WWFIRST Certificate Install - Windows

(If you require assistance, please contact daniel.delattre@wwfirst.ca)

What is a Digital Certificate and why use it?

What is a Digital Certificate

A Digital Certificate is an electronic "password" that allows a person or organization to exchange data securely over the Internet using the public key infrastructure (PKI). Digital Certificate is also known as a public key certificate or identity certificate. It's similar to a passport or driver's license. It lets you know "officially" who each person or organization is.

Why is security needed on the Internet?

The Internet is an open communications network that was not originally designed with security in mind. If we want to use the Internet as a communication tool, users must be able to communicate securely.

What does security provide?

- Identification / Authentication:

The persons / entities with whom we are communicating are really who they say they are.

- Confidentiality:

The information within the message or transaction is kept confidential. It may only be read and understood by the intended sender and receiver.

- Integrity:

The information within the message or transaction is not tampered accidentally or deliberately with en route without all parties involved being aware of the tampering.

- Non-Repudiation:

The sender cannot deny sending the message or transaction, and the receiver cannot deny receiving it.

- Access Control:

Access to the protected information is only realized by the intended person or entity.

Why a WWFIRST Certificate Authority (CA)?

Why do I need to install a new WWFIRST Certificate Authority?

A Certificate Authority (CA) issues digital certificates that contain a public key and the identity of the owner. The matching private key is not made available publicly, but kept secret by the end user who generated the key pair.
The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates. CAs use a variety of standards and tests to do so.
In essence, the Certificate Authority is responsible for saying "yes, this person is who they say they are, and we, the CA, verify that". It's similar to a passport or driver's license office.

Why create our own?

If we want to create an officially recognized Certificate to communicate with the Elegoo Smart Robot Cars, it will cost us several thousands of dollars each year. If we create our own, it's free.

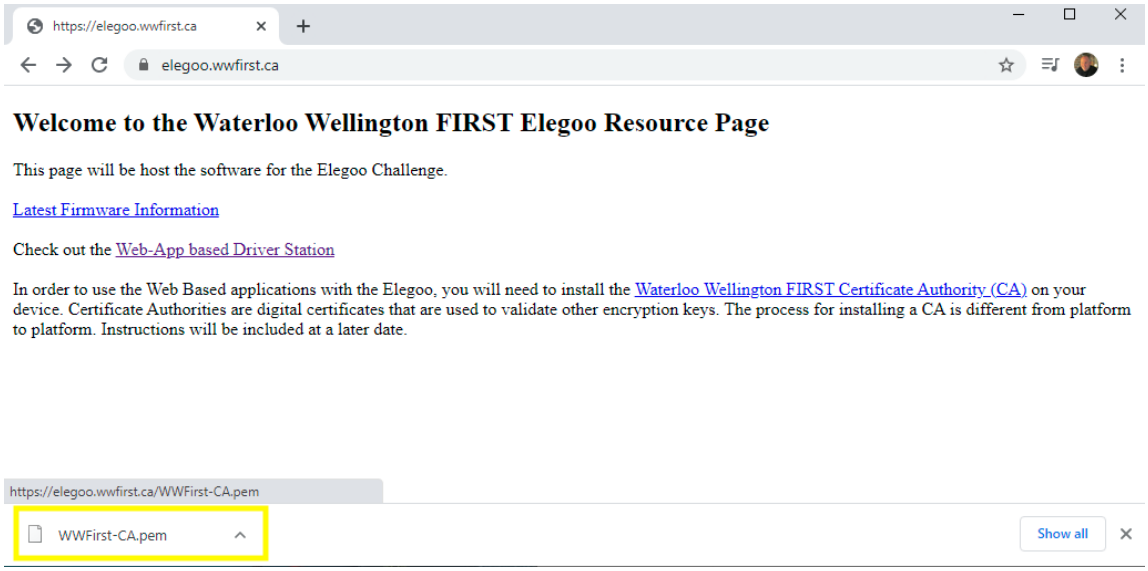
The only trust is between the Driver Station server, the Elegoo Smart Robot Car and the device you use to control the robot car. The certificates are *not* used for anything else, and we can assure that each robot car and control device communicates with the server over their own "secure channel".

Okay, so how do I install this now?

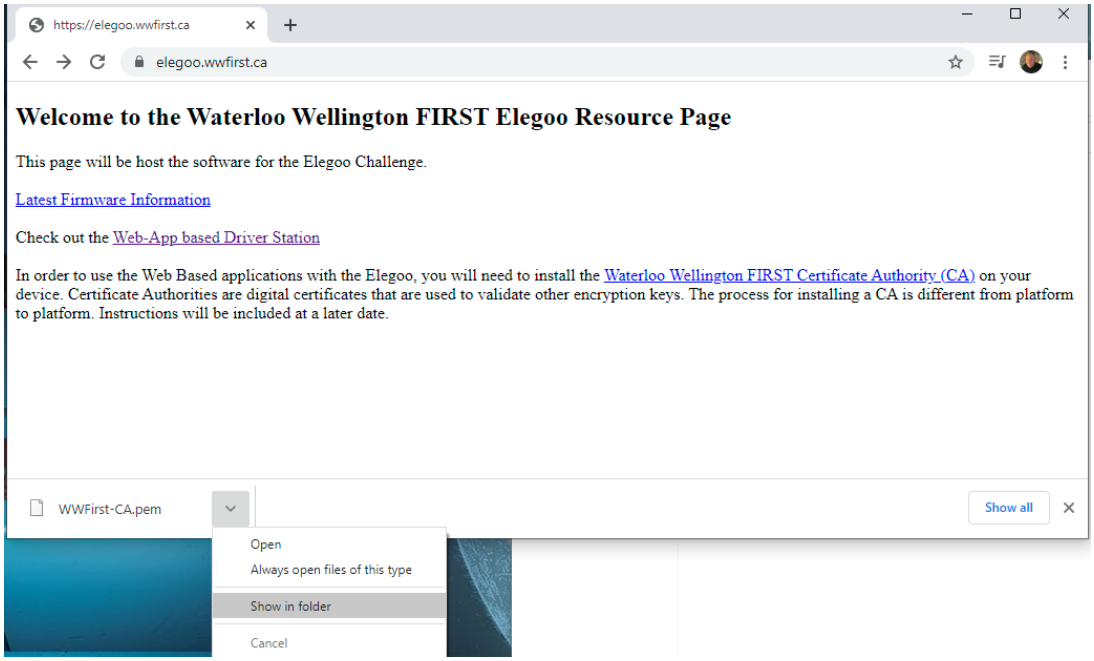
This is done slightly differently in each Operating System, but we will guide you step by step with as many screenshots as possible.

1. Navigate to the https://elegoo.wwfirst.ca site

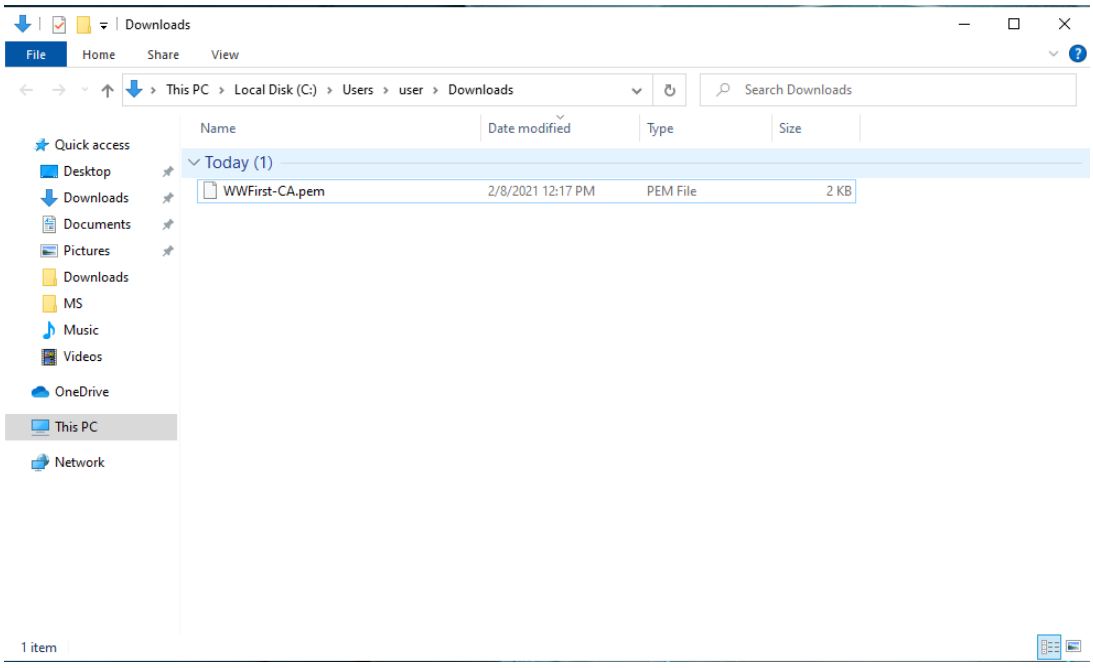
2. Click on the Waterloo Wellington FIRST Certificate Authority link and download the WWFIRST-CA.pem file.



3. Right click on the file and click on Show in folder.

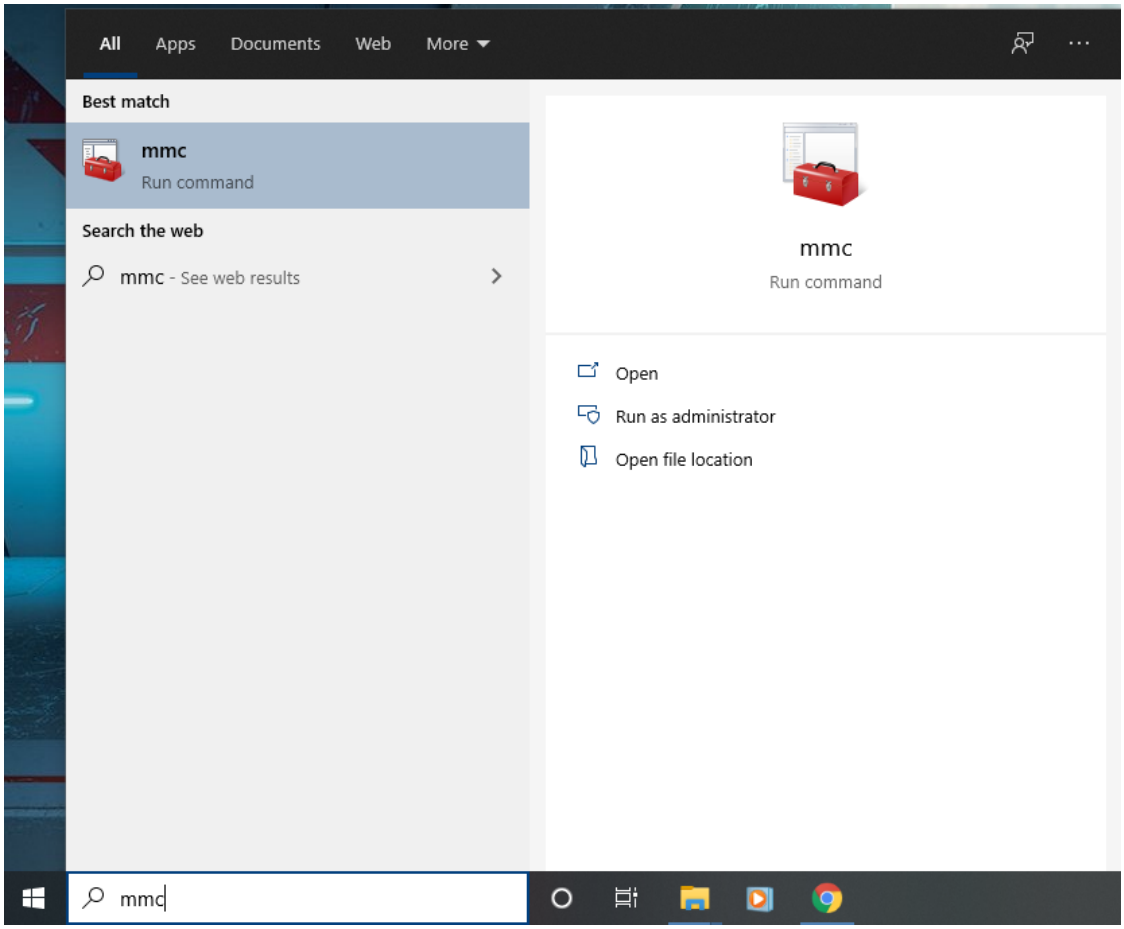


4. You will notice the following file: WWFirst-CA.pem. Remember where it is on your computer (the “This PC” bar at the top).

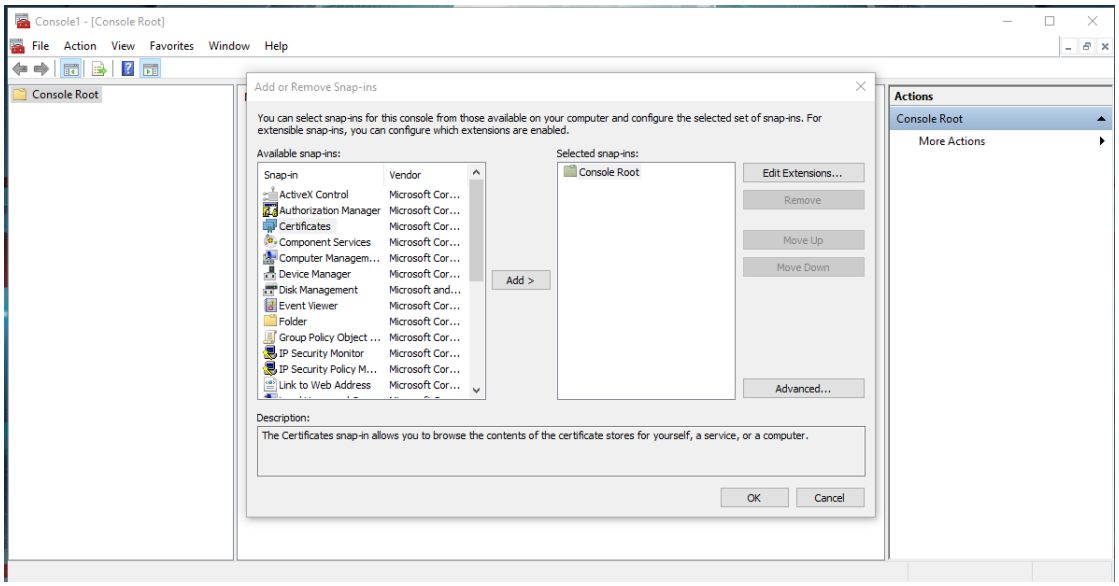


We will now install this root certificate.

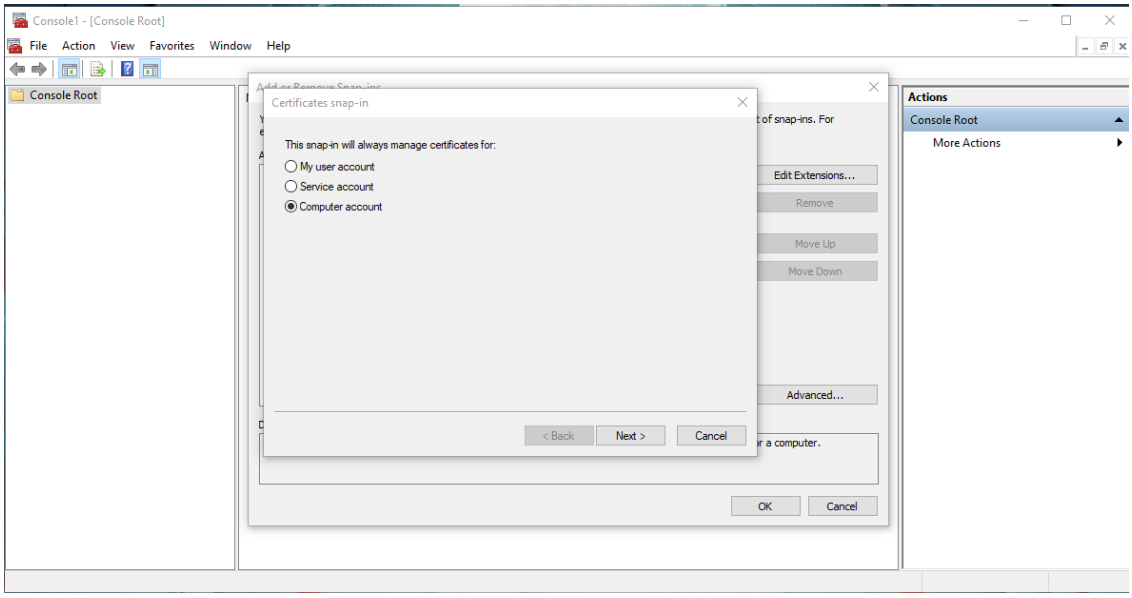
5. Click on the search space at the bottom and type in mmc and press enter.



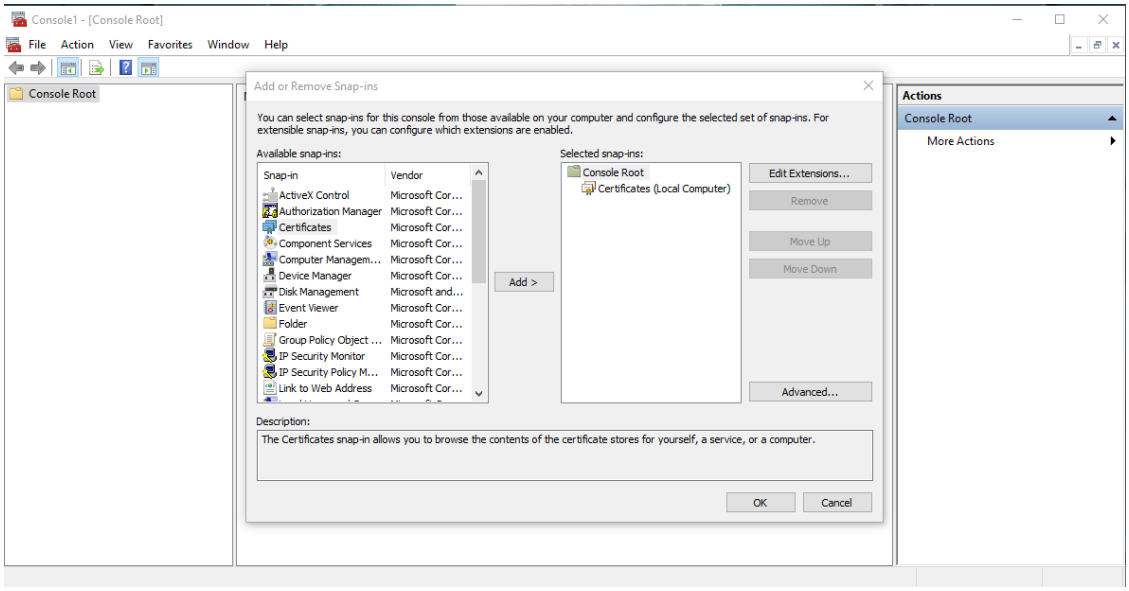
6. Once the MMC opens, Go to File menu, click Add/Remove Snap In, and add the Certificates snap-in for Local Computer.



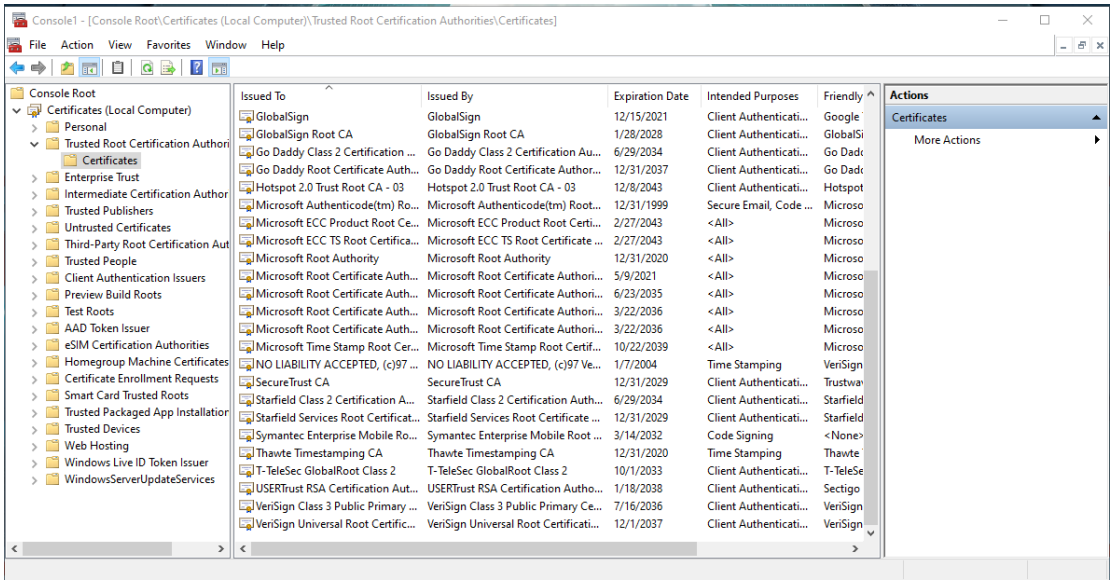
7. Make sure to pick “Computer Account” ! Select “Local Computer” if that option comes up.



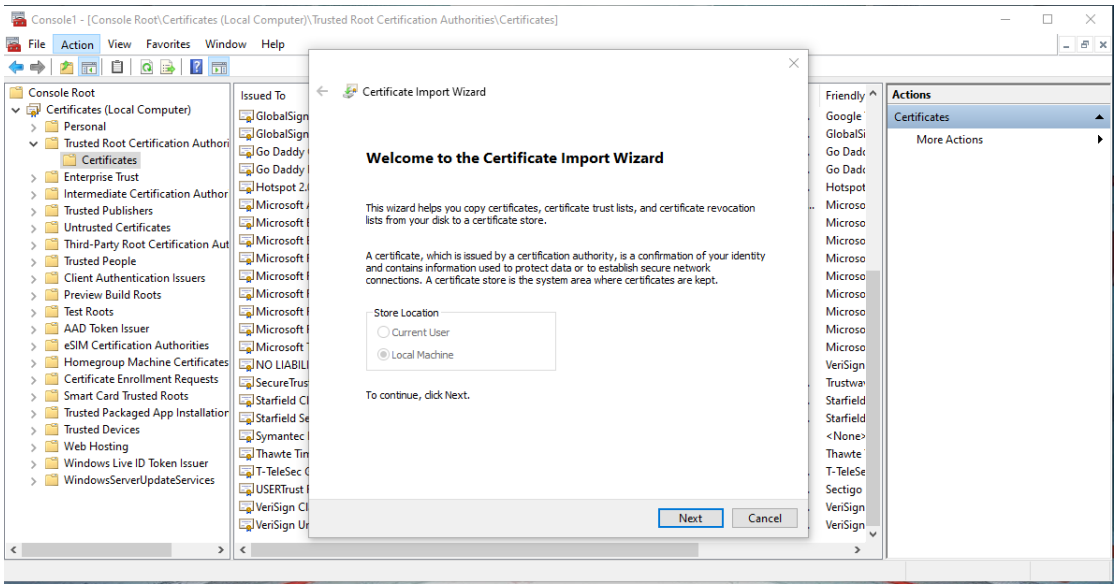
8. You will now see the following window and click OK.



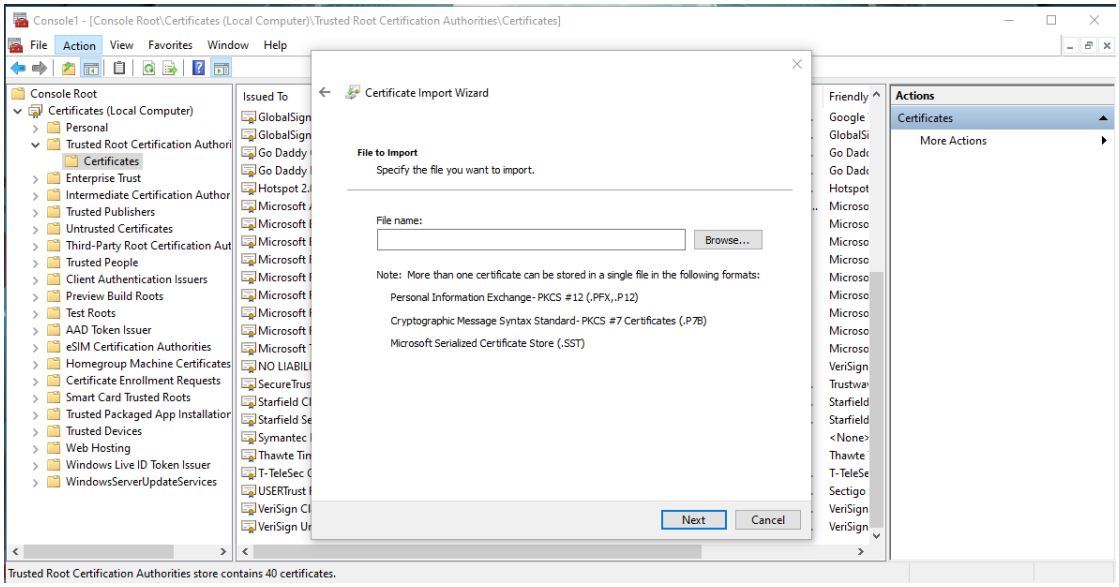
9. The following window will now pop up. If the folder tree isn’t opened, click the arrow to the left of “Certificates”. Navigate to “Trusted Root Certification Authority” and click on its arrow to see the Certificates folder.



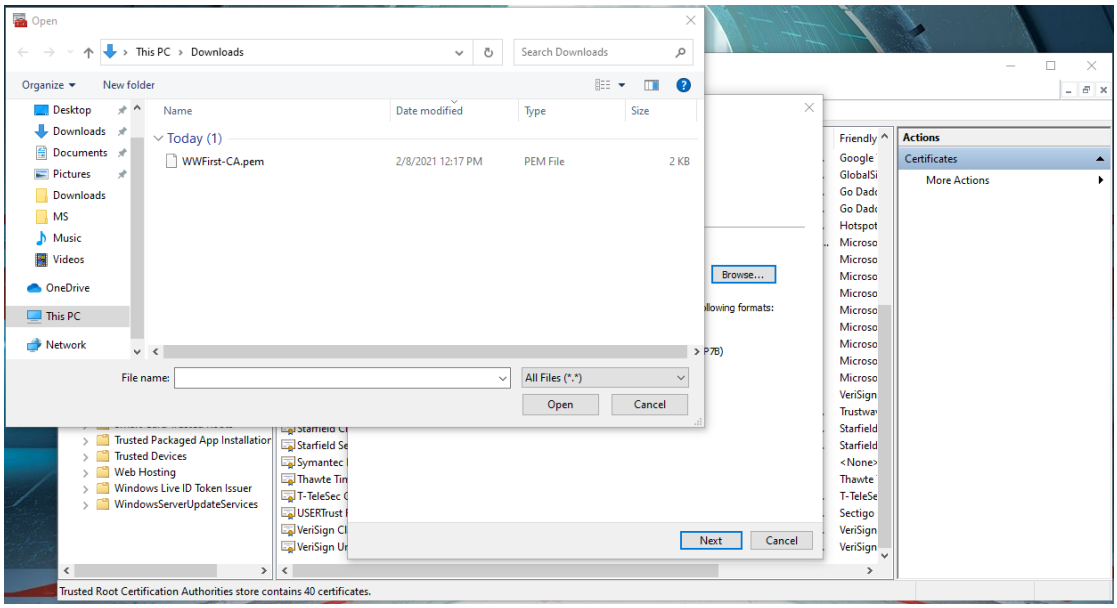
10. Right-click in the “Certificates” folder and select All Tasks > Import.



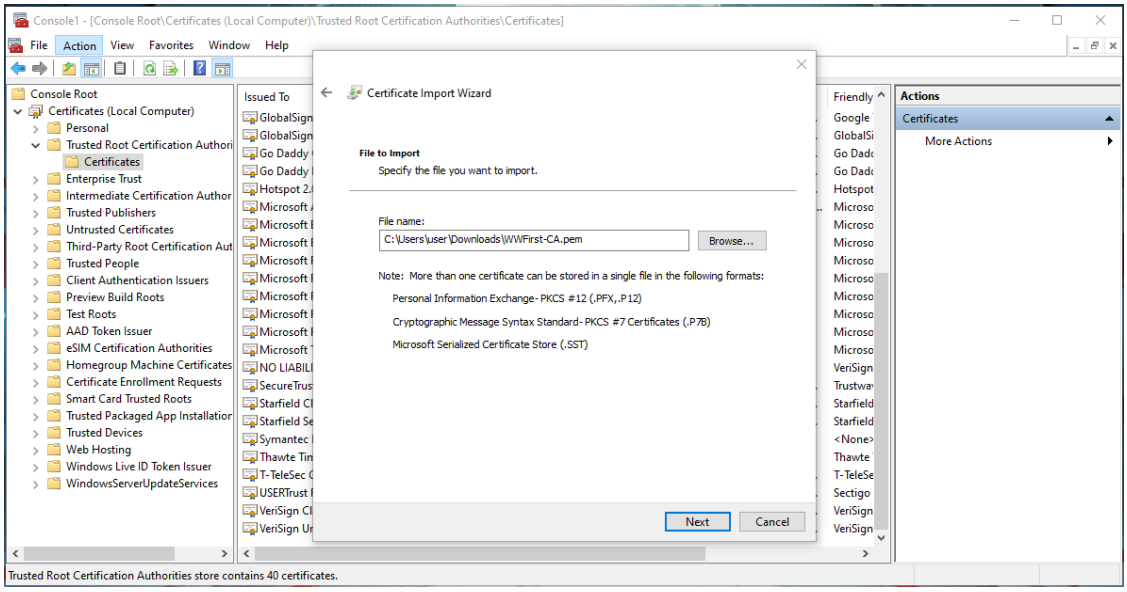
11. Click next to be able to browse to the file we previously downloaded. Click Browse.



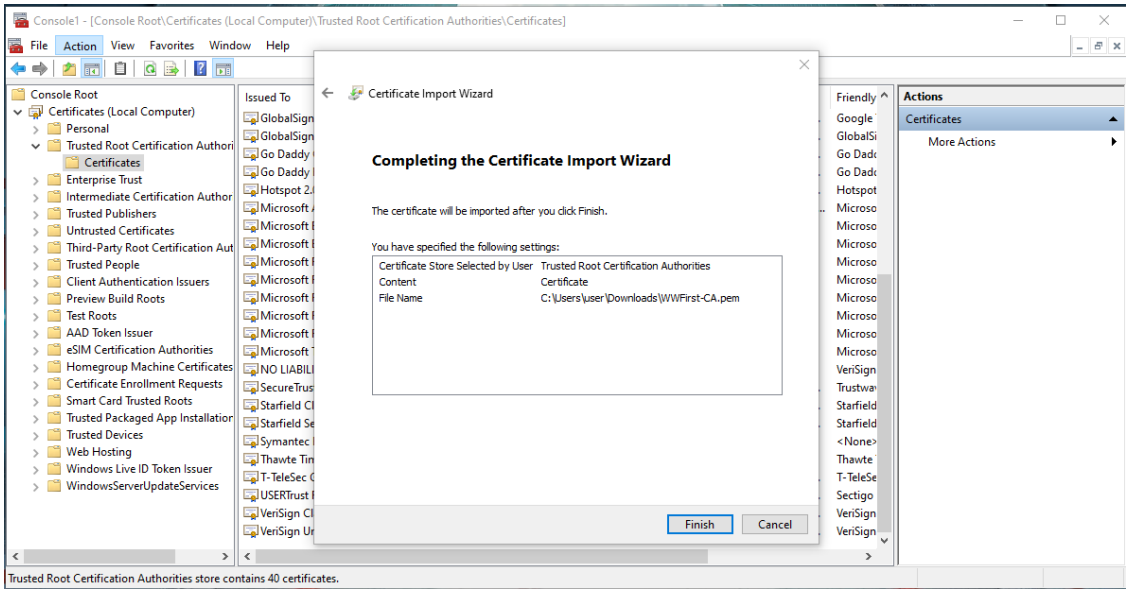
12. Make sure to select “All Files” to the right of the File name space and look for the WWFirst-CA.pem file. Select the file and click Open. Click Next.



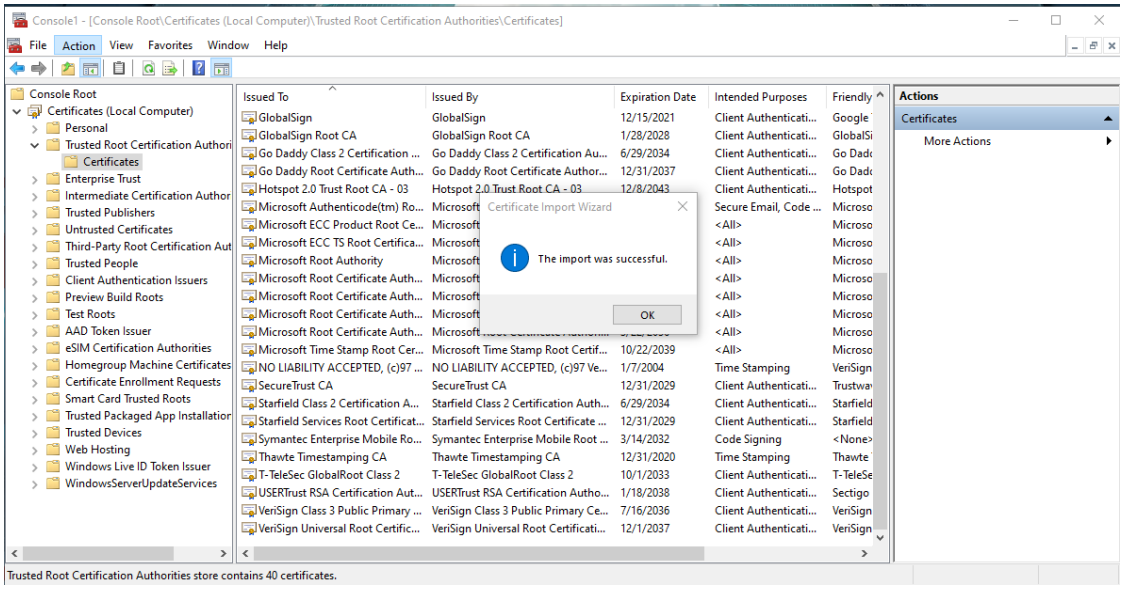
13. Click the Next button.



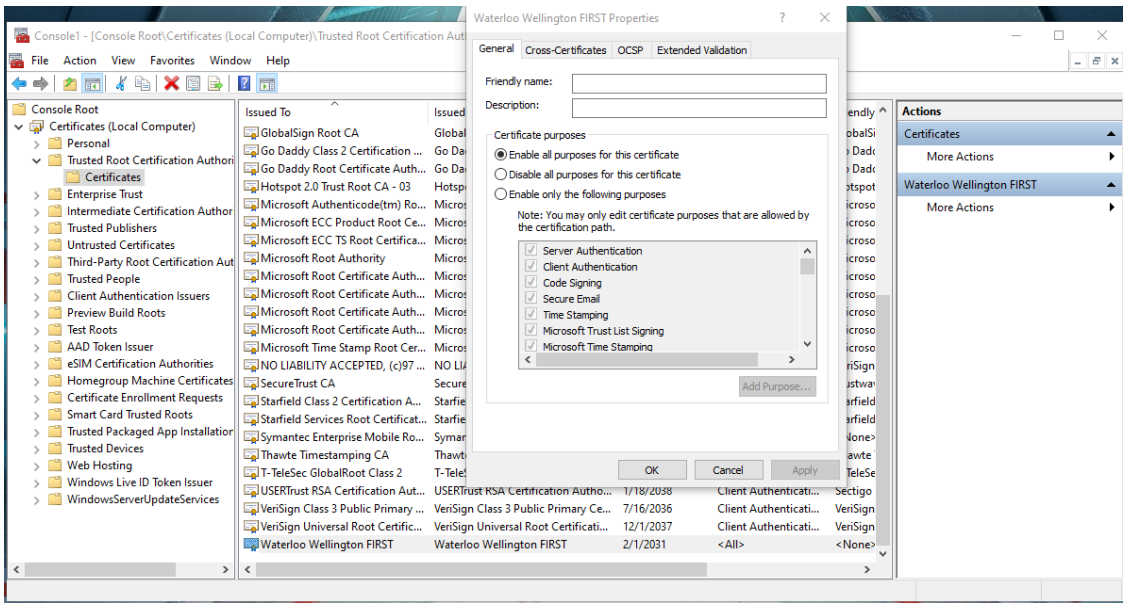
14. Click Finish button to make sure the certificate is added.



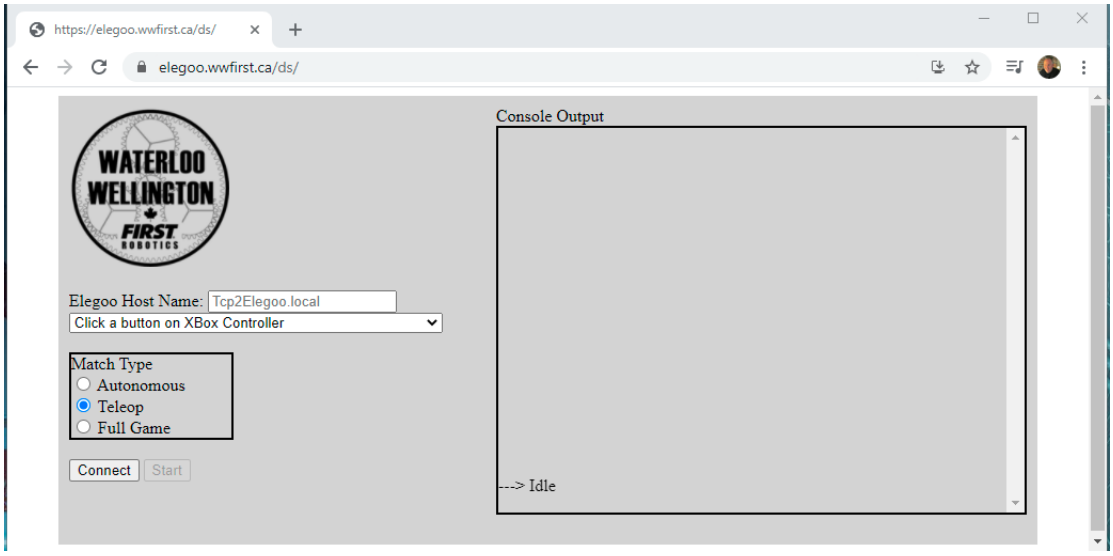
15. Make sure the import was successful.



16. You should now see the Waterloo Wellington FIRST certificate in the list. Check the properties (right-click > Properties) to ensure “Enable all purposes for the certificate” is checked off.



17. You can now navigate to the online Driver Station at https://elegoo.wwfirst.ca/ds/.



That's it.

When you close the MMC console you don't have to save the console settings. That's just to save having the Certificates snap in listed in your console. It doesn't affect the installed certificates.