



Integration Guide | PUBLIC
2024-03-21

Turkey Electronic Invoices and Delivery Notes: Setting Up SAP Integration Suite (SAP ERP, SAP S/4HANA) - Cloud Foundry environment

Content

- 1 Disclaimer. 3**
- 2 Introduction. 4**
- 3 Prerequisites. 5**
 - 3.1 Registration with the Tax Authorities and an Application Service Provider. 5
 - 3.2 Installation of eDocument Full Solution. 5
- 4 Connectivity Steps. 6**
 - 4.1 Setup of Secure Connection. 6
 - Set Up Your Tenants. 6
 - Retrieve and Save Public Certificates. 7
 - Upload the Certificates. 8
 - Authenticate Integration Flows. 8
- 5 Configuration Steps in SAP Integration Suite. 10**
 - 5.1 Deploy User Credentials. 10
 - 5.2 Copy Published Package. 11
 - 5.3 Deploy Integration Flows. 12
- 6 Configuration Steps in SAP ERP or SAP S/4HANA. 15**
 - 6.1 Create Logical Ports in SOAMANAGER. 15

1 Disclaimer

This documentation refers to links to Web sites that are not hosted by SAP. By using such links, you agree (unless expressly stated otherwise in your agreements with SAP) to this:

- The correctness of the external URLs is the responsibility of the host of the Web site. Please check the validity of the URLs on the corresponding Web sites.
- The content of the linked-to site is not SAP documentation. You may not infer any product claims against SAP based on this information.
- SAP does not agree or disagree with the content on the linked-to site, nor does SAP warrant the availability and correctness. SAP shall not be liable for any damages caused by the use of such content unless damages have been caused by SAP's gross negligence or willful misconduct.

2 Introduction

You use SAP Integration Suite to establish the communication with your service provider and transfer to them the electronic tax invoices in XML format you have created using the SAP Document and Reporting Compliance solution. This document lists the required setup steps you must perform in your SAP S/4HANA system and SAP Integration Suite tenant so that the integration between the systems works.

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

ⓘ Note

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

ⓘ Note

This document describes functionality that is provided by the Integration Package itself, that is, by the artifacts that are deployed in the SAP Integration Suite tenant. It may happen, however, that in the SAP S/4HANA system 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 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.

3.1 Registration with the Tax Authorities and an Application Service Provider

You must ensure the following:

- You have completed registration with the tax authorities (TRA) for the invoice and delivery note scenarios.
- You have completed registration with an application service provider for the invoice and delivery note scenarios.

The application service provider issues user credentials (username and password) for your VKNs. You need to configure these user credentials on your tenant. In addition, you need to get service URLs from your application service provider and configure them in integration flows.

You can find application service providers who are in partnership with SAP from [SAP App Center](#) . Search with the keyword **SAP Document and Reporting Compliance**.

3.2 Installation of eDocument Full Solution

The eDocument Full solution is installed in your test and production systems.

- For the generic part, refer to the Installation Guide for eDocument attached to SAP Note [2134248](#) .
- For the invoice scenario, refer to the SAP Notes under the *Full Solution* section in SAP Note [2214845](#) .
- For the delivery note scenario, refer to the SAP Notes under the *Full Solution* section in SAP Note [2711030](#) .

4 Connectivity Steps



4.1 Setup of Secure Connection

You establish a trustworthy SSL connection to set up a connection between the SAP back-end systems and the SAP Integration Suite. For more information, see [Connecting a Customer System to Cloud Integration](#).

Outbound HTTP connections are required, and are supported with specific, public certificates.

You use SAP ERP Trust Manager (transaction `STRUST`) to manage the certificates required for a trustworthy SSL connection. The certificates include public certificates to support outbound connections, as well as trusted certificate authority (CA) certificates to support integration flow authentication.

Refer to the system documentation for more information regarding the certificate deployment to SAP back-end systems. In case of issues, refer to the following SAP notes:

- [2368112](#)  Outgoing HTTPS connection does not work in AS ABAP
- [510007](#)  Setting up SSL on Application Server ABAP

For more information, see [Operating and Monitoring Cloud Integration](#).

Note

If you encounter any issues in the information provided in the SAP Integration Suite product page, open a customer incident against the `LOD-HCI-PI-OPS` component.

Client Certificate

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

For information about creating your own certificate and get it signed by a trusted certificate authority (CA), see [Authenticate Integration Flows \[page 8\]](#).

4.1.1 Set Up Your Tenants

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](#).

📘 Note

The SAP Document and Reporting Compliance solution requires the **Cloud Integration capability**. You need to activate this capability in the step **Provisioning the Capabilities**.

4.1.2 Retrieve and Save Public Certificates

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

Prerequisites

If you do not find any integration flows in your tenant then refer to and .

Context

Find and save the public certificates from your SAP Integration Suite runtime.

Procedure

1. Access the SAP BTP cockpit, and navigate to your subaccount (tenant) page.
2. Click the subscriptions link to display the subscriptions for your subaccount.
3. Use the tenant URL you created as defined in the prerequisites of this document. The URL has the following format: **https://<tenant>.cfapps.<data center>.hana.ondemand.com**, where <tenant> corresponds to the dynamic part and is unique for each subaccount and <data center> corresponds to the data center you are using.
4. In the *Operations* view, choose *Manage Integration Content* and select *All* to display the integration flows available.
5. Select an integration flow to display its details.
6. Copy the URL listed within the *Endpoints* tab, and paste the URL into your web browser.
7. When prompted by the *Website Identification* window, choose *View certificate*.
8. Select the root certificate, and then choose *Export to file* to save the certificate locally.
9. Repeat these steps for each unique root, intermediate and leaf certificate, and repeat for both your test and production tenants.

4.1.3 Upload the Certificates

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

Context

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

Procedure

1. Access transaction `STRUST`.
2. Navigate to the PSE for **SSL Client (Anonymous)** and open it by double-clicking the PSE.
3. Switch to edit mode.
4. Choose the *Import certificate* button.
5. In the *Import Certificate* dialog box, enter or select the path to the required certificates and choose *Enter*. The certificates are displayed in the *Certificate* area.
6. Choose *Add to Certificate List* to add the certificates to the *Certificate List*.
7. Save your entries.

4.1.4 Authenticate Integration Flows

Create an own certificate and get it signed by a trusted certificate authority (CA) to support integration flow authentication.

Context

You use the SAP ERP Trust Manager (transaction `STRUST`) for this purpose.

This process is required only if you use certificate-based authentication (that is, you choose the **x.509 SSL Client Certification** option in your settings for SOAMANAGER).

Procedure

1. Access transaction `STRUST`.

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

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

The CA may have specific requirements and request company-specific data, they may also require time to analyze your company before issuing a signed certificate. When signed, the CA provides the certificate for import.

5. Navigate to the PSE for **SSL Client Standard** and open it by double-clicking the PSE.
6. Switch to edit mode.
7. Choose the *Import certificate* button.
8. In the *Import Certificate* dialog box, enter or select the path to the CA-signed certificate and choose *Enter*. The certificate is displayed in the *Certificate* area.
9. Choose *Add to Certificate List* to add the signed certificate to the *Certificate List*.

Ensure that you import the CA root and intermediate certificates to complete the import.

10. Save your entries.

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

5 Configuration Steps in SAP Integration Suite

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

5.1 Deploy User Credentials

You must deploy the user credentials that you've got from your application service provider to the SAP Integration Suite tenant.

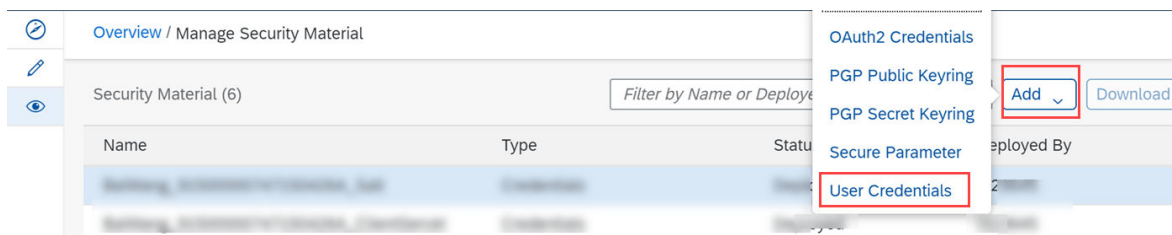
Note

User credentials for the delivery note scenario and invoices scenario may vary.

Procedure

To configure a pair of credentials (username and password), follow the steps below:

1. Log into your SAP Integration Suite tenant.
2. Go to *Monitor* (Operations view) and open the *Security Material* app.
3. Click *Add* on the top right corner of the browser window. Select *User Credentials*.



An *Add User Credentials* dialog box appears.

Add User Credentials

***Name:**

Description:

***Type:** ▼

***User:**

Password:

Repeat Password:

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

4. In the *Name* field, create a name for your credentials.
5. In the *User* field, enter the user name.
6. In *Password* field, enter the password.
7. In the *Repeat Password* field, repeat the password.
8. Choose *Deploy*.

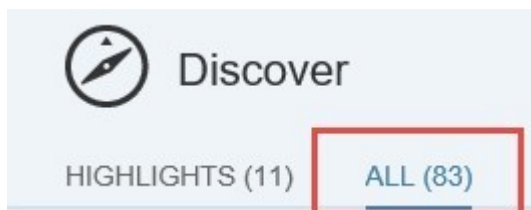
5.2 Copy Published Package

Context

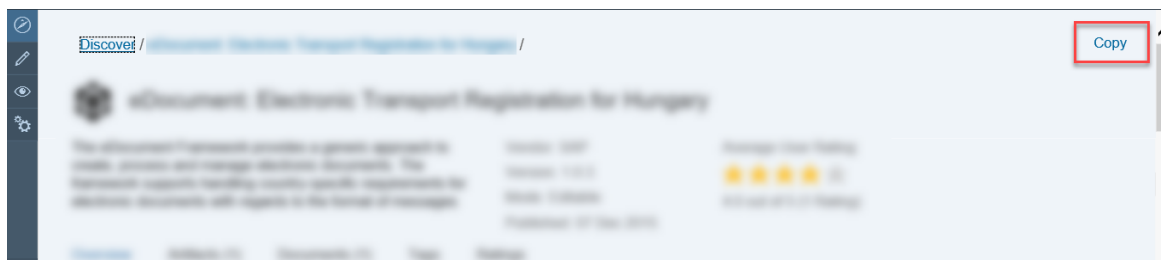
Copy the package *SAP Document and Reporting Compliance: Electronic Invoices and Delivery Notes for Turkey* to the target tenant as follows:

Procedure

1. Log in to your SAP Integration Suite tenant.
2. Choose **Discover** > **All** > .



3. Search for *SAP Document and Reporting Compliance: Electronic Invoices and Delivery Notes for Turkey*.
4. Select the package and choose *Copy*.



5.3 Deploy Integration Flows

Context

The following integration flows are available in the integration package *SAP Document and Reporting Compliance: Electronic Invoices and Delivery Notes for Turkey*:

Integration Flow	Explanation
Turkey Invoice via Any Service Provider	Deploy this integration flow if you want to use a service provider other than Foriba .
Turkey eArsiv via Any Service Provider	Deploy this integration flow if you want to send electronic consumer invoices via a service provider other than Foriba .
<div style="border: 1px solid #ccc; padding: 5px; background-color: #f9f9f9;"> <p>Note</p> <p>To send electronic consumer invoices via a service provider other than Foriba, you must deploy both the Turkey Invoice via Any Service Provider and Turkey eArsiv via Any Service Provider integration flows.</p> </div>	
Turkey Invoice via Specific Service Provider	Deploy this integration flow if you want to send and receive electronic invoices via the service provider Foriba .
Turkey Delivery Note via Any Service Provider	Deploy this integration flow if you want to send and receive electronic delivery notes via a service provider other than Foriba .
Turkey Delivery Note via Specific Service Provider	Deploy this integration flow if you want to send and receive electronic delivery notes via the service provider Foriba .

For each integration flow, you must configure several parameters as described below:

Procedure

1. Open the integration package that you copied.
2. Go to the *Artifacts* tab page.
3. Choose **► Actions ► Configure ▾** for the integration flow you want to configure.
4. Choose the *Sender* tab. Make the following settings:
 - In the *Address* field, keep the default address or enter a custom sender address. If you have multiple company codes, instead of copying the integration package for each company code, you may want to copy an integration flow for each company code. In this case, to differentiate the sender addresses for different company codes, you can define custom, company code-specific sender addresses.
 - From the *Authorization* dropdown list, select an authorization type. The available options are:

Authorization Type	Description
<i>User Role</i>	Select this authorization type if you want to use basic authentication (user/password) or client certificate authentication with Certificate-to-User-Mapping.
<i>Client Certificate</i>	Select this authorization type if you want to use client certificate authentication without Certificate-to-User-Mapping. For more information, see Cloud Integration – How to Setup Secure Outbound HTTP Connection using Key-store Monitor .

See the following example:

The screenshot shows the configuration interface for a sender. At the top, there are tabs for 'Sender', 'Receiver', and 'More'. The 'Sender' tab is selected. Below the tabs, the 'Connection' section is visible, containing the following configuration fields:

- Sender: Sender
- Adapter Type: SOAP
- Address: /Turkey/Inposia/eDelivery
- User Role: ESBMessaging.send

5. Choose the *Receiver* tab. Make settings as follows:
 - In the *Address* field, enter the service URL that you got from your service provider.
 - In the *Credential Name* field, enter the name of the credential that you deployed to your tenant (see [Deploy User Credentials \[page 10\]](#)).

Sender **Receiver** More

Connection	Receiver:	ServiceProvider
	Adapter Type:	SOAP
	Address:	https://sapservice-test.elogo.com.tr/SAPEDeliveryService.svc
	Authentication:	Basic
	Credential Name:	GEN_Elogo_credential

In More Tab, you can add External Namespace which are required by the Service provider, for Example for eLogo- <http://www.sap.com/eDocument/DeliveryNote/V1.0/>

Also add SP_ADAPTER_TYPE as SOAP, if you are working for eLogo.

- In **More** tab, you can add External Namespace which is required by the Service provider, for Example for eLogo- <http://www.sap.com/eDocument/DeliveryNote/V1.0/>. Add SP_ADAPTER_TYPE as SOAP, if you are working for eLogo.

Example for eLogo: <http://www.sap.com/eDocument/DeliveryNote/V1.0/>

Sender Receiver **More**

Type:	All Parameters
external namespace:	http://www.sap.com/eDocument/DeliveryNote/V1.0/
SP_Adaptor_Type:	SOAP

- Choose **Deploy** to deploy it to the server.

6 Configuration Steps in SAP ERP or SAP S/4HANA

Some steps are required in your SAP ERP or SAP S/4HANA system.

6.1 Create Logical Ports in SOAMANAGER

Context

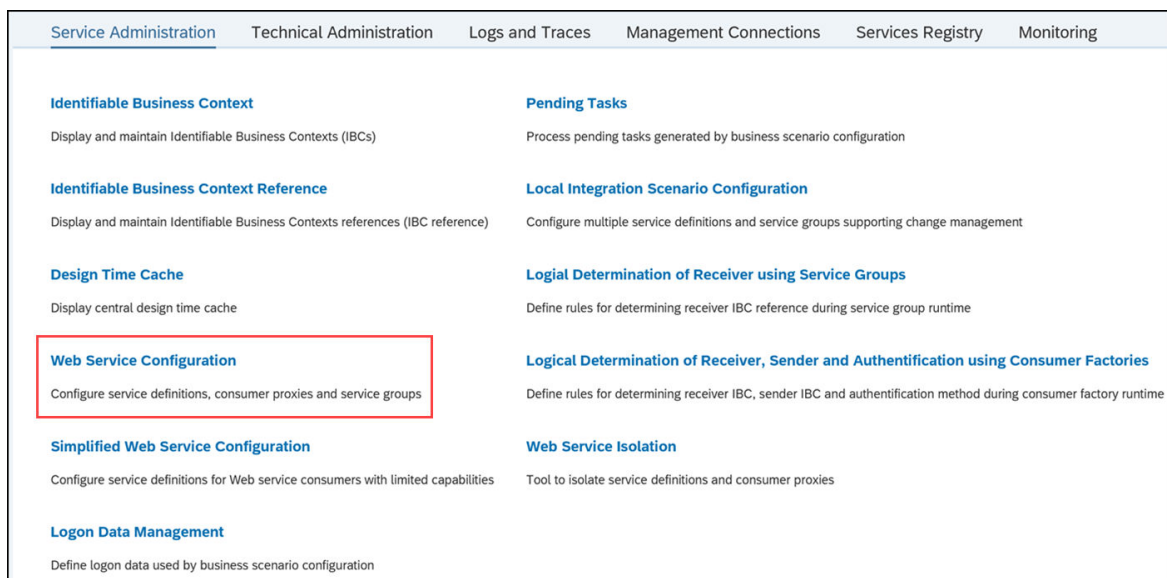
You connect the required proxies to your SAP Integration Suite tenant via logical ports. In a test SAP ERP or SAP S/4HANA system, you configure the logical ports to connect to your test SAP Integration Suite tenant. In a productive SAP ERP or SAP S/4HANA system, you configure the logical ports to connect to your productive SAP Integration Suite tenant.

Note

Depending on your product version, the look and feel of the screens in your system may differ from the screenshots in this document.

Procedure

1. Call up transaction SOAMANAGER. Choose *Web Service Configuration*.



- Search for the proxies for Turkey with the search criterion **object name containing CO_EDO_TR***.

The following proxies appear in the search results:

Proxy Name	Description
CO_EDO_TR_CLIENT_EDESPATCH_SER	Turkey Delivery Note Services
CO_EDO_TR_CLIENT_EINVOICE_SERV	Turkey elnvoice: eFactura
CO_EDO_TR_CONS_INV_TRANSM_SERV	Turkey elnvoice: eArsiv
CO_EDO_TR_CLIENT_EINVOICE_SER1	Turkey elnvoice: Get User List

Note

If you want to implement eFactura, you should create a logical port for both the CO_EDO_TR_CLIENT_EINVOICE_SERV and CO_EDO_TR_CLIENT_EINVOICE_SER1 proxies.

- Select a proxy and create a logical port for it. Choose **Create** > **Manual Configuration**.

The screenshot shows the 'Define Logical Ports' configuration screen. At the top, there are tabs for 'Overview', 'Configurations', and 'Details'. Below the tabs, there are several buttons: 'Create' (with a dropdown arrow), 'Set Log.Port Default', 'Activate', 'Deactivate', and 'Delete'. The 'Create' dropdown menu is open, showing a list of configuration options: 'WSDL Based Configuration', 'Manual Configuration' (highlighted with a red box), 'Process Integration Runtime', 'Local Shortcut Configuration', 'Service Registry Based Configuration', 'Template Based Configuration', and 'WSDL based Configuration with Template'. Below the dropdown, there is a table with columns for 'State' and 'Logical Port'.

- Enter a logical port name and description. Choose **Next**.

Note

Ensure that the logical port configurations correspond to the settings you made when setting up SAP Application Interface Framework as described in the attachments of the following SAP Notes:

- SAP Note [2214857](#) for electronic invoices
- SAP Note [2744568](#) for electronic delivery notes

5. On the *Consumer Security* tab, make authentication settings. Choose *Next*.

The authentication settings depend on the authentication level of the communication between your SAP ERP or SAP S/4HANA system and SAP Integration Suite. Proceed as follows:

- If you use the basic authentication, select *User ID / Password*. Enter the value of your `clientid` in the *User Name* field, and the value of your `clientsecret` in the *Password* field. You create these values for your service instance in SAP Integration Suite. For more information, see [Creating Service Instances](#).

- If you use certificate-based authentication, select *X.509 SSL Client Certification* and choose the certificate you have uploaded to `STRUST`. You must configure this certificate in SAP Integration Suite too. For that you create a service instance using the required `grant_type`. You create the service key using the certificate uploaded to the `STRUST`. For more information, see [Defining a Service Key for the Instance in the Cloud Foundry Environment](#).

Note

If you do not see this option or cannot select it, check SAP Note [2368112](#) and SAP Note [510007](#).

- On the *HTTP Settings* tab, select the *URL components* radio button and make the following settings:

Setting	Remark
<i>Protocol</i>	Select <i>HTTPS</i> .
<i>Host</i>	Enter the host name of the integration flow that you want to communicate with.
<i>Port</i>	Enter 443 , which is the standard port for the HTTPS protocol.
<i>Path</i>	Find the path of the related integration flow from your SAP Integration Suite tenant.
<i>Proxy</i>	Enter the information about your company's network proxy.

You can find the host name and path of an integration flow, as follows:

- From the menu on the left, choose *Monitor*.
- Select *Manage Integration Content* (All).
- Search for the integration flow.
- Find the host name and path from the endpoint URL on the *Endpoints* tab.
The composition of an endpoint URL is **https://<host name>/<path>**.

The screenshot shows the 'Endpoints' tab in the SAP Integration Suite interface. The 'Endpoints' tab is selected, and the following table is displayed:

Endpoints	Status Details	Artifact Details	Log Configuration
<code>https://<host name>/<path></code>			
WSDL			
WSDL without policies			

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

8. No settings are required on the *Identifiable Business Context* tab. Choose *Next*.
9. No settings are required on the *Operation Settings* tab. Choose *Finish*.

Note

SAP Integration Suite does not support WebService Pin for testing your configuration.

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



10. Remember to create logical ports for each proxy and to execute the following steps in the SAP back-end systems, see SAP Note [2683318](#) for more information.
 - Define the SOA service names and assign the logical ports to the combination of a SOA service name and a company code in the `EDOSOASERV` view.
 - Assign the SOA service names you created before to an interface ID in the `EDOINTV` view.

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.

© 2024 SAP SE or an SAP affiliate company. All rights reserved.

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

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

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

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

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