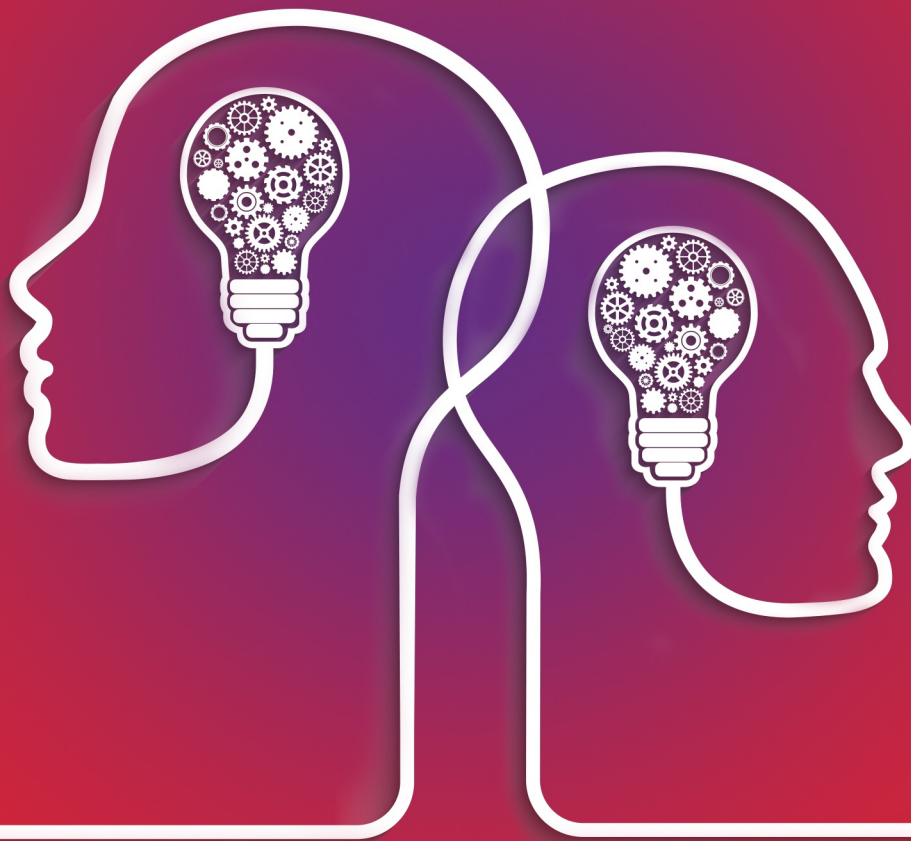
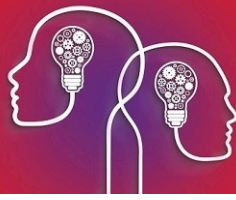


Bp VIP.net

My Health Record Setup Guide



VIP.net knowledge base 



Legal notices

This document is classified as commercial-in-confidence. Unauthorised distribution of this information may constitute a breach of our Code of Conduct, and may infringe our intellectual property rights. This information is collected and managed in accordance with our Privacy Policy, available on our [website](#).

Copyright © 2021

Best Practice Software believe the information in this User Manual is accurate as of its publication date. The information is subject to change without notice.

You may only copy, change, or use the User Manual as required for your own use as permitted under the End User Licence Agreement or the Order Form. User Manuals are intended for reference only and do not preclude the need for training.

Best Practice Software Pty Ltd Best Practice Software New Zealand Ltd
PO Box 1911 PO Box 1459
Bundaberg Queensland Australia Hamilton New Zealand 3240
4670
www.bpssoftware.net

The information contained in the User Manual is intended to be a guide only. Best Practice Software does not provide any warranty in relation to its currency, accuracy, or completeness and, unless otherwise required by law, will not accept any liability in relation to any loss or damage suffered by you or any third party in reliance on the information contained in the User Manual.

Last updated: 13 July 2021



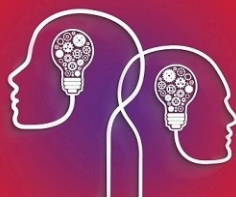
Install a NASH certificate

NASH is the National Authentication Service for Health to enable secure access and the sharing of health information. The new NASH certificate issued by Health Professional Online Services (HPOS) will enable use of both the Online Provider Directory and My Health Records in Bp VIP.net.

Set up PRODA and obtain your NASH certificate

Run through the following tasks to obtain your NASH certificate and passphrase. Your practice may already have performed some of the steps.

	Action	Resource
1.	Register with PRODA (Provider Digital Access) and obtain your PRODA account login Username and Password.	Services Australia (PRODA)
2.	Obtain your HPI-O number through HPOS.	Services Australia (HPI-O)
3.	Obtain a NASH PKI Certificate through HPOS. An example success message from Online Services is shown below.	Services Australia (NASH)
4.	The passcode for your NASH PKI certificate will be sent via SMS to phone of the applicant registered in step 3. You will need this passcode when installing the NASH certificate.	Sent by SMS
5.	Copy the digital NASH PKI certificate to the Bp VIP.net server.	
6.	Install Medicare Online for Bp VIP.net.	Set up Medicare Online Claiming
7.	Download the following certificates from Verizon Certificates Australia > Quick Links > Medicare Australia PKI: <ul style="list-style-type: none">■ Sha1 Root CA Certificate■ Sha1 OCA Certificate■ Sha2 Root CA Certificate■ Sha2 OCA Certificate Sha1 certificates will become deprecated for use as Medicare PKI certificates in the future.	Verizon Certificates Australia
8.	Copy all certificates from step 7 to the Bp VIP.net server.	
9.	Create a Group policy for the certificates so that all users within your domain can access the certificates for My Health Record. Your IT service provider can assist.	Microsoft Knowledge Base



Health Professional
Online Services

Organisation snapshot

Success: Your request has been successful and the details have been updated.

The details for this organisation are displayed below.
To make updates, amend the information and select 'Submit'.
For details of your network, select [Network map](#).

Summary | **Services** | **Names** | **Contacts** | **Addresses** | **ELS** | **OMR** | **HPI-I Links** | **HPD** | **CSP Links** | **Certificates**

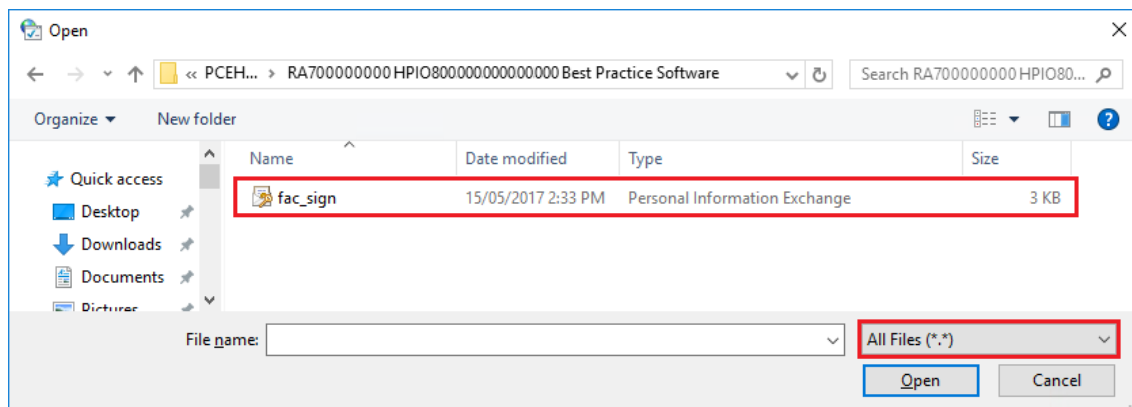
Certificate details

Certificate Type	Distinguished Name	RA Number	Certificate Expiry Date	Status	Action
NASH	CN=general.80036XXXXXXXXXXXXXXXXXXXXX changed_dc=XXXXXXXXXXXXXXXXXXXXX	0000000000	01/05/2021	Active	Download Revoke

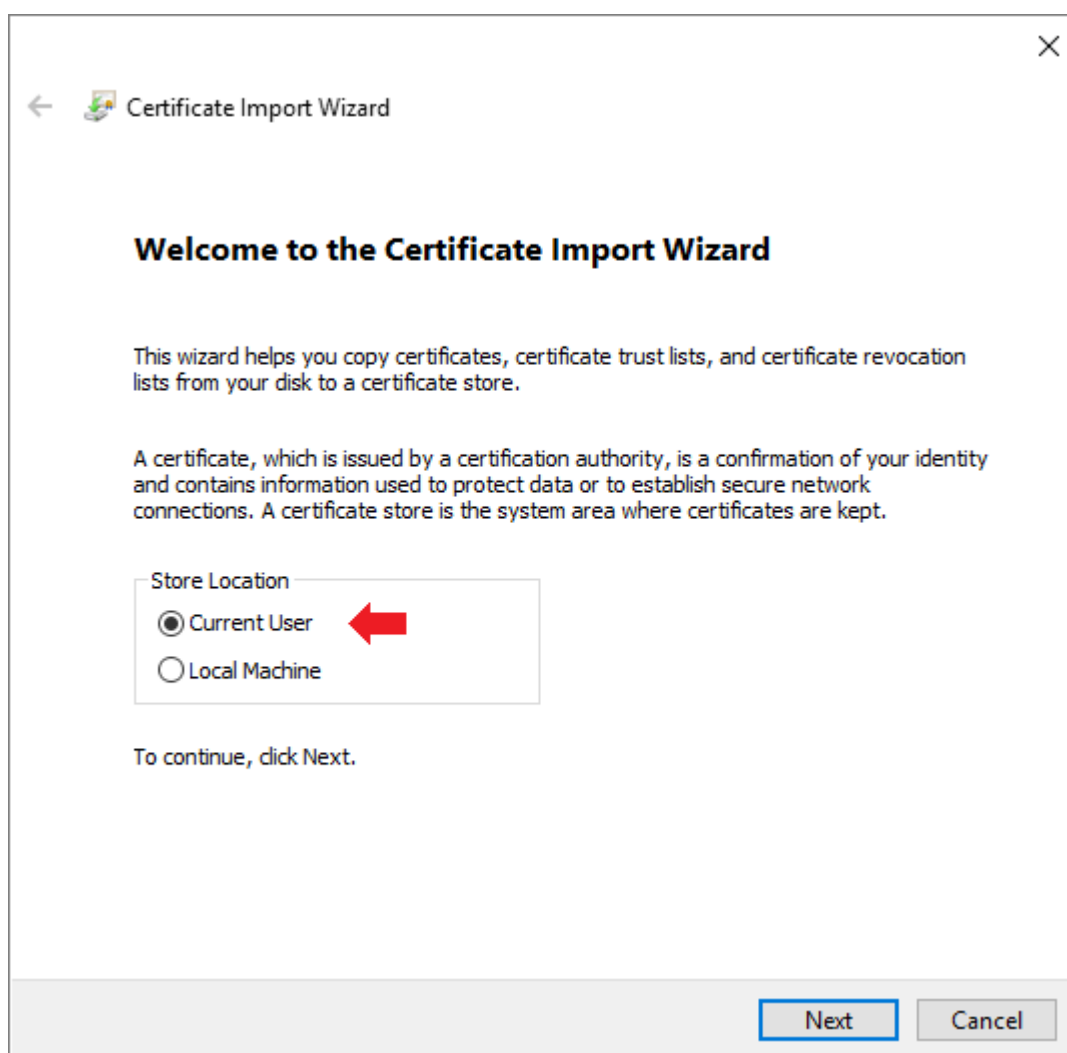
[Cancel](#)

Install the NASH certificate

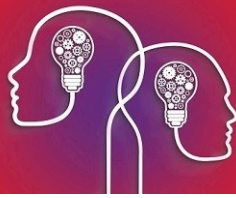
1. In a Windows File Explorer, browse to the downloaded NASH certificate.



2. Double click the **fac_sign** file to open it. The **Certificate Import Wizard** screen is displayed.
3. Change the **Store Location** to **Current User**.



4. Click **Next**. The **File name** displays the fac_sign certificate.



← Certificate Import Wizard

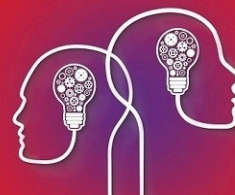
File to Import
Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX,.P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

5. Click **Next** on **Certificate Import Wizard**.
6. Enter your PIC passphrase you received by SMS.



← Certificate Import Wizard

Private key protection
To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☐ Display Password

Import options:

☐ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

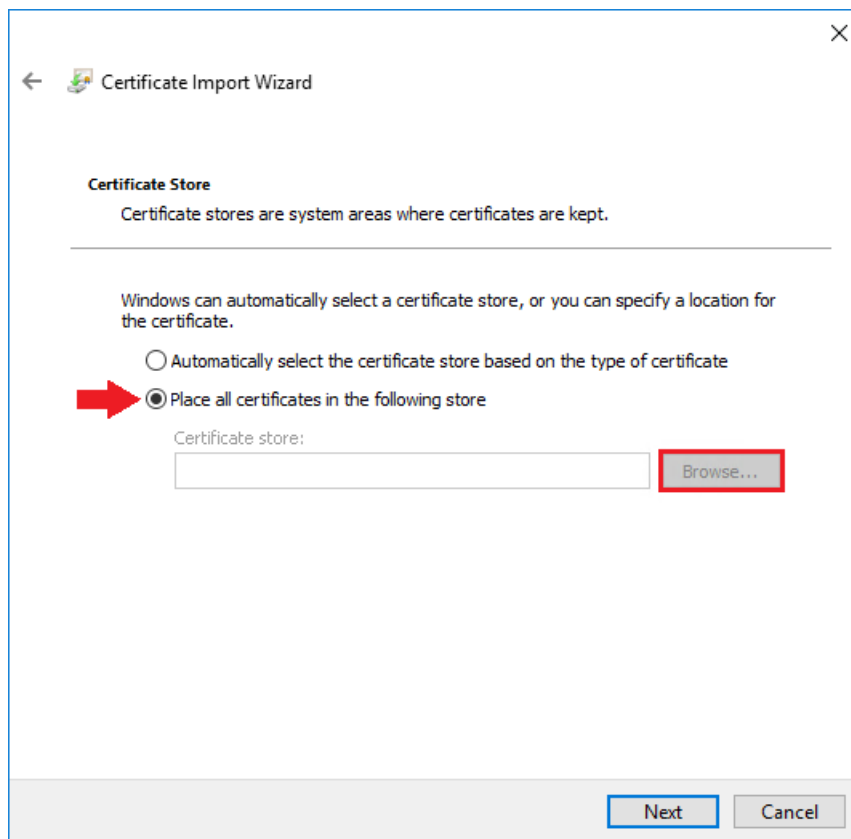
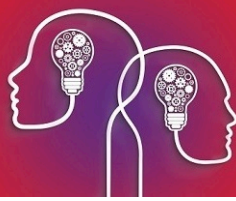
☒ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

☒ Include all extended properties.

Next Cancel

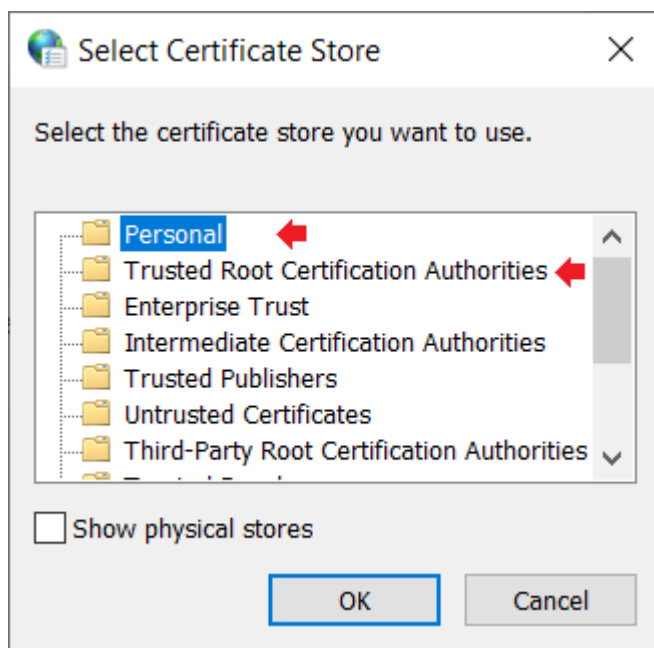
***Tip:** You can select **Mark this key...** as exportable but this is optional.*

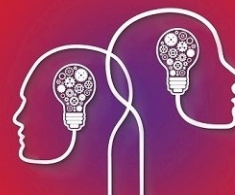
7. Click **Next**.



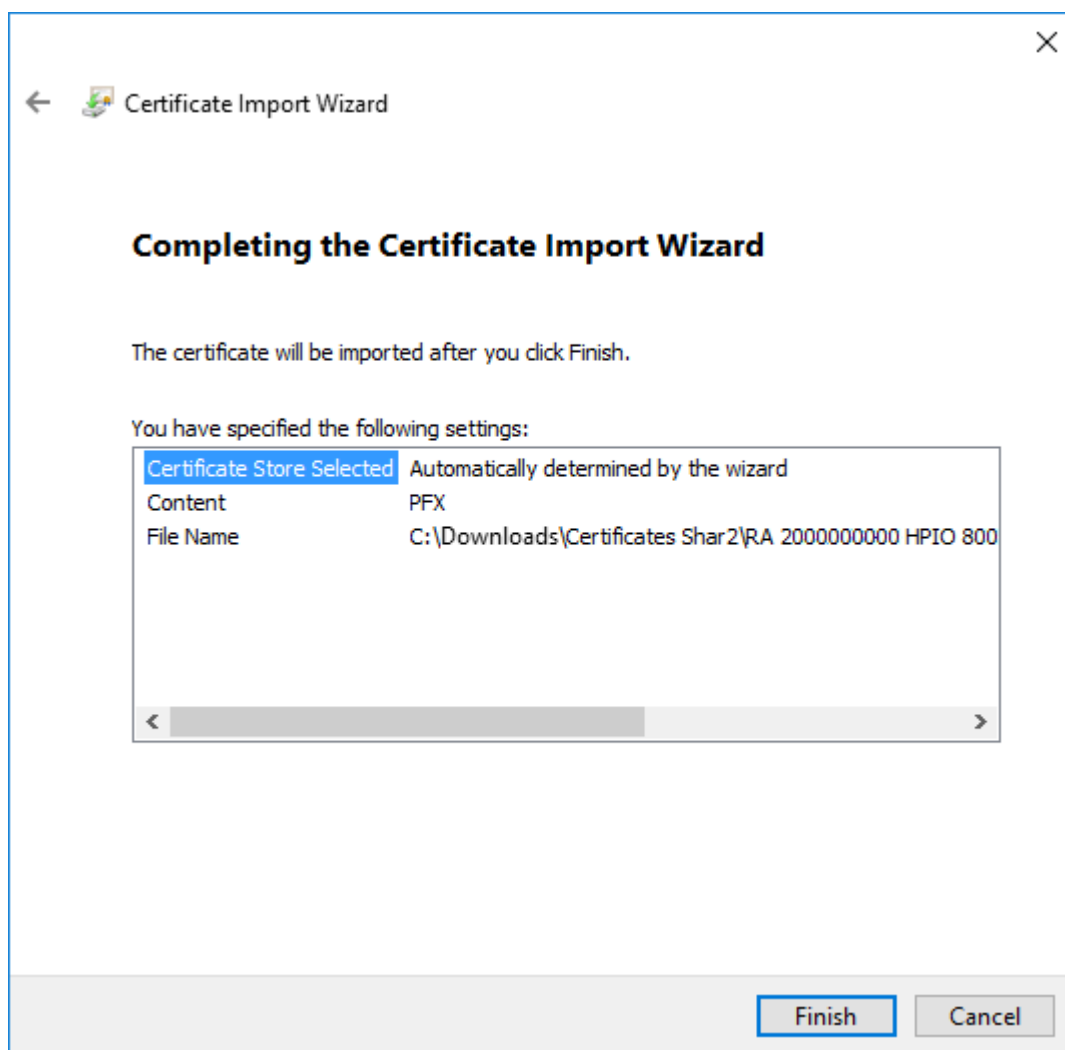
8. Select **Place all certificates in the following store** and click the **Browse** button.

The **Select Certificate** screen is displayed.

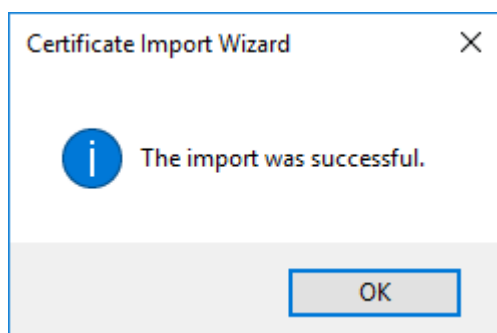




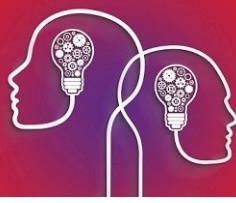
9. Select **Personal** and click **OK**.
10. Click **Finish** to complete the certificate import.



11. Click **OK** on the import success notification.



12. Repeat steps **1 - 7** and select the **Trusted Root Certificate Authorities** certificate store.
13. Repeat steps **10 - 12** to complete the certificate import.



Import the OCA and Root CA Certificates

The OCA and Root CA certificates must be installed with the NASH certificate to form the chain of trust for the NASH certificate to validate. You can follow the instructions for [Installing the Nash certificate](#) to install these certificates; the only difference will be the **Certificate Store** selected in Step 8.

1. Browse to and double-click the **OCA certificate Sha1** certificate file. Select either **Current User** or **Local Machine** (requires administration rights).
2. Import the certificate into Certificate Manager as you did the NASH certificate. However, at step 8, select to import into the **Intermediate Certification Authorities** store.
3. Browse to and double-click the **OCA certificate Sha21** certificate file. Select either **Current User** or **Local Machine**.
4. Import the certificate into Certificate Manager as you did the Sha1 certificate. At step 8, select to import into the **Intermediate Certification Authorities** store.
5. Browse to and double-click the **Root CA certificate Sha1** certificate file. Select either **Current User** or **Local Machine**.
6. Import the certificate into Certificate Manager as you did the OCA certificates. However, at step 8, select to import into the **Trusted Root Certification Authorities** store.
7. Browse to and double-click the **Root CA certificate Sha2** certificate file. Select either **Current User** or **Local Machine**.
8. Import the certificate into Certificate Manager as you did the Sha1 certificate. At step 8, select to import into the **Trusted Root Certification Authorities** store.

Certificate import is complete.

Important: Because the NASH, OCA, and Root CA certificates have only been installed under one user, speak to your IT to create a Group policy for the certificates so that all users within your domain can access the certificates for My Health Record to view and upload records.



Troubleshoot NASH certificate installation

When running HI Provider Directory or accessing My Health Record from Bp VIP.net, you may receive one of the following errors:

- An error occurred attempting to connect to the HI service. No certificate was found with serial number 'nnnnnn'.
- An error occurred attempting to connect to the HI service. Keyset does not exist.
- Unable to access a PCEHR for this patient. Could not establish secure channel for SSL/TLS with Authority Error.
- Unable to access My Health Record for this patient. Certificate was not found with criteria 'xxxxxx'.

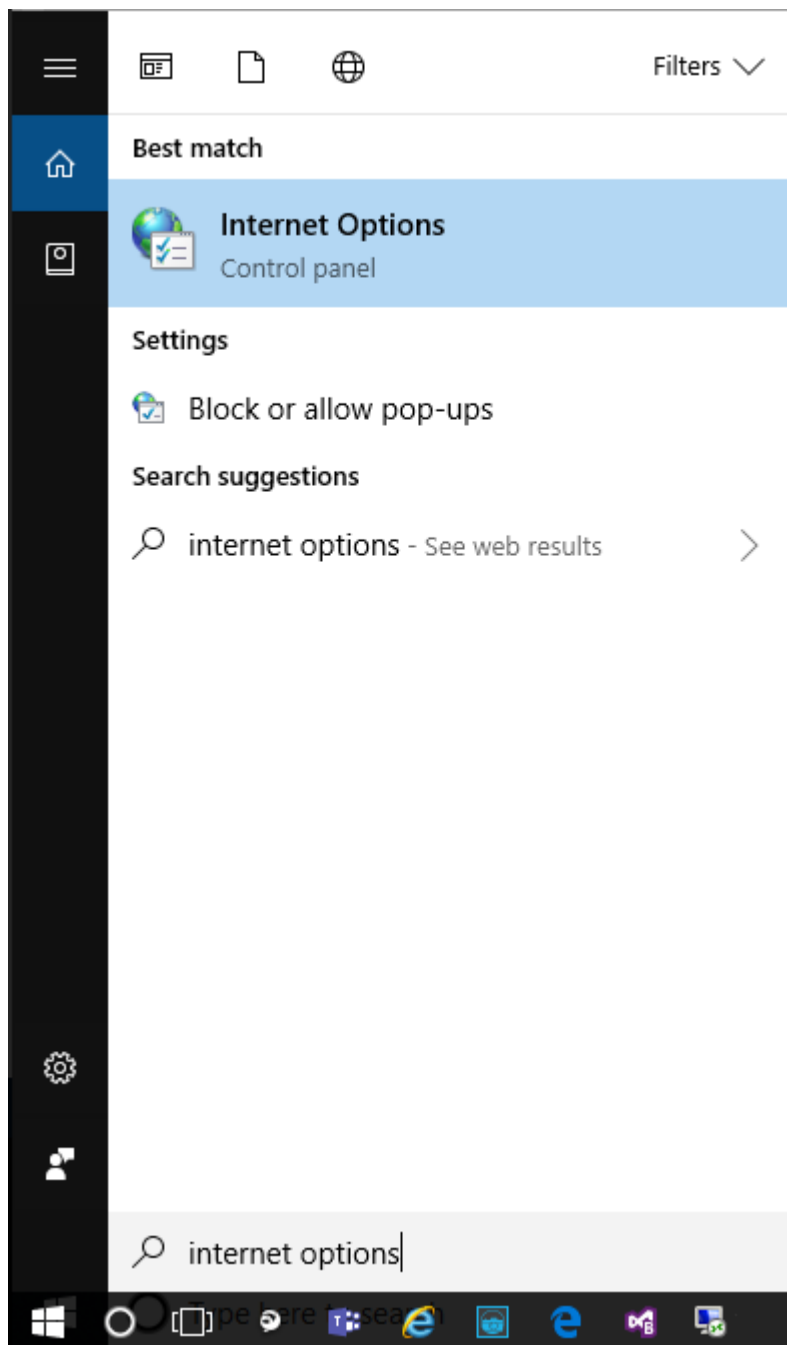
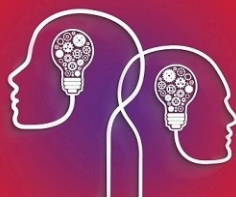
These errors are caused by the NASH certificate not being imported correctly, or Windows not trusting a PKI certificate because the Medicare certificate did not install.

For most Bp VIP.net installations, NASH certificates are only installed on the server computer. When Bp VIP.net is started on a client computer, the client will pull any updated certificates from the server and install them in the client's Windows certificate store. You may still need to do individual installations of the NASH certificate for Thick Client set ups.

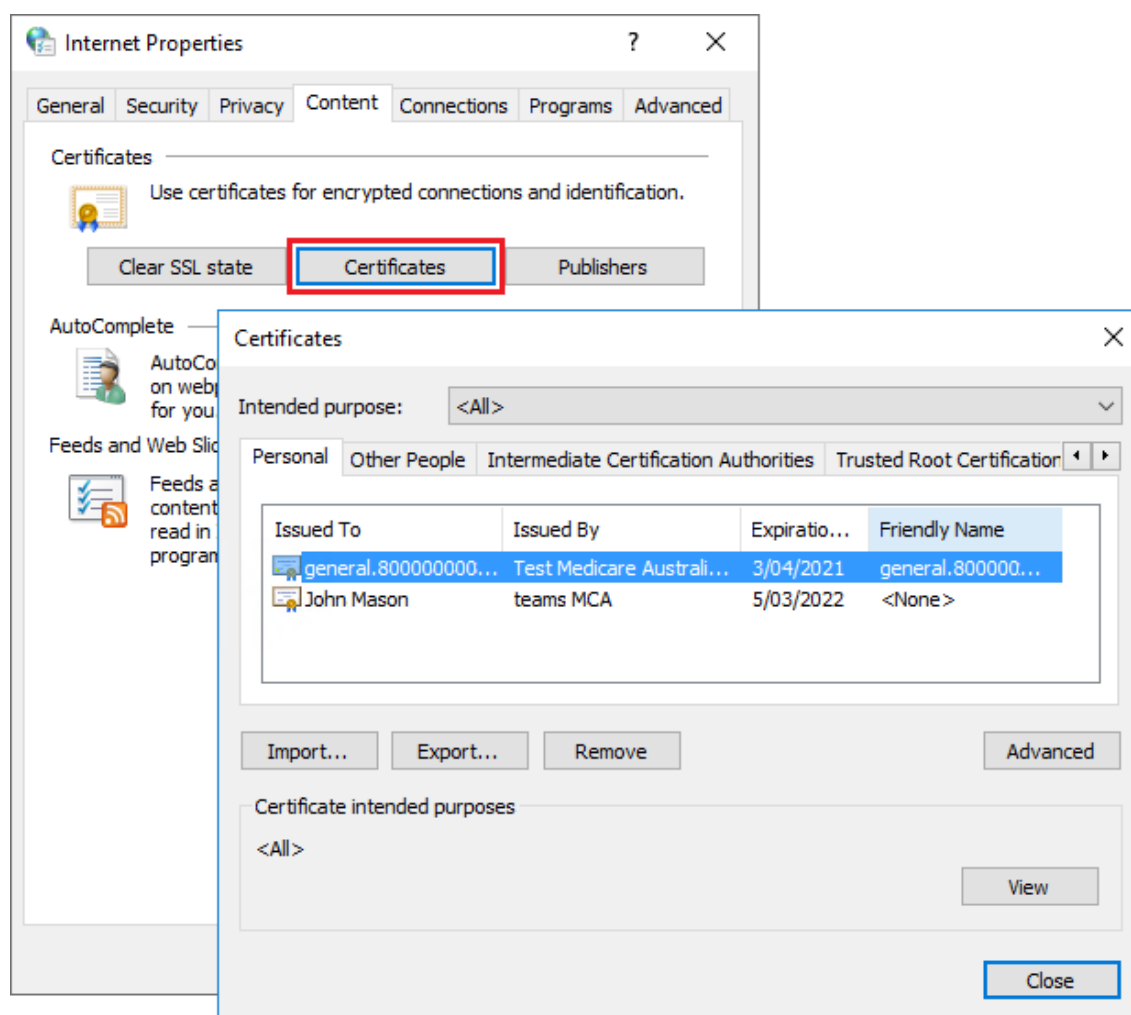
Can Windows verify the Site certificate?

Perform this step first to determine how to correct the issue.

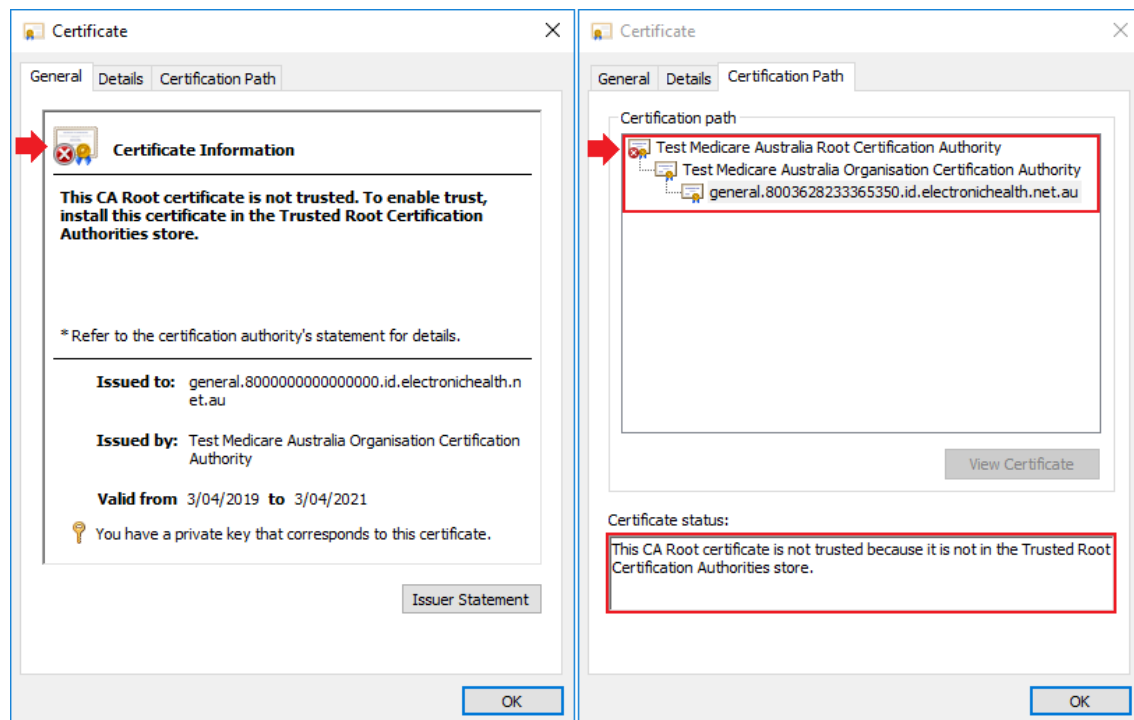
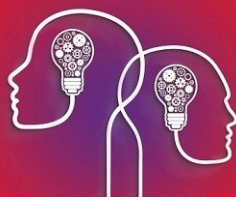
1. From the **Windows** desktop, run a search for 'internet options'. Double-click the result to open the **Internet Options** settings.



2. Select the **Content** tab and click **Certificates** to open the **Certificates** window.



3. Double-click your practice's HI certificate in the **Personal** tab of the **Certificates** window. The HI certificate will contain your practice name in the **Issued to** column.
4. Inspect the information provided in the **General** tab.



5. Click on the **Certificate Path** to verify the chain of trust.

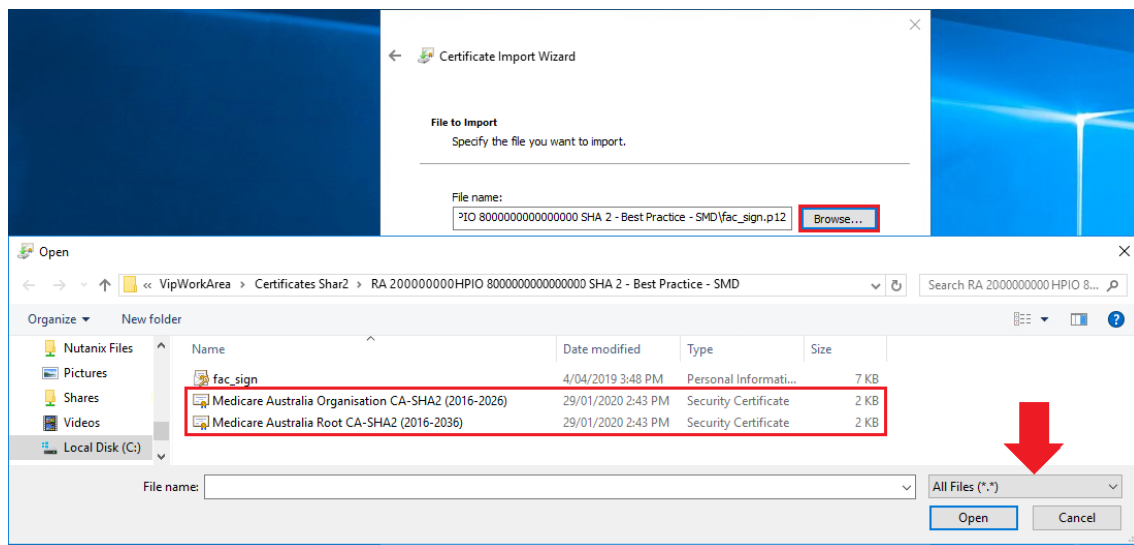
If a red cross is indicated on any of the levels of the chain of trust and the **Certification status** reports that the CA Root certificate is not in the Trusted Root Certification Authorities store, the chain has not been established.

Try the following to resolve the chain of trust:

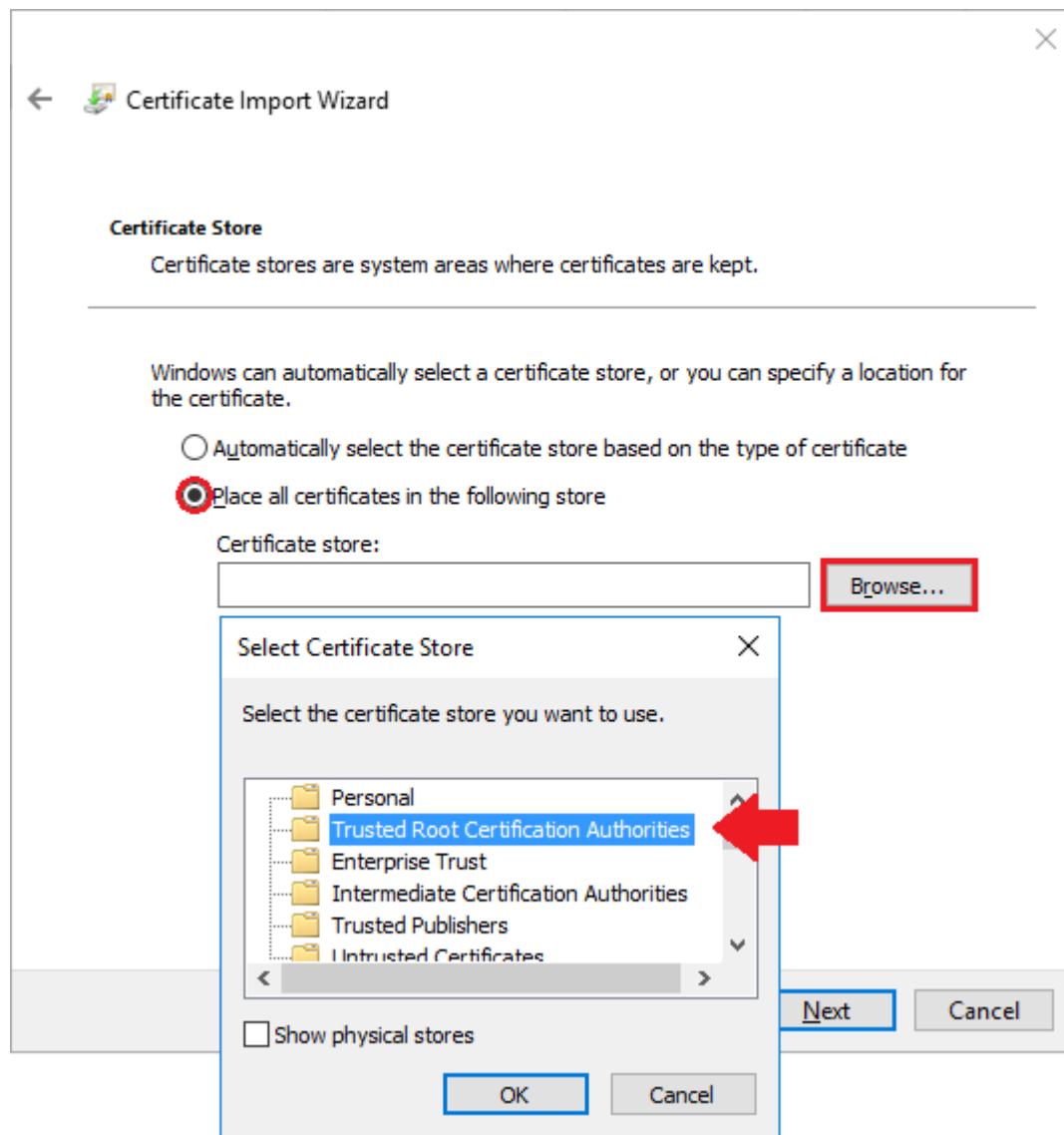
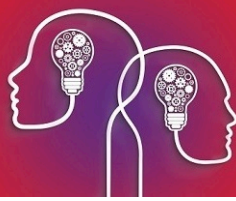
1. If the **Certification status** reports that the CA Root certificate is not trusted, check that the NASH certificate has been installed on the local machine rather than through **Internet Options**. Installing it the local machine establishes the chain of trust as it installs all certificates within the NASH certificate.
2. Import the **Root** and **Organisation** certificates into the Trusted certificate store.

Install the root and organisation certificates

1. Double click on the **fac_sign** Personal Information Exchange file to open the **Certificate Import Wizard**.
2. Select **Local Machine** in the **Store Location** section and click the **Next** button.
3. On the **File to Import** screen select the **Browse** button to display the contents of the NASH certificate.



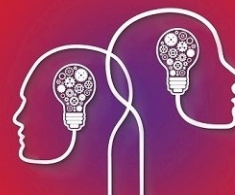
- Page 15



6. Select **Place all certificates in the following store** and click the **Browse** button.
7. Select **Trusted Root Certification Authorities** from the **Certificate Store**.

Important: Install the certificate into both the *Personal* and *Trusted Root Certificate* stores. You will need to do this one at a time.

8. Click the **OK** button.
9. Click **Next** on the **Certificate Import Wizard**.
10. Click the **Finish** button to complete the import.
11. Repeat the steps above to import the **Root Certificate**.
12. Verify the chain of trust is now established for the NASH certificate.

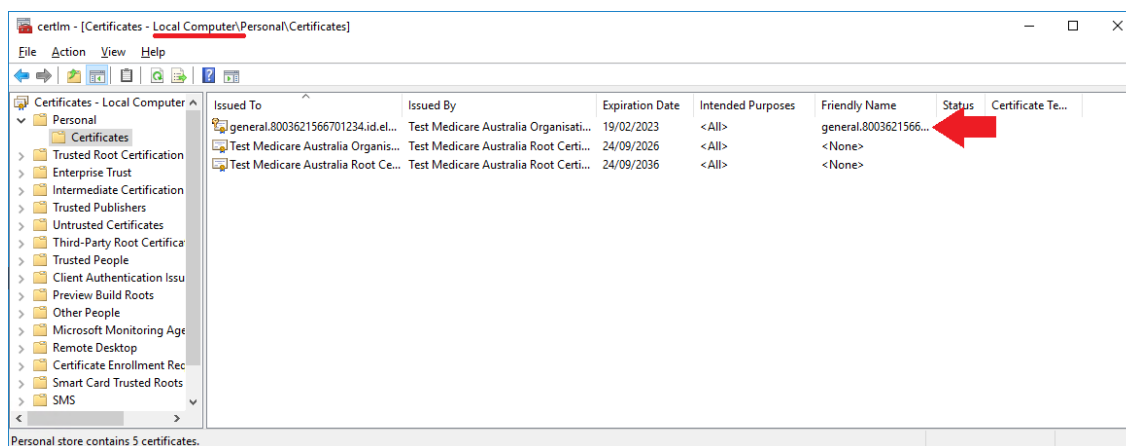


Configure Bp VIP.net with the NASH Certificate

When the NASH certificate has installed successfully, Bp VIP.net must be configured to enable the use of both **Provider Directory (Health Index)** and **My Health Record (MHR)**.

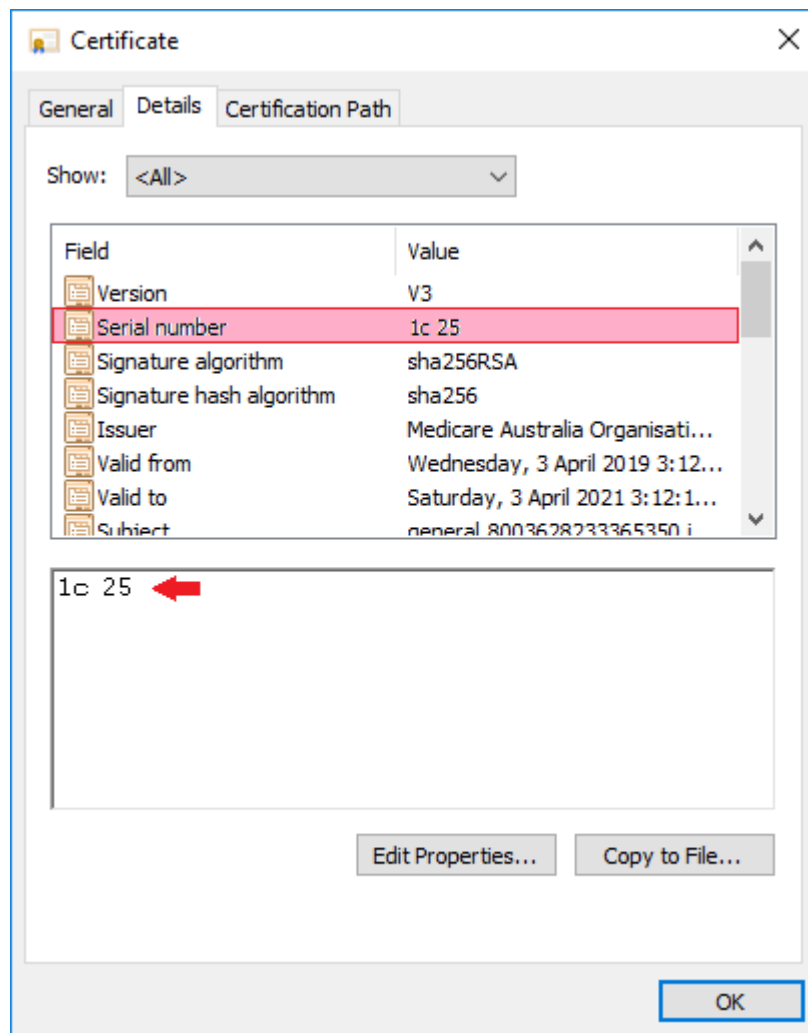
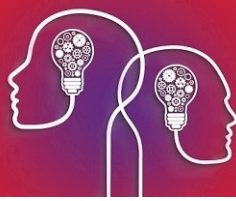
Configure the NASH Certificate

1. Click on the Windows **Start** menu and type in 'Manage Computer Certificates'. Click **Enter**.
2. When the **Certificate Manager (Local Computer)** window is displayed, double click on the general certificate.



The Certificate screen is displayed.

3. Select the **Details** tab on the **Certificate** screen.



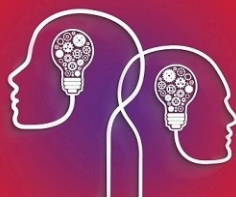
4. Select the **Serial number** and copy the number from the panel below.
5. Click **OK** to close the certificate screen.
6. Open Bp VIP.net and select **Setup > Facility Preferences > General Preferences**. The **Facility Preferences** screen is displayed.
7. On the **Facility** tab, select **HealthLink** from the **Online External Provider Directory** field.



8. Select the **Communications** tab.

Important: The **HIService Start Date** must be entered when the location certificates are completed.

9. Click on the **Details** button in the **HI Service Details** section to enter the NASH certificate details. The **HI Service Location Certificates Form** is displayed.



HIService Location Certificates Form

Browse Details

Certification Type ☒ HIService ☐ My Health Record

Location Name BP Software HI

Location ID BPC00000

Password (Passphrase) *****

Attached Organisation BPC_@, Best Practice Clinic

HPI-O Number

Certificate Serial No

Contact Person Name

Contact Phone

Contact Email

OK Cancel

10. Enter a **Location Name**.

Note: It is advisable to set the **HIService certificate** with the HI descriptor at the end to distinguish it from the **My Health Record certificate**.

11. Enter your **Location ID**, or Minor ID, which is provided by Best Practice Software.
12. Enter your NASH Certificate passphrase that you received via SMS.
13. Click in the **Attached Organisation** field to select your main internal facility record.

Note: The **HPI-O Number** will populate through if it has already been recorded on the **Facility Details (F3)** screen. If it has not yet been recorded, record the HPI-O in facility details after setting up the certificate.



HIService Location Certificates Form

Browse Details

Certification Type ☒ HIService ☐ My Health Record

Location Name

Location ID

Password (Passphrase)

Attached Organisation

HPI-O Number

Certificate Serial No

Contact Person Name

Contact Phone

Contact Email

OK Cancel

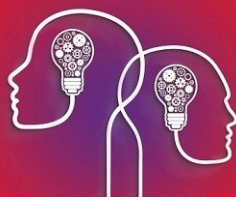
14. Enter the **Certificate Serial Number** as copied from the **Certificate Details** tab. Ensure there are no spaces in the serial number.
15. Enter the **contact details** (these details are not required for the certificate to work).
16. Click **OK** to complete the **HI Certificate** form.
17. If the **My Health Record** certificate details have not been previously recorded , a notification will display prompting the set up of the **My Health Record** certificate.

MyHealthRecord

The MyHealthRecord certificate is not set up. Would you like to set up the MyHealthRecord certificate using the current certificate?

OK Cancel

18. Click **OK**.
19. The **My Health Record** details are populated into the form.



HIService Location Certificates Form

Browse Details

Certification Type ☐ HIService ☒ My Health Record

Location Name

Location ID

Password (Passphrase)

Attached Organisation

HPI-O Number

Certificate Serial No

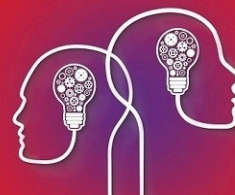
Contact Person Name

Contact Phone

Contact Email

OK Cancel

20. Enter a MHR descriptor at the end of the **Location Name**.
21. Click **OK** to complete the set up of the certificates.
22. Enter the start date (the date the certificate was issued) into **HI Service Start Date** field.
23. Click **OK** to complete this configuration.



Record practice and provider HPI numbers

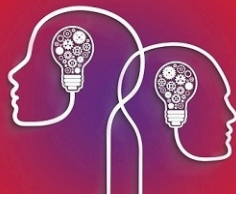
Record your practice's HPI-O number

The numerical code on the NASH certificate name is your organisation's HPI-O number.

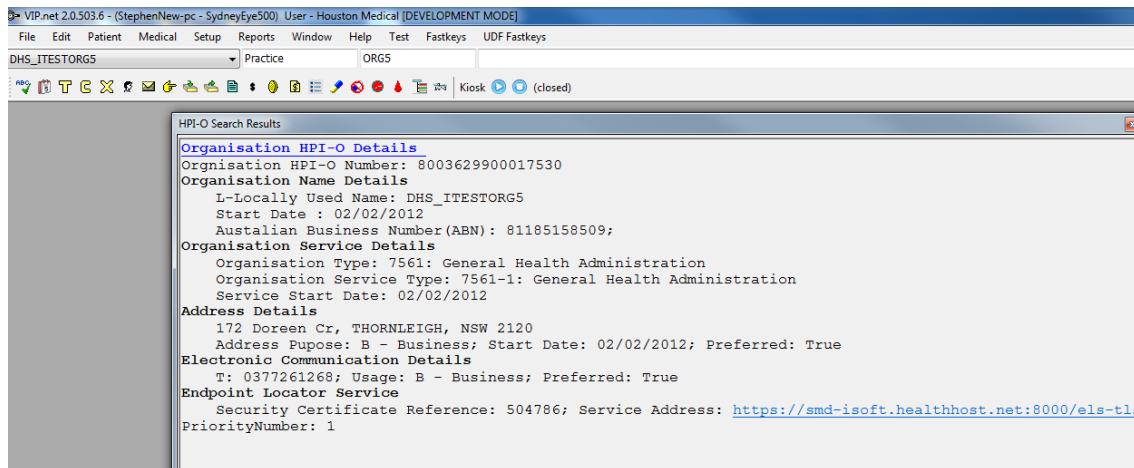
1. Log in to Bp VIP.net as an administrator user.
2. Press **F2** to search for your practice as an organisation. Open the practice's **Organisation Details** window (F3).
3. On the **Details** tab, record the practice's HPI-O number in **HPI-O Number**.

4. Click **OK**. Bp VIP.net will automatically attempt to validate the supplied HPI-O number and alert the user of success or failure. A successful lookup will return the details of the organisation associated with the HPI-O. The **Update Organisation Details** message is displayed.
5. Click **No** to keep existing demographic information in the Organisation Details and only validate the HPI-O number, or click **Yes** to update all demographic information with the record on the Health Provider Directory.

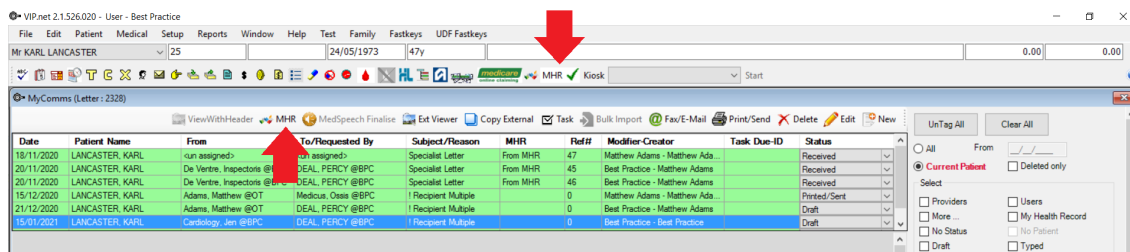
Tip: The **HI Verification** button can also be used to verify the HPI-O number, but an auto-



matic validation is run on entering a number.

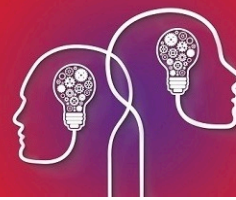


My Health Record setup is complete. A logged-in user with a HPI-I recorded can submit and view documents and other health summaries to the **My Health Record** service from **MyComms** or the **MHR** button on the tool bar.



Set HPI-I number for a provider

1. Log in to Bp VIP.net as an administrator user.
2. From Bp VIP.net, select **Setup > Security > Maintain Users**. The **Setup Users** window will appear.
3. Select the user that requires My Health Record access and click **Details**.
4. Record the provider's **HPI-I Number**.



Setup Users

Details

Login ID: JSMITH [Set Password...] ☐ Inactive

Surname: Smith

First Names: John

Provider: [] ☐ Is Provider?

Security Group: Provider [v] [Access Rights]

HPI-I Number: 8003610833335085

[OK] [Cancel]

5. Click **OK**.

Verify a HPI-number

1. The HPI-I number can be verified by running the **HI verification** on the **Provider** screen.
2. Select **Setup > Providers > This Clinic**.

Providers (Id: 520)

Internal

Surname: DEAL, First Names: PERCY, Title: Dr, Sex: M, Date of Birth: / /, Type: Specialist, Credentials: ABC, Revenue: 8003-6165-6668-1675, Tags: []

Facility Details

Name: Test Health Service 614, Building/Box: Unit 7.08, No/Street: 64 KYM Break, Suburb/City: WAVE HILL, Postcode: 0852, State: NT, Country: Australia, Phone: 61 02, Fax: 61 02

Provider Contact Details

Building/Box: Unit 7.08, No/Street: 512 IGNATIUS ST, Suburb/City: PERTH, Postcode: 7300, State: TAS, Country: Australia, Home: [], Mobile: 02, Business: 61 02, Fax: 61 02, Other: [], Email: SUPPORT@BPSOFTWARE.NET

Display

DEAL, PERCY @BPC, Background Colour: [], Font Colour: [], Unit: []

Communications

Letter [x] Email [] RSD [] Fax [], Message Provider: [], RSD Address: [], Numbers: LSPN: [], Provider: [], Prescriber: 526365, MBRN: [], Std Unit: [], HPI-I Number: 8003-6165-6668-1675, Entity Id: [], AHPRA Number: []

Online Provider Directory

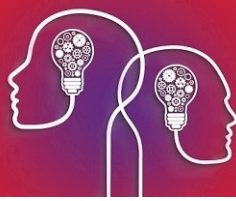
Not Linked with Directory [x], Unlink from Directory [x]

HI Verification

HI Verification

[OK] [Cancel]

3. Select the internal provider and click the **Modify** button.
4. Record the **HPI-I Number** and click the **HI Verification** button at the bottom of the screen.



5. The **Healthcare Identifiers** screen is displayed and the **Identifier Search with HPI-I Number** option selected.

Healthcare Identifiers

Personal Details		Australian Street Address		International Address	
Family Name	DEAL	Unit Type/Number		Building/Box	
Given Name	PERCY	Level Type/Number		No./Street	
Sex	M	Building/Box	Unit 7.08	Suburb/City	
Provider Type Code	2513: Occupational and Environmental Health Pr	No./Street	512 IGNATIUS ST	Postcode	
Provider Specialty Code	251311: Environmental Health Officer	Suburb/City	PERTH	State	
Provider Specialisation Code		Postcode	7300	Country	Australia
Wildcard Search String		Country	Australia		
HPI-I Number	8003-6165-6668-1675				

☒ Identifier Search with HPI-I Number
☐ Demographic Search with Provider Details
☐ Demographic Search with AUS Street Address
☐ Demographic Search with International Address
☐ Wildcard Search

Search

Transmission Log Close

6. Click **Search**.

The **HPI-Search Results** screen is displayed with the matched provider.

7. Click **OK** and click **Yes** on the **Update Provider Details** prompt to update information.
8. Click **Close** and **OK** to complete.
9. Record the HPI-I number for each internal provider who wishes to access **My Health Record**.

Important: If the HPI-I validation fails, ensure the provider has registered their record as 'searchable' on the Health Provider Directory. Providers must ring Healthcare Identifier Service Enquiry Line at Digital Health to register their record as 'searchable'.

Last modified 22 June 2021

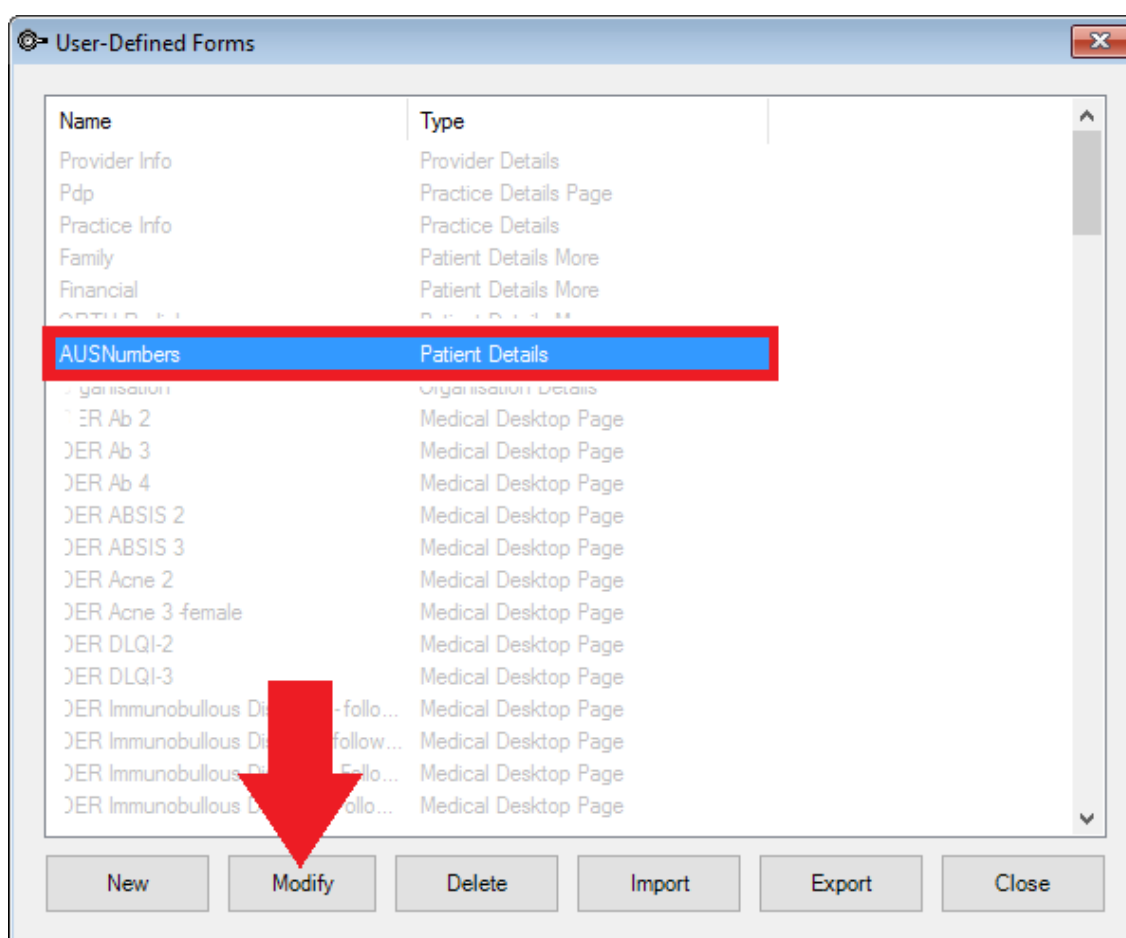


Recording patient IHI numbers (Australia)

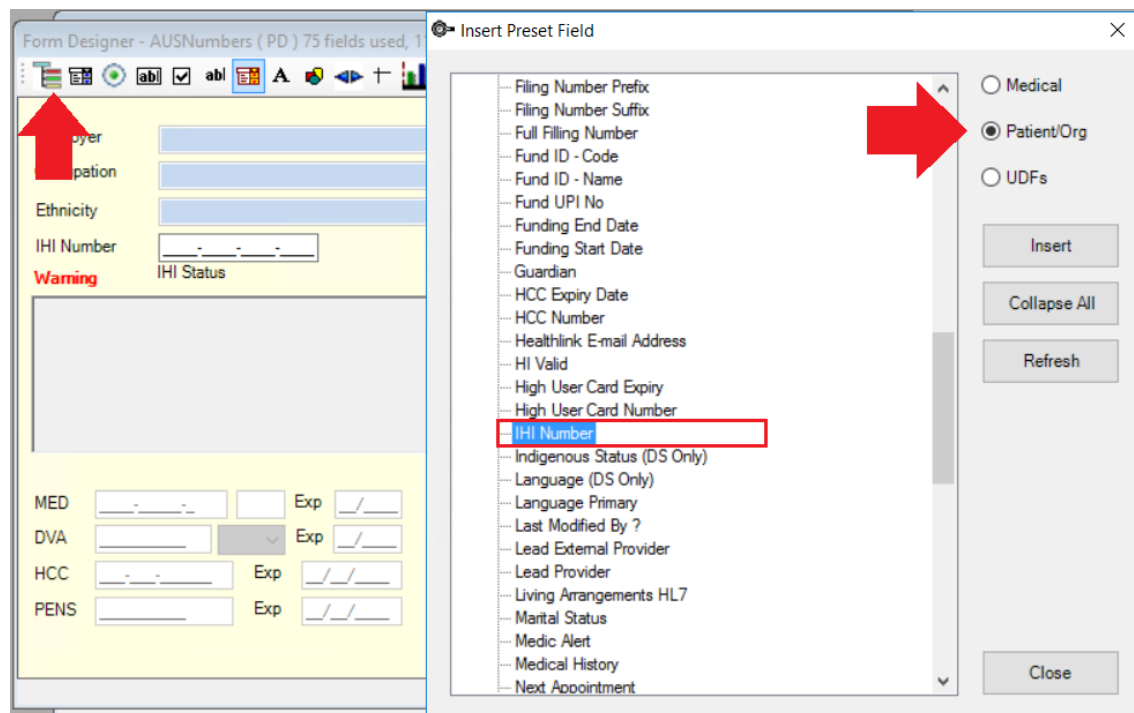
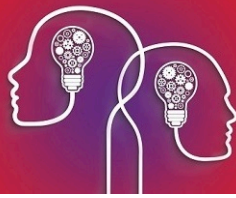
To access My Health Record, a patient must have an IHI number recorded in their **Patient Details** on Bp VIP.net. Ensure that your **Patient Details (F3)** screen has the **IHI Number** field.

Add IHI field to the Patient Details User Defined Form

1. Click **Setup > User-Defined Forms** and select the **Patient Details UDF** and click **Modify**.



2. On the **Form Designer**, click the **Preset** button, select the field type as **Patient/Org**.
3. Click the **+** next to the **Patient** group and select 'IHI Number' and click **Insert**.



4. Position the **IHI Number** field on the UDF and click **F12** to save.
5. Click **F3** to reopen the **Patient Details** screen and verify the field has been added.

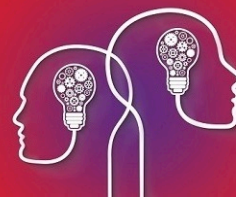
Record and verify the patient IHI number

There are various different ways to verify the IHI number for the patient.

1. If you have the IHI number for the patient, enter it in the **IHI Number** field and click **OK**.

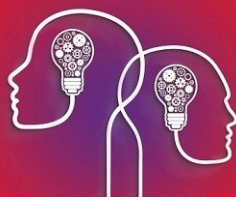
Bp VIP.net will automatically verify the number and a **Verified Active** date and time will be displayed below the **IHI Number** field. The **MHR** button in the tool bar will display with a green tick to show that this patient is verified and opted in to **My Health Record** by default.

A **green bullseye** will display next to the patients age to indicate successful verification. A **black bullseye** indicates the IHI number has not been recorded and validated.



Important: When an IHI number is recorded for a patient, Bp VIP.net automatically verifies the number on saving the patient's details. If the number is not verified, the entered number will not save and a warning will be displayed. It is advisable to store the number provided in the **Notes** section until you can verify the validity of the number if this happens. If you delete part of the number in error, the automatic validation will delete the rest of the number and you will either need to obtain the number again from the patient, or use their Medicare and DVA numbers to verify the IHI number again.

2. If you do not have the IHI number, you can run verifications using the patients Medicare or DVA numbers.
3. Enter the patient details including the **Medicare** or **DVA** number into the **Patient Details (F3)** screen and click the **HI Verification** button at the bottom of the screen.



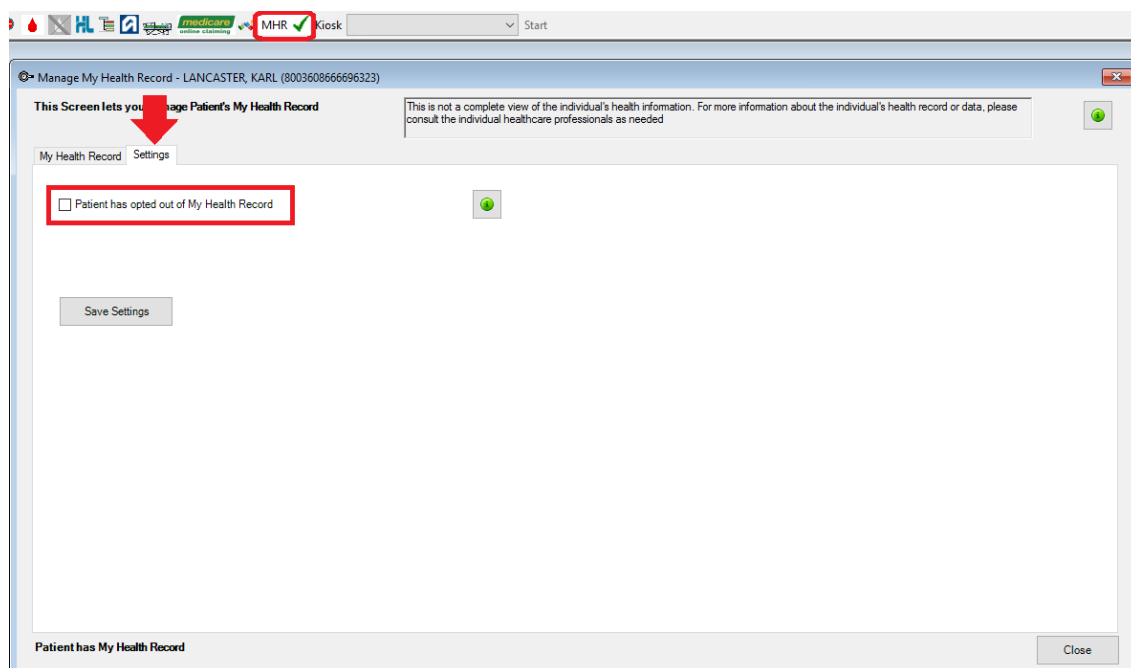
4. The patient information is populated and the **ID Number Search with Medicare Number** is selected by default. Click **Search**.
5. Click **OK** on the **Search Results** pop-up.
6. Click **Yes** to the **Update Patient Details** message to populate the IHI number into the **Patient Details** screen.
7. Click OK on the **Patient IHI Number/Status Updated** message.
8. Click **Close**.
9. The details will have populated back into the **Patient Details** screen and the verification status is recorded.

Accessing My Health Record

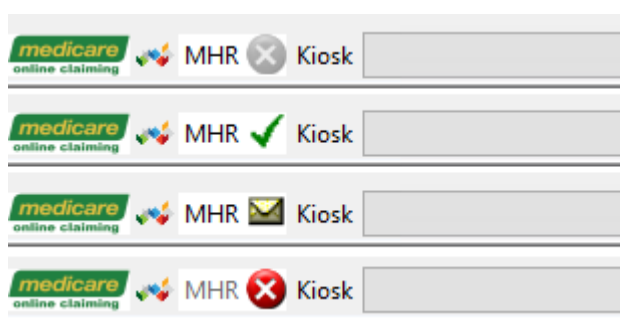
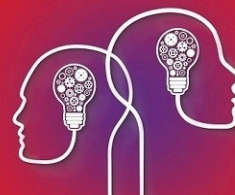
Important: The following My Health Record screen and button on the tool bar will be available in the Topaz release of Bp VIP.net.

Access to a patient's **My Health Record** can either be done through the **MHR** button on the tool bar or through clicking **Patient > Manage My Health Record**.

Bp VIP.net will opt in patients by default but this can be changed by clicking on the **Settings** tab and selection **Patient has opted out of My Health Record** and clicking **Save Settings**.



The **MHR** button in the tool bar also indicates the patient's activity on **My Health Record**.



- The **grey cross** indicates the patient is not IHI verified and therefore there is no access to **My Health Record**.
- The **green tick** indicates the patient is IHI verified and there is access to **My Health Record**.
- The **envelope** indicates that there are new uploaded documents in the patient **My Health Record**.
- The **red cross** indicates that the patient is IHI verified but either does not have a **My Health Record** or access is restricted and an access code can be provided by the patient. Please see the [My Health Record page](#) for more information on setting access codes on My Health Record. Accessing the My Health Record will prompt the access code to be added into the **My Health Record - Access Level** screen.

