Integration Guide | PUBLIC
2024-01-18

Egypt Electronic Invoicing: Setting Up SAP Cloud Integration (SAP S/4HANA Cloud) - 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 Egypt is taken care of by SAP Cloud Integration. In order to get SAP Cloud Integration working, there are some required steps on both your SAP S/4HANA Cloud system and SAP Cloud Integration tenant.

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

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

3 Prerequisites

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

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 Cloud Integration. 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 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.

3.2 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.

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

To be able to deploy the security content you must be assigned the `AuthGroup.Administrator` role.

If you are a first-time user, you must first set up your users (members) and their authorizations in the SAP BTP cockpit.

3.3 Retrieve and Save Public Certificates

Prerequisites

If you do not find any integration flows in your tenant then refer to Copy Integration Flows [page 13] and Configuring Integration Flows [page 14].

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. 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 Cloud Integration

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

4.1 General Information

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

Egypt e-Invoicing Integration Flows

Integration Flow 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
Egypt Search Documents	com.sap.GS.Egypt.SearchDocuments
Egypt Trust Digital Signature Integration	com.sap.GS.Egypt.EgyptTrustDigitalSignatureIntegration

> **i Note**
>
> The *Egypt Get Recent Documents* integration flow is obsolete.

Document Notification Integration Flows

Integration Flow Name in WebUI	Project Name/Artifact Name
Egypt ERP Ping	com.sap.GS.Egypt.ERPPing
Egypt ERP Notification	com.sap.GS.Egypt.ERPNotifications

> **Note**
>
> The integration flows *Egypt ERP Ping* and *Egypt ERP Notification* are supported only for S/4HANA versions 2021 onwards.

4.2 Deploy Credentials to Tenants

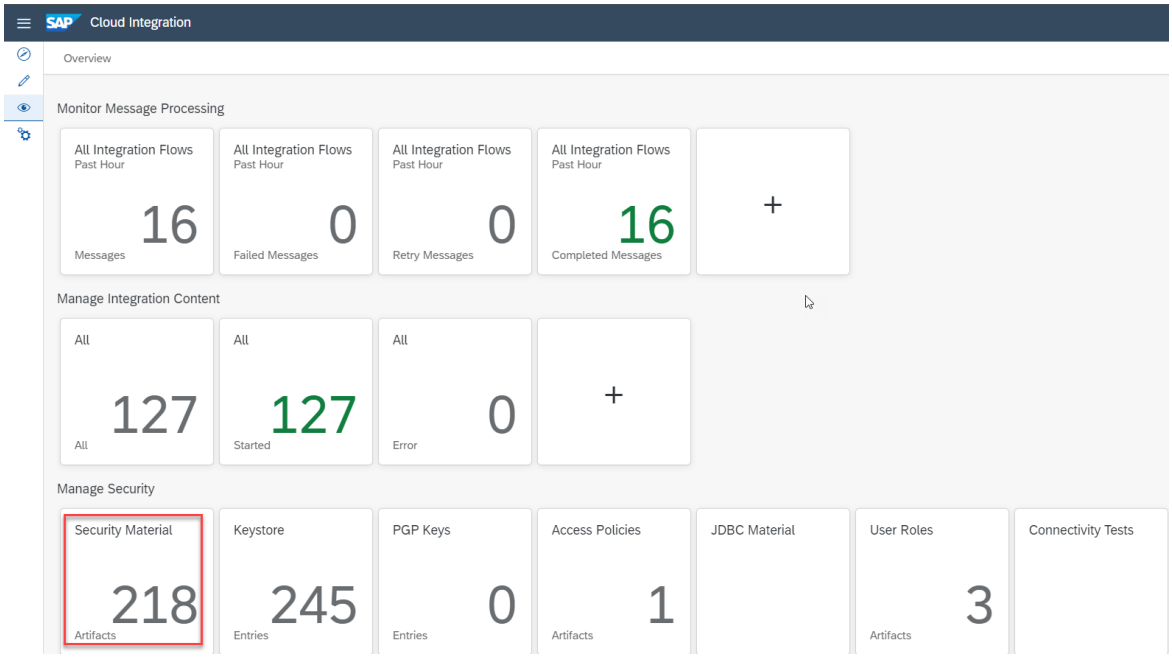
To establish a connection between the SAP Cloud Integration and tax authority servers, you must obtain several security materials, and then add these to the SAP Cloud Integration tenant.

4.2.1 Add Credentials for Authenticating Signature Device

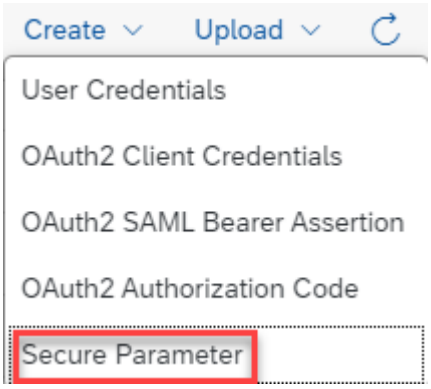
SAP Cloud Integration uses a *Secure Parameter* to authenticate the communication with Signing device/server. For the Egypt eInvoice scenario, you must include credentials that are recognized by the eSeal provider like eTrust. A *Secure Parameter* is used to specific if a technical user is registered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

If you use the Egypt Trust Signing Server then you can follow the steps in this section to deploy the Name and Secure Parameter to your SAP Cloud Integration 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.

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*.

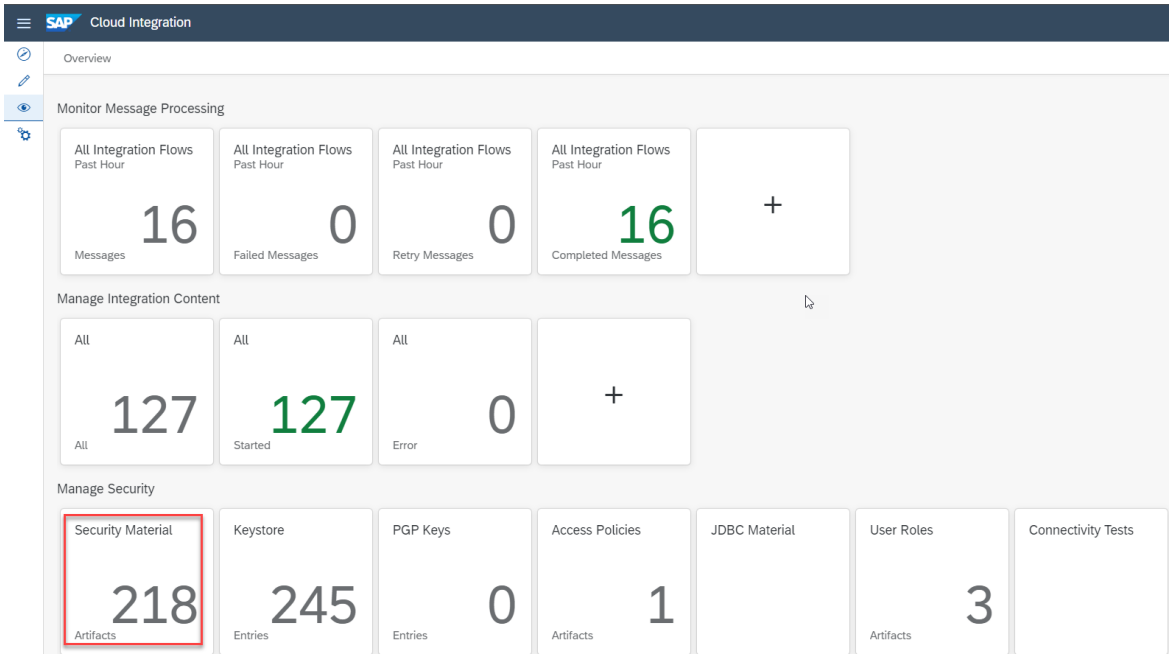
4.2.2 Add Credentials for Authenticating Tenant at Tax Authority

SAP Cloud Integration 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.

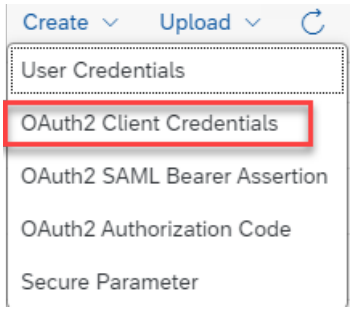
You need to add and deploy your *OAuth2 credentials* as Client Credentials in the Security Material section of your SAP Cloud Integration tenant.

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

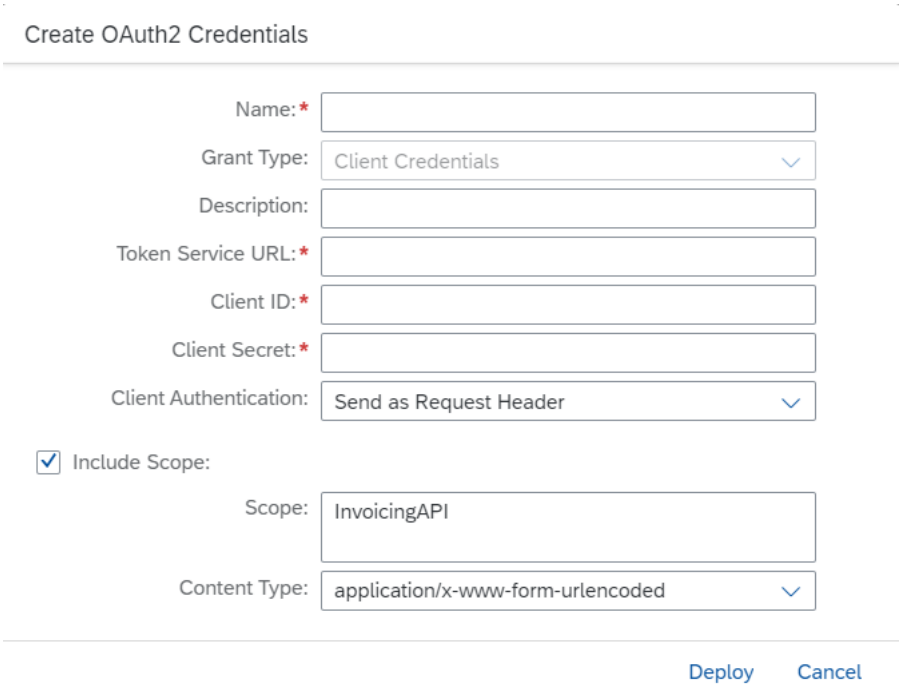
1. In your browser, go to the *Overview* tab and choose *Security Material*.



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



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



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*.

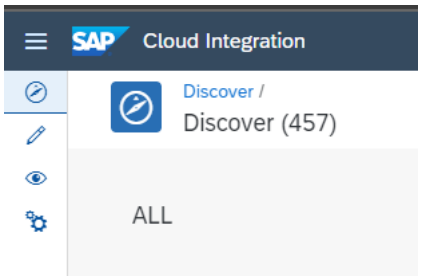
4.3 Copy Integration Flows

Context

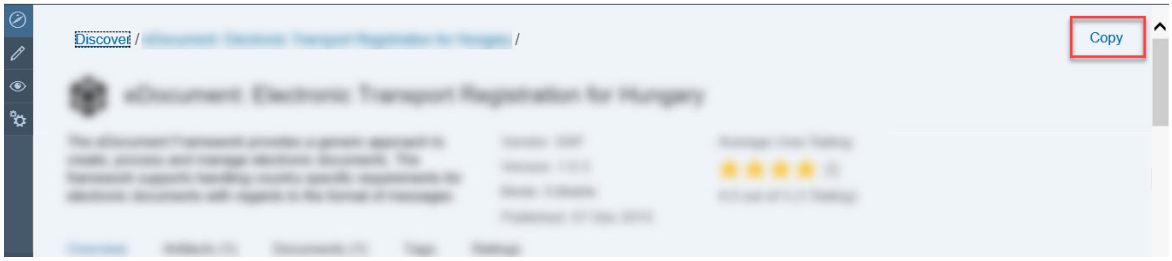
Copy all integration flows in the package *SAP Document and Reporting Compliance: Electronic Invoice for Egypt* to the target tenant as follows:

Procedure

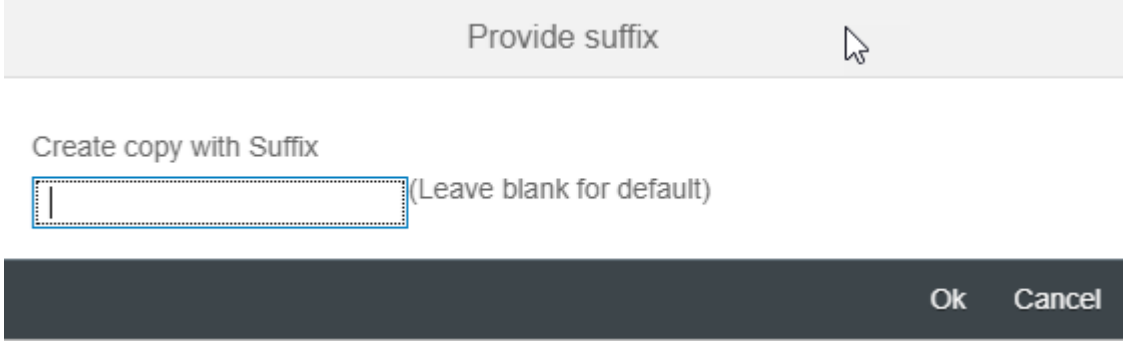
1. In your browser, go to the WebUI of the tenant (URL: <Tenant URL>/itspaces/#shell/catalog).
2. Choose *Discover* > *All*.



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 nine *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
   - Egypt Search Documents
   - Egypt Trust Digital Signature Integration
   - Egypt ERP Notification
   - Egypt ERP Ping

   > **i Note**
   >
   > The *Egypt Get Recent Documents* integration flow is obsolete.

   Please follow the steps in the below sections to configure your integration flows.

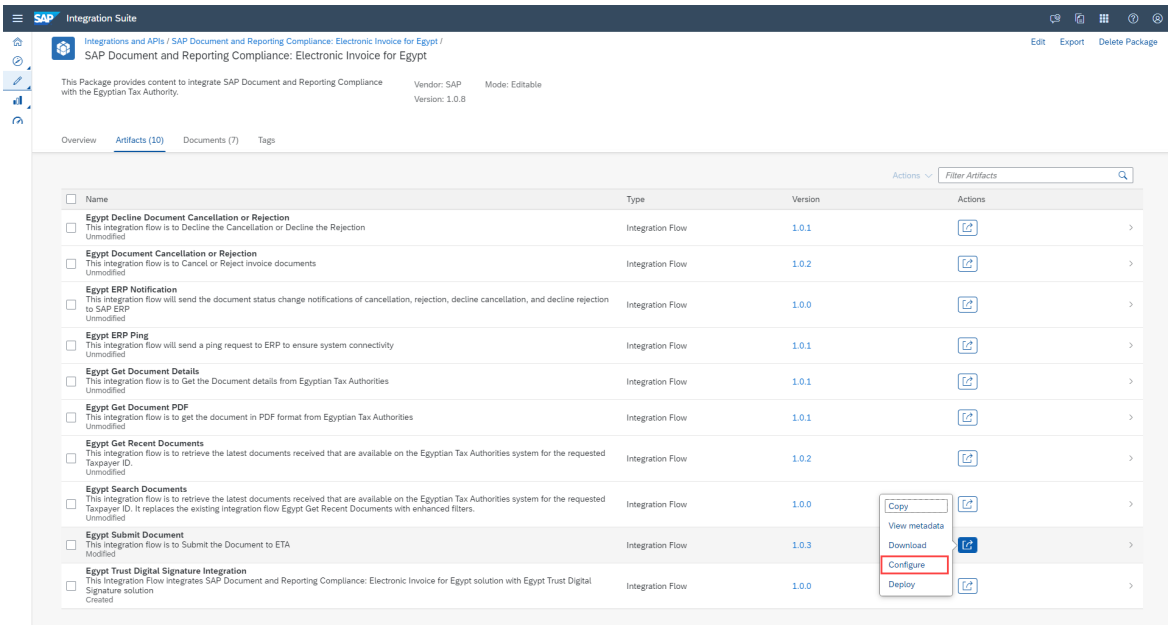
4.4.1 Configuring Egyptian Tax Authority's Integration Flows

Context

Take *Egypt Submit Document* as an example, similar steps should be done for the other integration flows.

Procedure

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



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

> ### Note
>
> `Signing_Server_Process_Address` parameter is only valid for *Egypt Submit Document* integration flow. For more information on what value you need to enter for this parameter, please refer to Integration with Signing Server [page 17].

> ### 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.

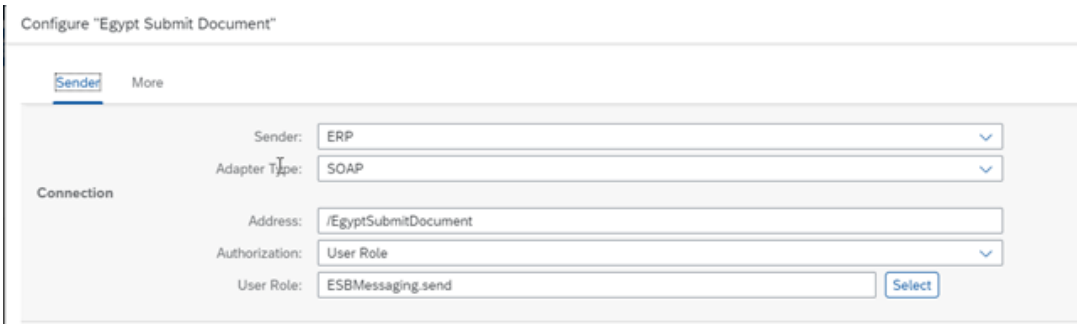
There are specific URLs you need to enter for different integration flows.

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

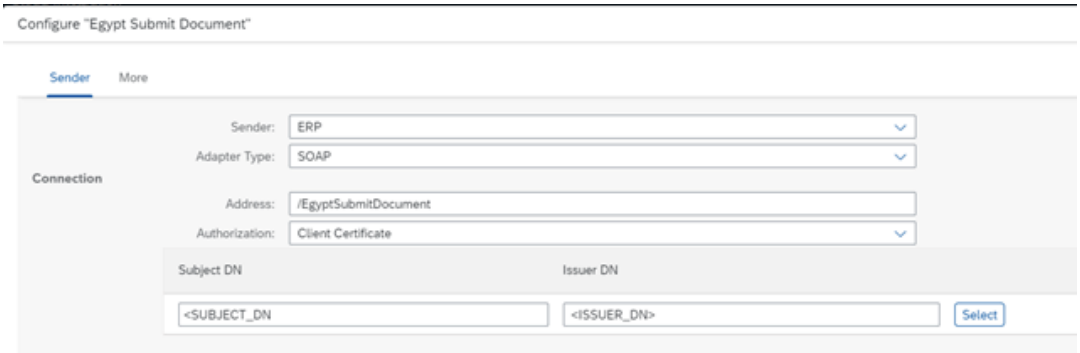
3. Choose *Configure* > *Sender* tab.
   - Use the `Address` parameter to set up the integration package address. Normally you don't have to change this field. In case you change the field, make sure to use the same address when configuring the logical ports in the next chapter.
   - Use the `Authorization`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

4. 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.

4.4.2 Integration with Signing Server

The standard package contains the *Egypt Trust Digital Signature Integration* integration flow by default to integrate the *Egypt Submit Document* integration flow with the Egypt Trust Digital Signature solution. You can create your own integration flow in the standard package based on the Signing Server you are using.

The *Egypt Submit Document* integration flow provides the externalized parameter `Signing_Server_Process_Address` to enter the address of customer developed integration flow, which is used to integrate with the preferred Digital Signature solution.

The *Egypt Submit Document* integration flow will send the JSON version of the electronic invoice to the customer developed integration flow via ProcessDirect receiver adaptor.

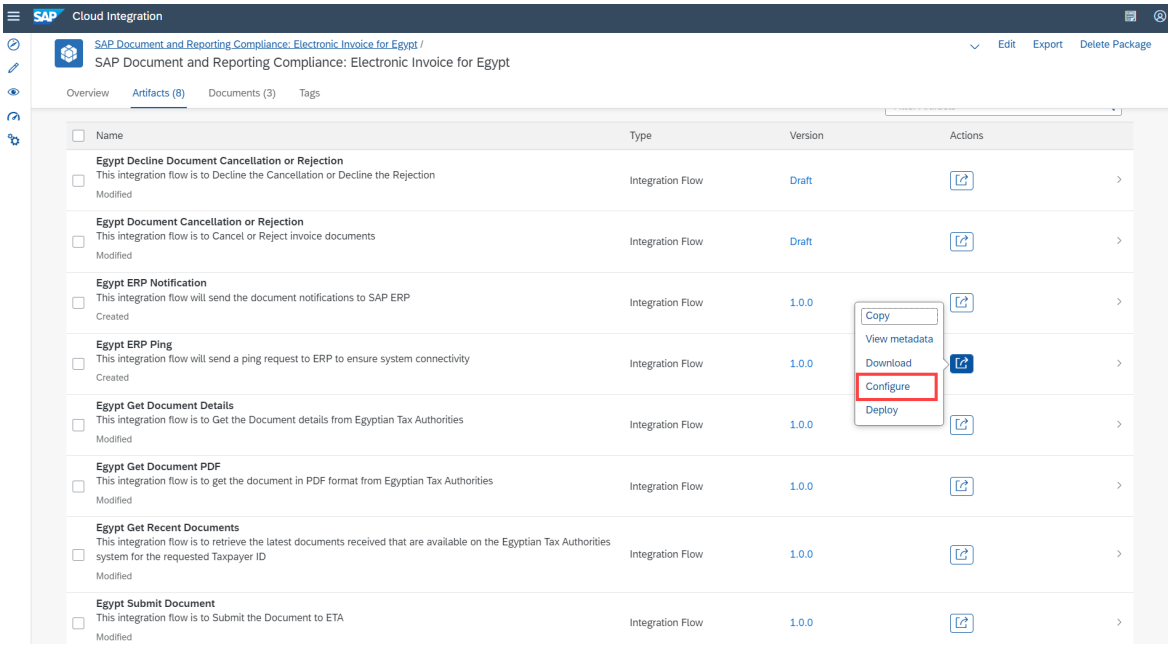
The customer developed integration flow is expected to receive the request from *Egypt Submit Document* via ProcessDirect sender adaptor and send back a response with the message body containing only the Digital Signature in Base64 format.

4.4.3 Configuring Egypt ERP Ping Integration Flow

Provides instructions for configuring integration flow for Egypt ERP Ping.

Procedure

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



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

> ### 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
ERP_PROD_URL	`http://<host>/sap/bc/srt/scs_ext/sap/erp_ping`
ERP_TEST_URL	`http://<host>/sap/bc/srt/scs_ext/sap/erp_ping`

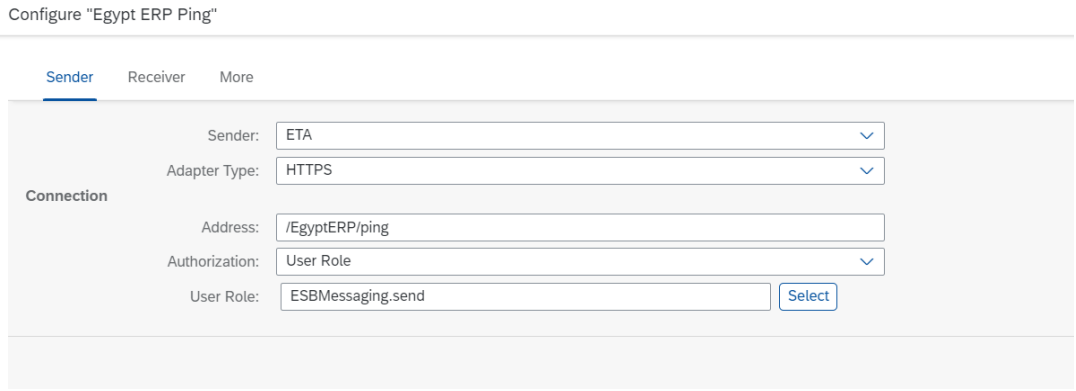
> ### Note
>
> If the target ERP system is not hosted publicly then you can expose the system via SAP Cloud Connector.

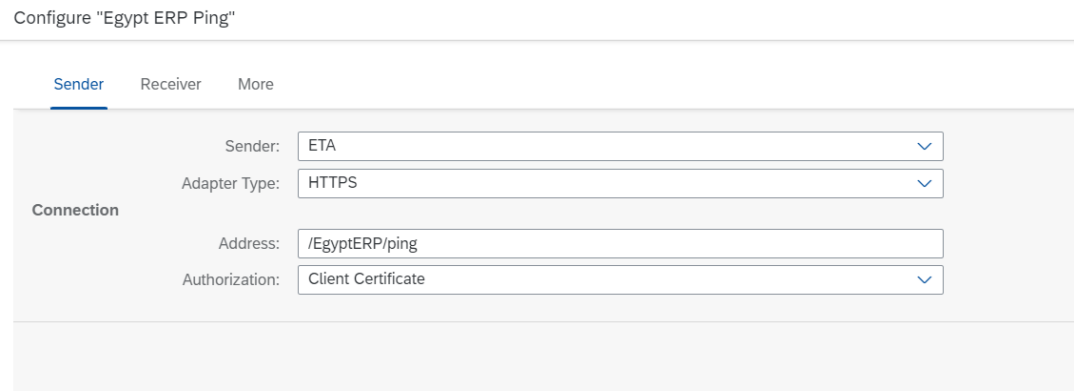
3. Choose *Configure* > *Sender* tab.

- 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.

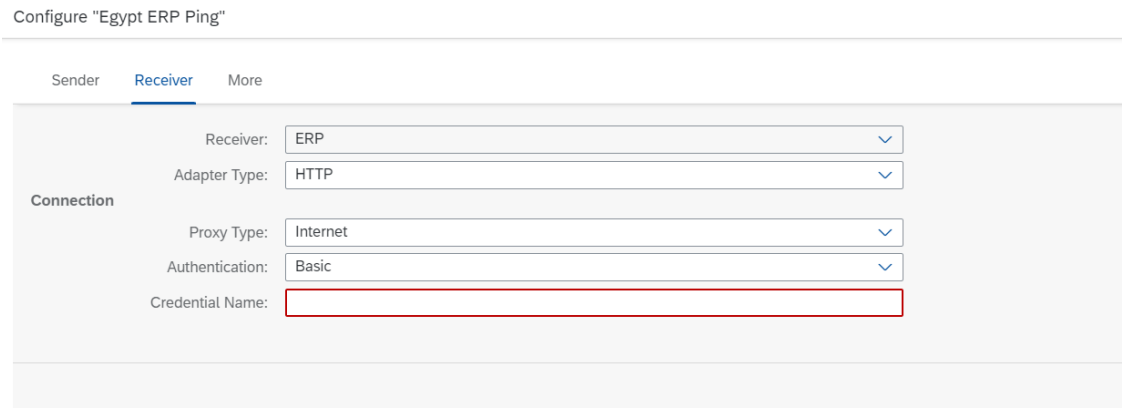
Value	Description
User Role	You want to use basic authentication (user/password).
Client Certificate	You want to use client certificate authentication.

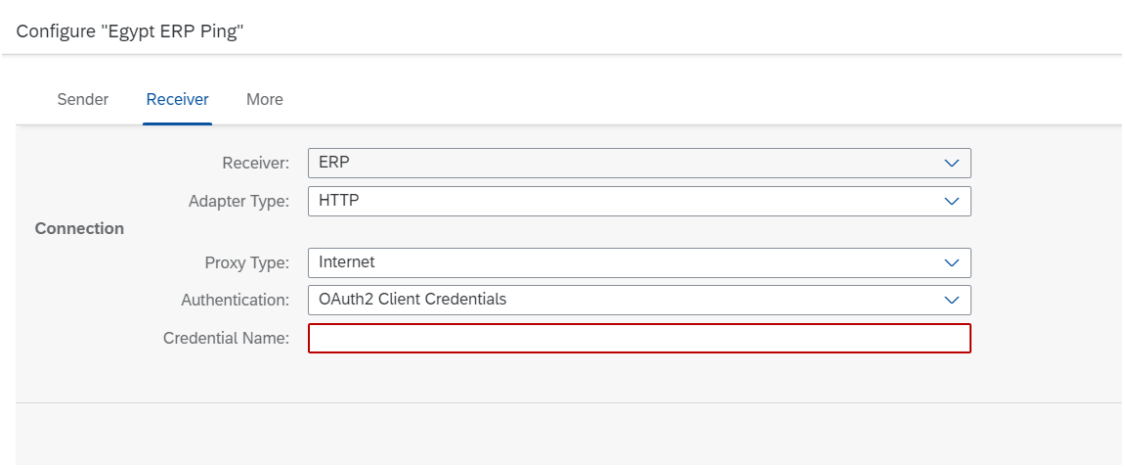
- Use the `User Role` parameter to configure the role based on which the inbound authorization is checked. Choose *Select* to get a list of all available roles.
  The role `ESBMessaging.send` is provided by default.

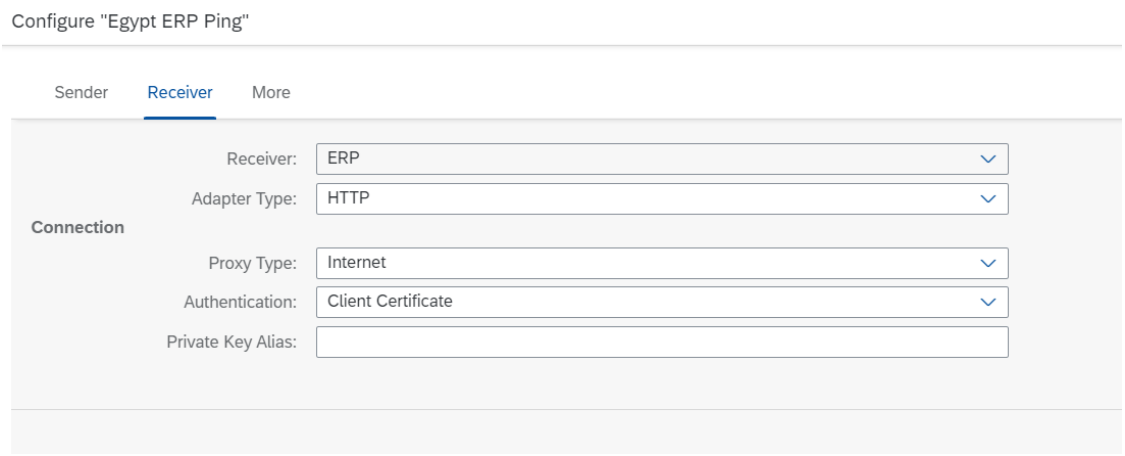




4. Choose *Configure* > *Receiver* tab.
   - You can select the *Proxy Type* as **`Internet`** or **`On-Premise`** if you are using SAP Cloud Connector.
   - You can select the *Authentication* as **`Basic`**, **`OAuth2 Client Credentials`**, or **`Client Certificate`**.
   - For the *Credential Name* (or *Private Key Alias* if you are using **`Client Certificate`** as the Authentication method) you need to enter the value of the *Secure Parameter* from the security material.







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

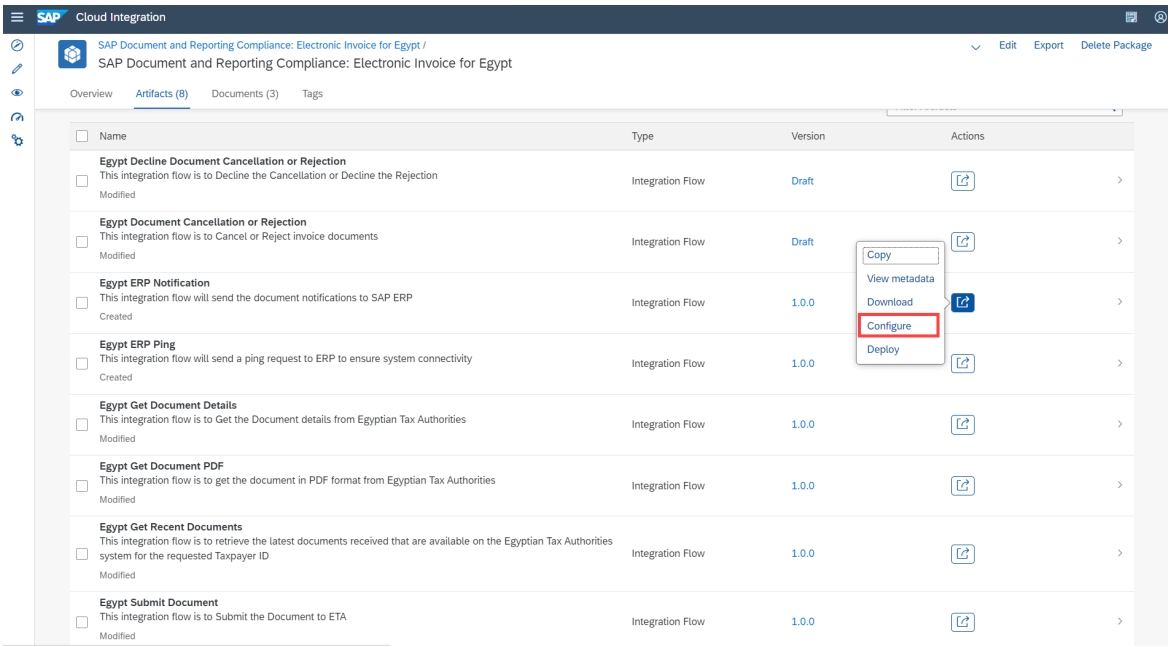
> **i Note**
>
> Depending on the version of your tenant, after pressing these buttons, a warning message can appear.

4.4.4 Configuring Egypt ERP Notification Integration Flow

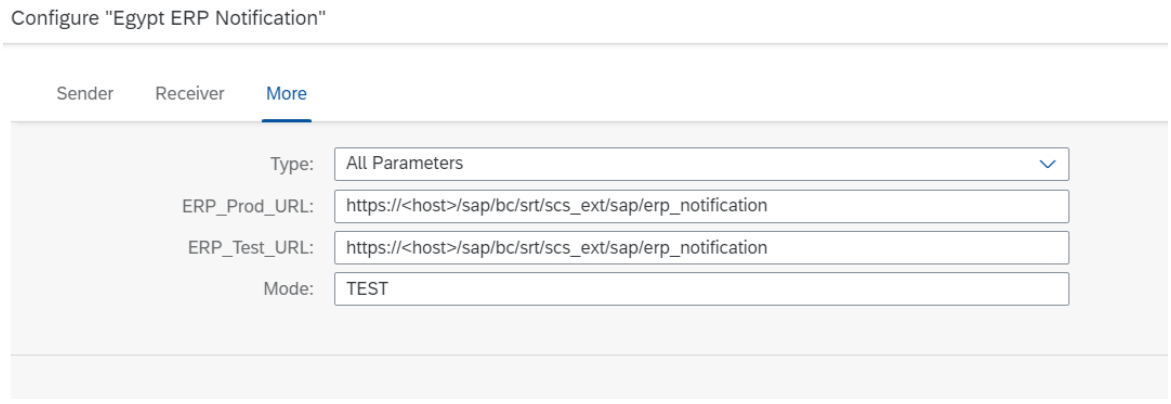
Provides instructions for configuring integration flow for Egypt ERP Notification.

Procedure

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



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



> ### 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.

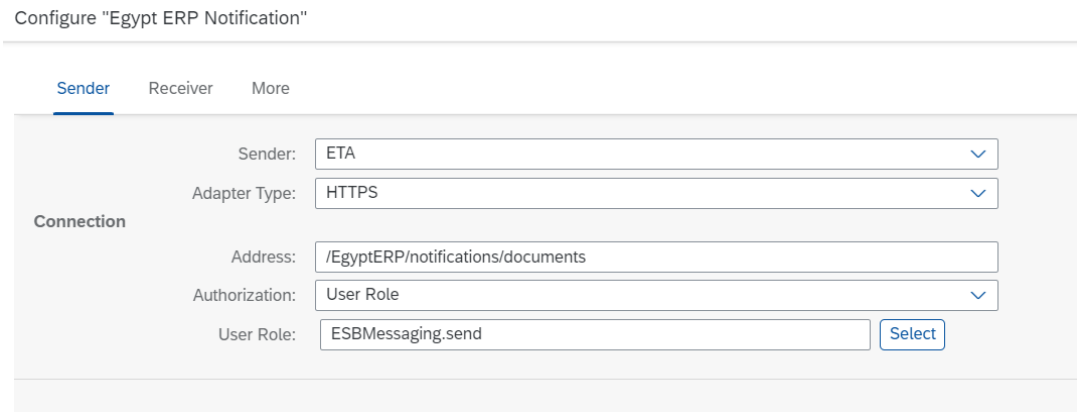
Parameter Name	URL
ERP_PROD_URL	`https://<host>/sap/bc/srt/scs_ext/sap/erp_notification`
ERP_TEST_URL	`https://<host>/sap/bc/srt/scs_ext/sap/erp_notification`

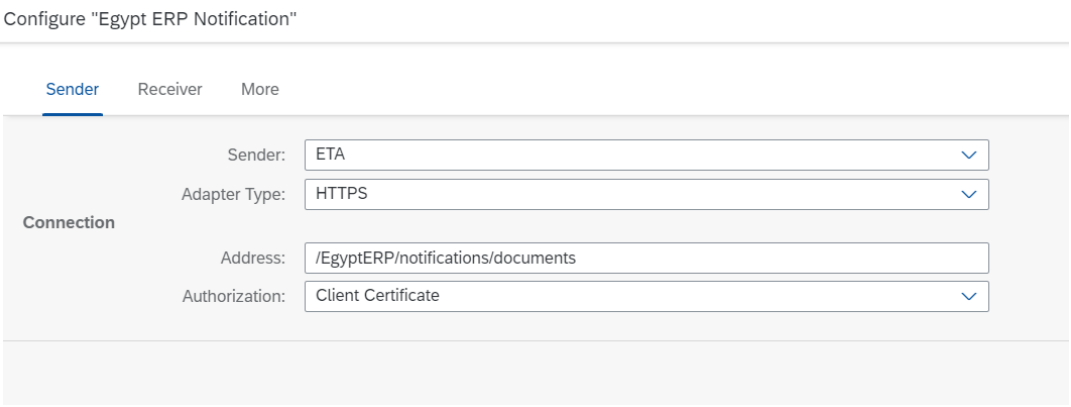
> **i Note**
>
> If the target ERP system is not hosted publicly then you can expose the system via SAP Cloud Connector.

3. 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.

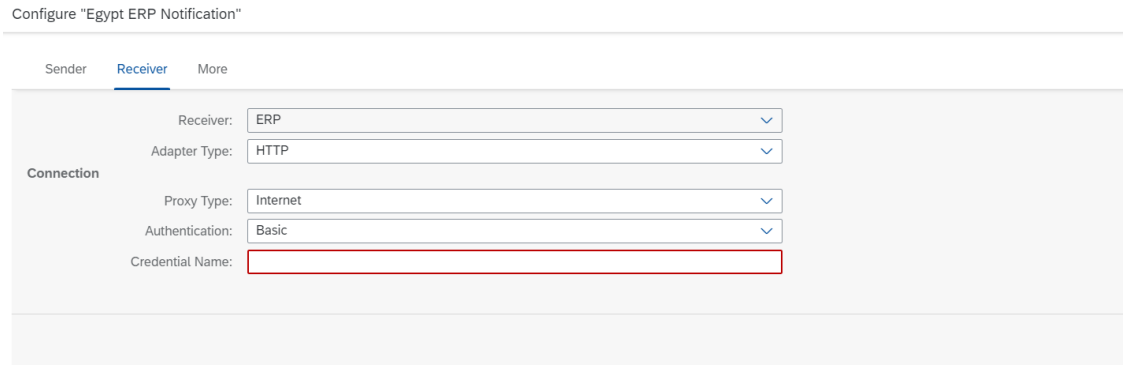
Value	Description
User Role	You want to use basic authentication (user/password).
Client Certificate	You want to use client certificate authentication.

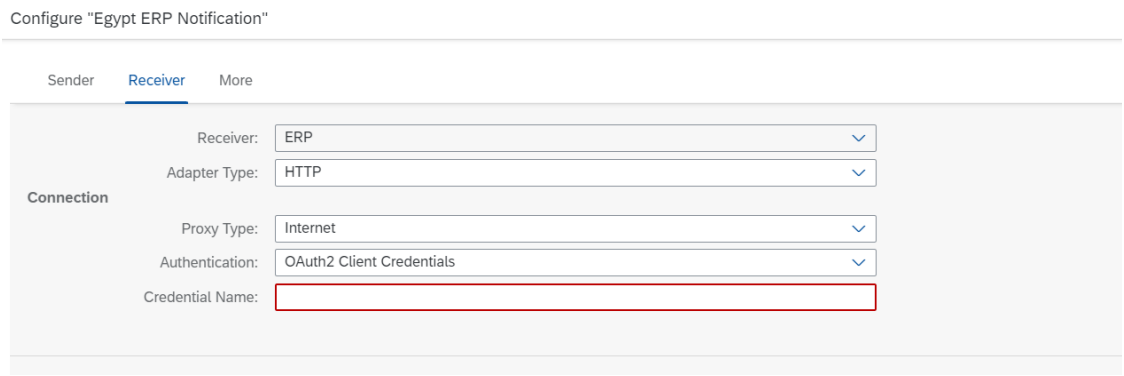
   - Use the `User Role` parameter to configure the role based on which the inbound authorization is checked. Choose *Select* to get a list of all available roles.
     The role `ESBMessaging.send` is provided by default.

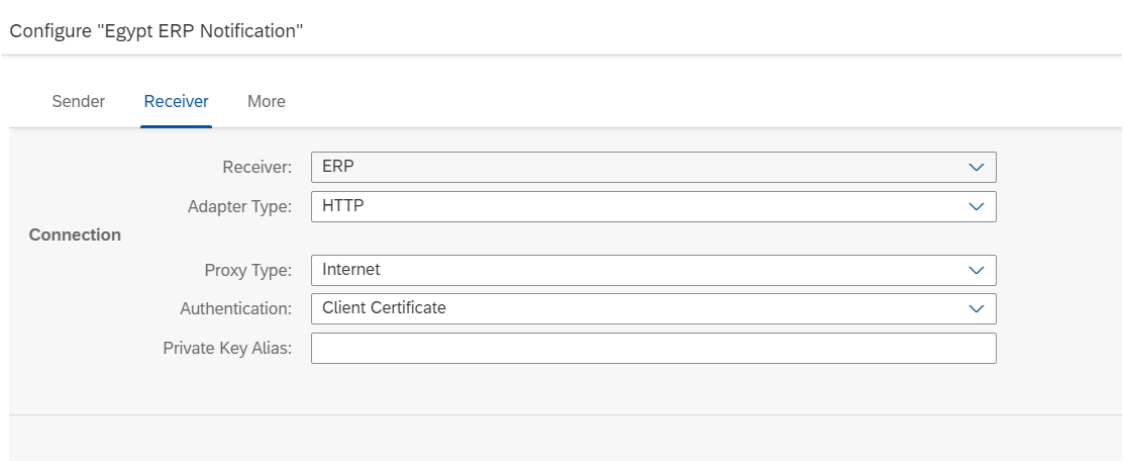




4. Choose *Configure* > *Receiver* tab.
    - You select the *Proxy Type* as **`Internet`** or **`On-Premise`** if you are using SAP Cloud Connector.
    - You can select the *Authentication* as **`Basic`**, **`OAuth2 Client Credentials`**, or **`Client Certificate`**.
    - For the *Credential Name* (or *Private Key Alias* if you are using **`Client Certificate`** as the Authentication method) you need to enter the value of the *Secure Parameter* from the security material.







5. 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

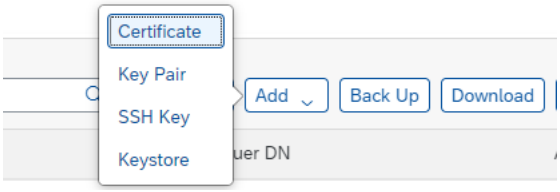
Procedure

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`

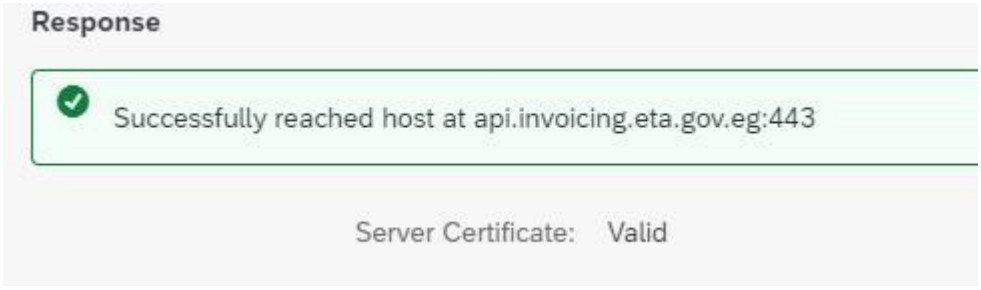
  Port: `443`
- Clear the options **`Authenticate with Client Certificate`** and **`Valid Server Certificate Required`**.

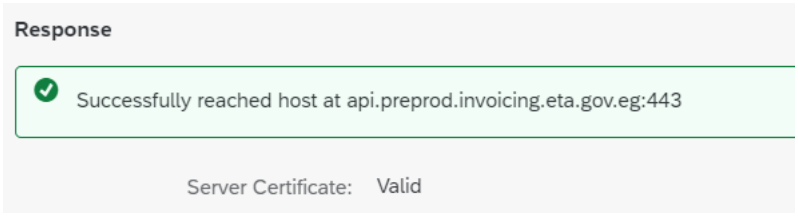
4. Choose *Send*.
5. Download and extract the Server Certificate Chain.
6. Navigate to *Manage Security* from step 2. Choose *Keystore*.
7. Add all the extracted Certificates, one after another. Choose *Add* > *Certificate*. Browse and choose a certificate to upload. Choose *Add*.



> **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 Cloud Integration tenant.

Prerequisites

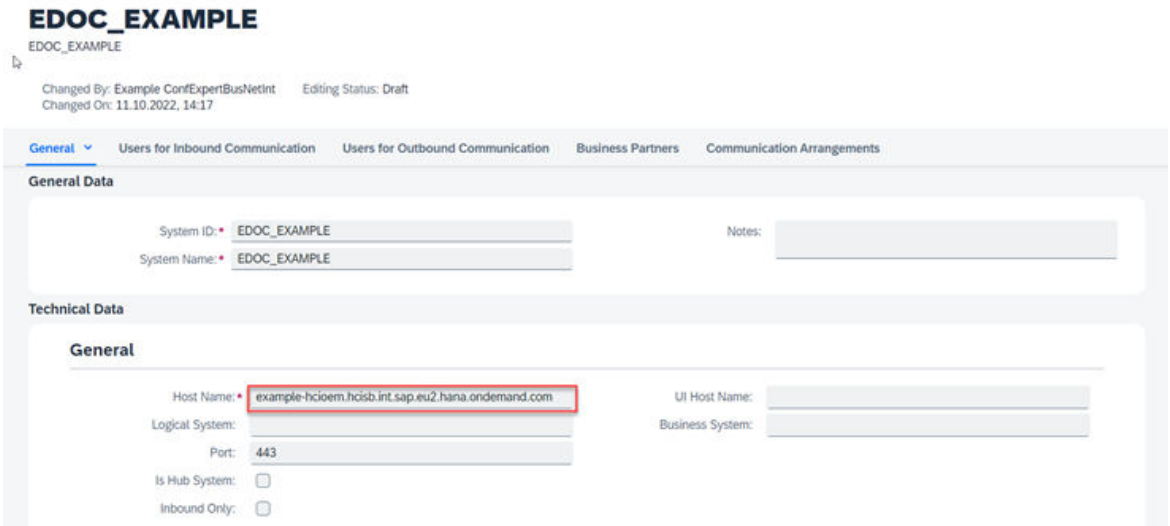
1. Live SAP Cloud Integration test or productive tenant must be available.
2. Communication management setups are not transportable and must be explicitly maintained in quality and production systems.
3. The SAP S/4HANA Cloud user, who is following this guide, must be assigned to a business role that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

Procedure

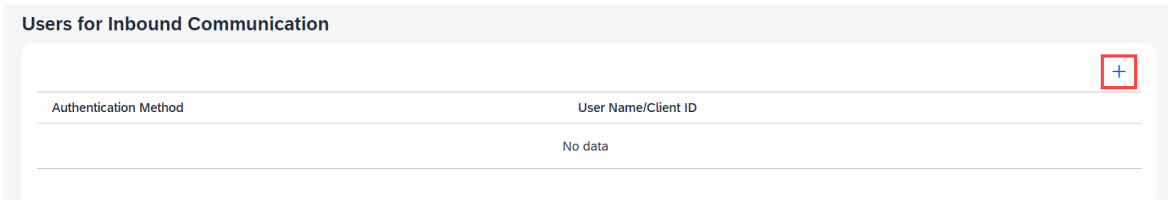
1. Login to your S/4HANA Cloud tenant with the Cloud User.
2. Find and launch the app *Communication Systems.*

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 Cloud Integration 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>*.

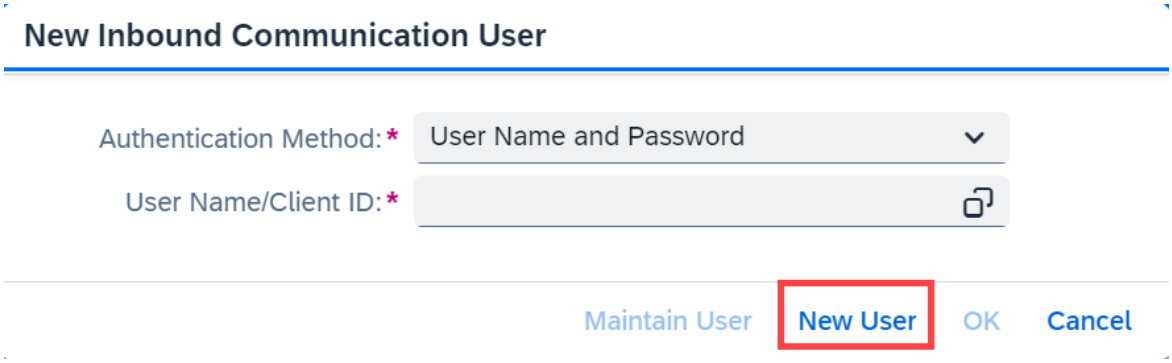


6. Scroll down, and choose + next to *User for Inbound Communication*.



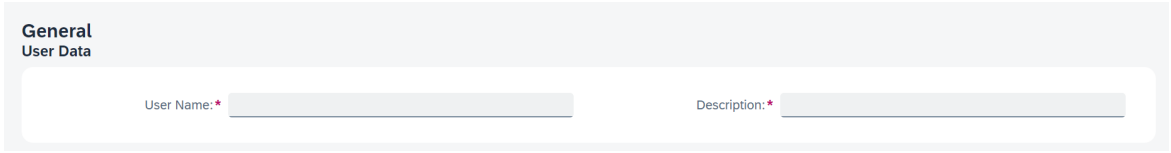
> **i Note**
>
> This step is **optional** if you do not want to use Inbound Communication for notifications.

7. In the new pop-up window, choose *New User*.

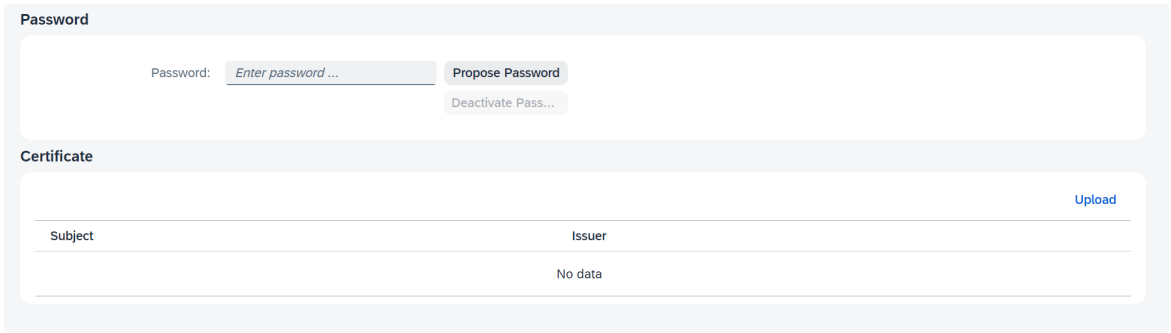


> **i Note**
>
> You can also select an Inbound Communication User if you have already created a user using the *Create Communication User* app. For this, you need to select the *Authentication Method* as either **`User Name and Password`** or **`SSL Client Certificate`**. You can select your communication user in the *User Name/Client ID* field.

8. In the *Create Communication User* app, enter the *User Name* and *Description* under *User Data*.

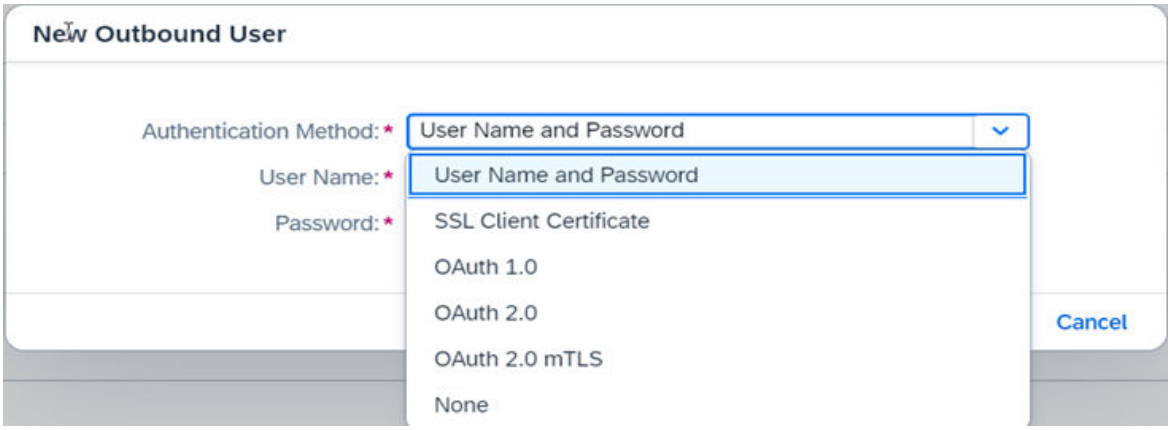


9. You can enter a *Password* or select a *Certificate* and then click *Create* to create a communication user.



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

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



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

> **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.

12. Choose *Save*.

5.2 Configuring Communication Arrangement

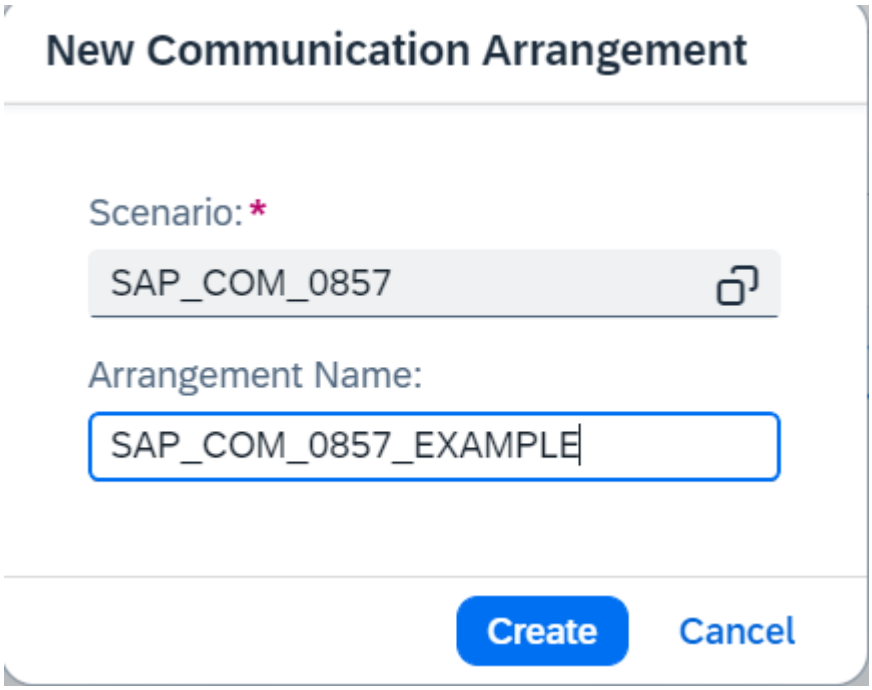
Configuration steps for SAP S/4HANA Cloud Communication Arrangement.

Procedure

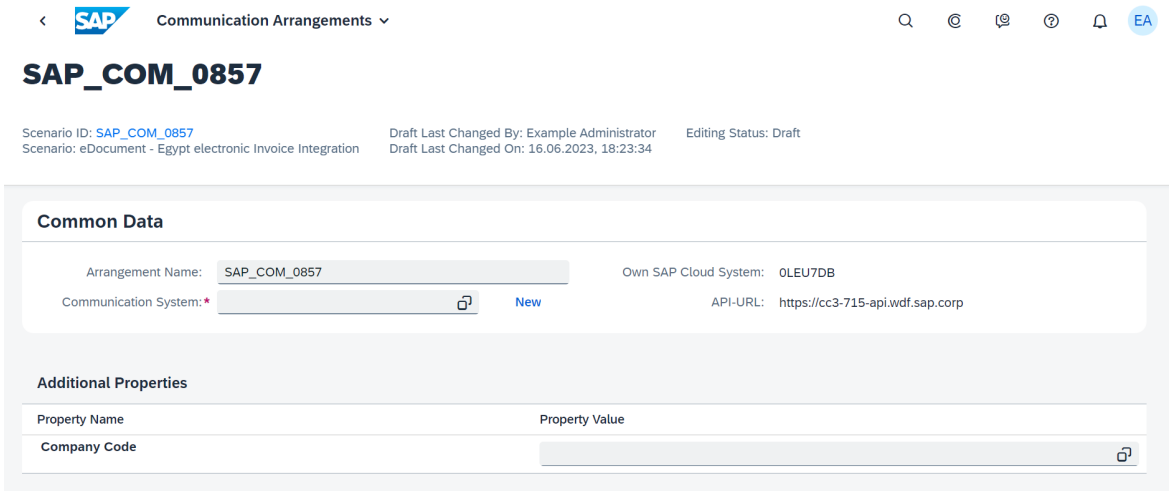
1. Login to your S/4HANA Cloud tenant with the Cloud User.
2. Find and launch the app *Communication Arrangements*.

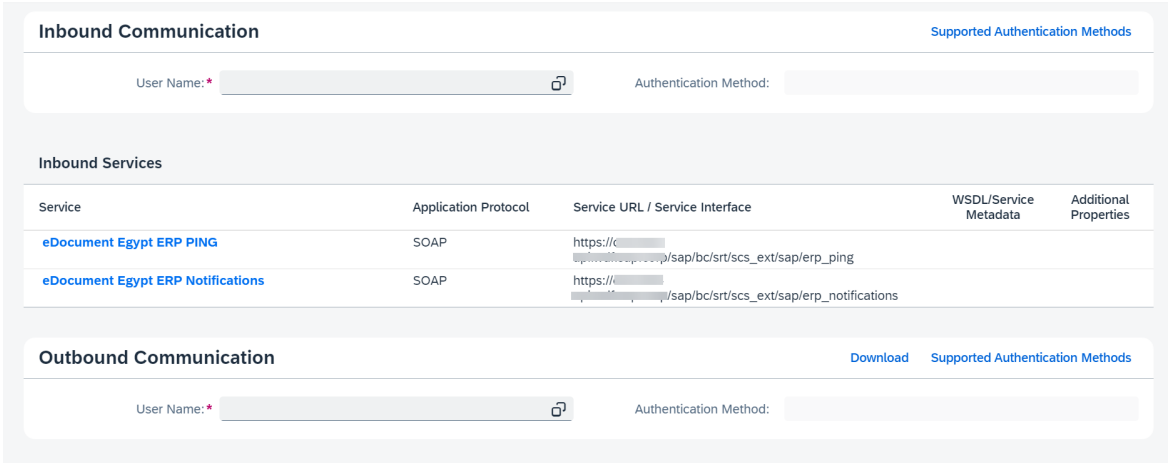
3. Choose *New*. In the new pop-up window, enter the *Scenario* as `SAP_COM_0857` (which is the one designated for communication with the tax authority via SAP Cloud Integration package) and an *Arrangement Name*. For *Arrangement Name* it is recommended to choose a name like `SAP_COM_0857_<name of SAP Cloud Integration tenant>`.

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

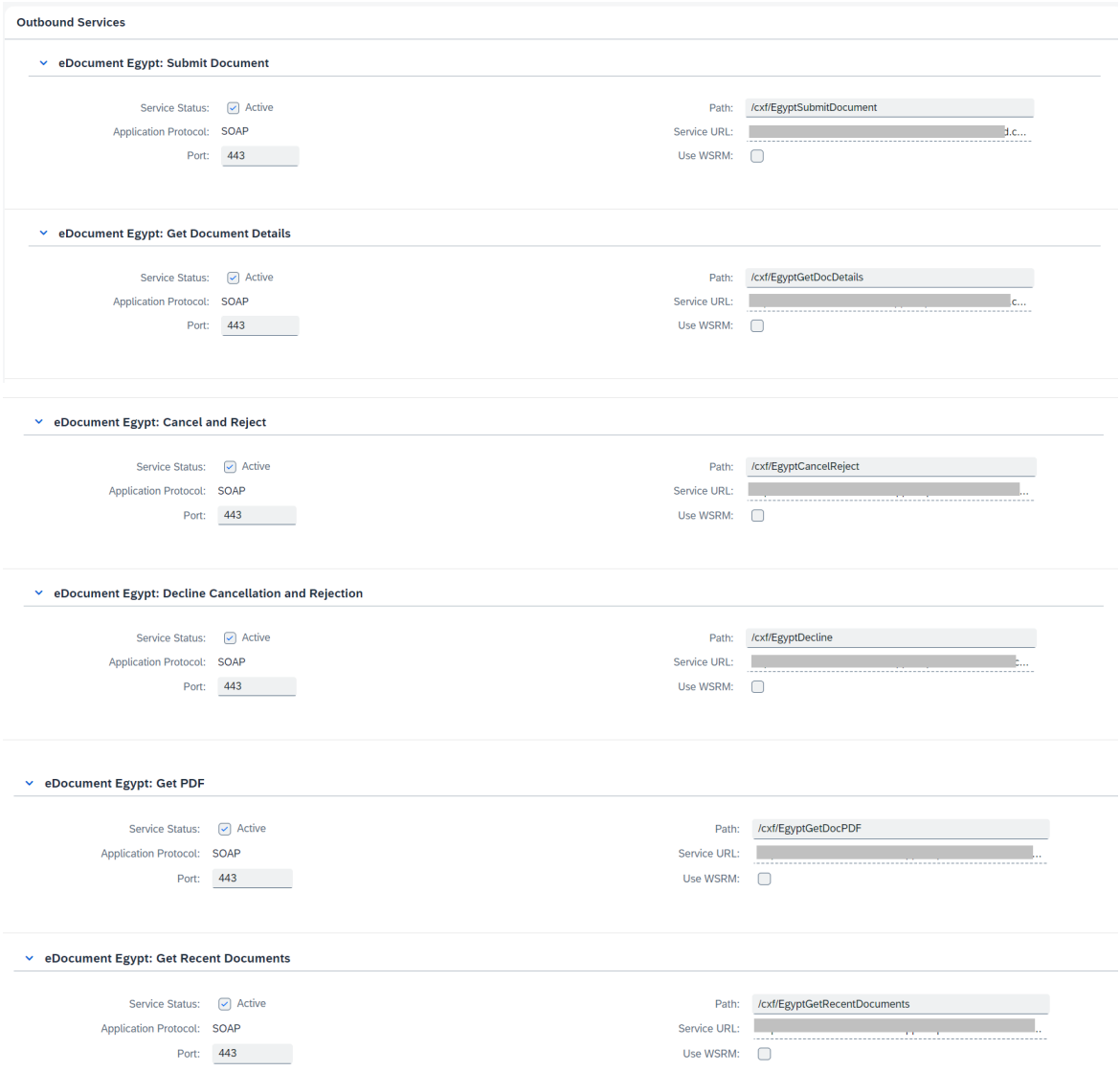


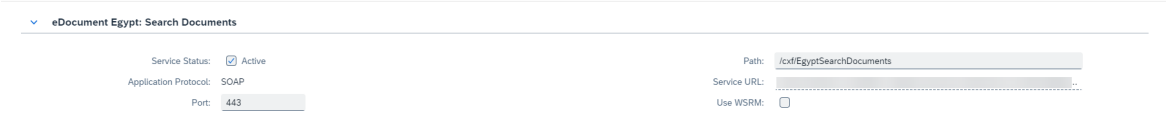
4. Choose *Create*.
5. In the new window, choose the communication system (for example, `EDOC_EXAMPLE`), Additional Properties, Inbound Communication and Outbound Communication created in the previous step.





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