SPEAR User Guide - Importing a digital certificate onto a USB security token

Purpose of this Guide

The purpose of this guide is to assist SPEAR users to import their existing digital certificate from their computer onto a USB security token.

Note

If you have not yet downloaded and installed your digital certificate from DigiCert, please follow the steps in ‘User Guide 33B – Installing a digital certificate on a USB security token’ instead.

Important - Software required

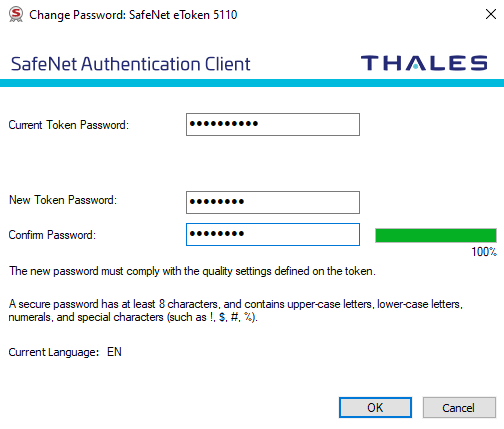
Please ensure the SafeNet Authentication Client has been installed prior to commencing the steps below. This can be downloaded from the DigiCert website:

<https://www.digicert.com/StaticFiles/SafeNetAuthenticationClient-x64.msi>

If you experience issues installing this software, please contact your IT department to ensure you have the required privileges.

1. Insert your token and change the password

Once the software has been installed, insert your USB security token into one of your computer’s USB ports. If this is the first time you’ve used this token, the software will prompt you to change your password.



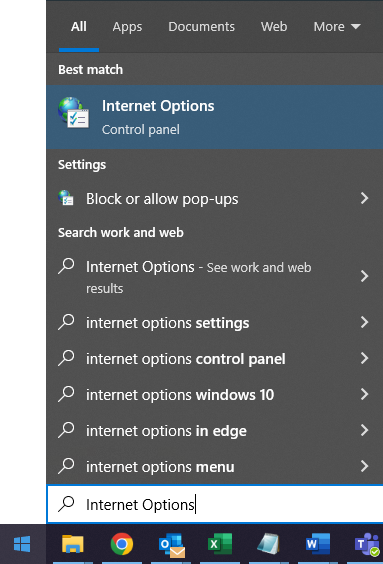
**NOTE: The default token password is: 1234567890**

Enter and confirm a new password to protect your USB security token.

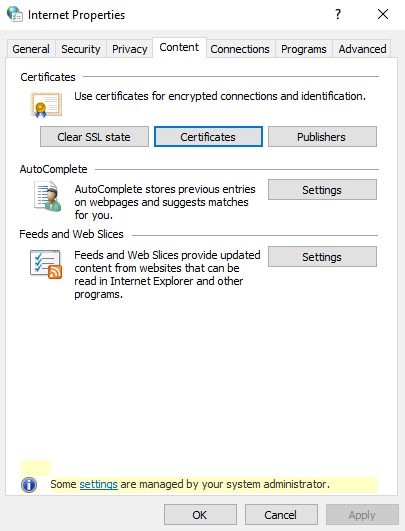
This is the password that you will be asked to enter when you digitally sign in SPEAR

2. Back up your digital certificate

Click on the Windows start button and type “Internet Options”. When the Internet Options icon appears, click on it to open the Internet Properties window.

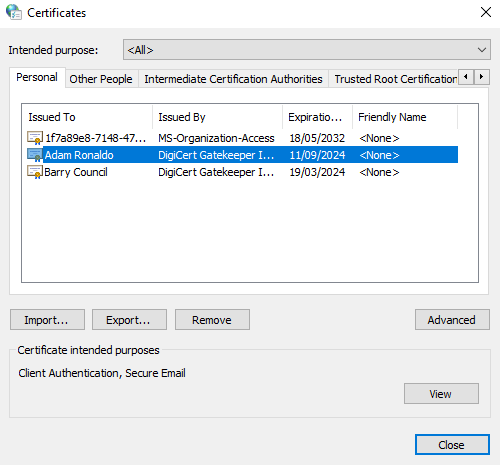


Click on the ‘Content’ tab and then click on the ‘Certificates’ button.



From the ‘Personal’ tab, click on the certificate you use in SPEAR and then click on the ‘Export’ button.

**Note: Ensure the certificate is valid and issued by “DigiCert Gatekeeper Issuing CA”.**



Certificates used in SPEAR are issued by **DigiCert Gatekeeper Issuing CA**

Click ‘Next’ on the first screen of the Certificate Import Wizard. On the second screen, select ‘Yes, export the private key’ and click ‘Next’.



Select ‘Yes’ to export the private key.

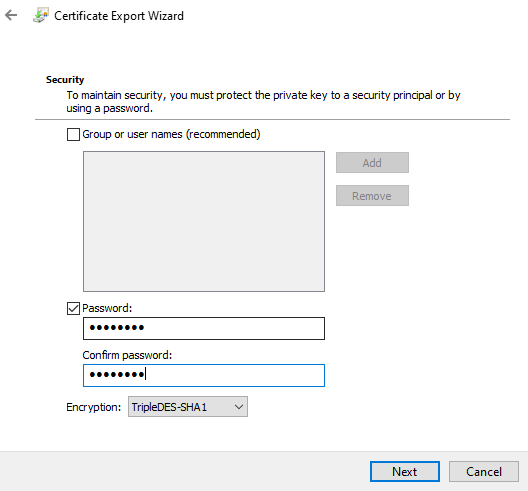
**NOTE: Failing to do this step will result in your backup files being in the incorrect format.**

Ensure ‘Personal Information Exchange’ is the selected format and select the relevant options below before clicking ‘Next’.

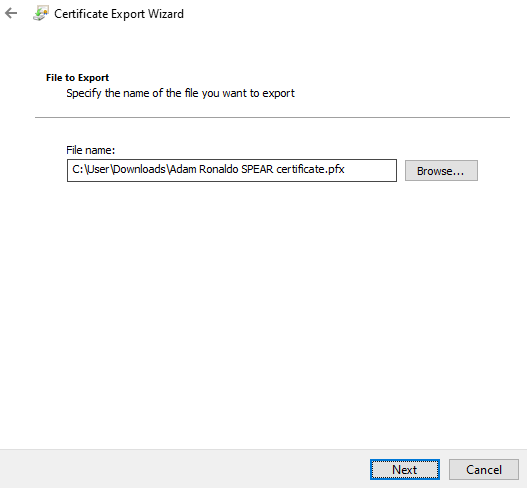


Ensure that you **DO NOT TICK** ‘Delete the private key if the export is successful’. All remaining options can be ticked.

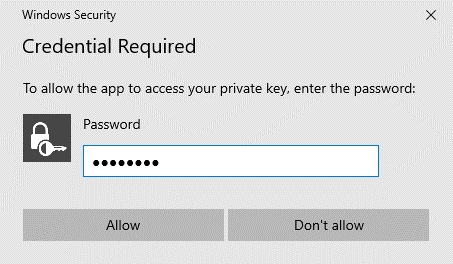
Ensure the password checkbox is ticked and enter a password to protect your digital certificate back up file. You may wish to use the same password that you use to digitally sign in SPEAR. Depending on your operating system, you may need to use at least eight characters, one of which should be uppercase.



Click ‘Browse’ and select a folder in which to store your digital certificate back up file. Enter a recognisable file name and click ‘Save’. Click on the ‘Next’ button and then click on the ‘Finish’ button.



If you are prompted to provide the password for your digital certificate, enter it in the Password field and click ‘Allow’, otherwise just click ‘Allow.

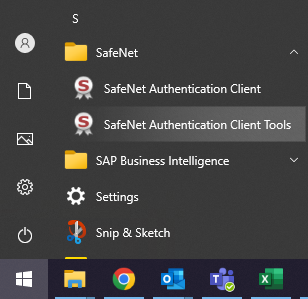


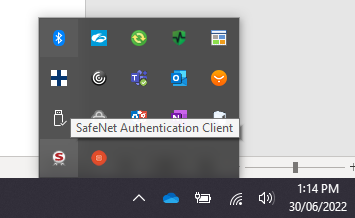
If you are not prompted for a password, simply click on ‘Allow’.

If the password was correct, you will receive confirmation that the export was successful. You should now have a digital certificate back up file with a .pfx file extension located in the nominated folder.

3. Open the SafeNet Authentication Client Tools software

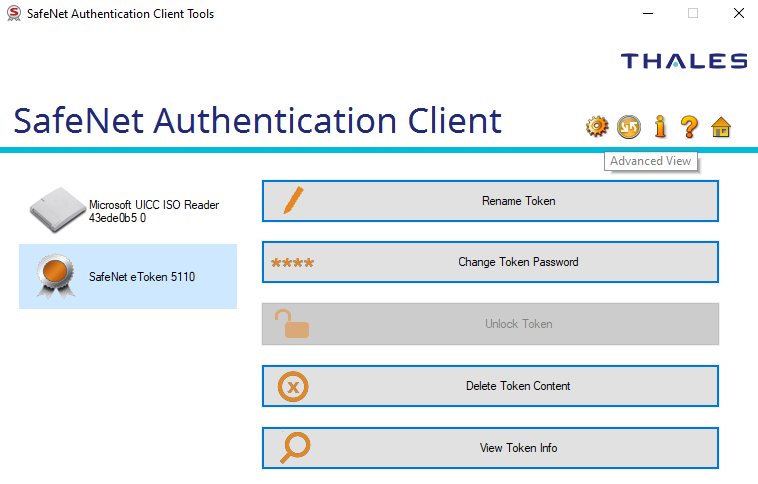
Open the SafeNet Authentication Client Tools software by locating it in your Windows Start menu, or alternatively you can double click on the SafeNet icon in your taskbar.





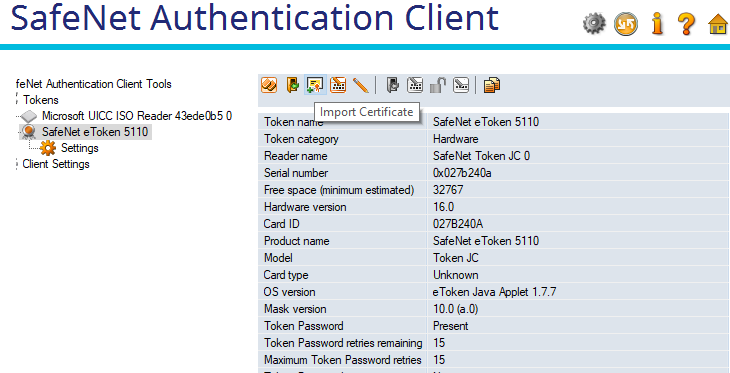
**OR**

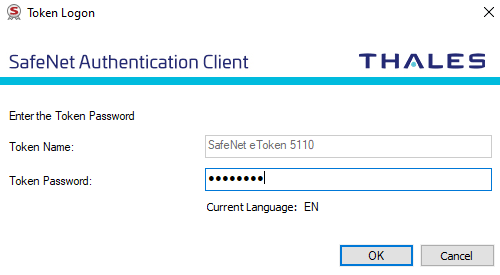
Ensure that the SafeNet token is selected and click on the ‘Advanced View’ icon.

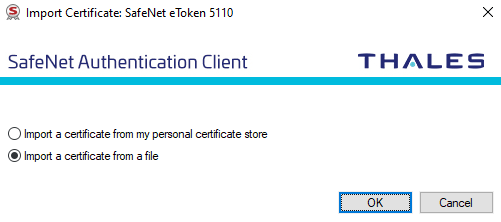


4. Import your digital certificate

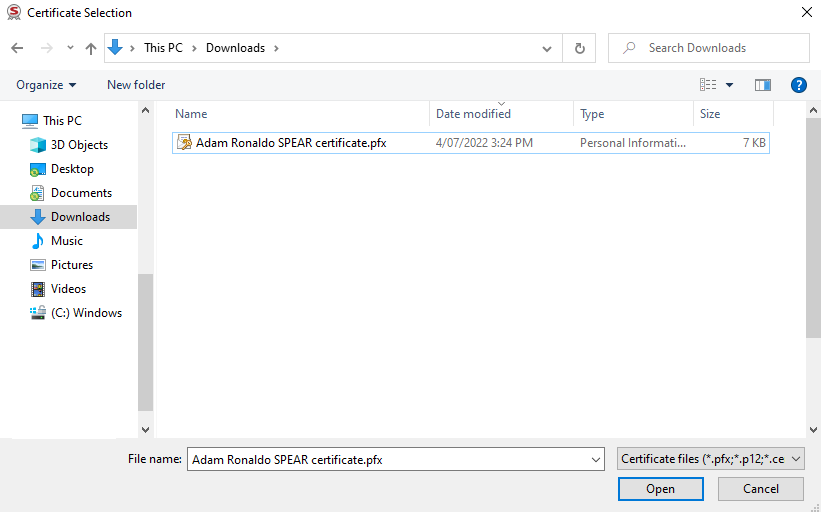
Click on the ‘Import Certificate’ icon and, if prompted, enter the token password you set in step 1 and click ‘OK’.

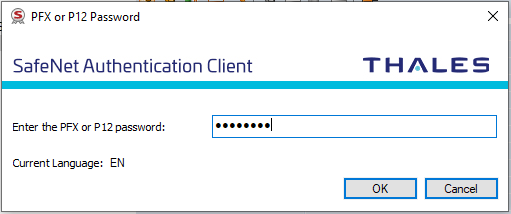




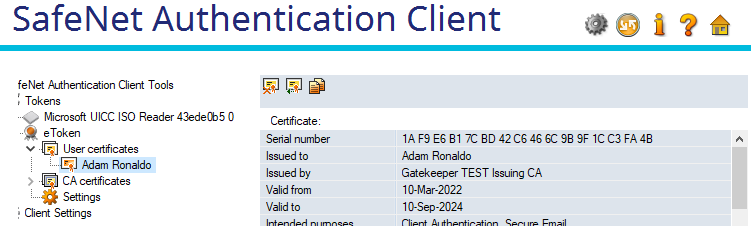
Select ‘Import a certificate from a file’ and click ‘OK’.

Browse to where you saved the digital certificate back up file and click on the file before clicking on ‘Open’.



Enter the password that you set when creating the digital certificate back up file and click on ‘OK’.

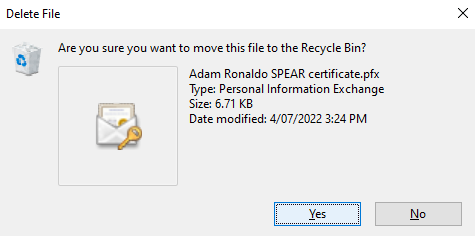
If the password was correct, you will receive confirmation that the certificate was imported successfully and the certificate will be listed in the SafeNet Authentication Client software under ‘User certificates’.



What next?

If you will be using your certificate in SPEAR to sign key documents, you can now test it. Please see User Guide 34 – Testing your digital certificate for more information.

For security reasons, once you have successfully tested your digital certificate in SPEAR, it is recommended you browse to the location where you saved the certificate back up file in .pfx format and delete it.



Need more information?

Further information on this topic can be found by:

* Speaking with your IT department if you’re unable to install the software
* Visiting the SPEAR website [www.spear.land.vic.gov.au/SPEAR](http://www.spear.land.vic.gov.au/SPEAR)
* Contacting the SPEAR Service Desk on 9194 0612 or email [spear.info@delwp.vic.gov.au](mailto:spear.info@delwp.vic.gov.au)