PUBLIC
2020-03-06

SAP Document Compliance for Portugal eInvoicing: Setting Up SAP Cloud Platform Integration (SAP ERP and SAP S/4HANA)

THE BEST RUN SAP

Content

1 Introduction

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

The setup steps are typically done by an SAP Cloud Platform Integration consulting team, which is responsible for configuring the SAP back-end systems and the connection with SAP Cloud Platform Integration. This team may be also responsible for maintaining the integration content and certificates/credentials on the SAP Cloud Platform 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 Platform Integration 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 service provider 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 and SAP S/4HANA.

2 Prerequisites

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

1. eDocument Portugal Full Solution: All relevant notes are installed in the test and/or productive systems.
2. SAP Cloud Platform Integration test/productive tenants are live.
3. You have configured the connection from SAP back-end system to SAP Cloud Platform Integration. Please refer to the following document: http://www.sdn.sap.com/irj/scn/index?rid=/library/uuid/4037b5a5-47a5-3110-e891-f3d9dbafbe86.

2.1 Installation of eDocument Framework

You have installed and configured the eDocument Framework in your test and productive systems. If you did not install the latest support package for your system, refer to the SAP Note 2134248 for the installation guide of SAP Notes.

Application Help for eDocument

For more information about features and country availability of each solution, see the application help in the product page for eDocuments. https://help.sap.com/viewer/p/SAP_E_DOCUMENT. To find the latest published documentation for eDocument for your country, follow the steps below:

1. Choose from *Version* the release you are interested in.
2. To get to the documentation for a given country, under *Application Help* choose *View All* and select your country.

3 Connectivity Steps

3.1 Set Up of Secure Connection

You establish a trustworthy SSL connection to set up a connection between the SAP back-end systems and the SAP Cloud Platform Integration.

Inbound HTTP connections are not required for Portugal. 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 iFlow 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, refer to Operations guide for SAP Cloud Platform Integration

> **i Note**
>
> If you encounter any issues in the information provided in the SAP Cloud Platform Integration product page, open a customer incident against the `LOD-HCI-PI-OPS` component.

3.1.1 Retrieve and Save Public Certificates

Context

Find and save the public certificates from your SAP Cloud Platform Integration worker node.

> **i Note**
>
> If you are using SAP S/4HANA Cloud, some certificates are shared by multiple iFlows.

Procedure

1. Access the SAP Cloud Platform cockpit, and navigate to your subaccount (tenant) page.
2. Click the subscriptions link to display the subscriptions for your subaccount.
3. Select the subscription with suffix **`iflmap`** as this corresponds to your worker node within SAP Cloud Platform Integration.

   Alternatively, use the URL emailed to you with your SAP Cloud Platform Integration subscription details. The URL has the following format **`https://xxxxxxx.hana.ondemand.com/itspaces`**.
4. Choose *Manage Integration Content* and select *All* to display the integration flows (iFlows) available.
5. Select an iFlow 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.

3.1.2 STRUST Configuration

You use the SAP ERP Trust Manager (transaction `STRUST`) to store and manage the certificates required to support connectivity between SAP back-end systems and SAP Cloud Platform Integration.

Upload the Certificates

Context

Store the public certificates used for your productive and test tenants.

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.

Authenticate iFlow

Context

Create an own certificate and get it signed by a trusted certificate auhority (CA) to support iFlow authentication.

Procedure

1. Access transaction `STRUST`.
2. Create your own PSE (for example, Client SSL Standard) and then generate a certificate sign request.
3. Export the certificate sign request as a `*.csr` file.
4. Arrange for the certificate to be signed by a trusted certificate authority (CA).

   If you are using a client certificate, this must be signed by one of the root certificates supported by the load balancer. A self-signed certificate is not suitable. For more information see Load Balancer Root Certificates Supported by SAP.

   The CA may have specific requirements and request company-specific data, they may also require time to analyze your company before issuing a signed certicate. When signed, the CA provides the certificate for import.
5. Navigate to the PSE for **SSL Client Standard** and open it by double-clicking the PSE.
6. Switch to edit mode.
7. Choose the *Import certificate* button.
8. In the *Import Certificate* dialog box, enter or select the path to the CA-signed certificate and choose *Enter*. The certificate is displayed in the *Certificate* area.
9. Choose *Add to Certificate List* to add the signed certificate to the *Certificate List*.

   Ensure that you import the CA root and intermediate certificates to complete the import.
10. Save your entries.

    The certificates can now be used in the SOA Manager (transaction `SOAMANAGER`).

3.2 Set Up SAP Cloud Platform Integration Tenants

SAP Cloud Platform Integration test and production tenants are live and users in the tenants have the rights to copy the integration package and to configure and deploy the integration flows (iFlows).

When your tenants are provisioned, you receive an email with the Tenant Management (TMN) URL. You need this URL for the configuration of the SAP back-end systems.

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

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

4 Configuration Steps

4.1 General Information

The package **SAP Document Compliance: Electronic Invoicing for Portugal** contains the following iFlows:

iFlows for eDocument for Portugal

iFlow Name in WebUI	Project Name/Artifact Name
Portugal Send Invoice	com.sap.GS.Portugal.SendInvoice
Portugal Receive Message	com.sap.GS.Portugal.ReceiveMessage

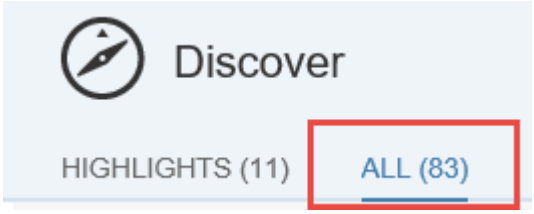
4.2 Copying Integration Flows

Context

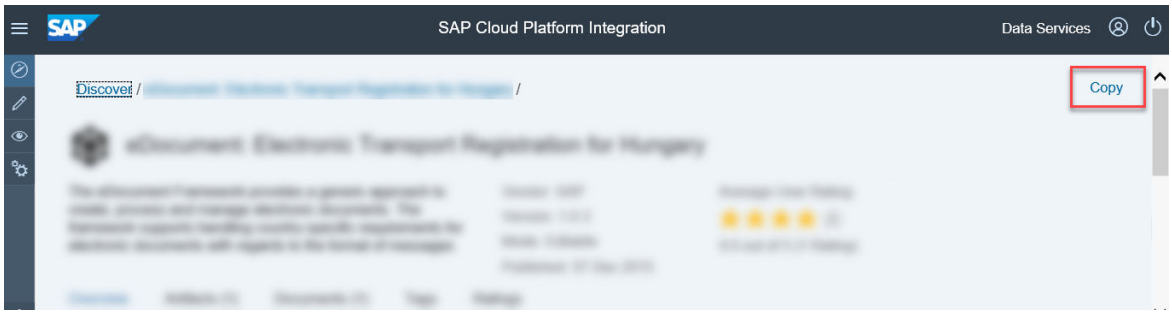
Copy all iFlows in the package SAP Document Compliance: Electronic Invoicing for Portugal to the target tenant as follows:

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 Compliance: Electronic Invoicing for Portugal**.
4. Select the Package and choose *Copy*.



4.3 Configuring Integration iFlows

Provides instructions for Configuring Integration iFlows.

Context

You configure the package that you have copied as described in .

Procedure

1. There are 2 *Artifacts* in the integration package SAP Document Compliance: Electronic Invoicing for Portugal:
   - Portugal: Send Invoice
   - Portugal: Receive Message
2. Choose *Actions* > *Configure* for the artifact you are configuring.

   > **Note**
   >
   > Not all external parameters exist for each integration flow. Configure only the ones which are available.

3. Choose *Configure* > *More* tab (in some versions it may be *Externalized Parameters*)
   - Use the `Mode` parameter to set up the integration package usage mode:

Value	Description
TEST	To use the test system of the service provider.

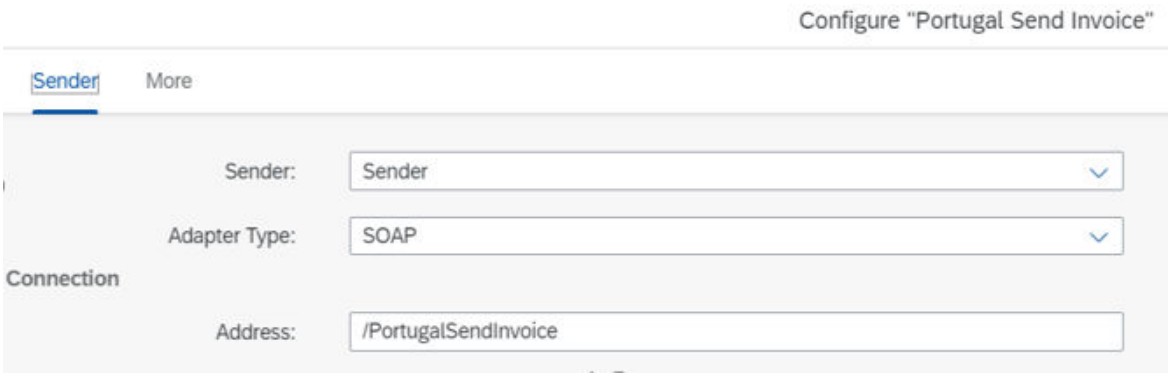
Value	Description
PROD	To use the productive (that is, legally binding) system of the service provider.

- Use the `Enable Logging` parameter to configure whether you want to activate logging functionally for all the messages:

Value	Description
true	The system adds log files to a message.
false	Logging disabled.

- Use the `PROD_API_URL` and `TEST_API_URL` parameters to configure the URL address of the service provider API endpoint for productive and test system respectively.

4. 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.



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

4.4 Service Provider

Provides a description of the service provider.

Saphety is one of the registered service providers for signing eInvoices in Portugal. SAP establishes communication with Saphety.

eSPAP (Entidade de Servicos Partihados da Administracao Publica, I.P.) is the Portuguese government organization responsible for eInvoice. It provides the formats of eInvoice for Portugal.

A customer is an organization with tax identification. A customer is identified in Saphety's network by its country code and tax identification, for example: PT123456789. Handling multiple tax identifications is possible. Each tax identification is a different customer.

Each customer requires a provisioning process.

4.4.1 Creating Technical User

Provides a description of how a service user enables the service provider to access the SAP Cloud Platform tenant.

Context

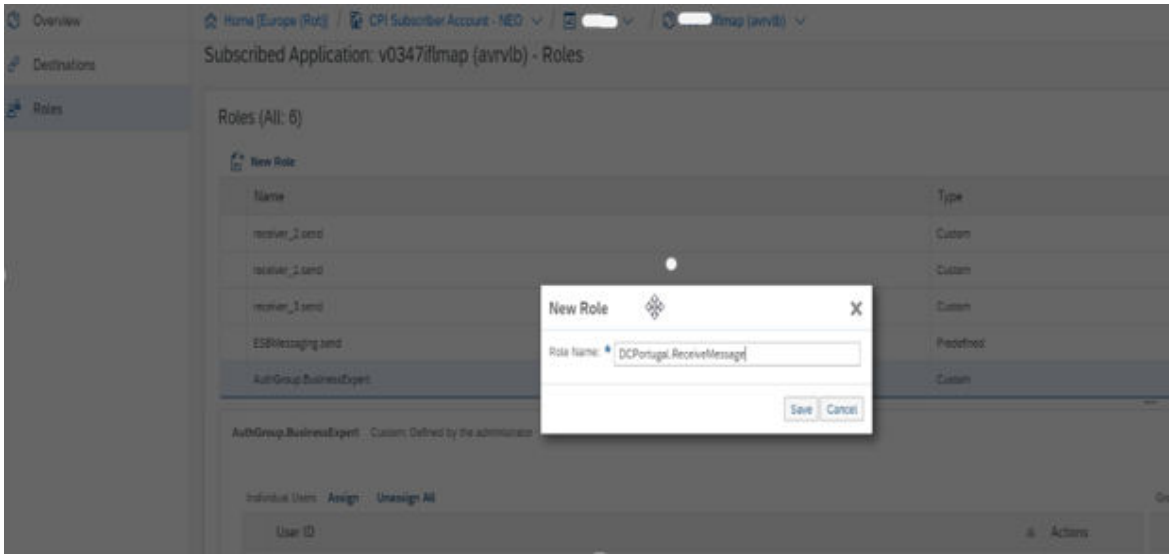
Users can be maintained in two ways in SAP Cloud Platform Integration:

- The default settings where CPI authenticates itself with SAP ID Service. Follow these instructions: https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/f489d66b6edc4eb682e65076e0d873f8.html
- The custom settings where CPI authenticates itself against the custom SCP Identity Authentication Service (IAS). Follow these instructions: https://help.sap.com/viewer/6d6d63354d1242d185ab4830fc04feb1/Cloud/en-US/348deef7f29b40909b151c8dc9a11d53.html

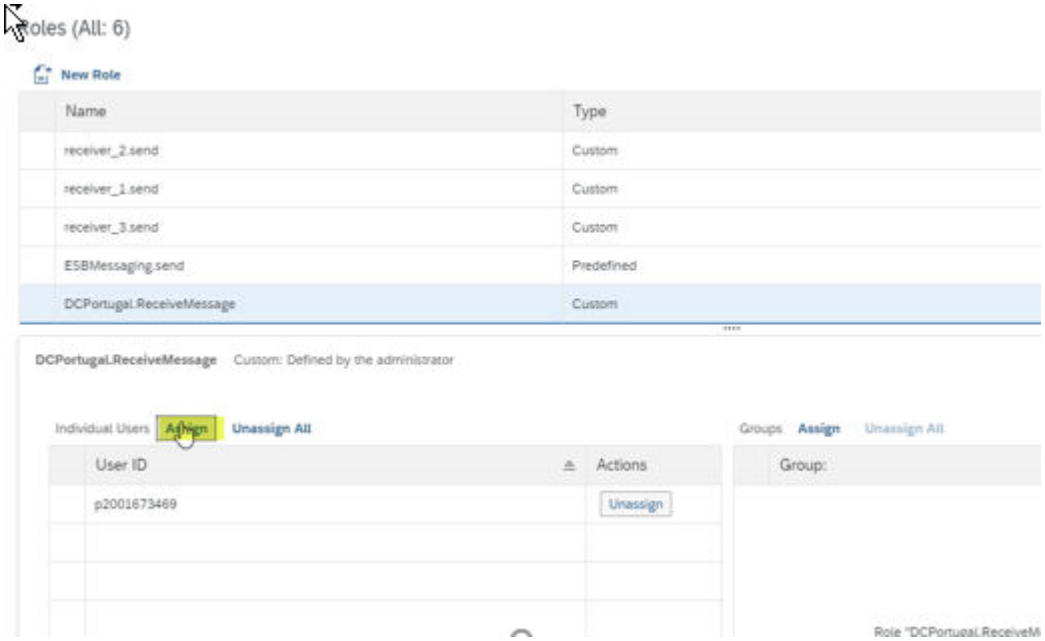
4.4.2 Creating Custom Role

Provides a description of how to authorize the technical user to access the endpoint.

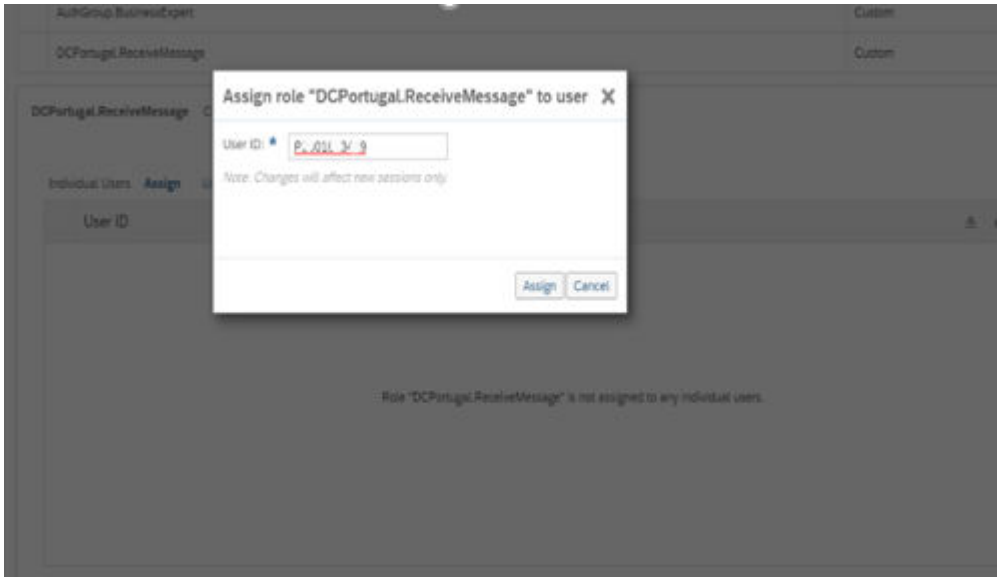
1. Access the SAP Cloud Platform cockpit, and navigate to your subaccount (tenant) page.
2. Choose the *Subscriptions* link to display the subscriptions of your subaccount.
3. Choose the subscription with suffix **`iflmap`** as it corresponds to your worker node within SAP Cloud Platform Integration. Alternatively use the URL e-mailed to you with your SAP Cloud Platform Integration subscription details. The URL has the following format **`https://xxx.hana.ondemand.com/itspaces`**.
4. Choose *Roles* to display the roles for your SAP Cloud Platform Integration worker node.
5. Choose *New Role* and enter the role name **`DCPortugal.ReceiveMessage`**. Choose *Save*.



6. Choose the created role and *Assign*



7. Enter the ID of the technical user.

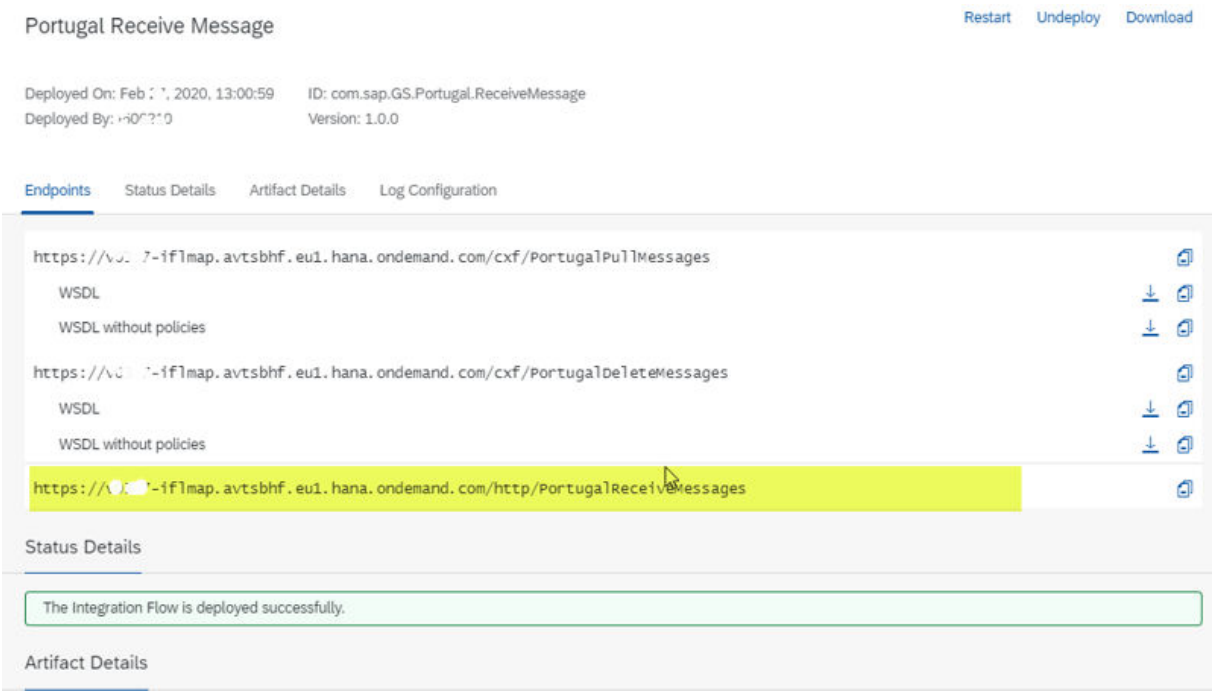


> **i Note**
>
> Make sure that no other access is granted to the technical user.

4.4.3 Sharing Details with the Service Provider

Provides a description of how to share details with the service provider.

Share the following details with the service provider: Service URL (see highlighted part in screenshot), Technical User ID, Password.



⚠ Caution

- If the service provider informs you with the error code “404”, check if the iflow was successfully deployed and the URL is available to receive the messages
- If the service provider informs with the error code “403”, check the following details:
  • The technical user is assigned with an appropriate role (DCPortugal.ReceiveMessage)
  •The user credentials are correct.

4.4.4 Creating Credentials

Provides a description of how to enter the credentials from the service provider in SAP Cloud Platform Integration.

Context

To get access to the webservices provided by the service provider, the credentials received from the service provider are entered in SAP Cloud Platform Integration.

Procedure

1. Access the SAP Cloud Platform cockpit and navigate to your subaccount (tenant).
2. Choose the *Subscriptions* link to display the subscriptions for your account
3. Choose the subscription with suffix **`iflmap`** as this corresponds to your worker node within SAP Cloud Platform Integration. Alternatively, use the URL e-mailed to you with your SAP Cloud Platform Integration subscription details. The URL has the following format **`https://xxx.hana.ondemand.com/itspaces`**.
4. Navigate to the *Manage Security* section and choose *Security Material*.
5. Choose *Add User Credentials* and enter the following data and choose *Deploy* to save the changes.

Option	Description
Name	**`<VAT_code>_<SystemType>`** where <VAT_code> is the company's VAT in the SAP system <SystemType> is TEST or PROD depending on the type of your tenant Example: PT123456789_TEST
Description	Enter the name of the company.

Option	Description
User	Enter the username from the service provider.
Password	Enter the password received from the service provider.

6. Choose *Deploy* to save the changes.

4.5 Creating Logical Ports in SOAMANAGER

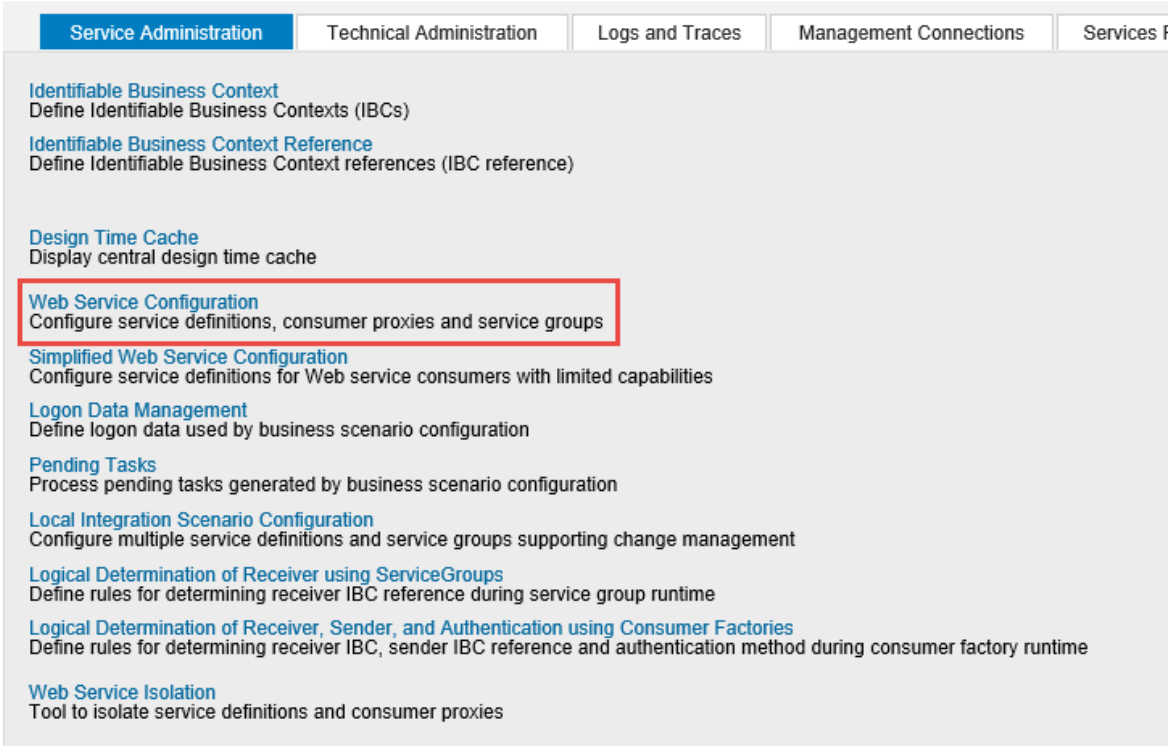
Context

You configure proxies which are needed to connect to the SAP Cloud Platform Integration tenant via logical ports. In test SAP back-end systems, the logical ports are configured to connect to the test tenant. In productive SAP back-end systems, the logical ports are configured to connect to the productive SAP Cloud Platform Integration tenant.

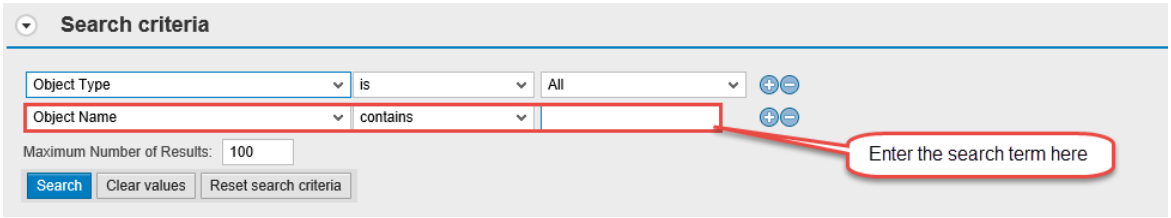
> **i** Note
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

Procedure

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



2. Find the proxies for SAP Document Compliance (eDocument) for Portugal with search term `CO_EDO_PT*`.

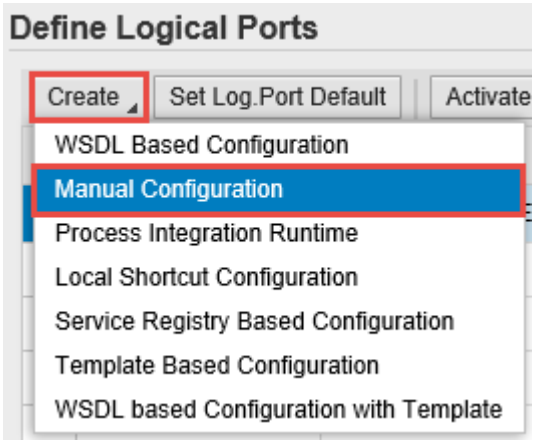


The following table lists the proxies and the logical port name, description and path for each proxy.

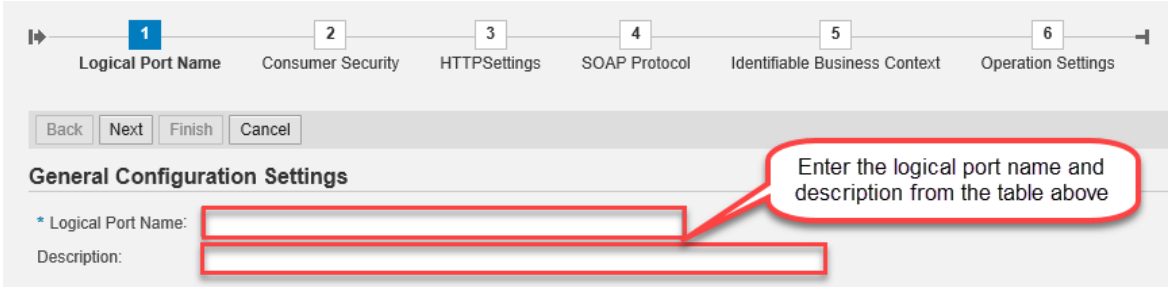
List of Proxies, Logical Port Names, and Paths

Proxy Name	Logical Port Name	Description	Path
CO_EDO_PT_SEND_IN-VOICE_V1_0	EDO_PT_SEND_INVOICE	eDocument Portugal - Send Invoice	/cxf/PortugalSendInvoice
CO_EDO_PT_SEND_CRED-ITNOTE_V1_0	EDO_PT_SEND_CREDIT-NOTE	eDocument Portugal – Send Credit Note	/cxf/PortugalSendInvoice
CO_EDO_PT_RE-CEIVE_MESSAGE_V1_0	EDO_PT_PULL_MESSAGE	eDocument Portugal – Pull Message	/cxf/PortugalPullMessages
CO_EDO_PT_RE-CEIVE_MESSAGE_V1_0	EDO_PT_DELETE_MES-SAGE	eDocument Portugal – De-lete Message	/cxf/PortugalDeleteMes-sages

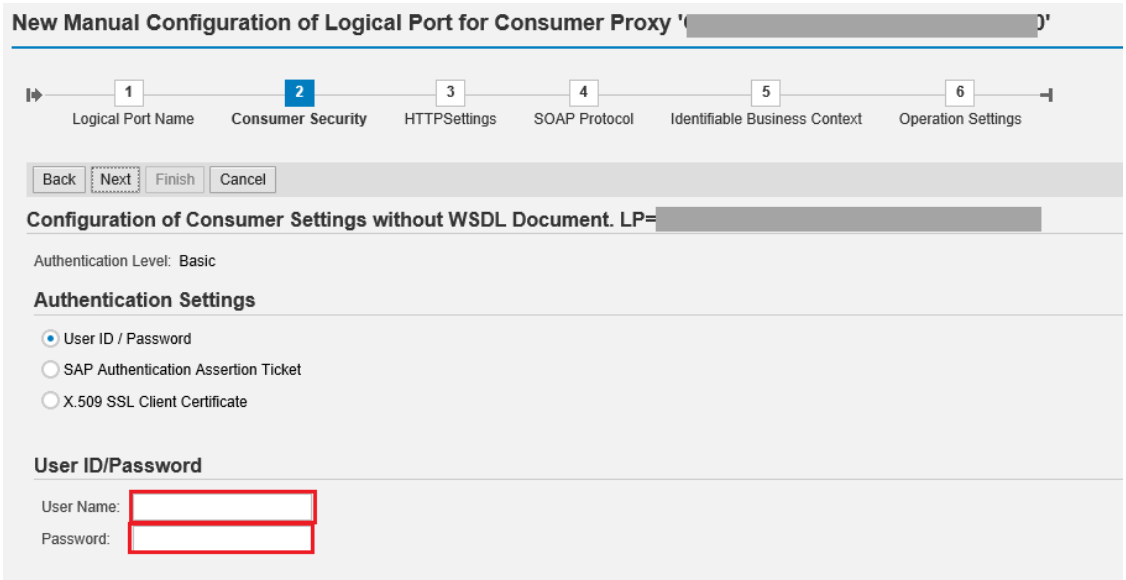
3. In the *Result List*, select a proxy from the list above and create a logical port for each proxy. Choose *Create* > *Manual Configuration*.



4. Enter the logical port name and a description.



5. The configuration you do in the *Consumer Security* tab in the *Configuration* screen depends on the security being used in the communication between the SAP back-end system and SAP Cloud Platform Integration.
   a. If you use the basic authentication, select the *User ID / Password* and enter *User Name* and *Password*.



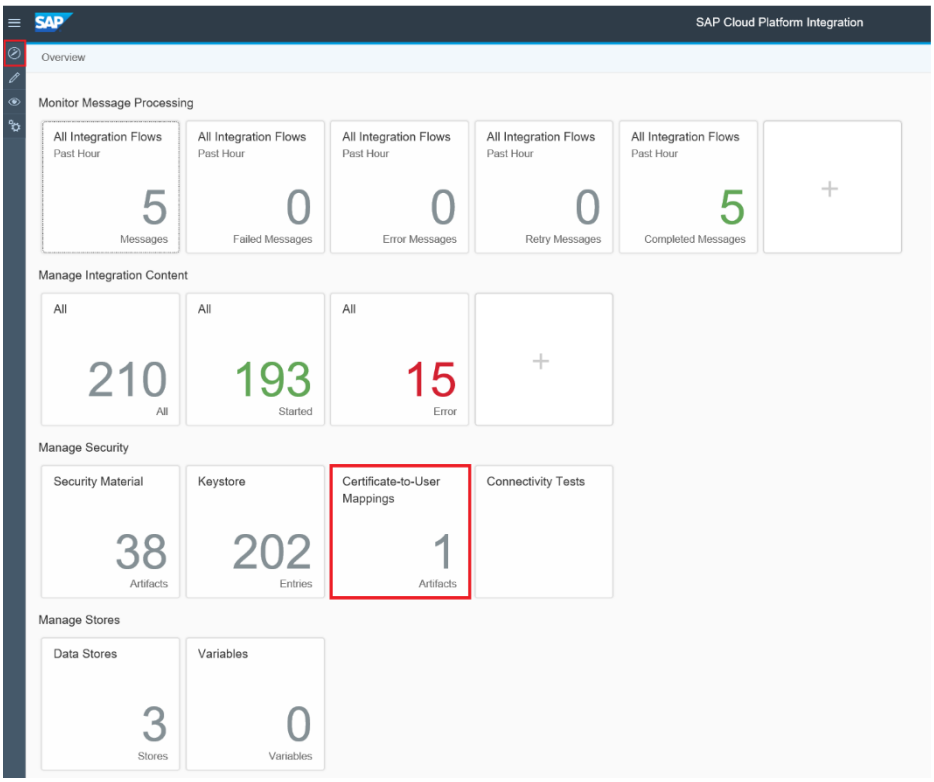
   b. If you use certificate-based authentication, select *X.509 SSL Client Certification*. Ensure that the required certificates are available in the `STRUST` transaction.

      Note: If you do not see this option or cannot select it, check the SAP Notes 2368112 and 510007

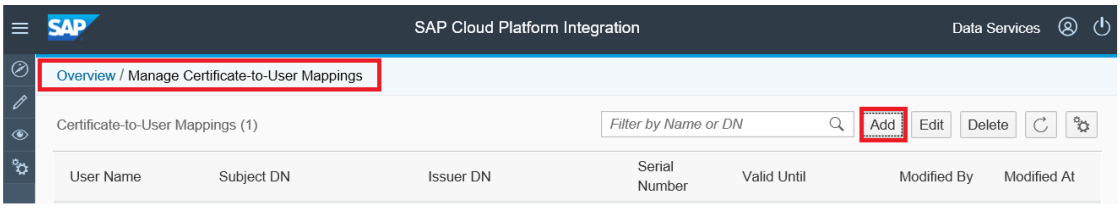
Additionally, you map the certificate to a user of your tenant with the `ESBMessaging.send` role. First, you export the certificate from the `STRUST` transaction. Save it locally and upload it to SAP Cloud Platform Integration in the `Certificate-to-User Mappings`

a. Export the SSL Client PSE of the `STRUST` transaction.

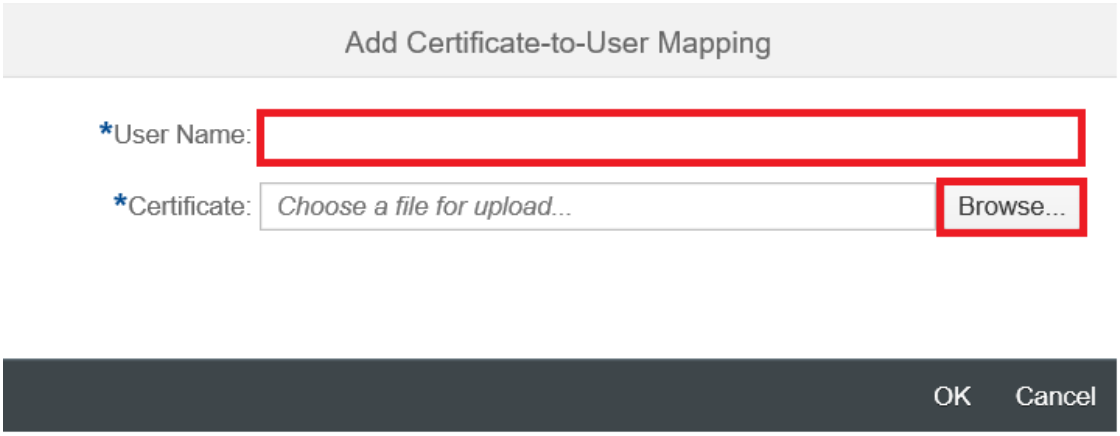
b. Go to SAP Cloud Platform Integration under *Overview* > *Certificate-to-User Mappings*



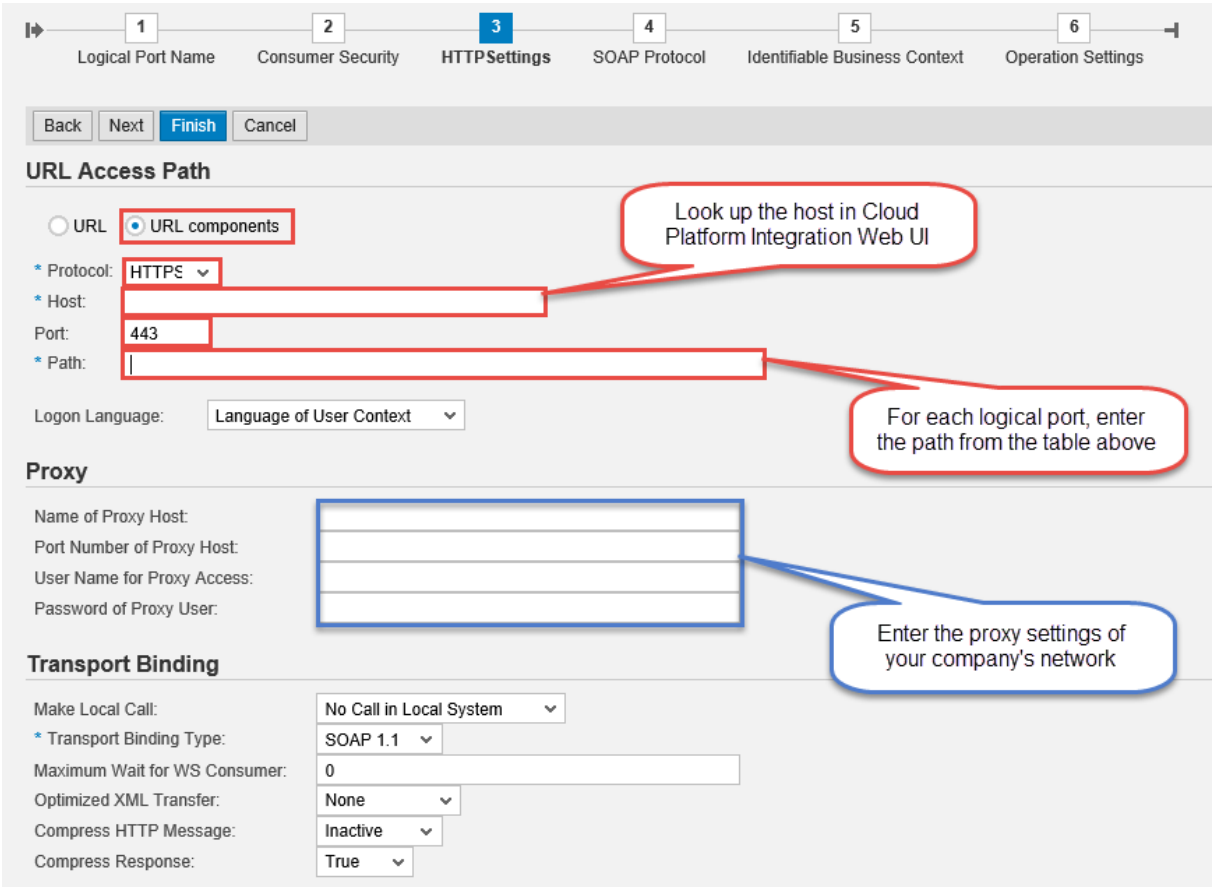
a. Choose *Add*.



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

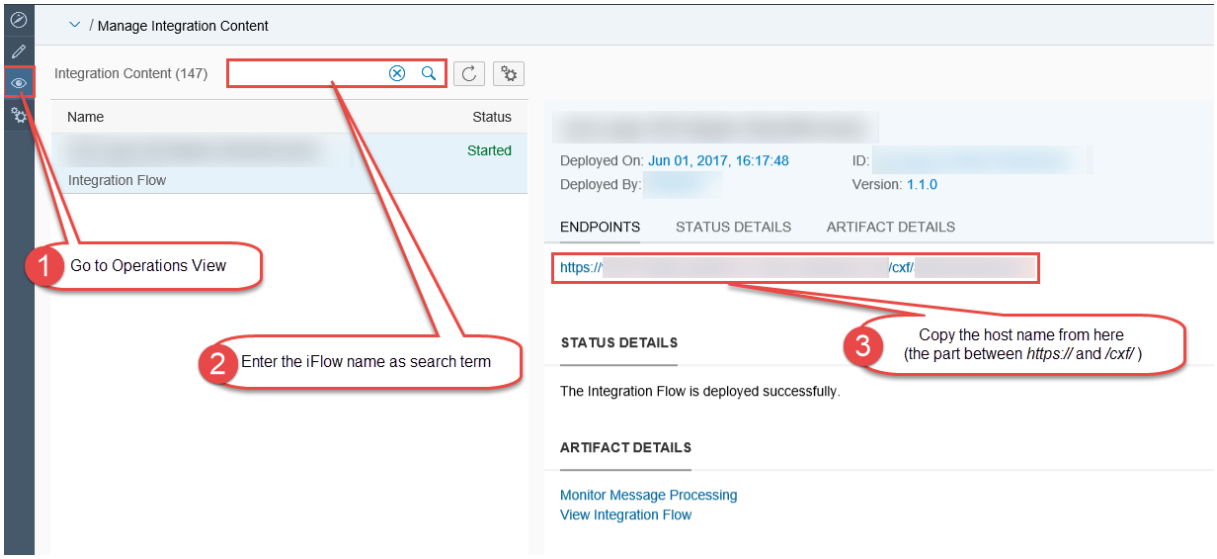


6. On the *HTTP Settings* tab, make the following entries:



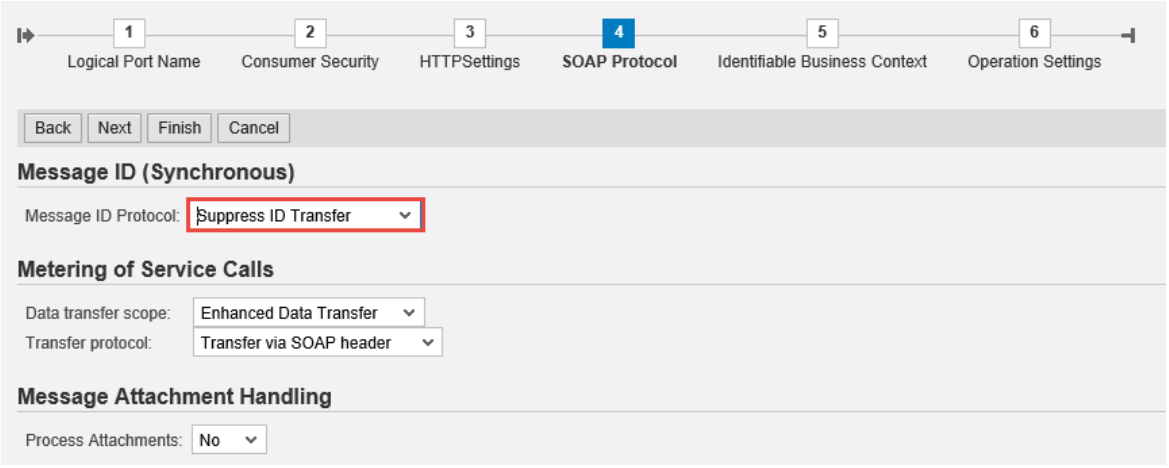
Port 443 is the standard port for the HTTPS protocol.

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



> ### Note
>
> The entries for the proxy fields depend on your company's network settings. The proxy server is needed to enable the connection to the internet through the firewall.

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



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

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

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

9. Remember to create logical port(s) 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 Testing the Integration

Describes the steps to test the integration of SAP Document Compliance (eDocument) with the integration scenario from SAP Cloud Platform Integration.

Context

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

Procedure

1. In the back-end system, go to the *eDocument Cockpit* (EDOC_COCKPIT) transaction, in the relevant process.
2. Select an eDocument and check the status of the eDocument in the Cockpit and perform the following actions, accordingly:
   a. If the status of the eDocument is `Created`, the eDocument was created but not submitted yet. In this case, select it and choose *Submit*. This action triggers the creation of the XML and the subsequent communication with SAP Cloud Platform Integration.
   a. If the status is green or yellow, but not `Created`, the communication with SAP Cloud Platform Integration was triggered and was probably successful. You can double-check if the message went through on the SAP Cloud Platform 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.

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.

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.

Gender-Related Language

We try not to use gender-specific word forms and formulations. As appropriate for context and readability, SAP may use masculine word forms to refer to all genders.

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.

www.sap.com/contactsap

THE BEST RUN SAP