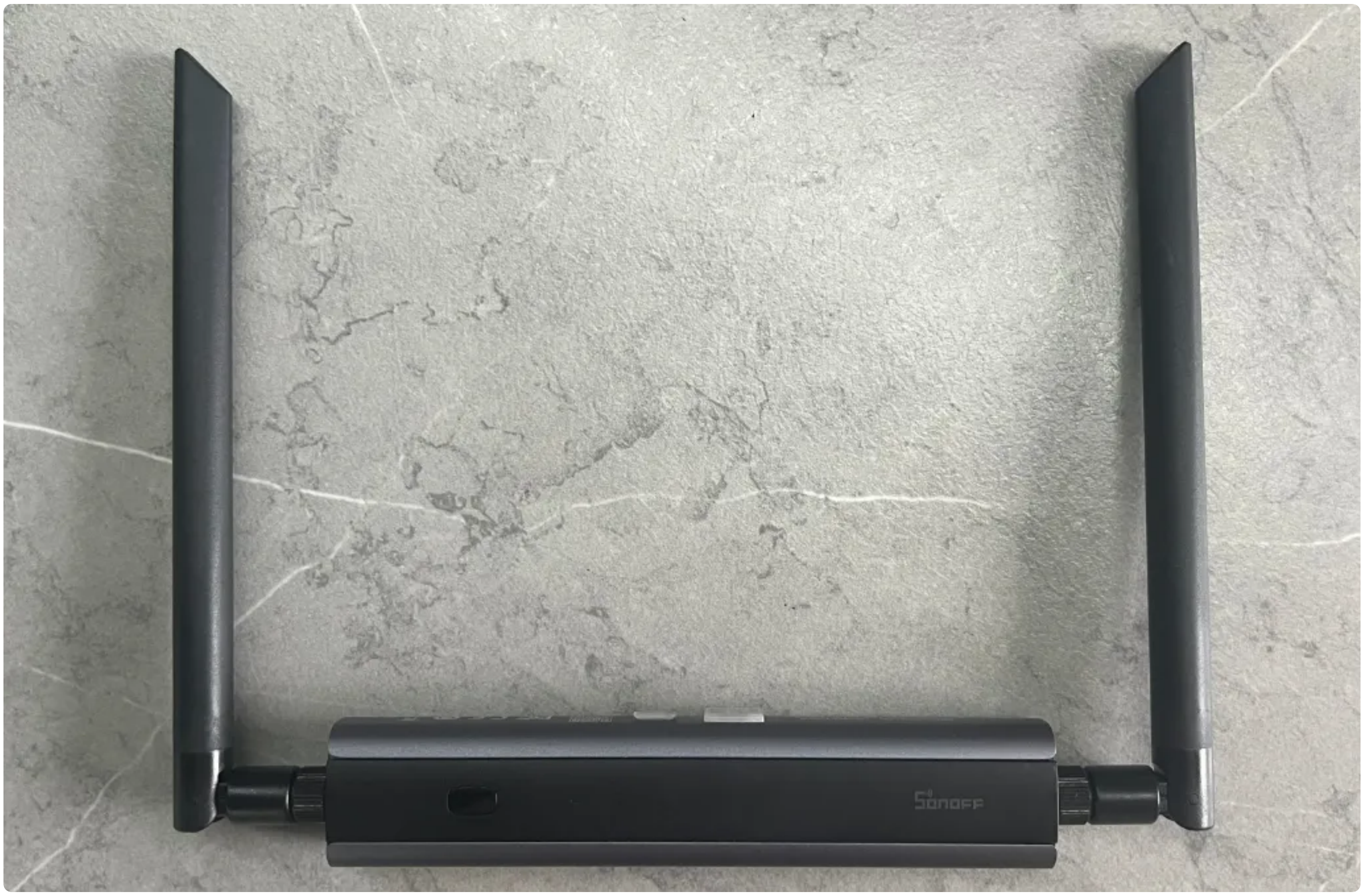
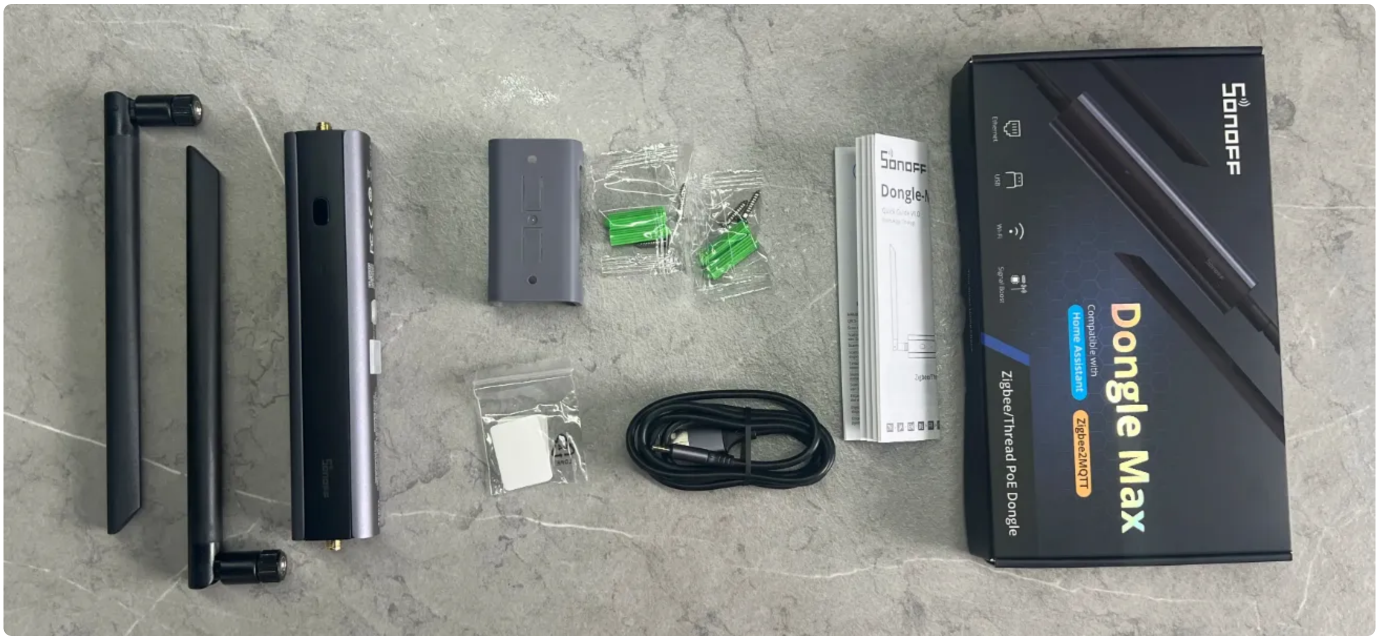
Dongle Max User Manual

Product Introduction

SONOFF Dongle Max (Hereinafter referred to as **Dongle-M**) is a Zigbee gateway developed based on ESP32D0+EFR32MG24, designed to connect Zigbee sub-devices to open-source platforms like Home Assistant and Zigbee2MQTT. It supports POE power supply and offers multiple connectivity options, making it adaptable to various usage scenarios.

Product Appearance





Package Contents

- Zigbee/Thread POE Dongle x1
- Bracket x 1
- Antenna x 2

- Double–sided tape x 2
- Screw accessory package x 2
- USB type–C cable (1m) x 1
- Quick guide x 1

Product Usage

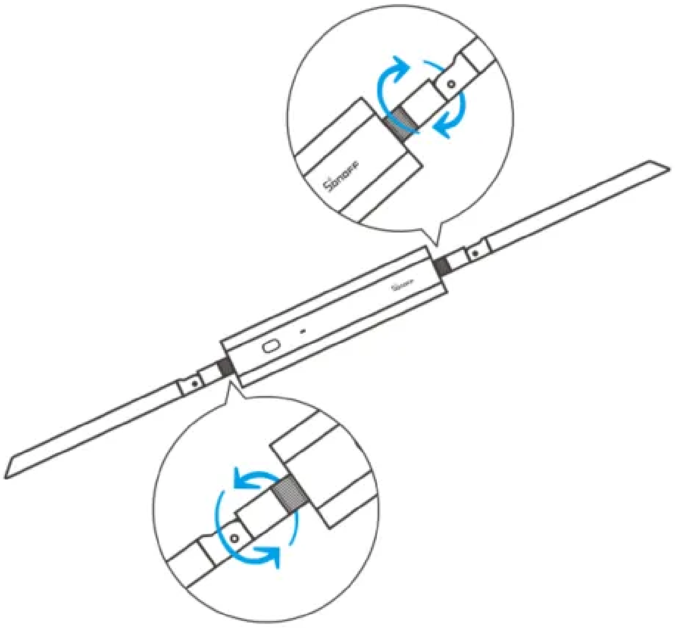
Step Overview

For first–time use, you can refer to the steps below to track your setup progress.

Step	Ethernet Method	Wi–Fi Method	USB Method
1	Install Antenna		
2	Ethernet Power and Connection	Wi–Fi Power and Connection	USB Power and Connection
3	Access the WEB Console		/
4	TCP Configuration to Open–source Platform		USB Configuration to Open–source Platform
5	Fixed the Device		

Step 1 Antenna Installation

The package includes two antennas, which should be attached to the left and right sides of the device respectively.



Step 2 Power Supply and Connection

Before installation, please choose a suitable connection method based on your usage habits or scenario:

Plan	Connection Method	Suitable Scenarios
A	Ethernet Connection	For environments with extendable network cables and LAN access, such as living rooms or bedrooms; or for utilizing idle Ethernet cables to achieve full–house coverage, such as in warehouses.
B	Wi–Fi Connection	When the device is not close to the host and there is no available Ethernet cabling. Ideal for rooms requiring flexible placement, such as bedrooms.

B	USB Connection	Close to the host device, connected via USB cable. Suitable for placement together with the host at a central home location, such as the living room.

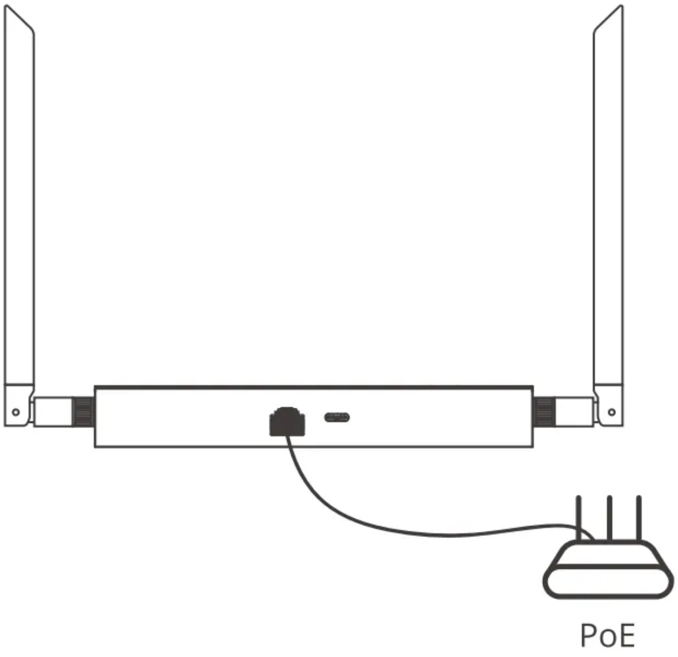
Plan A: Ethernet Connection

Device Power Supply

Before powering on the device, please check whether your router or switch supports PoE (Power over Ethernet).

- If supported, refer to the **PoE Power Supply** section below.
- If not supported, refer to the **Ethernet + Type-C Power Supply** section.

PoE Power Supply



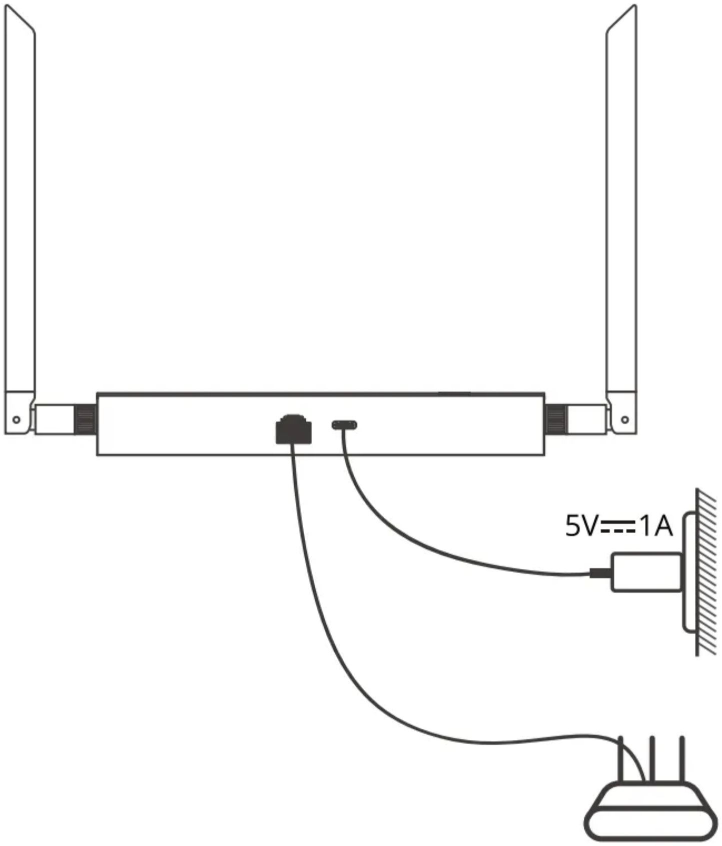
1. Connect the device to a PoE-enabled router, switch, or PoE power module using an RJ45 Ethernet cable. This completes the power connection.

2. Once powered on, the device indicator will remain **solid orange**, indicating that the device is receiving power properly.

   ⚠ **Note**: If using PoE power supply, ensure that your router or switch supports PoE. If your current network equipment does not support it, you may purchase a separate PoE power module to enable this functionality.

   If PoE power is not available, please supply power to the device via the Type–C port.

Ethernet + Type–C Power Supply



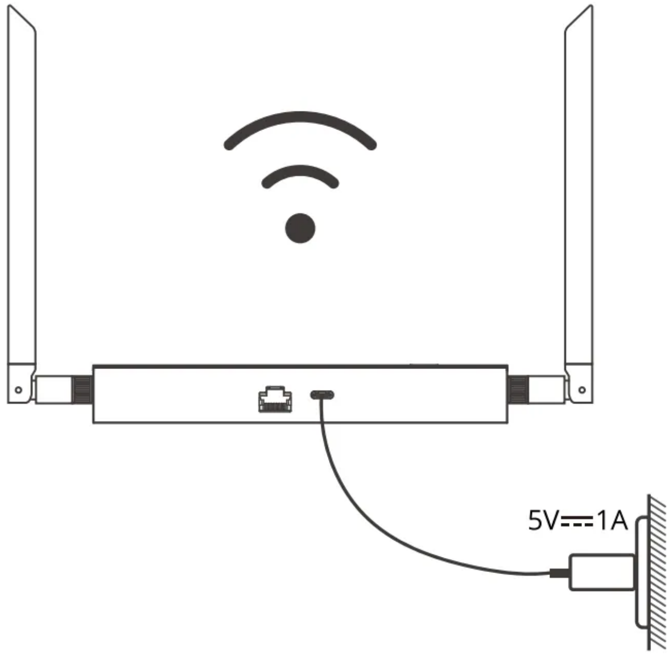
1. Use a Type–C charging cable: connect one end to the device's Type–C port, and the other end to a power adapter. Plug an RJ45 Ethernet cable into the network port and connect it to the router.
2. Once powered on, the device indicator will remain **solid orange**, indicating that the device is receiving power properly.

Connecting to the Router

1. After powering on, the device will attempt to connect to the router. When the indicator turns **solid blue**, the device is online.

2. Connect your mobile phone or computer to the same local network, and access the WEB console by entering the default domain `Dongle-M.local` in your browser. Once the page loads successfully, the WEB functions are ready to use.

Plan B: Wi-Fi Connection



Use a Type-C charging cable: connect one end to the device's Type-C port, and the other end to a power adapter. Plug an RJ45 Ethernet cable into the network port and connect it to the router.
Once powered on, the device indicator will remain solid orange, indicating that the device is receiving power properly.

Connecting to the Router

Before connecting to the router, you may choose a setup method based on your router's capabilities:

- For all router types: refer to the **AP Hotspot Configuration** section.
- If your router supports WPS: refer to the **WPS Configuration** section.

AP Hotspot Configuration

1. The device's AP hotspot is enabled by default when powered on. On your PC or mobile device, search for the AP SSID such as `SONOFF_Dongle-M_XXXX` . The first connection

does not require a password.
If no connection is made within 10 minutes, the AP hotspot will automatically shut down. Press the button to re-enable it.

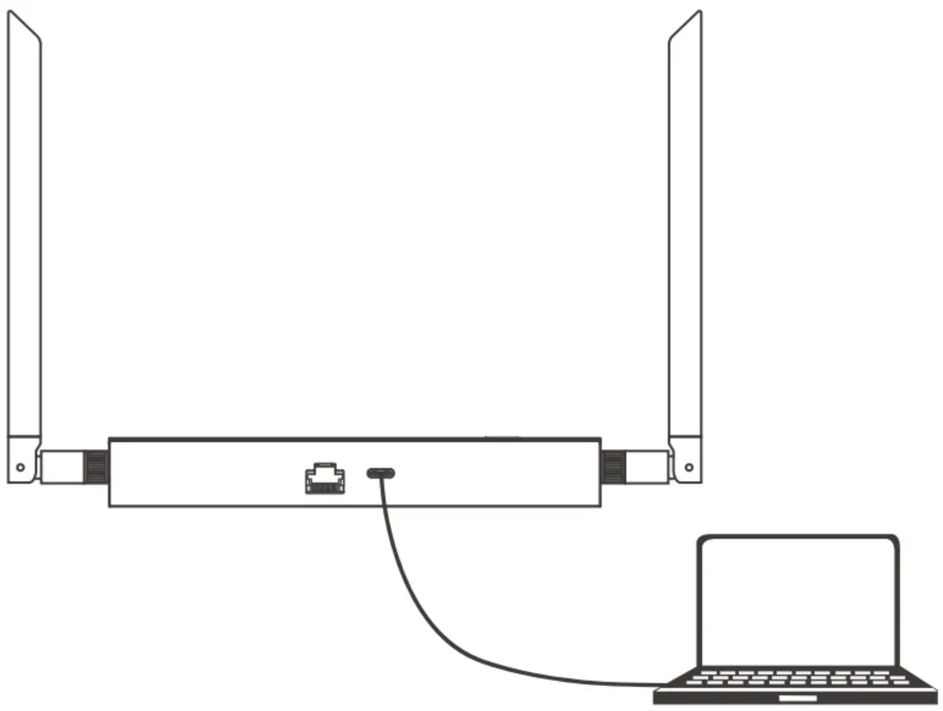
2. After connecting to the AP hotspot, the browser will automatically open the WEB interface. You will be prompted to set a password for WEB access. After configuration, the page will close and you must reconnect to the AP hotspot using the password you just set.
   If the browser does not open automatically, you can access the page manually via the default domain `Dongle-M.local`*.*
3. Re-enter the WEB interface, go to **Network Settings** on the left, select **WLAN Settings**, choose the appropriate Wi-Fi network, and connect.
4. Wait for the device to connect to the router. When the indicator turns **solid blue**, the device is online.
5. Connect your phone or PC to the same LAN, and access the WEB console by visiting `Dongle-M.local` in your browser. Once accessed successfully, you can use all WEB functions.

WPS Configuration

1. If your router supports WPS, press the WPS button on the router to start the pairing process.
2. Press the button on the Dongle-M once to enter WPS mode. The indicator will flash orange.
3. Wait for the device to connect to the router. If the connection is successful within 30 seconds, the indicator will turn **solid blue**, indicating the device is online.
4. Connect your phone or PC to the same LAN, and access the WEB console by visiting **`Dongle-M.local`** in your browser. Once accessed successfully, you can use all WEB functions.

Plan C: USB Connection

Device Power Supply



Use a Type-C charging cable: connect one end to the device's Type-C port, and the other end to the host device.
Once powered on, the device indicator will remain **solid orange**, indicating that the device is receiving power properly.

At this point, you may proceed to the **Accessing the Operating System** section for the next steps.

Step 3 Access the WEB Console

The device supports the following methods to access the WEB console via **Ethernet connection** and **Wi-Fi connection**:

Access Method	Description
Default URL	Connect to the same LAN as the device, then enter the default domain `Dongle-M.local` in the browser.
IP Address Access	Check the device's IP address in your router's management page, then enter the IP address in the browser.

Custom URL	If not your first login and you have configured the mDNS hostname in the WEB console––settings––mDNS Hostname, you can access it via the custom URL.

Set Login Password (Required)

On first use, you must set a password with at least 8 characters.
If using AP Hotspot Configuration, you will need to reconnect to the AP hotspot after changing the password, using the newly set password.

Configure Wireless Network (Optional)

You can add a 2.4GHz wireless network under **Network Settings → WLAN Connection**.
If both Ethernet and Wi-Fi are connected, the Ethernet connection will take priority.

Firmware Upgrade

You can perform a firmware upgrade under WEB console––**Firmware**.
It is recommended to upgrade the device to the latest stable firmware version before using Dongle-M to ensure optimal performance.

Step 4 Connecting to Operating System

Connecting to Z2M

1. Use the USB extension cable included with the Dongle-M to connect it as a Zigbee adapter for Zigbee2MQTT integration.

For example, in Home Assistant, following the steps:

1. Navigate to Settings > System > Hardware > All Hardware.

2. Search for "ttyUSB".

3. Copy the serial device path (e.g. /dev/ttyUSBx) or ID path (e.g. /dev/serial/by-id...).

serial:

```
port: <Device path, e.g. /dev/ttyUSBx> or <ID, e.g. /dev/serial/by-id...>
baudRate: 115200
adapter: ember
```

2. Network (TCP) Connection: Set up Zigbee2MQTT integration remotely over Wi-Fi or Ethernet using a TCP connection.

Using a hostname instead of an IP address is highly recommended to avoid unexpected disconnections if the IP changes.

serial:

```
port: tcp://Dongle-M.local:6638
baudRate: 115200
adapter: ember
```

Connecting to ZHA

1. Use the USB extension cable included with the Dongle-M to connect it as a Zigbee adapter for ZHA integration.

1.1 Auto-discovery: ZHA automatically discovers the Dongle-M and its device path during integration setup.

1.2 Manual Setup: If auto-discovery fails, enter the device path from Hardware settings, following the steps:

1. Navigate to Settings > System > Hardware > All Hardware.

2. Search for "ttyUSB".

3. Copy the serial device path (e.g. /dev/ttyUSBx) or ID path (e.g. /dev/serial/by-id...).

```
Radio Type: EZSP
Serial device path: <Device path, e.g. /dev/ttyUSBx> or <ID, e.g. /dev/serial/by-id...>
baudRate: 115200
Data flow control: software
```

2. Network (TCP) Connection: Set up ZHA integration remotely over Wi-Fi or Ethernet using a TCP connection.

2.1 Auto-discovery: ZHA automatically discovers the Dongle-M and its device path during integration setup.

2.2 Manual Setup: If auto-discovery fails, enter the device path from Hardware settings, following the steps:

1. Navigate to Settings > System > Hardware > All Hardware.

2. Search for "ttyUSB".

3. Copy the serial device path (e.g. /dev/ttyUSBx) or ID path (e.g. /dev/serial/by-id...).

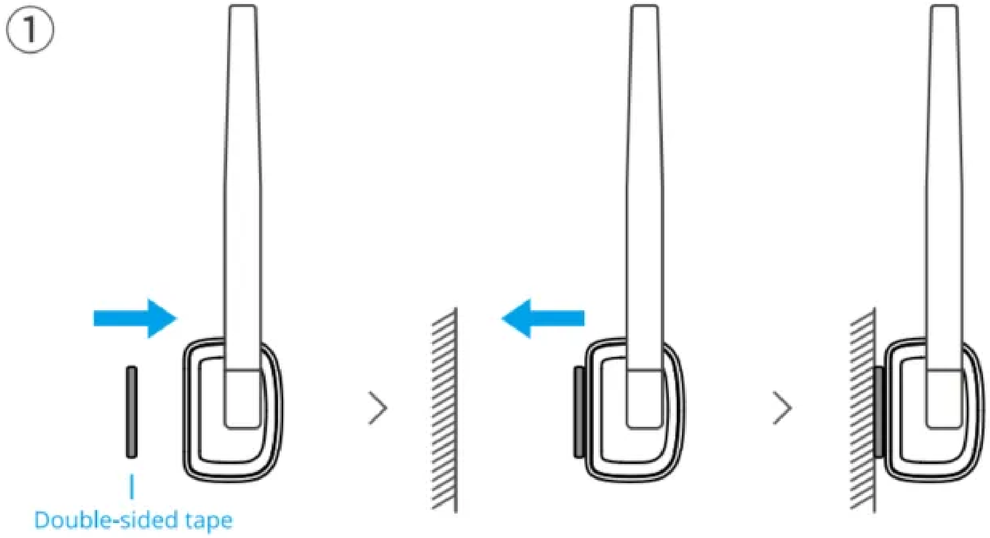
Note: Using a hostname instead of an IP address is highly recommended to avoid unexpected disconnections if the IP changes.

```
dio Type: EZSP
Serial device path: socket://Dongle-M.local:6638
Port speed: 115200
Data flow control: software
```

Step 5: Fixed the Device

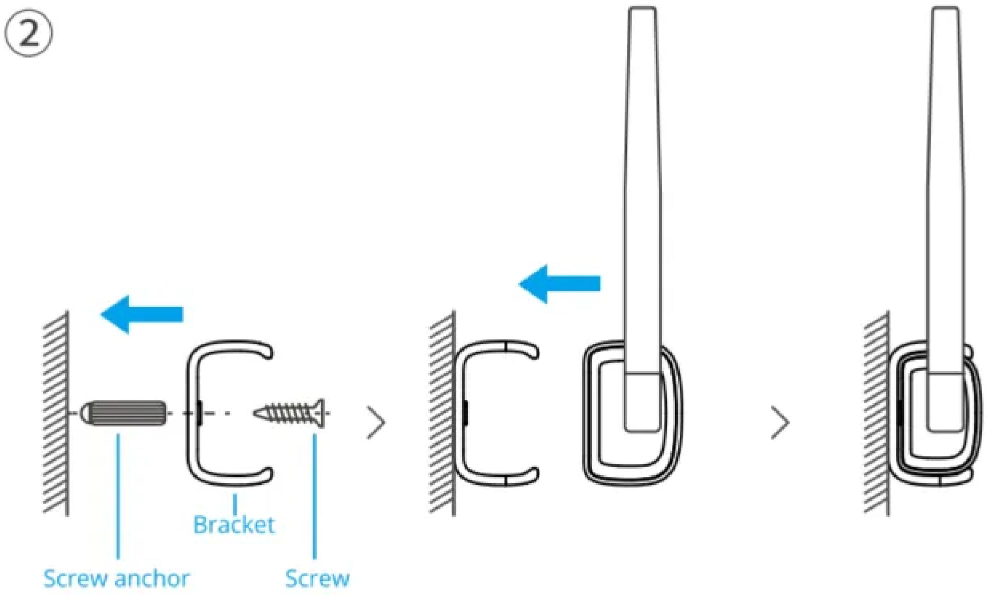
Once the device is functioning properly, you can choose one of the following methods to fixed it:

1. **Adhesive Installation**
   Use the included double-sided adhesive tape to attach the device to a flat surface.



2. **Bracket Installation**

Use screws to secure the bracket, then mount the device onto the bracket.

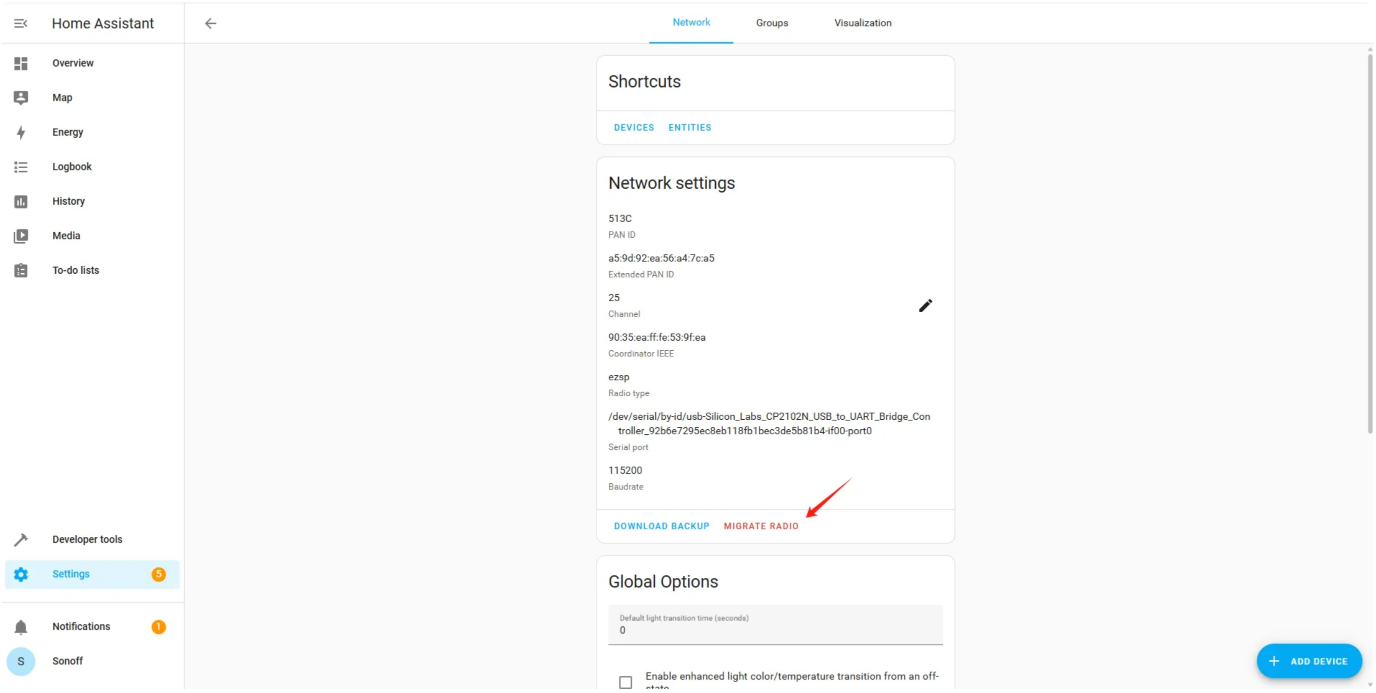


Feature Guide

Migrate from one adapter to another（Optional)

Migrating involves risks, which may lead to the need to re-pair zigbee devices. You can decide whether to proceed with the migration at your own discretion.

- In ZHA, you can migrate via the **"Migrate Radio"**.



Shortcuts

Network settings

513C
PAN ID

a5:9d:92:ea:56:a4:7c:a5
Extended PAN ID

25
Channel

90:35:ea:ff:fe:53:9f:ea
Coordinator IEEE

ezsp
Radio type

/dev/serial/by-id/usb-Silicon_Labs_CP2102N_USB_to_UART_Bridge_Controller_92b6e7295ec8eb118fb1bec3de5b81b4-if00-port0
Serial port

115200
Baudrate

Global Options

Default light transition time (seconds)
0

□ Enable enhanced light color/temperature transition from an off-state

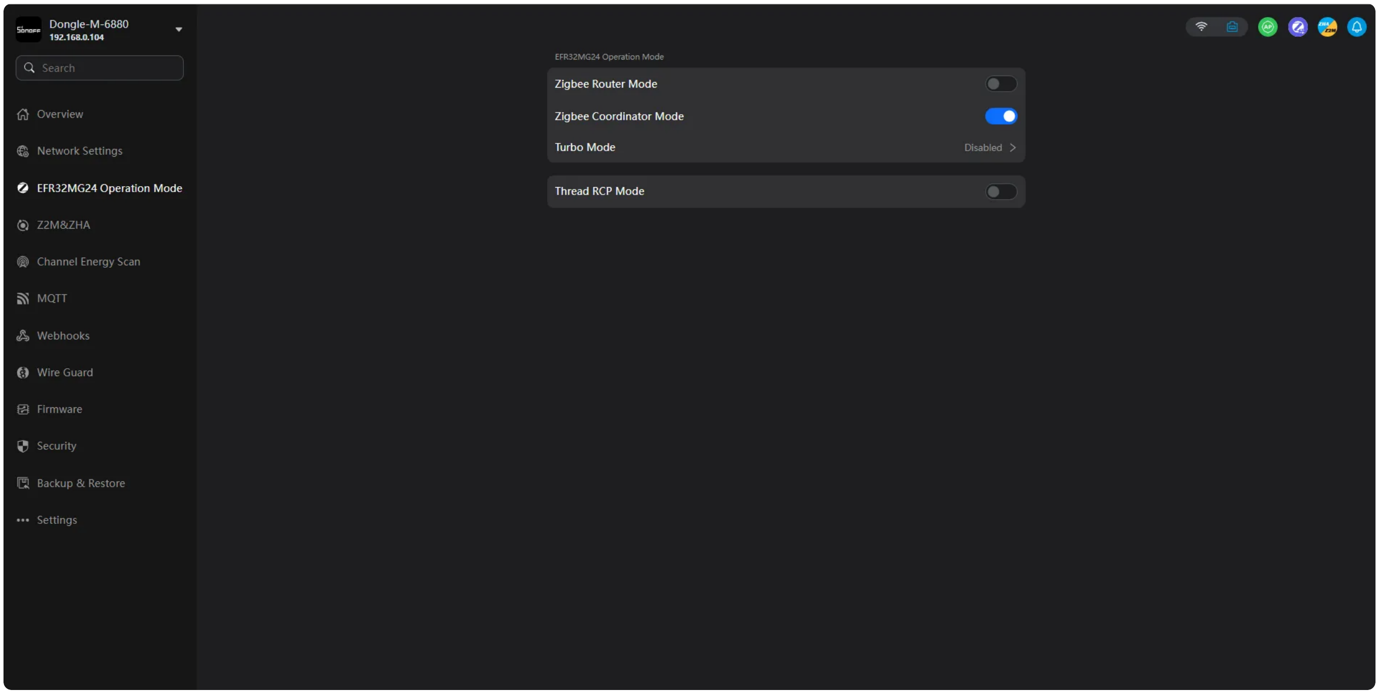
- In Z2M, please refer to the following link for detailed information and operation procedures:

https://www.zigbee2mqtt.io/guide/faq/#how-do-i-migrate-from-one-adapter-to-another

Switch Operation Mode

You can switch the device's operating mode under **ESP32MG24 Operation Mode**.

For example, you can configure it to function as a **Zigbee Coordinator, Zigbee Router** or switch to **Thread RCP firmware**.



EFR32MG24 Operation Mode

Zigbee Router Mode ○

Zigbee Coordinator Mode ●

Turbo Mode Disabled >

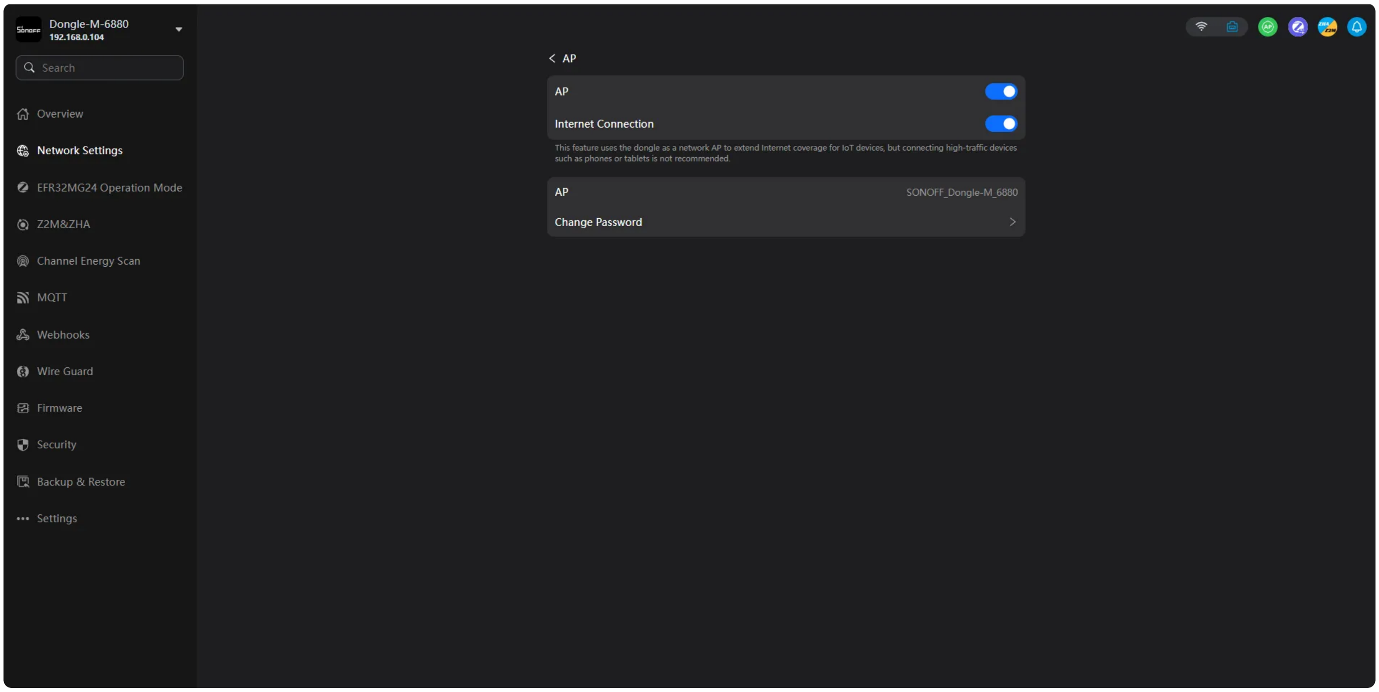
Thread RCP Mode ○

Enable Device AP Hotspot

After enabling the AP hotspot, the device can function similarly to a Wi-Fi router, providing network access for up to 8 IoT devices.

Under **Network Settings -- AP**, you can enable the device’s AP and configure the SSID and password.

Once configured, your IoT devices can connect to this AP hotspot.



< AP

AP ●

Internet Connection ●

This feature uses the dongle as a network AP to extend Internet coverage for IoT devices, but connecting high-traffic devices such as phones or tablets is not recommended.

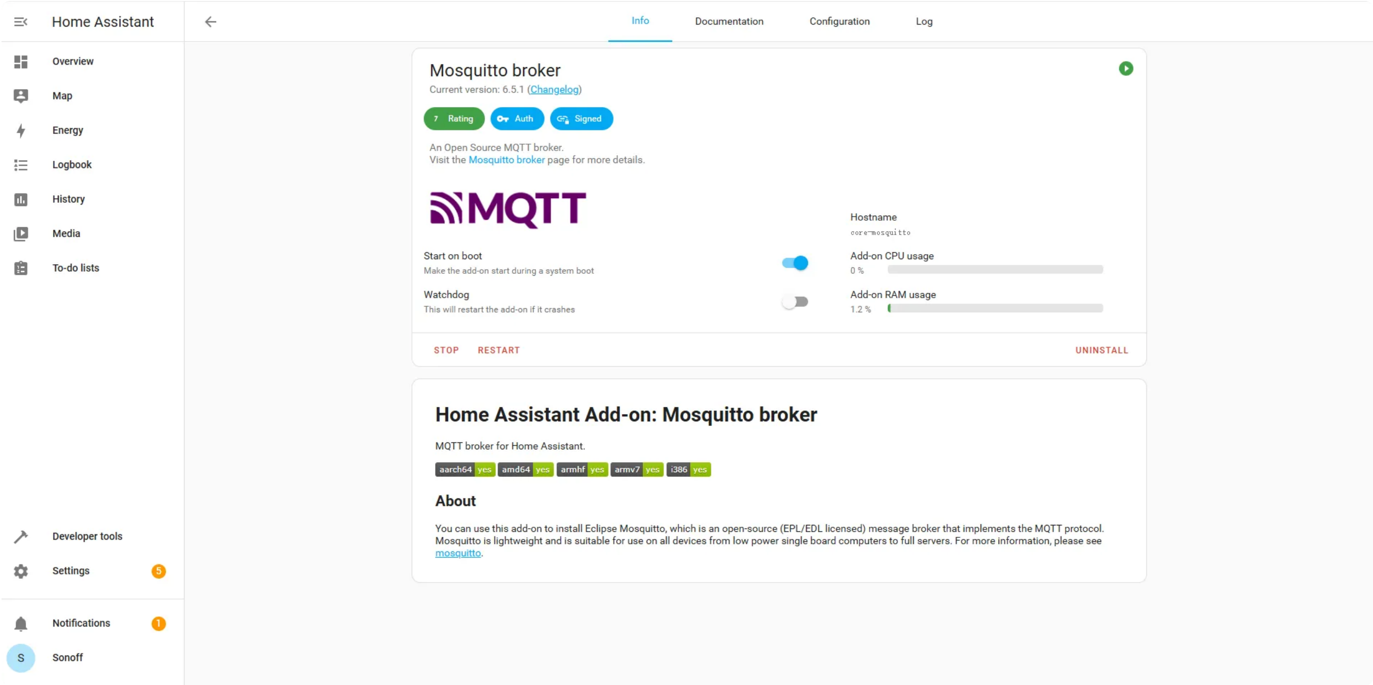
AP SONOFF_Dongle-M_6880

Change Password >

MQTT Settings

1. Configure Mosquitto Broker

1. **Install the Mosquitto Add-on**
   In HA's management interface, go to **Settings → Add-ons → Add-on Store**, search for and install the **Mosquitto broker** add-on. After installation, click **Start** and ensure the add-on runs normally.



Mosquitto broker

Current version: 6.5.1 (Changelog)

An Open Source MQTT broker.
Visit the Mosquitto broker page for more details.

Start on boot
Make the add-on start during a system boot

Watchdog
This will restart the add-on if it crashes

Hostname
core-mosquitto

Add-on CPU usage
0 %

Add-on RAM usage
1.2 %

Home Assistant Add-on: Mosquitto broker

MQTT broker for Home Assistant.

About

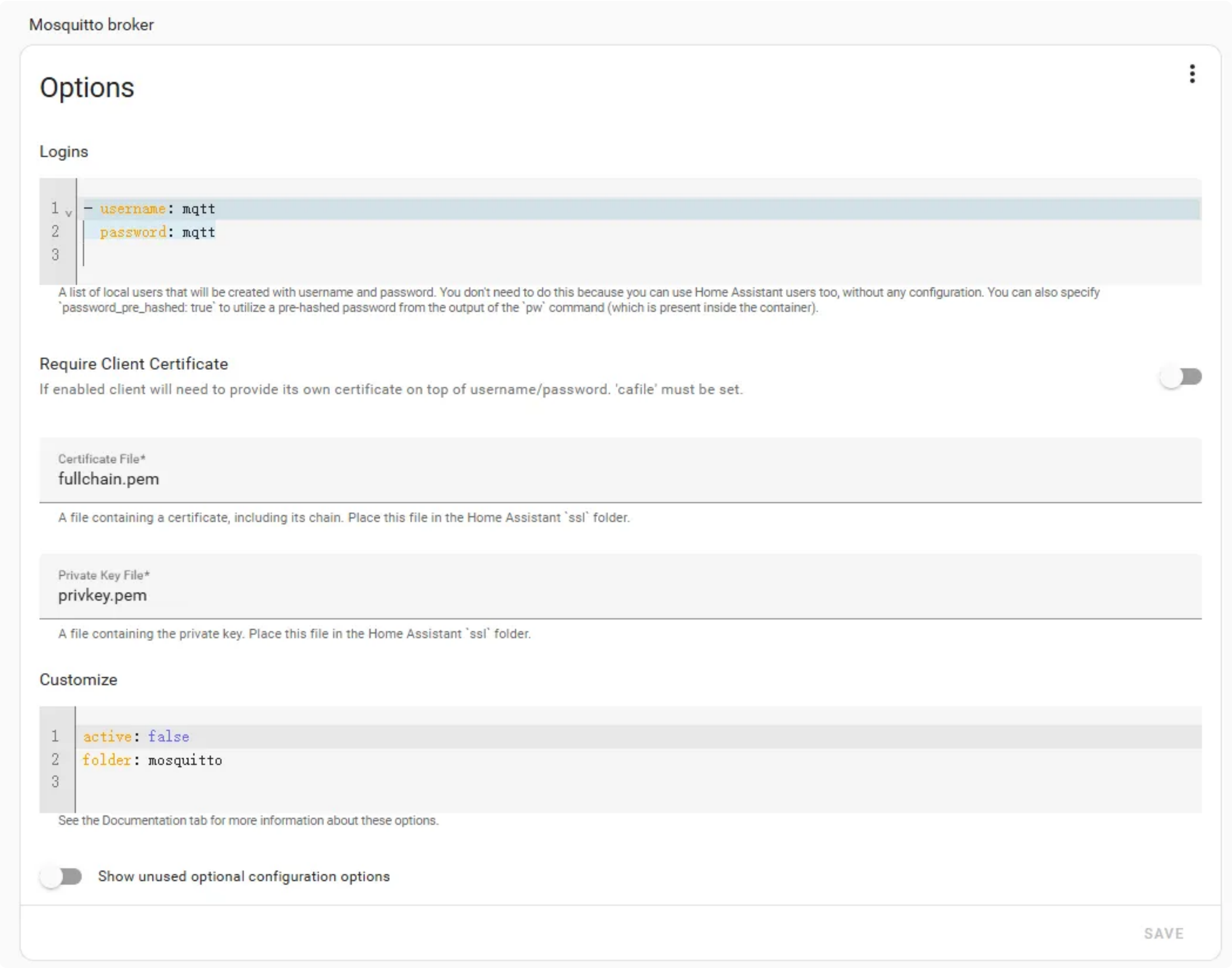
You can use this add-on to install Eclipse Mosquitto, which is an open-source (EPL/EDL licensed) message broker that implements the MQTT protocol. Mosquitto is lightweight and is suitable for use on all devices from low power single board computers to full servers. For more information, please see mosquitto.

2. **Set Username and Password**

   In the Mosquitto add-on configuration page, refer to the following settings to edit (example):

```
- username: mqtt
  password: mqtt
```

Save the changes and restart the add-on.



Mosquitto broker

Options

Logins

```
- username: mqtt
  password: mqtt

```

A list of local users that will be created with username and password. You don't need to do this because you can use Home Assistant users too, without any configuration. You can also specify `password_pre_hashed: true` to utilize a pre-hashed password from the output of the `pw` command (which is present inside the container).

Require Client Certificate

If enabled client will need to provide its own certificate on top of username/password. 'cafile' must be set.

Certificate File*

fullchain.pem

A file containing a certificate, including its chain. Place this file in the Home Assistant `ssl` folder.

Private Key File*

privkey.pem

A file containing the private key. Place this file in the Home Assistant `ssl` folder.

Customize

```
active: false
folder: mosquitto

```

See the Documentation tab for more information about these options.

Show unused optional configuration options

2. Configure Dongle-M to Connect to Mosquitto

1. **Get Mosquitto Server Information**

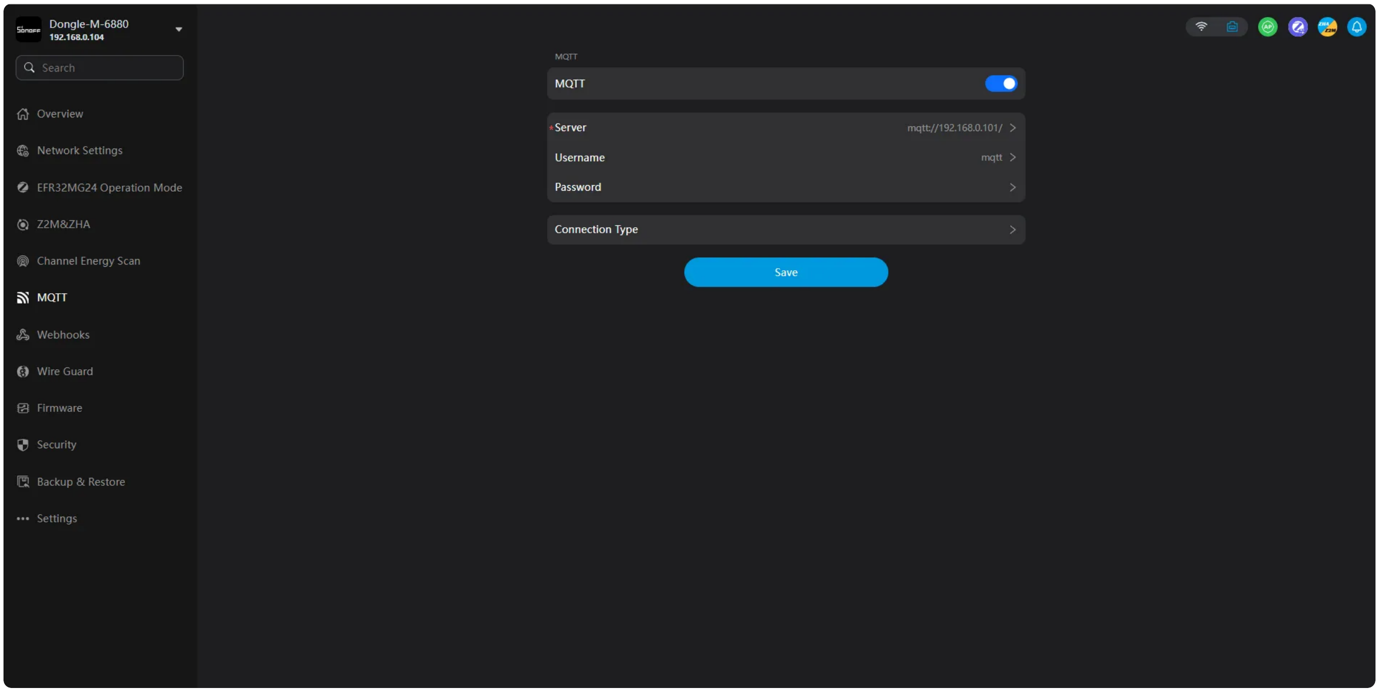
   Record the Mosquitto server address (usually the HA host's IP, e.g., `192.168.1.100`) .

2. **Set Dongle-M Parameters**

   In Dongle-M's configuration interface, enter:

   - **Server Address**: mqtt://HA host IP (e.g. `mqtt://192.168.1.100`)
   - **Username**: `mqtt`
   - **Password**: `mqtt`

     Save the settings. Verify that Dongle-M connects successfully via Mosquitto logs or a client tool (e.g., MQTT Explorer).



MQTT

MQTT: on

Server: mqtt://192.168.0.101/

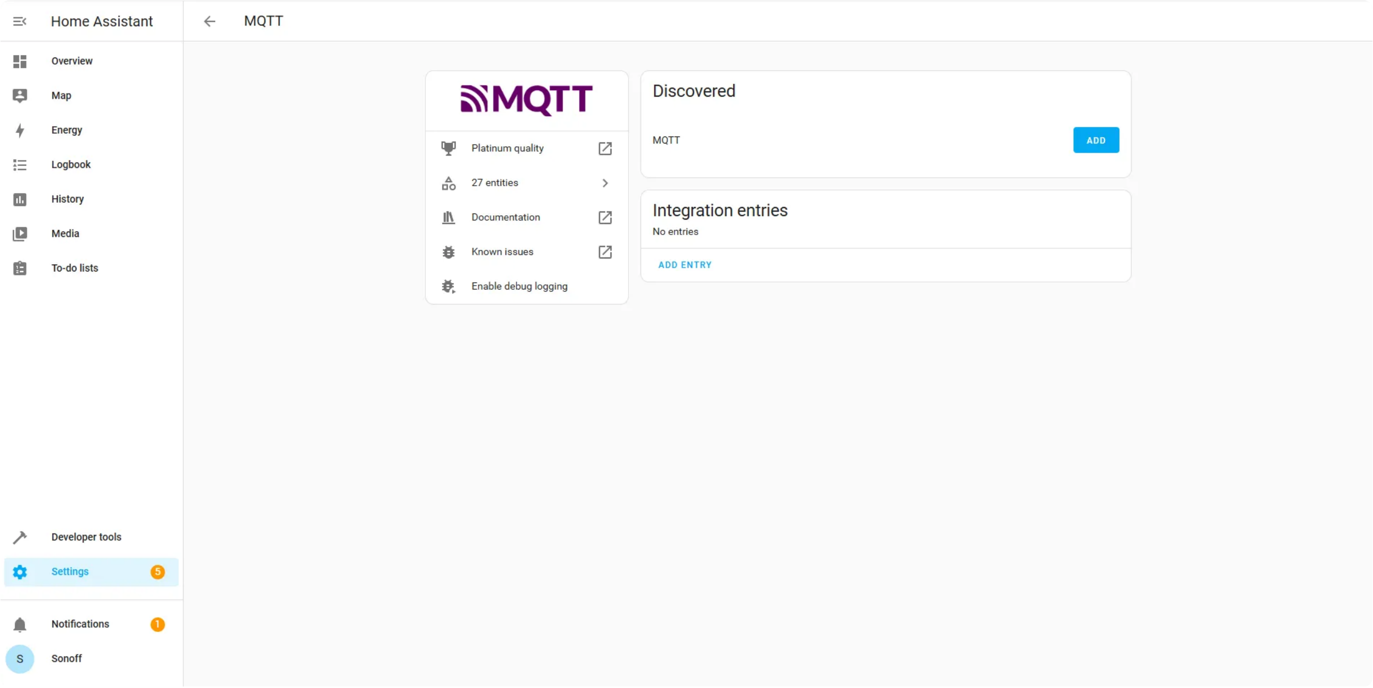
Username: mqtt

Password

Connection Type

3. Add MQTT Integration in HA

Go to **Settings → Devices & Services → Add Integration**, search for and select **MQTT**. Dongle-M can be automatically found in it, and click **ADD** to add it.



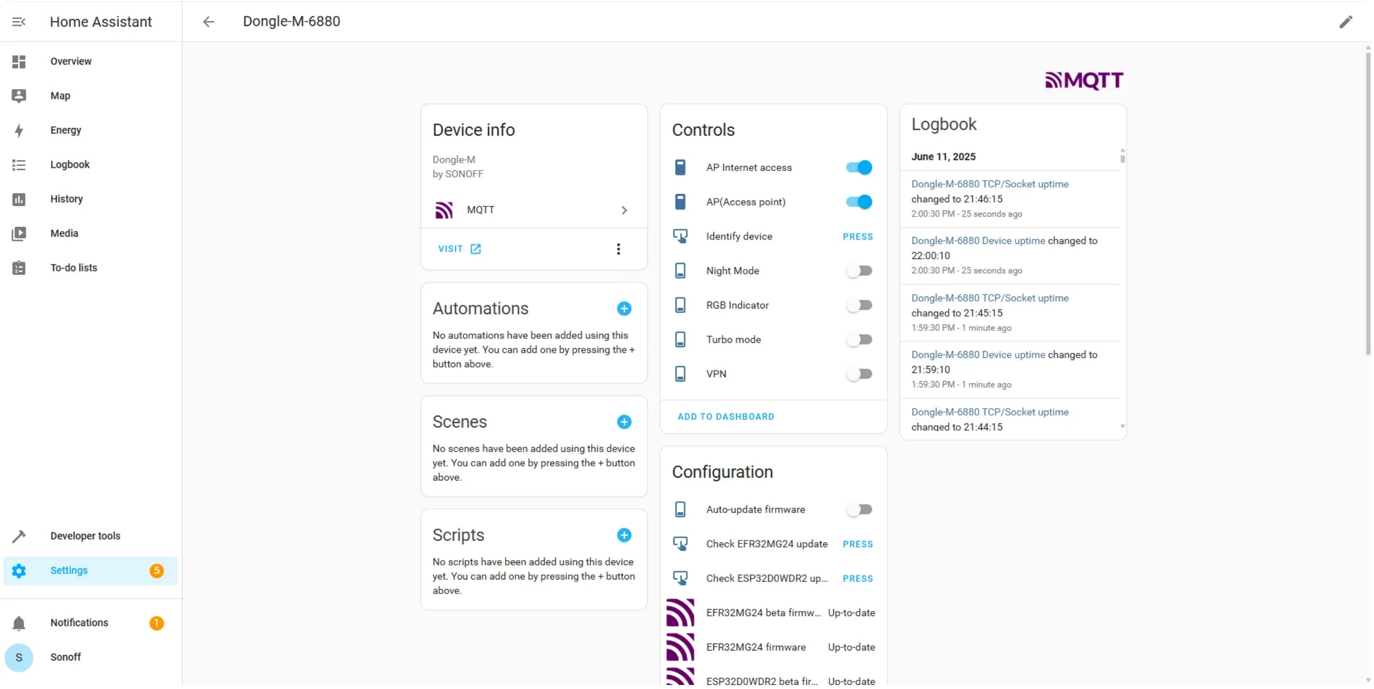
Discovered

MQTT

Integration entries

No entries

Once completed, you can control the multiple selection settings of Dongle-M in HA.



Device info

Dongle-M
by SONOFF

MQTT

VISIT

Automations

No automations have been added using this device yet. You can add one by pressing the + button above.

Scenes

No scenes have been added using this device yet. You can add one by pressing the + button above.

Scripts

No scripts have been added using this device yet. You can add one by pressing the + button above.

Controls

- AP Internet access: on
- AP(Access point): on
- Identify device: PRESS
- Night Mode: off
- RGB Indicator: off
- Turbo mode: off
- VPN: off

ADD TO DASHBOARD

Configuration

- Auto-update firmware: off
- Check EFR32MG24 update: PRESS
- Check ESP32D0WDR2 up...: PRESS
- EFR32MG24 beta firmw...: Up-to-date
- EFR32MG24 firmware: Up-to-date
- ESP32D0WDR2 beta fir...: Up-to-date

Logbook

June 11, 2025

Dongle-M-6880 TCP/Socket uptime changed to 21:46:15
2:00:30 PM - 25 seconds ago

Dongle-M-6880 Device uptime changed to 22:00:10
2:00:30 PM - 25 seconds ago

Dongle-M-6880 TCP/Socket uptime changed to 21:45:15
1:59:30 PM - 1 minute ago

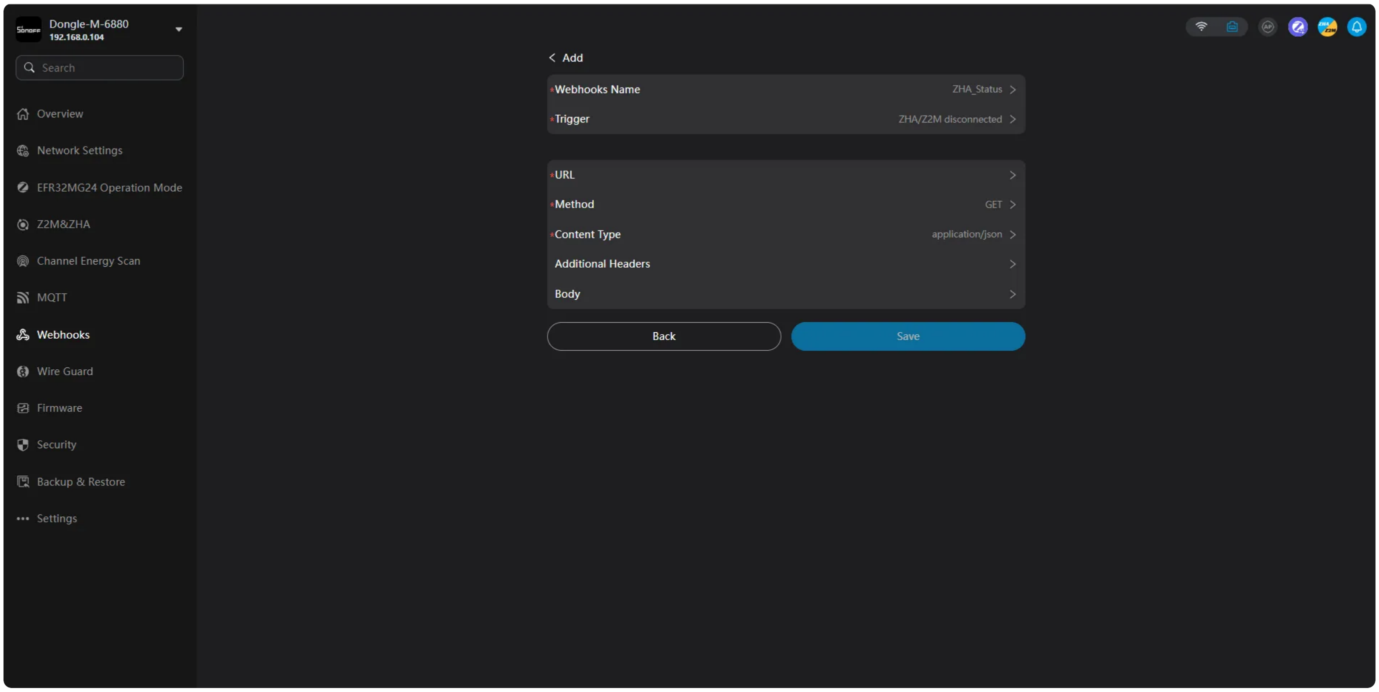
Dongle-M-6880 Device uptime changed to 21:59:10
1:59:30 PM - 1 minute ago

Dongle-M-6880 TCP/Socket uptime changed to 21:44:15

Webhooks

1. In **Webhooks**, click **Add** to create a webhook with various functionalities.
2. Set a name for the webhook, then choose a **trigger**. The following triggers are currently supported:

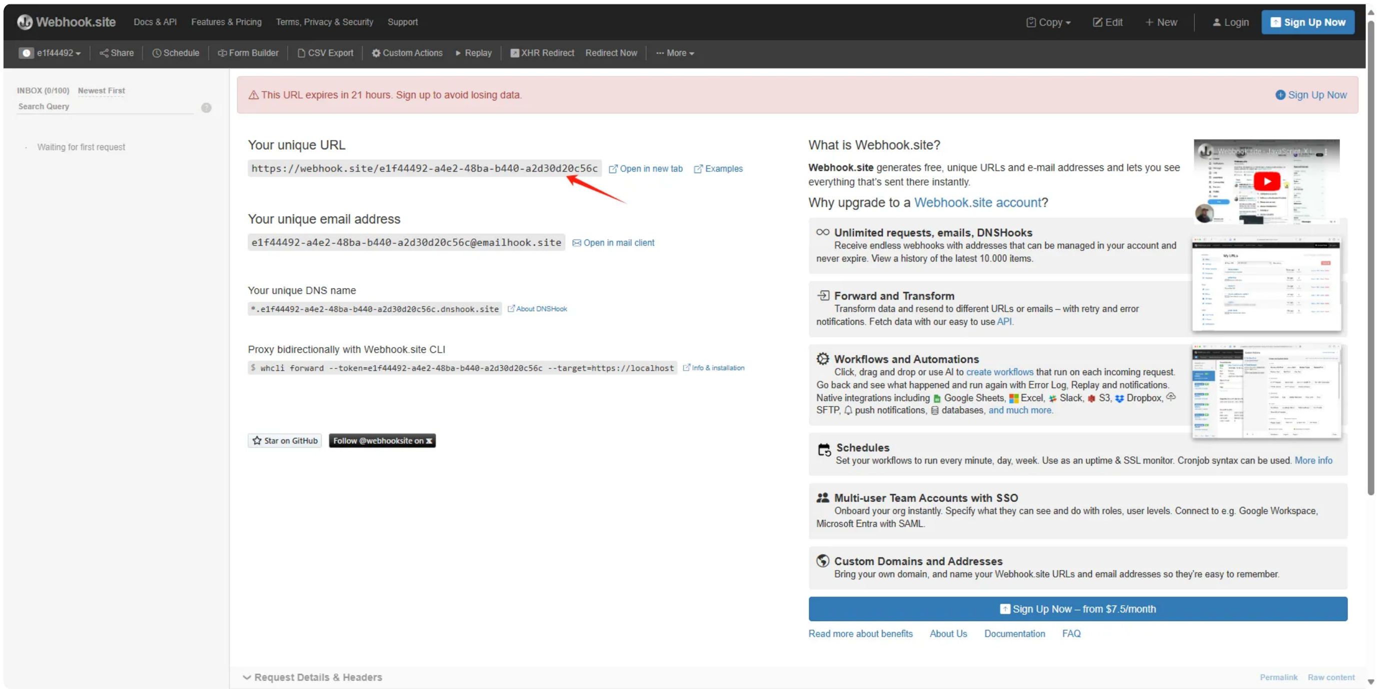
- ZHA/Z2M disconnected
- IP Address conflict
- Hostname conflict
- Channel energy scan
- Auto backup files



< Add

*Webhooks Name	ZHA_Status >
*Trigger	ZHA/Z2M disconnected >
*URL	>
*Method	GET >
*Content Type	application/json >
Additional Headers	>
Body	>

3. Specify the target **URL**. You can use any service that supports webhooks. In the following example, we use `webhook.site` — copy the unique URL provided and paste it into the configuration.



⚠ This URL expires in 21 hours. Sign up to avoid losing data.

Your unique URL

`https://webhook.site/e1f44492-a4e2-48ba-b440-a2d30d20c56c`

Your unique email address

`e1f44492-a4e2-48ba-b440-a2d30d20c56c@emailhook.site`

Your unique DNS name

`*.e1f44492-a4e2-48ba-b440-a2d30d20c56c.dnshook.site`

Proxy bidirectionally with Webhook.site CLI

```
$ whcli forward --token=e1f44492-a4e2-48ba-b440-a2d30d20c56c --target=https://localhost
```

What is Webhook.site?

Webhook.site generates free, unique URLs and e-mail addresses and lets you see everything that's sent there instantly.

Why upgrade to a Webhook.site account?

Unlimited requests, emails, DNSHooks
Receive endless webhooks with addresses that can be managed in your account and never expire. View a history of the latest 10.000 items.

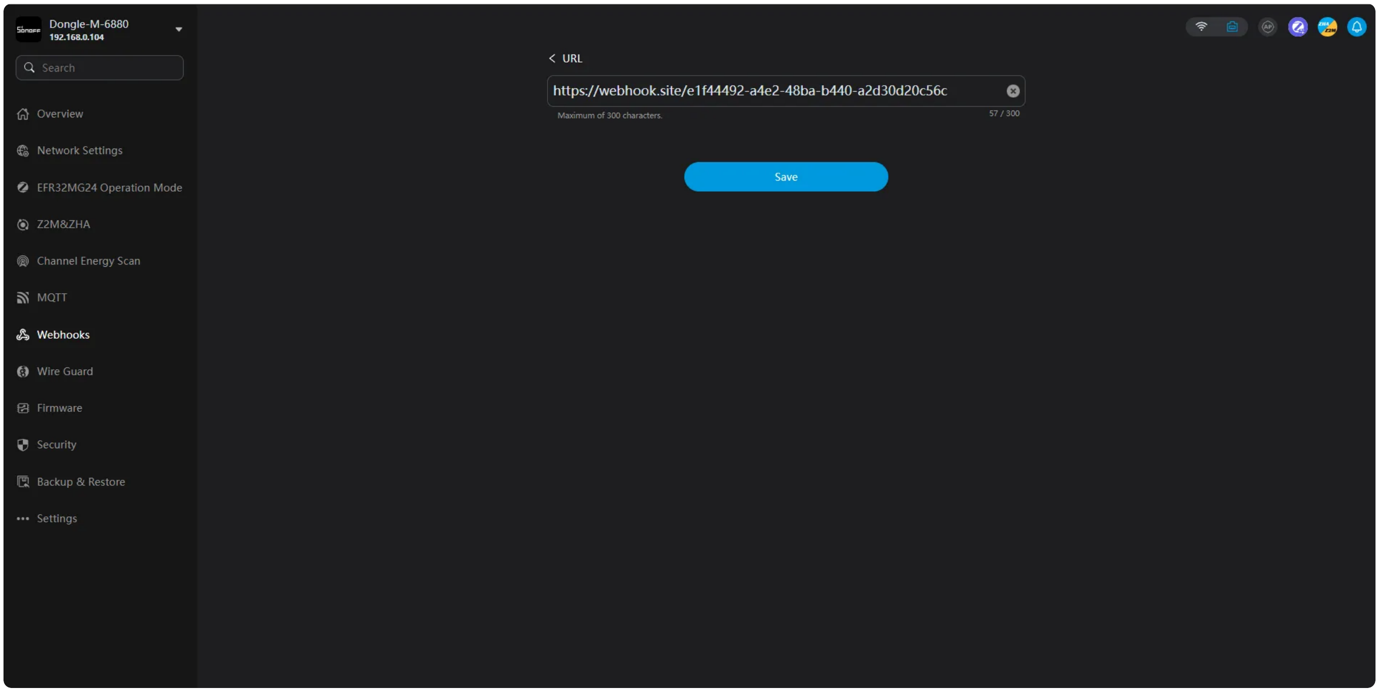
Forward and Transform
Transform data and resend to different URLs or emails – with retry and error notifications. Fetch data with our easy to use API.

Workflows and Automations
Click, drag and drop or use AI to create workflows that run on each incoming request. Go back and see what happened and run again with Error Log, Replay and notifications. Native integrations including Google Sheets, Excel, Slack, S3, Dropbox, SFTP, push notifications, databases, and much more.

Schedules
Set your workflows to run every minute, day, week. Use as an uptime & SSL monitor. Cronjob syntax can be used. More info

Multi-user Team Accounts with SSO
Onboard your org instantly. Specify what they can see and do with roles, user levels. Connect to e.g. Google Workspace, Microsoft Entra with SAML.

Custom Domains and Addresses
Bring your own domain, and name your Webhook.site URLs and email addresses so they're easy to remember.

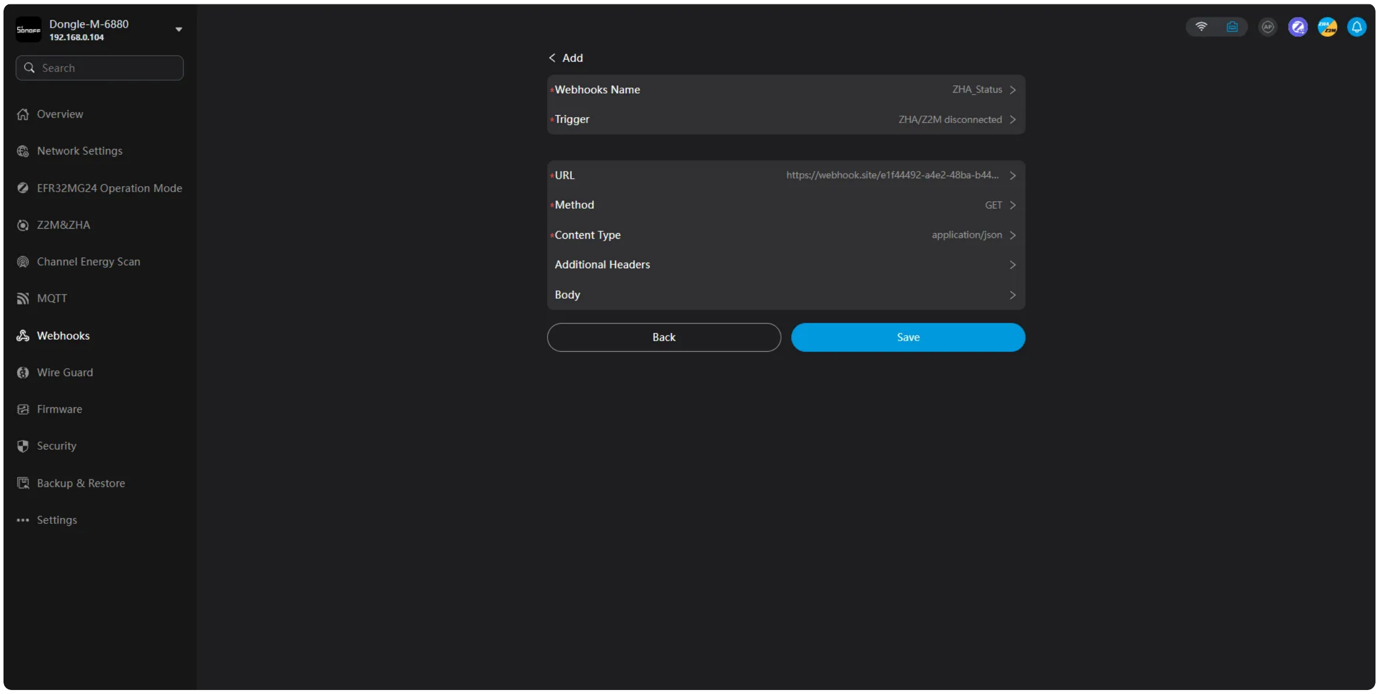


URL

https://webhook.site/e1f44492-a4e2-48ba-b440-a2d30d20c56c

Maximum of 300 characters. 57 / 300

4. After saving, the webhook will be ready for use.



Add

*Webhooks Name ZHA_Status

*Trigger ZHA/Z2M disconnected

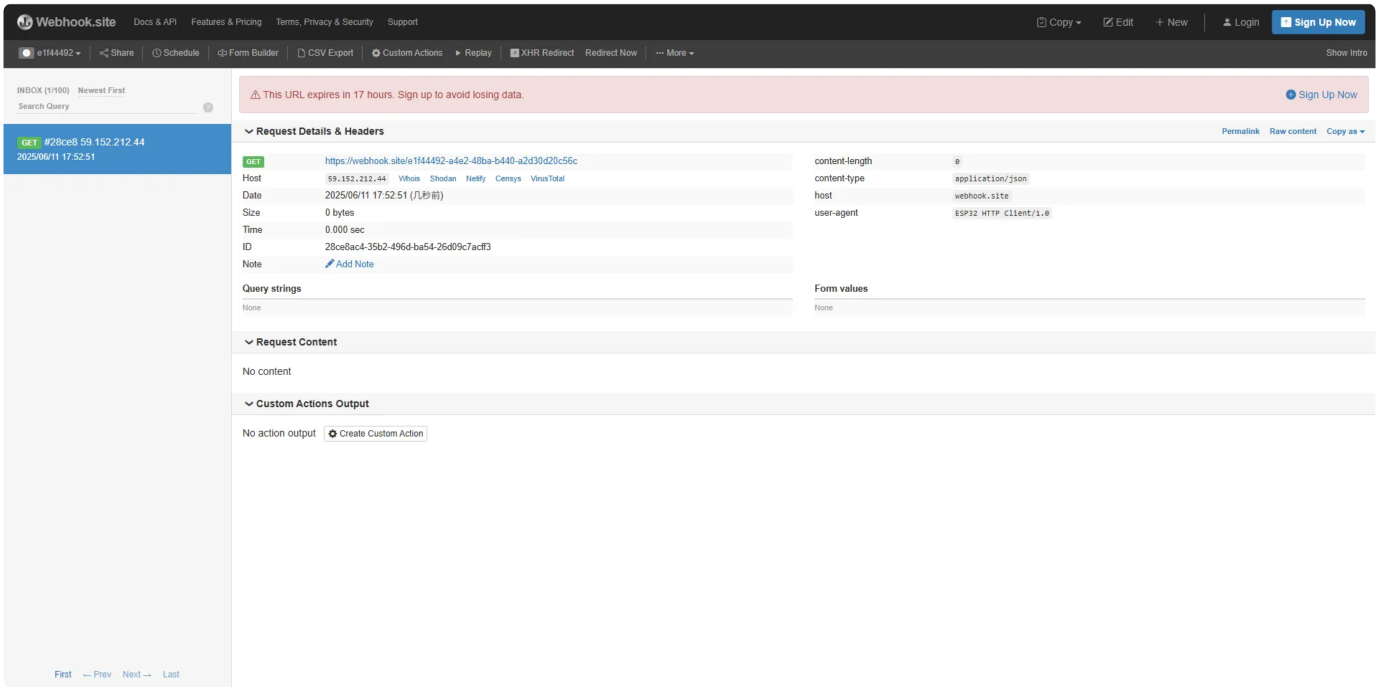
*URL https://webhook.site/e1f44492-a4e2-48ba-b44...

*Method GET

*Content Type application/json

Additional Headers

Body



GET #28ce8 59.152.212.44
2025/06/11 17:52:51

⚠ This URL expires in 17 hours. Sign up to avoid losing data.

Request Details & Headers

GET	https://webhook.site/e1f44492-a4e2-48ba-b440-a2d30d20c56c
Host	59.152.212.44 Whois Shodan Netify Censys VirusTotal
Date	2025/06/11 17:52:51 (几秒前)
Size	0 bytes
Time	0.000 sec
ID	28ce8ac4-35b2-496d-ba54-26d09c7acff3
Note	Add Note

content-length	0
content-type	application/json
host	webhook.site
user-agent	ESP32 HTTP Client/1.0

Query strings
None

Form values
None

Request Content

No content

Custom Actions Output

No action output

VPN Feature (Wire Guard)

Before configuring a WireGuard client on the Dongle-M, you must first set up your own WireGuard server.

For a reference guide on configuring a WireGuard server in Home Assistant, please refer to the following community add-on documentation:

Home Assistant Community Add-on: WireGuard