



Integration Guide | PUBLIC
2023-01-05

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

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
 - Add Credentials for Authenticating Signature Device. 7
 - Add Credentials for Authenticating Tenant at Tax Authority. 9
 - 4.3 Copy Integration Flows. 12
 - 4.4 Configuring Integration Flows. 13
 - 4.5 Retrieve and Save Server Certificate Chain of Tax Authority. 15
- 5 Configuration Steps for SAP S/4HANA Cloud. 17**
 - 5.1 Configuring Communication System. 17
 - 5.2 Configuring Communication Arrangement. 19

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 Egypt 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.

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*.

3.1 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 iFlow 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

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

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

4.1 General Information

The package *SAP Document and Reporting Compliance: Electronic Invoice for Egypt* contains the following iFlows:

iFlows for Document and Reporting Compliance for Egypt

iFlow Name in WebUI	Project Name/Artifact Name
Egypt Submit Document	com.sap.GS.Egypt.SubmitDocument
Egypt Document Cancellation or Rejection	com.sap.GS.Egypt.CancelReject
Egypt Get Recent Documents	com.sap.GS.Egypt.GetRecentDocuments
Egypt Get Document Details	com.sap.GS.Egypt.GetDocDetails
Egypt Get Document PDF	com.sap.GS.Egypt.GetDocPDF
Egypt Decline Document Cancellation or Rejection	com.sap.GS.Egypt.Decline

4.2 Deploy Credentials to Tenants

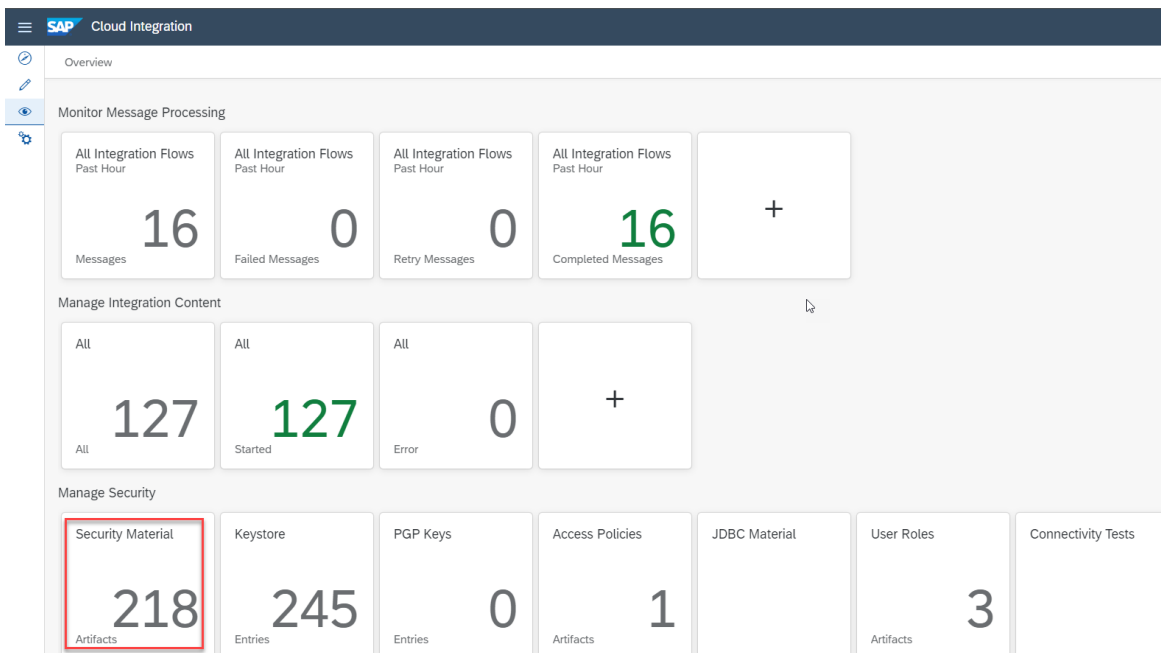
To establish a connection between the SAP Integration Suite and tax authority servers, you must obtain several security materials, and then add these to the SAP Integration Suite tenant.

4.2.1 Add Credentials for Authenticating Signature Device

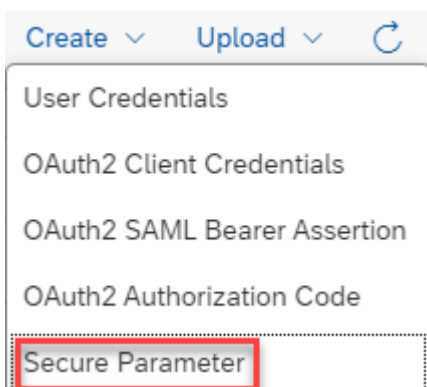
SAP Integration Suite uses a *Secure Parameter* to authenticate the communication with Signing device/server. For the Egypt eInvoice scenario, you must include credentials that are recognized by the eSeal provider like eTrust. A *Secure Parameter* is used to specific if a technical user is registered with a signing device/server.

Deploy the Name and Secure Parameter to your SAP Integration Suite tenant.

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



2. Choose *Create* on the right corner and choose *Secure Parameter*.



3. Enter the name, description and secure parameter, and deploy them.

Create Secure Parameter

Name: *

Description:

Secure Parameter: *

Repeat Secure Parameter: *

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

You need to add Secure Parameter as follows:

- Name: The required format for the *Name* is "edoc_egypt_<type>_<taxpayerid>" (For example, edoc_egypt_secretkey_123456789).

i Note

Here the <type> can be:

- pin
- thumbprint
- secretkey
- signingServer

The *Name* is case sensitive.

- Description: 'Egypt Security Material Type'
- Secure Parameter: The value of the pin, thumb print, secret key and signing server should be entered for the *Secure Parameter*.

i Note

For the Signing Server security material the Secure Parameter is in the form of a URL. The required format of the URL is "<protocol>://<IP Address>:Port" (For example, Http://1.2.3.4:9999).

- Repeat Secure Parameter: Re-enter the value of the *Secure Parameter*.

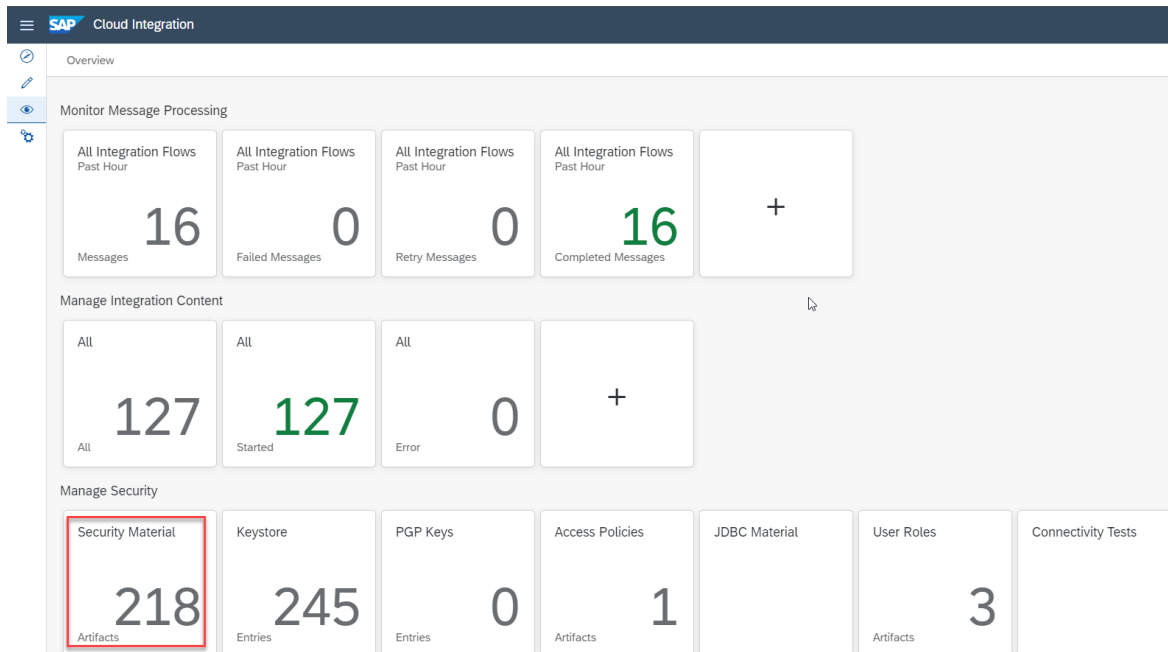
4.2.2 Add Credentials for Authenticating Tenant at Tax Authority

SAP Integration Suite uses a *OAuth2 Credential* to authenticate the communication with tax authority's system. For the Egypt eInvoice scenario, you must include credentials that are recognized by the tax authority (Egyptian Tax Authority, ETA). A *OAuth2 Credential* is specific to a technical user registered in the Online Invoicing System of the tax authority.

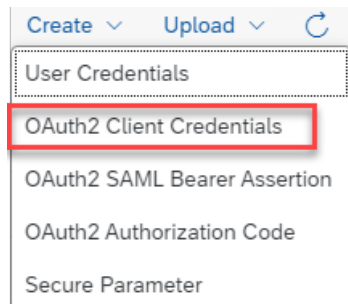
You need to add and deploy your *OAuth2 credentials* as Client Credentials in the Security Material section of your SAP Integration Suite tenant.

The user needs to add and deploy their credentials in the Test and Production systems based on the Tenants.

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



2. Choose *Create* on the right corner and choose *Secure Parameter*.



3. Enter the name, description and secure parameter, and deploy them.

Create OAuth2 Credentials

Name: *	<input type="text"/>
Grant Type:	Client Credentials <input type="button" value="v"/>
Description:	<input type="text"/>
Token Service URL: *	<input type="text"/>
Client ID: *	<input type="text"/>
Client Secret: *	<input type="text"/>
Client Authentication:	Send as Request Header <input type="button" value="v"/>
<input checked="" type="checkbox"/> Include Scope:	
Scope:	InvoicingAPI <input type="text"/>
Content Type:	application/x-www-form-urlencoded <input type="button" value="v"/>

You need to add the Client Credentials as follows:

- Name: The required format for the *Name* is "edoc_egypt_eta_<mode>_<taxpayerid>" (For example, edoc_egypt_eta_prod_123456789).

i Note

Here the <mode> can be:

- test
- prod

The *Name* is case sensitive.

- Token Service URL: To get the access token there are two types of service URLs based on the mode:
 - Test: <https://id.preprod.eta.gov.eg/connect/token>
 - Prod: <https://id.eta.gov.eg/connect/token>
- Client ID: Enter the *Client ID* received after registration with ETA.
- Client Secret: Enter the *Client Secret* received after registration with ETA.
- Scope: Enter the value "InvoicingAPI" for the *Scope*.

i Note

Select the *Include Scope* check box in order to enter the *Scope* and *Content Type*.

- Content Type: Select the value "application/x-www-form-urlencoded" for the *Content Type*.

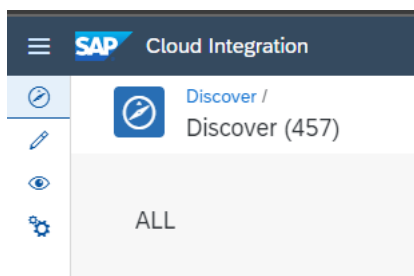
4.3 Copy Integration Flows

Context

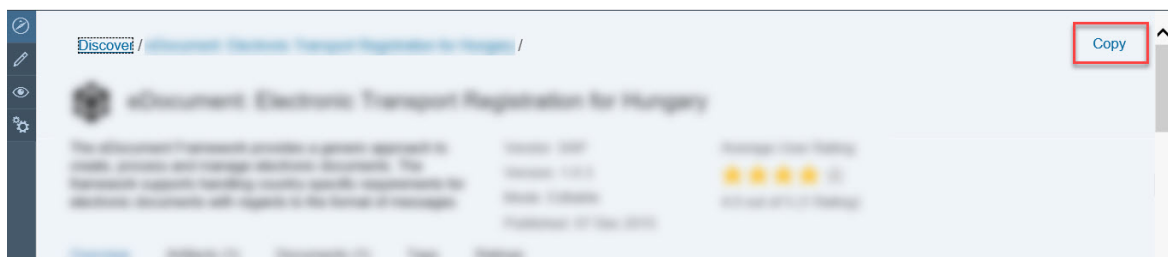
Copy all iFlows in the package *SAP Document and Reporting Compliance: Electronic Invoice for Egypt* to the target tenant as follows:

Procedure

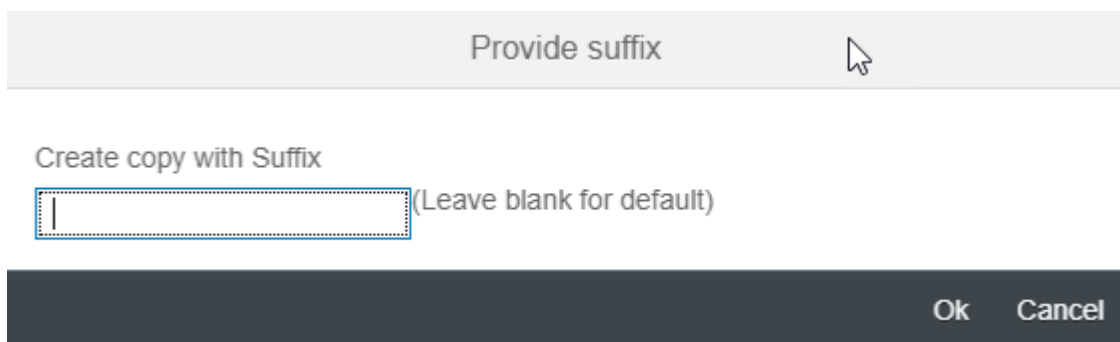
1. In your browser, go to the WebUI of the tenant (URL: <Tenant URL>/itspaces/#shell/catalog).
2. Choose **Discover** > **All**.



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



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



4.4 Configuring Integration Flows

Context

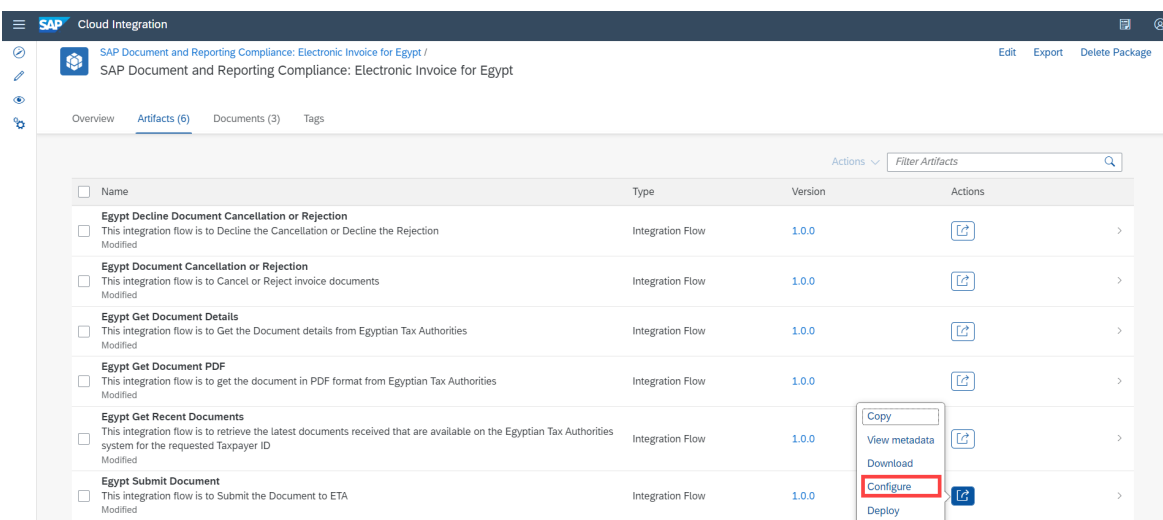
You configure the package that you've copied as described in [Copy Integration Flows](#).

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 Egypt](#) package.
3. Go to the [Artifacts](#) tab page.
4. There are six [Artifacts](#) in the integration package [SAP Document and Reporting Compliance: Electronic Invoice for Egypt](#):
 - Egypt Submit Document
 - Egypt Document Cancellation or Rejection
 - Egypt Get Recent Documents
 - Egypt Get Document Details
 - Egypt Get Document PDF
 - Egypt Decline Document Cancellation or Rejection

Take [Egypt Submit Document](#) as an example, similar steps should be done for the other iFlows:

5. Choose [Actions](#) [Configure](#) for the artifact you're configuring.



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

Configure "Egypt Submit Document"

Sender **More**

Type:	All Parameters
Language:	EN
Mode:	TEST
Receiver_Prod_URL:	https://api.invoicing.eta.gov.eg
Receiver_Test_URL:	https://api.preprod.invoicing.eta.gov.eg

Note

When you configure the *Mode* as "TEST" or "PROD" the "TEST" or "PROD" APIs will be triggered along with the "TEST" or "PROD" credentials.

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

Parameter Name	URL
RECEIVER_PROD_URL	https://api.invoicing.eta.gov.eg
RECEIVER_TEST_URL	https://api.preprod.invoicing.eta.gov.eg

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 "Egypt Submit Document"

[Sender](#) [More](#)

Connection

Sender: ERP

Adapter Type: SOAP

Address: /EgyptSubmitDocument

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 "Egypt Submit Document"

[Sender](#) [More](#)

Connection

Sender: ERP

Adapter Type: SOAP

Address: /EgyptSubmitDocument

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.

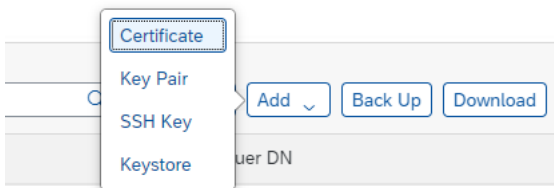
4.5 Retrieve and Save Server Certificate Chain of Tax Authority

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

Procedure

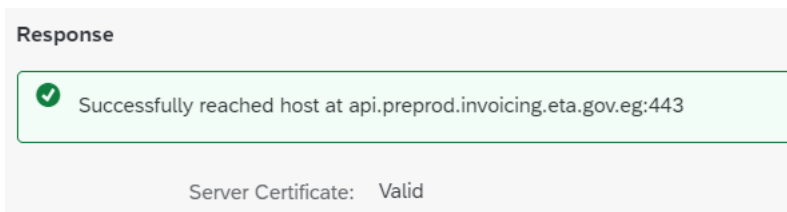
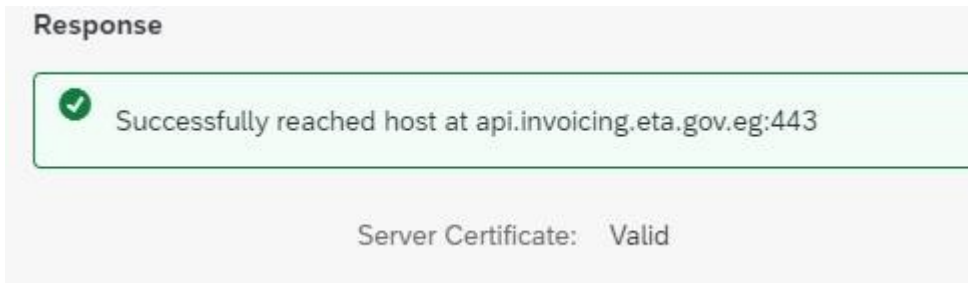
1. In your browser, navigate to the WebUI of the tenant (URL: <Tenant URL>/itspaces/shell/monitoring/).
2. Under [Manage Security](#), choose [Connectivity Tests](#).
3. Choose [TLS](#). Enter the following details:

- Host: There are two *Host* names based on the type of tenant:
 - PROD: `api.invoicing.eta.gov.eg`
 - TEST: `api.preprod.invoicing.eta.gov.eg`
 - 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*.



i Note
 You should add the TEST or PROD certificates based on the *Host* name entered in Step 3.

8. Repeat steps 3 and 4 after adding all the certificates.



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 Integration Suite tenant>`. For example, if the tenant host name is `example-tmn.avt.eu1.hana.ondemand.com`, then System ID is `EDOC_EXAMPLE`.

New Communication System

System ID: * EDOC_EXAMPLE
System Name: * EDOC_EXAMPLE

Create

Cancel

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>`.

EDOC_EXAMPLE
EDOC_EXAMPLE

Changed By: Example ConfExpertBusNetint Editing Status: Draft
Changed On: 11.10.2022, 14:17

General Users for Inbound Communication Users for Outbound Communication Business Partners Communication Arrangements

General Data

System ID: * EDOC_EXAMPLE Notes:
System Name: * EDOC_EXAMPLE

Technical Data

General

Host Name: * UI Host Name:
Logical System: Business System:
Port:
Is Hub System:
Inbound Only:

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

Users for Outbound Communication

Authentication Method	User Name / Certificate / Client ID

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_0857* (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_0857_<name of SAP Integration Suite tenant>*.

For example, `SAP_COM_0857_EXAMPLE` for tenant host name beginning with `example-tmn.avt.eu1.hana.ondemand.com`.

New Communication Arrangement

Scenario: *

SAP_COM_0857

Arrangement Name:

SAP_COM_0857_EXAMPLE

Create Cancel

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

SAP Communication Arrangements Search in: "Apps" EA

SAP_COM_0857_EXAMPLE

Scenario ID: SAP_COM_0857 Scenario: eDocument - Egypt electronic Invoice Integration Draft Last Changed By: Example Administrator Editing Status: Draft
Draft Last Changed On: 17.10.2022, 13:31:01

Common Data

Arrangement Name: SAP_COM_0857_EXAMPLE Own SAP Cloud System: OLEU10H
Communication System: [Select] New API URL: https://cx3-715-api-wdf.sap.com

Outbound Communication Download Supported Authentication Methods

User Name: [Select] Authentication Method: [Select]

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

Outbound Services

▼ eDocument Egypt: Submit Document

Service Status: Active
 Application Protocol: SOAP
 Port: 443

Path: /cxf/EgyptSubmitDocument
 Service URL::c...
 Use WSRM:

▼ eDocument Egypt: Get Document Details

Service Status: Active
 Application Protocol: SOAP
 Port: 443

Path: /cxf/EgyptGetDocDetails
 Service URL:c...
 Use WSRM:

▼ eDocument Egypt: Cancel and Reject

Service Status: Active
 Application Protocol: SOAP
 Port: 443

Path: /cxf/EgyptCancelReject
 Service URL:
 Use WSRM:

▼ eDocument Egypt: Decline Cancellation and Rejection

Service Status: Active
 Application Protocol: SOAP
 Port: 443

Path: /cxf/EgyptDecline
 Service URL:
 Use WSRM:

▼ eDocument Egypt: Get PDF

Service Status: Active
 Application Protocol: SOAP
 Port: 443

Path: /cxf/EgyptGetDocPDF
 Service URL:
 Use WSRM:

▼ eDocument Egypt: Get Recent Documents

Service Status: Active
 Application Protocol: SOAP
 Port: 443

Path: /cxf/EgyptGetRecentDocuments
 Service URL:
 Use WSRM:



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 a 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.

© 2022 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.