

# Configuring the MQTT Modules to re-use Ignition SSL Certificates

## SSL/TLS Enable the Ignition Web Server

Ignition supports certificates from both your organization's internal CA, as well as commercial CAs (Verisign, GoDaddy, Comodo, etc.).

Review the following list for the required certificates:

- Private Key
- Certificate Signed By A Certificate Authority (CA)
- Any Intermediate CA Certificates (Provided by your CA)
- Root CA Certificate (Provided by your CA)

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.

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

The screenshot shows the Ignition Web Server interface. On the left is a dark blue sidebar with a menu. The main content area is white and displays the 'Certificate Details' for the 'Web Server' module. At the top of the main area, a green banner indicates 'SSL / TLS ENABLED' and 'CA-Signed SSL Certificate installed.' Below this, a table shows the details of the active SSL certificate. The table has two columns: 'Subject' and 'Common Name'. The 'Subject' row shows 'Common Name' as '\*.chariot.io'. The 'Common Name' row shows 'Common Name' as '\*.chariot.io'. The 'Issuer' row shows 'Issuer' as 'DigiCert Inc'. The 'Country' row shows 'Country' as 'US'. The 'Organization' row shows 'Organization' as 'GeoTrust TLS DV RSA Mixed SHA256 2020 CA-1'. The 'Common Name' row shows 'Common Name' as 'GeoTrust TLS DV RSA Mixed SHA256 2020 CA-1'. The 'Version' row shows 'Version' as '3'. The 'Signature Algorithm' row shows 'Signature Algorithm' as 'SHA256withRSA'. The 'Not Valid After' row shows 'Not Valid After' as 'Mon Sep 26 2022 16:59:59 GMT-0700'. The 'Not Valid Before' row shows 'Not Valid Before' as 'Thu Sep 02 2021 17:00:00 GMT-0700'. At the bottom of the table, there are two links: 'Upload Trusted CA-signed SSL Certificate...' and 'Return to Web Server...'. The sidebar menu includes sections for 'SYSTEM', 'NETWORKING', and 'SECURITY'. The 'SYSTEM' section includes 'Overview', 'Backup/Restore', 'Ignition Exchange', 'Licensing', 'Modules', 'Projects', 'Redundancy', and 'Gateway Settings'. The 'NETWORKING' section includes 'Web Server', 'Gateway Network', and 'Email Settings'. The 'SECURITY' section includes 'General', 'Auditing', 'Users, Roles', 'Service Security', 'Identity Providers', 'Security Levels', and 'Security Zones'.

Ignition

Config > Network > Web Server > Certificate Details

SSL / TLS ENABLED  
CA-Signed SSL Certificate installed.

Active SSL Certificate

Subject	
Common Name	*.chariot.io
Issuer	
Country	US
Organization	DigiCert Inc
Common Name	GeoTrust TLS DV RSA Mixed SHA256 2020 CA-1
Version	3
Signature Algorithm	SHA256withRSA
Not Valid After	Mon Sep 26 2022 16:59:59 GMT-0700
Not Valid Before	Thu Sep 02 2021 17:00:00 GMT-0700

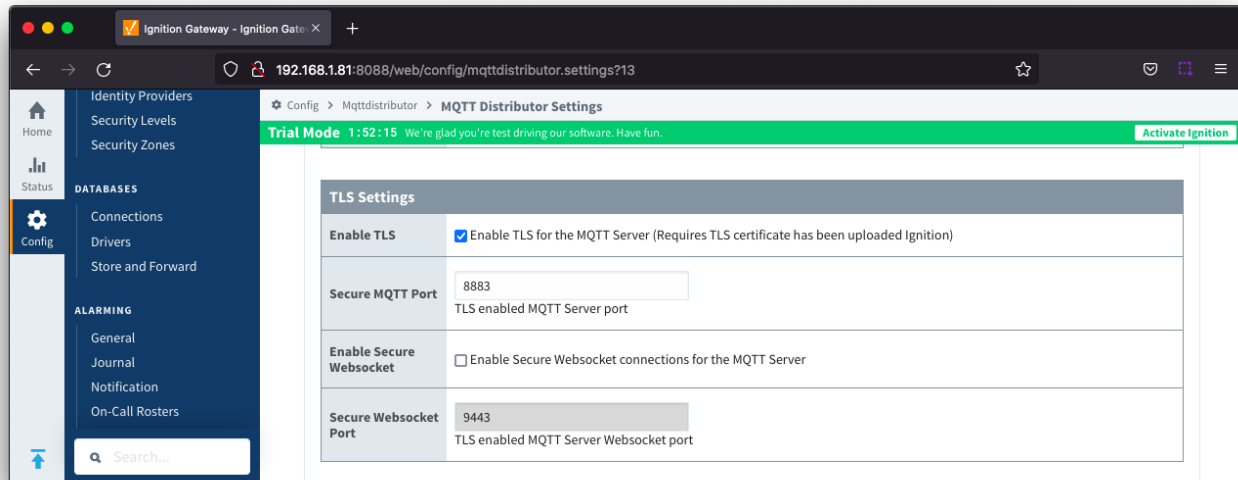
→ Upload Trusted CA-signed SSL Certificate...

→ Return to Web Server...

## Configure MQTT Distributor to use SSL/TLS

Once the Ignition Web Server has been SSL enabled, 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.

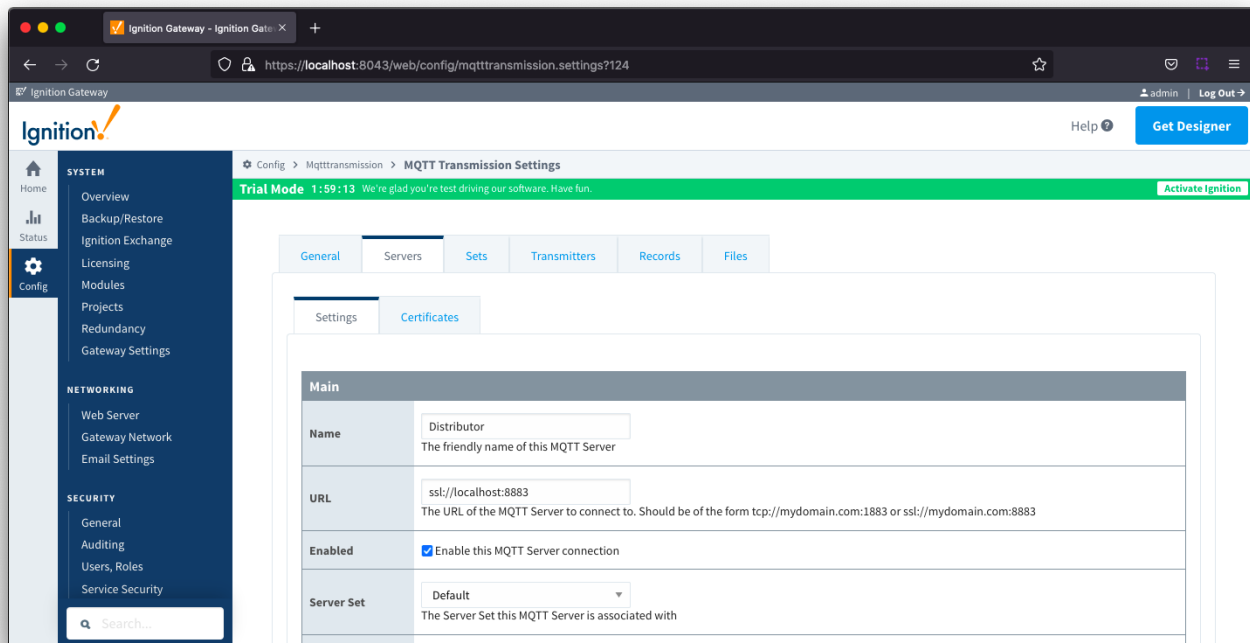


## Configure MQTT Engine and MQTT Transmission to use SSL/TLS

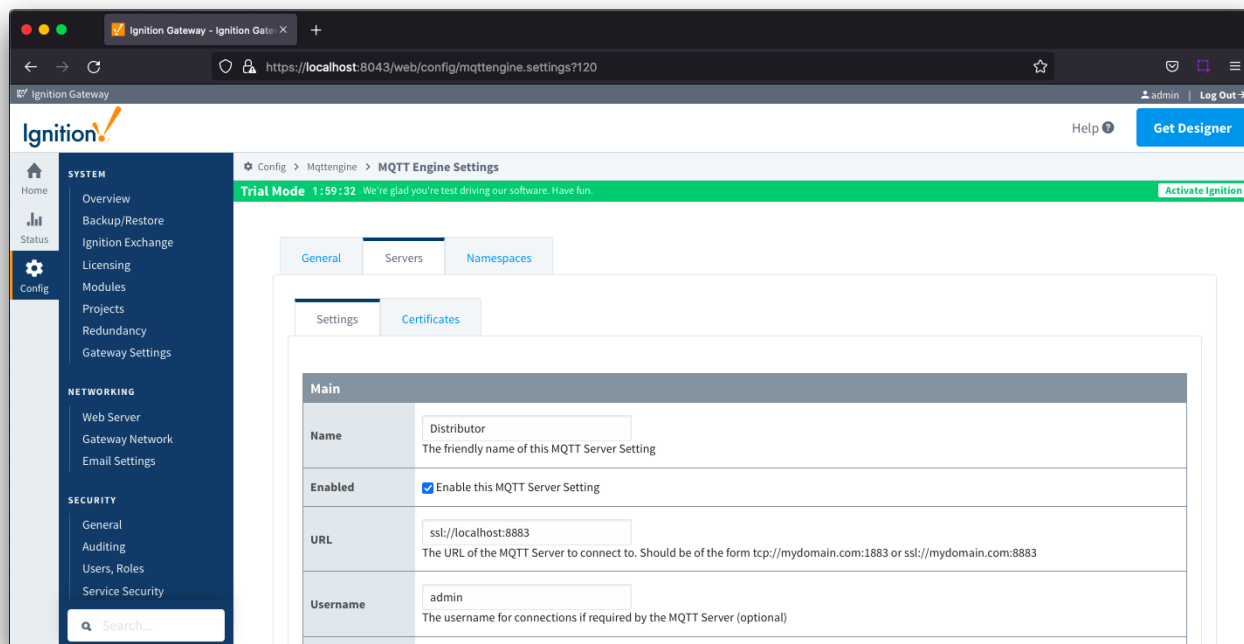
Once TLS has been enabled for MQTT Distributor, the only change required for MQTT Engine and MQTT Transmission to connect to Distributor over SSL/TLS is to update the MQTT Server URL.

Update each of the servers with the appropriate MQTT Server URL for your environment. For example, '[ssl://localhost:8883](https://localhost:8883)'

For MQTT Transmission, navigate to the [Servers Settings Main section](#) and update the URL as shown below:



For MQTT Engine, navigate to the [Servers Settings Main](#) section and update the URL as shown below:



At this point MQTT Engine and MQTT Transmission should show they're connected to MQTT Distributor over SSL/TLS.

