Configuration Guide

Enhanced Reporting Requirements full communication using REST APIs

Document Version: 1.1 – 2024-11-30

CUSTOMER

SAP Enhanced Reporting Integration with Revenue Online Services gateway – Ireland

Using REST API with SAP Cloud 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	2023-10-30	Document created and released
1.1	2024-11-30	Document created and released

CUSTOMER
© 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 Integration to establish a secure communication with Revenue Online Services (ROS) and transfer electronic documents created using the Enhanced Reporting Requirements Full communication solution from SAP Ireland. This document lists the required setup steps needed 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 also be 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(artifacts that are deployed in the SAP Cloud Integration tenant). Please refer to the relevant SAP back-end systems documentation for more information.*

For the sake of simplicity in this guide, SAP back-end systems 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 ' SMART PAYE Full Communication' Solution

You installed and configured the "SMART PAYE FULL Communication" solution in your test and productive SAP back-end systems. If you did not install the latest support package for your system, refer to the latest SAP Note.

> **Note**
>
> *Installation of the SMART PAYE Full Communication solution is a pre-requisite to using the ERR solution*
>
> - *3170034 - SMART PAYE: Full Communication*

2.2 Set Up of Secure Connection

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

Communication is always initiated from the SAP Backend systems, and as such HTTPS connections need to be set up.

You use the SAP ERP Trust Manager (transaction `STRUST`) to manage the certificates required for a SSL connection. The certificates are trusted certificate authority (CA) certificates to support iFlow authentication.

In addition, you will need to install certificates on SAP Cloud Integration to sign and encrypt data that is transmitted to ROS.

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
- 3326192 –
-

For more information, refer to the following:

1. "Operations guide for SAP Cloud Integration."
2. Technical Integration with SAP S/4HANA or SAP ERP

> **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.*

© 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 Integration Tenants

Users in SAP Cloud Integration test and production tenants have the authorisation 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 ROS SSL Certificate

SSL certificates are needed to ensure the SSL encryption of the communication layer between SAP Cloud Integration and ROS servers. The ROS SSL certificate for HTTPS communication can be downloaded by accessing the ROS website and using the browser to download the certificate.

> **Note**
>
> *Instructions how to download the SSL Certificate from https://www.ros.ie/ 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 ERN Certificates

In addition to the SSL certificates mentioned above, ERN certificates are required to sign and encrypt the contents of the messages flowing between SAP Cloud Integration and ROS. These certificates can be downloaded or requested using the normal ROS help desk or support.

2.6 Partner Directory URL

The relationship between the ERN and the actual certificate itself is stored in the Partner directory. The Partner Directory is a secure storage area in the cloud and is accessed by the ODATA URL which can be found in the SAP BTP Cockpit → Applications → Application '<tenant>tmn' → Application URLs →URL ending with '/api'

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

Note

More details about Partner Directory can be found also here:
https://api.sap.com/package/IntegrationFlowDesignGuidelinesPartnerDirectoryGuidelines

2.7 Partner Directory SSL Certificate

The actual SSL certificate for HTTPS communication with the Partner Directory API can be downloaded from the Partner Directory URL.

Note

Instructions how to download the SSL Certificate from the Tenant Management URL 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."

Further help can be found in the appendix of this document

2.8 Partner Directory User

This guide will describe the connection to the Partner Directory by using a User with the required authorization as described on the SAP Help Portal:
https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/LATEST/en-US/0fe80dc9d3be4dfbbb89ee4c791d326e.html

Note

It's possible to also access the Partner Directory by other ways like OAuth2. More information can be found on: https://blogs.sap.com/ e.g. here https://blogs.sap.com/2017/07/25/cloud-integration-partner-directory-step-by-step-example/.

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

3 Configuration Steps in SAP Cloud Integration

3.1 General Information

The package SAP Enhanced Reporting Integration with Revenue Online Services gateway - Ireland contains the following iFlows:

iFlow Name in WebUI	Artifact ID
Enhanced Reporting Submission	Enhanced_Reporting_Submission
Check ERR Submission	Check_ERR_Submission
Check ERR Run	CheckERRRunRequest
Request Monthly ERR Report	Request_Monthly_ERR_Report
Groovy Scripts for Enhanced Reporting	Groovy Script

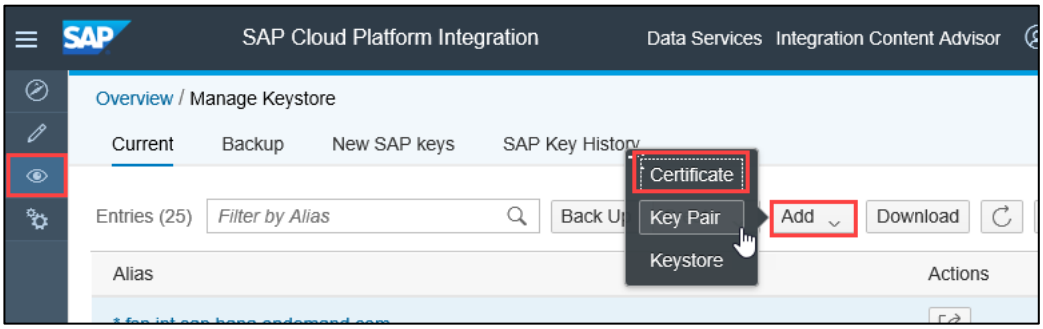
3.2 Deploying Key Pairs and Certificates

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

3.2.1 Uploading of ROS 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**

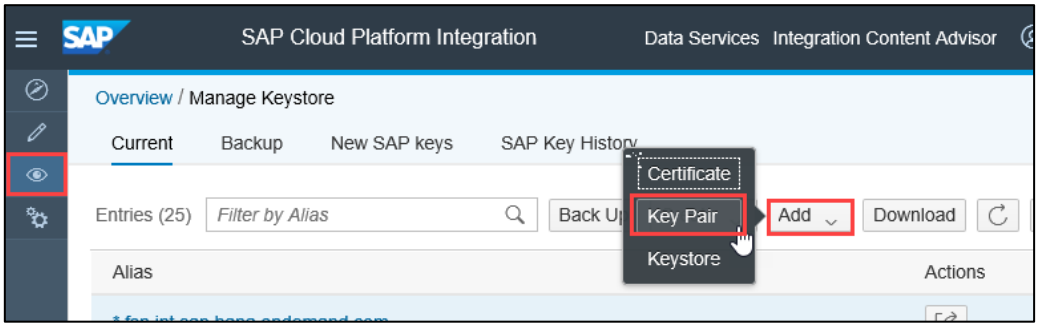
© 2016 SAP SE or an SAP affiliate company. All rights reserved.



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

3.2.2 Uploading of ERN Certificates to Keystore

1) In the SAP Cloud integration, open the *Overview* section
2) In the *Manage Security* section, click the **Keystore** tile
3) Click the *Add* button and select **Key Pair**

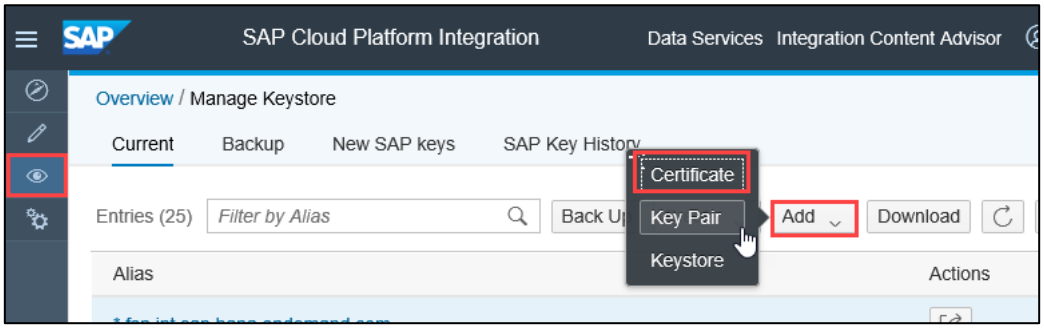


4) In the pop-up window, enter the **Alias** for the Key Pair if you would like one, otherwise if you leave this field blank, the system is auto populate the alias name. Then select the certificate and enter the corresponding password for this file in the **Password** field. The password needs to be extracted using the ABAP report HIEUPWDEXTRACTOR. See SAP back-end documentation for details on how to do this.

3.2.3 Uploading of Tenant Management SSL Certificate to Keystore

1) In the SAP Cloud integration, open the *Overview* section
2) In the *Manage Security* section, click the **Keystore** tile

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



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

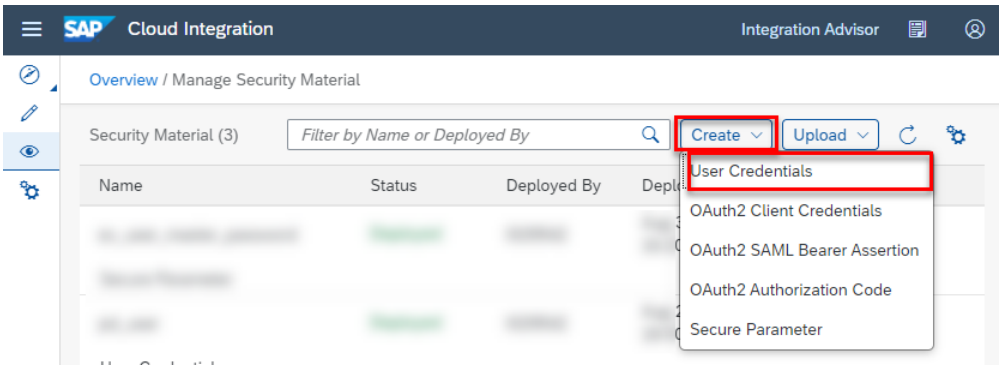
In the pop-up window, enter the **Alias** for the Key Pair (e.g. `tmn_ssl`). Then select the file with

4) Partner Directory SSL Certificate. The file with the certificate should be in CRT or CER format.

3.3 Store Sensitive Information into Security Material

3.3.1 Store Details of Partner Directory User Details

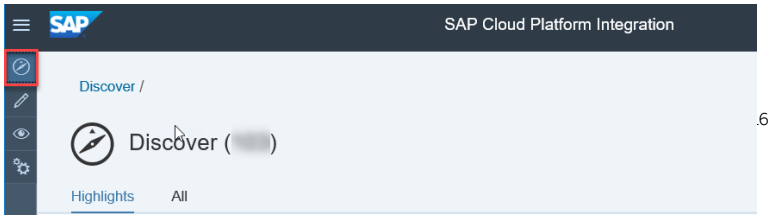
1) In the SAP Cloud integration, open the *Overview* section
2) In the *Manage Security* section, click the **Security Material** tile



3) Click the *Create* button and select **User Credential**
4) In the pop-up window, enter the **Name** for the User Credential as ERN_PD_USER . Fill in User Name and Password of the Partner Directory User.

3.4 Copy Published Integration Package

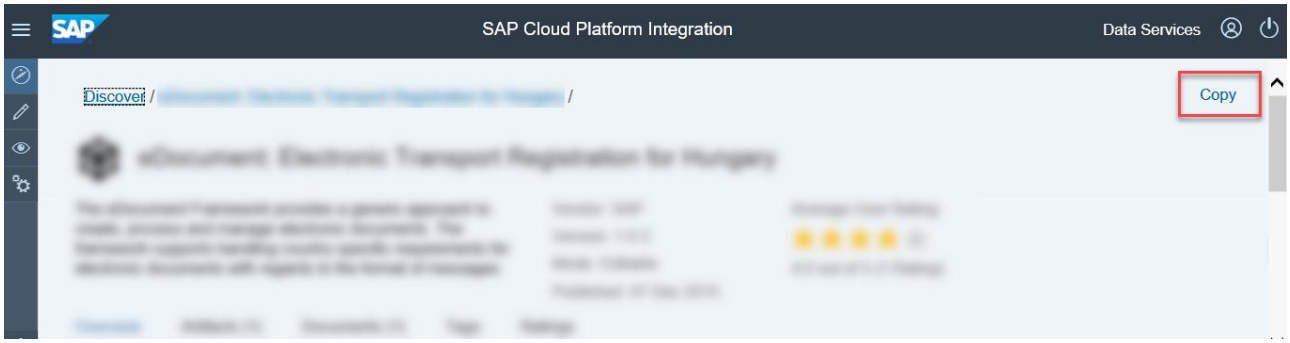
1) In the *Discover* section of your tenant, select the package



.6 SAP SE or an SAP affiliate company. All rights reserved.

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

3.5 Configure Integration Flows

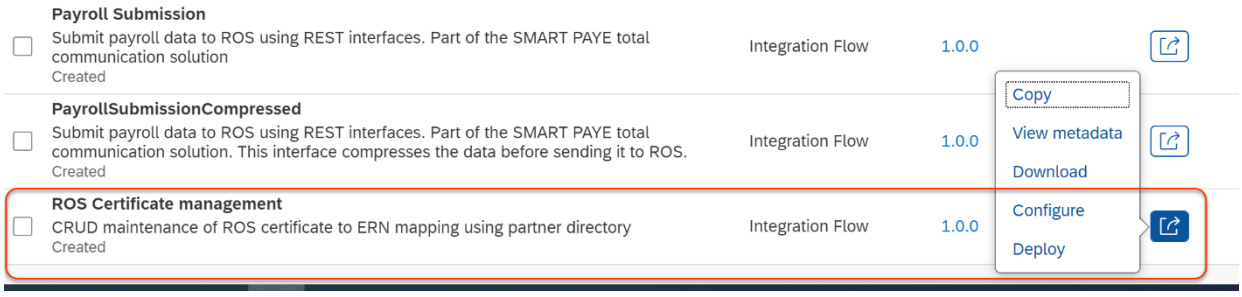


Note

The following steps must be executed for the package that was copied as described in chapter 3.4

3.5.1 Configuration of ROS Certificate management iFlow

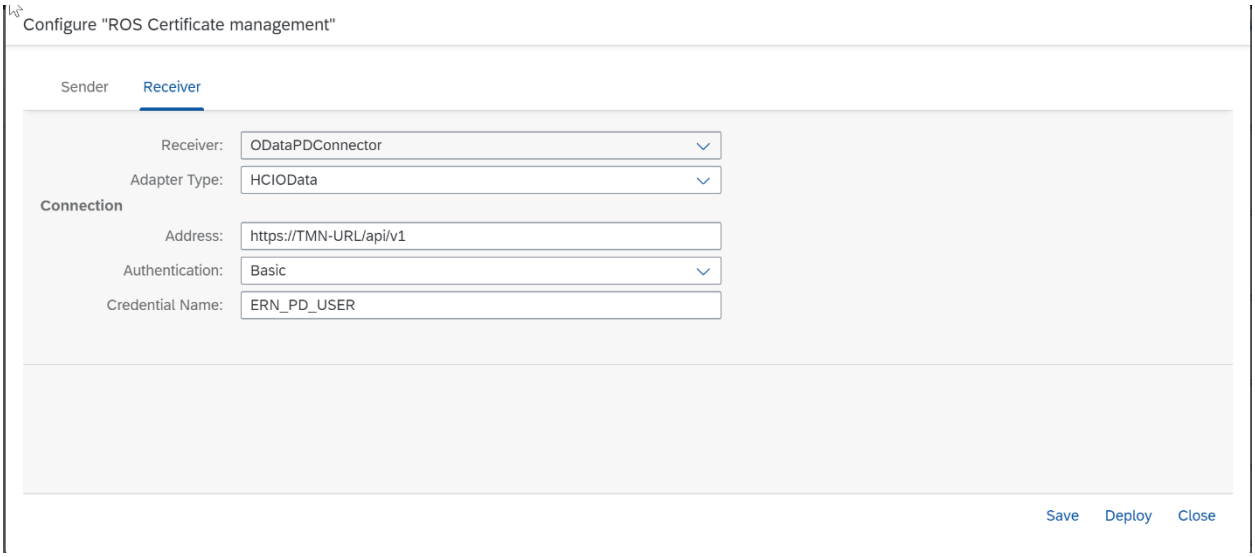
1) Go to the integration package that was copied from the original .
2) Click the *Artifacts* tab
3) Click on the *Actions* button that corresponds to integration flow **ROS Certificate management** and choose **Configure**



Click the *Receiver* tab

4) Fill the Partner Directory URL as the value for *Address* field (e.g. `https://{tenant}-tmn.{something}.hana.ondemand.com/api/v1/`)
5) Select value "`Basic`" in the *Authentication* field
6) Fill in the name of Security Material with Partner Directory User (see chapter, Store Details of Partner Directory User Details) value for the *Credential Name* field (ERN_PD_USER)

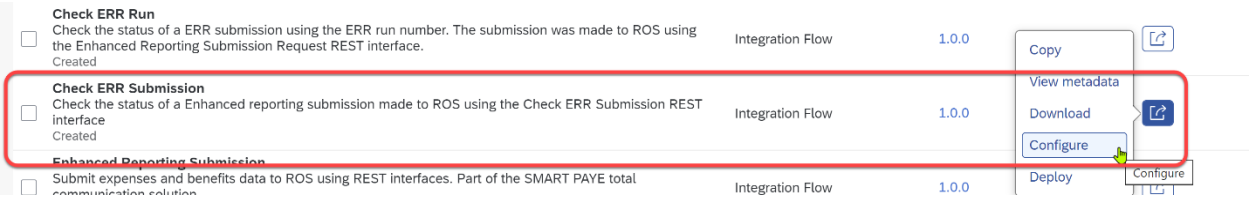
© 2016 SAP SE or an SAP affiliate company. All rights reserved.



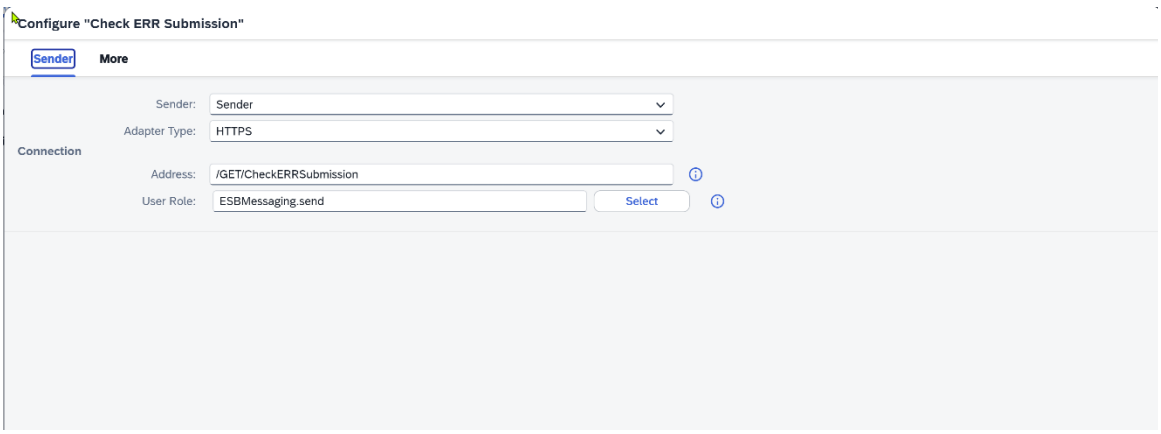
Select *Deploy*.

3.5.2 Configuration of Check ERR Submission iFlow

1) Go to the integration package that was copied from the original *SAP Enhanced Reporting with Revenue Online Services gateway – Ireland.*
2) Click the *Artifacts* tab
3) Click on the *Actions* button that corresponds to integration flow **Check ERR Submission** and choose **Configure**



Click the *Sender* tab



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

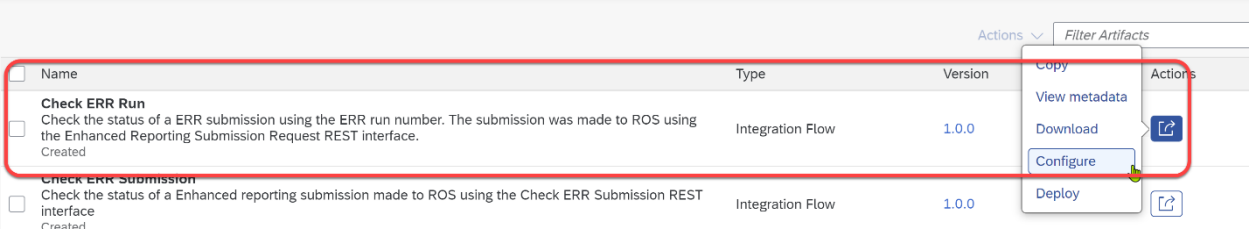
4) Configure the User role with the role that you would like to assign to the user.
5) Only enter an alternate sender endpoint in the address field if you wish to change the default and are very clear of the reasons you wish to change it for. Otherwise leave the default value as it is. If you change this field, you MUST make sure your corresponding RFC also reflects the change.

6) Select *Deploy*.
7) Configuration Steps in SAP ERP or SAP SuccessFactors Employee Central Payroll
8) 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.*

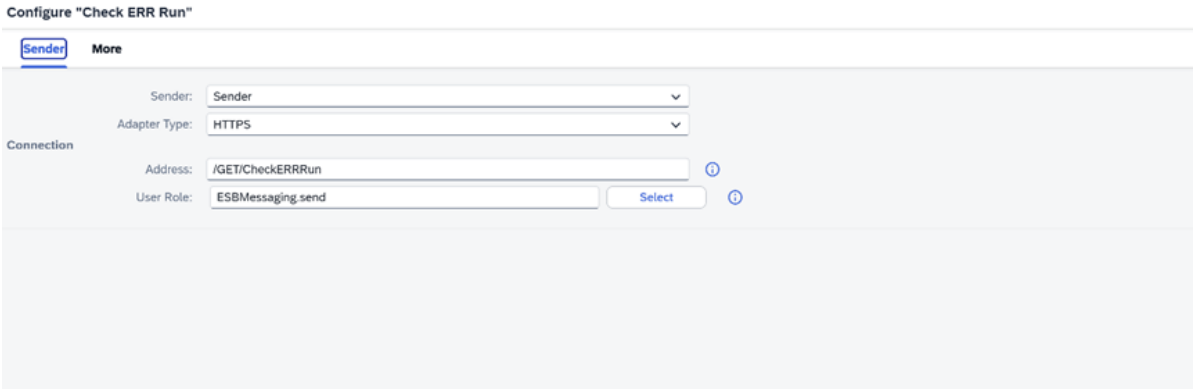
3.5.3 Configuration of Check ERR Run iFlow

1) Go to the integration package that was copied from the original .
2) Click the *Artifacts* tab
3) Click on the *Actions* button that corresponds to integration flow **Check ERR Run** and choose **Configure**



Click the *Sender* tab

4) Configure the *User role* with the role that you would like to assign to the user.



5) Only enter an alternate sender endpoint in the address field if you wish to change the default and are very clear of the reasons you wish to change it for. Otherwise leave the default value as it is. If you change this field, you MUST make sure your corresponding RFC also reflects the change.

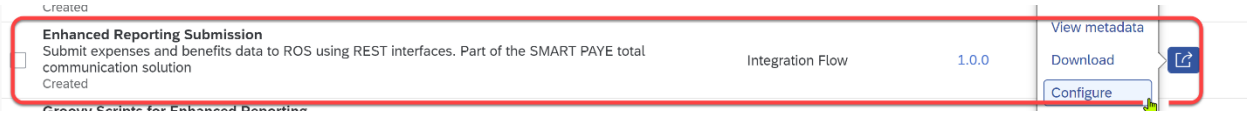
CUSTOMER
© 2016 SAP SE or an SAP affiliate company. All rights reserved.

6) Select *Deploy*.
7) Configuration Steps in SAP ERP or SAP SuccessFactors Employee Central Payroll
8) In the SAP back-end system, you need to configure the HTTPS connection to the CI solution.

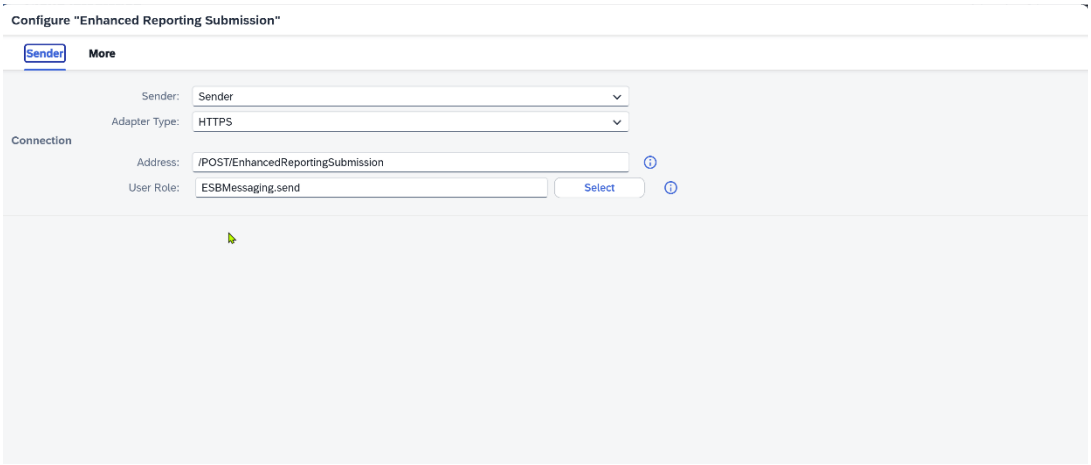
> **Note**
>
> *Some details (names of tabs etc.) might be slightly different depending on your release version.*

3.5.4 Configuration of Enhanced Reporting Submission

1) Go to the integration package that was copied from the original .
2) Click the *Artifacts* tab
3) Click on the *Actions* button that corresponds to integration flow **Enhanced Reporting Submission** and choose **Configure**



4) Click the *Sender* tab
5) Configure the *User role* with the role that you would like to assign to the user.



6) Only enter an alternate sender endpoint in the address field if you wish to change the default and are very clear of the reasons you wish to change it for. Otherwise leave the default value as it is. If you change this field, you MUST make sure your corresponding RFC also reflects the change.
7) Select *Deploy*.
8) Configuration Steps in SAP ERP or SAP SuccessFactors Employee Central Payroll
9) In the SAP back-end system, you need to configure the HTTPS connection to the CI solution.

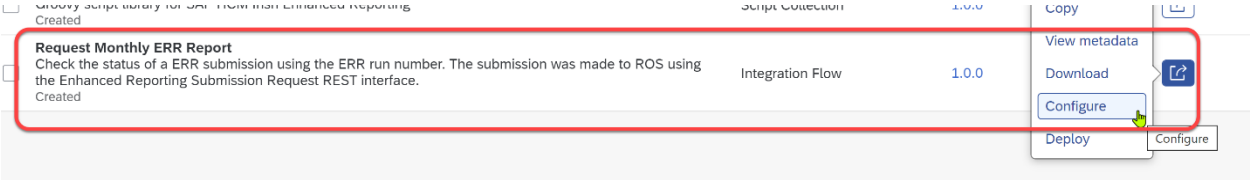
© 2016 SAP SE or an SAP affiliate company. All rights reserved.

Note

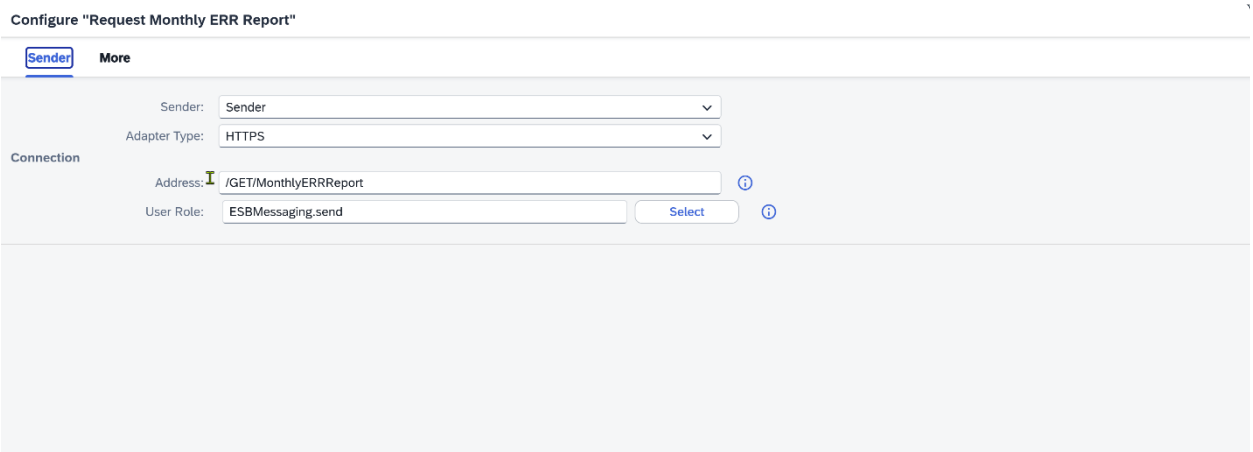
Some details (names of tabs etc.) might be slightly different depending on your release version.

3.5.5 Configuration of Request Monthly ERR Report iFlow

1) Go to the integration package that was copied from the original .
2) Click the *Artifacts* tab
3) Click on the *Actions* button that corresponds to integration flow **Request Monthly ERR Report** and choose **Configure**



4) Click the *Sender* tab



5) Configure the *User role* with the role that you would like to assign to the user.
6) Only enter an alternate sender endpoint in the address field if you wish to change the default and are very clear of the reasons you wish to change it for. Otherwise leave the default value as it is. If you change this field, you MUST make sure your corresponding RFC also reflects the change.
7) Select *Deploy*.
8) 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.

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

3.6 Configuration of HTTP connections (RFC) for each iFlow

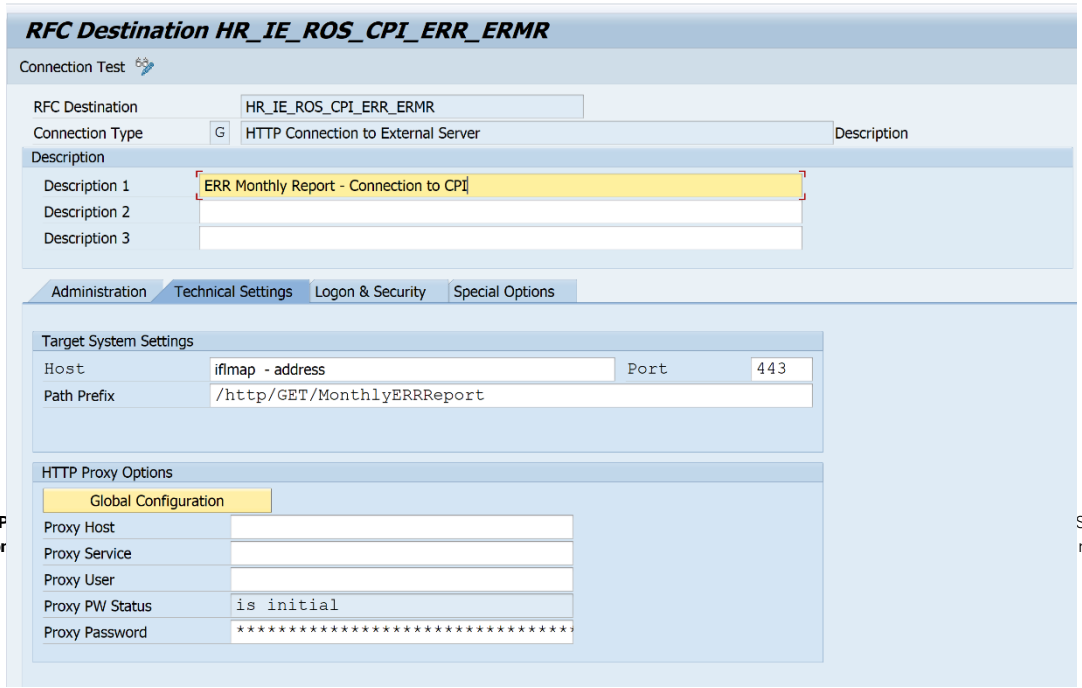
To set up the HTTPS connection, you need the URL of the tenant (the TMN URL you received when the tenant was provisioned). You can also find the URL in the CI Overview → Manage Integration Content → Select deployed iFlows. See example below.

> **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 each of the values from the table below for the connection name
4) Set connection type **G** (HTTP Connection to External Server)
5) Enter **a description** in the *Description* field from the table below
6) On the *Technical Settings* tab, enter the following values
   a) Target Host: **< IFLMAP URL for the CI tenant>**

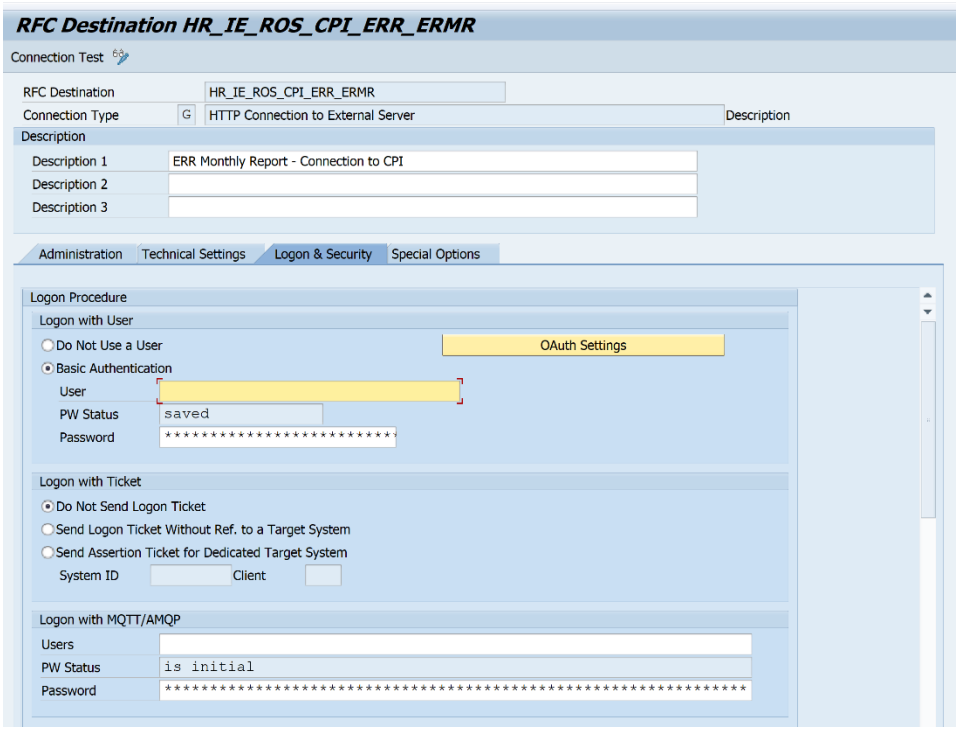
> **Note**
>
> *Make sure that you don't enter "https://" in the field, Target Host*
>
> *Example: 1234567890-iflmap.hcisbp.eu3.hana.ondemand.com*

   b) Service No.: **443**
   c) Path Prefix: **enter the path prefix from the table below**
   d) HTTP Proxy Options **<Enter own HTTP proxy values>**



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.



Note

More information can be found on SAP Help Portal
https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/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

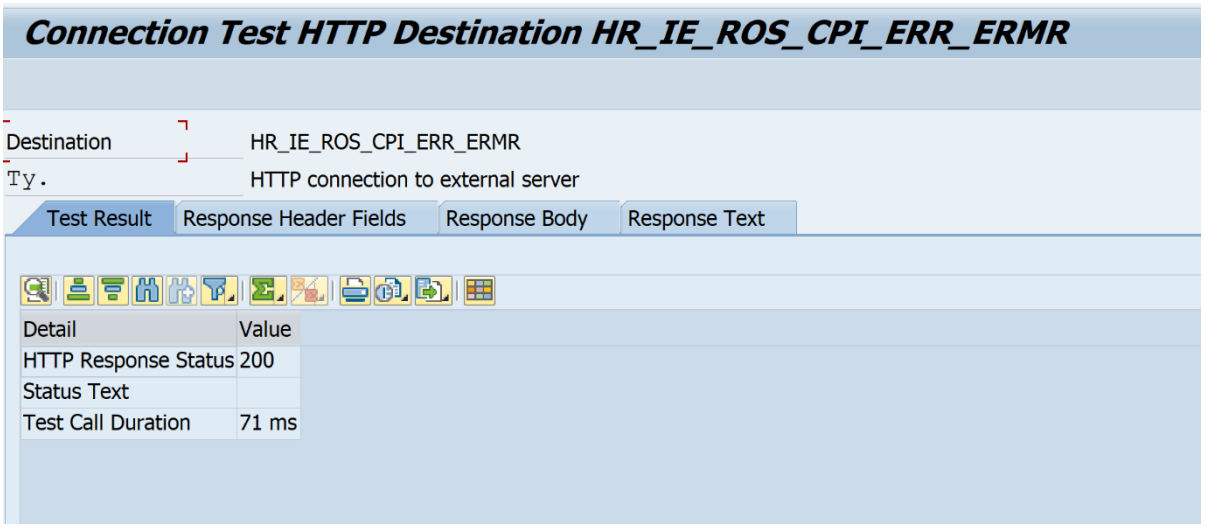
ii) *Logon with ticket*: Select **Do Not Send Logon Ticket**

iii) *Security options*: Select **SSL Active** and **SSL Certificate Default SSL Client (Standard)**

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 **200**

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



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

3.6.1 Table of RFC connections

Use the table below as a proposal to create RFC destinations for each of the ROS services you will use.

REST Messages	RFC Destination	Description1	Path Prefix
Check ERR Submission	HR_IE_ROS_CI_CHECK_ERR_SUB	Check ERR submission	/http/GET/CheckERRSubmission
Check ERR Run	HR_IE_ROS_CI_ERR_RUN	Check ERR Run	/http/GET/CheckERRRun
Enhanced Reporting Submission	HR_IE_ROS_CI_ERR_SUB	Enhanced reporting submission	/http/POST/EnhancedReportingSubmission
Request Monthly ERR Report	HR_IE_ROS_CI_ERR_MONTHLY	Request Monthly ERR Report	/http/GET/MonthlyERRReport

> **Note**
>
> *1) 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.*
>
> *2) The above table is just a proposal of values for the RFC destination and description. You can customize these to suit your organisations naming conventions*
>
> *3) The host name is the* **< IFLMAP URL for the CI tenant>** *URL address of your CI tenant*
>
> *4) Log on and security settings must be setup according to your organisations requirements.*

1) 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.

> **Note**
>
> *More information can be found on SAP Help Portal*
> *https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/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)**

2) If everything is correctly set then **HTTP Response Status** should be with Value **490**

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

3.6.2 Configure B2A Manager constants

The RFC destinations created in the above steps have to be linked to the respective iFlows using the B2A manager constants table T50BK. Use the table below to configure the constants, DESTN, DEST1, DEST2 and DEST3. Make sure you enter the name of the RFC destination you have created.

a) Navigate to the transaction Table View maintenance (SM30)

b) Type in V_T50BK and make sure you are editing constants for country version 11

(In the Determine Work Area: Entry dialog box, 11 in the HCM Localization field)

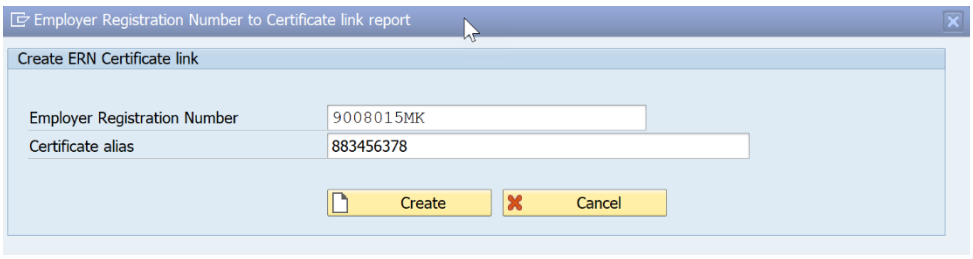
ERR submission constants

Grouping	Document Type	Constant	RFC Destination	Remarks
ROS	ERCR	DESTN	HR_IE_ROS_CPI_ERR_RUN	RFC destination – Check ERR run
ROS	ERCS	DESTN	HR_IE_ROS_CPI_CHECK_ERR_SUB	RFC destination – Check ERR submission
ROS	ERMR	DESTN	HR_IE_ROS_CI_ERR_MONTHLY	RFC destination – Monthly ERR report
ROS	ERRS	DEST1	HHR_IE_ROS_CPI_ERR_SUBMISSION	RFC destination – ERR submission
ROS	ERRS	DEST2	HR_IE_ROS_CPI_CHECK_ERR_SUB	RFC destination – Check ERR submission

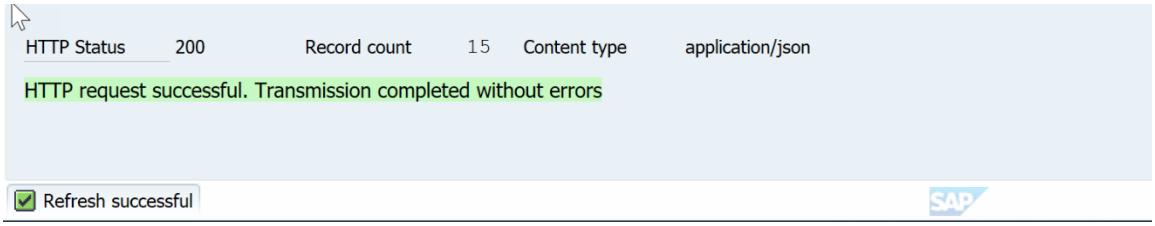
3.7 Store of Enterprise User Details into Partner Directory

To store Enterprise User Details into Partner Directory, follow these steps:

1) Execute the transaction code **PC00_M11_ERN_CERT**
2) A list of ERNs and associated certificate names will be displayed if already in the partner directory. Otherwise, you get a blank screen with the options to Create, Update and Delete entries
3) To create a new entry, press the Create link button.
4) Fill the **Employer Registration Number** and **Certificate alias** values according



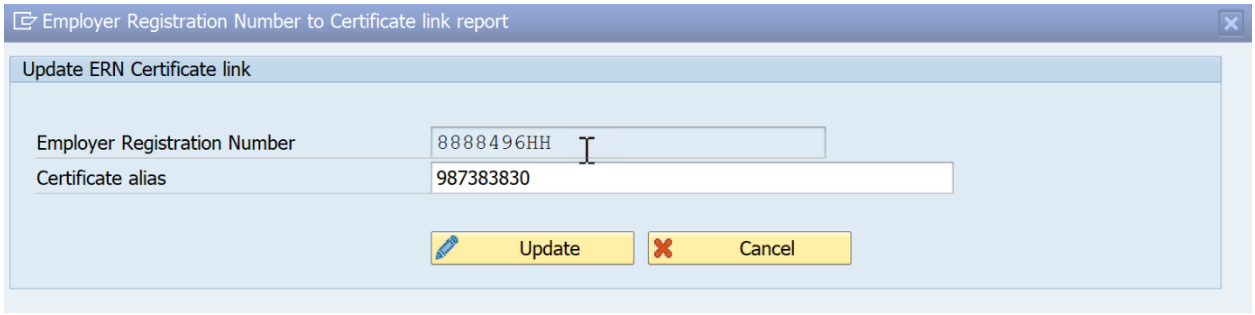
5) Click the *Create (F8)* button
6) If everything is *OK* then output will look like this:



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

7) To Update an existing record with a new certificate alias, select the line and press the *Update link* button.

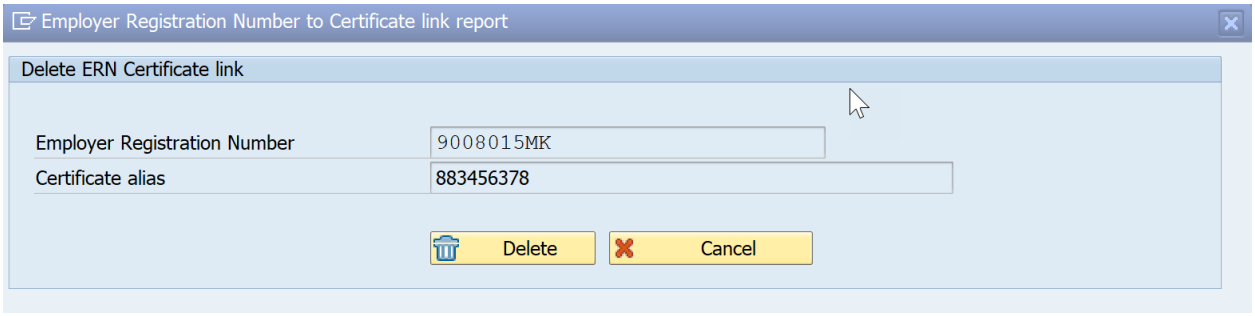
8) Enter the new alias and press the Update button

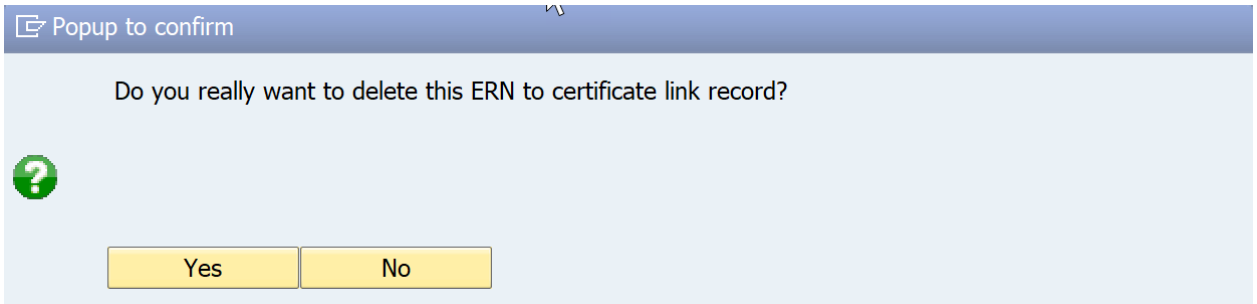


If successful, you will see the confirmation message at the bottom of the screen

9) To delete an existing record with a new certificate alias, select the line and press the *Delete link* button.

10) Confirm your intention to delete by confirming on the popup.

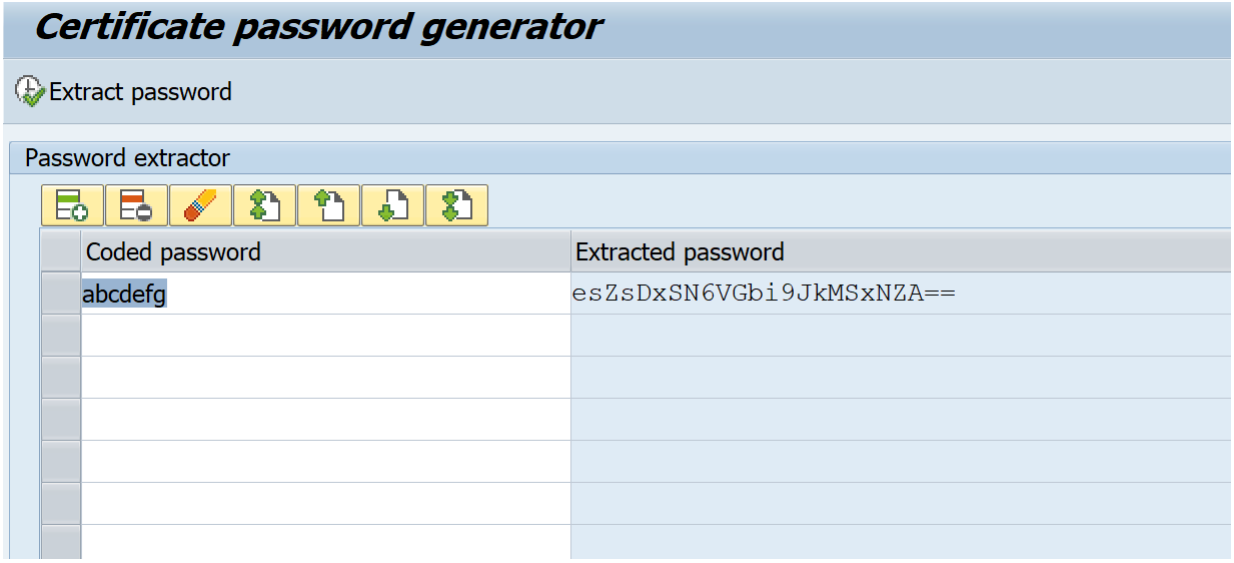




3.8 Password extractor program

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

The password that is sent to you when you request a new certificate for your ERN is encoded value. The actual password must be decoded and extracted from that value.



1. Execute the transaction code **PC00_M11_PWD_EXTRACT**
2. Enter the supplied coded password in the ALV list and press the execute button.
3. The decoded and extracted password is displayed.

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

4.0 Common Issues/Errors:

1. How to Upload SSL Certificates
2. How to Get SAP Cloud Integration Management URL
3. How to Get SAP Cloud Integration Runtime URL
4. Certificate expiry alerts in your CF tenant are failing with "Unexpected character '=' (code 61); expected a semi-colon after the reference for entity 'client_id'"
5. OAuth with Client Credentials Grant for API Clients

© 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: