HealthLink

Part of Clanwilliam

13/06/2025

Browser Enrolment User Guide

Welcome to the Browser Enrolment User Guide. This guide provides step-by-step instructions to help you securely download, install, and manage your digital certificate issued by HealthLink. The enrolment process is designed to ensure that only the authorised user can access and install the certificate, using a combination of email verification and a unique enrolment code sent via SMS. Before you begin, please review the key requirements and important notes to avoid any issues during installation. Following this guide carefully will help ensure a smooth and secure setup of your digital certificate.

Key points

- An EMAIL is sent to the registered user of the certificate.
- A text message containing an enrolment code is sent to the users mobile. Note: To ensure only the intended user receives the certificate this must be the users mobile.
- The enrolment code and the users registered identifier are required to complete the enrolment process. These should be only known by the user.

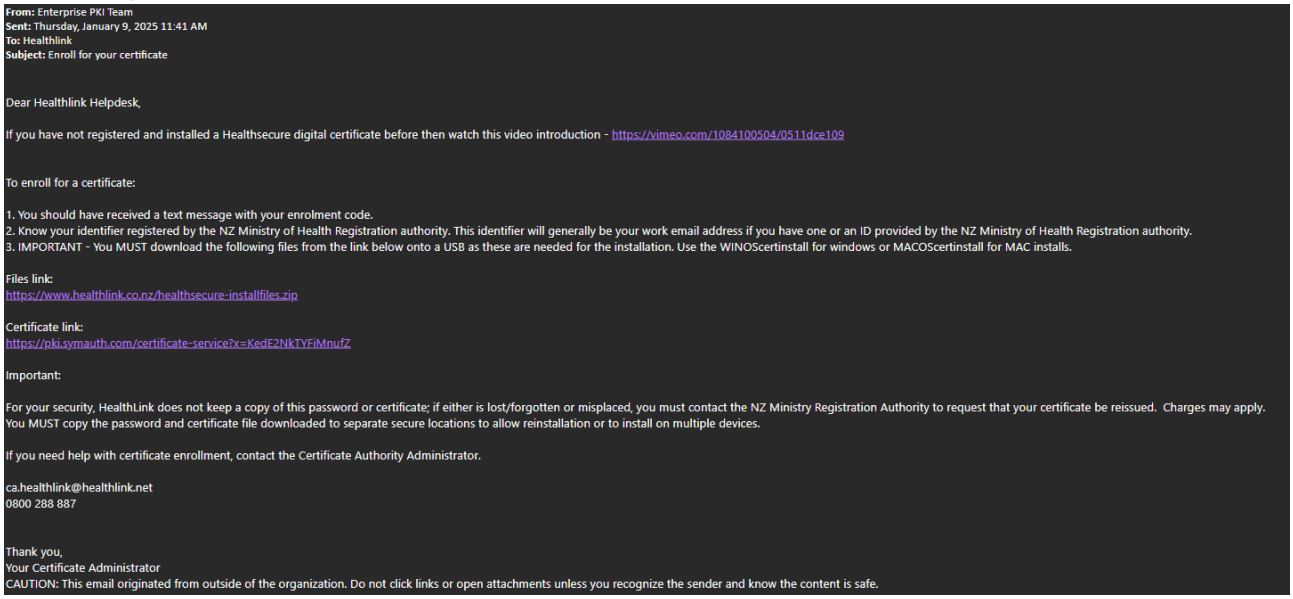
Few things to know before proceeding

- This is a **one-time** download, that cannot be downloaded a second time.
- You must complete the installation in **one sitting**. once you have clicked on “install certificate”, you will not be able to return.
- You must use the email address that is **registered with the HealthSecure application form**.
- Make sure you have **copied** and **saved** your certificate password during the install (HealthLink cannot retrieve your password).
- Certificate will need to be **revoked** and **re-issued** if you have failed to follow these steps.

Download and Install Certificate

The browser enrolment process interface includes a general description of steps to commence the certificate download and then install. The process includes information that uses one browser and operating system as an example so this may not be exactly how you will achieve the same outcome. In general, you should be able to use all the default behaviour of your browser and pc, i.e. double clicking and use default settings.

This quick video guide illustrates this Video User Guides. If you need assistance, please contact helpdesk@healthlink.net or 0800 288 887.



From: Enterprise PKI Team
Sent: Thursday, January 9, 2025 11:41 AM
To: Healthlink
Subject: Enroll for your certificate

Dear Healthlink Helpdesk,

If you have not registered and installed a Healthsecure digital certificate before then watch this video introduction - https://vimeo.com/1084100504/0511dce109

To enroll for a certificate:

1. You should have received a text message with your enrolment code.
2. Know your identifier registered by the NZ Ministry of Health Registration authority. This identifier will generally be your work email address if you have one or an ID provided by the NZ Ministry of Health Registration authority.
3. IMPORTANT - You MUST download the following files from the link below onto a USB as these are needed for the installation. Use the WINOScertinstall for windows or MACOScertinstall for MAC installs.

Files link:
https://www.healthlink.co.nz/healthsecure-installfiles.zip

Certificate link:
https://pki.symauth.com/certificate-service?x=KedE2NkTYFiMnufZ

Important:

For your security, HealthLink does not keep a copy of this password or certificate; if either is lost/forgotten or misplaced, you must contact the NZ Ministry Registration Authority to request that your certificate be reissued. Charges may apply.
You MUST copy the password and certificate file downloaded to separate secure locations to allow reinstallation or to install on multiple devices.

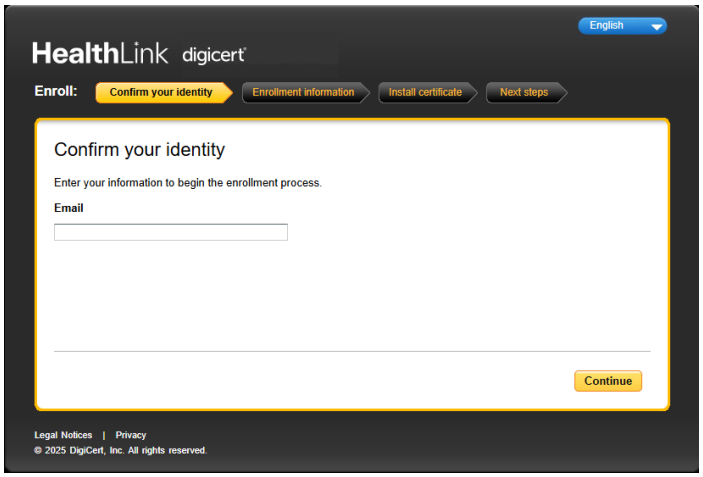
If you need help with certificate enrollment, contact the Certificate Authority Administrator.

ca.healthlink@healthlink.net
0800 288 887

Thank you,
Your Certificate Administrator
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Step 1 - Authorised recipient verification

When the user clicks the emailed Certificate URL they are taken through a process to verify their identity (as the authorised recipient), verify the certificate details are as expected and then download and install the certificate.

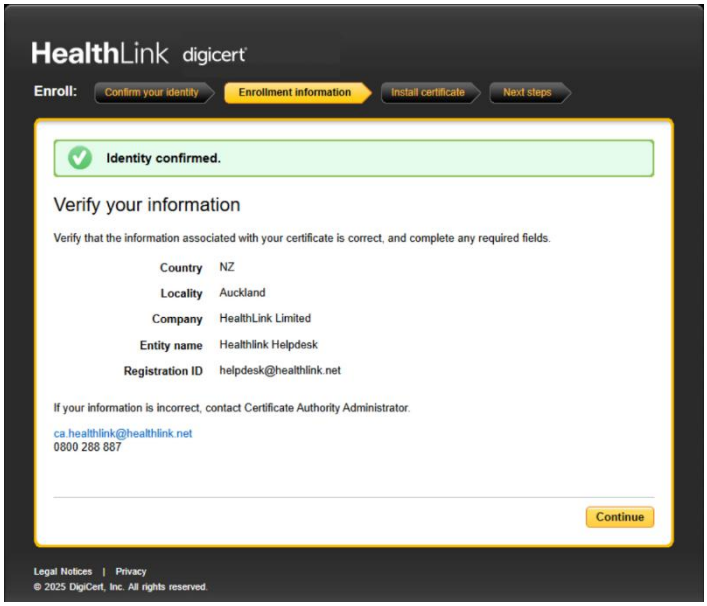


These identifiers are unique identifier for the certificate in the form of an email address and an enrolment code only know by the authorised certificate manager or the user of the certificate.

Refer to the Appendix for wrong email and enrolment code notes

Step 2 - Verify the certificate information is as expected

Once the recipient has entered the correct email and enrolment codes the certificate details are presented to confirm the details registered are still valid or correct.

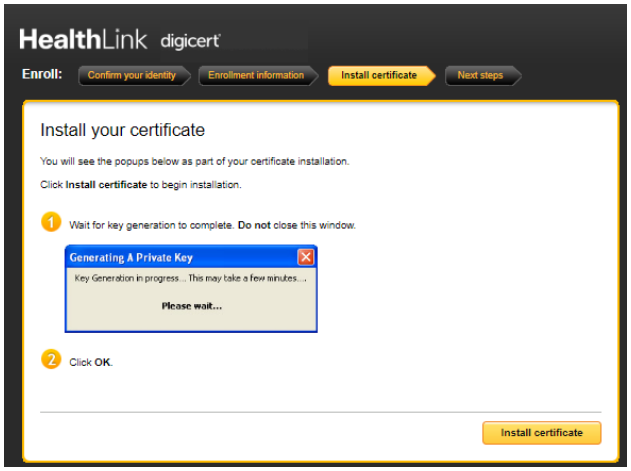


▾ Details are not correct

These are the details provided to the registration authority so if need changing you will have to contact the registration authority to reissue the certificate.

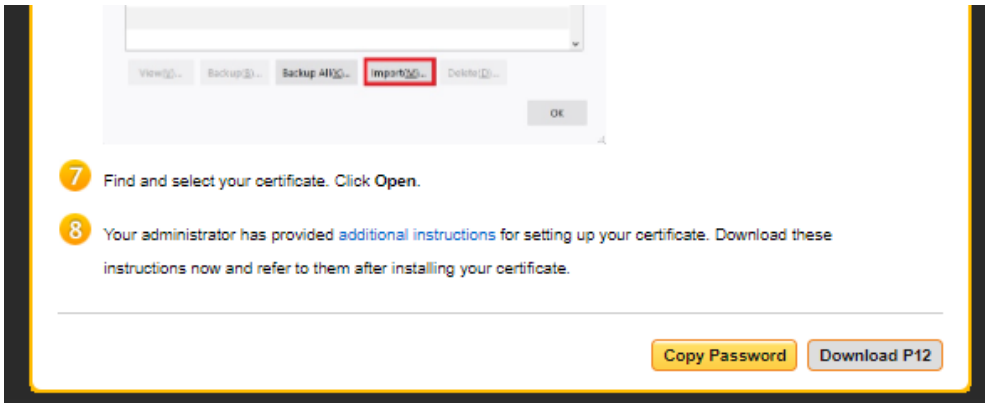
The registration authority contact details can be found here - [Digital Certificates - HealthLink]

Step 3 – Install certificate



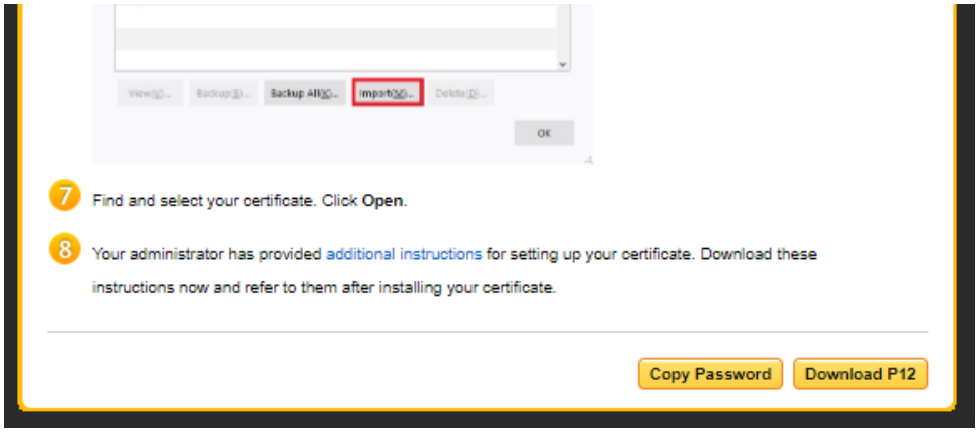
Click install certificate, this will start the download process.

Step 4 – Copy password



Scroll to the bottom of the screen and click copy password, then paste the password somewhere secure so it is not lost.

Step 5 – Download P12



Click Download P12

Your certificate and private key password must be backed up and secured separately.

These cannot be recovered. In the event either are lost and are needed to reinstall the certificate then a new certificate will need to be reissued.

Step 6 - Save password and certificate

Save the password securely for future reference.

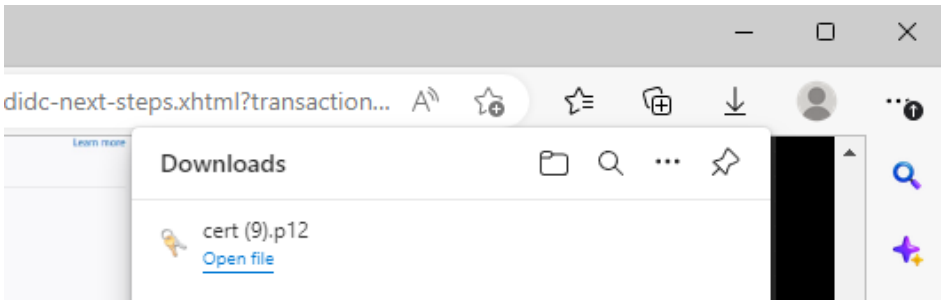
You can paste the password that is in the clipboard (cntrl v) into a secure location.

For example you could use windows sticky notes, an email to yourself or a password manager tool like Google Password Manager.

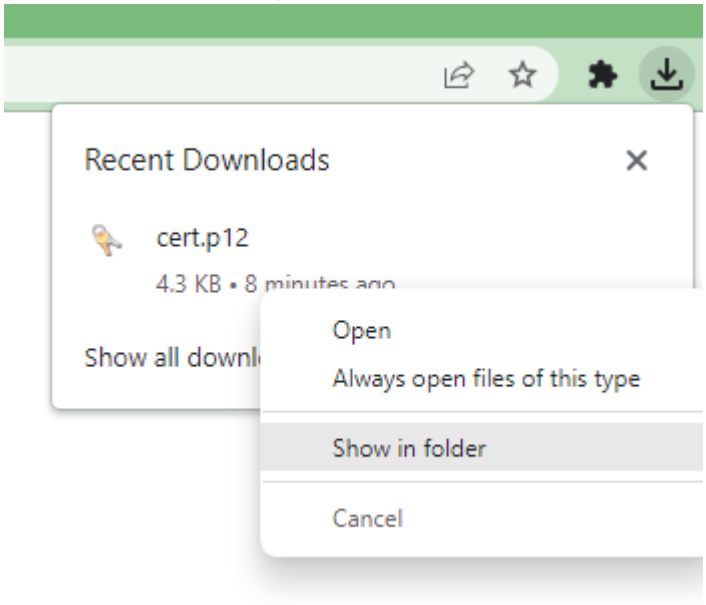
The important note is wherever you save this password it should only be accessible by you and available for reinstalling the certificate.

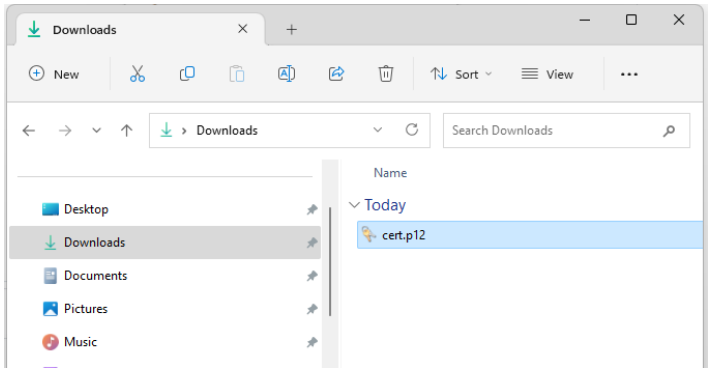
Save the certificate file (cert.p12) for future reference

The certificate is downloaded to the browsers default download location with the file name cert.p12.

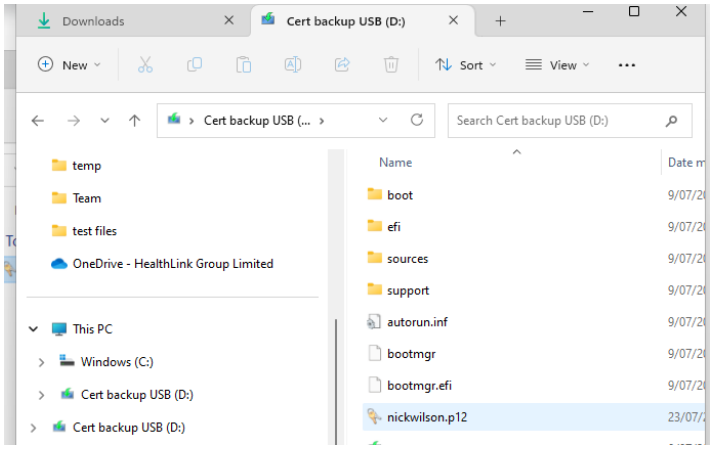


Right click the file and click show in folder or open your file explore and open the downloads folder (usual default location) to find the certificate file,





Rename the file so you can identify specific certificate and then copy from the download folder to a USB or a secure network drive that is accessible by you only for certificate installations.

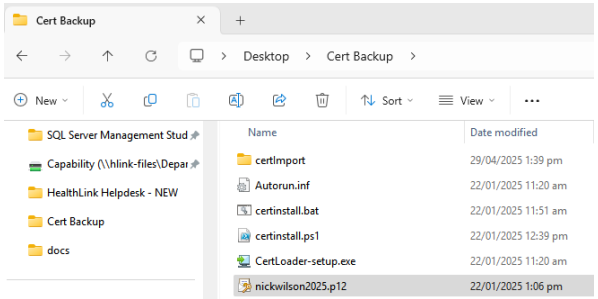


Refer to the appendix for CA Administrator note only - Enrolment status changed now

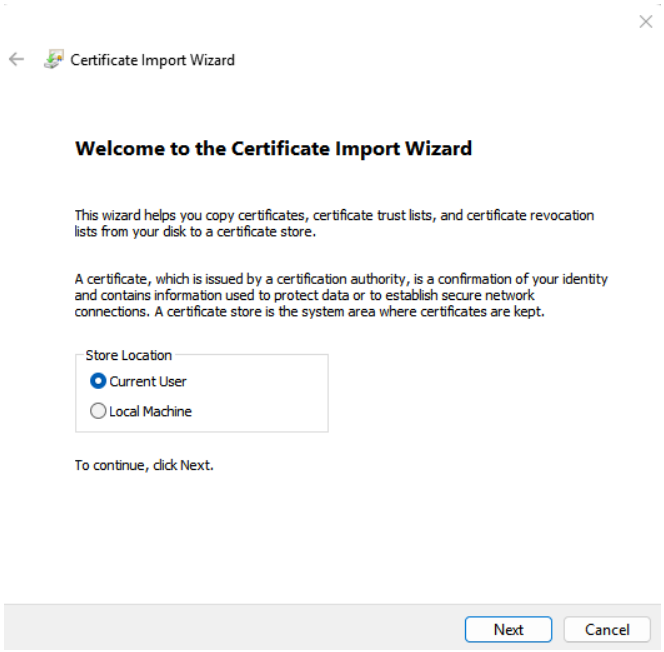
Certificate Install for Browser

You should now have your certificate and certificate password securely saved ready for installation.

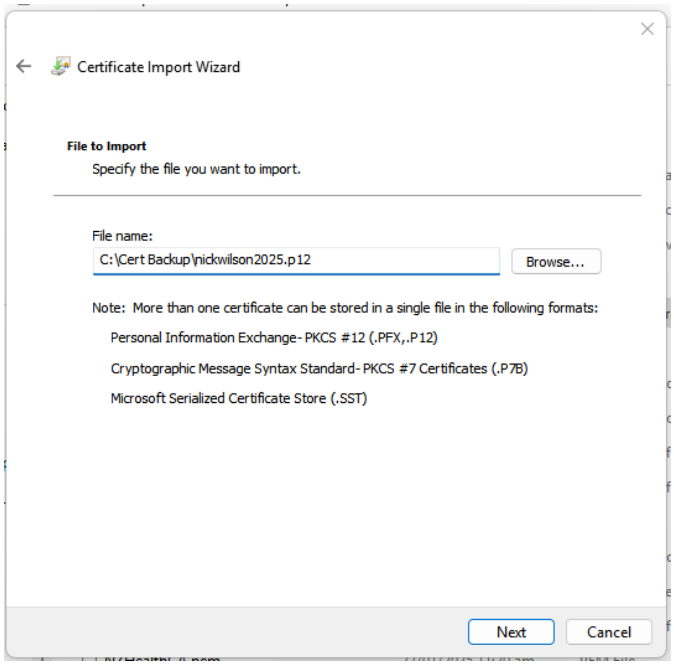
Step 1: Run the .p12 file that was downloaded earlier.



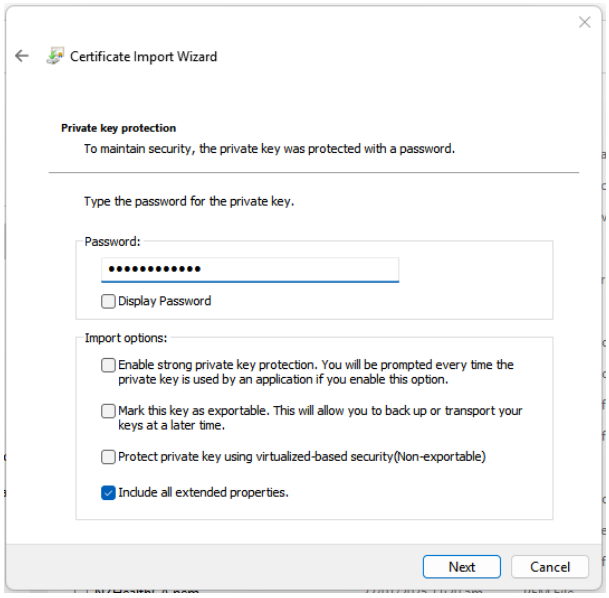
Step 2: Select “Current User” and click Next



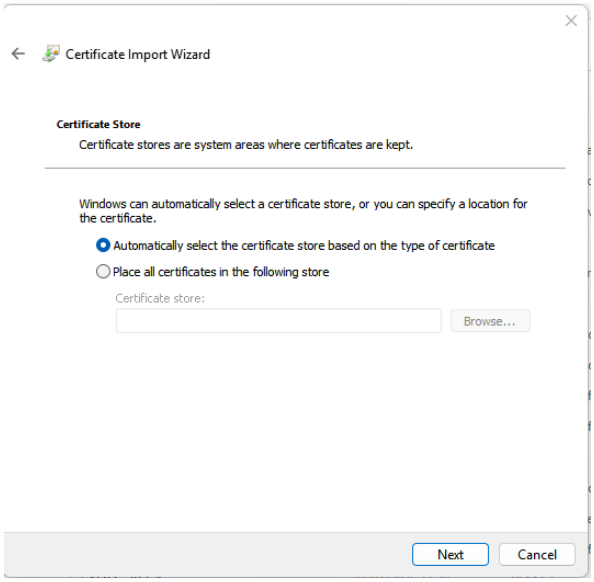
Step 3: Click Next again



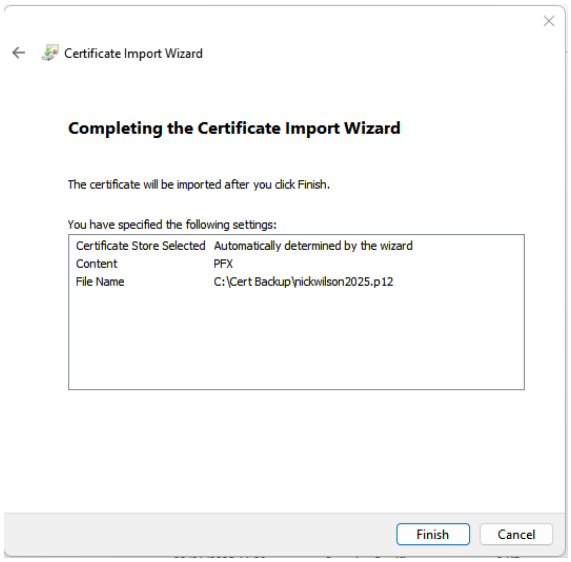
Step 4: Enter the password for the certificate and click next.



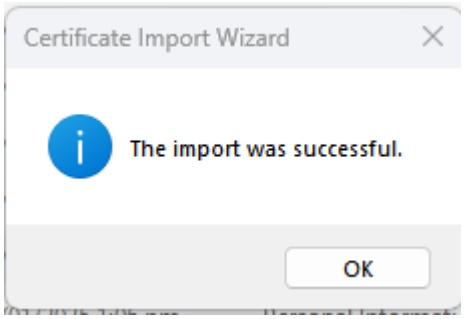
Step 5: Select “Automatically select the certificate store based on the type of certificate” and click next



Step 6: Click Finish



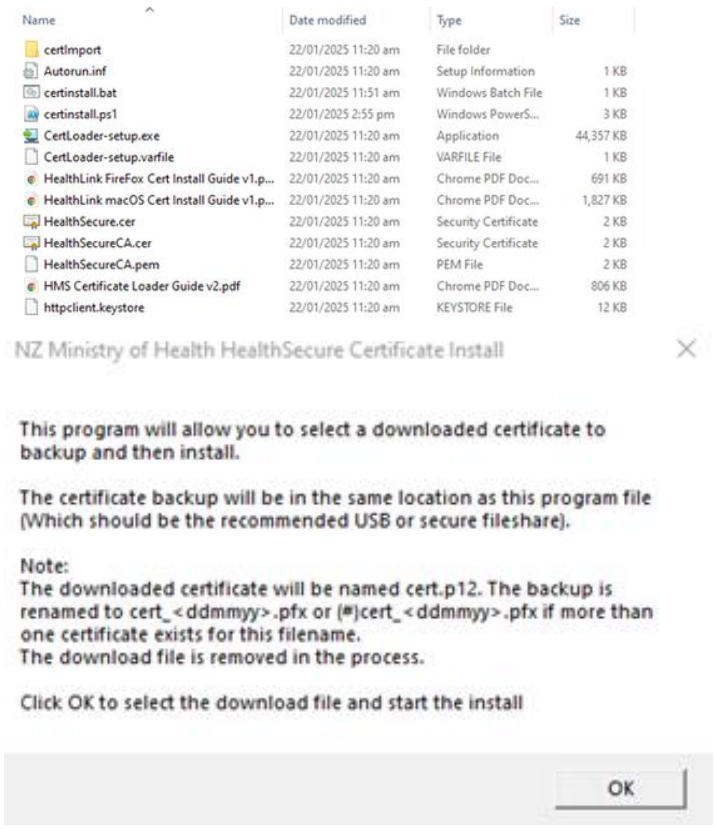
Step 7: Installation complete



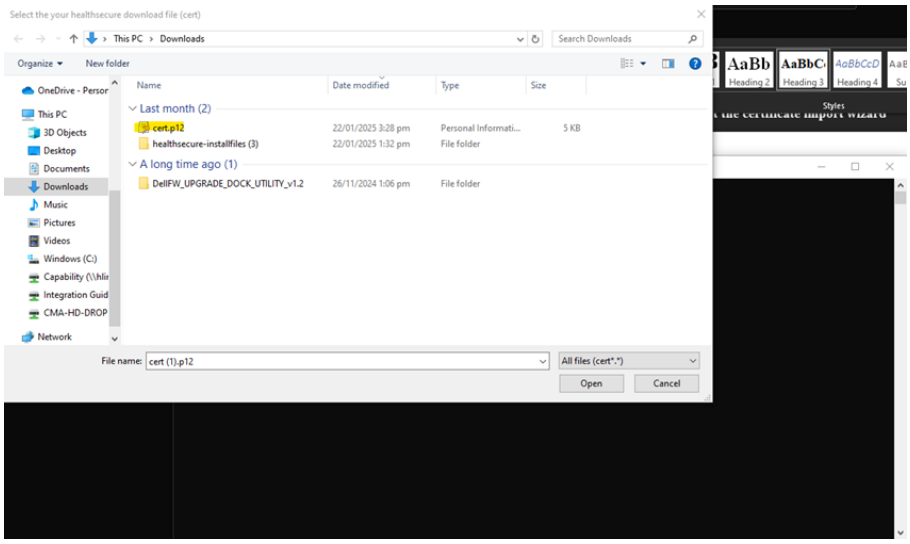
Certificate Install for ESA

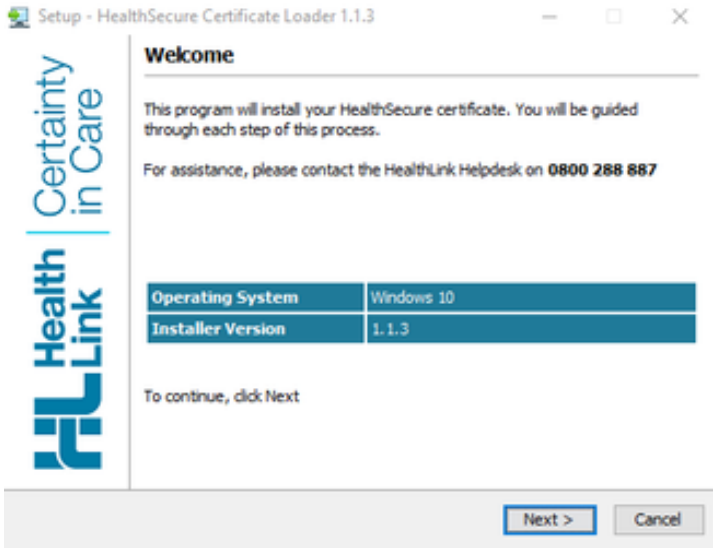
Step 1 - Double click the certinstall.bat to start the installation

Run the certinstall.bat and if that does not work, try the certinstall.ps1 file, and a pop-up will appear. After pressing "OK," you will be prompted to select the certificate, which is "cert.p12" that you have downloaded. It will then be renamed as shown in the image below. Make sure to copy it from the download folder to a USB or a secure network drive accessible only by you for certificate installations.



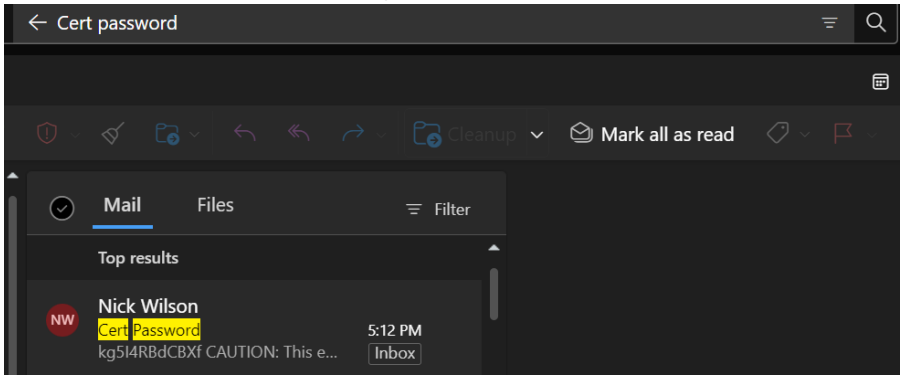
Step 2 - Select the cert.p12 and install it with setup loader (with default values)

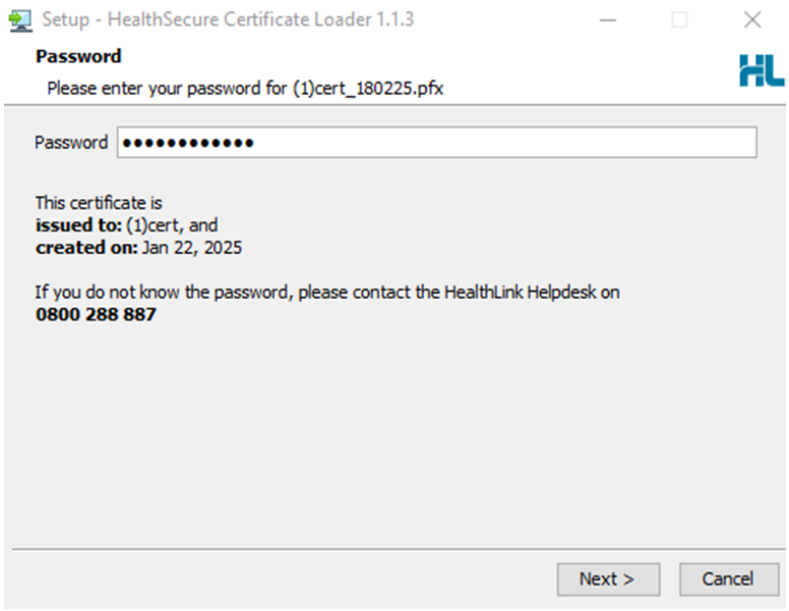




Step 3 - Copy the password from your secure location and click next with default values

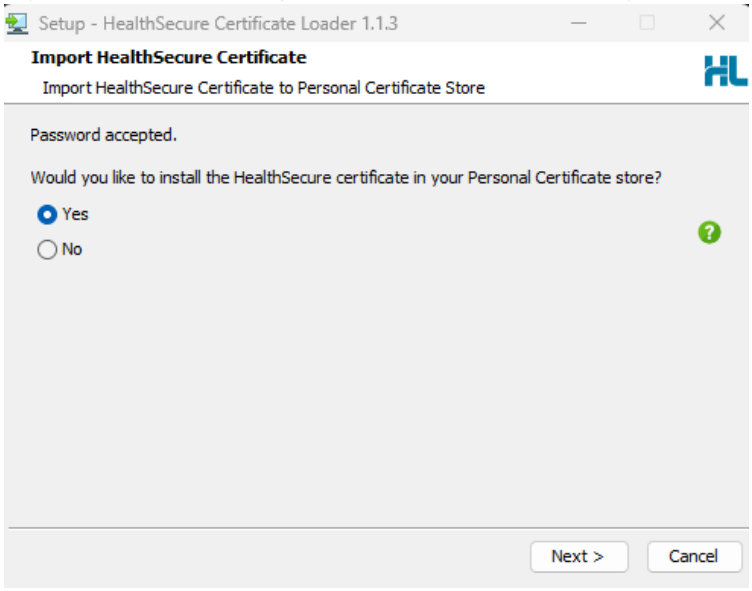
You can use an Email to save your password.

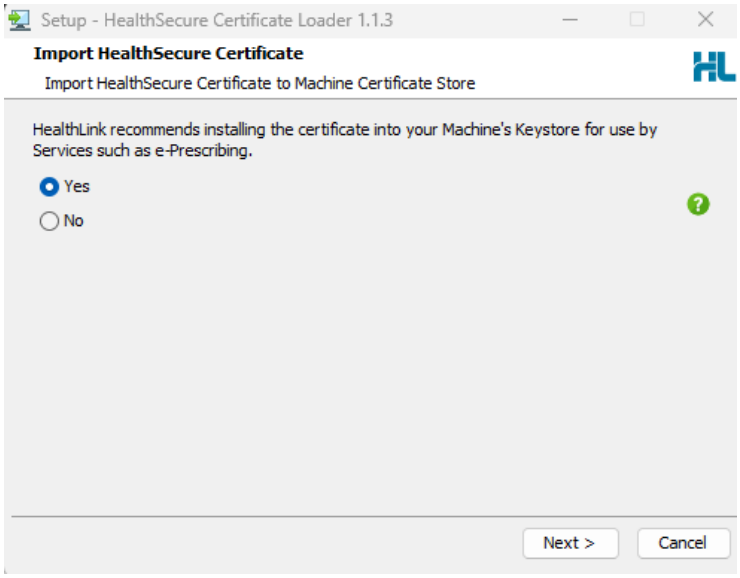


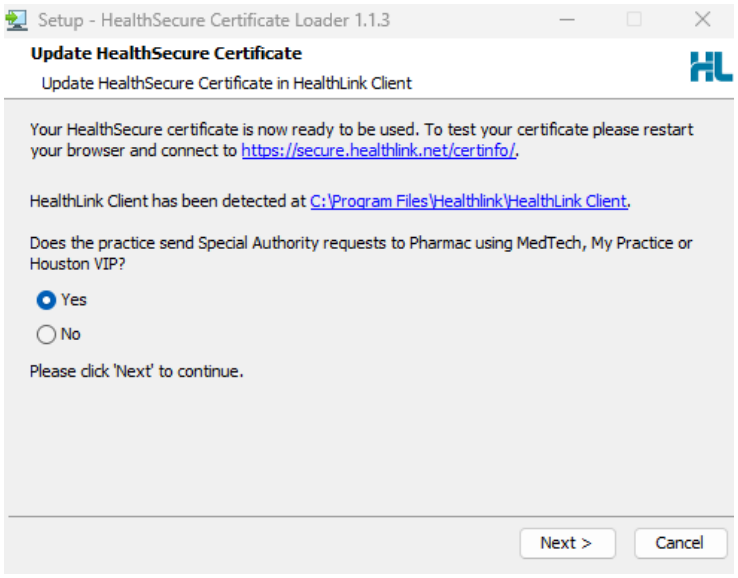


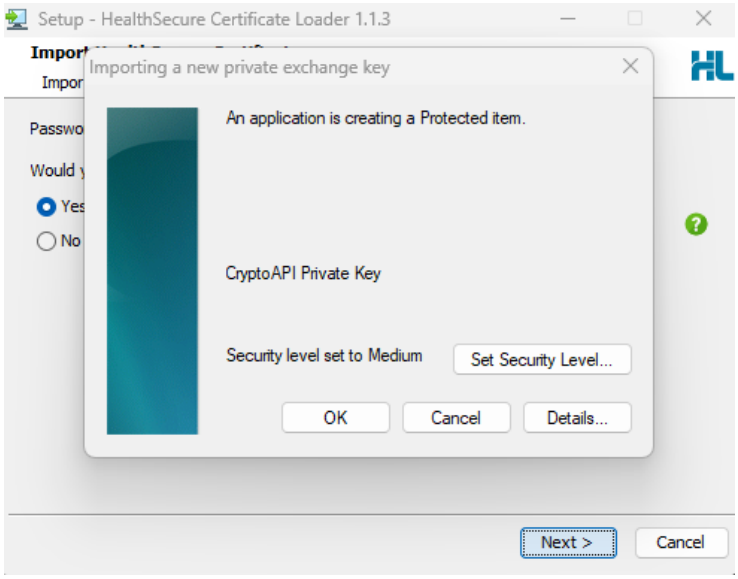
Step 4 - Complete install, clicking next with defaults and finish

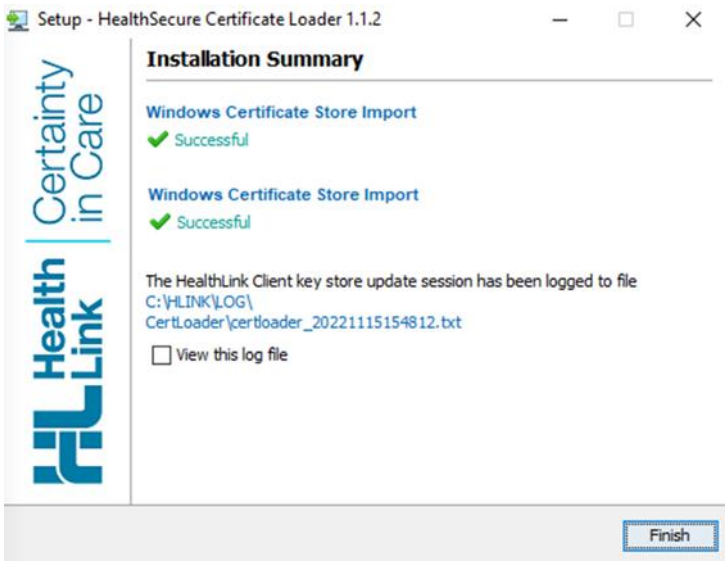
If your practice is using Electronic Special Authority, make sure to tick “Yes”.






Setup - HealthSecure Certificate Loader 1.1.3
Update HealthSecure Certificate
Update HealthSecure Certificate in HealthLink Client
Your HealthSecure certificate is now ready to be used. To test your certificate please restart your browser and connect to https://secure.healthlink.net/certinfo/.
HealthLink Client has been detected at C:\Program Files\Healthlink\HealthLink Client.
Does the practice send Special Authority requests to Pharmac using MedTech, My Practice or Houston VIP?
Yes
No
Please click 'Next' to continue.
Next >
Cancel

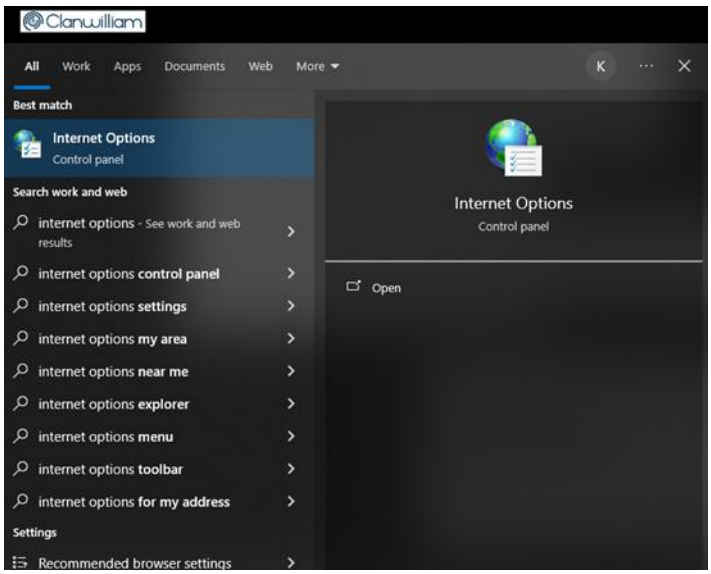

Setup - HealthSecure Certificate Loader 1.1.3
Importing a new private exchange key
An application is creating a Protected item.
CryptoAPI Private Key
Security level set to Medium
Set Security Level...
OK
Cancel
Details...
Next >
Cancel


Setup - HealthSecure Certificate Loader 1.1.2
Installation Summary
Windows Certificate Store Import
Successful
Windows Certificate Store Import
Successful
The HealthLink Client key store update session has been logged to file
C:\HLINK\LOG\
CertLoader\certloader_20221115154812.txt
View this log file
Certainty in Care
Health Link
Finish

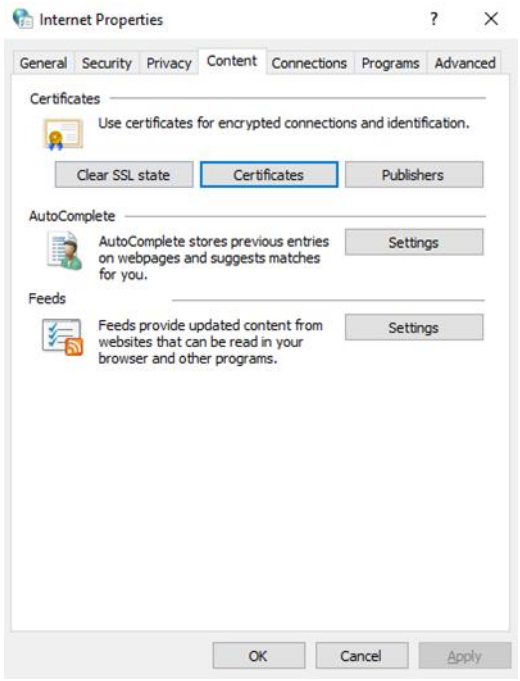
Check installed or existing installed Health Secure Certificates

You can confirm the certificate has been installed or if the device has already had a Healthsecure certificate installed using internet options.

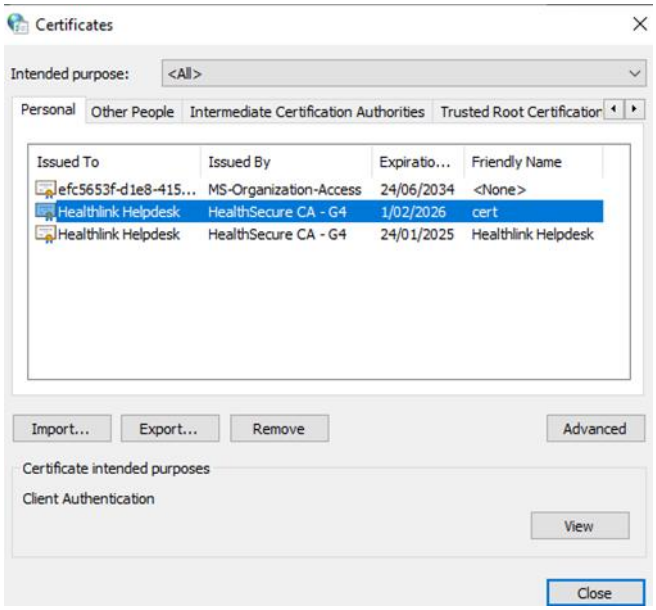
Type in “internet options” in the search bar



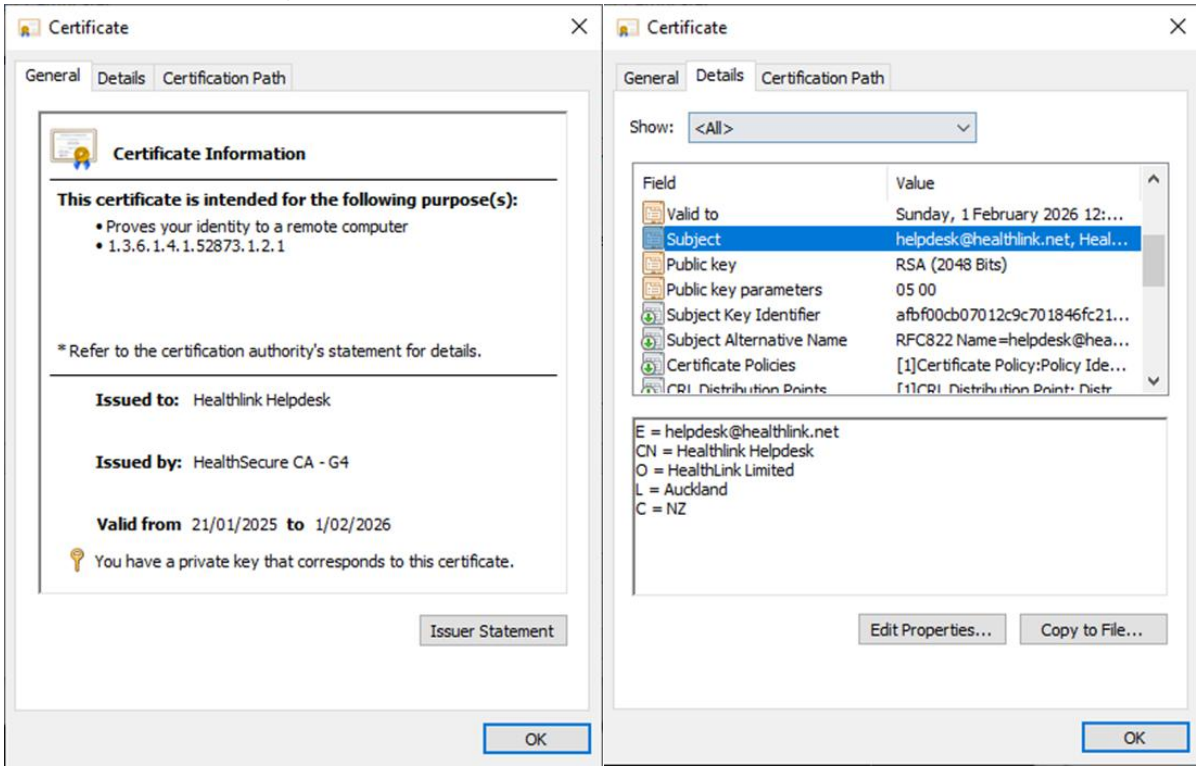
Click on Content > Certificates



Double click your certificate in the personal tab - Friendly name cert



Select Details and Subject. Your details should be shown.



Refer to the appendix for information regarding No root key installed "not enough information" message.

Appendix

User notification messages

Source User notification messages

Enrolment code message

An enrolment code is required to reduce the risk of private certificates being downloaded by anyone other than the intended recipient whose identity has been verified by registration authority. This code is sent separately from the certificate enrolment URL email.

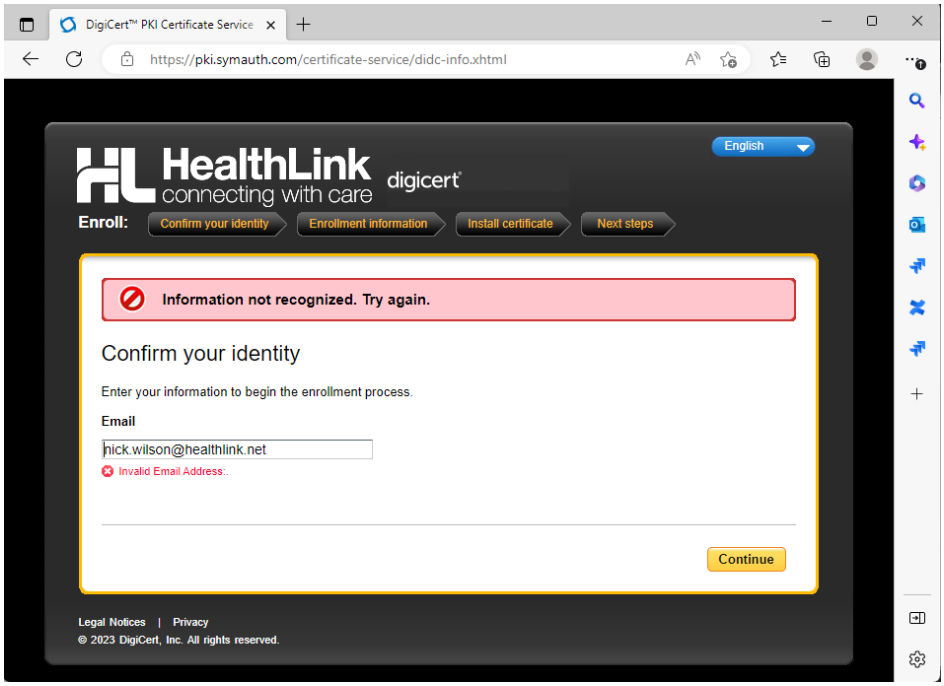
```
Your NZ Ministry of Health Digital Certificate enrolment has been completed and
an enrolment email has been sent to the email address you provided to the NZ MOH
Registration authority. To complete the enrolment process you will need to enter
this code <enter code>.

If you have not received an enrolment email please contact the CA Administrator
on 0800 288 887
```

User guide process exception notes

Wrong email entered

If the user supplies an incorrect email the process cannot continue.

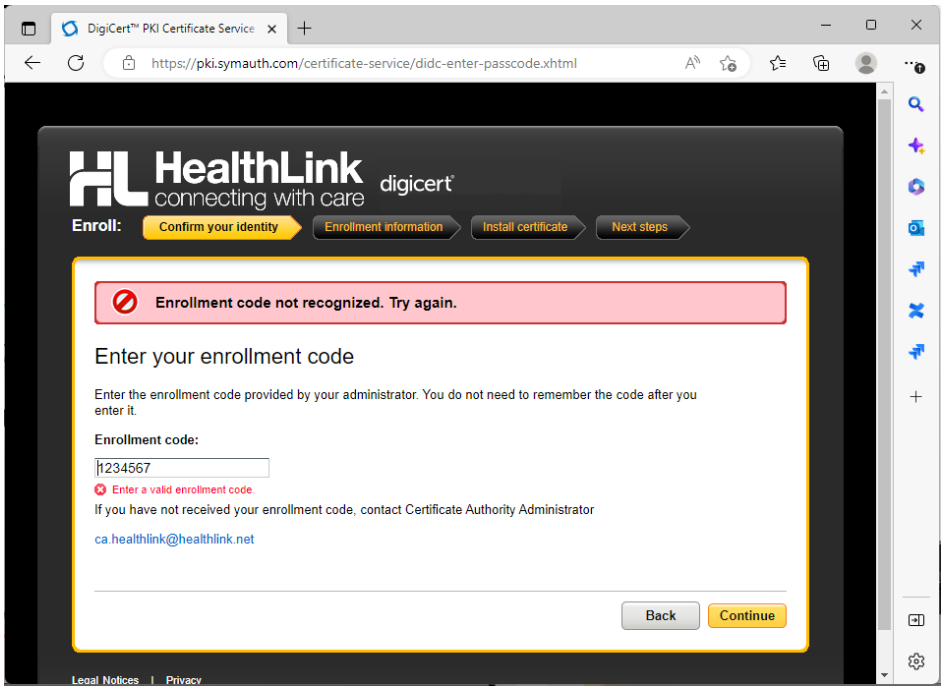
The email is not always the same email address as the one the enrolment URL is sent to. The NZ MOH registration authority would have confirmed this detail during the registration process. If the user does not have this information, then they will have to contact the NZ MOH Registration Authority.



Wrong enrolment code entered

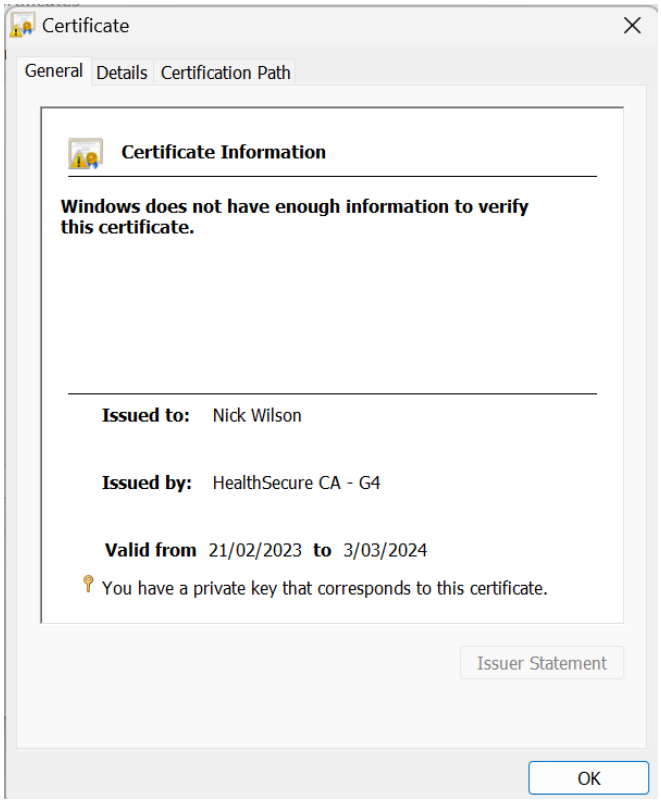
The enrolment code is only available by text. If the user has not received the enrolment code message this can be resent to the registered mobile number. If the mobile number has changed or incorrect at the time of registering with the NZ MOH Registration authority (NZ MOH RA) then they must contact the NZ MOH RA to get the mobile number updated.

The enrolment code can be resent to the approved mobile number.



No root key installed "not enough information" message

The root trust is not required for most web applications, their systems will have the root and will be able to verify the certificate is from the trusted chain. If the application provider requires the root to be installed and trusted on your device then install the root using this installation guide.



HealthLink
0800 288 887

Email
helpdesk@healthlink.net

www.healthlink.co.nz