Health Care Home Risk Stratification Tool

Installation Guide

Version 5.11.0

Contents

Requirements

It is recommended that each practice engage with their IT support staff to install the RST Tool and contact Precedence Support with any queries. Completion of each step of the installation is essential to enable functionality of the tool

Precedence Connector

The Risk Stratification Tool requires the installation and configuration of the Precedence Connector

Broadband Internet Connection

The Risk Stratification Tool requires an internet connection for the completion of each Patient Eligibility Certificate

Recommended Internet Speed

The minimum recommended internet speeds for the risk stratification tool are:

- Download speed: 3 Mbps
- Upload speed: 0.5 Mbps

Recommended Software Environment

- Windows 7 or higher
- Windows server 2008 R2 or higher
  Microsoft .Net Framework 3.5 must be installed prior to installing Precedence Connector for Windows Server 2008 R2.

https://www.microsoft.com/en-au/download/details.aspx?id=21

Recommended Internet Browsers

- Google Chrome version 39 (or higher)
- Firefox version 34 (or higher)
- Safari
- Microsoft Edge
- Internet Explorer 10 (or higher)

Compatible Practice Software

- Medical Director 3
- Best Practice (v.1.8.2 or higher)
- Zedmed (v.22.02 or higher)
- MedTech Evo
- MedTech 32
- Communicare (Installation guide available upon request)

Install Precedence Connector: Standalone Mode

Precedence Connector can be downloaded from the Precedence Health Care website:

1. Navigate to **http://cdm.net.au/help**
2. Select **Downloads** and then **cdmNet Desktop Software**
3. Click on **Run** to launch the Precedence Connector Wizard
4. Click on **Install** to start the installation (Figure 1)

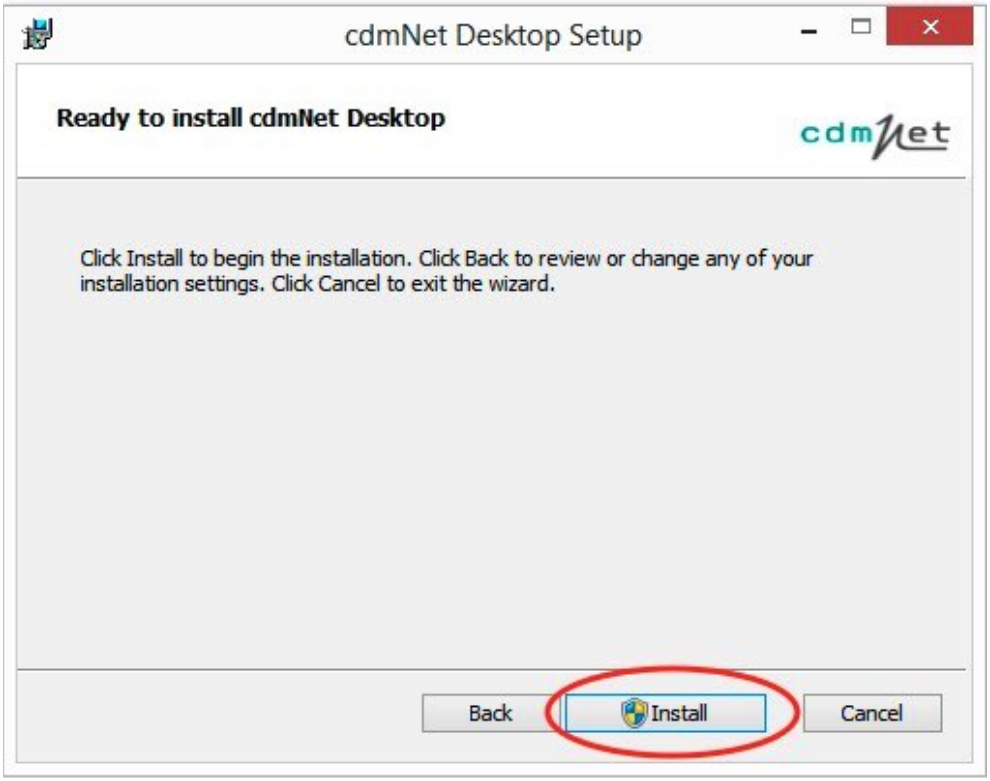

Figure 1: Click Install to start the Installation

5. Tick the box to accept the Terms of Use and click **Next**

6. Select the option **Install just for you** if you do not have Administrator privileges or **Install for all users of this machine** if you have Administrator privileges (Figure 2).

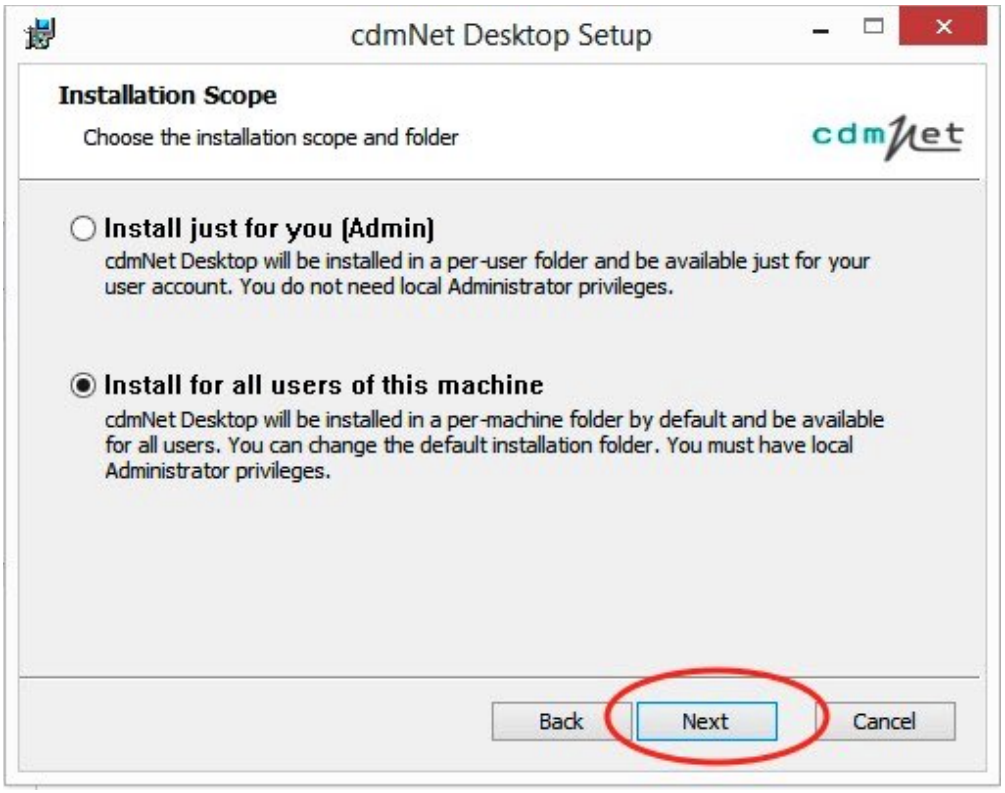

Figure 2 cdmNet Desktop Setup

7. Accept the default folder location or change to another folder location

8. Click on **Install** and then click on **Finish** to complete the installation process

Install Precedence Connector: Terminal Server or Citrix

The process for installing in a Terminal Server or Citrix environment is similar to the Standalone Mode

1. Follow the steps **Install Precedence Connector: Standalone Mode** to install cdmNet Desktop for all users on the Terminal Server or Citrix

2. Configure the Precedence Connector settings for each Terminal Server account (see Configure Precedence Connector Settings pages 14)

Install Precedence Connector: Server / Client Mode

The Precedence Connector can be installed on the server. Clients can then connect to, and store, the server settings. Please ensure you have the IP address of the designated server machine

Server Mode Configuration

1. Follow the steps **Install Precedence Connector: Standalone Mode** to install the Precedence Connector on the designated server machine

2. Click on the Precedence Connector application from the tray area and select **Settings** (Figure 3)

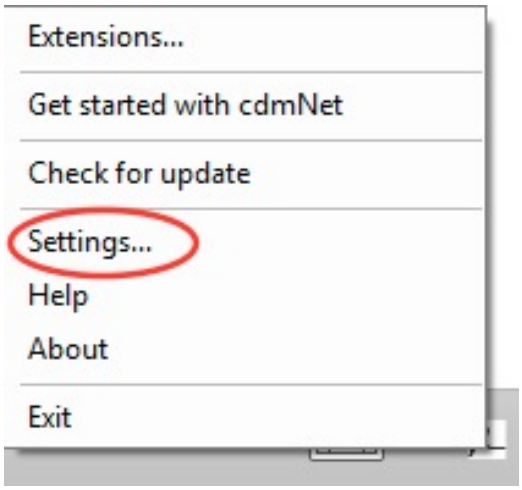

Figure 3: Settings

3. Click on **Advanced** and then **Change Operation Mode** (Figure 4)

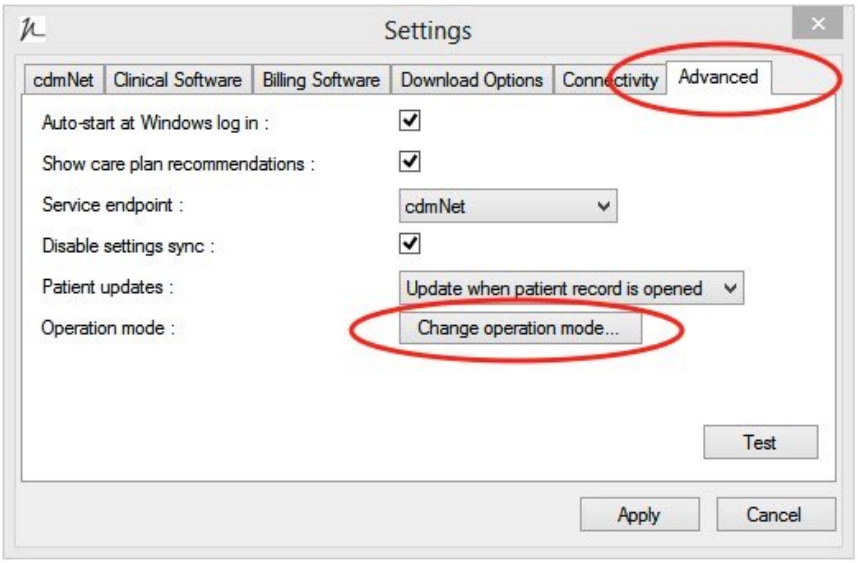

Figure 4: Change Operation Mode

4. Change to **Server Mode** and click on **Close** (Figure 5)

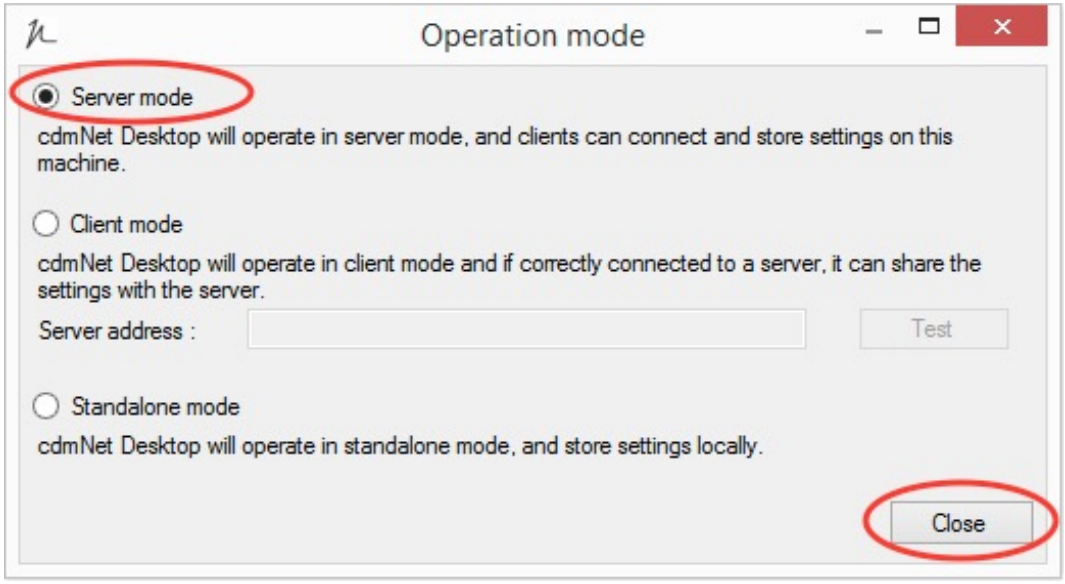

Figure 5: Change to Server Mode

Client Mode Configuration

1. Repeat the steps to **Install Precedence Connector: Standalone Mode** on any client machines
2. Click on the Precedence Connector application from the tray area and select **Settings** (Figure 3)
3. Click on **Advanced** and then **Change Operation Mode** (Figure 4)
4. Change to **Client Mode** and enter the server IP address
5. Click on **Test** and if correct click on **Close** (Figure 6)

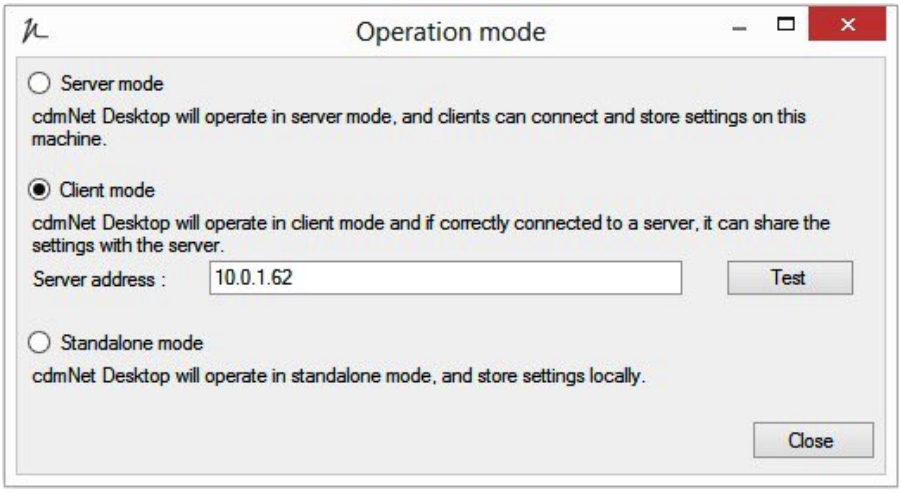

Figure 6: Change to Client mode and Enter the Server IP Address

Clinical Software Configuration

To allow the Precedence Connector to integrate with your clinical software, the following information must be configured in your Precedence Connector

Database server instance (Medical Director, Zedmed, Best Practice)
The Precedence Connector will make a best guess at the server name to connect to your clinical software. However, in some cases this will need to be configured manually. The database server instance should be the same as where the practice software has been installed

Medical Director Configuration

1. Click on the Precedence Connector application from the tray area and select **Settings**

2. Click on **Clinical Software** (Figure 7)

3. Select **Medical Director** from the drop down list

4. Check the **Database server instance** is correct

5. Click on **Test**

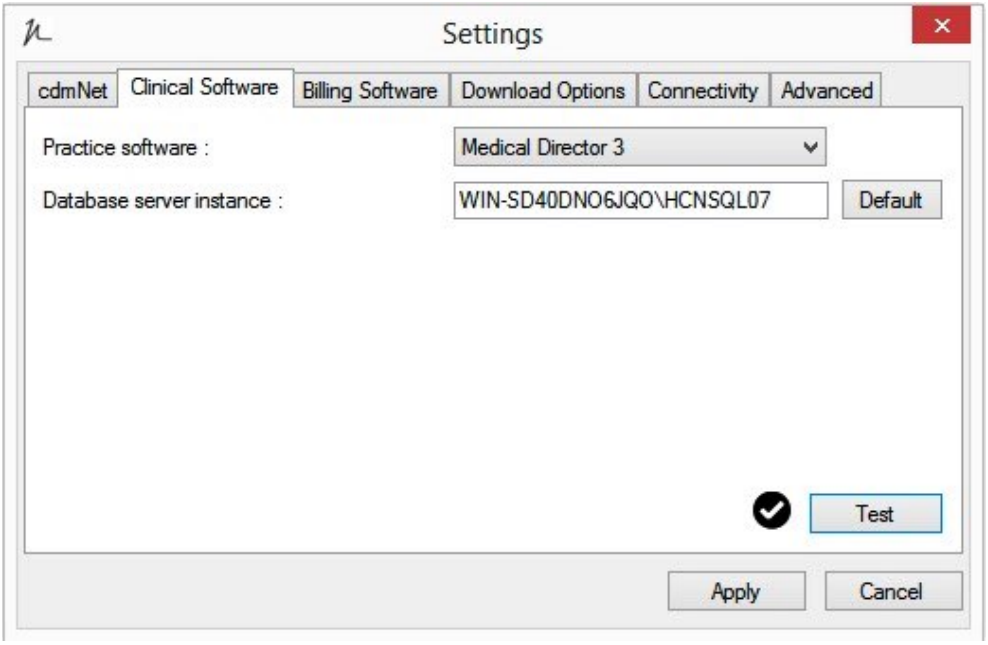

Figure 7: Medical Director 3 Configuration

Zedmed Configuration

1. Click on the Precedence Connector application from the tray area and select **Settings**
2. Click on **Clinical Software** (Figure 8)
3. Select **Zedmed** from the drop down list
4. Check the **Database server instance** is correct
5. Click on **Test**

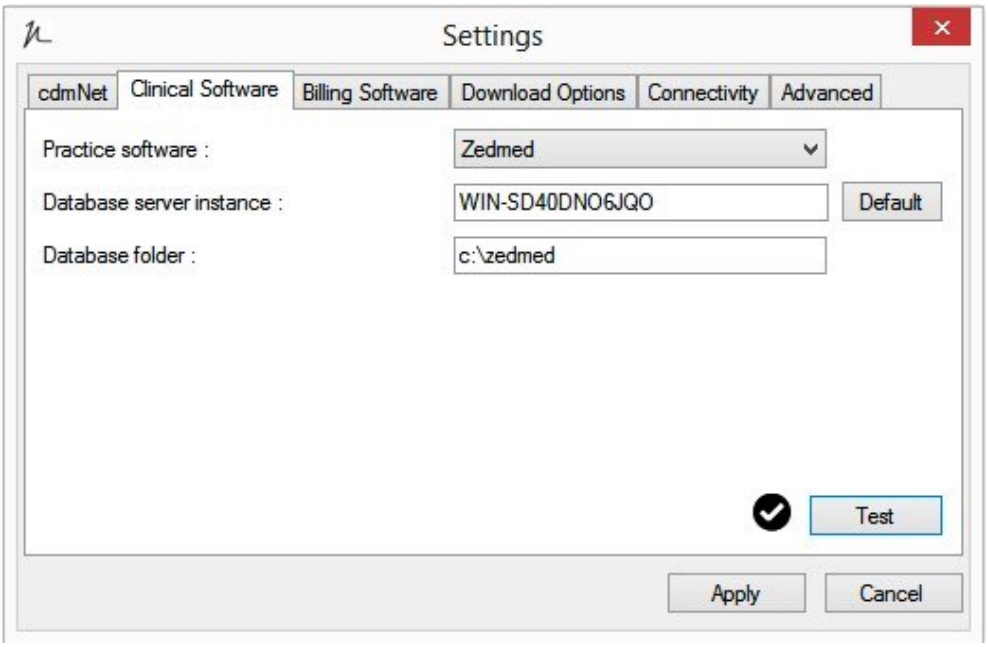

Figure 8: Zedmed Configuration

Best Practice Configuration

1. Click on the Precedence Connector application from the tray area and select **Settings**

2. Click on **Clinical Software**

3. Select **Best Practice** from the drop down list

4. Check the **Database server instance** is correct

Role based access roles
If Best Practice is version 1.8.2 or above you can enable access to the Best Practice database **without** a password.

To enable this:

1. Navigate to the **Setup** menu of Best Practice and select **Configuration**
2. Select **Database** from the left hand side
3. Next to **External data access** roles tick Clinical, Billing and Appointments and then **Save** (Figure 9)

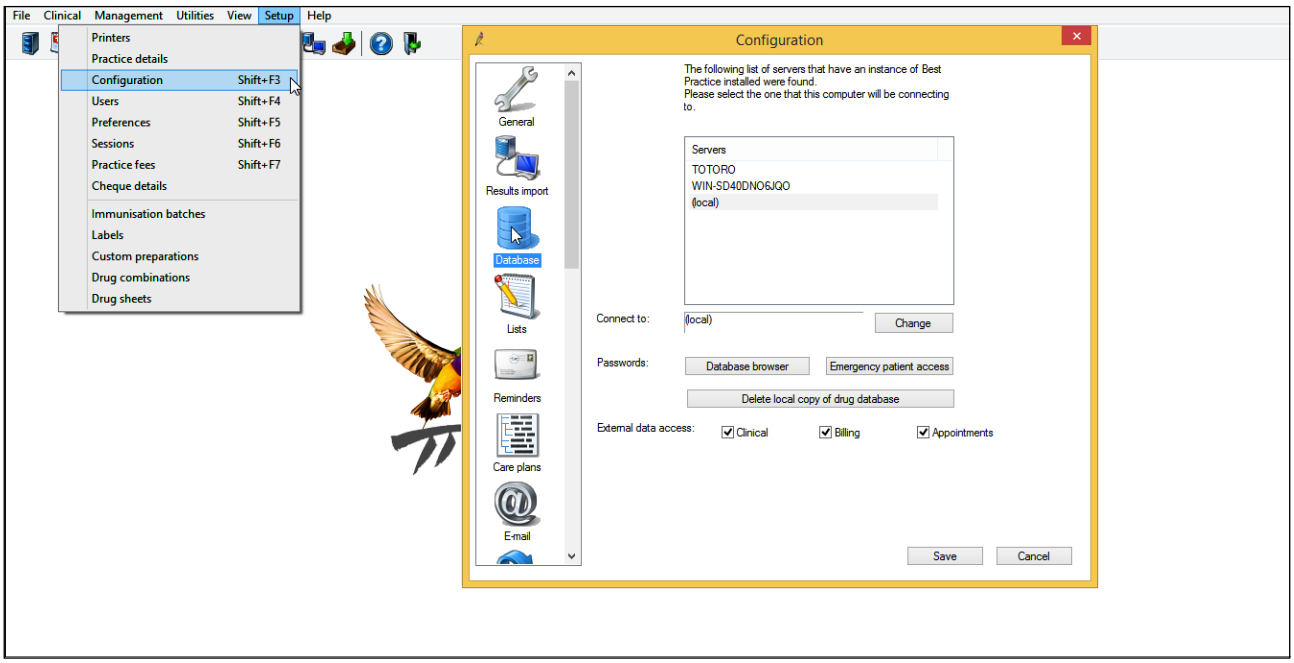

Figure 9: Enable External Data Access Roles

4. Click on the Precedence Connector application from the tray area and select **Settings**

5. Click on **Clinical Software**

6. Select **Use external data access** roles and click on **Test** (Figure 10)

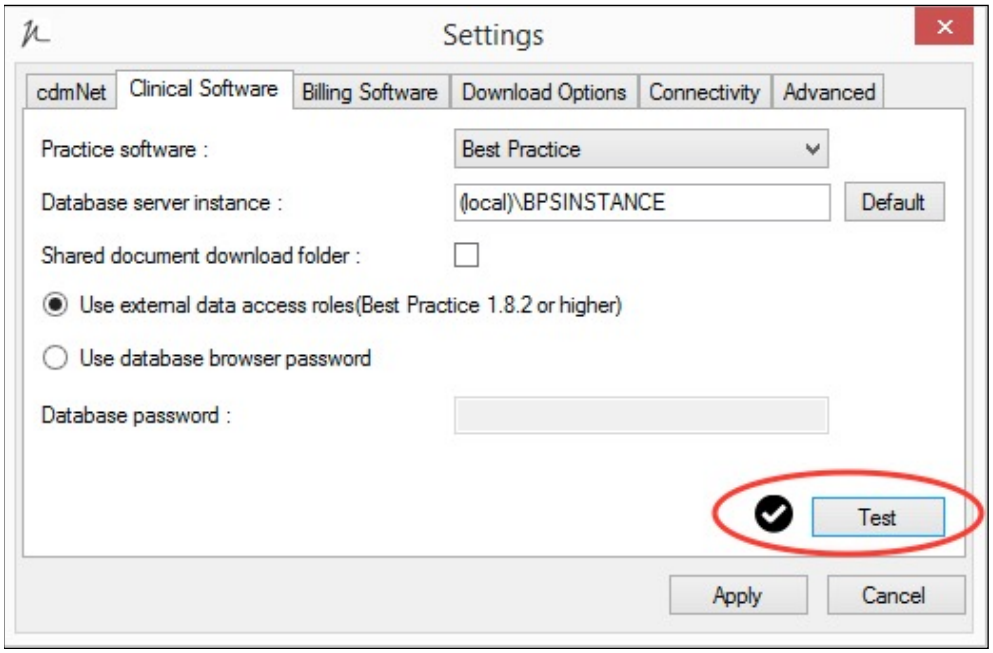

Figure 10: Use External Data Access Roles

Browser Password

If a password has been set for the Best Practice database:

1. Click on the Precedence Connector application from the tray area and select **Settings**
2. Click on **Clinical Software** (Figure 11)
3. Select **Best Practice** from the drop down list
4. Select **Use database browser password**
5. Enter the password and click on **Test**

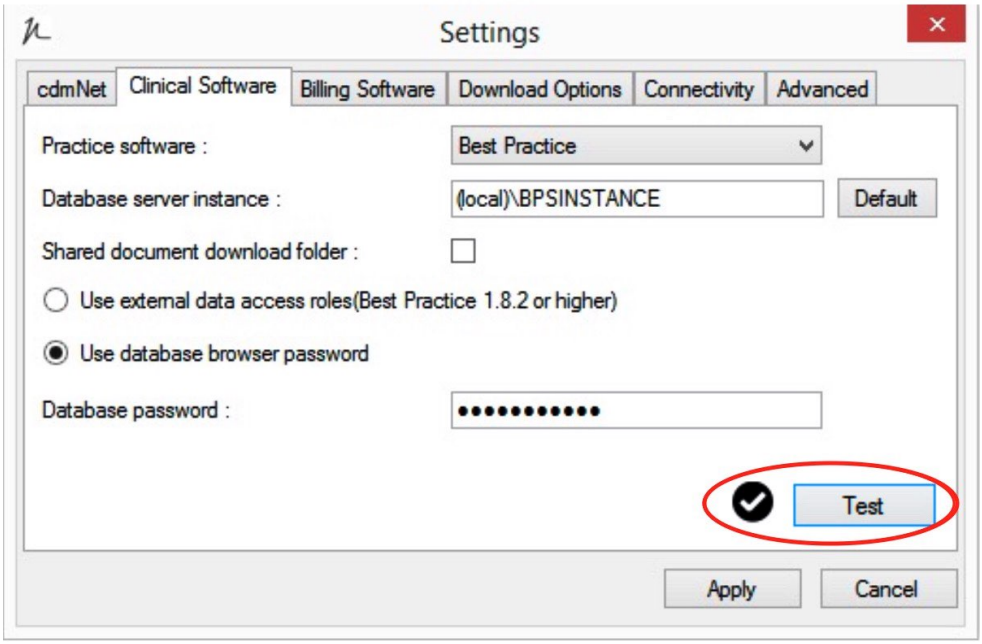

Figure 11: Use Database Browser Password

Configure User Settings

Once the Precedence Connector has been installed and the clinical software settings have been configured, please login to your clinical software.

1. Click on the Precedence Connector from the tray area and select **Settings** (Figure 12)

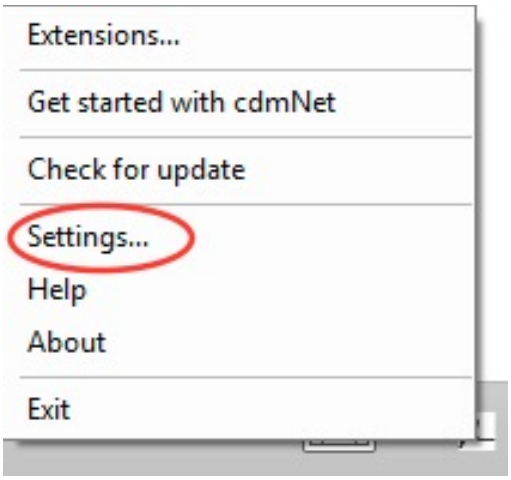

Figure 12: Precedence Connector Settings

2. Navigate to the **cdmNet** tab

3. Select the relevant user in the list clinical software user accounts (Figure 13)

4. Click **Edit**

5. Enter the username a password provided in the Health Care Homes registration form

6. **Save** and **Apply**

7. Repeat steps 3-6 until all user credentials have been saved in the connector

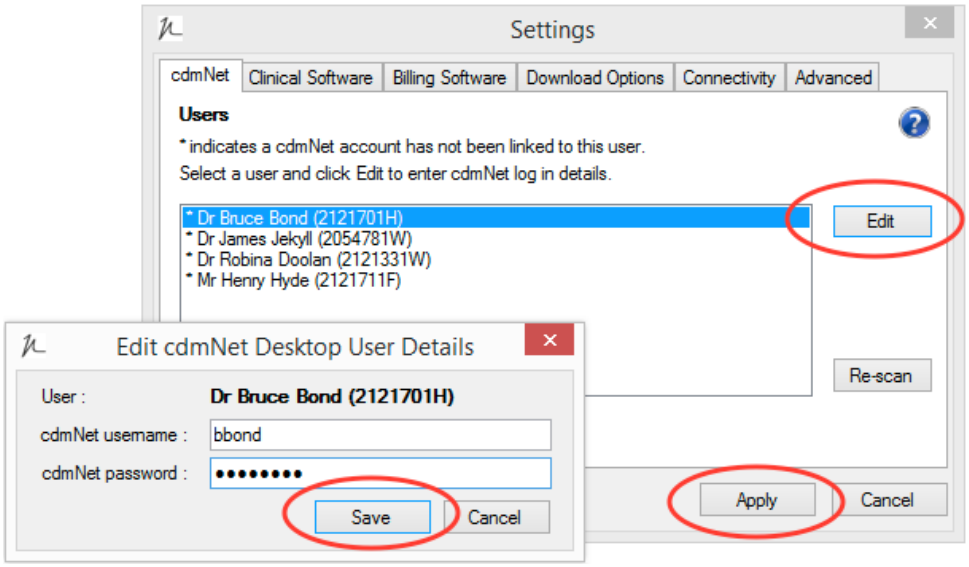

Figure 13: Save user credentials

Turn off care plan recommendations

This settings will need to be configured on the sever, if running Client/Server mode. Alternatively, please configure per machine.

1. Click on the Precedence Connector from the tray area and select **Settings** (Figure 12)

2. Navigate to the **Advanced** tab (Figure 14)

3. Untick 'Show care plan recommendations and **Apply**

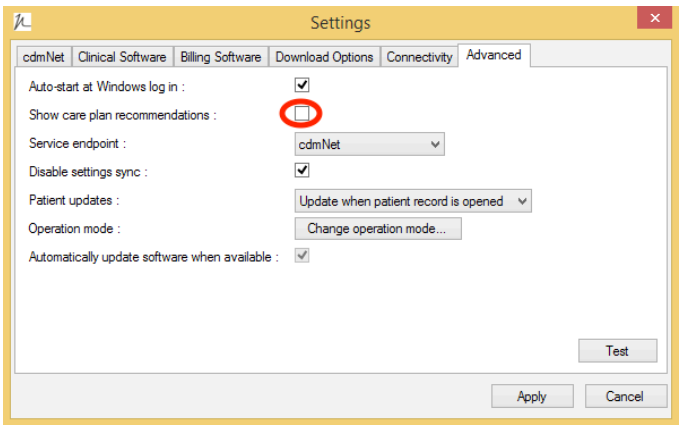

Figure 14: Untick 'show care plan recommendations'

Configure the Risk Stratification Tool

The Risk Stratification Tool must be configured through the Precedence Connector Extensions

1. Click on the small Precedence Connector icon in the task bar and select **Extensions**

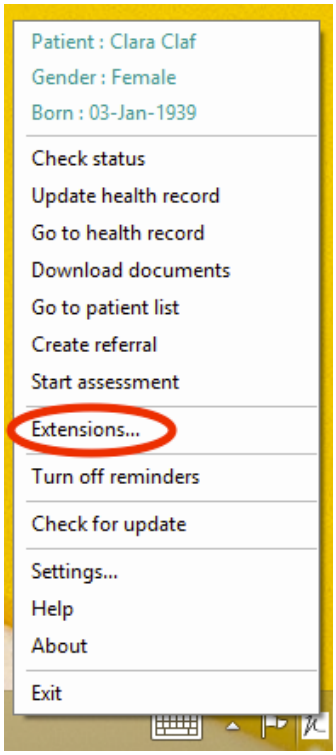

Figure 15: Extensions can be found through the Precedence Connector menu

2. Select **Configure…** next to Health Care Home Risk Stratification (Australian Government)

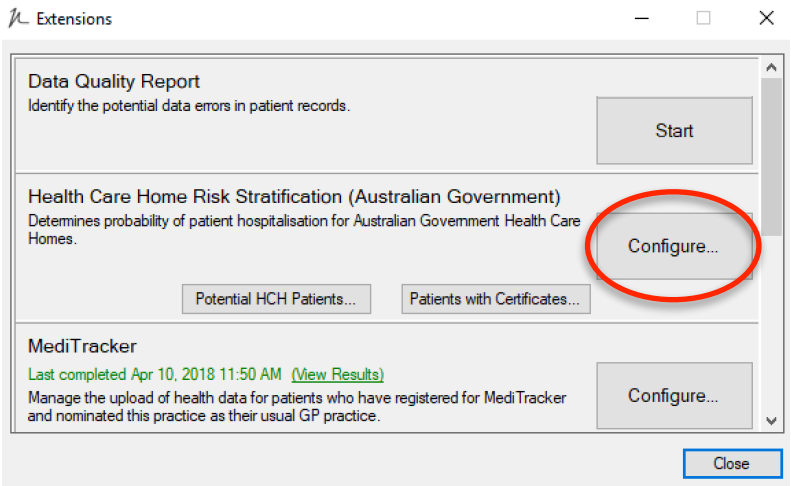

Figure 16: Overview of Extensions

3. Enter your user credentials, provided in the Health Care Homes registration form and **Save**. These credentials must first be configured in the users settings, outlined on page 15 (Figure 13). The credentials entered must belong to a user with access to **ALL** practice software records.

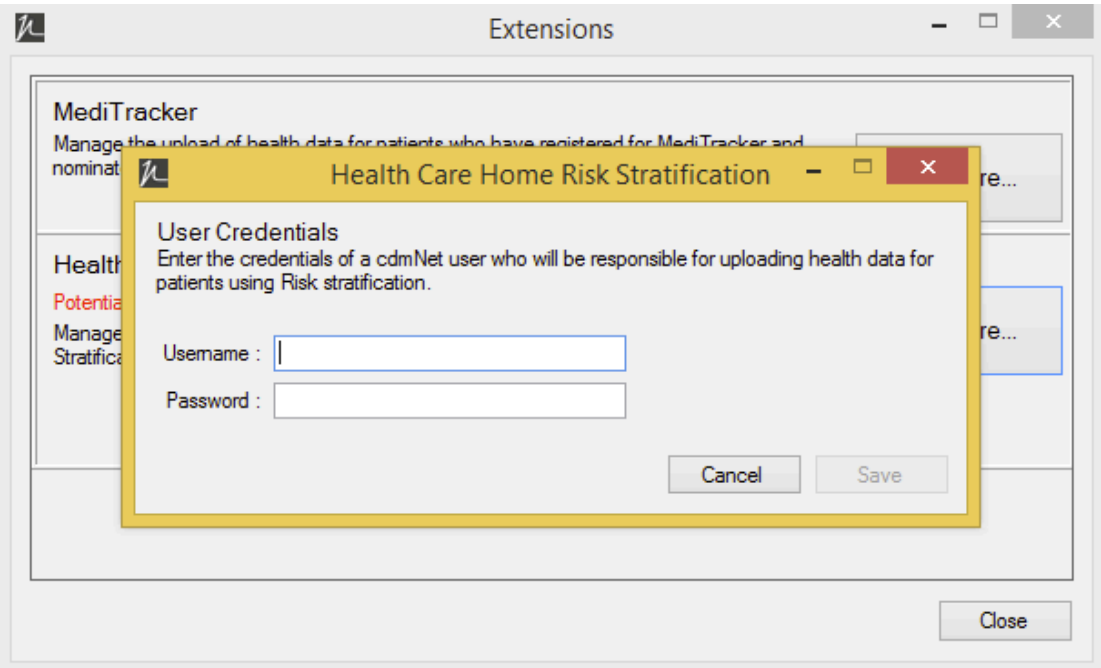

Figure 17: Enter user credentials

Configure Import Path

The Import Path will allow the Health Care Home Risk Stratification Certificate to be imported back into the practice software.

Medical Director

The Medical Director Import path must be set up **per MD login** and each user must have **their own** cdmnetdocuments[*MDuser*] folder

1. Create a folder for each user on the shared network titled **cdmnetdocuments[*MDUser*]**
   For example:
   //terminalserver/cdmnetdocumentsuser1
   //terminalserver/cdmnetdocumentsuser2

2. Login to Medical Director as User 1 and navigate to **Manage Communications** via the **Tools** menu

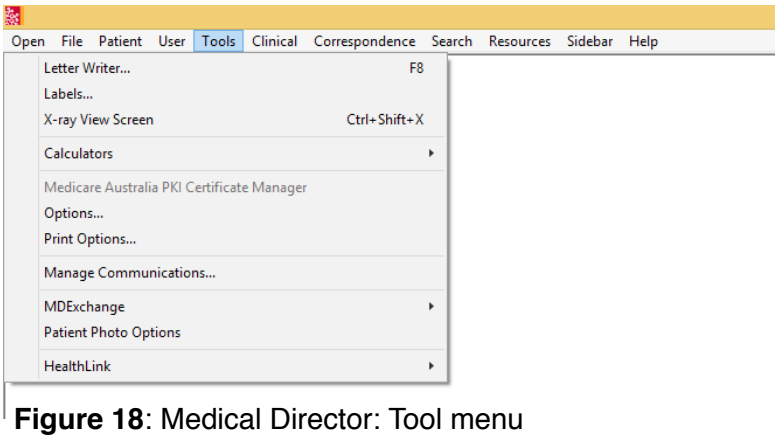

Figure 18: Medical Director: Tool menu

3. In the **General** tab, set the **Import Database** to Live Data. Next set the **Automatic Import Interval** to 2 minutes

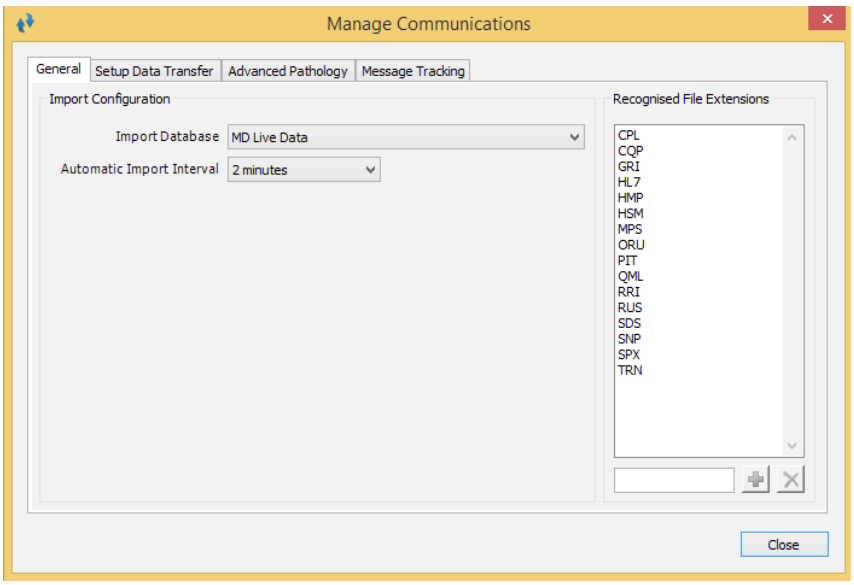

Figure 19: Medical Director: Manage Communications

4. In the **Setup Data Transfer** tab, click Add to open the **Setup Data Transfer Details** pop-up

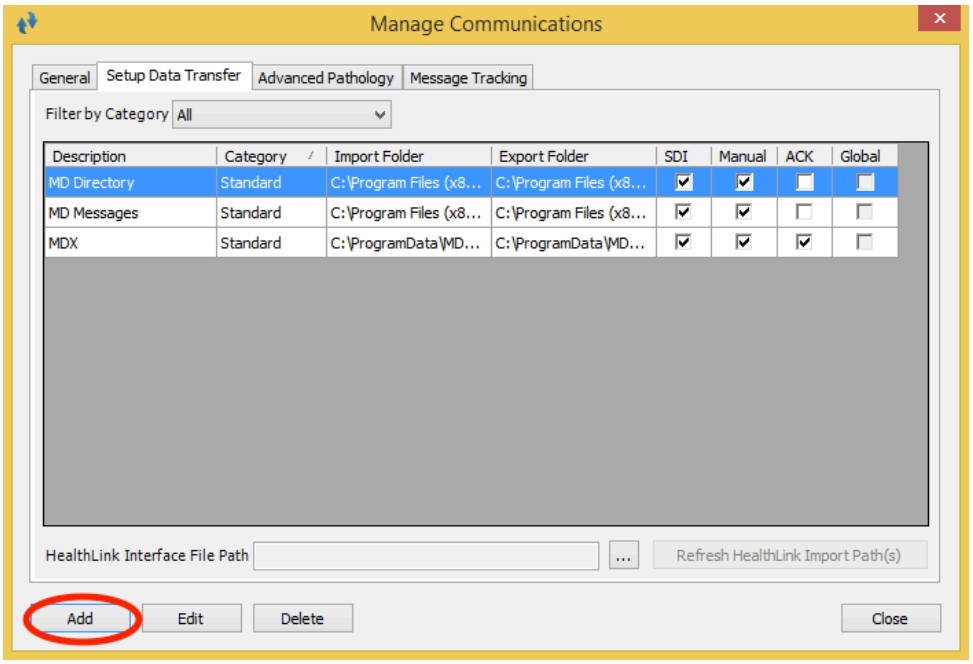

Figure 20: Setup data transfer

5. In both **Description** and **Categories**, please type the relevant file name e.g. **cdmnetdocumentsuser1**

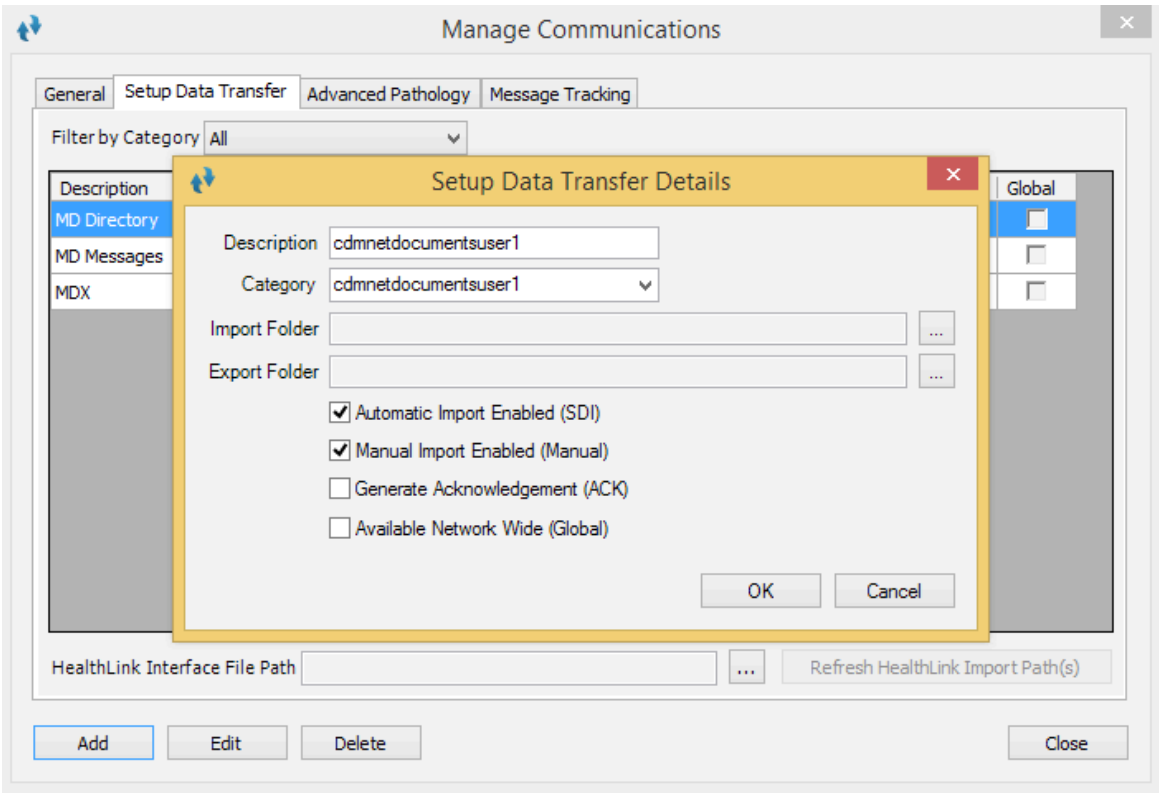

Figure 21: Edit search path details

6. Click the '…' next to both **Import Folder** and **Export Folder** to search and add your folder; **cdmnetdocumentsuser1** and select OK

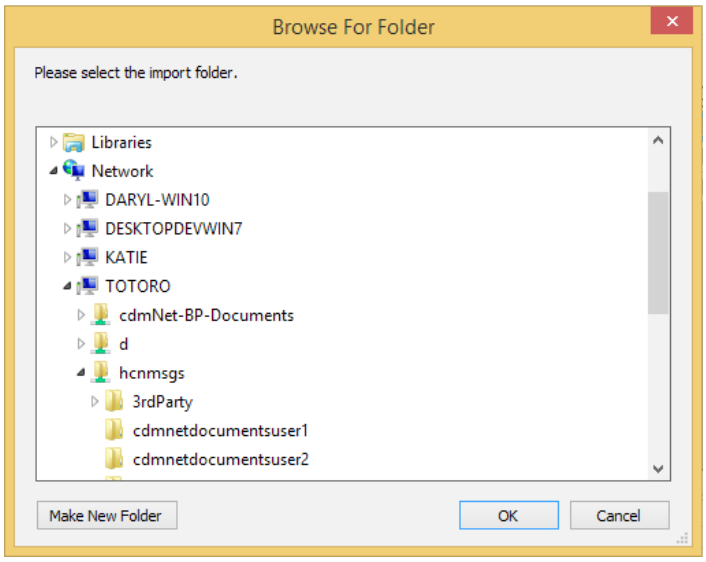

Figure 22: Search for folder

7. Ensure the **Automated Import Enabled (SDI)** and **Manual Import Enabled (Manual)** tick boxes are both ticked

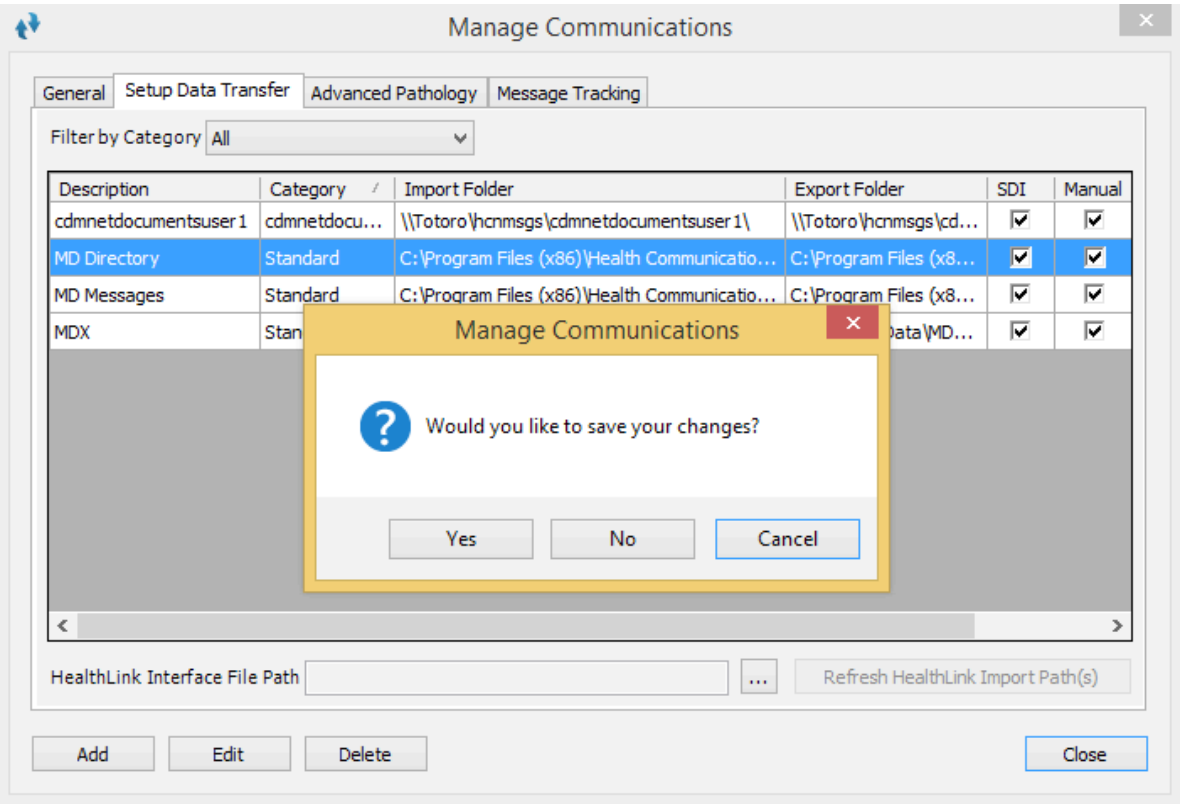

Figure 23: Save changes and Close

8. Select Close, then Yes in order to save your changes

9. Repeat for each MD login
Note: When you log in to User 2 and so on, you will be able to see the download path that has already been added for User 1 however this path will NOT be recognised for User 2 by MD

10. Once the certificate has been downloaded via the Precedence Connector, it can be found in the relevant practitioner's inbox in Medical Director, where it will need to be added to the patient record

Best Practice

The import path for Best Practice can be configured in two different ways depending on your set up; standalone machine or server environment

Standalone Machine

1. Create a folder on your desktop titled **cdmnetdocuments**

2. Login to Best Practice and navigate to **Configuration** through the **Setup** menu

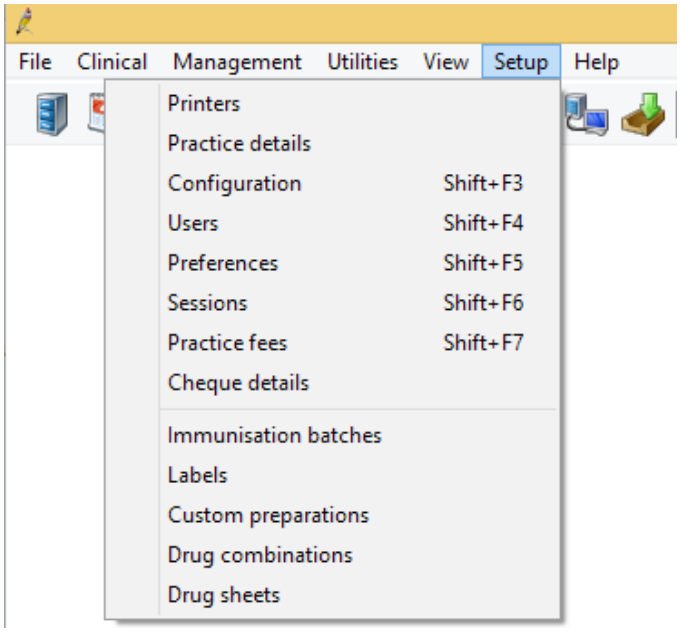

Figure 24: Best Practice set up menu

3. Click **Add** and search your computer for the file created in step 1; **cdmnetdocuments**

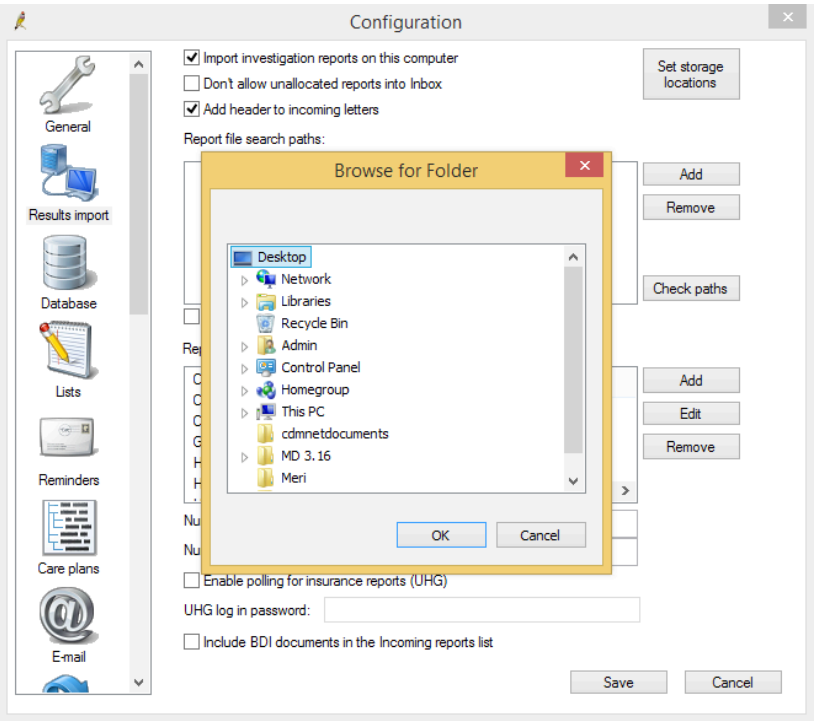

Figure 25: 'Add' cdmnet documents folder to Report file search paths

4. **Save**

5. Once the certificate has been downloaded via the Precedence Connector, it can be found in **Unchecked Reports** when the patient's file is open in Best Practice

6. Repeat steps 1-4 for each user profile/Windows login

Server Environment

1. Create a shared folder on the server titled **cdmnetdocuments**. All users must have rights to read and write to this folder.

2. Login to Best Practice and navigate to **Configuration** through the **Setup** menu (Figure 24: Best Practice Setup Menu)

3. Click **Add** and search your computer for the file created in step 1; **cdmnetdocuments** (Figure 25: Browse for cdmNetdocuments folder). Please ensure you are using a network path (rather than a local path)

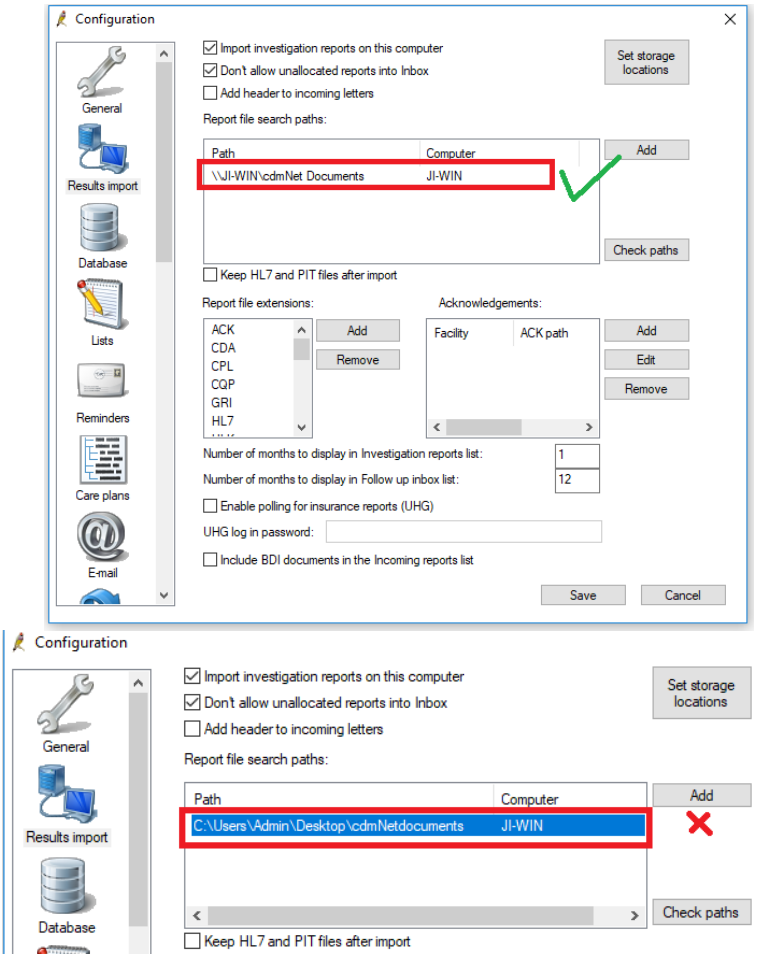

Figure 26: Add shared network path

4. **Save**

5. Open the Precedence Connector Settings and go to the **Clinical Software** tab

6. Tick **Shared document download folder** and **Apply**

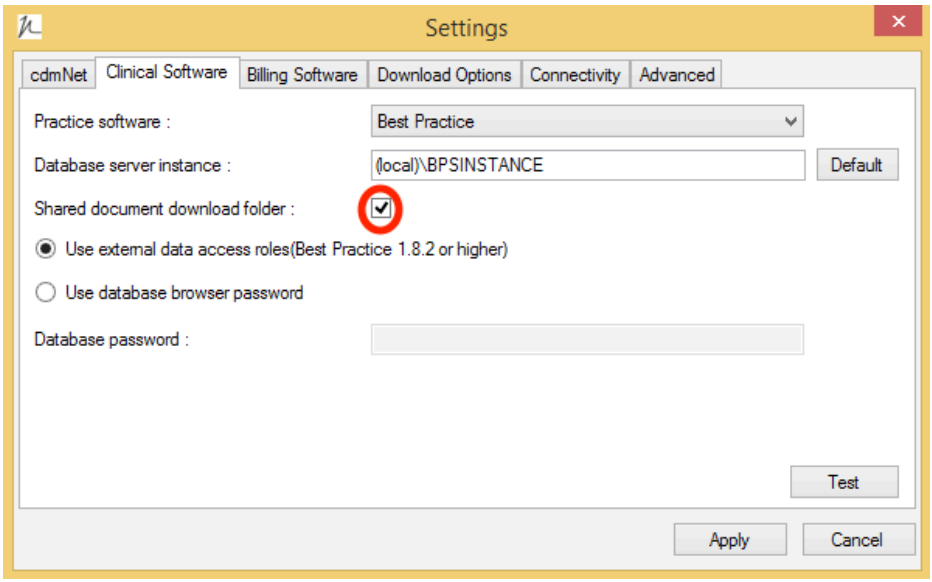

Figure 27: Precedence Connector: Clinical Software Settings

Zedmed

cdmNet Desktop sets up the functionality of this feature in Zedmed automatically. No extra settings are required in order for the certificate to be downloaded

Once the certificate has been downloaded via the Precedence Connector, it can be found through the patient's Zedmed record under Results - **Import Laboratory Results**

Testing

Once installation and set up is complete, please email Precedence Support (details below) to organise a remote access session to test the Risk Stratification Tool is working correctly. You will need to register one of the below listed test patients in your clinical software for the purpose of the test.

Name: John Test
DoB: 1st October 1955
Gender: Male
Medicare number: 3068 28021 1 /1

Name: Susie Test
DoB: 1st September 1960
Gender: Female
Medicare number: 4862 16089 1 / 1

Precedence Support

For further assistance or technical support please contact the Precedence Help Desk.

Phone: 1300 236 638 between 8.30am and 8.00pm (AEST Monday to Friday)

Email: support@precedencehealthcare.com