Mexico Electronic Documents: Setting Up SAP Cloud Integration (SAP S/4HANA Cloud) - Neo environment

TABLE OF CONTENTS

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

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

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

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 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 6 on how to create a certificate using private and public key information available.

3.2 Configurations for Electronic Documents

For more information, see the documentation for electronic documents for Mexico on SAP Help Portal at https://help.sap.com/viewer/product/SAP_S4HANA_CLOUD. Select your product version. In the *Product Assistance* section, select a language and then select *Country/Region-Specific Functions -> Mexico -> General Functions -> Document and Reporting Compliance*.

3.3 Setup of SAP Cloud Integration

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 Configuration Steps in SAP Cloud Integration

4.1 Deploy the Customer Certificate and Credentials to SAP Cloud Integration

If your PAC is Edicom, you can use an Edicom-specific integration flow to communicate with Edicom. If your PAC is Pegaso, you can use a Pegaso-specific integration flow to communicate with Pegaso. Before sending an XML file using either of the two integration flows, SAP Cloud 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 Integration tenant.

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

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

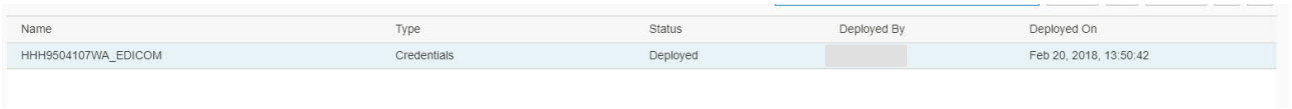
1. Deploy the certificate (as private key with the alias <RfcEmisor>) in the JAVA_KEYSTORE.
   See chapter 6 on how to create a single certificate chain containing both the private key and public certificate.

   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:

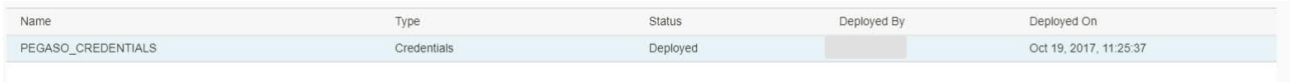


Name	Type	Status	Deployed By	Deployed On
HHH9504107WA_EDICOM	Credentials	Deployed		Feb 20, 2018, 13:50:42

   Note: Your <RfcEmisor> may contain special characters that are not supported in credentials names. In this case, you need to replace the special characters with underscores (_). For example, your <RfcEmisor> is HH&9504107WA_EDICOM. The character & is invalid. You need to enter HH_9504107WA_EDICOM as your credentials name.

   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.

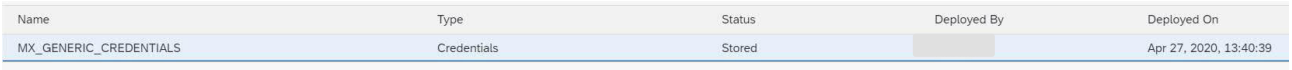
   Here's an example:



Name	Type	Status	Deployed By	Deployed On
PEGASO_CREDENTIALS	Credentials	Deployed		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		Apr 27, 2020, 13:40:39

2. Deploy the public certificate for testing in the JAVA_KEYSTORE of the test tenant. Deploy the public certificate for production use in the JAVA_KEYSTORE of the production tenant.

4.2 Copy the Integration Package

This package contains the following integration flows:

Integration Flow 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 Pegaso for Withholding Tax Certificate	MexicoWTC_Pegaso
Mexico Document Compliance Edicom for Withholding Tax Certificate	MexicoWTC_Edicom
Mexico Document Compliance Generic	MexicoeDocument_generic

There are two integration flow 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 integration flows on your tenant:

Integration Flow Name in WebUI	Explanation
Mexico Document Compliance	Whether you PAC is Edicom or Pegaso, you must deploy this integration flow.
Mexico Document Compliance Edicom	If your PAC is Edicom, in addition to the integration flow **Mexico Document Compliance**, deploy this integration flow as well.
Mexico Document Compliance Pegaso	If your PAC is Pegaso, in addition to the integration flow **Mexico Document Compliance**, deploy this integration flow as well.
Mexico Document Compliance Pegaso for Withholding Tax Certificate	If your PAC is Pegaso and you want to issue electronic withholding tax certificates, in addition to the integration flow **Mexico Document Compliance**, deploy this integration flow as well.
Mexico Document Compliance Edicom for Withholding Tax Certificate	If your PAC is Edicom and you want to issue electronic withholding tax certificates, in addition to the integration flow **Mexico Document Compliance**, deploy this integration flow as well.

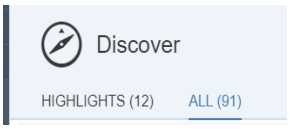
Option 2

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

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

Do the following to copy the integration package:

1. Log in to your SAP Cloud 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 and Reporting Compliance: Electronic Documents for Mexico** and press ENTER.
5. Select the package **SAP Document and Reporting Compliance: Electronic Documents for Mexico**. In the upper right corner, choose **Copy**.

4.3 Deploy Integration Flows

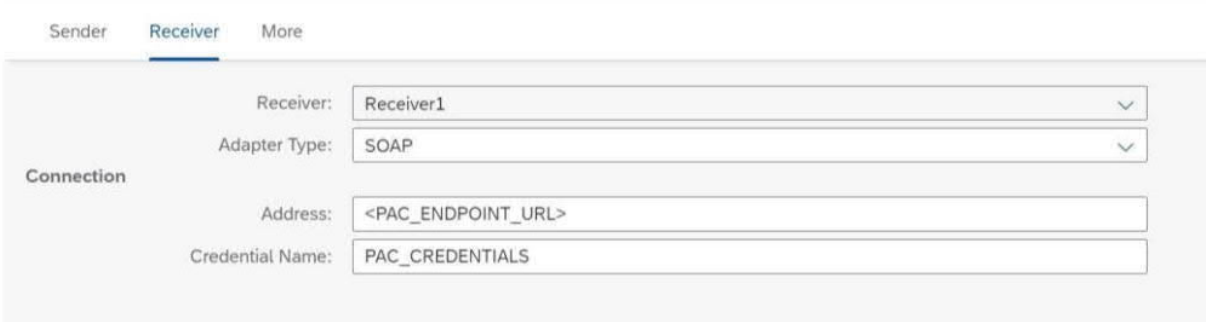
Do the following to deploy the required integration flows:

Configuring Integration Flows

1. Click on the package **SAP Document and Reporting Compliance: Electronic Documents for Mexico**.
2. Go to the **Artifacts** tab page.
3. For the integration flow that you want to change, choose **Actions** > **Configure**.
4. Choose **Save**.

To deploy the generic integration flow Mexico **Document Compliance Generic**, follow the instructions below:

1. Configure the following externalized parameters:
   - **Sender**: endpoint URL of the integration flow
   - **Receiver**: endpoint URL from PAC
   - Credential Name: credential name maintained in the keystore
2. Choose **Deploy**.

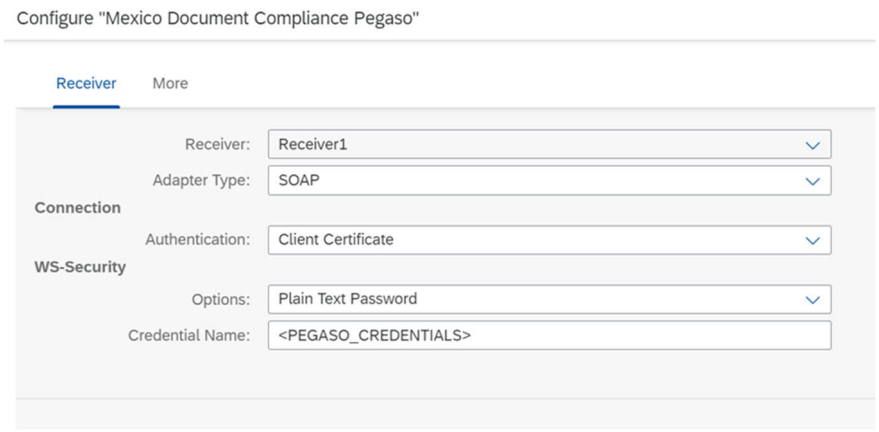


If you use the integration flow “Mexico Document Compliance Pegaso”, proceed as follows:

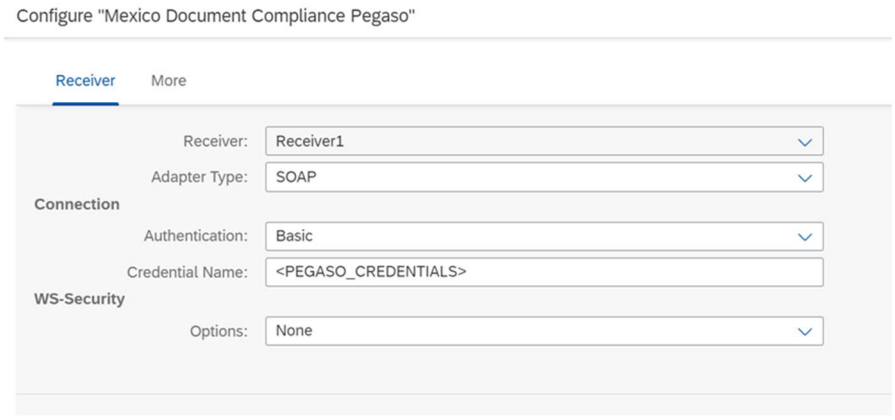
1. Make the following settings:

   - **Authentication**: This setting depends on the Pegaso web service that you use.

     If you use the **Gateway service** from Pegaso, select the **Client Certificate** authentication type and then make the following settings:
     - **Options**: Select **Plain Text Password**.
     - **Credential Name**: Enter the credential name that you’ve configured in the keystore.

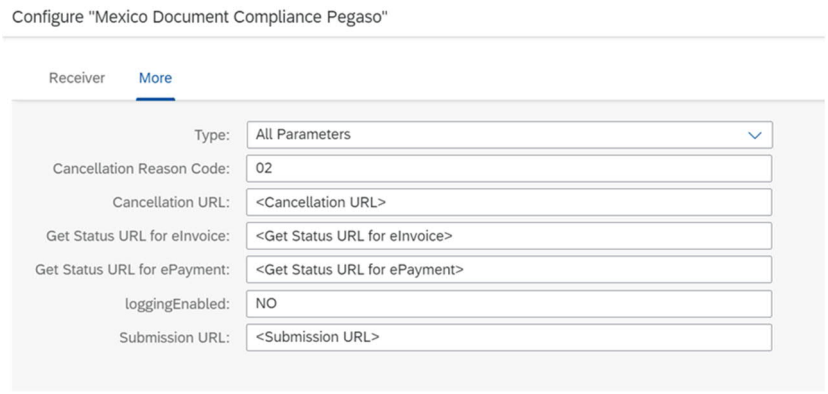


     If you use the Azure service from Pegaso, select the Basic authentication type and then make the following settings:
     - **Credential Name**: Enter the credential name that you’ve configured in the keystore.
     - **Options**: Select **None**.



   - **Submission URL**: Enter the endpoint URL of the web service that submits electronic invoices and payment documents.
   - **Cancellation URL**: Enter the endpoint URL of the web service that cancels electronic invoices and payment documents.

- **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests.
  Note: As of SAP S/4HANA Cloud 2202.1, you can also fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents**. In that case, leave this parameter blank.
- **Get Status URL for eInvoice**: Enter the endpoint URL of the web service that gets statuses of invoice cancellation requests.
- **Get Status URL for ePayment**: Enter the endpoint URL of the web service that gets statuses of payment cancellation requests.
- **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.



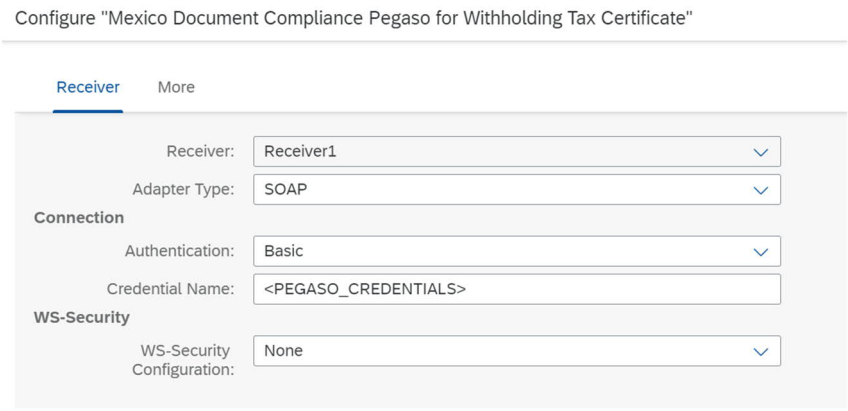
2. Choose **Deploy**.
3. Test the connection.

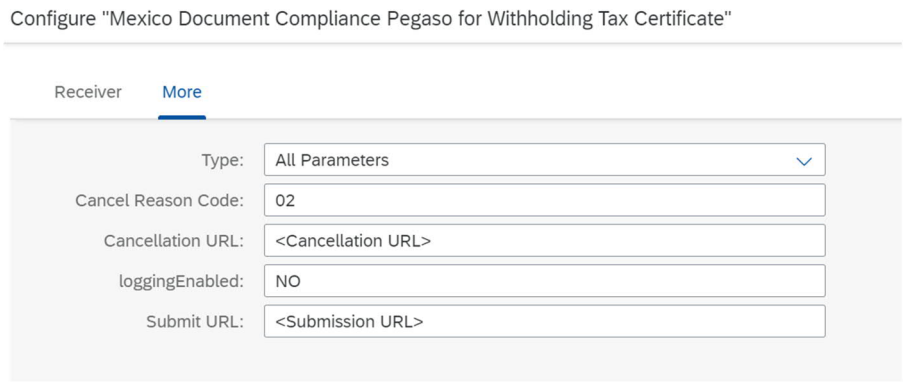
Before testing, ensure the handshake certificate from Pegaso is already deployed in the keystore of the tenant. There is no constraint on the alias here. When downloading the handshake certificate, you can store it under any name.

If you use the integration flow "Mexico Document Compliance Pegaso for Withholding Tax Certificate", proceed as follows:

1. Make the following settings:

- **Authentication**: Select the Basic authentication type and then make the following settings:
  - **Credential Name**: Enter the credential name that you've configured in the keystore.
  - **WS-Security Configuration**: Select **None**.
- **Submission URL**: Enter the endpoint URL of the web service that submits withholding tax certificates.
- **Cancellation URL**: Enter the endpoint URL of the web service that cancels withholding tax certificates.
- **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests.
  Note: As of SAP S/4HANA Cloud 2202.1, you can also fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents**. In that case, leave this parameter blank.
- **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.





2. Choose **Deploy**.
3. Test the connection.

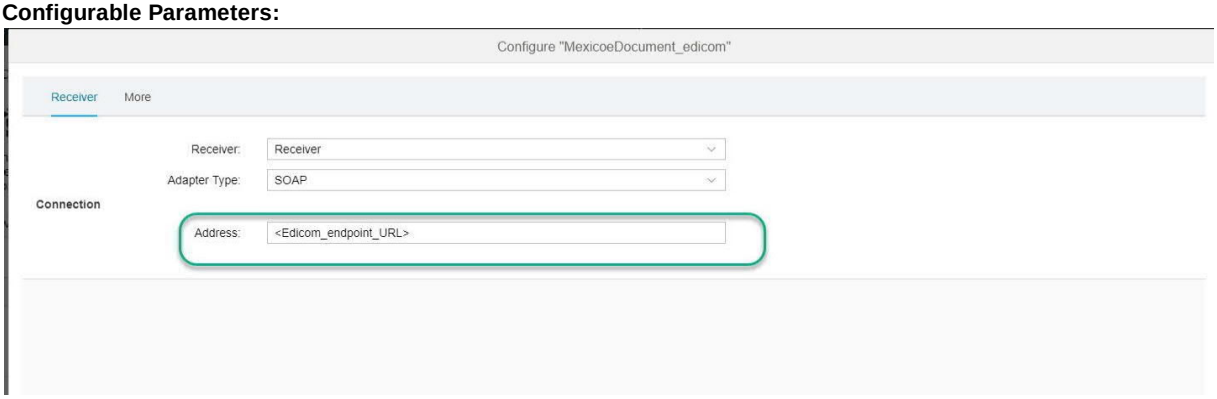
Before testing, ensure the handshake certificate from Pegaso is already deployed in the keystore of the tenant. There is no constraint on the alias here. When downloading the handshake certificate, you can store it under any name.

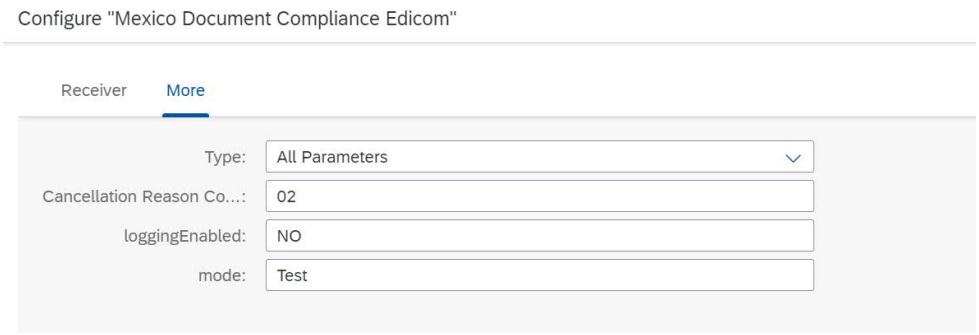
If you use the integration flow "Mexico Document Compliance Edicom", proceed as follows:

1. Configure the following externalized parameters of the integration flow **Mexico Document Compliance Edicom**:
   - **Address**: 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.
   - **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests. **Note**: As of SAP S/4HANA Cloud 2202.1, you can also fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents**. In that case, leave this parameter blank.
   - **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.
2. Choose **Deploy**.

   Before testing, download the handshake certificate from the endpoint that Edicom has provided and store it in the keystore of the tenant. There is no constraint on the alias name that you use to store this certificate. You can store it under any name.

Configurable Parameters:



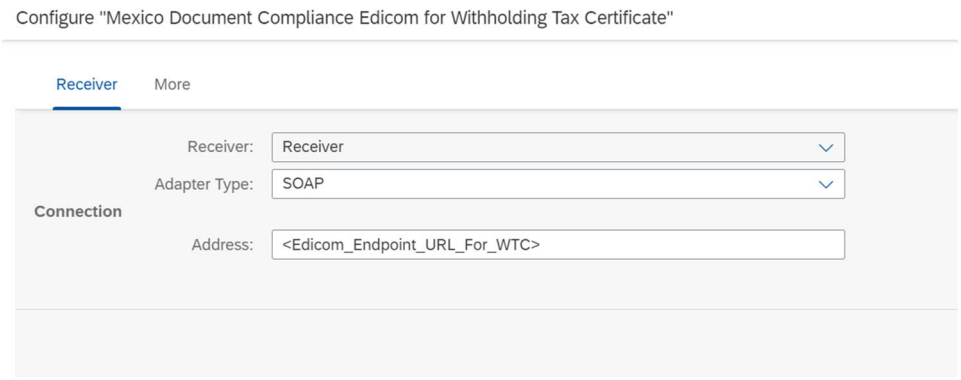


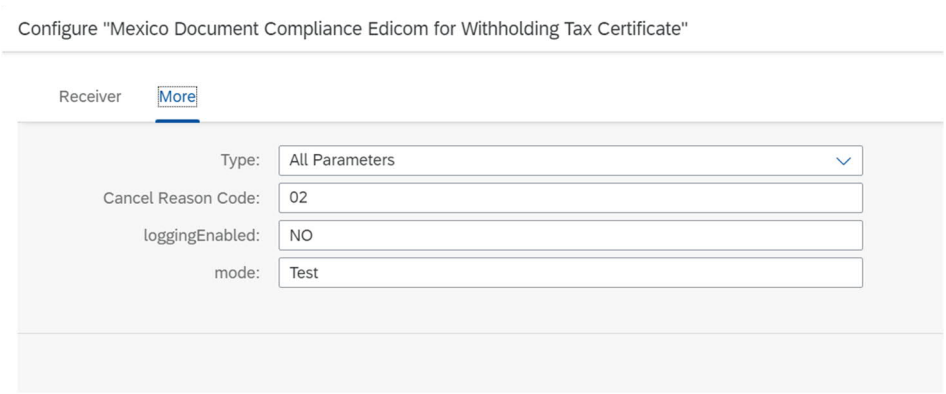
After deploying all the required integration flows, note down the URLs of the endpoints for each service. The endpoints are used in the communication arrangement configurations.

If you use the integration flow “Mexico Document Compliance Edicom for Withholding Tax Certificate”, proceed as follows:

1. Make the following settings:

- **Address**: Enter the endpoint URL from Edicom that submits withholding tax certificates.
- **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.
- **Cancellation Reason Code**: Enter a fixed cancellation reason code for all cancellation requests.
  Note: As of SAP S/4HANA Cloud 2202.1, you can also fill in cancellation reason codes through the eDocument Cockpit or the BAdI **Filling of Cancellation Data for Electronic Documents**. In that case, leave this parameter blank.
- **loggingEnabled**: Enter **YES** if you want to log requests and response messages. Otherwise, enter **NO**.





2. Choose **Deploy**.
3. Test the connection.

Before testing, ensure the handshake certificate from Pegaso is already deployed in the keystore of the tenant. There is no constraint on the alias here. When downloading the handshake certificate, you can store it under any name.

5 Configuration Steps in SAP S/4HANA Cloud

5.1 Configure a Communication System

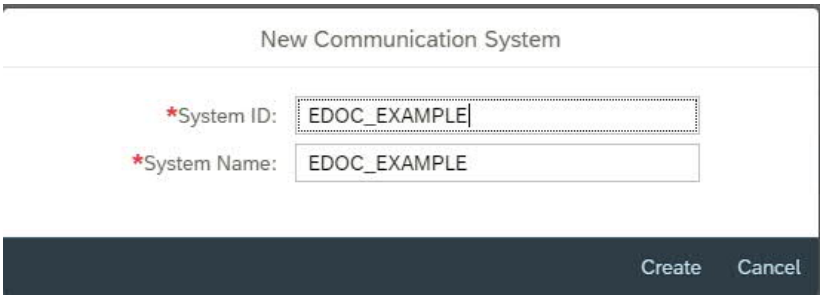
Note the following:

- Communication management settings are not transportable and should be explicitly maintained in quality and production systems.
- The S/4HANA Cloud user, who is following the guide, must be assigned to a business role that contains the business catalog SAP_BCR_CORE_COM for accessing communication management apps.

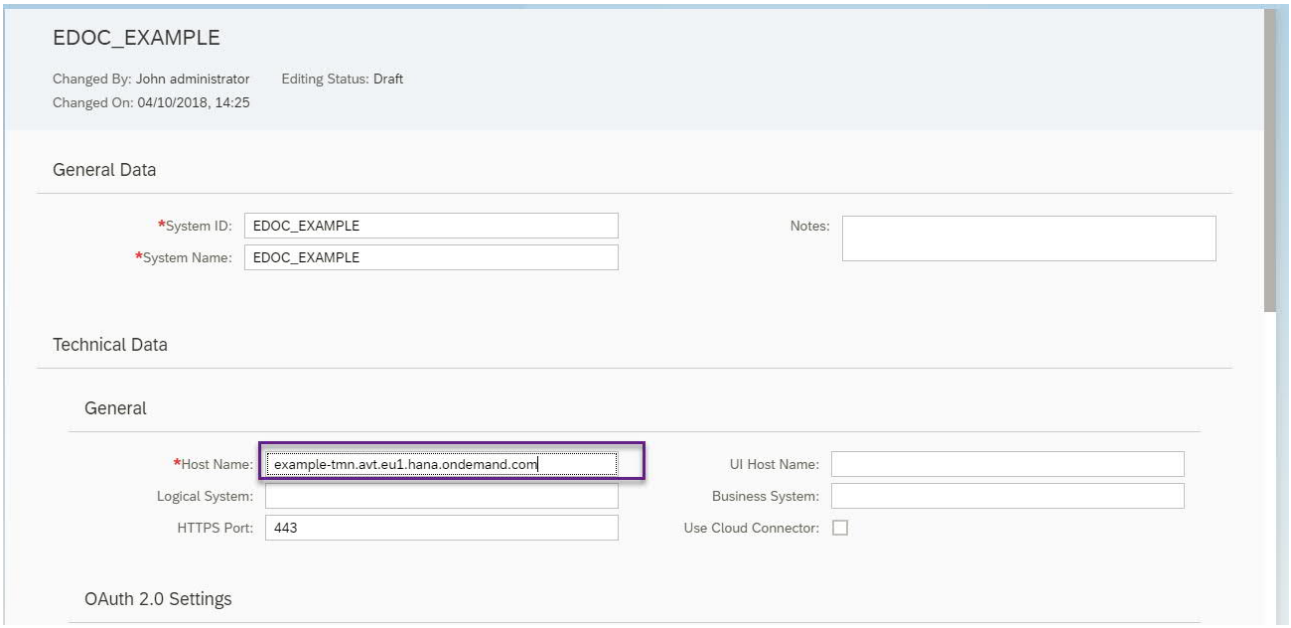
Make settings as follows:

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

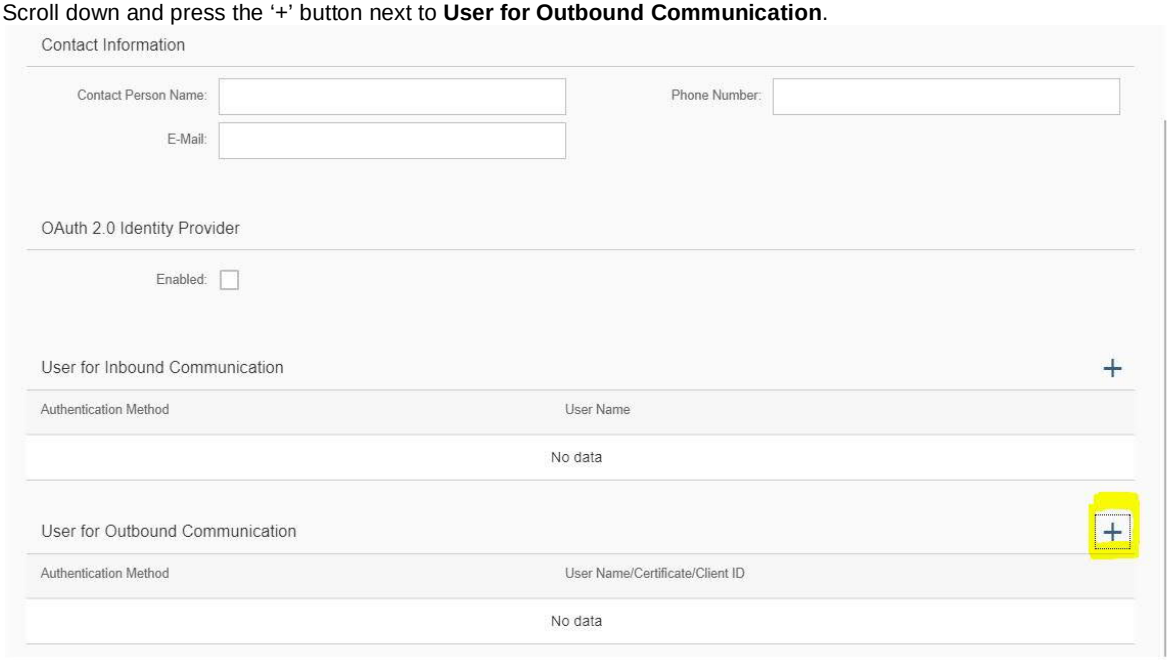
3. Click **New**. In the pop-up window, enter the ID and description of your communication system. It is recommended to name it like *EDOC_<name of SAP Cloud Integration tenant>.* For example, *EDOC_EXAMPLE* for a tenant host name beginning with *example-tmn*.



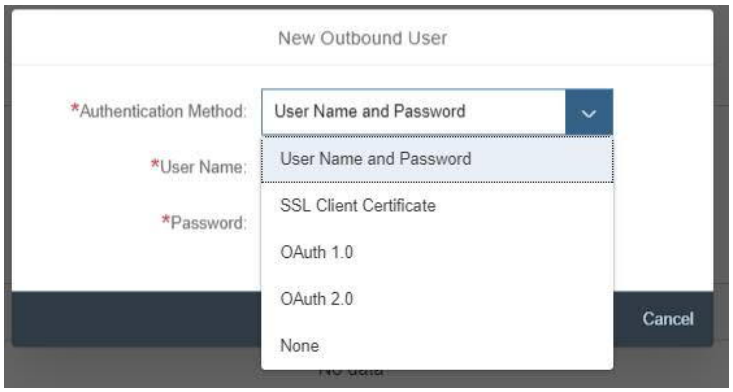
4. Click **Create**.
5. On the next page, enter the host name and port of your tenant.
   You can find the host name for your SAP Cloud Integration tenant, as follows:
   a. From the menu on the left, choose **Monitor**.
   b. Select **Manage Integration Content (All)**.
   c. Search for the integration flow for the scenario you are configuring.
   d. Find the host name from the **Endpoints** tab.
   e. The composition of an endpoint URL is **https://<host name>/<path>**.



6. Scroll down and press the '+' button next to **User for Outbound Communication**.



7. In the new popup window, select the appropriate authentication method to connect to your SAP Cloud Integration tenant.



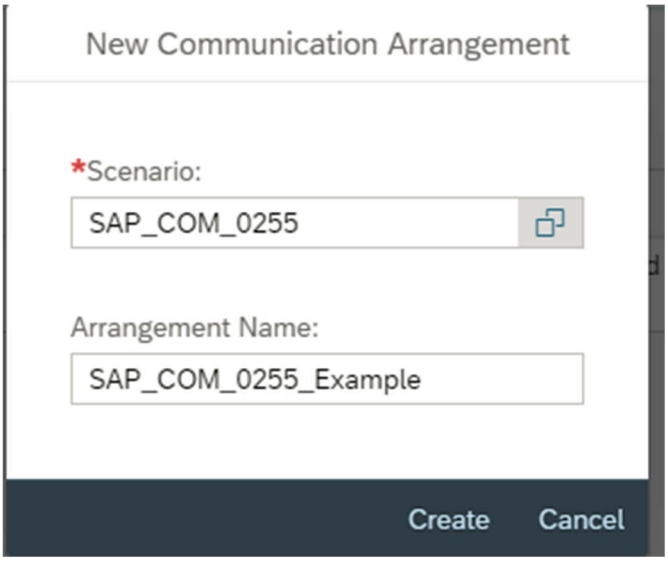
- For the authentication method **User Name and Password**, enter the user name and password of your SAP Cloud Integration tenant user that allows the communication with SAP S/4HANA Cloud.
- For the authentication method **SSL Client Certificate**, select the **Default Client Certificate** type and choose **Create**.

8. Save the changes.

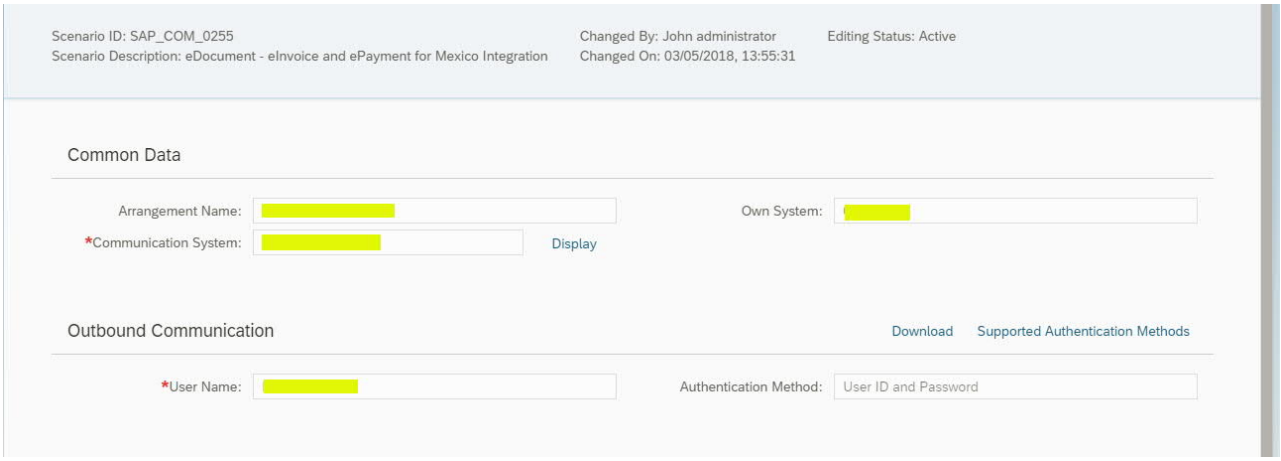
5.2 Configure a Communication Arrangement

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

3. Click **New**. In the pop-up window, enter the ID and description of your communication system.
4. In the new popup window, enter the scenario SAP_COM_0255 and arrangement name. It is recommended to choose a name like SAP_COM_0255_ <name of SAP Cloud Integration tenant>. For example, SAP_COM_0225_EXAMPLE for a tenant host name beginning with example-tmn.



5. Click **Create**.
6. In the new window, choose the communication system created in the previous step.

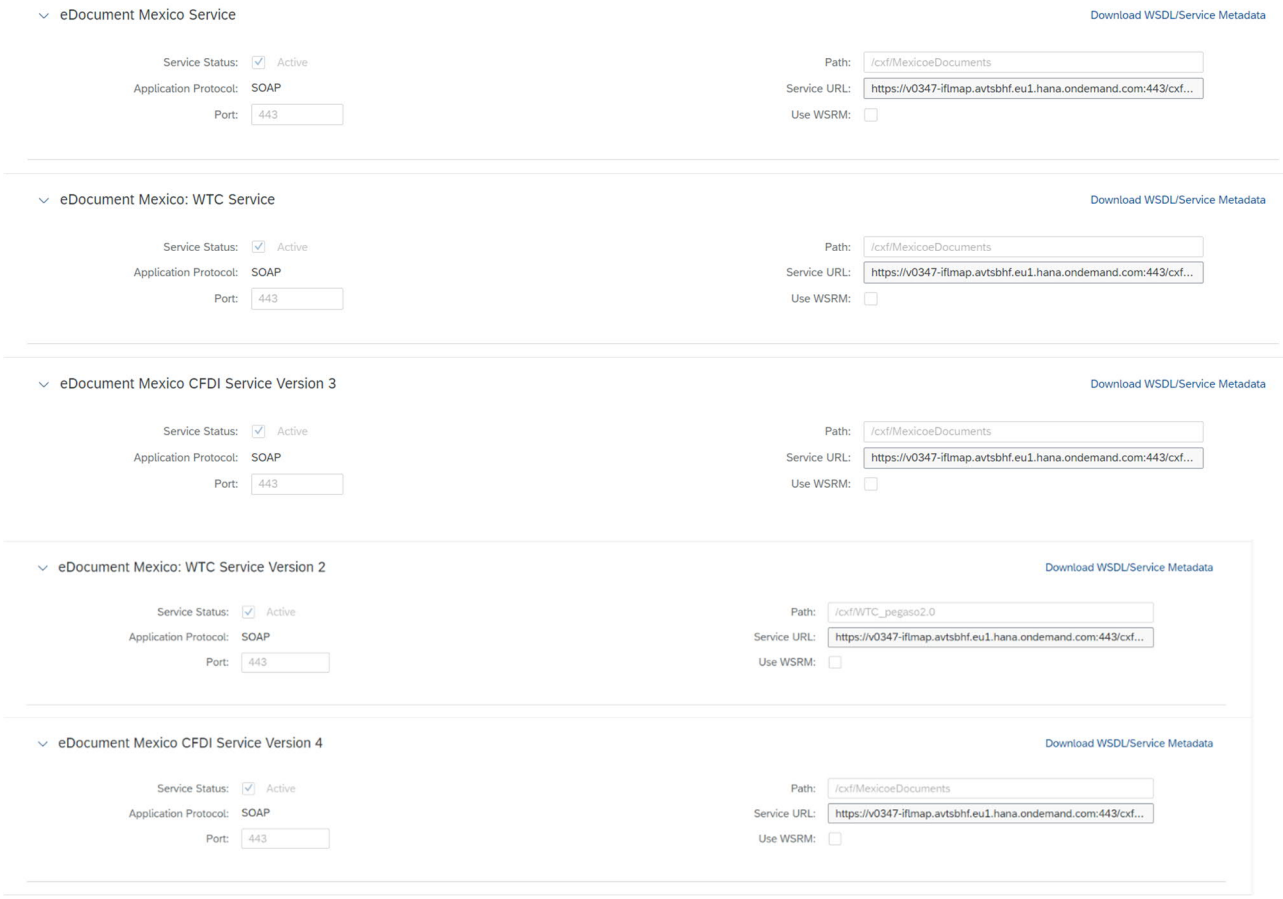


7. For each outbound service, enter the path of the corresponding integration flow.

   See the following table for the outbound service that you should use:

Document Type	Available eDocument Interface Version	Corresponding Outbound Service
Invoices, payment receipt complements, delivery notes	**Interface Version 2** Use this interface version if you want to submit and cancel documents in compliance with CFDI version 3.3.	eDocument Mexico Service
	Interface Version 3 Use this interface version if you want to submit documents in compliance with CFDI version 3.3 and cancel documents in compliance with CFDI version 4.0.	eDocument Mexico CFDI Service Version 3
	Interface Version 4 (available as of SAP S/4HANA Cloud 2202.2) Use this interface version if you want to fully comply with CFDI version 4.0.	eDocument Mexico CFDI Service Version 4
Withholding tax certificates	**Interface Version 1** Use this interface version if you want to submit documents in compliance with CFDI version 3.3 and cancel documents in compliance with CFDI version 4.0.	eDocument Mexico: WTC Service
	Interface Version 2 (available as of SAP S/4HANA Cloud 2202.2) Use this interface version if you want to fully comply with CFDI version 4.0.	eDocument Mexico: WTC Service Version 2

Note:
To set eDocument interface versions, use the configuration activity **Redefine Activation Date for Interface Version**.



8. Save the changes.

6 Appendix

6.1 Generate and Import Certificates

6.1.1 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)

6.1.2 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 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:

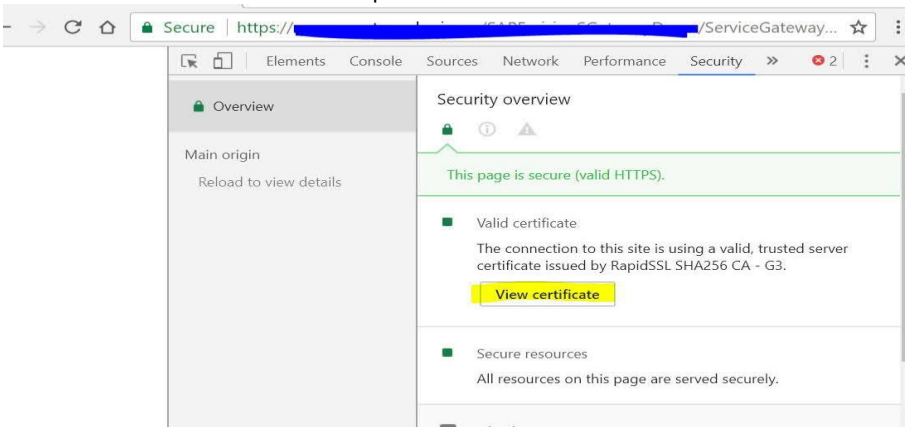
1. Click on **Create a New Keystore**. Select JKS as the type of the new Keystore.
2. Choose **Tools** -> **Import Key Pair** and select the pkcs12 file.
3. Enter a password and click on **Save**.

As the next step, you import the JKS file into the Keystore of SAP Cloud Integration under the alias described in step 1 of the section **Deploy the Customer Certificate and Credentials to SAP Cloud Integration**.

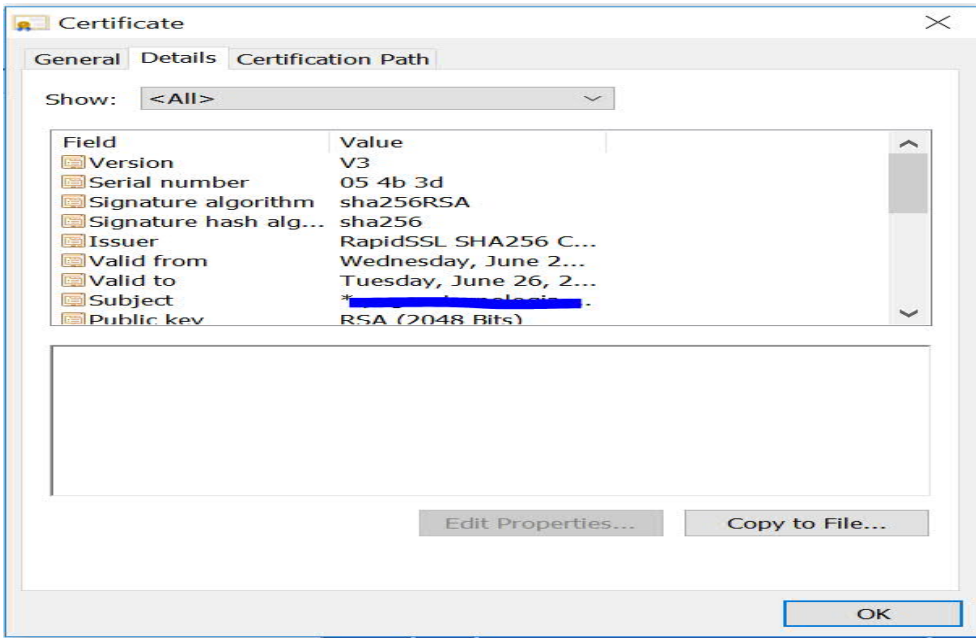
6.1.3 Import the Handshake Certificate

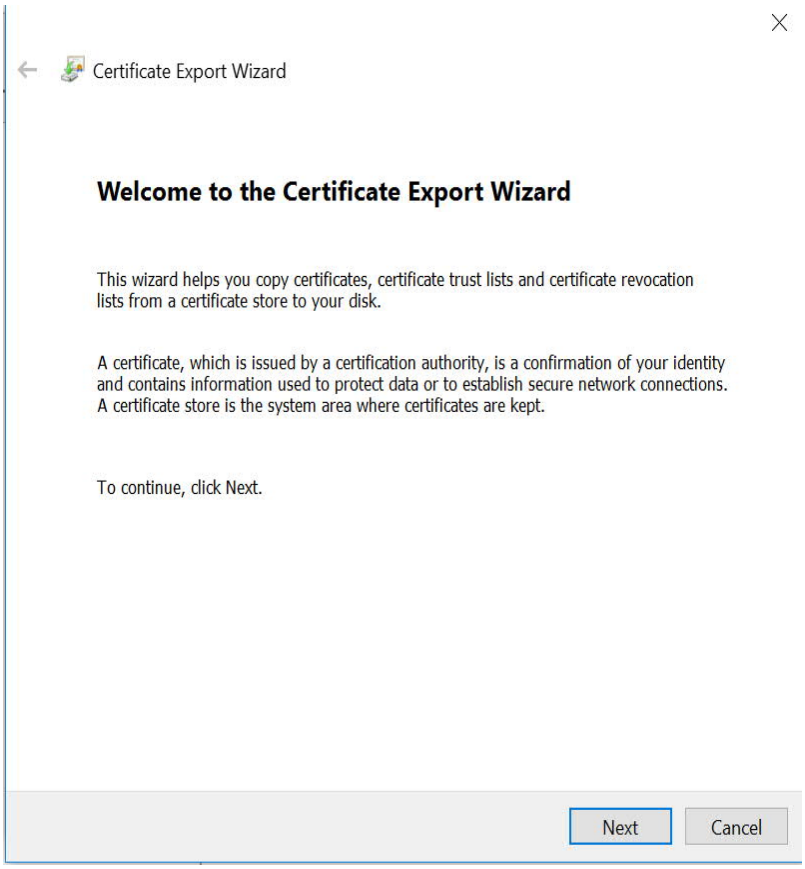
Irrespective of whether the signing happens in SAP Cloud Integration or not, you must download the handshake certificate from the endpoint that is used to connect to the PAC.

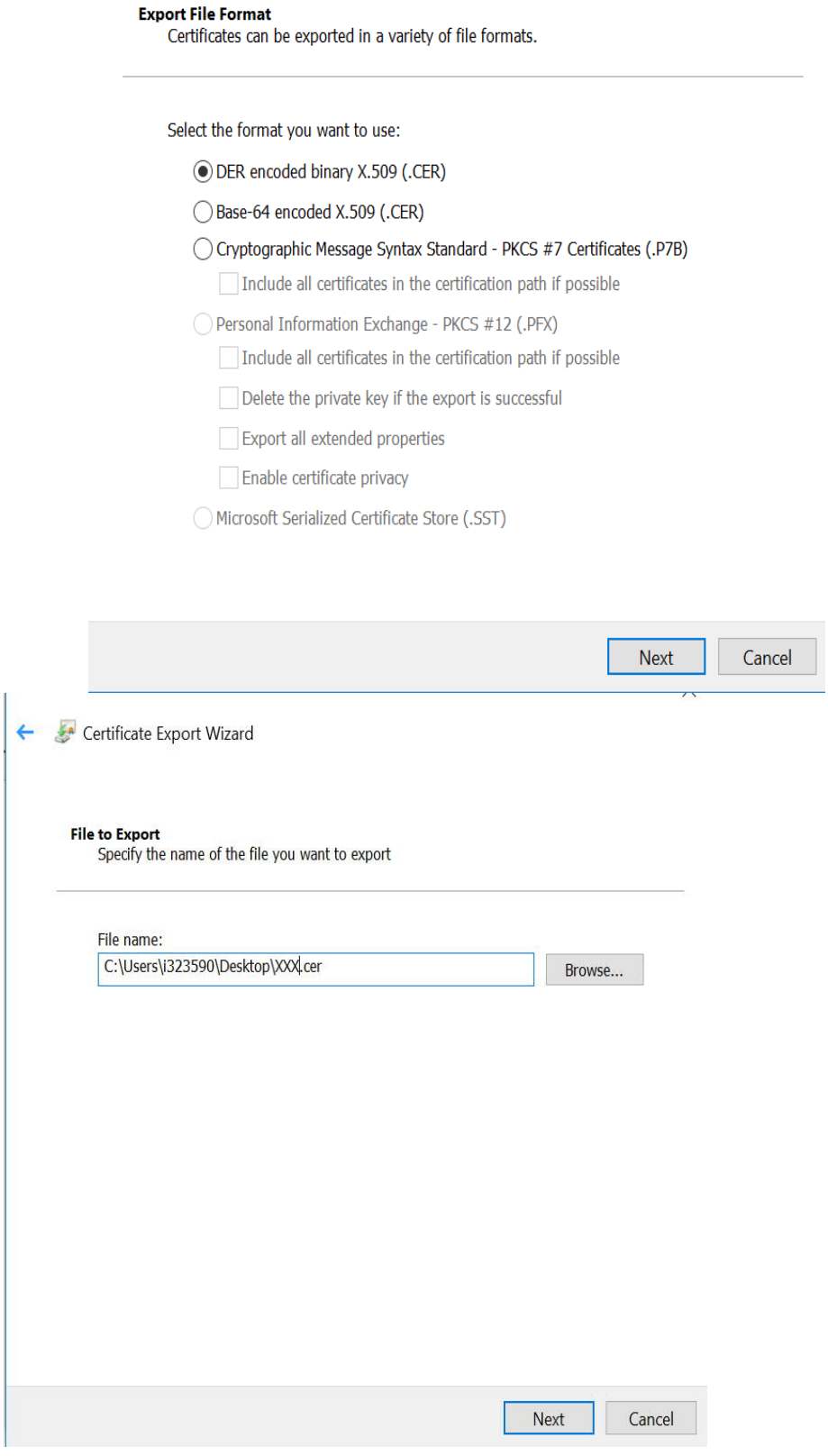
1. Enter the URL into the browser and press F12.



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 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