Secure Chariot MQTT Server communication using SSL/TLS

The Chariot® MQTT Server can be enabled to use SSL/TLS to allow secure communication with the Chariot Web UI (HTTPS) as well as secure communication between MQTT clients (MQTTS).



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

Setting Up SSL/TLS

The first step in setting up SSL/TLS is obtaining the necessary files to provide to the Chariot MQTT Server. There are three files that need to be uploaded to the Chariot MQTT Server in order to setup SSL/TLS communication.

- Private Key
 - A Private Key that was used to generate the Certificate Signing Request (CSR) and obtain the signed Server Certificate.
 - Must be an RSA Provate Key of type PKCS1 or PKCS8 in PEM format. Note: PCKS8 support was added in release 2.3.1
 - Review How to identify my Private Key type to verify type.
- · Server Certificate signed by a CA
 - The signed Certificate that the Chariot MQTT Server will use for SSL/TLS communication.
 - Must be a X.509 SSL Certificated in PEM format.
- Root CA Chain
 - A public root Certificate Authority (CA) certificate and any/all public intermediate CA certificates between the root and the CA that issued the certificate in PEM format. If there are no intermediate CAs, then the chain is made up of only the public root CA certificate.
 - ° Must be a list of X.509 certificates in PEM format.

See here for more information on obtaining a signed Certificate.

Once these files are obtained, log into the Chariot MQTT Server Web UI and navigate to the Configuration System page as shown below:

🔴 🔴 🌒 🧭 Mariot	× +			
\leftarrow \rightarrow C \textcircled{a}	0 🔏 35.153.79.228:8080/#/system		⊌ ☆	II\ 🖸 🍭 🗳 👬 ≡
Chariot admin		Trial License Active 01:51:33		
STATUS	System			
	Home > System			
光 Users	Configuration Certificates			
යා Roles				
MQTT Credentials	Enable HTTP			
MQTT Server	HTTP Port 💿	8080		٢
Č License	Enable HTTPS 💿			
System	HTTPS Port	8443		۲
				Update

An "SSL Not Setup" indicator at the top should show that SSL/TLS has not yet been set up. If this indicator says "SSL Setup", you may need to first delete any existing Certificates before setting up a new one, see here for instructions. Click on either the indicator or the Certificates tab to navigate to the following page:

🔴 🔴 🌒 🧭 Mariot	× +				
\leftarrow \rightarrow C \textcircled{a}	0 🔏 35.153.79.228:8080/#/system		🗵 ☆	III\ 🗉 🛎 🗳	11 ≡
Chariot admin		Trial License Active 01:36:37			
	System				
🛯 Dashboard					
CONFIGURATION	Home > System				
爰 Users	Configuration Certificates				
🗱 Roles	Upload the following files and then click "Setup SS	SL"			
MQTT Credentials					
MQTT Server	STATUS FILE TYPE	NAME	TIME		
ð License	🚫 Private Key 🍥			Ĺ	
System	CA Chain			⊥	
	🚫 Certificate 🎯			Ĺ	
				Setup SSL	
+					

Use the right side links to upload the three required files.

🗧 🔵 🔵 🚿 Chariot	× +					
← → C' ŵ	0 🔏 35.153.79.228	::8080/#/system		🗵 🕁	III\ 🗉 🛎 🗳	11 ≡
Chariot	Trial License Active 01:34:32					
STATUS	Syste	em Not Setup				
[] Bashboard	Home > System					
CONFIGURATION	Home > System					
器 Users	Configuration	Certificates				
ය Roles	Links of the first					
MQTT Credentials	Upload the fol	lowing files and then click	Setup SSL"			
	STATUS	FILE TYPE	NAME	TIME		
 Morr server License 	\odot	Private Key 💿	localhost.key.pem	September 24, 2020 10:47 AM		
System	\odot	CA Chain 🕜	ca-chain.cert.pem	September 24, 2020 10:47 AM	Ĩ	
	\odot	Certificate	localhost.cert.pem	September 24, 2020 10:47 AM		
					Setup SSL	
→						

Once the three files have been successfully uploaded, click the "Setup SSL" button on the bottom right.



You should now see the SSL Certificate details along with the name of the files that were uploaded. SSL has now been setup.

Anonymous Client Connections

Chariot MQTT Server still requires MQTT credentials to authenticate incoming client connections, even when using client certificates to set up a TLS/SSL session. If clients will not be sending an MQTT username and password, anonymous connections must be enabled.

To enable anonymous connections, navigate to the Configuration MQTT Server Configuration tab and set Allow Anonymous

	A 102 169 1 91:0 00 /#/methamia		~	
	V 192.100.1.01.0000/#/induserver		¥	ତ ଥ =
rius Chariot ao admin	Enable Secure			
ATUS	Secure Port	8883		Ŷ
u∺ Dashboard ₀0] Logging	Enable WebSocket 💿			
🖇 Sparkplug	WebSocket Port	8090		\$
√ матт	Enable Secure WebSocket 💿			
û Alerts	Secure WebSocket Port	8091		Ş
DNFIGURATION 怨 Users	Bind Address 💿	0.0.0.0		
🕆 Roles	Allow Anonymous 💿			
MQTT Credentials	Anonymous MQTT Credentials	None Selected		•
MQTT Server				
License king up fonts.googleapis.com				Update

By default, an anonymous client connection will be allowed to publish and subscribe on # unless the Anonymous MQTT Credentials has been selected.

This will allow you to select any of the configured MQTT Credentials, configured under Configuration MQTT Credentials, and MQTT Chariot will use the Publish and Subscribe ACLs for that MQTT Credential for all anonymous connections.

A Password will need to be configured for this MQTT Credential but will not be used by MQTT Chariot

Deleting an SSL/TLS Certificate

(ī)

In order to remove an SSL Certificate, navigate to the Configuration System Certificates tab where the SSL Certificate details are displayed. The "Delete SSL" button on the bottom right can be clicked to completely remove the SSL Certificates and keys that were previously uploaded to setup SSL. This will revert the Chariot MQTT Server to a pre-setup state as shown below:

🔴 🔴 🌒 🚿 Chariot	× +					
\leftarrow \rightarrow C \textcircled{a}	0 🌠 35.153.79.228:8080/#/system		⊘ ☆	\ ⊡ © 0 #	Ξ	
Chariot		Chariot Message ×	1 7			
	S vetom	SSL successfully deleted				
STATUS	G [∩] SSL Not Setup					
[]] Dashboard	Home > System					
CONFIGURATION	nome - System					
終 Users	Configuration Certificates					
🕸 Roles	Lipload the following files and then click "Setup SSI"					
MQTT Credentials	opious are following mes and arene					
MQTT Server	STATUS FILE TYPE	NAME	TIME			
م License	Private Key 💿			1		
	CA Chain			↑ .		
System						
	Certificate 💿			1.		
				Setup SSL		
+						

Notes

Getting a Certificate from a Certificate Authority

The first step to securing MQTT communication is to get a certificate from a CA. There are many available such as Verisign, Thawte and RapidSSL. There are also a number of other certificate authorities available. The general process is as follows:

- Generate a RSA key
 - This is the private key and used for encryption/decryption of data. Keep this private and don't share it with anyone including the CA. However, the Chariot MQTT Server will need it to encrypt/decrypt data.
- Create a Certificate Signing Request (CSR)
 - Generally the CA can provide instructions on how to generate a CSR. Windows, Linux, and OSX all have tools available for generating a CSR and there is lots of documentation online about all of them.
 - Make sure the Common Name specified in the CSR matches the server URL (i.e. example.com). Also, do not include www. because this will used for MQTT.
- Give the CSR to the CA
- The CA will then provide back a public certificate for use with MQTT Distributor
- In some cases depending on the CA an intermediate certificate may also be required. If so, the CA will also provide this.

Creating a Self-Signed Certificate

Creating your own CA, intermediate CA, and generating your own signed certificates can be done following the three steps below using some open source tooling. Note creating an Intermediate CA is not explicitly required, but is recommended if you will be using self-signed certs in a private network in production. If this is simply for development that step can be skipped and the root CA can be used to sign server certificates. Again, using self-signed certs in production over the Internet is not recommended.

- Create the Root Pair
 Create and Sign the Intermediate Pair
 Create and Sign the Server pair

 Make sure the Common Name specified in the CSR matches the server URL that will be used by the clients (i.e. 192.168.1.100). It could also be the network hostname.