

Gateway Services

July 2026

Developer Portal Registration and Credential Management guide



New Zealand Government



Inland Revenue
Te Tari Taake

Table of Contents

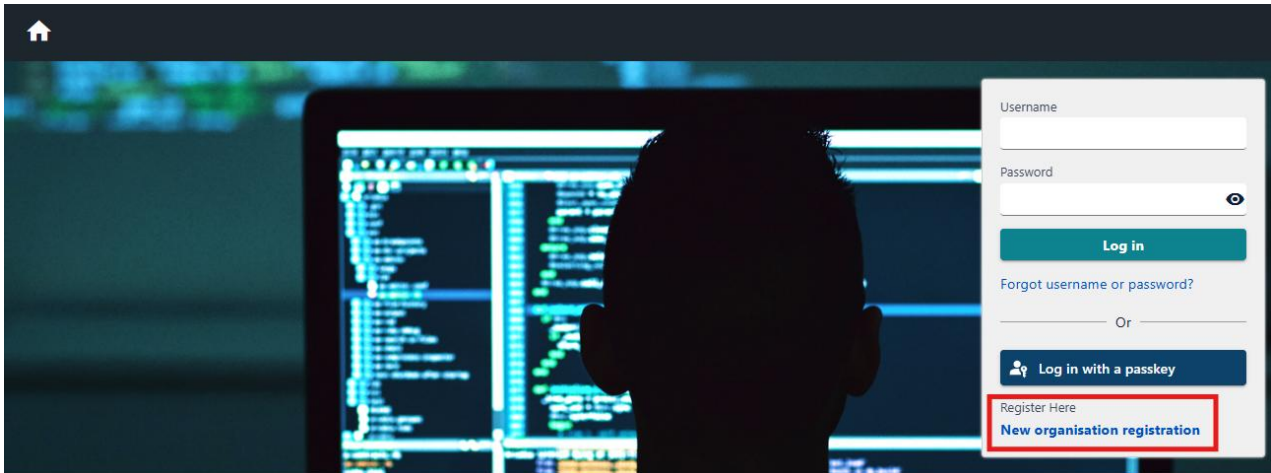
1.	Organisation Registration on the Developer Portal	3
2.	Manage additional logons.....	6
3.	Obtaining and Managing Client Certificates.....	8
4.	Certificate Chain and Security.....	12
5.	PFX Certificate.....	12
6.	Renewing Client Certificates.....	13
7.	Important note for Apple macOS users.....	14
8.	OAuth Credential Management.....	15

1. Organisation Registration on the Developer Portal

Step 1 – New Organisation Registration

Please note: you will receive an email for approval of the product request from Gateway Customer Support Portal with a link for registration to the developer portal.

Click on “New organisation registration”



Step 2 – How to use the portal screen

Please note: The organisation's Key Office Holder is required to create this account. This individual must be authorised to accept the Terms of Use on behalf of the organisation and will have the ability to add, remove, and manage user permissions associated with this account.

Review the details on the page and select “Yes” for both the prerequisites and click “Next”

Step 3 – Developer Portal Registration Screen

Provide your organisation name you register with at the gateway customer support portal and other information and click "Next".

Developer portal registration

Registration information Register

Provide organisation details below to integrate with the gateway services

Organisation details

Organisation name *

Provide business number

Organisation website

If a New Zealand company you can [search the NZBN register](#).

Cancel

< Previous

Next >

[Privacy and Security Policy](#) | [Contact us](#)
© Copyright 2021 Inland Revenue.
[Conditions of use](#)

For more info on government services go to

Te Kāwanatanga o Aotearoa
New Zealand Government

Step 4 – Nominated contact details

Provide the Key Office Holders contact details and review the terms of use and submit the registration form and close the confirmation screen.

Developer portal registration

Registration information Register Create login

Nominated contact

Provide details for a nominated person to be the primary point of contact. They will be given login details for this account.

Nominated contact full name *

Contact email address *

Mobile phone country

Create username *

Mobile phone number *

Terms of Use

[Your Privacy](#)
[Your Security](#)

☐ I agree to the [Terms of Use](#) for Inland Revenue's digital services.

Cancel

< Previous

Submit

Step 5 – Set your password

You will receive an email to set your password.
Please note: Password generation email expires in 30 minutes.

Step 6 – Protect your Developer Portal profile with two-step verification

Please select you preferred two-step verification method and complete the process.

Important Note: You are not required to follow steps under Manage an Integration

2. Manage additional logons

We suggest having at least 2 members of your organisation having 'Full' access to cover for any absences

Click on <Manage My Profile> then click on "I want to..." tab and click on "Manage Additional logons. Click on "Add" and provide required information to create a logon.

Please note: You must have a "full access" role to manage credentials in the Developer Portal.

The screenshot shows the Developer Portal interface. At the top, there is a dark header with a home icon and a user profile icon. Below the header, the main content area is divided into sections. The 'Lagon' section shows 'GWS'. The 'Alerts' section shows 'Product integration in progress' and 'There are 4 unread messages'. A red box highlights the 'Welcome, GWS' message, which includes the text 'You last logged in on Friday, Jun 12, 2026 8:43:14 AM' and a 'Manage My Profile' link with a notification icon. Below this, there is a navigation bar with tabs: 'Main', 'Integrations', 'Credentials', 'Service Activity', and 'Service Notifications'. A search bar is present with the placeholder text 'What are you looking for?'. Below the search bar, there are three main sections: 'Read documentation', 'Manage an integration', and 'Test a file upload'. The 'Manage an integration' section has a list of steps: 'Step 1: Gateway service integration', 'Step 2: Access test environment', 'Step 3: Deploy to production', and 'Upload supporting document(s)'. The 'Test a file upload' section has a list of actions: 'Request access' and 'Test a file upload'. Below this, there is another dark header with a home icon and a user profile icon. Below the header, the main content area is divided into sections. The 'Manage my profile' section shows 'GWS'. Below this, there is a navigation bar with tabs: 'Profile', 'Security', 'Alerts', and 'I want to...'. The 'I want to...' tab is highlighted with a red box. Below the navigation bar, there is a search bar with the placeholder text 'Type to filter'. Below the search bar, there are two main sections: 'Access management' and 'My activity'. The 'Access management' section has a list of actions: 'Manage additional logons' (highlighted with a red box) and 'Cancel my logon'. The 'My activity' section has a list of actions: 'Search submissions' and 'View activity'. At the bottom of the page, there is a footer with links to 'Privacy and Security Policy', 'Contact us', '© Copyright 2021 Inland Revenue', and 'Conditions of use'. On the right side of the footer, there is a logo for 'Te Kāwanatanga o Aotearoa New Zealand Government' and the text 'For more info on government services go to'.

Home

Manage my profile

GWS

Profile Security Alerts **I want to...**

Type to filter

Access management

- Manage additional logons** Manage logons associated to your customer.
- Cancel my logon Cancel your Developer Portal logon. This will remove access to all of your existing integrated services.

My activity

- Search submissions View or search your submissions.
- View activity View your activity on e-Services.

Privacy and Security Policy | Contact us
© Copyright 2021 Inland Revenue.
Conditions of use

For more info on government services go to
Te Kāwanatanga o Aotearoa
New Zealand Government

Confirmation email will be sent to the new user to reset their password.



[<](#) Additional logons

Add additional logon

PIVTEST
1-500-029-000



Lagon

Create a logon for someone else

Username *

Required

Name *

Required

Email *

Required

Confirm email

Access role

Read Only

▼

 User access enables read-only access to all services

Cancel

[<](#) Previous

Next [>](#)

Access Role needs to be set to "Full", so they can request new Client Certificates or renew Client Certificates.

3. Obtaining and Managing Client Certificates

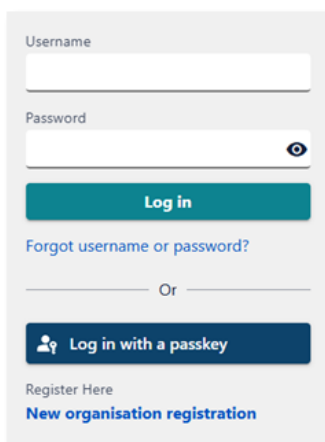
Requesting a new Client Certificate:

Step 1 – log in

Log in to the Developer Portal.

Important: You must have a “full access” role to manage credentials in the Developer Portal.

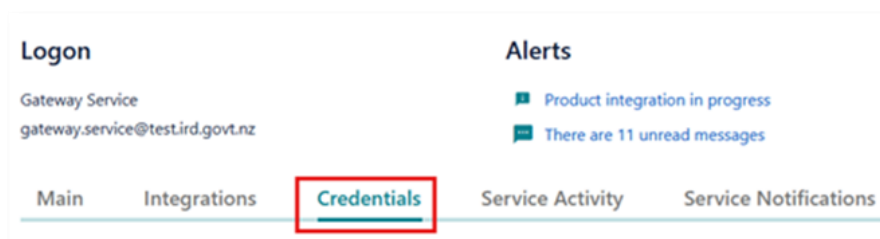
If you do not currently have a Developer Portal user account, please reach out to gatewayServices@ird.govt.nz for further instructions.

A login form for the Developer Portal. It features a 'Username' field, a 'Password' field with a toggle for visibility, a teal 'Log in' button, a link for 'Forgot username or password?', an 'Or' separator, a dark blue button for 'Log in with a passkey', a 'Register Here' link, and a link for 'New organisation registration'.

Step 2 – select credential

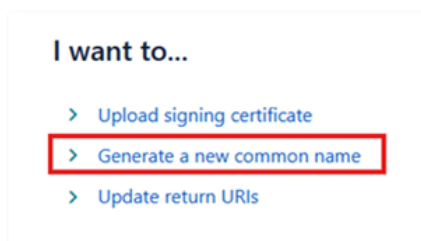
Please note, IR assigns credentials after the Developer Portal registration is complete, so there may be a delay before you can move ahead with this step.

Navigate to the **Credentials** tab and select an existing credential for Test or Prod.

A screenshot of the Developer Portal dashboard. The 'Logon' section shows 'Gateway Service' and the email 'gateway.service@test.ird.govt.nz'. The 'Alerts' section shows 'Product integration in progress' and 'There are 11 unread messages'. The navigation bar at the bottom includes 'Main', 'Integrations', 'Credentials' (highlighted with a red box), 'Service Activity', and 'Service Notifications'.

Step 3 – generate a new common name

Navigate to the 'I want to...' menu and select **Generate a new common name**



I want to...

- > Upload signing certificate
- > **Generate a new common name**
- > Update return URIs

Step 4 – edit name and reference fields

By default, the **Name** field uses the first eight characters of your company name, and the **Reference** field is set to "client". These fields are editable and form part of the Common Name.

Certificate Request

Name

Reference

Description



- The 'Name' field is auto filled with the first eight characters of your organisation's name.
- The optional 'Reference' and 'Description' fields may be used to provide additional identifying information.
- Both the 'Name' and 'Reference' fields (maximum of eight characters) are customisable and form part of the Common Name.

Step 5 – edit the Organization Name, Organization Unit and Country

Additional details like **Organization Name**, **Organization Unit** and **Country** can be added which forms part of the OpenSSL command. This will appear in the Client Certificate.

Copy and store the OpenSSL command to generate a private key and the Certificate Signing Request (CSR) file. Generate the CSR file by running the OpenSSL command in any supported CSR tool. This CSR file will be uploaded in step 8.

Then click **Submit** to proceed.

Important: Keep the private key secure.

Open SSL

Organization Name

Organization Unit

Country

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"
```

Step 6 – confirmation

Select **Close** on the confirmation screen to continue.

Confirmation

 You have successfully submitted: **Generate Common Name**

Name

Customer Identifier **1-512-115-948**

Date received **29-Jan-2026 13:30:43**

Submitted by logon

Confirmation number **0-019-482-240**

Printable copy

Close

Step 7 – upload CSR

From the Certificate Requests table, select the **Upload CSR** for the available Common Names.

Certificate Requests

Show History 

Common Name	Description	Created	Status
		29-Jan-2026	Upload CSR

Step 8 – validate CSR

Select **Choose file** to upload the CSR generated with the provided OpenSSL command or another supported CSR tool and select **Submit**.

Upload a file to continue

Upload Certificate Signing Request file *

Required

Choose file

Step 9 – approval and download

The Gateway Services Team reviews and approves the new Client Certificate request.

Once processed you will receive an automated email confirming the new Client Certificate is ready for download.

Download the new Client Certificate in either a PEM or DER file encoded format. Both formats include a full certificate chain.

Choose Export Format

PEM

Exports the certificate in PEM base64 string format with the ".pem" extension.

DER

Exports the certificate in DER binary format with the ".cer" extension.

4. Certificate Chain and Security

Inland Revenue runs a Private PKI, meaning certificates are not signed by external Certificate Authorities.

IR will operate separate certificate chains for production and non-production environments.

5. PFX Certificate

The Developer Portal does not generate PFX (PKCS#12) files directly. Digital service providers must create their own PFX files using a command line tool like OpenSSL.

```
openssl pkcs12 -export -inkey <private.key> -in <fullchain.pem> -out  
<output.pfx>
```

6. Renewing Client Certificates

Renewing the Client Certificates requires uploading a new CSR file. Select the **Renew** link in the Issued Client Certificates table and follow the certificate request process.

The screenshot shows the IR's certificate management portal. At the top, there is a navigation bar with a home icon and a user profile icon. Below the navigation bar, there are three main sections: 'Credential' (with a shield icon and a redacted area), 'Alerts' (with a checkmark icon and the text 'There are no alerts'), and 'I want to...' (with three links: 'Upload signing certificate', 'Generate a new common name', and 'Update return URIs'). Below these sections, there are four tabs: 'Certificates', 'Common Names', 'Return URIs', and 'OAuth Credentials'. The 'Certificates' tab is selected. Under the 'Certificates' tab, there are two sections: 'Certificate Requests' and 'Issued Client Certificates'. The 'Certificate Requests' section shows a table with columns 'Common Name', 'Description', 'Created', and 'Status', and a message 'There are no certificate requests.' The 'Issued Client Certificates' section shows a table with columns 'Common Name', 'Description', 'Issued Date', 'Expired Date', and 'Download'. The first row of the table has a redacted 'Common Name' and 'Description', and 'Issued Date' of '09-Feb-2026' and 'Expired Date' of '09-Feb-2027'. There are 'Download' and 'Renew' links for this certificate. The 'Renew' link is highlighted with a red box.

- Certificates are valid for 1 year and can be renewed any time before expiration.
- Automated email reminders will be sent to the original requestor before the certificate expiry.
- You are required to rotate the CSR and private key for security. The portal will detect duplicate CSR reuse.
- Your certificate renewal request will be processed automatically, and the new client certificate will be available for download immediately.

API Automation Tools

API automation tools are not available for IR's certificate management solution.

Transition and Legacy Support

- Existing certificates issued by trusted CAs will remain valid until the certificate expiry or until **30 September 2026**, whichever comes first.
- Legacy Common Names and public CA certificates will be phased out once all digital service providers (DSPs) and Government Agencies have transitioned.
- IR will only support IR issued client certificates from 1 October 2026.

7. Important note for Apple macOS users

The default version of OpenSSL included with macOS does not generate a CSR that meets the required specifications. This is because macOS uses LibreSSL, a fork of OpenSSL that is not fully compatible.

Although not officially provided by OpenSSL, Homebrew is widely accepted and referenced by OpenSSL maintainers and macOS documentation writers.

Install the official OpenSSL distribution using Homebrew:

1. Install Homebrew (if not already installed):

`https://brew.sh/`

2. Install OpenSSL:

`brew install openssl`

Once installed, use the Homebrew-provided OpenSSL binary located at:

`/opt/homebrew/bin/openssl`

This version should be used instead of the macOS default (LibreSSL) when generating CSRs.

Important:

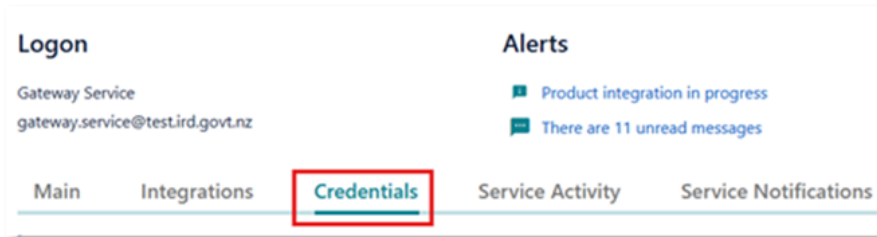
- This installs OpenSSL **alongside** LibreSSL
- It does **not replace** `/usr/bin/openssl`
- You must adjust your PATH or reference it explicitly

8. OAuth Credential Management

To view your OAuth Credential and maintain Return URI.

Step 1 – select credential

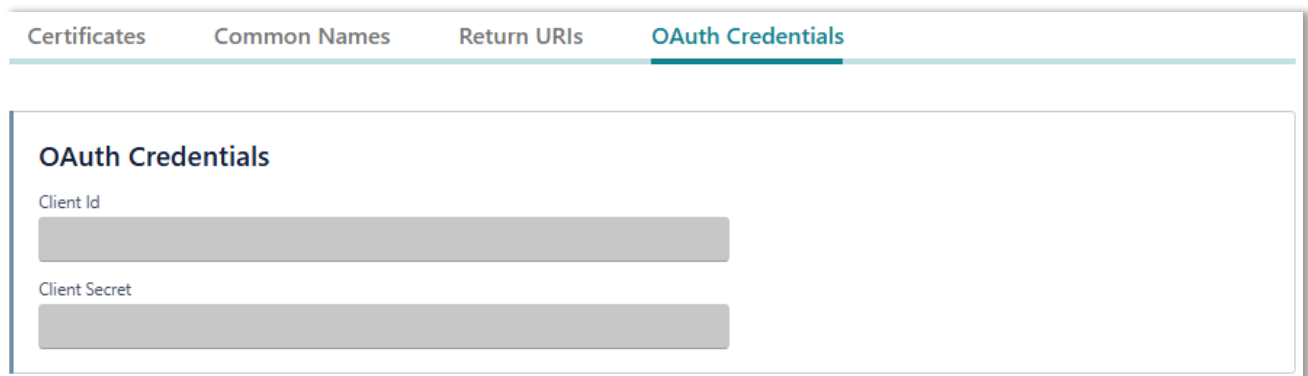
Navigate to the **Credentials** tab and select an existing credential.



Step 2 – select the OAuth Credentials tab.

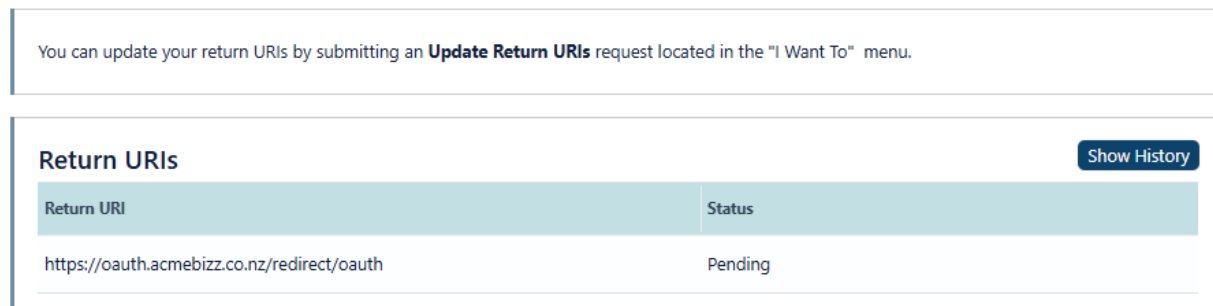
Please note, this step is completed by IR before you can proceed to step 3.

If your Client Id and Client Secret is missing, please raise a support case via the Gateway Customer Support Portal.



Step 3 – select the Return URIs tab.

View current Return URIs.



Step 4 – update Return URIs.

To add/update a Return URI, select the **Update return URIs** link from the **I want to... menu** and follow the process.

Please refer to platform provider guidance for the return URIs you have to add.

The screenshot shows a user interface with a dark header bar containing a home icon and a user profile icon. Below the header, there is a navigation bar with a '< Home' link. The main content area is divided into three sections: 'Credential', 'Alerts', and 'I want to...'. The 'Credential' section shows a shield icon, the text 'PIVTEST', 'Acme Bizz', and 'Valid from 01-July-2026'. The 'Alerts' section shows a checkmark icon and the text 'There are no alerts'. The 'I want to...' section contains three links: 'Upload signing certificate', 'Generate a new common name', and 'Update return URIs', which is highlighted with a red box. Below these sections is a horizontal tab bar with four tabs: 'Certificates', 'Common Names', 'Return URIs' (which is selected and highlighted), and 'OAuth Credentials'. Below the tab bar, there is a message box that says 'You can update your return URIs by submitting an **Update Return URIs** request located in the "I Want To" menu.' Below the message box is a section titled 'Return URIs' with a 'Show History' button. This section contains a table with two columns: 'Return URI' and 'Status'. The table has one row with the value 'https://oauth.acmebizz.co.nz/redirect/oauth' in the 'Return URI' column and 'Pending' in the 'Status' column.

< Home

Credential
PIVTEST
Acme Bizz
Valid from 01-July-2026

Alerts
✓ There are no alerts

I want to...
> Upload signing certificate
> Generate a new common name
> **Update return URIs**

Certificates Common Names **Return URIs** OAuth Credentials

You can update your return URIs by submitting an **Update Return URIs** request located in the "I Want To" menu.

Return URIs [Show History](#)

Return URI	Status
https://oauth.acmebizz.co.nz/redirect/oauth	Pending

Press 'Submit' to complete the process and to activate the return URI.

Important Note: There is no requirement to upload a signing certificate.