Integration Guide | PUBLIC
2023-11-14

Saudi Arabia Electronic Invoicing Setting Up SAP Integration Suite (SAP S/4HANA Cloud) - Cloud Foundry Environment

THE BEST RUN SAP

Content

1 Disclaimer. 3

2 Introduction. 4

3 Prerequisites. 5

3.1 Setup of Secure Connection. 5

3.2 Retrieve and Save Public Certificates. 6

4 Configuration Steps in SAP Integration Suite. 7

4.1 General Information. 7

4.2 Deploy Credentials to Tenants. 7

Basic Authentication. 7

OAuth2 Client Credentials Authentication. 9

4.3 Copy Integration Flows. 11

4.4 Configure Integration Flows. 12

4.5 Retrieve and Save Server Certificate Chain of Tax Authority. 15

5 Configuration Steps for SAP S/4HANA Cloud. 16

5.1 Configuring Communication System. 16

5.2 Configuring Communication Arrangement. 18

1 Disclaimer

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

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

2 Introduction

You use SAP Cloud Integration to establish the communication with external systems with whom you want to exchange electronic documents created with *SAP Document and Reporting Compliance*. This document lists the required setup steps you perform in the SAP ERP or SAP S/4HANA system* and the SAP Cloud Integration tenant so that the integration between the systems works.

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

> **i Note**
>
> This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Integration Suite tenant. It may happen, however, that in the SAP S/4HANA Cloud tenant the access to such functionality is only partially implemented. Additionally, it may also happen that the tax authority servers do not provide all services that are described in this document. Please refer to SAP S/4HANA Cloud documentation and to the relevant tax authority information, respectively.

For the sake of simplicity in this guide, we mention SAP back-end systems when something refers to both SAP ERP or SAP S/4HANA.

3 Prerequisites

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

You have set up your tenant as follows:

- If you have subscribed to Process Integration, perform all the initial setup steps described in Initial Setup of SAP Cloud Integration in Cloud Foundry Environment.
- If you have subscribed to Integration Suite, perform all the initial setup steps described in Initial Setup.

  > **i Note**
  >
  > SAP Document and Reporting Compliance requires the *Cloud Integration capability*. You need to activate this capability in the step *Provisioning the Capabilities*.

- 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 Setup of Secure Connection

You establish a trustworthy SSL connection to set up a connection between the SAP S/4HANA Cloud tenant and the SAP Integration Suite. For more information, see Connecting a Customer System to Cloud Integration.

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

You use *Maintain Client Certificates* app 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 S/4HANA Cloud tenant.

For more information, see Operating and Monitoring Cloud Integration.

> **i Note**
>
> If you encounter any issues in the information provided in the SAP Integration Suite 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.

3.2 Retrieve and Save Public Certificates

You perform this action in the SAP S/4HANA Cloud tenant 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 11] and Configure Integration Flows [page 12].

Context

Find and save the public certificates from your SAP Integration Suite 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. 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 <tenant> corresponds to the dynamic part and is unique for each subaccount and <data center> corresponds to the data center you are using.
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 Configuration Steps in SAP Integration Suite

Required steps in SAP Integration Suite.

4.1 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

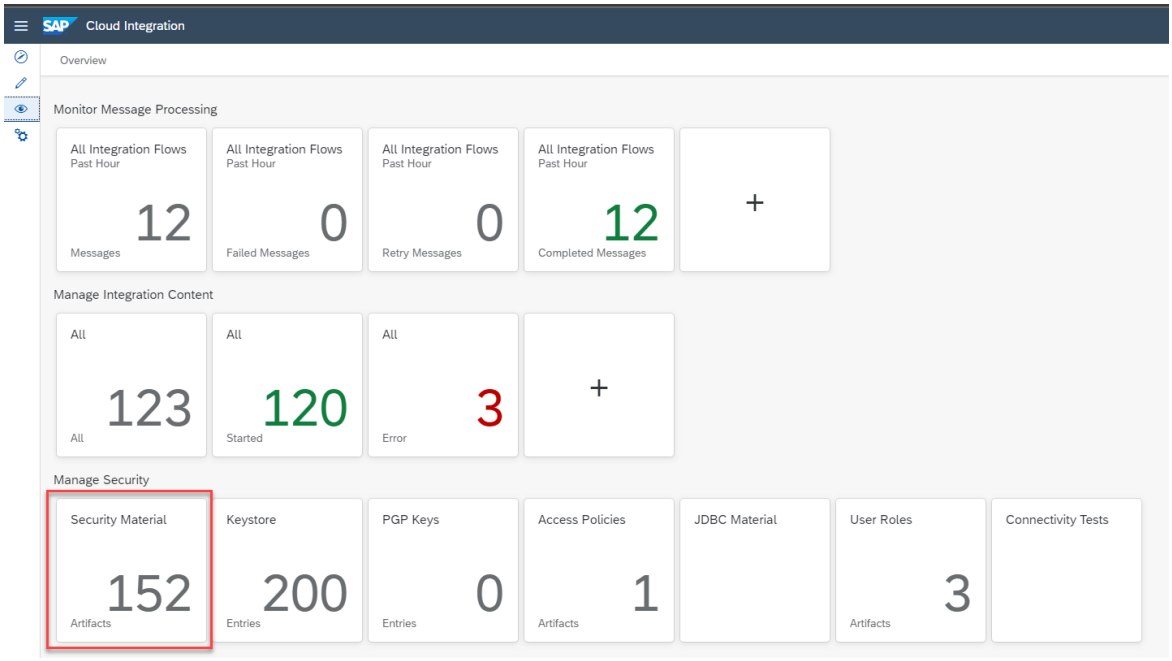
4.2 Deploy Credentials to Tenants

4.2.1 Basic Authentication

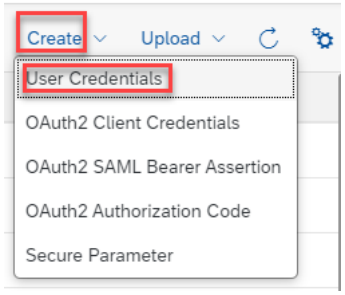
Procedure

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

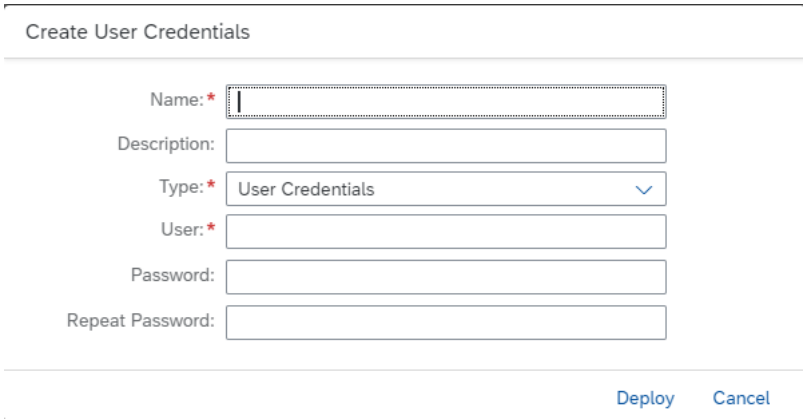
a. In your browser, go to the *Overview* tab and choose *Security Material*.



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>

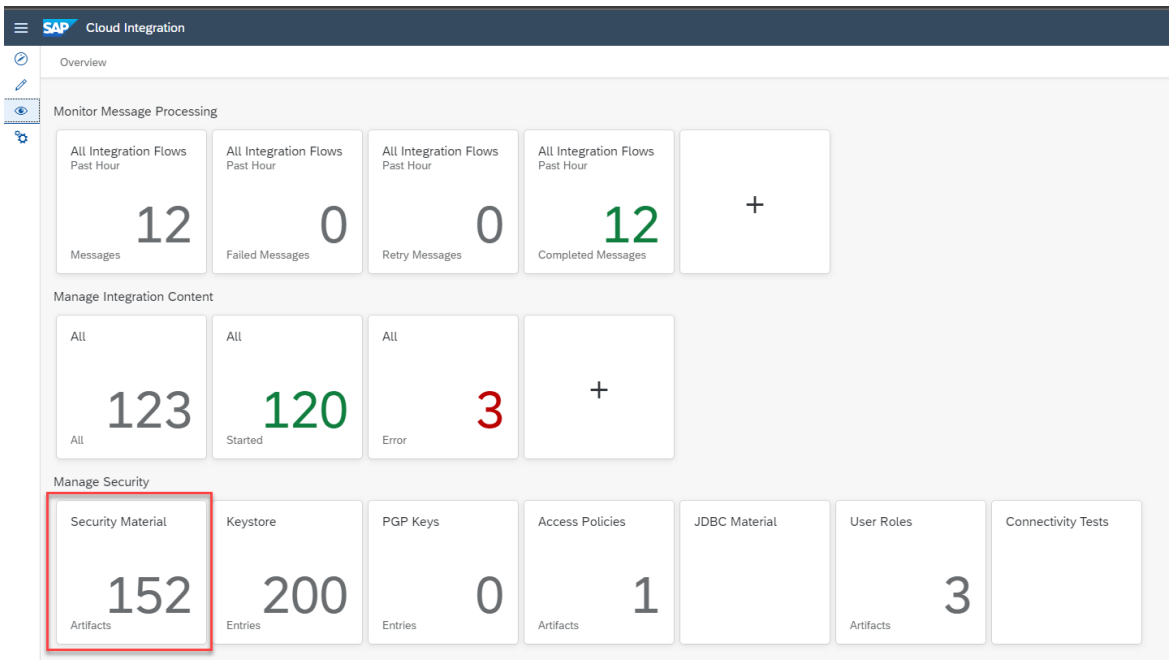
> **i Note**
>
> Your <**Tenant User ID**> and your <**Tenant Password**> has to be replaced with the value of your SAP Integration Suite tenant's User ID and Password respectively.
>
> Your <**Tenant User ID**> should have **CredentialsEdit** and **SecurityMaterialEdit** role templates assigned to it. For creating a new role collection with the above mentioned role templates, please refer Configuring User Access to the Application.
>
> 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

4.2.2 OAuth2 Client Credentials Authentication

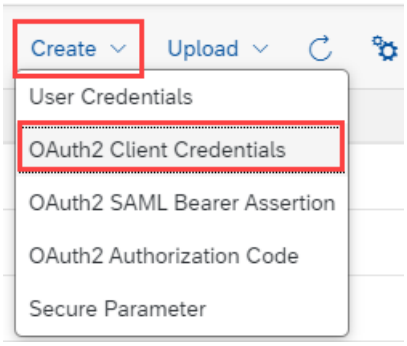
Procedure

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

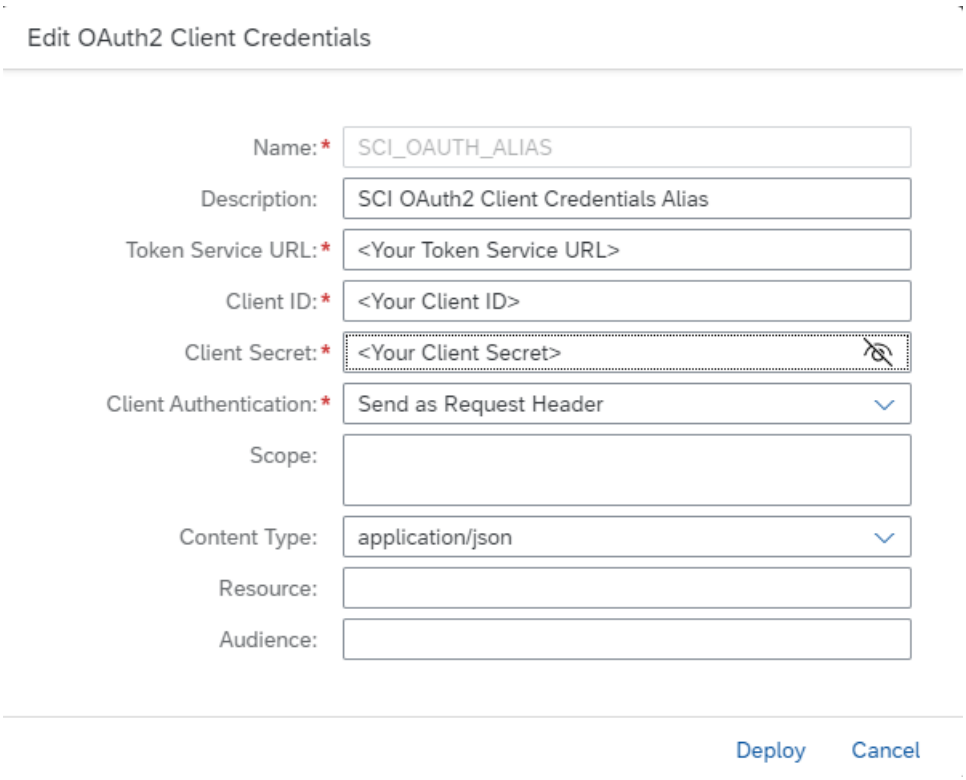
a. In your browser, go to the *Overview* tab and choose *Security Material*.



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 <**Client Secret**> has to be replaced with the values *clientid*, *clientsecret*, and *tokenurl* from your Service key respectively.

> Your <**Client ID**> should have *CredentialsEdit* and *SecurityMaterialEdit* role templates assigned to it. For creating a new Service Key with the above mentioned role templates, please refer Creating OAuth Client Credentials for Cloud Foundry Environment | SAP Help Portal.

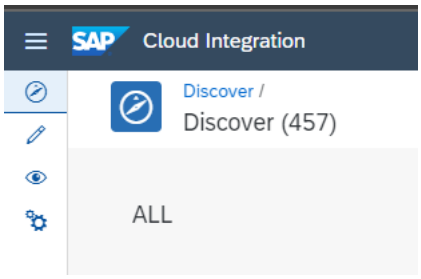
4.3 Copy Integration Flows

Context

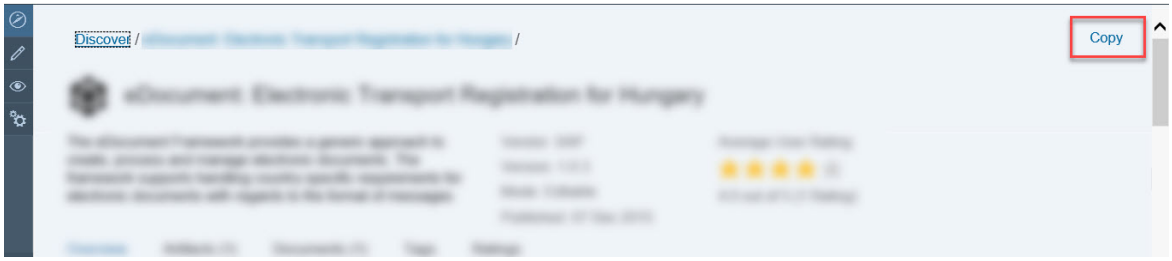
Copy all integration flows in the package *SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia* to the target tenant as follows:

Procedure

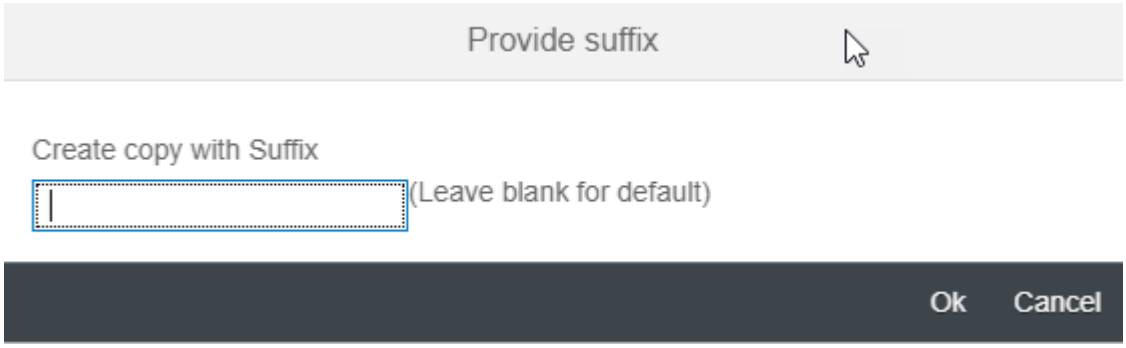
1. In your browser, go to the WebUI of the tenant (URL: <Tenant URL>/itspaces/#shell/catalog).
2. Choose *Discover* > *All*.



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*.



4.4 Configure Integration Flows

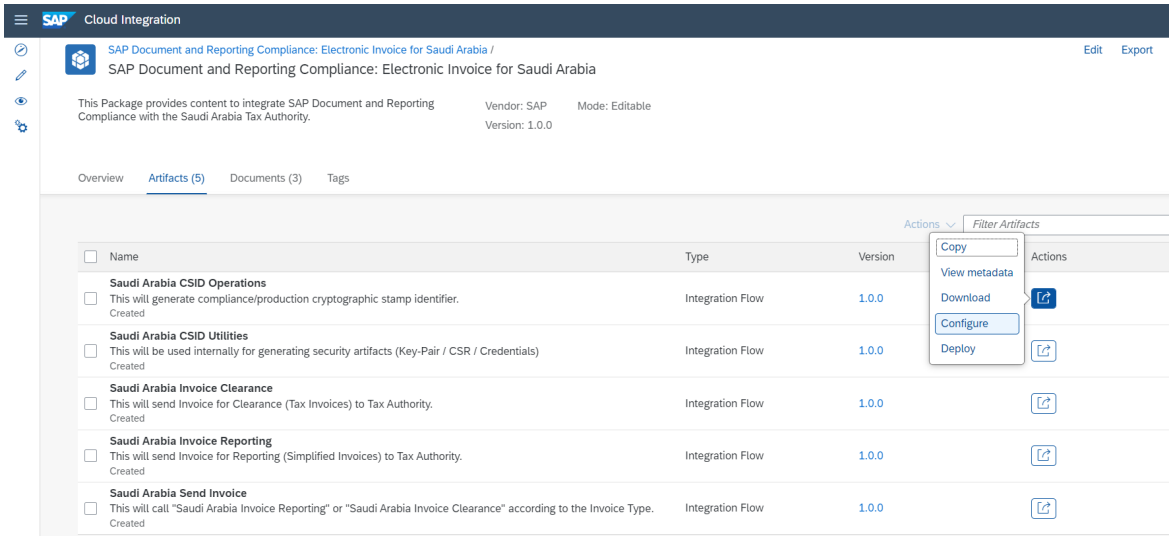
Context

You configure the package that you've copied as described in Copy Integration Flows [page 11].

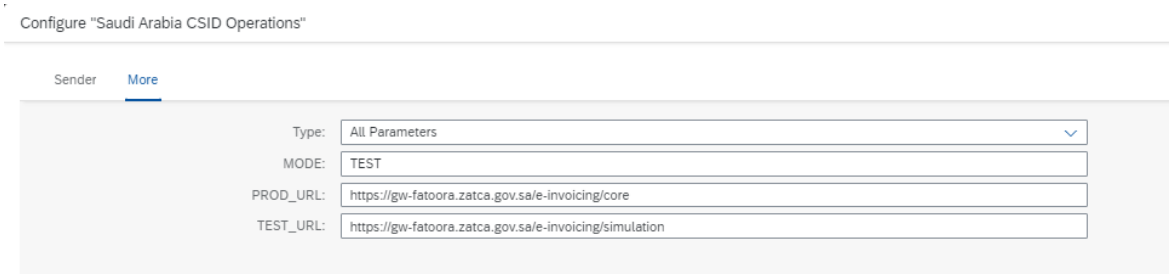
Procedure

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://<subdomainName>.it-cpi<xxx>.cfapps.<datacenter>.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`

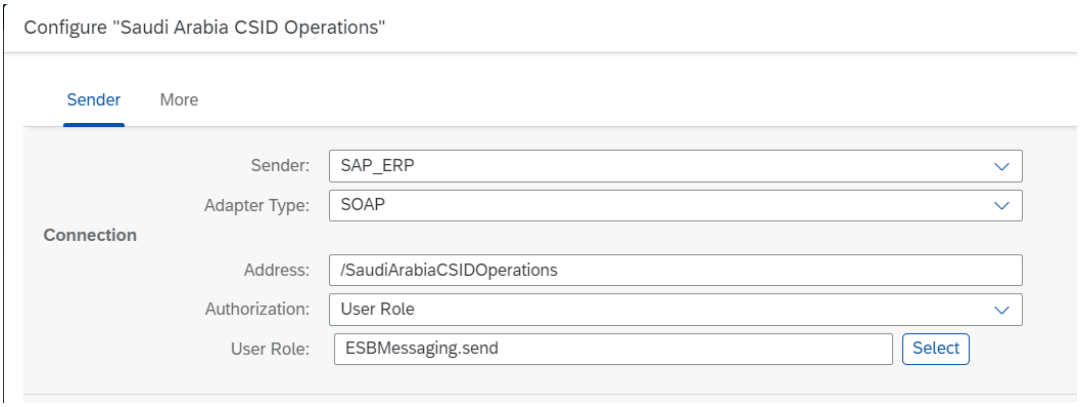
> **i Note**
>
> For test systems, you can use the Mode as `TEST` and for production systems, you can use the Mode as `PROD`.
>
> For Basic Authentication, use `SCI_CREDENTIAL_ALIAS` as credential name and for OAuth2 Client Credentials Authentication, use `SCI_OAUTH_ALIAS` as credential name.

7. Choose *Configure* > *Sender* tab.

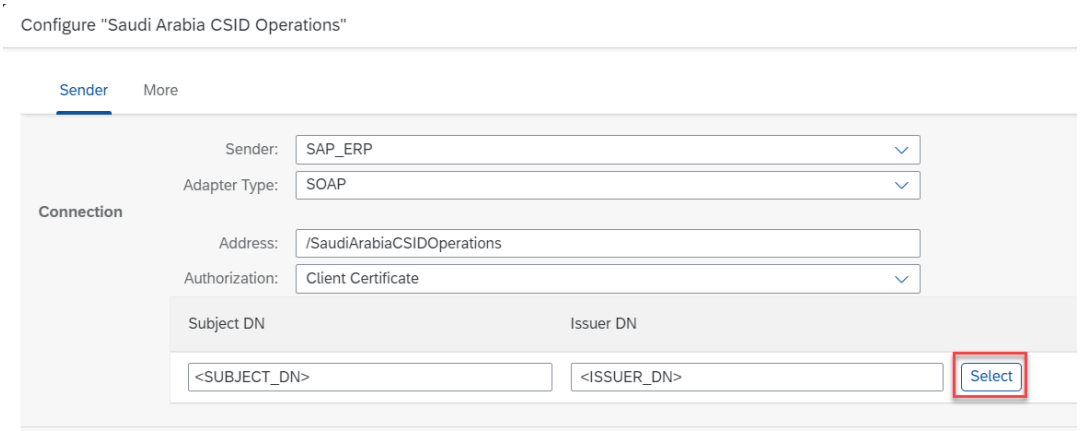
   - Use the `Address` parameter to set up the integration package address. Normally you don't have to change this field. In case you change the field, make sure to use the same address when configuring the logical ports in the next chapter.
   - Use the `Authorization` parameter to configure the authorization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

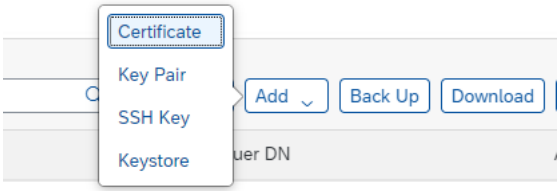
> **Note**
>
> Depending on the version of your tenant, after pressing these buttons, a warning message can appear. You can ignore these messages by choosing *Close*.

4.5 Retrieve and Save Server Certificate Chain of Tax Authority

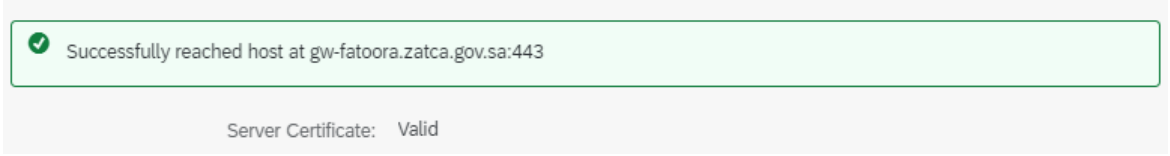
You can find and save the Server Certificate Chain from your Tax Authority

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.



5 Configuration Steps for SAP S/4HANA Cloud

The following sections tell you the necessary configuration you do in SAP S/4HANA Cloud.

5.1 Configuring Communication System

Create a communication system that represents your SAP Integration Suite tenant.

Prerequisites

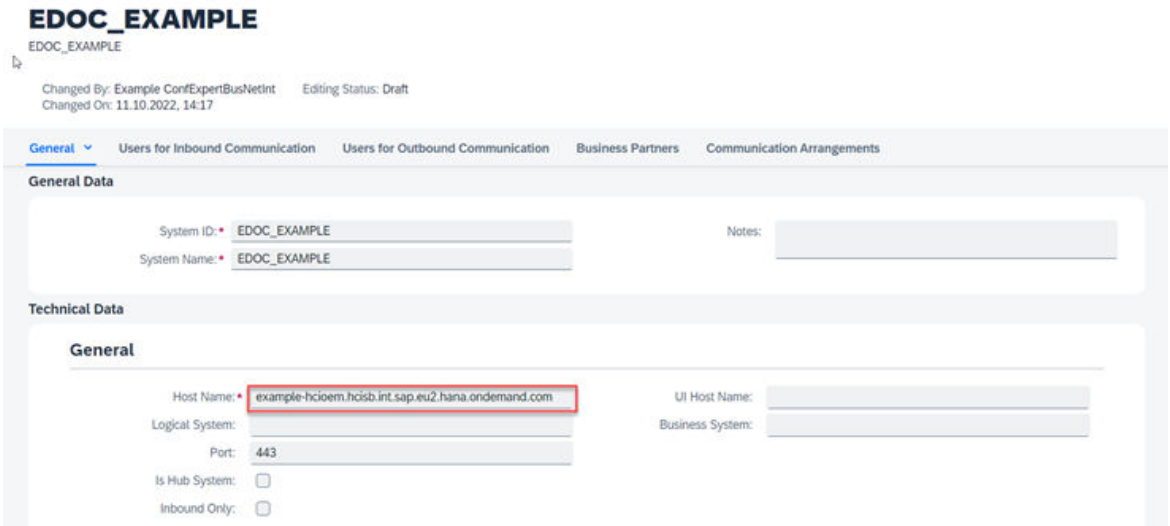
1. Live SAP Integration Suite test or productive tenant must be available.
2. Communication management setups are not transportable and must be explicitly maintained in quality and production systems.
3. The SAP S/4HANA Cloud user, who is following this guide, must be assigned to a business role that contains the business catalog `SAP_BCR_CORE_COM` (Communication Management) for accessing communication management apps.

Procedure

1. Login to your S/4HANA Cloud tenant with the Cloud User.
2. Find and launch the app *Communication Systems.*

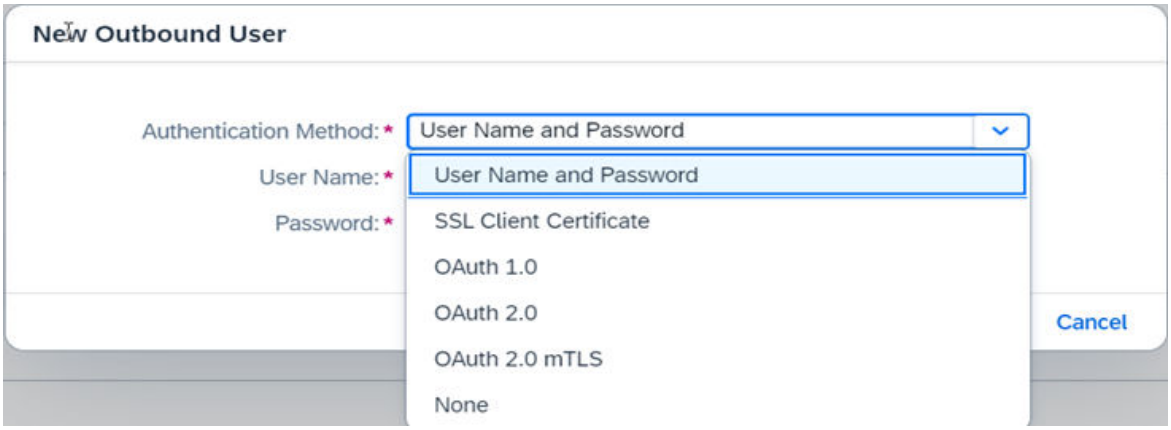
3. Choose *New*, and in the pop-up window, enter the *System ID* and *System Name* of your communication system. Naming convention of *System ID* is `EDOC_<name of SAP Cloud Integration tenant>`. For example, if the tenant host name is `example-tmn.avt.eu1.hana.ondemand.com`, then System ID is `EDOC_EXAMPLE`.

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



6. Scroll down, and choose + next to *User for Outbound Communication*.

7. In the new pop-up window, select the appropriate authentication method to connect to your SAP Integration Suite tenant, as described in the Implementation Guide.



- For the authentication method *User Name and Password*, enter the user name and password of your SAP Integration Suite 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.*

> **i Note**
>
> If you want to create your own Client Certificate, please refer https://help.sap.com/docs/SAP_S4HANA_CLOUD/55a7cb346519450cb9e6d21c1ecd6ec1/cb18de0f63b648d1a44bfe9bec1a4415.html?locale=en-US.

8. Choose *Save*.

5.2 Configuring Communication Arrangement

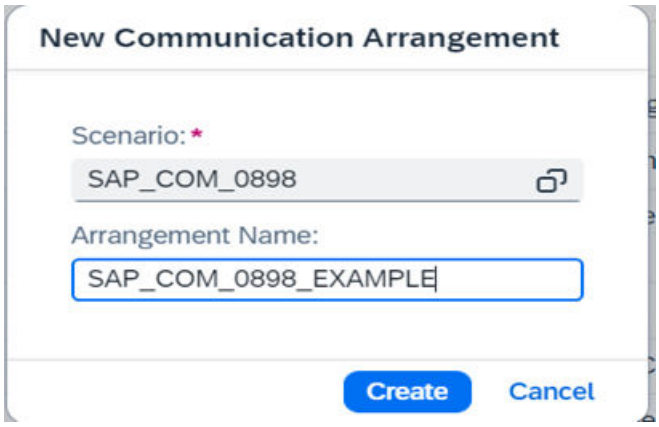
Configuration steps for SAP S/4HANA Cloud Communication Arrangement.

Procedure

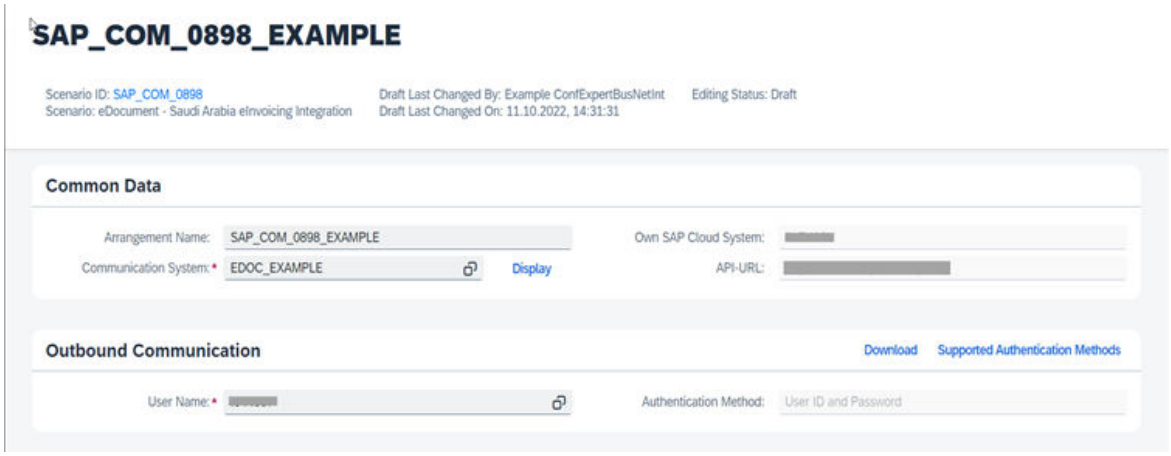
1. Login to your S/4HANA Cloud tenant with the Cloud User.
2. Find and launch the app *Communication Arrangements*.

3. Choose *New*. In the new pop-up window, enter the *Scenario* as `SAP_COM_0898` (which is the one designated for communication with the tax authority via SAP Integration Suite package) and an *Arrangement Name*. For *Arrangement Name* it is recommended to choose a name like `SAP_COM_0898_<name of SAP Integration Suite tenant>`.

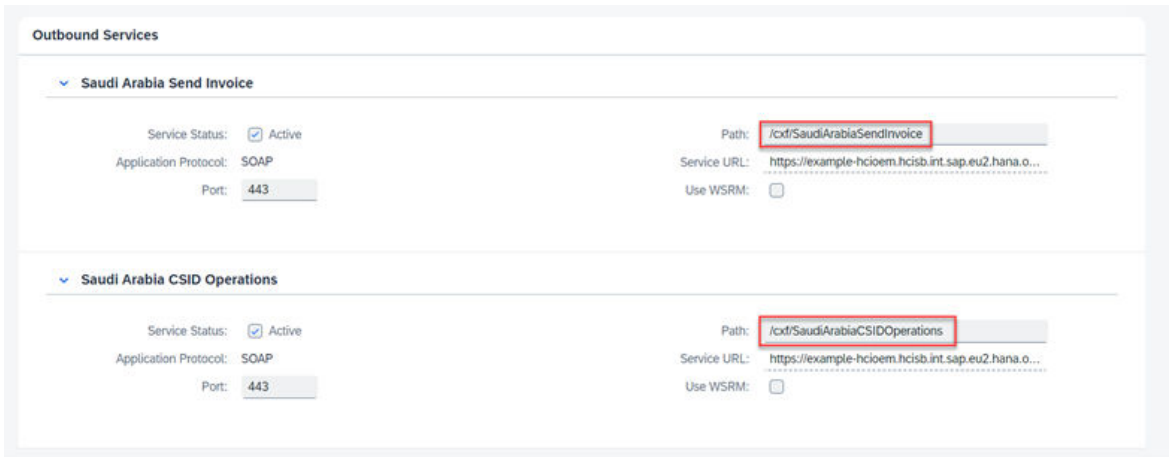
For example, `SAP_COM_0898_EXAMPLE` for tenant host name beginning with `example-tmn.avt.eu1.hana.ondemand.com`.



4. Choose *Create*.
5. In the new window, choose the communication system (for example, `EDOC_EXAMPLE`) and Outbound Communication created in the previous step.



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



7. Choose *Save*.

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