



WWFIRST Certificate Install - MacOS

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

What is a Digital Certificate and why use it?	2
What is a Digital Certificate	2
Why is security needed on the Internet?	2
Why a WWFIRST Certificate Authority (CA)?	3
Why do I need to install a new WWFIRST Certificate Authority?	3
Why create our own?	3
Okay, so how do I install this now?	4



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

Welcome to the Waterloo Wellington FIRST Elegoo Resource Page

This page will be host the software for the Elegoo Challenge.

[Latest Firmware Information](#)

Check out the [Web-App based Driver Station](#)

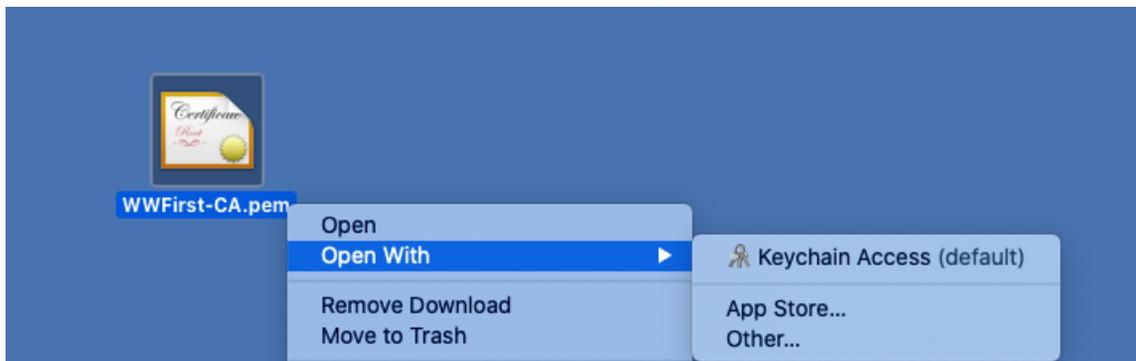
In order to use the Web Based applications with the Elegoo, you will need to install the [Waterloo Wellington FIRST Certificate Authority \(CA\)](#) on your device. Certificate Authorities are digital certificates that are used to validate other encryption keys. The process for installing a CA is different from platform to platform. Instructions will be included at a later date.

2. Click on the Waterloo Wellington FIRST Certificate Authority link and download the WWFIRST-CA.pem file. Moving forward, we moved the downloaded file to the desktop to make it easier to take screenshots.

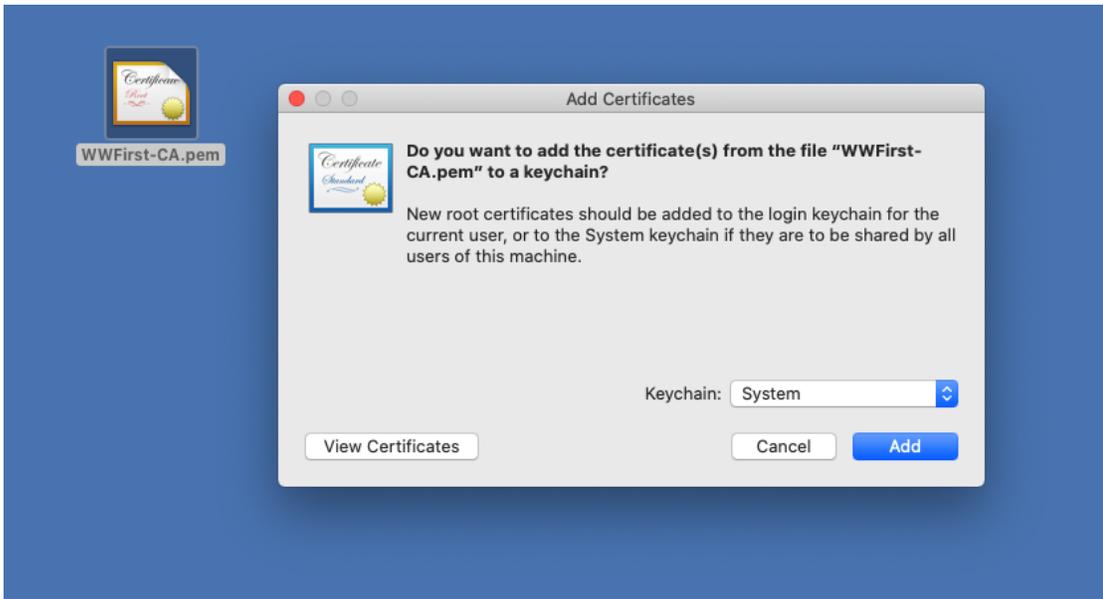
In order to use the Web Based applications with the Elegoo, you will need to install the [Waterloo Wellington FIRST Certificate Authority \(CA\)](#) on your device. Certificate Authorities are digital certificates that are used to validate other encryption keys. The process for installing a CA is different from platform to platform. Instructions will be included at a later date.



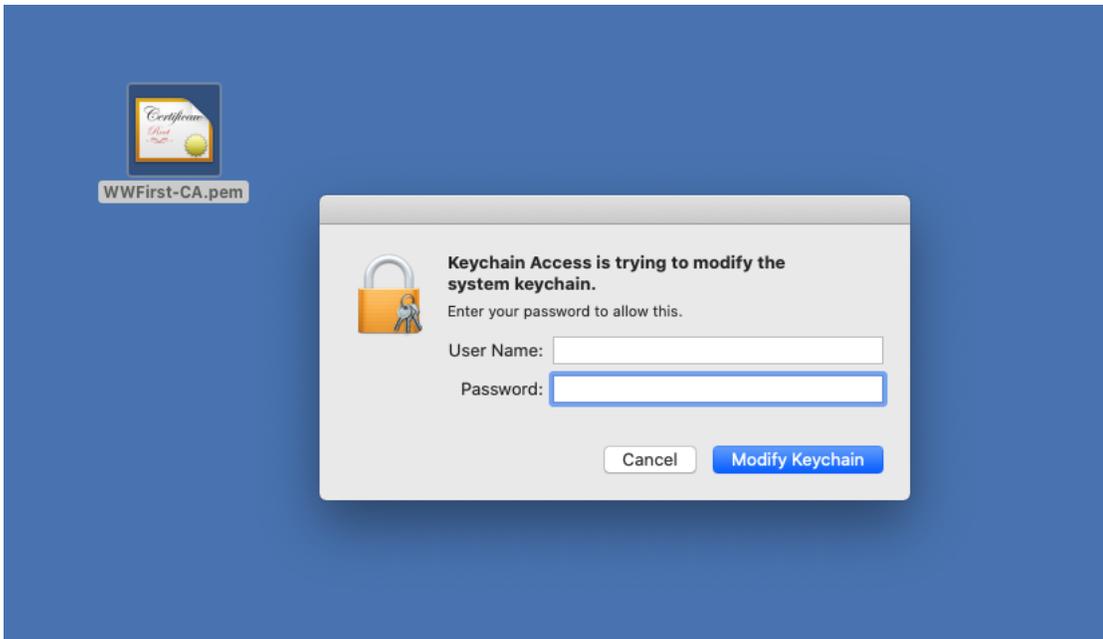
3. Right click on the file and click on Open With... Keychain Access



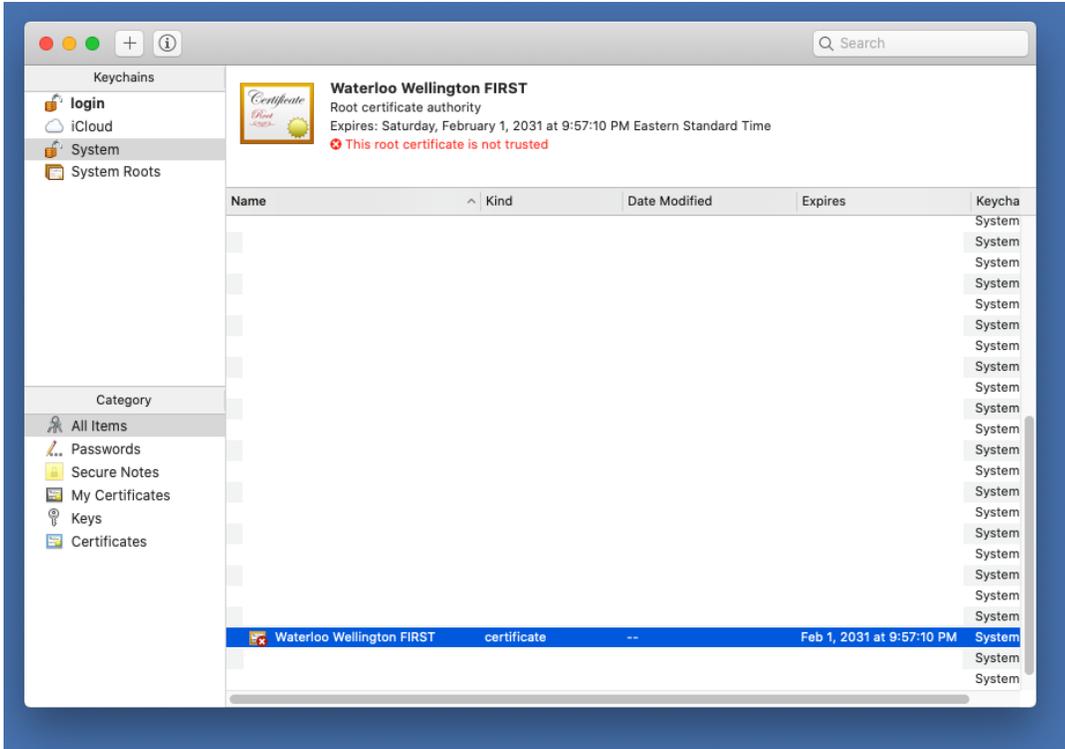
- Click on the Keychain dropdown list and pick “System”, then click the Add button.



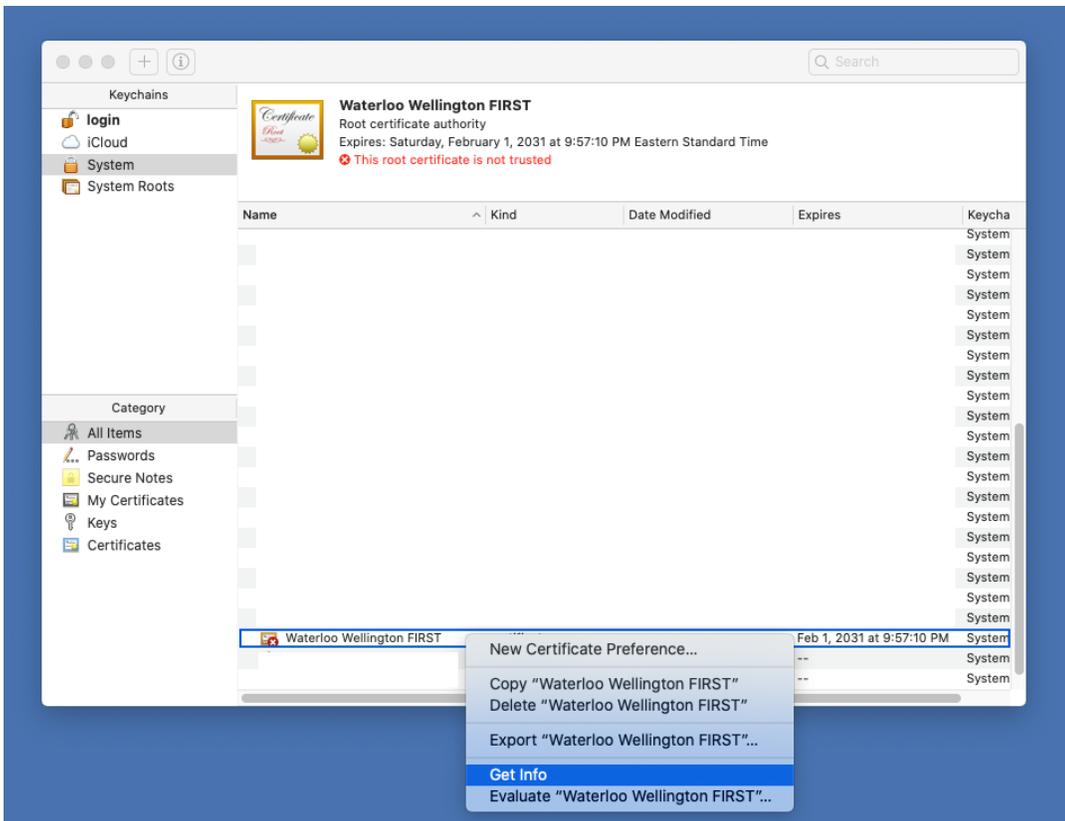
- Provide your administrative password to continue.



- Scroll down the list of “System” certificates to the Waterloo Wellington FIRST. Even though you installed the certificate, you cannot use it before you “Trust” it.

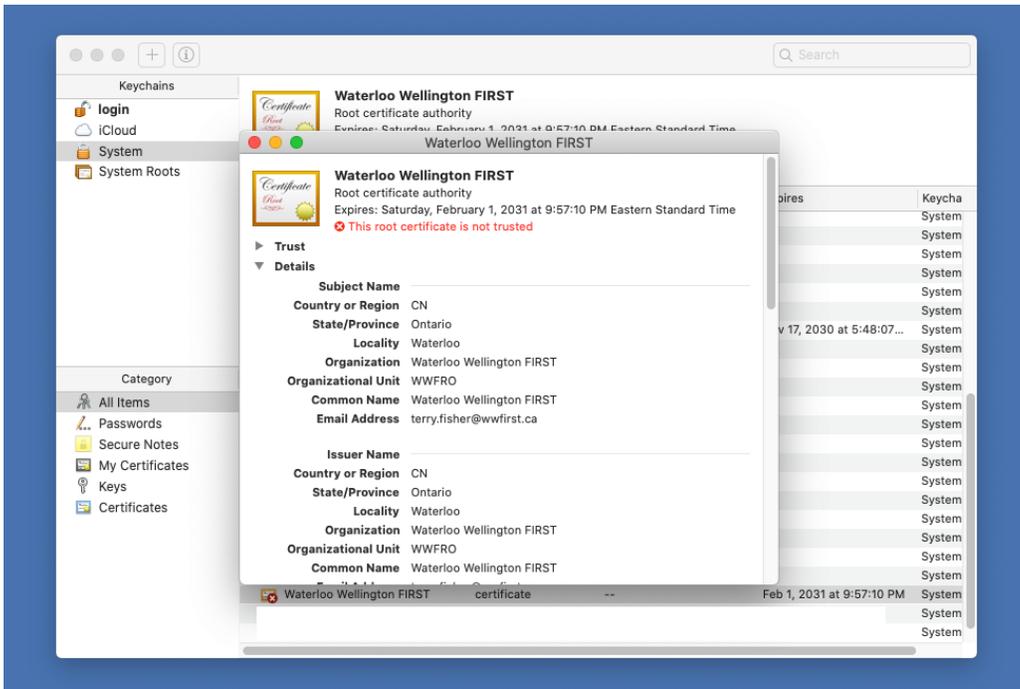


7. Right click the Waterloo Wellington FIRST certificate and click on the “Get Info” option.

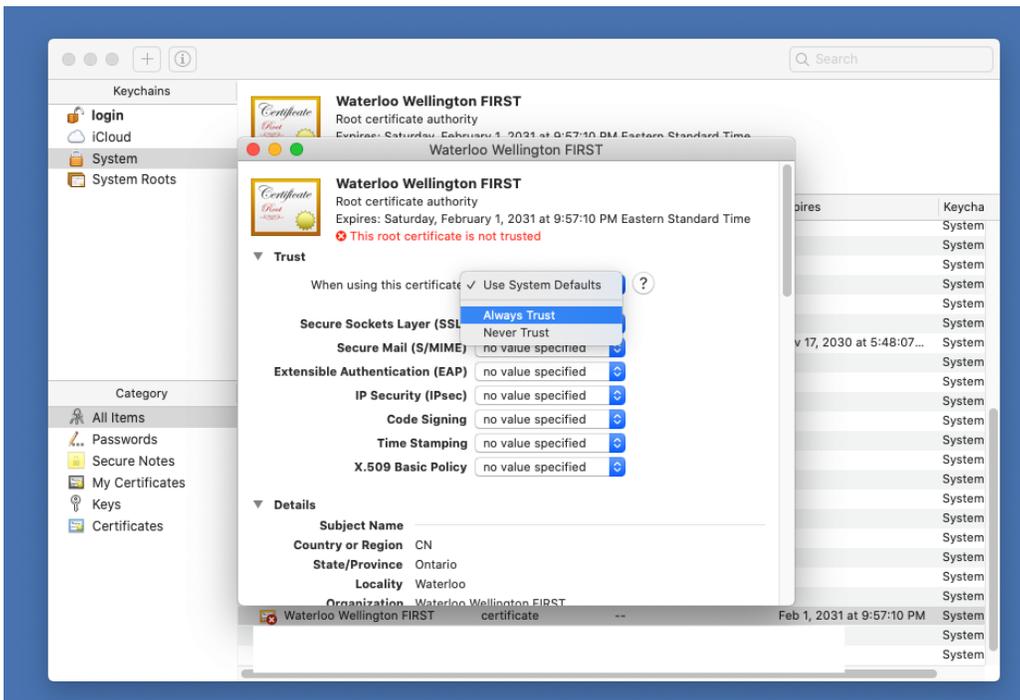




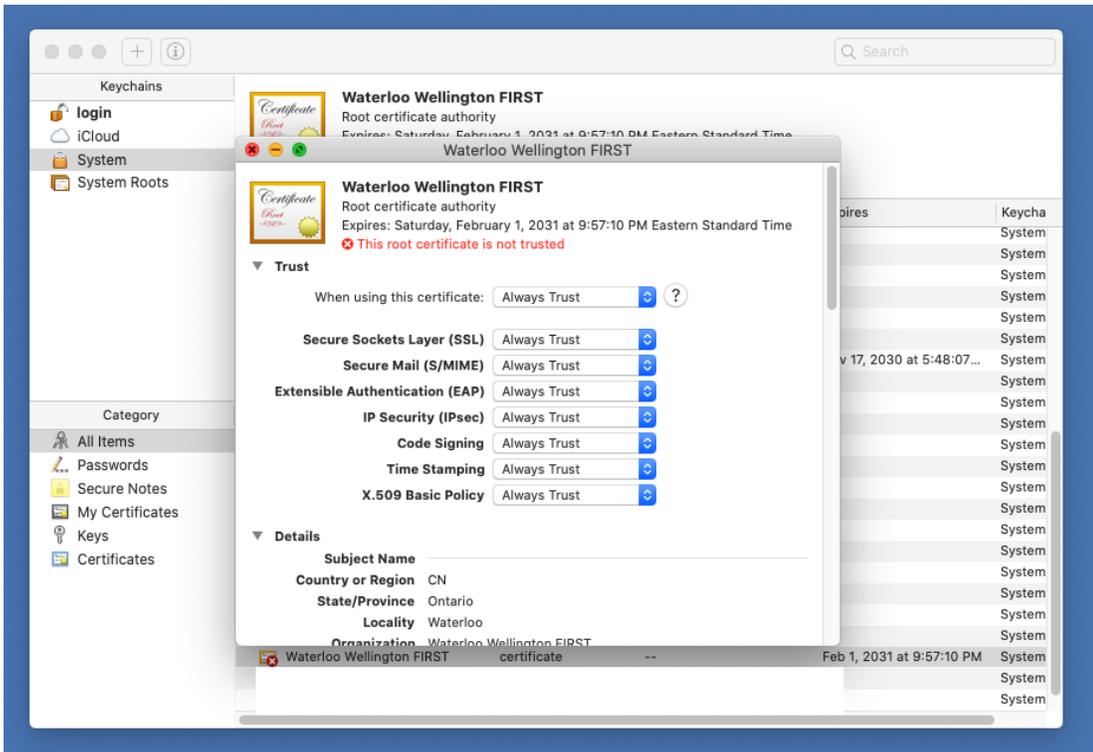
8. You will now see the full details of the WWFIRST certificate. Click on “Trust”



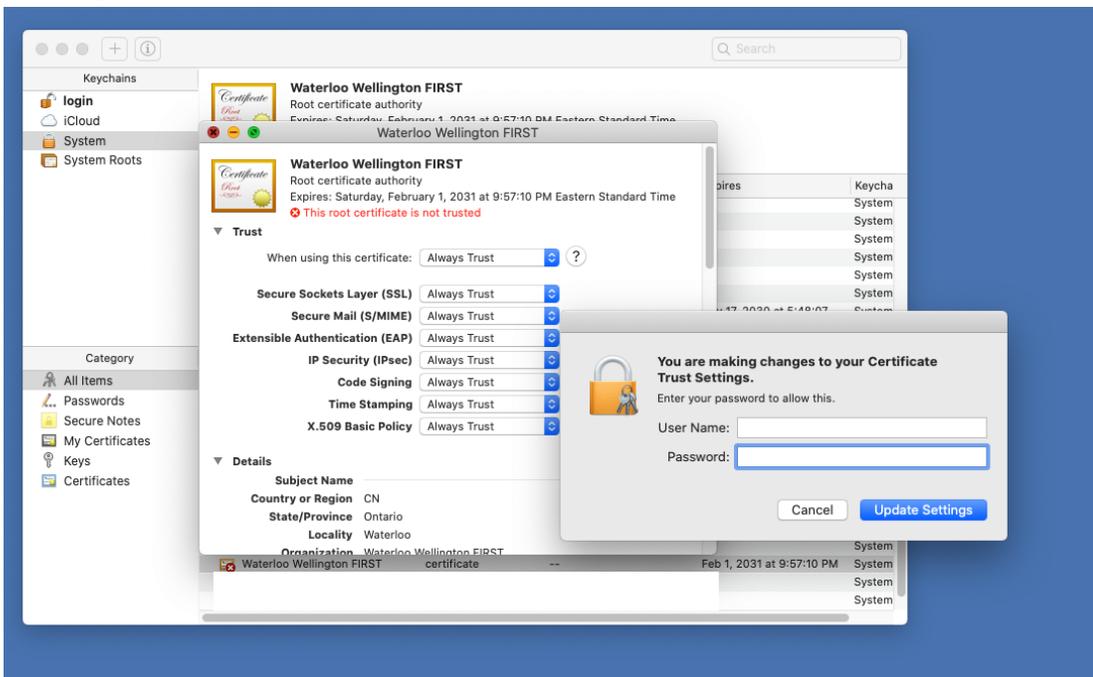
9. Scroll down the list and pick “Always Trust”.



10. This will modify the certificate to full trust.

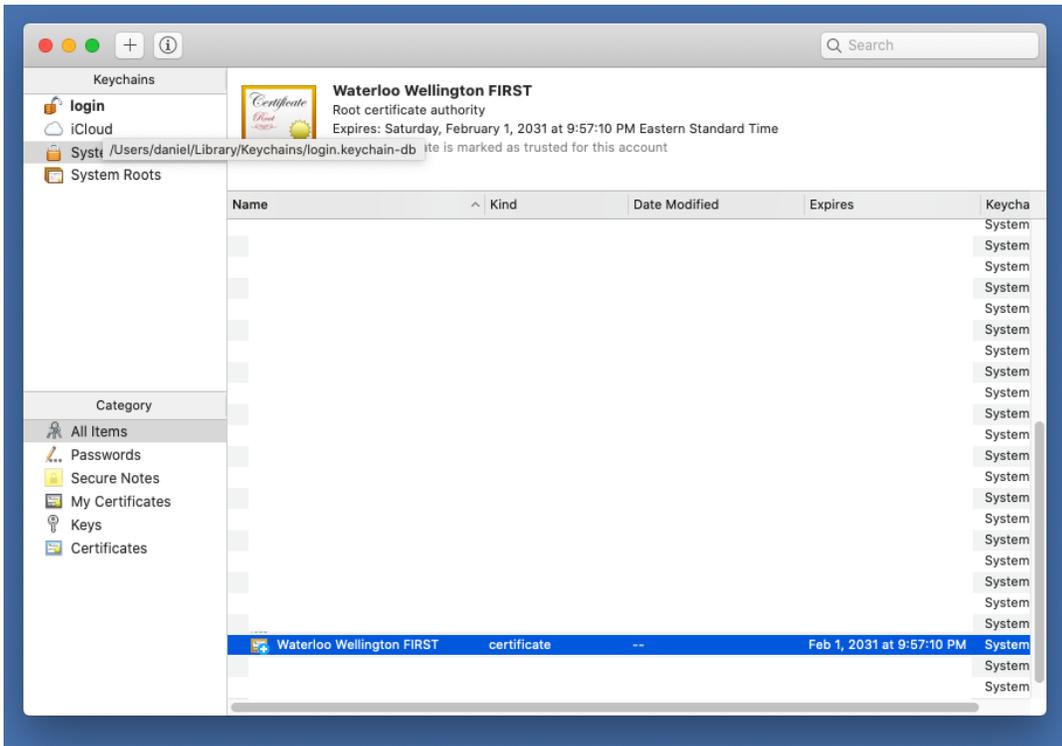


11. Once again provide your administrative credentials to proceed.

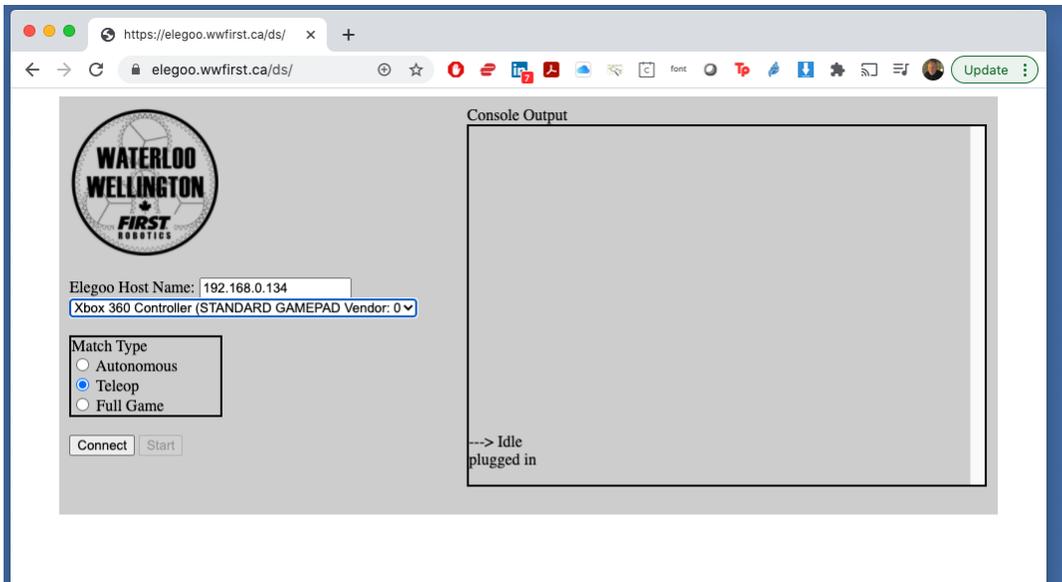




12. You will notice that the Waterloo Wellington FIRST certificate has no more Red X.



13. You are now ready to join the WWFIRST Online Drive Station.



That's it.