Secure MQTT Communication using SSL or TLS

MQTT Modules can be enabled to use SSL/TLS to encrypt the communication between MQTT clients which is useful if used on a public network.

> ⚠ MQTT communications are not encrypted by default and enabling SSL/TLS is highly recommended on a public network.

Ignition supports certificates from both your organization's internal CA, as well as commercial CA's (Verisign, GoDaddy, Comodo, etc). Self-signed certificates can be generated by Ignition and they are useful for testing environment and non-public networks.

> ⛔ Self-signed certificates should not be used in a production environment on a public network.

As of module release version 4.0.4, the Cirrus Link modules are capable of reusing the existing Ignition web server provided SSL certificates to secure your MQTT communication. This is the recommended process to secure your MQTT communication using SSL/TLS.

Follow the links below to configure Ignition SSL and the MQTT modules:

- I am using MQTT modules version 4.0.4 or higher and
  - I need to obtain a security certificate from a Certificate Authority (CA)
  - I have a security certificate from a Certificate Authority (CA)
  - I have a Self-signed Certificate created outside of Ignition
  - I need to create and use an Ignition generated Self-Signed Certificate
- I am using MQTT modules version pre 4.0.4

> ⛔ If updating Ignition SSL certificates whilst SSL in enabled at MQTT Distributor, you will need a module restart or configuration change save of the MQTT Distributor module

Additional Resources

- Inductive Automation's Ignition download with free trial
  - Current Ignition Release
- Cirrus Link Solutions Modules for Ignition
  - Ignition Strategic Partner Modules
- Support questions
  - Check out the Cirrus Link Forum: https://forum.cirrus-link.com/
  - Contact support: support@cirrus-link.com
- Sales questions
  - Email: sales@cirrus-link.com
  - Phone: +1 (844) 924-7787
- About Cirrus Link
  - https://www.cirrus-link.com/about-us/