Mexico Electronic Documents: Setting Up SAP Cloud Platform Integration (SAP S/4HANA, SAP ERP) - Cloud Foundry environment

TABLE OF CONTENTS

1 Disclaimer

This documentation refers to links to websites 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

The communication part of processing electronic documents in Mexico is taken care of by SAP Cloud Platform Integration. In order to get SAP Cloud Platform Integration working, there are some required steps on both your SAP S/4HANA or SAP ERP system and SAP Cloud Platform Integration tenant.

These steps are typically taken care of by an SAP Cloud Platform Integration consulting team, who is responsible for configuring the SAP S/4HANA or SAP ERP - SAP Cloud Platform Integration connection and maintaining the integration content and certificates/credentials on the SAP Cloud Platform Integration tenant.

Note: This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Cloud Platform Integration tenant. It may happen, however, that in the SAP S/4HANA or SAP ERP system 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 or SAP ERP documentation and to the relevant tax authority information, respectively.

3 Prerequisites

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

3.1 Registration at SAT

Registration at SAT is completed. And the following data is available:

- Certificate used for digital signatures (private key + password).
- Public certificate to verify the SOAP response deployed in the keystore of your SAP Cloud Platform Integration tenant. Obtain the certificate from SAT.

  For more information, see http://www.sat.gob.mx/informacion_fiscal/factura_electronica/Paginas/certificado_sello_digital.aspx.

Create a keystore using the private key and public key information available. Refer to chapter 7 on how to create a certificate using private and public key information available.

3.2 eDocument Full Solution

The eDocument Full solution is installed in your test and production systems.

For the generic part, refer to the Installation Guide for eDocument attached to SAP Note 2134248.

For the Mexico-specific part, refer to SAP Note 2526771 for SAP ERP systems, and SAP Note 2565791 for SAPS/4HANA systems.

4 Secure Connection

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 Platform Integration.

Inbound HTTP connections are not required for Mexico. 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 iFlow 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 Operations guide for SAP Cloud Platform Integration.

Note: If you encounter any issues in the information provided in the SAP Cloud Platform 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.

4.1.1 Setup of SAP Cloud Platform Integration

You have performed all initial setup steps described in Initial Setup of SAP Cloud Platform Integration in Cloud Foundry Environment. After completing the tenant provisioning step, you get your own tenant URL.

4.1.2 Retrieve and Save Public Certificates

Context

Find and save the public certificates from your SAP Cloud Platform Integration worker node.

Procedure

1. Access the SAP Cloud Platform 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 XXXXXXX corresponds to the dynamic part and is unique for each subaccount.

4. Choose *Manage Integration Content* and select All to display the integration flows (iFlows) available.
5. Select an iFlow 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 Platform 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 iFlow

Create an own certificate and get it signed by a trusted certificate auhority (CA) to support iFlow authentication.

Context

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

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

Procedure

1. Access transaction STRUST.
2. Create your own PSE (for example, Client SSL Standard) and then generate a certificate sign request.
3. Export the certificate sign request as a *.csr file.
4. Arrange for the certificate to be signed by a trusted certificate authority (CA).
   If you are using a client certificate, this must be signed by one of the root certificates supported by the load balancer. A self-signed certificate is not suitable. For more information see Load Balancer Root Certificates Supported by SAP.
   The CA may have specific requirements and request company-specific data, they may also require time to

analyze your company before issuing a signed certicate. When signed, the CA provides the certificate for import.

5. Navigate to the PSE for SSL Client Standard and open it by double-clicking the PSE.
6. Switch to edit mode.
7. Choose the *Import certificate* button.
8. In the *Import Certificate* dialog box, enter or select the path to the CA-signed certificate and choose *Enter*.
   The certificate is displayed in the *Certificate* area.
9. Choose *Add to Certificate List* to add the signed certificate to the *Certificate List*.
   Ensure that you import the CA root and intermediate certificates to complete the import.
10. Save your entries.
    The certificates can now be used in the SOA Manager (transaction SOAMANAGER).

5 Configuration Steps in SAP Cloud Platform Integration

5.1 Deploy the Customer Certificate and Credentials to SAP Cloud Platform Integration

If your PAC is Edicom, you can use an Edicom-specific iFlow to communicate with Edicom. If your PAC is Pegaso, you can use a Pegaso-specific iFlow to communicate with Pegaso. Before sending an XML file using either of the two iFlows, SAP Cloud Platform Integration signs it using a private/public key pair and client certificate. In these cases where the signing is done by SAP, you need to provide an SSL certificate recognized by the tax authority and a pair of private/public key. This information must be available in the keystore on your SAP Cloud Platform Integration tenant.

This integration package also provides a generic iFlow, which is meant to work with any PAC. If you use this generic iFlow to communicate with your PAC, the PAC does the signing.

Do the following to deploy your credentials and certificate on SAP Cloud Platform Integration:

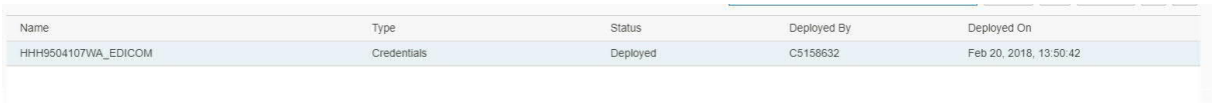
1. Deploy the certificate (as private key with an alias <RfcEmisor>) in the JAVA_KEYSTORE.
   See chapter 7 on how to create a single certificate chain containing both private key and public certificate.

Here's an example:

Alias	Type	Owner	Valid Until	Last Modified At	Actions
hhh9504107wa	Key Pair	Tenant Administrator	May 18, 2021, 09:24:56	Feb 13, 2018, 18:06:50	

For Edicom, credentials for the endpoint must be obtained and stored in the tenant under the name **<RfcEmisor>_EDICOM**. If you have multiple company codes, you do not need to copy the package for every company code. You just need to maintain the credentials for every <RfcEmisor>.

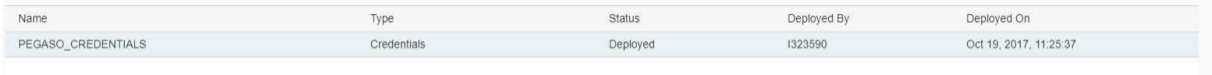
Here's an example:



Name	Type	Status	Deployed By	Deployed On
HHH9504107WA_EDICOM	Credentials	Deployed	C5158632	Feb 20, 2018, 13:50:42

For Pegaso, credentials (username and password) for the endpoint must be obtained and stored in the tenant under the name **PEGASO_CREDENTIALS**. If you have multiple company codes, you must copy the package for every company code.

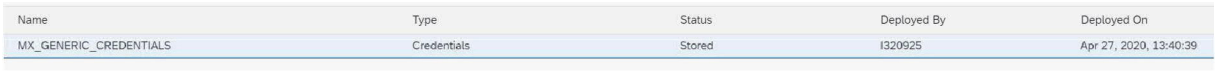
Here's an example:



Name	Type	Status	Deployed By	Deployed On
PEGASO_CREDENTIALS	Credentials	Deployed	I323590	Oct 19, 2017, 11:25:37

For other PACs, credentials (username and password) for the endpoint must be obtained and stored in the tenant under the name **MX_GENERIC_CREDENTIALS**. If you have multiple company codes, you must copy the package for every company code.

Here's an example:



Name	Type	Status	Deployed By	Deployed On
MX_GENERIC_CREDENTIALS	Credentials	Stored	I320925	Apr 27, 2020, 13:40:39

2. Deploy the public certificate for STAGING in the TEST tenant's JAVA_KEYSTORE and the public certificate for PRODUCTION in the PRODUCTION tenant's JAVA_KEYSTORE.

   The details on how to create a jks file are available in chapter 7.

5.2 Copy Integration Package

This package contains the following iFlows:

iFlow Name in WebUI	Project Names/Artifacts Name
Mexico Document Compliance	MexicoeDocument
Mexico Document Compliance Edicom	MexicoeDocument_edicom
Mexico Document Compliance Pegaso	MexicoeDocument_pegaso
Mexico Document Compliance Generic	MexicoeDocument_generic

There are two iFlow deployment options. The option that you should choose depends on your PAC.

Option 1

If your PAC is Edicom or Pegaso, you can use this deployment option. Deploy the following iFlows on your tenant:

iFlow Name in WebUI	Explanation
Mexico Document Compliance	Whether you PAC is Edicom or Pegaso, you must deploy this iFlow.
Mexico Document Compliance Edicom	If your PAC is Edicom, in addition to the iFlow Mexico Document Compliance, deploy this iFlow as well.
Mexico Document Compliance Pegaso	If your PAC is Pegaso, in addition to the iFlow Mexico Document Compliance, deploy this iFlow as well.

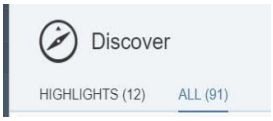
Option 2

If you choose a PAC other than Edicom or Pegaso, use this deployment option. Deploy the following iFlow on your tenant:

iFlow Name in WebUI	Explanation
Mexico Document Compliance Generic	You can find PACs who are SAP partners and can handle requests from this iFlow from SAP App Center. Search with the keyword "SAP Document Compliance".

Do the following to copy the integration package:

1. Log in to your SAP Cloud Platform Integration tenant.
2. From the menu in the upper left corner, choose **Discover**.
3. Go to the tab page **ALL**.



4. In the search field, enter **SAP Document Compliance: Electronic Invoices and Payment Receipt Complements for Mexico** and press ENTER.

5. Select the package **SAP Document Compliance: Electronic Invoices and Payment Receipt Complements for Mexico**. In the upper right corner, choose **Copy**.

5.3 Deploy Integration Flows

Do the following to deploy an iFlow:

Configuring iFlows

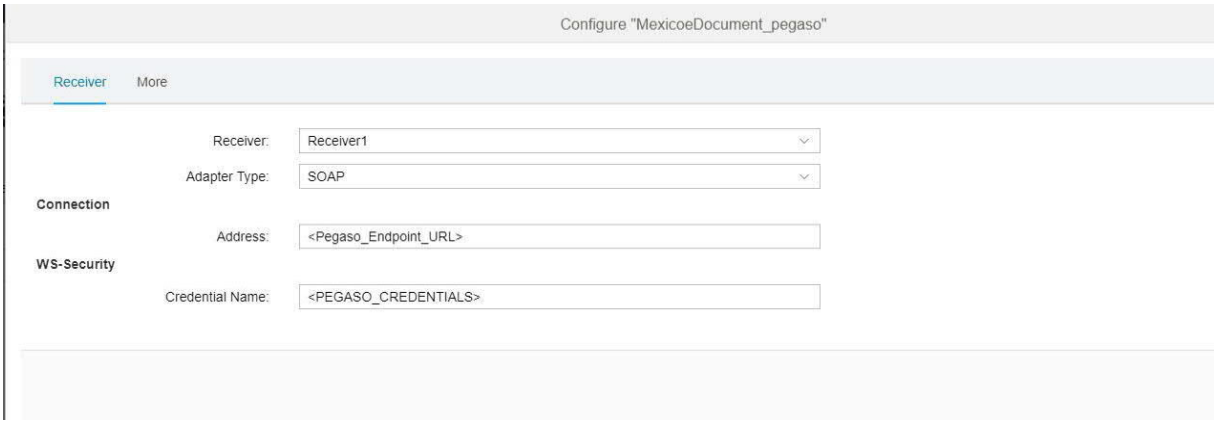
1. Click on the package **SAP Document Compliance: Electronic Invoices and Payment Receipt Complements for Mexico**.
2. Go to the **Artifacts** tab page.
3. For the iFlow that you want to change, choose **Actions** > **Configure**.
4. Choose **Save**.

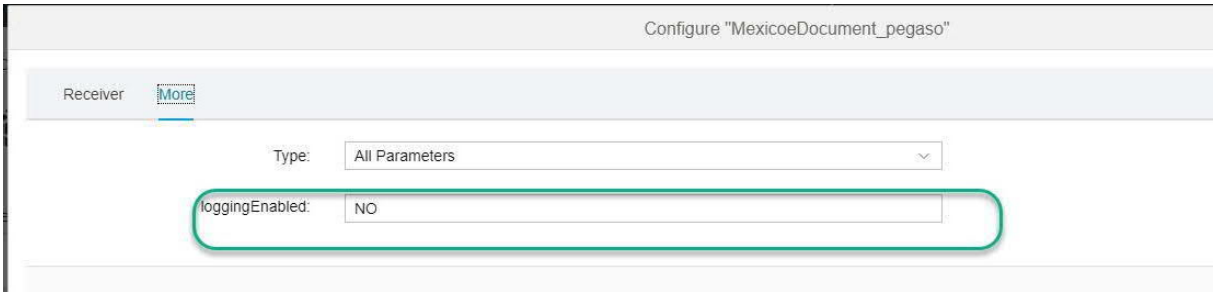
For Pegaso, follow the instructions below:

1. Configure the following externalized parameters of the iFlow **Mexico Document Compliance Pegaso**:
    - URL: endpoint URL of the webservice from Pegaso
    - eInvoice_URL: endpoint URL for getting statuses of eInvoice cancellation requests
    - ePayment_URL: endpoint URL for getting statuses of ePayment cancellation requests

2. Enter the credential name that is maintained in the keystore.
3. Execute checks and deploy the iFlow in the tenant.
4. Before testing, ensure the handshake certificate from Pegaso is downloaded and deployed in the tenant keystore. There is no constraint in the alias here. So, download and store it under any name.

Configurable Parameters:

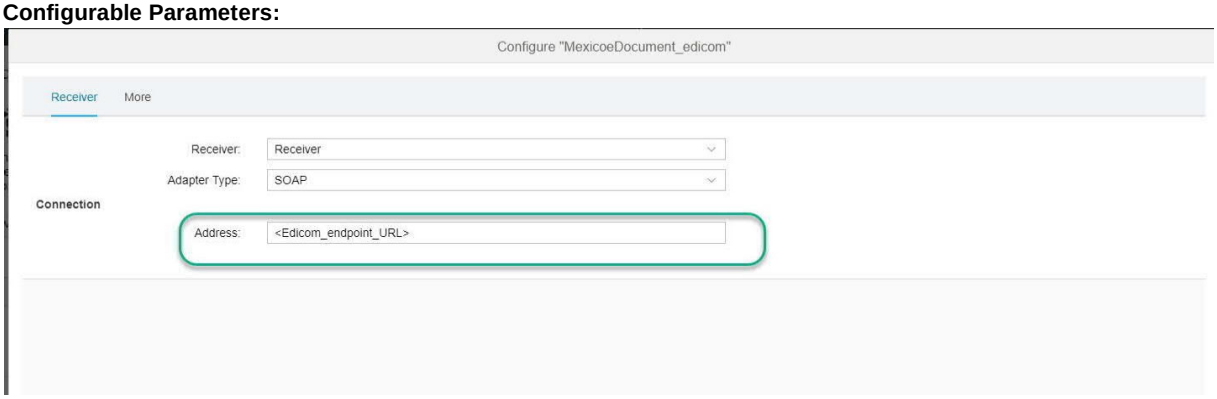


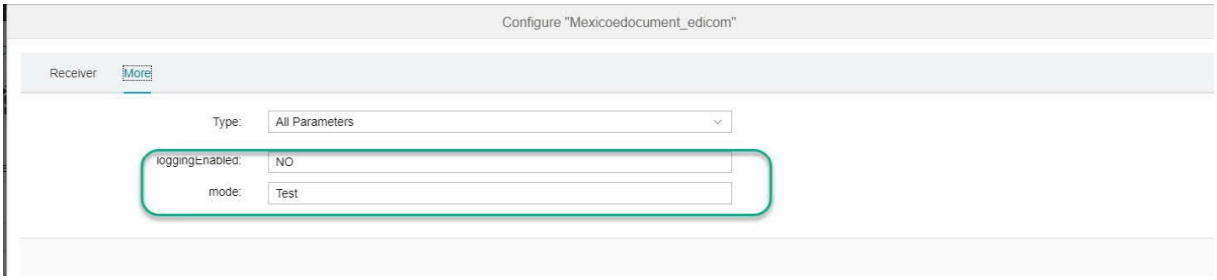


For Edicom, follow the instructions below:

1. Configure the following externalized parameters of the iFlow **Mexico Document Compliance Edicom**:
   - url: endpoint URL from Edicom
   - mode: The default mode is Test. Possible values are Test and Prod. Choose a mode based on the runtime environment. Edicom uses a common url for test and production modes.
2. Execute checks and deploy the iFlow.
3. Before testing, download the handshake certificate from the endpoint which Edicom has provided and store itin the tenant's keystore. There is no dependency on the alias name which you use to store this certificate. You can store it under any name.

Configurable Parameters:

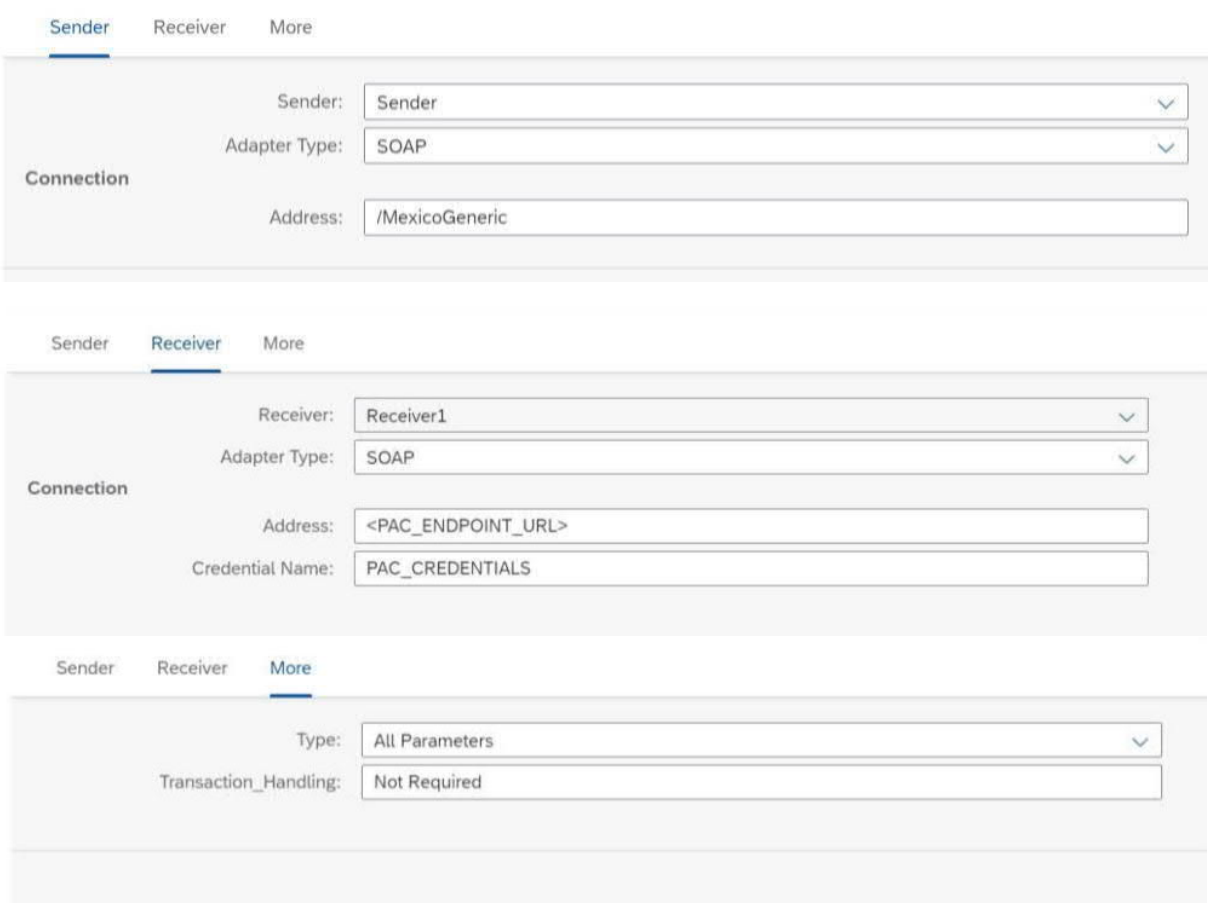




For the generic iFlow **Mexico *Document Compliance Generic***, follow the instructions below:

1. Configure the following externalized parameters:
   - Sender Address: endpoint URL of the iFlow
   - Receiver Address: endpoint URL from PAC

2. Enter the credential name that is maintained in the keystore.
3. Execute checks and deploy the iFlow in the tenant.



After deploying all the required iFlows, note down the URLs of the endpoints for each service. The endpoints are used in the SOAMANAGER configurations.

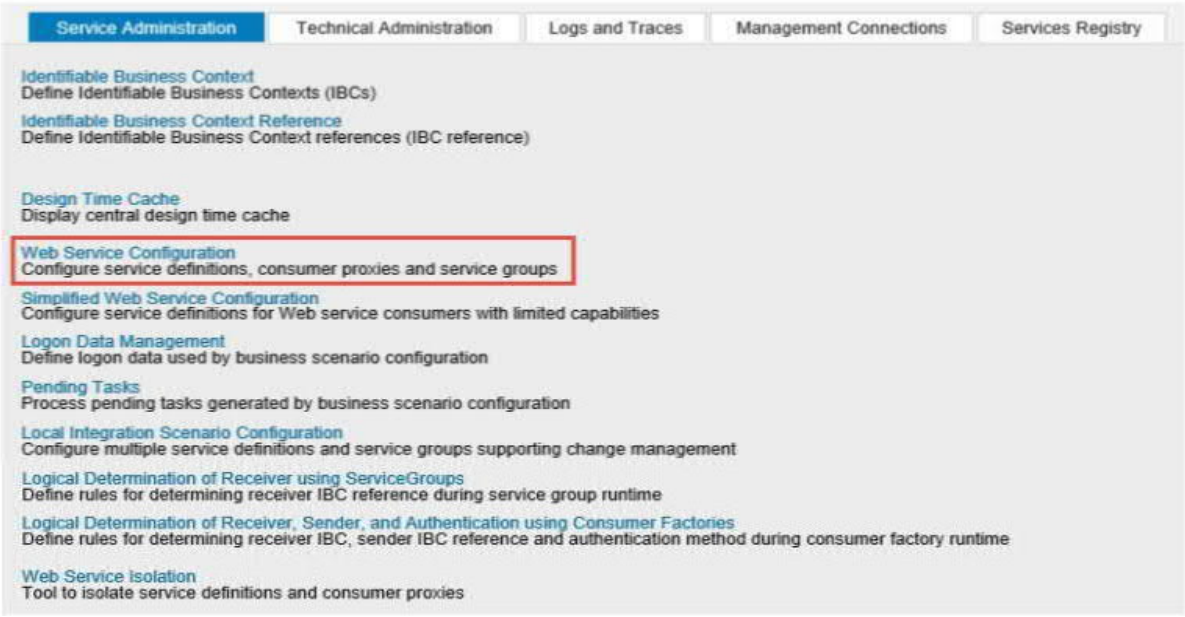
6 Configuration Steps in SAP ERP or SAP S/4HANA

6.1 Create Logical Ports in SAP ERP or SAP S/4HANA

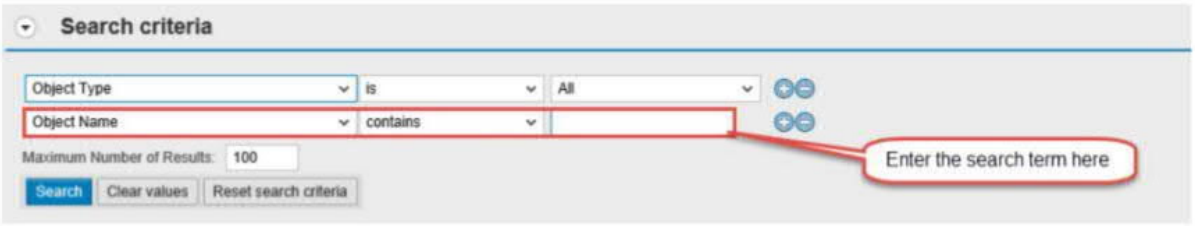
Proxies must be connected to the SAP Cloud Platform Integration tenant via logical ports. In the SAP ERP or SAP S/4HANA test system, the logical ports are configured to connect to the test SAP Cloud Platform Integration tenant. In the productive SAP ERP or SAP S/4HANA system, the logical ports are configured to connect to the productive SAP Cloud Platform Integration tenant.

Proceed as follows:

1. In your SAP ERP or SAP S/4HANA system, go to transaction *SOAMANAGER* and select **Web Service Configuration**.



2. Search for the proxies for Mexico with the search term **CO_EDO_MX_***



If you use the Pegaso-specific or Edicom-specific iFlow, use one of the following proxies:

Proxy Name	Logical Port Name	Description	Path
CO_EDO_MX_CFDI_EDOCUMENTS	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoeDocuments
CO_EDO_MX_CFDIE_EDOCUMENTS * Available since integration package version 1.1.0	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoeDocuments

See SAP Note 2825133 for information about what the proxy **CO_EDO_MX_CFDIE_EDOCUMENTS** does.

If you use the generic iFlow, use the following proxy:

Proxy Name	Logical Port Name	Description	Path
CO_EDO_MX_CFDIE_EDOCUMENTS	MX_EDOCUMENT	Mexico eDocument	/cxf/MexicoGeneric

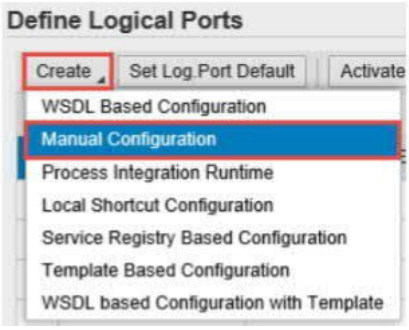
Both the logical port name and path can be customized.

Note: You must maintain the maintenance view EDOSOASERV for each company code in your SAP ERP or SAP S/4HANA system.

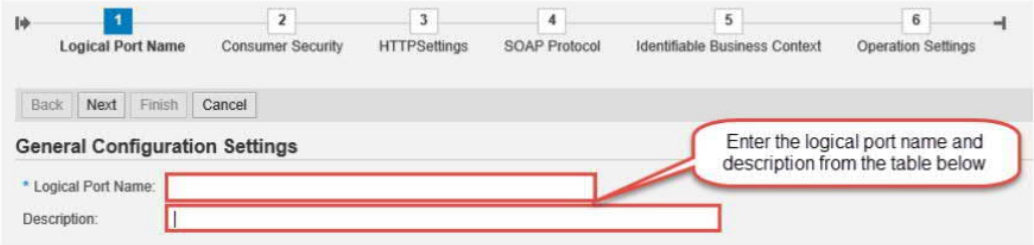
For example:

SOA SERVICE NAME	Company code	Logical Port	SOA Service Description
MX_EDOCUMENT	XXXX	MX_EDOCUMENT	Mexico eDocument SOA service

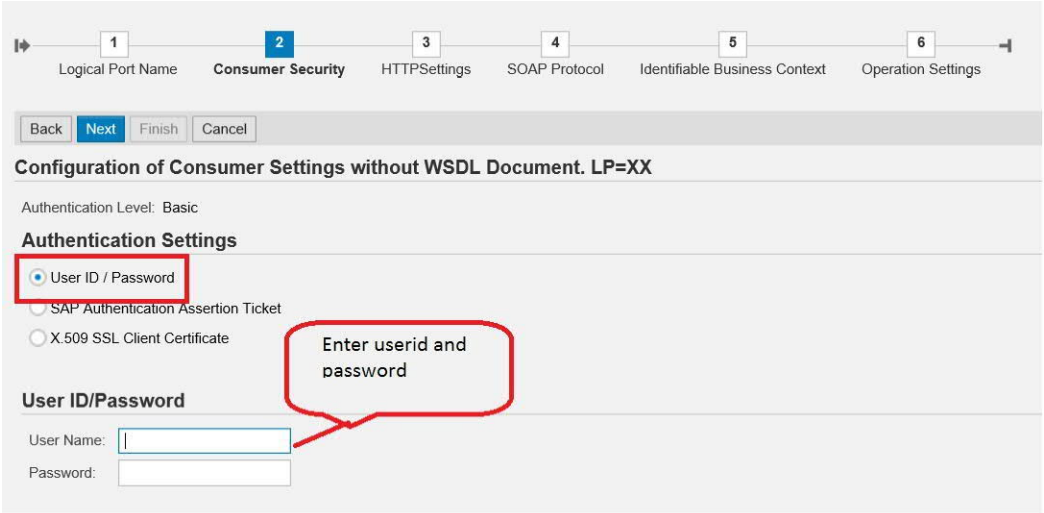
3. In the result list, select a proxy and create a logical port for it. Choose *Create* > *Manual Configuration*.



4. Enter the logical port name and a description.

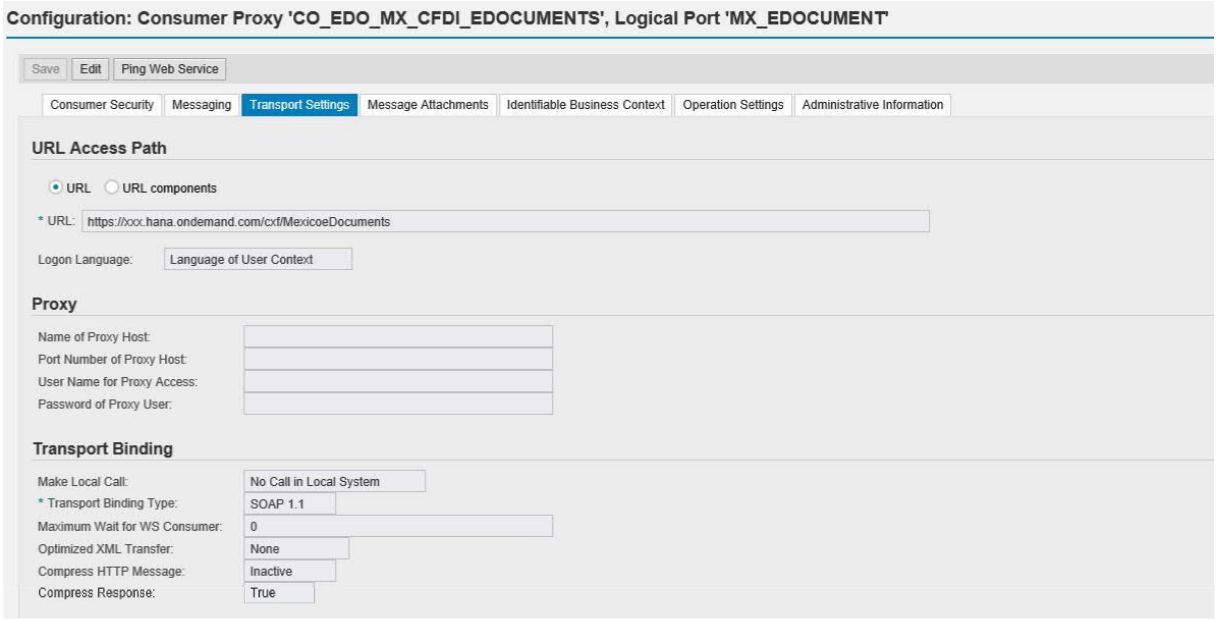


5. The **Consumer Security** configuration depends on the security being used for the SAP ERP or SAP S/4HANA - SAP Cloud Platform Integration communication.
    a. If you use the basic authentication, enter the value of the **clientid** for *User Name*, and the value of **clientsecret** for *Password*. You create these values for your service instance in SAP Cloud Platform Integration. See Creating Service Instances.
    b. If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have uploaded to STRUST. You must configure this certificate in SAP Cloud Platform Integration 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.

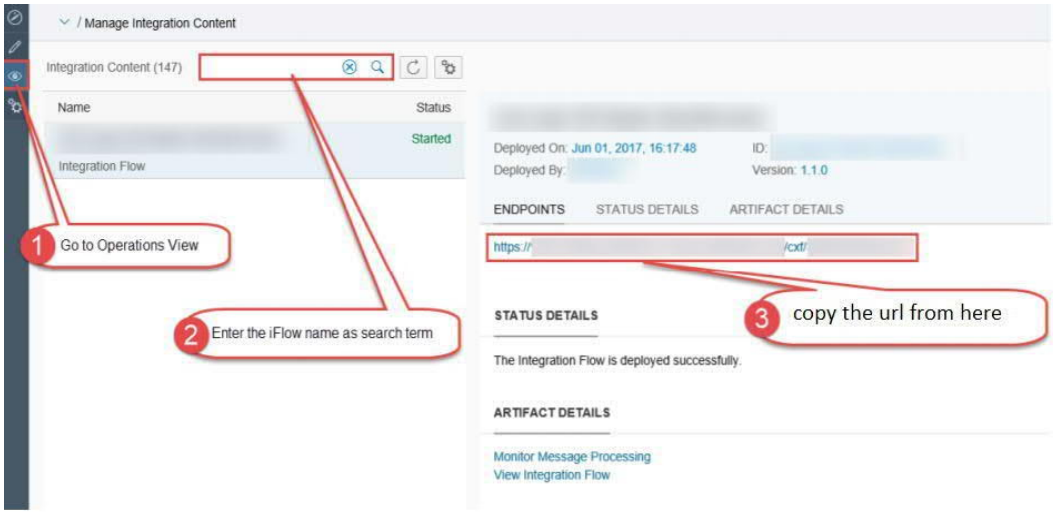


6. On the **HTTP Settings** tab page, make the following settings:

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



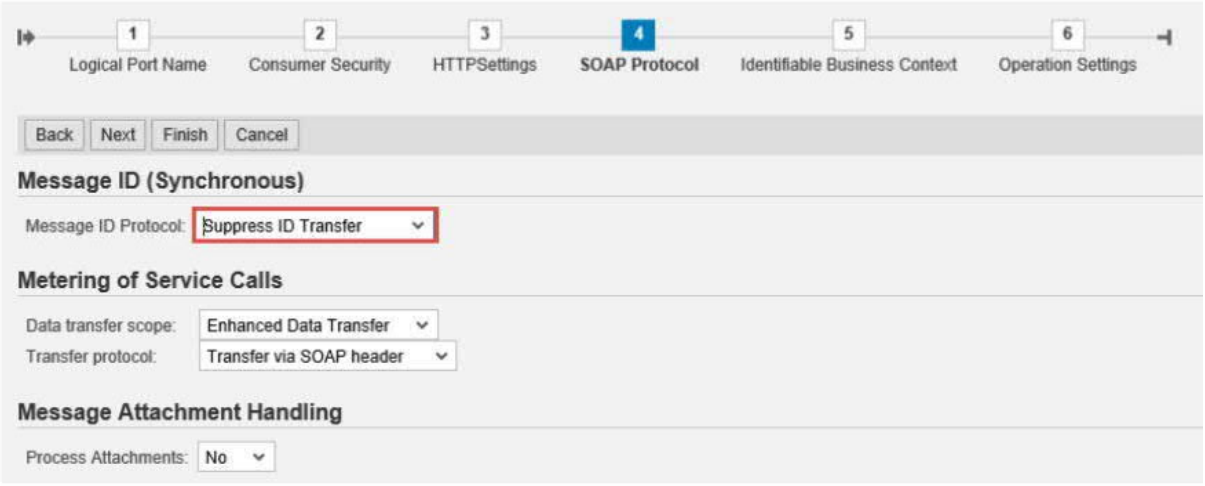
To find the Host, go to SAP Cloud Platform Integration Web UI. Under **Managed Integration Content**, go to **Monitor** -> **All**. Use the search to find your integration flow as shown in the screenshot below:



:

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 in the tabs **Identifiable Business Context** and **Operation Settings**. Just select **Next** and then **Finish**.

7 Appendix

7.1 Generate and Import Certificates

7.1.1 Prerequisites

- Install OPENSSL in your system (http://slproweb.com/products/Win32OpenSSL.html).
- You can also download Keystore Explorer for creating the keystore.
  (http://keystore-explorer.sourceforge.net/downloads.php)

7.1.2 Generate PKCS#12 File from the Certificate and Key File

After the successful installation of openssl for Windows, follow the steps below to generate the keystore file that you can import into SAP Cloud Platform Integration:

1. Open command prompt in the folder where openssl is installed.
2. Convert the key file to pkcs8 format.
   openssl pkcs8 -inform DER -in aaa010101aaa_CSD_01.key -passin pass:a0123456789 -outform PEM -out CSD_01.key.pem -passout pass:a0123456789
3. Convert the certificate to pkcs8 format. openssl x509 -inform DER -in aaa010101aaa_CSD_01.cer -outform PEM -out CSD_01.cer.pem.
4. Append the certificate and key file to one file. copy CSD_01.key.pem+CSD_01.cer.pem CSD_01_chain.pem.
5. Convert pem file to pkcs12.
   openssl pkcs12 -in CSD_01_chain.pem -passin pass:a0123456789 -export -out CSD_01.p12 -name SAT -passout pass:a0123456789

In the Keystore Explorer, make the following settings:

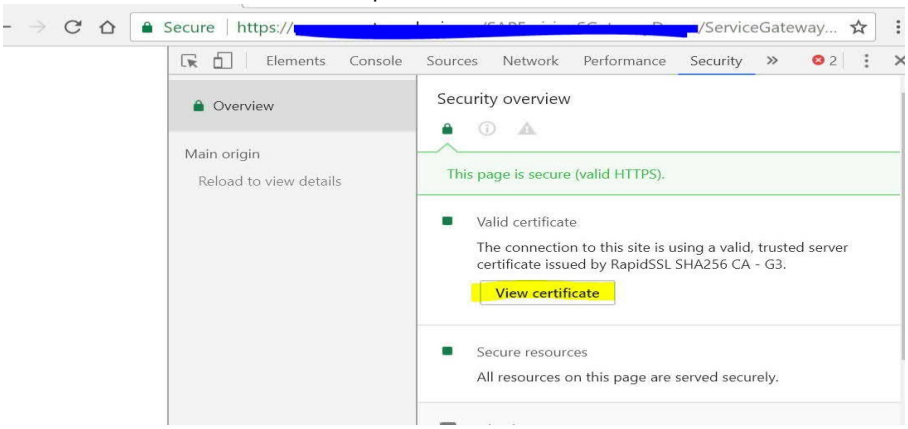
1. Click on *Create a New Keystore*, select the type of new Keystore as JKS.
2. Choose *Tools->Import Key Pair* and select the pkcs12 file created.
3. Enter a password and click on *Save*.
4. The created JKS file can be imported into SAP Cloud Platform Integration Keystore under a specific alias.

The same *alias* should be used as *external parameter* while deploying the iFlow.

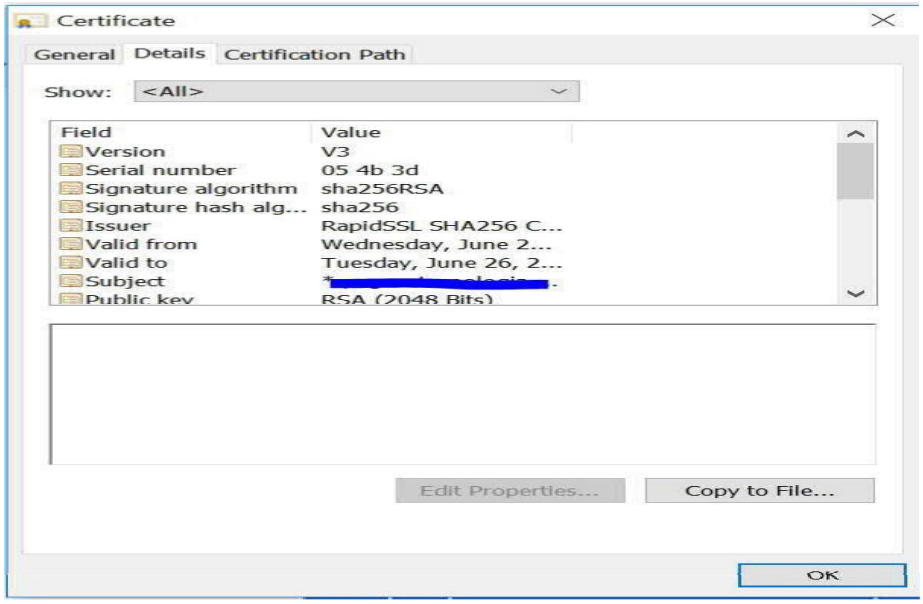
7.1.3 Import the Handshake Certificate

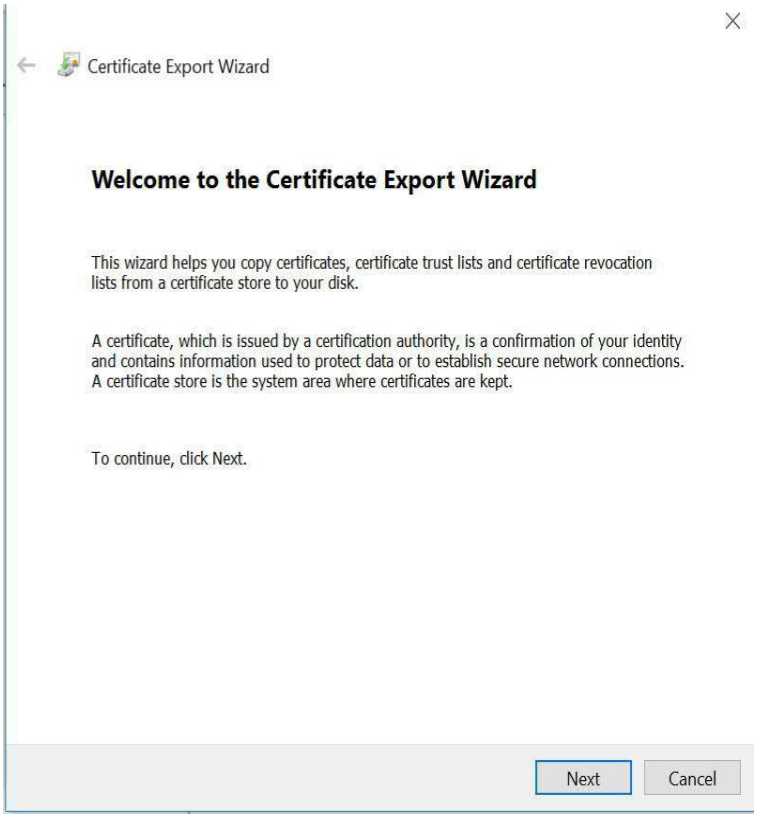
Irrespective of whether the signing happens in SAP Cloud Platform Integration or not, you must download the handshake certificate from the endpoint that is used to connect to the PAC.

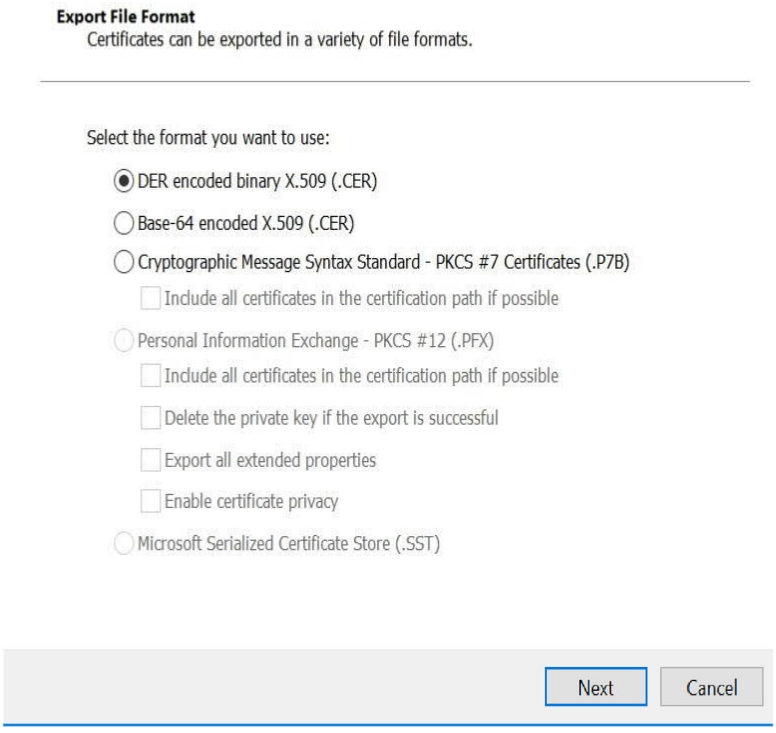
1. Enter the URL into the browser and press F12.

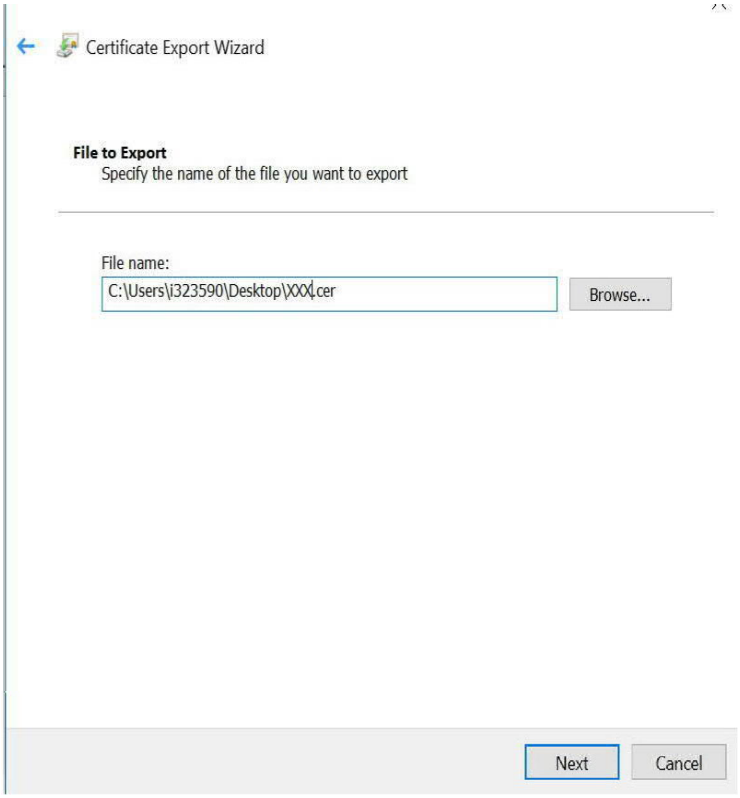


2. Click on *View certificate* -> *Copy to file*, choose *Next* and select options as below until you reach *Finish*. You can import this certificate into a keystore and load it to the SAP Cloud Platform Integration tenant keystore.




Certificate Export Wizard
Welcome to the Certificate Export Wizard
This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.
A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.
To continue, click Next.
Next
Cancel


Export File Format
Certificates can be exported in a variety of file formats.
Select the format you want to use:
DER encoded binary X.509 (.CER)
Base-64 encoded X.509 (.CER)
Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)
Include all certificates in the certification path if possible
Personal Information Exchange - PKCS #12 (.PFX)
Include all certificates in the certification path if possible
Delete the private key if the export is successful
Export all extended properties
Enable certificate privacy
Microsoft Serialized Certificate Store (.SST)
Next
Cancel


Certificate Export Wizard
File to Export
Specify the name of the file you want to export
File name:
C:\Users\i323590\Desktop\XXX.cer
Browse...
Next
Cancel

www.sap.com