

Application Note

Connecting to the SignalFire Cloud using Ignition from Inductive Automation

OVERVIEW

Situations exist when Ranger users need to access the Ranger data by another system in addition to the SignalFire Cloud service. In these situations, a secure connection to the SignalFire MQTT broker can be configured, there is a setup fee associated with this option. Contact SignalFire for details.

This guide details how to configure Ignition to connect to the SignalFire MQTT broker, but any host that supports the MQTT Sparkplug protocol could be used.

CONFIGURATION

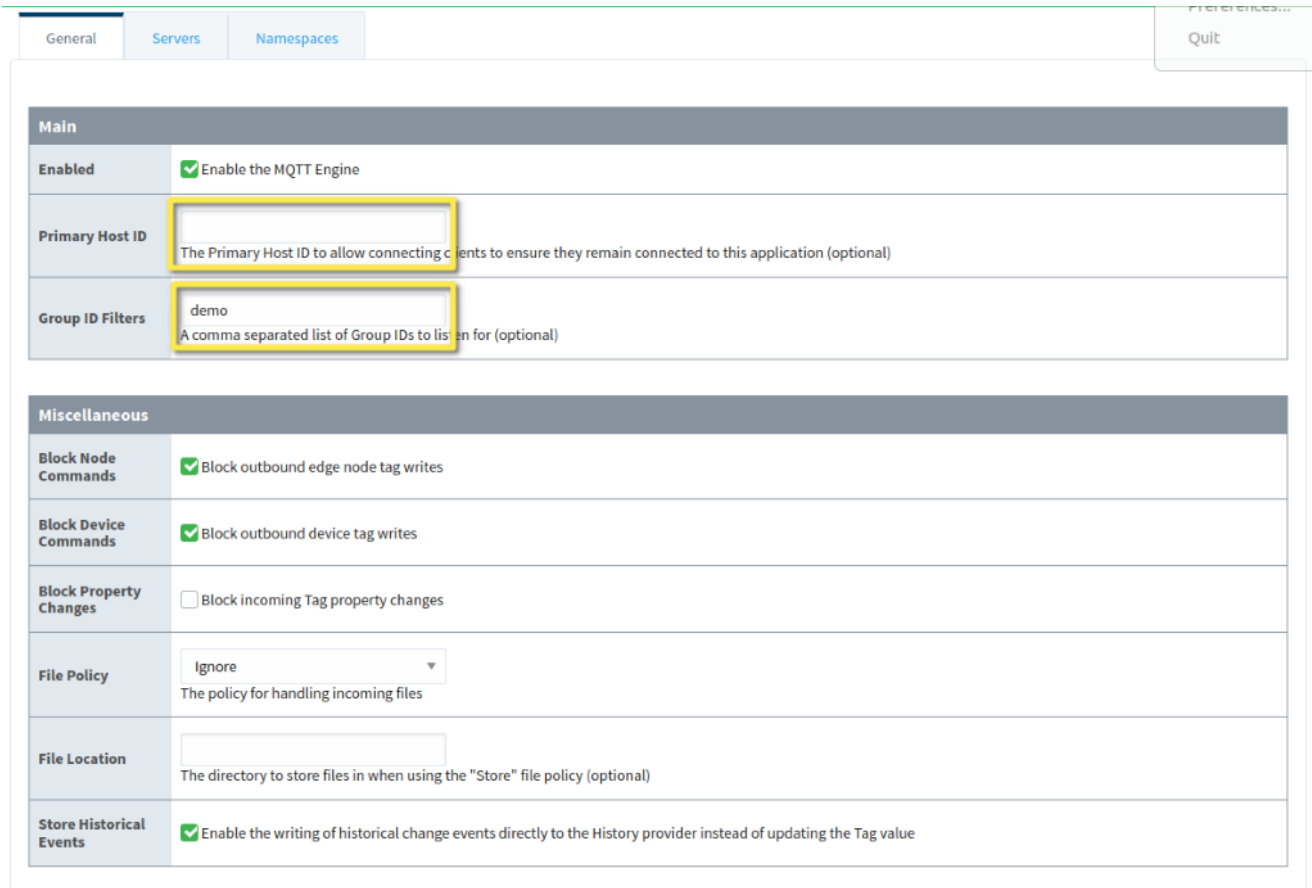
You will need to know the case-sensitive group name for your account, as provided by SignalFire. In these examples, we will be using the name "demo".

You will also need the three certificate files provided by SignalFire, with names like:

- demo-group.cert.pem
- demo-group.private.key
- sf-mqtt.ca.pem

Be sure to protect the "private" file and only give it to people who should have full access to your account. Also, be aware that the SignalFire broker is configured to only allow one connection at a time per private key. If a second connection opens using the same key, the first connection will be closed. This means if you have two clients both configured to auto-reconnect to the broker using the same key, they will keep bouncing each other offline back and forth. Additional certificates must be obtained for each connection.

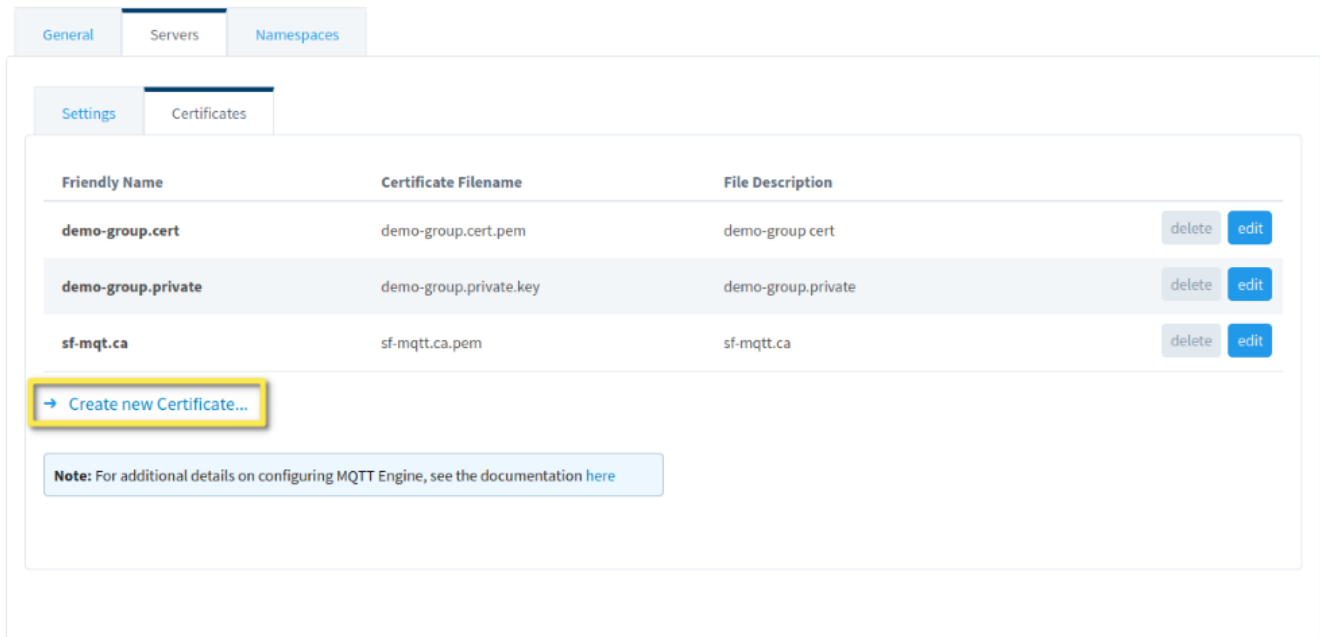
Login to the administration web page of Ignition. On the left side click "Config", then far down the left column click on "MQTT Engine"/"Settings".



Main	
Enabled	<input checked="" type="checkbox"/> Enable the MQTT Engine
Primary Host ID	<input type="text"/> The Primary Host ID to allow connecting clients to ensure they remain connected to this application (optional)
Group ID Filters	<input type="text" value="demo"/> A comma separated list of Group IDs to listen for (optional)

Miscellaneous	
Block Node Commands	<input checked="" type="checkbox"/> Block outbound edge node tag writes
Block Device Commands	<input checked="" type="checkbox"/> Block outbound device tag writes
Block Property Changes	<input type="checkbox"/> Block incoming Tag property changes
File Policy	<input type="text" value="Ignore"/> The policy for handling incoming files
File Location	<input type="text"/> The directory to store files in when using the "Store" file policy (optional)
Store Historical Events	<input checked="" type="checkbox"/> Enable the writing of historical change events directly to the History provider instead of updating the Tag value

On the "General" MQTT config page, the only required settings are to ensure that the "Primary Host ID" box is empty, and that the group name is included in the "Group ID Filters" box. If you plan on configuring and controlling your Ranger devices from this Ignition instance, you should also un-check the "Block Node Commands" and "Block Device Commands" boxes. Leaving them checked makes the Ignition server behave in a read-only manner over MQTT, which may be desirable depending on your needs.



Next, go to the "Servers" tab at the top, then the "Certificates" sub-tab. Upload all three certificate files using the "Create New Certificate" link on the bottom. The exact friendly name and file description entered don't matter, but we recommend just using the filename unless you have a reason to do otherwise. After you've uploaded all three, the certificates page should look like above.

Next, go to the "Servers" tab at the top, then the "Settings" sub-tab, and then click "Create New MQTT Server Setting".

Main	
Name	<input type="text" value="dev-mqtt1"/> The friendly name of this MQTT Server Setting
Enabled	<input checked="" type="checkbox"/> Enable this MQTT Server Setting
URL	<input type="text" value="ssl://dev-mqtt1.signal-fire.cloud:8883"/> The URL of the MQTT Server to connect to. Should be of the form tcp://mydomain.com:1883 or ssl://mydomain.com:8883
Username	<input type="text" value="demo-group"/> The username for connections if required by the MQTT Server (optional)
Password	<input type="password" value="•"/> The password for connections if required by the MQTT Server (optional)
Password	<input type="password" value="•"/> Re-type password for verification.

In the "Main" box on top, enter the information exactly as shown, but change the Username to be the same as the beginning of your private certificate file, leaving off the ".private.key" portion. The username in this example would be *demo-group*. The password can be any non-empty string, I usually just put in a single "x".

- Name: dev-mqtt1
- URL: ssl://dev-mqtt1.signal-fire.cloud:8883
- Username: (*beginning of private.key filename*)
- Password: x

TLS	
CA Certificate File	<input type="text" value="sf-mqt.ca"/> CA Certificate file currently in use
Client Certificate File	<input type="text" value="demo-group.cert"/> Client certificate file currently in use
Client Private Key File	<input type="text" value="demo-group.private"/> Client private key file currently in use
Password	<input type="password"/> The password associated with the certificate's private key (optional)
Password	<input type="password"/> Re-type password for verification.
Hostname Verification	<input checked="" type="checkbox"/> Enable TLS Hostname Verification

In the "TLS" box in the middle, pick the files you uploaded in the drop-down boxes, leave the password boxes empty, and enable hostname verification.

Show advanced properties

Advanced	
Client ID	<input type="text" value="demo-group"/> The MQTT Client ID for connections to the MQTT Server. If left blank one will be auto-generated (optional)
Keep Alive	<input type="text" value="30"/> The MQTT Client keep alive time (in seconds) (default: 30)
Filtered Namespaces	<input type="text"/> Comma separated list of namespaces (e.g. B&B Wzzard, Elecsys, Xirgo) to be disabled for this MQTT Server connection (optional)

Check "Show advanced properties", and then in the "Advanced" box, enter the Username again as the "Client ID".

Finally, click "Save Changes" and it will return you to the MQTT broker status view. If everything is working properly, you should expect Ignition to connect to the SignalFire broker within seconds, and show a status of "Connected".

General Servers Namespaces

Settings Certificates

Name	URL	Username	CA Certificate File	Status	
dev-mqtt1	ssl://dev-mqtt1.signal-fire.cloud:8883	demo-group	sf-mqt.ca	Connected	delete edit

→ [Create new MQTT Server Setting...](#)

Note: Outbound node and device tag writes are BLOCKED (see Advanced Settings tab)
For additional details on configuring MQTT Engine, see the documentation [here](#)

CONCLUSION

The secondary MQTT connection allows users to take advantage of the SignalFire cloud interface, while simultaneously being able to subscribe to the Ranger data to bring it into another system for a local display, data historian, or other SCADA processes.