WiFi Pineapple Mark VII

WiFi Pineapple Documentation

The industry standard pentest platform has evolved. Equip your red team with the WiFi Pineapple® Mark VII. Newly refined. Enterprise ready.

> The e-book PDF generated by this document may not format correctly on all devices. For the most-to-date version, please see https://docs.hak5.org

Setup

Setting up your WiFi Pineapple

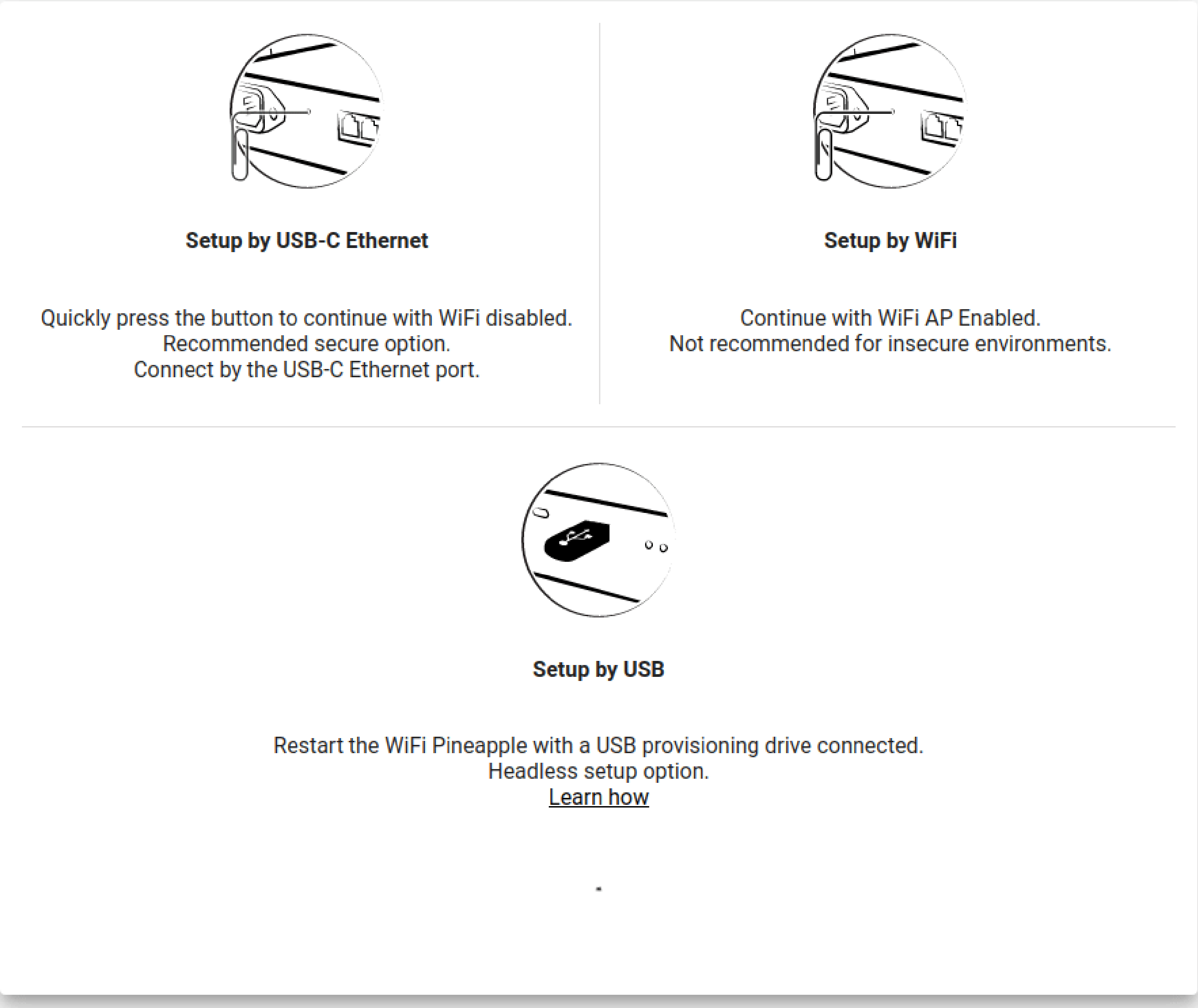
Once you've connected to the WiFi Pineapple, this guide teaches you how to navigate the Setup wizard.

Once you've connected to the WiFi Pineapple and it has fully booted, you will be able to access the WiFi Pineapple Stager at http://172.16.42.1.

The WiFi Pineapple ships with a slimmed down firmware called **the stager**. This approach enables you to always have the latest firmware for the out-of-the-box set-up, due to the latest firmware being downloaded.

Getting the latest firmware via Over-The-Air

To start, begin by verifying that you are in the presence of the WiFi Pineapple. You can do this by pressing the reset button in one of the ways described on-screen.



Setup by USB-C Ethernet

Quickly press the button to continue with WiFi disabled.
Recommended secure option.
Connect by the USB-C Ethernet port.

Setup by WiFi

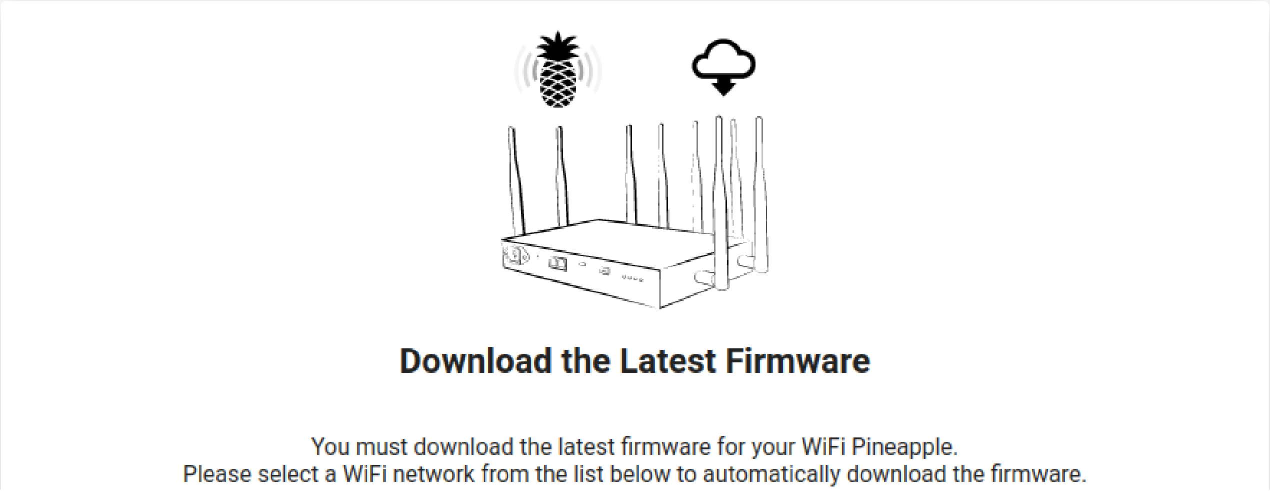
Continue with WiFi AP Enabled.
Not recommended for insecure environments.

Setup by USB

Restart the WiFi Pineapple with a USB provisioning drive connected.
Headless setup option.
Learn how

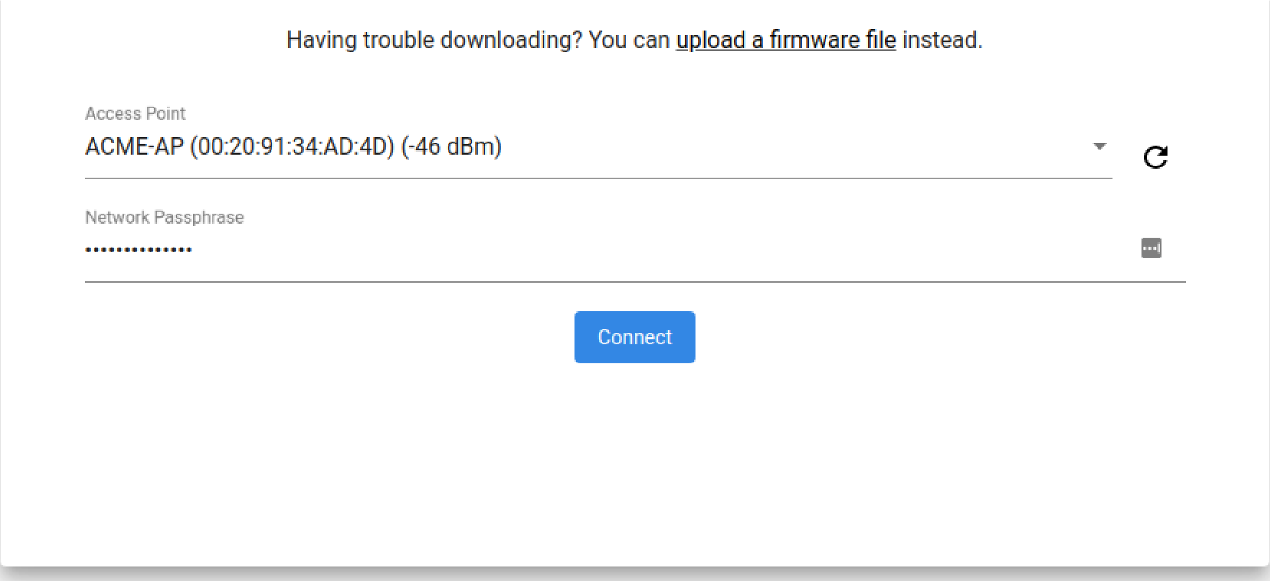
> ⓘ Continuing withing the **Setup by USB-C Ethernet** option will still allow you to use WiFi to connect to a network and download the firmware.

Next, connect to an Access Point you know the credentials to. Doing this will establish an internet connection for the WiFi Pineapple, and the latest firmware will be automatically downloaded.



Download the Latest Firmware

You must download the latest firmware for your WiFi Pineapple.
Please select a WiFi network from the list below to automatically download the firmware.



Having trouble downloading? You can upload a firmware file instead.

Access Point

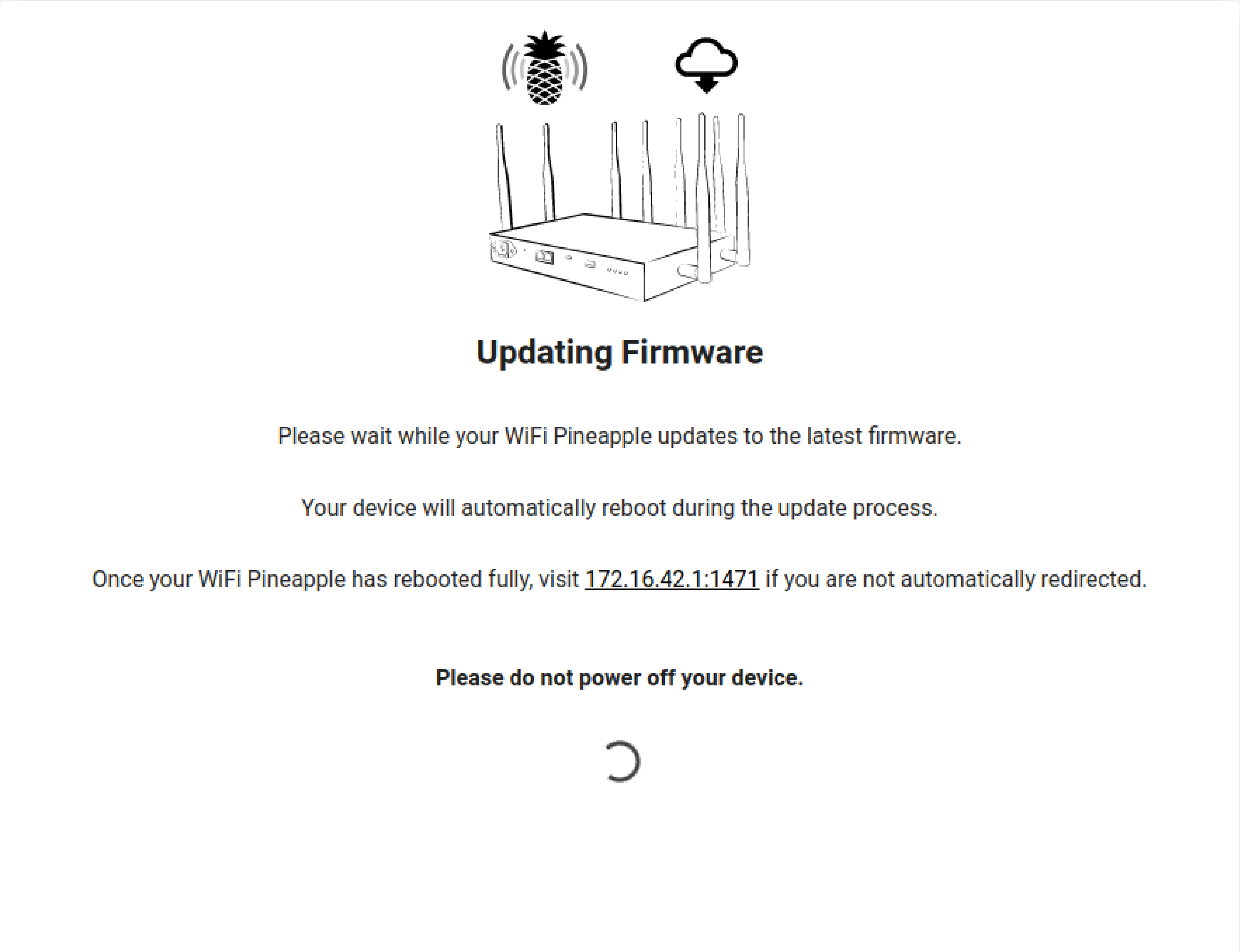
ACME-AP (00:20:91:34:AD:4D) (-46 dBm)

Network Passphrase

••••••••••••••

Only WPA2 and WPA networks are supported in the stager.

After the connection is successfully established, the firmware will be automatically downloaded and flashed to your WiFi Pineapple. Once the upgrade is complete, you will be able to access the WiFi Pineapple at http://172.16.42.1:1471 again.



Updating Firmware

Please wait while your WiFi Pineapple updates to the latest firmware.

Your device will automatically reboot during the update process.

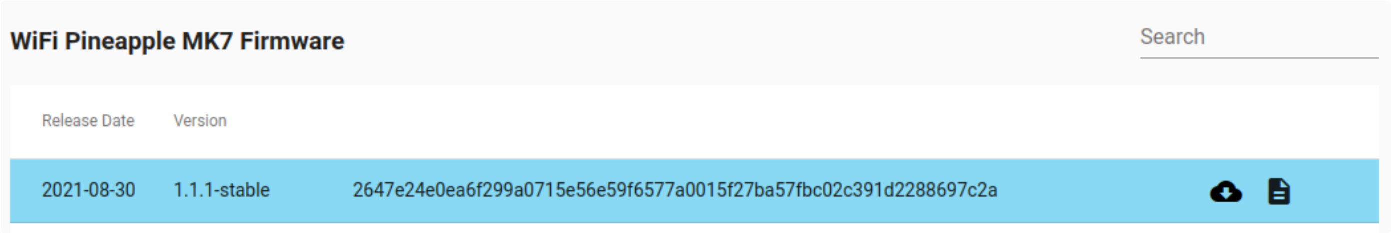
Once your WiFi Pineapple has rebooted fully, visit 172.16.42.1:1471 if you are not automatically redirected.

Please do not power off your device.

Uploading the firmware manually

As an alternative to getting the firmware over-the-air, you may choose to upload the firmware to the WiFi Pineapple manually. This can be useful if you are having difficulties connecting to an Access Point, or if you don't have one available.

To start, begin by downloading the latest firmware from the Hak5 Download Portal. The latest releases are always at the top of the table, and highlighted blue.



WiFi Pineapple MK7 Firmware

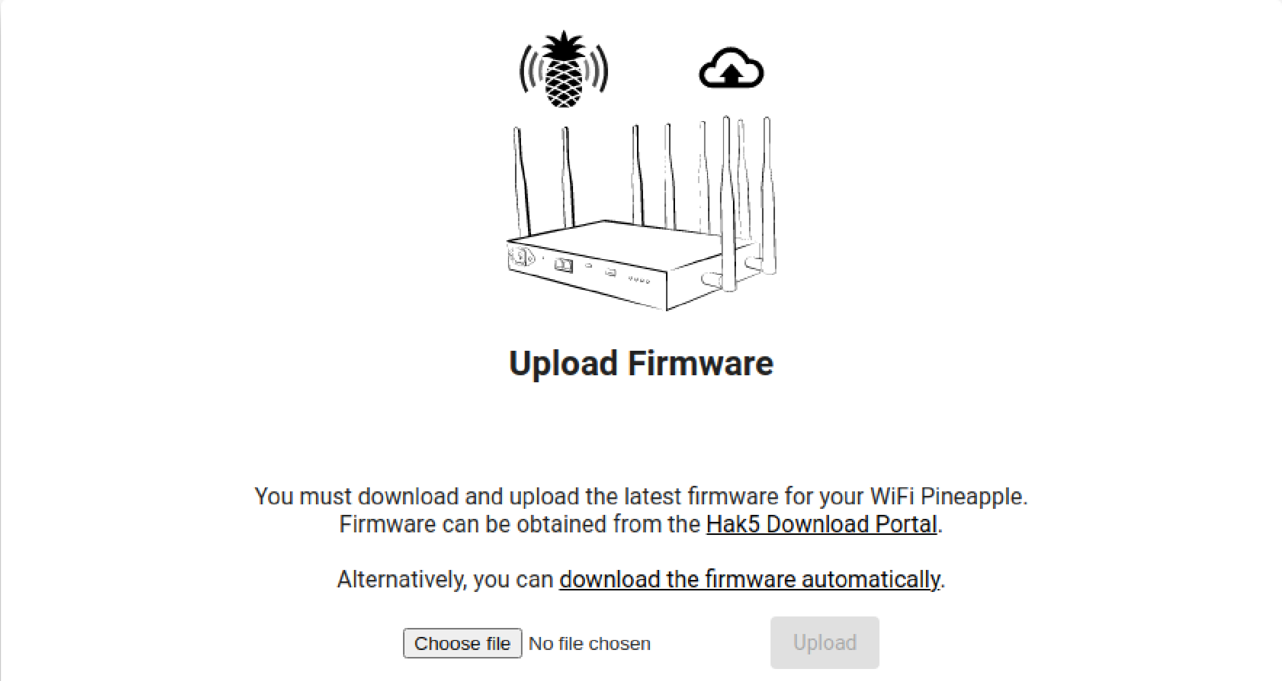
Search

Release Date	Version			
2021-08-30	1.1.1-stable	2647e24e0ea6f299a0715e56e59f6577a0015f27ba57fbc02c391d2288697c2a	⬇	🗎

Once the file is downloaded, verify the SHA256 sum with the one listed on the download portal.

> ⓘ If the SHA256 sum of the downloaded file does not match the one listed on the website, do not upload it to the WiFi Pineapple, as it may be corrupted.

Next, you can upload it to the WiFi Pineapple by clicking the **upload a firmware instead** link on the Network page.



Upload Firmware

You must download and upload the latest firmware for your WiFi Pineapple.
Firmware can be obtained from the Hak5 Download Portal.

Alternatively, you can download the firmware automatically.

After uploading, the file will be checked and flashed to the WiFi Pineapple.

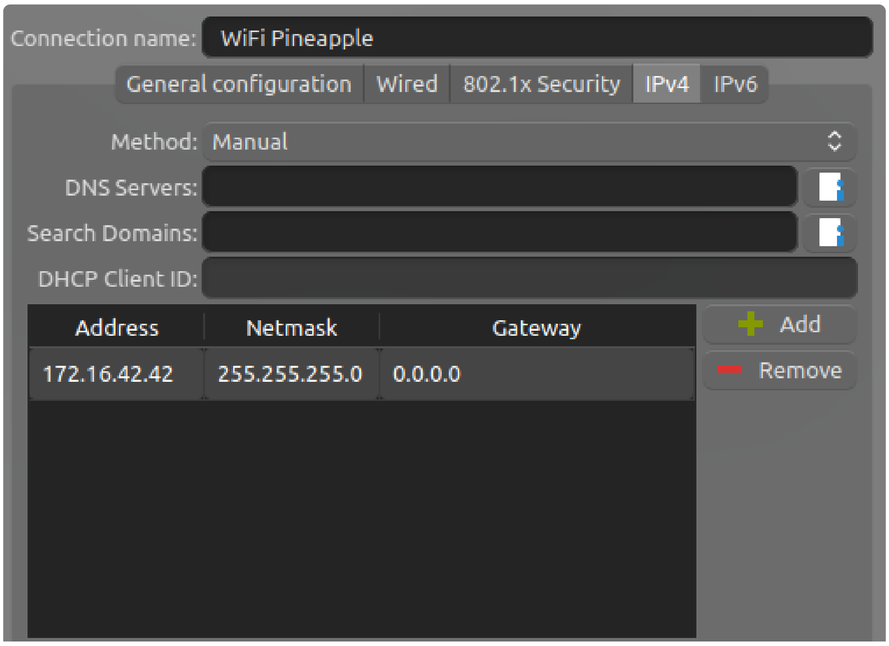
Connecting to the WiFi Pineapple on Linux

This guide teaches the basics of connecting to the WiFi Pineapple on Linux-based operating systems.

Configuration via GUI

To configure the WiFi Pineapple's USB Ethernet interface, you can use the NetworkManager GUI commonly included in Linux distributions.

1. Connect the WiFi Pineapple to your computer via the USB-C cable.
2. Once the device has fully booted, open your computers networking settings.
3. Find the new USB Ethernet device, and configure it to use the following IPv4 settings:
    1. IP: 172.16.42.42
    2. Netmask: 255.255.255.0
    3. Gateway: Unset, or 0.0.0.0



Connection name: WiFi Pineapple

Method: Manual

DNS Servers:

Search Domains:

DHCP Client ID:

Address	Netmask	Gateway
172.16.42.42	255.255.255.0	0.0.0.0

□ IPv4 is required for this connection

ⓘ You may need to disconnect and reconnect the interface for your changes to take place.

Configuration via CLI

To configure the WiFi Pineapple's USB Ethernet interface via the command line, you can make use of the `ip` tools commonly included in Linux distributions.

1. Connect the WiFi Pineapple to your computer via the USB-C cable.
2. Once the device has fully booted, open the Terminal emulator and run the following:

```
$ sudo ip link set eth0 down
$ sudo ip addr add 172.16.42.42/255.255.255.0 dev eth0
$ sudo ip link set eth0 up
```

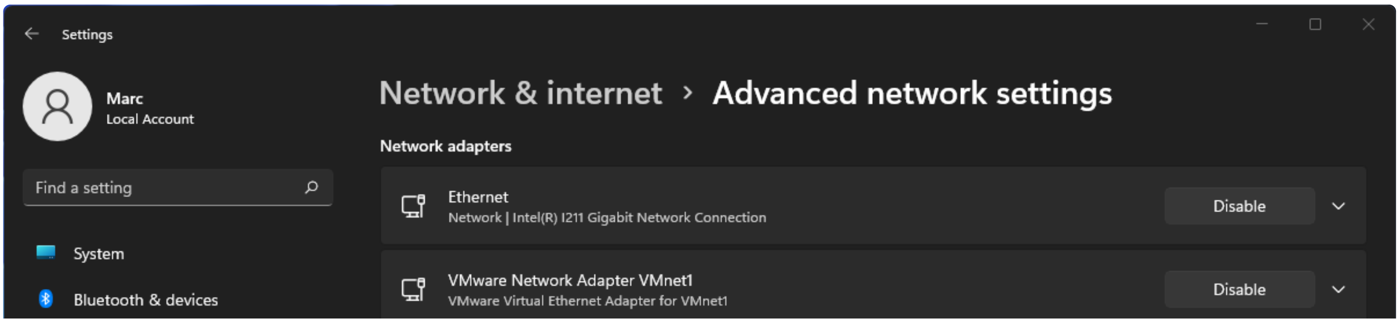
Connecting to the WiFi Pineapple on Windows

This guide teaches the basics of connecting to the WiFi Pineapple on Windows.

ⓘ The following guide is designed to work on Windows 11, although the same or similar steps apply to Windows 10/8.1/8/7 too.

Configuration via GUI

Start by opening the **Network & Internet** settings in the Windows settings application. Scroll down to **Related settings** and click **More network adapter options**.

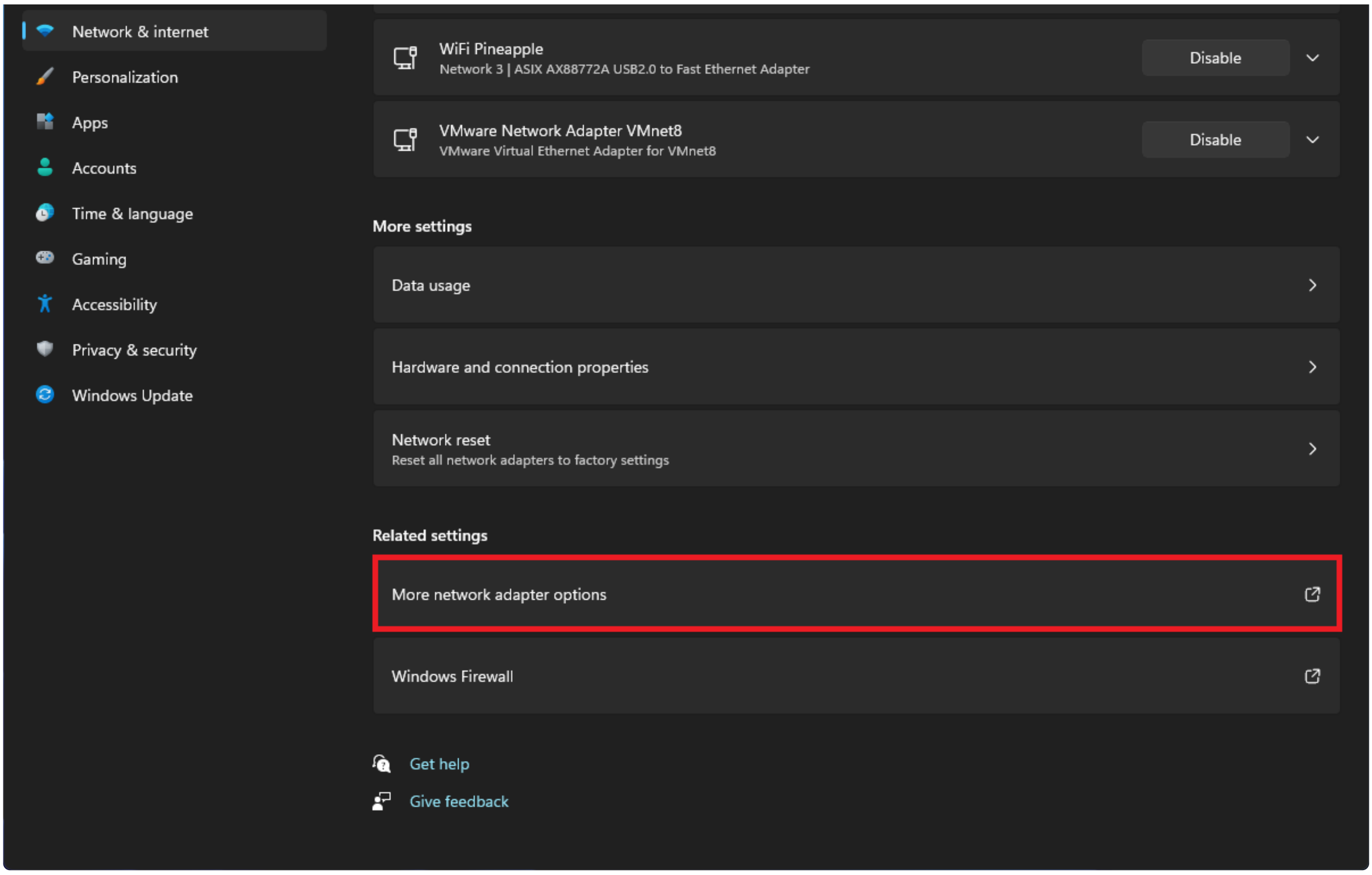


Network & internet › Advanced network settings

Network adapters

Ethernet
Network | Intel(R) I211 Gigabit Network Connection
Disable

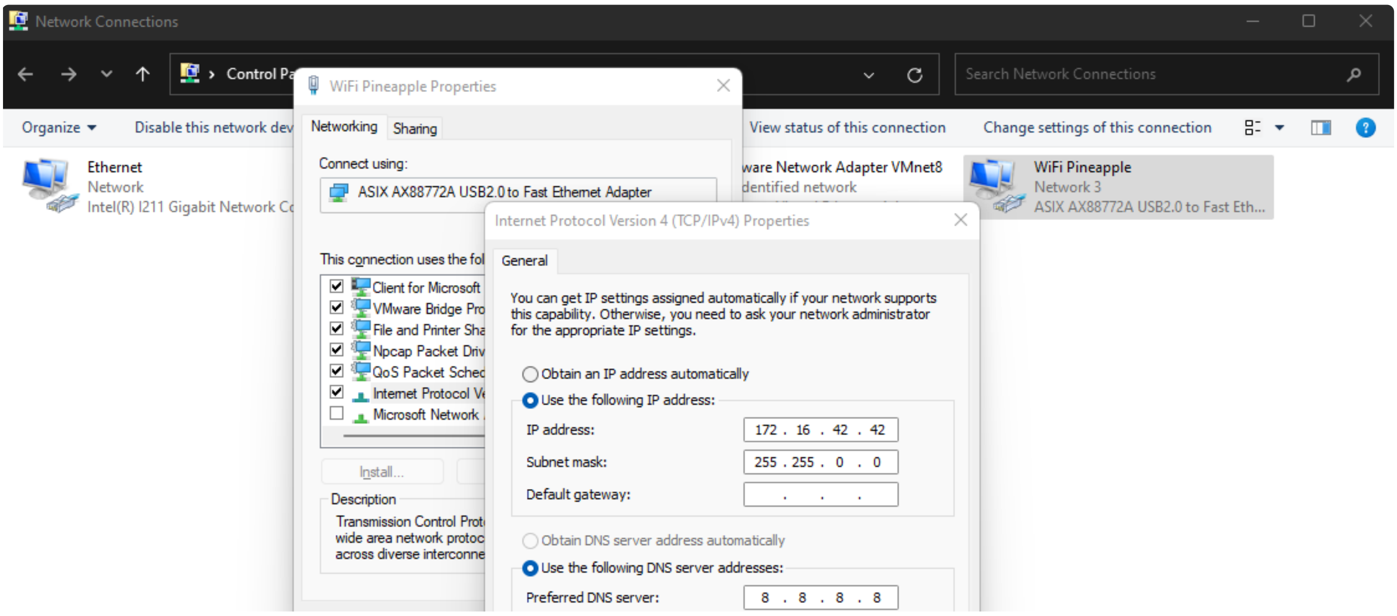
VMware Network Adapter VMnet1
VMware Virtual Ethernet Adapter for VMnet1
Disable


Network & internet
Personalization
Apps
Accounts
Time & language
Gaming
Accessibility
Privacy & security
Windows Update
WiFi Pineapple
Network 3 | ASIX AX88772A USB2.0 to Fast Ethernet Adapter
Disable
VMware Network Adapter VMnet8
VMware Virtual Ethernet Adapter for VMnet8
Disable
More settings
Data usage
Hardware and connection properties
Network reset
Reset all network adapters to factory settings
Related settings
More network adapter options
Windows Firewall
Get help
Give feedback

In the new window, **right click** the adapter that represent your WiFi Pineapple and select **Properties**. Then, select the text **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties** again.

In the new properties window, configure the following static settings:

- IP Address: **172.16.42.42**
- Subnet Mask: **255.255.0.0**
- Default Gateway: **Blank**
- Preferred DNS: **8.8.8.8**
- Alternate DNS: **8.8.4.4**


Network Connections
Control Pa
Search Network Connections
Organize
Disable this network dev
View status of this connection
Change settings of this connection
Ethernet
Network
Intel(R) I211 Gigabit Network Co
ware Network Adapter VMnet8
dentified network
WiFi Pineapple
Network 3
ASIX AX88772A USB2.0 to Fast Eth...
WiFi Pineapple Properties
Networking
Sharing
Connect using:
ASIX AX88772A USB2.0 to Fast Ethernet Adapter
This connection uses the fol
Client for Microsoft
VMware Bridge Pro
File and Printer Sha
Npcap Packet Driv
QoS Packet Sched
Internet Protocol Ve
Microsoft Network
Install...
Description
Transmission Control Prot
wide area network protoc
across diverse interconne
Internet Protocol Version 4 (TCP/IPv4) Properties
General

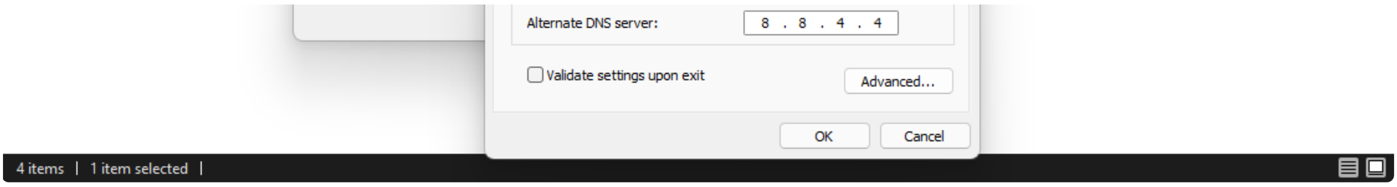
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 16 . 42 . 42
Subnet mask: 255 . 255 . 0 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

Preferred DNS server: 8 . 8 . 8 . 8



Alternate DNS server: 8 . 8 . 4 . 4

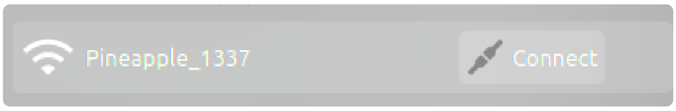
☐ Validate settings upon exit

> You may set your own preferred and alternate DNS servers if desired, but Google's DNS is recommended.

Connecting to the WiFi Pineapple over WiFi

This guide instructs you on how to connect to the WiFi Pineapple's Open AP during setup.

The WiFi Pineapple serves an Open AP for you to connect to for the purposes of completing device setup. The SSID of the AP is `Pineapple_XXXX`, where the 'XXXX' is the last 4 characters of the devices MAC address.



After connecting to the AP, you will receive an IP via DHCP from the WiFi Pineapple.

Setup by USB Disk

The WiFi Pineapple may be provisioned "headless" — meaning without intervention interactively. This means that you can take a fresh WiFi Pineapple Mark VII out of its box and set it up with the latest firmware and your settings of choice without connecting it to a computer or smartphone.

Preparing the USB drive

Once prepared, the USB drive will be properly formatted and contain a config.txt file, an upgrade-x.x.x.bin file, and optionally a device.config file (if using with Cloud C2).

Format the drive

The USB drive must contain only a single partition and be formatted as one of the following:

- ext4
- exFAT / FAT
- NTFS

Download the firmware

Once your USB drive has been formatted with a supported filesystem, Download the upgrade file from the Hak5 Download Portal to the root of the USB drive.

> Make sure you keep the original name of the file (upgrade-x.x.x.bin).

> It is best practice to validate file integrity by verifying the SHA256 sum of the download.

Create the config.txt

On the root of the USB flash disk, create a config.txt file using a standard text editor such as Notepad (Windows), textEdit (Mac), or vim/nano (Linux) containing the below information. Make sure the txt file is saved in ASCII format. Modify the settings as per your desired configuration.

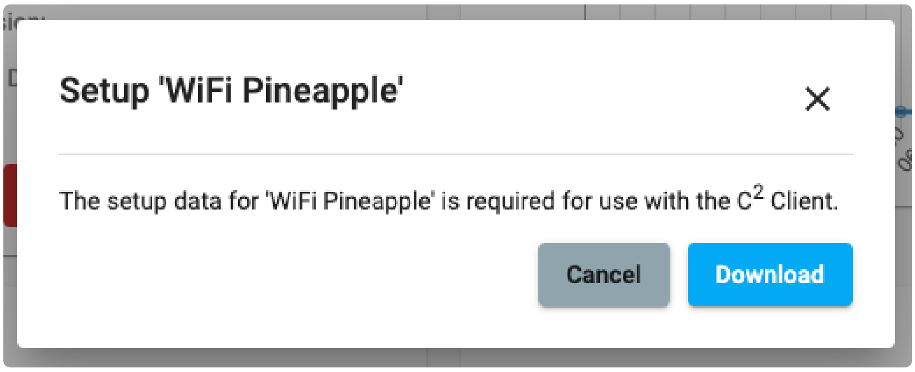
```
# This file automatically configures the WiFi Pineapple.
# To enroll your WiFi Pineapple automatically, edit the below variables.
# Save as config.txt on the root of an ext4/exFAT/FAT/NTFS USB flash drive.
# Connect to the WiFi Pineapple USB host port before applying power for the
# first time. During firmware installation, the LED will flash Red/Blue.
# DO NOT DISCONNECT POWER DURING FIRMWARE INSTALLATION!
# For more information, visit https://docs.hak5.org
#
# General System Configuration
#
ROOT_PASSWORD="hak5pineapple"
HOSTNAME="pineapple"
TIMEZONE="utc"
#
# Wireless AP Configuration
#
MANAGEMENT_SSID="Pineapple_Management"
MANAGEMENT_PSK="AGoodWPA-PSKPassphrase"
MANAGEMENT_HIDDEN=1
MANAGEMENT_DISABELD=0
OPEN_SSID="Open"
OPEN_HIDDEN=0
COUNTRY_CODE=US

#
# Filters Configuration
#
CLIENT_FILTER="ALLOW"
SSID_FILTER="ALLOW"
#
# Hak5 Cloud C2 Configuration
#
```

```
ENABLE_C2=1
#
# Software License Agreement:
# https://hak5.org/pages/software-license-agreement
#
ACCEPT_LICENSE=TRUE
```

Add the Cloud C2 provisioning file (optional)

In addition to the config.txt and upgrade-x.x.x.bin files on the root of the USB drive, a Cloud C2 device.config provisioning file may be included.

To generate this file, create a new WiFi Pineapple device on your Cloud C2 instance, then navigate to the device's overview page and click the Setup button from the description card.



Setup 'WiFi Pineapple'

The setup data for 'WiFi Pineapple' is required for use with the C^2 Client.

Power on the WiFi Pineapple with the USB Drive

From a powered off state, place your USB drive into the USB Type-A port on the WiFi Pineapple, then connect it to a power source. Once the device is fully booted, it will automatically mount and find the upgrade file on the device. If the firmware file is valid, the device will then perform the firmware upgrade and reboot as indicated by the flashing red/blue LED.

> ⚠ During the firmware installation process, as indicated by the red/blue LED status, DO NOT disconnect the power source. Doing so will render the device inoperable.

Once the firmware has installed, you may connect to the WiFi Pineapple network and visit the web interface at http://172.16.42.1:1471.

UI Overview

Introduction to the UI

An introduction to the WiFi Pineapple Web UI

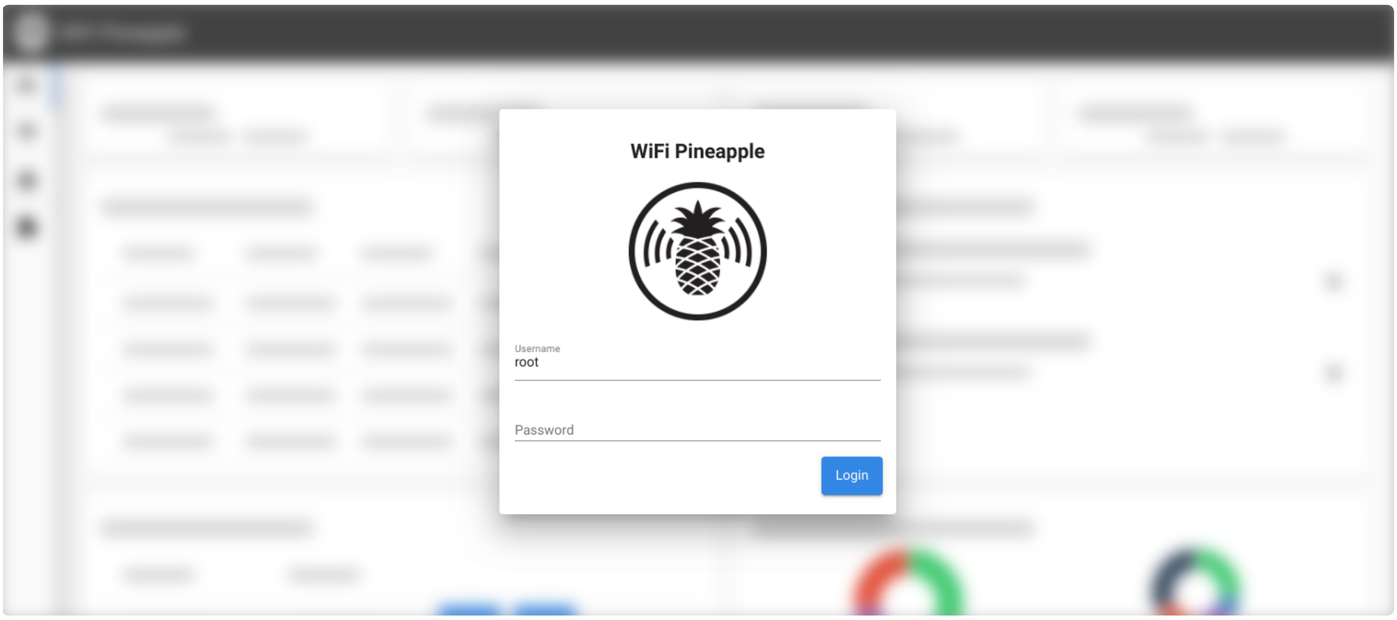
Opening the User Interface

The management interface is available at http://172.16.42.1:1471 and is accessible from the USB Ethernet connection and the management WiFi network configured during Setup.

> ⓘ Note the port in the URL: 1471. Without this port, you will get a blank page from the default webserver!

Logging In

Upon browsing to the UI, you'll be greeted with the login page. The username is root, while the password is the one you set during Setup.

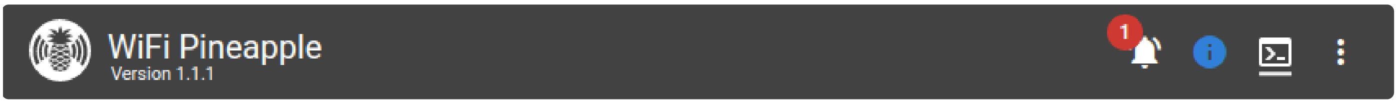

WiFi Pineapple

Username
root

Password

Navigating the UI

Once you've logged in, you'll see the Dashboard. At the top of the page is the title bar, which includes the current firmware version and buttons to view **Notifications**, view **Informational Messages**, or open the **Web Terminal**. The context menu (three dots) holds additional, less common options.

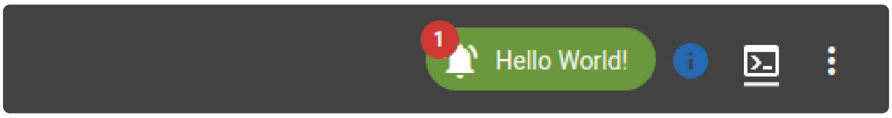


WiFi Pineapple title bar

Notifications

Notifications are a way for the system or modules to indicate a change in status or other message. They can have one of 5 notification levels: **Info**, **Warning**, **Error**, **Success** or **Unknown**. The messages are given a preview for a brief time in the title bar.

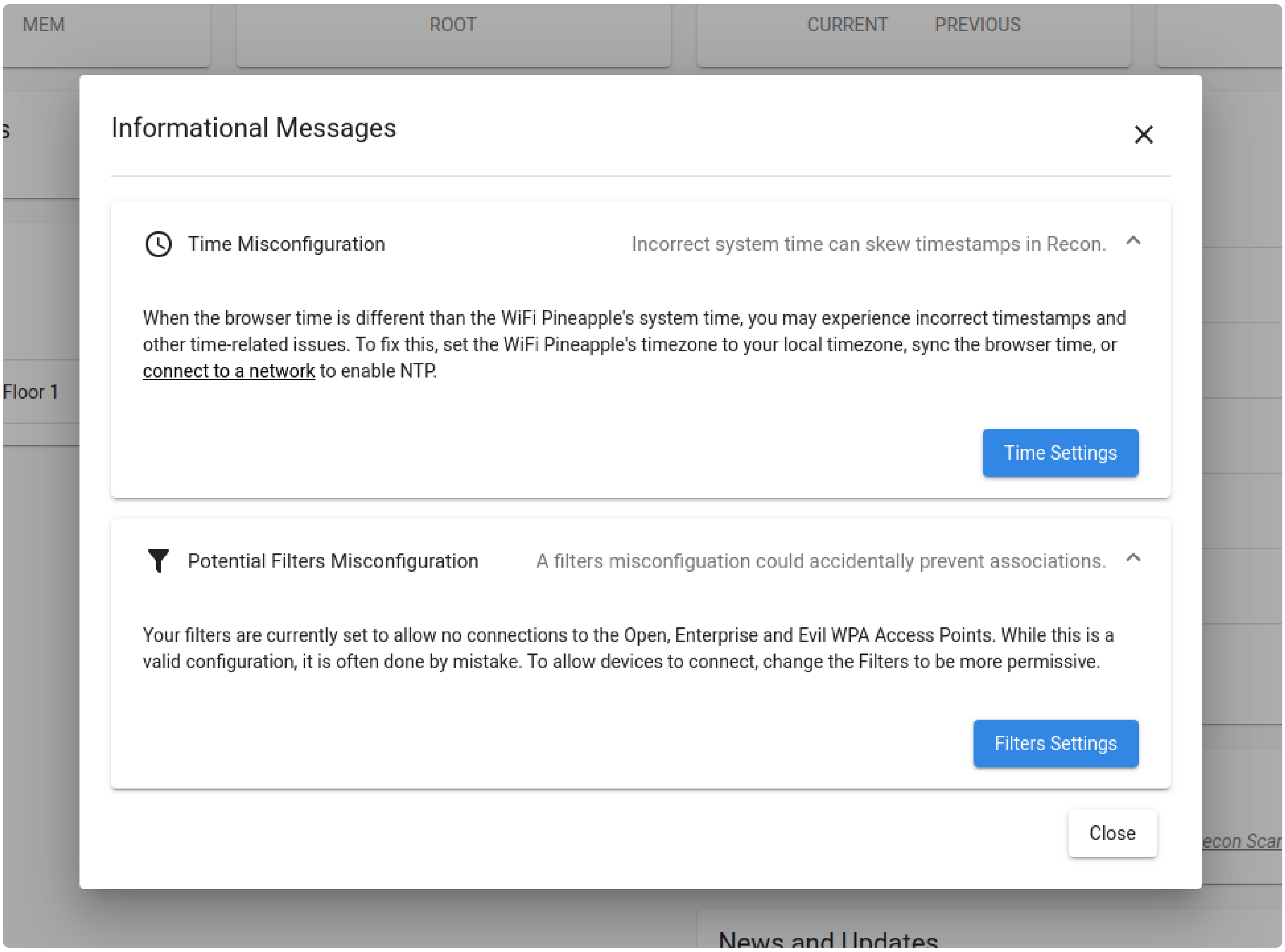
Click on the notifications icon to view all messages.



WiFi Pineapple notifications

Informational Messages

Informational Messages show you potential misconfigurations with your WiFi Pineapple, as well as telling you potential fixes for them.



Informational Messages

Time Misconfiguration — Incorrect system time can skew timestamps in Recon.

When the browser time is different than the WiFi Pineapple's system time, you may experience incorrect timestamps and other time-related issues. To fix this, set the WiFi Pineapple's timezone to your local timezone, sync the browser time, or connect to a network to enable NTP.

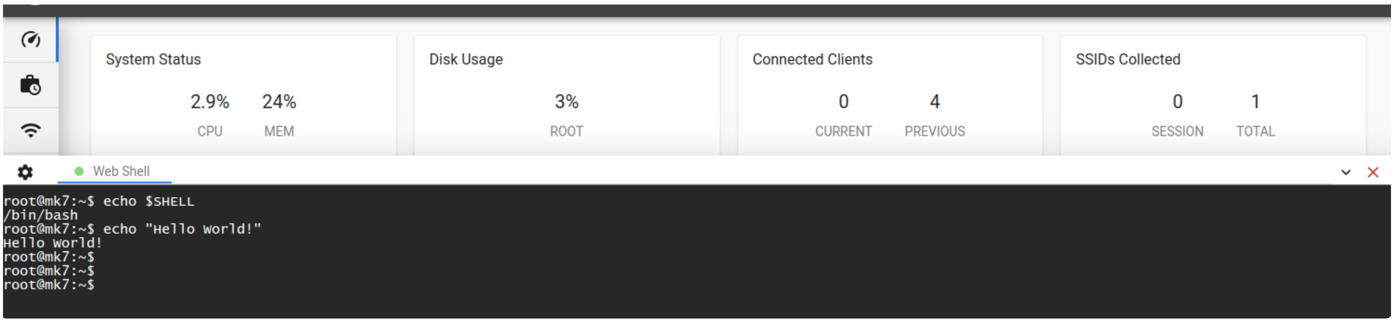
Potential Filters Misconfiguration — A filters misconfiguation could accidentally prevent associations.

Your filters are currently set to allow no connections to the Open, Enterprise and Evil WPA Access Points. While this is a valid configuration, it is often done by mistake. To allow devices to connect, change the Filters to be more permissive.

Example misconfigurations

Web Terminal

The Web Terminal offers a fully featured Bash shell on the WiFi Pineapple without needing to use SSH. You can use it to completely manage the device, run tools, install packages and do anything else you would expect from a Linux computer.

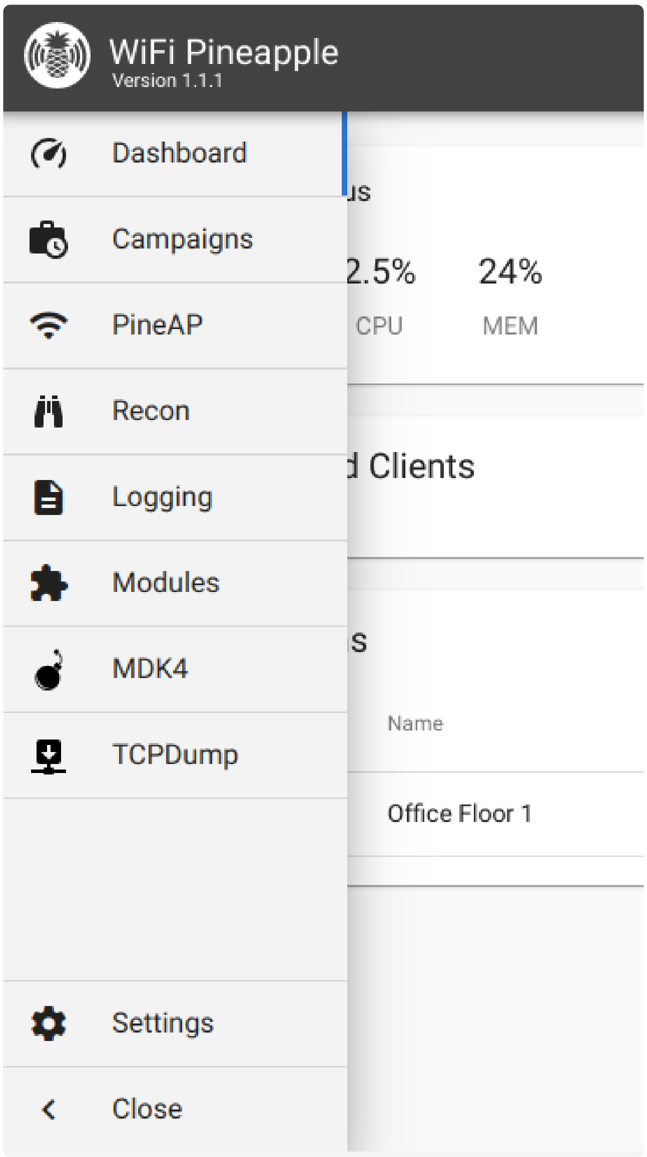


```
root@mk7:~$ echo $SHELL
/bin/bash
root@mk7:~$ echo "Hello world!"
Hello world!
root@mk7:~$
root@mk7:~$
root@mk7:~$
```

The WiFi Pineapple web shell

Sidebar

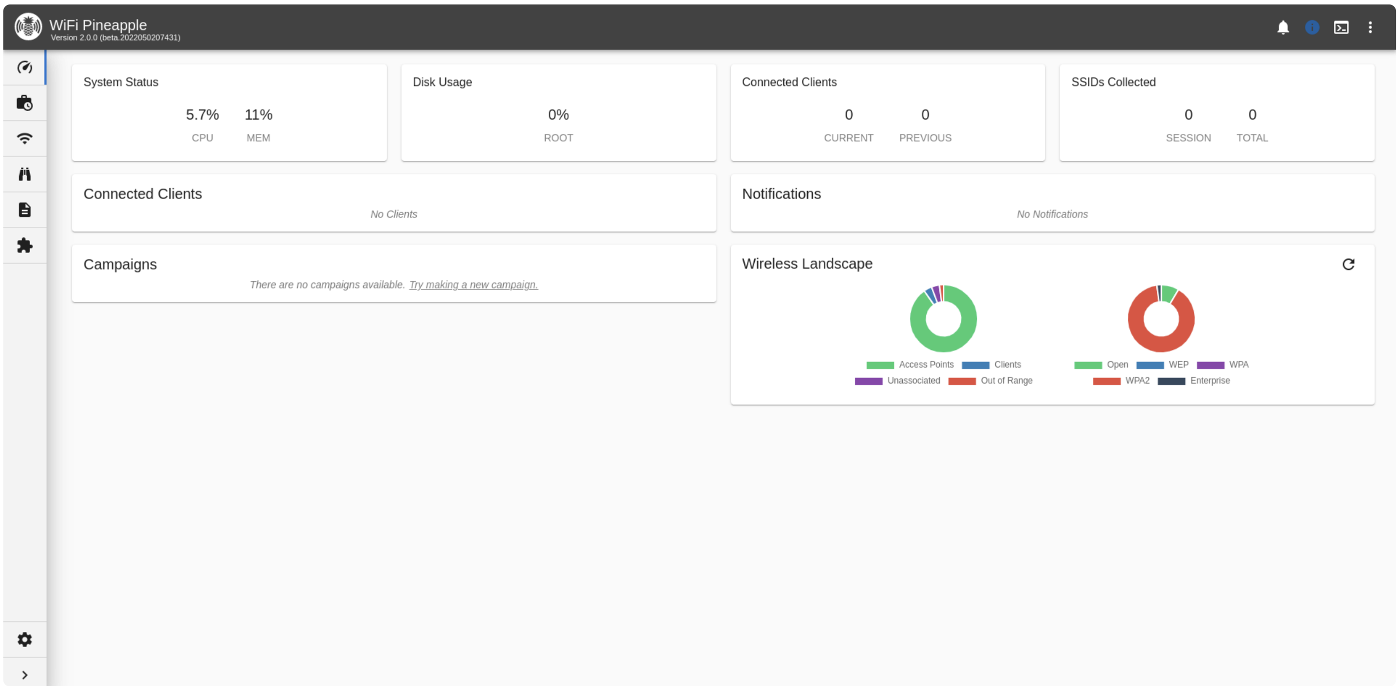
On the side of the page, you will see the **Sidebar**. This sidebar houses convenient links to the system modules, and downloaded modules can be added to the sidebar for speedy access. You can extend the sidebar, showing the full names, by clicking the **Show More** button anchored at the bottom.



Dashboard

The Dashboard is the landing page for the WiFi Pineapple management UI, and provides at a glance insights to the system and its services.

The WiFi Pineapple UI Dashboard shows an at-a-glance status of some of the components of the device.



WiFi Pineapple
Version 2.0.0 (beta.2022050207431)

System Status
5.7% CPU
11% MEM

Disk Usage
0% ROOT

Connected Clients
0 CURRENT
0 PREVIOUS

SSIDs Collected
0 SESSION
0 TOTAL

Connected Clients
No Clients

Notifications
No Notifications

Campaigns
There are no campaigns available. Try making a new campaign.

Wireless Landscape

WiFi Pineapple Dashboard

Cards

Along the top of the page, multiple cards show different system status numbers, such as CPU and RAM usage, Disk usage and Client Stats. These stats automatically update when viewing the Dashboard.

Connected Clients

MAC Address, IP Address and Connected Time can be viewed for all clients connected to non-Management access points. You can also kick a specific client by using the Kick button.

> ⓘ Some clients may automatically reconnect quickly. Client's can be denied association via the Filters.

Notifications

Notifications are a way for the system or modules to indicate a change in status or other message. They can have one of 5 notification levels: **Info**, **Warning**, **Error**, **Success** or **Unknown**.

Campaigns

The campaign **status**, **name** and **type** show a brief description of current campaigns, along with a toggle button to enable or disable them.

Wireless Landscape

Brief statistics from the latest Recon scan provide an at-a-glance view without having to dive into details of the scan.

News and Updates

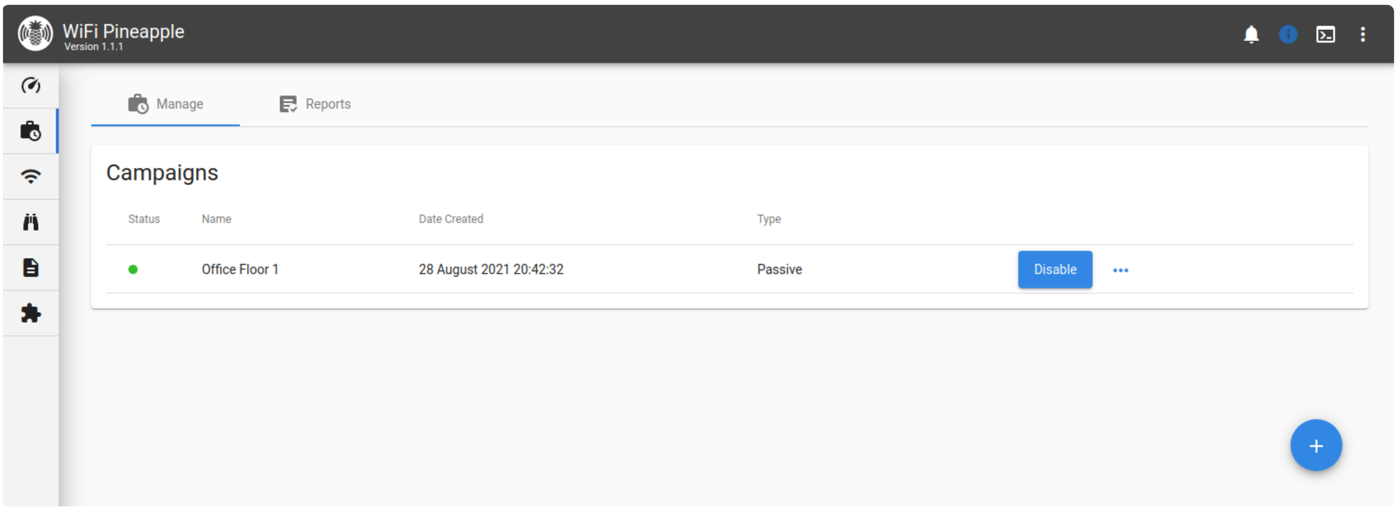
Latest news and release notes from Hak5.

Campaigns

Campaigns allow you to create automated tasks to ease an engagement, with the ability to generate a report at the end or on an interval.

Manage

Campaigns that have been created are listed in a table, showing the current status, name, creation date and campaign type. You can enable or disable your campaigns with the Enable/Disable toggle, and edit or remove them by clicking the "..." menu button.

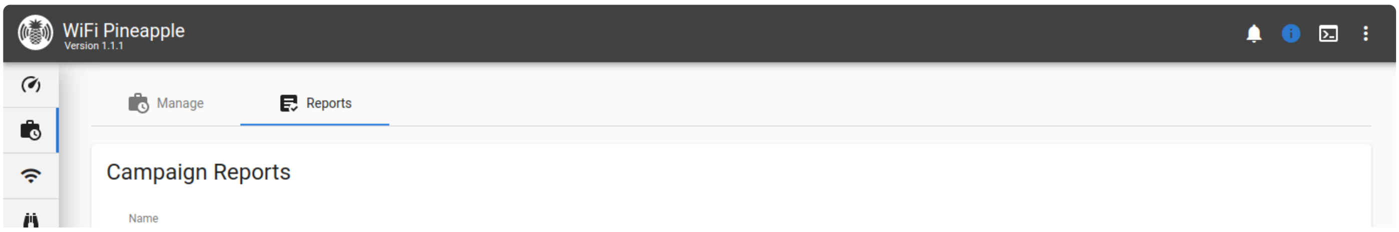


Campaigns

Status	Name	Date Created	Type
●	Office Floor 1	28 August 2021 20:42:32	Passive

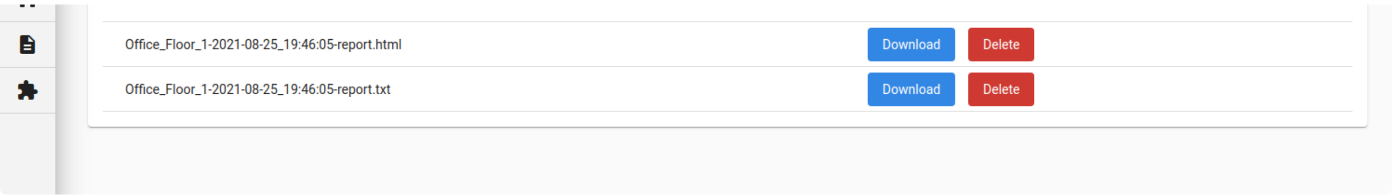
Reports

From the Reports tab, you can download and delete the reports that have been generated by your campaigns.



Campaign Reports

Name



Office_Floor_1-2021-08-25_19:46:05-report.html Download Delete

Office_Floor_1-2021-08-25_19:46:05-report.txt Download Delete

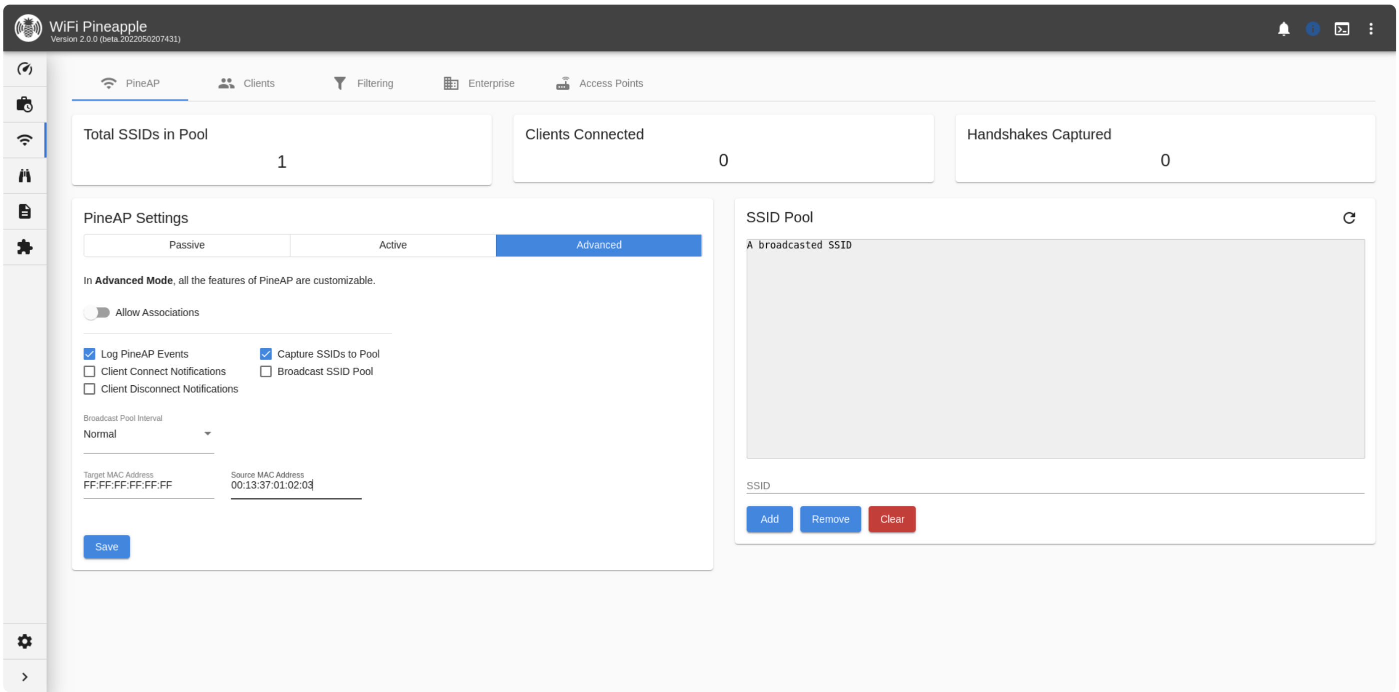
PineAP

PineAP is the center of the WiFi Pineapple's rogue access points, client management and filtering.

PineAP Settings

The main PineAP page is used to manage the PineAP Daemon settings and status. You can manage individual daemon settings by selecting the **Advanced** tab, or you may select preset settings with the Passive or Active tabs.

On the right hand side, you can find the current SSID pool. These SSIDs can be automatically collected in the Passive and Active modes, or by selecting the "Capture SSIDs to Pool" option in Advanced. You can use the field below and the Add, Remove and Clear buttons to manually add or remove SSIDs.



Total SSIDs in Pool 1

Clients Connected 0

Handshakes Captured 0

PineAP Settings

In **Advanced Mode**, all the features of PineAP are customizable.

Allow Associations

☑ Log PineAP Events
□ Client Connect Notifications
□ Client Disconnect Notifications
☑ Capture SSIDs to Pool
□ Broadcast SSID Pool

Broadcast Pool Interval: Normal

Target MAC Address: FF:FF:FF:FF:FF:FF

Source MAC Address: 00:13:37:01:02:03

SSID Pool

```
A broadcasted SSID
```

PineAP Settings

SSID Pool Capture

When "Capture SSIDs to Pool" is enabled, SSIDs seen passively (observed probe requests) and through recon mode are automatically added to the pool of target SSIDs.

Broadcast SSID Pool

When enabled, the WiFi Pineapple will actively advertise previously seen SSIDs. This may be useful for capturing clients looking for specific access points in their list of previous connections.

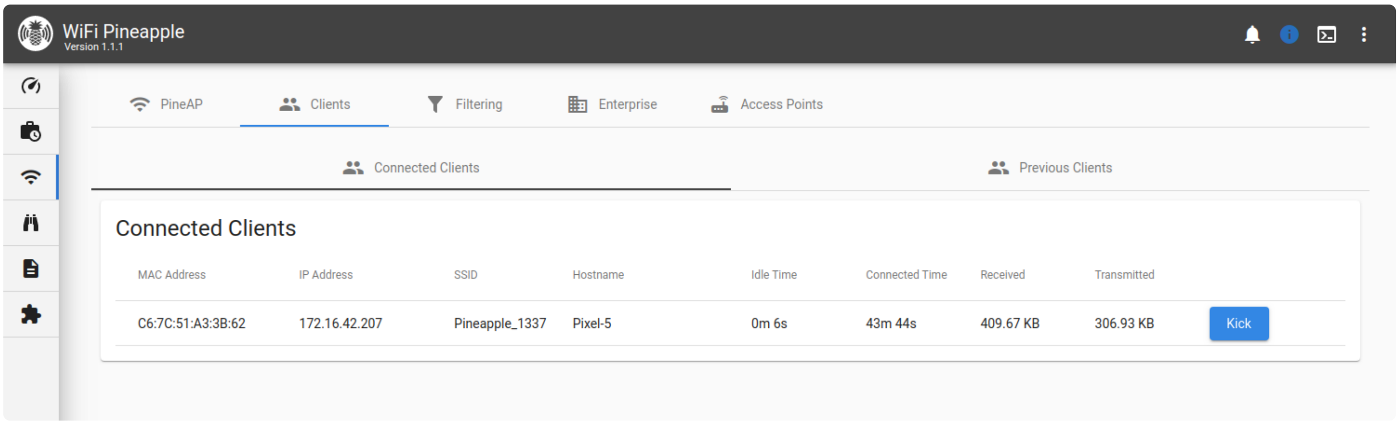
SSID Pool

When **Broadcast SSID Pool** is enabled, the WiFi Pineapple will advertise any SSIDs seen in the pool. This can cause clients looking for those networks to connect to the WiFi Pineapple Open network.

The SSID pool can be automatically populated by **Recon Mode** when the **SSID Pool Capture** option is selected, or SSIDs can be manually added to it.

Clients

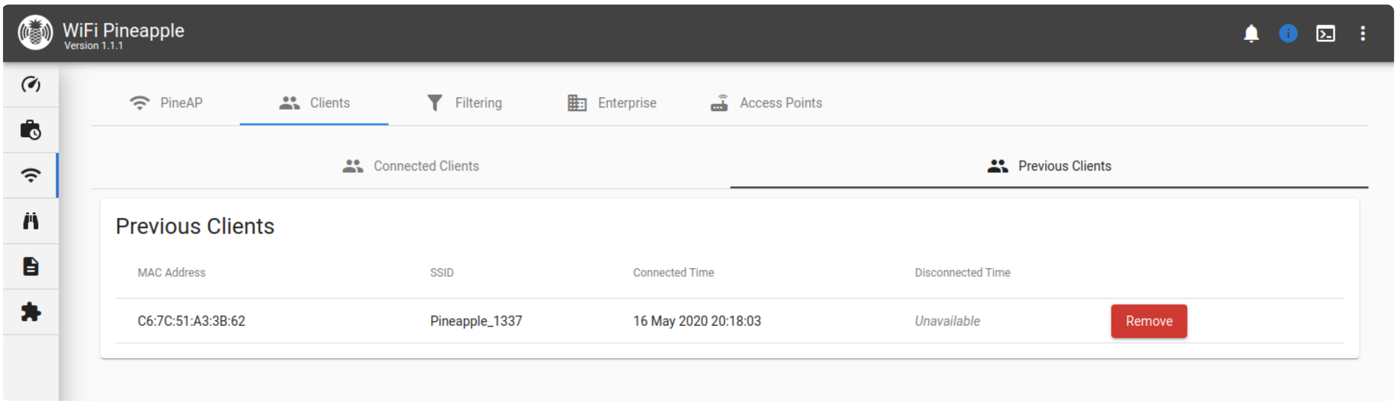
The clients page provides two views for clients, split into connected clients and previous clients. From the **Connected Clients** you can view information about each connected client, including MAC, IP Address and the SSID they associated to, as well as the ability to kick them from the network.



Connected Clients

MAC Address	IP Address	SSID	Hostname	Idle Time	Connected Time	Received	Transmitted	
C6:7C:51:A3:3B:62	172.16.42.207	Pineapple_1337	Pixel-5	0m 6s	43m 44s	409.67 KB	306.93 KB	Kick

Switching to the **Previous Clients** tab shows you a record of all previous associations to the rogue access points hosted by the WiFi Pineapple. Clients that have not yet disconnected from the network have a disconnect time of "Unavailable".



Previous Clients

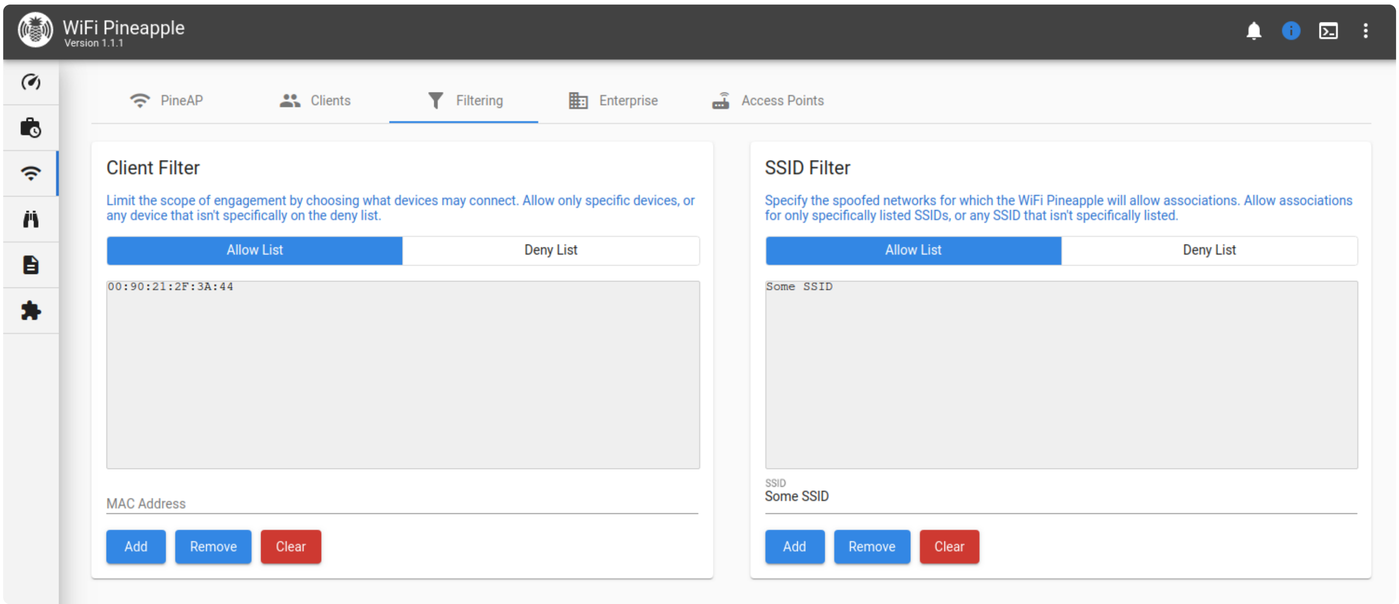
MAC Address	SSID	Connected Time	Disconnected Time	
C6:7C:51:A3:3B:62	Pineapple_1337	16 May 2020 20:18:03	*Unavailable*	Remove

Filtering

The filtering page allows you to have fine control over what devices can connect to your WiFi Pineapple. You can do this by combining two filters: the **Client Filter** and the **SSID Filter**, with two modes each: **Allow** or **Deny**.

With the client filter you may limit the scope of engagement by choosing what devices may connect. Allow only specific devices, or any device that isn't specifically on the deny list.

With the SSID filter you may specify the spoofed networks for which the WiFi Pineapple will allow associations. Allow associations for only specifically listed SSIDs, or any SSID that isn't specifically listed.



Client Filter

Limit the scope of engagement by choosing what devices may connect. Allow only specific devices, or any device that isn't specifically on the deny list.

```
00:90:21:2F:3A:44
```

MAC Address

SSID Filter

Specify the spoofed networks for which the WiFi Pineapple will allow associations. Allow associations for only specifically listed SSIDs, or any SSID that isn't specifically listed.

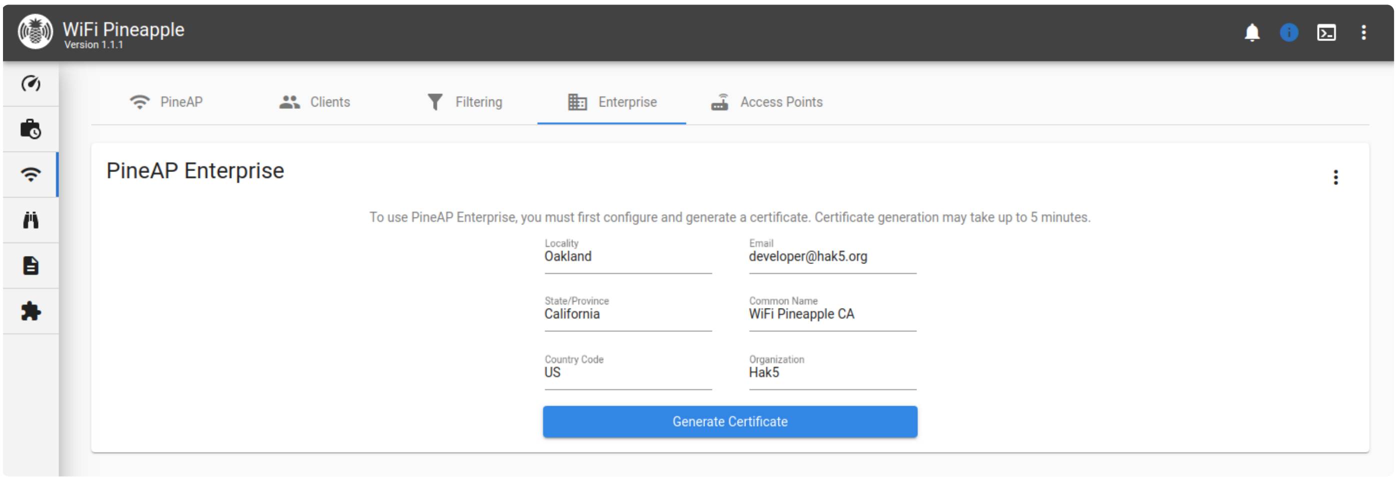
```
Some SSID
```

SSID: Some SSID

Enterprise

The **Enterprise** tab allows you to configure a WPA-EAP Enterprise rogue access point. To begin, fill in the form to generate the EAP configuration and certificates.

Enterprise, or EAP, WiFi authentication is typically used on corporate networks with per-user logins on the network. It is protected by a SSL certificate, which must be created first.



PineAP Enterprise

To use PineAP Enterprise, you must first configure and generate a certificate. Certificate generation may take up to 5 minutes.

Locality: Oakland
Email: developer@hak5.org
State/Province: California
Common Name: WiFi Pineapple CA
Country Code: US
Organization: Hak5

Enterprise certificate generation

Once the certificate has been generated, you'll see easy to use options to configure the rogue enterprise access point, and view the challenge data any connected clients provide. Generating the certificate will take a moderate amount of time while the WiFi Pineapple gathers random data.

The information in the enterprise certificate is arbitrary. Some WiFi clients show the user the data entered in the certificate, while others may only show a certificate hash.

Properly configured WiFi Enterprise clients will reject unknown certificates, however many devices do not offer proper configuration and may either blindly accept new certificates, or prompt the user to accept the certificate.

Authentication Methods

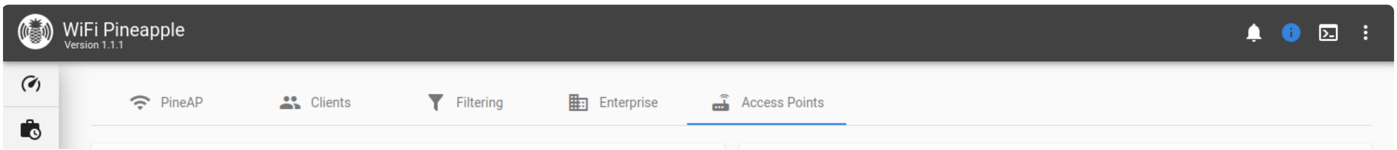
When advertising an enterprise network, the WiFi Pineapple supports three authentication types:

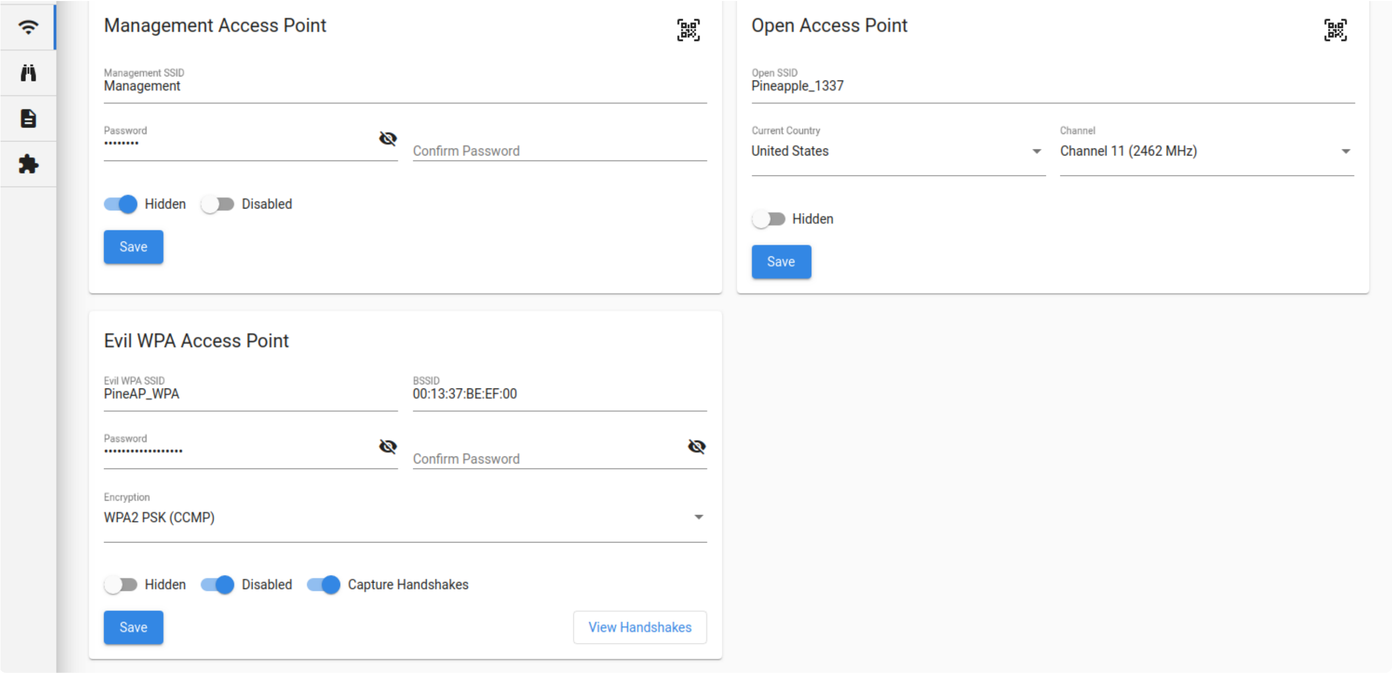
1. Any
   The WiFi Pineapple will allow a client with any authentication method to connect. If possible, the WiFi Pineapple will inform the client it is allowed to connect. Clients connecting with EAP-GTC will connect as normal and the user login saved, while clients connecting with EAP-MSCHAPv2 will receive an error, but the MSCHAPv2 hash challenge will be captured and logged.
2. MSCHAPv2
   MSCHAPv2 is the most common authentication method for enterprise clients. A MSCHAPv2 client uses a hashed authentication method which does not disclose the password.
   The WiFi Pineapple cannot answer the hash challenge without knowing the users password: A MSCHAPv2 client will not be able to *fully* connect to the WiFi Pineapple access point, but the challenge hash will be captured and logged, and can be processed offline to derive the user password.
3. GTC
   GTC is a simpler authentication protocol. Clients using GTC will disclose the full username and password, and will connect to the WiFi Pineapple as normal. The username and password will be logged.

For maximum compatibility, leave the authentication method as **Any**. To try to force clients to use a more vulnerable authentication method, switch to **GTC**. To capture hashes from clients which are configured to only support MSCHAPv2, use **MSCHAPv2** mode.

Access Points

The **Access Points** tab allows you to configure the other access points hosted on the WiFi Pineapple: The **Management AP**, **Open AP**, and **Evil WPA/2 AP**.





Management Access Point

Management SSID: Management

Password: ••••••••

Confirm Password

Hidden (on) · Disabled (off)

Open Access Point

Open SSID: Pineapple_1337

Current Country: United States

Channel: Channel 11 (2462 MHz)

Hidden (off)

Evil WPA Access Point

Evil WPA SSID: PineAP_WPA

BSSID: 00:13:37:BE:EF:00

Password: ••••••••••••••••••

Confirm Password

Encryption: WPA2 PSK (CCMP)

Hidden (off) · Disabled (on) · Capture Handshakes (on)

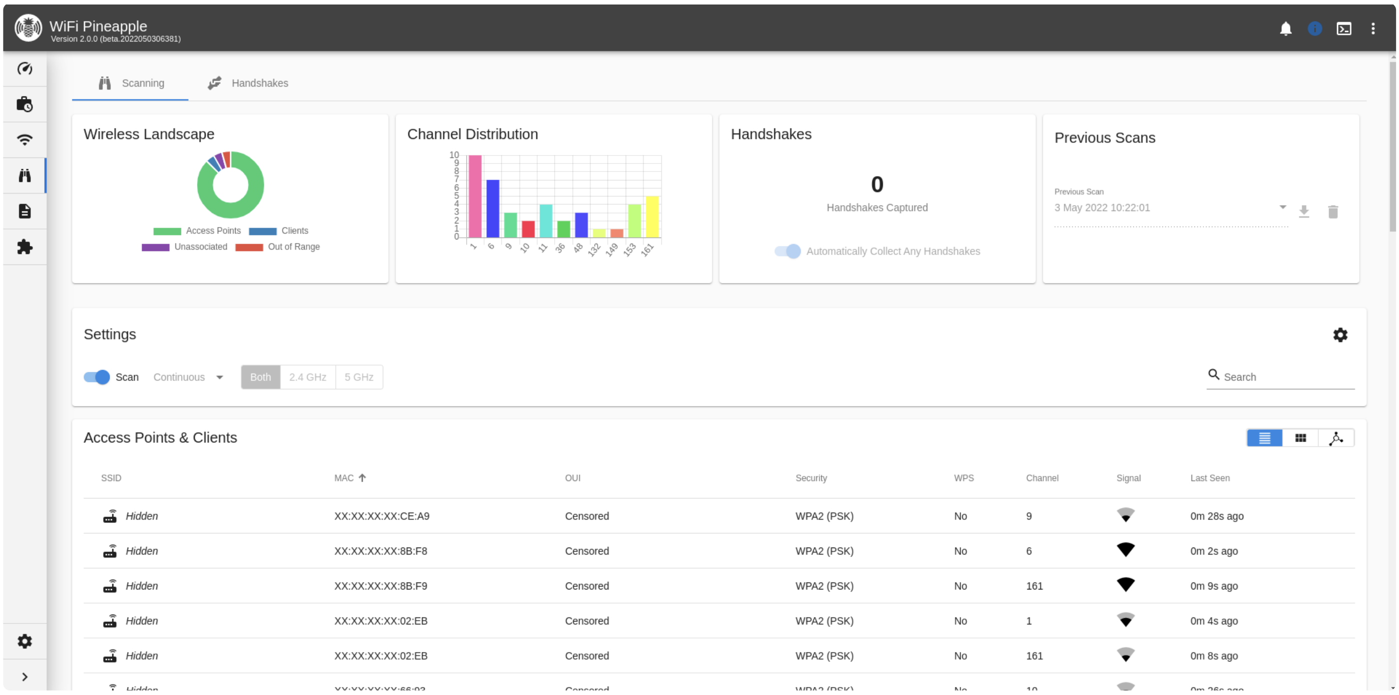
Recon

Recon is the WiFi landscape scanning tool incorporated into the WiFi Pineapple.

Scanning

On the main Recon page, you can see an at-a-glance overview of the current wireless landscape, with a list of discovered APs and their associated clients, unassociated clients, and clients that have gone out of range in table form.

To change to a mobile friendly view, select the card button next to the table icon in the **Access Points & Clients** card.



WiFi Pineapple
Version 2.0.0 (beta.2022050306381)

Handshakes

0
Handshakes Captured

Automatically Collect Any Handshakes (on)

Previous Scans

Previous Scan: 3 May 2022 10:22:01

Settings

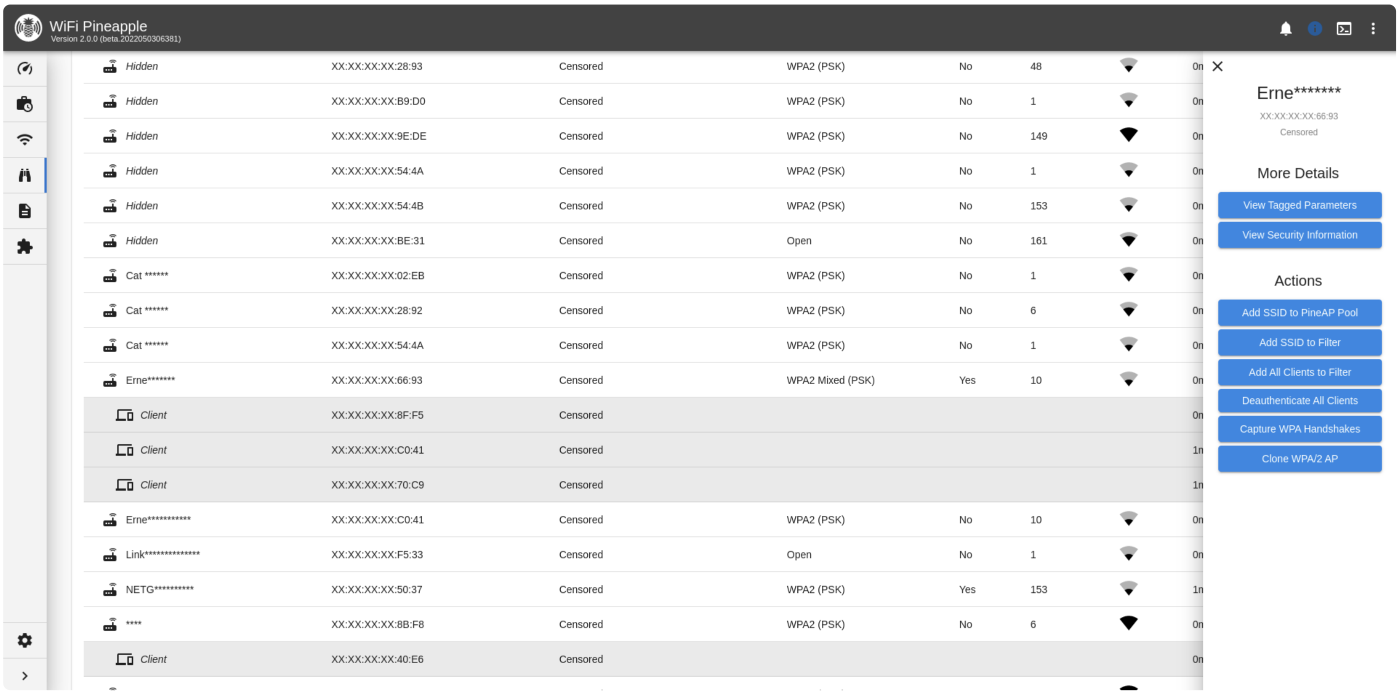
Scan (on) · Continuous · Both · 2.4 GHz · 5 GHz

Access Points & Clients

SSID	MAC ↑	OUI	Security	WPS	Channel	Signal	Last Seen
Hidden	XX:XX:XX:XX:CE:A9	Censored	WPA2 (PSK)	No	9		0m 28s ago
Hidden	XX:XX:XX:XX:8B:F8	Censored	WPA2 (PSK)	No	6		0m 2s ago
Hidden	XX:XX:XX:XX:8B:F9	Censored	WPA2 (PSK)	No	161		0m 9s ago
Hidden	XX:XX:XX:XX:02:EB	Censored	WPA2 (PSK)	No	1		0m 4s ago
Hidden	XX:XX:XX:XX:02:EB	Censored	WPA2 (PSK)	No	161		0m 8s ago
Hidden	XX:XX:XX:XX:66:93	Censored	WPA2 (PSK)	No	10		0m 26s ago

> ⓘ You can change Recon settings, such as scan location and displayed table columns, by selecting the Settings gear icon on the right side of the **Settings** card.

By clicking on an AP or Client in the list, a side menu will slide out from the right. From here you can select options specific to the type of device you selected, such as capturing handshakes or cloning, or adding MAC addresses to the Filters.



WiFi Pineapple
Version 2.0.0 (beta.2022050306381)

Hidden	XX:XX:XX:XX:28:93	Censored	WPA2 (PSK)	No	48	▼	0n
Hidden	XX:XX:XX:XX:B9:D0	Censored	WPA2 (PSK)	No	1	▼	0n
Hidden	XX:XX:XX:XX:9E:DE	Censored	WPA2 (PSK)	No	149	▼	0n
Hidden	XX:XX:XX:XX:54:4A	Censored	WPA2 (PSK)	No	1	▼	0n
Hidden	XX:XX:XX:XX:54:4B	Censored	WPA2 (PSK)	No	153	▼	0n
Hidden	XX:XX:XX:XX:BE:31	Censored	Open	No	161	▼	0n
Cat ******	XX:XX:XX:XX:02:EB	Censored	WPA2 (PSK)	No	1	▼	0n
Cat ******	XX:XX:XX:XX:28:92	Censored	WPA2 (PSK)	No	6	▼	0n
Cat ******	XX:XX:XX:XX:54:4A	Censored	WPA2 (PSK)	No	1	▼	0n
Erne*******	XX:XX:XX:XX:66:93	Censored	WPA2 Mixed (PSK)	Yes	10	▼	0n
Client	XX:XX:XX:XX:8F:F5	Censored					0n
Client	XX:XX:XX:XX:C0:41	Censored					1n
Client	XX:XX:XX:XX:70:C9	Censored					1n
Erne***********	XX:XX:XX:XX:C0:41	Censored	WPA2 (PSK)	No	10	▼	0n
Link**************	XX:XX:XX:XX:F5:33	Censored	Open	No	1	▼	0n
NETG**********	XX:XX:XX:XX:50:37	Censored	WPA2 (PSK)	Yes	153	▼	1n
****	XX:XX:XX:XX:8B:F8	Censored	WPA2 (PSK)	No	6	▼	0n
Client	XX:XX:XX:XX:40:E6	Censored					0n

Erne*******
XX:XX:XX:XX:66:93
Censored

More Details

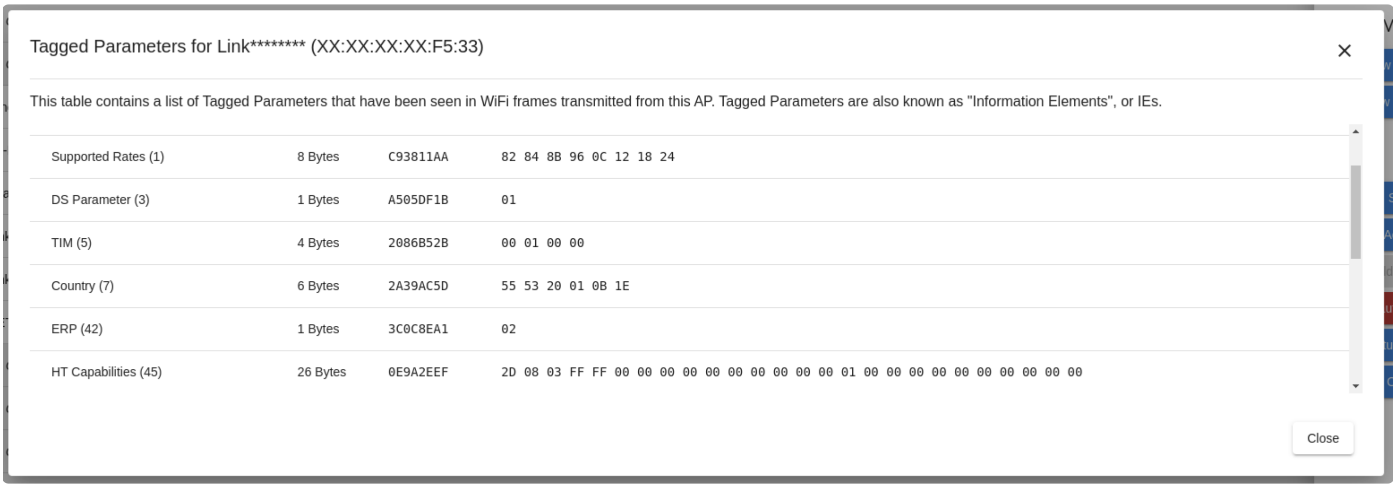
Actions

Access point details

Tagged Parameters

The tagged parameter views offers an in-depth look at the exact parameters advertised by the network.

Tagged parameters are included in the beacon packets which advertise a WiFi network, and contain information about the encryption, channel selection, surrounding traffic, and more.



Tagged Parameters for Link******** (XX:XX:XX:XX:F5:33)

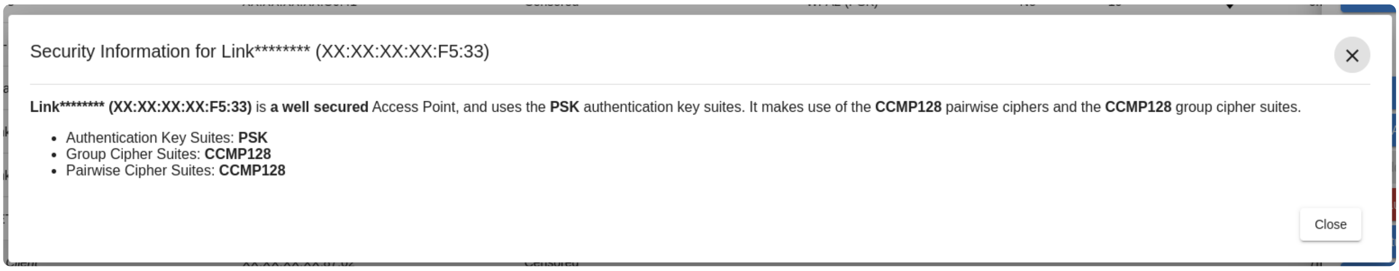
This table contains a list of Tagged Parameters that have been seen in WiFi frames transmitted from this AP. Tagged Parameters are also known as "Information Elements", or IEs.

Supported Rates (1)	8 Bytes	C93811AA	82 84 8B 96 0C 12 18 24
DS Parameter (3)	1 Bytes	A505DF1B	01
TIM (5)	4 Bytes	2086B52B	00 01 00 00
Country (7)	6 Bytes	2A39AC5D	55 53 20 01 0B 1E
ERP (42)	1 Bytes	3C0C8EA1	02
HT Capabilities (45)	26 Bytes	0E9A2EEF	2D 08 03 FF FF 00 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00 00 00

Example tagged parameters

Security Information

The security information panel offers a simplified explanation of the security options employed by the network.



Security Information for Link******** (XX:XX:XX:XX:F5:33)

Link****** (XX:XX:XX:XX:F5:33)** is **a well secured** Access Point, and uses the **PSK** authentication key suites. It makes use of the **CCMP128** pairwise ciphers and the **CCMP128** group cipher suites.

- Authentication Key Suites: **PSK**
- Group Cipher Suites: **CCMP128**
- Pairwise Cipher Suites: **CCMP128**

Example security information

Deauthenticating Networks and Clients

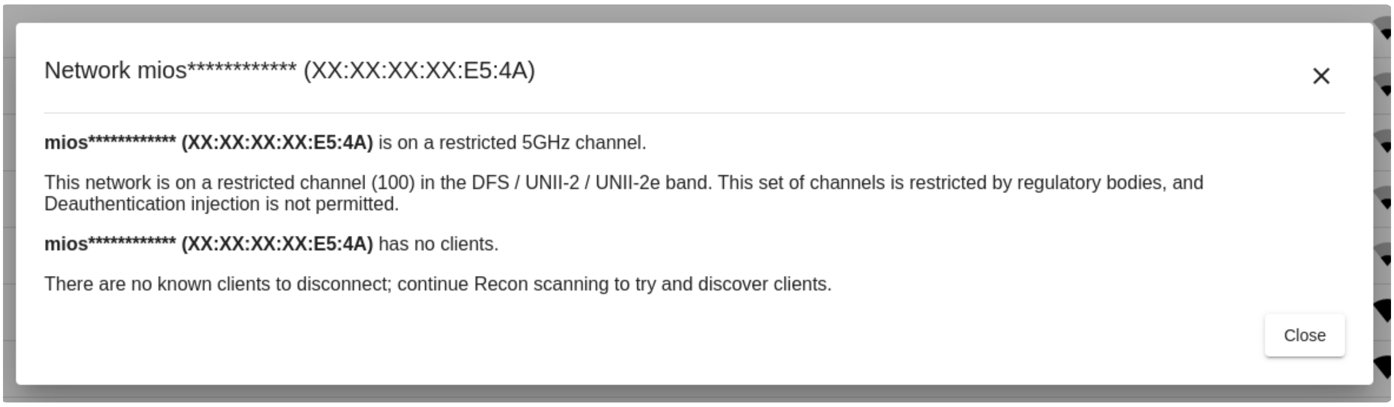
Deauthenticating clients sends a forged WiFi packet which indicates that the client is no longer authorized on the access point.

The WiFi Pineapple can deauthenticate all clients on an access point, or specific single clients.

Deauthenticating a client can be used to migrate the client to another access point, such as the **EvilWPA/2 Twin** access point. It can also be used to cause a client to reconnect to a network, generating a WPA Handshake.

Deauthenticating clients and networks is not possible when:

- There are no clients on the network.
- The client or network uses MFP, or Management Frame Protection. MFP is an extension to the WiFi standards which is designed to prevent impersonation of an access point. This prevents forged deauthentication packets from being respected by the client.
- The client or network is on a restricted channel. The FCC and other regulatory bodies around the world enforce extremely strict limits on part of the 5GHz band known as DFS / UNII-2 / UNII-2e which prohibits transmission on these frequencies if not communicating with an access point.



Network mios************ (XX:XX:XX:XX:E5:4A)

mios********** (XX:XX:XX:XX:E5:4A)** is on a restricted 5GHz channel.

This network is on a restricted channel (100) in the DFS / UNII-2 / UNII-2e band. This set of channels is restricted by regulatory bodies, and Deauthentication injection is not permitted.

mios********** (XX:XX:XX:XX:E5:4A)** has no clients.

There are no known clients to disconnect; continue Recon scanning to try and discover clients.

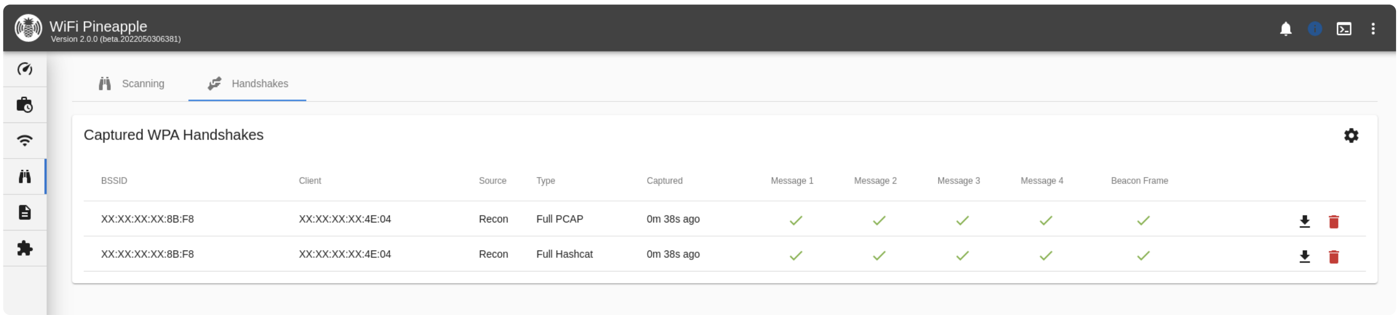
An example warning when deauthentication is not possible

Handshakes

The Handshakes tab shows any captured handshakes. Handshakes are captured in **PCAP** and **Hashcat's 22000** format.

Handshakes that list **Recon Capture** as the source show that they were captured during a Recon scan or a Recon handshake capture.

Handshakes captured from the Evil WPA AP show as **Evil WPA/2 Twin**.



Captured WPA Handshakes

BSSID	Client	Source	Type	Captured	Message 1	Message 2	Message 3	Message 4	Beacon Frame
XX:XX:XX:XX:8B:F8	XX:XX:XX:XX:4E:04	Recon	Full PCAP	0m 38s ago	✓	✓	✓	✓	✓
XX:XX:XX:XX:8B:F8	XX:XX:XX:XX:4E:04	Recon	Full Hashcat	0m 38s ago	✓	✓	✓	✓	✓

Handshake capture

> You can change where the handshakes are saved on the WiFi Pineapple by clicking the Settings icon.

Handshakes

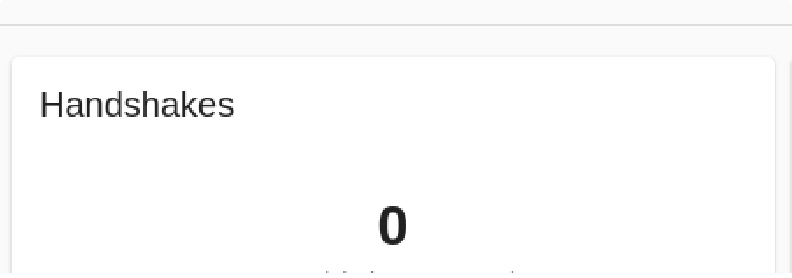
Collecting and using WPA Handshakes.

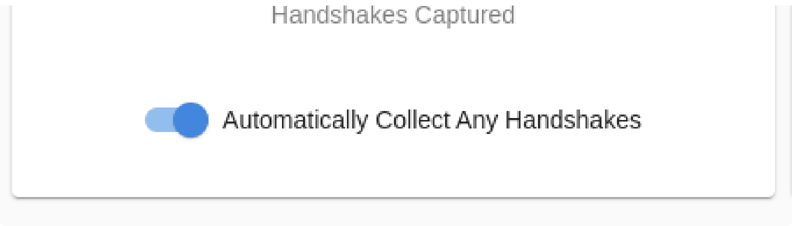
Automatic Handshake Capture

Handshakes are part of normal WiFi traffic when a client joins or refreshes a network.

The WiFi Pineapple can automatically collect handshakes which are caught during a recon scan, with no extra effort.

Automatic handshake capture can be enabled in the Recon panel.



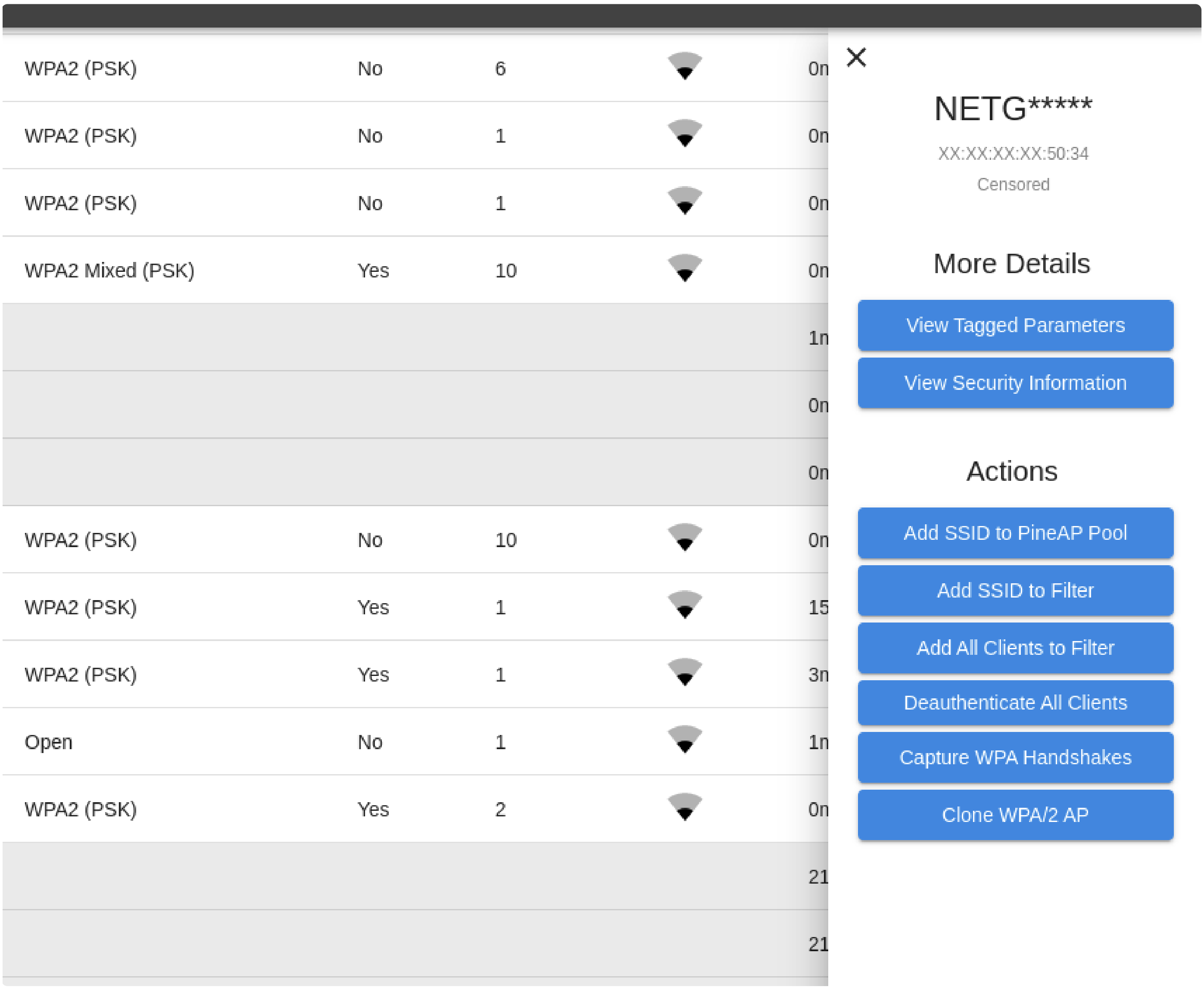

Handshakes Captured

☑ Automatically Collect Any Handshakes

Handshake collection card

Direct Handshake Capture

A specific network may be targeted for handshake capture by selecting the network, then selecting "Capture Handshakes" from the menu:



WPA2 (PSK)	No	6	0n
WPA2 (PSK)	No	1	0n
WPA2 (PSK)	No	1	0n
WPA2 Mixed (PSK)	Yes	10	0n
			1n
			0n
			0n
WPA2 (PSK)	No	10	0n
WPA2 (PSK)	Yes	1	15
WPA2 (PSK)	Yes	1	3n
Open	No	1	1n
WPA2 (PSK)	Yes	2	0n
			21
			21

Capturing handshakes from a network

Directed handshake capture parks the WiFi Pineapple on the same channel as the target device and waits for handshake packets. Remaining on the target channel increases the chances of capturing a complete handshake.

Causing clients to reconnect by using the "Deauthenticate All Clients" option, or deauthenticating a specific client, can increase the chances of capturing a handshake.

EvilWPA Handshakes

The EvilWPA access point clone is able to capture partial handshakes presented by a client, even when it is not possible to fully authenticate the client.

These half-handshakes can be leveraged by hashcat to attack the original passphrase.

Modules

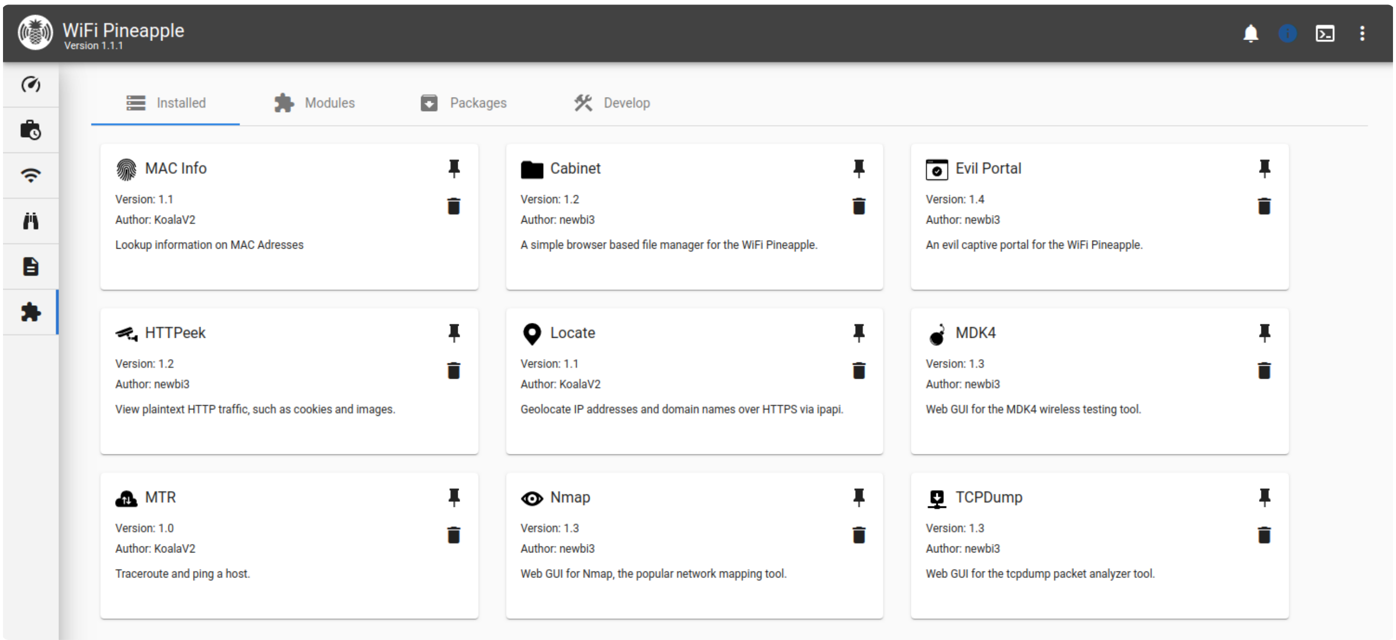
WiFi Pineapple Modules allow the interface to be extended to support new community built features or offer front-ends to command line tools. A vast library of packages is also available.

Modules

Modules are typically contributed by the WiFi Pineapple community, and extend the functionality of the WiFi Pineapple UI. Typically modules offer a graphical front end to existing tools.

> ⓘ Can't find a module for a tool you want? Check out the Packages section to see if there is a command-line equivalent already! You can also help contribute to the module repository!

The main Modules page lists installed modules; to access the module click the corresponding card. To uninstall modules, click the trashcan icon.



MAC Info
Version: 1.1
Author: KoalaV2
Lookup information on MAC Adresses

Cabinet
Version: 1.2
Author: newbi3
A simple browser based file manager for the WiFi Pineapple.

Evil Portal
Version: 1.4
Author: newbi3
An evil captive portal for the WiFi Pineapple.

HTTPeek
Version: 1.2
Author: newbi3
View plaintext HTTP traffic, such as cookies and images.

Locate
Version: 1.1
Author: KoalaV2
Geolocate IP addresses and domain names over HTTPS via ipapi.

MDK4
Version: 1.3
Author: newbi3
Web GUI for the MDK4 wireless testing tool.

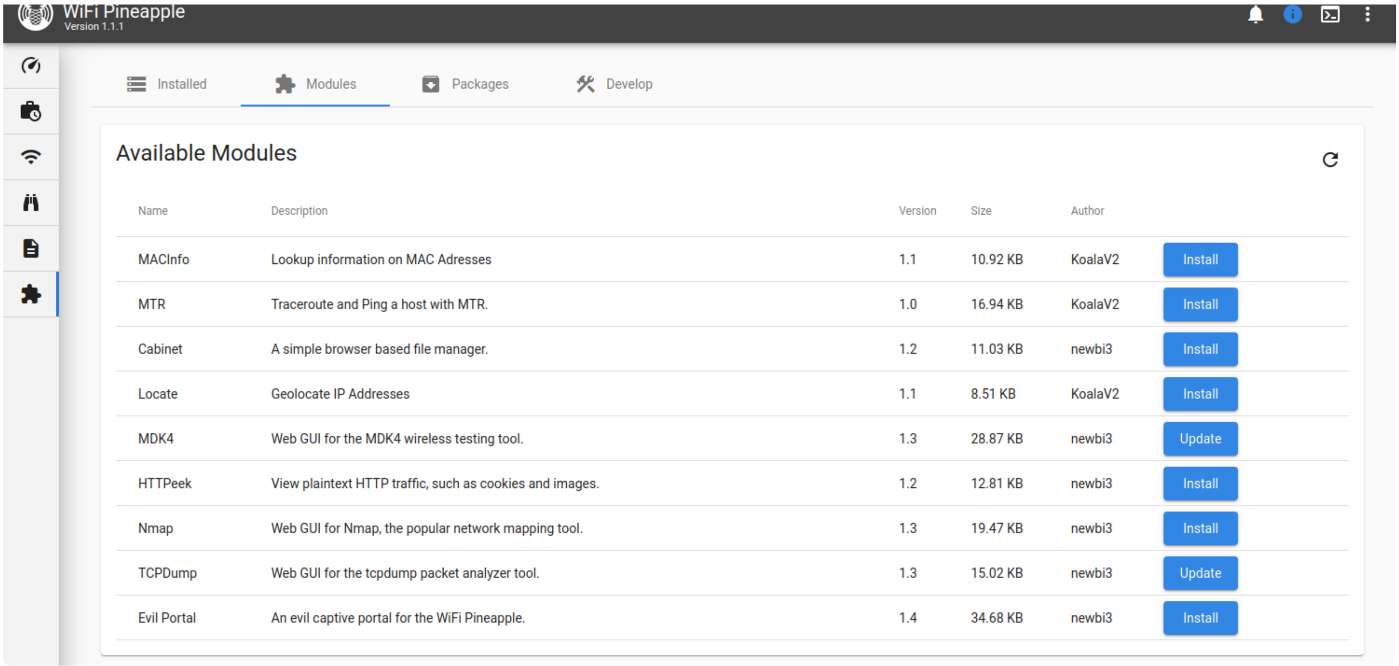
MTR
Version: 1.0
Author: KoalaV2
Traceroute and ping a host.

Nmap
Version: 1.3
Author: newbi3
Web GUI for Nmap, the popular network mapping tool.

TCPDump
Version: 1.3
Author: newbi3
Web GUI for the tcpdump packet analyzer tool.

A list of installed modules

For a list of available modules that you haven't installed, or to view updates for installed modules, you switch to the **Modules** tab. Here you can view the name, description, version, size and author of the module. To install modules or update them, click the **Install/Update** button.



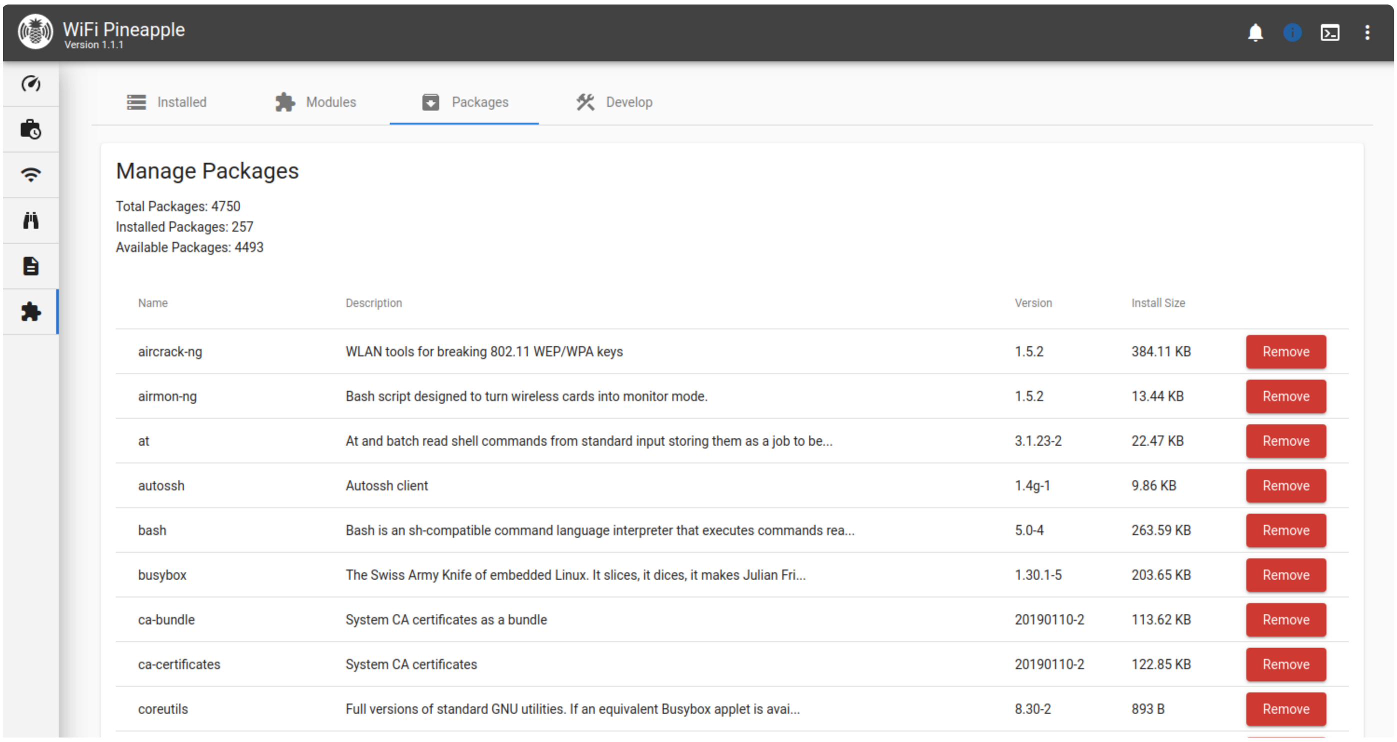
Available Modules

Name	Description	Version	Size	Author	
MACInfo	Lookup information on MAC Adresses	1.1	10.92 KB	KoalaV2	Install
MTR	Traceroute and Ping a host with MTR.	1.0	16.94 KB	KoalaV2	Install
Cabinet	A simple browser based file manager.	1.2	11.03 KB	newbi3	Install
Locate	Geolocate IP Addresses	1.1	8.51 KB	KoalaV2	Install
MDK4	Web GUI for the MDK4 wireless testing tool.	1.3	28.87 KB	newbi3	Update
HTTPeek	View plaintext HTTP traffic, such as cookies and images.	1.2	12.81 KB	newbi3	Install
Nmap	Web GUI for Nmap, the popular network mapping tool.	1.3	19.47 KB	newbi3	Install
TCPDump	Web GUI for the tcpdump packet analyzer tool.	1.3	15.02 KB	newbi3	Update
Evil Portal	An evil captive portal for the WiFi Pineapple.	1.4	34.68 KB	newbi3	Install

Packages

The packages tab allows you to browse a variety of available tools and drivers for your WiFi Pineapple. These packages often contain a command line utility, which can be accessed via SSH or via the Web Terminal.

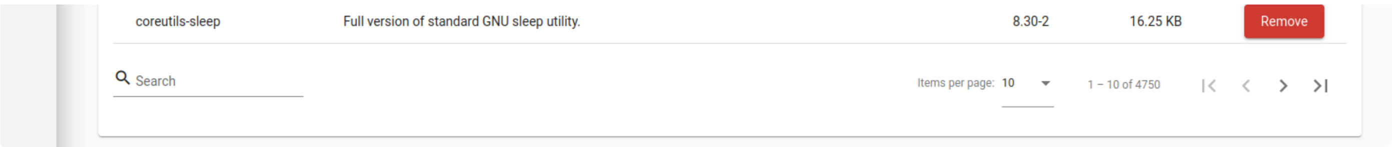
> ⓘ Press the backtick (`) key on your keyboard or click the terminal icon in the upper right to open the Web Terminal, or connect via standard SSH to access the WiFi Pineapple command line.



Manage Packages

Total Packages: 4750
Installed Packages: 257
Available Packages: 4493

Name	Description	Version	Install Size	
aircrack-ng	WLAN tools for breaking 802.11 WEP/WPA keys	1.5.2	384.11 KB	Remove
airmon-ng	Bash script designed to turn wireless cards into monitor mode.	1.5.2	13.44 KB	Remove
at	At and batch read shell commands from standard input storing them as a job to be...	3.1.23-2	22.47 KB	Remove
autossh	Autossh client	1.4g-1	9.86 KB	Remove
bash	Bash is an sh-compatible command language interpreter that executes commands rea...	5.0-4	263.59 KB	Remove
busybox	The Swiss Army Knife of embedded Linux. It slices, it dices, it makes Julian Fri...	1.30.1-5	203.65 KB	Remove
ca-bundle	System CA certificates as a bundle	20190110-2	113.62 KB	Remove
ca-certificates	System CA certificates	20190110-2	122.85 KB	Remove
coreutils	Full versions of standard GNU utilities. If an equivalent Busybox applet is avai...	8.30-2	893 B	Remove



coreutils-sleep	Full version of standard GNU sleep utility.	8.30-2	16.25 KB	Remove

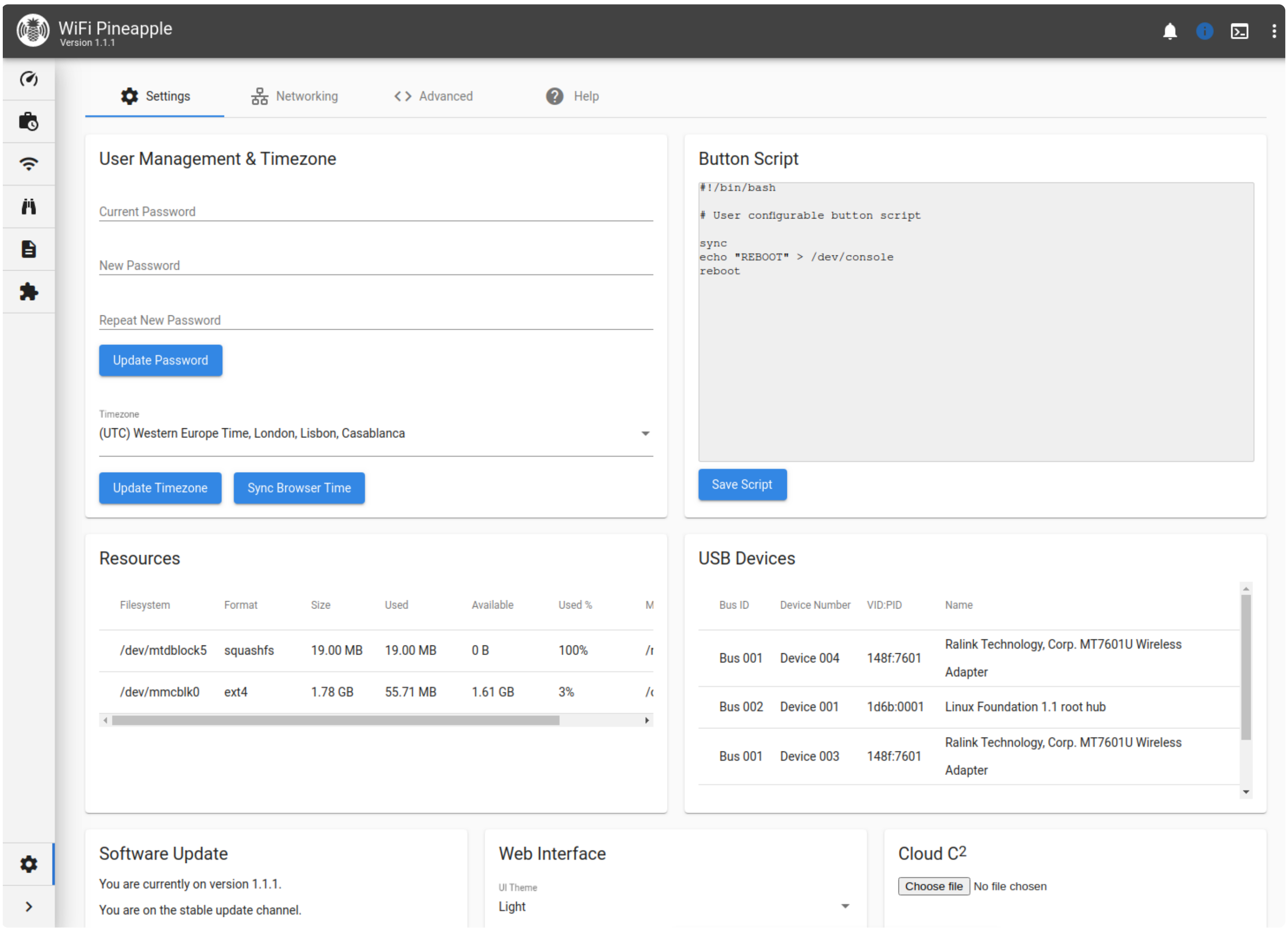
Package settings

Settings

The Settings page allows you to modify aspects of your WiFi Pineapple, check for updates and customise the user interface.

Settings

From the main **Settings** page, you can configure the password and timezone and button script. On the second row of cards, you can view the currently mounted file systems and connected USB devices. On the bottom row, you can check for software updates, change the UI theme and configure the device for Hak5 Cloud C².



User Management & Timezone

Timezone: (UTC) Western Europe Time, London, Lisbon, Casablanca

Button Script

```
#!/bin/bash

# User configurable button script

sync
echo "REBOOT" > /dev/console
reboot
```

Resources

Filesystem	Format	Size	Used	Available	Used %	M
/dev/mtdblock5	squashfs	19.00 MB	19.00 MB	0 B	100%	/r
/dev/mmcblk0	ext4	1.78 GB	55.71 MB	1.61 GB	3%	/c

USB Devices

Bus ID	Device Number	VID:PID	Name
Bus 001	Device 004	148f:7601	Ralink Technology, Corp. MT7601U Wireless Adapter
Bus 002	Device 001	1d6b:0001	Linux Foundation 1.1 root hub
Bus 001	Device 003	148f:7601	Ralink Technology, Corp. MT7601U Wireless Adapter

Software Update

You are currently on version 1.1.1.

You are on the stable update channel.

Web Interface

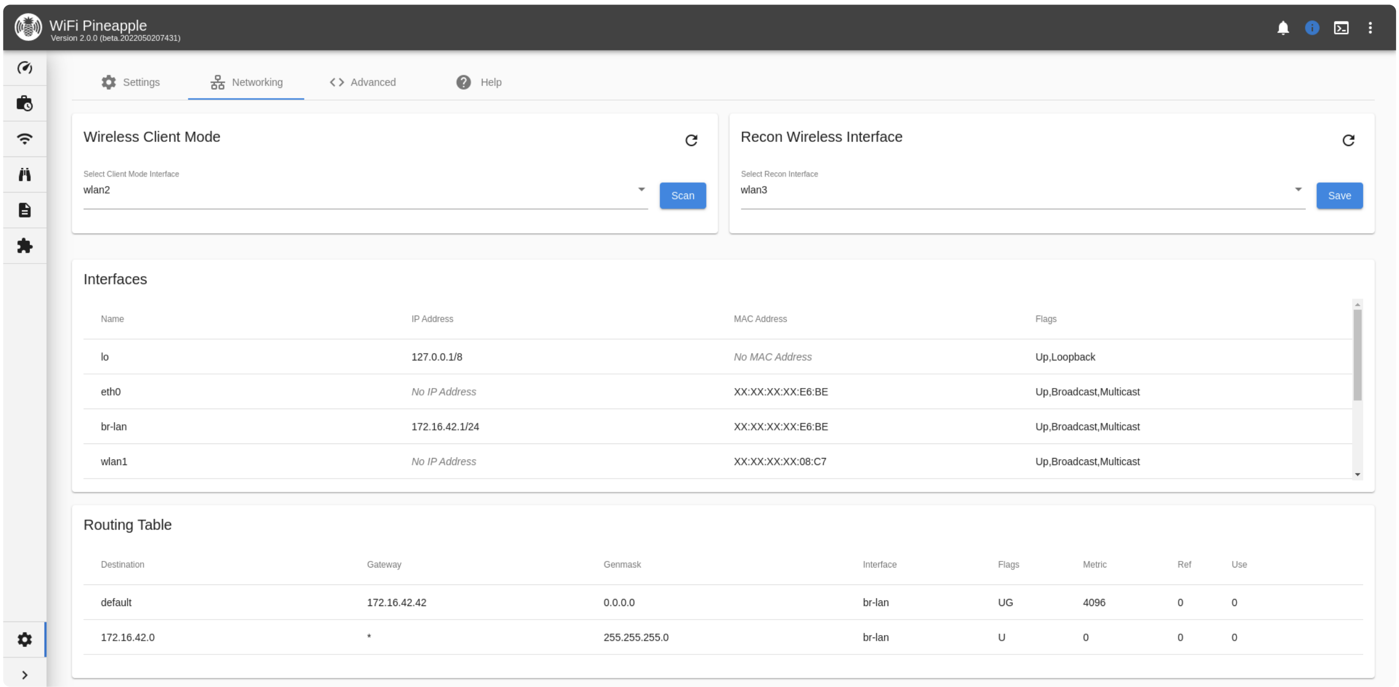
UI Theme: Light

Cloud C2

Typical settings

Networking

The **Networking** tab shows easy to use cards for configuring a Client connection to another Access Point, set the interface used for Recon as well as listing the current interfaces and routing table.



WiFi Pineapple
Version 2.0.0 (beta.2022050207431)

Wireless Client Mode

Select Client Mode Interface: wlan2

Recon Wireless Interface

Select Recon Interface: wlan3

Interfaces

Name	IP Address	MAC Address	Flags
lo	127.0.0.1/8	*No MAC Address*	Up,Loopback
eth0	*No IP Address*	XX:XX:XX:XX:E6:BE	Up,Broadcast,Multicast
br-lan	172.16.42.1/24	XX:XX:XX:XX:E6:BE	Up,Broadcast,Multicast
wlan1	*No IP Address*	XX:XX:XX:XX:08:C7	Up,Broadcast,Multicast

Routing Table

Destination	Gateway	Genmask	Interface	Flags	Metric	Ref	Use
default	172.16.42.42	0.0.0.0	br-lan	UG	4096	0	0
172.16.42.0	*	255.255.255.0	br-lan	U	0	0	0

Typical Network Settings

Client Mode

The most common method for connecting the WiFi Pineapple to the Internet is to use client mode networking. This allows the WiFi Pineapple to connect to an existing WiFi network as a typical client, in the same fashion as a laptop or smartphone would.

Recon Interfaces

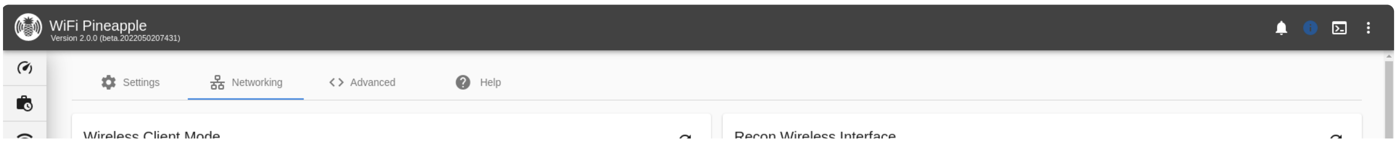
The recon interface is used by the WiFi Pineapple when scanning for WiFi networks and clients, and for deauthing networks and clients.

The default recon interface is `wlan1`, the built-in 2.4GHz WiFi radio.

When a compatible USB WiFi device, such as the Hak5 MK7AC Adapter is connected, the `wlan3` interface will become available and can be used for scanning 2.4GHz *and* 5GHz channels.

USB Ethernet

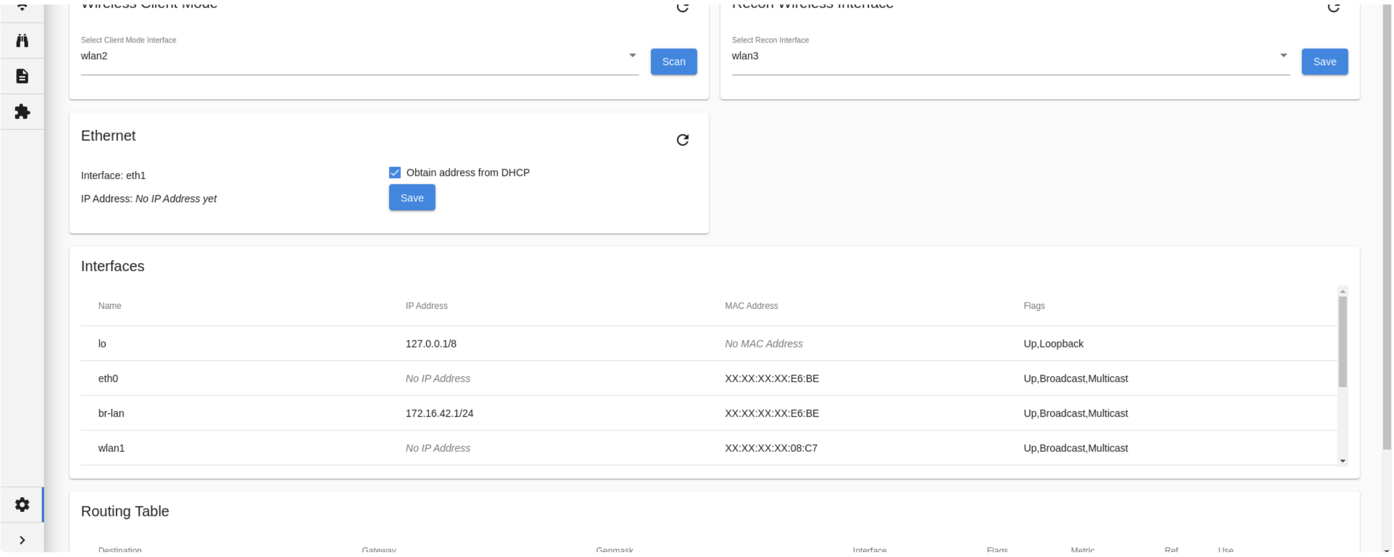
When a compatible USB Ethernet device is connected, the settings interface will display options for configuring a DHCP (default) or static IP address on the interface.



WiFi Pineapple
Version 2.0.0 (beta.2022050207431)

Wireless Client Mode

Recon Wireless Interface



Select Client Mode Interface

wlan2

Select Recon Interface

wlan3

Ethernet

Interface: eth1

IP Address: *No IP Address yet*

☑ Obtain address from DHCP

Interfaces

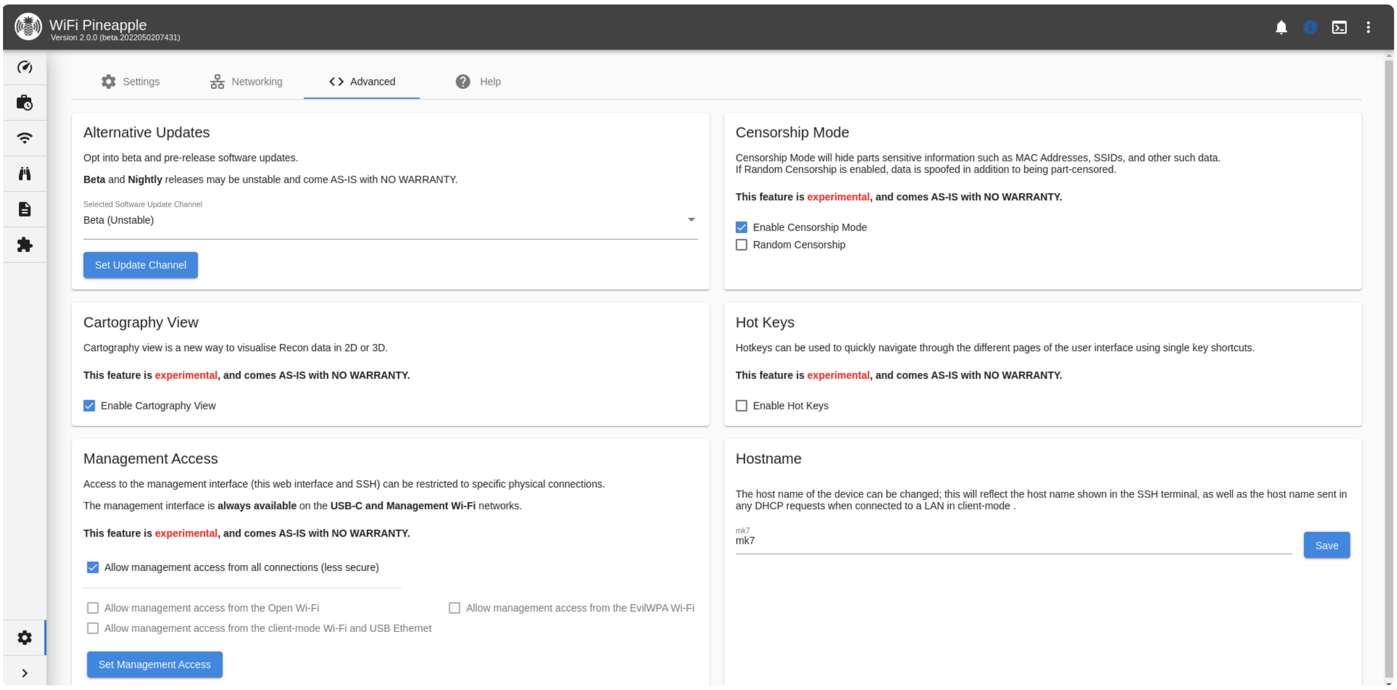
Name	IP Address	MAC Address	Flags
lo	127.0.0.1/8	*No MAC Address*	Up,Loopback
eth0	*No IP Address*	XX:XX:XX:XX:E6:BE	Up,Broadcast,Multicast
br-lan	172.16.42.1/24	XX:XX:XX:XX:E6:BE	Up,Broadcast,Multicast
wlan1	*No IP Address*	XX:XX:XX:XX:08:C7	Up,Broadcast,Multicast

Routing Table

Ethernet configuration settings

Advanced

The **Advanced** tab shows options to change the current update channel for opting into Beta firmware releases. From here you can also access experimental features such as Censorship (hiding sensitive information in the UI) and Cartography (2D or 3D map of Recon data).



Alternative Updates

Opt into beta and pre-release software updates.

Beta and **Nightly** releases may be unstable and come AS-IS with NO WARRANTY.

Selected Software Update Channel

Beta (Unstable)

Censorship Mode

Censorship Mode will hide parts sensitive information such as MAC Addresses, SSIDs, and other such data.
If Random Censorship is enabled, data is spoofed in addition to being part-censored.

This feature is experimental, and comes AS-IS with NO WARRANTY.

☑ Enable Censorship Mode

☐ Random Censorship

Cartography View

Cartography view is a new way to visualise Recon data in 2D or 3D.

This feature is experimental, and comes AS-IS with NO WARRANTY.

☑ Enable Cartography View

Hot Keys

Hotkeys can be used to quickly navigate through the different pages of the user interface using single key shortcuts.

This feature is experimental, and comes AS-IS with NO WARRANTY.

☐ Enable Hot Keys

Management Access

Access to the management interface (this web interface and SSH) can be restricted to specific physical connections.

The management interface is **always available** on the **USB-C and Management Wi-Fi** networks.

This feature is experimental, and comes AS-IS with NO WARRANTY.

☑ Allow management access from all connections (less secure)

☐ Allow management access from the Open Wi-Fi

☐ Allow management access from the EvilWPA Wi-Fi

☐ Allow management access from the client-mode Wi-Fi and USB Ethernet

Hostname

The host name of the device can be changed; this will reflect the host name shown in the SSH terminal, as well as the host name sent in any DHCP requests when connected to a LAN in client-mode .

mk7

mk7

Advanced Settings

Alternative Updates

To participate in the WiFi Pineapple Beta Program, select the "Beta" channel from alternative updates. When new firmware is available, it will show up as an update in the beta channel!

Censorship Mode

Attempt to obfuscate MAC addresses, SSIDs, and other identifiable information in the UI. This option is predominately for streamers, educators, and anyone taking screenshots or making presentations using the WiFi Pineapple.

Remember - always be safe when broadcasting data which could be used to perform location lookups, such as MAC addresses and unique SSIDs. Always review your content before streaming and posting to make sure that no identifiable information is being shown despite censorship attempts.

Cartography Mode

Enable an optional view of network topology and connected clients, found in the Recon panel.

Hotkeys

Enable single-press hotkeys to navigate the web UI

Management Access

By default, the WiFi Pineapple allows access to the management interface (the WiFi Pineapple UI) and the SSH server by default on all interfaces.

To prevent users on the Open and EvilWPA networks, or other users on the WiFi and Ethernet networks the WiFi Pineapple is connected to, from accessing the management interfaces, they can be excluded here.

The management interfaces are *always* available via the USB-C connection and the Management wireless network.

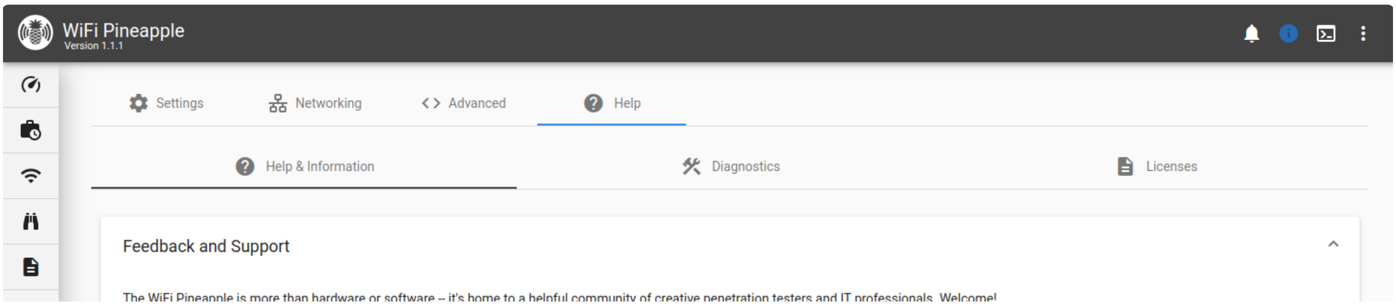
Hostname

Change the default host name of the Pineapple device. This changes the name as shown in the SSH and web shells, and the host name used in DHCP requests sent in WiFi Client mode or over USB Ethernet.

Help

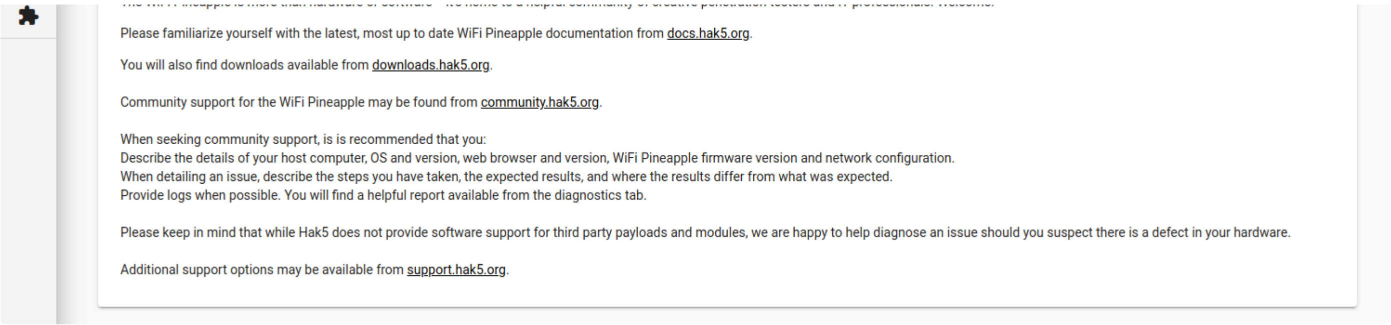
The **Help** tab is split into 3 sub-pages: **Help & Information**, **Diagnostics**, and **Licenses.**

The **Help & Information** page offers links to more resources like this and Hak5 community outlets.



Feedback and Support

The WiFi Pineapple is more than hardware or software -- it's home to a helpful community of creative penetration testers and IT professionals. Welcome!



The WiFi Pineapple is more than hardware or software – we're home to a helpful community of creative penetration testers and IT professionals. Welcome!

Please familiarize yourself with the latest, most up to date WiFi Pineapple documentation from docs.hak5.org.

You will also find downloads available from downloads.hak5.org.

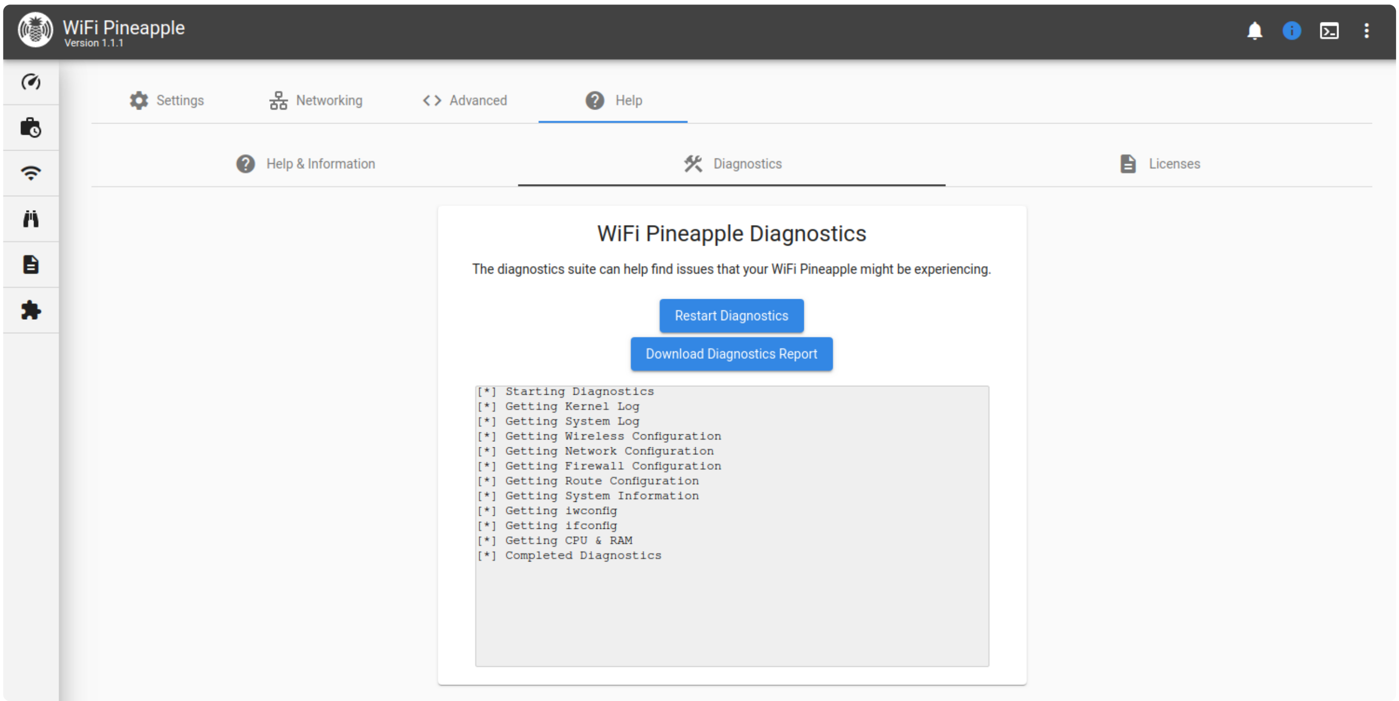
Community support for the WiFi Pineapple may be found from community.hak5.org.

When seeking community support, is is recommended that you:
Describe the details of your host computer, OS and version, web browser and version, WiFi Pineapple firmware version and network configuration.
When detailing an issue, describe the steps you have taken, the expected results, and where the results differ from what was expected.
Provide logs when possible. You will find a helpful report available from the diagnostics tab.

Please keep in mind that while Hak5 does not provide software support for third party payloads and modules, we are happy to help diagnose an issue should you suspect there is a defect in your hardware.

Additional support options may be available from support.hak5.org.

The **Diagnostics** tab lets you generate a convenient diagnostics file that can be used to help troubleshoot any issues you may be experiencing with your WiFi Pineapple.



WiFi Pineapple Diagnostics

The diagnostics suite can help find issues that your WiFi Pineapple might be experiencing.

```
[*] Starting Diagnostics
[*] Getting Kernel Log
[*] Getting System Log
[*] Getting Wireless Configuration
[*] Getting Network Configuration
[*] Getting Firewall Configuration
[*] Getting Route Configuration
[*] Getting System Information
[*] Getting iwconfig
[*] Getting ifconfig
[*] Getting CPU & RAM
[*] Completed Diagnostics
```

Cloud C²

Connecting the WiFi Pineapple to Cloud C²

Cloud C²

Cloud C² makes it easy for pen testers and IT security teams to deploy and manage fleets of Hak5 gear from a simple cloud dashboard.

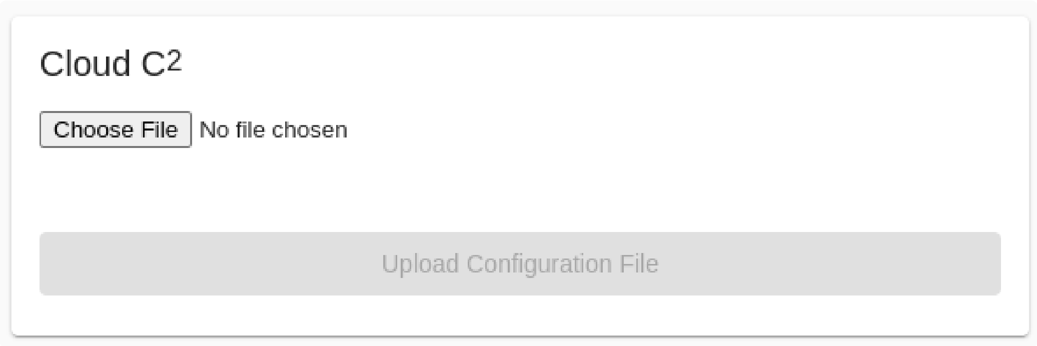
Cloud C² is a self-hosted web-based command and control suite for networked Hak5 gear that lets you pentest from anywhere.

Linux, Mac and Windows computers can host the Cloud C² server while Hak5 gear such as the WiFi Pineapple, LAN Turtle and Packet Squirrel can be provisioned as clients.

Connecting to Cloud C^2

Once you have Cloud C^2 installed and configured, adding a WiFi Pineapple to your server is simple!

1. Create a device in your Cloud C^2 instance following these steps
2. Download the device configuration file
3. Navigate to "Settings" on the WiFi Pineapple
4. Click the "Choose File" button in the Cloud C^2 card
5. Upload your configuration file



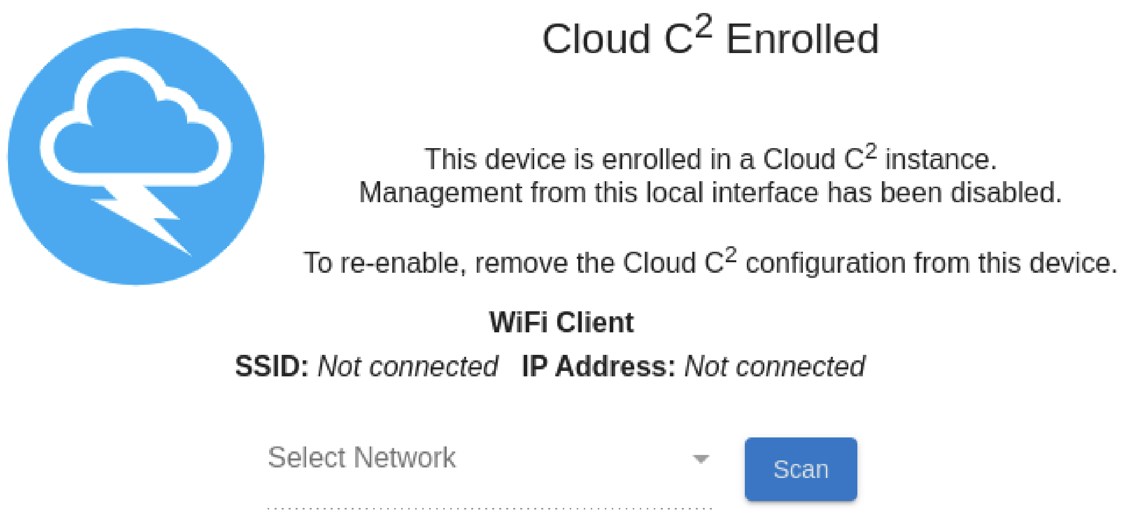
Cloud C^2

Uploading a Cloud C^2 configuration

WiFi Pineapple and Cloud C^2

Once connected to a server, the Cloud C^2 service takes over most configuration and operation of the WiFi Pineapple.

Typical operations such as starting, stopping, and viewing recon scans, configuring filters, etc, are managed centrally by the Cloud C^2 server, and the local WiFi Pineapple UI is paused. The Cloud C^2 alert on the WiFi Pineapple allows for basic network configuration.



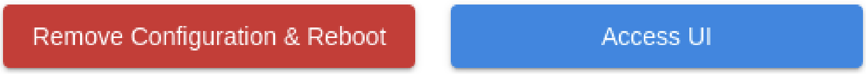
Cloud C^2 Enrolled

This device is enrolled in a Cloud C^2 instance.
Management from this local interface has been disabled.

To re-enable, remove the Cloud C^2 configuration from this device.

WiFi Client

SSID: *Not connected* **IP Address:** *Not connected*



A WiFi Pineapple running under Cloud C^2

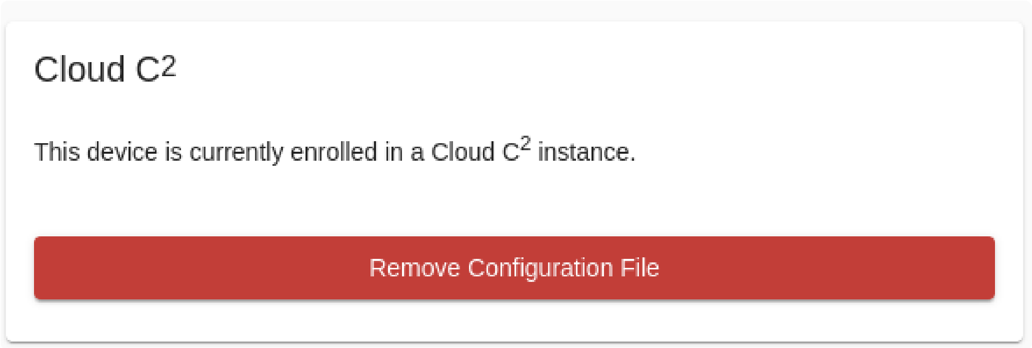
Should you find it necessary to make changes to the WiFi Pineapple locally, the UI can be re-enabled by the "Access UI" button.

> ⚠ **Warning** - The Cloud C^2 server will overwrite some configuration options, such as the PineAP and Recon Scan controls. Local control of the WiFi Pineapple while connected to Cloud C^2 should only be used for configuration changes that cannot be made remotely.

Disconnecting from Cloud C^2

Your WiFi Pineapple can be unsubscribed from Cloud C^2 by clicking the "Remove Configuration & Reboot" button.

If you are in Local UI Bypass mode, it can be unsubscribed by navigating to "Settings" and using "Remove Configuration File" in the Cloud C^2 card.


Cloud C^2

This device is currently enrolled in a Cloud C^2 instance.

Removing the Cloud C^2 connection from Settings

Developer Documentation

Developer Resources

The WiFi Pineapple developer documentation, for things such as **Rest API usage**, **Python API usage**, **Module development** and more is currently available on GitHub.

Soon, they will be transferred to new sections here.

Contributing to the Module Repository

As mentioned in the WiFi Pineapple Mark VII Modules documentation, part of the process is forking and cloning the WiFi Pineapple Modules Git Repository. Once you have developed your module idea, you are encouraged to contribute to this repository by submitting a Pull Request with your module!

Reviewed and Approved pull requests will add your module to the WiFi Pineapple's module download site, where they will be able to be downloaded directly from the WiFi Pineapple management interface.

WiFi Basics

Introduction to WiFi

In order to get the most out of the WiFi Pineapple, it’s best to have a basic understanding of some WiFi principals. This will lay the foundation to mastering the PineAP Suite – the WiFi sniffing and injection engine at the core of the WiFi Pineapple. Armed with this knowledge you’ll be equipped to execute a responsible and successful wireless audit by following our recommended wireless auditing workflow.

The purpose of this section is not to be all encompassing on the low level operation of the IEEE 802.11 specification lovingly known as WiFi, but rather a crash course in the absolute basics necessary for understanding the operation of PineAP and other WiFi Pineapple components.

Radios and Chipsets

Every WiFi radio is a transceiver, meaning it can transmit (TX) and receive (RX) information. Not every radio is created equal, however, as their capabilities may differ significantly. Software support in particular may inhibit an otherwise fine bit of silicon. In particular, modes of operation may be restricted either by hardware or software.

For the most part chipsets from Atheros and Mediatek have excellent support, with a few Ralink and Realtek chipsets having made a name for themselves in the infosec community as well. Radio chipsets typically interface with a computer over a bus like PCI or USB. A WiFi radio is often called a wireless network interface controller (WNIC or Wireless NIC).

On the other hand a SoC (System on a Chip) is a special WiFi chipset which combines the radio with its own CPU. WiFi SoCs, unlike typical x86-based PCs, traditionally run MIPS or ARM based CPUs. While lower in clock speed than their PC counterparts, they’re specifically optimized for high performance networking. The WiFi Pineapple Mark VII is based on Mediatek MT7601U and MT7610U chipsets.

Stations and APs

Technically speaking in regards to the architecture of any wireless network, each component is referred to as a station (STA). There are two categories of stations in an infrastructure mode WiFi setup — the base station (access point) and station (client). Be aware of this terminology as it may come up in other programs and documentation. Generally the WiFi Pineapple will refer to base stations as their more common name, access point or simply AP, and stations as clients or client devices.

Transmit Power

There are four aspects which influence the overall transmission power of a WiFi radio. The first in the chain is what's being transmitted from the chipset or SoC natively. This is typically around 20 dBm or 100 mW and is often expressed in the operating system as txpower.

Next is any given amplifier which will boost the source signal before it reaches the antenna. This additional element to the chain is not necessarily integrated with the SoC, and thus may not reflect the actual txpower determined by the operating system.

The final part of the chain is the antenna, which offer the gain as rated in dBi. Additionally, higher gain antennas may be equipped, with 9 dBi being a common size for a standard omnidirectional antenna.

The total output power of this chain is expressed as EIRP, or equivalent isotropically radiated power. The EIRP is calculated by adding the output power of the radio (plus any amplification) in dBm with the gain of the antenna in dBi. For example a 24 dBm (250 mW) radio with a 5 dBi antenna will have a total output power of 29 dBm (800 mW).

Local regulations will determine the maximum transmission power of any WiFi equipment. For example in the United States the FCC states that a 2.4 GHz point-to-multipoint system may have a maximum of 36 dBm EIRP (4 watts) while point-to-point systems may achieve much higher EIRP.

Antennas

Antennas impact how a signal is transmitted or received.

An antenna can not **create** power, it can only **shape** the signal. An antenna offers signal gains in one aspect at the cost of other aspects.

Antennas are typically *directional*, where the signal gains are concentrated in one direction, or *omnidirectional*, where the signal is optimized for reception from all directions.

The WiFi Pineapple ships with standard *omnidirectional* antennas. These are the most appropriate for typical use cases where the goal is to detect access points and clients in the surrounding area.

Antenna Gains

Antenna gains are typically measured in *dBi*, or "dB over isotropic", a theoretical perfect antenna with no gain.

The higher the gain, the more the signal is impacted.

> ⓘ Remember - more gain is not always better! There is always a trade-off with signal gain!

Omnidirectional Antennas

Omnidirectional antennas are typically found on access points, WiFi interface cards, and of course the WiFi Pineapple.

An omnidirectional antenna is designed to radiate in a roughly spherical shape.

As the gain of an omnidirectional antenna increases, the *horizontal coverage* increases but the *vertical coverage* decreases.

> ⓘ Excessively high gains on omnidirectional antennas can be detrimental! Above approximately 9dBi of gain, the vertical range of the antenna can become so limited that clients and access points more than a foot or two higher or lower than the device are invisible!

Directional Antennas

Directional antennas can be used to shape the signal in a specific direction. Typically directional antennas cover an arc measured in degrees.

Directional antennas can be useful for targeting a specific device or area, but often are not the best solution for general data gathering.

Channels and Regions

Radio spectrum is divided up into channels. In the 2.4 GHz spectrum there are 14 channels, with channels 1, 6, 11 and 14 being non-overlapping. As described above in terms of bandwidth, the first channel in the 802.11g protocol begins at 2.400 GHz and ends at 2.422 GHz for a total bandwidth of 22 MHz. The first channel is then described as being centered at 2.412 GHz.

Channel availability is determined by region, with North America only having legal use of channels 1-11 while Europe and most of the world may use channels 1-13. Japan is special and gets access to all of the channels including 14 all to itself.

The 5 GHz spectrum is much more complicated in regards to bandwidth and channel availability by region with further restrictions on indoor/outdoor use. In the United States the FCC designates U-NII (Unlicensed National Information Infrastructure) bands 1-3 available, with 45 channels in total operating in 20, 40, 80 and 160 MHz bandwidth.

The WiFi Pineapple Mark VII operates in the 2.4 GHz band, with optional support for 5GHz operation using a supported USB WiFi device, while the WiFi Pineapple Enterprise operates in both the 2.4 and 5 GHz bands.

It’s also important to note that similar to modes of operation, a radio can only occupy one channel at a time.

For this reason channel hopping is necessary in order to obtain a complete picture of the given spectrum. When performing a Recon scan, the WiFi Pineapple will switch one of its radios into monitor mode to passively listen on a channel. The radio will take a moment to note any data of interest on each channel before moving on to the next.

Further information on WiFi channels, their regulatory domains, and how they are mapped, can be found on resources such as Wikipedia.

Protocols

There are several WiFi protocols known by their letter designated IEEE 802.11 specifications, such as 802.11a, 802.11b, 802.11g, 802.11n, and 802.11AC. The differences are related to frequency (aka band or spectrum), data rate (aka throughput or transfer speed), bandwidth, modulation and range.

Bandwidth is often confused with data rate. While there is often a correlation between greater bandwidth and greater data rate, in terms of radio the bandwidth refers to the difference between the upper and lower frequencies of a given channel as measured in hertz. For example, with the 802.11b and 802.11g protocols the first channel will have a lower frequency of 2.400 GHz and an upper frequency of 2.422 GHz for a total of 22 MHz bandwidth, however the 802.11g protocol uses a more advanced encoding scheme allowing for significantly faster data rates in the same amount of bandwidth.

Modulation also affects data rate, with the most common modulation types being OFDM or Orthogonal frequency-division multiplexing and QAM or Quadrature Amplitude Modulation. In addition to being a mouthful, these are digital encoding techniques used to cram a lot of data on a small amount of spectrum. Typically newer 802.11 WiFi standards offer either improvements to the encoding scheme, or entirely new encoding schemes.

802.11a and 802.11b were the first mainstream WiFi protocols, introduced in 1999. 802.11a operates in the 5 GHz band with speeds up to 54 Mbps while 802.11b operates in the 2.4 GHz band with speeds only up to 11 Mbps. Today, these networks are more rare to find, though when they are it’s typically indicative of aging infrastructure.

Modern networks are usually 802.11n and 802.11ac, with data rates as high as 1800 Mbps, though typically lower speeds are actually observed. As the WiFi standards evolve and new products make their way into the marketplace, the common devices evolve.

Typically older devices are still able to use more modern access points via backwards compatibility: An 802.11n device can typically connect to an 802.11ac access point, but will only be able to do so at 802.11n speeds. Not all newer standards are backwards compatible with all devices, however.

Modes of Operation

Most commonly a WiFi radio will operate in one of three modes: Master, Managed, or Monitor. Additional possible modes (including ad-hoc, mesh, peer-to-peer, and repeater) and are both less common and outside the scope of this quick guide.

An Access Point (or simply AP) will operate in Master Mode while client devices operate in Managed Mode.

Monitor mode, sometimes called RFMON for Radio Frequency MONitor, is a special mode that allows the radio to passively monitor all traffic in the given area, and requires special support in the drivers and firmware of the wireless device.

Keep in mind that not all radios have each of these capabilities and some radios have drivers that can only operate in one mode at a time.

Logical Configurations

WiFi networks can operate in a number of configurations, from point-to-point, point-to-multipoint, and multipoint-to-multipoint.

Point-to-point is simply a network of two. Multipoint-to-multipoint is where any node of the network can communicate with any other and is often called an ad-hoc, peer-to-peer or mesh network.

The most common configuration is point-to-multipoint, where a central access point is host to numerous client devices. This is also known as Infrastructure mode. An example of which might be a wireless router in your home with several laptops, phones, game consoles and the like connected. For the most part, this is the configuration we will be focusing on with the WiFi Pineapple.

MAC Addresses

Often called a physical address (PHY addr), the Media Access Control address (MAC address) is a unique identifier assigned to each Network Interface Controller (NIC). Typically this address is “burned” into the ROM of the network interface hardware, though often it may be changed via software.

MAC Addresses are formed by six sets of two hexadecimal digits (octets), typically separated by a dash (-) or colon (:) and may be either universally or locally administered. For example, 00:C0:CA:8F:5E:80.

Universally administered MAC addresses are unique to each network interface manufacturer. The first three octets represent the manufacturer or vendor as its Organizationally Unique Identifier (OUI). In the example above, 00:C0:CA represents the OUI for ALFA, INC – a popular Taiwanese WiFi equipment maker. OUIs are assigned by the Institute of Electrical and Electronics Engineers, Incorporated (IEEE). The vendor of any particular OUI may be determined by checking the IEEE MAC database, or the Wireshark OUI Lookup Tool. A database of OUI ranges is included in the WiFi Pineapple to display the manufacturer of devices.

Locally administered MAC addresses are typically assigned by the network administrator, replacing the universally administered address burned into ROM. For example, one may set their MAC address to DE:AD:BE:EF:C0:FE. This is sometimes called MAC spoofing.

Broadcast and Multicast MAC Addresses

Often with WiFi networks it is necessary to transmit the same bit of information to all stations. To facilitate this, the WiFi specification includes a special broadcast address. Expressed as the MAC

FF:FF:FF:FF:FF:FF, transmissions destined to this address are meant for all stations in the vicinity.

While normally a WiFi interface is only concerned with traffic to and from its own MAC address, the default behavior is to also listen for messages bound to the broadcast address. An example of which is a beacon – a frame which advertises the presence of an access point. A beacon sent to broadcast will be “seen” by all stations in the area.

Similarly, a multicast address is a special type of address which operates like a broadcast address for the most part. Multicast addresses are used to set groups of devices which must communicate to many devices simultaneously, or special services such as mDNS and other service discovery protocols.

SSIDs

If you’ve been using WiFi for a while – and if you’re reading this we'll assume you have been – you’ve undoubtedly run across the term SSID. It’s the human readable “network name” associated with a WiFi Network – like “Joe’s Coffee” or “LAX Airport Free WiFi” or depending on your apartment building, perhaps a lewd comment directed toward neighbors. This “network name” is known as the Service Set Identifier. It can be up to 32 characters long and may identify either a Basic or Extended Service Set.

The majority of WiFi networks are Basic Service Sets (BSS). That is to say a single access point with multiple connected clients – be it laptops, tablets, gaming consoles or IoT coffee makers. Every station (both clients and AP) in the BSS are identified by a Basic Service Set Identification (BSSID). The BSSID is derived from the access point’s MAC address. Specifically the MAC address of the wireless NIC as the access point may also have an Ethernet Network Interface Controller with its own unique MAC address.

Extended Service Sets are larger WiFi networks whereby multiple access points, each with their own BSSID, all share the same SSID or “network name”. For instance a college or corporate campus may require many access points to cover the entire property. In this case the SSID is called an ESSID for Extended Service Set Identification, which facilitates client roaming.

A wireless client considers any access point with the same SSID to be part of the same network, and may choose to connect to any of the available APs. This forms some of the fundamental basis of the **Evil WPA Twin** attack.

802.11 Frame Types

WiFi frames come in three types, each containing several subtypes; control frames, data frames and management frames.

Control frames simply allow data exchange between stations, with Request to Send (RTS), Clear to Send (CTS) and Acknowledgement (ACK) frames facilitating communication with as little loss as possible. Frame loss is in inherent part of WiFi and control frames are intended to best coordinate shared usage of the available spectrum.

Data frames constitute the majority of WiFi communication, with the payload or frame body containing the actual TCP, UDP, or other packets. Since the basic data frame has a limit of 2312 bytes, the actual packets may be broken up into many fragments.

Management frames enable WiFi maintenance, such as advertising the presence of an access point as well as connecting to or disconnecting from such access point.

802.11 Frame Structure

The meat and potatoes of WiFi. Essentially everything transmitted by a wireless NIC comes in the form of a frame. They are the basic unit of most digital transmissions, and surround or encapsulate packets.

Frame Structure

A typical WiFi frame is broken up into several sections, consisting of a MAC header, payload and frame check sequence

The MAC header contains a Frame Control Field which includes, among other things, the 802.11 protocol version and frame type. Address fields including the BSSID, source and destination are also part of this section.

The Payload or frame body contains the actual information (typically a data packet) of either a management or data frame.

The Frame Check Sequence (FCS) concludes the frame with a cyclic redundancy check (CRC) sum of the MAC header and payload. This is used to verify the integrity of the frame and is essential to fault tolerance.

Management Frames

To enable the joining and leaving of a Basic Service Set, management frames contain subtypes such as *beacon*, *probe*, *association*, and *authentication*.

Beacon frames come in only one variety, and advertise the presence of an access point. They contain everything a client needs to know about a network in order to connect, including the SSID, supported data rates, protocol and other parameters pertinent to the APs modulation. Access points regularly transmit beacons, typically several times per second, to the broadcast address.

Beacon frames are essential for network discovery. When a client passively scans for nearby access points, it does so by listening for beacon frames. Typically this is done in conjunction with channel hopping, whereby a client will listen on each channel for a brief period before moving on to the next.

Probe frames further network discovery and come in two variety, *probe requests* and *probe responses*. Probe requests are transmitted by clients seeking access points. Probe responses are the access point’s replies to these client requests.

When a probe request is transmitted by a client seeking an access point, this is considered active scanning. The client will transmit to the broadcast address either a general probe request or a directed probe request. The former simply asks “what access points are around” while the later specifies the particular SSID for which the client seeks.

The probe response includes all of the basic information about the network also included in the beacon frame.

Association frames come in five forms: the *association request*, *association response*, *reassociation request*, *reassociation response*, and *disassociation*. Respectively, these can simply be thought of as “I’d like to be friends”, “Ok, we will/won’t be friends”, “Remember me, I’m your friend”, “I do/don’t remember you” and “Get lost, friend”.

Similar to probe frames, the requests are transmitted by clients while the responses by access points. Disassociation frames in particular are sent by any station wishing to terminate the association. This is the graceful way to ending an association, giving the station a heads up that the conversation is over and allowing it to free up memory in the association table.

Authentication frames are similar to association frames in that they enable the relationship between client and access point to form. Originally only two security states existed for WiFi – Open or Wired Equivalent Privacy (WEP). The later is a broken and deprecated technology which has given way to more secure schemes such as WPA2 and 802.1X. For this reason authentication frames are almost always open, regardless of the security state, with the actual authentication handled by subsequent frames after the station is both authenticated and associated. In this case a client will send an authentication request with the access point sending an authentication response.

Deauthentication frames act similar to **disassociation frames** and are sent from one station to another as a way to terminate communications. For example, an access point may send a deauthentication frame to a client if it is no longer authorized on its network. When this unencrypted management frame is spoofed by a third party, the technique is often called a deauth attack.

Frame Injection

It should be apparent that much of WiFi operation relies on trust, particularly with regard to the validity of source and destination addresses. Given these values may be spoofed, it’s with the technique of frame injection that various attacks may be carried out.

Simply put, frame injection is the process of transmitting any WiFi frame desired, regardless of an association with any station. One example may be a beacon frame injected into the air with specific values set to aid the penetration tester.

Another example may be a deauthentication frame with a spoofed source and destination address. Not all radios and software support this ability. This technique is leveraged by the PineAP suite for a number of attacks using the WiFi Pineapple hardware.

Association and State

With an understanding of management frames, we can explore the states of association. In this example we’re looking at the steps necessary for a connection between a client and an open access point.

In the **Unauthenticated and Unassociated** state, the client seeks the access point. This is either done passively by listening to the broadcast address for beacon frames transmitted by the access point, or actively by transmitting a probe request.

Once the client has received either a probe response or beacon frame from the access point, it can determine its operating parameters (channel, protocol, data rate, modulation details, etc). The client will then send the access point an authentication frame requesting access. In the case of an open network, the access point will send the client back an authentication frame responding with a success message.

Now the client is **Authenticated and Unassociated**. Next the client will send the access point an association request. The access point will reply with an association response.

If successful, the client will now be **Authenticated and Associated**. At this point any additional security, such as WPA2, may be negotiated. Otherwise in the case of an open network, the usual first network interactions will occur. These are the same as in wired networks, and typically begin with obtaining IP address information from a DHCP server on the host network.

In the case of the WiFi Pineapple, the client network is open and the DHCP server will assign new clients with addresses in the 172.16.42.0/24 range

FAQ / Troubleshooting

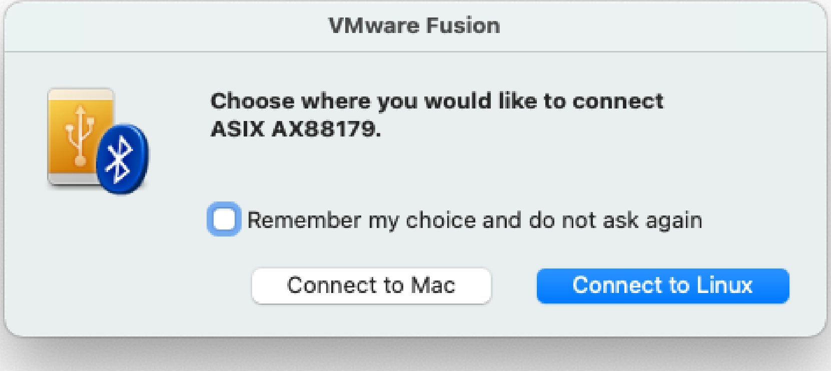
MacOS Support

Starting with macOS Big Sur (macOS 11), changes to the driver model has broken support for the ASIX AX88772 USB Ethernet ASIX chipset.

This is the chipset used by the WiFi Pineapple Mark VII for the wired LAN interface is accessible via the USB-C port.

A driver is available for Apple macOS 10.9 to 10.15 from the manufacturer at https://www.asix.com.tw/en/support/download

It is recommended to instead use a Linux or Windows computer when operating the WiFi Pineapple Mark VII via the USB-C port. This does not impact operation from the Wireless LAN.

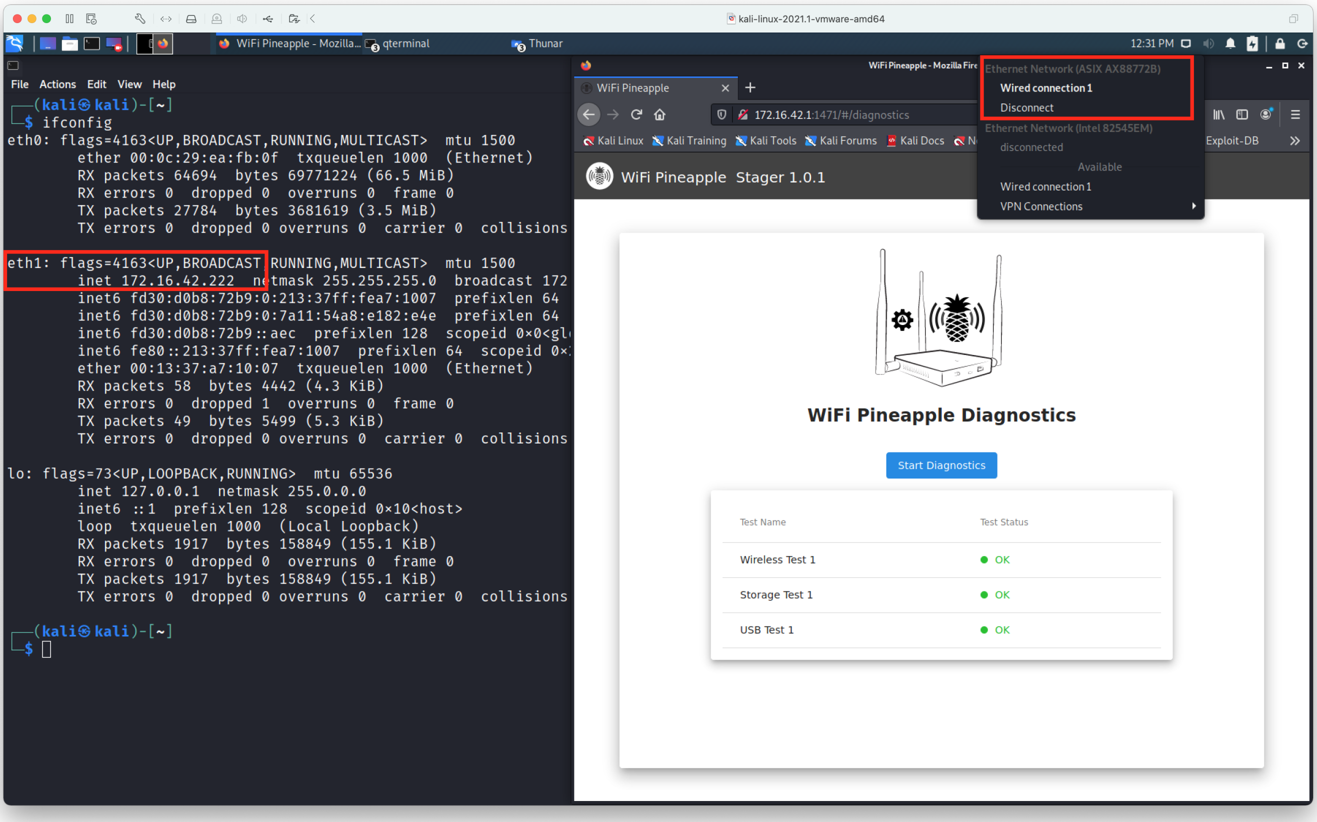


VMware Fusion

Choose where you would like to connect ASIX AX88179.

□ Remember my choice and do not ask again

Alternatively, a virtual machine with USB-passthrough support may be used. Users have reported success with VMware Fusion and Kali Linux on macOS 11 and above.


kali-linux-2021.1-vmware-amd64
WiFi Pineapple - Mozilla...
qterminal
Thunar
12:31 PM
File Actions Edit View Help
WiFi Pineapple - Mozilla Fire
WiFi Pineapple
Ethernet Network (ASIX AX88772B)
Wired connection 1
Disconnect
Ethernet Network (Intel 82545EM)
disconnected
Available
Wired connection 1
VPN Connections
Kali Linux
Kali Training
Kali Tools
Kali Forums
Kali Docs
Exploit-DB
WiFi Pineapple Stager 1.0.1
Start Diagnostics

```
┌──(kali㉿kali)-[~]
└─$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        ether 00:0c:29:ea:fb:0f  txqueuelen 1000  (Ethernet)
        RX packets 64694  bytes 69771224 (66.5 MiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 27784  bytes 3681619 (3.5 MiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

eth1: flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500
        inet 172.16.42.222  netmask 255.255.255.0  broadcast 172
        inet6 fd30:d0b8:72b9:0:213:37ff:fea7:1007  prefixlen 64
        inet6 fd30:d0b8:72b9:0:7a11:54a8:e182:e4e  prefixlen 64
        inet6 fd30:d0b8:72b9::aec  prefixlen 128  scopeid 0x0<gl
        inet6 fe80::213:37ff:fea7:1007  prefixlen 64  scopeid 0x
        ether 00:13:37:a7:10:07  txqueuelen 1000  (Ethernet)
        RX packets 58  bytes 4442 (4.3 KiB)
        RX errors 0  dropped 1  overruns 0  frame 0
        TX packets 49  bytes 5499 (5.3 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

lo: flags=73<UP,LOOPBACK,RUNNING>  mtu 65536
        inet 127.0.0.1  netmask 255.0.0.0
        inet6 ::1  prefixlen 128  scopeid 0x10<host>
        loop  txqueuelen 1000  (Local Loopback)
        RX packets 1917  bytes 158849 (155.1 KiB)
        RX errors 0  dropped 0  overruns 0  frame 0
        TX packets 1917  bytes 158849 (155.1 KiB)
        TX errors 0  dropped 0 overruns 0  carrier 0  collisions

┌──(kali㉿kali)-[~]
└─$ 
```

172.16.42.1:1471/#/diagnostics

WiFi Pineapple Diagnostics

Test Name	Test Status
Wireless Test 1	● OK
Storage Test 1	● OK
USB Test 1	● OK

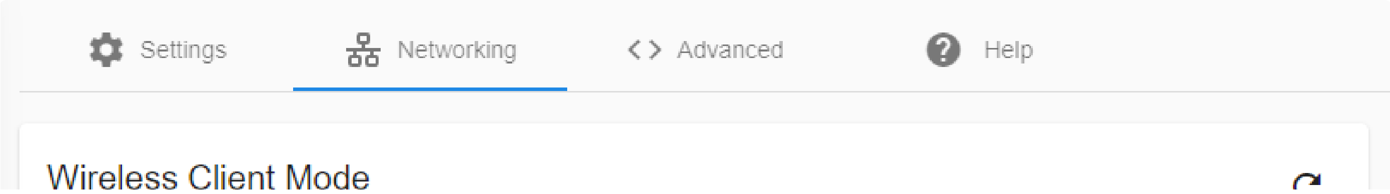
⚠ Because of recent changes to macOS's device driver model, macOS version 11 and above is not supported.

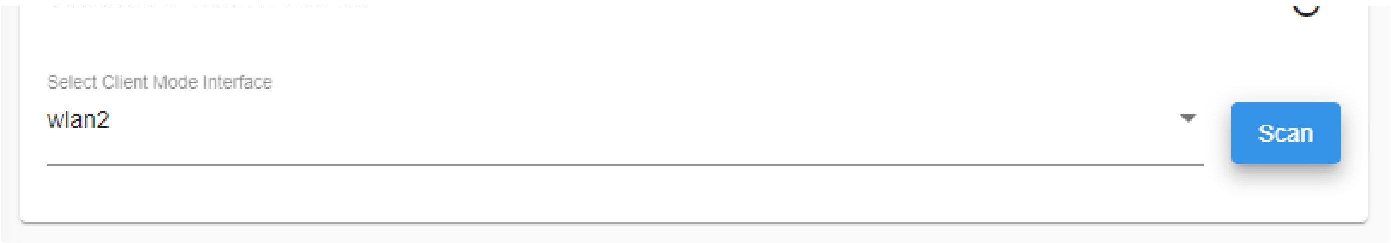
Establishing an Internet Connection

Configuring a Client Mode Connection

You may use a radio on the WiFi Pineapple to connect to an external WiFi network, for getting an internet connection or for communicating with other devices on that network.

To configure a client mode connection, navigate to **Settings > Networking** in the User Interface. You will be presented with a card labelled **Wireless Client Mode**.

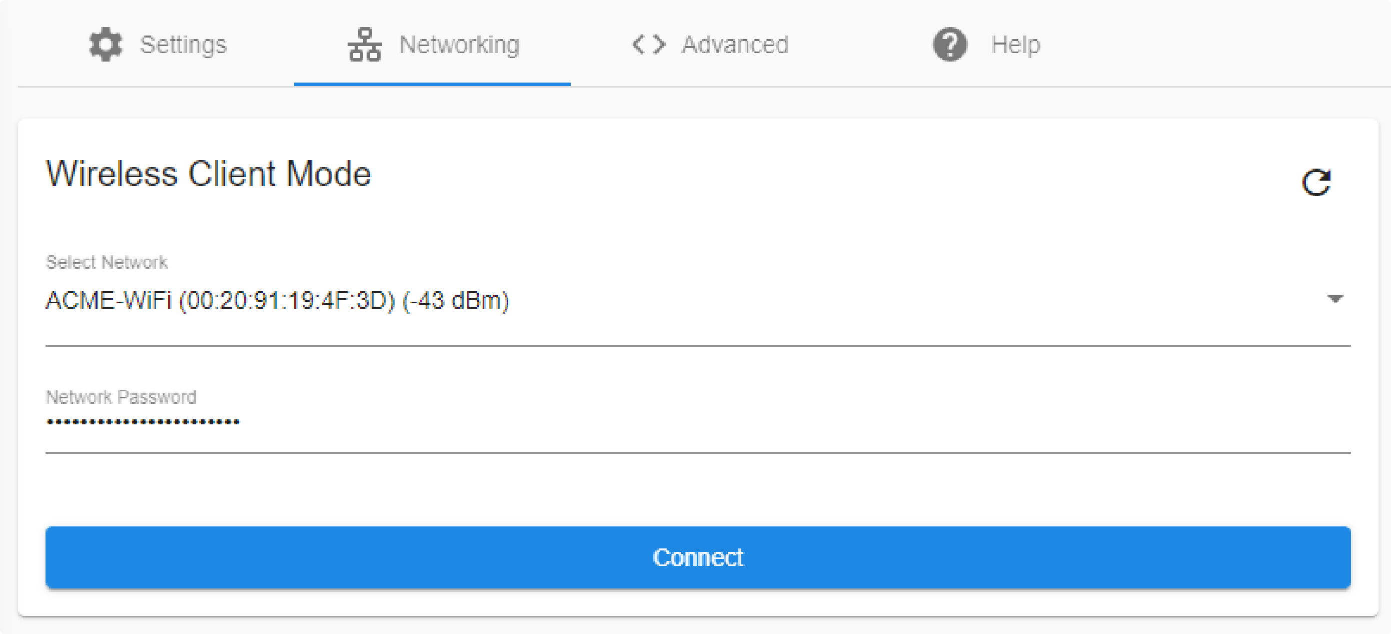




Select Client Mode Interface
wlan2

ⓘ While you may select other wireless interfaces for Client Mode, you are **greatly** recommended to use wlan2, as it is dedicated for Client Mode.

After clicking the **Scan** button, a list of surrounding wireless networks will be listed for you. Select the SSID you wish to connect to, and enter the SSID or PSK if required. Click **Connect** to start a connection.

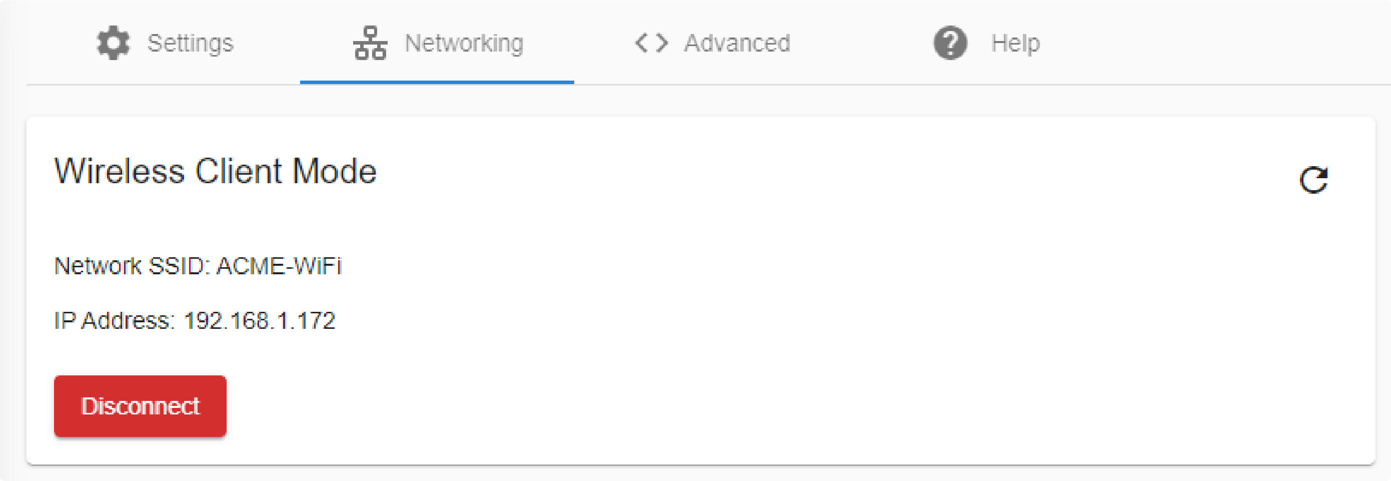


Wireless Client Mode

Select Network
ACME-WiFi (00:20:91:19:4F:3D) (-43 dBm)

Network Password
•••••••••••••••••••••••

If the connection is successful, you will be presented with the associated SSID and an acquired IP, if DHCP is enabled on the network.



Wireless Client Mode

Network SSID: ACME-WiFi

IP Address: 192.168.1.172

ⓘ If you are required to set a static IP address, you must do so via the command line. Press the

> backtick (`) on your keyboard to open a Web Terminal.

> ⓘ The Wireless Client Mode configuration is automatically saved, and an attempt to reconnect will happen every boot, automatically.

Configuring ICS on Linux

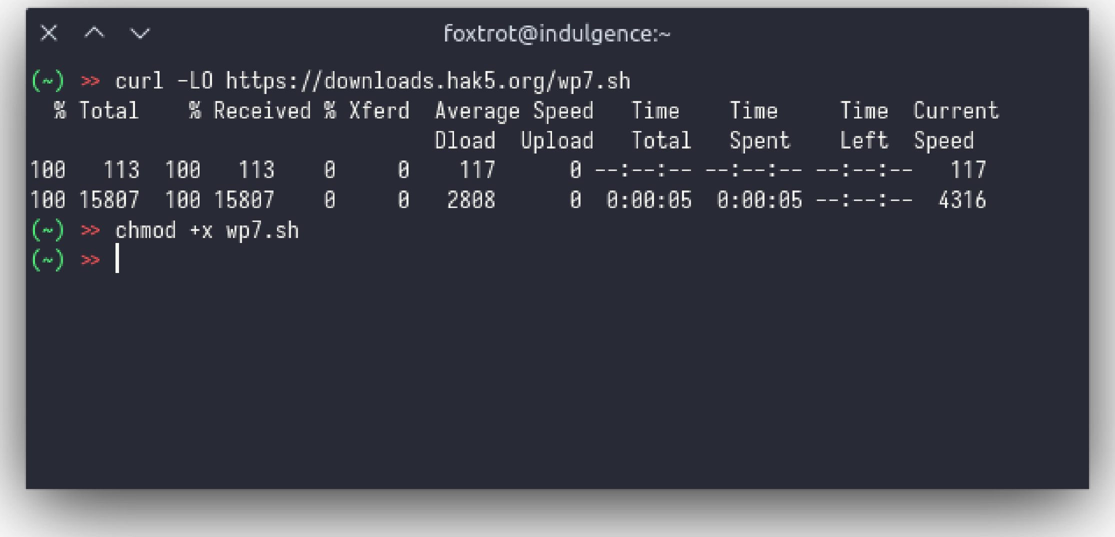
ICS, or **Internet Connection Sharing**, can be used to share internet from your computer to the attached WiFi Pineapple, over it's USB-C Ethernet connection.

Turning on connection sharing with Linux is generally easy, and is further simplified with the `wp7.sh` script available on the Hak5 Download Portal. The `wp7.sh` script will guide you through the setup process.

Getting Started

Start by opening the Terminal emulator for your Linux distribution. On Ubuntu, Gnome Terminal can be found by searching for "Terminal".

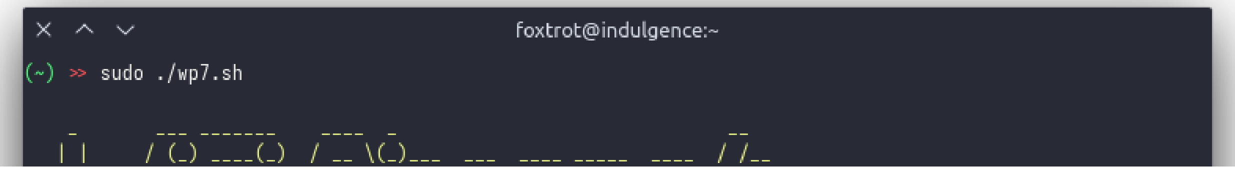
Once the Terminal is open, get the WP7.sh script, and mark it as executable with `chmod`.



foxtrot@indulgence:~

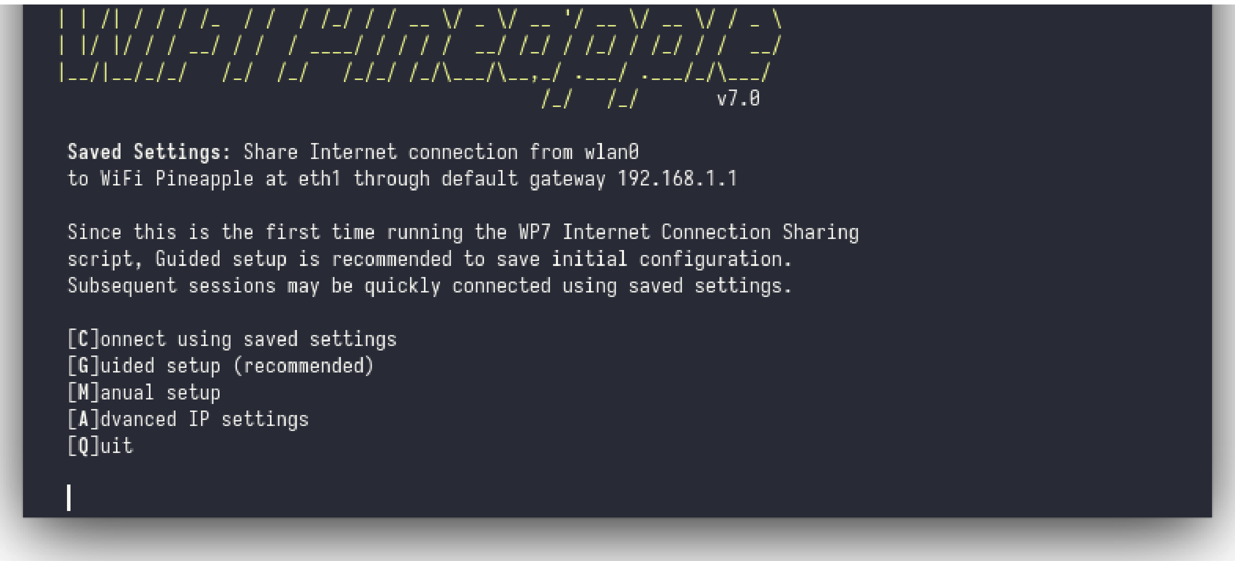
```
(~) >> curl -LO https://downloads.hak5.org/wp7.sh
  % Total    % Received % Xferd  Average Speed   Time    Time     Time  Current
                                 Dload  Upload   Total   Spent    Left  Speed
100   113  100   113    0     0    117      0 --:--:-- --:--:-- --:--:--   117
100 15807  100 15807    0     0   2808      0  0:00:05  0:00:05 --:--:--  4316
(~) >> chmod +x wp7.sh
(~) >> 
```

Once you've done that, execute the script as root, with `sudo ./wp7.sh`.



foxtrot@indulgence:~

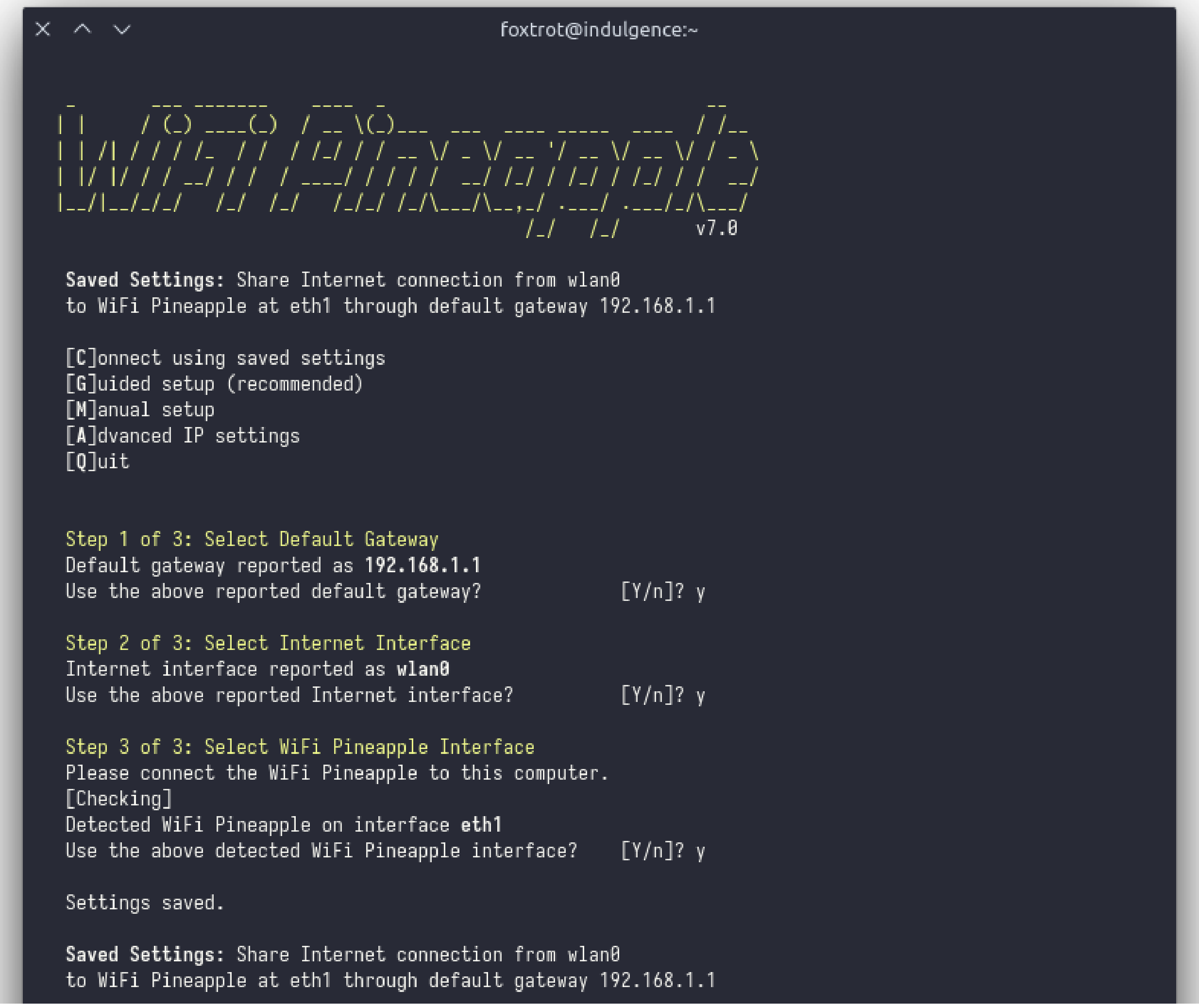
```
(~) >> sudo ./wp7.sh

  _      ___ _______    ____  _                          __
 | |    / (_) ____(_)  / __ \(_)___  ___  ____ _____  ____  / /__
```



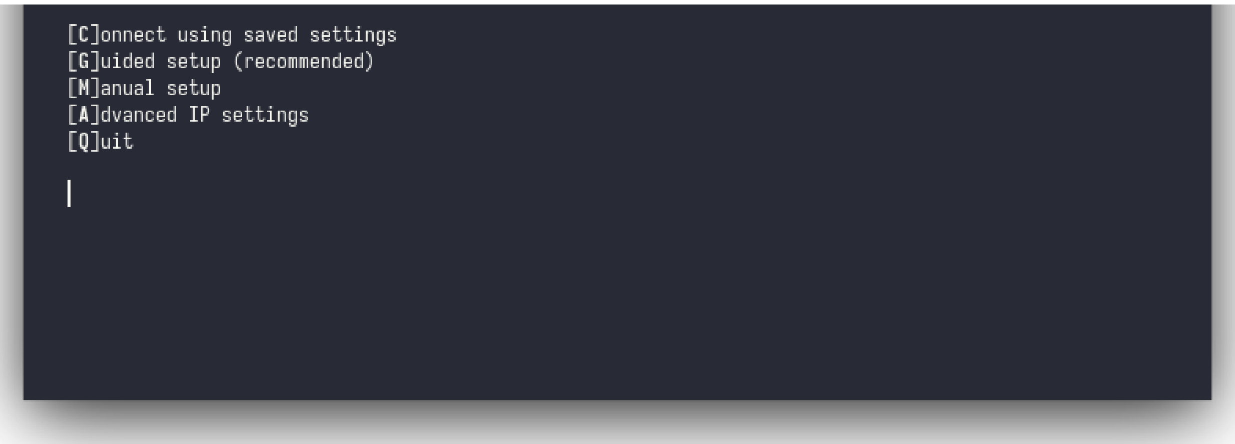
```
| | /| / / / /_  / /  / /_/ / / __ \/ _ \/ __ `/ __ \/ __ \/ / _ \
| |/ |/ / / __/ / /  / ____/ / / / /  __/ /_/ / /_/ / /_/ / /  __/
|__/|__/_/_/   /_/  /_/   /_/_/ /_/\___/\__,_/ .___/ .___/_/\___/
                                            /_/   /_/      v7.0

 Saved Settings: Share Internet connection from wlan0
 to WiFi Pineapple at eth1 through default gateway 192.168.1.1

 Since this is the first time running the WP7 Internet Connection Sharing
 script, Guided setup is recommended to save initial configuration.
 Subsequent sessions may be quickly connected using saved settings.

 [C]onnect using saved settings
 [G]uided setup (recommended)
 [M]anual setup
 [A]dvanced IP settings
 [Q]uit

 |
```

Guided Setup Mode

In this mode, the ICS script will try to automatically determine which interface is the WiFi Pineapple, and what your current network settings are. To do this, press **G** on your keyboard and follow the on-screen instructions.



```
 _       ___ _______    ____  _                              __
| |     / (_) ____(_)  / __ \(_)___  ___  ____ _____  ____  / /__
| | /| / / / /_  / /  / /_/ / / __ \/ _ \/ __ `/ __ \/ __ \/ / _ \
| |/ |/ / / __/ / /  / ____/ / / / /  __/ /_/ / /_/ / /_/ / /  __/
|__/|__/_/_/   /_/  /_/   /_/_/ /_/\___/\__,_/ .___/ .___/_/\___/
                                            /_/   /_/      v7.0

 Saved Settings: Share Internet connection from wlan0
 to WiFi Pineapple at eth1 through default gateway 192.168.1.1

 [C]onnect using saved settings
 [G]uided setup (recommended)
 [M]anual setup
 [A]dvanced IP settings
 [Q]uit


 Step 1 of 3: Select Default Gateway
 Default gateway reported as 192.168.1.1
 Use the above reported default gateway?            [Y/n]? y

 Step 2 of 3: Select Internet Interface
 Internet interface reported as wlan0
 Use the above reported Internet interface?         [Y/n]? y

 Step 3 of 3: Select WiFi Pineapple Interface
 Please connect the WiFi Pineapple to this computer.
 [Checking]
 Detected WiFi Pineapple on interface eth1
 Use the above detected WiFi Pineapple interface?   [Y/n]? y

 Settings saved.

 Saved Settings: Share Internet connection from wlan0
 to WiFi Pineapple at eth1 through default gateway 192.168.1.1
```



```
[C]onnect using saved settings
[G]uided setup (recommended)
[M]anual setup
[A]dvanced IP settings
[Q]uit

|
```

Now you can press **C** to connect.

> ⓘ Note that you may need to toggle the USB-C Ethernet interface in your Network Manager before the script will detect your WiFi Pineapple.

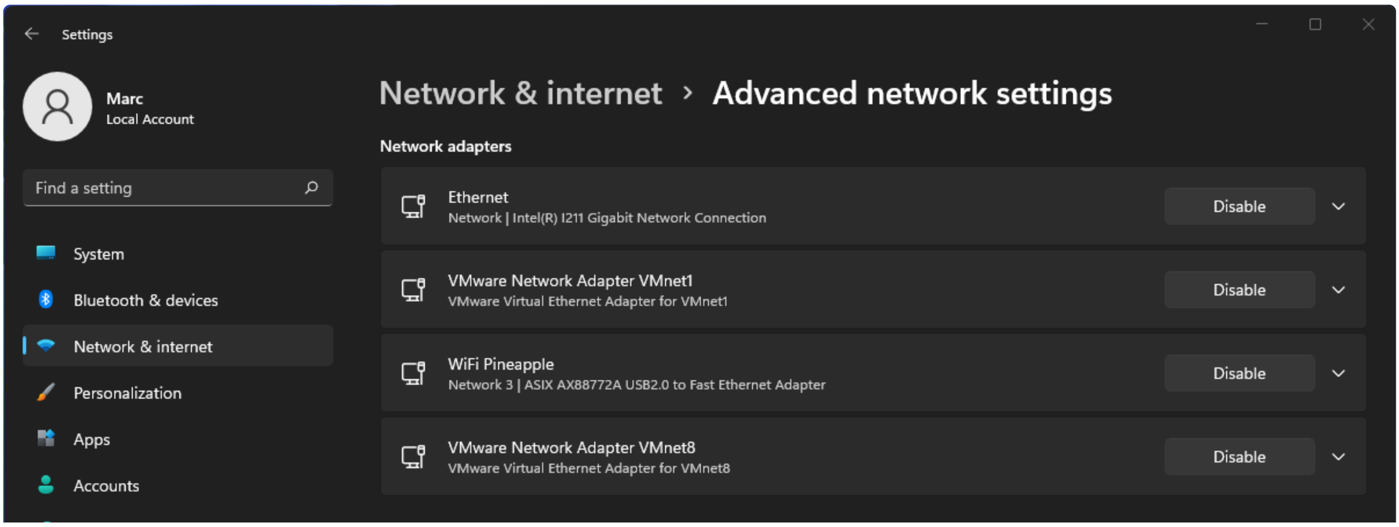
Configuring ICS on Windows

On Windows, Internet Connection Sharing is achieved by using Window's "Network Sharing" feature, by sharing one internet-enabled interface to the WiFi Pineapples.

> ⓘ The following guide is designed to work on Windows 11, although the same or similar steps apply to Windows 10/8.1/8/7 too.

Configuring the Internet facing interface

Start by opening the **Network & Internet** settings in the Windows settings application. Scroll down to **Related settings** and click **More network adapter options**.

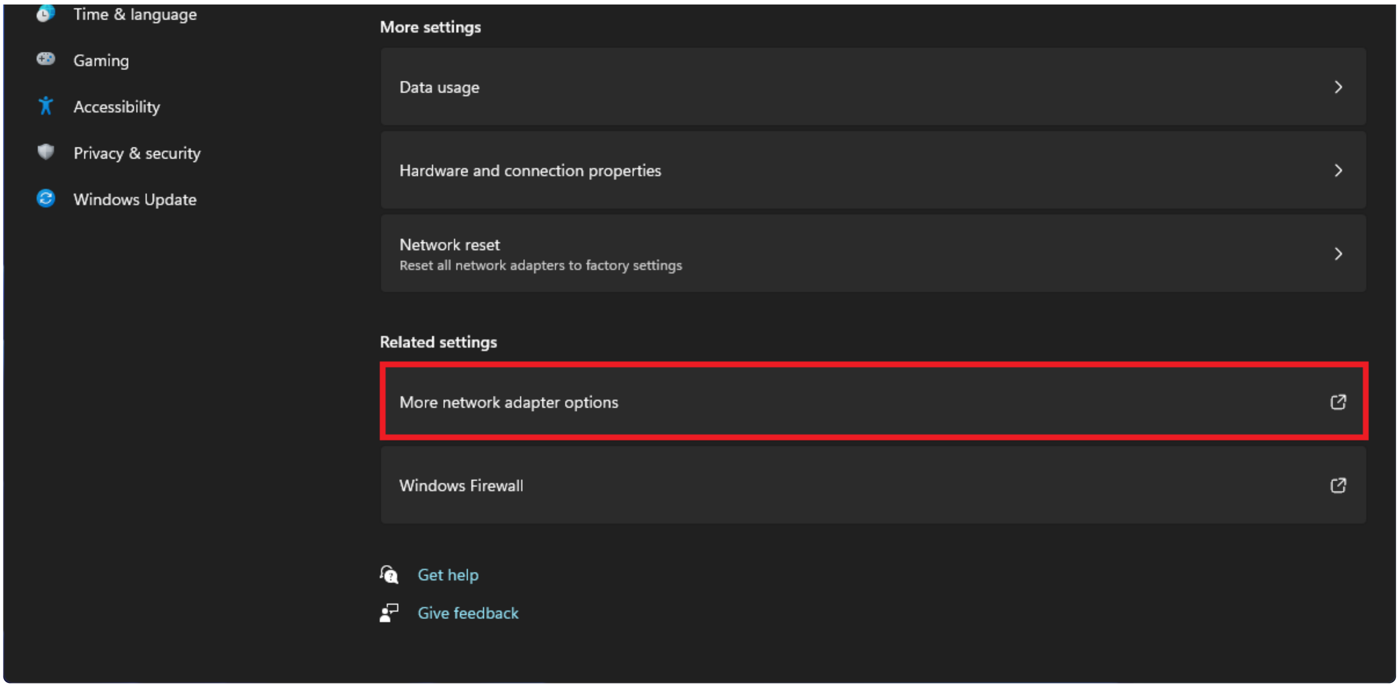


Ethernet
Network | Intel(R) I211 Gigabit Network Connection

VMware Network Adapter VMnet1
VMware Virtual Ethernet Adapter for VMnet1

WiFi Pineapple
Network 3 | ASIX AX88772A USB2.0 to Fast Ethernet Adapter

VMware Network Adapter VMnet8
VMware Virtual Ethernet Adapter for VMnet8



More settings

Data usage

Hardware and connection properties

Network reset
Reset all network adapters to factory settings

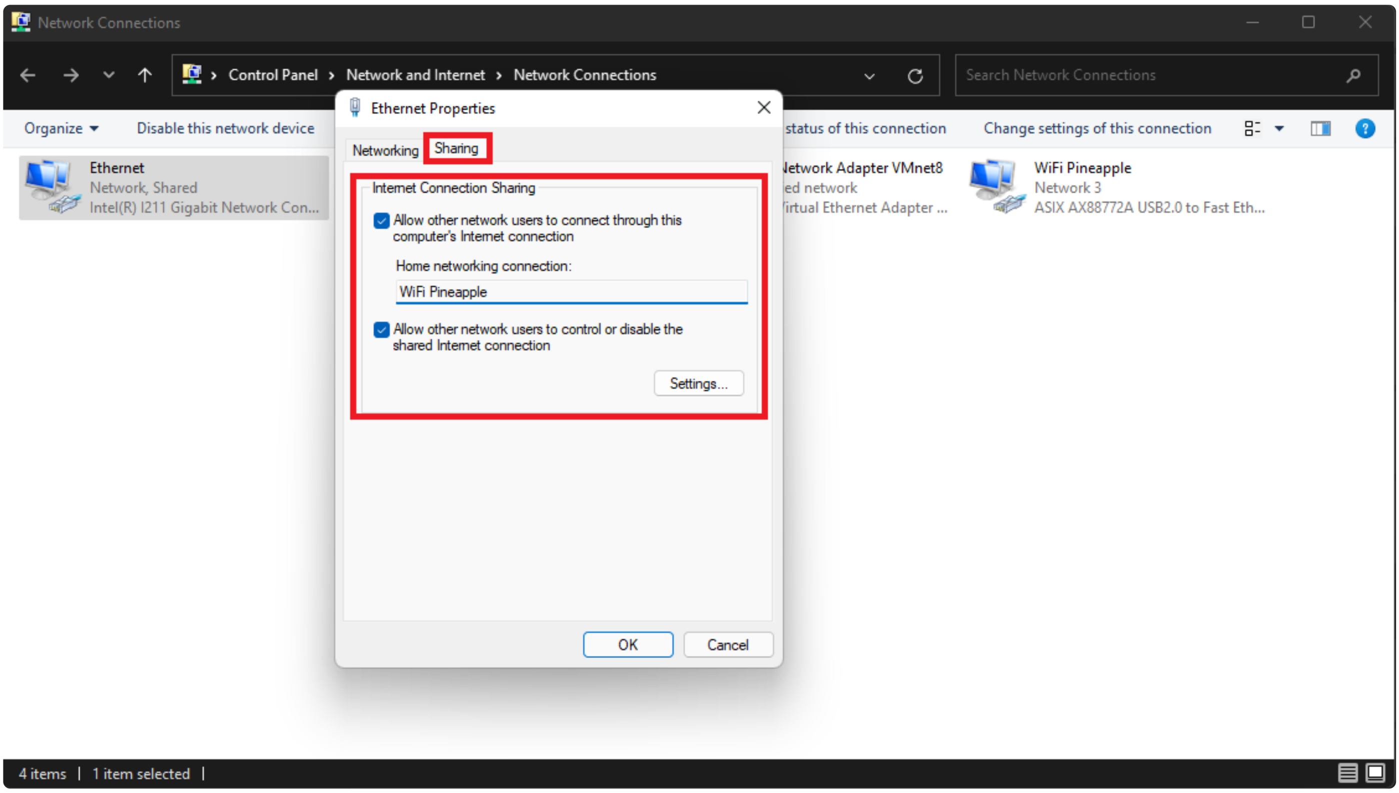
Related settings

More network adapter options

Windows Firewall

In the new window, **right-click the Internet facing adapter, and select "Properties".** In this guide, the Internet facing adapter is the interface named **Ethernet**.

Once you're in the properties window, select the **Sharing** tab, and then check the box to allow other users to connect. Then, **select the WiFi Pineapple adapter** and click **OK**.


Network Connections
Control Panel › Network and Internet › Network Connections
Search Network Connections
Organize
Disable this network device
status of this connection
Change settings of this connection

Ethernet
Network, Shared
Intel(R) I211 Gigabit Network Con...

letwork Adapter VMnet8
ed network
irtual Ethernet Adapter ...

WiFi Pineapple
Network 3
ASIX AX88772A USB2.0 to Fast Eth...

Ethernet Properties

Networking | Sharing

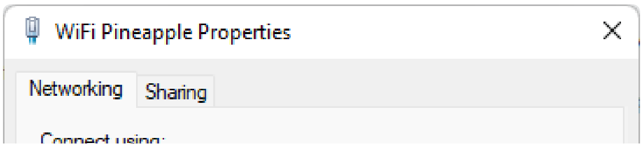
Internet Connection Sharing

☑ Allow other network users to connect through this computer's Internet connection

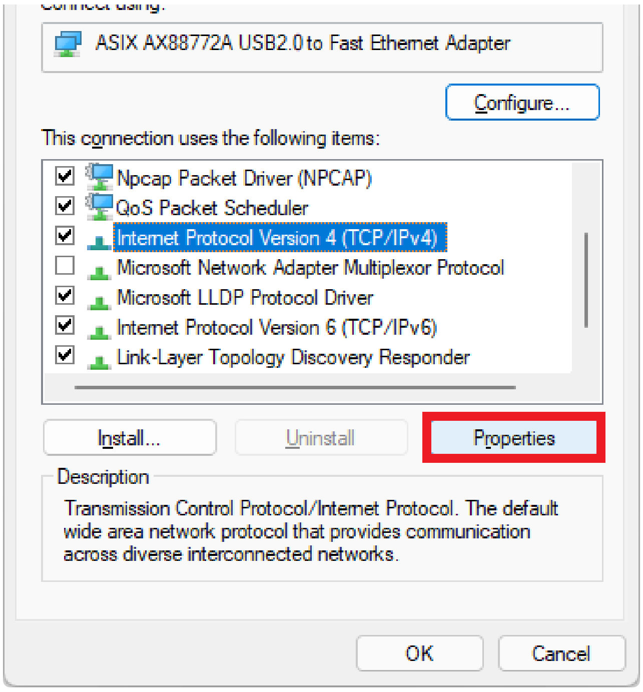
Home networking connection:
WiFi Pineapple

☑ Allow other network users to control or disable the shared Internet connection

Next, configure the WiFi Pineapple adapter by **right clicking and selecting "Properties".** In the new window, select the text that says **Internet Protocol Version 4 (TCP/IPv4)** and select **Properties**.


WiFi Pineapple Properties

Connect using:


Connect using:

ASIX AX88772A USB2.0 to Fast Ethernet Adapter

This connection uses the following items:

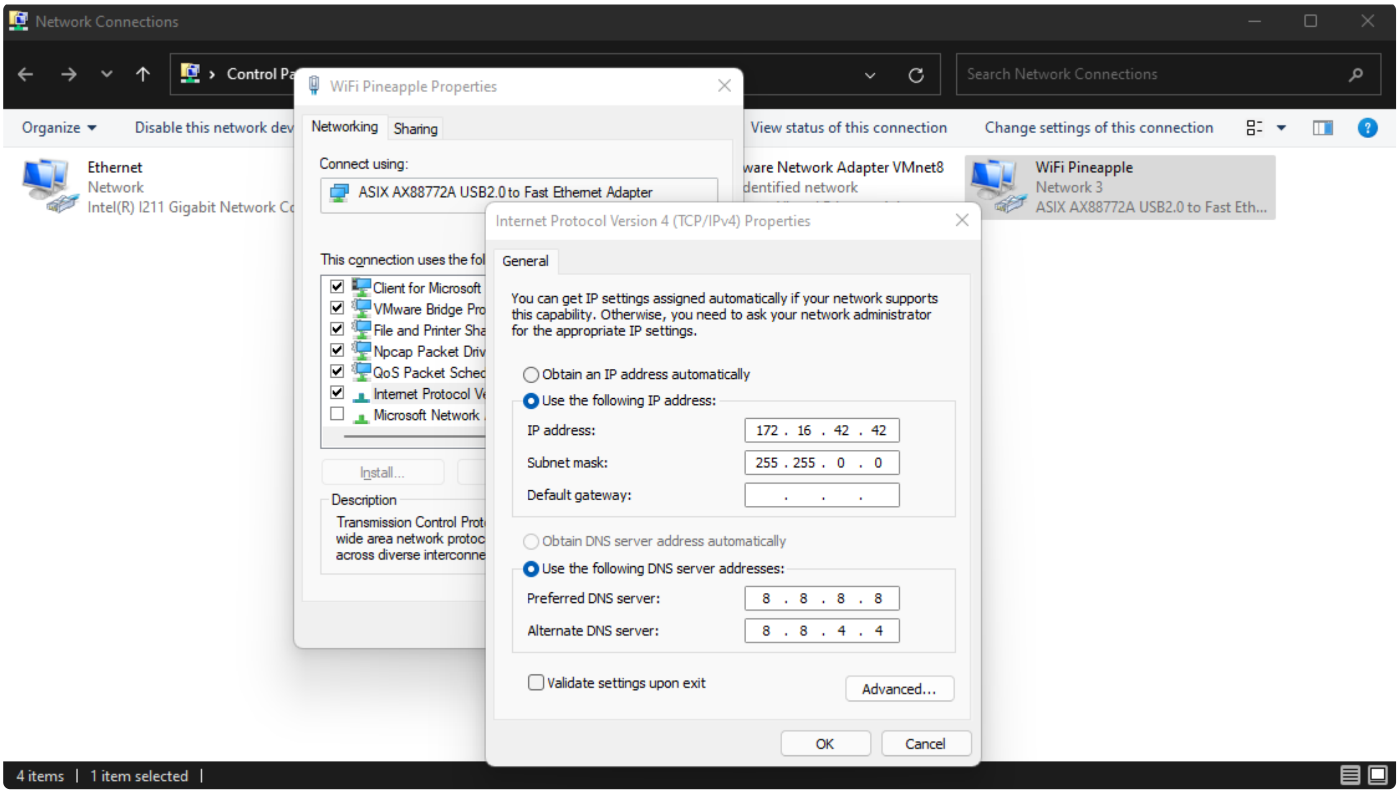
- ☑ Npcap Packet Driver (NPCAP)
- ☑ QoS Packet Scheduler
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☐ Microsoft Network Adapter Multiplexor Protocol
- ☑ Microsoft LLDP Protocol Driver
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Finally, set the adapters IP settings as follows:

- IP Address: **172.16.42.42**
- Subnet Mask: **255.255.0.0**
- Default Gateway: **Blank**
- Preferred DNS: **8.8.8.8**
- Alternate DNS: **8.8.4.4**


Network Connections
Control Pa
Search Network Connections
Organize
Disable this network dev
View status of this connection
Change settings of this connection
Ethernet
Network
Intel(R) I211 Gigabit Network Co
ware Network Adapter VMnet8
dentified network
WiFi Pineapple
Network 3
ASIX AX88772A USB2.0 to Fast Eth...
WiFi Pineapple Properties
Networking
Sharing

Connect using:

ASIX AX88772A USB2.0 to Fast Ethernet Adapter

This connection uses the fol

- ☑ Client for Microsoft
- ☑ VMware Bridge Pro
- ☑ File and Printer Sha
- ☑ Npcap Packet Driv
- ☑ QoS Packet Sched
- ☑ Internet Protocol Ve
- ☐ Microsoft Network

Transmission Control Prot wide area network protoc across diverse interconne

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically
● Use the following IP address:

IP address: 172 . 16 . 42 . 42
Subnet mask: 255 . 255 . 0 . 0
Default gateway: . . .

○ Obtain DNS server address automatically
● Use the following DNS server addresses:

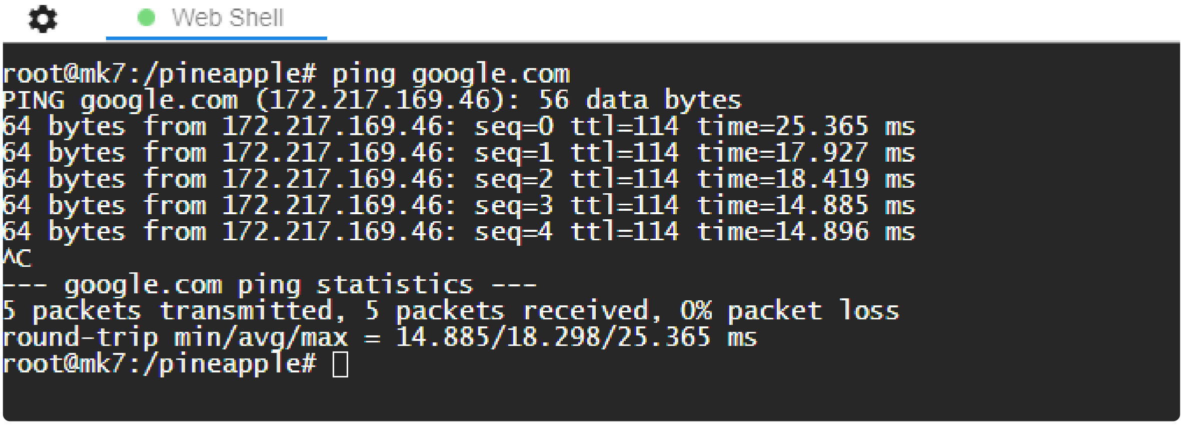
Preferred DNS server: 8 . 8 . 8 . 8
Alternate DNS server: 8 . 8 . 4 . 4

☐ Validate settings upon exit

ⓘ You may set your own preferred and alternate DNS servers if desired, but Google's DNS is

> recommended.

After clicking **OK** to save the settings, your WiFi Pineapple will now be able to access the internet through the USB-C interface connected to your computer.



```
root@mk7:/pineapple# ping google.com
PING google.com (172.217.169.46): 56 data bytes
64 bytes from 172.217.169.46: seq=0 ttl=114 time=25.365 ms
64 bytes from 172.217.169.46: seq=1 ttl=114 time=17.927 ms
64 bytes from 172.217.169.46: seq=2 ttl=114 time=18.419 ms
64 bytes from 172.217.169.46: seq=3 ttl=114 time=14.885 ms
64 bytes from 172.217.169.46: seq=4 ttl=114 time=14.896 ms
^C
--- google.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 14.885/18.298/25.365 ms
root@mk7:/pineapple# 
```

Configuring a USB Ethernet Adapter

Some USB Ethernet Adaptors are supported out-of-the-box. For a reference of supported adapter chipsets, look at the table below.

Manufacturer	Chipset	Description
ASIX	AX88179	ASIX USB2.0 Ethernet 10/100
Realtek	RTL8152	Realtek USB2.0 Ethernet 10/100
Realtek	RTL8153	Realtek USB3.0 Ethernet 10/100/1000

Installing kernel modules for other chipsets

If your USB Ethernet adaptor has a chipset that isn't listed above, it is possible that an available driver/kernel module is available for the WiFi Pineapple MK7.

You can check this by going to the WiFi Pineapple's Web Interface, and going to **Modules > Packages**, and searching for the name of your chipset.

Password Reset

On firmware versions 1.1.0 and later, you may reset a lost password by holding the Reset button for 10 seconds or longer. Upon success, the LED will flash a rainbow colour sequence and reboot.

After the device reboots, you will be able to login with the password `hak5pineapple`. You are strongly advised to change this after logging in.

> If the LED does not flash rainbow colours, the button was not pressed down long enough, or was not pressed firmly enough to fully engage the button. Try using a pen cap or similar blunt solid object to make sure the button is fully pressed!

Factory Reset and Recovery

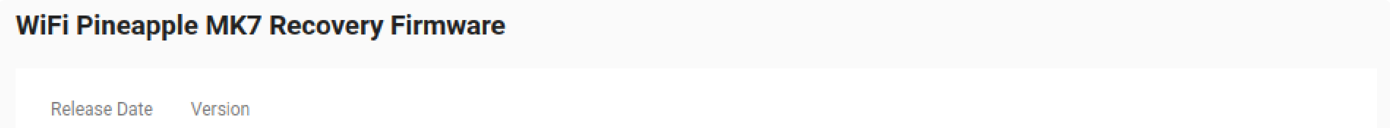
To restore your WiFi Pineapple back to a factory state, or to recover from a bad configuration, you can perform a **Firmware Recovery**.

The factory recovery method consists of using the device bootloader to flash the recovery firmware, and in turn, the final firmware.

Video Tutorial

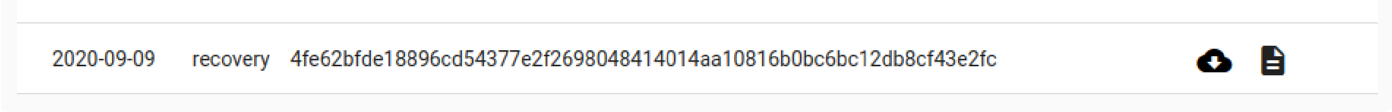
Preparation

To begin, download the latest recovery file from the Hak5 Download Portal.



WiFi Pineapple MK7 Recovery Firmware

Release Date Version



2020-09-09	recovery	4fe62bfde18896cd54377e2f2698048414014aa10816b0bc6bc12db8cf43e2fc

Once downloaded, verify the SHA256 sum of the downloaded file, and make sure your WiFi Pineapple is unplugged.

To start the process, **hold down the reset button while applying power** to the WiFi Pineapple.

The WiFi Pineapple status LED will flash **RED**.

After approximately three flashes of the LED, **let go of the reset button** and continue to the next step.

The LED should blink **RED** rapidly, and then remain **SOLID RED**. If the status LED changes to **BLUE**, disconnect the power and repeat the process. Make sure the button is held in firmly, and release the button after approximately three flashes of the **RED** LED.

Assigning a Static IP Address

Linux

Assign the WiFi Pineapple's interface a static IP address of **172.16.42.42**. More in-depth instructions can be found in the Linux Setup page.

Windows

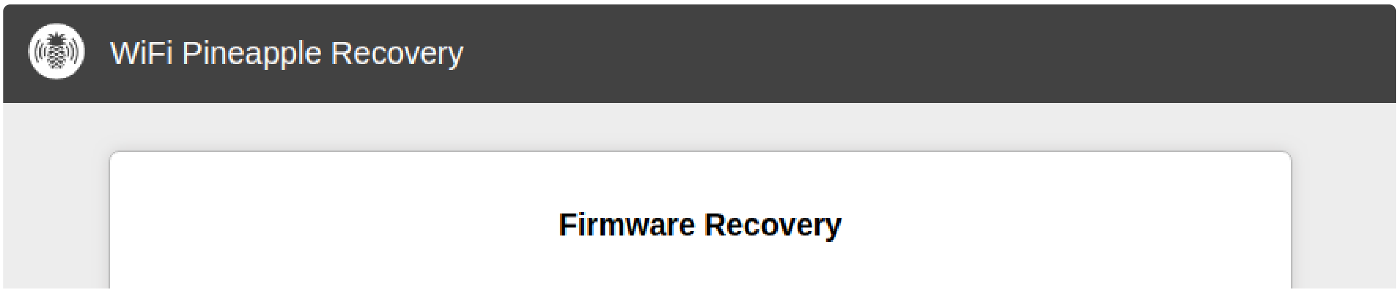
Assign the WiFi Pineapple's interface a static IP address of **172.16.42.42**. More in-depth instructions can be found in the Windows Setup page.

> ⓘ New to static IP address assignments in Windows? Check this tutorial.

Uploading the Recovery to the WiFi Pineapple

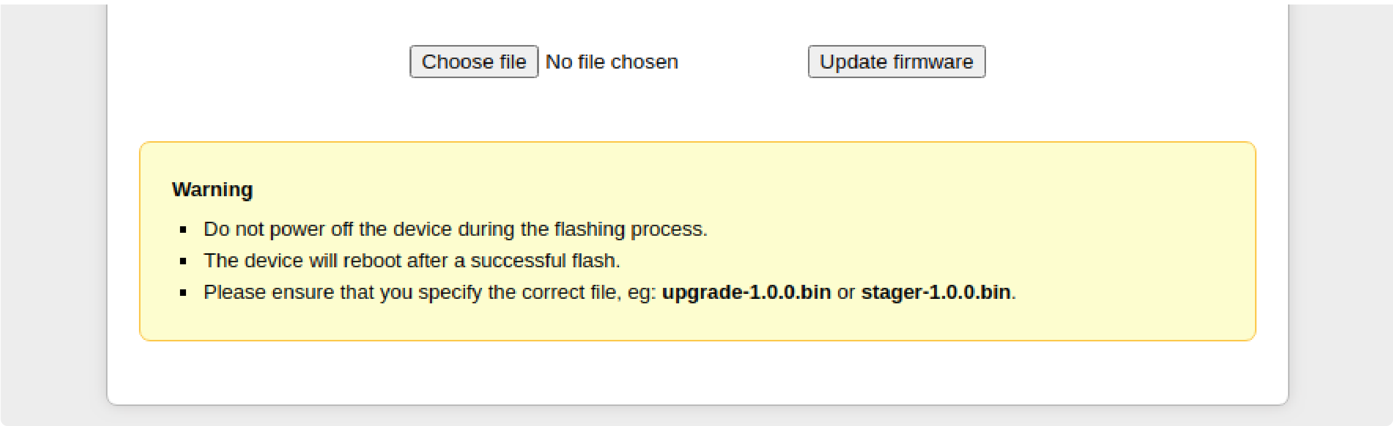
Once a static IP address has been assigned, open your browser and navigate to http://172.16.42.1. You'll then be greeted by a screen prompting you to upload a **.bin image**.

> ⓘ Be sure to navigate to http://172.16.42.1 *with no port*. To flash the recovery image you need to access the webserver on the default port - trying to connect to the WiFi Pineapple UI on port 1471 *will not work*!



WiFi Pineapple Recovery

Firmware Recovery



Warning

- Do not power off the device during the flashing process.
- The device will reboot after a successful flash.
- Please ensure that you specify the correct file, eg: **upgrade-1.0.0.bin** or **stager-1.0.0.bin**.

Select **Choose file** and then select the downloaded **recovery file** from earlier. After clicking **Update firmware**, the device will begin flashing. **Do not** attempt to flash a normal WiFi Pineapple firmware now - it won't work! You'll be able to flash the full firmware during the setup process once recovery is complete!

> ⚠ **Do not unplug the device.** Doing so will potentially damage your device. It will automatically reboot once complete.

Once the process is complete, you will be able to set the device up again. See the Setup section for more details.

> ⓘ Once the device has finished flashing, you will need to navigate to http://172.16.42.1:1470 to complete the setup process, same as the first time you configured it!

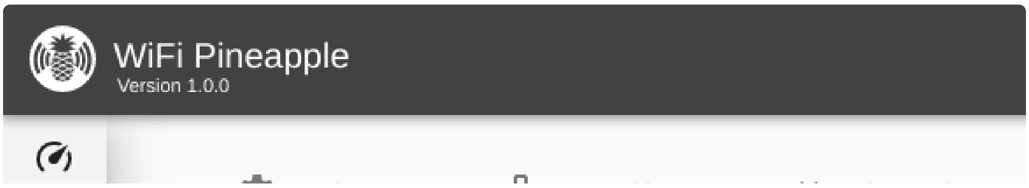
WiFi Pineapple Beta Updates

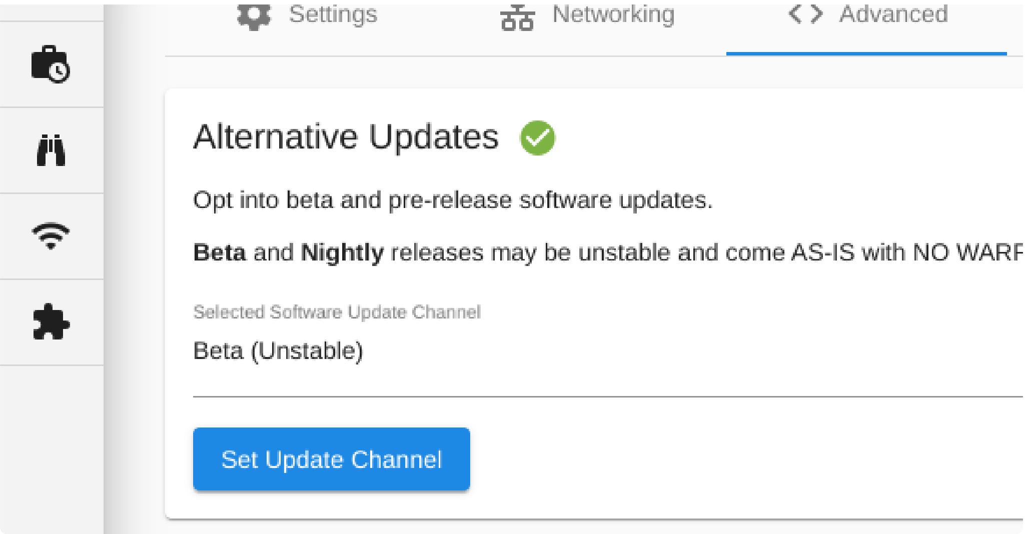
The WiFi Pineapple has multiple **update channels** for its update mechanism. These channels allow you to specify what type of firmware release you want to use on your WiFi Pineapple.

Currently, there are two update channels:

- **Stable**
- **Beta** - Pre-release updates that may be unstable, but may also contain new bug fixes, features and more.

To manage your selected update channel, go to **Settings > Advanced** in the Web Interface.





Alternative Updates ✓

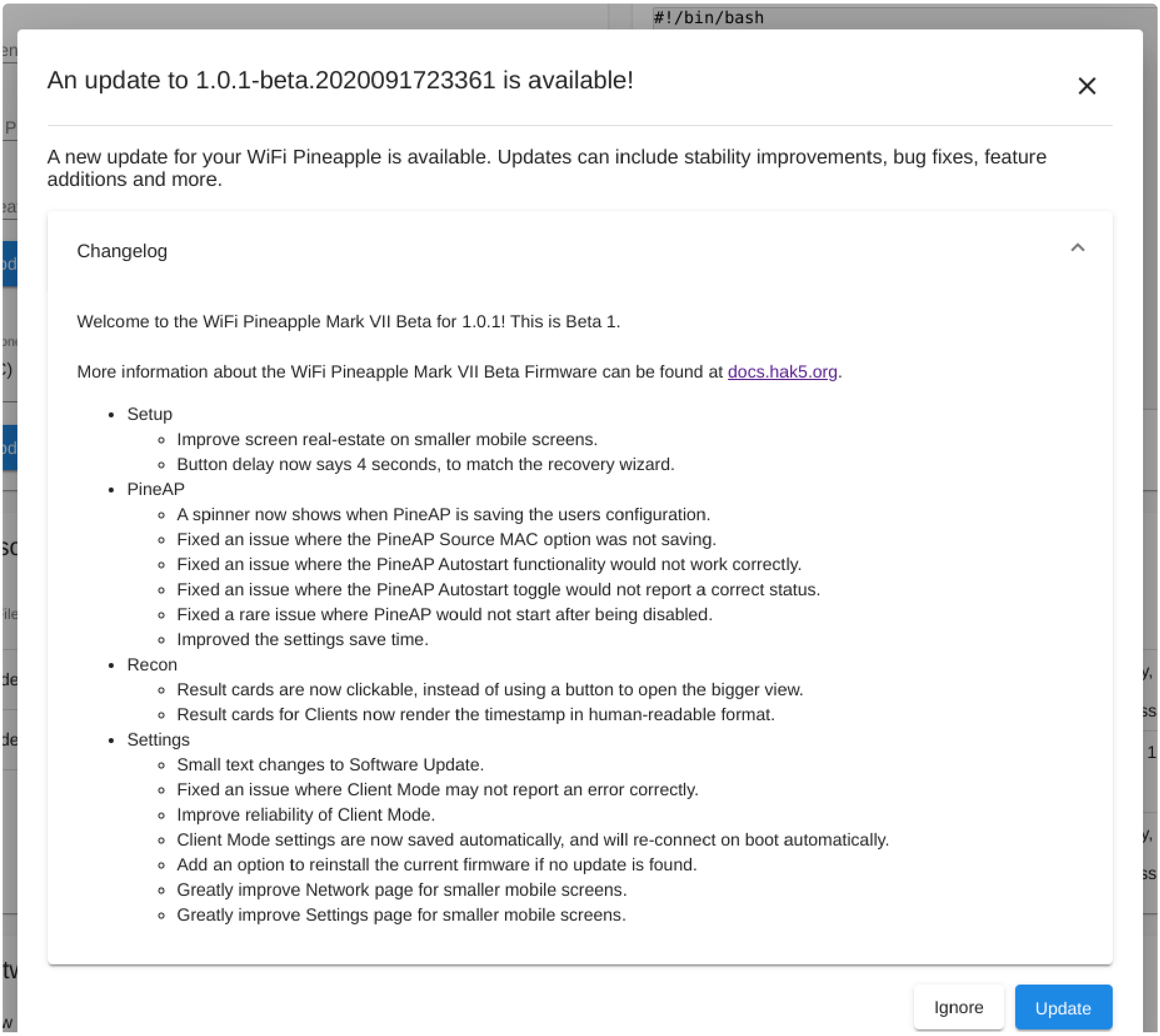
Opt into beta and pre-release software updates.

Beta and **Nightly** releases may be unstable and come AS-IS with NO WARF

Selected Software Update Channel
Beta (Unstable)

Using the drop-down list and the **Set Update Channel** button, you'll be able to change the update channel. You may set the channel back to Stable at any time.

Once you've picked an alternative channel, go back to the **Settings** tab and **Check for new updates.** If an update is available, you will be presented with the option to update.



An update to 1.0.1-beta.2020091723361 is available!

A new update for your WiFi Pineapple is available. Updates can include stability improvements, bug fixes, feature additions and more.

Changelog

Welcome to the WiFi Pineapple Mark VII Beta for 1.0.1! This is Beta 1.

More information about the WiFi Pineapple Mark VII Beta Firmware can be found at docs.hak5.org.

- Setup
  - Improve screen real-estate on smaller mobile screens.
  - Button delay now says 4 seconds, to match the recovery wizard.
- PineAP
  - A spinner now shows when PineAP is saving the users configuration.
  - Fixed an issue where the PineAP Source MAC option was not saving.
  - Fixed an issue where the PineAP Autostart functionality would not work correctly.
  - Fixed an issue where the PineAP Autostart toggle would not report a correct status.
  - Fixed a rare issue where PineAP would not start after being disabled.
  - Improved the settings save time.
- Recon
  - Result cards are now clickable, instead of using a button to open the bigger view.
  - Result cards for Clients now render the timestamp in human-readable format.
- Settings
  - Small text changes to Software Update.
  - Fixed an issue where Client Mode may not report an error correctly.
  - Improve reliability of Client Mode.
  - Client Mode settings are now saved automatically, and will re-connect on boot automatically.
  - Add an option to reinstall the current firmware if no update is found.
  - Greatly improve Network page for smaller mobile screens.
  - Greatly improve Settings page for smaller mobile screens.

Compatible 802.11ac Adapters

The WiFi Pineapple Mark VII supports 802.11ac monitor and frame injection with a supported adaptor.

The WiFi Pineapple Enterprise comes equipped with 3 MT7612U 802.11ac capable radios, but you may add more via USB if desired.

Adaptor	Chipset
Hak5 MK7AC Adapter	MT7612U
AWUS036ACM	MT7612U
EP-AC1605 **V1** (**V2 is incompatible)**	MT7612U

Installing drivers for other WiFi Adapters

While the WiFi Pineapple has support for MT7612U and MT7601U devices out of the box, you can also install drivers for a wide range of other chipsets, such as other **MT76-based** devices, **ath9k** and **ath10k** devices, and some **Realtek** dongles.

To find drivers, you can use the **Package Manager** found in the Web Interface under **Modules > Packages**. Search for keywords related to the chipset in your adapter.

Please be advised that only adapters based on MT7612U are **confirmed to work correctly** in all circumstances, and other WiFi adapters may not work or have available drivers at all, or may only work partially or cause unexpected behavior like crashes, reboots, etc. Not all WiFi cards or drivers are equal in capability or performance!

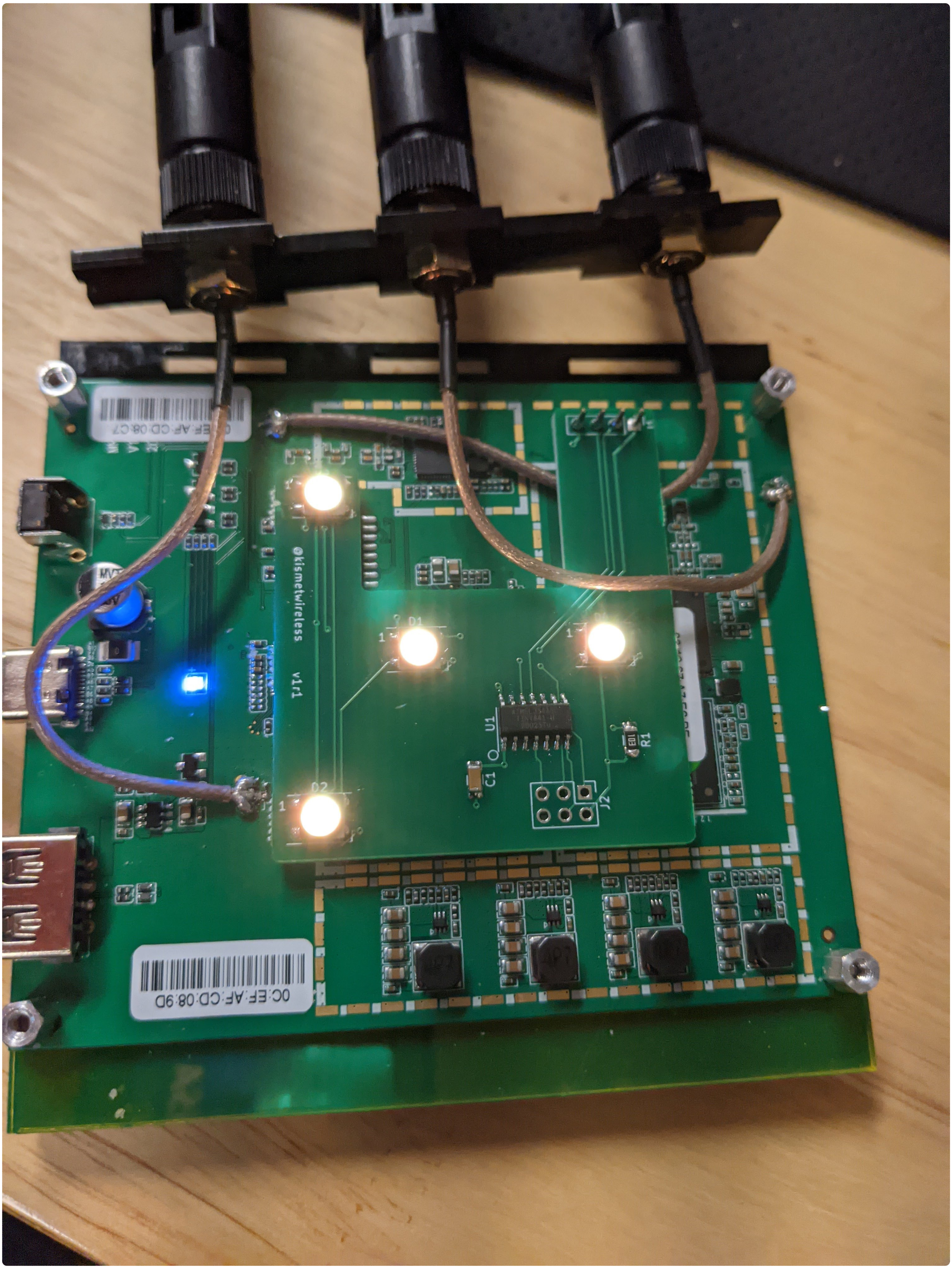
More information about a specific adapter can usually found with resources such as DeviWiki.

Extras

MK7 LED Mod Installation

The MK7 LED mod is an add-on board for the Hak5 WiFi Pineapple Mark VII which adds some bling and fun LEDs. Proceeds from the case help support Kismet development, too!

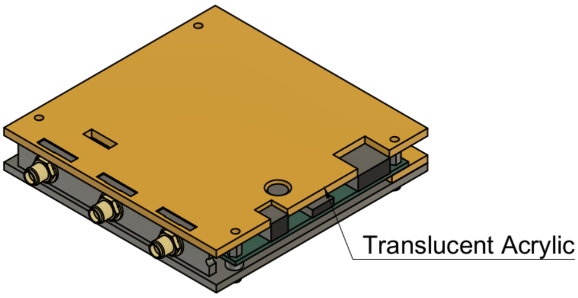
See the install instructions from https://www.kismetwireless.net/mk7-led-mod/.

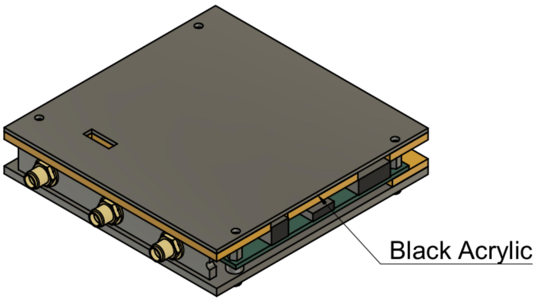

0C:EF:AF:CD:08:C7
©kismetwireless
v1r1
D1
D2
U1
C1
R1
J2
0C:EF:AF:CD:08:9D

MK7 Kismet Case Installation

The Kismet Special Edition case for the WiFi Pineapple Mark VII helps support Kismet development and gives your WiFi Pineapple an extra flair.

See the assembly instructions from https://www.kismetwireless.net/mk7-kismet-case/.


Translucent Acrylic


Black Acrylic