

QUANTUM
RUDDER[®]
Network and Services Controller

USER GUIDE

Copyright Information

The copyright and trademark specifications mentioned in this document are subject to change without prior notice. All the content, including the Quantum Networks® logo, is the property of Zen Exim Pvt. Ltd. Other brands or products mentioned in this document may be trademarks or registered trademarks of their respective owners. It is strictly prohibited to use, translate or transmit the contents of this document in any form or by any means without obtaining prior written permission from Zen Exim Pvt. Ltd.

Document Abstract

This document explains how to Configure and Manage Quantum Rudder (Quantum Networks' Cloud Controller).

Contents

Glossary	7
Web Interface Feature List.....	9
Account Setup on Quantum RUDDER	10
Login to Quantum RUDDER Web Interface	11
About Web Interface	12
Side panel and Main Screen	12
Top Panel	13
Icon Description	14
Cloud Menu.....	15
Dashboard.....	15
Sites.....	21
Site Dashboard.....	23
Site Devices	24
Site Clients.....	25
Wireless.....	25
WLAN.....	25
Access Point.....	32
Independent AP configuration.....	32
AP Group configuration	37
Wi-Fi Mesh	40
Router (AP).....	41
Gateway.....	41
Switch.....	42
Profiles.....	43
Hotspot.....	43
Authentication	44

AAA.....	45
Active Directory.....	46
LDAP.....	47
Custom API.....	47
Scheduling.....	48
QoS.....	48
Guest.....	49
Splash Portal.....	49
Guest Pass.....	51
Guest Profile.....	52
Quantum Secure+.....	53
Portal.....	53
Policy.....	54
ACL.....	55
Layer 2 ACL.....	55
Layer 3ACL.....	56
OS Policy.....	57
MAC Whitelist.....	57
Security Centre.....	58
URL Filtering.....	58
Application Filtering.....	59
Application Group.....	59
App Filtering.....	59
Device Policy.....	60
WIDS.....	60
Services.....	60
DHCP.....	61
SNMP.....	61
SMTP.....	62
SMS.....	63
Notifications.....	63

Syslog.....	64
Tools.....	65
Floor Plan	65
Outdoor Plan	65
Logs.....	65
Administrative.....	65
User	66
Alerts	66
Events	66
Guest.....	66
WIDS.....	67
Mesh.....	67
Support.....	67
Technical Support.....	67
Crash Report.....	67
TAC	67
Client Connection	67

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 an IP address to devices.
Static	A <i>static</i> Internet Protocol (<i>IP</i>) address (<i>static IP</i> address) is a fixed IP Address assigned to the device.
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 can transfer data at high speeds.
LAN	Local Area Network
WAN	Wide Area Network
VLAN	Virtual Local Area Network allows several networks to work virtually as one LAN.
SSID	Service Set Identifier is a unique ID that consists of 32 characters and is used for naming wireless networks.
WPA2	WPA2 (Encryption Method) - Wi-Fi Protected Access 2 - Pre-Shared Key is a method of securing your network using Pre-Shared Key (PSK) for authentication.
WPA-Mixed	With WPA mixed (Encryption Method) mode, devices can be connected with both WPA (TKIP) and WPA2 (AES) encryption methods.
TKIP	TKIP (Temporal Key Integrity Protocol) is an encryption protocol included as part of the IEEE 802.11i standard for wireless LANs (WLANs). It was designed to provide more secure encryption than the notoriously weak Wired Equivalent Privacy (WEP), the original WLAN security protocol.
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 you select 20/40 MHz mode, the router decides to use 20 or 40 MHz based on the interference/contention the router detected.
-------------------	---

Term	Definition
Wireless 2.4 GHz	2.4 GHz band provides great distance coverage, however, transmits data at slower speeds.
Wireless 5 GHz	The 5 GHz band provides less coverage, however, transmits data at faster speeds.
Authentication method - Open	Open authentication allows any device to authenticate and then attempt to communicate with the Access Point. By using open authentication, any wireless device can authenticate with the Access Point but the device can communicate only if its Wired Equivalent Privacy (WEP) keys match the Access Point's WEP keys. Devices not using WEP do not attempt to authenticate with an Access Point that is using WEP.
Authentication method - 802.1x EAP	This authentication type provides the highest level of security for your wireless network. 802.1x (also known as WPA-prise), is an authentication method by which users are authenticated using an external RADIUS server.
WIDS	A Wireless Intrusion Detection System (WIDS) monitors the radio <i>frequencies</i> for the presence of unauthorized, rogue Access Points. The system monitors the radio <i>frequencies</i> used by wireless LANs and immediately alerts a systems administrator whenever a rogue Access Point is detected.
Rogue AP	Quantum RUDDER supports Rogue AP detection. A Rogue Access Point is a wireless Access Point that may be installed on a secure network without explicit authorization from a local network administrator, whether added by a well-meaning employee or a malicious attacker.
SMTP	SMTP- Simple Mail Transfer Protocol is a protocol for sending e-mail messages between servers.

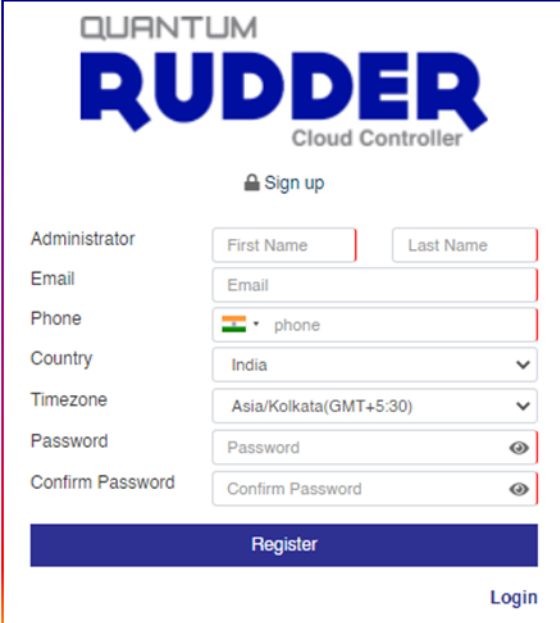
Web Interface Feature List

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

Account Setup on Quantum RUDDER

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



The screenshot shows the registration page for Quantum RUDDER Cloud Controller. At the top, the logo reads "QUANTUM RUDDER Cloud Controller". Below the logo is a "Sign up" button with a lock icon. The registration form includes the following fields:

- Administrator:** Two input fields for "First Name" and "Last Name".
- Email:** A single input field for the email address.
- Phone:** A dropdown menu for country selection (currently showing the Indian flag) followed by a "phone" input field.
- Country:** A dropdown menu currently set to "India".
- Timezone:** A dropdown menu currently set to "Asia/Kolkata(GMT+5:30)".
- Password:** An input field with a toggle icon to show/hide the password.
- Confirm Password:** An input field with a toggle icon to show/hide the password.

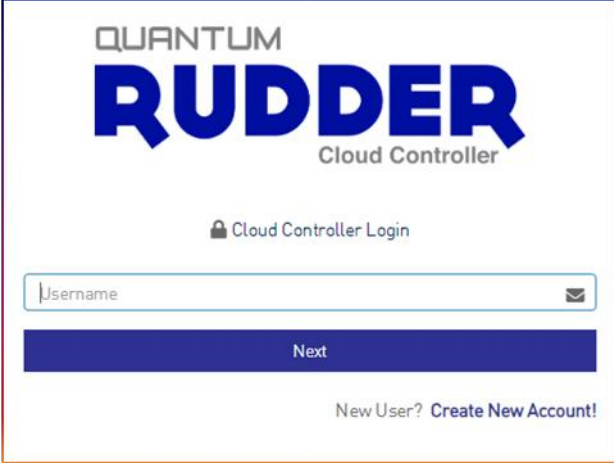
At the bottom of the form is a large blue "Register" button. In the bottom right corner, there is a "Login" link.

Figure 1

- Follow the steps as guided on the screen for Registration.
- Verify Quantum RUDDER© account from registered Email ID.
- Once the account gets validated, it turns the page to "Add License Key" (User will get the license key from 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>
- Credentials and click Login.



The screenshot shows the login interface for Quantum RUDDER. At the top, the logo reads "QUANTUM RUDDER Cloud Controller". Below the logo is the text "Cloud Controller Login" with a lock icon. There is a text input field labeled "Username" with a small envelope icon on the right. Below the input field is a dark blue button labeled "Next". At the bottom, there is a link that says "New User? Create New Account!"

Figure 2

- Successful log in redirects to Quantum RUDDER dashboard.

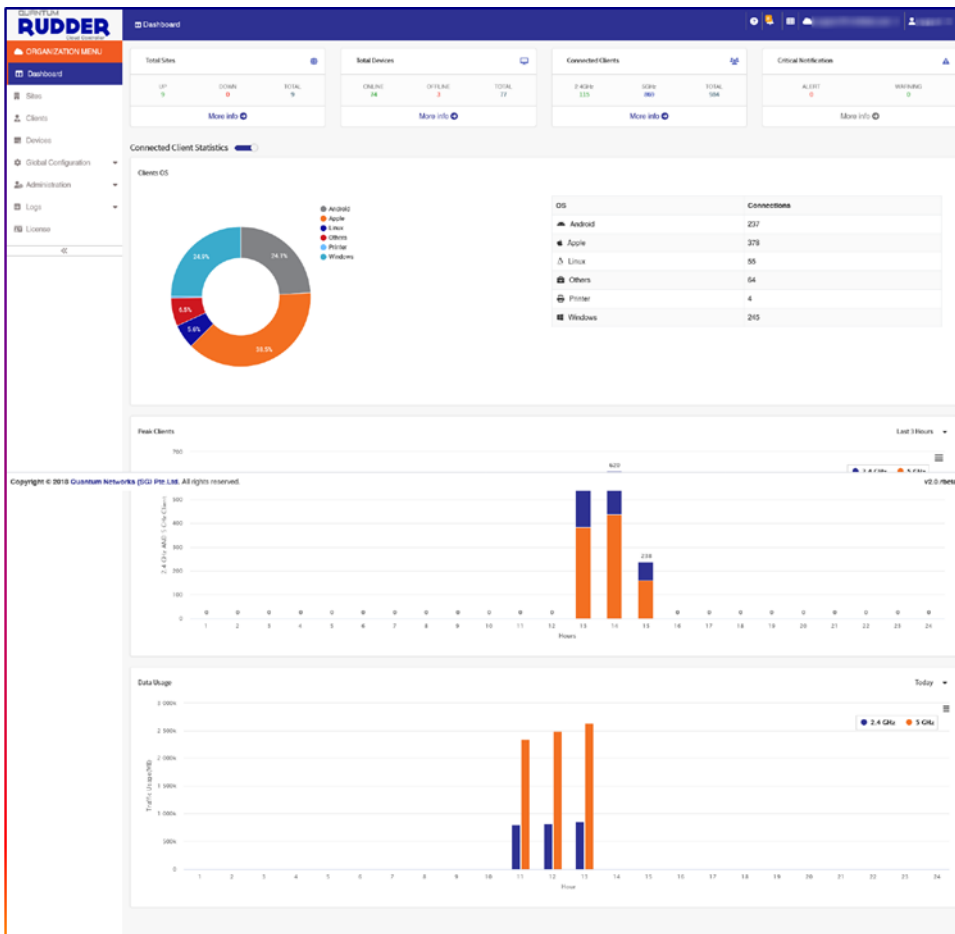


Figure 3

About Web Interface

Side panel and Main Screen

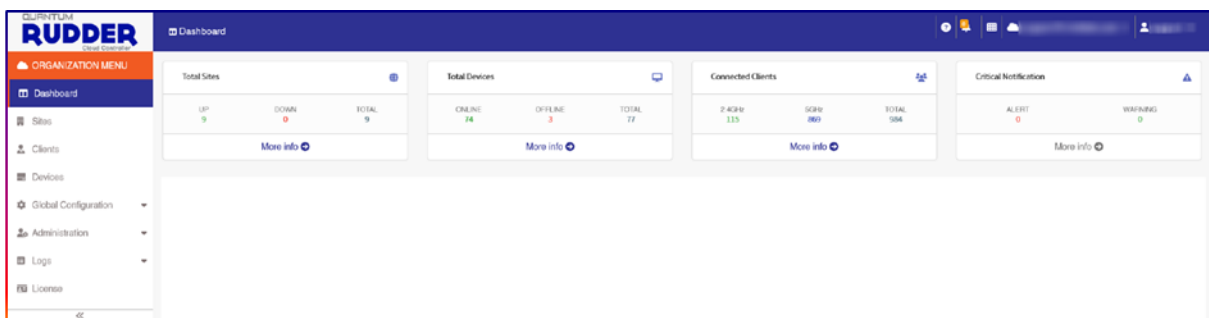


Figure 4

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 and Create a new configuration.
Main Screen	Selected parameter options, where admin can work.

Top Panel

The top panel provides “Critical Alerts”, “Edit Current Cloud” and manage “Cloud Admin” features as described below.

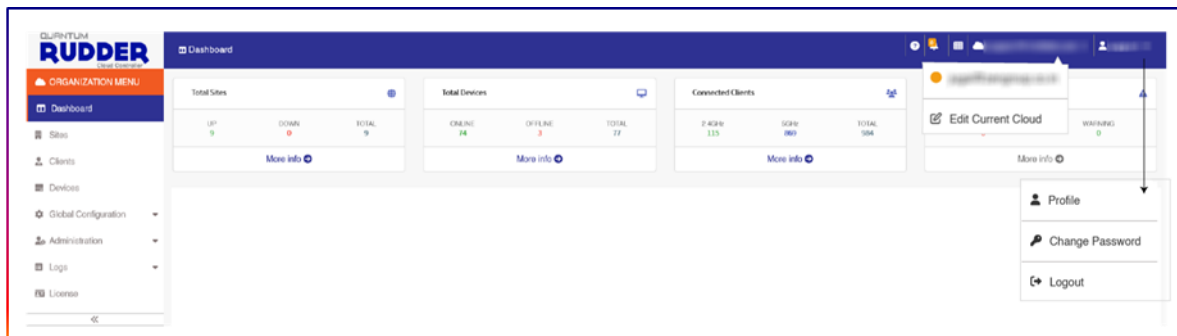







Figure 5

Top Panel – Icon	Description
	Help: To access documentation
	Critical Alerts: Critical Alerts like Device Reboot, High CPU Utilization, High Memory Utilization and Exceeded Maximum Connected Clients.
	Will provide direct Access: Quantum Rudder / Quantum UnGrid / QIM (Identity Management)
	Edit Current Cloud: To edit the current cloud click the "Cloud" icon and select "Edit Current Cloud". Modify as required.
	Cloud Admin Detail: This option allows the admin user to view or edit existing details.
	Change Password: The option allows to change the admin password.

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 new site or any other related parameters.
	Clear Log : clear all logs till date.

Cloud Menu

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.

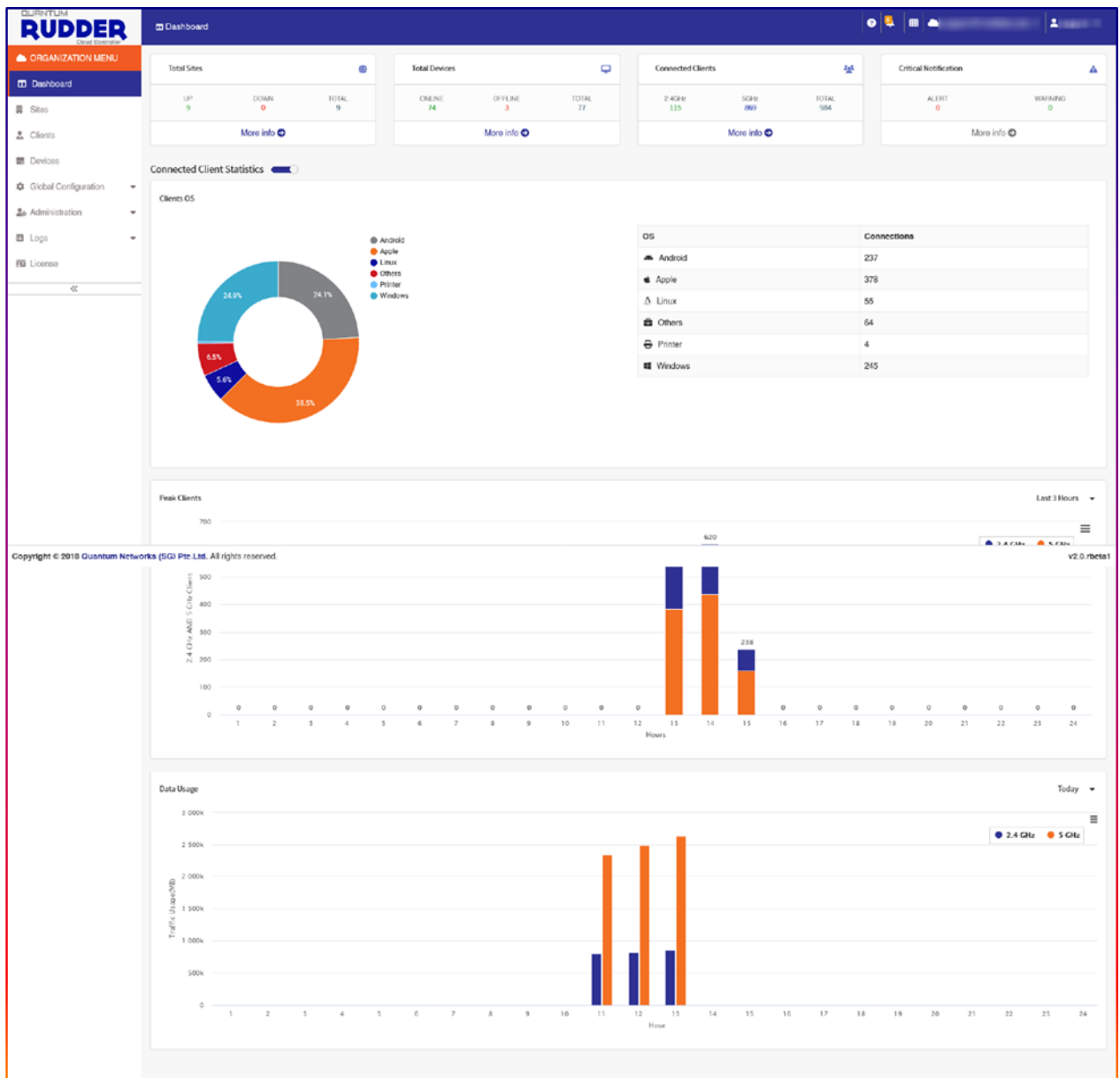


Figure 6

Total Sites:

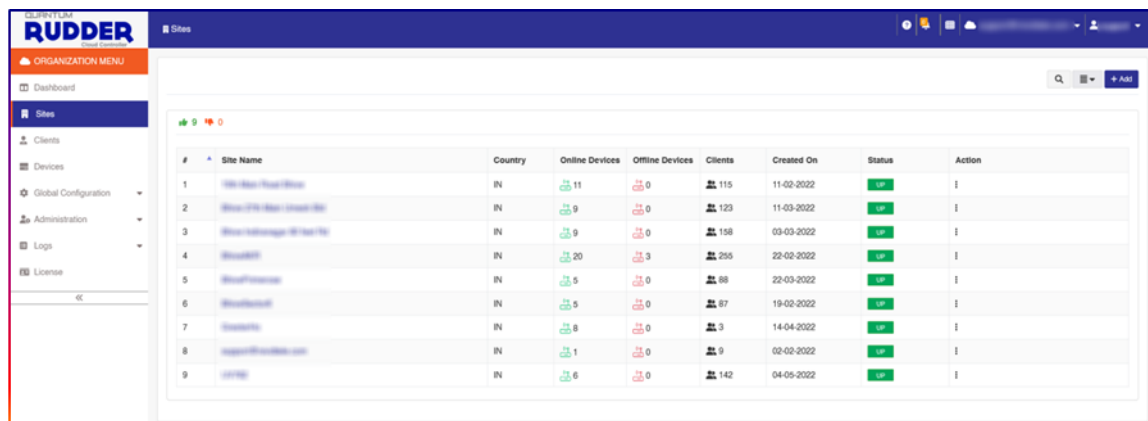
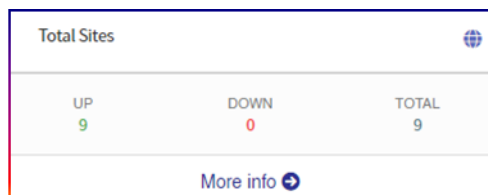


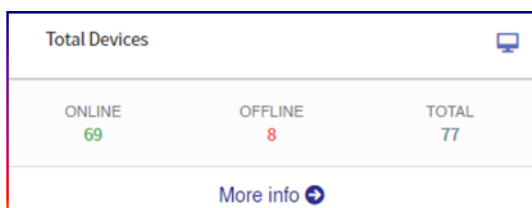
Figure 7

Total Site	
Up	Total number of sites that are Up. Site status will be "UP" even if no device is registered or Provisioned.
Down	Total number of Down sites. Site "Down" if the devices are unable to communicate with Quantum RUDDER.
Total	Number of sites created on Quantum RUDDER.
More Info	Detailed information.

Total Site – More info	
Site Name	Name of site
Country	Site location
Online Devices	Total number of Online devices on the site
Offline Devices	Total number of Offline devices on the site
Clients	The number of connected clients on the site

Created On	Site creation date
Status	The site status (Up or Down)
Action	Admin can edit or delete the site

Total Device:



#	Device	Device type	AP MAC	Sr No.	Name	Local IP	Model No.	Public IP	Device Uptime	Clients	2.4 CH	5 CH	Location	Connection Status
1		AP	88:87:23:23:23:23	1234567890	QN_0083 F5	192.168.9.207	QN-I-220	106.51.91.135	5D6h:33min	26	A-6	A-36	-	ONLINE
2		AP	88:87:23:23:23:23	1234567890	QN_0084-193F	192.168.8.62	QN-I-220	106.51.91.135	5D6h:33min	19	A-6	A-36	-	ONLINE
3		AP	88:87:23:23:23:23	1234567890	QN_008C DD	192.168.11.66	QN-I-220	106.51.91.135	5D6h:33min	11	A-1	A-161	-	ONLINE
4		AP	88:87:23:23:23:23	1234567890	QN_008C FB	192.168.11.96	QN-I-220	106.51.91.135	5D6h:32min	26	A-11	A-149	-	ONLINE
5		AP	88:87:23:23:23:23	1234567890	QN_00AE2D	192.168.10.64	QN-I-220	106.51.91.135	5D6h:32min	21	A-1	A-36	-	ONLINE
6		AP	88:87:23:23:23:23	1234567890	QN_00AE48	192.168.10.91	QN-I-220	106.51.91.135	5D6h:32min	23	A-1	A-48	-	ONLINE
7		AP	88:87:23:23:23:23	1234567890	QN_00B0-733F	192.168.9.28	QN-I-220	106.51.91.135	5D6h:32min	12	A-11	A-48	-	ONLINE
8		AP	88:87:23:23:23:23	1234567890	QN_00B0 B5	192.168.9.94	QN-I-220	106.51.91.135	5D6h:33min	18	A-6	A-149	-	ONLINE
9		GWY	88:87:23:23:23:23	1234567890	QN-009810	106.51.91.135	QN-S-100	106.51.91.135	5D5h:24min	-	-	-	-	ONLINE

Figure 8

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 devices connected
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 device
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	Public IP on which the Access Point is running
Device Uptime	Will show how long the AP has been up since it has been powered up or restarted
Clients	The number of connected clients on the device
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 location of the Access Point
Connection Status	Current status of the device (Online / Offline?)

Connected Clients:

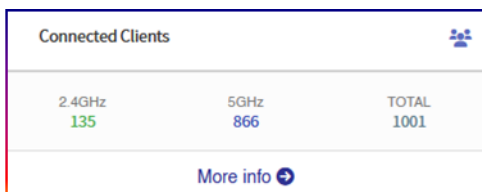


Figure 9

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
Action	Administrator can freeze, block the Internet access or disconnect the user

Critical Alert:

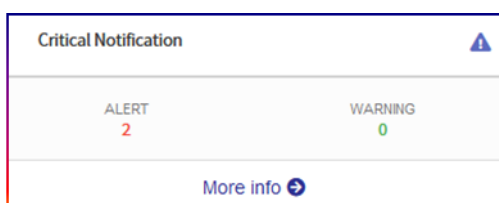


Figure 10

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: Administrator can view graphical analytics for Active Clients among the cloud like their connected device OS, Clients trend, Traffic usage.

Sites

Create a **New Site**

Go to **Site**, click **Add** to create new site.

Site Name

Description

Regulatory Country: India

Address Line 1

Address Line 2

City

State/Province/Region

ZIP Code

Latitude

Longitude

DEVICE LOGIN DETAILS

Device Username

Device Password

GENERAL SETTINGS

Do you want to clone site?

Site List: select

Submit Back

Figure 11

New Site detail

Site Name	Site name
Description	Details for reference
Regulatory Country	Select Regulatory Country
Address Line 1	Site address
Address Line 2	Site address
City	City
State/Province/Region	Region
ZIP Code	Location ZIP code
Latitude	Location latitude
Longitude	Location longitude

Device Login Detail

Device Username	Device username
Device Password	Device password

General Settings

Do you want to clone the site?	The enabled option will provide permission to clone configuration from other sites to this site.
Site List	Displays the pre-configured sites list.

Site Dashboard

The Site dashboard provides summarized information about the selected site.

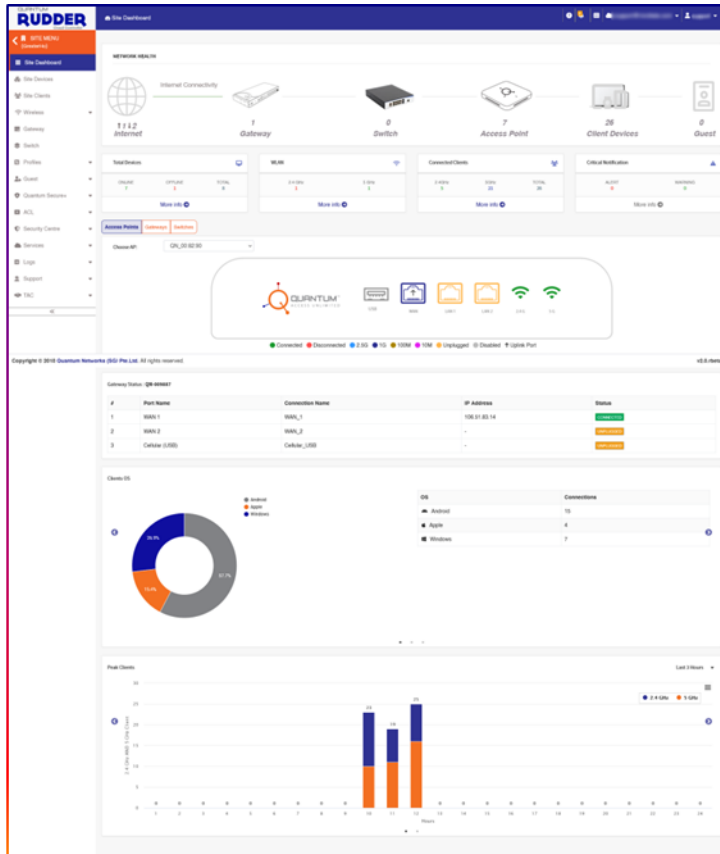


Figure 12

Parameter	Description
Network Health	The option will display the overall site internet connectivity status. In router mode, it will display which port is active as WAN and its status. It will display the current active WAN port status whether it is primary or secondary.
Internet Health	The enabled parameter shows upload and downloads internet bandwidth available in Access Point at the selected period of time.
Total Devices	This option provides existing AP status i.e. how many Access Points are Online, Offline, or Provisioned on that 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 Critical Notification.

Critical Notification	Critical alerts like Device Reboot, High CPU, and Memory Utilization. Maximum limit of connected clients, if any.
Access Points / Gateway /Switches	Displays the number of Access Points connected to the system.
Gateway Status	Displays the status of the connected Gateway devices on the system.
Clients OS	Displays the client list with their respective OS.
Peak Clients	Displays a graph presentation of clients joining the network against the time they connect to the network, along with the frequencies they bind.

Note: Click “More Info” for further details.

Site Devices

This option provides details of all provisioned Access Points with current status Online, Offline, and Provisioned, along with connected clients.

The screenshot shows the 'Site Devices' page in the RUDDER interface. It features a sidebar menu on the left with options like Site Dashboard, Site Clients, Wireless, Gateway, Switch, Profiles, Guest, Quantum Secure+, ACL, Security Centre, Services, Logs, Support, and TAC. The main content area displays a table of devices with the following columns: #, Device, Device type, AP MAC, Sr No., Name, Local IP, Model No., Public IP, Device Uptime, Clients, 2.4 CH, 5 CH, Location, and Connection Status. The table lists 8 devices, including 7 Access Points (AP) and 1 Gateway (GWY). The APs are mostly in an 'ONLINE' state, while one (QN_00.AC7A) is 'OFFLINE'. The GWY (QN-S-100) is also 'ONLINE'.

#	Device	Device type	AP MAC	Sr No.	Name	Local IP	Model No.	Public IP	Device Uptime	Clients	2.4 CH	5 CH	Location	Connection Status
1		AP			QN_00.82.90	192.168.10.31	QN-1220	106.51.83.14	2D5h:59min	1	A-1	A-36	-	ONLINE
2		AP			QN_00.82.D2	192.168.10.97	QN-1220	106.51.83.14	2D2h:57min	1	A-6	A-157	-	ONLINE
3		AP			QN_00.87.E5	192.168.10.223	QN-1220	106.51.83.14	2D5h:58min	24	A-6	A-36	-	ONLINE
4		AP			QN_00.8A.5E	192.168.8.57	QN-1220	106.51.83.14	2D5h:58min	1	A-1	A-161	-	ONLINE
5		AP			QN_00.8D.F1	192.168.10.161	QN-1220	106.51.83.14	2D5h:59min	0	A-11	A-36	-	ONLINE
6		AP			QN_00.AC7A	-	QN-1220	-	-	-	-	-	-	OFFLINE
7		AP			QN_00.AD.1C	192.168.10.228	QN-1220	106.51.83.14	2D5h:59min	0	A-1	A-36	-	ONLINE
8		GWY			QN-009887	106.51.83.14	QN-S-100	106.51.83.14	2D6h:	-	-	-	-	ONLINE

Figure 13

Site Clients

This option provides details of all users/guest devices connected across the selected site.

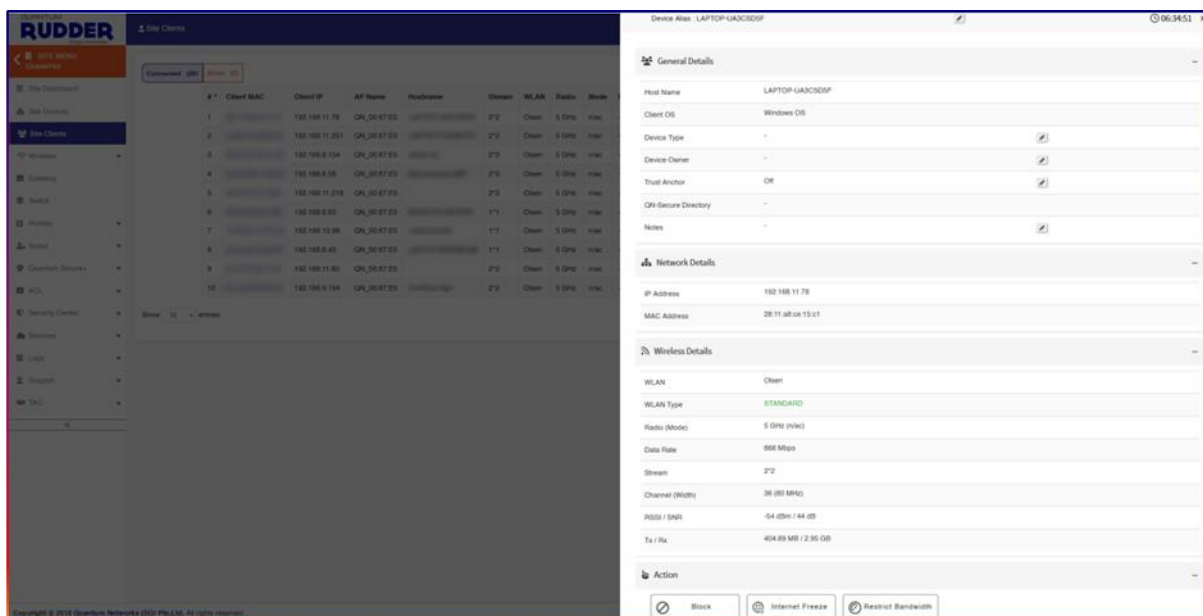


Figure 14

Note: By clicking "Client Mac", the Administrator can Block a particular client MAC, Freeze the internet or put restrictions on bandwidth with the Action option.

Wireless

WLAN

Wireless networks available on the site can be added, edited or deleted from here.

To add a new Wireless Local Area Network (WLAN)

Go to **Cloud Menu > Site > Select Site > Configuration > Wireless > Add**

General Settings

The screenshot shows the 'GENERAL SETTING' form for adding a new WLAN. It includes input fields for 'WLAN Name', 'SSID', and 'SSID Description'. There are toggle switches for 'Enable SSID', 'Broadcast SSID', and 'Client Isolation'. The 'Radio' section has two radio buttons for '2.4 GHz' and '5 GHz', with the '5 GHz' option selected.

Figure 15.1

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

Method

METHOD

Access Type: Standard

Authentication Method: Open

Figure 15.2

Method	Default Value
Access Type : Standard	Access Type : Standard Auth. Method : Open
Authentication Method : Open or 802.1x EAP	
Access Type : Hotspot (WISPr) (Refer Note 1)	
Authentication Method : Open or 802.1x EAP	
Authentication Profile: Select Authentication Profile from the dropdown list which is to be associated with this Wireless Local Area Network.	
Hotspot Profile: Select Hotspot Profile from the dropdown list which is to be	

associated with this Wireless Local Area Network.	
Access Type : Guest access (Refer Note 1)	
Authentication Method : Choose the authentication method "open" or "802.1xEAP"	
Guest panel Profile: Choose Hotspot Profile, which is to be associated with this Wireless Local Area Network.	

Note 1: For Access Type

Hotspot (WISPr) : Before configuring Access Type as Hotspot (WISPr), create Authentication Profile and Hotspot Profile.

To create Authentication Profile, go to

Site > Configuration > Authentication > Add

To create Hotspot Profile, go to

Site > Configuration > Hotspot > Add

Guest Access: To select Access Type as Guest Access, create Splash Portal Profile and Guest Policy Profile.

To create Splash Portal Profile, go to

Site > Configuration > Guest > Splash Portal

To create Guest Policy Profile, go to

Site > Configuration > Guest > Guest Profile

Authentication method - Allows mixed networks of WPA and WPA2 compliant devices. You can use this if your network has a mixture of old devices that only support WPA TKIP and new devices that support WPA2 and AES.

Terms Detail Description

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

Terms Detail Description

Algorithm	This algorithm provides enhanced security over TKIP, and is the only encryption algorithm supported by the 802.11i standard.
	TKIP: TKIP is a stopgap encryption protocol introduced with WPA to replace the very-insecure WEP encryption at the time.
Encryption Method	WPA2: WPA encryptions that comply with the 802.11i security standard,
	None: No encryption; communications are sent in clear text.
	WPA-Mixed: Allows mixed networks of WPA and WPA2 compliant devices. You can use this if your network has a mixture of older clients that only support WPA and TKIP, and newer client devices that support WPA2 and AES.

Security Settings

The screenshot shows a configuration window titled "SECURITYSETTING". It contains three input fields: "Encryption Method" with a dropdown menu showing "WPA2", "Algorithm" with a dropdown menu showing "AES", and "Key" with a text input field and a small eye icon to the right.

Figure 15.3

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

Network Setting

NETWORK SETTINGS

Routing Option: Bridge To WAN

VLAN: 1

Figure 15.4

Parameter	Description	Default Value
Routing Option	Use this option to select the routing option as "Bridge To WAN" or "NAT To WAN". By default, it is "Bridge To WAN". If AP is a Master AP, select "NAT To WAN". To make Access Point as Master Access Point, Go to Site > Configuration > Network > Gateway > Enable WAN Profile	Bridge To WAN
VLAN	Each Wireless Interface (SSIDs) can be configured with a specific VLAN ID (1-4094). Enter a valid VLAN ID assigned to the clients on this WLAN (1-4094).	1

Advance Settings

ADVANCE WIRELESS SETTINGS

Roaming

- 802.11r:
- 802.11k:
- 802.11v:
- Threshold Roaming:

Beacon Elements

- 802.11d:
- DTIM Interval:
- U-APSD:
- Inactivity Timeout: None minutes

Traffic Shaping

- CoS:

Radio Control

- Disable Band Balancing:
- Max Clients: 50 Per Radio

Wireless Security

- 802.11w MFP:
- OFDM Only (Disables 802.11b):
- BSS Min Rate: Default
- Mgmt Tx Rate: 6 mbps
- Proxy ARP:

Access Control List

- Layer 2 ACL:
- Layer 3 ACL:

Traffic Monitoring

- URL Filtering:
- App Policing:

Client Restrictions

- Scheduling Profile:
- Internet Freeze:
- OS Policy:
- Rate Limit:

Figure 15.5

Parameter	Description	Default Value
Roaming:		
802.11r	When a device roams from one AP to another on the same network, 802.11r uses Fast Basic Service Set Transition (FT) to authenticate supported devices more	Disabled

	quickly.	
802.11k	Supported devices can search quickly for nearby available APs as roaming targets by creating an optimized list of channels. When the signal strength of the current AP weakens, the device will scan for target APs from this list.	Enabled
802.11v	Allows client devices to exchange information about the network topology, including information about the RF environment, making each client network-aware, facilitating overall improvement of the wireless network.	Enabled
Threshold Roaming	This ensures the best possible performance at all times.	Disabled
Beacon Elements:		
802.11d	Allow the radio to show its Country Information.	Disabled
DTIM Interval	The DTIM interval indicates the DTIM period in beacons. With default value 1, the client checks for buffered data on the AP at every beacon.	1
U-APSD	U-APSD / WMM Power Save is a power saving mechanism of the IEEE 802.11e amendment for QoS.	Enabled
Inactivity Timeout	The users to miss out on any activities for a certain amount of time will be disconnected automatically.	None
Traffic Shaping:		
QoS	Enable this option to create guest pass policy like pass validity, effective period as well as expiry period under Cloud Menu > Site > Click on created site/select the required site > Guest > Guest Policy.	Disabled
Radio Control:		
Disable Band Balancing	Disabling Band Balancing will allow the AP to connect a new client automatically without any band preferences.	
Max Clients	Allows limiting the maximum number of clients per radio.	
Wireless Security:		
802.11w MFP	IEEE 802.11w standard, known as Management Frame Protection. The Management Frame Protection increases the security by providing data confidentiality of management frames	Disabled
OFDM Only (Disables 802.11b)	Old (legacy) 802.11b wireless devices impact the performance of any Wi-Fi network on the 2.4 GHz band. When enabled, 802.11b legacy device cannot be associated with your SSID.	Disabled
BSS Min Rate	Users will be able to get connected at the minimum rate speed.	
Mgmt Tx Rate	The user will transfer the data frame at a certain speed in the SSID.	
Proxy ARP	Proxy ARP is a technique by which a proxy device on a given network answers the ARP queries for an IP address that is not on that network. The proxy is aware of the location of the traffic's destination and offers its own MAC address as the	Disabled

	destination.	
Access Control List :		
Layer 2 ACL	Enabling Layer 2 ACL will Allow/Deny users with particular MAC addresses to connect to the system.	
Layer 3 ACL	Enabling Layer 3 ACL will allow the users to access only particular Websites and URLs. Access to other Websites and URLs will be blocked.	
Traffic Monitoring		
URL Filtering	It will block all the URLs that were added to the list while creating the profile.	
App Policing	It will block Applications that were added to the list while creating the profile.	
Client Restrictions		
Scheduling Profile	Control which hours of the day or days of the week to enable/disable WLAN service.	Disabled
Internet Freeze	If enabled, clients will not be able to access the Internet through this Wireless network.	Disabled
OS Policy	Allow or Deny wireless clients based on specific OS / Device type. Either OS Policy or Access Control List can be enabled at a time.	Disabled
Rate Limit	Limit the rate or speed of download and upload requests of the clients.	Disabled

DHCP Settings

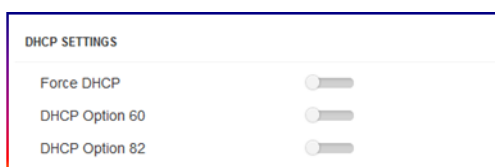


Figure 15.6

Parameter	Description	Default Value
Force DHCP	Enable this option to force clients to obtain a valid IP address from DHCP within the specified number of seconds.	Disabled
DHCP Option 60	Configuring DHCP option 60 helps in identifying the incoming DHCP client. If the vendor class identifier (VCI) advertised by the DHCP client matches with the DHCP server, the server decides to exchange the vendor-specific information (VSI) configured as part of the DHCP option 43.	Disabled
DHCP Option 82	DHCP relay agent information, also known as DHCP option 82, enables a DHCP relay agent to insert information about a client's identity into a DHCP client request sent to a DHCP server. This option can be used to assist DHCP servers to	Disabled

	implement a dynamic address policy.	
--	-------------------------------------	--

Access Point

Independent AP configuration

Go to **Cloud Menu > Site > Select Site > Wireless > Access Point**

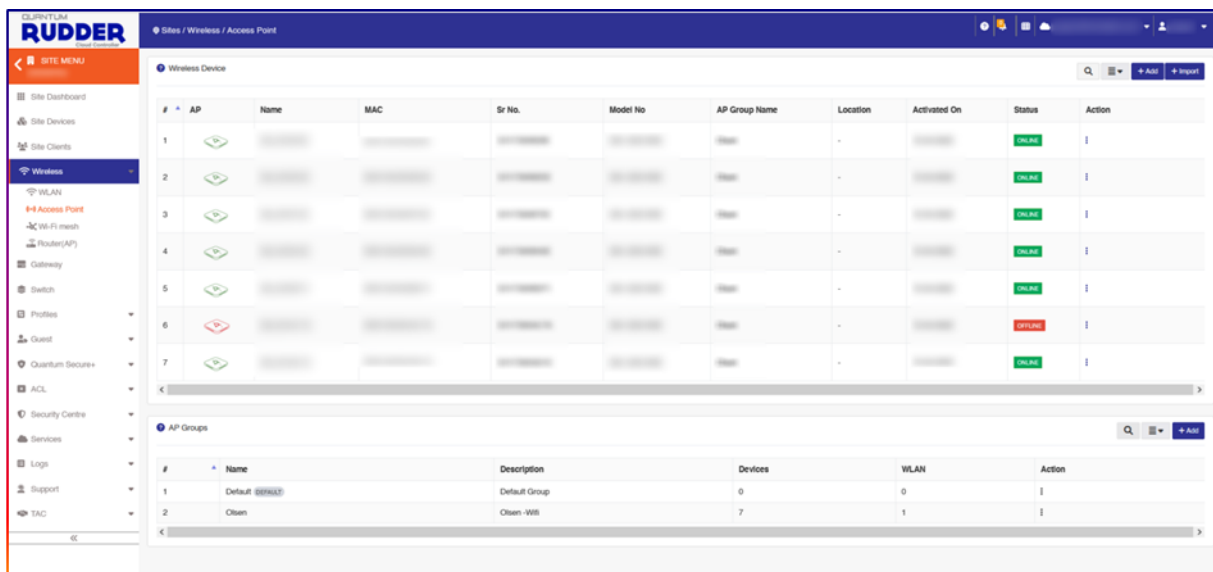


Figure 16

Top Panel Options	Description
Search	Search available Access Points by their MAC or Serial number or AP group name.
Export	The administrator can export wireless device detail in pdf or CSV.
Add	Option to add Pre-provisioning AP manually.
Import	The administrator can import Pre-provisioning AP CSV files and upload them. (Sample CSV file format, admin can download with "Sample File" option).

Wireless Device	Description
Name	Access Point name.
MAC	MAC address of the Access Point.

Sr.No	Serial Number of the Access Point.
Model No	Device model number.
AP Group Name	Access Point group name under which AP is laying.
Location	Device location detail.
Activated On	Device activation date.
Status	Current status of Access Point (Device).
Action	Add: Admin can edit the Access Point detail. Delete: Admin can delete the Access Point. Reboot: Admin can reboot the individual Access Point. AP Transfer: Admin can transfer the AP to another group.

Click on desired AP for basic configuration settings.

General Setting

General Setting

Name

Location

GPS Coordinates ,

Enable LED Status AP Group settings On Off

Parameter	Description	Default Value
Name	Access Point name	
Location	Location detail	
GPS Coordinates	Location Latitude and Longitude	
Enable LED Status	AP Group settings:	On
	On: Indicates the LED light.	
	Off: Turns LED light indication off.	

Figure 17.1

WAN Configuration

Figure 17.2

IP Address Setting	
Select Port	Select Access Point port which needs to be configured.
IP Schema Type	Static: Assign IP address with Subnet, Gateway and DNS details.
Use this option to define IP schema as Static / DHCP / or Keep AP setting	DHCP: Device will acquire IP from DHCP server.
	Keep AP setting: Select this option to continue with current configuration.

Radio Configuration

Figure 17.3

Enable this option to set Radio parameters in the Access Point locally. In Disable mode, configurations will take place as set in Access Point Group settings.

Parameter	Description	Default Value
-----------	-------------	---------------

Override AP Group Radio Configuration	Enable to override the Radio configuration of AP Group and configure Radios locally in the Access Point.	Disabled
Wireless 2.4 GHz	2.4 GHz Radio: Enable / Disable	Disabled
	Channel Bandwidth: Select channel bandwidth from the dropdown list. It can be 20/40 MHz or 20 MHz.	
	Change Range: Choose Auto or select required channel from the dropdown list.	
	Max Tx Power: Choose Auto or select specific level of transmit power from the dropdown list.	
Wireless 5 GHz	5 GHz Radio: Enable / Disable as per the requirement.	Disabled
	Channel Bandwidth: Select channel bandwidth from the dropdown list. It can be 20/40/80MHz or 20/40 MHz or 20 MHz.	
	Change Range Indoor: Choose Auto or select required channel from the dropdown list.	
	Change Range Outdoor: Choose Auto or select required channel from the dropdown list.	
	Max Tx Power: Choose Auto or select specific level of transmit power from the dropdown list.	

Port Configuration

#	Port	Action	Type	VLAN
1	eth0	<input checked="" type="checkbox"/>	Access Port	Untag ID 1 Members 1,2,3,...,405
2	eth1	<input checked="" type="checkbox"/>	Trunk Port	Untag ID 11 Members 1,2,3,...,405
3	eth2	<input checked="" type="checkbox"/>	Trunk Port	Untag ID 11 Members 1,2,3,...,405

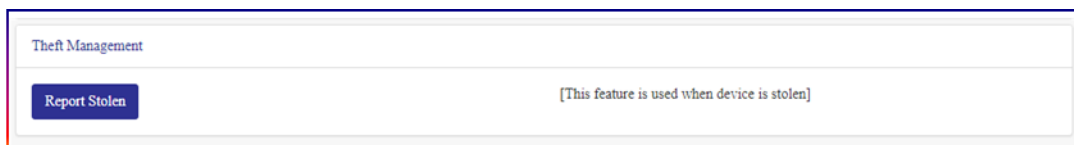
Figure17. 4

This option is used to configure the Virtual-LAN (VLAN) parameters on the Ethernet ports of the AP.

Parameter	Description	Default Value
Type	Port Type:	Port : Enabled

	<p>Trunk Port: Allow multiple VLAN (1~4094); PVID (untagged VLAN ID) configurable.</p> <p>Access Port: A single VLAN, packets untagged.</p>	Type : Trunk Port VLAN : Untag ID : 1
VLAN	Assign Untagged VLAN ID handled on the port.	
Members	In the case of a Trunk port, assign Member VLAN IDs with reference to the respective port with a comma. Can manage multiple VLAN IDs.	

Theft Management



“Report Stolen” - If the device is stolen.



Figure 17.5

Click on “Report Recovery” – When the user recovers the device back at their end, they can click on the Report Recovery option for the recovered device.

Maintenance

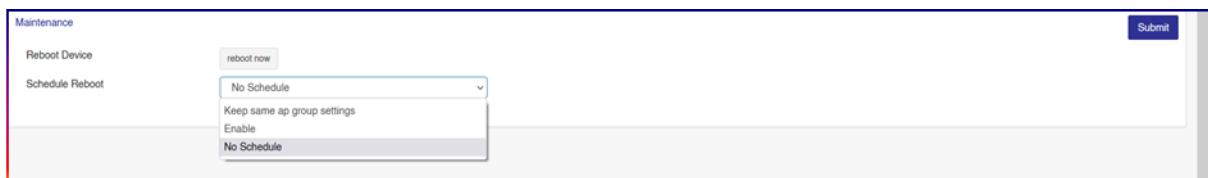


Figure17. 6

Enabling this feature allows the users to automatically reboot the device at a certain schedule in order to avoid any possible harm to the device.

AP Group configuration

AP group configuration is used to make changes to the Access Points separately and differentiate between multiple Access Points on the same network without having to make changes to the other ones.

To create an Access Point Group follow below procedure.

Go to **Cloud Menu > Site > Select Site > Wireless > Access Point > AP group > Add**

The screenshot displays the 'Access Point' configuration page in the RUDDER interface. The left sidebar shows the navigation menu with 'Wireless' selected. The main content area is titled 'Sites / Wireless / Access Point' and contains the following sections:

- GENERAL:** Fields for Name, Description, and Regulatory Country (set to India).
- WIRELESS 2.4 GHz:** Status toggle (on), Channel Bandwidth (20 MHz), Channel Range (Auto), and Max Tx Power (Auto).
- WIRELESS 5 GHz:** Status toggle (on), Channel Bandwidth (Auto), Channel Range Indoor (Auto), Channel Range Outdoor (Auto), and Max Tx Power (Auto).
- MEMBER WLAN:** A table listing WLANs and their associated radios.
- MEMBER DEVICE:** A section with a button to 'Add devices to mark as a group member'.
- ADVANCE SETTING:** Includes Channel Management (Speedychannel and Channelswitch), Band Management (Enabled Band Steering, Band Steering Mode, and Band Balancing), and Device Management (LED Status, Schedule Reboot, and Reboot).

#	WLAN Name	Radio
<input type="checkbox"/>	WLAN1	2.4.5
<input type="checkbox"/>	WLAN2	2.4.5
<input type="checkbox"/>	WLAN3	2.4.5
<input type="checkbox"/>	WLAN4	2.4.5
<input type="checkbox"/>	WLAN5	2.4.5

Figure 18

General

Figure 18.1

Parameter	Description	Default Value
General Setting	<p>Name: Name of Access Point Group</p> <p>Description: Edit description for reference.</p>	
Wireless 2.4 GHz	<p>Channel Bandwidth: Choose channel bandwidth from the dropdown. It can be Auto / Auto (40/20 MHz) or Auto (20 MHz).</p>	Auto
	<p>Channel Range: Choose Auto or select manual required channel from the dropdown.</p>	Auto
	<p>Max Tx Power: Choose auto or select a specific level to transmit power from the dropdown.</p>	Auto
Wireless 5 GHz	<p>Channel Bandwidth: Choose channel bandwidth from the dropdown. It can be Auto / Auto (40/20/80/160 MHz) or Auto (20 MHz).</p>	Auto
	<p>Channel Range (Indoor/Outdoor): Choose Auto or select the manual required channel from the dropdown.</p>	Auto
	<p>Max Tx Power: Choose auto or select a specific level of transmit power from the dropdown.</p>	Auto
Member WLAN		
WLAN	<p>WLAN: All created WLANs will be the members of a default Access Point group. All these WLANs will be list out in a new group as well. Choose the required WLAN needed to be active as a member of respective group.</p>	
Member Device	Displays the member devices.	

Advance Setting

The screenshot displays the 'Advance Setting' configuration page, divided into three main sections:

- Channel Management:**
 - Speedychannel (Dynamic channel Selection): Enabled (toggle)
 - Channelswitch (Automatic Channel Switch): Enabled (toggle)
 - Scan Interval: 1 (dropdown menu)
- Band Management:**
 - Enabled Band Steering: Enabled (toggle)
 - Band Steering Mode: Prefer 5 GHz (dropdown menu)
 - Band Balancing: Disabled (toggle)
- Device Management:**
 - LED Status: Enabled (toggle)
 - Schedule Reboot: Enabled (toggle)
 - Scheduling Profile: Select (dropdown menu)
 - Reboot: Reboot Now (button)

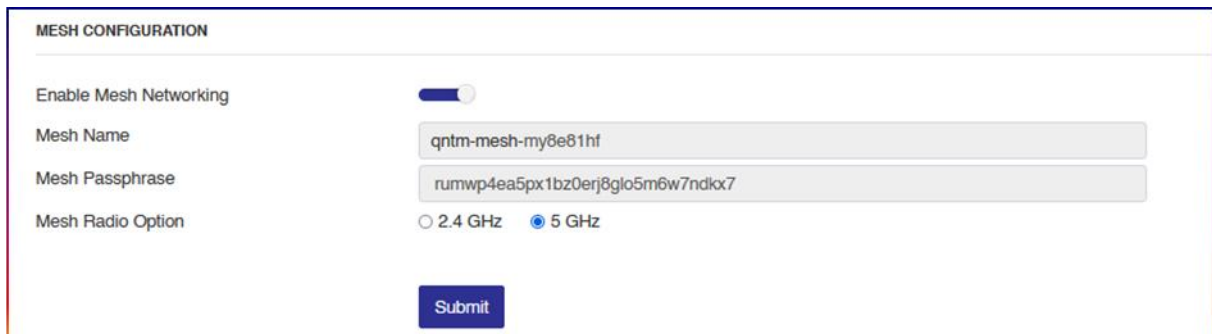
At the bottom, there are 'Submit' and 'Back' buttons.

Figure 18.2

Parameter	Description	Default Value
Channel Management		
Speedy channel (Dynamic channel Selection)	When Enabled, it will frequently scan over the air interference and allocate the most reliable channel to AP for the best performance.	Disabled
Channel switch (Automatic Channel Switch)	When Enabled, Quantum AP will scan over the air interference every day at a scheduled time and allocate the most reliable channel to AP for the best performance.	Disabled
Scan Interval	Allows choosing the desired time interval to scan channels.	
Band Management		
Enabled Band Steering	Allows choosing a preferred bandwidth.	
Band Steering Mode	Allows choosing between the preferred 5 GHz bandwidth or to choose moderately.	Enabled
Band Balancing	Balances the clients based on the specified % ratio load by distributing clients between 2.4 GHz and 5 GHz radios.	
Device Management		
LED Status	Allows blinking the LED indicator.	Disabled
Schedule Reboot	Allows Rebooting AP at a particular time.	Disabled
Scheduling Profile	Enabling Schedule Profile will allow choosing the Scheduled Profile to bind.	
Reboot	Manually Reboots the AP.	

Wi-Fi Mesh

Mesh routers allows the users to have greater coverage with faster speeds and more reliable connection in the network. Mesh Wi-Fi systems provide multiple access points broadcast in the same network.



The screenshot shows a web interface titled "MESH CONFIGURATION". It contains the following elements:

- Enable Mesh Networking:** A toggle switch that is currently turned on (blue).
- Mesh Name:** A text input field containing the value "qntm-mesh-my8e81hf".
- Mesh Passphrase:** A text input field containing the value "rumwp4ea5px1bz0erj8glo5m6w7ndkx7".
- Mesh Radio Option:** Two radio buttons. The "2.4 GHz" option is unselected, and the "5 GHz" option is selected (indicated by a blue dot).
- Submit:** A blue button located at the bottom center of the configuration area.

Figure 19

Parameter	Description	Default Value
Mesh Configuration		
Enable Mesh Networking	Enable by clicking the toggle button.	Disabled
Mesh Name	Name of the Mesh network.	
Mesh Passphrase	!!..TO BE LOOKED UPON..!!	
Mesh Radio Option	Select the Radio frequency.	

Router (AP)

Figure 20

Parameter	Description	Default Value
Router Profile Settings		
Router Profile	Enable by clicking on the toggle button.	Disabled
Router AP	Select the AP from the list.	
WAN Port	Select a WAN Port from the list.	eth0
IP Schema	Select the IP Schema from the list.	Keep AP Setting
Enabled Secondary WAN	Enable Secondary WAN by clicking on the toggle button.	Disabled
WAN Port	Select a WAN Port from the list.	eth0
IP Schema	Select the IP Schema from the list.	Keep AP Setting

Gateway

Figure 21

Parameter	Description
Name	Displays name of the device.
Sr. No	Displays serial Number of the device.
MAC	Displays MAC address of the device.
Model No	Displays Model number of the device.
IP Address	Displays IP Address of the device.

Activation Date	Displays the date of activation of the device.
Status	Displays the status of the device. ONLINE/OFFLINE
Action	Reboot: Reboots the device. View: Displays the details of the Gateway device. Delete: Removes the device from the network.

Switch

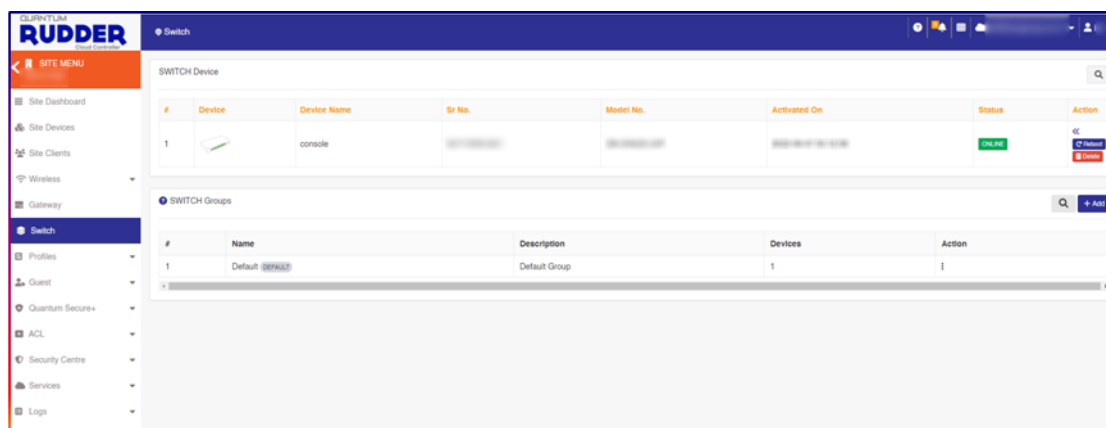


Figure 22

Parameter	Description
Device	Displays the model of the device.
Device Name	Displays the name of the device.
Sr. No	Displays serial number of the device.
Model No	Displays model number of the device.
Activated On	Displays the date of activation of the device.
Status	Displays the status of the device. ONLINE/OFFLINE
Action	Reboot: Reboots the device Delete: Removes the device from the network.

Profiles

Hotspot

To create an External Guest Portal Server for Guest authentication -

Go to **Cloud Menu > Site > Select Site > Profiles > Hotspot > Add**

The screenshot shows a web form titled "HOTSPOT PROFILE" with several sections: "HOTSPOT PROFILE" (Name, Description), "CAPTIVE PORTAL" (Portal URL, Portal Secret, Confirm Portal Secret), "USER SESSION" (Session Timeout, Ideal Timeout), "NETWORK SETTINGS" (DNS Domain, NAS ID), and "WALLED GARDEN" (Exception URL, Mac White List). The form includes "Submit" and "Back" buttons at the bottom.

Figure 23

Hotspot	Parameter	Description
Hotspot Profile	Name	Name of Hotspot profile.
	Description	Detail for reference.
Captive Portal	Portal URL	Captive portal (splash page) redirection URL.
	Portal Secret	Portal secret.
	Confirm Portal Secret	Portal secret to confirm.
User Session	Session Timeout	Assign a time limit to which the user will get disconnected and be required to log in again.
	Ideal Timeout	It's a period of inactivity from user. When there is no traffic from the user, once the timeout is reached, user will be disconnected from the Hotspot

Network Settings	DNS Domain	Use this option for the Domain name for the Hotspot.
	NAS ID	Enter the Network Access Server identifier of this device. The NAS-ID parameter is sent in RADIUS access and accounting request messages.
Walled Garden	Exception URL	Use this option to allow domains to be accessed by the users without Authentication. Clients accessing these domains will not be redirected to the splash page.
	Enable MAC White List	Selected list devices will be whitelisted and allow getting access without authentication. To configure MAC White List, Go to Cloud Menu > Site > Select required site > ACL > Mac Whitelist

Authentication

To create an Authentication profile, go to **Cloud Menu > Site > Select Site > Profiles > Authentication > Add**

The screenshot shows a web interface for configuring an authentication profile. The breadcrumb path is 'Sites / Profiles / Authentication'. The form has three main sections: 'Name' with a text input field, 'Description' with a text input field, and 'Authentication Method' with a dropdown menu. The dropdown menu is currently open, displaying the following options: 'Select', 'Select' (highlighted), 'AAA', 'Active Directory', 'LDAP', and 'Custom API'.

Figure 24

Parameter	Description
Name	Name of Authentication profile
Description	Detail for reference
Authentication Method	AAA., Active Directory, LDAP, Custom API

AAA

Select AAA to configure External Guest Portal for Guest authentication.

The screenshot shows a configuration page titled 'Sites / Profiles / Authentication'. It contains several input fields and a dropdown menu. The 'Authentication Method' dropdown is set to 'AAA'. Below this, there are two sections: 'AUTHENTICATION SERVER' and 'ACCOUNTING SERVER'. Each section has five input fields: 'Server IP Address', 'Secondary Server IP Address', 'Authentication Port', 'Shared Secret', and 'Confirm Shared Secret'. The 'Shared Secret' and 'Confirm Shared Secret' fields have eye icons to toggle visibility. At the bottom, there are 'Submit' and 'Back' buttons.

Figure 25

Parameter	Description
Name	Name of Authentication profile
Description	Detail for reference
Authentication Server	
Server IP Address	Authentication server primary IP address
Secondary Server IP Address	Authentication server secondary IP address
Authentication Port	Authentication server authentication port
Shared Secret /Confirm Shared Secret	Shared Secret provided by RADIUS server provider
Accounting Server	
Server IP Address	Accounting server primary IP address
Secondary Server IP	Accounting server secondary IP address

Address	
Accounting Port	Accounting server accounting port
Shared Secret /Confirm Shared Secret	Shared Secret provided by RADIUS server provider

Active Directory

The screenshot shows a web interface for configuring an authentication profile. The breadcrumb trail is 'Sites / Profiles / Authentication'. The form includes the following fields:

- Name:** A text input field.
- Description:** A text input field.
- Authentication Method:** A dropdown menu with 'Active Directory' selected.
- PRIMARY SERVER:** A section header.
- IP Address:** A text input field with a dashed line indicating a required character.
- Port:** A text input field.
- Windows Domain Name:** A text input field with a help icon.

At the bottom of the form are two buttons: 'Submit' (blue) and 'Back' (orange).

Figure 26

Parameter	Description
Name	Name of Authentication profile
Description	Detail for reference
Authentication Method	Select the Authentication Method for configuration.
Primary Server	
IP Address	Enter the Public IP address of the Active Directory.
Port	Enter the Port number.
Windows Domain Name	Enter the Domain name in the correct syntax. For example, Google.com it will be written as dc=google,dc=com.

LDAP

Figure 27

Parameter	Description
Name	Name of Authentication profile
Description	Detail for reference
Authentication Method	Select LDAP from the dropdown menu.
Primary Server	
IP Address	Enter the IP address of the LDAP server.
Port	Enter the default port number.
Base Domain Name	Enter the domain name on which the LDAP is hosted.
Admin Domain Name	Enter the name of the Admin profile.
Admin Password / Confirm Password	Enter the password for the profile. / Re-enter the password to confirm.
Key Attribute	Enter a key attribute from which the profile can be searched.
Search Filter	Enter a search filter to lookout for particular class.

Custom API

Figure 28

Scheduling

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

Enable Scheduling Profile – Use the Scheduling profile to control which hours of the day or days of the week to enable/disable WLAN service. For example: a WLAN for Employee use at an Office can be configured to provide wireless access only during Office hours. Click on a day of the week to enable/disable this WLAN for the entire day. Colored cells indicate WLAN enabled. Click and select specific times of day as shown below.

Figure 29

Parameter	Description
Name	Profile Name
Description	Detail for reference
Schedule Plan	Click in the box to set up time zone with respect to date and week day

QoS

Quality of Service refers to the capability of a network to provide better service and performance to specific network traffic. A Differentiated Services Code Point (DSCP) is a packet header value that can be used to request high priority or best-effort delivery for traffic.

Prioritize the access category by dragging row.

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

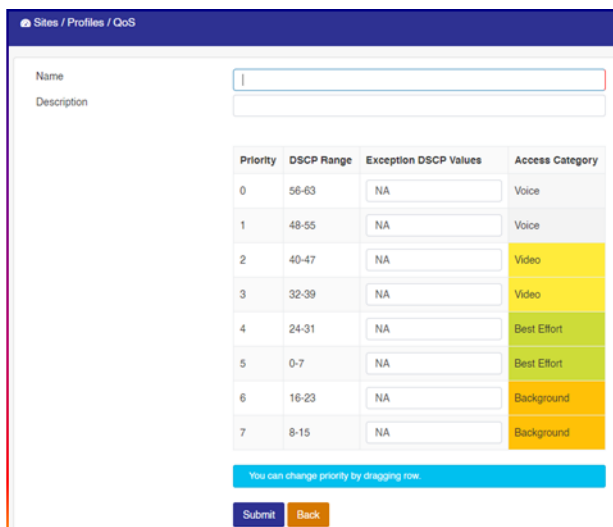


Figure 30

Guest

For managing guest access go to **Cloud Menu > Site > Select Site > Guest**

Guest Access configuration contains several options.

1. Splash Portal
2. Guest Pass
3. Guest Policy

Splash Portal

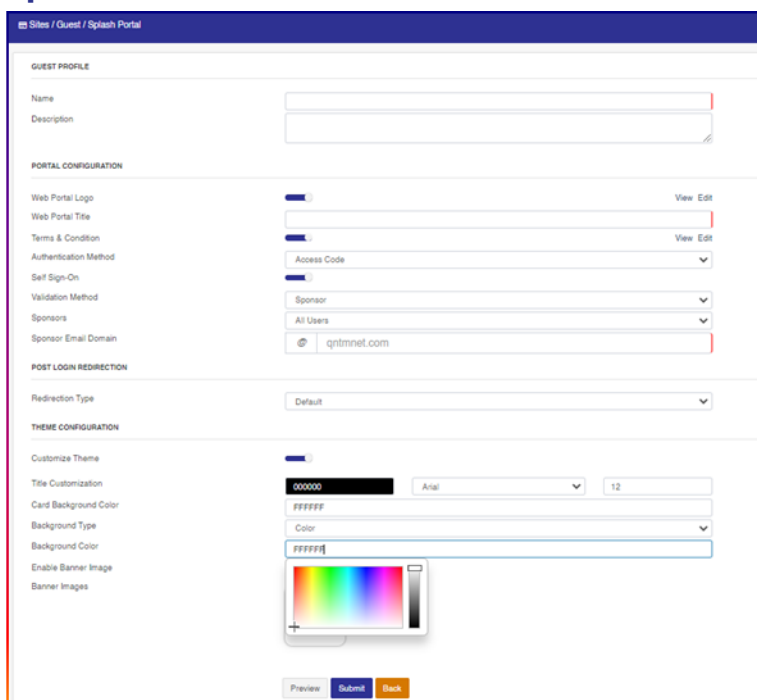


Figure 31

Parameter	Description	Default Value
Guest Profile		
Name	Name of the guest profile.	
Description	Detail for reference.	
Portal Configuration		
Web Portal Logo	Upload logo image. You can also view previously uploaded images with the "View" option.	Disabled
Web Portal Title	Web Portal title name.	
Term & Condition	Upload customized Terms and Condition document in "HTML" format. Can also view previously uploaded.	Disable – Default T&C would be visible
Authentication Method	Select authentication method Click through: Users will get OTP on their registered mobile number to get authenticated. Access Code: Users need to collect access code manually from the concerned person to get authenticate.	Click Through
Self Sign-on	By Enabling "Self Sign On", sponsors option will be active.	Disabled
Sponsors	Provide option to set sponsors as a list or domain-based.	All Users
Sponsor Email Domain	Define the domain name.	
Post Login Redirection		
Redirection Type	Define the specific Web Page URL for redirection after getting authenticated.	
Theme Configuration		
Customize Theme	Enable for customization.	Disabled
Title Customization	Set title text color, font and font size.	
Card Background Color	Set Background Color for KYC form area.	
Background Type	Select type of the background, it can be color or image.	
Background Color	Set background color.	
Enable Banner Image	Select Background image from destination path.	Disabled
Banner Image	Option to upload multiple backgrounds.	

Guest Pass

This option is used to generate a Guest pass. Users can generate single or multiple passes by selecting the appropriate option. Users can also share unused passes with other users as well as clear the passes by selecting the option.

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

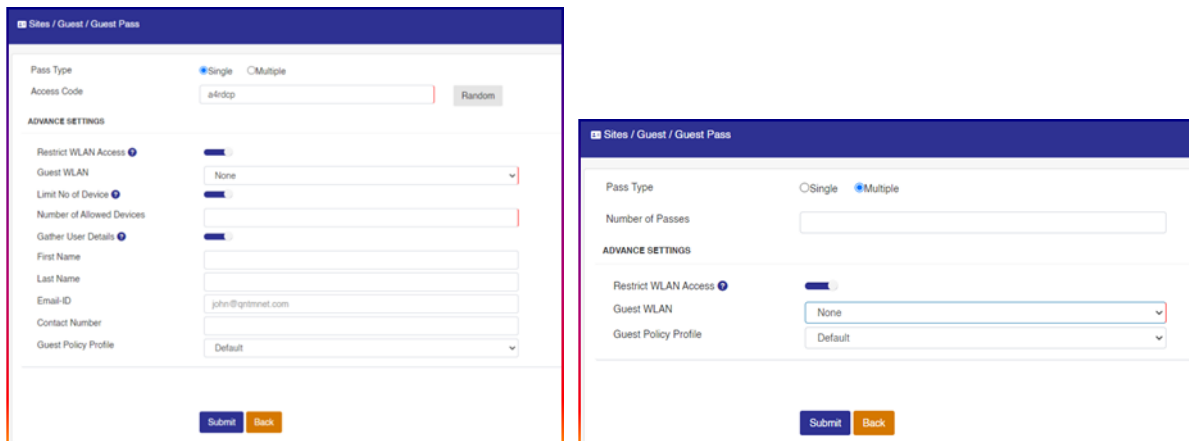


Figure 32

Select type, Single for individual pass generation or Multiple to create multiple passes.

Parameter	Description
Pass Type- Single	
Access Code	Admin can create code manually or generate it randomly.
Advance Settings	
Restrict WLAN Access	Enabling will connect a particular WLAN without authentication.
Guest WLAN	Select a Guest WLAN profile from the dropdown list.
Limit No of Device	Limits the number of devices.
Gather User Detail	
First Name	User's First Name.
Last Name	User's Last Name.
Email-Id	User's Email-ID.

Contact Number	User's Contact number.
Guest Policy Profile	Select guest profile from the dropdown.
Pass Type- Multiple	
Number of Passes	Enter the number of passes to avail for clients.
Advance Settings	
Restrict WLAN Access	Enabling will connect a particular WLAN without authentication.
Guest WLAN	Select a Guest WLAN profile from the dropdown list.
Guest Policy Profile	Select guest profile from the dropdown.

Guest Profile

This option is used to create guest pass policies like pass validity, effective period as well as the expiry period.

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

This screenshot shows the notification settings for a guest profile. It includes two sections for email and SMS notifications. Each section has a toggle switch to enable or disable the notification, followed by a dropdown menu to select a profile and a text area for a template. A 'Submit' button is located at the bottom.

This screenshot shows the main configuration page for a guest profile. The breadcrumb trail at the top reads 'Sites / Guest / Guest Profile'. The form contains several fields: 'Profile Name' and 'Description' (text inputs), 'Pass Valid For' (text input with a 'Mins' dropdown), 'Pass Effective Since' (radio buttons for 'Creation time' and 'From first use'), 'Expiry Guest Pass' (text input with a 'Days' dropdown), 'Enable Quota' (toggle), 'Quota Limit' (text input with a 'GB' dropdown), 'Enable Bandwidth' (toggle), 'Upload Bandwidth' (text input with a 'Kbps' dropdown), and 'Download Bandwidth' (text input with a 'Kbps' dropdown). 'Submit' and 'Back' buttons are at the bottom.

Figure 33

Parameter	Description
Profile Name	Profile Name.
Description	Edit description for reference.
Pass Valid for	Pass validity period in Minutes / Hours / Days.
Pass Effective Since	Pass effective Period since pass can be valid for use.
Expiry Guest Pass	Guest passes expiration duration.
Enable Quota	Set Quota limit on service plan.
Enable Bandwidth	Set upload and download bandwidth limit.
Enable Mail Notification	Will send access code via mail to respective client.
SMTP Profile	Select respective SMTP profile. To created profile Go to Cloud Menu > Site > Select Site > Services > SMTP > Add
SMS Configuration	Enable to send access code via SMS. To create profile Go to Cloud Menu > Site > Select Site > Services > SMS > Add

Quantum Secure+

Quantum Secure+ delivers secure network access by providing each device and user with a unique login credential.

Portal

To create Guest login page

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

Figure 34

Parameter	Description	Default Value
Name	Define portal name.	-
Description	Add description, if any.	-
Type	Select type of authentication, Web authentication / Quantum SECURE+.	
	Web authentication:	
	Quantum SECURE+:	
Portal Configuration		
Logo Image	Provide option to upload logo image. (Size – Not to exceed 1 Mb)	-
Title	Define title text. (Like welcome message on login page)	Disabled
Title Customization	Customize font Color, Style and Size.	Disabled
Login Button Text	Define login button text.	Disabled
Login Button Customization	Customize login button.	Disabled

Policy

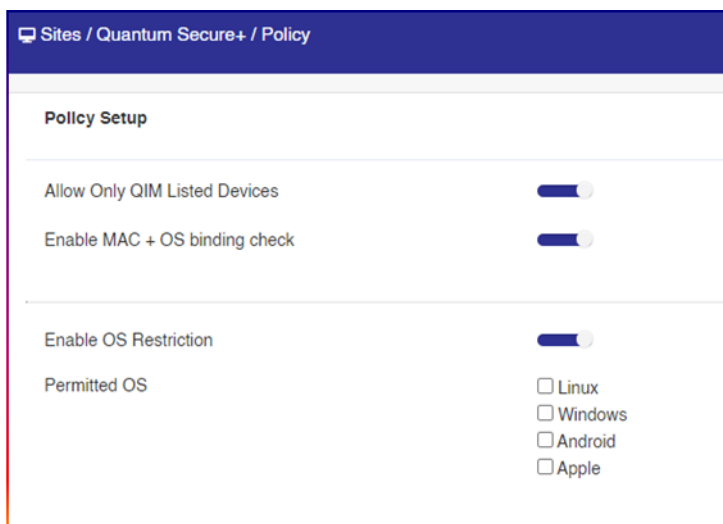


Figure 35

Define Webauth policy.

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

Parameter	Description	Default Value
Allow Only Listed Devices MAC	If enabled – only the device MAC listed in the “Directory” will have access.	Disabled
To add devices: Go to Cloud Menu > Directory > Users > Add		
Allow Only OS	Use this option when required to allow particular OS devices for access. (for Quantum Secure+ feature)	Disabled

ACL

Layer 2 ACL

Go to **Cloud Menu > Site > Select Site > ACL > Layer 2 ACL > Add**

Access Control List (L2): An ACL can be created to allow/deny specific devices. MAC addresses in the allow/deny list are allowed/blocked.

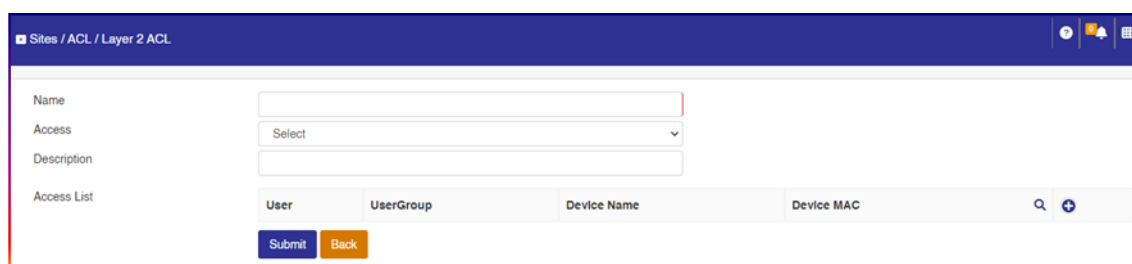


Figure 36

Parameter	Description
Name	Profile Name.
Access	“Allow ” or “Deny” WLAN access to the clients.
Description	Enter detail for reference.

Access List	Add Users with User Group, Device and their MAC address.
-------------	--

Layer 3ACL

Go to **Cloud Menu > Site > Select Site > ACL > Layer 3 ACL > Add**

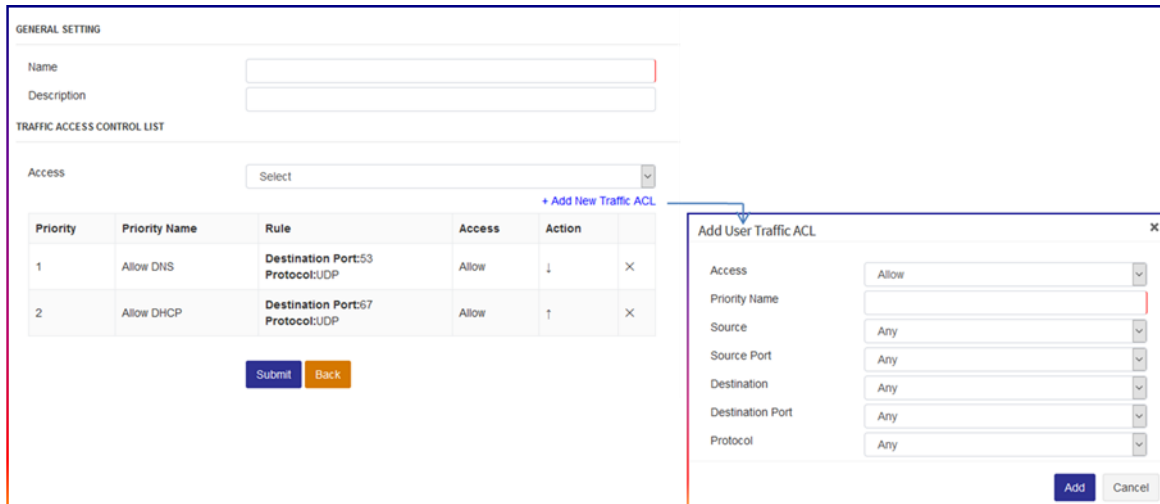


Figure 37

Parameter	Description
Name	Profile Name.
Description	Detail for reference.
Traffic Access Control List	Set up time zone with respect to date and weekday.

Add User Traffic ACL

Parameter	Description
Access	Administrator can allow or block User Traffic.
Priority Name	
Source	Allow/Block user traffic using Source IP address or Subnet.
Source Port	Allow/Block user traffic by using Source Port or Port Range.
Destination	Allow/Block user traffic using Destination IP address or Subnet.
Destination Port	Allow/Block user traffic by using Destination Port or Port Range.

Protocol	Select protocol type TCP, UDP, TCP + UDP.
----------	---

OS Policy

OS Policy can allow or deny wireless clients based on specific OS/device type. Access Control List cannot be enabled if OS Policy is enabled.

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

Figure 38

Parameter	Description
Name	Profile Name.
Description	Detail for reference.
Default Action	Allow or Deny access for selected OS/Hardware based devices.
OS / Hardware	Select as per the requirement.
MAC Exception	
Action	Allow or Deny access for listed MAC devices.
MAC List	Add MAC address of devices.

MAC Whitelist

Devices get access without authentication.

Go to **Cloud Menu > Site > Select Site > ACL > MAC Whitelist**

Figure 39

Parameter	Description
Name	Profile Name.
Description	Detail for reference.
Type	Select MAC Whitelist / Client Isolation.
MAC List	Add MAC Addresses to be Whitelisted.

Security Centre

URL Filtering

This option allows the admin to block the particular URLs from access.

Go to **Cloud Menu > Site > Select Site > Security Center > URL Filtering**

Figure 40

Parameter	Description
Profile Name	Profile Name.
Description	Detail for reference.
Add URL	Enter the URL. Add multiple URLs by clicking on the "+" option.

Application Filtering

This option allows the admin to block the access of particular Applications.

Go to **Cloud Menu > Site > Select Site > Security Center > Application Filtering**

Application Group

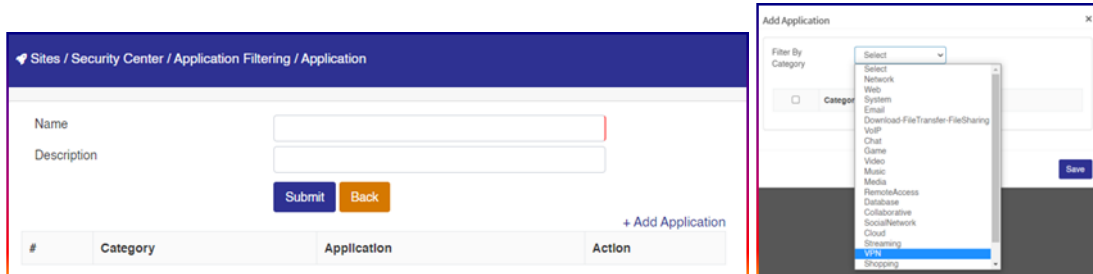


Figure 41

Parameter	Description
Name	Profile Name.
Description	Detail for reference.
Add Application	Add the applications to be blocked by clicking on the "+" option.

App Filtering

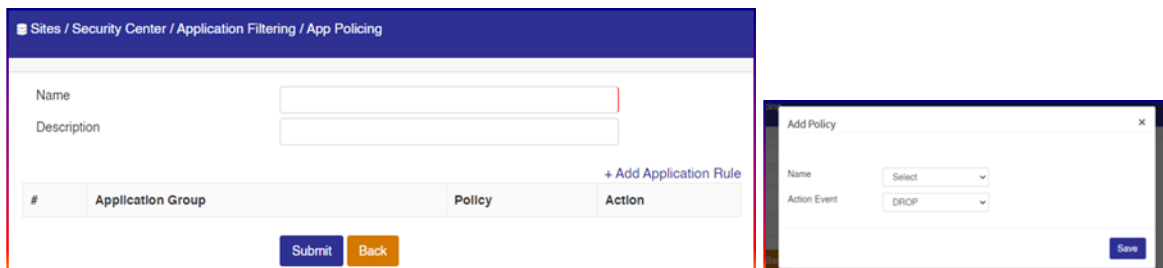


Figure 42

Parameter	Description
Name	Profile Name.
Description	Detail for reference.
Add Application Rule	

Device Policy

Administrator can see list of client MAC with applied policies.

Refer: [Site Clients](#)

WIDS

Wireless Intrusion Detection System (WIDS) monitors the radio *frequencies* for the presence of unauthorized, rogue Access Points. The system monitors radio *frequencies* used by wireless LANs and immediately alerts the systems administrator whenever a rogue Access Point is detected.

Go to **Cloud Menu > Site > Select Site > Security Center > WIDS**

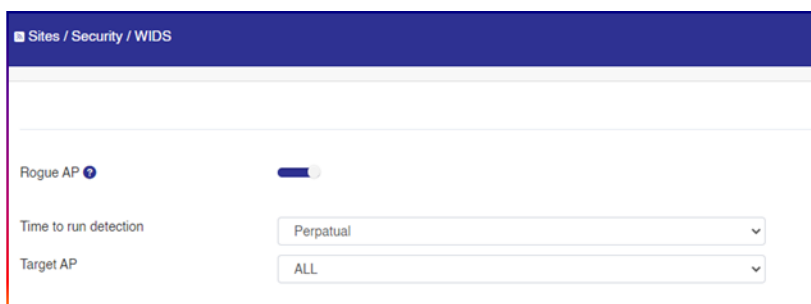


Figure 43

Services

Configure DHCP, SNMP, SMTP, SMS, Notifications, Syslog, Tools, Floor Plan and Outdoor Plan for AP managed by Quantum RUDDER.

DHCP

Figure 44

SNMP

Simple Network Management Protocol (SNMP) is an application-layer protocol used to manage, monitor network devices, detect network faults and sometimes even used to configure remote devices.

Go to **Cloud Menu > Site > Select Site > Services > SNMP > Add**

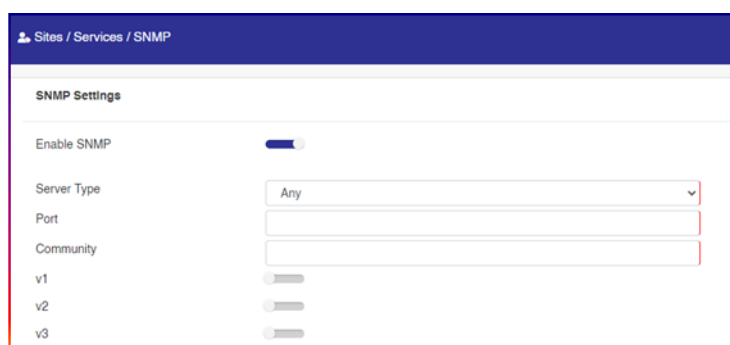


Figure 45

Parameter	Description
Enable SNMP	Enable SNMP to receive immediate notifications for AP and system issues.
Server	The SNMP server IP address.
Port	UDP Port.
Community	Community name defines the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the Access Point. If the community is incorrect, the device simply ignores the request and does not respond.
v1	Enable SNMPv1 to provide a simple means for retrieving data. Security is provided through the community.
v2	Enable SNMPv2 to provide additional and more efficient methods to request data and add new data types (such as 64-bit counters) so that the monitoring system could get more accurate data.

v3	Enable SNMPv3 to support the highest level of security for SNMP communication.
----	--

SMTP

For Setting up an Email Notification Alert, an SMTP profile is required.

Go to **Cloud Menu > Site > Select Site > Services > SMTP > Add**

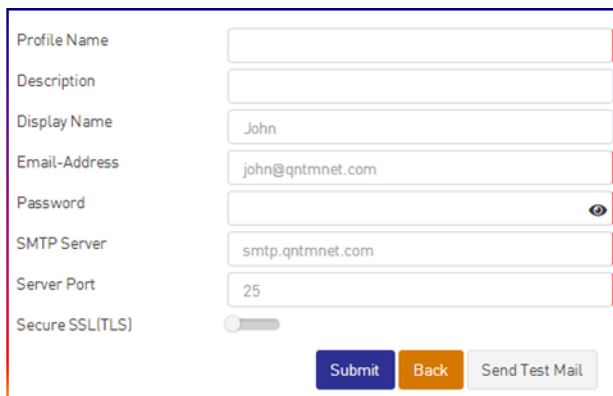


Figure 46

Parameter	Description
Profile Name	Profile Name.
Description	Description for reference.
Display Name	Display name.
Email Address	The email address from which Cloud Manager will send Alert Emails.
Password	Password for the Email address.
SMTP Server	Type the full name of the server provided by your ISP or mail administrator.
Server Port	Type the SMTP port number provided by your ISP or mail administrator. The default SMTP port number is 25 or 587.
Secure SSL (TLS)	Enable SSL to enhance secure communications over the Internet.

SMS

Configure SMS settings for Guest Pass delivery via SMS.

Go to **Cloud Menu > Site > Select Site > Services > SMS > Add**

Figure 47

Parameter	Description
Profile Name/ Description	Profile Name./ Description for reference.
Provider	Select Provider from the dropdown, SMS Country, Twilio or SMS Gupshup account for SMS delivery.
Username	Username (Provided by SMS gateway provider to access your account)
Password	Password (Provided by SMS gateway provider to access your account)
Sender ID	Sender ID provided by SMS service provider.
Gateway API URL	Define API URL.
SMS Template	Set SMS Template (Define only approved template by SMS Provider)

Notifications

Notification Type	Send mail	Notify App	Log	Alert
Devices Unreachable from Cloud	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Pre-Provision Failed	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Device Rebooted	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Channel Changed	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Management Tunnel	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Figure 48

Syslog

Enable Syslog, if required.

Go to **Cloud Menu > Site > Select Site > Services > Syslogs > Enable**

The screenshot shows a configuration page for Syslog. At the top, there is a 'Syslog' toggle switch that is turned on. Below it, 'Syslog Type' is a dropdown menu set to 'Cloud'. 'Syslog IP' is a text input field containing '192.168.1.1'. 'Port' is a text input field containing '5', and 'Protocol' is a dropdown menu set to 'TCP'. A blue button labeled 'Test Syslog Server Connection' is positioned below these fields. Underneath, there are four more toggle switches: 'Alert', 'Warning', 'Administrative Log', and 'User Log', all of which are currently turned off.

Figure 49

Parameter	Description	Default Value
Enable Syslog	Enable to receive alerts and logs from Quantum RUDDER.	Disabled
Syslog Type	Select Syslog type Cloud or Local.	
Syslog IP	The IP address of the Syslog server to receive alerts and logs from Quantum RUDDER.	
Port	By default, the Syslog port number is 514. The port number with TCP or UDP protocol if the Syslog server is using a different port.	
	Test Syslog server connection	
Alert	Enable to activate Alert logs. Admin can view Alerts log under Cloud Menu > Site > Logs	Disabled
Warning	Warning message will be forwarded to the Syslog server if enabled.	Disabled
Administrative log	Enable to activate Administrative logs. Admin can view Administrative log under Cloud Menu > Site > Logs	Disable
User log	Enable to activate User logs. Admin can view User log under Cloud Menu > Site > Logs	Disabled

Tools

Enable Services for the Internet Health check, in case required.

Go to **Cloud Menu > Site > Select Site > Services > Tools > Enable**

Enabling Tools will display the connected client devices and their traffic data statistics on the Dashboard Menu screen.

Floor Plan

Floor plan basically allows to create a blueprint of the entire site including the walls, partitions, etc. We can then place APs in the plan to check the network connectivity and strength at different locations to finalize the ideal placement of APs.

Outdoor Plan

Outdoor plan serves the same purpose as the floor plan but for outdoor devices. It allows to create a blueprint of the site to check network connectivity and strength for outdoor location to decide the ideal setup of APs placements.

Logs

RUDDER provides multiple log options for the selected time period that can be used for monitoring and troubleshooting purpose.

Go to **Cloud Menu > Site > Select Site > Logs > Click on Required Logs**

Administrative

Parameter	Description
Date	Created log Date
Time	Created log Time
Administrator	Administrator name
Log Description	Log detail
Site	Respective site name

User

Parameter	Description
Name	Client connection status
Description	Log detail
Log Date / Time	Log creation date & time

Alerts

Parameter	Description
Date	Creation Date of respective log
Time	Creation Time of respective log
Resource	The respective log system resource
Description	Log description in detail. i.e. even happened with respective Access Point
Site	Name of Site which particular Access Point belongs

Events

Parameter	Description
Date	Creation Date of respective log
Time	Creation Time of respective log
Name	Name of the Event.
Description	Log description of the event in details with results.

Guest

Parameter	Description
Code	Using which the guest access code client got connected.
Start Time	Client start/connection time.
Stop Time	Client stop/disconnected time.
Duration	Client total connection time duration.
Download	The total download (in KB/MB/GB/TB) for client in the session.
Upload	The total upload (in KB/MB/GB/TB) for client in the session.

Total Data Transfer	The total data transfer (in KB/MB/GB/TB) for client in the session.
Local IP	Client IP address
Client MAC	Client MAC address

WIDS

RUDDER supports Rogue AP detection. It is an important component in securing the Wireless network. SSID Spoofing is a parameter that finds an SSID that looks like one of your authorized SSIDs which can be a part of your network broadcast using an Access Point by a hacker.

Parameter	Description
Rogue MAC	MAC address of the rogue AP.
SSID	The name of the Wireless network that the rogue AP is broadcasting.
Encryption	The security status whether it is Encrypted or not.
Channel	The radio channel used by the rogue AP.
Threat Level	The type of threat level such as SSID Spoofing, MAC Spoofing, Rogue AP.
Last Detected	The last Date and time when the rogue AP was detected by Quantum RUDDER.

Mesh

Mesh Networks are set up to connect the clients and devices of the same network through an efficient route. Mesh establishes a stable connection throughout the network space.

Support

Technical Support

Go to **Cloud Menu > Site > Select Site > Support > Technical Support**

Please email to support@qntmnet.com for technical support.

Crash Report

Go to **Cloud Menu > Site > Select Site > Support > Crash Report > Enable**

Enabling Crash Report allows submitting Crash Report, in case of any. The reports will be sent to the tech team automatically.

TAC

Client Connection

The Admin can check Clients' MAC connection on their selected APs.