WiFi Pineapple- 7th Gen: Mark VII / Enterprise

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.

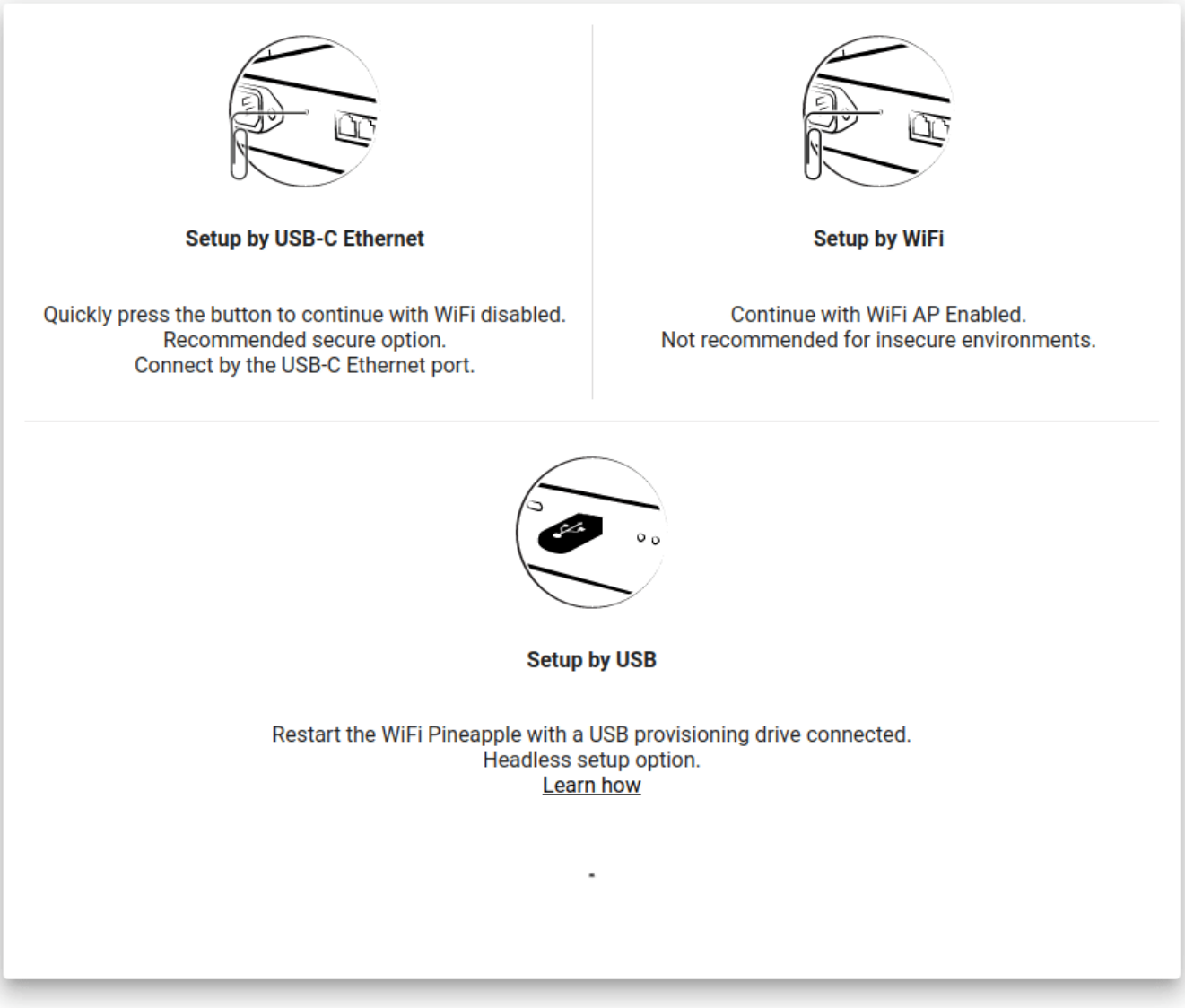
Once you've connected to the WiFi Pineapple and it has fully booted, you will be able to access the WiFi Pineapple Stager at http://172.16.42.1.

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

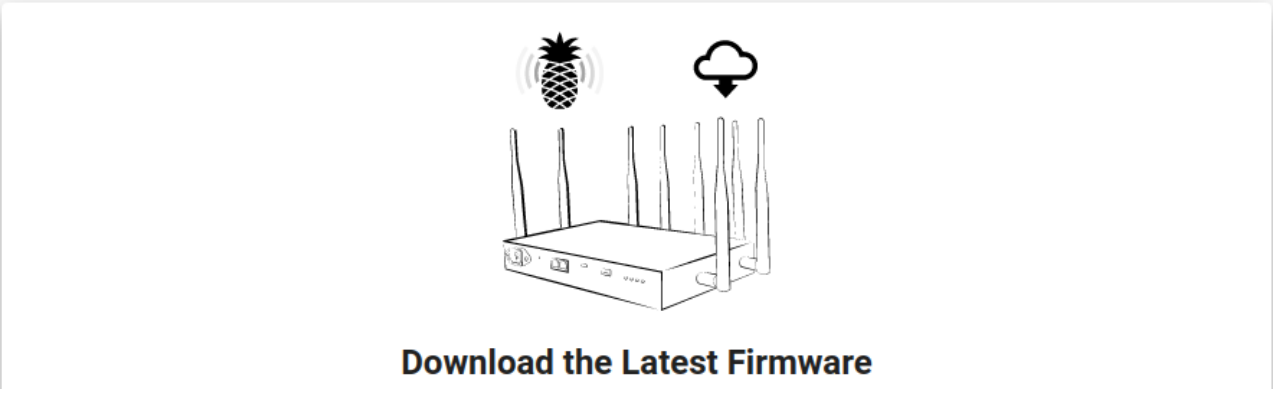
To start, begin by verifying that you are in the presence of the WiFi Pineapple. You can do this by pressing

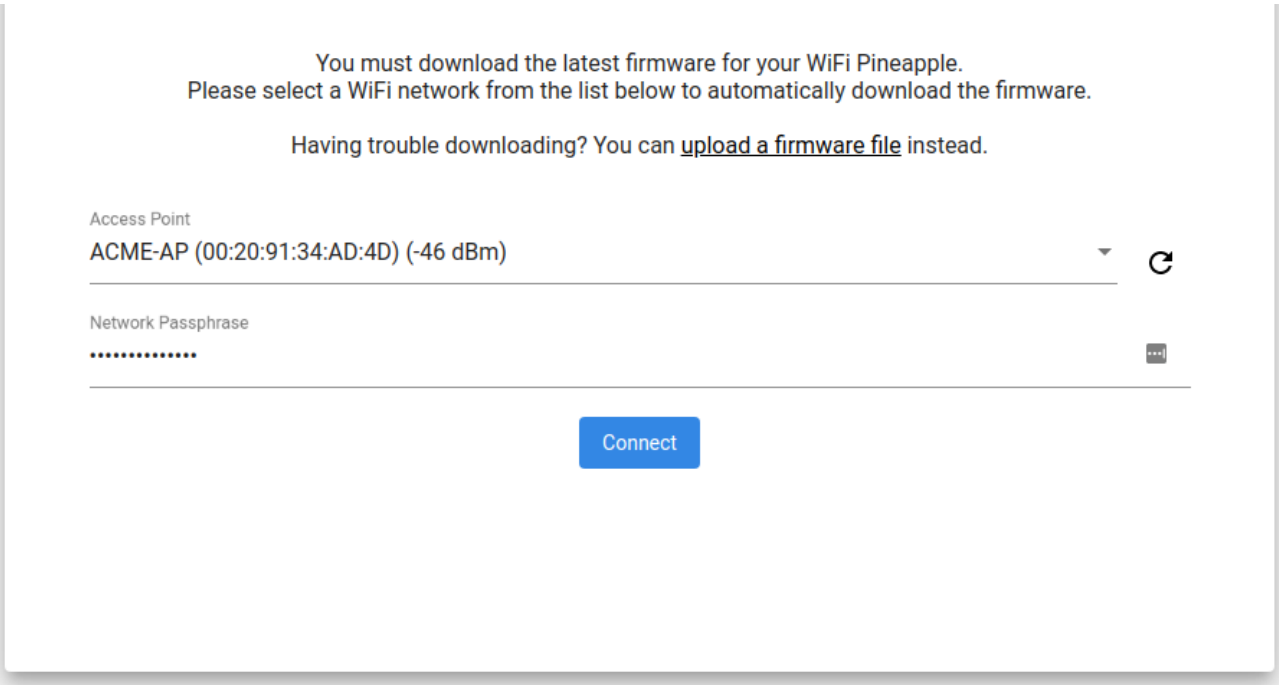
the reset button in one of the ways described on-screen.



> 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.

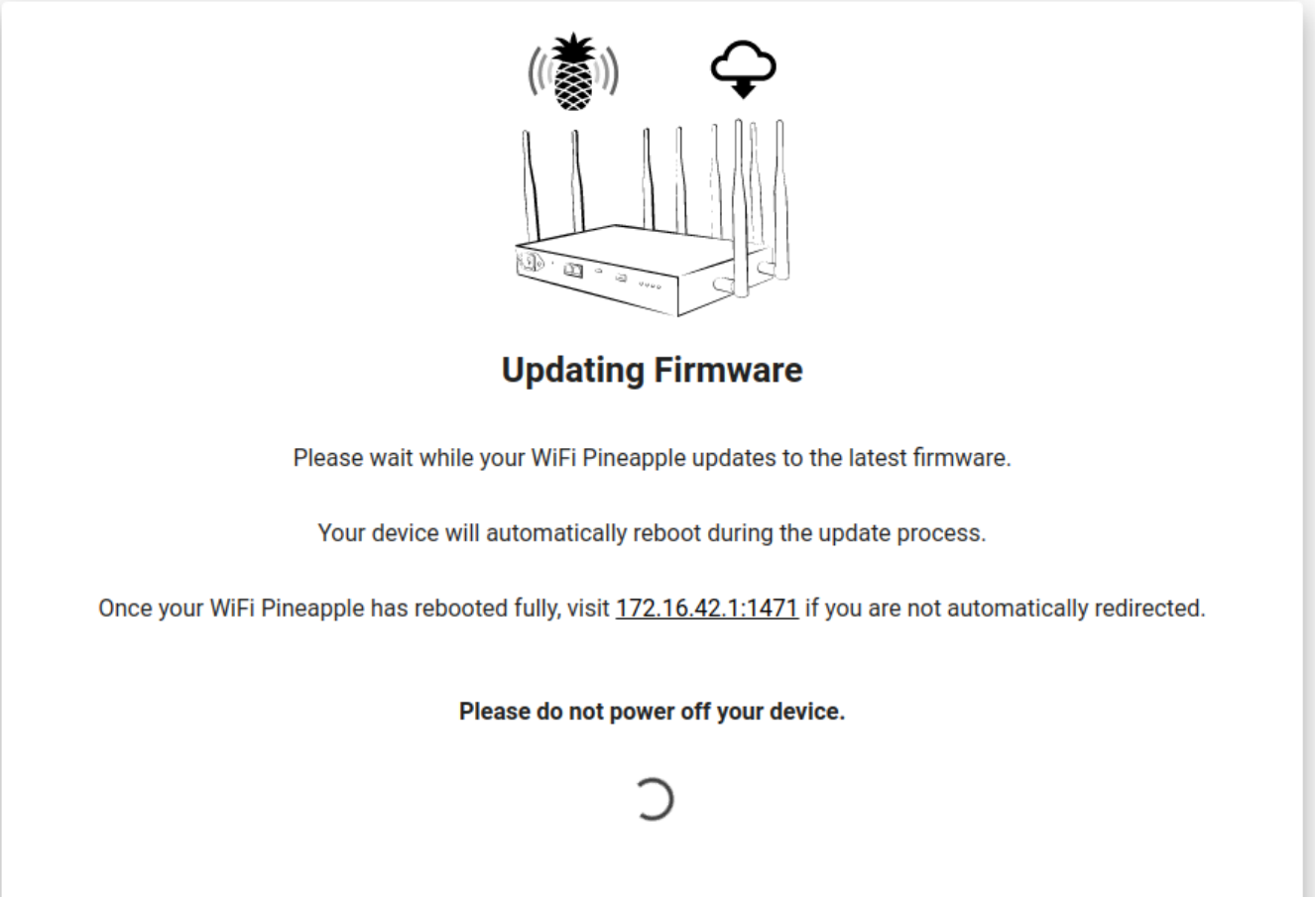
Next, connect to an Access Point you know the credentials to. Doing this will establish an internet connection for the WiFi Pineapple, and the latest firmware will be automatically downloaded.





> ⓘ Only WPA2, WPA and Open networks are currently supported in the stager.

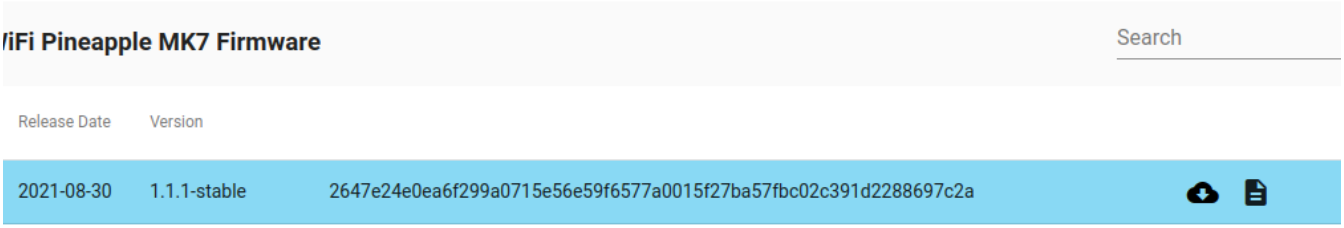
After the connection is successfully established, the firmware will be automatically downloaded and flashed to your WiFi Pineapple. Once the upgrade is complete, you will be able to access the WiFi Pineapple at https://172.16.42.1:1471 again.



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.

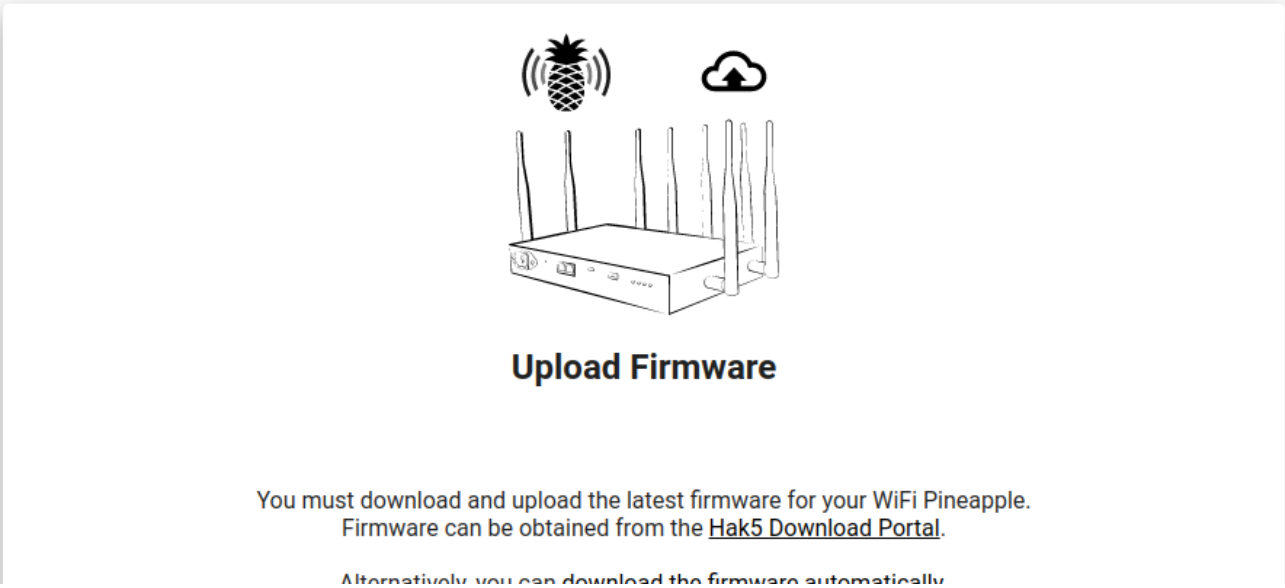
To start, begin by downloading the latest firmware from the Hak5 Download Portal. The latest releases are always at the top of the table, and highlighted blue.

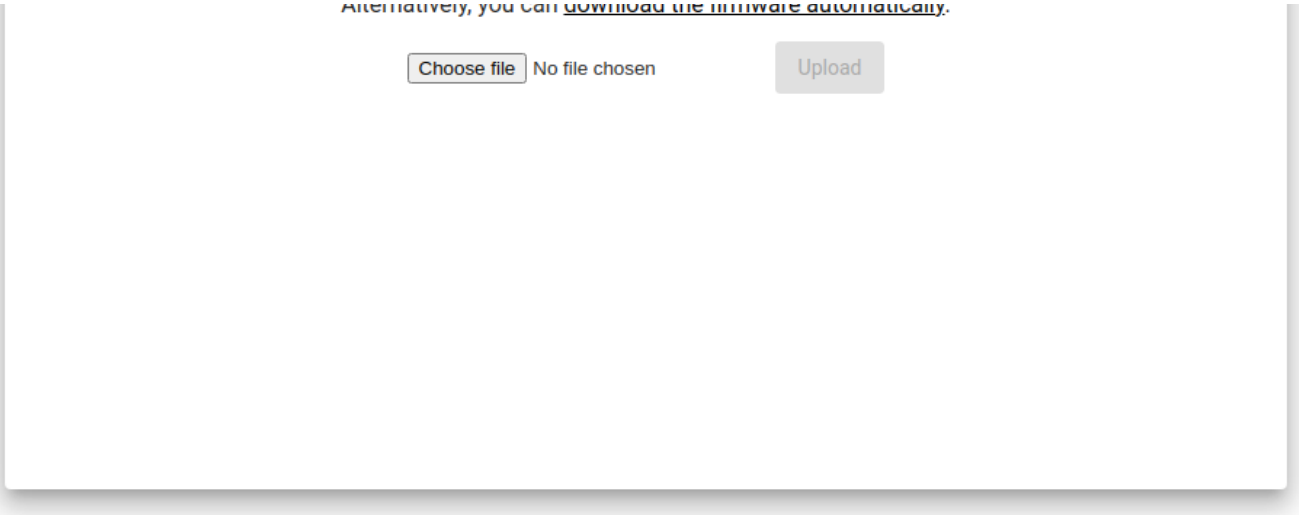


Once the file is downloaded, verify the SHA256 sum with the one listed on the download portal.

> 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.





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

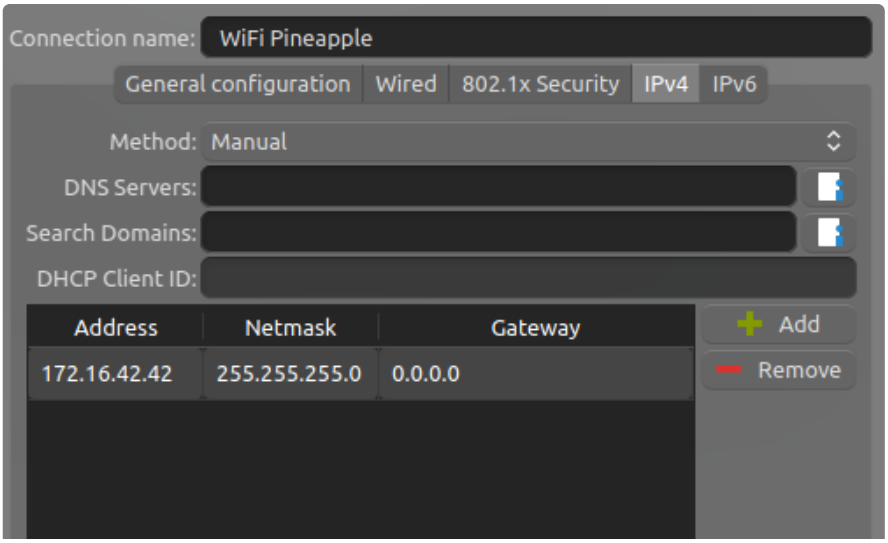
Connecting to the WiFi Pineapple on Linux

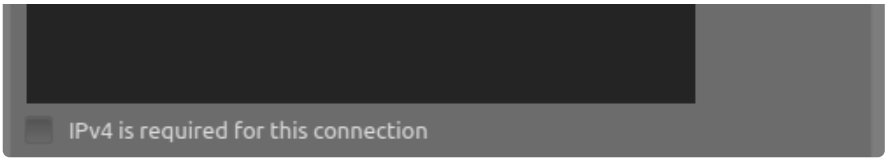
This guide teaches the basics of connecting to the WiFi Pineapple on Linux-based operating systems.

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





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
```

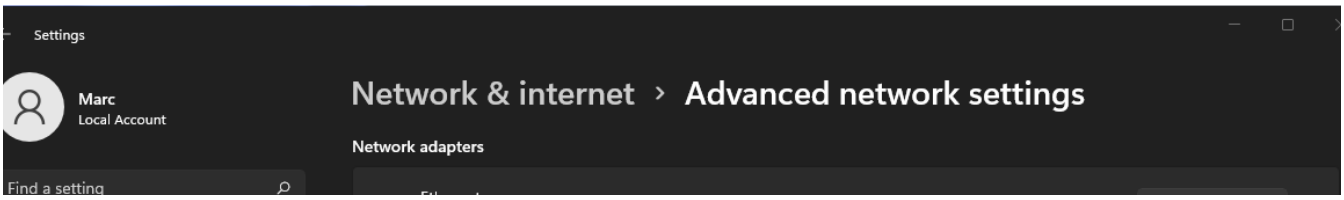
Connecting to the WiFi Pineapple on Windows

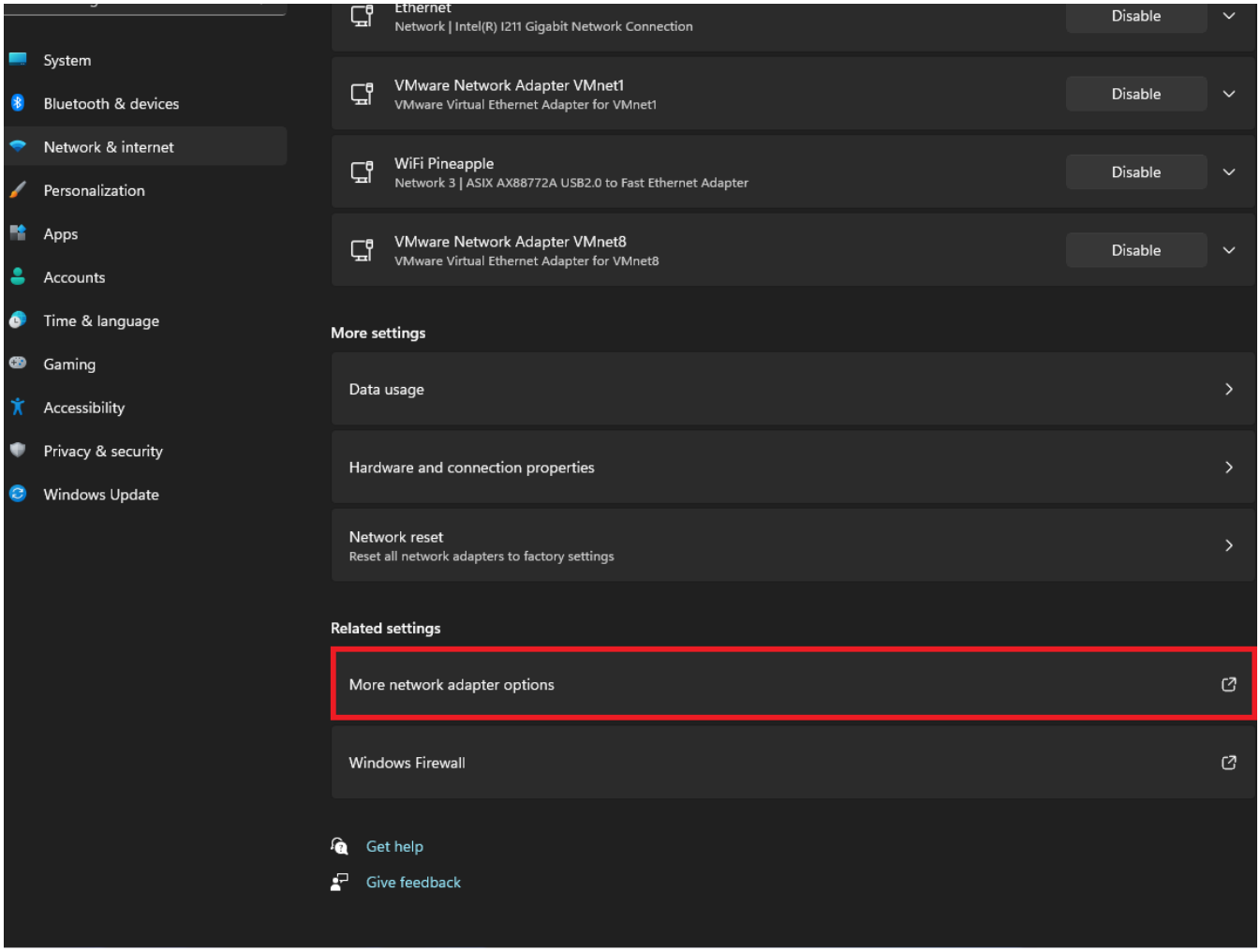
This guide teaches the basics of connecting to the WiFi Pineapple on Windows.

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**.

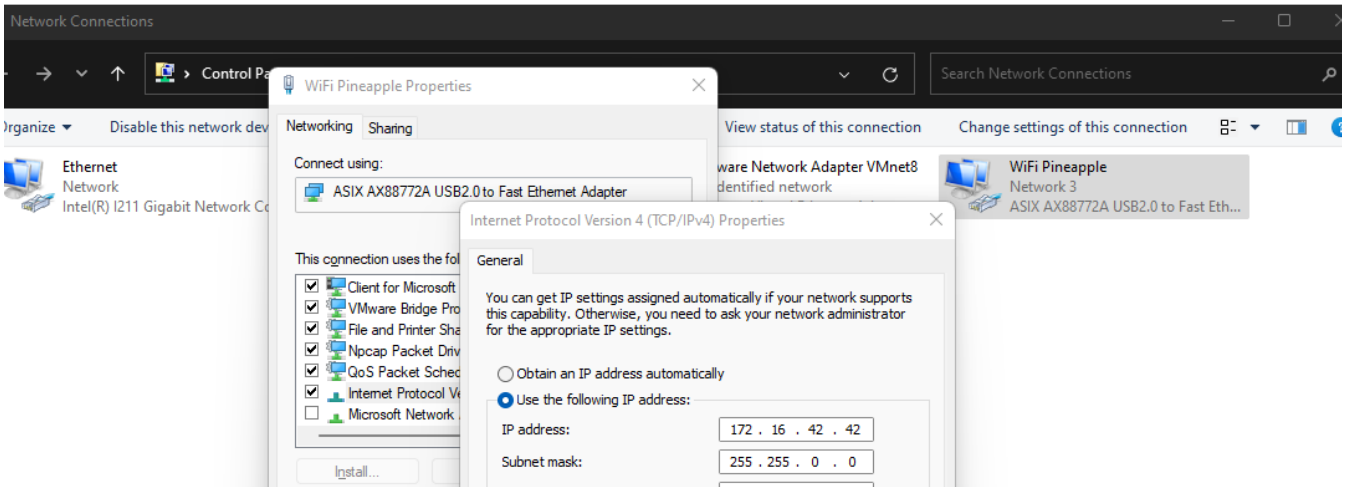


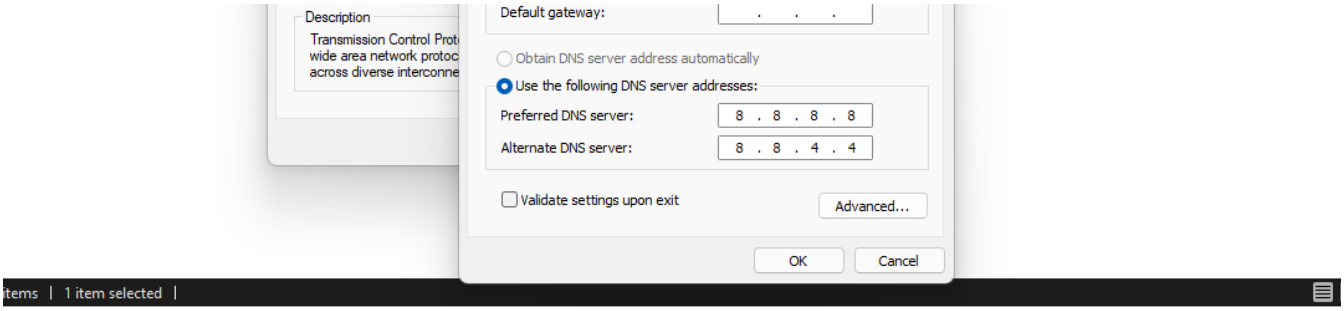


In the new window, **right click** the adapter that represent your WiFi Pineapple and select **Properties**. Then, select the text **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties** again.

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**





> 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. This is useful for mass-deployments.

The USB flash disk used to provision the WiFi Pineapple must contain only a single partition formatted with either the FAT32 or EXT4 file system.

On the root of the USB flash disk, include the latest upgrade-x.x.x.bin from downloads.hak5.org as well as a config.txt file containing the below information. Make sure the txt file is saved in ASCII format. Modify the settings as per your desired configuration.

```
1 ##########################################################################################
2 # This file is used to configure automatic enrollment of your WiFi Pineapple Mark VII
3 # To enroll your WiFi Pineapple automatically, edit this file and place it on the
4 # root of a USB flash disk when performing the first boot.
5 # For more information, visit https://docs.hak5.org
```

```
##############################################################################################
# Generic 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
```

USB Firmware Installation

From the WiFi Pineapple Recovery, it is possible to provide an update to the WiFi Pineapple via a USB flash drive. This can be used to setup your WiFi Pineapple if it doesn't have access to the internet.

Preparing the USB drive

The USB drive must be formatted as one of the following:

- ext4
- exFAT / FAT
- NTFS

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). After verifying the SHA256 sum of the download with the one listed on the Download Portal, safely eject the USB drive.

Performing the firmware update

From a powered off state, place your USB drive into the USB Type-A port on the WiFi Pineapple, and

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 to the new version afterwards.

To confirm if the device has found and accepted the firmware file, you may visit the UI at http://172.16.42.1:1471 (if connected to a computer) or observe a flashing red and blue pattern from the LED indicator.

UI Overview

Introduction to the UI

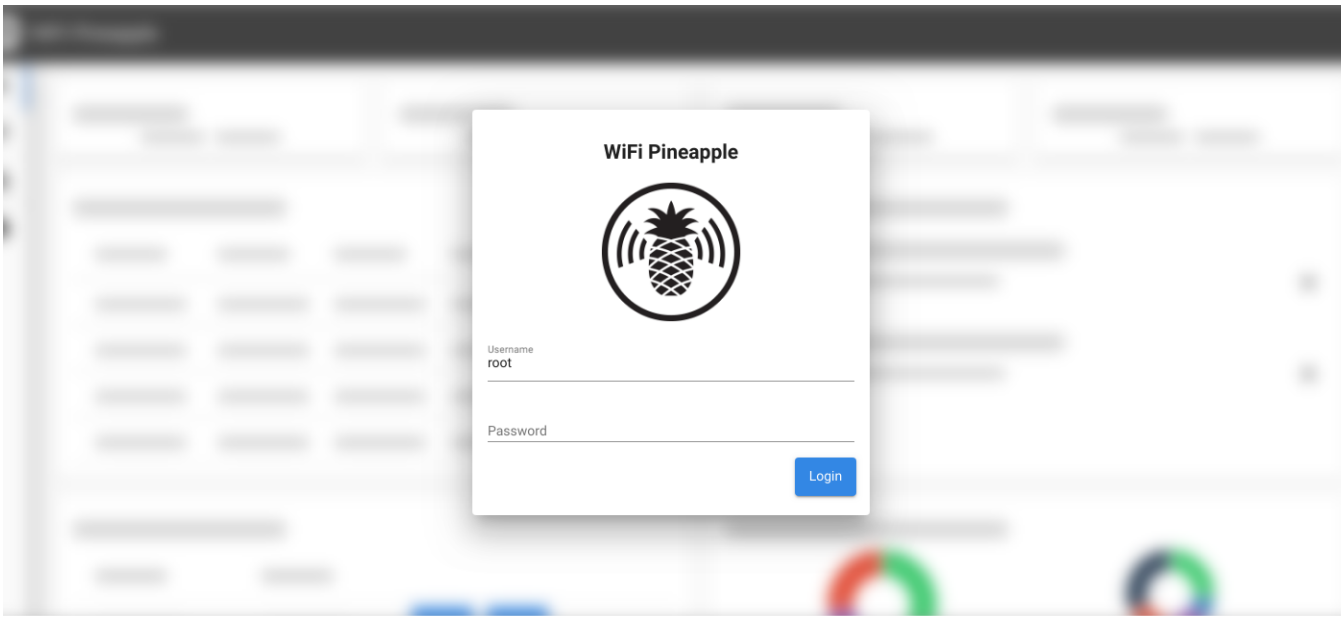
An introduction to the WiFi Pineapple Web UI

Opening the User Interface

Once you're connected to the WiFi Pineapple, you can always use the Management UI by navigating to 172.16.42.1:1471. You can also access the interface via a WAN connection, by specifying the IP of your WiFi Pineapple once it's connected to another network.

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.



Navigating the UI

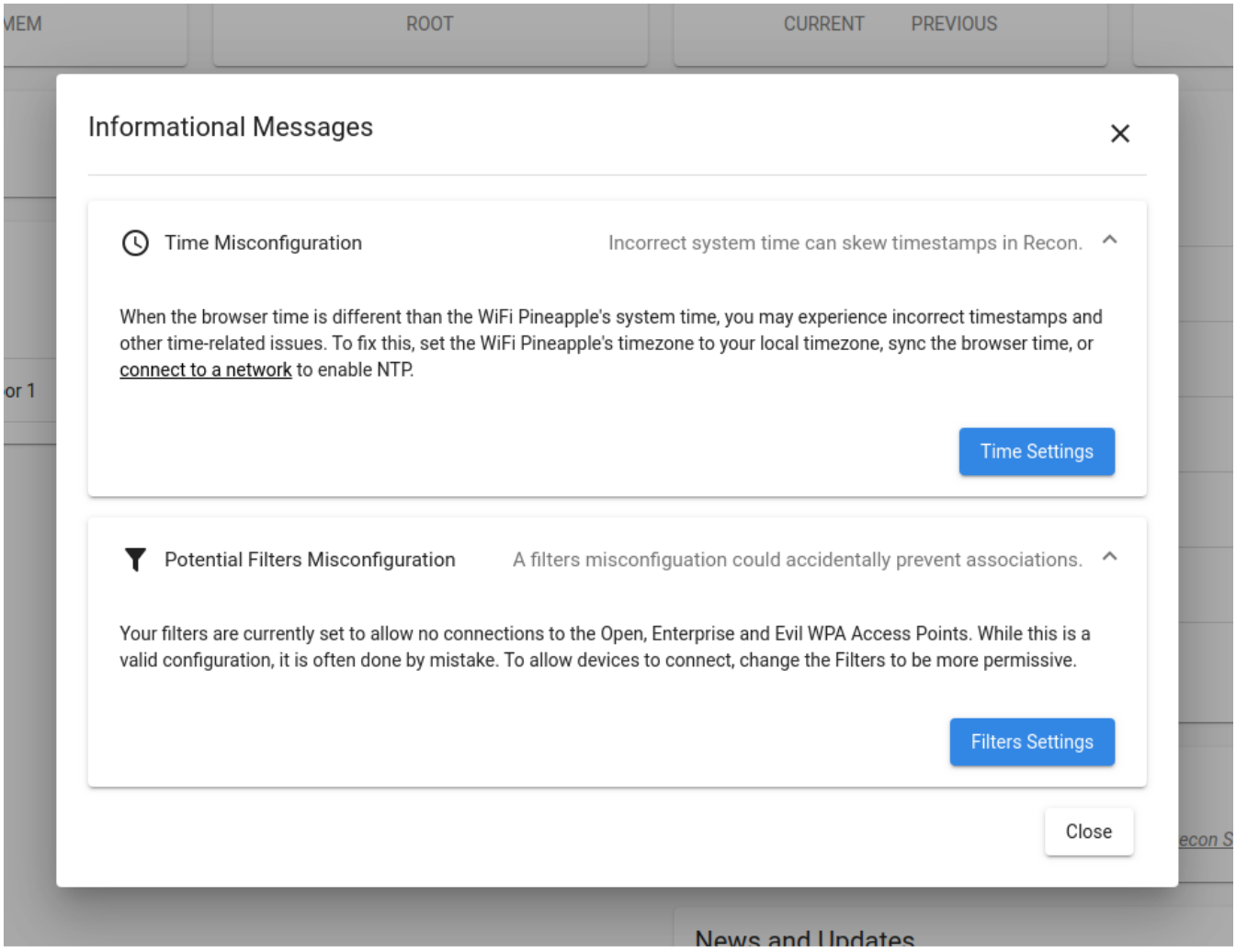
Once you've logged in, you'll see the Dashboard. At the top of the page is the title bar, which includes the current firmware version and buttons to view **Notifications**, view **Informational Messages**, open the **Web Terminal** as well as a context menu for more.

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.

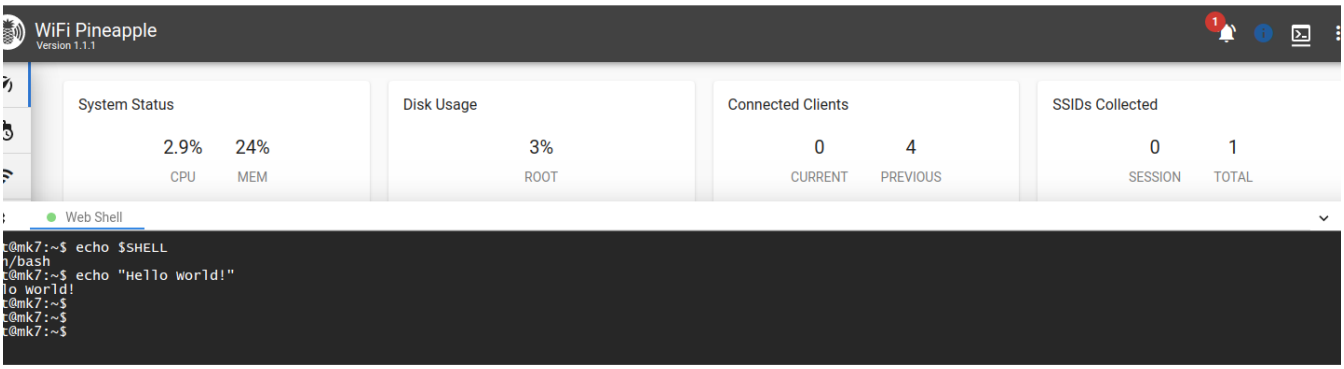
Informational Messages

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



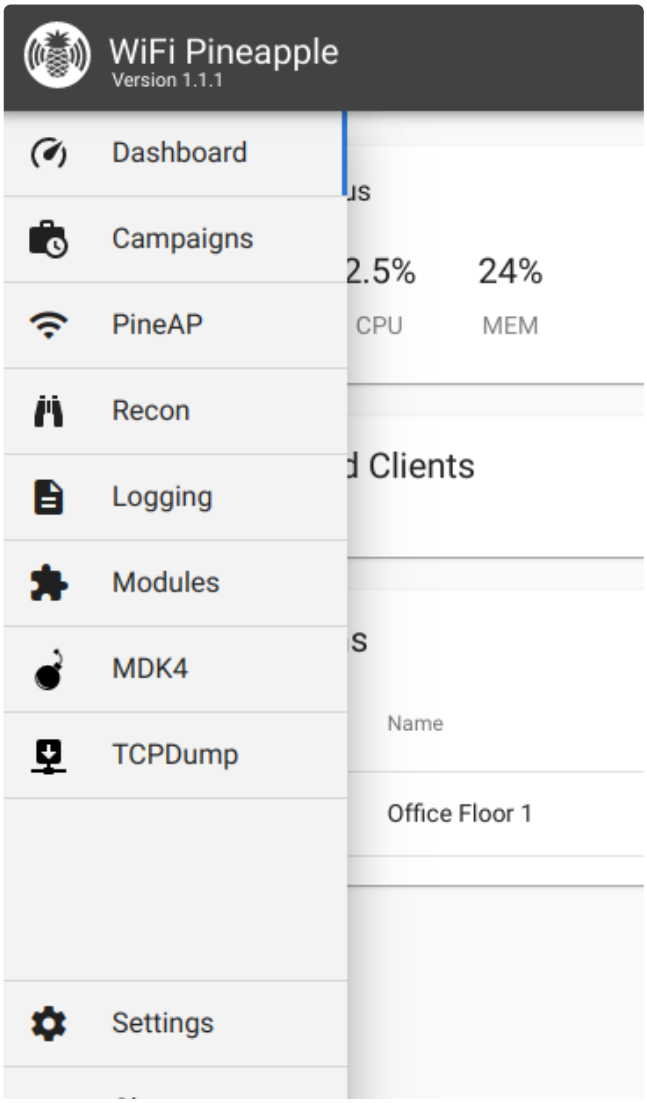
Web Terminal

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.



Sidebar

On the side of the page, you will see the **Sidebar**. This sidebar houses convenient links to the system modules, and can be used to pin installed modules to. You can extend the sidebar outwards by clicking the **Show More** button anchored at the bottom.

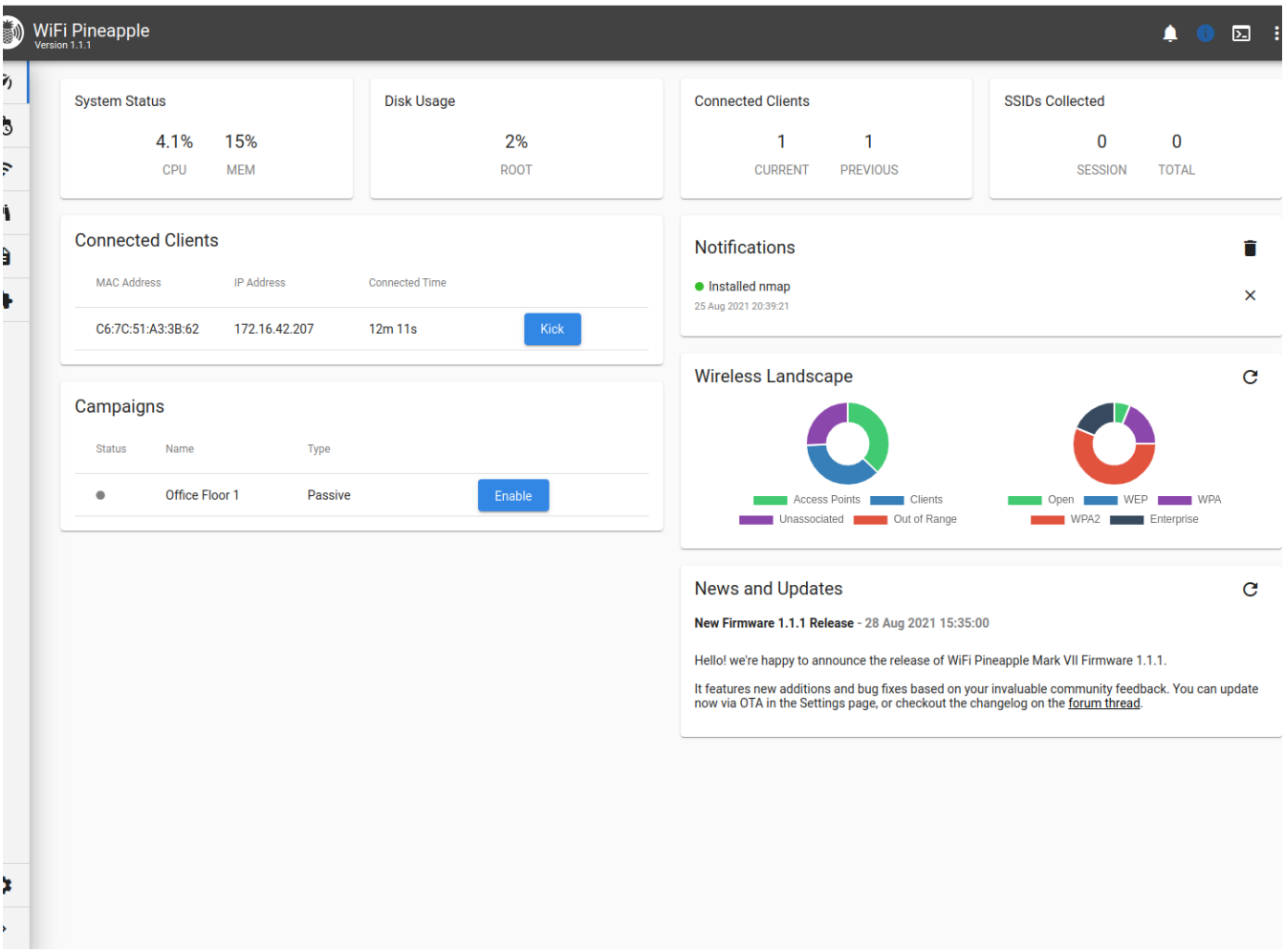


Close

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.



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

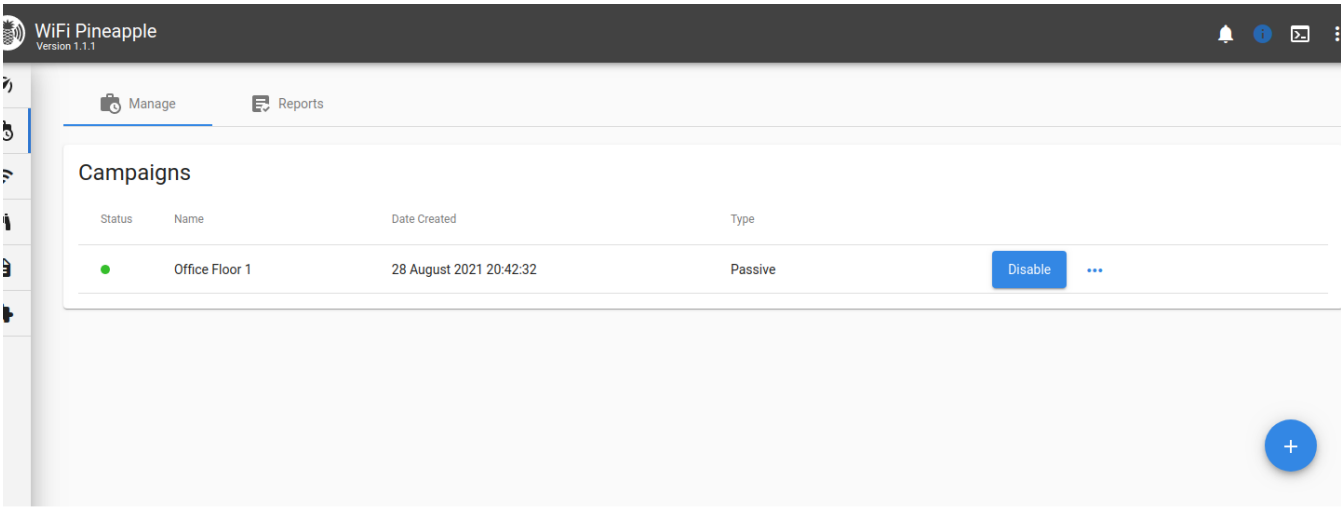
Latest news and release notes from Hak5.

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.

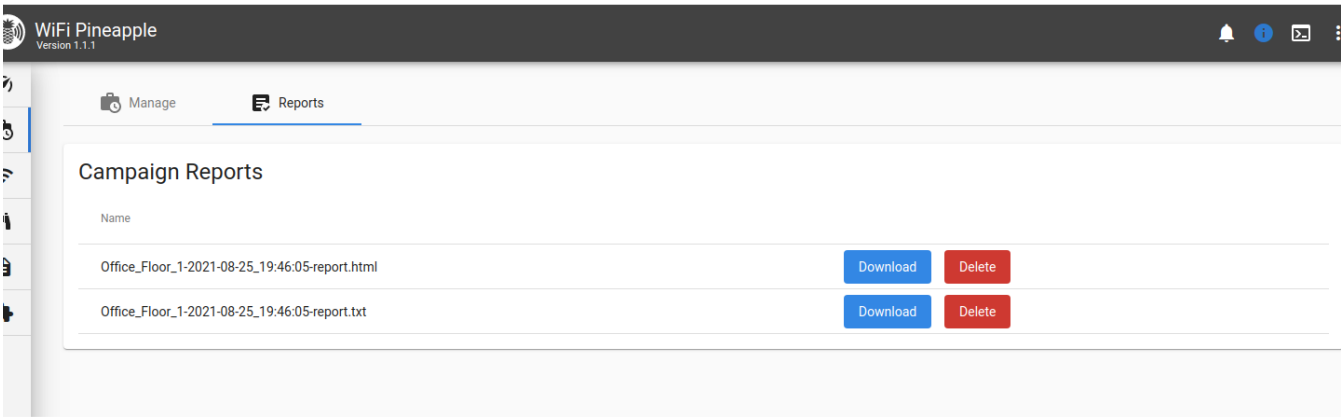
Manage

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.



Reports

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



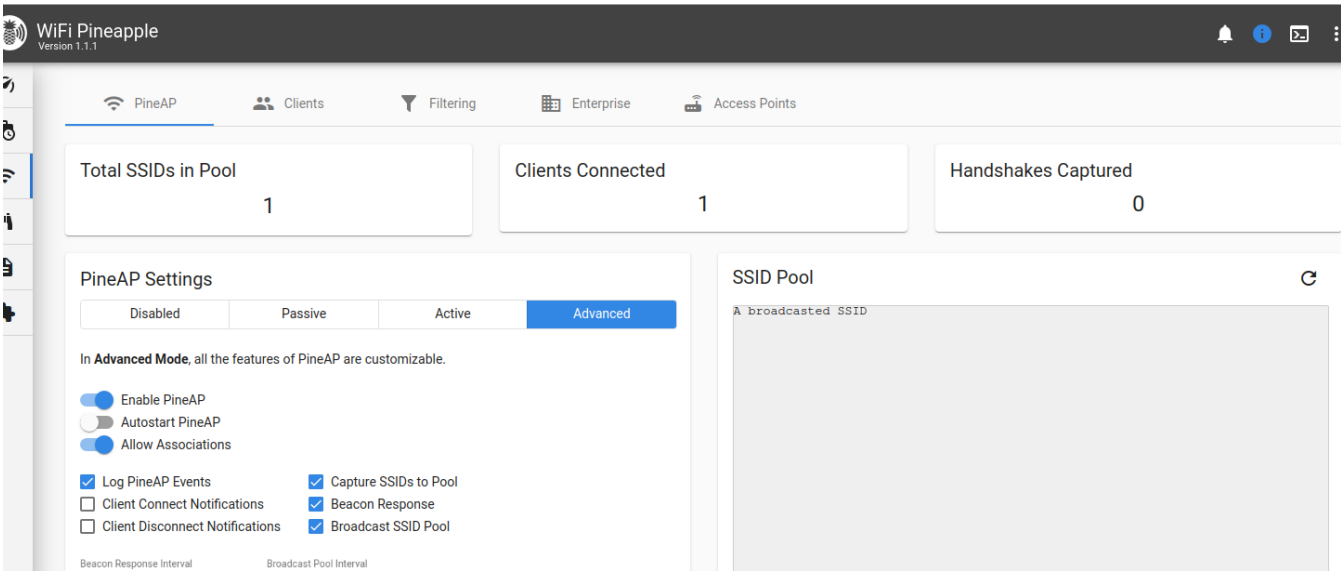
PineAP

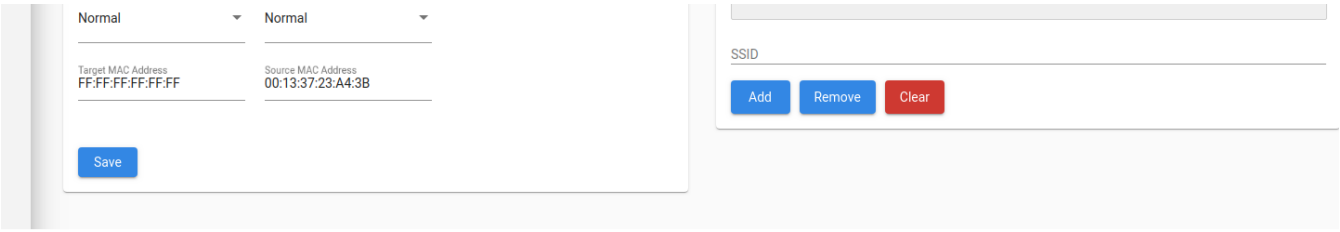
PineAP is the center of the WiFi Pineapple's rogue access points, client management and filtering.

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.

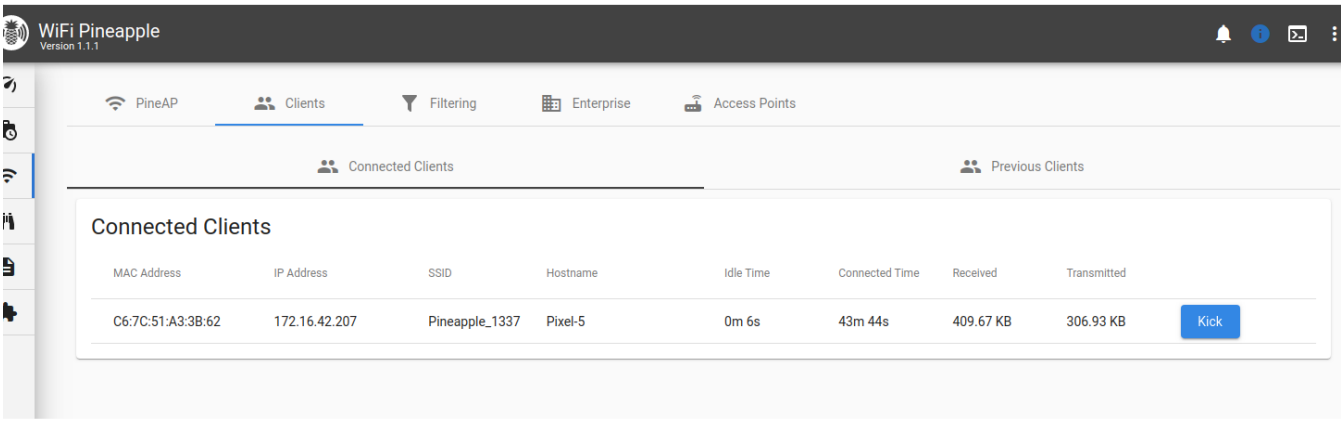
On the right hand side, you can find the current SSID pool. These SSIDs can be automatically collected in the Passive and Active modes, or by selecting the "Capture SSIDs to Pool" option in Advanced. You can use the field below and the Add, Remove and Clear buttons to manually add or remove SSIDs.



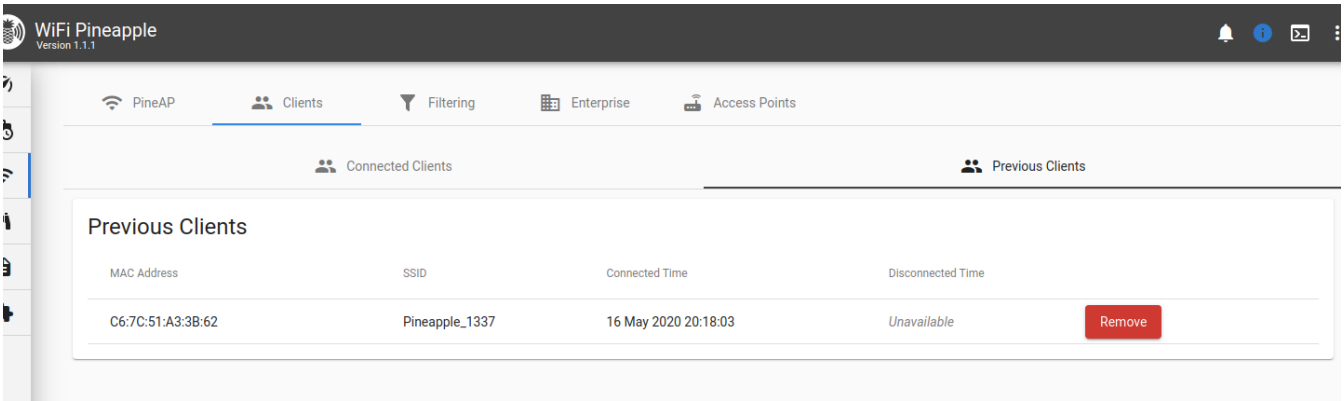


Clients

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.



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".

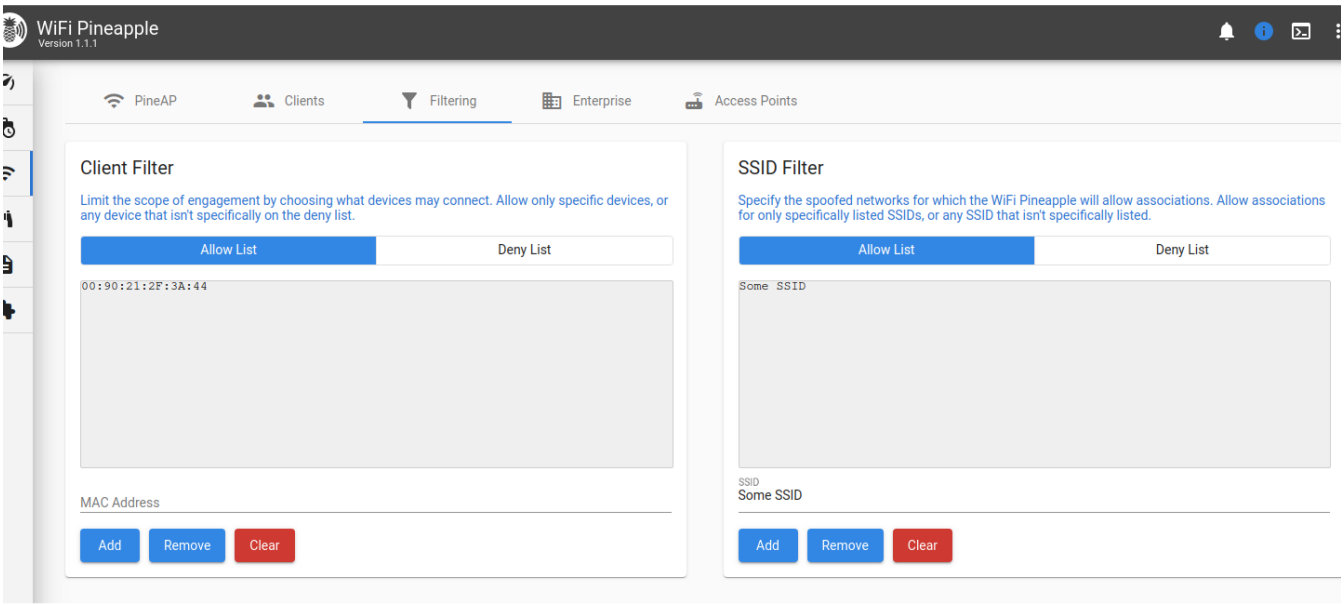


Filtering

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**.

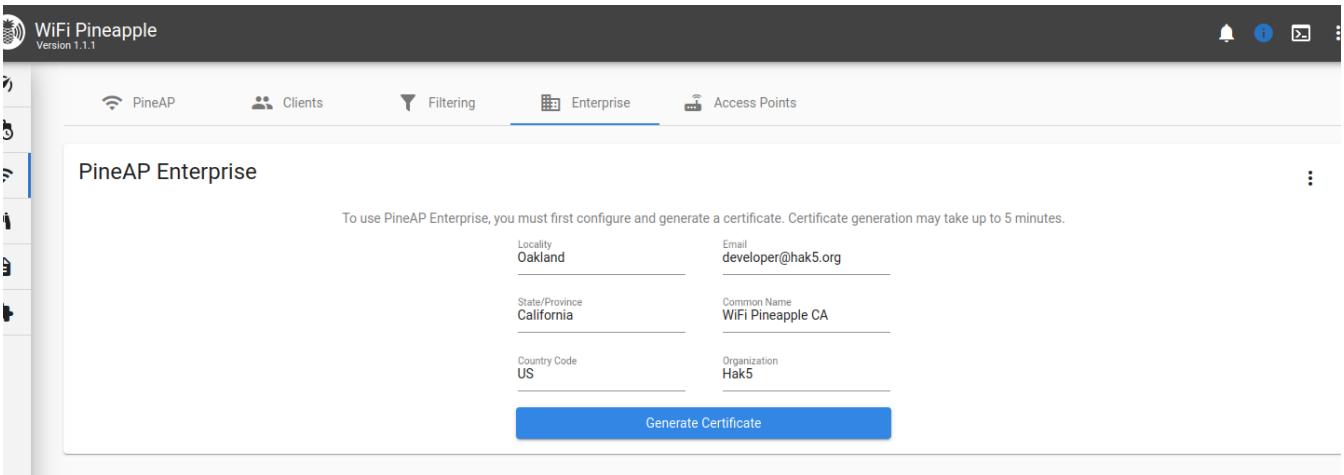
With the client filter you may limit the scope of engagement by choosing what devices may connect. Allow only specific devices, or any device that isn't specifically on the deny list.

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.



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.

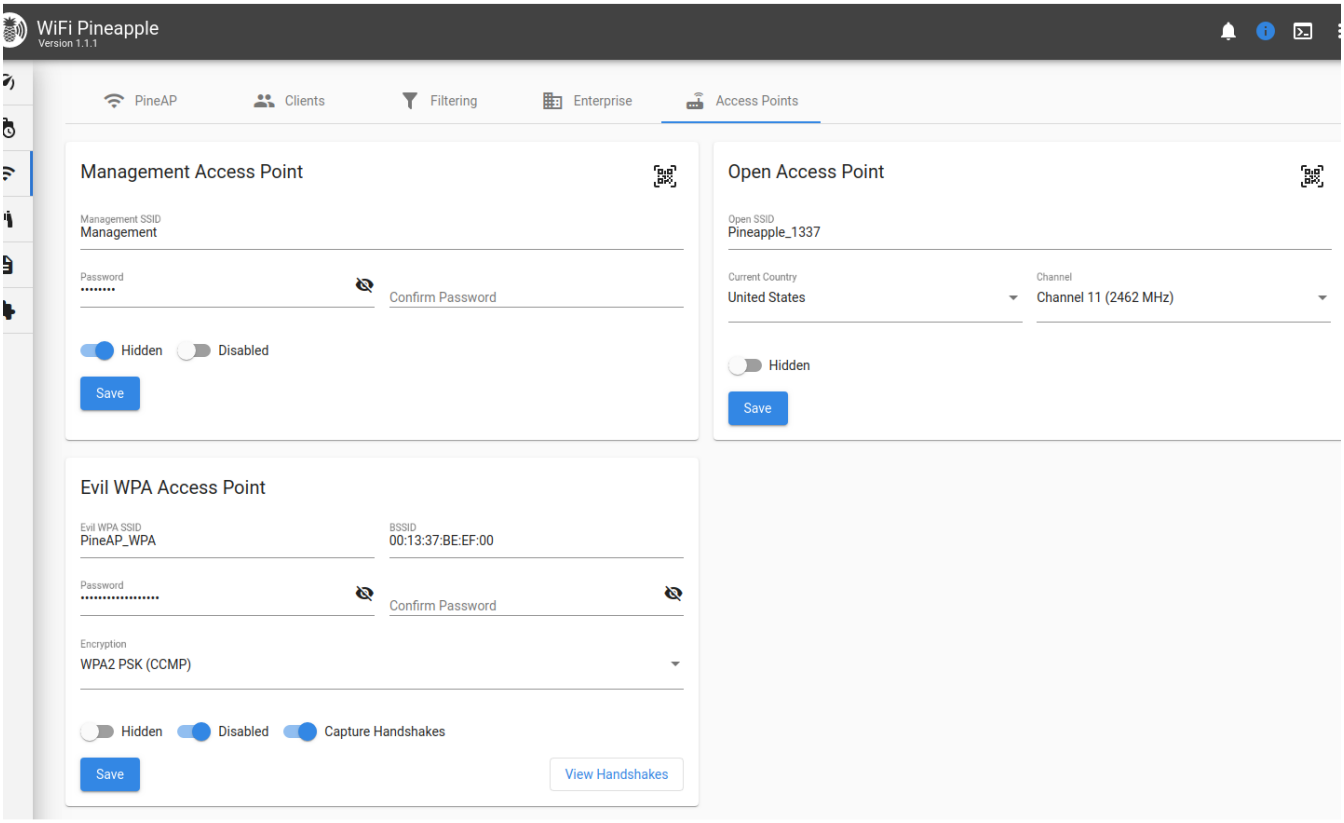


Once the certificate has been generated, you'll see easy to use options to configure the rogue enterprise access point, and view the challenge data any connected clients provide.

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**.



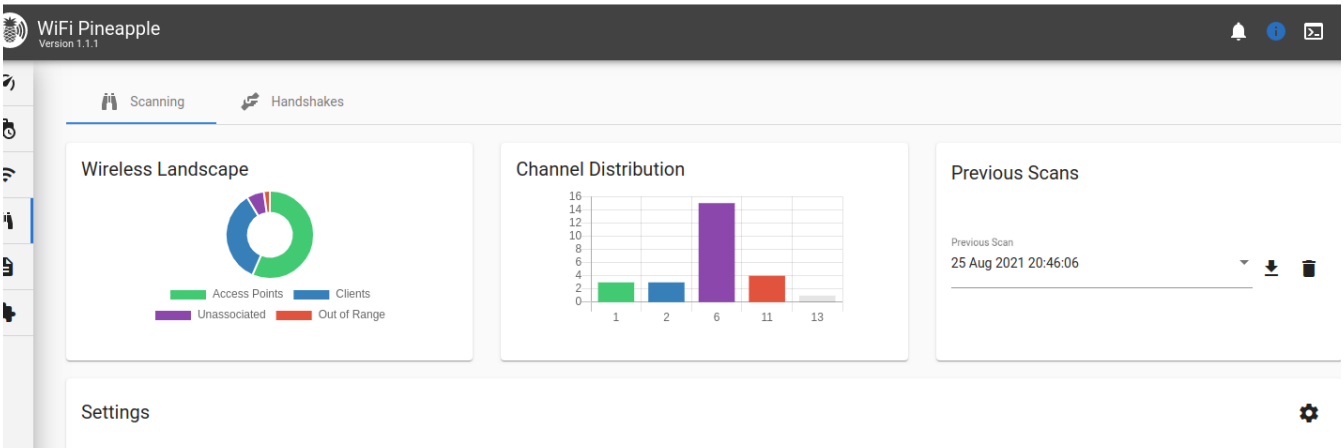
Recon

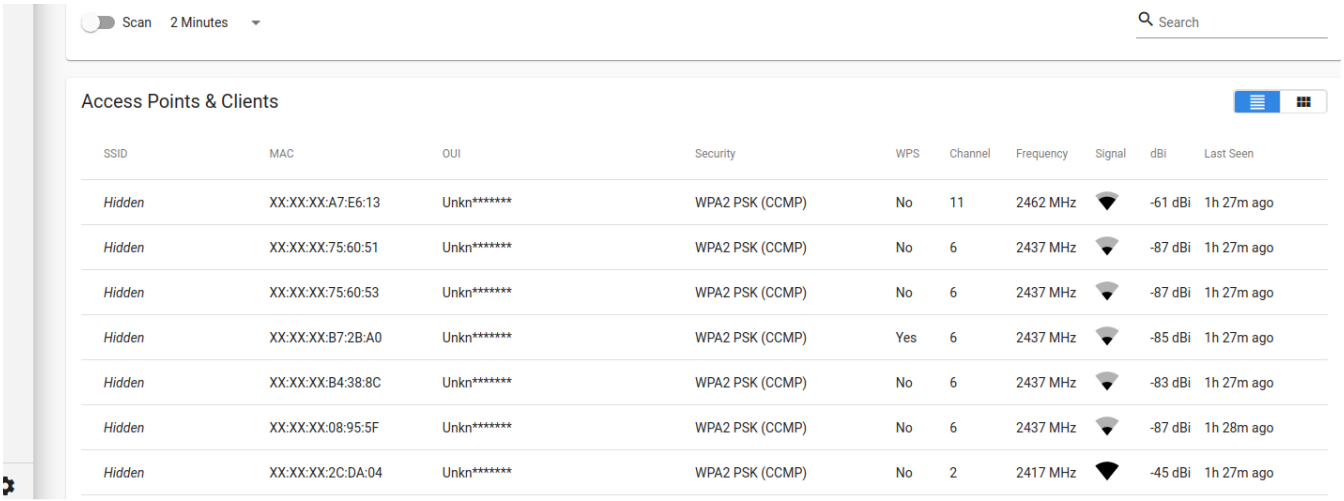
Recon is the WiFi landscape scanning tool incorporated into PineAP.

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.

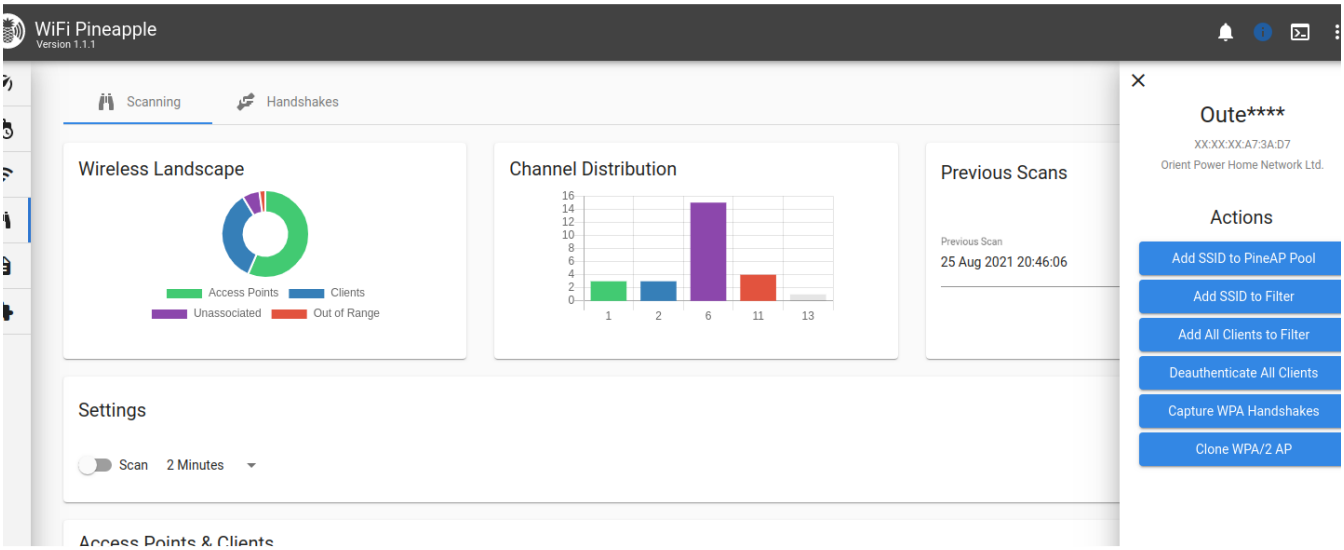
To change to a mobile friendly view, select the card button next to the table icon in the **Access Points & Clients** card.





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

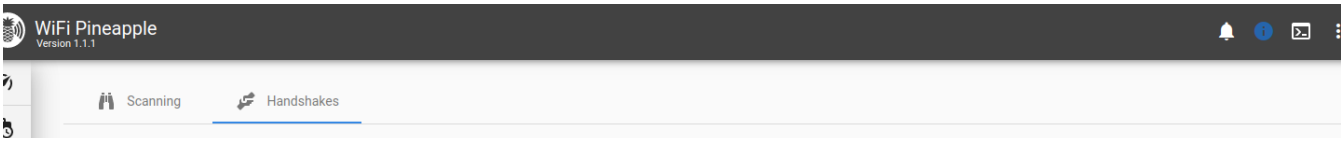
By clicking on an AP or Client in the list, a side menu will slide out from the right. From here you can select options specific to the type of device you selected, such as capturing handshakes or cloning, or adding MAC addresses to the Filters.

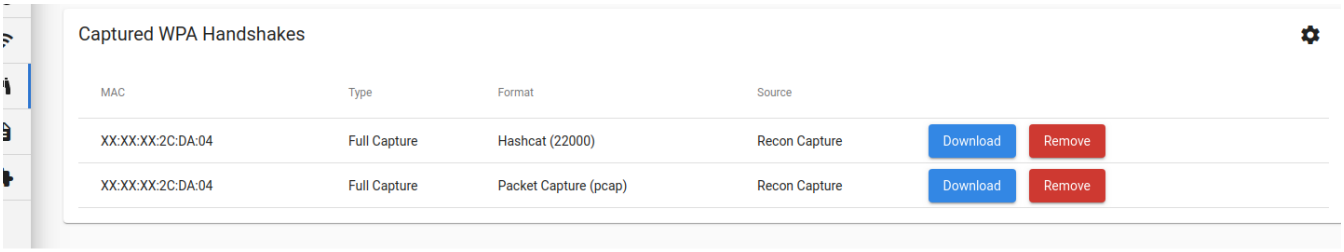


Handshakes

Switching to the Handshakes tab allows you to view 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**.





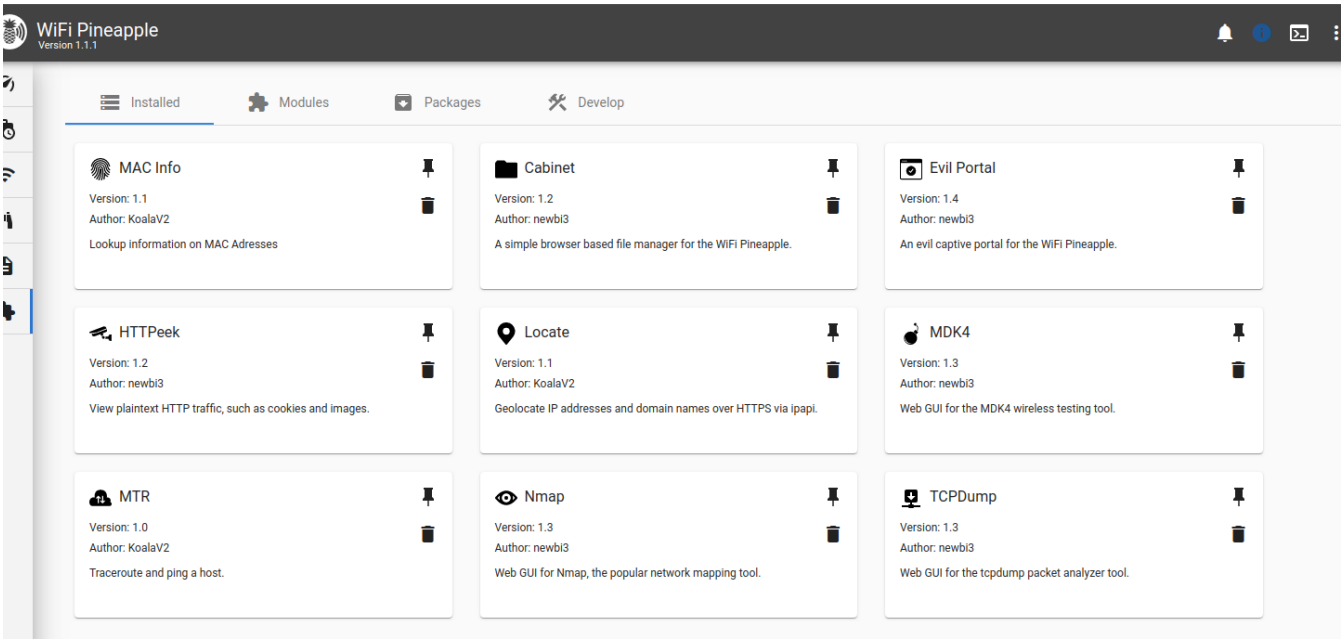
You can specify the Handshake save location by clicking the Settings icon.

Modules

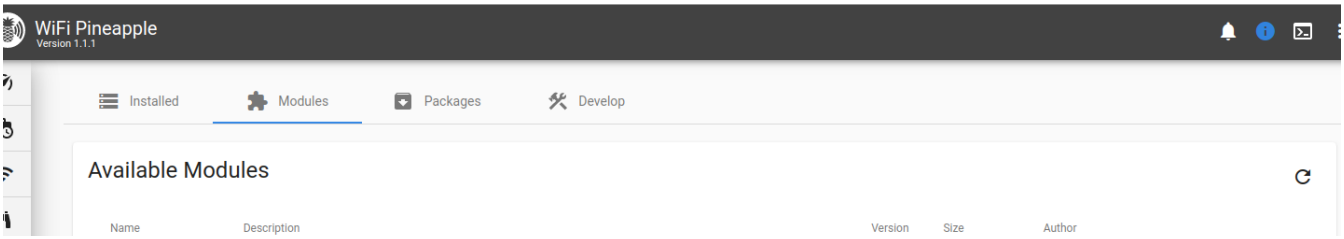
WiFi Pineapple Modules allow the interface to be extended to support new community built features or offer front-ends to command line tools. A vast library of packages is also available.

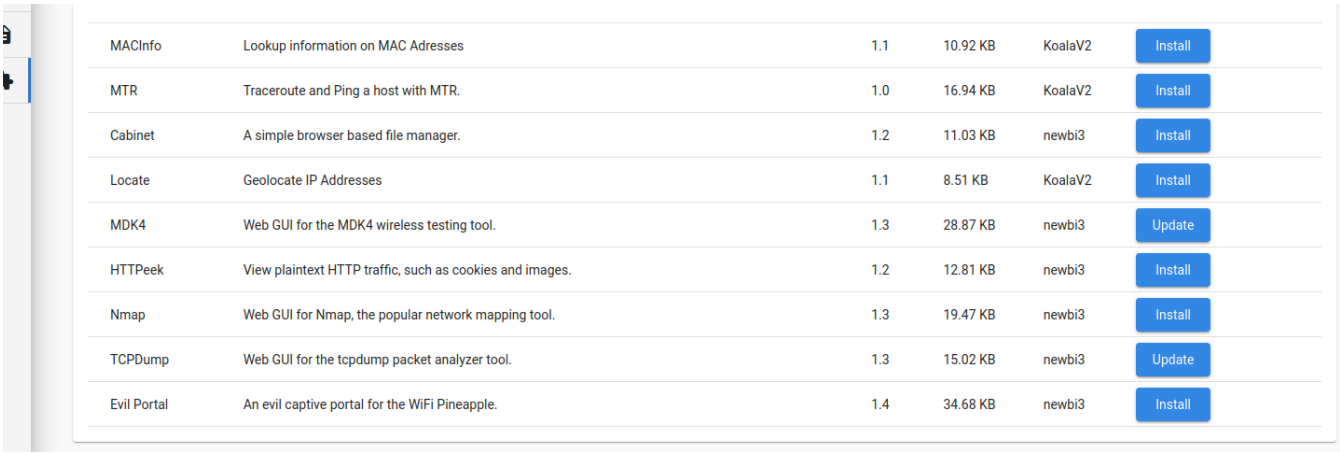
Modules

The main Modules page shows you a list of cards, one for each installed module. To access these modules you can click on the card. You can also uninstall them by clicking on the trashcan icon.



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.





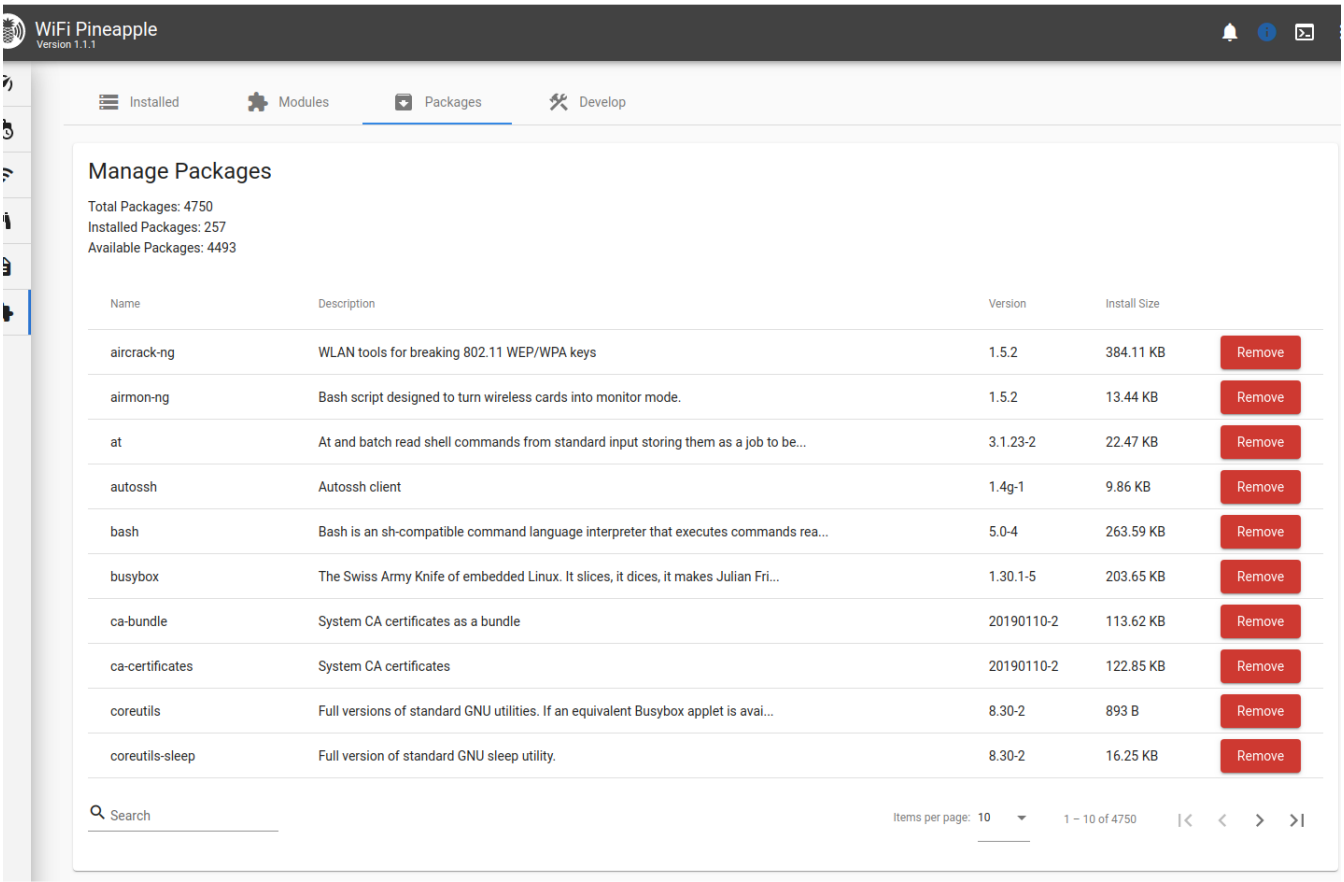
MACInfo	Lookup information on MAC Adresses	1.1	10.92 KB	KoalaV2	Install
MTR	Traceroute and Ping a host with MTR.	1.0	16.94 KB	KoalaV2	Install
Cabinet	A simple browser based file manager.	1.2	11.03 KB	newbi3	Install
Locate	Geolocate IP Addresses	1.1	8.51 KB	KoalaV2	Install
MDK4	Web GUI for the MDK4 wireless 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 to use, which can be accessed via SSH or via the Web Terminal.

> Press the backtick (`) key on your keyboard to open the Web Terminal.

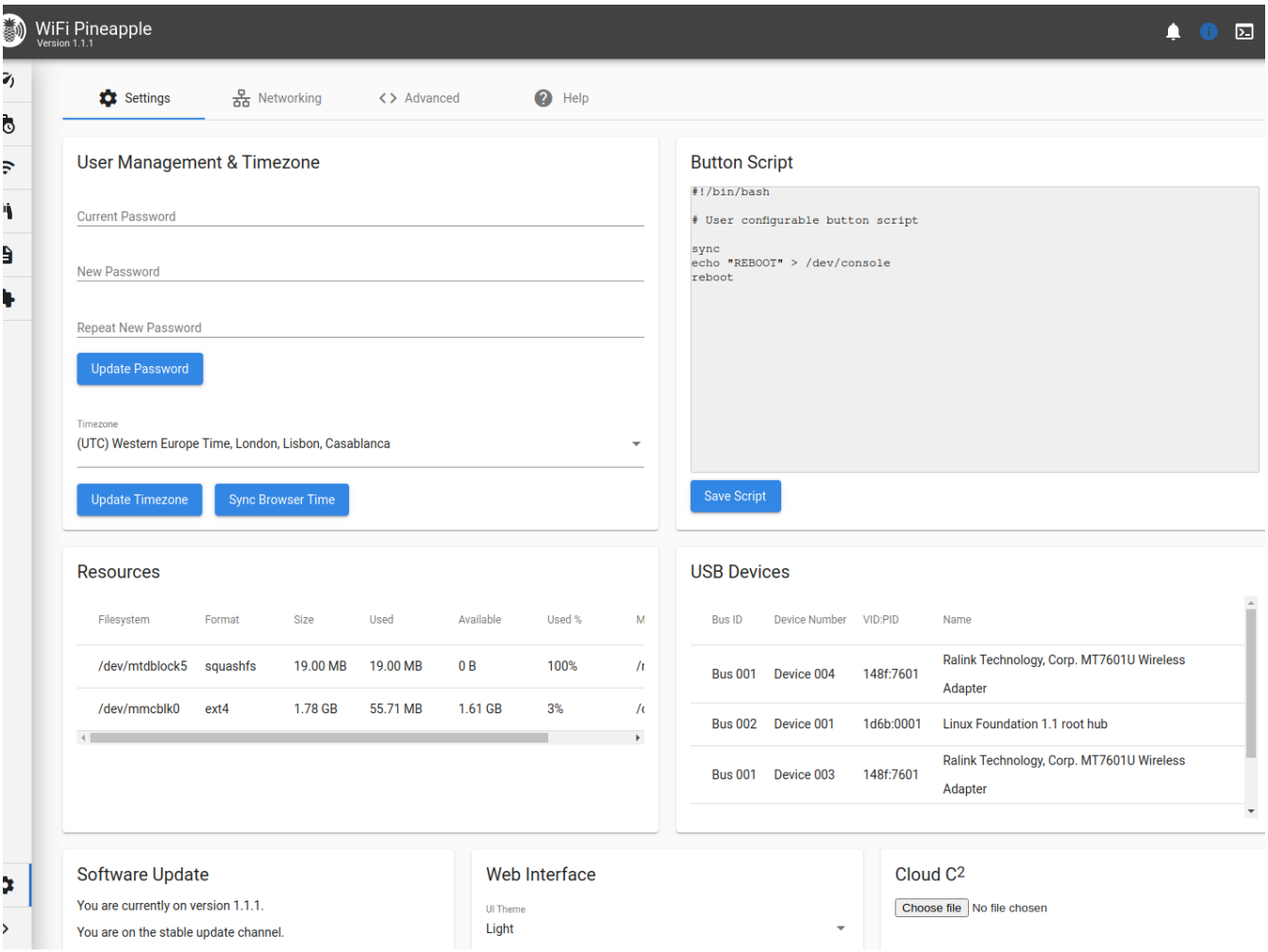


Settings

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

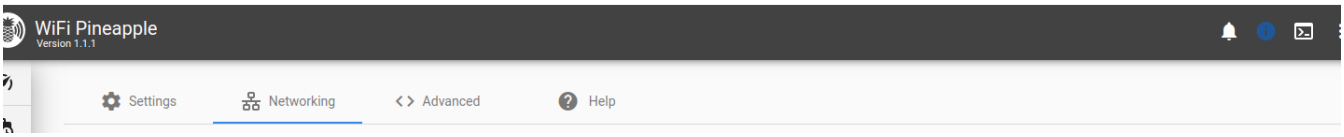
Settings

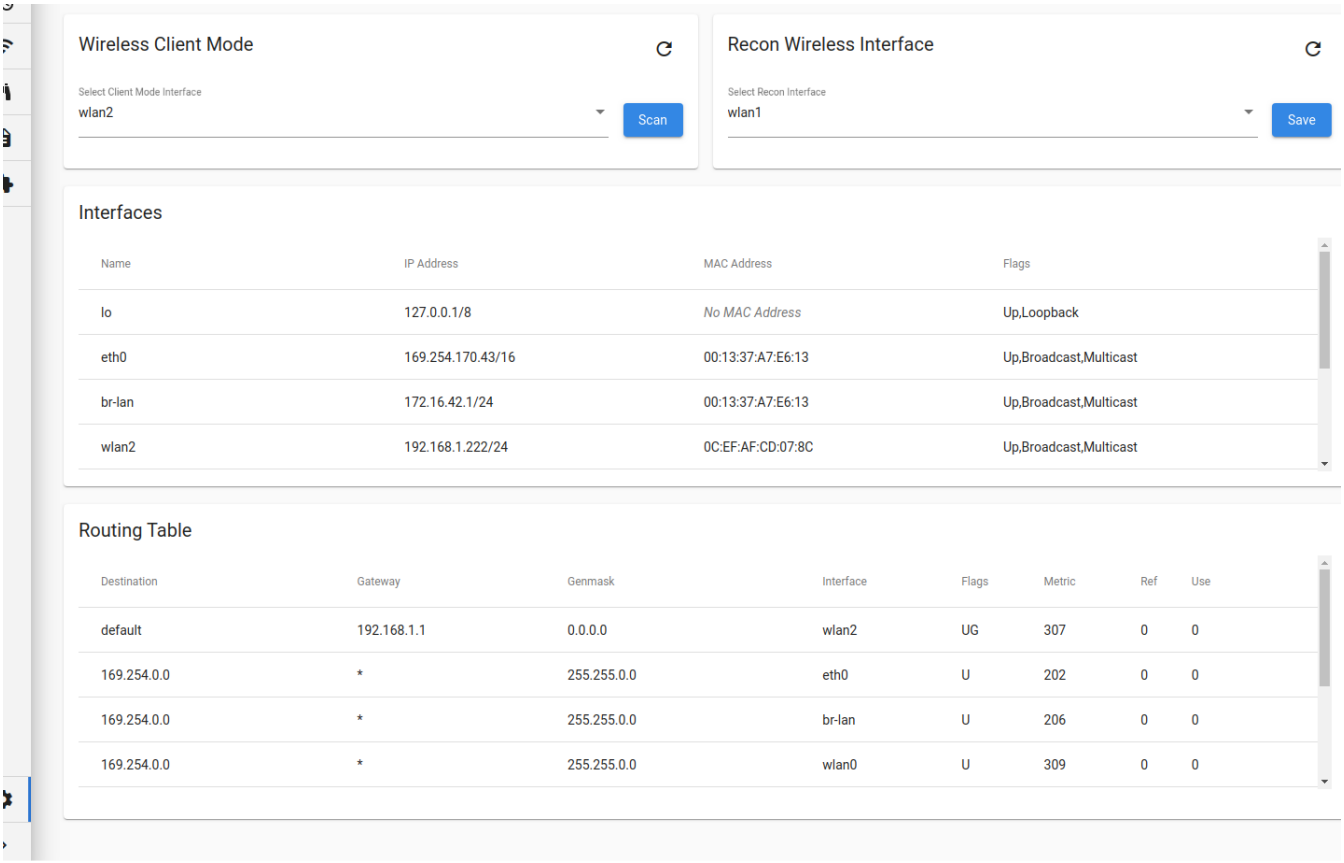
From the main **Settings** page, you can configure the password and timezone and button script. On the second row of cards, you can view the currently mounted file systems and connected USB devices. On the bottom row, you can check for software updates, change the UI theme and configure the device for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



Networking

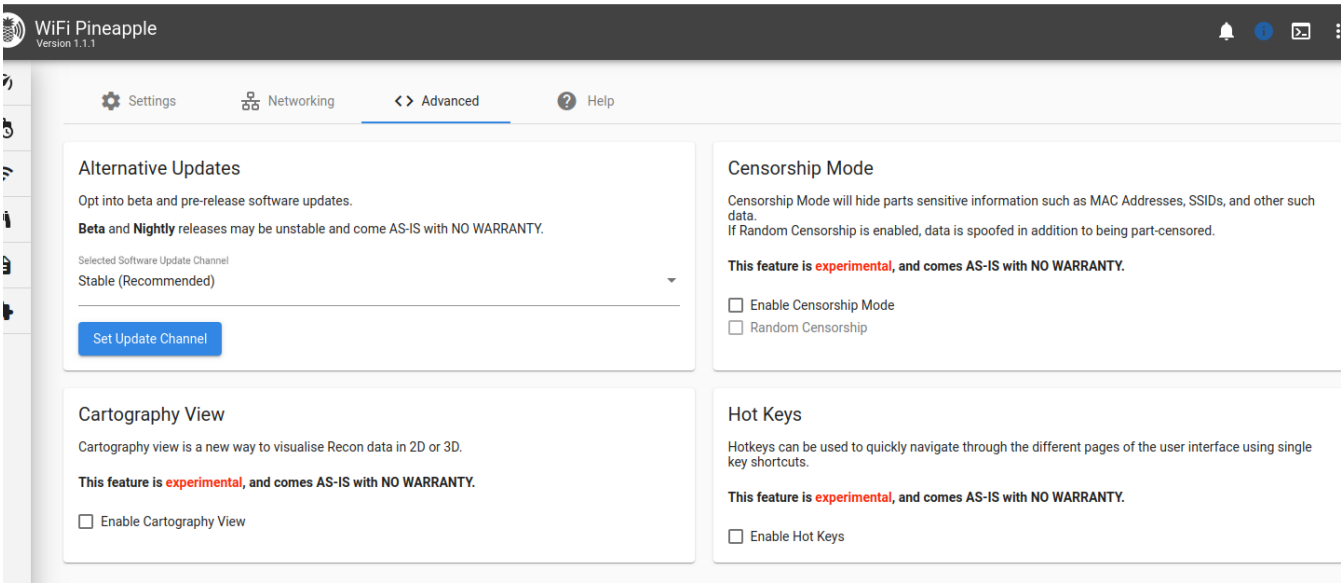
The **Networking** tab shows easy to use cards for configuring a Client connection to another Access Point, set the interface used for Recon as well as listing the current interfaces and routing table.





Advanced

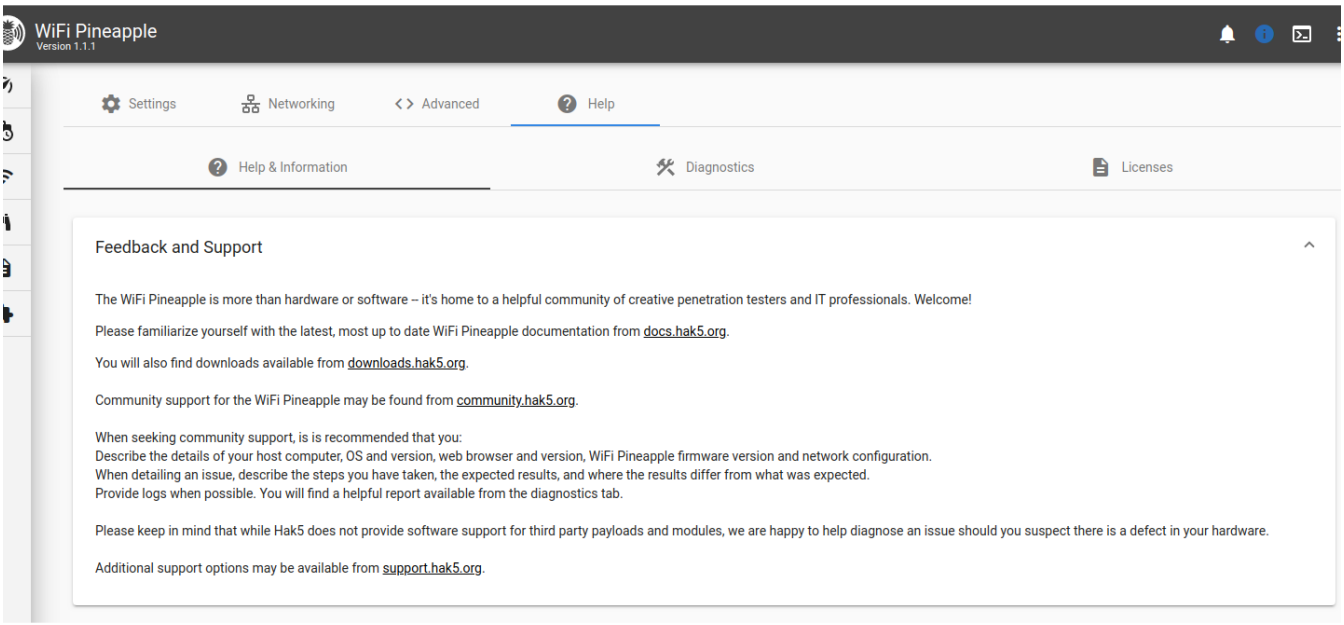
The **Advanced** tab shows options to change the current update channel for opting into Beta firmware releases. From here you can also access experimental features such as Censorship (hiding sensitive information in the UI) and Cartography (2D or 3D map of Recon data).



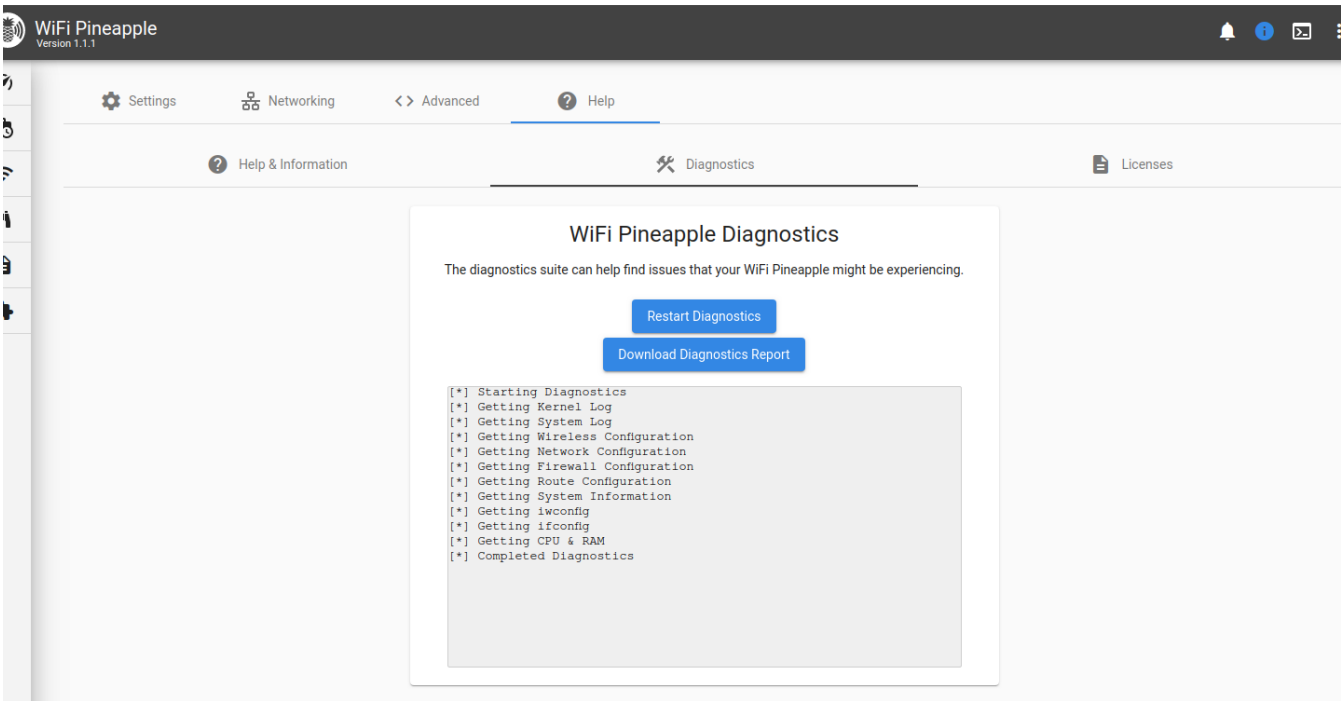
Help

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.



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.



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).

Lastly, 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.

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 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. For example 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 and 802.11n. Generally their 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 802.11g protocol 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. An 802.11n based network using 40 MHz bandwidth will occupy nearly twice the spectrum as the 22 MHz wide 802.11g channel and similarly achieve a much faster data rate.

Modulation also affects data rate, with the most common modulation type being OFDM or Orthogonal frequency-division multiplexing. In addition to being a mouthful, it's a digital encoding technique used to cram a lot of data on a small amount of spectrum. It's the same technology used in DSL modems and 4G mobile broadband. The important takeaway is that OFDM supersedes the older DSSS modulation technique used in 802.11b.

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. These networks are more rare to find, though when they are it's typically indicative of aging infrastructure.

Nowadays 802.11g and 802.11n are more commonly found with data rates up to 54 Mbps and 150 Mbps respectively. Both operate in the 2.4 GHz band with the latter capable of operating in the 5 GHz band as well.

An important thing to consider about protocols is that WiFi radios operating on newer protocols almost always contain backwards compatibility, so an access point using the 802.11g standard may be just as enticing to a client device capable of using the newer 802.11n standard.

Modes of Operation

Most commonly a WiFi radio will operate in one of three modes: Master, Managed, Monitor. Additional modes include ad-hoc, mesh and repeater and are both less common and outside the scope of this 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.

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 NIC hardware, though 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 NIC 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.

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 considered MAC spoofing.

Broadcast MAC Address

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 NIC 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.

Service Sets and Identifiers

If you've been using WiFi for a while – and if you're reading this book I'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.

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

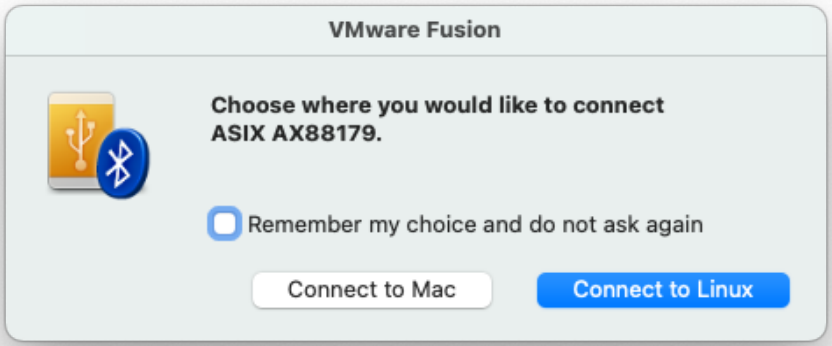
MacOS Support

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.

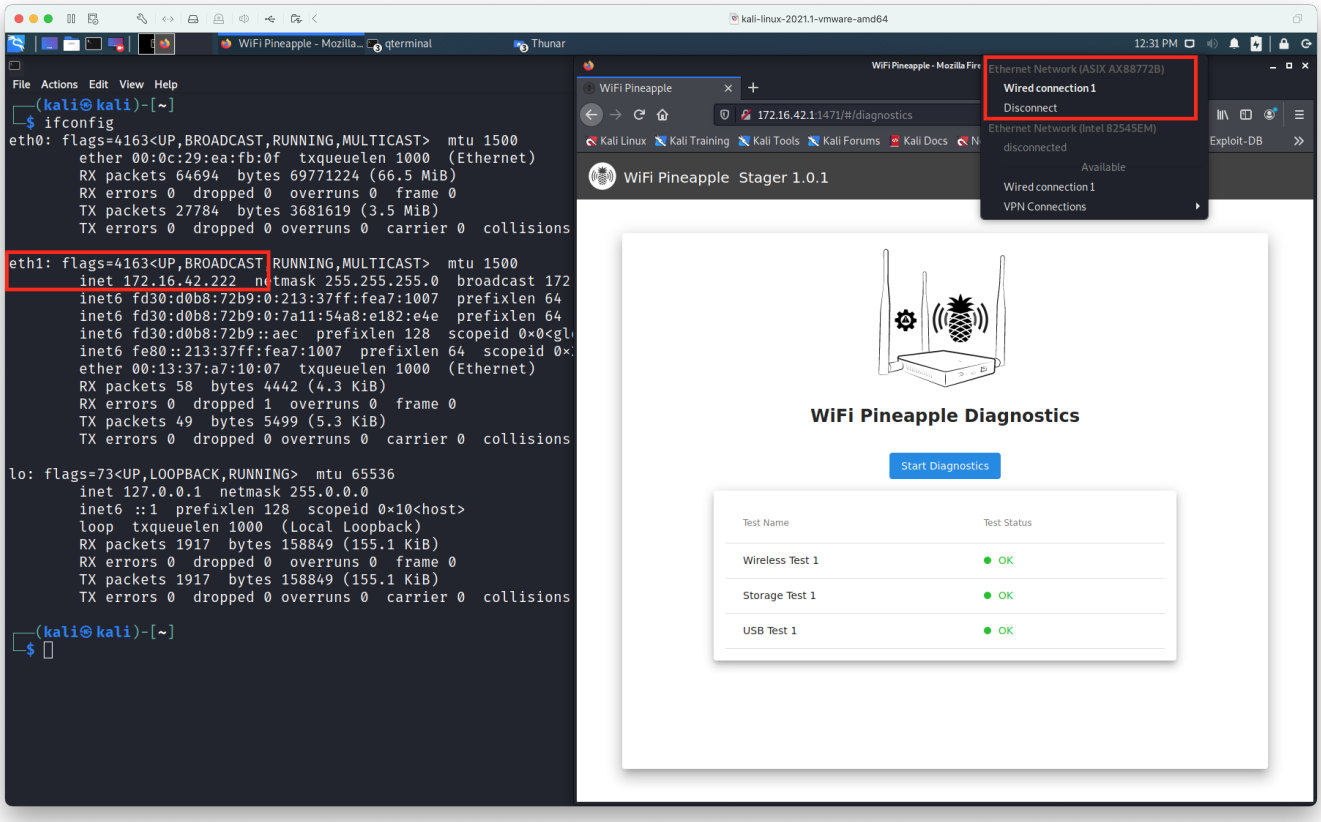
A driver is available for Apple macOS 10.9 to 10.15 from the manufacturer at https://www.asix.com.tw/en/support/download

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.



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.



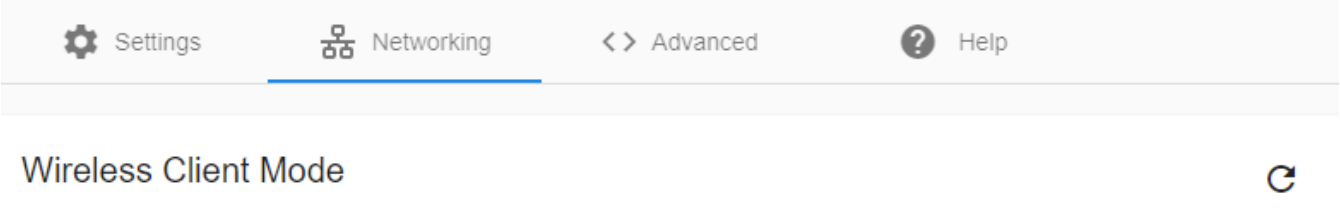
> ⚠ Because of recent changes to macOS's device driver model, macOS version 11 and above is not supported.

Establishing an Internet Connection

Configuring a Client Mode Connection

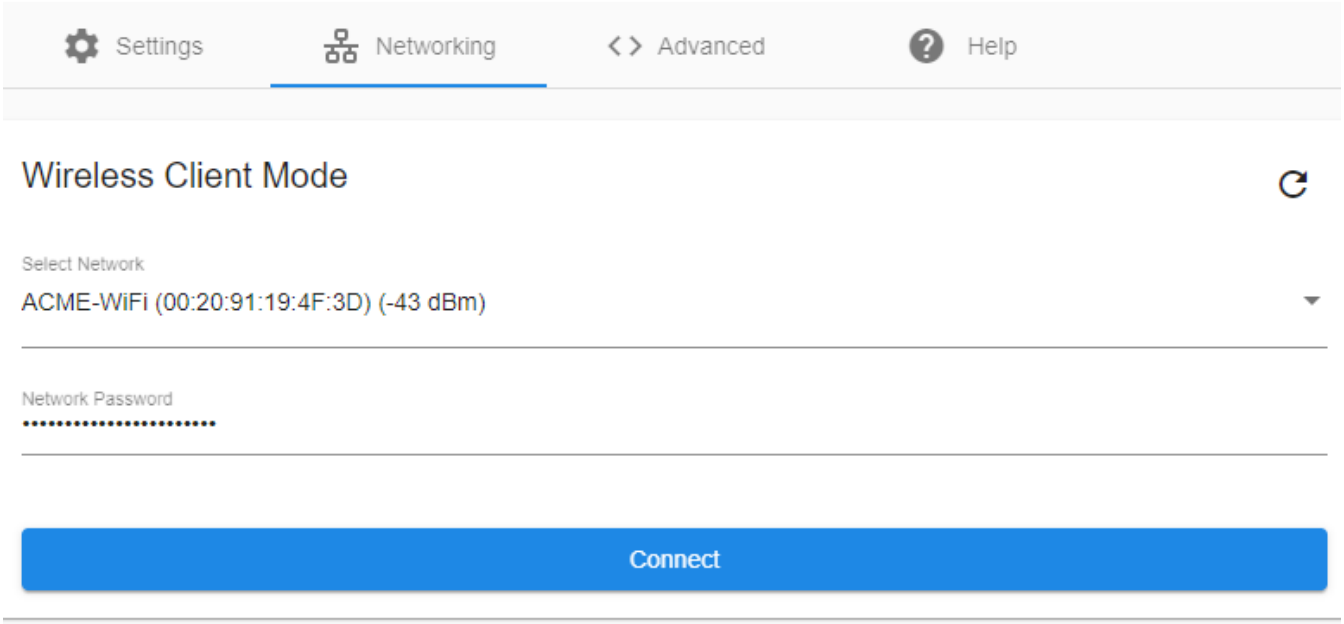
You may use a radio on the WiFi Pineapple to connect to an external WiFi network, for getting an internet connection or for communicating with other devices on that network.

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**.

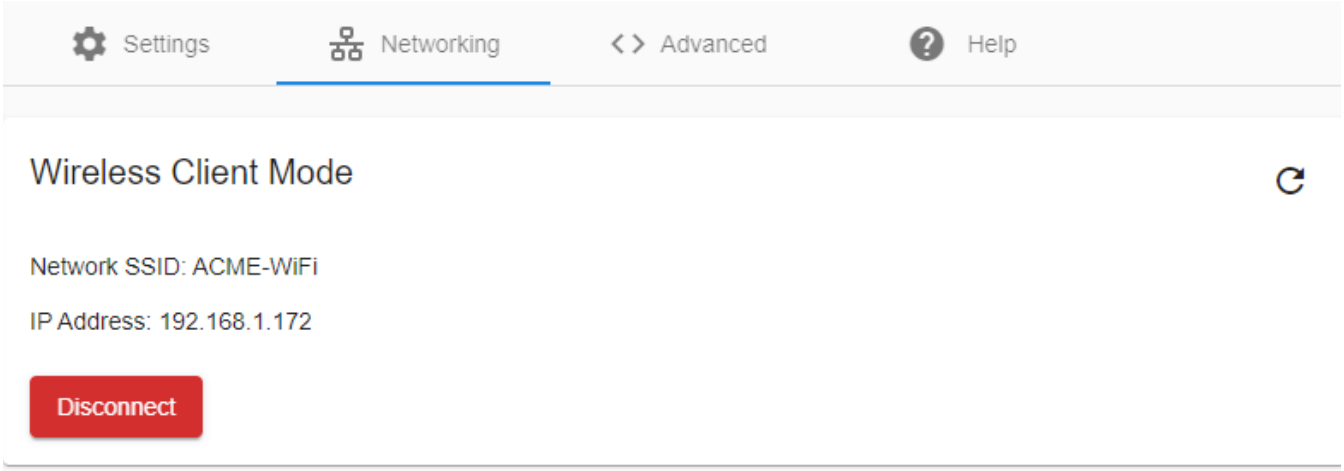


While you may select other wireless interfaces for Client Mode, you are **greatly** recommended to use wlan2, as it is dedicated for Client Mode.

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.



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



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

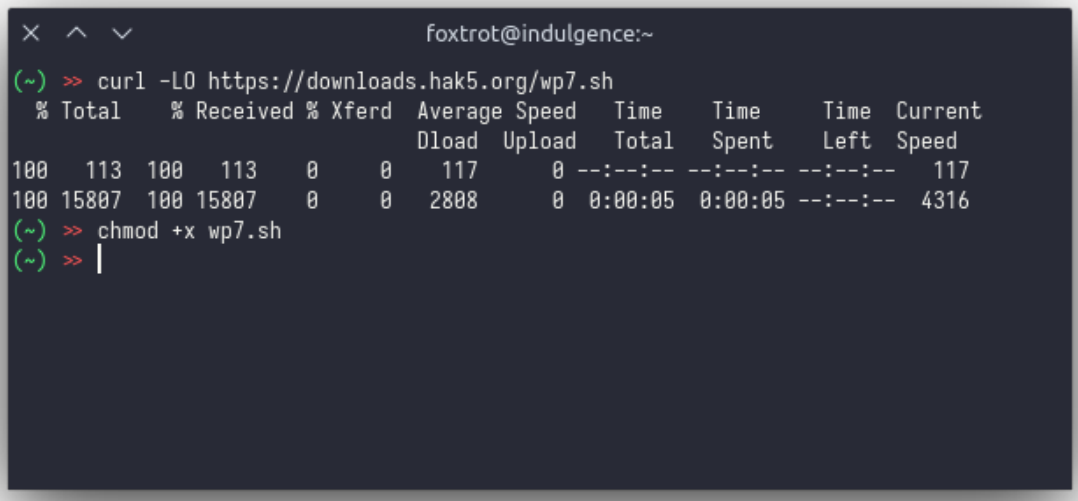
ICS, or **Internet Connection Sharing**, can be used to share internet from your computer to the attached WiFi Pineapple, over it's USB-C Ethernet connection.

On Linux, this is easy to accomplish with the use of the WiFi Pineapple ICS Script, referred to as **wp7.sh**. It is a shell script that will guide you through the ICS setup process.

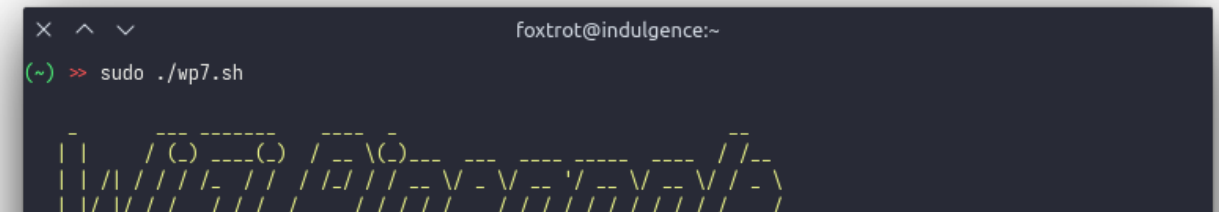
Getting Started

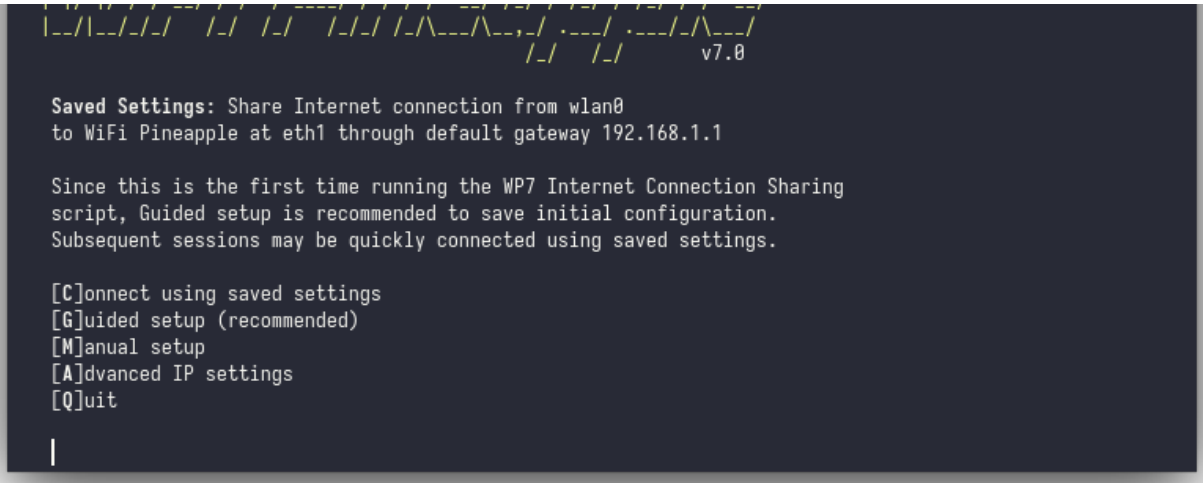
Start by opening the Terminal emulator for your Linux distribution. On Ubuntu, Gnome Terminal can be found by searching for "Terminal".

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



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





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.

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.

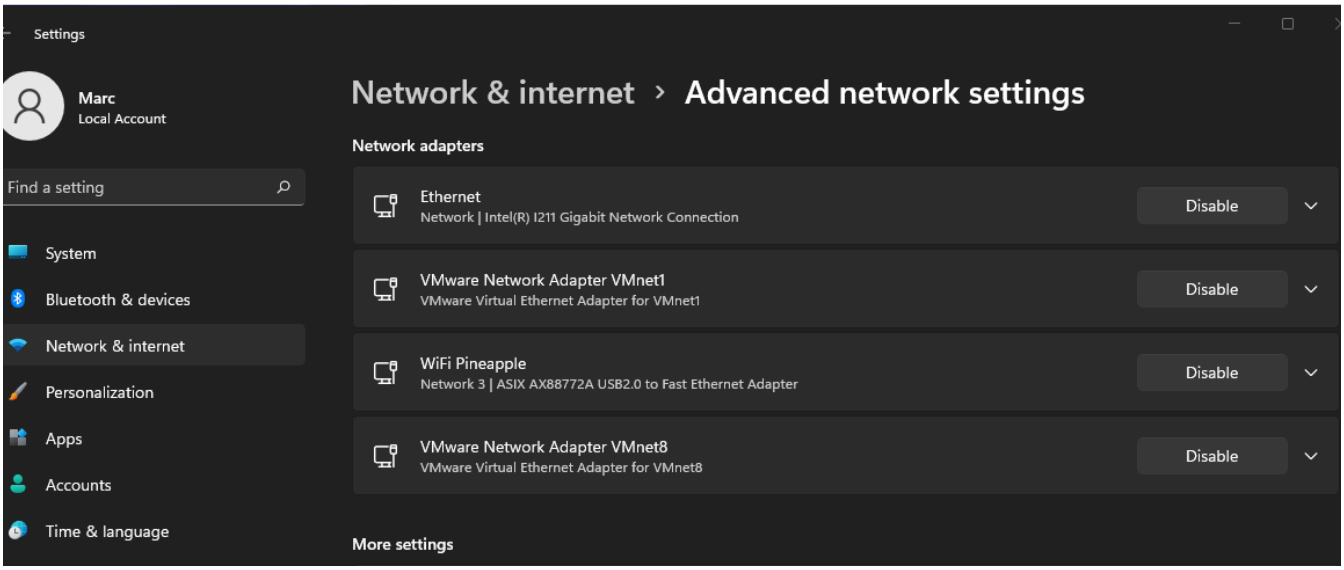
Configuring ICS on Windows

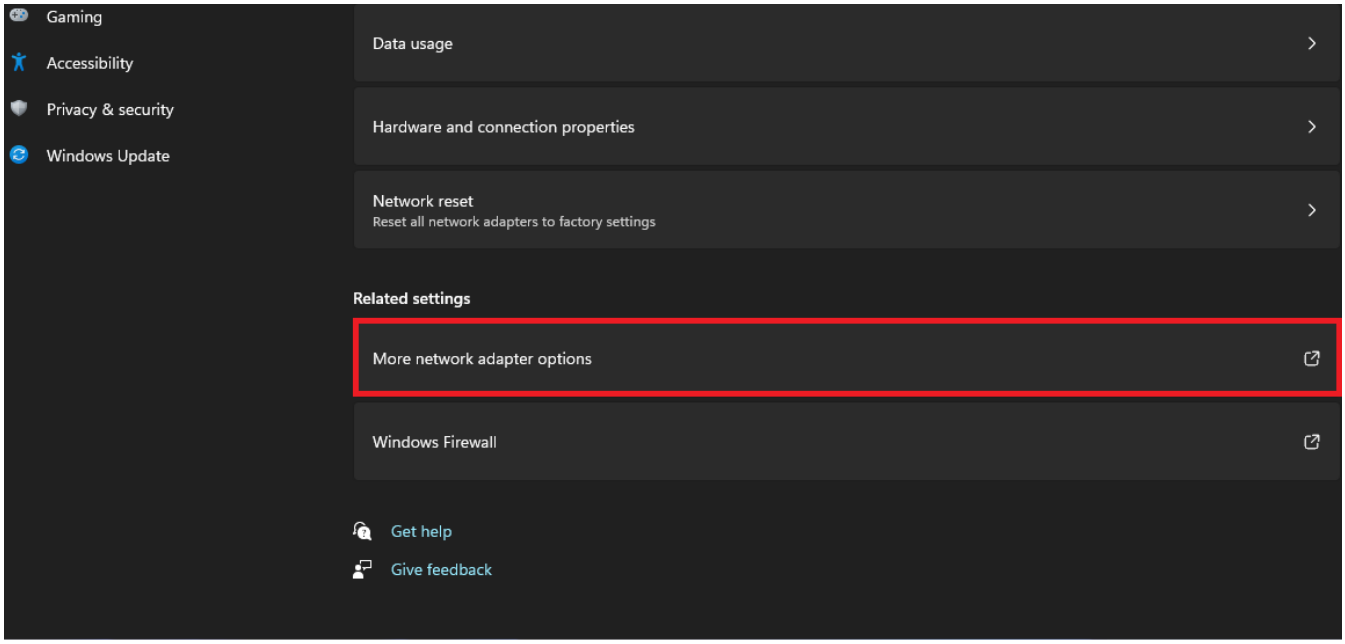
On Windows, Internet Connection Sharing is achieved by using Window's "Network Sharing" feature, by sharing one internet-enabled interface to the WiFi Pineapples.

> 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

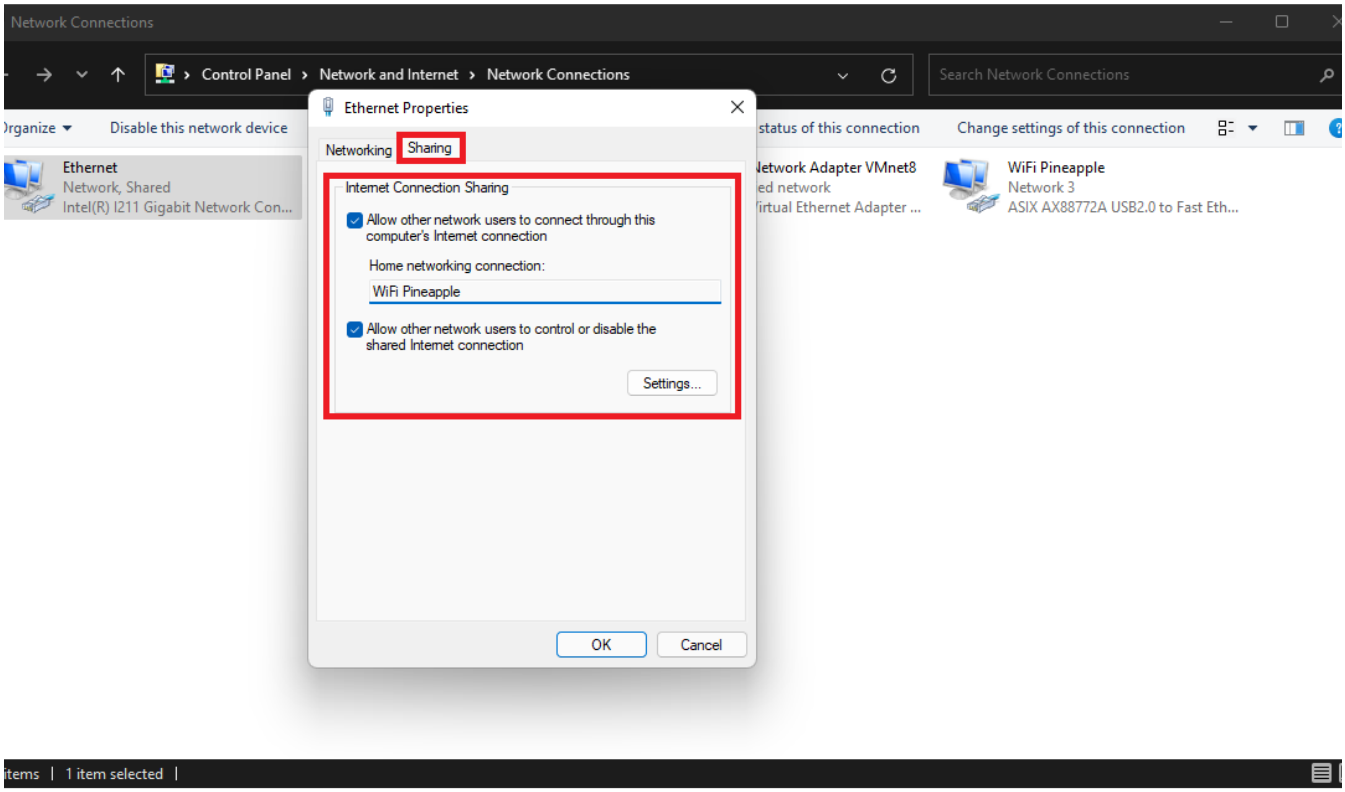
Start by opening the **Network & Internet** settings in the Windows settings application. Scroll down to **Related settings** and click **More network adapter options**.



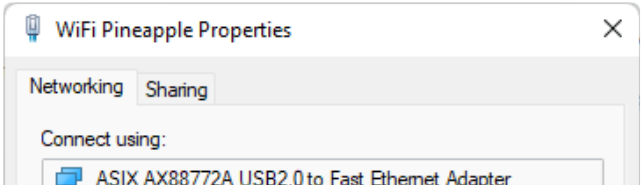


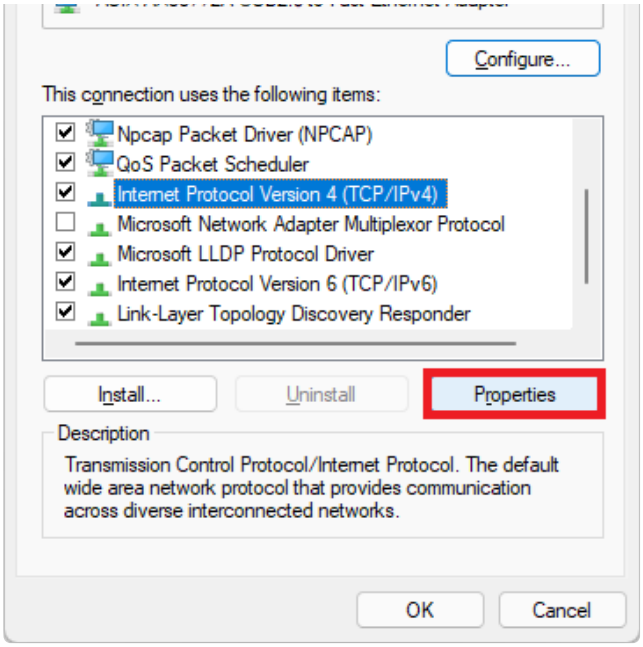
In the new window, **right-click the Internet facing adapter, and select "Properties".** In this guide, the Internet facing adapter is the interface named **Ethernet**.

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**.



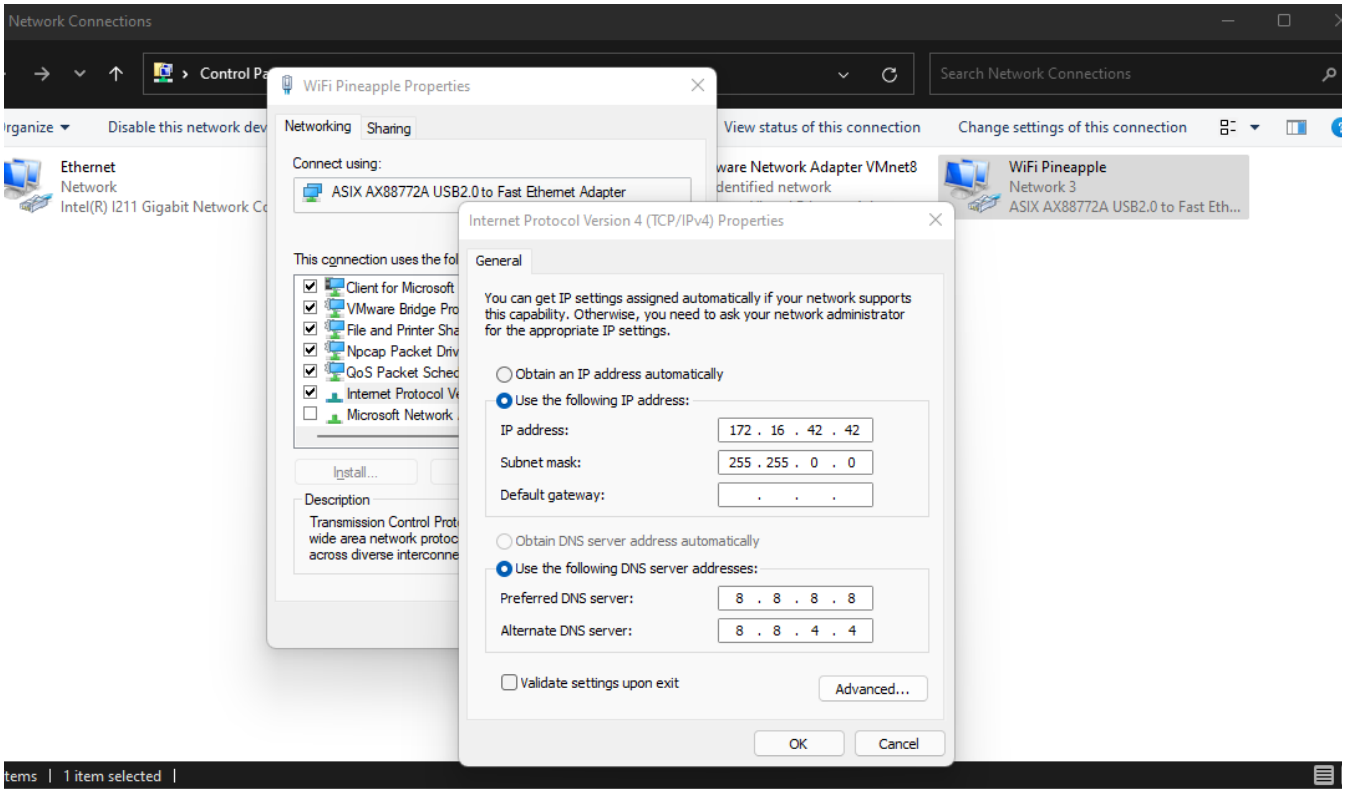
Next, configure the WiFi Pineapple adapter by **right clicking and selecting "Properties".** In the new window, select the text that says **Internet Protocol Version 4 (TCP/IPv4)** and select **Properties**.





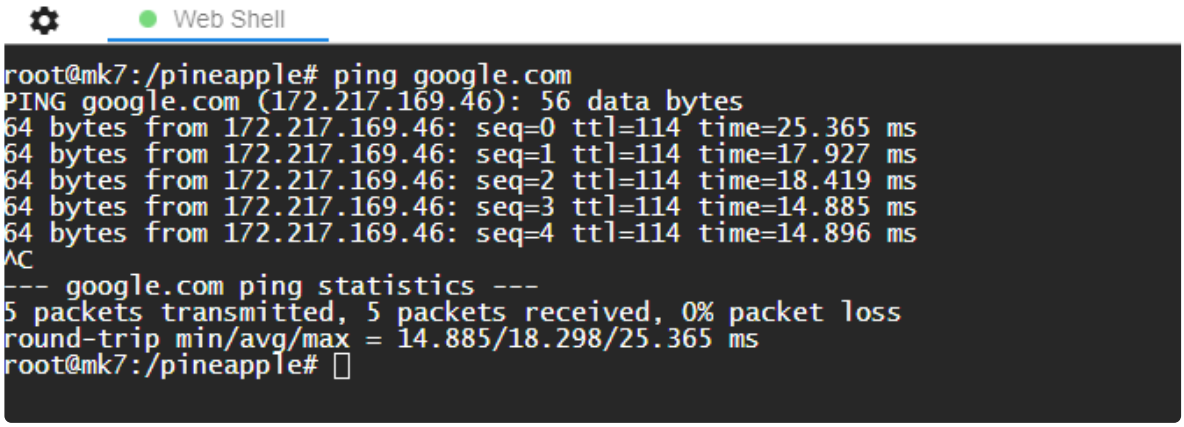
Finally, set the adapters IP settings as follows:

- 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**



> 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.



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 7

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.

Factory Reset and Recovery

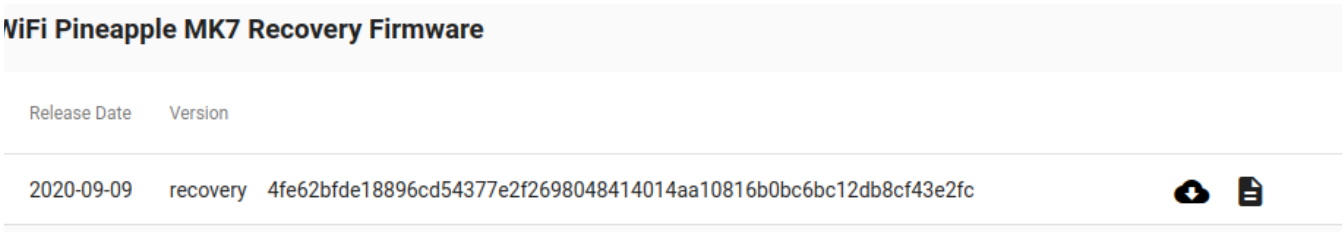
To restore your WiFi Pineapple back to a factory state, or to recover from a bad configuration, you can perform a **Firmware Recovery**.

The firmware recovery method consists of using the device bootloader to flash the stager.

Video Tutorial

Preparation

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



Once it's downloaded, verify the SHA256 sum of the downloaded file, **hold down the reset button while applying power** to the WiFi Pineapple. On the WiFi Pineapple Mark 7, the LED will flash red, on the WiFi Pineapple Mark 7 Enterprise, the system LED will flash blue.

After a few seconds of the flashing LED, **let go of the reset button** and continue to the next step.

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.

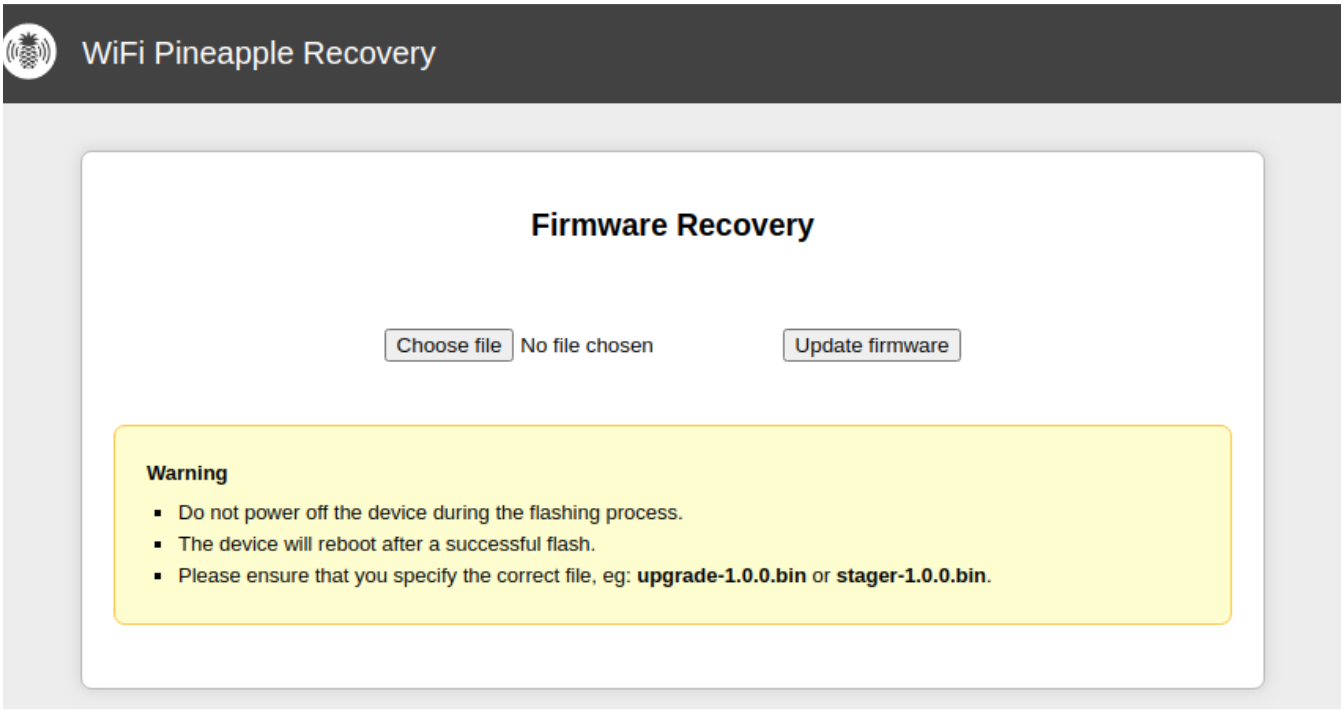
Windows

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 Stager 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**.



Select **Choose file** and then select the downloaded stager file from earlier. After clicking **Update firmware**, the device will begin flashing.

> ⚠ **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.

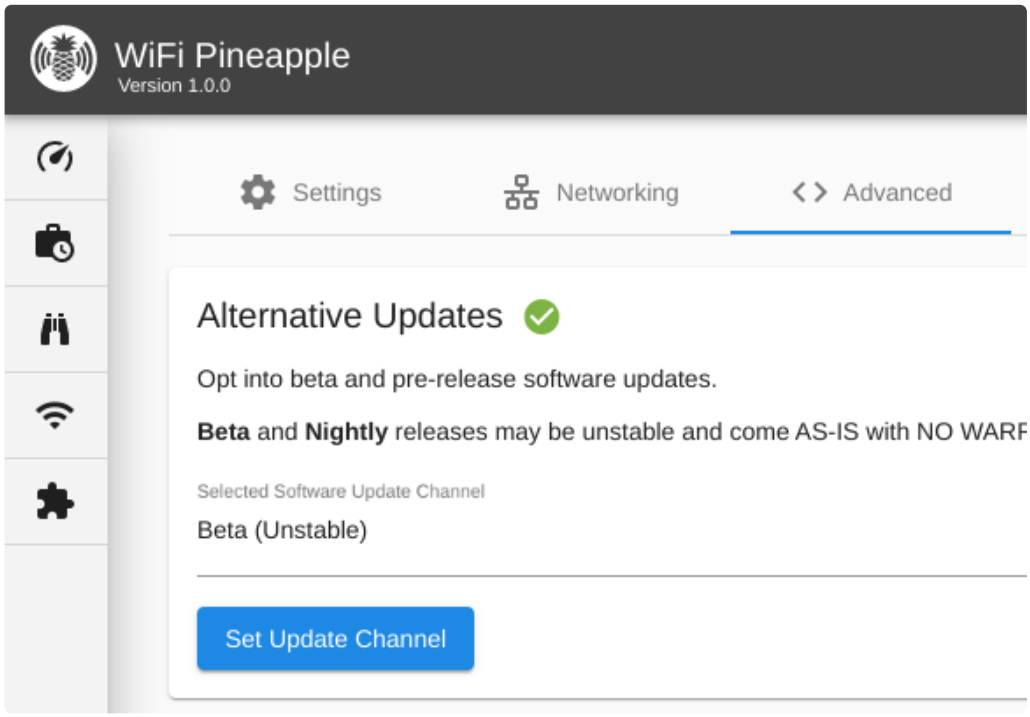
WiFi Pineapple Beta Updates

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:

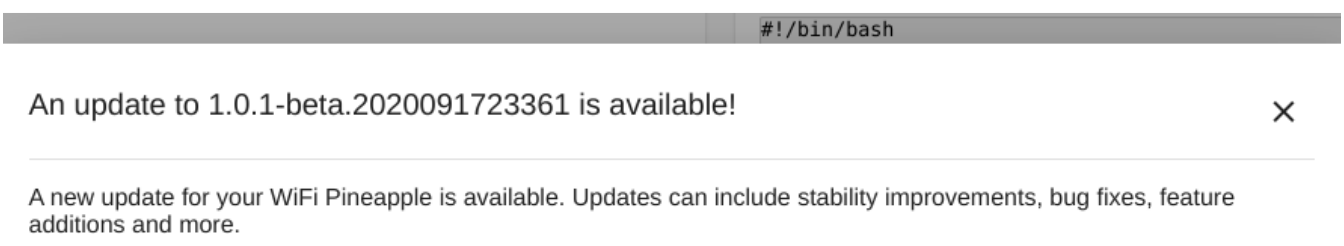
- **Stable**
- **Beta** - Pre-release updates that may be unstable, but may also contain new bug fixes, features and more.

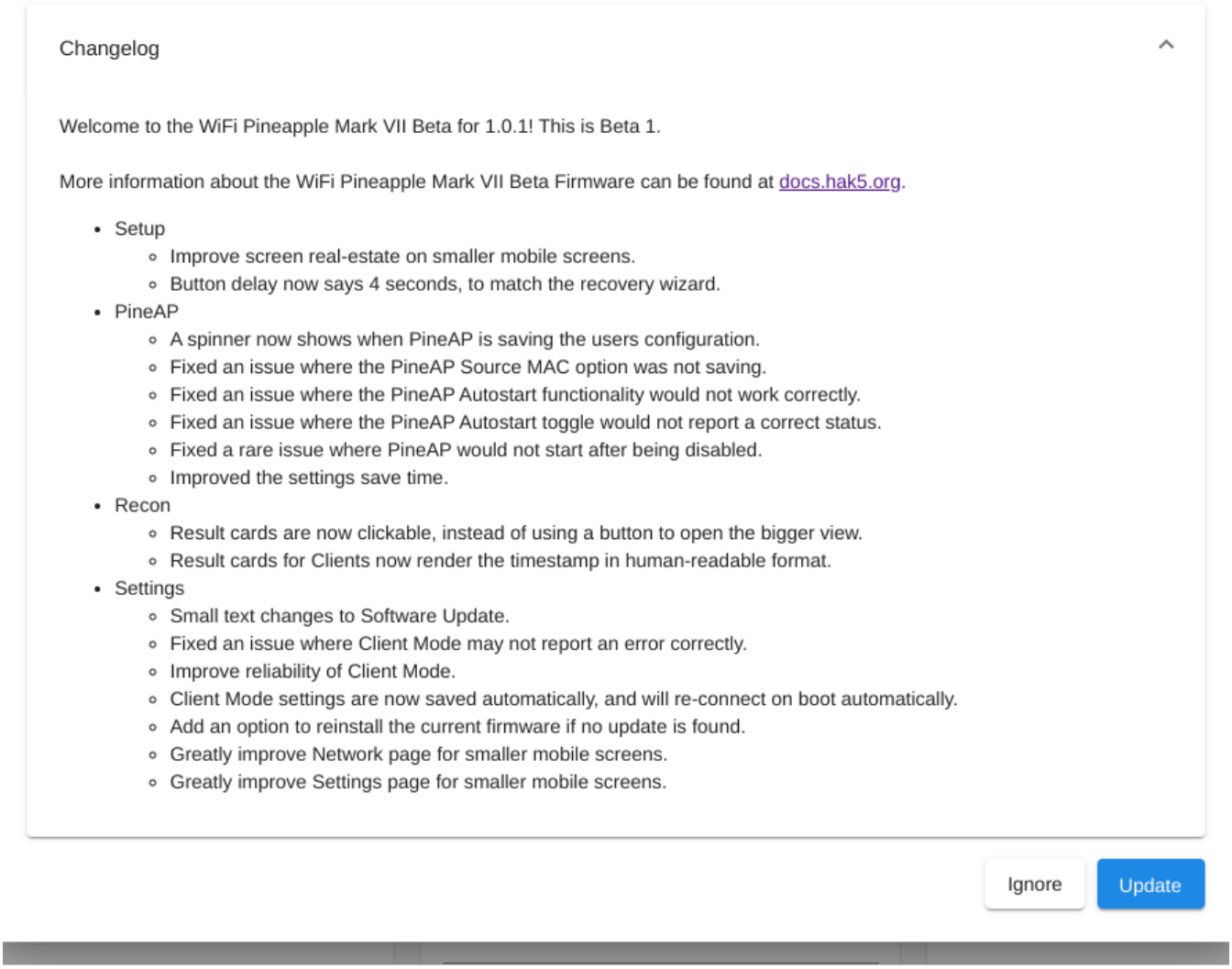
To manage your selected update channel, go to **Settings > Advanced** in the Web Interface.



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.





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 Adaptors

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 adaptor.

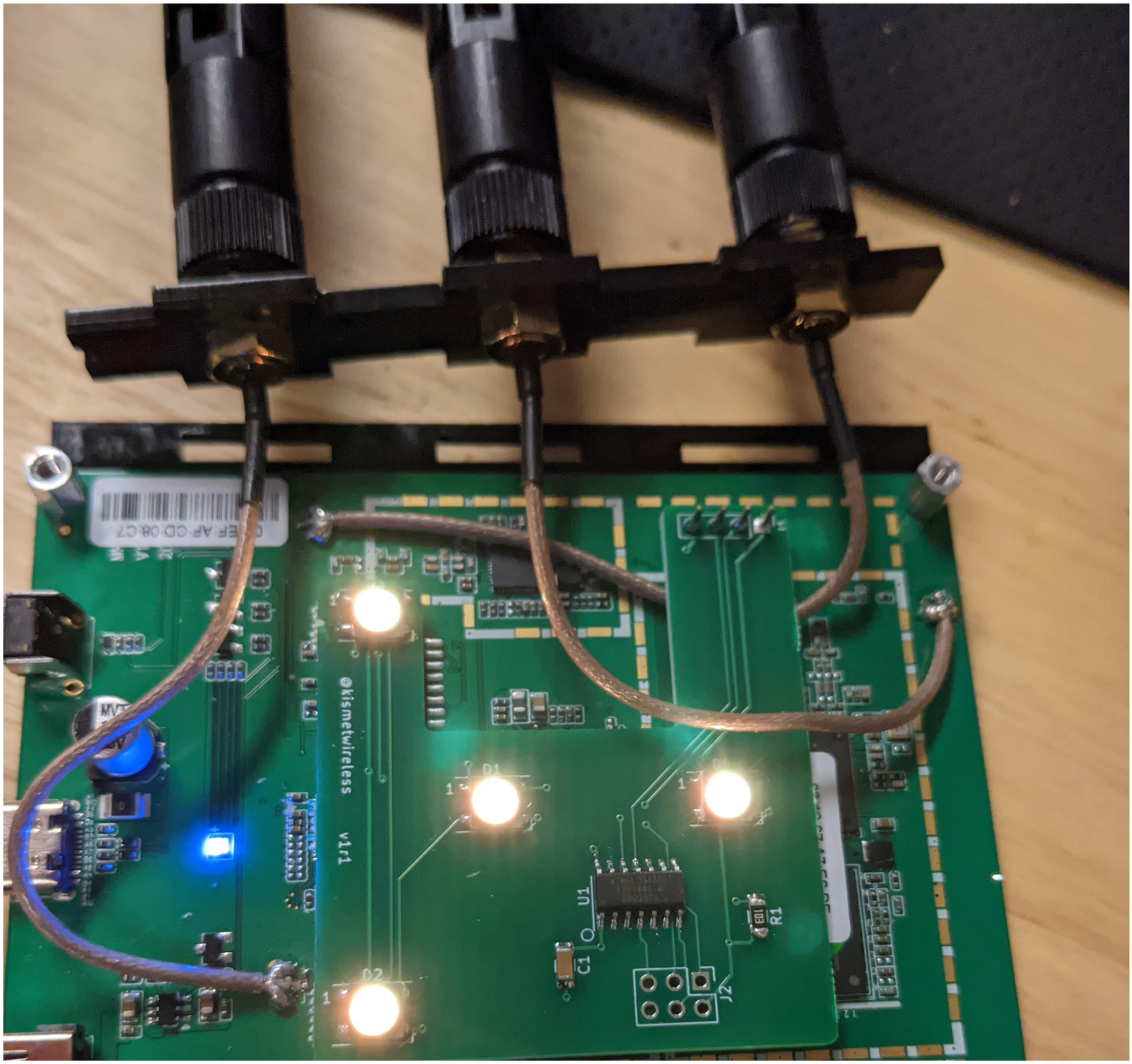
More information about your specific adaptor can usually found with resources such as WikiDevi.

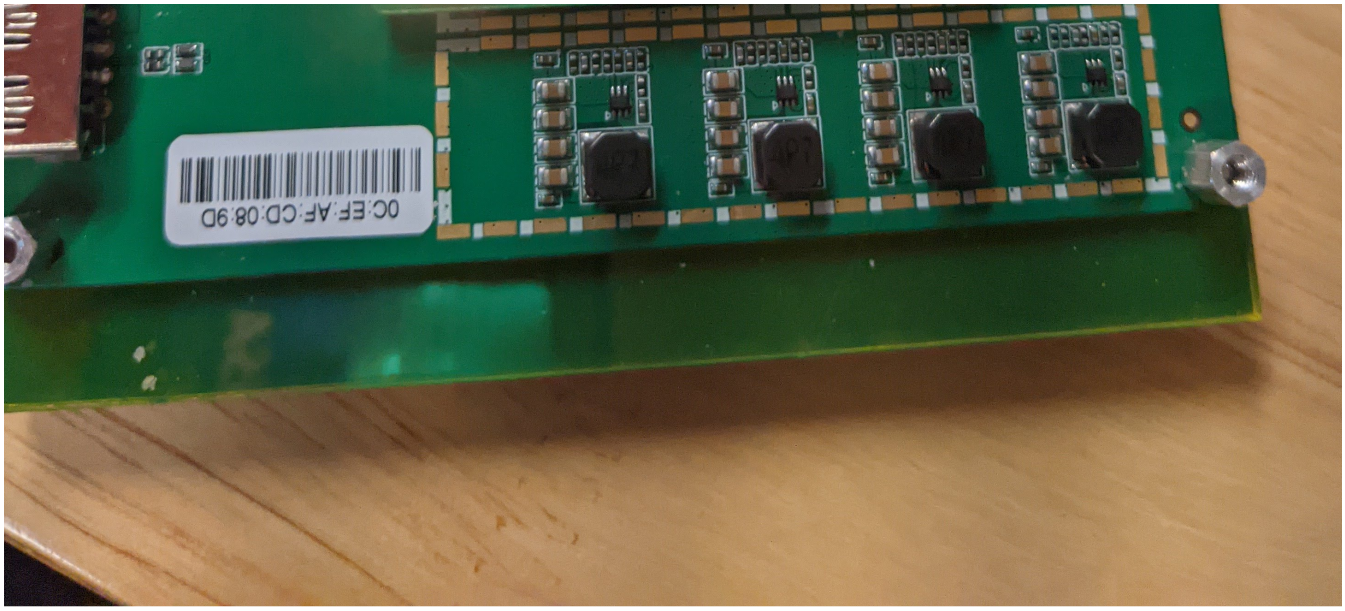
Extras

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/.





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/.