

# Synology Security Guide & Best Practices

Steps for securing Synology NAS system

- [User Security & Access Control](#)
- [Remote Access Setup](#)
- [Synology Firewall Setup](#)

# User Security & Access Control

The majority of NAS security needs to be done preventatively to easily recover from potential issues that might arise in the future.

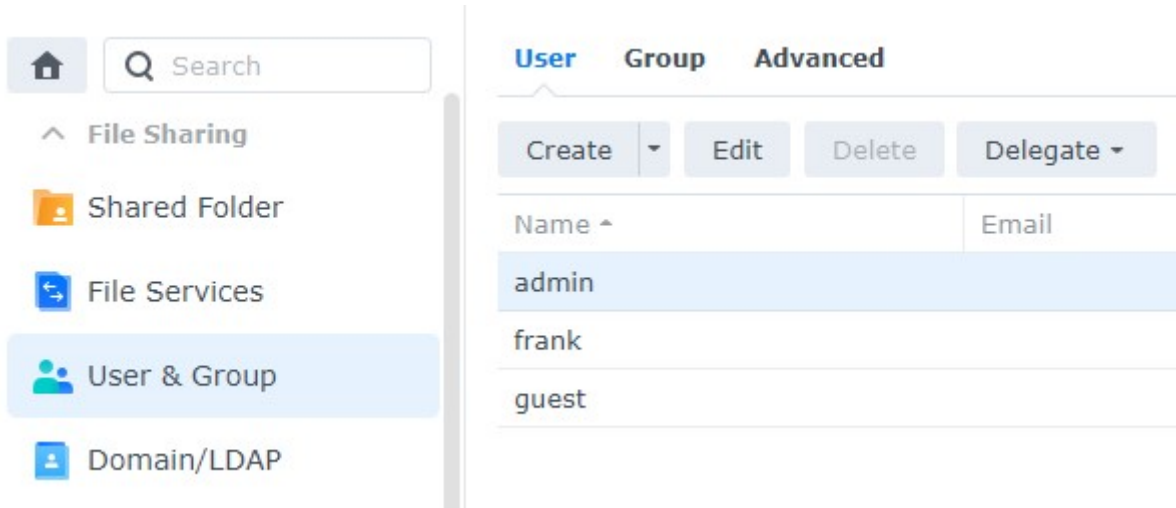
It's important to note that cybersecurity is always evolving and staying up to date with best practices is important. These are things I normally change, but depending on your needs, you can potentially secure your NAS even further.

Making sure that every user on NAS system is properly created, assigned, and given least amount of privilege, can help with reducing any type of cyberattack.

## Disable Admin Account

First we must create a new user and ensure that they have admin permissions before disabling the admin user. Disabling Guest account is good practice as well, but it's personal preference, if group based access is properly managed.

1. Select **Control Panel**, then select **User & Group** and **Edit** the admin user



1. Select **Disable this account**, then select **Save**. This will ensure that the admin account is disabled

**Info** User Groups Permissions Quota Speed Limit

Name \*:

Description:

Email:

Password: Last changed: 09/15/2020

[Change Password](#)


Disallow the user to change account password

Password is always valid if the password expiration is enabled

Disable this account

Immediately

After:

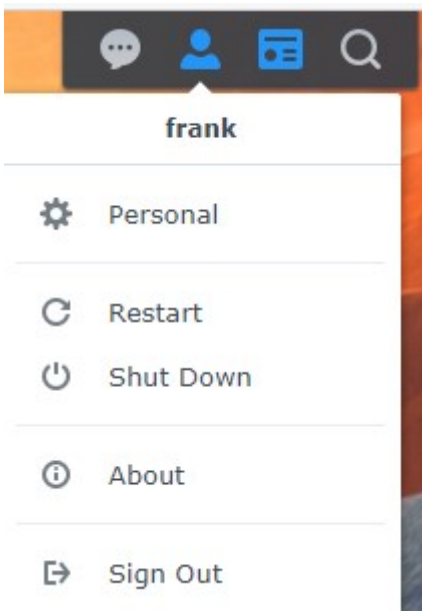
\* This field is required.

[Cancel](#)

[Save](#)

## Enable Two Factor Authentication

1. Select the **Person** icon in the top right and select **Personal**



2. Select **Enable 2-step Authentication**. The email service will need to be enabled for this

## Sign-in Method

Use a verification code (OTP) as the second sign-in step to strengthen your account security.

### 2-Factor Authentication

Add an extra layer of security by implementing a second authentication step.



3. Select **2-step Authentication**, then **Verification code (OTP)**.
4. Select **Next** to protect your DSM account with **2-factor Authentication**

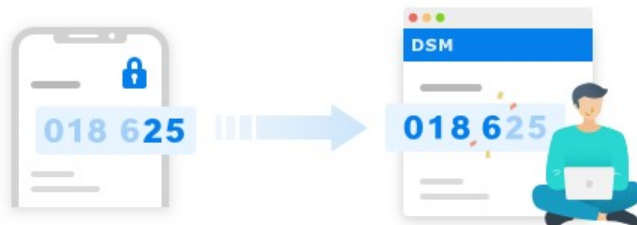
#### Set up 2-factor authentication



### Protect your DSM account with 2-factor authentication

2-factor authentication requires you to enter your password along with a verification code (OTP) when signing in to VirtualDSM. You can receive an OTP code even if your mobile device is offline.

**Note:** Enabling 2-factor authentication applies to Synology package logins. [Learn more](#)



Back

Next

The next section will suggest that you install Synology's Secure SignIn. **This is not required.** This is simply Synology's TOTP application – you are free to use whatever TOTP application you'd like.

5. Scan the **QR code**, enter the **code**, then select **Next**.
6. Set up the **Email service provider**, then select **Next**
7. Two-factor authentication is now set up

If you'd like to force all users to set up two-factor authentication

1. Go to **Control Panel**
2. Under **Security** select **Account** and under 2-Factor Authentication select All users or Specific users or groups. It's good idea to have any users that can remotely access NAS to have MFA setup, both TOTP and Push Notification with **Synology Secure SignIn**

The screenshot shows the Windows Control Panel interface. On the left is a navigation pane with categories like File Sharing, User & Group, and Security. The main area is titled 'Account' and shows 'Secure SignIn Service' with a status of 'Connection failed'. Below that, the '2-Factor Authentication' section is expanded, showing a checkbox for 'Enforce 2-factor authentication for the following users' with radio button options for 'Administrator group users', 'All users', and 'Specific users or groups'. A 'Settings' button is visible below these options. A note at the bottom of the section says 'Note: You can set up 2-factor authentication for your account in [Personal](#).' The 'Account Protection' section is partially visible at the bottom.

## Enable Auto Block

Auto block will automatically block IP addresses that have failed a certain number of logins during a certain period of time.

1. Open **Control Panel** and select **Security**
2. Select **Account**. Ensure **Enable auto block** is selected. Set the **Login Attempts** and **Within parameters** to be what you'd like, then apply. This will ensure that IP addresses are automatically blocked after a certain number of failed login attempts

The screenshot shows the Windows Control Panel interface. On the left, the 'Security' category is selected. The main content area is titled 'Protection' and contains the 'Auto Block' settings. The 'Enable auto block' checkbox is checked. Below it, there are input fields for 'Login attempts' (set to 5) and 'Within (minutes)' (set to 10). The 'Enable block expiration' checkbox is unchecked. Below that, there is an input field for 'Unblock after (days)' (set to 0).

Control Panel

Security Account Firewall Protection Certificate Advanced

^ Auto Block

Enable this option to block IP addresses with too many failed login attempts. For support, see DSM Help.

Enable auto block

An IP address will be blocked if it reaches the number of failed login attempts with

Login attempts:

Within (minutes):

Enable block expiration

When block expiration is enabled, blocked IP addresses will be unblocked after the

Unblock after (days):

## Disable SSH

There are multiple reasons why you might want to use SSH, but if you're not **actively** using it, you should disable it. Even if you enable two-factor authentication above, SSH does **not** use it. For this reason, if your network is compromised, an attacker can try and brute force your password through SSH.

1. Open **Control Panel**, then select **Terminal & SNMP**.
2. Ensure that **Enable SSH** service is not checked off.

- Home
- Search
- File Sharing
  - Shared Folder
  - File Services
- User & Group
- Domain/LDAP
- Connectivity
  - External Access
  - Network
  - Security
- Terminal & SNMP

Terminal SNMP

Use Terminal service to login and manage your system. SSH/Tel administrators group. Please refer to [Terminal](#) for more details.

Enable Telnet service

Enable SSH service

Port:

Advanced Settings

**Note:** It is recommended to set a strong password for the login

# Remote Access Setup

# Synology Firewall Setup