Quantum Networks

Access Point | Firmware Release Note

Firmware: 7.0.1.B1

Month of Release: March, 2025

Copyright Information

Contents

Devices Supported

Quantum Networks: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN_I-210-Plus, QN-I-220, QN-H-220, QN-O-230 (Standalone & Cloud Controlled)
** Features may vary depending on the device model and operation mode of Access Point.*

Important Notices

- Firewall rules - Allow rudder.qntmnet.com and reports.qntmnet.com in the destination field.

- While upgrading firmware in Access Point, please make sure the power supply should not be interrupted. This may corrupt firmware in Access Point. It is advisable to use a power source from UPS.

- Device (s) may reboot post firmware upgrade. The activity is not advised during peak hours or in critical production networks.

Wireless Features

Features	Description
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-I-220, QN-H-220, QN-O-230	
WMM	Defines and optimizes traffic for multiple concurrent applications competing for network resources by prioritizing Wi-Fi network traffic.
DHCP Option 43 support	Supports DHCP Option 43 to detect the onboard URL for device onboarding in an on-premises server.
Session Control	Manages sessions by restricting them based on predefined rules at different levels, such as per host, per subnet, per IP range, and per port.
CoA	Modifies connected users' state, including quota, bandwidth, data limits, and disconnection.
MAC-Auth	Performs MAC authentication before wireless authentication in Standard, Hotspot, and 802.1x modes, with preferred MAC delimiter options.
BSSID Details	Displays BSSID details of both radios for each SSID.
VSA Support	Adds support for WISPr-Location-Id, WISPr-Location-Name, WISPr-Logoff-URL, and WISPr-Redirect-URL in Hotspot, and WISPr-Location-Id and WISPr-Location-Name in 802.1x SSID.
Hotspot 2.0	Supports Hotspot 2.0, allowing clients to connect and roam between public wireless networks and cellular networks.
LLDP Support	Allows devices to advertise their information to directly connected peers/ neighbours.
Random MAC Detection	Detects client devices connected to the AP using random MAC addresses.
Wi-Fi Calling	Enables seamless Wi-Fi calling with the highest network traffic priority for uninterrupted voice connectivity.
DiffServ	Classifies Layer 3 traffic and applies differentiated treatment for optimal resource use.
Application Whitelisting	Restricts wireless client devices to only specified application traffic while blocking other internet traffic.
URL Whitelisting	Restricts wireless client devices to only specified URL traffic while blocking other internet traffic.
Radio Mode Control	Configures 2.4 GHz and 5 GHz radios to broadcast specific 802.11n/ac/ax modes, allowing only specified standards to connect.
RTS/CTS Threshold	The RTS/CTS threshold improves network stability and reduces collisions. It ranges from 0 to 2347 octets.
Multicast to Unicast conversion	Converts wireless multicast traffic to unicast, ensuring high-quality video transmission to a large number of clients.
Walled Garden in Secure Plus	Supports a walled garden in Secure+ SSID, enabling devices to connect directly without following the authentication process.
Bandwidth Restriction	Manages bandwidth by restricting upload and download speeds at different levels, such as SSID-based, per-client, per-host, OS-based, port-based, user group-wise.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-O-230	
WLAN Priority	Configures SSID priority to allocate more airtime for higher-priority networks.

Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus	
Bonjour Forwarding	Allows Apple devices to discover and communicate with each other across multiple VLANs using the Bonjour protocol
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus	
DSCP / PCP Tag	Marks DSCP/PCP tags on specific applications' outbound traffic.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-I-210-Plus	
Application Usage	Monitors internet usage at various levels, including per client, per application, and per SSID, with date and time tracking.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-I-220, QN-H-220	
DPC	Enables tunnelling of user traffic to secure data transmission between remote and local data centres.

Access Point Features

Features	**Description**
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-I-220, QN-H-220, QN-O-230	
IPDR Logs	Support sending IPDR logs in the form of IPFix, NetFlow, or RFC Syslog standard.
Reboot Button Control	Control the function of the hard reboot/reset button to prevent misuse.
mDNS & IPv6 Management	Manage traffic flow for mDNS and IPv6 to restrict mDNS or IPv6-related flooding or allow cast devices on the network.
Local GUI access	Control access to the local GUI of the Access Point.
NTP Server	Specify NTP server details to sync AP time with its time zone.
Link Local address	Identify the AP's WAN IPv6 Link-Local Address and Interface Identifier.
Local GUI Login	Allow local AP login with a customized HTTP port for security purposes.
SNMP v3	Add support for SNMP version 3 to enhance security through authentication.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-H-245, QN-I-210-Plus, QN-I-220, QN-H-220	
TACACS+	Allow TACACS+ client authentication on the LAN port for security.
Supported Models: QN-I-490, QN-I-470, QN-I-270	
URL Logs	Support to send surfed Website URLs of each wireless clients to syslog.
Supported Models: QN-I-490, QN-I-470	
AP as Controller	Support AP to manage up to 15 APs as a controller.

Internetworking Features

Features	Description
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus , QN-I-220, QN-H-220	
L2 GRE	Creates a Layer 2 tunnel to extend the network and ensure secure communication between the server and client using the GRE tunnelling protocol.
L2TP	Creates a Layer 2 tunnel for secure communication between the server and client using the L2TP tunnelling protocol.
Wireguard	Creates a tunnel for secure communication between the server and client using the WireGuard tunnelling protocol.
OVPN	Creates a tunnel for secure communication between the server and client using the OVPN tunnelling protocol.
Routing Protocol	
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus	
RIP	When enabled, it allows communication between different networks using the RIP routing protocol.
OSPF	When enabled, it allows communication between different networks using the OSPF routing protocol.
Other Features	
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus QN-I-220, QN-H-220, QN-O-230	
DMZ Host	A DMZ host is a device on the internal network with all UDP and TCP ports open and accessible from the external network, similar to port forwarding.
ALG Control	Application Layer Gateway enables the parsing of application-layer payloads and decides whether to allow or deny traffic to the application server.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus QN-I-220, QN-H-220	
UPnP	When enabled, it allows networking devices such as personal computers and printers to discover each other's presence on the network using a set of protocols called UPnP.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-220, QN-H-220	
Ad-Block	When enabled, it identifies and restricts elements such as advertisements. It only works in Router Mode.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-H-220	
Safe-Search	When enabled, it restricts users from accessing adult or violent content. It only works in Router Mode.

Services

Features	Description
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-220, QN-H-220, QN-O-230	
Spectrum Analysis	Displays information in graph form about Wi-Fi interference caused by Wi-Fi devices, Bluetooth devices, microwave ovens, etc., across both radio bands.
Spectrum Channel metric	Provides detailed channel statistics in graph form, including Channel Availability, Channel Efficiency, Channel Load, and Noise Floor.

Spectrum FFT Duty cycle	Displays the Spectrum FFT Duty Cycle graph, illustrating the duty cycle percentage for each frequency in the channel bands of both radios.
WIFI Analyzer	The Wi-Fi Analyzer graph functions as the ultimate tool for debugging, analysing, and monitoring neighbouring Access Points (APs) in the surrounding environment.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-H-220, QN-I-220, QN-O-230	
WDS	Enables wireless network extension with P2P/P2MP connectivity by linking access points via WLAN without requiring a wired backbone.

Diagnostics

Features	Description
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-I-220, QN-H-220, QN-O-230	
PCAP Capture	Allows capturing a PCAP file of wired and wireless mediums for troubleshooting issues.
ARP Scan	Allows the use of the ARP protocol to discover IPs and hosts on the WAN network.
Host Discovery	Allows fetching the MAC address details of a specific IP address.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-O-230	
AP Link Statistics	Allows measuring live internet bandwidth consumption on the WAN link.
Internet Speed Test	Allows performing a speed test to measure the internet bandwidth available on the AP.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-220, QN-H-220, QN-O-230	
Airbender	Provides detailed information on channel utilization and interference caused by neighboring APs.

Wireless Intrusion Detection/Prevention (HAWKEYE)

Features	Description
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-H-245, QN-O-240, QN-I-210-Plus, QN-I-220, QN-H-220, QN-O-230	
Rogue SSID	AP reports when it detects an untrusted SSID being broadcast in the RF environment.
MAC Spoofing	AP reports when it detects a duplicate BSSID of a trusted AP being broadcast by other devices in the RF environment.
SSID Spoofing	AP reports when it detects the same SSID name being broadcast by another AP in the RF environment.
Honeypot / Evil Twin	AP reports when it detects both a duplicate BSSID and SSID name of a trusted AP in the RF environment.
NULL Probe Request	AP reports when it detects a probe response with no SSID name (hidden SSID) in the RF environment.
AdHoc Connection	AP detects and blocks AdHoc connections for a configurable time in Rudder when a malicious client tries to use a valid device's hotspot.
Password Guessing	AP reports when it detects a Password Guessing attack and blocks it for a configurable time in Rudder (an attempt to connect to an SSID by trying different password

	combinations).
Misconfigured AP Detection	AP reports Misconfigured APs when it detects SSIDs in the RF environment that differ from Rudder's settings.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-O-230	
RTS Abuse Attack	AP reports when it detects a flood of RTS frames in the RF environment.
CTS Abuse Attack	AP reports when it detects a flood of CTS frames in the RF environment.
Auth Attack	AP reports when it detects an authentication attack (an attempt to obtain the pre-shared PSK by sniffing the 4-way handshake).
Assoc Attack	AP reports detected association attacks—attempts to connect clients to malicious APs.
Fata jack tool	AP reports when it detects a FataJack attack (an attempt to disconnect station devices using spoofed authentication frames containing an invalid authentication algorithm number).
Man in the Middle	AP reports when it detects a MITM attack (an attempt to intercept communication between an AP and a client device to steal information).
DHCP snooping server	AP reports when it detects a rogue DHCP server (a client was assigned an IP address through a malicious DHCP server) in the network.
Power Save	AP reports when it detects a Power Saver attack (an attempt to send spoofed frames to the AP to increase buffer size, pretending that the client device is in sleep mode).
AP Flood Attack	AP reports when it detects an AP Flood attack (an attempt to delay client connections by flooding the AP with beacon frames).
Block ACK DoS	AP reports when it detects a Block ACK DoS attack (an attempt to obstruct client connections by manipulating the window sequence number of a specific client).
Malformed Frame-Assoc Request	AP reports when it detects a Malformed Frame - Assoc Request (a defective association frame with a null SSID, which may disrupt AP functionality).
Malformed Frame-Auth	AP reports when it detects a Malformed Frame-Auth (incorrect data in management authentication request frames that can cause a security breach).
Deauth Attack	AP reports when it detects a Deauthentication (Deauth) attack and prevents it if 802.11w (Protected Management Frames) is enabled on the wireless SSID (an attempt to disconnect clients by sending forged deauth frames to the AP or clients).
Disassoc Attack	AP detects and reports Disassociation attacks, preventing them if 802.11w (Protected Management Frames) is enabled on the SSID.
Omerta Attack	AP detects and reports Omerta Deauth attacks and prevents them if 802.11w (PMF) is enabled on the SSID.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-H-245, QN-O-240, QN-I-490, QN-O-230,	
Dos Attack	AP reports when detects DoS attack (attempts to break down the function of AP by flooding with large traffic sent by single source device) in network.
DDos Attack	AP reports when detects DDoS attack (attempts to break down the function of AP by flooding with large traffic sent by different source device) in network.
Port Scanning	AP reports when detects Portscanning (attempts to get details of AP's port) in network.
Supported Models: QN-I-490, QN-I-470, QN-I-270	
SSH Brute force	AP reports when detects SSH Brute force attack (attempts to gain access of AP using different combinations of username and password)in network.

Enhancement	
Features	**Description**
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-I-220, QN-H-220, QN-O-230	
QNPSK	Achieve the same Quantum secure functionality with a user database stored in the cloud, allowing unlimited user support.
High efficiency Mode	Enables the AP to operate at 802.11ax data rates on both 2.4 GHz and 5 GHz bands.
Tx power reduction	Adjusts AP's Tx power by percentage.
Dynamic VLAN	Dynamic VLAN automatically assigns devices or users to specific VLANs based on authentication and policies assigned by the Radius Server.
Layer 2 ACL	Existing connected Wi-Fi users will not be disconnected when a new MAC address is added or removed from the L2 profile.
Client Isolation	Allows management by restricting communication between clients connected to different or the same VLAN.
Walled Garden	Supports configuring a walled garden at various levels, such as range, CIDR, and suffix domain.
Legacy encryptions	Adds support for additional encryption methods: WEP-64, WEP-128, and WPA in SSID.
Mesh	Mesh clients extend the wireless LAN by connecting to a Mesh gateway AP.
Encryption Method	Adds encryption support for DES-CBC, 3DES, and AES-CBC in IPSec.
Dual stack	Supports both IPv4 and IPv6 simultaneously in WAN connections.
STP	When enabled, applies the STP protocol to a specific LAN profile to prevent Layer 2 loops in router mode.
Event Log	Collects various event logs of hotspot client devices, such as client connections and deauthentication due to events like quota surpassing, idle timeout, or device shutdown.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-H-245, QN-I-210-Plus, QN-I-220, QN-H-220 QN-O-230,	
IPv6 RA setting	When enabled it allows client devices to create it's own local IPv6 address based on configured flags in router mode.
Supported Models: QN-I-490, QN-I-470, QN-I-270, QN-O-240, QN-I-210-Plus	
Application filtering	Extended and re-categorized the application database for more effective filtering.

Report an Issue

If you are facing any difficulty in firmware upgradation or need technical assistance, contact support@qntmnet.com or call 18001231163.