Creating and Using an Ignition generated Self-Signed Certificate

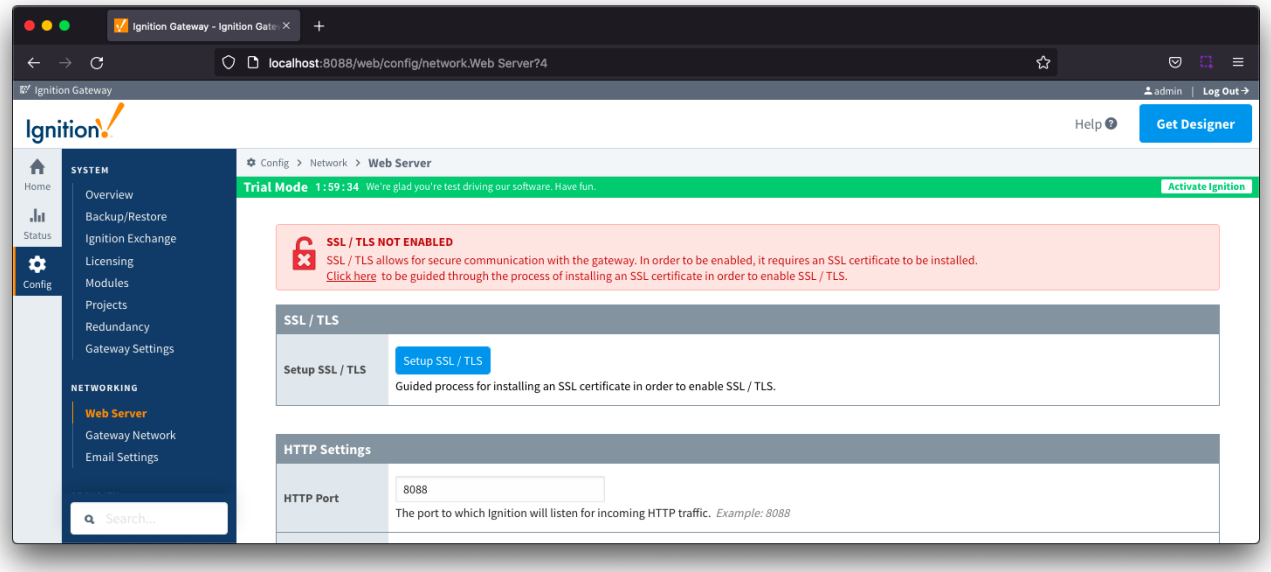
Self-signed certificates can be used with Ignition and the Cirrus Link modules and they are useful for testing environments and non-public networks.

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

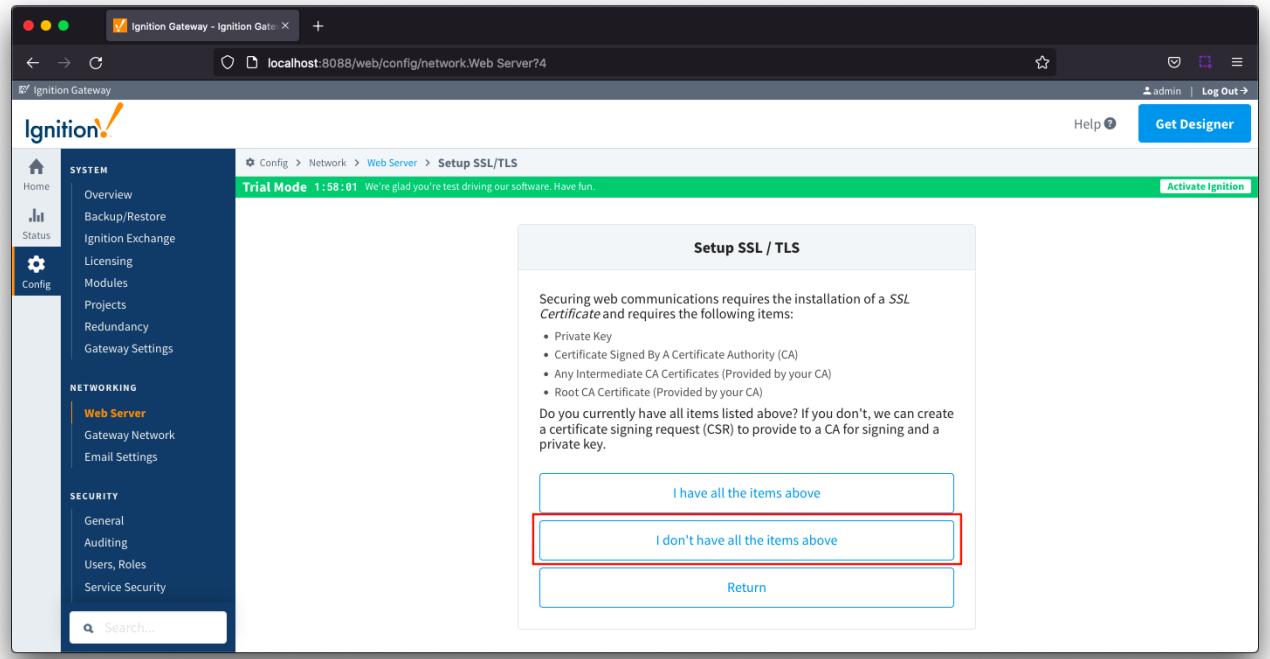
Ignition has made it simple to create a self-signed certificate through the Setup SSL / TLS wizard but there are additional steps needed to be able to use that certificate with the MQTT modules.

Ignition

Navigate to Config > NETWORKING > Web Server from the Ignition left hand menu bar and select Setup SSL / TLS

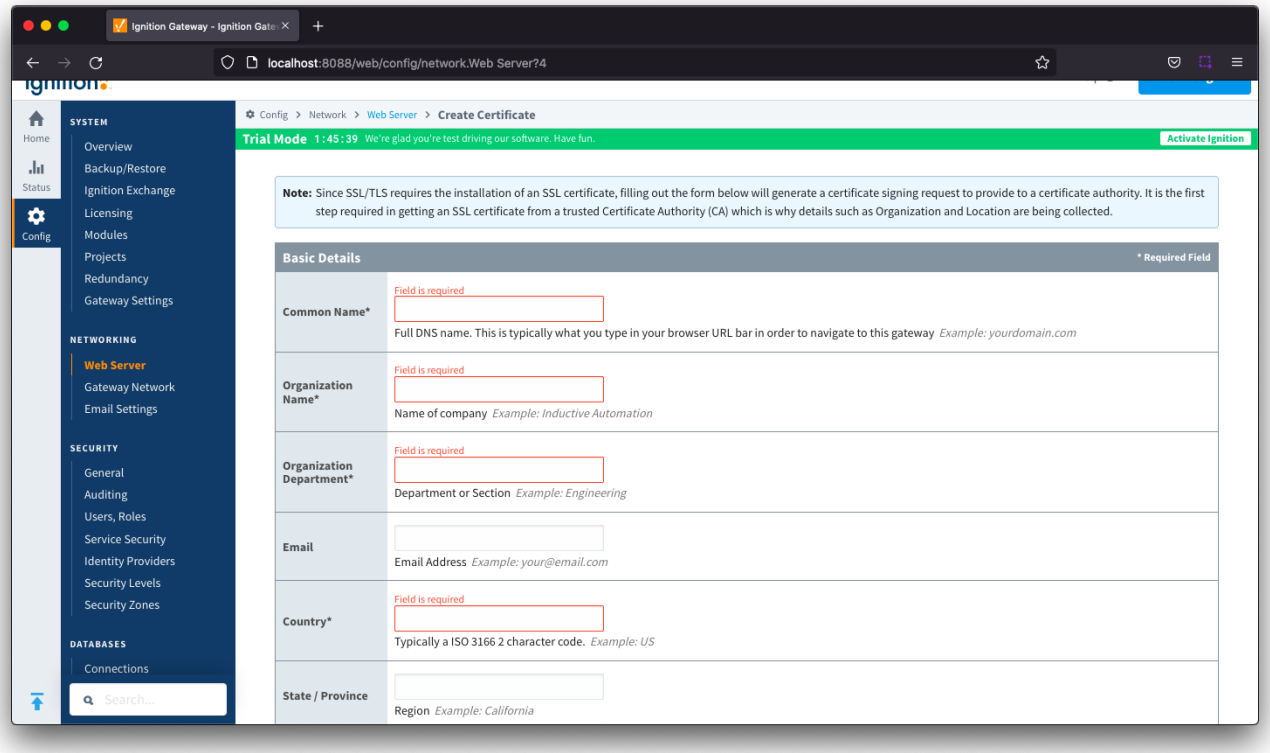


Select the option "I don't have all the items above"

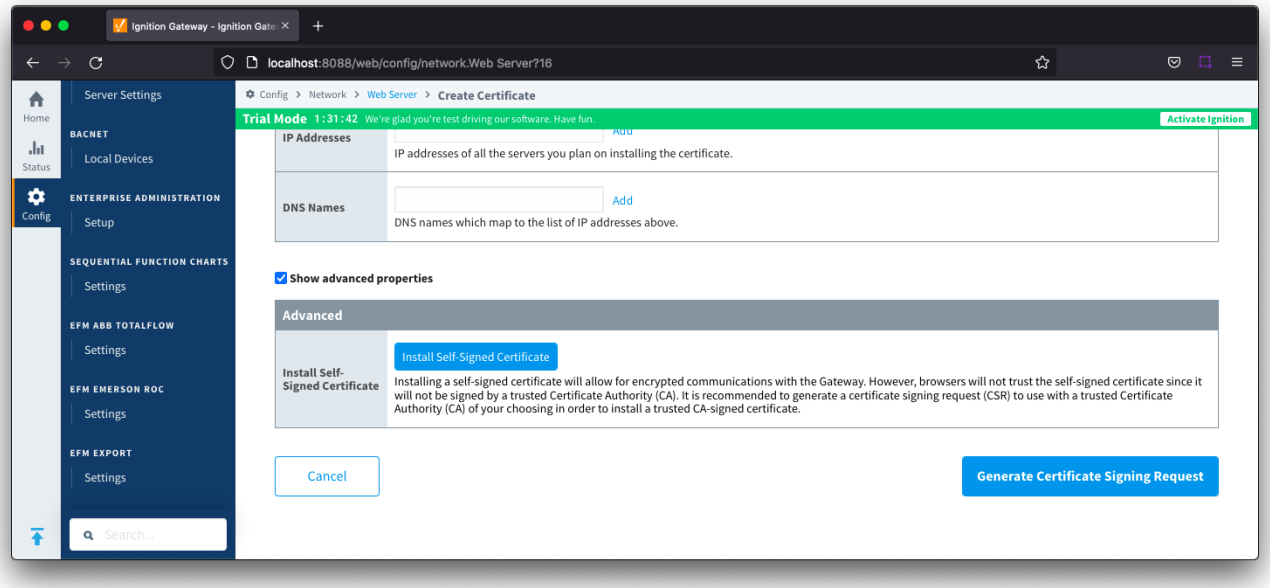


Complete the required fields highlighted in red.

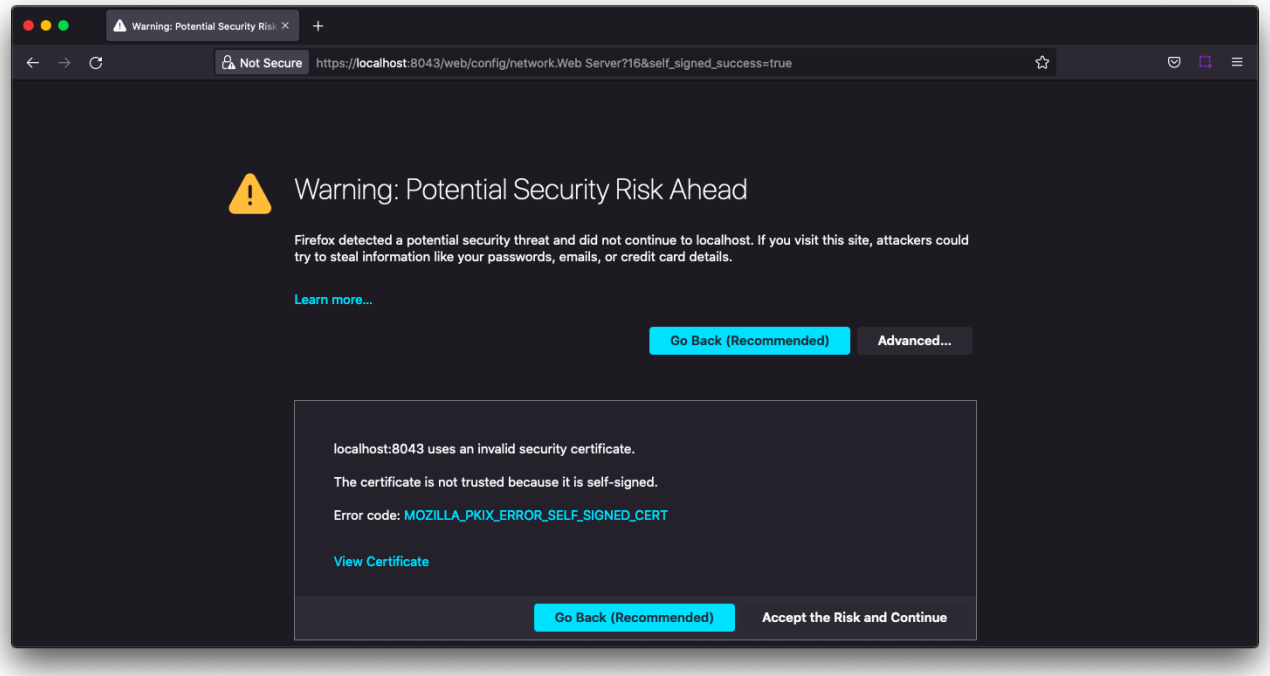
> Set the Common Name to the 'mydomain' used in the URL for your MQTT Server connection which is in the format ssl://mydomain.com:8883. The MQTT modules use the certificate Common Name to validate the chain of trust for the certificate. For example if you are connecting to ssl://localhost:8883, the Common Name should be set to 'localhost'.



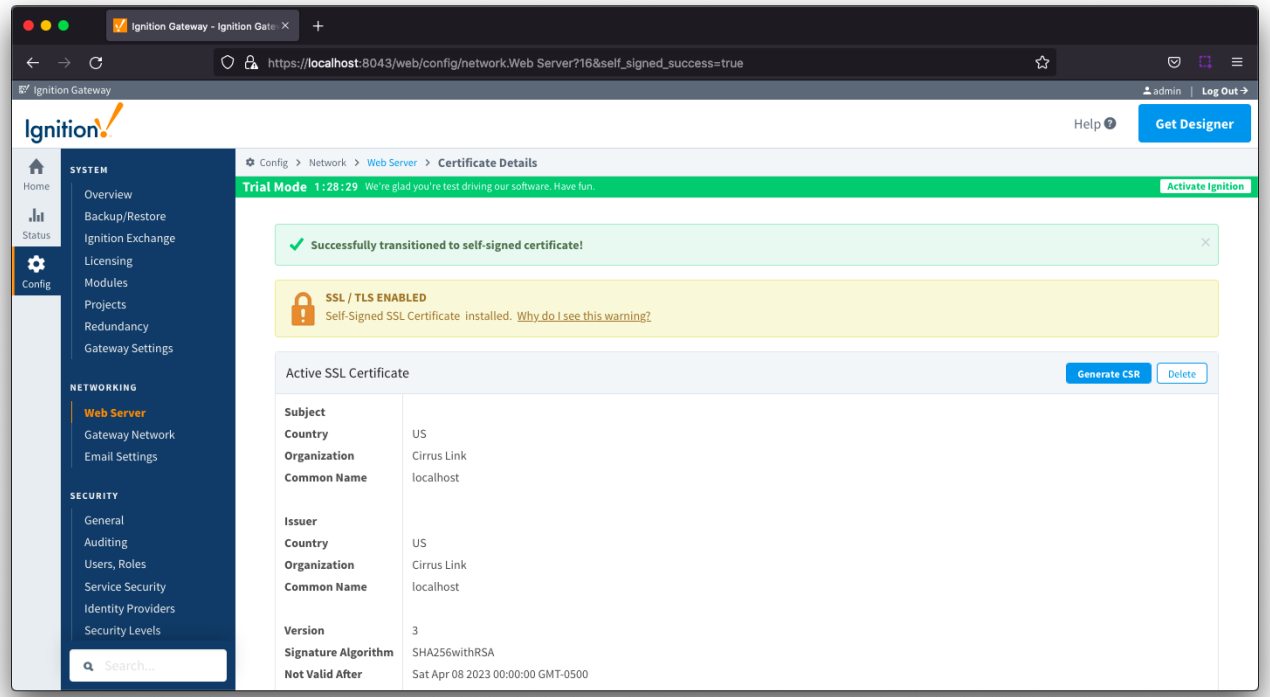
Select the Show advanced properties checkbox and then the Install Self-Signed Certificate button



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



Ignition will now show that you have successfully transitioned to self-signed certificate and that SSL /TLS is enabled.



Extract CA Certificate from ssl.pfx file

To allow the MQTT modules to validate the chain of trust for the self-signed certificate, you will need to upload the CA Certificate to each module.

First you will need to extract the CA Certificate chain from ssl.pfx file created in the webserver directory of your installed Ignition system

Run the following command from the webserver directory to generate a .pem file. Note : this command will create a file named "cert.pem"

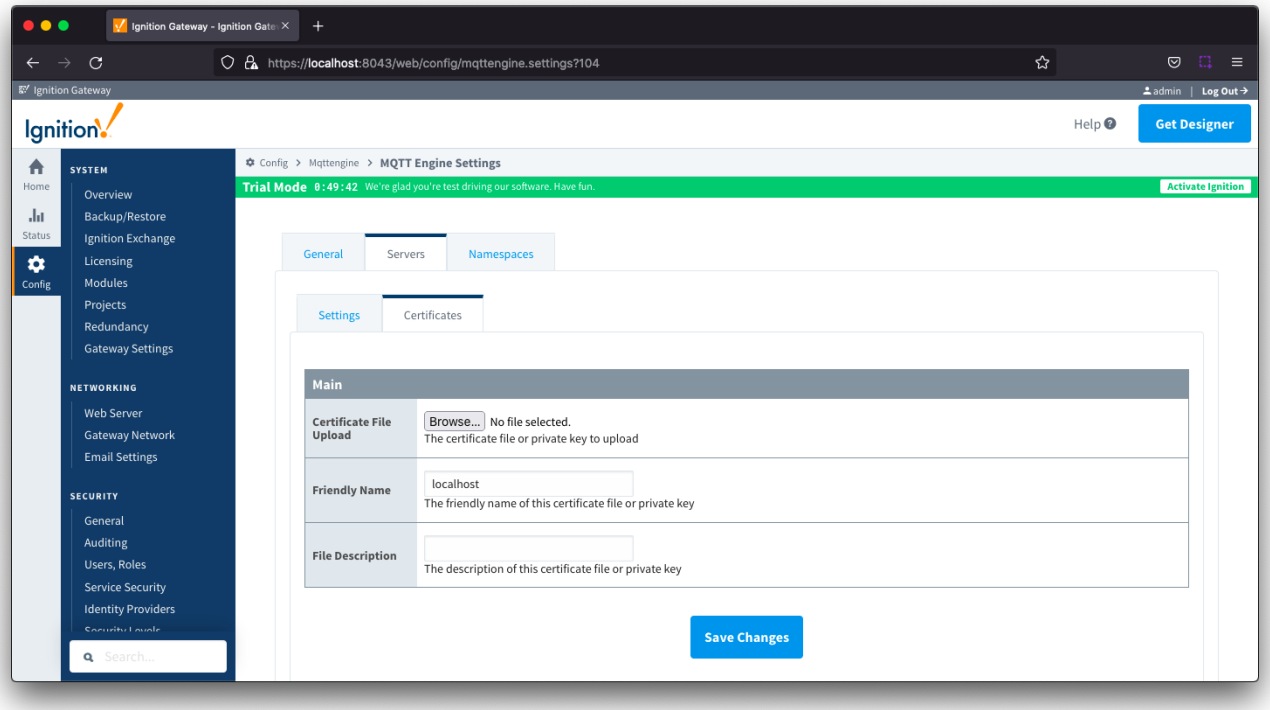
```
openssl pkcs12 -in ssl.pfx -nokeys -clcerts -nodes -passin pass:ignition | openssl x509 -out cert.pem
```

MQTT Modules

Upload Certificate

Now you will need to upload this .pem certificate for each of the MQTT Engine and MQTT Transmission modules. Navigate to the Servers > Certificates section for each module and select Create New Certificate.

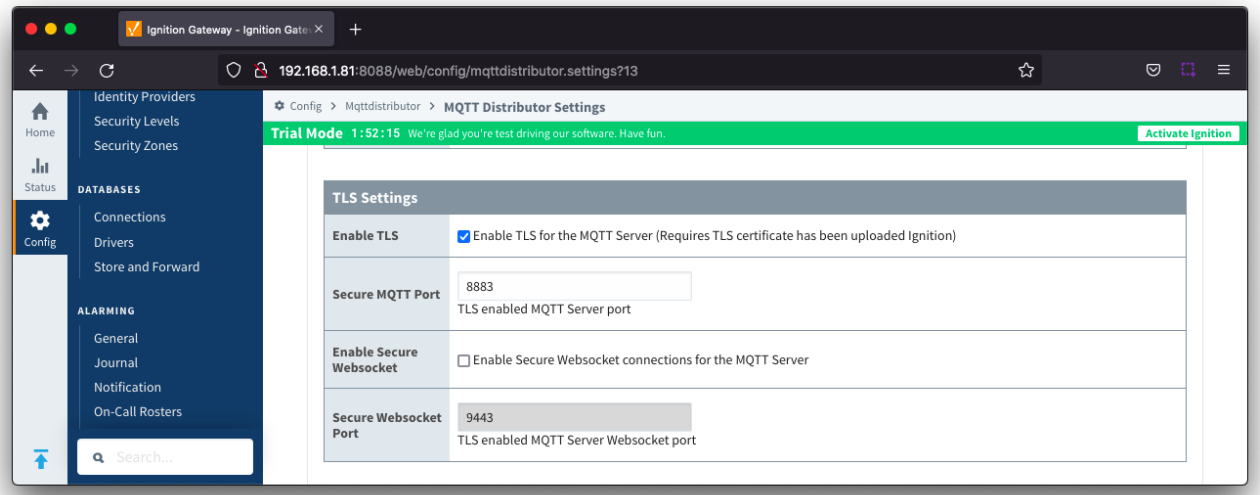
Browse to your cert.pem file to upload, configure a friendly name and Save Changes.



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.

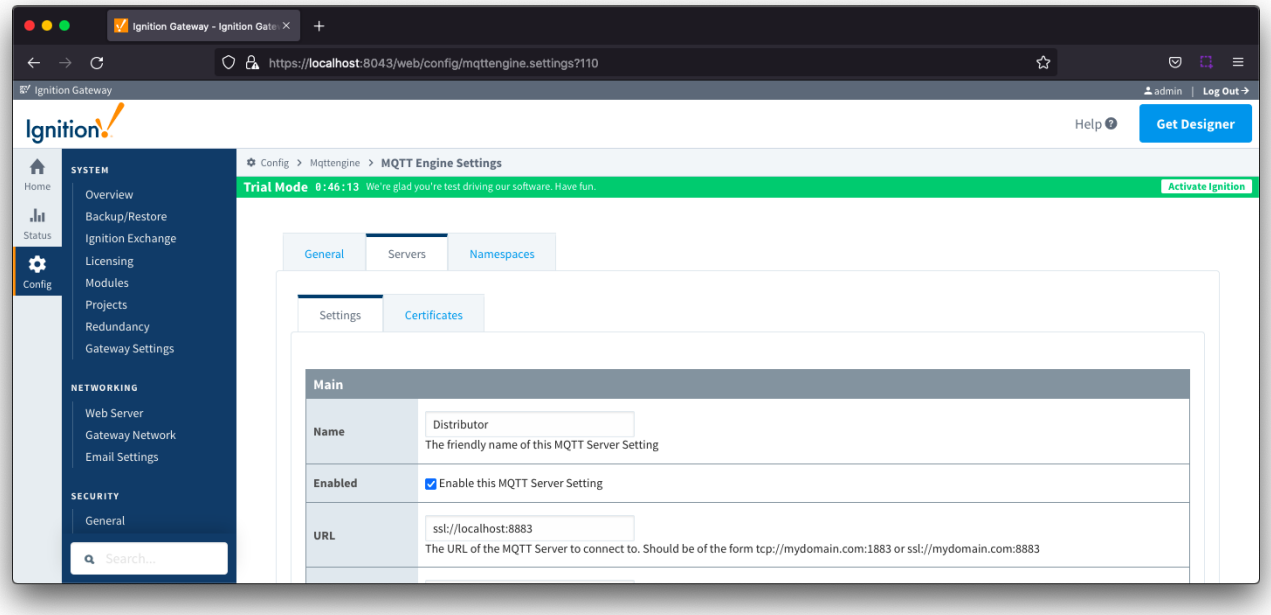


Configure MQTT Engine and MQTT Transmission to use SSL/TLS

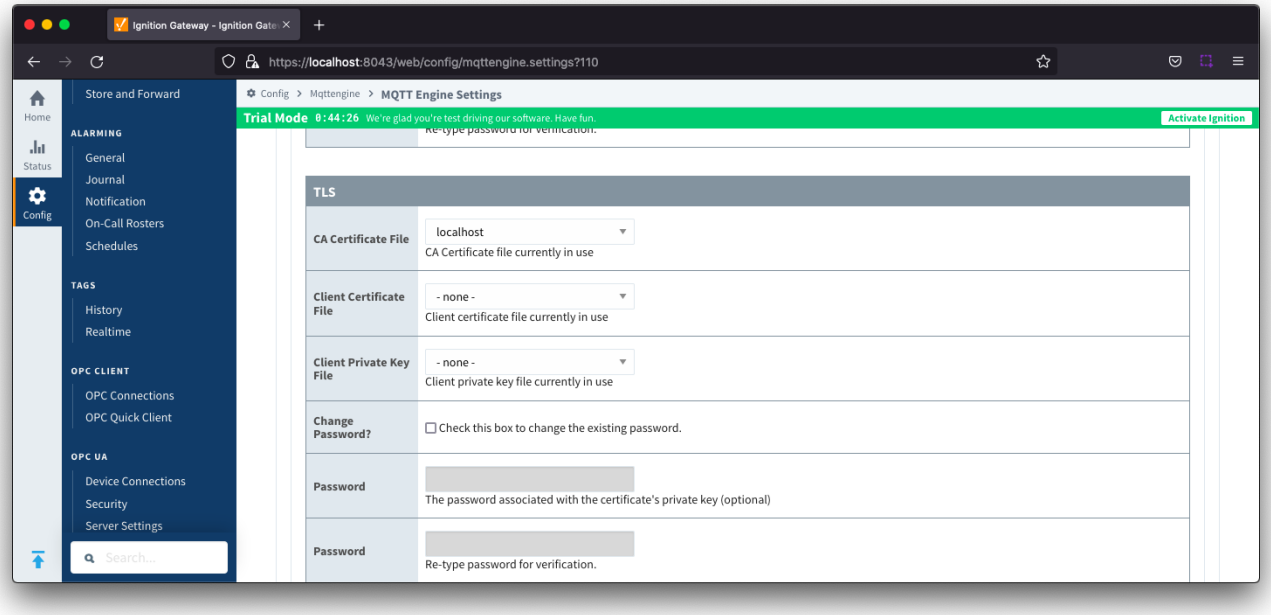
For MQTT Engine and MQTT Transmission to connect to Distributor over SSL/TLS you will need to update each Server configuration.

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

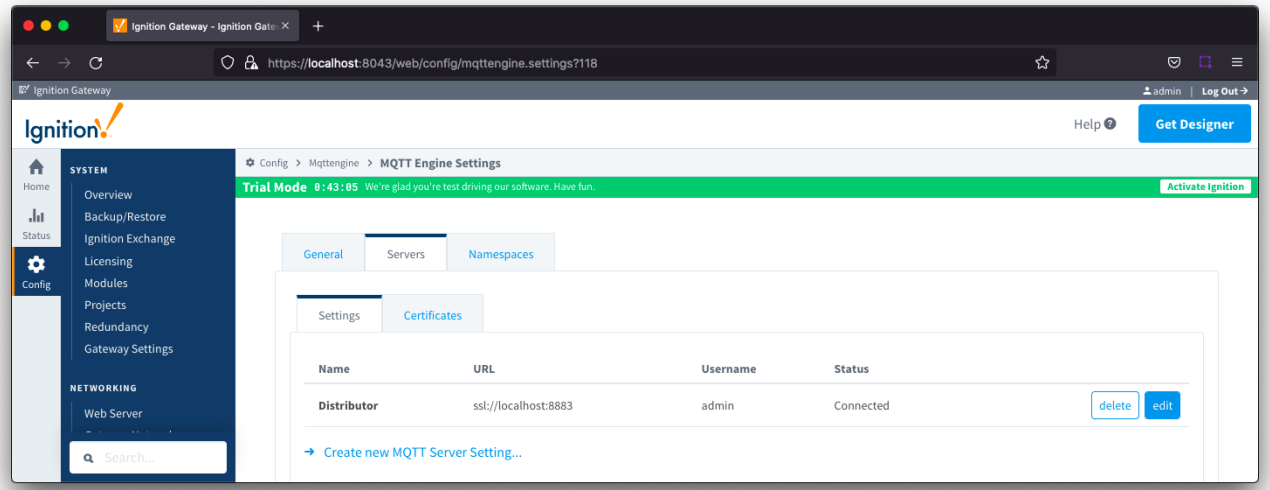
> ⚠ The mydomain for the URL should match the Common Name for your self-signed certificate



Navigate to the TLS section and select your certificate 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.


Ignition Gateway - Ignition Gate
https://localhost:8043/web/config/mqttengine.settings?118
Ignition Gateway
admin | Log Out
Ignition
Help
Get Designer
Home
Status
Config
SYSTEM
Overview
Backup/Restore
Ignition Exchange
Licensing
Modules
Projects
Redundancy
Gateway Settings
NETWORKING
Web Server
Search...
Config > Mqttengine > MQTT Engine Settings
Trial Mode 0:43:05 We're glad you're test driving our software. Have fun.
Activate Ignition
General
Servers
Namespaces
Settings
Certificates
Name
URL
Username
Status
Distributor
ssl://localhost:8883
admin
Connected
delete
edit
Create new MQTT Server Setting...