Security Handbook

Protection Guidelines to keep your NAS Safe & Secure

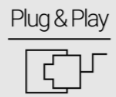
Safety Sheet – Basic things you can not ignore

FIRST TIME INITIATING NAS

Administrator
Don't use default settings!
Create a new admin

Passwords
Use secure Password policies

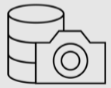
2FA
Enhances the security
of user accounts



UPnP
Turn off Plug and Play
to avoid attackers

EVERYDAY / REGULAR TASKS

Backup
More than one backup location!
Use 3-2-1 Backup Strategy



Snapshots
Capture data constantly
to present data lost

Updates
Keep software
up-to-date automatically

VPN
Establish a VPN connection
for remote access

ONE TIME TASK - ENABLE & BE SAFE PERMANENTLY

QuFirewall
Download from APP center
and enable it

Security Counselor
Download from APP center
and enable it

Safety Sheet – Advanced settings for IT

FOR PEOPLE WITH A BIT MORE KNOW HOW

Introduction

Security Guide

In this short security guide, you will find some useful explanations about which settings you can use to ensure the optimal protection of your data.

There is always a trade-off between comfort and security, which every user must decide for themselves.

This guide provides a short overview of the most important topics.

Detailed information and instructions can be found at: https://www.qnap.com/en

What is ransomware?

Ransomware are malicious programs that lock the computer or encrypt files and block you from accessing your own data.

Victims will be extorted a ransom to decrypt the affected files, or they will be unable to open the affect files ever again.

How can you protect yourself from ransomware?

Ransomware is a rising threat against both business and home users that targets computers and network-based devices.

Hackers are constantly finding new ways to place malicious software.

QNAP is aware of this increasing danger and is constantly working to provide the best possible protection against malware.

The following examples are intended to show you how you can best protect yourself according to your needs.

When first time initiating NAS

Administrator Account

The administrator account on QTS is „admin“ by default. For security reasons, it is not recommended to choose a generic and easily guessable name for a system-critical account, as this way a possible hacker only needs to guess the correct password to gain complete control over your system. To protect yourself from such a scenario, we strongly recommend creating another system administrator account and disabling the default „admin“ account. Furthermore, an administrator account should only be used for administrative tasks, such as maintenance tasks. For the actual use of the QNAP NAS, it is recommended to strictly separate administrator functions and user functions.

Note: The option to disable the „admin“ account is only available on QTS 4.1.2 or higher versions.

CREATE NEW ADMINISTRATOR ACCOUNT

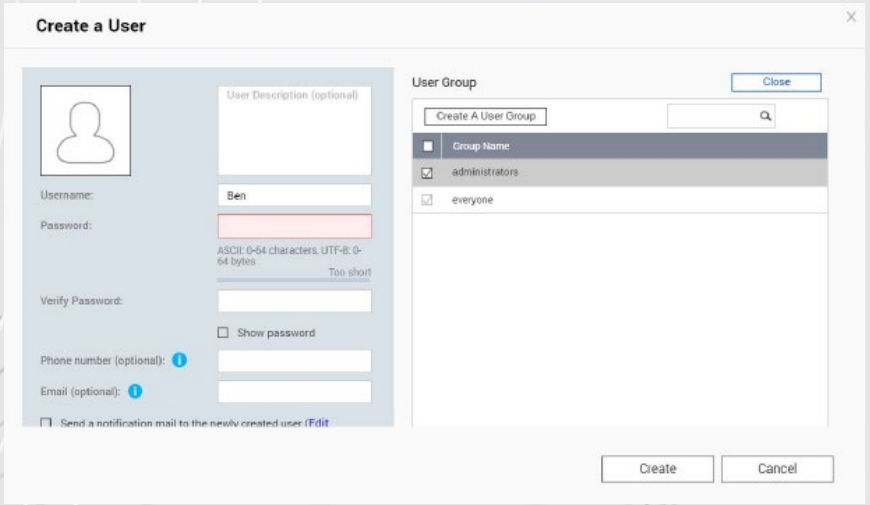
DISABLE THE ADMINISTRATOR ACCOUNT „ADMIN“

USE ADMINISTRATOR ACCOUNT ONLY FOR ADMINISTRATIVE TASKS

When first time initiating NAS

How to deactivate the “Admin“ User account

For passwords on your QNAP NAS, there are a few setup options that will greatly increase the security of your system. Of course, if you use your QNAP NAS exclusively on your own, only you are responsible for implementing the recommended rules for passwords. The basic rules for a secure password are simple:

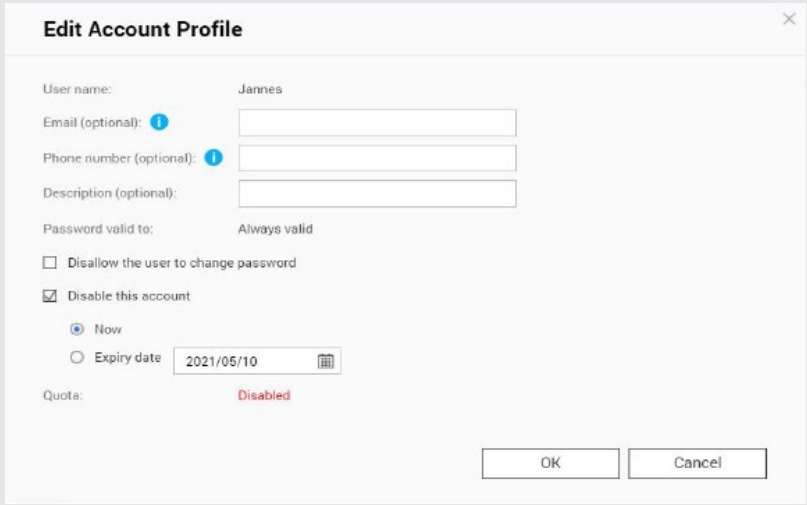


Create a new administrators account

1. Log in to QTS using the „admin“ account.

2. Select Control Panel > Users.

3. Create a user (in this example „Ben“) and assign him to the „Administrators“ user group.



Disable „Admin“ account

1. Log in to QTS as Ben.

2. Select Control Panel > Users and edit the „admin“ account profile.

3. Click „Disable this account“ and select „OK“.

When first time initiating NAS

Password Policies

For passwords on your QNAP NAS, there are a few setup options that will greatly increase the security of your system.

Of course, if you use your QNAP NAS exclusively on your own, only you are responsible for implementing the recommended rules for passwords.

The basic rules for a secure password are simple:

Sufficiently long

Special characters

Lower and upper case letters

Never use the same password for different applications

Change the password regularly

If the QNAP NAS is also available to other users, the administrator should set certain rules for passwords and have them enforced by the QNAP NAS.

This will ensure that the rules mentioned above are followed. A brief explanation can be found on the following page.

When first time initiating NAS

Password Policies

1. Go to Control Panel > System > Security > Password Policy.

2. Under Password strength, select the criteria

1. The new password contains characters from at least three of the following classes: Lowercase letters, uppercase letters, digits and special characters.

2. No character in the new password may be repeated three times (or more) (example: AAA).

3. The password must not be the same as the corresponding user name, not even backwards.

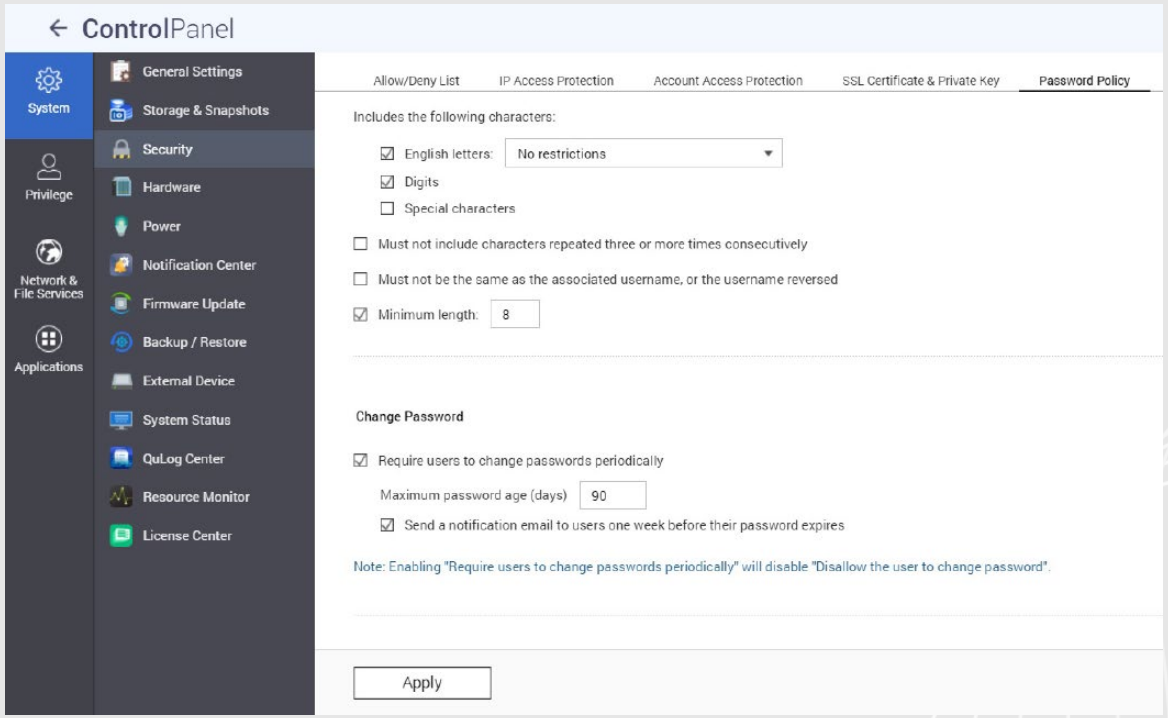
3. Under Change Password, select Require users to change passwords periodically

Important: Enabling this setting disables the setting Prohibit users from changing the password

1. Specify the maximum number of days for which the password is valid

2. Optional: Select Send a notification email to users one week before their password expires

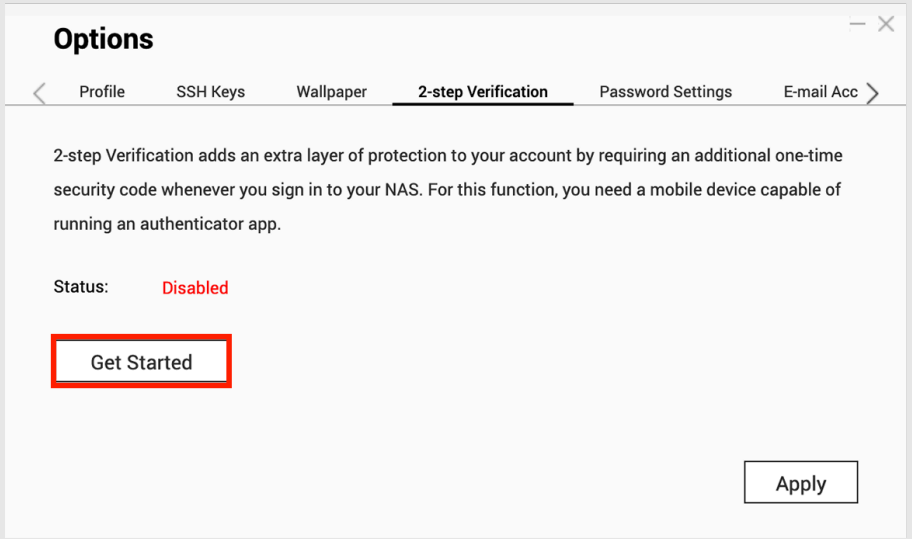
4. Click apply.

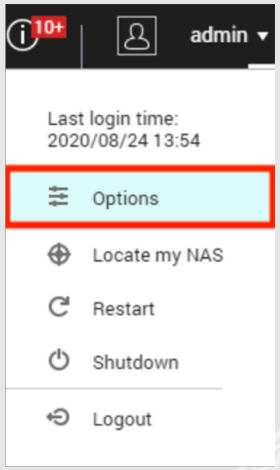


When first time initiating NAS

2FA

2-step verification enhances the security of user accounts. Once enabled, you will need to enter a one-time security code (6 digits) in addition to your password whenever you sign in to the NAS. 2-step verification requires a mobile device with an authenticator app which supports the Time-based One-Time password (TOTP) protocol. Supported apps include Google Authenticator (Android/iPhone/BlackBerry)
or Authenticator (Windows Phone).To use this function, follow the below steps:





1. Install the authenticator app on your mobile device.

2. Under Password strength, select the criteria

3. Go to "Options" > "2-step Verification" and click "Get Started".

1. Configure your authenticator app by scanning the QR code or by entering the Secret Key into the app.

2. Enter the code generated from the app to the NAS to verify the correct configuration.

3. Select an alternative verification method by emailing you a security code or by answering a security question if you cannot use your mobile device. To email a security code, the SMTP server must be properly configured in “Control Panel” > “Notification” >”E-mail”

A detailed explanation of the setup, can be found on our tutorial website:
https://www.qnap.com/en/how-to/tutorial/article/how-to-enhance-account-security-using-2-step-verification

When first time initiating NAS

Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is used to control devices (audio devices, routers, printers, smart TVs) across manufacturers. It allows devices in the network to understand each other and certain functions to run automatically without the user having to become active. In this case, for example, the QNAP NAS can use UPnP to instruct the router to simply let certain incoming connection requests through. Again, it's up to you to balance between convenience and security. For less experienced users, we recommend disabling the UPnP feature on your router and in your QNAP NAS. You can find out how to make these settings on your router from the manufacturer of your router.

Important:

If UPnP is enabled in your router, any software and device in your home network can configure the router as desired. Thus, it is possible that certain ports are opened in the firewall. These serve as an entrance for attacks from outside.

Dont connect the NAS to the WAN from a Modem, we strongly suggest building up the NAS behind the Router.

Disable UPnP forwarding on the QNAP NAS

1. Go to myQNAPcloud > Auto Router Configuration

2. Uncheck „Enable UPnP Port forwarding“ and Apply

Everyday / Regular Tasks

3-2-1 Backup Strategy

Backup

It is an individual question where, how and how often you back up your data. The decisive factors here are security needs, the relevance of the data and the available options.

However, there is a rule of thumb that should be followed to reliably back up important data.

Important: *RAID is not a backup, it protects you against hard disk failures. Snapshots protect you against ransomware attacks from your local computer.*

The 3-2-1 Backup Strategy

While the first line of defense against being affected by malicious software is being careful and practicing sensible usage habits

(regularly updating your software, not opening untrustworthy emails, not visiting unknown websites, etc), you should always remember to back up your data.

No backup plan is perfect, but 3-2-1 Backup is a good start. Keep 3 copies of important files, keep the files on at least 2 types of storage media, and store 1 copy off-site.

Important data should be backed up at least **3 copies**: 1 main file and 2 backup files.

One of the backups is to be stored offsite (outside the home or business).

Archives are stored on **2 different** backup media to protect against various types of hazards.

Everyday / Regular Tasks

Snapshots

What are snapshots?

Snapshots are images of the data you have saved on your QNAP NAS. The first time you take a snapshot, all of your storage is captured. All subsequent snapshots then only record the content that has changed since the last snapshot. Snapshots are very space saving because they are block based.

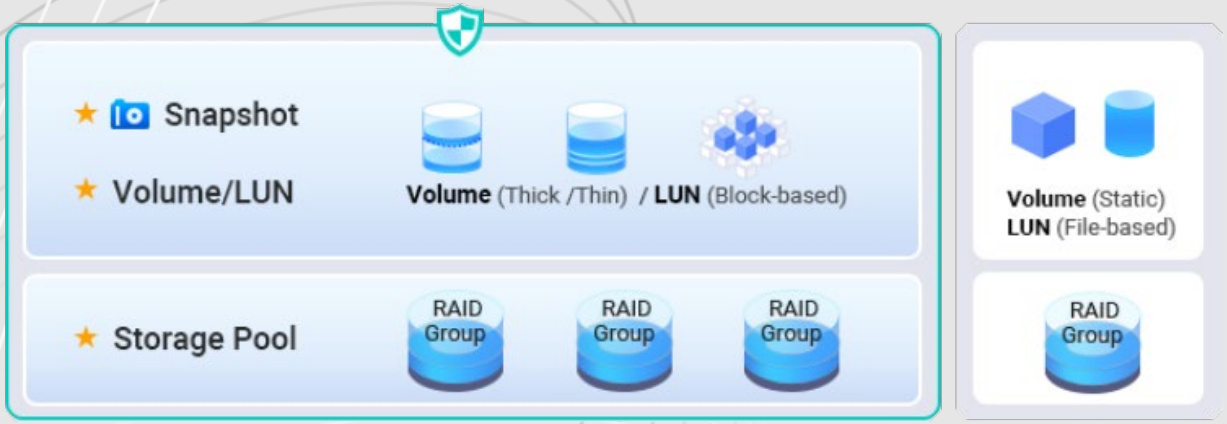
Important:

Snapshot is not a backup. It allows access to previous versions in case they were accidentally deleted or content was accidentally changed.

You can find a detailed description of this topic on our website:

https://www.qnap.com/solution/snapshots/en-us/

Setup Snapshots



Everyday / Regular Tasks

Automatic Updates

Updates

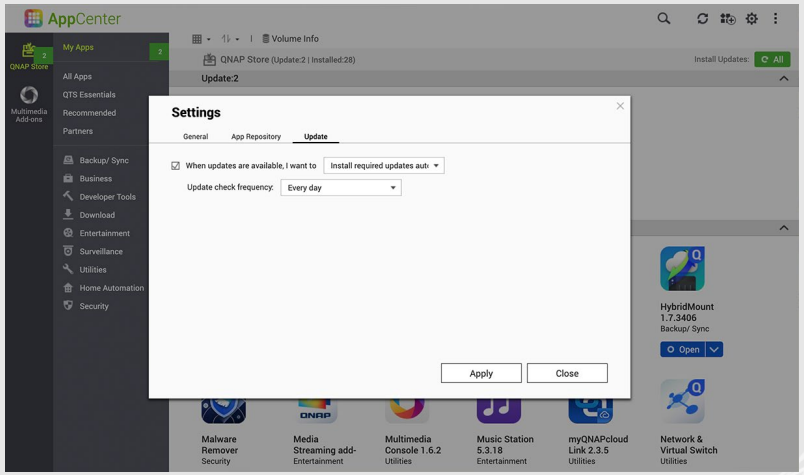
Up-to-date system software is important with your NAS. QNAP is constantly working to close emerging security gaps and occasionally adds new features to the system.
Updates should therefore always be applied promptly in order to protect your data as best as possible.
If your QNAP NAS is connected to the internet and you have not changed the default settings, your device will automatically check for the latest system software and alert you to it.
You should then make sure to update it. Be aware that your QNAP NAS will need a reboot to do this and will be unavailable for 5-10 minutes. You also have the option to manually install the latest system software.
This is necessary if your QNAP NAS is not connected to the internet and thus cannot automatically check for and download updates. If you want to know if your firmware is up to date, please do the following.

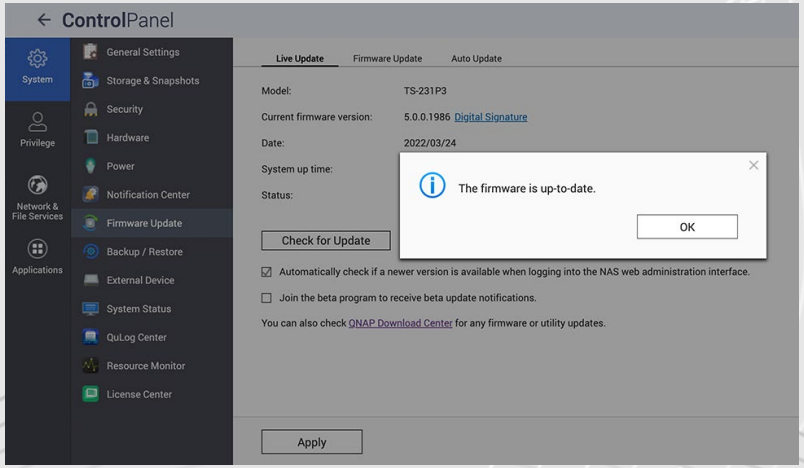
Real time firmware update

1. Log in as ‚Administrator‘
2. Open Control Panel > Firmware Update
3. Open Live Update
4. Click Check for update

Update apps automatically

1. Go to App Center
2. Go to settings
3. Open Update
4. Select „When updates are available…“
5. Select Install all updates automatically





Everyday / Regular Tasks

VPN

What is VPN?

VPN is a virtual private network. In our case, it is intended to establish secure access to the QNAP NAS while on the road. A VPN server runs on the QNAP NAS and a special VPN software runs on the device that is used on the road. A tunnel is set up between these two through the Internet. The advantage of this is that the connection is protected by authentication and encryption and can only be used by authorized persons. Such a VPN connection therefore behaves in the same way as if both devices were logged into the same network. This means that local resources can be accessed without further ado. Once set up, the VPN connection can be easily used again and again and secure access to the home network is guaranteed.We always recommend establishing a connection via VPN while on the road. The speed of data transfer suffers somewhat, but the connection is secure.

How to set up and use VPN?

A detailed explanation of the setup, can be found on our tutorial website:
https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn

Recommendation for remote access

myQNAPcloud Link & VPN (Port Forwarding VPN Service Ports required,
we recommend to enable QuFirewall for better protection)

One time Tasks

QuFirewall

What is QuFirewall

QuFirewall is a firewall management application for your QNAP device. By integrating a powerful and easy-to-use profiling system, QuFirewall allows you to control and verify connections to your device. QNAP recommends that you install QuFirewall on your QNAP NAS and limit the allowed IP addresses to a specific region or subnet.

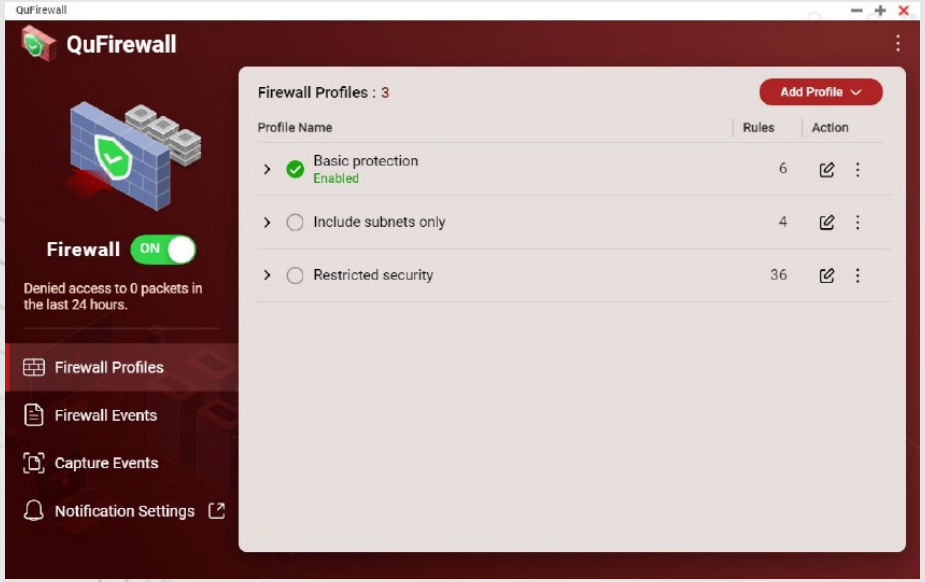
Setup QuFirewall

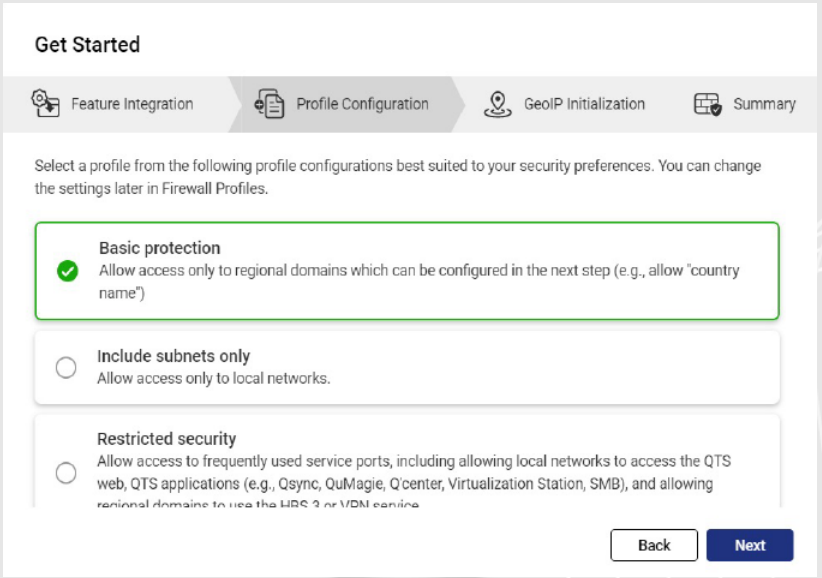
1. Install QuFirewall from the App Center

2. Select a profile configuration

3. Choose your region

4. Click Finish





One time Tasks

Security Counselor

What is „Security Counselor“?

Security Counselor is your security portal for QNAP NAS. It scans your system for vulnerabilities and provides recommendations to protect your data against various attack methods. Based on the security requirements of your network environment, you can choose one of the three default security policies (Basic/Intermediate/Advanced). The Security Checkup function will use your selected policy when it scans your system. You can also configure your own policy by selecting the Custom security policy.

Basic

Intermediate

Advance

Custom

A security scan can be performed manually or on a schedule to ensure maximum protection.

The schedule can be set in different ways (daily/weekday/weekend/specific day of the week) to ensure that your work is not interrupted.

You can click on the scan results and Security Counselor will guide you to the appropriate system section to change the related settings to secure your NAS.

One time Tasks

Security Counselor

Set up „Security Counselor“

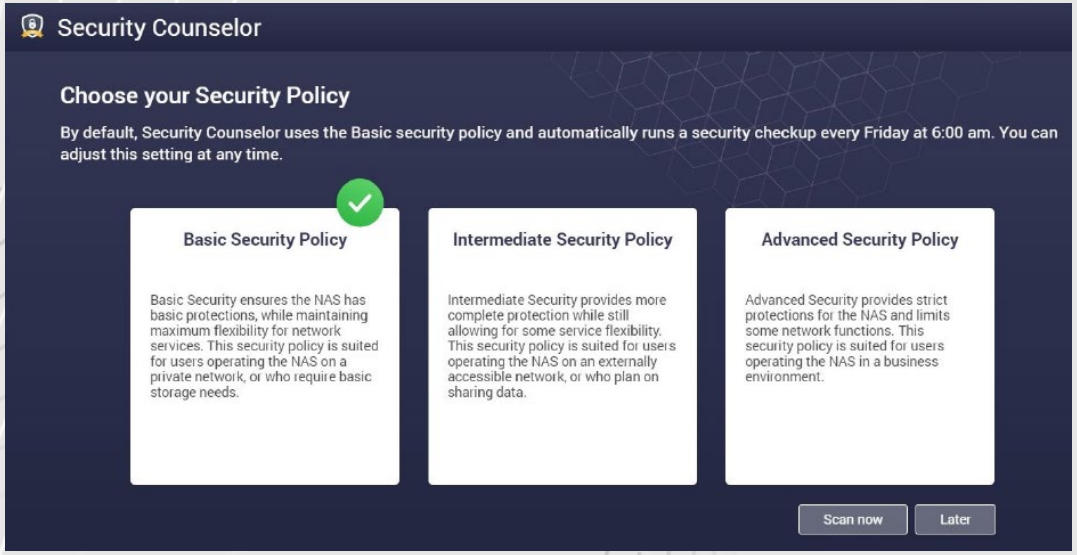
1. Download Security Counselor from the App Center

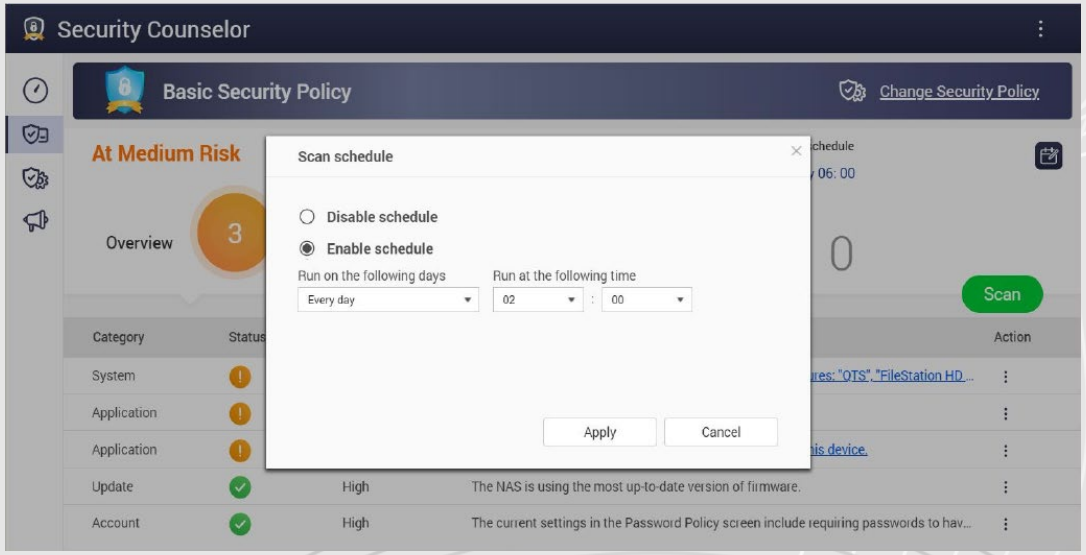
2. Choose a Security Policy an click on Scan now

3. To create a schedule, go to the Security Checkup (green)

4. Go to Scan schedule (rot)

5. Select your desired times and click Apply





Advanced settings

Encryped Connection

Use encrypted HTTPS connections

If you want to connect to your QNAP NAS from outside of your own network, you should make sure that the data is encrypted. This protects you from third parties being able to „read“ your data. You can ensure this by using protected connections. These are, for example, HTTPS instead of HTTP or FTPS instead of FTP. The S stands for „Secure“. The data transfer is now encrypted with a certificate so that the authenticity of the respective party is ensured.

1. Open Control Panel > System > Security and go to the SSL Certificate & Private Key .

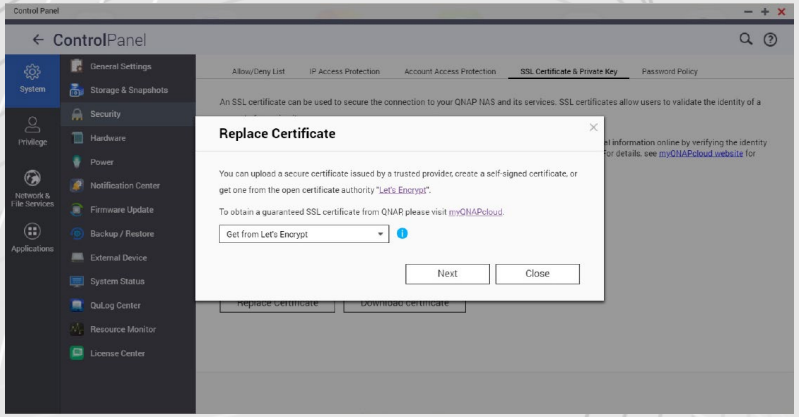
2. Click Replace Certificate.

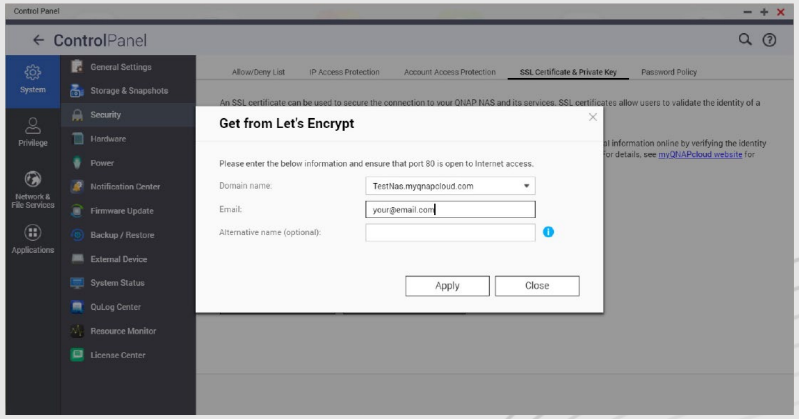
3. Select Get from Let’s Encrypt.

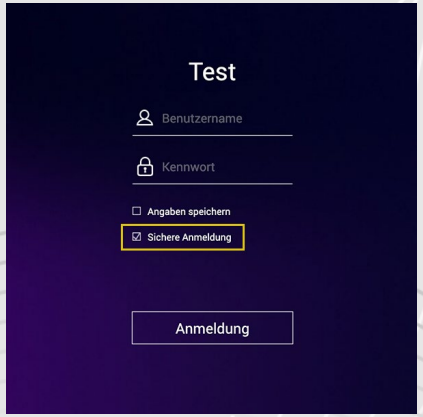
4. Under Domain name, enter the name or DDNS under which the NAS can be reached.

5. Enter your e-mail address for registration with Lets’s Encrypt.

6. Select Secure login when logging in to the web interface







Advanced settings

Ports

What are ports?

A port allows communication between your computer and another computer as well as the internet. A firewall closes unused ports to prevent malware from entering your computer through them. By setting up port forwarding, you can use online services and other internet applications that accept connections from the internet or allow users on the internet to access web and remote servers and other services on your home network.

Changing the default ports

You should change the default ports in your router’s configuration such as 21, 22, 80. 443. 8080 and 8081 to random custom port numbers. For example, change port number 8080 to 9527. For information on how to do this, contact your router manufacturer.

DO NOT PORT FORWARDING "System Port" / unnecessary service ports (e.g. SSH, Telnet)

Disable port forwarding on unnecessary service ports can reduce attack surface. After port forwarding, these service ports can be access by anybody via Internet

Instructions

Backup:	https://www.qnap.com/en/how-to/tutorial/article/hybrid-backup-sync
Admin account:	https://www.qnap.com/en/how-to/faq/article/can-i-rename-the-default-admin-account
Password policy:	https://www.qnap.com/en/how-to/knowledge-base/article/setup-the-password-policy-to-require-the-change-periodically
UPnP:	https://docs.qnap.com/nas-outdated/QTS4.3.5/en/GUID-907F01D9-68D9-4449-A4D1-3213E19D0124.html?
Encryption:	https://www.qnap.com/en/how-to/tutorial/article/how-to-use-ssl-certificates-to-increase-the-connection-security-to-your-qnap-nas
VPN:	https://www.qnap.com/en/how-to/tutorial/article/how-to-set-up-and-use-qvpn
Port forwarding:	https://www.qnap.com/en/how-to/faq/article/how-do-i-set-up-port-forwarding-on-the-nas
How to use QuFirewall:	https://www.qnap.com/en/how-to/tutorial/article/how-to-use-qufirewall
Updates:	https://www.qnap.com/en/how-to/tutorial/article/how-to-update-your-qnap-nass-firmware
Security Counselor:	https://www.qnap.com/solution/security-counselor/en-us/