Integration Guide | PUBLIC
2023-06-02

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

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.

> **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 Installation of eDocuments Full Solution

You have installed and configured the eDocument Full solution in your test and productive systems. If you did not install the latest support package for your system, see the SAP Note 2030855 (for SAP ERP) or 2344815 (for SAP S/4HANA) for the list of SAP Notes to be installed for Chile. For generic information about the installation of the eDocument Framework, refer to the SAP Note 2134248 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.

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.

> **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`).

4.2 Registration at SII

You have completed registration at SII up to the point where SII expects the homologation test documents to be sent by you. This means that you have done the following:

- You have a certificate used for digital signature (private key + password).
- You have completed the environment certification process as per the document "MANUAL PARA EMPRESAS USUARIAS" from SII. There is a valid CAF authorization XML file for the document type to be communicated to SII at the end of this process.
- You have created a certificate using the private key and public key information available in the authorization XML file from the previous step. For information on how to create a certificate using private and public key information available in the CAF XML file, see the section below.

4.2.1 Generating and Importing Certificates

You generate the private key from the CAF authorization XML file, create a key pair and a keystore and import the keystore as described in this topic.

Context

Perform the steps below:

Procedure

1. Upload the number range to the system from the CAF XML file and download the private key.

   To do that, follow the steps below:

   a. In Customizing for *Cross-Application Components*, choose *General Application Functions* > *Document and Reporting Compliance* > *Country/Region-Specific Settings* > *Chile* > *Electronic Document Processing* > *Create/Delete Number Ranges*.

This opens the *Create/Delete Number Range* (`EDOC_CL_NR_XML_UPLOAD`) report.

b. Choose *Create from XML file* and specify the company code, DTE (numbering object `EDOC_CL<NN>`) and the path to the CAF XML file that you downloaded from SII.

c. Execute the report to upload the CAF XML file.

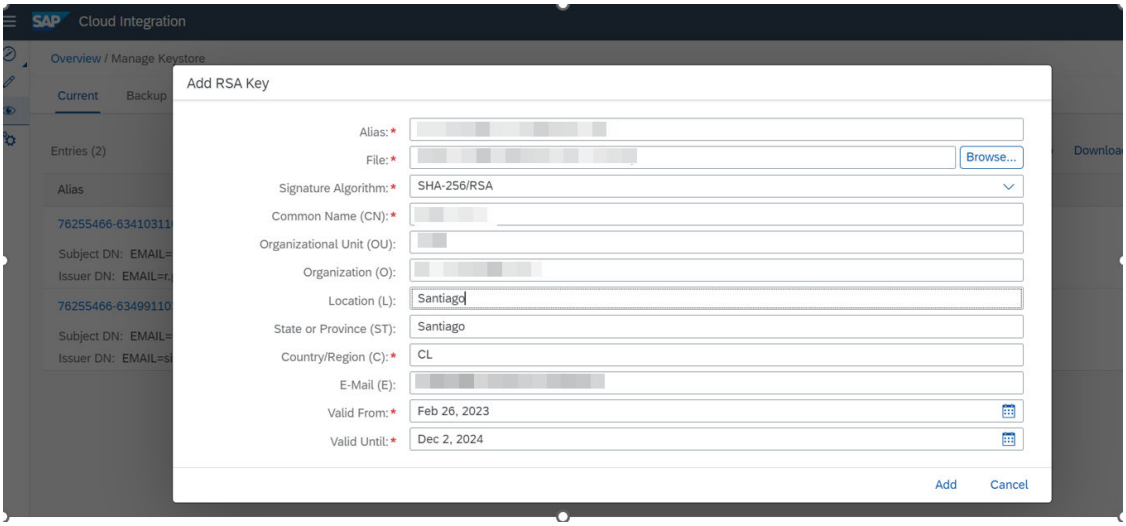
The report also downloads the RSA key file for the XML, which includes the private key from the CAF XML file. This element is required for signing.

2. Upload the RSA key file in the keystores as follows:

a. Choose the *Keystore* tile in the *Manage Security* section.

b. Choose *Add RSA Key* on the *Current* tab, above the table.

c. Choose *Browse* and select the RSA key on your local disk. You can only upload PEM-encoded RSA keys in PKCS#1 format. For more information, refer https://help.sap.com/docs/CLOUD_INTEGRATION/368c481cd6954bdfa5d0435479fd4eaf/b8ba4a3d62054775bb8264f6e31b8d71.html.



> **Note**
>
> The *Alias* name should be the same as the RSA key file name, excluding the file type extension.

d. Select *Add*.

5 Configuration Steps in SAP Integration Suite

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

5.1 Deploy Customer Certificate and Credentials to Tenants

You must request the private key used for signing and deploy the certificate (as private key with an alias) in the tenants' JAVA_KEYSTORE.To allow the integration flows to be updated with minimal adaptation effort, the alias used for the private key and for the credential must be as follows:

Private key alias: **chilesignaturekey**

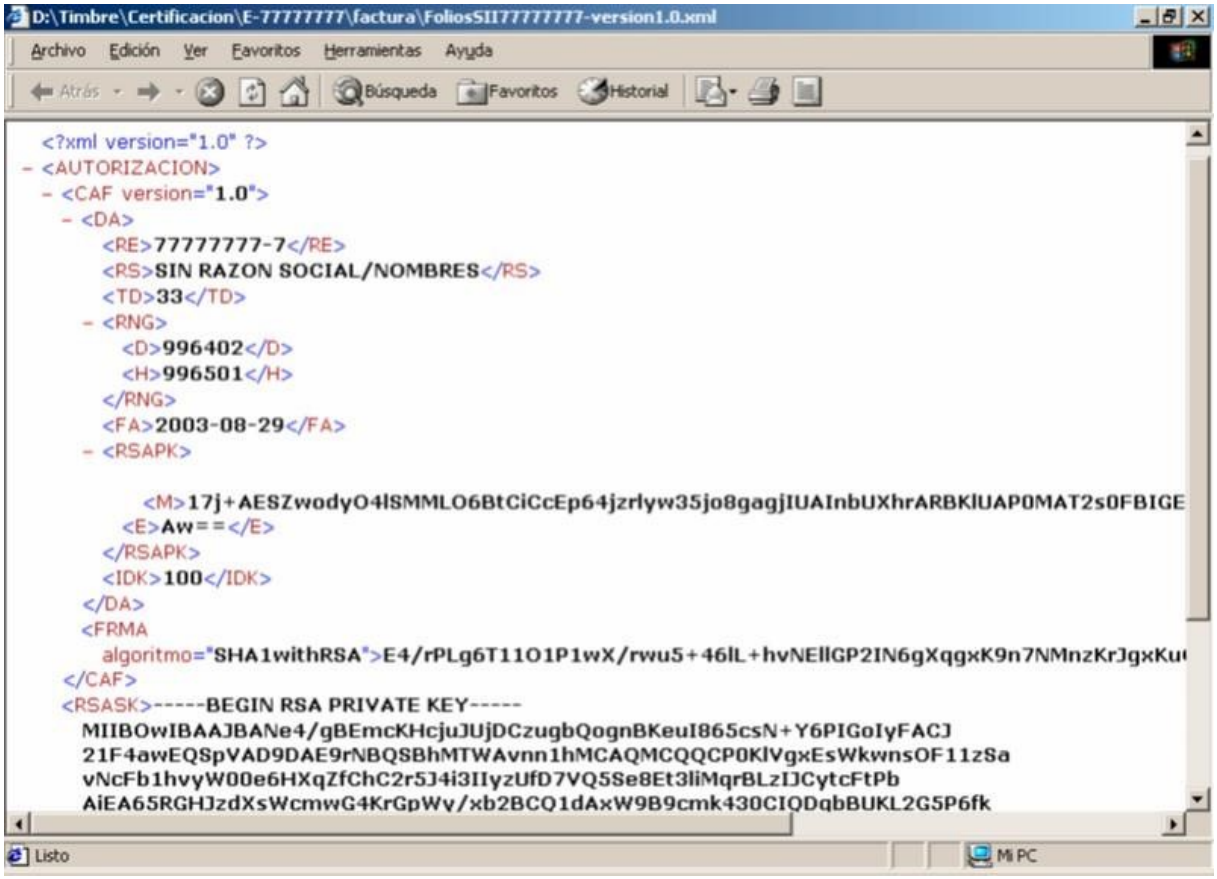
You must create and deploy the private key to sign and generate the DTE Digital Seal in the tenants' JAVA_KEYSTORE. The private key is generated from the CAF authorization files received from SII per DTE type.

There will be as many private keys as DTE types.

The private key must have an alias name that is a concatenated string with values of nodes RE, TD, D, H and FA from the CAF authorization XML received from SII.

For example, for the CAF XML file shown in the figure below, the alias name of the certificate must be the following:

77777777-7339964029965012003-08-29



For information about how to create a private key from the CAF Authorization XML files, see Generating and Importing Certificates [page 9].

From version 2.4.2 onwards, the dynamic private key *Alias* is enabled for the following integration flows, which is of the format **`chilesignaturekey_xxxxx`**, where **`chilesignaturekey`** is the suffix and **`xxxxx`** is your company tax ID. The system concatenates the suffix and extracts your company tax ID from the XML file. For example, if company tax ID is *76255466-6*, then the private key alias will be **`chilesignaturekey_76255466-6`**.

This feature is available for the following integration flows only:

Integration Flow Name	Dynamic Signature Enabled	Externalized Credentials	Externalized Address
Chile Send DTE	Yes	Yes	Yes
Chile Get DTE Status	Yes	Yes	Yes
Chile Sign DTE	Yes	Yes	Yes
Chile Send Receivable Transfer File	Yes	Yes	Yes
Chile Get Receivable Transfer File Status	Yes	Yes	Yes

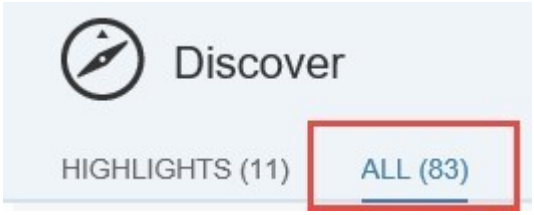
Integration Flow Name	Dynamic Signature Enabled	Externalized Credentials	Externalized Address
Chile Boleta	Yes	Yes	Yes
Chile Send Boleta	Yes	Yes	Yes
Chile Fetch Boleta Status	Yes	Yes	Yes
Chile Submit Boleta	Yes	Yes	Yes
Chile Get Boleta Token	Yes	NA	NA
Chile Sign Boleta	Yes	NA	NA
Chile Get Boleta Status	Yes	Yes	Yes
Chile Submit Daily Summary Boleta	Yes	Yes	Yes
Chile Get Daily summary Boleta Status	Yes	Yes	Yes
Chile Get DTE Token	Yes	NA	NA
Chile Query DTE Customer Response	Yes	Yes	Yes
Chile Process Incoming DTE	No	Yes	Yes
Chile Sign Delivery Note Ledger	No	Yes	Yes
Chile Pull SII Emails	No	Yes	Yes
Chile Process SII Emails	No	Yes	Yes

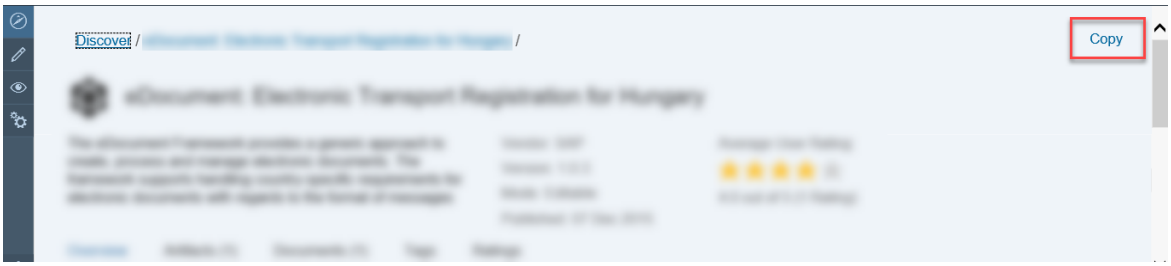
5.2 Copy Published Package

Context

Copy the package *SAP Document and Reporting Compliance: Electronic Documents for Chile* to the target tenant as follows:

Procedure

1. Log in to your SAP Integration Suite tenant.
2. Choose *Discover* > *All* > .


3. Search for *SAP Document and Reporting Compliance: Electronic Documents for Chile*.
4. Select the package and choose *Copy*.


5.3 Deploy Integration Flows

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

Context

The following integration flows are available in the integration package *SAP Document and Reporting Compliance: Electronic Documents for Chile*:

Integration Flow Name in WebUI	Project Name/Artifact Name
Chile Send DTE	com.sap.GS.Chile.SendMultipleDTE
Chile Get DTE Status	com.sap.GS.Chile.GetStatus
Chile Sign DTE	com.sap.GS.Chile.SignEnvioDTE
Chile Sign Sales and Purchase Ledger	com.sap.GS.Chile.SPLedger
Chile Sign Delivery Note Ledger	com.sap.GS.Chile.DeliveryNoteLedger

Integration Flow Name in WebUI	Project Name/Artifact Name
Chile Sign Daily Boleta Summary	com.sap.GS.Chile.DailyBoletaSummary
Chile Sign Monthly Boleta Summary - Obsolete	com.sap.GS.Chile.MonthlyBoletaSummary
Chile Process Incoming DTE	com.sap.GS.Chile.IncomingEnvioDTE
Chile Process Receipt	com.sap.GS.Chile.EnvioRecibo
Chile Configure Value Mappings	com.sap.GS.Chile.ValueMappings
Chile Send Mail	com.sap.GS.Chile.SendMail
Chile Send IDTE Acknowledgement	com.sap.GS.Chile.IncomingACKSII
Chile Send Receivable Transfer File	com.sap.GS.Chile.SendRTF
Chile Get Receivable Transfer File Status	com.sap.GS.Chile.ChileGetRTFStatus
Chile Boleta	com.sap.GS.Chile.Boleta
Chile Send Boleta	com.sap.GS.Chile.SendBoleta
Chile Fetch Boleta Status	com.sap.GS.Chile.FetchBoletaStatus
Chile Submit Boleta	com.sap.GS.Chile.SubmitBoleta
Chile Get Boleta Token	com.sap.GS.Chile.GetBoletaToken
Chile Sign Boleta	com.sap.GS.Chile.SignBoleta
Chile Get Boleta Status	com.sap.GS.Chile.GetBoletaStatus
Chile Submit Daily Summary Boleta	com.sap.GS.Chile.ChileSubmitDailySummaryBoleta
Chile Get Daily summary Boleta Status	com.sap.GS.Chile.ChileDailySummaryBoletaStatus
Chile Get DTE Token	com.sap.GS.Chile.ChileGetDTEToken
Chile Query DTE Customer Response	com.sap.GS.Chile.QueryCustomerResponse
Chile Pull SII Emails	com.sap.GS.Chile.PullSIIEmails
Chile Process SII Emails	com.sap.GS.Chile.ProcessSIIEmails

Procedure

1. Select the integration flow in the WebUI and choose *Deploy*.
2. After all the integration flows are deployed, note down the URLs of the endpoints for each service. Also, provide the endpoint URLs for SII in the externalized parameters of the integration flows for the test and production tenants.

For more information about how to change the endpoint URLs as per test and production environment, see Configure Integration Flow Receiver URLs [page 16].

3. To verify in the WebUI that the deployment has been successful, choose *Run* from the menu in the upper left corner.

   The integration flows must be in state *DEPLOYED*.

5.4 Configure Integration Flow Receiver URLs

Context

The integration flow endpoints are different for the test and production environment of SII and are as follows:

> **i Note**
>
> Endpoint URLs for Boletas are subject to change by SII. Visit https://www4c.sii.cl/bolcoreinternetui/api/ to cross-check the endpoint URLs below.

Receiver	Environment	URL
`SII_SEED`	Test	https://maullin.sii.cl/DTEWS/CrSeed.jws
	Production	https://palena.sii.cl/DTEWS/CrSeed.jws
`SII_TOKEN`	Test	https://maullin.sii.cl/DTEWS/GetTokenFromSeed.jws
	Production	https://palena.sii.cl/DTEWS/GetTokenFromSeed.jws
`SII_SEND_DTE` or `SII`	Test	https://maullin.sii.cl/cgi_dte/UPL/DTEUpload
	Production	https://palena.sii.cl/cgi_dte/UPL/DTEUpload
`SII_GET_STATUS`	Test	https://maullin.sii.cl/DTEWS/QueryEstDte.jws
	Production	https://palena.sii.cl/DTEWS/QueryEstDte.jws
`SII_STAT_AV`	Test	https://maullin.sii.cl/DTEWS/services/QueryEstDteAv
	Production	https:// palena.sii.cl/DTEWS/services/QueryEstDteAv

Receiver	Environment	URL
`SII_STAT_UP` or `Daily Summary Status`	Test	https://maullin.sii.cl/DTEWS/QueryEstUp.jws
	Production	https:// palena.sii.cl/DTEWS/QueryEstUp.jws
`SendMail`	Test/Production	Optional (If you maintain the credential name, make sure that credentials are deployed in your tenant with the same name.)
`Receiver1` (IDTE Ack to SII – receiver) or `Get_Hist_Events`	Test	https://ws2.sii.cl/WSREGISTRORECLAMODTECERT/registroreclamodteservice
	Production	https://ws1.sii.cl/WSREGISTRORECLAMODTE/registroreclamodteservice
`RTF_Get_Cesion_Status`	Test	https://maullin.sii.cl/DTEWS/services/wsRPETCConsulta
	Production	https://palena.sii.cl/DTEWS/services/wsRPETCConsulta
`RTF_Get_Envelop_Status`	Test	https://maullin.sii.cl/DTEWS/services/wsRPETCConsulta
	Production	https://palena.sii.cl/DTEWS/services/wsRPETCConsulta
`SII_SEND_RTF`	Test	https://maullin.sii.cl/cgi_rtc/RTC/RTCAnotEnvio.cgi
	Production	https://palena.sii.cl/cgi_rtc/RTC/RTCAnotEnvio.cgi
Boleta_Get_Status	Test	https://apicert.sii.cl/recursos/v1/boleta.electronica/$%7bproperty.RutEmisor%7d-$%7bproperty.DVEmisor%7d-$%7bproperty.TipoDoc%7d-$%7bproperty.FolioDoc%7d/estado?rut_receptor=$%7bproperty.RutReceptor%7d&dv_receptor=$%7bproperty.DVReceptor%7d&monto=$%7bproperty.Monto%7d&fechaEmision=$%7bproperty.Fecha%7d

Receiver	Environment	URL
	Production	https://api.sii.cl/recursos/v1/boleta.electronica/$%7bproperty.RutEmisor%7d-$%7bproperty.DVEmisor%7d-$%7bproperty.TipoDoc%7d-$%7bproperty.FolioDoc%7d/estado?rut_receptor=$%7bproperty.RutReceptor%7d&dv_receptor=$%7bproperty.DVReceptor%7d&monto=$%7bproperty.Monto%7d&fechaEmision=$%7bproperty.Fecha%7d
SII_Token	Test	https://apicert.sii.cl/recursos/v1/boleta.electronica.token
	Production	https://api.sii.cl/recursos/v1/boleta.electronica.token
SII_Seed	Test	https://apicert.sii.cl/recursos/v1/boleta.electronica.semilla
	Production	https://api.sii.cl/recursos/v1/boleta.electronica.semilla
Chile_Bol	Test	https://pangal.sii.cl/recursos/v1/boleta.electronica.envio
	Production	https://rahue.sii.cl/recursos/v1/boleta.electronica.envio

To change these parameters on the WebUI, perform the following steps:

Procedure

1. From the menu in the upper left corner, choose *Design*.
2. Click on the *SAP Document and Reporting Compliance: Electronic Documents for Chile* package and then on *Package Content*.
3. For the integration flow that you want to change, choose *Actions* > *Configure*.
4. On the *Receiver* tab, make changes as required.

   See the following example:

5. Choose *Save*.

5.5 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

1. In the *Operations* view, click the *User Roles* tile.
2. Choose *Add* and enter a role name and a role description and click *Add*.
3. To assign the custom role to the integration, go to *Cloud Cockpit*, choose your subaccount and create an instance as described in this topic Creating Service Instances.

   > **i Note**
   >
   > In step 3.e of the procedure in the Creating Service Instances topic, enter the user role you created in step 2 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 JSON format. Enter the code in the text field and choose *Next*.

4. Proceed with the steps to create a service key as described in Creating Service Instances.

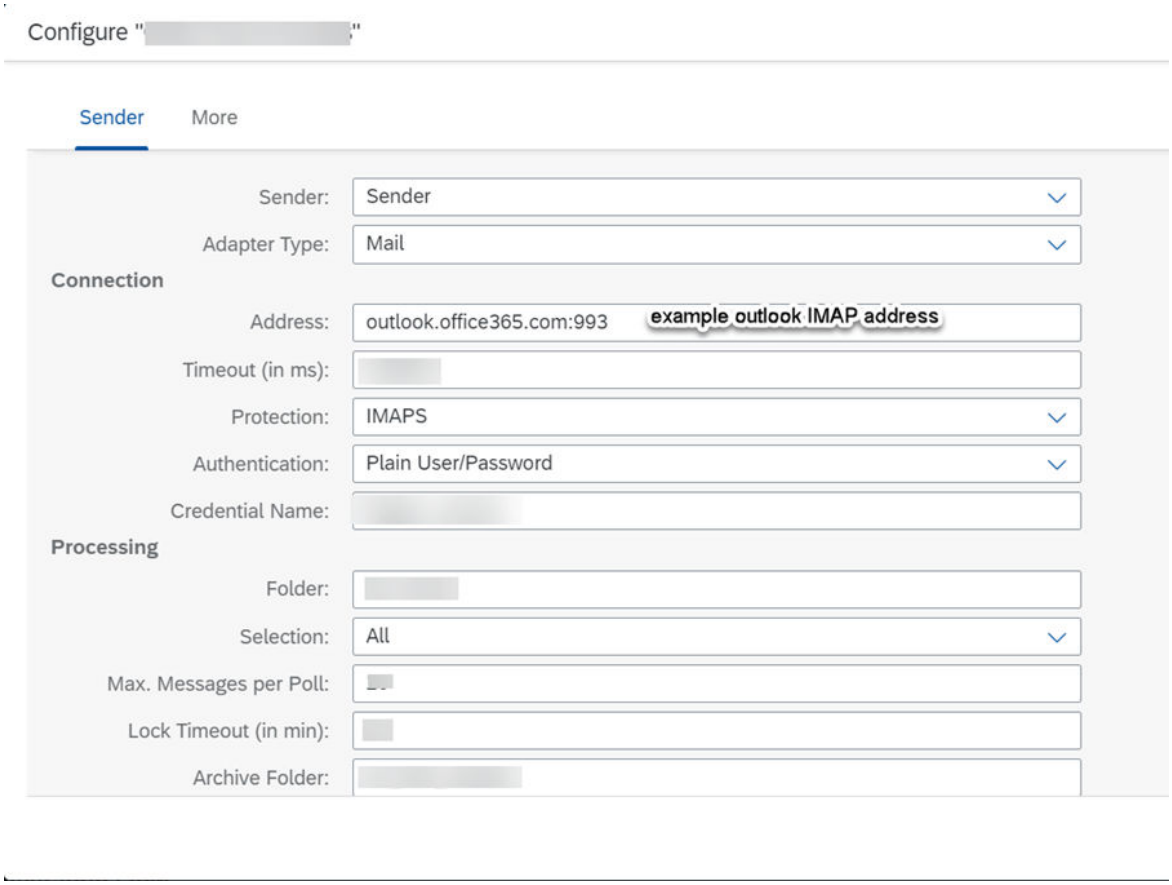
   You generate a service key that holds the authentication information with the custom role.

5.6 Configure Chile Pull SII E-Mails Integration Flow

This section provides the configurations required to be done before deploying the `Chile Pull SII Emails` integration flow.

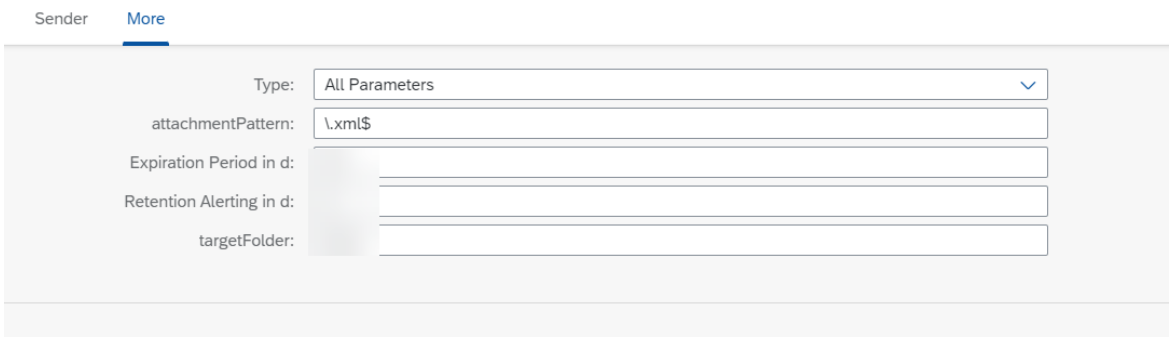
Procedure

1. Enter the following values in the *Sender* tab to set up the connection details for your e-mail address.
    - The address of your email server.
    - Timeout parameter (in milliseconds)
    - Type of authentication
    - Credential name for authentication
    - Name of the folder from where the acknowledgment mails are pulled.
    - Type of selection: *All* or *Undeard*
    - Maximum messages to be polled.
    - Lock timeout criteria (in minutes)
    - Name of the archive folder, where the acknowledgment mails are stored after pulling.
    - Scheduler criteria based on your requirement



Example of a configuration done on the Sender tab.

2. Enter the following values in the *More* tab.
   - Attachment pattern: Enter **`\.xml$`** in this filed.
   - Expiry period (in days)
   - Retention alerting period (in days)
   - Target folder



Example of a configuration done on the More tab.

6 Configuration Steps in SAP Backend Systems

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

6.1 Set Up Connection with Backend System

If you are using basic authentication, the SAP Integration Suite tenant needs to have basic authorization enabled for the test user (SCN credentials). If you are using certificate-based authentication, you need to maintain the certificates properly on the SAP Integration Suite tenant keystore and on the integration flows.

To change the authentication type 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 Chile* package and then on the integration flow that you want to change.
3. In the lower right corner, choose *Edit*.
4. On the sender side, click on *ERP*.

   > **i** Note
   >
   > You must click directly on the letters or on the icon on the left.

5. In the *Authentication Type* dropdown box, select either *Basic Authentication* or *Certificate Based Authentication*.
   When you select *Certificate Based Authentication*, you have to upload a certificate. Choose *Add* to assign additional certificates.

6.2 Create Logical Ports in SOAMANAGER for Cloud Foundry

Required steps for configuring SOAMANAGER to connect SAP backend system with SAP Integration Suite.

Prerequisites

You must refer to the instructions provided in SAP Note 3329749 to establish the configurations necessary for using the new boleta integration flows from version `2.4.9` of the `SAP Document Compliance: Electronic Documents for Chile` package.

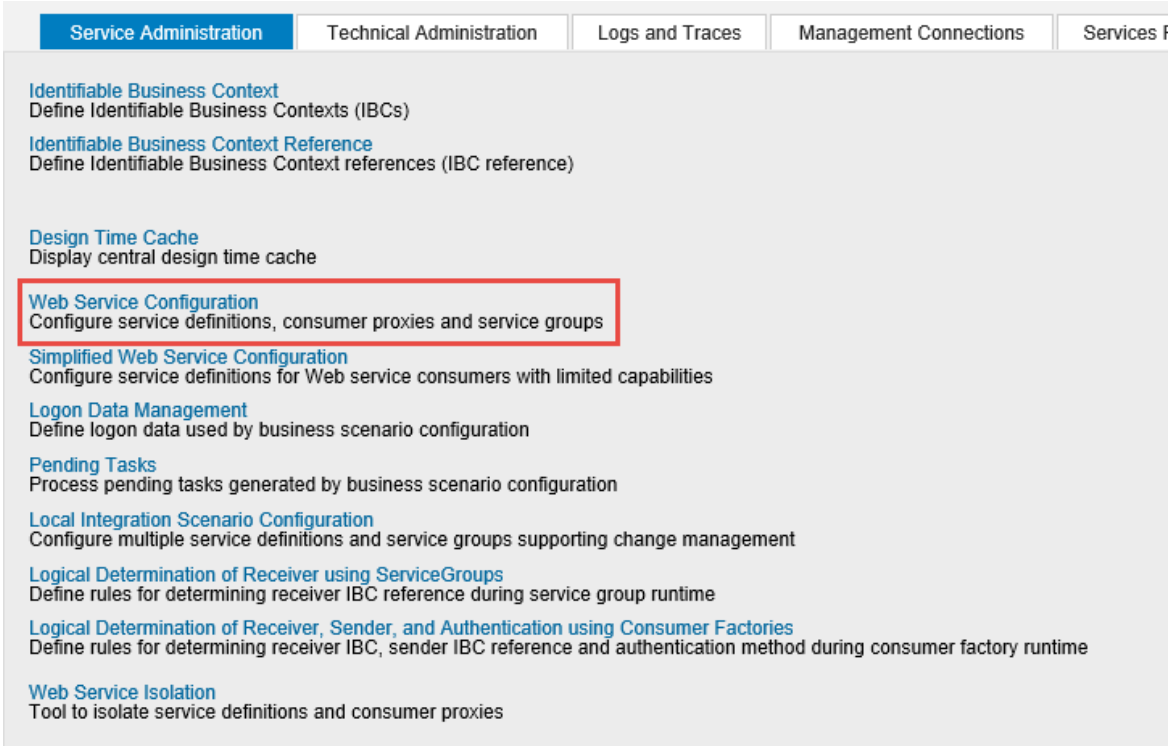
Context

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.

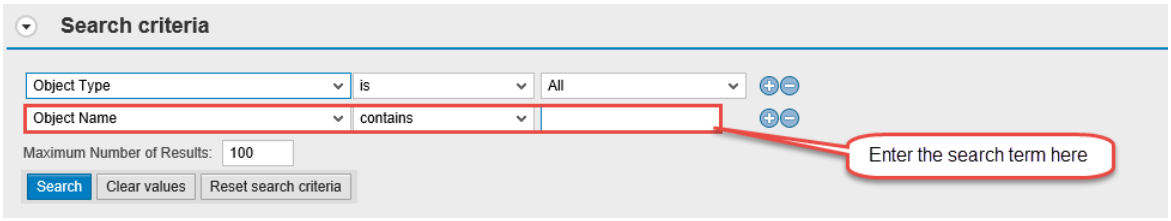
> **i** Note
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

Procedure

1. `SOAMANAGER` transaction and search for *Web Service Configuration* .



2. Find the proxies for Chile with search term CO_EDO_CL*.



The following table lists the proxies and the logical port names, and the relevant endpoints:

List of Proxies, Logical Port Names, and Paths

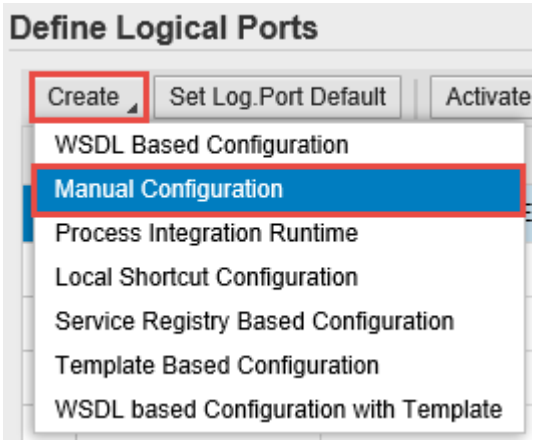
Proxy Name	Logical Port Name	Endpoint URL
CO_EDO_CL_DTE_TRANSMIS_SERV	EDO_CL_DTE_TRANS-MIS_SERV_PORT	/cxf/ChileSendMultipleDTE
CO_EDO_CL_DTE_GETSTATUS_SERV	EDO_CL_DTE_GETSTA-TUS_SERV_PORT	/cxf/ChileEnvioDTEGetStatus
CO_EDO_CL_LEDGER_SERV	EDO_CL_LEDGER_SERV_PORT	/cxf/ChileSignSPLedger
CO_EDO_CL_DELIVERYNOTE_SERV	EDO_CL_DELNOTE_SERV_PORT	/cxf/ChileSignDeliveryNoteLedger
CO_EDO_CL_CHILE_DAILY_BO-LETA_S	EDO_CL_DLY_SUMM_TRANSM_SERV_PORT	/cxf/ChileSIgnDailyBoletaSummary

Proxy Name	Logical Port Name	Endpoint URL
CO_EDO_CL_MONTHLY_BOLETA_SERV - Obsolete	EDO_CL_MON_SUMM_TRANSM_SERV_PORT	/cxf/ChileSIgnMonthlyBoletaSummary
CO_EDO_CL_IDTE_SERV	EDO_CL_IDTE_SERV_PORT	/cxf//ChileIncomingEnvioDTE
CO_EDO_CL_IDTE_ENVIORECIB_SERV	EDO_CL_IDTE_ENVIORECIB_PORT	/cxf//ChileSignEnvioRecibo
CO_EDO_CL_IDTE_ACKTOSII_SERV	EDO_CL_IDTE_SIIACK	/cxf/ChileIncomingSIIACK
CO_EDO_CL_IDTE_ACKTOSII_SERV	EDO_CL_IDTE_FECHAREQ	/cxf/ChileIncomingSIIACK
CO_EDO_CL_RTF_SERV	EDO_LP_CHILE_RTF_GET_STATUS	/cxf/ChileGetRTFStatus
CO_EDO_CL_RTF_SERV	EDO_LP_CHILE_RTF_SUBMIT	/cxf/ChileSendRTF
CO_EDO_CL_BOLETA_V11	EDO_CL_BOLETA_GETSTATUS_V11	/cxf/ChileBoletaOperationsV11
CO_EDO_CL_BOLETA_V11	EDO_CL_BOLETA_SUBMIT_V11	/cxf/ChileBoletaOperationsV11
CO_EDO_CL_DAILY_BOLETA_SUMMARY	EDO_CL_DLYSUMBOL_SUBMIT	cxf/ChileSubmitDailySummaryBoleta
CO_EDO_CL_DAILY_BOLETA_SUMMARY	EDO_CL_DLYSUMBOL_GETSTATUS	cxf/ChileDailySummaryBoletaStatus
CO_EDO_CL_IDTE_ACKTOSII_SERV	EDO_CL_DTE_CUSTOMER_STATUS	cxf/ChileQueryDTECustomerResponse
CO_EDO_CL_SIGN_ENVIODTE	EDO_CL_SIGN_ENVIODTE_SERV_PORT	/cxf/ChileSignEnvioDTE
CO_EDO_CL_CHILE_MAIL_UPDATE	EDO_CL_SII_EMAIL	/cxf/ChileProcessEmails

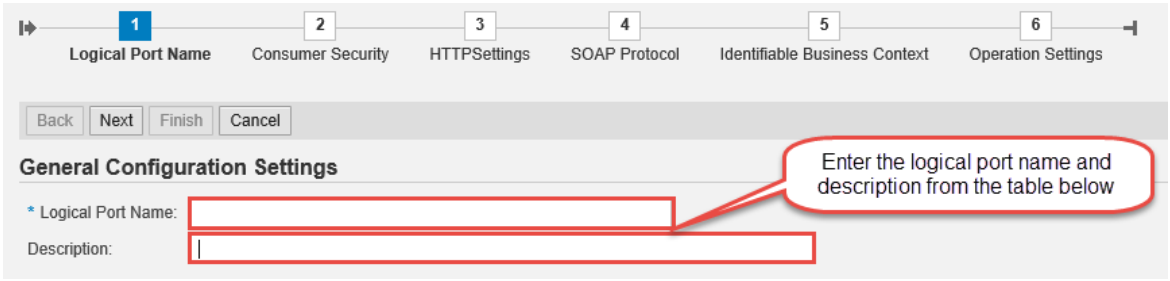
Add the following descriptions to the ports:

- EDO_CL_DTE_TRANSMIS_SERV_PORT: Chile eDocument - DTE Transmission Service
- EDO_CL_DTE_GETSTATUS_SERV_PORT: Chile eDocument - DTE Get Status Service
- EDO_CL_LEDGER_SERV_PORT: Chile eDocument - Sign Ledger Service

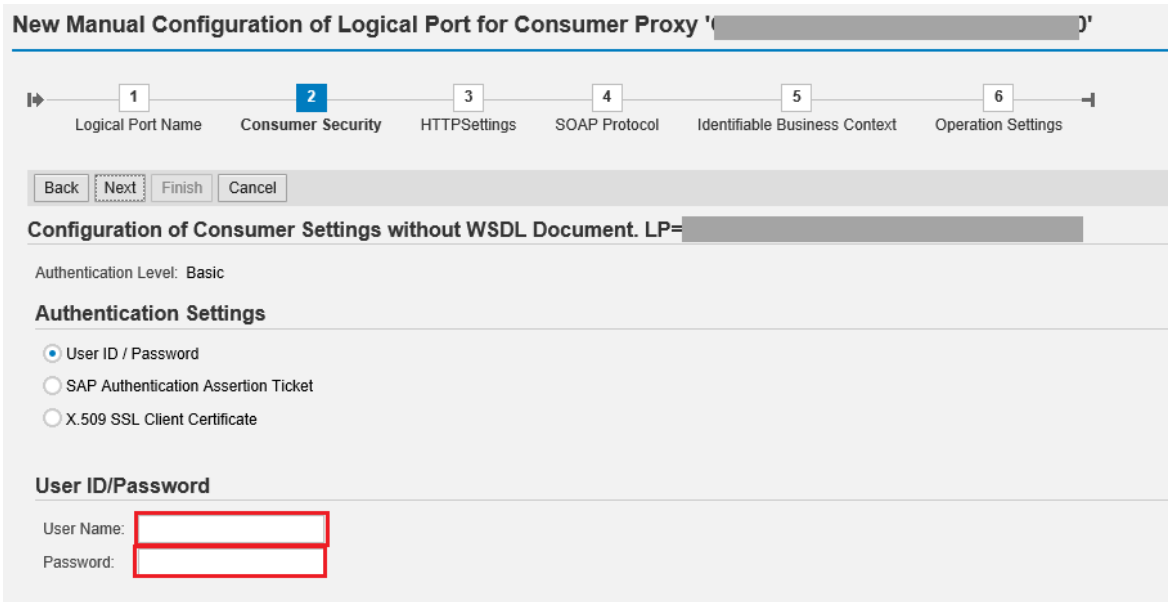
3. In the *Result List*, select a proxy and create a logical port for each proxy. Choose *Create* > *Manual Configuration*.



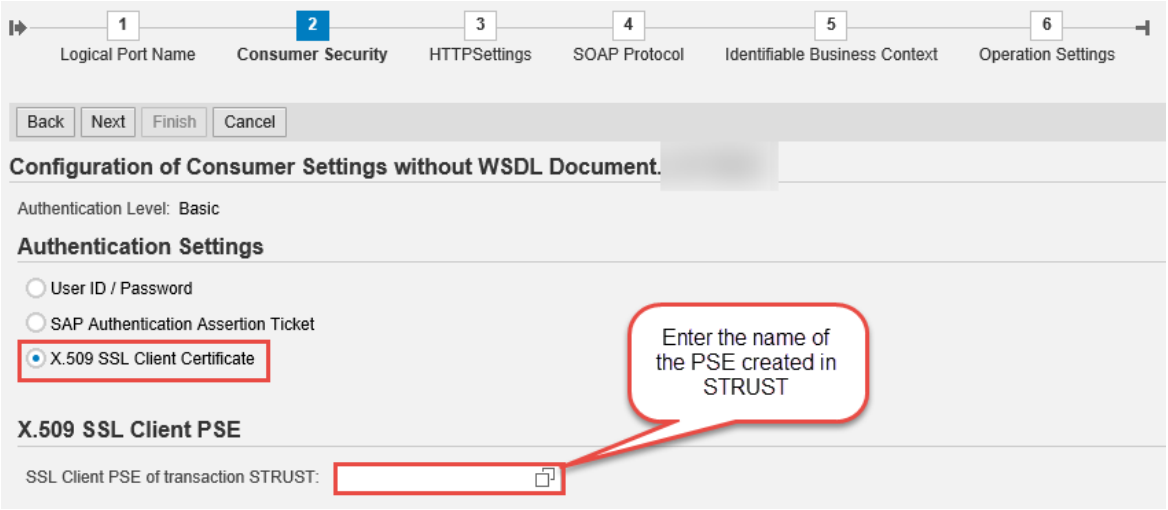
4. Enter the logical port name and a description.



5. The configuration you perform in the *Consumer Security* tab in the *Configuration* screen depends on the security used in the communication between the back-end system and SAP Integration Suite.

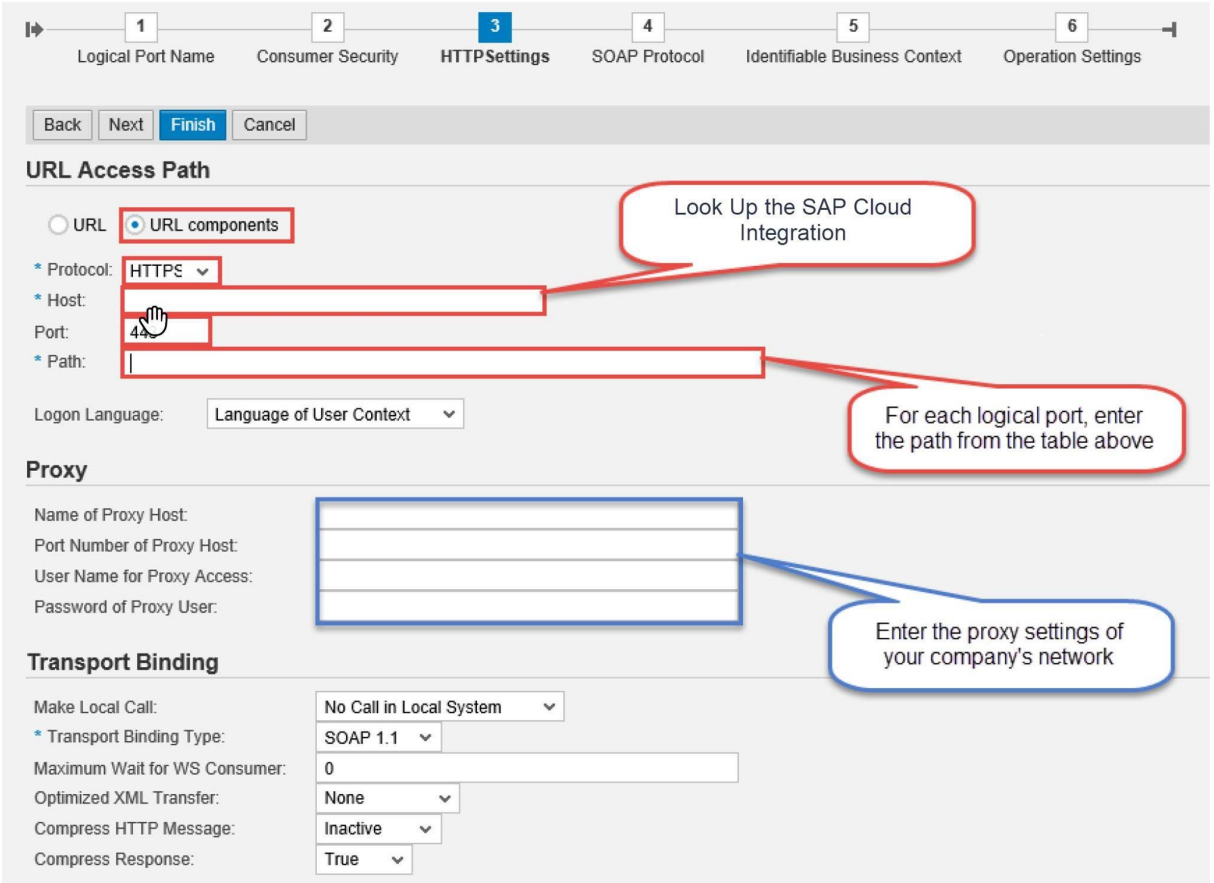


- If you use the basic authentication for *User Name*, enter the value for the **clientid** and for *Password*, enter the value for **clientsecret**. You have created these values for your service instance in SAP Integration Suite. See Creating Service Instances.



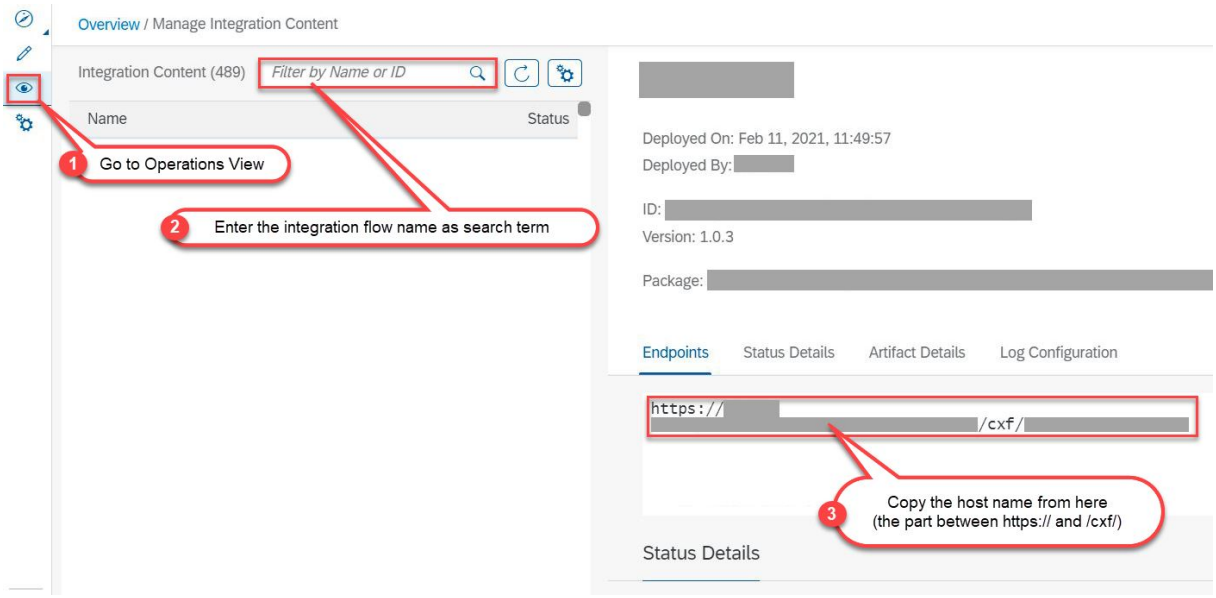
- If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have updloaded to STRUST. You must configure this certificate in SAP Integration Suite too. For that you create a service instance using the required grant_type. You create the service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



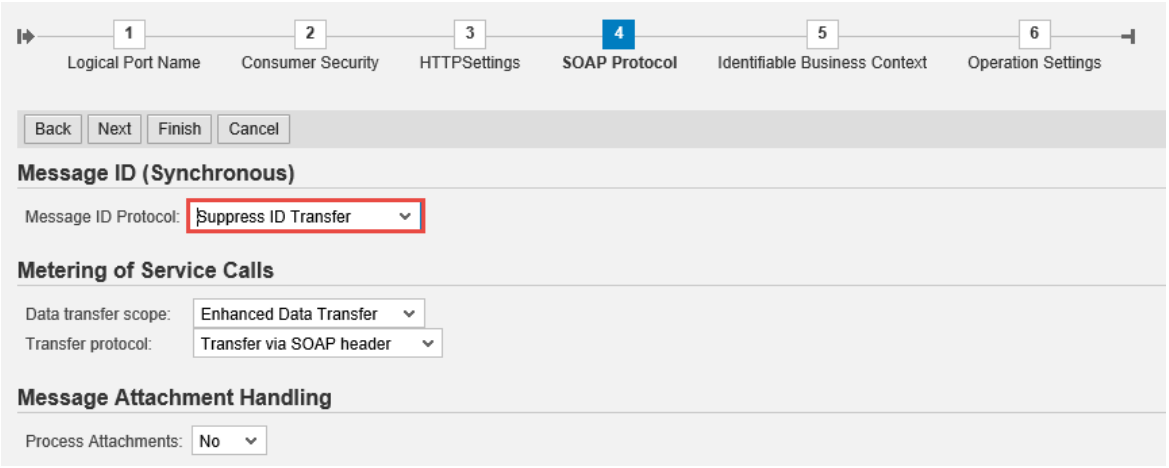
Port 443 is the standard port for the HTTPS protocol.

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 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.

9. Remember to create logical ports for each proxy and to execute the steps below 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 `EDOINTV` view.

For more information, see the AIF setup SAP Notes (for example, 2069251 for SAP ERP). For a full of list of AIF setup SAP Notes, see the Installation Overview Notes for Chile.

7 Configuration Steps for SAP S/4HANA Cloud

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

7.1 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.

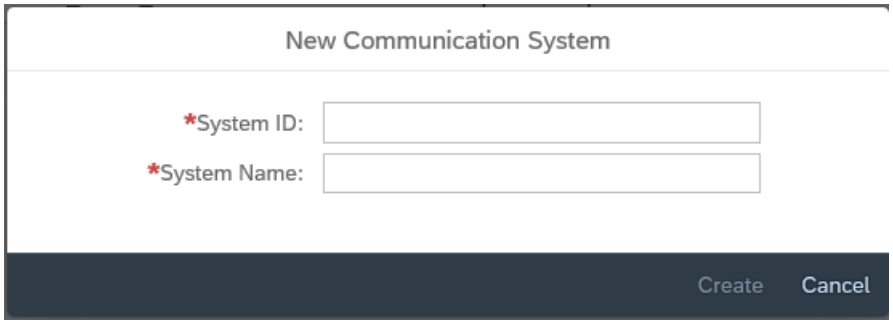
Procedure

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.



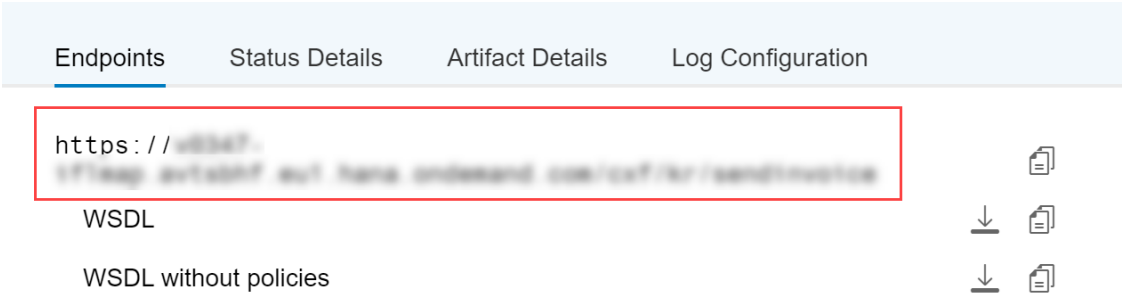
4. Choose *Create*.

   An editing screen for the communication system appears.

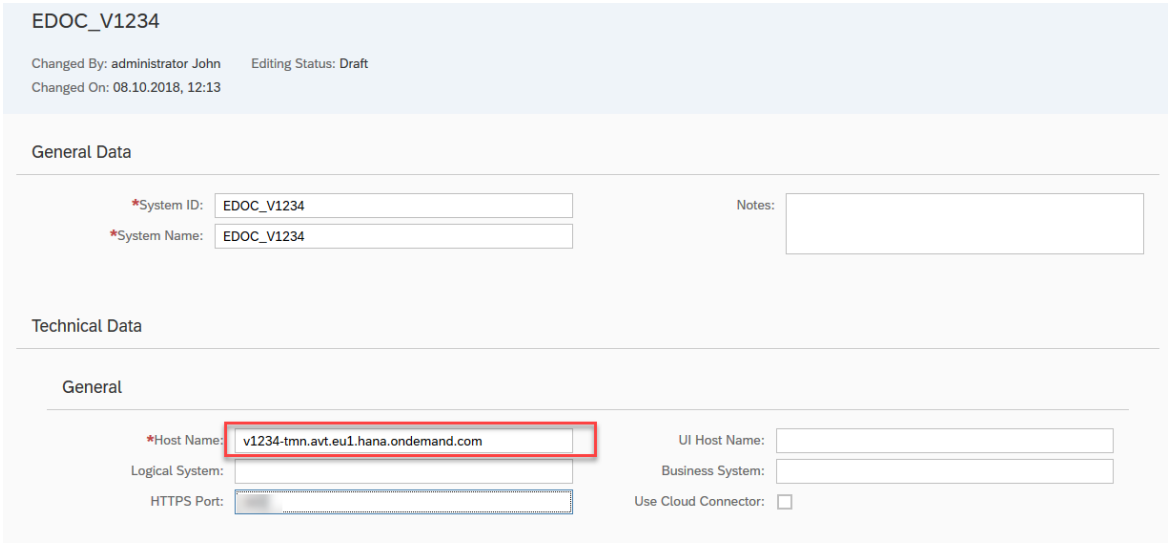
5. In the *Technical Data* section, enter the host name and HTTPS port of your SAP Integration Suite tenant.

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

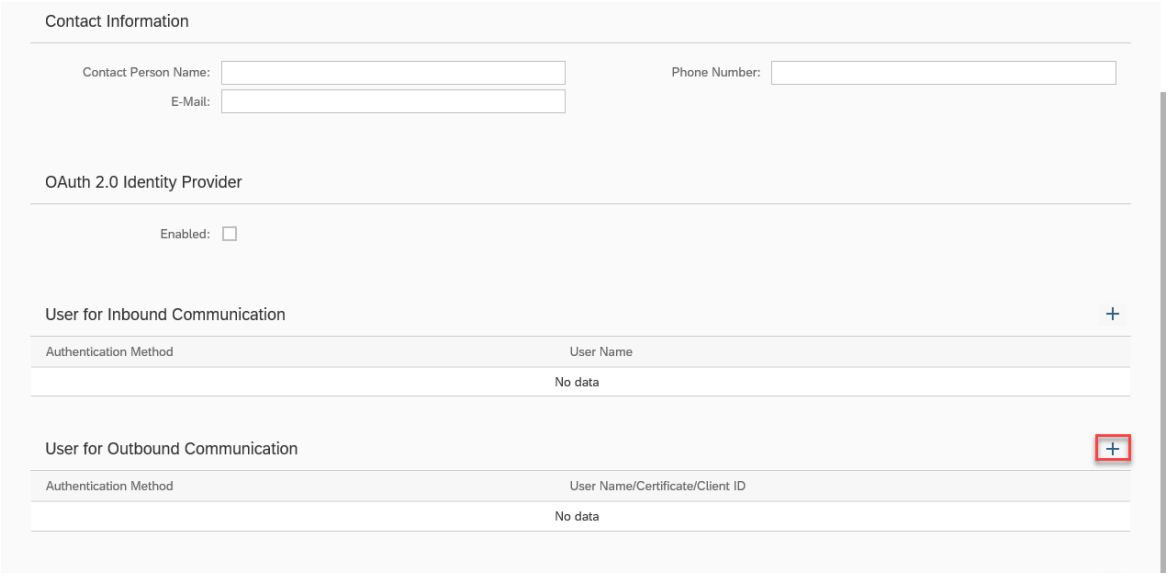
   1. From the menu on the left, choose *Monitor*.
   2. Select *Manage Integration Content* (All).
   3. Search for the integration flow for the scenario you are configuring.
   4. Find the host name from the *Endpoints* tab.
      The composition of an endpoint URL is **https://**`<host name>/<path>`.



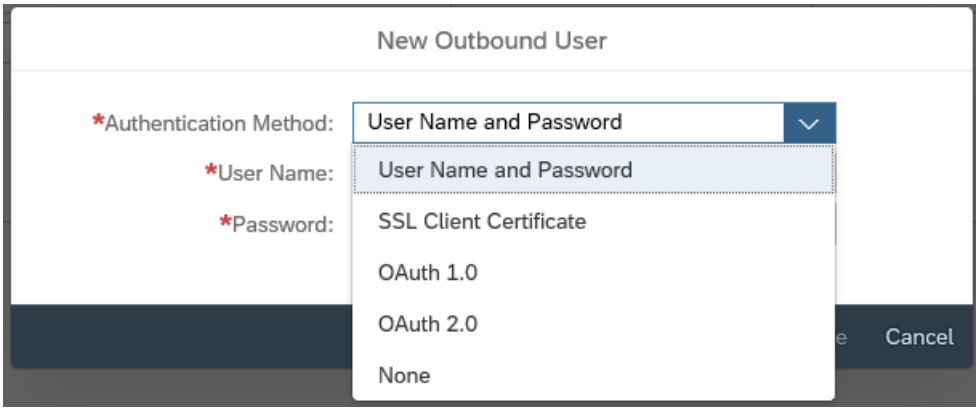
   See the following example:



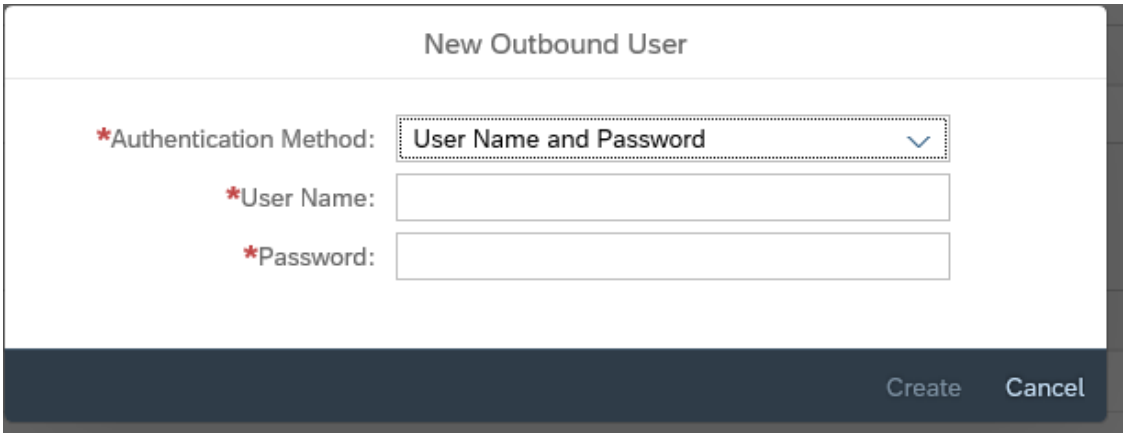
6. In the *User for Outbound Communication* section, choose +.



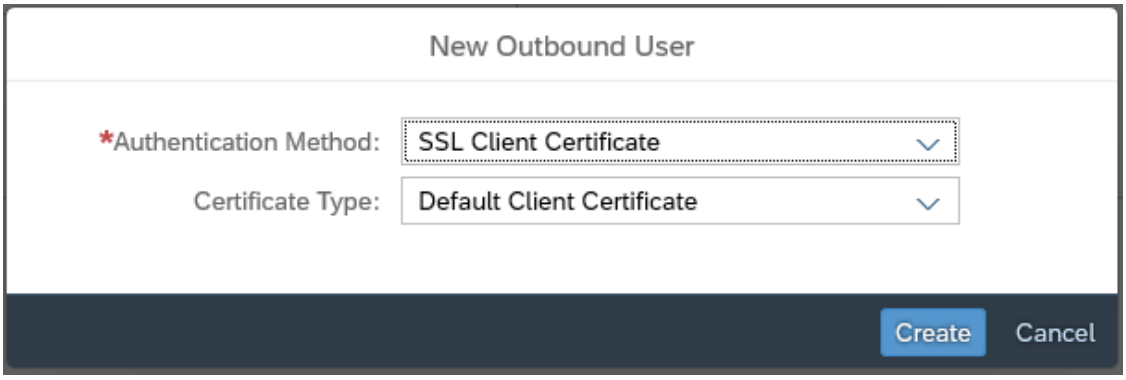
7. Select an authentication method, which is used to connect to your SAP Integration Suite tenant. Proceed as follows:



- 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*.

7.2 Configure Communication Arrangement

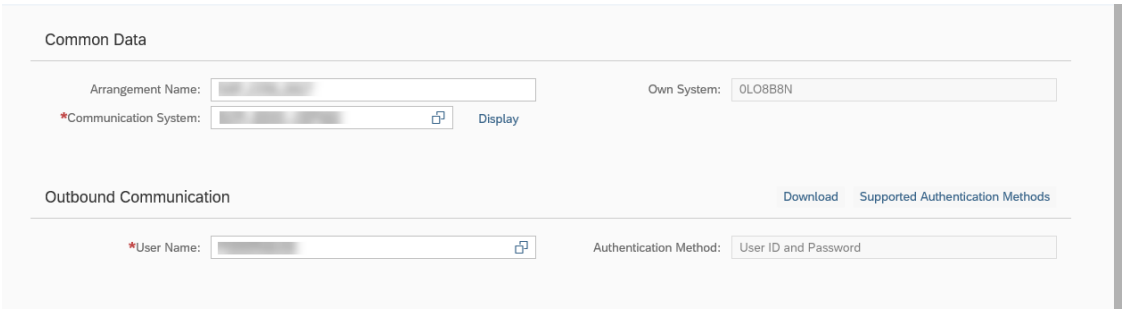
Configuration steps for SAP S/4HANA Cloud Communication Arrangement.

Procedure

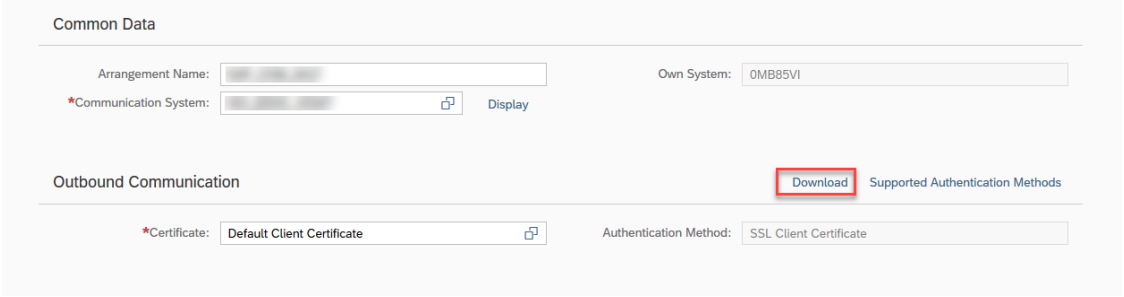
1. Login to your S/4HANA Cloud tenant with the Cloud User.
2. Find and launch the application *Communication Arrangements*.

3. Choose *New*. In the new pop-up window, enter the scenario `SAP_COM_0669` (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_0669_<name of SAP Integration Suite tenant>`, for example, `SAP_COM_0669_V1234` for tenant host name beginning with v1234-tmn.

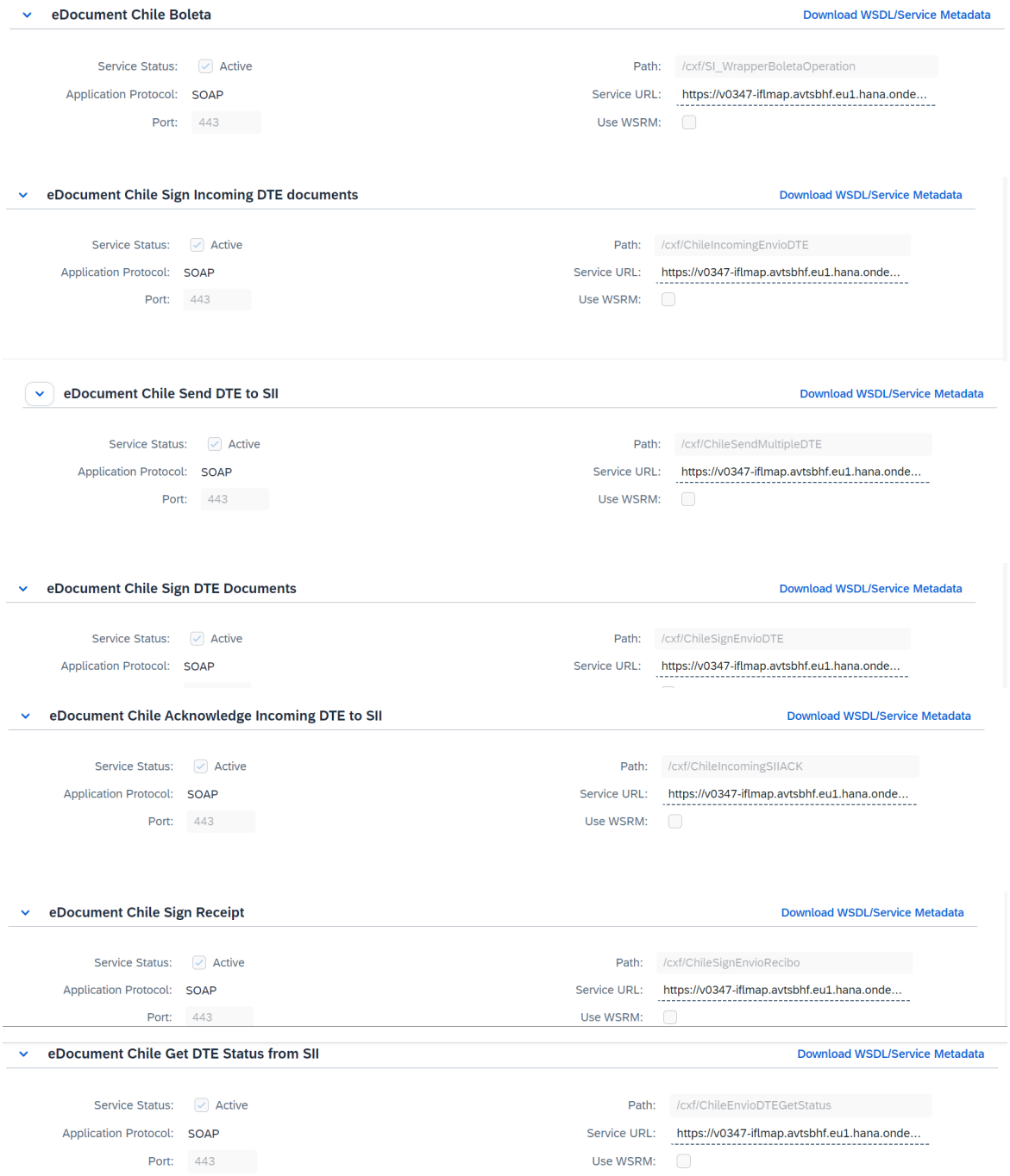
4. Choose *Create*.
5. In the new window, choose the communication system created in the previous step (for example, `EDOC_V1234`) and the authentication method, relevant to the communication system.
    - If the authentication is by User ID, then select *User Name and Password* from the *Outbound Communication*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

8 Testing the Communication

Context

To test the communication, we recommend that you create and send an electronic document from SAP S/4HANA Cloud. The way you do this depends on how the system is configured to generate and send eDocuments. Follow the steps described below.

Procedure

1. Create a relevant document for Chile (for example, an invoice).

   > **i** Note
   >
   > If the system is configured to generate an electronic document for the selected document type, an instance of the eDocument will be created as soon as the document is posted (for example, when you save a billing document).

2. Go to the *eDocument Cockpit* app.
3. From the *Result Overview*, select the relevant process for Chile.
4. Select the eDocument and choose *Submit* to trigger the communication with SAP Integration Suite. The system displays the eDocuments that match the search on the right side of the Cockpit.
5. From the list of eDocument displayed, find the one that you just created and check the following:
   - You can double-check if the message went through on the SAP Integration Suite tenant.
   - You can double-click on the *Interface Message GUID* field to navigate to AIF and look at the log. Communication errors will be 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 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