Indigo

Bp Premier Medicare Online Claiming Setup for Single Location

Legal notices

Copyright © 2018 Best Practice Software. All rights reserved.

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 4670	Hamilton New Zealand 3240

www.bpsoftware.net

The information contained in the User Manual is intended to be a guide only. BPS 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: July 2018

Intended for usage with Bp Premier version Indigo.

This User Manual is sourced from the Best Practice Software Bp Premier Indigo **Knowledge Base**.

Set up online claiming

You must set up online claiming to process Medicare patient claims. The following instructions describe how to set up online claiming if your practice uses a **single Minor ID**. This usually means your practice has only one location.

If your practice or organisation has multiple Minor IDs registered with Medicare, the configuration process will be slightly different. Search for 'multiple minor IDs' in the Bp Premier knowledge base for more information.

> ⚠️ **Important:** *If you are using another management package that uses Online Claiming, you will need to finalise and receipt all claims in that package **before** configuring Bp Premier for Online Claiming. Medicare Online Claiming can only operate from one software package at a time.*

If you have set up Medicare Online previously at your practice, you may already have completed steps and .

If you changed to Bp Premier from another billing package

If you recently changed from another billing package, your practice will most likely not have the correct Medicare components installed on your system. Before you continue with the configuration, check the following:

1. Check that you have Bp Premier version 1.7.0.500 or higher installed. From the main menu, click **Help** > **About** and check that the version or Build No. shows 1.7.0.500 or higher.

2. In File Explorer, browse to the C:\ drive of the Bp Premier server PC and look for the folder C:\Program Data\BPOnline.

   If the folder does not exist, the Medicare components have not been installed during the installation of Bp Premier. To apply these components, close down the Bp Premier server and reapply the program upgrade for your version of Bp Premier. When you reach the **Online Claiming** installation screen, tick **Install the Best Practice Software Online Claiming module**.

3. Browse again to the folder c:\Program Data\BPOnline. If the folder still does not exist, contact Best Practice Software support for assistance.

Installing the Medicare module

You can install the Bp Premier Medicare module if you did not select to install this module the first time you installed Bp Premier. This module allows Bp Premier to connect to Medicare to verify patient Medicare/DVA eligibility and send patient and bulk bill claims online.

1. Locate the program upgrade media for your version of Bp Premier. This might be a DVD sent to you by Best Practice Software, or an .exe file that you downloaded from the Best Practice Software website.
2. Run the upgrade file.
3. Proceed through the upgrade screens, leaving default values for everything until you reach the **Online Claiming installation** option.
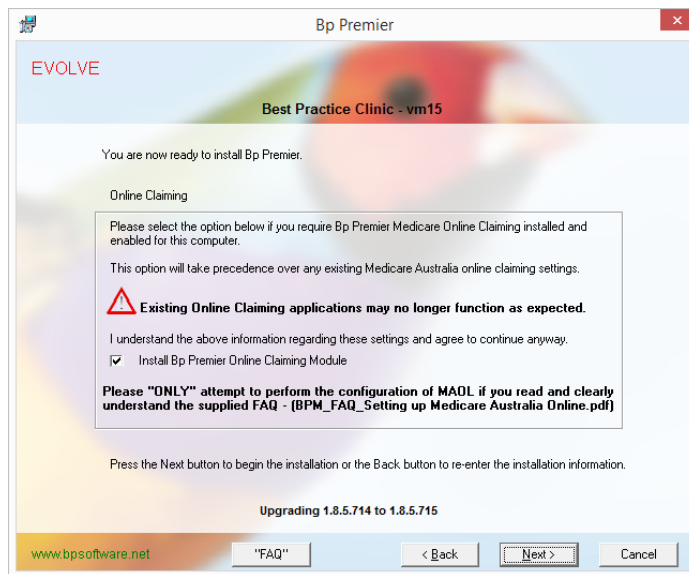
4. Tick the checkbox **Install Bp Premier Online Claiming Module** and click **Next**.
5. Complete the rest of the installation using the default values. You can now enable online claiming in Bp Premier.

1. Obtain your Minor ID

The Minor ID is an 8 digit number derived from your Best Practice Software Site ID.

1. Identify your Site ID. Select **Help** > **About** from the main Bp Premier screen. Your Site ID is displayed in the bottom left of the screen.
2. Take your Site ID and prefix it with the letters **BPS**.
3. Pad the ID with zeroes so that the total length is 8 characters.

For example:

- If your Best Practice Software Site ID is 849, your Medicare Minor ID number would be BPS00849.
- If your Best Practice Software Site ID is 1234, your Medicare Minor ID number would be BPS01234.

Important: *If your practice has multiple locations, it is not possible to have multiple Medicare Minor IDs within Bp Premier. All claims received by Medicare will use the location selected on the* **Setup > Configuration > Online claiming** *screen when transmitting. In Bp Premier, however, you can filter Medicare batches by provider and location.*

2. Register with Medicare

All practitioners wishing to use Medicare Australia Online (MAOL) will need to register and obtain Medicare Site certificates. Contact Medicare eBusiness centre on 1800 700 199 to obtain the application forms. When completing the form, you will need to provide your practice's Minor ID.

- If you are already registered but are using another management package, you can use your current certificates to set up Medicare Online in Bp Premier, but you will still need to notify Medicare to tell them you are now using Bp Premier. You will have to supply your new Minor ID .
- If you are not currently registered, you will need to register and apply for a Medicare Site Certificate. You will have to supply your Minor ID.
- Each time you add a new doctor to the practice, you will have to notify Medicare to add this doctor.

The *Practice Details Form* for online claiming and *Payee Provider Banking Details Form* can be found in the list of Medicare forms at:

http://www.humanservices.gov.au/health-professionals/forms/

3. Enable online claiming

1. Log in to the Bp Premier server as a user with administrator permissions.
2. Select **Setup** > **Configuration** from the main screen. Select the **Online claiming** tab.

3. Complete the fields in this screen, using the table below for guidance.

Field	Description
Activate Online Bulk Bill Claiming	Tick to activate online claiming for bulk billing, if your practice offers bulk billing (or Direct Bill) and wishes to process bulk billing claims through Medicare online claiming.
Activate Online Private Patient Claiming	Tick to activate online claiming for private patients, if you wish to process patient claims through Medicare online claiming.
Activate Tyro Integrated EFTPOS	Tick this option if your practice uses a Tyro terminal and you wish to process EFTPOS payments through the Tyro terminal.
Activate EasyClaim Private Patient Claiming	Tick this option if your practice uses a Tyro terminal and you wish to process real-time Medicare Easyclaims through the Tyro terminal.

Field	Description
Always send private patient claims by best available method	Tick if you intend to use the Online Patient Claiming for private billings and wish to default for all private claims to be sent to Medicare.
Minor ID	Enter your practice's single Minor ID. If your practice uses multiple minor IDs, you will have to set up each practice location and minor ID in the **Practice Details** screen.
Multiple Medicare Locations	Leave this checkbox unticked.
Proxy details	If your practice network uses a proxy server, enter the **Proxy ID** and **Proxy password** for the proxy server so that online claiming can connect through the proxy.
A5 Vouchers	Tick to print Medicare and DVA vouchers as two separate A5 pages. If not selected, the two copies will be printed side by side on a single A4 page.
Print 2 copies of vouchers	Tick if you wish to print two copies of each Medicare assignment form.
Maximum No of vouchers in a batch	Defaults to 80. This is the recommended maximum batch size, but can be reduced. Best Practice Software do not recommend that you increase this value.
Default number of months to display when viewing all batches	Sets the default number of months to display when viewing batches from the **Direct Bill Batches** screen.
Path to Certificate Store	The certificate store is created on the Bp Premier server and shared by all workstations where transmission to Medicare is to occur. This path is where Bp will store the certificates after they are imported using the **Import Medicare Certificate** and **Import site certificates** buttons. DO NOT copy your Medicare certificates manually into this folder. Certificates must be imported using the buttons. Do not change this folder from C:\ProgramData\BPOnline\.

4. Click **Change** to display the **Path to Certificate Store** screen. Click **Save**. Bp will prompt that the certificate store does not exist and ask 'Would you like to create one now?'

5. Click **Yes** to create the store. You will be prompted for a password for the certificate store. This password MUST be the same as the password provided to you from Medicare with your certificates. This is called your Personal Identification Code (PIC).

Note: Do not misplace this password. You are responsible for this password; Best Practice Software cannot retrieve this for you.

6. Click **Import Medicare certificate** to import the Medicare Australia public key. The **HeSA Certificates** screen will appear, showing the currently installed certificates.
7. Click **Change folder**. Browse to your Medicare CDROM, or the location where you have stored your PKI certificates, and click **OK**.
8. Select a certificate labelled 'Medicare Australia...' and click **Attach**. If the certificate is imported successfully, Bp Premier will display 'The certificate was successfully imported'.
9. Repeat step 8 for each certificate labelled with 'Medicare Australia'.
10. Click **Close** to close the **HeSA Certificates** screen. Keep the **Configuration** screen open.

4. Import site certificates

This function imports the HeSA Location certificate, which is the practice's certificate to digitally sign data sent to Medicare.

1. On the Bp Premier server, insert the CD you received from Medicare that contains your practice's certificates.
2. From the **Online claiming** tab of the **Configuration** screen, click **Import Site certificates**. The **HeSA Certificates** screen will appear.
3. Click **Change folder**, browse to the CD drive. and click **OK**. The screen should display any site certificates found in that location. There should be two certificates called **fac_encrypt.p12** and **fac_sign.p12**. Select one of the files displayed and click **Attach**. Bp Premier will display a message when the certificate has been imported.
4. Repeat for the other certificate displayed.

Note: If a certificate called trust.p12 is present, this certificate cannot be attached and will produce an error message if attempted.

5. Click **check certificate expiry**. The **HeSA Certificates** screen will appear. There should be at least five items listed similar to those on the example below.
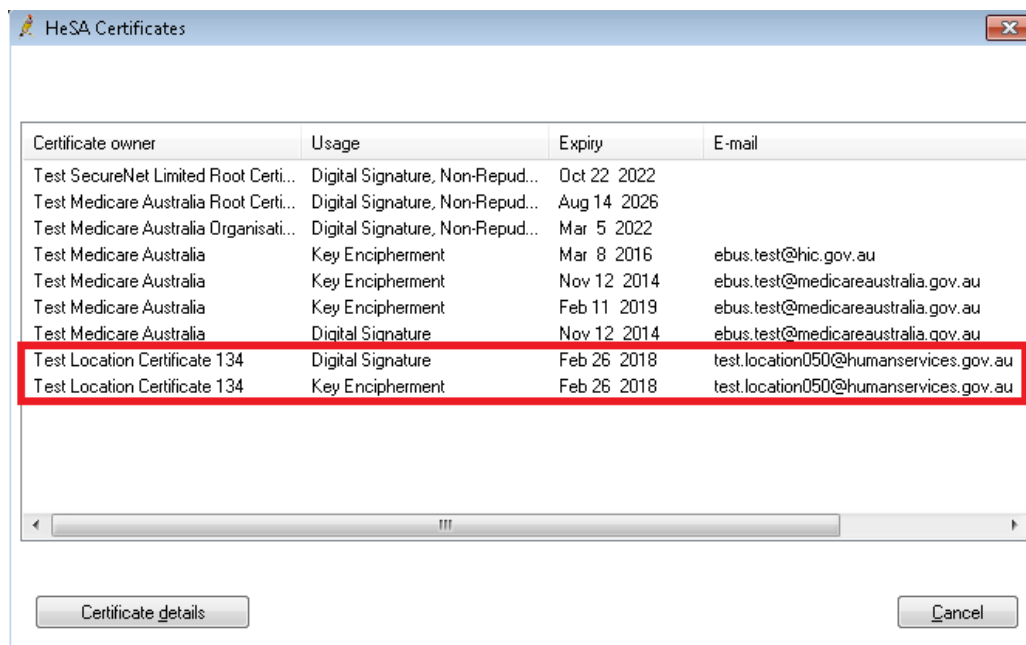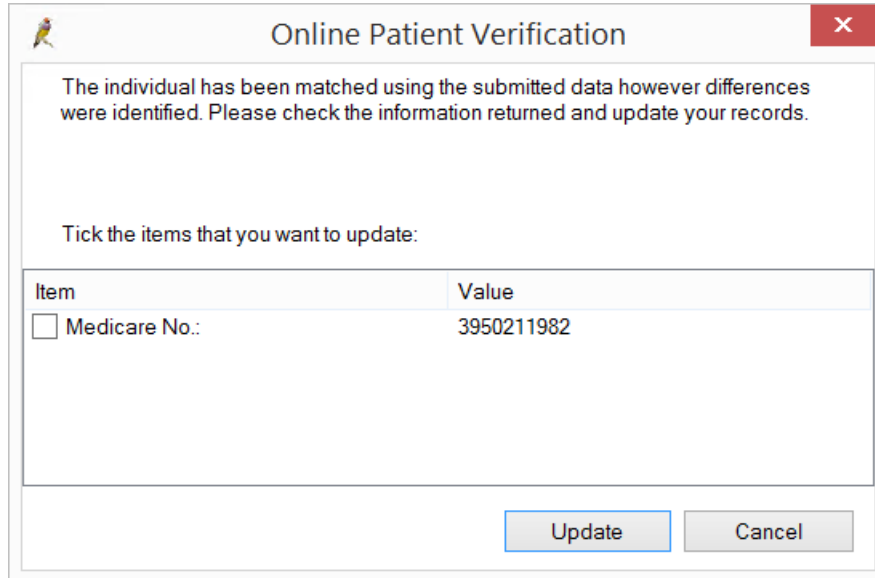
Two should mention 'Medicare Australia' in the **Certificate owner** column (these are Medicare Australia's certificates) and two should mention the clinic name (in the example, 'Location 173').

6. Check that all the **Expiry** dates are future dates.
7. Press **Cancel** to return to the **Configuration** screen.
8. Press **Save** to save these changes.

5. Test the link to Medicare

Before sending your first batch, Best Practice Software suggest that you test the link to Medicare.

1. From the main screen of Bp Premier, select **View** > **Patients**. The **Patient list** screen will appear. Enter a surname or part to **Search for**.
2. Select a patient name and click **View details**. The **Edit patient** screen will appear.
3. Click **Medicare / DVA eligibility check** at the bottom of the screen. This will contact Medicare and check whether the **Medicare No.** is valid for this patient. If the communication is working correctly, Bp Premier will display a message similar to the one below.

Online Patient Verification

The individual has been matched using the submitted data however differences were identified. Please check the information returned and update your records.

Tick the items that you want to update:

Item	Value
☐ Medicare No.:	3950211982

Update   Cancel

4. If the test is successful, you can configure each workstation to access the Medicare certificate store. Exit the **Edit patient** screen.

If the test is not successful, contact Best Practice Software Support via phone or email to diagnose the problem.

6. Configure all workstations

1. Exit from Bp Premier on the server.
2. Browse to the folder C:\ProgramData\BPOnline on the server and share the folder across the network.
3. Give all Windows users who access Bp Premier 'full control' permissions to the folder and its contents.
4. Browse to the file HIC.psi, right-click and select **Properties** > **Security** tab. Ensure that all users have 'full control' permission to this file.

   Note: Your practice's IT support can help if you are unsure how to share folders and change access permissions.

5. Go to the first workstation. Ensure that Bp Premier version 1.7.0.500 or higher has been installed and that the folder C:\ProgramData\BPOnline exists on that workstation. If this folder is not found on the workstation, for the version of Bp Premier on this workstation. When you reach the **Online Claiming** installation screen, tick **Install the Best Practice Software Online Claiming module**.
6. Log in to Bp Premier on the workstation.

7. Select **Setup** > **Configuration** from the main screen. Select the **Online claiming** tab.

8. Tick **Activate Online Bulk Bill Claiming**, **Activate Online Private Patient Claiming**, or both, depending on the online claiming services your practice offers.

9. Set the **Location Name** to your practice's Main Surgery and the **Location code** for your practice is correct.

10. Beside **Path to certificate store**, click **Change** and either type in the UNC path to the certificate store on the server (for example, '\\servername\BPOnline') or browse to this folder and click **Save**.

11. Click **Check certificate expiry**. If sharing has been set up correctly for the certificate store, Bp Premier will display the certificates and their expiry dates.

12. Follow the steps outlined in **5. Test the link to Medicare on page 9** to confirm that the work-station can communicate to Medicare.

13. Repeat steps 5—12 on all workstations on the network.

Best Practice Software recommend that you create an online batch with just a few transactions and transmit this as a test. If the test batch is successful, you can create larger batches for transmission.

7. Clear AIR Register

Each time an immunisation is recorded for a child, a record is written to the **Australian Immunisations Register** (AIR). If you have been using Bp Premier for a while but have been transmitting immunisation data via another application, you should clear out the AIR in Bp Premier prior to your first online transmission from Bp Premier.

To clear the AIR:

1. Select **Utilities** > **Australian Immunisation Register** from the main screen. The **Australian Immunisation Register** screen will appear.

2. Select all records. Use Ctrl+Click if you need to.

3. Select **File** > **Exclude Current Record**.

If you wish to have a hard copy of the records you can select **File** > **Print** and print the list. Once the printing is complete, you will be prompted 'Do you want to mark these immunisation records as notified to Australian Immunisations Register'. Click **Yes** to mark all records and remove them from the list.

Certificate expiry and update

You may periodically need to update the PKI certificates issued by Medicare. Certificate updates are distributed by Best Practice Software through the regular drug updates, but you'll need to import them from the **Configuration** screen.

Before you update your Medicare certificates, ensure that your practice has updated Bp Premier with the latest data update. To check which data update you have installed, log in to Bp Premier and select **Help** > **About**. The **Last drug update** field shows the most recent installed data update.

You can also use public key certificates to renew your site certificate instead of receiving a renewal certificate from Medicare. See **Renew Medicare Site certificate using public key on page 17** for more information.

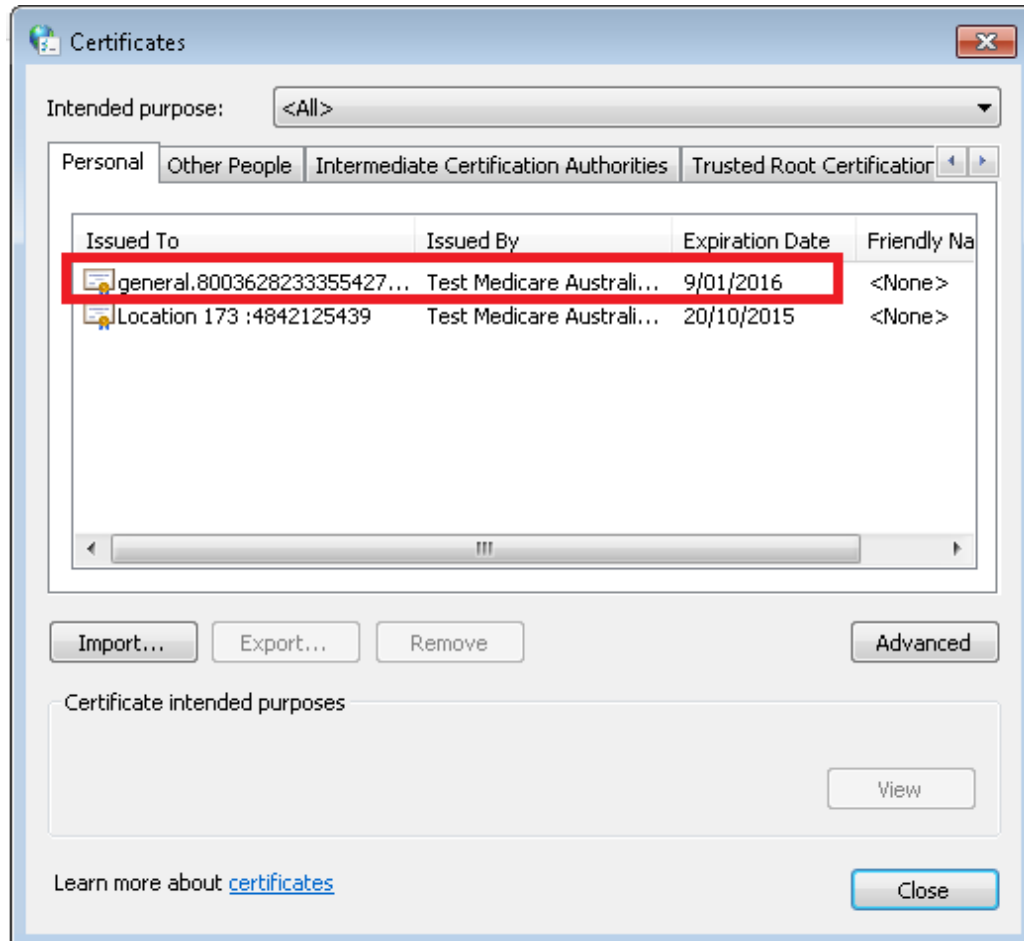### How do I check the NASH certificate expiry date?

Follow the instructions on any Bp Premier workstation that has successfully uploaded to My Health Record online.

1. Click the Windows logo in the bottom left of the toolbar, or click the Windows logo button on the keyboard.
2. Click the **Search** icon (magnifying glass) in the top right to slide in the Search bar.
3. Type 'internet options' into the Search bar and select **Internet Options** from the list. The **Internet Properties** screen will appear.
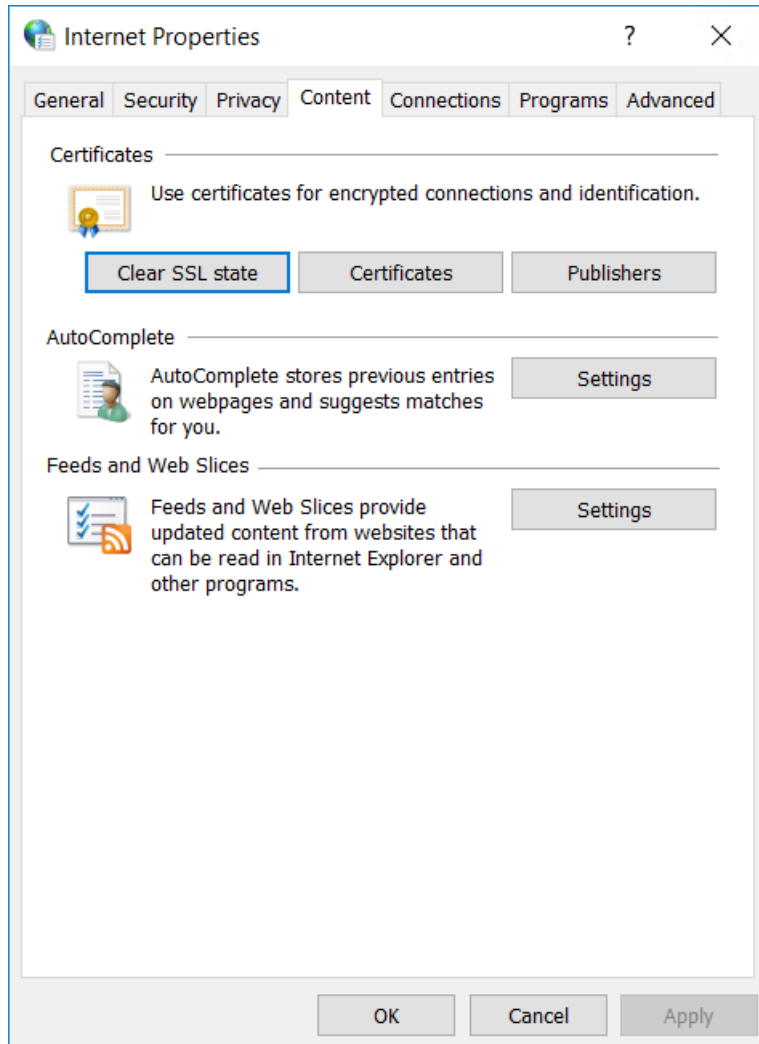
Your version of Windows may be different to the screenshot above.

4. In the **Internet Properties** screen, select the **Content** tab. Click **Certificates**. The **Certificates** screen will appear.

5. The NASH certificate is indicated in red. The name should be 'general' followed by the HPI-O number for the practice.

Note: If there are multiple NASH certificates shown, the current certificate will have the latest expiry date.

How do I check the site certificate expiry date?

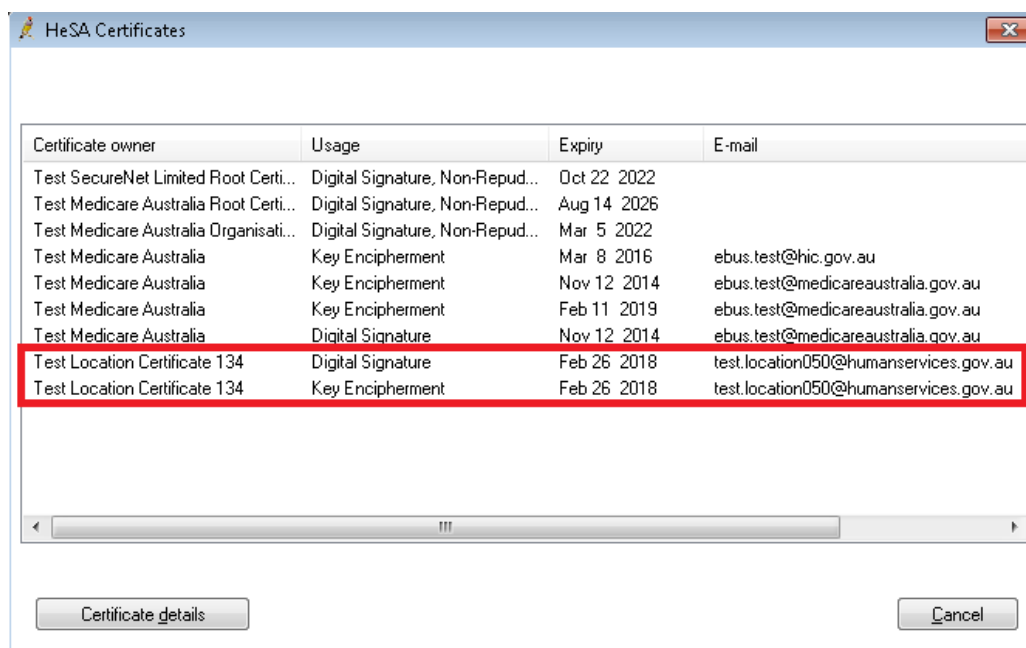You can check the certificate expiry for the site certificate from Windows, or from Bp Premier.

From Windows:

Follow the instructions for **How do I check the NASH certificate expiry date? on page 12** The site certificate is the certificate with the practice's name in the **Issued To** column (the first column).

From Bp Premier:

If online claiming has been set up on a workstation, you can check from Bp Premier.

1. Log in to Bp Premier on the server as a user who has a high level of permissions (for example, the Principal Doctor or Practice Manager).
2. Select **Setup** > **Configuration** > **Online Claiming**.
3. Click **Check certificate expiry**. The **HeSA Certificates** screen will appear.

4. Test certificates are shown in the screen example above. In your screen, the site certificate will have your practice under the **Certificate owner** column and your practice's email registered with Medicare in the **E-mail** column.
5. Click **Cancel** to return to the **Configuration** screen.

Import Medicare certificates

1. From the **Online Claiming** tab of the **Configuration** screen, click **Import Medicare certificate**. The **HeSA Certificates** screen will be displayed.
2. Click **Change folder**. The **Browse for folder** screen will appear.
3. Browse to the folder C:\Program Files\Best Practice Software\BPS\MedicareCerts and click **OK**. You should see four certificates listed.
4. Select the first certificate and click **Attach**. You should get the message 'The certificate was successfully imported'.
5. Click **OK**.
6. Repeat steps 4–5 for each Medicare certificate in the **Hesa Certificates** screen.
7. Click **Close** to return to the **Configuration** screen.
8. Click **Check certificate expiry**. The **HeSA Certificates** screen should now show at least two extra entries with a **Certificate owner** of 'Medicare Australia' with future expiry dates.

9. Click **Cancel** to return to the **Configuration** screen.

10. Click **Save** to save the settings and exit.

11. Perform a patient Medicare / DVA eligibility check to check that Bp Premier can still connect to the Medicare servers.

Renew Medicare Site certificate using public key

Follow the instructions below to renew your site certificates:

1. Install PKI Certificate Manager.
2. Download public digital certificates.
3. Renew your site certificate.

Before you begin:

- Perform the instructions on the Bp Premier machine with the certificate store installed (the file HIC.psi). This is usually the Bp Premier server.
- You will need the PIC passphrase that came with your Medicare site certificate.

Install PKI Certificate Manager

You may have already downloaded PKI Certificate Manager as part of previous online claiming configuration. Check that you have the latest version.

1. Open the following link in an internet browser: **www.humanservices.gov.au**.
2. Scroll to the bottom of the page and click **PKE Certificate Manager Installer**. The zip file will be downloaded to your browser's default download folder.
3. Double-click the downloaded zip file to extract the contents.
4. Navigate to the **win** folder in the extracted file and double-click **PKI Manager Installer V2.3.20.exe**.
5. Click through the install wizard to install the certificate manager.

Download public digital certificates

⚠️ *Important: Public certificates **cannot** be used to online claim. These certificates allow you to update expired PKI certificates using the certificate manager.*

1. Open the following link in an internet browser: **Certificates Australia**.
2. Enter at least one of the following pieces of information and click **Search!**:
    - First Name of person registered against the site certificate
    - Surname or RA Number
    - Email address registered against the site certificate (email is the quickest search)
    - Organisation name registered against the site certificate.

Healthcare Public Directory Search

First Name:		Surname / RA Number:	
Email address:	john.grace@smithstreetgp.net.au		
Organisation name:			
An Australian State:	NSW ▼		

Search!

▸   **Click here for search tips**

Click **Click here for search tips** for guidelines on effective searches and using the * wildcard.

3. Any matching certificates will be returned. Click **Download** next to the Signing Certificate **and** the Encryption Certificate and download both files to a known location. You will need to supply the location of these certificates in the final step.

   Details have been blanked in the example below.


Matching Certificates

Note: A maximum of **50** entries will be displayed.

To download a certificate in the standard MIME format, press the green **Download** button next to it. A few programs (for example, old versions of Netscape) need the certificate in **application/x-x509-email-cert** MIME format; press the **Netscape** button for this format.

cn=   ,ou=   ,o=
     ,l=BRISBANE CITY,st=qld,c=AU
Email:
Download Netscape 27 Sep 2016 to 27 Sep 2021 (policy; Encryption Certificate)
Download Netscape 27 Sep 2016 to 27 Sep 2021 (policy; Signing Certificate)

Renew your site certificate

1. From the Windows desktop, open Control Panel. The path to Control Panel will depend on the version of Windows:

   ▪ Select ⊞ > Apps > Windows System > Control Panel.
   ▪ Search for 'control panel' in Windows toolbar or Start page.

2. Select 'Small icons' from the **View by** drop-down in the top right hand corner.
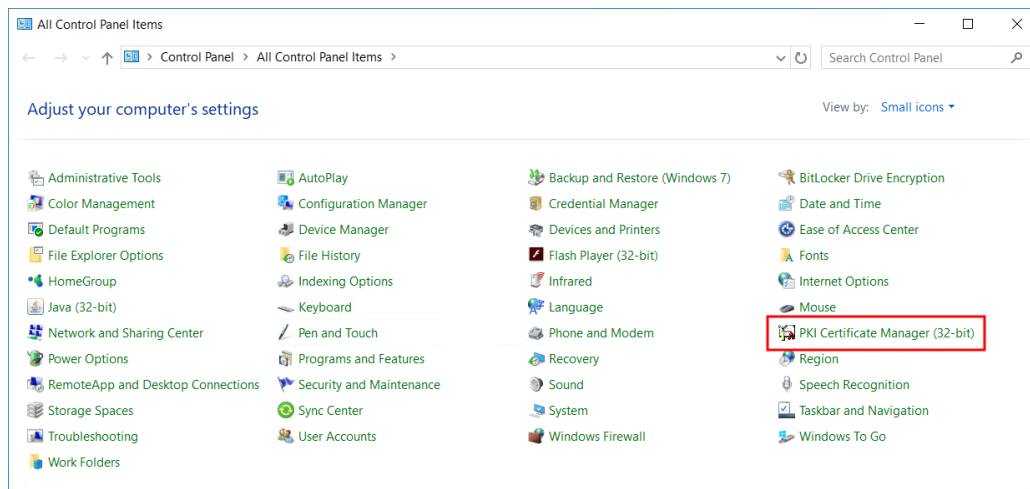
3. Click **PKI Certificate Manager**. The **Store Setup Wizard** will open.
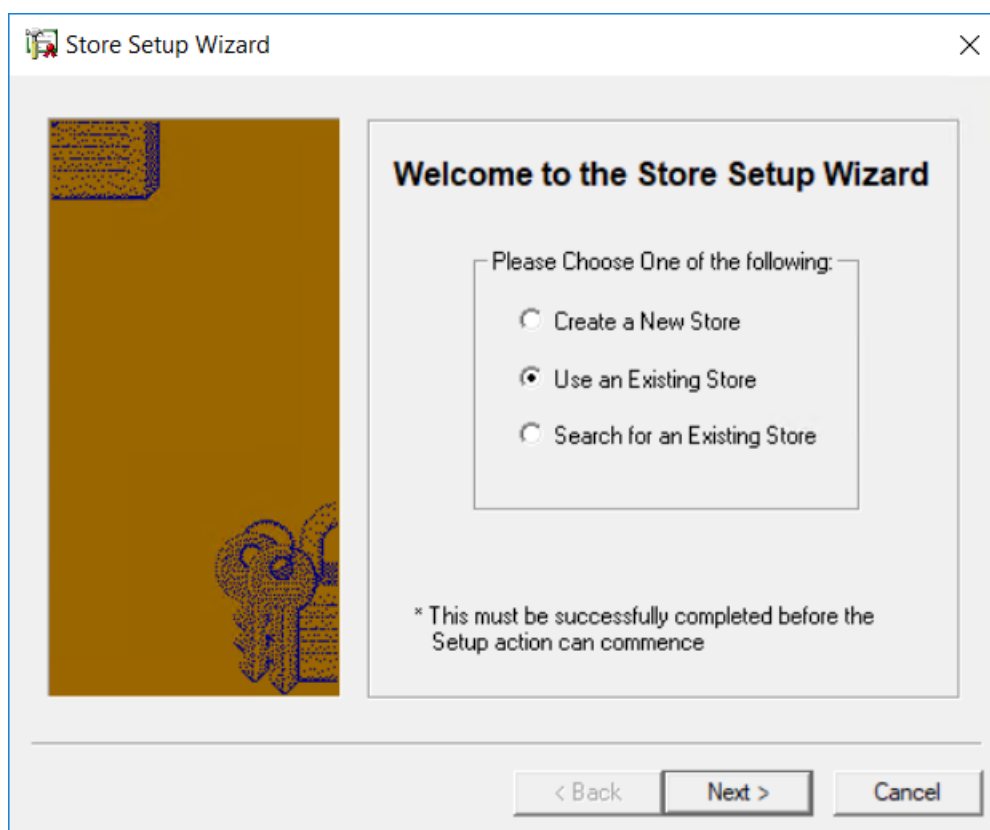
4. Select **Use an Existing Store** and click **Next**.
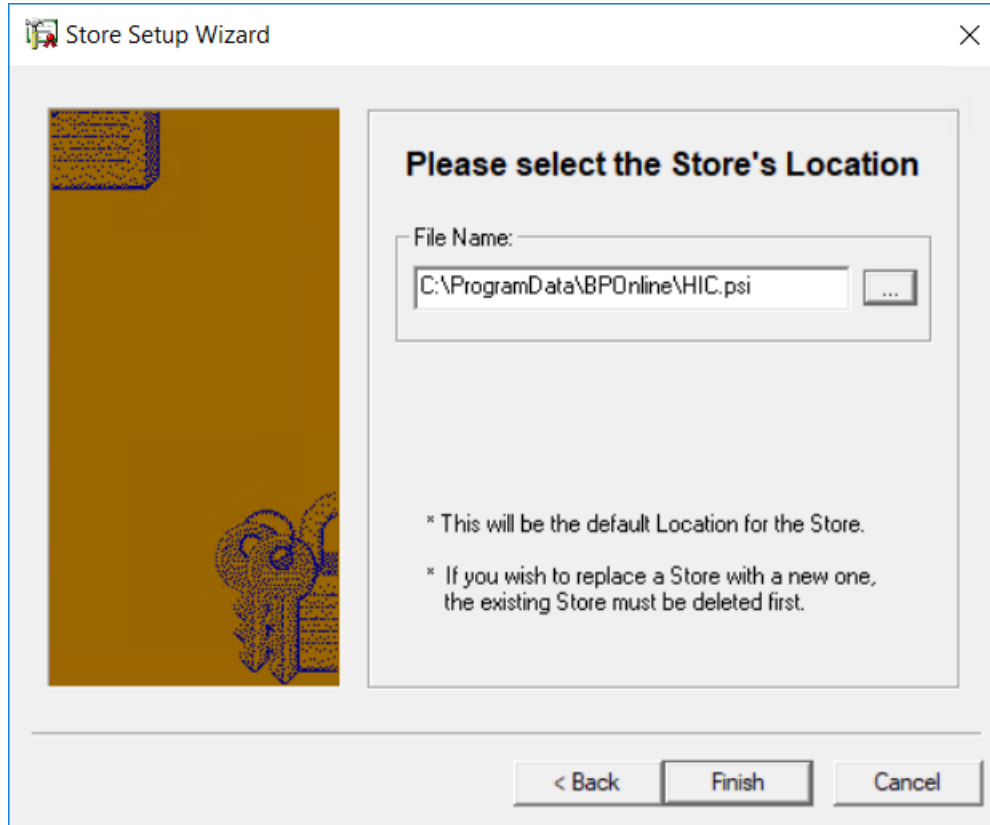
5. Browse to the location of the Bp Premier certificate store file **hic.psi**. By default, this file is in C:\ProgramData\BPOnline on the server. If you're unsure of the path to the HIC file, in Bp Premier, select **Setup** > **Configuration** > **Online Claiming** and check the **Path to certificate store** value.

6. Click **Finish**. The PKI Certificate Manager will open, showing the certificates stored in the HIC file.
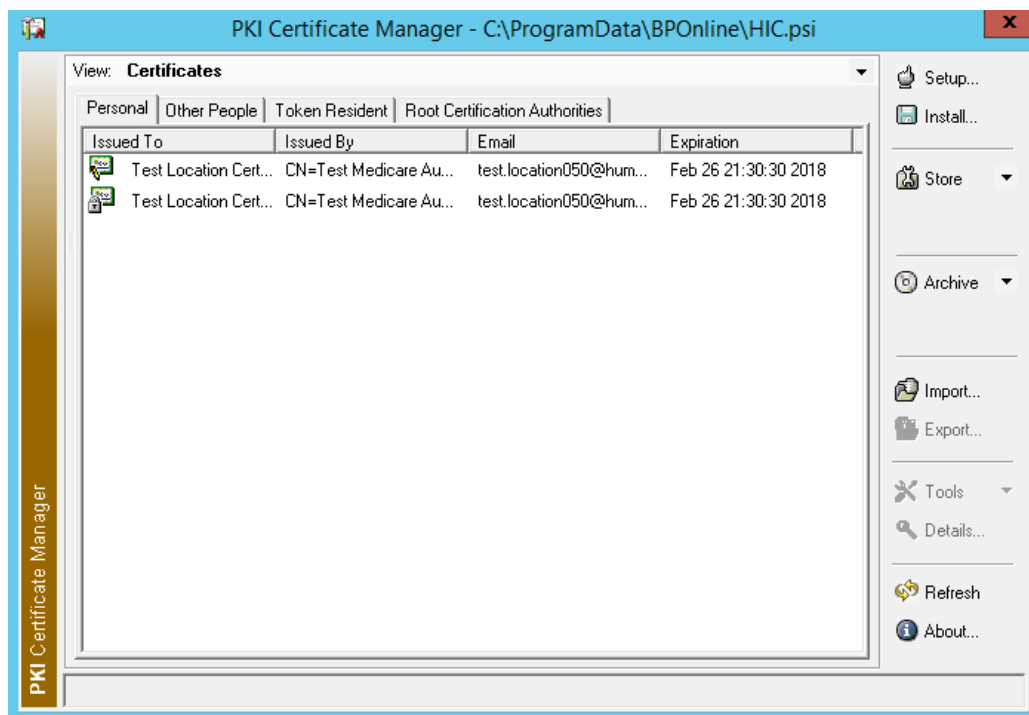
7. Leave the certificate manager open. Press [⊞ Windows key] + E to open a file explorer. Browse to the location of the public certificates that you downloaded in step 3 of **Download public digital certificates on page 17**.

8. Drag the Encrypt and Sign .cer public certificate files and drop into the PKI Certificate Manager. The certificate manager will prompt you for the Medicare site certificate PIC passphrase.

9. Enter the passphrase and click **OK**. The listed site certificates should have their **Expiration** value updated.

10. Close PKI Certificate Manager.

If you encounter any issues throughout this process, contact Human Services eBusiness on 1800 700 199, or email at **ebusiness@humanservices.gov.au**.

Bp Premier Support can be contacted on 1300 401 111, using options 1, 1. Or email at **support@bpsoftware.net**.

Export Medicare site certificates

Medicare site certificates can be used for:

- Access to Health Identifier services for HI lookups
- eRx Script exchange.

Medicare does not always distribute new certificate disks to practices that use Medicare Online when their certificates expire. Instead, Medicare provides a facility to renew the practice's certificates when sending and receiving claims.

Medicare certificates are used by eRx Script exchange for sending electronic scripts and by Bp Premier for HI Lookups. These certificates cannot be updated automatically by Medicare's renewal facility. You may be required to export the certificates using Medicare's PKI certificate manager.

More information on Medicare's PKI Certificate Manager can be found on the Department of Human Services website **here**.

Before you can export certificates

Identify the certificate store location

1. The Medicare Certificate store file is called **HIC.psi**. On the Bp Premier server, browse to c:\Program Data\BPOnline in a file explorer and check that a file called HIC.psi exists in the folder.
2. If the file is not in this location, log in to Bp Premier on the server and go to **Setup** > **Configuration** > **Online Claiming**.
3. Identify the path displayed in the **Path to Certificate store** field. The path will usually be a UNC path (for example, '\\servername\BPOnline').

Obtain PIC passphrase

Ensure you have the letter from Medicare that identifies the PIC passphrase for Online Claiming. The PIC password is linked to the store file and the practice certificates and is required to export certificates.

Install PKI certificate manager

1. If Medicare's PKI certificate manager has not been installed, download the certificate manager software from the **Department of Human Services**.
2. Unzip and install PKI Certificate Manager Software on the computer where the certificate store is located.

Identify the export folder

Create a new folder with a meaningful name on the server on which you installed PKI certificate manager. Use this folder to export the certificates.

You are now ready to export the certificates.

Export from PKI Certificate Manager

1. On the computer on which you installed PKI Certificate Manager, open the Windows Control Panel.
2. Double-click **PKI Certificate Manager**.
3. If this is the first time that PKI certificate manager has been used, the software will ask you for the location of the store.

   If the software does not ask, click on **Setup** on the right of the screen. Select **Use an Existing Store** and click **Next**.
4. Browse to the **Path to Certificate store** you identified. By default, the path should be **c:\ProgramData\BPOnline\HIC.psi**. Click **Finish**.
5. The **View Certificates** screen will appear. Click on the **Personal** tab to view all personal certificates held in this certificate store.
6. Highlight the first certificate that shows the practice name and click **Export**. The **Certificate Export** screen will appear.
7. Enter the PIC passphrase.
8. If the password is valid, the **Certificate Export** screen will appear. Browse to the folder where you want to export the certificates to.
9. Type in the filename **FAC_Sign.p12** and select the file type **P12**.
10. Click **Open** and tick **Include Private Key**.
11. Click **Next**.
12. Enter the PIC Passphrase again. Click **Finish**.
13. Repeat steps 6–12 for the other certificate with the practice name held in the store. However, at step 9, type in the filename **FAC_Encrypt.p12** instead and keep following the instructions.
14. Close the PKI Certificate Manager.

The certificates can now be used for HI Lookups or eRx.

Troubleshoot online claiming

If you are having trouble connecting and sending requests to Medicare online, Best Practice Software recommend that you contact your IT technician and work through the following possible errors and resolutions. If issues still exist, contact Best Practice support for further assistance.

Before you begin troubleshooting

Check all of the following common problems first:

1. Does C:\ProgramData\BPOnline exist?

   If not, download and run the **Bp Medicare Module** utility for your version of Bp Premier. Steps are described in the first troubleshooting entry in the table below.

2. If this machine is the server, does the **HIC.psi** file exist in folder c:\ProgramData\BPOnline?

3. Check **Help** > **About** > **System Info**. The variables at the bottom of the page must point to C:\ProgramData\BPOnline and not the old HIC folder.

4. Is the correct version of Java installed:
   - Bp Medicare V5 Module (for version Indigo) requires **Java 6 update 26 SE 6u26**

   Note: How to check the Java version depends on your Windows version. On Windows 8 and later, go to Start > Apps > Java > About Java. On earlier versions, go to Control Panel > Programs > Java.

5. Check there a file called **HicOnline-6.11-2.jar** in the folder C:\ProgramData\BPOnline\Lib.

6. Select **Setup** > **Configuration** > **Online Claiming** from the main Best Practice screen. Click **Check Certificate Expiry** to check that all certificates are current.

7. Check that the folder C:\Program Files\Best Practice Software\BPS\Medicare Certs exists on this machine.

Troubleshooting online claiming

Error Message	Issues and resolutions
Certificate Path could not be created	The BPOnline folder does not exist. To check, browse to the C: drive of the PC and look for the folder c:\ProgramData\BPOnline. If it does not exist: 1. Open the Best Practice Software website **www.bpsoft-ware.net** in a browser. 2. Select **Resources** > **Bp Premier Downloads** from the menu. 3. Under the **Utilities** section, click to expand **Bp Medicare V5 Module**. 4. Click **Download** to download the .exe file to the default Downloads folder, or right-click download and select **Save link as...** or **Save target as...** to download the file to a known location. Run the utility. This may require a reboot of the machine.
	The passphrase you have entered is not correct. Ensure that you are typing the PIC code from the letter you received from Medicare with your certificates.
Site Certificate could not be attached	The passphrase that was entered into Best Practice does not match the certificates. Check that the Medicare Disc has the same number as the PIC code document.
	The site certificates are not for this practice or they are expired.
PKI Certificate path could not be found	The configuration setting **Path to certificate store** on this workstation is not pointing to the BPOnline folder on the PC that MAOL was configured on first (\\server\BPOnline\). 1. Select **Setup** > **Configuration** > **Online Claiming** from the main Best Practice screen. 2. Check that **Path to certificate store** points to the correct BPOnline folder.
	The BPOnline folder on the PC where the certificate store is does not have sufficient permissions, or is not set to shared. On the PC, check that the BPOnline folder is shared and that 'everyone' has full access to this folder.
	Check the practice location is the first one in the database.

Error Message	Issues and resolutions
De-Secure Failure	The two SecureNet certificates were not imported during the Import Medicare certificates process. 1. Select **Setup** > **Configuration** > **Online Claiming** from the main Best Practice screen. 2. Click **Import Medicare Certificates**. 3. Click **Change folder**. Browse to the folder C:\Program Files\Best Practice Software\BPS\Medicare Certs and click **OK**. The system should show six certificates. 4. Double-click on each of the certificates to attach them to the system. If the system does not show six certificates: 1. Open the Best Practice Software website **www.bpsoftware.net** in a browser. 2. Select **Resources** > **Bp Premier Downloads** from the menu. 3. Under the **Utilities** section, click to expand **Bp Medicare V5 Module**. 4. Click **Download** to download the .exe file to the default Downloads folder, or right-click download and select **Save link as...** or **Save target as...** to download the file to a known location. Run the utility, which may require a reboot of the machine. This will place the six certificates needed into the Medicare Certs folder so you can import them again following the steps above.
Error 1014 Unable to Locate the EasyClaim PKI Class	The local machine environment variables are not set correctly. 1. Open the Best Practice Software website **www.bpsoftware.net** in a browser. 2. Select **Resources** > **Bp Premier Downloads** from the menu. 3. Under the **Utilities** section, click to expand **Bp Medicare V5 Module**. 4. Click **Download** to download the .exe file to the default Downloads folder, or right-click download and select **Save link as...** or **Save target as...** to download the file to a known location. Run the utility, which may require a reboot of the machine. This will set the variables required to point to Bp Premier.

Error Message	Issues and resolutions
	The **Path to certificate store** on this workstation is not pointing to the BPOnline folder on the PC that MAOL was configured on first (\\server\BPOnline\). 1. Select **Setup** > **Configuration** > **Online Claiming** from the main Best Practice screen. 2. Check that the **Path to certificate store** is set correctly. If not, click the browse button and browse to the folder on the server or workstation where the certificate store is located.
Error 1011 Unable to find Java Virtual machine library	The Bp Premier Medicare module requires a specific version of Java: ▪ Bp Medicare Module V5 (Indigo and later) requires Java 6 Update 26 (version 6.0.260) Browse to the folder C:\Program Files (x86)\Java folder and check if there is a folder called or **JRE6**. If the folder does not exist: 1. Open the Best Practice Software website **www.bpsoftware.net** in a browser. 2. Select **Resources** > **Bp Premier Downloads** from the menu. 3. Under the **Utilities** section, click to expand **Bp Medicare V5 Module**. 4. Click **Download** to download the .exe file to the default Downloads folder, or right-click download and select **Save link as…** or **Save target as…** to download the file to a known location. Run the utility and check the Java version again. If it is still incorrect, you may need to contact your IT support, because your user account may not have permission to install new software on your PC.

Error Message	Issues and resolutions
Error 9011 The software product used to create the transaction is not certified for this function. Contact the Medicare Australia eBusiness Service Centre for further assistance.	The local machine variables are not set correctly. 1. Open the Best Practice Software website **www.bpsoft-ware.net** in a browser. 2. Select **Resources > Bp Premier Downloads** from the menu. 3. Under the **Utilities** section, click to expand **Bp Medicare V5 Module**. 4. Click **Download** to download the .exe file to the default Downloads folder, or right-click download and select **Save link as...** or **Save target as...** to download the file to a known location. Run the utility, which may require a reboot of the machine. This will set the variables required to point to Bp Premier.
A problem has been encountered accessing PKI services. Ensure that the Medicare Australia and site certificates have been imported and they have not passed their expiry date.	Check that the practice has the correct Minor ID (Site ID) in the **Online claiming** screen.
	Most likely that the email address on the Medicare Certs is HIC rather than MedicareAust. Delete the Medicare certs and import them again from the BPS\MedicareCerts folder

Error Message	Issues and resolutions

	The wrong passphrase has been entered into Bp Premier, the certificates may be expired, or a change of practice name has caused a mismatch between the name on the site certificates and the name registered with Medicare.
	
	1. Select **Setup** > **Configuration** > **Online Claiming** from the main Best Practice screen.
	2. Click **Check Certificate Expiry**:
	3. If the expiry check produces an error, delete the **HIC.psi** store file and import the certificates into Bp Premier again.
	4. If the **Check Certificate Expiry** screen opens, check the expiry date for all the certificates listed.
	
	    If the site's certificates are expired, you must contact Medicare to obtain new certificates.
	
	    If the Medicare certificates are expired, update using the certificates provided by Best Practice Software. Follow the steps in De-Secure Failure on page 26 to update the Medicare certificates.
	
	5. From the Medicare online disc with the site certificates, copy the RA number that appears on the disc. The RA number can also be found by viewing the site certificate details from the **Check certificate expiry** screen.
	6. In an Internet browser, go to **http://www.certificates-australia.com.au/general/cert_search_health.sht,** type the RA number into the search box, and find the name that the certificates are registered to.
	7. Check that this is the same name used when submitting paperwork to Medicare to use Bp Premier for online claiming. If not, you will need to call E-Business, ask for the Revoke and Re-Issue certificates documentation, and fill the forms to get new site certificates.

Error 9111 If createCryptoStore - a PSI Store already exists in the nominated folder or A problem has been encountered using PKI services. Repeating the function call should be successful	Check the permissions for the c:\ProgramData\BPOnline folder on the PC. Check that the file **HIC.psi** exists in this folder and also has the correct permissions. Check that the folder is shared and that 'everyone' has full control of this folder and the subfolders and files.

Error Message	Issues and resolutions
	Can also be an issue with the wrong Medicare Certificates. Check the email address. If address is 'HIC', the wrong certificates are imported. Check that the certificates in the folder C:\Program Files\Best Practice Software\BPS\MedicareCerts are the latest. If not, run the utility **BP_MedicareCerts.exe**.
Error 9422 Clinical condition information missing or incomplete	The BPOnline folder on this machine does not have the correct files in the Lib folder or the path is pointing to the wrong path. Check the BPOnline folder to see if the file **HicOnline-6.11-2.jar** is there. If the file is not there: 1. Open the Best Practice Software website **www.bpsoft-ware.net** in a browser. 2. Select **Resources** > **Bp Premier Downloads** from the menu. 3. Under the **Utilities** section, click to expand **Bp Medicare V5 Module**. 4. Click **Download** to download the .exe file to the default Downloads folder, or right-click download and select **Save link as…** or **Save target as…** to download the file to a known location. Run the utility, which may require a reboot of the machine. The BPOnline folder and variables will be updated.

Error Message	Issues and resolutions
No Business Object for current user exists for the supplied session ID	The Medicare system variables aren't pointing to the correct path and an incorrect version of Java is installed. **Disable RX HIC online** 1. Log into RX. 2. Select **Utilities** > **Practice** > **Accounts tabs**. On the left hand bottom corner, make sure option **USE HIC ONLINE** is ticked. 3. Go to **Utilities** > **HIC online**. Delete the existing data path, leave the data path blank, and save. 4. Select **Utilities** > **Practice** > **Accounts tabs**. Untick **Use HIC online**. **Download and run Bp Premier Medicare utility** 1. Open the Best Practice Software website **www.bpsoft-ware.net** in a browser. 2. Select **Resources** > **Bp Premier Downloads** from the menu. 3. Under the **Utilities** section, click to expand **Bp Medicare V5 Module**. 4. Click **Download** to download the .exe file to the default Downloads folder, or right-click download and select **Save link as…** or **Save target as…** to download the file to a known location. This utility may require a reboot of the machine. This will install the BPOnline folder again and reset the environment variables. **Check system variable** 1. From the Windows desktop, press the Windows key + R to open the **Run** window. 2. From the command prompt, type 'set' and press Enter. 3. Find the string that reads 'java_jre_dll=C:\Program Files\Java\j2re1.4.2_17\bin\client\jvm.dll' and confirm it matches the one listed in RX.
The HCL Certificate used to sign the transmission is not the Certificate currently registered against the Location ID	This means that the Medicare location certificate that has been imported is not registered for Online claiming. Contact Medicare to confirm that you have the correct certificate for your practice.