

Security Guide

Security Guide

1 Preface

- 2 Common Attacks
- 3 Basic Network Equipment Concepts
- 4 Various Ways to Connect from Internet to NAS

Avoid Exposing NAS to Internet

- 8 Connect NAS Correctly
- 9 Check Router Settings
- 12 Check NAS Settings
- 15 Network Related Settings Checklist

NAS Security Settings

- 17 Set Up System Notifications
- 24 Enable Firmware (QTS / QuTS hero)
 - Automatic Update
- 25 App Update Settings
- 27 Disable or Remove Unnecessary
 - Functions
- 29 Disable Telnet / SSH
- 30 Strengthen System Account Security
- 34 Set Password Policy
- 35 Enable Access Protection
 - (IP / Account)
- 36 Enable Two-Step Verification (2SV)
- 39 Change Default Ports
- 40 View Access Logs
- 41 Install and Enable Security Apps
- 42 Security Counselor
- 45 Malware Remover

FAQ | 58

- 46 QuFirewall
- 51 Enable Scheduled Snapshots
- 53 Set Snapshot Deletion Policy
- 54 NAS Security Settings Checklist

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.

		Attacks	
Response	Password Cracking	Vulnerability Attack (N-day)	Vulnerability Attack (0-day)
Avoid Exposure to Internet	V	V	V
Update Software (System and Apps)	х	V	Δ
Enable Automatic Update (System and Apps)	Х	V	Δ
Use Strong Passwords for All Accounts	V	Х	Х
Disable Default "admin" Account	V	Х	Х
Enable 2-Step Verification	V	Х	Х
Enable Access Protection	Δ	Х	Х
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 ∆: 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

Various Ways to Remotely Connect to NAS

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.

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	• Vulnerable to cyber at- tacks • Fastest connection • Fastest connection • Vulnerable to cyber at- tacks • No defense against 0-Day vulnerability at- tacks		 Have a clear understanding of the associated risks Familiar with network set- tings Have created multiple back- ups for important data Have a disaster recovery plan
Enable VPN server on the router*	• Relatively simple to set up	 No login failure notifica- tion, 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 with- out feeling any differ- ence Also supports Client-to- Site VPN 	 Additional equipment required 	 Requires multi-point access and remote backup Requires value-added appli- cations

* 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







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

myQNAPcloud >	•	0	e'	S	۵.	<u>।</u> admin ▼	(1 ¹⁰⁺)
myQNAPcloud							- + ×
0							4
Overview Auto Router Configuration My DDNS Publish Services myQNAPcloud Link Access Control SSL Certificate	Enable UPnP Port forwarding Enable this function to allow access to your NAS from the Interne Note: This function only works with the UPnP supported devices. Status : N/A	tt via an UPnP rot	ıter.				

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"

myQNAPclou	x	Q 🖆	S (10+	nasadmin ▼	8 (1 ¹⁰⁺	۲
myQNAPcloud					- 1	a x
						1
Overview My DDNS Published Services myQNAPeloud Link Access Control SSL Certificate	Enable UPAP Port forwarding Enable this function to allow access to your NAS from the Inte Note: This function only works with the UPAP supported device Status : N/A	met via an UPnP router. 15.		my FA Au De Ab	QNAPcloud Tour Q to Router Configuration bug Report out	

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



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".

myQNAPcloud	×	Q É	S 🖓	nasadmin ▼	\$ (1 ¹⁰⁺)
myQNAPcloud					- a ×
					1
Overview					
My DDNS	Access Control				
Published Services					
myQNAPcloud Link					
Access Control					
SSL Certificate	Device access controls Customized	• ()			
	Devices can only be seard Public	e. The search i	results will be invisible to	other users. If someone wit	hout an invite
	Customized		incorton.		
	Who can access Add Clear All			Search	
	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".

myQNAPcloud	× Q É Ø	(<mark>10+</mark>) 옷 na:	sadmin ▼ 0000	(1 ¹⁰⁺)
myQNAPcloud				- a ×
				3
Uverview Wy DDNS Published Services myQNAPcloud Link Access Control SSL Certificate	Number of the services You can publish NAS services to myQNAPcloud website. (https://www.myqnapcloud.com). Select "Publish" to publish the NAS services to myQNAPcloud website. Select "Private" to the same published NAS services from public access. The private services on myQN NAS Services NAS Service NAS Web File Station Web Server Photo Station Secure NAS Web Secure NAS Web Secure NAS Web Secure Web Server	Status Enabled Disabled Disabled Disabled Enabled Disabled Disabled Disabled Disabled	Publish Publis	th
	Secure Photo Station	Disabled		
	Secure Music Station	Disabled		
	Apply ●			

Network Settings Checklist

Hardware Related

 \square NAS is connected behind a router

 \square NAS obtains intranet IP address

Router

 \Box Disable router "DMZ" function

 \Box Disable router "Port Forwarding" rule

□ Disable router "UPnP" function

NAS

 $\hfill\square$ Disable the NAS "Auto Router Configuration UPnP Port Forwarding" function

 $\hfill\square$ Set NAS "myQNAPcloud Link Access Control" to "Private" or "Customized"

 \square 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:







uide



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.



 $\mathbb{Q} \ \mathbb{Q}$ Once created, you'll see the email account you've added in the list.

	Notification	. X		Q	🖺		<u>ل ا</u>	२ nasadmin	• 000		(b)
Notifica	tion Center									-	+ ×
	Notification Cente								ŝ	* ?	í
ίí	Overview	Activ		Inactive		\square	Inactiv		st)	Inactiv	e
5	Notification Queue and History	E-mail		SMS		Instant Mes	saging		Push Ser	ice	
•□	Service Account and Device Pairing	Here you can add SMTP ser	ices. Notification Ce	nter will send notifi	cations to recipi	ients via the sp	ecified SMTP set	vices.			
P	System Notification Rules										
8	Global Notification Settings	+ Add SMTP Service									_
		Service Provider		E-mail			A	ction			
		🞦 Gmail ★		aditionagina	0.000		4	1 🖸 🗇			
											_

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 \bigoplus " next to "Recipient". You can also "Add Pair" to send notifications in multiple ways at the same time.

	Notificatio	n X	C	2 É	Í	3 1	옷 nasadmi	in∙ °oo		(j)
otifica	ition Center								-	+ ×
4	Notification Cen	ter						ŝ	* ?	(j)
	والمتعربية والمستعدية والمتكر									
	Overview	Create alert notification rule					- ×	Inactive		
	Notification Queue and History	Name and Events	2 Methods and Re	aciniante	0.	ummany				
□□	Service Account and Device Pairing	· Hume and Events) methods and ne	copienta	0.	i in in in it is in the second s				
P	System Notification Rules	Select the delivery methods and specify the	ne recipients. You ca	an add multiple meth	nods and recipie	ents. + Add	Pair			
8	Global Notification Settings	Pair1 (1/1)					^			
		Method E-mail	•				B			
		Sender		Recipient		Add	0			
		Select SMTP service		Select NAS Us	er)					
				E-mail 1			1	severity		
		Type the text	0	CONTRACTOR OF TAXABLE			J	ncations.		
		Cancel			Bac	sk	Vext			



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".

	Notificatio	n X 🖹 🛱 🗘 🦹 nasadmin • 🕴 😷
lotifica	tion Center	— + ×
<i>"</i>	Notification Cen	ter 💩 🦄 🕐 🛈
	Overview	Create event notification rule
	Notification Queue and History	Name and Events 2 Notification Criteria 3 Methods and Beniniants 4 Summary
₀□	Service Account and Device Pairing	
	System Notification Rules	Name this rule and select events. Notification Center will send notifications to recipients when the selected events occur.
	Global Notification Settings	Rule name Rule - 1
		□ Select all Displayed Items 2 Firmware Update ✓
		🛛 🔮 Firmware Update (1/1)
		☑ Firmware Update
		re event these
		Cancel

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

	Notificatio		in • 🖇 🚺
otifica	tion Center		- + ×
	Notification Cen	ter	🏟 🛠 ?? (i)
	Overview	Create event notification rule - ×	Active
	Notification Queue and History	Name and Events Natification Criteria A Methods and Recipionts A Summary	
▫▢	Service Account and Device Pairing		
	System Notification Rules	Specify the severity levels, keywords, and time range of notifications that you want to receive.	
	Global Notification Settings	Image: Construction Image: Construction Keyword Filter Image: Construction	
		All messages • - Only send notifications for events that occur during a certain time period. Time range: 00 • 2 00 • ~ 23 • 2 59 •	ve event hese
		Cancel Back 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.

Notification Cer	iter	🕸 🛠 🕐 🤅
ரு Overview எ Notification Queue and	Create event notification rule	Active
History Service Account and Device Pairing	Name and Events O Notification Criteria Methods and Recipients O Summary	
System Notification Rules	Select the delivery methods and specify the recipients. You can add multiple methods and recipients.	
Settings	Pairt (1/1) Method E-mail Sender Select SMTP service Method Select NAS User E-mail 1 Custom subject line (optional)	went se
	Cancel Back Next	

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

Notificatio	n X	Q É S Q	nasadm	in• °° €	(i)
Notification Center					+
Notification Cen	ter			🕸 Ҟ 🕐 (D
႐ို့ Overview လျှော် Notification Queue and History	Create event notification rule		- × 1	Active	
 Service Account and Device Pairing System Notification Rules Global Notification Settings 	Name and Events Notification Criteria Selected Event Categories Firmware Update (1) Firmware Update	 Methods and Recipients 	4 Summary		
	Notification Criteria Severity Level ① Information	Back	Finish	re event hese	

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

000	Control Panel X	🔍 🗐 🗿 🖓 🗚 nasadmin • 🕴 🗍	
← C	ontrolPanel		Q. (?)
System System Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Solutions Privilege Privilege Solutions Privilege Privil	Image: Control of Contro	Firmware Update Manual installation Firmware Update Settings When firmware automatically 	

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 C All " button on the top-right to update all apps.



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

App Center								- a ×
	AppCenter						Q 01	i⊕ 🗘 :
NAP Store	Му Аррз	∰ QNAP Store (olume Info Installed:9)					
HD HybridDesk Station	All Apps QTS Essentials Recommended Partners	HBS 3 Hybrid	Helpdesk 3.0.9	License Center	Malware	Network &	Notification	
Multimedia Add-ons	 Backup/ Sync Business Content Management 	Backup Sync Backup/Sync	Utilities	1.7.17 Utilities	Remover Security	Virtual Switch Utilities	Center Utilities	
	Q2 Entertrainment □ Surveillance ペ Utilities 由 Home Automation ♥ Security	QTS SSL Certificate Utilities	QuLog Center 1.5.0.724 Utilities	Resource Monitor 1.2.0 Utilities				

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.



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.

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

 \Rightarrow "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 " (B)" 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.

📮 System Status			(?)
System Information	letwork Status System Service	Hardware Information	
Service *	Status	Port	Description
Antivirus	Disabled	-	
Apple Networking	Disabled	-	
DDNS Service	Disabled	-	
Disk Management	Disabled	3260	
Domain Controller	Disabled	-	
FTP Service	Disabled	21	Maximum connections:30
LDAP Server	Disabled	-	
Microsoft Networking	Enabled	-	Server type :Standalone server Workgroup:WORKGROUP Enable WINS server :Disabled

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,



Strengthen System Account Security

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"

Disable Telnet / SSH

29

Control Pa	inel				-	
¢	Control Panel				Q	?
	TS-453D	Firmware version: QTS 5.0.1.2131 Serial number: Q202T00013C	CPU: Intel(R) Celeron(R) J4125 CPU, up to Memory: 16 GB (15 GB usable)	2700 MHz (4 cores, 4 threads)		
	System You can change time zone and language settings, manage storage space & external devices, enable notifications as security protection, update NAS firmware, and restore the NAS to factory default settings.	 General Settings Hardware Firmware Update 	 Storage & Snapshots Power Backup / Restore 	 Security Notification Center External Device more>> 		
	Privilege You can create users & groups, manage access permissions for local & domain users, and set up disk quotas.	🔔 Users 😋 Quota	🕵 User Groups 📩 Domain Security	🧧 Shared Folders 🐴 Domain Controller		
	Network & File Services You can manage network connections, set up 0LFT for file harding set retension nules for the network respels bin, and enable NFS Service and WebDAV protocols and protocols for Microsoft and Apple.	 Network & Virtual Switch Telnet / SSH QuFTP Telnet / SSH 	∞ Network Access <u>↓</u> , SNMP SNMP Network Recycle Bin	 △ Win/Mac/NFS/WebDAV 		

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



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"

ntrol Pa	anel				
Φ	ControlPanel	Firmware version: QTS 5.0.1.2131 C	CPU: Intel(R) Celeron(R) J4125 CPU, up to 2	2700 MHz (4 cores, 4 threads)	Q. (?)
		Serial number: Q202T00013C N	Memory: 16 GB (15 GB usable)		
	System You can change time zone and language settings, manage storage space & external devices, enable notifications a security protection, update NAS firmware, and restore the NAS to factory default settings.	 General Settings Hardware Firmware Update 	 Storage & Snapshots Power Backup / Restore 	 Security Notification Center External Device more>> 	
	Privilege You can create users & groups, manage access permissions for local & domain users, and set up disk quotas.	LUSERS Quota	🔮 User Groups 🃩 Domain Security	🤕 Shared Folders 📣 Domain Controller	
	Network & File Services You can manage network connections, set up QUFT for file hadning, set retention nules for the network recycle bin, and enable NFS Service and WebXAV protocols and protocols for Microsoft and Apple.	X Network & Virtual Switch Telnet / SSH QuFTP Service	≫ Network Access <u>III</u> SNMP Network Recycle Bin	△ Win/Mac/NFS/WebDAV	
	(a) Applications You can use the web server and MariaDB to host	🜉 HDMI Display Applications	O Multimedia Console	📀 Web Server	

Click "Create" > "Create a User"

÷	Cont	t rol Panel					Q ()
ŝ	12	Users	Create - Delete	Advanced Settings -	1	.ocal Users	• Q
System	- 2	User Groups	Create a User	Description	Quota	Status	Action
	- 0	Shared Folders	Create Multiple Users	administrator	-	Enable	
ĕ	C	Quota	[Import/Export Users		Ξ.	Enable	?223:
Privilege		Domain Security					
6							
Network &		Domain Controller					
Application							



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



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

Control Banel	Control Panel		Q 🖆 🤅	ē (,	ি্র admin ▼	000	
Control Panel Control Panel System Prinlege Prinlege Prinlege Prinlege Prinlege Prinlege Prinlege Prinlege	Control Panel C	Create - Delete Advanced S demane admin # nasadmin new_admin	ettings •	▲ ↓ ↓ Lasta 202 202 1 2 00018 4 0 0 0 - 0 0 - 0 0 0 0 0	Logout	· .	× Q 0 Action 2 @ 2 2 @ 2

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

Control Pa	nel				- a ×
÷	Control	Panel			Q (?)
	🏩 Us	Create a User		X	Q. Action
O Privilege	i Sh C Qu Do A Do	2	User Description (optional)	User Group Close *	(7/8/2) 7/8/21
Network 8 File Service	is and the second se	Usemame:	new_admin	✓ everyone	
	21	Password:	ASCII: 0-64 characters, UTF-8: 0- 64 bytes Fair		
		Verify Password:	Show password		
		Mobile phone (optional): 🕕	Empty 💌		
		Email (optional): 🕕			
		User must change the pass	word at first logon		
				Create Cancel	Show 10 × Item(s)

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

HQ-MKT-NAS
<u>A</u> new_admin ⊗
Remember me
∟ Secure login

Set Password Policy

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

Control Pan	el							- a ×
÷	Control Panel							Q. (?)
£ĝ}	🤽 Users	Create -	Delete Advar	iced Settings -		Local Users	•	٩
System	🧟 User Groups	Usernai		Description	Quota	Status	Ac	tion
	Shared Folders	admin		administrator		Enable		80
8	Cuata	nasadm	in		-	Enable	Edit Ace	ount Profile
Privilege		new_ad	min 🛱		-	Enable		80:
	Domain Security							
Network &	📥 Domain Controller							
File Services								

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

← (ControlPanel			Q (?)
		Create Delete Advanced Settings Local Use	rs	* Q
	🔏 User Groups		tatus	Action
	Shared Folders	Edit Account Profile	hable	
	Quota		hable	
	Domain Security	User name: admin	hable	(? Ø (& (2) : :)
6	A Domain Controller	Email (optional):		
Network & File Services		Mobile phone (optional): 🕕 Empty 🔻		
		Description (optional): administrator	1000	
		Password valid to: Always valid		
replications		☑ Disable this account		
		Now		
		O Expiry date 2022/08/24		
		Note: Cannot set the quota size limitation for this user.		
		OK Cancel		

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

Control Pa	nel						- a ×
÷	ControlPanel						Q (?)
ξĝ3	🤽 Users	Create Delete Advanced Set	ttings -		Local Users	•	Q
System	i User Groups	Username			Status	Act	tion
	Shared Folders	admin admin	administrator	-	Disabled	24	1
2	C Quota	nasadmin nasadmin		-	Enable	704	1.
Privilege		□ new_admin ☵		=	Enable	724	1.
Network & File Service	Domain Security						

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 Two-Step Verification (2SV)

"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.



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.

	o	General Settings	Allow/Deny L	ist IP Access Protection	count Access Protection	SSL Certificate & Private Key Password Policy 2-Step Verification
System	ō	Storage & Snapshots	Disable account	its automatically when they fail too m	any login attempts within	a specified time period. You can view the disabled accounts in Users.
0		Security	Licere: All un	nore not in the administratore group		
C Privilege		Hardware	oscis. Paras	a a a a a a a a a a a a a a a a a a a		
<u> </u>	۲	Power	SSH	Time interval: 5 minute(s)	Failed login attempts:	: 5
🎲 Network &	2	Notification Center	Telnet	Time interval: 5 minute(s)	Failed login attempts:	5
File Services	٢	Firmware Update				★ If "Account Access Protection" is
⊞		Backup / Restore	HTTP(S)	Time interval: 5 minute(s)	Failed login attempts:	enabled for the administrator ac-
Applications	-	External Device	-	-		count, there is a chance that all ad-
		System Status	L] FIP	Time interval: 5 minute(s)	Falled login attempts:	ministrator accounts will be disabled
		QuLog Center	SAMBA	Time interval: 5 minute(s)	Failed login attempts:	due to password cracking attacks. At
	M	Resource Monitor				that time, the "admin" account can
		License Center	AFP	Time interval: 5 minute(s)	Failed login attempts:	⁶ only be re-enabled through the reset
			RTRR	Time interval: 5 minute(s)	Failed login attempts:	function, and the "admin" account password will also be reset. Remem-
			Rsync	Time interval: 5 minute(s)	Failed login attempts:	ber to change your password after
			Apply]		reset.

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.

36

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.

Options
2-Step Verification
2-step Verification adds an extra layer of protection to your account by requiring an additional one-time security code whenever you sign in to your NAS. For this function, you need a mobile device capable of running an authenticator app.
Status: Disabled
Get Started
Exit

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.

2-Step Verification	×
Confirm your 2-step verification settings	
Enter the security code generated by the authenticator app to ensure correct configuration.	
Security code: 377954	
Verify	
Successfully verified. You can now proceed to the next step.	
Back Next Cancel	

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.

Select an alternative verification method	
If you cannot use your mobile device, this alternative verification method can email you a security code or provide you with a security code by answering a security question.	·
 Security question 	
What is your pet's name?	
E-mail	
uniterengigene ant	
Step 2/2	

Change Default Ports

39

View Access Logs

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.



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.

40

	QuLog Center											:
	Overview	Acc	ess L	og								
	Local device		iroupin	g mode 🔹 🟟 Display si	syle • [→ E	Export Logs 🔹			Q Specif	ý keywords		•
	Event Log	Total	log ei	ntries:50								
	Access Log	8	0	A 13 () 37				Tip: Click	a severity level bu	utton to display the selected	severity leve	el logs.
	Online Users			Time	Hoor	Course ID	Compute	Connecti	Accesso	Action		
	Log Settings			2022/08/28 00:40:26	User	10.06.48	compute	CMP	Dublic/@	Read		
Ð	QuLog Service			2022/08/28 00:49:38	new_admin	10.20.40	cedito-m	OMD	Public/@	Deleted		-1
	Log Sender		•	2022/08/28 00:49:33	new_admin	10.26.48	ceanc-m	SMB	Public/Ac	Deleted		
	Log Receiver		0	2022/08/28 00:49:12	new_admin	10.26.48	cedric-m	SMB	Public/Ac	Read		
	Sender Devices		0	2022/08/28 00:49:12	new_admin	10.26.48	cedric-m	SMB	Public/Ac	Read	1	
	All Devices		(1)	2022/08/28 00:49:12	new_admin	10.26.48	cedric-m	SMB	Public/Ac	Read	:	
\wedge	Notification Settings		1	2022/08/28 00:49:00	new_admin	10.26.48	cedric-m	SMB	Public/.D	Read	:	
4	not not octango		1	2022/08/28 00:49:00	new_admin	10.26.48	cedric-m	SMB		Logged in	3	
			A	2022/08/28 00:48:58	new_admin	10.26.48	cedric-m	SMB		Failed to log in	:	
			4	2022/08/28 00:48:57	new_admin	10.26.48	cedric-m	SMB		Failed to log in		
			()	2022/08/28 00:17:00	nasadmin	10.26.48		HTTP	Administr	Logged in	:	
		144	(î) ∢	9099/08/97 93-50-01 Page 1 /1 ▶	now admin ⊮ g	10 26 AR		SSH/SETP Display item:	 1 - 50 ,Total: 50	Show 50	▼ Iten	n(s)

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.

QuLog	Center					- a ×
	QuLog Center					
іі Ф	Overview Local device	Log Settings Event Log Settings	ccess Log Settings	Event Indicators		
	Event Log Access Log Online Users	Maximum number of entries:	5 million	•		
2	Log Settings QuLog Service Log Sender	Archive and move log entries Destination folder: Destination folder: Destea All Access Logs	s to the specified location Please choose a destina	after reaching the datab	base limit.	
	Log Receiver Sender Devices All Devices Notification Settings	Connection Types Select the connections you want to	o log.			
₽		☑ HTTP/HTTPS ☑ FTP ☑ Telnet	☑ SSH/SI ☑ AFP (M ☑ SMB	-TP lac)	☑ ISCSI ☑ RADIUS ☑ WebDAV	
		Apply				

Install and Enable Security Apps

Security Counselor

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".



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.



43

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 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

QuFirewall

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.



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

QuFirewall	×	C		S 🗘	<u>ি</u> nasadmin •		(10+ (10+	۲
Firewall							-	a ×
								÷
	Get Started					Actio	in	
	🚱 Feature Integration	Profile Configuration	GeolP Initia	alization	Summary			
Firewall OFF	QuFirewall allows inbound p QTS Control Panel is incorp in one place.	backet inspection with multiple orated with QuFirewall to allow	customizable rules. users access and co	The security feature ontrol security functi	s of ons			
activate firewall services.	The <u>Control Panel > System</u> the installation process. Th	> Security > Allow/Deny List fue e Allow/Deny List is displayed a	unctions will be migra as a rule in the QuFire	ated to QuFirewall du ewall rule.	uring			
Firewall Profiles	O The migrated features QuFirewall is uninstalle	will be restored back to their ini d. The migrated features are no	tial configuration in C ot reserved by QuFire	TS Control Panel if wall after you uninst	all			
Event Counts	the application.				_			
Capture Events	Control Allow/Deny List		2 0	Firewall Profile :				
Notification Settings	8							
				Back	Next			

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.

QuFirewall		Q	é é	j 4	A admin • 8
QuFirewall					- 3
🥎 QuFirewall					
Firewall Profiles : 3					Add Profile 🗸
Profile Name					Rules Action
Service Service Basic protection					6 C :
Interface	ІР Туре	Service Port	Protocol	Source	Permission
Firewall ON Application (3)]				Allow
OuFirewall has denied access to					Deny
0 events in the last 24 hours. TOR (1530)					Deny
Denied IP addresses (0)					Deny
Firewall Profiles Adapter 1	IPv4	Any	Any	10.26.0.0/16	Allow
Event Counts	IPv4	Any	Any	Hong Kong	Allow
All	IPv4	Any	Any	Any	Deny
Capture Events PSIRTv6 (0)					Deny
Notification Settings [2]					Deny
Adapter 1	IPv6	Any	Any	fe80::/64	Allow
All	IPv6	Any	Any	Hong Kong	Allow
All	IPv6	Any	Any	Any	Deny

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.

49

QuFirewall		and the second of the	(- 0	
े QuFirewall									
Fi Pr	rewal rofile	l Profiles : 3	Rules	Add Profile V Editation					
	0	Basic protection Enabled					6	C :	
		Interface	ІР Туре	Service Port	Protocol	Source	F	Permission	
Firewall 💿 🔵	Firewall ON Application (3) 📟								
OuFirewall has denied access to		PSIRT (1641)					D	leny	
0 events in the last 24 hours.		TOR (1530)					D	leny	
		Denied IP addresses (0) 🔤					Deny		
E Firewall Profiles		Adapter 1	IPv4	Any	Any 10.26.0.0/16		A	llow	
Event Counts		All	IPv4	Any	Any	Hong Kong	A	llow	
		All	IPv4	Any	Any	Any	D	leny	
Capture Events		PSIRTv6 (0)					D	leny	
Notification Settings [2]		TORv6 (845)					C	leny	
		Adapter 1	IPv6	Any	Any	fe80::/64	A	llow	
		All	IPv6	Any	Any	Hong Kong	A	llow	
		All	IPv6	Any	Any	Any	C	leny	

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.

	irewall X				Q	É	A (10 1	<u>ি</u> admin ▼	••••	•
QuFirewall										
	Edit Profi	e						->	Add Profile	~
Ø	Profile Name	Basic p	IPv6 Rules (3)				C	+ Add Rule	C :	
Firewall 💿	Priority (Ø ON	Interface	Service Port	Protocol	Source	Permission	Action		
QuFirewall has denied			Application (3) 🔤				Allow			
u events in the last 24	\equiv		PSIRT (1641)				Deny			
Firewall Profile	=		TOR (1530)				Deny			
Event Counts	=		Denied IP addresse	es (0) 🛄			Deny			
	=		Adapter 1	Any	Any	10.26.0.0/16	Allow	CŪ		
Capture Events	=		All	Any	Any	Hong Kong	Allow	20		
Notification Se	The defau priority to	It profiles a provide ad	illow access to all inte ded security to your d	erfaces by default. evice.	. QNAP recomme	ends adding a "d	eny all" rule and assignin	g it the lowest		
	Diag a	ina are	op to chang	eorder			Apply	Cancel		

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".

	Edit Profile							- :	Add Profil
	Profile Name	Basic p	rotection						re: :
	IPv4 Rule	s (4)	IPv6 Rules (4	4)			(+	- Add Rule	ssion
	Priority 🕕	ON 🖸	Interface	Service Port	Protocol	Source	Permission	Action	
s denied	≡		Application (3)				Allow		_
ast 24	≡	\checkmark	PSIRT (1641)				Deny		
Profile	≡		TOR (1530)				Deny		
ounte	≡		Denied IP addre	sses (0) 🚥			Deny		
Junis	=		All	Any	Any	Taiwan	Allow	60	
Events	≡		Adapter 1	Any	Any	10.26.0.0/16	Allow	60	
tion Se	The default	profiles a	llow access to all	interfaces by default. (NAP recomme	ends adding a "deny	all" rule and assigning	it the lowest	

Enable Scheduled Snapshots

51

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.

\star You must b	* You must back up your data before converting volumes to avoid potential data loss.													
Storage & Snapshots								- = >						
清 Storage & Snap	shots					Exte	ernal Storage Devices 🔻	\$ @ \$						
🐼 Overview		Storage Space Stor	age Pool: 1, Volume: 3,	LUN: 0	[Create	• Snapshot •	Manage 🖸						
		Name/Alias	Status	Туре	Snapshot Re	Snapshot	Capacity Percent Used							
Storage		🗸 Storage Pool 1 🧅	📀 Ready				5.83 TB							
Disks/VJBOD		금 Data	🛛 Ready	Thin volume	-	-	2.97 TB							
Storage/Snapshots		🛁 System (Syste	m) 🛛 🐼 Ready	Thin volume	-	10 :9	98.20 GB							
Cache Acceleration		Thick	🧭 Ready	Thick volume	-	-	494.54 GB							
External Storage														
 Overview Storage Diska/VJBOD Storage/Snaps Cache Accelera External Storag Remote Disk Topology Snapehot Back Snapehot Baci 	Thick Name/Alia Capacity: Free Size: Thin: No SSD cach Status: F Utilization 100 %	Management 1: Thick 494.45.468 € 494.47.68 2: - :- :- :- :- :- :- :- :- :- :	· Open Thick djustments to	■ Used 0.0 Management t free up "Storag	1%(72.04 MB) ■ Free S o make relev se Pool" space	Size: 99.99% (////////////////////////////////////	+ × Actions • C Remove Resize Volume Set Threshold Set Caching Storage Check File System Rename Volume Alias Format Convert to Thin Volume	Manage 🖓						

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.

Storage & Snapshots — 💷 🗙									
Storage & Snapshots									
🔗 Overview	Storage Space Storage Pool: 1, Volume: 2, LUN: 0				Create	•	Snapshot 🗸 Man	age 🖸	
Storane	Name/Alias	Status	Туре	Snapshot Rep	Snapshot	Сар	Take a Snapshot		
	🗸 Storage Pool 1 🧅	🔇 Ready		_			Snapshot Replica		
DISKS/VJBOD	🕞 Data	📀 Ready	Thin volume	-	-	1	Snapshot Manager		
Storage/Snapshots	Gystem (System)	🧭 Ready	Thin volume	-	10 :9		Import Spanshot	_	
Cache Acceleration							Global Settings		
External Storage							Giobal Settings		

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.

D 9	📴 Snapsho	Nt Manager Repol Guaranteed Snaps	hot Space - 🔅 ?
⊘ Ov ⊜ Sta	D R	Snapshot Settings Schedule Snapshot Retention Pool Guaranteed Snapshot Space	×] G
Di	Q, ∷≣+ () () Name(0/0)	How many Snapshot can I have? The snapshot retention policy determines how long to keep a snapshot or how many total snapshots to keep. When the specifies value is exceeded, the system deletes the expired snapshot or the oldest snapshot automatically.	Copen in File Station
Ca Ex Re		Maximum amount of time to keep: 0 Months Maximum number of snapshots to keep: 0 Snapshots	
		Smart Versioning Hourly snapshots: 24	
li⊙ Sn Sr		Daily snapshots: 7	
		Weekly snapshots: 4 Monthly snapshots: 12	
OK HM			and the second se

Set Snapshot Deletion Policy

NAS Security Settings Checklist

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



□ 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"



54

FAQ

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

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.

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

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.

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

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.

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

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?

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?

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.

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

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

Why do I keep getting a NAS login failure warning?

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.

Why do all my files have strange filenames?

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.

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

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.

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

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.





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:





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.

		QNAP
	1111	2 0 2 3
МЕМО		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

QNAP may make changes to specification and product descriptions at any time, without notice. Copyright $\[mathbb{C}$ 2023 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.