by HFCL
Infinite Possibilities

User Manual (GUI)
Indoor & Outdoor Access Point

Wi-Fi 6

Ion4xi/ ion4x/ion4xe

Software Version   :
Release Date   : 5th March, 2021

Copyright Notice

Legal Disclaimer

About HFCL Limited

HFCL Limited delivers innovative, customized and competitive products and latest solutions in the high technology telecommunications infrastructure sector, thereby enabling its customers to stay ahead of their peers in technology and network efficiency.

The company's core specialization lies in manufacturing and providing a wide range of turnkey solutions. HFCL Limited has implemented several Greenfield projects (setting up CDMA & GSM networks, satellite communications, wireless spectrum management and DWDM optical transmission network), rolled out over 100,000 kilometres of OFC network, implemented over 25,000 2G/3G cell sites, provided high security applications to Defence and has developed expertise in the areas of Railways, Homeland Security and Smart cities.

Correspondence

HFCL Limited
8, Commercial Complex,
Masjid Moth, Greater Kailash II,
New Delhi-110048, India

Contact us at: +91 1130882624/2626
For your queries please mail us at:
Sales**:** sales.corp@hfcl.com
Enquiry: info@hfcl.com
Investors: investor@hfcl.com

Revision History

Date	Rev No.	Description	By
10-03-2021	A0-00	Initial Draft	Himankush

Table of Contents

CONFIDENTIAL

CONFIDENTIAL

List of Figures

CONFIDENTIAL

List of Tables

CONFIDENTIAL

1   About this Document

1.1   Purpose

This document helps you to understand IO products and provides information to familiarize you with the product features. It also guides you through the installation process and the entire software user set.

1.2   Intended Audience

The intended audiences for this document are:

1. Network Administrators
2. System Administrators
3. Product managers
4. System Integration and Verification team at HFCL Limited.

1.3   Document Conventions

The different conventions used in this document are explained in the following table:

Convention	Description
Note	Note provides information about important features or instructions. This appears with a background.
Caution	This alerts you to potential damage to a program, device, or system. This appears with a background.
Warning	This alerts you to potential injury or fatality. It may also alert you to potential electrical hazards. This appears with a background.
Courier new font	File and directory names are represented in Courier New font.
Bold font	Any option that needs to be selected or typed in the user interface is represented using bold font.
<home_directory>	Command variables, the values of which you must supply.
cd$HOME	A command that you must enter in a Command Line Interface (CLI) exactly as written. This appears with a background.

1.4   Terms and Abbreviations

The different terms and abbreviations used in this document are explained in the following table:

Terms and Abbreviations

Terms/Abbreviation	Expansion
AP	Access Point
BLE	Bluetooth Low Energy
CLI	Command-Line Interface
COS	Class Of Service
CPU	Central Processing Unit
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSCP	Differentiated Services Code Point
EMS	Element Management System
GI	Guard Interval
GPS	Global Positioning System
GUI	Graphic User Interface
HAL	Hardware Abstraction Layer
HTTP	Hypertext Transfer Protocol
IEEE	Institute Of Electrical And Electronics Engineers
IP	Internet Protocol
IPV4	Internet Protocol Version 4
IPV6	Internet Protocol Version 6
KBPS	Kilobits Per Second
L2TP	Layer 2 Tunneling Protocol
L2VPN	Layer 2 Virtual Private Network
LAN	Local Area Network
LED	Light-Emitting Diode

LMAC	Lower Media Access Control
MAC	Media Access Control
MBPS	Megabits Per Second
MCS	Modulation And Coding Scheme
MIMO	Multiple-Input And Multiple-Output
MPEG	Moving Picture Experts Group
MTU	Maximum Transmission Unit
NTP	Network Time Protocol
OSD	On Screen Display
P2MP	Point-To-Multipoint
P2P	Point-To-Point
PCP	Priority Code Point
POE	Power Over Ethernet
PTZ	Pan, Tilt, Zoom
QAM	Quadrature Amplitude Modulation
QOS	Quality Of Service
RFID	Radio Frequency Identification
RJ	Registered Jack
RSSI	Elative Received Signal Strength
RX	Received
SNMP	Simple Network Management Protocol
SNR	Signal-To-Noise Ratio
SSH	Secure Shell
STA	Station
TDMA	Time-Division Multiple Access
TX	Transmission
U-BOOT	Universal Boot-Loader
UBR	Unlicensed Band Radio

UID	User Id
UTP	Unshielded Twisted Pair
VAP	Virtual Access Point
VGA	Video Graphic Adapter
VLAN	Virtual Local Area Network
WAN	Wide Area Network
WDS	Wireless Distribution System
WIDS	Wireless Intrusion Detection System
WLC	Wireless Lan Controller
WPA	Wi-Fi Protected Access

2   Product Overview

Thank you for choosing the IO Access Point (AP). IO Access Points are oriented to next generation high-speed wireless access. The Access Point Configuration is controlled through GUI.

Following are the variants of IO product family:

1. Dual Band 2x2:2 Indoor Access Point (ion4xi).
2. Dual Band 2x2:2 Outdoor Access Point (ion4x/ion4xe).

3   Federal Communication Commission Certified

These equipment are 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.

These 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 these 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 of the following measures:

1. Reorient or relocate the receiving antenna.
2. Increase the separation between the equipment and receiver.
3. Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
4. Consult the dealer or an experienced radio/TV technician for help.

FCC Caution:

To assure continued compliance, any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment. (Example - use only shielded interface cables when connecting to computer or peripheral devices).

FCC Radiation Exposure Statement:

These equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. These equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter. The antennas used for this transmitter must be installed to provide a separation distance of at least 20 cm from all persons and must not be co-located or operating in conjunction with any other antenna or transmitter.

These devices complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions:

1. These devices may not cause harmful interference
2. These devices must accept any interference received, including interference that may cause undesired operation.

3.1 Dual Band 2x2:2 Indoor Access Point

Technical specifications of this variant are given below:

FEATURES	INDOOR 2x2 AP (ion4xi)
Description	Dual Band Indoor Access Point with integrated 2.4 and 5 GHz radio, capable of delivering throughput up to 1.78 Gbps, with 2x2:2 Multi-User MIMO and 802.11ax compliance
Peak Throughput (aggregate)	Up to 1.78 Gbps
Wi-Fi Standard Support	802.11 a/b/g/n/ac/ac Wave 2/ax
No. of Radios	Dual concurrent 2.4 GHz and 5 GHz (with extended 5 GHz channel support, country-specific restrictions apply)
MU-MIMO	2x2:2
Max Transmit Power	2.4 GHz– up to 30 dBm and 5 GHz– up to 30 dBm (will depend on country specific guidelines)
Antenna Type	Integrated Omni-directional antennas
Antenna Gain	4 dBi for both 2.4 GHz and 5 GHz
Maximum User Support	1024
Channel Bandwidth	20, 40, 80 MHz
Modulation	Up to 1024 QAM
Wireless Security	802.11i, 802.1x / EAP, Hidden, WIPS, WEP, WPA-PSK, WPAEnterprise, WPA2-PSK, WPA2-EAP, WPA2-PSK-Mixed, WPA2-Enterprise, WPA3-Personal and WPA3-Enterprise, WPA3-SAE, WPA3-SuiteB, MAC, Radius based, EAP Type (EAP-TLS, EAPTTLS/ MSCHAPv2, PEAPv0/EAP- MSCHAPv2, EAP-SIM), Protected Management Frames
WAN Protocols	Static IPv4/IPv6, DHCP client v4/v6

Figure 1: Dual Band 2x2:2 Indoor Access Point - Specifications & Highlights-1

Figure 2: Dual Band 2x2:2 Indoor Access Point - Specifications & Highlights-2

3.2   Dual Band 2x2:2 Outdoor Access Point (ion4x/ion4xe)

The Dual Band 2x2:2 outdoor Access Point has two factory fitted variants: one with integrated antennas (ion4x) and the other with connectors for external antennas (ion4xe). Technical specifications are given below:

FEATURES	OUTDOOR 2x2 AP (ion4x/ion4xe)
Description	Dual Band Outdoor Access Point with integrated 2.4 and 5 GHz radio, capable of delivering throughput up to 1.78 Gbps, with 2x2:2 Multi-User MIMO and 802.11ax compliance
Peak Throughput (aggregate)	Up to 1.78 Gbps
Wi-Fi Standard Support	802.11 a/b/g/n/ac/ac Wave 2/ax
No. of Radios	Dual concurrent 2.4 GHz and 5 GHz (with extended 5 GHz channel support, country-specific restrictions apply)
MU-MIMO	2x2:2
Max Transmit Power	2.4 GHz– up to 30 dBm and 5 GHz– up to 30 dBm (will depend on country specific guidelines)
Antenna Type	Integrated directional antennas with 120° beamwidth/Option for external antennas
Antenna Gain	14 dBi on 2.4 GHz and 14 dBi on 5 GHz (Integrated variant) As per physical antenna gain (External variant)
Maximum User Support	1024
Channel Bandwidth	20, 40, 80 MHz
Modulation	Up to 1024 QAM
Wireless Security	802.11i, 802.1x / EAP, Hidden, WIPS, WEP, WPA-PSK, WPAEnterprise, WPA2-PSK, WPA2-EAP, WPA2-PSK-Mixed, WPA2-Enterprise, WPA3-Personal, WPA3-Enterprise, WPA3-SAE, WPA3-SuiteB, MAC, Radius based, EAP-SIM, EAP-TLS, EAPTTLS, EAP, Protected Management Frames
WAN Protocols	Static IPv4/IPv6, DHCP client v4/v6

Figure 3: Dual Band 2x2:2 Outdoor Access Point - Specifications & Highlights-1

FEATURES	OUTDOOR 2x2 AP (ion4x/ion4xe)
Mesh Support	Self-creating, Self-healing EasyMesh
Maximum number of SSID (per radio)	16
BLE Support	No
Ethernet support/ Ports/Interface	1 X 10/100/1000BASE-T Ethernet 1 X 2500 Base X Optical Ethernet SFP
Rogue AP Detection and Prevention	Yes
Receiver Sensitivity	-97 dBm or better
Power Supply	IEEE 802.3at PoE/PoE+
Power Consumption (Max)	17 W
Wireless QOS	WMM (802.11e)
Band Steering Support for Dynamic RF Optimization	Yes
Geo-Location	N/A
Management	Standalone (via GUI) or through on-premise based solution or cloud-based
Enclosure Type	Two-piece enclosure with UV protected ABS + PC top body and aluminium bottom body
Enclosure Dimensions	178 X 178 X 73 mm
Weight	1.20 kg (for Integrated antenna variant) and 1.20 kg (for External antenna variant)
Operating Temperature	-15°C to 60°C
Humidity	5 to 95% (non-condensing)
Certifications	FCC Class A, CE, Passpoint 2.0, IP 67, EasyMesh

Figure 4: Dual Band 2x2:2 Outdoor Access Point - Specifications & Highlights-2

4   Hardware Setup

4.1   System Requirements

Before installing the access point, make sure that your system includes the following:

1. 10/100/1000 Mbps local area network device such as a hub or switch.
2. The Category 5 UTP straight-through Ethernet cable with RJ-45 connector included in the package, or one like it.
3. We can power up the device through PoE adaptor which should be 803at/af compliant. A 100–240 V, 50–60 Hz AC power source.
4. A web browser to configure the devices.
5. At least 802.11b/g-compliant devices.

4.2   Packaging Content – For ion4xi/ion4x/ion4xe variants of this product

Your box contains the following items:

1. User can choose any of the Access Point model mentioned below:
    a. Dual Band 2x2:2 Indoor Access Point (ion4xi).
    b. Dual Band 2x2:2 Outdoor Access Point (ion4x/ion4xe).
2. Mounting bracket kit.
3. Quick Start Guide with cabling and access point setup instructions. If any parts are incorrect, missing, or damaged, contact HFCL Limited customer care support.

5   Getting to Know the IO Access Point

5.1   Dual Band 2x2:2 Indoor Access Point

5.1.1   Back / Side View

A basic overview of the back/side view of the indoor AP is given below:
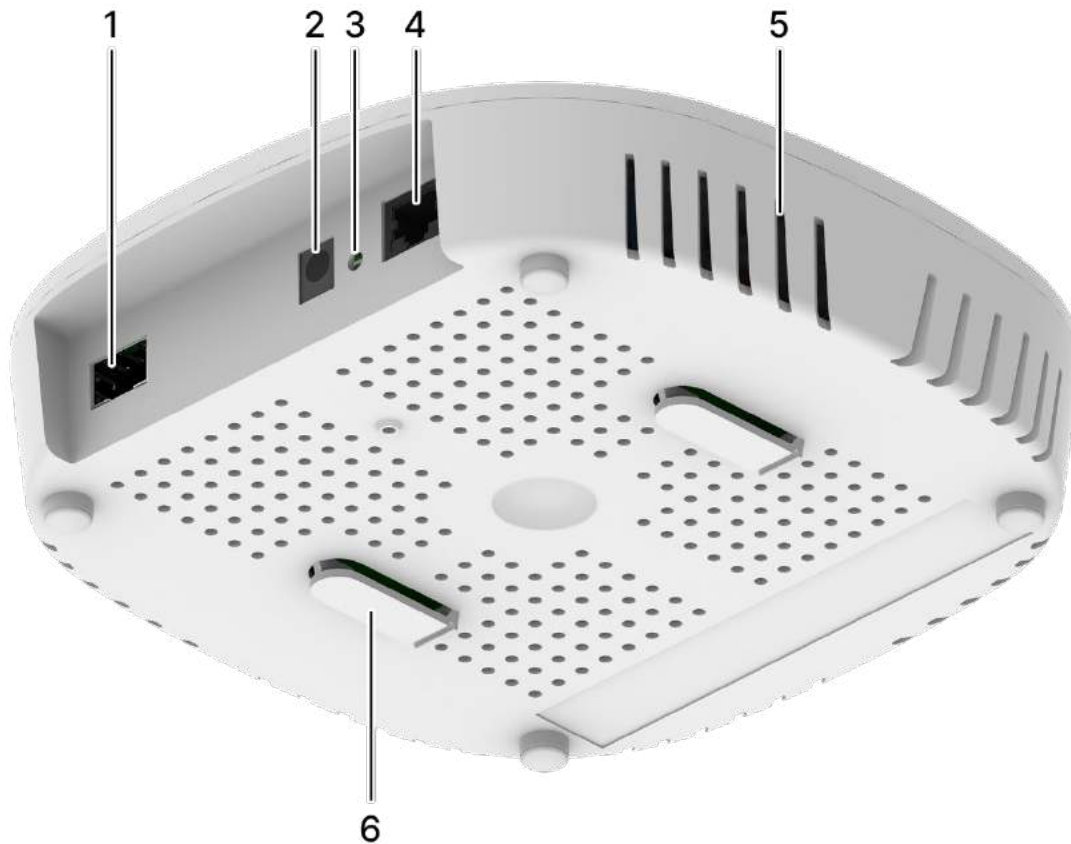
Figure 5: Side view of the indoor AP

Information displayed in the above figure is detailed in the table below:

Table 1: List of information displayed in side view of the indoor AP

Callout	Name	Description
1.	SFP Port	Connects fiber cable with the maximum data transfer rate capability of 2.5 Gbps
2.	DC Jack	Power up the Access Point with a DC adaptor
3.	Power LED	This LED glows in Green color to notify the user that device is powered ON
4.	LAN + PoE Port	Used for powering up the device via PoE adaptor. The same port carries the data

Callout	Name	Description
5.	Vent	Transfers the heat in the ambient
6.	Mounting Slot	This helps in the attachment of mounting bracket and indoor AP in case of wall and ceiling mounting

5.1.2   Top / Side View

A basic overview of the top/side view of the indoor AP is given below:
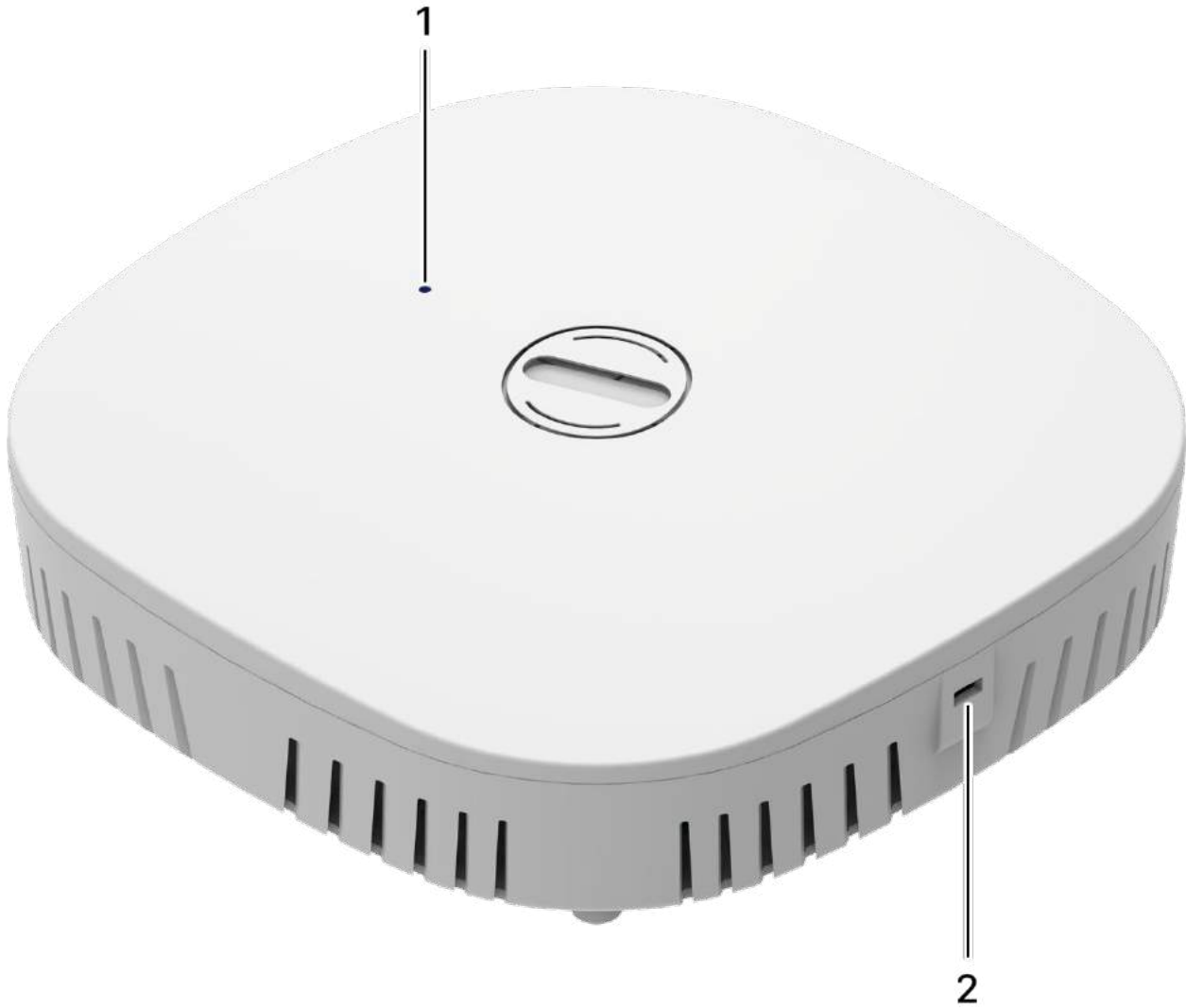
Figure 6: Top Side view of the indoor AP

Information displayed in the above figure is detailed in the table below:

Table 2: List of information displayed in top side view of the indoor AP

Callout	Name	Description
1.	Status LED	This LED glows in Green color to notify the user that the 2.4GHz radio is active
		This LED glows in Blue color to notify the user that the 5GHz radio is active
		This LED glows in Cyan color to notify the user that both 2.4GHz & 5GHz radio are active
2.	Kensington Lock	This slot is provided for the Kensington Lock

5.2   Dual Band 2x2:2 Outdoor Access Point

5.2.1   Front / Side View

A basic overview of the front/side view of the outdoor AP is given below:

Figure 7: Front/side view of the outdoor AP (ion4x)

Information displayed in the above figure is detailed in the table below:

Table 3: List of information displayed in front/side view of the outdoor AP

Callout	Name	Description
1.	SFP Port	Connects fiber cable with the maximum data transfer rate capability of 2.5 Gbps
2.	Power LED	This LED glows in Green color to notify the user that device is powered ON
	2.4 GHz LED	This LED glows in Blue color when 2.4 GHz wireless network interface comes up
	5 GHz LED	This LED glows in Blue color when 5 GHz wireless network interface comes up

Callout	Name	Description
3.	LAN + PoE Port	Used for powering up the device via PoE adaptor. The same port carries the data
4.	Kensington Lock	This slot is provided for the Kensington Lock

5.3 Back View

Back side overview of the outdoor AP is given below:
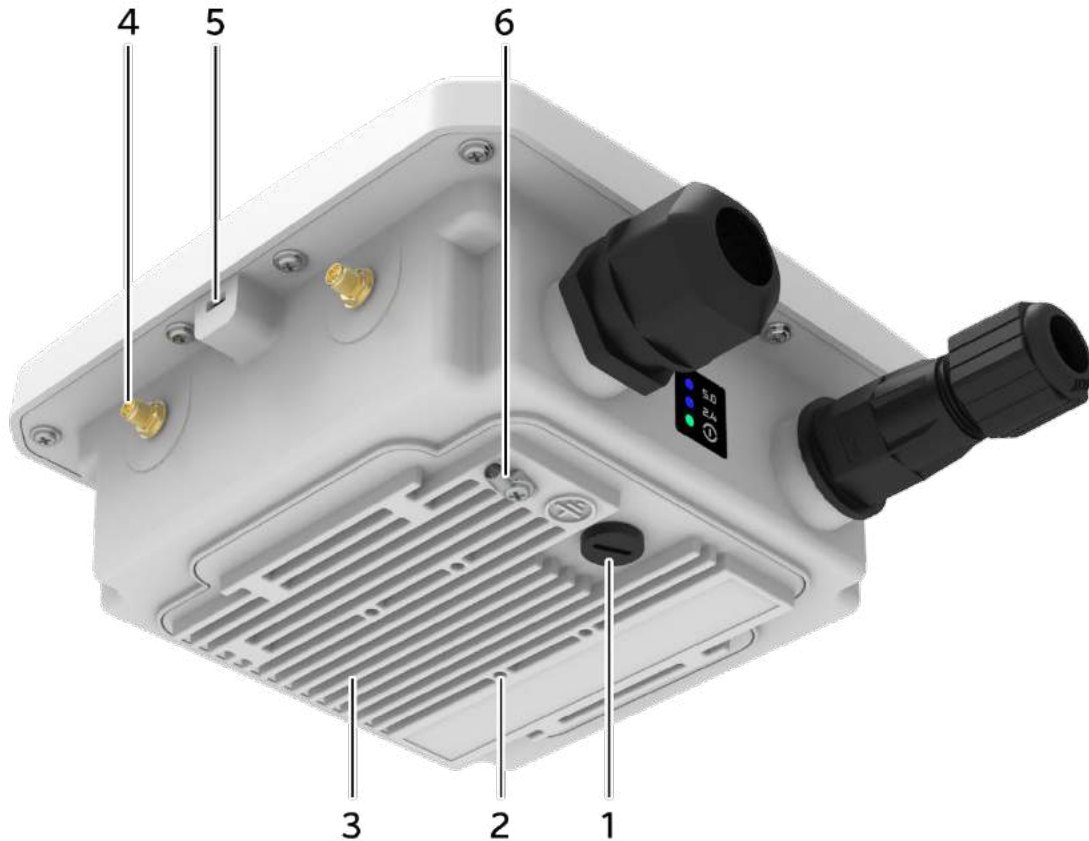
Figure 8: Back view of the outdoor AP (ion4xe)

Information displayed in the above figure is detailed in the table below:

Table 4: List of information displayed in back view of the outdoor AP

Callout	Name	Description
1.	Humidity controller cap	Cap to control the humidity
2.	Screws for Mounting bracket	This helps in the attachment of mounting bracket and outdoor AP in case of pole and wall mounting
3.	Thermal Plate (Heat Transfer)	It helps in heat transfer from the board environment to Ambient.

Callout	Name	Description
4.	External antenna connectors	Total 2 n-type antenna connectors or 2 SMA connectors are available for ion4xe variant of 2x2:2 outdoor AP. These connectors are not available in ion4x variant, as the variant has integrated antennas
5.	Kensington Lock	This slot is provided for the Kensington Lock
6.	Grounding point	The outdoor AP is grounded at this point

Note: The Reset button of outdoor AP is located below the humidity controller cap. Turn the humidity controller cap in counter clock wise direction and remove it from the access point. Use an appropriate pointed object to press the button. It serves two functions:

1. Restart: Press and release the Reset button quickly.
2. Restore to Factory Default Settings: Press and hold the Reset button for more than five seconds.

6   Initial Setup

Observe the following safety precautions and avoid damage to the access point:

1. Do not power the device during installation.
2. Do not subject the device to high temperatures.
3. Keep away from high voltage cables.
4. Disconnect the device before cleaning it.
5. Do not wipe the device with a damp cloth.
6. Do not wash the device with liquid.
7. Do not open the enclosure when the AP is working.
8. Fasten the device tightly.

6.1   Dual Band 2x2:2 Indoor Access Point

Power up the device using PoE Adaptor or DC Adaptor as shown below:
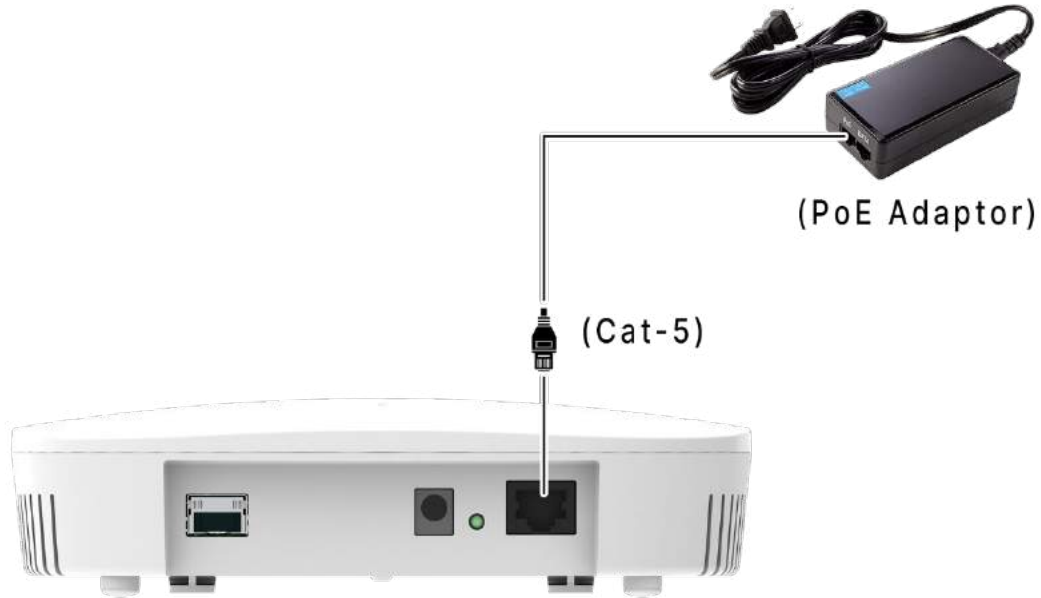
Figure 9: Power up the device using PoE adaptor

Figure 10: Power up the device using DC adaptor

6.1.1   Connect to the Indoor Access Point

Follow the steps mentioned below and connect to the indoor AP through GUI:

1. Configure a computer with a 1-domain static IP address e.g. 192.168.1.10 and a subnet mask of 255.255.255.0.
2. For help configuring a static IP address on your computer, check the instructions or online help that came with that computer.\
3. Connect the Ethernet cable to the computer.
4. Connect the other end of the Ethernet cable to the PoE adaptor (Data/In port). Use the unused port (P+D/Out) of PoE adaptor and connect it to the LAN + PoE port of the device.
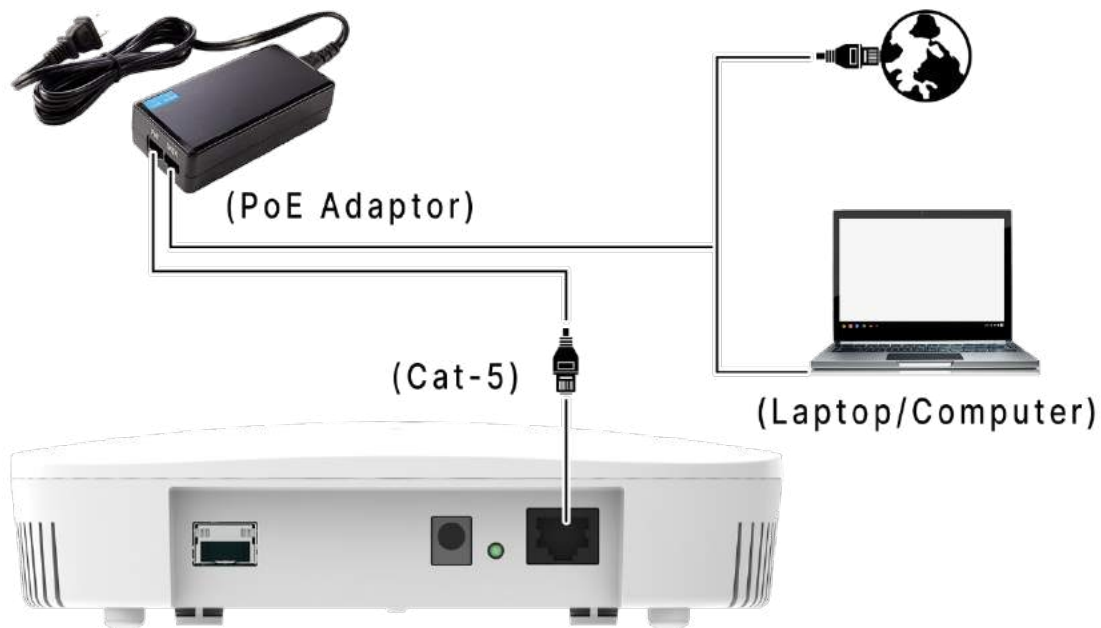
Figure 11: Connect to the network

5. Device will be powered On.
6. Open a web browser and enter the "AP static IP address" (**192.168.1.1**) in the address bar.
7. A login screen will appear.

6.2   Dual Band 2x2:2 Outdoor Access Point

Power up the device using PoE Adaptor as shown below:

Figure 12: Power up the device using PoE adaptor

6.2.1   Connect to the Outdoor Access Point

Follow the steps mentioned below and connect to the outdoor AP through GUI:

1. Configure a computer with a 1-domain static IP address e.g. 192.168.1.1 and a subnet mask of 255.255.255.0.
2. For help configuring a static IP address on your computer, check the instructions or online help that came with that computer.\
3. Connect the Ethernet cable to the computer.
4. Connect the other end of the Ethernet cable to the PoE adaptor (Data/In port). Use the unused port (P+D/Out) of PoE adaptor and connect it to the LAN + PoE port of the device.
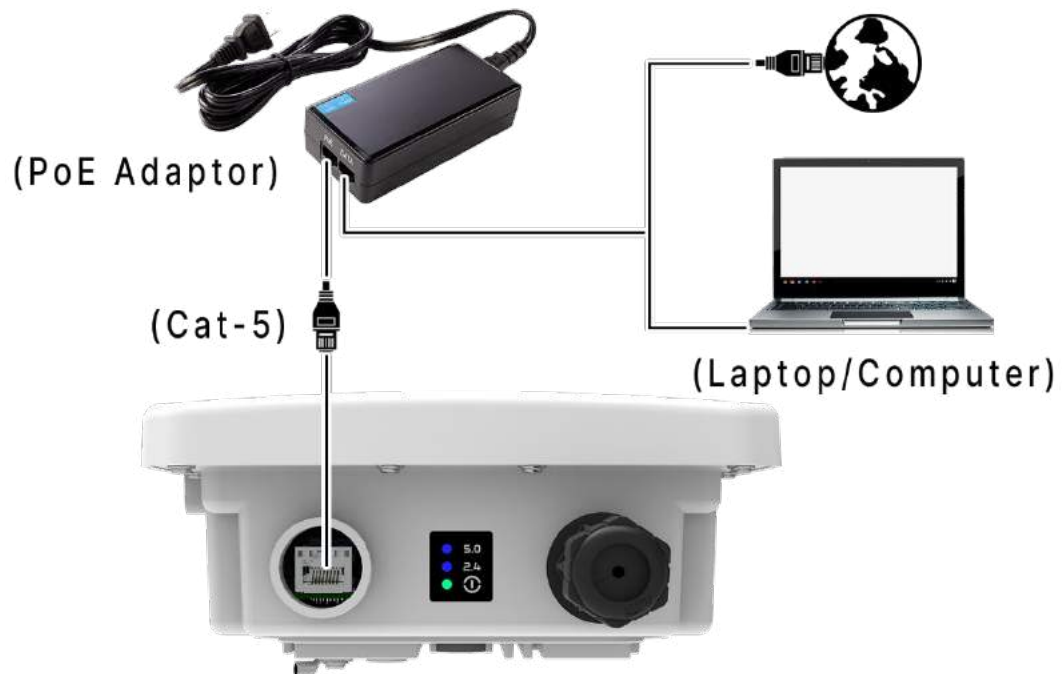
Figure 13: Connect to the network

5. Device will be powered On.
6. Open a web browser and enter the "AP static IP address" (**192.168.1.1**) in the address bar.
7. A login screen will appear.

7   Connect to the Thick Access Point and Log In

You can connect to the access point's web management interface to view or change its LAN and wireless access settings. Refer the procedure mention in "Connect to the Indoor Access Point" and "Connect to the Outdoor Access Point" section and connect to a thick mode access point.

7.1   Login through GUI

This is the 1st screen of AP GUI. It provides access to the users with valid login credentials only. The login credentials will determine the access rights of the user.

A basic overview of the same is shown below:
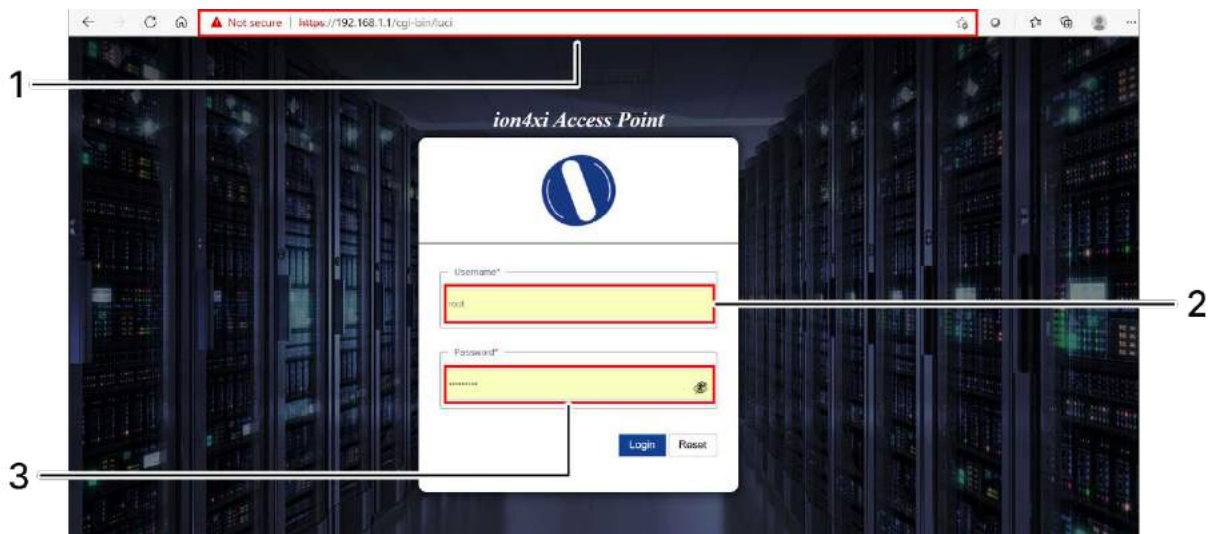
Figure 14: Basic overview of login screen

Follow the steps given below to login through GUI:

Table 5: List of actions to login through GUI

Callout	Name	Description
1.	Web browser	Open a web browser and enter the "IP address of the AP" in the address bar. 192.168.1.1 is the default IP address
2.	User name	Enter the valid "User ID"
3.	Password	Enter the valid "Password"

Click on "Login", a successful/authenticated login will take the user to Status Overview screen.

33

8   Status overview screen

The screen provides the status overview of:

1.   System summary

2.   System feature

3.   Software

4.   Hardware

8.1   System summary

A basic layout of the system summary is given below:
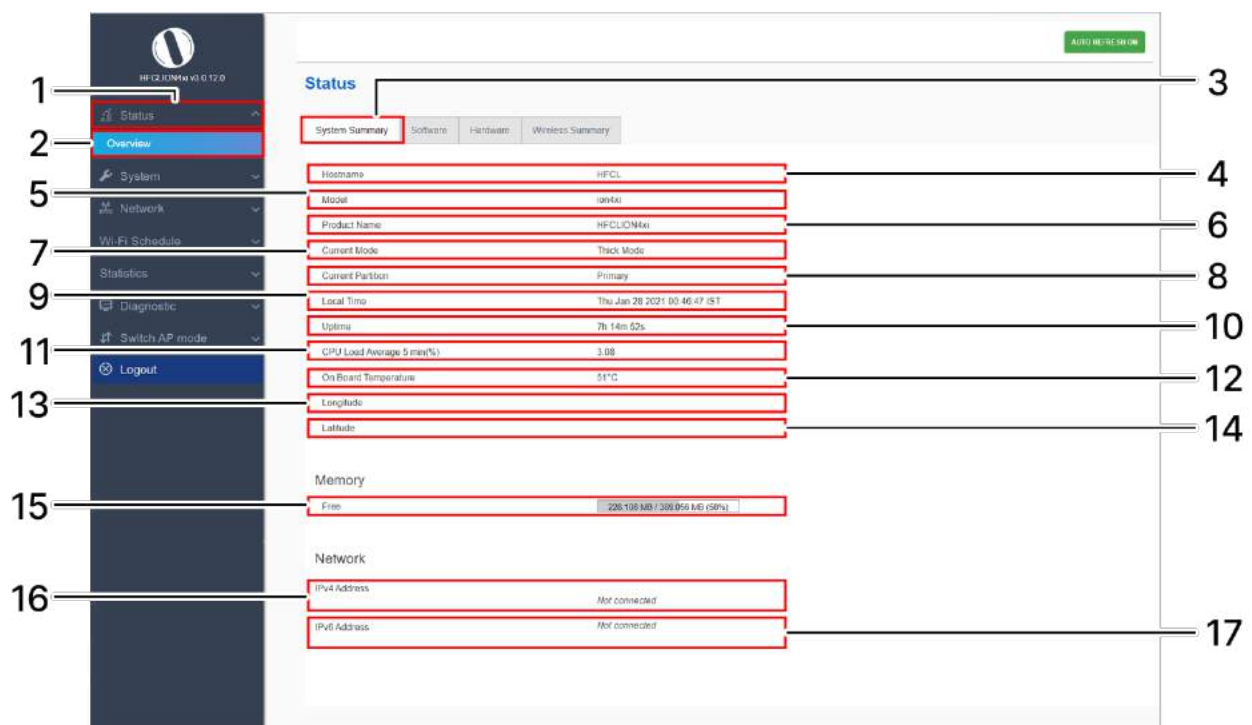
Figure 15: Basic layout of the system summary screen

Follow the steps given below to view the system summary:

Table 6: List of information displayed in the system summary

Callout	Name	Description
1.	Status	Click on the "Status" dropdown
2.	Overview	Click on "Overview" option
3.	System summary	Click on "System summary" option
4.	Hostname	Displays the "Hostname" assigned to the respective AP in the "System Configuration" screen

Callout	Name	Description
5.	Model	Displays the model number of the product. The same is configured with the factory settings of the device and reflects in this section on system boot up
6.	Product Name	Displays the name of the product
7.	Current Mode	Displays the current acting mode of the AP (Thick mode or Thin mode)
8.	Current Partition	Displays the current partition in use (Primary or Secondary)
9.	Local Time	Displays the date and time details according to the time zone allocated in the "System Configuration" screen
10.	System uptime	Displays the time duration since the respective AP board is up and successfully running without any shutdown
11.	CPU Load Average 5 min	Displays the average load on the device
12.	On Board Temperature	Displays the board temperature
13.	Longitude	Displays the longitude coordinates of the Access Point
14.	Latitude	Displays the latitude coordinates of the Access Point
15.	Memory	Displays the used and free CPU memory of the Access Point
16.	IPv4 Address	Displays the allocated IPv4 address
17.	IPv6 Address	Displays the allocated IPv6 address

8.2   System software

A basic layout of the system software is given below:
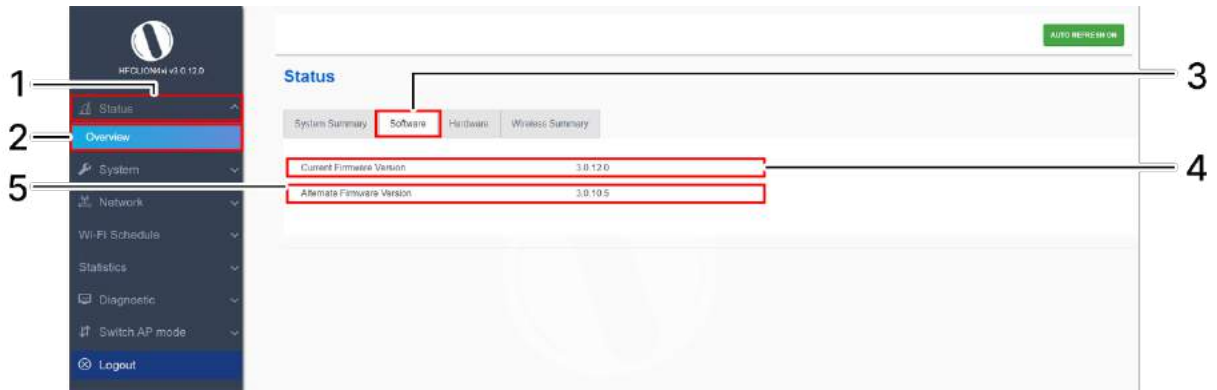
Figure 16: Basic layout of the system software screen

Follow the steps given below to view the system software information:

Table 7: List of information displayed in the system software screen

Callout	Name	Description
1.	Status	Click on the "Status" dropdown
2.	Overview	Click on "Overview" option
3.	Software	Click on "Software" option
4.	Current Firmware Version	Displays the current firmware version of the respective AP. The operating system is based on openwrt project model
5.	Alternate Firmware Version	Displays the alternate firmware version of the respective AP

8.3   System hardware

A basic layout of the system hardware is given below:
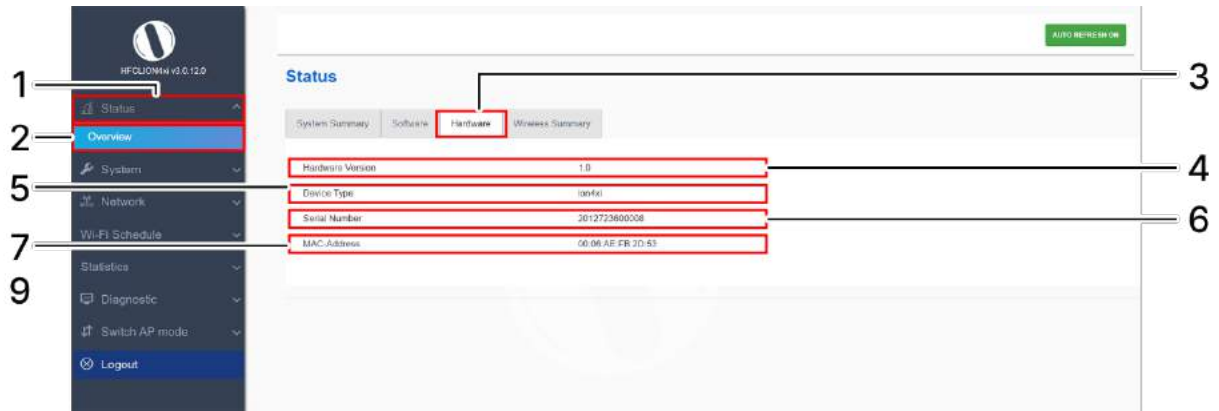
Figure 17: Basic layout of the system hardware screen

Follow the steps given below to view the system hardware information:

Table 8: List of information displayed in the system hardware screen

Callout	Name	Description
1.	Status	Click on the "Status" dropdown
2.	Overview	Click on "Overview" option
3.	Hardware	Click on "Hardware" option
4.	Hardware Version	Displays the current hardware version of the respective AP
5.	Device Type	Displays the device type (Indoor or Outdoor)
6.	Serial Number	Displays the serial number of the respective AP. The same is configured with the factory settings of the device and reflects in this section on system boot up
7.	MAC-Address	Displays the MAC address assigned to the product. The same is configured with the factory settings of the device and reflects in this section on system boot up

8.4   System Wireless

A basic layout of the system wireless is given below:
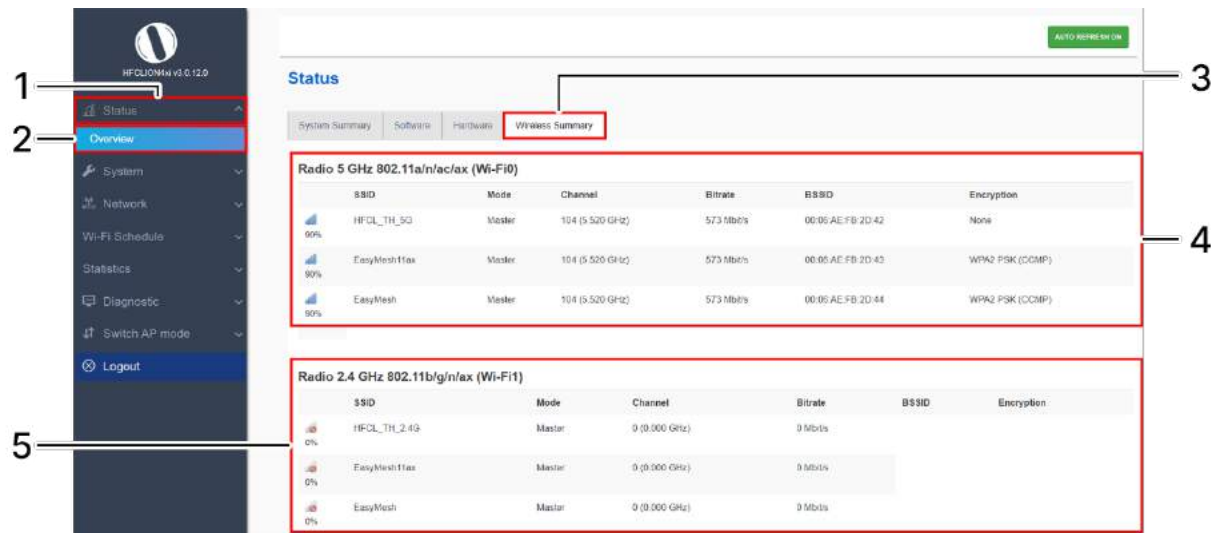
Figure 18: Basic layout of the system wireless screen

Follow the steps given below to view the system wireless summary:

Table 9: List of information displayed in the system wireless screen

Callout	Name	Description
1.	Status	Click on the "Status" dropdown
2.	Overview	Click on "Overview" option
3.	Wireless Summary	Click on "Wireless Summary" option
4.	SSID at 5 GHz	Displays all SSIDs radiating at 5 GHz radio along with some basic information in the respective information columns
5.	SSID at 2.4 GHz	Displays all SSIDs radiating at 2.4 GHz radio along with some basic information in the respective information columns

9   System maintenance screen

The maintenance activities of the respective access point are executed from this screen. The list of options available for the user is given below:

1. System general and log settings
2. Admin password configuration
3. Backup/Flash Firmware
4. Reboot
5. Factory Reset

9.1   System general settings

The user can configure the basic aspects of the respective access point, like its hostname and the timezone. A basic overview of the screen is given below:
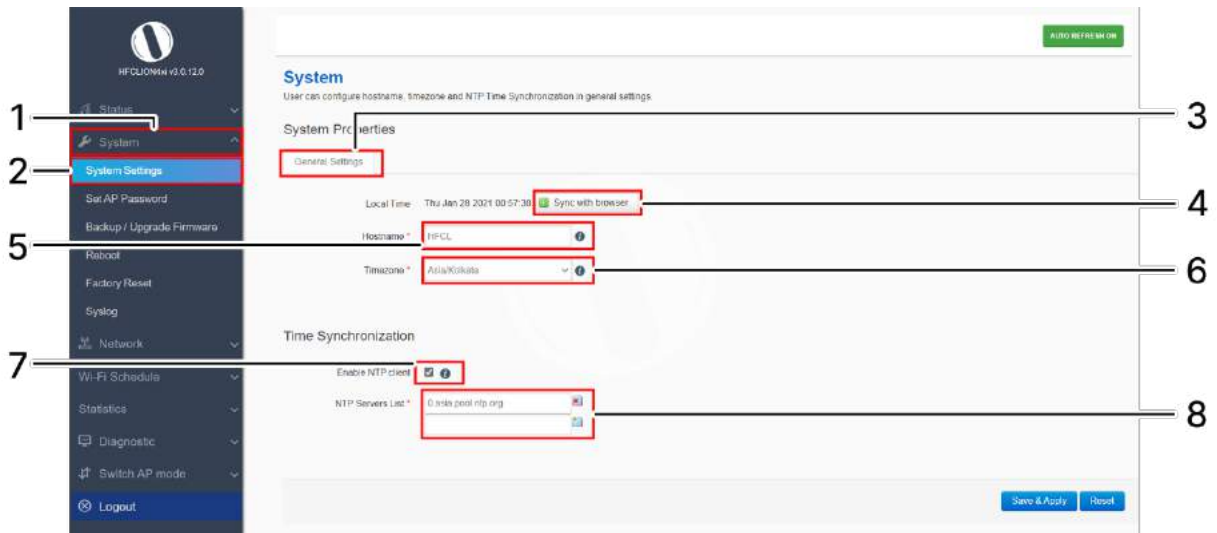
Figure 19: Basic overview of the system general settings screen for thick AP

Follow the steps given below and configure the system general settings for the thick AP:

Table 10: List of actions to configure the system general settings for thick AP

Callout	Name	Description
1.	System	Click on "System" dropdown
2.	System Settings	Click on "System Settings" option
3.	General Settings	Click on "General Settings" option
4.	Local Time	Displays the local date and time of the region. The user can click on "Sync with browser" option to sync the date and time
5.	Host Name	Enter the "Hostname". The same will be reflected in the system summary of status overview screen

Callout	Name	Description
6.	Time Zone	Select the respective "Timezone" from the dropdown list. It represents the region of the globe that observes a uniform standard time for legal, commercial, and social purposes. The date and time of the respective timezone will be reflected in the system summary of status overview screen.
7.	Time sync/ NTP	Click on the check box and enable or disable the NTP client
8.	NTP Server candidates	Click on the + icon and add multiple servers

Click on "Save & Apply" to save the system admin password configuration or click "Reset" to configure the same again.

CONFIDENTIAL

9.3   Set Password for thick AP

This screen provides the user with options to change the default password for respective thick access point. The default username is "root" and the default admin password is "root".

A basic overview of the screen is given below:

Figure 20: Basic overview of the system admin password configuration screen for thick AP

Follow the steps given below and configure the system admin password for the thick AP:

Table 11: List of actions to configure the password for thick AP

Callout	Name	Description
1.	System	Click on "System" dropdown
2.	Set AP Password	Click on "Set AP Password" option
3.	Current Password	Enter the existing password
4.	New Password	Enter a new valid password
5.	Confirm Password	Enter the password again for confirmation

Click on "Save & Apply" to save the system admin password configuration or click "Reset" to configure the same again.

9.4   Backup/Flash Firmware

Downloading the configuration files at an external drive location and updating the configuration files from an external file is a common feature. It helps the user to keep a backup of different configuration files and even makes it easier to apply the same in multiple devices. The device supports dual firmware.

9.4.1   Generate Backup

Download the existing configuration of the device in a file with this option. The user can use this backup file and apply the same configuration again from "Upload configuration or backup" screen. This avoids configuration of each and every parameter again and again, if a similar configuration is already available in the backup files.

A basic overview of the Backup/Flash Firmware screen to generate the backup is given below:
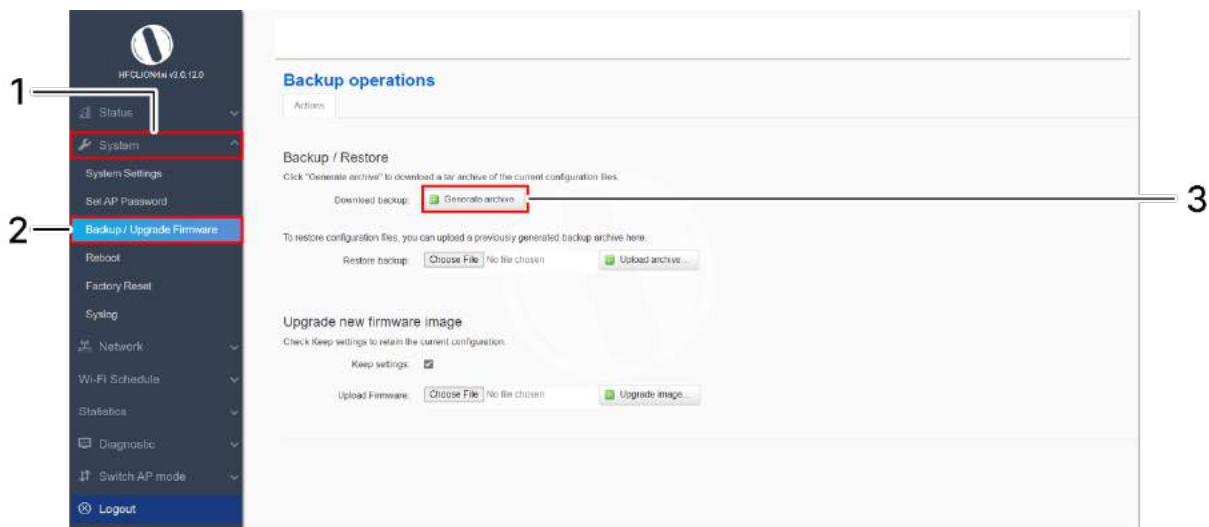
Figure 21: Basic overview of the backup/flash firmware screen to generate backup

Follow the steps given below to generate a backup of current device's configuration and files:

Table 12: List of actions to generate a backup of current device's configuration and files

Callout	Name	Description
1.	System	Click on "System" dropdown in navigation tollbar
2.	Backup/Upgrade Firmware	Click on "Backup/Upgrade Firmware" option
3.	Download backup	Click on "Generate archive" option to download the backup. The user can select the location in his computer to extract and save the configuration and system files.

9.4.2   Upload configuration or backup

Use an existing valid configuration file or device backup file and change the device parameters respectively from this screen. The user can apply similar configuration to multiple devices or can apply different type of configurations to various set of devices with minimal of the effort.

A basic overview of the Backup/Flash Firmware screen to upload data and configuration from an external file is given below:
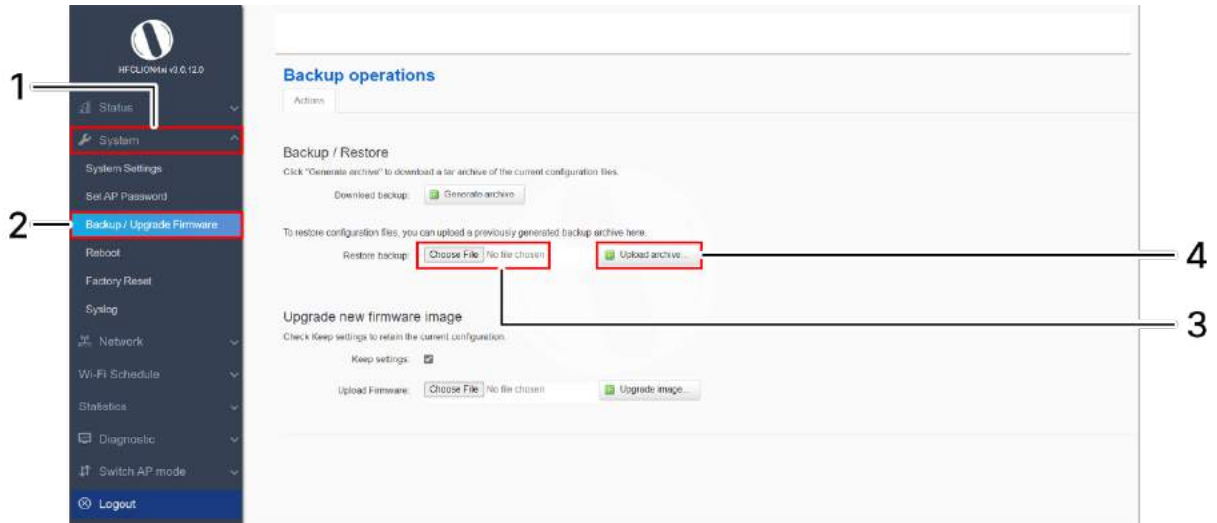
Figure 22: Basic overview of the backup/flash firmware screen to upload configuration

Follow the steps given below to upload data and configuration from an external file:

Table 13: List of actions to upload configuration from an external file

Callout	Name	Description
1.	System	Click on "System" dropdown in navigation tollbar
2.	Backup/Upgrade Firmware	Click on "Backup/Upgrade Firmware" option
3.	Browse/Restore backup	Click on "Chose File" option and select the file in your computer to restore the backup file or any other valid configuration file
4.	Restore backup	Click on "Upload archive" option to apply the configurations from selected file

9.4.3   Upgrade firmware

The firmware is stored in the flash memory and can be updated with new versions to include new features or to modify the existing one. This AP has two partitions. The firmware version is always uploaded in the alternate partition to keep the current firmware image restored which is located in the current partition of access point. When we upgrade new firmware, the existing firmware will become backup firmware. If any issues found in new firmware, the backup firmware will be booted.

Save the software file in system drive of your laptop or system. Refer the image below:
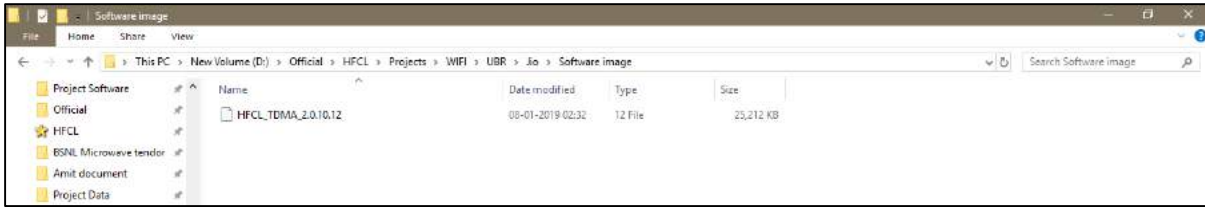
Figure 23: Software file in the system drive

In the above figure, the software file is saved in the "D" drive.

A basic overview of the Backup/Flash Firmware screen to upgrade the firmware from an external file is given below:
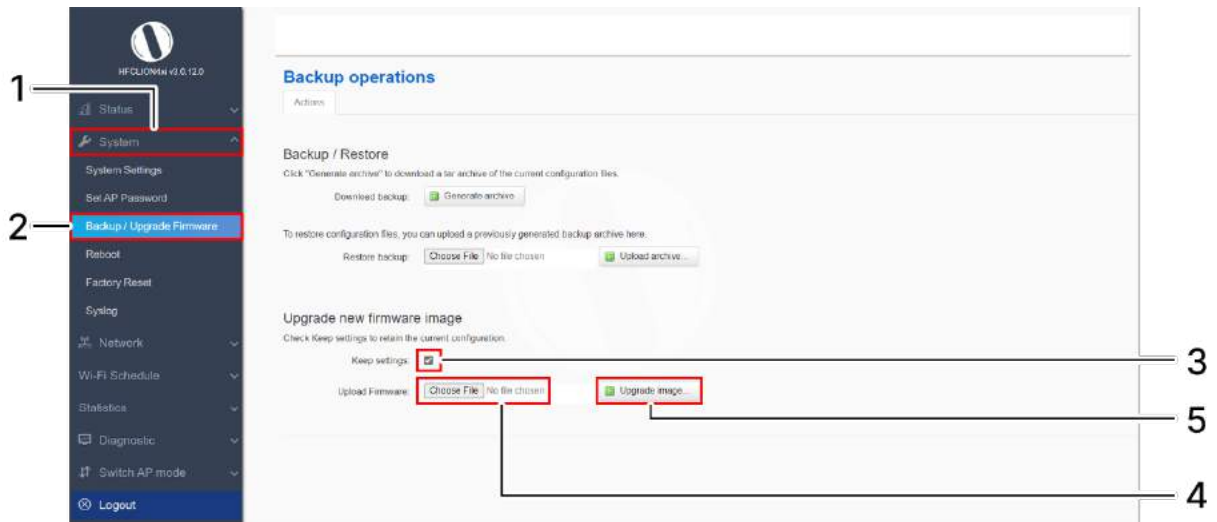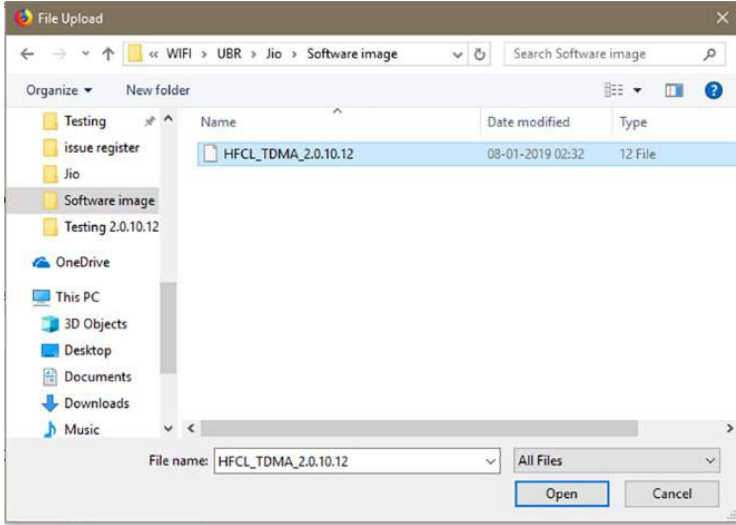
Figure 24: Basic overview of the backup/flash firmware screen to upgrade the firmware

Follow the steps given below to upgrade the firmware from an external file:

Table 14: List of actions to upgrade the firmware from an external file

Callout	Name	Description
1.	System	Click on "System" dropdown in navigation tollbar
2.	Backup/Upgrade Firmware	Click on "Backup/Upgrade Firmware" option
3.	Selection box/Keep settings	Click on "Selection box" to retain the existing device configuration (or) deselect the "Selection box" to discard

Callout	Name	Description
		the same while updating the firmware of the device with a new version.
4.	Browse/Image	Click on "Browse" option. A popup window will appear on the screen. Go to the respective folder of software file and select the sysupgrade-compatible image to replace the running firmware. Refer image below.

Click on open, once the compatible images is selected.

Callout	Name	Description
5.	Upgrade Image	Click on "Upgrade image" to upload a sysupgrade-compatible imagec a`1

It will show a new page, which will have checksum, file size and other information. Click on Proceed after checking software version.

9.5   Reboot

Reboot restarts the device with existing configuration. We can change the firmware when the device is rebooted with different partitions. Based on the selected partition, the corresponding firmware will be loaded into the device as working firmware

A basic overview of the Reboot screen is given below:
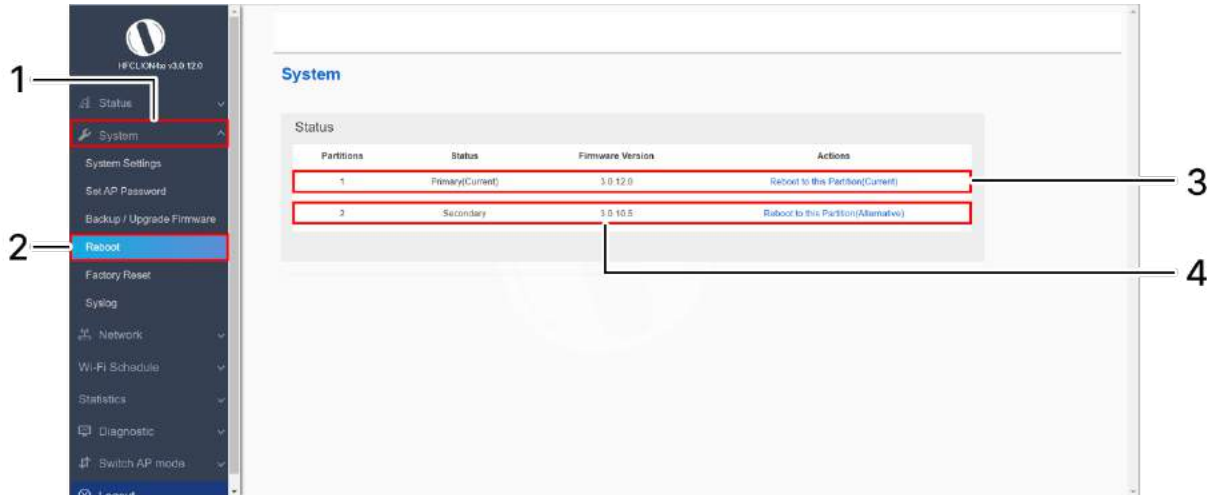
Figure 25: Basic overview of the reboot screen

Follow the steps given below and reboot the AP:

Table 15: List of actions to reboot the AP

Callout	Name	Description
1.	System	Click on "System" dropdown in navigation tollbar
2.	Reboot	Click on "Reboot" option
3.	Reboot to Current partition	Click on "Reboot to Current partition" option. Device will boot from current partition, and the firmware version present in the current partition will be in use
Or		
4.	Reboot to Alternate partition	Click on "Reboot to alternate partition" option. Device will boot from alternate partition, and the firmware version present in the alternate partition will be in use. The firmware upgrade always happen on alternate partition. Use this option and reboot to the latest uploaded firmware version

9.6   Factory Reset

The device has factory assigned settings and configurations on deployment. The user can set the device to the same from this screen. The device will be configured back to factory settings and the existing settings and configurations will be discarded. It is recommended to take backup before setting the device to factory reset.

A basic overview of the Factory Reset screen is given below:
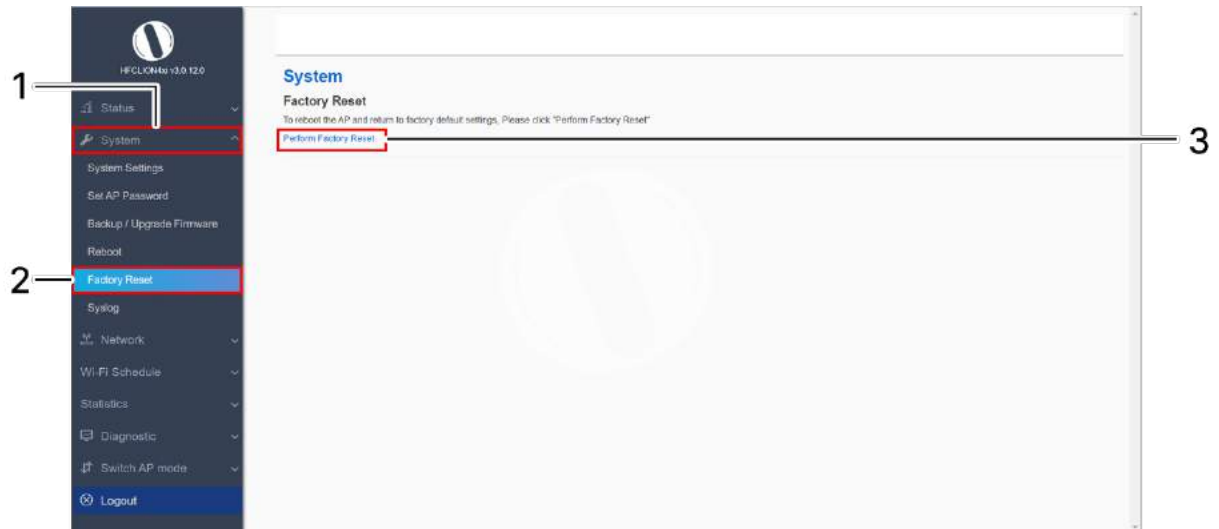
Figure 26: Basic overview of the factory reset screen

Follow the steps given below and factory reset the access point:

Table 16: List of actions to factory reset the access point

Callout	Name	Description
1.	System	Click on "System" dropdown in navigation toolbar
2.	Factory Reset	Click on "Factory Reset" option
3.	Perform Factory Reset	Click on "Perform Factory Reset" option to factory reset the respective access point

9.7   System log settings

If user wants to see the back-end logs or if user faces any issue, logs relevant to the AP's application software are populated in the "Diagnostic/System Log" screen for monitoring purpose. The same can be uploaded to an external server and the configuration for the same is performed in this screen. Event messages or corresponding messages will be sent to the logging server based on the configured log level.0

A basic overview of the screen is given below:

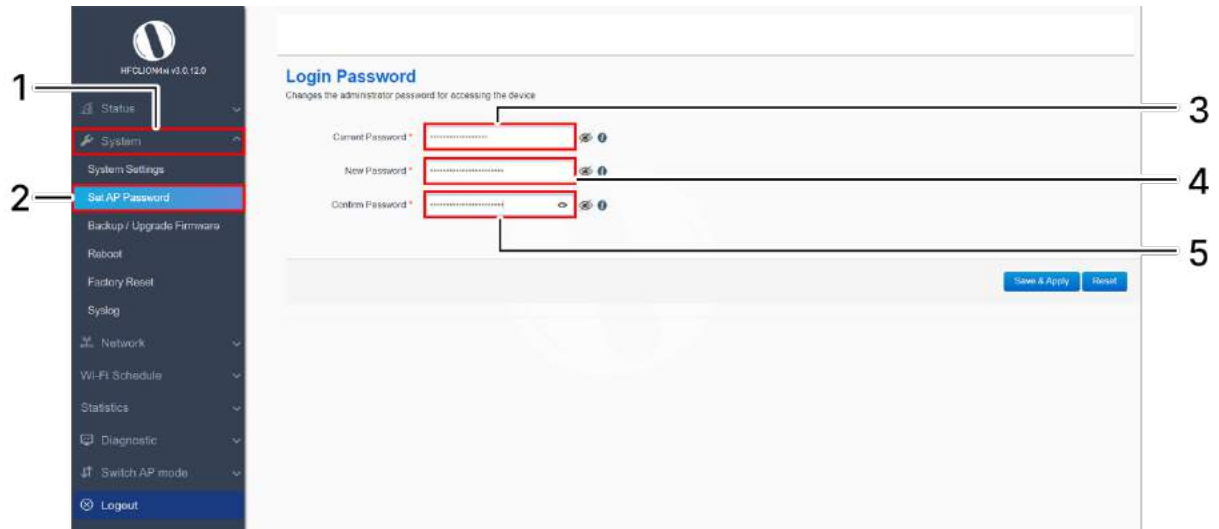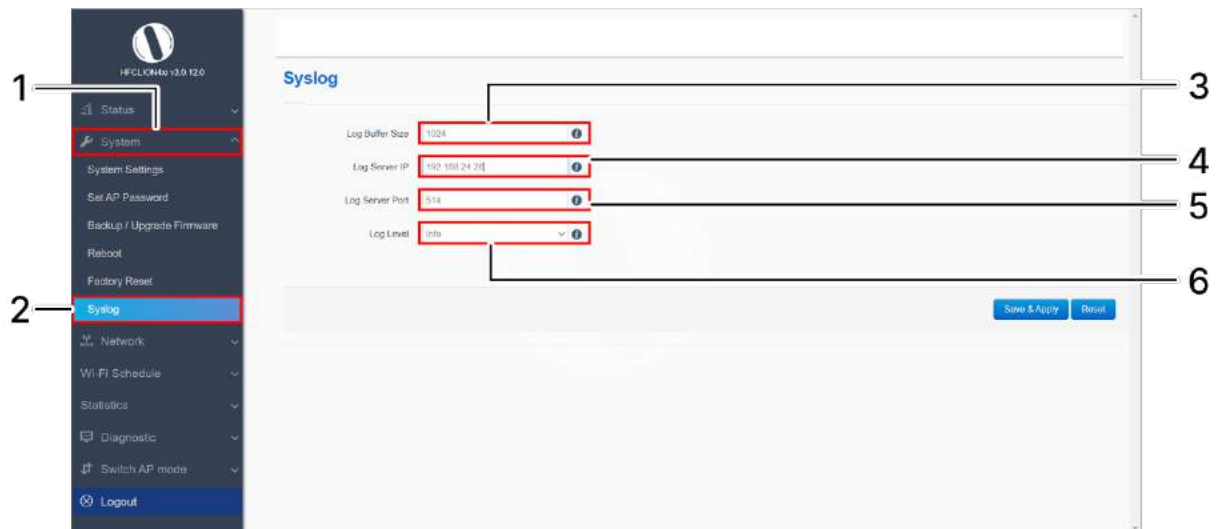*Figure 27: Basic overview of the system general settings screen for thick AP*

Follow the steps given below and configure the system general settings for the thick AP:

Table 17: List of actions to configure the system general settings for thick AP

Callout	Name	Description
1.	System	Click on "System" dropdown
2.	Syslog	Click on "Syslog" option
3.	Log Buffer Size	Allocate the size for the log file. Once the file size has reached to its limit a new log file will be generated
4.	External system log server	Enter the "External system log server" address. The system logs are uploaded to the external server on regular interval if the external server is specified with this option
5.	External system log server port	Enter the "External system log server port" number
6.	Log output level	Select the "Log output level" from the dropdown list (Debug/Info/Notice/Warning/Error/Critical/Alert/Emergency). Categorization of the system logs is specified in the backend. The selection of "Log output level" determines the type of logs to be displayed in system log screen. The "Debug" option shows all of the system logs. E.g.: If "Debug" is selected, all logs from

Callout	Name	Description
		debug to emergency will be logged and if "Notice" is selected, logs from Notice to Emergency will be logged

Click on "Save & Apply" to save the system admin password configuration or click "Reset" to configure the same again.

10   Network interfaces of thick AP

A basic overview of the network interface screen for thick AP is given below:
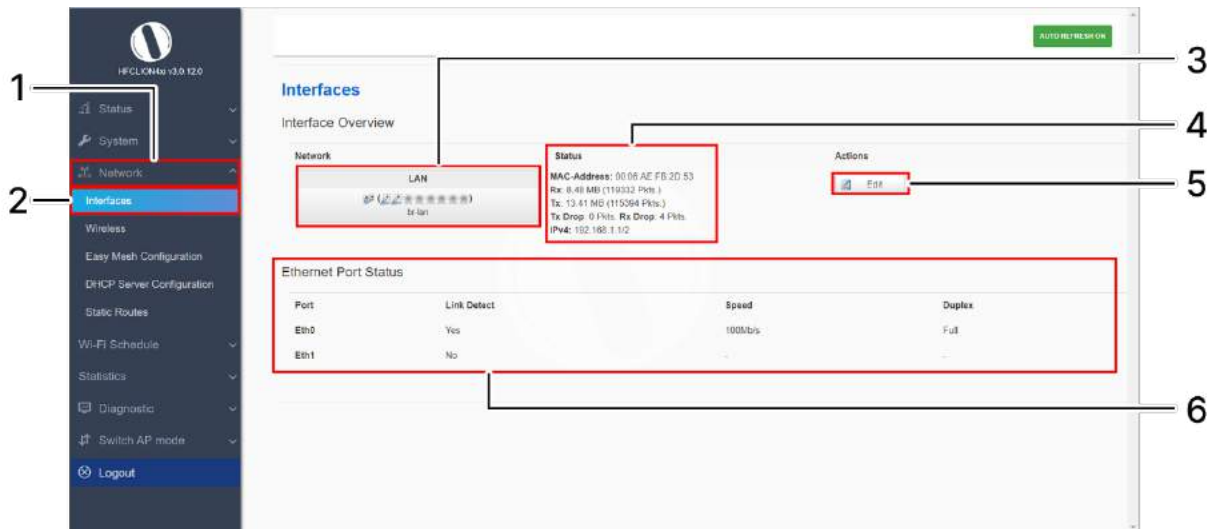
Figure 28: Basic overview of the interface configuration screen for thick AP

Follow the steps given below to view/edit the interface configuration of thick AP:

Table 18: List of actions to view/edit the network configuration of thick AP

Callout	Name	Description
1.	Network	Click on "Network" dropdown
2.	Interfaces	Click on "Interfaces" option
3.	Network/Interface overview	Displays the type of network interface available in the device. The above figure shows the LAN interface overview
4.	Status	Displays the status of the LAN interface with the respect to the parameters shown in above figure
5.	Edit	Click on "Edit" option to configure the LAN-interface settings
6.	Ethernet Port Status	Displays the port status of the respective device

The user can click on "edit" option to further modify the following configurations:

1.   General setup

CONFIDENTIAL

10.1 General Network interface setup configuration for thick AP

The default IP address of the access point is set to 192.168.1.1. The user can change the current static IP address of the device from this screen. DHCP client (DHCP client or DHCPv6 client) option is to get the dynamic IP address from reachable DHCP server in the network. Once the protocol is set to DHCPv4 client or DHCPv6 client, the device will automatically get the IP address (IPv4 or IPv6) from the DHCP server.

Click on the "Edit" option in interface screen as shown in "Figure 28: Basic overview of the interface configuration screen for thick AP". A basic overview of the network interface setup configuration screen to switch network protocol is given below:
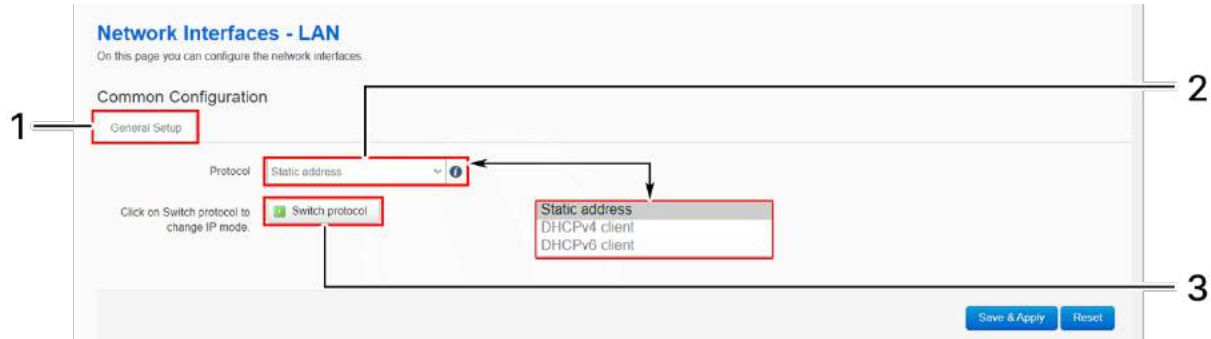
Figure 29: Basic overview of the network interface setup configuration screen to switch protocol for thick AP

Follow the steps given below to switch network protocol:

Table 19: List of actions to switch network protocol for thick AP

Callout	Name	Description
1.	General Setup	Click on "General Setup" option
2.	Protocol	Select the protocol desired protocol from the dropdown list (Static address/DHCPv4 client/DHCPv6 client)
3.	Really switch protocol	Click on "Switch protocol" to confirm the protocol switch

10.1.1   Static IP configuration for thick AP

The default IP address of the access point is set to 192.168.1.1. User can change the default IP address with an unused IP address. Refer "Figure 29: Basic overview of the network interface setup configuration screen to switch protocol for thick AP" and set the protocol to static address.

Refer the figure below to provide the static address parameters:
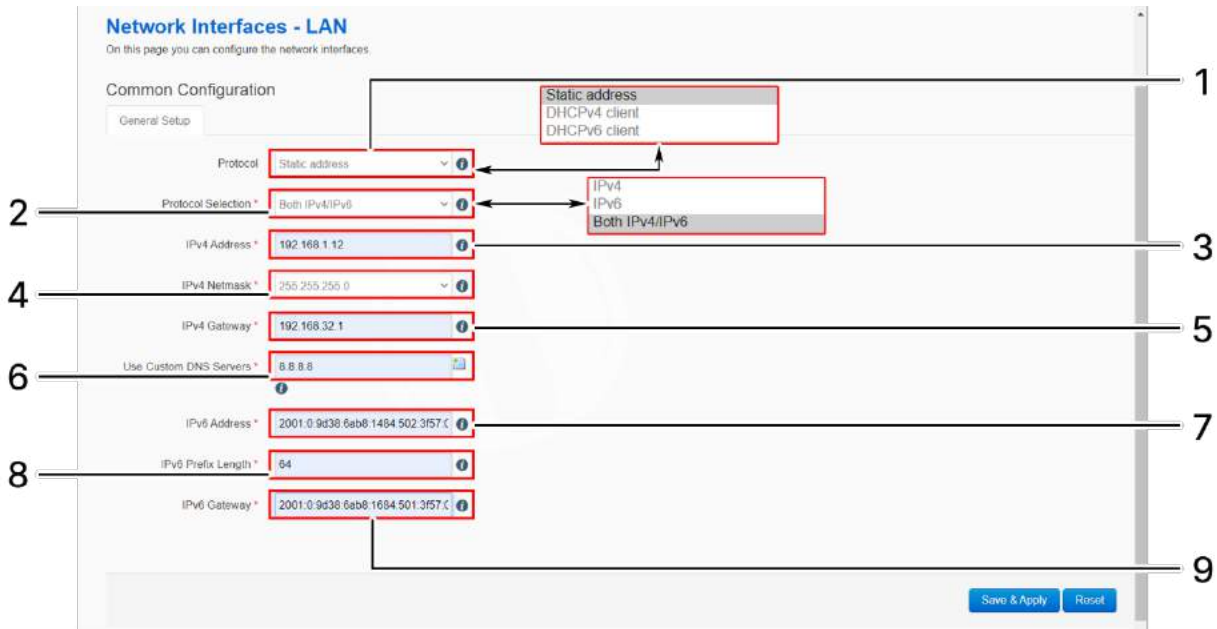
Figure 30: Basic overview of static address parameters for general network interface setup for thick AP

Follow the steps given below to provide static address parameters for thick AP:

Table 20: List of actions to provide static address parameters for thick AP

Callout	Name	Description
1.	Protocol	The protocol is set to ""Static address". Enter the following parameters for the same
2.	Protocol Selection	Set the static address protocol to IPv4/IPv6/Both IPv4 & IPv6. Below parameters are shown with respect to IPv4 & IPv6 protocol selection
3.	IPv4 address	Enter the "IPv4 address". This is a unique address of the Host/Device eg.192.168.100.10
4.	IPv4 netmask	Enter the "IPv4 netmask". This specifies the number of bits for network part and host part e.g.255.255.255.0
5.	IPv4 gateway	Enter the "IPv4 gateway". Gateway address is given to reach other network device e.g.192.168.100.254
6.	Use custom DNS servers	Enter the "DNS server". Click on add icon to add multiple DNS servers. DNS server is to resolve the transition of domain name to IP and IP to domain name

Callout	Name	Description
7.	IPv6 address	Enter the "IPv6 address". Unique address of the Host/Device e.g.2001:11::100
8.	IPv6 prefix length	Specify the prefix length for IPv6 address. Specifies the number of bits that belong to network part. The prefix-length specifies a range of devices e.g. IPv6 prefix length = 64 means range of IP addresses between 2001:0DB8:ABCD:0012:0000:0000:0000:0000 and 2001:0DB8:ABCD:0012:FFFF:FFFF:FFFF:FFFF.
9.	IPv6 gateway	Enter the "IPv6 gateway". Gateway address is given to reach other network device e.g.2001:11::1

Click "Save & Apply" to save the general network setup configuration or click "Reset" to configure the same again.

10.1.2   DHCPv4 client configuration for thick AP

If the protocol is set to DHCPv4 client, the device will automatically get the IPv4 address from the DHCP server. Refer "Figure 29: Basic overview of the network interface setup configuration screen to switch protocol for thick AP" and set the protocol to DHCPv4 client.

Refer the figure below and switch the protocol to DHCPv4 client for thick AP:
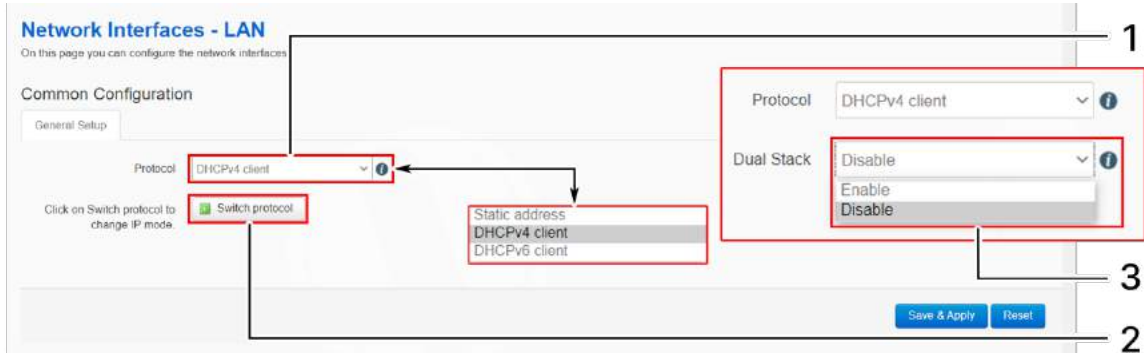
Figure 31: Basic overview of network interface screen to set the protocol to DHCPv4 for thick AP

Follow the steps given below to set the protocol to DHCPv4 for thick AP:

Table 21: List of actions to set the protocol to DHCPv4 for thick AP

Callout	Name	Description
1.	Protocol	Set the protocol from the dropdown list (Static address/DHCPv4 client/DHCPv6 client) to DHCPv4
2.	Really switch protocol	Click on "Switch protocol" to confirm the protocol switch
3.	Dual Stack	Once the protocol switch is confirmed, the user can enable/disable the dual stack option. If enabled, The device will be allocated with both IPv4 and IPv6 address through the DHCP server

Click "Save & Apply" to save the general network setup configuration or click "Reset" to configure the same again.

10.1.3   DHCPv6 client configuration for thick AP

If the protocol is set to DHCPv6 client, the device will automatically get the IPv6 address from the DHCP server. Refer "Figure 29: Basic overview of the network interface setup configuration screen to switch protocol for thick AP" and set the protocol to DHCPv6 client.

Refer the figure below and switch the protocol to DHCPv6 client for thick AP:
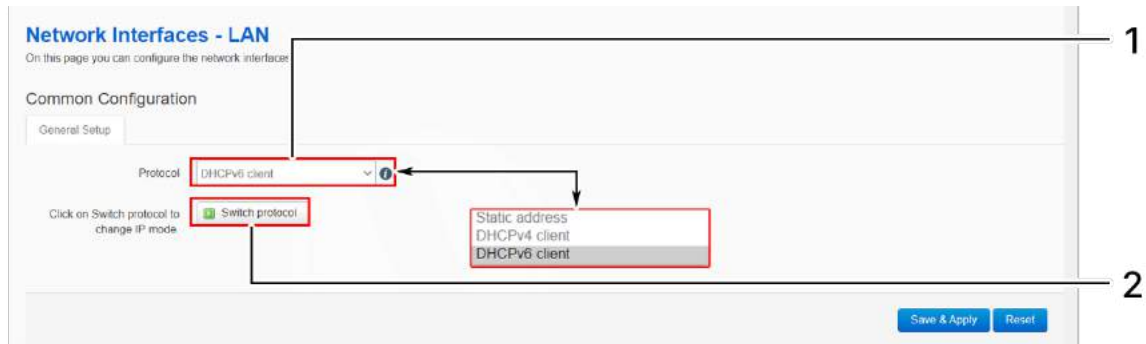
Figure 32: Basic overview of network interface screen to set the protocol to DHCPv6 for thick AP

Follow the steps given below to set the protocol to DHCPv6 for thick AP:

Table 22: List of actions to set the protocol to DHCPv6 for thick AP

Callout	Name	Description
1.	Protocol	Set the protocol from the dropdown list (Static address/DHCPv4 client/DHCPv6 client) to DHCPv6
2.	Really switch protocol	Click on "Switch protocol" to confirm the protocol switch

Click "Save" to save the general network setup configuration or click "Reset" to configure the same again.

10.2 Network/Wireless/Radio and SSID configuration of thick AP

The wireless configuration screen of thick AP GUI enables the user to view and configure radio and SSID parameters. Multiple SSID can be added separately for 2.4 and 5 GHz radio. Radio configuration remains same for all SSIDs operating at the respective 2.4 and 5 GHz radio. All clients associated with respective SSID are also listed in a tabular form in this screen along with some basic information.

A basic overview of the wireless configuration screen for thick AP is given below:
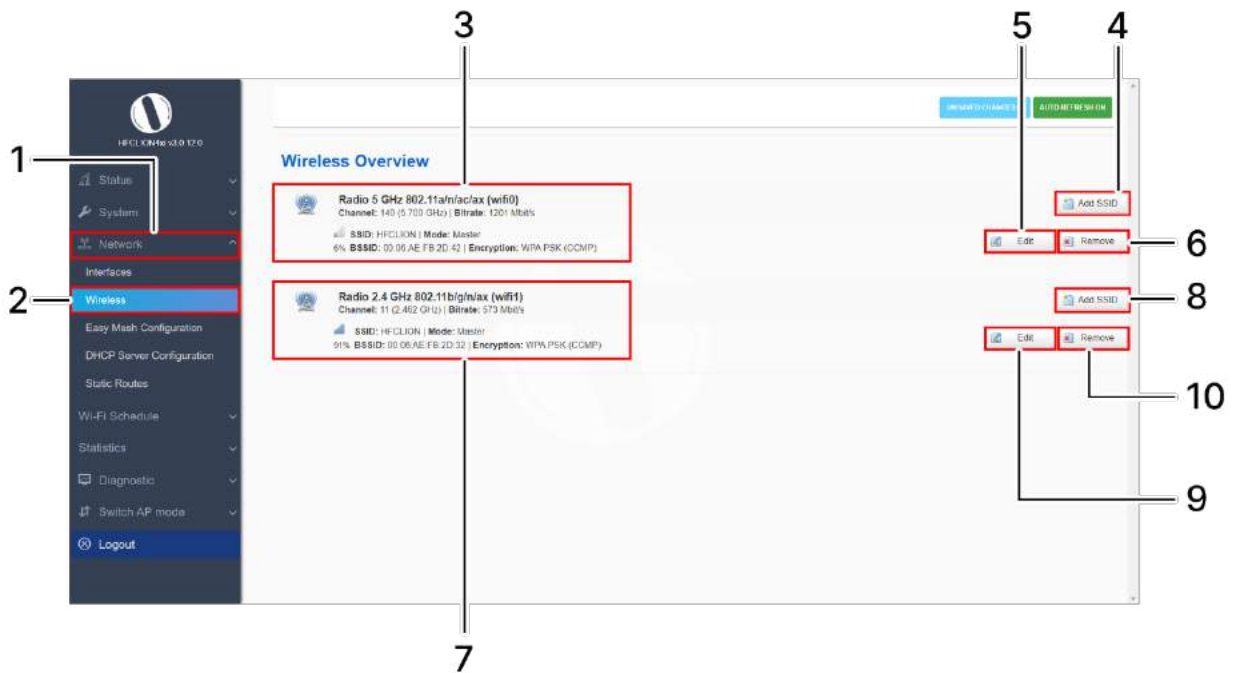
Figure 33: Basic overview of the wireless configuration screen for thick AP

Follow the steps given below to view the wireless configuration of thick AP:

Table 23: List of actions to view the wireless configuration of thick AP

Callout	Name	Description
1.	Network	Click on "Network" dropdown
2.	Wireless	Click on "Wireless" option
3.	5 GHz overview	Displays the overview of 5 GHz radio along with the list of associated SSIDs as shown in the above figure
4.	Add SSID/Radio Configuration	Click on the "Add" option to configure a new SSID or to update the radio configuration parameters at 5 GHz
5.	Edit SSID	Click on "Edit" option to modify the parameters of respective SSID configuration at 5 GHz
6.	Remove SSID	Click on "Remove" option to delete the respective SSID at 5 GHz

Callout	Name	Description
7.	2.4 GHz overview	Displays the overview of 2.4 GHz radio along with the list of associated SSIDs as shown in the above figure
8.	Add SSID/Radio Configuration	Click on the "Add" option to configure a new SSID or to update the radio configuration parameters at 2.4 GHz
9.	Edit SSID	Click on "Edit" option to modify the parameters of respective SSID configuration at 2.4 GHz
10.	Remove SSID	Click on "Remove" option to delete the respective SSID at 2.4 GHz

10.2.1   5 GHz radio configuration

This screen provides the user with options to configure the 5 GHz radio parameters such as channel bandwidth, respective channel or the channel selection process, and the power for the radio signal transmission. Refer the "Figure 33: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (4) to configure 5 GHz radio parameters.

A basic overview of the 5 GHz radio configuration screen is given below:
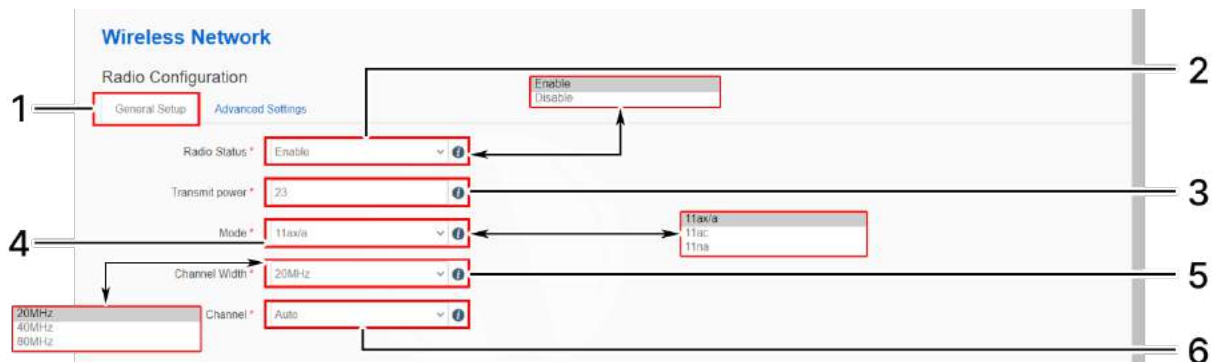
Figure 34: Basic overview of the 5 GHz radio configuration screen

Follow the steps given below and for 5 GHz radio configuration of thick AP:

Table 24: List of actions for 5 GHz radio configuration of thick AP

Callout	Name	Description
1.	General Setup	Click on "General Setup" option
2.	Radio Status	Enable or disable the 5 GHz radio with this option
3.	Tx Power (dBm)	Enter the "Tx Power" value. The wireless radio signal will be transmitted with the specified Tx power value. The user can set the Tx power value from the range of 6 dBm to 30 dBm
4.	Mode	Select the radio operating mode from the dropdown list (802 11a/ac/a+n/ax). Channel width and channel list varies with respect to the selected mode (802 11a/ac/a+n/ax)

CONFIDENTIAL

Callout	Name	Description
5.	Channel Width	Select the "Channel Width" from the dropdown list (20 MHz/40 MHz/80 MHz)
6.	Channel	Select the "Channel" from the dropdown list. The device will choose the channel by itself, if "auto" channel is selected. Channels available in the dropdown list are: 36/40/44/48/52/56/60/64/149/153/157/161/165/169/ 173

Click "Save & Apply" to save the 5 GHz radio configuration of thick AP or click "Reset" to configure the same again.

10.2.2   2.4 GHz radio configuration

This screen provides the user with options to configure the 2.4 GHz radio parameters such as channel bandwidth, respective channel or the channel selection process, and the power for the radio signal transmission. Refer the "Figure 33: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (8) to configure 2.4 GHz radio parameters.

A basic overview of the 2.4 GHz radio configuration screen is given below:
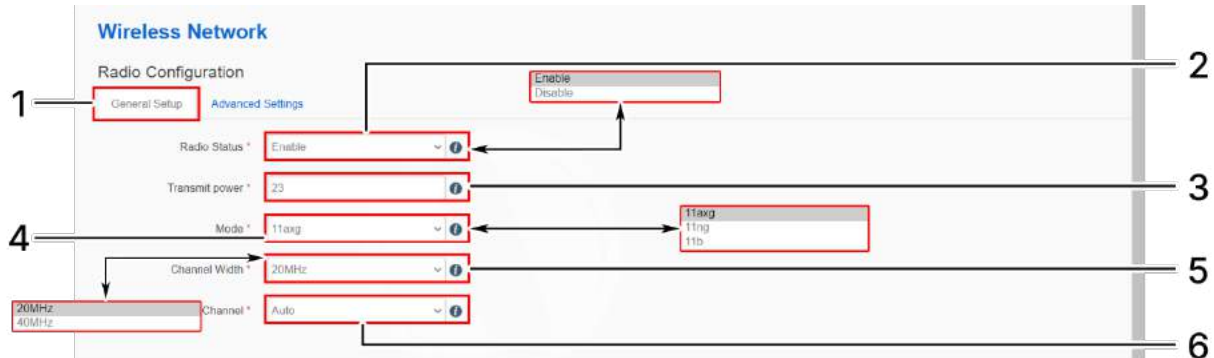
Figure 35: Basic overview of the 2.4 GHz radio configuration screen

Follow the steps given below and for 2.4 GHz radio configuration of thick AP:

Table 25: List of actions for 2.4 GHz radio configuration of thick AP

Callout	Name	Description
1.	General Setup	Click on "General Setup" option
2.	Radio Status	Enable or disable the 2.4 GHz radio with this option
3.	Tx Power (dBm)	Enter the "Tx Power" value. The wireless radio signal will be transmitted with the specified Tx power value. The user can set the Tx power value from the range of 6 dBm to 30 dBm
4.	Mode	Select the radio operating mode from the dropdown list (802 11b/ng/axg). Channel width and channel list varies with respect to the selected mode (802 11b/ng/axg)
5.	Channel Width	Select the "Channel Width" from the dropdown list (20 MHz/40 MHz)
6.	Channel	Select the "Channel" from the dropdown list. The device will choose the channel by itself, if "auto" channel is selected. For 20 MHz channel width, available channels are: 1/2/3/4/5/6/7/8/9/10/11/12/13

Click "Save & Apply" to save the 2.4 GHz radio configuration of thick AP or click "Reset" to configure the same again.

10.2.3   Advanced radio configuration (2.4 GHz and 5 GHz)

This screen provides the user with options to configure the advanced radio parameters (2.4 GHz and 5 GHz) such as country code and Tx/Rx chain mask. Refer the "Figure 33: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (8) for 2.4 GHz or Add SSID/Radio Configuration option (4) for 5 GHz to configure advanced radio parameters.

A basic overview of the advanced radio parameters (2.4 GHz and 5 GHz) configuration screen is given below:
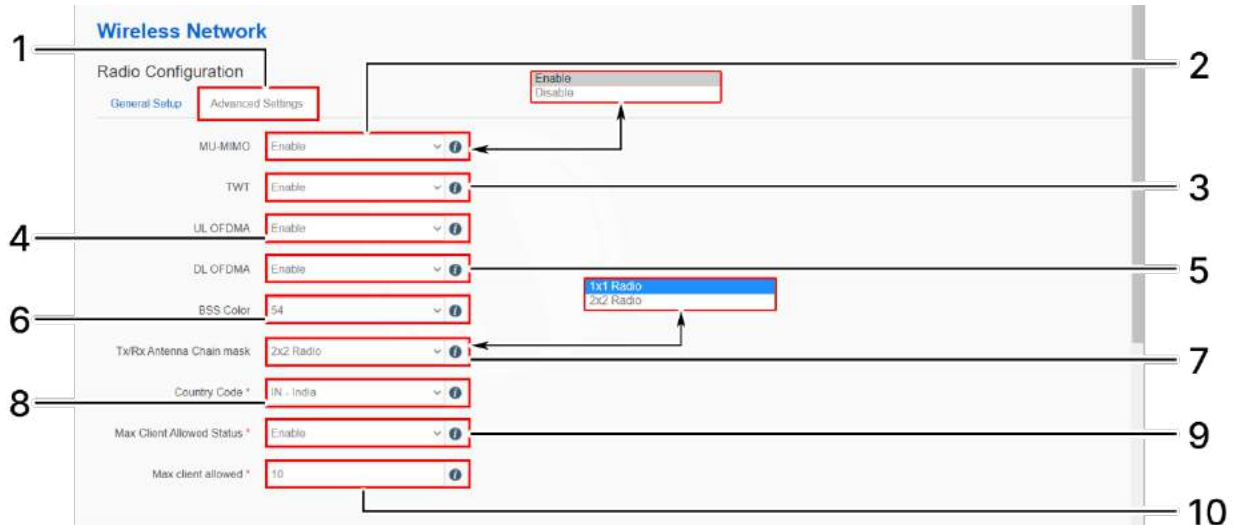
Figure 36: Basic overview of the advanced radio parameters (2.4 GHz and 5 GHz) configuration screen

Follow the steps given below for advanced radio parameters (2.4 GHz and 5 GHz) configuration of thick AP:

Table 26: List of actions for advanced radio parameters (2.4 GHz and 5 GHz) configuration of thick AP

Callout	Name	Description
1.	Advanced Settings	Click on "Advanced Settings" option
2.	MU-MIMO	Enable/Disable the MU-MIMO feature of the radio
3.	TWT	Enable/Disable the target wake time feature from the radio
4.	UL OFDMA	Enable/Disable the UL OFDMA feature of the radio
5.	DL OFDMA	Enable/Disable the DL OFDMA feature of the radio
6.	BSS Color	Allocate a BSS color code from the dropdown list
7.	Tx/Rx Antenna Chain mask	Select the chain mask from the dropdown list (1x1/2x2)
8.	Country Code	Select the country code from the dropdown list. Channels are listed in accordance to the selected country
9.	Max Client Allowed Status	Enable/Disable the max client restriction with this option
10.	Max Client Allowed	Define the number of clients allowed to connect with the respective radio

Click "Save & Apply" to save the advanced radio parameters (2.4 GHz and 5 GHz) configuration of thick AP or click "Reset" to configure the same again.

10.2.4   SSID configuration

Refer the "Figure 33: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (8) for 2.4 GHz or Add SSID/Radio Configuration option (4) for 5 GHz to configure new SSIDs. Click on Edit option (9) for 2.4 GHz or Edit option (5) for 5 GHz to edit existing SSIDs. This screen provides the user with options to configure the SSID operating at both 2.4 and 5 GHz radio. The SSID configuration parameters are further categorized as follows:

1. General setup
2. Wireless Security
3. MAC Filter
4. Advanced Settings

10.2.4.1   SSID/General setup (2.4 GHz and 5 GHz)

Refer the "Figure 33: Basic overview of the wireless configuration screen for thick AP" and click on Add SSID/Radio Configuration option (4) to configure 5 GHz radio parameters or click on Add SSID/Radio Configuration option (8) to configure 2.4 GHz radio parameters. A basic overview of the screen to configure general SSID parameters is given below:

Figure 37: Basic overview of the screen to configure general SSID parameters

Follow the steps given below and configure the general SSID parameters:

Table 27: List of actions to configure the general SSID parameters

Callout	Name	Description
1.	General Setup	Click on "General Setup" option
2.	VAP Status	Enable or disable the VAP with this option. Once disabled, the SSID will not be available in the search anymore.
3.	SSID	Enter a unique name for the SSID
4.	Mode	By default the SSID mode is set to "Access Point". This type of SSID is used by the clients to connect with the respective access point
5.	Network	Select the network interface from the dropdown list

Callout	Name	Description
6.	Hide SSID	Enable/Disable SSID broadcast with this option. Once disabled, the SSID will not be available in the search anymore. The user can still associate with the SSID if valid authenticated credentials are provided

Click "Save & Apply" to save the general SSID configuration of thick AP or click "Reset" to configure the same again.

10.2.4.2   SSID/Wireless security (2.4 GHz and 5 GHz)

By default the wireless security is set to "No Encryption", and few of the other options provided to change the encryption accordingly are as follows:

1. **No Encryption:** Any device can connect to the network. Not recommended.
2. **WPA-PSK(Wi-Fi Protected Access):** WPA is part of the wireless security standard (802.11i) standardized by the Wi-Fi Alliance and was intended as an intermediate measure to take the place of WEP while the 802.11 standard was being prepared. It supports TKIP/AES encryption. The personal authentication is the pre-shared key (PSK) that is an alphanumeric passphrase shared with the wireless peer.
3. **WPA2-PSK:** WPA2 is the implementation of security standard specified in the final 802.11i standard. It supports AES encryption and this option uses pre-shared key (PSK) based authentication.
4. **WPA-PSK/WPA2-PSK Mixed mode:** Allows both WPA and WPA2 clients to connect simultaneously using PSK authentication.
5. **WPA2-EAP:** Allows you to use WPA2 with RADIUS server authentication.
6. **WPA3-Enterprise:** Enterprise, governments, and financial institutions have greater security with WPA3-Enterprise. WPA3-Enterprise also offers an optional mode using 192-bit minimum-strength security protocols and cryptographic tools to better protect sensitive data.

10.2.4.2.1   Key based Wireless security Encryption

A basic overview of the screen to configure wireless security parameters of SSID is given below:

Figure 38: Basic overview of the screen to configure wireless security parameters of SSID

Follow the steps given below and configure the wireless security parameters of SSID:

Table 28: List of actions to configure the wireless security parameters of SSID

Callout	Name	Description
1.	Wireless Security	Click on "Wireless Security" option
2.	Encryption	Select the encryption protocol from the dropdown list (No Encryption/WPA-PSK/WPA2-PSK/ WPA-PSK /WPA2-PSK_Mixed_Mode/WPA3 Personal/WPA3 Personal Mixed /OWE (Opportunistic Wireless Encrypt)). No passphrase is needed in case of "Open" and "OWE (Opportunistic Wireless Encrypt)"type network authentication protocol

Callout	Name	Description
3.	Key	Enter a unique password for the SSID

Click "Save & Apply" to save the wireless security configuration of SSID or click "Reset" to configure the same again.

10.2.4.2.2   RADIUS based Wireless security Encryption

A basic overview of the screen to configure wireless security parameters of SSID is given below:

Figure 39: Basic overview of the screen to configure wireless security parameters of SSID (RADIUS)

Follow the steps given below and configure the wireless security parameters of SSID:

Table 29: List of actions to configure the wireless security parameters of SSID (RADIUS)

Callout	Name	Description
1.	Wireless Security	Click on "Wireless Security" option
2.	Encryption	Select the encryption protocol from the dropdown list (WPA2-EAP/WPA3 Enterprise/WPA3 Enterprise Transition/WPA3 SuiteB)
3.	RADIUS Authentication Server	Enter a valid IP address of the RADIUS Authentication Server
4.	RADIUS Authentication Port	Enter a valid port of the RADIUS Authentication Server
5.	RADIUS Authentication Secret	Enter a valid key for the authentication at RADIUS server
6.	RADIUS Accounting Server	Enter a valid IP address of the RADIUS Accounting Server
7.	RADIUS Accounting Port	Enter a valid port of the RADIUS Accounting Server
8.	RADIUS Accounting Secret	Enter a valid key for the authentication at RADIUS accounting server

Click "Save & Apply" to save the wireless security configuration of SSID or click "Reset" to configure the same again.

10.2.4.3   SSID/MAC filter (2.4 GHz and 5 GHz)

The user can add multiple MAC addresses with allow and deny policy and the same is mapped with respective SSID. A basic overview of the screen to configure the MAC filter for SSID configuration is given below:

Figure 40: Basic overview of the screen to configure the MAC filter for SSID configuration

Follow the steps given below and configure the MAC filter for SSID configuration:

Table 30: List of actions to configure the MAC filter for SSID configuration

Callout	Name	Description
1.	MAC-Filter	Click on "MAC-Filter" option
2.	MAC address filter	Click on the dropdown and disable or set the allow/deny policy for the MAC filter
3.	MAC List	Click on the dropdown and select the MAC address from the list or click on "Custom" to add the MAC address manually. Click on the "+" icon to add multiple MAC addresses

Click "Save & Apply" to save the MAC filter configuration or click "Reset" to configure the same again.

10.2.4.4   SSID/Advanced settings (2.4 GHz and 5 GHz)

A basic overview of the screen to configure the advanced parameters of SSID configuration is given below:

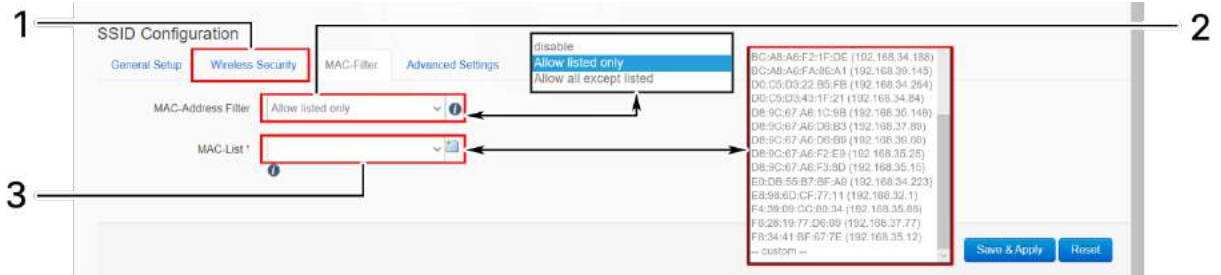*Figure 41: Basic overview of the screen to configure the advanced parameters of SSID configuration*

Follow the steps given below and configure the advanced parameters of SSID configuration:

Table 31: List of actions to configure the advanced parameters of SSID configuration

Callout	Name	Description
1.	Advanced Settings	Click on "Advanced Settings" option
2.	Client Isolation	Click on the check box and enable or disable the client isolation feature. If the feature is enabled, it prevents client to client communication
3.	802.11 r Fast Transition	Enable/Disable the L2 roaming to allow/restrict client roaming within the same SSID
4.	Mobility ID	Allocate a mobility ID from within the range of 0000 to FFFF. Maximum allowed length of the ID is restricted to 4
5.	RTS Status	Enable/Disable the RTS
6.	RTS Threshold	Set the RTS/CTS Threshold value. The supported range is between 256 to 2346
7.	CTS Protection Mode	Enable/Disable the CTS
8.	DTIM Interval	Specify the time to wake up the clients from sleep mode to receive traffic within the range of 1ms to 255ms
9.	Beacon Interval	Specify the time interval at which the beacon packets are to be transmitted within the range of 100ms to 300ms
10.	Wi-Fi Multimedia	Enable/Disable the Wi-Fi Multimedia option. It will control the upstream traffic flow from client to AP and downstream traffic flowing from AP to client device
11.	Max Client Limit	Assign the number of clients to be connected with the respective SSID within the range of 1 to 64
12.	Wi-Fi Multimedia Power Save	Enable/Disable the Wi-Fi Multimedia Power Save option
13.	VLAN Status	Enable/Disable the VLAN. By default VLAN ID will be set to 1
14.	VLAN ID	Set the VLAN ID within the range of 1 to 4094
15.	Option 82	Enable/Disable the option 82. It will add client VLAN ID to the option 82 field in case of IPv4
16.	Option 18	Enable/Disable the option 18. It will add client VLAN ID to the option 18 field in case of IPv6
17.	Rate Limit	Enable/Disable the rate limit. The rate limit can be set based on per VAP or client
18.	Upload Limit (Mbps)	Set the upload limit if rate limit is enabled
19.	Download Limit (Mbps)	Set the download limit if rate limit is enabled
20.	ATF Enable	Enable/Disable the ATF feature

Callout	Name	Description
21.	ATF Scheduling	Set the ATF scheduling to either "Fair Time Scheduling" or "Strict Time Scheduling"
22.	Air Time %	Set the air time between 10 to 100
23.	TX STBC	Enable/Disable the Tx space time block coding
24.	RXSTBC	Enable/Disable the Rx space time block coding
25.	Number of Spatial Streams	Set the number of spatial streams between 1 to 2
26.	NAS ID	Allocate a NAS ID. It is a combination of alphanumeric characters with maximum of 32 characters

Click "Save & Apply" to save the advanced parameters of SSID configuration or click "Reset" to configure the same again.

10.3 Network/EasyMesh configuration of thick AP

A wireless mesh network serves as a network of radio nodes organized in a mesh topology. All APs participating in mesh topology does not need to have a wired connection for backhaul connectivity and only one root AP serves that purpose.

Mesh configuration require access points to operate in two operating modes as follows:

1. **Controller AP:** Controller AP have wired connections, for example, Ethernet backhaul to a wired network and to cNMS.
2. **Agent AP:** Repeats wireless signals to extend range without being connected with cable to Access Point, or with clients.

Mesh configuration allows access points to connect with each other in mesh topology. An access point (Controller AP) is connected to the wired network with the use of wireless connections over the 802.11 radio backhaul and other agent access points act as repeaters in mesh topology. In case of a mesh node failure, the surrounding nodes automatically re-connect and resume service without downtime. Nodes identify the best next hop and connect with it automatically.

A basic overview of the mesh configuration screen for thick AP is given below:
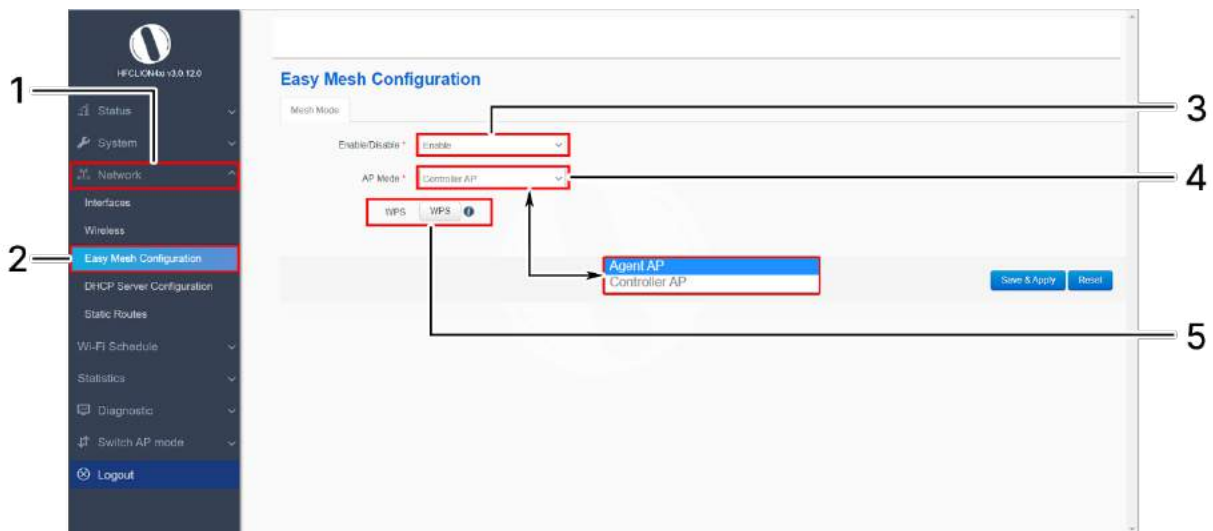
Figure 42: Basic overview of the mesh configuration screen for thick AP

Follow the steps given below to view the mesh configuration of thick AP:

Table 32: List of actions to view the mesh configuration of thick AP

Callout	Name	Description
1.	Network	Click on "Network" dropdown
2.	Easy Mesh Configuration	Click on "Mesh Configuration" option
3.	Mesh Mode	Enable or disable the EasyMesh mode. If enabled, provide the following parameters
4.	AP Mode	Select the contributing mode of the access point in the EasyMesh topology from the drop down list (Controller

Callout	Name	Description
		AP/Agent AP). If the AP mode is set to "Controller AP", make sure that the AP is connected to the wired network. Agent AP automatically connects to the controller AP if they are of the same vendor
5.	WPS	Click on this option to connect with an AP which belong to any other vendor. Make sure the "WPS" option is also enabled in the vendor AP and the AP supports EasyMesh configuration. This action lasts for only few seconds. Click on the "WPS" option again if the connection has not established within few seconds.

Click "Save & Apply" to save the advanced parameters of SSID configuration or click "Reset" to configure the same again.

10.4 DHCP server configuration of thick AP

The AP itself can act as a DHCP service provider for the connected clients and configuration for the same is executed from this screen. A basic overview of the screen to enable thick AP as DHCP server (IPv4) is given below:

Figure 43: Basic overview of the screen to enable thick AP as DHCP server (IPv4)

Follow the steps given below to enable thick AP as DHCP server (IPv4):

Table 33: List of actions to enable thick AP as DHCP server (IPv4)

Callout	Name	Description
1.	Network	Click on "Network" dropdown
2.	DHCP Server Configuration	Click on "DHCP Server Configuration" option
3.	DHCP Server	Enable the thick AP as DHCP server and enter the following parameters
4.	Protocol Selection	Set the protocol to IPv4 and provide the following parameters
5.	IPv4 Address	Enter the address in IPv4 format for the DHCP server
6.	IPv4 Netmask	Select the netmask from the dropdown list
7.	IPv4 Gateway	Enter the address in IPv4 format for the DHCP gateway
8.	Use Custom DNS Servers	Enter the IP address for DNS server. Click on add icon and multiple DNS servers
9.	Start IP Address	Enter a start IP address. The DHCP server assigns the new IP addresses to the clients from the defined start IP address
10.	End IP Address	Enter an end IP address. The DHCP server assigns the IP addresses to the clients till the defined end IP address

Callout	Name	Description
11.	Lease Time	Enter a value to set a limit on the lease time. New addresses will be assigned to the associated clients once the previous lease has expired as per the specified lease time

Click "Save & Apply" to enable thick AP as DHCP server or click "Reset" to configure the same again.

A basic overview of the screen to enable thick AP as DHCP server (IPv6) is given below:

Figure 44: Basic overview of the screen to enable thick AP as DHCP server (IPv6)

Follow the steps given below to enable thick AP as DHCP server (IPv6):

Table 34: List of actions to enable thick AP as DHCP server (IPv6)

Callout	Name	Description
1.	Network	Click on "Network" dropdown
2.	DHCP Server Configuration	Click on "DHCP Server Configuration" option
3.	DHCP Server	Enable the thick AP as DHCP server and enter the following parameters
4.	Protocol Selection	Set the protocol to IPv6 and provide the following parameters
5.	DHCPv6 Mode	Select the mode from the dropdown list (Stateless/Stateless+Stateful/Stateful)
6.	IPv6 Address	Enter the address in IPv6 format for the DHCP server
7.	IPv6 Prefix Length	Specify the prefix length for IPv6 address. Specifies the number of bits that belong to network part. The prefix-length specifies a range of devices

Callout	Name	Description
		e.g. IPv6 prefix length = 64 means range of IP addresses between 2001:0DB8:ABCD:0012:0000:0000:0000:0000 and 2001:0DB8:ABCD:0012:FFFF:FFFF:FFFF:FFFF.
8.	IPv6 Gateway	Enter the "IPv6 gateway". Gateway address is given to reach other network device e.g.2001:11::1
9.	Use Custom DNS Servers	Enter the IP address for DNS server. Click on add icon and multiple DNS servers
10.	Lease Time	Enter a value to set a limit on the lease time. New addresses will be assigned to the associated clients once the previous lease has expired as per the specified lease time

Click "Save & Apply" to enable thick AP as DHCP server or click "Reset" to configure the same again.

10.5 Static Routes

User can configure static routes and redirect packets to the destination network. A static route is a pre-determined pathway that a packet must travel to reach a specific host or network.

A basic overview of the static route configuration screen for thick AP is given below:
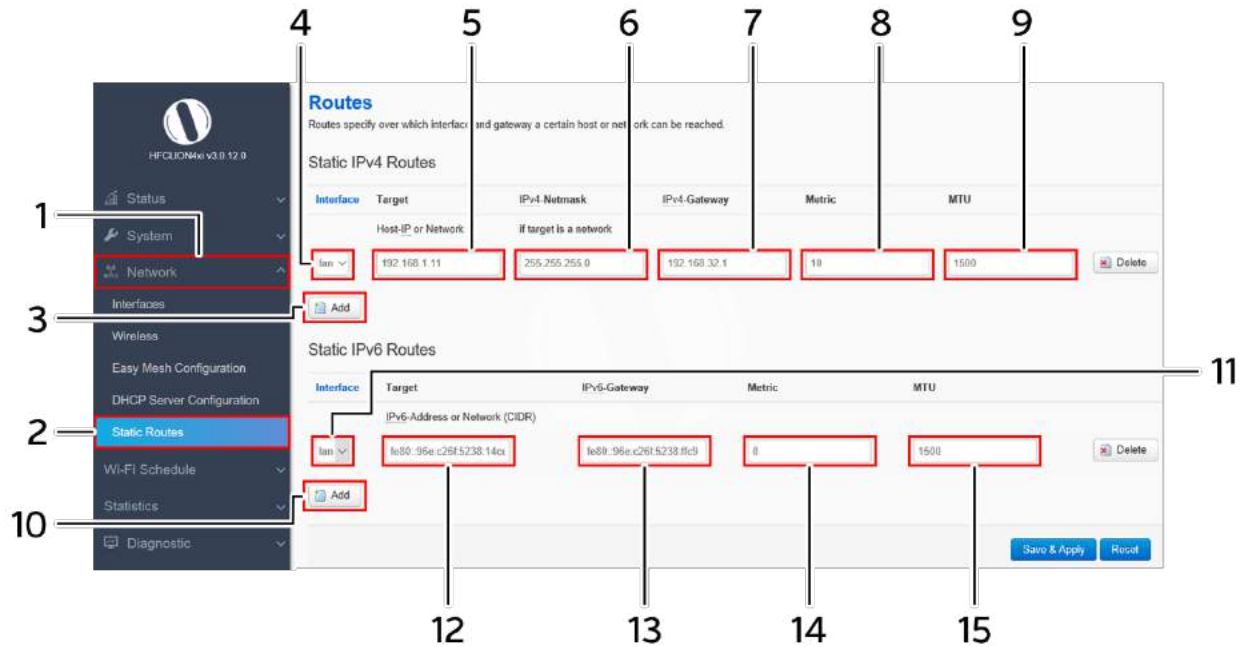
Figure 45: Basic overview of the static route configuration screen for thick AP

Follow the steps given below for static route configuration of thick AP:

Table 35: List of actions for static route configuration of thick AP

Callout	Name	Description
1.	Network	Click on "Network" dropdown
2.	Static Routes	Click on "Static Routes" option
		Static IPv4 Routes
3.	Add	Click on "Add" option to add a new static route in IPv4 format
4.	Interface	Select the physical network interface through which this route is accessible from the dropdown list
5.	Target	Enter the IP address of the destination host or network in IPv4 format to which the route leads
6.	IPv4-Netmask	Enter the IPv4 netmask for the destination host or network. By default subnet mask is set to 255.255.255.255

Callout	Name	Description
7.	IPv4-Gateway	Enter the IP address of the gateway in IPv4 format through which the destination host or network can be reached. If the current AP is being used to connect network with the Internet, then your gateway IP is the AP's IP address. If you have another router handling your network's Internet connection, enter the IP address of that router instead
8.	Metric	Enter a value that defines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen
9.	MTU	Enter the MTU size, by default it is set to 1500.

Click "Save & Apply" to save the static IPv4 route configuration or click "Reset" to configure the same again.

Static IPv6 Routes		
10.	Add	Click on "Add" option to add a new static route in IPv6 format
11.	Interface	Select the physical network interface through which this route is accessible from the dropdown list
12.	Target	Enter the IP address of the destination host or network in IPv6 format to which the route leads
13.	IPv6-Gateway	Enter the IP address of the gateway in IPv6 format through which the destination host or network can be reached. If the current AP is being used to connect network with the Internet, then your gateway IP is the AP's IP address. If you have another router handling your network's Internet connection, enter the IP address of that router instead
14.	Metric	Enter a value that defines the priority of the route. If multiple routes to the same destination exist, the route with the lowest metric is chosen
15.	MTU	Enter the MTU size, by default it is set to 1500.

Click "Save & Apply" to save the static IPv6 route configuration or click "Reset" to configure the same again.

11   Wi-Fi Schedule

This screen is provided with options to create, edit, or delete a Wi-Fi schedule. A basic overview of the screen is given below:

Figure 46: Basic overview of the Wi-Fi schedule screen

Follow the steps given below to view Wi-Fi schedule screen:

Table 36: List of actions to view Wi-Fi schedule screen

Callout	Name	Description
1.	Wi-Fi Schedule	Click on "Wi-Fi Schedule" dropdown
2.	Schedule	Click on "Schedule" option
3.	Status	Displays the current Wi-Fi status as Enabled or Disabled
4.	Add Schedule	Enter a unique name and click on "Add" option to create a new schedule event. Configure the schedule event as discussed in the section below

A basic overview of the schedule parameters are given below:

Figure 47: Basic overview of the Wi-Fi schedule screen

Follow the steps given below to create, edit, or delete a Wi-Fi schedule:

Table 37: List of actions to create, edit, or delete a Wi-Fi schedule

Callout	Name	Description
1.	Enable event	Click on the check box to enable the newly created schedule event. If kept deselected the event will not be listed in the scheduled jobs
2.	Event days	Select the days for the event
3.	Stop Wi-Fi	Assign the time from the dropdown list to stop the Wi-Fi. The stop Wi-Fi time must be after the start Wi-Fi
4.	Start Wi-Fi	Assign the time from the dropdown list to start the Wi-Fi
5.	Add Schedule	Enter a unique name and click on "Add" option to create an another new schedule event
6.	Delete Event	Click on the "Delete" option of the respective schedule to remove it from the list

Click "Save & Apply" to save the Wi-Fi schedule or click "Reset" to configure the same again. All enabled events are listed in the Scheduled Jobs screen.

12   View Schedule Job

All Wi-Fi schedules are listed in this screen. A basic overview of the schedule job screen is given below:
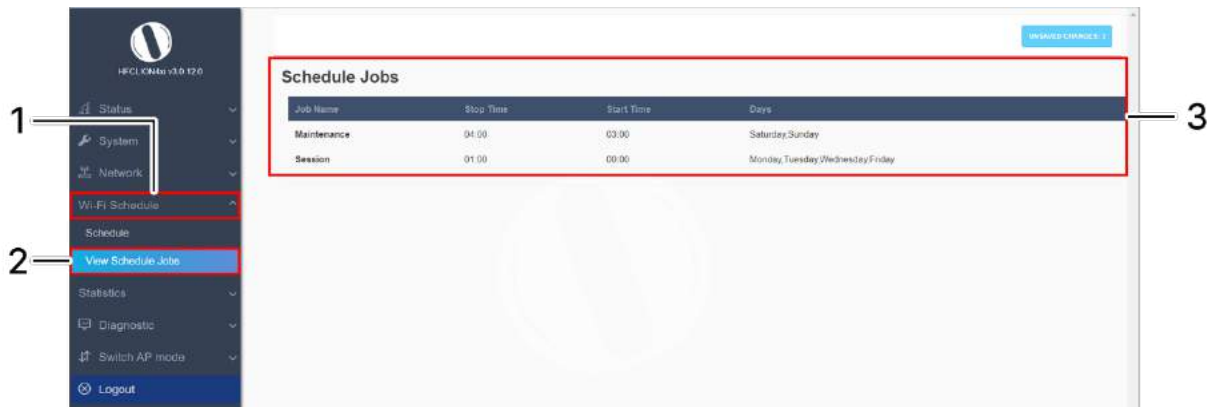

Figure 48: Basic overview of the view schedule job screen

Follow the steps given below to view schedule job screen:

Table 38: List of actions to view schedule job screen

Callout	Name	Description
1.	Wi-Fi Schedule	Click on "Wi-Fi Schedule" dropdown
2.	View Schedule Job	Click on "View Schedule Job" option
3.	Schedule Jobs	Displays all the enabled Wi-Fi schedules in a listed form

13   Statistics

13.1 Real-time Graphs/Load

The real time load graph shows the CPU load of last 3 min and the graph is refreshed at every 3 sec interval. In addition to the displayed graph the user can find the average and the peak CPU load values of the respective AP. A basic overview of the Real-time load graphs screen is given below:
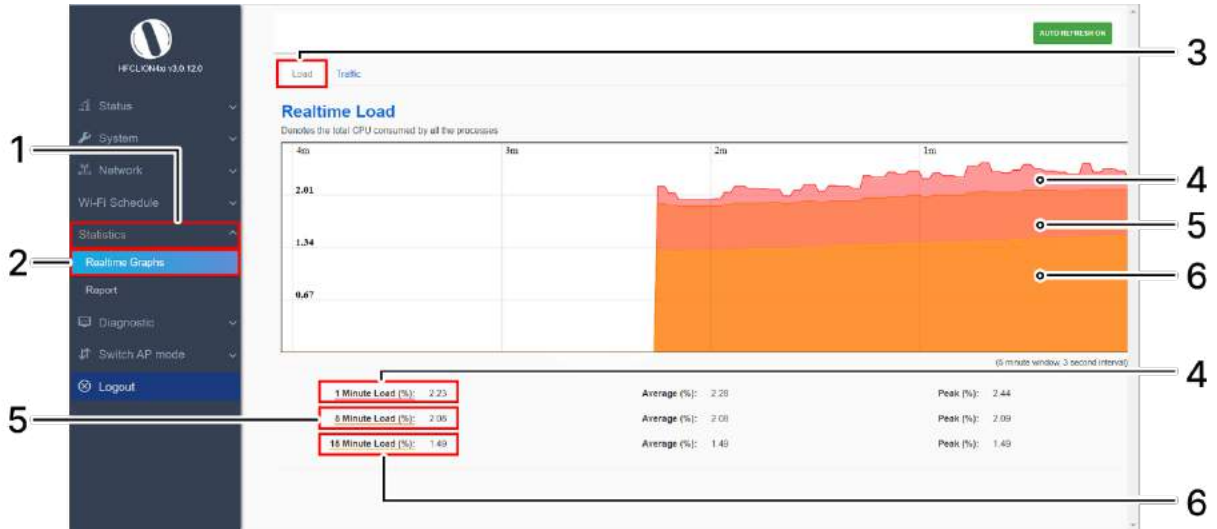

Figure 49: Basic overview of the Real-time graphs/ load

Follow the steps given below to view the real-time load graphs of the AP:

Table 39: List of actions to view real-time load graphs

Callout	Name	Description
1.	Statistics	Click on "Statistics" dropdown
2.	Real-time graphs	Click on "Real-time graphs" option
3.	Real-time Load	Click on the load option to view the load statistics
4.	1 Minute Load	Displays the color coded load in last 1 minute
5.	5 Minute Load	Displays the color coded load in last 5 minute
6.	15 Minute Load	Displays the color coded load in last 15 minute

13.2 Real-time Graphs/Traffic

The real time load/traffic graph shows the CPU load of last 3 min and the graph is refreshed at every 3 sec interval. In addition to the displayed graph the user can find the inbound and outbound traffic of the associated SSIDs, bridge interface, and Ethernet interfaces along with average and the peak traffic values. A basic overview of the Real-time graphs traffic screen is given below:

Figure 50: Basic overview of the Real-time graphs/ traffic

Follow the steps given below to view the real-time traffic graphs of the AP:

Table 40: List of actions to view real-time traffic graphs

Callout	Name	Description
1.	Statistics	Click on "Statistics" dropdown
2.	Real-time graphs	Click on "Real-time graphs" option
3.	Real-time Traffic	Click on the traffic option to view the traffic statistics
4.	Real-time Traffic	Select any of the interface to check the inbound and outbound traffic across it. The graphs are available to show the traffic across SSIDs, Bridge Interface, and Ethernet Interface (eth-0 and eth-1)
5.	Inbound	Displays the inbound traffic at the selected interface in color coded format
6.	Outbound	Displays the outbound traffic at the selected interface in color coded format

14 Diagnostics

Following are the diagnostic features provided in thick AP GUI.

14.1 Routes

This screen is provided to view the active routes on the system. A basic overview of the screen to view the active routes is given below:
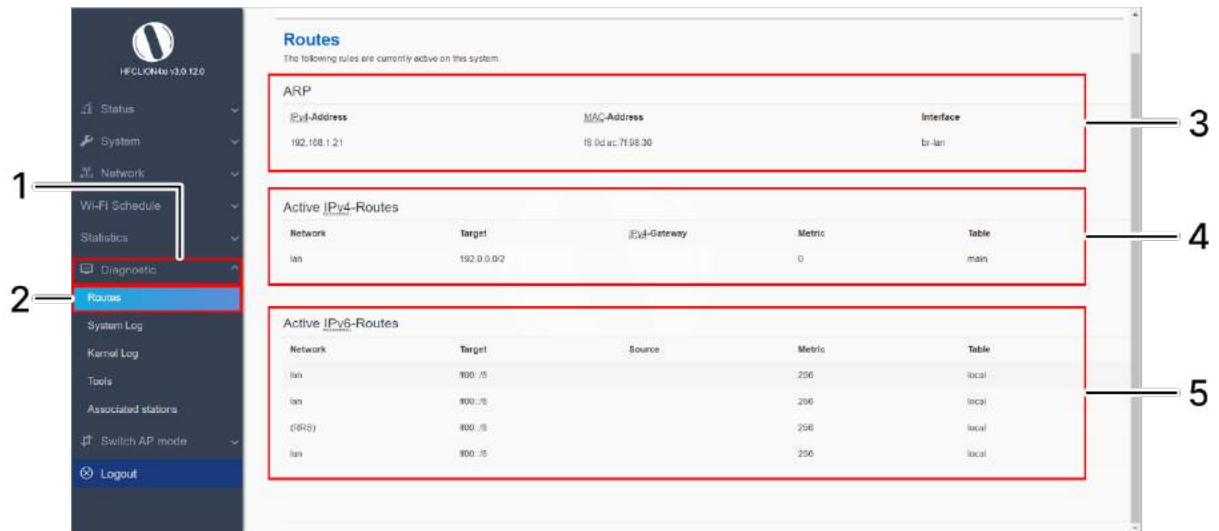

Figure 51: Basic overview of the screen to view the active routes

Follow the steps given below to view the active routes on the system:

Table 41: List of actions to view the active routes on the system

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	Routes	Click on "Routes" option
3.	ARP	Displays the MAC addresses of all reachable IPs. The Address Resolution Protocol (ARP) is a communication protocol used for discovering the link layer address, such as a MAC address associated with a given internet layer address, typically an IPv4 address.
4.	Active IPv4 Routes	Displays all the IPv4 routes which are active at present
5.	Active IPv6 Routes	Displays all the IPv6 routes which are active at present

14.2 System Log

This screen is provided to view the AP logs if the user faces any issue or wants to view the back-end logs. Only new logs are shown in this screen. However, old logs are stored in the database but will not be shown in this screen.

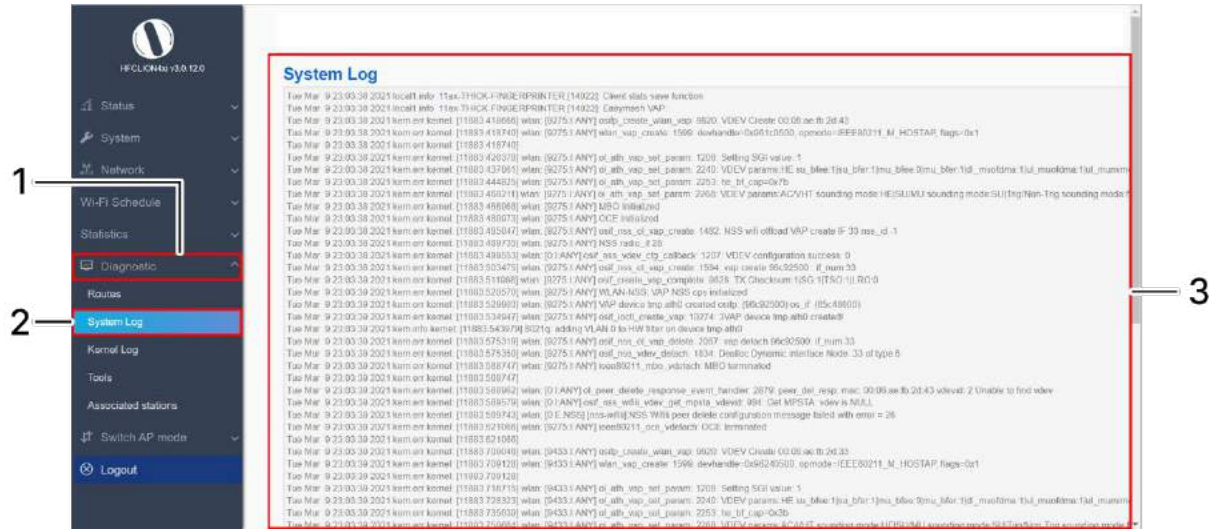A basic overview of the System Log screen is given below:

Figure 52: Basic overview of the System Log screen

Follow the steps given below to view the system log of AP:

Table 42: List of actions to view the system log

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	System Log	Click on "System Log" option.
3.	Logs	Logs relevant to the AP application software are displayed here for monitoring purpose

14.3 Kernel Log

Boot logs, driver logs, Wi-Fi and firmware related logs are listed in this screen. Kernel log will be accumulated from boot up time till shut down time of the respective AP.

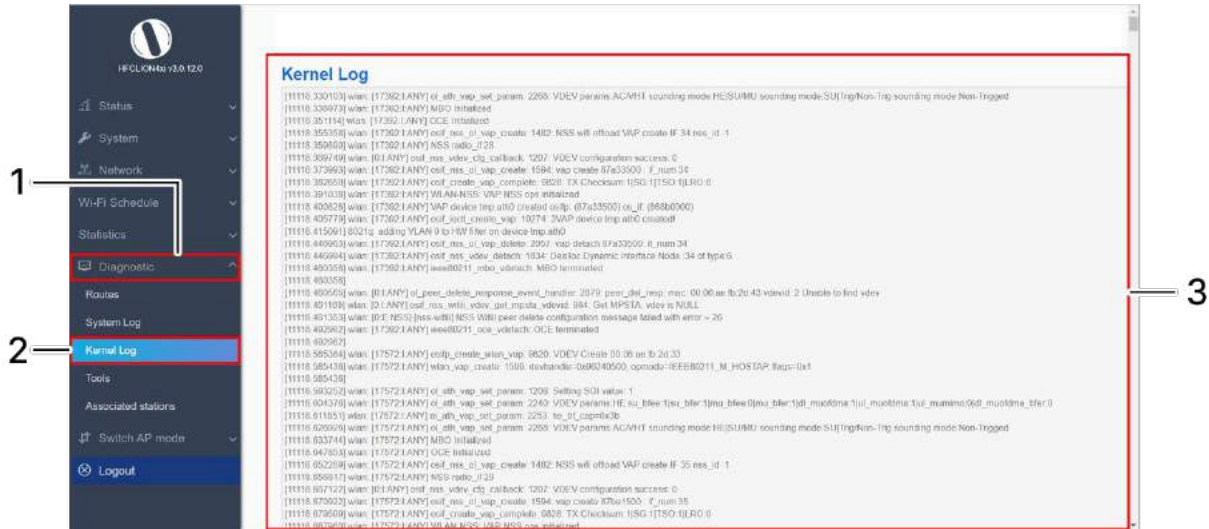A basic overview of the Kernel Log screen is given below:

Figure 53: Basic overview of the Kernel Log screen

Follow the steps given below to view the Kernel log of the AP:

Table 43: List of actions to view the kernel log

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	Kernel Log	Click on "Kernel Log" option
3.	Logs	Boot logs, driver logs, Wi-Fi and firmware related logs are displayed here for monitoring purpose

14.5 Diagnostic Tools

As part of diagnostics, the user can perform the following activities:

1. The user can check if the link connection is established or not with "Ping" option
2. The user can trace the route of the established link with "Traceroute" option

14.5.1   Check the network connection/status

This utility is used to test connectivity between the respective AP and another device on the network. A basic overview of the Diagnostic Tools screen to check the connection status is given below:
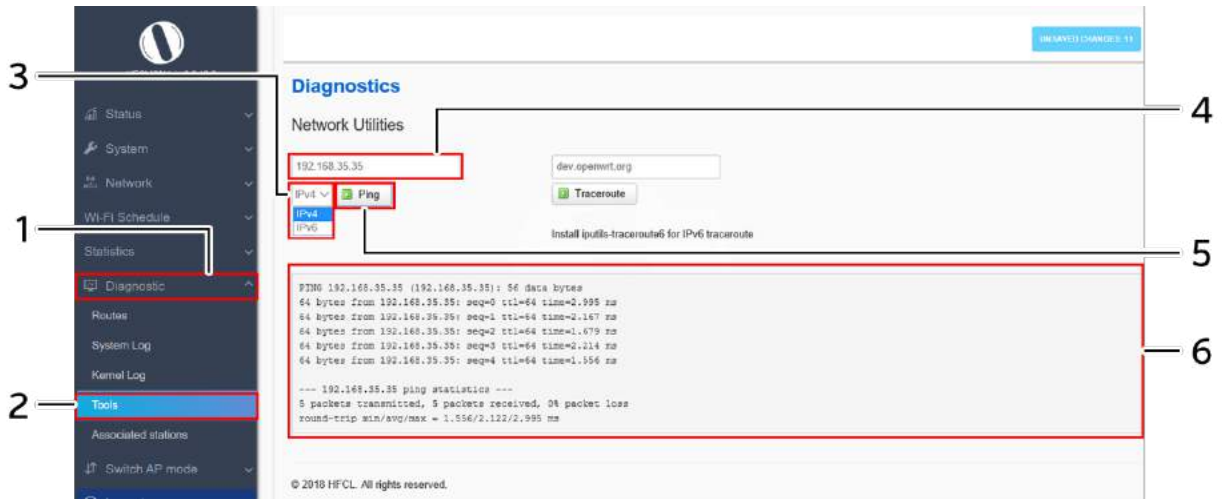

Figure 54: Basic overview of the diagnostics tool screen to check the connection status

Follow the steps given below to check the connection status:

Table 44: List of actions to check the connection status

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	Tools	Click on "Tools" option
3.	Address type	Select the IP address type from the dropdown list (IPv4, IPv6)
4.	IP Address	Enter the IP address of the device with which the user wants to check the connection status
5.	Ping	Click on "Ping" option to check the connection status. It will check the network connection/status with entered IP address
6.	Feedback window	Check the response on the feedback window to know the connection status. The status is shown in terms of transmitted packets and received packets with packet data loss

14.5.2   Check the route of the established network connection

This utility will display all the routers present between the destination IP address and this AP. Up to 30 "hops" (intermediate routers) between the AP and the destination can be monitored.

A basic overview of the Diagnostic Tools screen to check the route of established connection is given below:
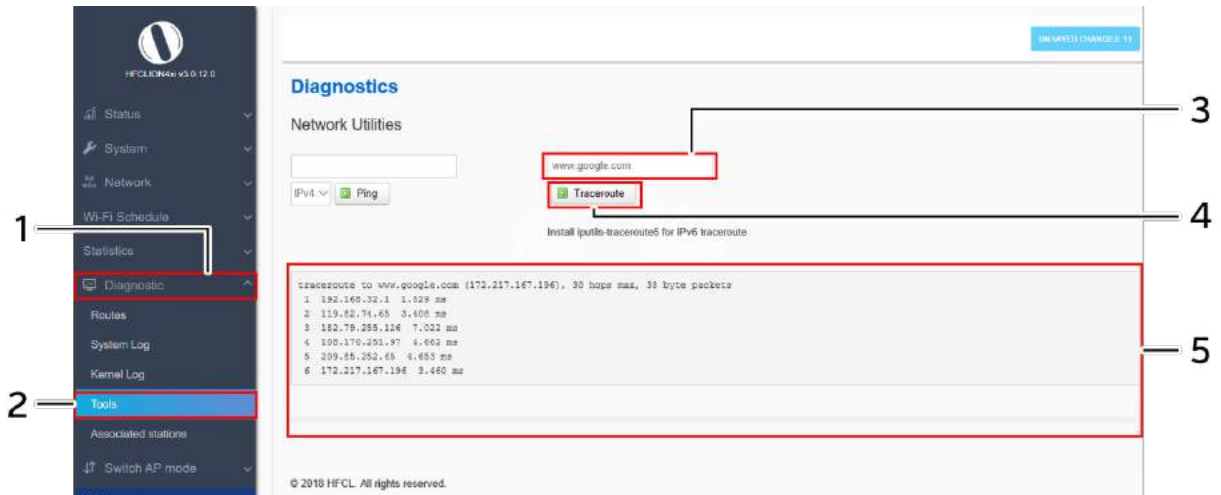

Figure 55: Basic overview of the diagnostics tool screen to check the route of established connection

Follow the steps given below to check the route of established connection:

Table 45: List of actions to check the route of established connection

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	Tools	Click on "Tools" option
3.	IP Address	Enter the IP address or the domain name of the destination with which the user wants to check the connection route
4.	Traceroute	Click on "Traceroute" option to check the connection route. It traces the network path/route to the entered IP address or domain name
5.	Feedback window	Check the response on the feedback window to know the connection route.

14.6 Associated Stations

The list of connected clients along with the relevant information in respective information columns is populated in this screen. A basic overview of the screen to show connected clients is given below:
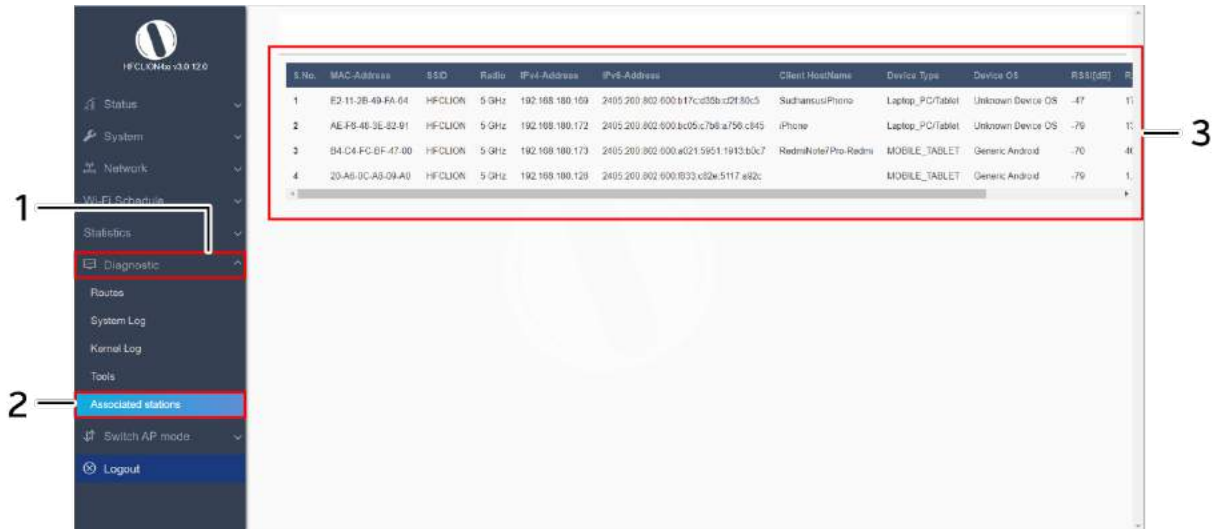

Figure 56: Basic overview of the screen to show connected clients

Follow the steps given below to view connected clients:

Table 46: List of actions to view connected clients

Callout	Name	Description
1.	Diagnostics	Click on "Diagnostics" dropdown
2.	Associated Stations	Click on "Associated Stations" option
3.	Client List	Displays all connected clients a listed form. Refer the above image for more information on relevant information with respect to connected clients

15   Logout

Click on the logout option to terminate the user session.

.

16   Installation Setup

IO Indoor AP can be mounted onto the wall or ceiling, whereas the outdoor AP can be wall-mounted or pole mounted. Perform the steps discussed in below sections for the appropriate installation of indoor and outdoor APs:

16.1 Mounting of Dual Band 2x2:2 Indoor Access Point (Wall and Ceiling)

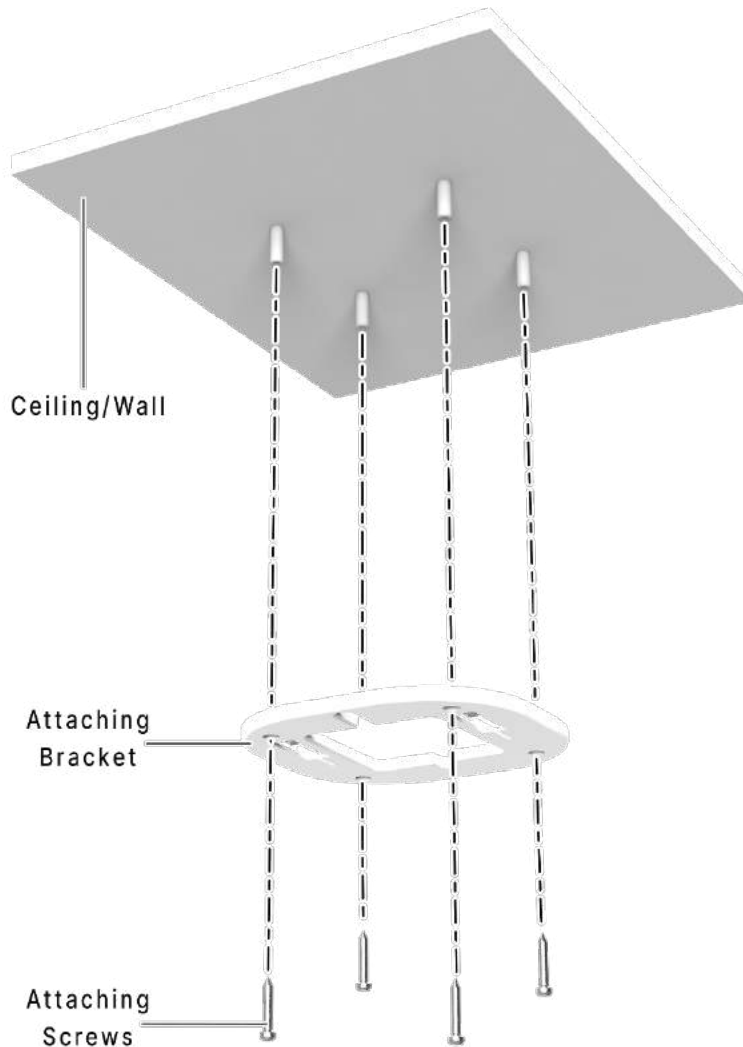1.   Refer the image below for attaching parts required for wall/ceiling mounting of AP:
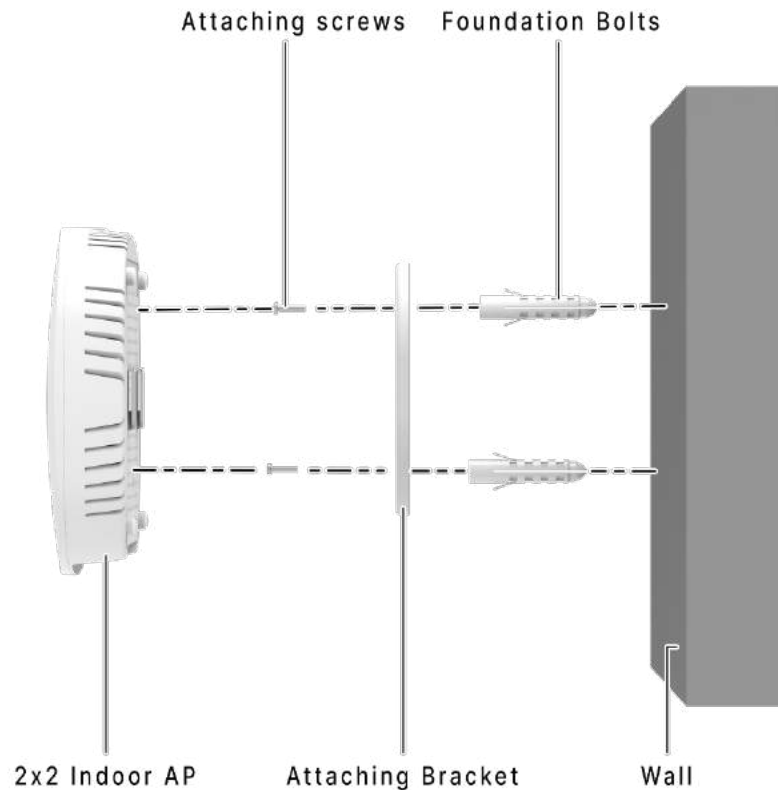
Figure 57: Attaching parts for wall/ceiling mounting of indoor AP

2.   Place the attaching bracket on to the wall or ceiling and mark the holes to drill. Drill holes of appropriate size.
3.   Insert the foundation bolts in the drilled holes of wall/ceiling.

4. Use the supplied screws and mount the attaching bracket on to the wall or ceiling as shown below:
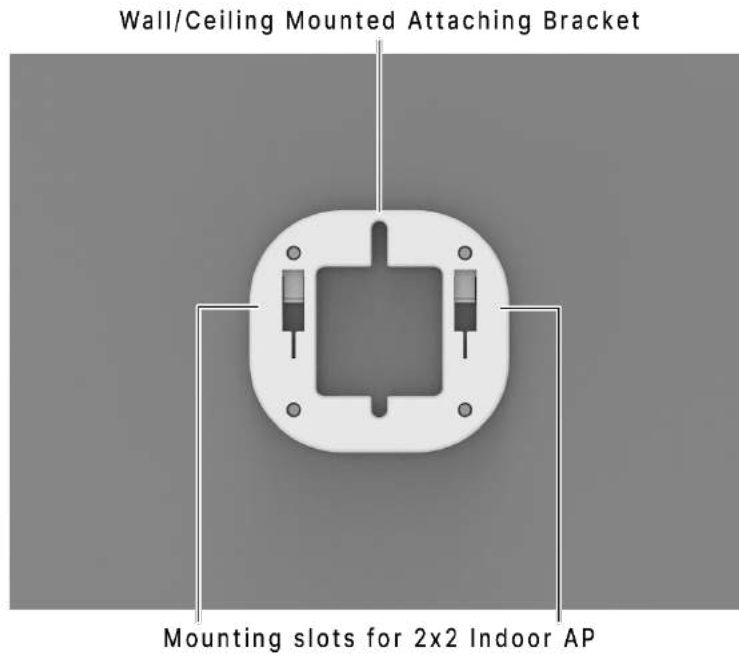

Figure 58: Attaching bracket on to the wall or ceiling for indoor AP

Note: Make sure that the attaching bracket is tightly installed before mounting the access point on the wall or ceiling.
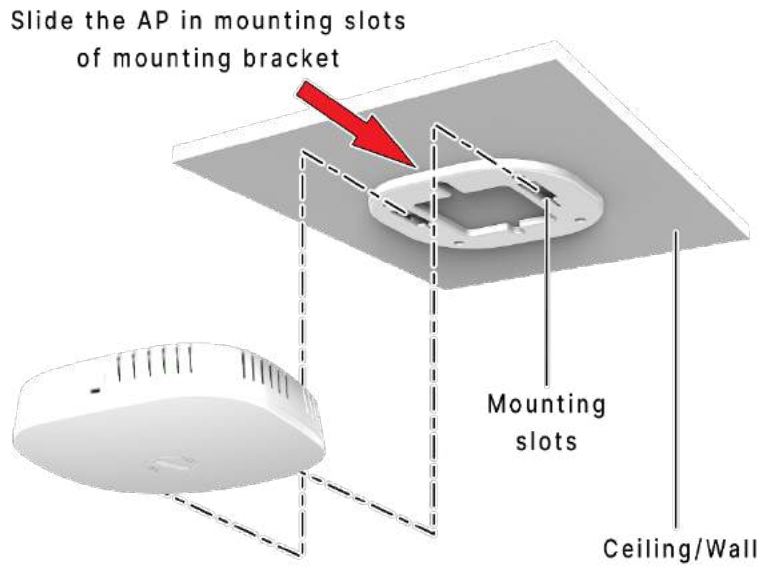
5. Refer the image below for wall mounted attaching bracket:
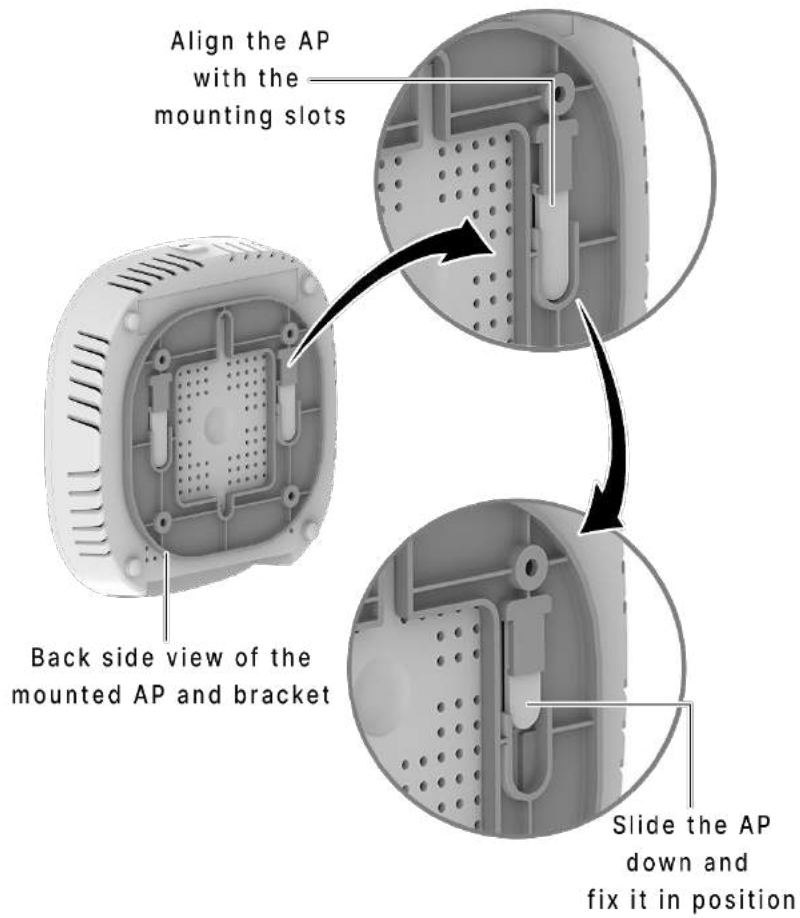

Figure 59: Wall/ceiling mounted attaching bracket

6. Align the mounting slots of indoor AP and attaching bracket as shown below:

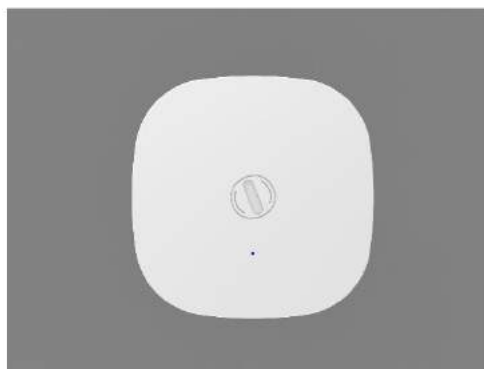*Figure 60: Alignment of mounting bracket with indoor AP*

7.   Refer the image below for backside view of wall/ceiling mounted AP:

Figure 61: Backside view of attaching bracket with indoor AP

8.   The wall or ceiling mounted AP is shown below:

Figure 62: Wall/ceiling mounted indoor AP

9.   Slightly push and slide the access point out from the mounting slots of attaching bracket to unmount the AP.

CONFIDENTIAL

16.2 Mounting of Dual Band 2x2:2 Outdoor Access Point (Pole and Wall)

2x2 outdoor AP has four holes on its back side for the attachment of mounting bracket, as shown in "Figure 8: Back view of the outdoor AP" of this document. The mounting bracket is designed in such a way that the AP can be mounted on the wall as well as on the pole with the help of its attaching parts. It provides the freedom of movement to the AP even after the mounting.

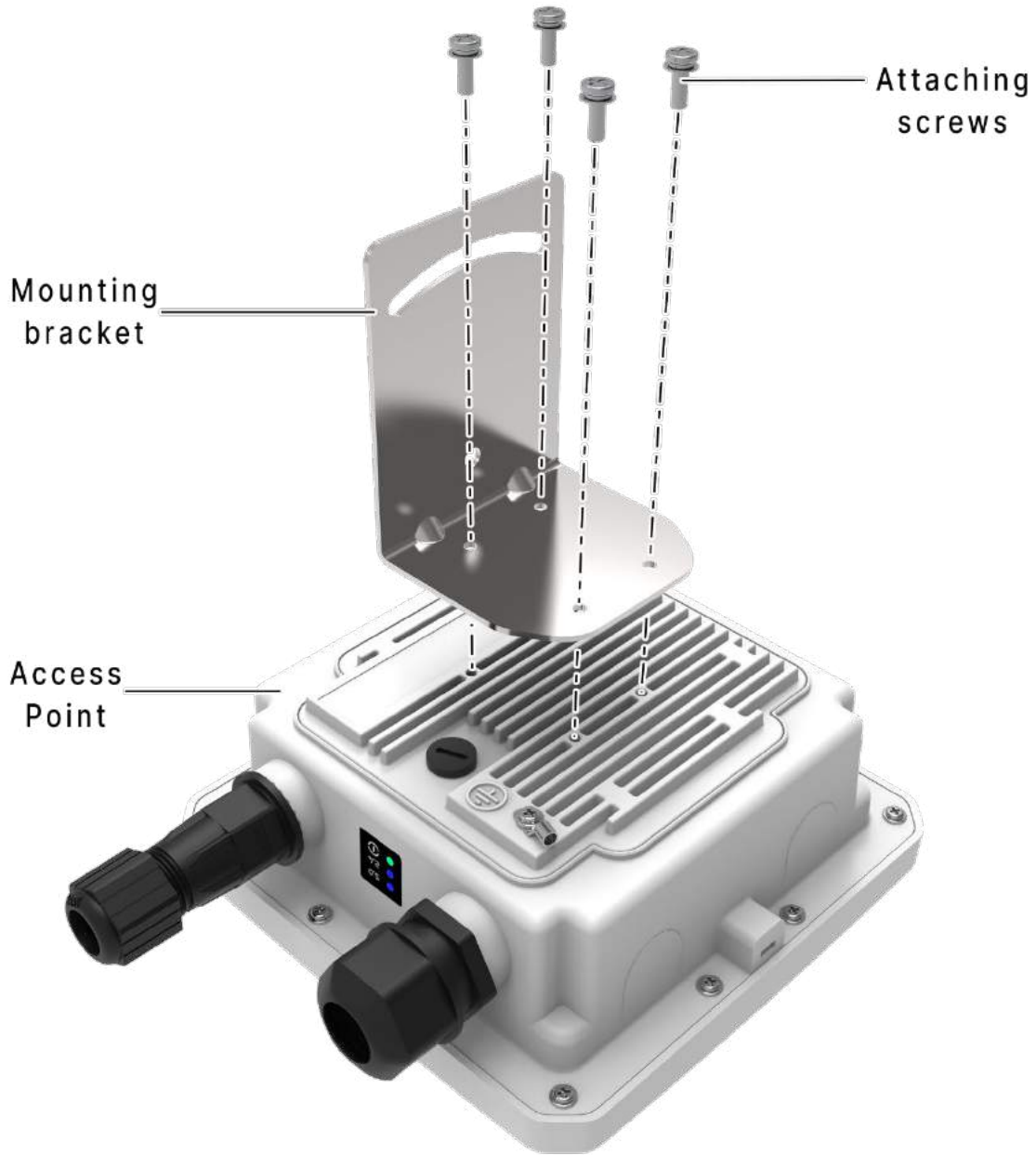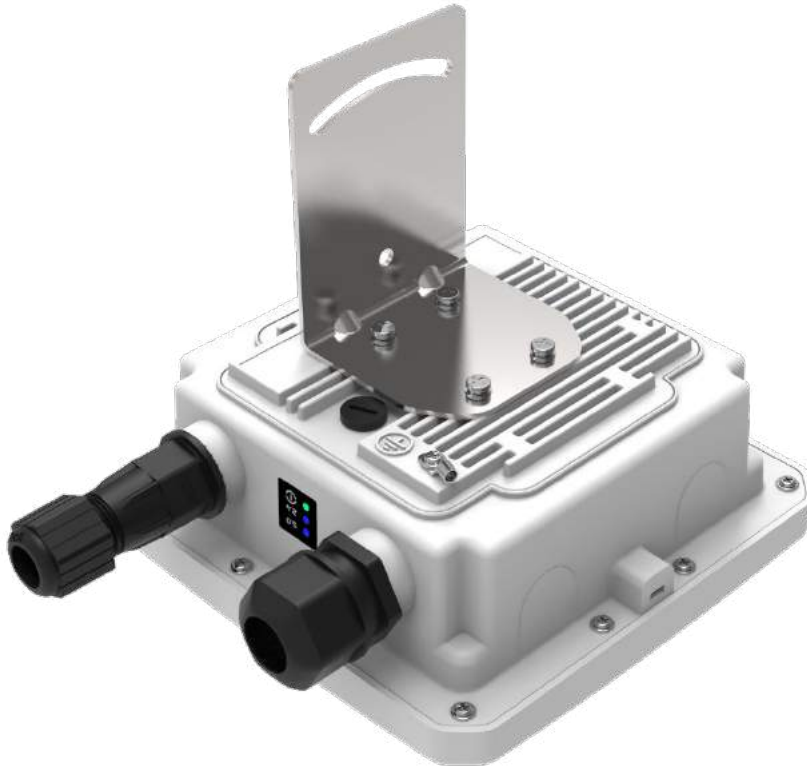1. The mounting bracket is fixed onto the mounting holes of 2x2 outdoor AP as shown in the figure below:

Figure 63: Mounting bracket attachment with the 2x2 outdoor AP

2.   Final alignment of the mounting bracket with 2x2 outdoor AP is as shown below:

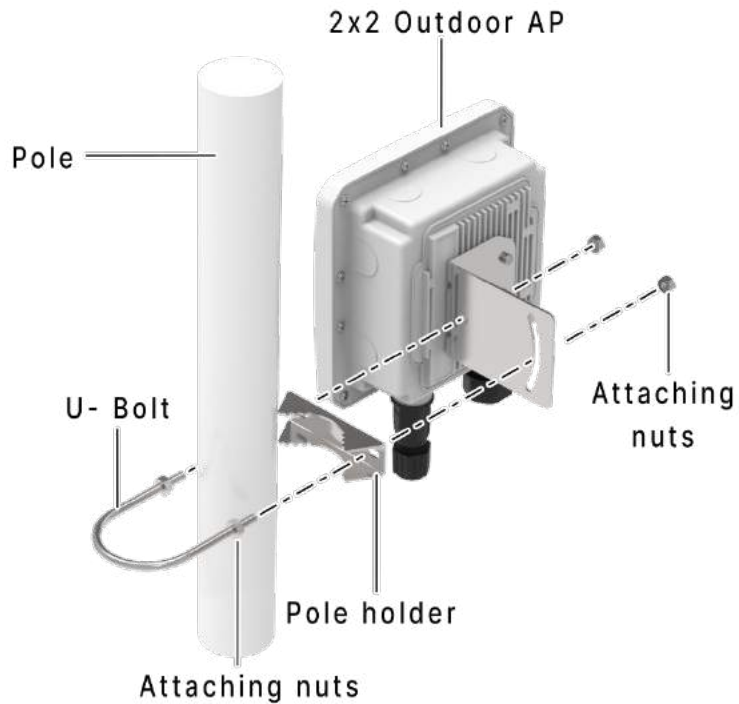*Figure 64: Mounting bracket alignment with the 2x2 outdoor AP*

The mounting instructions of 2x2 outdoor AP is detailed in further sections below.

16.2.1   2x2 outdoor AP mounting to the Pole

Follow the steps given below and mount the device onto the pole:

1. Align the bracket mounted AP with pole holder and U-bolt as shown below:

Figure 65: Overview of the 2x2 outdoor AP with pole and mounting bracket attaching parts

2. Pass the U-bolt through the cuts of pole holder and mounting bracket. Tighten it in place with attaching nuts.
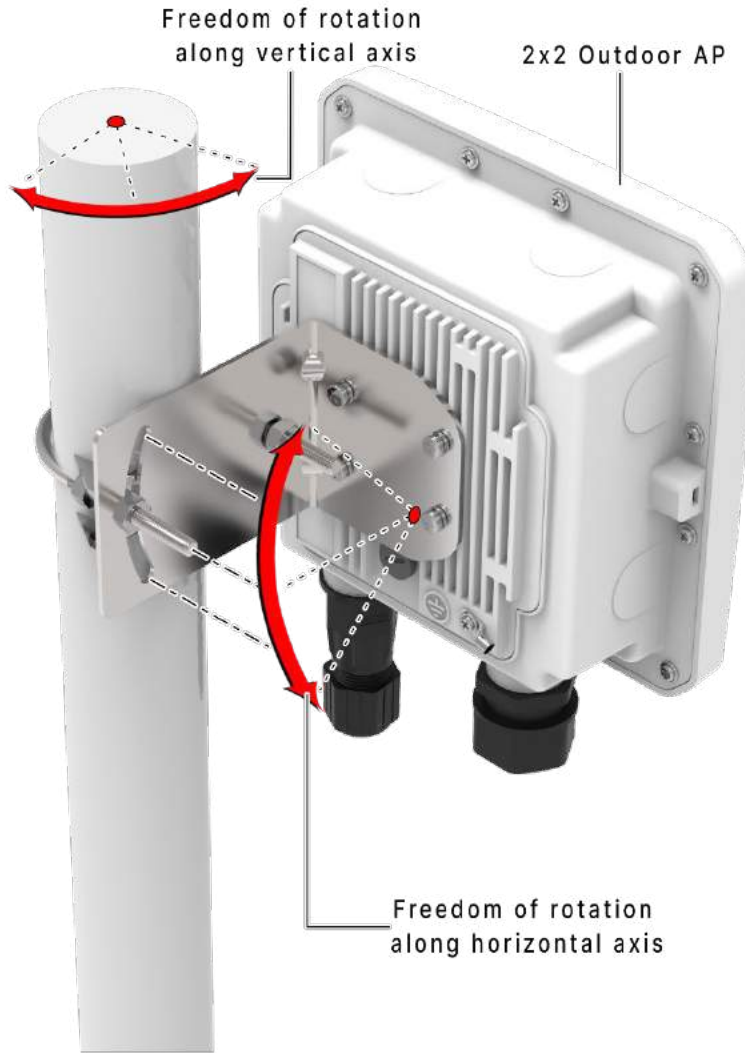
Figure 66: Final alignment of 2x2 outdoor AP and mounting bracket

3. As shown above, the 2x2 outdoor AP has the freedom of movement along the vertical and horizontal axis.

4.   The final alignment of 2x2 outdoor AP in a pole mounting is shown in the figure below:
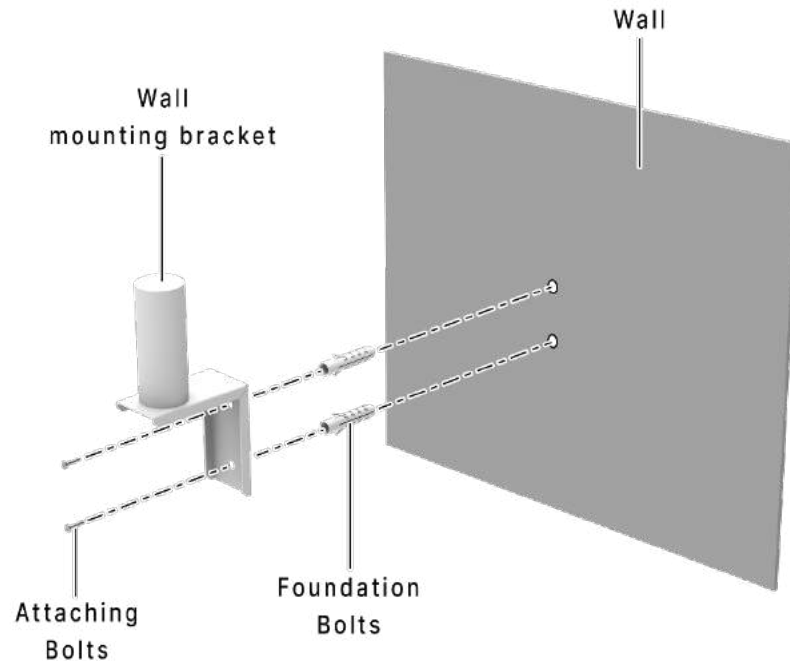

Figure 67: Basic overview of pole mounted 2x2 outdoor AP

16.2.2   2x2 outdoor AP mounting to the Wall

To mount the device onto the wall, foundation bolts and attaching bolts are needed along with the wall mounting bracket. Refer the image given below:

Figure 68: Items needed for wall mounting of the device

Follow the steps given below and mount the device onto the wall:

1. Take the reference from the printed sheet provided along with the wall mounting bracket and mark the position of the holes on the wall.
2. Use the drill machine to drill 2 holes with a 6mm drill tool on respective marked positions.
3. Push the foundation bolts into the holes with a hammer.
4. Align the drilled holes with the holes of wall mounting bracket.
5. Insert the attaching bolts through the holes of mounting bracket into the wall.
6. Wall mounting bracket is fixed to the wall.
7. Mount the device on to the wall mounting bracket as discussed in pole mounting process.

Figure 69: Basic overview of wall mounted 2x2 outdoor AP

CONFIDENTIAL

16.3 Grounding of AP

The AP should be properly grounded upon installment. The IO's 2x2 outdoor AP has a grounding position at the back side of the device as shown below:

Figure 70: Grounding point of 2x2 outdoor AP

A grounding strap can be made from the ring lug terminal of M4 size and a medium length copper wire of suggested gauge AWG-6 (4.1 mm).

Insert the grounding wire and flush it till the end of the terminal. Use the crimp tool and reshape or compress the terminal. Use an M4x10 machine screw and attach the crimped lug with AP.
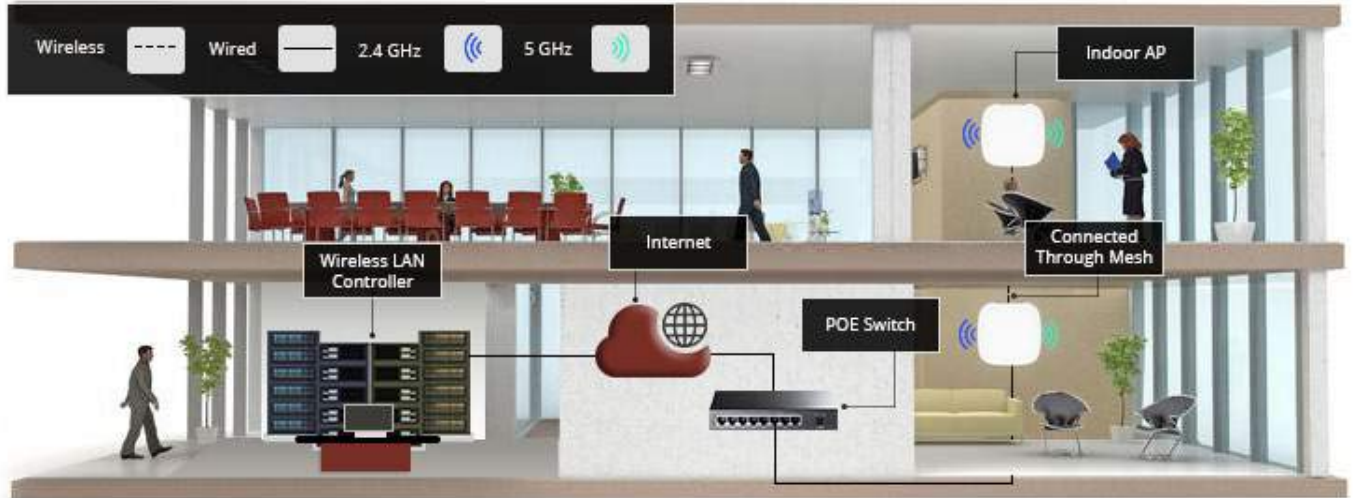
17   Use Cases

A.   Indoor Access Point

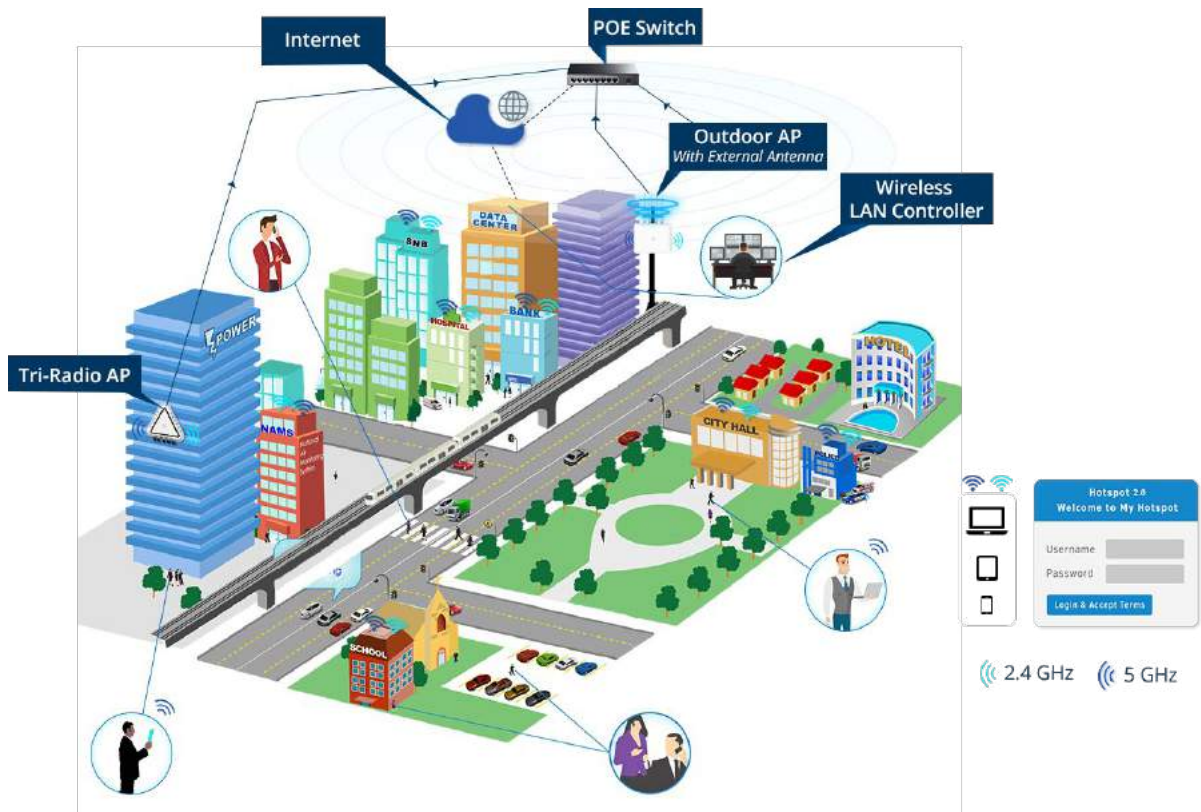*Figure 71: Use Case Diagram of Indoor AP*

B.   Outdoor Access Point

Figure 72: Use Case Diagram of Outdoor AP

CONFIDENTIAL