



Integration Guide | PUBLIC
2023-06-02

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

Content

- 1 Disclaimer. 3**
- 2 Introduction. 4**
- 3 Prerequisites. 5**
 - 3.1 Installation of eDocuments Full Solution. 5
- 4 Connectivity Steps. 6**
 - 4.1 Setup of Secure Connection. 6
 - Set Up SAP Cloud Integration Tenants. 7
 - Retrieve and Save Public Certificates. 7
 - Upload the Certificates. 8
 - Authenticate Integration Flows. 8
 - 4.2 Registration at SII. 9
 - Generating and Importing Certificates. 10
- 5 Configuration Steps in SAP Integration Suite. 12**
 - 5.1 Deploy Customer Certificate and Credentials to Tenants. 12
 - 5.2 Copy Published Package. 14
 - 5.3 Deploy Integration Flows. 15
 - 5.4 Configure Integration Flow Receiver URLs. 17
 - 5.5 Configure Chile Pull SII E-Mails Integration Flow. 20
- 6 Configuration Steps in SAP Backend Systems. 22**
 - 6.1 Set Up Connection with Backend System. 22
 - 6.2 Create Logical Ports in SOAMANAGER 22
- 7 Configuration Steps for SAP S/4HANA Cloud. 30**
 - 7.1 Configure Communication System. 30
 - 7.2 Configure Communication Arrangement. 33
- 8 Testing the Communication. 36**

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 Cloud Integration 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 Cloud Integration tenant so that the integration between the systems works.

The setup steps are typically done by an SAP Cloud Integration consulting team, which is responsible for configuring the SAP back-end systems and the connection with SAP Cloud Integration. This team may be also responsible for maintaining the integration content and certificates/credentials on the SAP Cloud Integration tenant.

i Note

This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Integration Suite tenant. It may happen, however, that in the SAP S/4HANA Cloud tenant 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 SAP S/4HANA Cloud 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 prerequisites described in this section are fulfilled.

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

You use SAP ERP Trust Manager (transaction STRUST) to manage the certificates required for a trustworthy SSL connection. The certificates include public certificates to support outbound connections, as well as trusted certificate authority (CA) certificates to support integration flow authentication.

Refer to the system documentation for more information regarding the certificate deployment to SAP back-end systems. In case of issues, refer to the following SAP notes:

- [2368112](#)  Outgoing HTTPS connection does not work in AS ABAP
- [510007](#)  Setting up SSL on Application Server ABAP

For more information, refer to [Operating and Monitoring Cloud Integration](#)

i Note

If you encounter any issues in the information provided in the SAP Cloud Integration product page, open a customer incident against the LOD-HCI-PI-OPS component.

Client Certificate

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

For information about creating your own certificate and get it signed by a trusted certificate authority (CA), see [Authenticate Integration Flows \[page 8\]](#).

4.1.1 Set Up SAP Cloud Integration Tenants

Ensure that your SAP Cloud Integration test and production tenants are live, and users in the tenants have the rights to copy the integration package and to configure and deploy the integration flows.

When your tenants are provisioned, you receive an email with a Tenant Management (TMN) URL. You need this URL when configuring on your SAP S/4HANA Cloud tenant the communication with the SAP Cloud Integration tenant.

To be able to deploy the security content you must be assigned the `AuthGroup.Administrator` role.

If you are a first-time user, you must first set up your users (members) and their authorizations in the SAP BTP cockpit.

4.1.2 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.

Context

Find and save the public certificates from your SAP Cloud Integration 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. Select the subscription with suffix **iflmap** as this corresponds to your worker node within SAP Cloud Integration.

Alternatively, use the URL emailed to you with your SAP Cloud Integration subscription details. The URL has the following format **`https://xxxxx.hana.ondemand.com/itspaces`**.

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.

4.1.3 Upload the Certificates

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

Context

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

Procedure

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

4.1.4 Authenticate Integration Flows

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

Context

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

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

Procedure

1. Access transaction STRUST.

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

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

The CA may have specific requirements and request company-specific data, they may also require time to analyze your company before issuing a signed certificate. When signed, the CA provides the certificate for import.

5. Navigate to the PSE for **SSL Client Standard** and open it by double-clicking the PSE.
6. Switch to edit mode.
7. Choose the *Import certificate* button.
8. In the *Import Certificate* dialog box, enter or select the path to the CA-signed certificate and choose *Enter*. The certificate is displayed in the *Certificate* area.
9. Choose *Add to Certificate List* to add the signed certificate to the *Certificate List*.

Ensure that you import the CA root and intermediate certificates to complete the import.

10. Save your entries.

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

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.

The screenshot shows the 'Add RSA Key' dialog box in the SAP Cloud Integration interface. The dialog contains the following fields and options:

- Alias: [Text input field]
- File: [Text input field] with a 'Browse...' button
- Signature Algorithm: SHA-256/RSA (dropdown menu)
- Common Name (CN): [Text input field]
- Organizational Unit (OU): [Text input field]
- Organization (O): [Text input field]
- Location (L): Santiago
- State or Province (ST): Santiago
- Country/Region (C): CL
- E-Mail (E): [Text input field]
- Valid From: Feb 26, 2023
- Valid Until: Dec 2, 2024

Buttons: Add, Cancel

i 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

```

<?xml version="1.0" ?>
- <AUTORIZACION>
- <CAF version="1.0">
- <DA>
  <RE>7777777-7</RE>
  <RS>SIN RAZON SOCIAL/NOMBRES</RS>
  <TD>33</TD>
- <RNG>
  <D>996402</D>
  <H>996501</H>
</RNG>
  <FA>2003-08-29</FA>
- <RSAPK>

  <M>17j+AESZwodyO4ISMML06BtCiCcEp64jzrlyw35jo8gagJIUAInbUXhrARBKIUAP0MAT2s0FBIGE
  <E>Aw==</E>
</RSAPK>
  <IDK>100</IDK>
</DA>
<FRMA
  algoritmo="SHA1withRSA">E4/rPLg6T1101P1wX/rwu5+46lL+hvNEllGP2IN6gXqgxK9n7NMnzKrJgxKui
</CAF>
<RSASK>-----BEGIN RSA PRIVATE KEY-----
MIIBOwIBAAJBANe4/gBEmcKHcjUjJDCzugbQognBKeuI865csN+Y6PIGoIyFACJ
21F4awEQSpVAD9DAE9rNBQSBhMTWAvenn1hMCAQMCQQCP0KIVgxEsWkwnsOF11zSa
vNcFb1hvyW00e6HXqZfChC2r5J4i3I1yzUfD7VQ5Se8Et3liMqrBLzIJCytCftPb
AiEA65RGHJzdXsWcmwG4KrGpWv/xb2BCQ1dAxW9B9cmk430CIODqbBUKL2G5P6fk

```

For information about how to create a private key from the CAF Authorization XML files, see .

From version 2.4.2 onwards, the dynamic private key *Alias* is enabled for the following integration flows, which is of the format **chilesignaturekey_XXXX**, where **chilesignaturekey** is the suffix and **XXXX** 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
Chile Boleta	Yes	Yes	Yes

Integration Flow Name	Dynamic Signature Enabled	Externalized Credentials	Externalized Address
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

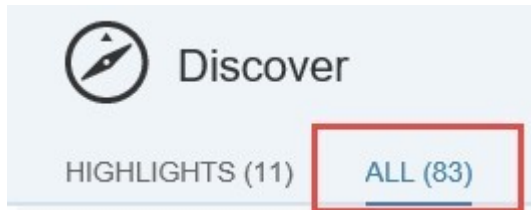
5.2 Copy Published Package

Context

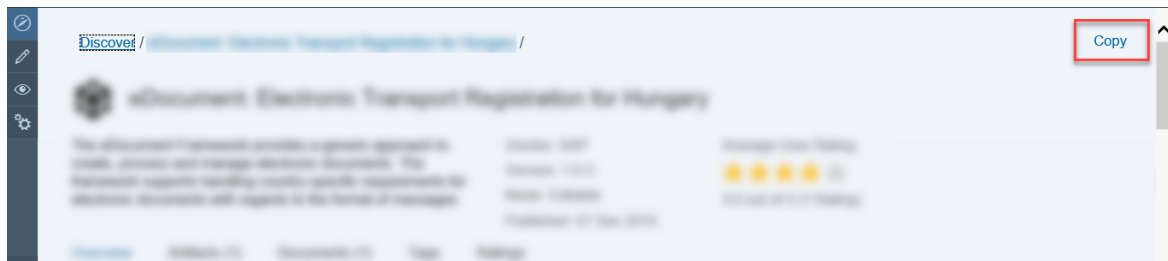
Copy the package [SAP Document and Reporting Compliance: Electronic Documents for Chile](#) to the target tenant as follows:

Procedure

1. Log in to your SAP Cloud Integration 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 \[page 17\]](#).

- 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:

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/WSREGISTRORECLAMODE/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/es-tado?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:

The screenshot shows a configuration window with three tabs: SENDER, RECEIVER (selected), and PARAMETERS. Under the RECEIVER tab, there are three configuration fields:

- Receiver:** A dropdown menu with the value "SII_SEND_DTE" selected.
- Adapter Type:** A dropdown menu with the value "HTTP" selected.
- Address:** A text input field containing the URL "https://example/cgi_dte/UPL/DTEUpload".

5. Choose [Save](#).

5.5 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

Configure " [redacted] "

Sender More

Connection

Sender: ▾

Adapter Type: ▾

Address:

Timeout (in ms):

Protection: ▾

Authentication: ▾

Credential Name:

Processing

Folder:

Selection: ▾

Max. Messages per Poll:

Lock Timeout (in min):

Archive Folder:

Example of a configuration done on the Sender tab.

2. Enter the following values in the *More* tab.

- Attachment pattern: Enter `\.xml$` in this field.
- Expiry period (in days)
- Retention alerting period (in days)
- Target folder

Sender **More**

Type: ▾

attachmentPattern:

Expiration Period in d:

Retention Alerting in d:

targetFolder:

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 Cloud Integration 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 Cloud Integration 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 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

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

Prerequisites

You must refer to the instructions provided in SAP Note [3329749](#) to establish the configurations necessary for using the new boleto integration flows from version 2.4.9 of the *SAP Document Compliance: Electronic Documents for Chile* package.

Context

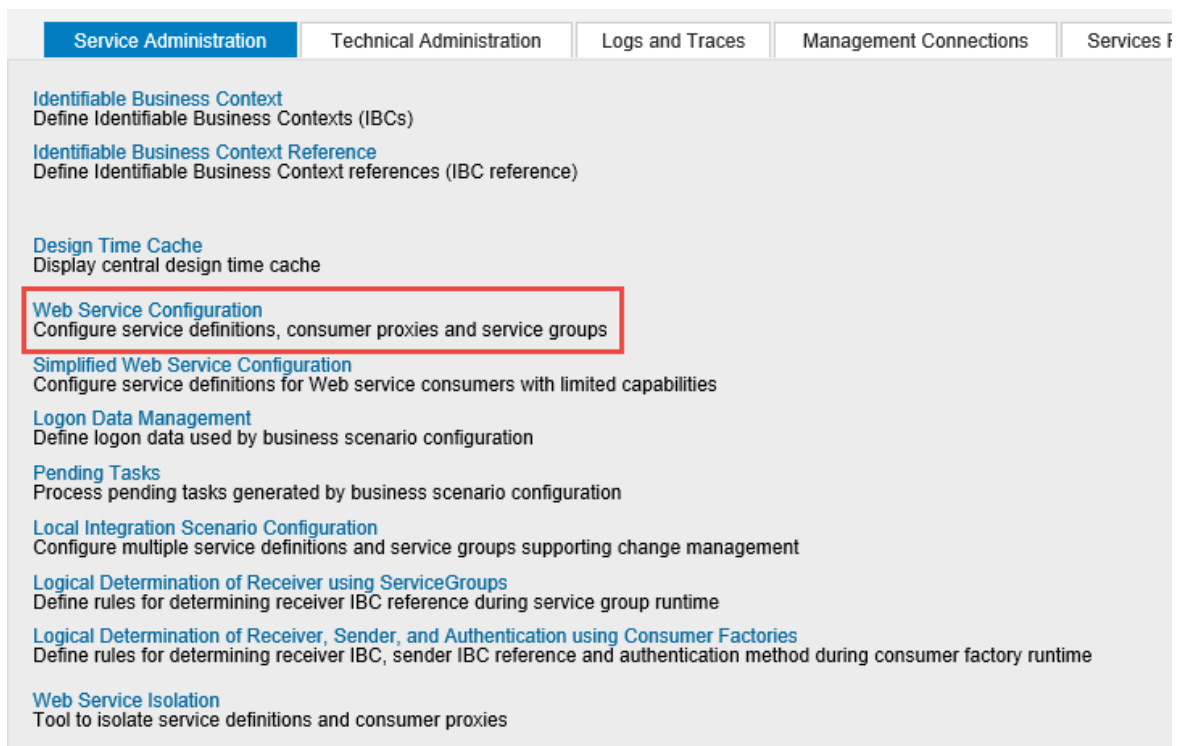
You configure proxies which are needed to connect to the SAP Cloud Integration tenant via logical ports. In test SAP back-end systems, the logical ports are configured to connect to the test tenant. In productive SAP back-end systems, the logical ports are configured to connect to the productive SAP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

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*.



The screenshot shows the SOAMANAGER transaction menu with the following items:

- Service Administration** (selected)
- Technical Administration
- Logs and Traces
- Management Connections
- Services f

Identifiable Business Context
Define Identifiable Business Contexts (IBCs)

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

Design Time Cache
Display central design time cache

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

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

Logon Data Management
Define logon data used by business scenario configuration

Pending Tasks
Process pending tasks generated by business scenario configuration

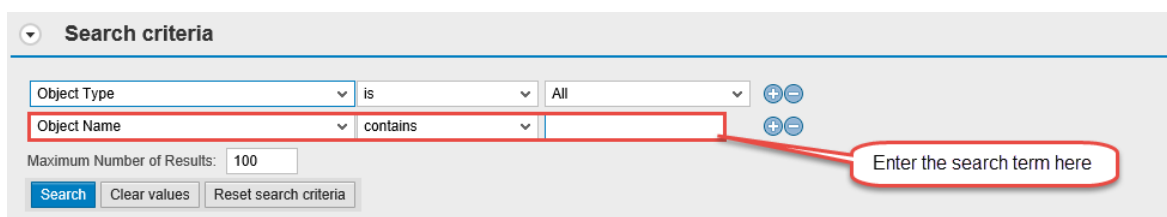
Local Integration Scenario Configuration
Configure multiple service definitions and service groups supporting change management

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

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

Web Service Isolation
Tool to isolate service definitions and consumer proxies

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



The screenshot shows the search criteria dialog with the following fields:

- Object Type: is All
- Object Name: contains

Maximum Number of Results: 100

Buttons: Search, Clear values, Reset search criteria

Callout bubble: Enter the search term here

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

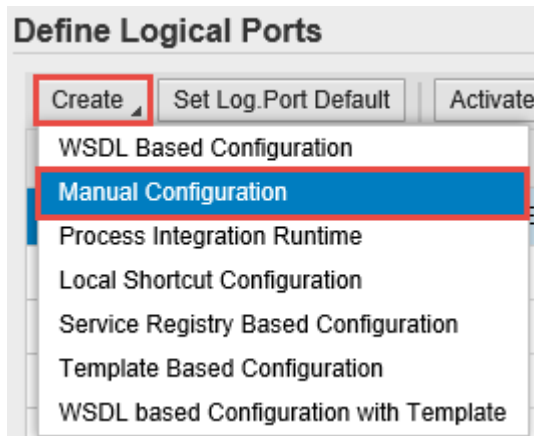
List of Proxies, Logical Port Names, and Paths

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_SER V_PORT	/cxf/ChileSlgnDailyBoletaSummary
CO_EDO_CL_MONTHLY_BO- LETA_SERV - Obsolete	EDO_CL_MON_SUMM_TRANSM_SER V_PORT	/cxf/ChileSlgnMonthlyBoletaSum- mary
CO_EDO_CL_IDTE_SERV	EDO_CL_IDTE_SERV_PORT	/cxf//ChileIncomingEnvioDTE
CO_EDO_CL_IDTE_ENVIORE- CIB_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_SUM- MARY	EDO_CL_DLYSUMBOL_SUBMIT	cxf/ChileSubmitDailySummaryBoleta
CO_EDO_CL_DAILY_BOLETA_SUM- MARY	EDO_CL_DLYSUMBOL_GETSTATUS	cxf/ChileDailySummaryBoletaStatus
CO_EDO_CL_IDTE_ACKTOSII_SERV	EDO_CL_DTE_CUSTOMER_STATUS	cxf/ChileQueryDTECustomerRes- ponse
CO_EDO_CL_SIGN_ENVIODTE	EDO_CL_SIGN_EN- VIODTE_SERV_PORT	/cxf/ChileSignEnvioDTE
CO_EDO_CL_CHILE_MAIL_UPDATE	EDO_CL_SII_EMAIL	/cxf/ChileProcessEmails

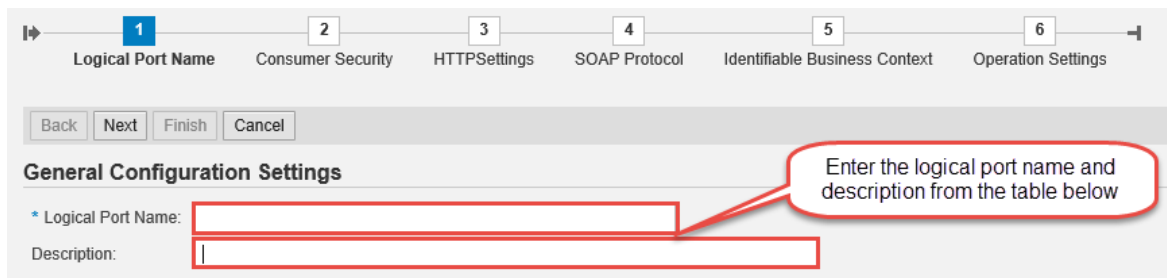
Add the following descriptions to the ports:

- 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 SAP back-end system and SAP Cloud Integration.
 - If you use the basic authentication, select the *User ID / Password* and depending on the environment your service is currently running, enter the **User Name** and **password**.
 - If you use certificate-based authentication, select *X.509 SSL Client Certification*. Ensure that the required certificates are available in the STRUST transaction.

i Note

If you do not see this option or cannot select it, check the SAP Notes [2368112](#) and [510007](#).

New Manual Configuration of Logical Port for Consumer Proxy 'XXXXXXXXXXXX'

1 Logical Port Name 2 Consumer Security 3 HTTPSettings 4 SOAP Protocol 5 Identifiable Business Context 6 Operation Settings

Back Next Finish Cancel

Configuration of Consumer Settings without WSDL Document. LP=XXXXXXXXXXXX

Authentication Level: Basic

Authentication Settings

User ID / Password
 SAP Authentication Assertion Ticket
 X.509 SSL Client Certificate

User ID/Password

User Name:

Password:

Additionally, you map the certificate to a user of your tenant with the `ESBMessaging.send` role. First, you export the certificate from the `STRUST` transaction. Save it locally and upload it to SAP Cloud Integration in the `Certificate-to-User Mappings`

1. Export the SSL Client PSE of the `STRUST` transaction.
2. Got to SAP Cloud Integration under `Overview > Certificate-to-User Mappings >`

Overview

Monitor Message Processing

All Integration Flows Past Hour 5 Messages	All Integration Flows Past Hour 0 Failed Messages	All Integration Flows Past Hour 0 Error Messages	All Integration Flows Past Hour 0 Retry Messages	All Integration Flows Past Hour 5 Completed Messages	+
-----------------------------------------------------	------------------------------------------------------------	-----------------------------------------------------------	-----------------------------------------------------------	---------------------------------------------------------------	---

Manage Integration Content

All 210 All	All 193 Started	All 15 Error	+
-------------------	-----------------------	--------------------	---

Manage Security

Security Material 38 Artifacts	Keystore 202 Entries	Certificate-to-User Mappings 1 Artifacts	Connectivity Tests
--------------------------------------	----------------------------	------------------------------------------------	--------------------

Manage Stores

Data Stores 3 Stores	Variables 0 Variables
----------------------------	-----------------------------

3. Choose `Add`.

Overview / Manage Certificate-to-User Mappings

Certificate-to-User Mappings (1) Filter by Name or DN Add Edit Delete Refresh Settings

User Name	Subject DN	Issuer DN	Serial Number	Valid Until	Modified By	Modified At

- Enter a user name with `ESBMessaging.send` role, upload the SSL Client PSE of the STRUST transaction and choose *OK*.

Add Certificate-to-User Mapping

*User Name:

*Certificate:

OK
Cancel

- On the *HTTP Settings* tab, make the following entries:

1 Logical Port Name
2 Consumer Security
3 HTTP Settings
4 SOAP Protocol
5 Identifiable Business Context
6 Operation Settings

Back
Next
Finish
Cancel

URL Access Path

URL URL components

* Protocol: HTTPS

* Host:

Port: 443

* Path:

Logon Language: Language of User Context

Proxy

Name of Proxy Host:

Port Number of Proxy Host:

User Name for Proxy Access:

Password of Proxy User:

Transport Binding

Make Local Call: No Call in Local System

* Transport Binding Type: SOAP 1.1

Maximum Wait for WS Consumer:

Optimized XML Transfer: None

Compress HTTP Message: Inactive

Compress Response: True

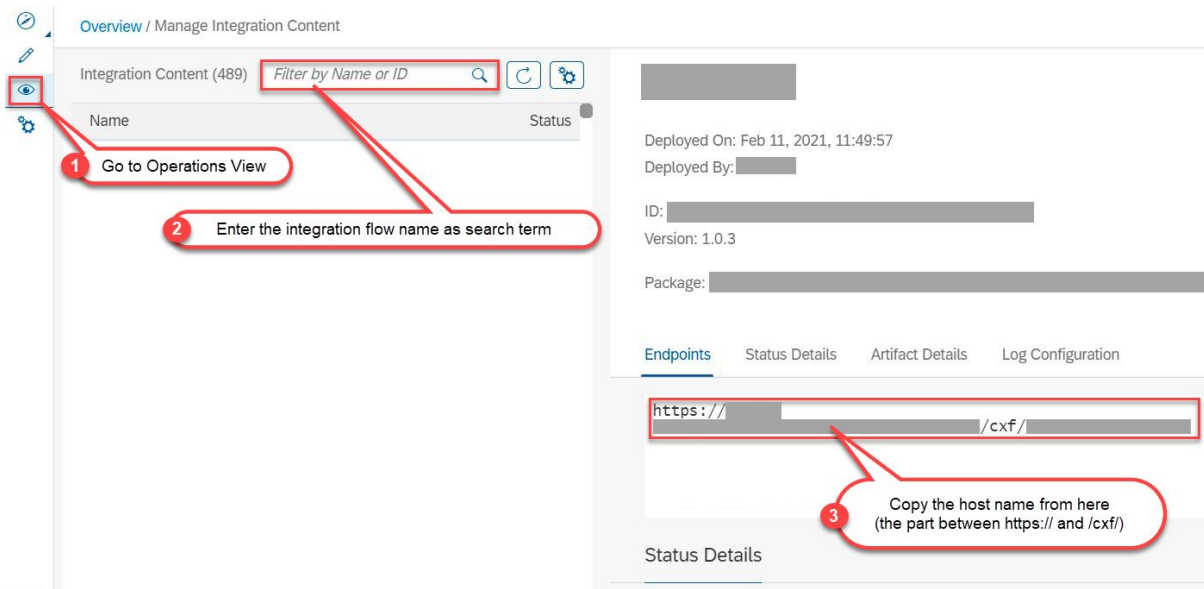
Look Up the SAP Cloud Integration

For each logical port, enter the path from the table above

Enter the proxy settings of your company's network

Port 443 is the standard port for the HTTPS protocol.

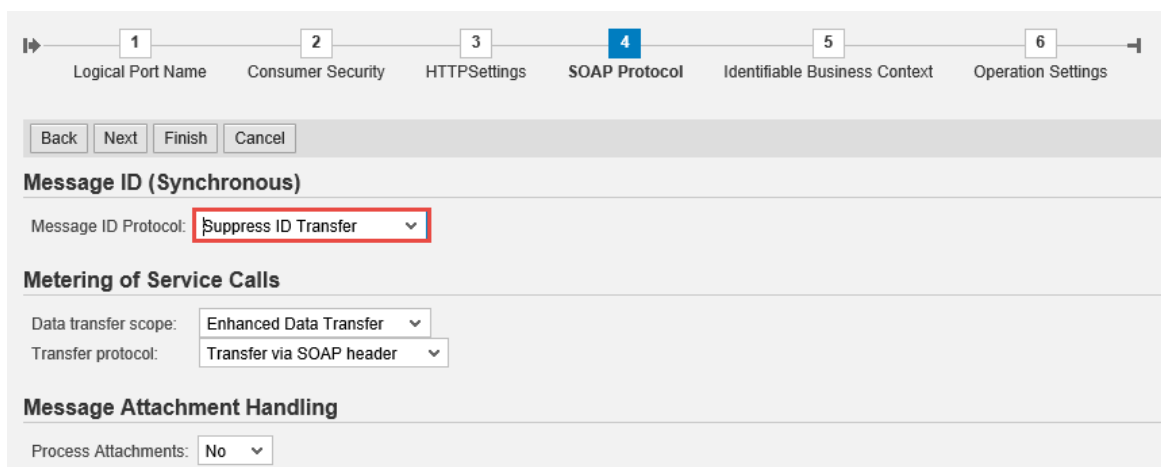
To find the Host, go to SAP Cloud Integration Web UI and under Managed Integration Content, go to [Monitor](#) [All](#). Use the search to find your integration flow as in the screenshot below:



Note

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

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



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

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

- Remember to create logical 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.

New Communication System

*System ID:

*System Name:

Create Cancel

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>**.

Endpoints
Status Details
Artifact Details
Log Configuration

https://v1234- v1234-tmn.avt.eu1.hana.ondemand.com/soap/...	
WSDL	
WSDL without policies	

See the following example:

EDOC_V1234

Changed By: administrator John Editing Status: Draft
Changed On: 08.10.2018, 12:13

General Data

*System ID: <input style="width: 150px;" type="text" value="EDOC_V1234"/>	Notes: <input style="width: 150px;" type="text"/>
*System Name: <input style="width: 150px;" type="text" value="EDOC_V1234"/>	

Technical Data

General

*Host Name: <input style="width: 200px; border: 1px solid red;" type="text" value="v1234-tmn.avt.eu1.hana.ondemand.com"/>	UI Host Name: <input style="width: 150px;" type="text"/>
Logical System: <input style="width: 150px;" type="text"/>	Business System: <input style="width: 150px;" type="text"/>
HTTPS Port: <input style="width: 100px;" type="text"/>	Use Cloud Connector: <input type="checkbox"/>

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

The screenshot shows a configuration interface with the following sections:

- Contact Information:** Includes input fields for 'Contact Person Name', 'E-Mail', and 'Phone Number'.
- OAuth 2.0 Identity Provider:** Includes an 'Enabled' checkbox.
- User for Inbound Communication:** A table with columns 'Authentication Method' and 'User Name'. The current entry shows 'No data' for both.
- User for Outbound Communication:** A table with columns 'Authentication Method' and 'User Name/Certificate/Client ID'. The current entry shows 'No data' for both. A red box highlights a '+' icon to the right of this section header.

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

The 'New Outbound User' dialog box is shown with the following fields and options:

- *Authentication Method:** A dropdown menu is open, displaying the following options: 'User Name and Password', 'SSL Client Certificate', 'OAuth 1.0', 'OAuth 2.0', and 'None'. 'User Name and Password' is currently selected.
- *User Name:** A text input field.
- *Password:** A text input field.

Buttons for 'Cancel' and 'Create' are visible at the bottom right of the dialog.

- 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](#).

The 'New Outbound User' dialog box is shown with the following fields and options:

- *Authentication Method:** A dropdown menu is closed, displaying 'User Name and Password'.
- *User Name:** A text input field.
- *Password:** A text input field.

Buttons for 'Create' and 'Cancel' are visible at the bottom right of the dialog.

- 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](#).

New Outbound User

*Authentication Method: SSL Client Certificate ▼

Certificate Type: Default Client Certificate ▼

Create Cancel

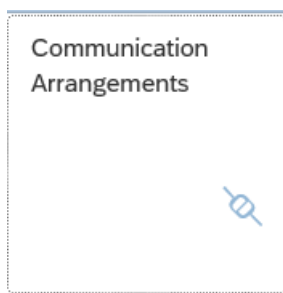
8. Choose *Save*.

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 Path: /cxf/SI_WrapperBoletaOperation
Application Protocol: SOAP Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Port: 443 Use WSRM:

▼ **eDocument Chile Sign Incoming DTE documents** [Download WSDL/Service Metadata](#)

Service Status: Active Path: /cxf/ChileIncomingEnvioDTE
Application Protocol: SOAP Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Port: 443 Use WSRM:

▼ **eDocument Chile Send DTE to SII** [Download WSDL/Service Metadata](#)

Service Status: Active Path: /cxf/ChileSendMultipleDTE
Application Protocol: SOAP Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Port: 443 Use WSRM:

▼ **eDocument Chile Sign DTE Documents** [Download WSDL/Service Metadata](#)

Service Status: Active Path: /cxf/ChileSignEnvioDTE
Application Protocol: SOAP Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Use WSRM:

▼ **eDocument Chile Acknowledge Incoming DTE to SII** [Download WSDL/Service Metadata](#)

Service Status: Active Path: /cxf/ChileIncomingSIIACK
Application Protocol: SOAP Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Port: 443 Use WSRM:

▼ **eDocument Chile Sign Receipt** [Download WSDL/Service Metadata](#)

Service Status: Active Path: /cxf/ChileSignEnvioRecibo
Application Protocol: SOAP Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Port: 443 Use WSRM:

▼ **eDocument Chile Get DTE Status from SII** [Download WSDL/Service Metadata](#)

Service Status: Active Path: /cxf/ChileEnvioDTEGetStatus
Application Protocol: SOAP Service URL: https://v0347-iflmap.avtsbhf.eu1.hana.onde...
Port: 443 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.

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

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