

## New Zealand IRD- Registering for Payroll Services

PUBLIC





## TABLE OF CONTENTS

|                                                                                   |    |
|-----------------------------------------------------------------------------------|----|
| OVERVIEW .....                                                                    | 3  |
| 1 INLAND REVENUE ONBOARDING AND ASSOCIATED .....                                  | 3  |
| 1.1 SAP Customer Onboarding Guide.....                                            | 3  |
| 1.2 Customer Support Portal for the Gateway.....                                  | 3  |
| 1.3 IR1266 Due Diligence Questionnaire guide .....                                | 3  |
| 1.4 Developer Portal Registration and Credential Management Guide.....            | 4  |
| 2 REQUESTING AN IR ISSUED CERTIFICATE AND IMPORTING INTO SCI .....                | 4  |
| 3 REGISTERING THE RETURN_URL .....                                                | 7  |
| 3.1 Setting the Sender Channel Address using user parameter for OAUTH IFLOW ..... | 7  |
| 3.2 Determine the return_url.....                                                 | 8  |
| 4 TESTING THE CONNECTION TO IRD .....                                             | 10 |
| 5 CHANGING CPI ENVIRONMENT/DEREGISTERING.....                                     | 10 |



## OVERVIEW

In 2026, Inland Revenue (IR) introduced its own certificate management solution and no longer accepts certificates issued by third parties. Previously, SAP registered customer return URLs and provided SCI Integration certificate common name details to Inland Revenue on behalf of customers. Under the new process, which is mandatory from 30 September 2026, the relationship between the customer and Inland Revenue is more direct and self-managed. Customers must request their own unique certificate directly from Inland Revenue and are responsible for renewing the IR-issued certificate.

To request a certificate, an authorised office holder must register their organisation for Gateway Services and agree to Inland Revenue's terms and conditions. Access will then be granted to the Gateway Services Support Portal and IR's Developer Portal, where the authorised office holder can specify which users within their organisation should be granted access. Access to the Developer Portal is required to:

- Request an IR-issued certificate.
- View the unique client ID, which must be configured in the payroll system and several SCI iFlows.
- View the client secret, which must be configured in several SCI iFlows.
- Specify the return URL.

Access to the Gateway Services Support Portal is required to lodge support tickets with Inland Revenue, for example if there are issues requesting or renewing a certificate.

These processes are controlled by Inland Revenue, and the relevant documentation is attached as part of the Pay Day Filing Integration Package documentation.

Note that the required IR registration process involves multiple steps, so sufficient time should be allocated when initially onboarding.

## 1 INLAND REVENUE ONBOARDING AND ASSOCIATED DOCUMENTS

### 1.1 SAP Customer Onboarding Guide

This document explains the Inland Revenue onboarding process for new customers and shows the steps in the process at a high level. This document should be read first.

### 1.2 Customer Support Portal for the Gateway

The starting point for registration is for an authorised person to register the organisation for Gateway services. It is an online form and most fields are self-explanatory. An authorised person must complete this because one of the questions is to accept Inland Revenue's conditions of use terms.

There are a couple of fields where some suggested input is recommended for SAP customers, and this is documented in this guide. Inland Revenue will review the information and issue a user name for the person requesting registration. The user then creates their own password.

Note that this document also contains some general information about the Gateway Services Support Portal which is useful when a ticket needs to be raised.

### 1.3 IR1266 Due Diligence Questionnaire guide

Once access has been created to the Gateway Services Support portal the user must select 'Submit a Product Request' and Inland Revenue will then create a task in the Portal for an IR1266 Due Diligence Questionnaire to be completed. SAP will be supplying answers to some of the questions so the IR1266 Due Diligence Questionnaire Guide should be consulted to assist with completion of this.

Inland Revenue will review the questionnaire and once approved will notify the user and direct the user to register for access to the Developers Portal.

This is a good time for the user to raise a support ticket in the Gateway to specify who else within the organisation should be given access to the Support Portal. This is likely to be technical support people (more than one person is recommended in case the main person is absent). Note that the requested users should have emails that are consistent with your organisation's email domain name. If technical support has been outsourced the relevant third-party person(s) should be allocated a company email.

#### 1.4 Developer Portal Registration and Credential Management Guide

Initial registration for the Developers Portal should also be completed by an authorised office holder as the person requesting access will need to accept IR's terms and conditions. They will then specify who the key contact within their organisation should be for Pay Day Filing and who should be given access (and to what level). Details of this process is documented in the **Reference Guide 3 - Developer Portal Registration and Credential Management Guide**.

The guide also explains how to request/new an IR issued certificate and how to maintain OAUTH credentials.

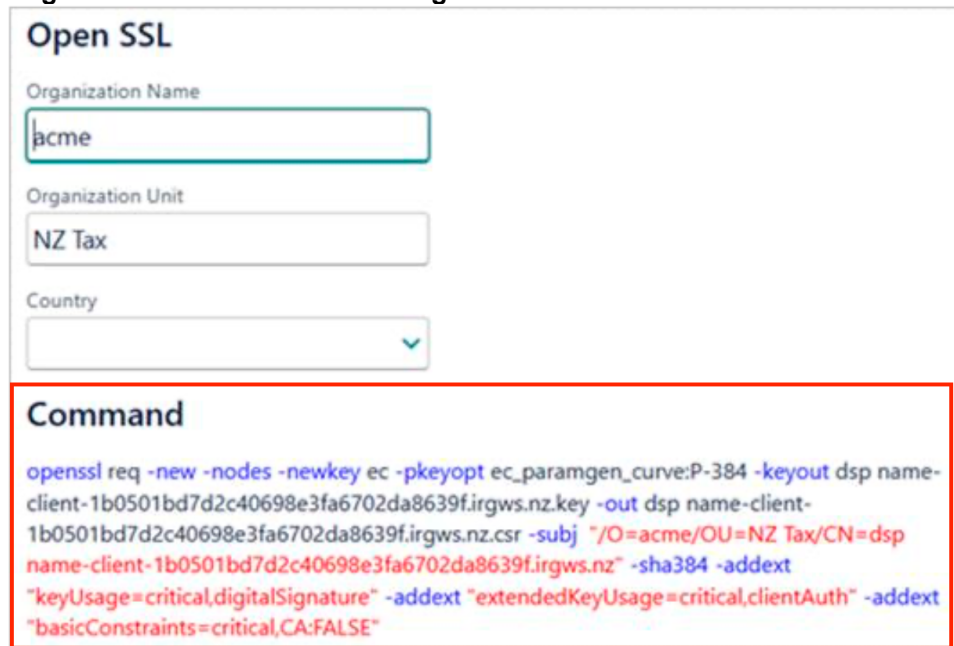
## 2 REQUESTING AN IR ISSUED CERTIFICATE AND IMPORTING INTO SCI

### 2.1 Requesting an IR issued Certificate

The **Reference Guide 3 - Developer Portal Registration and Credential Management Guide** details the steps within the IR Developers portal to request a certificate.

**Note:** The commands in this section are provided as examples. On Windows, the commands may vary.

2.1.1 Copy the string below the Command from step 3.5 in **Reference Guide 3 - Developer Portal Registration and Credential Management Guide**.



The screenshot shows a web form titled "Open SSL" with three input fields: "Organization Name" (containing "acme"), "Organization Unit" (containing "NZ Tax"), and "Country" (empty with a dropdown arrow). Below the form, a red-bordered box contains the following command:

```
openssl req -new -nodes -newkey ec -pkeyopt ec_paramgen_curve:P-384 -keyout dsp name-client-1b0501bd7d2c40698e3fa6702da8639f.irgws.nz.key -out dsp name-client-1b0501bd7d2c40698e3fa6702da8639f.irgws.nz.csr -subj "/O=acme/OU=NZ Tax/CN=dsp name-client-1b0501bd7d2c40698e3fa6702da8639f.irgws.nz" -sha384 -addext "keyUsage=critical,digitalSignature" -addext "extendedKeyUsage=critical,clientAuth" -addext "basicConstraints=critical,CA:FALSE"
```

2.1.2 In Mac/Windows, open the terminal/cmd and paste the command and execute/enter. This will generate 2 files: **.CSR** and **.KEY**



sapnz-test-e29ed97e37b4403fbdb1f77503e76c8a.irgws.nz.csr



sapnz-test-e29ed97e37b4403fbdb1f77503e76c8a.irgws.nz.key

2.1.3 Upload this .csr file in step 3.8 in **Reference Guide 3 - Developer Portal Registration and Credential Management Guide**

2.1.4 Once IRD approves, you will get an option to download the new certificate in PEM or DER format as mentioned in step 3.9 in **Reference Guide 3 - Developer Portal Registration and Credential Management Guide**. Once you manually extract those, you'll have 3 files: Client.cer, Intermediary.cer and Root.cer

sapnz-test-e29ed97e37b4403fbdb1f77503e76c8a.irgws.nz.20260319-20270318

| Name                                                                                                                                                         | Date Modified | File Size |
|--------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------|-----------|
|  sapnz-test-e29ed97e37b4403fbdb1f77503e76c8a.irgws.nz.20260319-20270318.cer | 2026-03-20    | 677 bytes |
|  Inland Revenue Trusted NonProd Intermediary ECDSA G1.cer                   | 2026-03-20    | 666 bytes |
|  Inland Revenue Trusted NonProd Root G1.cer                                | 2026-03-20    | 619 bytes |

Note:

- Rename the files for a shorter name in the local machine.
- Also change the extension to .CRT from cer

2.1.5 Generate KeyPair using 4 files: 3 above files and the key file from step 2.1.2

2.1.6 Open a terminal/cmd and run the command: This will concatenate the root and Intermediary

```
cat intermediary.crt root.crt > chain.crt
```

Note: Please check the terminal that there are no errors while the file is generated

2.1.7 In the same terminal/cmd, now run the command:

```
openssl pkcs12 -export -out bundle.pfx -inkey private.key -in
certificate.crt -certfile chain.crt
```

Note: It will ask for a password. This password will be later asked when uploading the file in keystore in step 2.2.3

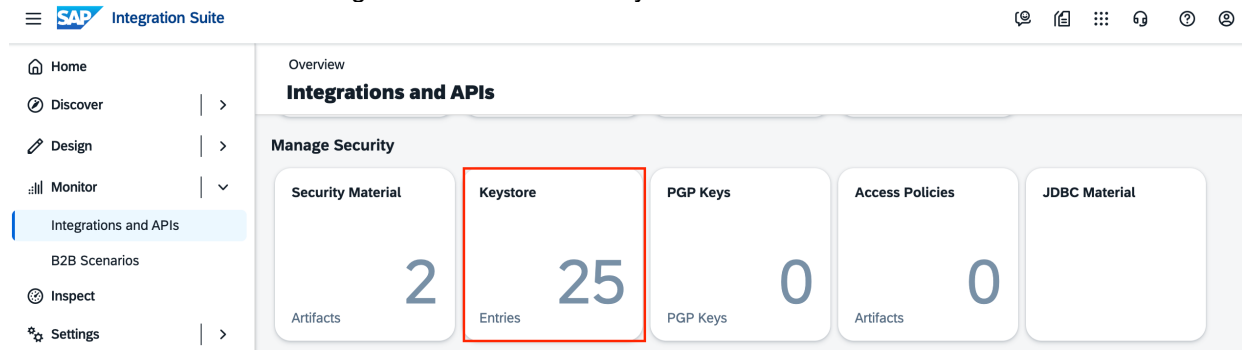
```
[I353407@KTH06CQHXL sapnz-test-e29ed97e37b4403fbdb1f77503e76c8a.irgws.nz.20260319-20270318 (2) % openssl pkcs12 -export -o
ut bundle.pfx -inkey private.key -in certificate.crt -certfile chain.crt
Enter Export Password:?
```

The file bundle.pfx is generated. This file is used as key in step 2.2.3

## 2.2 Importing the IR issued Certificate into SCI

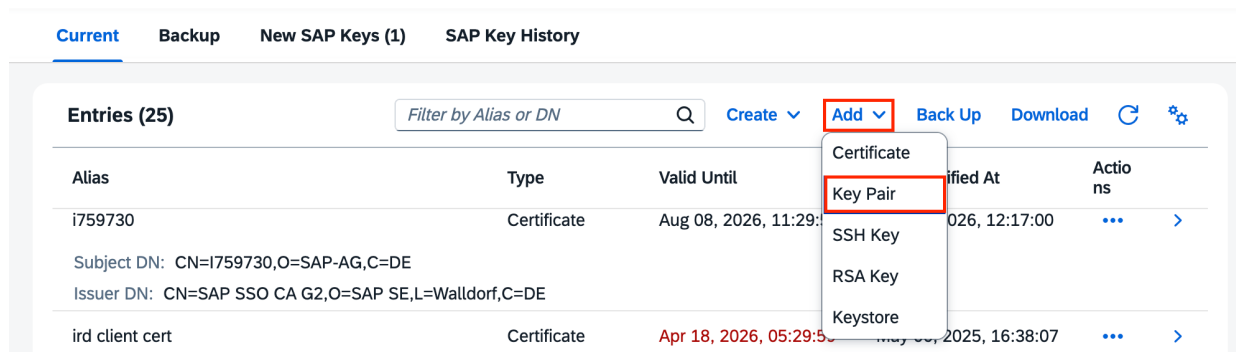
After obtaining the certificate, follow the steps below to import it into the SAP Cloud Integration keystore.

### 2.2.1 Go to Monitor -> Integrations and APIs -> Keystore



### 2.2.2 Click on Add -> Select KeyPair

[Overview](#) / Manage Keystore



### 2.2.3 Enter the following:

#### Add Key Pair

Alias: \*

File: \*

Password: \*

Alias: ird\_gateway\_integrationcertificate (recommended but this can be anything you want)

File: bundle.pfx file got from step 2.1.7

Password: Set in step 2.1.7

This Alias is used as the Private Key Alias in the Receiver configuration of following integration flows as described in the **New Zealand Inland Revenue Reporting for Payroll** configuration guide:

- Employee Services – Create V2
- Employee Services – Update V2
- Employee Services – Terminate V2
- Employment Information – Pay Date File V2

### 2.2.4 Click on Add

### 2.2.5 Click on Confirm when you get a warning as below:

**Confirm Key Pair**

Could not establish trust to the key pair by the certificates contained in the keystore.  
You may confirm that you trust the key pair 'ird\_gateway\_test' by checking the fingerprint.

**Certificate Details**

Owner: Tenant Administrator  
Key Type: EC  
Key Size: 384  
Signature Algorithm: SHA384withECDSA  
Subject DN: CN=Inland Revenue Trusted NonProd Root G1,OU=GWS PKI,O=Inland Revenue,C=NZ  
Issuer DN: CN=Inland Revenue Trusted NonProd Root G1,OU=GWS PKI,O=Inland Revenue,C=NZ  
Serial Number: 0xEC667BEA85047890175AFCEA0F62705EA2125C  
Version: 3  
Valid From: Feb 08, 2026, 16:30:00  
Valid Until: Feb 06, 2036, 16:30:00

**Fingerprints**

SHA-1:  
6C:27:F3:6F:E4:91:A1:B1:C6:BB:23:D0:44:35:0B:27:17:E4:97:F4

SHA-256:  
5B:D4:D6:D3:C7:E8:34:44:D7:F7:47:0E:46:3F:5C:E4:66:D5:96:DE:CE:11:DD:E5:D6:5E:F7:EC:12:5B:EF:BE

SHA-512:  
3B:62:31:02:C5:5A:A5:C0:AF:8F:32:6B:BC:CE:94:A8:0F:63:F3:AA:44:3A:B4:3D:F3:86:F0:73:FF:77:30:88:  
22:FA:16:23:F9:F8:F2:12:1E:E5:D3:14:B7:09:9E:14:C3:32:84:08:F5:6C:6A:85:82:55:4A:E7:30:EE:3A:34

Confirm

Cancel

### 3 REGISTERING THE RETURN\_URL

The return\_url must be updated in the IR Developers Portal. The following details how to determine the return\_url. The instructions for updating the IR Developers Portal are explained in the OAuth Credential Management section of the **Reference Guide 3 - Developer Portal Registration and Credential Management Guide**.

#### 3.1 Setting the Sender Channel Address using user parameter for OAUTH IFLOW

The external parameter is provided to enable customers to configure the data as per their requirement. The sender channel for *OAUTH Token V2* iflow is HTTP.

The *OAUTH Token V2* integration flow uses the Sender Channel Address configured in the HTTP sender channel. This value forms the suffix of the return\_url that must be registered with Inland Revenue (IR).

Follow these steps to set the Sender Channel Address:

- 1) Go to the integration package that was copied from the original 'New Zealand Inland Revenue Reporting for Payroll Version 2'

| Integration Packages (2)                               |          |         |                 |                               |                                                                                           |        | new zealand <span>×</span> <span>Q</span> <span>↓↑</span> |  |
|--------------------------------------------------------|----------|---------|-----------------|-------------------------------|-------------------------------------------------------------------------------------------|--------|-----------------------------------------------------------|--|
| Name                                                   | Mode     | Version | Created By      | Created Date                  | Description                                                                               | Action |                                                           |  |
| New Zealand Inland Revenue Reporting Payroll Version 2 | Editable | 1.1.3   | anand.s@sap.com | Mon, 11 Mar 2024 07:29:35 GMT | This package provides the integration flows for New Zealand Pay Date Reporting Version 2. |        |                                                           |  |

- 2) Click on the Artifacts tab
- 3) Click on action button that corresponds to integration flow 'OAUTH Token V2'.

|                                                                                                                                                                              |                  |       |     |   |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------|-------|-----|---|
| <b>Employment Information - Pay Date File V2</b><br>Payment information of all the employees paid by an organization within a pay period will be reported to IRD<br>Modified | Integration Flow | 1.0.5 | ... | > |
| <b>OAUTH Token Revoke V2</b><br>This is used to revoke the OAUTH token in the Inland Revenue server.<br>Modified                                                             | Integration Flow | 1.1.2 | ... | > |
| <b>OAAUTH Token V2</b><br>This is used for getting the OAUTH 2.0 token from Inland Revenue server<br>Modified                                                                | Integration Flow | 1.1.2 | ... | > |
| <b>OAAUTH Token Validation Backend V2</b><br>This is used to validate the token in the backend while sending files from B2A manager.<br>Modified                             | Integration Flow | 1.1.2 | ... | > |
| <b>OAAUTH Token Validation V2</b><br>This is used to validate the token obtained from Inland Revenue server for its expiry<br>Modified                                       | Integration Flow | 1.1.2 | ... | > |

- Copy
- Git Pull
- Git Push
- View metadata
- Download
- Configure
- Deploy

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

## Sender Tab

The sender for this scenario is the IRD server. The IRD 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.

Configure "OAAUTH Token V2"

Runtime Profile: Cloud Integration

**Sender** Receiver More

**Connection**

Sender: Sender

Adapter Type: HTTPS

Address: /return

Authorization: User Role

User Role: ESBMessaging.send

Select

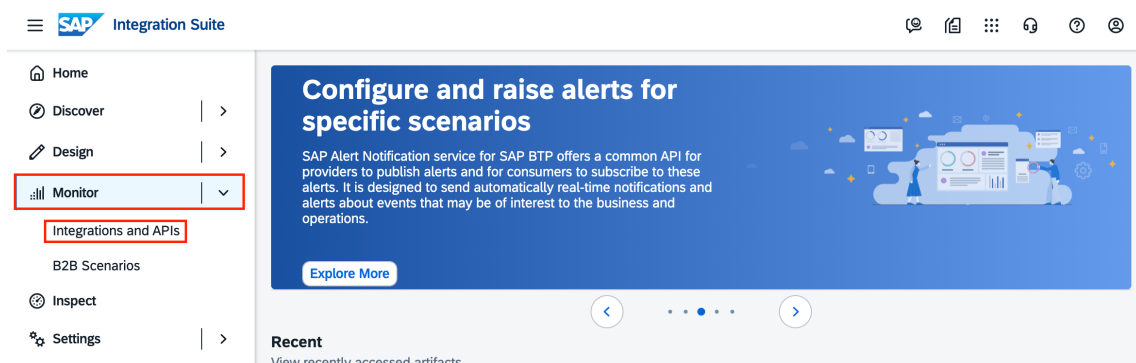
The address configured here will be the suffix used to form the RETURN\_URL for OAUTH 2.0 token as required by IRD.

## Note:

- The connection address must be unique within a tenant.
- If a valid Connection Address is already configured, no further changes are required.

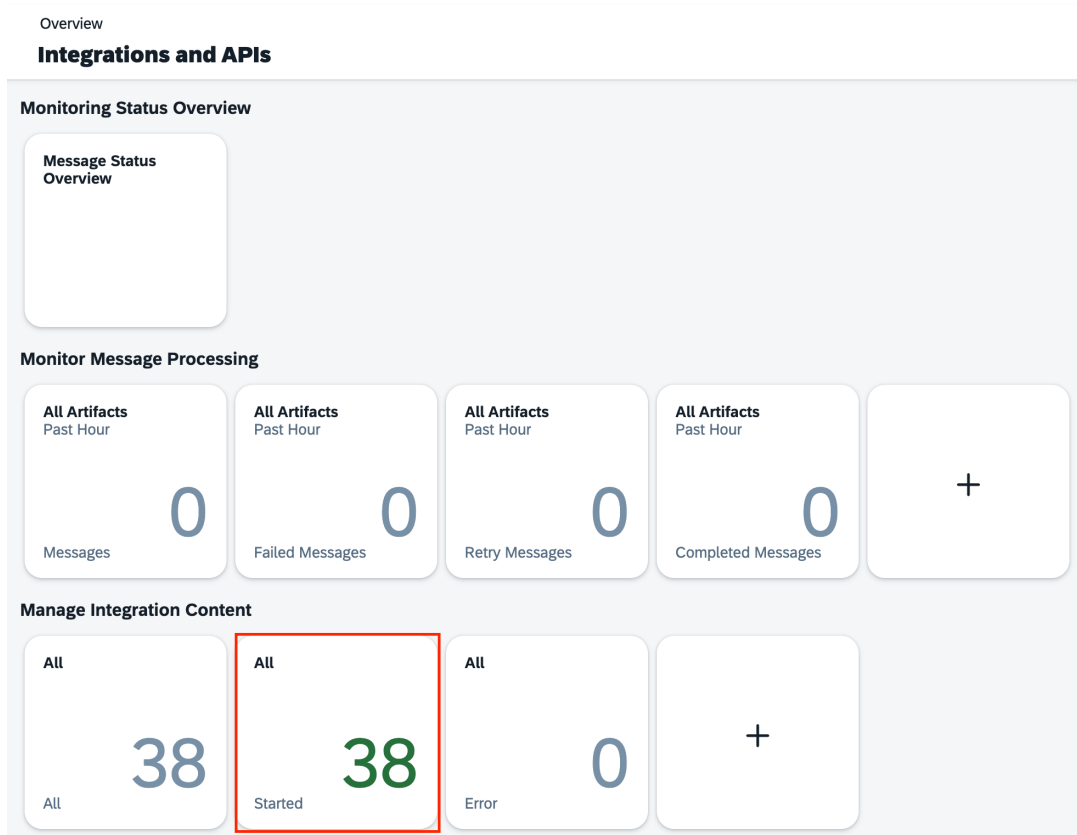
## 3.2 Determine the return\_url

1. Go to SAP Cloud Integration Suite



Click on Monitor -> Integration and APIs

2. Click on Manager Integration Content -> Started



3. Search for *OAuth Token V2* iFlow in the search bar and click on it

Overview / Manage Integration Content

### Manage Integration Content

Integration Content (38)

oauth x Q

| Name                                     | Status  |
|------------------------------------------|---------|
| <b>OAuth Token V2</b>                    | Started |
| Integration Flow                         |         |
| OAuth Token Validation V2.1 Test         | Started |
| Integration Flow                         |         |
| OAuth Token Validation Backend V2.1 Test | Started |
| Integration Flow                         |         |
| OAuth Token Revoke V2.1 Test             | Started |
| Integration Flow                         |         |
| OAuth2_Token                             | Started |
| Integration Flow                         |         |

#### OAuth Token V2.1 Test

Restart Undeploy Download

Deployed On: Jun 24, 2026, 14:49:57 ID: OAuth\_Token\_V2.1\_Test  
Deployed By: arnab.chandra01@sap.com Version: 1.0.2  
Package: New Zealand Inland Revenue Reporting for Payroll Version 2 Test

Endpoints Status Details Artifact Details Log Configuration

##### Endpoints

<https://payroll-b2g-integration-rjwejfze.it-accd003-rt.cfapps.eu12.hana.ondemand.com/http/return>

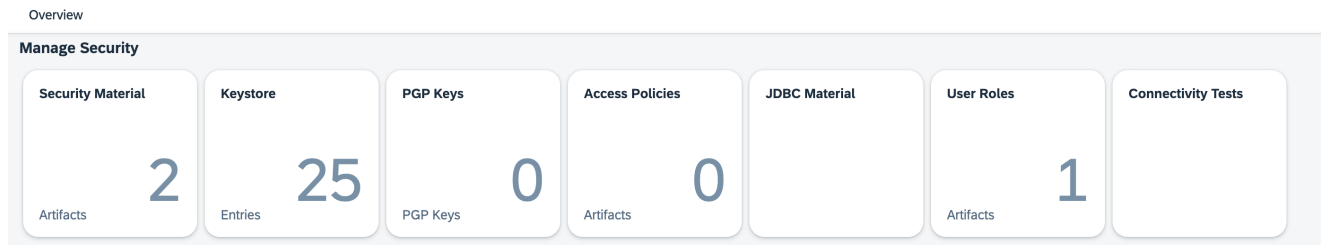
##### Status Details

The highlighted link in the “Endpoints” section is the return\_url that must be registered in the IR Developer Portal.

## 4 TESTING THE CONNECTION TO IRD

Once the IR certificate has been imported into the SAP Cloud Integration keystore and configured for use, you can test the connection from your SCI tenant to the IRD server.

- a. Go to the operations overview section of the SCI tenant



- b. Click on “Connectivity Tests” tab and select the TLS tab.

Host: [services.ird.govt.nz](https://services.ird.govt.nz)

Port: 4046

Select “Authenticate with Client Certificate”

Alias: ird\_gateway\_integrationcertificate

(Or the alias used when importing the IR-issued certificate into the SAP Cloud Integration keystore)

Click the button “Send” to test the connectivity. You should get the below response.

The screenshot shows the 'Connectivity Tests' page with the 'TLS' tab selected. The 'Request' section contains the following fields: Host (test5.services.ird.govt.nz), Port (4046), and a checked box for 'Authenticate with Client Certificate'. The 'Alias' field is set to 'ird\_gateway\_integrationcertificate'. There are also checkboxes for 'Include new SAP Key' (unchecked) and 'Valid Server Certificate Required' (checked). A 'Send' button is at the bottom. The 'Response' section shows a green success message: 'Successfully reached host at test5.services.ird.govt.nz:4046'. Below this, it lists 'Client Certificate Alias: ird\_gateway\_integrationcertificate' and 'Server Certificate: Valid'. There are expandable sections for 'Server Certificate Chain' and 'Trusted CAs for Client Certificates', each with a 'Download' link.

## 5 CHANGING CPI ENVIRONMENT/DEREGISTERING

If the SCI environment is changed, e.g. move to Cloud Foundry, the return url will change and the new return\_url will need to be updated in the Developers Portal. Whilst you transition to the new environment it is acceptable to have two return-urls listed but as soon as there is no filing from the old system, the old return\_url should be removed.

Your registration details are still linked to SAP and hence if you move away from SAP Payroll you should create a case in the Gateway Services Support Portal to advise IR accordingly so that your details can be decommissioned.

[www.sap.com/contactsap](http://www.sap.com/contactsap)

© 2018 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.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

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. See <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.