

Certificate Wizard Walkthrough

Overview

This guide is an indepth guide on how to generate a certificate using the Client Cert Request Util available [HERE](#).

Keeping the same directory



Keep the Client Cert Request Util in a centralised folder without moving between generating the REQ and KEY files, and then returning the Partial Certificate. Failure to do so will mean you will not be able to complete your certificate. Keeping in a single folder on the desktop or in documents will make things easier to keep track of.

Request a new certificate

1. Run the Request Util program and then select **Request a new certificate**.



- 1 Overview
 - 2 Request a new certificate
 - 3 Complete a returned certificate
 - 3.1 Import Completed Certificate Request into Windows
 - 3.2 Export to P12
 - 3.2.1 Install P12 into Windows
 - 3.2.2 The password you entered is incorrect
- 3.2.1 I mp ort nt poin ts for imp orti ng the certi ficat e to re- exp ort
- 3.2.2 I mp ort nt poin ts for exp orti ng the certi ficat e for use in olde r Ope rati ng syst ems.

2. Fill out the fields required with the relevant information, and continue clicking next.



Medical-Objects Client Certificate Wizard

File Help

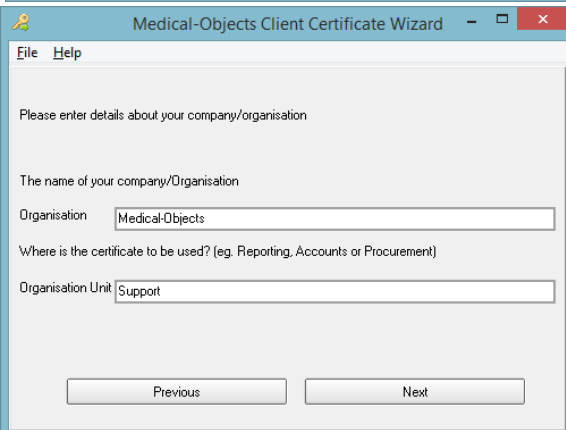
Please enter details related to the location the certificate will be used in.
If you are unsure of the location please use your company location.

Country: Australia

State: QLD

Suburb: Buderim

Previous Next



Medical-Objects Client Certificate Wizard

File Help

Please enter details about your company/organisation

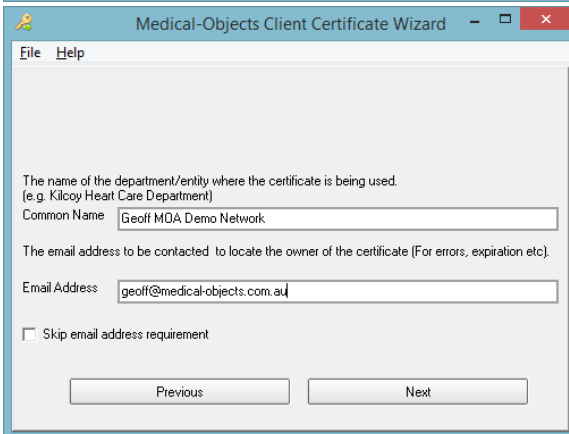
The name of your company/Organisation

Organisation: Medical-Objects

Where is the certificate to be used? (eg. Reporting, Accounts or Procurement)

Organisation Unit: Support

Previous Next



Medical-Objects Client Certificate Wizard

File Help

The name of the department/entity where the certificate is being used.
(e.g. Kilcoy Heart Care Department)

Common Name: Geoff MDA Demo Network

The email address to be contacted to locate the owner of the certificate (For errors, expiration etc).

Email Address: geoff@medical-objects.com.au

Skip email address requirement

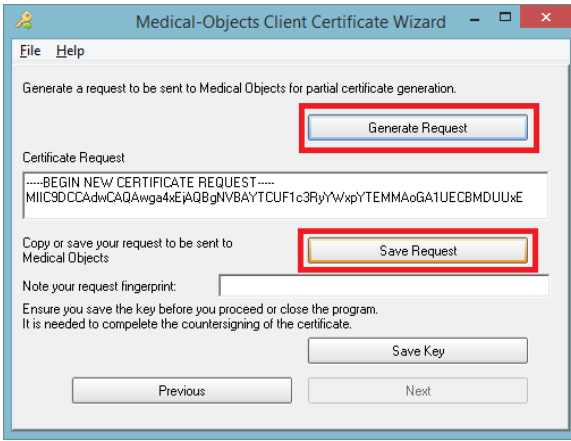
Previous Next

Common Name

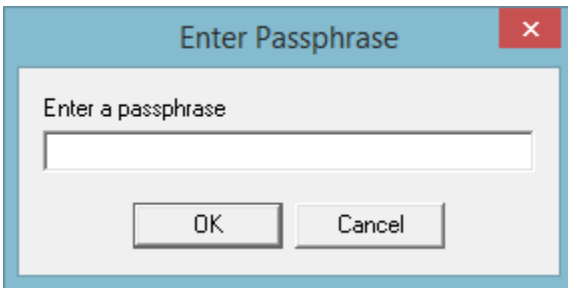


The **Common Name** field will be what shows up in the Certificate Selection screen in the browser. This common name should reflect the user you are generating the request for.

3. Click **Generate Request**, and then click on **Save Request** and choose a location to save the **Request File** (.req).



4. Click **Save Key** and choose a location to save the **Key File** (.key). Select a passphrase that will unlock the key upon returning the partial certificate (not the final password for login).



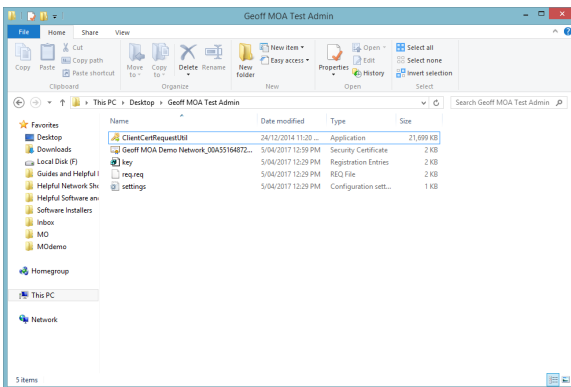
5. The saved **Request file** will need to be supplied to the Medical Objects staff member you have been in contact with so they can supply you the certificate for the next step.

WARNING

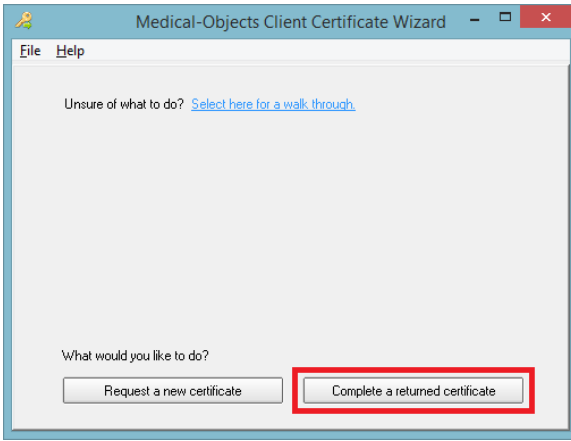
⚠ Never send your key file to anyone. Your certificate would be considered compromised and no longer suitable to secure connections. Please contact Medical Objects if this is the case to have your certificate reissued.

Complete a returned certificate

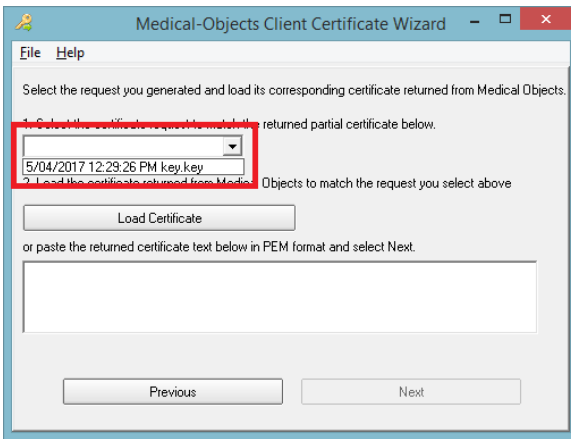
1. Download and move the returned partial certificate.cer file into the original directory that you ran the RequestUtil.exe from as previewed below:



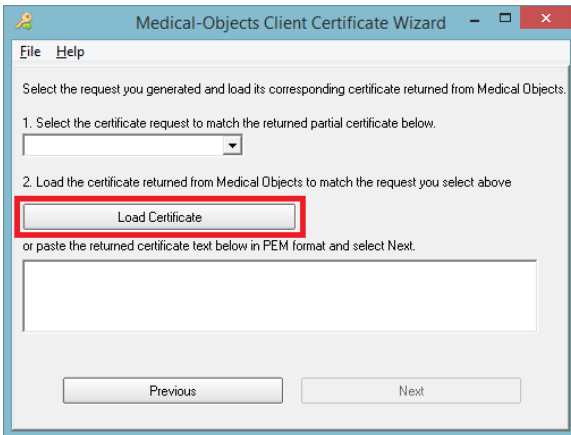
2. Run the Request Util program and then select **Complete a returned certificate**.

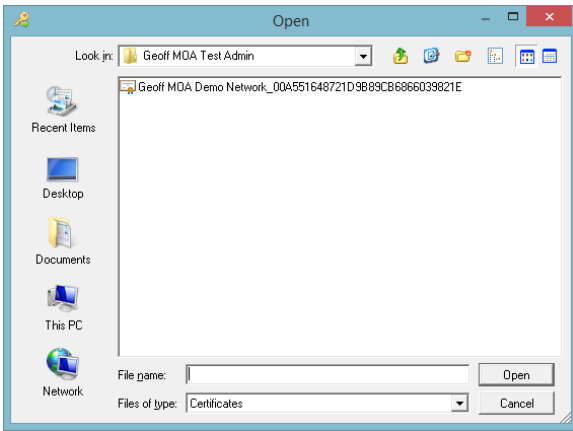


3. Select the corresponding Key file that correctly matches to the returned partial certificate.

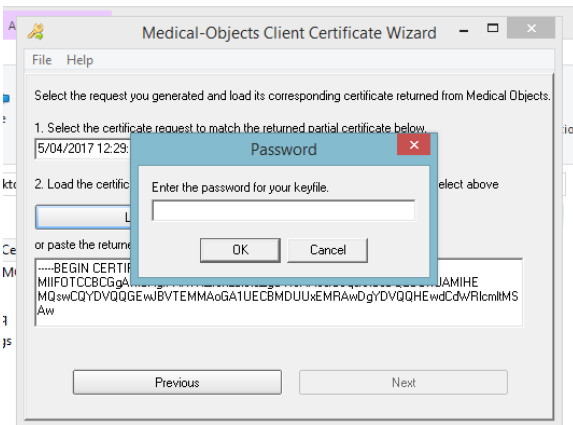


4. Click on Load Certificate and open the returned partial certificate file.

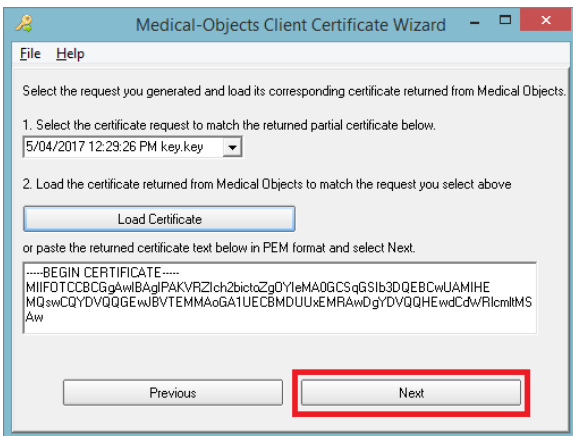




5. Enter the password of the **Key** file that you set earlier in **Step 4** of **Request a new certificate**.




6. Click **Next**.



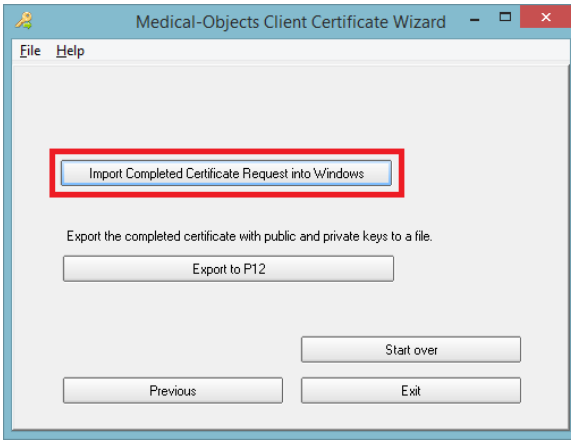
7. From here you can either import the certificate from within the wizard, or export the full certificate and import it once saved as a file.

Import Completed Certificate Request into Windows

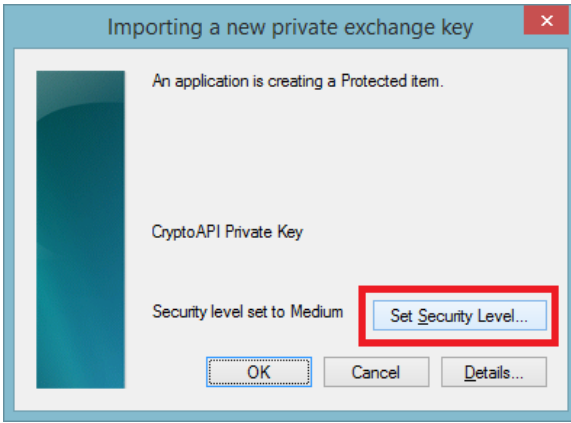
Warning

 This step is only required if you are using the certificate in Windows on the machine you are on and want to be prompted (This is a safer option) when the certificate is used. Subsection "Export to P12" is recommended instead if you have an automated system that can't supply a password to log into the certificate.

1. Select **Import Completed Certificate Request into Windows**.



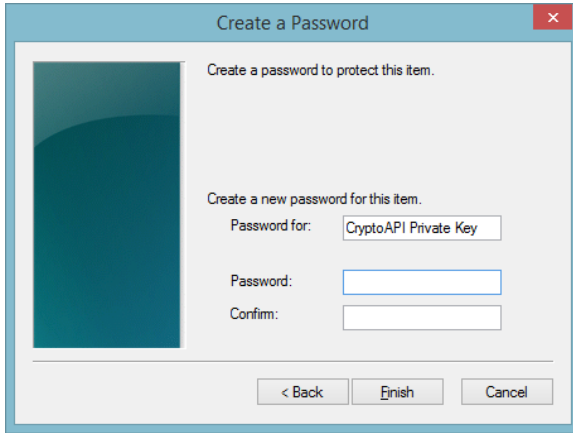
2. Click **Set Security Level**.



3. Change to **High**, and click Next.

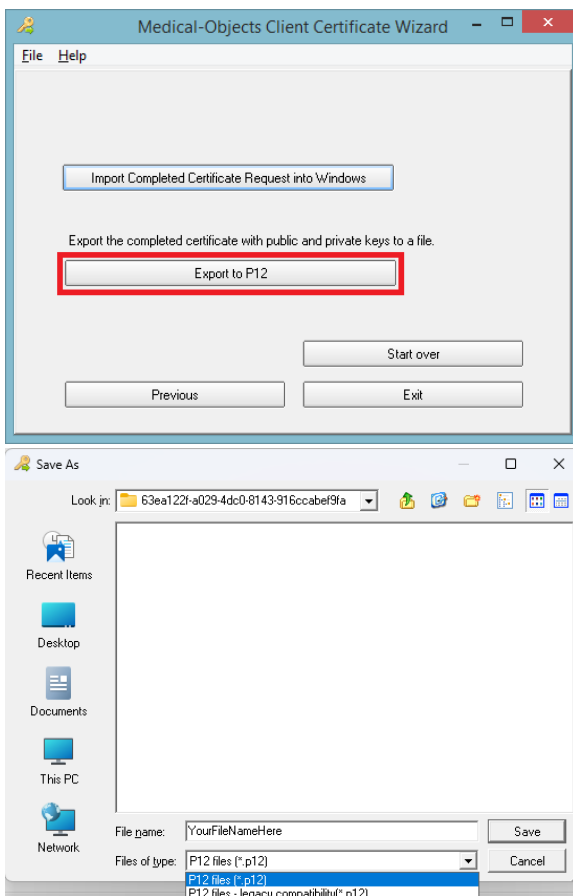


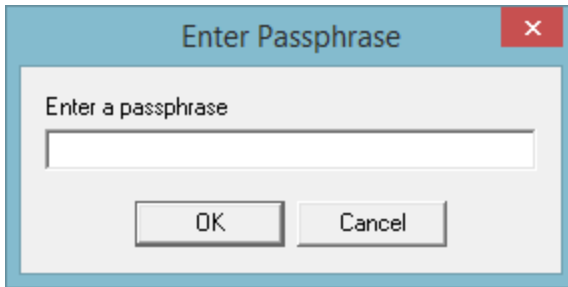
4. You will then be required to set a password that will be utilised when using the certificate to login. Once configured, click finish.



Export to P12

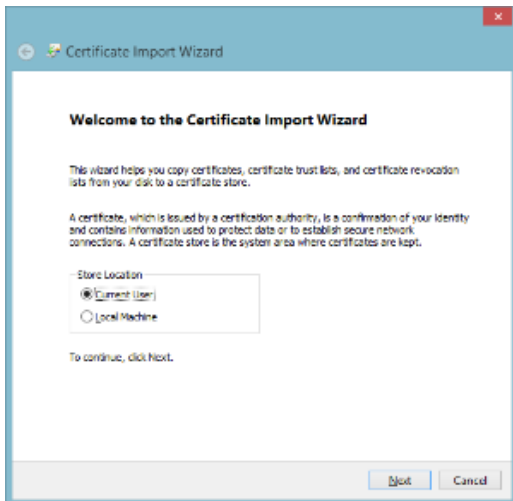
1. Select **Export to P12**, and choose a location to **save the file**, such as the folder you have been working in, and **set a password** that will unlock the certificate (not the final password). Note per the second screenshot when you choose where to save the file, and the name to save it as, you can also set the **Files of type** to **legacy compatibility** if you have an older version of Windows. You could Export to P12 twice and save in each format just in case. When you try to import the certificate into Windows and it won't accept the correct password this is the most likely cause.



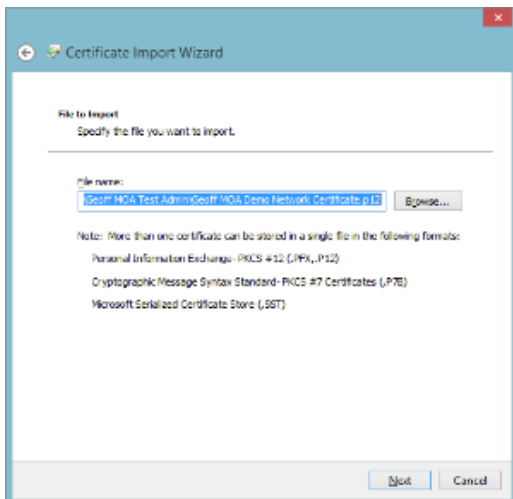


Install P12 into Windows

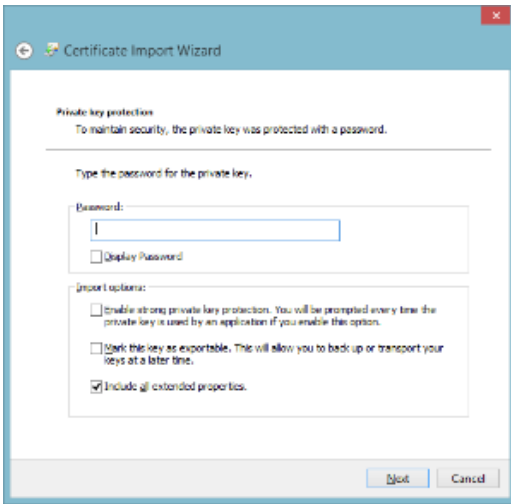
1. Double click the saved certificate, which should now start the Certificate Import Wizard (depending on Windows version). Keep **Current User** selected and click next.



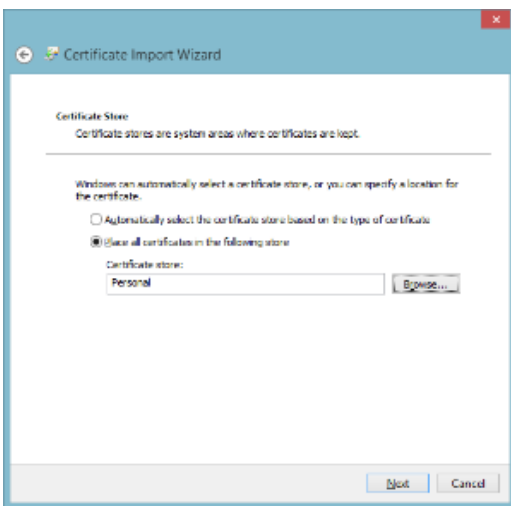
2. Leave file name as is, and click next.



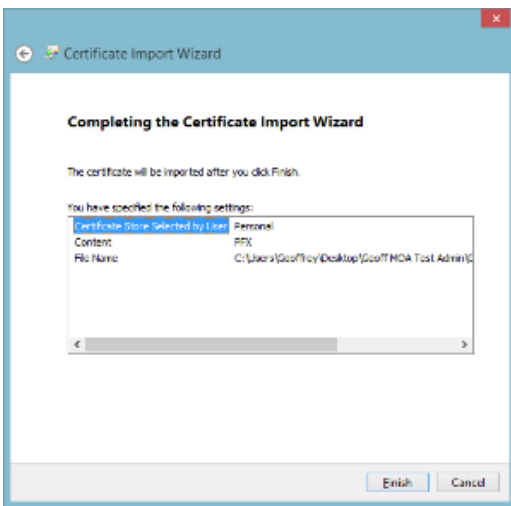
3. Type in the password used earlier in **Step 1**. Also would be recommended to tick **Enable strong private key protection** (Do not do this if you have an automated system that can't supply a password to login to the certificate).



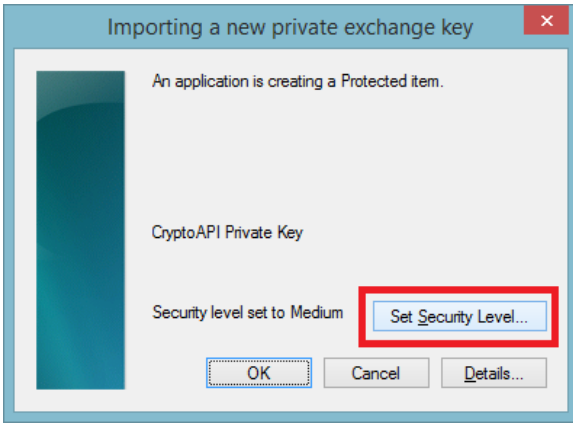
4. Select **Place all certificates in the following store**, and choose **Personal**. Click Next.



5. Click Finish on the next screen to complete the wizard.



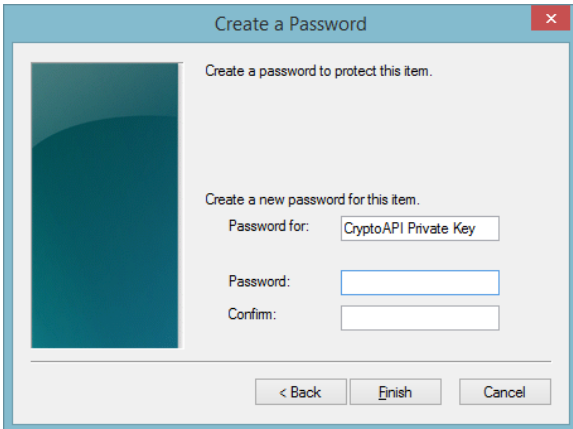
6. Click **Set Security Level**.



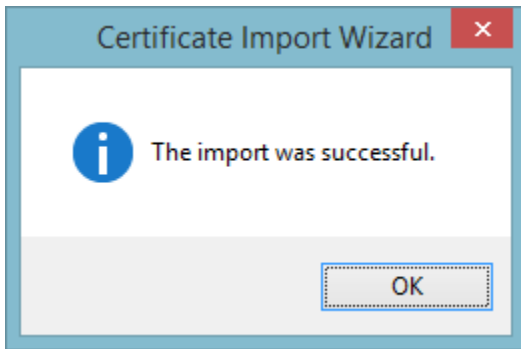
7. Change to **High**, and click Next.



8. You will then be required to set a password that will be utilised when using the certificate to login. Once configured, click finish.



9. The final **The import was successful** prompt should appear.

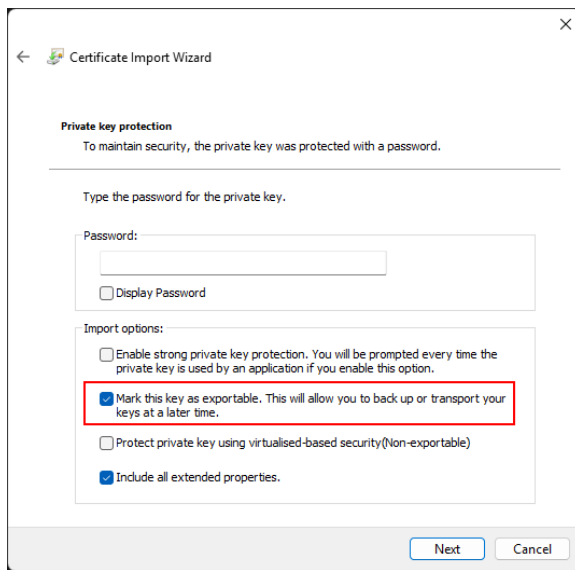


The password you entered is incorrect

This can happen with older Windows Operating systems that don't support newer certificate storage encryption formats. The **legacy compatibility** option should have been chosen in step one of **Export to p12** section above if you had an older Operating System. If you can no longer export the certificate then the certificate can be imported on a newer Windows Operating system and then exported again using TripleDES-SHA1. The file that is created should then work on your older Operating System.

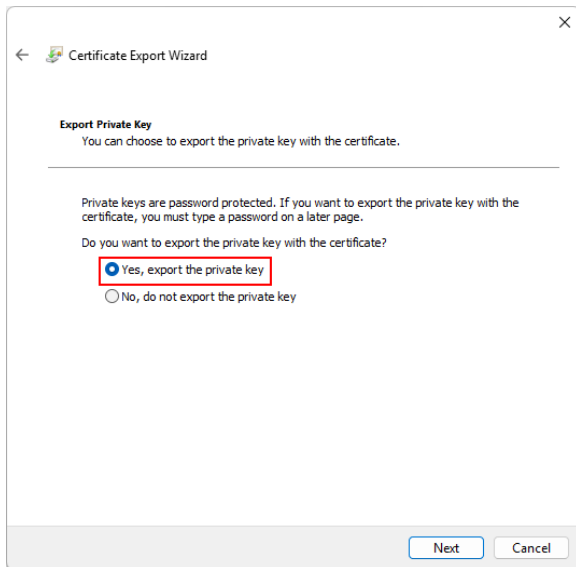
Important points for importing the certificate to re-export

When importing the certificate on the newer Operating System you must set the **Mark this key as exportable** option per the screenshot below.

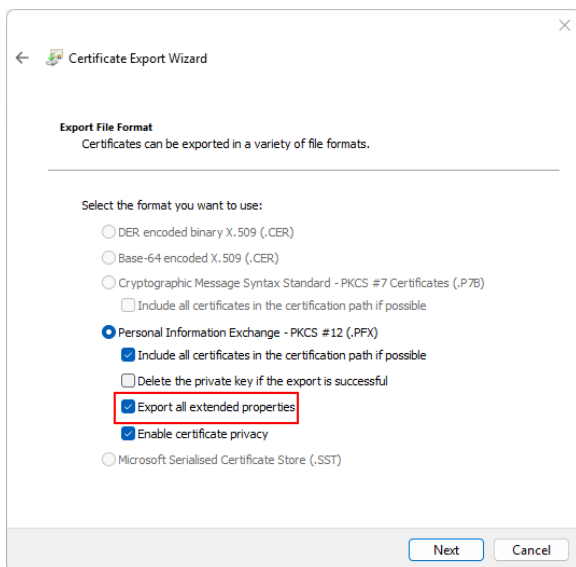


Important points for exporting the certificate for use in older Operating systems.

Set **Yes, export the private key**



Set **Export all extended properties**



Set **TripleDES-SHA1**. A Password is also advised. You will need to remember it to input when you install the certificate on the old Operating System.

← Certificate Export Wizard

Security
To maintain security, you must protect the private key to a security principal or by using a password.

Group or usernames (recommended)

Password:

Confirm password:

Encryption: TripleDES-SHA1