

Configuration Guide

TaxCard

Document Version: 1.1 – 2023-05-17

CUSTOMER

SAP ERP Integration with VERO Portal Tax Card

Using REST API with SAP Cloud Integration

Typographic Conventions

Type Style	Description
<i>Example</i>	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.

Document History

Version	Date	Change
1.0	2023-04-21	Initial version
1.1	2023-05-17	Updated URL in section 2.5

Contents

1	Introduction	5
2	Prerequisites.....	6
2.1	Installation of 'HRFI: Tax Card API Communication' Solution	6
2.2	Set Up of Secure Connection.....	6
2.3	Set Up SAP Cloud Integration Tenants.....	7
2.4	VERO SSL Certificate	7
2.5	VERO REST API Key	7
3	Configuration Steps in SAP Cloud Integration	8
3.1	General Information.....	8
3.2	Deploying Key Pairs and Certificates.....	8
3.2.1	Uploading of Vero SSL Certificate to Keystore	8
3.3	Obtaining a certificate	9
3.3.1	Creating a new certificate in CI	9
3.3.2	Saving Certificate Request (CSR).....	10
3.3.3	Certificate Service report	11
3.4	Copy Published Integration Package	13
3.5	Configure Integration Flows.....	13
3.5.1	Configuration of Request Tax Card iFlow.....	14
4	Configuration Steps in SAP ERP or SAP SuccessFactors Employee Central Payroll	15
4.1	Configuration of connection to Enterprise Certificate User Manager	15

1 Introduction

You use SAP Cloud 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 Finland. This document lists the required setup steps you perform in the SAP ERP or SAP SuccessFactors Employee Central Payroll and the SAP Cloud Integration tenant so that the integration between the systems works.

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

2 Prerequisites

2.1 Installation of 'HRFI: Tax Card API Communication' Solution

You installed and configured the "HRFI: Tax Card API Communication" solution in your test and productive SAP back-end system. If you did not install the latest support package for your system, refer to the latest SAP Note with latest improvements of the "HRFI: Tax Card API Communication" 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 the configurations steps described in this guide are as follows:

- 3303494 - HRFI: Tax Card API Communication

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 Integration.

Inbound HTTPS connections are not required for Finland. 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 Integration."](#)

Note

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

Client Certificate

If you 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 Integration Tenants

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

2.4 VERO SSL Certificate

The actual VERO SSL certificate for HTTPS communication is always used on the VERO main web page <https://avoinomavero.vero.fi/APIPortal/>. In case of issues VERO support can be contacted to get the actual VERO SSL Certificate.

Note

Instructions how to download the SSL Certificate from <https://avoinomavero.vero.fi/APIPortal/> by using the internet browser can be found on the internet by using a common internet search engine with the query "Download the SSL Certificate from a Website."

2.5 VERO REST API Key

The VERO REST API Key is required for communication with VERO by using REST API. More information can be found here: [Varmennepalvelu - Tulorekisteri \(vero.fi\)](#) or VERO support can be contacted to get VERO REST API Key.

Note

It's recommended to get the VERO REST API Key for the SAP Cloud Integration tenant owner organization.

3 Configuration Steps in SAP Cloud Integration

3.1 General Information

The package SAP ERP Integration with VERO Portal Tax Card contains the following iFlows:

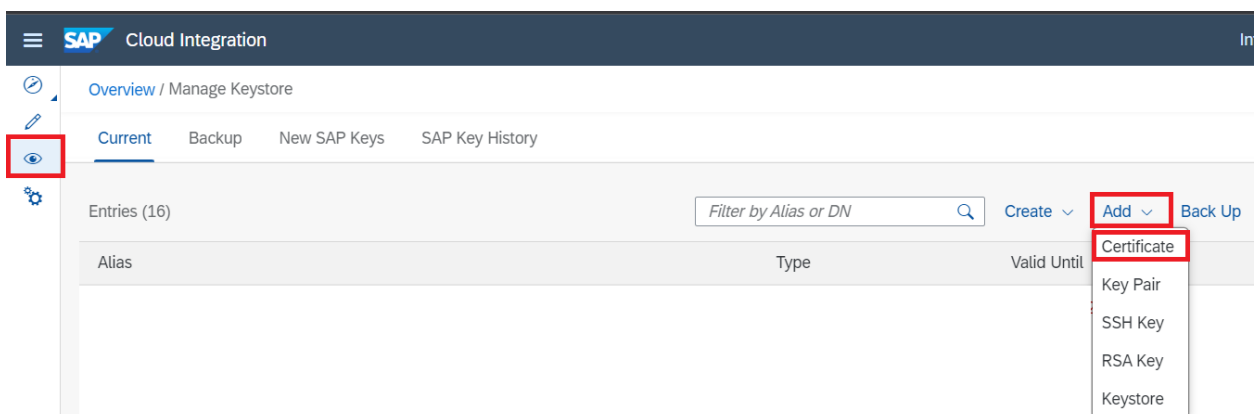
iFlow Name in WebUI	Project Name/Artifact Name
Request Tax Card	com.sap.GS.HR.FI.TaxCard

3.2 Deploying Key Pairs and Certificates

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

3.2.1 Uploading of Vero SSL Certificate to Keystore

- 1) In the CI, open the *Overview* section
- 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. `vero_ssl`). Then select the file with VERO SSL Certificate. The file with the certificate should be in CRT or CER format.



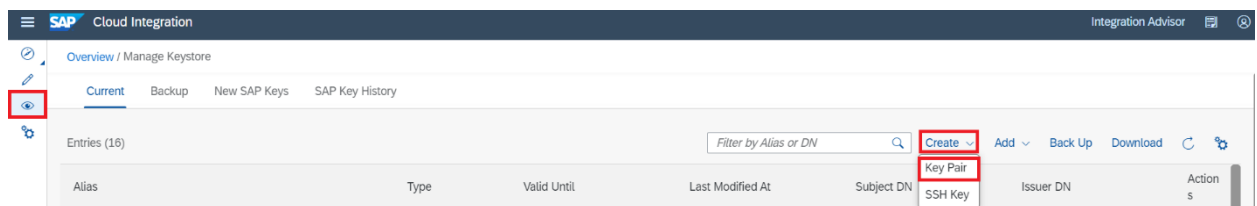
3.3 Obtaining a certificate

Please note that the VERO portal is not the issuer of the certificates for the communication. The service uses certificates issued by Income Register (KATRE) – for more information see [Vero Certificates for Production](#). If you have already installed the KATRE solution and have received a valid certificate, you can proceed to the section 3.4 and use this certificate in configuration.

If you haven't used the communication with income register before, you will need to implement the communication to the Certificate Service. See the SAP notes 2686707, 2715944 and the integration package [KATRE](#). The iFlows SignNewCertificate, GetCertificate and RenewCertificate will be necessary for obtaining and maintenance of the certificates.

3.3.1 Creating a new certificate in CI

- 1) In the CI, open the [Overview](#) section
- 2) In the [Manage Security](#) section, click the **Keystore** tile
- 3) Click the [Add](#) button and select **Certificate**



- 4) Fill the fields:
 - o Key Type: RSA
 - o KeySize: 204
 - o Algorithm: RSA with SHA-512
 - o CN: <Business ID>
 - o O: <Name of your organization>
 - o C: FI

Create Key Pair

Alias: * user_pk

Key Type: * RSA

Key Size: * 2048

Signature Algorithm: * SHA-512/RSA

Common Name (CN): * 7060986-6

Organizational Unit (OU):

Organization (O): Annimiikka Testifirma OY

Location (L):

State or Province (ST):

Country/Region (C): * FI

E-Mail (E):

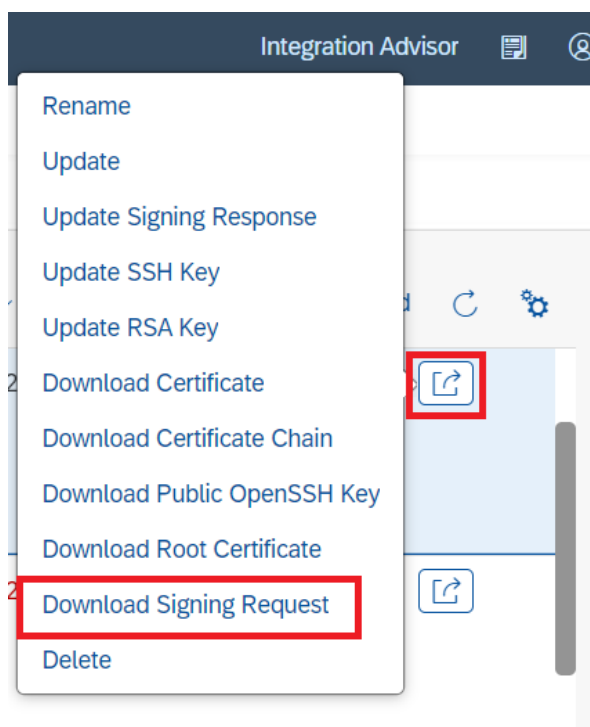
Valid From: * Apr 13, 2023

Valid Until: * Apr 13, 2025

Create Cancel

3.3.2 Saving Certificate Request (CSR)

- 1) On the newly created certificate, click the action button
- 2) In the menu, choose *Download Signing Request*
- 3) Save the CSR file



3.3.3 Certificate Service report

The Certificate Service report HFIIRCERT (transaction PC00_M44_IR_CERT) can be used for obtaining a new certificate or renewing an existing one.

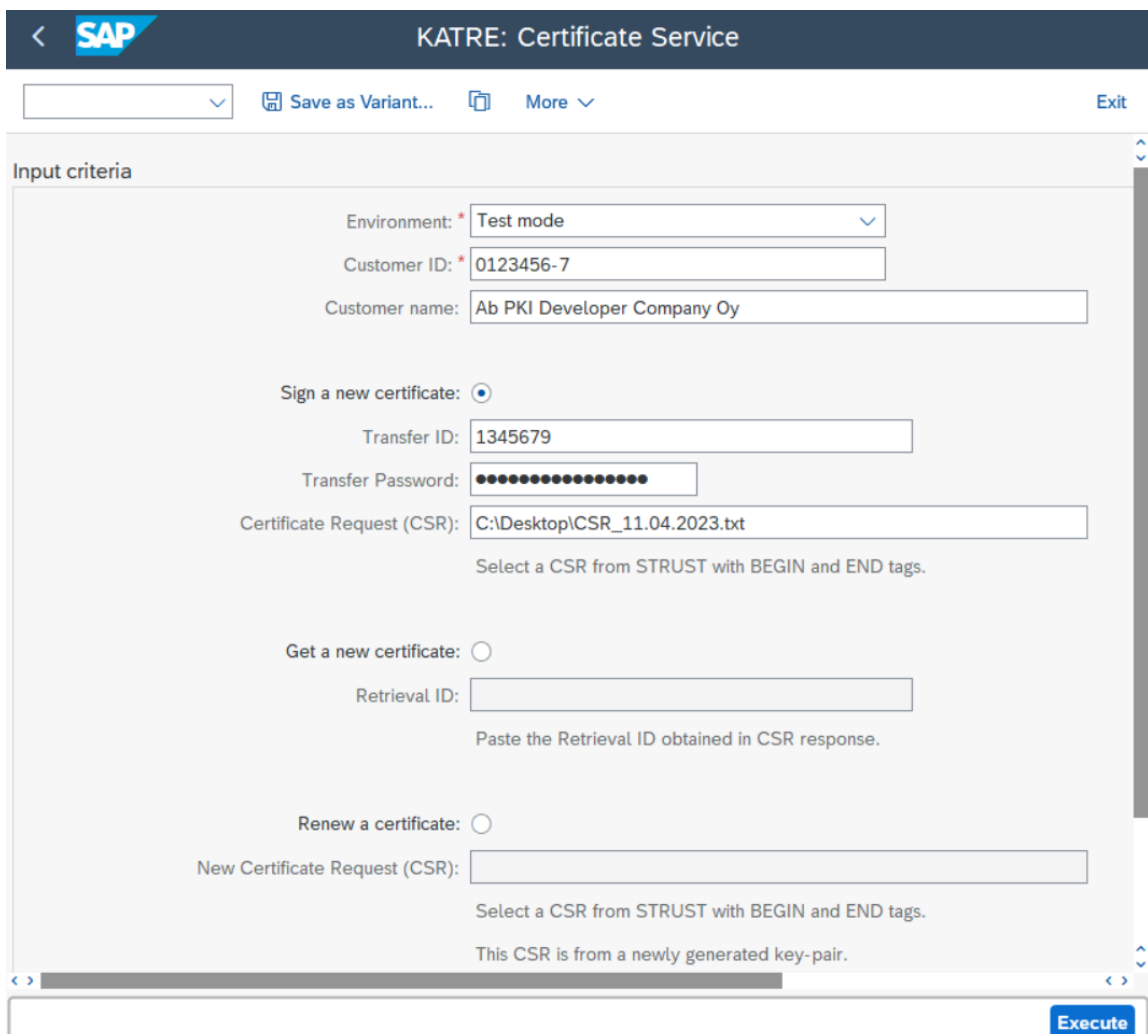
Note

A certificate is needed for signing submission with an XML digital signature and for SSL communication.

- 1) Open the transaction PC00_M44_IR_CERT.
- 2) Fill the selection screen with your data and select the first radio button *Sign a new certificate*
- 3) Press F4 to select a *Certificate Request (CSR)* saved from the CI.

Example

This is an example of how you can call the Certificate Test Bench (for testing the Certificate Service):



The screenshot shows the SAP KATRE: Certificate Service input criteria screen. The header includes the SAP logo and the title 'KATRE: Certificate Service'. Below the header are navigation options: a dropdown menu, 'Save as Variant...', 'More', and 'Exit'. The main area is titled 'Input criteria' and contains several input fields and radio buttons. The 'Sign a new certificate' radio button is selected. The fields are: Environment (Test mode), Customer ID (0123456-7), Customer name (Ab PKI Developer Company Oy), Transfer ID (1345679), Transfer Password (masked with dots), Certificate Request (CSR) (C:\Desktop\CSR_11.04.2023.txt), and a note 'Select a CSR from STRUST with BEGIN and END tags.'. Below this are options for 'Get a new certificate' and 'Renew a certificate', both with unselected radio buttons. The 'Get a new certificate' section has a Retrieval ID field and a note 'Paste the Retrieval ID obtained in CSR response.'. The 'Renew a certificate' section has a New Certificate Request (CSR) field and a note 'This CSR is from a newly generated key-pair.'. At the bottom right is an 'Execute' button.

- 4) If you run the report with the option *Display XML response*, the XML received from the authority is displayed in the next screen. *Press Back* (F3) to continue



Caution

Please, make sure to save the Certificate, it will be needed in the next step of the process!

- 9) Copy the whole certificate (without the BEGIN/END sections) to your clipboard.
- 10) Paste the certificate into a text editor (e.g. Notepad) and save as *certificate_response.p7b*
- 11) In CI, in Overview section, Manage Security, tile Keystore, click on the action button of certificate created in step 3.3.1.
- 12) Select Update Signing Response and chose the certificate file saved from the Certificate Service report.

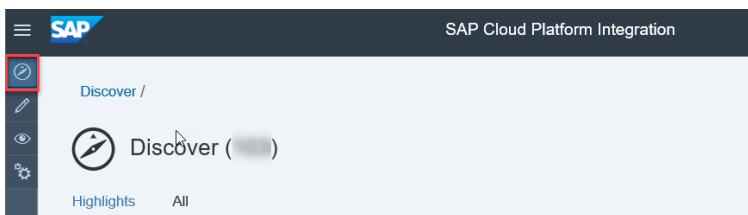


Note

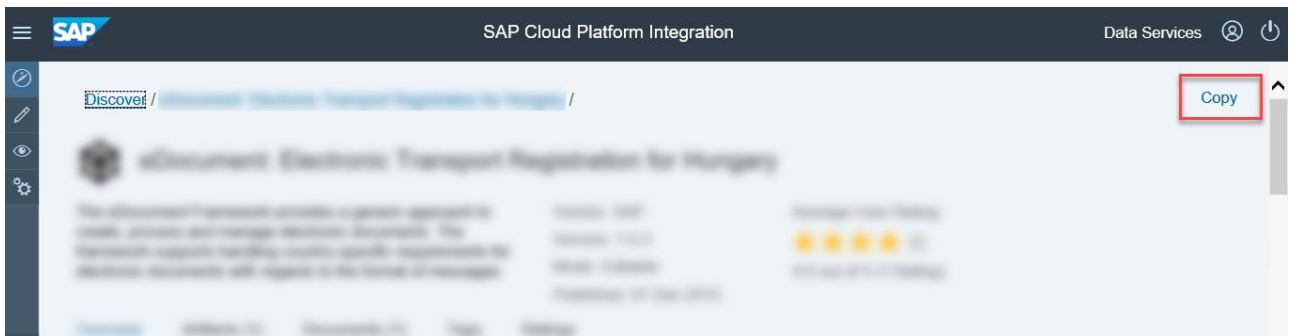
To renew an existing certificate, follow the same procedure; only choose the third radiobutton and select a CSR generated from a new SSL Client Identity. For more information about the process, please, refer to the Incomes Register website.

3.4 Copy Published Integration Package

- 1) In the *Discover* section of your tenant, select the package SAP ERP Integration with VERO Portal Tax Card.



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



3.5 Configure Integration Flows

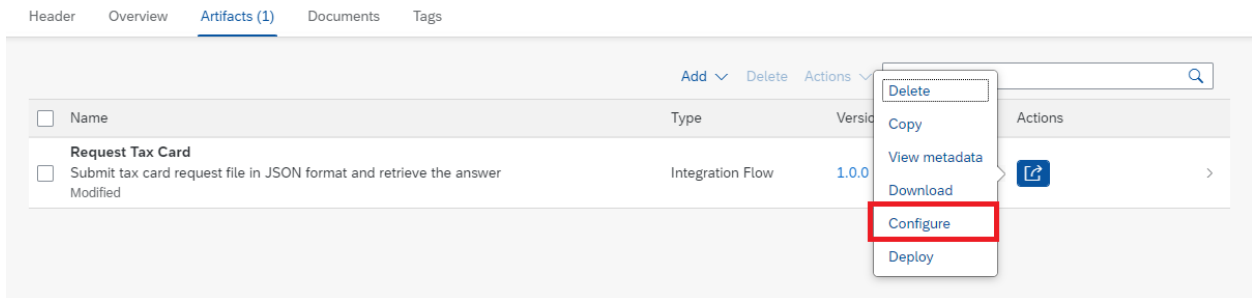


Note

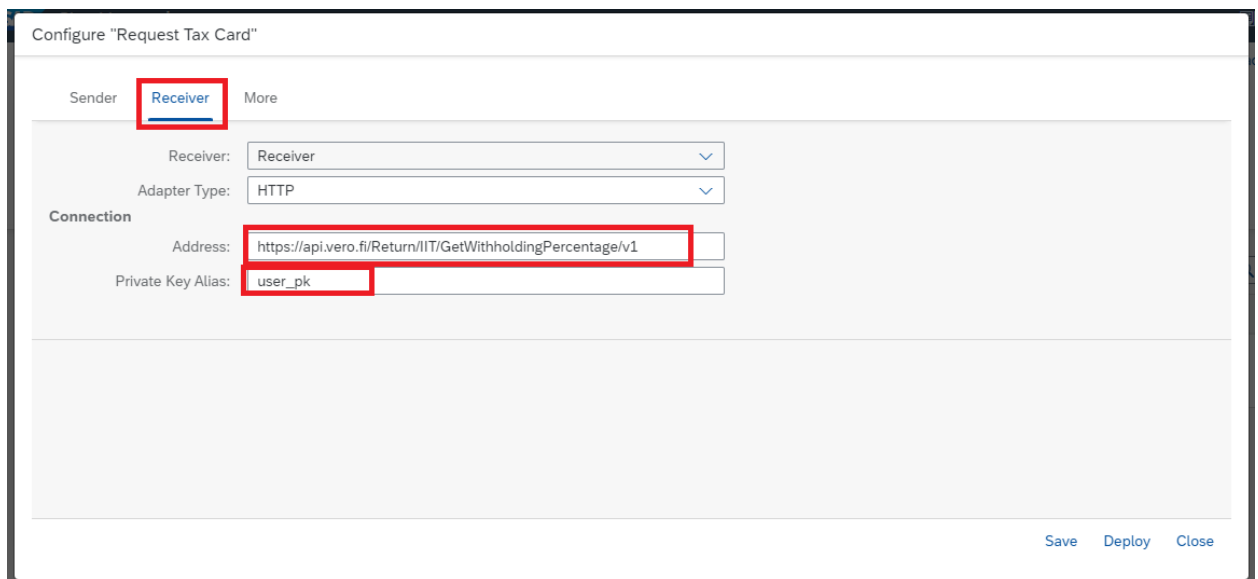
The following steps must be executed for the package that was copied as described in chapter 3.3.

3.5.1 Configuration of Request Tax Card iFlow

- 1) Go to the integration package that was copied from the original SAP ERP Integration with VERO Portal Tax Card.
- 2) Click the *Artifacts* tab



- 3) Click on the *Actions* button that corresponds to integration flow Request Tax Card and choose **Configure**
Click the *Receiver* tab



- 4) Fill the URL for productive environment (the current information and URLs can be found on the web https://avoinomavero.vero.fi/APIPortal/_/ under API Documentation -> Return -> Individual Income Tax -> Withholding Percentage Request)
- 5) Fill the name of Private key as the name of the Enterprise certificate created as described in Chapter 3.3
- 6) Select *Deploy*.

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

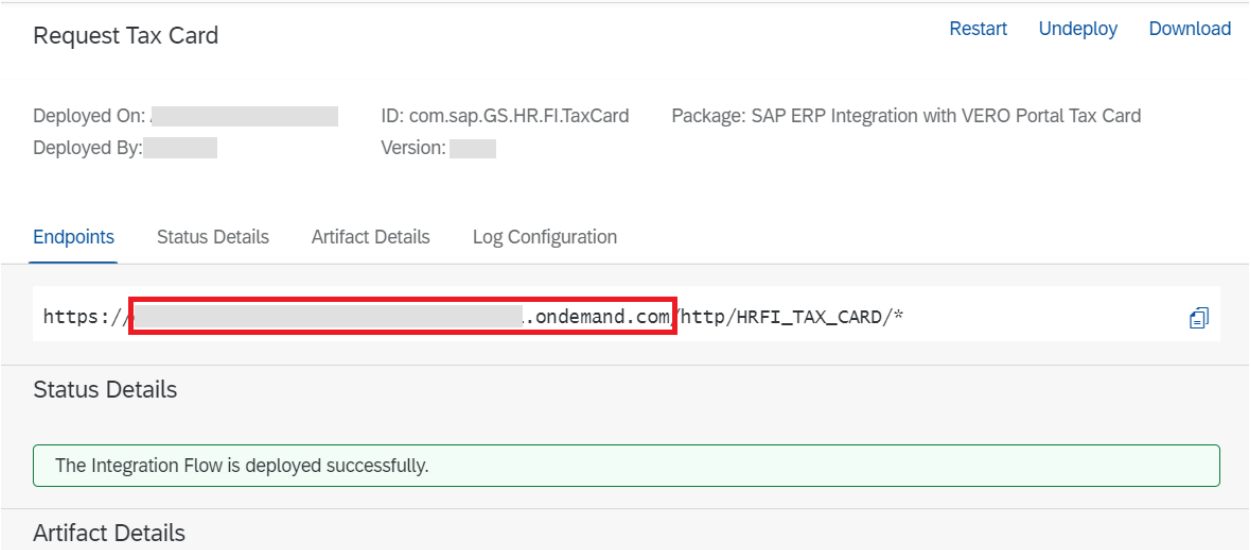
In the SAP back-end system, you need to configure the HTTPS connection to the CI solution.

Note

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

4.1 Configuration of connection to Enterprise Certificate User Manager

To set up the HTTPS connection, you need the URL of the tenant (the TMN URL you received when the tenant was provisioned). You can also find the URL in the CI Overview → Manage Integration Content → Select deployed Enterprise Certificate User Manager iFlow.



The screenshot shows the SAP Integration Suite interface for the 'Request Tax Card' iFlow. At the top right, there are buttons for 'Restart', 'Undeploy', and 'Download'. Below this, the deployment details are shown: 'Deployed On: [redacted]', 'ID: com.sap.GS.HR.FI.TaxCard', 'Package: SAP ERP Integration with VERO Portal Tax Card', 'Deployed By: [redacted]', and 'Version: [redacted]'. There are four tabs: 'Endpoints', 'Status Details', 'Artifact Details', and 'Log Configuration'. The 'Endpoints' tab is active, showing the URL 'https://[redacted].ondemand.com/http/HRFI_TAX_CARD/*' with a copy icon. Below the URL, the 'Status Details' section shows a green message box: 'The Integration Flow is deployed successfully.' The 'Artifact Details' section is also visible.

Note

To setup a secure HTTPS connection between the SAP back-end system and the SAP Cloud Integration tenant, add the load balancer root certificate to the SAP back-end system trust store.

- 1) Execute the transaction code **SM59**
- 2) To create a new connection, select *Edit* → *Create*
- 3) For the RFC destination, enter value **HR_FI_CPI_TC_REST_API** for the connection name

- 4) Set connection type **G** (HTTP Connection to External Server)
- 5) Enter **CI -Tax Card** in the *Description* field
- 6) On the *Technical Settings* tab, enter the following values
 - a) Target Host: <IFLMAP URL for the CI tenant>

i Note

Make sure that you don't enter "https:///" in the field, Target Host
 Example: 1234567890-iflmap.hcisbp.eu3.hana.ondemand.com

- b) Service No.: **443**
- c) Path Prefix: **/http/HRFI_TAX_CARD/**
- d) HTTP Proxy Options <Enter own HTTP proxy values>

The screenshot displays the SAP configuration page for an RFC Destination named 'HR_FI_CPI_TC_REST_API'. The 'Technical Settings' tab is active, showing the following configuration details:

- RF Destination:** HR_FI_CPI_TC_REST_API
- Connection Type:** G (HTTP Connection to External Server)
- Description:** CI -Tax Card
- Target System Settings:**
 - Host:** [Redacted] ondemand.com
 - Port:** 443
 - Path Prefix:** /http/HRFI_TAX_CARD/
- HTTP Proxy Options:**
 - Global Configuration:**
 - Proxy Host:** [Redacted]
 - Proxy Service:** [Redacted]
 - Proxy User:** [Redacted]
 - Proxy PW Status:** is initial

- 7) Click the *Logon & Security* tab
 There are two options for setting up the authentication: **basic authentication** or **client certificate-based authentication**. The more secure option is to use client certificates.

a) **Basic Authentication**

Create a user in Cloud Integration and assign the **ESBMessaging.send** role.

i Note

More information can be found on SAP Help Portal

<https://help.sap.com/viewer/368c481cd6954bd5d0435479fd4eaf/Cloud/en-US/24585cc503334e6c917ef383efb5558a.html?q=ESBMessaging.send>

In the *Logon & Security* tab enter:

- i) *Logon with user*: Choose **Basic Authentication** and enter a valid **user** and **password** for logging on to CI
- ii) *Logon with ticket*: Select **Do Not Send Logon Ticket**
- iii) *Security options*: Select **SSL Active** and **SSL Certificate Default SSL Client (Standard)**

The screenshot shows the SAP Cloud Integration configuration interface for an RFC Destination named 'HR_FI_CPI_TC_REST_API'. The 'Logon & Security' tab is active. Under 'Logon Procedure', 'Logon with User' is selected with 'Basic Authentication' chosen. The 'User' field is filled with a greyed-out value, and 'PW Status' is 'saved'. Under 'Logon with Ticket', 'Do Not Send Logon Ticket' is selected. Under 'Logon with MQTT/AMQP', 'Users' and 'PW Status' fields are present. In the 'Security Options' section, 'Status of Secure Protocol' is set to 'Active', and 'SSL Client PSE ID' is 'DEFAULT SSL Client (Standard)'. There is also a checkbox for 'Do Not Use Certificate for Logon' which is unchecked.

b) **Client certificate-based authentication**

Set up the client certificate in the SAP back-end system and upload to Cloud Integration in the certificate-

to-user mapping as described in the blog <https://blogs.sap.com/2017/06/05/cloud-integration-how-to-setup-secure-http-inbound-connection-with-client-certificates/>

- 8) To perform a quick test, click on **Connection Test** button
If everything is correctly set then **HTTP Response Status** should be with Value **400**

Destination: HR_FI_CPI_TC_REST_API
Ty. : HTTP Connection to External Server

Test Result Response Header Fields Response Body Response Text

Detail	Value
Status HTTP Response	400
Status Text	
Duration Test Call	1778 ms

- 9) In your tenant, you under Overview-> Monitor Message Processing, you should see one successfully executed Request Tax Card integration flow

Cloud Integration

Overview / Monitor Message Processing

Time: Past Hour Status: All

Mar 30, 2023, 15:20:21 - Mar 30, 2023, 16:20:21

Messages (2) 1 / 1

Artifact Name	Status
Request Tax Card	Completed
Mar 30, 2023, 16:18:12	1 sec 643 ms



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:



SAP