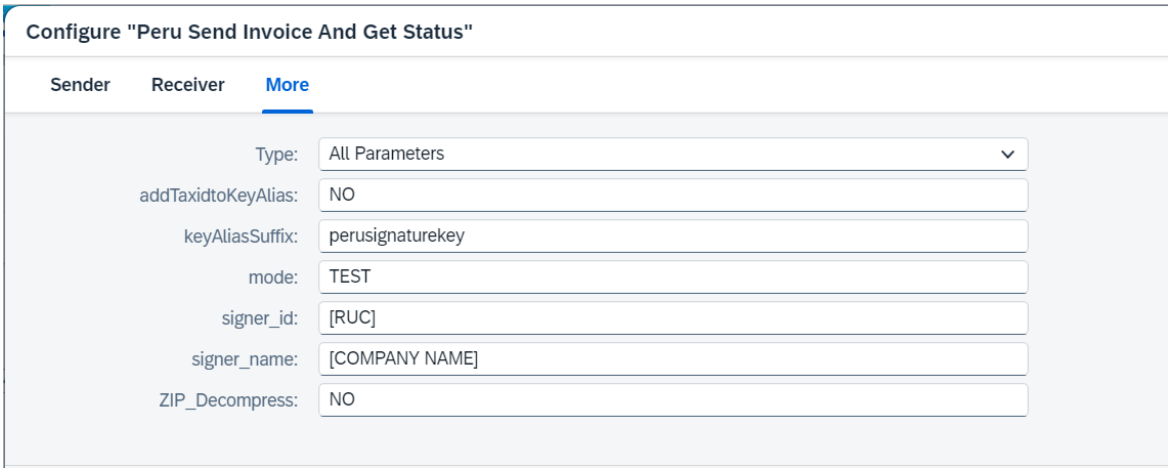
Procedure

1. Choose *Design* from the upper left corner of the page.
2. Click on the package that you copied in the previous section.
3. Go to the *Artifacts* tab page.
4. Choose *Actions* > *Configure* for the relevant integration flow.

5. Choose the *Sender* tab and enter the company code as a suffix in the *Address* field.



6. Choose the *More* tab and enter the company code as a suffix in the *PrivateKeyAlias* field.



7. Save your changes.

   Leave the default settings on the *Receiver* tab as they are.
8. Deploy the private key *perusignaturekey<company code>* and security artifact *peruwstokencredentials<company code>* for each of the companies by repeating the steps mentioned in section .

6.4 Deploy Integration Flows

Perform the steps below to deploy integration flows in the WebUI.

1. Select the integration flow in the WebUI and choose *Deploy*.
   The integration flows must be deployed on the SAP Integration Suite test tenant with mode *TEST*. On the productive SAP Integration Suite tenant, the integration flows must be deployed with mode *PROD*.
2. After all the integration flows are deployed, note down the URLs of the endpoints for each service.

7 Configuration Steps in SAP Backend Systems

The following sections tell you the necessary configuration you do in SAP Backend Systems.

7.1 Create Logical Ports in SOAMANAGER

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

For Peru, there are six different proxies that need to be connected to the SAP Integration Suite tenant via logical port.

The information in the following sections is based on the assumption that one SAP back-end client connects to one SAP Integration Suite tenant. In the first section below, the SAP back-end system sends all eDocuments to the same logical port independent of the company code.

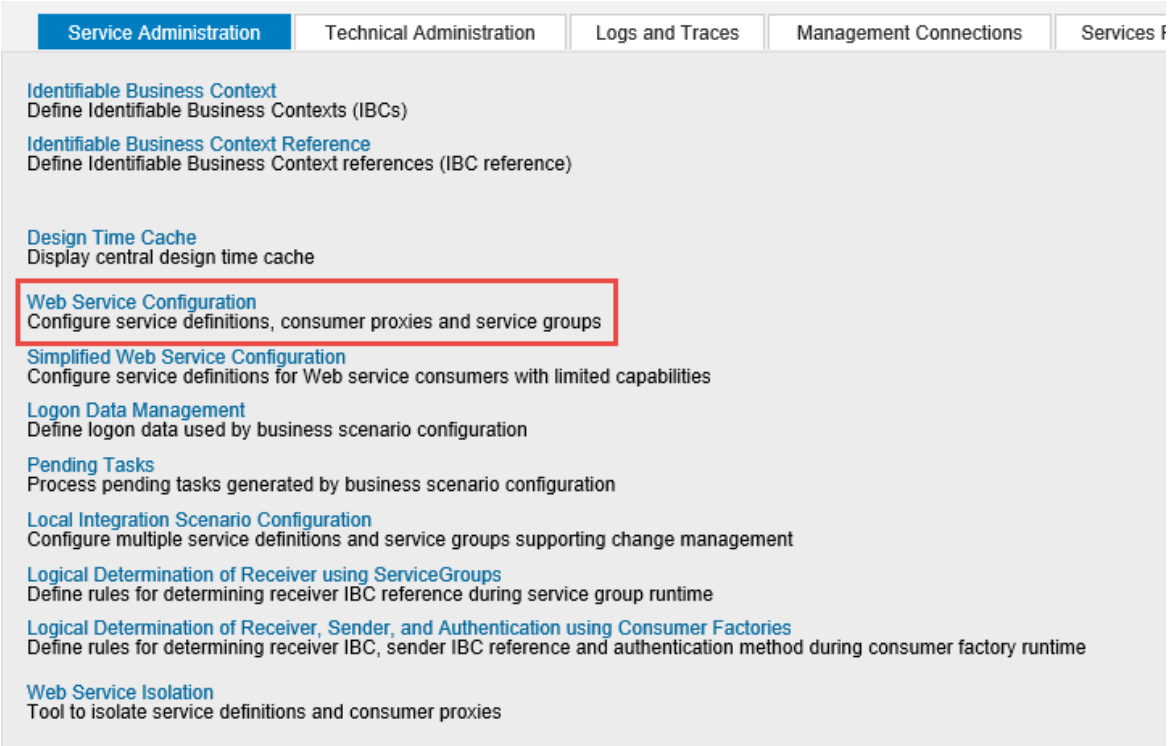
In the second section, eDocuments are sent to different logical ports depending on the company code. This scenario is enabled with SAP Note 2170178. Refer to that SAP Note for further configuration of the system.

7.1.1 Create Logical Ports Independent of Company Code

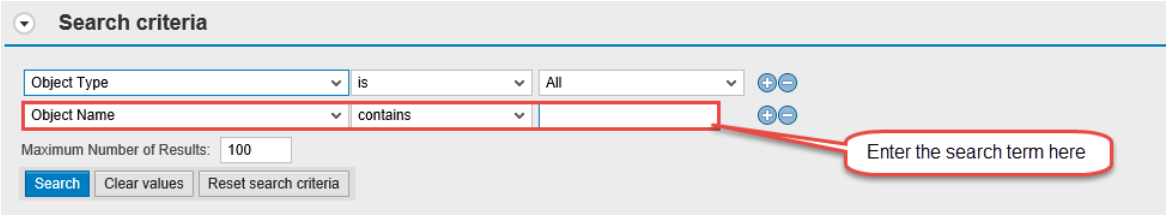
Perform the steps below to create logical ports in case eDocuments must be sent to the same logical ports independent of the company code.

Procedure

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



2. Find the proxies for SAP Document and Reporting Compliance for Peru with search term **CO_EDO_PE***.

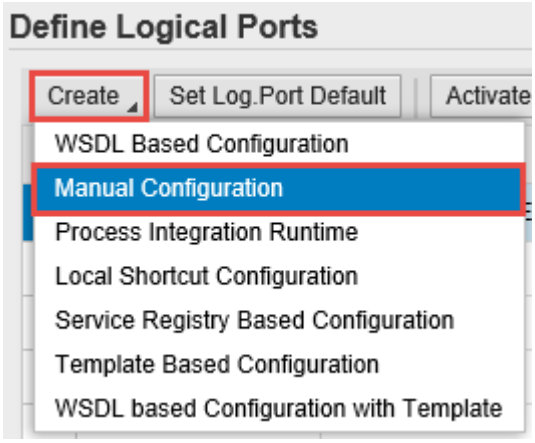


The following table lists the proxies, the logical port name and path for each proxy.

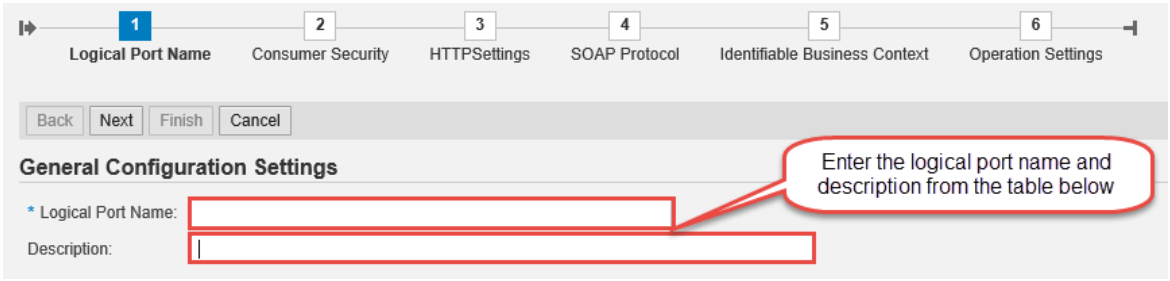
Proxy Name	Logical Port Name	Endpoint URL (Customizable)
CO_EDO_PE_DOCUMENT_TRANSM_SERV	EDO_PE_DOCUMENT_TRANSM_SERV_PORT	/cfx/PeruGenericInvoiceV2
CO_EDO_PE_DLY_SUMM_TRANSM_SERV	EDO_PE_DLY_SUMM_TRANSM_SERV_PORT	/cxf/PeruSummaryDocumentsTransmission
CO_EDO_PE_GET_STATUS_INV_SERV	EDO_PE_GET_STATUS_SERV_PORT	/cxf/PeruGetStatusInv
CO_EDO_PE_TAX_CERT_TRANS_SERV	EDO_PE_TAX_CERT_TRANS_SERV_PORT	/cxf//PeruTaxCertificate
CO_EDO_PE_VOID_DOC_TRANSM_SERV	EDO_PE_VOID_DOC_TRANSM_SERV_PORT	/cxf/PeruVoidedDocumentsTransmission

Proxy Name	Logical Port Name	Endpoint URL (Customizable)
CO_EDO_PE_E_DOC_PERU_DOCUMENT	EDO_PE_DOCUMENT_TRANSM_SERV_PORT	/cfx/PeruGenericInvoiceV2
CO_EDO_PE_DELNE_DOC_PERU_DELIV	EDO_PE_DELNOTE_TRANSM_SERV_PORT	/cxf/PeruDeliveryNote
CO_EDO_PE_DELN_GETE_DOC_PERU_G	EDO_PE_DELNOTE_GETSTAT_SERV_PORT	/cxf/PeruDeliveryNote

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.



Logical Port Name	Description
EDO_PE_DOCUMENT_TRANSM_SERV_PORT	Peru eDocument – Invoice Credit and Debit Memo Transmission
EDO_PE_DLY_SUMM_TRANSM_SERV_PORT	Peru eDocument – Daily Summary Transmission Service
EDO_PE_GET_STATUS_SERV_PORT	Peru eDocument – Get Status for Invoice and Summaries Service
EDO_PE_TAX_CERT_TRANS_SERV_PORT	Peru eDocument – WTC & CTC Transmission Service

Logical Port Name	Description
EDO_PE_VOID_DOC_TRANSM_SERV_PORT	Peru eDocument – Voided Documents Transmission Service
EDO_PE_DELNOTE_TRANSM_SERV_PORT	Peru eDocument –Delivery Note Transmission
EDO_PE_DELNOTE_GETSTAT_SERV_PORT	Peru eDocument – Get Status for Delivery Note

7.1.2 Create Logical Ports Dependent on Company Code

Perform the steps below to create logical ports in case eDocuments from different company codes must be sent to different logical ports.

Prerequisites

In your SAP back-end system, you must install SAP Note 2170178 as a prerequisite.

Context

This scenario can be required, for example, when eDocuments from a different company code must be signed with a different signature in SAP Integration Suite and therefore must be sent to different instances of an integration flow.

> **Note**
>
> If you use a dynamic private key alias, you do not need to perform any of the steps described in this section. The dynamic private key alias is available from version 2.0.5 onwards.

Procedure

1. Maintain the logical ports for each set of integration flow instances as described in section Create Logical Ports Independent of Company Code [page 27].

   You only need to change the *URL Access Path* field, the rest of the fields remain the same. For example, two company codes **CC11** and **CC22** use different signatures, which means that eDocuments belonging to these company codes must be signed by different integration flows. In SOAMANAGER, you must maintain two logical ports for each ABAP proxy, that is, one logical port per company code. One company (in this case CC11) will be the default and the other one needs to be explicitly differentiated by adding the company code to the technical names, as shown below:

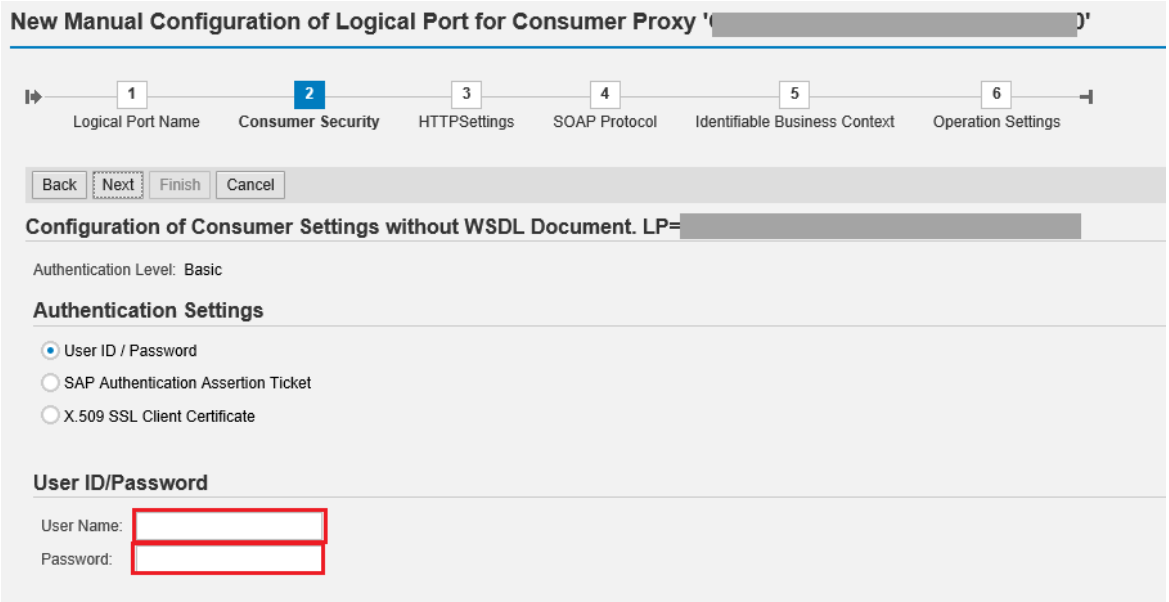
Proxy Name	Logical Port Name	Endpoint URL (Customizable)
CO_EDO_PE_DOCUMENT_TRANSM_SERV	EDO_PE_DOCUMENT_TRANSM_SERV_PORT	/cfx/PeruGenericInvoiceV2
	EDO_PE_DOCUMENT_**CC22**_TRANSM_SERV _PORT	/cfx/PeruGenericInvoiceV2_CC22 (*)
CO_EDO_PE_DLY_SUMM_TRANSM_SERV	EDO_PE_DLY_SUMM_TRANSM_SERV_PORT	/cxf/PeruSummaryDocumentsTransmission
	EDO_PE_DLY_SUMM_**CC22**_TRANSM_SERV_PORT	/cxf/PeruSummaryDocumentsTransmission_CC22 (*)
CO_EDO_PE_GET_STATUS_INV_SERV	EDO_PE_GET_STATUS_SERV_PORT	/cxf/PeruGetStatusInv
	EDO_PE_GET_STATUS_INV_**CC22**_SERV_PORT	/cxf/PeruGetStatus_CC22 (*)
CO_EDO_PE_VOID_DOC_TRANSM_SERV	EDO_PE_VOID_DOC_TRANSM_SERV_PORT	/cxf/PeruVoidedDocumentsTransmission
	EDO_PE_VOID_DOC_**CC22**_TRANSM_SERV_PORT	/cxf/PeruVoidedDocumentsTransmission_CC22 (*)
CO_EDO_PE_E_DOC_PERU_DOCUMENT	EDO_PE_DOCUMENT_TRANSM_SERV_PORT	/cfx/PeruGenericInvoiceV2
	EDO_PE_DOCUMENT_TRANSM_SERV_PORT	/cfx/PeruGenericInvoiceV2_CC22 (*)
CO_EDO_PE_DELNE_DOC_PERU_DELIV	EDO_PE_DELNOTE_TRANSM_SERV_PORT	/cxf/PeruDeliveryNote
	EDO_PE_DELNOTE_CC22_TRANSM_SERV_PORT	/cxf/PeruDeliveryNote_CC22(*)
CO_EDO_PE_DELN_GETE_DOC_PERU_G	EDO_PE_DELNOTE_GETSTAT_SERV_PORT	/cxf/PeruDeliveryNote
	EDO_PE_DELNOTE_CC22_GETSTAT_SERV_PORT	/cxf/PeruDeliveryNote_CC22(*)

> **Note**
>
> Entries marked with (*) are example URLs and do not exist. In a real scenario, the URLs are defined by copying the integration flows and adapting the URL in the copied instance.

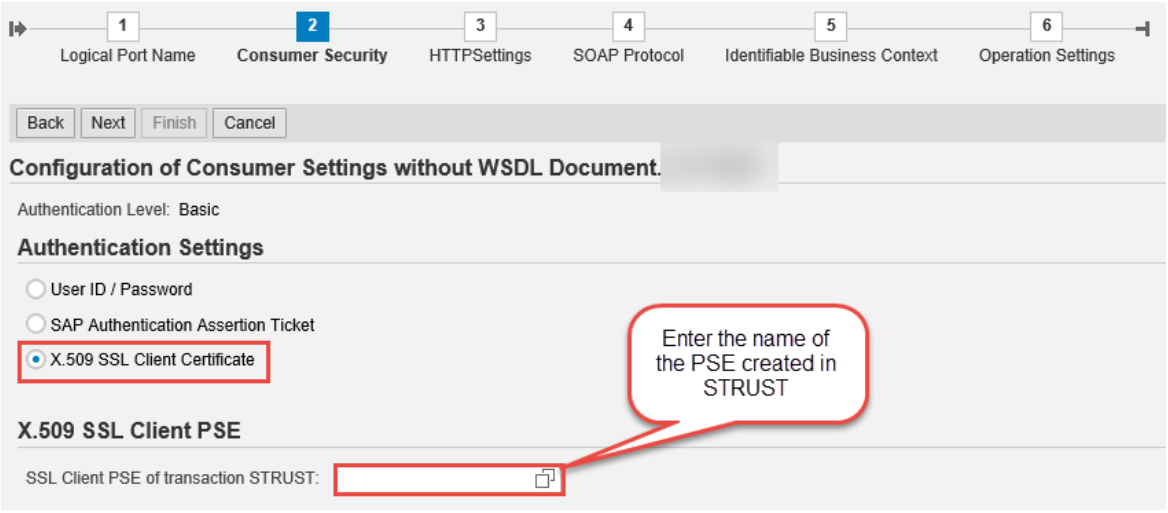
In the SAP back-end system, the configuration in view **EDOSOASERV** could look as follows:

SOA Service Name	Company Code	Logical Port
PE_DOC_TRANSM	CC11	EDO_PE_DOCUMENT_TRANSM_SERV_PORT
PE_DOC_TRANSM	CC22	EDO_PE_DOCUMENT_**CC22**_TRANSM_SERV _PORT
PE_DLY_SUMM_TRANSM	CC11	EDO_PE_DLY_SUMM_TRANSM_SERV_PORT
PE_DLY_SUMM_TRANSM	CC22	EDO_PE_DLY_SUMM_**CC22**_TRANSM_SERV_PORT
PE_GET_STATUS	CC11	EDO_PE_GET_STATUS_INV_SERV_PORT
PE_GET_STATUS	CC22	EDO_PE_GET_STATUS_INV_**CC22**_SERV_PORT
PE_VOID_DOC_TRANSM	CC11	EDO_PE_VOID_DOC_TRANSM_SERV_PORT
PE_VOID_DOC_TRANSM	CC22	EDO_PE_VOID_DOC_**CC22**_TRANSM_SERV_PORT
PE_DEL_TRANSM	CC11	EDO_PE_DELNOTE_TRANSM_SERV_PORT
PE_DEL_TRANSM	CC22	EDO_PE_DELNOTE_**CC22**_TRANSM_SERV_PORT
PE_DEL_GETSTAT	CC11	EDO_PE_DELNOTE_GETSTAT_SERV_PORT
PE_DEL_GETSTAT	CC22	EDO_PE_DELNOTE_**CC22**_GETSTAT_SERV_PORT

2. 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.

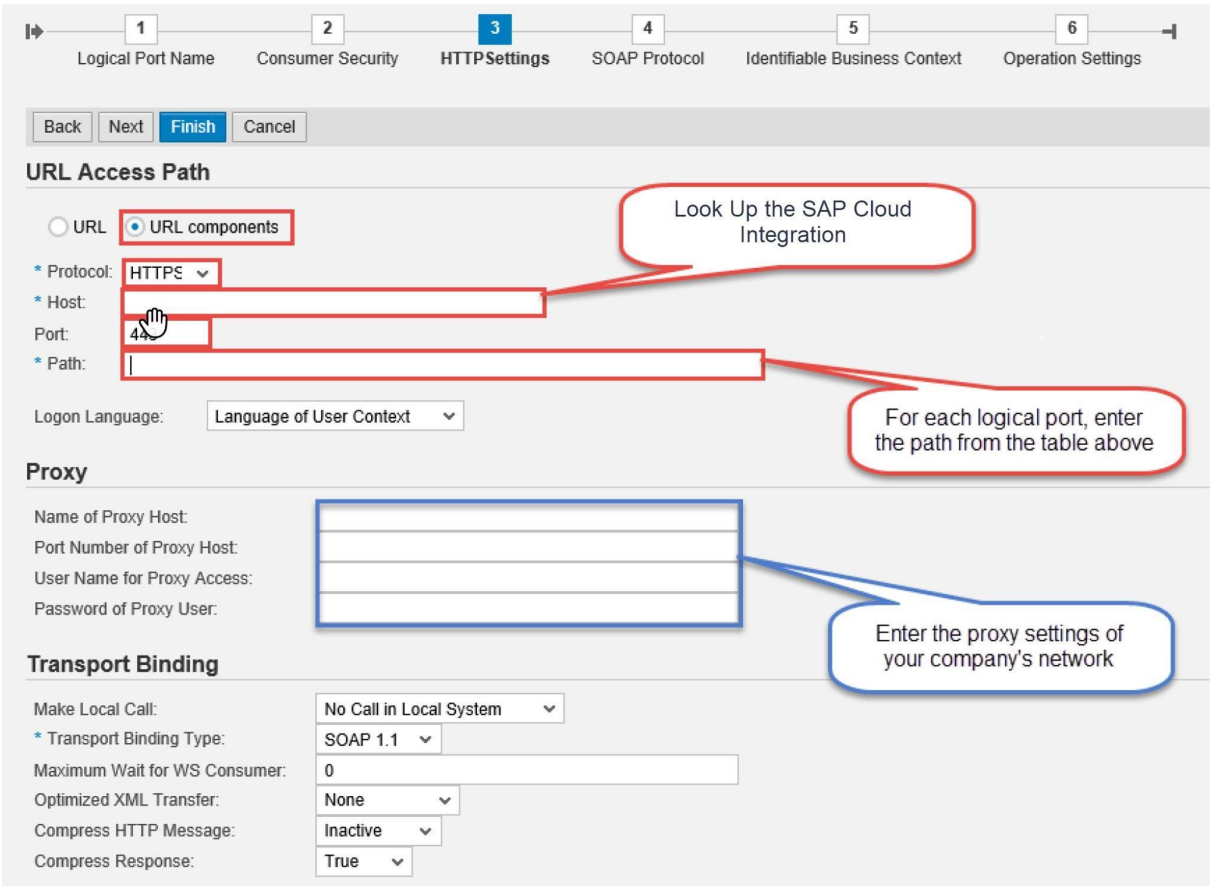


- If you use the basic authentication for *User Name*, enter the value for the **clientid** and for *Password*, enter the value for **clientsecret**. You have created these values for your service instance in SAP Integration Suite. See Creating Service Instances.



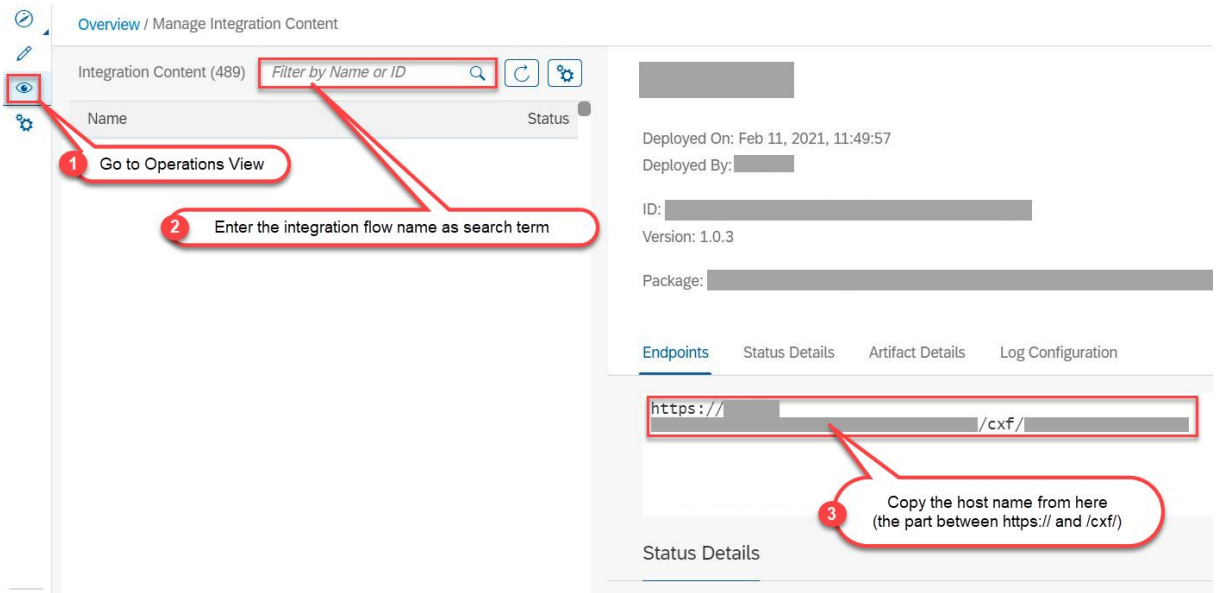
- If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have updloaded to STRUST. You must configure this certificate in SAP Integration Suite too. For that you create a service instance using the required grant_type. You create the service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

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



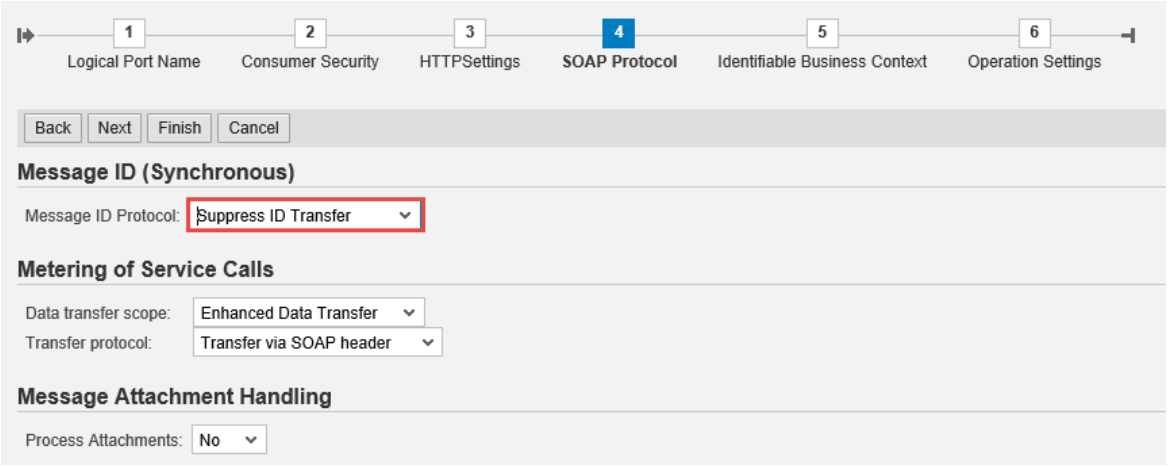
Port 443 is the standard port for the HTTPS protocol.

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.

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



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

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

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

6. Remember to create logical ports for each proxy and to execute the following steps in the SAP back-end systems.

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

8 Configuration Steps for SAP S/4HANA Cloud

The following sections tell you the necessary configuration you do in SAP S/4HANA Cloud.

8.1 Configure Communication System

Create a communication system that represents your SAP Integration Suite tenant.

Prerequisites

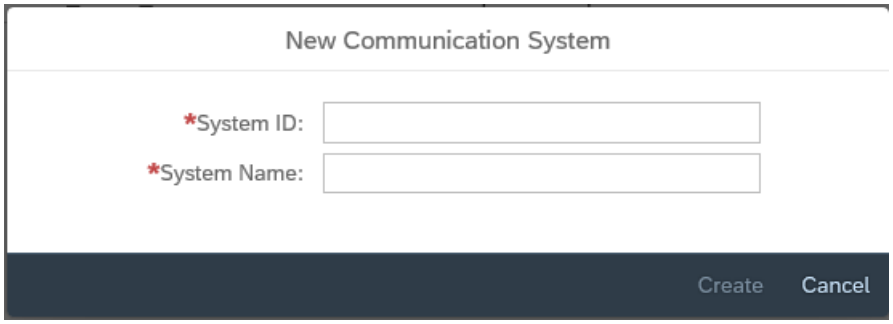
- Live SAP Integration Suite test or productive tenant must be available.
- Communication systems and communication arrangements are not transportable. Configure them in both your quality and production systems.
- The SAP S/4HANA Cloud user, who configures communication systems and communication arrangements, must be assigned a business role with the business catalog `SAP_BCR_CORE_COM` (*Communication Management*) for accessing communication management apps.

Procedure

1. Log in to your S/4HANA Cloud tenant.
2. Find and launch the *Communication Systems* app. Choose *New*.

   A *New Communication System* dialog box appears.
3. Create a system ID and give it a descriptive name.

   For example, if the host name of your SAP Integration Suite tenant is `v1234-tmn.avt.eu1.hana.ondemand.com`, you can use `EDOC_V1234` as the system ID.



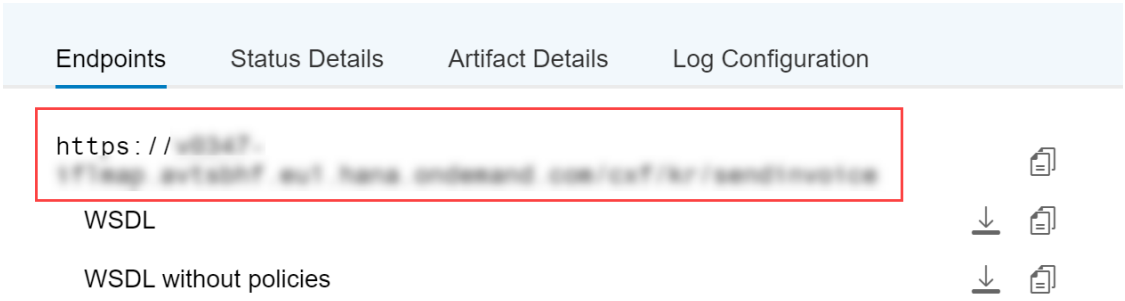
4. Choose *Create*.

   An editing screen for the communication system appears.

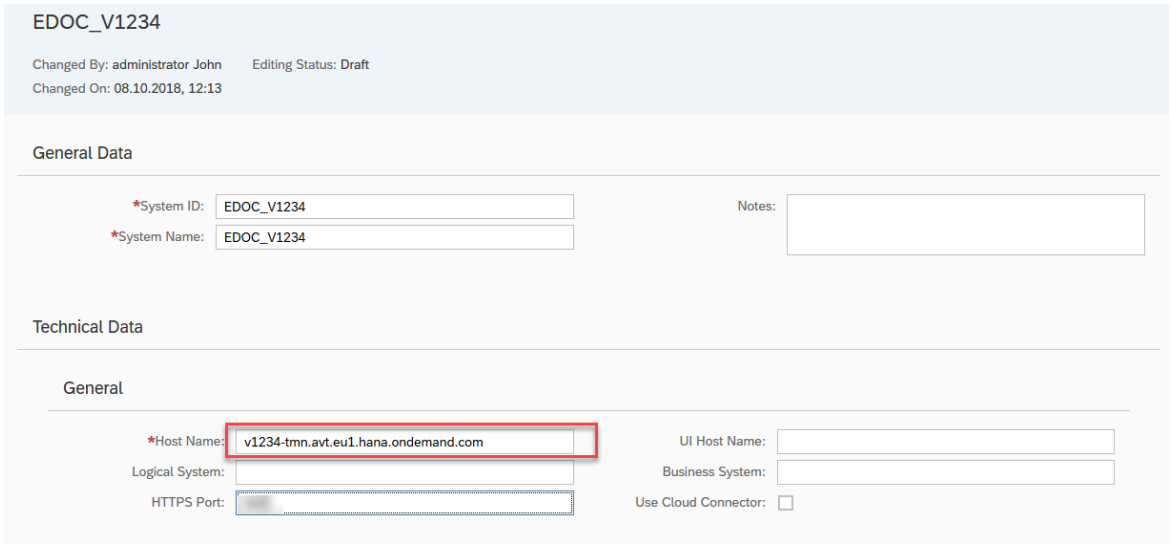
5. In the *Technical Data* section, enter the host name and HTTPS port of your SAP Integration Suite tenant.

   You can find the host name for your SAP Integration Suite tenant, as follows:

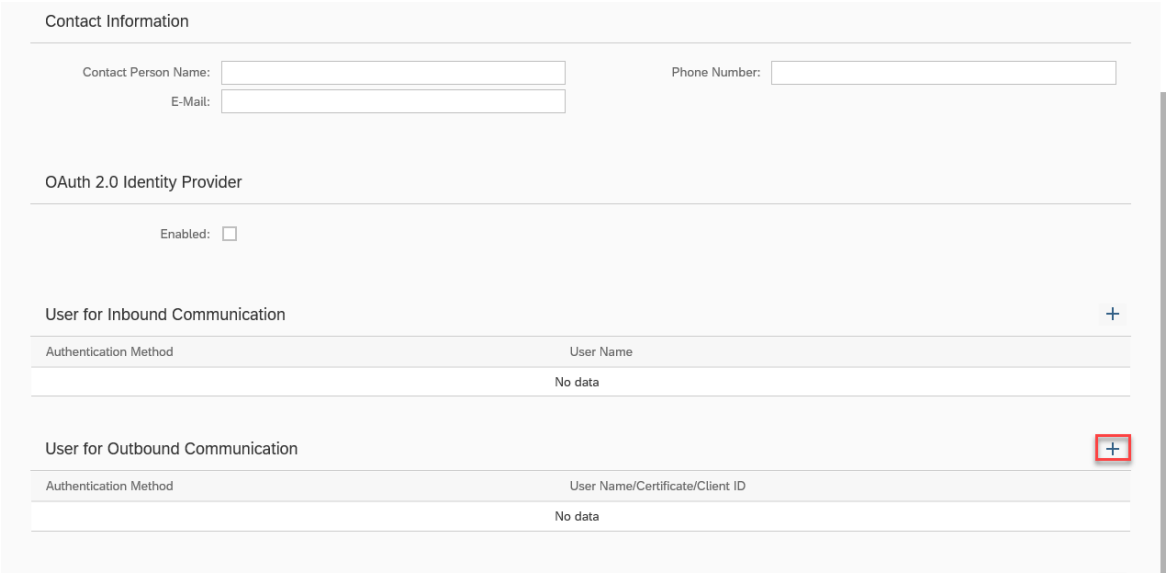
   1. From the menu on the left, choose *Monitor*.
   2. Select *Manage Integration Content* (All).
   3. Search for the integration flow for the scenario you are configuring.
   4. Find the host name from the *Endpoints* tab.
      The composition of an endpoint URL is **https://**`<host name>/<path>`.



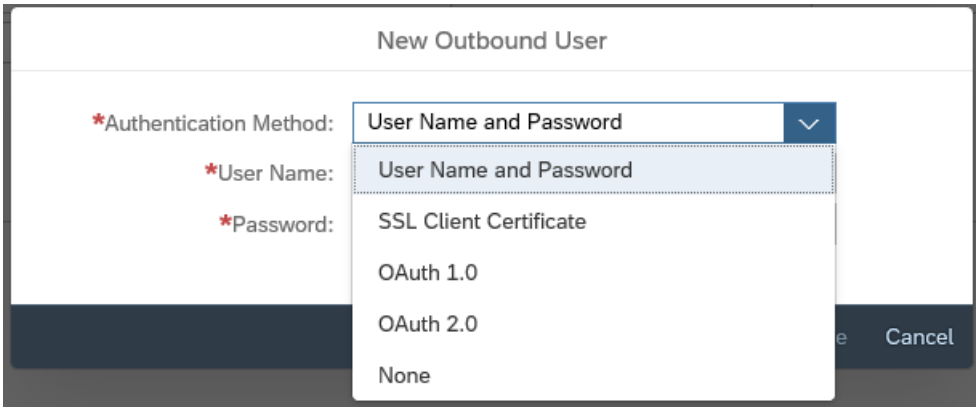
   See the following example:



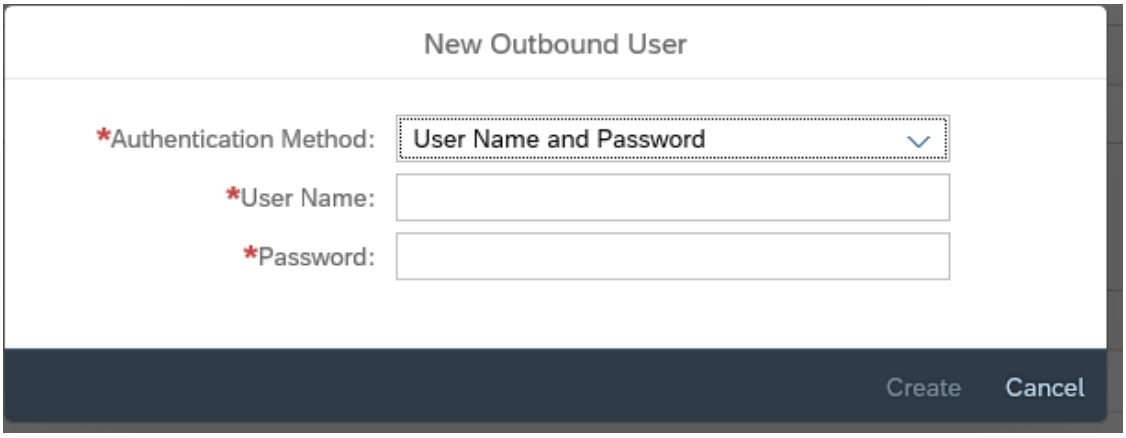
6. In the *User for Outbound Communication* section, choose +.



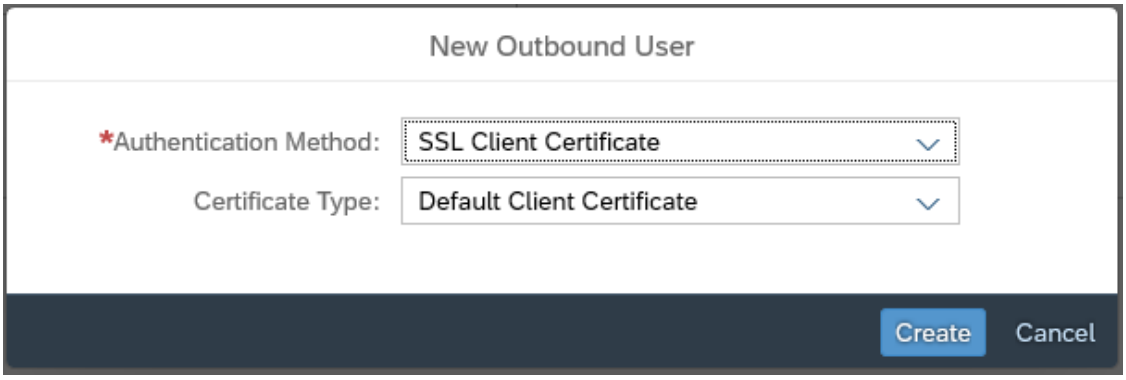
7. Select an authentication method, which is used to connect to your SAP Integration Suite tenant. Proceed as follows:



- If you select the authentication method *User Name and Password*, for *User Name* enter the value for the **clientid** and for *Password*, the value for the **clientsecret**. You create these values for your service instance in SAP Integration Suite. For more information, see Creating Service Instances.



- If you select the authentication method *SSL Client Certificate*, select the *Default Client Certificate* type and choose *Create*. 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 SAP S/4HANA Cloud. For more information, see Defining a Service Key for the Instance in the Cloud Foundry Environment.



8. Choose *Save*.

8.2 Configure Communication Arrangement

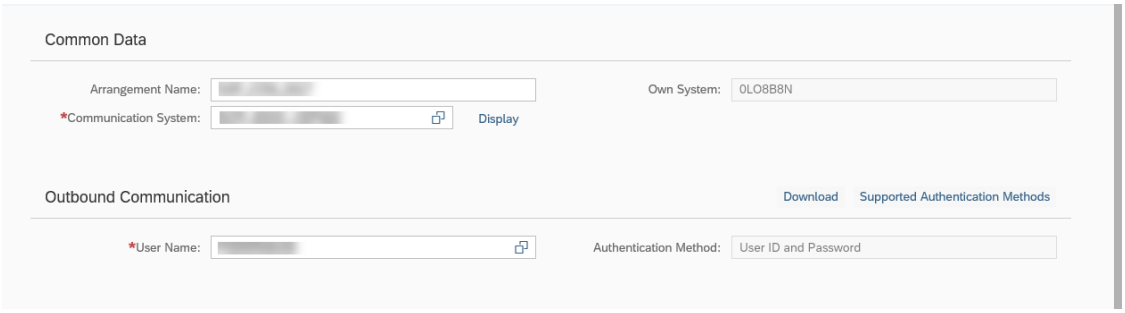
Configuration steps for SAP S/4HANA Cloud Communication Arrangement.

Procedure

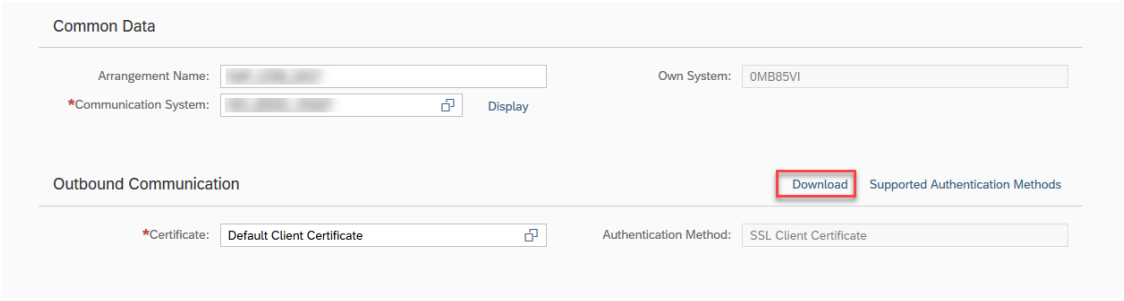
1. Login to your S/4HANA Cloud tenant with the Cloud User.
2. Find and launch the application *Communication Arrangements*.

3. Choose *New*. In the new pop-up window, enter the scenario `SAP_COM_0873` (which is the one designated for communication with the tax authority via SAP Integration Suite package) and an *Arrangement Name*. For arrangement name, it is recommended to choose a name like `SAP_COM_0873_<name of SAP Integration Suite tenant>`, for example, `SAP_COM_0873_V1234` for tenant host name beginning with v1234-tmn.

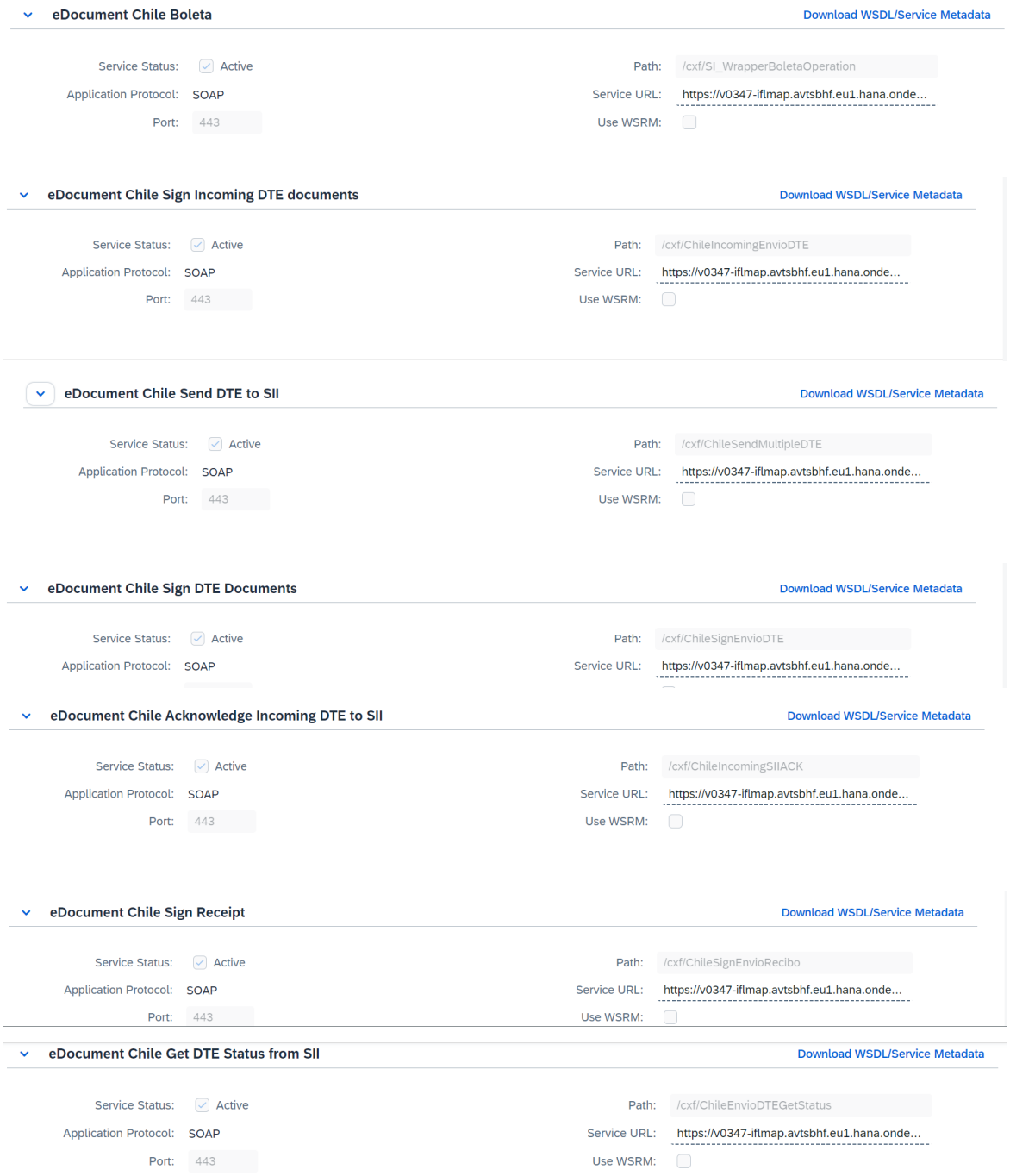
4. Choose *Create*.
5. In the new window, choose the communication system created in the previous step (for example, `EDOC_V1234`) and the authentication method, relevant to the communication system.
    - If the authentication is by User ID, then select *User Name and Password* from the *Outbound Communication* list.



    - If the authentication method is Default Client Certificate, download the certificate here and upload it to SAP Integration Suite.



6. Enter the path part for your integration flow URL for all outbound services.
7. Choose *Save*.


eDocument Chile Boleta
Download WSDL/Service Metadata
Service Status: Active
Application Protocol: SOAP
Port: 443
Path: /cxf/SI_WrapperBoletaOperation
Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Use WSRM:
eDocument Chile Sign Incoming DTE documents
Download WSDL/Service Metadata
Service Status: Active
Application Protocol: SOAP
Port: 443
Path: /cxf/ChileIncomingEnvioDTE
Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Use WSRM:
eDocument Chile Send DTE to SII
Download WSDL/Service Metadata
Service Status: Active
Application Protocol: SOAP
Port: 443
Path: /cxf/ChileSendMultipleDTE
Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Use WSRM:
eDocument Chile Sign DTE Documents
Download WSDL/Service Metadata
Service Status: Active
Application Protocol: SOAP
Path: /cxf/ChileSignEnvioDTE
Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
eDocument Chile Acknowledge Incoming DTE to SII
Download WSDL/Service Metadata
Service Status: Active
Application Protocol: SOAP
Port: 443
Path: /cxf/ChileIncomingSIIACK
Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Use WSRM:
eDocument Chile Sign Receipt
Download WSDL/Service Metadata
Service Status: Active
Application Protocol: SOAP
Port: 443
Path: /cxf/ChileSignEnvioRecibo
Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Use WSRM:
eDocument Chile Get DTE Status from SII
Download WSDL/Service Metadata
Service Status: Active
Application Protocol: SOAP
Port: 443
Path: /cxf/ChileEnvioDTEGetStatus
Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Use WSRM:

9 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.

10 Troubleshooting

In this section, you can find useful information for solving errors that can occur during the communication with the tax authorities in Peru (SUNAT) using the web service.

10.1 Error Codes

When calling web services, there are many error codes that indicate possible issues with communication.

These codes are provided by the tax authorities in Peru (SUNAT) and can be found under the link below:

Since this is an external, country-specific document, the error list (Codigos de Error) are only described in Spanish. SAP SE or its affiliated companies are not responsible for its availability, content or accuracy.

10.2 Proxy Errors in Backend Systems

Error information is sent back by SUNAT as SOAP fault. When the ABAP Proxy in the backend systems receives the SOAP fault, the *eDocument Cockpit* shows the following error message:

```
Proxy Error GENERAL_ERROR Error during proxy processing (PART U: NKNOWN (NULL)
```

The actual error information can be seen in one of the following ways:

- In the payload trace of transaction `SRT_UTIL` in the backend system
  Note: The trace must be activated before you start the `EDOC_COCKPIT` transaction.
- In the payload trace of SAP Cloud Integration
- In the Message Processing Log (MPL) of your integration service

10.3 "Get Status" Test Web Service Not Working

At the time of publishing this document, the SUNAT test web service did not implement the “Get Status” service. Calling this service always returns “ticket not found”.

10.4 SOAP Fault “MustUnderstand Headers”

If you get this error when communicating with SAP Integration Suite, check the configuration in SOAMANAGER. The issue is probably caused by not selecting the checkbox *Message ID Protocol Suppress ID Transfer*.

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 an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP