< https://infosec.exchange/@jaimyn>

# MQTT – How to use ACLs and multiple user accounts

By Jaimyn Mayer < https://blog.jaimyn.dev/author/jabelone/>

January 30, 2017 < https://blog.jaimyn.dev/mqtt-use-acls-multiple-user-accounts/>

I've previously written about how awesome MQTT is and how it's an integral part of my home automation system < https://blog.jaimyn.dev/category/home-automation/> . This tutorial will show you how to make your MQTT broker more secure. In any sort of information technology you should always use the principle of least privileges. Basically, only give each account the bare minimum access that they ***actually*** need.

## 1) Define Needs

Lets use my home automation system as an example. I'll limit to just a few clients in this example. I have my automation server (home assistant), a WiFi light (a sonoff) and a light sensor. Lets state the minimum needs of each client:

### Home Assistant

- Process all MQTT messages to allow full control of devices and to run automation scripts

### WiFi light (sonoff)

- Subscribes to "**cmnd/light/POWER**" for control
- Subscribes to "**cmnd/light/UPDATE**" for OTA updates
- Publishes to "**stat/light/POWER**" for status and confirmation

### Light Sensor

- Subscribes to "**cmnd/sensor/kitchen/light**" for a manual sensor reading
- Subscribes to "**cmnd/sensor/kitchen/light/set**" to change settings
- Subscribes to "**cmnd/sensor/UPDATE**" for OTA updates
- Publishes to "**stat/sensor/kitchen/level**" with current light level

## 2) Create User Accounts

We can now see we have three clients with distinct, separate needs. This is a good case where three MQTT user accounts would be beneficial. Let's say our Light Sensor has a security flaw that accidentally exposes the password, we don't want to give someone full access to our system!

If you haven't already, follow **Digital Ocean's tutorial < https://www.digitalocean.com/community/tutorials/how-to-install-and-secure-the-mosquitto-mqtt-messaging-broker-on-ubuntu-16-04>** on setting up and securing Mosquitto. To add a new user account is quite easy. Simply run the following command and follow the prompts to enter a password.

```
sudo mosquitto_passwd /etc/mosquitto/passwd <new-user>
```

So in total, you should run 3 commands that look something like these, note how I like to obscure the usernames a little. Call me paranoid, but it makes them just a little bit harder to guess.

```
sudo mosquitto_passwd /etc/mosquitto/passwd homeassist
sudo mosquitto_passwd /etc/mosquitto/passwd sonoffswitch
sudo mosquitto_passwd /etc/mosquitto/passwd lightsense
```

## Note: make sure you use a *very* secure password for the home assitant account as it will have full access!

### 3) Tell Mosquitto to use ACLs

Open your mosquitto configuration file:

```
sudo vim /etc/mosquitto/conf.d/default.conf
```

Add the following line, specifying where you put your ACL file. (I put mine in the same directory as the passwd file)

```
acl_file /etc/mosquitto/acl
```

### MQTT has two types of wildcards:

1. "#" means literally everything and is "recursive" so can only be used on the end of a topic.
    a. example "**cmnd/light/#**" will receive every message from topics that start with "**cmnd/light**".
2. "+" meanse literally everything but only one level, so one or more may be used inside a topic.
    a. example "**stat/+/POWER**" could receive the "**POWER**" message from every device.

### Generate your ACLs

Open your ACL file and add your topics and user accounts to it like below. Note the three types of permissions; there are read, write and readwrite. Wild cards may also be used. Also, please for the sanity of future you document what each one does!

```
# Give Home Assitant full access to everything
user homeassist
topic readwrite #

# Allow the sonoffs to read/write to cmnd/# and stat/#
user sonoffswitch
topic readwrite cmnd/#
topic readwrite stat/#

# Allows the light sensor to read/write to the sensor topics
user lightsense
topic cmnd/sensor/#
topic stat/sensor/#
```

Notice how the light sensors have a similar permission level as the sonoffs? The sensors don't need to read/write to the sonoffs so they shouldn't be allowed. However, we may want the sonoffs to be able to directly read the sensors.

### 4) Save and profit ??

Save all the settings and make sure they're right. Normally I wouldn't reccomend it, but it may be useful to right down the usernames and passwords of all the accounts. This could save a lot of confusion with all the different accounts. (of course you should destroy the passwords after)

Be sure to restart both home assitant if you've got it running and the Mosquitto server so that the changes can be applied.

```
sudo service mosquitto restart
sudo service homeassistant restart
```

Let me know how you go or if you run into trouble in the comments below. I couldn't find much documentation on actually implementing ACLs and multiple user accounts so hopefully this makes it easier for others.

 **Up ↑**