Configuration Guide
CSSZAPEP
Document Version: 1.0 – 2019-10-23

CUSTOMER

Human Experience Management solutions from SAP Integration with Czech Social Security Administration

Using Web Services with SAP Cloud Platform Integration

Typographic Conventions

Type Style	Description
Example	Words or characters quoted from the screen. These include field names, screen titles, pushbuttons labels, menu names, menu paths, and menu options. Textual cross-references to other documents.
Example	Emphasized words or expressions.
`EXAMPLE`	Technical names of system objects. These include report names, program names, transaction codes, table names, and key concepts of a programming language when they are surrounded by body text, for example, SELECT and INCLUDE.
`Example`	Output on the screen. This includes file and directory names and their paths, messages, names of variables and parameters, source text, and names of installation, upgrade and database tools.
`Example`	Exact user entry. These are words or characters that you enter in the system exactly as they appear in the documentation.
`<Example>`	Variable user entry. Angle brackets indicate that you replace these words and characters with appropriate entries to make entries in the system.
`EXAMPLE`	Keys on the keyboard, for example, `F2` or `ENTER`.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Document History

Version	Date	Change
1.0	2019-10-23	Initial version

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Contents

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

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 Human Experience Management solutions from SAP for Czech Republic. This document lists the required setup steps you perform in the SAP ERP or SAP SuccessFactors Employee Central Payroll and the SAP Cloud Platform Integration tenant so that the integration between the systems work.

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.

> **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 Czech Social Security Administration 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 Czech Social Security Administration 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 SuccessFactors Employee Central Payroll.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

2 Prerequisites

2.1 Installation of 'APEP for SCPI' Solution

You installed and configured the "APEP for SCPI" solution in your test and productive SAP ERP or SAP SuccessFactors Employee Central Payroll systems. If you did not install the latest support package for your system, refer to the latest SAP Note with latest improvements of "APEP for SCPI" solution.

> **Note**
>
> *Minimal SAP Notes which need to be in SAP ERP or SAP SuccessFactors Employee Central Payroll systems to be able to complete all configurations steps described in this guide are following:*
> *2832073 - HRCZ - APEP for SCPI - November 2019 [1] - SPROXY*
>
> *2836189 - HRCZ - APEP for SCPI - November 2019 [2] - Source code*
>
> *Recommended SAP Notes are latest SAP Notes for 'APEP for SCPI' solution.*

2.2 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.

Inbound HTTPS connections are not required for Czech Republic. Outbound HTTPS connections are required and are supported with specific public certificates.

You use the 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 the "Operations guide for SAP Cloud Platform Integration."

> **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.*

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

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.

2.3 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).

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.

2.4 Czech Social Security Administration Public Key Certificate

The actual Czech Social Security Administration public key certificate is published on CSSZ's web page at: *Služby pro vás → Předávání předepsaných tiskopisů (e-Podání) → Ke stažení → Šifrovací certifikát ČSSZ*

2.5 Czech Social Security Administration SSL Certificate

The actual Czech Social Security Administration SSL certificate for HTTPS communication is published on CSSZ's web page at : *Služby pro vás → Předávání předepsaných tiskopisů (e-Podání) → Ke stažení → SSL certifikáty VREP / APEP → Certifikát epodani.cssz.cz.*

> **Note**
>
> *Certificate for t-epodani.cssz.cz is for use by software vendors (not for use on the customer's test system).*

2.6 Qualified System Certificate

More information about the required type of certificate is published on CSSZ's web page at: *Služby pro vás → Předávání předepsaných tiskopisů (e-Podání) → Informace pro SW vývojáře → Elektronický podpis* .

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

> **Note**
>
> *The customer's certificate used by this solution is the* `qualified system certificate`*. Because the certified documents will be sent automatically, the qualified system certificate is the certificate which should be used in such a case.*

The qualified system certificate must be registered at the Czech Social Security Administration. More information about this registration is published on CSSZ's web page at: *Služby pro vás → Předávání předepsaných tiskopisů (e-Podání) → Základní informace → Registrace na okresní správě sociálního zabezpečení k e - Podání za zaměstnavatele (zasílanému s uznávaným elektronickým podpisem prostřednictvím VREP/APEP).*

> **Note**
>
> *Remind the client that only one qualified certificate is required to receive e-submission for multiple variable symbols and/or multiple e-submission services. More information is published at CSSZ's web page under Služby pro vás → Tiskopisy → Tiskopisy určené pro pověřování jiných subjektů k eSlužbám ČSSZ.*

2.7 Encryption Certificate for DZDPN Notification

According to information published on CSSZ's web page at: *Služby pro vás → Předávání předepsaných tiskopisů (e-Podání) → Informace pro SW vývojáře → Definice jednotlivých druhů e - Podání → Speciální e - Podání DZDPN eNeschopenky → Komentovaný popis rozhraní pro zaměstnavatele pro získání dat z eNeschopenky is in chapter 3.2 APEP služba pro elektronická podání* must encrypt the certificate for "Data related to temporary sick leave for employer" notification (DZDPN) and fulfill following requirement:

- As an encryption certificate, it is possible to use a certificate that meets the minimum requirements of NÚKIB:https://www.nukib.cz/en/uredni-deska/ from 28.11.2018.

  > **Note**
  >
  > *The information above mentioned is the responsibility of the Czech Social Security Administration (CSSZ). SAP cannot be made liable for its correctness and accuracy.*

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

3 Configuration Steps in SAP Cloud Platform Integration

3.1 General Information

The package Human Experience Management solutions from SAP Integration with CSSZ APEP for Czech Republic contains the following iFlows:

iFlow Name in WebUI	Project Name/Artifact Name
Data Request	com.sap.GS.HR.CZ.APEP.DataRequest
Dispose	com.sap.GS.HR.CZ.APEP.Dispose
Poll	com.sap.GS.HR.CZ.APEP.Poll
Submit	com.sap.GS.HR.CZ.APEP.Submit

3.2 Deploying Key Pairs and Certificates

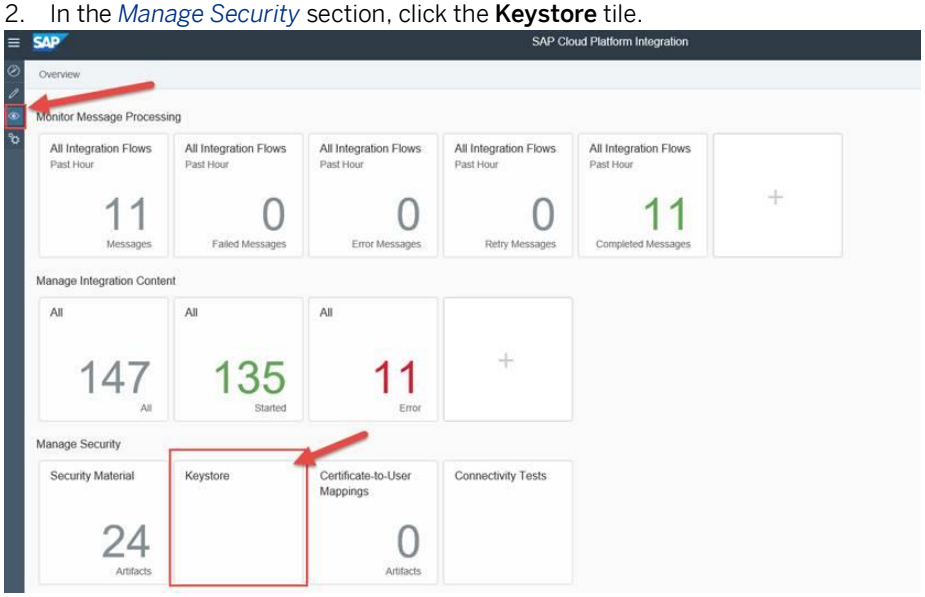
You deploy the key pairs and certificates to the SAP Cloud Platform Integration tenants.

3.2.1 Uploading of Czech Social Security Administration Public Key Certificate to Keystore

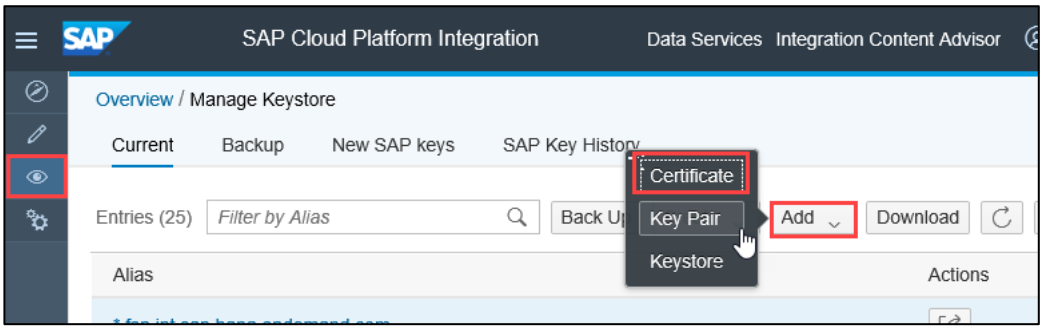
1. In the CPI, open the *Overview* section.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

2. In the *Manage Security* section, click the **Keystore** tile.



3. Click the *Add* button and select **Certificate**.



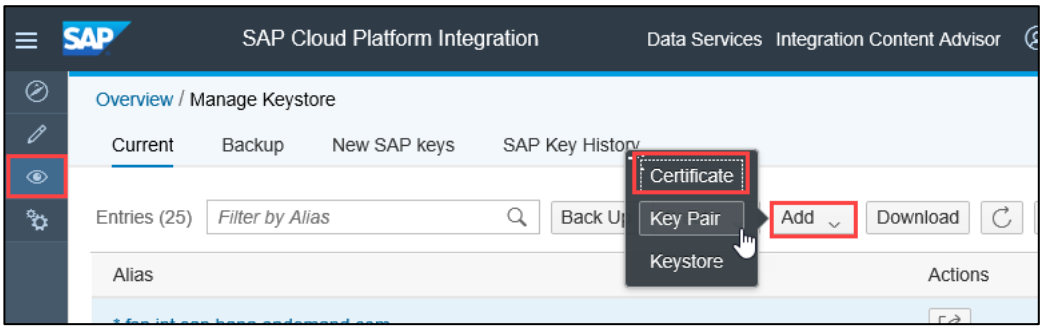
4. In the pop-up window, enter the **Alias** for the Key Pair (e.g. `cssz_public_key`). Then select the file with the Czech Social Security Administration Public Key Certificate. The file with certificate should be in CRT or CER format.

> **Note**
>
> *Same Czech Social Security Administration Public Key Certificate is also used for verification of signature when final status of submission is received.*

3.2.2 Uploading of Czech Social Security Administration SSL Certificate to Keystore

1. In the CPI, open the *Overview* section.
2. In the *Manage Security* section, click the **Keystore** tile.
3. Click the *Add* button and select **Certificate**.

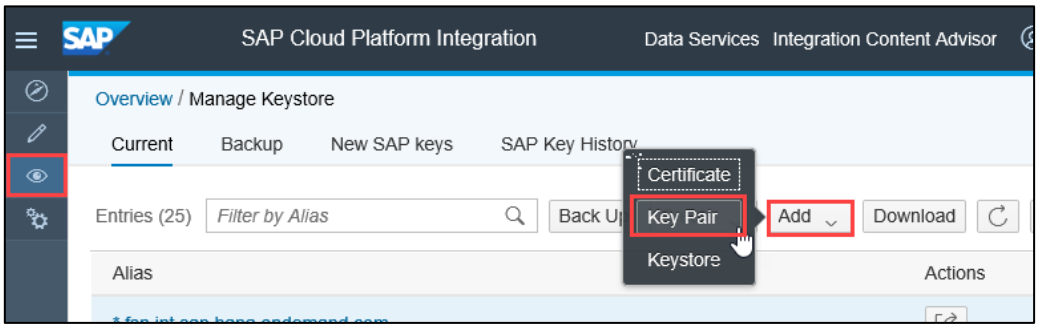
© 2016 SAP SE or an SAP affiliate company. All rights reserved.



4. In the pop-up window, enter the **Alias** for the Key Pair (e.g. `epodani_cssz_cz`). Then select the file with Czech Social Security Administration SSL Certificate. The file with the certificate should be in CRT or CER format.

3.2.3 Uploading of Qualified System Certificate to Keystore

1. In the CPI, open the *Overview* section.
2. In the *Manage Security* section, click the **Keystore** tile.
3. Click the *Add* button and select **Key Pair**.

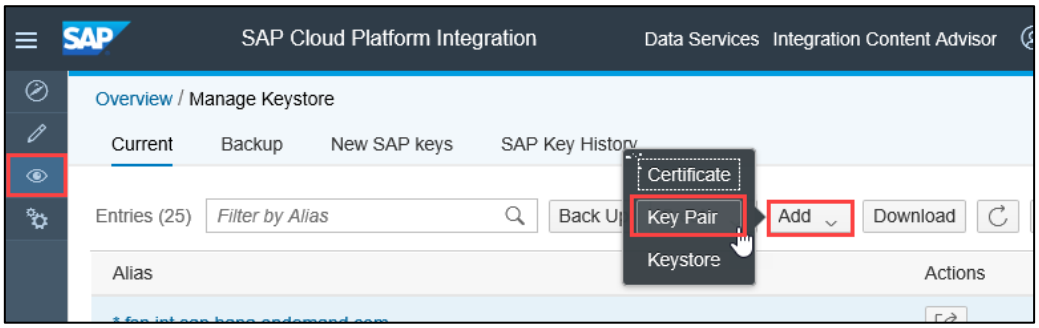


4. In the pop-up window, enter the **Alias** for the Key Pair (e.g. `customer_key_pair`). Then select the file with *Qualified System Certificate*. The file with the certificate should be in P12 or PFX format. Enter the corresponding password for this file in **Password** field.

3.2.4 Uploading of Encryption Certificate for DZDPN Notification to Keystore

1. In the CPI, open the *Overview* section.
2. In the *Manage Security* section, click the **Keystore** tile.
3. Click the *Add* button and select **Key Pair**.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

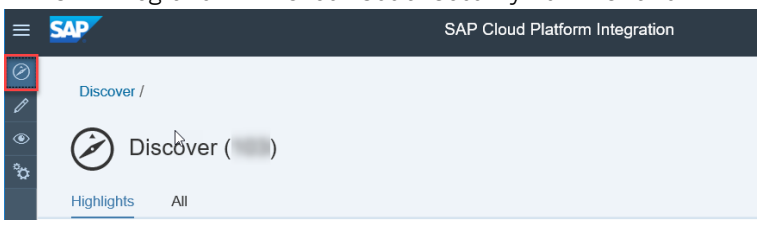


4. In the pop-up window, enter the **Alias** for the Key Pair (e.g. `dzdpn_key_pair`). Then select the file with Encryption Certificate for DZDPN Notification. The file with the certificate should be in P12 or PFX format. Enter the corresponding password for this file in **Password** field.

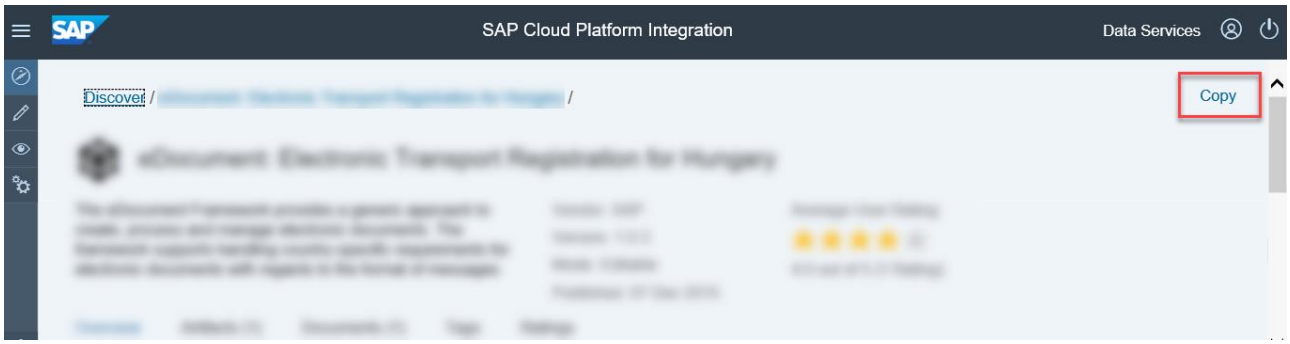
> **Note**
>
> *The public part of the Encryption Certificate for DZDPN Notification will be sent to the Czech Social Security Administration as part of the DZDPN request. The DZDPN response from the Czech Social Security Administration will be encrypted with the provided public certificate and the private part will be used for decryption.*

3.3 Copy Published Integration Package

1. In the *Discover* section of your tenant, select the package Human Experience Management solutions from SAP Integration with Czech Social Security Administration.



2. Select the package and click *Copy* in the upper right corner.



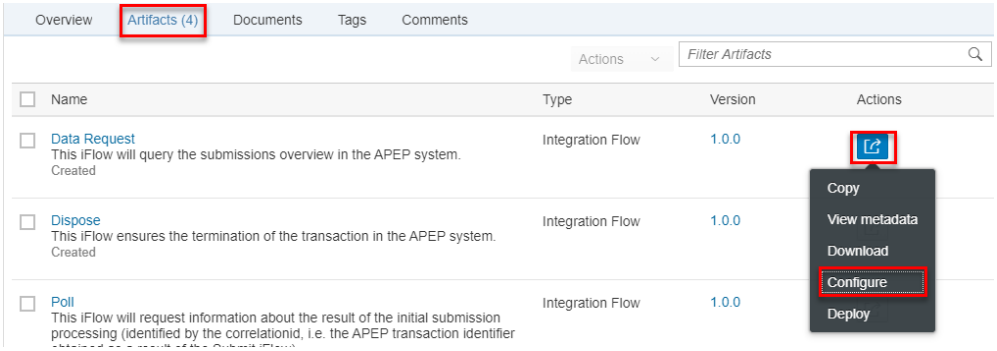
© 2016 SAP SE or an SAP affiliate company. All rights reserved.

3.4 Configure Integration Flows

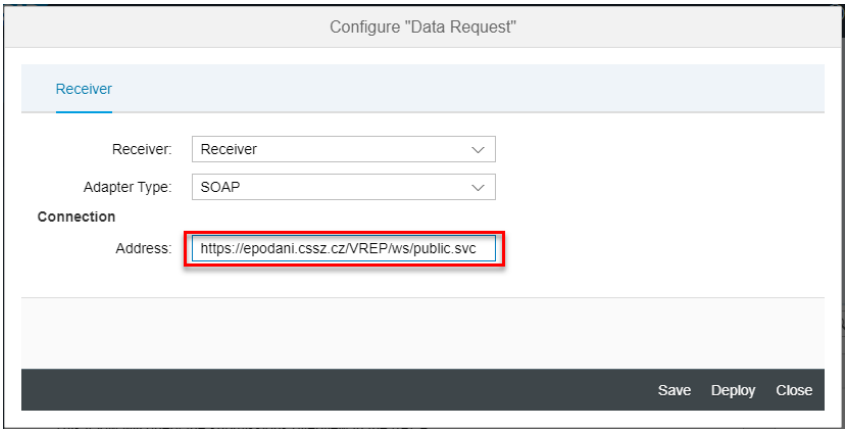
> **Note**
>
> *The following steps must be executed for the package that was copied as described in chapter 3.3.*

3.4.1 Configuration of Data Request iFlow

1. Go to the integration package that was copied from the original Human Experience Management solutions from SAP Integration with Czech Social Security Administration.
2. Click the *Artifacts* tab
3. Click on the *Actions* button that corresponds to integration flow **Data Request** and choose **Configure**



4. Click the *Receiver* tab
5. Fill the URL for productive APEP (it's described on the same web page as the SSL certificates - see Chapter 2.5) as value for *Address* field (e.g. `https://epodani.cssz.cz/VREP/ws/Public.svc`)



6. Select *Deploy*.

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

3.4.2 Configuration of Dispose iFlow

1. Go to the integration package that was copied from the original Human Experience Management solutions from SAP Integration with Czech Social Security Administration
2. Click the *Artifacts* tab
3. Click on *Actions* button that corresponds to integration flow **Dispose** and choose **Configure**
4. Click the *Receiver* tab
5. Fill URL for productive APEP (it's described on the same web page as SSL certificates - see Chapter 2.5) as value for *Address* field (e.g. `https://epodani.cssz.cz/VREP/ws/Public.svc`)
6. Select *Deploy*

3.4.3 Configuration of Poll iFlow

1. Go to the integration package that was copied from the original Human Experience Management solutions from SAP Integration with Czech Social Security Administration.
2. Click the *Artifacts* tab
3. Click on *Actions* button that corresponds to integration flow **Poll** and choose **Configure**
4. Click the *Receiver* tab
5. Fill URL for productive APEP (it's described on a same web page as SSL certificates - see Chapter 2.5) as value for *Address* field (e.g. `https://epodani.cssz.cz/VREP/ws/Public.svc`)
6. Click the *More* tab
7. Fill the alias of the public certificate which is used for signature verification by Czech Social Security Administration as value for *verify_cert_alias* field (e.g. `cssz_public_key`, see Chapter 3.2.1)

   > **Note**
   >
   > *If the value of verify_cert_alias is set as empty, then signature verification process will be turned off and received data will be processed without verification.*

8. Select *Deploy*

3.4.4 Configuration of Submit iFlow

1. Go to the integration package that was copied from the original Human Experience Management solutions from SAP Integration with Czech Social Security Administration
2. Click the *Artifacts* tab
3. Click on *Actions* button that corresponds to integration flow **Poll** and choose **Configure**
4. Click the *Receiver* tab
5. Fill URL for productive APEP (it's described on a same web page as SSL certificates - see Chapter 2.5) as value for *Address* field (e.g. `https://epodani.cssz.cz/VREP/ws/Public.svc`)
6. Click the *More* tab

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

7. Fill the alias of public certificate which is used for encryption of content which is send to Czech Social Security Administration as the value for *encrypt_cert_alias* field (e.g. **`cssz_public_key`**, see Chapter 3.2.1)
8. Fill the alias of the key pair which is used for the signing of content which is sent to Czech Social Security Administration as value for *sign_cert_alias* field (e.g. **`customer_key_pair`**, see Chapter 3.2.3)
9. Fill the alias of the key pair which is used as an encryption certificate for DZDPN notification as the value for *dzdpn_cert_alias* field (e.g. **`dzdpn_key_pair`**, see Chapter 3.2.4)
10. Select *Deploy*

© 2016 SAP SE or an SAP affiliate company. All rights reserved.

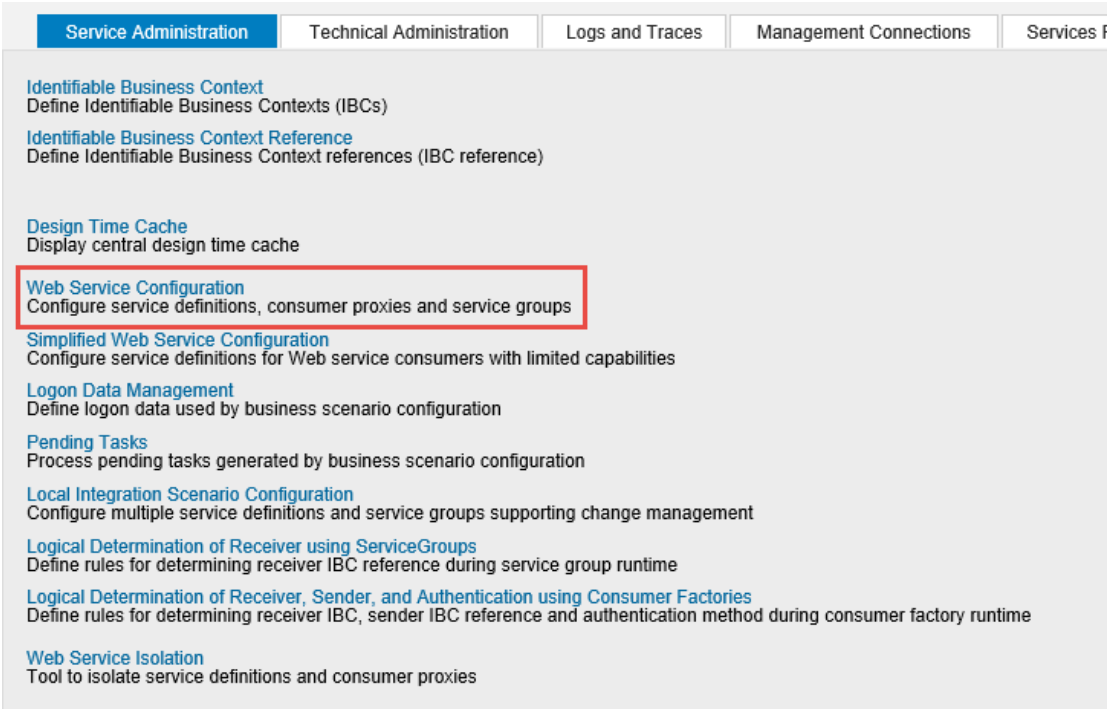
4 Configuration Steps in SAP ERP or SAP SuccessFactors Employee Central Payroll

4.1 SOAMANAGER configuration

The SOA Manager is a transaction for configuring and monitoring Web Services. It is run in a web browser.

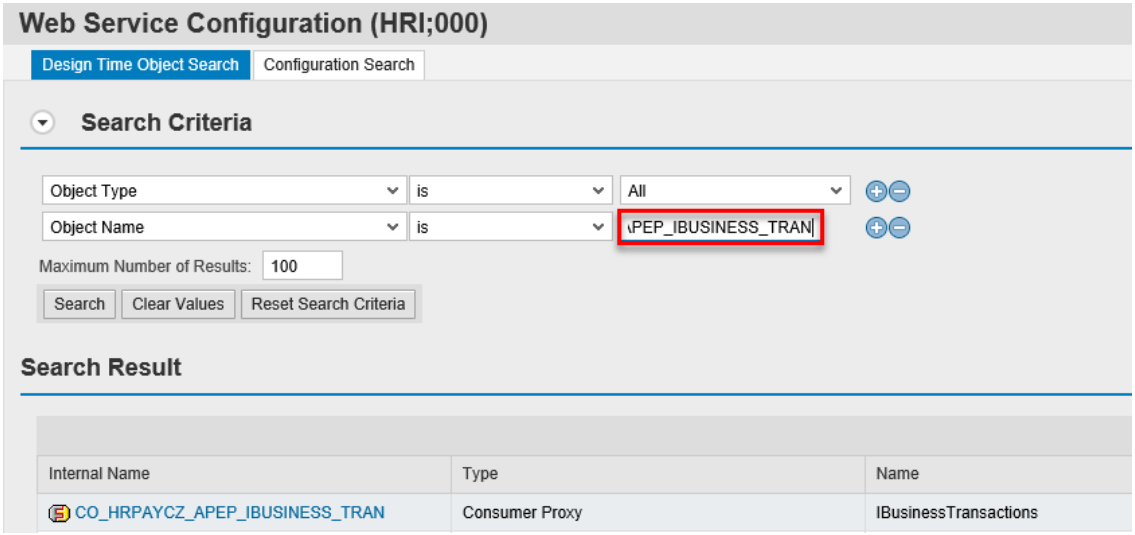
> **Note**
>
> *Some details (names of tabs etc.) might be slightly different depending on your release version.*

1. Execute the transaction code **SOAMANAGER. This opens a new window in your web browser**
2. **In the Service Administration tab,** click *Web Service Configuration* **link**



3. Then in the *Search Criteria* section, type the Object Name **CO_HRPAYCZ_APEP_IBUSINESS_TRAN**

CUSTOMER
© 2016 SAP SE or an SAP affiliate company. All rights reserved.

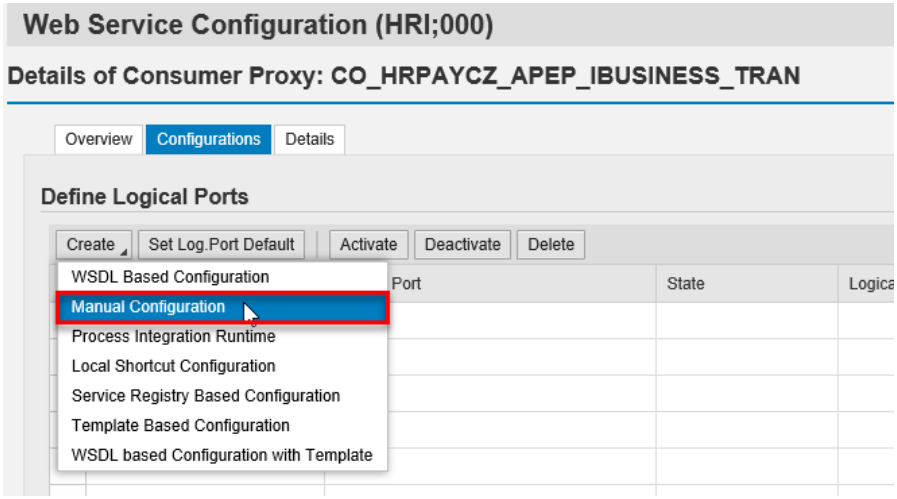


4. Click the Internal name **CO_HRPAYCZ_APEP_IBUSINESS_TRAN**
5. The following table lists the logical port name, description, and, path for each logical port.

Logical Port Name	Description	Path
DATA_REQUEST	CPI port for DataRequest operation	/cxf/HCI/PAYROLL/CZ/APEP/DATA_REQUEST
DISPOSE	CPI port for Dispose operation	/cxf/HCI/PAYROLL/CZ/APEP/DISPOSE
POLL	CPI port for Poll operation	/cxf/HCI/PAYROLL/CZ/APEP/POLL
SUBMIT	CPI port for Submit operation	/cxf/HCI/PAYROLL/CZ/APEP/SUBMIT

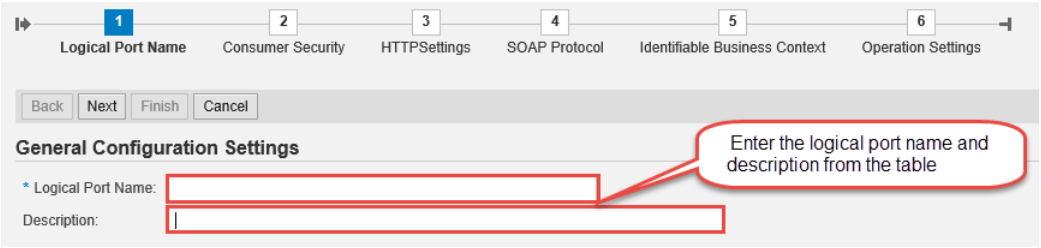
Following steps needs to be repeated for each line from this table using values from this line.

6. In the **Configurations** tab, click the *Create* button and select *Manual Configuration*.

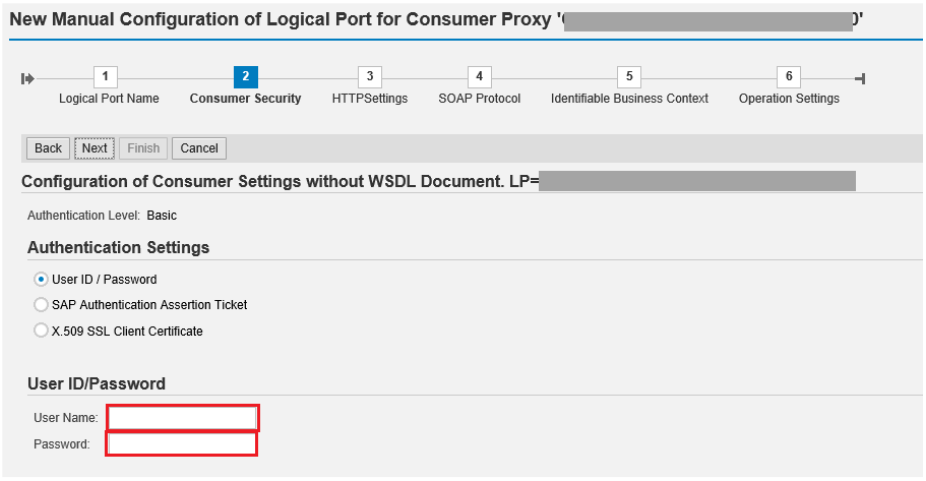


7. Step 1 - **Logical Port name**
   Enter the *Logical Port Name* and a *Description*.

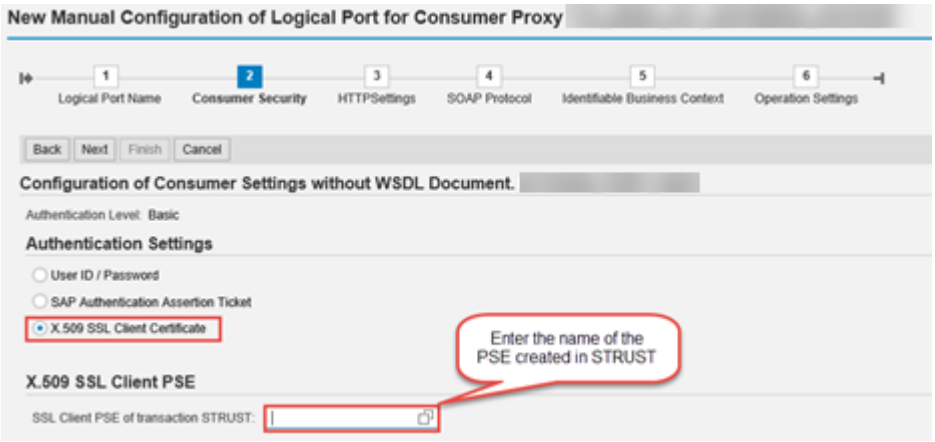
© 2016 SAP SE or an SAP affiliate company. All rights reserved.



8. Click *Next*.
9. Step 2 - **Consumer Security**
   The Consumer Security tab page configuration depends on the security being used for the SAP ERP or SAP



   S/4HANA - SAP CLOUD PLATFORM INTEGRATION communication.
   a) If you use basic authentication, select the User ID / Password radio button and enter the User Name and Password.
   b) If you use certificate-based authentication, select the X.509 SSL client certificate radio button and ensure that the required certificates are available in transaction STRUST.



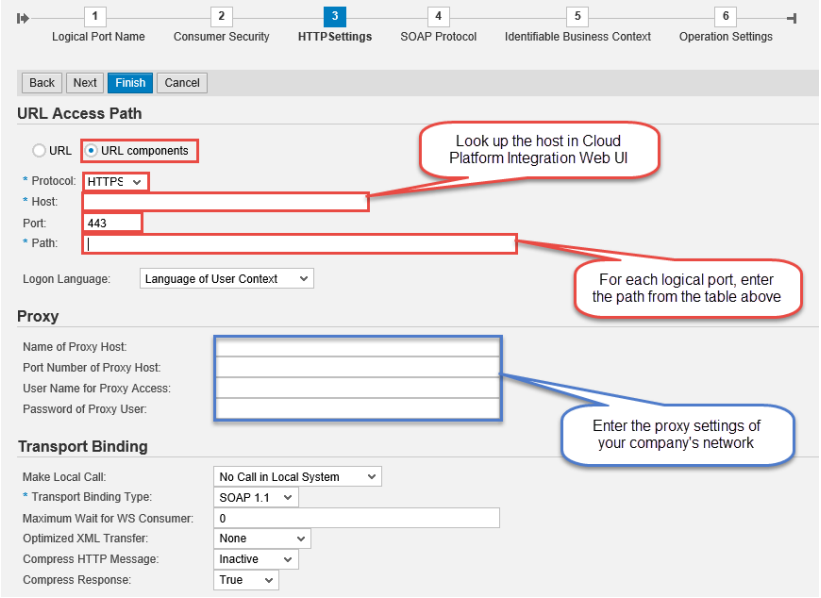
> **Note**
>
> *If you do not see this radio button or cannot select it, please refer to SAP Notes mentioned in Chapter 2.2.*

10. Click *Next*.
11. Step 3 - **HTTP Settings**
    On the HTTP Settings tab page, make the following entries:

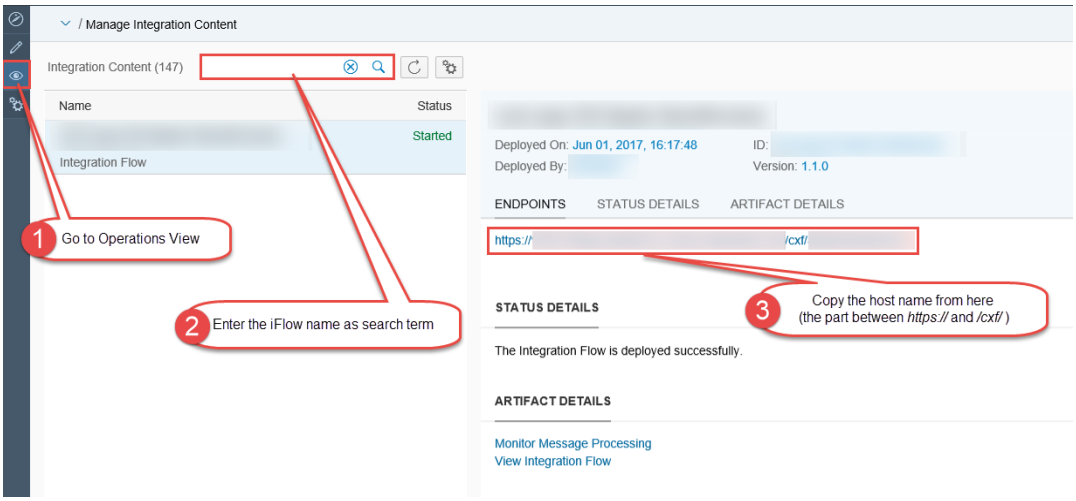
© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Note

The screenshots may look slightly different in your system depending on the release, but all the required fields must be available.



Enter the appropriate values in the fields above according to the information below:
Port 443 is the standard port for the HTTPS protocol.
To find the Host, go to *Cloud Integration Web UI*, choose *Monitor* and under *Managed Integration Content* go to *All*. Use the search to find your integration flow as shown in the screenshot below:

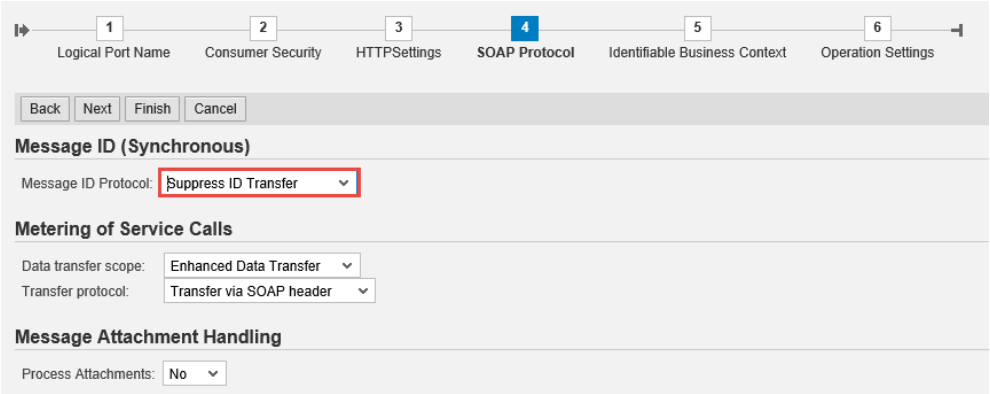


Note that the entries for the *Proxy* fields depend on your company's network settings. The proxy server is needed to enable the connection to the internet through the firewall.

12. Click *Next*.

13. Step 4 - **SOAP Protocol**:
Set *Message ID Protocol* to `Suppress ID Transfer`

CUSTOMER
© 2016 SAP SE or an SAP affiliate company. All rights reserved.

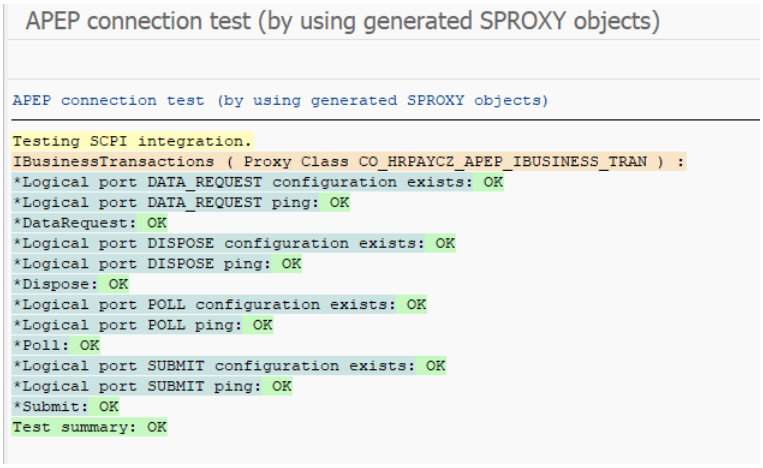


14. No settings are required in the *tabs Identifiable Business Context* and *Operation Settings*. Just select *Next* and then *Finish*.

4.2 Basic Connection Test

To test the communication, the best way is to execute the test report from your SAP ERP or SAP SuccessFactors Employee Central Payroll. Follow these steps:

1. Execute the transaction code **SA38 (or SE38).**
2. Fill the Program field with the value **`HCZUCPI0_CHECK_SPROXY`**.
3. Click the *Execute (F8)* button.
4. If *Test summary* is *OK* then basic test of connection to Czech Social Security Administration through SCPI was success.



CUSTOMER
© 2016 SAP SE or an SAP affiliate company. All rights reserved.

www.sap.com/contactsap

© 2016 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.
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 http://www.sap.com/corporate-en/legal/copyright/index.epx#trademark for additional trademark information and notices.

Material Number: