Management Efficiency

Optimize the steps and processes for operation, configuration, and management −more convenient and efficient.
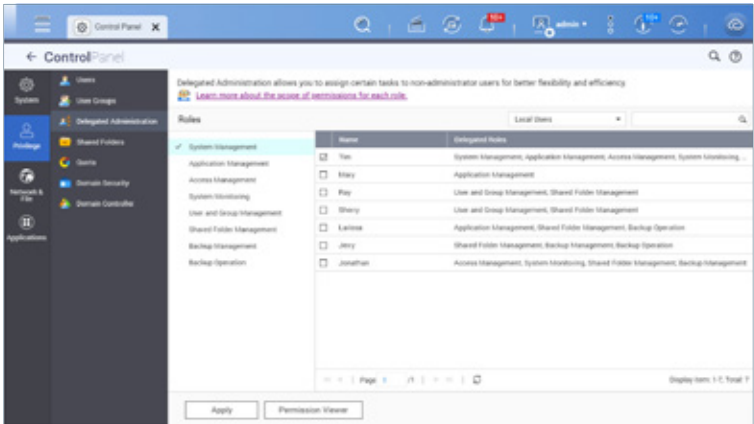
Backup/restore NAS system configuration with greater flexibility

The backup and restore feature for NAS system settings now offers enhanced flexibility, allowing users to select specific elements like network configurations or permissions settings to restore, ensuring more tailored and convenient system management.

	BEFORE	NOW
Back up system configuration:	A BIN file is generated and downloaded to your computer. The actual backup details are kept undisclosed.	▪ Backup content details, including system, network, and privilege settings, are provided. ▪ You can encrypt the backup file.
Restore system configuration:	▪ Restore using the BIN file. ▪ The destination NAS must be the same model and have the same QuTS hero version as the backup NAS.	▪ Perform selective restoration for specific items (such as permission settings, network configuration, and more). ▪ The destination NAS can be a different model and have different QuTS hero version than the backup NAS

More convenient AD domain login

QuTS hero h5.2 supports automatic matching of AD domain user accounts, eliminating the need to input the AD domain name again. Simply log in using a domain account to access the NAS.

Delegated administration improves management productivity and data security

NAS administrators can delegate 8 types of roles to other users with specified permissions to management tasks and NAS data. For growing organizations, role delegation helps ease management workloads without sacrificing data access controls.

Supports AES-128-GMAC for SMB signing acceleration

It greatly increases data signing efficiency over SMB 3.1.1 and enhances the CPU utilization of the NAS system. (Only applicable in Windows Server 2022 and Windows 11 clients)

QNAP Authenticator supports passwordless login

The QNAP Authenticator mobile app is available for setting up two-step log-in process to NAS accounts, including time-based one-time passwords, QR code scanning, and login approval. Passwordless login is also supported.

QNAP SYSTEMS, INC.

www.qnap.com

QNAP

High-performance ZFS-based operating system with greater reliability

The ZFS-based QuTS hero operating system not only prioritizes data integrity and security but also offers advantages in optimizing SSD applications that other file systems cannot match. QuTS hero NAS provides a variety of storage solutions that fully utilize the benefits of ZFS, including a rich selection of HDD+SSD hybrid storage models, assisting enterprises in seamlessly integrating them into their IT infrastructure.

Meets diverse business needs

Media and Entertainment production	Enterprises	Data Centers
QuTS hero inline data compression and deduplication enhances smooth video editing	QuTS hero empowers high-performance VDI and future-proofed disaster recovery planning	QuTS hero emphasizes data security, supports virtualization, and cloud integration

SMB Transmission

Faster access speed, better system performance.

Kernel Mode SMB Daemon acceleration technology

In high-speed SMB transmission environments, QuTS hero h5.2 can utilize the CPU's Kernel Mode to accelerate transfers while maintaining the necessary User Mode for other SMB functions. Coupled with enabling SMB Multichannel, performance takes another leap forward!

4 x 25GbE, Sequential Throughput (1M)

With Kernel Mode SMB Daemon

Read	Write
11265 MB/s	**11240** MB/s

Without Kernel Mode SMB Daemon

Read	Write
4173 MB/s	7178 MB/s

4 x 25GbE, Random IOPS (4K)

With Kernel Mode SMB Daemon

Read	Write
489451	**729304**

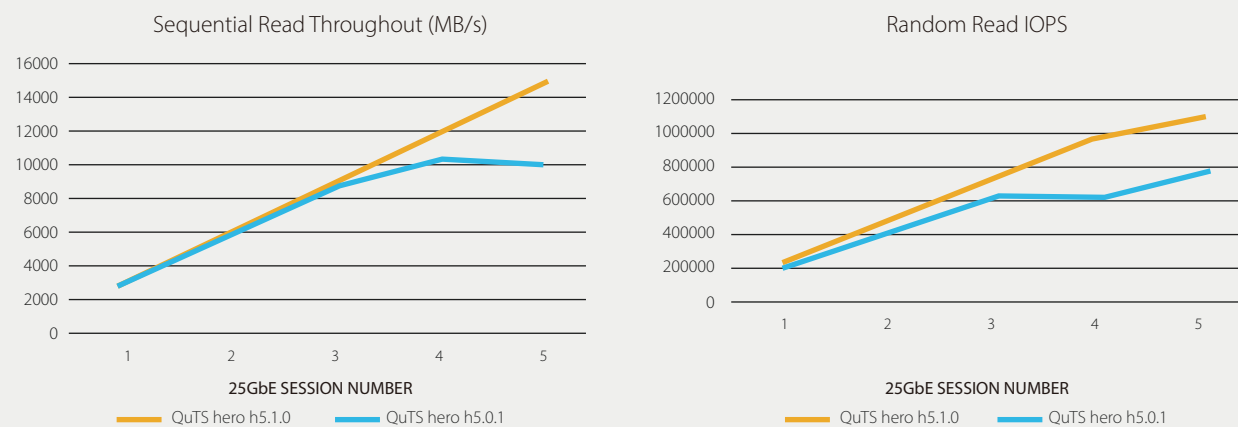**Without Kernel Mode SMB Daemon**

Read	Write
88979	159746

SMB multichannel for full throughput and multi-path protection

SMB multichannel aggregates multiple network connections to maximize available bandwidth with higher transfer speeds – especially ideal for large file and multimedia transfer. SMB multichannel also allows network fault tolerance to prevent service interruption.

Improved iSCSI read performance by socket zero-copy

In high-speed data transmission, iSCSI performance is possibly affected by CPU overhead. QuTS hero 5.1.0 supports socket zero-copy technology that significantly offloads CPU resources, thus improving read performance for iSCSI LUN.
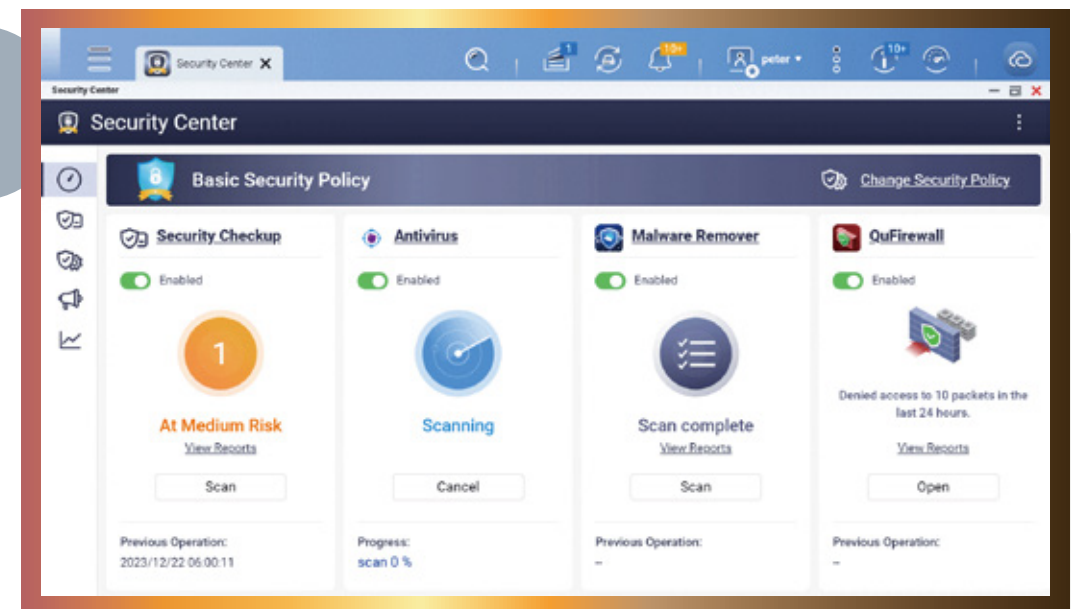
Sequential Read Throughout (MB/s)

25GbE SESSION NUMBER

— QuTS hero h5.1.0　　— QuTS hero h5.0.1

Random Read IOPS

25GbE SESSION NUMBER

— QuTS hero h5.1.0　　— QuTS hero h5.0.1

System & Data Security

Exponentially strengthen data safety with proactive defenses and security updates.

Security Center safeguards against ransomware threats

The Security Center actively defends against ransomware by monitoring file activities on the NAS. Upon detecting unusual activity, it swiftly implements protective actions—protecting, backing up, or blocking access—to significantly reduce the risk and impact of data loss from ransomware or other threats.

Supports SED with new TCG-Ruby standard

Enhances security by providing encryption for entire drives, complying with modern NVMe and other storage technologies. This aligns with enterprise and data center needs, ensuring adherence to regulations like GDPR, HIPAA, and HITECH.

WORM (Write Once, Read Many)

By enabling WORM, written data cannot be overwritten, modified, or deleted. This ensures the integrity and immutability of archived data for a specified period, making it suitable for specific use cases and compliance retention policies.

Enhanced performance of encrypted folders/LUNs

You can encrypt the contents of specific shared folders and LUNs to prevent unauthorized access. From QuTS hero, the performance of encrypted shared folders and LUNs has been greatly enhanced.

■ **Supports OpenSSL LTS 3.0.9**

Long-term support version. Ensures the security of network communication.

■ **Supports IEEE 802.1X**

Enables the NAS to access the network through 802.1X authentication in a secure environment.

■ **Implements AppArmor**

Enhances system security to mitigate security threats from both internal and external sources.

■ **Supports HTTP Strict Transport Security (HSTS)**

Forces browsers to use HTTPS connections, reducing the risk of connection hijacking.