Integration Guide | PUBLIC
2023-09-01

Saudi Arabia Electronic Invoicing: Setting Up SAP Cloud Integration (SAP ERP, SAP S/4HANA) - Neo Environment

THE BEST RUN SAP

Content

1 Disclaimer

This documentation refers to links to Web sites that are not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

- The correctness of the external URLs is the responsibility of the host of the Web site. Please check the validity of the URLs on the corresponding Web sites.
- The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
- SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

2 Introduction

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

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

3 Prerequisites

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

1. Document and Reporting Compliance: All relevant notes are installed in the test and/or productive systems.
2. SAP Cloud Integration test/productive tenants are live.
3. You have configured the connection from SAP back-end system to SAP Cloud Integration.
4. You have registered your VAT Number in the tax authority's (Fatoora) portal. For more information, please refer the following links:
   - Fatoora portal user manual.pdf (zatca.gov.sa)
   - E-invoicing Detailed Technical Guidelines.pdf (zatca.gov.sa)
   - E-Invoicing (zatca.gov.sa)

3.1 Implementation for Electronic Document Processing Framework

You have implemented and configured the Electronic Document Processing Framework in your test and productive systems. If you did not install the latest support package for your system, refer to the SAP Note 2134248 for the implementation guide of SAP Notes.

Application Help for Electronic Document Processing

For more information about features and country/region availability of each solution, see the application help documentation

- SAP S/4HANA: *Product Assitance* > *English* > *Local Version* > *<Region>* > *<Country/Region>* > *Cross-Application Functions* > *Document and Reporting Compliance*.
- SAP ERP: *Application Help* > *SAP Library* > *Local Version* > *<Region>* > *<Country/Region>* > *Cross-Application Functions* > *Document and Reporting Compliance*.

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.

Outbound HTTP connections are required, and are supported with specific, public certificates.

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

Refer to the system documentation for more information regarding the certificate deployment to SAP back-end systems. If there are 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 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're using a client certificate, this must be signed by one of the root certificates supported by the load balancer. A self-signed certificate isn't 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 Setup of 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 (iFlows).

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

Prerequisites

If you do not find any integration flows in your tenant then refer to Copy Integration Flows [page 14] and Configure Integration Flows [page 15].

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 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

5.1 General Information

The package *SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia* contains the following integration flows:

Integration Flows for Document and Reporting Compliance for Saudi Arabia

Integration Flow Name in WebUI	Project Name/Artifact Name
Saudi Arabia CSID Operations	com.sap.GS.SaudiArabia.CSIDOperations
Saudi Arabia CSID Utilities	com.sap.GS.SaudiArabia.CSIDUtilities
Saudi Arabia Invoice Clearance	com.sap.GS.SaudiArabia.InvoiceClearance
Saudi Arabia Invoice Reporting	com.sap.GS.SaudiArabia.InvoiceReporting
Saudi Arabia Send Invoice	com.sap.GS.SaudiArabia.SendInvoice

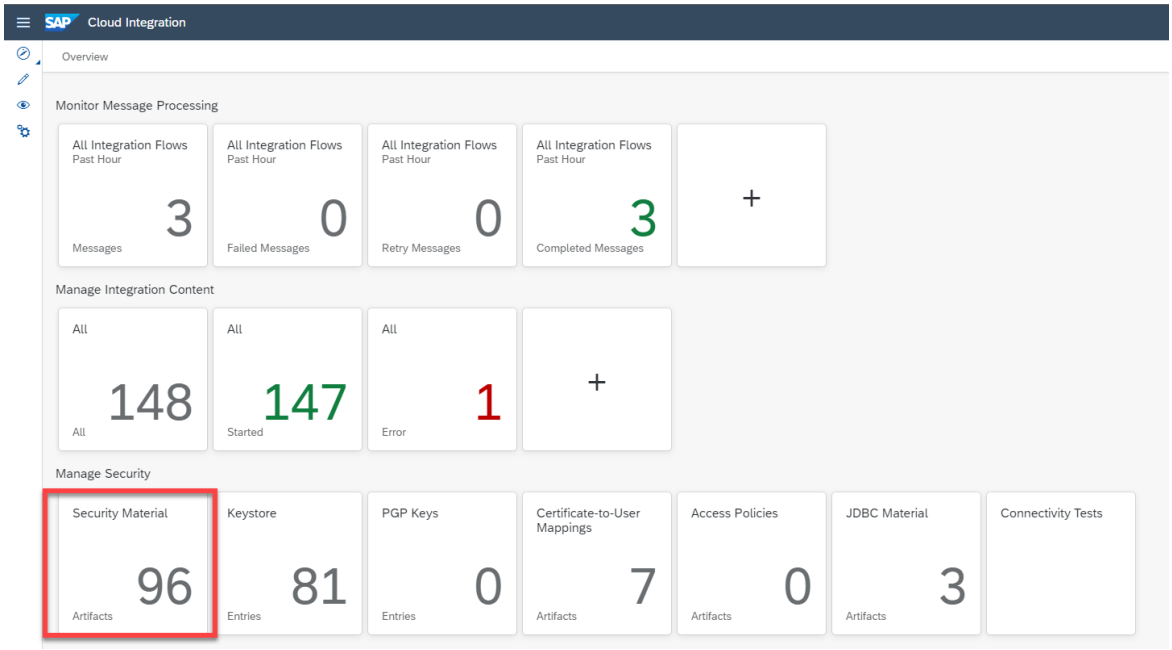
5.2 Deploy Credentials to Tenants

5.2.1 Basic Authentication

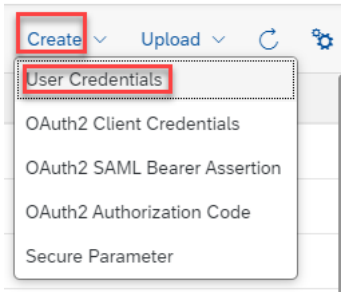
Procedure

Deploy the user ID and password to your SAP Cloud Integration tenant.

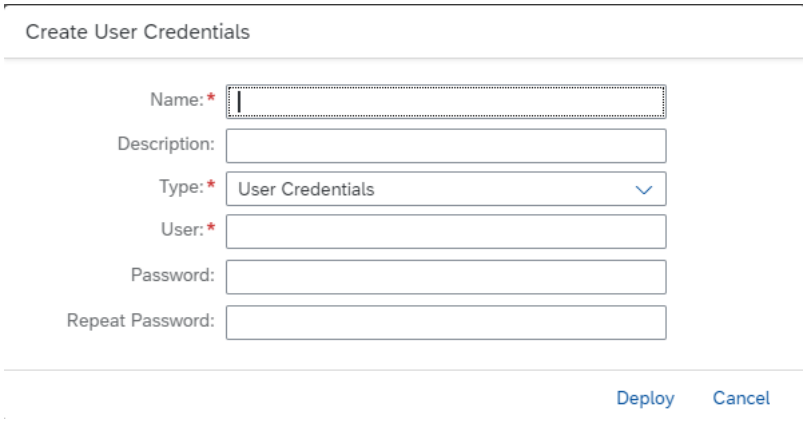
a. In your browser, go to the *Overview* tab and choose *Security Material*.



b. Choose *Create* on the right corner and choose *User Credentials*.



c. Enter the name, username and password, and deploy them.



You need to add User Credentials as follows:

- Name : 'SCI_CREDENTIAL_ALIAS'
- Description : 'SCI Credential Alias'
- Type : 'User Credentials'
- User : <Tenant User ID>
- Password : <Tenant Password>

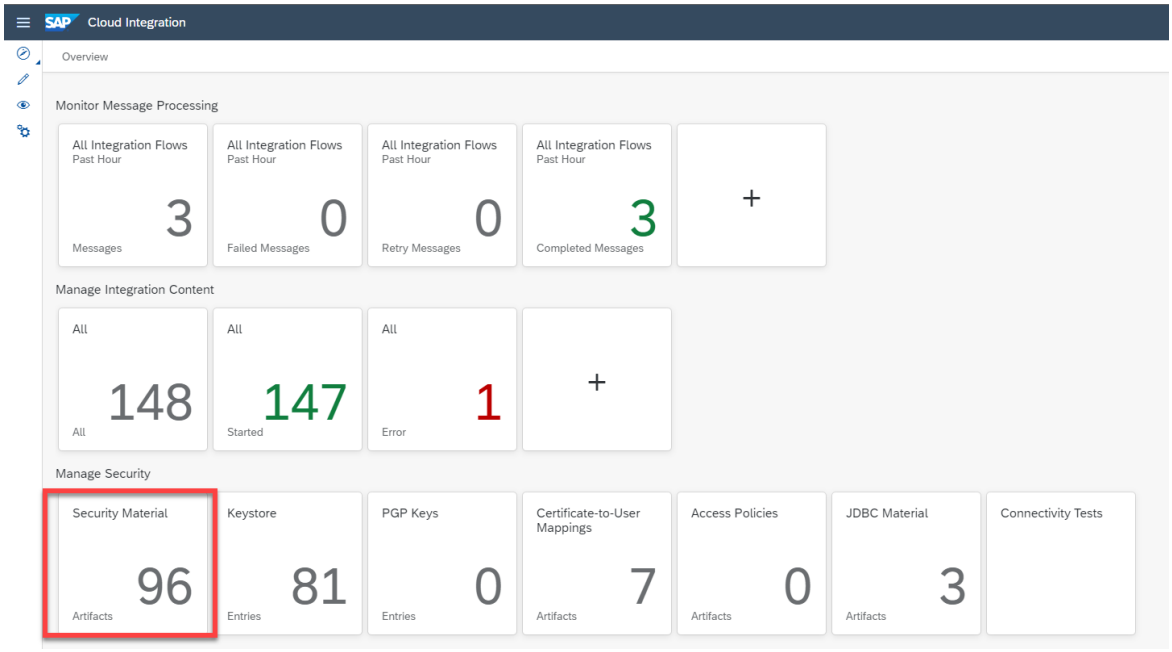
> **Note**
>
> Your <**Tenant User ID**> and your <**Tenant Password**> has to be replaced with the value of your SAP Cloud Integration tenant's User ID and Password respectively.
>
> Your <**Tenant User ID**> should have **IntegrationOperationServer.read**, **NodeManager.deploycredentials**, **NodeManager.read**, **NodeManager.deploycontent** and **NodeManager.deploysecuritycontent** roles assigned to it. For the assignment of the above mentioned roles, please refer Assigning Users and Roles.
>
> The credentials maintained here are used to authenticate SAP Cloud Integration OData API calls for managing the security content. For example, creating Keypair and User Credentials (issued by tax authority) in SCI tenant, as part of onboarding process with the tax authority. For more information, please refer the following links:
>
> - Security Content | SAP Help Portal
> - Overview | Security Content | SAP Business Accelerator Hub

5.2.2 OAuth2 Client Credentials Authentication

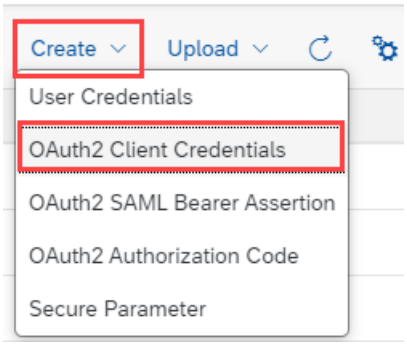
Procedure

Deploy the Client ID and Client Secret to your SAP Cloud Integration tenant.

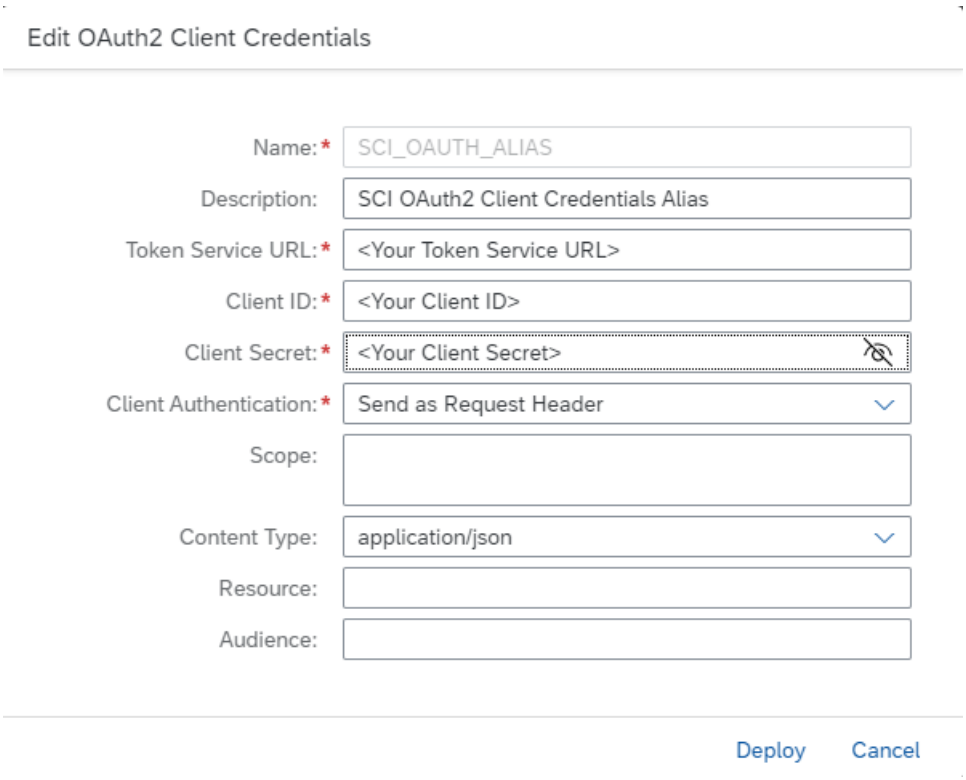
a. In your browser, go to the *Overview* tab and choose *Security Material*.



b. Choose *Create* on the right corner and choose *OAuth2 Client Credentials*.



c. Enter the name, Token Service URL, Client ID and Client Secret, and deploy them.



You need to add OAuth2 Client Credentials as follows:

- Name : 'SCI_OAUTH_ALIAS'
- Description : 'SCI OAuth2 Client Credentials Alias'
- Token Service URL : <Token Service URL>
- Client ID : <Client ID>
- Client Secret : <Client Secret>
- Client Authentication : 'Send as Request Header'
- Content Type : 'application/json'

> **i Note**
>
> <**Token Service URL**>, <**Client ID**> and your <**Client Secret**> has to be replaced with the values *Client ID*, *Client Secret*, and *Token Endpoint* from your OAuth Client respectively. For creating a new OAuth Client, please follow the below steps,

1. Go to the SAP BTP cockpit and open the subaccount.
2. Choose *Security* > *OAuth*. Choose the *Clients* tab.
   Note: The *Token Endpoint* (<Token Service URL>) can be taken from *Branding* tab, under *OAuth URLs* section.
3. Choose *Register New Client*. The ID is automatically generated.
4. Enter a name for the client.
5. In the *Subscription* field, select the appropriate Subaccount/Application.
6. In the *Authorization Grant* field, select *Client Credentials*.
7. In the *Secret* field, define a password of your choice.
8. Choose *Save*.

Your <**`Client ID`**> should have IntegrationOperationServer.read, NodeManager.deploycredentials, NodeManager.read, NodeManager.deploycontent and NodeManager.deploysecuritycontent roles assigned to it. For the assignment of the above mentioned roles, please refer *OAuth2.0* section in SAP Note 2773752.

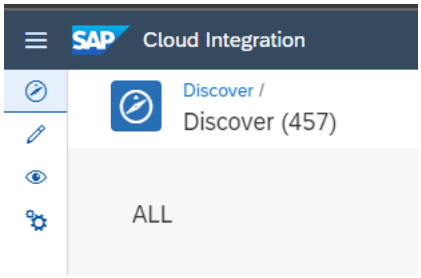
5.3 Copy Integration Flows

Context

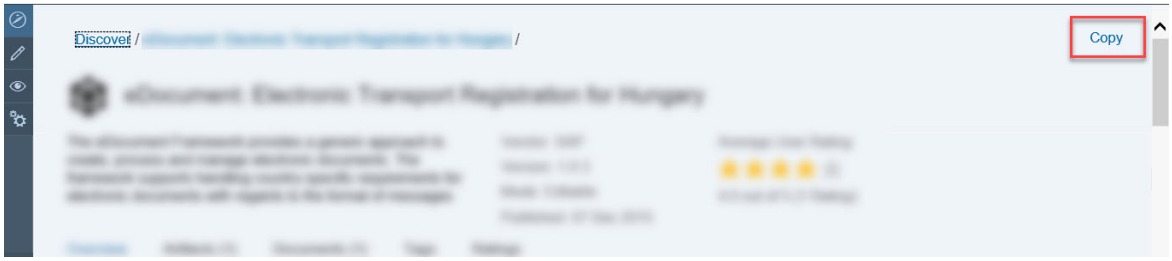
Copy all integration flows in the package *SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia* to the target tenant as follows:

Procedure

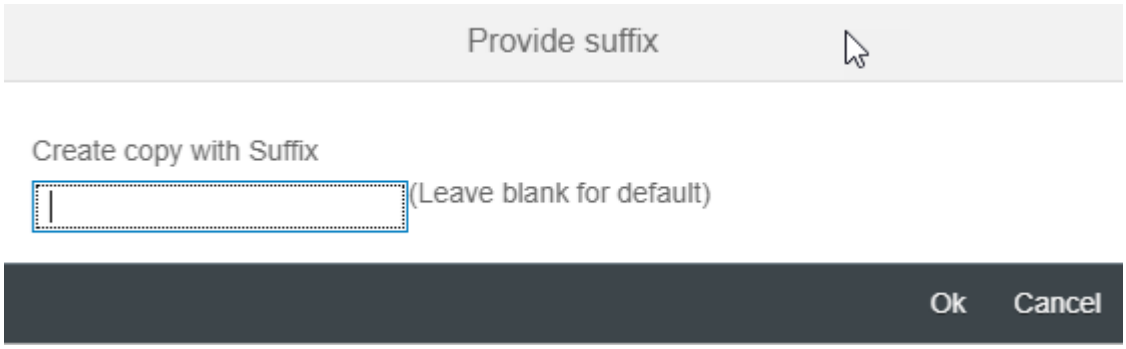
1. In your browser, go to the WebUI of the tenant (URL: <Tenant URL>/itspaces/#shell/catalog).
2. Choose *Discover* > *All*.



3. Search for *SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia*.
4. Select the Package and choose *Copy*.



5. In the *Provide suffix* dialog box, leave the field blank, and choose *Ok*.



5.4 Configure Integration Flows

Context

You configure the package that you've copied as described in Copy Integration Flows [page 14].

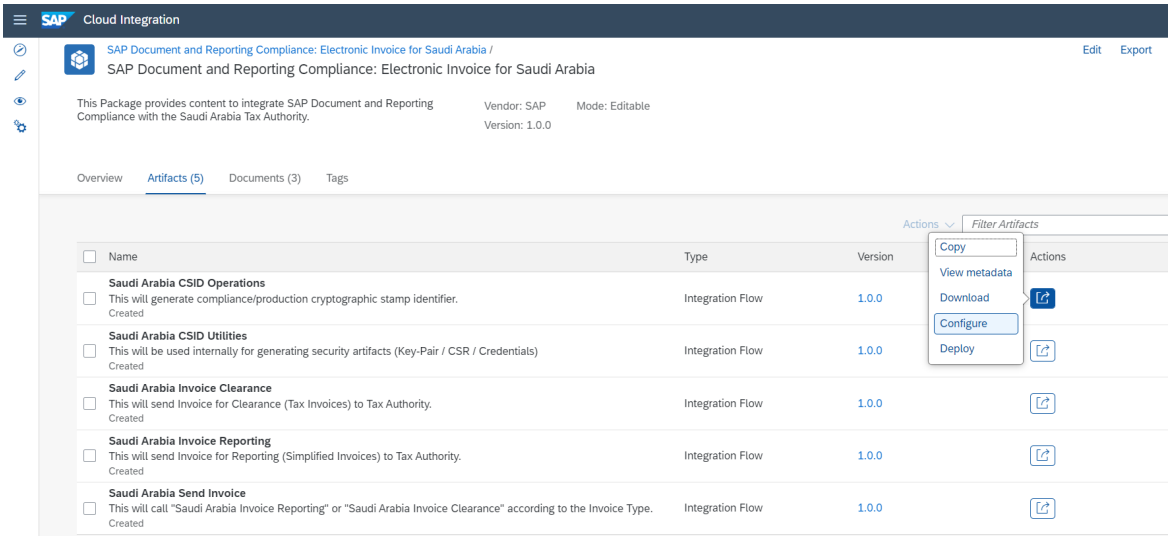
Procedure

1. Choose *Design* from the upper left corner of the page.
2. Click on the package that you copied from the original *SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia* package.
3. Go to the *Artifacts* tab page.
4. There are five *Artifacts* in the integration package *SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia*:
   - Saudi Arabia CSID Operations
   - Saudi Arabia CSID Utilities
   - Saudi Arabia Invoice Clearance
   - Saudi Arabia Invoice Reporting

- Saudi Arabia Send Invoice

Take *Saudi Arabia CSID Operations* as an example, similar steps should be done for the other integration flows:

5. Choose *Actions* > *Configure* for the artifact you're configuring.



6. Choose *Configure* > *More* tab (in some versions it may be *Externalized Parameters*).

There are specific URLs you need to enter for different integration flows.

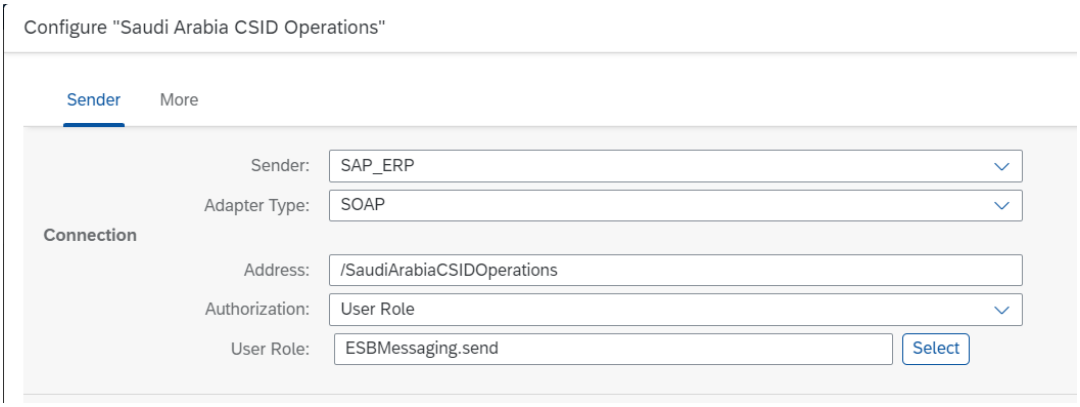
Parameter Name	Value
SCI_HOST	Your tenant URL. For example: `https://xxxxx.hana.ondemand.com`
PROD_URL	`https://gw-fatoora.zatca.gov.sa/e-invoicing/core`
TEST_URL	`https://gw-fatoora.zatca.gov.sa/e-invoicing/simulation`
Mode	`TEST` / `PROD`
Authentication	`Basic` / `OAuth2 Client Credentials`
Credential Name	`SCI_CREDENTIAL_ALIAS` / `SCI_OAUTH_ALIAS`

> **Note**
>
> For test systems, you can use the Mode as `TEST` and for production systems, you can use the Mode as `PROD`.
>
> For Basic Authentication, use `SCI_CREDENTIAL_ALIAS` as credential name and for OAuth2 Client Credentials Authentication, use `SCI_OAUTH_ALIAS` as credential name.

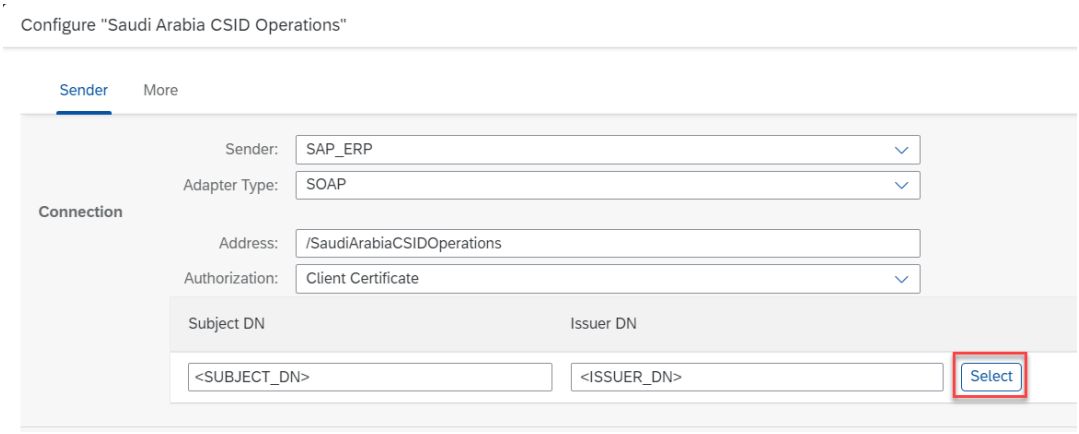
7. Choose *Configure* > *Sender* tab.
   - Use the `Address` parameter to set up the integration package address. Normally you don't have to change this field. In case you change the field, make sure to use the same address when configuring the logical ports in the next chapter.
   - Use the `Authorization` parameter to configure the authorization type.

Value	Description
User Role	You want to use basic authentication (user/password).
Client Certificate	You want to use client certificate authentication.

   - Use the `User Role` parameter to configure the role based on which the inbound authorization is checked. Choose *Select* to get a list of all available roles.
     The role `ESBMessaging.send` is provided by default.



   - Use the `Subject DN` and `Issuer DN` parameters to configure the Certificate based on which inbound authorization is checked. Choose *Select* and upload the required Certificate from your local machine.



8. Choose *Save* and *Deploy* to deploy it actively to server. Note down the URLs of the endpoints for each service.

> **i Note**
>
> Depending on the version of your tenant, after pressing these buttons, a warning message can appear. You can ignore these messages by choosing *Close*.

5.5 Create Logical Ports in SOAMANAGER

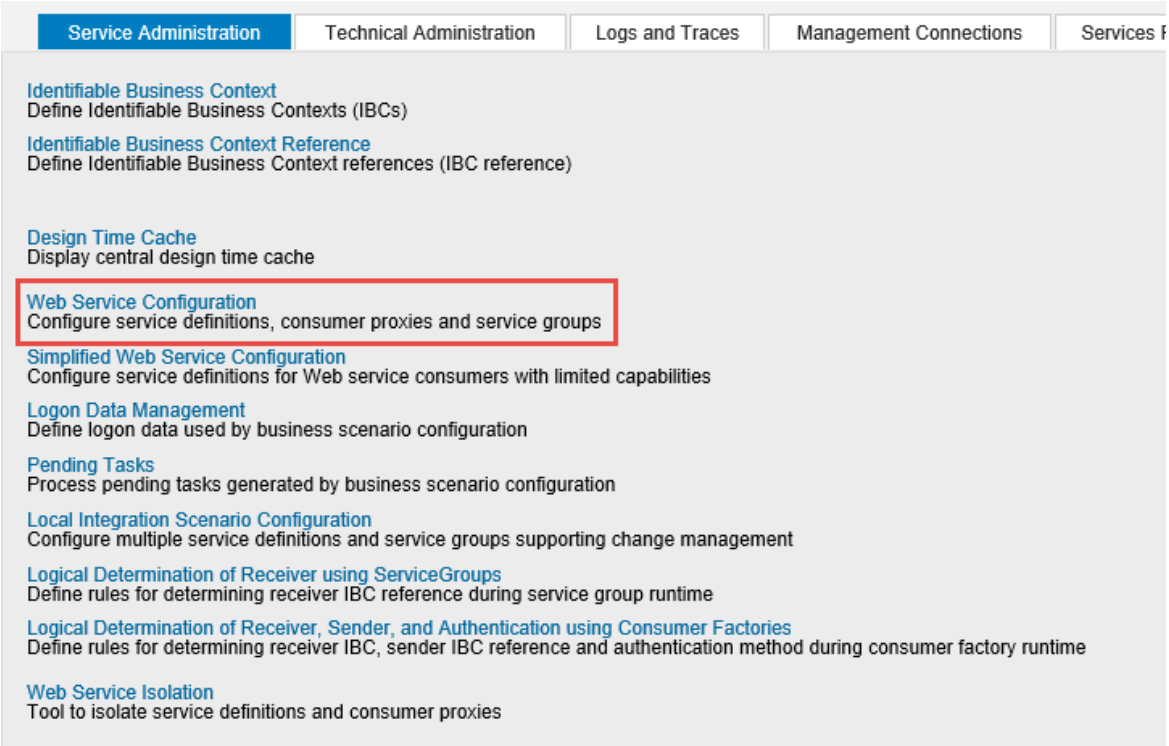
Context

You configure proxies that 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.

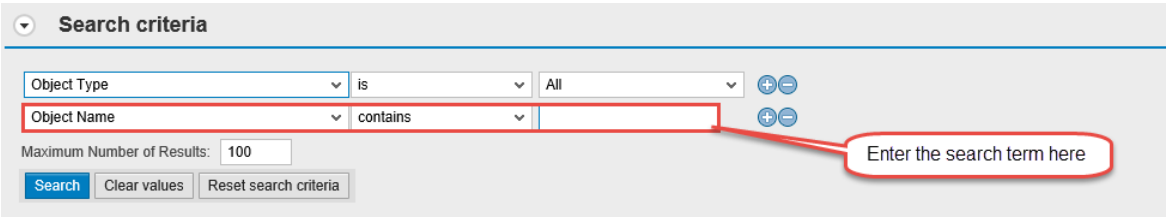
> **i Note**
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

Procedure

1. In your SAP back-end system, go to the `SOAMANAGER` transaction and search for *Web Service Configuration*.



2. Find the proxies for SAP Document and Reporting Compliance (eDocument) for Saudi Arabia with search term **`*edo*sa*`** .



The following table lists the proxies and the logical port name, description, and path for each proxy.

Logical Port details for CSID Operations proxy:

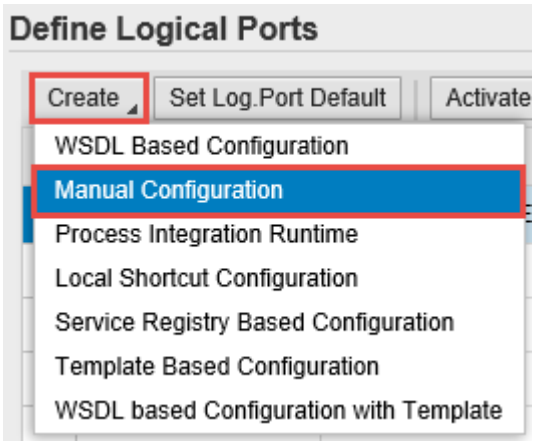
Proxy Name	CO_EDO_SA_CSID_OPERATIONS
Logical Port Name	EDO_SA_CSID
Description	Saudi Arabia: CSID Operations
Path	/cxf/SaudiArabiaCSIDOperations

Logical Port details for Send Invoice proxy:

Proxy Name	CO_EDO_SA_SEND_INVOICE_V2_0
Logical Port Name	EDO_SA_SEND_INVOICE
Description	Saudi Arabia Send Invoice

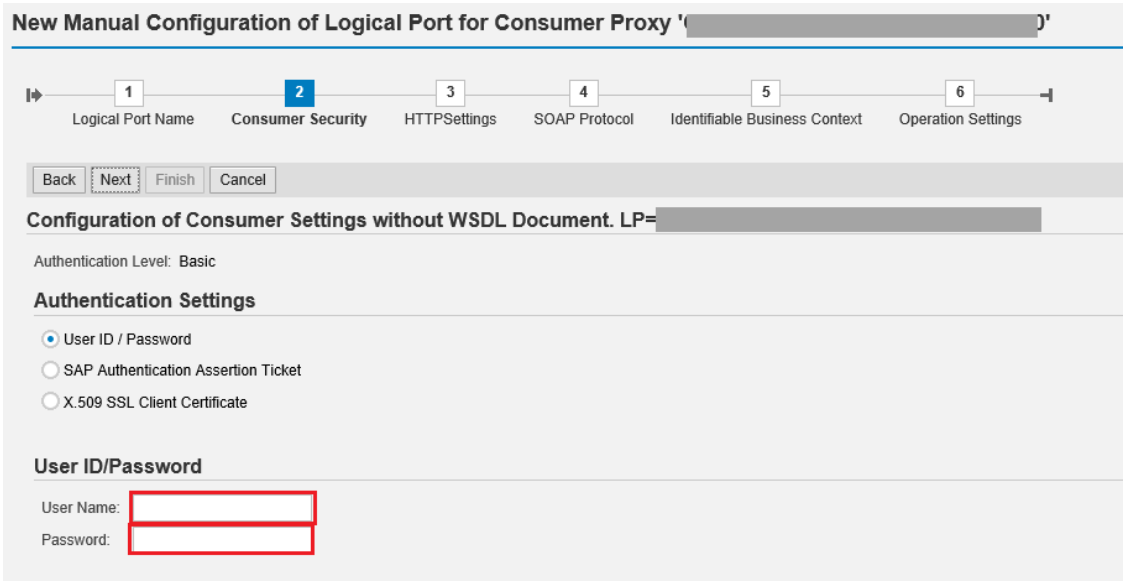
Path	/cxf/SaudiArabiaSendInvoice

3. In the *Result List*, select a proxy from the list above 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 do in the *Consumer Security* tab in the *Configuration* screen depends on the security being used in the communication between the SAP back-end system and SAP Cloud Integration.
   a. If you use the basic authentication, select the *User ID / Password* and enter *User Name* and *Password*.

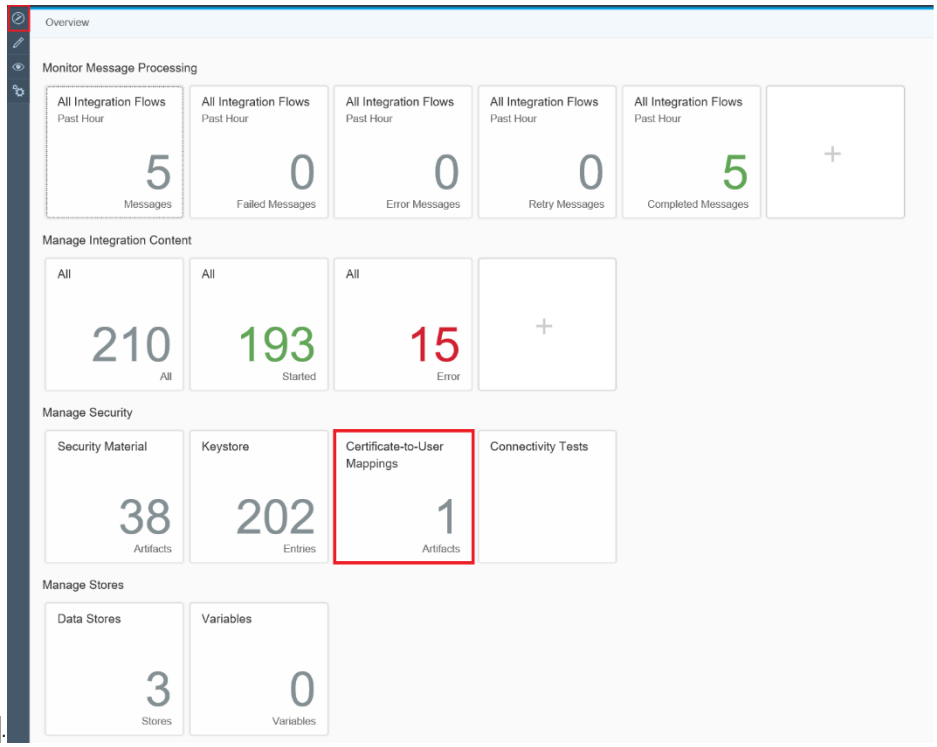


b. If you use certificate-based authentication, select *X.509 SSL Client Certification*. Ensure that the required certificates are available in the `STRUST` transaction.

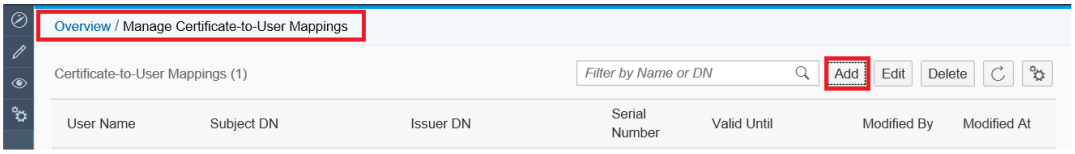
Note: If you don't see this option or can't select it, check the SAP Notes 2368112 and 510007

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`

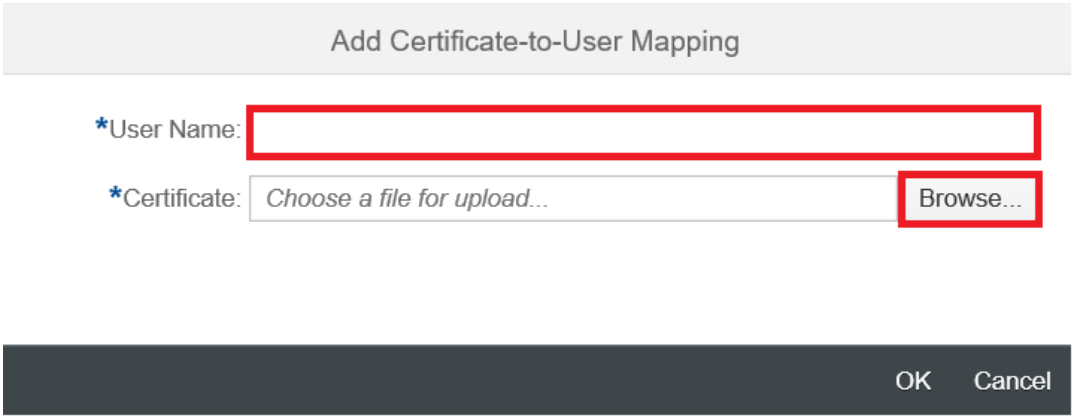
1. Export the SSL Client PSE of the `STRUST` transaction.
2. Go to SAP Cloud Integration under *Overview* > *Certificate-to-User Mappings*.



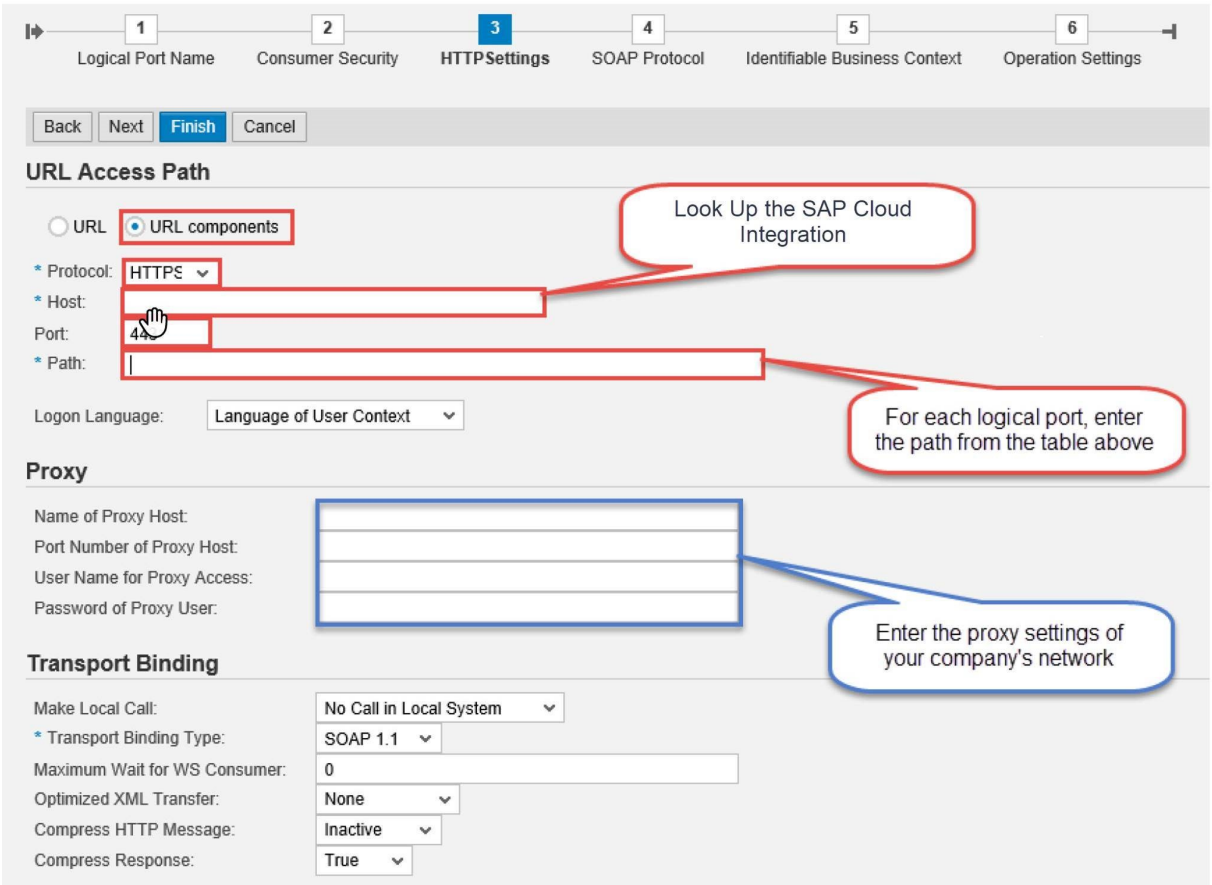
3. Choose *Add*.



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

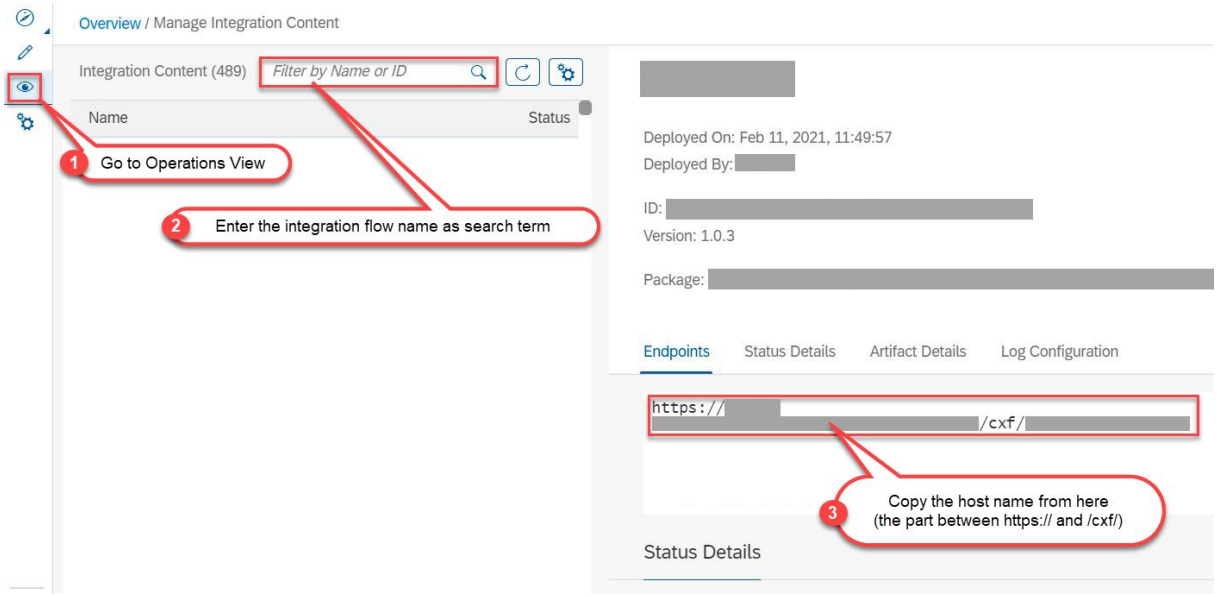


6. On the *HTTP Settings* tab, make the following entries:



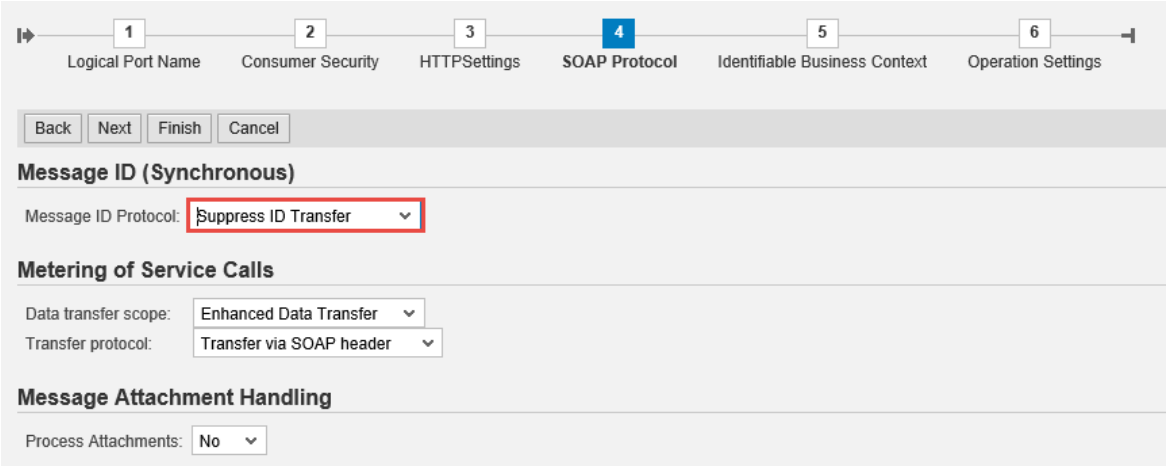
Port 443 is the standard port for the HTTPS protocol.

To find the Host, go to SAP 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.

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



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

   To check if the connection works, choose Ping Web Service. If the connection works, the system shows the following result (HTTP 405 Service Ping ERROR: Method Not Allowed).

   You can set up an HTTP connection in the `SM59` transaction. Maintain a host and a port of SAP Cloud Integration service and execute a connection test. If there is a successful connection, you receive an error with HTTP return code 500.

9. Remember to create logical ports for each proxy and to execute the following steps in the SAP back-end systems, see SAP Note 2683318 for more information.

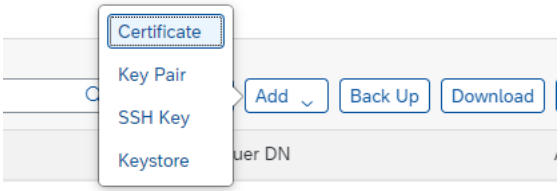
- Define the SOA service names and assign the logical ports to the combination of a SOA service name and a company code in `EDOSOASERV` view.
- Assign the SOA service names you created before to an interface ID in `EDOINTV` view

5.6 Retrieve and Save Server Certificate Chain of Tax Authority

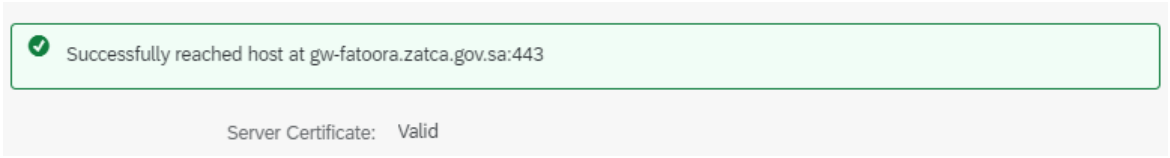
You can find and save the Server Certificate Chain from your Tax Authority

Procedure

1. In your browser, navigate to the WebUI of the tenant (URL: `<Tenant URL>/itspaces/shell/monitoring/`).
2. Under *Manage Security*, choose *Connectivity Tests*.
3. Choose *TLS*. Enter the following details:
   - Host: `gw-fatoora.zatca.gov.sa`
     Port: `443`
   - Clear the options **`Authenticate with Client Certificate`** and **`Valid Server Certificate Required`**.
4. Choose *Send*.
5. Download and extract the Server Certificate Chain.
6. Navigate to *Manage Security* from step 2. Choose *Keystore*.
7. Add all the extracted Certificates, one after another. Choose *Add* > *Certificate*. Browse and choose a certificate to upload. Choose *Add*.



8. Repeat steps 3 and 4 with the option **`Valid Server Certificate Required`** checked.



6 Test the Integration

Describes the steps to test the integration of SAP Document and Reporting Compliance with the integration scenario from SAP Cloud Integration.

Context

The best way to test if the integration works is to create and submit an eDocument from SAP backend system and see if that reaches the destination system, typically the tax authority's system.

Procedure

1. In the back-end system, go to the *eDocument Cockpit* (EDOC_COCKPIT) transaction, in the relevant process.
2. Select an eDocument and check the status of the eDocument in the Cockpit and perform the following actions, accordingly:
   a. If the status of the eDocument is `Created`, the eDocument was created but not submitted yet. In this case, select it and choose *Submit*. This action triggers the creation of the XML and the subsequent communication with SAP Cloud Integration.
   a. If the status is green or yellow, but not `Created`, the communication with SAP Cloud Integration was triggered and was probably successful. You can double-check if the message went through on the SAP Cloud Integration tenant. Alternatively, you can use a trace from the `SRT_UTIL` transaction to look at the XMLs transmitted via web services from the SAP back-end systems.
   b. If the status is red, an error happened during the submission of the eDocument. Select the *Interface Field* to be directed to the Application Interface Platform (AIF) where you can check the log. Any communication errors are displayed there.
3. If the eDocument is successfully submitted, the status changes to *Accepted by Tax Authority*, then the connection to tax authority has been correctly set up.

Important Disclaimers and Legal Information

Hyperlinks

Some links are classified by an icon and/or a mouseover text. These links provide additional information.
About the icons:

- Links with the icon : You are entering a Web site that is not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:
  - The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
  - SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.
- Links with the icon : You are leaving the documentation for that particular SAP product or service and are entering an SAP-hosted Web site. By using such links, you agree that (unless expressly stated otherwise in your agreements with SAP) you may not infer any product claims against SAP based on this information.

Videos Hosted on External Platforms

Some videos may point to third-party video hosting platforms. SAP cannot guarantee the future availability of videos stored on these platforms. Furthermore, any advertisements or other content hosted on these platforms (for example, suggested videos or by navigating to other videos hosted on the same site), are not within the control or responsibility of SAP.

Beta and Other Experimental Features

Experimental features are not part of the officially delivered scope that SAP guarantees for future releases. This means that experimental features may be changed by SAP at any time for any reason without notice. Experimental features are not for productive use. You may not demonstrate, test, examine, evaluate or otherwise use the experimental features in a live operating environment or with data that has not been sufficiently backed up.
The purpose of experimental features is to get feedback early on, allowing customers and partners to influence the future product accordingly. By providing your feedback (e.g. in the SAP Community), you accept that intellectual property rights of the contributions or derivative works shall remain the exclusive property of SAP.

Example Code

Any software coding and/or code snippets are examples. They are not for productive use. The example code is only intended to better explain and visualize the syntax and phrasing rules. SAP does not warrant the correctness and completeness of the example code. SAP shall not be liable for errors or damages caused by the use of example code unless damages have been caused by SAP's gross negligence or willful misconduct.

Bias-Free Language

SAP supports a culture of diversity and inclusion. Whenever possible, we use unbiased language in our documentation to refer to people of all cultures, ethnicities, genders, and abilities.

www.sap.com/contactsap

THE BEST RUN SAP