Configuration Guide
AltinnECRestAPI
Document Version: 1.0 – 2021-11-03

CUSTOMER

Human Experience Management solutions from SAP Integration with Altinn REST API

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`.

Document History

Version	Date	Change
1.0	2021-11-03	Initial version
1.1	2025-09-25	Adding configurable field Address to all integration flows

Contents

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 Norway. 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 Altinn 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 Altinn 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 'HRNO-Altinn REST API' Solution

You installed and configured the "HRNO-Altinn REST" 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 "HRNO-Altinn REST" 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:*
>
> - *3111340 - HRNO - Altinn REST API – November 2021 [2] - source code*
> - *Recommended SAP Notes are latest SAP Notes for 'HRNO-Altinn REST API' solution as it's described in SAP Note 3111909.*

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 Norway. 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 Altinn SSL Certificate

The actual Altinn SSL certificate for HTTPS communication is always used on the Altinn main web page https://www.altinn.no/. More information can be found here: https://www.altinn.no/en/help/ or Altinn support can be contacted to get the actual Altinn SSL Certificate.

> **Note**
>
> *Instructions how to download the SSL Certificate from https://www.altinn.no/ 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 Enterprise Certificate

More information about the required enterprise certificate is published on the Altinn web page at: https://www.altinn.no/en/help/logging-in/altinn-alternative-log-in-methods/enterprise-certificate/ or Altinn support can be contacted to get more information .

> **Note**
>
> *Remind the client that only one enterprise certificate is supported in "HRNO-Altinn REST API" solution. It's recommended to use Enterprise Certificate of SAP Cloud Integration tenant owner. Rights for electronic communication on behalf of other organizations can be assigned in the Altinn web portal.*

2.6 Altinn REST API Key

The Altinn REST API Key is required for communication with Altinn by using REST API. More information can be found here: https://altinn.github.io/docs/api/rest/kom-i-gang/ (only in Norwegian) or Altinn support can be contacted to get Altinn REST API Key.

> **Note**
>
> *It's recommended to get the Altinn REST API Key for the SAP Cloud Integration tenant owner organization.*

2.7 Enterprise User in Altinn

More information about how to create an Enterprise User in Altinn is published on the Altinn web page at: https://www.altinn.no/en/help/logging-in/altinn-alternative-log-in-methods/enterprise-certificate/ or Altinn support can be contacted to get more information .

> **Note**
>
> *More Enterprise Users can be created for one Enterprise Certificate. Each Enterprise User can have different rights e.g., to represent different organizations.*

> **Note**
>
> *The "HRNO-Altinn REST API" solution allows you to have one Enterprise User for one system user in the SAP back-end system. The same Enterprise User can be used by more system users in the SAP back-end system, or each system user in SAP back-end system can use their own Enterprise User.*

2.8 Partner Directory URL

Enterprise User details will be stored in the Partner Directory under a random Globally Unique Identifier. The Partner Directory 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'

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

2.9 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."*

2.10 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/.*

3 Configuration Steps in SAP Cloud Integration

3.1 General Information

The package Human Experience Management solutions from SAP Integration with Altinn REST API contains the following iFlows:

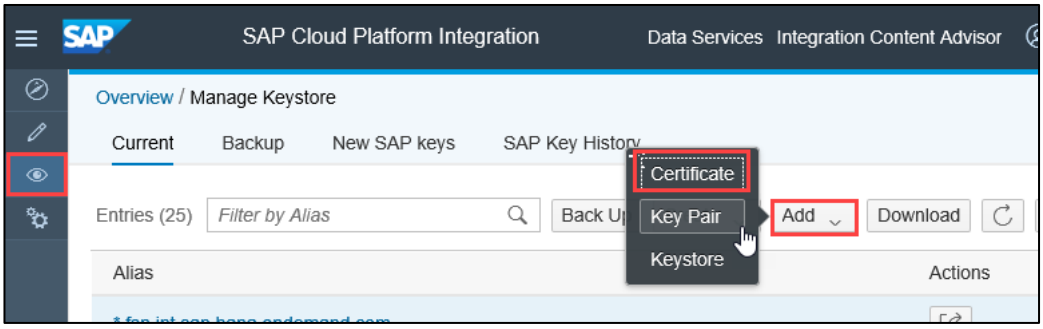
iFlow Name in WebUI	Project Name/Artifact Name
Enterprise Certificate User Manager	com.sap.GS.HR.NO.Altinn.EC.USR_MNG
Enterprise Certificate REST API Gateway to Altinn	com.sap.GS.HR.NO.Altinn.EC.REST_API

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 Altinn SSL Certificate to Keystore

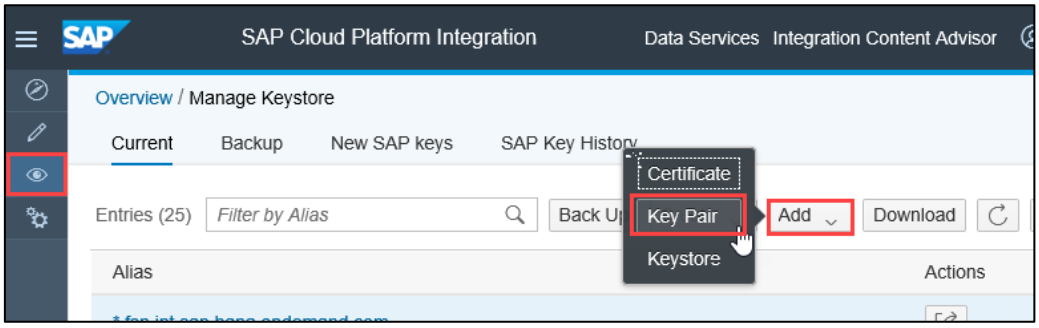
1) In the CPI, open the *Overview* section
2) In the *Manage Security* section, click the **Keystore** tile
3) Click the *Add* button and select **Certificate**



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

3.2.2 Uploading of Enterprise Certificate to Keystore

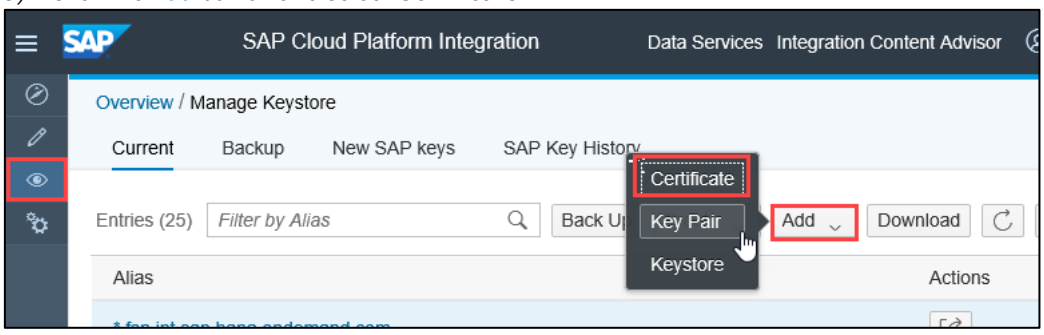
1) In the CPI, open the *Overview* section
2) In the *Manage Security* section, click the **Keystore** tile
3) Click the *Add* button and select **Key Pair**



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

3.2.3 Uploading of Tenant Management 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**

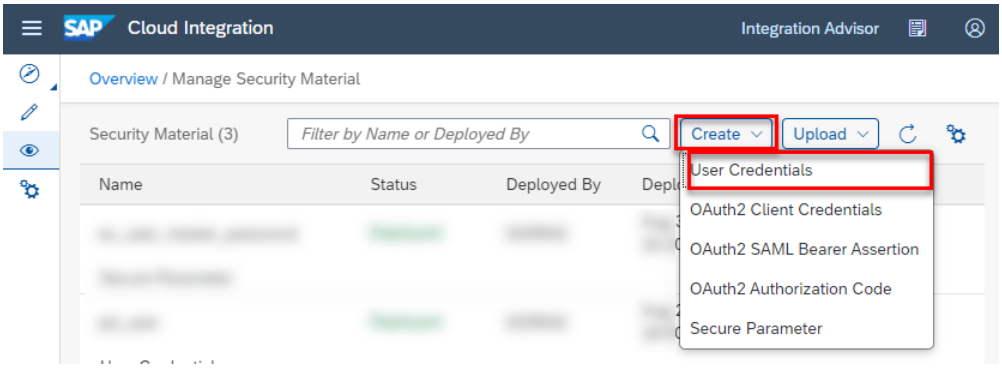


4) In the pop-up window, enter the **Alias** for the Key Pair (e.g. `tmn_ssl`). Then select the file with Partner Directory SSL Certificate. The file with the certificate should be in CRT or CER format.

3.3 Store Sensitive Information into Security Material

3.3.1 Store Details of Partner Directory User Details

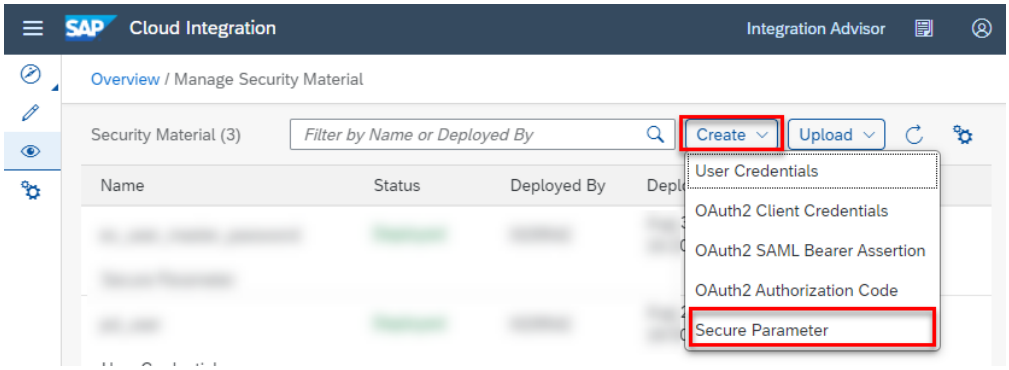
1) In the CPI, open the *Overview* section
2) In the *Manage Security* section, click the **Security Material** tile
3) Click the *Create* button and select **User Credential**



4) In the pop-up window, enter the **Name** for the User Credential (e.g. `pd_user`). And fill in User Name and Password of the Partner Directory User.

3.3.2 Store Master Password for Enterprise User Details

1) In the CPI, open the *Overview* section
2) In the *Manage Security* section, click the **Security Material** tile
3) Click the *Create* button and select **Secure Parameter**

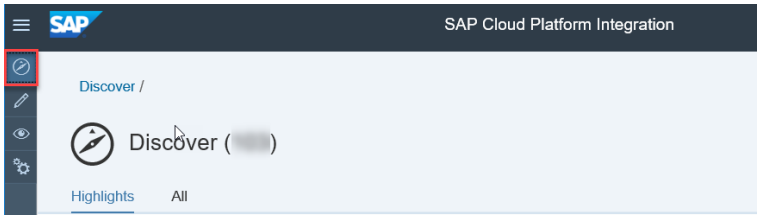


4) In the pop-up window, enter the **Name** for the User Credential (e.g. `ec_user_master_password`). And fill in the Master Password as Secure Parameter.

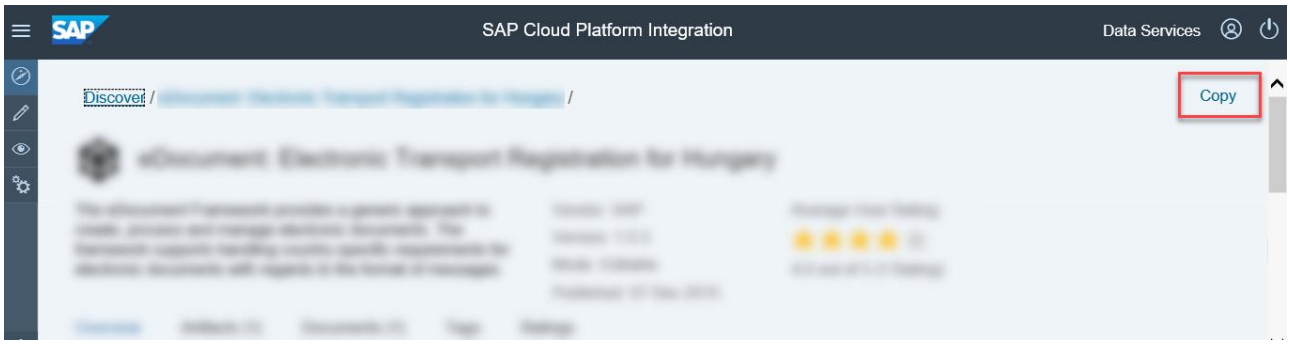
> **Note**
>
> *All Enterprise Users details will be stored with using this Master Password. If the Master Password will be changed in this Secure Parameter, then the already stored Enterprise User details will be unreadable and needs to be stored again.*

3.4 Copy Published Integration Package

1) In the *Discover* section of your tenant, select the package Human Experience Management solutions from SAP Integration with Altinn REST API.



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



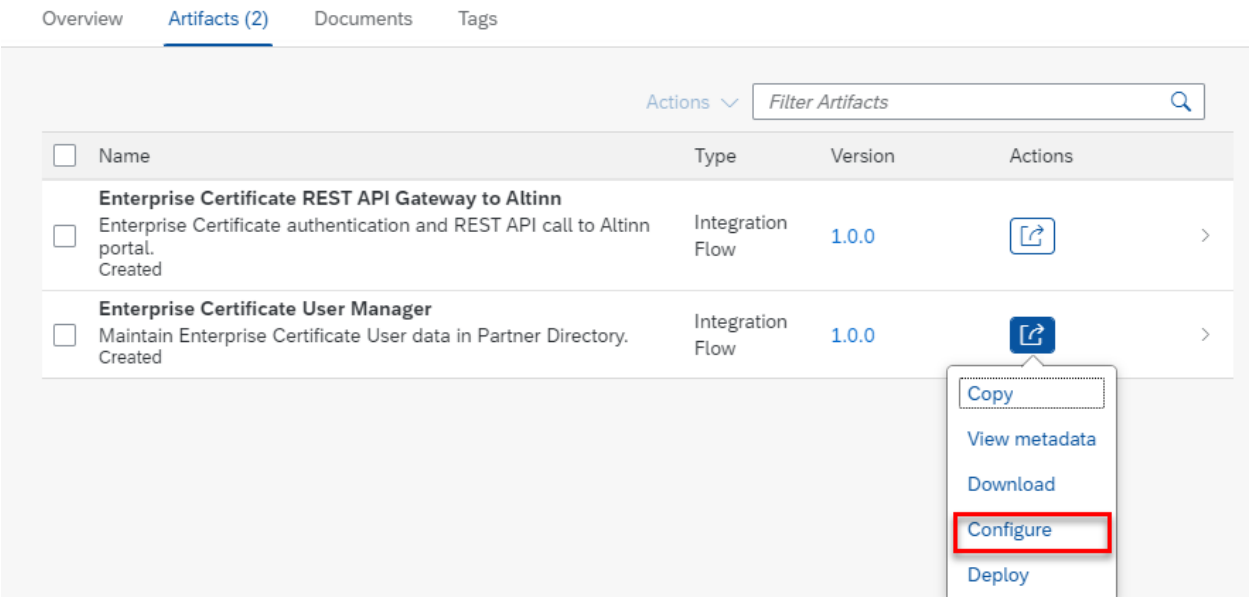
3.5 Configure Integration Flows

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

3.5.1 Configuration of Enterprise Certificate User Manager iFlow

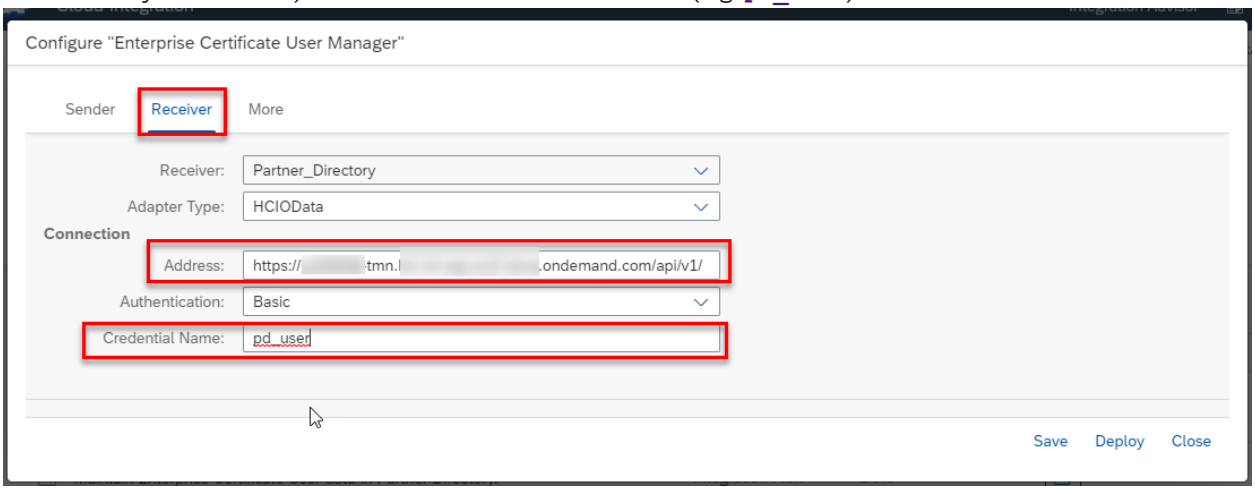
1) Go to the integration package that was copied from the original Human Experience Management solutions from SAP Integration with Altinn REST API.
2) Click the *Artifacts* tab

3) Click on the *Actions* button that corresponds to integration flow **Enterprise Certificate User Manager** and choose **Configure**



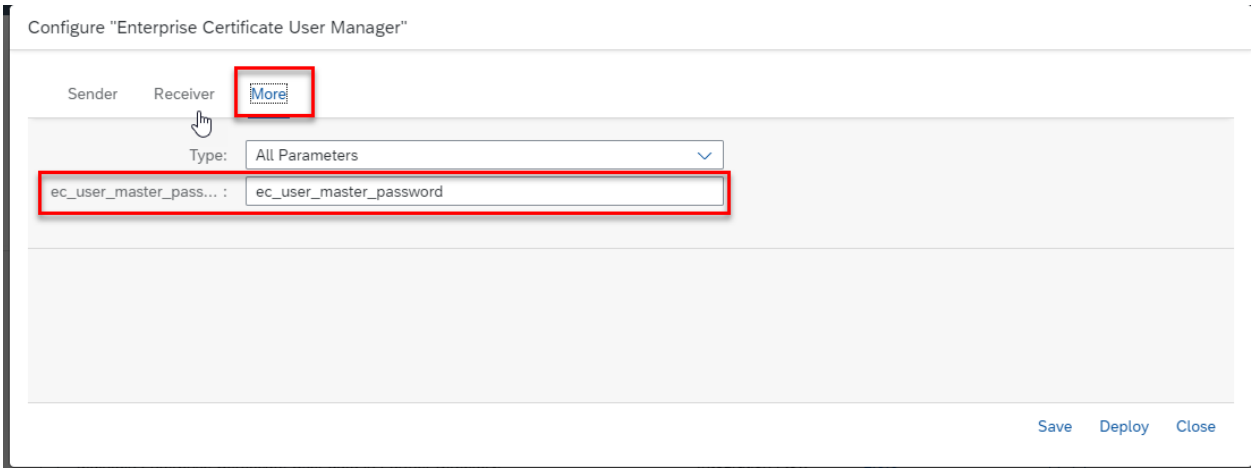
Click the *Receiver* tab

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 (e.g. **`pd_user`**)



7) Click the *More* tab

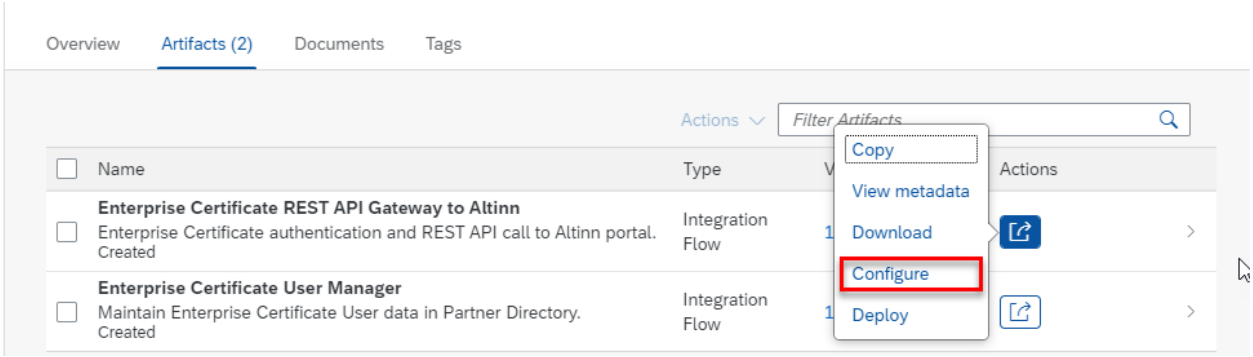
8) Fill in the name of Security Material with Master Password (see chapter Store Master Password for Enterprise User Details) value for the *ec_user_master_password_alias* field (e.g. **`ec_user_master_password`**)



9) Select *Deploy*.

3.5.2 Configuration of Enterprise Certificate REST API Gateway to Altinn iFlow

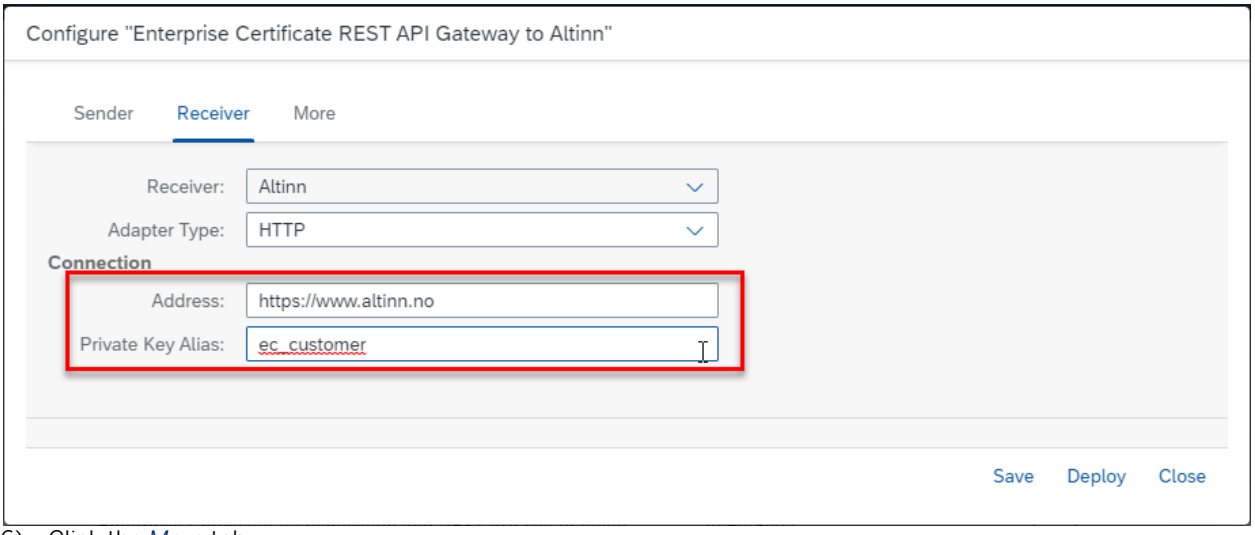
1) Go to the integration package that was copied from the original Human Experience Management solutions from SAP Integration with Altinn REST API.
2) Click the *Artifacts* tab
3) Click on the *Actions* button that corresponds to integration flow **Enterprise Certificate REST API Gateway to Altin** and choose **Configure**



Click the *Receiver* tab

4) Fill in the Altinn URL as value for *Address* field (e.g. **`https://www.altinn.no`**)

5) Fill the alias of the key pair with the Enterprise Certificate (see chapter Uploading of Enterprise Certificate to Keystore) as the value for the *Private Key Alias* field (e.g. **`ec_customer`**)

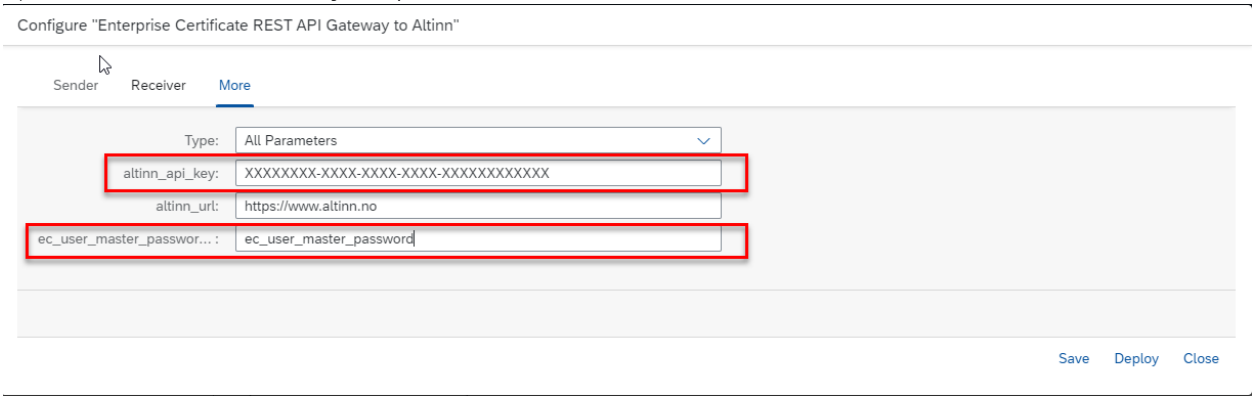


6) Click the *More* tab

7) Fill in the value of the Altinn REST API Key (see chapter Altinn REST API Key) to *altinn_api_key* field (e.g. **`12345678-1A2B-3C4D-5E6F-9876543210AB`**)

8) Fill in the name of the Security Material with the Master Password (see chapter Store Master Password for Enterprise User Details) value for *ec_user_master_password_alias* field (e.g. **`ec_user_master_password`**)

9) Field *altinn_url* will already be updated with the value from *the Address* field on the *Receiver* tab



10) Select *Deploy*.

> **Note**
>
> A new configurable field *Address* was added to the sender tab in the configuration version 1.1. Changing the default value in this field needs to be reflected in the next steps – section 4.1 (in path prefix field, use URL to the CI for each changed iflow as */http/<your configured value>*),

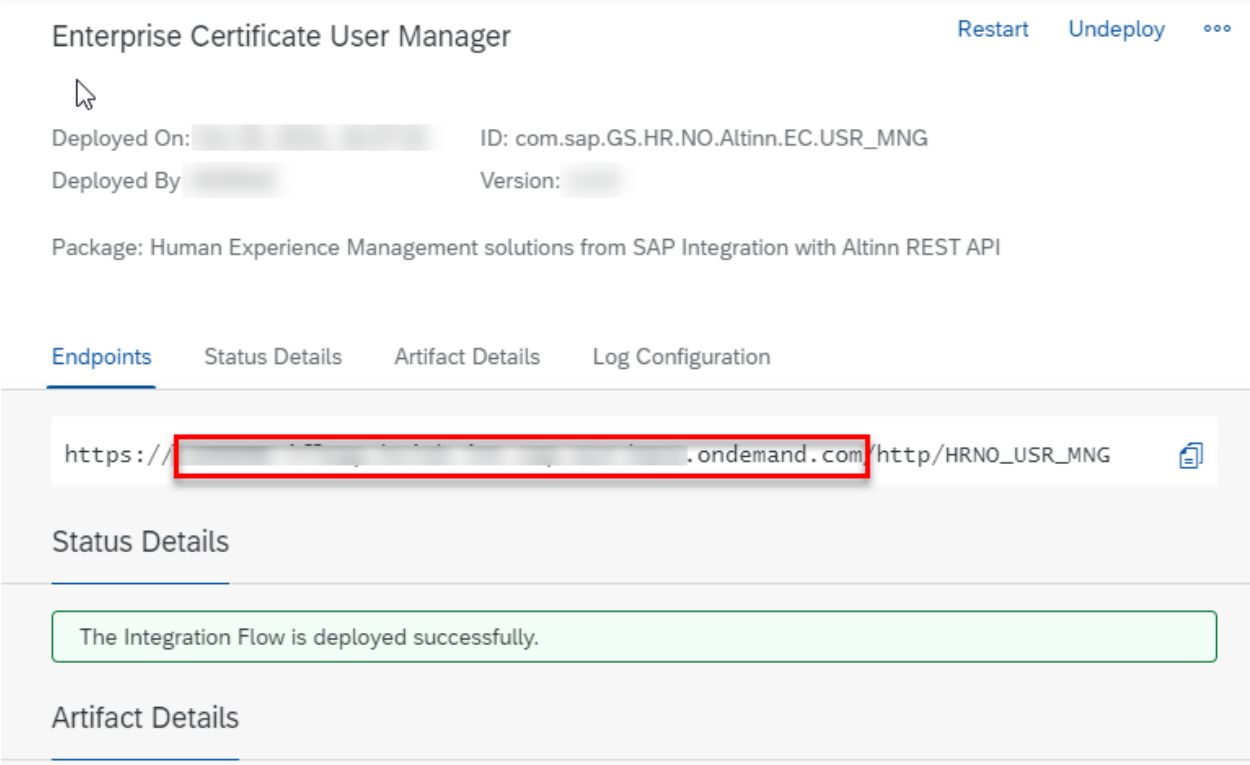
4 Configuration Steps in SAP ERP or SAP SuccessFactors Employee Central Payroll

In the SAP back-end system, you need to configure the HTTPS connection to the CPI 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 CPI Overview → Manage Integration Content → Select deployed Enterprise Certificate User Manager iFlow.

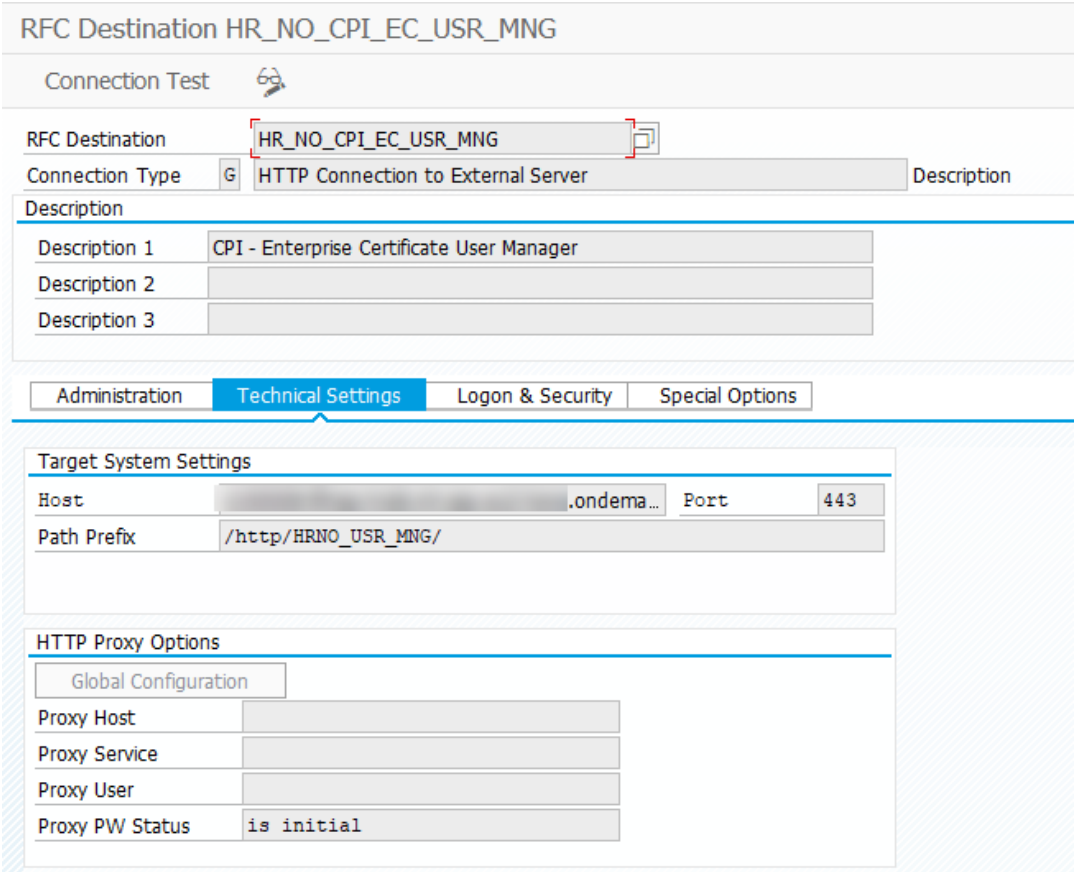


> **Note**
>
> *To setup a secure HTTPS connection between the SAP back-end system and the SAP Cloud Integration tenant, add the load balancer root certificate to the SAP back-end system trust store.*

1) Execute the transaction code **SM59**
2) To create a new connection, select *Edit → Create*
3) For the RFC destination, enter value **HR_NO_CPI_EC_USR_MNG** for the connection name
4) Set connection type **G** (HTTP Connection to External Server)
5) Enter **CPI - Enterprise Certificate User Manager** in the *Description* field
6) On the *Technical Settings* tab, enter the following values
   a) Target Host: **< IFLMAP URL for the CPI 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: **/http/HRNO_USR_MNG/**
   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

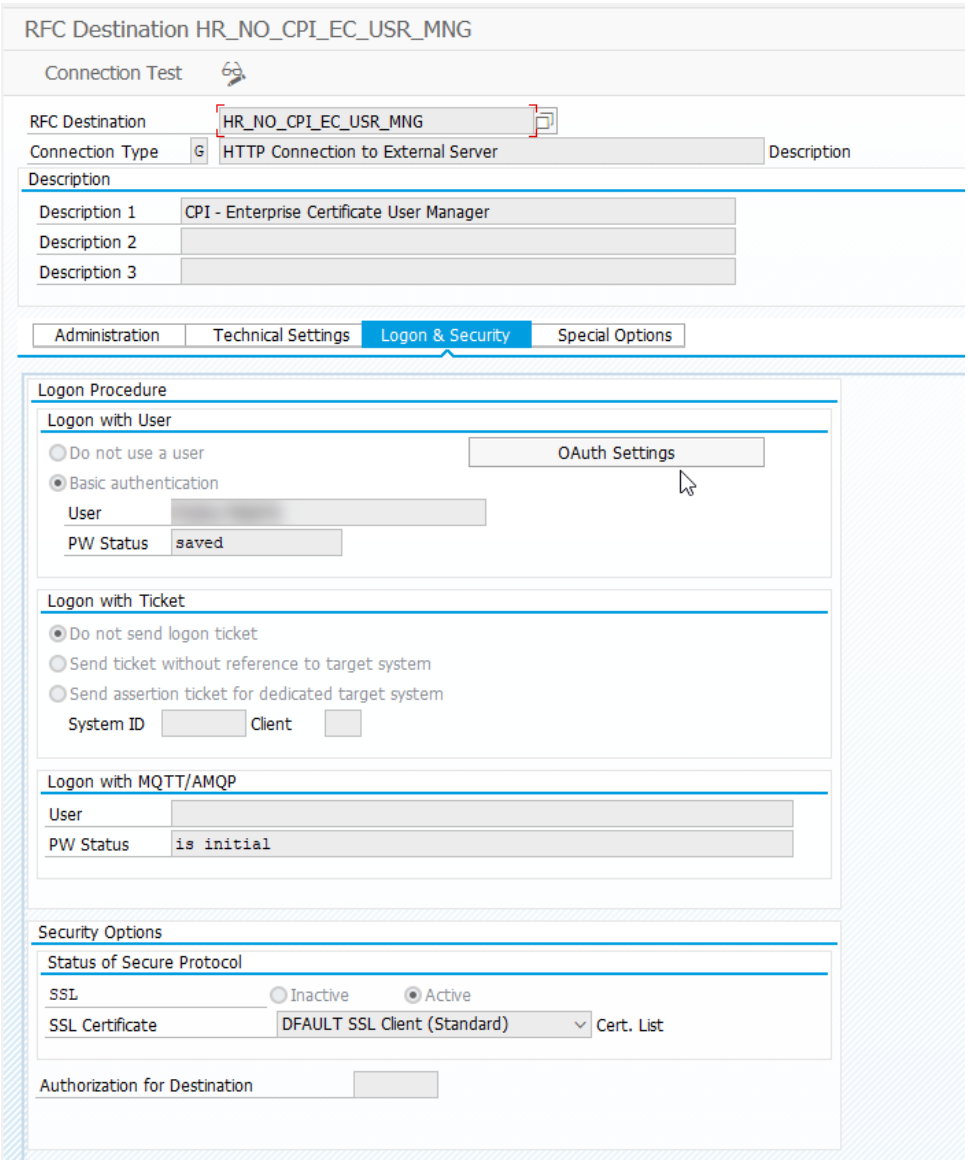
More information can be found on SAP Help Portal
https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/24585cc503334e6c917ef383efb5558a.html?q=ESBMessaging.send

In the *Logon & Security* tab enter:

i) *Logon with user*: Choose **Basic Authentication** and enter a valid **user** and **password** for logging on to CPI

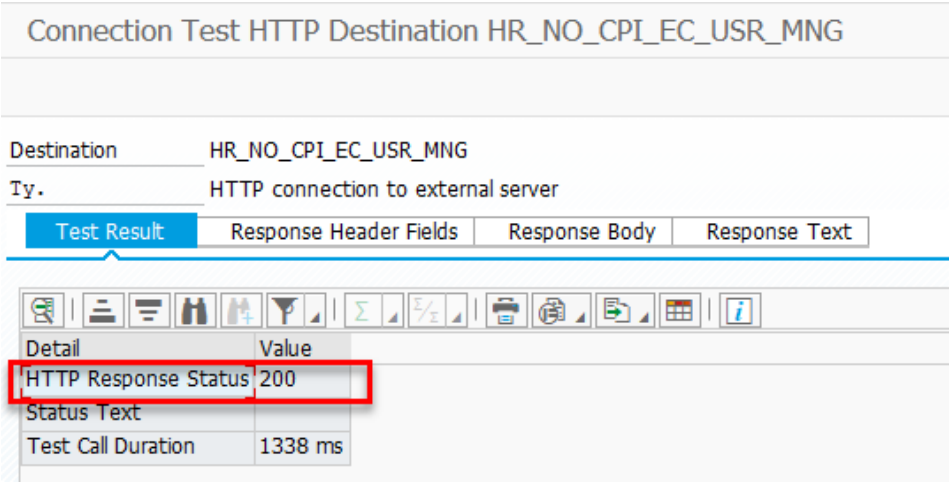
ii) *Logon with ticket*: Select **Do Not Send Logon Ticket**

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



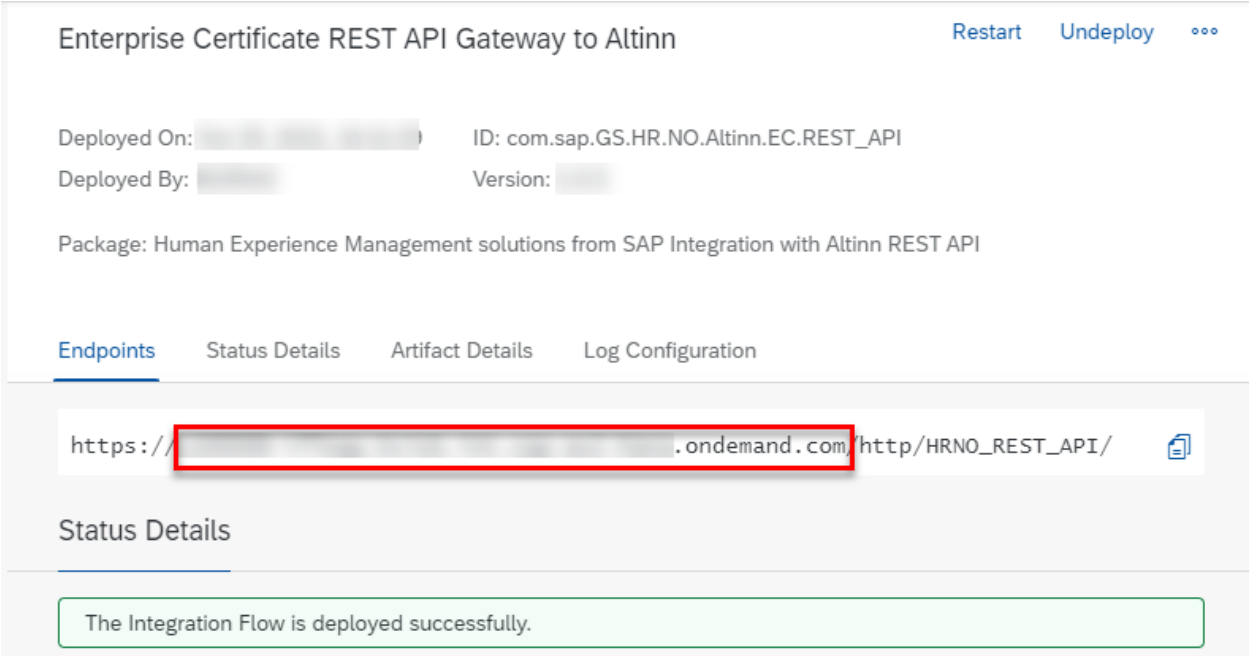
b) **Client certificate-based authentication**
Set up the client certificate in the SAP back-end system and upload to Cloud Integration in the certificate-to-user mapping as described in the blog https://blogs.sap.com/2017/06/05/cloud-integration-how-to-setup-secure-http-inbound-connection-with-client-certificates/

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**



4.2 Configuration of connection to Enterprise Certificate REST API Gateway to Altinn

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 CPI Overview → Manage Integration Content → Select deployed Enterprise Certificate REST API Gateway to Altinn iFlow



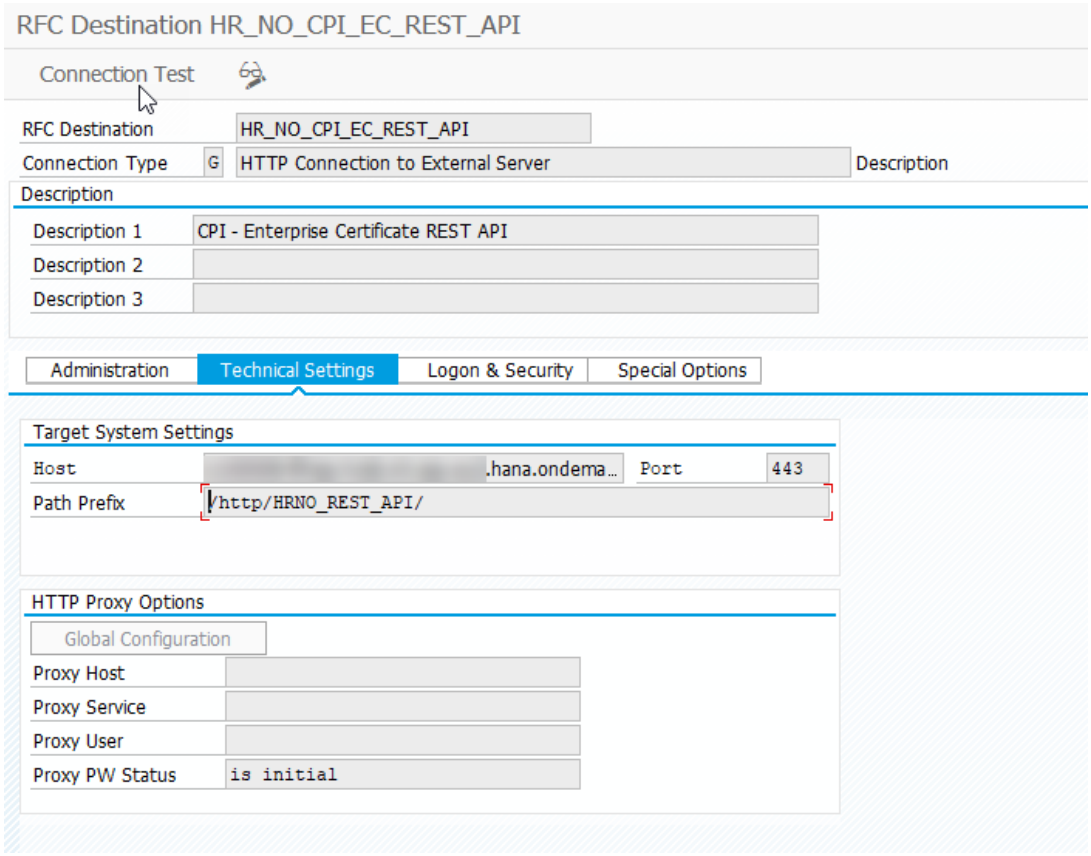
> **Note**
>
> *To setup a secure HTTPS connection between the SAP back-end system and the SAP Cloud Integration Tenant, add the load balancer root certificate to the SAP back-end system trust store.*

1) Execute the transaction code **SM59**
2) To create a new connection, select *Edit → Create*
3) For the RFC destination, enter value **HR_NO_CPI_EC_REST_API** for the connection name
4) Set connection type **G** (HTTP Connection to External Server)
5) Enter **CPI - Enterprise Certificate REST API** in the *Description* field
6) On the *Technical Settings* tab, enter the following values
   a) Target Host: **< IFLMAP URL for the CPI 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: **/http/HRNO_REST_API/**

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.

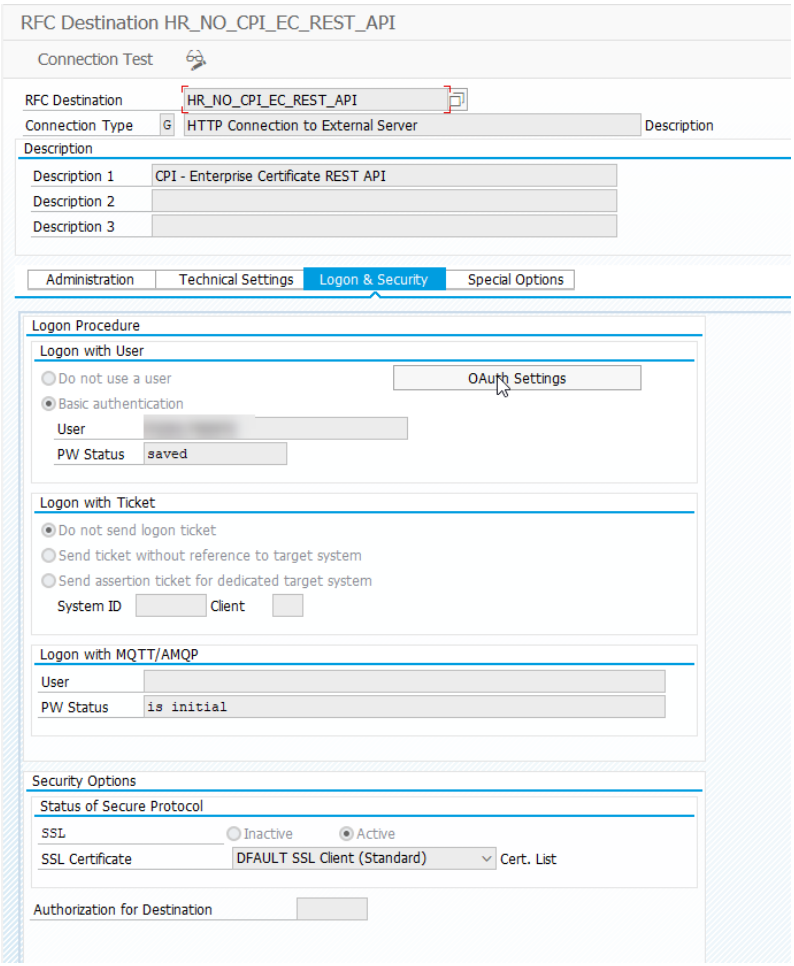
> **Note**
>
> *More information can be found on SAP Help Portal*
> *https://help.sap.com/viewer/368c481cd6954bdfa5d0435479fd4eaf/Cloud/en-US/24585cc503334e6c917ef383efb5558a.html?q=ESBMessaging.send*

In the *Logon & Security* tab enter:

i) *Logon with user*: Choose **Basic Authentication** and enter a valid **user** and **password** for logging on to CPI

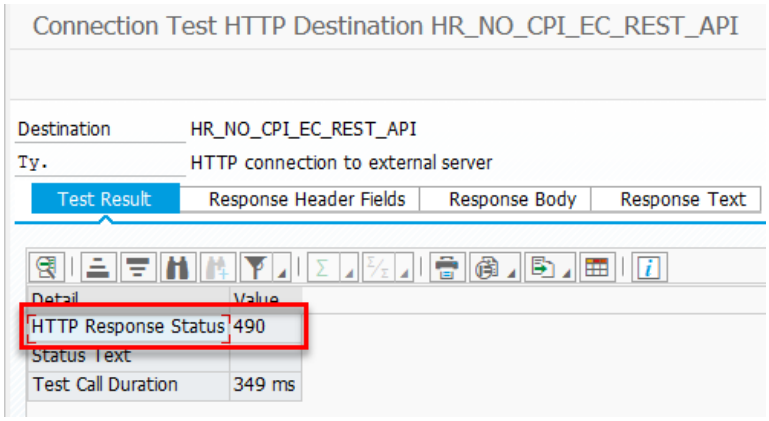
ii) *Logon with ticket*: Select **Do Not Send Logon Ticket**

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 **490**



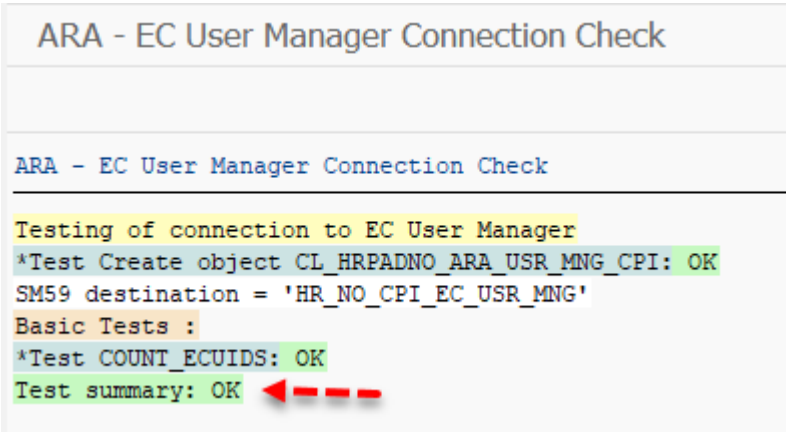
4.3 Basic Communication Tests

To test the communication, the best way is to execute the test reports from your SAP back-end system.

4.3.1 Test of Basic Communication with Enterprise Certificate User Manager iFlow

To test the communication with Enterprise Certificate User Manager iFlow follow these steps:

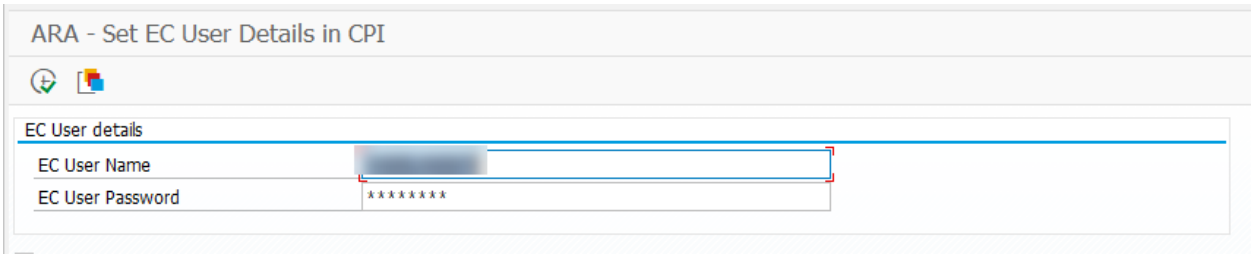
1) Execute the transaction code **SA38 (or SE38)**
2) Fill the Program field with the value **HNOUARA_UM_CHECK**
3) Click the *Execute (F8)* button
4) If *Test summary* is *OK* then basic test of connection to Enterprise Certificate User Manager iFlow was success



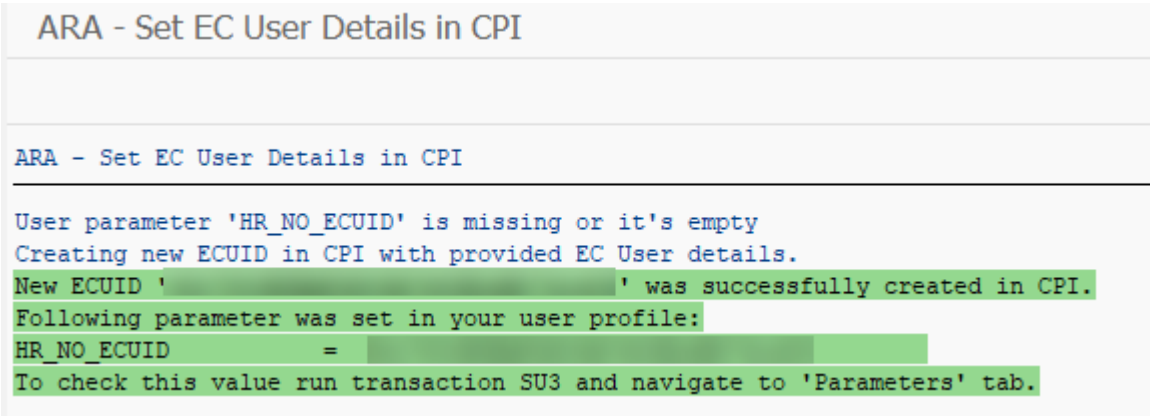
4.3.2 Store of Enterprise User Details into Partner Directory

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

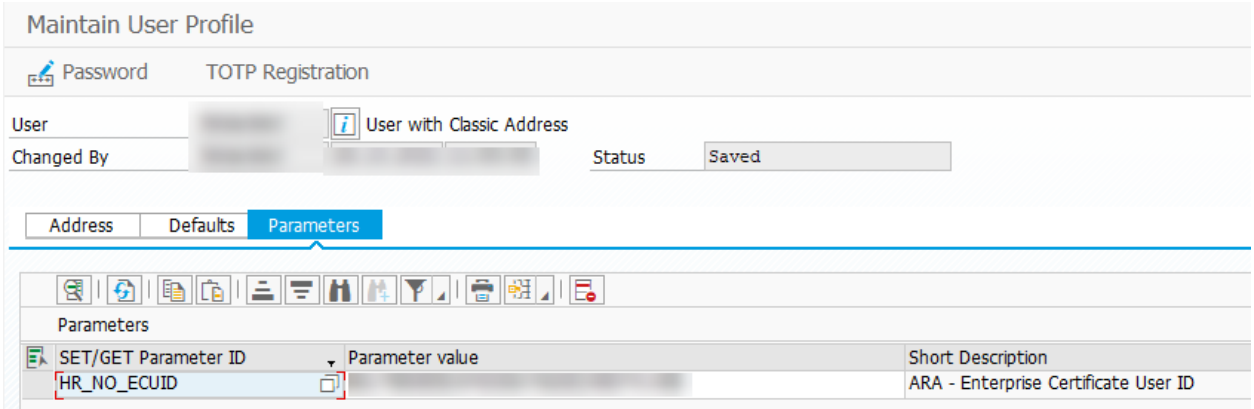
1) Execute the transaction code **PC00_M20_ARA_ECUID**
2) Fill the **EC User Name** and **EC User Password** values according Enterprise User registration in Altinn (see chapter Enterprise User in Altinn)



3) Click the *Execute (F8)* button
4) If everything is *OK* then output will look like this:



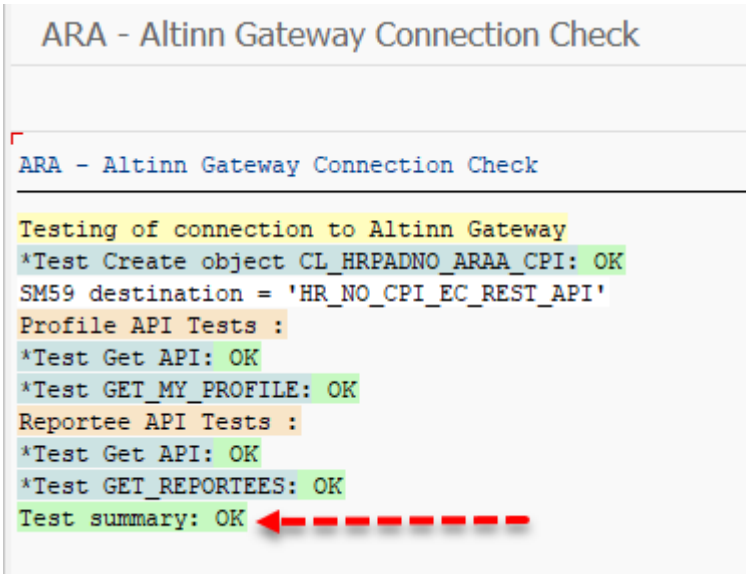
5) To verify check **HR_NO_ECUID** parameter in transaction **SU3** according instructions



4.3.3 Test of Basic Communication with Enterprise Certificate REST API Gateway to Altinn iFlow

To be able to test the communication with Enterprise Certificate REST API Gateway to Altinn, it's necessary to have completed the chapter Store of Enterprise User Details into Partner Directory.
To test, follow these steps:

1) Execute the transaction code **SA38 (or SE38)**
2) Fill the Program field with the value **HNOUARA_GW_CHECK**
3) Click the *Execute (F8)* button
4) If *Test summary* is *OK* then basic test of connection to Enterprise Certificate REST API Gateway to Altinn was success



www.sap.com/contactsap

Material Number: