



Integration Guide | PUBLIC
2023-11-14

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

Content

1	Disclaimer.	3
2	Introduction.	4
3	Prerequisites	5
4	Connectivity Steps.	6
4.1	Setup of Secure Connection.	6
	Retrieve and Save Public Certificates.	7
	Upload the Certificates.	8
	Authenticate Integration Flows.	8
5	Configuration Steps in SAP Integration Suite.	10
5.1	General Information.	10
5.2	Deploy Credentials to Tenants.	10
	Basic Authentication.	10
	OAuth2 Client Credentials Authentication.	12
5.3	Copy Integration Flows.	14
5.4	Configure Integration Flows.	15
5.5	Create Logical Ports in SOAMANAGER.	18
5.6	Retrieve and Save Server Certificate Chain of Tax Authority.	23
6	Test the Integration.	25

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 Integration Suite to establish the communication with external systems and transfer to them the electronic documents you have created using the [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 Integration Suite tenant so that the integration between the systems works.

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

i Note

Although the service name SAP Integration Suite is used in the guide title and throughout the guide, this guide also applies to SAP Cloud Integration running in the Cloud Foundry environment. If you were onboarded before July 2020, the service you use is SAP Cloud Integration. The initial setup steps for the two services are different, while the integration flow settings and configuration steps in your back-end system are the same. See the Set Up Your Tenants section for their respective initial setup steps.

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 back-end systems 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 the relevant SAP back-end systems 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.

1. You have installed in the test and productive systems all necessary SAP Notes for the Document and Reporting Compliance Solution.
2. 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**.

3. 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 \(zatca.gov.sa\)](#) ➡

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 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 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. 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, 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 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](#).

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 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 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.

4.1.2 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 Integration Suite.

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.

4.1.3 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 certificate. 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 Integration Suite

The following sections tell you the necessary configuration you do in SAP Integration Suite.

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

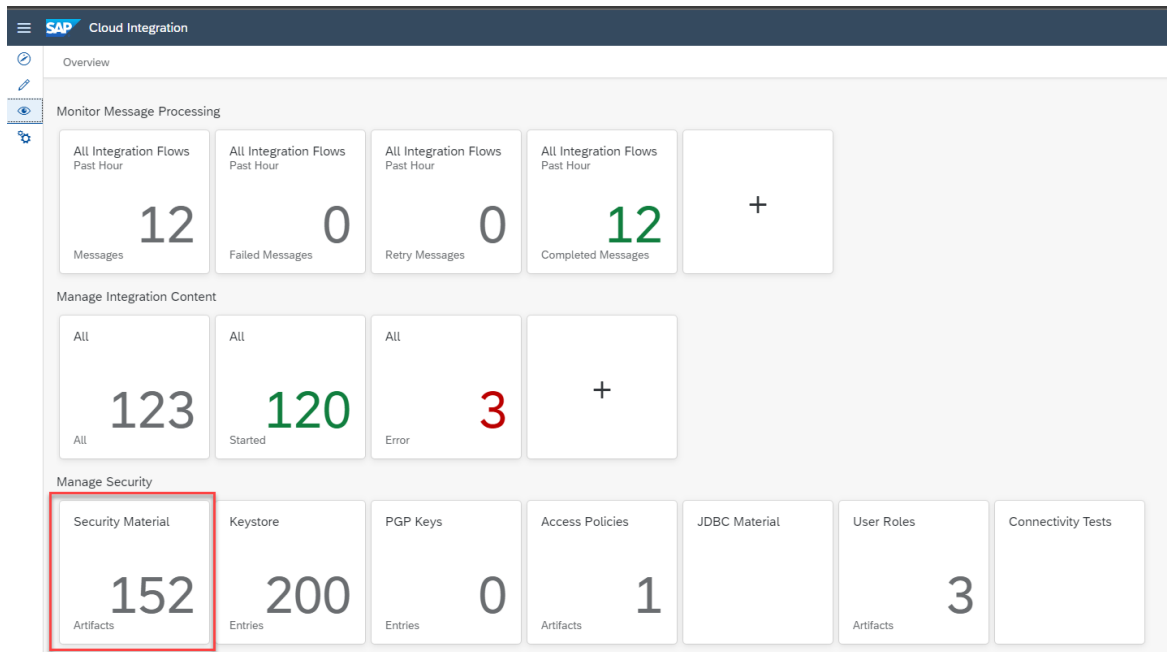
5.2 Deploy Credentials to Tenants

5.2.1 Basic Authentication

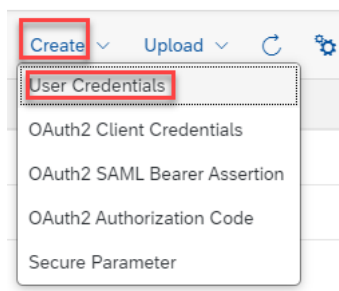
Procedure

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

- 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.

Create User Credentials

Name: *

Description:

Type: *

User: *

Password:

Repeat Password:

[Deploy](#) [Cancel](#)

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 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:

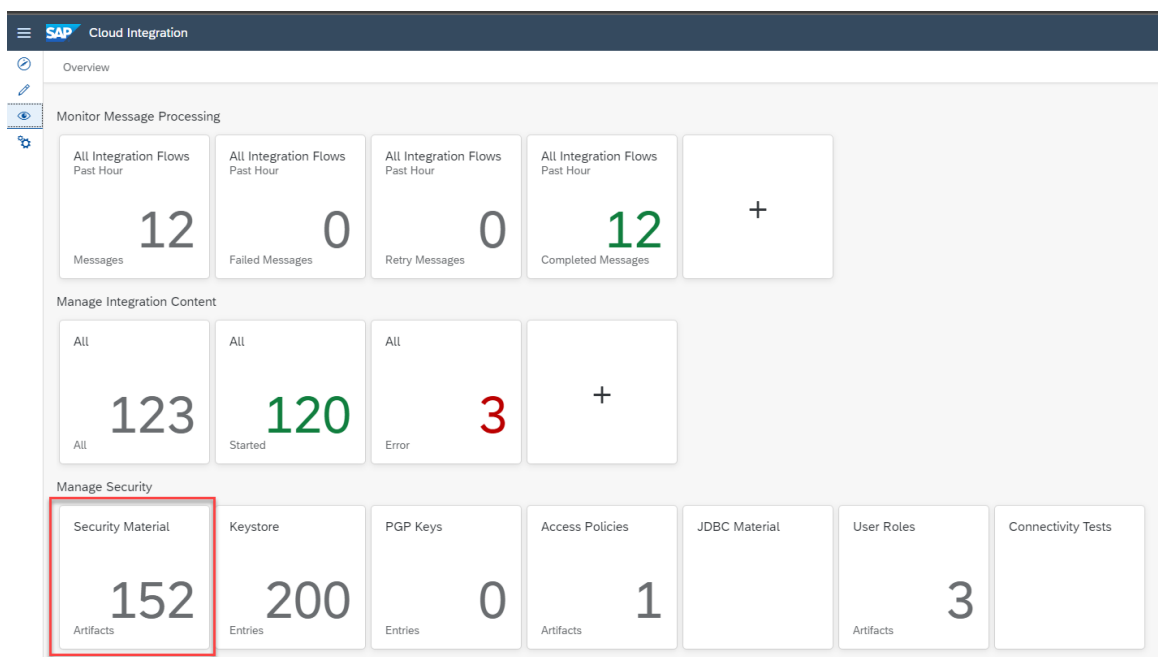
- [Security Content | SAP Help Portal](#)
- [Overview | Security Content | SAP Business Accelerator Hub](#)

5.2.2 OAuth2 Client Credentials Authentication

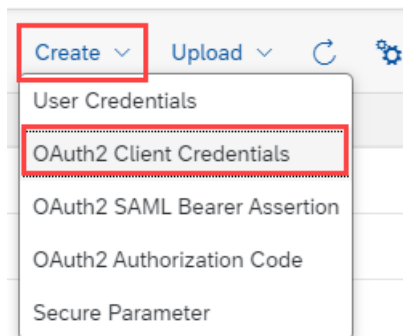
Procedure

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

- 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.

Edit OAuth2 Client Credentials

Name: *	<input type="text" value="SCI_OAUTH_ALIAS"/>
Description:	<input type="text" value="SCI OAuth2 Client Credentials Alias"/>
Token Service URL: *	<input type="text" value="<Your Token Service URL>"/>
Client ID: *	<input type="text" value="<Your Client ID>"/>
Client Secret: *	<input type="password" value="<Your Client Secret>"/>
Client Authentication: *	<input type="text" value="Send as Request Header"/>
Scope:	<input type="text"/>
Content Type:	<input type="text" value="application/json"/>
Resource:	<input type="text"/>
Audience:	<input type="text"/>

[Deploy](#) [Cancel](#)

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](#).

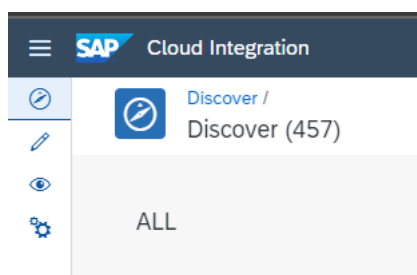
5.3 Copy Integration Flows

Context

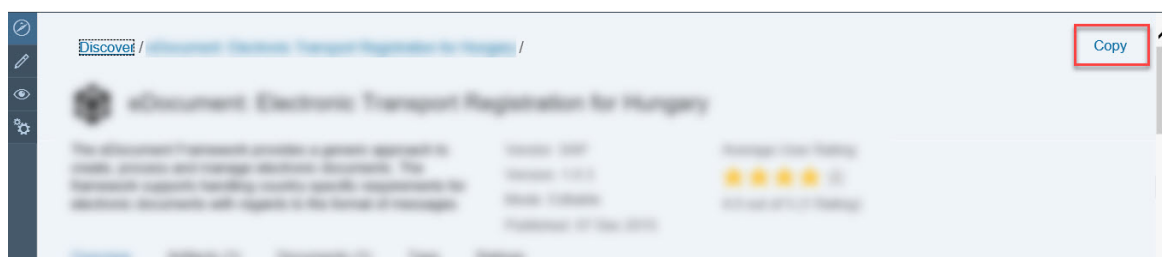
Copy all integration flows in the package [SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia](#) to the target tenant as follows:

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**.

Provide suffix

Create copy with Suffix

(Leave blank for default)

Ok

Cancel

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.

SAP Cloud Integration

SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia /

SAP Document and Reporting Compliance: Electronic Invoice for Saudi Arabia

This Package provides content to integrate SAP Document and Reporting Compliance with the Saudi Arabia Tax Authority. Vendor: SAP Mode: Editable Version: 1.0.0

Overview **Artifacts (5)** Documents (3) Tags

Name	Type	Version	Actions
<input type="checkbox"/> Saudi Arabia CSID Operations This will generate compliance/production cryptographic stamp identifier. Created	Integration Flow	1.0.0	Copy View metadata Download Configure Deploy
<input type="checkbox"/> Saudi Arabia CSID Utilities This will be used internally for generating security artifacts (Key-Pair / CSR / Credentials) Created	Integration Flow	1.0.0	
<input type="checkbox"/> Saudi Arabia Invoice Clearance This will send Invoice for Clearance (Tax Invoices) to Tax Authority. Created	Integration Flow	1.0.0	
<input type="checkbox"/> Saudi Arabia Invoice Reporting This will send Invoice for Reporting (Simplified Invoices) to Tax Authority. Created	Integration Flow	1.0.0	
<input type="checkbox"/> Saudi Arabia Send Invoice This will call "Saudi Arabia Invoice Reporting" or "Saudi Arabia Invoice Clearance" according to the Invoice Type. Created	Integration Flow	1.0.0	

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

Configure "Saudi Arabia CSID Operations"

Sender **More**

Type: All Parameters

MODE: TEST

PROD_URL: https://gw-fatoora.zatca.gov.sa/e-invoicing/core

TEST_URL: https://gw-fatoora.zatca.gov.sa/e-invoicing/simulation

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

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.

Configure "Saudi Arabia CSID Operations"

Sender More

Connection

Sender: SAP_ERP

Adapter Type: SOAP

Address: /SaudiArabiaCSIDOperations

Authorization: User Role

User Role: ESBMessaging.send **Select**

- 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.

Configure "Saudi Arabia CSID Operations"

Sender More

Connection

Sender: SAP_ERP

Adapter Type: SOAP

Address: /SaudiArabiaCSIDOperations

Authorization: Client Certificate

Subject DN: <SUBJECT_DN>

Issuer DN: <ISSUER_DN> **Select**

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

Required step for configuring the Integration Package for electronic documents and SAP Integration Suite.

Context

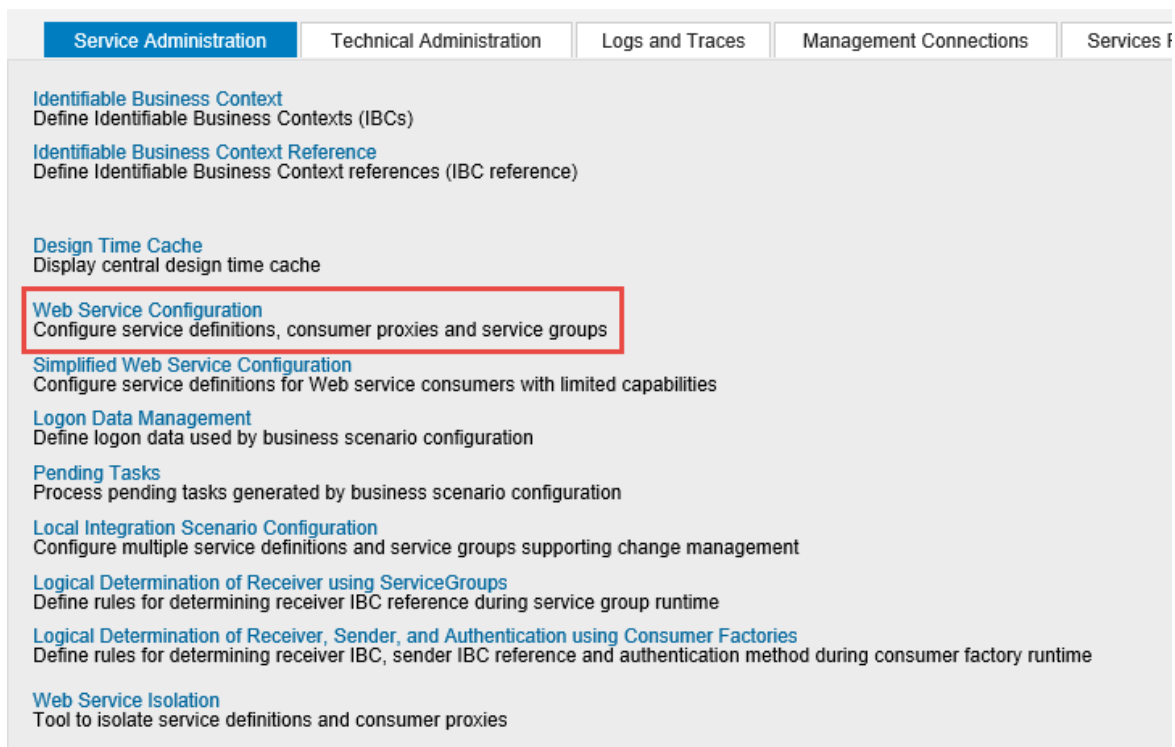
You configure proxies that are needed to connect to the SAP Integration Suite tenant via logical ports. In test SAP back-end systems, the logical ports are configured to connect to the test tenant. In productive SAP back-end systems, the logical ports are configured to connect to the productive SAP Integration Suite 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](#).



- 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.

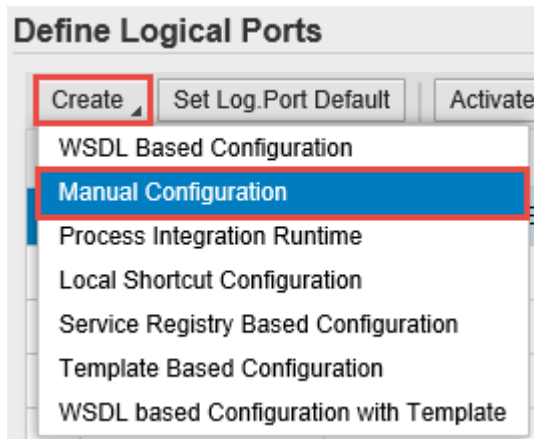
Logical Port details for CSID Operations proxy:

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

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 back-end system and SAP Integration Suite.

- If you use the basic authentication for *User Name*, enter the value for the **clientid** and for *Password*, enter the value for **clientsecret**. You've created these values for your service instance in SAP Integration Suite. See [Creating Service Instances](#).

1 Logical Port Name 2 Consumer Security 3 HTTPSettings 4 SOAP Protocol 5 Identifiable Business Context 6 Operation Settings

Back Next Finish Cancel

Configuration of Consumer Settings without WSDL Document.

Authentication Level: Basic

Authentication Settings

☐ User ID / Password

☐ SAP Authentication Assertion Ticket

☒ X.509 SSL Client Certificate

X.509 SSL Client PSE

SSL Client PSE of transaction STRUST:

Enter the name of the PSE created in STRUST

- If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you've uploaded to STRUST. You must configure this certificate in SAP Integration Suite 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 [Client Certificate Authentication for Integration Flow Processing | SAP Help Portal](#).
6. On the *HTTP Settings* tab, make the following entries:

1 Logical Port Name 2 Consumer Security **3 HTTP Settings** 4 SOAP Protocol 5 Identifiable Business Context 6 Operation Settings

Back Next **Finish** Cancel

URL Access Path

☐ URL ☒ **URL components**

* Protocol: **HTTPS**

* Host:

Port: **443**

* Path:

Logon Language: **Language of User Context**

Proxy

Name of Proxy Host:

Port Number of Proxy Host:

User Name for Proxy Access:

Password of Proxy User:

Transport Binding

Make Local Call: **No Call in Local System**

* Transport Binding Type: **SOAP 1.1**

Maximum Wait for WS Consumer:

Optimized XML Transfer: **None**

Compress HTTP Message: **Inactive**

Compress Response: **True**

Port 443 is the standard port for the HTTPS protocol.

To find the Host, go to SAP Integration Suite Web UI and under Managed Integration Content, go to **Monitor** **All**. Use the search to find your integration flow as in the screenshot below:

Overview / Manage Integration Content

Integration Content (489) **Filter by Name or ID**

1 Go to Operations View

2 Enter the integration flow name as search term

Deployed On: Feb 11, 2021, 11:49:57
Deployed By:

ID:

Version: 1.0.3

Package:

Endpoints Status Details Artifact Details Log Configuration

3 Copy the host name from here (the part between https:// and /cxf/)

i 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.

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

The screenshot shows the 'SOAP Protocol' configuration tab, which is the fourth step in a six-step wizard. The steps are: 1. Logical Port Name, 2. Consumer Security, 3. HTTPSettings, 4. SOAP Protocol (active), 5. Identifiable Business Context, and 6. Operation Settings. Below the step indicators are buttons for 'Back', 'Next', 'Finish', and 'Cancel'. The 'Message ID (Synchronous)' section has a 'Message ID Protocol' dropdown menu set to 'Suppress ID Transfer'. The 'Metering of Service Calls' section has 'Data transfer scope' set to 'Enhanced Data Transfer' and 'Transfer protocol' set to 'Transfer via SOAP header'. The 'Message Attachment Handling' section has 'Process Attachments' set to 'No'.

- 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 Integration Suite service and execute a connection test. If there is a successful connection, you receive an error with HTTP return code 500.

- 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

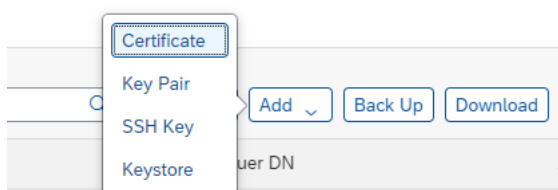
5.6 Retrieve and Save Server Certificate Chain of Tax Authority

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

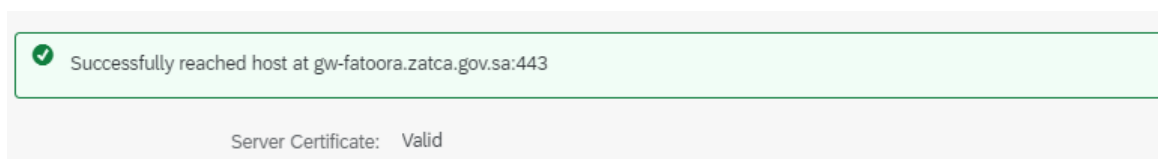
Procedure

- 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 Integration Suite.

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 Integration Suite.
 - a. If the status is green or yellow, but not *Created*, the communication with SAP Integration Suite was triggered and was probably successful. You can double-check if the message went through on the SAP Integration Suite 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.

© 2023 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company. The information contained herein may be changed without prior notice.

Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

Please see <https://www.sap.com/about/legal/trademark.html> for additional trademark information and notices.