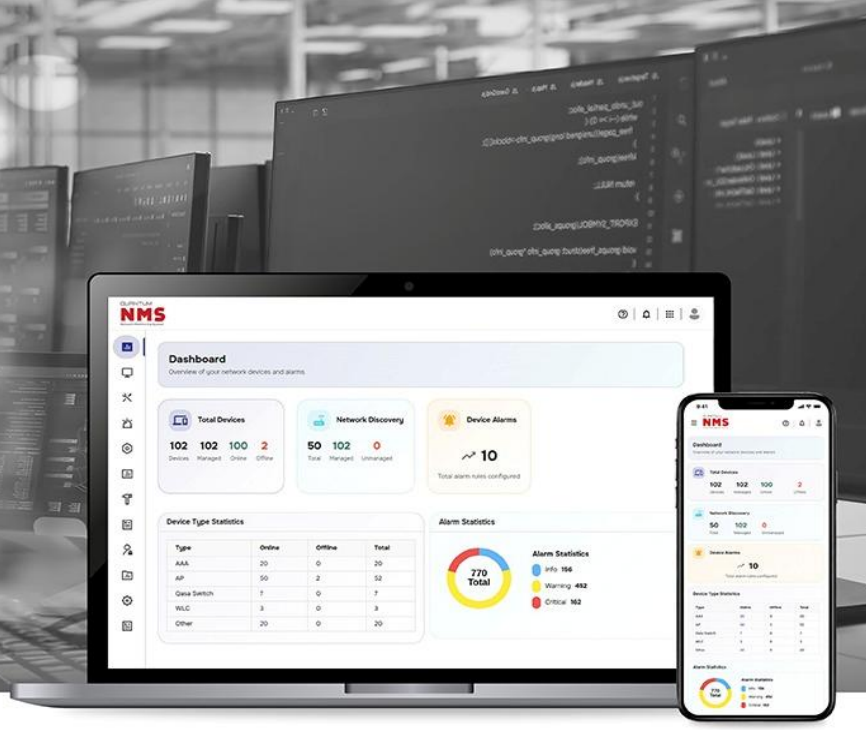
QUANTUM

NMS

Network Monitoring System

Enterprise On-Premises Network Monitoring & Management Platform

- Unified Control
- Secure Intelligence
- Smart Visibility
- Secure Automation



Product Overview

QNMS is a centralized network management platform designed for deploying, monitoring, managing, and troubleshooting wired and wireless network infrastructure. It provides unified visibility, automation, and control across multi-vendor environments with scalable architecture and high availability.

Discovery & Visibility

Auto-scans IP ranges and supports manual device addition for complete visibility.

Real-time Health

Monitors device health, interface stats, and uptime with real-time visibility.

Proactive Alerting

Threshold alarms and SNMP traps with full lifecycle management.

Bulk Deployment

Deploys bulk config templates with dynamic variables for faster network changes.

Benefits

On-prem deployment

On-premises Active-Passive HA deployment with no cloud dependency.

Automation-ready

Template-based configs, scheduled tasks, and cron-driven discovery reduce manual effort and errors.

Multi-vendor support

Supports multi-vendor integration via SNMP, WMI, SSH, and API.

Flow intelligence

Analyzes traffic via sFlow and NetFlow v5/v9 with top-talker, app, and protocol breakdowns.

Unified dashboard

Unified dashboard for monitoring, control, and reporting

Built-in diagnostics

Ping, Traceroute, SNMP testing, and a MIB browser – all accessible without any CLI tools.

Key Highlights

Core Monitoring & Device Management

Feature	Description
Device Discovery	Auto-scan IP ranges via SNMP/WMI/SSH; scheduled cron-based and manual addition
Device Management	Centralized inventory with real-time up/down/unknown status
SNMP Polling Engine	Batch polling with rate control; OID-based custom metric collection
Rack & Room View	Physical rack layout visualization with slot-level device placement
Multi-Vendor Support	Quantum, Cisco, HP, Dell and other SNMP-capable vendors
Network Hierarchy	Site → Building → Floor grouping with site-wise reporting
Interface Monitoring	Per-device interface stats, utilization, errors, and status

Configuration Management

Feature	Description
Device Templates	Category → Type → Template hierarchy; vendor & OID assignments
Monitoring Templates	Metric collection definitions, unit categories, monitoring groups
Config Templates	Dynamic variable substitution; batch deployment to device groups
Credential Profiles	SNMP v1/v2c/v3, WMI, SSH/Telnet credential sets
Task Management	Scheduled task automation with cron-based scheduling and execution history
Backup & Restore	Device and system configuration backup and restore

Alarm & Notification Engine

Feature	Description
Threshold Alarms	Per-device alarm rules with severity classification; active alarm dashboard
SNMP Trap Handling	Trap reception & parsing; OID/trap definition; severity mapping (Roadmap)
Alarm Lifecycle	Real-time triggering, acknowledgment with audit trail, full history log
Syslog Collection	Receive device syslog events; correlation with alarm engine
Notification Channels	Email (SMTP), in-app notifications, Webhook (Roadmap)
Notification Rules	Rule-based routing per alarm type; multi-channel delivery (Roadmap)

Flow Analysis – sFlow / NetFlow / IPFIX

Capability	Detail
Supported Protocols	sFlow, NetFlow v5/v9, IPFIX (Roadmap)
Collection Ports	NetFlow: 2055 | sFlow: 6343 | IPFIX: 4739
Traffic Classification	Application-mapping tables for app-level traffic classification
QoS Mapping	DSCP value mapping to quality-of-service traffic classes
Endpoint Identification	MAC address and IP alias mapping for source/destination labels
Top-Talker Analysis	Top applications, hosts, and protocols breakdown
Visual Analyzer	Protocol charts and trend graphs for flow data

Reporting & Analytics

Report / Feature	Description
Supported Protocols	sFlow, NetFlow v5/v9, IPFIX (Roadmap)
Collection Ports	NetFlow: 2055 | sFlow: 6343 | IPFIX: 4739
Traffic Classification	Application-mapping tables for app-level traffic classification
QoS Mapping	DSCP value mapping to quality-of-service traffic classes
Endpoint Identification	MAC address and IP alias mapping for source/destination labels
Top-Talker Analysis	Top applications, hosts, and protocols breakdown
Visual Analyzer	Protocol charts and trend graphs for flow data

Network Diagnostic Tools

Tool	Description
Ping (ICMP)	Test device reachability directly from the NMS server
Traceroute	Map network path hops to any target device
SNMP Test	Validate SNMP connectivity and credential correctness
MIB Compiler	Upload and compile vendor-specific MIB files
MIB Browser	Explore compiled MIB trees and browse OID hierarchies

Administration & Security

Feature	Description
User Management	User creation with roles, active/inactive control, enforce password change on login
Role-Based Access Control	Granular menu-level permissions; Module → Menu → Permission hierarchy
Multi-Role Support	Assign multiple roles per user for flexible access control
Activity Audit Logging	All user actions timestamped with IP address tracking
Session Logging	Login/logout session logs for compliance and forensics
API Security	Secure API key-based integrations

System Settings & High Availability

Setting / Feature	Description
System Configuration	System name, locale, time zone, NTP server assignment
Network Interface Mgmt	Physical & virtual interface management; DHCP per interface
Firmware & Updates	Centralized firmware upload and appliance update
Backup & Restore	Full system backup and restore from backup file
License Management	License activation and management
System Health	CPU, memory, disk, and services monitoring
High Availability	Active-Passive cluster; failover detection and cluster state management

Hardware Specifications – On-Premises Appliance

The QNMS hardware appliances are purpose-built for enterprise on-premises deployments, offering maximum performance, redundancy, and port density in a 1U rack form factor.

Parameters	RR-400	RR-300	RR-200
Appliance Overview			
Appliance Type	Hardware (1U Rack-mount)		
Max Monitored Devices	Up to 2,500 devices	Up to 2,500 devices	Up to 1000 devices
High Availability	Yes – Active-Passive Cluster		
Deployment	On-Premises		
Interfaces & Connectivity			
10/100/1000BASE-T Ethernet Ports	8 ports	6	6
1G SFP Port	1 port	2	2
10G SFP+ Ports	4 ports	2	2
1/10G SFP+ Ports*	4 ports	-	-
USB Ports	2 × USB 3.1	2 x USB 3.2 Gen1	2 x USB 3.2 Gen1
Management Port	1 port (dedicated OOB)		
Console Port	1 × Micro USB + 1 × RJ45 Serial	1 x RJ45 Serial	1 x RJ45 Serial
Physical Dimensions			
Form Factor	1U Rack-mount		
Dimensions (W × H × D)	430 × 44 × 400 mm	270 x 44 x 160 mm	270 x 44 x 160 mm
Weight	6.5 kg (14.3 lbs)	1.410 kg (3.11 lbs)	1.480 kg (3.26 lbs)
Environmental			
Operating Temperature	0°C – 40°C (32°F – 104°F)	0~ 40°C (32~104°F)	0~ 40°C (32~104°F)
Storage Temperature	-20°C – 80°C (-4°F – 176°F)	-20~80°C (-4~176°F)	-20~80°C (-4~176°F)
Relative Humidity	0% – 90% @ 90°C, non-condensing	0 to 90% @40°C, non-condensing	0 to 90% @40°C, non-condensing

Power Supply			
Power Source	1+1 Hot Swappable Redundant AT	12 V DC, 5 A Power Adapter	12 V DC, 3.34 A Power Adapter
Maximum Power Consumption	280W	60W	40W
Input Voltage Range	100V AC – 240V AC	100 V AC to 240 V AC	100 V AC to 240 V AC
Input Frequency	47 – 63 Hz	50-60 Hz	50-60 Hz

Virtual Specifications – Software Deployment

QNMS can be deployed as a virtual appliance or software instance on standard hypervisor or cloud-compatible infrastructure, offering flexibility for organizations without dedicated hardware.

Parameters	Model
Minimum VM Resource Requirements	
vCPU	4 cores
RAM	8 GB
Storage (OS + App)	100 GB
Network Interfaces	1 vNIC
Max Monitored Devices	Up to 500
High Availability (Virtual)	
HA Mode	Active-Passive cluster configuration
Failover	Automatic failover with cluster state management
Backup	Full system backup and restore from backup file
Storage HA	Shared storage or replicated volumes recommended