ReturnToWorkSA

V9.3.3 Release Notes

Medtech32 Australia

April 2016

These Release Notes contain important information for Medtech Evolution users. Please ensure that they are circulated amongst all your relevant staff. We suggest that they are filed safely for future reference.

Contents

For further information on this release, or any other queries regarding the **Medtech32 Version 9.3.3 ReturnToWorkSA new Certificate Update**, please contact the **Medtech Helpdesk** on **1800 148 165** or alternatively, email support@medtechglobal.com.

Prerequisites

Please review the following prerequisites and ensure they are met prior to running the update:

IMPORTANT NOTE

This update MUST be applied immediately after a successful upgrade to Medtech32 Version 9.3.3 Build 4999 (April 2016 – Release 2) has been completed. All database prerequisites and backup requirements would have then been applied safely prior to the update process.

- Ensure the minimum version and build requirements are met.

IMPORTANT NOTE

Your practice MUST be on Medtech32 VERSION 9.3.3 Build 4999 (April 2016 – Release 2) to install this update. If you ARE NOT currently on this version or higher, please DO NOT continue.

This can be checked by logging into Medtech32 and selecting *Help* ► *About Medtech32*.

- Ensure the person(s) who will be performing the update have **READ THROUGH** the release notes.

  IMPORTANT: This document contains valuable information that, if not read, could seriously affect the update process and/or possible down time of your network.

- Ensure you are ALWAYS logged onto Windows with **ADMINISTRATIVE RIGHTS** when performing ANY installation, update or maintenance tasks.

- Ensure ALL users (including remote users) have **LOGGED OUT** of Medtech32 and ALL scheduled utilities, backup or maintenance tasks that require access to the databases have been **STOPPED**.

- Due to compatibility issues, the **"Check for Updates Automatically"** option MUST be **DISABLED** in the Java Control Panel, as Medtech cannot guarantee that any future versions of Java will be compatible.

- **MAPI COMPATIBLE** e-mail client MUST be installed and configured on any Server or Client that needs to transmit SAWorkCover eWMC.

- Ensure you have the **Store Password** or **Location Pass Phrase** of the PKI Certificate Store (i.e. hic.psi) for Medicare Australia Online.

Introduction

This document provides an overview on how to install and replace your existing ReturnToWorkSA eWMC (Electronic WorkCover Medical Certificate), with the latest updated one for V9.3.3.

IMPORTANT NOTE RE: ReturnToWorkSA eWMC

While Medtech values the feedback received from our users in relation to changes within the Medtech32 software, it is important to note the following in regards to implementing any change requests for ReturnToWorkSA eWMC functionality:

All changes made to the Medtech32 application in relation to ReturnToWorkSA eWMC functionality have been made in accordance with ReturnToWorkSA and Medicare Australia specifications. Medtech is required to adhere to these specifications for the creation, storing, encrypting, transmitting and printing of eWMC in the Medtech32 application, and thus the information contained and detailed cannot be altered.

IMPORTANT NOTE

WARNING: It is HIGHLY recommended to employ ONLY qualified system engineers when performing ANY installation and upgrade. The consequences of ruining a database during upgrade could possibly lead to data corruptions and, as a result, data loss and systems downtime.

If in doubt, please consult with your IT technician/service provider, or contact one of the Medtech Channel Partners listed on our website:

http://www.medtechglobal.com/aus/medtech-online-au/support-3.html

NOTE: Please ONLY run the update when your site is not required to be up and running in a short amount of time. It is recommended to run the update after hours or on the weekend where you would have ADEQUATE TIME to complete the update.

NOTE: The amount of time required to run the update is dependent on the specification of your server and the size of ALL databases.

IMPORTANT NOTE

Current eWMC claims will be accepted until 30 Jun 2016 and ReturnToWorkSA has yet to provide Medtech with integration requirements for new replacement system.

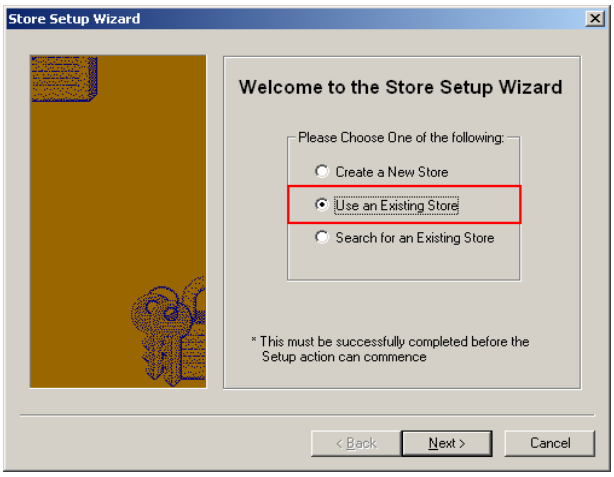
Certificate Update Installation

The Medtech32 ReturnToWorkSA eWMC Certificate Update must be run on the Medtech32 Server machine. The following procedures ONLY need to be run ONCE for EACH practice (or once per server if your practice has multiple servers).

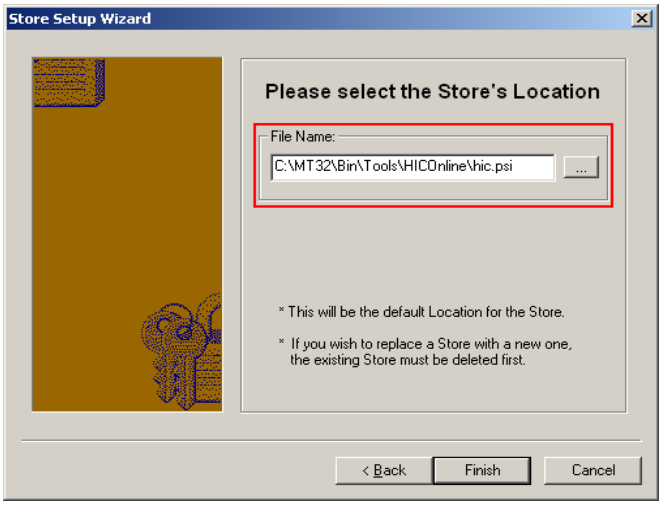
NOTE: If you are uncertain which computer is the Medtech32 Server, please contact your IT technician or service provider who has performed the Medtech32 installation and/or upgrade.

1. Go to **Windows Start Menu ▸ Control Panel ▸ PKI Certificate Manager**.

   If PKI Certificate Manager has not been previously used and configured under the currently logged in Windows user, the **Store Setup Wizard** screen will be displayed:



   Select the **Use an Existing Store** option, then click on the **Next** button to continue. The **Select the Store's Location** screen will be displayed:



Browse to or **Type** in the file path and file name of the existing PKI Certificate Store. By default, the file path should be located LOCALLY on the Server under the **C:\MT32\Bin\Tools\HICOnline** directory, and the file name should always be **hic.psi**.

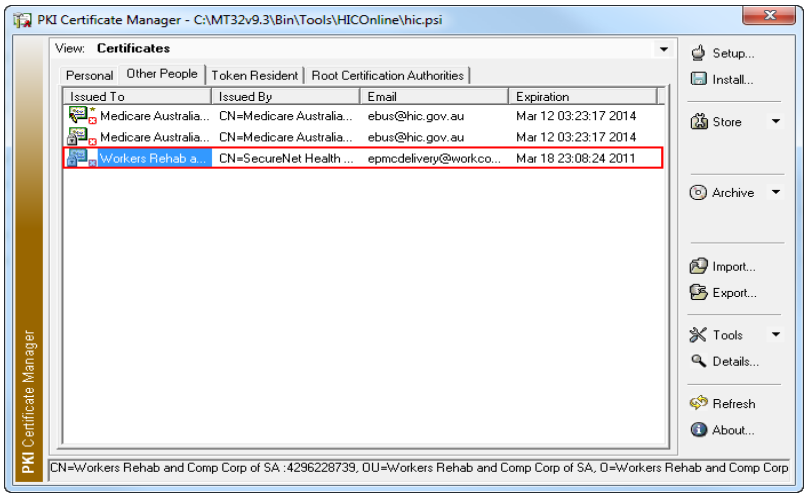
IMPORTANT: All Medtech32 users MUST be granted read/write/modify permissions to the **HICOnline** folder and its subdirectories.

If Medtech32 is installed on a different path, you MUST **Browse** to or **Type** in the correct file path where Medtech32 is installed.

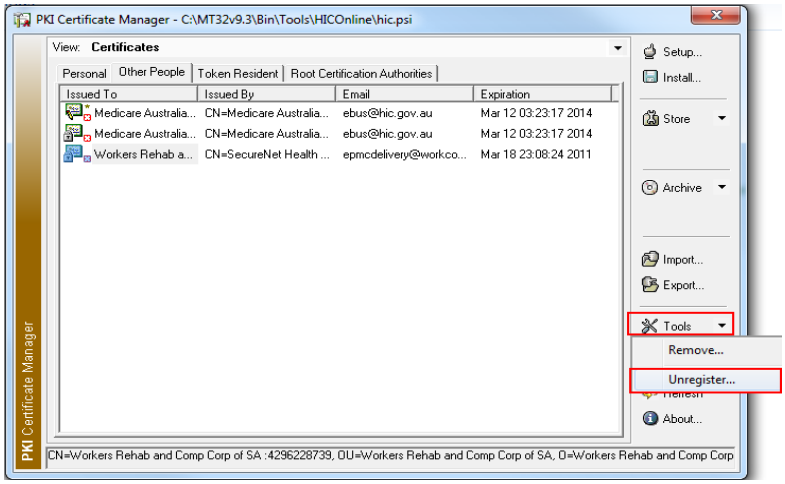
NOTE: If you are uncertain where Medtech32 is installed, please contact your IT technician or service provider who has performed the Medtech32 installation and/or upgrade.

Click on the **Finish** button to open **PKI Certificate Manager**.

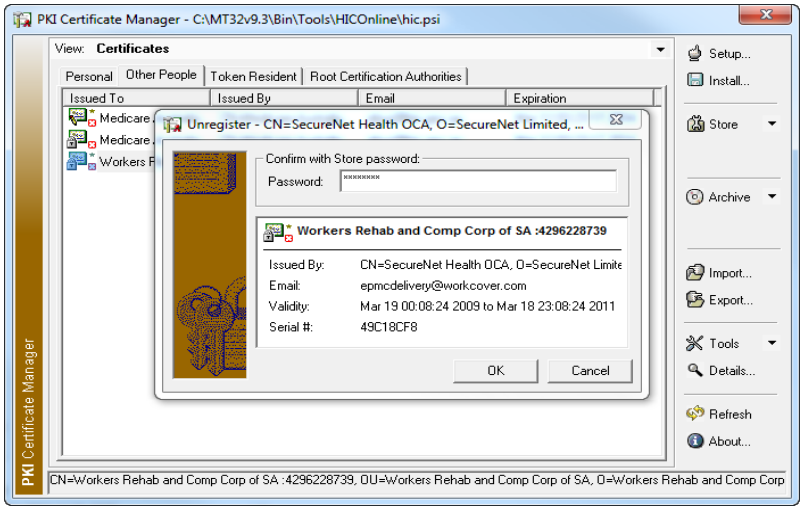
2. Select the ReturnToWorkSA Certificate from **PKI Certificate Manager** ▸ **Other People** tab.



Unregister the Old Certificate from **Tools** ▸ **Unregister**



Type in the **Store Password** you have originally created when setting up the PKI Certificate Store for Medicare Australia Online, then click on the **Next** button to continue.



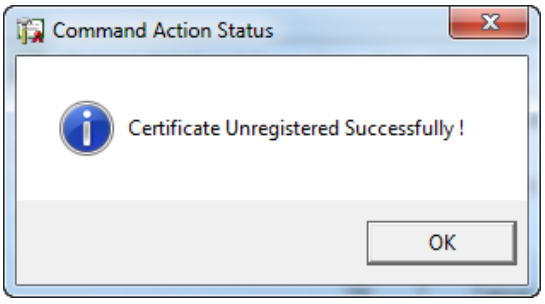
HINT: This is same as the **Location Pass Phrase** that you use within Medtech32 for Medicare Australia Online Bulk Bill and Repat Batching, Patient Claims and ACIR Registrations.

WARNING: The Store Password is required for installing the ReturnToWorkSA Certificate (and any renewal certificates in the future) and for generating, encrypting and transmitting eWMC Claims in Medtech32.

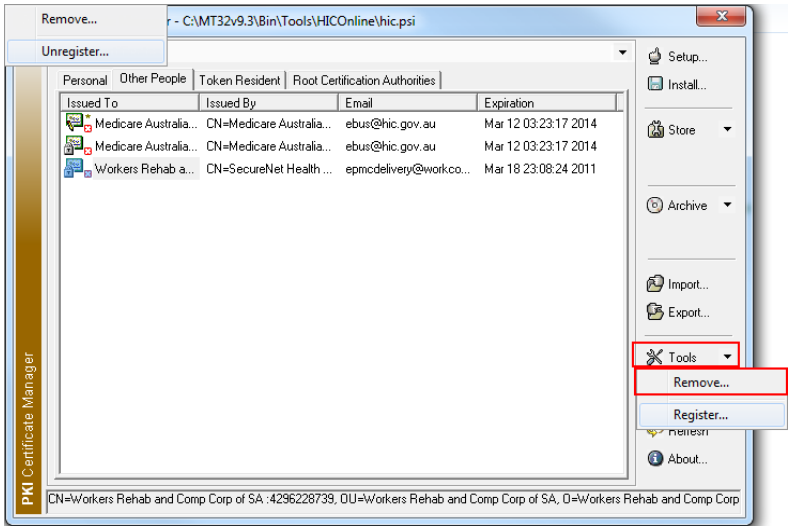
IMPORTANT: Please make note of the following rules from Medicare Australia in regards to the Store Password:

- Do not write this password down or tell anybody else this password. This password is important and must be protected.

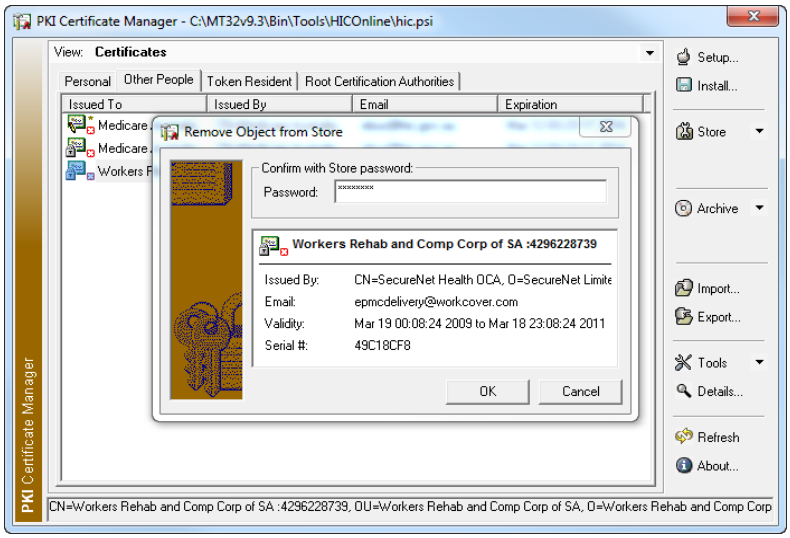
Certificate unregistered information message will be displayed



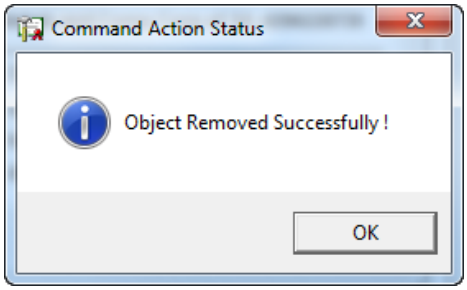
3. **Remove** the Old Certificate from **PKI Certificate Manager ▸ Other People** tab.



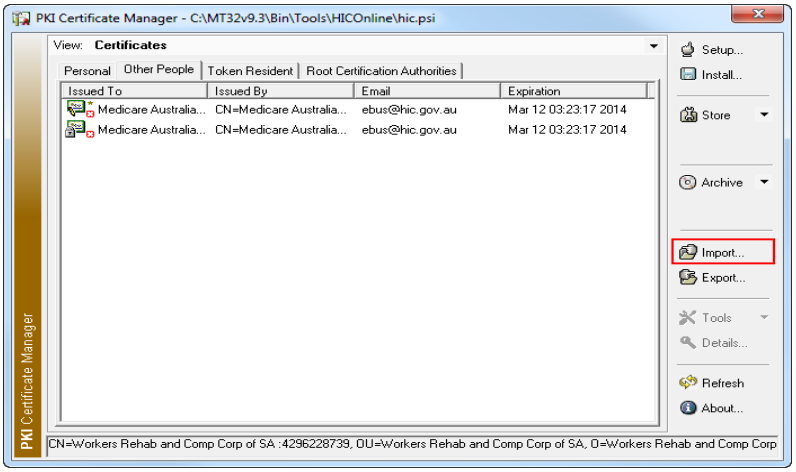
Type in the **Store Password** you have originally created when setting up the PKI Certificate Store for Medicare Australia Online, then click on the **Next** button to continue.



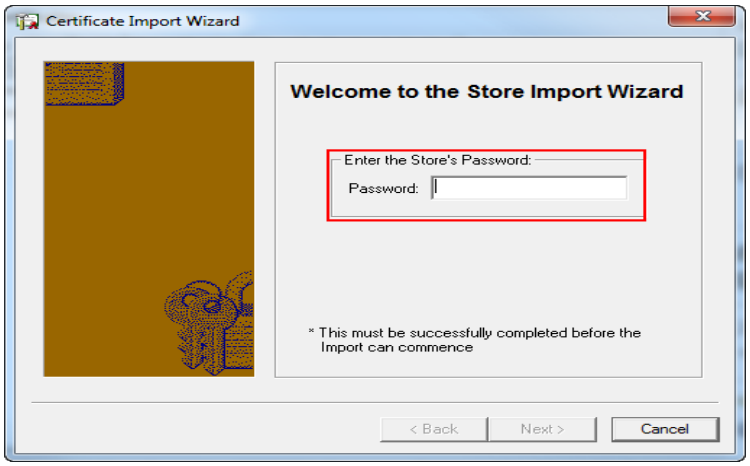
Certificate removed information message will be displayed



Click on the **Import** button to continue.

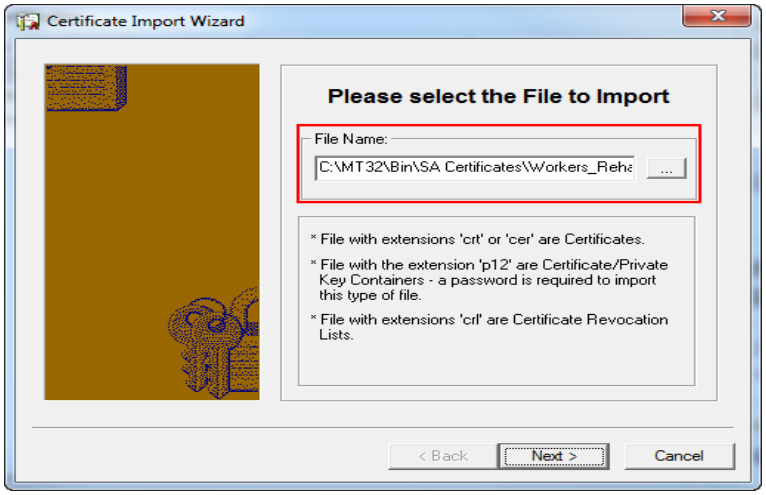


4. The **Store Import Wizard** will be displayed:



Type in the **Store Password** you have originally created when setting up the PKI Certificate Store for Medicare Australia Online, then click on the **Next** button to continue.

5. The **Select the File to Import** screen will be displayed:

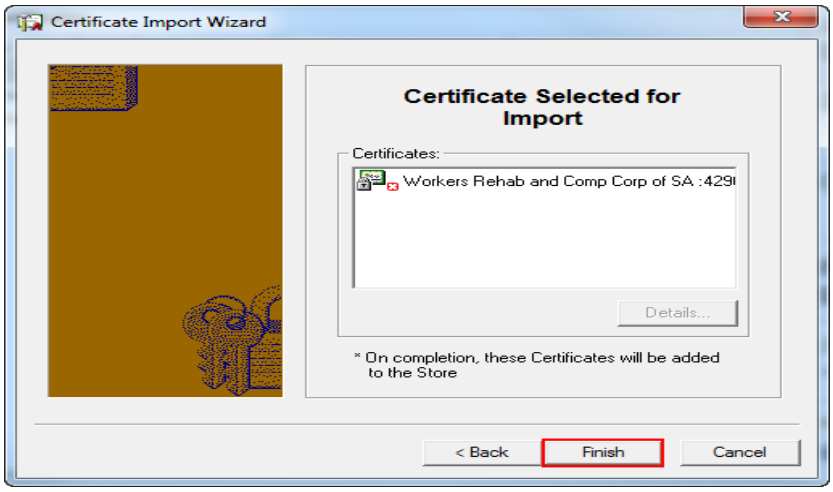


Browse to or **Type** in the file path and file name of the PKI Certificate File. The file path is located in the **Medtech32** installed folder under the **Bin\SA Certificates** directory, where the certificate file **Workers_Rehab_and_Comp_Corp_of_SA_Encrypt.cer** can be found.

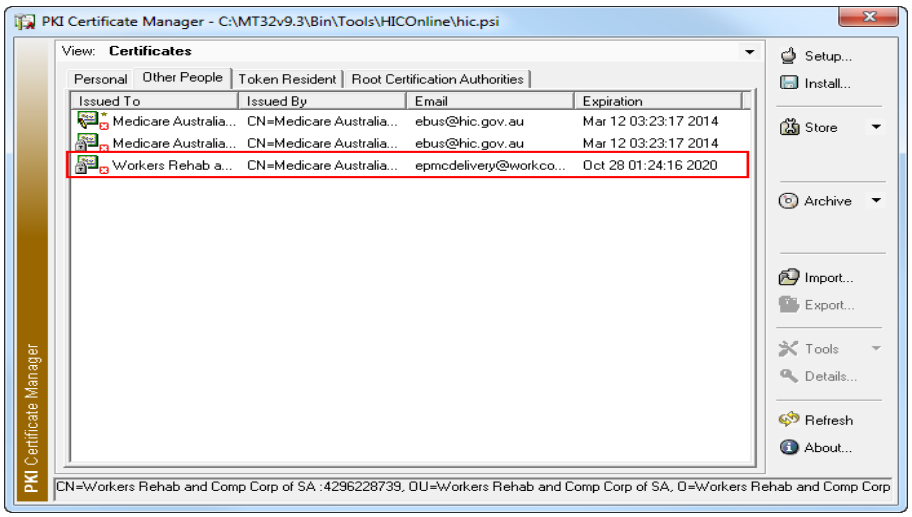
NOTE: If you are uncertain which computer is the Medtech32 Server, or the location of the Medtech32 application, please contact your IT technician or service provider who has performed the Medtech32 installation and/or upgrade.

6. Click on the **Next** button to continue.

7. Click on the **Finish** button to import the PKI Certificate File.



8. The ReturnToWorkSA Certificate will now be listed under the **Other People** tab with new expiry date.



Exit the PKI Certificate Manager by clicking on the button on the top right corner of the screen.

To ensure the certificate is properly registered in PKI Certificate Manager, transmit a eWMC claims to SA WorkCover using the new certificates after the update.

If you require more information or assistance, please contact Medtech Support:

- Via the Medtech32 application [Help ► Contact Support]
- Email: support@medtechglobal.com
- Phone: 1800 148 165