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

| 🔴 😑 🔹 🚣 Warning | : Potential Security Risk $	imes$ + | | | | | |
|-----------------|-------------------------------------|---|-----------------------------|-------------------|---|-------|
| ÷ → C | A Not Secure https://loc | alhost:8043/web/config/network.Web Server?16&self_signed_su | ccess=true | | ☆ | ⊠ □ ≡ |
| | | | | | | |
| | | | | | | |
| | ♪ Warnir | na [.] Potential Security Risk Ahea | h | | | |
| | | | | | | |
| | Firefox detec try to steal in | ted a potential security threat and did not continue to locall formation like your passwords, emails, or cre <u>dit card details</u> | ost. If you visit this site | , attackers could | | |
| | Learn more | | | | | |
| | | | | | | |
| | | Go Back (| Recommended) | Advanced | | |
| | | | | | | |
| | | | | | | |
| | localh | ost:8043 uses an invalid security certificate. | | | | |
| | The ce | ertificate is not trusted because it is self-signed. | | | | |
| | Error o | code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT | | | | |
| | View C | Certificate | | | | |
| | | | | | | |
| | | Go Back (Recommended) | Accept the Risk a | nd Continue | | |

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

| | → C O | https://localhost:8043/web/d | onfig/network.Web Server?2 | ☆ | ⊘ ⊻ □ |
|------|--------------------|------------------------------|--|--------|-----------------|
| gni | tion | | | Help | Get Designer |
| | SYSTEM | Config > Network > Web Set | ver > Certificate Details | | |
| ne | Overview | Trial Mode 0:26:53 We're gl | id you're test driving our software. Have fun. | | Activate Igniti |
| | Backup/Restore | | | | |
| tus | Ignition Exchange | | N ED | | |
| • | Licensing | CA-Signed SSL | Certificate installed. | | |
| nfig | Modules | | | | |
| | Projects | | | | |
| | Redundancy | Active SSL Certificat | e | Genera | te CSR Delete |
| | Gateway Settings | Subject | | | |
| | | Country | US | | |
| | NETWORKING | State/Province | Kansas | | |
| | Web Server | Locality | Spring Hill | | |
| | Gateway Network | Organization | Cirrus Link Solutions | | |
| | Email Settings | Common Name | localhost | | |
| | SECURITY | | | | |
| | Conord | Issuer | | | |
| | Auditing | Country | US | | |
| | Auditing | State/Province | Kansas | | |
| | Sonvice Security | Organization | Cirrus Link Solutions | | |
| | Identity Providers | Common Name | CLS Testing Intermediate CA | | |
| | Security Levels | | | | |
| | Security Zones | Version | 3 | | |
| | Contrast Contrast | Signature Algorithm | SHA256withRSA | | |
| | DATABACEC | Not Valid After | Sun Aug 13 2028 19:35:13 GMT-0500 | | |
| - 1 | Caranah | Not Valid Before | Tue May 08 2018 19:35:13 GMT-0500 | | |

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-----
HIF8DCCA9igAwIBAgIJAK7yLN2Y9PrMMA0GCSqGSIb3DQEBCwUAMIGEMQswCQYD
.....
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.

| $\leftrightarrow \circ \circ$ | https://localhost:8043/we | b/config/mqttengine.settings?104 | ☆ | ⊠ 🛄 ≣ |
|-------------------------------|------------------------------|---|--------|------------------|
| Ignition Gateway | | | | ≗admin Log Out |
| gnition | | | Help 🕜 | Get Designer |
| SYSTEM S | Config > Mqttengine > MQTT | Engine Settings | | |
| ome Overview | rial Mode 0:49:42 We're glad | you're test driving our software. Have fun. | | Activate Ignitio |
| Backup/Restore | | | | |
| atus Ignition Exchange | General Serv | ers Namespaces | | |
| nfie Modules | | | | |
| Projects | Sattings | atificator | | |
| Redundancy | Settings | ertificates | | |
| Gateway Settings | | | | |
| NETWORKING | Main | | | |
| Web Server | Certificate File | Browse No file selected. | | |
| Gateway Network | Upload | The certificate file or private key to upload | | |
| Email Settings | | lacalhart | | |
| SECURITY | Friendly Name | The friendly name of this certificate file or private key | | |
| General | | | | |
| Users, Roles | File Description | The description of this sortificate file or private law | | |
| Service Security | | The description of ans certaincace me of private key | | |
| Identity Providers | | | | |
| Cocurity Lovale | | 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.

| ← - | \rightarrow C | 08 | 192.168.1.81:8088/web/con | fig/mqttdistributor.settings?13 | \$ |
|-------------|------------------------|----|------------------------------|--|------------------|
| | Identity Providers | < | Config > Mqttdistributor > N | AQTT Distributor Settings | |
| Home | Security Levels | | rial Mode 1:52:15 We're gla | ad you're test driving our software. Have fun. | Activate Ignitio |
| .hi | Jecunty zones | | | | |
| Status | DATABASES | | TLS Settings | | |
| 🔹 Config | Connections Drivers | | Enable TLS | Enable TLS for the MQTT Server (Requires TLS certificate has been uploaded Ignition) | |
| | Store and Forward | | Secure MOTT Port | 8883 | |
| | ALARMING | | | TLS enabled MQTT Server port | |
| | General Journal | | Enable Secure Websocket | Enable Secure Websocket connections for the MQTT Server | |
| | On-Call Rosters | | Secure Websocket Port | 9443 | |
| - | o Search | | | ILS enabled MQTT Server Websocket port | |

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.

| $\leftrightarrow \rightarrow \mathbf{G}$ | 🔿 🔒 https://localhost:8043/ | web/config/mqttengine.settings?110 | ☆ | |
|--|-----------------------------|---|--------|-------------------|
| Ignition Gateway | | | | Log Out |
| gnition | | | Help 🕜 | Get Designer |
| SYSTEM | 🌣 Config > Mqttengine > MQ | ITT Engine Settings | | |
| ome Overview | Trial Mode 0:46:13 We're g | lad you're test driving our software. Have fun. | | Activate Ignition |
| Backup/Restore | | | | |
| atus Ignition Exchange | | | | |
| Licensing | General S | ervers Namespaces | | |
| onfig Modules | | | | |
| Projects | Settings | Certificates | | |
| Redundancy | | | | |
| Gateway Settings | | | | |
| NETWORKING | Main | | | |
| Web Server | | Distributor | | |
| Gateway Network | Name | The friendly name of this MQTT Server Setting | | |
| Email Settings | | | | |
| SECURITY | Enabled | ✓ Enable this MQTT Server Setting | | |
| General | URL | ssl://localhost:8883 | | |
| | | The URL of the MQTT Server to connect to. Should be of the form tcp://mydomain.com:1883 or ssl://mydomain.com:888 | 1 | |

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

| \rightarrow C | O A https://localhost:8043/web/config/mqtt | tengine.settings?110 | ☆ | ⊠ 🛄 ≡ |
|--------------------------------|--|---|---|------------------|
| E Store and Forward | Config > Mqttengine > MQTT Engine Settin Trial Mode 0:44:26 We're glad you're test driving Recype pass | ngs ig our software, Have fun sword for Vermication. | | Activate Ignitio |
| Journal Notification | TLS | | | |
| On-Call Rosters Schedules | CA Certificate File localhost CA Certificate | ▼ te file currently in use | | |
| TAGS History Realtime | Client Certificate File - none - Client certific | v icate file currently in use | | |
| OPC CLIENT OPC Connections | Client Private Key File Client private | v te key file currently in use | | |
| OPC Quick Client | Change Password? Check this | is box to change the existing password. | | |
| Device Connections Security | Password The passwor | rd associated with the certificate's private key (optional) | | |
| Server Settings | Password Re-type pass | sword for verification. | | |

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

| $- \rightarrow C$ | O https://localhost:8043/web/o | onfig/mqttengine.settings?118 | | | \$ | ⊚ □ |
|-------------------|-----------------------------------|--|----------|-----------|--------|-----------------------|
| Ignition Gateway | | | | | | Log Ou⊥admin Log Ou |
| gnition | | | | | Help 🔮 |) Get Designer |
| SYSTEM | Config > Mqttengine > MQTT Er | gine Settings | | | | |
| ne Overview | Trial Mode 0:43:05 We're glad you | 're test driving our software. Have fun. | | | | Activate Igniti |
| Backup/Restore | | | | | | |
| lgnition Exchange | Control | | | | | |
| Licensing | General Servers | Namespaces | | | | |
| nfig Modules | | | | | | |
| Projects | Settings Cert | ficates | | | | |
| Gateway Settings | | | | | | |
| | Name | URL | Username | Status | | |
| NETWORKING | Bistollusten | and (ille and the estimated | - desta | Connected | | |
| Web Server | Distributor | ssi://localnost:8883 | admin | Connected | de | edit |
| | Create new MOTT | Conver Cotting | | | | |
| Q Search | | server setting | | | | |