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.



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

$\leftarrow \rightarrow \mathbf{C}$	O D localhost:8088/web/config/network:Web Server?4	☆	
Ignition Gateway			💄 admin Log Out
Ignition		Help 🕜	Get Designer
SYSTEM	Config > Network > Web Server		
lome Overview	Trial Mode 1:59:34 We're glad you're test driving our software. Have fun.		Activate Ignitio
Backup/Restore			
tatus Ignition Exchang	SSL / TLS NOT ENABLED		
Licensing	SSL / TLS allows for secure communication with the gateway. In order to be enabled, it requires an SSL certificate to be installed.		
onfig Modules	Citex here to be guided through the process of installing an ODE certaincate in order to enable ODE / 123.		
Redundancy	SSL/TLS		
Gateway Setting	Setup SSL / TLS Setup SSL / TLS		
NETWORKING	Guided process for installing an SSL certificate in order to enable SSL / TLS.		
Web Server			
Gateway Networ	HTTD Sattings		
Email Settings			
	HTTP Port 8088		
O Search	The port to which Ignition will listen for incoming HTTP traffic. Example: 8088		

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

$\leftarrow \rightarrow \mathbf{C}$	O D localhost:8088/web/config/network.Web Server?4	☆	
Ignition Gateway			💄 admin Log Out
gnition		Help (Get Designer
SYSTEM	Config > Network > Web Server > Setup SSL/TLS		
lome Overview	Trial Mode 1:58:01 We're glad you're test driving our software. Have fun.		Activate Ignitio
Backup/Restore			
tatus Ignition Exchange	Setup SSL / TLS		
Licensing			
onfig Modules	Securing web communications requires the installation of a SSL		
Redundancy	Certificate and requires the following items:		
Gateway Settings	Private Key Cartel First Clarad Dud Cartel (Cathering (Cathering))		
	Certificate Signed By A Certificate Authority (CA) Any Intermediate CA Certificates (Provided by your CA)		
NETWORKING	Root CA Certificate (Provided by your CA)		
Web Server	Do you currently have all items listed above? If you don't, we can create		
Gateway Network	a certificate signing request (CSR) to provide to a CA for signing and a private key.		
Email Settings			
SECURITY	I have all the items above		
General			
Auditing	I don't have all the items above		
Users, Roles			
Service Security	Return		

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'.

→ C	O D localhost:8088/web/	config/network.Web Server?4 🗘 😇 🗌
SYSTEM	Config > Network > Wet	Server → Create Certificate
e Overview Backup/Restore	Trial Mode 1:45:39 We'	re glad you're test driving our software. Have fun. Activates
s Ignition Exchange Licensing	Note: Since SSL/TL: step required	S requires the installation of an SSL certificate, filling out the form below will generate a certificate signing request to provide to a certificate authority. It is the first in getting an SSL certificate from a trusted Certificate Authority (CA) which is why details such as Organization and Location are being collected.
Projects	Basic Details	* Required Field
Redundancy Gateway Settings	Common Name*	Field is required
NETWORKING		Full DNS name. This is typically what you type in your browser URL bar in order to navigate to this gateway Example: yourdomain.com
Web Server Gateway Network Email Settings	Organization Name*	Field is required Name of company Example: Inductive Automation
SECURITY General Auditing	Organization Department*	Field is required Department or Section Example: Engineering
Users, Roles Service Security Identity Providers	Email	Email Address Example: your@email.com
Security Zones	Country*	Field is required
Connections		lypically a ISO 3166 2 character code. Example: US
Q Search	State / Province	Parine Exemple College

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

	0	localhost:8088/web/	config/network.Web Server?16	☆	. □
Ser	ver Settings	🌣 Config 🗲 Network 🎽 Web	Server > Create Certificate		
me BACNE II LOC	т al Devices	Trial Mode 1:31:42 We'n IP Addresses	e glad you're test driving our software. Have fun Ruu IP addresses of all the servers you plan on installing the certificate.		Activate Ign
ENTER	PRISE ADMINISTRATION	DNS Names	Add DNS names which map to the list of IP addresses above.		
seque Set	NTIAL FUNCTION CHARTS	✓ Show advanced p	roperties		
EFM A	BB TOTALFLOW	Advanced			
EFM EF	MERSON ROC	Install Self- Signed Certificate	Installing a self-signed certificate will allow for encrypted communications with the Gateway. However, browsers v will not be signed by a trusted Certificate Authority (CA). It is recommended to generate a certificate signing reque Authority (CA) of your choosing in order to install a trusted CA-signed certificate.	will not trust the self-signed ce st (CSR) to use with a trusted C	rtificate since it Certificate
EFM EX	(PORT	Cancel		Generate Certificate Sig	ning Request

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

🛑 🔵 🌑 🚺 Warning: Potentia	Security Risk × +		
$\leftarrow \rightarrow \mathbf{C}$	A Not Secure https://localhost:8043/web/config/network.Web Server?16&self_signed_success=true	۲	⊚ ⊑
	A Marning: Datastial Casurity Dials Abaad		
	varning: Potential Security Risk Anead		
	Firefox detected a potential security threat and did not continue to localhost. If you visit this site, attacke try to steal information like your passwords, emails, or credit card details.	rs could	
	Learn more		
	Go Back (Recommended) Advance	ced	
	localhost:8043 uses an invalid security certificate.		
	The certificate is not trusted because it is self-signed.		
	Error code: MOZILLA_PKIX_ERROR_SELF_SIGNED_CERT		
	View Certificate		
	Go Back (Recommended) Accept the Risk and Conti	inue	

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.

\rightarrow C	C A https://localhost:80	13/web/config/mqttengine.settings?104	☆	
Ignition Gateway				Ladmin Log Out
gnition			Help 🕑	Get Designer
SYSTEM	🌣 Config > Mqttengine >	MQTT Engine Settings		
me Overview	Trial Mode 0:49:42 W	re glad you're test driving our software. Have fun.		Activate Ignitio
Backup/Restore				
tus Ignition Exchange	General	Servers Namespaces		
Licensing				
Projects				
Redundancy	Settings	Certificates		
Gateway Settings				
NETWORKING	Main			
Web Server	Certificate	Rrowse No file selected		
Gateway Network	Upload	The certificate file or private key to upload		
Email Settings				
SECURITY	Friendly Na	localhost The friendly name of this certificate file or private key		
General				
Auditing	File Descrip	ion		
Service Security		The description of this certificate file or private key		
Identity Providers				
Cocurity Lovole		Save Changes		
Q Search				

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	0 👌 1	92.168.1.81:8088/web/com	fig/mqttdistributor.settings?13	☆		. ≡
A Home	Identity Providers Security Levels	¢ Ti	Config > Mqttdistributor > N	IQTT Distributor Settings		Activate	Ignitio
.l.i Status	Security Zones		TLS Settings				
Config	Connections Drivers		Enable TLS	Enable TLS for the MQTT Server (Requires TLS certificate has been uploaded Ignition)			
	ALARMING		Secure MQTT Port	8883 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 TLS 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.

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

$\leftarrow \rightarrow C$	O A https://localhost:8043	/web/config/mattengine.settings?110	\$7	
Ignition Gateway		,	~	sidmin Lior Out
gnition			Help 🛙	Get Designer
Б SYSTEM	🌣 Config 🗲 Mqttengine 🗲 M	QTT Engine Settings		
Overview	Trial Mode 0:46:13 We're	glad you're test driving our software. Have fun.		Activate Ignitio
Licensing Modules Projects Redundancy Gateway Settings	General Settings	Servers Namespaces Certificates		
NETWORKING	Main			
Web Server Gateway Network Email Settings	Name	Distributor The friendly name of this MQTT Server Setting		
	Enabled	✓ Enable this MQTT Server Setting		
SECURITY		sel//localhost.0092		

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

	ignition outcine,	y - Igilition Gaterix			
← -	> C	O 🔒 https:	//localhost:8043/web	/config/mqttengine.settings?110	⊚ □ ≡
♠	Store and Forward	🌣 Config >	Mqttengine > MQTT B	Engine Settings	
lome		Trial Mod	e θ:44:26 We're glad y	ou're test driving our software. Have fun. Nersype password for vermeation.	Activate Ignitio
 tatus	General				
\$	Journal Notification		TLS		
nfig	On-Call Rosters Schedules		CA Certificate File	localhost	
	TAGS History Realtime		Client Certificate File	- none - • • Client certificate file currently in use	
	OPC CLIENT OPC Connections		Client Private Key File	- none - v Client private key file currently in use	
	OPC Quick Client		Change Password?	□ Check this box to change the existing password.	
	Device Connections Security		Password	The password associated with the certificate's private key (optional)	
Ŧ	Server Settings		Password	Re-type password for verification.	

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

\rightarrow C	O A https://localhost:8043/web/	config/mqttengine.settings?118			☆	. ⊂
gnition Gateway						ᆂ admin Log Ou
Inition					Help 🕻	Get Designer
SYSTEM	Config > Mqttengine > MQTT E	ngine Settings				
e Overview	Trial Mode 0:43:05 We're glad ye	u're test driving our software. Have fun.				Activate Igniti
Backup/Restore						
s Ignition Exchange	General Server	Namespaces				
Licensing	General	Naniespaces				
eg Modules Projects						
Redundancy	Settings Cer	tificates				
Gateway Settings						
NETWOOKING	Name	URL	Username	Status		
Web Conver	Distributor	ssl://localhost:8883	admin	Connected	de	elete
web server						
a Count	→ Create new MOT	Server Setting				