

Support for https protocol for ITAS APIs

Hivedome now offer support for the secure https protocol to be used with ITAS APIs.

For Certificate installation instructions see below

Distribute A Self-Signed Certificate

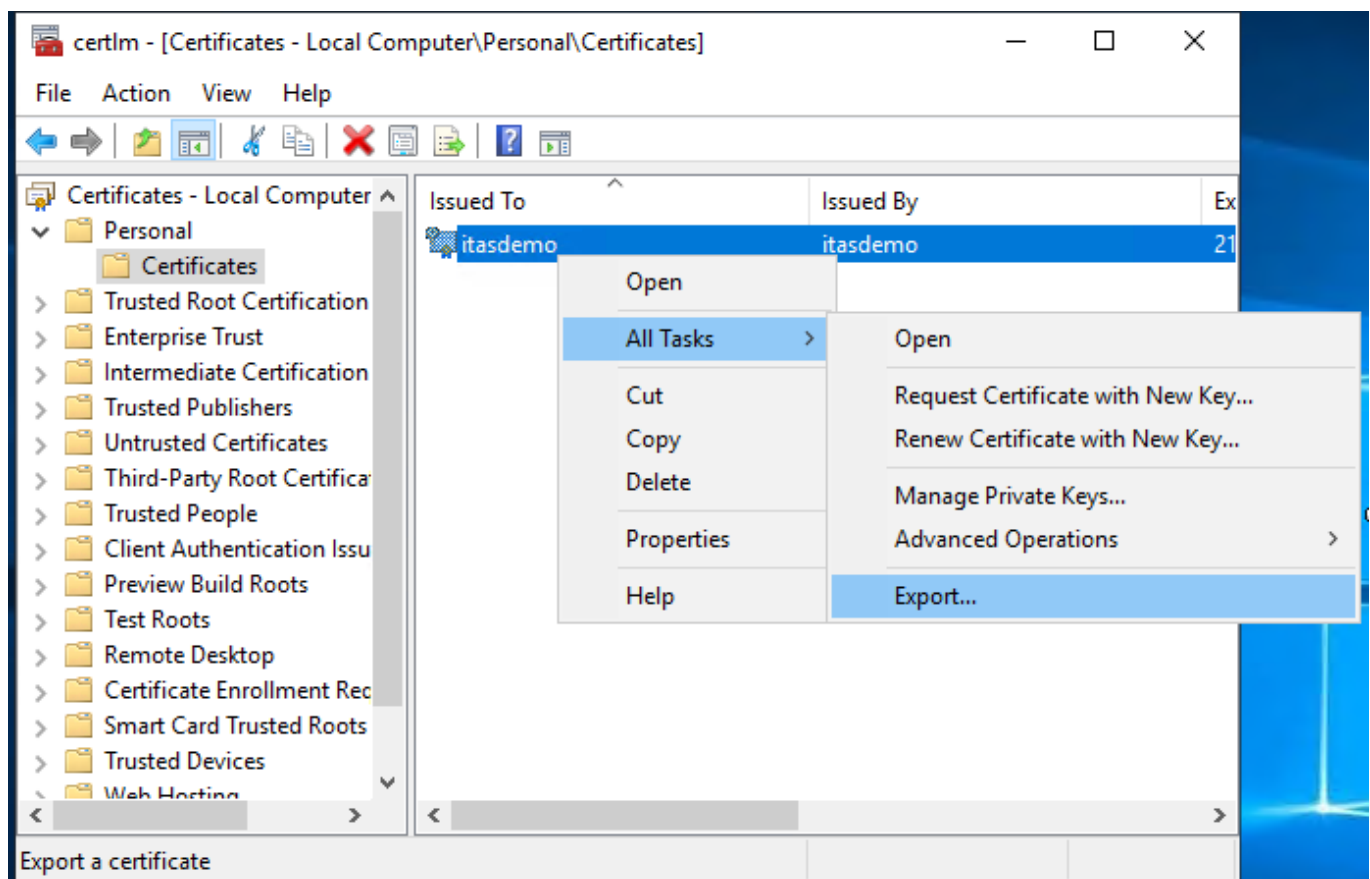
This is a two-step process. Exporting the certificate from the ITAS Application Server and importing the exported certificate on to each of the client computers where Trader Desktop is used.

Exporting A Certificate

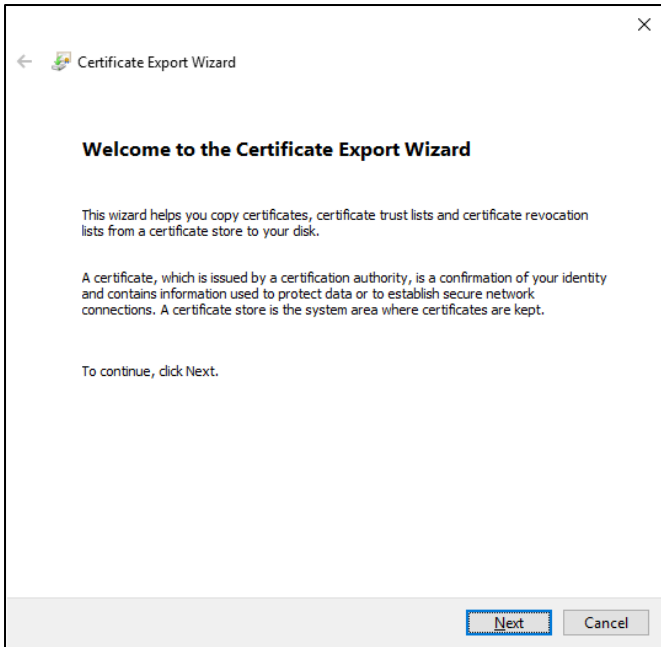
Log onto the ITAS Application server.

Run certlm.msc. Navigate to **Personal > Certificates** and find the certificate that bears the same name as the application server.

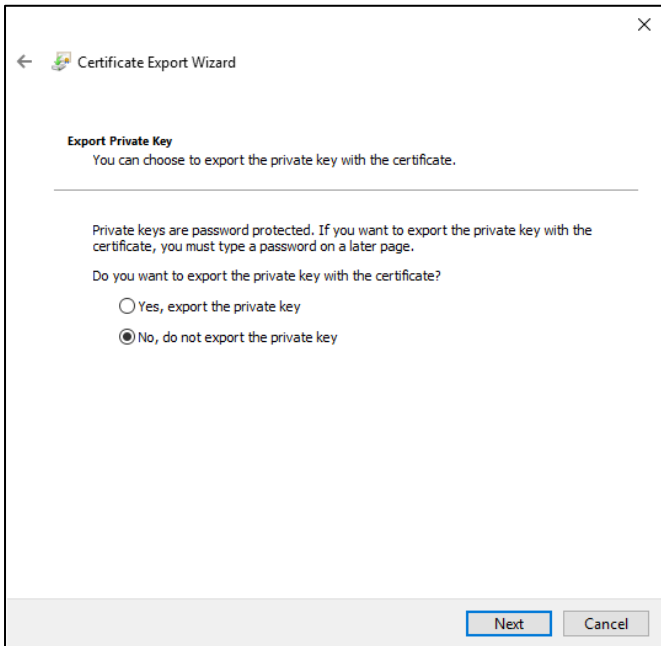
Right click on the certificate and choose **All Tasks > Export**.



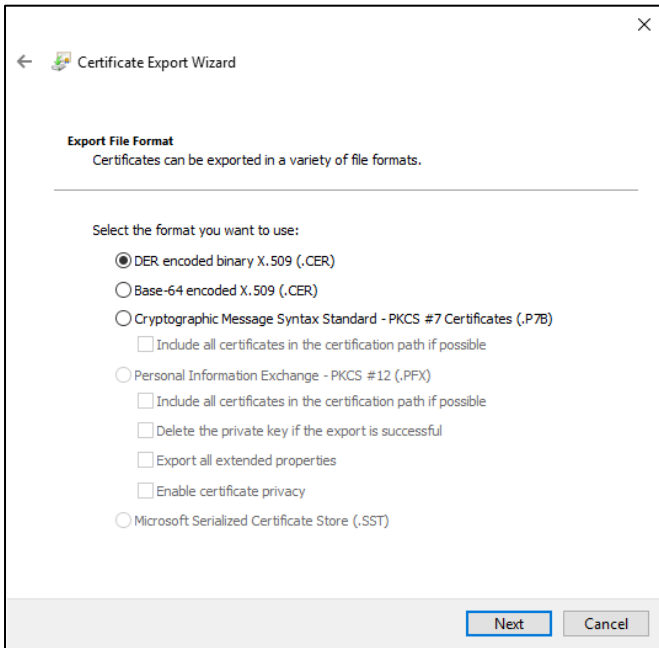
On the following screen, click **Next**.



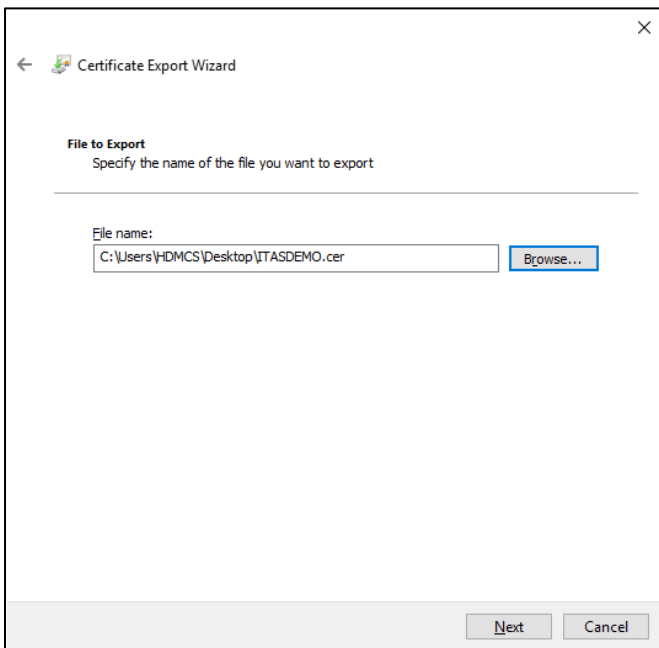
Ensure **“No, do not export the private key”** is selected and click **Next**.



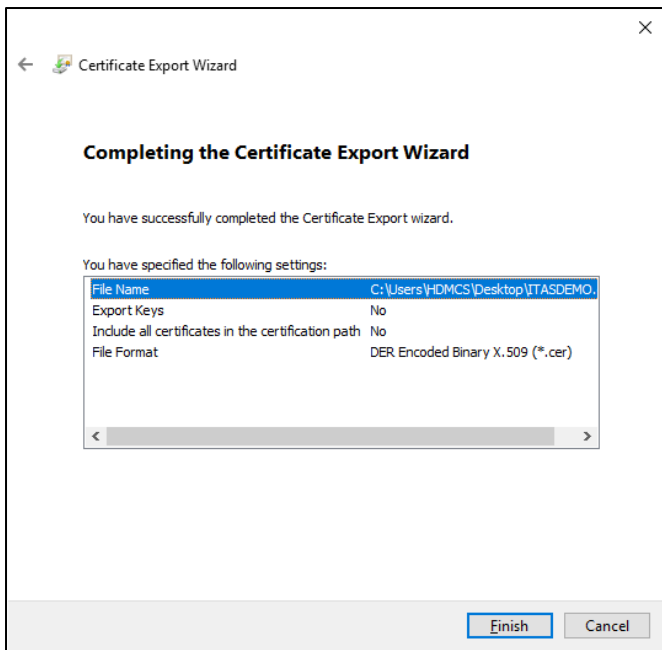
Ensure that “**DER encoded binary X.509 (.CER)**” is selected and Click **Next**.



Browse to the location where you want to save the exported file and click **Next**.



Finally, click **Finish**.

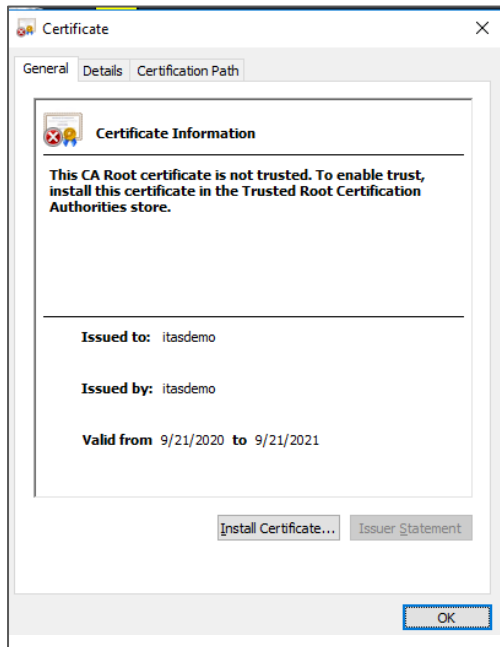


Once the Certificate Export Wizard is closed, ensure that a .cer file is created in the location selected.

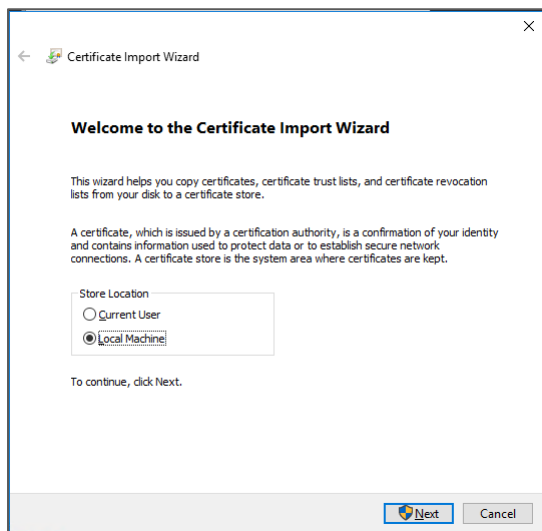
Importing A Certificate

Once the certificate is exported, it can be imported to each client machine that will connect to Trader Desktop and or ITAS web services.

Import the certificate by copying the exported .cer file to the client machine. **Double click** on this file to launch the Certificate Import Wizard, click **“Install Certificate”**.



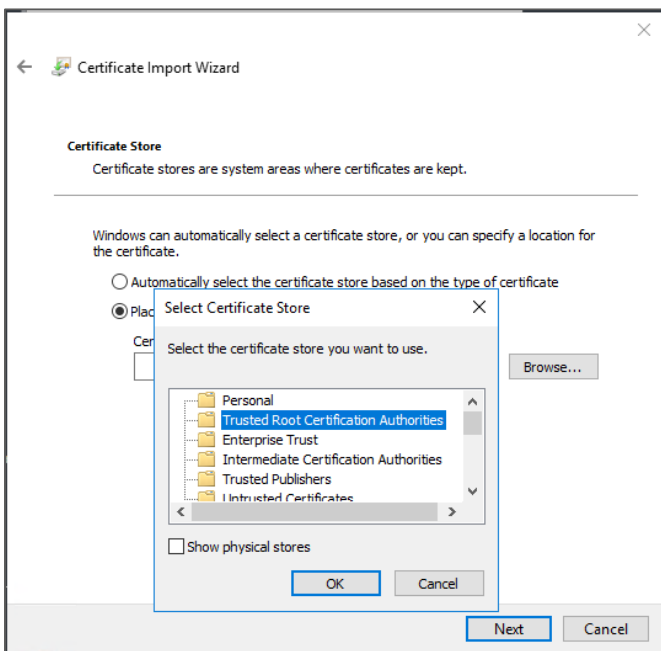
On the next screen Select **“Local Machine”** and click **Next**.



If User Access Control is enabled, the following message should appear:

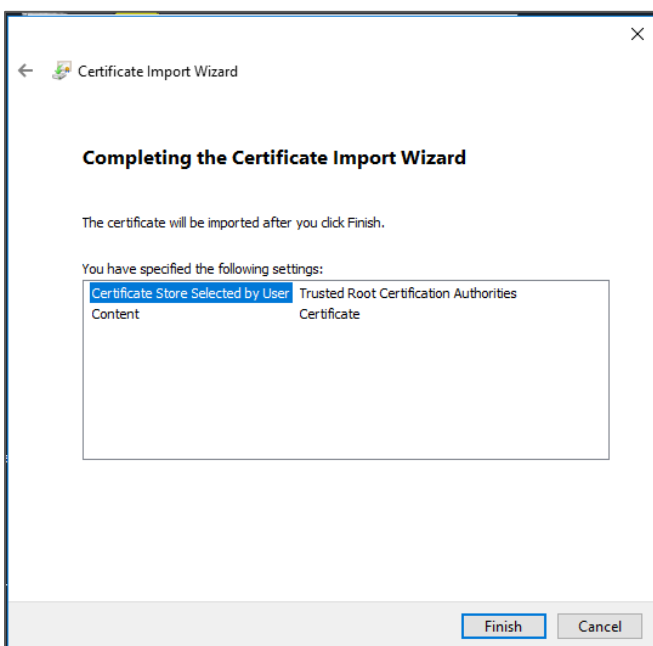


Click **Yes** and then select “**Place all certificates in the following store**” and Browse to **Trusted Root Certification Authorities**.

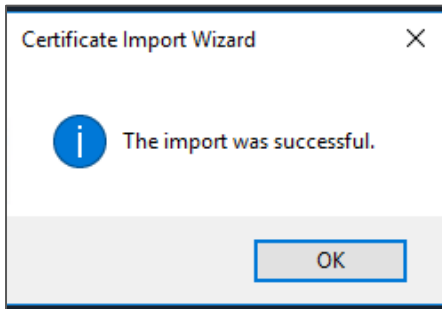


Click on **OK** and then **Next**.

On the final screen, click **Finish**.



Click **OK** to close Certificate Import Wizard.



Run certlm.msc. Navigate to **Trusted Root Certification Authorities > Certificates** and locate the certificate that was just imported.

If you have many machines which will need to connect to ITAS web services, then carrying out this procedure on each of them may be time consuming. This can be automated if required.

Using Your Own Local Certificate

If your organization has an internal certificate server that can produce and sign a certificate for your ITAS application server, and that will be trusted by machines on your internal network, you can use this certificate instead.

Your application server should already have a certificate in the certificate store for the local machine under **Personal**, this will bear the same name as the application server. If you simply replace this with the one generated by your internal certificate server and then run the ITAS deployment tool, it will deploy all web services using this certificate.

Follow the relevant instructions on the next page for Installing a Public or Local certificate:

Using Your Own Public Certificate

If you wish to have ITAS services accessed from outside of the local network, then there are a few ways to achieve this. You will need a public hostname address and a certificate to match. You may choose to have a web application firewall sit in-front of the ITAS Web Services. This can be configured with the public hostname address and the matching certificate. It can be set up to accept requests on the public address and forward those requests to the internal address. The configuration for this is outside of the scope of this document.

Alternatively, you may choose to set up your firewall to allow direct access to the ITAS application server from the outside. To do this Hivedome will need to be informed of the public address so that we can set the configuration files in order that the webservice are deployed with bindings to that hostname.

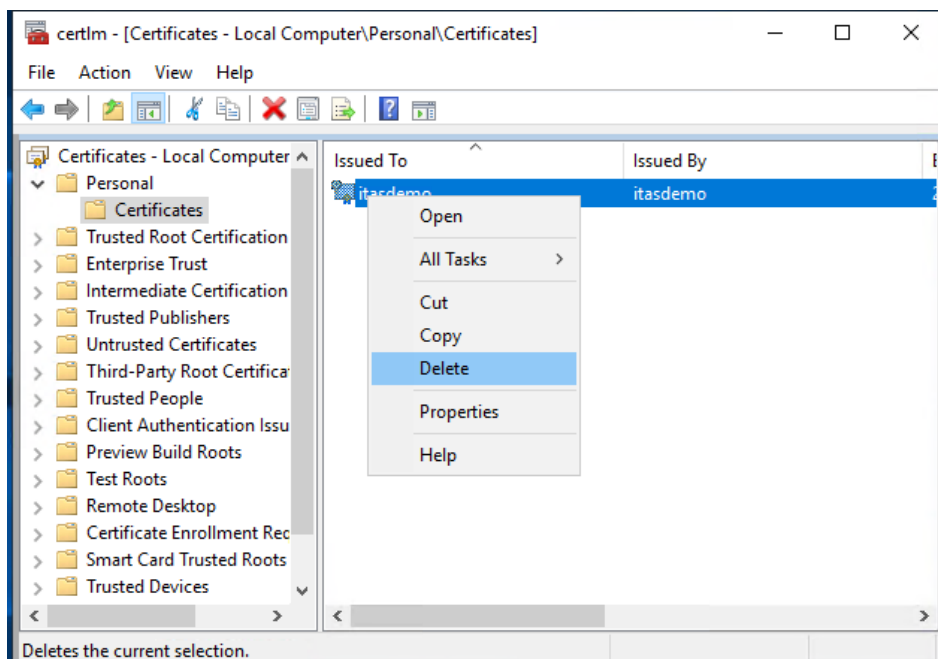
The ITAS deployment process will check if there is already a certificate available in the certificate store (in the local machine personal store) and use that certificate with the web bindings that it creates.

Follow the relevant instructions on the next page for Installing a Public or Local certificate:

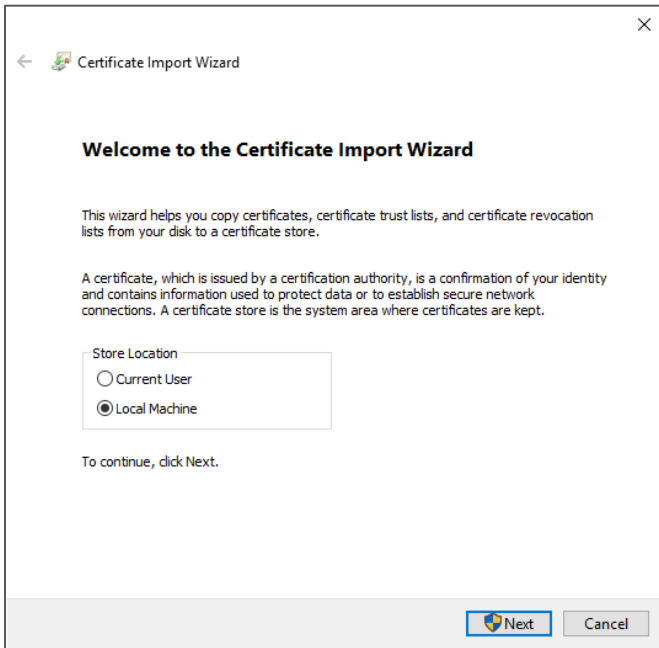
Installing A Public or Local Certificate

This can be achieved as follows providing you have a pfx file and the password for that pfx file:

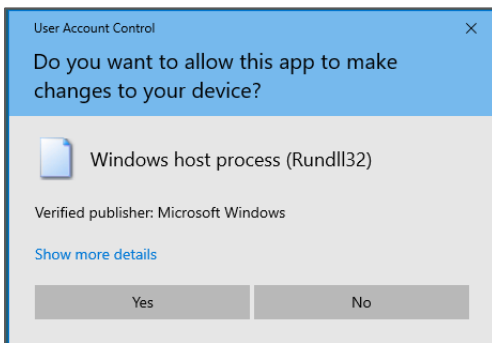
Launch certlm.msc and delete the existing certificate.



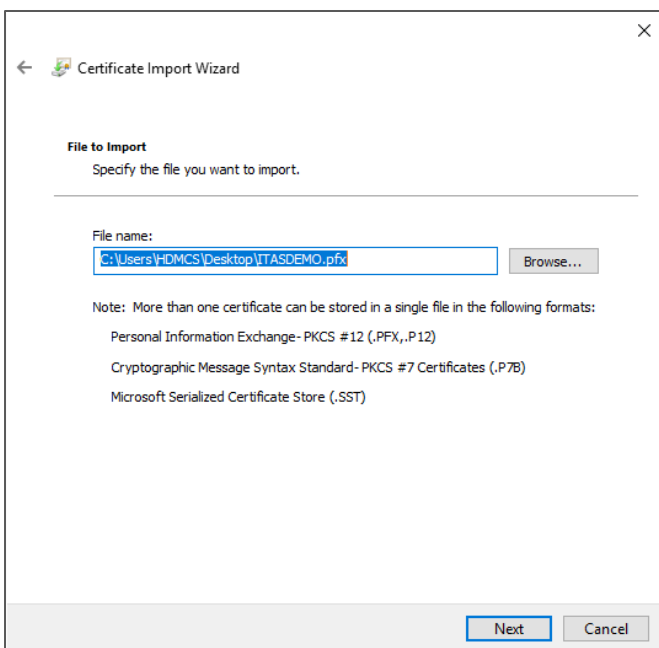
Double click on the PFX file. Select “**Local Machine**” and then click **Next**.



If User Access Control is enabled, the following message should appear:

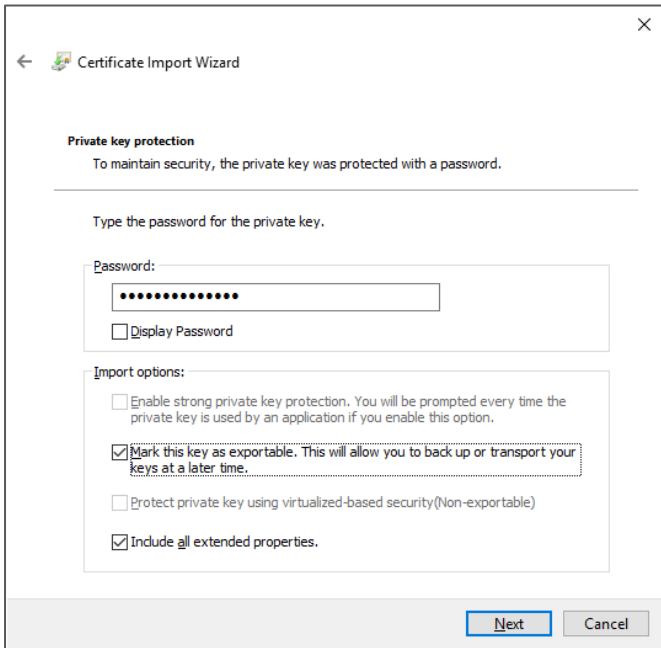


Click **Yes** and the path to the pfx file you double clicked on should be displayed on the next screen.



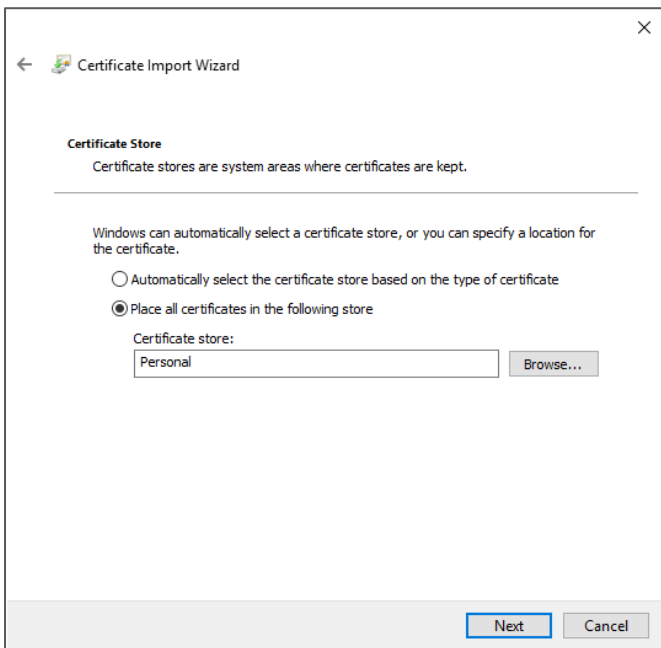
Click **Next**.

Set a **Password** then tick **“Mark this key as exportable”** ensure that **“Include all extended properties”** is ticked before clicking on **Next**.



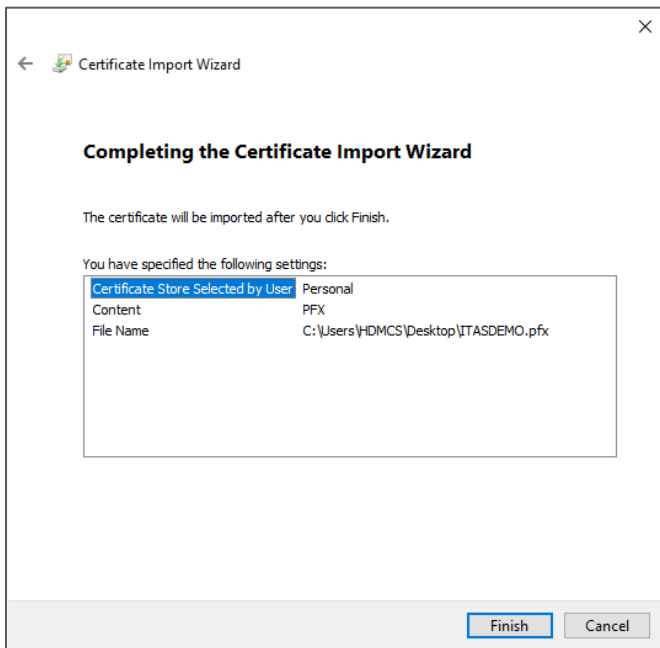
The screenshot shows the 'Certificate Import Wizard' window at the 'Private key protection' step. The title bar reads 'Certificate Import Wizard'. Below the title bar, there is a back arrow icon and the text 'Certificate Import Wizard'. The main content area is titled 'Private key protection' and contains the following text: 'To maintain security, the private key was protected with a password.' Below this is a horizontal line. The text 'Type the password for the private key.' is followed by a 'Password:' label and a text input field containing ten black dots. Below the input field is a checkbox labeled 'Display Password'. Underneath is the 'Import options:' section with three checkboxes: 'Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.' (unchecked), 'Mark this key as exportable. This will allow you to back up or transport your keys at a later time.' (checked), and 'Protect private key using virtualized-based security (Non-exportable)' (unchecked). Below these is another checked checkbox: 'Include all extended properties.' At the bottom right of the window are two buttons: 'Next' and 'Cancel'.

Select **“Place all certificates in the following store.”** Browse to **Personal** and click **Next**.



The screenshot shows the 'Certificate Import Wizard' window at the 'Certificate Store' step. The title bar reads 'Certificate Import Wizard'. Below the title bar, there is a back arrow icon and the text 'Certificate Import Wizard'. The main content area is titled 'Certificate Store' and contains the following text: 'Certificate stores are system areas where certificates are kept.' Below this is a horizontal line. The text 'Windows can automatically select a certificate store, or you can specify a location for the certificate.' is followed by two radio button options: 'Automatically select the certificate store based on the type of certificate' (unselected) and 'Place all certificates in the following store' (selected). Below the selected option is the text 'Certificate store:' followed by a text input field containing the word 'Personal' and a 'Browse...' button. At the bottom right of the window are two buttons: 'Next' and 'Cancel'.

On the final screen, click **Finish**.



Allowing ITAS to generate a public certificate

The ITAS deployment process can create a certificate from 'Let's Encrypt' using WinACME. If no suitable certificate is found ITAS will attempt to use WinACME to generate a domain validation certificate. To do so it will need to demonstrate control of the public hostname included in the certificate. 'Let's Encrypt' will challenge WinACME to do so by publishing a particular code on the http website that responds at that hostname. If the firewall is forwarding http traffic (port 80) to the default website on the ITAS application server then this will work automatically.

For more information or assistance with this install, please contact your ITAS representative or support team.