QNAP

2023

Security Guide

2023

Security Guide

INDEX

Avoid Exposing NAS to Internet

NAS Security Settings

Preface

QNAP attaches great importance to security. In the face of rising threats, QNAP has continuously improved hardware and software designs to provide users with solutions that are both secure and convenient.

QNAP's Product Security Incident Response Team (PSIRT) is responsible for handling security issues related to QNAP products. In addition to handling cyber security-related incidents, PSIRT also manages the reporting, investigation, remediation and announcement of vulnerabilities in various products.

QNAP is also committed to product security enhancements. In the past, products were designed to be more convenient and easier for users to set up and use. With increasing cyberattacks against networked devices in recent years, QNAP's product design perspective has also changed, and product design has shifted to Security by Design to serve as a gatekeeper for users and ensure that users can deal with related threats.

The tutorial will help users in setting up the NAS correctly to improve security. If you have any questions, contact our technical support team for assistance:

For product vulnerabilities and security-related incident information, refer to and subscribe to the QNAP Security Advisories:

https://www.qnap.com/go/security-advisories/

QNAP Customer Service:

https://service.qnap.com/

Common Attacks

To know how to defend against cyberattacks, you must know how they are launched. As far as attacks on NAS are concerned, most attacks are launched through the Internet. The attacks are mostly of two types: "password cracking" and "vulnerability attack". Here, "vulnerability attack" can be divided into "N-day" and "0-day".

"N-day" refers to exploiting a patched vulnerability to launch an attack, and most of the current active attacks fall into this category. You can effectively defend against such attacks by ensuring you always install the latest security patches and updates.

"0-day" means exploiting an unknown vulnerability to launch an attack, and vendors can only issue security patches after the fact. These attacks can only be effectively defended by preventing attackers from connecting to the device.

The following table shows the responses to different attacks for users' reference.

Response	Attacks		
	Password Cracking	Vulnerability Attack (N-day)	Vulnerability Attack (0-day)
Avoid Exposure to Internet	V	V	V
Update Software (System and Apps)	X	V	Δ
Enable Automatic Update (System and Apps)	X	V	Δ
Use Strong Passwords for All Accounts	V	X	X
Disable Default "admin" Account	V	X	X
Enable 2-Step Verification	V	X	X
Enable Access Protection	Δ	X	X
Enable Firewall	Δ	Δ	Δ
Receive System Notifications	Δ	Δ	Δ
Change Default Ports	Δ	Δ	Δ
Disable/Remove Unnecessary Functions	Δ	Δ	Δ

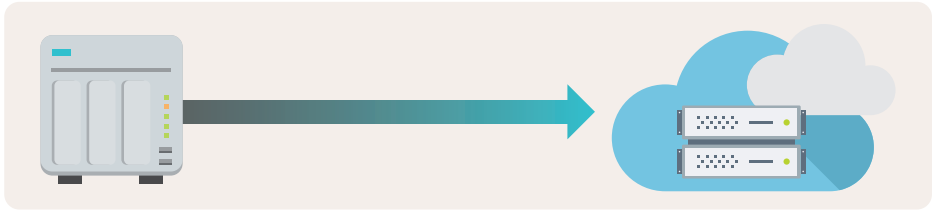
V: Effective X: Not effective Δ: Possibly effective (means that the attack can be mitigated or the risk of being attacked lowered)

"Avoid Exposure to Internet" can effectively prevent attackers from connecting to and launching attacks on your device. This tutorial starts with "Avoid Exposure to Internet", and then provides a complete "NAS Security Settings" tutorial to improve NAS defensive capabilities.

Basic Network Equipment Concepts

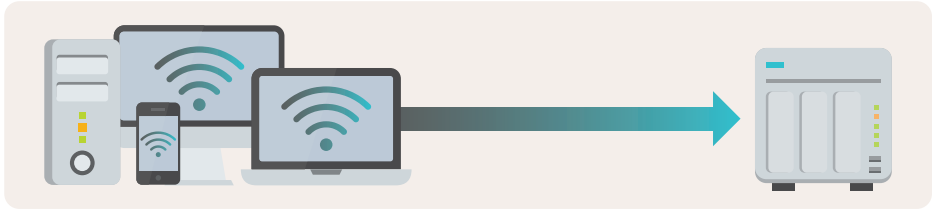
As a networked device, NAS have two connection directions.

01 | NAS external connection



A NAS generally requires external connectivity to function properly. For example, basic system functions such as automatic updates and sending notifications. In addition, In addition, if you need to back up NAS data to a public cloud, or use the NAS to back up data from other devices or public clouds (such as virtual machines, Google Workspace, or Microsoft 365), computers or servers, the NAS must be able to initiate outgoing connections.

02 | Other Devices (Such as Computers, Mobiles, or Other Servers) Connecting To NAS



If you need to use any functions or services provided by the NAS, including accessing files, entering the settings interface, you must be able to initiate connections to the NAS.

If your router does not have a DMZ, Port Forwarding or UPnP, the router will block the traffic from the Internet. Only devices on the local network will be able to access the NAS.

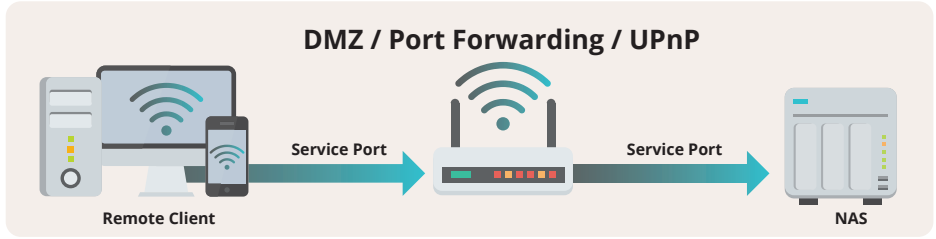
When the router is enabled and the above functions are set, everyone on the Internet can connect to the open port, and then forward to the NAS according to the rules on the router, and then log in and use the related functions normally. However, it will also provider hackers with the means to attack with password cracking or exploitation of software vulnerabilities, thus posing security risks.

Various Ways to Remotely Connect to NAS

01 | Enable and configure DMZ, Port Forwarding or UPnP on the router

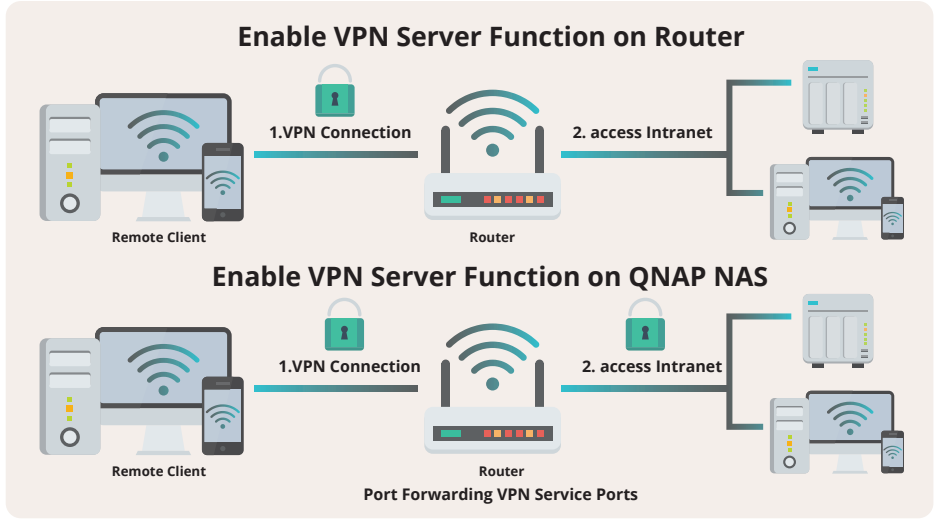
This method has security risks. Unless you are an expert in network configuration and understand the risks involved, QNAP does not recommend using it*. Since the router will pass traffic to intranet devices, if there is no firewall installed between the router and the NAS to block malicious traffic, hackers can easily launch network attacks. However, even if a firewall is installed (by using a basic firewall or purchasing an enterprise-grade firewall) it is not guaranteed to block every attack.

* QNAP only recommends opening relatively low-risk VPN service ports to the Internet, while other high-risk service ports such as system management, SMB, and SSH services should not be easily accessible from the Internet.



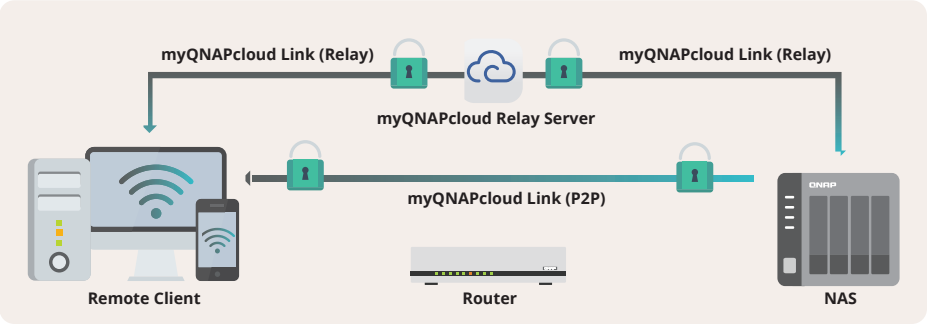
02 | Enable VPN Server Function on Router or QNAP NAS

Some routers support VPN server functions (such as QNAP QHora and QMiro series routers), while QNAP NAS also supports multiple VPN servers. Once enabled and properly configured, you can access each device on the intranet with a VPN-encrypted connection from the Internet to the VPN server, providing a high level of security.



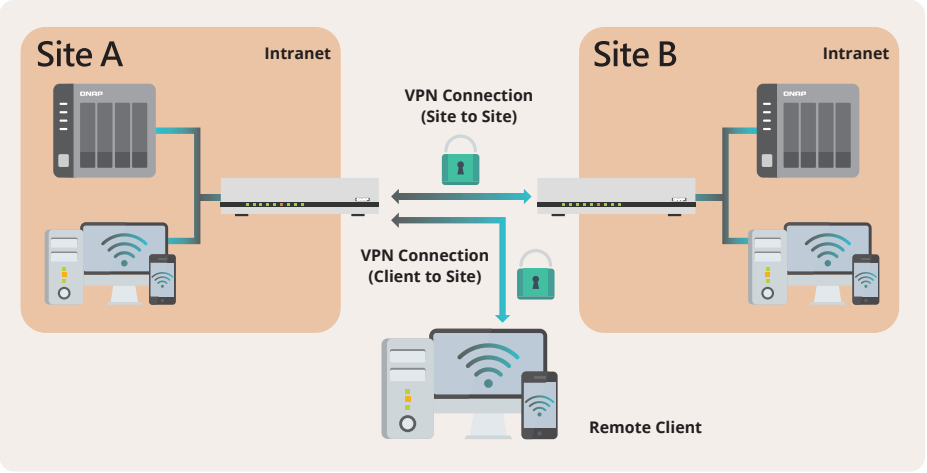
03 | Use myQNAPcloud Link Secure Connection

Router setup is not required if you use myQNAPcloud Link to connect to NAS, as it can open the NAS service directly to the Internet. myQNAPcloud Link will establish a connection through a relay server or peer-to-peer technology (P2P) according to the network environment. The entire connection will be encrypted to ensure security.



04 | Use SD-WAN or Site-to-Site VPN Products

Unlike the VPN server function (Client-to-Site VPN) mentioned above, SD-WAN or Site-to-Site VPN establishes secure encrypted VPN connection between two or more routers in different locations. Simply put, devices on a Site-to-Site VPN network can be connected to each other as if they were on the same intranet, making it ideal for users with multiple locations. With Client-to-Site VPN, you can access your NAS from anywhere.



You can choose a connection method that suits you according to the comparison table. QNAP has multiple secure connection solutions to meet the needs of users.

Connection Method	Advantages	Disadvantages	Suitable Users
Enable and configure the router DMZ/Port Forwarding of UPnP	• Fastest connection	• Vulnerable to cyber attacks • No defense against 0-Day vulnerability attacks	• Have a clear understanding of the associated risks • Familiar with network settings • Have created multiple backups for important data • Have a disaster recovery plan
Enable VPN server on the router*	• Relatively simple to set up	• No login failure notification, auto-blocking, and firewall function • Fewer VPN protocols supported • Performance limited by router hardware	• Not familiar with network settings • Not care about transmission speed
Enable VPN server function on QNAP NAS*	• Supports multiple VPN protocols • Compatible with NAS firewall (QuFirewall) • Supports login failure notification and auto-blocking	• Settings are slightly more complicated	• Familiar with network settings • Need to frequently access many files from the Internet
Use myQNAPcloud Link secure connection	• Easiest to set up • Support access control • NAS does not need to be exposed to the Internet	• Slower connection	• Not familiar with network settings • Infrequently access the NAS from the Internet • Network environment where WAN IP address cannot be obtained
Use SD-WAN or Site-to-Site VPN products*	• Once set up, intranet users can use it without feeling any difference • Also supports Client-to-Site VPN	• Additional equipment required	• Requires multi-point access and remote backup • Requires value-added applications

*** QNAP NAS supports:**

myQNAPcloud Link / VPN Servers (L2TP/IPsec, OpenVPN, WireGuard, QBelt) /QuWAN SD-WAN

*** QNAP Router Supports:**

QuWAN SD-WAN / VPN Servers (L2TP/IPsec, OpenVPN, WireGuard, QBelt)

Refers to general home routers

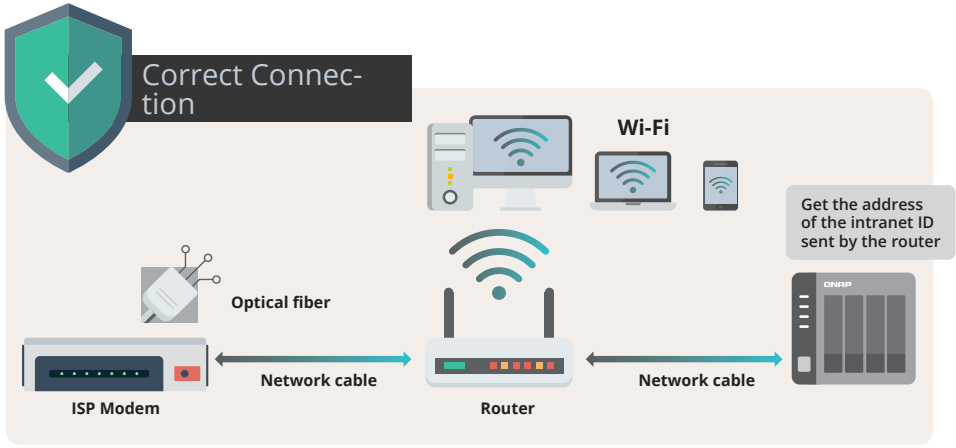
01

NAS Security Settings Guide

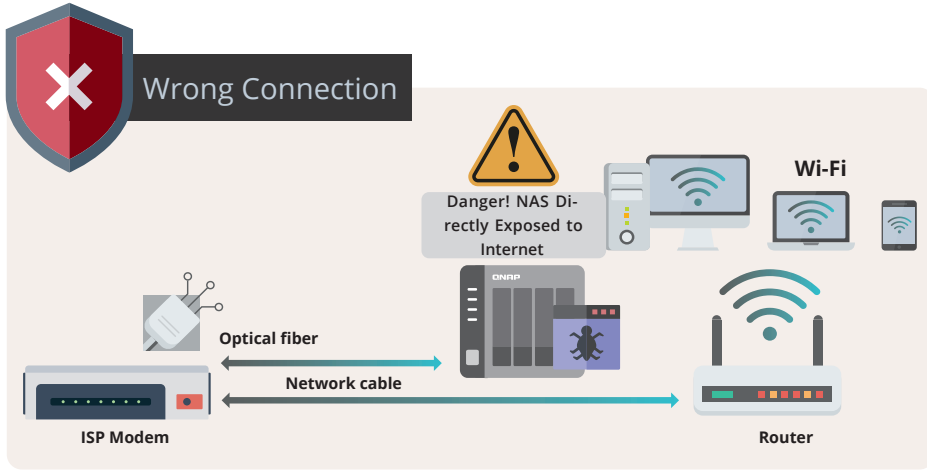
Avoid Exposing NAS to Internet

Connect NAS Correctly

Please make sure your NAS is connected to the router. With proper setup, the router can block connections from the Internet for you, allowing your NAS to hide from the Internet and avoid cyber attacks.



If you connect the NAS to the modem provided by the ISP, your NAS will obtain the WAN IP address directly. In this case, anyone (including hackers) can connect to your NAS via the Internet, and even try to attack and intrude.

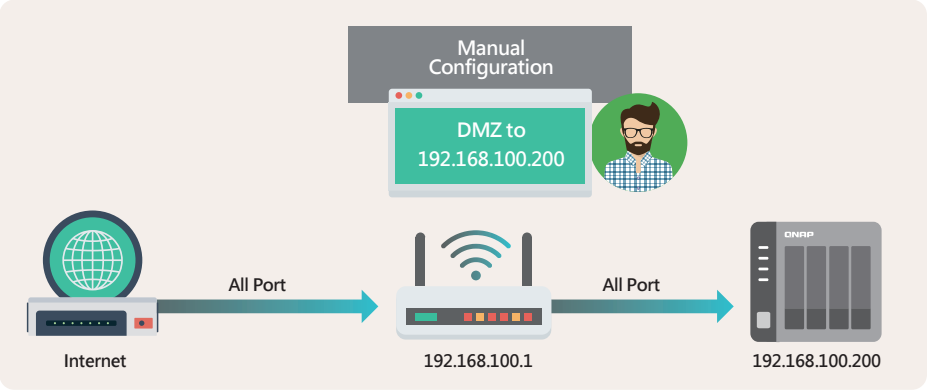


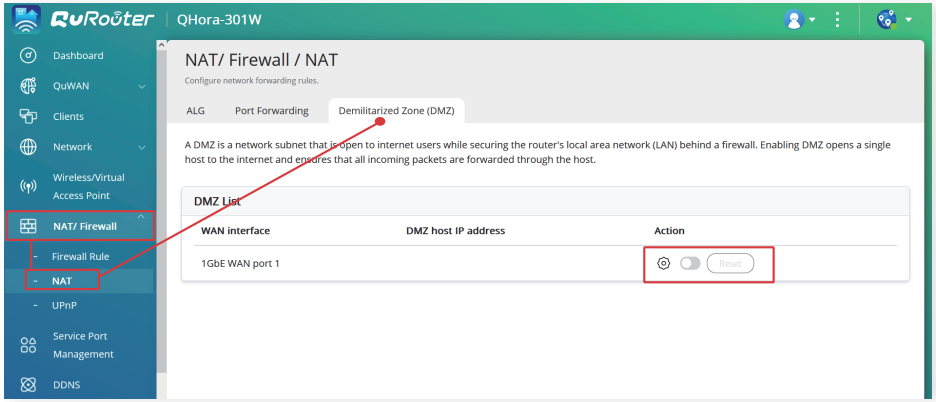
Check Router Settings

By default, theoretically no one can connect directly from the Internet to your device behind the router, but if you enable "DMZ (Demilitarized Zone)", "Port Forwarding" or "UPnP (Universal Plug and Play)", your router will forward packets to your selected device according to the rules you set, thus exposing your device to the Internet. If not needed, you should check and ensure that the following functions are disabled.

01 | Check DMZ (Demilitarized Zone)

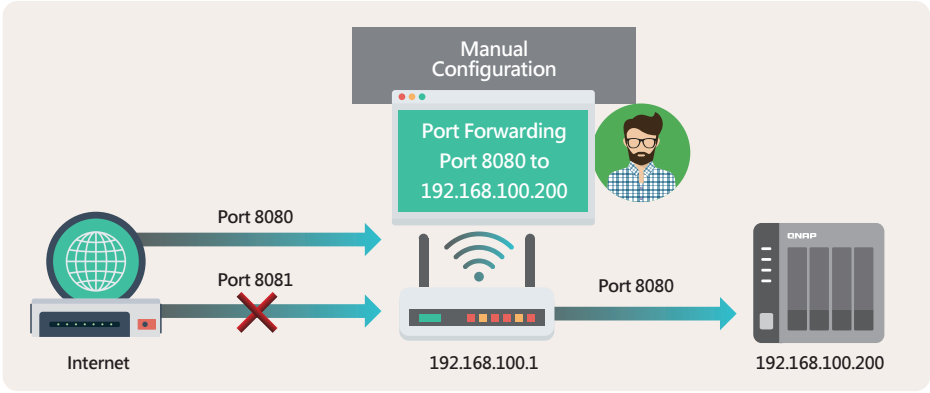
After enabling this function, all service ports of the device you have selected will be directly open to the Internet, that is, fully exposed to the Internet. To reduce security risks, disable this function.

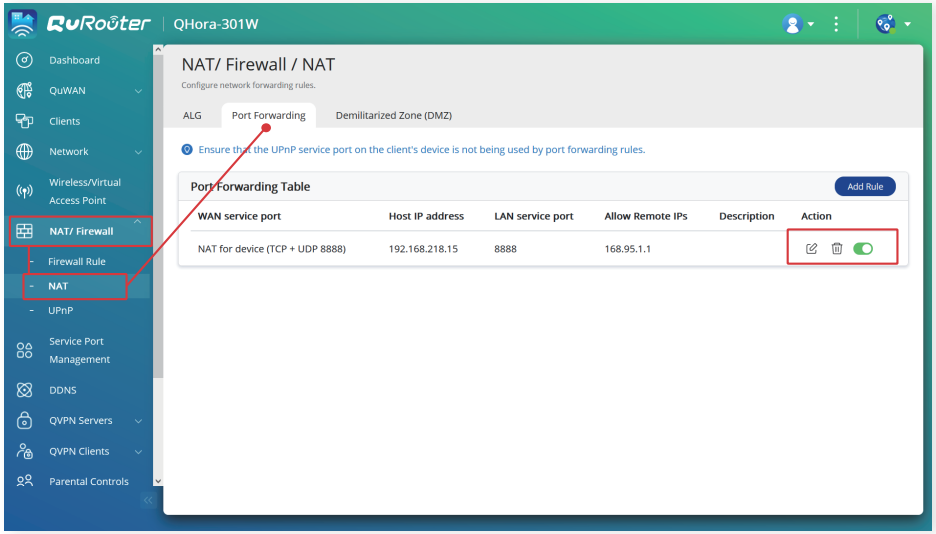




02 | Check Port Forwarding

This function allows you to open a specific service port on a device to the Internet, allowing anyone to access related services through the Internet. However, hackers can also launch attacks against open services from the Internet. Therefore, it is recommended to disable all port forwarding rules first, then set up NAS security settings, and then back up important data before using this feature to open some essential services to the Internet.

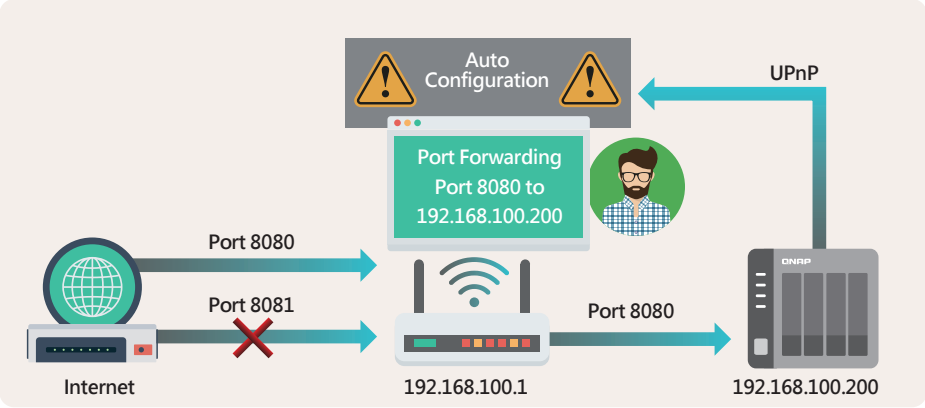


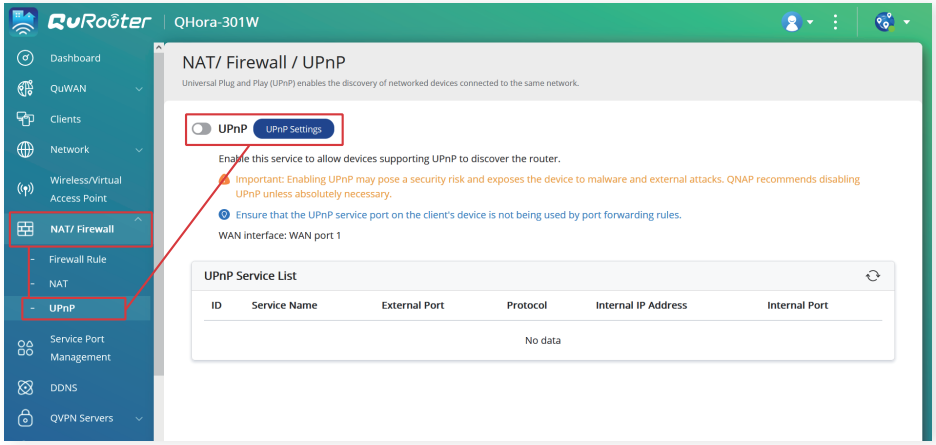


Check NAS Settings

03 | Check UPnP (Universal Plug and Play)

This function is equivalent to automatic port forwarding. After enabling this function, your device can automatically configure port forwarding using the relevant protocol. This function has serious security risks as it may expose your services to the Internet without your knowledge, or be exploited by hackers to open backdoors, so you should disable this function to improve security.





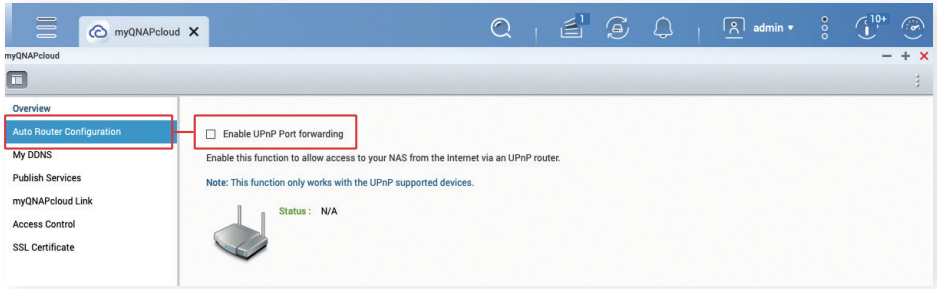
01 | Auto Router Configuration, UPnP Port Forwarding

Since some routers do not support disabling the UPnP function, please check the "Auto Router Configuration" setting on the NAS at the same time to ensure that this function is disabled.

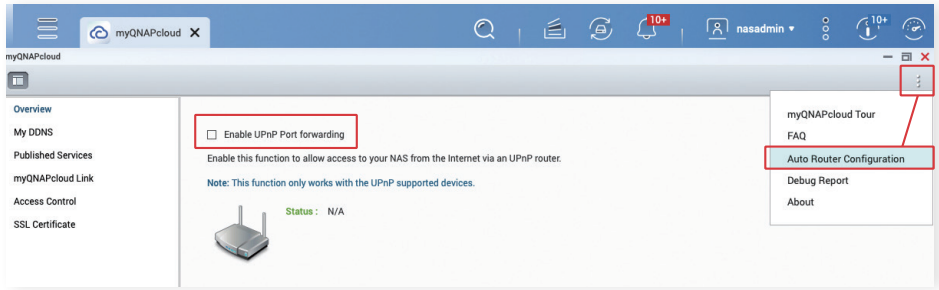
* This function is disabled by default from QTS 4.5.0 / QuTS hero h4.5.3 onwards.

To disable the "Auto Router Configuration" function:

1. Log in to the QTS / QuTS hero web management interface using an administrator account.
2. Open the menu in the top-left corner of the management interface and click "myQNAPcloud"
3. **QTS 5.0.0 / QuTS hero h5.0.0** or **Earlier:** Click "Auto Router Configuration" on the left menu



QTS 5.0.1 / QuTS hero h5.0.1 or **Later:** Click the menu icon ⋮ in the top-right corner and select "Auto Router Configuration"



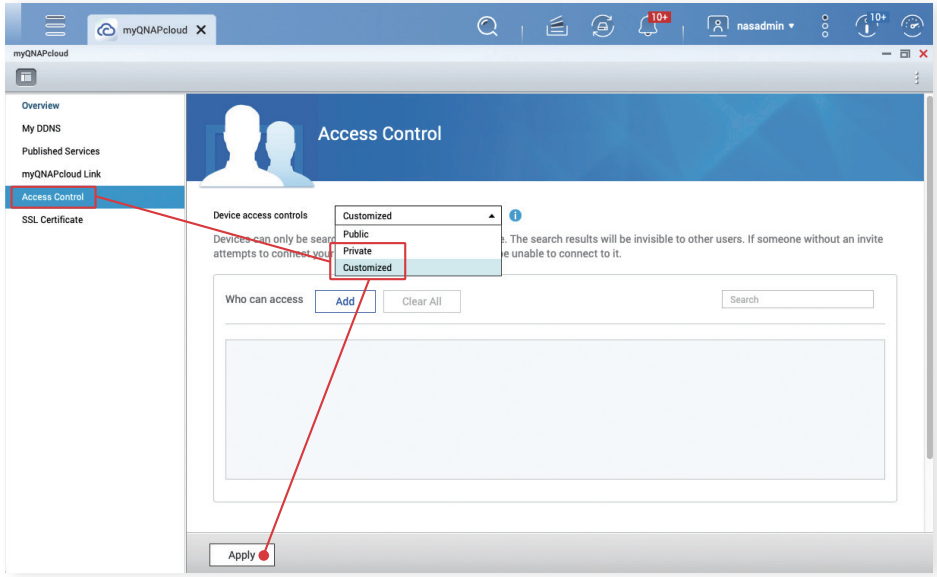
4. On the "Auto Router Configuration" settings page, uncheck "Enable UPnP Port Forwarding" and click "Apply".

02 | myQNAPcloud Link Access Control

myQNAPcloud Link is a secure connection cloud service provided by QNAP. Users can connect to their QNAP NAS through their chosen myQNAPcloud device name. myQNAPcloud Link provides access control settings. When the access control is set to "Public", anyone who knows your device name can use myQNAPcloud Link to connect to your NAS. Therefore, we recommend setting the access control to "Private" or "Customized". In both modes, users must log in to their QNAP ID in the Allowed Access List before they can use the myQNAPcloud Link to securely connect to cloud services.

* The default setting in Q TS 4.5.0 / Qu TS hero h4.5.3 (or later) is "Customized"

1. Log in to the QTS / QuTS hero web management interface using an administrator account
2. Click the menu in the top-left corner of the management interface, click "myQNAPcloud"
3. Click "Access Control" on the left side menu
4. On the "Access Control" settings page, set "Device access controls" to "Private" or "Customized", and then click "Apply".



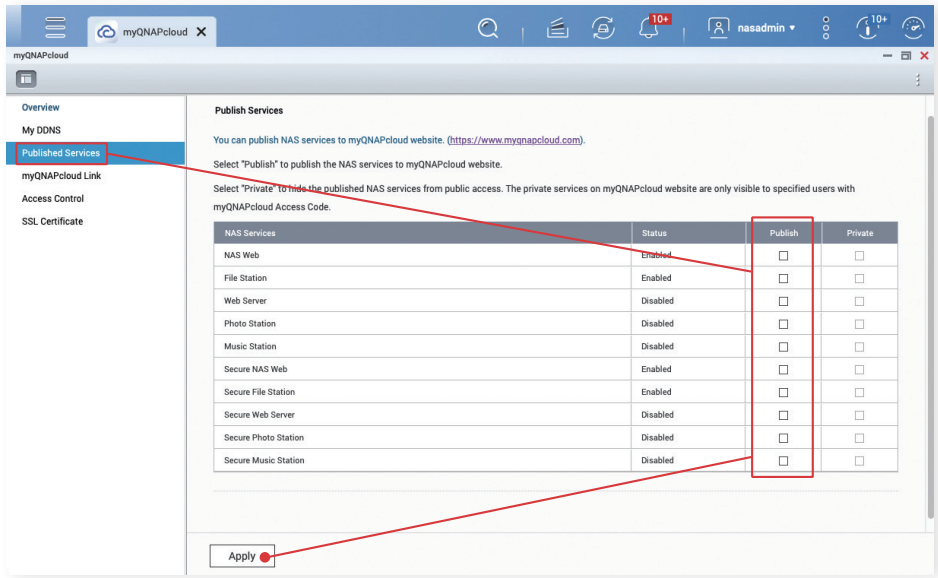
03 | Published Services

Published services can make it easier for users to use related functions on the myQNAPcloud website, but it also increases security risks. If you do not need to use this function, it is recommended to disable it to improve security.

* This function is disabled by default from QTS 4.5.0 / QuTS hero h4.5.3 onwards

"Published Services" Function:

1. Log in to the QTS / QuTS hero web management interface using an administrator account
2. Click the menu in the top-left corner of the management interface, click "myQNAPcloud"
3. Click "Published Services" on the left side menu
4. In the "Publish" field, uncheck all and click "Apply".



Network Settings Checklist

Hardware Related

☐ NAS is connected behind a router

☐ NAS obtains intranet IP address

Router

☐ Disable router "DMZ" function

☐ Disable router "Port Forwarding" rule

☐ Disable router "UPnP" function

NAS

☐ Disable the NAS "Auto Router Configuration UPnP Port Forwarding" function

☐ Set NAS "myQNAPcloud Link Access Control" to "Private" or "Customized"

☐ Disable the "Published Services" function

After checking and applying the above settings, your QNAP NAS will not be exposed to the Internet, and the risks of being attacked by hackers are greatly reduced. Please read on and check the rest of the settings to strengthen the QNAP NAS.

If you need to access NAS over the Internet, you can consider these three secure alternatives:

myQNAPcloud Link

Learn more

QVPN Service

Learn more

QuWAN SD-WAN

Learn more

02

NAS Security Settings Guide

NAS Security Settings

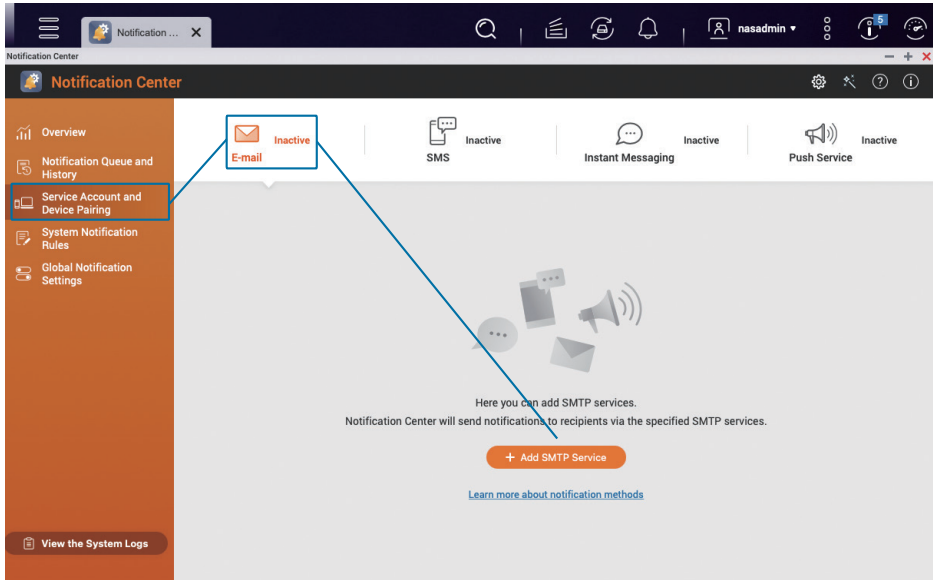
Set Up System Notifications

The built-in Notification Center can push notifications based on your settings, allowing users to keep track of the NAS status and react to abnormalities as soon as they are detected.

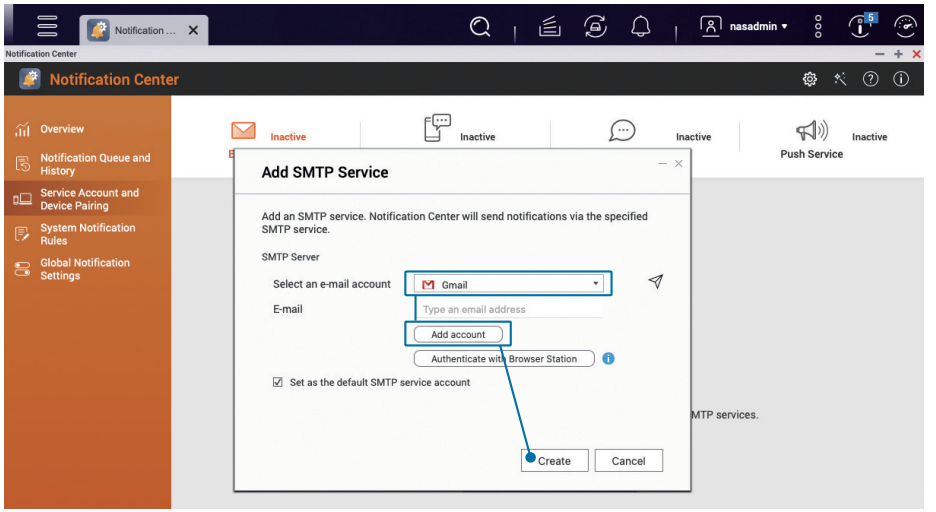
The following tutorial will teach you how to create two basic rules for "Email" to send "Alert Notifications" and "Firmware Update", and to add more rules if needed.

01 | Add "Email" Notification Method

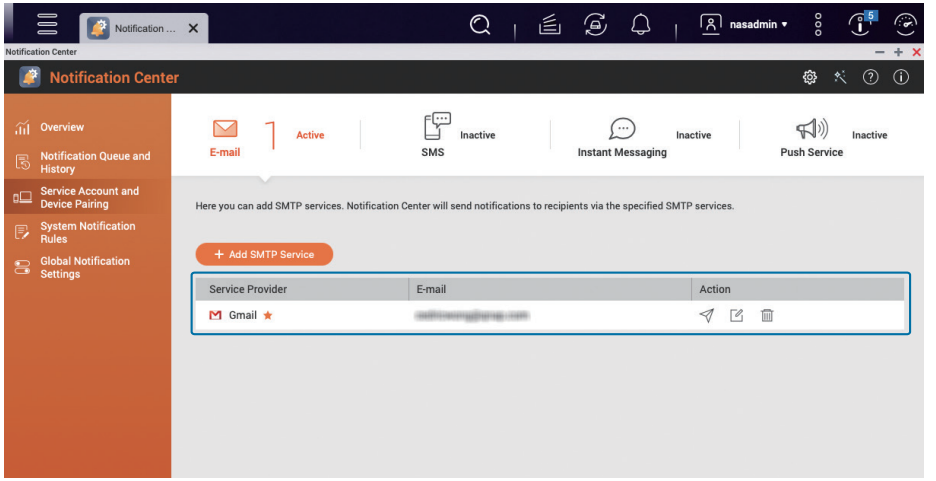
Open "Notification Center", click "Service Account and Device Pairing" on the left side menu, select "Email", and then click "Add SMTP Service"



Select an email account (the following uses Gmail as an example), click "Add Account", follow the instructions to complete the Gmail verification process, and click "Create" after the verification is complete.

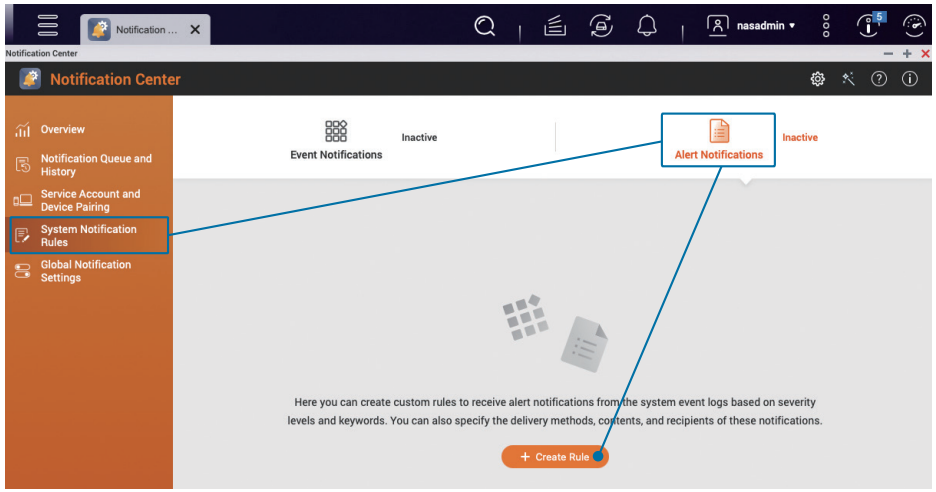


⇩⇩ Once created, you'll see the email account you've added in the list.

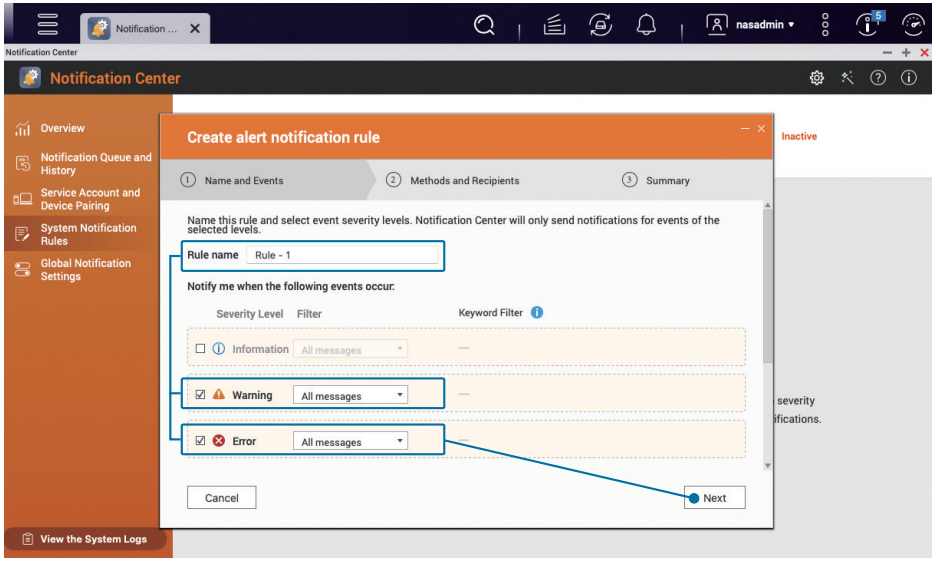


02 | Set Up "Alert Notifications"

On the left side menu of "Notification Center", click "System Notification Rules", select "Alert Notifications", and click "Create Rule".

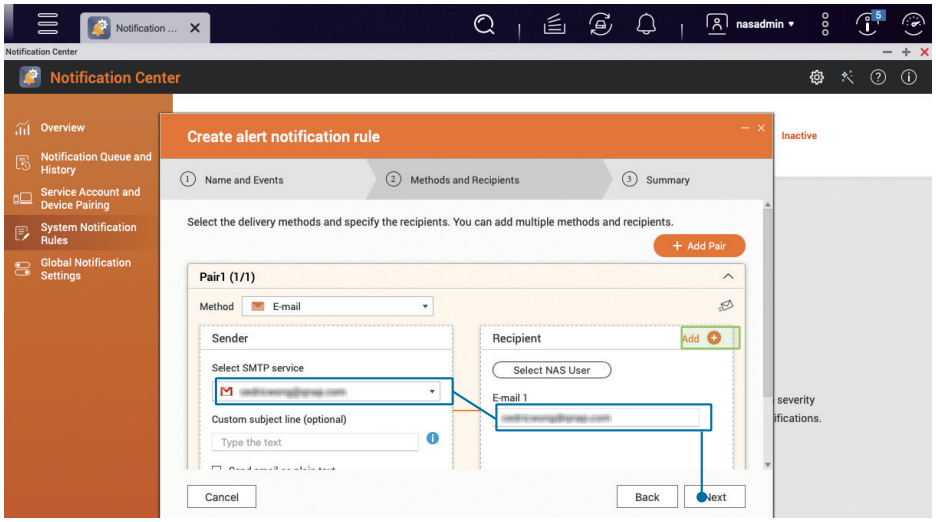


Modify the "Rule Name" according to your needs, check the two severity levels of "Warning" and "Error", and click "Next".

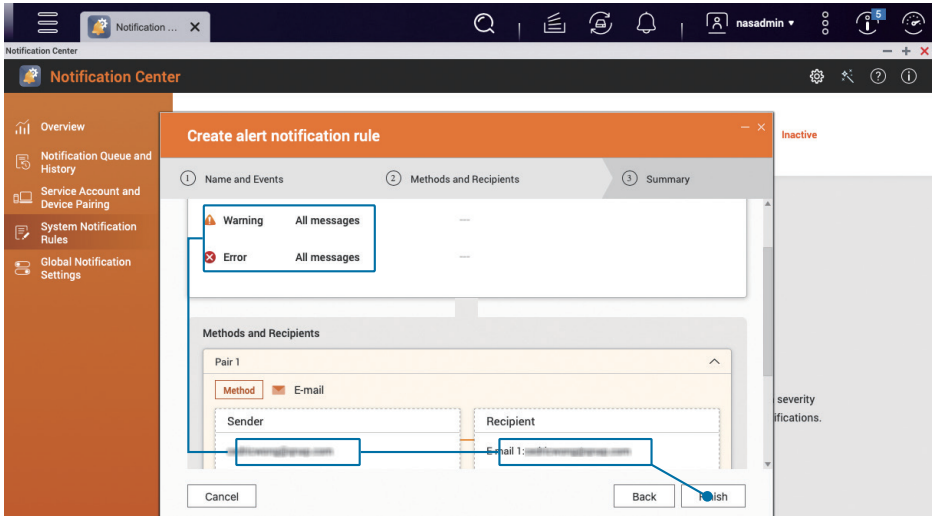


Set the delivery method and set the recipient, select the email account you just added as the "Sender" in the pairing, and then enter the "Email Address" of the "Recipient", and then click "Next".

If necessary, you can enter multiple recipients by clicking "Add ⊕" next to "Recipient". You can also "Add Pair" to send notifications in multiple ways at the same time.

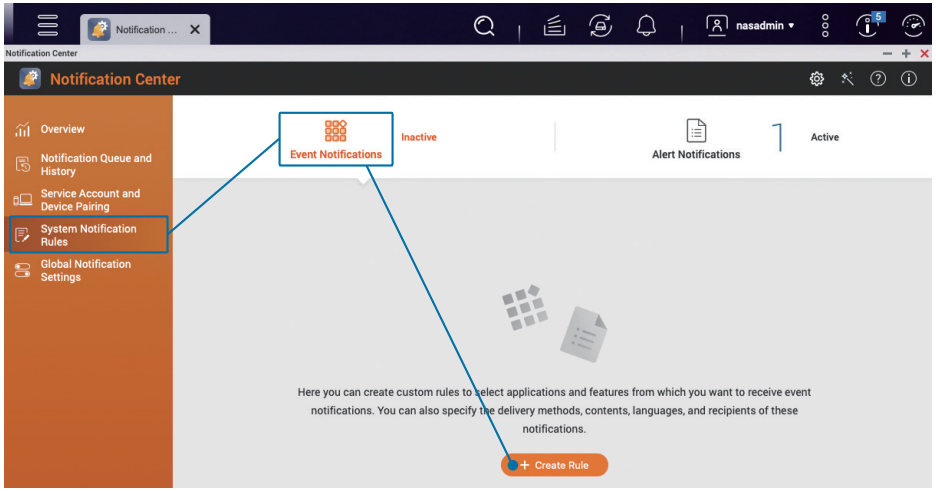


After confirming that the settings are correct, click "Finish" and the "Alert Notifications" settings will be complete.

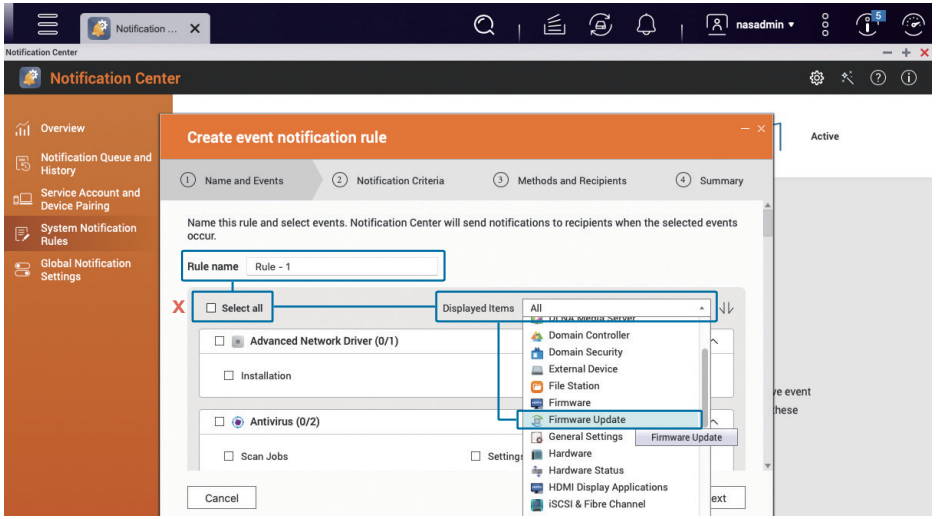


03 | Configure "Firmware Update" Notifications

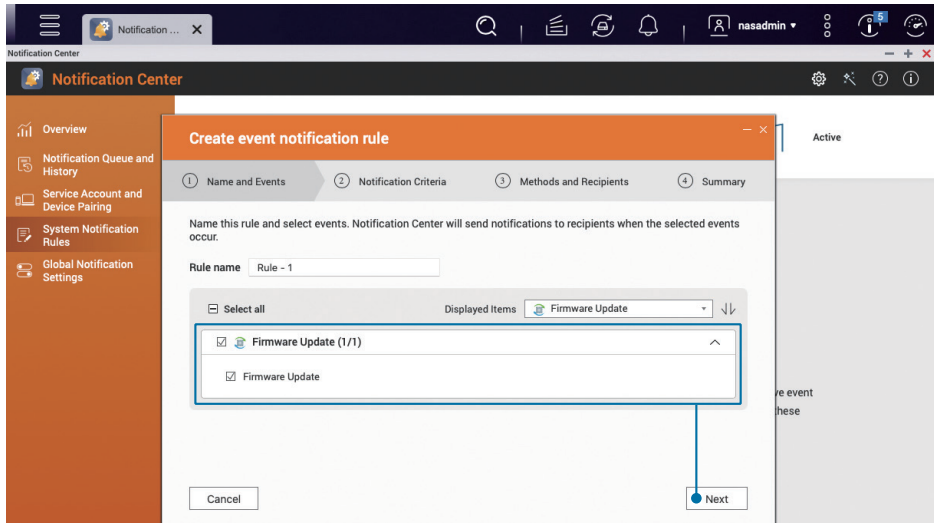
Click "System Notification Rules" on the left side menu of "Notification Center", select "Event Notifications", and then click "Create Rule".



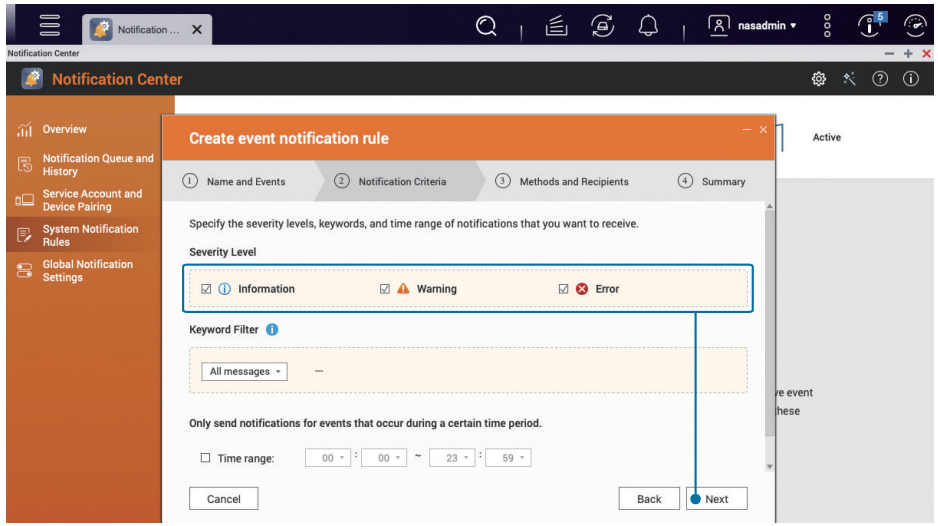
Modify the "Rule Name" according to your needs, uncheck "Select All", then select "Firmware Update" in the "Displayed Items" on the left, and then select the "Firmware Update" option below.



Check the "Firmware Update" option and click "Next".



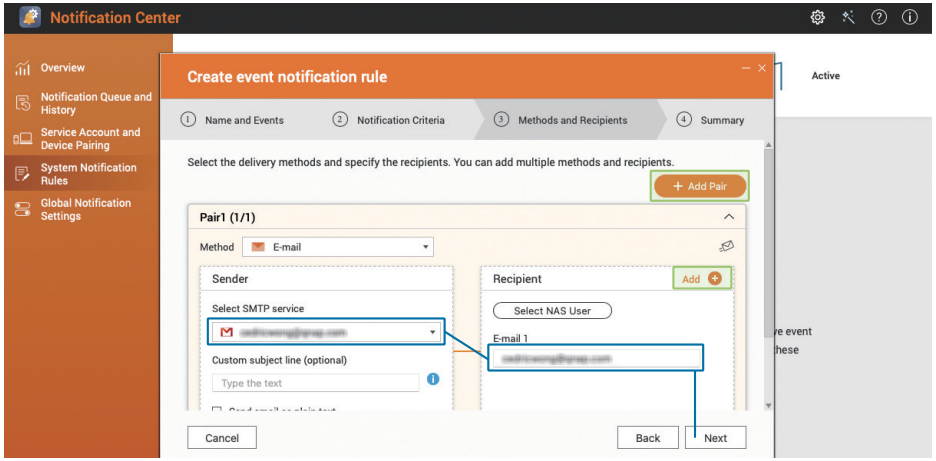
Check all severity levels, including "Information", "Warning" and "Error", click "Next".



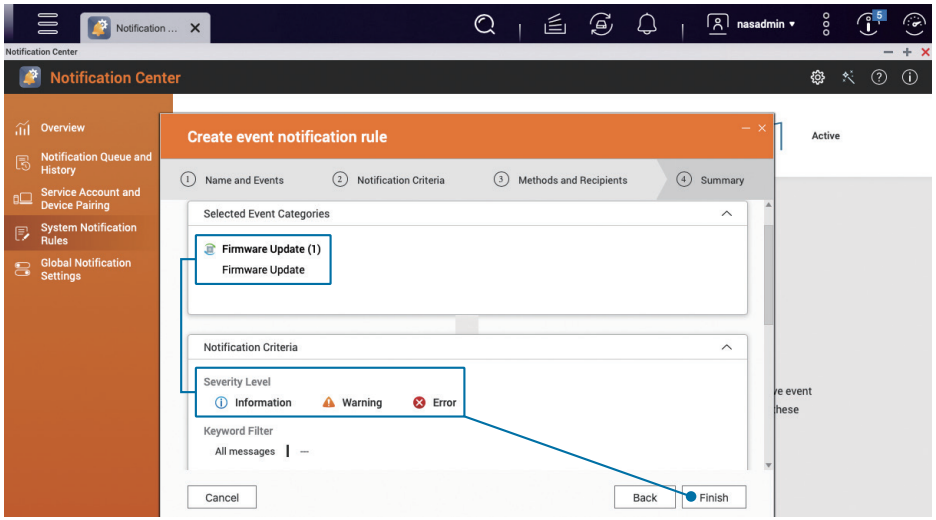
Enable Firmware (QTS / QuTS hero) Automatic Update

Set the delivery method and set the recipient. Since only the "Email" notification is currently set, select the email account you just added as the "Sender" in the pairing, and then enter the "Email address" of the "Recipient", and then click "Next".

If necessary, you can enter multiple recipients by clicking "Add ⊕ " next to "Recipient". You can also "Add Pair" to send notifications in multiple ways at the same time.

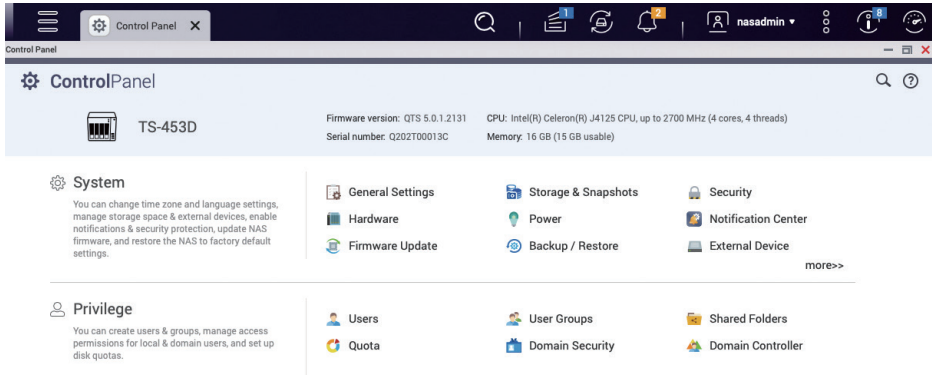


After confirming that the settings are correct, click "Finish" to complete the setting of "Firmware Update".



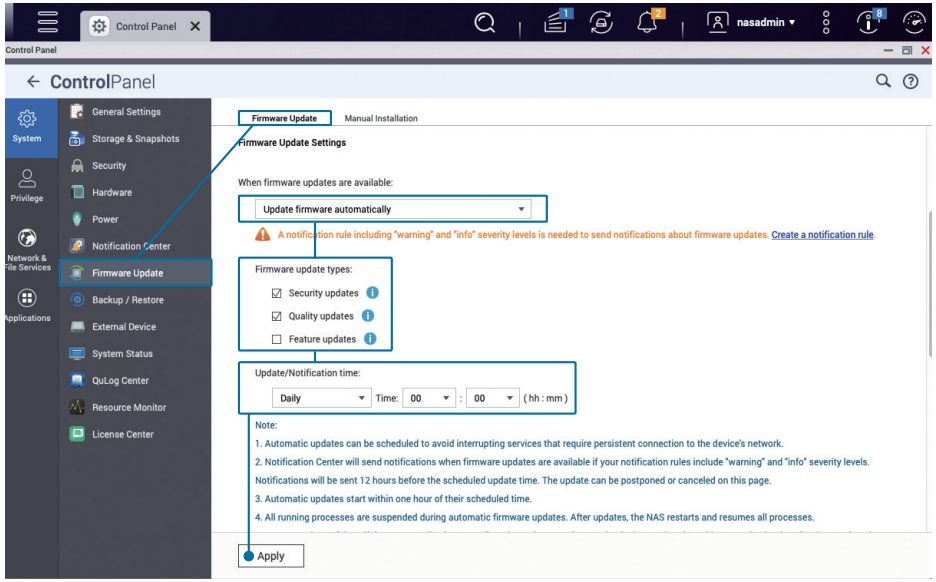
The automatic update function makes it easier to install updates for new features, bug fixes and vulnerabilities.

Open "Control Panel" and click "Firmware Update".



In "Firmware Update Settings", select "Update Firmware Automatically", and check "Security Updates" and "Quality Updates"; for "Update/Notification Time", it is recommended to set an off-peak time such as "00 : 00", and then click Apply.

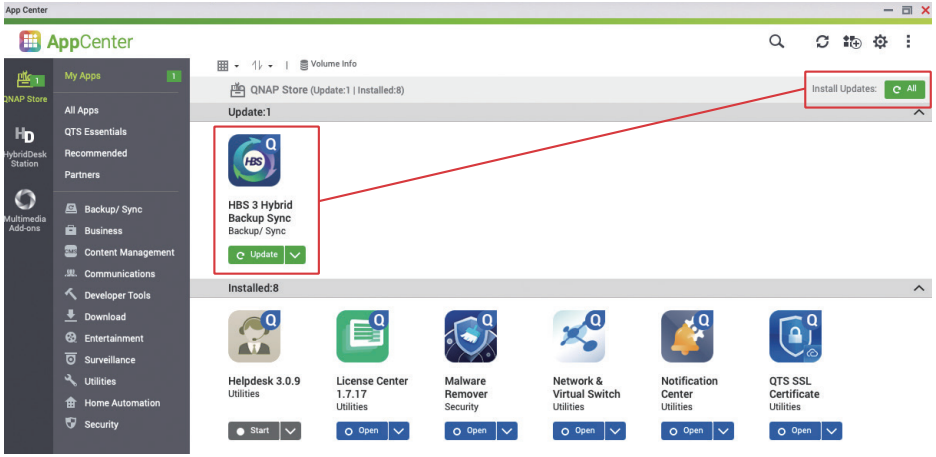
* For QTS 5.0.0 / QuTS hero h5.0.0 (or earlier), check "Recommended Version" on the "Automatic Update" page



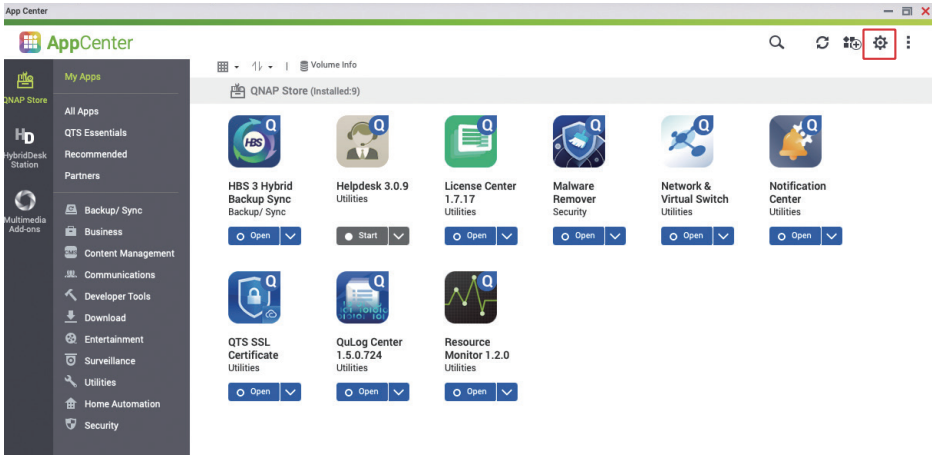
App Update Settings

App Center provides multiple apps to add more functions to your QNAP NAS, but the apps also need to be updated to enhance app functions, fix problems and vulnerabilities, and improve user experience.

Open "App Center" to see if there are any apps that need to be updated. If so, click the "All" button on the top-right to update all apps.

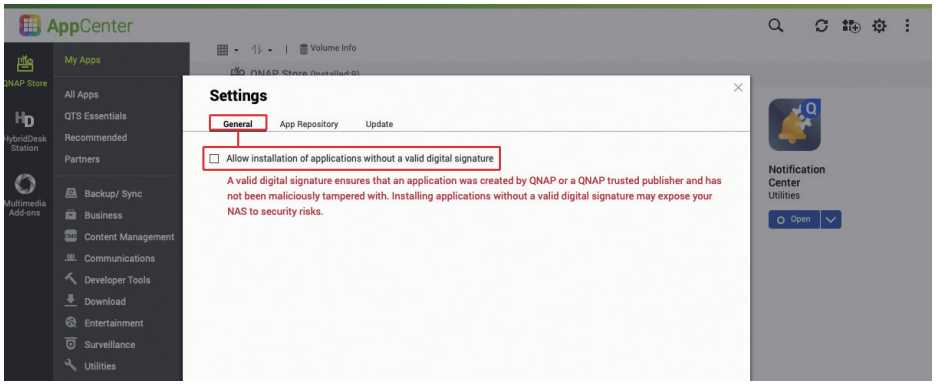


After the update is complete, click the "Settings" icon in the top-right corner to enter the settings page of the App Center.



QNAP or QNAP-trusted developers will add a digital signature to the app to ensure that it is genuine. It is recommended to uncheck "Allow installation of applications without a valid digital signature" to enhance security.

* It is unchecked by default, making it impossible to install apps without a valid digital signature

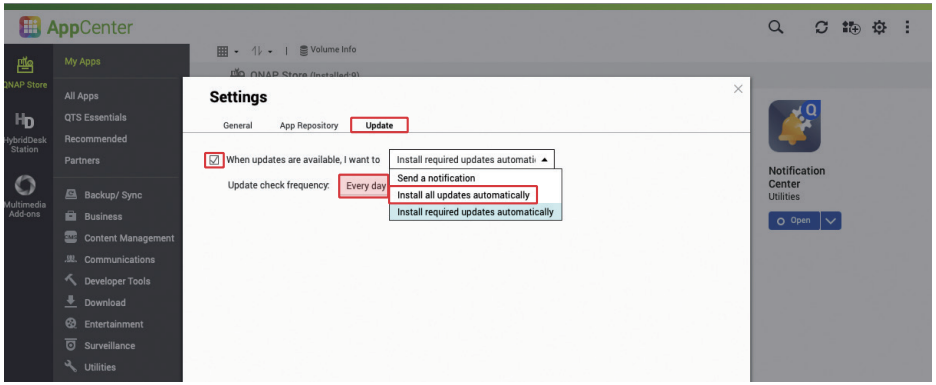


Click the Update tab, if there is no special need, it is recommended to select "Install all updates automatically", set the frequency to "Every Day", and click Apply to complete the setting.

⇨ "Required Updates" are mainly used to meet app and firmware dependencies, and will also include “major vulnerabilities updates".

⇨ "All Updates" includes all feature improvements, bug fixes, and all vulnerability patches. The update will be more frequent.

* The default is "Install all updates automatically"

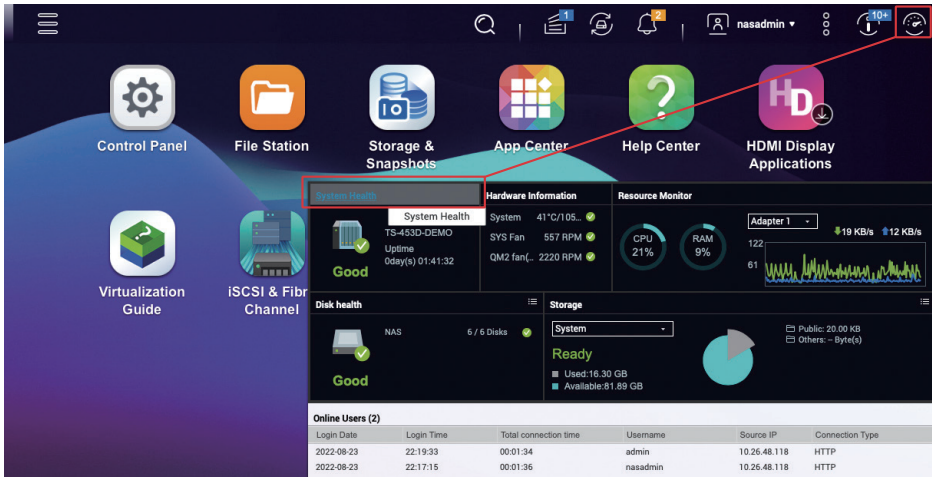


Disable or Remove Unnecessary Functions

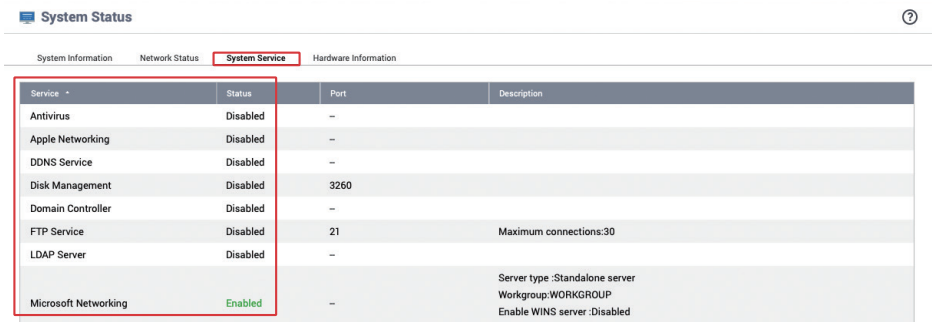
QNAP NAS provides a variety of functions and apps, but the more functions are enabled, the more potential attack vectors there are. You should regularly check and disable (or remove) unnecessary functions to enhance security and make the system work more smoothly.

* To enhance product security, from QTS 5.0.0 / QuTS hero h5.0.0, onwards non-essential functions are disabled by default at system initialization, and App Center will not install any non-essential apps by default. If the system was initialized before updating to QTS 5.0.0 / QuTS hero h5.0.0, please check what apps have been installed.

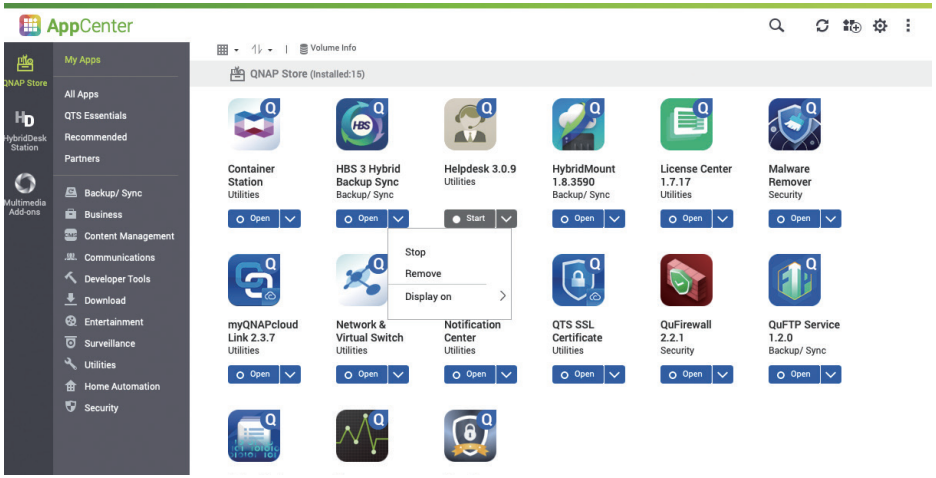
Click the "" button in the top-right corner to open the system "Dashboard", click "System Health" to open the "System Status" window.



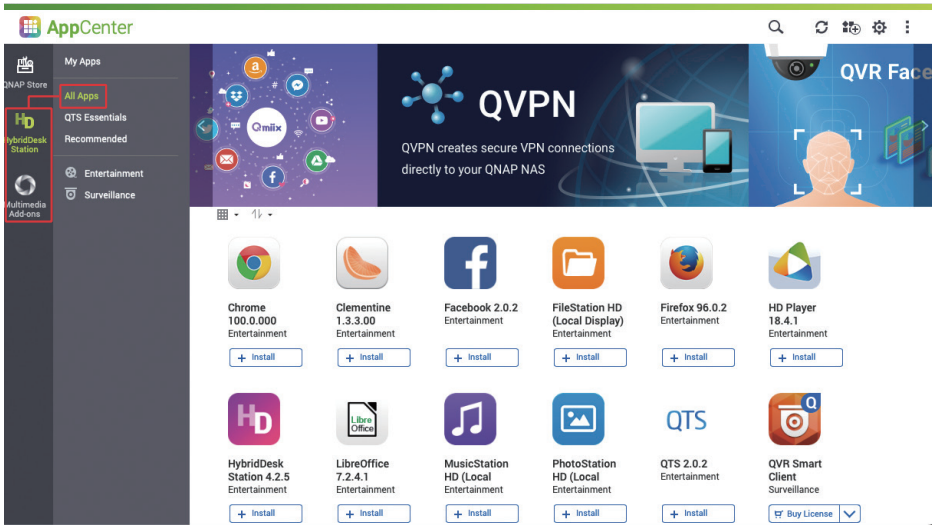
Click "System Service" to view the enabled system functions. You can go to the Control Panel to disable unneeded system functions.



In addition to the system built-in functions, you also need to check what are installed in App Center.



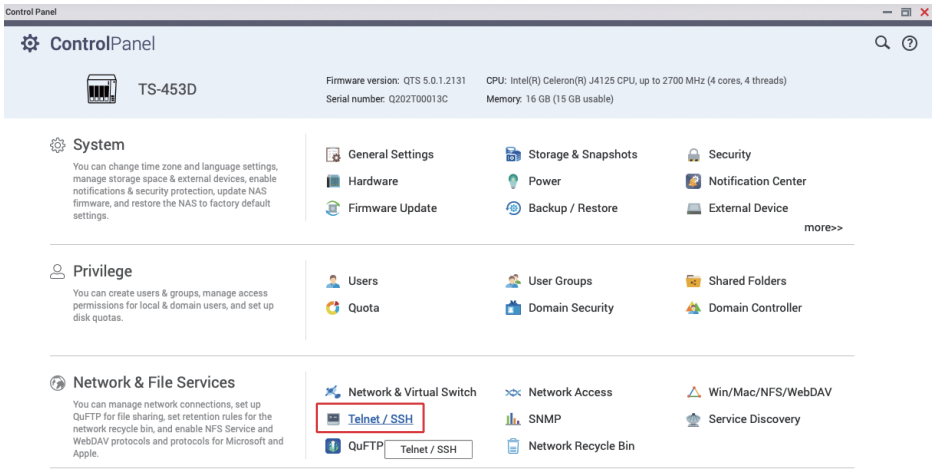
On the far left side, click "HybridDesk Station" and "Multimedia Add-ons" to see the status of the corresponding apps,



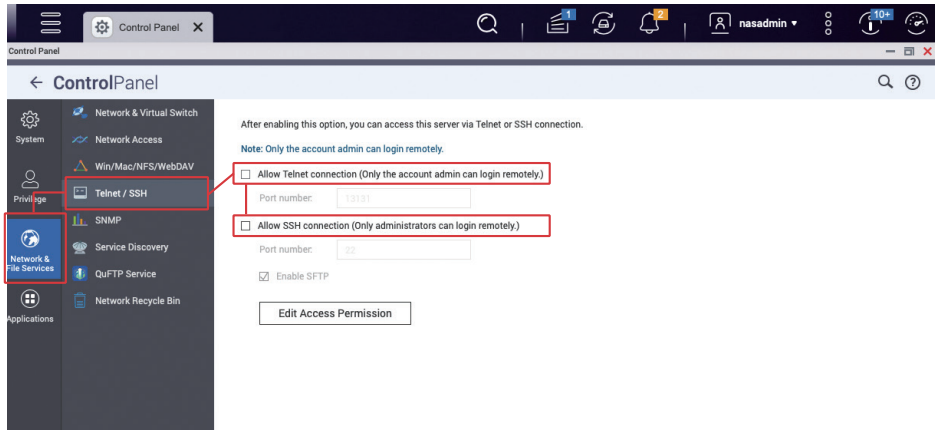
Disable Telnet / SSH

Unless you are using them, it is strongly recommended to disable Telnet and SSH. These two functions are generally used by QNAP customer service or professional IT personnel to maintain the system. General users should not need them, so it is recommended to disable them.

Open "Control Panel" and click "Telnet / SSH"



Uncheck "Allow Telnet Connection" and "Allow SSH Connection", then click "Apply".

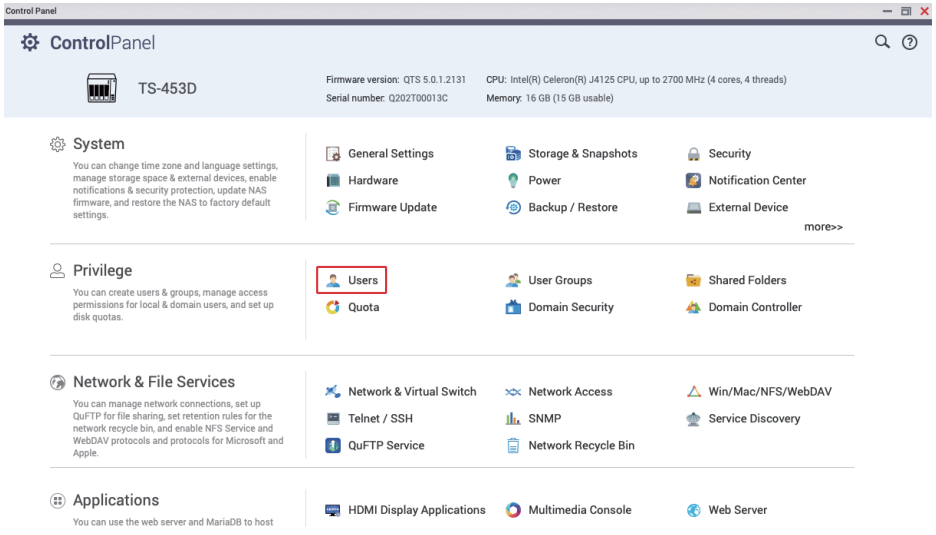


Strengthen System Account Security

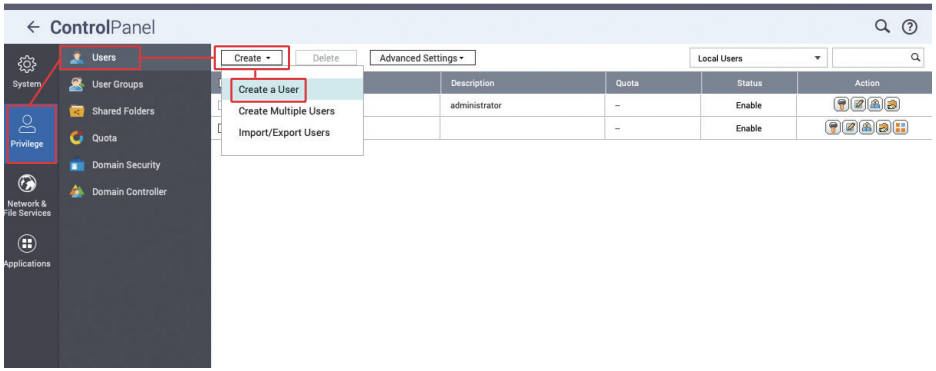
Disable the Default Administrator Account "admin"

Hackers who use brute force password cracking generally target the default administrator account "admin". If the system was initialized using QTS 4.5.4 / QuTS hero h4.5.4 (or earlier), the default administrator account "admin" will be active. Follow these steps to create a new administrator account and disable the "admin" account.

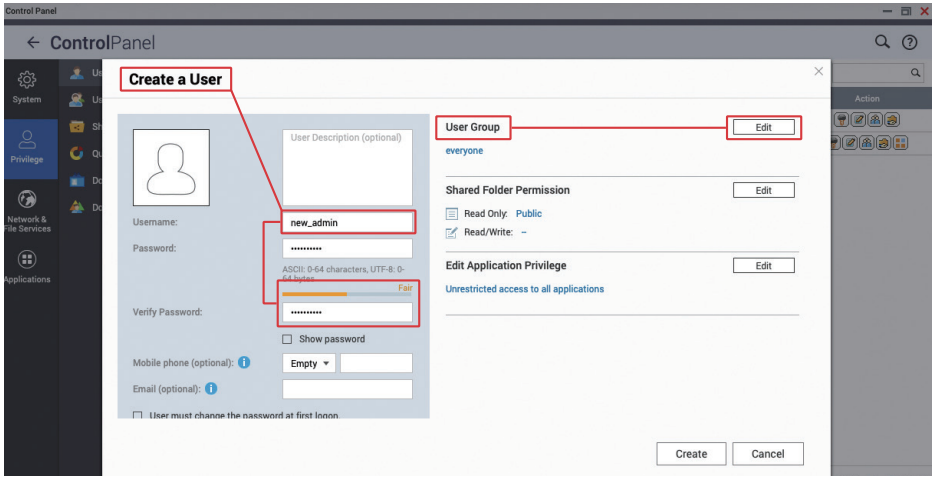
Open "Control Panel" and click "Users"



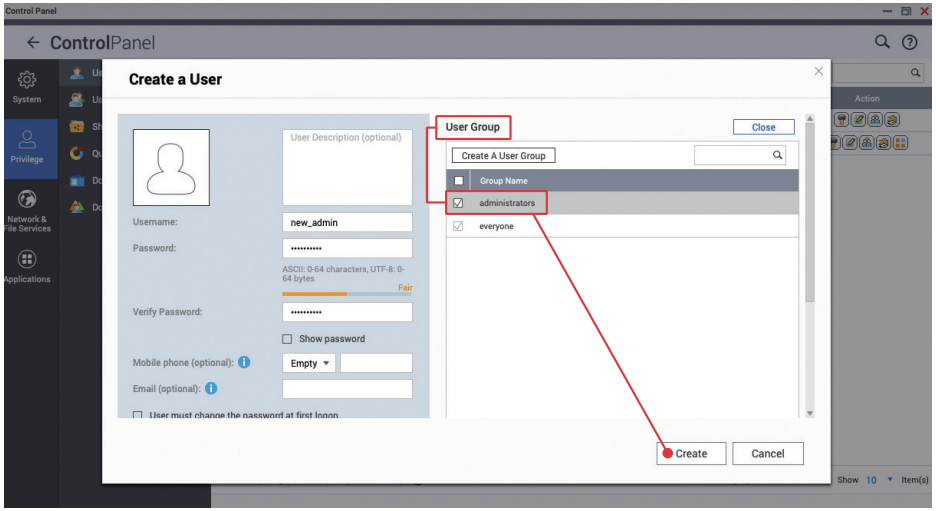
Click "Create" > "Create a User"



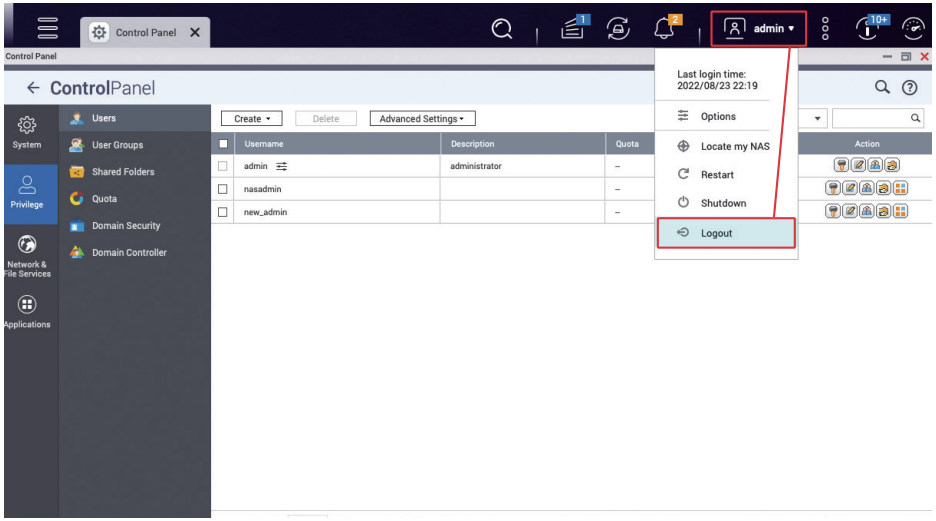
Enter the username for the administrator account, such as "new_admin", and set a Strong Password.



In the "User Group" section, click "Edit", check the "administrators" group, and click "Create" to add a new user.



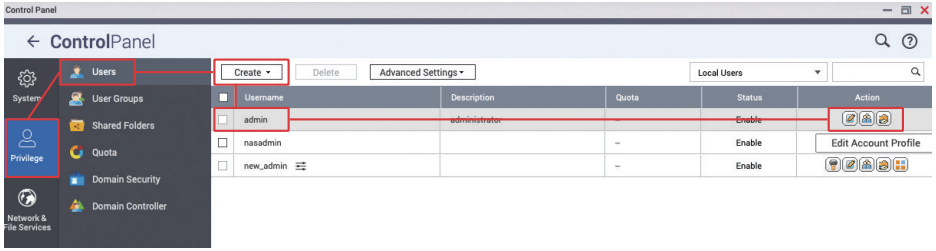
Click "admin" at the top, open the menu, and click "Logout" to log out of the QTS web management interface.



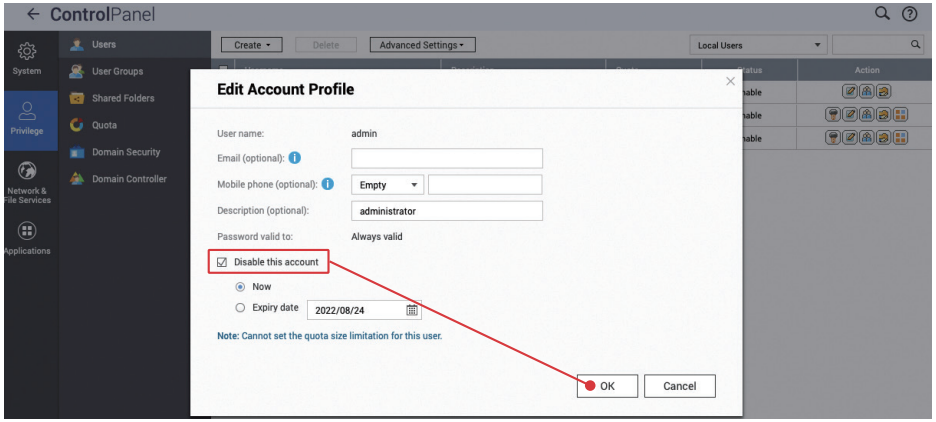
Use the "Administrator Account" you just created to log in to the QTS web management interface.

Set Password Policy

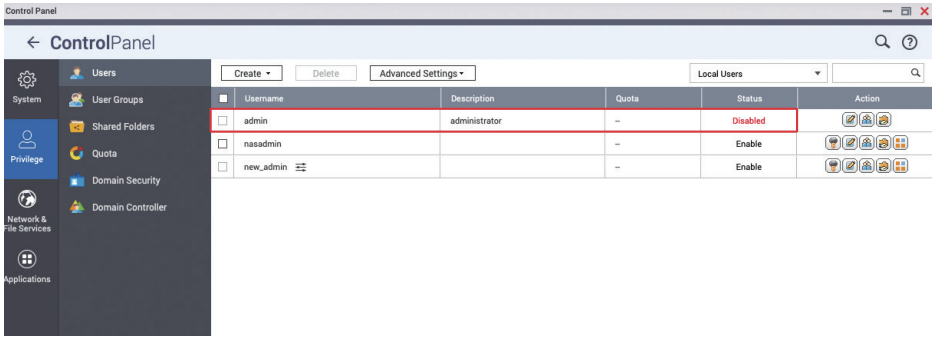
Open the "Control Panel" again, click "Users", in the "admin" row, click "Edit Account Profile"



Check "Disable this account" and click "OK" to finish

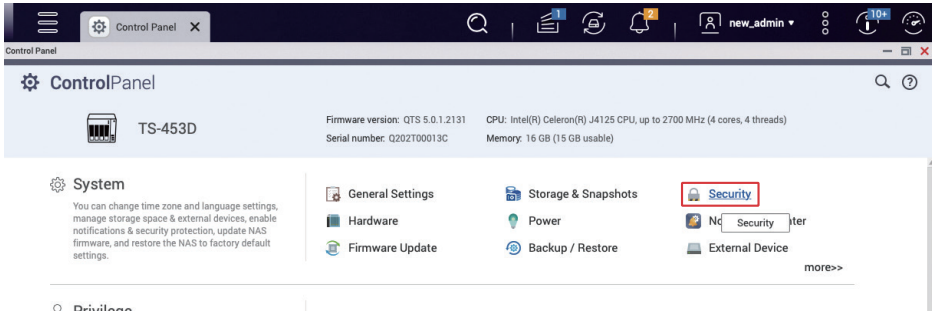


After completion, you can see that the "admin" status is "Disabled"

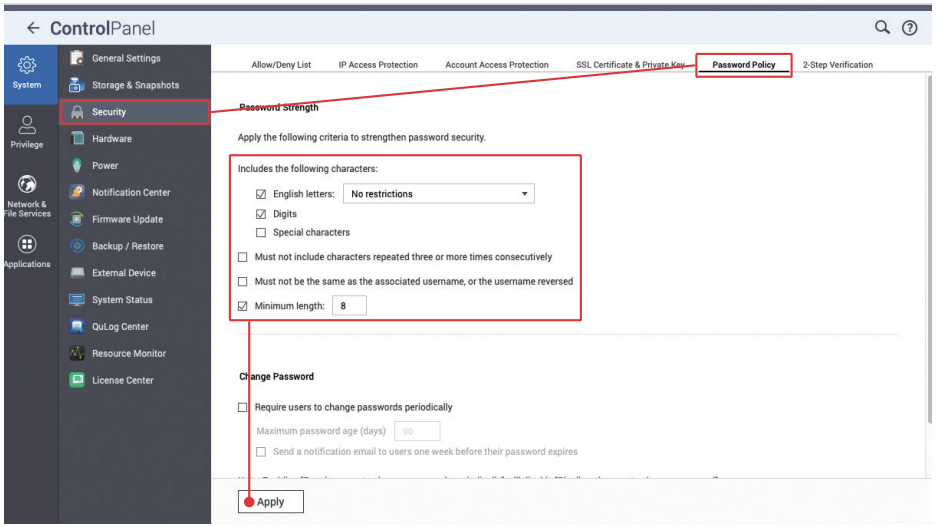


In addition to disabling the default administrator account "admin", you also must ensure that all accounts have strong passwords. With "Access Protection", it can help you block malicious login attempts. For greater security, you can enforce "two-step verification (2SV)" for all accounts to prevent password cracking and malicious logins.

Open "Control Panel" and click "Security Settings"



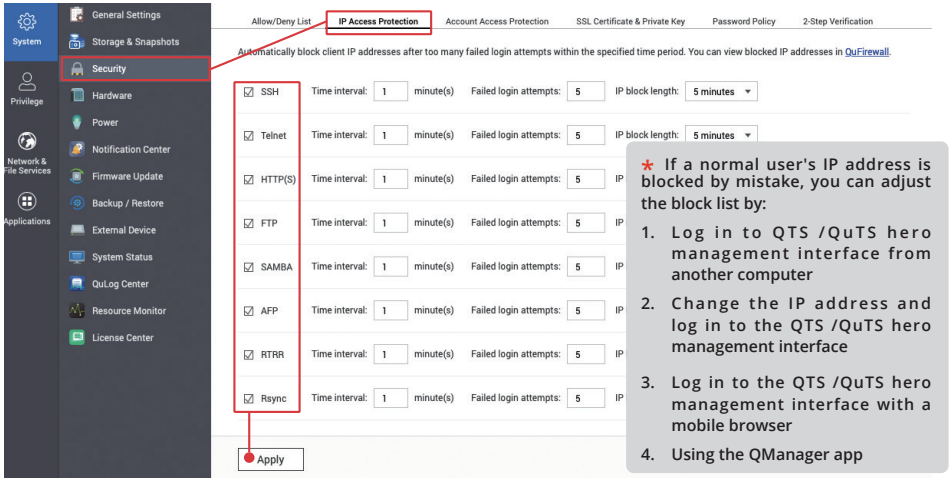
Click "Password Policy" to enter the setting page. If the system was initialized in QTS 5.0.0 / QuTS hero h5.0.0 (or later), the basic password strength conditions are enabled by default. You can set the strong password conditions according to your needs. The password can be set to contain "uppercase and lowercase English letters" and "numbers", and the password length is recommended to be at least "10 characters", click "Apply" after completion.



Enable Access Protection (IP / Account)

"IP Access Protection" and "Account Access Protection" can assist in preventing passwords from being cracked by brute force. When a specific IP or account fails to log in too many times, it will trigger IP blocking or account deactivation, preventing attackers from repeatedly trying passwords.

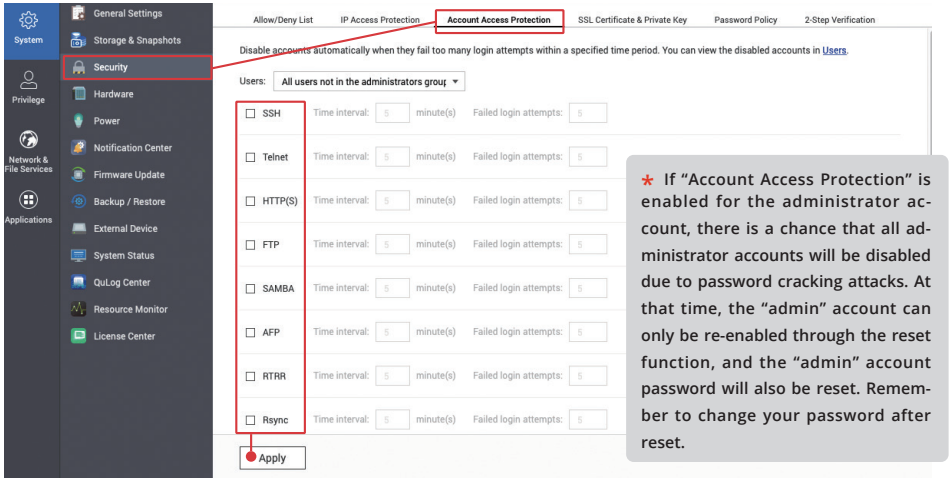
Click "IP Access Protection" to enter the setting page, check all services, set the "Time Interval", "Failed Login Attempts" and "IP Block Length" according to your needs, and then click "Apply" to complete the settings.



* If a normal user's IP address is blocked by mistake, you can adjust the block list by:

1. Log in to QTS /QuTS hero management interface from another computer
2. Change the IP address and log in to the QTS /QuTS hero management interface
3. Log in to the QTS /QuTS hero management interface with a mobile browser
4. Using the QManager app

Click "Account Access Protection" to enter the setting page, enable the relevant services, set the "Time Interval" and "Failed Login Attempts" according to your needs, and click "Apply" to complete the setting.

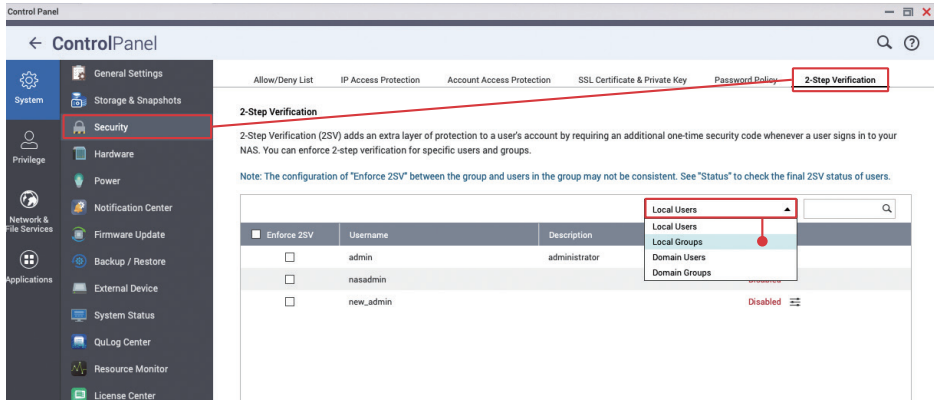


* If "Account Access Protection" is enabled for the administrator account, there is a chance that all administrator accounts will be disabled due to password cracking attacks. At that time, the "admin" account can only be re-enabled through the reset function, and the "admin" account password will also be reset. Remember to change your password after reset.

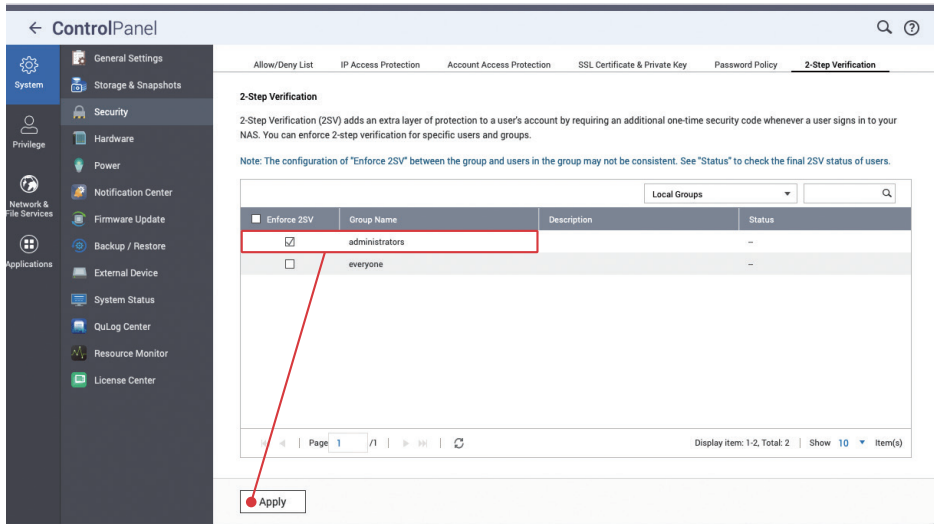
Enable Two-Step Verification (2SV)

Click "2-step verification" to enter the setting page, you can enforce the use of "2-step verification (2SV)" for "users" or "user groups". It is strongly recommended to enable 2SV for accounts in the "Administrators Group". For other accounts, assess the risks yourself and apply appropriate settings.

Click "Local Users" to open the menu and select "Local Groups".

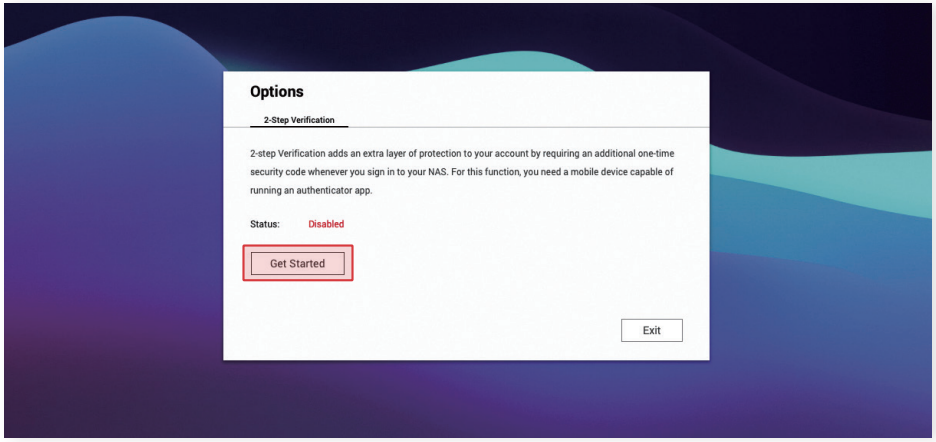


Check "Enforce 2SV" in "administrators" and click "Apply" to complete the setting.

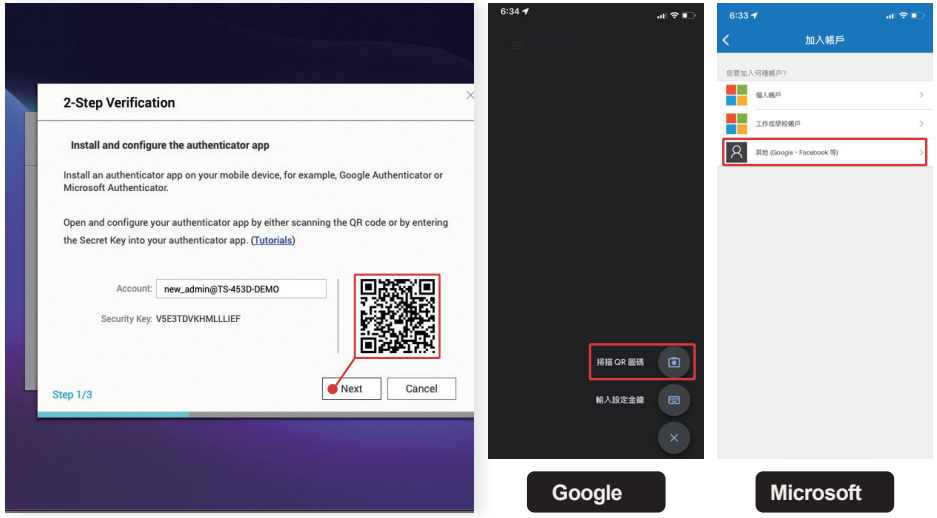


After enabling "Enforce 2SV", if the "Administrator" account has not been set up with "2-step verification (2SV)", the next time you log in, you will be forcibly directed to the "2-step verification (2SV)" setting page for setting up the account.

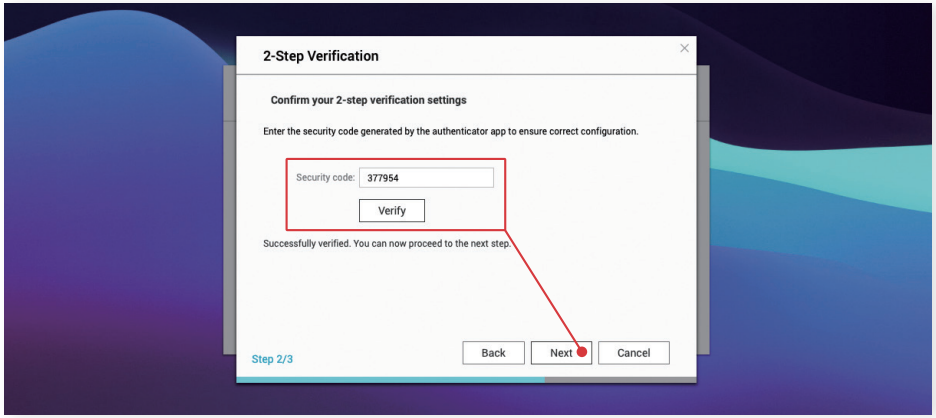
Re-login to the "System Administrator" account and click "Get Started" to start the setting.



Install "Google Authenticator" or "Microsoft Authenticator" on your mobile device, scan the QR code in the program to add the device, and then click "Next".



Enter the six-digit "Security Code" generated by "Google Authenticator" or "Microsoft Authenticator", and click "Verify". After verification, click Next to continue.

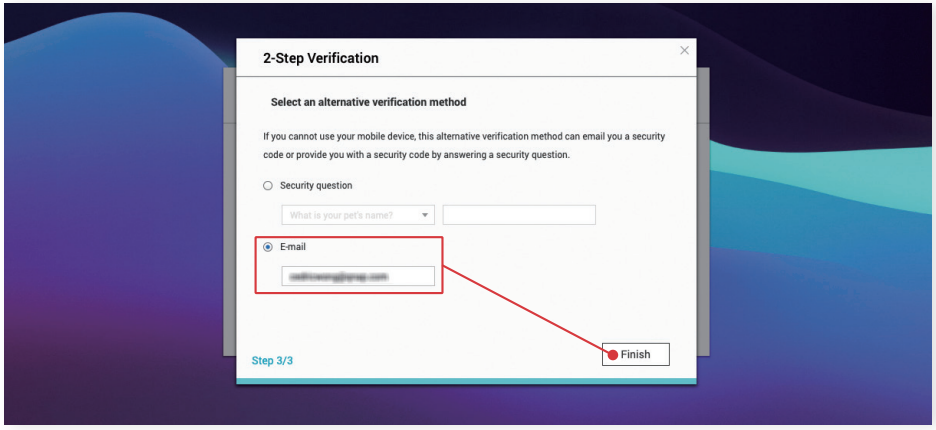


To set up an alternative verification method*, you can select "Security Question"** or "Email"***, fill it out and click "Finish" to enable "2-step verification (2SV)".

* If you cannot get the "Security Code" from an authenticator app, you can receive a "Security Code" by answering the "Security Question" or by using "Email".

** Answer the "Security Question" correctly to pass 2-step verification. Do not use simple or easy-to-guess questions and answers.

*** You must add the "email" notification method in the "Notification Center" to use this function.



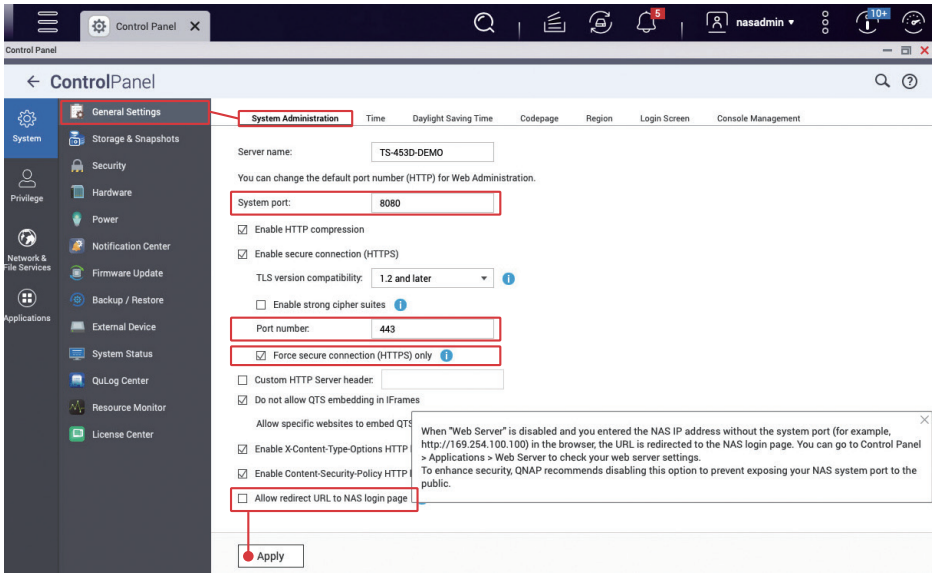
Change Default Ports

Each service running on the NAS has a corresponding service port. Except for some standardized service ports that cannot be modified, the rest can be defined by users.

When a hacker is looking for an attack target, or using the IoT search engine that is often used by hackers, the default port is usually tried first. To reduce the risk of being attacked, you must change the default ports of common services. As far as attacks against NAS are concerned, the most common target is the "system port". The following will demonstrate how to change the "system port". The ports for other functions can be modified on the corresponding settings page. Please be sure to modify them before using the related services for security.

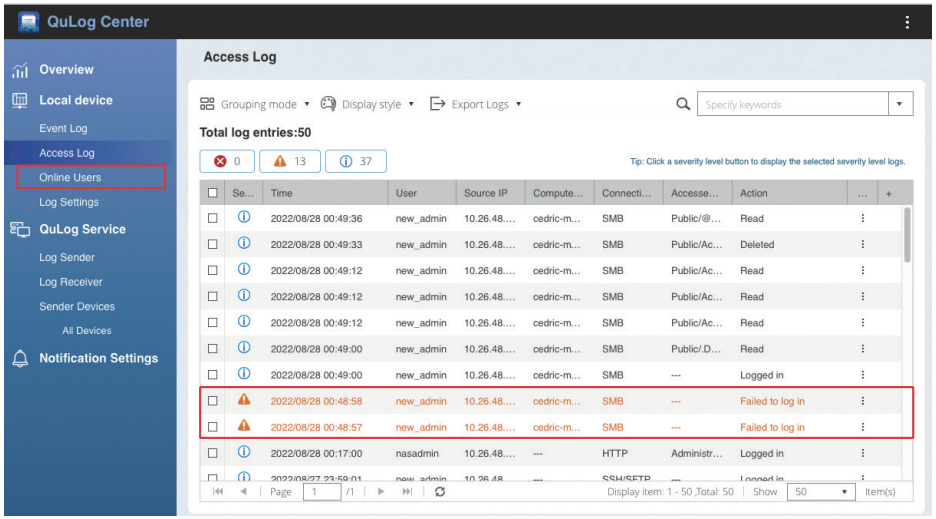
Open "Control Panel", click "General Settings", the "System Port (HTTP)" default is "8080", you can enter a port number between 1 and 65535 such as "56789"; for "System port (HTTPS)", that is, the system port (default is "443") with the "secure connection" function enabled, it is also recommended to change it. At the same time, it is also recommended to check "Force secure connection (HTTPS) only" to ensure that all users transmit data through HTTPS, and helping to prevent hackers from intercepting sensitive information such as account passwords.

In addition, it is also recommended to uncheck "Allow redirect URL to NAS login page" to prevent the "System Port" from being exposed due to automatic redirection. After the change, click "Apply" to complete the setting.

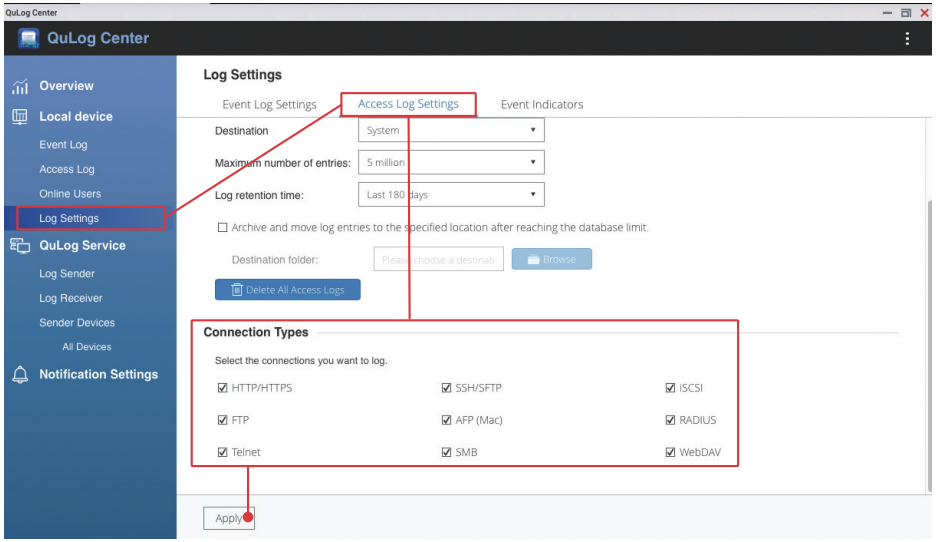


View Access Logs

Access logs can help you view the user's file access, operation, and login history. When a problem occurs, checking access logs should be the first step taken to diagnose the underlying issues.



Open "QuLog Center", click "Log Settings" on the left menu, switch to "Access Log Settings" page, in "Connection Types", check all connections, and then click "Apply" to complete the setting.



Install and Enable Security Apps

QNAP provides several security apps to improve NAS security. Setting up these apps can improve NAS security and allow users to have peace of mind.

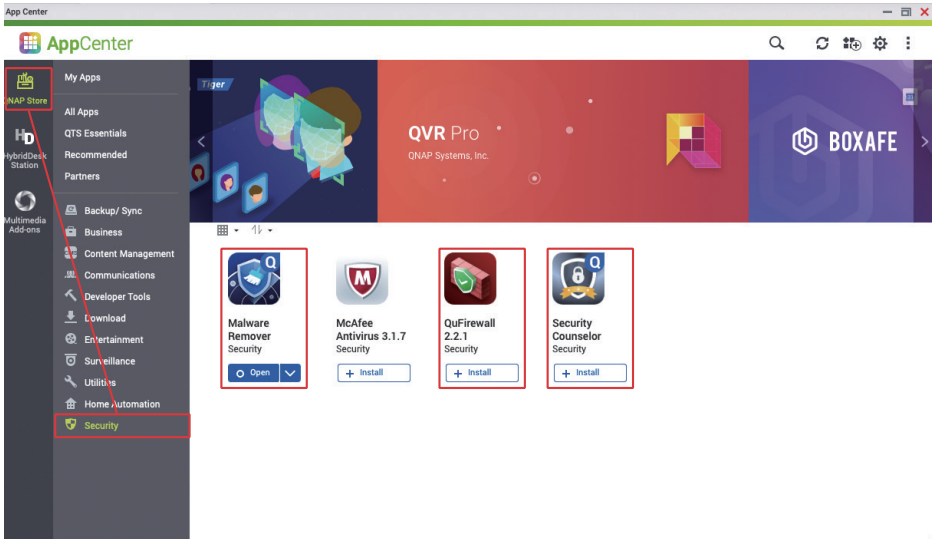
Security Counselor regularly checks the security of your NAS settings and informs you of potential risks.

Malware Remover scans and removes detected malware from your NAS.

QuFirewall provides basic firewall functionality for QNAP NAS, blocking as many hackers as possible from connecting to your NAS.

Open "App Center", click "Security" on the left, install "Security Counselor", "Malware Remover"* and "QuFirewall".

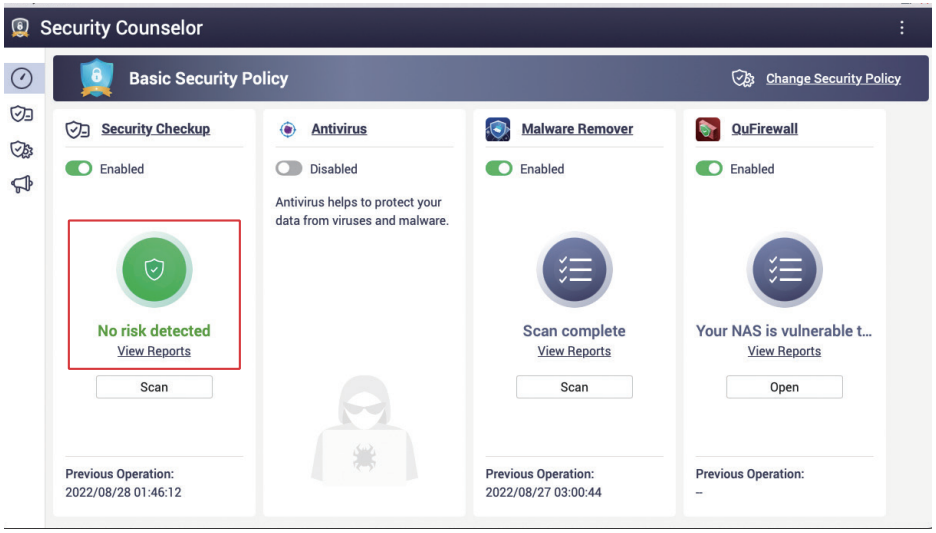
* Malware Remover is preloaded on QTS 4.4.3 (and later) and QuTS hero



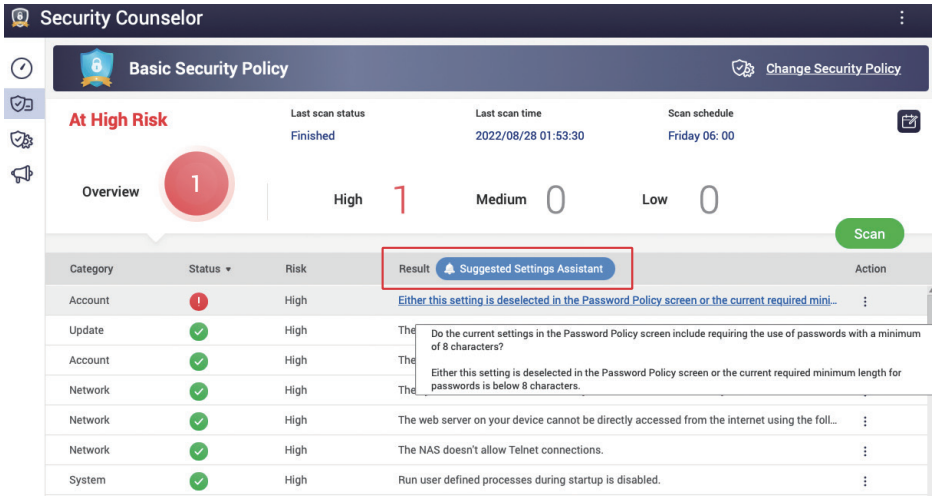
Security Counselor

Open "Security Counselor", select "Basic Security Policy", and click "Scan Now".

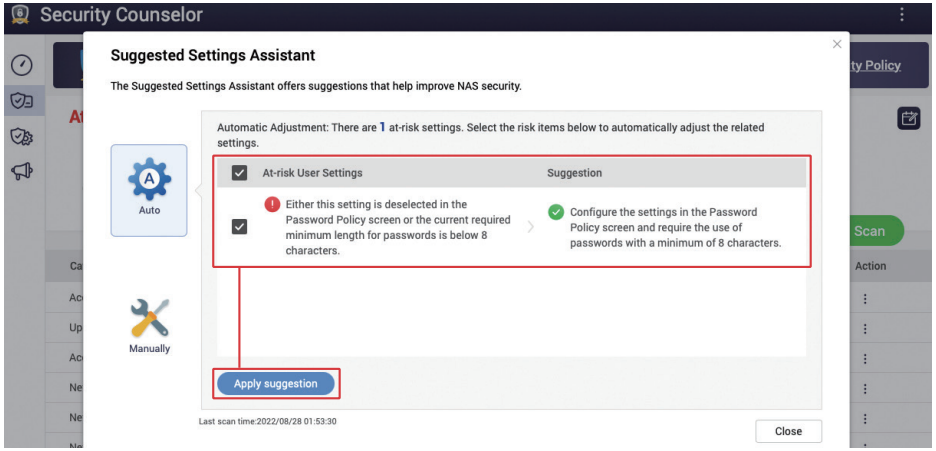
After the scan completes, normally the result is "No Risk Detected". If a risk is detected, click "View Reports" for details and follow the instructions to modify the settings.



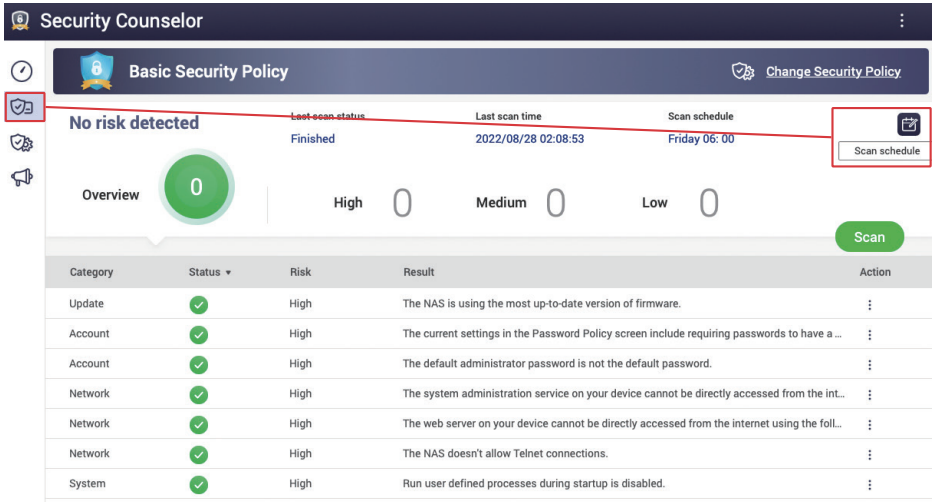
The following are the scan results caused by "high-risk" with deliberately modified wrong settings. Click the "Suggested Settings Assistant" to help you adjust the settings.



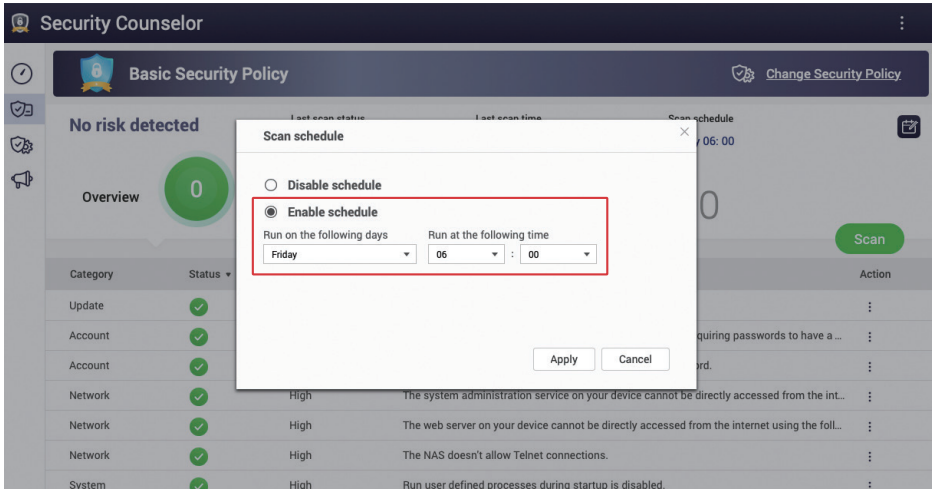
The "Suggested Settings Assistant" lists relevant suggestions. After reading and confirming, click "Apply Suggestion" and the system will automatically apply the relevant settings for you. Some settings must be modified manually, click the "Manually" tab on the left, and adjust the settings as suggested. After applying the changes, the scan will automatically restart. You can check the scan results again to ensure that no security risks have been detected on the NAS.



Click "Security Checkup" on the left to enter the scan result screen, and then click "Scan Schedule" on the right to open the scan schedule setting screen.

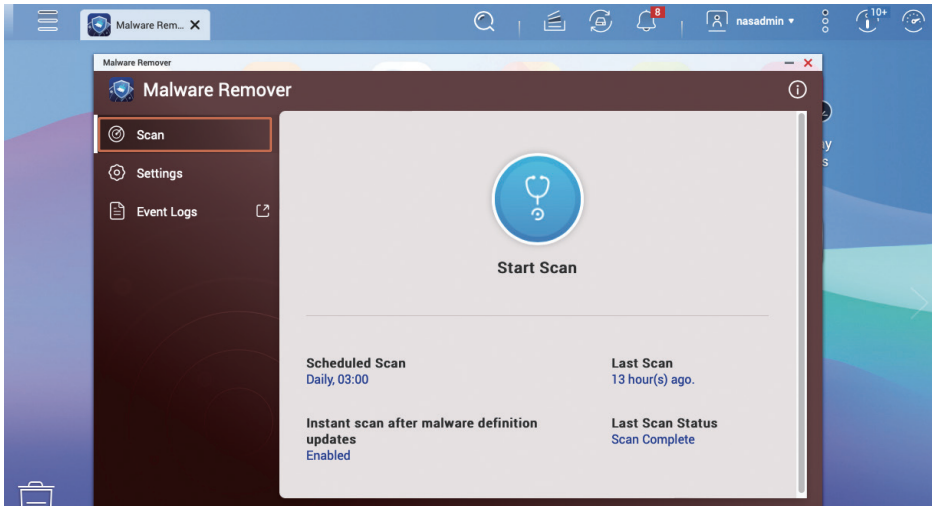


"Scan Schedule" is recommended to be set to at least once a month, so that the system can regularly check the settings and system status. If a risk is detected and the Notification Center is set up correctly, you will receive a notification so that it can be handled as soon as possible.

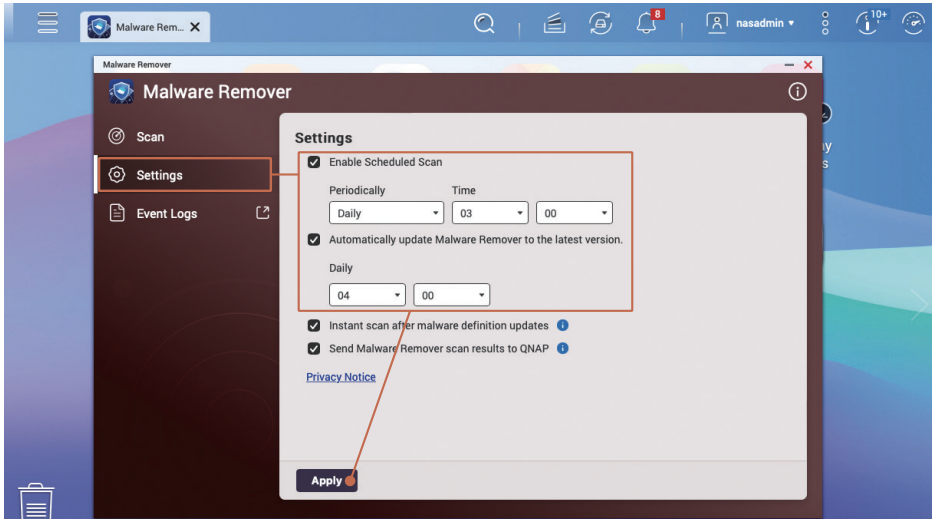


Malware Remover

Open "Malware Remover", the status of the last scan is displayed, click "Settings" on the left.

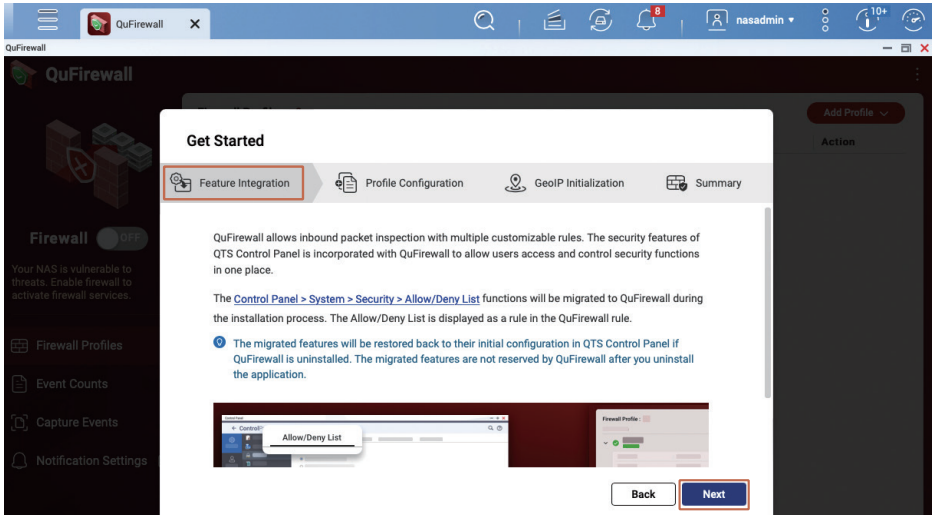


"Scan Schedule" is recommended to be set to once a day, so that "Malware Remover" regularly checks the system status. Also make sure that the "Automatically update Malware Remover to the latest version" remains checked.

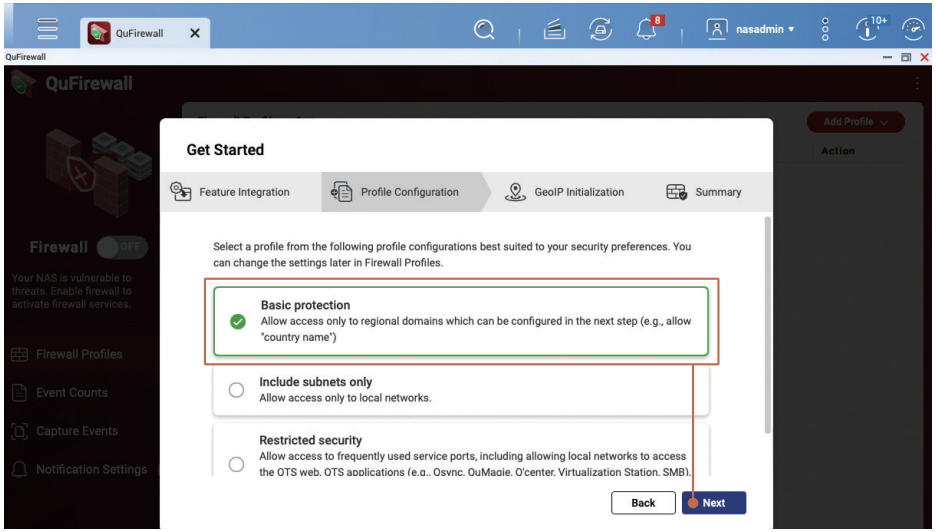


QuFirewall

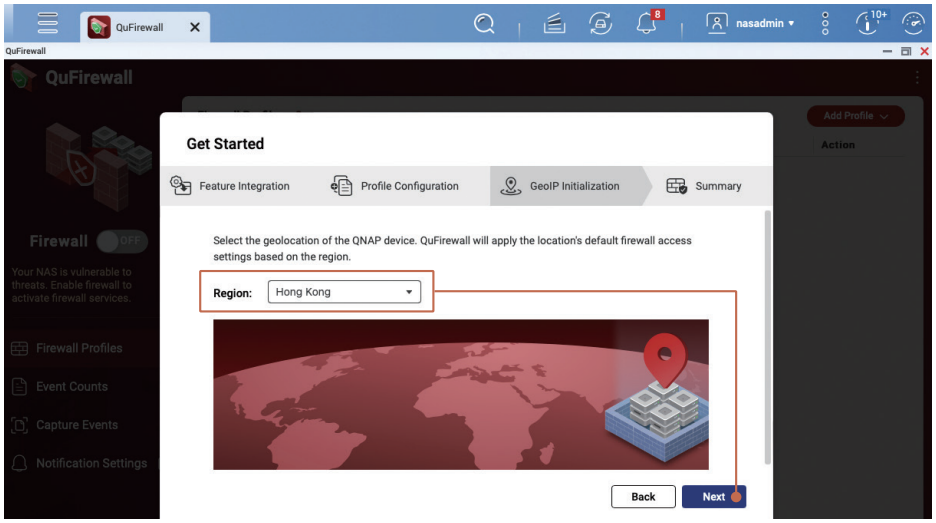
Open "QuFirewall". If this is your first time using QuFirewall the Get Started screen is displayed. After reading, click "Next" to continue.



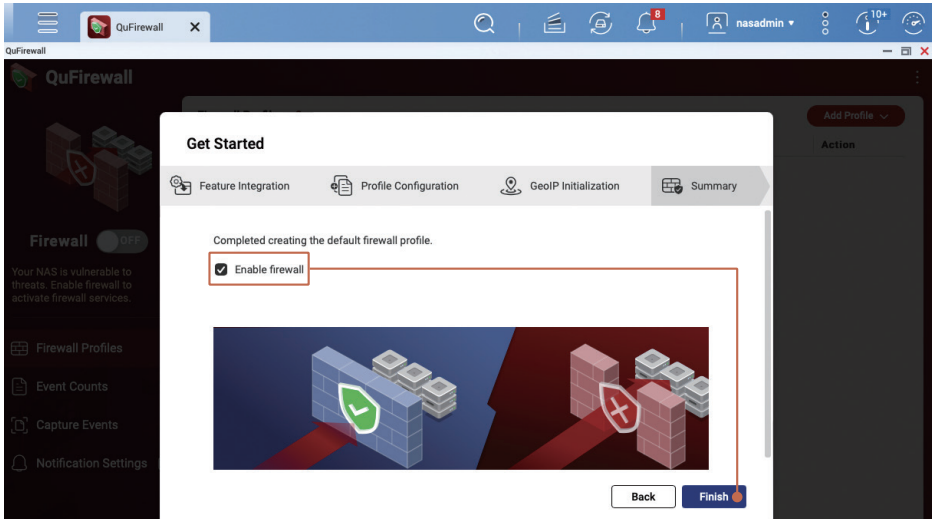
If your network has no special needs, it is recommended to select "Basic Protection", and then click "Next" to continue.



Set a region according to your location. For example: if you are in Taiwan, select "Taiwan"; if you are in Hong Kong, please select "Hong Kong"; if you are in Macau, please select "Macao". You can add more regions later. Click "Next" to continue.

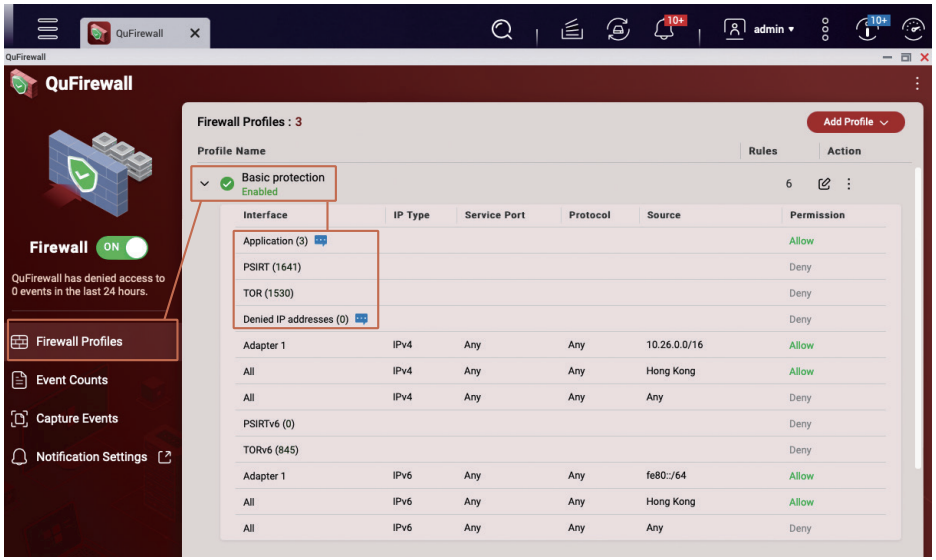


Check "Enable Firewall", then click "Finish" to apply the settings and enable the firewall.



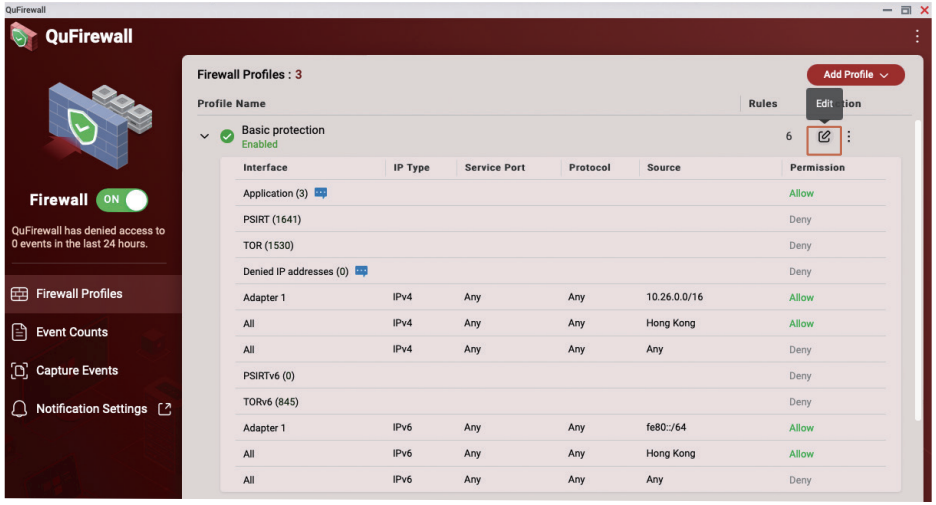
Go to the QuFirewall Profiles page and you will see that "Basic protection" is enabled. Click "Basic protection" to expand and view the corresponding firewall rules. The rules are checked against the information in the incoming packets, which are allowed to pass or be blocked according to the firewall rules. The firewall rules will be executed in sequence. If the conditions are not met, the next line of rules will be checked. If they are not met, they will fall into the last "deny all" rule, and the firewall will block the relevant connections.

- "Application" rules are created by the system to ensure that the system functions properly.
- "PSIRT" rule is a blacklist compiled by QNAP PSIRT. It contains IP addresses that are known to attack QNAP NAS.
- "TOR" rule is used to block connections from the TOR Network. TOR Network is widely used by criminals because of its anonymity, and blocking it can reduce the risk of being attacked.
- "Denied IP addresses" are IP addresses blocked by the "IP Access Protection" function or the blacklist manually added by the user.

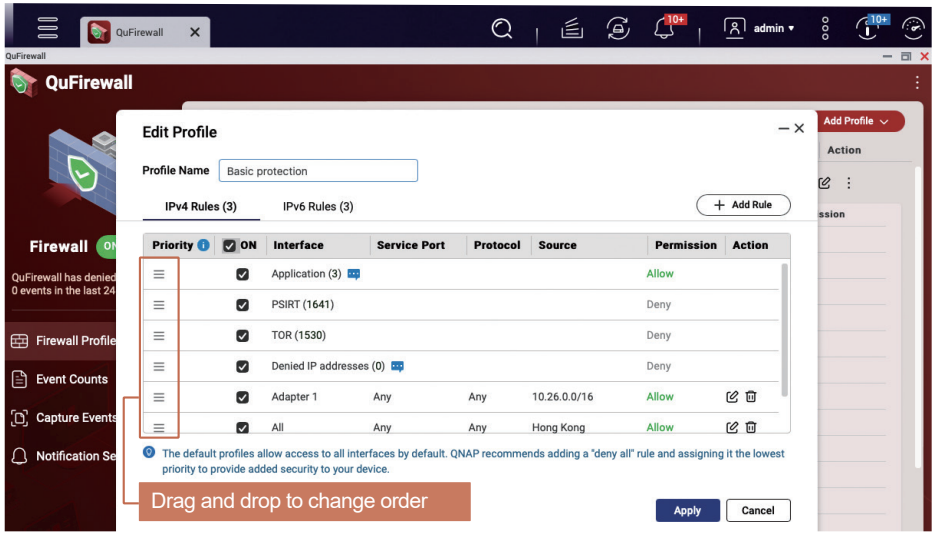


Other rules can be customized by the user, and under basic protection settings, only Internet connections from the same intranet and from the same region will be "allowed". QNAP recommends using the concept of "whitelisting" to manage your custom rules to strictly limit the IP addresses that can connect to the NAS.

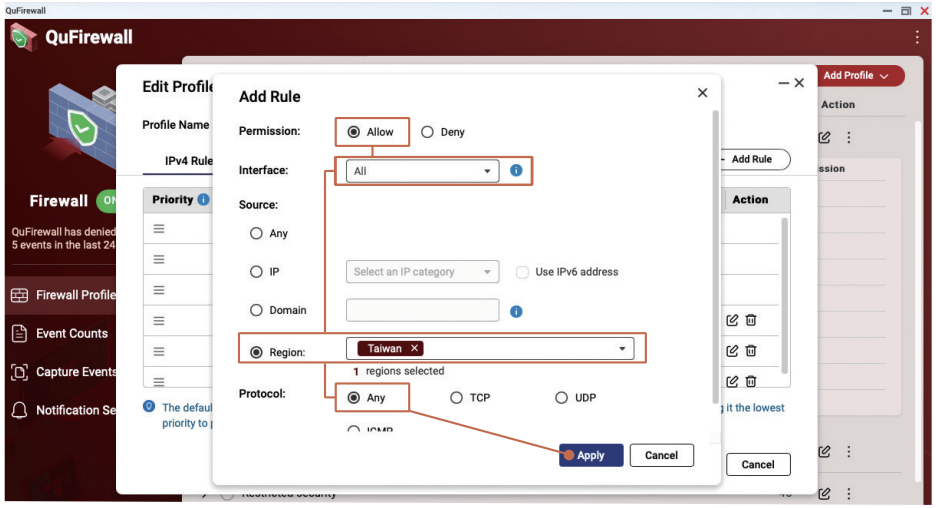
The following demonstrates how to edit firewall rules. Click the "Edit" button to edit the Firewall Profiles screen.



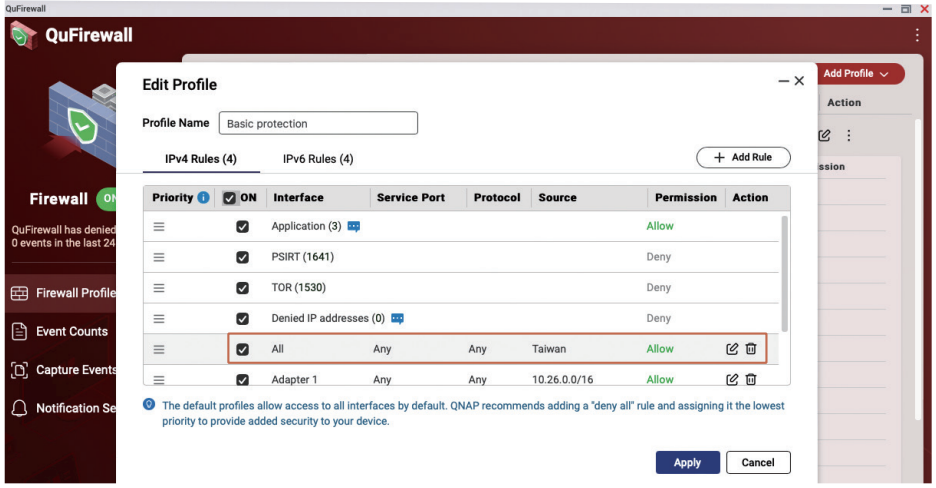
On the Edit Profile screen, you can change the order of rules or add new rules. The following example adds one more region that is allowed connection, click "Add Rule" to enter the setting screen.



For example, to allow connections from Taiwan, "Permission" needs to be set to "Allow"; "Interface" set to "All"; "Region" for "Source", then select "Taiwan"; "Protocol" set to "Any", then click "Apply" to add the rule when finished.



On the "Edit Profile" page, you can see the newly added rules. If necessary, you can adjust the order of the rules. After confirming that they are correct, click "Apply".



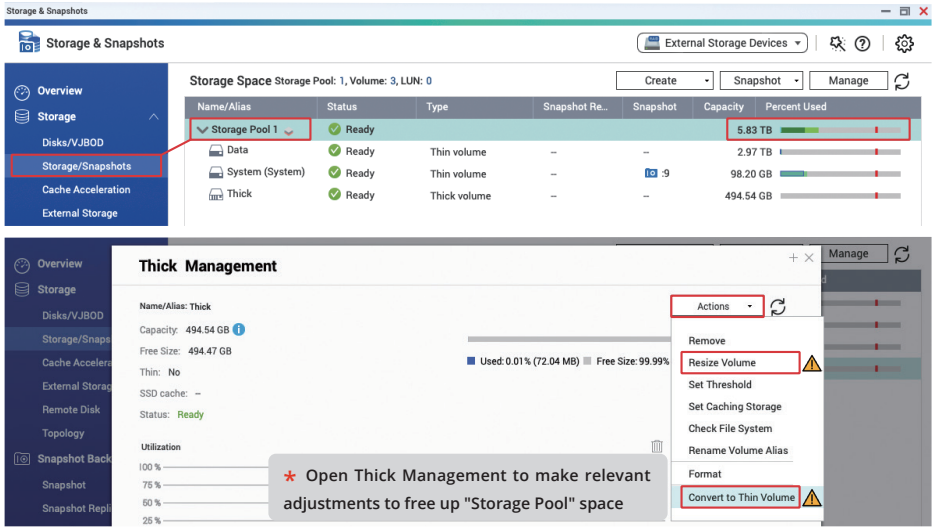
Enable Scheduled Snapshots

The snapshot function can protect your important data by creating multi-version restore points. You can set a snapshot schedule on the QNAP NAS to allow the system to automatically create snapshots according to the schedule as basic data protection.

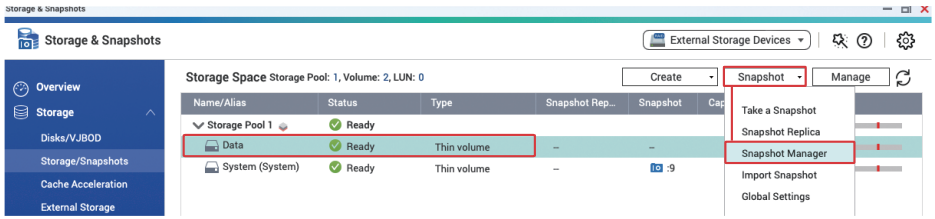
* Scheduled snapshots are enabled by default for "full/thin volumes" created by QTS 5.0.0
* In QTS 5.0.1 (and later) only "thin volumes" have scheduled snapshots enabled by default
* "Shared folders" created by QuTS hero h5.0.1 (and later) will enable scheduled snapshots by default

Open "Storage & Snapshots", click "Storage/Snapshots" on the left, and make sure that "Storage Space" is a "Storage Pool" structure and that the "Storage Pool" has enough free space for the snapshot function to work. If your volume type is "full volume", you can consider "Resize Volume*" and "Convert to Thin Volume*" to free up "Storage Pool" space for snapshot function.

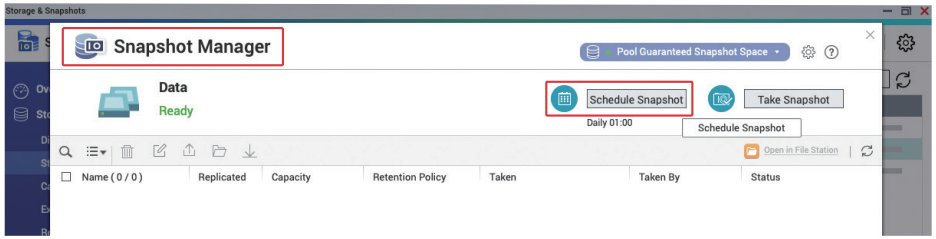
* You must back up your data before converting volumes to avoid potential data loss.



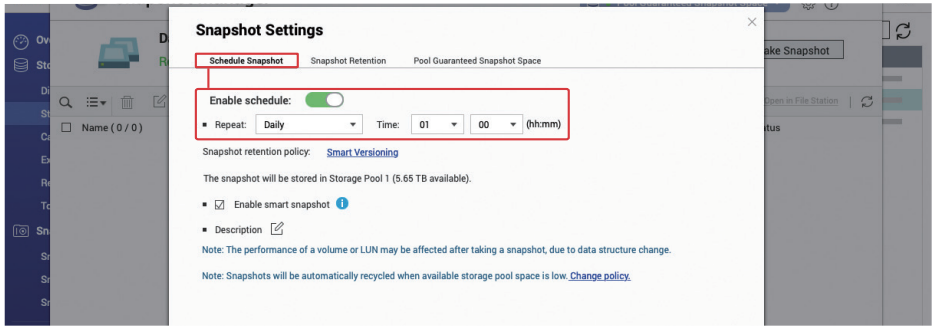
After confirming that there is enough space in the "Storage Pool" on the NAS, first click "Volume", then click "Snapshot" at the top, and click "Snapshot Manager" in the menu.



Go to the "Snapshot Manager" setting page of "Volume" and click "Schedule Snapshot" at the top right.

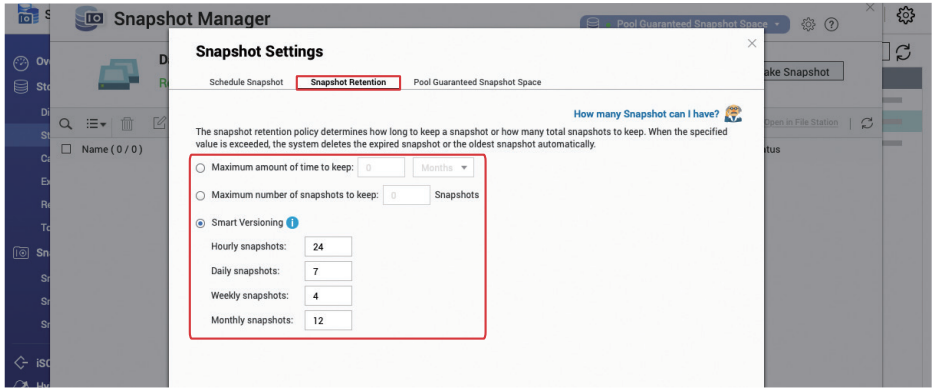


Switch "Enable Schedule" to "Enable" state, and then modify the schedule according to your needs. It is recommended to use "Daily" or "Weekly".



You can set a snapshot retention policy to limit the number of snapshots and prevent snapshots from taking up too much space.

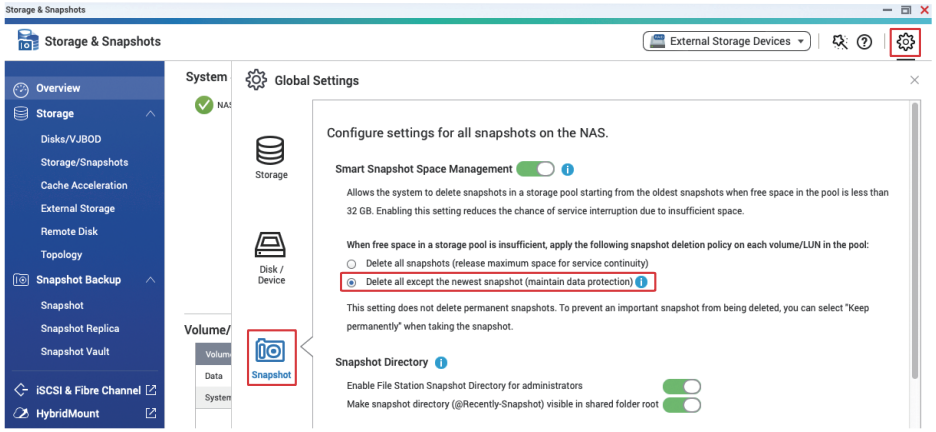
It is recommended to set "Smart Versioning", that is, the Grandfather-Father-Son rule (GFS), so as to retain enough versions for data protection. After the setting is completed, click "OK" to apply the settings.



Set Snapshot Deletion Policy

When the storage pool has insufficient space, the system will delete snapshots based on your settings to maintain normal system service and avoid potential service interruption caused by insufficient space.

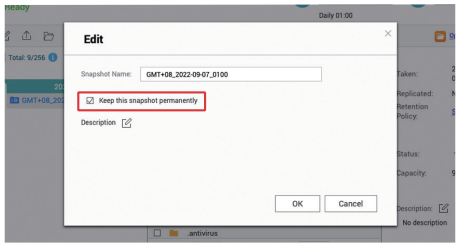
In "Storage & Snapshots", click the "Settings" button in the top-right corner, open "Global Settings", and click "Snapshot". It is recommended to set it to "Delete all except the newest snapshot" to avoid all snapshots being recovered and losing protection.

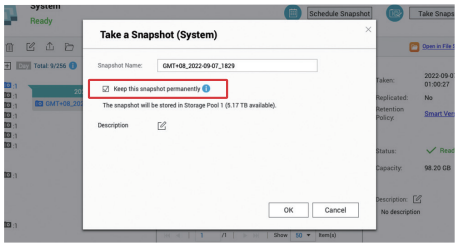


If you want the system to keep all snapshots even when the "Storage Pool" has insufficient space, disable "Smart Snapshot Space Management". Please note that this will cause the "Storage Pool" to enter the "read-only/delete" state when the "Storage Pool" space is insufficient. You must manually delete the snapshot to restore the "Storage Pool" to normal operation. Be sure to regularly check the space usage after disabling this function.

To avoid protection failure due to the snapshot deletion policy, it is recommended to set all or part of the snapshots to "Keep the snapshot permanently"* after storing a large amount of data to prevent the snapshots from being recycled by the system.

* Must delete manually to free up space. It is recommended to manually create and delete regularly





NAS Security Settings Checklist

- ☐ **Setting Up Notification Center**
  - ☐ Set at least one notification method
  - ☐ Create "Alert Notifications" rules
  - ☐ Create "Firmware Update" notification rules
- ☐ **Enable Firmware Automatic Update (QTS / QuTS hero)**
- ☐ **Configure App Center**
  - ☐ Update all apps to the latest version
  - ☐ Prohibit installation of applications that do not have a valid digital signature
  - ☐ Enable automatic updates
- ☐ **Disable or Remove Unnecessary Functions**
  - ☐ Check if enabled services are necessary
  - ☐ Check if enabled **App Center** apps are necessary
  - ☐ Disable **SSH**
  - ☐ Disable **Telnet**
- ☐ **Strengthen System Account Security**
  - ☐ Disable Default "admin" Account
  - ☐ Set Password Policy
  - ☐ Enable IP Access Protection
  - ☐ Enable Two-Step Verification (2SV)
- ☐ **Change Default System Port**
- ☐ **Enable Access Log**
- ☐ **Install and Enable Security Apps**
  - ☐ Security Counselor
    - ☐ Start scheduled scan
  - ☐ Malware Remover
    - ☐ Start scheduled scan
  - ☐ QuFirewall
    - ☐ Enable firewall
    - ☐ Set **Geo-IP** region
    - ☐ Enable **PSIRT** rules
    - ☐ Enable **TOR** rules
- ☐ **Enable Scheduled Snapshots**
  - ☐ Regularly set "Keep the snapshot permanently"

FAQ

Q Is it more secure to disconnect the NAS from the Internet?

A No. NAS "disconnection" generally refers to cutting off NAS from the network so that it cannot initiate connections to the outside world. Although some malware requires an external connection to execute, there are still malware that can successfully perform malicious actions without an external connection. Therefore, not only will it fail to prevent hackers from performing illegal actions, it will also prevent some system functions from functioning properly, such as automatic software updates and notifications. The correct approach is to limit the traffic to the NAS, such as avoiding exposure to the Internet, to improve security.

Q My hard disk is configured with RAID, does it mean that I don't need backup?

A No. RAID is not a backup method. RAID levels above 0 are only intended to provide redundancy against disk failure. RAID provides no protection against data deletion or encryption. Therefore, it is recommended to properly back up data according to the 3-2-1 backup principle.

Q I have already set up "snapshots", does it mean that I don't need backup?

A No. Because "snapshots" are stored on the same set of hard drives as your data, data will still be lost if there is a RAID failure. In addition, if hackers can obtain sufficient privileges (such as successfully cracking the administrator account), the "snapshot" may also be deleted. Therefore, it is recommended to properly backup the snapshot files according to the 3-2-1 backup principle.

Q My NAS is not exposed to the Internet, does it mean that it is impossible to be attacked?

A No. Although most cyber attacks come from the Internet, the NAS is still at risk of being attacked on the intranet. For example, if another computer or device on your intranet is hacked or affected by malware, it may be used to attack and spread to other devices on the intranet. Installing antivirus software and deploying network security products on your computer can help you deal with related threats. For example, QNAP ADRA NDR can detect suspicious intranet activities and automatically isolate them. At the same time, it is also recommended to properly back up data according to the 3-2-1 backup principle.

Q My NAS has been in use for a long time, how do I check if there is malware installed?

A If you notice that the processor load is abnormally high, experience software update failures, or if there are unknown apps in the App Center, it is possible that a malicious program has been installed. It is recommended to install and use the latest version of Malware Remover. If you still cannot solve the issue, contact the QNAP technical support team for assistance.

Q If it is necessary for me to open some services to the Internet, what should I do to ensure security?

A Please make sure that the NAS has the latest version of firmware and apps installed. You can enable QuFirewall to provide basic firewall protection, and the "PSIRT" and "TOR" rules can help you block some hackers' connections. If you are a business or enterprise user, it is recommended to use a higher-level firewall solution. In addition, if storage pool space permits, you can create "snapshots" for basic data protection. It is also recommended to properly back up data according to the 3-2-1 backup principle to prepare for the worst-case scenario and prevent potential data loss.

Q My NAS is old and does not support the latest version of QTS, can it still be used safely?

A Legacy and End of Life (EOL) models have limited support and should only be used for intranet/offline backup.

Q Why do I keep getting a NAS login failure warning?

A If the IP address of the failed login comes from the Internet, it means that your NAS is under brute force password cracking attack. You should avoid exposing your NAS to the Internet, and follow this tutorial to strengthen your NAS. If the IP address of the failed login is from the intranet, please check whether the device with that IP address has malware installed.

Q Why do all my files have strange filenames?

A This is a symptom of a ransomware infection. Check the NAS access logs to determine whether the encryption action is from another computer or the NAS itself. If your NAS has been affected by ransomware, then you should take adequate steps to stop the spread of the infection. If necessary, contact the QNAP technical support team for assistance.

Q What should I do if my NAS is infected with ransomware?

A Most ransomware uses unbreakable encryption methods. If there is no correct key, the files cannot be unlocked, so the files can only be restored by backup or snapshot.

Modify the router settings according to this tutorial immediately to avoid exposing the NAS to the Internet and to prevent secondary attacks. Secondly, you should immediately suspend all synchronization tasks and set snapshots to be permanently retained to avoid losing backup files. If your data has backups or snapshots that you can restore, you can restore the files after updating the NAS firmware and apps and after completing the Malware Remover scan. If the data is not backed up, please back up the ransom note left by the ransomware and the method of paying the ransom, and then try to use methods such as data recovery to recover some data. If necessary, contact the QNAP technical support team for assistance.

Q I keep seeing media reports of QNAP patching product vulnerabilities. Does this mean that QNAP products are not secure?

A There is no perfect software and hardware in the world. Whether it is proprietary software developed by various manufacturers or open-source software, or even hardware, vulnerabilities are always found and then patched by manufacturers. Like other major technology companies, QNAP continues to patch known vulnerabilities, and then releases update files for users to update as soon as possible to ensure the security of users' devices and data. QNAP PSIRT also issue cybersecurity notifications for external disclosure, so that users can act against issues that arise. QNAP believes that dealing with vulnerabilities in an open and transparent manner can protect users' right to know and help improve product safety. Users are also invited to subscribe to the QNAP Security Advisories to obtain relevant, accurate and complete information before media reports.

QNAP Security Advisories:
https://www.qnap.com/go/security-advisories/

Q What is the 3-2-1 backup principle?

A The 3-2-1 backup principle is a well-known backup principle in the IT industry. It prepares for the worst-case scenario. It ensures that in the event of a disaster, there are backup files to restore data to avoid losses and ensure safety.

"3" in Backup 3-2-1 means at least three backup copies; "2" means at least two storage media; and "1" means at least one copy is an Offsite Backup.

Based on the 3-2-1 backup principle, there will be backup files that can be restored regardless of accidental modification, deletion, hardware damage, virus infection, and disasters such as fires and floods.

To satisfy this principle, QNAP NAS includes Hybrid Backup Sync 3 (HBS3), Snapshot Replica, and SnapSync (supported by QuTS hero only) to back up data on the NAS to an offsite NAS, public cloud, external storage, other file servers, and/or other devices to ensure that nothing is lost.

Hybrid Backup Sync 3 (HBS3) Related Tutorials:
https://www.qnap.com/go/how-to/tutorial/article/hybridbackup-sync

Snapshot Replica Related Tutorials:
https://www.qnap.com/go/how-to/tutorial/article/savesnapshots-to-other-qnap-nas-with-snapshot-replica

SnapSync Tutorials:
https://www.qnap.com/go/how-to/tutorial/article/bestpractices-for-the-configuration-of-realtime-snapsync

To improve security, you can add Offline Backup or backup to QuTS hero's WORM (Write Once Read Many) storage space to prevent data from being tampered with.

MEMO

2023

Security Guide

QNAP

QNAP SYSTEMS, INC.

TEL : +886-2-2641-2000 FAX: +886-2-2641-0555 Email: qnapsales@qnap.com

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