Eliminating Security Warnings When Using Walchem Default Certificate

When the user first accesses a controller that is programmed to use HTTPS Webserver Mode and the Default Certificate, the browser will redirect to a warning page saying that this website does not have a valid certificate and should not be trusted.

The user needs to click Advanced and then “Continue to <controller IP> anyway (not recommended)”. After that, they don’t get redirected anymore, but there is still a red warning in the address bar that the controller website is Not Secure.

On the Walchem website, we’ve added a link to our root certificate file. Any user can import this file into the Trusted Root Certification Authorities Store on their computer and after that, all controllers’ webpages will be accepted as secure, regardless of the browser used on that computer. The file name is iwakitrustservices.ca.crt.

Each browser in a PC has a slightly different path to follow to accomplish this. The Safari browser on MacOS has its own procedure. Save the root certificate to your computer and then follow the instructions as follows:

Chrome

Select the Customize icon ⋮

Select Settings

Select Security and Privacy

Select Security

Select Manage Certificates

Select Import to launch the Import Wizard, then Next

Browse to the file location to select the root file then Next

Select Place all certificates in the following store and choose Trusted Root Certification Authorities, then Next

Select Finish

Firefox

Select the Open Menu icon ☰

Select Options

Select the Privacy & Security tab

Select View Certificates

Select the Authorities tab and then Import…

Browse to the iwakitrustservices.ca.crt root file and choose Open

In the Downloading Certificate window, select Trust this CA to identify websites and then OK

Microsoft Edge

Select the Settings and More icon ···

Select Settings

Select Privacy Search and Services

Select Manage Certificates

Select Import to launch the Import Wizard, then Next

Browse to the file location to select the root file then Next

Select Place all certificates in the following store and choose Trusted Root Certification Authorities, then Next

Select Finish

Safari on MacOS

From the Go menu, select Utilities

Launch the Keychain Access utility

Under Keychains, select System

From the File menu, select Add Keychain…

Choose the iwakitrustservices.ca.crt root file, verify the Destination Keychain is System, and select Open

Select Always Trust