INTEGRATION GUIDE | CONFIDENTIAL
2020-06-10

Italy eInvoice: Setting up SAP Cloud Platform Integration (SAP ERP, SAP S/4HANA) - Neo environment

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 tax authority servers do not provide all services that are described in this document. Please refer to the relevant SAP back-end systems documentation and to the relevant tax authority information, respectively.

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

2 Prerequisites

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

1. eDocument 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.

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. For more information, refer to the documentation of the SAP Cloud Platform Integration

Inbound HTTP connections are not required for Italy. 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.

Client Certificate

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

3.1.1 Retrieve and Save Public Certificates

You perform this action in the back-end systems only if you are using certificate-based authentification. Not required for basic authentification.

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`).

3.1.3 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).

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.

3.2 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. For more information, refer to the documentation of the SAP Cloud Platform Integration

Inbound HTTP connections are not required for Italy. 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.

Client Certificate

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

3.3 Set Up Aruba Connection

You use the SAP Cloud Platform Integration tenants to store and manage the certificates required to support connectivity between the Aruba signing service and SAP Cloud Platform Integration.

Context

These tasks **only** apply to domestic companies that use Aruba signing services; these companies must create aliases and deploy the Aruba service iFlow for the production tenant.

Create Aliases and their Credentials

Context

In order to configure Aruba's digital signature in SAP Cloud Platform Integration, you need to create two aliases for each VAT within your productive tenant, and assign their credentials.

The aliases are:

- signatory `edoc_italy_aruba_prod_<VAT_code>`
- delegate or technical user `edoc_italy_aruba_deleg_prod_<VAT_code>`

The user will be taken from the credential `edoc_italy_aruba_prod_{IVA}`.

> **i** Note
>
> The credentials must be set without the **`@faSAP`** domain.

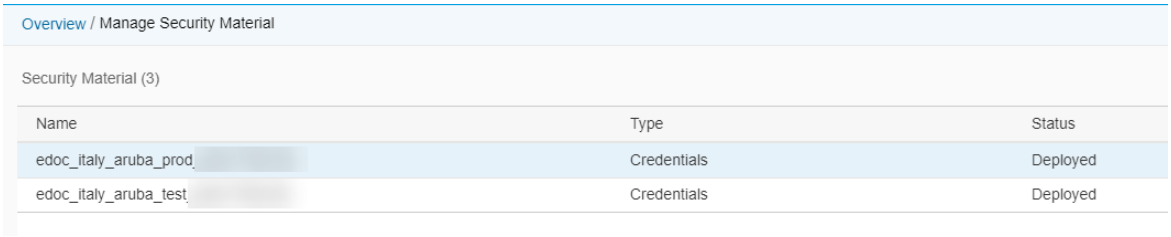
Procedure

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. Navigate to the *Manage Security* section, and choose *Select Material*.



5. Choose *User Credentials* and enter the following data:.

Field	Entry
Name	**`edoc_italy_aruba_prod_<VAT_code>`**, where **`<VAT_code>`** is the company's VAT on the SAP production system
Description	Enter the name of the signatory for example, **`Maria Rossi`**.
User	Enter the username of the signatory released by Aruba, without the **`@faSAP`** suffix. For example, if the signatory's username is **`abcdef50a20e435q@faSAP`**, then you enter **`abcdef50a20e435q`** .
Password	Enter a dummy password, e.g. **`1234567`**.

6. Choose *Deploy* to save the changes.
7. Repeat the steps using the delegate alias to create a delegate (edoc_italy_aruba_deleg_prod_<VAT_code>) or a technical user (edoc_italy_aruba_test _<VAT_code>).

Retrieve and Save the Transport Certificates

Procedure

1. Copy the URLs listed below, and paste them into your web browser.

Environment	URL
Test	https://arss.demo.firma-automatica.it/ArubaSignService/ArubaSignService
Production	https://arss-sap.actalis.it/ArubaSignService/ArubaSignService

2. When prompted by the *Website Identification* window, choose *View certificate*.

3. Select the root certificate, and then choose *Export to file* to save the certificate locally.
4. Repeat these steps for each unique root, intermediate and leaf certificate, and repeat for both your test and production tenants.

Upload the Certificates to the Keystore

Procedure

1. Access SAP Cloud Platform Integration.
2. Navigate to the *Manage Security* section, and choose *Keystore*.
3. Choose *Certificate* and import all the transport certificates.
4. Save your entries.

3.4 Registration at Tax Authorities

To send and receive invoices through the Exchange System (Italian: Sistema de Interscambio, SdI) of the Italian tax authorities, your company needs to register two web-service channels for the SDICoop Service on their official website. You use these channels for the following purposes:

- To send outbound invoices and outcome notifications related to inbound invoices from the eDocument Framework (using SAP Cloud Platform Integration) to the Exchange System.
- To receive inbound invoices and status notifications related to outbound invoices from the Exchange System.

> **i** Note
>
> Multiple companies in a group can share a channel, and send all invoices through the registered channel to SdI.

To complete communication channel registration at the Italian tax authorities, see SAP Note 2583309.

You need to complete the steps outlined in the **Communication Channel Registration** document, including:

- Generate certificate signing requests (CSRs) for both outbound and inbound communications
- Create the channel registration request
- Sign and send the request

3.4.1 Deploying Key Pairs, Certificates and Credentials

Context

When registration with the Exchange System (Italian: Sistema de Interscambio, SdI) is successful, you will receive an email to your CEM (Italian: Posta Elettronica Certificata PEC) address confirming that the channel has been registered.

Additional steps are required for inbound and outbound communication security. This involves deploying the key pairs, certificates and the credentials to the SAP Cloud Platform Integration tenants.

To finalize communication channel registration at the Italian tax authorities, see SAP Note 2583309. You need to complete the steps outlined in the **Communication Channel Registration** document, including:

- Sign and send the request
- Understand the information received from the SdI
- Upload security elements to SAP Cloud Platform Integration keystore
- Configure SSL host-owned signed certificate
- Add tax authority (Italian: Agenzia Delle Entrate) certificates to the SSL host
- Create custom domains
- Add the certificate-to-user mapping

Create Aliases and their Credentials

Context

In the Registration at Tax Authorities [page 11] task, you registered a communication channel for the company. Now, you create aliases for each key pair, and upload the credentials for the company to the productive tenant.

Two aliases (and their credentials) are required for each VAT within your productive tenant. Create the alias for the key pair according to the following naming convention:

- Non-production environment, `edoc_italy_key_test_<VAT_code>*`
- Production environment, `edoc_italy_key_prod _<VAT_code>*`

* You can use the same communication channel registration for multiple VAT codes. In that case, add to your test/productive tenant the same key-pair multiple times using corresponding VAT-code specific aliases

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. Navigate to the *Manage Security* section, and choose *Select Material*.
5. Choose *User Credentials* and enter the following data:.

Field	Entry
Name	**`edoc_italy_key_test_<VAT_code>`**, where **`<VAT_code>`** is the company's VAT on the SAP production system
Description	Enter the name of the signatory for example, **`Maria Rossi`**.
User	Enter the username of the signatory.
Password	Enter a dummy password, e.g. **`1234567`**.

6. Choose *Deploy* to save the changes.
7. Repeat the steps for each alias.
8. Deploy the public certificates and the root certificates of the Exchange System in the keystore. You download them from the Exchange System website in the *Manage the Channel* section after you have successfully registered the registration channel.

4 Configuration Steps in SAP Cloud Platform Integration

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

4.1 General Information

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

iFlows for eDocument for Italy

iFlow Name in WebUI	Project Name/Artifact Name
Italy Receive Invoice	com.sap.GS.Italy.ReceiveInvoice
Italy Receive Notification	com.sap.GS.Italy.ReceiveInvoiceNotification
Italy Send Invoice	com.sap.GS.Italy.SendInvoice
Italy: Send Outcome Notification	com.sap.GS.Italy.SendOutcomeNotification
Italy: Sign Service Aruba	com.sap.GS.Italy.SignServiceAruba

4.2 Copying Integration Flows

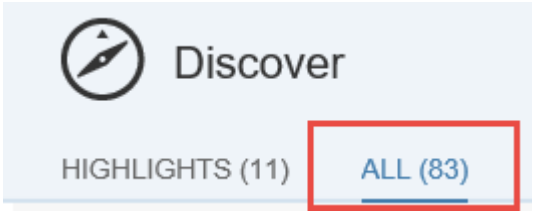
Context

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

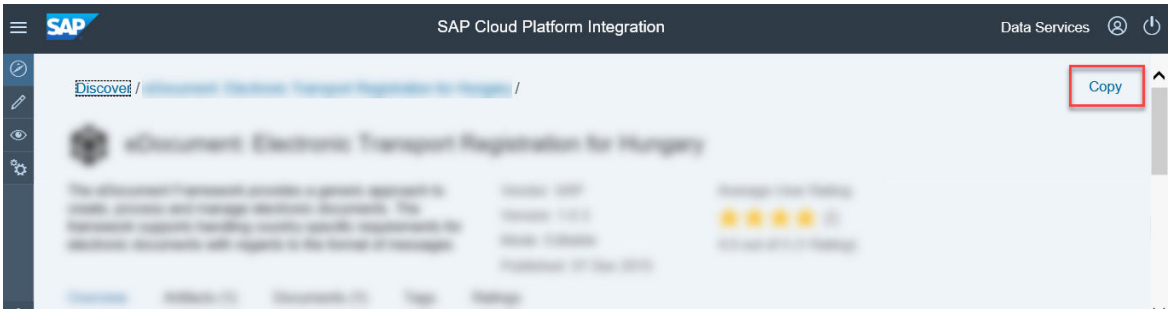
Procedure

1. 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 Italy**.
4. Select the Package and choose *Copy*.



4.3 Configuring Integration iFlows

Context

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

Procedure

1. There are 5 *Artifacts* in the integration package SAP Document Compliance: Electronic Invoicing for Italy:
   - Italy: Receive Invoice
   - Italy: Receive Notification
   - Italy: Send Invoice
   - Italy: Send Outcome Notification
   - Italy: Sign Service Aruba
2. Choose *Actions* > *Configure* for the artifact you are configuring.

> **i 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:

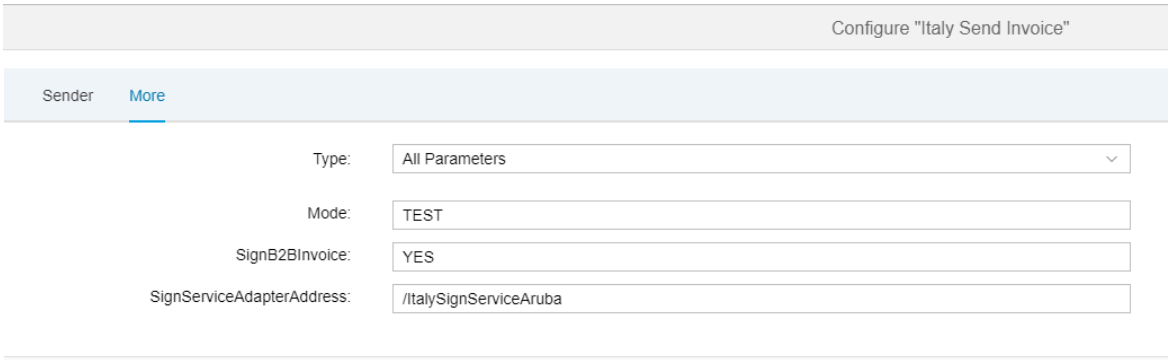
Value	Description
TEST	To use the test system of the tax authority or the signing service.
PROD	To use the productive (that is, legally binding) system of the tax authority or the signing service.

   - Use the `SignB2BInvoice` parameter to configure whether you want B2B invoices to be signed or not:

Value	Description
YES	The system signs B2B invoices.
NO	The system does not sign B2B invoices.

   Note: The system always signs B2G invoices.

   - Use the `SignServiceAdapterAddress` parameter to configure the address of the signing integration flow. Normally you don't have to change this field. It is only required in case you are using your custom iFlow to sign invoices and notifications

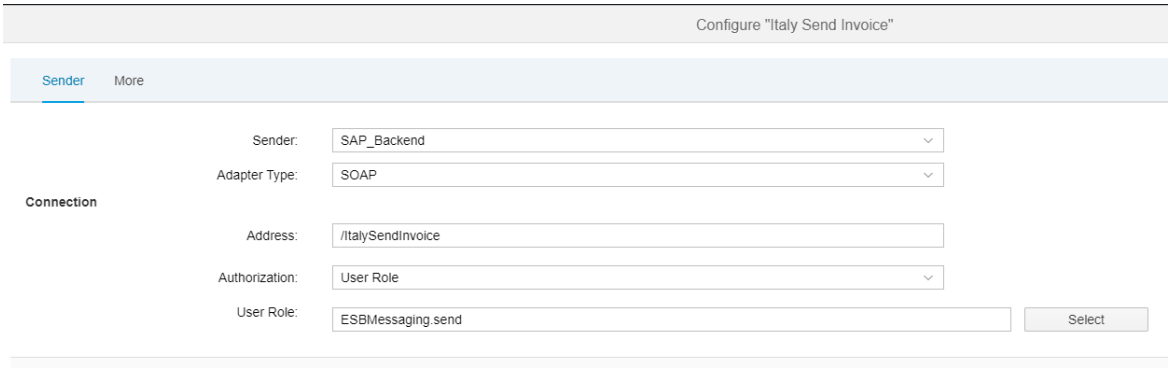


4. Choose *Configure* > *Sender* tab.
   - Use the `Address` parameter to set up the integration package address. Normally you don't have to change this field. In case you change the field, make sure to use the same address when configuring the logical ports in the next chapter.
   - Use the `Authorization`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

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

Value	Description
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.



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 messages can appear. You can ignore these messages by choosing *Close* . The first two warnings are related to the payload attachments; currently the invoice registration process does not support or require message attachments (for example, scanned copies of invoices) in any stage of processing and communication.

4.4 Creating Logical Ports in SOAMANAGER

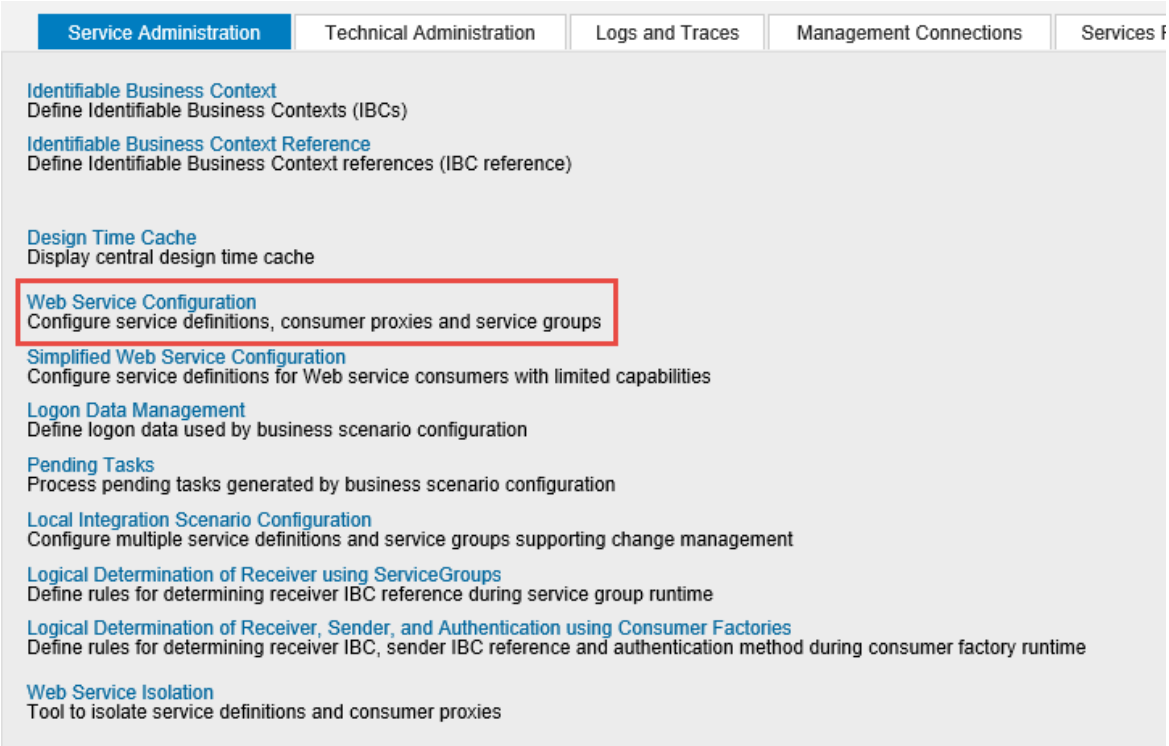
Context

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.

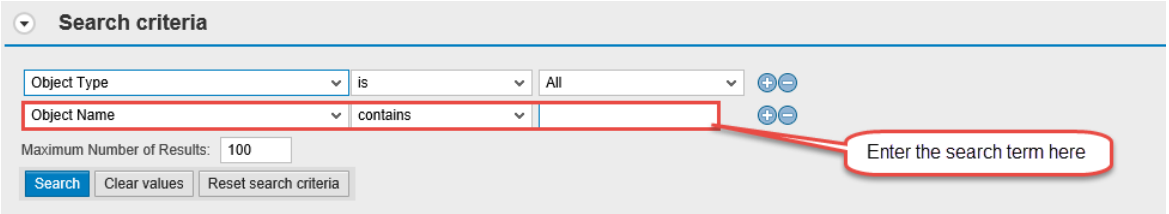
> **i Note**
>
> Depending on your release, the look-and-feel of the screens in your system may differ from the screenshots displayed below.

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 Italy with search term **`CO_EDO_IT*`**.



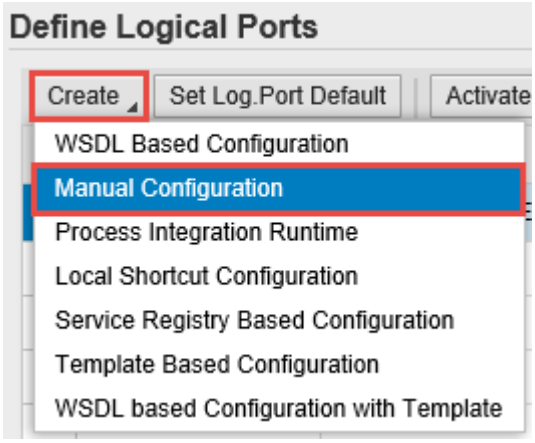
The following table lists the proxies and the logical port name, description and path for each proxy.

List of Proxies, Logical Port Names, and Paths

Proxy Name	Logical Port Name	Description	Path
CO_EDO_IT_RECEIVE_IN-VOICE_V1_0	EDO_IT_RECEIVE_IN-VOICE_DELETE	eDocument Italy - Delete In-voice	/cxf/ItalyDeleteInvoice
CO_EDO_IT_RECEIVE_IN-VOICE_V1_0	EDO_IT_RECEIVE_IN-VOICE_PULL	eDocument Italy – Pull In-voice	/cxf/ItalyPullInvoice
CO_EDO_IT_RECEIVE_NO-TIF_V1_0	EDO_IT_RECEIVE_NO-TIF_DELETE	eDocument Italy – Delete Notification	/cxf/ItalyDeleteNotification

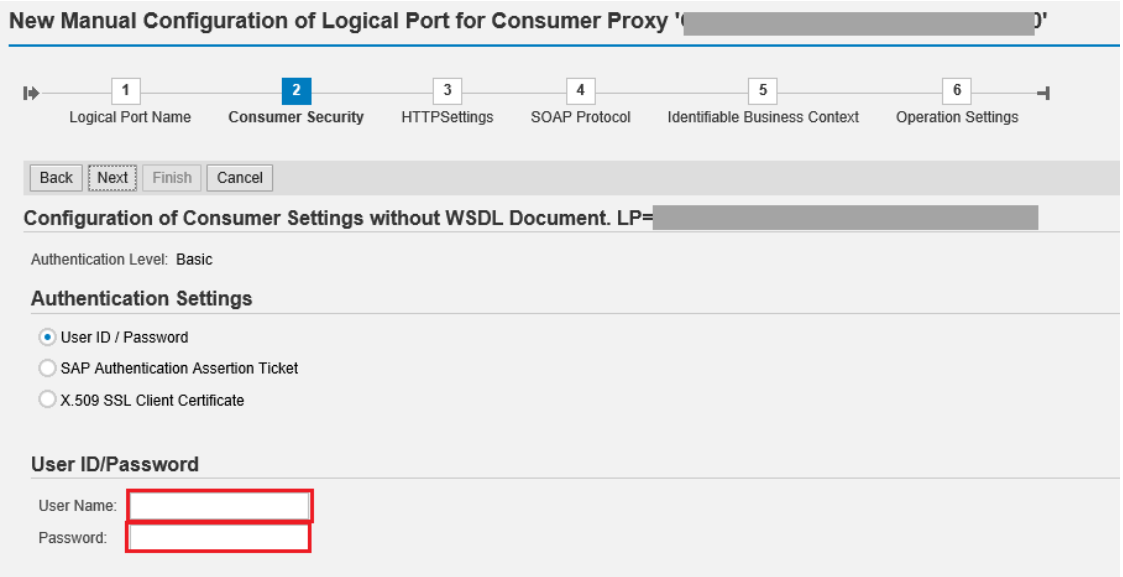
Proxy Name	Logical Port Name	Description	Path
CO_EDO_IT_RECEIVE_NOTIF_V1_0	EDO_IT_RECEIVE_NOTIF_PULL	eDocument Italy – Pull Notification	/cxf/ItalyPullNotification
CO_EDO_IT_SEND_INVOICE_V1_0	EDO_IT_SEND_INVOICE	eDocument Italy – Send Invoice	/cxf/ItalySendInvoice
CO_EDO_IT_SEND_NOTIF_V1_0	EDO_IT_SEND_NOTIF	eDocument Italy – Send Outcome Notification	/cxf/ItalySendOutcomeNotification

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*.



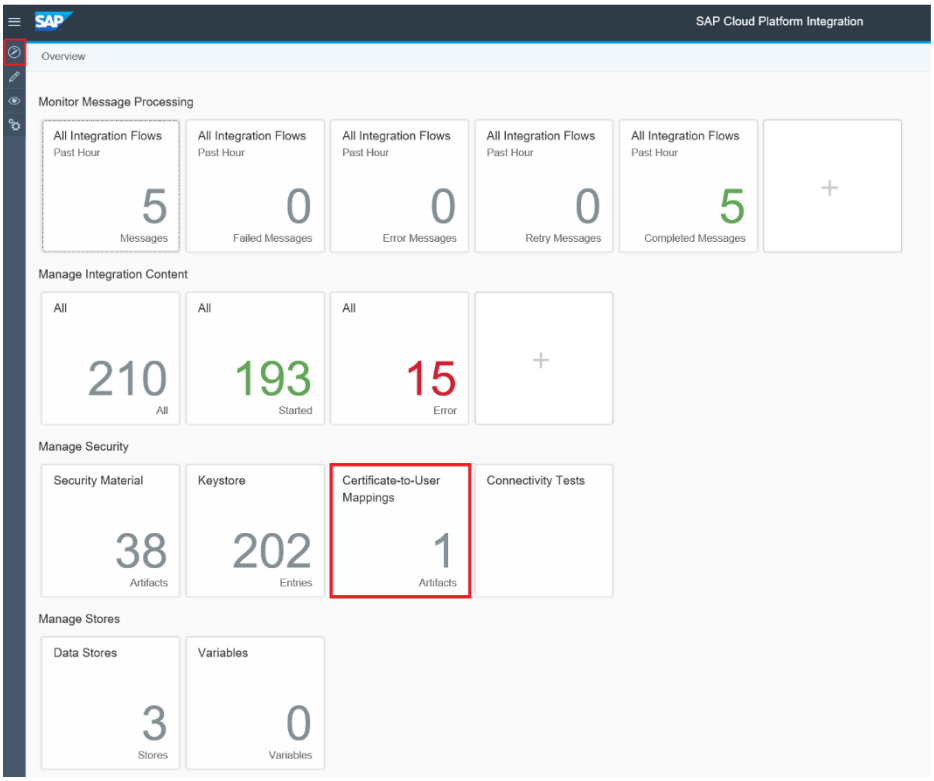
b. If you use certificate-based authentication, select *X.509 SSL Client Certification*. Ensure that the required certificates are available in the `STRUST` transaction.

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

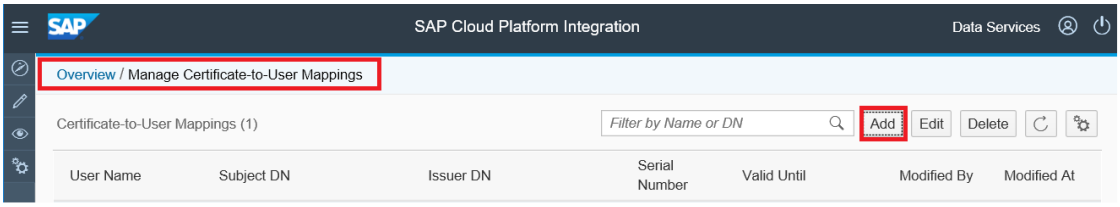
   Additionally, you map the certificate to a user of your tenant with the `ESBMessaging.send` role. First, you export the certifcate from the `STRUST` transaction. Save it locally and upload it to SAP Cloud Platform Integration in the `Certificate-to-User Mappings`

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

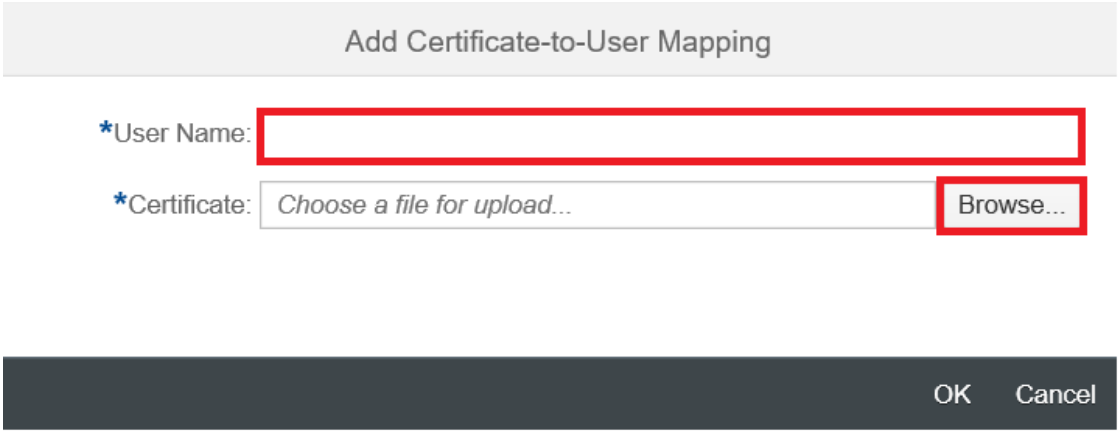
b. Got to SAP Cloud Platform Integration under *Overview* > *Certificate-to-User Mappings*



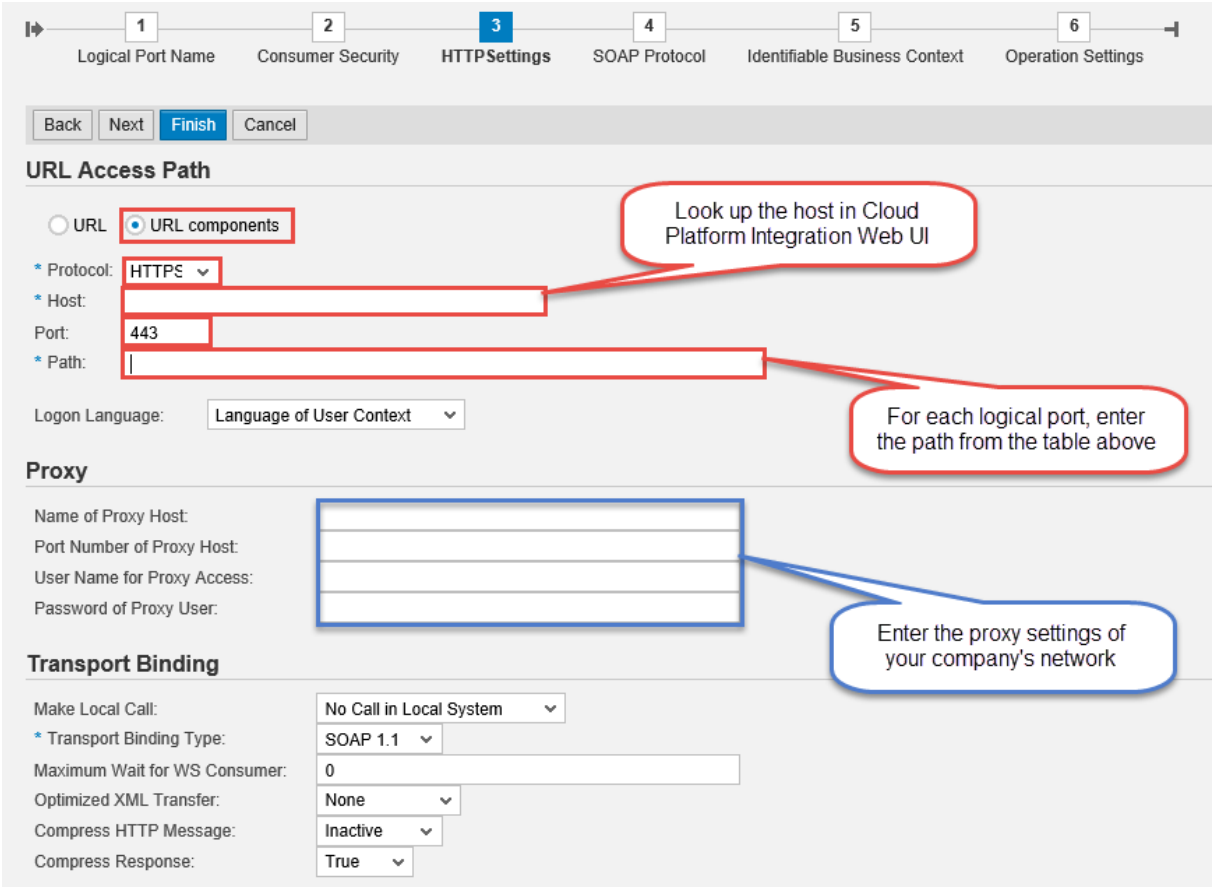
a. Choose *Add*.



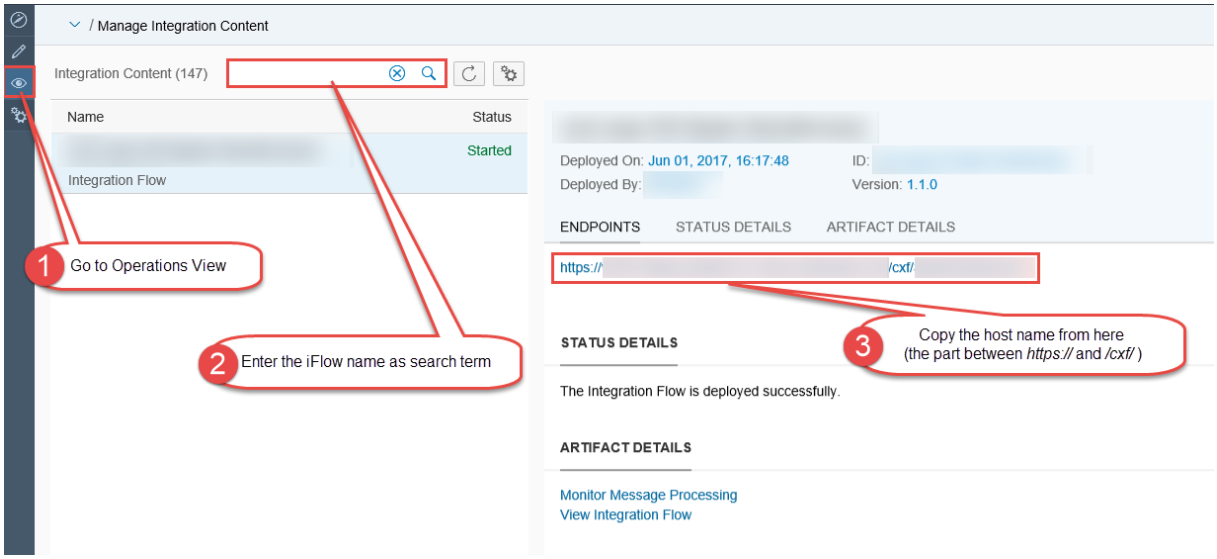
b. Enter a user name with `ESBMessaging.send role`, upload the `SSL Client PSE` of the `STRUST` transaction and choose *OK*.



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

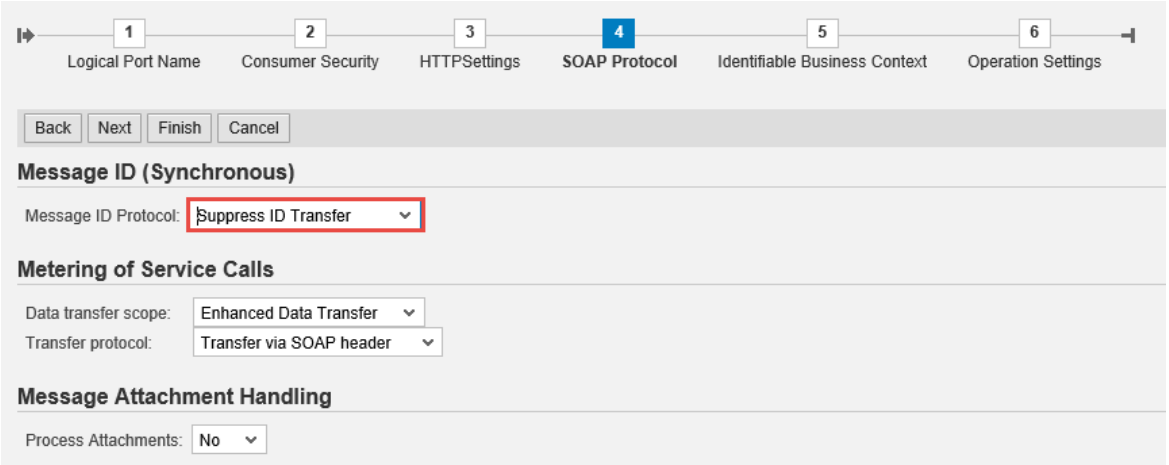


Port 443 is the standard port for the HTTPS protocol.
To find the Host, go to SAP Cloud Platform Integration Web UI and under Managed Integration Content, go to *Monitor* > *All*. Use the search to find your integration flow as in the screenshot below:



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

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 scenarion 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 tax authority's system.

Procedure

1. In the back-end system, go to the *eDocument Cockpit* (EDOC_COCKPIT) transaction, in the relevant process.
2. Select an eDocument and check the status of the eDocument in the Cockpit and perform the following actions, accordingly:
   a. If the status of the eDocument is `Created`, the eDocument was created but not submitted yet. In this case, select it and choose *Submit*. This action triggers the creation of the XML and the subsequent communication with SAP 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