

# QNAP NAS

## Information Security Manual

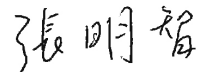


QNAP SYSTEMS, INC.

Thank you for using QNAP products and for entrusting your data to QNAP NAS for safekeeping. We greatly appreciate your support and consider your trust in us to be our most precious asset. To this end we strive for perfection by constantly improving our products and security.

In today's world with a growing number of attacks, malware, and security concerns, we felt the need to provide you with the following information to help you proactively defend yourself and your digital assets. We hope that by combining the advice in this guide with sensible IT usage habits that all of our users can protect their devices and data from current and emerging threats.

QNAP Systems, Inc.



General Manager

[www.qnap.com](http://www.qnap.com)

## Best practices for improving security

Data protection methods are constantly trying to keep pace with evolving hacking techniques. To keep their data and devices protected, NAS users have a lot of tools at their disposal – including password protection, permission settings, file level encryption, operating system and software updates, network connection settings, and apps for data backup and disaster recovery. QNAP products have information security features that are multi-faceted and robust. Below are nine (9) information security points to help our users quickly gain a basic understanding of information security.

1. Remove unknown or suspicious user accounts
2. Remove unknown or rarely used NAS applications
3. Disable automatic router settings in myQNAPcloud
4. Set up device access controls
5. Do not disclose the default port number on the Internet
6. Install and run the latest version of Malware Remover
7. Routinely change the passwords of every user account
8. Update installed applications to the latest versions
9. Ensure that the operating system and/or system software of your networked devices is always up to date

Later, we will explain QNAP's various information security designs one by one, and further build a comprehensive NAS defense plan.

## Use strong passwords

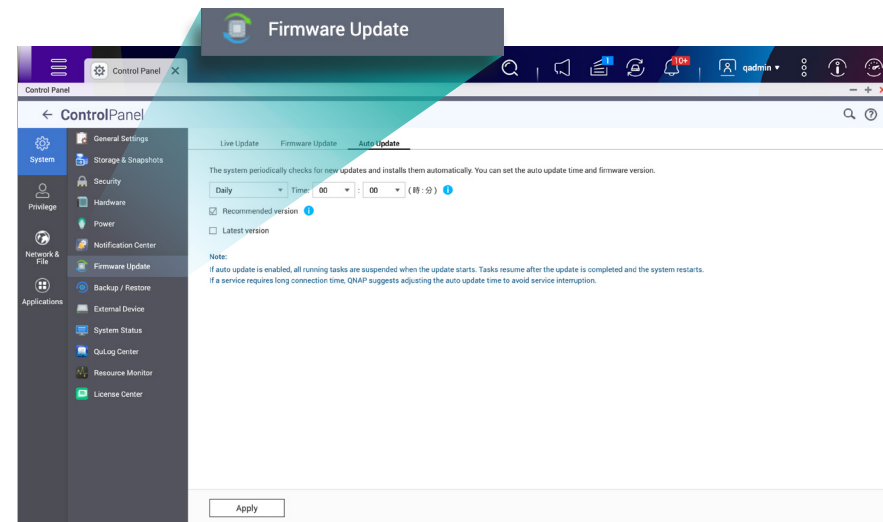
Attempting to access a user's account is the most common attack vector for hackers. This is usually carried out by hackers trying out default or common passwords, or by using social engineering (for example: if someone used a pet or child's name as a password, someone may be able to guess it). To mitigate the threat of a user account being compromised, we recommend disabling the default admin account and mandating that all users set strong passwords as described below.

Condition	Description
English letters	Include a mixture of uppercase and lowercase characters
Numbers	Include at least one number
Special characters	Include at least one special character (such as<ADD SPECIAL CHARACTERS HERE>)
Avoid repetition	Do not use repeated characters (such as AAA or 111)
Exclude user name	Do not use the username anywhere in the password, including backwards. For example, the user name is: W user1 and the password is: 1resu.
Minimum length	It is recommended to use a password of at least 8 characters. The maximum length of a password is 64 characters.

In addition to using strong passwords, users should also change their passwords periodically. You can specify the number of days a user's password is valid in the system settings.

## Software updates are important

Running out-of-date software on your NAS and other networked devices puts your entire network at risk. The QNAS development team actively monitors and patches potential security vulnerabilities as soon as they are discovered, and releases updates for the operating system and apps as soon as possible. We recommend that users keep their apps up to date in the App Center, and also enable automatic updates in the Firmware Update section of the QTS system. The QNAS website contains Release Notes that provide information on fixes and improvements made in new software versions.

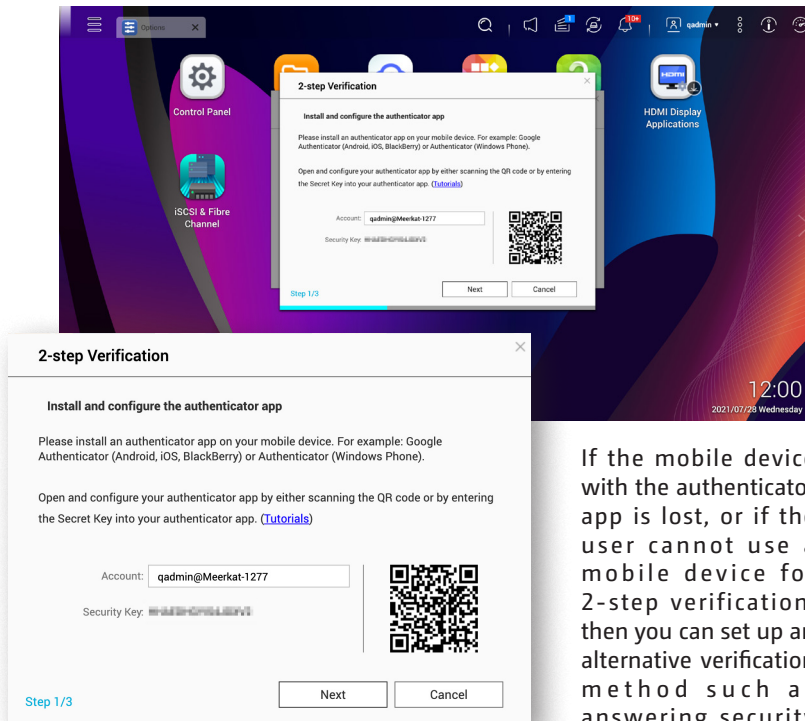


From QTS 4.5.3, the App Center will automatically update apps with new versions by default (NAS that cannot upgrade beyond QTS 4.5.3 can enable automatic updates using the console interface). If your NAS is not connected to the Internet, you can download updates from the QNAS Download Center and then manually install them on your NAS.

## Enable 2-step verification

2-step verification greatly enhances the security of user accounts. When enabled, users will be prompted to enter a code from an authenticator app on their mobile device before they can finish logging into their account. This adds an extra layer of security to user accounts that can greatly reduce the potential of hackers from unlawfully accessing user accounts.

To use 2-step verification, you must install a verification app on your mobile device. This app must use a time-based one-time password (TOTP) algorithm to build an authentication service. QTS supports Google Authenticator (Android, iOS and BlackBerry) and Authenticator (Windows Phone) for 2-step verification.



If the mobile device with the authenticator app is lost, or if the user cannot use a mobile device for 2-step verification, then you can set up an alternative verification method such as answering security questions or choosing to have a security code sent by email.

## Let us evaluate security for you

There are inherent security risks when connecting any device to the Internet, which is why QNAP have provided the Security Counselor app. This app audits the potential security vulnerabilities on your NAS and provides recommendations for system configuration adjustments to prevent your NAS from being compromised.

In Security Counselor you can specify different security level recommendations based on NAS usage requirements. Scans can also be performed on a scheduled basis. You can also adjust other settings, including IP blocking, security credentials, and password policies.

### Security Counselor



## Instantly remove threats

Regular scans can be helpful to see if your NAS has been affected by malware, with detected malware being removed. Malware Remover also automatically downloads the latest malware definitions to give you the greatest protection against new and emerging malware threats.

### Malware Remover



You can also configure the scan results of Malware Remover to be sent to QNAP, allowing us to update our malware definitions and to assist in strengthening the security of all QNAP NAS users.

## Install a security firewall for the NAS

Networked security threats do not differentiate between internal and external networks, and network-based firewalls (boundary) set up at the edge of local networks is insufficient at ensuring all-round security. Currently, the concept of Zero Trust Networks is becoming mainstream, and you can install and enable QuFirewall on QNAP devices to create a Host-Based firewall (micro-boundary) to protect your critical data and services.

### QuFirewall



QuFirewall is a free QNAP NAS app that allows you to set incoming network traffic rules to allow/deny connections and improve the security of Internet-connected NAS. QuFirewall also supports GeoIP, which can be used to detect and deny connections from specified geographic regions. For even greater protection, you can consider installing the popular open source firewall pfSense from Virtualization Station's Virtual Machine Marketplace.

## Do not leave your NAS exposed

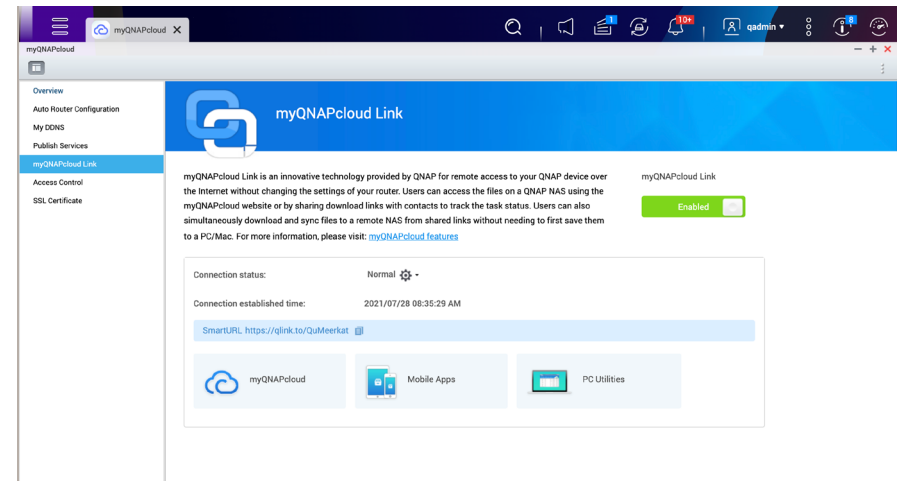
Your QNAP NAS is potentially vulnerable to snooping if it connects directly to the Internet unprotected. By using botnets or websites such as Shodan, attackers can potentially lock down devices and launch attacks. This is controlled in the port forwarding settings of routers and modems. If you enable manual forwarding, automatic port forwarding (UPnP; Universal Plug and Play) or demilitarized zone (DMZ), then your QNAP NAS is directly connected to the Internet. Direct connection to the Internet also occurs when the QNAP NAS obtains a public IP address directly (static/PPPoE/DHCP).

When you need to remotely access your NAS, the safest way is to establish a secure VPN connection or use the myQNAPcloud Link application. If you do not use these connection methods, you must install the QNAP NAS behind your router and firewall. If the NAS is behind a router but is connected to the Internet through port forwarding, you should specify a new port number on the router. Do not use port numbers such as 22, 443, 80, 8080, or 8081.

## Security tips for remote connections

One of the best things about NAS is universal access to your files and services from any device at any time. To make remote connection easier and more secure, we developed the myQNAPcloud Link application, which connects to your NAS (via P2P connection) so you can securely connect to NAS without requiring extra firewall settings or directly exposing the NAS.

Remotely connecting via DDNS services used to require tedious setup processes, but myQNAPcloud Link provides a simple remote connection that allows you to connect to your QNAP NAS wherever you are, just as if you were carrying it with you.



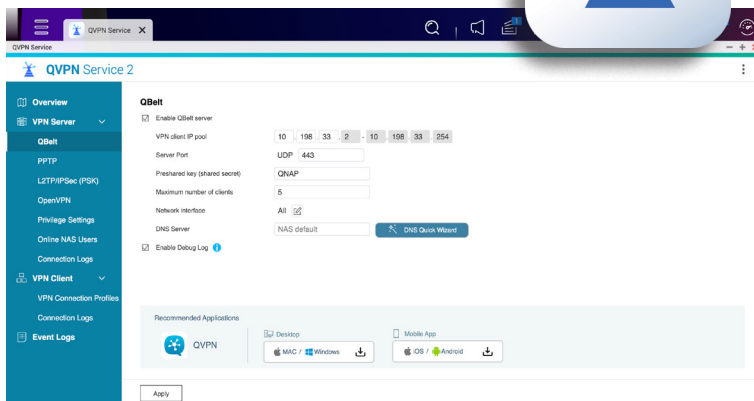


## Establish a secure VPN connection

In addition to the myQNAPcloud Link remote connection, setting up your own Virtual Private Network (VPN) server on your QNAP NAS using the QVPN Service provides a higher level of secure connection that allows for more secure communication between your devices and the NAS. In addition, you can also connect QNAP NAS to other VPN servers.

QBelt, QNAP's QVPN-exclusive VPN protocol, can further reduce the chance of VPN connections being detected. A computer or mobile device can use the QVPN Device Client to connect to the VPN server on the QNAP NAS or to the QuWAN service.

### QVPN Service



## Built-in security features

In addition to the many security-enhancing applications mentioned above, QNAP's NAS operating systems (QTS and QuTS hero) have a wide range of built-in security settings to add extra layers of protection to your NAS.

- **IP Blacklist and Whitelist:** Use the whitelist to restrict connections to authorized IP addresses only, while the blacklist can be used to automatically block certain IP addresses from connecting to the NAS.
- **Auto-blocking:** Set your NAS to block users/IP addresses that have failed to log in after a specified number of attempts. This is useful to prevent brute-force attacks and ensure device security.
- **HTTPS connection:** Enable an HTTPS connection to NAS and you can choose to encrypt your connection with a self-signed/myQNAPcloud/Let's Encrypt TLS certificate to ensure higher security.
- **Multiple backup solutions:** Fully back up your NAS in multiple ways, including with snapshots and backing up/syncing to a remote server or cloud storage service.
- **Permissions Control:** In addition to information security controls, setting folder permissions gives users more privacy, which not only ensures the security of confidential information, but also complies with regulatory requirements.
- **Logs and notifications:** The system has full built-in event logs and notifications, ensuring detailed traceability of operations and saving time for IT maintenance.

# Data Protection

## Install anti-virus software

In addition to the free ClamAV antivirus built into QTS, you can also purchase McAfee Antivirus, a well-known antivirus software, for advanced protection. QNAP users can manually or schedule scans to protect their data from viruses, repair files that have been infected, quarantine infected files, and receive the latest virus definitions to protect against new and emerging viruses. McAfee Antivirus licenses can be purchased in the QNAP Software Store with durations of up to 3 years.

## Remove unknown risks

User accounts should be monitored and modified based on your requirements. You should remove accounts that are no longer needed or revoke all its permissions if the account will be needed later. You can do this from "Control Panel" > "Permissions" > "Users". You should also monitor what apps users have installed and verify if they are needed after a user account is removed. If at any point you find a user account that you do not recognize or have no recollection of creating, then it should be removed immediately.

## McAfee Antivirus

Scan your NAS for malware either manually or on a schedule with the McAfee antivirus engine.

Essential	Pro	Premium
Antivirus Annual Subscription For NAS	Antivirus Bi-Yearly Subscription For NAS	Antivirus Tri-Yearly Subscription For NAS
USD \$25.00 /Year	USD \$50.00 /2 Years	USD \$70.00 /3 Years
<a href="#">SUBSCRIBE NOW</a>	<a href="#">SUBSCRIBE NOW</a>	<a href="#">SUBSCRIBE NOW</a>





## QNAP's security team is on standby around the clock

QNAP was certified in 2018 by MITRE, an international non-profit organization, as a CVE Numbering Authority. This enables QNAP to assign CVE identifiers for security issues in QNAP products. QNAP's Product Security Incident Response Team (PSIRT) receives real-time information security notifications from around the world, proactively investigates vulnerabilities, publicly discloses threats, and responds to vulnerability notifications within 24 hours of receiving them.

We recommend that users regularly check the QNAP Information Security Bulletin and subscribe to the QNAP Information Security Newsletter to get the most up-to-date information and updates. In the event of a security incident, follow the QNAP PSIRT team's recommended practices to help prevent a security incident from compromising your NAS.

Advisory	Status	Impact	CVE	Last Updated	Affected Product(s)
<b>Improper Access Control Vulnerability in Legacy HBS 3 (Hybrid Backup Sync)</b>  <b>QNAP SA ID:</b> QSA-21-19  <b>First Published:</b> 2021-07-06	Resolved	Critical	CVE-2021-28809	2021-07-06	Certain QNAP NAS
<b>Summary:</b> An improper access control vulnerability has been reported to affect certain legacy versions of HBS 3 (Hybrid Backup Sync). If exploited, this vulnerability allows attackers to compromise the security of the operating system. We have already fixed this vulnerability in the following versions of HBS 3 QTS 4.3.6... <a href="#">Learn More</a>					
Multiple Command Injection Vulnerabilities in QTS and QUTS hero	Resolved	Medium	CVE-2021-28802 CVE-2021-28804	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in QLog Center	Resolved	Medium	CVE-2020-36196	2021-06-25	Certain QNAP NAS
Stored XSS Vulnerability in Q-center	Resolved	Medium	CVE-2021-28803	2021-06-25	Certain QNAP NAS
XSS Vulnerability in QTS and QUTS hero	Resolved	Medium	CVE-2020-36194	2021-06-25	Certain QNAP NAS
DNSpoof Vulnerabilities in QTS	Resolved	Medium	CVE-2020-25684 CVE-2020-25685 CVE-2020-25686	2021-06-28	Certain QNAP NAS



## What should I do if my NAS is hit by an encryption attack?

Ransomware attacks can vary in their effects and attack vectors, so it is hard to set a recommended general response to an attack. To prepare against potential attacks, we strongly recommend following best practices for backup and disaster recovery: daily backups, save backups to multiple devices, use snapshots and snapshot backups. Also remember to subscribe to QNAP's information security newsletter to get the latest updates.

If you suspect that your NAS or other networked devices has been compromised (such as an abnormally high CPU usage caused by unknown applications/services, login failures, unknown files in folders, or unauthorized encryption of files) then you should immediately remove your NAS from your network and disconnect your network from the Internet. Your NAS should be then immediately shut down\*, and the QNAP Helpdesk contacted for further information. You should also verify the integrity of your backups and potentially check if they have been compromised.

The Malware Remover app can be used to potentially clear the malware from your system. Ensure that you are using the most up-to-date version of Malware Remover.

If you are using snapshots and have confirmed that your snapshot files are not affected, you can use the snapshot recovery feature to recover your valuable data.

\* In most cases, immediately shutting down the NAS when an attack is first detected is the best practice. Only a few encryption attacks can cause the NAS to lose the decryption key after shutting down. Users are advised to pay attention to the QNAP Information Security Bulletin.

## Information security is QNAP's top priority

QNAP's commitment to information security is uncompromising. We actively maintain information security and combine the strengths of our partners and the community to ensure the security of QNAP products for your peace of mind.



# QNAP SYSTEMS, INC.

TEL : +886-2-2641-2000 FAX: +886-2-2641-0555 Email: [qnapsales@qnap.com](mailto:qnapsales@qnap.com)

Address : 3F, No.22, Zhongxing Rd., Xizhi Dist., New Taipei City, 221, Taiwan

QNAP may make changes to specification and product descriptions at any time, without notice.

Copyright © 2021 QNAP Systems, Inc. All rights reserved.

QNAP® and other names of QNAP Products are proprietary marks or registered trademarks of QNAP Systems, Inc.

Other products and company names mentioned herein are trademarks of their respective holders.

## Netherlands (Warehouse Services)

Email: [nlsales@qnap.com](mailto:nlsales@qnap.com)

TEL: +31(0)107600830

## China

Email: [cnsales@qnap.com](mailto:cnsales@qnap.com)

TEL: +86-400-028-0079

## Japan

Email: [jpsales@qnap.com](mailto:jpsales@qnap.com)

FAX: 03-6435-9686

## US

Email: [usasales@qnap.com](mailto:usasales@qnap.com)

TEL: +1-909-595-2782

## India

Email: [indiasales@qnap.com](mailto:indiasales@qnap.com)

## France

Email: [frsales@qnap.com](mailto:frsales@qnap.com)

## Thailand

Email: [thsales@qnap.com](mailto:thsales@qnap.com)

TEL: +66-2-5415988

## Germany

Email: [desales@qnap.com](mailto:desales@qnap.com)