Morse Micro
reaching farther™

MM6108 - OpenWrt 2.7

Web UI User Guide

© 2024 Morse Micro | morsemicro.com

Table of Contents

1 Overview **5**
2 Device Setup **6**
2.1 EKH01 6
2.1.1 Basic setup 7
2.2 EKH03 8
2.2.1 Basic setup 9
2.3 Browser support 10
2.4 Standard setup scenarios 11
2.4.1 Standalone Access Point with client devices 11
2.4.2 Using HaLow as a 'virtual wire' (Layer 2 bridge) 11
2.4.3 Non-standalone Access Point with routing 12
3 Configuration of Operating Modes **13**
3.1 Initial Setup 13
3.2 Standalone AP and STA 15
3.2.1 Access Point configuration 16
3.2.2 Station / Client configuration 17
3.2.3 (Optional) Add upstream internet connectivity 18
3.2.4 (Optional) Add upstream internet connectivity via LTE 19
3.3 'Virtual Wire' - Layer 2 bridging 20
3.3.1 Access Point configuration 20
3.3.2 Station / Client configuration 21
3.4 Non-standalone AP with routing 21
3.4.1 Access Point configuration 21
3.4.2 Station configuration 21
3.5 Setting a custom static IP 22
3.6 Reset the device to default configuration 23
3.6.1 Access to web UI is available 23
3.6.2 SSH access is available 23
3.6.3 No network access - EKH01 23
3.6.4 No network access (Option 1) - EKH03 23
3.6.5 No network access (Option 2) - EKH03 23
3.7 Using DPP QR code 24
3.7.1 On the AP 24
3.7.2 On the STA 24
3.7.3 Using the Morse Micro App 25
3.8 Using DPP push button 29

3.9 802.11s Mesh Configuration 31
3.9.1 Mesh STA / Mesh Point configuration 32
3.9.2 Mesh Gate configuration 33
3.9.3 (Optional) Add upstream internet connectivity in Mesh Gate mode 35
3.9.4 Additional 802.11s Mesh settings 35
3.10 EasyMesh 36
3.10.1 Theory of Operation 36
3.10.2 EasyMesh Controller Configuration 36
3.10.3 EasyMesh Agent Configuration 37
3.10.4 Pairing EasyMesh devices 38
3.10.5 EasyMesh Status 39
4 Wavemon and Ping Testing 40
5 Setting up iPerf3 traffic testing 40
5.1 AP configuration 42
5.2 STA configuration 43
5.3 Web user interface 44
6 Range Testing 45
7 Video Streaming 47
7.1 Setting up 48
7.2 Accessing the Video Streams 48
7.3 Configuration 49
7.3.1 Live View 50
8 Page Descriptions 51
8.1 Home 51
8.2 Quick Config 52
8.2.1 Network Interfaces 53
8.2.2 Wireless 53
8.3 Statistics > Morse 55
8.4 Status > Realtime Graphs > Wireless 55
8.5 Services > Terminal 56
8.6 System > Backup / Flash Firmware 56
9 Additional Configuration Parameters 57
9.1 Disable AMPDU 57
9.1.1 Via UI 57
9.1.2 Via CLI 58
9.2 Fragmentation Threshold 58
9.2.1 Via UI 58
9.2.2 Via CLI 58

9.3 Unified Scaling Factor / Unscaled Interval 59
9.3.1 Via UI 59
9.3.2 Via CLI 59
9.4 DTIM Interval 60
9.4.1 Via UI 60
9.5 Beacon Interval 61
9.5.1 Via UI 61
9.6 BSS Color 62
9.6.1 Via UI 62
9.6.2 Via CLI 62
9.7 Other HaLow settings 63
9.8 morse_cli 63
9.9 Thin LMAC 64
9.9.1 Via UI 64
9.9.2 Via CLI 64
10 UI Configuration Architecture 66
11 Troubleshooting 68
11.1 Updating firmware 68
12 Revision History 69

1 Overview

Thank you for choosing to evaluate Morse Micro 802.11ah HaLow for use in your application. This guide will get you started using the kit and evaluating the 802.11ah technology. It is primarily intended for users of the web UI but will mention other configuration methods for reference.

The Morse Micro web UI provides a graphical interface for viewing and modifying device configurations, particularly the operating mode and HaLow radio parameters. The interface is available on EKH01 and EKH03 evaluation kits and is based on OpenWrt's standard LuCI interface.

Section 2 of this document provides a brief description on how to set up the hardware and outlines the basic scenarios that might be used for evaluation. Section 3 explains how to configure a system for the first time using the Morse Micro web UI. Sections 4 and 5 describe how to test the performance of Wi-Fi HaLow using Wavemon and iPerf3. Section 8 outlines some of the available UI screens and tools, while Section 9 provides advanced configuration tips that are not usually required but may be useful in some situations. Section 10 explains the configuration architecture, including how UI configuration propagates through the system to effect changes. Section 11 provides some troubleshooting advice for common problems.

Throughout this document, references to 'AP' imply a Wi-Fi Access Point and references to 'STA' imply a Wi-Fi station.

2 Device Setup

A brief description of the hardware and browser set-up is included below for configuration via the web UI, along with a description of the standard test setup scenarios.

2.1 EKH01

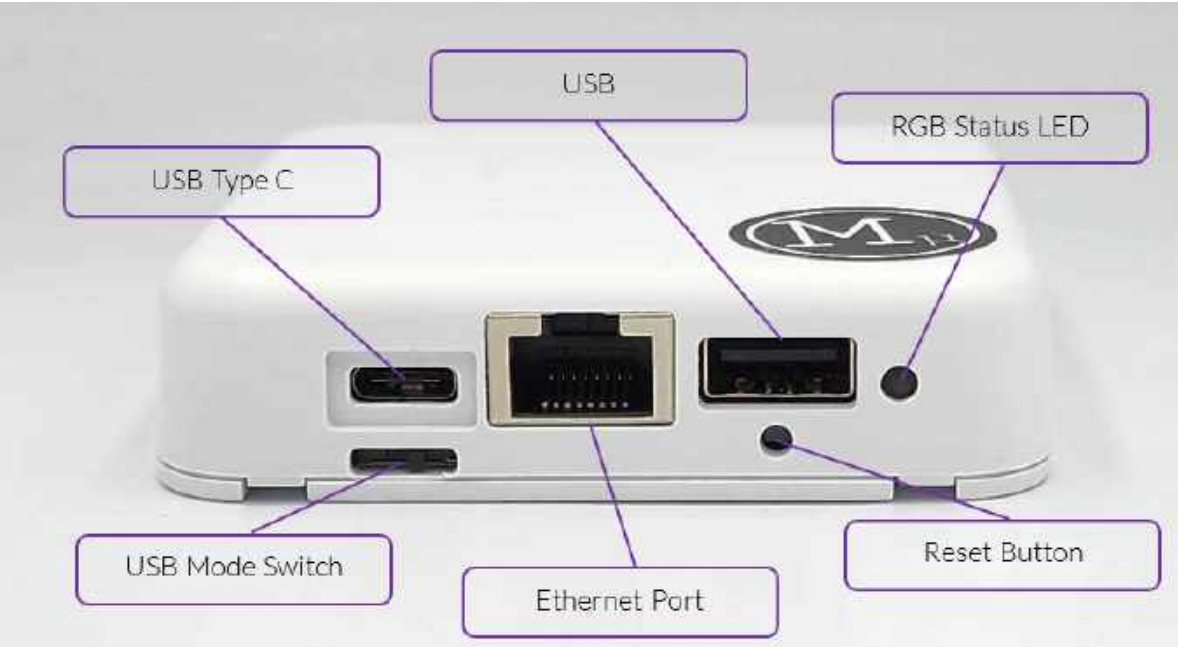
- **microSD card** - this contains the device firmware.
- **Status LEDs** - the red LED indicates power, and the green LED indicates HaLow network activity.
- **USB Type-C** - USB-C port for supplying power to the EKH01. The kit includes an AC adapter that converts mains power to 5V for the EKH01 via the USB-C connector.
- **Micro HDMI** - Micro HDMI display outputs for EKH01, only used for debugging.
- **Headphone Jack** - not typically used.

- **USB Ports** - USB-A ports for connecting peripherals and USB to serial adapter. Any of these ports can be used for serial console access, but note the cable must be plugged in at boot time to be detected. The serial console operates at 115,200 bps 8N1 by default.
- **Ethernet** - Ethernet port for either a LAN connection (e.g. a laptop) or an upstream WAN connection (e.g. gateway router).
- **(Optional) Camera** - the device may include a camera depending on the kit version ordered.

2.1.1 Basic setup

1. Connect the antenna to the HaLow antenna connector on top of the unit.
2. Optional - connect an RJ45 Ethernet cable to the Ethernet port if required.
3. Optional - connect a USB-serial cable to any of the USB ports if required for debugging. This is not usually required.
4. Once power is supplied, it should take the device around 60 seconds to boot up and be operational.

2.2 EKH03



- **USB Type-C** powers the board and can function as an Ethernet-to-USB adapter if the USB mode switch is in the leftmost position.
- **USB** can be used for connecting peripheral devices to the EKH03 and provides a UART interface which can be accessed via a 3.3V TTL serial USB cable. For advanced users, UART access is also available through header pins on the internal PCB.
- **RGB Status LED** is a multi-color LED that is used to indicate the status of the device (see Basic setup for details).
- **USB Mode Switch** selects whether to use the USB-C or Ethernet port for the LAN connection. The direction of the switch determines which port is selected (*left* - USB-C for Ethernet, *right* - Ethernet port for Ethernet).
- **Ethernet Port** for either a LAN connection (e.g. a laptop) or an upstream WAN connection (e.g. gateway router).
- **Reset button** can be used to reset the device. Pressing and holding the button for 5 seconds (until flashing green) will reboot the device. Holding for more than 10 seconds (until flashing yellow) will trigger a full factory reset of the device, returning it to the default configuration. This button is also used for DPP push button connections. For more details, see sections 3.6and 3.8.
- **2.4 GHz Wi-Fi** provides an access point which is brought up on the EKH03 by default. It is also automatically bridged to the Ethernet interface.

2.2.1 Basic setup

1. Connect the provided antenna to the HaLow Antenna Connector shown.
2. Plug the power adapter into the USB-C connector on the EKH03. The included USB-C to USB-A cable can also connect the EKH03 to a power source, such as a laptop or phone charger (via the USB-C connector).
3. Once the device is powered, the RGB LED will display the status of the device (see table).

Status	LED Color (behaviour)	Graphical Example
Booting stage 1 (bootloader)	Yellow (solid)	
Booting stage 2 (linux)	Green (flash 1.5 per sec)	
Fully booted	Green (solid)	
DPP running	Purple (flash 1 per sec)	
DPP failed (remains for 5 secs)	Purple (flash 5 per sec)	
Fully booted and HaLow connected	Purple (solid, flash activity)	
Error	Red (flash 10 per sec)	
Rebooting	Green (flash 1.5 per sec)	
Upgrading	Blue (flash 1.5 per sec)	
Factory resetting	Yellow (flash 5 per sec)	

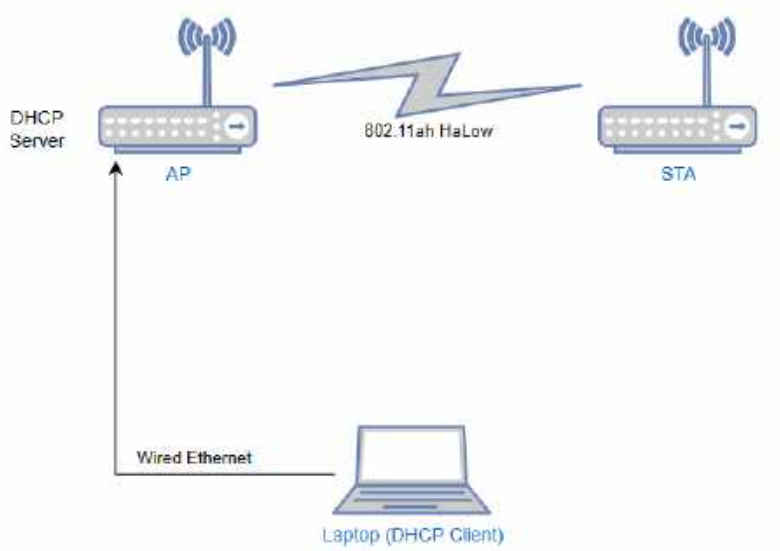
2.3 Browser support

The web UI has been tested and verified to work with up to date releases of the following browsers:

- Google Chrome
- Firefox
- Microsoft Edge
- Apple Safari

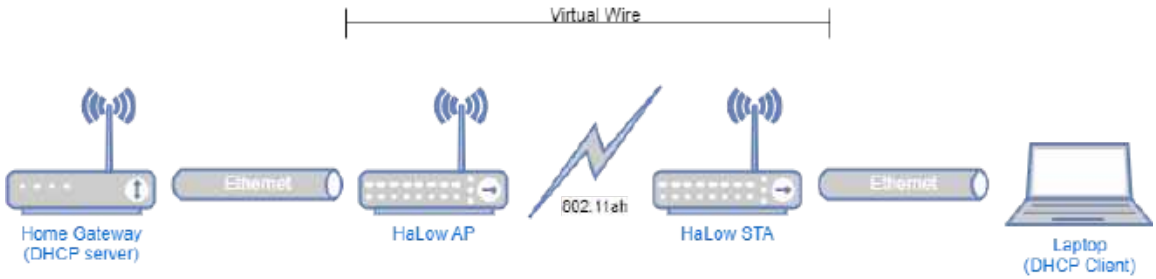
2.4 Standard setup scenarios

2.4.1 Standalone Access Point with client devices



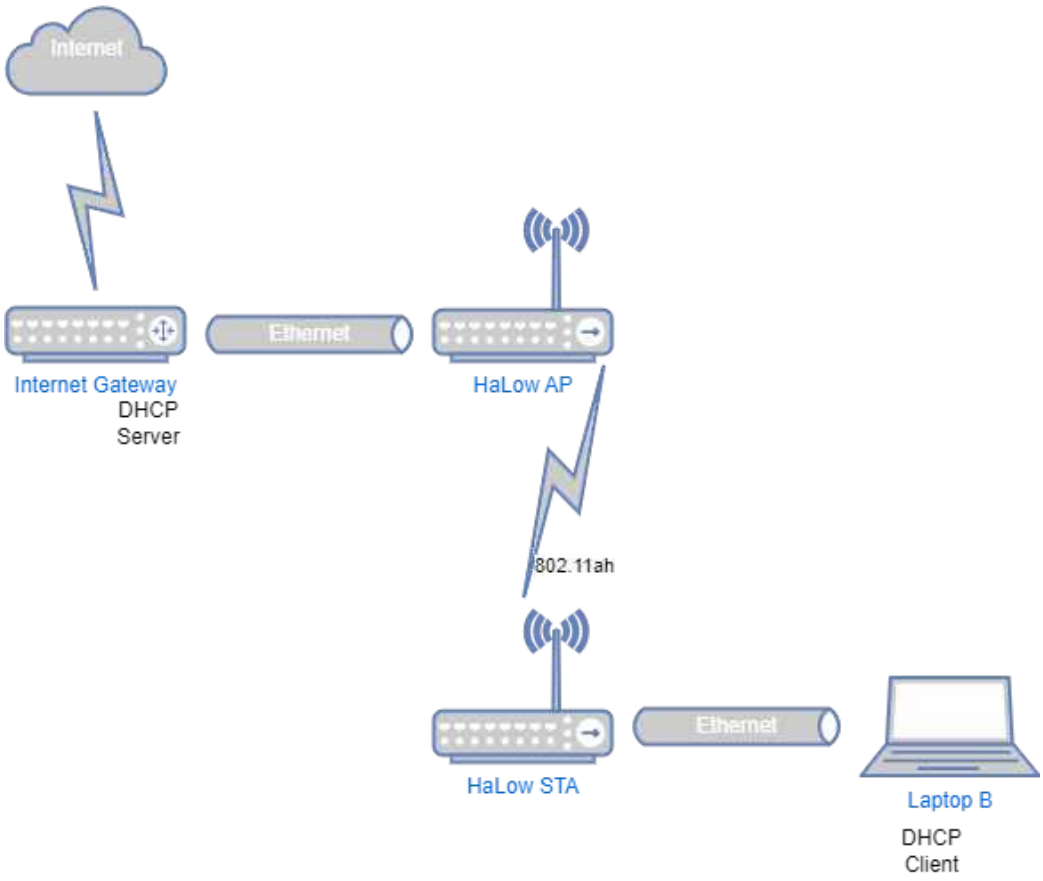
This configuration is typically used for standalone testing of a HaLow connection. It is useful in closed network scenarios where connected devices do not require access to external networks. The key here is that the traffic will only go between the AP and STA and is completely isolated from any external networks. If you're unsure which setup to use, start with this one.

2.4.2 Using HaLow as a 'virtual wire' (Layer 2 bridge)



In this configuration HaLow is transparent to the rest of the devices in the network. The HaLow link is used as a means of providing a 'virtual' Ethernet connection between two points where it may not be practical to run a physical cable. This scenario is useful as a simple way to test HaLow with real-world traffic by introducing it into an existing network without having to adjust the configuration of the non-HaLow devices.

2.4.3 Non-standalone Access Point with routing



This scenario is a more complicated version of the one above, where rather than using bridging to simplify the setup, each device is a router with its own DHCP server and local network. This allows for a more complex network configuration, but is more difficult to set up. It is also robust in that if the HaLow links goes down, the station will still have an IP address and the web UI will be reachable.

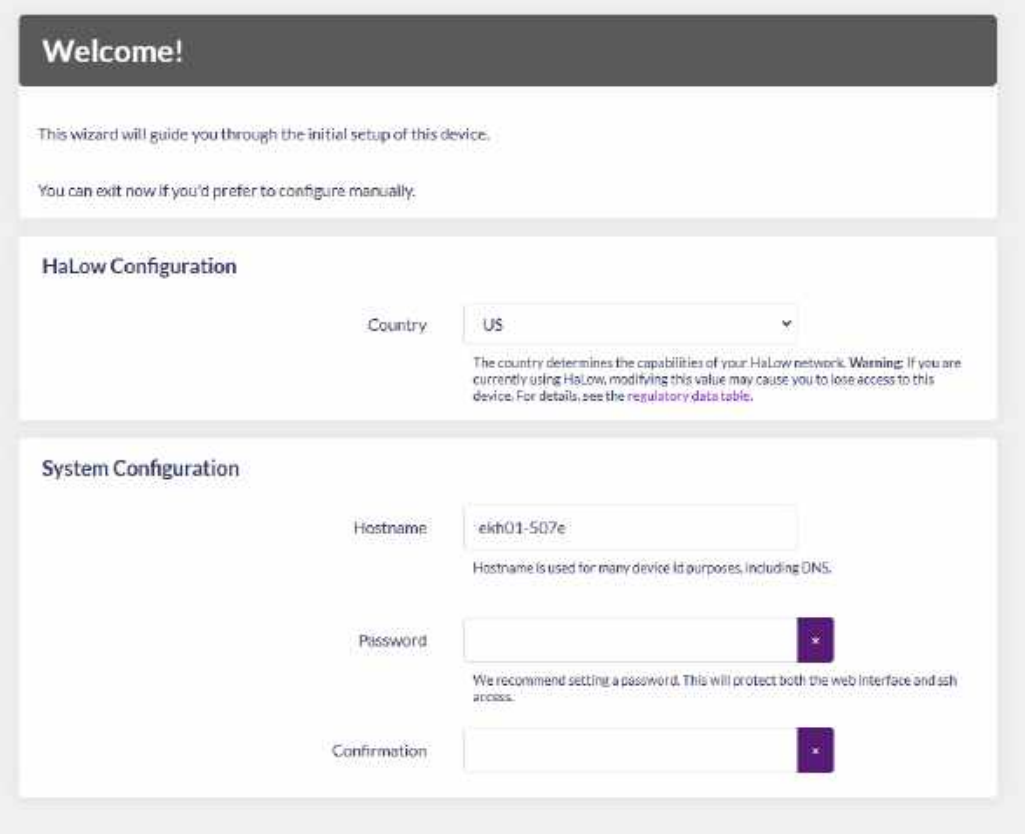
This scenario is useful for evaluating the HaLow device's ability to handle traffic flows at Layer 3, but places more load on the CPU. Unless you have a specific reason to use this approach, bridging is a simpler alternative.

3 Configuration of Operating Modes

Evaluation kits are dispatched in a default configuration, and this guide assumes the devices will be used starting in that state. If the kits have been used previously you may need to reset them to their default state before following the steps below. See Section 3.6 for instructions on how to reset devices to the default configuration.

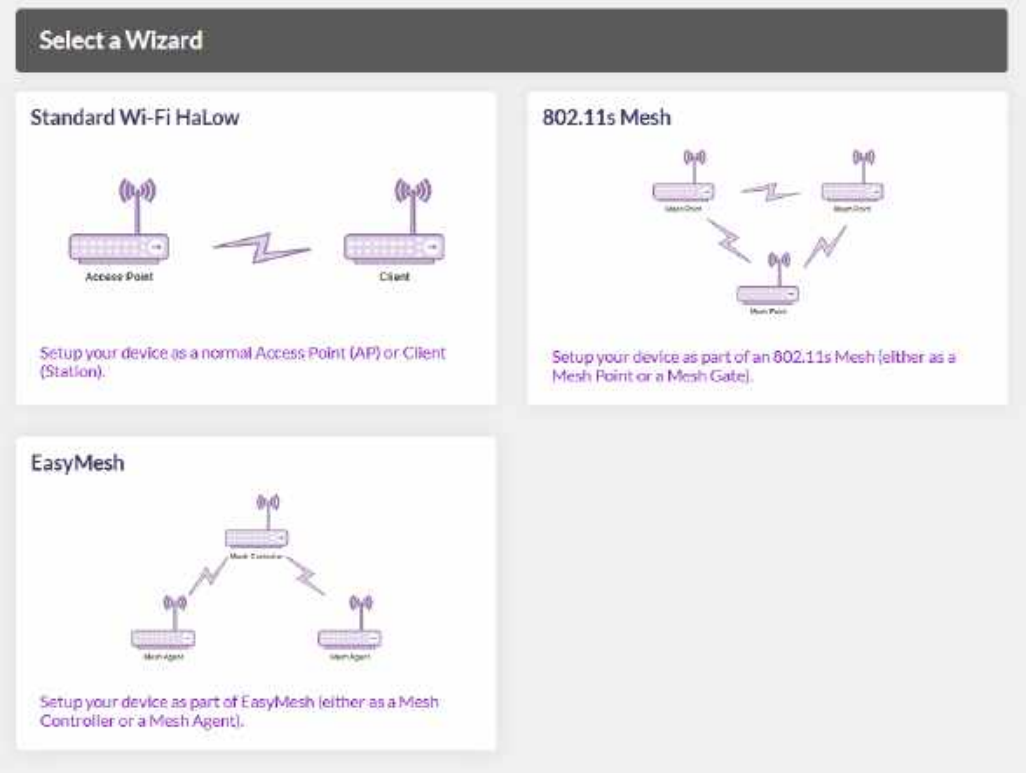
Since the 2.3.x release of OpenWrt a configuration wizard has been included in the UI to aid with quick setup of devices. This guide now focuses on using the configuration wizard, but it is also possible to use the standard configuration pages in the UI to set up the device.

3.1 Initial Setup



1. Connect your laptop to the Morse Micro HaLow device via an Ethernet cable.
2. Ensure that the Ethernet interface on the laptop is configured as a DHCP client (this is usually default, so often no change is required).
3. Open a web browser and go to the following address: http://10.42.0.1
4. Select the **Country** (for regulatory requirements) and optionally a unique **Hostname** for the device and a **Password** (which secures SSH and web access):
5. Click **Apply** in the bottom right.

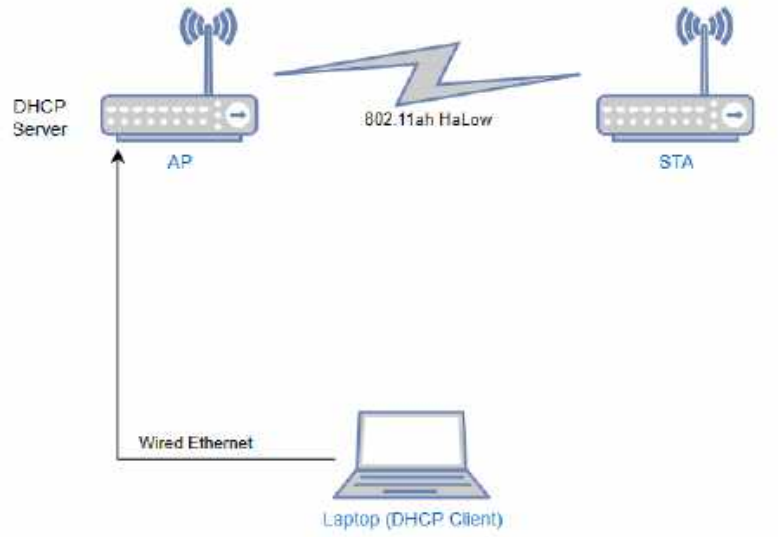
The next screen will present an option to configure the device either as a standalone AP/STA or as part of a mesh network using 802.11s mesh or EasyMesh. For first time users, the Standard Wi-Fi HaLow wizard is the best option to start with. Mesh configurations allow multiple APs to be linked in order to provide an even wider coverage area.



The following sections assume that the Standard Wi-Fi HaLow wizard has been selected.

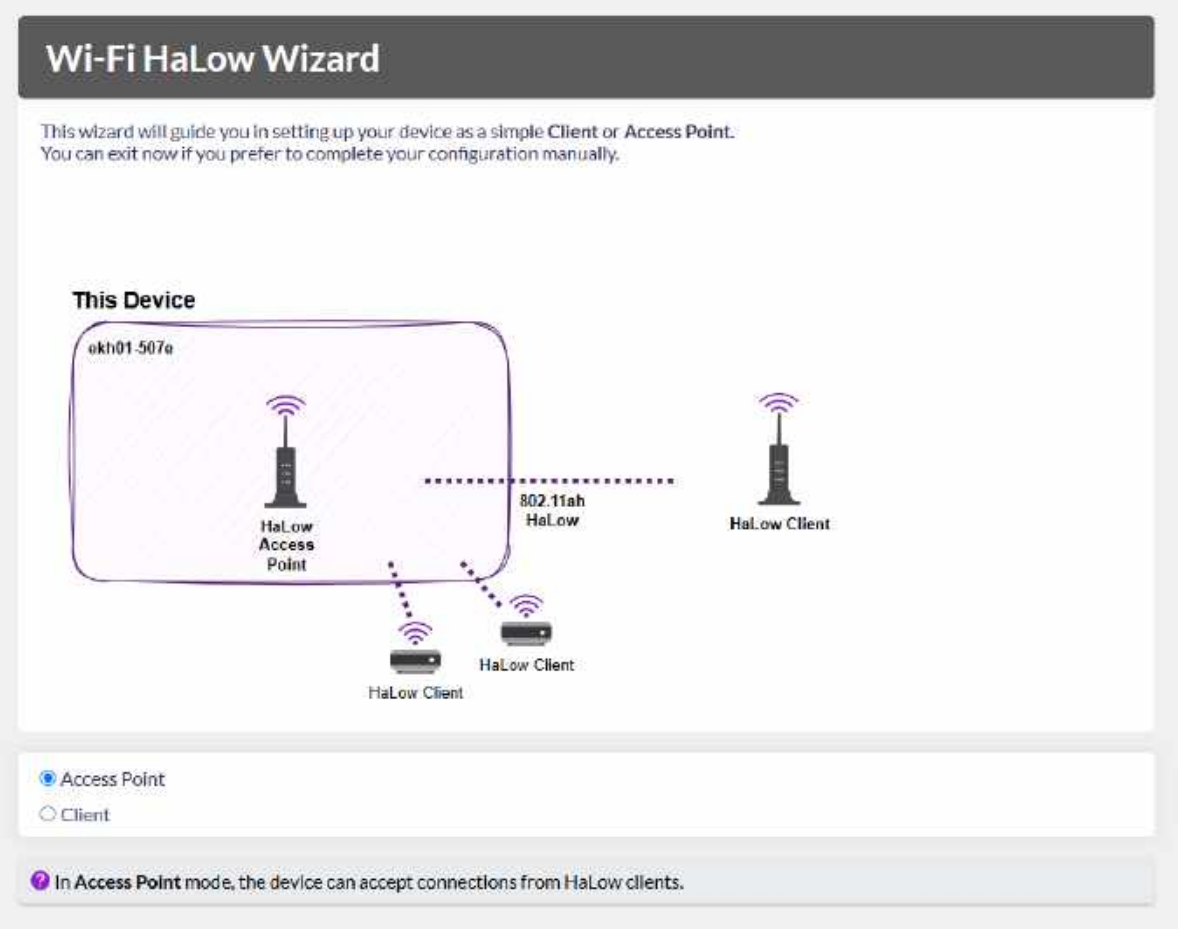
3.2 Standalone AP and STA

This section outlines how to configure the AP and STA per the scenario defined in 2.4.1.



3.2.1 Access Point configuration

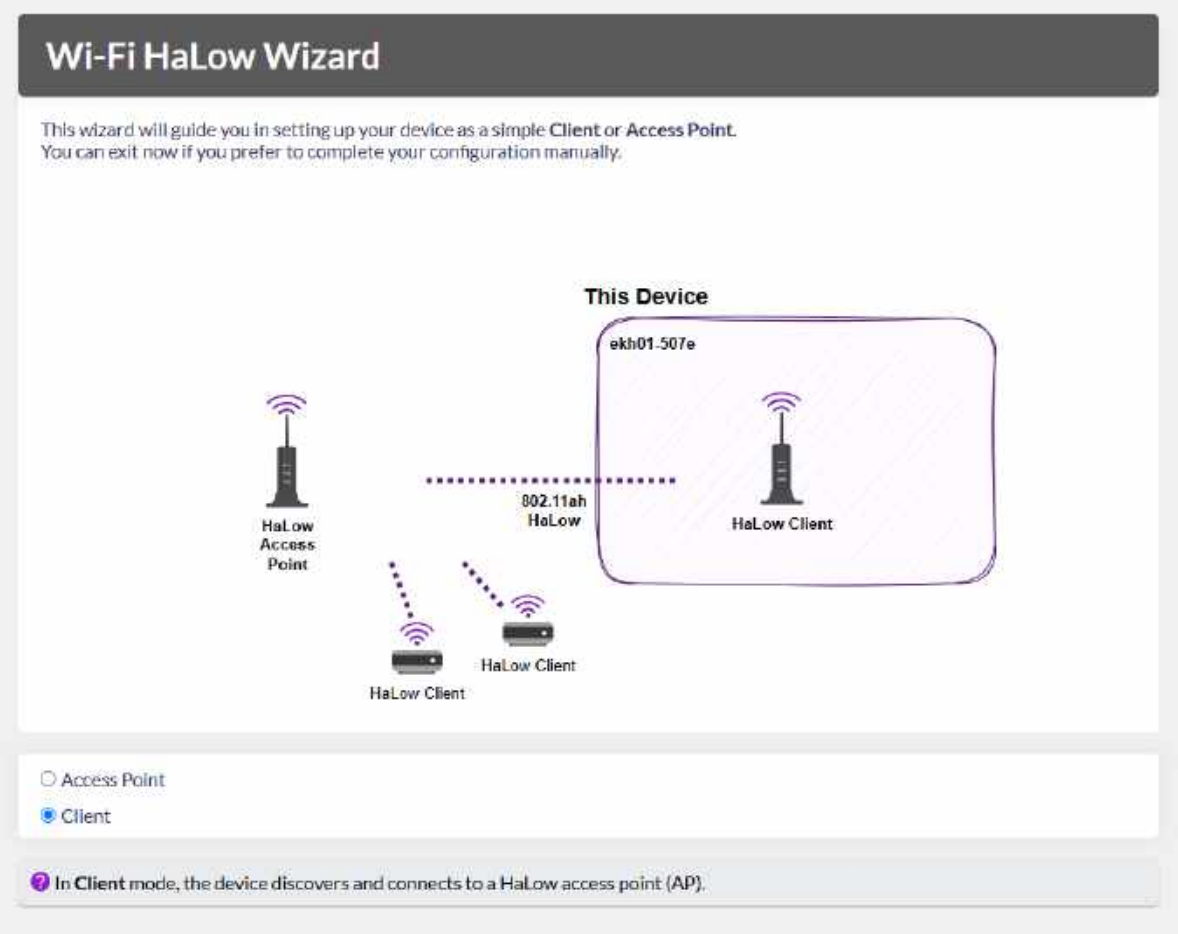
1. Follow the steps in 3.1 to connect to the device at http://10.42.0.1 and set the region.
2. For **Mode** selection, choose 'Access Point':



3. Click the **Next** button at the bottom right to go to the next page.
4. On the following pages:
    a. **Setup HaLow Network - AP** has a default SSID and passphrase which you can change if you wish. The Width and Channel options can be left as default. Then click **Next**.
    b. Upstream **Network** should be set to 'None'. Click **Next**.
5. You can then **Apply** your configuration on the final page.

3.2.2 Station / Client configuration

1. Disconnect your laptop from the Ethernet interface of your AP (from Section 3.2.1 above) to prevent IP address conflicts with the client.
2. Follow the steps in Section 3.1 to connect to the device and set the region.
3. For the **Mode** selection, choose 'Client' and click **Next**.



4. On the **Connect to a HaLow Network** page, choose 'Manual credentials' and then **Scan** to find the SSID you entered for your AP. Enter the previously set passphrase and click **Next.**
5. For the **Traffic Mode**, select 'Bridge' and click **Next**.
6. If your device has 2.4 GHz capability, you will be presented with an **Enable Access Point** toggle which you can switch off if standard Wi-Fi access is not needed. Click **Next.**
7. Once you have saved the configuration by clicking **Apply**, you should disconnect your laptop from the Station and reconnect it to the AP. You can find the Station's HaLow IP in the **DHCP Leases** card on the **Home** page of the AP web UI.

3.2.3 (Optional) Add upstream internet connectivity

In many situations it is helpful to have an upstream connection to the internet. The following instructions outline how to connect your AP to an upstream gateway which can provide internet access to the HaLow devices.

It assumed that the upstream gateway provides the following:

- a DHCP server to allocate an address to your AP.
- a DNS server, provided via a DHCP offer.
- a gateway address, assigned via a DHCP offer.

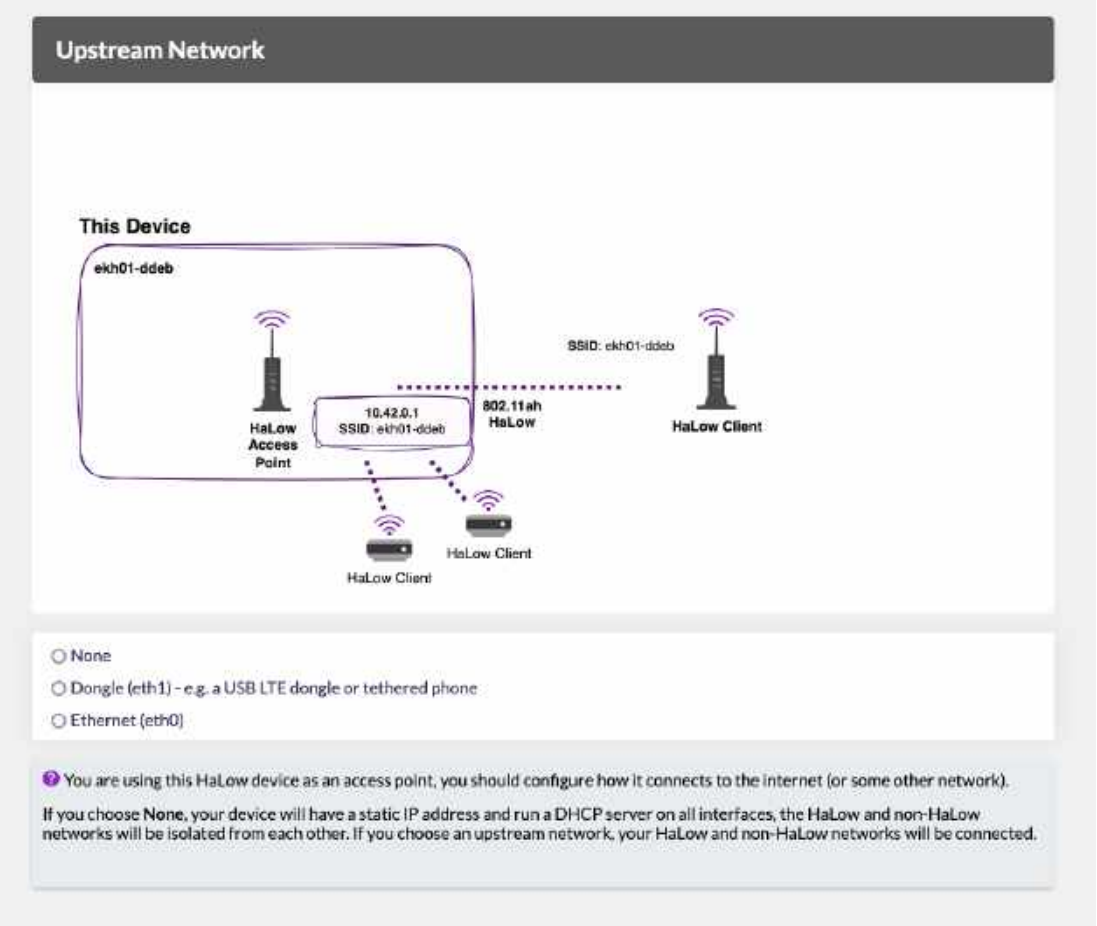
The steps are as follows:

1. Connect a laptop to your HaLow device as described in Section 3.1 and navigate to the admin interface (usually http://10.42.0.1).
2. If the wizard does not come up because you've already configured your device, go to **Wizards** in the side menu.
3. On the **Upstream Network** page, choose 'Ethernet', and set the **Traffic Mode** to 'Router'.
4. **Apply** the configuration on the final page.
5. Use an Ethernet cable to connect your AP to the existing network.
6. To access the device's admin interface again, you can access 192.168.12.1 over the HaLow link or you will need to determine the address allocated by your network's DHCP server. See section 3.6 for how to reset your device if you lose access.

3.2.4 (Optional) Add upstream internet connectivity via LTE

Using an LTE dongle for upstream internet connectivity is also supported (instead of via the Ethernet port). An LTE dongle will be automatically discovered and shown as another option available in the **Upstream Network** page. Follow the steps from Section 3.2.3, but choose 'Dongle' when selecting the upstream network to use (step 3).

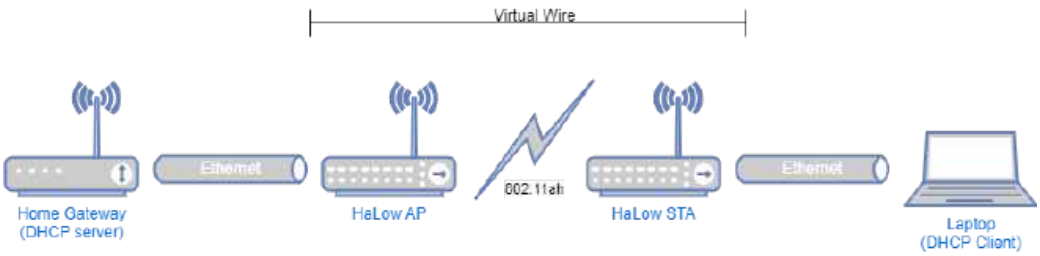
Connectivity via the LTE dongle behaves the same as Ethernet.



Note: Only dongles that do not require a specific driver are supported (such as via CDC/RNDIS).

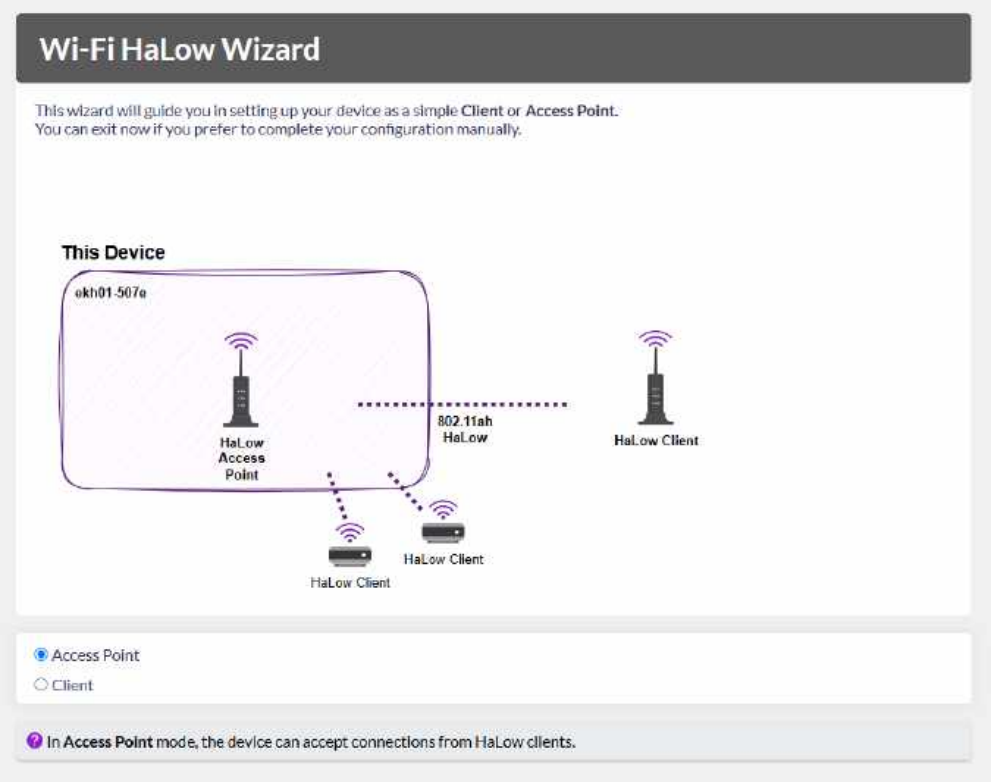
3.3 'Virtual Wire' - Layer 2 bridging

The following outlines how to configure the AP and STA per the scenario defined in 2.4.2.



3.3.1 Access Point configuration

1. Follow the steps in 3.1 to connect to the device (http://10.42.0.1) and set the region.
2. For **Mode** selection, choose 'Access Point':



3. Click the **Next** button at the bottom right to go to the next page.
4. On the following pages:
    a. **Setup HaLow Network - AP** has a default SSID and passphrase which you can change if you wish. The Width and Channel options can be left as default. Then click **Next**.

b. **Upstream Network** should be 'Ethernet'. Selecting Ethernet will show a new option for **Traffic Mode** which should set to 'Bridge'. Click **Next**.

5. You can then **Apply** your configuration on the final page.

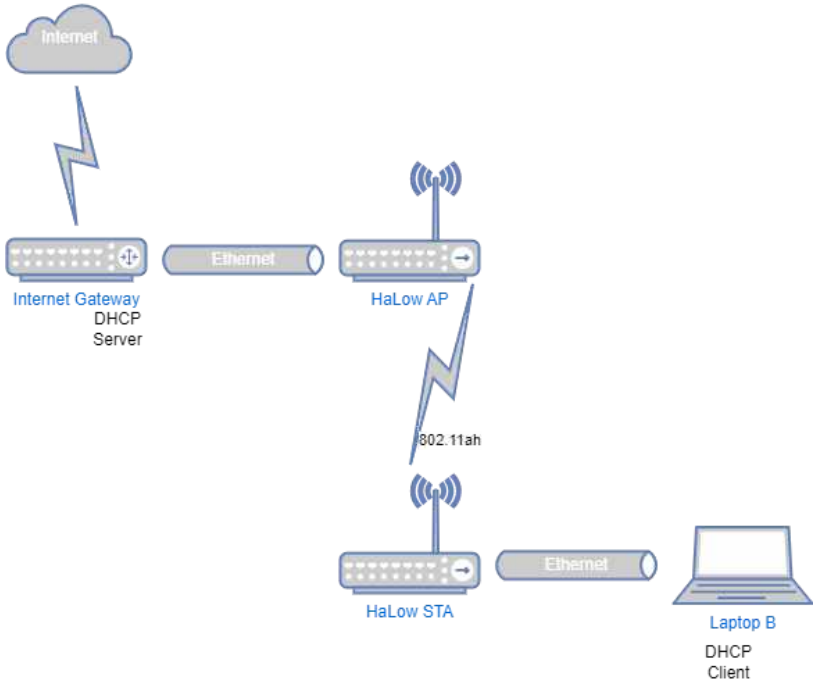
To access the device's admin interface again, you will need to check the IP address allocated by your network's DHCP server. See section 3.6 for how to reset your device if you lose access.

3.3.2 Station / Client configuration

Follow the instructions in 3.2.2. Once you've saved your configuration, however, your station's IP address will be allocated by your network's DHCP server and will be accessible on that network.

3.4 Non-standalone AP with routing

This section outlines how to configure the AP and STA per the scenario defined in 2.4.3.



3.4.1 Access Point configuration

Follow 3.2.1 and 3.2.3 to configure an Access Point with **Uplink** set to 'Ethernet' and **Device Mode** set to 'Router'.

3.4.2 Station configuration

Follow the STA configuration for the scenario in 3.1, but for **Device Mode** choose 'Extender'.

3.5 Setting a custom static IP

By default, devices configured as an AP are reached via 10.42.0.1 on the Ethernet interface and 192.168.12.1 on the HaLow interface. If the two interfaces are bridged together, they will both use the same 192.168.12.x/24 subnet and the device will be reached on 192.168.12.1 via both interfaces.

In simple topologies this default setup is often sufficient, however in setups with multiple APs it can become necessary to configure custom static addresses to ensure each device has a unique IP address. Static IP addresses can also be useful to ensure that devices configured as STAs always are reachable at the same address, particularly when many similar STAs are on a given HaLow network. DHCP, which is the default on Ethernet and HaLow interfaces, will assign different addresses to STAs each time otherwise.

To configure a static IP address on either the Ethernet or HaLow interface, browse in the UI to the **Quick Config** option in the side menu.

3.6 Reset the device to default configuration

This section outlines how to get the device back to a default configuration in different situations. All firmware releases use SquashFS with an overlay which allows for full factory resets.

3.6.1 Access to web UI is available

In this scenario, you can login to the device and go to the 'System > Backup/Flash Firmware' page. Selecting 'Reset to defaults' will reset the device's configuration and reboot.

3.6.2 SSH access is available

In this scenario, you can login to the device via ssh (`ssh root@<ipaddress>`) and run the following command at the prompt:

```
firstboot -y && reboot
```

3.6.3 No network access - EKH01

This scenario can occur when the IP address of the device has been changed, and it is not obvious what the address is. The quickest method here is to remove the SD card and write a new firmware image to it using a tool such as Balena Etcher.

3.6.4 No network access (Option 1) - EKH03

This scenario can occur when the IP address of the device has been changed, and the user is unable to identify it via the lease list on their DHCP server. Using a suitable object, press and hold the reset button, shown in Section 2.3 for more than 10 seconds to reset the device to factory defaults. It will first start flashing slowly green (for a normal reset) after 5 seconds, then after 10 seconds will quickly flash yellow. Release the button once it's flashing yellow.

3.6.5 No network access (Option 2) - EKH03

This scenario requires using a serial console cable to access the device. Section 2.2 of this guide shows the location of the USB port on the EKH03 where a 3.3V TTL serial USB cable can be used to connect a computer to this port. Once connected, a suitable terminal emulator program will be needed to connect to it, such as PuTTY in Windows or picocom in Linux.

Once connected to the serial console, run the following command to reset the configuration:

```
firstboot -y && reboot
```

3.7 Using DPP QR code

Device provisioning protocol (DPP) provides a simple process to onboard stations into an existing wireless network. Station devices are provisioned by scanning a QR code with a "configurator" device already associated with the network.

3.7.1 On the AP

No explicit action is required to enable DPP in AP mode. Simply set your device to work as an AP with SAE security.

Note that if you are using 802.11s mesh, this does not by default include AP functionality, and the hostapd process will not be started. The hostapd process is required for DPP to function. It is possible to run 802.11s Mesh with an AP, this mode is known as a 'Mesh Gate' - see Section 3.9.2 for details.

The credentials for the AP DPP configurator are set in `/etc/dppd/auth_secrets.txt`, you will be asked for these in the mobile app after selecting the AP to provision a device to. The default username is **morse** and the default password is **HaLow**.

3.7.2 On the STA

To enable DPP through the web UI, after setting your Device as a client via the wizard, set DPP in the page where it asks for credentials to connect to a HaLow network and proceed to the last page of the wizard where the QR code is shown.

Alternatively, you can also view the QR code from the **Home** page, on the HaLow **Uplink** card.

To start provisioning, use the Morse Micro DPP app on the phone to scan the QR code.

Note: The DPP QR code is not persistent on EKH01 devices and will change if updating the image without using the 'Keep settings and retain current configuration' option or if updating the image on the microSD card using a computer.

After a successful provision, SSID, key, and encryption will be set automatically.

3.7.3 Using the Morse Micro App

Note: In order to use the Morse Micro App, you will need to connect a compatible HaLow AP to the same network as your phone. For example, you can connect via the EKH03 2.4 GHz AP.

To prepare a phone to act as a configurator - a device which scans and sends provisioning information to the AP - follow the steps below.

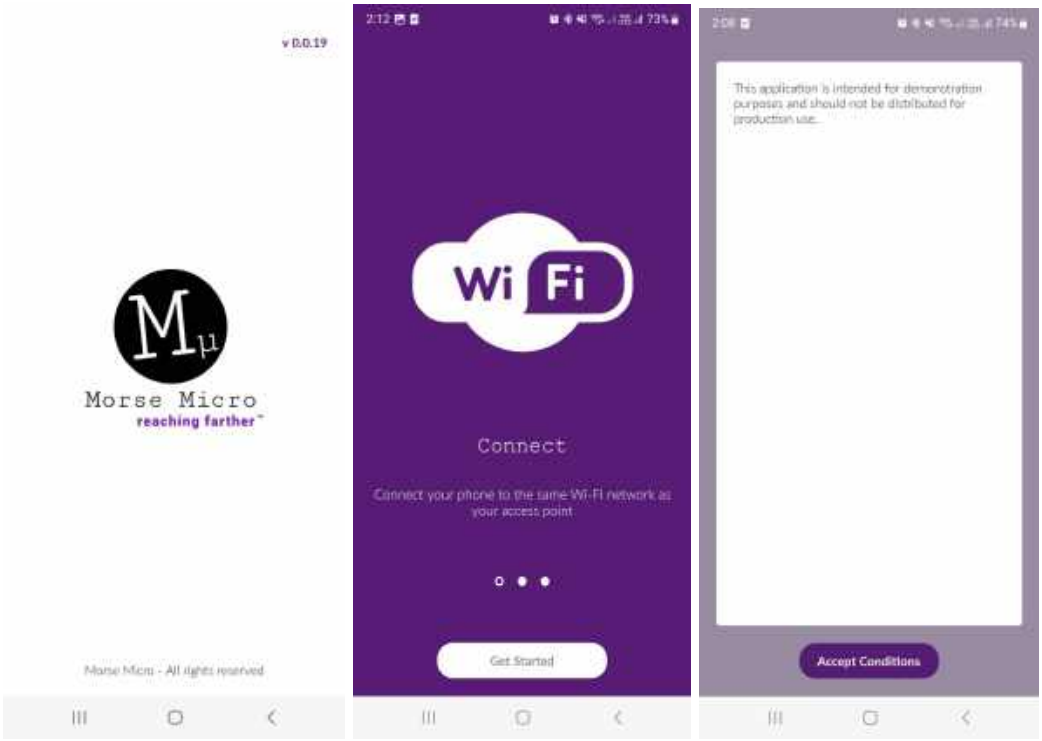
To download the Morse Micro DPP application for:

Apple iOS (needs authorization):
https://testflight.apple.com/join/LnXpFMPj

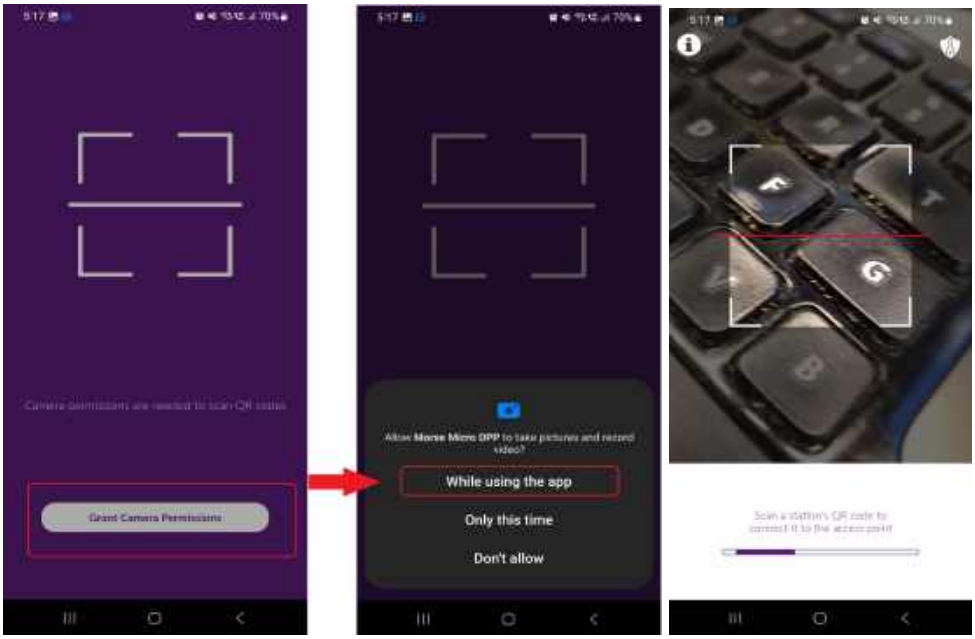
Android, use the link below:
https://app.bitrise.io/app/26fcf521506b532d/build/fb927766-2eaa-425f-a2b2-19f1342b432d/artifact/ce4e33d57257f294/p/bd9fd36d28dc80f5edef30ade4899720

or scan this QR code with your phone:

After the app is installed, open the app - if it is the first time running the app you will see a welcome/tutorial screen otherwise it will go straight to the 'Accept Conditions' screen. Click 'Get Started' if needed, and then 'Accept Conditions' to begin using the app.



When prompted, grant the application access to your camera, so it can read QR codes.

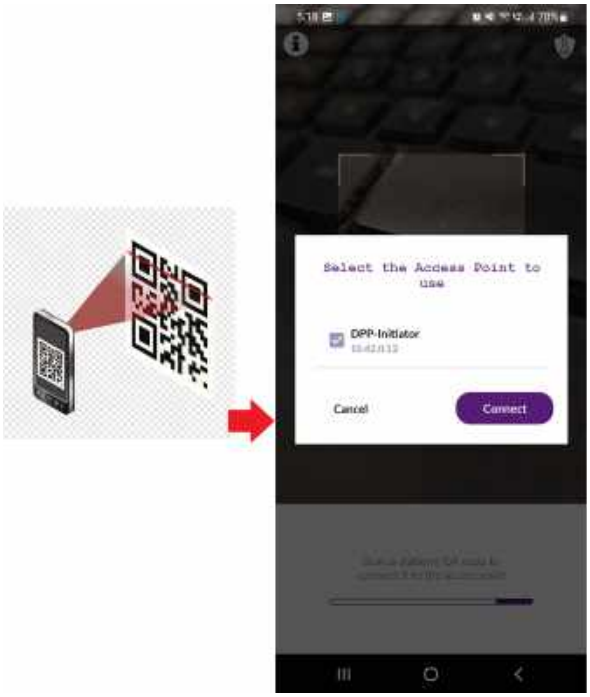


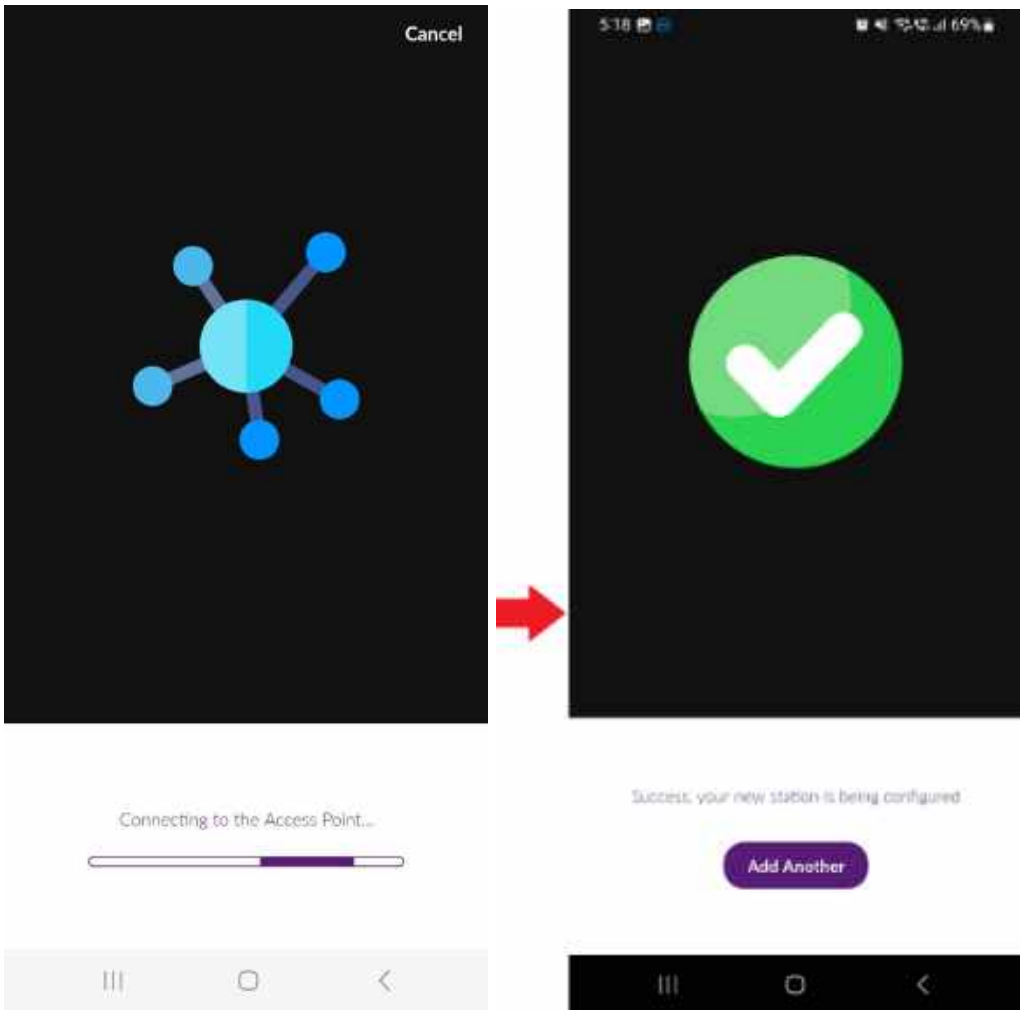
When you see the screen on the right (above), your app is ready to capture a QR code from the device to be provisioned.

Before capturing a QR code, set up the credentials for accessing the AP by clicking the icon in the top right corner that looks like a key on a shield. You will need to enter the username and password of the DPP server on the AP.

The current default username is **morse** and the password is **HaLow**.

Point the camera at the QR code to scan it. When you scan a station's QR code, the app will show you a dialog with a list of available DPP servers on your network. Select the desired AP and tap on **Connect**.



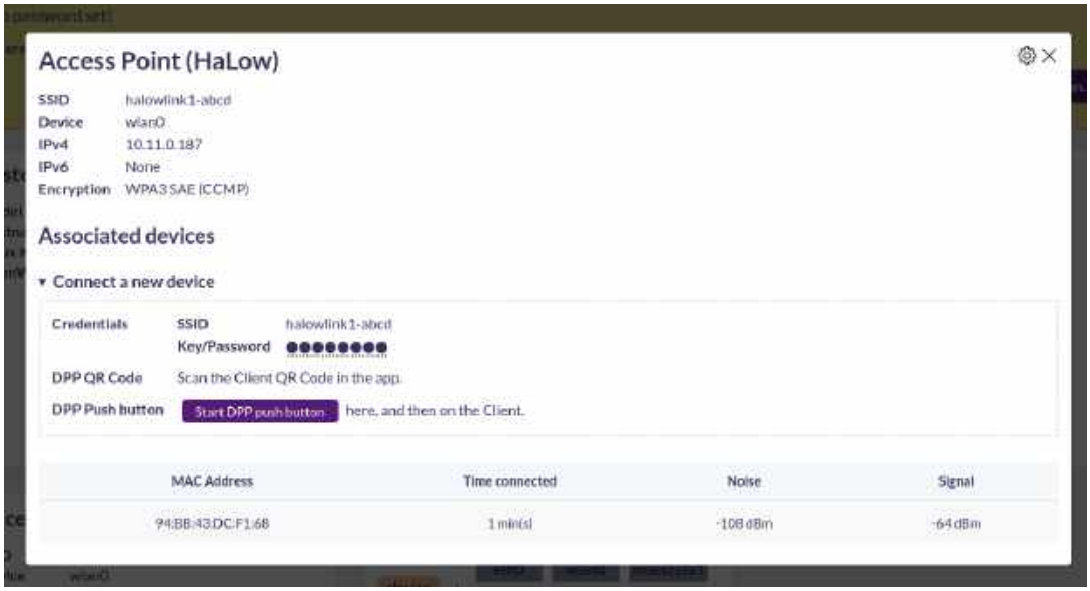


At the end the confirmation screen will be shown. To provision additional devices, click on “Add Another” to go back to the QR scanner .

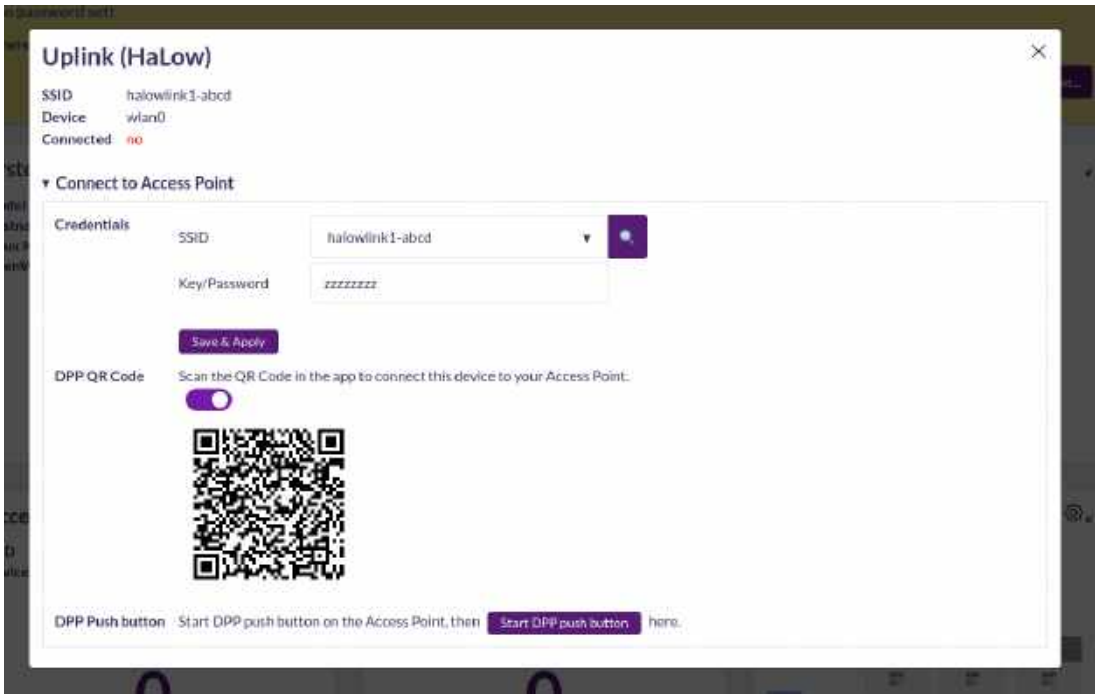
Note: Once this process is completed, it means the device has been provisioned but not necessarily connected yet. Check the station list on the AP to verify the device has connected.

3.8 Using DPP push button

To utilize DPP (Device Provisioning Protocol) using the push button, simply set your device as an Access Point or Station and save the configurations. Then expand the **Access Point (HaLow)** card on the **Home** page of the Access Point and click on the 'Start DPP Push button'.



Simultaneously on the Station, expand the **Uplink (HaLow)** card on the **Home** page and click **Start DPP Push button**.

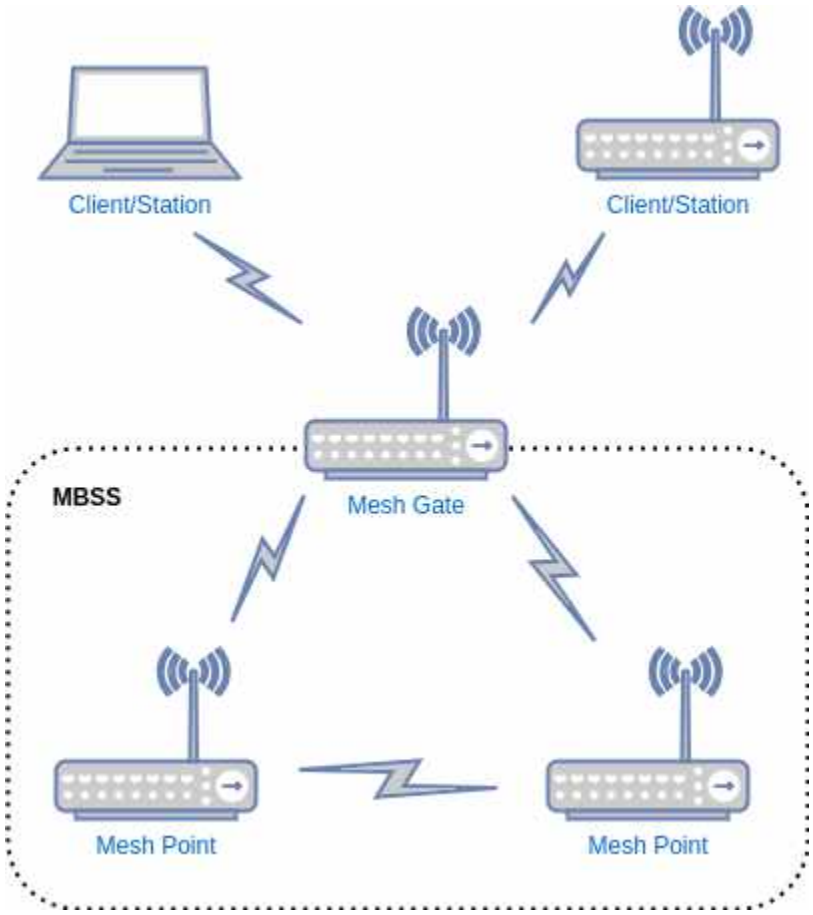


Upon successful completion of the DPP process the Station connection status will change to *yes*.

On the EKH03 the physical 'reset' button on the device can also be used for DPP. Pushing the button for less than 2 seconds will start the DPP push button process, if the device has been configured as an Access Point or Station. The RGB status LED will indicate that the DPP push button process is running, see the EKH03 setup section for details.

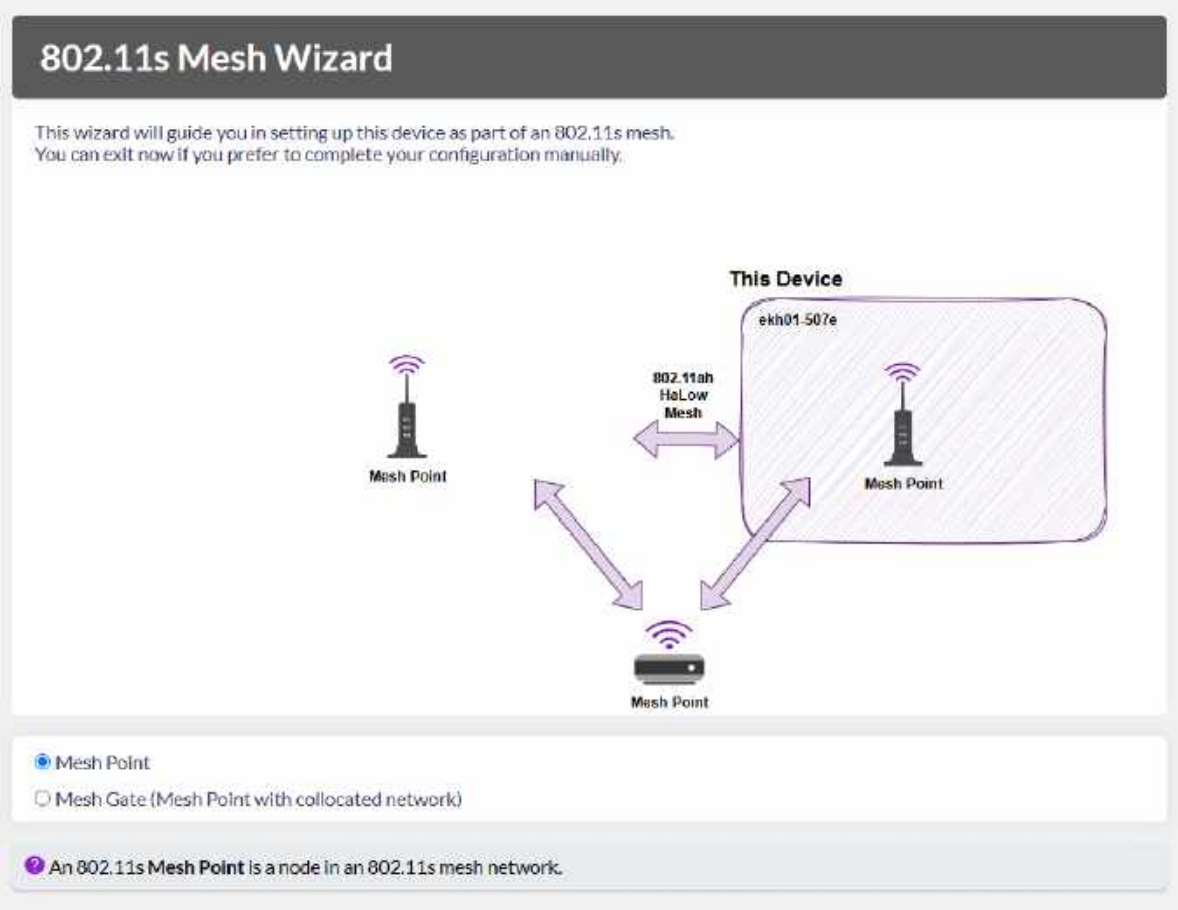
3.9 802.11s Mesh Configuration

802.11s mesh networks aim to increase coverage and range by establishing peer-to-peer links between the various neighbor mesh STAs in the mesh topology. Only mesh capable devices can join the mesh BSS (MBSS) or make use of the mesh functionality provided by the MBSS. Interaction with non-mesh capable devices is handled via mesh gateways (potentially co-located with a non-mesh AP).



3.9.1 Mesh STA / Mesh Point configuration

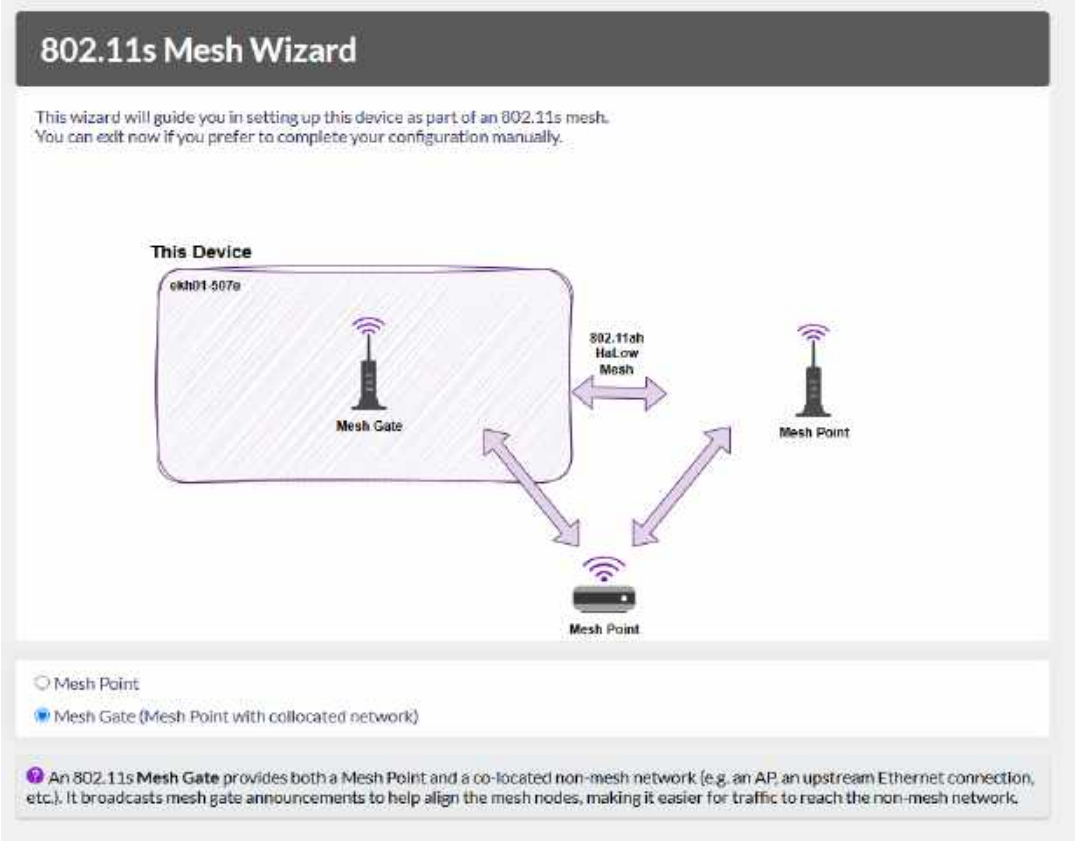
1. As a prerequisite, ensure that your device is configured with the appropriate region and a channel. Refer to steps in 3.1 to connect to the device and set the region.
2. Once you decide to configure your device as a Mesh Point, navigate to the **Wizards** config in the side menu and select **802.11s Mesh Wizard.**
3. As a first step, choose 'Mesh Point' as the mode and then click **Next**.



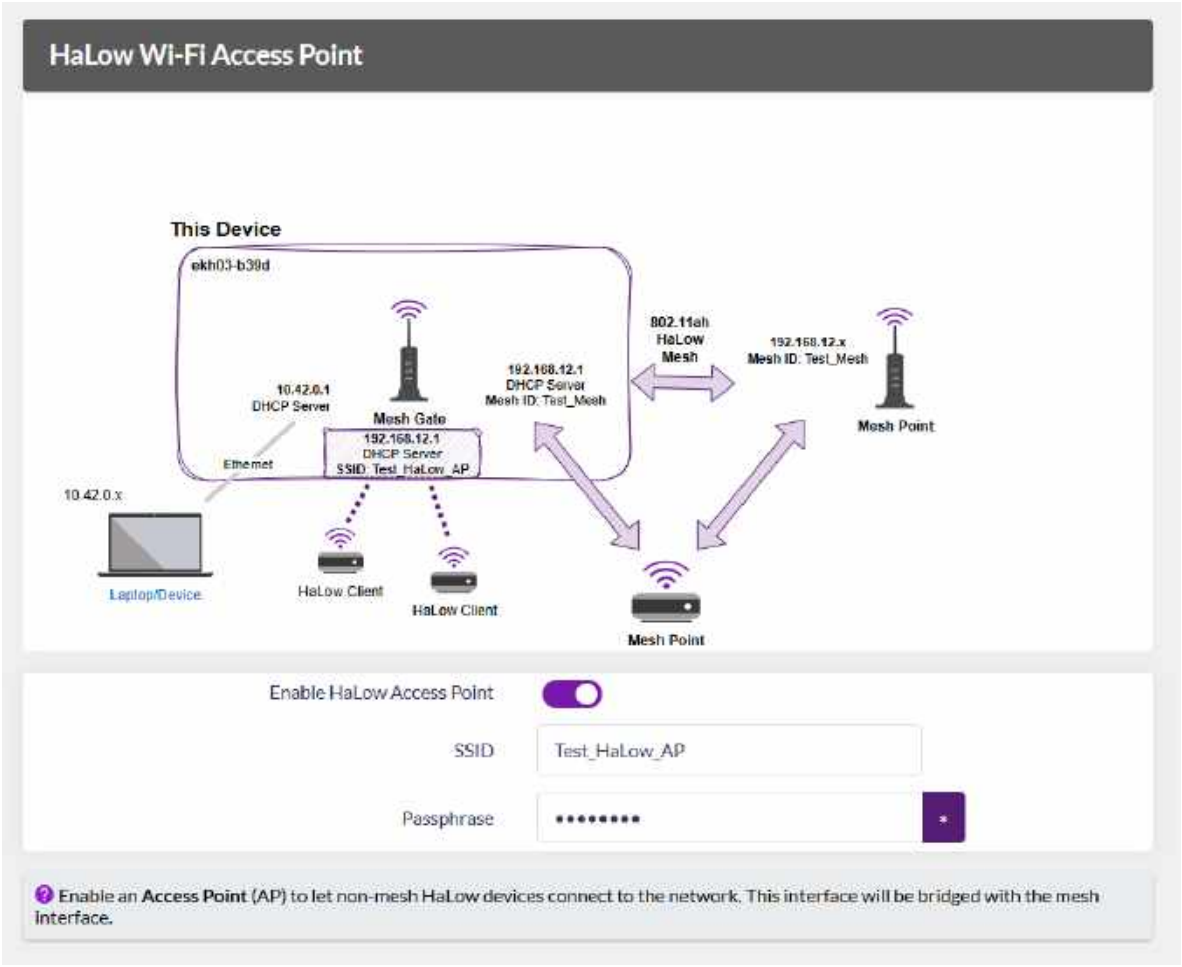
4. On the **Setup Mesh Network** set an appropriate Mesh ID, encryption and passphrase. Then click **Next**.
5. For the **Traffic Mode**, select 'Bridge' and click **Next**.
6. After saving the configuration (by clicking 'Apply'), disconnect your laptop from the Mesh Point and connect it either to the Mesh Gate or another Mesh Point to integrate it into the Mesh Network and obtain an IP address for the device. To access the Mesh Point's admin interface again, navigate to the **Home** page of the Mesh Gate's admin interface and inspect the **DHCP Leases**.

3.9.2 Mesh Gate configuration

1. As a prerequisite, ensure that your device is configured with the appropriate region and a channel. Refer to steps in 3.1 to connect to the device and set the region.
2. Once you decide to configure your device as a Mesh Gate, navigate to the **Wizards** config in the side menu and select **802.11s Mesh Wizard.**
3. As a first step, choose 'Mesh Gate' as the mode and then click **Next.**



4. On the **Setup Mesh Network** page set an appropriate Mesh ID, encryption and passphrase. Then click **Next**.
5. On the following page, **Upstream Network** should be *None*. Click **Next**.
6. For a Mesh Gate, you have the option to set up an additional **HaLow Wi-Fi Access Point** interface (Co-located AP) alongside the Mesh interface to extend the HaLow network if needed. On the **HaLow Wi-Fi Access Point** page, if you enable the AP, then ensure to fill in the SSID, encryption and password for that interface. Please note, that this AP interface that is created is always bridged with the Mesh interface in the Mesh Gate mode. Then click **Next**.



7. You can then **Apply** your configuration on the final page.

3.9.3 (Optional) Add upstream internet connectivity in Mesh Gate mode

Typically a Mesh Gate is a device that provides access to one or more distribution systems via the wireless medium for the mesh basic service set (MBSS). In many situations it is helpful to have an upstream connection to the internet. The following instructions outline how to connect your Mesh Gate to an upstream internet gateway.

It assumed that the upstream gateway provides the following:

- a DHCP server to allocate an address to your AP.
- a DNS server, provided via a DHCP offer.
- a gateway address, assigned via a DHCP offer.

The steps are as follows:

1. Connect a laptop to your HaLow device as described in Section 3.1 and navigate to the admin interface (usually http://10.42.0.1).
2. Go to the **Wizard** config in the side menu and select **802.11s Mesh Wizard**.
3. Repeat the steps 3 and 4 as in Section 3.9.2.
4. On the **Upstream Network** page, choose 'Ethernet', and set the **Traffic Mode** to 'Router'.
5. Refer to step 6 in 3.9.2 and then proceed to **Apply** the configuration on the final page.
6. Use an Ethernet cable to connect your Mesh Gate to your existing network.
7. To access the device's admin interface again, you can access 192.168.12.1 over the HaLow link or you will need to determine the address allocated by your network's DHCP server. See section 3.6 for how to reset your device if you lose access.

3.9.4 Additional 802.11s Mesh settings

1. In addition to configuring the 802.11s Mesh settings through the wizard, you can access further options by navigating to the **Advanced Config > Network > Wireless** page. Click on **Edit** next to the Mesh Interface to access and adjust the advanced mesh settings available in this section.
2. If you decide to enable B.A.T.M.A.N for the Mesh Interface in Mesh Gate mode, remember to include the AP interface (if it exists) in the same network. You can achieve this by adding the same network name to the AP interface in **Network > Wireless > Edit (AP) > Interface Configuration > Network.**
3. To configure a static IP address on either the Ethernet or HaLow interface, set it in the **Quick Config** page, found in the side menu.

3.10 EasyMesh

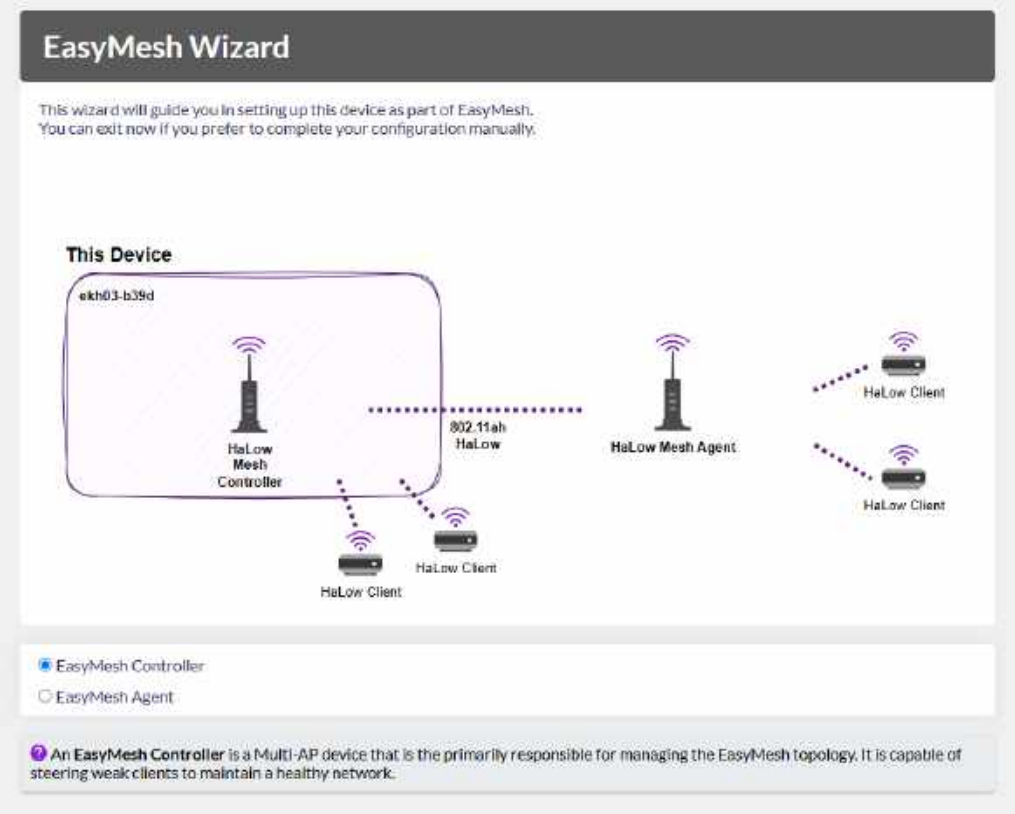
3.10.1 Theory of Operation

EasyMesh is a Wi-Fi branded, standards-based solution for meshing together access points to provide an extended coverage area (but with reduced bandwidth available to stations). EasyMesh forms a tree structure with a controller at the root that controls the mesh network, and agent APs that connect both upstream towards the controller and downstream towards stations. Stations are agnostic to mesh, and continue to connect to the closest AP as usual.

The current implementation supports up to 4 agents in addition to the controller, with at most 2 agents between the controller and a station.

3.10.2 EasyMesh Controller Configuration

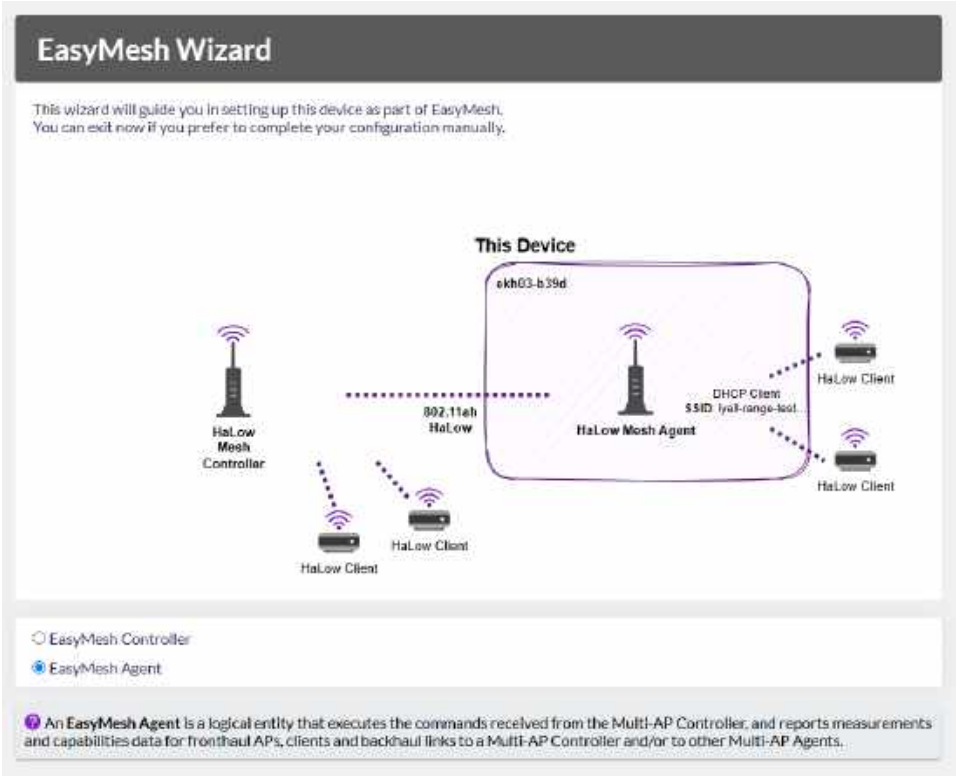
1. As a prerequisite, ensure that your device is configured with the appropriate region and a channel. Refer to steps in 3.1 to connect to the device and set the region.
2. Once you decide to configure your device as an EasyMesh Controller, navigate to the **Wizards** config in the side menu and select **EasyMesh Wizard.**
3. As a first step, choose 'Easymesh Controller' as the mode and then click **Next**.



4. On the **Setup EasyMesh Network** page set an appropriate SSID and passphrase. Encryption is defaulted to WPA3-SAE. Then click **Next**.
5. On the following page, **Upstream Network** should be 'None'. Click **Next.**
6. You can then **Apply** your configuration on the final page.
7. Proceed to Section 3.10.4 for pairing the device with other Agents.

3.10.3 EasyMesh Agent Configuration

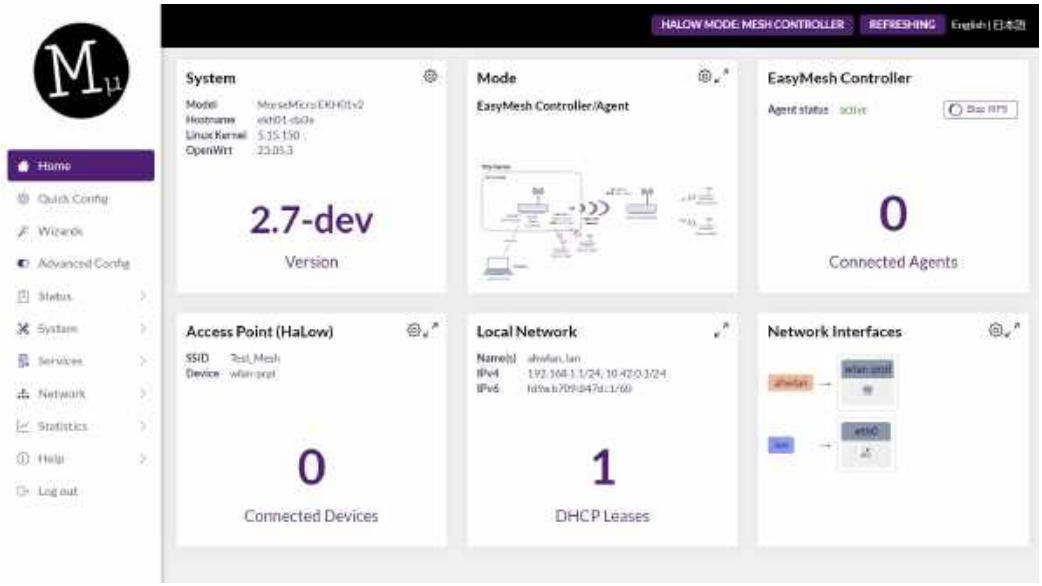
1. As a prerequisite, ensure that your device is configured with the appropriate region and a channel. Refer to steps in 3.1 to connect to the device and set the region.
2. Once you decide to configure your device as an EasyMesh Agent, navigate to the **Wizards** config in the side menu and select **EasyMesh Wizard.**
3. As a first step, choose 'EasyMesh Agent' as the mode and then click **Next**.



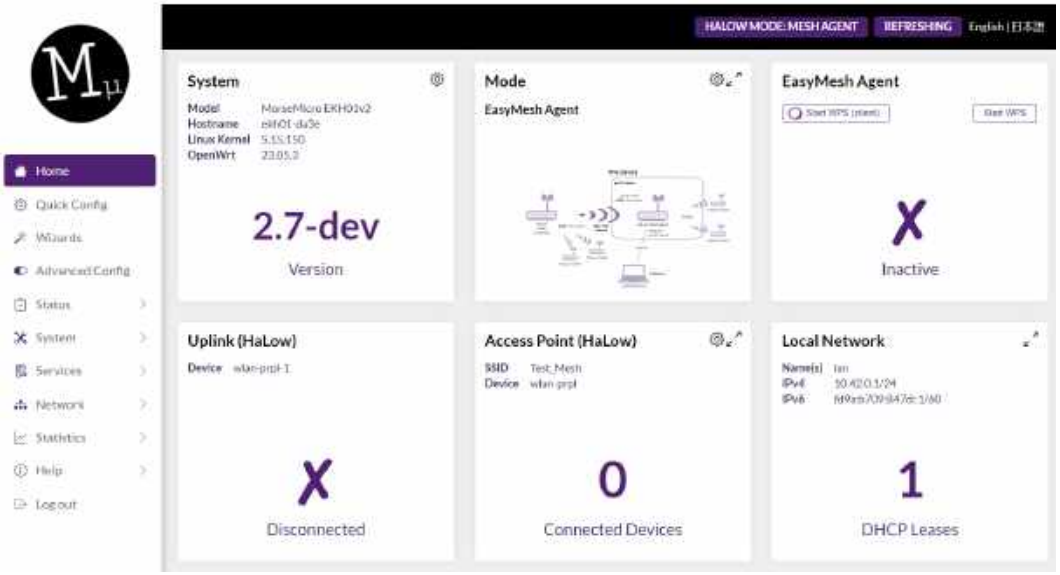
4. For the **Traffic Mode**, select 'None' and click **Next**.
5. After saving the configuration by clicking 'Apply', navigate to the **Quick Config** page and set an IP address for the Ethernet which is different to the EasyMesh Controller's IP address so that it allows you access the UI of both devices at the same time.
6. Proceed to section 3.10.4 for pairing the device with EasyMesh Controller or other Agents.

3.10.4 Pairing EasyMesh devices

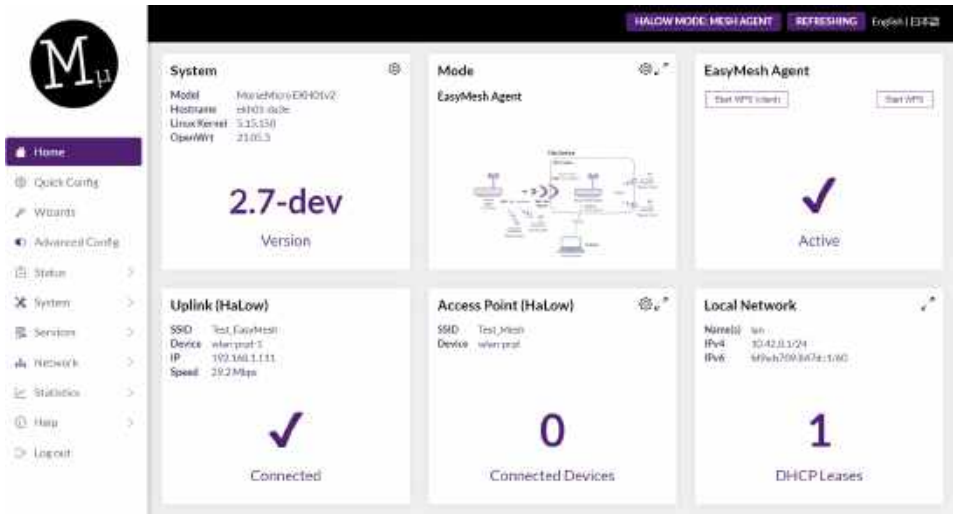
1. As a prerequisite ensure that your device is configured either as an EasyMesh Controller or Agent following in the steps in sections 3.10.2 or 3.10.3 respectively.
2. On the EasyMesh Controller, Navigate to the **Home** page in the UI, and once the Agent Status shows *Active* in the EasyMesh card, click on the **Start WPS** button.



3. Simultaneously, on the EasyMesh Agent device, navigate to the **Home** page in the UI, and in the EasyMesh card, click on the **Start WPS (client)** button to pair itself with the Controller.

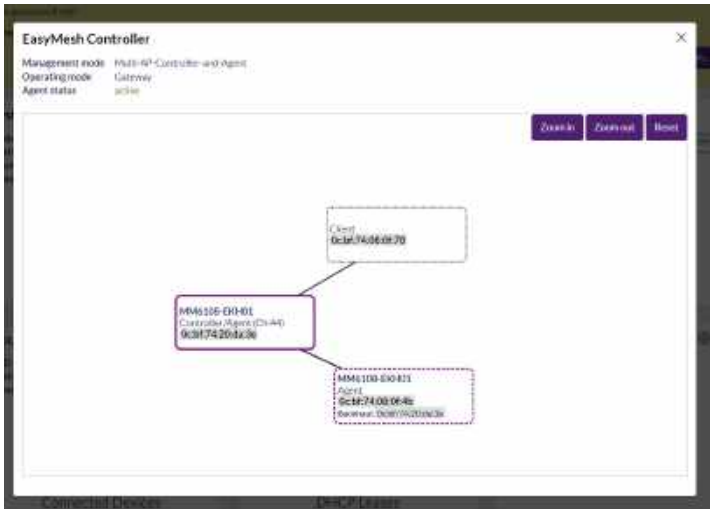


4. Upon successful completion of WPS pairing the Home page will show the Agent Status as *Active*.



3.10.5 EasyMesh Status

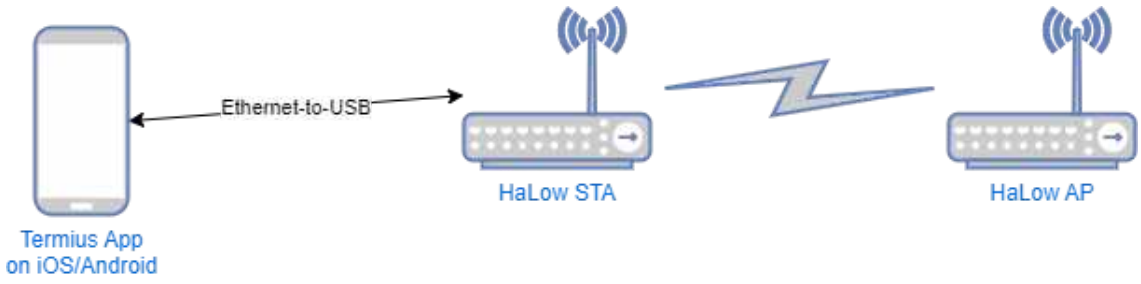
To confirm that EasyMesh has been enabled and is working, status information is available on the **Home** page of the **EasyMesh Controller**, which displays the number of **Connected Agents**. Clicking on **Connected Agents** in the EasyMesh card on the UI will open a topology diagram:



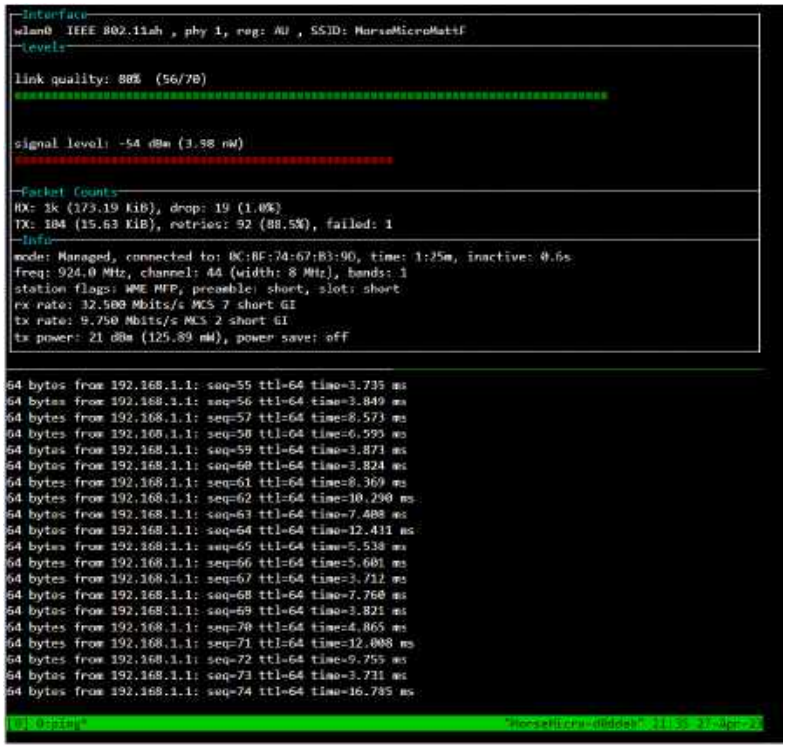
Logs are also available from **Advanced Config > Status > System Log** when EasyMesh is enabled. If these are not visible, you may need to logout of the frontend due to caching.

4 Wavemon and Ping Testing

Wavemon provides a powerful way to quickly test the performance and quality of a HaLow connection in the field. All that is required is a mobile phone, HaLow AP, HaLow STA (with a suitable power supply) and a USB-Ethernet cable to connect the mobile to one of the HaLow devices. The diagram below shows how to setup the equipment:



To run wavemon, the mobile device will need to be able to run an SSH session (e.g. using Termius for Android/iOS). Once an SSH session has been started run the command `pt` from the command line interface and a wavemon ping test will be begin:



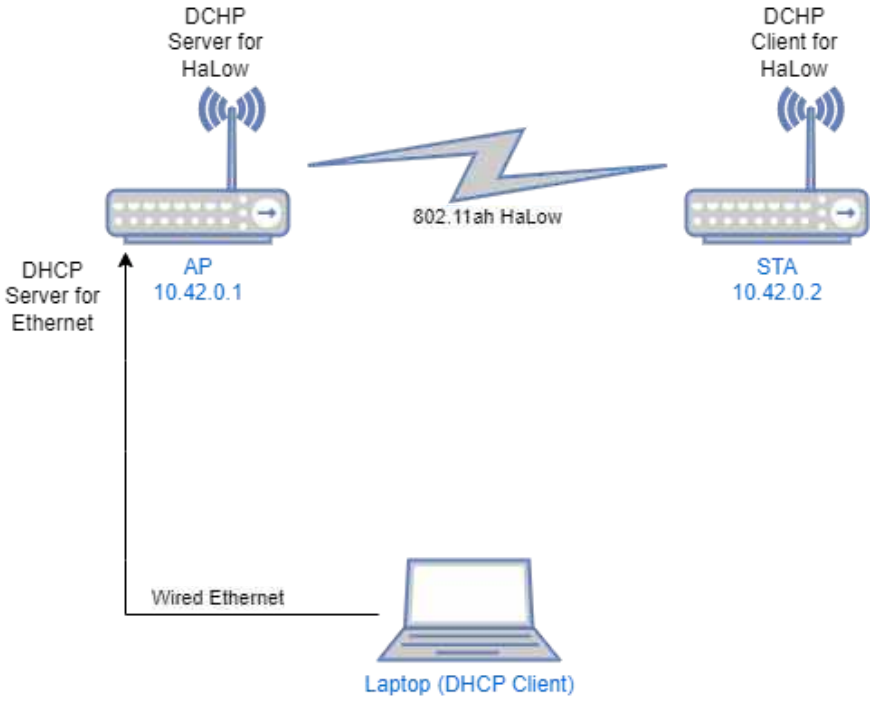
Note that `pt` will ping 192.168.12.1 by default, but an alternate address can be provided as an argument to the script, e.g. `pt 1.2.3.4`.

5 Setting up iPerf3 traffic testing

iPerf3 testing provides a tool for analysing the quality of HaLow connections by sending a stream of traffic and measuring the speed, throughput and latency.

The following guide outlines how to run iPerf3 tests between two devices connected via HaLow. In the diagram below, there are two devices, an AP and a STA, which may be any of the available evaluation kits (EKH01, EKH03). The older iPerf2 (just called tool also comes pre-installed on these evaluation kits and can be used instead of the newer iPerf3.

In this setup the AP will be the iPerf server and the STA will be the iPerf3 client, but these roles can be changed as needed.

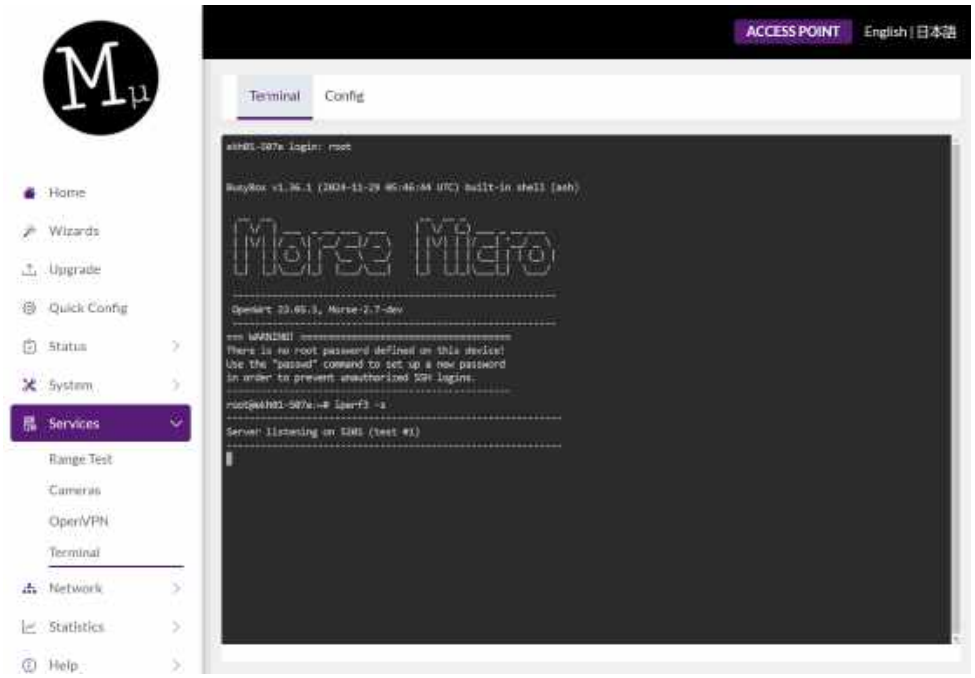


5.1 AP configuration

1. Setup a standalone AP as outlined in Section 3.2.1.
2. Navigate to the **Quick Config** page in the side menu of the UI. Select 'Access Point' as mode for the wireless interface and configure only the following settings:

Configuration item	Value
Region	AU (or as appropriate)
Ethernet Network IP address	10.42.0.1 (default)
Enabled HaLow DHCP server	Enabled

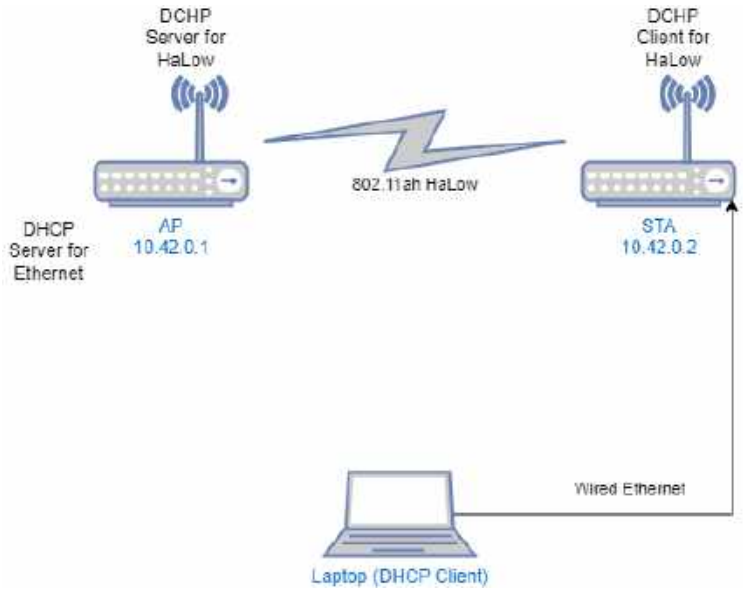
3. Navigate to the **Advanced Config > Services > Terminal** page in the side navigation bar. Note that the credentials will be the same as used to login to the web UI.
4. Type `iperf3 -s` and press enter to launch the iperf3 server.



5. Remove the Ethernet cable from the device and begin setting up the iPerf3 client.

Note: If the server keeps shutting down prematurely, it is recommended to restart it using tmux (included in the image).

5.2 STA configuration

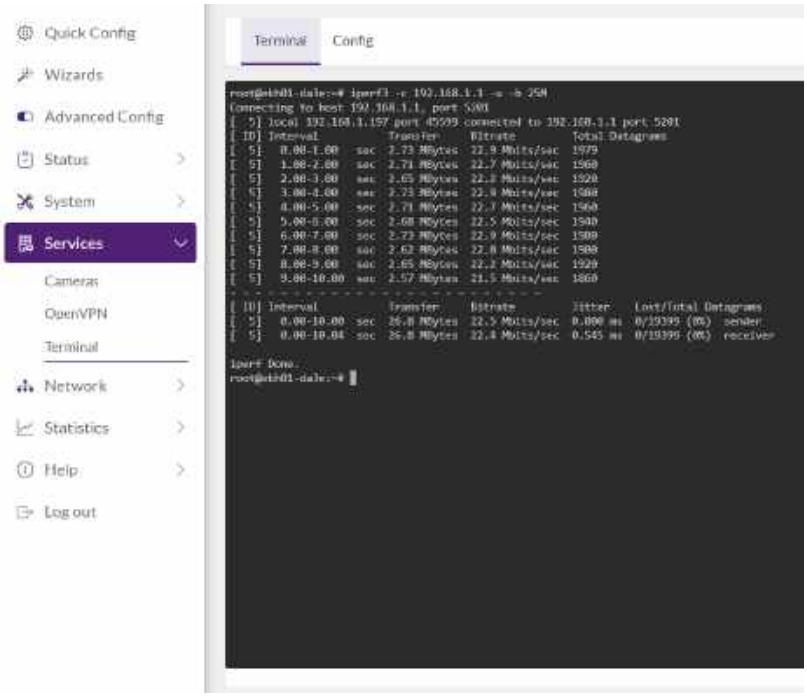


1. Connect an antenna (if applicable).
2. Connect an Ethernet cable from your PC to the RJ45 port of the Morse Micro device.
3. Connect a USB-C power cable to the Morse Micro AP device.
4. Power the unit on and wait ~60 seconds to allow the device to start up.
5. In a web browser on the laptop, navigate to the web UI of the device (http://10.42.0.1 by default). Close the wizard (click 'X' on the top right) if it's enabled.
6. Navigate to the **Quick Config** page in the side menu of the UI. Select 'Client' as mode for the wireless interface and configure the following settings (the rest can remain as default):

Configuration item	Value
Region	AU (or as appropriate)
Ethernet Network IP address	10.42.0.2
SSID / Encryption / Password	Match the AP config
HaLow IP Method	DHCP

7. Navigate to the **Advanced Config > Services > Terminal** page in the side navigation bar. Note the credentials will be the same as used to login to the web UI.

8. Type `iperf3 -c <ip_address> -u -b 25M` where `<ip_address>` is the IP address of the other side of the HaLow link and press enter to launch the iPerf3 client. The STA will connect as an iPerf3 client to the server running on the AP to run traffic between them, testing the link.

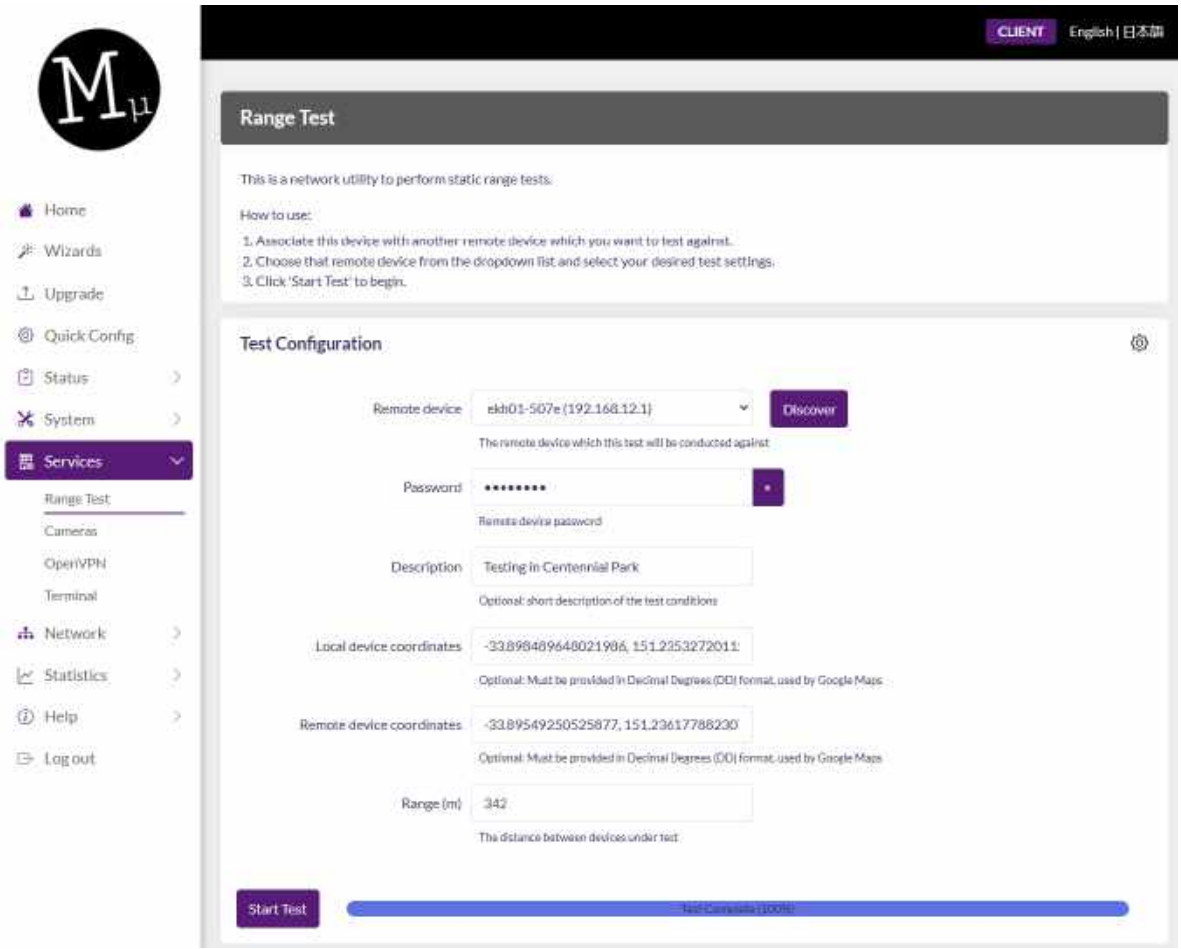


5.3 Web user interface

You can also run iPerf in server and client mode via the web UI. This can be accessed from the top menu in UI by browsing to **Advanced Config > Network > Diagnostics**.

6 Range Testing

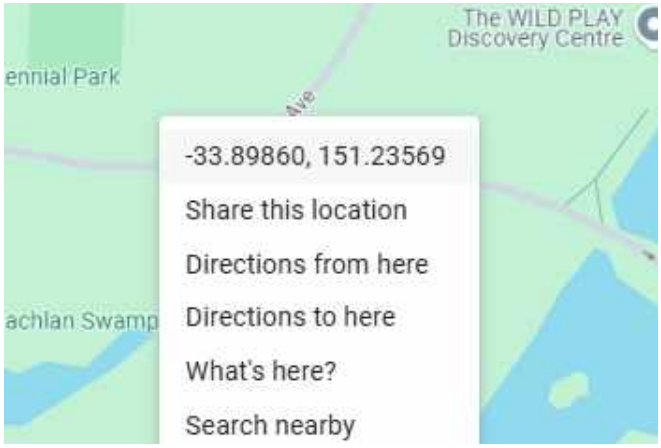
The Range Test application is designed as a simple way to analyse HaLow network performance by automating iPerf3 tests and collecting realtime statistics. It is a useful tool for quickly assessing signal strength, data throughput, and connection quality across different environments.



Note: before using this application ensure that all devices being tested are running the same version of Morse OpenWrt. This tool can run with different types of evaluation kit (i.e. between an EKH03 and an EKH01) but the software versions must be the same on each unit.

To use the range testing tool:

1. Connect the devices being tested on the same HaLow network of any type outlined in this guide.
2. Set up the devices in the locations you want to test and select one to connect your laptop to. This will be referred to as the local device.
3. In a web browser navigate to the web UI of the device (http://10.42.0.1 by default).
4. Navigate to **Services > Range Test**.
5. Click the Discover button to populate the 'Remote device' dropdown.
6. Select the HaLow IPv4 address of the remote device you want to test against. **Note:** if multiple IPs appear in a particular option (e.g., 10.42.0.1, 192.168.12.1), the local device is also connected to the remote via another method such as 2.4 GHz or Ethernet. Extra connections should be removed for optimal results.
7. Fill in the 'Password' field if the remote device has one.
8. Optional - Provide user notes about the test for reference in the 'Description' field.
9. Optional - If you want to log the coordinates of the local and remote devices and have the range calculated automatically enter the coordinates into the local and remote device coordinates fields respectively. These values can be easily found by right clicking the relevant locations on Google Maps and then selecting the coordinates which will automatically place them in your clipboard (pictured below).



10. If you have entered valid coordinates as outlined in the steps above, the 'Range (m)' field should automatically populate, otherwise you must manually enter a value.
11. Optional - If you click the ⚙ icon in the top left corner of the **Test Configuration** subsection, you can modify the data directions and protocols which you would like to test.

12. Click **Start Test** and a progress bar will appear showing the status of the current test. This can be cancelled at any time by clicking the **Stop** button.

After the test completes, a row in the **Results Summary** subsection should appear, as pictured below. This result can be deleted by clicking the trash icon, or a JSON file containing all the raw data can be downloaded via the **Download** button. The **Download All** button yields a similar file with all the JSON blobs in an ordered array. The downloadable JSON data is intended for helping engineers with remote debugging

Note: test results are volatile to avoid overwhelming limited memory resources and will be deleted if power is removed or the device is rebooted.

7 Video Streaming

OpenWrt supports video streaming functionality where cameras attached to stations can stream video to an AP, viewable via the UI. This functionality includes automatic discovery of cameras on the HaLow network which are running compatible firmware (detailed below in station configuration). Any ONVIF-compliant cameras on the network which support H.264 streams will be detected automatically.

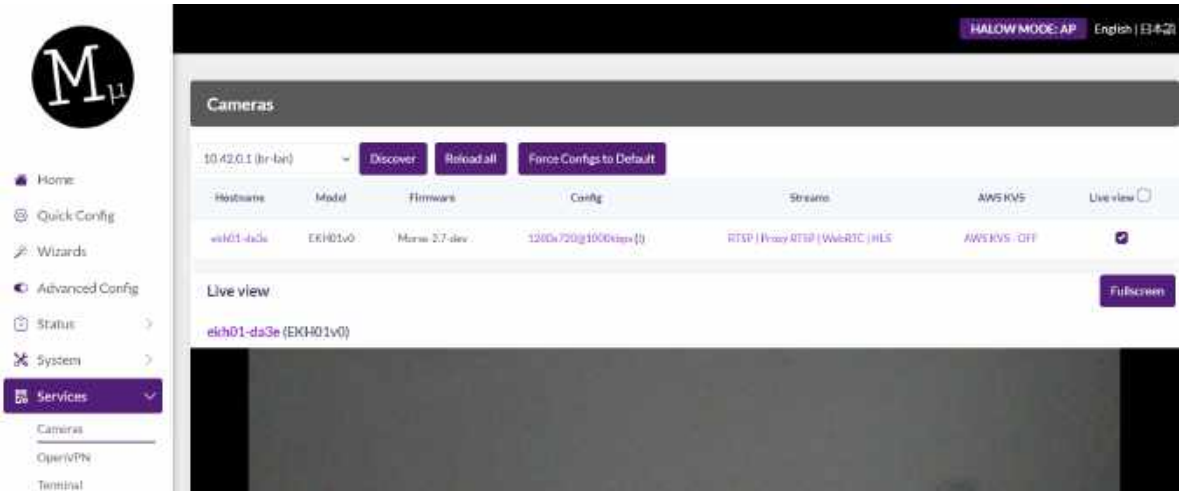
Note: When using the EKH03 as an AP, the web UI can display a maximum of two livestreams simultaneously due to CPU and memory requirements when proxying the streams.

7.1 Setting up

Follow Section 3 to configure your network and determine the IP address of your AP.

7.2 Accessing the Video Streams

In the web UI of the access point navigate to **Advanced Config > Services > Cameras**:



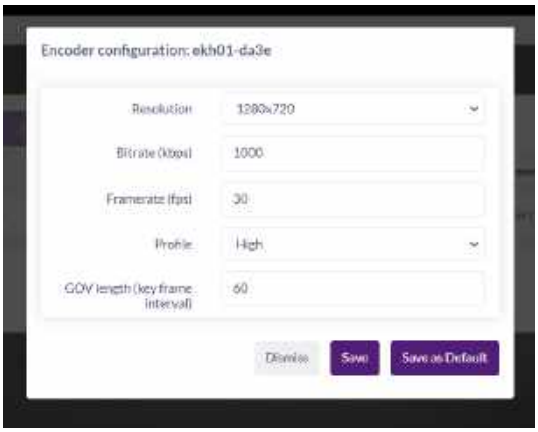
The AP will automatically discover all ONVIF cameras on the network. Note that it will only scan the selected network attached to the interface listed next to the **Discover** button. After scanning it will automatically start streaming from the discovered cameras.

The checkboxes under the 'Live view' column are used to select which video streams should be displayed.

7.3 Configuration

The following options are available for configuring video streaming:

- **Discover** finds all cameras on the selected interface.
- **Reload All** reloads all the previously discovered camera streams.
- **Force Configs to Default** changes all camera configurations to the default configuration. Hovering over the button displays the default settings.
- **Config** opens a window to modify the camera's configuration.



  - **Resolution** of the camera
  - **Bitrate** of the video stream
  - **Framerate** of the video stream
  - **Profile** for the H.264 compression
  - **GOV length** sets number of frames between each key frame
- **Streams** selects the type of stream you want to view (opens in a new window).
- **Live View** selects whether to show a live stream on the current page (via WebRTC).
- **Fullscreen** shows a combined fullscreen view of all the currently enabled streams. To see a fullscreen view of an individual stream, hover over the stream to bring up the video controls.

7.3.1 Live View

Cameras can also be configured from the live view window, that includes the resolution, bitrate, framerate and brightness.

8 Page Descriptions

This section describes some of the pages available in the web UI.

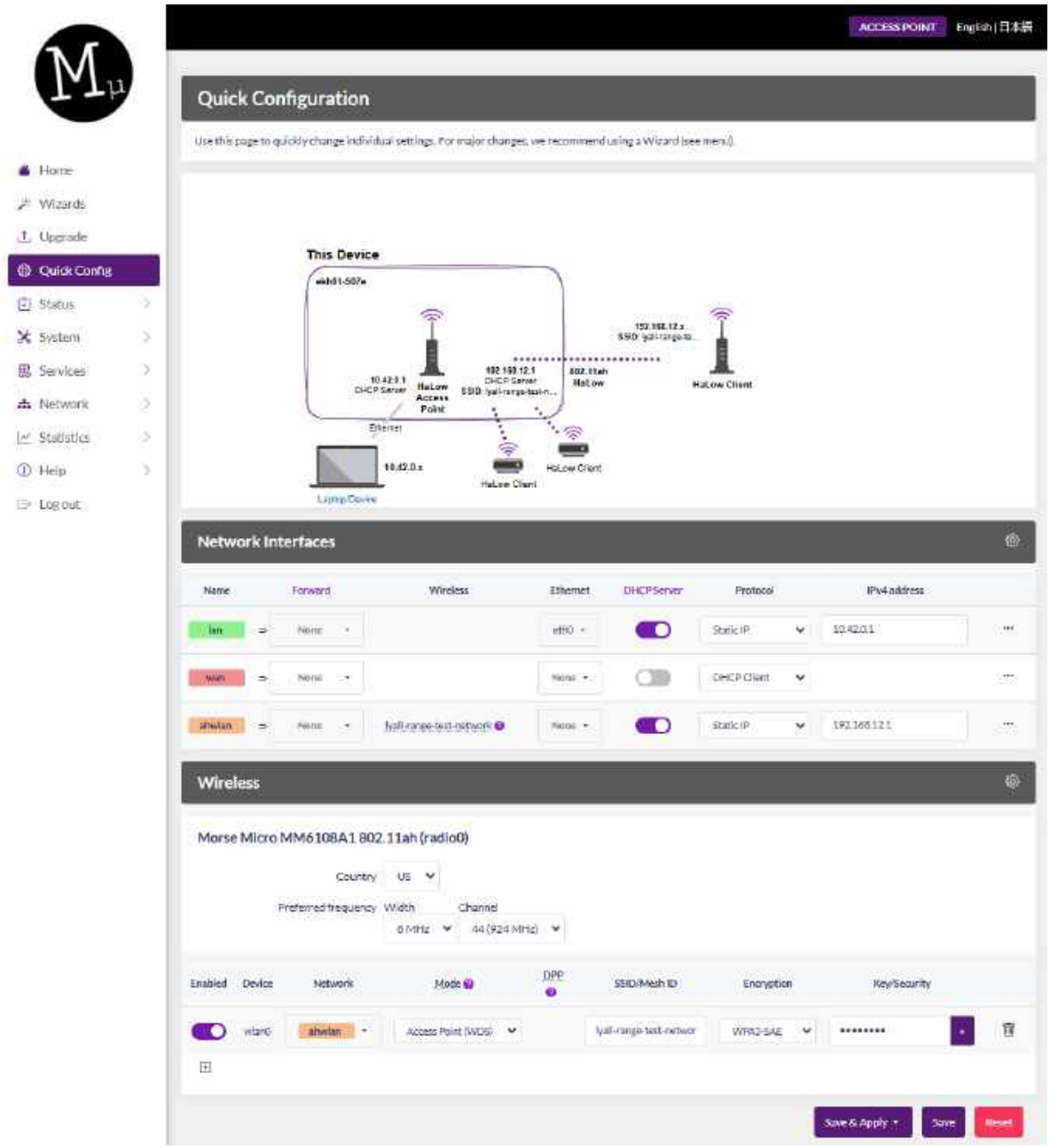
8.1 Home

The Home page provides a comprehensive view of the device's current status. It includes several key sections to help users understand the overall state of their device.

- **System** provides general details about the device, including the software version and model name. This section is essential for identifying the device and understanding its current firmware status.
- **Mode** displays the operational mode of the device and includes a configuration representation with a topology diagram. This visual aid helps users see how their device is configured and operating within the network.
- **HaLow Network Status** shows the current status of the HaLow network, including any connected clients if the device is functioning as an Access Point. This information is crucial for monitoring the HaLow network's health and connected devices.
- **Uplink Information** provides the status of the uplink connection, offering details about connectivity. This section ensures users are aware of their device's connection to the wider network or internet.
- **Local Network Info** gives detailed information about the local network, including DHCP lease information if the DHCP server is enabled. This section helps users manage their local network and understand IP address assignments within their network.
- **Network Interfaces Information** displays the groupings of network interfaces, showing how they are organized and connected. This information is important for managing and troubleshooting network interfaces.
- **EasyMesh Status** offers a topology view, showing the network's structure and connections between devices. It also lists the number of connected agents and provides options for WPS (Wi-Fi Protected Setup) pairing, making it easier to add new devices to the network.
- Additionally clicking on the symbol in each of these cards will navigate to the corresponding advanced configuration page.

8.2 Quick Config

The **Quick Config** page can be used to make any changes to the existing configuration on the device. Note that settings do not take effect until the **Save & Apply** button at the bottom of the page is clicked.



8.2.1 Network Interfaces

This section allows you to make changes to the Network configuration. The following fields are available:

- **Name** displays the network name. The configurations for this network and the list of Ethernet and Wireless interfaces mapped to this network are displayed in the corresponding row.
- **Forward** enables traffic forwarding between the source and the selected network. Click 'Forward' for advanced firewall settings.
- **Ethernet** selects an Ethernet port and maps it to the specified network.
- **DHCP Server** enables the DHCP server for the network. Click 'DHCP Server' for advanced DHCP and DNS configurations.
- **Protocol** sets either 'Static IP' for manual IP address configuration or 'DHCP client' to retrieve an IP from a DHCP server if available. Using DHCP is generally preferred.
- Click the three dots at the end of the row to configure the following options:
- **Netmask** sets the netmask for the interface. This option is available only if the protocol is set to 'Static IP'.
- **Gateway** sets the IP address of the upstream gateway for default IP traffic routing. This option is available only if the protocol is set to 'Static IP'.
- Click on the ⚙ symbol, to navigate to the advanced Network Configuration page.

8.2.2 Wireless

This section allows you to modify the wireless settings. The available fields are:

- **Country** defines the regulatory region for your HaLow device. This setting applies restrictions on channel, bandwidth, power and duty cycle to ensure compliance with local regulations. Only supported regions will appear in the drop-down list. For more information, refer to the MM6108 Channels Guide document.
- **Preferred Frequency Width** selects the operating bandwidth for the HaLow network. The dropdown menu is automatically populated based on the Country selection.
- **Channel** chooses the frequency channel for the HaLow network. The dropdown menu is automatically populated based on the selected Preferred Frequency Width.

The list of available wireless interfaces and their configurations are displayed in the corresponding row:

- **Enabled** indicates the status of the wireless interface. Toggle the slider to enable or disable the wireless interface.
- **Device** displays the name of the wireless interface.

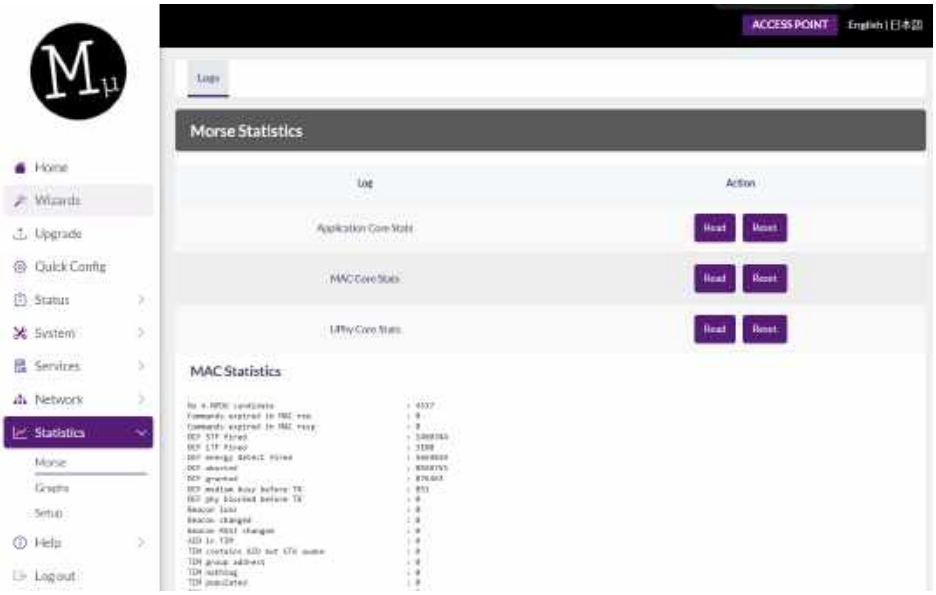
- **Mode** selects the mode of operation for the wireless interface. Options include: Access Point (WDS), Access Point (no WDS), Client (WDS), Client (no WDS), Mesh Point, Ad-Hoc (IBSS), Monitor and None.
- **DPP** lets the device broadcast a DPP preference for connection establishment.
- **SSID/Mesh ID** configures the SSID for connection. The field initially shows the currently configured SSID. In Client mode, clicking the 🔍 icon will scan for visible HaLow networks and populate the dropdown with visible SSIDs. If the SSID is not visible, you can manually enter the name and press enter to set it. In Mesh Point mode, enter the Mesh ID here.
- **Encryption** selects the encryption method for data sent over the HaLow network. Available methods include OWE, SAE, Enterprise security (EAP), and None (Open security):
  - OWE (Opportunistic Wireless Encryption) - Ensures privacy between the station and access point without requiring a password or station authentication.
  - SAE (Simultaneous Authentication of Equals) - Uses pre-shared passwords for symmetric encryption, suitable for mesh networks.
  - EAP (Enterprise Security) - Requires RADIUS server configuration for the Access Point and TLS, TTLS, or PEAP authentication credentials for the Client.
- **Password** is visible when SAE is selected as the encryption method. It configures the password used to authenticate and set up encryption between the station and the access point.

Click on the ⚙ icon to navigate to the advanced **Wireless Configuration** page and click **Edit** on the network's corresponding row to modify the following configurations in the **Interface Configuration** subsection:

- **802.11w Management Frame Protection** (Wireless Security) provides additional protection for management frames used for tasks such as authentication, de-authentication, association, disassociation, beacons, and probes. By default, this feature is set to 'required,' meaning management frames are encrypted, and forged frames can be rejected.
- **DTIM Interval** (Advanced Settings) specifies the DTIM (Delivery Traffic Indication Message) period to use, defined as the number of consecutive beacon intervals between DTIM transmissions.
- **Station inactivity limit** (Advanced Settings) sets the maximum number of seconds a wireless client (station) can remain inactive before the AP considers it disconnected or inactive.
- **Beacon Interval** (Advanced Settings) defines how often beacons are broadcast, measured in time units where 1 TU is equal to 1.024 milliseconds.

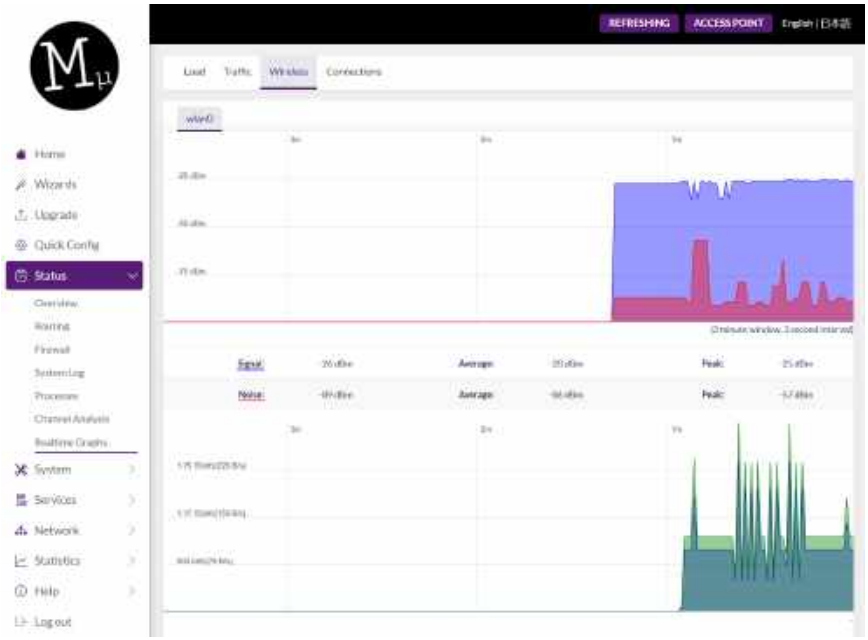
8.3 Statistics > Morse

This page provides processor core statistics on the MM6108 chip. **Read** displays the current statistics of a given core, whilst **Reset** sets counters back to zero. The underlying information on this page is gathered via the `morse_cli` command, which is also available via the CLI.



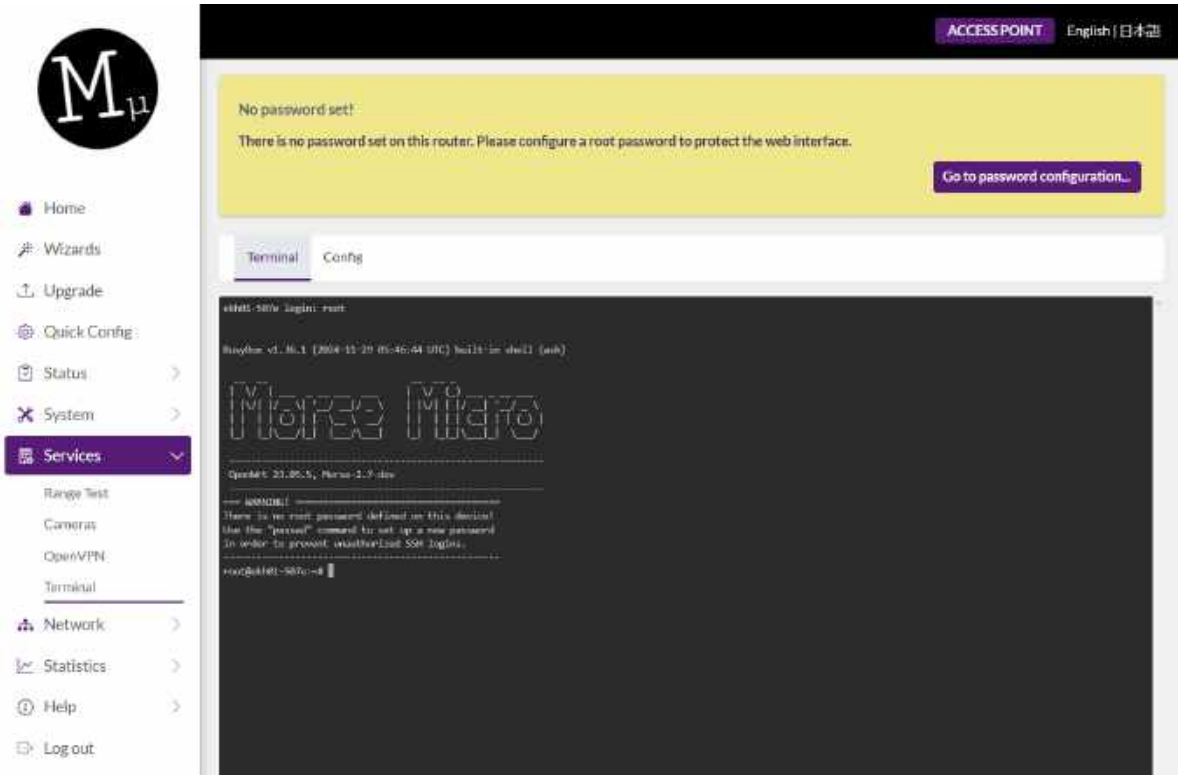
8.4 Status > Realtime Graphs > Wireless

This page displays live HaLow statistics graphs, showing the last 3 minutes of data, updated at a 3 second interval. The graphs are signal strength, data rates, and MCS respectively.



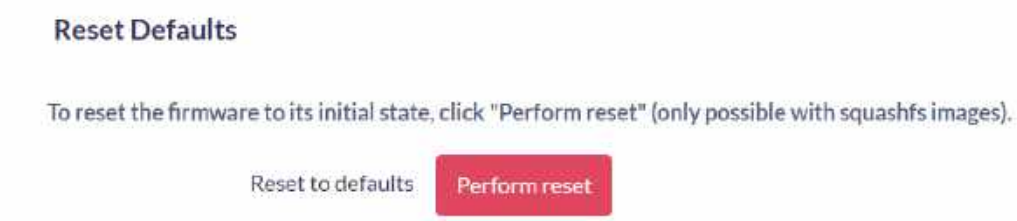
8.5 Services > Terminal

This page allows the user to spawn a usable shell in the web browser.



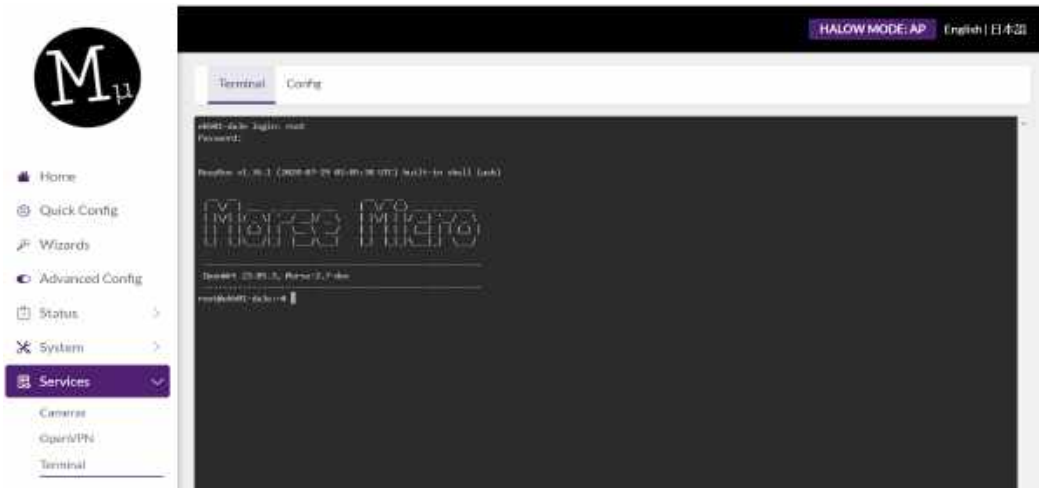
8.6 System > Backup / Flash Firmware

The **Perform reset** button allows you to factory reset the device.



9 Additional Configuration Parameters

Some advanced configurations are useful to control HaLow behavior (particularly during certifications) and are documented here. Some may only be available via the CLI. If unsure, it is best not to modify default values unless advised by a Morse Micro engineer to do so.



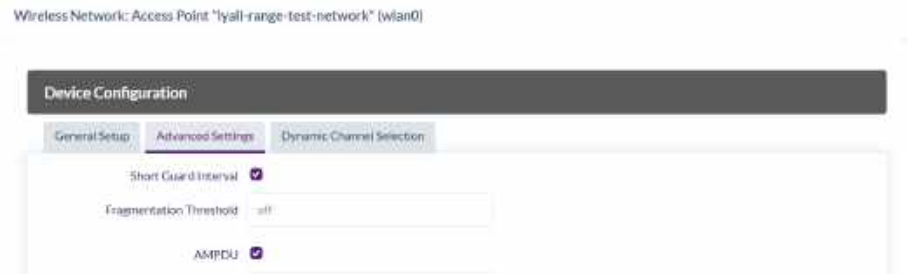
For advanced users this CLI is also available via SSH and serial with the same credentials.

9.1 Disable AMPDU

9.1.1 Via UI

AMPDU can be configured in the advanced settings under the **Advanced Config > Network > Wireless** menu. Click **Edit** next to the HaLow network that is to be configured:

Navigate to the **Advanced Settings** tab under **Device Configuration** and untick 'AMPDU':



9.1.2 Via CLI

AMPDU can be disabled by entering `morse_cli -i wlan0 ampdu disable` into the CLI.

Note: Configurations made via the CLI are not persistent across reboots. To ensure your settings are saved permanently, please configure them through the UI.

9.2 Fragmentation Threshold

9.2.1 Via UI

In the same configuration section as described above for AMPDU, there is an option for configuring the fragmentation threshold. To disable this feature enter 'off' into the field, otherwise enter the number of bytes beyond which fragmentation should occur.

9.2.2 Via CLI

The fragmentation threshold can be set with the `iw` tool:

```
iw phy <phyname> set frag <fragmentation threshold|off>
```

Where the `<phyname>` is provided by the `iw list | grep Wiphy` command which might return something like:

```
Wiphy phy1
```

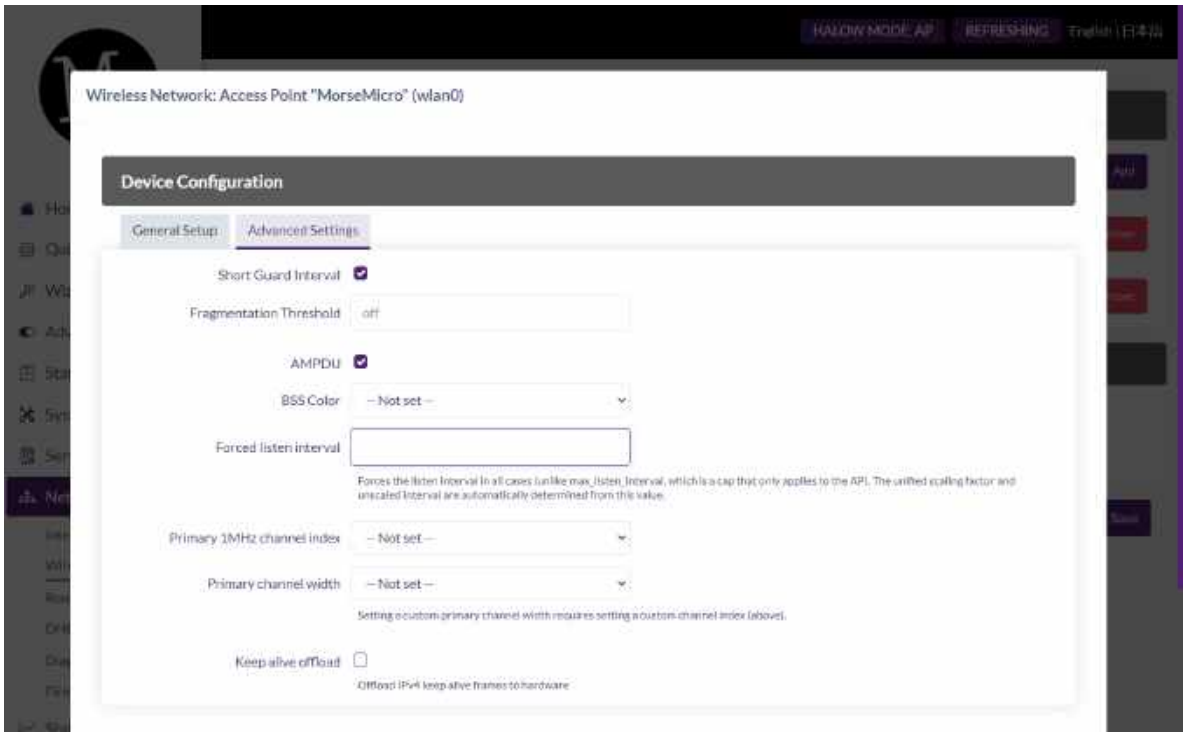
Where `phy1` is the `<phyname>`. The integer following `phy` enumerates every time the driver is (re)loaded.

Note: Configurations made via the CLI are not persistent across reboots. To ensure your settings are saved permanently, please configure them through the UI.

9.3 Unified Scaling Factor / Unscaled Interval

9.3.1 Via UI

Navigate to the **Advanced Config > Network >Wireless** page and then choose **Edit** beside the HaLow network. Use the 'Forced listen interval' input in the **Advanced Settings** tab of the **Device Configuration** section:



9.3.2 Via CLI

The USF and UI and must be set together, with the `morse_cli` tool using the command:

```
morse_cli -i wlan0 li <unscaled interval> <unified scaling factor>
```

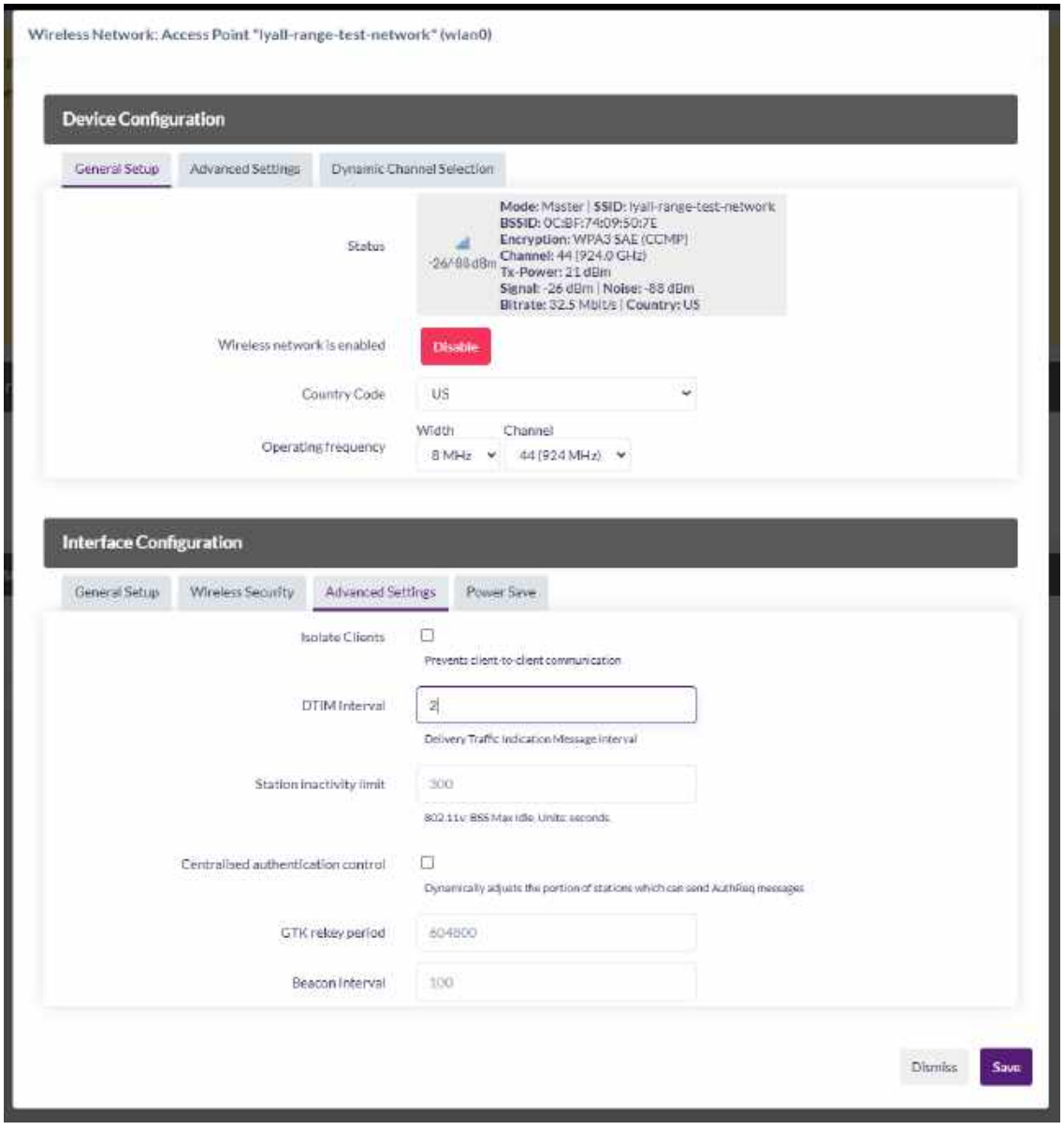
Where `<unscaled interval>` multiplied by `<unified scaling factor>` must be less than or equal to the integer value 65536.

Note: Configurations made via the CLI are not persistent across reboots. To ensure your settings are saved permanently, please configure them through the UI.

9.4 DTIM Interval

9.4.1 Via UI

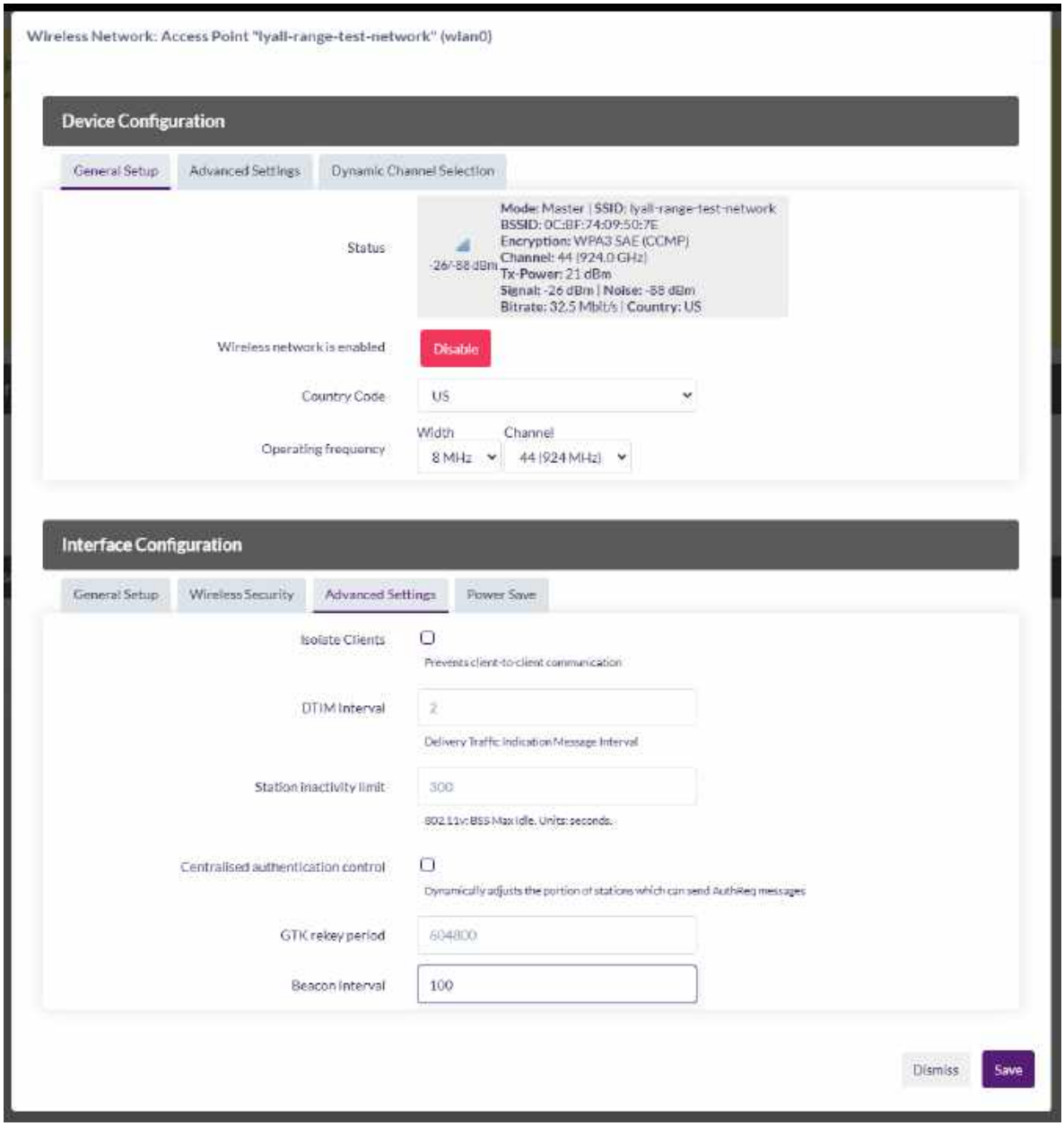
Beacon interval can be configured by navigating to the **Advanced Config > Network > Wireless** page and then choosing **Edit** beside the HaLow network. Set the 'DTIM Interval' input in **Advanced Settings** tab of the **Interface Configuration** section:



9.5 Beacon Interval

9.5.1 Via UI

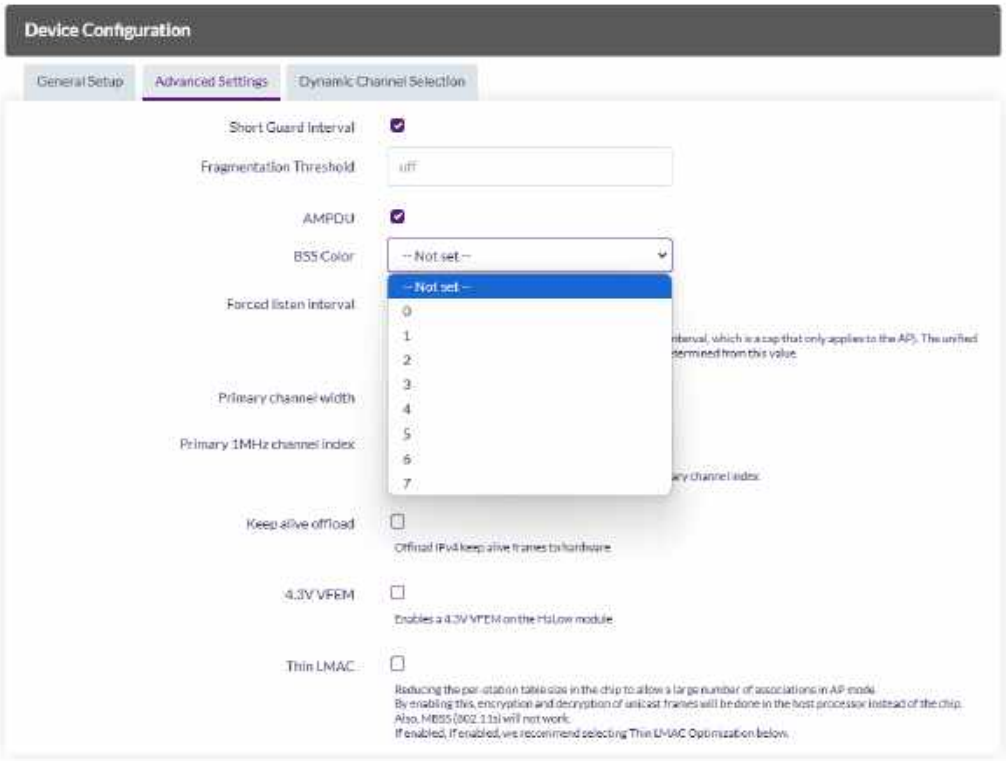
Beacon interval can be configured by navigating to the **Advanced Config > Network >Wireless** page and then choose 'Edit' beside the HaLow network. Use the 'Beacon Interval' in **Advanced Settings** tab of the **Interface Configuration** section:



9.6 BSS Color

9.6.1 Via UI

Navigate to the **Advanced Config > Network > Wireless** page and then choose 'Edit' beside the HaLow network. Use the 'BSS Color' list in **Advanced Settings** tab of the **Device Configuration** section:



9.6.2 Via CLI

BSS color can be configured using the following command:

```
morse_cli -i wlan0 bsscolor <value>
```

Where `<value>` is an integer from 0 to 7.

Note: Configurations made via the CLI are not persistent across reboots. To ensure your settings are saved permanently, please configure them through the UI.

9.7 Other HaLow settings

Other advanced settings are available within the text files found at `/etc/config/`. Generic options are defined in the OpenWrt documentation: https://openwrt.org/docs/guide-user/network/wifi/basic.

9.8 morse_cli

`morsectrl` is a command line utility that allows low-level access and control of the Morse radio chip. It is not intended to be included on consumer devices.

`morse_cli` contains a subset of `morsectrl` commands and is used by netifd to configure the radio (see Section 10). It is intended to be shipped on consumer devices.

In the EKH01 and EKH03 both of these utilities are included. For more information about their available options, refer to their respective command help messages via `-h`.

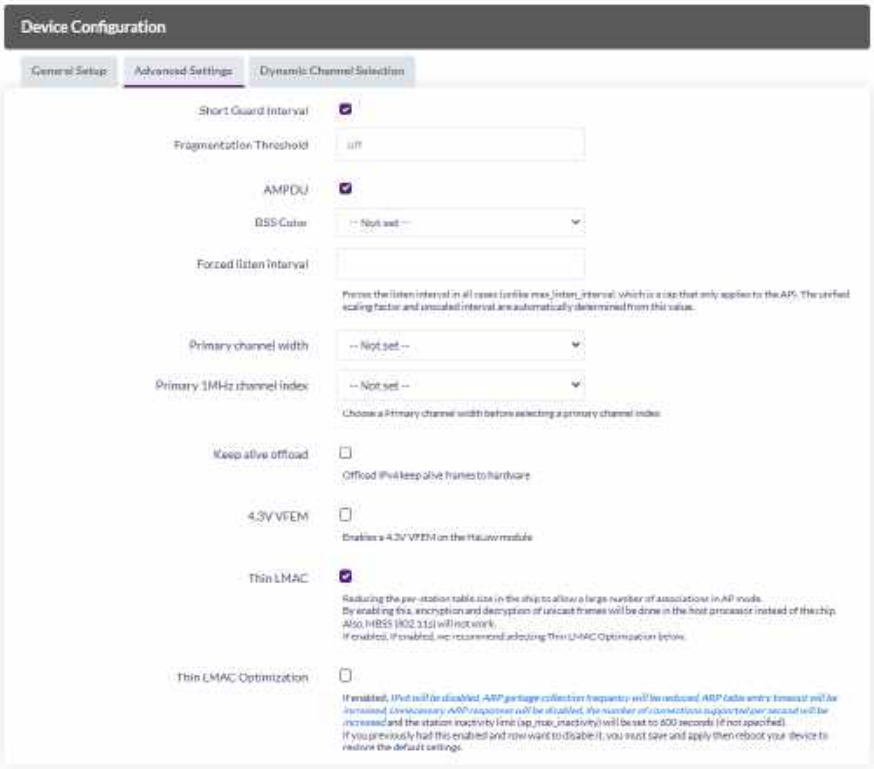
Note: Configurations made via the CLI are not persistent across reboots. To ensure your settings are saved permanently, please configure them through the UI.

9.9 Thin LMAC

Thin LMAC mode allows the firmware running in AP mode to support a large number of associations. This is achieved by reducing the per-station table memory from 88 bytes to 8 bytes inside the chip and moving them to the upper layers of the stack onto the host processor.

9.9.1 Via UI

To enable Thin LMAC through UI navigate to **Advanced Config > Network >Wireless** and choose 'Edit' beside the HaLow network. Select the 'Thin LMAC' option in **Advanced Settings** tab of the **Device Configuration** section:



9.9.2 Via CLI

Enable thin LMAC from command line with the following CLI commands:

```
uci set wireless.radio1.thin_lmac='1'

uci commit

reload_config
```

Disable thin LMAC by setting the above option back to 0 or deleting it from UCI.

9.9.1 Thin LMAC considerations

Since the goal of thin LMAC is to allow a large number of stations, there are some further suggested changes that may be helpful to reduce unnecessary traffic. These include:

- Disabling IPv6
- Reducing ARP garbage collection frequency
- Increasing ARP table entry timeout
- Disabling unnecessary ARP responses

It is also recommended to increase the number of connections supported per second as there might be a large number of simultaneous connections through the AP. In the UI, an 'Thin LMAC Optimization' option is provided to easily apply this set of recommended actions.

10 UI Configuration Architecture

This section outlines how changes to configuration in the UI are applied to the system.

From OpenWrt 2.0.2 onwards, the web UI configuration pages use the `LuCI.uci` API to configure a standard set of UCI configuration sections, which are stored in `/etc/config/`. Starting from OpenWrt 2.6, the Morse > HaLow Configuration page, previously based on a shim layer, has been replaced with a more resilient **Quick Config** page.

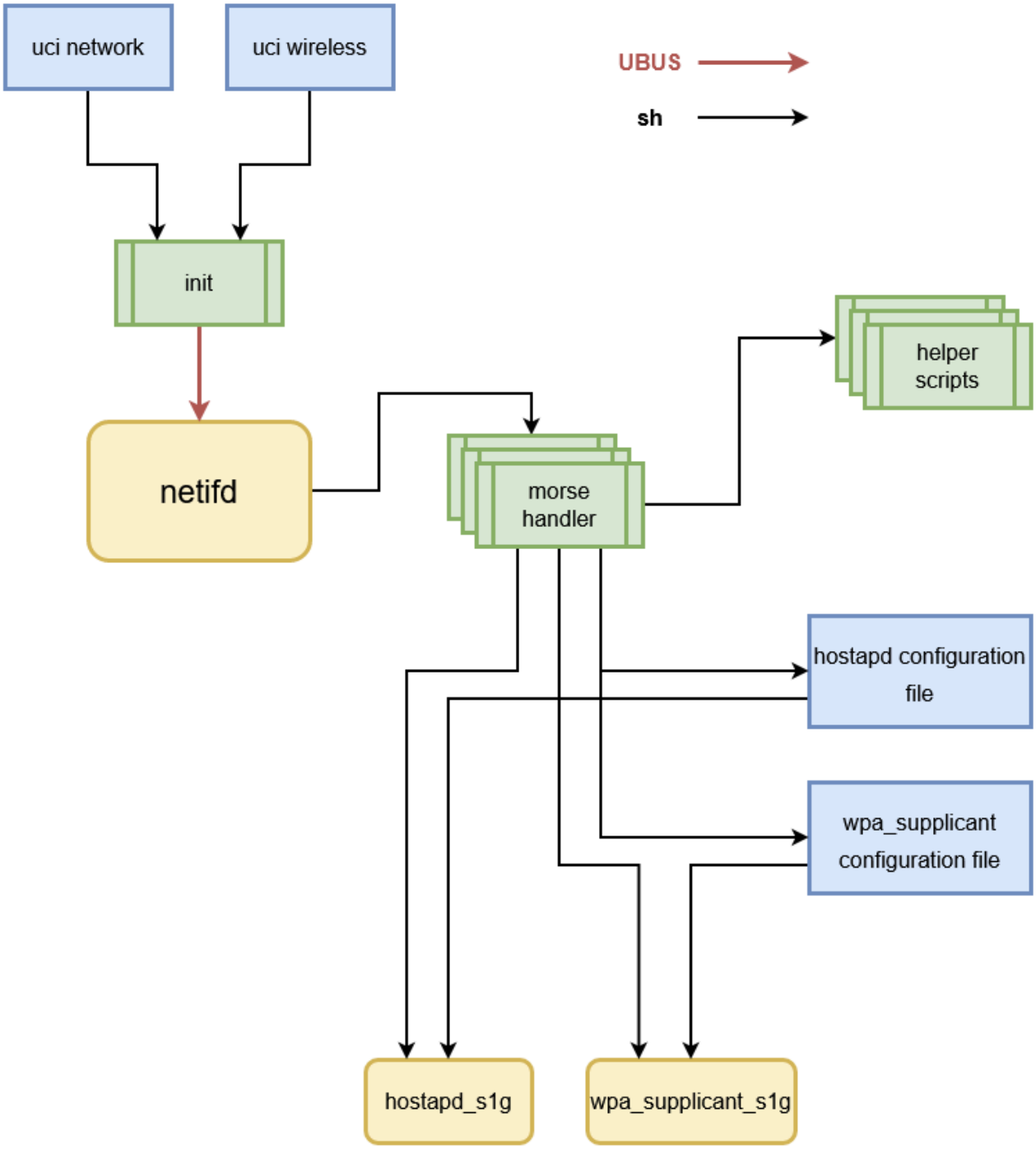
The **Quick Config** page addresses many of the pitfalls of the earlier HaLow Config page. Unlike the previous version it does not rely on hardcoded UCI sections, offering greater flexibility by directly getting or setting configurations in the underlying UCI configurations.

The network service daemon, netifd, examines changed UCI configurations upon reload and calls the necessary handler scripts to update the affected components. For a UCI `wireless.wifi-device`, netifd invokes wireless protocol handlers located in `/lib/netifd/wireless/*.sh`. For MorseMicro HaLow devices, the UCI configuration includes `type=morse`, triggering netifd to load `/lib/netifd/wireless/morse.sh`.

This protocol handler carries out the following:

- Parses sections with a Morse type of `wifi-device` in `/etc/config/wireless`
- Kills `hostapd_s1g` and `wpa_supplicant_s1g`
- Tears down the HaLow configured interfaces
- Rebuilds any morse module parameters - e.g. region information
- Reloads the morse driver module if parameters have changed
- Brings up the HaLow interface
- Creates appropriate `hostapd` or `wpa_supplicant` configuration files.
- Starts `hostapd_s1g` or `wpa_supplicant_s1g` as required.

The image below captures the execution flow of this process:



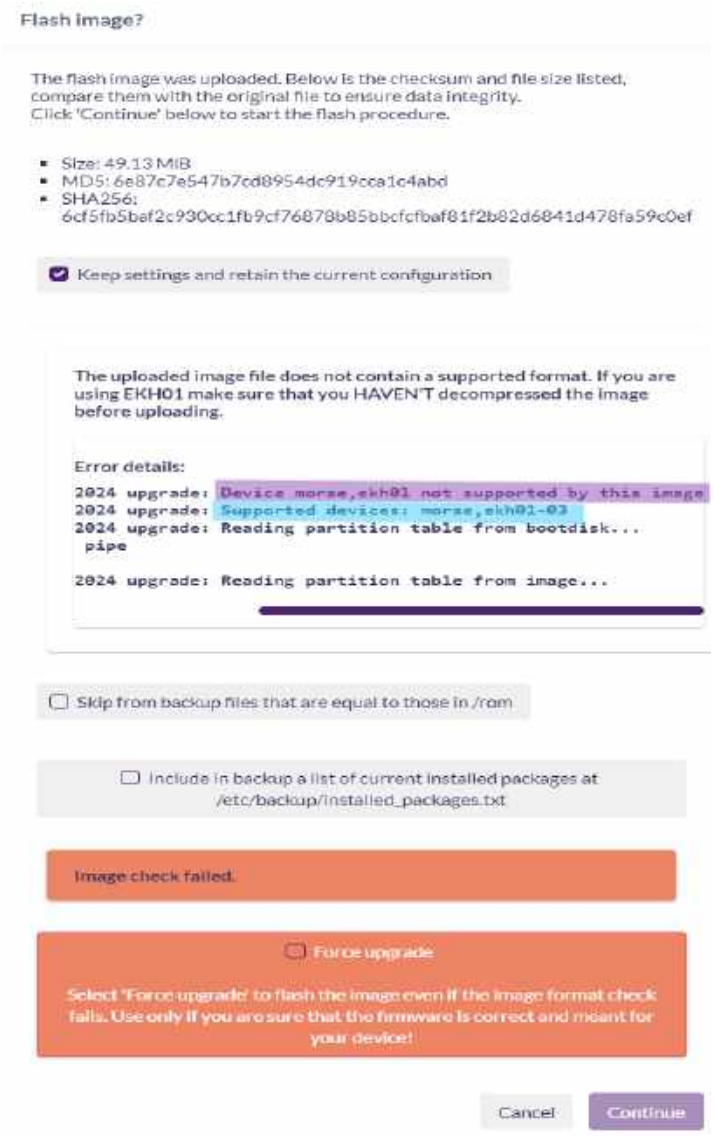
11 Troubleshooting

11.1 Updating firmware

Occasionally a platform name is updated, which can result in an error during upgrade e.g. “The uploaded image does not contain a supported format”(see below image). This is expected for the following upgrades:

- Updating an EKH01 from an image older than 2.3.3 to an image version 2.3.3 or higher.

Before proceeding, check that the ‘Supported devices’ line matches the device revision; the device revision is printed on the case, and on a sticker on the case.



Note 1: This line describes the image currently running on the device.

Note 2: This line describes the image you are trying to install. Match the device name you see here to the information printed on your device.

When you have verified the image matches the device, click ‘Force Upgrade’ and continue. The warning will not be shown again for future upgrades.

12 Revision History

Release Number	Release Date	Release Notes
01	12/01/2021	• Initial release
02	12/02/2022	• Update for firmware release 1.3
03	04/03/2022	• IPERF Traffic Setup • Added Tools > HaLow Firmware Upgrade
04	05/10/2022	• Updated for the LuCI interface • Added in EKH01
05	10/10/2022	• Improved formatting and reworded some sections for clarity. • Added UI Configuration architecture
06	20/10/2022	• Added example of how to run wavemon for basic HaLow testing
07	18/10/2022	Add description of key setup scenarios, and refactored configuration to match these. • Removed references to custom configurations, and manual configuration except where not available in UI. • Other general improvements
08	22/11/2022	• Updated device images
09	12/12/2022	• Updated formatting and cover page image
10	6/01/2023	• Updated for UCI configuration • Updated default IP address to 10.42.0.1
11	27/02/2023	• Correct some typos
12	02/06/2023	• Update for new HaLow configuration page • Update for new EasyMesh feature • Update for new Video UI feature • Update for adding internet connectivity
13	03/11/2023	• General update and 1st release to Doc. Control
14	12/12/2023	• Updated for 2.4.4 release
15	7/03/2024	• Updated for 2.5.0 release

Release Number	Release Date	Release Notes
16	21/03/2024	• Updated for 2.5.2 release
17	28/03/2024	• Updated LED flash pattern for button presses (section 2.2.1)
18	02/08/2024	• Updated for 2.6 release
19	17/12/2024	• Updated for 2.7 release • Updated EKH03 LED changes • Added LTE features section
20	20/12/2024	• Updated for 2.7.1 release • Added Range Testing section

Morse Micro
reaching farther™