eDocument Chile – Electronic Invoicing

SAP Cloud Platform Integration Setup Guide

TABLE OF CONTENTS

1 INTRODUCTION

The communication part of the eDocument Full Solution for processing electronic documents in Chile is taken care by SAP Cloud Platform Integration. To get SAP Cloud Platform Integration working, there are some required steps on both the SAP ERP system or SAP S/4HANA system* and the SAP Cloud Platform Integration tenant.
These steps are typically done by an SAP Cloud Platform Integration consulting team, which is responsible for configuring the SAP backend systems and the connection with SAP Cloud Platform Integration, as well as maintaining the integration content and certificates/credentials on the SAP Cloud Platform Integration tenant.

* For the sake of simplicity in this guide, we mention **SAP backend systems** when something refers to both SAP ERP and SAP S/4HANA.

2 PREREQUISITES

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

2.1 Installation of eDocument Full Solution

You have installed the eDocument Full Solution your test and/or productive systems. See SAP Note 2030855 for an overview of which SAP Notes are required for the Full Solution.

2.2 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:

1) You have a certificate used for digital signature (private key + password).
2) 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.
3) Create a certificate using the private key and public key information available in the AUTHORIZATION xml from the previous step. Refer to Section 5.2 on how to create certificate using private and public key information available with the CAF xml.

2.3 Setting Up SAP Cloud Platform Integration Tenants

SAP Cloud Platform Integration test and productive tenants are live and users in the tenants have sufficient rights to copy the integration package and to configure and deploy the integration flow.

2.4 Setting Up Secure Connection

To set up a connection between the SAP backend systems and the SAP Cloud Platform Integration, you must establish a trustworthy SSL connection. More reference information can be found in Application Help for SAP Cloud Platform Integration.

Note: The above listed link is maintained by the SAP Cloud Platform Integration team. If you encounter any issue in the linked documentation, please open a support ticket against the component **LOD-HCI-PI-OPS.**

3 CONFIGURATION STEPS

3.1 Deploy Customer Certificate and Credentials 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 iFlows to be updated with minimal adaptation effort, the alias used for the private key and for the credential should be as follows:

Private key alias: chilesignaturekey

You must create and deploy the private key (as mentioned in Section 2.2) 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 shown in the figure below, the alias name of the certificate must be:

'77777777-7339964029965012003-08-29'.

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

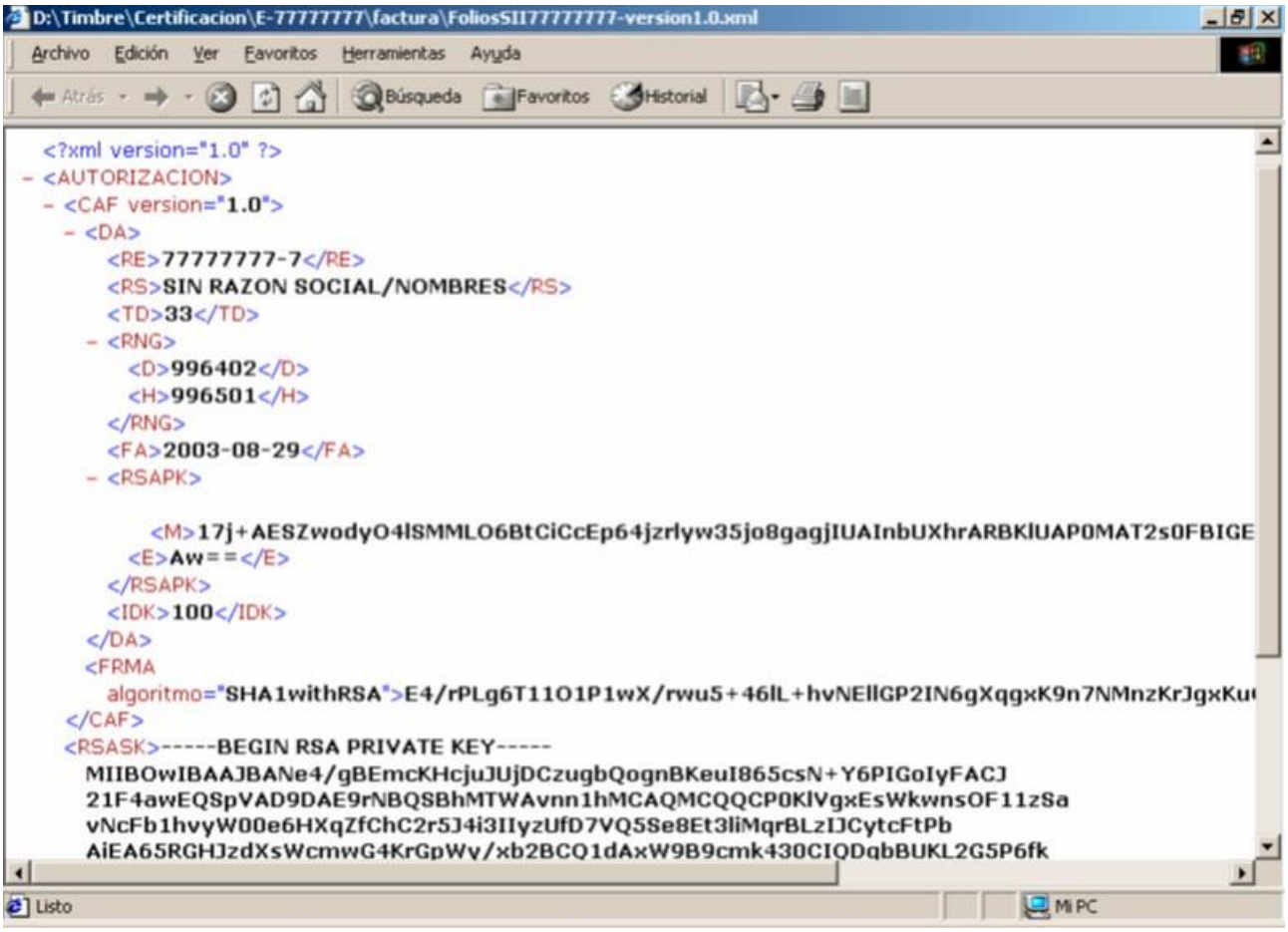


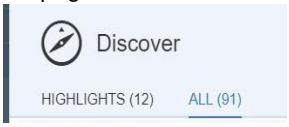
Figure 2.1.1 – CAF XML Sample

3.2 Copy Published Package

For Chile, the package *eDocument: Electronic Invoicing for Chile* is available, which contains the following iFlows:

iFlow Name in WebUI	Project Names/Artifacts Name
EnvioDTE Transmission	com.sap.GS.Chile.SendMultipleDTE
EnvioDTE Get Status	com.sap.GS.Chile.GetStatus
Sign Sales & Purchase Ledger	com.sap.GS.Chile.SPLedger
Sign Delivery Note Ledger	com.sap.GS.Chile.DeliveryNoteLedger
Sign Envio Boleta	com.sap.GS.Chile.EnvioBoleta
Daily Boleta Summary	com.sap.GS.Chile.DailyBoletaSummary
Monthly Boleta Summary	com.sap.GS.Chile.MonthlyBoletaSummary
Acknowledge Incoming EnvioDTE	com.sap.GS.Chile.IncomingEnvioDTE
Acknowledge Incoming Goods Receipt	com.sap.GS.Chile.EnvioRecibo
Value Mappings	com.sap.GS.Chile.ValueMappings
Send Mail	com.sap.GS.Chile.SendMail
Acknowledge IDTE status to SII	com.sap.GS.chile.IncomingACKSII

1. In your browser, go to the WebUI of the tenant (URL: /itspaces/#shell/catalog)
2. From the menu in the upper left corner, choose  *Discover.*
3. Go to tab page *ALL*.



4. In the *Search* field, enter *eDocument: Electronic Invoicing for Chile* package and press *ENTER.*

5. Select the package and in the upper right corner, choose *Copy*.

3.3 Deploy Integration Flows

Deploy iFlows on the SAP Cloud Platform Integration tenants. To deploy an iFlow in the WebUI, select it and choose *Deploy*. After all the iFlows 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 iFlows for the test and production tenants.

For more information about how to change the endpoint URLs as per test and production environment, see the Appendix of this document.

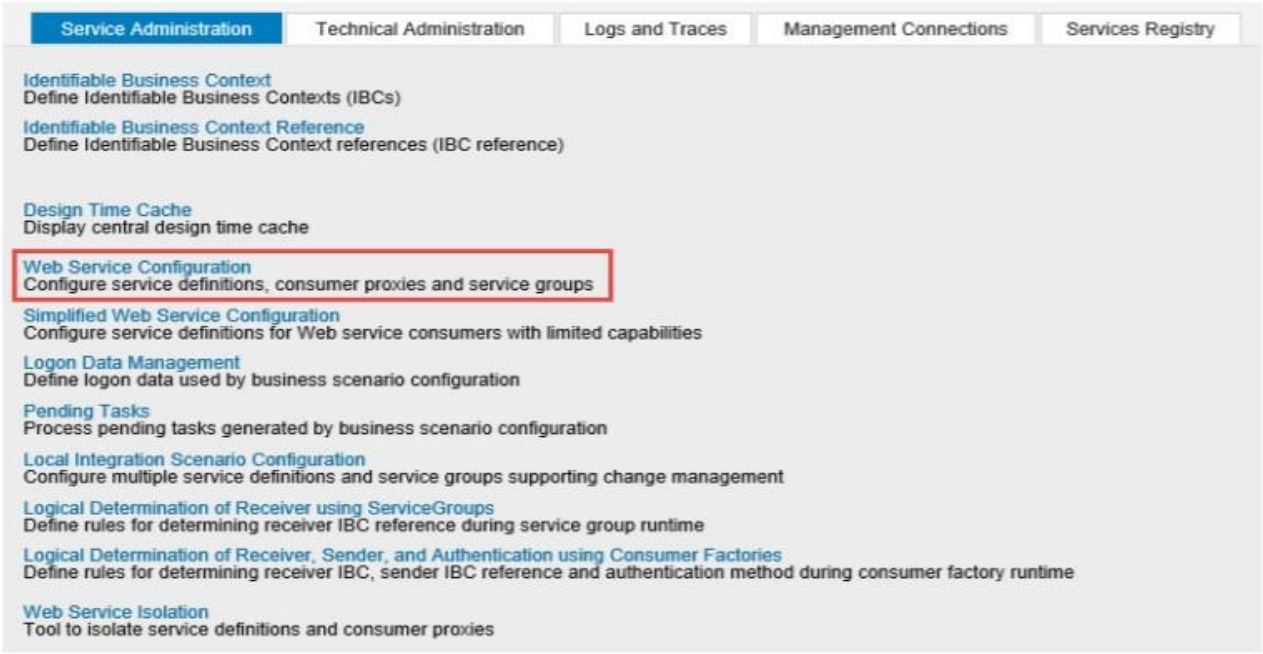
3.4 Set Up Connection with Backend System

If you are using basic authentication, the 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 tenant Keystore and on the iFlows.

3.5 Create Logical Ports in SOAMANAGER

There are three different proxies that need to be connected to the SAP Cloud Platform Integration tenant through logical port. In the test system, the logical ports will be configured to connect to the test tenant. In the productive system, the logical ports will be configured to connect to the productive tenant.

1. In your SAP backend system, go to transaction *SOAMANAGER* and select *Web Service Configuration.*



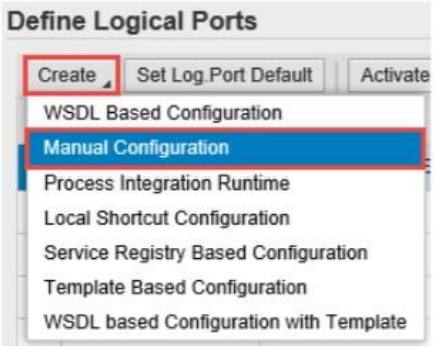
2. Find the proxies for Chile with search term **CO_EDO_CL*.**
The following table lists the proxies, the logical port names, and the relevant endpoints:

Proxy Name	Port Name	Endpoint URL
CO_EDO_CL_DTE_TRANSMIS_SERV	EDO_CL_DTE_TRANSMIS_SERV_PORT	/cxf/ChileSendMultipleDTE
CO_EDO_CL_DTE_GETSTATUS_SERV	EDO_CL_DTE_GETSTATUS_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_BOLETA_SERV	EDO_CL_BOLETA_SERV_PORT	/cxf/ChileSignBoleta
CO_EDO_CL_CHILE_DAILY_BOLETA_S	EDO_CL_DLY_SUMM_TRANSM_SERV_PORT	/cxf/ChileSIgnDailyBoletaSummary
CO_EDO_CL_MONTHLY_BOLETA_SERV	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

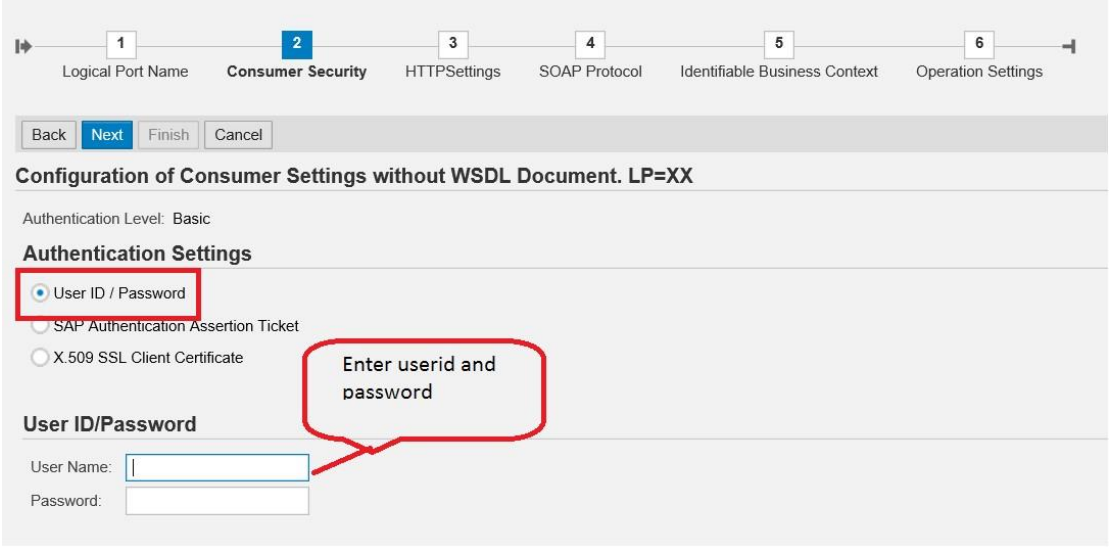
Also add the following descriptions to the ports:
EDO_CL_DTE_TRANSMIS_SERV_PORT: Chile eDocument - DTE Transmission Service
EDO_CL_DTE_GETSTATUS_SERV_PORT: Chile eDocument – DTE Get Status Service
EDO_CL_LEDGER_SERV_PORT: Chile eDocument – Sign Ledger Service

3. In the result list, select a proxy and create logical port(s) for each proxy. Choose *Create* > *Manual Configuration*.



4. Enter the *Logical Port Name* and a *Description*.

5. The *Consumer Security* tab page configuration depends on the security being used for the SAP backend system - SAP CLOUD PLATFORM INTEGRATION communication.
    a. If you use basic authentication, select the *User ID / Password* radio button and enter the *User Name* and *Password*.
    b. If you use certificate-based authentication, select the *X.509 SSL client certificate* radio button and ensure that the required certificates are available in transaction *STRUST*.



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

Note: The screenshots may look slightly different in your system depending on the release, but all the required fields should be available.

The port should be configured as shown in the example below, replacing the access URL with the tenant URL provisioned to you and the proxy settings with the ones from your SAP backend systems:

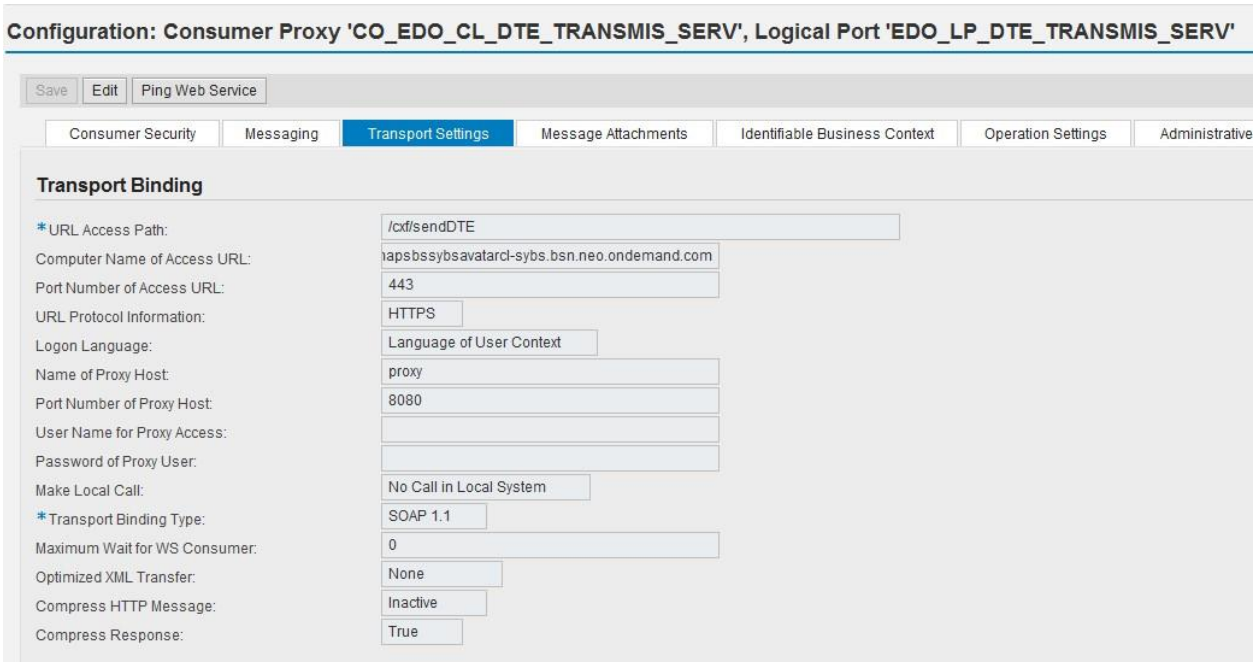
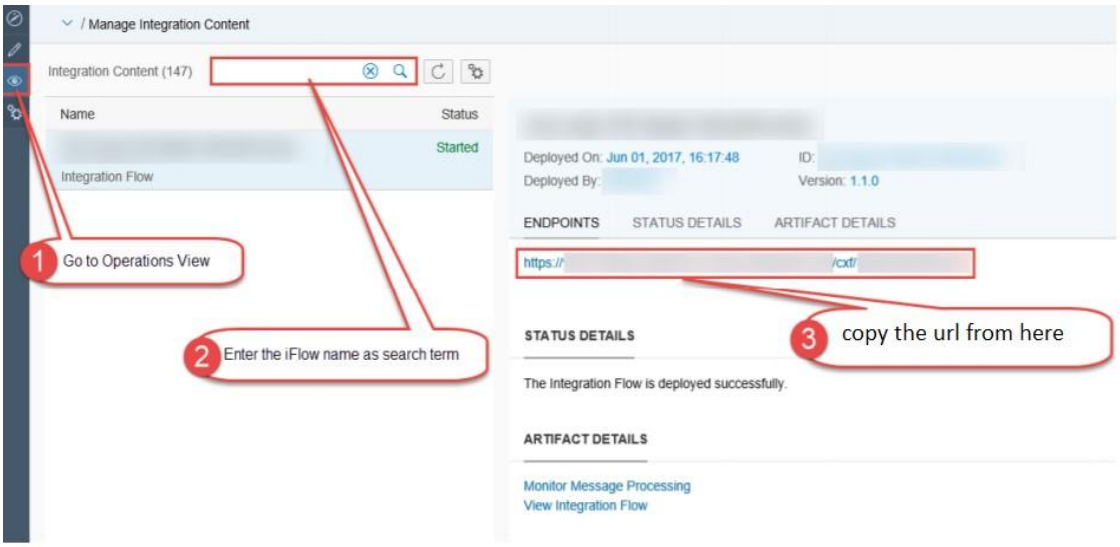


Figure 2.5.1 – SOA Manager Transport Settings

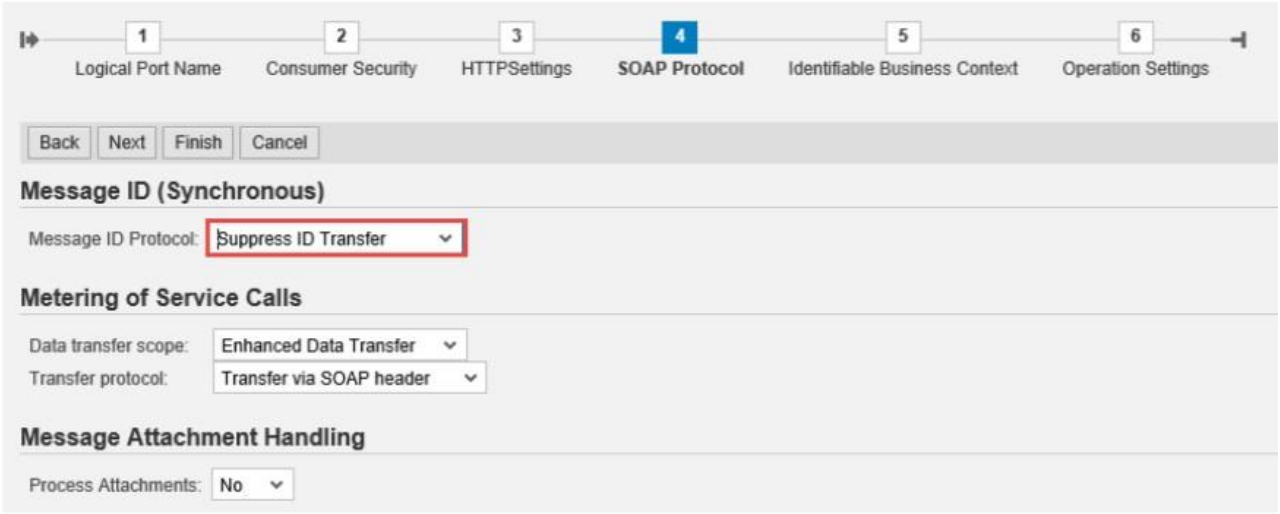
Enter the appropriate values in the fields above according to the information below:

- To find the URL, go to Cloud Platform Integration Web UI, choose *Operations View*  and under *Managed Integration Content* go to *All*. Use the search to find your iFlow as shown in the screenshot below:



- 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 *Messaging* tab page, set the value of the *Message ID Protocol* field to *Suppress ID Transfer*.



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

In the test tenant, you must use the URL access of the SAP Cloud Platform Integration test tenant. In the productive tenant, you must use the URL access of the SAP Cloud Platform Integration productive tenant.

The *Consumer Security* tab configuration depends on the security being used for the SAP backend system - SAP Cloud Platform Integration communication (basic authentication or certificate-based).

Important Note: It is important that you maintain the URLs correctly in the test and productive systems' SOAMANAGER, as they will be pointing to iFlows that behave differently and contact different endpoints in the authority system (SII).

4 TESTING

To test the communication the best way is to create and send an eDocument from SAP backend systems. How you can achieve this depends on how the system is configured to generate and send eDocuments. You must follow these steps:

1) Ensure that you have installed all the SAP Notes relevant to the Full Solution for Chile you have followed all the manual configuration steps.
2) Create a relevant document for eDocument for Chile (for example, an invoice).

   Note: If the system is configured to generate an eDocument for the selected document type, the system creates an instance of the eDocument as soon as you post the document (for example, when you choose the "post goods issue" function).

   You can configure the eDocument to be sent automatically on posting or you must trigger it from the eDocument Cockpit.
3) Go to the eDocument Cockpit by running the **EDOC_COCKPIT** transaction.
4) Select the relevant process in the Cockpit and find the document that you just created.
5) Check the status of the eDocument and act accordingly: ○ If the status of the eDocument is *Created*, the eDocument was created but not submitted yet. In this case, choose the *Submit* pushbutton to trigger the communication with SAP Cloud Platform Integration. ○ If the status is green or yellow, but not *Created,* the communication with SAP Cloud Platform Integration was triggered and was probably successful. You can double-check if the message went through on the

   SAP Cloud Platform tenant; or you can use a trace from transaction "SRT_UTIL" to look at the XMLs transmitted via web services from the SAP backend systems. ○ If the status is red, an error happened during submission. Click on the *Interface* field to jump to AIF and look at the log. Communication errors will be displayed there.

5 APPENDIX

5.1 iFlow Receiver URLs

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

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	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
SII_STAT_UP	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, please make sure that credentials are deployed in your tenant with the same name)

Receiver1 (IDTE Ack to SII – receiver)	Test	https://ws2.sii.cl/WSREGISTRORECLAMODTECERT/registroreclamodteservice
	Production	https://ws1.sii.cl/WSREGISTRORECLAMODTE/registroreclamodteservice

To change the parameters in the WebUI, do the following:

1. From the menu in the upper left corner, choose *Design.*
2. Click on the *eDocument: Electronic Invoicing for Chile* package and then on *Package Content*.
3. For the iFlow that you want to change, choose *Actions* > *Configure*.
4. After changing the parameters, choose *Save*.

For example:

5.2 Generating and Importing Certificates – CAF Certificate Handling

Prerequisites

- Install OPENSSL in your system.
- Download CMDER from the relevant URL. This is the utility used for generating the .crt file from the .key file. You can download the full version.
- You can also download Keystore Explorer for creating the keystore.

Generating Private Key from CAF Authorization XML

1. Run the report EDOC_CL_NR_XML_UPLOAD to upload the number range in the system. The report also downloads the .key file for the xml which has the private key from CAF file.

   Alternatively, create the .key file. The .key file should contain the private key contained in the CAF xml. Name the file as mentioned in the CAF naming in section 2.1.

```
1  -----BEGIN RSA PRIVATE KEY-----CRLF
2  MIIBOQIBAAJBALZDsv6KR2PnsmQfOWWBekMC0qE2y0vUMKOD1jc7vpyd52ZFZkLhCRLF
3  ...CRLF
4  KepEp6IhgSpiUd08+N3iRSpZiW5PAiEAm2MDXVCWIFGOu6k921xU9Y6ScLQTBoHqCRLF
5  i65YJvgHsTT8mfqmkqYClPp2wVdw3KA/zzistis=CRLF
6  -----END RSA PRIVATE KEY-----CRLF
7
```

2. Open the Command prompt and go to the path where OpenSSL is installed (inside Bin). Use the following OPENSSL command to convert the .key file to a .csr file:
   openssl req -new -key <filename>.key -out <filename>.csr

It will ask for the details below. You will find these details in your certificate received from SII.

- Country Name(2 letter code) : ○ State of Province Name (full name): ○ Locality Name (eg. City) ○ Organization Name (eg. Company) ○ Organization Unit Name (eg. Section): ○ Common Name (e.g. server FQDN or Your Name): ○ Email Address:
- Challenge Password(Optional):

Note: Here <filename> is the name with which 'EDOC_CL_NR_XML_UPLOAD' report created file.

3. Use the following OPENSSL command to create a .crt file from the .key and .csr file:
   openssl x509 -req -days 365 -in <filename>.csr -signkey <filename>.key -out <filename>.crt

   Note: Here <filename> is the name with which 'EDOC_CL_NR_XML_UPLOAD' report created file.

After successful creation of key value pair certificates (<filename>.key and <filename>.crt), you need to raise incident under 'LOD-HCI-PI-OPS' for asking to upload the key value pair in your tenant keystore.

Please mention that the alias name should be the same as .key & .crt files (<filename>). If it is changed, you will get a dump in the iFlow.

www.sap.com