QUANTUM NETWORKS

QUANTUM RUDDER®

Network and Services Controller

USER GUIDE

Copyright Information

Document Abstract

This document provides detailed instructions for configuring and managing Quantum Rudder, a web-based cloud controller.

Glossary

The 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 IP addresses to client devices.
Static	A static Internet Protocol (IP) address, or static IP address, is a fixed IP address assigned to a device manually.
PPPoE	Point-to-Point Protocol over Ethernet, a network protocol for encapsulating Point-to-Point Protocol (PPP) frames inside Ethernet frames.
WLAN	A Wireless Local Area Network is a wireless network that transfers data between wireless devices.
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 user network using a 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 in 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.
AES	AES (Advanced Encryption Standard) is an encryption protocol that is much more secure as it uses longer encryption keys.
Band steering	Band steering detects the capability of the wireless client device. If it is dual-band capable, it pushes the client to connect to the less congested 5GHz network.
Channel Bandwidth	By increasing the channel width, we can increase the speed and throughput of a wireless broadcast. By default, the 2.4 GHz frequency uses a 20 MHz channel width.802.11n can combine two 20 MHz channels to form an effective bandwidth of 40MHz. 40 MHz enables higher data transmission rates to be achieved as compared to 20 MHz. When user select 20/40 MHz mode, the router decides to use 20 or 40 MHz based on the interference/contention the router detected.

SNMP	SNMP, which stands for Simple Network Management Protocol, is a standard protocol used to manage and monitor devices on a network.
DL	Downlink
GE	Gigabit Ethernet
GUI	Graphical User Interface
IP	Internet Protocol
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control (MAC) manages device access and data transmission in a network using unique MAC addresses
MTU	Maximum Transmission Unit
QoS	Quality of Service
RF	Radio Frequency
TCP	Transmission Control Protocol
UDP	User Datagram Protocol

Web Interface Feature List

List of available features admin can manage and configure from Quantum RUDDER web interface.

- Monitor Sites, Devices, Wireless Clients
- Manage Multiple Sites
- Manage Access Point's
- Manage WLANs
- Guest Access Management
- General Reports
- Syslog Reports
- SMTP and SMS profiles for notifications
- Administration activity like Configuration, Firmware Upgrade
- Manage Hotspots
- Manage Quantum Secure+
- Layer 2 ACL, Layer 3 ACL, OS Policy, Session Control
- Trouble Shooting Tools, SNMP, Floor Plan and Outdoor Plan Services
- Services, Logs Reports
- Support
- Manage Security Services
- Manage all Quantum Profiles

Account Setup on Quantum Rudder

- Browse https://rudder.qntmnet.com.
- Click "**Create New Account"** to sign up for a new account.

Figure 1

- Follow the steps as guided on the screen for Registration.
- Verify the Quantum Rudder account from the registered Email ID.
- Once the account gets validated, it turns the page to "Add License Key" (User will get the license key from the respective (Partner / Resource).
- Account on Quantum RUDDER© (Quantum Networks' Cloud Controller) is now ready to use.

Login to Quantum Rudder Web Interface

- Go to https://rudder.qntmnet.com
- Enter the registered credentials and click Login

Figure 2

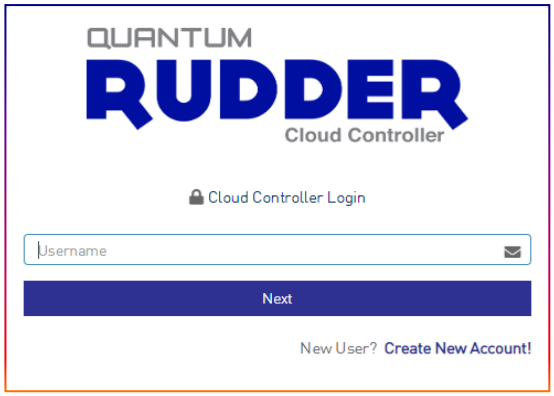


Figure 3

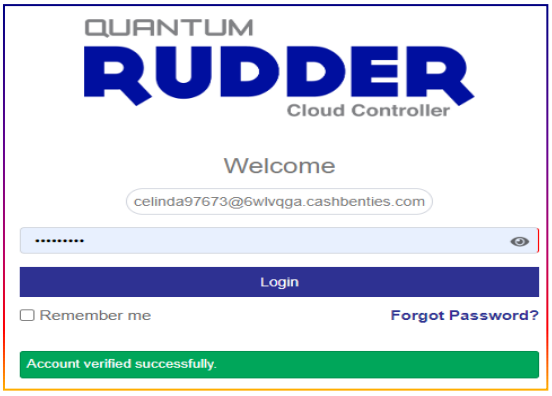


Figure 4

Successful log in redirects to Quantum RUDDER dashboard.

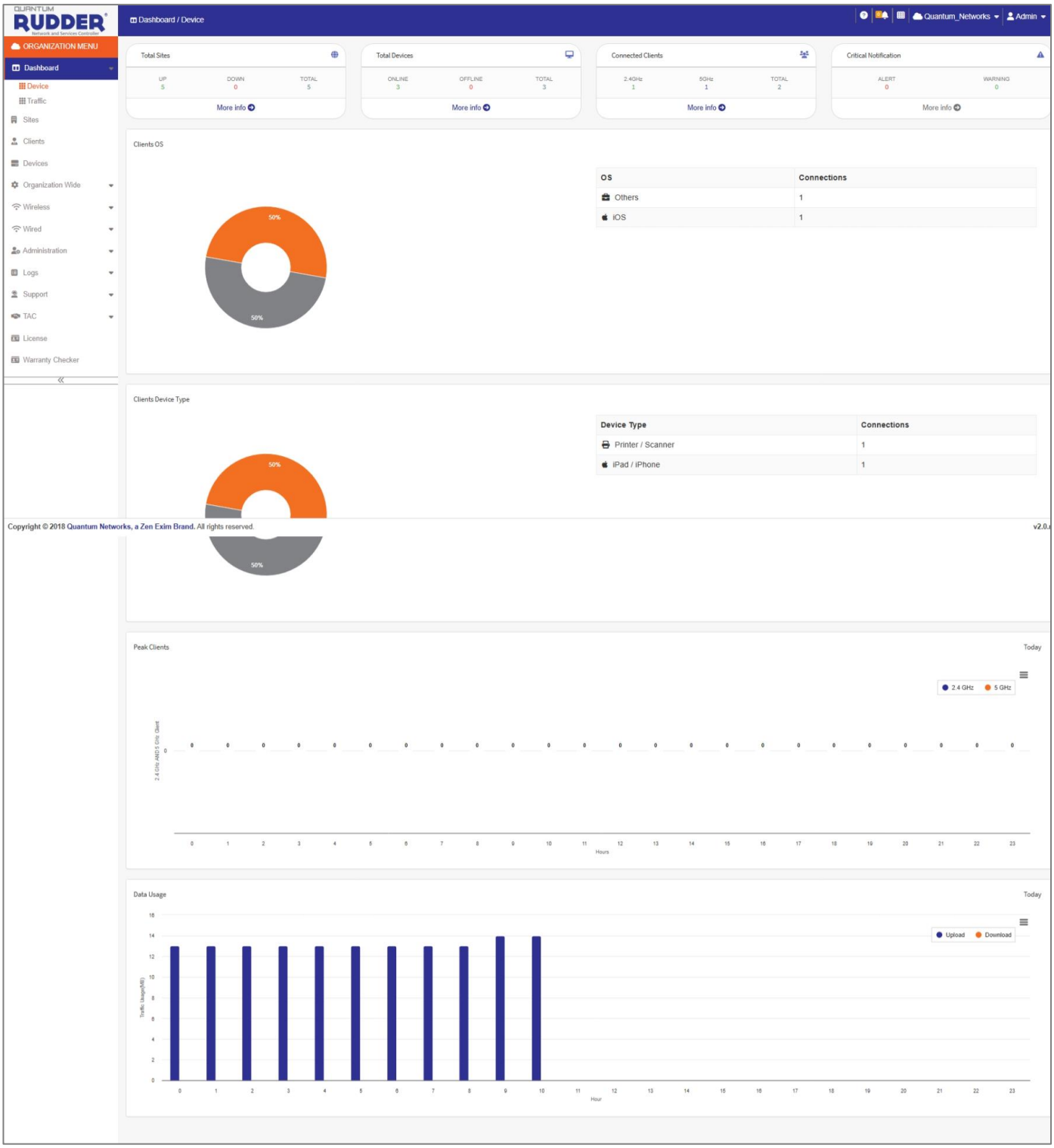


Figure 5

Organization Menu

Navigating the Quantum Rudder Pannel

The Quantum Rudder web interface is a graphical user interface (GUI) for managing and monitoring user networking devices, venues, and wireless networks.

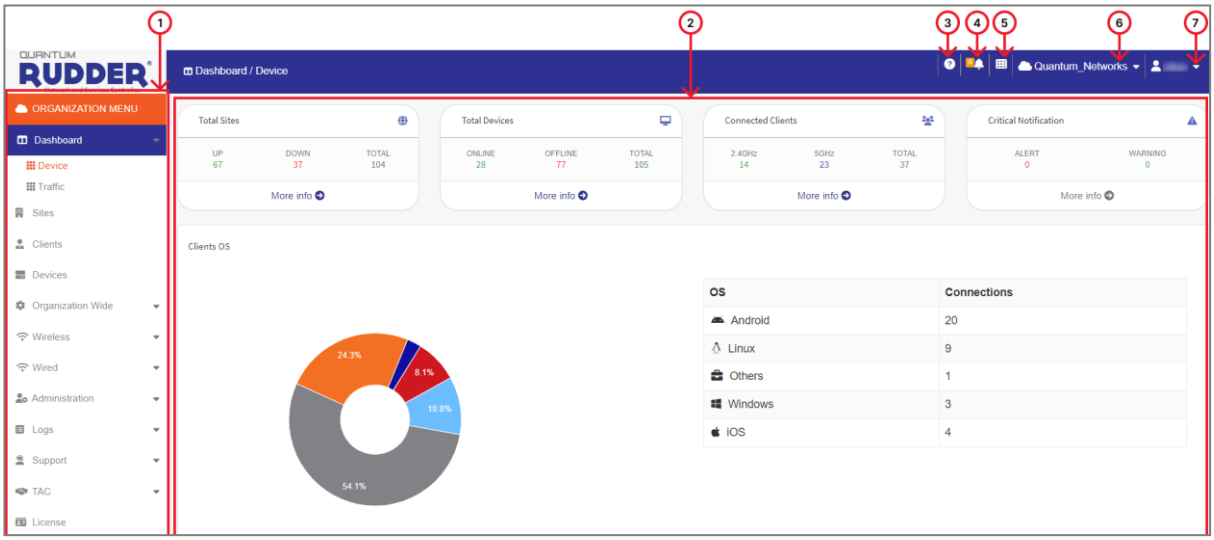


Figure 6

Sr.	Name	Description
1	Navigation bar	Use the navigation bar to navigate through the main pages of Rudder Cloud, which include: o Dashboard o Sites o Clients o Devices o Organization Wide o Wireless o Administration o Logs o Supports o TAC o License o Warranty Checker
2	Content area	When a user clicks an item on the navigation bar, the related information (tables, lists, graphs, configuration options, etc.) is displayed in the content area. By default, the following information is shown: o Total Sites o Total Devices o Connected Clients

		o Critical Notification o Client OS o Client Device Type o Peak Clients o Data Usage
3		Help: To access documentation.
4		Critical Alerts: Critical alerts include device reboot, high CPU utilization, high memory utilization, and exceeded maximum connected clients.
5		Will provide direct access to Quantum Rudder, Quantum UnGrid, and QIM (Quantum Identity Management).
6		Edit Current Cloud: To edit the current cloud, click the "Cloud" icon and select **"Edit Current Cloud."** Modify as required.
7		Cloud Admin Detail: This option allows the admin user to view or edit existing details. Change Password: This option allows the user to change the admin password.

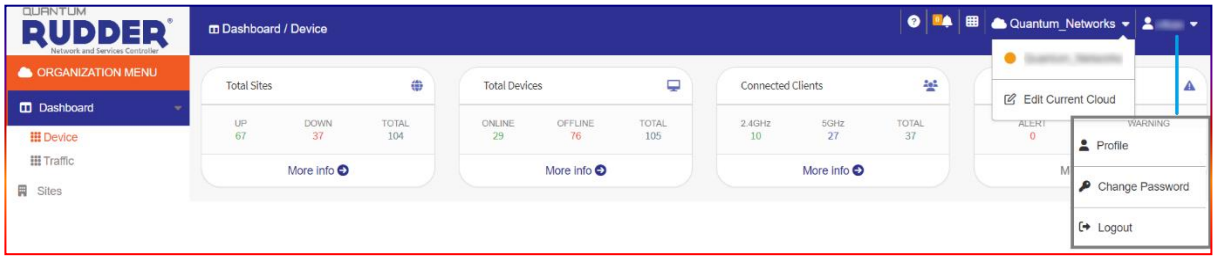


Figure 7

Top panel	The top panel provides “Critical Alerts,” “Edit Current Cloud,” and “Manage Cloud Admin” features.
Side panel	Admin can select the required option to view, edit, or create a new configuration.
Main screen	Selected parameter options where the admin can work.

Icon Description

Icon	Description
	Search : To Search.
	Edit : To Edit.
	Delete : To Delete.
	Export : Export to excel file.
	Transfer : To Transfer AP from one site to another site.
	Alerts : View critical Alerts.
	Cloud Admin : Edit Cloud Admin detail.
	Current Cloud : Edit Cloud detail.
	Settings : Select/change parameter fields for display.
+ Add	**Add** : Add new site or any other related parameters.
Clear Log	**Clear Log** : clear all logs till date.

Dashboard

Quantum Rudder dashboard provides a summary of events. It gives summarized details of total sites, device information, connected clients, critical alarm and warning if any.

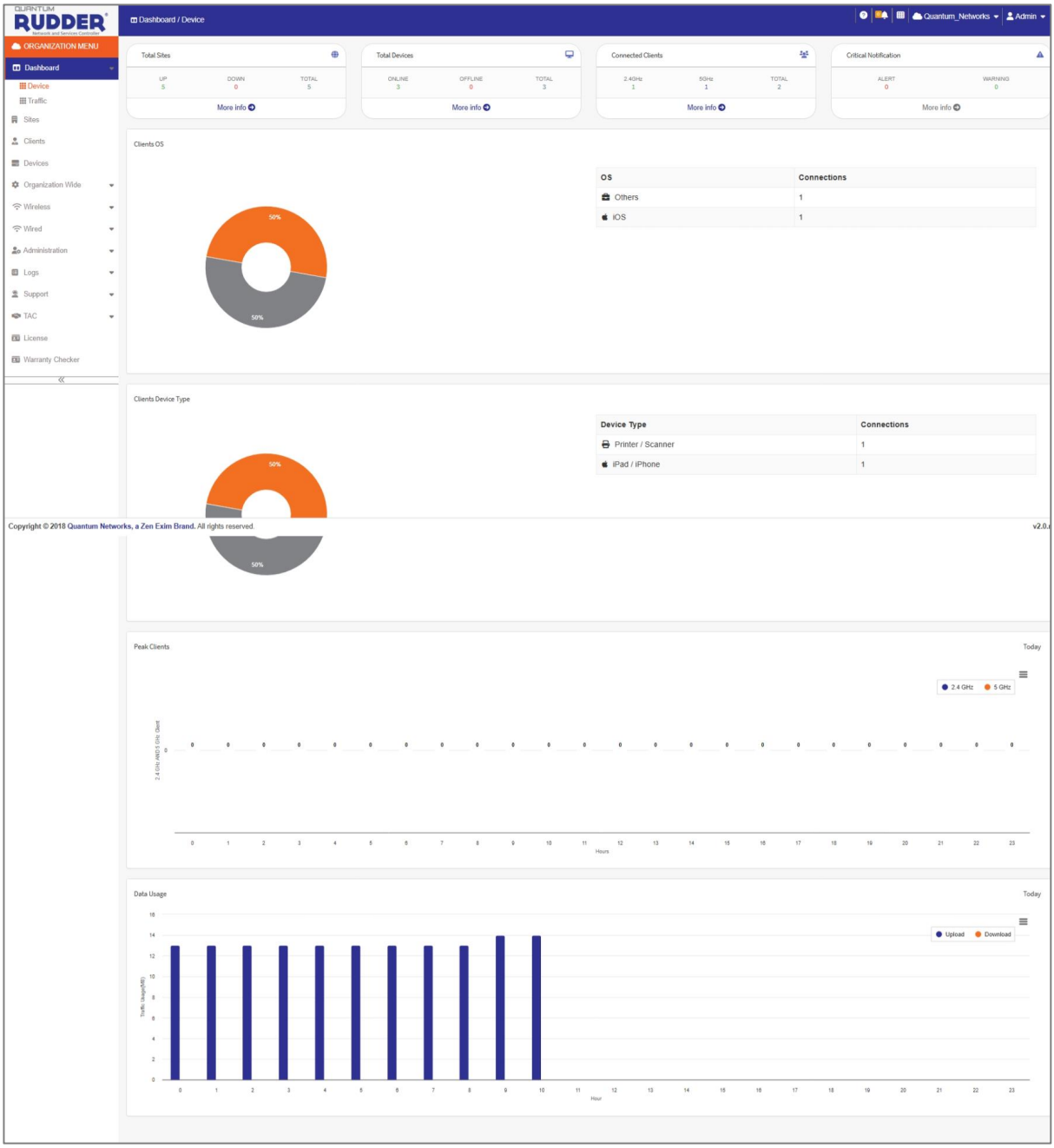


Figure 8

Devices

Total Sites

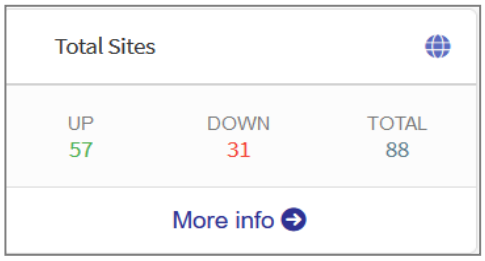


Figure 9

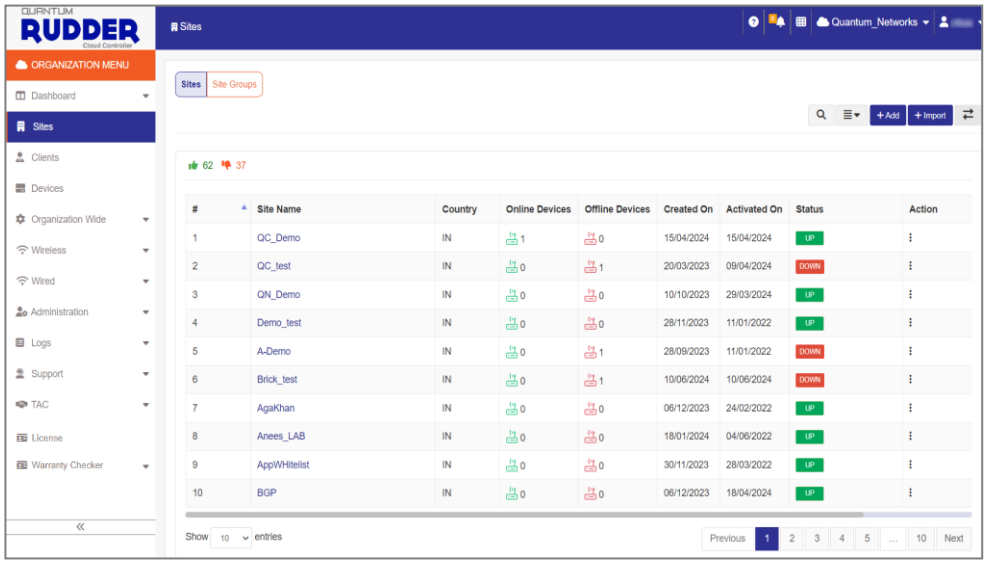


Figure 10

Total Sites	
Up	The total number of sites with online devices is considered 'UP.' A site's status will be 'UP' even if no device is registered or provisioned.
Down	Total number of down sites. A site is considered "down" if the devices cannot communicate with Quantum Rudder.
Total	Number of sites created on Quantum Rudder.
More info	Detailed information.
Total Site – More info	
Site name	Displays the name of the site.
Country	Site location.
Online devices	Total number of Online devices on the site.
Offline devices	Total number of Offline devices on the site.
Created on	Site creation date.
Status	The site status (Up or Down).
Action	Admin can edit or delete the site.

Total Devices

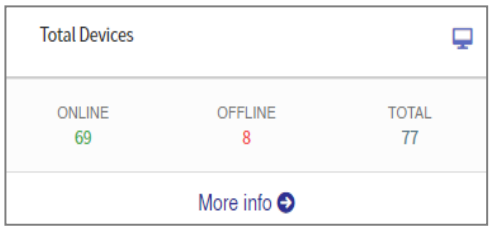


Figure 11

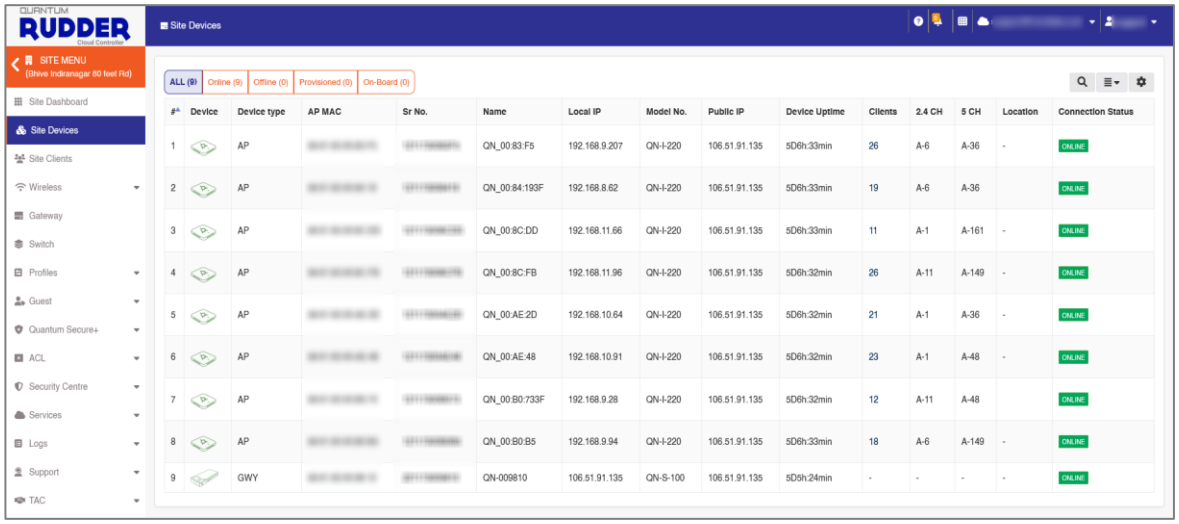


Figure 12

Total Device: Provides all devices connected to Quantum RUDDER. An administrator can filter the data by Online, Offline, and Provisioned device.

Total Device	
Online	Total number of access points functioning and linked to the cloud controller.
Offline	Total number of devices disconnected.
Total	Total number of devices registered or provisioned.

Total Device –Click More info for further details	
Device type	Device type whether it is an Access point / Switch / Gateway.
AP MAC	MAC address of the device.
Sr. no	The serial number of devices.
Name	Device name.
Local IP	Local IP address of the device.
Model no.	Device model number.
Site name	Site name under which the AP has been Registered/Provisioned.
Public IP	A public IP is assigned to the Access Point.
Device uptime	It will show how long the AP has been up since it has been powered up or restarted

Clients	The number of wireless clients connected to an access point.
2.4 CH	The configured channel in the device, where "M-XX" represents manual channel settings while "A-XX" represents the channel has been selected automatically.
5 CH	
Location	User define the location of the Access Point
Connection status	Current status of the device (Online / Offline?)

Connected Clients

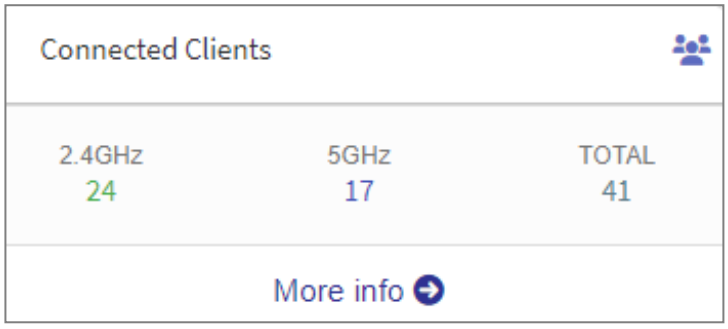
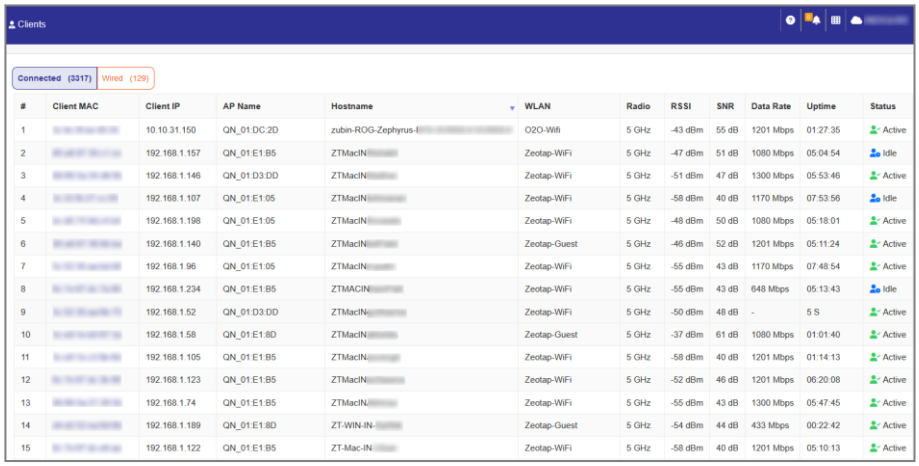


Figure 13

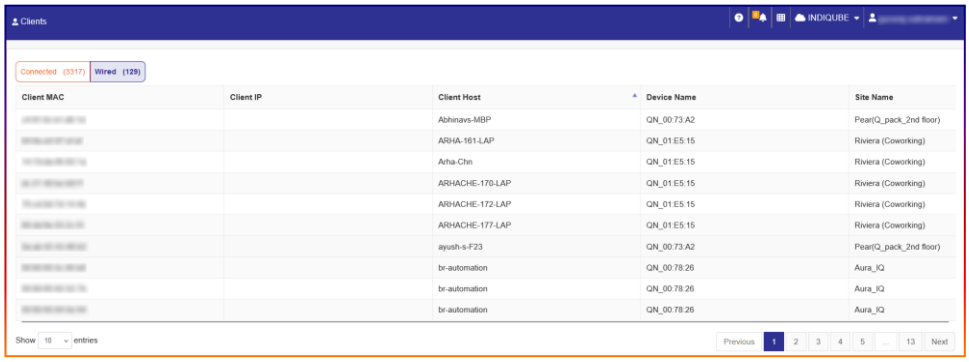
Connected Clients



#	Client MAC	Client IP	AP Name	Hostname	WLAN	Radio	RSSI	SNR	Data Rate	Uptime	Status
1	[redacted]	10.10.31.150	QN_01:DC:2D	zubin-ROG-Zephyrus-[redacted]	O2O-Wifi	5 GHz	-43 dBm	55 dB	1201 Mbps	01:27:35	Active
2	[redacted]	192.168.1.157	QN_01:E1:B5	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-47 dBm	51 dB	1080 Mbps	05:04:54	Idle
3	[redacted]	192.168.1.146	QN_01:D3:DD	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-51 dBm	47 dB	1300 Mbps	05:53:46	Active
4	[redacted]	192.168.1.107	QN_01:E1:05	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-58 dBm	40 dB	1170 Mbps	07:53:56	Idle
5	[redacted]	192.168.1.198	QN_01:E1:05	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-48 dBm	50 dB	1080 Mbps	05:18:01	Active
6	[redacted]	192.168.1.140	QN_01:E1:B5	ZTMacIN[redacted]	Zeotap-Guest	5 GHz	-46 dBm	52 dB	1201 Mbps	05:11:24	Active
7	[redacted]	192.168.1.96	QN_01:E1:05	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-55 dBm	43 dB	1170 Mbps	07:48:54	Active
8	[redacted]	192.168.1.234	QN_01:E1:B5	ZTMACIN[redacted]	Zeotap-WiFi	5 GHz	-55 dBm	43 dB	648 Mbps	05:13:43	Idle
9	[redacted]	192.168.1.52	QN_01:D3:DD	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-50 dBm	48 dB	-	5 S	Active
10	[redacted]	192.168.1.58	QN_01:E1:8D	ZTMacIN[redacted]	Zeotap-Guest	5 GHz	-37 dBm	61 dB	1080 Mbps	01:01:40	Active
11	[redacted]	192.168.1.105	QN_01:E1:B5	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-58 dBm	40 dB	1201 Mbps	01:14:13	Active
12	[redacted]	192.168.1.123	QN_01:E1:B5	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-52 dBm	46 dB	1201 Mbps	06:20:08	Active
13	[redacted]	192.168.1.74	QN_01:E1:B5	ZTMacIN[redacted]	Zeotap-WiFi	5 GHz	-55 dBm	43 dB	1300 Mbps	05:47:45	Active
14	[redacted]	192.168.1.189	QN_01:E1:8D	ZT-WIN-IN-[redacted]	Zeotap-Guest	5 GHz	-54 dBm	44 dB	433 Mbps	00:22:42	Active
15	[redacted]	192.168.1.122	QN_01:E1:B5	ZT-Mac-IN[redacted]	Zeotap-WiFi	5 GHz	-58 dBm	40 dB	1201 Mbps	05:10:13	Active

Figure 14

Wired Clients



Client MAC	Client IP	Client Host	Device Name	Site Name
[redacted]		Abhinavs-MBP	QN_00:73:A2	Pear(Q_pack_2nd floor)
[redacted]		ARHA-161-LAP	QN_01:E5:15	Riviera (Coworking)
[redacted]		Arha-Chn	QN_01:E5:15	Riviera (Coworking)
[redacted]		ARHACHE-170-LAP	QN_01:E5:15	Riviera (Coworking)
[redacted]		ARHACHE-172-LAP	QN_01:E5:15	Riviera (Coworking)
[redacted]		ARHACHE-177-LAP	QN_01:E5:15	Riviera (Coworking)
[redacted]		ayush-s-F23	QN_00:73:A2	Pear(Q_pack_2nd floor)
[redacted]		br-automation	QN_00:78:26	Aura_IQ
[redacted]		br-automation	QN_00:78:26	Aura_IQ
[redacted]		br-automation	QN_00:78:26	Aura_IQ

Show 10 entries
Previous 1 2 3 4 5 ... 13 Next

Figure 15

Connected Clients	
2.4GHz	Provides the number of clients connected on 2.4GHz
5GHz	Provides the number of clients connected on 5GHz
Total	Provides the total number of connected clients on all sites

Connected Clients – Click More info for further details	
Client MAC	Client MAC address
Client IP	IP address of the client device
AP name	Respective AP name
Hostname	Hostname
Stream	Signal stream
WLAN	WLAN name
Radio	Connected client radio detail
Mode	AP radio mode
RSSI	Wireless signal strength (Between AP and connected client)
Tx	Upload rate of the client device
Rx	Download rate of the client device
Data rate	Expected data rate
Uptime	AP uptime
Status	Current Status of the AP
Channel	2.4 GHz and 5 GHz channel
Device owner	Name registered under Quantum identity manager.
Device alias	Name of the AP alias
Device type	Type of the AP
AP location	Display the AP location
AP site name	The site name information helps administrators identify and manage access points within a network.
User name	User name of the AP
Action	The administrator can edit or delete internet access or disconnect the user.

Critical Notification

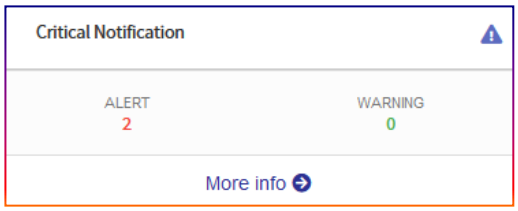


Figure 16

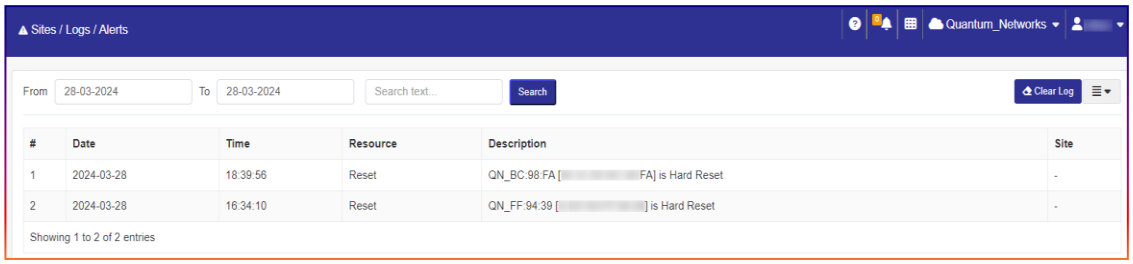


Figure 17

Critical Alert	
Alert	Alerts
Warning	Warning, if any

Critical Alert – Click More Info for further details	
Resource	Event happened
Created on date	Alert / Warning generation date
Created on time	Alert / Warning generation time
Description	Alert notification reason
Site	Site name

Note: The administrator can view graphical analytics for active clients in the cloud, including their connected device OS, client trends, and traffic usage.

Traffic

It allows the administrator to monitor the bandwidth consumption of connected client devices based on domain names, protocols, and applications. The administrator can apply filters on SSID, devices, or a specific duration (date).

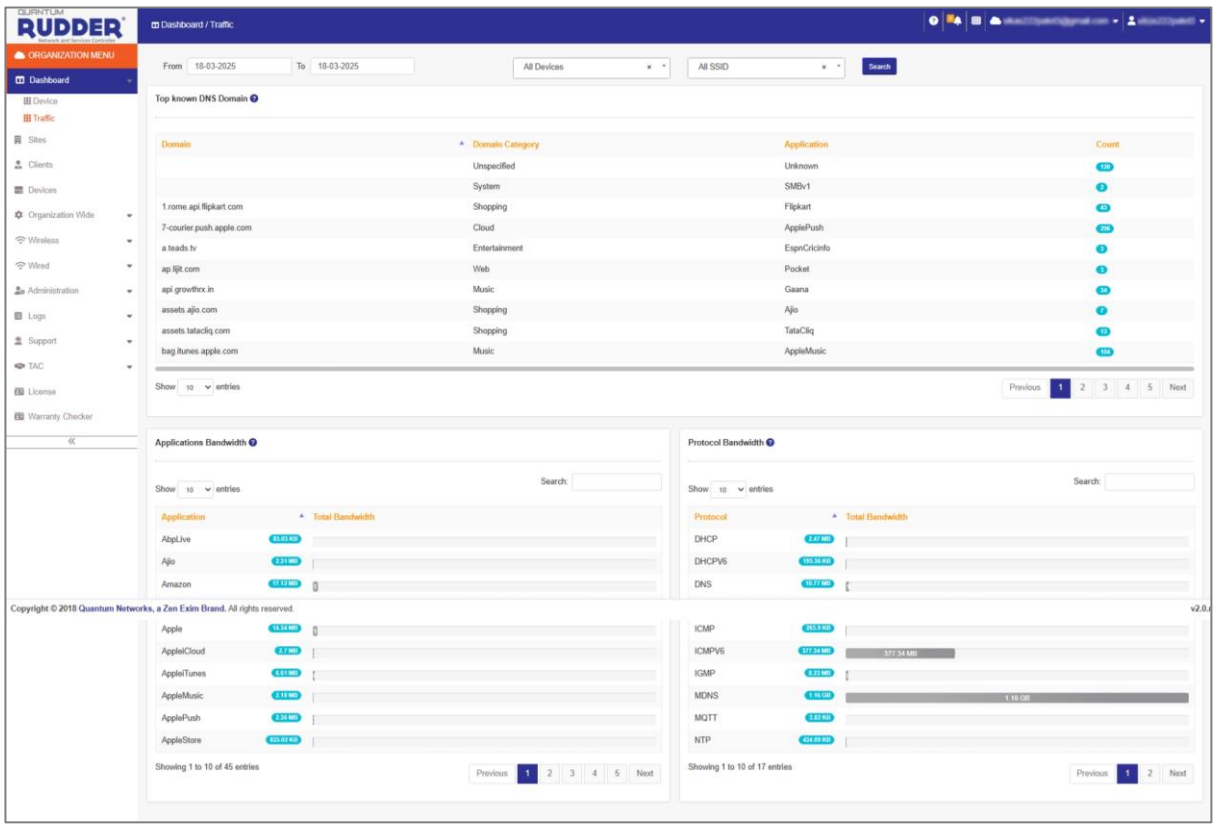


Figure 18

Sites

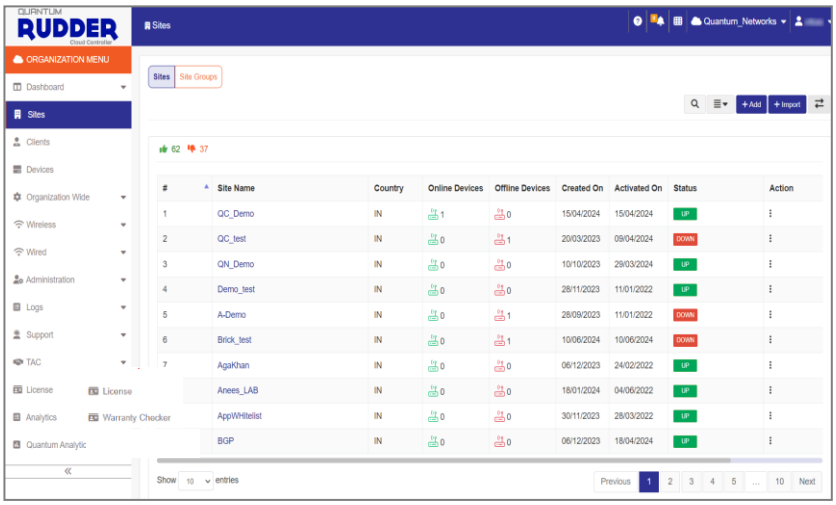


Figure 19

To create a new site, go to the **Sites** section and click "**Add**".

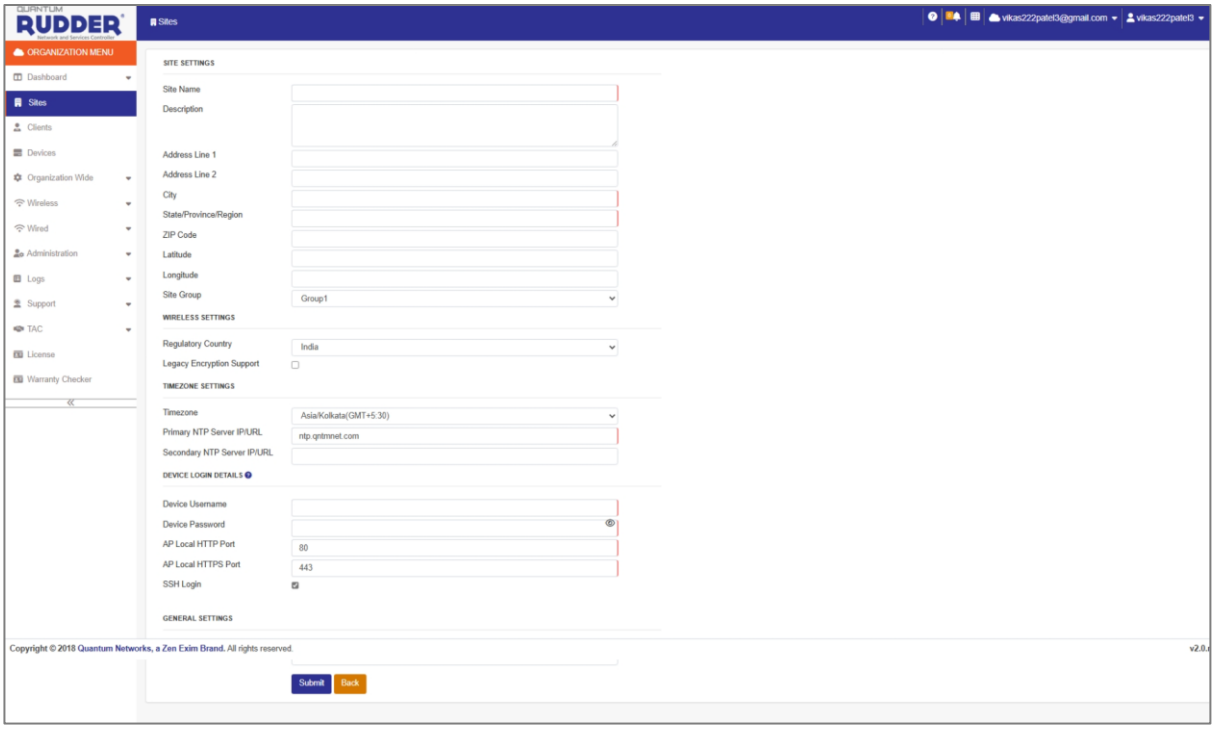


Figure 20

Parameter	Description	Default Value
Site Settings		
Site name	Name of the site.	None
Description	Reference details for the site.	None
Address line 1	Define full address.	None

Address line 2		None
City	City name where the site is located.	None
State/Province/Region	Region	None
ZIP Code	Location's ZIP code.	None
Latitude	Location's latitude.	None
Longitude	Location's longitude.	None
Site group	Select site group from the drop-down list.	None
Wireless Settings		
Regulatory country	Country info.	India
Legacy encryption support	Enables support for legacy encryption methods (WEP).	Disabled
Time zone Settings		
Time zone	The AP allows administrators to set the local time offset from Coordinated Universal Time (UTC) or Greenwich Mean Time (GMT).	Asia/Kolkata (GMT +5:30)
Primary NTP server IP/URL	The AP's primary NTP server IP address or URL synchronizes time across networked devices to ensure accuracy and consistency.	ntp.qntmnet.com
Secondary NTP Server IP/URL	Secondary NTP server IP address or URL.	None
Device Login Details: Allows the administrator to configure a username and password to log in to the local GUI of the device.		
Device Username / Password	Define the device username and password used for local device login.	None
AP local HTTP port	The specific port number on which the Access Point (AP) listens for HTTP communication within the local network.	80
AP local HTTPS port	The specific port number on which the Access Point (AP) listens for HTTPS communication within the local network.	443
SSH login	Allows the administrator to restrict or permit CLI access to the device through the SSH protocol.	Enabled
General Settings		
Do user want to clone the site?	Allows cloning the configuration of another site.	Disabled

Dashboard

The Site dashboard provides summarized information about the selected site.

Device

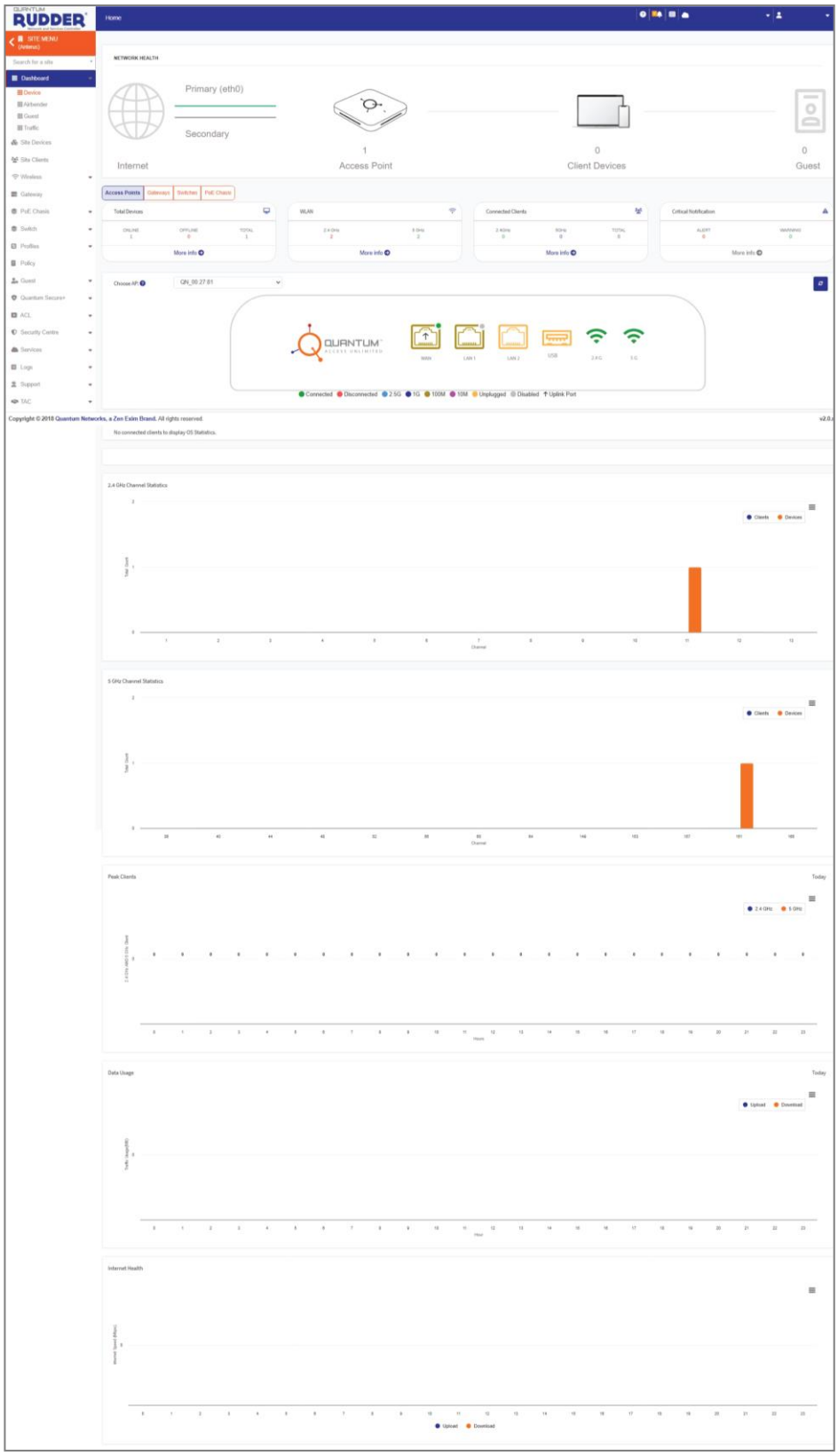


Figure 21

Parameter	Description
Network health	This option displays the overall site's internet connectivity status. In router mode, it shows which port is active as WAN and its status. It also indicates whether the currently active WAN port is primary or secondary.
Internet health	The enabled parameter displays the upload and download internet bandwidth available on the access point during the selected period.
Total devices	This option displays the current AP status, showing the number of Access Points that are online, offline, or provisioned at a particular site. Click "More Info" for further details.
WLAN	Number of WLAN profiles created for the site.
Connected clients	Total wireless users connected and the number of connected guests with critical notifications.
Critical notification	Critical alerts include device reboot, high CPU and memory utilization, and the maximum limit of connected clients, if applicable.
AP / Gateway /Switches	Displays the number of connected Access Points.
Gateway status	Displays the status of the connected gateway devices in the network.
Clients OS	Displays the client list along with their respective operating systems (OS).
Peak clients	It displays the number of clients connected to the network each hour in the form of a graph.

Note: Click “More Info” for further details.

Airbender

"Airbender" provides insights into channel usage and interfering neighbor APs on 2.4GHz and 5GHz bands. It helps identify congestion and interference, allowing users to optimize channel selection and improve network performance.

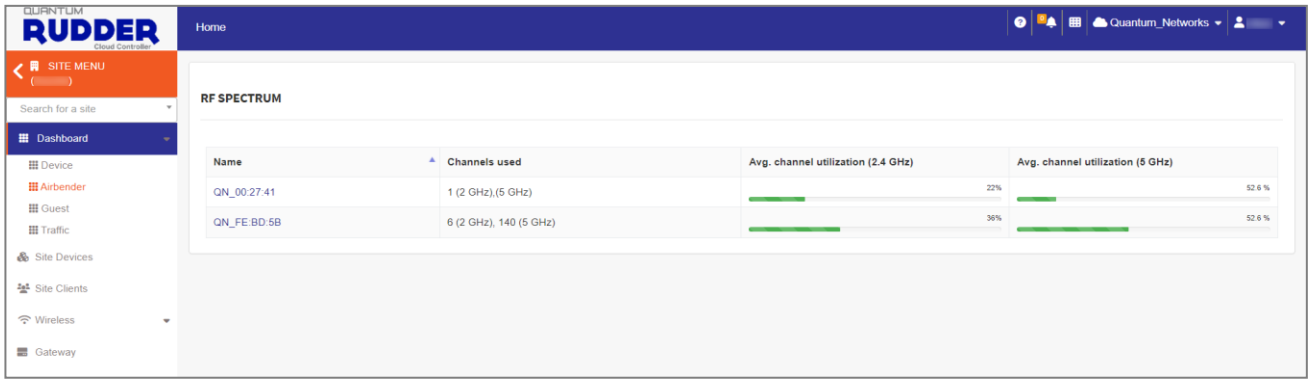


Figure 22

Utilization (2.4 GHz)

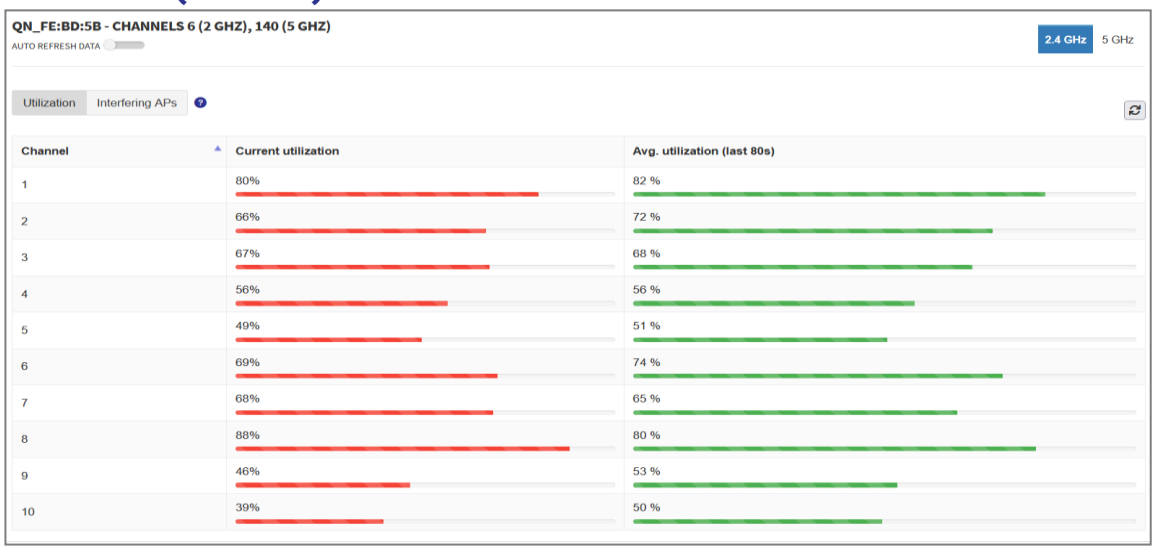


Figure 23

Utilization (5 GHz)

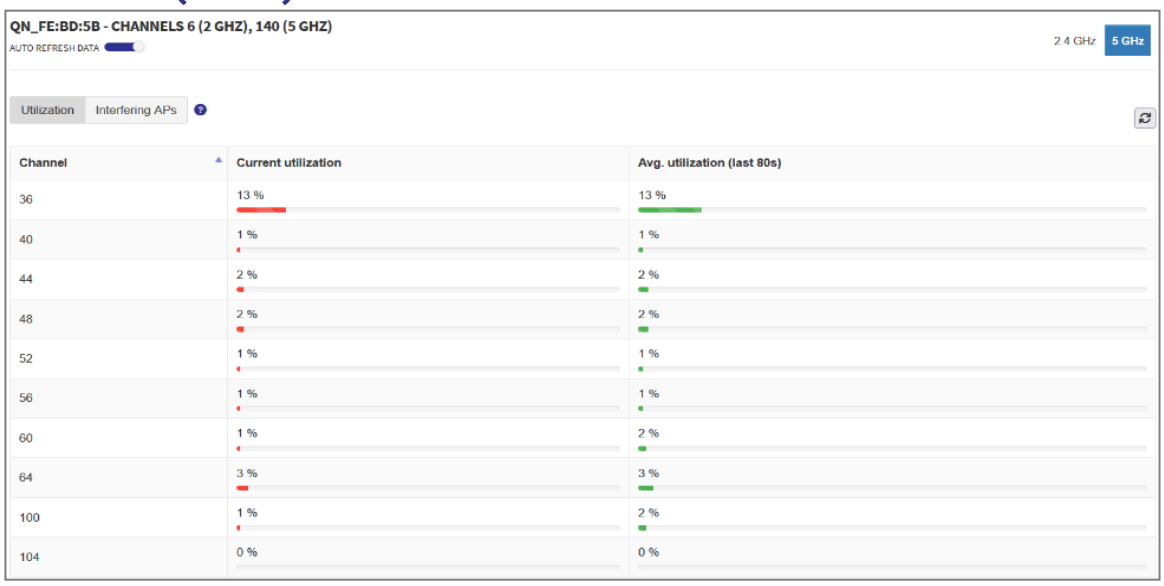


Figure 24

Parameter	Description
Utilization 2.4 GHz and 5 GHz	**Channel**: Lists of functioning channels.
	Current utilization: Displays the current airtime utilization channels on each band.
	Avg. utilization (last 80s): This shows the average utilization of airtime per 80 seconds.

Interfering Aps (2.4 GHz)

Figure 25

Interfering Aps (5 GHz)

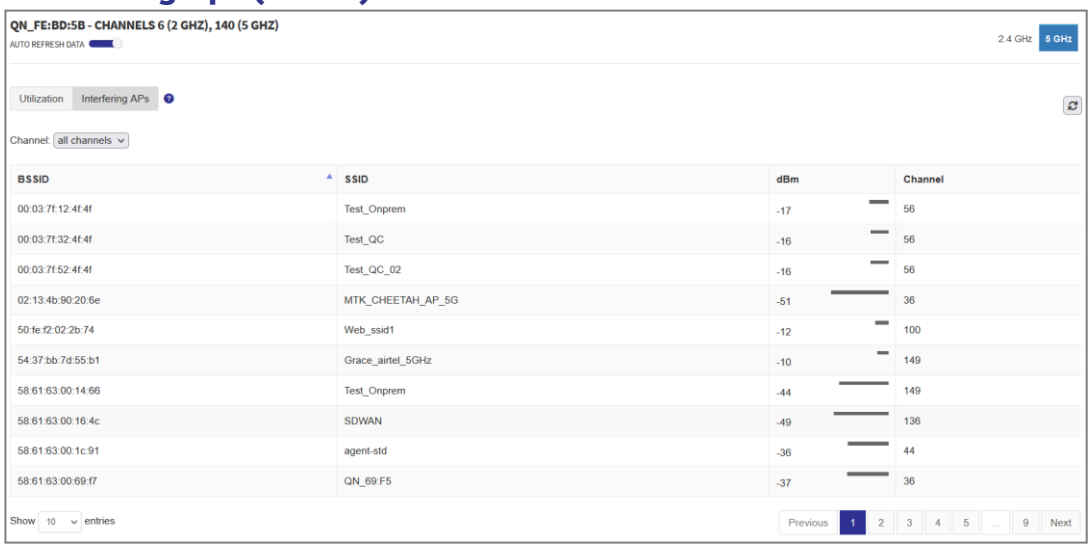


Figure 26

Parameter	Description
<u>Interfering Aps</u> 2.4 GHz and 5 GHz	**BSSID**: Displays Basic Service Set Identifier (BSSID) of SSID.
	SSID: Displays the name of SSID, creating interference on a particular channel.
	dBm: Displays the signal strength of SSID.
	Channel: Display the channel number on which SSID is broadcasted.

Guest

Displays key network metrics, including the total number of new registrations for the current day, successful authentications, unique authentications, login page visits, active subscribers, average connection time per subscriber, sub-organizations, hotspots under the organization, authenticated device breakdown by operating system, utilization by mobile/tablet/large screens, and top subscribers by data usage and connection time.

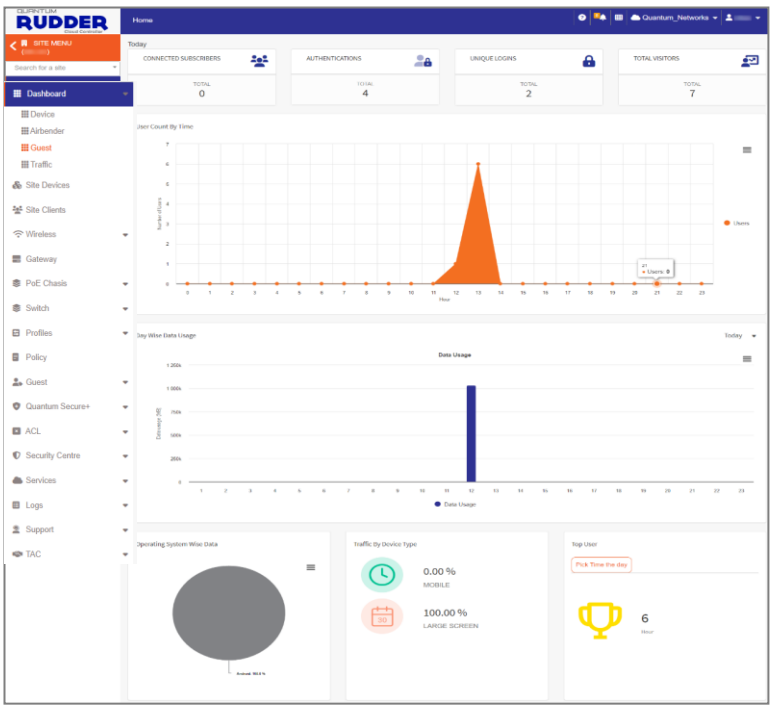


Figure 27

Parameter	Description
Connected subscribers	The number of devices or users currently connected to a specific Access Point.
Authentications	Total number of users authenticated through guest SSID logins.
Unique logins	Total number of unique users who logged into the Guest SSID.
Total visitors	Total number of visitors who have connected to the guest SSID in the cloud
User count by time	The number of visitor users connected over time, displayed as a chart.
Day wise data usage	The daily data usage of the guest user is shown as a chart.
Operating system wise data	Shows guest users' data usage based on their operating system, depicted in a chart.
Traffic by device type	Shows traffic based on device type, categorized as "Large Screen" or "Mobile Screen," and displayed as a percentage.
Top user	Show the user who logs in the most during a given day.

Traffic

It displays bandwidth consumption by domain, protocol, and application. Users can view data for all SSIDs and devices or apply filters for specific SSIDs and devices. Additionally, users can select a date range to view details within the specified period.

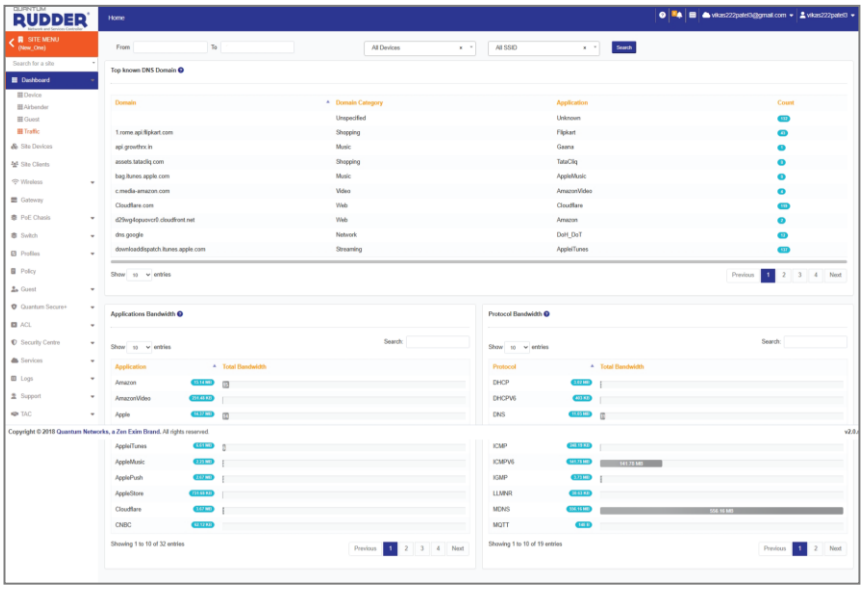


Figure 28

Parameter	Description
DNS Domains	Displays data usage by domains, based on the domain name, application name, and category.
App Bandwidth	Displays data usage, based on Applications.
Protocol Bandwidth	Displays data usage, based on Protocols.

Site Devices

This option displays details of all provisioned Access Points, including their current status (Online, Offline, or Provisioned) and a consolidated report for all.

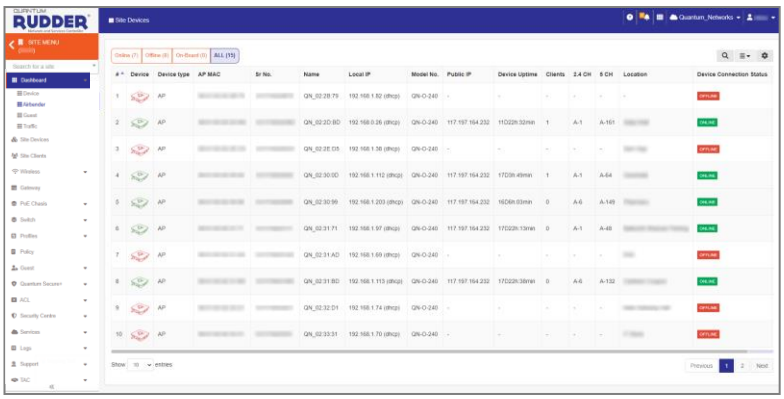
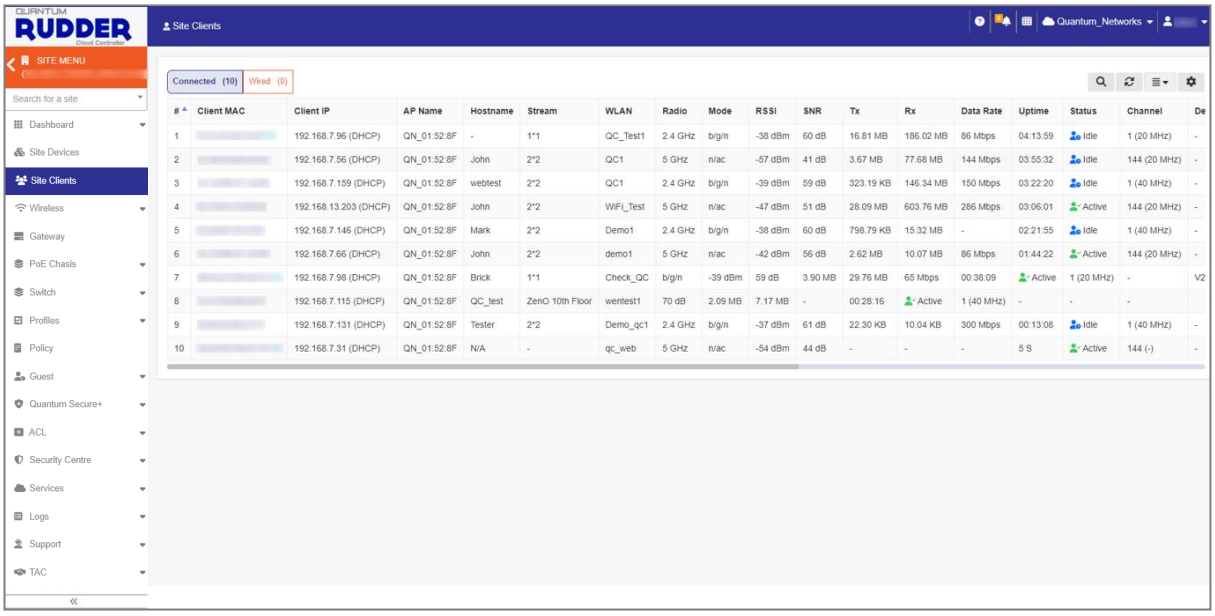


Figure 29

Site Clients

This option provides details of all client devices used by users/guests connected across the site.



#	Client MAC	Client IP	AP Name	Hostname	Stream	WLAN	Radio	Mode	RSSI	SNR	Tx	Rx	Data Rate	Uptime	Status	Channel	De
1		192.168.7.96 (DHCP)	QN_01:52:8F	-	1*1	QC_Test1	2.4 GHz	b/g/n	-38 dBm	60 dB	16.81 MB	186.02 MB	86 Mbps	04:13:59	Idle	1 (20 MHz)	-
2		192.168.7.56 (DHCP)	QN_01:52:8F	John	2*2	QC1	5 GHz	n/ac	-57 dBm	41 dB	3.67 MB	77.68 MB	144 Mbps	03:55:32	Idle	144 (20 MHz)	-
3		192.168.7.159 (DHCP)	QN_01:52:8F	webtest	2*2	QC1	2.4 GHz	b/g/n	-39 dBm	59 dB	323.19 KB	146.34 MB	150 Mbps	03:22:20	Idle	1 (40 MHz)	-
4		192.168.13.203 (DHCP)	QN_01:52:8F	John	2*2	WiFi_Test	5 GHz	n/ac	-47 dBm	51 dB	28.09 MB	603.76 MB	286 Mbps	03:06:01	Active	144 (20 MHz)	-
5		192.168.7.146 (DHCP)	QN_01:52:8F	Mark	2*2	Demo1	2.4 GHz	b/g/n	-38 dBm	60 dB	798.79 KB	15.32 MB	-	02:21:55	Idle	1 (40 MHz)	-
6		192.168.7.66 (DHCP)	QN_01:52:8F	John	2*2	demo1	5 GHz	n/ac	-42 dBm	56 dB	2.62 MB	10.07 MB	86 Mbps	01:44:22	Active	144 (20 MHz)	-
7		192.168.7.98 (DHCP)	QN_01:52:8F	Brick	1*1	Check_QC	b/g/n	-39 dBm	59 dB	3.90 MB	29.76 MB	65 Mbps	00:38:09	Active	1 (20 MHz)	-	V2
8		192.168.7.115 (DHCP)	QN_01:52:8F	QC_test	ZenO 10th Floor	wentest1	70 dB	2.09 MB	7.17 MB	-	00:28:16	Active	1 (40 MHz)	-	-	-	
9		192.168.7.131 (DHCP)	QN_01:52:8F	Tester	2*2	Demo_qc1	2.4 GHz	b/g/n	-37 dBm	61 dB	22.30 KB	10.04 KB	300 Mbps	00:13:08	Idle	1 (40 MHz)	-
10		192.168.7.31 (DHCP)	QN_01:52:8F	N/A	-	qc_web	5 GHz	n/ac	-54 dBm	44 dB	-	-	-	5 S	Active	144 (-)	-

Figure 30

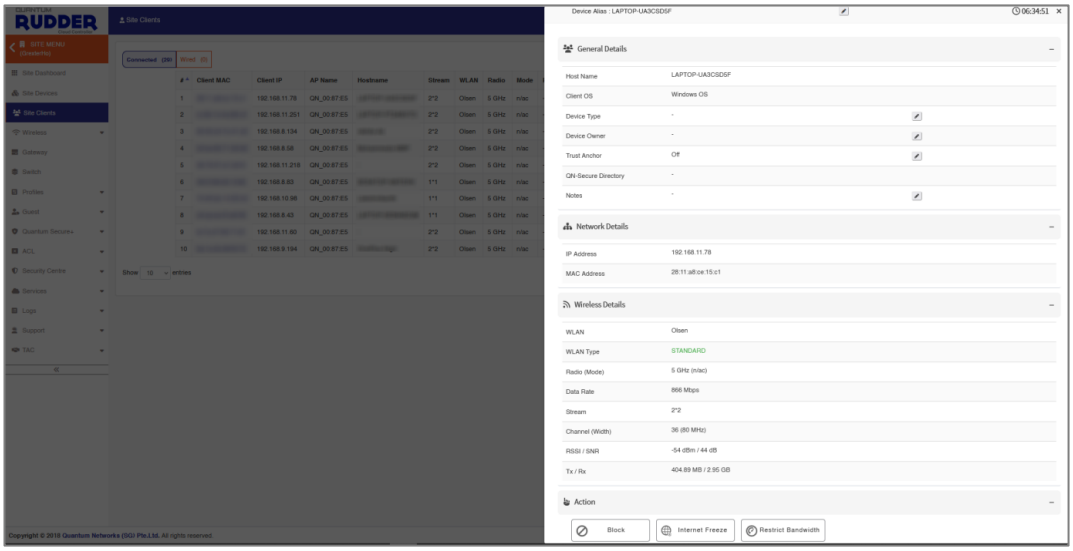


Figure 31

Note: By clicking "Client MAC," the administrator can block a client, freeze internet access, or restrict bandwidth using the Action option.

Figure 31.1

Action - Block Client

The Administrator can block the client by enabling the toggle button for the WLAN.
Follow these steps to block a client:

- Go to the **Actions** drop-down list.
- Select the network the client wants to block by clicking **"Block."**
- Click **"Submit."**

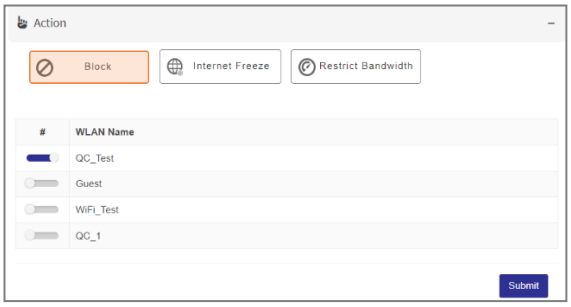


Figure 31.2

The blocked clients can be unblocked from device policy by disabling the toggle button. (Add same unblocking process for B/w restrict and internet freeze))
Go to Device Policy and ensure the client is blocked.

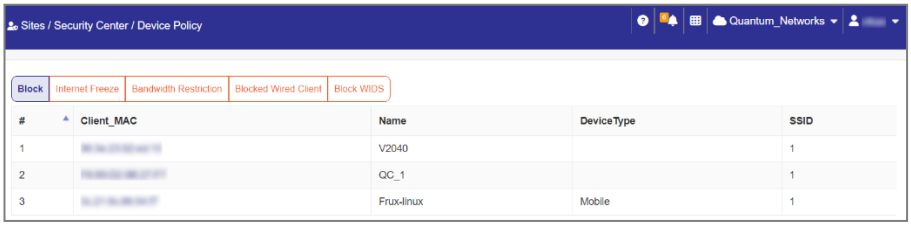


Figure 31.3

Action – Internet Freeze

The freeze device Mac will be unable to access internet from any SSID till the duration configured in schedule profile.

Follow the below steps for Internet Freeze client.

- Go to the **Actions** drop-down list.
- Select the **Scheduling Profile** from the drop-down list.
- Click **Submit**.

Enable the SSID with toggle button and input the Bandwidth required to restrict for the client device.

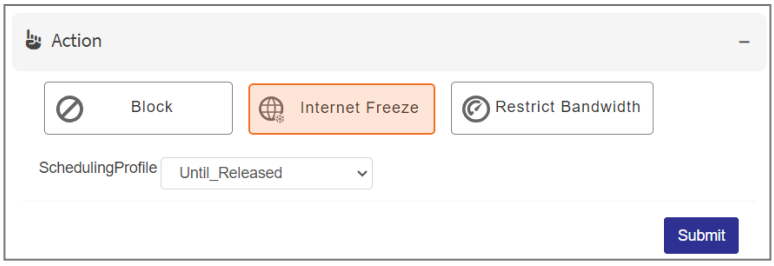


Figure 31.4

Go to the Device Policy and ensure that the client's internet freezes according to the scheduled profile. It is mandatory to configure scheduling before bind it with this feature.

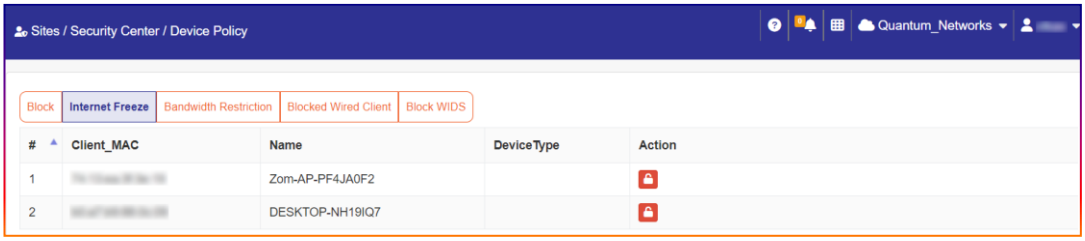


Figure 31.5

Action – Restrict Bandwidth

Follow the steps below to restrict bandwidth

- Go to the **Actions** drop-down list.
- Enable the SSID for the client that you want to restrict.
- Click **Submit**.

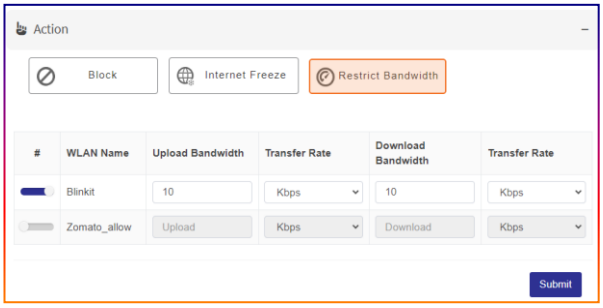


Figure 31.6

Wireless

The user can configure parameters required to manage and set up wireless devices with various options as per the requirements.

WLAN

With this section, the admin can configure wireless networks by creating a new SSID (WLAN), modifying an existing one if needed, and deleting it if unused.
To add a new Wireless Local Area Network (WLAN):
Go to **Cloud Menu > Site > Select Site > Configuration > Wireless > Add**

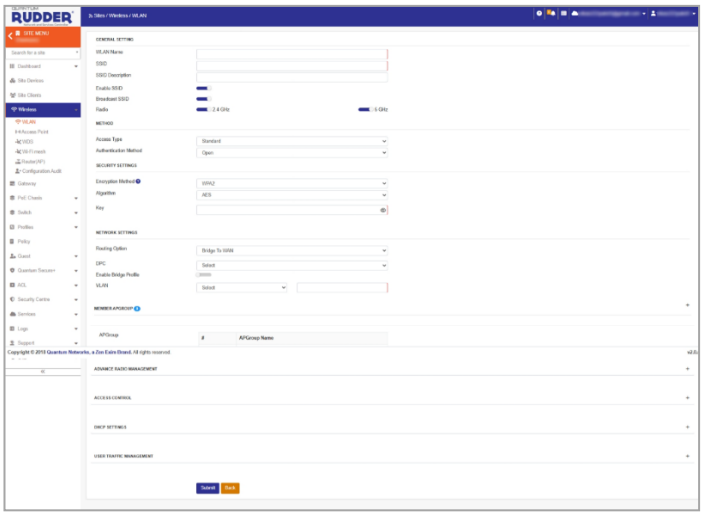
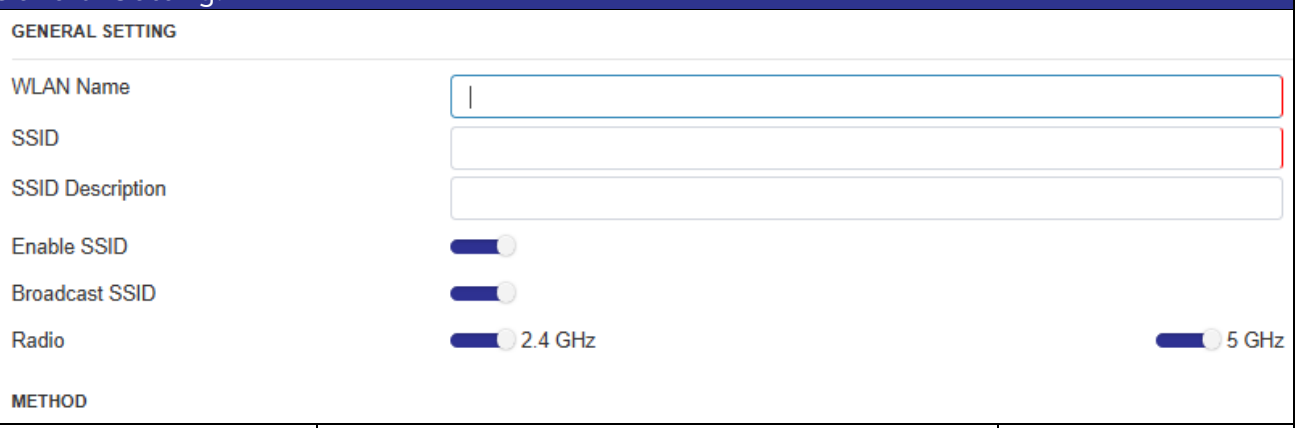


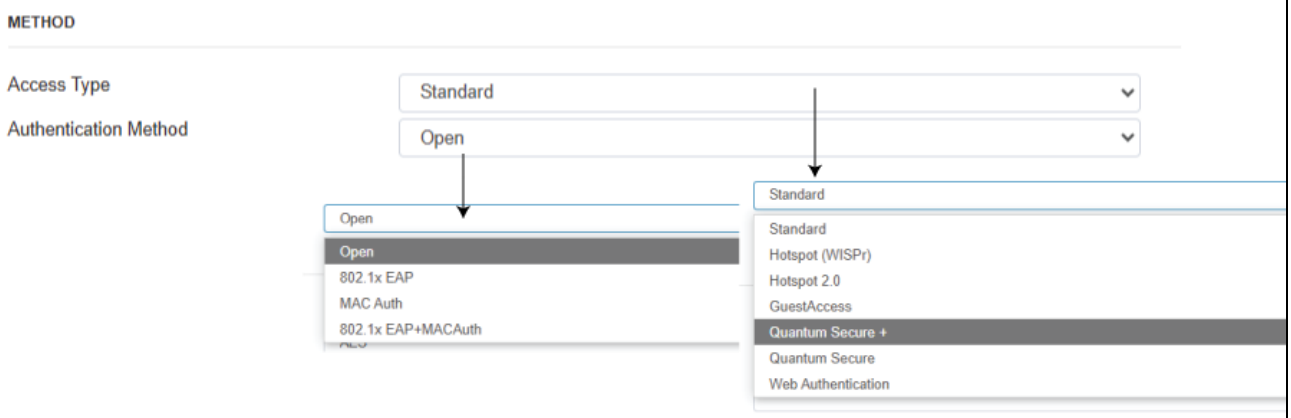
Figure 32

The individual sections under this parameter are described below:

Parameter	Description	Default Value
General Setting:		
		
WLAN Name	This Wireless LAN name is unique for management purposes only and is not visible to wireless clients.	None
SSID	The SSID name is visible to wireless clients (network). It can contain up to 32 alphanumeric characters and is case-sensitive.	None

SSID Description	Add an SSID description for admin reference.	None
Enable SSID	The broadcast of the SSID can be enabled or disabled using a toggle button.	Enabled
Broadcast SSID	If the broadcast is enabled using the toggle button, the SSID will be visible to users. If the broadcast is disabled using the toggle button, the SSID will be hidden and invisible to users. However, users can still connect to the SSID by manually configuring it on their client devices.	Enabled
Radio	Enable the required radio channels (2.4 GHz and 5 GHz).	Enabled

Method:
Select the required access type and the related authentication method.

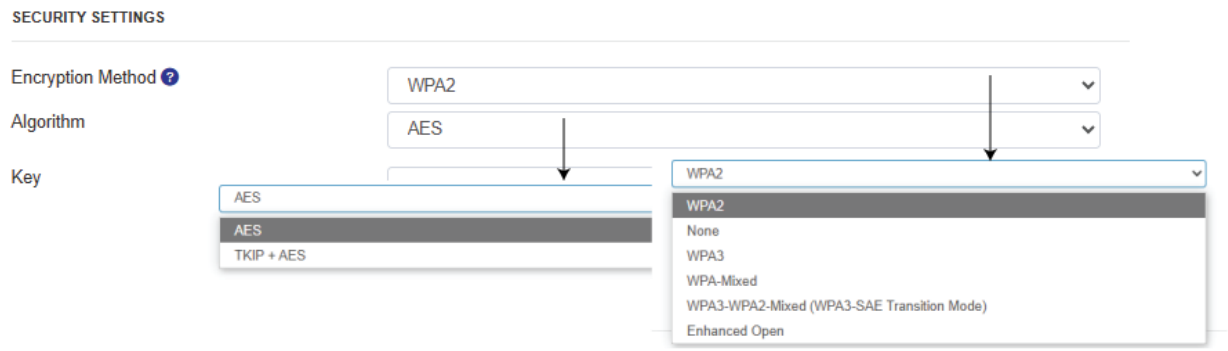


Access Type	Authentication Method	Description
Standard	Open, 802.1x EAP, MAC Auth, 802.1x EAP + MAC Auth	Standard Network Access is ideal for corporate and educational environments, offering seamless and secure authentication using WPA2/WPA3-Enterprise, 802.1X, RADIUS, or PSK, and can also be open without authentication.
Hotspot (WISPr)	Open	Hotspot (WISPr) Network Access is ideal for public Wi-Fi, using WISPr for external authentication via captive portals and third-party platforms, redirecting users to a login portal (e.g., social
	Authentication Profile: Select an Authentication Profile from the dropdown list to associate with this Wireless Local Area Network.	
	Hotspot Profile: Select the Hotspot Profile from the	

	dropdown list to associate it with this Wireless Local Area Network.	media, vouchers, or paid access), making it suitable for hospitality, retail, cafes, and public Wi-Fi deployments.
Guest access	Open	Guest Access Network provides temporary or limited-access Wi-Fi using a captive portal with access codes, vouchers, or sponsor approval, ideal for hotels, events, and enterprise guest networks, while a NAS device can assist in guest authentication by storing credentials, logs, and policies, integrating with RADIUS servers or captive portals.
	Splash Portal Profile: Select the Splash Profile from the dropdown list to associate it with this Wireless Local Area Network.	
	Guest Policy Profile: Select the Guest Policy Profile from the dropdown list to associate it with this Wireless Local Area Network	
	NAS Option: The NAS option allows the access point to connect to a NAS device.	
Quantum Secure+	Captive Portal Or QNPSK	Quick to deploy and use, it provides a unique passkey for each user, authenticated by the QIM authentication server.
	Quantum Secure+ Policy: Select the Quantum Secure+ Policy Profile from the dropdown list to associate it with this Wireless Local Area Network.	
	Splash Portal Select the Splash Portal Profile from the dropdown list to associate it with this Wireless Local Area Network.	
	User Group: Select the User Group from the dropdown list that is to be associated with this Wireless Local Area Network (Hold the Ctrl key to select multiple groups).	
Quantum Secure	Open	Quick to deploy and use, it provides a unique passkey for each user which is authenticated by access point.
	Quantum Secure+ Policy: Select the Quantum Secure Policy from the dropdown list to associate it with this Wireless Local Area Network.	
	User Group: Select the User Group from the dropdown list to	

	associate it with this Wireless Local Area Network. Hold the Ctrl key to select multiple groups.	
Web Authentication	Open	Web Authentication provides an option for Guest Access with an External Directory by integrating a captive portal with an external authentication system, such as Active Directory (AD), LDAP, RADIUS, or cloud-based identity providers. This allows guests to log in using credentials stored in an external directory.
	Authentication Profile: Select an Authentication Profile from the dropdown list to associate with this Wireless Local Area Network.	
	Splash Portal Profile: Select the Splash Portal Profile from the dropdown list to associate it with this Wireless Local Area Network.	

Security Settings



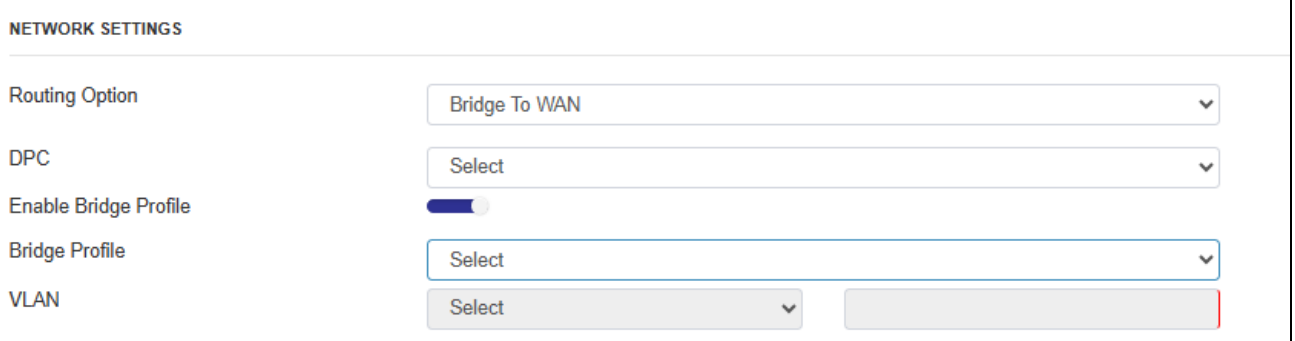
Parameter	Description	Default Value
Encryption Method	Choose an encryption method: WPA2, None, WPA-Mixed, WPA3-WPA2-Mixed (WPA3-SAE Transition Mode), Enhanced Open, WPA, WEP-64, or WEP-128.	WPA2
Algorithm	For the encryption method, WPA2 uses the AES algorithm, while WPA-Mixed uses the TKIP+AES algorithm.	AES
Key	Passphrase (password) of user choice.	None

Encryption Methods	Detail Description
WPA2	**WPA2 (Wi-Fi Protected Access 2)** is a security system for Wi-Fi networks. It replaces WPA and follows the IEEE 802.11i standard. WPA2 uses **AES encryption** to keep data safe and **CCMP** to ensure data integrity. It offers better security than WPA and is commonly used in modern

Note: Before configuring the **Access Type** and **Authentication Method**, you need to set up the related Hotspot, Authentication, Guest, and Splash Portal profiles as per the requirements.

WPA-Mixed	**WPA-Mixed** is a Wi-Fi security mode that supports both old and new devices. It allows older devices to connect using **WPA (TKIP)** while newer ones use **WPA2 (AES)**. This ensures compatibility but can weaken security since WPA is less secure. For better protection, **WPA2-Only** or **WPA3** is recommended.
WPA3-WPA2-Mixed	**WPA3-WPA2 Mixed** Mode allows both old and new devices to connect to the same Wi-Fi network. Newer devices use **WPA3** for better security, while older ones connect with WPA2. This helps upgrade security without disconnecting older devices. However, connections using **WPA2** won't get WPA3's advanced protection.
Algorithm	Detail Description
AES	**AES (Advanced Encryption Standard)** is a method used to protect digital data. It encrypts information using a fixed block size of 128 bits and supports keys of 128, 192, or 256 bits for security. AES is widely used in online security, such as protecting **Wi-Fi (WPA2/WPA3), VPNs,** and **websites.**
TKIP+AES	**TKIP**: An older encryption protocol used in WPA (Wi-Fi Protected Access). It enhances WEP security with per-packet key mixing, message integrity checks, and rekeying. **AES:** A more advanced encryption standard used in WPA2/WPA3, offering stronger security with block cipher encryption.

Network Setting



Parameter	Description	Default Value
Routing Option	Use this option to select the routing mode of AP such as 'Bridge to WAN' or 'NAT to WAN.' By default, it is set to 'Bridge to WAN.' 'NAT to WAN' can be configured if AP is functioning as router mode. To configure AP to router mode, go to **Site menu > Wireless > Router AP** and enable the mode by toggle button and selecting AP from drop down menu.	Bridge to WAN
Enable Bridge Profile	Bridge profile can be enabled or disabled by toggle button.	Disable

Bridge Profile	Select the required bridge profile from the drop-down list	
VLAN	Each wireless interface (SSID) can be configured with a specific VLAN ID (1-4094). If required, enter a valid VLAN ID (1-4094) to assign the network to clients on this WLAN. The default VLAN is always VLAN 1.	VLAN 1
Member AP Group		
Ap Group	All created AP groups will be listed here. The user can select the required group for each WLAN profile.	

Advance Radio Management:
With this option enable the required Wi-Fi roaming standards, beacon elements, radio control, and wireless security parameters

Parameter	Description	Default Value
Roaming		
802.11r	**802.11r** (Fast Roaming) reduces the authentication time of a client device roaming between access points, improving VoIP and video calls while minimizing connection drops.	Enable
802.11k	**802.11k** improves Wi-Fi roaming by reducing scanning time and helping devices quickly find the best access point for better performance.	Enable
802.11v	**802.11v** improves Wi-Fi by guiding devices to the best AP, reducing congestion, enhancing roaming, and optimizing battery life.	Enable
Beacon Elements		
802.11d	**802.11d** enables Wi-Fi devices to adapt to country-specific regulations for seamless global connectivity.	Disable
DTIM Interval	**DTIM Interval** controls how often it delivers buffered multicast and broadcast data to power-saving client devices, balancing battery life and network efficiency.	Disable
U-APSD	**U-APSD (Unscheduled Automatic Power Save Delivery)** reduces power consumption for Wi-Fi devices by allowing them to sleep longer and wake up only when needed, improving battery life and network efficiency.	Disable
Inactivity Timeout	**Inactivity Timeout** disconnects idle clients after a set period, freeing up resources and improving network efficiency.	None

Radio Control		
OFDM Only (Disables 802.11b)	Enabling **OFDM** blocks 802.11b legacy devices to maintain wireless network efficiency.	Enable
BSS Min Rate	**BSS Min Rate** sets the lowest data rate for client connections, improving efficiency by forcing devices to use faster rates and reducing airtime usage.	Default
Mgmt Tx Rate	**Mgmt Tx Rate** sets the transmission rate for management frames (beacons etc.), impacting network efficiency and connectivity stability.	6 mbps
Disable Band Balancing	**Disable Band Balancing** allows devices to connect freely to either 2.4 GHz or 5 GHz without the AP steering them to a specific band.	Enable
Max Clients	**Max Clients** limits the number of devices that can connect to each radio of an access point, preventing overload and ensuring stable performance.	150/Radio
RTS/CTS Threshold	The **RTS/CTS threshold** controls RTS/CTS by initiating an RTS/CTS exchange for data frames larger than the threshold and sending (without RTS/CTS) any data frames smaller than the threshold. The RTS/CTS packet size threshold ranges from 0 to 2347 octets.	Disable
Wireless Security		
802.11w MFP	**802.11w Management Frame Protection (MFP)** This standard is also known as Management Frame Protection. Management Frame Protection increases security by providing data confidentiality for management frames.	Disable
Proxy ARP	**Proxy ARP** reduces broadcast traffic by responding to ARP requests on behalf of clients, improving network efficiency.	Disable
WLAN Priority	**WLAN Priority** prioritizes traffic for better performance in high-traffic networks.	Default
Access Control		
ACL		
Layer 2 ACL	**L2 ACL** controls network access by filtering traffic at Layer 2 based on MAC addresses.	Disable
Layer 3 ACL	**Layer 3 ACL** based on pre-defined access or deny rules at different levels, such as source and destination IP addresses, ports, and protocols.	Disable
Session Control ACL	**Session Control ACL** restricts concurrent sessions based on predefined rules at different levels, such as	Disable

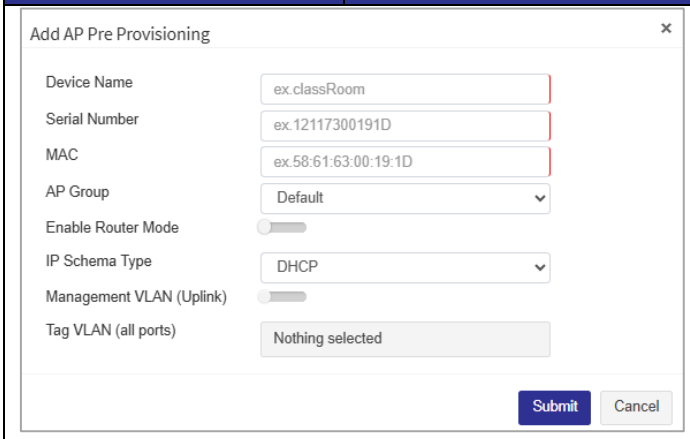
	source and destination IP addresses, ports, and protocols.	
Client Restrictions		
Scheduling Profile	**Scheduling Profile** automates Wi-Fi availability based on time rules, optimizing network usage and security.	Disable
Internet Freeze	**Internet Freeze** temporarily blocks internet access for selected devices, aiding control and management.	Disable
OS Policy	**OS Policy** enforces network rules based on a device's OS for better security and performance.	Disable
Rate Limit	When enabled, it restricts the bandwidth of clients at different levels, such as port, OS, per client, and host, for optimum utilization of bandwidth across the network.	Disable
Isolation		
Client Isolation	**Client Isolation** enhances security by preventing connected devices from communicating with each other, reducing risks like data interception and malware spread.	Disable
DHCP Settings		
Force DHCP	**Force DHCP** ensures clients obtain IP addresses via DHCP, preventing static IP use and enhancing network security and management.	Disable
DHCP Option 60	**DHCP Option 60** allows an access point to identify itself to the DHCP server using a vendor-specific string for optimized network configuration.	Disable
DHCP Option 82	**DHCP Option 82** enables access points to insert location and client information into DHCP requests, helping with network security, tracking, and IP address management.	Disable
User Traffic Management		
Traffic Shaping		
QoS	**QoS (Quality of Service)** prioritizes network traffic on an access point, ensuring better performance for critical applications like VoIP, video streaming, and gaming.	Disable
WMM	**WMM (Wi-Fi Multimedia)** prioritizes wireless traffic to improve the performance of voice, video, and real-time applications.	Disable
Wi-Fi Calling	**Wi-Fi Calling** allows voice calls over Wi-Fi by prioritizing call traffic, ensuring better call quality in low cellular coverage areas.	Disable

DiffServ	**DiffServ** prioritizes network traffic by classifying and managing data packets, ensuring better QoS for critical applications on the access point.	Disable
Traffic Monitoring		
URL Filtering	**URL Filtering** in an access point restricts access to specific websites, enhancing security and enforcing browsing policies.	Disable
App Policing	The **App policy** restricts or permits access to applications selected from the database based on different categories.	Disable
Multicast / Broadcast Support		
Multicast to Unicast	**Multicast to Unicast** improves reliability by converting multicast traffic into unicast for better performance.	Enable

Access Point

The administrator can manually add and configure an AP or import pre-provisioned APs using a CSV file, which can be downloaded as a sample using the "Sample File" option.

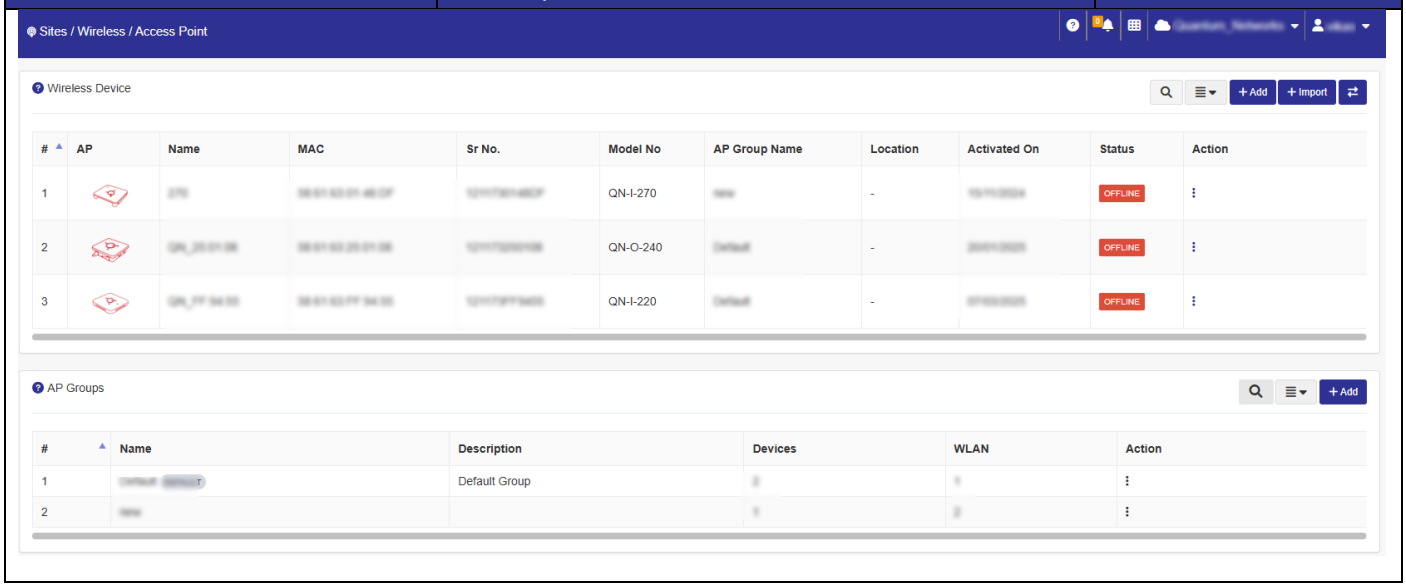
Wireless Device

Parameter	Description	Default Value
 Add AP Manually	 Import multiple AP detail (csv)file for Pre-Provisioning.	
Add AP manually > Go to Access Point > click on" ADD"		
Device Name	Add Device Name as per your choice.	None
Serial Number	Add device serial number.	None
MAC	Add device MAC address.	None
AP Group	Initially, the AP will bind to the default group, and the user can later transfer it to another AP group as needed. If AP groups are preconfigured, they will appear in the dropdown for selection.	Default
Enable Router Mode	The Enable Router Mode option in a wireless access point allows the AP to function as a router, managing network traffic between the LAN and WAN.	Disable
IP Schema Type	The IP Schema Type in access points defines how the AP obtains and manages its IP address within the network. **Static IP –** The AP is manually assigned a fixed IP address, ensuring stability and easier management. **Dynamic (DHCP) –** The AP obtains an IP address automatically from a DHCP server, simplifying deployment but subject to change.	DHCP
Management VLAN (Uplink)	The **Management VLAN (Uplink)** is a dedicated VLAN used for managing and monitoring the access point remotely.	Disable

Tag VLAN (all ports)	In **Tagged VLAN**, additional information is added to Ethernet frames to identify their belonging.	None
Add multiple AP's > Go to Access Point > click on" import"		
+ Import	Click on" import"- Download the sample file and add the Multiple AP's details in downloaded csv file and import it.	

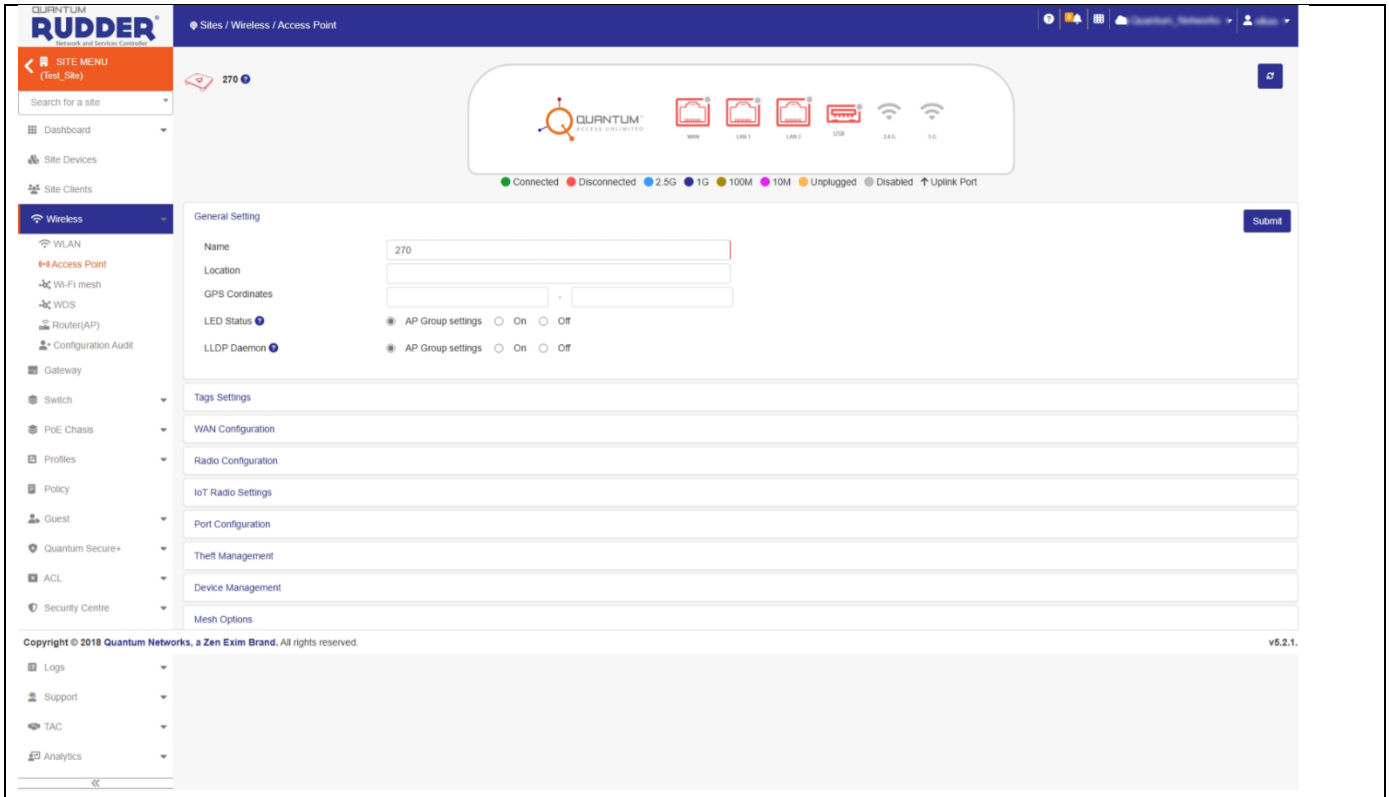
After being onboarded manually or through cloud configuration, the device will be listed under the **Wireless Devices** tab. The admin can view all devices here. To configure a specific Access Point (AP), click on its device icon. This will redirect to the individual configuration page for that device.

Parameter	Description	Default Value



On clicking the device icon, the following screen appears.

Parameter	Description	Default Value



General Setting

General Setting

Name 270

Location

GPS Cordinates ,

LED Status AP Group settings On Off

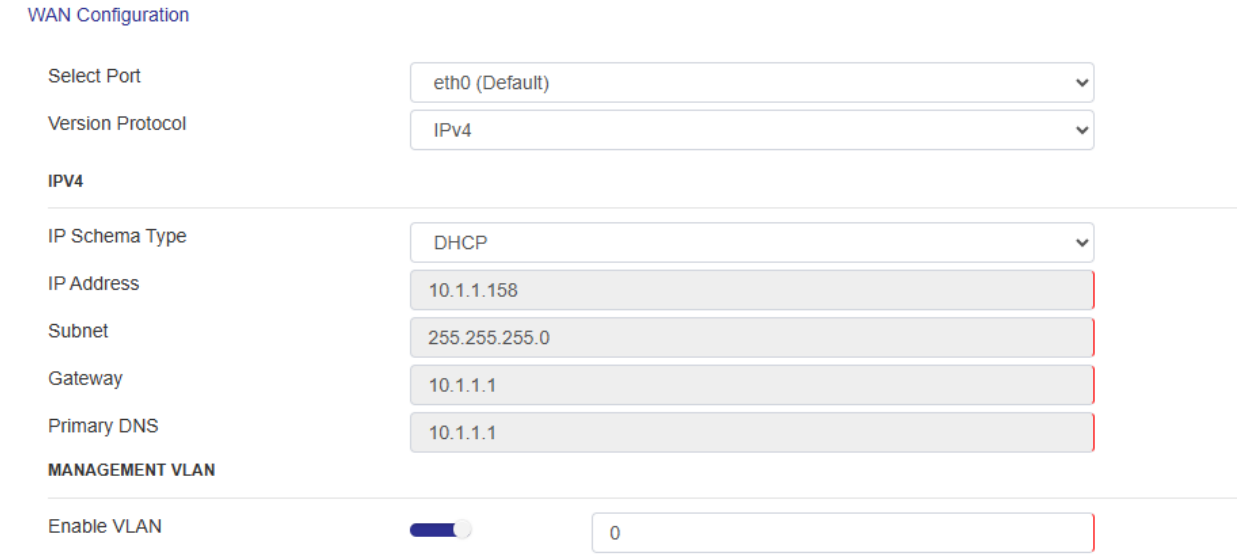
LLDP Daemon AP Group settings On Off

Name	Define AP group name.	None
Location	Add description for reference.	None
GPS Coordinates	Select regulatory country.	None
LED Status	Administrators can disable LED lights on QN Access Points to avoid drawing attention in public areas or indoor environments like hotel rooms and conference rooms. By default, LEDs are enabled.0	
LLDP Daemon	The AP transmits LLDP packets to advertise its presence and capabilities to directly connected neighbors. Advertised parameters include: System Name, Port ID, Device ID, Capabilities, and Time to Live (TTL).	

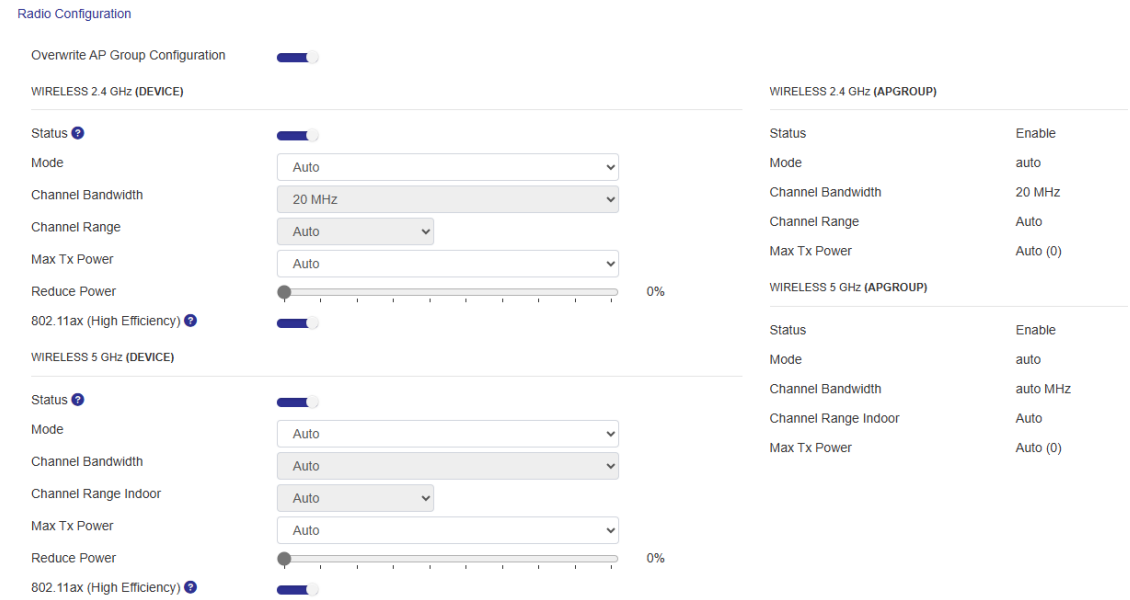
Tags Settings

TagOne

TagOne	TagOne in Access Point wireless settings refer to a VLAN ID used to tag SSID traffic for separate handling by network switches and routers.



Select Port	Select the Ethernet port that needs to be configured as WAN.
Version Protocol	Select the protocol version: IPv4 or IPv4 + IPv6.
IPv4	Configure the listed details as per the selected protocol version.
IP Scheme Type	It can be DHCP or Static.
IP Address Subnet Gateway Primary DNS	DHCP: The AP automatically obtains an IP address, subnet mask, gateway, and DNS from the ISP or upstream router. Static: Manually enter the IP address, subnet mask, gateway, and DNS server information.
Management VLAN	
Enable VLAN	Enable and assign a VLAN number that will function as the management network.



Radio Configuration

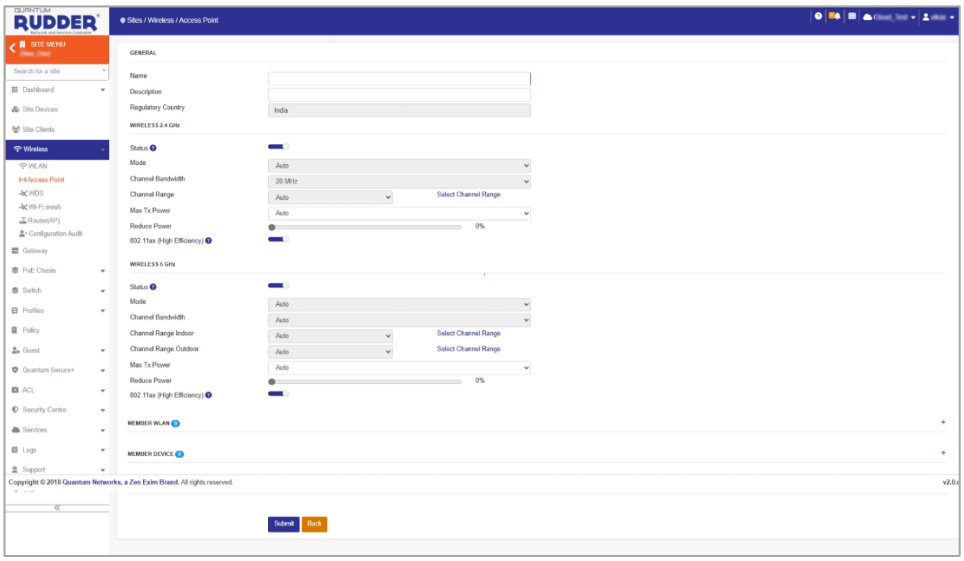
Overwrite AP Group Configuration: Enabling 'Override AP Group Configuration' will apply this AP's individual settings instead of the group configuration.	
WIRELESS 2.4 GHZ (DEVICE)	
Status	Enables or disables the radio (2.4 GHz band).
Mode	Sets the Wi-Fi standard (e.g., 802.11ax, ac, n). **802.11ax (High Efficiency)** is Wi-Fi 6, offering better speed, capacity, and efficiency.
Channel Bandwidth	Determines how wide the channel is (e.g., 20 MHz, 40 MHz, 80 MHz).
Channel Range	Specifies the range or specific channel number the AP uses for communication. Auto or manual selection helps avoid interference with nearby networks.
Max Tx Power	Set the maximum transmit power of the AP in dBm.
Reduce Power	Option to lower transmit power below the maximum, useful for reducing overlap or improving performance in dense deployments.
802.11ax (High Efficiency)	Enables Wi-Fi 6 features like OFDMA, BSS Coloring, and MU-MIMO. Improves performance in crowded environments with many clients.
WIRELESS 5 GHZ (DEVICE)	
Status	Enables or disables the radio (5 GHz band).
Mode	Sets the Wi-Fi standard (e.g., 802.11ax, ac, n). **802.11ax (High Efficiency)** is Wi-Fi 6, offering better speed, capacity, and efficiency.
Channel Bandwidth	Determines how wide the channel is (e.g., 20 MHz, 40 MHz, 80 MHz).
Channel Range	Specifies the range or specific channel number the AP uses for communication. Auto or manual selection helps avoid interference with nearby networks.
Max Tx Power	Set the maximum transmit power of the AP in dBm.
Reduce Power	Option to lower transmit power below the maximum, useful for reducing overlap or improving performance in dense deployments.
802.11ax (High Efficiency)	Enables Wi-Fi 6 features like OFDMA, BSS Coloring, and MU-MIMO. Improves performance in crowded environments with many clients.

IoT Radio Settings	
Scanning	
Scanning	Enabling **Scanning** under **IoT Radio Settings** allows the Access Point to actively detect nearby IoT devices over supported frequencies, typically 2.4 GHz.
Beaconing	
Advertising	Enabling "Advertising" will active listed below parameters.
UUID	Clicking on 'Generate UUID' will create a 128-bit identifier that distinguishes a specific beacon or group of beacons.
Major Assignment	**Major Assignment** is used to **group** a set of beacons under a common identifier—typically representing a larger area like a store, floor, or building.
Minor Assignment	**Minor Assignment** is used to **uniquely identify** individual beacons within that Major group—representing smaller locations or specific points.
Tx Power	**Tx Power** under **Beaconing** refers to the **transmit power level** at which the beacon signal is broadcast.
MQTT: Once BLE scanning is enabled, the system scans for nearby iBeacons and BLE sensor data, which can be forwarded to the configured MQTT broker via the MQTT-Telemetry Service.	
MQTT Telemetry Streaming On	Enabling "MQTT Telemetry Streaming" will active listed below parameters.
MQTT Broker	The MQTT broker address where the data will be published.
MQTT Topic	Assign the MQTT topic to which the data will be published.
MQTT QoS	Define Quality of Service level for message delivery: 0, 1, or 2.
Publish Frequency	Define Interval, in seconds. Users can define how frequently data is published to MQTT subscribers. Supported intervals include 1s, 2s, and 3s.
MAC address allow list	All Devices: BLE-enabled Quantum Access Points will scan for and collect data from all nearby BLE-enabled devices, such as iBeacons and sensors.

Port Configuration	
Port	Refers to the **physical Ethernet interface** on the access point
Action	**Enable/Disable** – Whether the port is active.
Type	**Select the port type.** **Access Port** – Carries traffic for a single VLAN (e.g., for end devices). **Trunk Port** – Carries multiple VLANs; usually used for uplink to switches or controllers.
Speed	Defines **port transmission speed.**
VLAN	Untag ID: Assign the **default VLAN ID assigned to untagged incoming traffic** on a port. Members: Refers to **which VLANs a particular port belongs to**. Auto Populated: Auto-populated from SSID and QPSK identity.
TACACS+	TACACS+ offering encryption of the entire payload (unlike RADIUS, which encrypts only passwords). Define the credentials used to authenticate a user via a TACACS+ server.
Theft Management	Theft Management is a security feature that detects, prevents, and responds to unauthorized removal or relocation of the AP.
Device Management	
Reboot Device	Click to reboot the access point immediately.
Schedule Reboot	Administrators can automatically reboot all their access points at a specified time to flush all cached memory and data stored in the AP.
Hard Reboot Button	When deploying APs in hostels and open public areas, it is possible that someone may misuse the APs. To prevent this, the admin can disable button functionalities, such as the reboot button, to ensure that no one disrupts the AP's functionality.
Hard Reset Button	When deploying APs in hostels or public areas, misuse is possible. Admins can disable button functions, like the reset button, to prevent disruption.
Mesh Options	
	
Once the Wi-Fi Mesh parameter is enabled under Site > Wireless > Wi-Fi Mesh, this option will appear in the section. By enabling Mesh Mode, the admin can choose and set the access point as either a Root AP or a Mesh AP.	

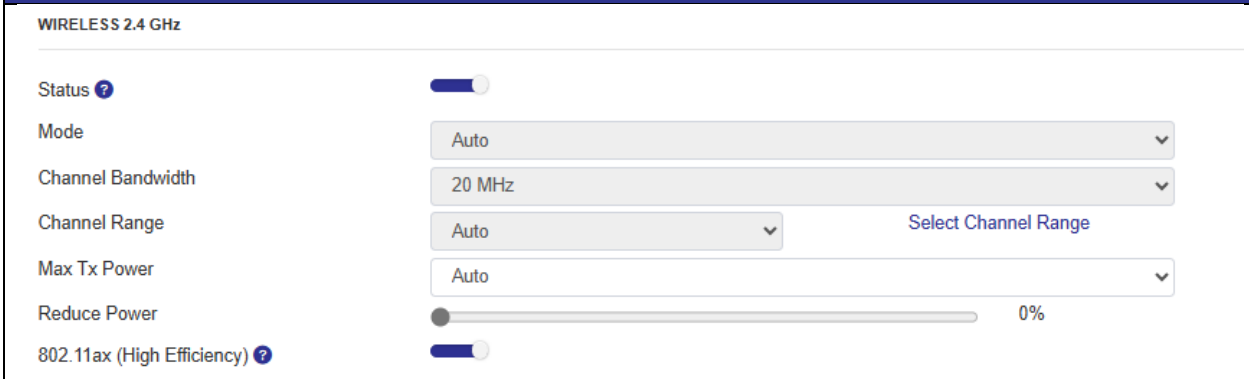
AP Groups

Create different AP groups as per the requirement.



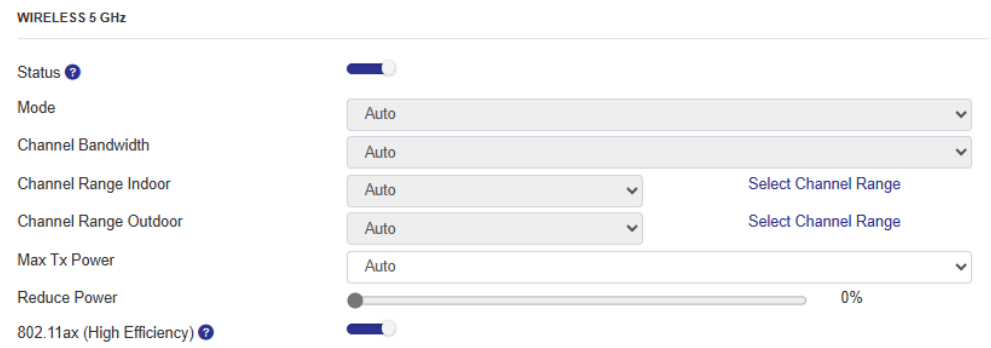
Parameter	Description	Default Value
GENERAL Name Description Regulatory Country India		
General		
Name	Define AP group name.	None
Description	Add description for reference.	None
Regulatory Country	Select regulatory country.	None

Wireless 2.4 GHz

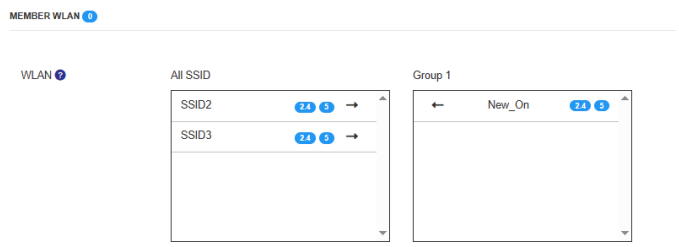


Status	Enable/Disable Radio channel as required.	Enable
Mode	Select Wi-Fi standards supported by access points, each offering varying speeds, frequencies, and efficiencies.	None
Channel Bandwidth	Select the range of frequencies used for data transmission. It determines network speed and capacity.	None
Channel Range	**Channel Range** refers to the set of available frequency channels that an AP can use for wireless communication. It helps reduce interference, optimize performance, and ensure stable connectivity.	None
Max Tx Power	It refers to the maximum transmission power output of the AP's radio signal. It determines signal strength, coverage area, and penetration through obstacles.	None
Reduce Power	**Reduce Power** in a wireless access point lowers transmission power to limit signal range, reduce interference, enhance security, and optimize performance. It allows for **precise control** over the transmission power, optimizing network performance.	None
802.11ax (High Efficiency)	An administrator can disable **802.11ax** mode on **Wi-Fi 6 access points** if certain legacy or IoT devices cannot detect or connect to **Wi-Fi 6 SSIDs**. Some older devices may not fully support or recognize the latest Wi-Fi 6 features, so disabling ax mode allows them to connect using older Wi-Fi standards like **802.11n or 802.11ac**.	Enable

Wireless 5 GHz



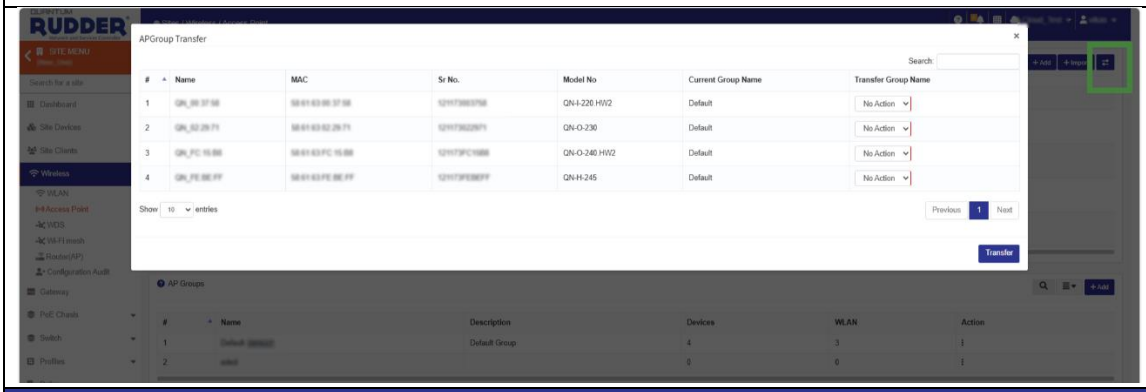
Status	Enable/Disable Radio channel as required.	Enable
Mode	Select Wi-Fi standards supported by access points, each offering varying speeds, frequencies, and efficiencies.	None
Channel Bandwidth	Select the range of frequencies used for data transmission. It determines network speed and capacity.	None
Channel Range Indoor	**Channel Range (Indoor)** defines available Wi-Fi channels based on frequency bands (2.4GHz, 5GHz, or 6GHz) and regional regulations, optimizing performance and minimizing interference.	None
Channel Range Outdoor	**Channel Range (Outdoor)** defines Wi-Fi channels optimized for outdoor use, ensuring better range, minimal interference, and regulatory compliance.	None
Max Tx Power	It refers to the maximum transmission power output of the AP's radio signal. It determines signal strength, coverage area, and penetration through obstacles.	None
Reduce Power	**Reduce Power** in a wireless access point lowers transmission power to limit signal range, reduce interference, enhance security, and optimize performance. It allows for **precise control** over the transmission power, optimizing network performance.	None
802.11ax (High Efficiency)	An administrator can disable **802.11ax** mode on **Wi-Fi 6 access points** if certain legacy or IoT devices cannot detect or connect to **Wi-Fi 6 SSIDs**. Some older devices may not fully support or recognize the latest Wi-Fi 6 features, so disabling ax mode allows them to connect using older Wi-Fi standards like **802.11n or 802.11ac**.	Enable
Note: Radio configuration can't change if Meshing is enabled in Site.		
Member WLAN		



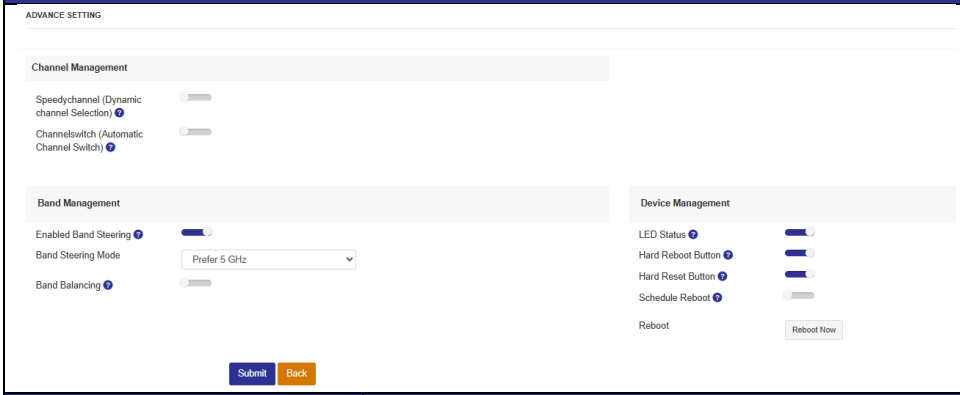
Move the required SSID from the list to the group that will share the same SSID, security settings, and network policies, ensuring seamless connectivity and communication within the WLAN.

Member Device

The access points in the same group will be listed here. The admin can select the access point group while adding it to a predefined AP group or move the access point to a specific group using the "AP Transfer" option, highlighted in green in the image below.



Advance Setting

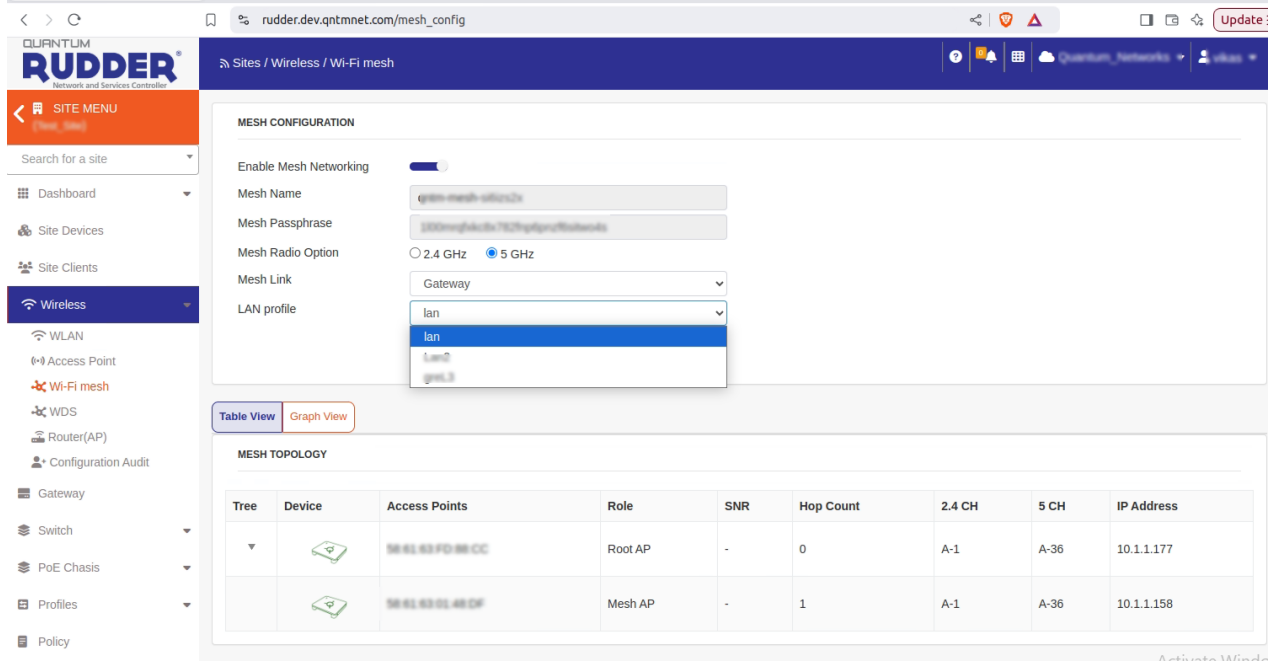


Channel Management		
Speedy channel (Dynamic channel Selection)	If enabled, the AP constantly scans the airtime (co-channel, adjacent, noise floor) and switches to the best channel if it detects any interference on the current channel.	Disable

	Caution: Devices that do not support 802.11h may frequently disconnect when the AP changes channels.	
Channel switch (Automatic Channel Switch)	If enabled, the AP scans the airtime at the configured interval and selects the best channel for optimal performance. Caution: Devices that do not support 802.11h may frequently disconnect when the AP changes channels.	Disable
Band Management		
Enabled Band Steering	**Band steering** in dual-band Wi-Fi directs capable devices to the less congested 5 GHz band for better performance. Quantum AP also supports post-association steering, moving 2.4 GHz clients to 5 GHz after connection. This ensures newer devices achieve peak speeds while older devices remain connected.	Enable
Band Steering Mode	It provides the option for band steering, whether it's required to move clients to 5 GHz aggressively or not.	Prefer 5 GHz
Band Balancing	It distributes clients between the 2.4 GHz and 5 GHz bands according to the configured ratio.	Enable
Device Management		
LED Status	Administrators can disable AP LED lights to avoid attention in public spaces or indoor environments. By default, LEDs are enabled on all QN APs.	Enable
Hard Reboot Button	In some locations like, hostels and public areas, admins can disable AP buttons like **Reboot** to prevent misuse and ensure uninterrupted operation.	Enable
Hard Reset Button	In some locations like, hostels and public areas, admins can disable AP buttons like **Reset** to prevent misuse and ensure uninterrupted operation.	Enable
Schedule Reboot	Administrators can schedule automatic AP reboots to clear cached memory and data.	Disable
Reboot	Click to Reboot Access Point.	

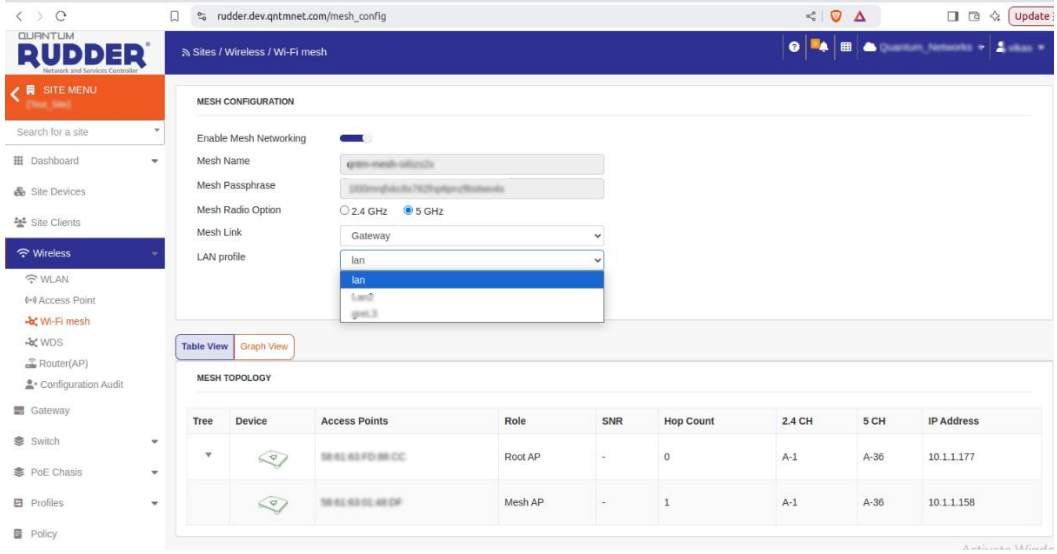
Wi-Fi Mesh

A Wi-Fi mesh network is a system of interconnected Wi-Fi devices, or nodes, where only the root device has a wired backbone, and the mesh devices work together over a wireless medium to create a seamless Wi-Fi network.

Parameter	Description	Default Value
		
Mesh Configuration		
Enable Mesh Networking	Enable the Mesh Networking feature based on requirements.	Disable
Mesh Name	Once the mesh network is enabled, the system automatically creates a mesh network name and passphrase, ensuring secure, seamless, and identifiable connectivity between mesh nodes.	None
Mesh Passphrase		
Mesh Radio Option	The selected radio serves as the backhaul for secure and stable communication between mesh nodes.	None
Mesh Link	Select required mode. **Bridge Mode:** This mode creates a bridge with the existing network without creating a separate subnet, as the mesh devices will be on the same network as the existing router. **Gateway Mode:** In this mode, the root device creates a separate network, and mesh devices connect to that network.	None
LAN Profile	Select a predefined LAN Profile from the dropdown. It defines the wired network settings for mesh nodes (Access Points) connected via Ethernet, helping	

	them integrate into the LAN and communicate with each other.	

Note: After submitting the above detail, go to Access Points > click on the image of the specific wireless device listed there to open the Wi-Fi Mesh options and configure the device as either a 'Root AP' or a 'Mesh AP'.

Table View

After defining the Access Point Role under **Access Points > Wireless Device** for a particular device, it will be reflected in the table view along with its defined role and other required details.
Graph View
The same details shown in the table view will also be displayed as a graph under this option.

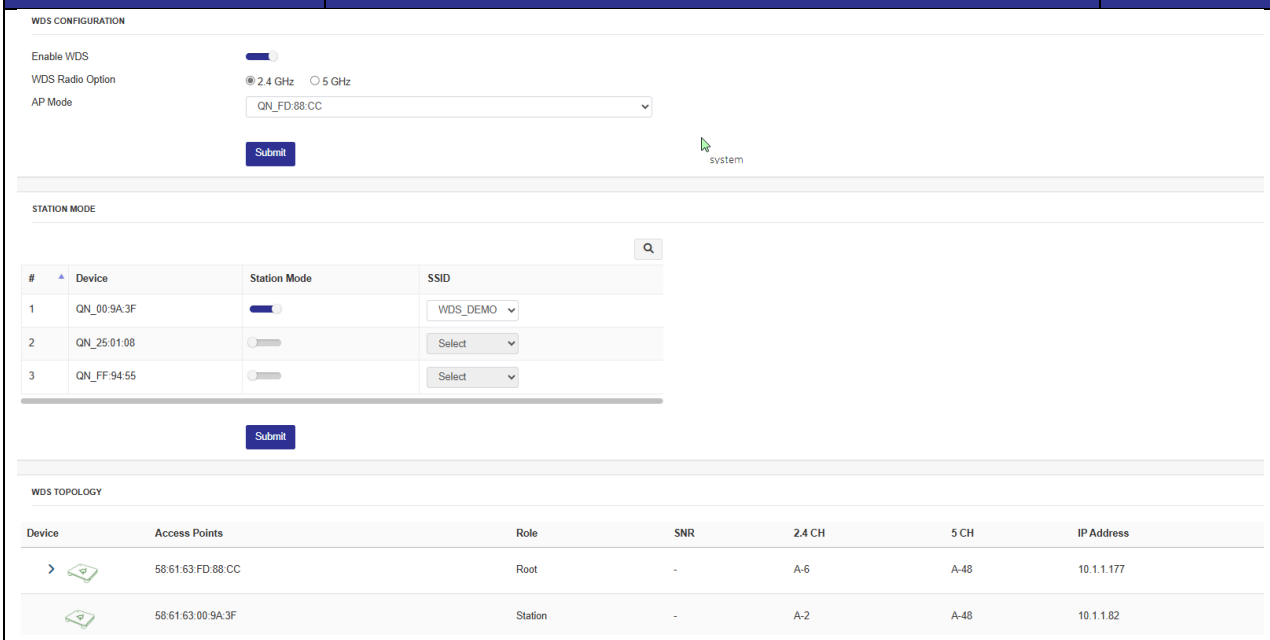
Knowledgebase:

Difference Between WDS and Mesh in an Access Point

Feature	WDS (Wireless Distribution System)	Mesh Networking
Connectivity	Uses a predefined static connection between APs.	Forms a dynamic, self-healing network between APs.
Configuration	Requires manual configuration of APs and links.	Automatically discovers and optimizes connections.
Scalability	Limited scalability, as each AP must be manually linked.	Highly scalable, with APs dynamically adding new nodes.
Performance	Can reduce throughput due to multiple retransmissions.	Optimized routing minimizes performance loss.
Fault Tolerance	If a WDS link fails, manual reconfiguration is needed.	If a node fails, traffic is rerouted automatically.

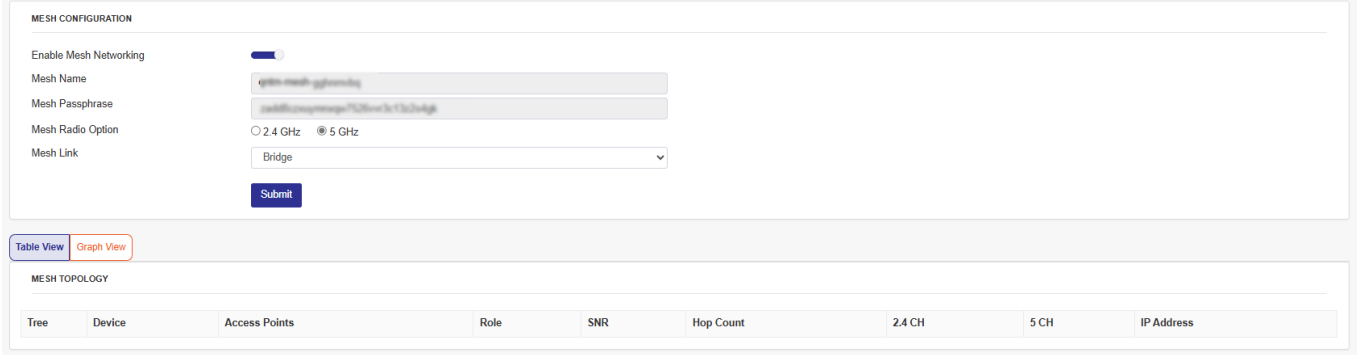
WDS

The Wireless Distribution System (WDS) feature in a wireless access point is used to extend the range of a wireless network by enabling access points to communicate with each other wirelessly without requiring a wired backbone.

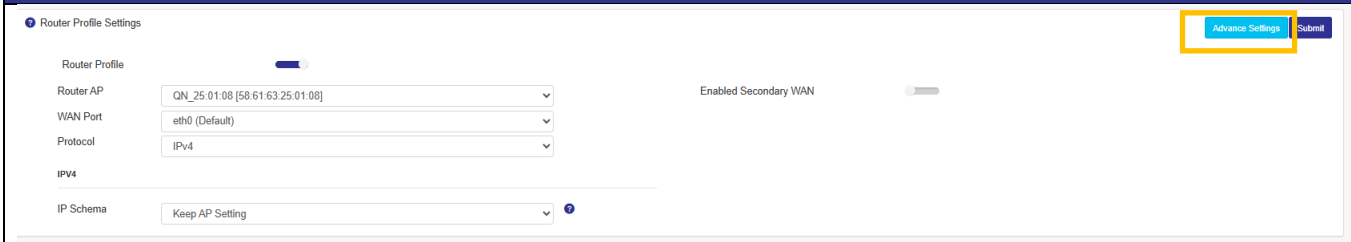
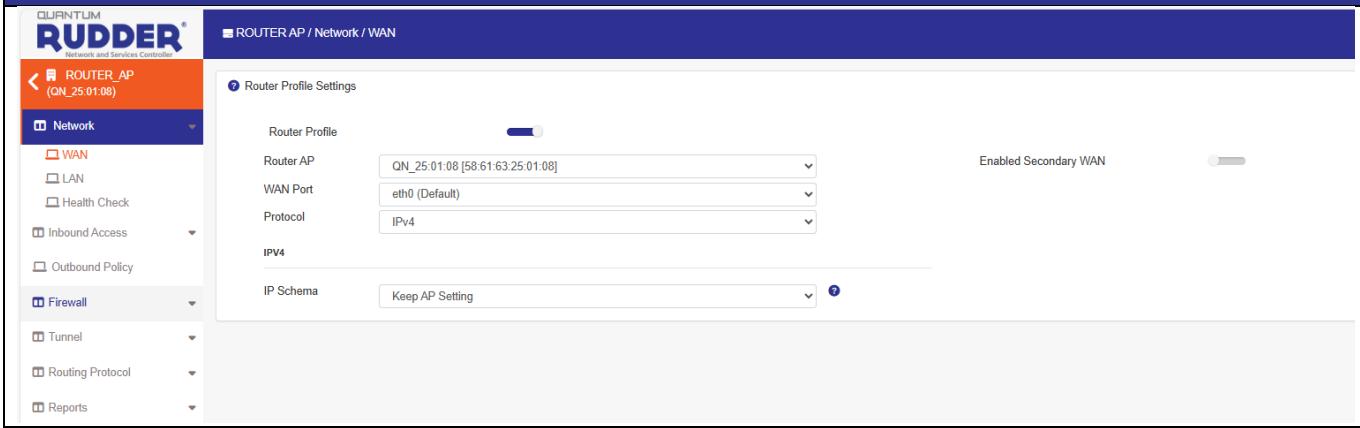
Parameter	Description	Default Value
		
WDS Configuration		
Enable WDS	Enable the WDS feature based on requirements.	Disable
WDS Radio Option	Select the radio band (2.4 GHz or 5 GHz) for communication between the WDS root and station.	2.4 GHz / 5 GHz
AP Mode	Select the AP from the dropdown menu that needs to be configured as a root AP for the WDS feature.	None
Station Mode		
Device	All other APs, excluding the one configured as the Root AP, will be listed under this option.	
Station Mode	Enable the mode as per requirement.	Disable
SSID	Select the SSID to be broadcast by the respective access point. The selected SSID will be broadcast by this specific AP, and any changes made to the SSID will be communicated to the access point via the Root AP.	
WDS Topology		
This option displays Access Point defined role details.		

Router (AP)

Extends coverage, bridges wired to wireless, supports seamless roaming, enhances capacity, and ensures stable connectivity.

Parameter	Description	Default Value
		
Router Profile Settings		
Router Profile		Disable
Router AP	When this mode is enabled, the access point acts as a gateway for network devices to connect to the internet and manages them by assigning IP addresses and providing security features such as a firewall and NAT.	None
WAN Port	The selected physical port with a wired medium is used to establish a connection with the Wide Area Network.	None
Protocol	Admin need to choose the network protocol for the router AP, either IPv4 only or both IPv4 and IPv6 for dual-stack support.	None
IPv4		
IP Schema	Defines the IP addressing method for the router AP, including: **Static IP –** Manually assign an IP address, subnet mask, gateway, and DNS. Suitable for networks requiring fixed addressing for stability and control. **DHCP–** The router AP automatically obtains an IP address, subnet, gateway, and DNS from the main router or DHCP server, simplifying network setup. **PPPoE** (Point-to-Point Protocol over Ethernet) – Requires a username and password provided by the ISP for authentication.	

Other		
VLAN	Untag VLAN on port.	Disable
Health Check	This feature is used to configure outbound policies for traffic load balancing.	
Dynamic DNS	Domain names convert network IP addresses into human-readable names for easier recognition. Dynamic DNS automatically updates DNS records when an IP address changes, enabling efficient and easy management.	
Enabled Secondary WAN		Disable
WAN Port	Select the port that needs to be configured to receive internet as secondary server.	
IP Schema	Defines the IP addressing method for the router AP secondary server.	Keep AP Setting (It will use the same method chosen by the admin for the primary server.)

Router AP – Advance Setting

On clicking the highlighted option "Advance setting" – it will redirect to below dashboard for further Advance configuration


Network		
WAN		

LAN		
Health Check		
Inbound Access		
Port Forwarding		
Outbound Access		
Firewall		
WAN Security		
NAT Forwarding		
Parental Control		
Tunnel		
IPsec		
VPN		
Routing Protocol		
RIP		
OSPF		
Reports		

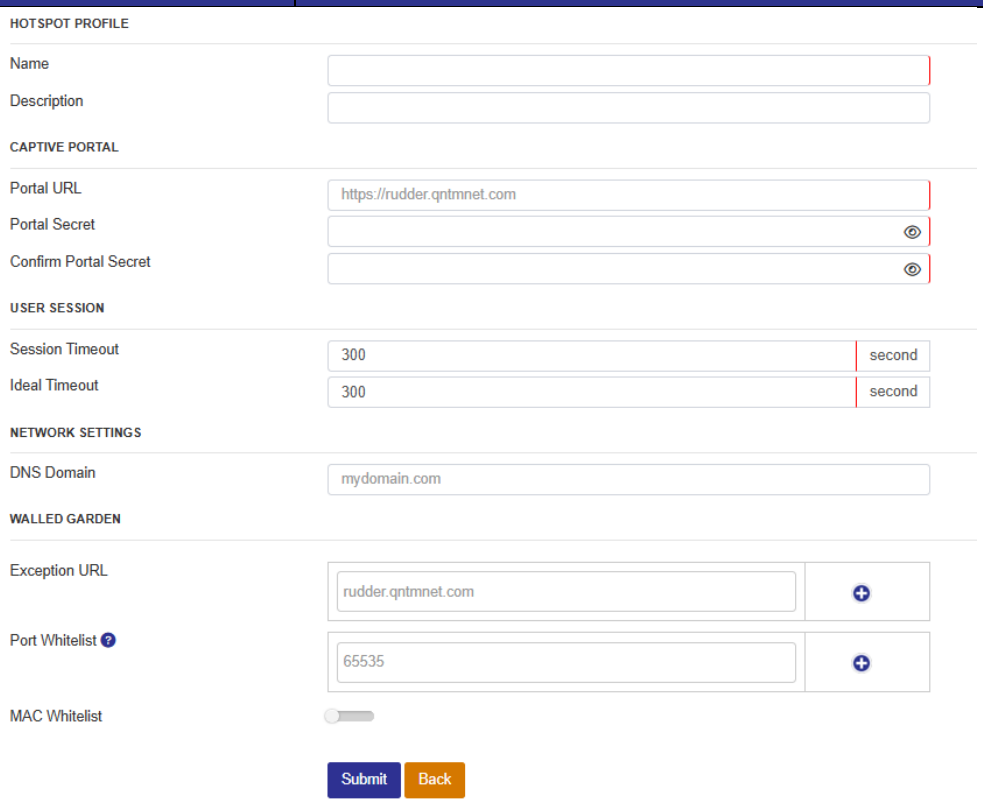
Configuration Audit

In Rudder, access point configurations can be applied at the group level and customized for specific devices using AP Group Override. If a Rudder-managed device fails to receive a configuration update, it will be marked as "Configuration Not in Sync."

Profiles

Profile is a network configuration that defines authentication, QoS, bandwidth control, and access policies for seamless and secure Wi-Fi connectivity. It includes Hotspot Authentication, Scheduling, DiffServ QoS, WMM, Bridge Mode, Hotspot 2.0, Wi-Fi Calling, Bandwidth Shaping, and Address/Host-based policies to optimize performance and user experience.

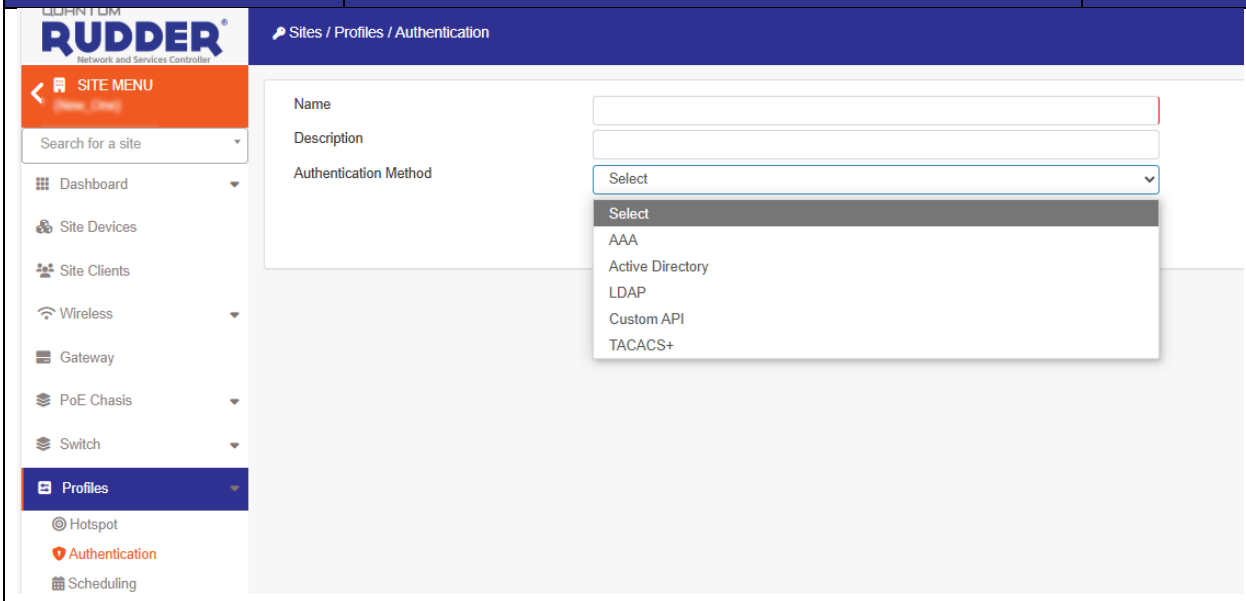
Hotspot

Parameter	Description	Default Value
		
Go to Cloud Menu > Site > Select Site > Profiles > Hotspot > Add		
Hotspot Profile		
Name	The **Hotspot Profile Name** is a unique identifier assigned to a hotspot setup.	
Description	In this field, admin can add a basic description about the hotspot for reference.	
Captive Portal		
Portal URL	Insert the Captive Portal (splash page) redirection URL, which will redirect the user to the login page.	
Portal Secret	A **Portal Secret** is a shared key or password used for secure communication between the captive portal and authentication servers (such as RADIUS). It will provide by QSMP team.	
Confirm Portal Secret	Re-enter the **Portal Secret.**	

User Session	
Session Timeout	**Session Time** refers to the duration a user is allowed to stay connected to a hotspot before requiring reauthentication. It defines how long a user's session remains active after successful login.
Ideal Timeout	Disconnects users after a period of inactivity.
Network Settings	
DNS Domain	**DNS** (Domain Name System) settings in a guest hotspot network ensure proper internet access, content filtering, and security.
Walled Garden	
Exception URL	Define the required **Exception URLs** that are accessible without authentication through the captive portal. These URLs are typically whitelisted to allow users to access essential services before logging in.
Port Whitelist	A **Port Whitelist** in a guest hotspot allows only certain network ports to stay open for essential services while blocking others to improve security. Allow traffic on specific ports before authentication.
MAC Whitelist	This feature allows only approved devices to connect using their MAC addresses, blocking all others. To configure MAC White List, Go to **Cloud Menu > Site > Select required site > ACL > Mac Whitelist**

Authentication

Parameter	Description	Default Value



Go to Cloud Menu > Site > Select Site > Profiles > Authentication > Add	
Name	Assign authentication profile name.
Description	Add description for reference.

Authentication method	Select the required authentication method from the dropdown list and define the respective fields that appear after selection.
As per the selected option, the required parameters will be displayed on the page for updating with the respective details.	
Authentication Method - AAA	
Authentication Server	
Server IP/URL	Assign authentication server IP - The authentication server IP or URL validates guest access by redirecting users to a login page for credentials, terms acceptance, or verification before internet access.
Secondary Server IP/URL	Assign a secondary authentication server IP address if needed. It serves as a backup if the primary server fails or becomes unreachable.
Authentication Port	Assign authentication port.
Shared Secret	Assign Shared Secret.
Confirm Shared Secret	Re-enter Shared Secret.
Accounting Server	
Server IP/URL	Assign accounting server IP - The authentication server IP or URL validates guest access by redirecting users to a login page for credentials, terms acceptance, or verification before internet access.
Secondary Server IP/URL	Assign a secondary authentication server IP address if needed. It serves as a backup if the primary server fails or becomes unreachable.
Accounting Port	Assign authentication port.
Shared Secret	Assign Shared Secret.
Confirm Shared Secret	Re-enter Shared Secret.
Location Information	
Location ID	Define a hotspot's physical location along with its geographical details.
Location Name	
Authentication Method – Active Directory	
Primary Server	
IP Address/URL	Assign the IP address of the Active Directory server used for authentication.
Port	Assign the communication port used for connecting to the AD server (typically 389 for LDAP or 636 for LDAPS).
Windows Domain Name	The domain name associated with the AD for user authentication.
AD Bridge	Enable the toggle button.
	Assign IP address of a service connects non-Windows systems to Active Directory for authentication and access control.

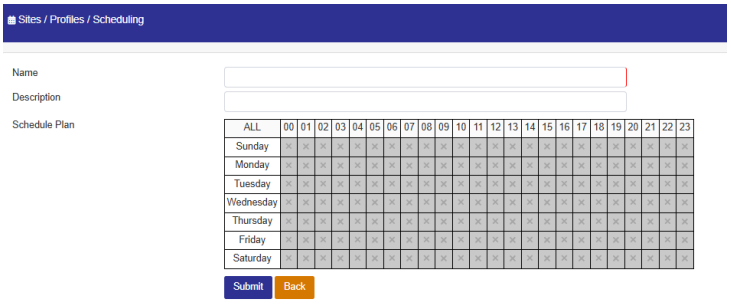
Authentication Method – LDAP	
Primary Server	
IP Address/URL	Assign the IP address or domain name of the LDAP server.
Port	Assign LDAP unencrypted LDAP.
Base Domain Name	Assign the base distinguished name (DN) for LDAP searches.
Admin Domain Name	Assign the base distinguished name (DN) for LDAP administrator.
Admin Password	Assign the password for the LDAP administrator.
Confirm Password	Re-enter the password.
Key Attribute	The LDAP attribute used for user identification
Search Filter	The filter to locate users in the directory.
Authentication Method – Custom API	
API Details	
API URL	Assign the web address (endpoint) where authentication requests are sent.
Method	Select HTTP method (e.g., POST, GET, PUT).
Header	Assign required headers.
Request Parameter Setup	
Query String	Parameters sent in the URL
Request Body	JSON or form data payload sent in the request.
Response Parameter Setup	
Content Type	**Select the Content Type** which defines the format of data sent and received in API requests and responses.
Authentication Method – TACAS+	
TACAS+ Details	
IP Address	Define the IP address of the TACACS+ server that handles authentication requests.
Port	Define the communication port used for TACACS+ authentication, typically 49 by default.
Auth Interval (Min)	Define the time interval (in minutes) after which re-authentication is attempted if required.
Shared Secret	Define the pre-shared key used for secure communication between the hotspot and the TACACS+ server to encrypt authentication messages.
Confirm Shared Secret	Re-entered the pre-shared key.

Scheduling

Go to **Cloud Menu > Site > Select Site > Profile > Scheduling > Add**

The Scheduling Profile used to automate the activation and deactivation of specific features—such as SSID broadcasting, client access, or bandwidth limits—based on predefined time and day settings.

Usage Example: An office WLAN for employees can be configured to provide wireless access only during office hours.

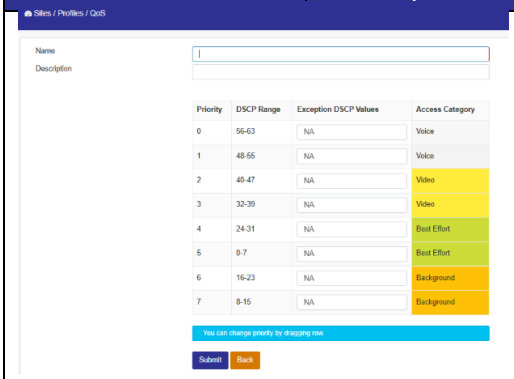
Parameter	Description
	
Name	Assign the **Profile Name.**
Description	In this field, admin can add a basic description about **Profile.**
Schedule Plan	Click on a **day of the week** to enable or disable the WLAN for the entire day. Colored cells indicate when the **WLAN** is enabled. Click and select specific time slots to customize **WLAN** availability throughout the day.

QoS

Quality of Service (QoS) refers to a network's ability to optimize performance by prioritizing specific types of traffic.

- **Differentiated Services Code Point (DSCP):** A packet header value used to classify and prioritize network traffic for high-priority or best-effort delivery.
- **Traffic Prioritization:** Assign higher priority to critical applications, ensuring optimal performance.

Go to **Cloud Menu > Site > Select Site > Profile > QoS > Add**

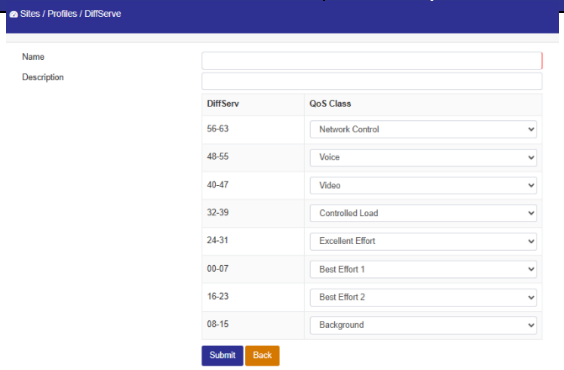
Parameter	Description
	
Name & Description	Assign the **Profile Name** and some basic description for reference.

To prioritize the access category, drag and reorder the rows accordingly.

DiffServe

It is a setting to prioritize Differentiated Services, where DiffServ is a network architecture designed to provide Quality of Service (QoS) by classifying and managing network traffic. It prioritizes packets based on their importance and assigns them to different traffic classes, ensuring that critical applications receive the necessary bandwidth and performance.

Go to **Cloud Menu > Site > Select Site > Profile > DiffServe > Add**

Parameter	Description
	
Name & Description	Assign the **Profile Name** and some basic description for reference.

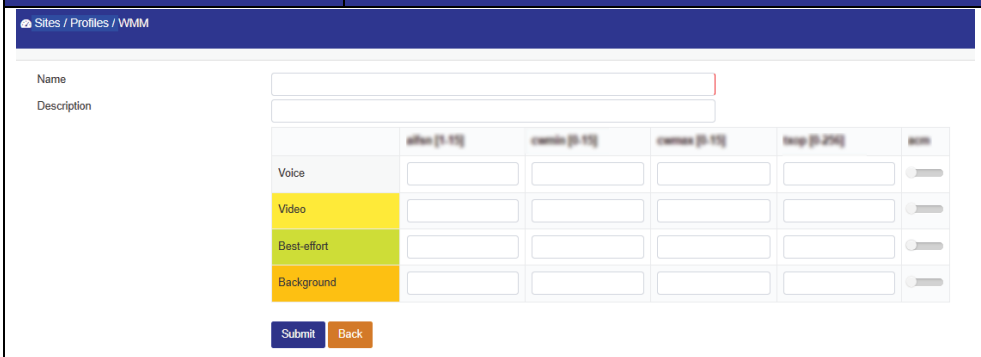
WMM

The Wi-Fi Multimedia (WMM) feature enhances Quality of Service (QoS) by prioritizing time-sensitive applications such as audio, video, and voice over less critical traffic. This feature applies only to wireless traffic.

- **Traffic Prioritization:** Ensures higher priority for real-time applications like video and voice.
- **Optimized Throughput:** Allocates network resources efficiently for better performance.
- **Reduced Latency:** Minimizes delays for time-sensitive applications.

- **Queue Management:** Places high-priority traffic in faster processing queues, ensuring smooth performance.

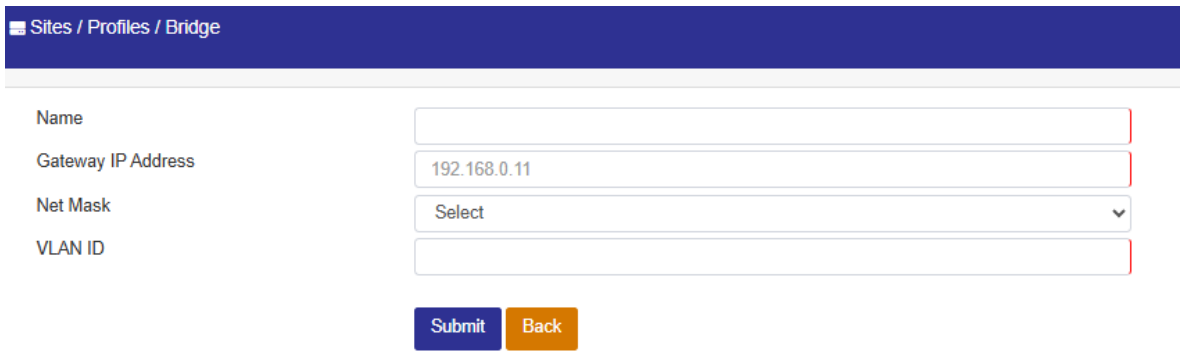
Go to **Cloud Menu > Site > Select Site > Profile > WMM> Add**

Parameter	Description
	
Name & Description	Assign the **Profile Name** and some basic description for reference.

Bridge

This profile will be used by the AP to gather information about the VLAN network, such as the VLAN gateway, which may be required by certain features to function properly.

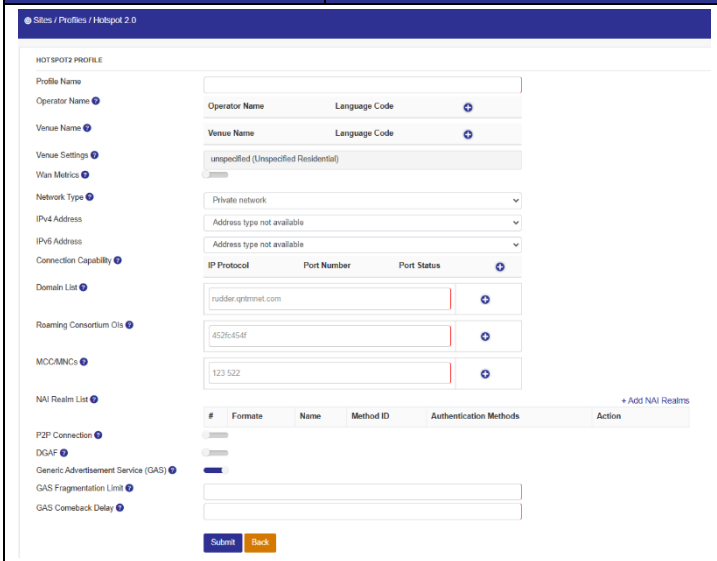
Go to **Cloud Menu > Site > Select Site > Profile > Bridge> Add**

Parameter	Description
	
Name	A unique identifier for the bridge interface.
Gateway IP Address	The IP address of the network gateway that routes traffic between networks
Net Mask	Defines the subnet mask to determine the network range.
VLAN ID	The VLAN identifier used to segment network traffic.

Hotspot 2.0

This feature allows mobile devices to seamlessly and securely connect to public Wi-Fi hotspot networks without requiring manual logins or password entry.

Go to **Cloud Menu > Site > Select Site > Profile > Hotspot 2.0> Add**

Parameter	Description	Default Value
		
Profile Name	Assign unique identifier for the Hotspot 2.0 configuration.	
Operator Name	The **Operator Name** specifies the Hotspot 2.0 operator along with the language code. The maximum length must not exceed 252 bytes. The language code indicates the language in which the operator's friendly name is specified, following the **ISO 639-2 standard**. Up to 32 operator names can be added.	

Venue Name	The **venue name**, along with the language code, can have a maximum length of 252 bytes. The language code specifies the language in which the venue name is provided, following the **ISO 639-2 standard**. Up to 32 venue names can be added.
Venue Settings	Venue Settings define where the AP is deployed, including venue groups and types. The venue group is selected from a predefined list, determining the available venue types. Up to 32 venue names can be added.
WAN Metrics	Enable the option as needed and specify WAN connection details, including link status and uplink/downlink speeds, for the wireless network.
Network Type	Select a Network Type from the predefined list. Choose at least one.
IPv4 Address	Specifies IPv4 addressing support for connected clients.
IPv6 Address	Specifies IPv6 addressing support for connected clients.
Connection Capability	The Connection Capability section defines supported protocols, port statuses, and wired network capabilities. Ensure firewall rules in the Wi-Fi profile align with port settings.

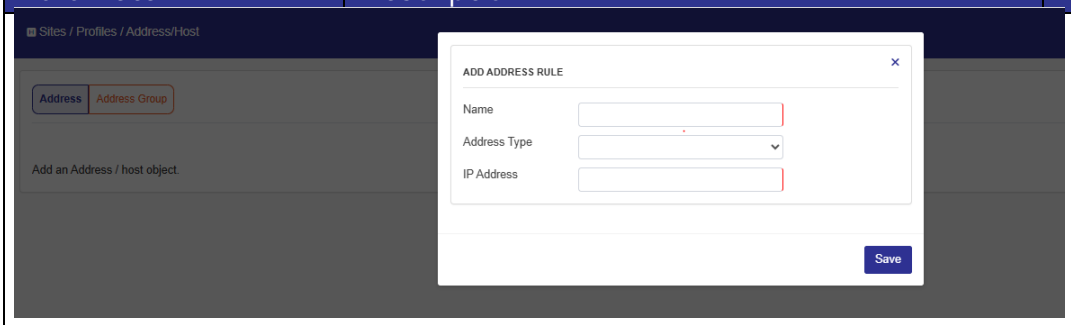
Domain List	The Domain Name List contains Hotspot 2.0 operator domain names, with a maximum of 32 domains. Each domain name must not exceed 255 bytes.
Roaming Consortium OIs	A roaming consortium allows network support for multiple service providers using unique hex identifiers. The first three are advertised in the beacon, with up to 32 supported. Each must be 3 bytes (6 hex) or 5 bytes (10 hex).
MCC/MNCs	The list of mobile networks supported by the AP can be configured in this option. Enter the three-digit Mobile Country Code (MCC) and the two- or three-digit Mobile Network Code (MNC), then click Add to include it in the list. Up to 32 entries can be added.
NAI Realm List	The NAI Realm List defines NAI realms linked to service providers or entities accessible through the AP. Each realm can include up to four EAP methods, listed in order of preference. Click EAP Settings in the Realm box to view the EAP methods for a specific realm.
P2P Connection	Issue this command to enable P2P device management. Disabled by default.
DGAF Off	If this feature is enabled, the AP does not forward downstream group-addressed frames. By default, it is disabled, allowing the AP to forward downstream group-addressed frames.
Generic Advertisement Service (GAS)	GAS, defined by 802.11u, allows a STA to obtain network information by exchanging Request and Response packets with the network.
GAS Fragmentation Limit	Defines the maximum size of GAS frames to ensure smooth communication between client devices and the hotspot.
GAS Comeback Delay	Specifies the wait time for clients requesting additional GAS responses when initial responses are fragmented or delayed.

Address/Host

This profile is used to configure bandwidth restrictions at the host, range, and subnet levels.

Go to **Cloud Menu > Site > Select Site > Profile > Address/Host> Add**

Parameter	Description	



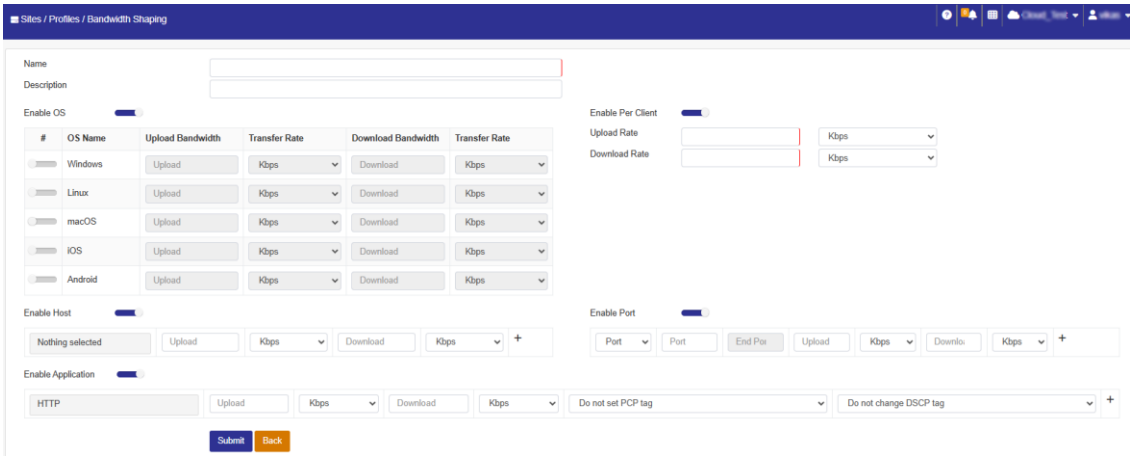
Parameter	Description	Default Value
Name	Assign unique identifier.	
Address Type	Select Type: **Host Range** – Specifies a range of IP addresses (e.g., 192.168.1.10 to 192.168.1.50) that can be allocated within the hotspot network. **Subnet** – Defines a network segment using a subnet mask (e.g., 192.168.1.0/24), allowing multiple devices within the subnet to communicate.	
IP Address	Enter IP Address.	

Bandwidth Shaping

This profile will be used to configure bandwidth restrictions at different levels (Port, Host, OS, etc.).

Go to **Cloud Menu > Site > Select Site > Profile > Bandwidth Shaping> Add**

Parameter	Description	



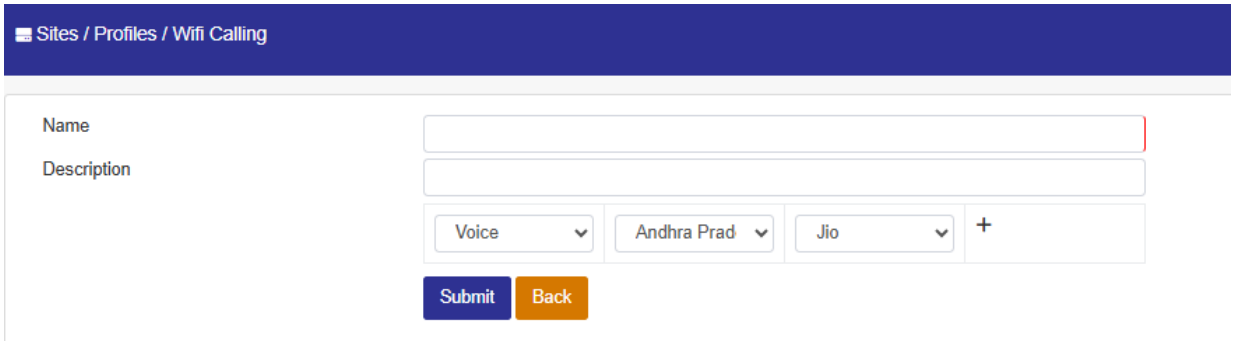
Parameter	Description	Default Value
Name	A unique identifier for the bandwidth shaping rule.	
Description	A brief explanation of the rule's purpose or scope.	
Enable OS	Enables bandwidth shaping based on the detected operating system (e.g., Windows, macOS, Android).	
Enable Host	Allows bandwidth control based on specific hostnames or IP addresses.	
Enable Application	Prioritizes or limits bandwidth for specific applications (e.g., streaming, gaming, VoIP).	
Enable Per Client	Allocates bandwidth limits individually for each connected client.	
Enable Port	Defines bandwidth rules based on network ports (e.g., HTTP on port 80, FTP on port 21).	

WiFi Calling

Wi-Fi calling allows making and receiving phone calls over a Wi-Fi network instead of using a cellular network. This feature is particularly useful in areas with poor cellular coverage but stable internet access.

Go to **Cloud Menu > Site > Select Site > Profile > WiFi Calling> Add**

Parameter	Description	

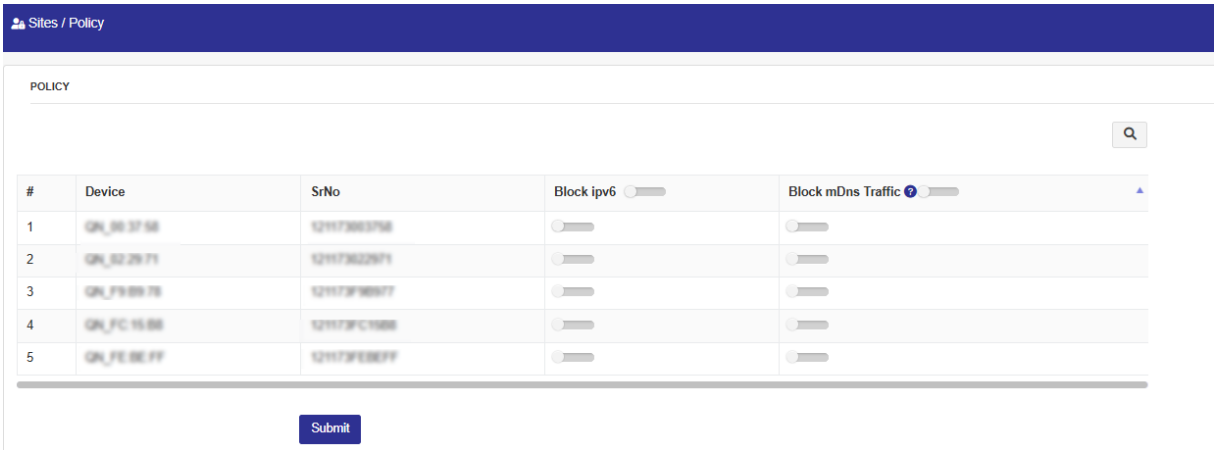


Parameter	Description	Default Value
Name & Description	Assign the **Name** and some basic description for reference.	

Policy

Go to **Cloud Menu > Site > Select Site > Policy**

Parameter	Description	

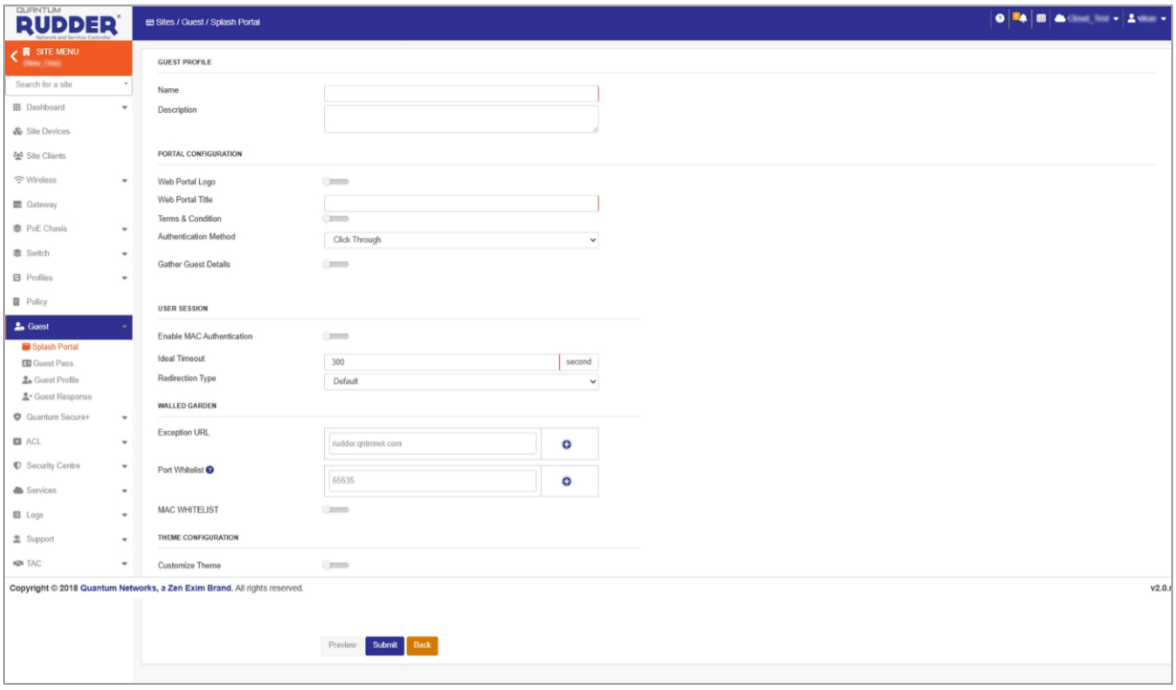


Description
Each onboarded access point will be listed here and can be individually configured to block IPv6 and block mDNS traffic based on network policies. **Blocking IPv6** prevents devices from using IPv6 addresses, ensuring only IPv4 traffic is allowed. **Blocking mDNS** (Multicast DNS) restricts local network service discovery, reducing unnecessary multicast traffic while enhancing security and performance.

Guest

A Guest Profile in the Splash Portal defines access policies for visitors, offering various authentication methods such as OTP, social login, or access codes. It manages guest responses, ensuring seamless and secure connectivity.

Go to **Cloud Menu > Site > Select Site > Guest**



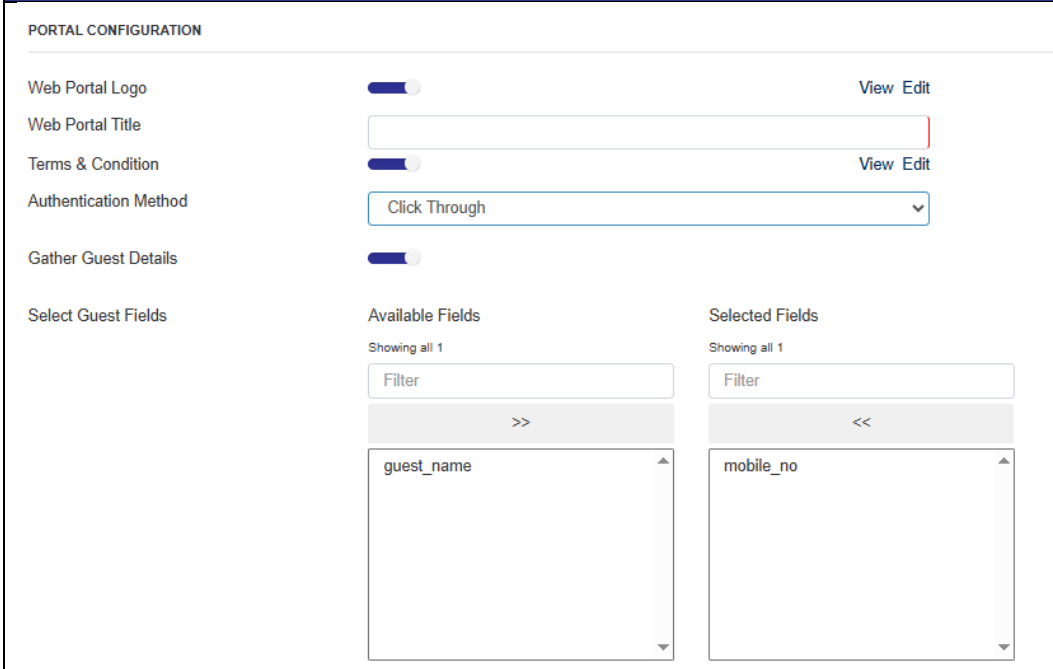
Splash Portal

Go to **Cloud Menu > Site > Select Site > Guest > Splash Portal**

The splash portal enables guest login with a logo, title, and authentication method. Guests accept terms & conditions before access, while admins collect user details by selecting relevant fields.

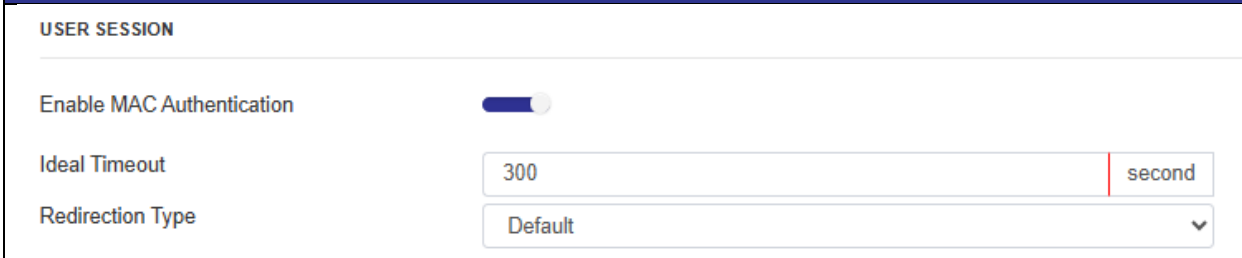
Parameter	Description	
GUEST PROFILE Name Description		
Guest Profile		
Parameter	Description	Default Value
Name	A unique identifier for splash portal policy	
Description	A brief explanation of the rule's purpose or scope.	

Portal Configuration



Web Portal Logo	Upload a custom logo displayed on the guest login page.	Disable
Web Portal Title	Set the title for the splash page to match branding or instructions.	
Terms & Condition	Display a required agreement that guests must accept before accessing the network.	Disable
Authentication Method	Choose the method for guest authentication, such as **Username/Password, OTP, Social Login, or Voucher Code**.	
Gather Guest Details	Enable collection of guest information for analytics or compliance.	Disable
Select Guest Fields	Define the specific fields to be collected, such as: **Name, Email, Phone Number, Custom Fields** (as required by the organization)	

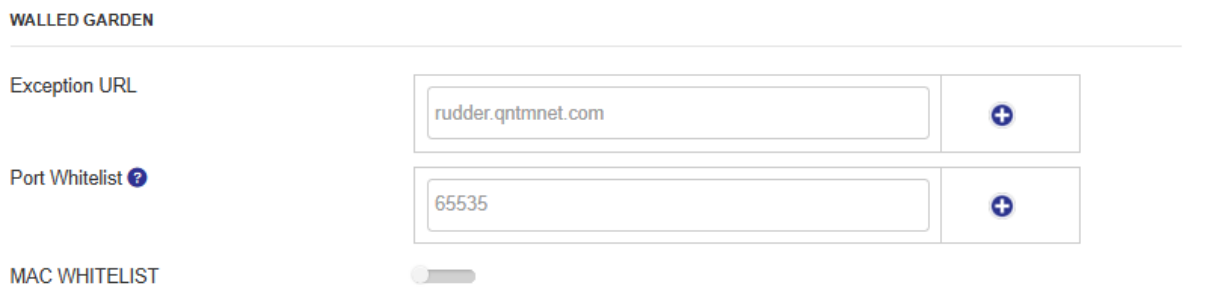
User Session



Enable MAC Authentication	When enabled, the system uses the device's MAC address to log in users automatically—useful for known or returning devices, so they don't need to enter login details every time.

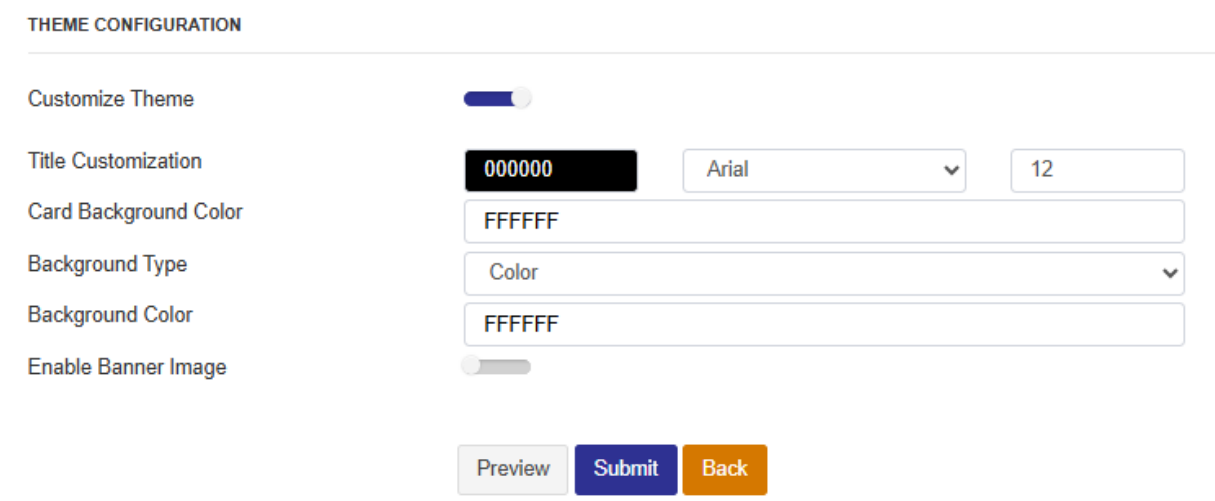
Ideal Timeout	Sets how long a user can be inactive before they are automatically logged out.
Redirection Type	Determines how users are redirected after connecting to the Wi-Fi after successful authentication.

Walled Garden



Exception URL	Add a list of websites (URLs) that guests can access without logging in to the portal.
Port Whitelist	Add a list of specific network ports that are allowed before authentication.
MAC Whitelist	Add a list of device MAC addresses that are exempt from authentication.

Theme Configuration



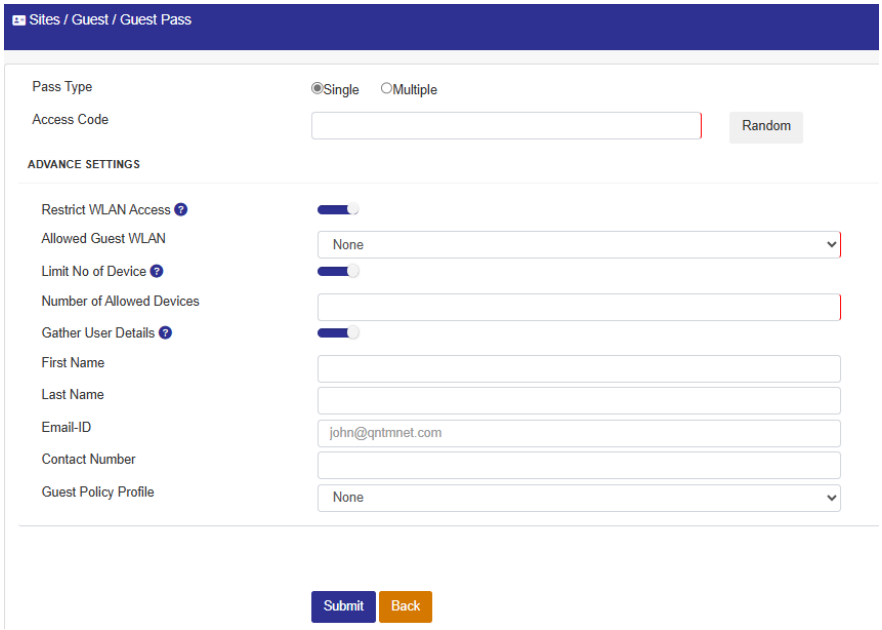
Customize Theme	This section allows the admin to visually personalize the guest Wi-Fi portal page to match the brand or venue style. The admin can adjust colors, images, and layout elements.	Disable
Title Customization	Allows the admin to modify the title text that appears on the portal page—such as changing font size, style, or color to better suit branding.	
Card Background Color	Refers to the color of the login card or form (the box where users enter their credentials). The	

	admin can choose a color that contrasts well with the background and maintains readability.	
Background Type	Determines what kind of background the portal page will have. It may be Solid Color or image.	
Background Color	Sets the color used for the portal page background if Background Type is set to Solid Color.	
Enable Banner Image	Toggle this ON to display a banner image at the top of the portal page—ideal for branding, promotions, or announcements.	Disable
Banner Images	Upload and manage one or multiple banner images. These are shown in the portal's banner section and can be static or rotate in a slideshow if multiple images are uploaded.	

Guest Pass

Guest Pass is an option to generate temporary access codes for guest users to access the internet. The admin can generate a single access code or select multiple entries to create multiple access codes that allows guests to connect to the internet for a limited duration based on predefined policies.

Go to **Cloud Menu > Site > Select Site > Guest > Guest Pass**

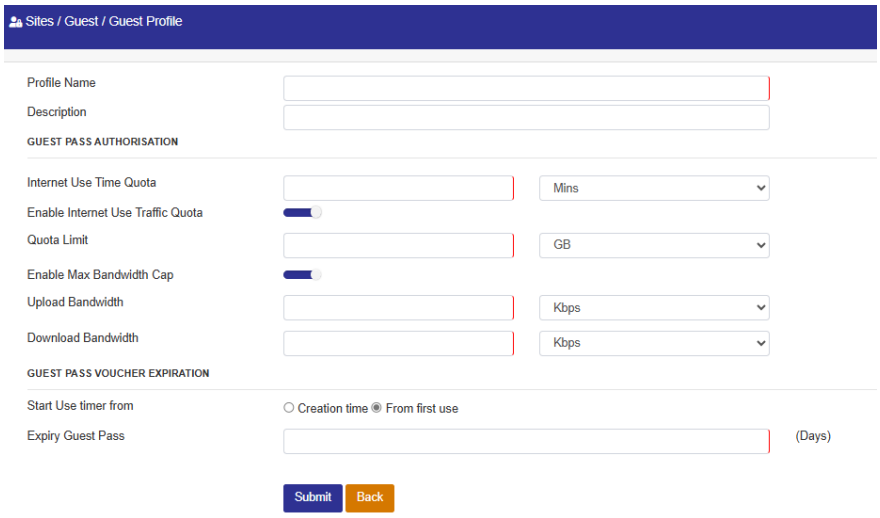
Parameter	Description
	

Parameter	Description	Default Value
Pass Type: Single		
Access Code	Select Access Code option: It can be Single or Multiple. When "Single" is selected, the system can generate a random code or the admin can define a custom code.	Random
Advance Settings		
Restrict WLAN Access	Enable WLAN restriction for this guest pass.	
Allowed Guest WLAN	Assign the required WLAN for guest login.	
Limit No of Device	Enable device restriction to limit concurrent device logins.	
Number of Allowed Devices	Assign the total number of devices that can connect using the same access code.	
Gather User Details	During registration, guests provide their First and Last Name for identification, contact number and an Email-ID (e.g., john@qntmnet.com) to receive the guest pass.	
First Name		
Last Name		
Email-ID		
Contact Number		
Guest Policy Profile	Select a predefined policy from the dropdown to define bandwidth limits, session duration, data quota, and other guest access rights.	
Pass Type: Multiple		
Number of Passes	Assign the total number of guest passes (i.e., access codes) to be generated simultaneously.	
Allowed Guest WLAN	Assign the required WLAN for guest login.	
Restrict WLAN Access	Enable WLAN restriction for this guest pass.	
Limit No of Device	Enable device restriction to limit concurrent device logins.	
Number of Allowed Devices	Assign the total number of devices that can connect using the same access code.	
Guest Policy Profile	Select a predefined policy from the dropdown to define bandwidth limits, session duration, data quota, and other guest access rights.	

Guest Profile

Go to **Cloud Menu > Site > Select Site > Guest > Guest Profile**

This option allows administrators to create guest pass policies by defining parameters such as pass validity, effective period, and expiry period for guest access.

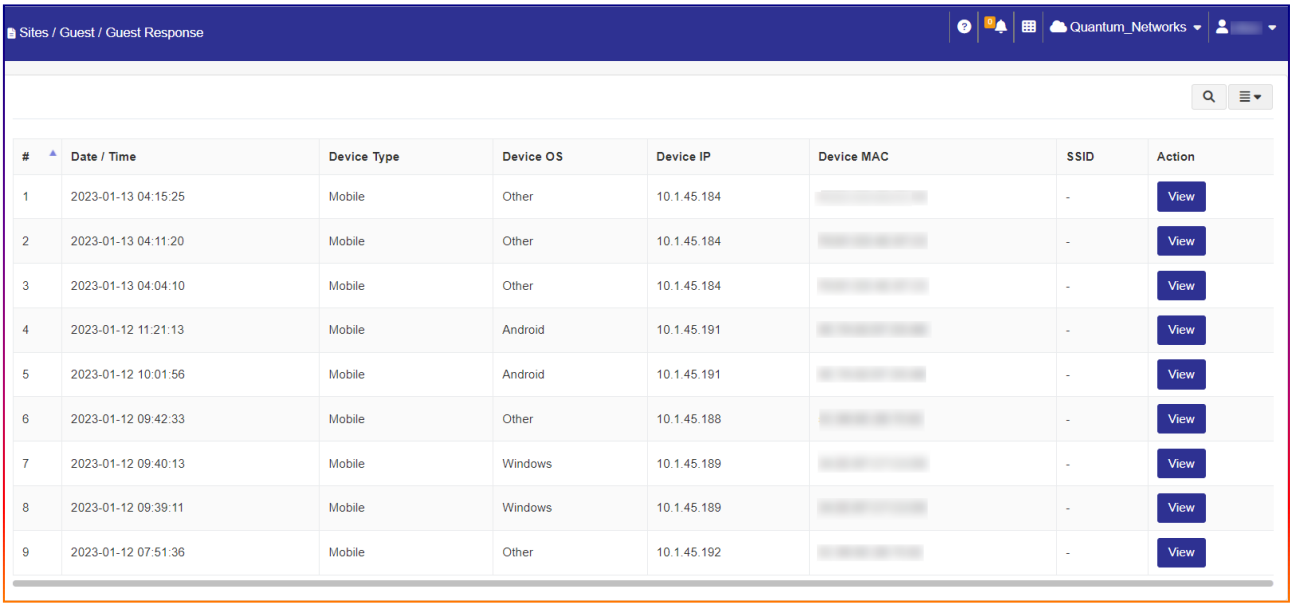
Click on Add – to create new guest profile	
	
Profile Name	A unique identifier for profile.
Description	A brief explanation of the profile.
Guest Pass Authorization	
Internet Use Time Quota	Defines the maximum duration (in minutes, hours, or days) a guest can use the internet after activation.
Enable Internet Use Traffic Quota	Option to enable or disable data usage tracking based on traffic volume.
Quota Limit	Sets the maximum amount of data (in MB or GB) a guest is allowed to use.
Enable Max Bandwidth Cap	Allows administrators to set upload and download speed limits for guest users.
Upload Bandwidth	Maximum upload speed (in Kbps or Mbps) allowed for guest devices.
Download Bandwidth	Maximum download speed (in Kbps or Mbps) allowed for guest devices.
Guest Pass Voucher Expiration	
Start use timer from	Defines when the validity timer should start.
Expiry Guest Pass	Absolute expiration date of the guest pass.

Guest Response

Guest response will display the user's session details, including the start and end date/time, the device detail which used for authentication, device OS, IP address assigned to the device, the SSID connected to, and the current status of the user—whether active or disabled.

Go to **Cloud Menu > Site > Select Site > Guest > Guest Response**

Parameter	Description	



#	Date / Time	Device Type	Device OS	Device IP	Device MAC	SSID	Action
1	2023-01-13 04:15:25	Mobile	Other	10.1.45.184		-	View
2	2023-01-13 04:11:20	Mobile	Other	10.1.45.184		-	View
3	2023-01-13 04:04:10	Mobile	Other	10.1.45.184		-	View
4	2023-01-12 11:21:13	Mobile	Android	10.1.45.191		-	View
5	2023-01-12 10:01:56	Mobile	Android	10.1.45.191		-	View
6	2023-01-12 09:42:33	Mobile	Other	10.1.45.188		-	View
7	2023-01-12 09:40:13	Mobile	Windows	10.1.45.189		-	View
8	2023-01-12 09:39:11	Mobile	Windows	10.1.45.189		-	View
9	2023-01-12 07:51:36	Mobile	Other	10.1.45.192		-	View

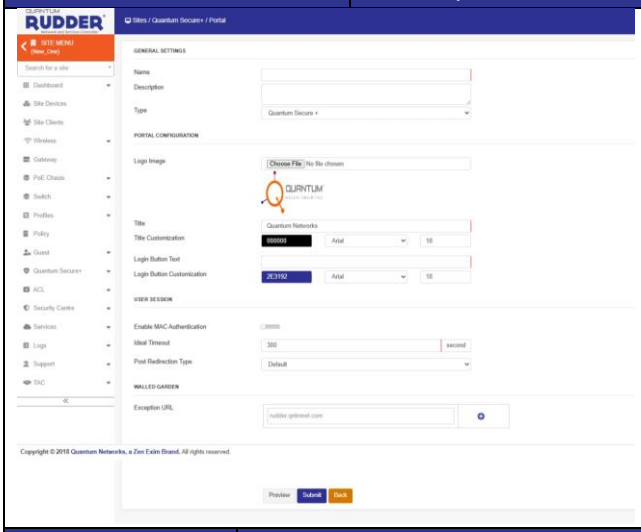
Quantum Secure+

Quantum SECURE+ ensures users authenticate via a web browser before accessing the internet. Each user logs in with unique credentials after connecting to the Wi-Fi (SSID) on any device.

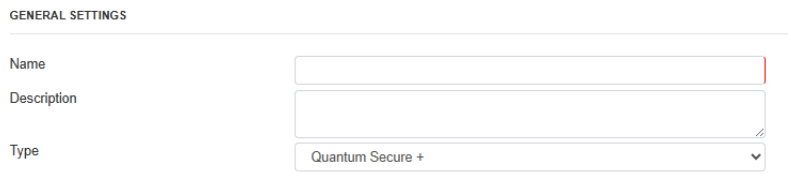
Portal

Go to **Cloud Menu > Site > Select Site > Quantum SECURE+ > Portal > Add**

Parameter	Description	

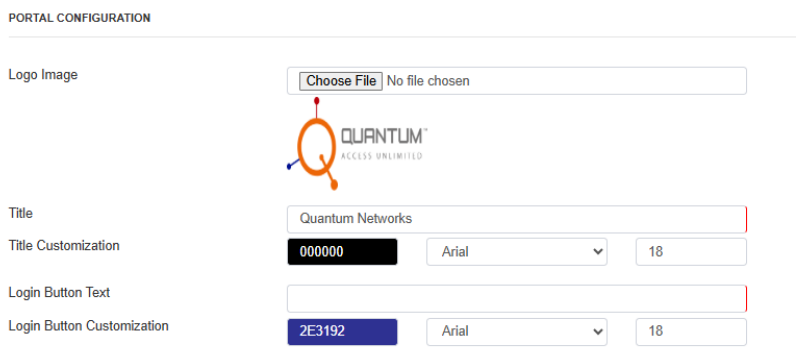


Parameter	Description	Default Value
General Settings		



Name	Unique name for identifying the Profile.
Description	Optional field to provide details.
Type	Select the authentication method: **Quantum Secure+:** For secure pass-based or MAC-based access. **Web Authentication:** Captive portal login through web-based credentials.

Portal Configuration

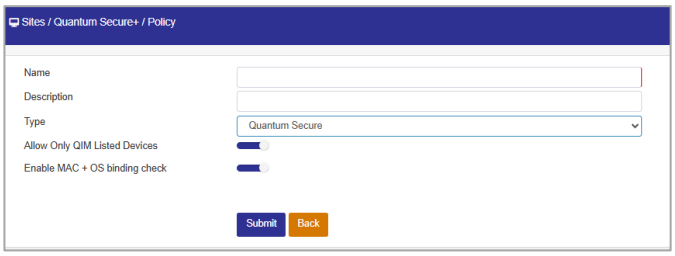
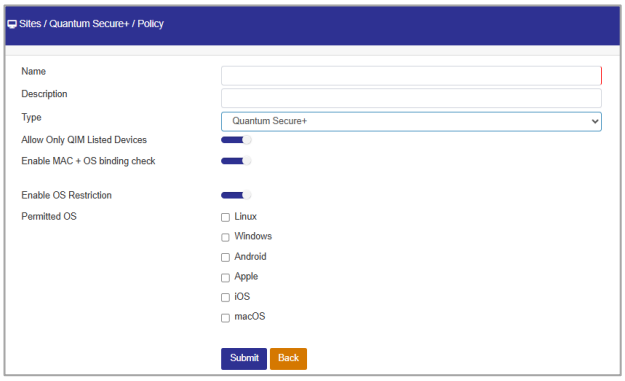


Logo Image	Upload a custom logo to display on the guest login page.
Title	Define main heading displayed on the login page
Title Customization	Modify the font, size, color, and style of the title.

Login Button Text	Text shown on the login/submit button.	
Login Button Customization	Customize button style, color, and appearance to match branding.	
User Session		
Enable MAC Authentication	Enables MAC-based login for returning users without needing to reauthenticate.	
Ideal Timeout	Automatically logs out inactive users after a set time (e.g., 5 minutes of inactivity).	
Post Redirection Type	Determines redirection after login.	
Walled Garden		
Exception URL	List of domains or IPs accessible without authentication i.e. URLs that bypass portal redirection even when accessed before login.	
Advance		
OSU	Enables self-registration or online sign-up for users without predefined credentials.	Disable

Policy

Cloud Menu > Site > Select Site > Quantum SECURE+ > Policy > Add

Policy	
	
Name	Unique name for identifying the Profile.
Description	Optional field to provide details.
Type	Select the policy from dropdown: Secure or Secure+

Allow Only QIM Listed Devices – Disable		
	Secure- Enable	Secure+- Enable
Enable OS Restriction	NA	Provide an option where the admin can enable OS restriction and activate the permitted OS list.
Allow Only QIM Listed Devices – Enable		
	Secure- Enable	Secure+- Enable
Enable MAC + OS binding check	Enable MAC + OS Binding Check: When enabled, this feature verifies that both the MAC address and the Operating System (OS) of the connecting device match the entries specified under the assigned QIM policy. If either the MAC or OS does not match, access will be denied based on the policy settings.	Additionally, with Secure+, it provides an option to allow permitted OS types that are not listed under the QIM policy.

ACL

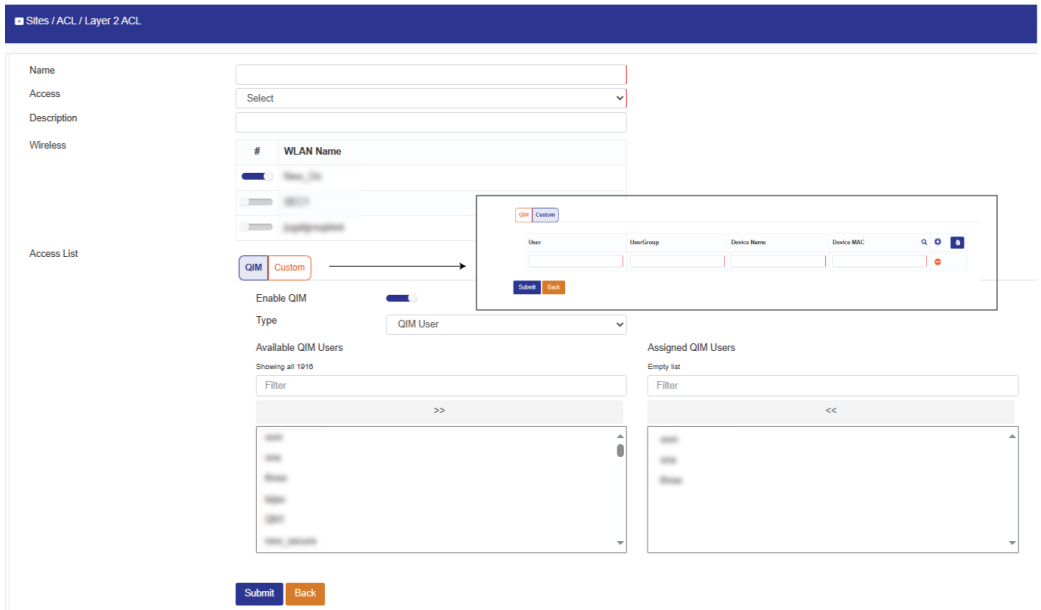
In an Access Point (AP), an Access Control List (ACL) manages network security by filtering traffic:

- Layer 2 ACL – Controls access via MAC addresses.
- Layer 3 ACL – Filters traffic based on IP addresses and protocols.
- Session Control – Restricts the number of sessions according to the defined policy.
- OS Policy – Restricts access based on device operating systems.
- MAC Whitelist – Allows only approved devices to connect.

Layer 2 ACL

Layer 2 ACLs filter traffic at the data link layer based on MAC addresses and Ether Type, enhancing security by controlling frame access within a VLAN or switch port.

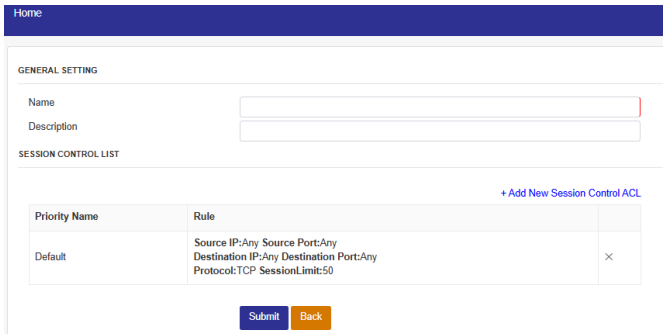
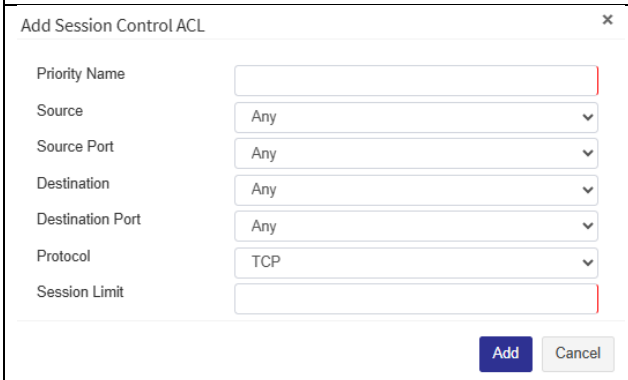
Cloud Menu > Site > Select Site > ACL > Layer 2 ACL > Add

Layer 2 ACL	
	
Name	Unique name for identifying the Profile.
Access	Select “Allow” or “Deny” from drop down as per the requirement.
Description	Optional field to provide details.
Wireless	Enable the SSID on which the Layer 2 ACL feature needs to be activated.
Access List	There are two options. The admin can enable the QIM option, which further provides two choices: select predefined users or user groups listed under QIM for whom this feature needs to be activated. Simultaneously, the admin can also configure custom users to whom the feature should be applied.

Session Control

Session control in ACL (Access Control List) refers to managing or restricting individual user sessions based on specific rules or policies. It's typically used in network devices like firewalls, routers, or wireless controllers to enforce security, user management, and traffic optimization.

Site > Select Site > ACL > Session Control > Add >Add New Session Control ACL

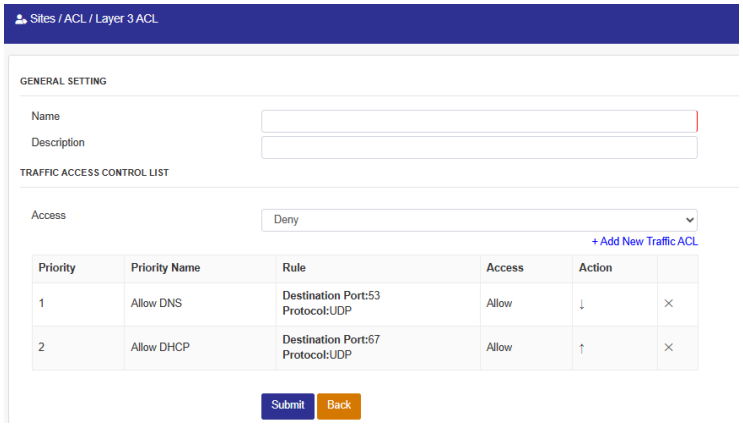
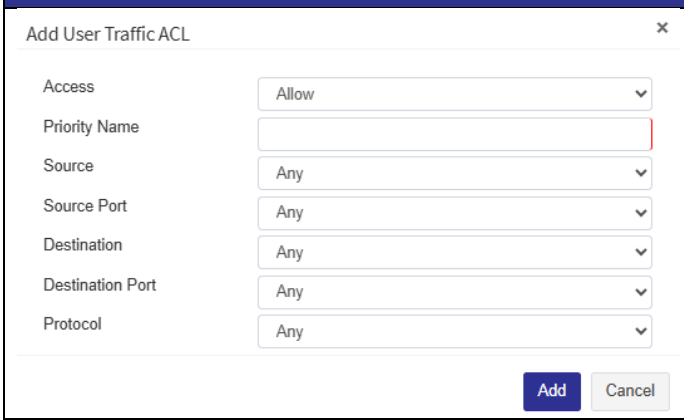
Session Control

Click on "Add New Session Control ACL"


Add Session Control ACL		
Priority Name	Determines the order of evaluation. Lower numbers are evaluated first. Important for matching the correct rule.	
Source	Assign the originating IP address or subnet of the traffic. E.g., 192.168.1.11 the individual IP or 192.168.1.0/24 to match all hosts in that subnet.	
Source Port	Assign the Port Number or Port Range on the source device.	
Destination	Assign the originating IP address or subnet of the traffic. E.g., 192.168.1.11 the individual IP or 192.168.1.0/24 to match all hosts in that subnet.	
Destination Port	Assign the target IP address or subnet where traffic is headed. Can be used to access a specific server or network.	
Protocol	Specifies the Layer 3 protocol type – typically TCP, UDP, TCP+UDP, ICMPV4 or ICMP, ESP, AH. Allows filtering based on protocol.	
Session Limit	It defines how many concurrent sessions can work simultaneously.	

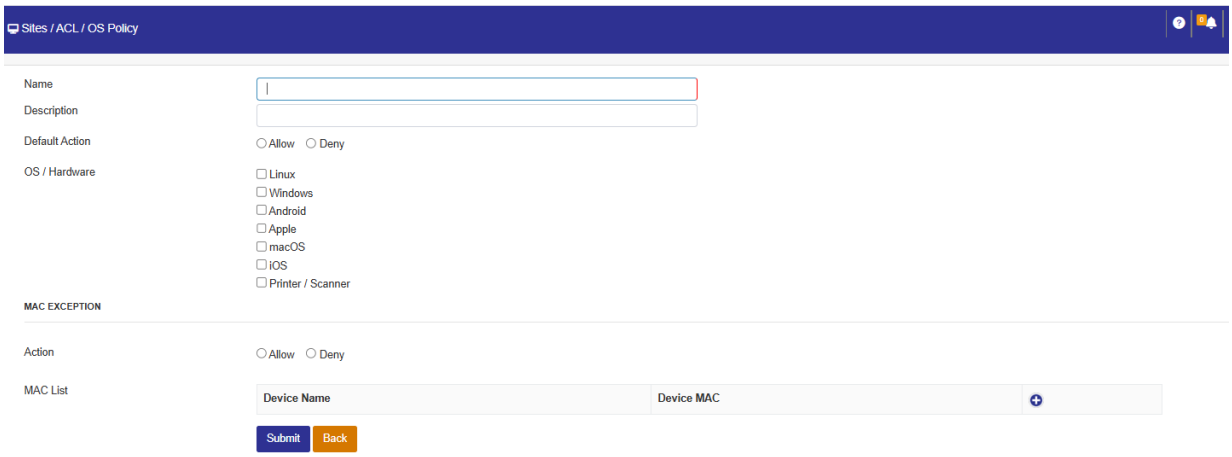
Layer 3 ACL

Layer 3 ACL (Access Control List) is a network security feature used to control the flow of IP traffic based on Layer 3 parameters.

Site > Select Site > ACL > Layer 3 ACL > Add > Add New Traffic ACL

Layer 3 ACL	
	
Name-Description	Unique name for identifying the Profile and Optional field to provide details.
Click on Add User Traffic ACL	
	
Access	Defines whether to Permit or Block the traffic that matches the rule.
Priority Name	Determines the order of evaluation. Lower numbers are evaluated first. Important for matching the correct rule.
Source	Assign the originating IP address or subnet of the traffic. E.g., 192.168.1.11 the individual IP or 192.168.1.0/24 to match all hosts in that subnet.
Source Port	Assign the Port Number or Port Range on the source device.
Destination	Assign the originating IP address or subnet of the traffic. E.g., 192.168.1.11 the individual IP or 192.168.1.0/24 to match all hosts in that subnet.
Destination Port	Assign the target IP address or subnet where traffic is headed. Can be used to access a specific server or network.
Protocol	Specifies the Layer 3 protocol type – typically TCP, UDP, TCP+UDP, ICMPV4 or ICMP, ESP, AH. Allows filtering based on protocol.

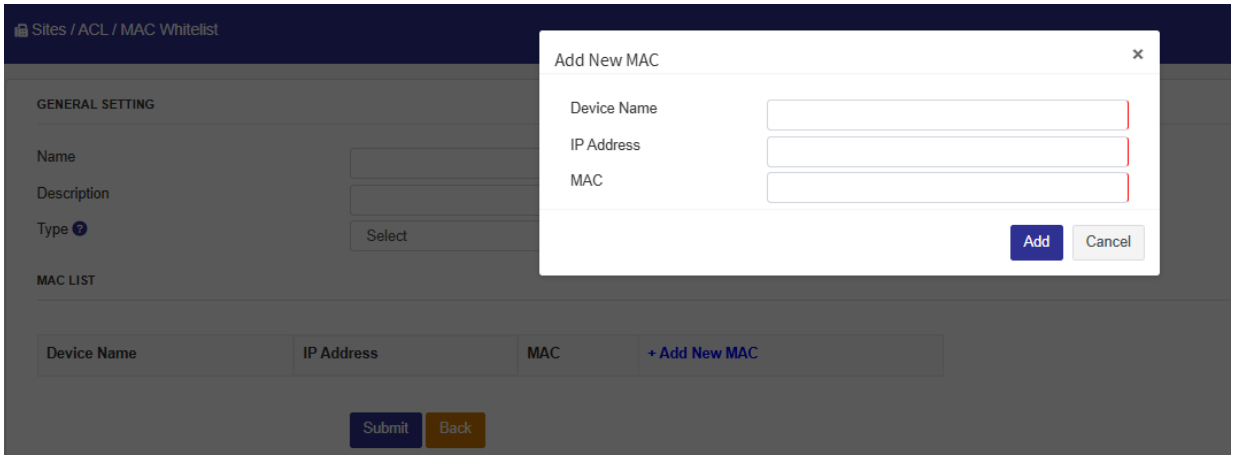
OS Policy



Name & Description	Unique name for identifying the Profile and Optional field to provide details.
Default Action	Defines the action (Allow or Deny) applied to all devices that do not match any defined OS or hardware rule.
OS / Hardware	Specifies the target device types (by operating system or hardware vendor). Example: Android, iOS, Windows, Linux, or specific hardware like Apple.
MAC Exception	
Action	The decision (Allow or Deny) for the devices that match the specified OS/Hardware in the rule.
MAC List	A list of MAC addresses to be either blocked or allowed depending on the policy action—used to enforce or override access based on MAC address.

MAC Whitelist

This profile allows the creation of a list of Media Access Control (MAC) addresses, which, when bound to an SSID, are permitted to access the network, provided some restriction policies are implemented.

MAC Whitelist


General Setting	
Name & Description	Unique name for identifying the Profile and Optional field to provide details.
Type	Select Allow/Deny to Permits/ Block devices listed under the profile.

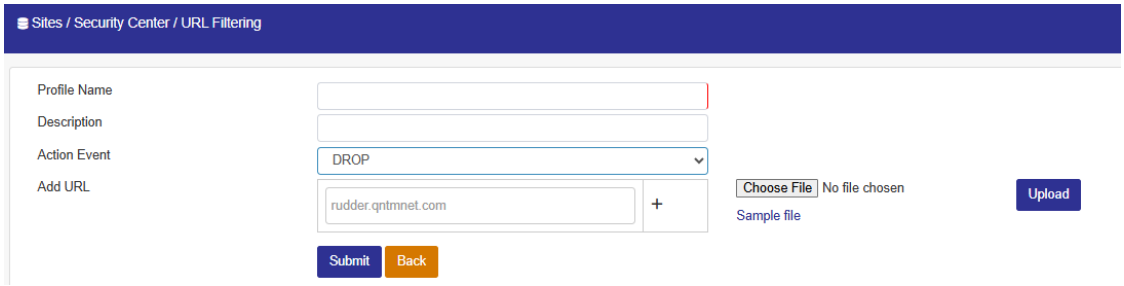
MAC List	
MAC Whitelisting	Allows only specific listed devices (by MAC address) to connect to the network.
Client Isolation	The list of MAC addresses to which the client isolation policy will not apply when a device tries to connect to an SSID with client isolation enabled.

Security Centre

URL Filtering

URL filtering is a security measure that allows or blocks access to specific Uniform Resource Locators (URLs) or websites as defined.

Site > Select Site > Security Centre> URL Filtering > Add

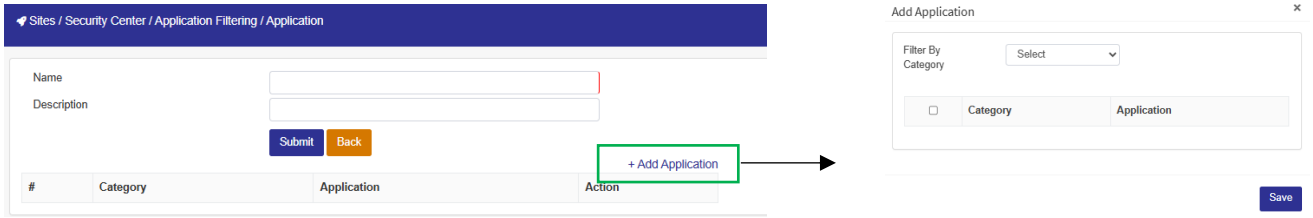
URL Filtering	
	
Profile Name & Description	Unique name for identifying the Profile and Optional field to provide details.
Action Event	These actions are defining URL filtering rules. DROP: The AP blocks or discards the URL request. The client is denied access. ACCEPT: The AP allows the URL request to proceed. The client is granted access.
Add URL	Add the required URL that needs to be allowed or denied from the client side as per the given policy.

Application Filtering

App filtering is a security measure that allows or blocks access to specific applications as defined by policy.

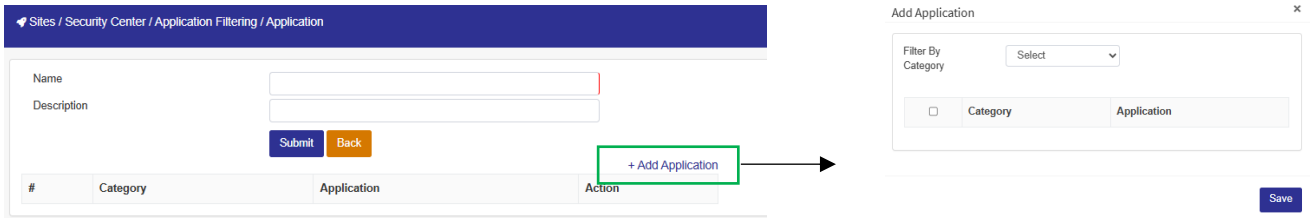
Application Group

Site > Select Site > Security Centre> Application Filtering > Application Group >Add

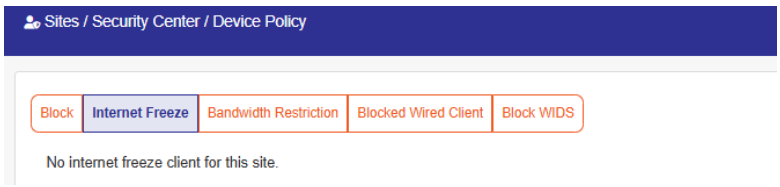
Application Group	
	
Application Group	An Application Group is a custom category that bundles multiple applications together for easier management. Admins can group apps based on categories with their respective services. Application Filtering is a control mechanism used to monitor, prioritize, block, or limit specific applications or application groups on the network.

App Filtering

Site > Select Site > Security Centre> Application Filtering > App Filtering >Add

App Filtering	
	
App Filtering	Select the preconfigured application group from the dropdown and assign access rights by choosing either Allow or Deny.

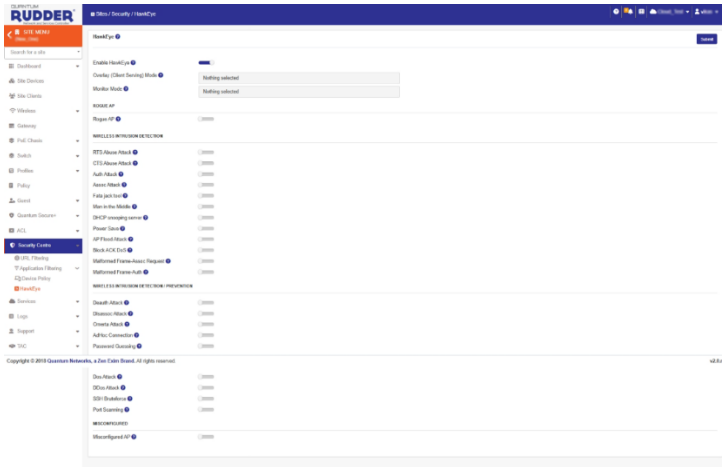
Device Policy

Device Policy

The option displays all clients along with their assigned policies, such as Block Clients, Internet Freeze, Bandwidth Restriction, Blocked Wired Clients, and Blocked WIDS details. From here, the admin can modify the rights for individual clients under each policy.

HawkEye

HawkEye is a centralized Security Center designed to monitor and manage the security posture of both wireless and wired networks.

Note: By default, the option is disabled.

HawkEye	
	
HawkEye is a centralized security platform for managing security across both wireless and wired networks. Enable HawkEye feature when required.	
Overlay Mode (Client Serving)	In Overlay Mode, the AP serves clients on 2.4 GHz and 5 GHz while simultaneously scanning for wireless, wired, and network intrusions. It detects rogue and misconfigured APs, identifies threats across all channels, and may cause brief packet loss or performance dips due to background scanning.
Monitor Mode	In Monitor Mode, both 2.4 and 5 GHz radios scan all available country-specific channels every 5 seconds, acting as sensors for wireless, wired, and network intrusion detection and prevention. They also detect rogue and misconfigured APs at set intervals. In this mode, client services are disabled.

Rogue AP: Rogue AP is the untrusted Access Point that can potentially disrupt network operations. An AP is considered to be a Rogue AP if it is seen in the RF environment but is not connected to the same wired network. An AP is considered to be a Wired-Rogue AP if it is both unauthorized and plugged into the wired side of the same network. Admin has to define UnTrusted and Trusted MAC OUI and SSID, based on that AP classify Rogue AP. During Rogue AP scanning, Wireless clients may face fluctuation in LAN and Internet connection in both 2.4 and 5 GHz band. We recommended using this functionality in dedicated Monitor mode only with disabled wireless functionality.	
Scan Duration	Enable this to set the scanning duration after which the AP will check the status.
OUI Details	Scanning can be performed based on Trusted MAC OUI, Trusted SSID, and Untrusted MAC OUI.
To effectively detect **Rogue SSIDs** and other wireless threats, enable the following security detection features	
Rogue SSID	Identifies an unauthorized SSID (network name) broadcast in the environment that mimics a legitimate network or serves malicious purposes.
MAC Spoofing	Identifies devices using fake MAC addresses to impersonate legitimate clients or APs.
SSID Spoofing	Detects unauthorized access points broadcasting the same SSID as your network to trick users.
Honeypot / Evil Twin	Flags access points that mimic trusted networks to capture user data or launch attacks.
NULL Probe Request	Identifies suspicious probe requests without SSID information, which may indicate reconnaissance or attack attempts.
Wireless Intrusion Detection	
RTS Abuse Attack	Detects and blocks devices flooding the AP with excessive RTS (Request to Send) frames to prevent network disruption.
CTS Abuse Attack	Prevents denial-of-service attempts by identifying continuous CTS (Clear to Send) frame abuse aimed at freezing the wireless channel.
Auth Attack	Blocks clients sending repeated or fake authentication requests that can overload the AP and deny service to genuine users.
Assoc Attack	Stops devices from sending massive association requests to fill the AP's client table, ensuring stable connections for real users.
Fata jack tool	Identifies activity from the FataJack penetration testing tool used to simulate attacks like deauthentication or spoofing.
Man in the Middle	Protects clients from MITM attacks by monitoring and blocking suspicious interception attempts.

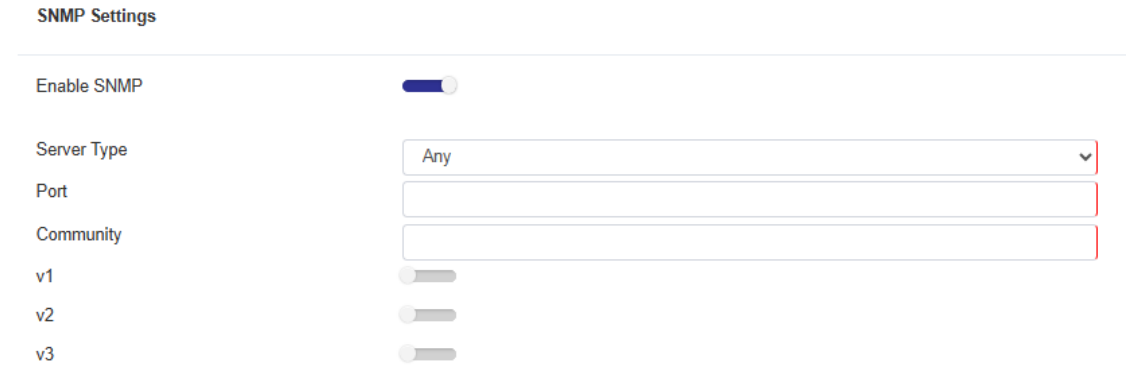
DHCP snooping server	Allows only trusted DHCP servers to assign IPs and prevents rogue DHCP servers from causing misconfigurations or redirecting traffic.
DHCP Snooping Details	Maintains logs of DHCP transactions including IP-to-MAC bindings and violations, helping with auditing and troubleshooting.
Power Save	Monitors and blocks misuse of the 802.11 power-saving mechanism that could delay or drop packets intentionally.
AP Flood Attack	Detects fake beacon or probe frame floods used to create phantom APs and overload the wireless spectrum.
AP Flood threshold	Set the maximum number of beacons/probes allowed per second to trigger alerts or block the flooding source.
Block ACK DoS	Identifies and blocks malformed Block Acknowledgement (Block ACK) frames used to exhaust AP resources.
Malformed Frame-Assoc Request	Blocks corrupted or malicious Association Request frames intended to exploit the AP's packet parser.
Malformed Frame-Auth	Detects and drops invalid Authentication frames that could be used in targeted wireless attacks.
Wireless Intrusion Detection / Prevention	
Deauth Attack	Detects fake deauthentication frames sent to disconnect users from the access point.
Disassoc Attack	Identifies false disassociation frames used to forcibly disconnect clients.
Omerta Attack	Monitors for passive attackers who silently capture traffic without transmitting.
AdHoc Connection	Detects unauthorized peer-to-peer wireless links between client devices.
Password Guessing	Tracks repeated authentication failures to identify brute-force or dictionary attacks.
Timeframe	Defines the monitoring window for tracking security events (e.g., 5 mins, 30 mins, 1 hour).
No of Attempts	Configures how many attempts (e.g., password tries or deauth frames) are allowed before the system triggers alerts or blocks.
Network Intrusion Detection / Prevention	
Dos Attack	Monitor and block attempts to overload the network or AP with excessive traffic that may lead to service disruption.
DDos Attack	Detect and mitigate distributed denial-of-service attacks originating from multiple sources aiming to flood the network.
SSH Bruteforce	rack and block repeated SSH login attempts to prevent unauthorized device access through brute-force techniques.
Port Scanning	Identify suspicious scanning activities that probe for open or vulnerable network ports.

Misconfigured	Flag devices with improper or insecure configurations that may pose a risk to network security.
Misconfigured AP	Detect access points with incorrect settings such as weak encryption, open SSIDs, or improper VLAN configurations.
Scan Duration	Set and control how frequently the system scans the network for intrusion attempts and anomalies (e.g., every 5 minutes, hourly).

Services

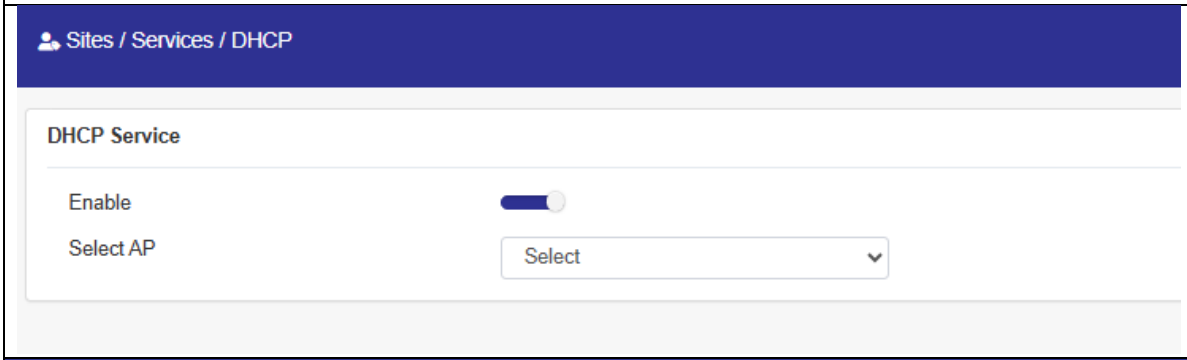
SNMP (Simple Network Management Protocol)

This protocol, when enabled on the AP, monitors and collects performance and device metrics using OIDs.



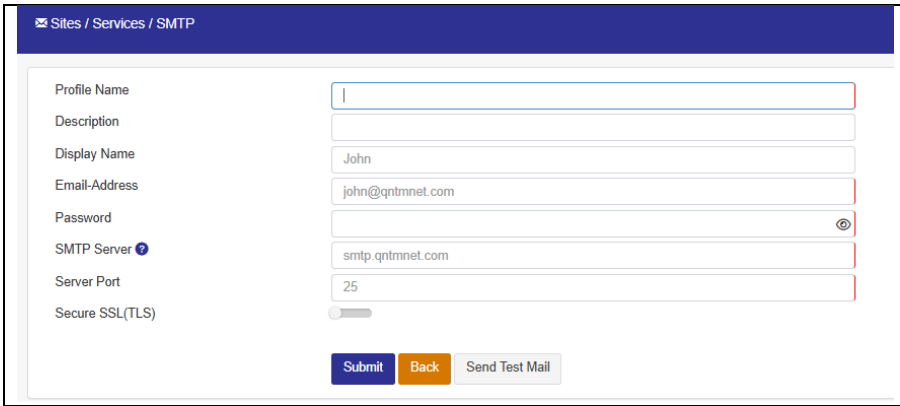
DHCP (Dynamic Host Configuration Protocol)

When enabled in Bridge Mode, the AP acts as a DHCP server for the entire network and assigns IP addresses to client devices based on the configured pool. It is mandatory to configure the AP with a static IP address before enabling the DHCP server.



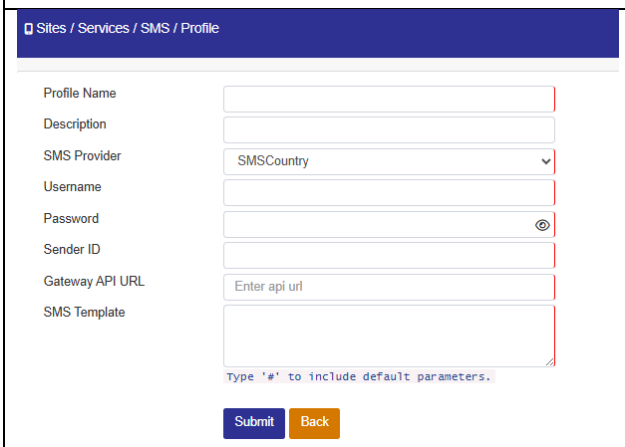
SMTP

Simple Mail Transfer Protocol (SMTP) is an internet standard used to send email messages. When an SMTP profile is configured on the AP, it can be used with features such as report scheduling or notification services to alert admins about specific events.



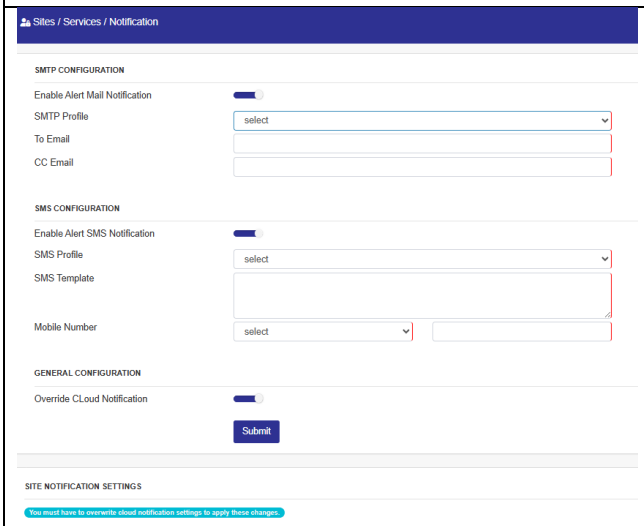
SMS

This feature allows the creation of a profile to integrate with an SMS service provider, enabling certain events to be reported to the admin. It can be used alongside reporting features such as 'Notification'.



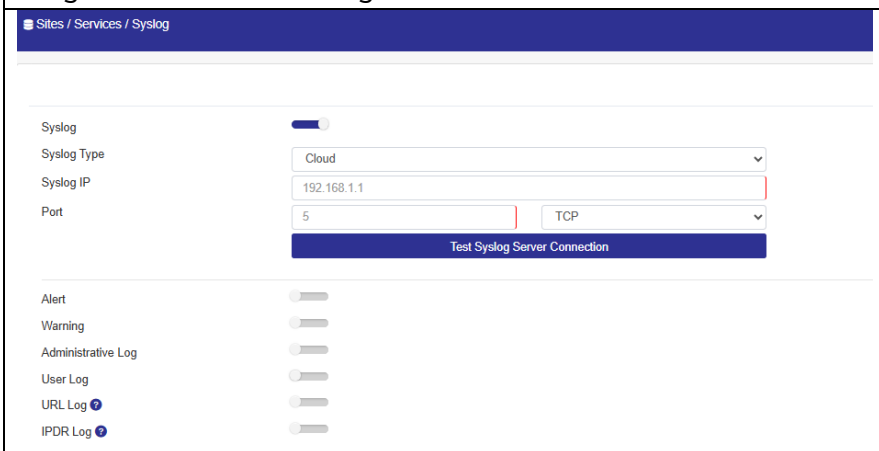
Notifications

Enable alerts for critical events such as device disconnection, high CPU usage, rogue AP detection, or bandwidth threshold breaches—keeping admins informed and responsive.



Syslog

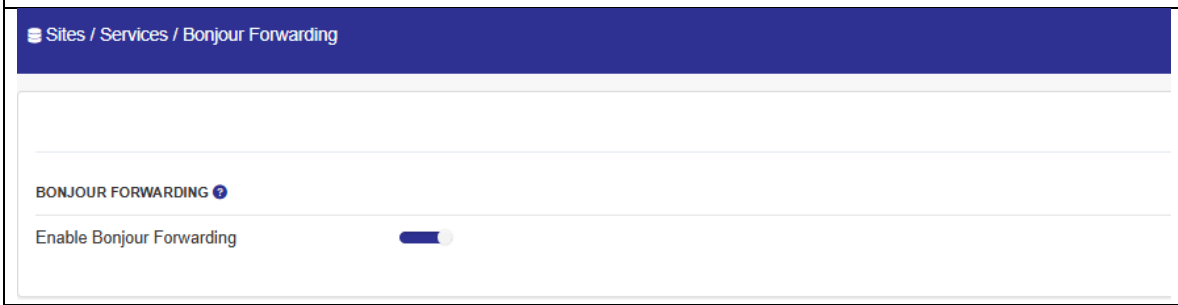
Forward system logs from access points to a central syslog server for audit, diagnostics, and long-term event tracking.



Bonjour Forwarding

Bonjour Forwarding allows Apple devices (like iPhones and Macs) to discover services such as printers and file sharing across different VLANs. It works by using an mDNS proxy to forward service announcements between networks.

Note: This feature cannot be used if Block mDNS Traffic is enabled.



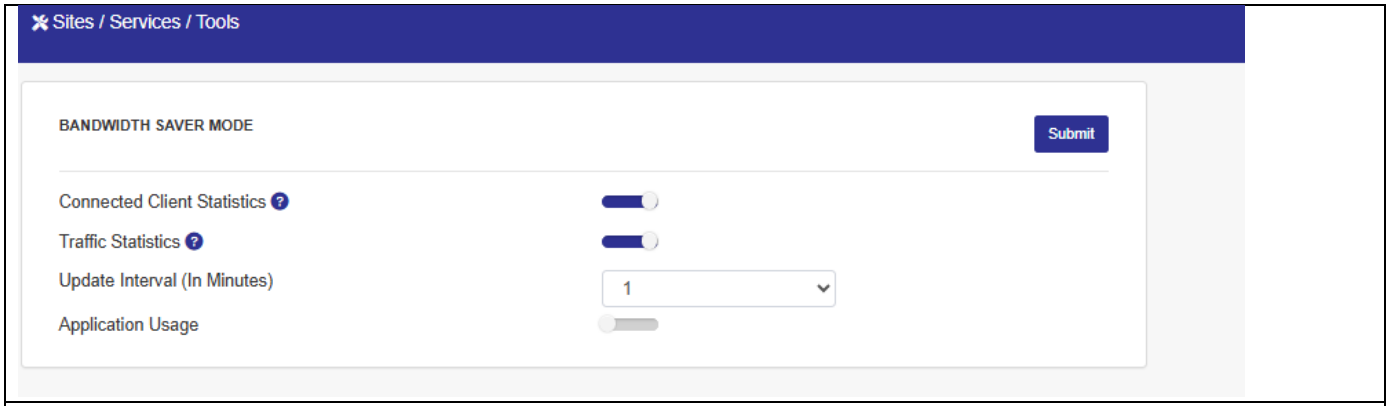
Tools

Connected Client Statistics: View live details of all connected clients, including signal strength, data rate, SSID, MAC address, and device type.

Traffic Statistics: Monitor upload/download traffic per access point or client—helps in identifying heavy users or network congestion.

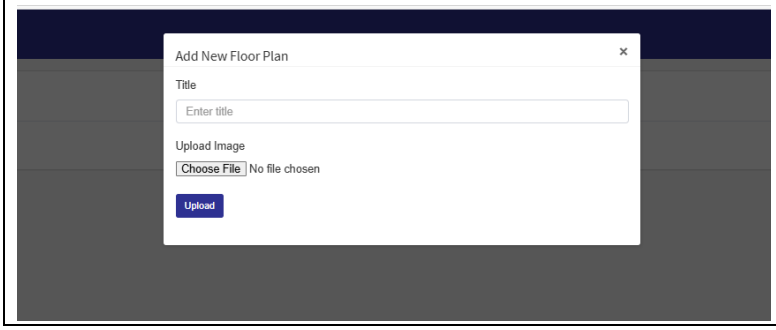
Update Interval (In Minutes): Set how frequently the dashboard refreshes data (e.g., every 1, 5, or 15 minutes) for real-time monitoring.

Application Usage: Track bandwidth consumption by application categories (e.g., social media, streaming, gaming) to identify usage trends or restrict non-business traffic.



Floor Plan

Visualize AP placement and coverage on uploaded floor maps. Helps with signal planning, client tracking, and interference zone identification.



RF Management

Monitor and optimize the wireless radio environment—adjust power levels, channels, band steering, and mitigate co-channel interference for better network performance.

Spectrum Analyzer:
Scans the radio frequency (RF) environment to detect interference from both Wi-Fi and non-Wi-Fi sources (e.g., microwaves, Bluetooth). Helps in identifying noisy channels that may degrade Wi-Fi performance.

Spectrum Channel Metric:
Provides a quality score for each channel based on interference and usage, guiding admins to select the best channel for reliable performance.

Spectrum FFT Duty Cycle:
Shows how often a specific frequency range is in use. A high duty cycle indicates heavy interference, helping admins understand RF congestion and make channel planning decisions.

WiFi Analyzer:
Displays real-time Wi-Fi metrics like signal strength, channel utilization, connected devices, and SSID visibility—useful for troubleshooting and optimizing AP placement and settings.

Logs

These log sections help administrators monitor system activities, track user actions, and troubleshoot issues efficiently.

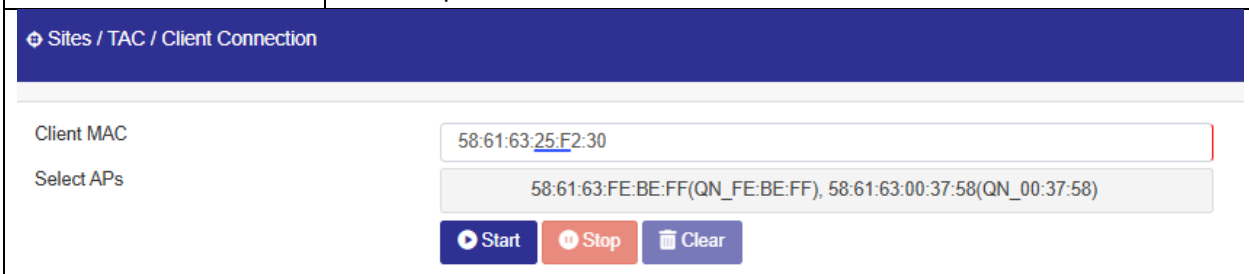
Parameter	Description
Administrative	Logs all admin activities such as configuration changes and access to critical settings. Useful for auditing and accountability.
Users	Provides logs of the connect and disconnect events of client devices connected to the AP.
Alerts	Provides logs of connect and disconnect events for client devices connected to the AP.
Events	Provides event logs such as the AP onboarding process, sync status with the cloud controller, and more.
Guest	Provides event logs such as the AP onboarding process, sync status with the cloud controller, and more.
HawkEye	Logs security-related events detected by the HawkEye module such as rogue APs, intrusion attempts, or WIDS/WIPS alerts.
Mesh	Captures logs related to mesh AP connectivity—such as link establishment, failures, or topology changes.
WDS	Captures logs related to WDS AP connectivity—such as link establishment.
Network	Tracks networking logs such as IP address changes, interface status, VLAN tagging, DHCP activity, and routing updates.
RRM	Logs automatic radio adjustments like power level tuning, channel changes, and band steering decisions made by the system.

Support

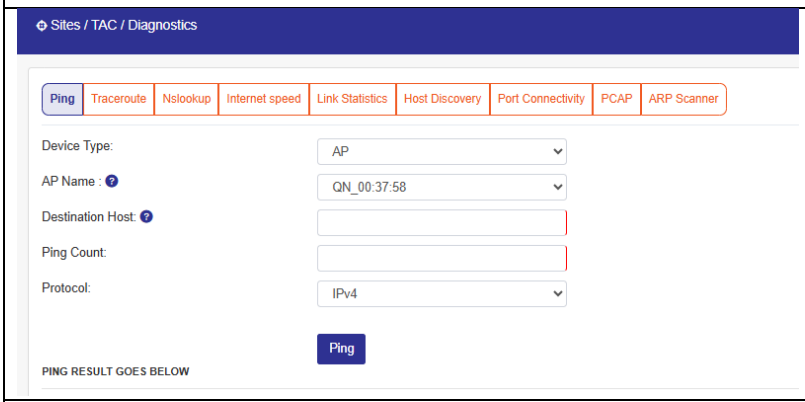
Parameter	Description
Technical Support	The admin can email support@qntmnet.com for any technical support assistance.
Crash Report	These reports capture memory dumps, error codes, and system state at the time of failure, helping developers or support engineers diagnose the root cause of hardware/software issues.

TAC

Parameter	Description
Client Connection	Enter the client MAC address and select the related Access Point from the dropdown to check which Access Point the client is connected to.



Diagnostics: Diagnostics provides tools to test, analyze, and troubleshoot network and device performance. It includes functions like ping, traceroute, speed tests, log reviews, and system health checks to help administrators quickly identify and resolve issues.



Ping: Sends ICMP echo requests to a host to test connectivity and measure round-trip time. Helps verify if a device or server is reachable.

Traceroute: Traces the path packets take to reach a destination. Identifies network hops and latency between the source and the target.

Nslookup: Performs DNS queries to resolve domain names to IP addresses. Useful for troubleshooting DNS issues.

Internet Speed: Measures upload and download speed from the Access Point to the internet. Helps evaluate bandwidth and connectivity performance.

Link Statistics: Displays detailed statistics about physical and logical network links such as link uptime, errors, dropped packets, and throughput.

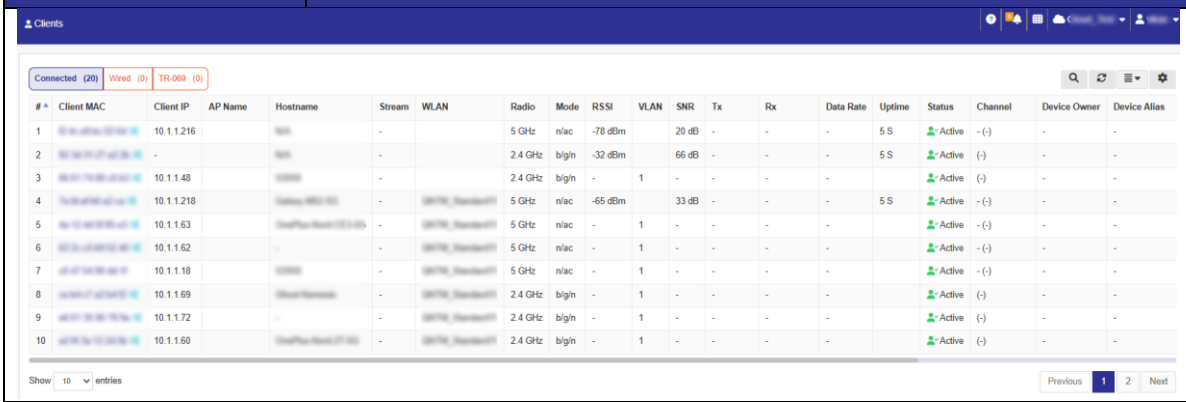
Host Discovery: Scans the local network to detect active devices. Useful for identifying connected clients and potential unauthorized systems.

Port Connectivity: Tests if a specific port on a remote server or device is open and reachable. Commonly used to check access to services (e.g., HTTP, SSH).

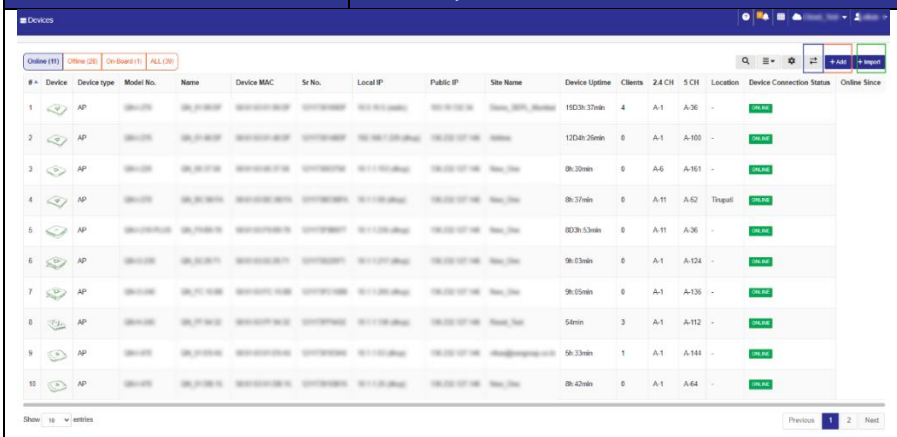
PCAP (Packet Capture): Captures and logs raw network traffic for analysis. Useful for deep packet inspection, debugging, and security audits.

ARP Scanner: Scans the subnet for devices using ARP requests. Helps map IP addresses to MAC addresses and identify connected clients.

Clients

Parameter	Description
	
Displays all Wi-Fi devices currently associated with all the APs across the organization, lists devices connected to the AP via Ethernet, and indicates if the client is being remotely managed via the TR-069 protocol.	

Devices

Parameter	Description
	
This option displays all available devices—Online, Offline, On-Board, All (Consolidated)—across all sites on this cloud.	
	By clicking the **'Add'** option on the top panel, the admin can perform AP Pre-Provisioning—configuring and registering an Access Point (AP) in the network management system before it is physically installed or powered on at the deployment site. The admin can either pre-provision a single AP or '**import'** a file containing details of multiple Access Points to perform bulk pre-provisioning.
	With this option, the admin can transfer an Access Point from one site to another.

	With this option, the admin can select the required fields to display in this section.
	With this option, the admin can extract report in csv or pdf format.

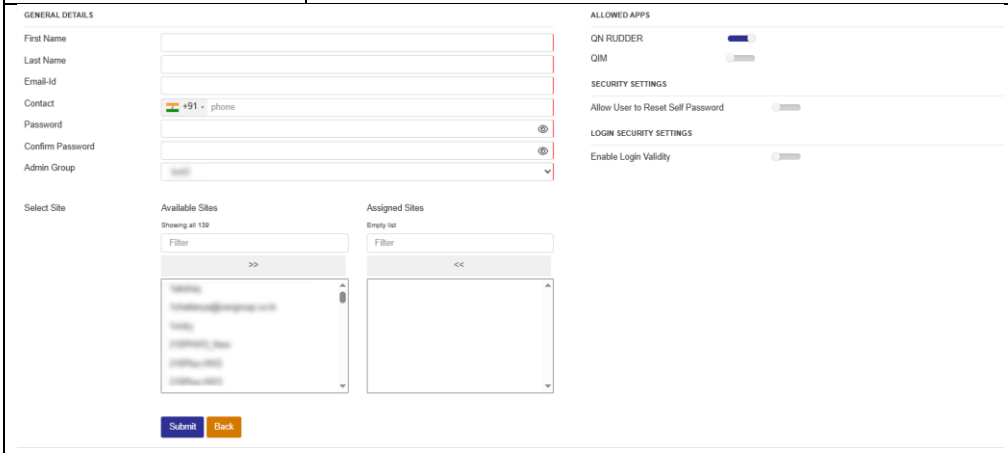
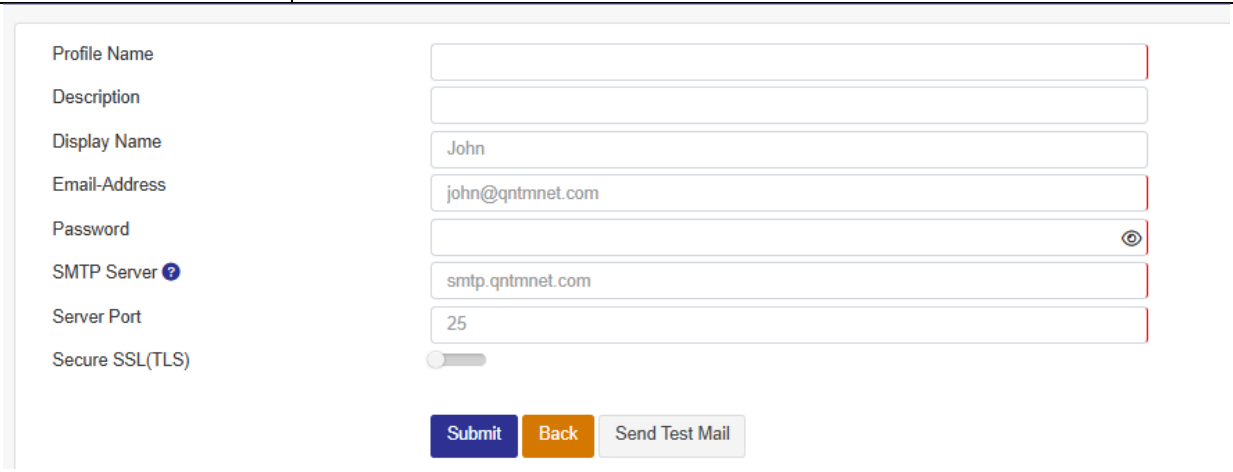
Organization Wide

Parameter	Description
VLAN	VLANs defined here can be configured as Data, Voice, Multicast, or Guest VLANs, and will be applicable across all sites under this organization/cloud account.
Scheduling	The Scheduling Profile is used to automate the activation and deactivation of specific features—such as SSID broadcasting, client access, or bandwidth limits—based on predefined time and day settings. The settings configured here will be applicable to all sites under the organization.
SNMP	SNMP Profile enables centralized monitoring and management of all access points across sites using SNMP tools, allowing performance tracking, alerting, and diagnostics from a single network management system.
Hotspot	Create a Hotspot Profile that can be configured and used globally across all sites under the cloud account. For detail configuration guideline click "Hotspot".
Authentication	Create an Authentication Profile that can be configured and used globally across all sites under the cloud account. For detail configuration guideline click "Authentication".
URL Filtering	URL filtering is a security measure that allows or blocks access to specific URLs or websites as defined. The profile configured here can be used globally across all sites under the cloud account.
Application Filtering	App Filtering is a security measure that allows or blocks access to specific applications as defined by policy. The configured profile here can be used globally across all sites under the cloud account.
Policy	Enabling this option will schedule a reboot based on the predefined schedule profile selected for the entire organization.
Syslog	This parameter enables centralized logging by forwarding system events, security alerts, and operational logs from access points to a specified Syslog server. This helps in real-time monitoring, troubleshooting, and compliance auditing across all sites managed under the cloud account.

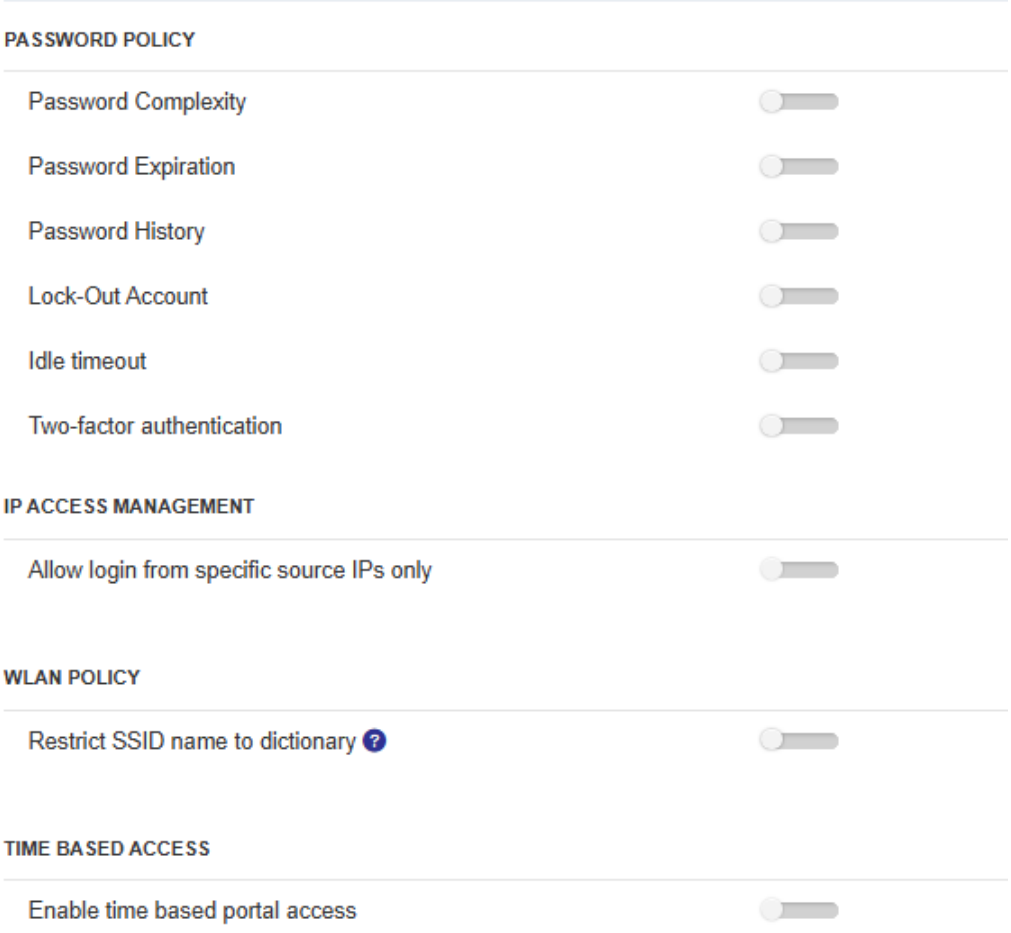
Wireless

Parameter	Description
WLAN	With this section, the admin can configure wireless networks by creating a new SSID (WLAN), modifying an existing one if needed, and deleting it if unused. This SSID can be used globally across this cloud organization. For detail configuration guideline click "WLAN".

Administration

Parameter	Description
Users	With this option, new users can be created by assigning different roles based on the requirement.
	
Active Session	Will show all active sessions globally across all sites.
Tags	
API Key	
SMTP	The added profile can be used globally across all sites where required.
	

Add on Service	Add-on services can be activated from this option, after which they will be available globally for all sites and can be utilized by any site based on its specific requirements.
Field Dictionary	
Firmware Management	The admin can upload and manage new firmware files and save them to the cloud, which can then be utilized by individual sites to upgrade devices with the new firmware versions.
Report Scheduler	The admin can set a scheduler for the selected report to run every 12 hours, daily, weekly, or monthly, and have it sent to a configured email ID using the selected SMTP profile.
Cloud Security	The admin can set policies related to password security, IP access management, restrict SSID access to specific directories, and define time-based access according to domain requirements.



Single Sign-on	Single Sign-On (SSO) Policy allows users to authenticate once using a central identity provider and gain access to multiple systems or applications without needing to log in separately to each one. It simplifies user experience, improves security by reducing password fatigue, and enables centralized access control across the organization.

Logs

Parameter	Description
Administrative Logs	The Admin Log provides a detailed record of administrative actions, including the date and time of the action, the source of the action (such as the web portal or mobile app), the administrator who performed the action, a description of the action (e.g., SSID update, user deletion), the site where the action was applied, and the source IP address from which the action was initiated, offering an audit trail for security and tracking purposes.
Quantum Secure+	Secure+ Logs capture detailed information about user sessions, including Username, Start Time, Stop Time, Duration, Download and Upload data, Total Data Transfer, IP Address, and MAC Address. These logs provide administrators with comprehensive insights into user activity, network usage, and security, helping with monitoring, troubleshooting, and compliance auditing.

Support

Parameter	Description
Remote Assistance	Remote Assistance enables authorized support personnel to access the system remotely for troubleshooting, secured by a Support PIN—a temporary, system-generated code. Enabling 2FA Support PIN adds an extra layer of security, ensuring only verified sessions can be initiated.

TAC

Parameter	Description
Diagnostics	Diagnostics provides tools to test, analyze, and troubleshoot network and device performance over the entire organization. It includes functions like ping, traceroute, speed tests, log reviews, and system health checks to help administrators quickly identify and resolve issues.

License

Description
License details include the unique License Key, its Type (e.g., Subscription or Trial), Activation date, Validity period (Valid Till), allowed Capacity Count with its respective Unit (such as Users or Devices), the applicable License Scope (device, site, or global), and the current Status indicating whether the license is active, expired, or inactive.

Analytics

The report provides overall analytics, covering all sites.

Parameter	Description
Data Usage	Analytics Overview provides detailed insights into deployed devices across all sites. It displays key information such as Site Name (where the device is located), Serial Number (Sr No.), MAC Address, Model Number, Activation Date, Expiry Date, and current Status (active, inactive, or expired). This helps in tracking device lifecycle, deployment status, and site-wise distribution for effective asset and license management.
Clients	It provides total client details based on the selected sites and the specified date range.
Historic Clients	istoric Clients Detail provides a comprehensive log of previously connected client devices, displaying information such as Client MAC, Client IP, AP Name, Hostname, WLAN (SSID), Radio (2.4 GHz or 5 GHz), Tx/Rx (data transmitted/received), RSSI (signal strength), SNR (signal-to-noise ratio), Connected On (connection timestamp), and Session Time (duration of connection), helping in analyzing user behavior, troubleshooting connectivity issues, and reviewing network usage patterns over time.
Device Link Statistics	
Client Connection Report	It will provide a graphical view that includes data from all sites, showcasing the Network Service Health and client connection status report.

Warranty Checker

Description
The Warranty Checker provides key device details, including Site Name, Serial Number (Sr No.), MAC Address, Model Number, Activation Date, Expiry Date, and Status, helping administrators track each device's warranty status to ensure timely support and replacement requests.

Quantum Analytics

Description