New Zealand Inland Revenue Reporting for Payroll

SAP Cloud Platform Integration Configuration Document

Public

Integration Package Version 1.0.2

Version	Date	Comment
1.0.0	12/07/2018	Initial release. Contains four artifacts for OAUTH Token and four artifacts each for create, update, terminate and pay date reporting.
1.0.1	06/09/2018	Included the steps for adding security certificate for inbound communication and added more information for implementing the solution.
1.0.2	12/02/2019	The data store operation in IFLOWs for ES and EI files have been removed. The token validation Backend IFLOW is enhanced to perform the validation online using IRD token service.

TABLE OF CONTENTS

1 OVERVIEW

In New Zealand information about employees and their payments must be sent to Inland Revenue each pay date. This information needs to be submitted directly from the SAP payroll system to Inland Revenue. The communication part of this process is taken care of by SAP Cloud Platform Integration.

There are multiple types of files that can be sent to Inland Revenue and each of these has their own 'iflows' created in SAP Cloud Platform Integration. However, before the files can be sent the appropriate authorization credentials must be established with Inland Revenue and an OAUTH token received. This token can be validated or revoked and each of these 'services' is also an 'inflow' in SAP Cloud Platform Integration.

In order to set up SAP Cloud Platform Integration for these processes, there are some required configuration steps in both the SAP payroll system and the SAP Cloud Platform Integration tenant. This document details that configuration. These steps are typically taken care of by an SAP Cloud Platform Integration consultant or SAP Basis person who is responsible for configuring the SAP ERP - SAP Cloud Platform Integration connection and maintaining the integration content and certificates/credentials on the SAP Cloud Platform Integration tenant.

Note that the Inland Revenue server currently has no ability to accept test files so the following assumes that all configuration is set for the production system.
For a full overview of the Pay Date Reporting process refer to SAP Note 2672190.

2 TECHNICAL SOLUTION IN MORE DETAIL

In order to facilitate the electronic submission of data Inland Revenue have established a protected service referred to as the Inland Revenue "Gateway" and have defined specifications for how software providers can communicate with that Gateway in a secure manner. (Note that this Gateway is also used for non-payroll related functions as well, e.g. GST reporting.)

Each software provider that uses this Gateway has to follow the guidelines issued by Inland Revenue and have to have performed a number of predefined tests to ensure that the information can be sent correctly. Only once that is successfully completed can that software provider's customers use the Gateway for filing.

The process as defined by Inland Revenue is as follows:

- The user interacts with their software system and it accesses the protected service provided by IR (the Gateway)
- The software system invokes an authorization API to get an authorization code and the user is directed to an IR log on page.
- The user logs on and is authenticated.
- IR issues an authorization code that is sent back to the software system.
- The software invokes IR's token service to redeem the authorization code for an OAUTH Access Token. (The token has a finite life.)
- The software then invokes the Gateway to file information with the OAUTH Access token in the header.

This process ensures that it is secure and that only MyIR users who are authorized to submit data for an organisation can send information. Data is submitted in XML format.

2.1 SAP Cloud Platform Integration (CPI)

In SAP's case the communication between the payroll and Inland Revenue's Gateway is managed by SAP Cloud Platform Integration (CPI).
Communication between the payroll system and CPI is performed using logical ports in the payroll system that connect to CPI via a combination of HTTPS and SOAP connections. The connection is authenticated using public certificates.

2.2 Process Overview

In order to perform the process mentioned above Inland Revenue's Gateway needs to know where to send response codes to and to be able to 'trust' that system. A registration process must therefore be completed before you can commence filing with Inland Revenue. That process involves supplying a return_URL (an address where responses are sent to) and a security certificate to Inland Revenue for your employer IRD number(s). This can only be done once CPI has been set up for NZ Pay Day Reporting and you will find details about the registration process in the CPI Configuration Guide for registration (refer to the details later in this document).

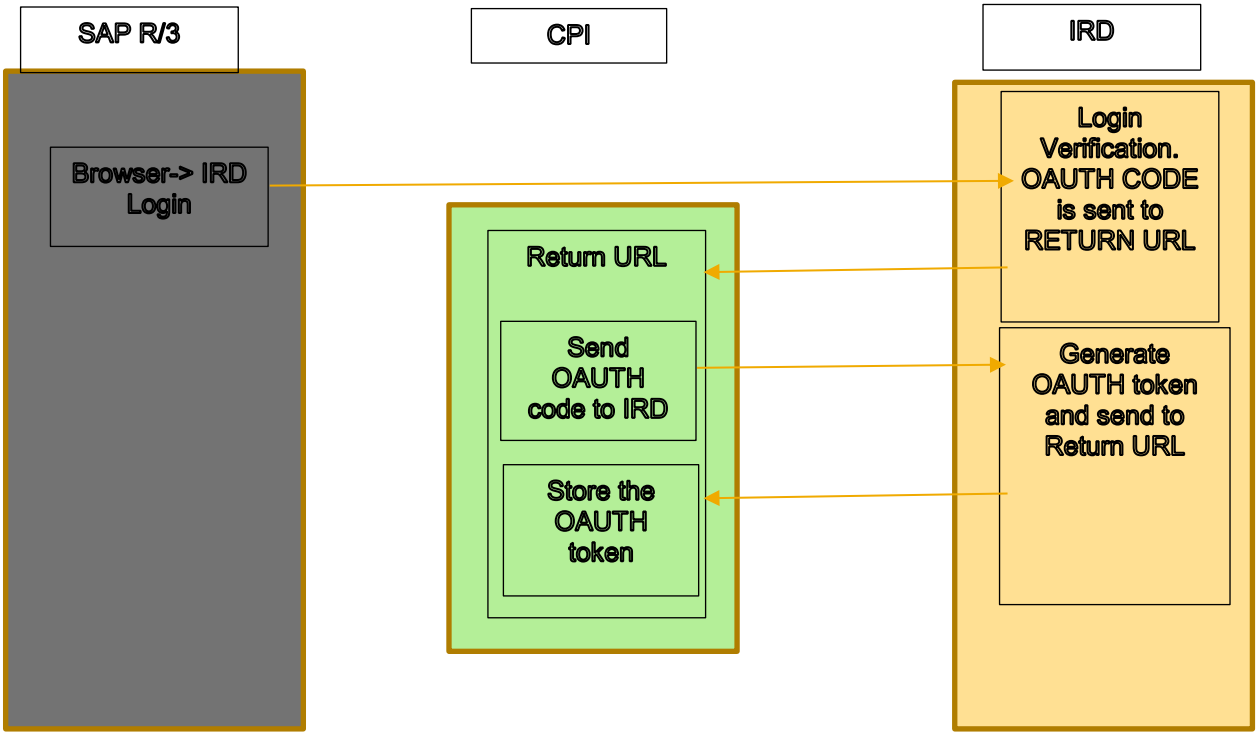
Once Inland Revenue has this information loaded in their system you can commencer Pay Day filing through the Gateway. The filing processing is essentially split into two steps:

- Obtaining the OAUTH token
- Submitting Data

2.2.1 Obtaining the OAUTH Token

The process to obtain a token is as follows:

- The user clicks a button in the B2A Manager transaction within the payroll system. This will route the user to a MyIR log on screen at Inland Revenue.
- The user is authenticated by Inland Revenue.
- The Gateway then returns a OAUTH code to the return_url held in their system, (i.e. your CPI system).
- CPI then uses this OAUTH code to send a request to the Gateway for an OAUTH Token.
- The token is sent back to CPI and held there.



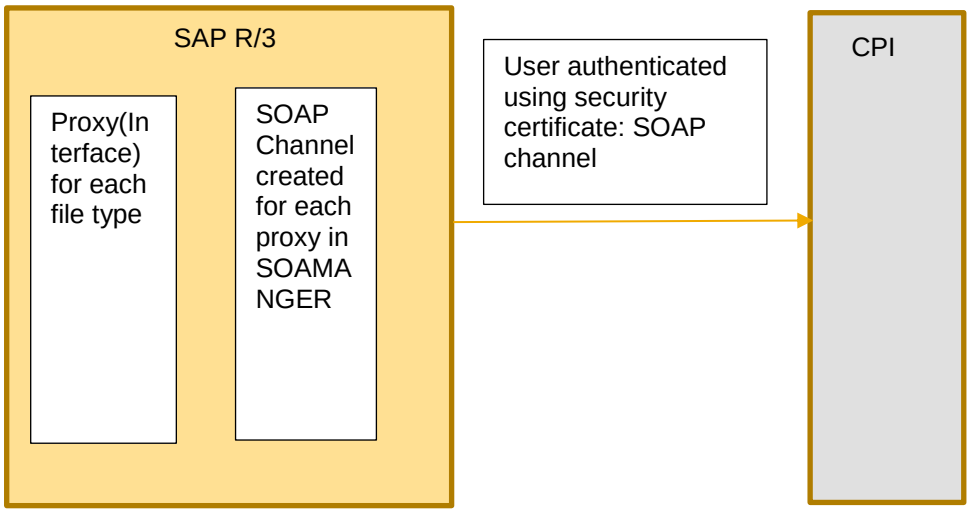
2.2.2 Submitting Data

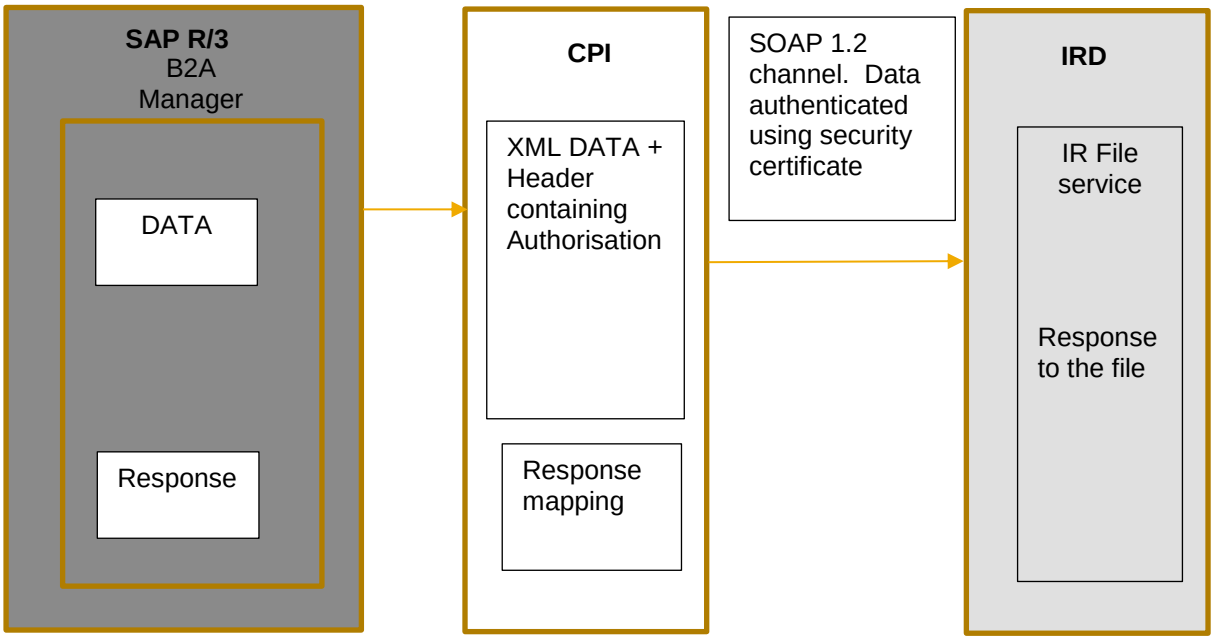
A valid OAUTH token must be obtained before files can be sent to Inland Revenue as that token is contained in the header information. The above process, therefore, acts as a prerequisite to this process. To submit data:

- A user runs HCM reports to extract relevant data and create the necessary files. These files are per legal entity and are managed in the payroll system in the B2A Manager. (Within B2A Manager the user is able to view the data contained in the files in XML format.)
- Within B2A Manager the user selects the file(s) to be sent and selects execute.
- B2A Manager sends the files to CPI where the XML pay load is formed according to the Inland Revenue requirements (including inserting the token into the header).
- CPI sends the data to Inland Revenue.
- Inland Revenue sends a response code to CPI. This shows whether the file was successfully or what type of error has occurred.
- CPI modifies that response into an understandable format for the payroll system and the user is able to view the result in B2A Manager.

When the data is sent from the payroll system to CPI it is done through the SOAP channel created in SOAMANAGER. Each SOAP channel refers to the corresponding proxy (interfaces) created in SPROXY. The proxies also have the response structures included and wait for the response to come from CPI after the data is sent. The SOAP channel created has the option to set the user level authentication (SAP recommends using security certificate for user authentication, but User Id and Password can also be used). The communication channel from CPI to Inland Revenue's Gateway (and the return response) is SOAP 1.2 which is configured as the receiver channel in the IFLOWS contained within CPI. The authentication at Inland Revenue is done using the security certificate (MUTUAL TLS method). The private key for this is stored in the key store within CPI and the public key is given to Inland Revenue as part of the registration process. This public key is then used in the SOAP channel.

Diagrammatically this process is as follows:





3 PREREQUISITES

Before you start with the activities described in this document, ensure that the following prerequisites are met in SAP Payroll system and SCPI.

3.1 Check SAP Note 2672190 is Applied in the SAP Payroll System

SAP Note 2672190 delivers new proxies for pay date reporting. The proxies are used to send the data from SAP payroll system to SCPI. Section 4 document discusses the steps for configuring the logical ports in the SOA manager for which this note has to be installed in the system.

3.2 Set up Tenant

If this is your first use of SAP Cloud Platform Integration (SCPI) refer to the Welcome Kit that you should receive when your tenant is first provisioned. This Kit contains a link to the SCPI Customer Success Portal (https://help.sap.com/viewer/p/SCP_CUSTOMER_SUCCESS_PORTAL/) where you can access a wide range of SCPI related resources.

You will also receive a “SAP Cloud Platform Integration Onboarding Guide’ to guide you through the initial setup to get your tenant up and running.

3.3 User Authorisations

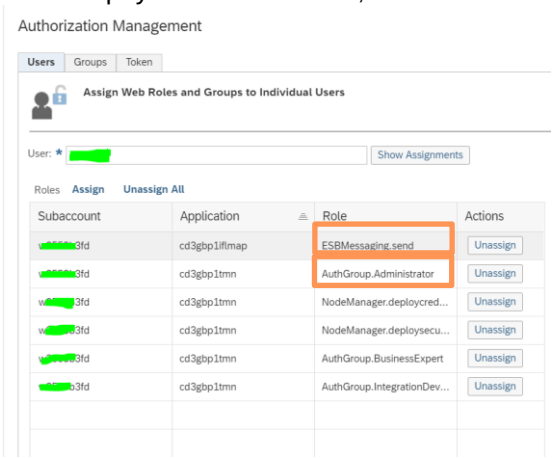
Ensure that users in the tenant have sufficient rights and privileges to copy the NZ integration package and to configure and deploy the integration flow.

SAP CLOUD PLATFORM INTEGRATION test and productive tenants are live and users in the tenants have sufficient rights and privileges to copy the integration package and to configure and deploy the integration flow.

To deploy the security content, the required role is ‘**AuthGroup.Administrator’**.

For the subsequent configuration of ERP, note down the URL of the tenant (it is the TMN URL which you received when the tenant was provisioned).

To send payload/data to SCPI, the user must have the role “ESBMessaging.send”.

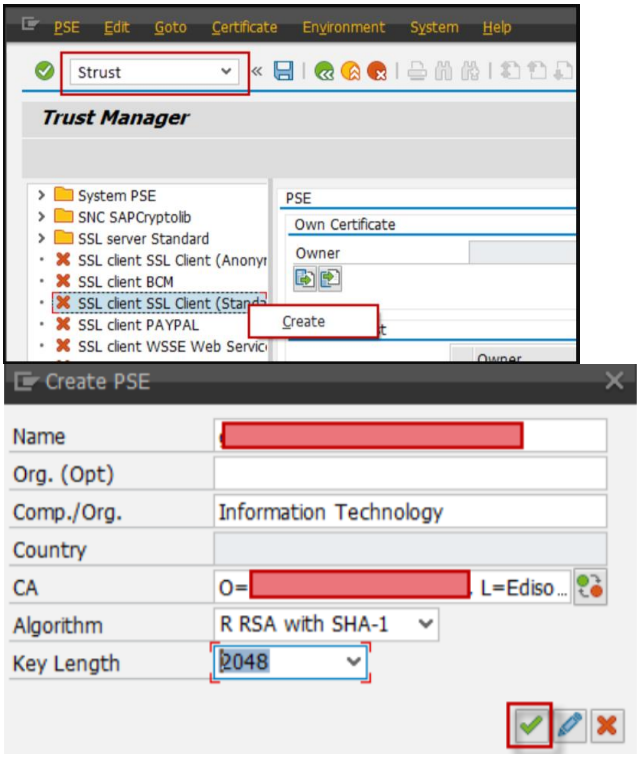


3.4 ECP/ SAP ERP Installing client certificate

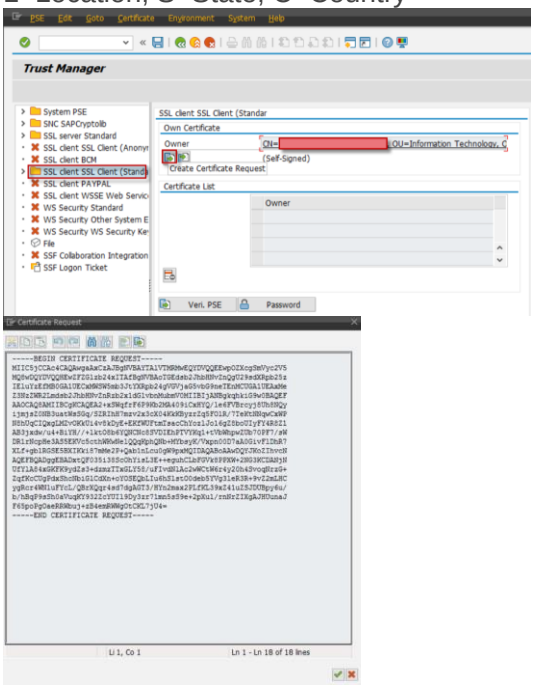
The certificate based authentication is a secure way of connecting two systems and SAP recommends customers to use the certificate based communication. The iflows which are in SCP shall be invoked/called using certificates and for this purpose a key pair needs to be installed in SAP ERP/ ECP system and its public certificate needs to be inxstalled in the iflows. The key pair should have been signed by a CA who is listed by SAP to be accepted by the SAP load balancer.

Once you get the certificate signed by the supported CA, the key pair needs to be installed in STRUST of SAP ERP/ECP system.

a. Go to STRUST transaction



b. Below is the example show DN of the certificate:
DN = CN=erpc.externaldomain.com, OU=Information Technology, O=mycompany Inc, L=Location, S=State, C=Country



c. This is the CSR. Copy the CSR and get it signed by a Certificate Authority.

Note: CA should be in the Trust list of SCPI. Please check for the latest SCPI trust list here.

d. Import the certificate response in STRUST.

4 SETUP STEPS IN SAP CLOUD PLATFORM INTEGRATION

As part of the initial release, there are eight SCPI artifacts delivered.

Four artifacts are related to authentication token.

- OAUTH Token: Iflow used for obtaining OAUTH token.
- OAUTH Token Validation: Iflow used to validate the OAUTH token.
- OAUTH Token Validation Backend: Iflow is called from the backend system while sending the payload to Inland Revenue.
- OAUTH Token Revoke: Iflow used to revoke the OAUTH token at Inland Revenue server

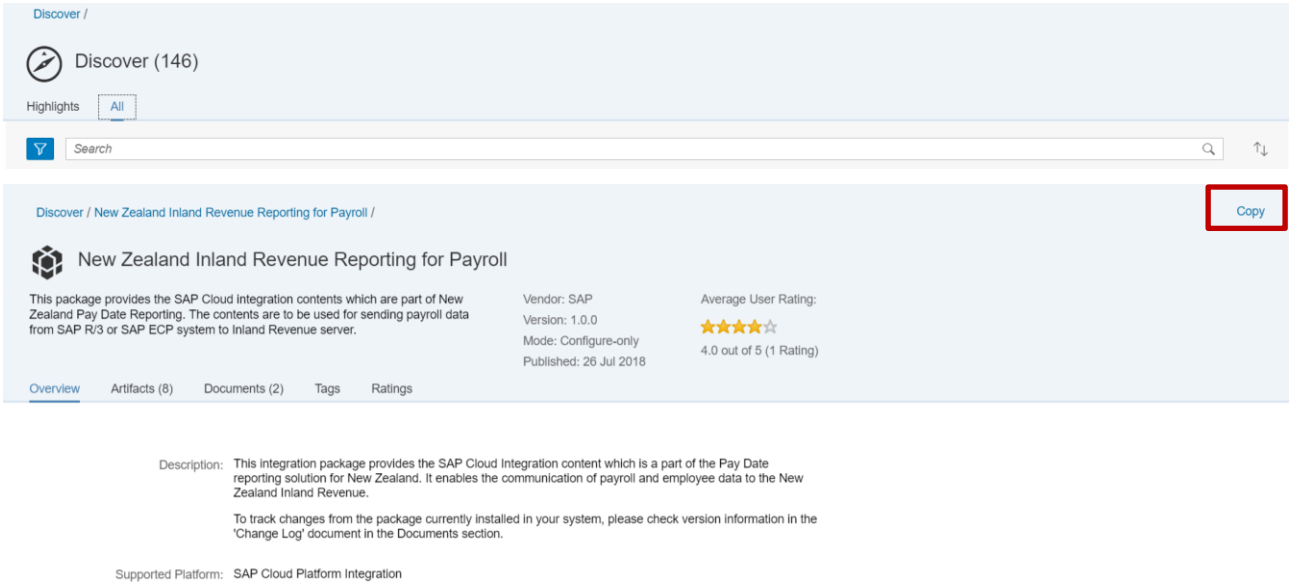
Four artifacts relate to the four types of XML files which are sent to Inland Revenue.

- Employee Services - Create: Iflow sends the details of employees who are hired in a pay period.
- Employee Services - Update: Iflow sends the details of employees who have had an update to master data in a pay period that should be reported.
- Employee Services - Terminate: Iflow sends the details employees who were terminated in a pay period.
- Employment Information - Pay Date File: Iflow sends the payment information of employees for a pay date.

To set up these iflows follow the details in the following steps:

4.1 Copy Published Package into Your Package

Go to the ‘Discover’ chapter of your tenant and find the package **‘New Zealand Inland Revenue Reporting for Payroll’**



Click on package name, then click ‘Copy’ in the upper right corner:

Note: the package version on the screenshot may differ from the one shown above.

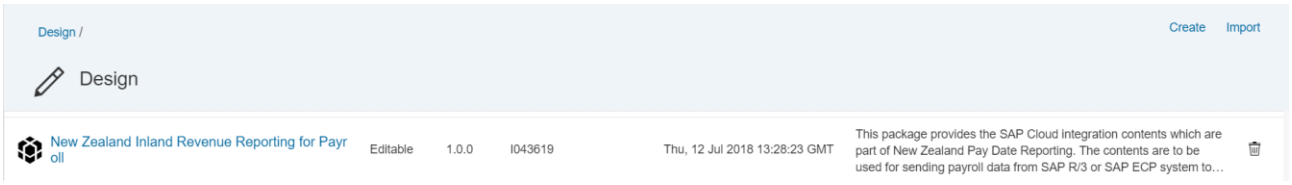
4.2 Configure Integration Flow for OAUTH token services

There are four artifacts which are delivered to process the OAUTH token and three out of them have HTTP as sender channel and one have SOAP as sender channel. The certificate based authorization for sender channel will differ for HTTP and SOAP.

4.2.1 OAUTH Token

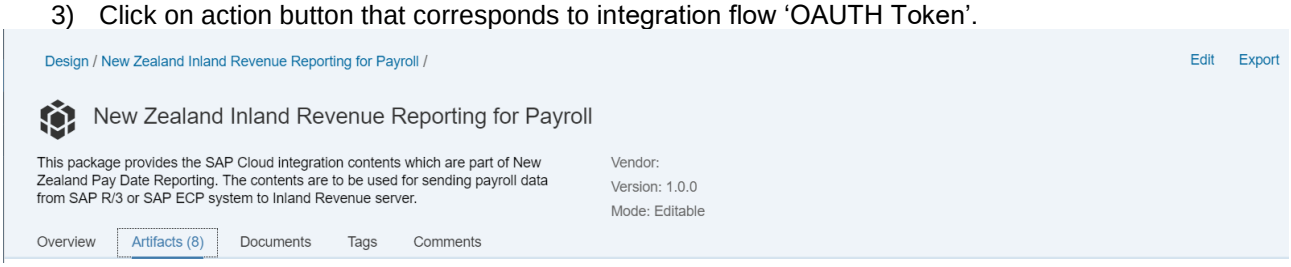
This integration flow is used to get the OAUTH token.
Steps:

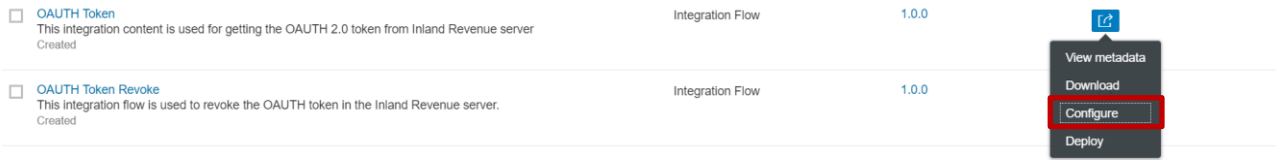
1) Go to the integration package that was copied from the original ‘New Zealand Inland Revenue Reporting for Payroll’



2) Click on the Artifacts tab

3) Click on action button that corresponds to integration flow ‘OAUTH Token’.





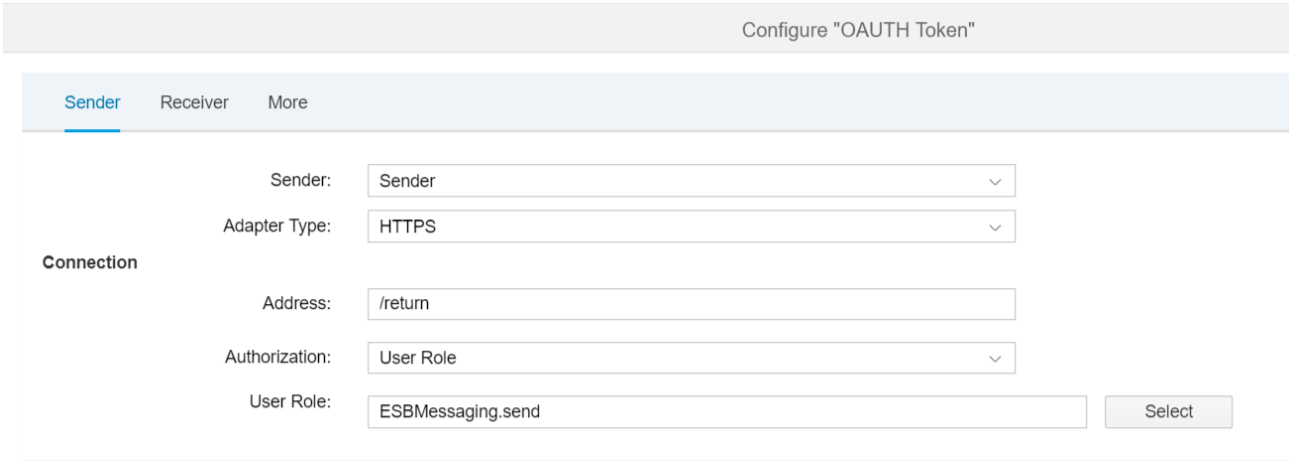
Note: the version of the integration on the screenshot may differ from the current one.

4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the Inland Revenue server. The Inland Revenue server will be routing the OAUTH Authorisation code which will be processed in this IFLOW and then sent to OAUTH server to get the OAUTH token.

- Update the connection address in the format "/XXXXX", where XXXX can be any meaningful word for return URL.

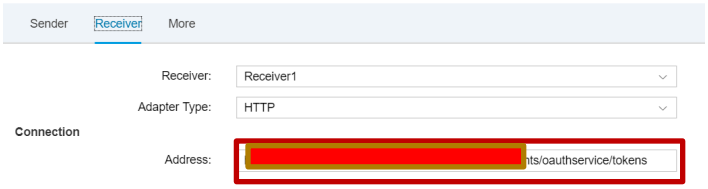


Note that the address configured here will be the suffix used to form the RETURN_URL for OAUTH 2.0 token which is referred to later in this document.

Note: The connection address has to be unique within a tenant.

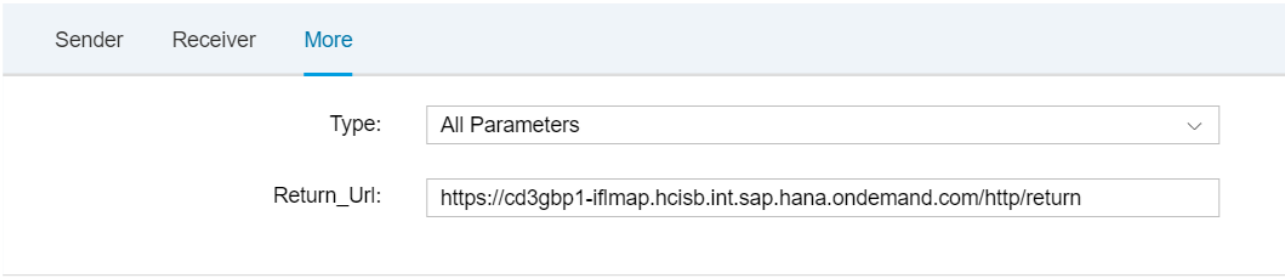
- In the Authorization field, define whether 'user role' or 'client certificate' will be used – refer to section 6 for configuring authorisations.

Receiver Tab



Address: Enter the following OAUTH production server URL.
https://services.ird.govt.nz/ms_oauth/oauth2/endpoints/oauthservice/tokens

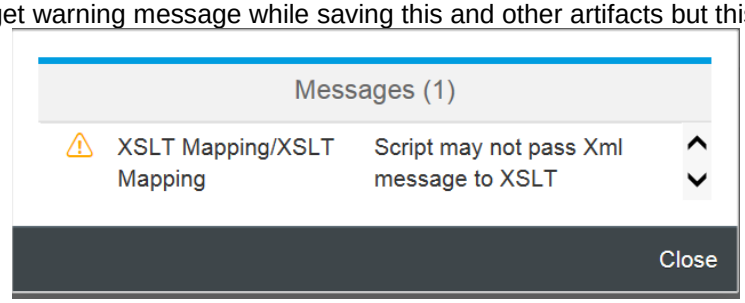
More Tab



Return_URI: Enter the return URI which will be registered with Inland Revenue (refer to the registration section at the end of this document to link to the documentation detailing how this is formed, in short it is a combination of the tenant http URL and the address parameter specified on the Sender tab).

5) Select *Save* and *Deploy* to save your configuration and to deploy it actively to server, respectively

Note: you may get warning message while saving this and other artifacts but this ok.

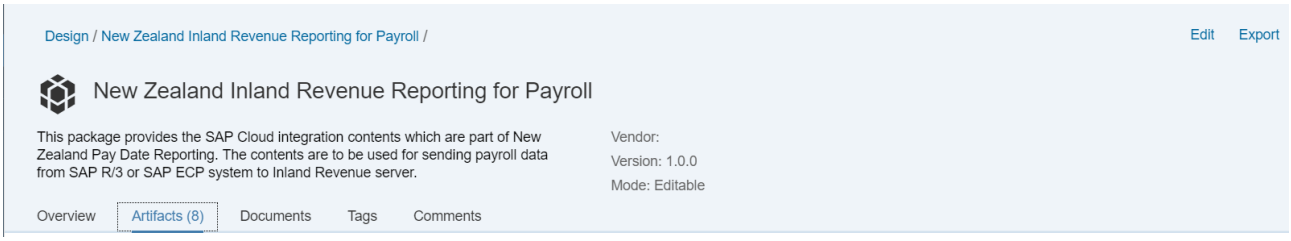


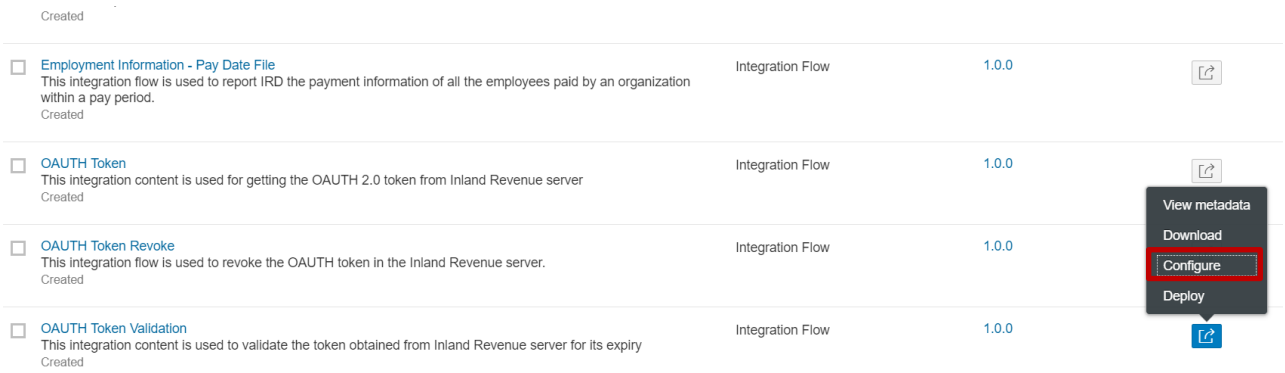
4.2.2 OAUTH Token Validation

This integration flow is used to validate the OAUTH token issued by the Inland Revenue server. A user can use this service to determine if the token is still active or whether they need to obtain a new one.

Steps:

1) Go to the integration package that was copied from the original 'New Zealand Inland Revenue Reporting for Payroll'
2) Click on the Artifacts tab
3) Click on action button that corresponds to integration flow 'OAUTH Token Validation'.



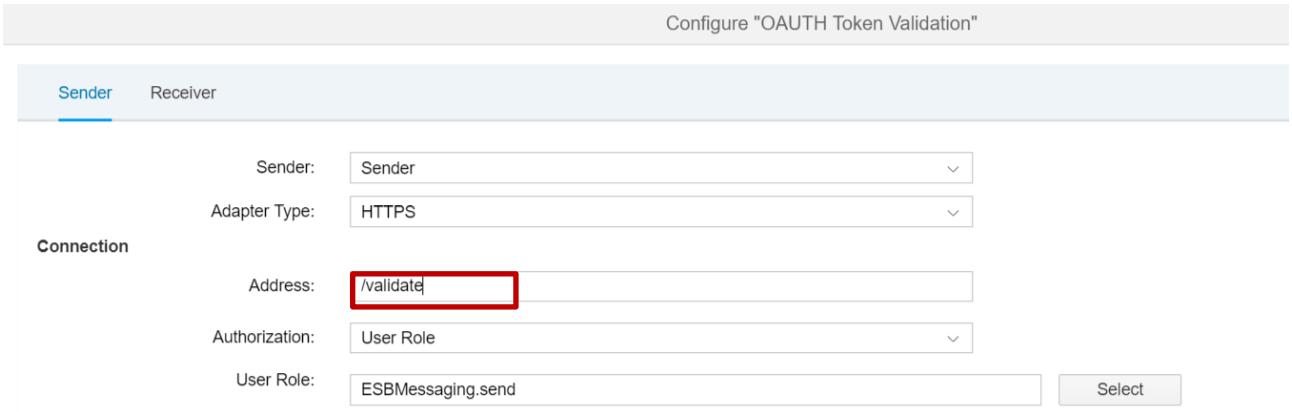


4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the HTTP request invoked by the end user from the B2A Manager transaction in SAP R/3 or ECP(PB2A) using “Validate Token” button. The request is then sent to the Inland Revenue server and a response is shown to the end user in HTML format.

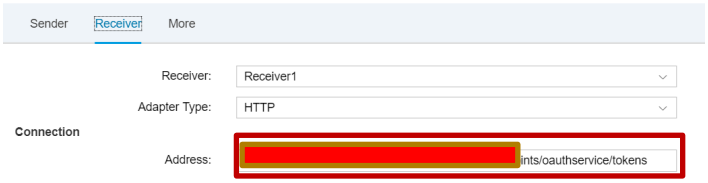
- Update the connection address in the format “/XXXXX”, where XXXXX can be any meaningful word for validating the token.



Note: The connection address must be unique within a tenant.

- In the Authorization field define whether ‘user role’ or ‘client certificate’ will be used – refer to section 6 for configuring authorisations.

Receiver Tab



Address: Enter the following OAUTH production server URL.
https://services.ird.govt.nz/ms_oauth/oauth2/endpoints/oauthservice/tokens

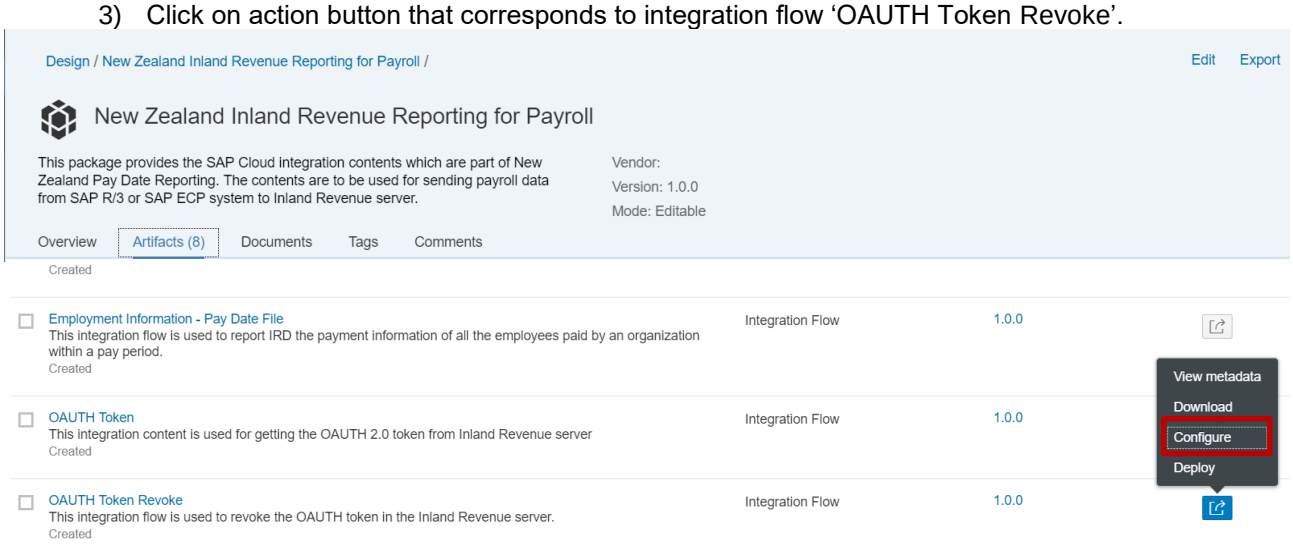
5) Select *Save* and *Deploy* to save your configuration and to deploy it actively to server, respectively.

4.2.3 OAUTH Token Revoke

This integration flow is used to revoke the OAUTH token issued by the Inland Revenue server. Once the token has been revoked communication with the Inland Revenue server ceases and a user must retrieve a new token for further communication.

Steps:

1) Go to the integration package that was copied from the original 'New Zealand Inland Revenue Reporting for Payroll'
2) Click on the Artifacts tab
3) Click on action button that corresponds to integration flow 'OAUTH Token Revoke'.

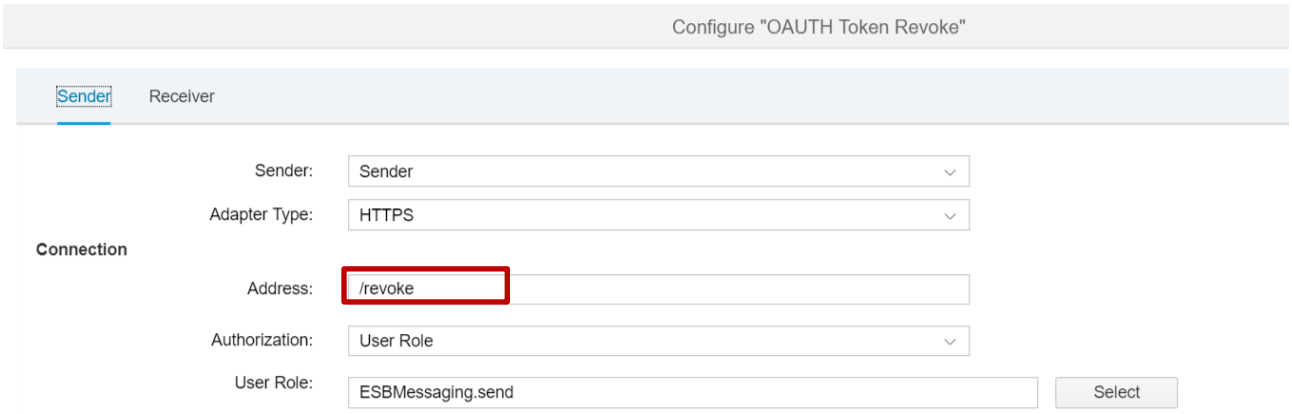


4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the HTTP request invoked by the end user from the B2A Manager transaction in SAP R/3 or ECP(PB2A) using "Revoke Token" button. The request is then sent to the Inland Revenue server and a response is shown to the end user in HTML format.

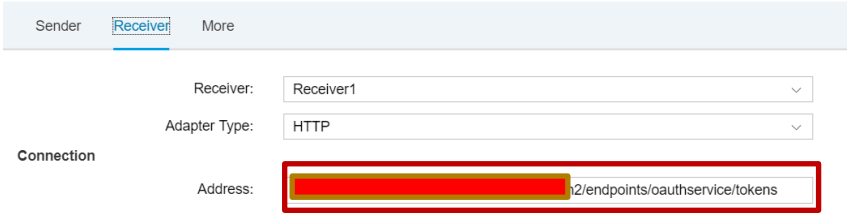
- Update the connection address in the format "/XXXXX", where XXXXX can be any meaningful word for revoking the token in Inland Revenue server.



Note: The connection address must be unique within a tenant.

- In the Authorization field define whether ‘user role’ or ‘client certificate’ will be used – refer to section 6 for configuring authorisations.

Receiver Tab



Address: Enter the following OAUTH production server URL.
https://services.ird.govt.nz/ms_oauth/oauth2/endpoints/oauthservice/tokens

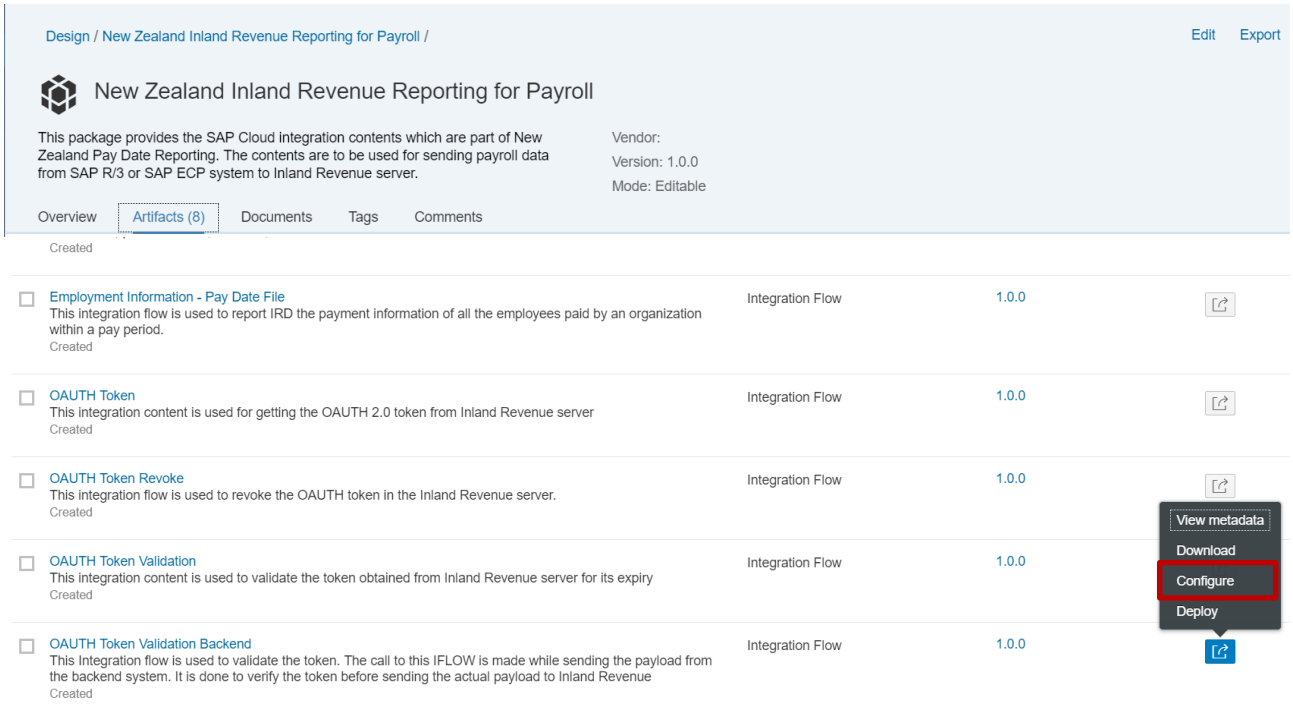
5) Select *Save* and *Deploy* to save your configuration and to deploy it actively to server, respectively

4.2.4 OAUTH Token Validation Backend

This Integration flow is used to validate the token. The call to this IFLOW is made while sending the payload from the backend system so that the token is verified before sending the actual payload to Inland Revenue.

Steps:

1) Go to the integration package that was copied from the original ‘New Zealand Inland Revenue Reporting for Payroll’
2) Click on the Artifacts tab
3) Click on action button that corresponds to integration flow ‘OAUTH Token Validation Backend’.

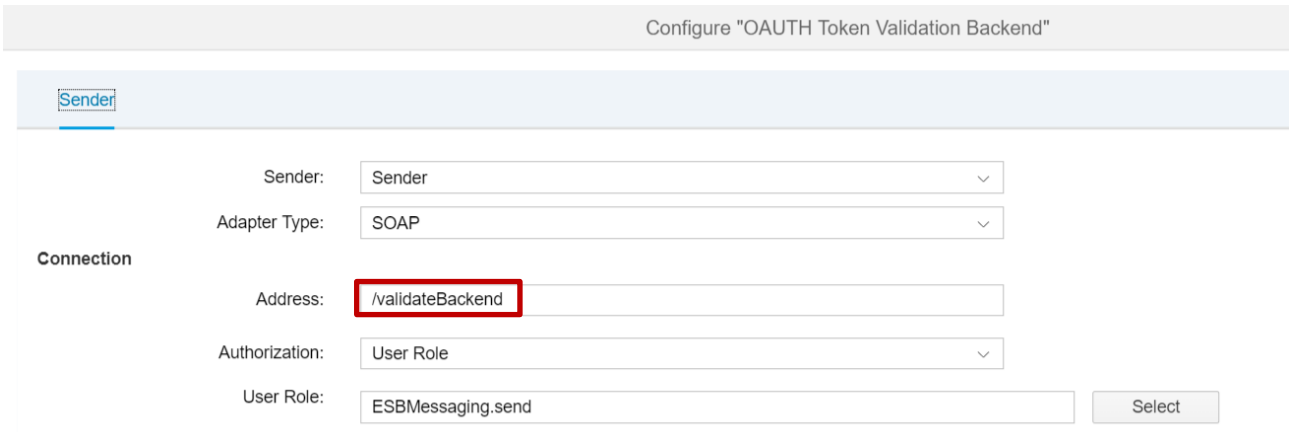


4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the SAP R/3 or SAP ECP system. The communication protocol for this connection used is SOAP. The connection is established in SAP R/3 or SAP ECP using SOA manager.

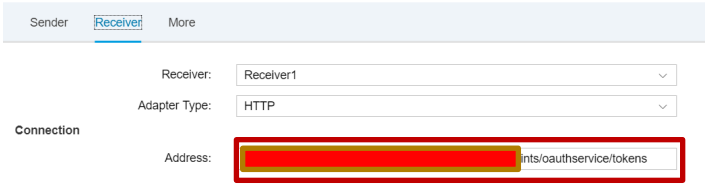
- Update the connection address in the format “/XXXXX”, where XXXXX can be any meaningful word for validating the token from backend system.



Note: The connection address must be unique within a tenant.

- In the Authorization field define whether ‘user role’ or ‘client certificate’ will be used – refer to section 6 for configuring authorisations.

Receiver Tab



Address: The OAUTH production server URL.
https://services.ird.govt.nz/ms_oauth/oauth2/endpoints/oauthservice/tokens

5) Select *Save* and *Deploy* to save your configuration and to deploy it actively to server, respectively

4.3 Configure Integration Flow for XML file communication

You will be configuring the Iflows which are specific to employee and payment files.

- **Employee Services:** Create, Update, Terminate
- **Employment Information:** Pay Date reporting

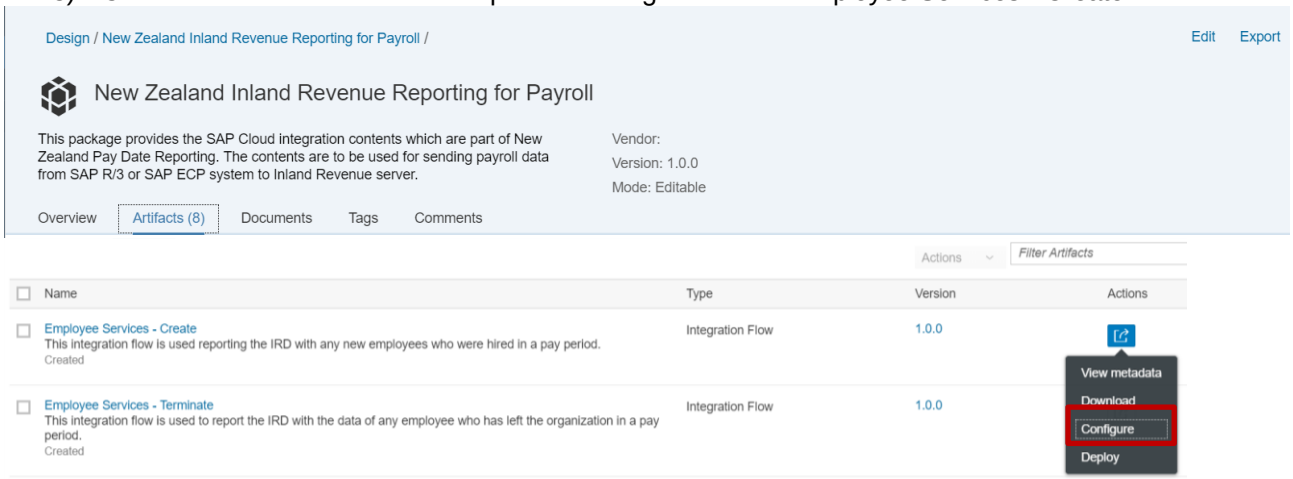
The Iflows used for the scenarios uses certificate Alias which is the security certificate going to be registered with Inland Revenue.

4.3.1 Employee Services: Create

This integration flow is used to update Inland Revenue with details of each new employee who was hired in a pay period.

Steps:

1) Go to the integration package that was copied from the original ‘New Zealand Inland Revenue Reporting for Payroll’
2) Click on the Artifacts tab
3) Click on action button that corresponds to integration flow ‘Employee Services - Create’.

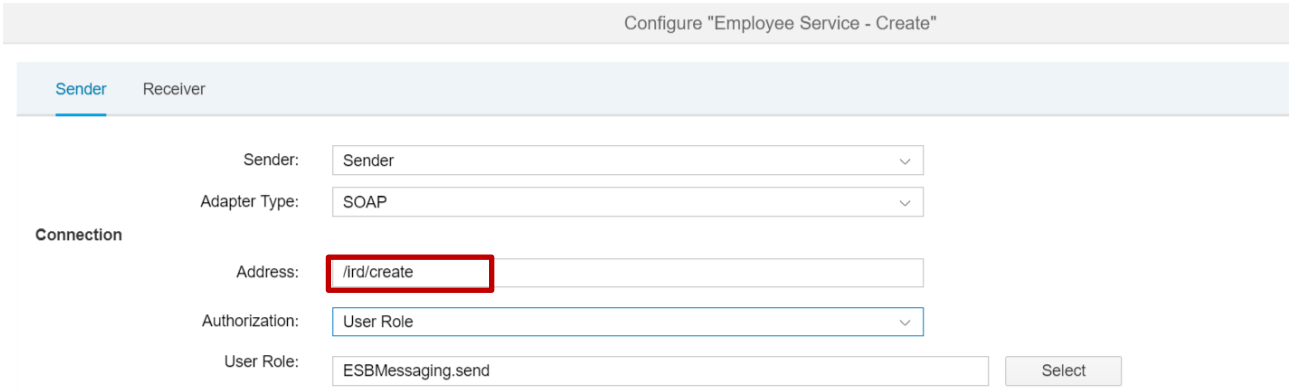


4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the SAP payroll system. The communication protocol for this connection used is SOAP. The connection is established in SAP payroll system using SOA manager.

- Update the connection address in the format "/XXXXX", where XXXXX can be any meaningful word for Inland Revenue ES create service.



Note: The connection address must be unique within a tenant.

- In the Authorization field define whether 'user role' or 'client certificate' will be used – refer to section 6 for configuring authorisations.

Receiver Tab

Address: Enter the following production Inland Revenue Employee Service URL address https://services.ird.govt.nz:4046/gateway/gws/employment/

Private Key Alias: Enter the Alias of the certificate which will be registered with Inland Revenue. (The Certificate Alias can be found in the Keystore – refer to the "New Zealand Inland Revenue – Registering for Payroll Services" document for more detail.

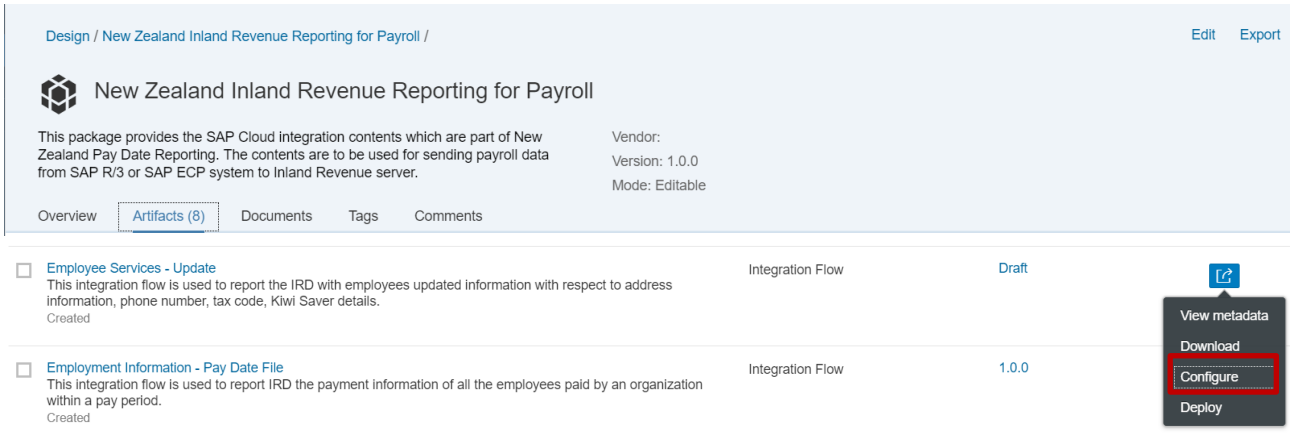
5) Select *Save* and *Deploy* to save your configuration and to deploy it actively to server, respectively

4.3.2 Employee Services: Update

This integration flow is used to update Inland Revenue when an existing employee has changes to KiwiSaver (e.g. opts out or joins), or has a change in personal details such as a tax code change or a name change.

Steps:

1) Go to the integration package that was copied from the original ‘New Zealand Inland Revenue Reporting for Payroll’
2) Click on the Artifacts tab
3) Click on action button that corresponds to integration flow ‘Employee Services - Update’.

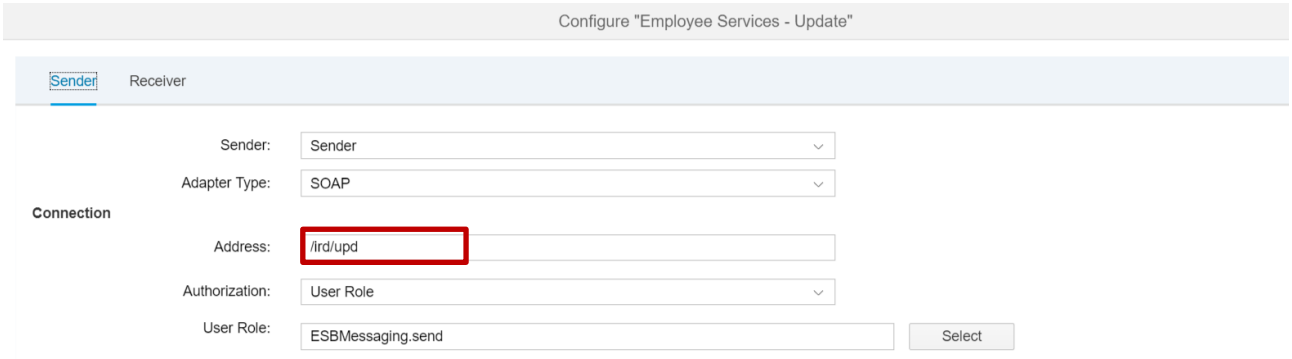


4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the SAP payroll system. The communication protocol for this connection used is SOAP. The connection is established in SAP payroll system using SOA manager.

- Update the connection address in the format “/XXXXX”, where XXXXX can be any meaningful word for Inland Revenue ES Update service.



Note: The connection address must be unique within a tenant.

- In the Authorization field define whether ‘user role’ or ‘client certificate’ will be used – refer to section 6 for configuring authorisations.

Receiver Tab

Address: Enter the following production Inland Revenue Employee Service URL address https://services.ird.govt.nz:4046/gateway/gws/employment/

Private Key Alias: Enter the Alias of the certificate which will be registered with Inland Revenue. (The Certificate Alias can be found in the Keystore – refer to the "New Zealand Inland Revenue – Registering for Payroll Services" document for more detail. This document is attached to SAP Note 2672190).

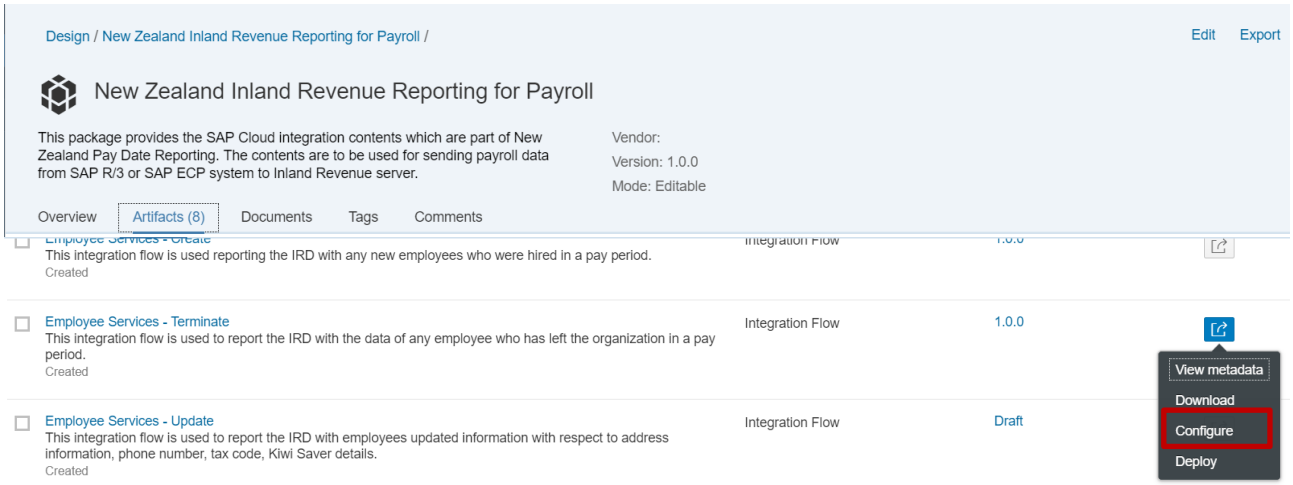
5) Select Save and Deploy to save your configuration and to deploy it actively to server, respectively.

4.3.3 Employee Services: Terminate

This integration flow is used to report any employees that are terminating employment.

Steps:

1) Go to the integration package that was copied from the original 'New Zealand Inland Revenue Reporting for Payroll'
2) Click on the Artifacts tab
3) Click on action button that corresponds to integration flow 'Employee Services – Terminate'

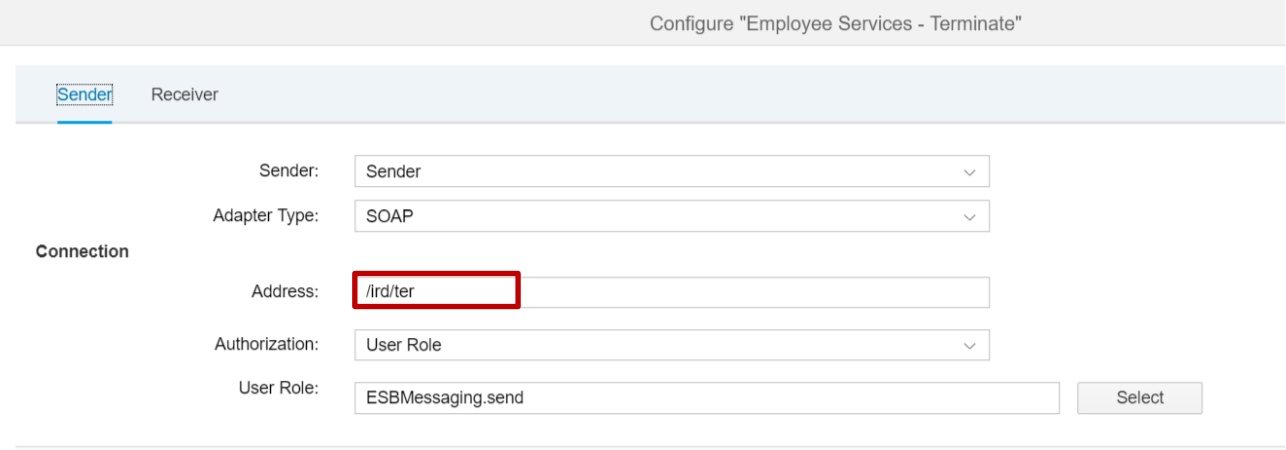


4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the SAP R/3 or SAP ECP system. The communication protocol for this connection used is SOAP. The connection is established in SAP R/3 or SAP ECP using SOA manager.

- Update the connection address in the format "/XXXXX", where XXXXX can be any meaningful word for Inland Revenue ES terminate service.



Note: The connection address must be unique within a tenant.

- In the Authorization field define whether 'user role' or 'client certificate' will be used – refer to section 6 for configuring authorisations.

Receiver Tab

Address: Enter the following production Inland Revenue Employee Service URL address https://services.ird.govt.nz:4046/gateway/gws/employment/

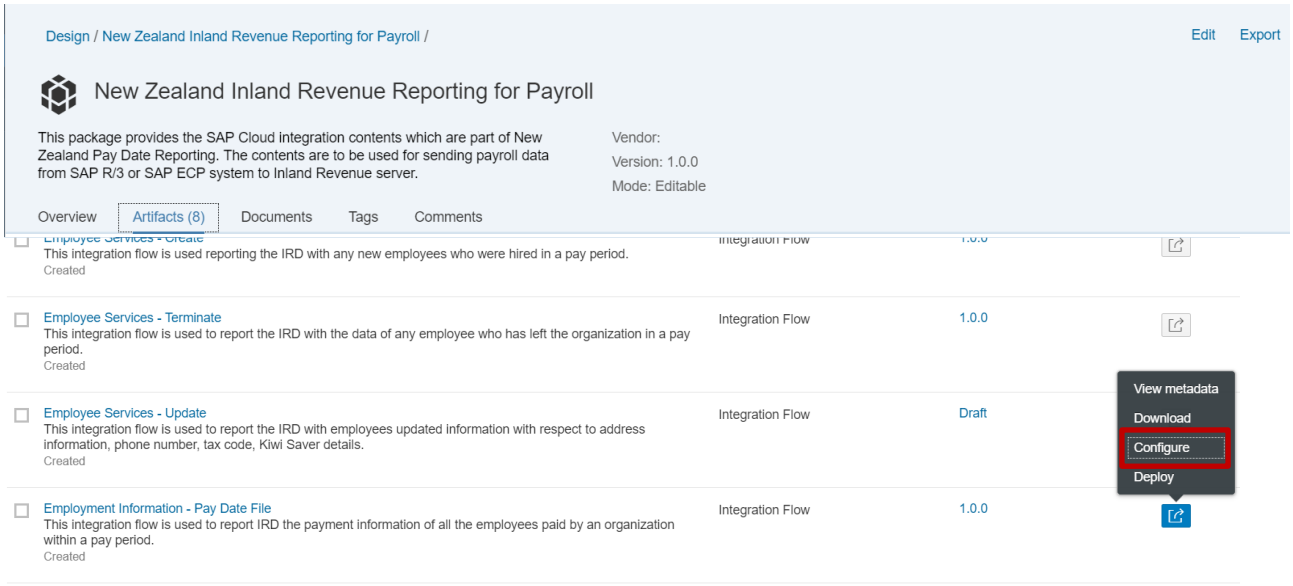
Private Key Alias: Enter the Alias of the certificate which will be registered with Inland Revenue. (The Certificate Alias can be found in the Keystore – refer to the "New Zealand Inland Revenue – Registering for Payroll Services" document for more detail. This document is attached to SAP Note 2672190).

5) Select Save and Deploy to save your configuration and to deploy it actively to server, respectively.

4.3.4 Employment Information: Pay Date File

This integration flow is used to update the Inland Revenue with any new employee who was hired in a pay period.
Steps:

1) Go to the integration package that was copied from the original ‘New Zealand Inland Revenue Reporting for Payroll’
2) Click on the Artifacts tab
3) Click on action button that corresponds to integration flow ‘Employment Information - Pay Date File.

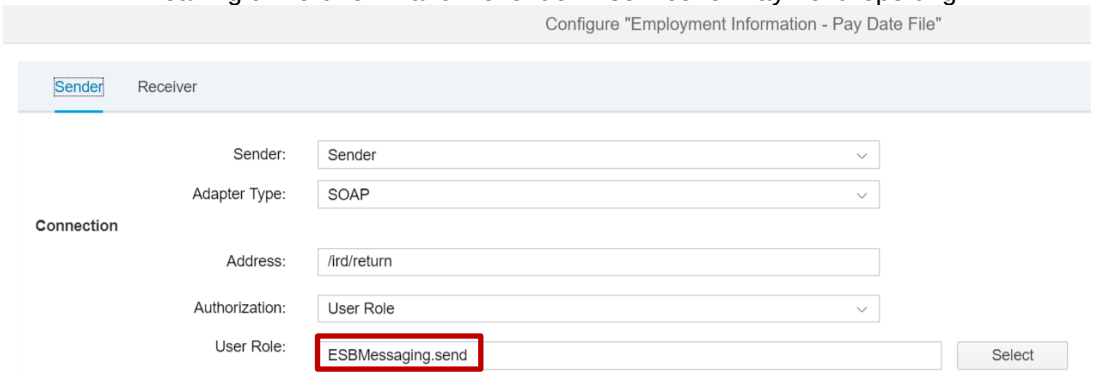


4) Choose *Configure* and maintain the following configuration parameters:

Sender Tab

The sender for this scenario is the SAP R/3 or SAP ECP system. The communication protocol for this connection used is SOAP. The connection is established in SAP R/3 or SAP ECP using SOA manager.

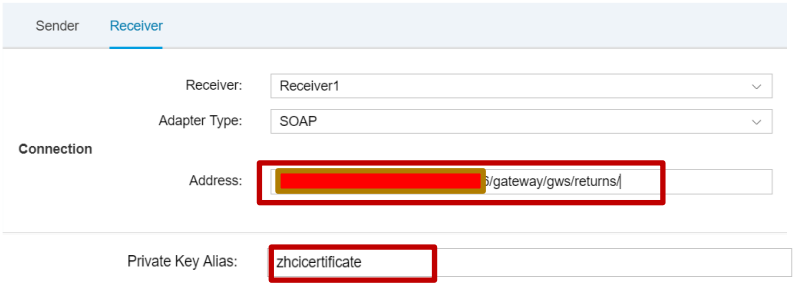
- Update the connection address in the format “/XXXXX”, where XXXXX can be any meaningful word for Inland Revenue EI service for Payment reporting.



Note: The connection address must be unique within a tenant.

- In the Authorization field define whether ‘user role’ or ‘client certificate’ will be used – refer to section 6 for configuring authorisations.

Receiver Tab



Address: Enter the following the production Inland Revenue Employment Information service URL https://services.ird.govt.nz:4046/gateway/gws/returns/

Private Key Alias: Enter the Alias of the certificate which will be registered with Inland Revenue. (The Certificate Alias can be found in the Keystore – refer to the "New Zealand Inland Revenue – Registering for Payroll Services" document for more detail. This document is attached to SAP Note 2672190).

5) Select Save and Deploy to save your configuration and to deploy it actively to server, respectively

5 SETUP STEPS IN SAP ERP OR SAP S/4HANA

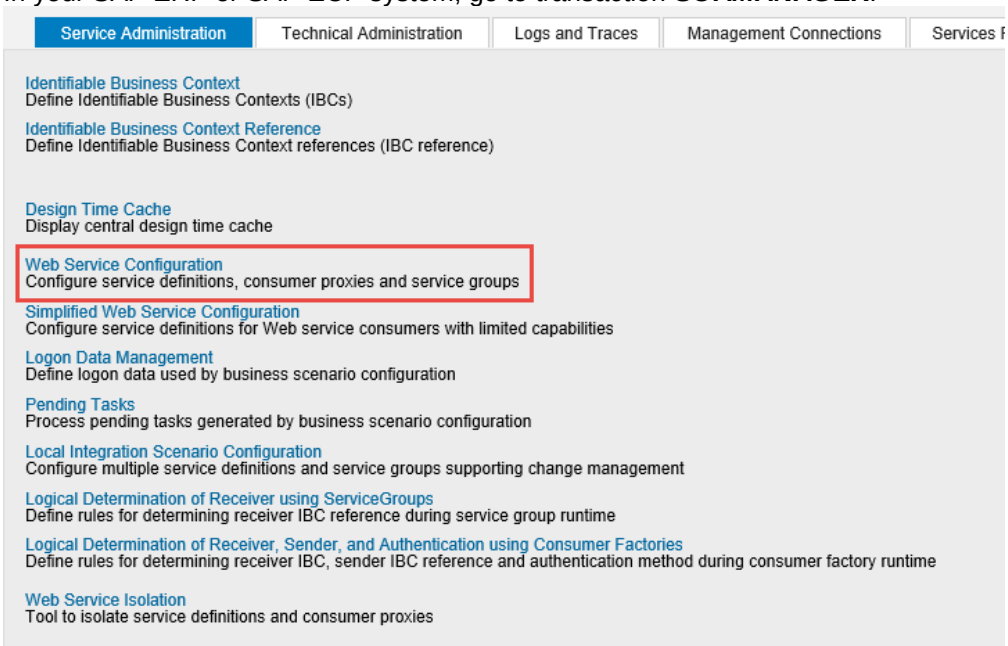
The connection between SAP Payroll system and SCPI needs to be established for communication purpose.

5.1 Create the logical ports in SOAMANAGER

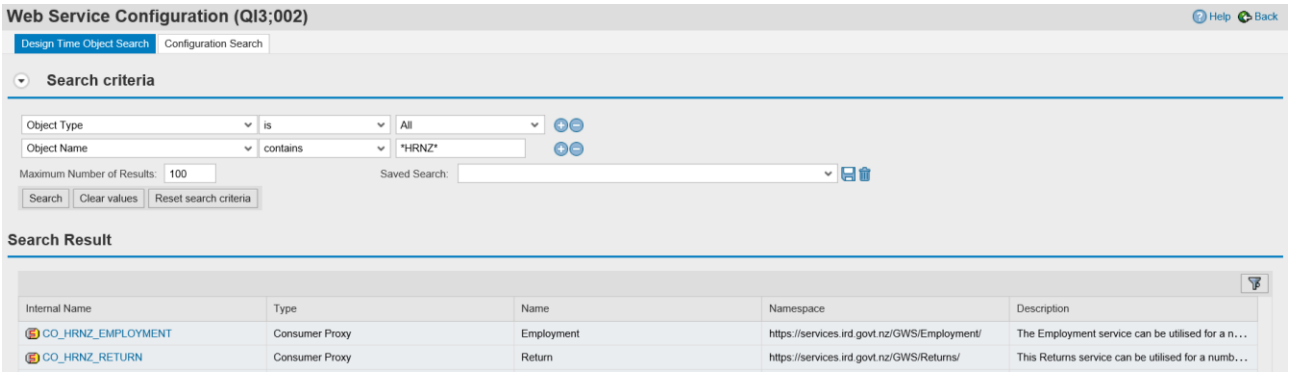
The proxies have to be connected to the SAP CLOUD PLATFORM INTEGRATION tenant via logical ports. In the productive SAP ERP or SAP ECP system, the logical ports are configured to connect to the productive SAP CLOUD PLATFORM INTEGRATION tenant.

Note: the look and feel of the screens in your system may differ from the screenshot below, depending on your release.

1. In your SAP ERP or SAP ECP system, go to transaction **SOAMANAGER**.



2. Select Web Service Configuration and find the proxies created for New Zealand Pay Date reporting. (Note that these will only be available if SAP Note 2672190 has been implemented.)



3. Create logical port(s) for each proxy.

The logical ports you will be creating are:

Proxy: **CO_HRNZ_TOKEN_CHECK**

Logical Port Name	Description	Corresponding IFLOW	Example CXF path
LP_CO_HRNZ_TOKEN_CHECK_HCI	LP for OAUTH token validation backend	OAUTH Token Validation Backend	/cxf/validatebackend

Proxy: **CO_HRNZ_EMPLOYMENT**

Logical Port Name	Description	Corresponding IFLOW	Example CXF path
LP_CO_HRNZ_EMPLOYMENT_CREATE_HCI	LP for Employee Service: Create File	Employee Service - Create	/cxf/ird/create
LP_CO_HRNZ_EMPLOYMENT_UPDATE_HCI	LP for Employee Service: Update File	Employee Service - Update	/cxf/ird/upd
LP_CO_HRNZ_EMPLOYMENT_TERMINATE_HCI	LP for Employee Service: Terminate File	Employee Services - Terminate	/cxf/ird/ter

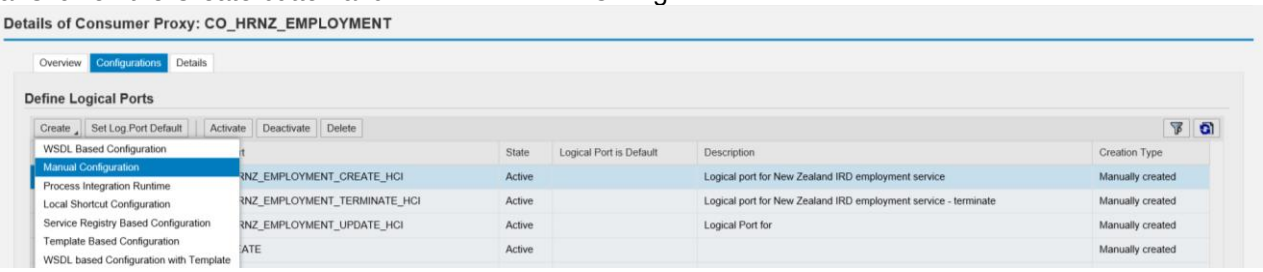
Proxy: **CO_HRNZ_RETURN**

Logical Port Name	Description	Corresponding IFLOW	Example CXF path
LP_CO_HRNZ_RETURN_HCI	LP for Employment Information: Return File	Employment Information - Pay Date File	/cxf/ird/return

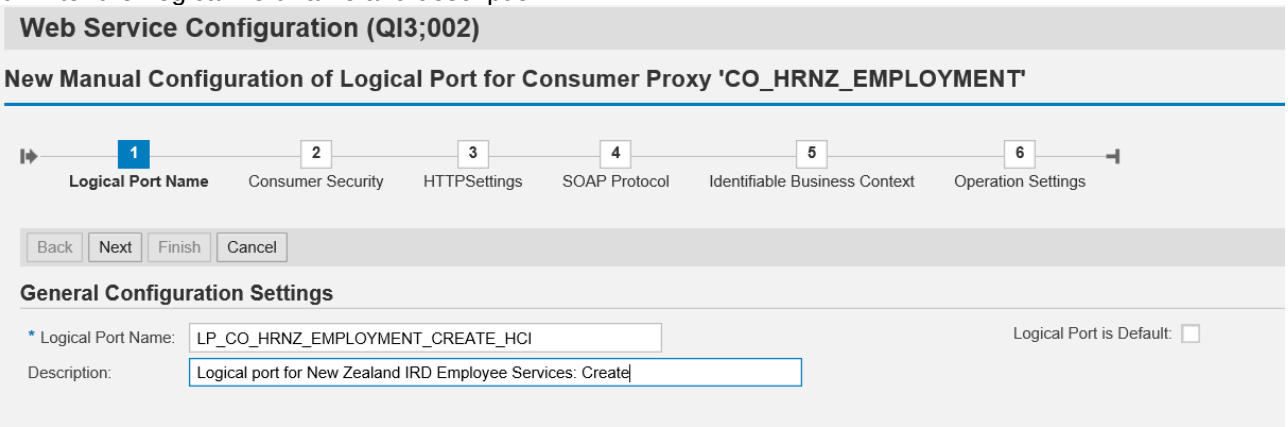
The steps are the same for all the logical ports.

This document has the example for “LP_CO_HRNZ_EMPLOYMENT_CREATE_HCI” and this can be used as an example to create each separate port.

a. Click on the Create button and choose “Manual Configuration”.



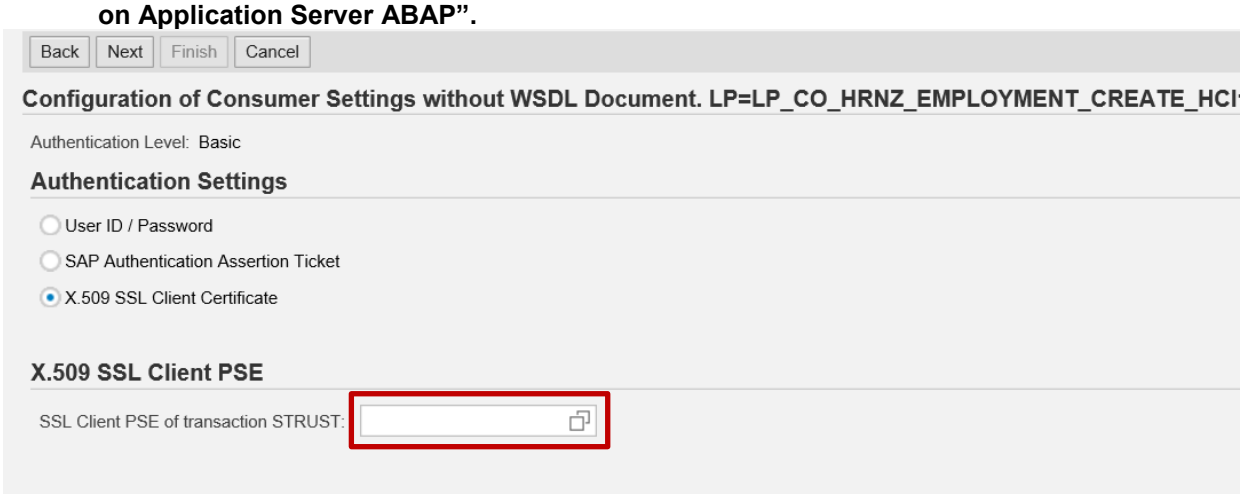
b. Enter the Logical Port name and description



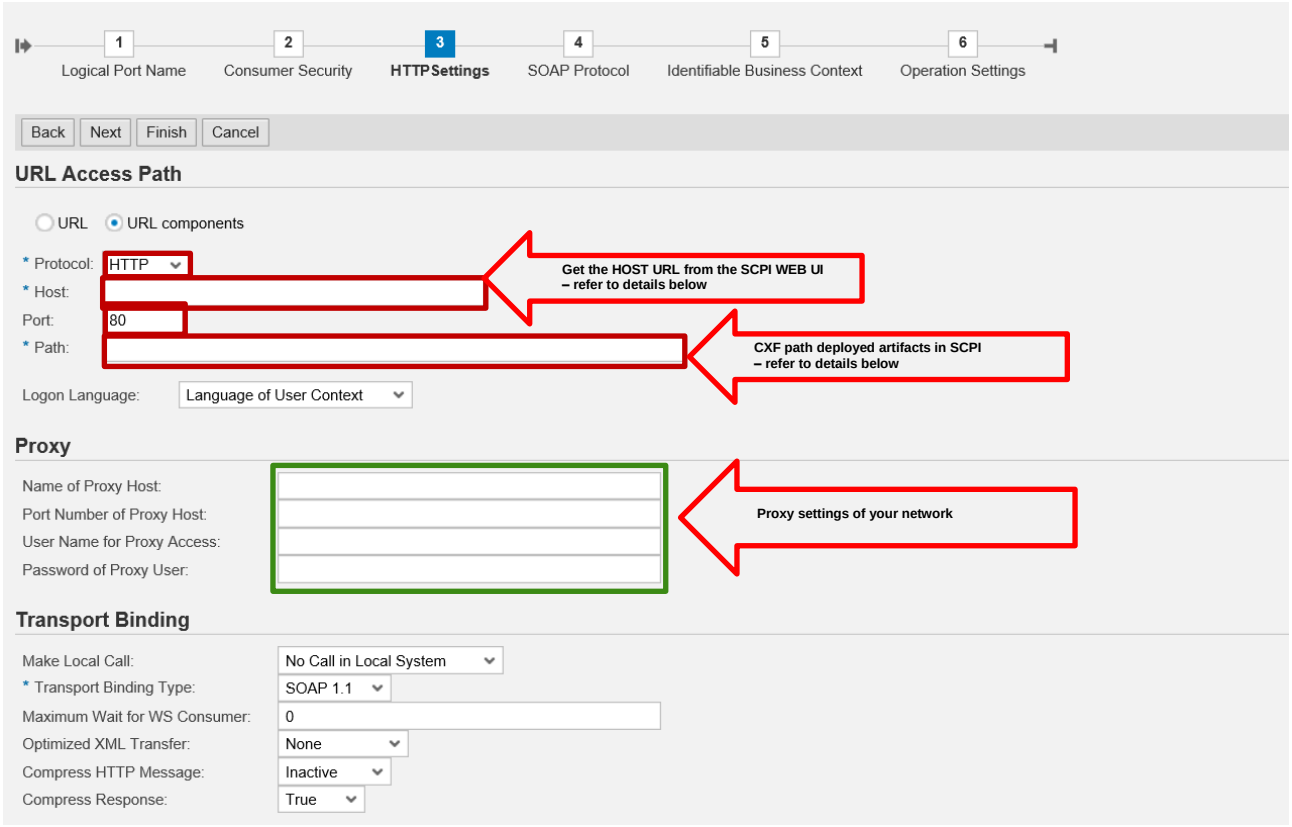
c. The *Consumer Security* tab page configuration depends on the security being used for the SAP ERP or SAP ECP - SAP CLOUD PLATFORM INTEGRATION communication.

- If you use basic authentication, select the *User ID / Password* radio button and enter the *User Name* and *Password*.
- If you use certificate-based authentication, select the *X.509 SSL client certificate* radio button and ensure that the required certificates are available in transaction *STRUST. (Note that this is the recommended SAP option.)*

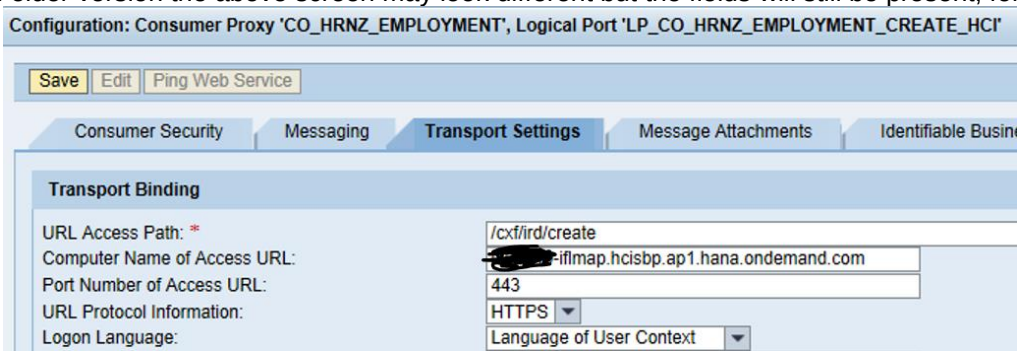
  Note: if you do not see this radio button or cannot select it, please refer to notes **2368112 “Outgoing HTTPS connection does not work in AS ABAP”** and **510007 “Setting up SSL on Application Server ABAP”.**



d. On the *HTTP Settings* tab page, make the following entries: **Note:** the screenshots may look slightly different in your system depending on the release, but all the required fields should be available.

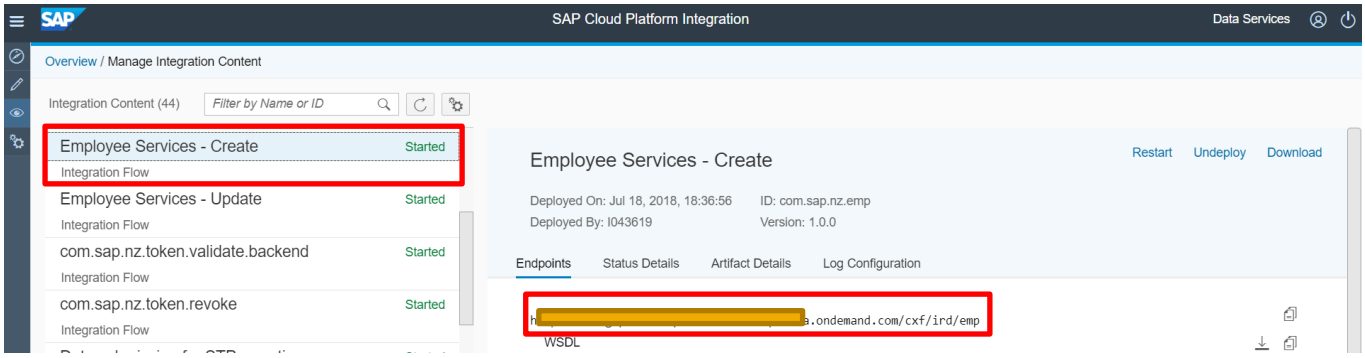


Note that in older version the above screen may look different but the fields will still be present, for example:



e. Get HOST URL & CXF path from SCPI WEB UI

To find the *Host*, go to Cloud Integration Web UI, choose *Monitor* and under *Managed Integration Content* go to *All*. Use the search to find your integration flow as in the screenshot below:

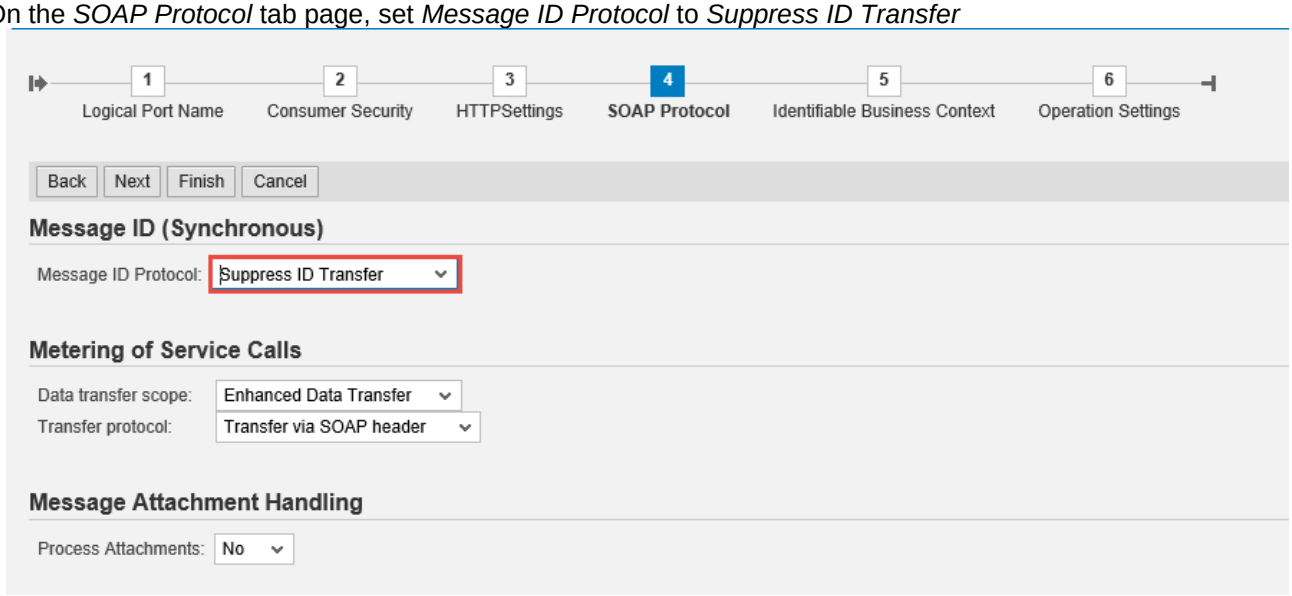


The URL found under the Endpoints section has the HOST URL and the CXF path.

Host url = xxxxxxxxxx.sap.hana.ondemand.com
CXF path = /cxf/ird/emp
Update the information in the HTTP settings section.

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

f. On the *SOAP Protocol* tab page, set *Message ID Protocol* to *Suppress ID Transfer*



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

NOTE: In case you want to test your configuration, **do not use** WebService Ping, as it is not supported by SAP Cloud Platform Integration. But you can setup a HTTP connection in transaction **SM59**. Maintain the host and port of SAP Cloud Integration service (e.g., for path /cxf/ird/create) and execute a connection test. In case of a successful connection you will receive an error with HTTP return code 500.

6 SENDER CHANNEL CONNECTION AUTHORIZATION

The iflows in this package can be authorized by either User Role or security certificate. The iflows by default has been set to “User Role” based authorization which would mean that if the iflow is invoked by an user for sending any file, the system would prompt a pop up for entering user id and password.

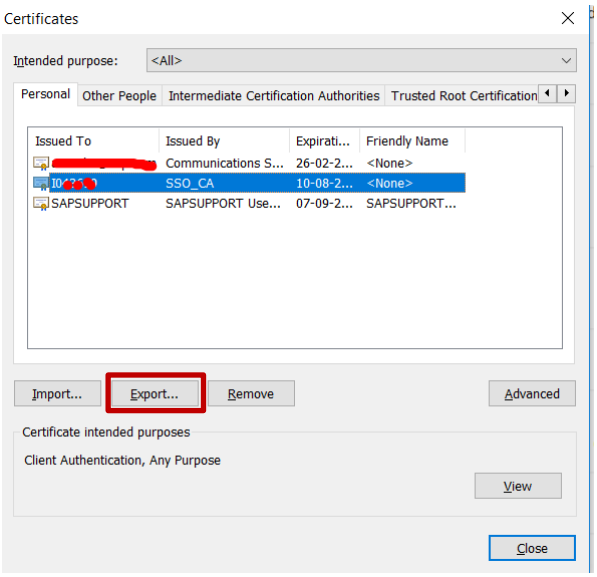
6.1 Certificate based authorization for HTTP sender channel

The Iflows, **OAUTH Token**, **OAUTH Token Validation** & **OAUTH Token Revoke** have HTTP as sender channel. These iflows are invoked through a browser. If you want to configure the authorization by Certificate, then you will have to use the client certificate which is installed in the PC.

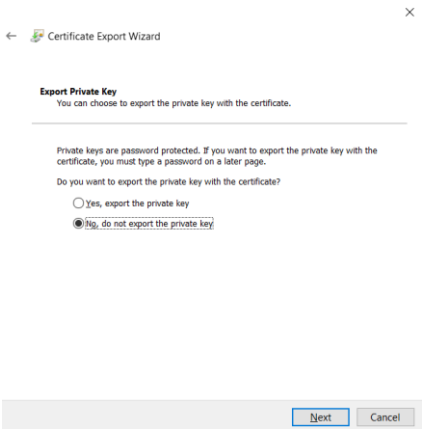
6.1.1 Download the public certificate from the browser.

a. Open internet explorer settings -> internet options -> content -> certificates

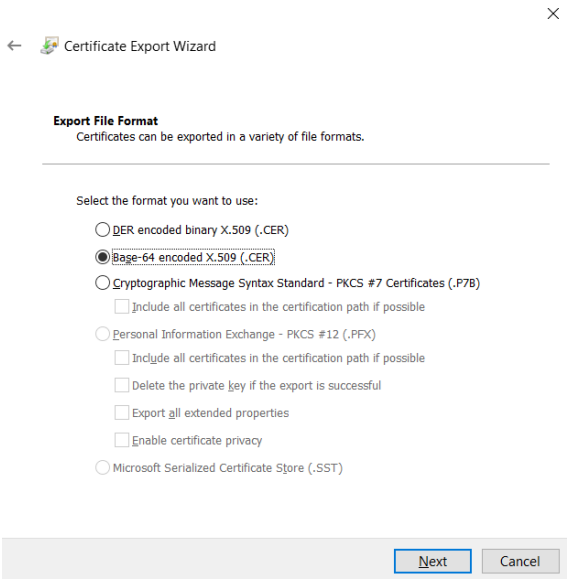
b. Select the certificate which you wish to use for authenticating the user and click on “Export” button.



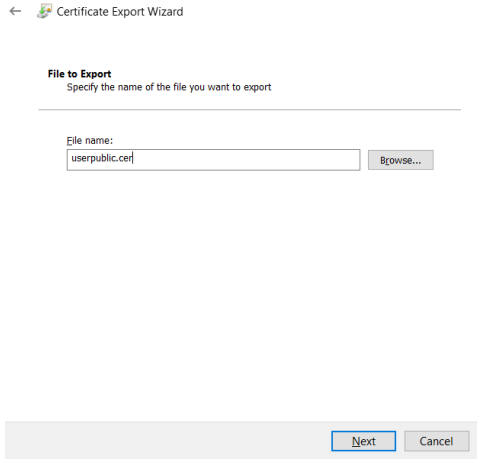
c. Select “No, do not export the private key”



d. Select “Base-64 encoded” option and save the



e. Saver the certificate with “.cer” extension.

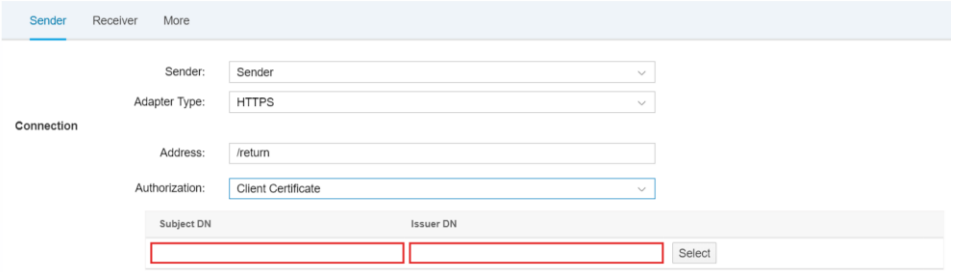


6.1.2 Assign the public certificate for authorization

The public certificate which was downloaded needs to the assigned in the iflow for authenticating the user call from browser. The assignment can be done in two ways.

a. Assign the Client certificate at IFLOW level.

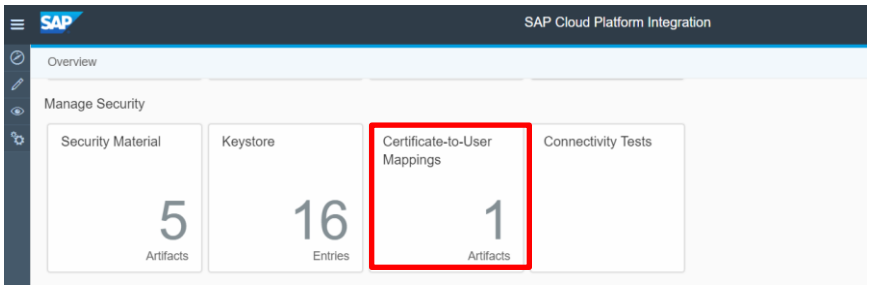
   This can be done by changing the authorization to “Client certificate”. And you can upload the public certificate by Clicking on the “Select” button.



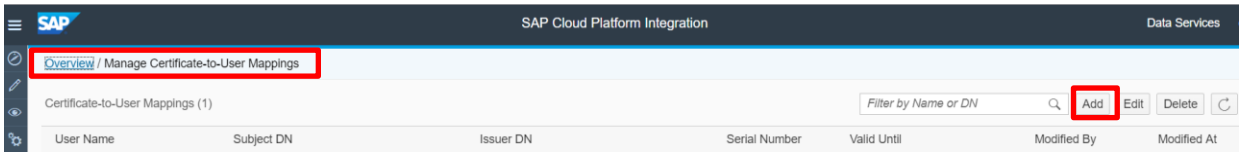
With this method you shall be able to assign only one certificate.

b. Use “User to certificate mapping”
With this method you will maintain “User Role” in the iflow while configuring but will have user to certificate mapping to authenticate the user. By default, user should have the role “**ESBMessaging.send**” to be able to invoke the iflow.

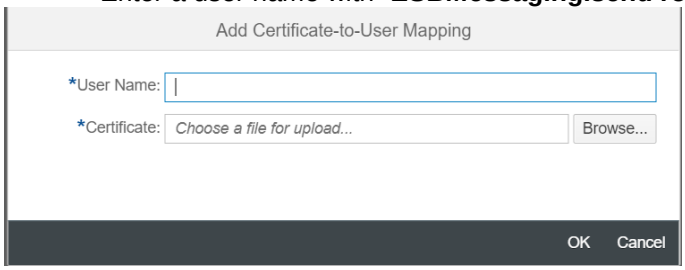
- Go to SAP Cloud Platform Integration-> Overview ->Certificate-to-User Mappings.



- Press button Add



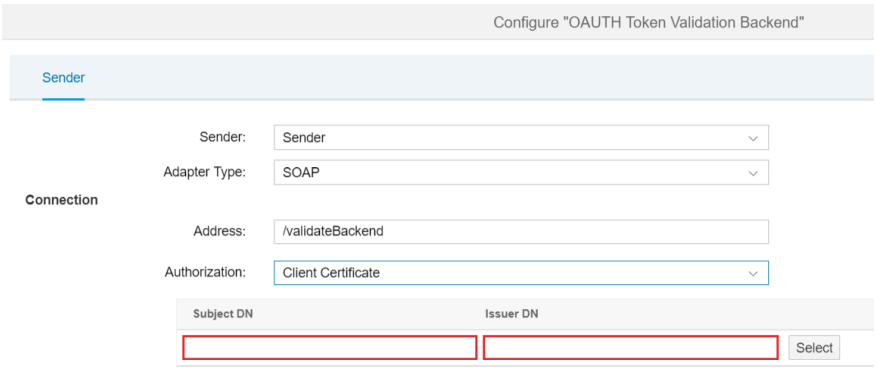
- Enter a user name with “**ESBMessaging.send role**”, upload the SSL certificate



6.2 Certificate based authorization for SOAP sender channel

The iflows Employee Service – Create, Employee Service – Update, Employee Service – Terminate, Employment Information - Pay Date File & OAUTH Token Validation Backend have SOAP as sender channel. If you wish to use client certificate for authentication, then you will have to assign the public certificate of the key pair used in SOA Manager configuration.

For example: choose “Client Certificate” as the Authorization type. Click on the select button to upload the public certificate of the key pair used while configuring the SOAP endpoint in SOA Manager.



7 REGISTER YOUR SCPI DETAILS WITH INLAND REVENUE

SAP Cloud Platform Integration (SCPI) uses a client certificate to authenticate the communication with external systems. At the Inland Revenue server, the authentication is done using MUTUAL TLS method. The public key of a key pair which is installed in SCPI tenant needs to be downloaded and then given to Inland Revenue for them to install in their server. This is part of the registration process that must be followed before you can fully test the connection to Inland Revenue.

Please refer to the document "**New Zealand Inland Revenue- Registering for Payroll Services**" for more information about the registration process. A copy of this document can be found with SAP Note 2672190.

www.sap.com/contactsap

THE BEST RUN SAP®