

Configuration Guide

Altinn3Interface

Document Version: 1.1 – 2026-03-30

CUSTOMER

SAP ERP Integration with Norwegian Altinn 3 Interface

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	2026-02-17	Initial version
1.1.	2026-03-30	Clarification of certificates needed in SAP Cloud Integration

Contents

1	Introduction	5
2	Prerequisites.....	6
2.1	Installation of 'SAP ERP Integration with Norwegian Altinn 3 Interface' Solution	6
2.2	Set Up of Secure Connection.....	6
2.3	Set Up SAP Cloud Integration Tenants.....	7
2.4	Skatteetaten SSL Certificate	7
2.5	Maskinporten SSL Certificate.....	7
2.6	Altinn SSL Certificate	8
2.7	Maskinporten setup.....	8
3	Configuration Steps in SAP Cloud Integration	9
3.1	General Information.....	9
3.2	Deploying Key Pairs and Certificates.....	9
3.2.1	Uploading of Enterprise Certificate to Keystore	9
3.2.2	Uploading of Skatteetaten, Altinn and Maskinporten SSL Certificate to Keystore	10
3.3	Copy Published Integration Package	11
3.4	Configure Integration Flows.....	12
3.4.1	Configuration of Employer's Tax Card iFlow	12
3.4.2	Configuration of Information on future deductions iFlow	13
3.4.3	Configuration of Maskinporten authorization for Altinn iFlow	14
3.4.4	Configuration of System and system user registration iFlow	15
4	Configuration Steps in SAP ERP or SAP SuccessFactors Employee Central Payroll	16
4.1	Configuration of connection to Employers tax card.....	16
4.2	Configuration of connection to Information on future deductions	20
4.3	Configuration of connection to System and system user registration	23

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 Capital 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.

i 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 'SAP ERP Integration with Norwegian Altinn 3 Interface' Solution

You installed and configured the "HRNO: Altinn v3 integration" 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 v3 integration" 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:

- 3653955 - HRNO: Altinn v3 integration

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 Skatteetaten SSL Certificate

The Skatteetaten SSL certificate for HTTPS communication can be downloaded from the urls mentioned in the documentation in sections 3.4.1 or 3.4.2 or Skatteetaten support can be contacted to get the actual Skatteetaten SSL Certificate.

Note

Instructions how to download the SSL Certificate 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 Maskinporten SSL Certificate

The Maskinporten SSL certificate for HTTPS communication can be downloaded from the urls mentioned in the documentation in section 3.4.4 or Maskinporten support can be contacted to get the actual Maskinporten SSL Certificate.

Note

Instructions how to download the SSL Certificate 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."

2.6 Altinn SSL Certificate

The Altinn SSL certificate for HTTPS communication can be downloaded from the urls mentioned in the documentation in section 3.4.3 or Altinn support can be contacted to get the actual Altinn SSL Certificate.

i Note

Instructions how to download the SSL Certificate 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."

2.7 Maskinporten setup

To communicate with the new Altinn interface, you will need to setup a Maskinporten client. Please follow the guide provided by Altinn on how to set this up. <https://docs.altinn.studio/nb/authorization/getting-started/maskinportenclient/>

During the process, save the created client id and the PEM/JWT authentication key uploaded as well as key id assigned to it.

3 Configuration Steps in SAP Cloud Integration

3.1 General Information

The package *SAP ERP Integration with Norwegian Altinn 3 Interface* contains the following iFlows:

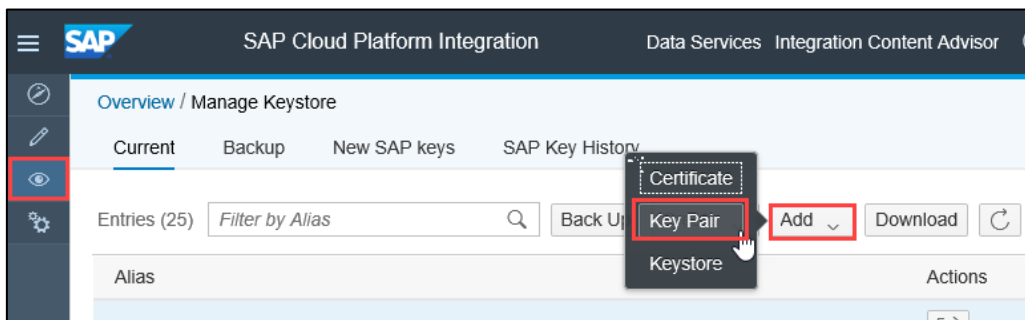
iFlow Name in WebUI	Project Name/Artifact Name
System and system user registration	com.sap.GS.HR.NO.Altinn3.System
Maskinporten authorization for Altinn	com.sap.GS.HR.NO.Altinn3.Maskiporten
Employers tax card	com.sap.GS.HR.NO.Altinn3.EmployersTaxCard
Information on future deductions	com.sap.GS.HR.NO.Altinn3.FutureDeductions

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 Company Certificate to Keystore

- 1) Locate a key pair corresponding to the public key you have uploaded to Maskinporten in section 2.7
- 2) In the CP, open the *Overview* section
- 3) In the *Manage Security* section, click the **Keystore** tile
- 4) Click the *Add* button and select **Key Pair**

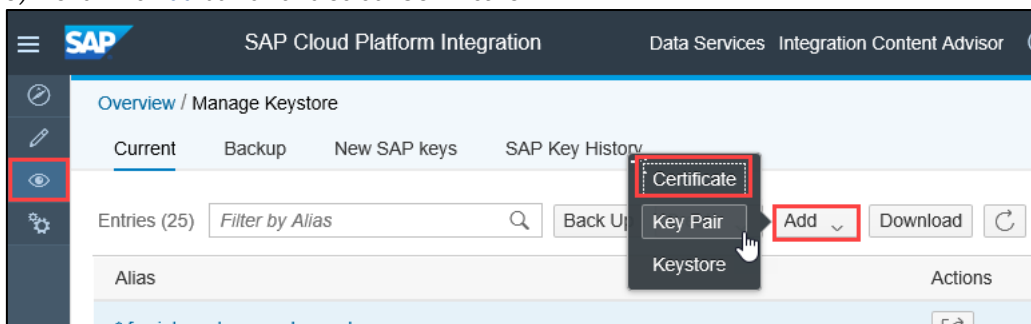


- 5) In the pop-up window, enter the **Alias** for the Key Pair (e.g. `ec_customer`). Then select the file with the Error! Reference source not found.. The file with the certificate should be in P12 or PFX format. Enter the corresponding password for this file in the **Password** field.

Please note this needs to be the key pair corresponding to the public key uploaded to Maskinporten in step 2.6.

3.2.2 Uploading of Skatteetaten, Altinn and Maskinporten SSL Certificate to Keystore

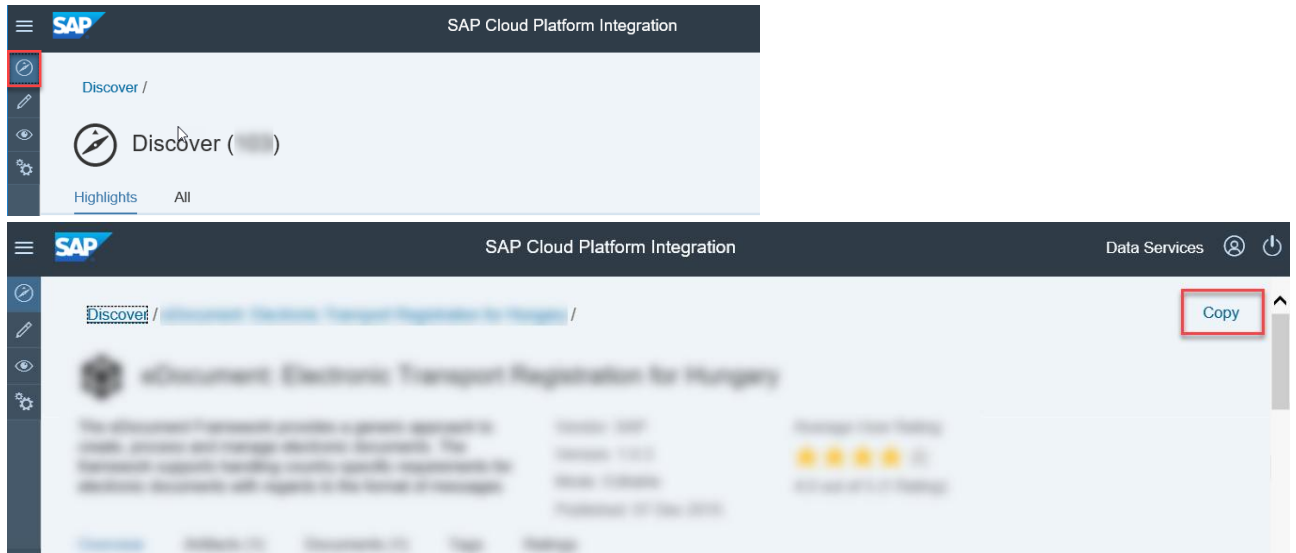
- 1) In the CPI, open the *Overview* section
- 2) In the *Manage Security* section, click the **Keystore** tile
- 3) Click the *Add* button and select **Certificate**



- 4) In the pop-up window, enter the **Alias** for the Key Pair (e.g. skatteetaten_ssl, altinn_ssl or maskinporten_ssl). Then select the file with Error! Reference source not found.s extracted in steps 2.4, 2.5. and 2.6 The file with the certificate should be in CRT or CER format.

3.3 Copy Published Integration Package

- 1) In the *Discover* section of your tenant, select the package Error! Reference source not found..



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

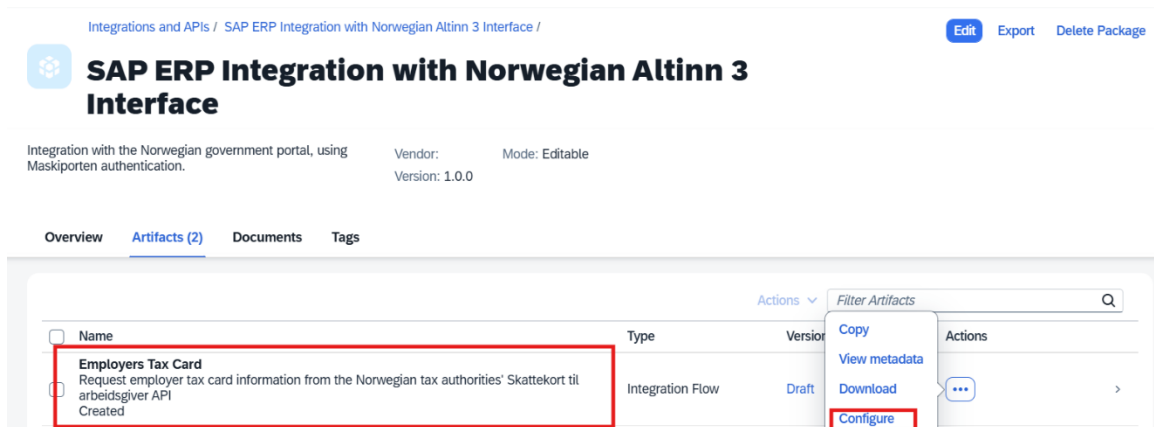
3.4 Configure Integration Flows

i Note

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

3.4.1 Configuration of Employer's Tax Card iFlow

- 1) Go to the integration package that was copied from the original *SAP ERP Integration with Norwegian Altinn 3 Interface*.
- 2) Click the *Artifacts* tab
- 3) Click on the *Actions* button that corresponds to integration flow **Employers Tax Card** and choose **Configure**



Click the *More* tab

- 4) Fill out the fields Address polling/sending to correspond to the environment you intend to use.
 - For test environment, put <https://api-test.sits.no/api/forskudd/skattekortTilArbeidsgiver/svar/> for polling and <https://api-test.sits.no/api/forskudd/bestillSkattekort> for sending
 - For production, put <https://api.skatteetaten.no/api/forskudd/skattekortTilArbeidsgiver/svar/> for polling and <https://api.skatteetaten.no/api/forskudd/bestillSkattekort> for sending
- 5) If needed, use the fields in tabs sender and receiver to support multiple instances of the integration flow. Please note that you will need to update the configuration of RFC connection in transaction SM59 to match the address in the Sender tab.

3.4.2 Configuration of Information on future deductions iFlow

- 1) Go to the integration package that was copied from the original *SAP ERP Integration with Norwegian Altinn 3 Interface*.
- 2) Click the *Artifacts* tab
- 3) Click on the *Actions* button that corresponds to integration flow **Information on future deductions** and choose **Configure**

The screenshot shows the SAP Cloud Integration interface for the package "SAP ERP Integration with Norwegian Altinn 3 Interface". The "Artifacts (4)" tab is selected, displaying a table of integration flows. The flow "Information on future deductions" is highlighted with a red box. A context menu is open over its "Actions" column, with the "Configure" option selected and highlighted with a red box.

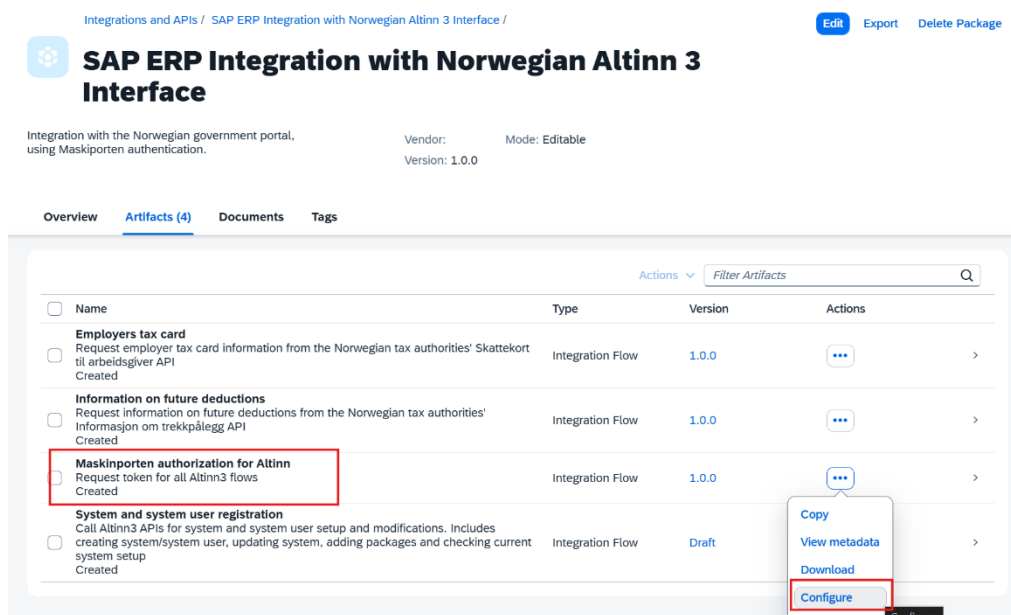
Name	Type	Version	Actions
Employers tax card Request employer tax card information from the Norwegian tax authorities' Skattekort til arbeidsgiver API Created	Integration Flow	1.0.0	...
Information on future deductions Request information on future deductions from the Norwegian tax authorities' Informasjon om trekkpålegg API Created	Integration Flow	1.0.0	... Copy View metadata Download Configure Deploy
Maskinporten authorization for Altinn Request token for all Altinn3 flows Created	Integration Flow	Draft	...
System and system user registration Call Altinn3 APIs for system and system user setup and modifications. Includes creating system/system user, updating system, adding packages and checking current system setup Created	Integration Flow	Draft	...

Click the *More* tab

- 4) Fill out the field Address sending to correspond to the environment you intend to use.
 - For test environment, put <https://api-test.sits.no/api/trekkpaalegg/v1>
 - For production, put <https://api.skatteetaten.no/api/trekkpaalegg/v1>
- 5) If needed, use the fields in tabs sender and receiver to support multiple instances of the integration flow. Please note that you will need to update the configuration of RFC connection in transaction SM59 to match the address in the Sender tab.

3.4.3 Configuration of Maskinporten authorization for Altinn iFlow

- 1) Go to the integration package that was copied from the original *SAP ERP Integration with Norwegian Altinn 3 Interface*.
- 2) Click the *Artifacts* tab
- 3) Click on the *Actions* button that corresponds to integration flow **Maskinporten authorization for Altinn** and choose **Configure**



Click the *Receiver* tab

- 4) Fill in the Maskinporten token URL as value for *Address* field (e.g. <https://test.maskinporten.no/token> for test or <https://maskinporten.no/token> for production)

Click the *More* tab

- 5) Fill the audience field with the desired Maskinported version url (test or production, e.g. <https://test.maskinporten.no/> or <https://maskinporten.no/>)
- 6) Fill in the value of the client id as generated in Maskinporten upon registration (see chapter Error! Reference source not found.) to *client id* field (e.g. **12345678-1A2B-3C4D-5E6F-9876543210AB**)
- 7) Fill the alias of the key pair with the Enterprise Certificate (see chapter Uploading of Company Certificate to Keystore) as the value for the *Credentials Alias* field (e.g. **ec_customer**)
- 8) Fill in the value of the key id as generated in Maskinporten upon registration (see chapter Error! Reference source not found.) to *key id* field (e.g. **12345678-1A2B-3C4D-5E6F-9876543210AB**)
- 9) Into field organization, input the organization identification number for the company registered in Maskinporten. If you are planning on submitting on behalf of multiple organization numbers, this will be the identification of the organization delegated the permissions via system user. The identification of the organization owning the data will be supplied during processing from the business system.
- 10) Select *Deploy*.
- 11) If needed, use the sender tab fields to configure multiple instances

3.4.4 Configuration of System and system user registration iFlow

- 1) Go to the integration package that was copied from the original *SAP ERP Integration with Norwegian Altinn 3 Interface*.
- 2) Click the *Artifacts* tab
- 3) Click on the *Actions* button that corresponds to integration flow **System and system user registration** and choose **Configure**

The screenshot shows the SAP Cloud Integration interface for the package 'SAP ERP Integration with Norwegian Altinn 3 Interface'. The 'Artifacts (4)' tab is active, displaying a table of integration flows. The flow 'System and system user registration' is highlighted with a red box. A context menu is open over this flow, with the 'Configure' option selected and highlighted by a red box. Other options in the menu include Copy, View metadata, Download, and Deploy. The table columns are Name, Type, Version, and Actions.

Name	Type	Version	Actions
Employers tax card Request employer tax card information from the Norwegian tax authorities' Skattekort til arbeidsgiver API Created	Integration Flow	1.0.0	...
Information on future deductions Request information on future deductions from the Norwegian tax authorities' Informasjon om trekkpålegg API Created	Integration Flow	1.0.0	...
Maskinporten authorization for Altinn Request token for all Altinn3 flows Created	Integration Flow	1.0.0	...
System and system user registration Call Altinn3 APIs for system and system user setup and modifications. Includes creating system/system user, updating system, adding packages and checking current system setup Created	Integration Flow	1.0.0	...

Click the *More* tab

- 4) Fill out the fields Prod/test environment address for both with the altinn host url.
 - For test environment, put <https://platform.tt02.altinn.no>
 - For production, put <https://platform.altinn.no>
- 5) Fill in the system endpoints as follows:
 - *System agent:* /authentication/api/v1/systemuser/request/vendor/agent
 - *System packages:* /accesspackages
 - *System registration:* /authentication/api/v1/systemregister/vendor
 - *System user:* /authentication/api/v1/systemuser/request/vendor
- 6) If needed, use the fields in tabs sender and receiver to support multiple instances of the integration flow. Please note that you will need to update the configuration of RFC connection in transaction SM59 to match the address in the Sender tab.

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

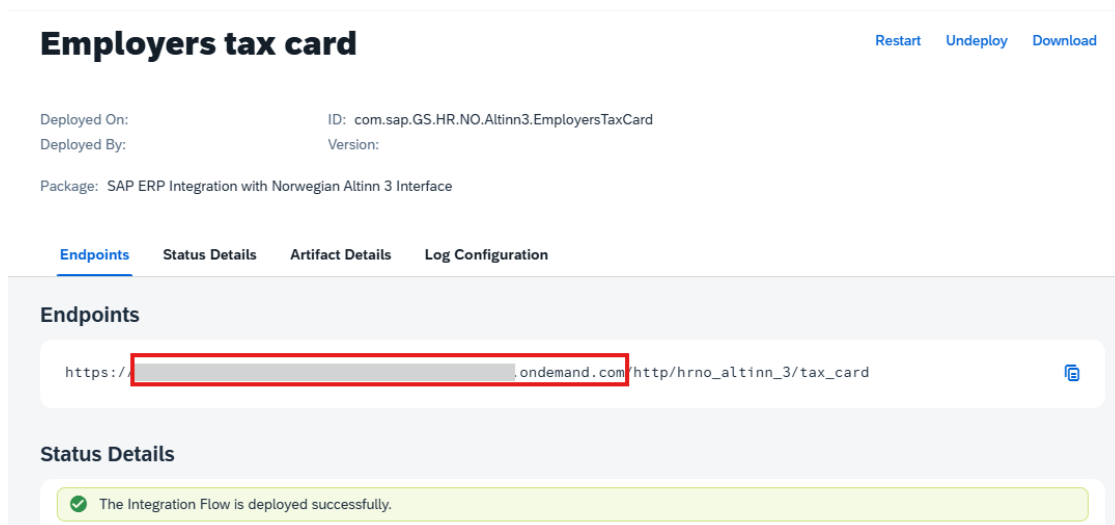
In the SAP back-end system, you need to configure the HTTPS connection to the CPI solution.

Note

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

4.1 Configuration of connection to Employers tax card

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 Employers tax card iFlow.



The screenshot displays the configuration page for the 'Employers tax card' iFlow. At the top, there are buttons for 'Restart', 'Undeploy', and 'Download'. Below this, the deployment details are shown: 'Deployed On:', 'Deployed By:', 'ID: com.sap.GS.HR.NO.Altinn3.EmployersTaxCard', and 'Version:'. The package is identified as 'SAP ERP Integration with Norwegian Altinn 3 Interface'. There are four tabs: 'Endpoints', 'Status Details', 'Artifact Details', and 'Log Configuration'. The 'Endpoints' tab is active, showing a URL: 'https://[redacted].ondemand.com/http/hrno_altinn_3/tax_card'. Below the 'Status Details' tab, a green message box indicates 'The Integration Flow is deployed successfully.'

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_ALTINN3_TAXC** for the connection name
- 4) Set connection type **G** (HTTP Connection to External Server)
- 5) Enter **CPI - Altinn 3 Tax Card** in the *Description* field

- 6) On the *Technical Settings* tab, enter the following values
- a) Target Host: < IFLMAP URL for the CPI 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/HRNO_ALTINN_3/TAX_CARD**
- d) HTTP Proxy Options <Enter own HTTP proxy values >

The screenshot shows the SAP configuration interface for an RFC Destination named 'HR_NO_CPI_ALTINN3_TAXC'. The 'Technical Settings' tab is active. The 'RFC Destination' field contains 'HR_NO_CPI_ALTINN3_TAXC'. The 'Connection Type' is set to 'G' (HTTP Connection to External Server). The 'Description' field contains 'Altinn 3 Tax Card'. Under 'Target System Settings', the 'Host' field is empty, 'Port' is '443', and 'Path Prefix' is '/http/HRNO_ALTINN_3/TAX_CARD'. Under 'HTTP Proxy Options', the 'Global Configuration' sub-tab is selected, and the 'Proxy PW Status' is '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>

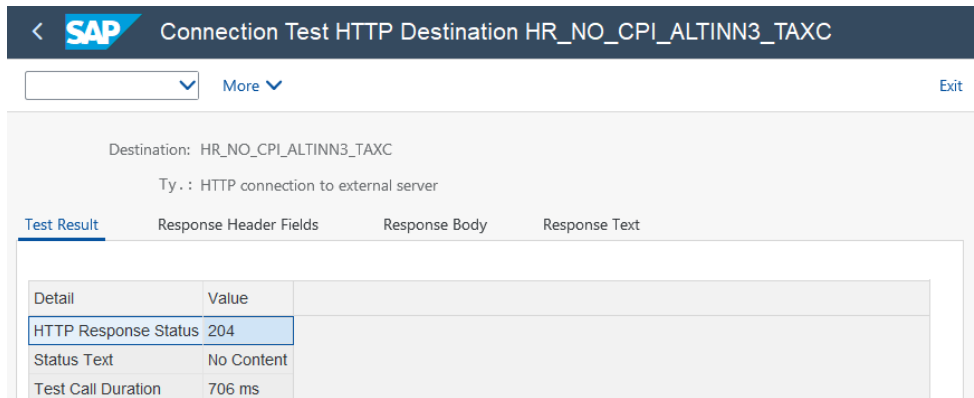
In the *Logon & Security* tab enter:

- i) *Logon with user*: Choose **Basic Authentication** and enter a valid **user** and **password** for logging on to CPI
- 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 displays the SAP configuration interface for an RFC Destination named 'HR_NO_CPI_ALTINN3_TAXC'. The interface is divided into several sections:

- Header:** Shows the destination name and navigation options like 'Connection Test', 'More', and 'Exit'.
- Basic Information:** Includes 'RFC Destination' (HR_NO_CPI_ALTINN3_TAXC), 'Connection Type' (G - HTTP Connection to External Server), and a 'Description' field.
- Description:** Three text input fields for 'Description 1', 'Description 2', and 'Description 3'. 'Description 1' contains 'Altinn 3 Tax Card'.
- Navigation:** Tabs for 'Administration', 'Technical Settings', 'Logon & Security' (selected), and 'Special Options'.
- Logon Procedure:**
 - Logon with User:** Radio buttons for 'Do Not Use a User' and 'Basic Authentication' (selected). Includes 'User' and 'PW Status' (saved) fields, and an 'OAuth Settings' button.
 - Logon with Ticket:** Radio buttons for 'Do Not Send Logon Ticket' (selected), 'Send Logon Ticket Without Ref. to a Target System', and 'Send Assertion Ticket for Dedicated Target System'. Includes 'System ID' and 'Client' fields.
 - Logon with MQTT/AMQP:** 'Users' and 'PW Status' (is initial) fields.
- Security Options:**
 - Status of Secure Protocol:** Radio buttons for 'SSL: Inactive' and 'Active' (selected).
 - SSL Client PSE ID:** A dropdown menu showing '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 **204**



4.2 Configuration of connection to Information on future deductions


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 Information on future deductions iFlow.

Information on future deductions [Restart](#) [Undeploy](#) [Download](#)


Deployed On: ID: com.sap.GS.HR.NO.Altinn3.FutureDeductions
Deployed By: Version:
Package: SAP ERP Integration with Norwegian Altinn 3 Interface

[Endpoints](#) [Status Details](#) [Artifact Details](#) [Log Configuration](#)

Endpoints

https://[redacted].ondemand.com/http/hrno_altinn_3/future_deductions 

Status Details

 The Integration Flow is deployed successfully.

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_ALTINN3_DED** for the connection name
- 4) Set connection type **G** (HTTP Connection to External Server)
- 5) Enter **CPI - Altinn 3 Information on future deductions** 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_altinn_3/future_deductions**

d) HTTP Proxy Options <Enter own HTTP proxy values>

The screenshot shows the SAP configuration interface for an RFC Destination named 'HR_NO_CPI_ALTINN3_DED'. The 'Technical Settings' tab is active, displaying the following fields:

- Target System Settings:**
 - Host: .ondemand.com
 - Port: 443
 - Path Prefix: /http/hrno_altinn_3/future_deductions
- HTTP Proxy Options:**
 - Global Configuration (selected)
 - Proxy Host: [Empty]
 - Proxy Service: [Empty]
 - Proxy User: [Empty]
 - 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 CPI
- ii) *Logon with ticket*: Select **Do Not Send Logon Ticket**
- iii) *Security options*: Select **SSL Active** and **SSL Certificate Default SSL Client (Standard)**

SAP RFC Destination HR_NO_CPI_ALTINN3_DED

Connection Test More Exit

RFC Destination: HR_NO_CPI_ALTINN3_DED

Connection Type: G HTTP Connection to External Server Description

Description

Description 1: Altinn 3 Information on future deductions

Description 2:

Description 3:

Administration Technical Settings **Logon & Security** Special Options

Logon Procedure

Logon with User

Do Not Use a User OAuth Settings

Basic Authentication

User: sb-f32b0c81-2baf-45cd-afb0-f449c03a24231b192_

PW Status: saved

Logon with Ticket

Do Not Send Logon Ticket

Send Logon Ticket Without Ref. to a Target System

Send Assertion Ticket for Dedicated Target System

System ID Client

Logon with MQTT/AMQP

Users:

PW Status: is initial

Security Options

Status of Secure Protocol

SSL: Inactive Active

SSL Client PSE ID: 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 **204**

SAP Connection Test HTTP Destination HR_NO_CPI_ALTINN3_DED

More Exit

Destination: HR_NO_CPI_ALTINN3_DED

Ty.: HTTP connection to external server

Test Result Response Header Fields Response Body Response Text

Detail	Value
HTTP Response Status	204
Status Text	No Content
Test Call Duration	958 ms

4.3 Configuration of connection to System and system user registration

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 System and system user registration iFlow.

The screenshot displays the configuration page for the 'System and system user registration' iFlow. At the top, there are buttons for 'Restart', 'Undeploy', and 'Download'. Below the title, the following details are shown: 'Deployed On:' (blank), 'ID: com.sap.GS.HR.NO.Altinn3.System', 'Deployed By:' (blank), and 'Version: :'. The package is identified as 'SAP ERP Integration with Norwegian Altinn 3 Interface'. A navigation bar includes 'Endpoints', 'Status Details', 'Artifact Details', and 'Log Configuration'. The 'Endpoints' section shows a URL: 'https://[redacted].ondemand.com/http/hrno_altinn_3/system'. The 'Status Details' section features a green message: 'The Integration Flow is deployed successfully.'

i 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_ALTINN3_SYS** for the connection name
- 4) Set connection type **G** (HTTP Connection to External Server)
- 5) Enter **CPI - Altinn 3 System register** in the *Description* field
- 6) On the *Technical Settings* tab, enter the following values
 - a) Target Host: < IFLMAP URL for the CPI 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/hrno_altinn_3/system**
- d) HTTP Proxy Options **<Enter own HTTP proxy values>**

The screenshot displays the SAP configuration page for an RFC Destination named 'HR_NO_CPI_ALTINN3_SYS'. The 'Technical Settings' tab is active, showing the following configuration details:

- RFC Destination:** HR_NO_CPI_ALTINN3_SYS
- Connection Type:** HTTP Connection to External Server
- Description:** Altinn 3 System register
- Target System Settings:**
 - Host:** [Empty field]
 - Port:** 443
 - Path Prefix:** /http/HRNO_ALTINN_3/SYSTEM
- HTTP Proxy Options:**
 - Global Configuration:** [Selected]
 - Proxy Host:** [Empty field]
 - Proxy Service:** [Empty field]
 - Proxy User:** [Empty field]
 - 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/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)**

SAP RFC Destination HR_NO_CPI_ALTINN3_SYS

Connection Test More Exit

RFC Destination: HR_NO_CPI_ALTINN3_SYS

Connection Type: HTTP Connection to External Server Description

Description

Description 1: Altinn 3 System register

Description 2:

Description 3:

Administration Technical Settings **Logon & Security** Special Options

Logon Procedure

Logon with User

Do Not Use a User OAuth Settings

Basic Authentication

User: sb-f32b0c81-2baf-45cd-afb0-f449c03a24231b192...

PW Status: saved

Logon with Ticket

Do Not Send Logon Ticket

Send Logon Ticket Without Ref. to a Target System

Send Assertion Ticket for Dedicated Target System

System ID Client

Logon with MQTT/AMQP

Users:

PW Status: is initial

Security Options

Status of Secure Protocol

SSL: Inactive Active

SSL Client PSE ID: 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 **204**

SAP Connection Test HTTP Destination HR_NO_CPI_ALTINN3_SYS

More Exit

Destination: HR_NO_CPI_ALTINN3_SYS

Ty.: HTTP connection to external server

Test Result	Response Header Fields	Response Body	Response Text
Detail	Value		
HTTP Response Status	204		
Status Text	No Content		
Test Call Duration	1081 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: