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 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.

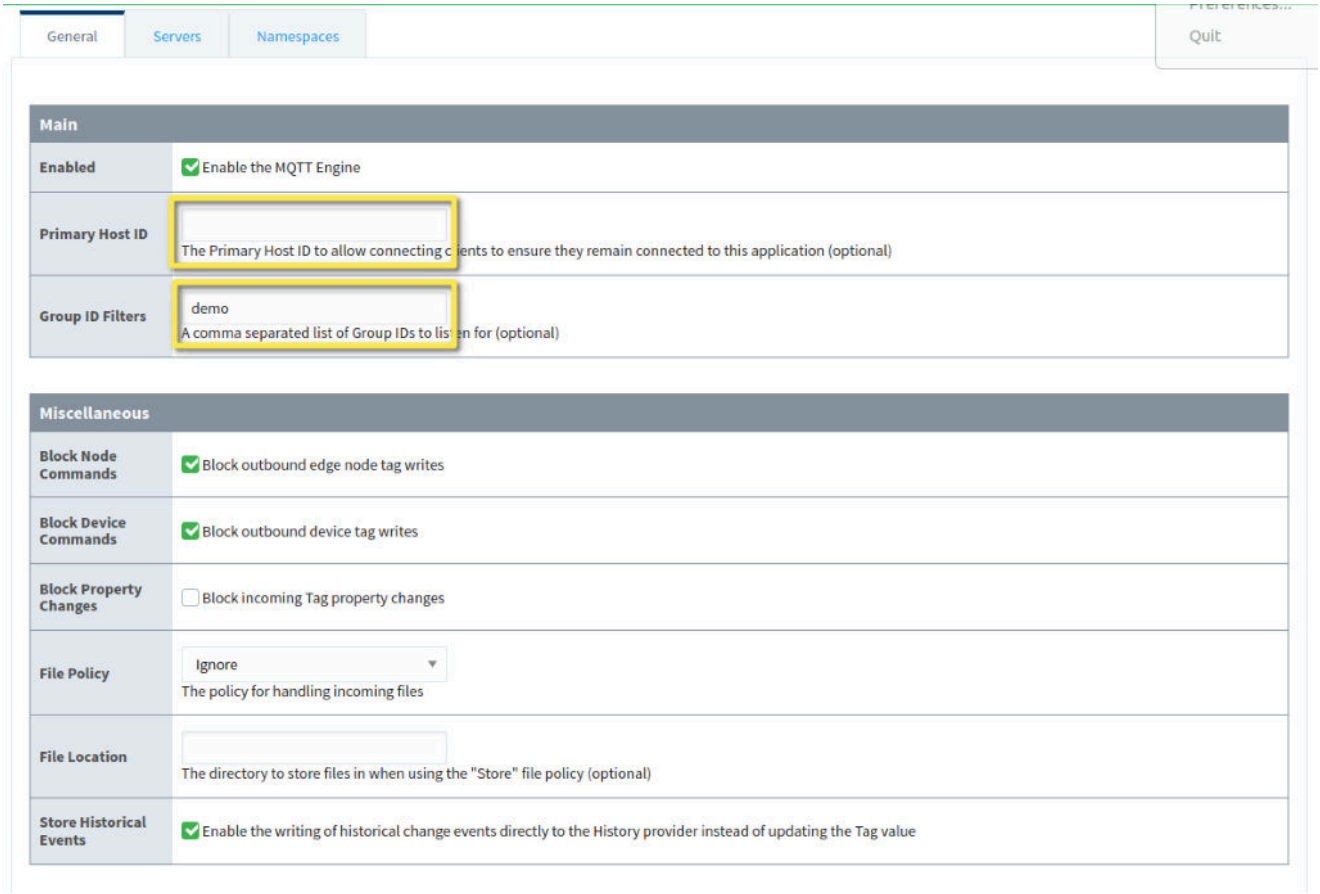
CONFIGURATION

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:

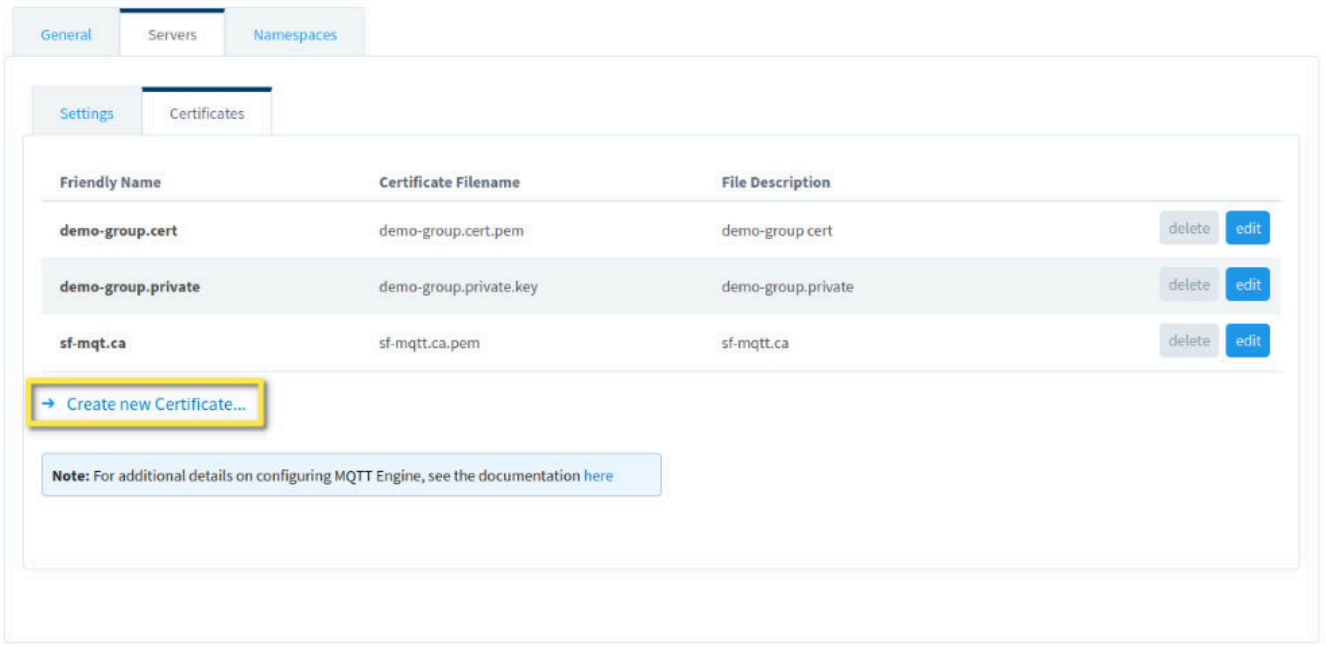
- demo-group.cert.pem
- demo-group.private.key
- sf-mqtt.ca.pem

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 open 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".



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.

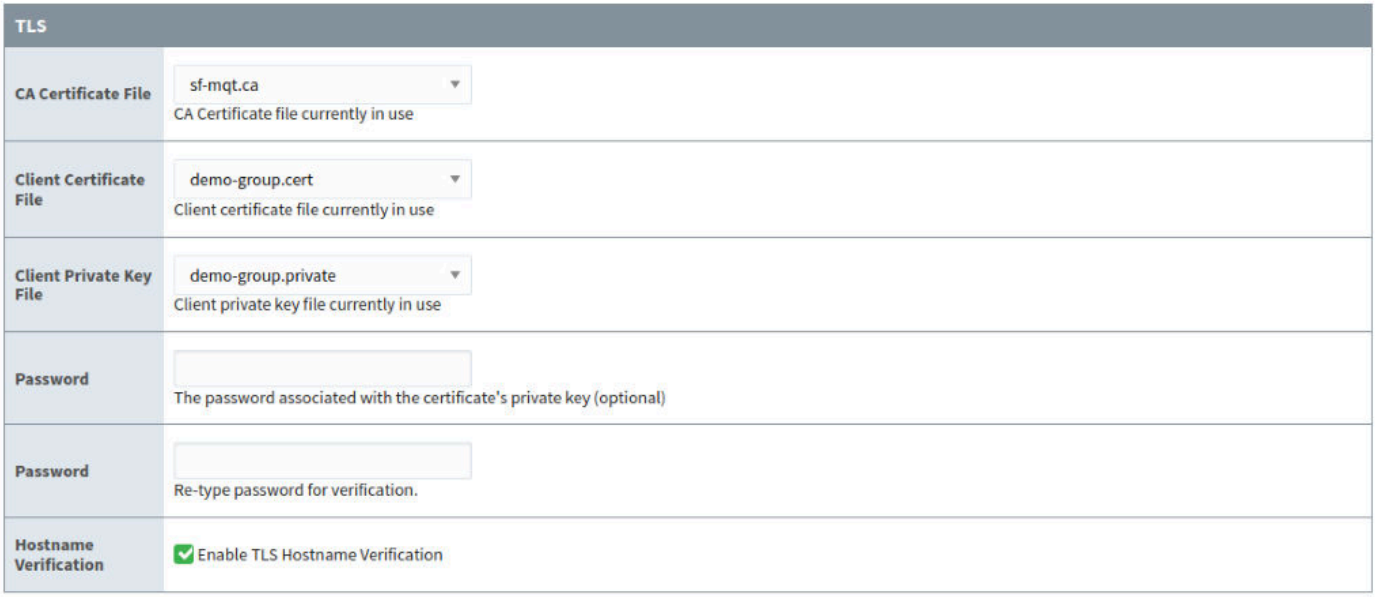


Next, go to the "Servers" tab at the top, then the "Certificates" sub-tab. Upload all three certificate files using the "Create New Certificate" link on the bottom. The exact friendly name and file description entered don't matter, but we recommend just using the filename unless you have a reason to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

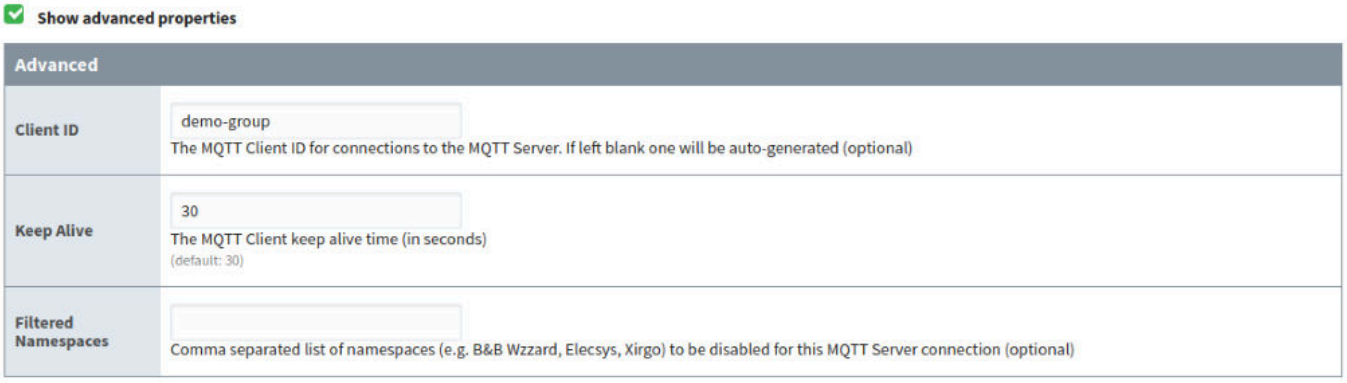
Main	
Name	dev-mqtt1 The friendly name of this MQTT Server Setting
Enabled	☑ Enable this MQTT Server Setting
URL	ssl://dev-mqtt1.signal-fire.cloud:8883 The URL of the MQTT Server to connect to. Should be of the form tcp://mydomain.com:1883 or ssl://mydomain.com:8883
Username	demo-group The username for connections if required by the MQTT Server (optional)
Password	• The password for connections if required by the MQTT Server (optional)
Password	• 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

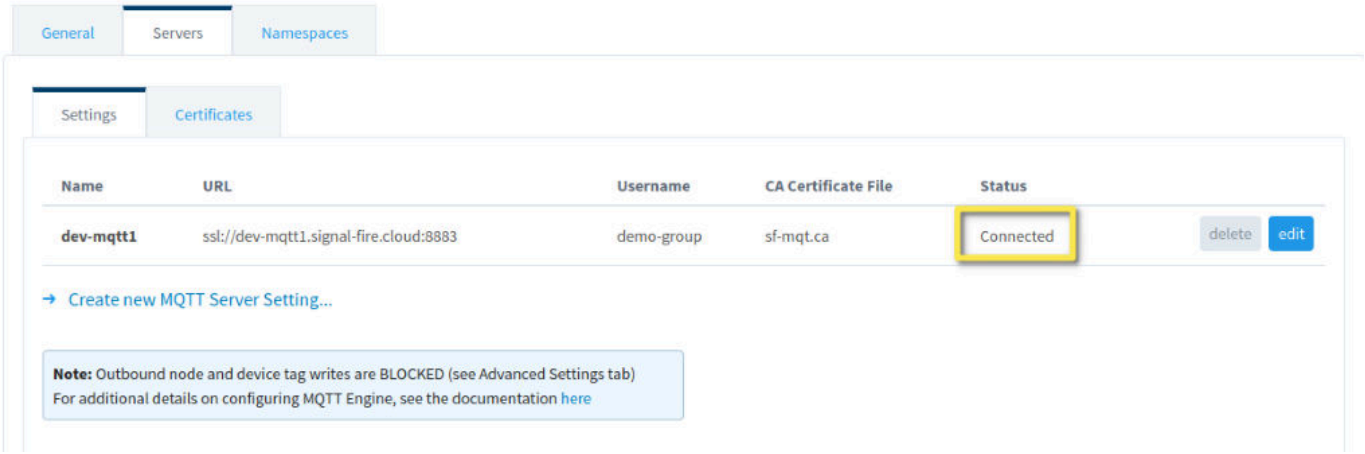


In the "TLS" box in the middle, pick the files you uploaded in the drop-down boxes, leave the password boxes empty, and enable hostname verification.



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”.



CONCLUSION

The secondary MQTT connection allows uses to take advantage of the SignalFire could 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.