Infinite 110
Wireless Router
User Manual

Table of Contents

Table of Contents **1**
Introduction **2**
Document Purpose **2**
Connect to Access Point Web UI 3
Features of Access Point Web UI **5**
Status **6**
Overview 6
Routes 9
Real-Time Graphs 11
System **12**
System 13
Administration 15
Backup/Flash Firmware 17
Reboot 19
Network **19**
Interfaces 20
Wifi 21
DHCP and DNS 22
Hostnames 24
Static Routes 25
Firewall 26
Diagnostics 28
Smart Queue Management 29
SNMPD 32

Introduction

Welcome to the user manual for the Infinite 110 Access Point Local UI. This user interface provides a local access point for configuring and managing the settings of your Infinite cloud controller. It allows you to make specific configurations directly on the access point itself, ensuring that the applied changes are only relevant to the access point being configured.

With the Infinite Access Point Local UI, you can access a range of configuration options that are specific to the access point. This includes network settings, security configurations, wireless settings, and various other parameters that enable you to tailor the functionality of the access point to your specific requirements.

It's important to note that the configurations made within the Local UI will only affect the access point being configured. This means that any changes you make will not impact other access points or the overall cloud controller system.

In this user manual, we will guide you through the various features and settings available within the Infinite Access Point Local UI. You will learn how to navigate the interface, configure network settings, manage wireless networks, and perform advanced tasks such as creating VLANs and implementing security measures.

Here are a few typical elements you might see on the user interface of a specific WiFi access point:

- **Status/Dashboard**: Displays fundamental data such as uptime, clients connected, bandwidth usage, RF levels, etc.
- **Configuration**: Network settings like SSID, security, VLANs, bandwidth limits, and fundamental RF tuning comprise configuration.
- **Administration**: Information about the device, the software version, and system logs for troubleshooting.
- **Management**: Integration of a cloud-based or on-premises controller for centralized management.
- **Connected Devices**: Lists every client that is connected, with the option to block or isolate devices.
- **Advanced Settings**: Extensive RF options, including transmit settings and channel/power selection.
- **Upgrade**: The capacity to search for and set up local or remote sources of firmware updates.

We hope this user manual will provide you with the necessary knowledge and instructions to effectively use the Infinite 110 Local UI and optimize the performance of your access points. Let's get started!

Document Purpose

This comprehensive guide is designed to provide you with detailed instructions and insights on effectively utilising the local (UI) of your access points. Within this user manual, we will explore the various tabs and functionalities available through the web UI, including Status, System, and Network.

- **Status**: The **Status** tab provides real-time information about your access point's current operating status and performance. You can view essential details such as the device's uptime, firmware version, connected clients, signal strength, and other key metrics. This tab offers valuable insights into the health and functionality of your access point, enabling you to monitor and troubleshoot issues efficiently.
- The **System** tab allows you to configure and manage settings related to the overall system and operation of your access point. You can customise administrative options, device reboot schedules, system logs, and authentication methods from here. This tab empowers you to tailor the access point's behaviour to suit your specific requirements and maintain optimal performance.
- The **Network** tab is a crucial section that allows you to manage network-specific settings and configurations for your access point. Here, you can set up wireless network parameters, such as SSIDs (Service Set Identifiers), security protocols, access controls, VLAN (Virtual Local Area Network) settings, and more. This tab provides you with the flexibility to design and control your network to maximise efficiency and security.

Throughout this user manual, we will provide step-by-step instructions, accompanied by relevant screenshots and explanations, to guide you through each tab and its associated functionalities. Whether you are a network administrator or an individual user, this manual aims to equip you with the knowledge and tools to navigate the access point web UI with ease and confidence.

With a comprehensive understanding of the access point web UI, you will be able to effectively monitor your access points' status, optimise system performance, and customise network settings according to your unique requirements.

Connect to Access Point Web UI

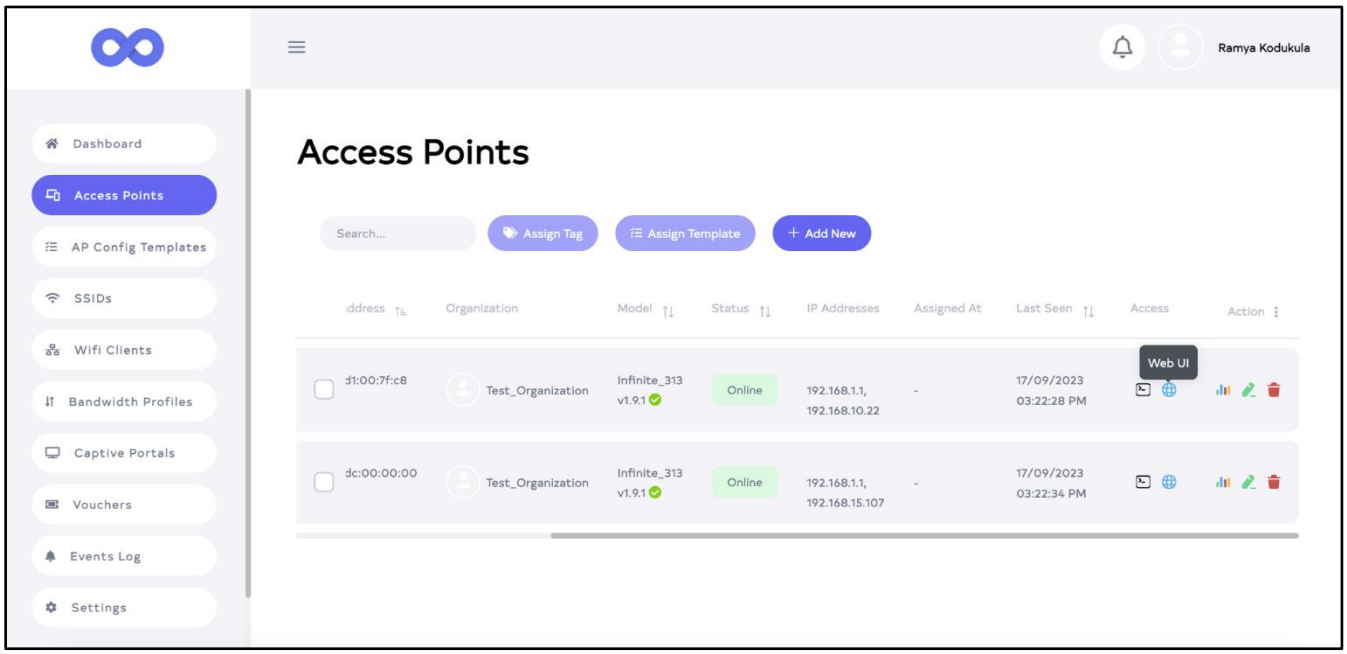
This user manual section will walk you through the steps required to access the Access Point Web UI. There are two methods for connecting to the local UI:

Step 1: Accessing Locally:

1. Connect a LAN cable from your computer to the access point's LAN interface.
2. Set your laptop's IP address to 192.168.1.x range. Ensure that the IP address is manually assigned rather than obtained via DHCP.
3. Open your preferred web browser and type the following address: **192.168.1.1**. You'll be taken to the local UI login page.
4. Enter "**Root**" as the username and "**gwcadmin**" as the password. You will have access to the local UI and its various settings and configurations once you have been authenticated.

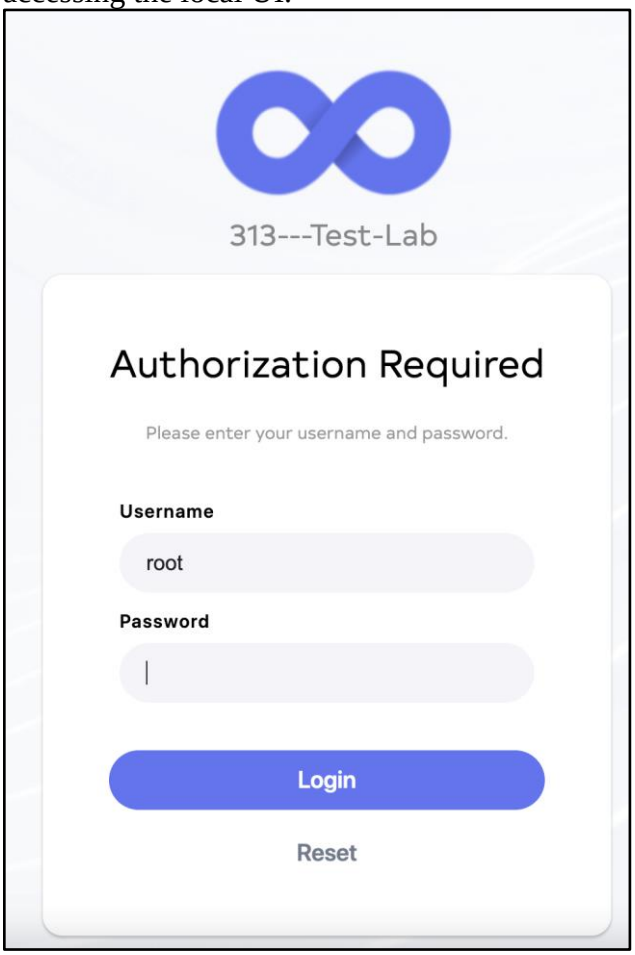
Step 2: Using the Infinite Cloud Controller to gain access

1. Log in to the Infinite Cloud Controller using your login credentials.
2. Select the specific access point you want to manage. With the access point's details, click on the "**Local UI**" tab.



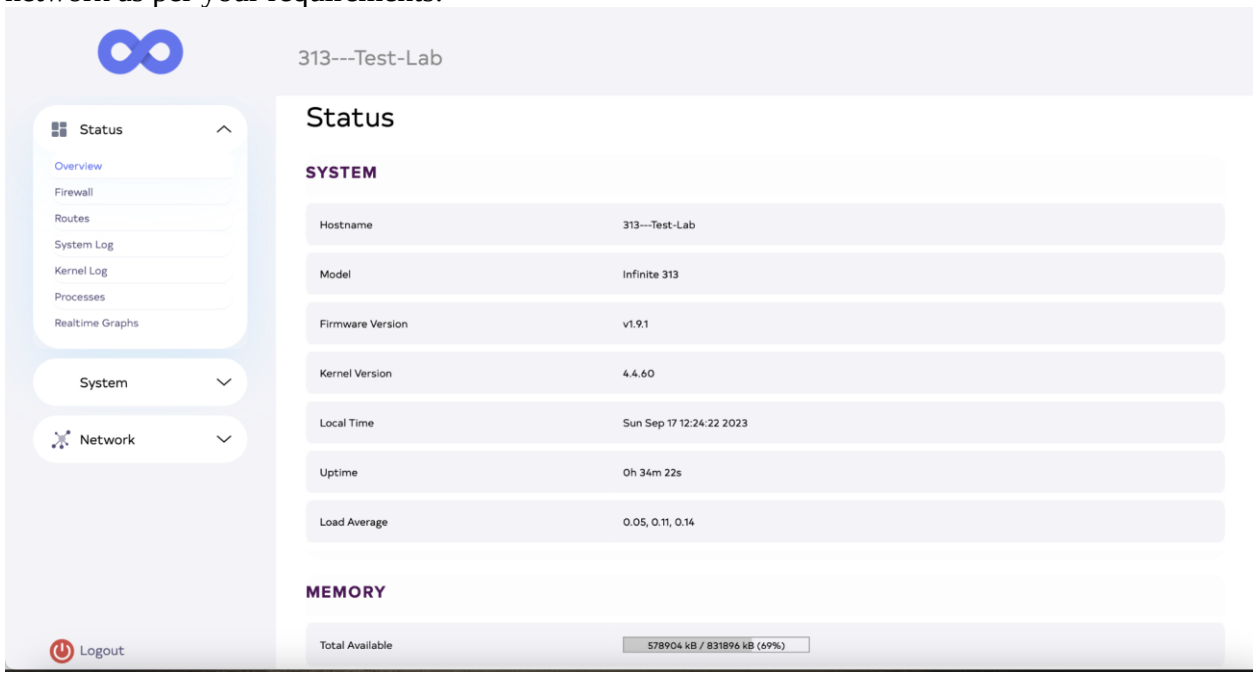
3. The browser will automatically redirect you to the local UI of the selected access point.

4. Enter the username and password if prompted, following the provided credentials for accessing the local UI.



5. By following these steps, you will be able to connect to the Access Point Web UI locally or through the Infinite Cloud Controller interface. Once connected, you can explore and configure different settings, monitor the access point's performance, and manage your

network as per your requirements.



Features of Access Point Web UI

Once you log in, you will be redirected to the Initial Setup Wizard landing page. This main dashboard has the following features:

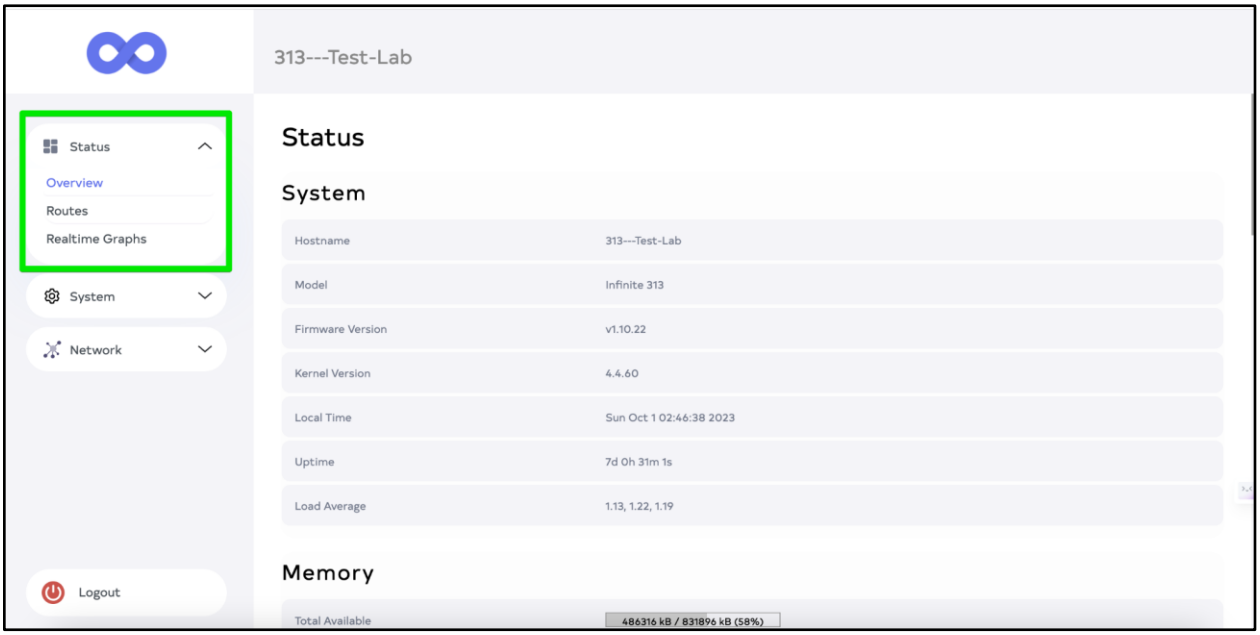
- **Status**: The **Status** tab provides real-time information about your access point's current operating quality and performance.
- **System**: The **System** tab allows you to configure and manage settings related to the overall system and operation of your access point.
- **Network**: The **Network** tab is a crucial section that allows you to manage network-specific settings and configurations for your access point.

Let us understand each one of them in detail.

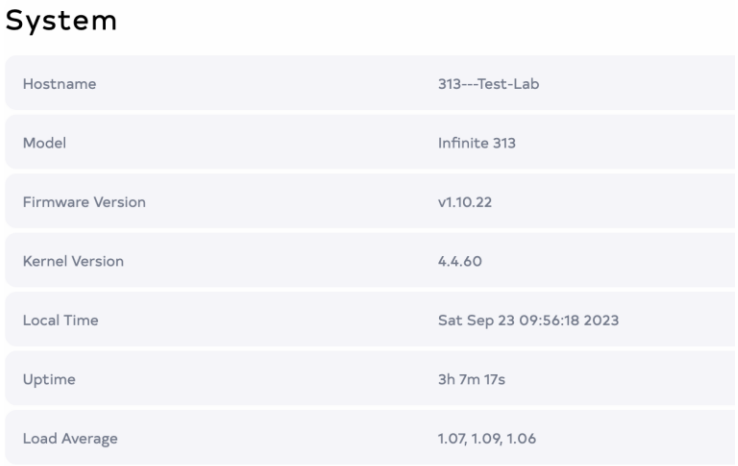
Status

Overview

Click on the **Overview** section of the **Status** tab to understand the point's system requirements, memory, network status, DHCP leases, DHCPv6 leases, wireless information, and associated stations.

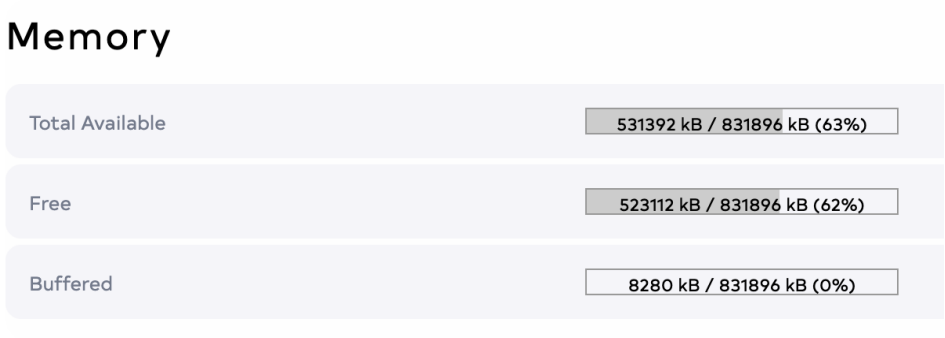


- **System**: This section displays key system information such as the access point's firmware version, hardware model, uptime (the time the access point has been running since the last reboot), and MAC address. It provides an overview of the access point's general status and identification details.

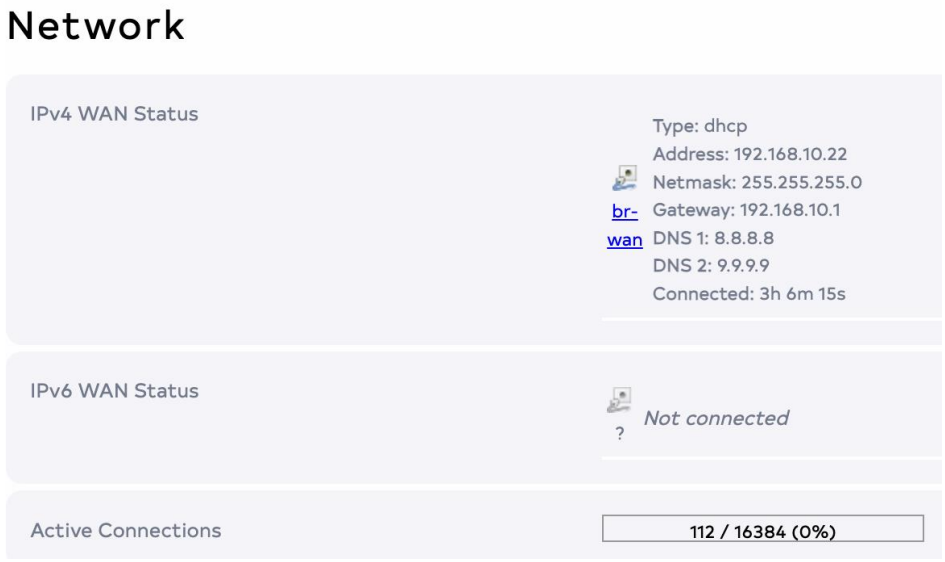


- **Memory**: The Memory section shows the usage of system memory, including details on the total memory available and the memory currently in use. It helps you monitor the

memory usage of the access point and identify any potential issues related to memory resources.

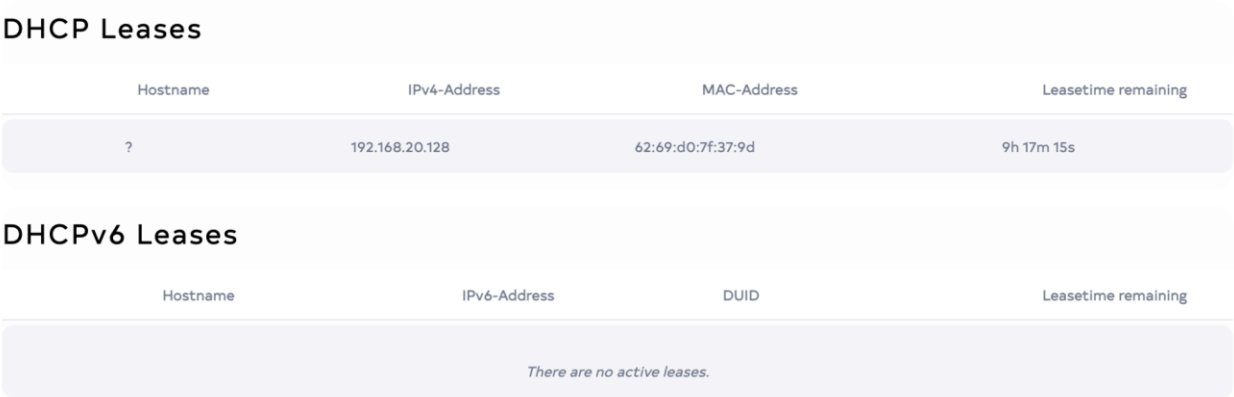


- **Network**: In this section, you can gather information about the access point's network configuration and connectivity. It displays details like the access point's IP address, subnet mask, default gateway, and DNS server addresses.



- **DHCP Leases**: This subsection provides an overview of the DHCP (Dynamic Host Configuration Protocol) leases issued by the access point. It shows information such as the IP address, MAC address, hostname, lease time, and lease expiration for each connected device. This data enables you to track and manage the devices that have

obtained IP addresses from the access point's DHCP server.



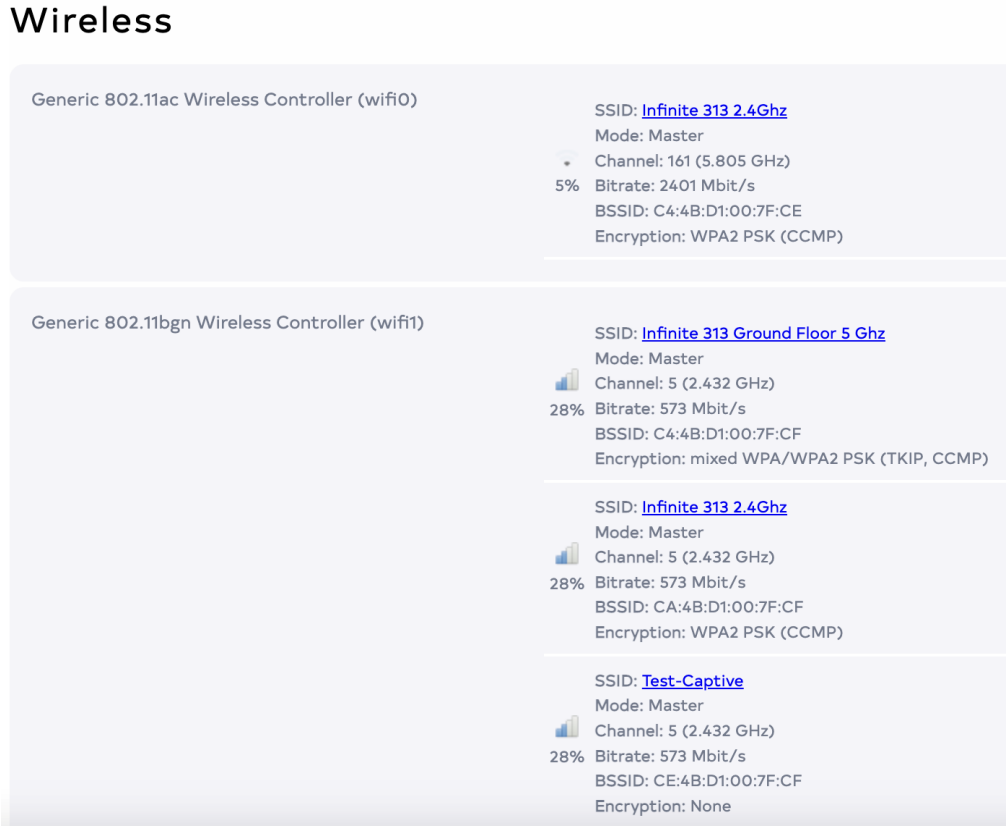
DHCP Leases

Hostname	IPv4-Address	MAC-Address	Leasetime remaining
?	192.168.20.128	62:69:d0:7f:37:9d	9h 17m 15s

DHCPv6 Leases

Hostname	IPv6-Address	DUID	Leasetime remaining
There are no active leases.			

- **DHCPv6 Leases**: Similar to DHCP leases, this subsection displays information about DHCPv6 (IPv6 version of DHCP) leases issued by the access point. It includes details such as the IPv6 address, DUID (DHCP Unique Identifier), IAID (Interface Association ID), lease time, and lease expiration for each connected device using IPv6.
- **Wireless Information**: This section includes details such as the SSID (Service Set Identifier), channel, signal strength, security type, encryption method, and number of associated clients. With this information, you can monitor the status and performance of the wireless networks and make necessary adjustments to optimise wireless connectivity.

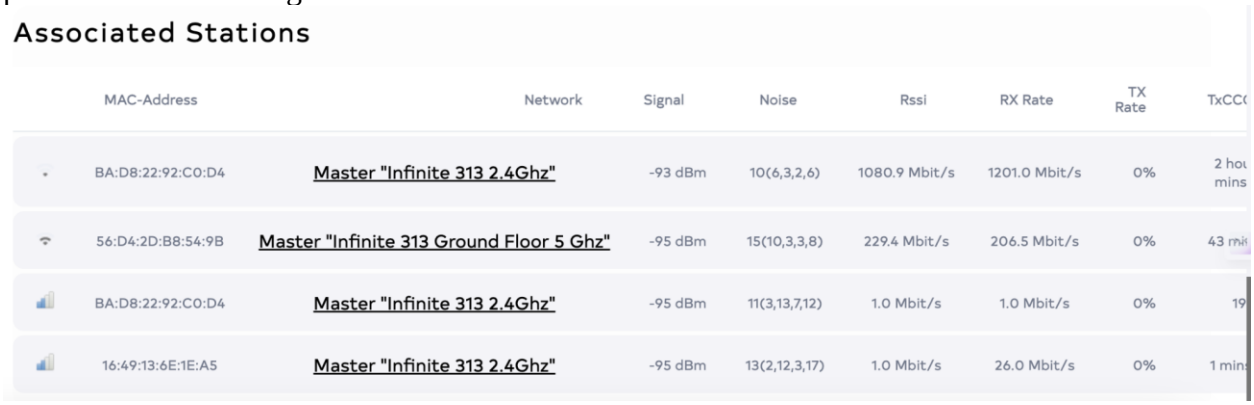


Wireless

Generic 802.11ac Wireless Controller (wifi0)	5%	SSID: Infinite 313 2.4Ghz Mode: Master Channel: 161 (5.805 GHz) Bitrate: 2401 Mbit/s BSSID: C4:4B:D1:00:7F:CE Encryption: WPA2 PSK (CCMP)
Generic 802.11bgn Wireless Controller (wifi1)	28%	SSID: Infinite 313 Ground Floor 5 Ghz Mode: Master Channel: 5 (2.432 GHz) Bitrate: 573 Mbit/s BSSID: C4:4B:D1:00:7F:CF Encryption: mixed WPA/WPA2 PSK (TKIP, CCMP)
	28%	SSID: Infinite 313 2.4Ghz Mode: Master Channel: 5 (2.432 GHz) Bitrate: 573 Mbit/s BSSID: CA:4B:D1:00:7F:CF Encryption: WPA2 PSK (CCMP)
	28%	SSID: Test-Captive Mode: Master Channel: 5 (2.432 GHz) Bitrate: 573 Mbit/s BSSID: CE:4B:D1:00:7F:CF Encryption: None

- **Associated Stations**: It shows information such as the MAC address, IP address (if assigned), signal strength, data rate, and activity status of each associated client. This

feature allows you to monitor the devices connected to your access point and identify any potential issues or irregularities.



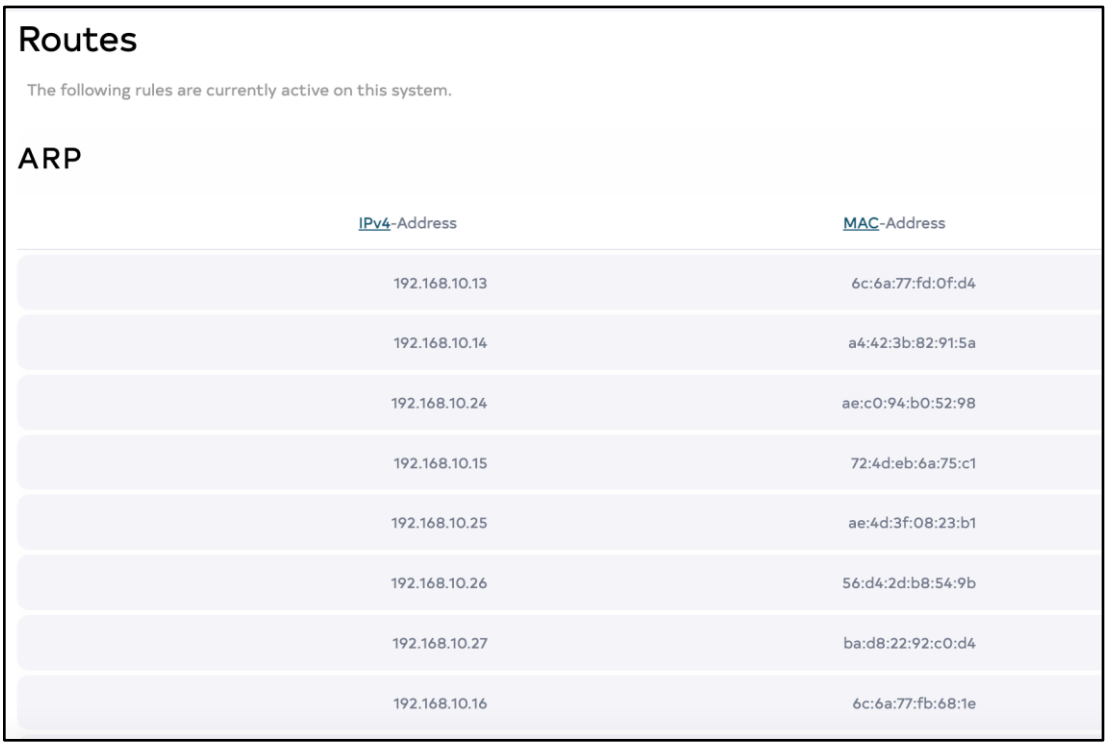
Associated Stations

MAC-Address	Network	Signal	Noise	Rssi	RX Rate	TX Rate	TxCC
BA:D8:22:92:C0:D4	Master "Infinite 313 2.4Ghz"	-93 dBm	10(6,3,2,6)	1080.9 Mbit/s	1201.0 Mbit/s	0%	2 hou mins
56:D4:2D:B8:54:9B	Master "Infinite 313 Ground Floor 5 Ghz"	-95 dBm	15(10,3,3,8)	229.4 Mbit/s	206.5 Mbit/s	0%	43 mi
BA:D8:22:92:C0:D4	Master "Infinite 313 2.4Ghz"	-95 dBm	11(3,13,7,12)	1.0 Mbit/s	1.0 Mbit/s	0%	19
16:49:13:6E:1E:A5	Master "Infinite 313 2.4Ghz"	-95 dBm	13(2,12,3,17)	1.0 Mbit/s	26.0 Mbit/s	0%	1 min

Routes

The Routes Tab in the Access Point Web UI provides a comprehensive overview of the active routes on the system. It includes the following route types:

- **ARP (Address Resolution Protocol)**: The ARP section displays the current ARP entries in the access point. ARP is used to map an IP address to a corresponding MAC address. It allows devices to communicate with each other over an Ethernet network.



Routes

The following rules are currently active on this system.

ARP

IPv4-Address	MAC-Address
192.168.10.13	6c:6a:77:fd:0f:d4
192.168.10.14	a4:42:3b:82:91:5a
192.168.10.24	ae:c0:94:b0:52:98
192.168.10.15	72:4d:eb:6a:75:c1
192.168.10.25	ae:4d:3f:08:23:b1
192.168.10.26	56:d4:2d:b8:54:9b
192.168.10.27	ba:d8:22:92:c0:d4
192.168.10.16	6c:6a:77:fb:68:1e

- **Active IPv4-Routes**: The Active IPv4-Routes section shows the active IPv4 routing entries in the access point. These routes define how network traffic is directed between different IP addresses or subnets, ensuring efficient data transmission within the network.

Active IPv4-Routes

Network	Target
wan	0.0.0.0/0
lan	192.168.1.0/24
wan	192.168.10.0/24
wan	192.168.10.1

- **Active IPv6-Routes**: The Active IPv6-Routes section displays the active IPv6 routing entries in the access point. Similar to IPv4 routes, IPv6 routes define how network traffic is routed between different IPv6 addresses or subnets.

Active IPv6-Routes

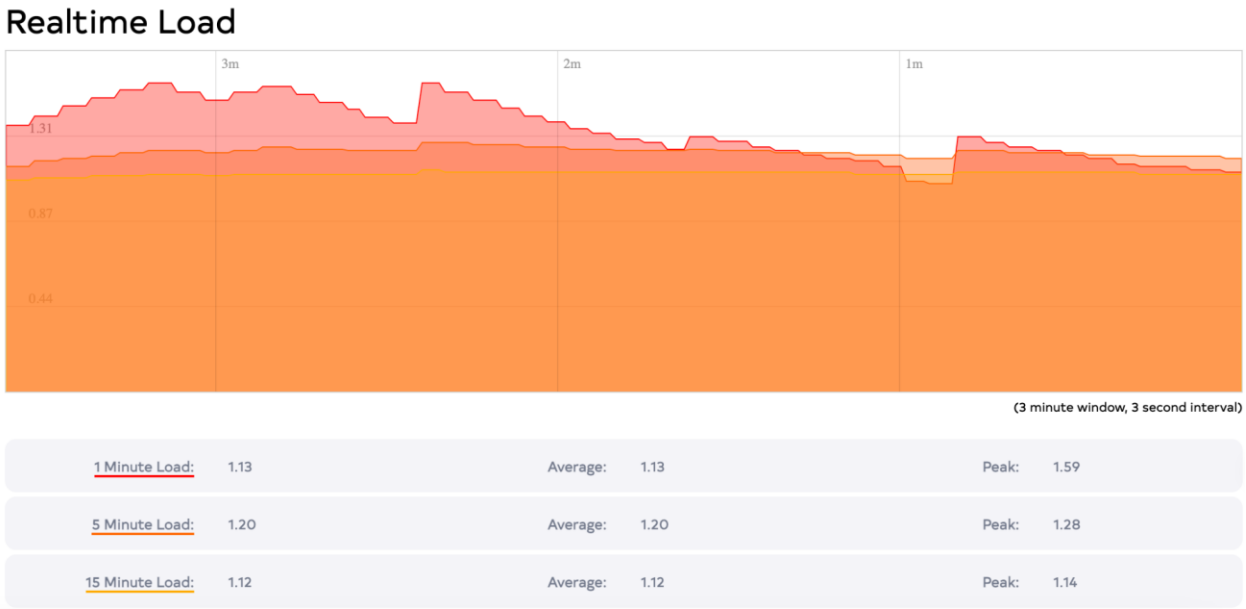
Network	Target
lan	ff00::/8
wan	ff00::/8
wan	ff00::/8
wan	ff00::/8
wan	ff00::/8
wan	ff00::/8

- I**Pv6 Neighbours**: The IPv6 Neighbours section provides information about the neighbouring devices in the IPv6 network. It shows the MAC address and IP address of the neighbouring devices to facilitate communication and ensure the smooth functioning of the network.

Real-Time Graphs

Within the Access Point Web UI, one of the notable features is the Real Time Graphs page. This page is designed to provide users with real-time graphical representations of various statistical data changes, allowing for quick monitoring and analysis.

Realtime Load: The Real Time Load section displays a tri-graph that provides insights into the average CPU load values in real-time. This graph consists of three colour-coded lines, each corresponding to the average CPU load over different time frames. The red line represents the average CPU load over the last minute, the orange line represents the average load over the past 5 minutes, and the yellow line represents the average load over the past 15 minutes. By observing these lines, you can assess the current and historical CPU load patterns of the access point.

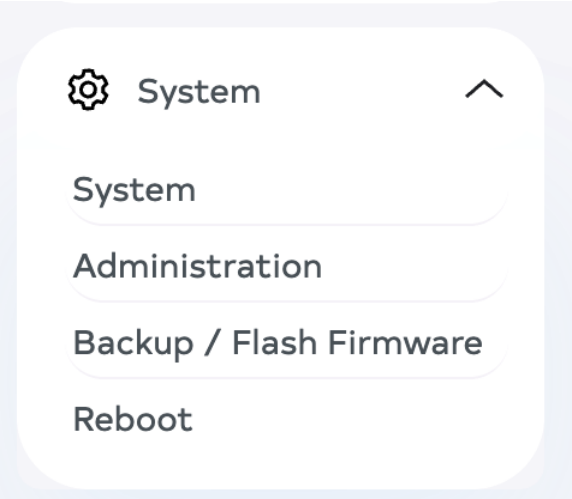


System

The System tab acts as a central hub for managing and configuring various aspects of your access point within the Access Point Web UI. You can adjust a variety of settings and options on this tab to alter the operation, conduct, and management of your access point.

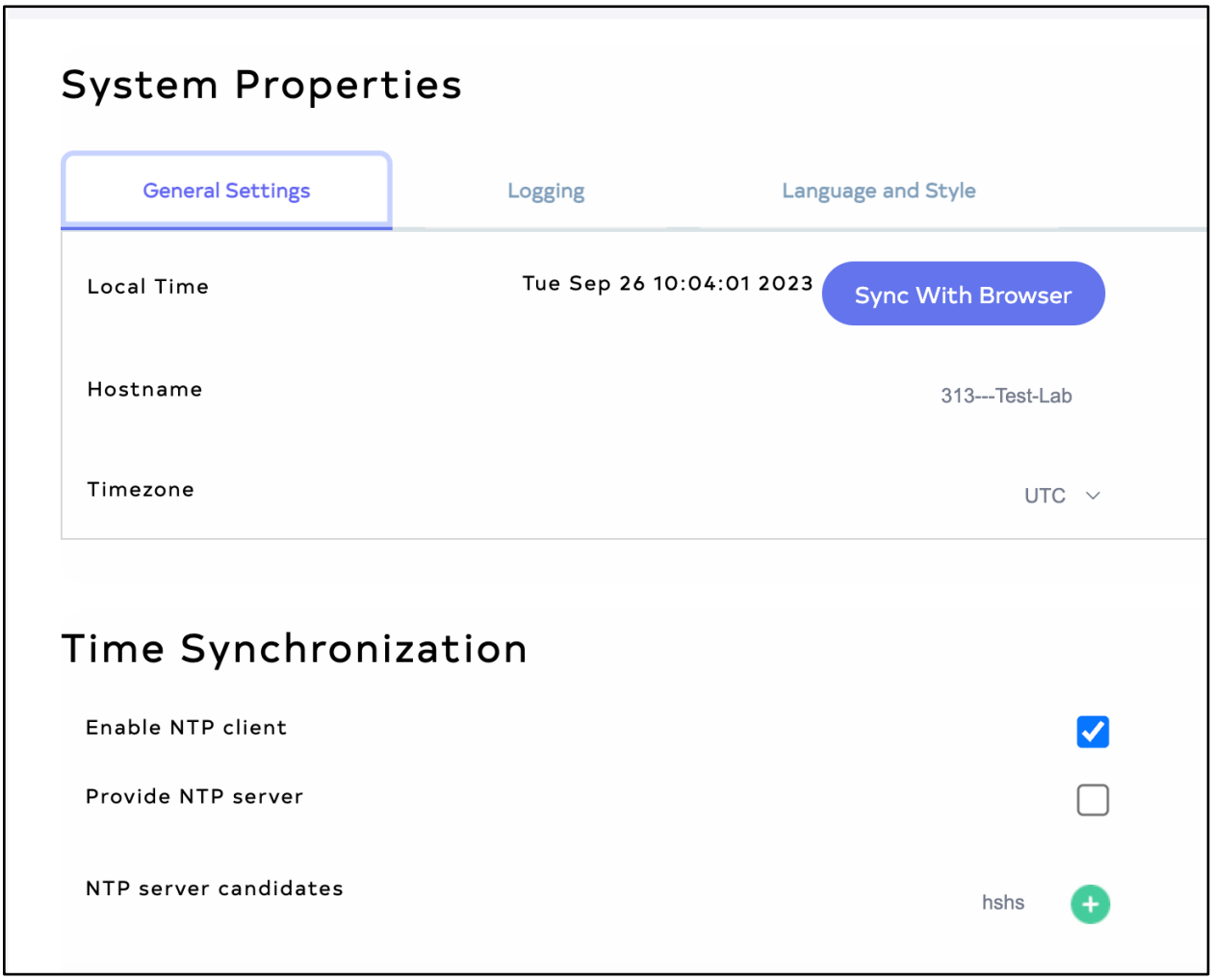
By giving you the ability to manage system-level configurations, carry out administrative functions, backup and update firmware, and start reboots when necessary, the System tab enables you to guarantee the smooth and effective operation of your access point. You can keep command over essential facets of your access point's operation by going to the System tab.

We will examine the Administration, Backup/Flash Firmware, and Reboot subsections under the System tab in the sections that follow.



System

General Properties: Click on this tab to configure the basic aspects of the device, like its hostname or the time zone.

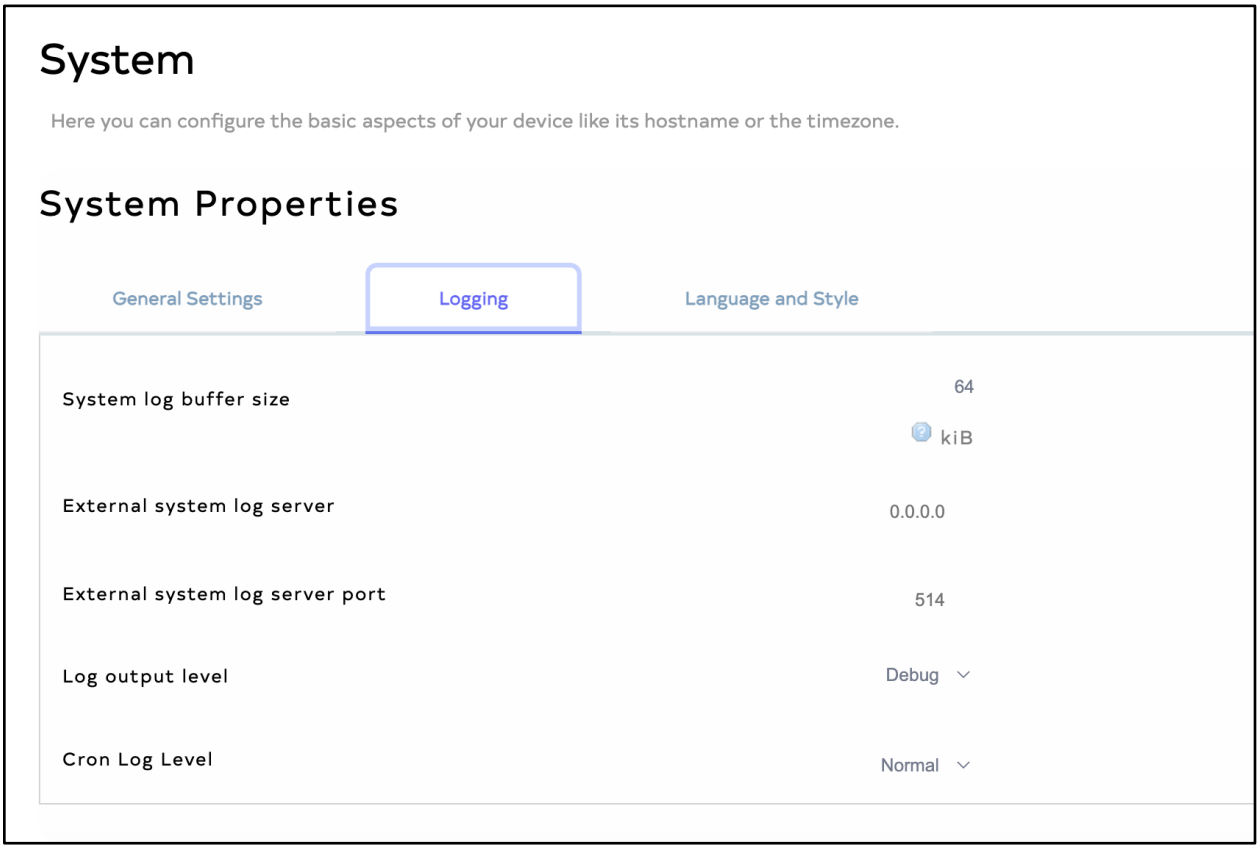


Time Synchronisation: One of the essential features of the Access Point Web UI is the ability to synchronise the access point's time with a trusted time source. This ensures that the access point has accurate time information, which is important for various network operations and security protocols.

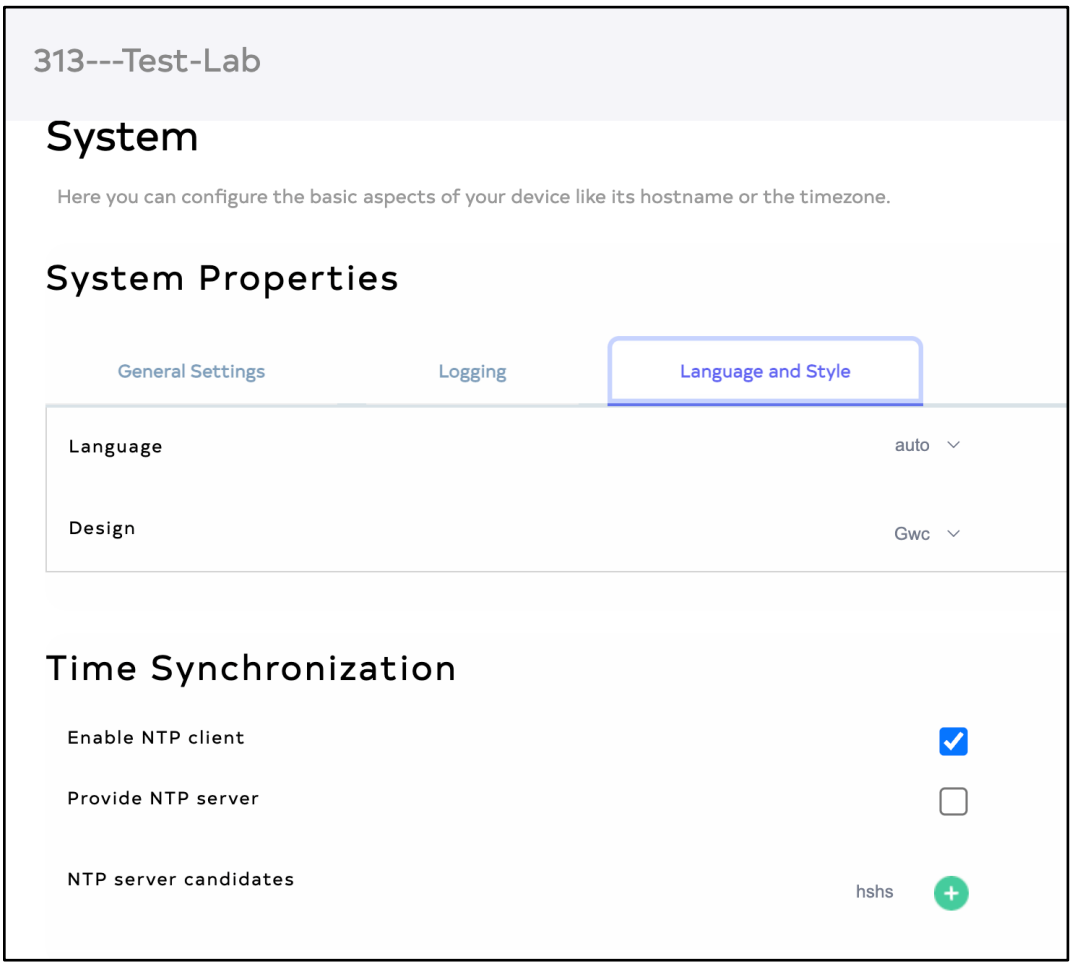
1. **Enable NTP Client**: Click on this checkbox to enable the NTP client to automatically synchronise its time with an NTP server.
2. **Provide NTP Server**: To configure time synchronisation through the Access Point Web UI, click on the NTP server checkbox.
3. **NTP Server Candidates**: Click on the plus button to add an NTP Server Candidate.

Logging Tab: The Logging tab provides settings related to system logging. Within this tab, you can configure the following properties:

1. **System Log Buffer Size**: This property determines the size of the system log buffer in kilobytes (kB). The value provided here is 64 kB, indicating the allocated buffer size for storing system logs.
2. **Help KiB**: This property refers to the amount of help information stored in kilobytes (kB). It specifies the available capacity for storing help-related documents or resources.
3. **External System Log Server**: This property allows you to specify the IP address of an external system log server. If configured, access point system logs can be sent to this server for centralised log management and analysis.
4. **Log Output Level**: This property determines the verbosity level of the access point's system logs. The available options usually include "Debug," "Info," "Warning," or "Error." The selected level determines the level of detail included in the logs.
5. **Cron Log Level**: This property determines the logging level for system cron jobs. Cron jobs are scheduled tasks that run periodically on the access point.



Language and Style: Click on this tab to set the language and design for the access point web UI.

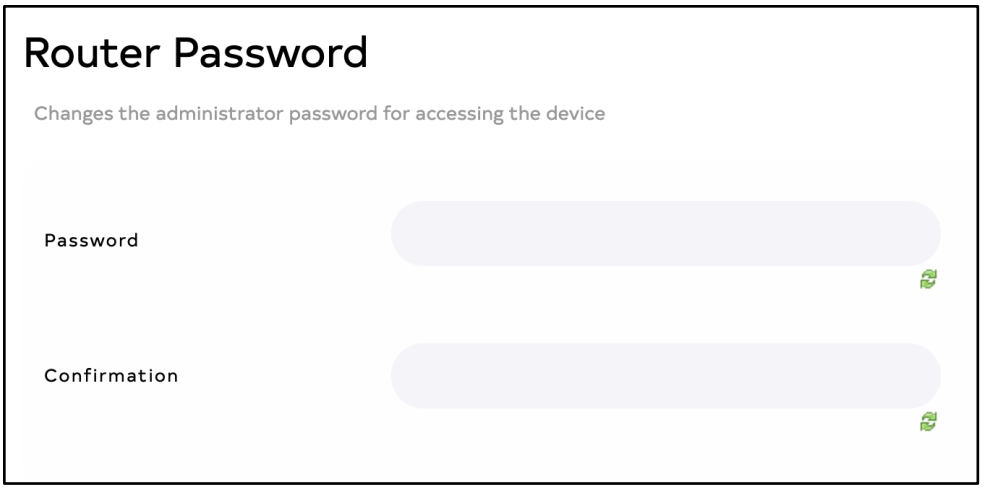


Administration

The Administration tab is a crucial section of the access point web UI, providing access to various settings and configurations for administrative purposes.
The Access Point Web UI supports SSH (Secure Shell) network shell access, allowing secure remote management and configuration through the command line. Additionally, it offers an integrated SCP (Secure Copy) server for secure file transfers to and from the access point.

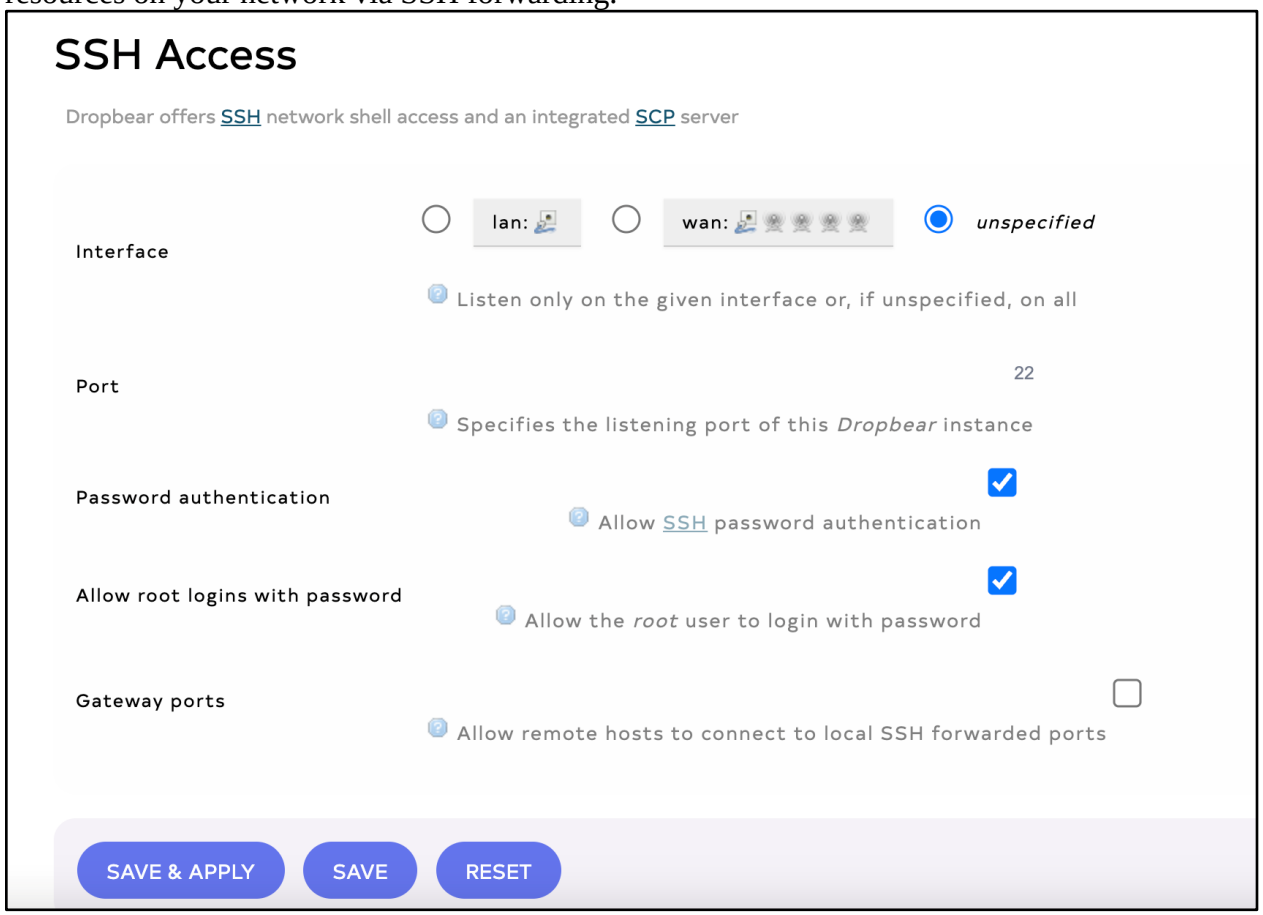
Now let us understand the various sections of this screen.

- **Router Password**: Enter the administrator password for accessing the device.



- **Interface**: Click one of the checkboxes to select different network interfaces available on the access point, including LAN and WAN interfaces.
- **Port**: This specifies the listening port of the Dropbear SSH instance. The default SSH port is set to 22, but you can modify it according to your requirements.
- **Password Authentication**: Select the checkbox to allow SSH password authentication. This option determines whether you can authenticate yourself using a password when connecting via SSH.
- **Allow Root Logins with Password**: Select the checkbox to enable the root user to log in with a password. This authentication method provides root-level access to the access point.
- **Gateway Ports**: Select this option to enable the ability for remote hosts to connect to local SSH forwarded ports. Enabling gateway ports allows external hosts to access

resources on your network via SSH forwarding.

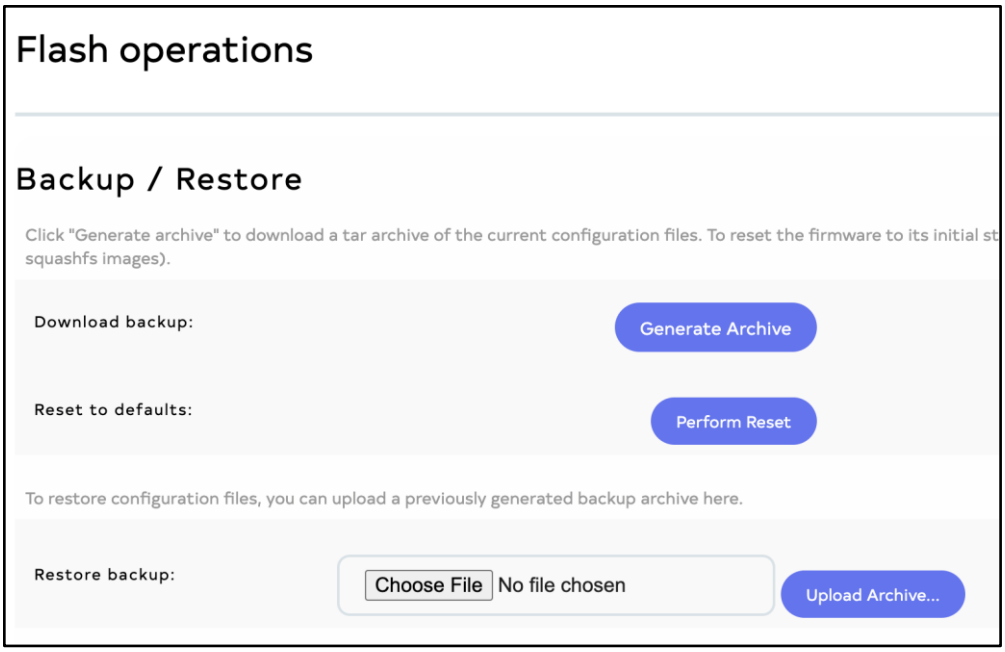


Backup/Flash Firmware

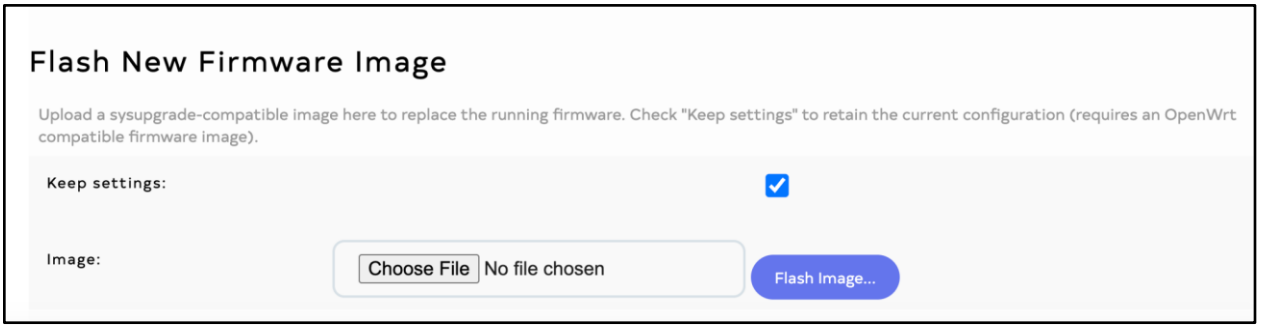
This section is designed to provide you with convenient methods to backup, restore, and manage firmware on your access point, ensuring smooth and efficient network operations.

Now let us understand the various sections of this screen.

- **Backup/Restore**: Click **Generate Archive** to download a tar archive of the current configuration files. To reset the firmware to its initial state, click **Perform Reset**. To restore configuration files, upload the previously generated backup archive and click **Upload Archive**.

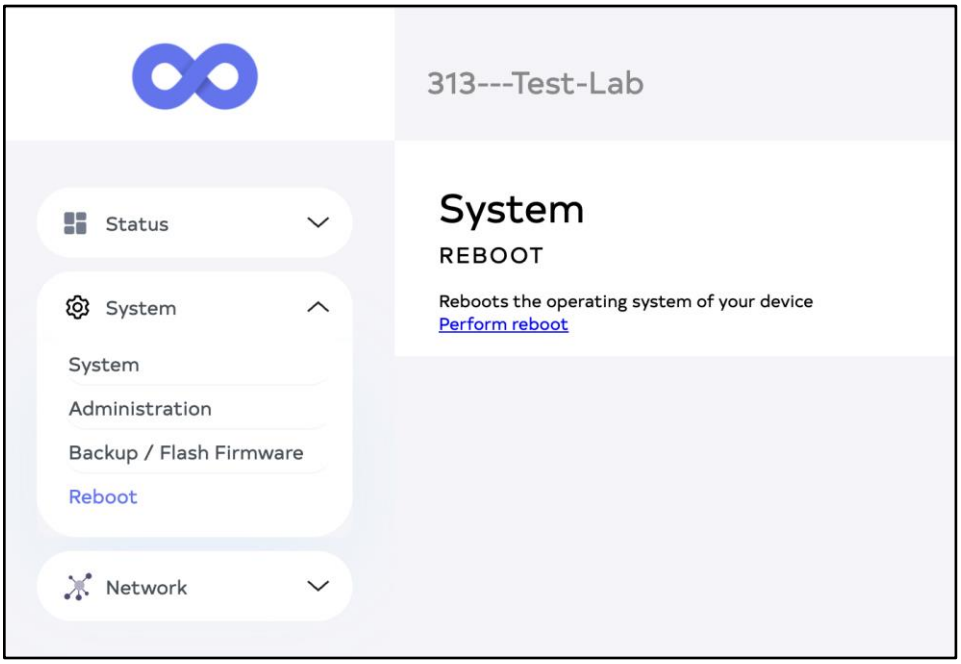


- **Flash New Firmware Image**: The web UI provides the functionality to flash new firmware onto your access point. You can upload a sysupgrade-compatible firmware image to replace the existing firmware. Select the **Keep settings** checkbox to retain the current configuration when applying the new firmware image.



Reboot

Click **Perform Reboot** to reboot the operating system of your device.



Network

The Network section within the Access Point Web UI is a vital part of managing and configuring your network settings. It gives you a centralised platform from which you can manage and alter different aspects of your network for optimum security and performance.

You can configure and manage wireless network parameters in the Network section, including SSIDs (Service Set Identifiers), security protocols like WPA2 or WPA3, access controls, and VLAN settings. With the help of these settings, you can establish multiple networks, divide user groups, and manage who has access to what resources or services.
Additionally, DHCP (Dynamic Host Configuration Protocol) settings, which enable automatic IP address assignment to connected devices on your network, can be configured in the Network section. If necessary, you can also specify static IP addresses for particular devices.

The network's Quality of Service (QoS) settings, which distribute network bandwidth and give traffic priority based on predefined rules, are also managed and controlled within this section. This improves network performance and guarantees that crucial applications or services get the necessary bandwidth.

Let's explore some of the key features.

Interfaces

The Interfaces section provides an overview of the network status for both the LAN and WAN interfaces. It includes information such as interface names, types, uptime, MAC addresses, data received and transmitted, and IPv4 addresses. These details are essential for understanding the current network configuration and monitoring network performance.

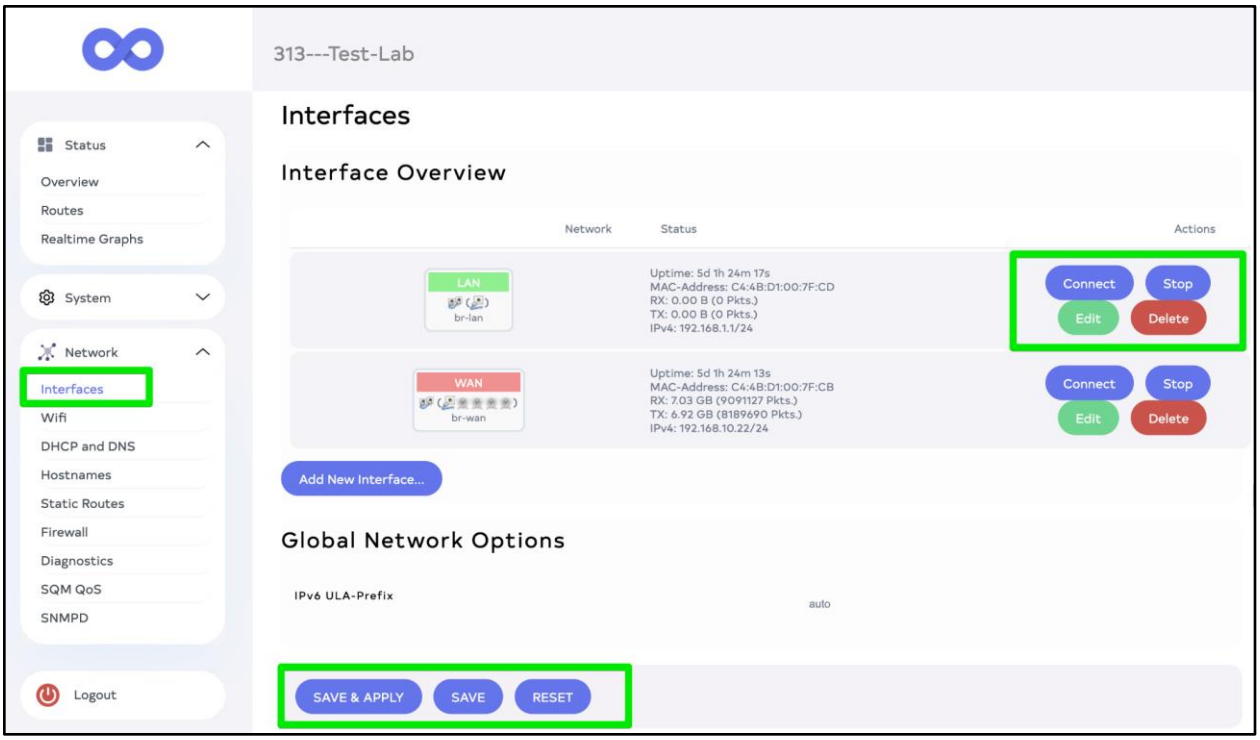
LAN/WAN Interface:

- **Network**: br-lan
- **Status**: The status of the LAN/WAN interface, such as uptime and connectivity.
- **Actions**: You can perform actions like connecting, stopping, editing, or deleting the LAN interface.
- **Uptime**: The duration the LAN interface has been active.
- **MAC Address**: The unique MAC address assigned to the LAN/WAN interface.
- **RX (Receive)**: Shows the amount of data (in bytes) and the number of packets received by the LAN/WAN interface.
- **TX (Transmit)**: Displays the amount of data (in bytes) and the number of packets transmitted by the LAN/WAN interface.
- **IPv4**: The IPv4 address and subnet mask assigned to the LAN/WAN interface.
- **Add New Interface**: Click on this button to add a new interface.

Global Network Options:

IPv6 ULA-Prefix: This option determines the IPv6 ULA (Unique Local Address) prefix used in the network.

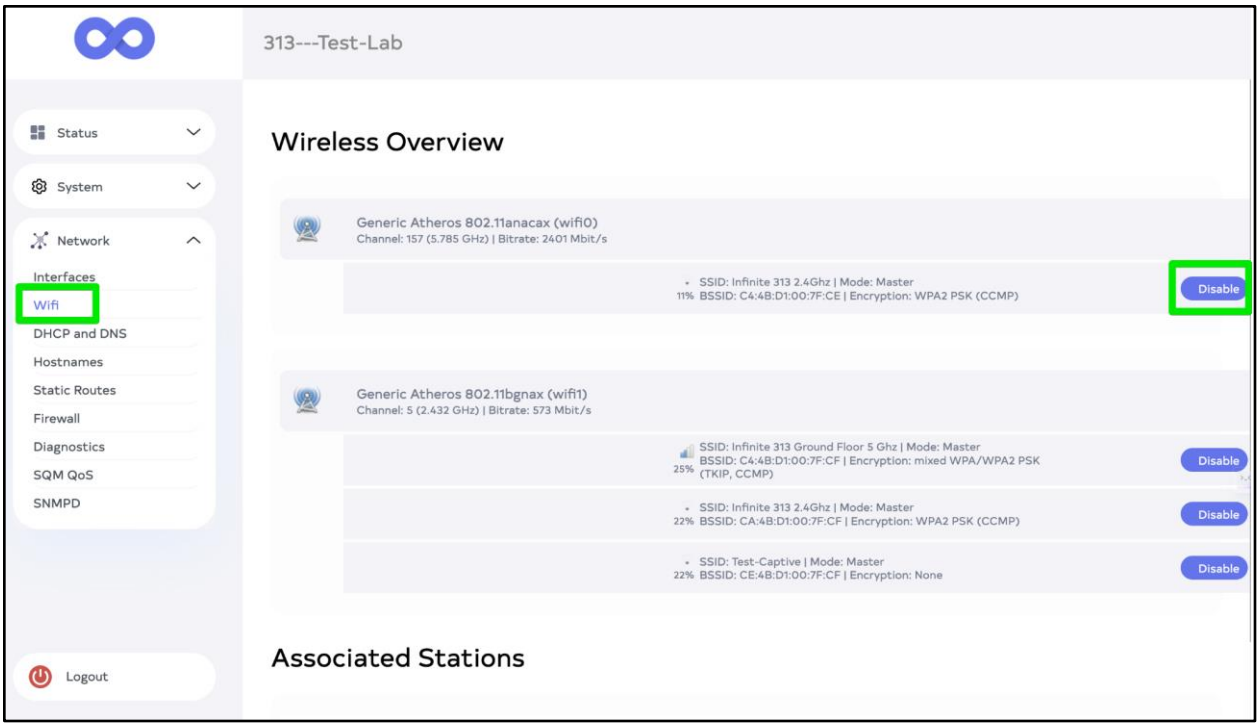
At the end of the section, click **Save&Apply** to save and apply the changes. Click **Save** to save changes, or **Reset** to reset the settings.



Wifi

The wireless overview provides detailed information about the wireless networks (Wi-Fi) available and their respective settings. The WiFi network details provide information about the technical aspects and settings of the specific wireless network.

Click **Disable** to disable the specific Wi-Fi network, which would cease its operation and prevent devices from connecting to it.



Associated Stations

Associated stations refer to devices that are connected to or associated with the access points. Currently, no information about associated stations is available.

Please note that the values provided on this screen are example values and may differ in every specific case. These specifications provide insights into the wireless networks available and their settings, enabling you to manage and optimise your network connections effectively.

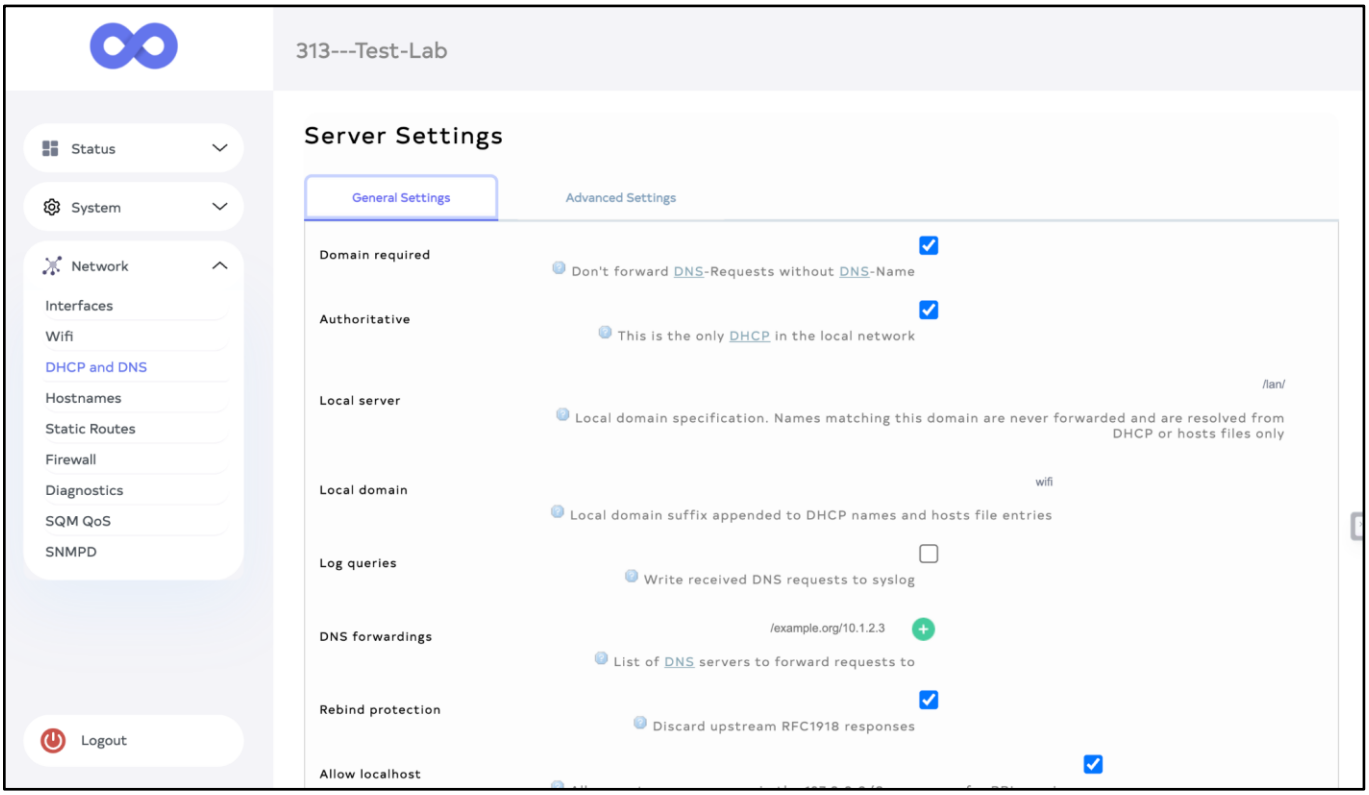
DHCP and DNS

Dnsmasq is a powerful tool that combines both DHCP server and DNS forwarder functionalities for NAT firewalls. Using Dnsmasq, you can effectively manage IP address allocation and DNS resolution within your network.
In this section, we will discuss the DHCP and DNS settings of your access point. The access point utilises a combined DHCP-Server and DNS-Forwarder called Dnsmasq to manage these functions for NAT firewalls.

Server Settings

This section provides general and advanced settings for the DHCP and DNS servers.

General Settings



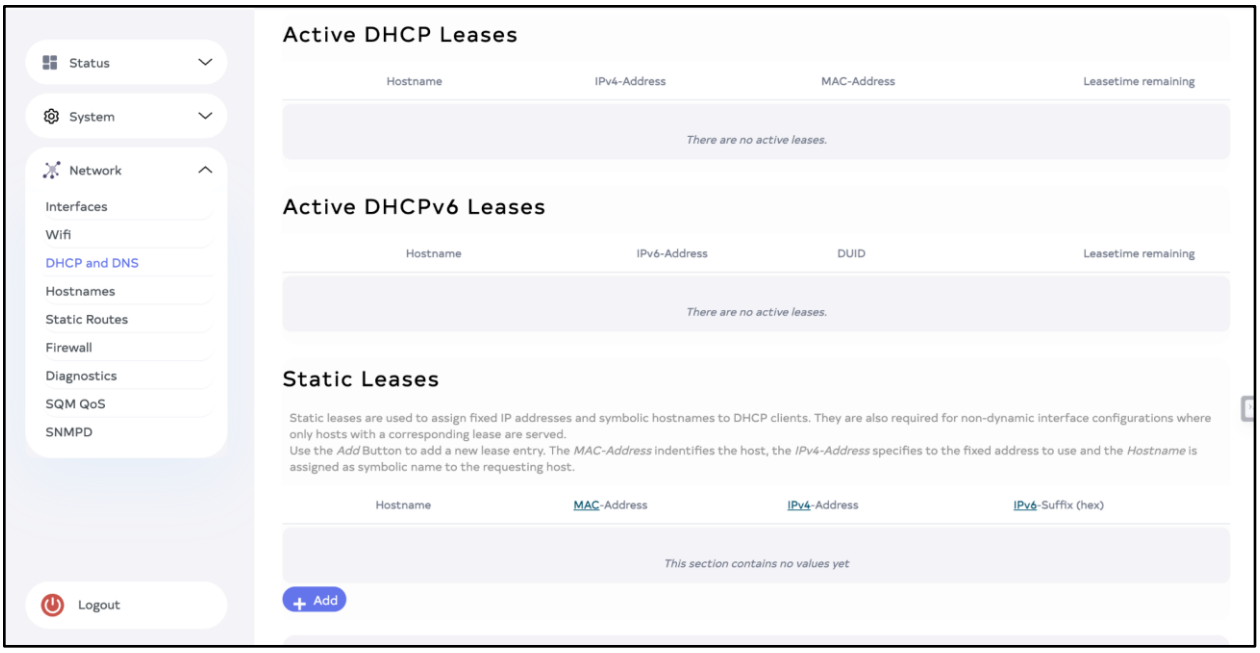
The General Settings tab contains the basic configurations of the server.

- **Domain required**: Select the checkbox to specify whether to forward DNS requests without a DNS name.
- **Authoritative**: Select the checkbox to indicate if this is the only DHCP server on the local network.
- **Local server**: This specifies the local domain for DHCP and hosts file resolution.
- **Local Domain**: Local domain suffix appended to DHCP names and hosts file entries
- **Log queries**: Select the checkbox to determine whether received DNS requests are logged to the system log.
- **DNS forwardings**: Specifies a list of DNS servers to forward requests to. Click on the plus button to add a new DNS server
- **Rebind protection**: Select this checkbox to discard upstream RFC1918 responses for protection.
- **Allow localhost**: Select this checkbox to permit upstream responses in the 127.0.0.0/8 range.
- **Domain whitelist**: Specifies a list of domains to allow RFC1918 responses for. Click on the plus button to add a new Domain

Active DHCP Leases: This section displays the currently active leases assigned by the DHCP server, including the hostname, IPv4 address, MAC address, and remaining lease time.

Active DHCPv6 Leases: This section displays the currently active DHCPv6 leases, including the hostname, IPv6 address, DUID, and remaining lease time.

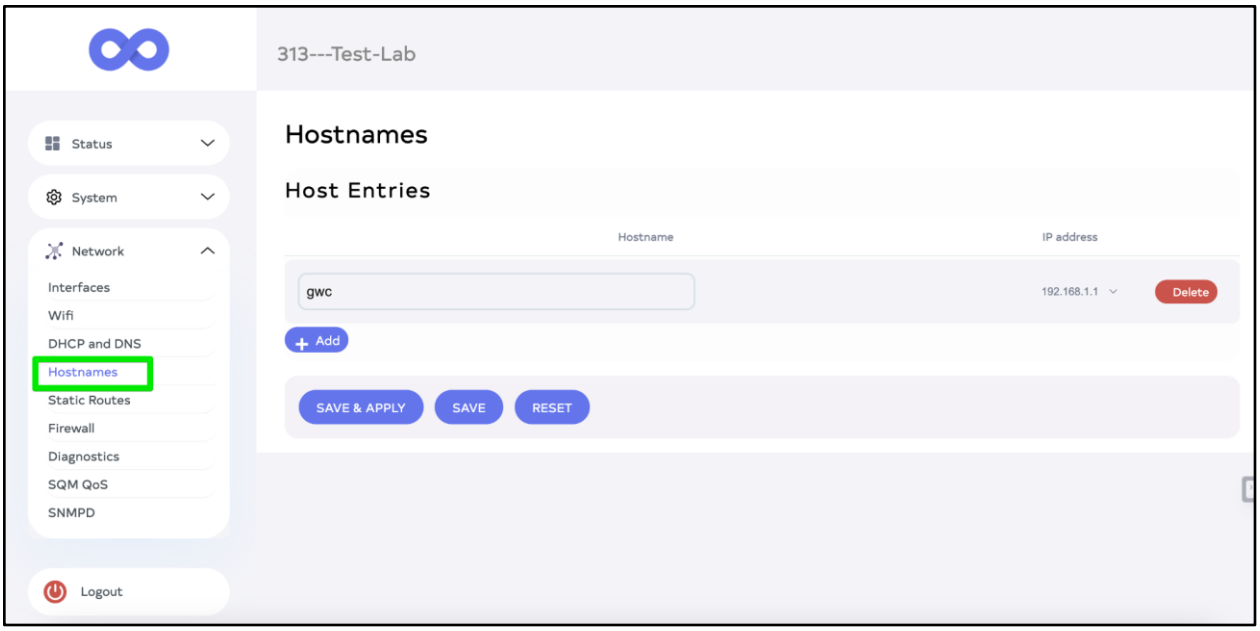
Static Leases: This section is used to assign fixed IP addresses and symbolic hostnames to DHCP clients. It is also necessary for non-dynamic interface configurations. Here, you can add new lease entries by specifying the MAC address, IPv4 address, and hostname.



At the end of the section, click **Save&Apply** to save and apply the changes. Click **Save** to save changes, or **Reset** to reset the settings.

Hostnames

The Hostnames feature allows you to manage and configure host entries for your network. Hostnames are used to associate memorable names with specific IP addresses, making it easier to identify and access devices on your network.



The Host Entries section within the Hostnames feature provides a table where you can add and manage the association between hostnames and IP addresses.

- **Hostname**: This column displays the hostname or name you want to associate with a specific IP address.
- **IP Address**: This column shows the corresponding IP address that the hostname should resolve to. Click on the "**Add**" button to enter the desired hostname and its corresponding IP address. Click on the "**Delete**" button to remove the association between a hostname and its IP address.

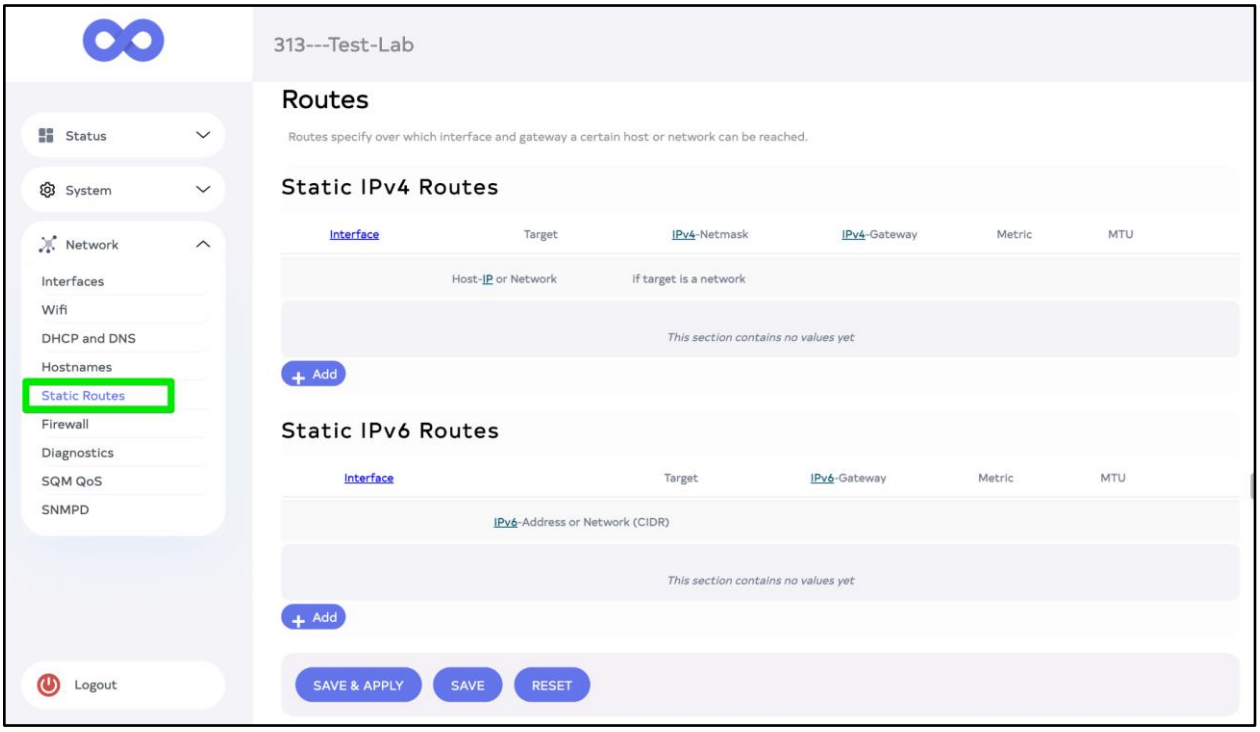
At the end of the section, click **Save&Apply** to save and apply the changes. Click **Save** to save changes, or **Reset** to reset the settings.

Static Routes

The Routes feature allows you to configure and manage your access point's routing settings. It allows you to specify how network traffic is routed between networks or subnets.

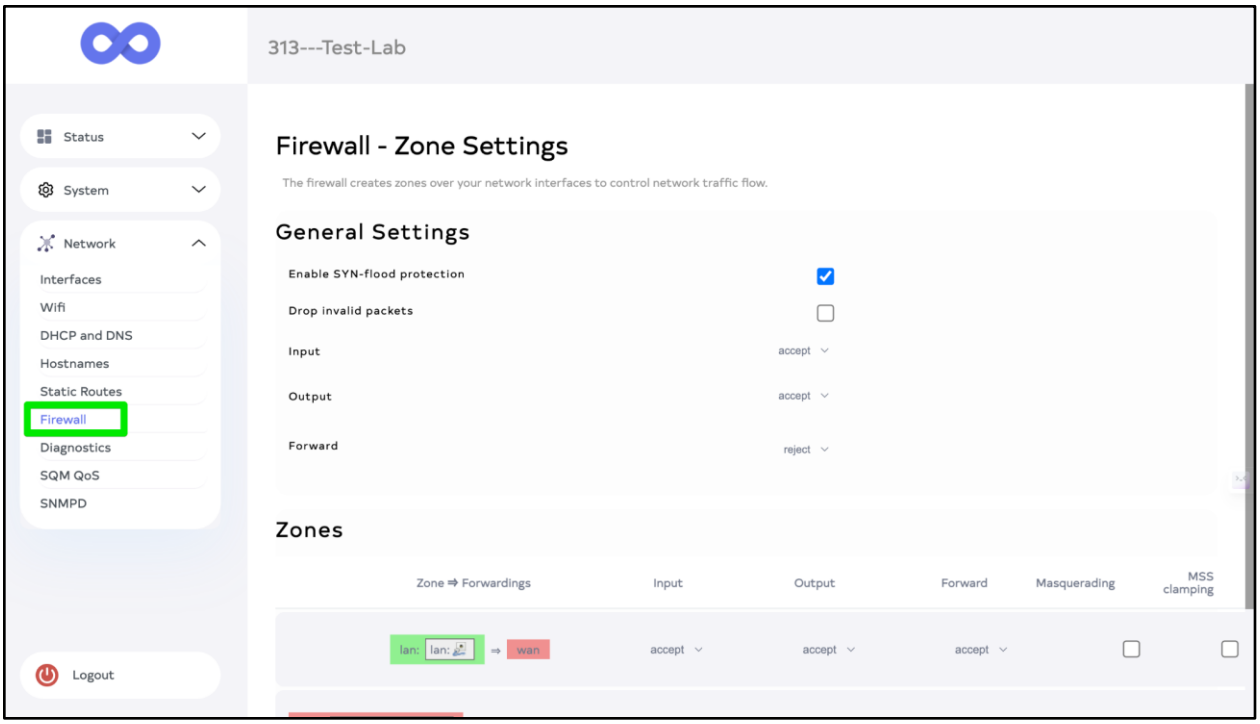
- **Static IPv4 Routes**: You can define static routes for IPv4 networks or individual host IP addresses in this section. By specifying the target IP address or network, IPv4 netmask, and the IPv4 gateway, you can determine over which interface and gateway a host or network can be reached. The metric and MTU values contribute to the optimization of the routing path and network performance. Click on the “**Add**” button to add a new Static IPv4 Route.

- **Static IPv6 Routes**: You can configure static IPv6 routes in this section. You can specify the IPv6 target address or network (in CIDR notation) as well as the IPv6 gateway. Click on the "**Add**" button to add a new Static IPv6 Route.



Firewall

The Firewall section in the Access Point Web UI allows you to configure and manage the firewall settings for your network. It provides controls to regulate the flow of network traffic and secure your network from unauthorised access.



General Settings

- **Enable SYN-flood protection**: Select this checkbox to enable protection against SYN flooding attacks, which are a type of DDoS attack.
- **Drop invalid packets**: When you enable this checkbox, the firewall will discard any incoming packets that are deemed invalid or malformed.
- **Input**: Click on the drop-down to choose the action to take for incoming traffic. In this case, it is set to "**accept**," which means that the firewall allows the traffic to pass through.
- **Output**: Click on the drop-down to choose the action to take for outgoing traffic. Here, it is also set to "**accept**," allowing outgoing traffic.
- **Forward**: Click on the drop-down to choose the action to take for forwarded traffic, which includes traffic between different zones within the network. In this case, it is set to "**reject**," which means that forwarded traffic is not allowed.

Zones

This section defines the different network zones and their respective settings.
These settings define the actions to be taken for traffic within the LAN and WAN. The specific adapters and wireless networks are also listed, along with their corresponding settings for input, output, and forward actions.

Diagnostics

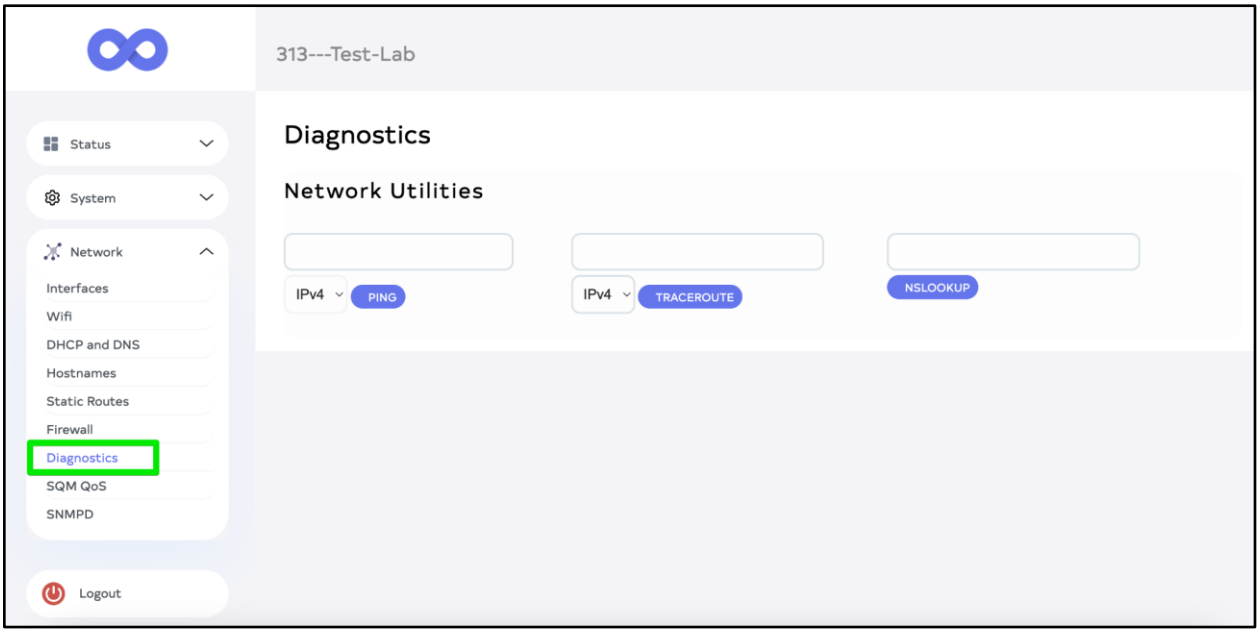
The Diagnostics section in the Access Point Web UI provides tools and functionalities that help you troubleshoot and diagnose network-related issues. It offers various features and utilities to assist in identifying and resolving connectivity problems.

Network Utilities

This feature provides a set of network diagnostic tools such as ping, traceroute, DNS lookup, and port scanning. These utilities help you test network connectivity, measure network latency, trace the route to a specific destination, resolve domain names to IP addresses, and check if specific ports are open or closed.

In Network Utilities, select either **IPv4** or **IPv6** from the drop-down menu to choose the IP version you want to perform diagnostic tests on. After selecting the IP version, you will have access to several tools:

- **Ping**: This tool allows you to send ICMP (Internet Control Message Protocol) echo request packets to a destination IP address to determine if it is reachable and measure the round-trip time (RTT) for the packets to reach their destination and return.
- **Traceroute**: Traceroute is used to trace the route that packets take from your access point to a specified destination IP address.
- **NSLookup**: NSLookup (Name Server Lookup) is a tool that enables you to query DNS (Domain Name System) servers to obtain information about a domain or IP address.



Smart Queue Management

In the Smart Queue Management (SQM) section, you can enable traffic shaping, fair queueing, active queue length management, and prioritisation on a specific network interface. SQM is a feature that helps optimise network performance and manage network congestion.

Queues

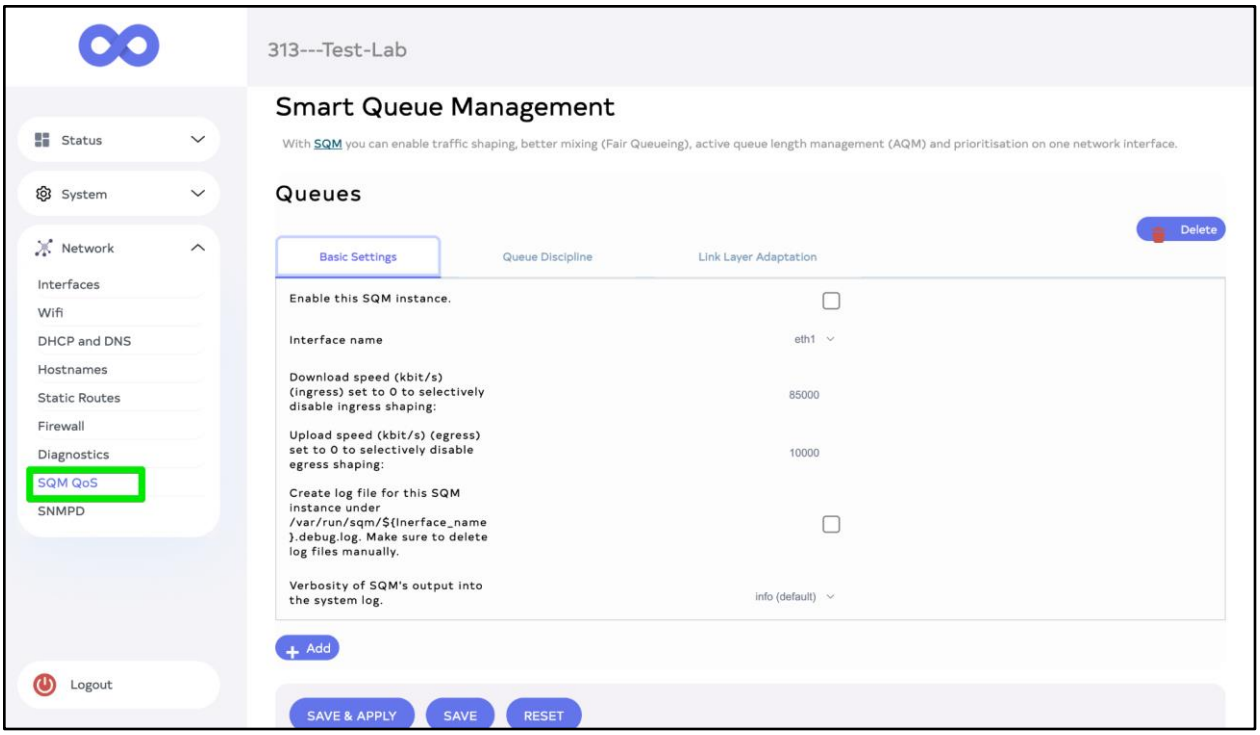
This section allows you to configure the settings related to the queues in the SQM instance. Queues help manage the flow of traffic by dividing it into manageable units.

Basic Settings

- **Enable this SQM instance**: Select the checkbox to enable or disable the SQM instance for a specific network interface.
- **Interface name**: Select the drop-down to choose the interface name (e.g., eth1) for which you want to enable SQM.

There are additional settings present in the provided input that allow for setting the download and upload speeds, creating log files for SQM instance debugging, and specifying the verbosity level of SQM's output into the system log.

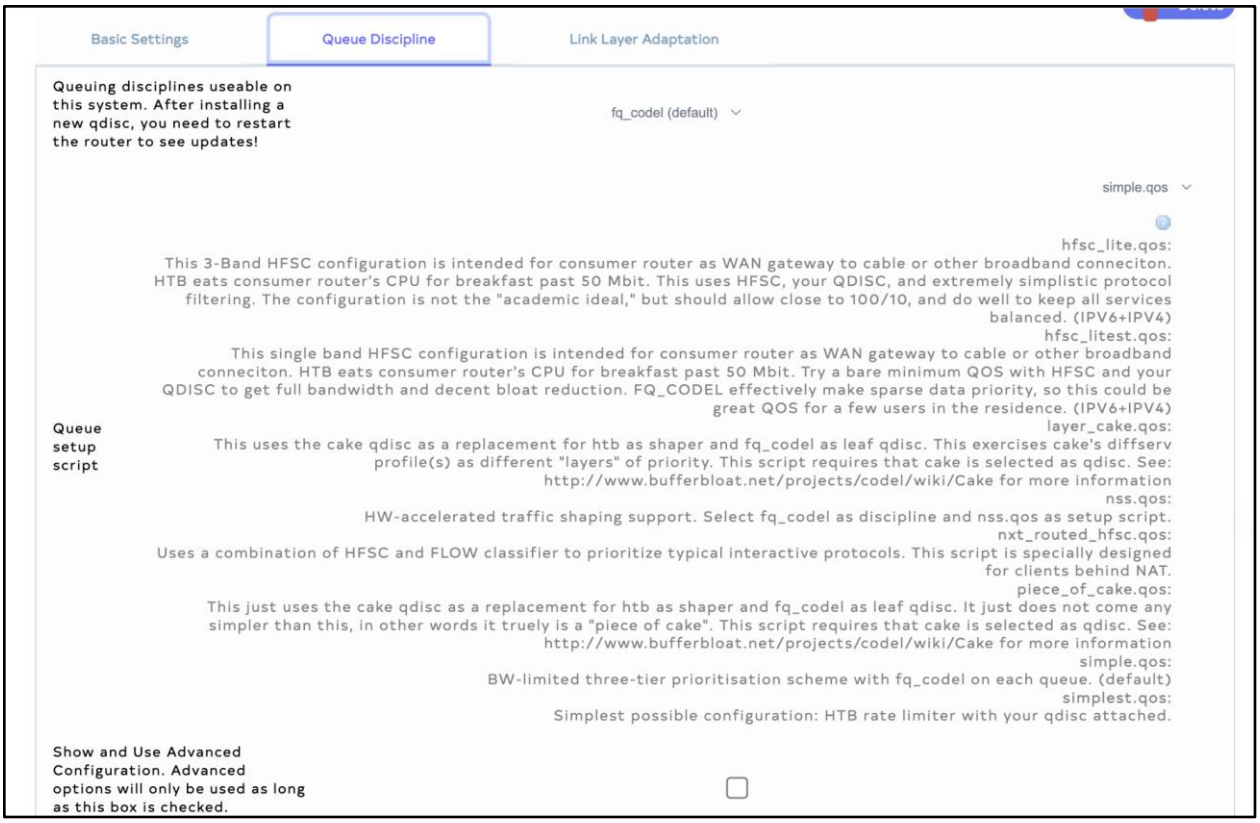
Click on the "**Delete**" button to delete the Queues. Click on the "**+Add"** button to add a new queue.



Queue Discipline

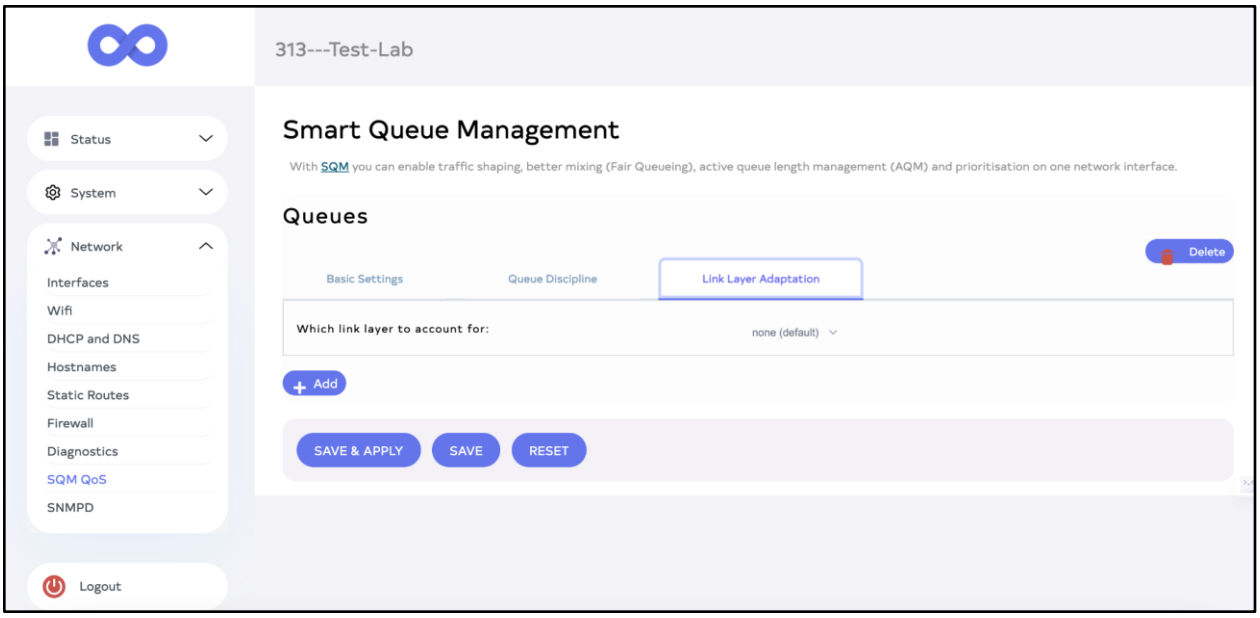
This setting determines the queuing discipline or algorithm used for managing traffic. The available options are listed, such as "fq_codel" which is the default option. Other options like "hfsc_lite.qos," "layer_cake.qos," or "piece_of_cake.qos" provide different configurations and algorithms suitable for specific use cases.

Additionally, advanced configuration options are available, and you can choose to show and use them by checking the "**Show and Use Advanced Configuration**" box. These advanced options provide more fine-grained control over the SQM settings, but they should be used with caution and understanding of their impacts on the network.



Link Layer Adaptation

The "Link Layer Adaptation" setting in the Smart Queue Management (SQM) feature allows you to choose the specific link layer to account for in order to optimise traffic shaping and management on your network interface. In this case, the available option is "**none**" which is the default setting.
The "**Link Layer**" refers to the network layer that is responsible for transmitting data over the physical link. By choosing the appropriate link layer adaptation, SQM can better understand and adapt to the characteristics of your network interface, ensuring more effective traffic shaping and management.



At the end of the section, click **Save&Apply** to save and apply the changes. Click **Save** to save changes, or **Reset** to reset the settings.

SNMPD

SNMPD is a master daemon/agent that allows for SNMP (Simple Network Management Protocol) functionality and management.

Agent Settings

This allows you to specify the address on which the SNMP agent should listen. The default setting is UDP port 161, which is the standard port used for SNMP communication. It provides an example of using UDP:161 or UDP:10.5.4.3:161 to specify the listening address.

Com2sec Security

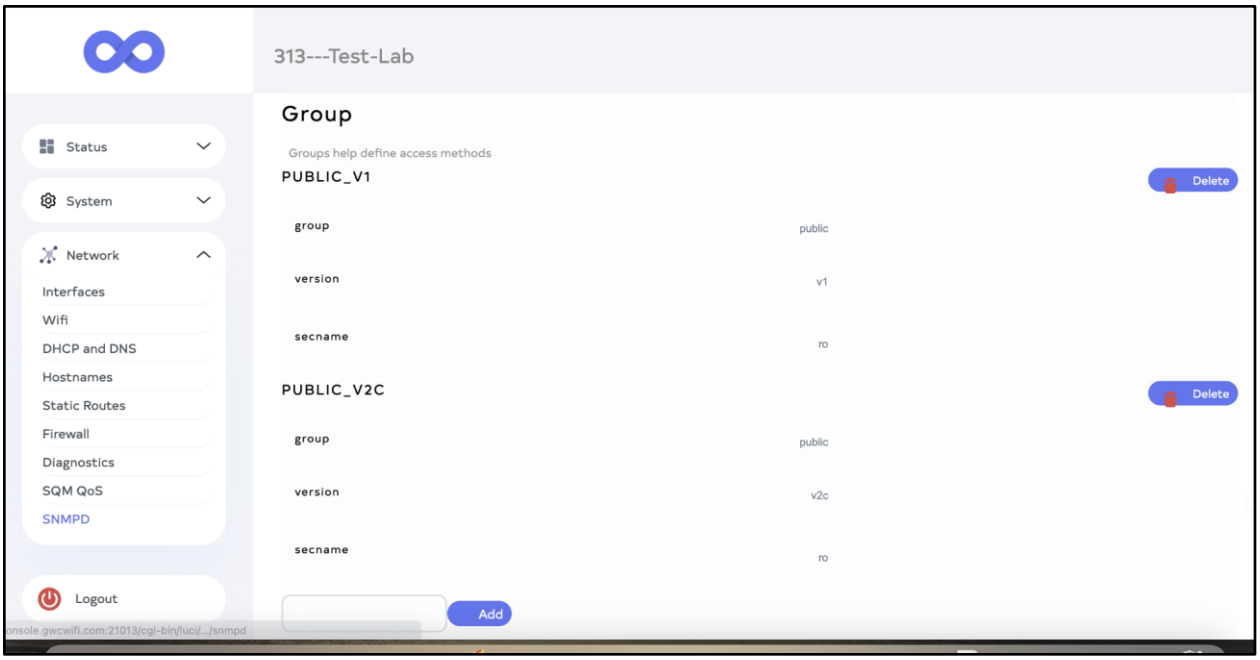
This section defines the community and security settings for SNMP access. You can edit them as per your requirements.

- **secname**: Specifies the section name. **Ro** defines the read-only (ro) access rights for the specified section.
- **source**: Specifies the source or origin of the SNMP request.
- **community**: Specifies the community string for the specified section. In this case, "public" is used as an example.

Group

This subsection is used to define groups, which help define access methods for SNMP.

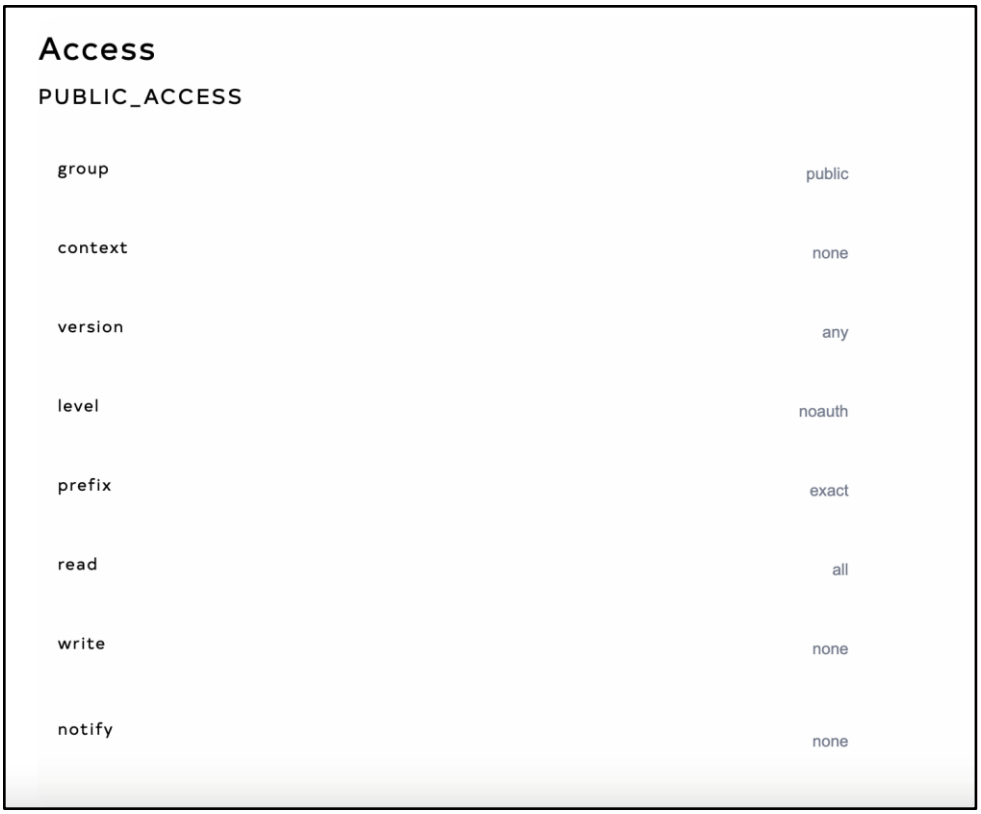
- **group**: Specifies the group name.
- **version**: Specifies the SNMP version associated with the group.
- **secname**: Specifies the security name associated with the group. In this case, "**PUBLIC_V1**" and "**PUBLIC_V2C**" are given as examples. Click **Add** to add a new group.



Access

This subsection defines the access settings for a specific group.

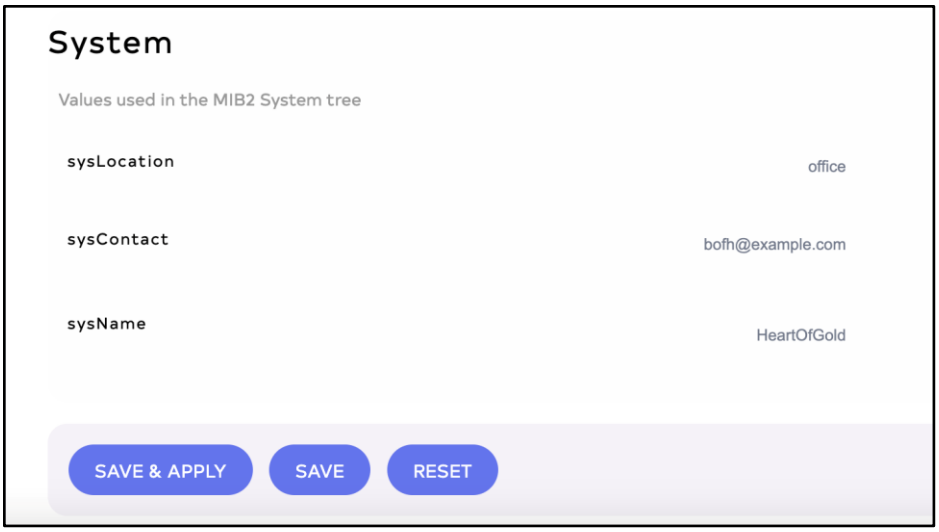
- **group**: Specifies the group name.
- **context**: Specifies the SNMP context associated with the group.
- **version**: Specifies the SNMP version associated with the group.
- **level**: Specifies the SNMP security level for the group.
- **prefix**: Specifies the SNMP prefix for the group.
- **read**: Specifies the read access rights for the group.
- **write**: Specifies the write access rights for the group.
- **notify**: Specifies the notification access rights for the group. In this case, "PUBLIC_ACCESS" is given as an example.



System

This subsection sets the values used in the MIB2 System tree, which provides information about the system.

- **sysLocation**: Specifies the location of the system.
- **sysContact**: Specifies the contact information for the system.
- **sysName**: Specifies the name of the system. In this case, "office", "bofh@example.com", and "HeartOfGold" are given as the example values.



FCC Statement

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:

(1) This device may not cause harmful interference, and

(2) This device must accept any interference received, including interference that may cause undesired operation.

FCC Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .This equipment should be installed and operated with minimum distance 30cm between the radiator& your body.

Note : This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates,uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.