Walchem Controller Encryption Training

April 2022

We have added HTTPS TLS/SSL encryption to controller web pages.

HTTPS web pages are offered for all Intuition-6, Intuition-9, W900 controllers and W600 controllers equipped with an enhanced Ethernet card and running software versions v3.39 (W600/W900) or v4.11 (Intuition-6 or -9) or higher.

The TLS or SSL encryption makes the content of the web traffic non-readable to casual eavesdroppers on the network. When logging into the controllers, the user name and password are not visible.

For a browser to trust the HTTPS website (the controller webserver in this case) the controller needs to have a valid certificate signed by a trusted authority. If there is no certificate, or the certificate is not signed, the user will get a warning message every time they connect to the controller.

We will include a self-signed certificate in the controller, which will still generate a warning since it is not signed by a trusted authority. In addition, the user can install their own certificate by uploading a PEM (Privacy-Enhanced Mail) file or files.

Programming the Controller

Under Config – Ethernet Settings

Webserver Mode

HTTP

HTTPS (Default)

Disabled

Disabled shuts off Ethernet communications completely.

Choosing HTTP makes the controller work as it always has, with unencrypted web traffic.

HTTPS enables encryption and a new menu choice will appear:

SSL Certificate

Default Cert (Default)

Upload PEM

The Default Cert is the self-signed Walchem certificate. If this choice is selected the user sees a new menu:

DNS Name

The network IT administrator can map the controller numeric IP to a domain name, which reduces the warning messages.

The user selects Upload PEM if their network IT administrator has provided their own trusted certificate. These new menus appear:

Import SSL Private Key File

Import SSL Server Certification File

Import SSL Root Certification File

For these menus, the user will be prompted to insert a USB stick with the file and touch Confirm to import it. When loading files from a USB stick, the files must be named private.key, server.crt, and/or root.crt and must be in the root folder on the stick.

When loading the files through the web interface, the user chooses a file stored on the PC, and any file name can be used for the files.

If the customer is installing their own certificates, they must install a server private key and a server certificate.

If they are installing a file linked to a trusted certificate authority, then they also import the Root Certificate that documents the path or chain of trust that links the server certificate to an authority.

Once the files are imported, the user touches “Apply SSL Certificate Files” to force a restart of the webserver and start using the imported files.

There is also a Delete SSL Certificate Files menu that appears after the files have been imported, allowing the user to remove the existing files and import new ones, if desired.

Ethernet Details

The Ethernet Details will show the Webserver Status:

HTTP

HTTPS/Default Cert

HTTPS/User Cert

Disabled

If the certificate failed to upload properly these status messages will not match the settings. For example, if the file upload failed or was not attempted, the controller will revert to using the default Walchem certificate.

The System Log will have one or more entries that describes the problem (if any):

System Log Messages

Valid user-supplied SSL certificate file(s) found; HTTPS encryption enabled

Default self-signed SSL certification used; HTTPS encryption enabled

No SSL Server certificate file found; HTTPS encryption disabled

Invalid SSL certificate file, HTTPS encryption disabled

Unable to load default self-signed SSL certificate file, HTTPS encryption disabled

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 has a slightly different path to follow to accomplish this. Instructions for each are on the website.