Configuring the MQTT Modules to use a non Ignition generated Self-Signed Certificate

Self-signed certificates can be used with Ignition and the Cirrus Link modules and they are useful for testing environments and non-public networks.

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

Ignition has made it simple to load a self-signed certificate through the Setup SSL / TLS wizard but there are additional steps needed to create and use a CA Certificate chain with the MQTT modules.

The CA Certificate chain will comprise of all Intermediate CA certificates, in order, and the Root CA concatenated into a single cert file.

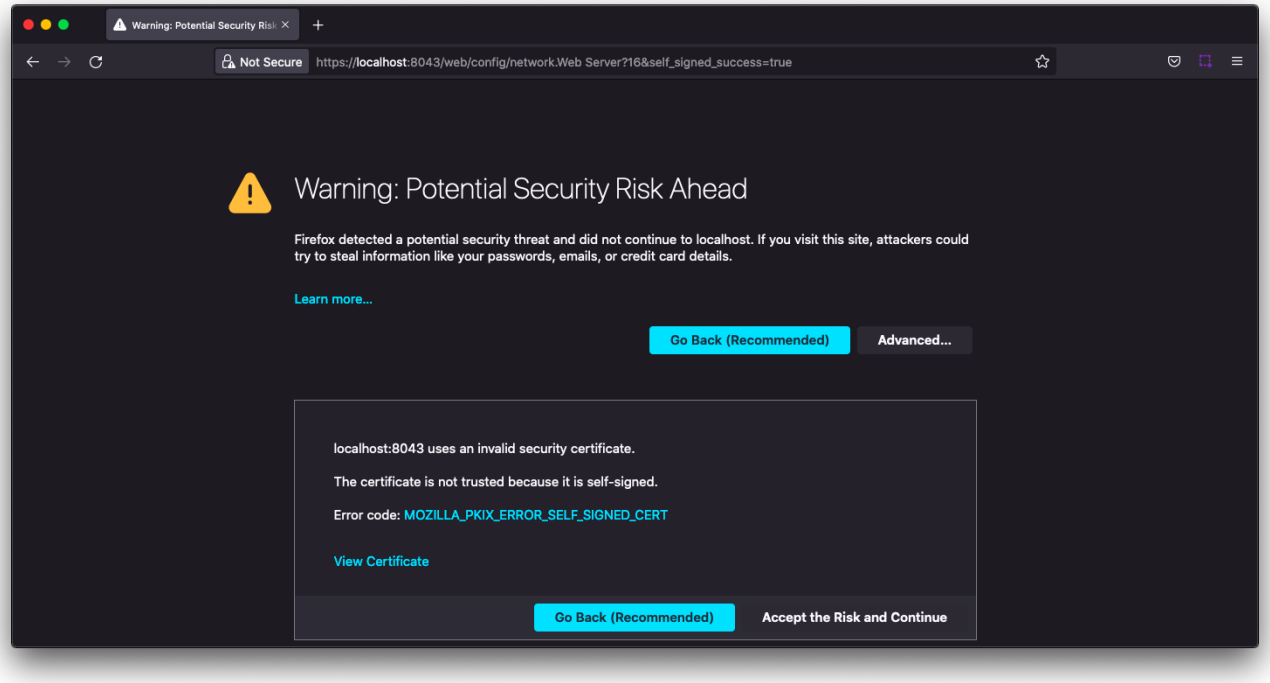
SSL/TLS Enable the Ignition Web Server

Review the following list for the required certificates:

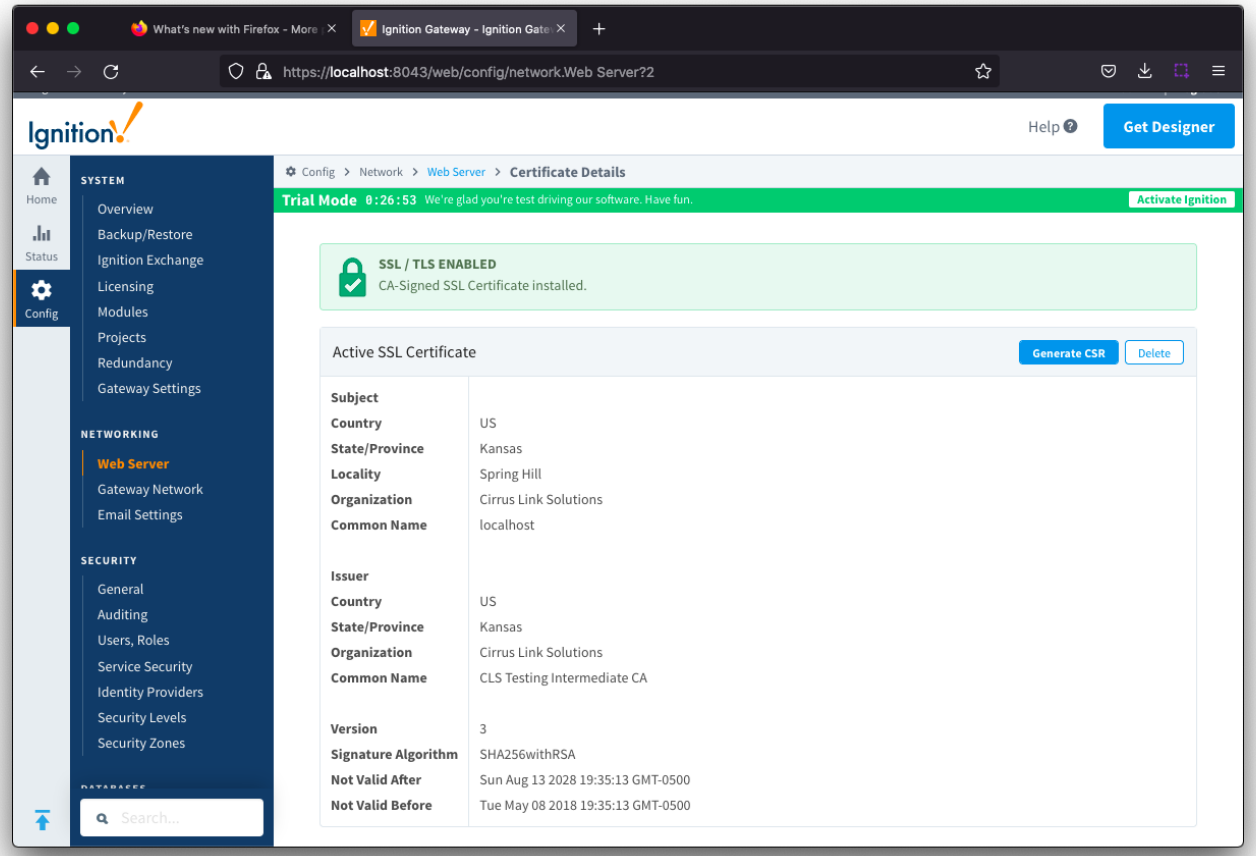
- Private Key
- Certificate
- Any Intermediate CA Certificates
- Root CA Certificate

Follow the steps outlined in the Ignition Secure Communication (SSL / TLS) document using the Certification wizard to import the certificates needed to SSL enable the Ignition Web Server.

You will be warned of a Potential Security Risk and will need to Accept the Risk and Continue



Once configured, you will be able to view the SLL/TLS Certificate details which should be displayed similar to the image below:



MQTT Modules

Create the CA Chain Certificate

Construct the CA Certificate chain by concatenating the Intermediate CA file(s) with the Root CA file into a new file.

> ⚠ The Intermediate CA file should be first in this new file. If you have multiple Intermediate CA Certificates then add them in order before adding the Root CA cert.

In this example, we have a single Intermediate CA which is the concatenated with a Root CA

cachain

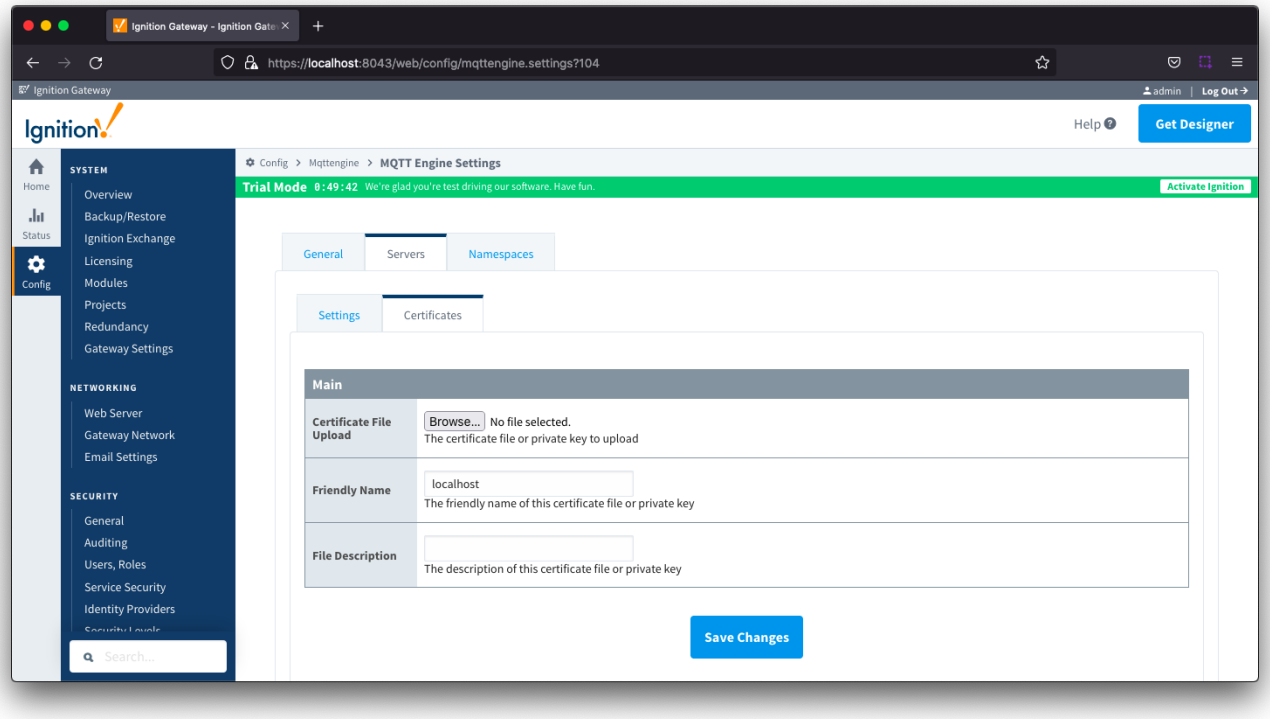
```
-----BEGIN CERTIFICATE-----
MIIF3TCCA8WgAwIBAgICEAAwDQYJKoZIhvcNAQELBQAwgYQxCzAJBgNVBAYTAlVT
......
HPdMojd3CnsdLcqfzt582nxlGbfYwpR3Y5XeMSHST2Wq1FLVLA3HE5iLtQAL0bwv
NfKkNSLtui2QpCV0dwY8XX8=
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
MIIF8DCCA9igAwIBAgIJAK7yLN2Y9PrMMA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
.....
CRTeBexRtq4VSm/Oi5fIT+euBLZTTsDdF+sxzJi9TP60Y0tD
-----END CERTIFICATE-----
```

If you do not have access to or cannot easily locate your Intermediate and/or Root CA Certificates, follow the steps in How do I find the Self-Signed Certificates loaded for Ignition.

Upload CA Certificate chain

The MQTT Engine and MQTT Transmission modules will both require the CA Certificate chain to be upload and applied. Navigate to the Servers > Certificates section for each module and select Create New Certificate.

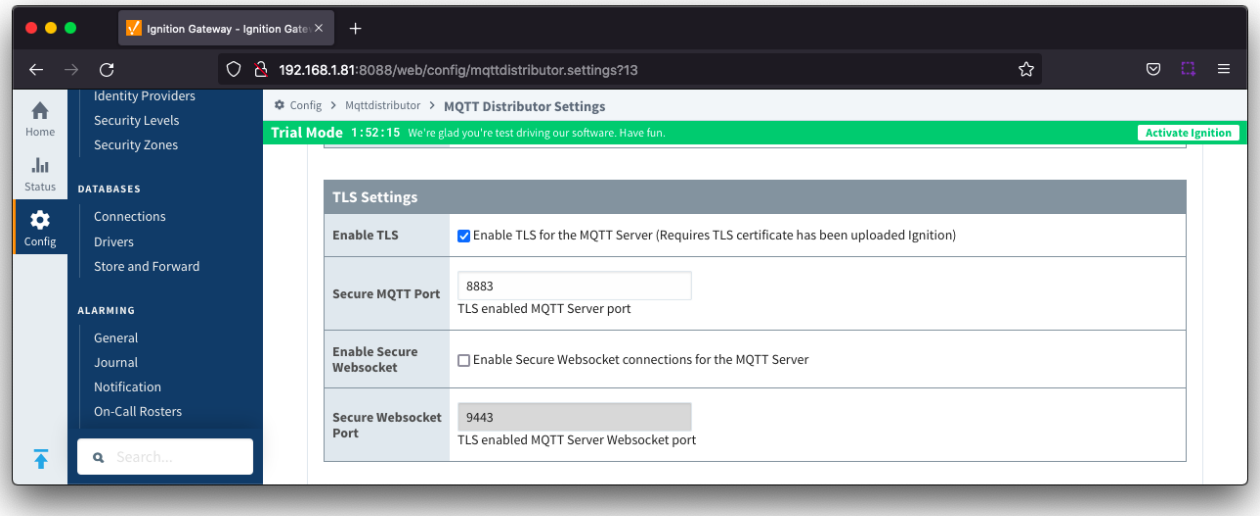
Browse to your CA Certificate chain file to upload, configure a friendly name and Save Changes.



Configure MQTT Distributor to use SSL/TLS

Enable SSL/TLS for MQTT Distributor by selecting the "Enable TLS" configuration setting under TLS Setting section for MQTT Distributor.

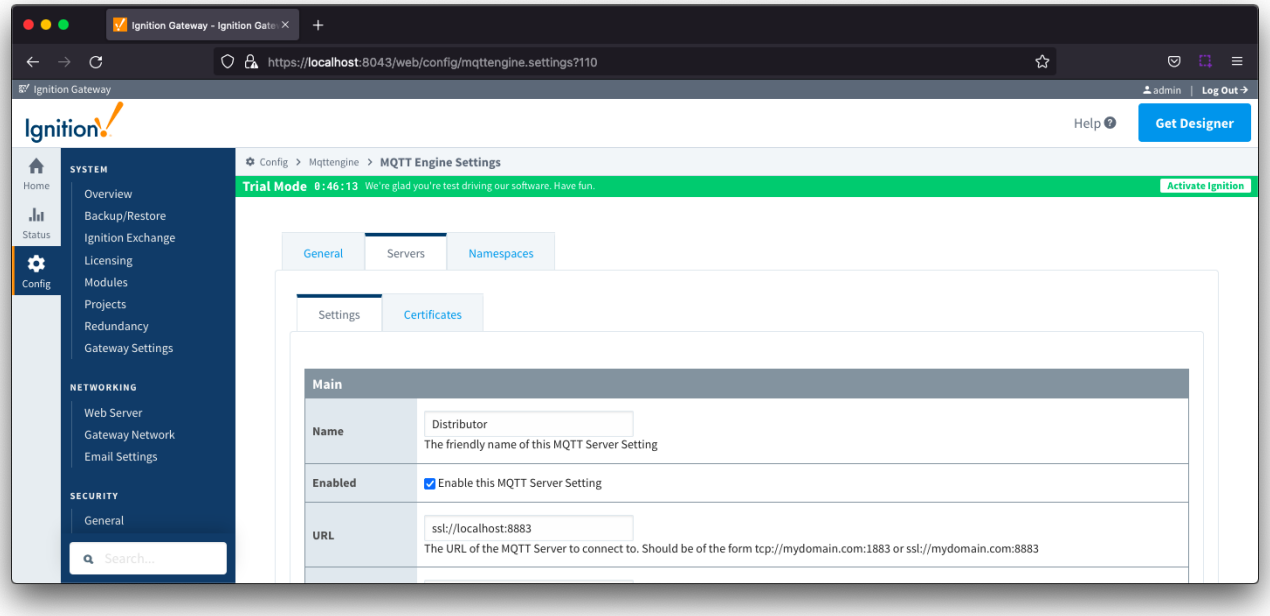
Click Save to confirm the configuration update.



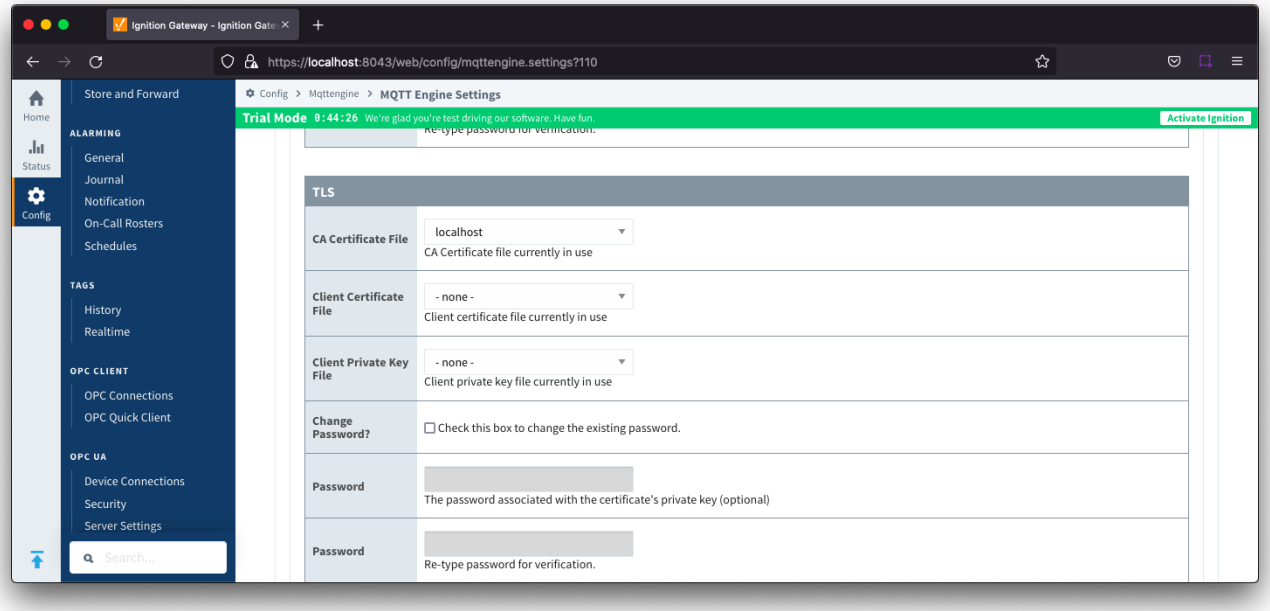
Configure MQTT Engine and MQTT Transmission to use SSL/TLS

For MQTT Engine and MQTT Transmission to connect to Distributor over SSL/TLS you will need to update each Server configuration.

For each module, navigate to the Servers Settings Main section and update the URL for your environment.



Navigate to the TLS section and select your CA Certificate chain file as the **CA Certificate File.** Click Save to confirm the configuration update.



MQTT Engine and Transmission should now show connected to Distributor over SSL/TLS.