SIGNALFIRE
WIRELESS TELEMETRY

RANGER CONNECTIVITY OPTIONS

1

RANGER
SignalFire Wireless Telemetry

MQTT
Sparkplug

SignalFire MQTT Broker

MQTT
Sparkplug

SignalFire Cloud

DB

2

RANGER

MQTT
Sparkplug

SignalFire MQTT Broker

MQTT
Sparkplug

SignalFire Cloud

DB

Customer Cloud

DB

3

RANGER

MQTT
Sparkplug

Customer MQTT Broker

MQTT
Sparkplug

Customer Cloud

DB

4

RANGER

MQTT
Sparkplug

SignalFire MQTT Broker

MQTT
Sparkplug

SignalFire Cloud

DB

API

Customer Cloud

DB

SIGNALFIRE RANGER CONNECTIVITY OPTIONS

1. SignalFire Cloud Method

The SignalFire Cloud is a feature rich web application fully hosted and managed by SignalFire. It offers the ultimate experience in terms of plug-and-play experience, from measuring to visualization. The interface is designed with a Do-It-Yourself (DIY) mindset allowing users to quickly make use of measurements coming from a RANGER. From starting up a RANGER ,assigning a widget to a variable, trending data, alarming on data, SMS and Email alarms by exception, scheduled reports, GPS monitoring, remote configuration , user management, customized dashboards and more. The web application requires a web browser and therefore works with smart phones, tablet readers, computers without the need to install any software.
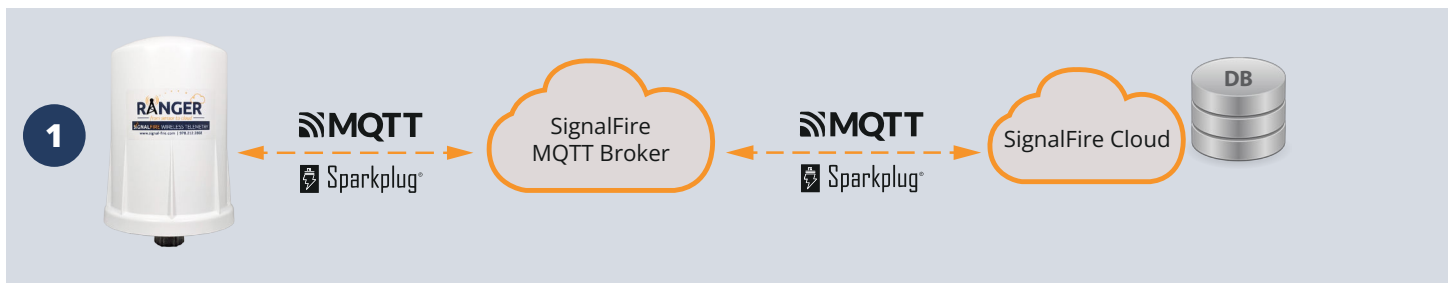
2. Subscribing from SignalFire's MQTT Broker

When using a private broker, the RANGER needs to first be configured to publish its data to said MQTT Broker. This is accomplished by connecting a computer running the RANGER toolkit software using a USB cable provided with the RANGER. The MQTT Broker is hosted by the user or a third party. The RANGER supports several modes for secured connection. TLS certificate with TLS validation and authentication is the most secured connectivity. The RANGER can be setup with a username and password as well to match the broker's credentials.

All the parameters (Tags, MQTT Topics) are available for use by the web application. Such web application must be capable of parsing SparkPlugB messages over MQTT. These parameters are listed in the published RANGER Tag Guide that can be found on the SignalFire website (www.signal-fire.com) and are fully available bi-directionally. If a Tag is writable, the hosting/publishing application can send a write command to change said parameter. In this scenario, SignalFire's technical support has no capabilities to remotely troubleshoot the RANGER because the RANGER isn't connected to SignalFire's MQTT Broker. Also, the HART Remote PACTware connectivity isn't possible as it requires HART Tunneling via the SignalFire Cloud.
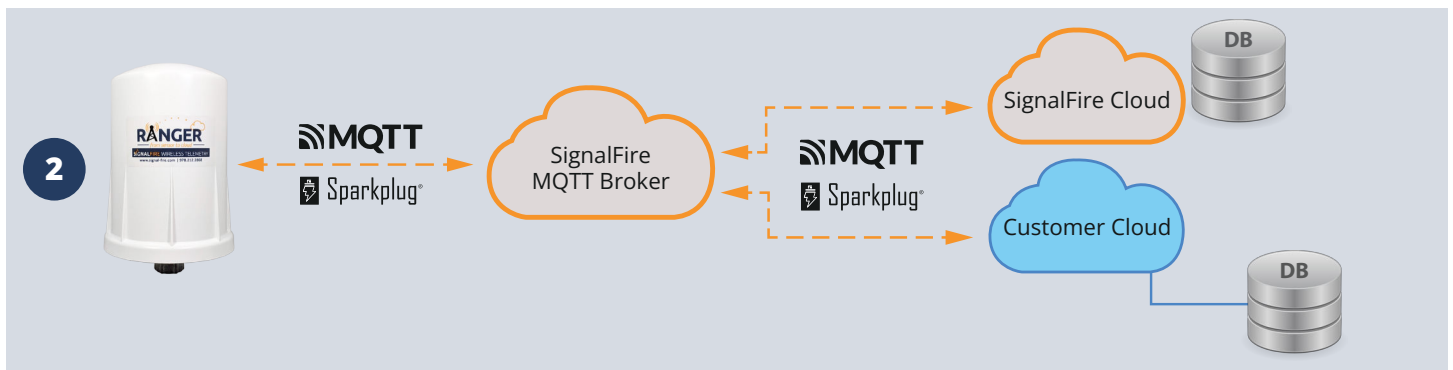
3. Private Broker Method

When using a private broker, the RANGER needs to first be configured to publish its data to said MQTT Broker. This is accomplished by connecting a computer running the RANGER toolkit software using a USB cable provided with the RANGER. The MQTT Broker is hosted by the user or a third party.   The RANGER supports several modes for secured connection. TLS certificate with TLS validation and authentication is the most secured connectivity.   The RANGER can be setup with a username and password as well to match the broker's credentials.

All the parameters (Tags, MQTT Topics) are available for use by the web application. Such web application must be capable of parsing SparkPlugB messages over MQTT. These parameters are listed in the published RANGER Tag Guide that can be found on www.signal-fire.com and are fully available bi-directionally. If a Tag is writable, the hosting/publishing application can send a write command to change said parameter. In this scenario, SignalFire's technical support has no capabilities to remotely troubleshoot the RANGER because the RANGER isn't connected to SignalFire's MQTT Broker. Also, the HART Remote PactWare connectivity isn't possible as it requires HART Tunneling via the SignalFire Cloud.
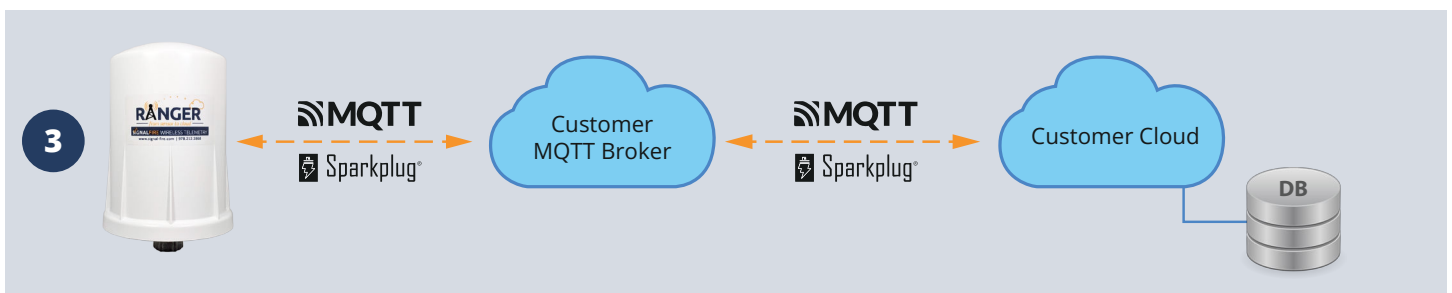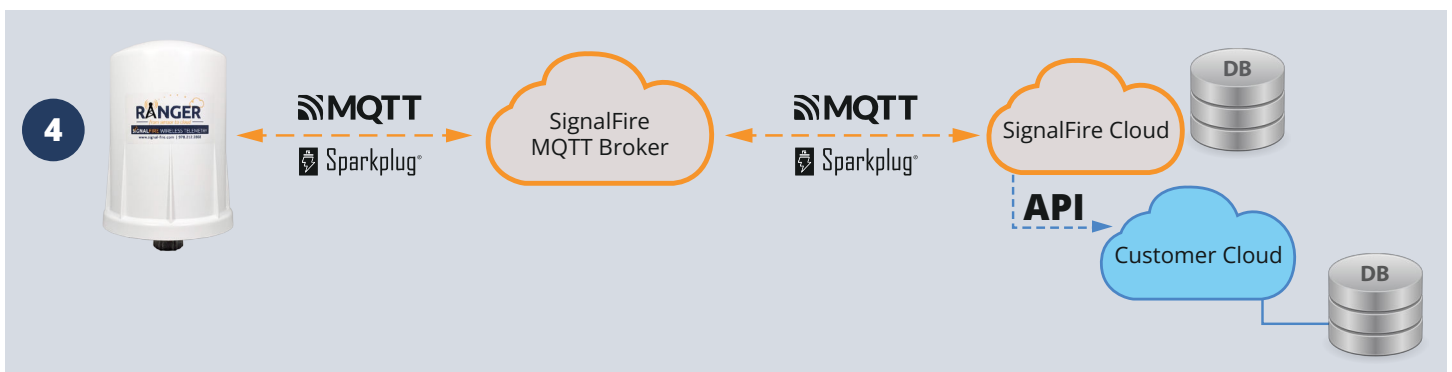

4. REST API Data Polling Method

For applications that don't support MQTT/SparkPlugB technology, SignalFire offers a REST API to poll data from the SignalFire Cloud's database. The REST API offers several commands to poll data from one or many RANGERs at once, to poll a time delimited series of values, etc. The data is formatted using JSON, a common data type widely used by many applications.

For a secured connection, SignalFire will setup a connection using a Token. Once SignalFire configures the account for API connectivity, the Token is requested by the user and can solely downloaded by the user who requested API integration. Every REST API request is secured using such Token.

The REST API implementation does require a subscription to the SignalFire Cloud. The benefit are the use of the SignalFire Cloud for setup, commissioning, troubleshooting, managing of RANGERs with remote technical support from SignalFire.

A user can implement the REST API commands using Python script, JavaScript or Curl. To facilitate the deployment, obtain the schema for the data and to validate the returned variables, the REST API is fully functional with tools like OpenAPI, Swagger or ReDoc.

SIGNALFIRE RANGER CONNECTIVITY CAPABILITIES CHART

Capability	SignalFire Cloud	SignalFire's MQTT Broker	Private Broker	REST API Data Polling
	Method #1	Method #2	Method #3	Method #4
MQTT Broker Hosted and Managed by SignalFire	☑	☑		☑
SignalFire Cloud Features & Ready to Use Web App	☑	☑	Not Applicable	☑
SignalFire Real Time Remote Support	☑	☑		☑
Data Connectivity Using MQTT SparkplugB	☑	☑	☑	☑
Data Connectivity Using REST API	Not Applicable	Not Applicable	Not Applicable	☑
Bi-Directional Communication with RANGER with SignalFire Cloud	☑	☑	Not Applicable	☑
Bi-Directional Communication with RANGER by 3rd party	Not Applicable	☑	☑	
Remote PACTware (or similar) for HART devices	☑	☑		☑
Published RANGER data Instantly Synchronized with Host	☑	☑	☑	
Automated Store Forward upon loss of communication	☑	☑	☑	☑