

This document describes common issues that may arise during the application process and or import/export of digital certificates. If this guide does not reference or resolve the issue you are experiencing, please contact [cert.admin@aes0.ca](mailto:cert.admin@aes0.ca) for further assistance. Topics addressed in this document are as follows:

- [Enrollment Delays](#)
- [Enrollment code not recognized](#)
- [Chrome or Edge Extension Error](#)
- [Certificate not trusted – installation of Root Security Certificate](#)
- [Firewall preventing you from accessing your certificate](#)
- [Unable to Login to ETS](#)
- [Installing certificates on a new computer](#)

Keep in mind that due to privacy parameters, information pertaining to digital certificates can only be disclosed to an [authorized contact](#) or certificate holder. If you do not know who your authorized contact is for your organization, you can reference the [Pool Participant list](#).

## Enrollment Delays

Delays in receiving approval for an ETS digital certificates request could be due to one of the following common issues:

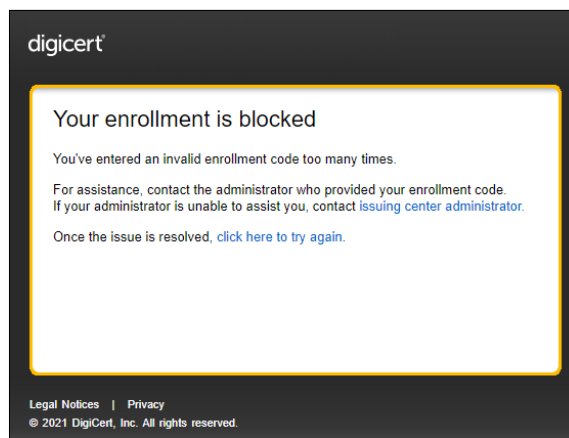
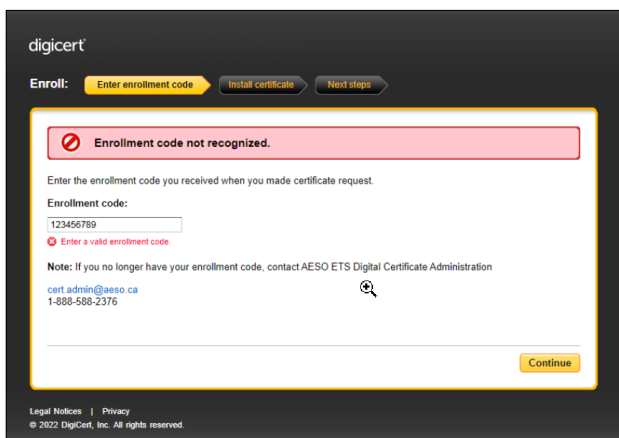
- User Access Request Form (step 1) was not submitted by an [authorized contact](#).
- User Access Request Form (step 1) is submitted using an older version of the form.
- The information submitted during the online enrollment (step 2) does not match step 1.

If you have not received approval of your digital certificate request within than 3 business days, please verify the steps above have been completed, and if necessary, send us an email at [cert.admin@aes0.ca](mailto:cert.admin@aes0.ca) for additional assistance.

Please note that our request form is updated on occasion as requirements change. It is recommended to visit our website to obtain the latest version, rather than saving local copies to your computer. The request form as well as our guides can be found by visiting the AESO website at [www.aeso.ca](http://www.aeso.ca) and following the path - Market > Market-Participation > System Tools > Energy Trading System Tools.

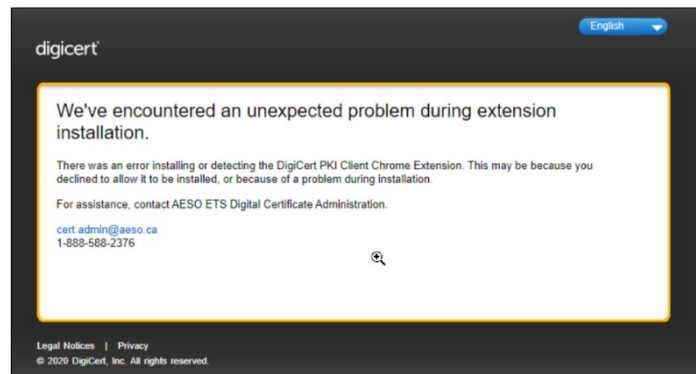
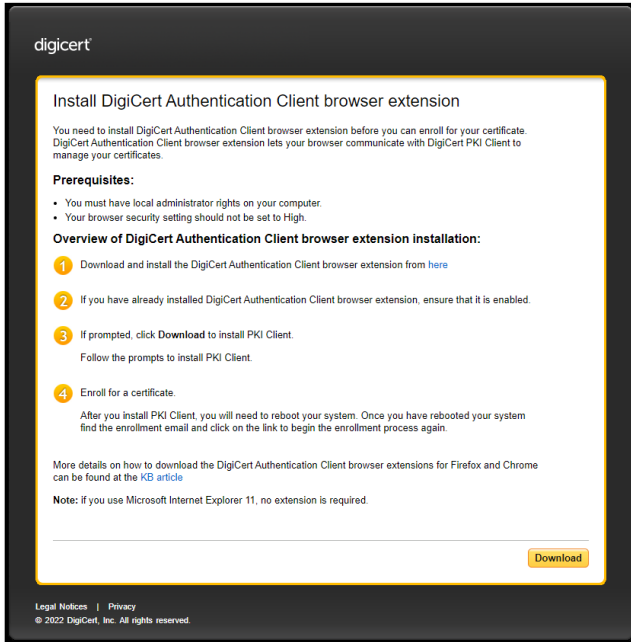
## Enrollment code not recognized

You may receive the following error messages if you have mistyped your enrollment code or if it has been more than 30 days since your Enrollment Request was approved. Your enrollment code can be obtained by contacting [cert.admin@aes0.ca](mailto:cert.admin@aes0.ca).



# Chrome or Edge Extension Error

Receipt of the below error messages may be received if there was an issue with installing an extension in your browser.



More information can be found by visiting the DigiCert website at: <https://knowledge.digicert.com/generalinformation/mpki-8-pki-client---chrome-extension-installation.html>.

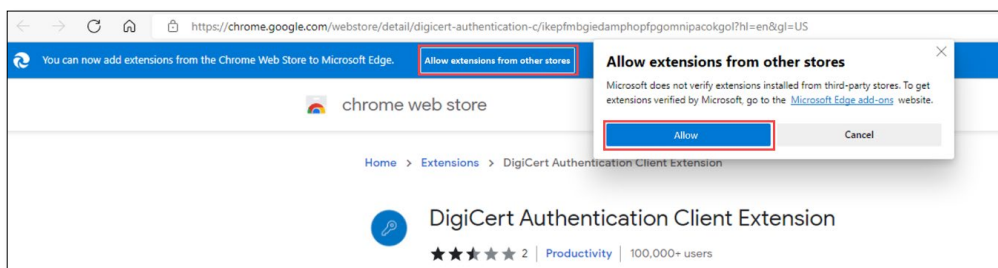
Instructions for installing the extension in Edge and Chrome follow below.

Note: The AESO's supported browser is Microsoft Edge.

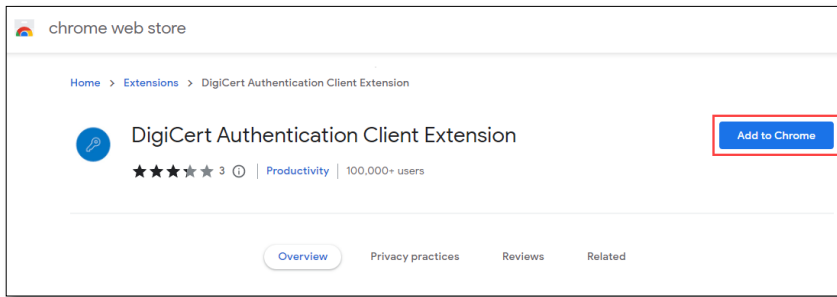
## Installing the Extension in Edge

1. Open below link in the Edge browser: <https://chrome.google.com/webstore/detail/digicert-authentication-c/ikepfmbgiedamphofpgomnipacokgo/>
2. Click on 'Allow extensions from other Stores' and a pop-up message will appear. Select 'Allow'.

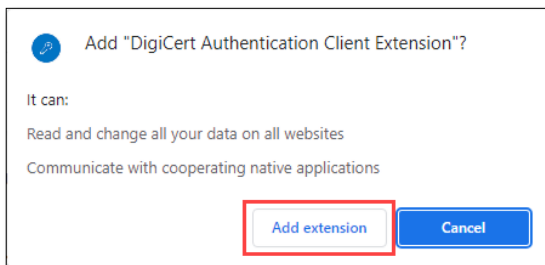
**Note:** Pop-ups may need to be enabled to allow the extension to be installed.



3. Click on the 'Add to Chrome' button.



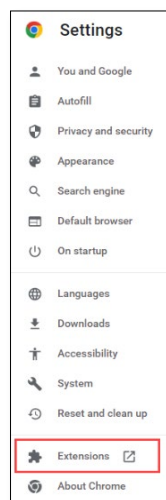
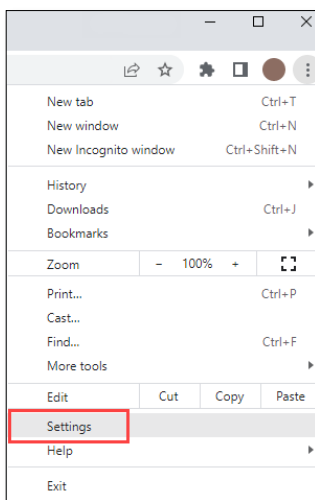
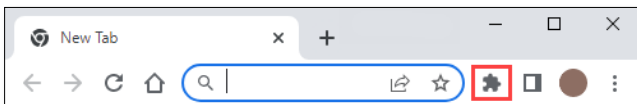
4. The following message will appear to add extension. Click on 'Add extension'.



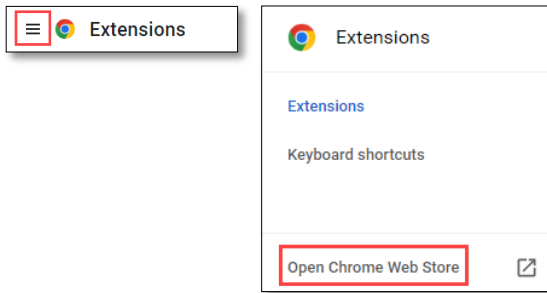
5. Retry the certificate installation process.

## Installing the Extension in Chrome

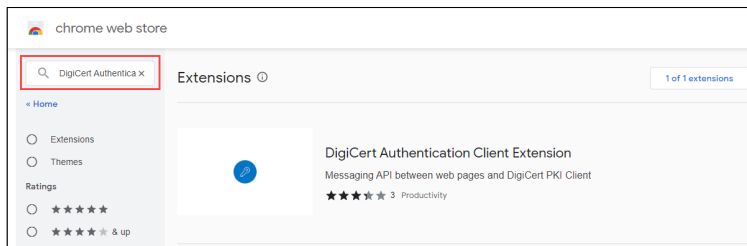
1. Open Google Chrome browser.
2. Go to extensions page by either clicking on the 'Extensions' icon on the top right (highlighted in below screenshot), or navigating to '3 dot elipses > settings > Extensions'.



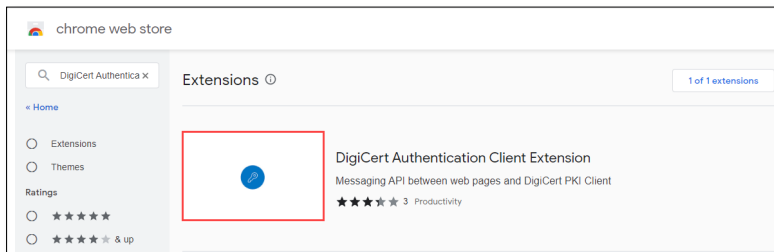
3. Click on 'Main menu', and then 'Open Chrome Web Store'.



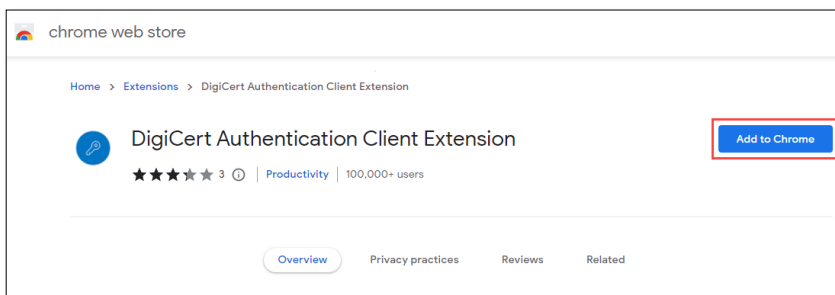
4. Search for 'DigiCert Authentication Extension' in the search box.



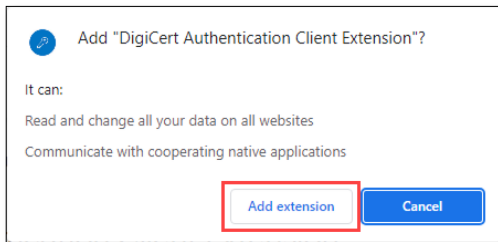
5. Click on the 'blue key symbol' to open the extension.



6. Click on 'Add to Chrome' button.



7. Click on 'Add extension'.

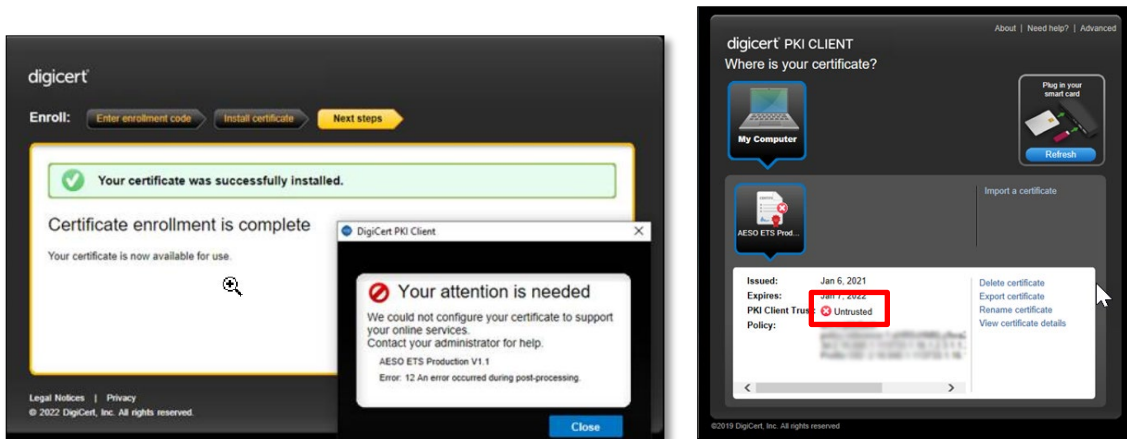


8. Retry the certificate installation process.

## Certificate not trusted – installation of Root Security Certificate

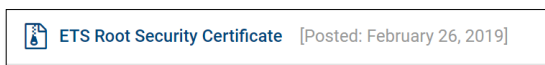
The following error messages may be displayed if there is an issue installing the root security certificate. A root security certificate is used to validate the individual digital certificates used to access ETS. The root security certificate is normally installed at the same time as an individual certificate. However, sometimes this process fails, and the root security certificate may need to be installed manually. The certificate can be found at <https://www.aeso.ca/market/market-participation/system-tools/energy-trading-system-tools/> - ETS Root Security Certificate. See installation instructions below.

**Note:** Access to ETS may still be possible without installation of the root security certificate.



To install the ETS Root Security Certificate, follow these instructions:

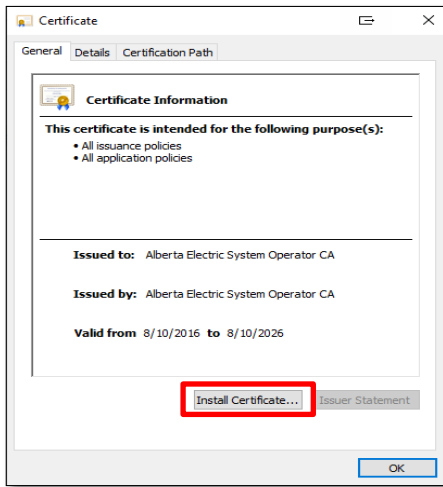
1. Select 'ETS Root Security Certificate'.



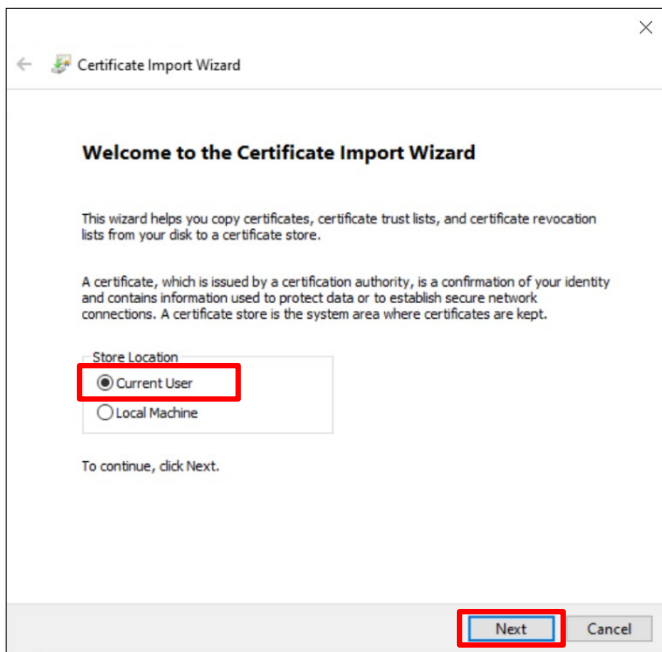
2. Open the downloaded zip file.



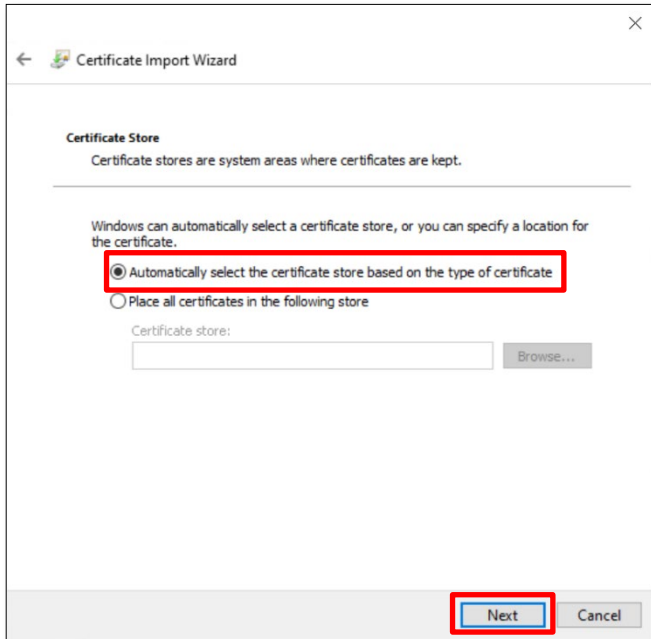
3. Double click on the Security Certificate file. You will see the following dialog box. Click 'Install Certificate'.



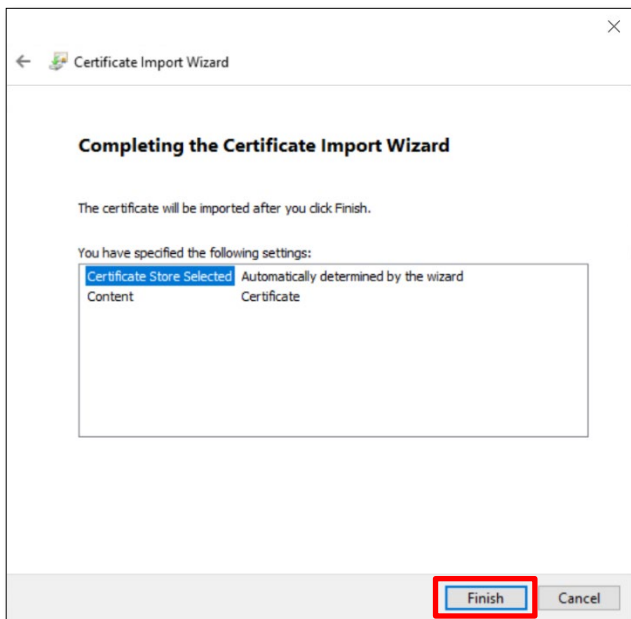
4. Select 'Current User' and 'Next'.



5. Select 'Automatically select the certificate store based on the type of certificate' and 'Next'.



6. Select 'Finish'



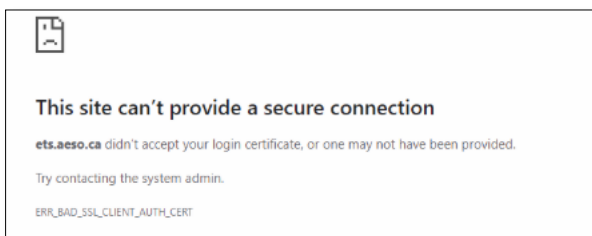
Once the certificate is installed you will need to close all browser windows as well as the PKI Client.

7. Reopen the PKI Client application. The certificate should now be shown as 'valid'.



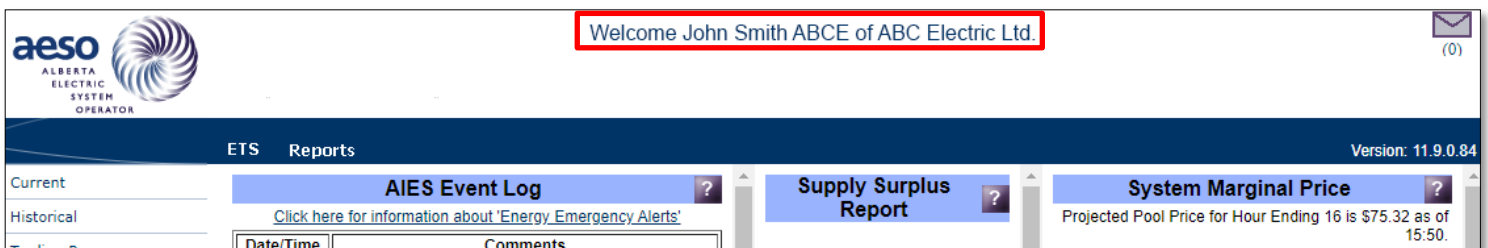
## Firewall preventing you from accessing your certificate

Some companies have firewalls that prevent the PKI Client application from retrieving a certificate. If you have followed the instructions and still cannot see your certificate, you may wish to contact your IT Department and verify PKI Client is not being blocked.



## Unable to Login to ETS

After installing your certificate and you have attempted to login to ETS, successful login will be indicated by a banner at the top of the screen welcoming you by name to ETS, "Welcome [your certificate name] of [company]".



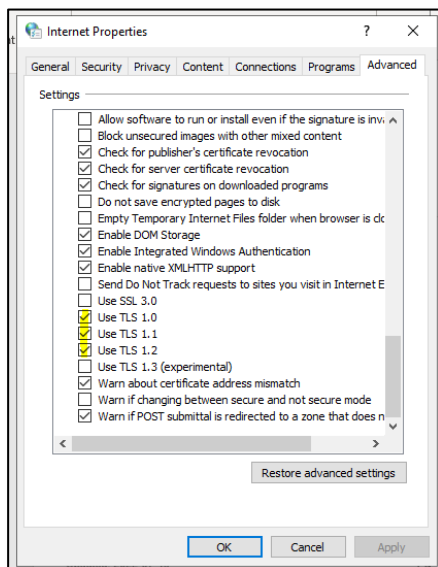
If you do not see your certificate name and you still see a login button in the top right corner (shown below) or if you have multiple certificates and you do not see your certificate in the list, this suggests your certificate is not properly installed.



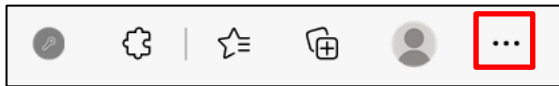


Below is a list of troubleshooting tips you can try:

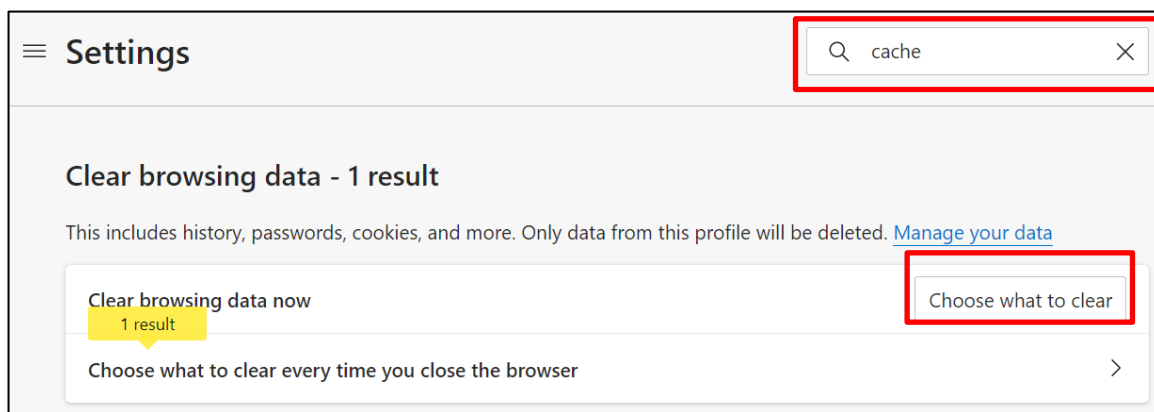
- Restart your computer.
- Confirm DigiCert PKI Client application was installed properly by searching for the application on your start menu and confirm it loads correctly.
- Confirm DigiCert PKI Client application installed is the latest version. This can be verified by opening DigiCert PKI Client, clicking 'About' and 'Check for updates'.
- In the DigiCert PKI Client application, confirm you see your certificate and confirm the certificate is not expired.
- Verify your certificate is listed in the 'personal' store of your browser (settings section) and the expiry date is in the future.
- Check to see if the Root Security certificate has been installed (instructions on installation of this certificate are noted in this document).
- Installation of your certificate may require additional operating system privileges. Check with your IT department.
- Make sure cookies are enabled as cookies are required for ETS to function properly.
- Check to see if your company firewall is blocking the ETS website. A timeout error may appear or the process never completes and ETS does not load. AESO has two IP addresses. Ensure your company firewall is not blocking these.
- If you selected the wrong certificate (e.g. the ETS training certificate), this will now become the default certificate used for ETS. Log into ETS, if it does not ask for a certificate and you do not see the Welcome line at the top of the screen start a new session in Edge by right clicking the Edge icon (in the start menu or in the task bar) and select 'New InPrivate window'. To reset the default certificate, log off your account or restart your computer, and then log in to ETS selecting the correct certificate.
- Check SSL configuration - To do so, open 'Internet Options' in Windows Control Panel. Click the 'Advanced' tab. Scroll down and ensure that TLS is enabled. For Windows TLS 1.3, ensure that TLS 1.2 is enabled and both TLS 1.0 and TLS 1.1 are disabled. Note – TLS 1.3 only works on Windows 11.



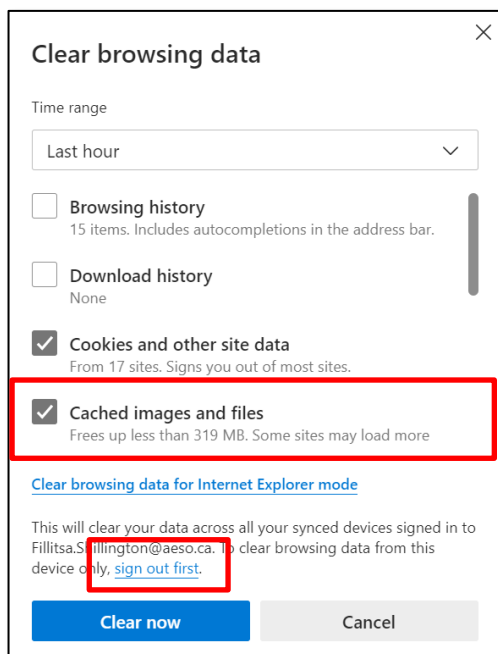
- Disable the HTTPS deep inspection - Network cybersecurity tools will sometimes be installed that are decrypting and re-encrypting network traffic to scan for malware. Sometimes this requires sites to be 'whitelisted', otherwise the connection between the browser and the website will fail (the browser and the website will detect that a third party has tampered with the connection). Asking for the deep inspection to be disabled will allow you to then test if connectivity works. If it does, then your security team will need to do the whitelisting of ets.aeso.ca.
- Clear cache - Close all browsers and open 'Internet Options' in Windows Control Panel. Click the 'Content tab'. Click the 'Clear SSL state' button. Open an Edge browser. Click the "..." beside your profile. Select 'Settings' from the drop down menu.



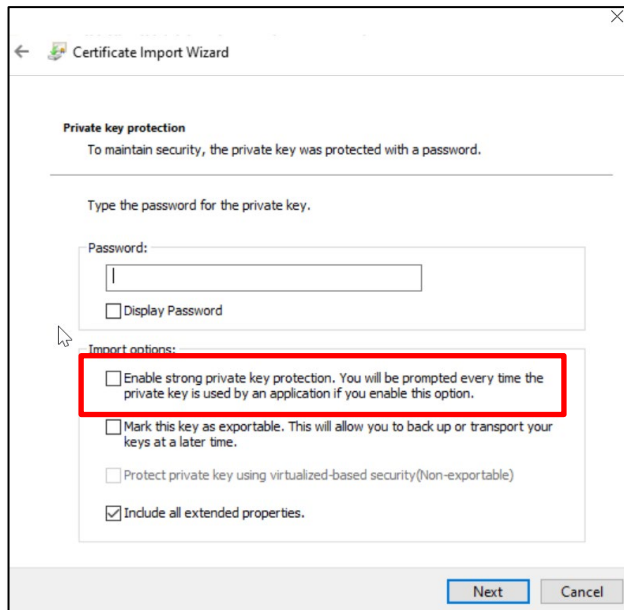
Enter "cache" in the search box. In 'Clear browsing data now' select 'Choose what to clear'.



Change the drop down to 'All time'. Uncheck 'Browsing History' and 'Download History'. Ensure only 'Cookies and other site data' and 'Cached images and files' are checked. If you use your Edge profile on multiple machines, you can 'sign out' on this browser first and then click the 'Clear now' button if you only wish to clear the cache on this machine.



- Certificate import **cannot** have strong private key protection enabled. When installing the certificate using Windows Certificate Import Wizard to import the certificate (instead of via PKI Client), at the step when you enter the certificate password you must uncheck 'Enable strong private key protection'.



## Installing certificates on a new computer

If you still have access to your old computer, you may follow the instructions below.

1. Export your digital certificate. For step-by-step instructions refer to our Exporting a Digital Certificate Guide at <https://www.aeso.ca/market/market-participation/system-tools/energy-trading-system-tools/>.
2. Transfer the exported certificate to your new computer.
3. If you have not already done so, download and install DigiCert PKI Client application on your new computer. For step-by-step instruction refer to our ETS Digital Certificate Enrollment Guide located at <https://www.aeso.ca/market/market-participation/system-tools/energy-trading-system-tools/>.
4. Import your digital certificate. For step-by-step instructions refer to our Importing Digital Certificates Guide at <https://www.aeso.ca/market/market-participation/system-tools/energy-trading-system-tools/>.

If you **did not export your existing certificate(s) before losing access to your old computer**, you may request reissue of your certificate by sending an email to [cert.admin@aeso.ca](mailto:cert.admin@aeso.ca). Your existing certificate will be revoked, and a new certificate will be issued.