Securing Ubiquiti WiFi Systems

- This guide is not enough:
  - https://help.ui.com/hc/en-us/articles/115006116807-Ubiquiti-s-Guide-to-Basic-Security

- Especially when BHIS shares stuff like this:
  - https://www.blackhillsinfosec.com/hacking-unifi-controller-passwords-for-fun-and-wifi/
  - "Remember, MongoDB is running without authentication. You only need local loopback privilege (even remotely) to modify the database. "

- And then, of course, there was this:
  - https://krebsonsecurity.com/2021/03/whistleblower-ubiquiti-breach-catastrophic/

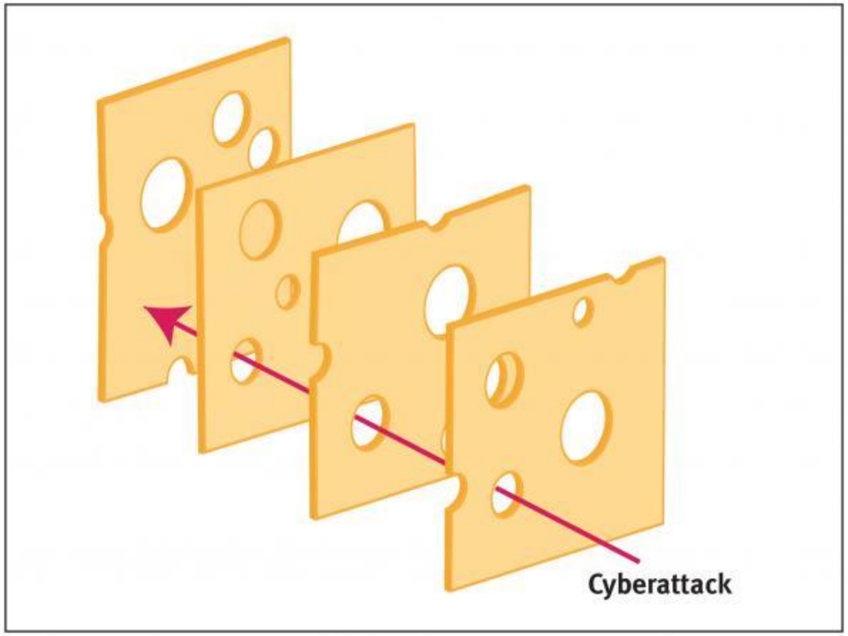
Security Cheese

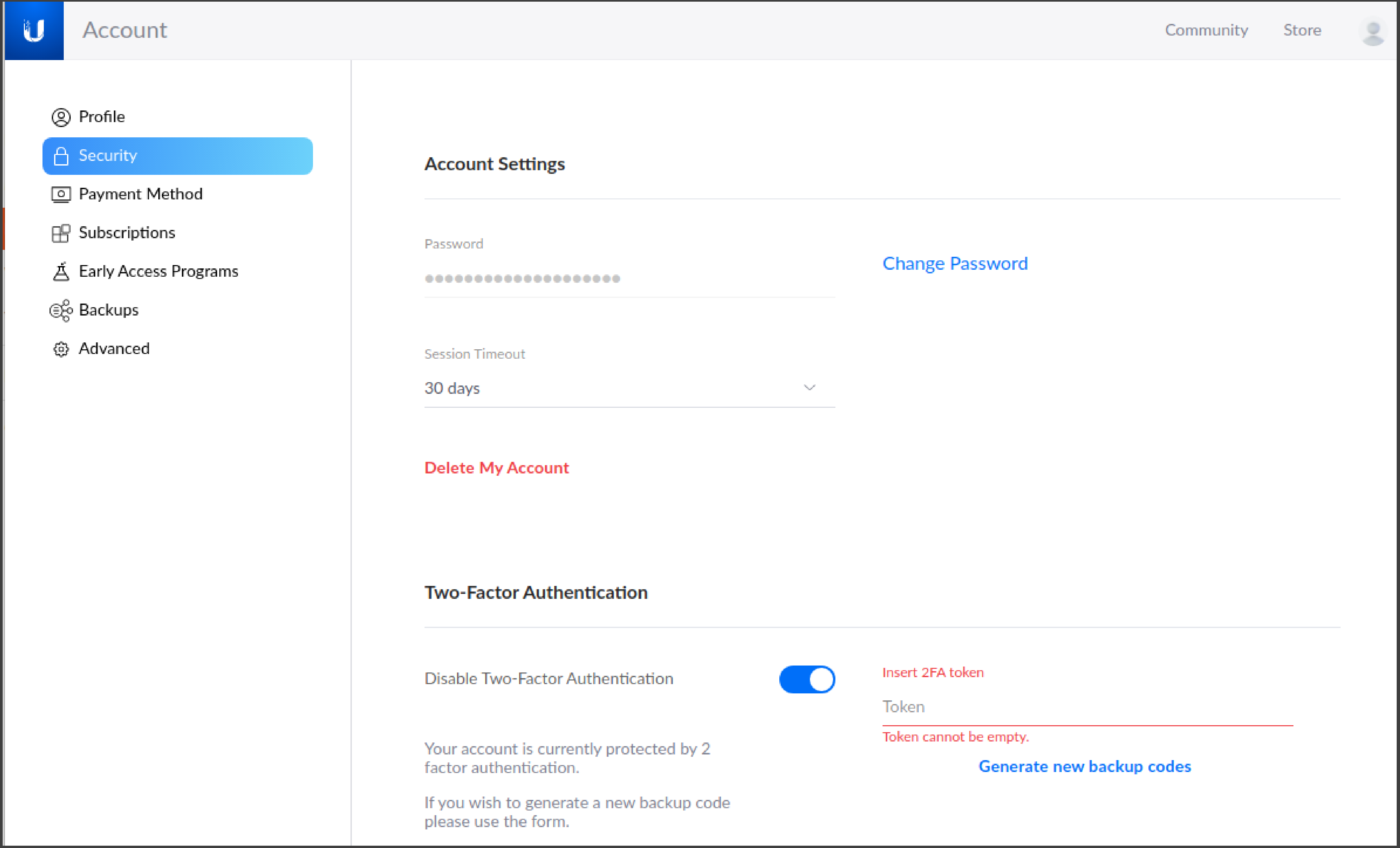
(Some call them pillars, triads and even add a fourth and it's a quadrant. It's all cheesy, so I'm calling them the 3 cheeses)

1. **Authentication –** Change the default passwords, set difficult to guess passwords, use MFA, use key-based authentication where available.

2. **Software Updates –** Keep software AND firmware up-to-date on all systems and devices. Replace legacy hardware that no longer receives updates.

3. **Configuration & Monitoring –** Configure the systems to alert you when updates are available, enable the appropriate level of security controls and secure configurations that often are not turned on by default.





Account Settings

Password
●●●●●●●●●●●●●●●●●●●●

Change Password

Session Timeout
30 days

Delete My Account

Two-Factor Authentication

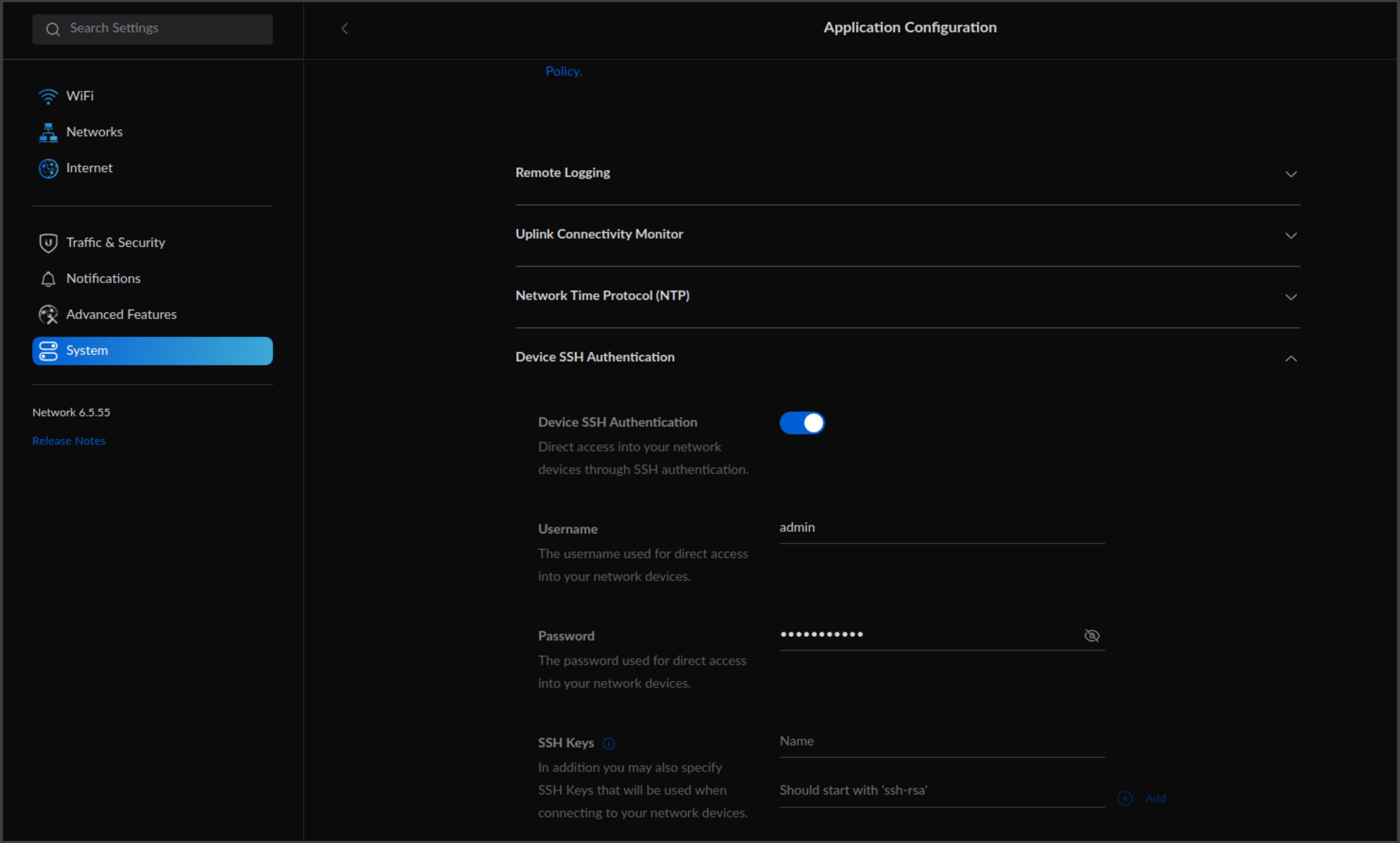
Disable Two-Factor Authentication

Insert 2FA token
Token
Token cannot be empty.

Generate new backup codes

Your account is currently protected by 2 factor authentication.

If you wish to generate a new backup code please use the form.



Application Configuration

Policy.

Remote Logging

Uplink Connectivity Monitor

Network Time Protocol (NTP)

Device SSH Authentication

Device SSH Authentication
Direct access into your network devices through SSH authentication.

Username: admin
The username used for direct access into your network devices.

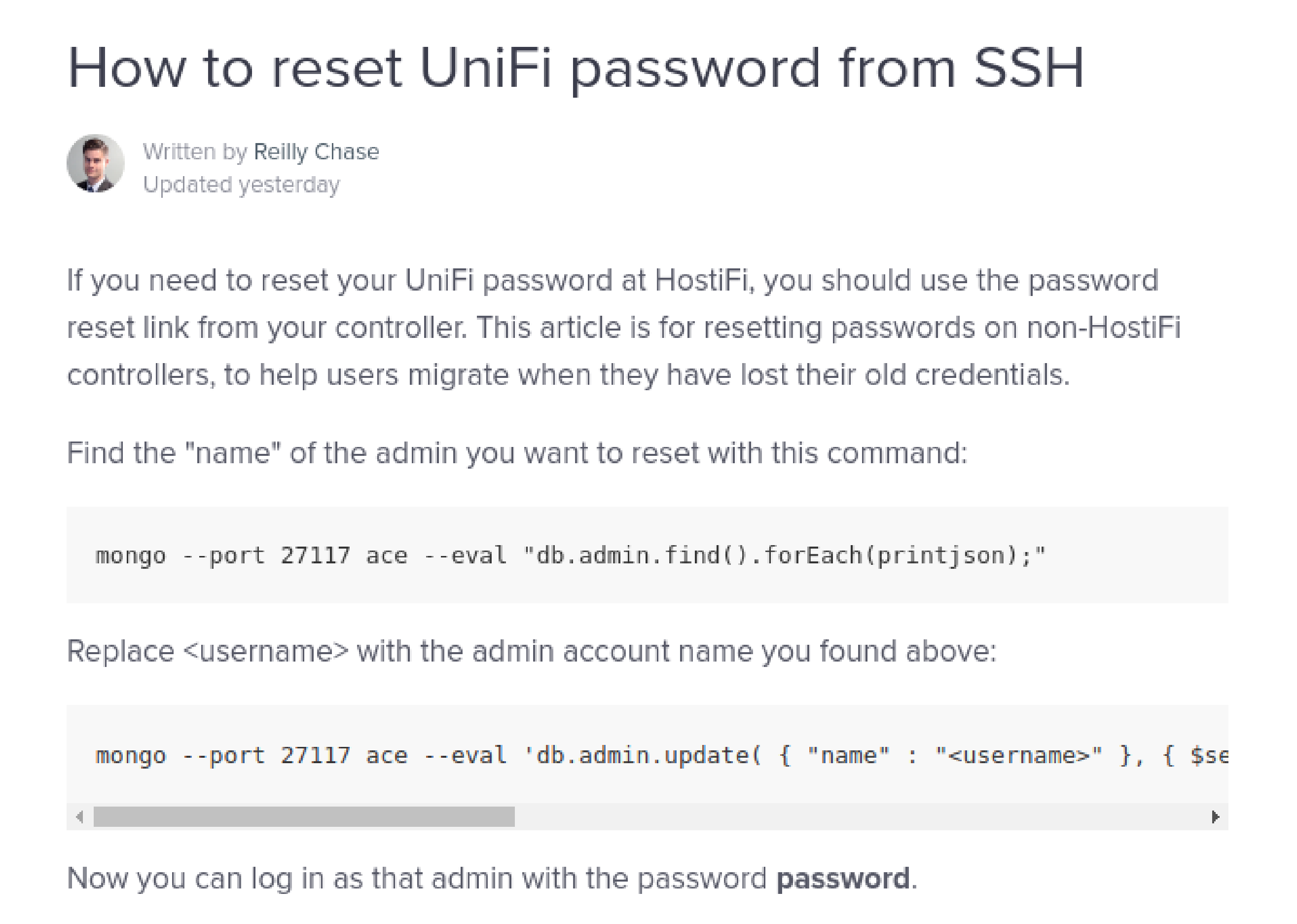
Password: ••••••••••••
The password used for direct access into your network devices.

SSH Keys: Name / Should start with 'ssh-rsa' ⊕ Add
In addition you may also specify SSH Keys that will be used when connecting to your network devices.

Store all of these in a password vault!

Defaults:

ubnt/ubnt
root/ubnt
admin/ubnt



How to reset UniFi password from SSH

Written by Reilly Chase
Updated yesterday

If you need to reset your UniFi password at HostiFi, you should use the password reset link from your controller. This article is for resetting passwords on non-HostiFi controllers, to help users migrate when they have lost their old credentials.

Find the "name" of the admin you want to reset with this command:

```
mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"
```

Replace <username> with the admin account name you found above:

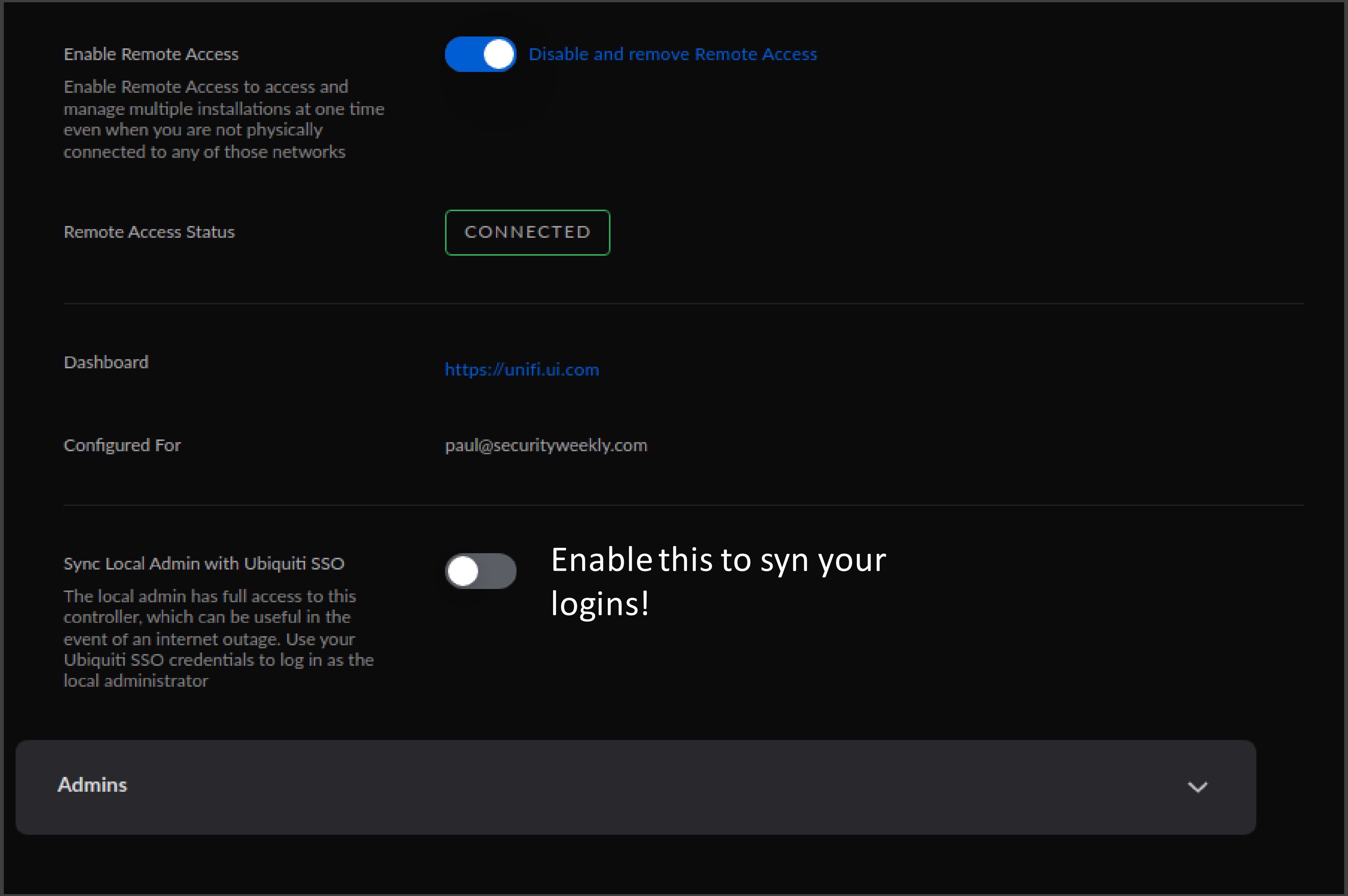
```
mongo --port 27117 ace --eval 'db.admin.update( { "name" : "<username>" }, { $se
```

Now you can log in as that admin with the password **password**.

```
mongo --port 27117 ace --eval "db.admin.find().forEach(printjson);"

mongo --port 27117 ace --eval 'db.admin.update( { "name" : "<username>" }, { $set : { "x_shadow" :
"$6$ybLXKYjTNj9vv$dgGRjoXYFkw33OFZtBsp1flbCpoFQR7ac8O0FrZixHG.sw2AQmA5PuUbQC/e5.Zu.f7pGuF7qBKAfT/JRZFk8/" }
} )'
```

https://support.hostifi.com/en/articles/3561102-how-to-reset-unifi-password-from-ssh



Enable Remote Access

Enable Remote Access to access and manage multiple installations at one time even when you are not physically connected to any of those networks

Remote Access Status: CONNECTED

Dashboard: https://unifi.ui.com

Configured For: paul@securityweekly.com

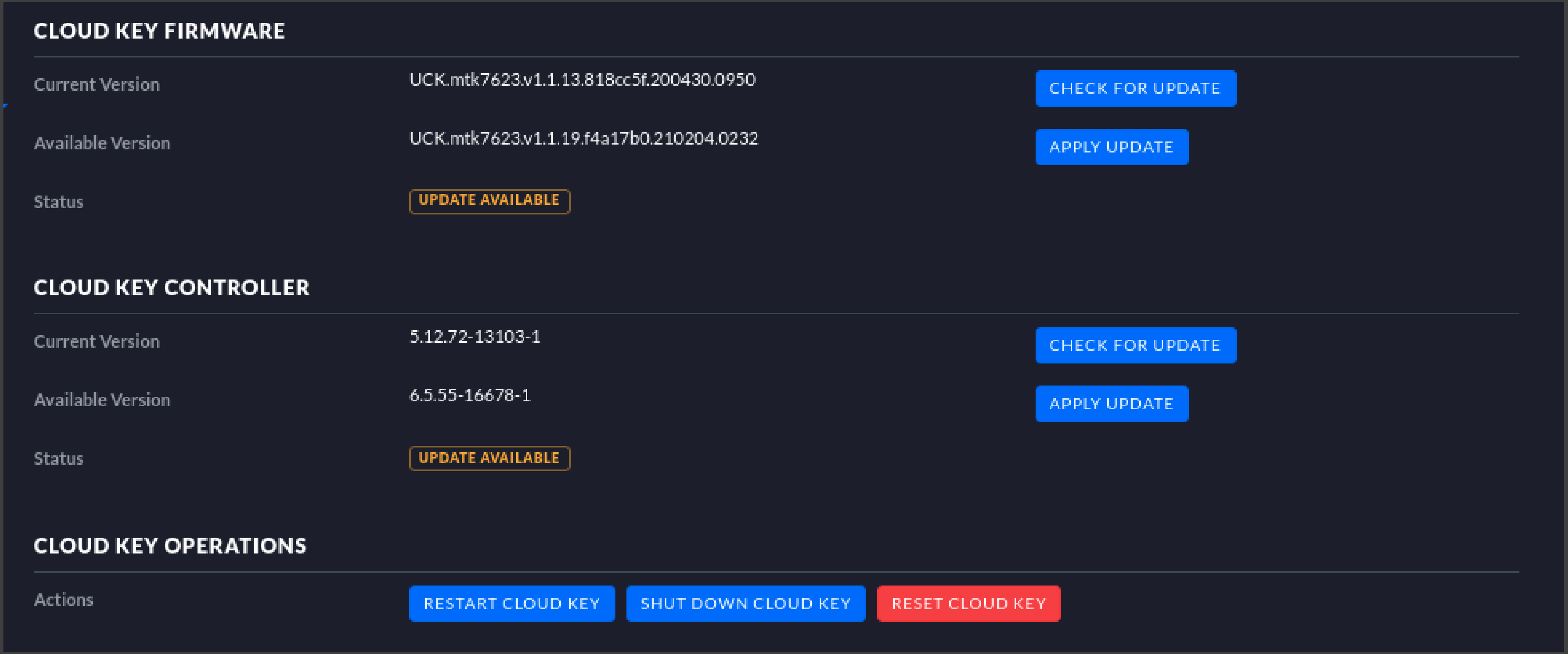
Sync Local Admin with Ubiquiti SSO

The local admin has full access to this controller, which can be useful in the event of an internet outage. Use your Ubiquiti SSO credentials to log in as the local administrator

Enable this to syn your logins!

Disable and re-enable after factory reset

There is a bug…



CLOUD KEY FIRMWARE

Current Version	UCK.mtk7623.v1.1.13.818cc5f.200430.0950	CHECK FOR UPDATE
Available Version	UCK.mtk7623.v1.1.19.f4a17b0.210204.0232	APPLY UPDATE
Status	UPDATE AVAILABLE	

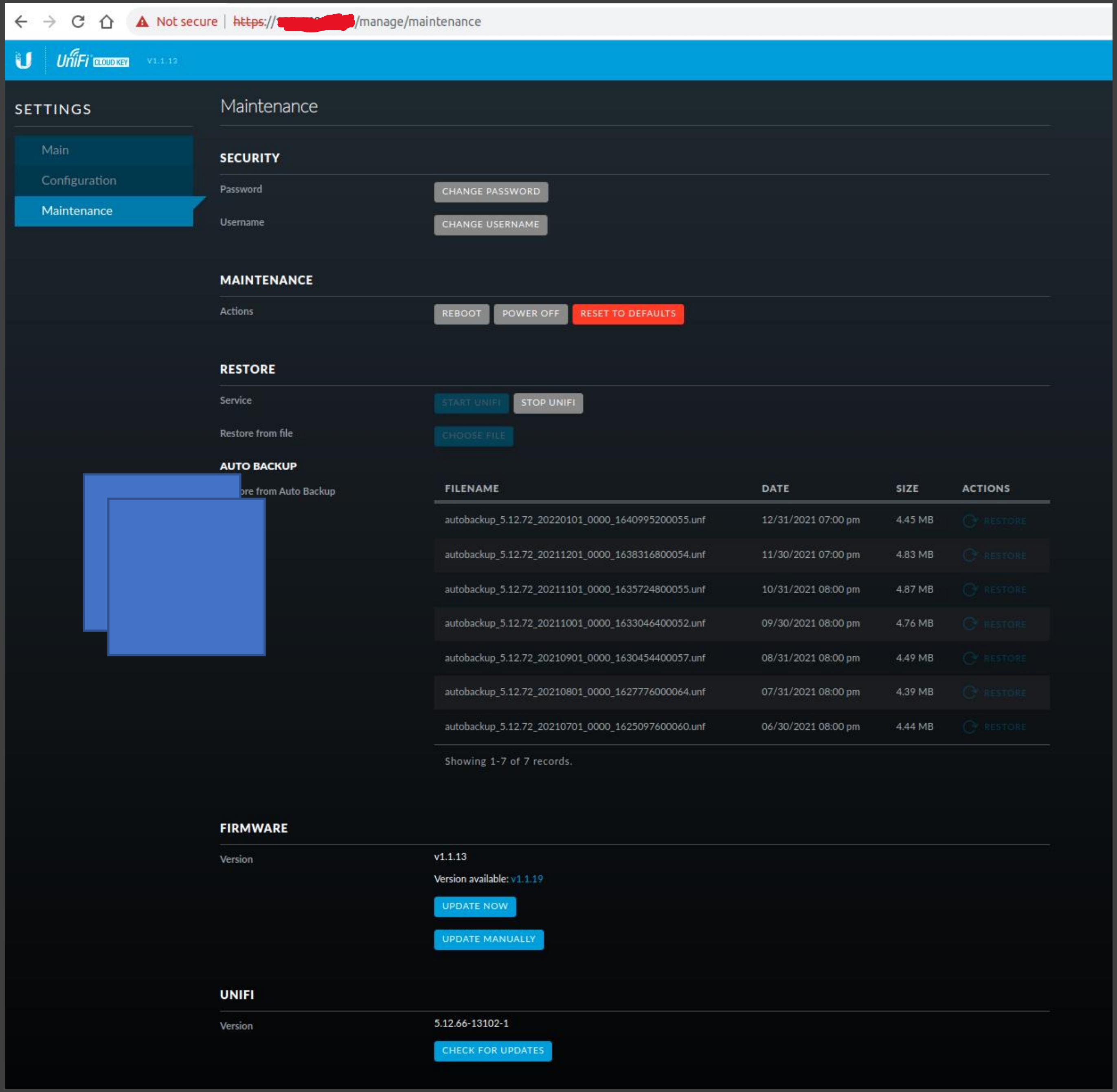
CLOUD KEY CONTROLLER

Current Version	5.12.72-13103-1	CHECK FOR UPDATE
Available Version	6.5.55-16678-1	APPLY UPDATE
Status	UPDATE AVAILABLE	

CLOUD KEY OPERATIONS

Actions

After factory reset, I was able to access the Cloud Key directly and upgrade...



SETTINGS

- Main
- Configuration
- Maintenance

Maintenance

SECURITY

Password: CHANGE PASSWORD

Username: CHANGE USERNAME

MAINTENANCE

Actions: REBOOT · POWER OFF · RESET TO DEFAULTS

RESTORE

Service: START UNIFI · STOP UNIFI

Restore from file: CHOOSE FILE

AUTO BACKUP

[redacted]ore from Auto Backup

FILENAME	DATE	SIZE	ACTIONS
autobackup_5.12.72_20220101_0000_1640995200055.unf	12/31/2021 07:00 pm	4.45 MB	RESTORE
autobackup_5.12.72_20211201_0000_1638316800054.unf	11/30/2021 07:00 pm	4.83 MB	RESTORE
autobackup_5.12.72_20211101_0000_1635724800055.unf	10/31/2021 08:00 pm	4.87 MB	RESTORE
autobackup_5.12.72_20211001_0000_1633046400052.unf	09/30/2021 08:00 pm	4.76 MB	RESTORE
autobackup_5.12.72_20210901_0000_1630454400057.unf	08/31/2021 08:00 pm	4.49 MB	RESTORE
autobackup_5.12.72_20210801_0000_1627776000064.unf	07/31/2021 08:00 pm	4.39 MB	RESTORE
autobackup_5.12.72_20210701_0000_1625097600060.unf	06/30/2021 08:00 pm	4.44 MB	RESTORE

Showing 1-7 of 7 records.

FIRMWARE

Version: v1.1.13

Version available: v1.1.19

UPDATE NOW

UPDATE MANUALLY

UNIFI

Version: 5.12.66-13102-1

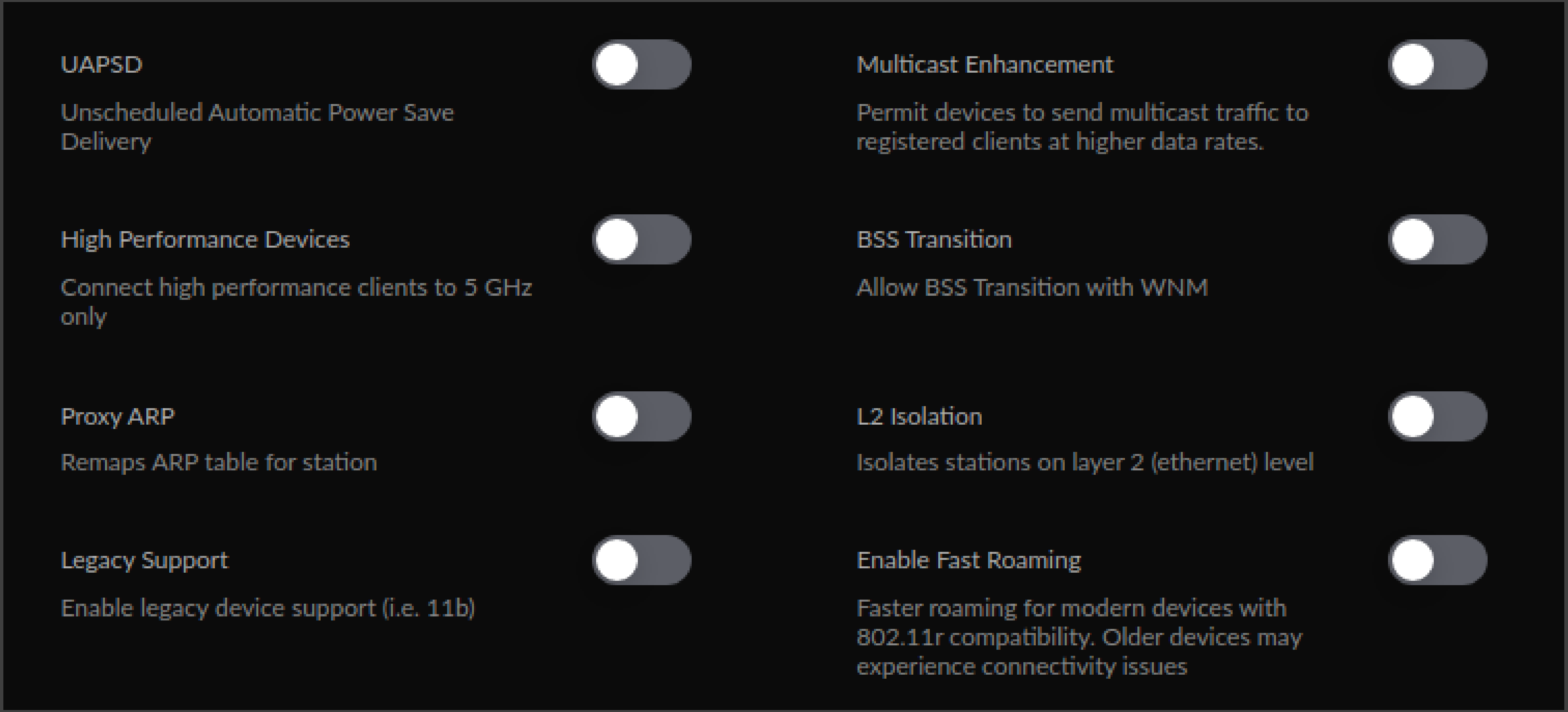
CHECK FOR UPDATES

If You Do Not Want To Buy A Cloudkey

```
$ docker run --detach \
--name=unifi-controller \
-e PUID=1000 \
-e PGID=1000 \
-e MEM_LIMIT=1024M `#optional` \
-p 3478:3478/udp \
-p 10001:10001/udp \
-p 8080:8080 \
-p 8081:8081 \
-p 8443:8443 \
-p 8843:8843 \
-p 8880:8880 \
-p 6789:6789 \
-v /home/ubuntu/config:/config \
--restart unless-stopped \
--privileged \
linuxserver/unifi-controller:arm64v8-latest
```

https://hub.docker.com/r/linuxserver/unifi-controller

Natively: https://community.ui.com/questions/Step-By-Step-Tutorial-Guide-Raspberry-Pi-with-UniFi-Controller-and-Pi-hole-from-scratch-headless/e8a24143-bfb8-4a61-973d-0b55320101dc



UAPSD ○

Unscheduled Automatic Power Save Delivery

Multicast Enhancement ○

Permit devices to send multicast traffic to registered clients at higher data rates.

High Performance Devices ○

Connect high performance clients to 5 GHz only

BSS Transition ○

Allow BSS Transition with WNM

Proxy ARP ○

Remaps ARP table for station

L2 Isolation ○

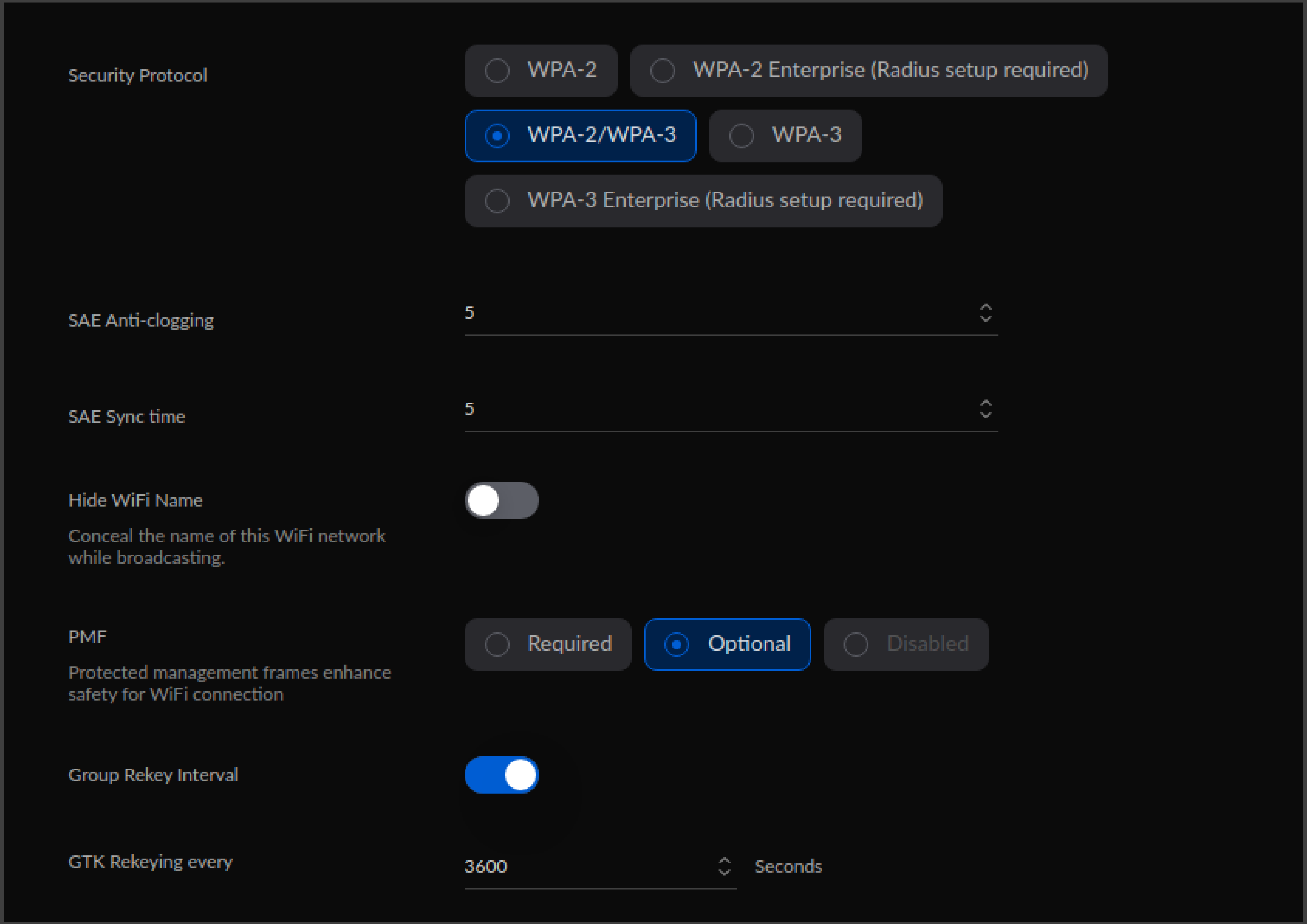
Isolates stations on layer 2 (ethernet) level

Legacy Support ○

Enable legacy device support (i.e. 11b)

Enable Fast Roaming ○

Faster roaming for modern devices with 802.11r compatibility. Older devices may experience connectivity issues



Security Protocol ○ WPA-2 ○ WPA-2 Enterprise (Radius setup required) ● WPA-2/WPA-3 ○ WPA-3 ○ WPA-3 Enterprise (Radius setup required)

SAE Anti-clogging 5

SAE Sync time 5

Hide WiFi Name ○ (off)

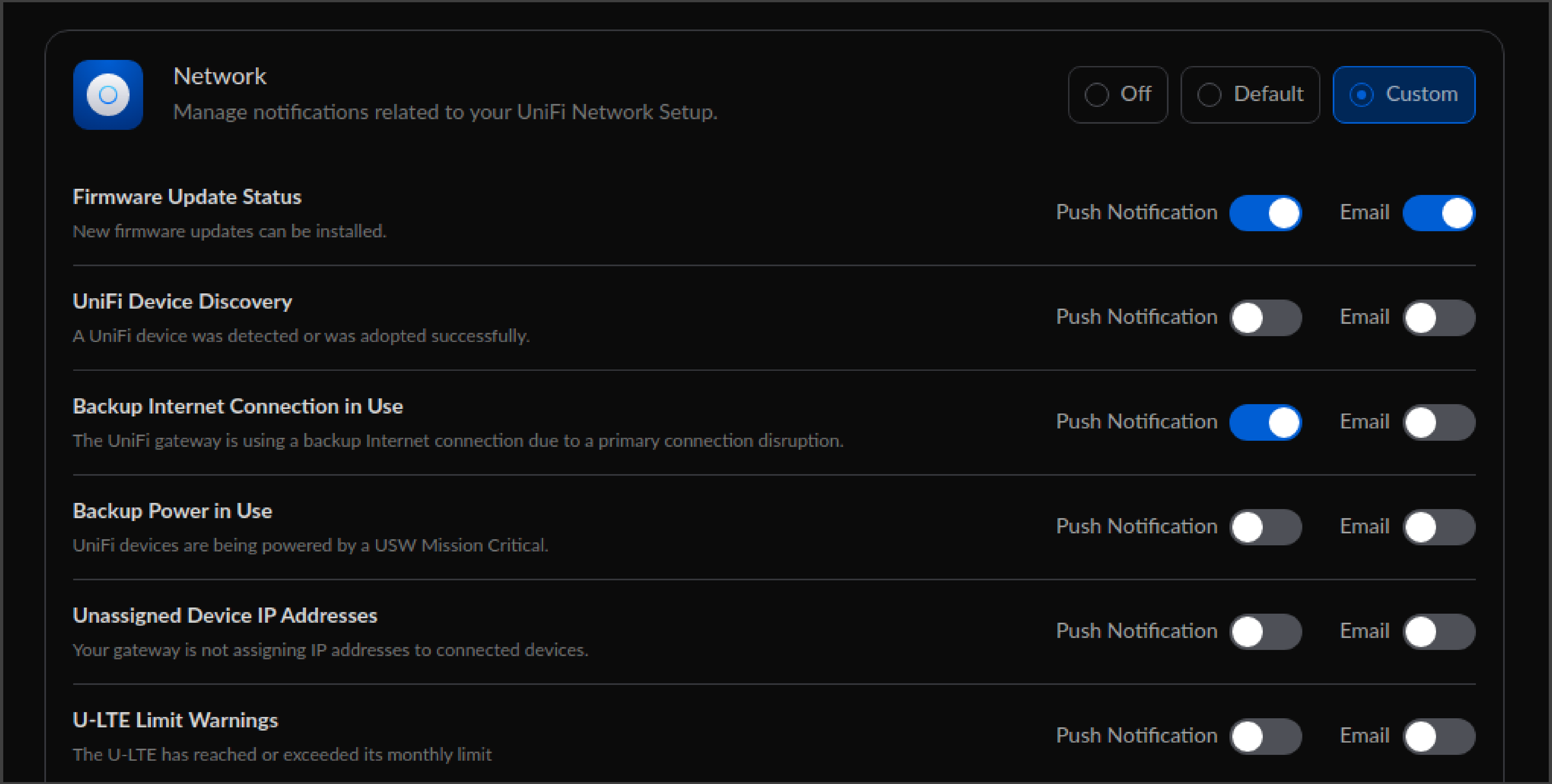
Conceal the name of this WiFi network while broadcasting.

PMF ○ Required ● Optional ○ Disabled

Protected management frames enhance safety for WiFi connection

Group Rekey Interval ● (on)

GTK Rekeying every 3600 Seconds



Network

Manage notifications related to your UniFi Network Setup.

○ Off ○ Default ● Custom

Firmware Update Status
New firmware updates can be installed.
Push Notification ☑ Email ☑

UniFi Device Discovery
A UniFi device was detected or was adopted successfully.
Push Notification ☐ Email ☐

Backup Internet Connection in Use
The UniFi gateway is using a backup Internet connection due to a primary connection disruption.
Push Notification ☑ Email ☐

Backup Power in Use
UniFi devices are being powered by a USW Mission Critical.
Push Notification ☐ Email ☐

Unassigned Device IP Addresses
Your gateway is not assigning IP addresses to connected devices.
Push Notification ☐ Email ☐

U-LTE Limit Warnings
The U-LTE has reached or exceeded its monthly limit
Push Notification ☐ Email ☐

Bonus: Decrypt Support and Backup Files

- https://github.com/zhangyoufu/unifi-backup-decrypt/blob/master/decrypt.sh

```
$ ./unifi_decrypt.sh unifi-20220126-1044.supp unifi_support
$ unzip ../unifi_support.zip


$ ls
devices  devices.json  logs  support_info.json  system.proper
ties  topology.json  webrtc
```