QUANTUM®
ACCESS UNLIMITED

User Guide

Standalone Access Point

Copyright Information

Contents

Introduction

Access Point Overview

This document explains how to configure and manage Standalone Access Point.

Quantum Networks' Wireless Access Point is the industry's most facile to utilize. It's a feature opulent Wi-Fi Access Point designed to bring power and simplicity together for sizably voluminous-scale indoor deployments.

Access Point can be deployed in Standalone Mode and can be managed through Quantum RUDDER, as part of the Quantum Wireless Smart WLAN system.

A wireless technology that sanctions wireless signals to navigate around interference, elongate wireless signal range, increment speeds as well as capacity for wireless networks.

Package Contents

Access Point package contains all of the items listed below.

- Access Point

- Quick setup guide

Glossary

Following terms are frequently used in this manual.

Term	Definition
AP	Access Point
DHCP	Dynamic Host Configuration Protocol (DHCP) is a network protocol that enables a server to automatically assign an IP address to devices.
Static	A *static* Internet Protocol (*IP*) address (*static IP* address) is a fixed IP Address assigned to the device.
PPPoE	PPPoE stands for Point-to-Point Protocol over Ethernet, a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames.
WLAN	Wireless Local Area Network is a wireless network that can transfer data at high speeds.
LAN	Local Area Network
WAN	Wide Area Network
VLAN	Virtual Local Area Network allows several networks to work virtually as one LAN.
SSID	Service Set Identifier is a unique ID that consists of 32 characters and is used for naming wireless networks.
WPA2	WPA2 (Encryption Method) - Wi-Fi Protected Access 2 - Pre-Shared Key, is a method of securing a wireless network using Pre-Shared Key (PSK) for authentication.
WPA-Mixed	With WPA mixed (Encryption Method) mode devices can be connected with both WPA (TKIP) and WPA2 (AES) encryption methods.
TKIP	TKIP (Temporal Key Integrity Protocol) is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP), the original WLAN security protocol.
Wireless 2.4 GHz	2.4 GHz band provides great distance coverage, however transmits data at slower speeds.
Wireless 5 GHz	The 5 GHz band provides less coverage, however transmits data at faster speeds.

Configuring Access Point in Standalone Mode

Access Point Initial Configuration

- Connect WAN port of the Access Point to network with internet access.
- You should see a new wireless network with SSID QN_XX:XX (where XX:XX are last four digits of Access Point MAC Address).
- Connect to QN_XX:XX SSID and browse Access Point's default IP "169.254.1.1". You should be greeted with welcome message.
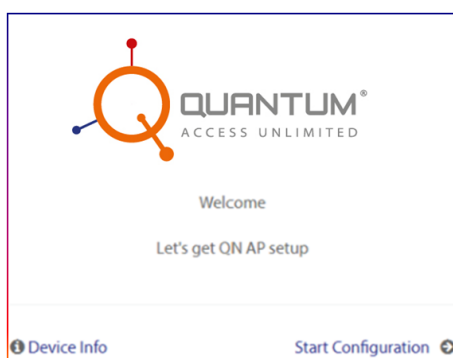

Figure 1

Setting Up Device IP Address

- Click Start Configuration (Refer Figure1).
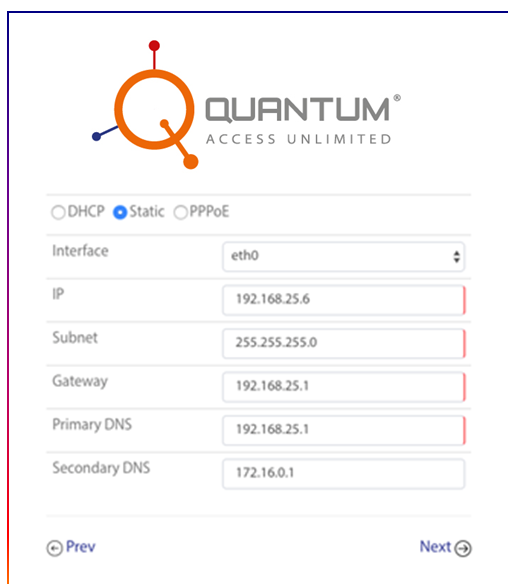- Configure IPv4 by selecting required option DHCP, Static or PPPoE and click Next.

Figure 2

Management Mode

Quantum Networks' Access Point can be configured in two modes:

Standalone

Independent management of each Access Point

Cloud Controlled

Centralized management of Access Point's using Quantum RUDDER

Access Point Quick Setup in Standalone Mode

- Select "**Management Mode**" as **"Standalone",** if each Access Point is to be configured and managed individually. Username and password for the device and click "**Next**".
- User can select Access Point's Operation Mode as **Bridge** or **Router**.

  Description: Difference between Access Point as a Bridge or a Router.

  - **Bridge** - In this mode, device connects to a wired or wireless router via an ethernet cable and extends the wireless coverage of your existing network.

  - **Router -** In this mode, device connects to the internet directly and share internet access to multiple wired and wireless devices. NAT and DHCP servers are enabled by default

  ### Bridge
  - Configure **WLAN** (SSID) parameters and click **Next.**
  - Review the Configuration Summary. Click **Reconfigure** if any changes are required or click **Finish** to complete the configuration.
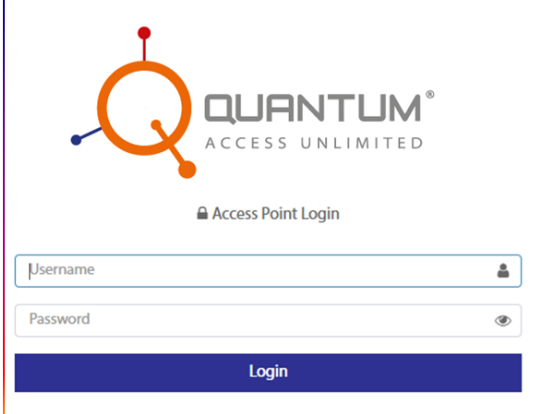
  ### Router
  - Configure **WLAN** (SSID) and **Local subnet** parameters and click **Next**.
  - Review the Configuration Summary. Click **Reconfigure** if any changes are required or click **Finish** to complete the configuration.

Navigation

Navigating the Web Interface

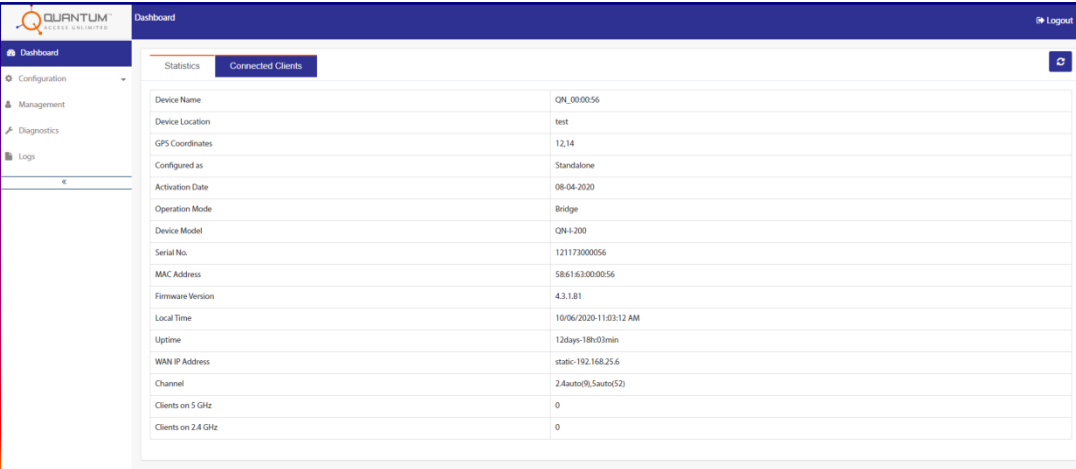- Open Web Browser and enter configured IP address of the Access Point.

Figure 3 AP Web Login Page

- Enter Username and Password (use the same created while quick setup process), click Login

Figure 4 Web Interface Dashboards

www.qntmnet.com

Access Point Configuration

Dashboard

Go to Configuration **> Dashboard**.

Device Name	QN_00:00:56
Device Location	test
GPS Coordinates	12,14
Configured as	Standalone
Activation Date	08-04-2020
Operation Mode	Bridge
Device Model	QN-I-200
Serial No.	121173000056
MAC Address	58:61:63:00:00:56
Firmware Version	4.3.1.B1
Local Time	10/06/2020-11:05:50 AM
Uptime	12days-18h:05min
WAN IP Address	static-192.168.25.6
Channel	2.4auto(9),5auto(52)
Clients on 5 GHz	0
Clients on 2.4 GHz	0

Figure 5 Dashboard

Statistics

Statistics	Description
Device Name	Name of device
Device Location	AP location
GPS Coordinates	GPS coordinates
Configured as	Management mode in which AP has been configured
Activation Date	Activation date of AP
Operation Mode	Configured operation mode of AP
Device Model	AP Model Detail
Serial no.	Serial number of the device
MAC	MAC address of the device
Firmware Version	Current AP firmware version
Local Time	Local current time as per selected country
Uptime	AP actual up time detail
WAN IP Address	Selected IP schema with IP detail – i.e. DHCP / Static / PPPoE
Channel	Active radio channel detail
Clients on 5 GHz	Connected clients on 5 GHz
Clients on 2.4 GHz	Connected clients on 2.4 GHz

Connected Clients

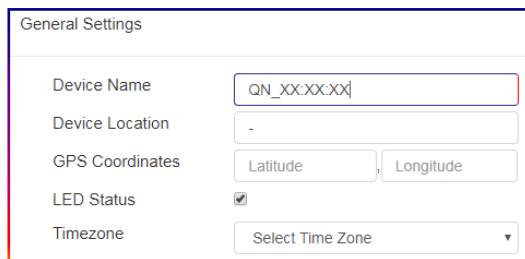| Parameter	Description
Radio	Radio detail through which clients has been connected
SSID	SSID name through which clients has been connected
MAC	MAC address of connected client device
IP	IP address taken by host device
Hostname	Host name
RSSI	Wireless signal strength. (Between AP and Connected client)
Connected Since	Time since AP get connected

Configuration

Device

Go to **Configuration > Device**.

Figure 6 Device General Setting

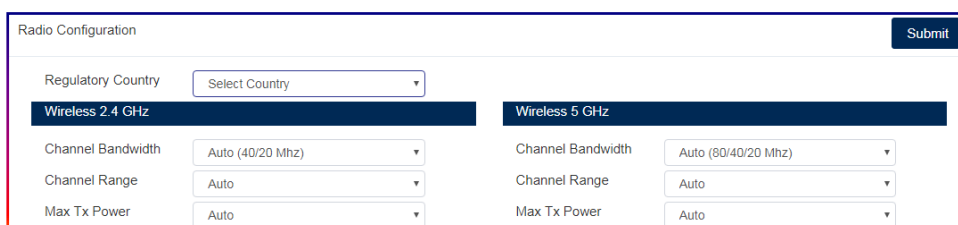| Parameter	Description	Default Value
Device Name	Type Device name of your choice. The device name identifies the AP among other devices on the network	
Device Location & GPS Coordinates	Device geographical location and GPS coordinates to keep track of the physical location of the AP	
LED Status	Power ON / OFF	Enabled
Time zone	Select time zone as per AP geographical location	Asia/Singapore

Figure 7 Device Radio Configurations

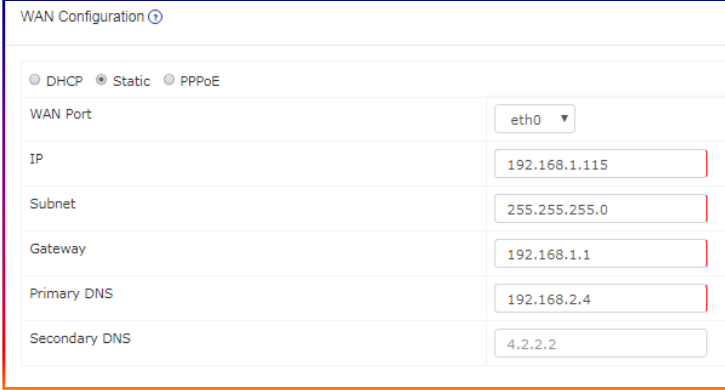| Parameter	Description	Default Value
Regulatory Country	Select country	Singapore
Wireless 2.4 GHz & Wireless 5 GHz	Channel Bandwidth: Choose channel bandwidth from dropdown. It can be Auto / Auto (40/20 MHz) or Auto (20 MHz). wider channel width means fewer channels available, and more interference with other Wireless signals	Auto (20 MHz)
	Channel Range: This option lets you select the channel used by the network. Choose Auto or for manual setting, Choose option "Manual auto", and Choose required channel range. If you choose Auto, the AP automatically selects the best channel	Auto
	Max Tx Power : Choose auto or select specific value from drop down	Auto

Figure 8 Device Access Point Login

Parameter	Description
Username	Access Point Username (created while quick setup)
Current Password	Current login Password. (created while quick setup)
New Password	New password
Confirm Password	Confirm new password

Internet

Go to **Configuration > Internet**.

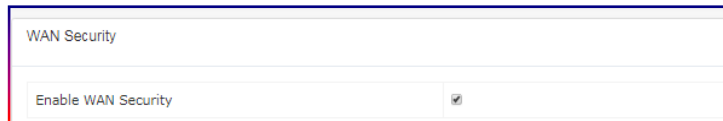
Figure 9 Internet setting

WAN Configuration

Parameter	Description
Select IP Schema Type DHCP / Static or PPPoE as per the requirement	
DHCP - currently-assigned IP address and subnet mask to Access Point.	WAN Port: Select port which needs to be configuring as WAN
	IP Address : IP address assign to AP
	Subnet Mask : subnet mask
	Gateway : Gateway
	Primary DNS : Primary DNS
	Secondary DNS : Secondary DNS
Static - Configure a static IPv4 address.	WAN Port: Select port which needs to be configure as WAN
	IP Address : Enter the static IP address that you want to assign to the AP
	Subnet Mask: Enter the subnet mask for the network
	Gateway: Enter the gateway IP address of the Internet interface
	Primary DNS: The IP address of the primary Domain Name System (DNS) server
	Secondary DNS: The IP address of the secondary Domain Name System (DNS) server
PPPoE	PPPoE Username, Password and Service name provided by the provider

WAN Security

Parameter	Description
WAN Security	Enable WAN Security when Access Point is in Gateway mode and need to maintain network security. WAN Security option available only when AP is configured in Gateway mode. This feature protects AP and LAN devices from unauthorized access from WAN

Figure 10 WAN Security

Port Forwarding

Figure 11 Port Forwarding

Parameter	Description
Rule Name	Rule name
Protocol	TCP or UDP Protocol
Type	Type of Port Mapping or Port Range
Ext.Port	Port Number
Dest. IP	Destination IP Address
Dest.Port	Port Number

Local Subnet

Local Subnet is available when AP is in Gateway mode.
Go to **Configuration > Local subnet >Add**.

Figure 12 Local Subnet

Parameter	Description
Name	Name of Local Subnet
IP Address	An IP address for the gateway. This address can be used to access the AP's web interface for configuration and monitoring from devices connected to this subnet
Subnet Mask	Subnet Mask for the network
DNS1	IP address of the primary Domain Name System (DNS) server
DNS2	IP address of the secondary Domain Name System (DNS) server
MTU Size	Default value 1500 bytes – Client can change the value. Maximum limit 1500 bytes - The maximum transmission Unit (MTU) is the maximum size of a single data unit of digital communications that can be transmitted over a network
DHCP Range Start	Starting address of DHCP range.(Enter an address in the same subnet as the Local IP Address)
DHCP Lease Count	Maximum number of clients that can be assigned addresses by DHCP in this subnet
Lease Time	Set lease time. DHCP server leases an address to a device after every interval of set time period
VLAN ID	VLAN ID to segment client traffic arriving from this subnet from other network traffic

Figure 13 Local Subnet – DHCP Reservation

With this feature user can provide fix IP address to the clients. As a result whenever the respective client connects to this Local Subnet, he will get the dedicated fix IP address always.

Bridge Profile

Go to **Configuration > Bridge > Add**
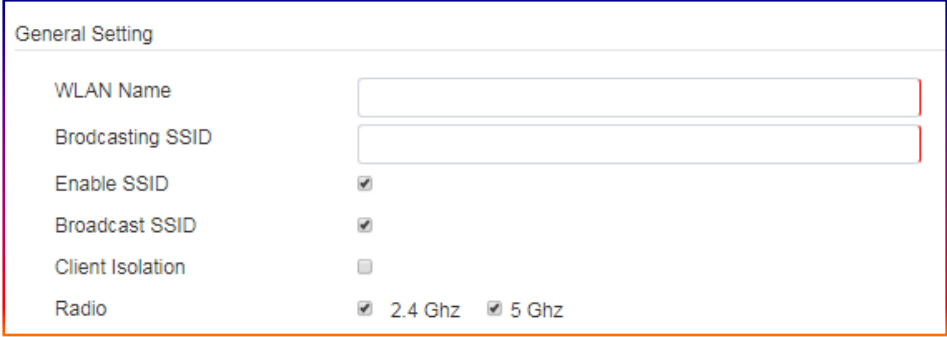
Figure 14 Bridge Profile

Parameter	Description
Name	Profile name
DHCP Server IP	DHCP server IP address of your network
Subnet Mask	Netmask for the network
VLAN ID	Network VLAN ID

Wireless

Go to **Configuration > Wireless > Add**.

Figure 15 Wireless General Setting

Parameter	Description	Default Value
WLAN Name	This Wireless LAN name is unique name for management purposes only and is not visible to wireless clients	
Broadcasting SSID	The SSID name that is visible by the wireless clients (Network). SSID can contain up to 32 alphanumeric characters and are case-sensitive	
Enable SSID	To enable a Broadcasting SSID. Choose Yes/No checkbox to enable/disable the SSID	Enabled
Broadcast SSID	Choose Yes/No checkbox to enable/disable the Broadcasting SSID. By selecting Yes the SSID name is visible to the wireless Clients and will be able to connect to the SSID. By selecting No the SSID name is not visible to the wireless Clients and is in Hidden mode and can add connect to the correct SSID required by the user	Enabled
Client Isolation	Choose Yes/No checkbox to prevent wireless clients from communicating to each other. Wireless client isolation enables subnet restrictions for connected clients. Click Enable if you want to prevent wireless clients associated with the same AP from communicating with each other locally. The default value is disabled	Disabled
Radio	Enable required Radio channels	Enabled Both

Figure 16 Wireless WLAN Setting

Parameter Access Type	Description	Default Value
Access Type		Access Type : Standard
Option 1		
Access Type	Standard	Auth. Method : Open
Auth. Method	Open	
Option 2		
Access Type	Hotspot (WISPr)	
Auth. Method	Open	
Hotspot Profile	Select pre-configured Hotspot profile from dropdown	
Option 3		
Access Type	Standard	
Auth. Method	802.1xEAP	
Server IP Address	RADIUS server primary IP address	
Secondary Server IP Address	RADIUS server secondary IP address	
Authentication Port	RADIUS server Authentication port	
Accounting Port	RADIUS server Accounting port	
Shared Secret	RADIUS server Shared secret provided by RADIUS server provider	
NAS ID	The **NAS**-**Identifier** is a RADIUS attribute that the client uses to identify itself to a RADIUS	

Note:
Hotspot (WISPr): To select "Access Type" Hotspot (WISPr), first need to create Hotspot Profile. To create Hotspot Profile, Go to **Site > Configuration > Hotspot > Add**

Parameter Authentication	Description
Authentication	Open: Any encryption method can be used. It allows you to configure a WPA2 or WPA-Mixed or "none" based encryption. By Choosing a WPA or WPA-Mixed, you can then enter a passphrase or key text of our choice
	802.1xEAP: 802.1X (also known as WPA-Enterprise), is an authentication method by which users are authenticated using an external RADIUS server

Figure 17 Wireless Security Setting

Security Setting includes Encryption Method, Algorithm and Key.

Parameter	Description	Default Value
Encryption	Choose encryption method WPA2, None or WPA-Mixed	WPA2
Algorithm	For encryption method WPA2 choose algorithm AES while for WPA-Mixed choose TKIP+AES algorithm	AES
Passphrase	passphrase (password) of your choice	

Parameter Detail Description	
Encryption	WPA2: WPA encryptions that comply with the 802.11i security standard
	None: No encryption; communications are sent in clear text
	WPA-Mixed: Allows mixed networks of WPA and WPA2 compliant devices. You can use this if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES

Algorithm	AES: This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard
	TKIP: TKIP is a stopgap encryption protocol introduced with WPA to replace the very –insecure WEP encryption at the time

www.qntmnet.com

Figure 18 Wireless Advance Setting

Parameter	Description	Default Value
Routing Option	Bridge to WAN: Forwards packets arriving on this port to the WAN (uplink) port and eventually to their external destinations using Layer 2 forwarding. NAT to WAN: Allows routing of packets to their destinations using Layer 3 Network Address Translation (NAT)	Bridge to WAN
VLAN	VLAN ID	1
Access Control List	Parameter allows controlling which devices are permitted to access your wireless networks	Disable
	Access: select option allows or deny	
	MAC List: devices entered into the Access Controls List are allowed or deny to access wireless network as per selected "Access" parameter. (Maximum limit 64 MAC per ACL profile)	
Enable Rate Limit	Parameter allows controlling upload/download data limit	Disable
	Upload Rate: Set upload data speed per device	
	Download Rate: Set download data speed per device	
Max. Clients (per radio)	Choose maximum number of client associated to the Radio	50

Ethernet Ports

Select **Configuration > Ethernet Port**

Figure 19 Ethernet Port Setting

Parameter	Description	Default Value
Type	This option is used to configure the virtual-LAN (VLAN) parameters for the Ethernet ports on the AP. Port Type: •Trunk Port: Allow multiple VLAN (1~4094); PVID (untagged VLAN ID) configurable. •Access Port: A single VLAN, packets untagged	Port : Enabled Type : Trunk Port VLAN :Untag ID : 1
VLAN	Assign Untagged VLAN ID handled on the port	
Members	In case of Trunk port, assign Member VLAN ID's with reference to respective port with comma separation. Can manage multiple VLAN ID's	

Hotspot

Select **Configuration > Hotspot**

Figure 20 Hotspot Profile Setting

Parameter	Value	Description
Hotspot Profile	Name	Name of Hotspot profile
Auth Profile	Server IP Address	Authentication server primary IP address
	Secondary Server IP	Authentication server secondary IP address
	Authentication Port	Authentication server authentication port
	Accounting Port	Accounting server accounting port
	Shared Secret	Shared Secret provided by RADIUS server provider
Captive Portal	Portal URL	Captive portal (splash page) redirection URL
	Portal Secret	Portal secret
User Session	Session Timeout	Assign time limit after which user will get disconnects and required to login again
	Ideal Timeout	It's a period of inactivity from user. When there is no traffic from the user, once the timeout is reached, user will be disconnected from the Hotspot
Network Settings	DNS Domain	Use this option to Domain name for the Hotspot
	NAS ID	Enter the Network Access Server identifier of this device. The NAS-ID parameter is sent in RADIUS access and accounting request messages
Walled Garden	Walled Garden	Use this option to allow domains which can be accessed by users without Authentication. Clients accessing these domains will not be redirected to the splash page

SNMP

Select **Configuration > SNMP**

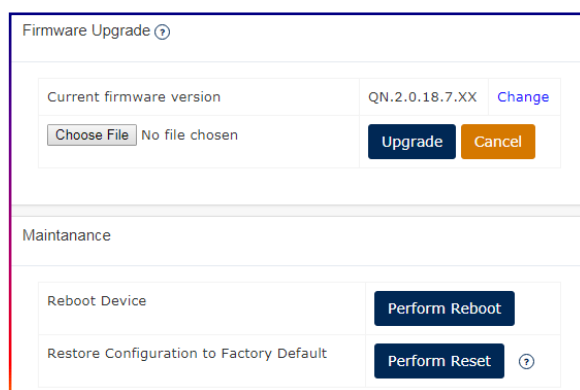Figure 21 SNMP Setting

Parameter	Description
Enable SNMP	To enable SNMP client services
Server	SNMP server IP address
Server	SNMP backup server IP
Port	SNMP communication port on server
Community	Community string
v1	Enable SNMP version 1 (As per the requirement)
v2	Enable SNMP version 2c (As per the requirement)
v3	Enable SNMP version 3 (As per the requirement)

Management

Use the Management option to perform below listed management task.
- To Upgrade Access Point Firmware.
- To Perform Reboot device.
- To Perform Restore Configuration to Factory Default.

Figure 22 Management option setting

Management	
Firmware Upgrade	
Current Version	Current running firmware version of the Access Point
Choose File	Click "Choose File" option to upload a downloaded firmware file to perform a firmware upgrade
Maintenance	
Reboot Device	Click "Perform Reboot" button to Reboot the Access Point
Restore Configuration to Factory Default	Click "Perform Reset" button to reset the configuration to the factory default settings. Your current configuration will be discarded. The device will be rebooted automatically to allow the settings to take effect

Diagnostics

Diagnostic option is a tool for diagnostics and connectivity test.

Figure 23 Diagnostics

Diagnostics	
Ping	Ping utility to manually check the connectivity of a particular LAN/WAN connection
Trace route	Trace route utility to analyze the connection path of a LAN/WAN connection
NsLookup	NsLookup utility for troubleshooting DNS problems, such as hostname resolution

Logs

Logs option is a tool to view Logs.

#	Datetime	Log Description
1		/usr/cloudfiles/QN_121700007_28466DeviceRadio_1561966835
2		/usr/cloudfiles/QN_121700007_APGroupSlaveRadio_1561966591
3		/usr/cloudfiles/QN_121700007_1211730011AF28466APGroupsSetting_1561965608
4		/usr/cloudfiles/QN_121700007_1211730011AF28466APGroupsSetting_1561963865

Figure 24 Logs