21st January 2021

Notice to introduce secure https protocol for ITAS APIs

Hivedome will be introducing support for the secure https protocol to be used with ITAS APIs in the second quarter of 2021.

Background

Trader Desktop includes several rest APIs: these include APIs used internally by the application, APIs used to integrate ITAS with other third-party systems and a Web Portal option that enables users to access ITAS data via the web.

Historically these APIs have been delivered using the insecure http protocol, but the next version of Trader Desktop, version 8.10.4.----, will include support for the secure https protocol to be used with these APIs. ITAS will continue to support the APIs over the existing insecure http protocol for the time being, to allow customers to switch to using the secure https systems, but http will eventually be made redundant.

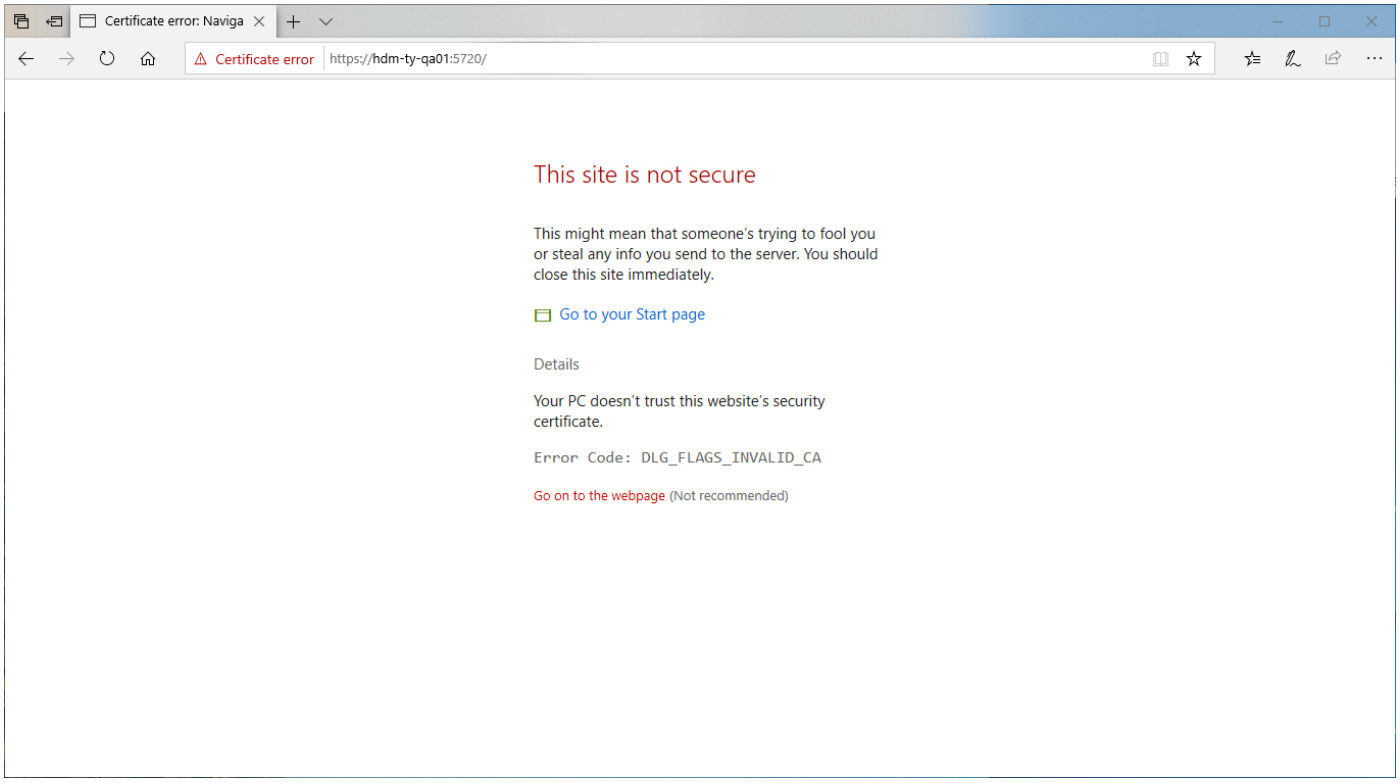
Requirements

Part of the challenge with the change is to manage the (SSL) certificate associated with https. The good news is that for the most basic ITAS installations, where Trader Desktop is run on a single server and where the ITAS application server is also installed on that same server, then this will be been done for you. However, if your users run Trader Desktop from a separate server or from workstations then action will need to be taken.

The https certificate serves two purposes. Firstly, it provides keys by which the data may be encrypted by the sender end and decrypted by the receiver. This is intended to prevent anybody on the network from eavesdropping or altering the data. Secondly it can provide assurance that the sender is indeed the computer you think it is. This is because no unauthorised computer should have access to the key that encrypts the data.

The secure versions of the API endpoints have already been created using a self-signed certificate: a certificate that serves the first of these purposes, to encrypt the traffic. However, it will not necessarily provide assurance as to the sender's identity. If the receiver has no way to verify that the certificate is the real deal, then it cannot use that certificate to verify the identity of the sender.

Browsing to the web address of a site secured with a certificate that your computer does not trust results in an error like the one below:



Similarly, secure API calls from Trader Desktop may fail if the computer running Trader Desktop does not trust the certificate.

The computer on which Trader Desktop and the ITAS web services reside already trusts this self-signed certificate, but other computers on your network will not unless you take one of the following two actions:

- Distribute the self-signed certificate to any client computer connecting to ITAS services.

  or

- If you already have a local certificate server trusted by computers on your network, then you may replace the self-signed certificate with one that is generated and signed by your own certificate server.

For Certificate installation instructions see below.

Distribute A Self-Signed Certificate

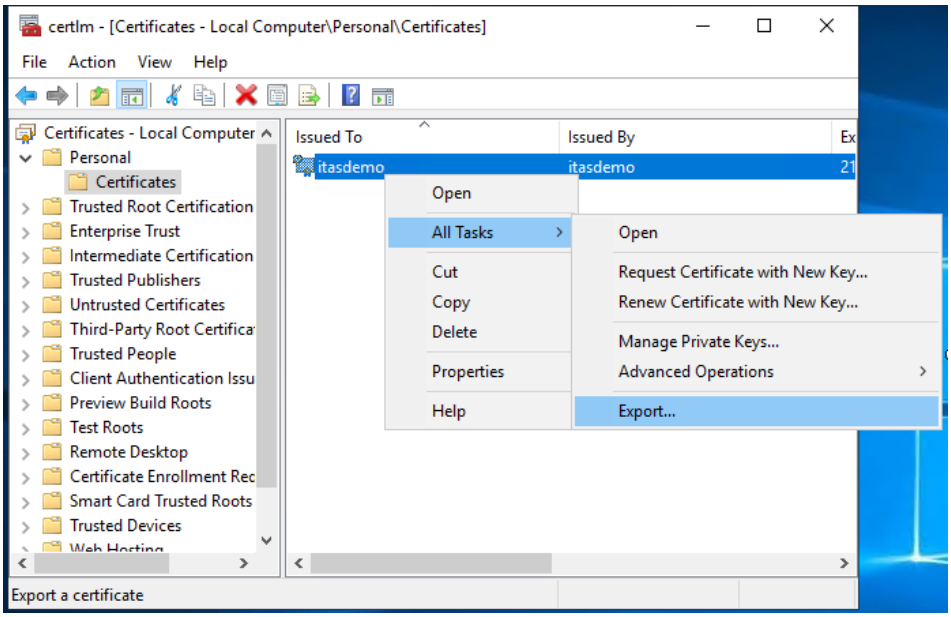
This is a two-step process. Exporting the certificate from the ITAS Application Server and importing the exported certificate on to each of the client computers where Trader Desktop is used.

Exporting A Certificate

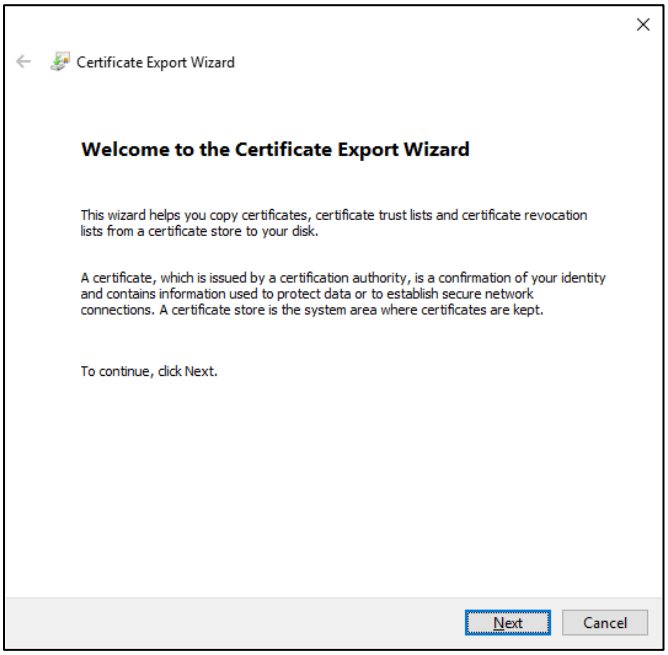
Log onto the ITAS Application server.

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

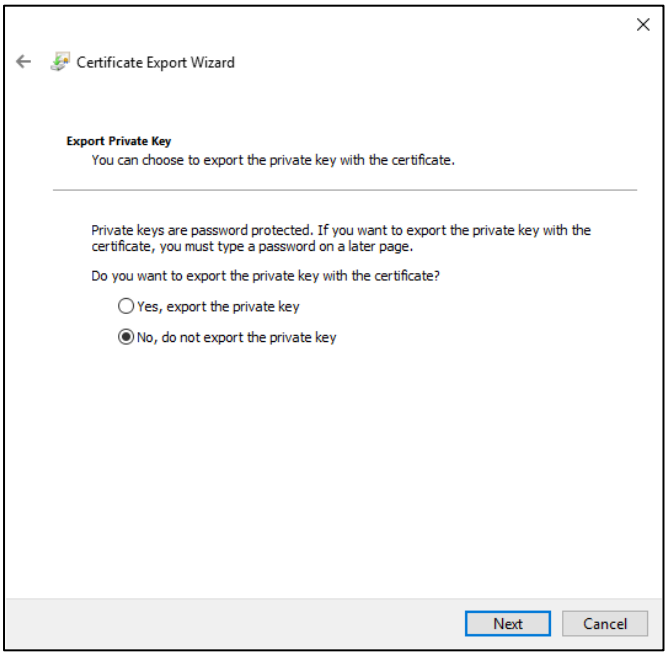
Right click on the certificate and choose **All Tasks** > **Export**.



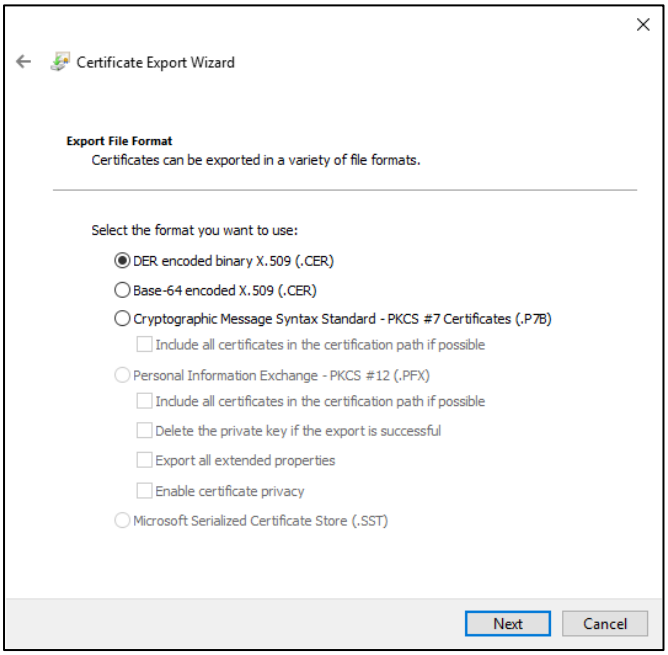
On the following screen, click **Next.**



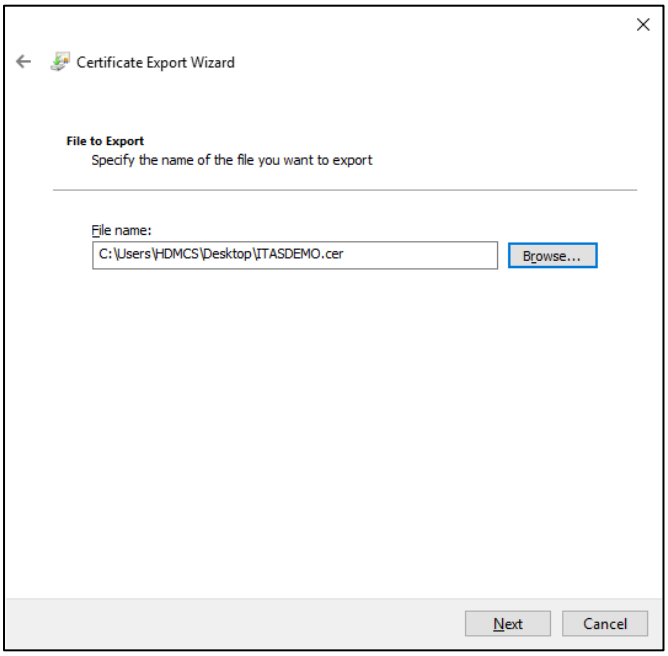
Ensure “**No, do not export the private key**” is selected and click **Next**.



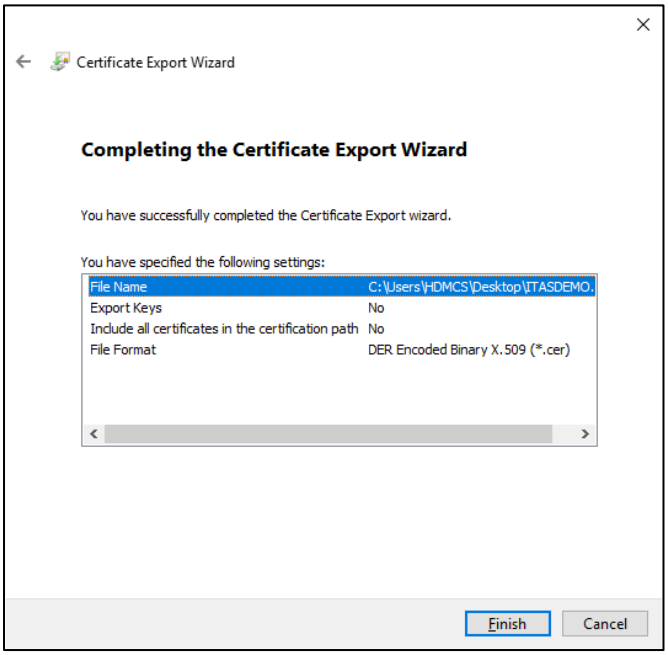
Ensure that “**DER encoded binary X.509 (.CER)**” is selected and Click **Next.**



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



Finally, click **Finish**.

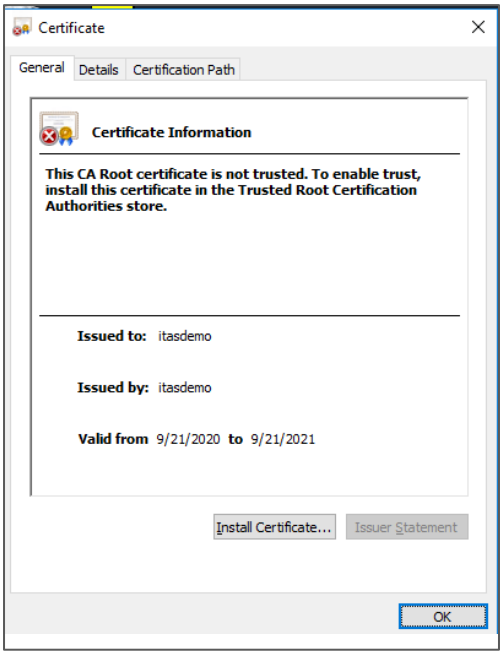


Once the Certificate Export Wizard is closed, ensure that a .cer file is created in the location selected.

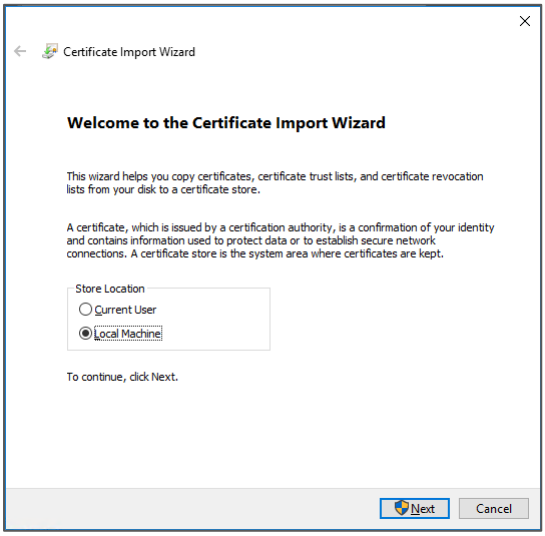
Importing A Certificate

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

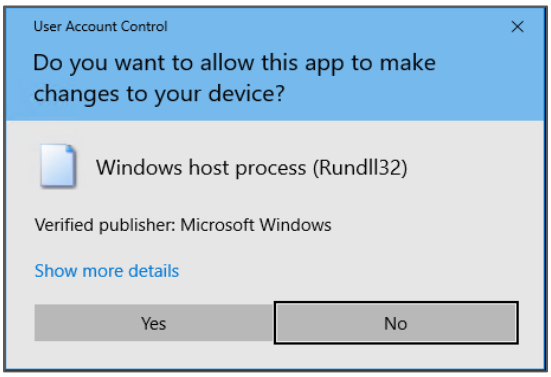
Import the certificate by copying the exported .cer file to the client machine. **Double click** on this file to launch the Certificate Import Wizard, click "**Install Certificate**".



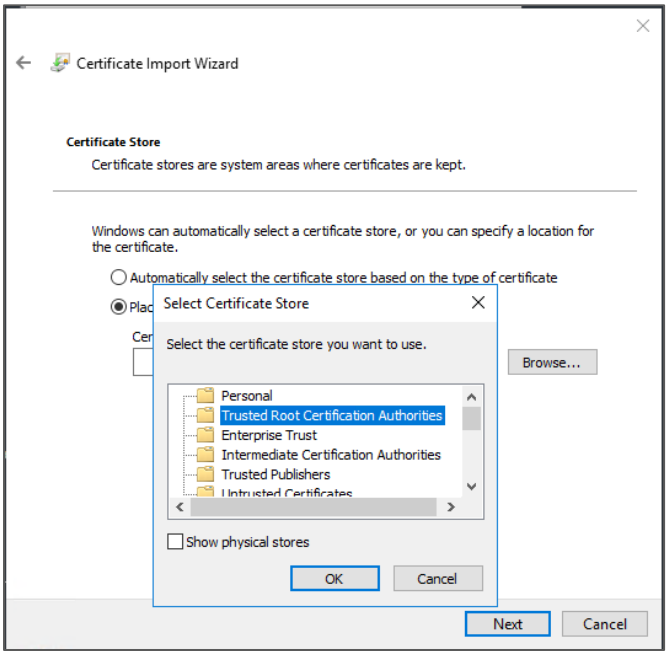
On the next screen Select "**Local Machine**" and click **Next**.



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

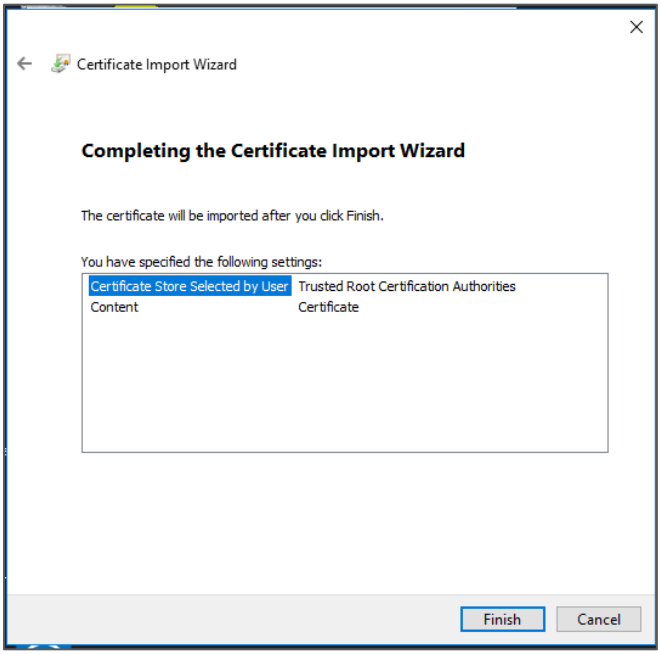


Click **Yes** and then select "**Place all certificates in the following store**" and Browse to **Trusted Root Certification Authorities**.

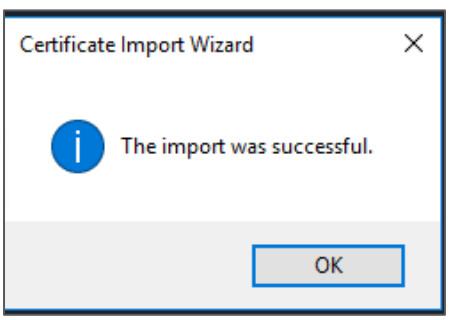


Click on **OK** and then **Next**.

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 webservices are deployed with bindings to that hostname.

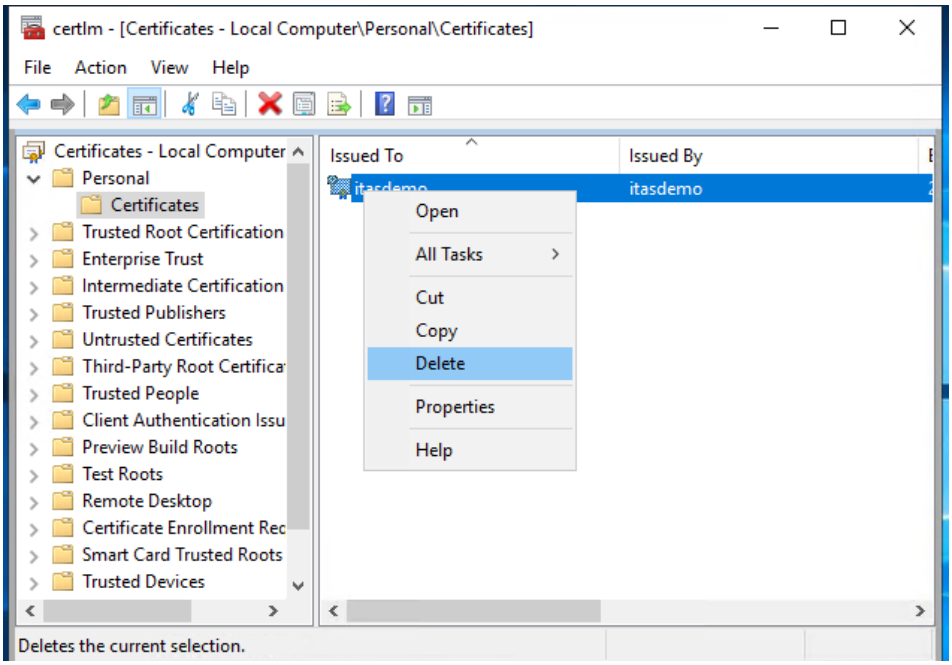
The ITAS deployment process will check if there is already a certificate available in the certificate store (in the local machine personal store) and use that certificate with the web bindings that it creates.

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

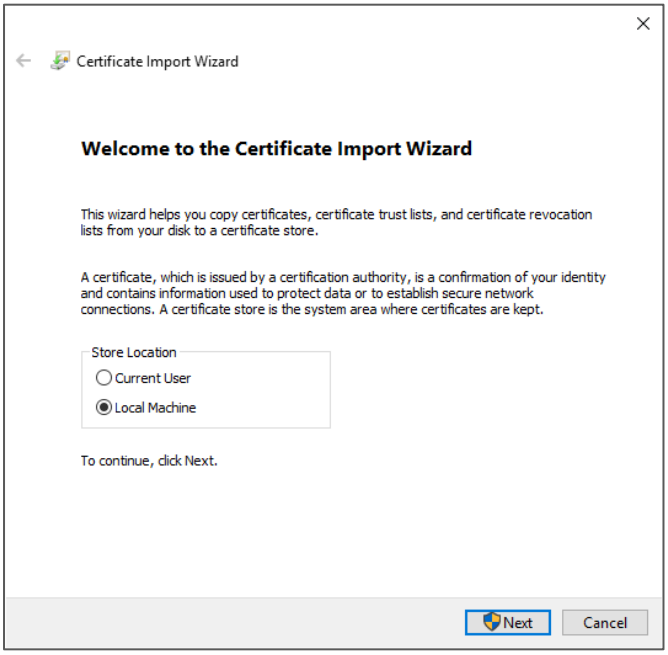
Installing A Public or Local Certificate

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

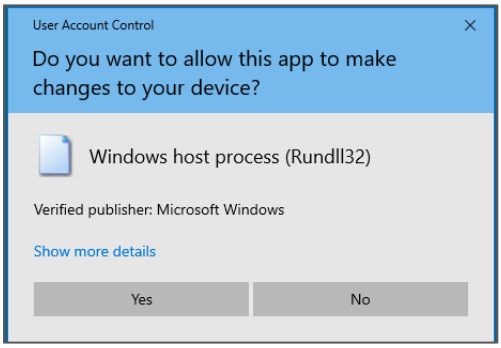
Launch certlm.msc and delete the existing certificate.



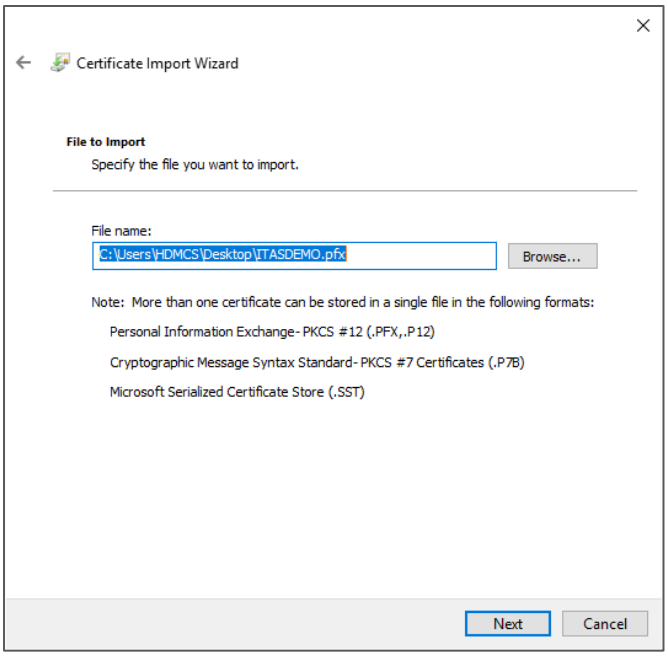
Double click on the PFX file. Select “**Local Machine**” and then click **Next**.



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

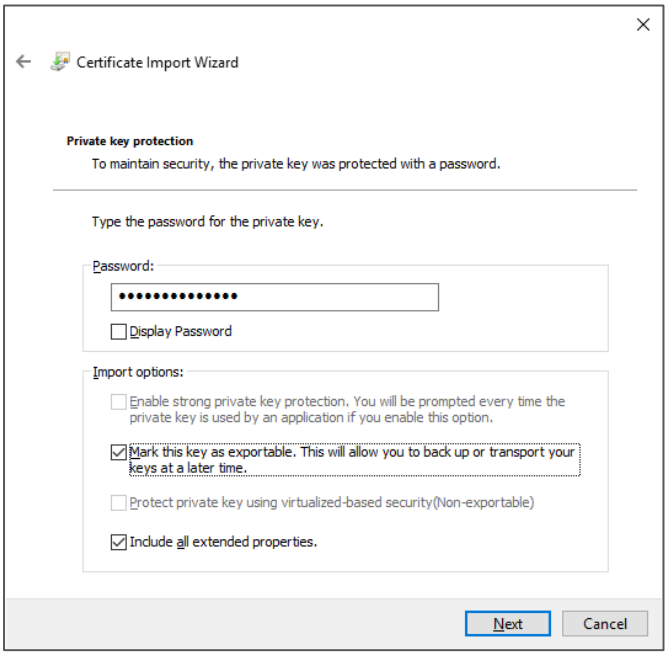


Click **Yes** and the path to the pfx file you double clicked on should be displayed on the next screen.

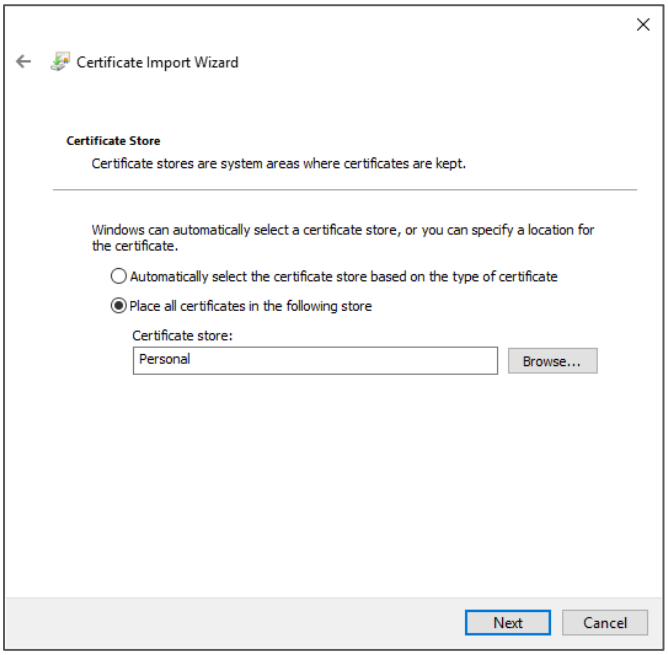


Click **Next**.

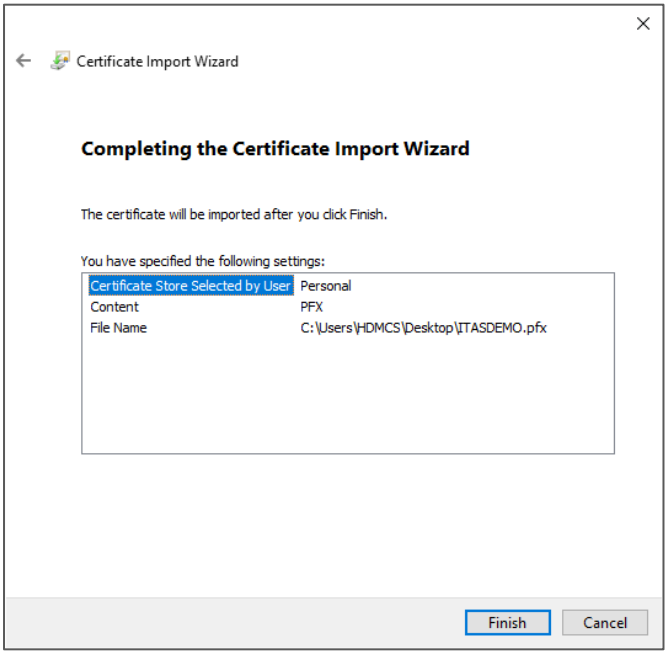
Set a **Password** then tick "**Mark this key as exportable**" ensure that "**Include all extended properties**" is ticked before clicking on **Next**.



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



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 assistant with this install, please contact your ITAS representative or support team.