

UGREEN NAS Knowledge Center:

Please click the link for video tutorials and application guide and more troubleshooting.

<https://support.ugnas.com/knowledgecenter/#/detail/eyJjb2RlIjojMCYmVlNkVndRlnO=>

The screenshot displays the UGREEN NAS Knowledge Center website. The top navigation bar includes links for Homepage, Application Tutorials, Video Tutorials, and Download Center. The main content area is titled "User Guide" and features a grid of 15 video tutorial thumbnails. The left sidebar contains a "Knowledge Base" section with a search bar and a list of categories including Application Guide, Video Tutorials, Installation Guide, Features Overview, and User Guide. The "User Guide" category is expanded, showing a list of topics such as "How to apply for TMDB API Key", "How to Set Up a Local Kodi NAS Library", "How to Set Up 2FA", "Getting to Know the Theater Player", "How to Perform Comprehensive...", "How to Add External Subtitles in Theater", "How to Achieve Two Way Data Sync Between...", "How to Add Peripheral or Network Folder as a...", "How to Set Up a Video Library", "How to Mount a UGREEN NAS iSCSI...", "How to use Collections in Theater", "How to Set Up Automatic Photo...", "How to Access Files on UGREEN NAS through...", and "How to use SMB protocol to achieve fa...".

How to Deploy Kavita on UGREEN NAS

The screenshot shows a video player displaying a tutorial titled "How to Deploy Kavita on UGREEN NAS". The video content shows a Kavita web interface with a sidebar menu and a main area displaying a list of books. The text "you can organize your own library efficiently" is visible at the bottom of the video frame.

```
services:
  kavita:
    image: jymilazzo/kavita:latest
    container_name: kavita
```

What troubleshooting does this file cover?

Please press Ctrl+F or Command+F on your keyboard and enter the problem

keywords to locate the corresponding solutions.

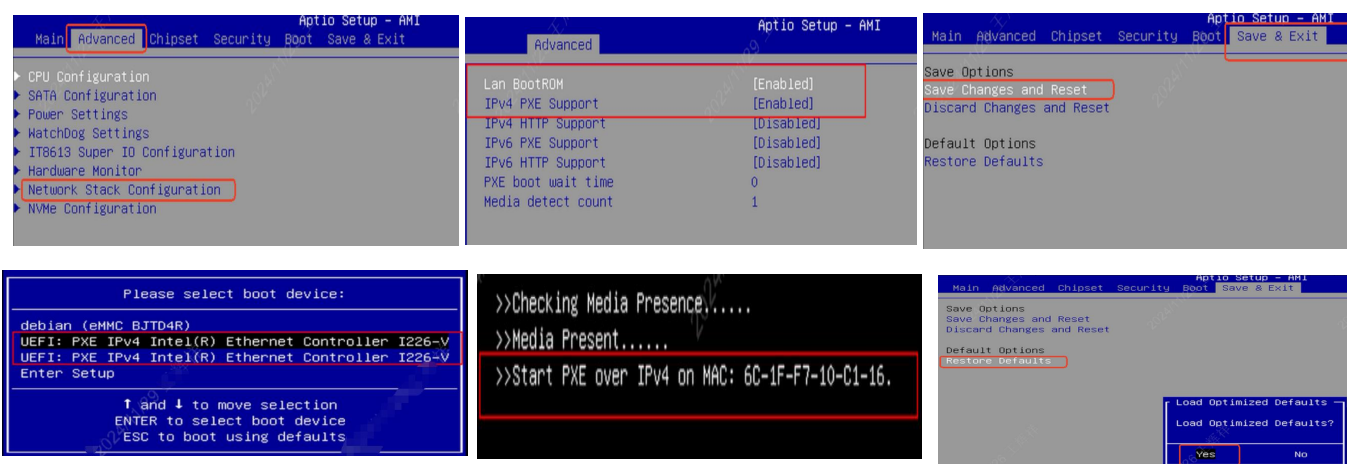
- Network Troubleshooting Guide

- [Reset Network And Password](#)
- [Hard disk not being recognized Troubleshooting guide](#)
- [How to disable watch dog in BIOS](#)
- [Backup a Computer](#)
- [Backup to External Hard Drive or USB Drive](#)
- [Change RAID Type](#)
- [SMB usage and configuration guidance](#)
- [SMB Service Not Working](#)
- [Troubleshooting Steps for Failure to Power On EN](#)
- [Troubleshooting Guide for NAS Device Detection Fai](#)
- [Troubleshooting abnormal fan noise](#)
- [How to generate system logs](#)
- [How to Perform a Factory Reset](#)
- [How to Remotely Access UGREEN NAS via UGREENlink](#)
- [Installing M.2 SSDs \(Optional\)](#)
- [Migrate Internal Storage Drives to a New UGREEN NAS Device](#)
- [UGOS Pro Firmware Update Guide](#)
- [How to Connect and Configure a UPS on a UGREEN NAS to Protect Your Data Protection During Power Interruptions?](#)
- [How to Build the Home Assistant Smart Home System with Docker](#)
- [Screenshot of Home Assistant](#)

Network troubleshooting process:

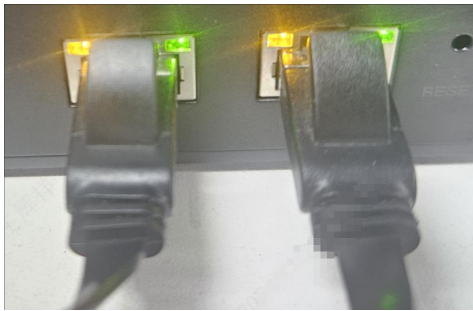
1. First, please ensure your network environment is functioning properly, such as the router and Ethernet cables. If everything is normal, proceed to the next step.
2. After connecting the Ethernet cable to the NAS, check whether the LAN indicator on the front panel is lit. If not, verify whether the yellow/green indicators on the **RJ45 Ethernet port** at the rear panel are lit. If they are both not lit, we can confirm an issue with the device's network card module, and we recommend that you start the after-sales process.
3. If, as described in Step 2, the front-panel LAN indicator lights up after connecting the Ethernet cable, check whether it is orange. If white light, the network status is normal. If it is orange, proceed to **Step 5**.
4. If the LAN light is off and the yellow/green light on the RJ45 Ethernet port is on, perform step 5.
5. Restart the NAS, press '**Ctrl+F12**' to enter the **BIOS** environment → select the **Advanced/Network Stack Configuration** menu → enable the **Lan BootROM IPv4 PXE Support** option → choose **Save & Exit / Save Changes and Restart** → reboot and press **Ctrl+F12** to enter the **UEFI PXE boot environment**.
6. Check whether the **PXE** boot correctly displays the network card's MAC address and whether the yellow indicator on the RJ45 port is blinking. If it is blinking:
 - (1) Select **Save & Exit Restore Defaults** to save and exit.
 - (2) Boot into the **UGOS PRO** environment, hold the reset button for **13 seconds** to reset the network settings, and observe whether the network indicator status returns to normal.
 - (3) If normal, use the **RESET** button to reconfigure the system's network settings.
 - (4) If still abnormal, this indicates a **UGOS PRO system network indicator malfunction**. We will start after-sales and arrange an inspection.If there is no blinking: The issue may be related to the **network card's PXE boot failure**, and repair will be required.

For clearer guidance, please refer to the attached diagram illustrating the BIOS settings and PXE boot process:



To further confirm the issue, we request you to provide the following images (as shown in the example):

- **Rear-panel RJ45 indicator status:** Left image (yellow/green light on), Right image (light off)

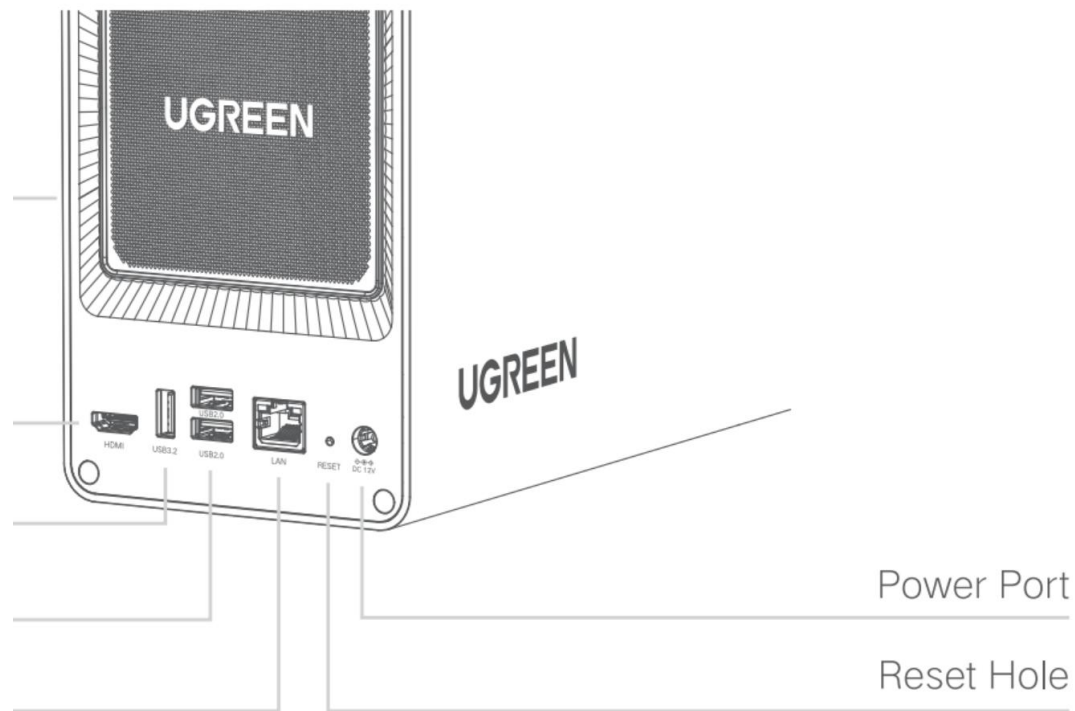


Front-panel LAN indicator status: From left to right—white light, orange light, unlit



Reset Network & Password

To reset the network settings and password, please follow these steps:



1. While the device is powered on, use a pin to press and hold the "RESET" button on the device for 5 seconds. Release the button after you hear a short beep.
2. The device will not restart during the reset process. Once the reset is complete, the network indicator light will remain solid white, indicating that the device is ready for use.

Note: This reset operation will not affect any data stored on your hard disk. After a successful reset, you can log in using the "admin" account with a blank password (this account is only for password reset purposes). After logging in, follow the setup wizard to create a new administrator password.

Troubleshooting for SATA hard disk not being recognized:

1. Please confirm your hard drive model:

Confirm whether the hard drive is on the official compatibility list:

- If not, please replace it with a compatible hard drive model.
- If it is, proceed to the next step.

2. Check if the Disk indicator light is lit white:

- If not, please ensure the hard drive is properly installed.
- If it is, proceed to [step 5](#).

3. If the Disk light is lit white, please check if the orange light is also displayed.

- If not, the Disk light is normal, and the hard drive is recognized normally.
- If the orange light is on, please confirm if the hard drive functions normally after formatting and repartitioning: If abnormal, please use **ext4/Btrfs** format partition.

4. Hard disk formatting partition:

If there are no abnormalities after formatting and partitioning the hard drive, please replace it with a hard drive that can be recognized and check if it works normally:

- If normal: The hard drive may be malfunctioning, please replace the hard drive.
- If not normal: There may be a fault with the product, and we will initiate the after-sales process for you. You will need to send your NAS to our service center for inspection.

5. Check if the hard drive interface appears normal

5.1 If not, perform the following steps:

- A. If the motherboard-side interface is damaged, after-sales inspection is required.
- B. If the hard drive-side interface is damaged, please replace it with an undamaged hard drive.
- C. If there is dirt or foreign objects on the surface, please clean it.

5.2 If normal, proceed to the next step.

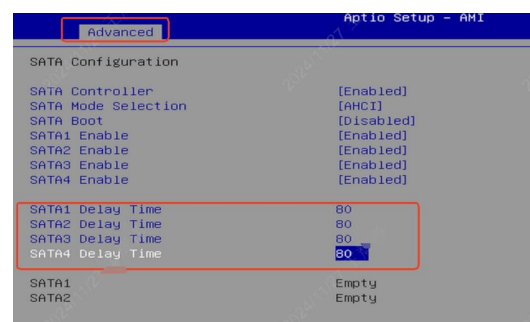
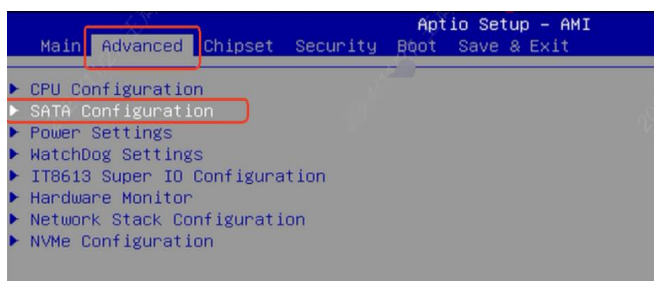
Check if the **BIOS SATA** delay time is set to **80s**:

- If not, please set the BIOS SATA delay time parameter to 80s.
- If it is, proceed to the next step.

6. After replacing the hard drive that can be recognized, check if it works normally:

- If not normal, the product may have a fault, and the after-sales process will be initiated.
- If normal: The hard drive may be malfunctioning, please replace the hard drive.

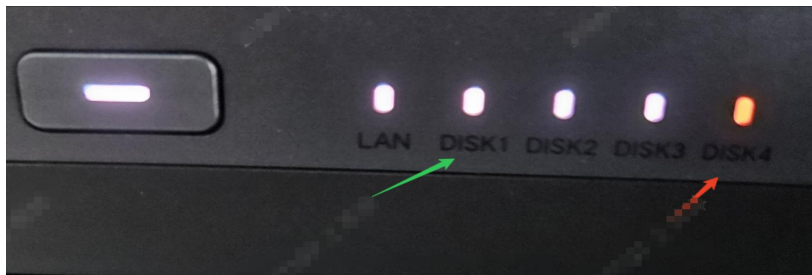
BIOS SATA delay time parameter settings



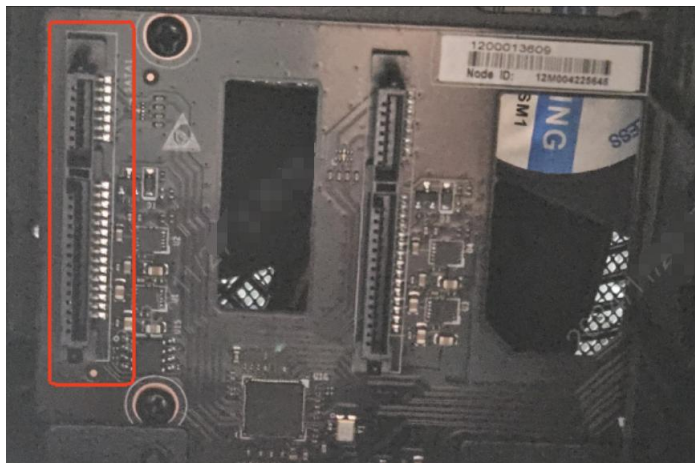
*The hard disk is not found and the indicator light is off:



*The orange indicator light indicates that the hard disk has not been initialized, contains partitions, or other abnormalities:

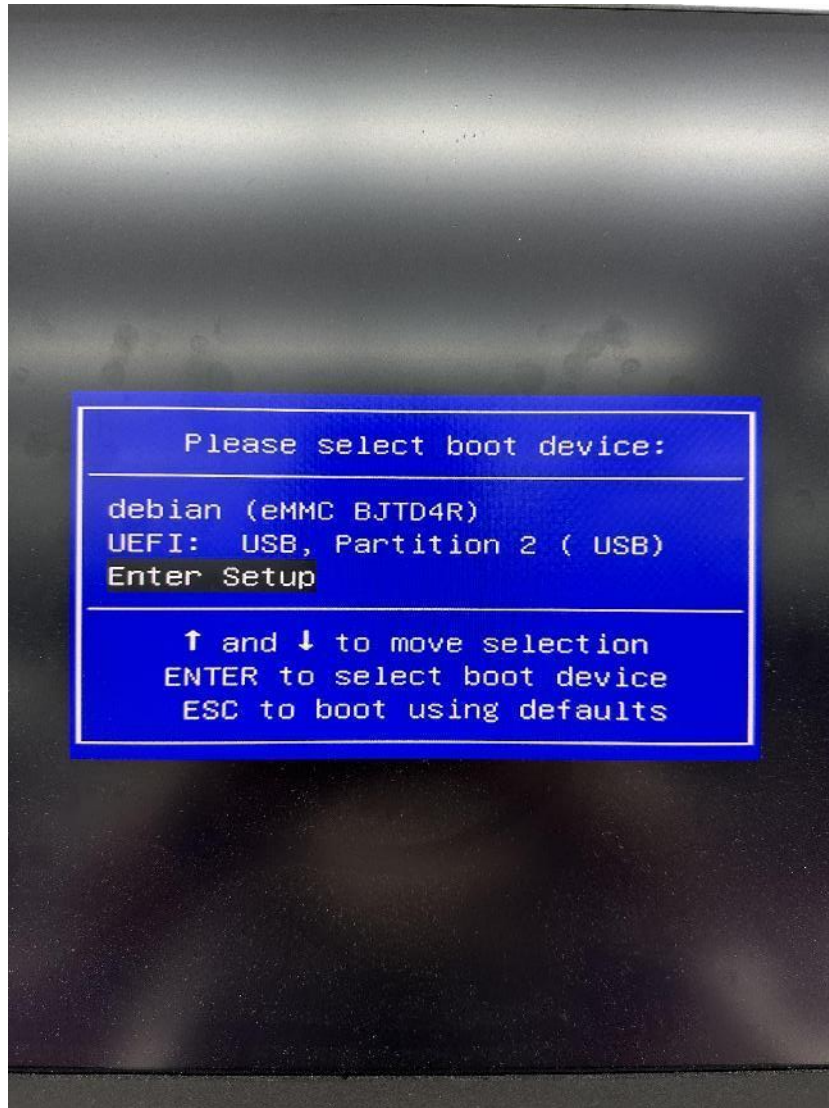


*Check the hard disk interface appearance, no damage, no dirt:

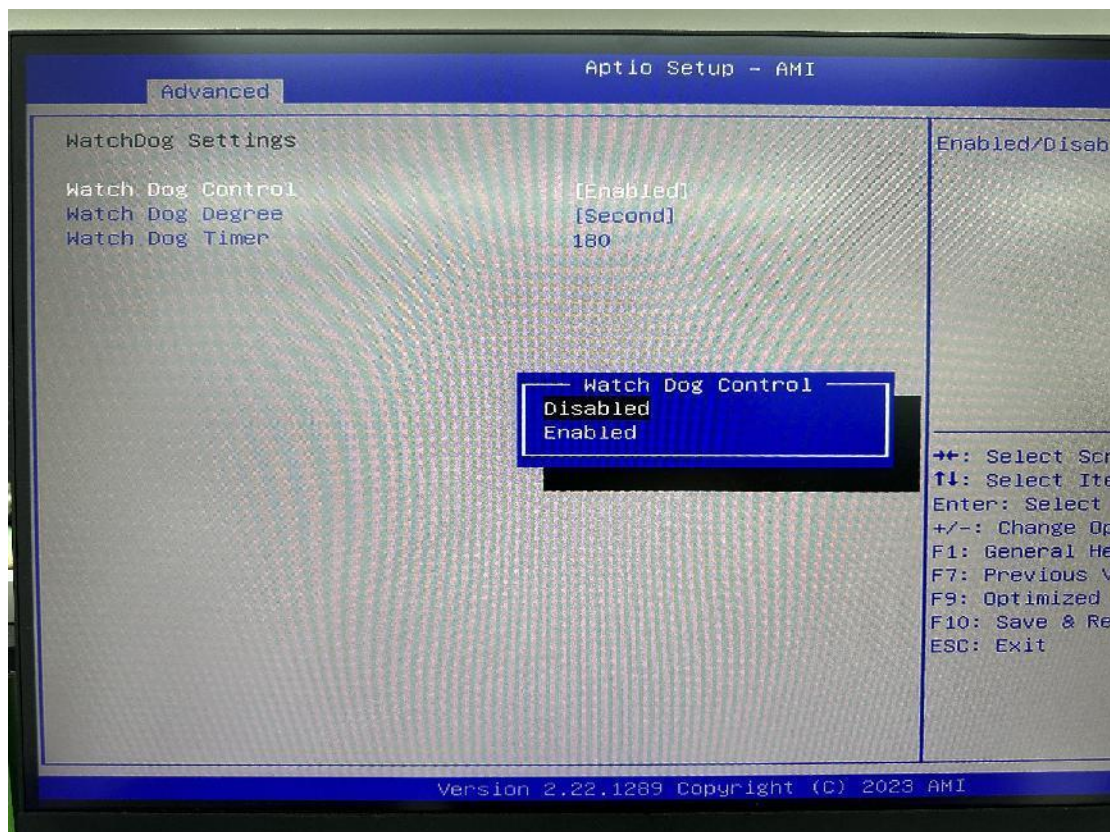
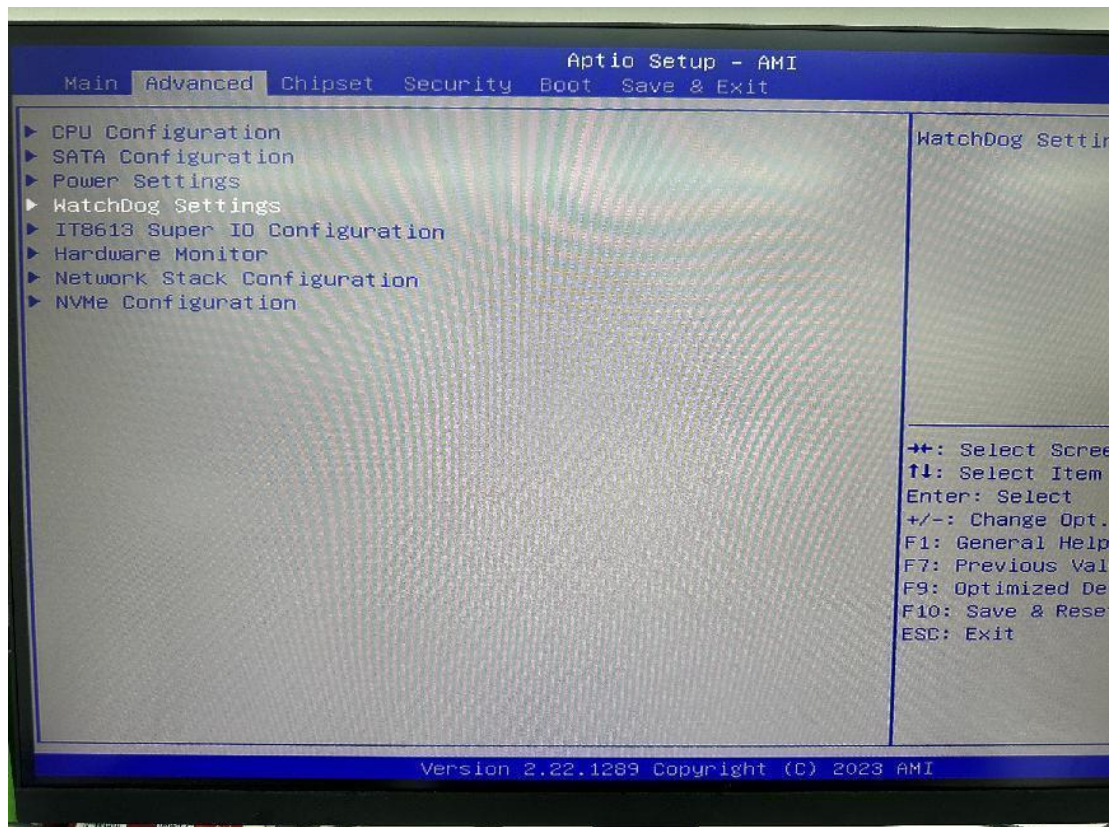


How to disable watch dog in BIOS

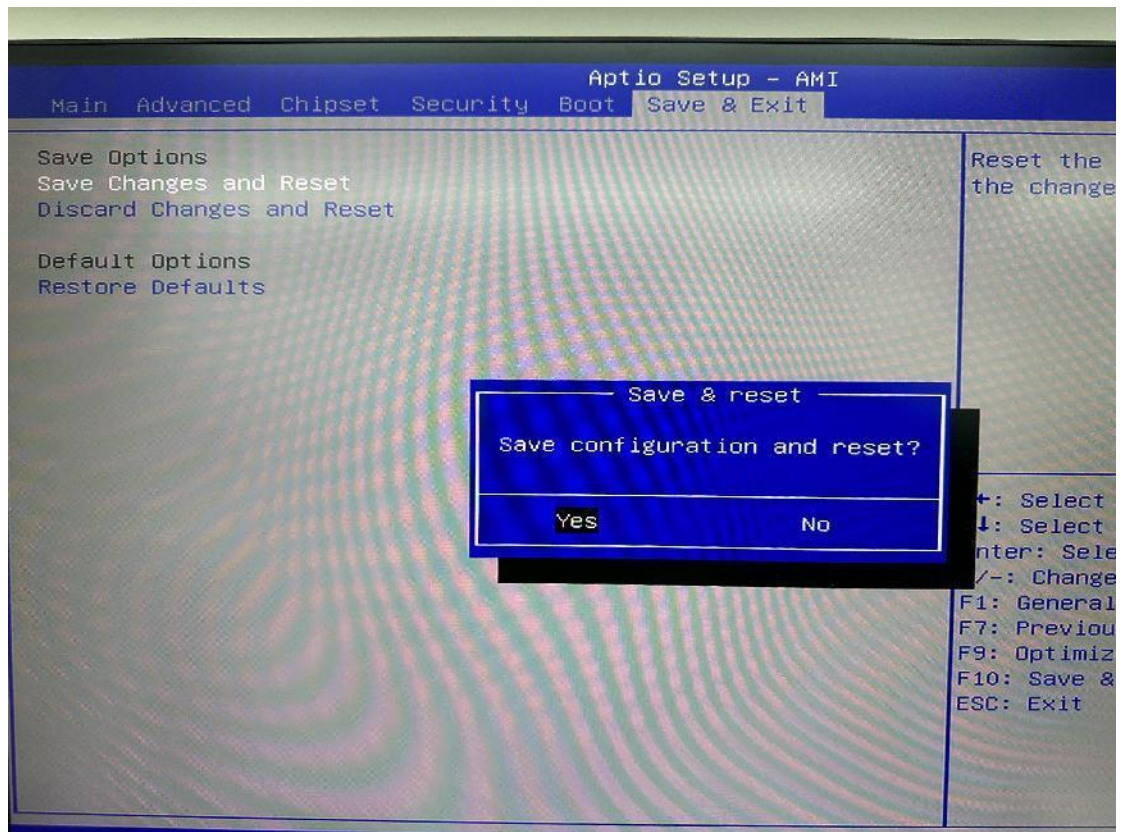
1. Power on your NAS and connect it to a monitor via HDMI cable. Press Ctrl+F12 continuously on your keyboard during the initial start up process and you will come to the following BIOS page. Choose the third option - **Enter Setup**



2. Then you will come to the following page, choose **Advanced > WatchDog Settings**, set **Watch Dog Control** as **Disabled**:



3. Press **Esc** on your keyboard and choose **Save & Exit > Save Changes and Reset** on the main board:



Choose **Yes** and you NAS will reboot and the Watch Dog will be disabled.

Backing up a computer to UGREEN Cloud involves transferring files from the computer to the UGREEN NAS. This functionality requires the use of the UGREEN NAS Client.

Create Backup Task

1. In the [Sync & Backup] interface, click on "Create backup task," then select "Backup this computer."

2. In the [File Filter] interface, choose the Computer Path that you need to back up to the UGREEN Cloud NAS.

3. If you want to exclude unnecessary files from being backed up, you can set up filter rules:

File Name or Extension Filtering: By selecting "Filter the following file names or file extensions" and adjusting the rules, you can exclude files that do not need to be backed up.

To add a new rule, click the "Add" button and enter the file name or extension (use ";" to separate multiple criteria).

To delete a rule, hover over the target rule and click the floating "X" button.

Below are the default filtering formats, which you can modify as needed.

*.tmp	*.temp
*.swp	*.link
.pst	~.*
@eadir	.SynologyWorkingDirectory
#recycle	desktop.ini
.DS_STORE	Icon\r
thumbs.db	\$Recycle.Bin
@sharebin	System Volume Information
Program Files	Program Files (x86)
ProgramData	#snapshot

4. After confirming that the settings are correct, click "Next" to continue.

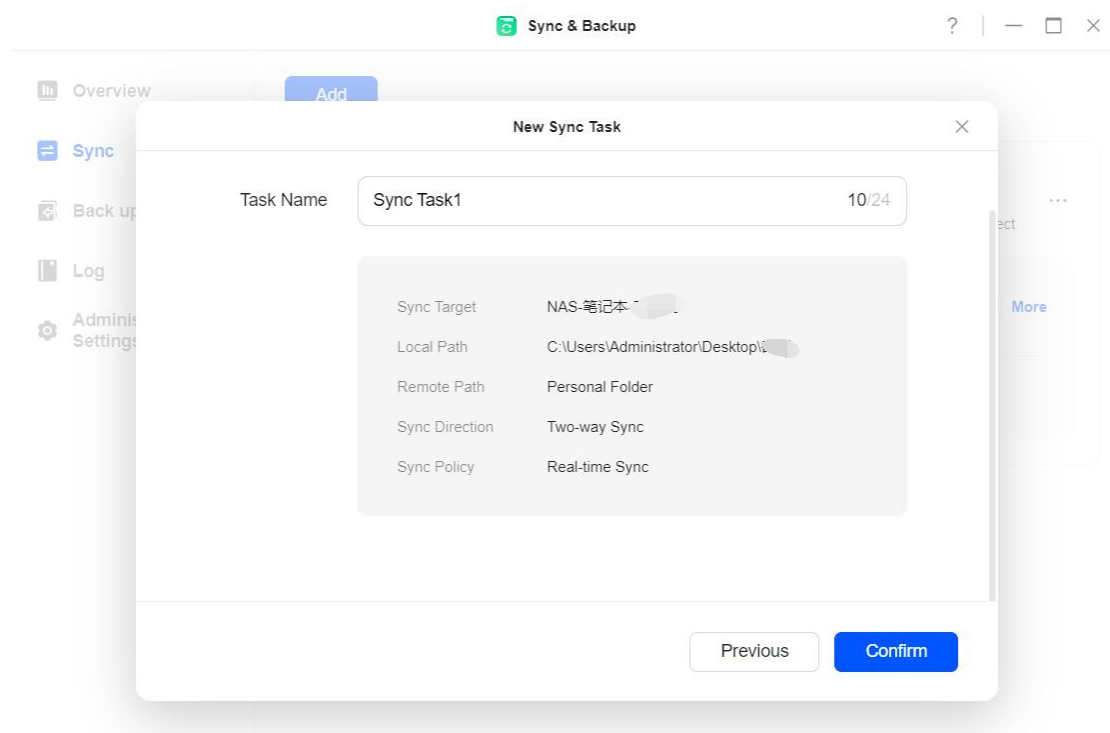
Configure Backup Task

In the [New Backup Task] interface, select the Backup Destination, which is the storage location on the local UGREEN NAS. You can choose the backup strategy, which supports "Backup after file change" or "Manual Backup." Manual backup will only execute when you manually click "Backup Now."

After completing the settings, click "Next Step" to continue.

Preview and Create Task

In the Preview interface, you can customize the task name and review all settings. If everything is correct, click "Confirm" to create the backup task.



Task Management

After the task is created, you can manage the connected devices in the Sync & Backup interface:

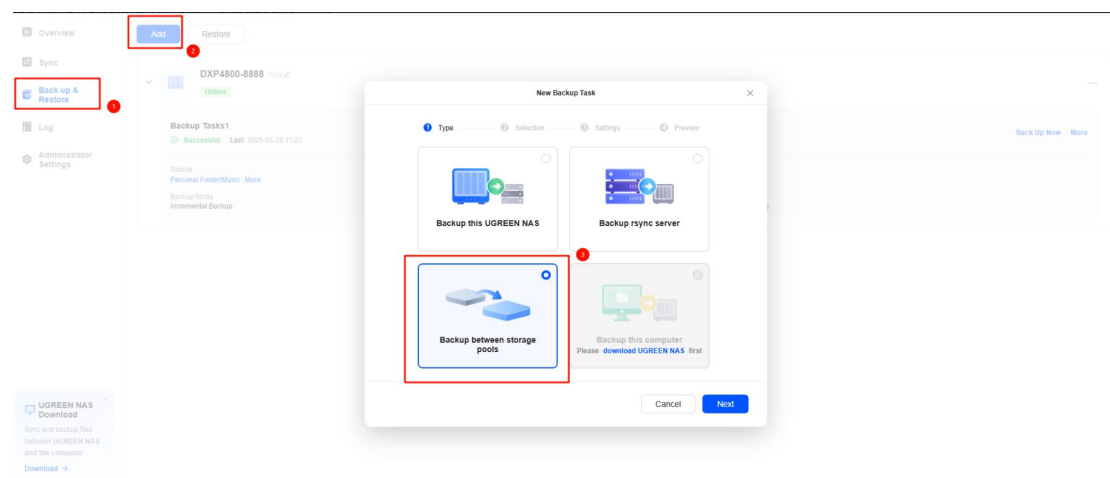
- Click the "..." button on the right side of the device to select Pause, Edit, or Delete the task.

Backup to External Hard Drive/USB Drive

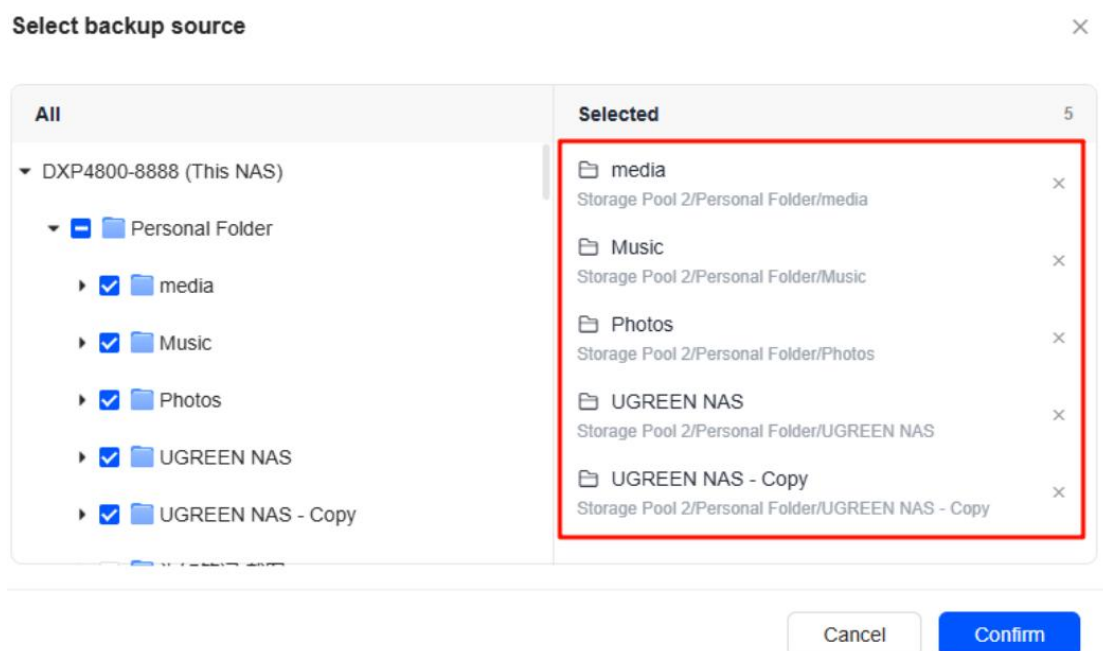
In the UGOS Pro system, the [Sync & Backup] app not only supports internal file synchronization and remote backup for NAS, but also provides the option to back up data to locally connected storage devices (such as external hard drives or USB drives). This feature is suitable for scenarios where users want to create local offline backups of important data, offering an extra layer of protection for data security.

User Guide

1. Open the [Sync & Backup] app and select [Backup & Restore] from the left sidebar.
2. Click the "Add" button in the upper-right corner of the page. In the pop-up window for selecting a backup type, choose "Backup Between Storage Pools" and click "Next" to continue.



3. Next, select the folders you want to back up. Click the [Backup Source] field to choose one or more internal folders on the NAS as the backup source (multiple backup sources are supported).



4. In the [Backup Destination] section, select the target folder on the mounted external hard drive or USB drive. If the external device is not displayed, please ensure it has been properly inserted and mounted (you can check this in [Files]).

1. After completing the settings, click "Next" to proceed to the next step.

7.UGOS Pro offers two backup modes: choose Incremental Backup if you want to retain previous backup files, or choose Mirror Backup if you need the destination to be exactly the same as the source. Select the mode according to your needs, then click "Next" to continue.

8.Set the backup plan. To avoid affecting daily usage, it is recommended to schedule the task during off-peak hours, such as at night.

9.Once configuration is complete, click "Next" to proceed.

The screenshot shows a window titled "New Backup Task" with a close button (X) in the top right corner. Below the title bar is a progress bar with four steps: 1. Type (checked), 2. Selection (checked), 3. Settings (active, highlighted with a blue circle), and 4. Preview (disabled). The main content area is divided into two sections. The first section is labeled "Backup Mode" and contains two radio button options. The first option, "Incremental Backup", is selected and has a description: "In single version, files created and modified on the source device will be copied to the backup destination, and files deleted from the source remain at the destination after backup". The second option, "Image Backup", is unselected and has a description: "For a single version, the backup destination will be the image copy of the source. If the destination has a file that does not exist at the source, the file will be deleted". The second section is labeled "Plan" and contains a checked checkbox for "On". Below this are two input fields: a dropdown menu currently showing "Every Day" and a time field showing "10:00" with a clock icon. At the bottom right of the window are two buttons: "Previous" and "Next".

10. On the [Preview] page, you can edit the task name, review the source and destination paths, as well as the backup mode and schedule configuration. After confirming all settings, click "Confirm" to immediately create and execute the backup task.

New Backup Task

×

✓ Type

✓ Selection

✓ Settings

4 Preview

Task Name

Backup Tasks2

13/50

Source

Personal Folder/media, Personal Folder/Music, Personal Folder/Photo...

Backup Destination

External Device/sdd1

Backup Mode

Incremental Backup

Backup Plan

Every Day 10:00

☒ Back up immediately after creation

Previous

Confirm

Notes

All tasks are centrally managed on the [Backup & Restore] page, where you can view progress, execution history, or manually run tasks at any time.

The [Backup Between Storage Pools] feature not only supports backups between multiple storage pools, but is also applicable for backing up data to external storage devices mounted to the system.

Change RAID Type

UGOS Pro allows you to change the RAID mode of your storage pool without losing existing data. For example, if you add enough available drives, you can upgrade the storage mode of your UGREEN NAS from RAID 1 to RAID 5. Currently, UGOS Pro supports upgrading from Basic mode to RAID 5 (the upgrade path is Basic > RAID 1 > RAID 5).

Please note: It is advisable to use hard drives that are compatible with your UGREEN NAS and listed in the "HDD/SSD Compatibility List". Using unsupported drives may impact system stability and could result in data loss.

Hard Drive Requirements

To change the RAID type of the storage pool, a sufficient number of available hard drives must be installed in the UGREEN NAS. The table below shows the minimum number of drives required for each RAID type:

RAID Type	Minimum Number of Drives Required
RAID 1	2
RAID 5	3

RAID Type Requirements and Restrictions

Not all RAID types can be converted to each other. For example, RAID 1 can be upgraded to RAID 5, while RAID 5 cannot be downgraded to RAID 1. The table below shows the target types to which each RAID type can be converted, along with the required number of drives.

Current RAID Type	Convertible Target Types	Required Additional Drives
Basic	RAID 1	1
Basic	RAID 5	2
RAID 1	RAID 5	1

Steps to Change RAID Type

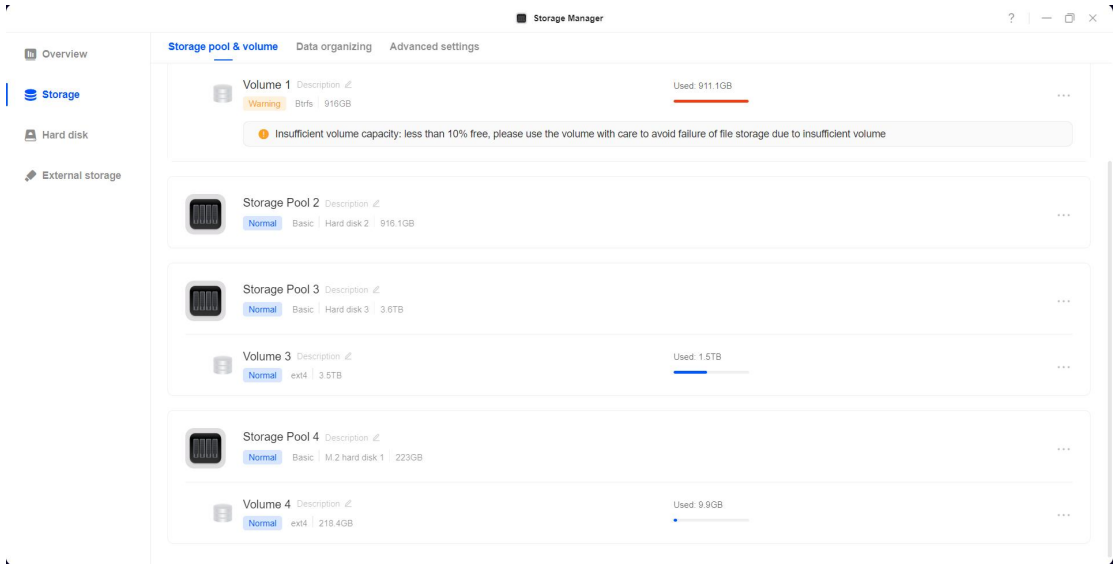
Preparation before starting:

1.

Ensure the storage pool status is healthy.

2.

When adding new hard drives to the storage pool, make sure there is at least one unused, healthy hard drive. The new hard drive should have a capacity equal to or greater than the smallest hard drive currently in the pool. It is also recommended that all hard drives be of the same model and type.



To change the RAID type of a storage pool:

1.

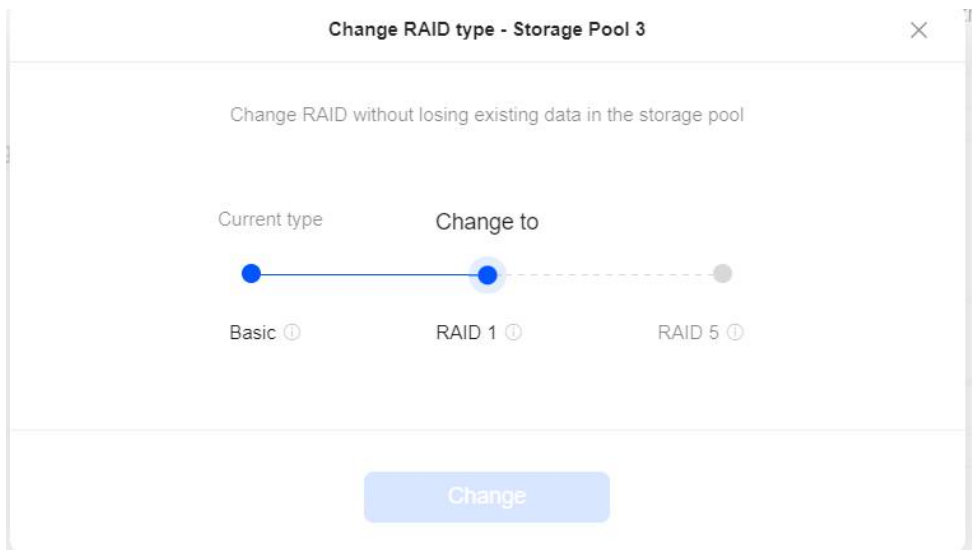
Navigate to **Storage Manager > Storage > Storage pool and volume**.

2.

Locate the storage pool whose RAID type you wish to change, click the "..." icon on the right, and select **"Change RAID Type"**.

3.

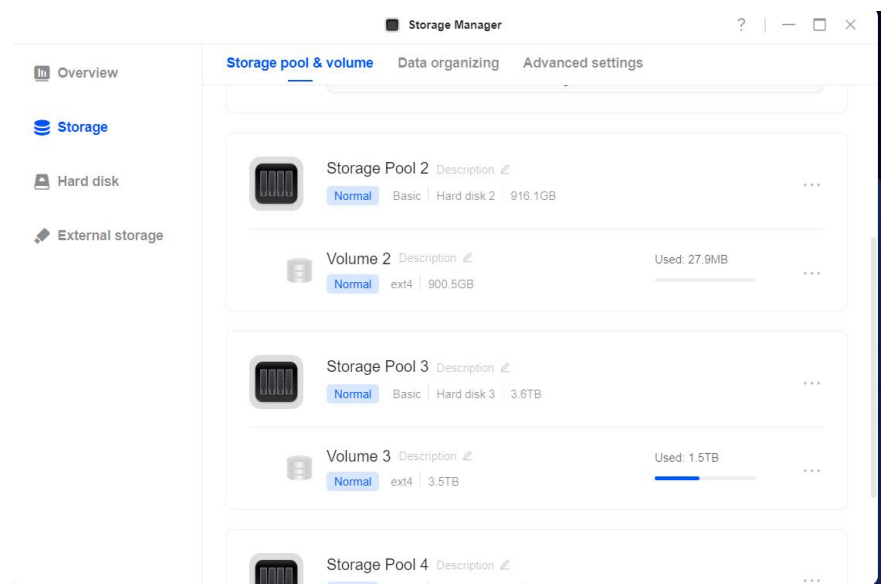
In the pop-up options, select the desired RAID type and click **"Change"**. *Note: The "Change" button will only be clickable if the current RAID type supports the change.*



1. Select the available hard drives to add to the storage pool. Note: All data on the newly added hard drives will be erased. Please ensure that you back up your data in advance.

2.

Confirm your settings and click **"Apply"** to complete the process. During the change, the storage pool status will change to **"Changing RAID Type."** Once the change is complete, the status will return to normal. You can click the **"..."** icon on the right of the storage pool to view its current RAID type.



Note:

1.

The RAID type change process for the storage pool may take a considerable amount of time and consume system resources, potentially leading to performance degradation. Therefore, it is recommended to perform this operation during periods of low device usage. During the process, ensure that your UGREEN NAS device remains powered on and avoid restarting it to prevent operational issues and data loss.

2.

In the Select New Hard Drive dialog, the list will only display RAID types that the current storage pool can be changed to. For example, if the current storage pool is in RAID 1, only RAID 5 will appear as an option.

3.

If an issue occurs with the hard drive during the change process, the RAID type will still be updated, which may result in the storage pool status changing to "Degraded."

SMB

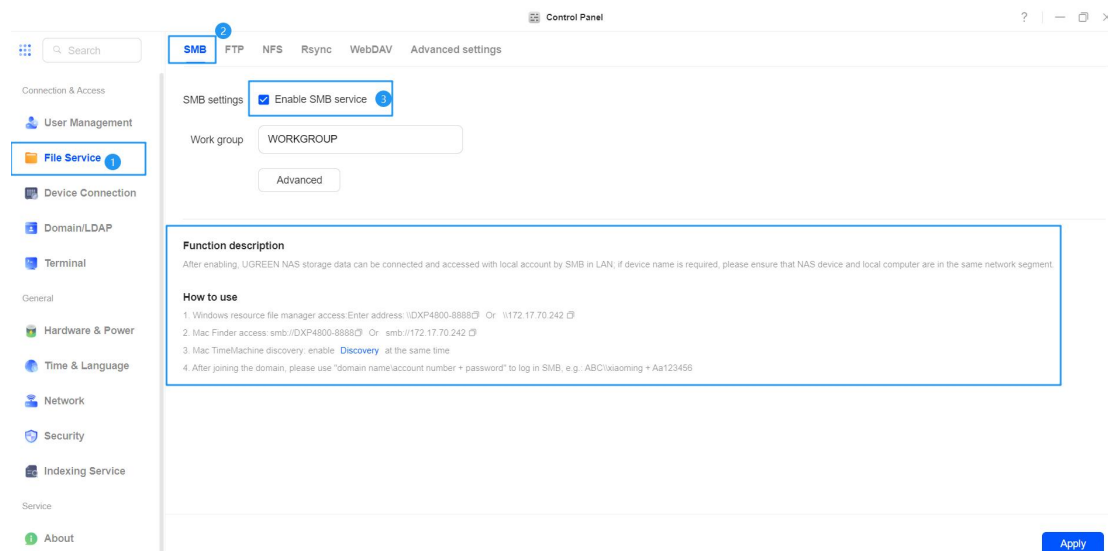
The SMB protocol is a core feature of UGREEN NAS for file sharing, allowing users to mount shared folders on local computers (Windows/macOS), mobile devices, and TVs within a local network. This enables centralized storage and cross-device access.

Features of SMB Service

- Cross-Platform Compatibility: Supports Windows, macOS, iOS, Android, and TV boxes for seamless access across multiple devices.
- High-Speed Large File Transfers: Optimized for batch read/write operations, ensuring faster data transmission.
- Multi-Version Protocol Support: Compatible with SMB1, SMB2, SMB2.1, and SMB3 to meet different system requirements.

Enable SMB Service

1. Open the "Control Panel" app and go to [File Service] > [SMB].
2. Check "Enable SMB Service", then click "Apply" to save the settings.



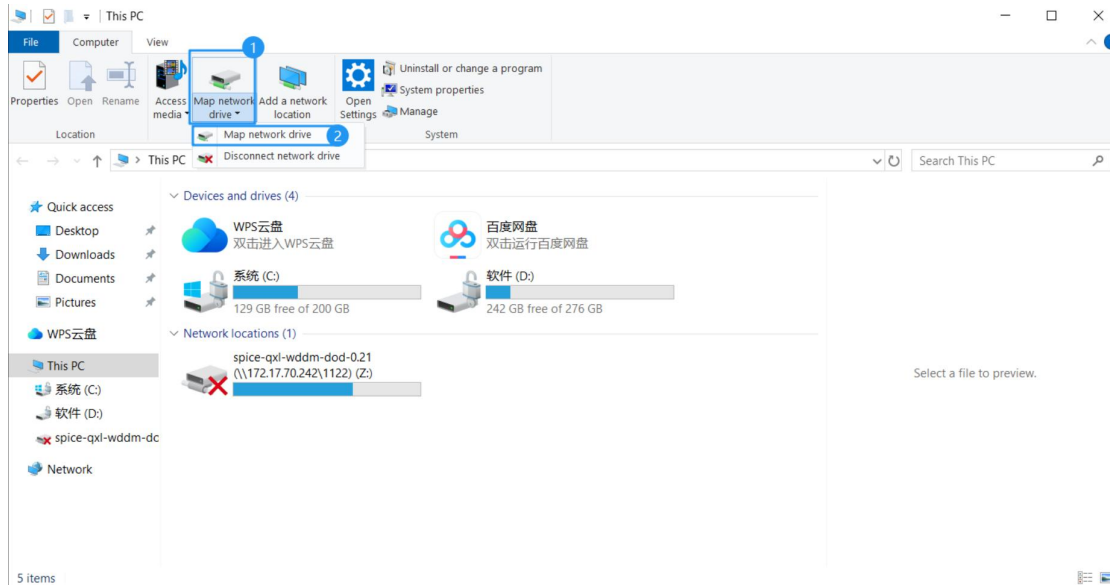
Note: You can quickly copy the address for later use by clicking the copy button in the "How to Use" section.

Mount UGREEN NAS as a Local Drive via SMB on Windows

Prerequisite: Ensure that both the NAS and the Windows device are connected to the same local network.

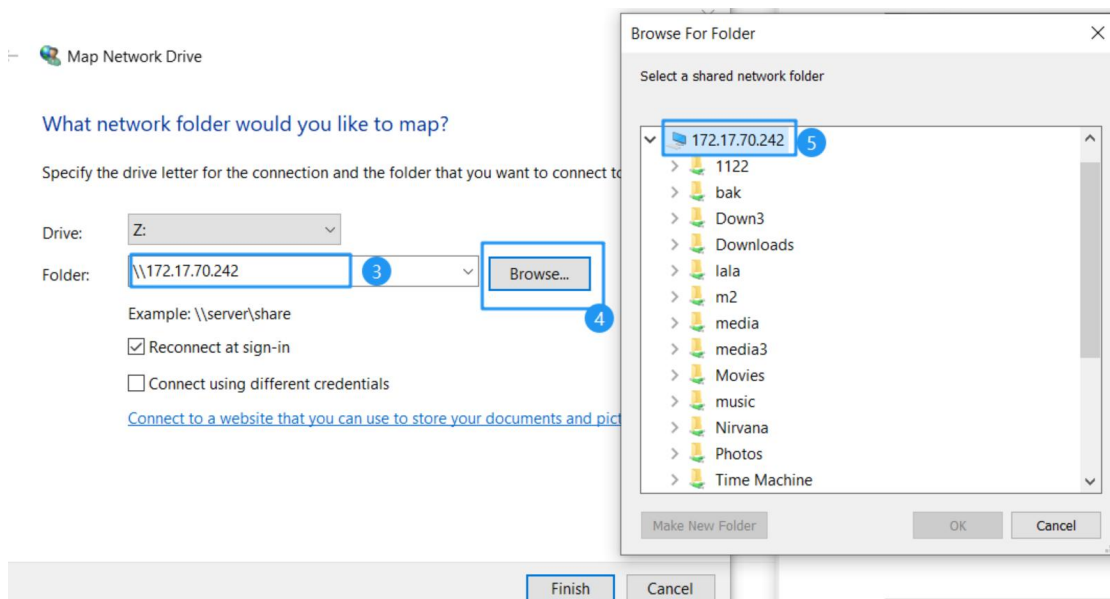
Method 1: Map Network Drive

1. Open This PC, click the "..." button in the top-right corner, and select "Map network drive".



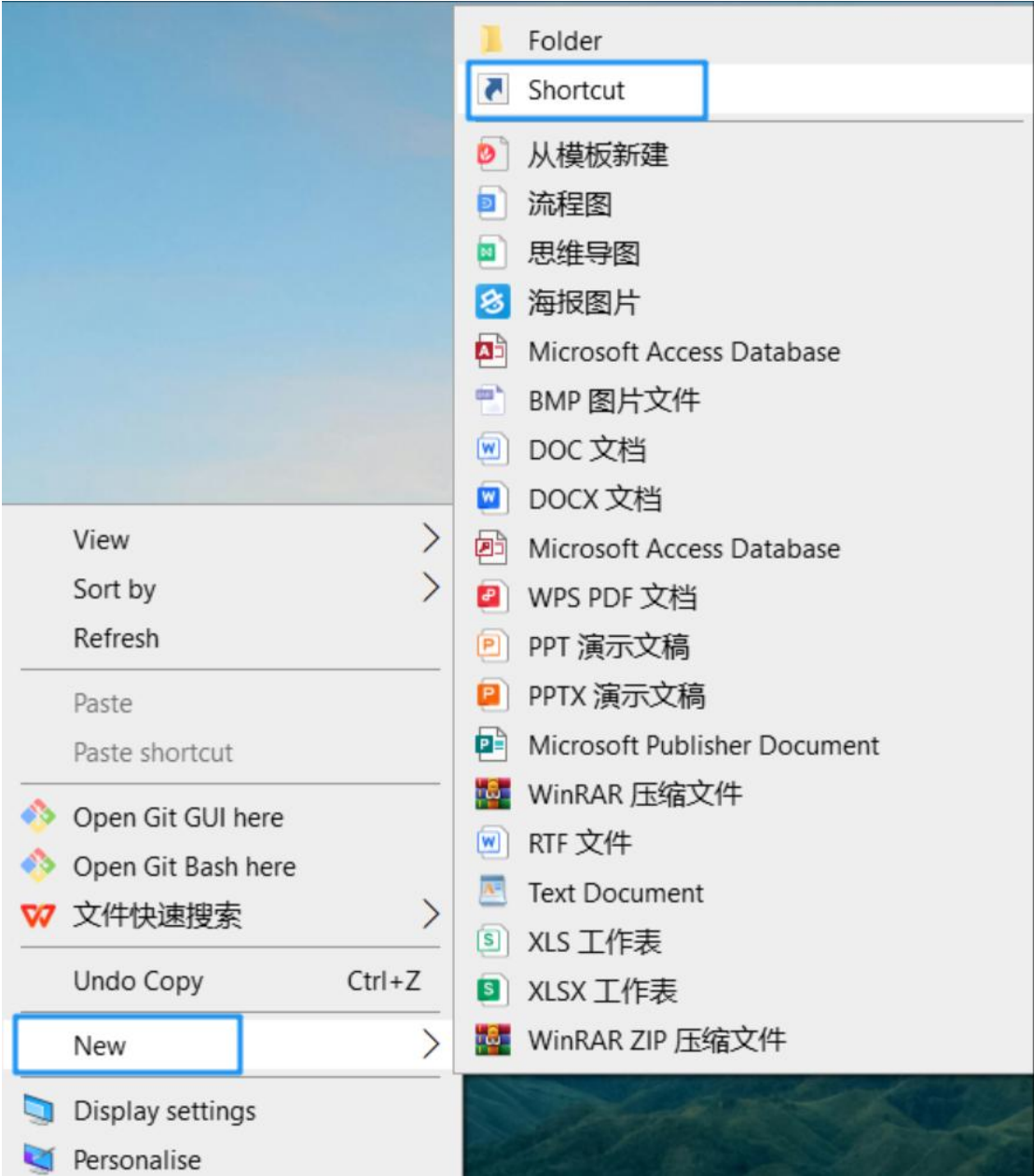
2. In the folder address field, enter the NAS IP address (e.g., \\172.17.70.242), then click "Browse" to select the device. In the network credentials prompt, enter your NAS account credentials for authentication.

3. Once verified, select the specific folder to map, then click "OK" > "Finish". The mapped drive will now appear in This PC.



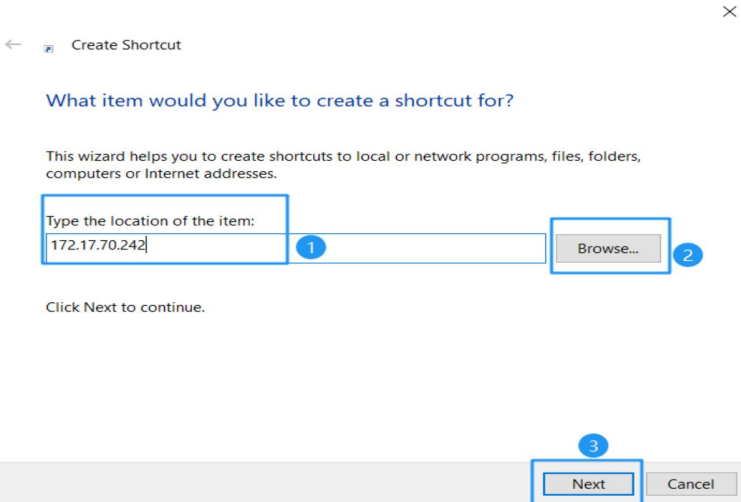
Method 2: Create a Shortcut

1. Right-click on an empty area of the desktop, select "New" > "Shortcut".

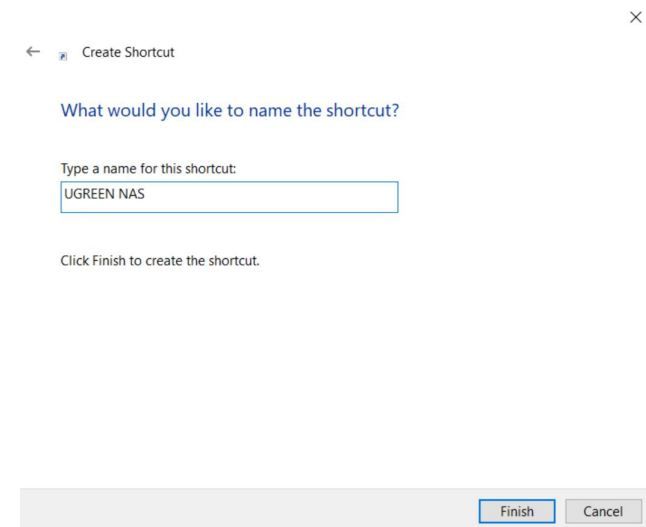


2. In the pop-up window, enter the NAS IP address (e.g., \\172.17.70.242) in the address field, then click "Browse" to select the device.

3. When prompted, enter your NAS account credentials for authentication. Once verified, select the specific folder and click "Next".



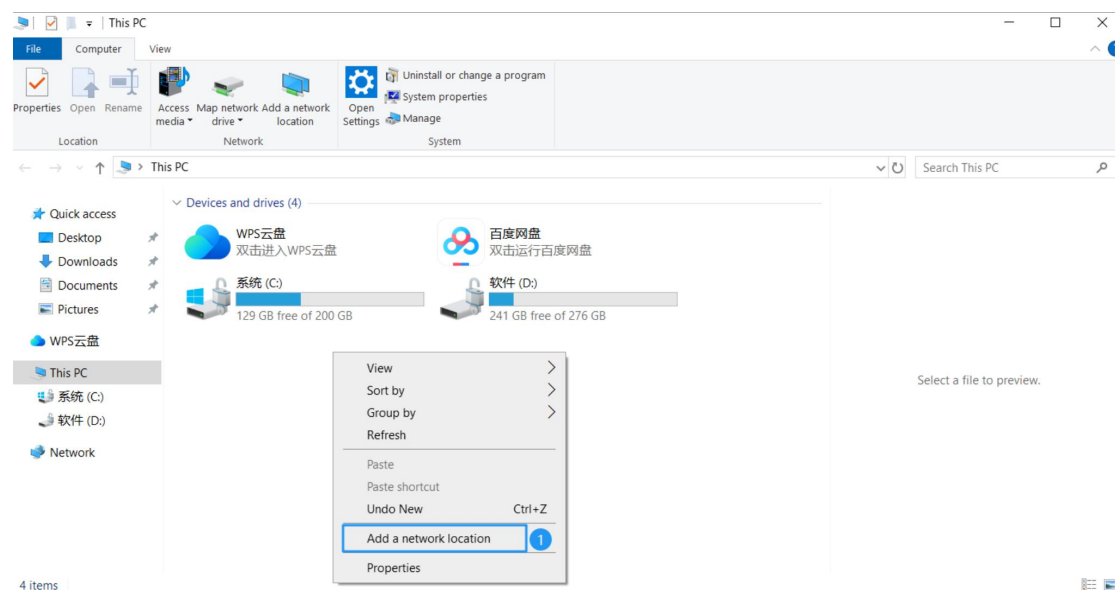
4. Name the shortcut and click "Finish" to create it.



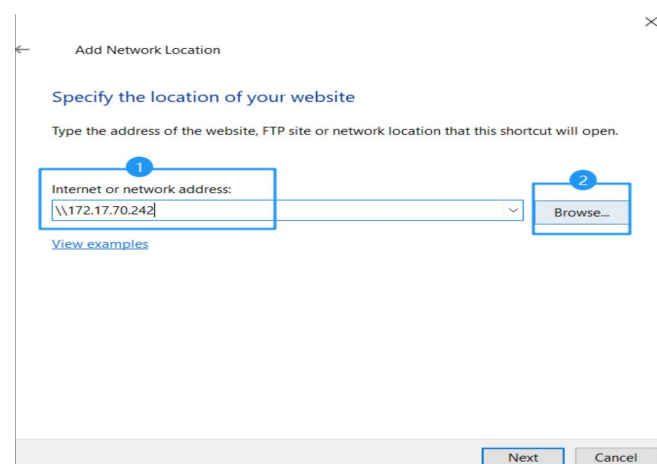
5. Double-click the desktop shortcut to quickly access the NAS folder.

Method 3: Mount a Network Location

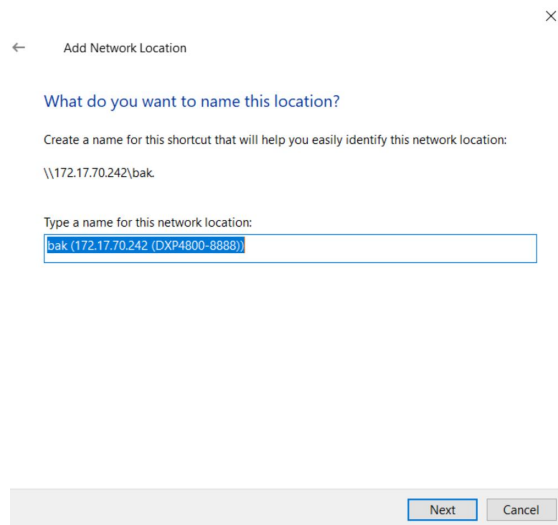
1. Open This PC, right-click on an empty area, and select "Add a network location".



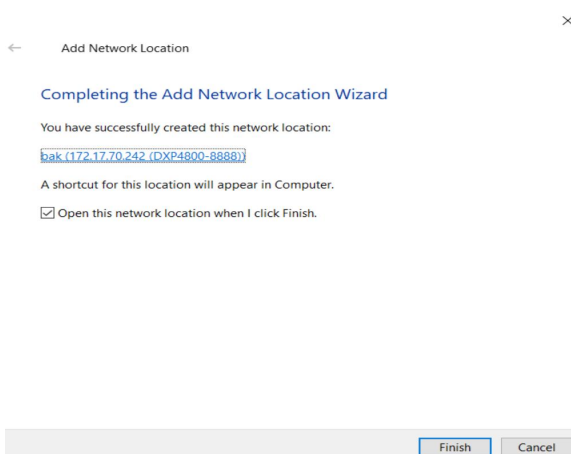
2. Follow the setup wizard and choose "Custom network location". In the address field, enter the NAS IP address (e.g., \\172.17.70.242), then click "Browse" to "select the device". Enter your NAS account credentials in the authentication prompt.
3. Once verified, select the specific folder and click "Next".



4. Name the network location and click "Next".

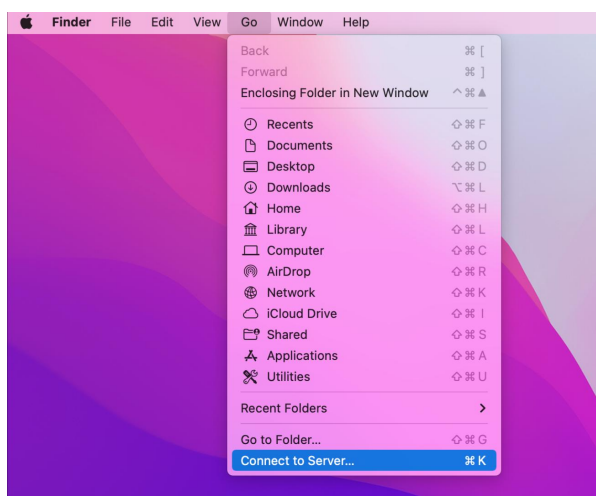


5. The setup is complete, and you can now access the shared folder.



Mount an SMB Shared Folder on macOS

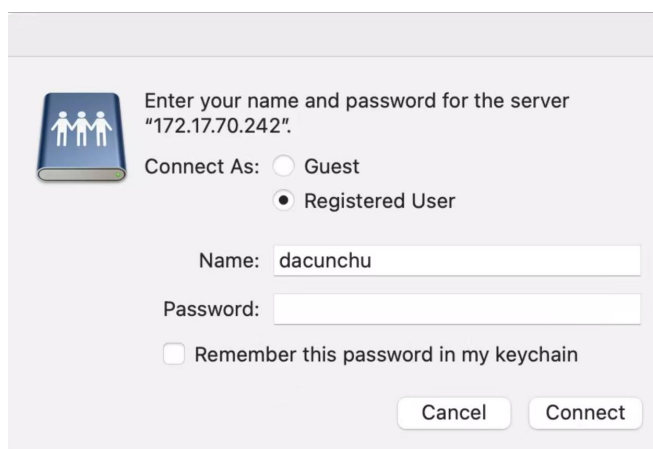
1. Open [Finder], click on "Go" in the top menu bar, and select "Connect to Server".



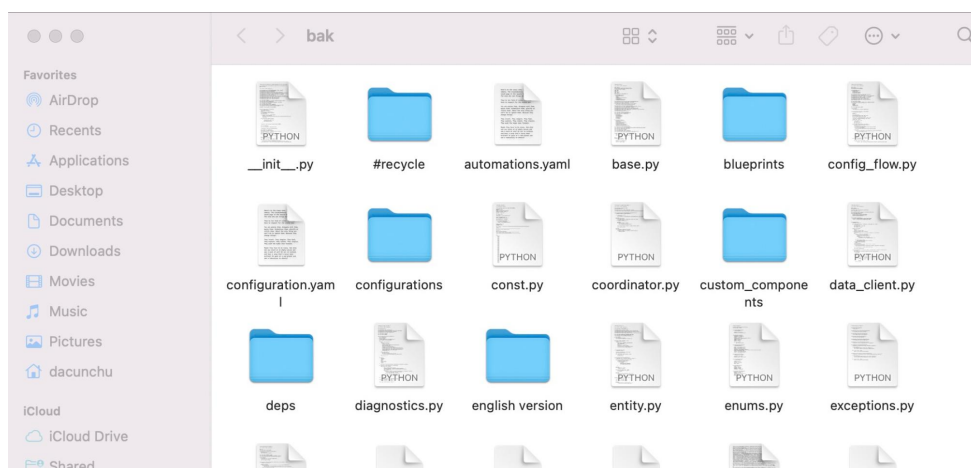
2. In the "Connect to Server", enter smb://NAS_IP (e.g., smb://172.17.70.242), then click "Connect".



3. Enter your NAS username and password for authentication. Once verified, the list of available shared folders will be displayed.

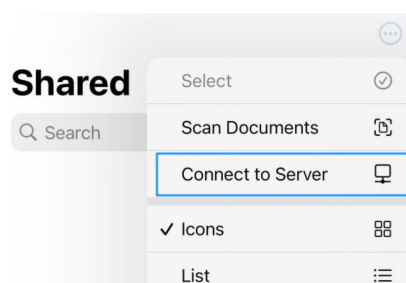


4. Select the shared folder you want to access and click to enter. You can now store and edit files within the folder.

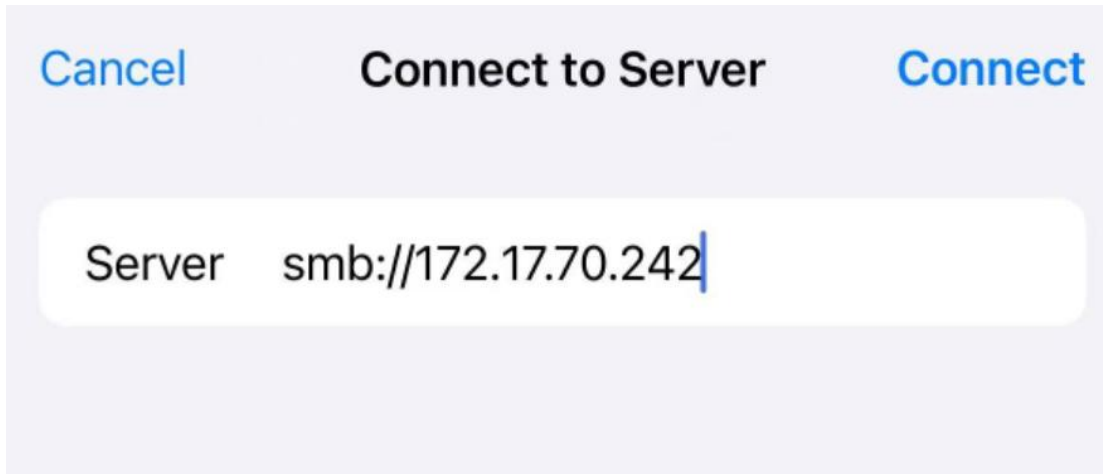


Access an SMB Shared Folder on iOS

1. Open the "Files" app, tap the "... " button in the top left corner, and select "Connect to Server".



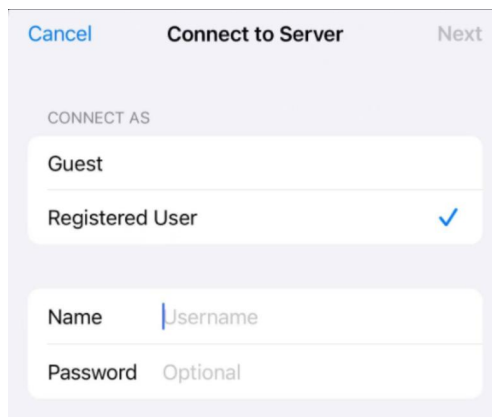
2. In the pop-up window, enter the NAS access address in the format smb://IP_address. For example, if the NAS IP address is 192.168.31.70, enter smb://192.168.31.70 and click "Connect".



Cancel **Connect to Server** Connect

Server smb://172.17.70.242

3. Enter your NAS username and password for authentication.



Cancel **Connect to Server** Next

CONNECT AS

Guest

Registered User ✓

Name Username

Password Optional

4. Once connected, you can find the NAS shared folder in the "Files" app. Click on the folder to access and transfer files.

SMB FTP NFS Rsync WebDAV Advanced SettingsSMB settings ☒ Enable SMB service

Work group

WORKGROUP

Advanced

Function description

After enabling, UGREEN NAS storage data can be connected and accessed with local account by SMB in LAN; if device name is required, please ensure that NAS device and local computer are in the same network segment.

How to use

1. Windows resource file manager access: Enter address: \\DXP2800-2E62 or \\10.0.0.36
2. Mac Finder access: smb://DXP2800-2E62 or smb://10.0.0.36
3. Mac TimeMachine discovery: enable [Discovery](#) at the same time
4. After joining the domain, please use "domain name\account number + password" to log in SMB, e.g., ABC\xiaoming + Aa123456

← → ↕ ↑ \\10.0.0.36

★ Quick access

- Documents
- Desktop
- Downloads
- Pictures
- 01 Weekly Leadership Team Meetings
- My Notebooks
- Journal Articles
- 2025 Business Expenses
- 09 Sketchup Drawings
- Data for Presentation
- 2025 Volusia County FL Taxes
- TEMP
- UGREEN
- Western Digital

OneDrive - GTA

This PC

My Passport (E:)

Network

DESKTOP-NUFPS4B

E6430S

Name

- Arris TG4482A
- DESKTOP-NUFPS4B
- E6430S
- E6430S: CompAdmin-1:
- E6430S: CompAdmin-2:
- EPSON00CA60 (ET-2850 Series)
- Roku Bedroom

File Explorer



Windows can't find '\\10.0.0.36'. Check the spelling and try again.

OK

Troubleshooting Steps for Failure to Power On:

1. Please check if any non-compatible devices(**HDD/SSD**) have been installed. If so, remove them and verify whether the system powers on normally.

If not, check whether the power indicator on the **ACDC adapter** lights up after plugging it into the socket. If it does not, replace the **AC power cable** with a compatible model and check again.

2. If the adapter's power indicator lights up, check whether the NAS host's power indicator lights up after connecting the power adapter.

If not, check whether the power button is working properly when pressed.

3. If the host's power indicator lights up, confirm whether there are **three long and two short beeps** during startup.

- If yes, clean the **RAM** modules with an eraser and check if the system powers on normally.

- If the issue persists, try replacing the **RAM** modules.

4. If there are no beeps during startup, check whether the system can boot into the **BIOS** environment (UGREEN screen). -Press **Ctrl+F12** at the same time to enter the BIOS.

- If you are unable to enter the BIOS, the problem may be related to the BIOS and the device may need to be repaired.

4.1 If it enters the BIOS, verify whether **GRUB & Booting UGOS PRO** starts normally and enters the **HDMI** direct playback interface.

- If not, UGOS Pro may have failed to boot, our engineers will provide remote support for you.

4.2 If it boots successfully into the HDMI playback interface, ensure the system remains stable without restarts.

4.3 If it restarts, check whether the **RESET** button works properly.

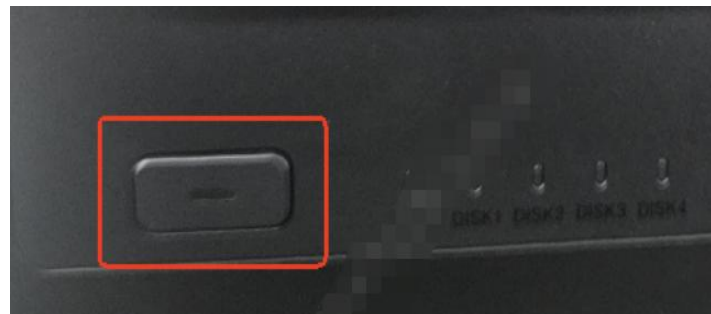
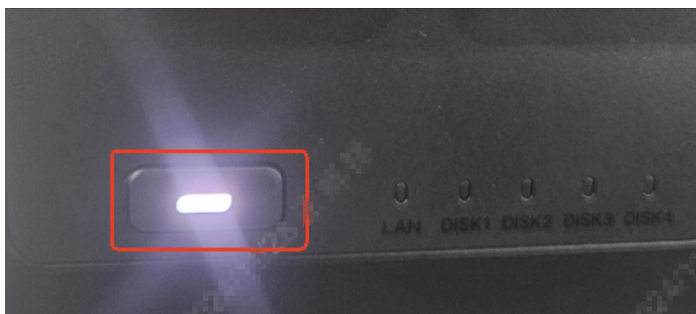
- If it does, the issue may be system-related, requiring testing and repair.

- If the RESET button is unresponsive, it may be faulty, and the device needs to be returned to our warehouse for repair.

ACDC power adapter indicator light status: on the left picture, off on the right:



Host power indicator light status: On in the left picture, off in the right:



System startup status BIOS environment logo on the left, UGOS Pro environment on the right:



Issue Overview and Context

When using your NAS device, you may encounter a "Device Not Detected" prompt, preventing a proper connection to the device. This issue can arise due to various factors, including network, hardware, or software anomalies. Below, we analyze common causes and provide detailed troubleshooting steps to help you quickly restore the device to normal operation.

Network Troubleshooting and Resolution

1. Check Physical Connections

Verify whether the NAS is properly connected to the network. For wired connections, check if the LAN indicator is flashing white. If the LAN indicator is flashing orange, it indicates a network issue.

Troubleshooting and Solutions

- **Inspect the Ethernet Cable:** Carefully examine the cable for physical damage such as cracks, bends, or breaks. Even minor damage can cause unstable or interrupted signal transmission.
- **Secure the Cable Connections:** Gently tug both ends of the Ethernet cable to verify they are securely inserted into the ports. If loose, reinsert the cable firmly until you hear a "click", indicating it is properly locked in place.
- **Replace Damaged Cables:** If the cable shows signs of damage or fails to perform during testing, replace it with a high-quality new cable. Opt for cables that meet industry standards (e.g., Cat5e, Cat6, or higher) to ensure optimal network performance.
- **Recheck Connections:** Recheck the connection: Ensure that the Ethernet cable between the NAS device and the router or switch is properly connected. Make sure one end of the cable is plugged into the corresponding port on the router or switch, and the other end is plugged into the NAS device.
- **Test the Network Connection:** After completing the steps above, attempt to access the NAS device to check if the network connection has been restored.

2. Test Network Connection

To ensure your NAS device is functioning correctly within the network and accessible from Windows or macOS systems, follow these steps for verification and troubleshooting.

Troubleshooting and Solutions

• Check the IP Address

Ensure that the NAS device has obtained a valid IP address. You can log in to the router's management interface to check whether the NAS device and its assigned IP address appear in the device list, and verify that no firewall rules or port restrictions are blocking communication with the NAS device.

• Verify the Network Connection

For Windows:

- Press **Win + R** to open the Run dialog.
- Type **cmd** and press **Enter** to open the Command Prompt.
- In the Command Prompt, type: **ping <NAS IP Address>** (e.g., **ping 192.168.1.100**), and then press **Enter**.

For macOS or Linux:

- Open the "Terminal" application.
- In the "Terminal", type: `ping <NAS IP Address>` (e.g., `ping 192.168.1.100`), and then press **Enter**.

• Analyze Ping Results

Successful Response: If the Ping command returns a result similar to the following, the network connection is functioning properly:

```
Pinging 192.168.1.100 with 32 bytes of data:
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64
Reply from 192.168.1.100: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

If the Ping command returns results like the examples below, it indicates a problem with the network connection to the NAS device:

```
Pinging 192.168.1.100 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping statistics for 192.168.1.100:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

• Confirm Network Settings

Identify IP Conflicts: If an IP address conflict is detected (another device is using the same IP address as the NAS), adjust the settings in the router's management interface to assign a fixed IP address to the NAS or change the IP address of the other device to avoid conflicts.

Restart Network Devices: Restarting the router, switch, and NAS device can resolve temporary network issues.

Hardware Troubleshooting and Resolution

1. Check the Device's Operational Status

Verify that the NAS device is powered on and properly connected to the power supply. Check whether the indicator lights are functioning as expected, and ensure their blinking patterns match the descriptions in the device's operational guidelines.

Solution: Ensure the power connection is stable and inspect the indicator light status.

2. Inspect the Power Connection

• Verify the Power Adapter:

Ensure you are using the original power adapter supplied with the device.

Inspect the adapter for visible damage, such as cracks or burn marks.

• Check the Power Outlet:

Confirm the outlet is supplying power by testing it with another electrical device.

If no power is detected, inspect your household circuit or contact your utility provider.

• Examine the Power Cord:

Ensure the cord is securely connected between the adapter and the device.

Look for damage, such as fraying or exposed wires.

- **Inspect the Device's Power Port:**

Remove any dust or debris from the port.

Check for physical damage.

3. Power On and Check Indicator Lights

- **Refer to the User Manual:**

Consult the device's manual or quick start guide for information about indicator light statuses.

- **Visit the Knowledge Center:**

Search for relevant tutorials using keywords related to the indicator lights.

- **Observe Indicator Lights:**

Monitor the indicator lights carefully after powering on the device, .

Compare their behavior to the descriptions in the manual or tutorials.

4. Power On and Check Indicator Lights

- **Light Not On:**

Recheck the power connection to ensure all components are securely connected and undamaged.

Try replacing the power adapter or cable.

If the problem persists, restart the device.

- **Flashing or Abnormal Light Color:**

Refer to the manual or tutorials to identify the specific error.

For hardware issues, contact customer support for repairs or part replacement.

For software issues, try resetting the device to factory settings.

5. Restart the Device

- **Perform a Normal Shutdown:**

Press and hold the power button for 5 seconds to shut down the device.

- **Disconnect Power:**

After shutting down, unplug the power cable and wait a few minutes before reconnecting it.

- **Power On the Device:**

Reconnect the power cable and press the power button to restart the device.

Observe the indicator lights to confirm normal operation.

By following these steps, you should be able to effectively diagnose and resolve power and indicator light issues. If the problem persists, contact technical support for further assistance.

Software Troubleshooting and Resolution

1. Troubleshooting and Resolving Software Issues

Ensure the client software, such as the UGREEN Cloud app, is correctly installed and updated to the latest version.

Resolution: Follow these steps to verify and update the client software:

- **Launch the Application:** Open the client software on your device.
- **Update the Software:** If the current version is outdated, check for updates. In some app stores, you may need to manually click the "Update" button, while others may automatically prompt you to install updates.
- **Restart the Application:** Once the update is complete, restart the client software to ensure all features of the new version are functioning correctly.

Keeping the client software updated ensures optimal functionality and enhances the overall user experience.

2. Remove Security Restrictions

Firewalls or antivirus software may block NAS scanning requests, causing access issues. Verify that the device is not subject to excessive access restrictions, such as IP whitelisting.

Resolution: Ensure the firewall settings on your computer or router do not block NAS scanning requests. If any restrictions are detected, modify the settings to allow the requests to pass through. Additionally, verify the settings of the scanning software to remove any potential firewall blocks.

Follow these steps to check and adjust firewall settings to ensure NAS scanning requests are successfully processed.

3. Adjust Computer Firewall Settings

- **Access Firewall Settings:**

Windows: Open the "Control Panel", navigate to "System and Security", and select "Windows Defender Firewall".

macOS: Go to "System Preferences", select "Security & Privacy", and click the "Firewall" tab.

- **Check the Firewall Status:**

Confirm the firewall is enabled. If not, activate it.

- **Permit the UGREEN App:**

Windows: Select "Allow an app or feature through Windows Defender Firewall". Click "Change settings", locate the UGREEN NAS app, and enable both private and public network options. If the app is not listed, click "Allow another app", browse for the app, and add it.

macOS: Click "Firewall Options", then use the "+" button to locate and add the UGREEN NAS app, ensuring it is allowed through the firewall.

- **Save Changes:** Click "OK" or "Apply" to save the adjustments.

4. Adjust Antivirus Firewall Settings

- **Access the Antivirus Software:**

Launch the antivirus software.

- **Access Settings Menu**

Navigate to its "Settings" or "Options" menu.

- **Locate Firewall Options:** Search for sections related to firewall or network configurations.
- **Allow Scanning Requests:** Ensure that the firewall settings within the antivirus program do not block the NAS. Adjust settings to permit these requests or disable the relevant restrictions.
- **Save and Restart:**

After completing the above steps, save the settings and restart the software to ensure the new settings take effect.

By following these steps, you can ensure that the firewall does not block client requests, allowing the scanning process to proceed smoothly.

Additional Methods for Troubleshooting

1. Reset Network Settings

If your network configuration is abnormal, consider resetting the NAS network settings to factory defaults. This can help resolve connection issues caused by improper configurations. Refer to the relevant [Reset Network & Password](#) guide for detailed instructions.

2. Inspect the Router or Switch

Network issues may result from an overloaded router or switch that has been running for an extended period. Restarting these devices often alleviates the problem. Simply power off the equipment, wait a few minutes, and then power it back on to clear caches and free up resources, restoring normal network operation.

3. Switch Network Mode

If your computer is using a wireless connection and frequently encounters unstable signals, try switching to a wired connection. A wired connection provides more stable data transmission speeds and significantly reduces the impact of external interference on network performance.

Troubleshooting abnormal fan noise

When you encounter fan noise or abnormal sounds, please follow these steps to troubleshoot and resolve the issue:

1. Initial inspection:

First, if you can provide a video/audio recording, it would be best to confirm whether there is noise or clicking sounds and other abnormal noises. If abnormal sounds are confirmed to exist:

2. Enter the BIOS to set parameters:

Press the **Ctrl + F12** key combination to enter the BIOS → Select the **Advanced** menu → Enter the **Hardware Monitor** option → Select **SYS SmartFan** → Change from **Automatic Mode** to **Manual Mode** → Change Set **SYSFan Speed 255 to 0** to disable automatic speed adjustment → Select **Save & Exit** → Select Save Changes and Restart to re-enter the BIOS → Confirm whether the above changes have been applied.

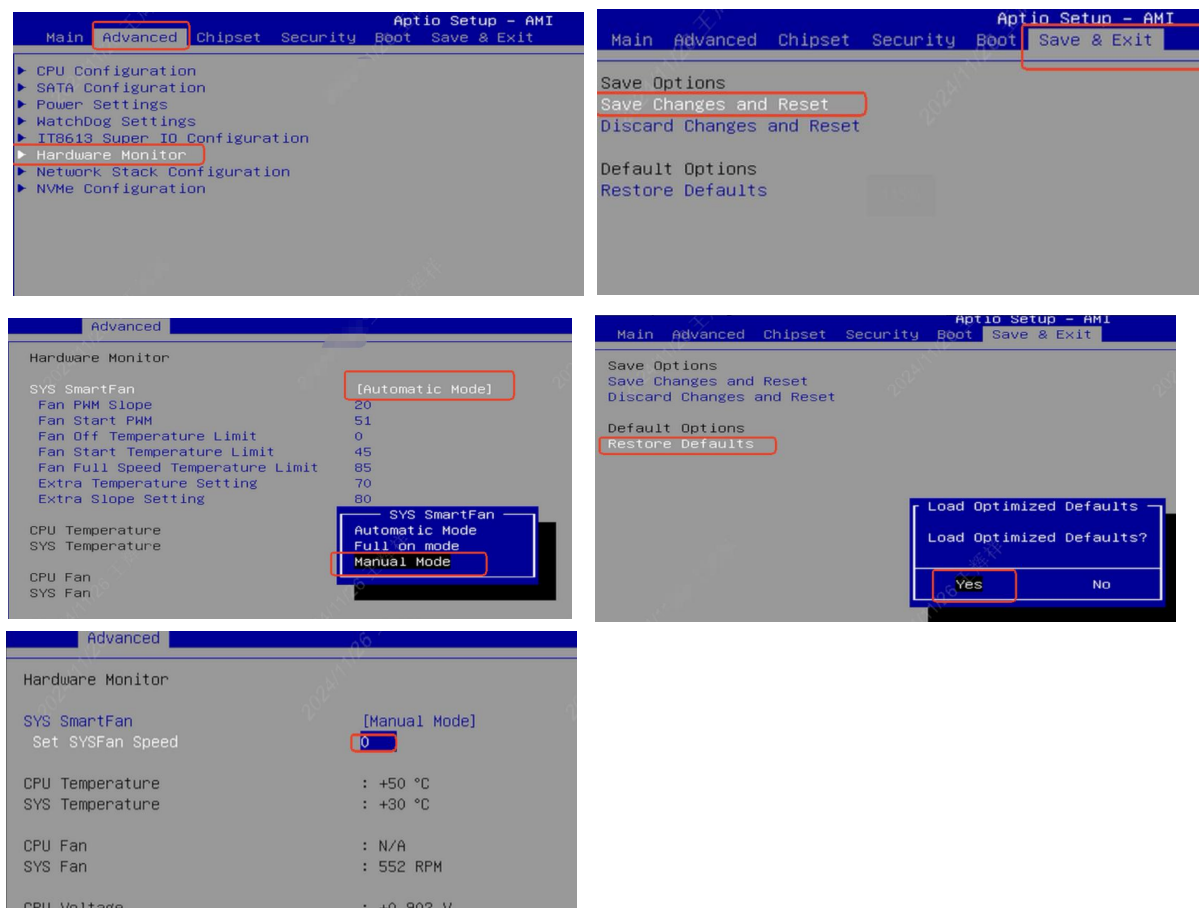
3. If the NAS still has abnormal sounds:

-If the sound comes from the **CPU fan** failure, it is recommended to initiate the after-sales process and send the device to our service center for inspection.

-If it comes from the **system fan**, we will send you a system fan accessory.

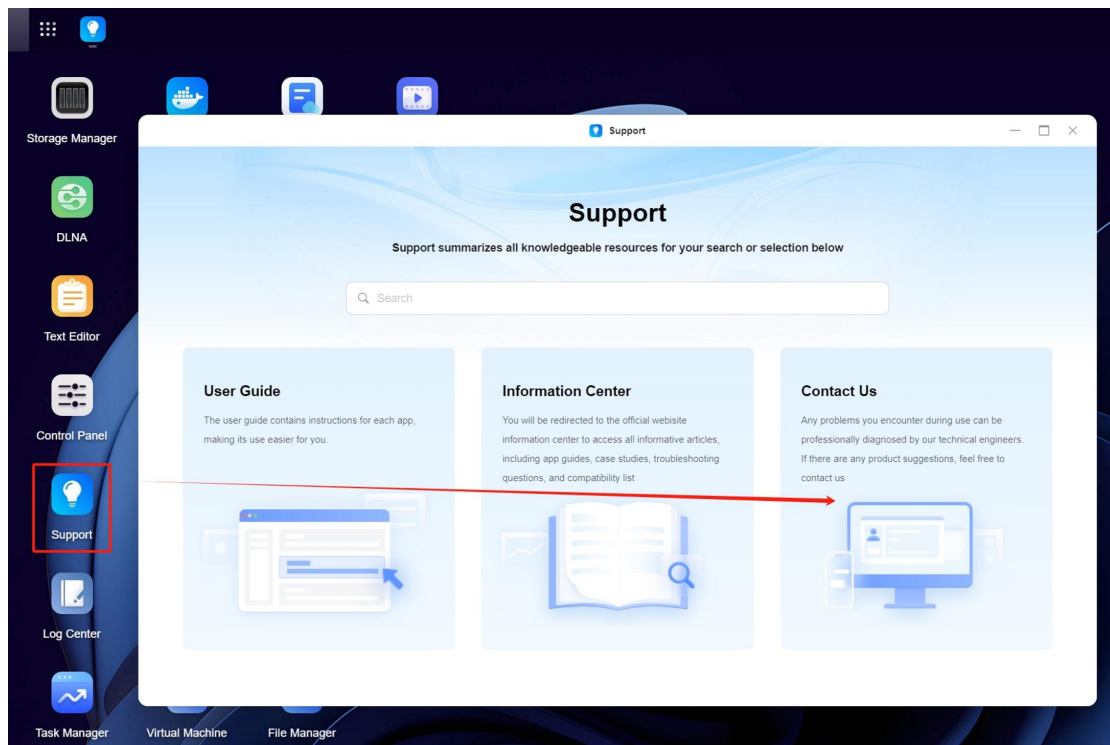
After completing all operations: Please ensure that you have selected '**Save & Exit**' and Restore Defaults to ensure the stability and security of the system.

BIOS fan parameter debugging settings

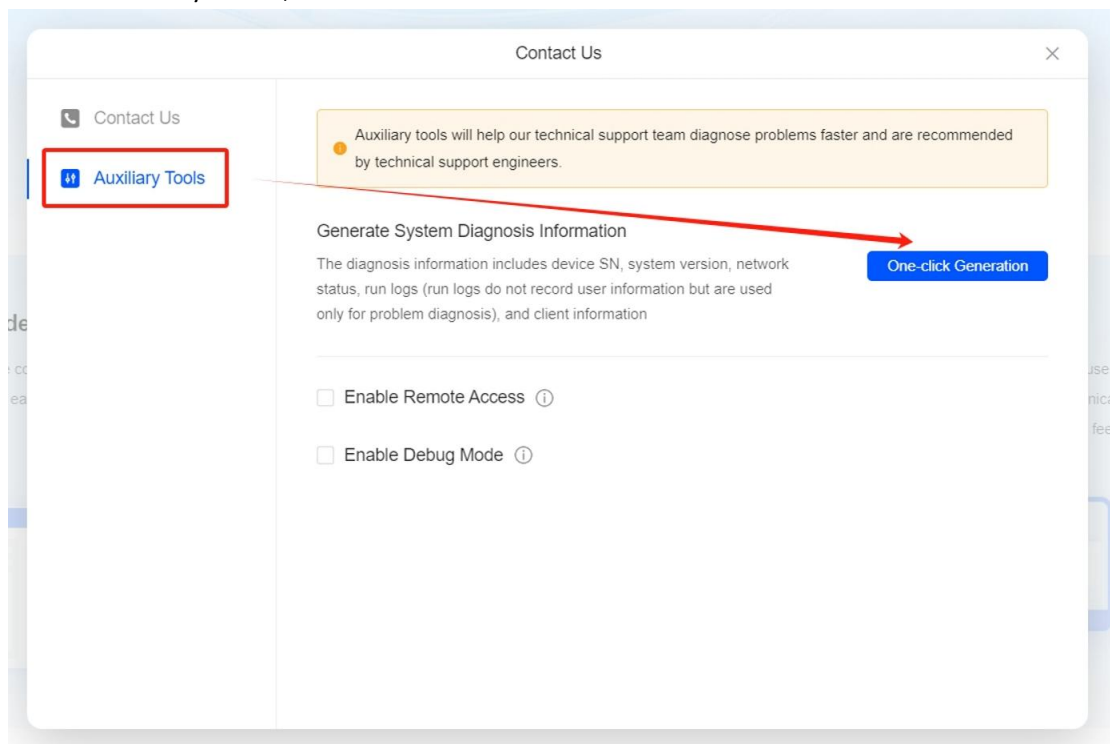


How to generate system logs

1.Click “ Support ”, and then click “ Contact Us ”.



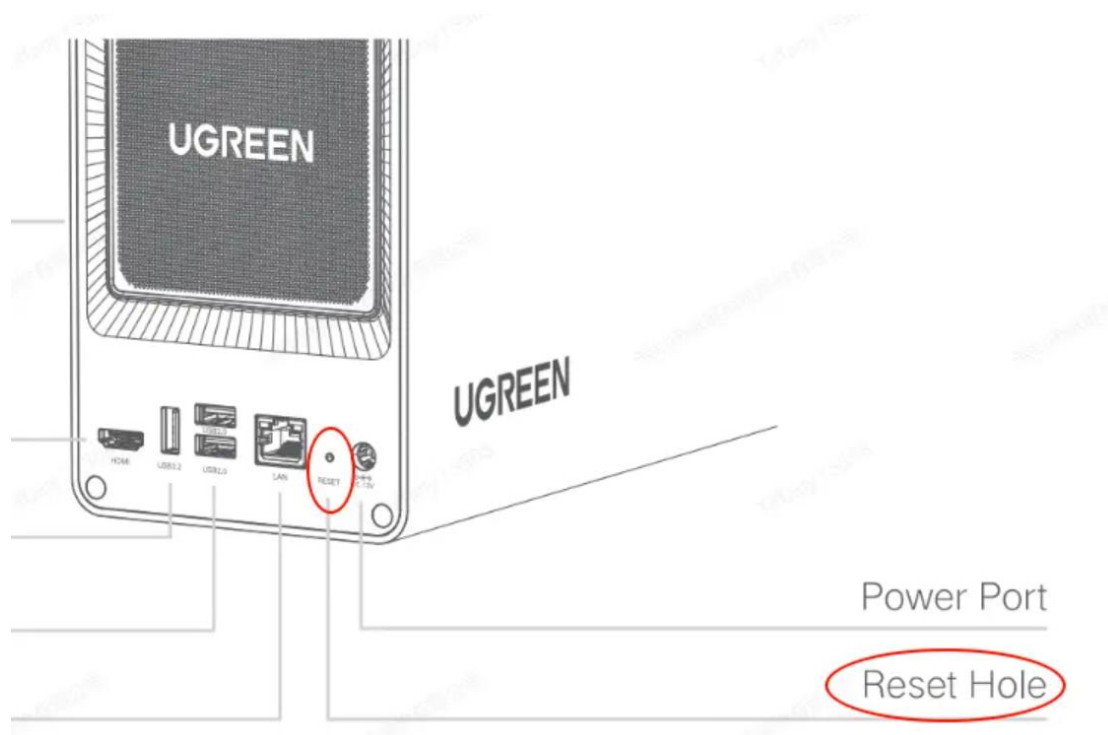
2.Click “ Auxiliary Tools ”, and then click “ One-click Generation ”.



How to Perform a Factory Reset?

If you need to restore your UGREEN NAS to its initial state, you can use either of the following two methods. A factory reset will clear all system settings and installed applications (such as Docker and virtual machines), but the data stored on the hard drives will not be deleted. To avoid unexpected issues, it is recommended to back up important data before proceeding.

Method One: Restore via the RESET Button on the Device

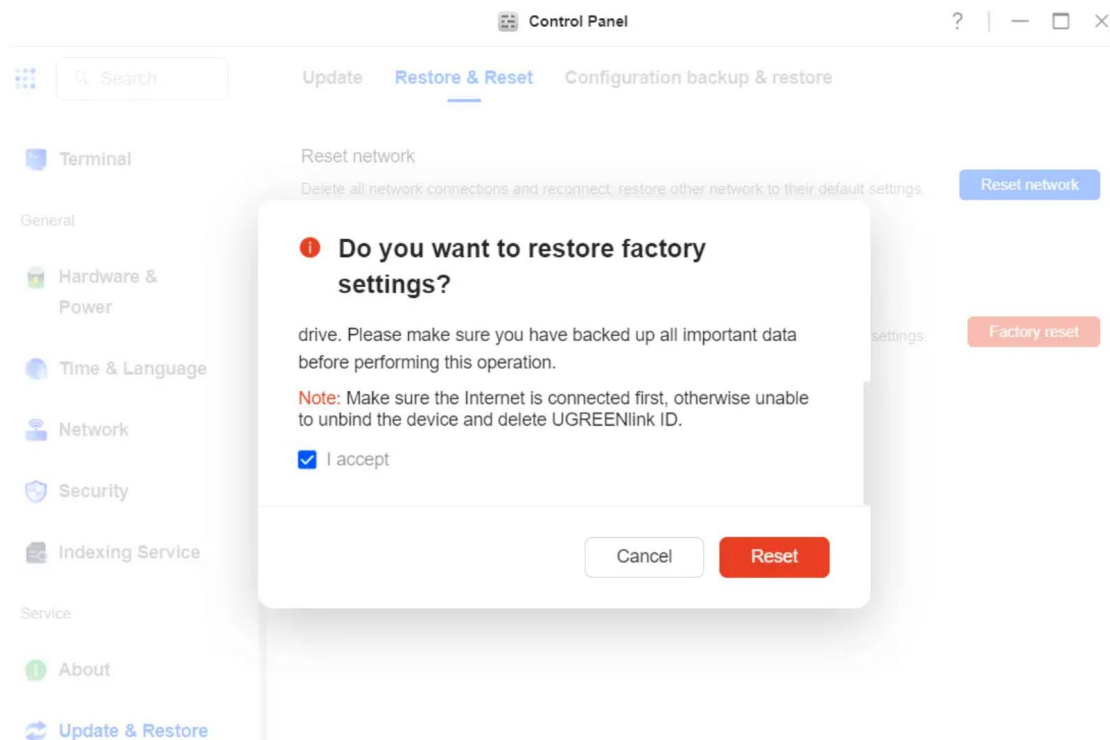


1. Keep the device powered on and running. Using a SIM ejector tool or another sharp object, press and hold the RESET button on the back of the device for 5 seconds, and you will hear a short beep.
2. Keep pressing for about 8 seconds until you hear three consecutive beeps, then release the button.

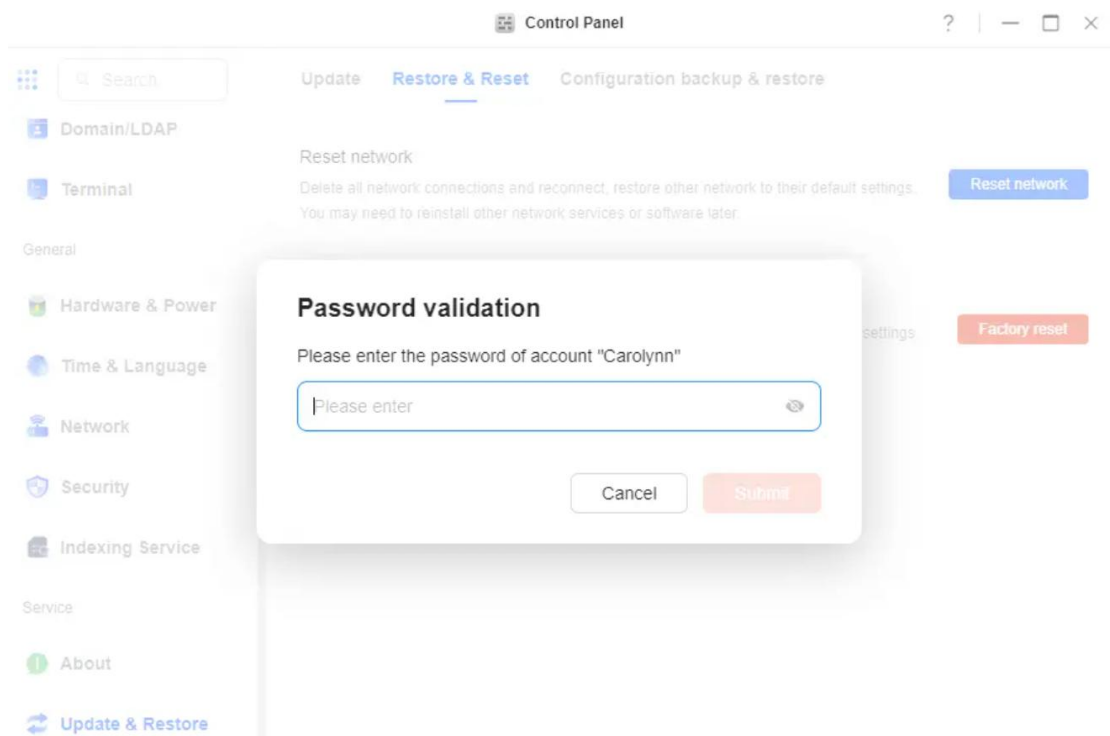
The system will automatically reboot and perform the factory reset operation. When the network indicator light stays solid white, the reset is complete, and you can rebind and initialize the device.

Method Two: Restore via Control Panel

1. Log in to the device using the administrator account, then go to "Control Panel">"Update & Restore">"Restore & Reset".
2. Click the "Factory reset" button to open the pop-up window;
3. In the pop-up, check "I accept", then click the "Reset" button;



4. Enter the password and click "Submit" to verify your identity. After successful verification, the system will begin the restoration process.



Notes

- Factory reset will erase all system settings;
- Factory reset will remove installed applications (including Docker containers, virtual machines, etc.);
- Factory reset will not delete personal data and files stored on the hard drive.

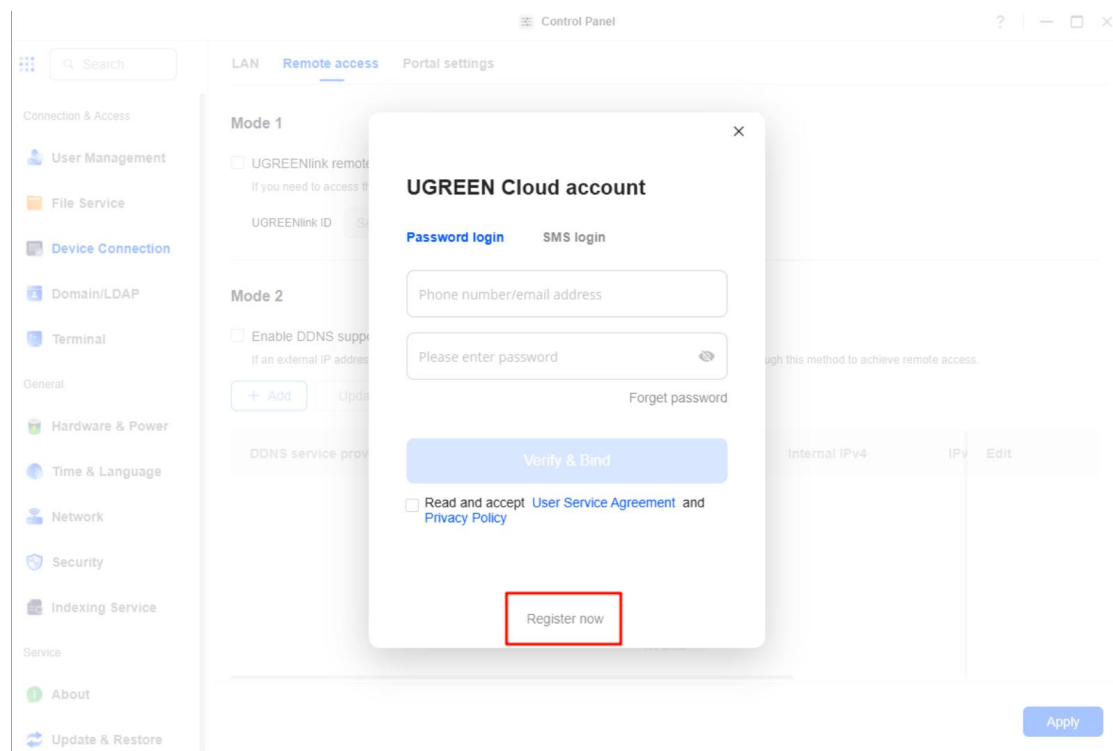
- To avoid data loss, it is recommended to manually back up important data to another safe location (such as an external hard drive or another NAS device) before proceeding.

How to Remotely Access UGREEN NAS via UGREENlink and FAQs

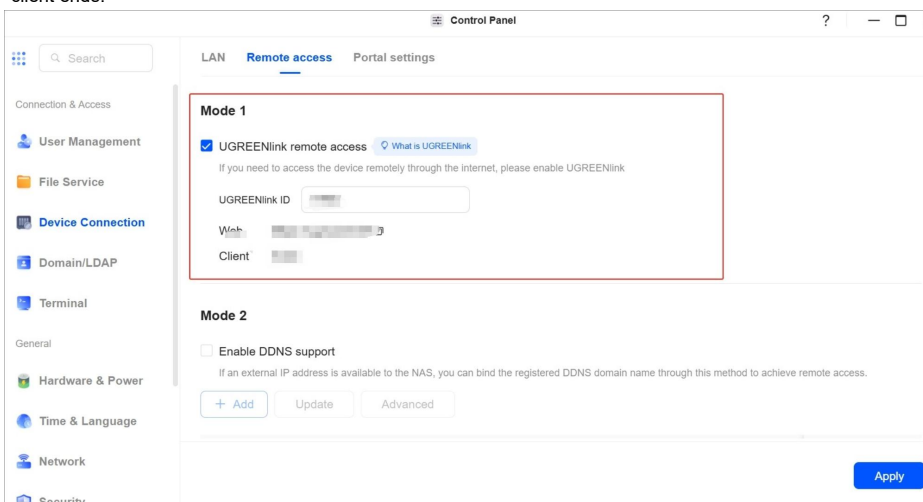
UGREENlink is a proprietary remote access service of the UGREEN UGOS Pro system, providing a secure and efficient way to connect remotely and allowing you to conveniently manage and access your UGREEN NAS devices. With this service, you can create a unique UGREENlink ID for your device to enable quick remote access.

Steps to enable UGREENlink service

1. After logging in to the UGOS Pro system, go to [Control Panel] > [Device Connection] > [Remote Access].
2. Tick the "Enable UGREENlink Remote Access Service" option. [Note: If you haven't registered a UGREEN NAS account, please click the "Register Now" to sign up.](#)



3. Enter an ID you wish to use (e.g., ugreen) in the UGREENlink ID field and click "Apply". [Note: It is recommended to use an easy-to-remember string for your ID. If the ID you set is already taken, the system will prompt you to re-enter one to avoid conflicts with other users' IDs.](#)
4. After successfully creating your UGREENlink ID, the page will display the addresses for remote access to the UGOS Pro web and client ends.



Notes:

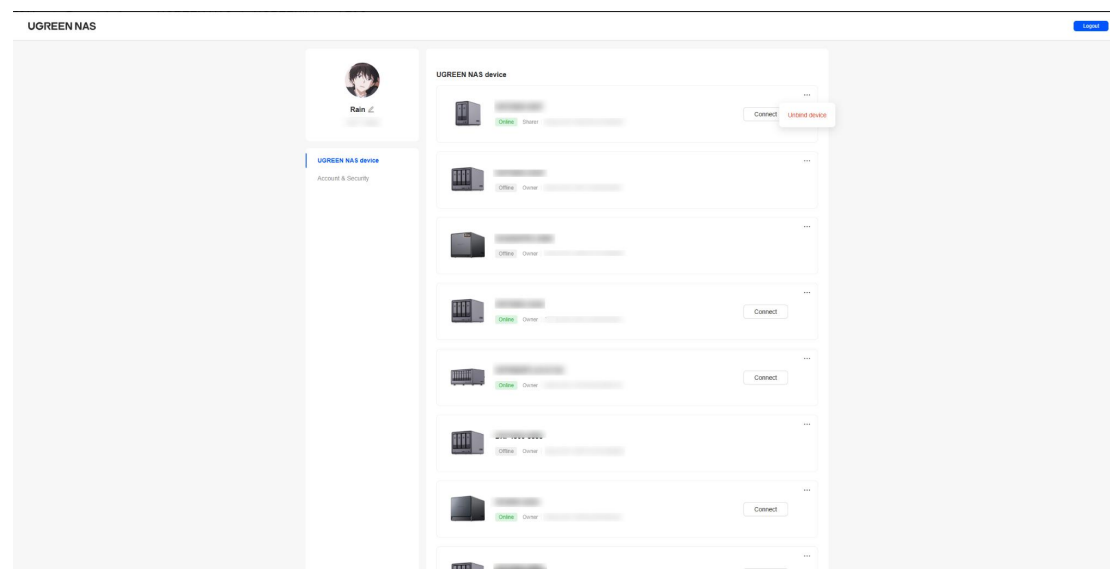
1. To use the UGREENlink service, you must first register or log in to your UGREEN NAS account.
2. After enabling UGREENlink, you can remotely access your NAS via the internet without complex port forwarding settings.
3. UGREENlink will automatically generate a unique subdomain corresponding to your UGREENlink ID for your NAS device and configure an SSL certificate for it to ensure secure access.

Frequently Asked Questions

Q1: How do I change the phone number associated with my UGREENlink?

A1: To change the admin phone number associated with your UGREENlink, follow these steps:

1. Open ugnas login URL in your browser and log in with the UGREENlink phone account you want to unbind.
2. Find the device you need to unbind and perform the unbind operation. [Note: After unbinding, UGREENlink cannot connect to the NAS device anymore, so it is recommended to operate within a local area network.](#)



3. Log in to the device, go to [Control Panel] > [Device Connection] > [Remote Access], uncheck the UGREENlink Remote Access Service, then recheck it, and the system will prompt you to bind a new phone number.

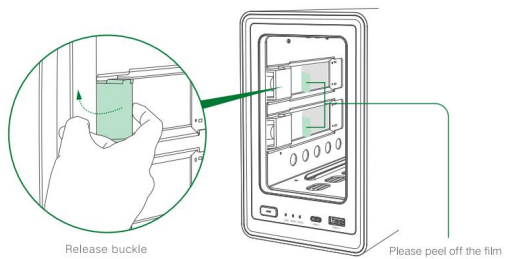
Q2: What is the difference between enabling UGREENlink and using DDNS?

A2: The UGREENlink service is designed to allow you to easily access your home NAS device via the internet regardless of your location, enabling seamless data connection and remote management. With UGREENlink enabled, you can easily access your NAS device on your phone or computer. DDNS (Dynamic Domain Name System) service allows you to access your NAS device from anywhere by mapping a dynamic IP address to a fixed domain name.

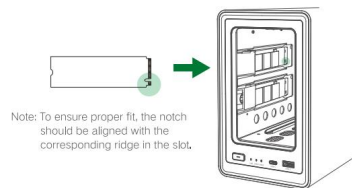
Installing M.2 SSDs (Optional)

What does installing an M.2 SSD do?
M.2 SSDs can be used as a normal storage drive or as a read/write cache to improve reading and writing performance of random data.

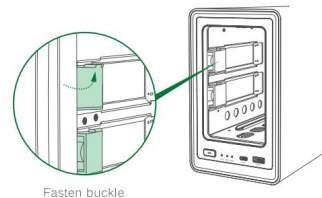
1. After powering off, pull the tray out to reveal the M.2 slot, located on the inner left side of the device. Pull back to release the buckle.



2. Insert M.2 SSD into the slot in the direction shown by the image below.



3. Gently press lifted end and fasten the buckle after SSD is firmly inserted.



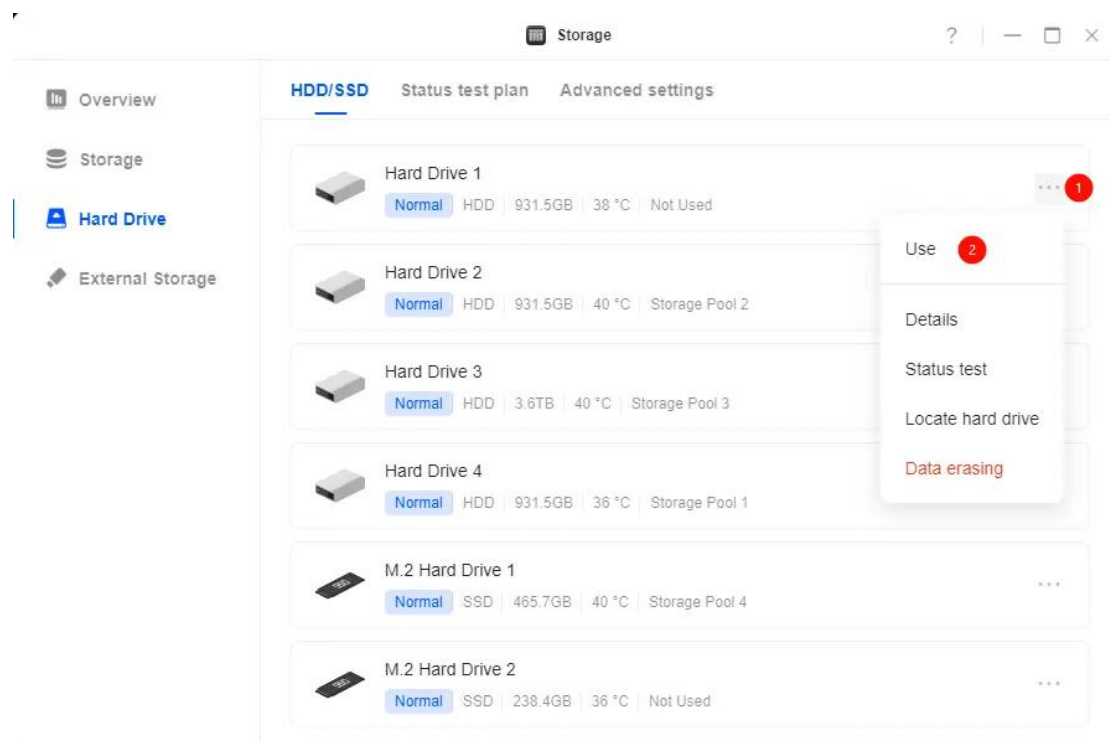
When replacing a UGREEN NAS with a new one, you can directly migrate the internal storage drives from the old NAS to the new device and continue using them as internal storage.

Note:

- This feature is only supported on UGREEN NAS devices running the UGOS Pro system.
- Migration is only supported between UGREEN NAS devices.
- Applications such as Docker and Virtual Machine must be reinstalled and redeployed on the new device; lossless migration is not supported.

Migration Steps

1. Install the internal storage drives from the old NAS into the new NAS device and power it on.
2. Log in to the management interface of the new NAS and open the "Storage" app.
3. Click "Hard Drive" > "HDD/SDD", and locate the drives migrated from the old NAS.
4. Click the "..." button next to the target drive and select "Use".



5. On the "Use hard drive" page, select "Internal Storage" and follow the on-screen instructions to complete the setup.

Use hard drive



Current hard disk can be used to:

Create storage pool

Hot spare hard disk

Change RAID type

Replace hard disk in the storage pool

For example, Hard Disk 3 is used as external storage only for reading and writing files



External storage

If Hard Disk 3 need to be converted to internal storage for deep utilization ⓘ

Internal storage

6. Once the process is complete, the data on the old NAS drives will be accessible as internal storage on the new NAS.

Please download this :

<https://api-eur.ugnas.com/api/system/v1/ua/temp/flashing/downloadUrl?id=1910&sn=EC752JJ4525308E0&urlId=1311&tokenId=2039984780191023104>

UGOS Pro Firmware Update Guide

1. Preparations Before UGOS Pro Firmware Update

This section provides a detailed guide on the preparations and considerations needed before updating the UGOS Pro firmware. To ensure a smooth update process, please read the following information carefully.

1.1 Applicable Models

This ISO image is applicable for the following UGREEN NAS products:

- DH2600
- DX4600*: DX4600、DX4600+、DX4600 Pro;
- DXP Series: DXP2800、DXP4800、DXP4800 Plus、DXP6800 Plus、DXP6800 Pro、DXP8800、DXP8800 Plus、DXP8800 Pro、DXP480T Plus。

For other products, please contact UGREEN's official technical support for assistance.

1.2 Data Backup

Before updating, it is crucial to back up all important personal data to the cloud or a computer. There are risks involved in this process, and improper operations may lead to data loss or device malfunction.

1.3 Obtain the Official ISO Image

1. Contact UGREEN NAS official technical support and provide the device serial number (SN).
2. Download the ISO image using the link provided by technical support (the link is valid for one download).

1.4 Create a Bootable USB Drive

This step requires using a disk writing tool on your computer to burn the image file onto a USB drive. The USB drive can be removed after the installation is complete. You can choose from disk writing tools such as Rufus, Balenaetcher, etc. The following example uses Rufus:

What is a UPS?

A UPS (Uninterruptible Power Supply) is a device that provides temporary backup power when the main electrical supply is interrupted. It is commonly used to protect NAS devices and the data they contain from loss or hardware damage caused by unexpected power outages.

This guide will show you how to properly connect and configure a UPS on a UGREEN NAS, ensuring seamless power protection and allowing the device to shut down safely in the event of a power loss, minimizing the risk of data loss.

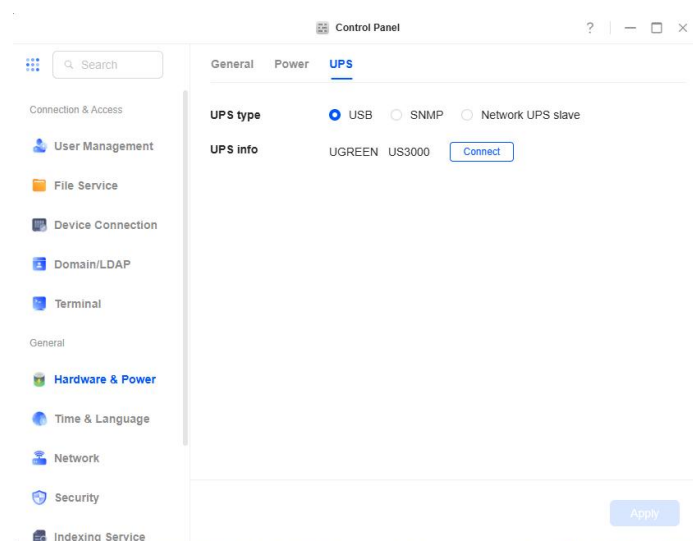
Connecting a UPS to a UGREEN NAS (Example: UGREEN US3000)

1. Choose a UPS model that is compatible with your UGREEN NAS.
2. Power off the NAS and disconnect its power adapter. **Note:** Make sure to stop all data transfers before shutting down the NAS to avoid data loss.
3. Plug the original NAS power adapter into a wall outlet, and connect the other end to the UPS's DC IN port.
4. Use a USB data cable to connect the UPS's USB port to the USB port on the back of the NAS.
5. Connect the UPS's DC OUT cable to the NAS's power input.
6. Once connected, the UPS's LED indicator will flash white. Log in to the UGOS Pro system to check the UPS's battery level and status information.

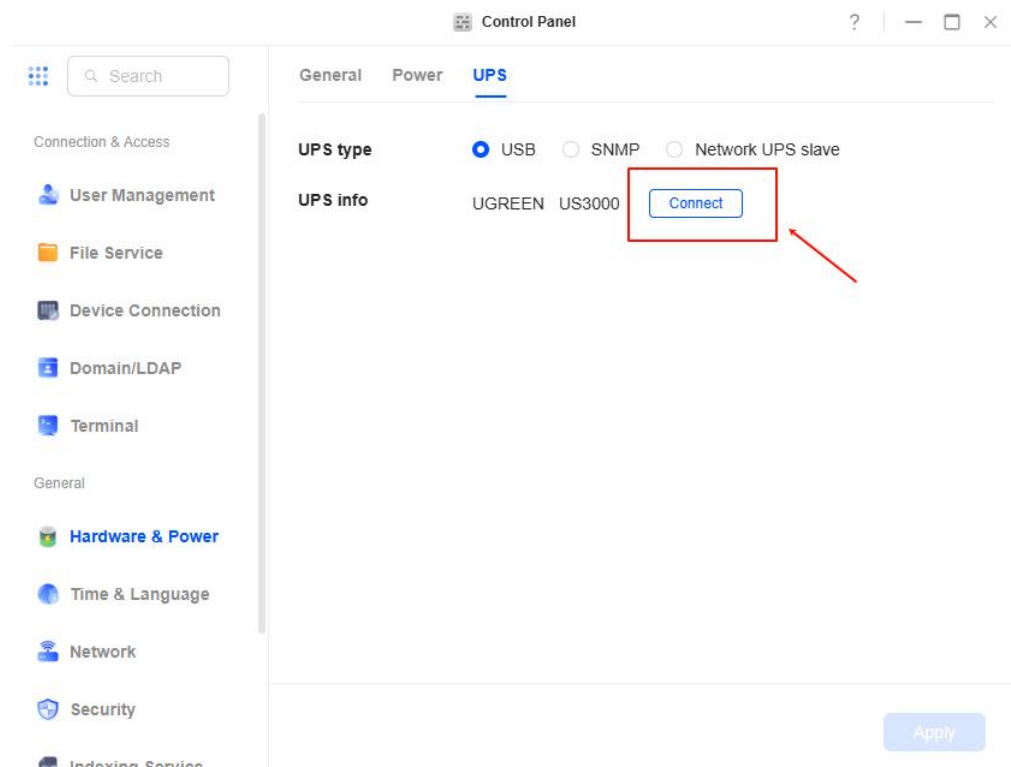
For more details, please refer to the official user manual of your UPS device.

Configure the UPS in UGOS Pro

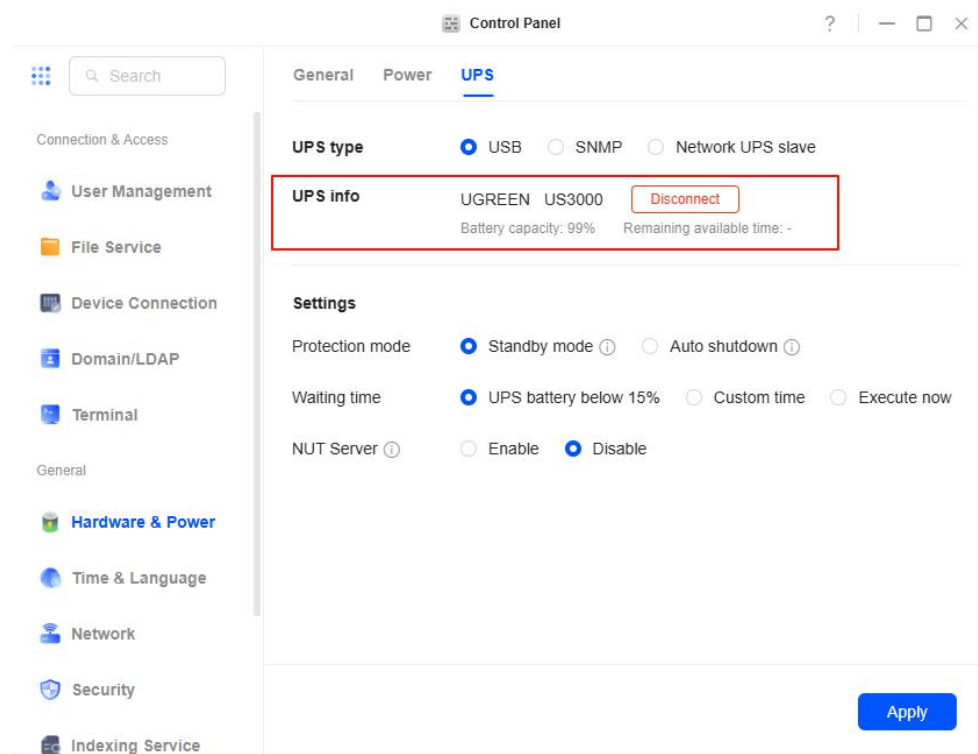
1. Log in to UGOS Pro, then go to [Control Panel] > [Hardware & Power] > [UPS]. The system will automatically detect any connected UPS device.



2. Click "Connect", and the UPS page will display the device's vendor and model information.



3. Once connected, you can view the UPS's current battery capacity and estimated remaining runtime.



4. Set the NAS protection method when the UPS loses mains power. The following two options are available:

Protection Mode	Description
Standby Mode	After a power loss, the NAS will stop all services to prevent data loss and shut down once the UPS battery is depleted. If [Power On Automatically When Power Is Restored] is enabled, it will restart automatically when mains power returns.
Auto Shutdown	The NAS will initiate a normal shutdown. If [Power On Automatically When Power Is Restored] is enabled, it will automatically restart when mains power is restored.

5. Set the delay time before the NAS protection mode activates after a mains power outage:

The screenshot shows the 'Control Panel' window with the 'UPS' tab selected. The left sidebar contains various system settings categories. The main content area displays the following settings:

- UPS type:** USB (selected), SNMP, Network UPS slave
- UPS info:** UGREEN US3000, Battery capacity: 99%, Remaining available time: -
- Settings:**
 - Protection mode:** Standby mode (selected), Auto shutdown
 - Waiting time:** UPS battery below 15%, Custom time (selected, 30 min), Execute now
 - NUT Server:** Enable, Disable (selected)

An 'Apply' button is located at the bottom right of the settings area.

- **UPS battery below 15%:** Check this option to have the NAS enter Standby Mode or Auto Shutdown when the UPS battery level falls below 15%.

- **Custom time:** Check this option to have the UGREEN NAS enter Standby Mode or Auto Shutdown after the configured power supply duration is reached.

- **Execute now:** Check this option to have the UGREEN NAS enter Standby Mode or Auto Shutdown immediately.

Note: Regardless of the protection mode selected, the UGREEN NAS will automatically shut down once the UPS battery is fully depleted.

6. After completing the above settings, click "Apply" to save.

7. It is recommended to simulate a power outage after UPS installation and configuration to ensure that the UGREEN NAS properly switches to UPS power and safely shuts down when battery is low.

Frequently Asked Question

Q: Do I need to manually connect and configure the UPS in the UGREEN NAS system?

A: Yes, you need to manually connect and configure the UPS in the system to ensure a valid connection with the NAS. If you do not require UPS support, you can also manually disconnect the UPS connection.

How to Build the Home Assistant Smart Home System with Docker

Home Assistant (HA) is an open-source smart home system built on Python, offering integration with various devices and highly customizable configurations. With Home Assistant, you can easily connect smart devices from different brands (such as cameras, fans, air conditioners) and leverage automation, group management, and UI customization features to create a personalized smart space. Additionally, HA supports Siri control, allowing users to manage home devices effortlessly through voice commands.

As open-source software, Home Assistant is available for free and is compatible with thousands of devices and services, enabling you to build a unified, intelligently connected home management system.



Deploy Container Using Docker Compose

To quickly deploy Home Assistant on UGREEN NAS, it is recommended to use Docker Compose for project management. This method is suitable when you need to create and manage multiple containers, making containerized management convenient. The following detailed steps will guide you how to deploy Home Assistant using Docker Compose.

Access the Docker Project Interface

In the UGOS Pro system of UGREEN NAS, open the "Docker" app, click [Project] > [Create] to start the project creation wizard.

Configure the Docker Compose File

In the wizard, you'll need to provide a Docker Compose configuration file. Below is the example configuration file for Home Assistant:

▼

复制代码

```
services:
  homeassistant:
    container_name: homeassistant # Container name
    image: homeassistant/home-assistant:latest # Container image
version
  restart: always # Container restart policy
  network_mode: host # Container network mode
  volumes:
    - ./homeassistant:/config # Mount directory for
configuration files storage
  environment:
    - TZ=Asia/Shanghai # Timezone setting
```

Parameter Details

volumes

Use the volumes directive to enable shared storage between the NAS main unit and the container.

`./` represents the directory where the Docker Compose file is located, and the `homeassistant` folder in this directory will be mapped to the `/config` directory in the container. All configuration files and databases for Home Assistant will be stored in this directory.

container_name

Assign the name `homeassistant` to the Docker container to facilitate direct management by container name.

image

Specify the Home Assistant Docker image to use. The `latest` tag ensures that the most recent version is pulled.

restart

Set the container's restart policy to `always` . This ensures the container restarts automatically, regardless of whether it stopped normally or unexpectedly.

network_mode

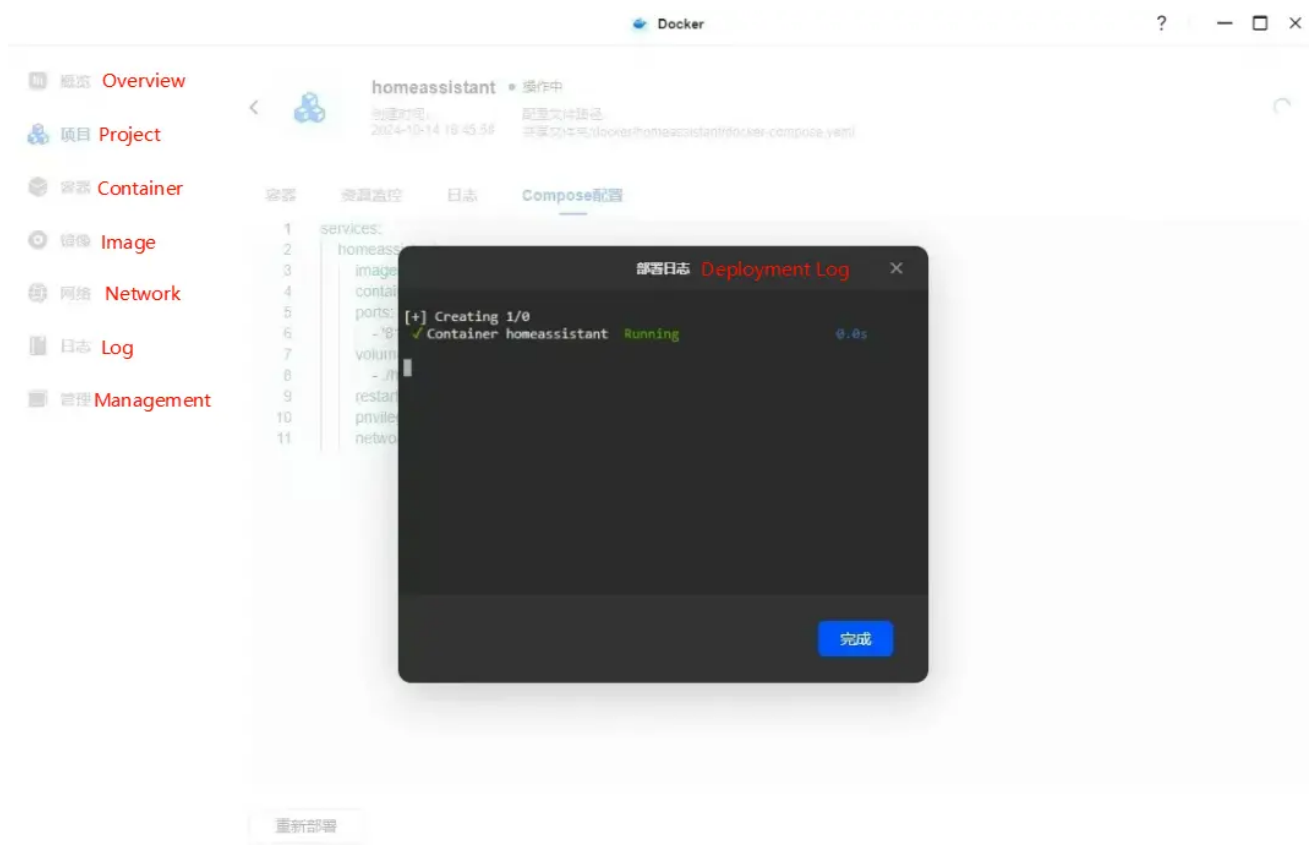
Configure the container's network mode as `host` , allowing the container to use the NAS host's network interface directly, simplifying communication with external smart devices.

environment

Use the environment variable `TZ=Asia/Shanghai` to set the container's time zone. This is essential for maintaining consistent timestamps for automated tasks and logs. You can adjust the time zone to match your location (e.g., `America/New_York` or `Europe/London`).

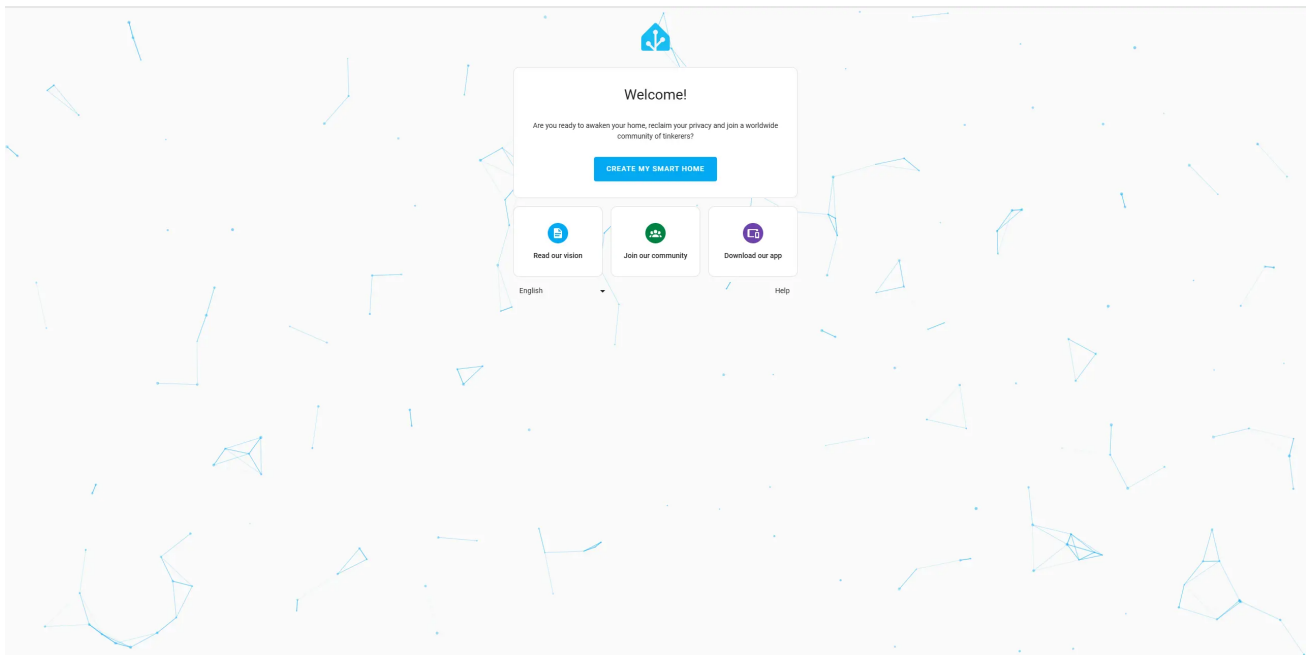
Deploy the Project

After confirming that the configuration file is correct, click [Deploy]. The system will automatically pull the image and start the container. Once the deployment is complete, you can access the Home Assistant console by visiting `http://<NAS_IP>:8123` in your browser.

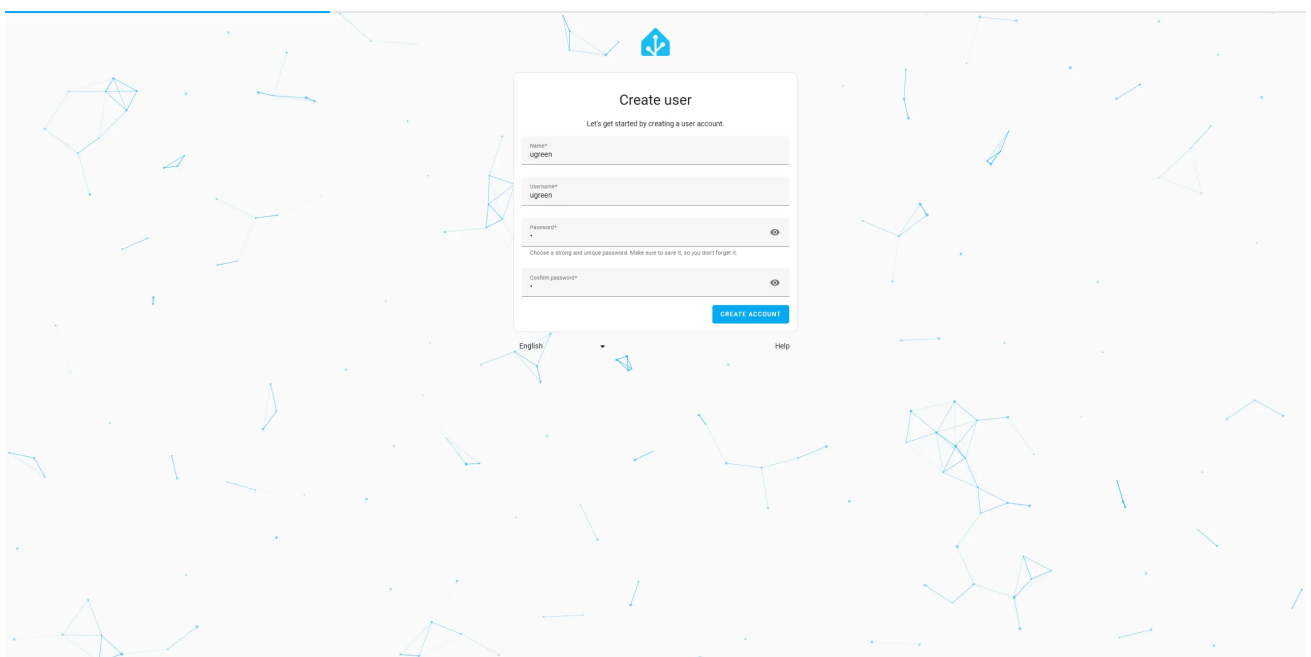


Access the Home Assistant Console

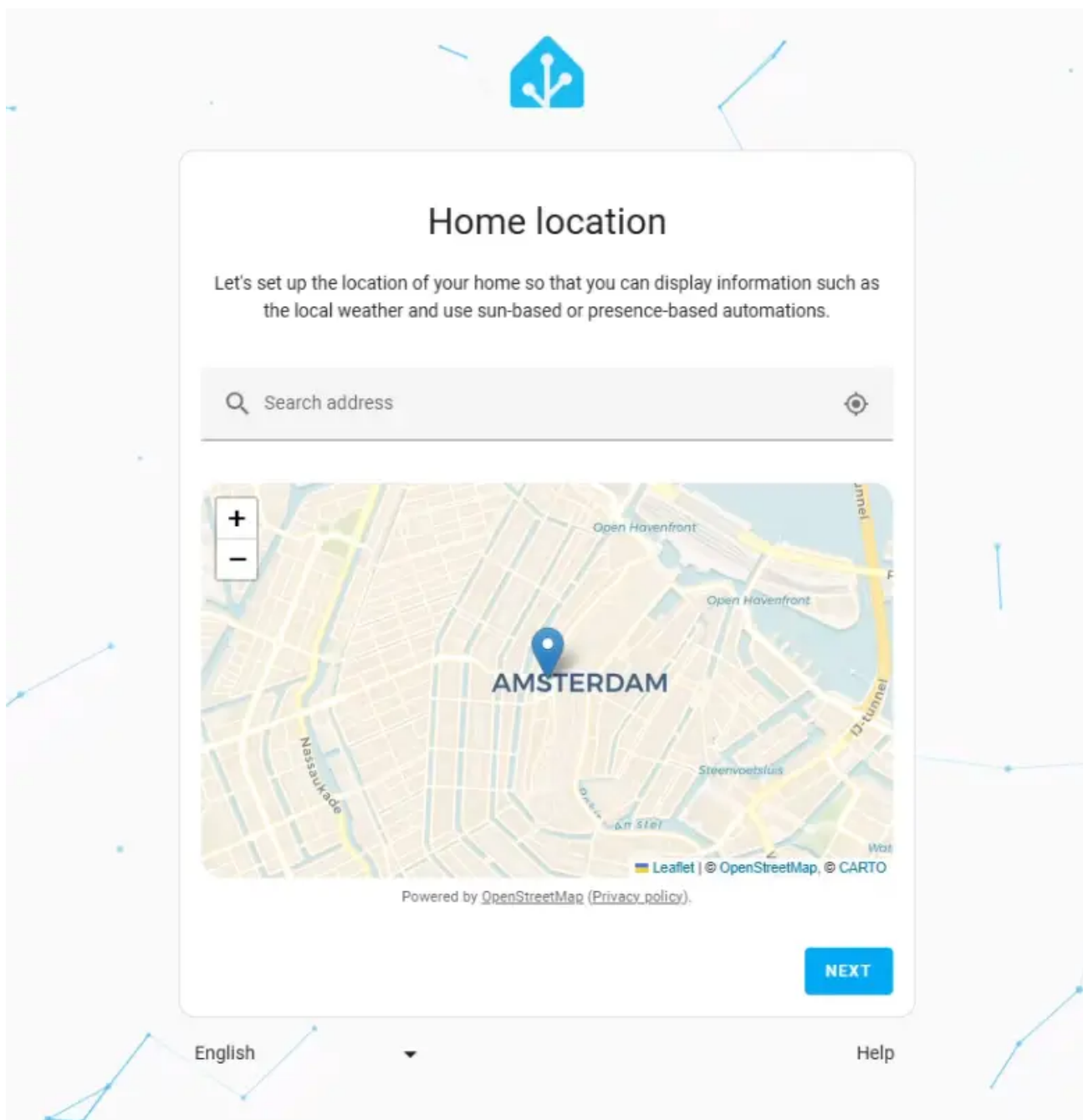
1. After the deployment is complete, open the browser and enter the NAS IP address and port to access the console. Click "CREATE MY SMART HOME" and follow the setup wizard to complete the configuration.



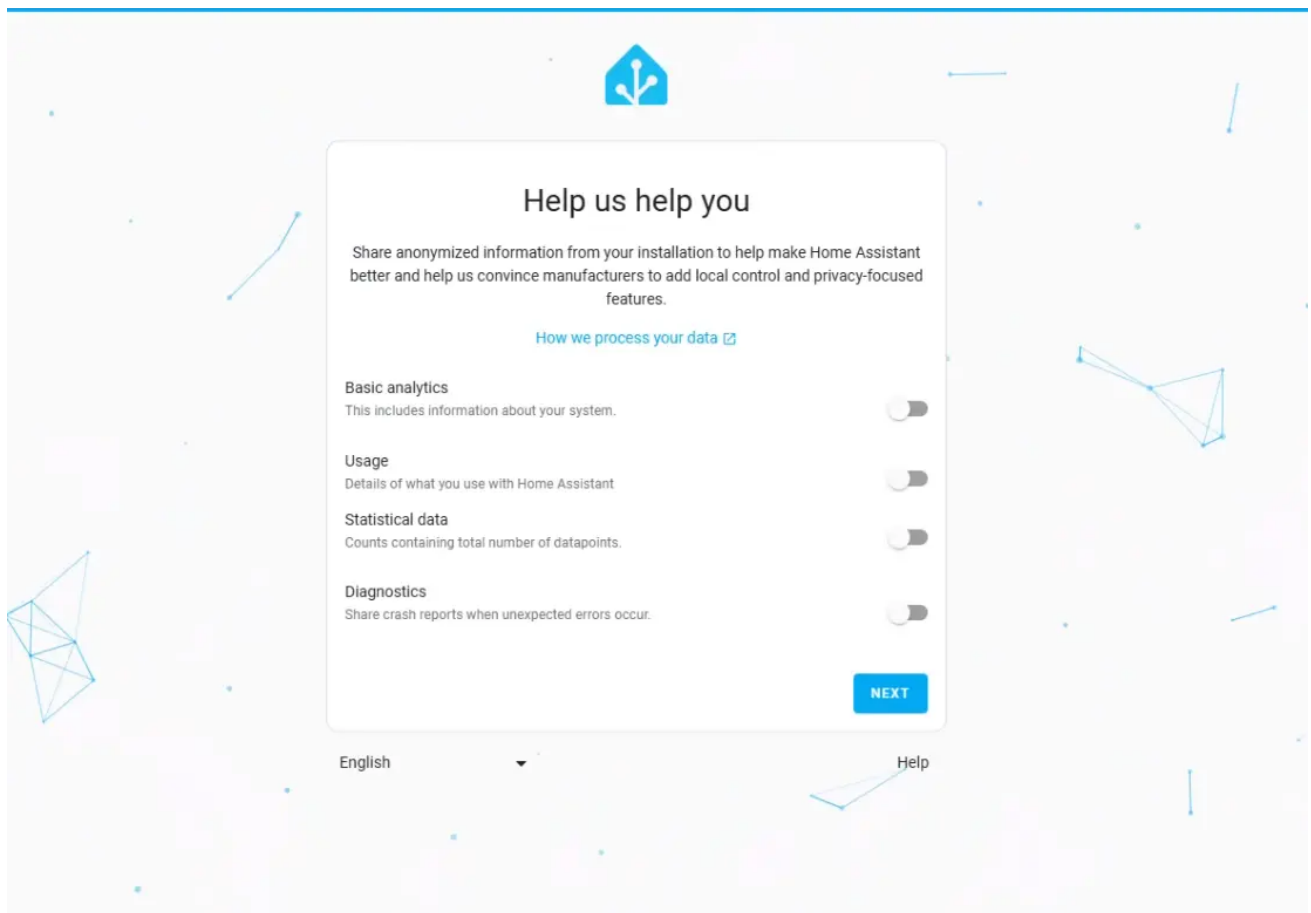
2. Follow the prompts to enter your name, username, and password to create your Home Assistant account.



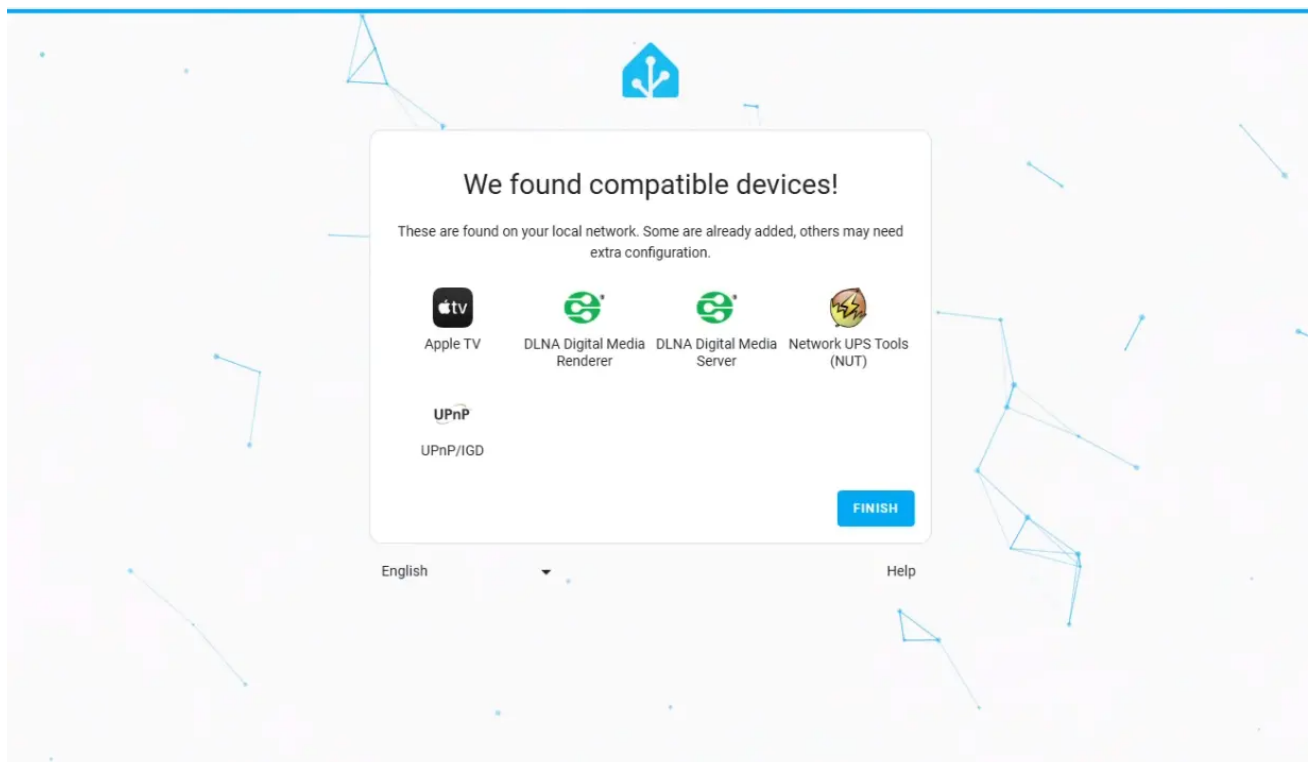
3. You can set your home's location based on your actual needs, or click "Skip" to proceed.



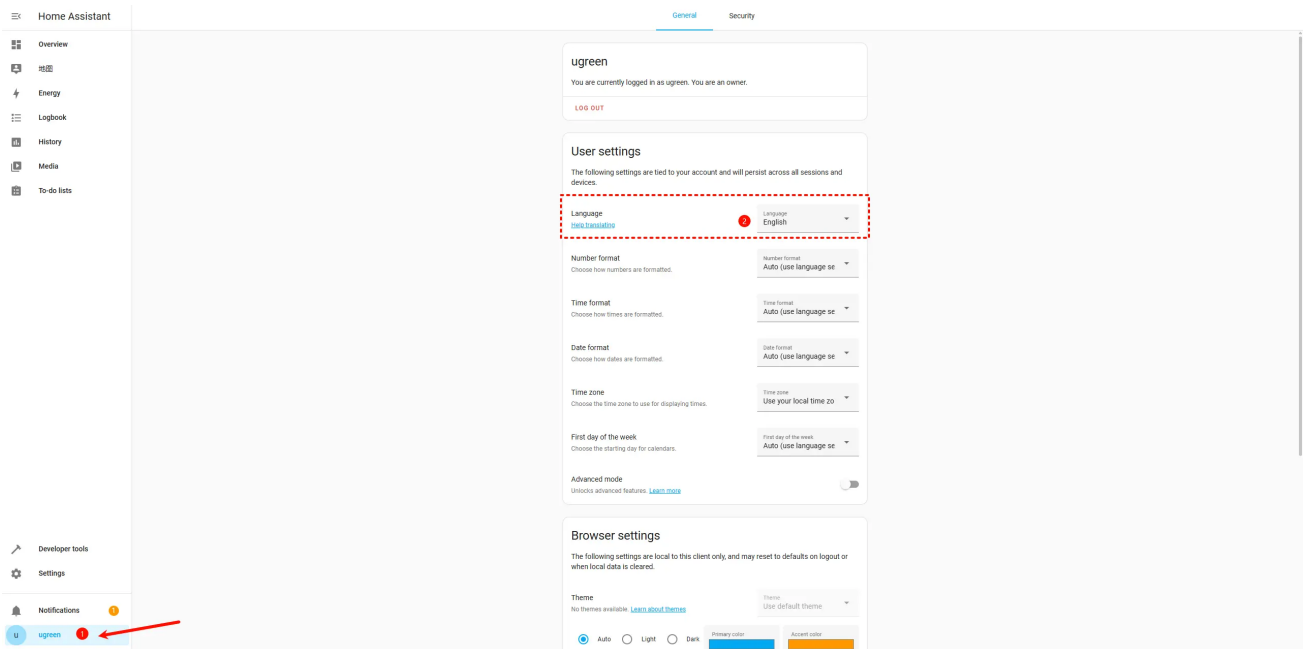
4. Choose whether to enable specific features as needed, then click "Next" to continue.



5. Click "FINISH" to access the Home Assistant home page. You can add devices, configure automation rules, and customize the dashboard here.



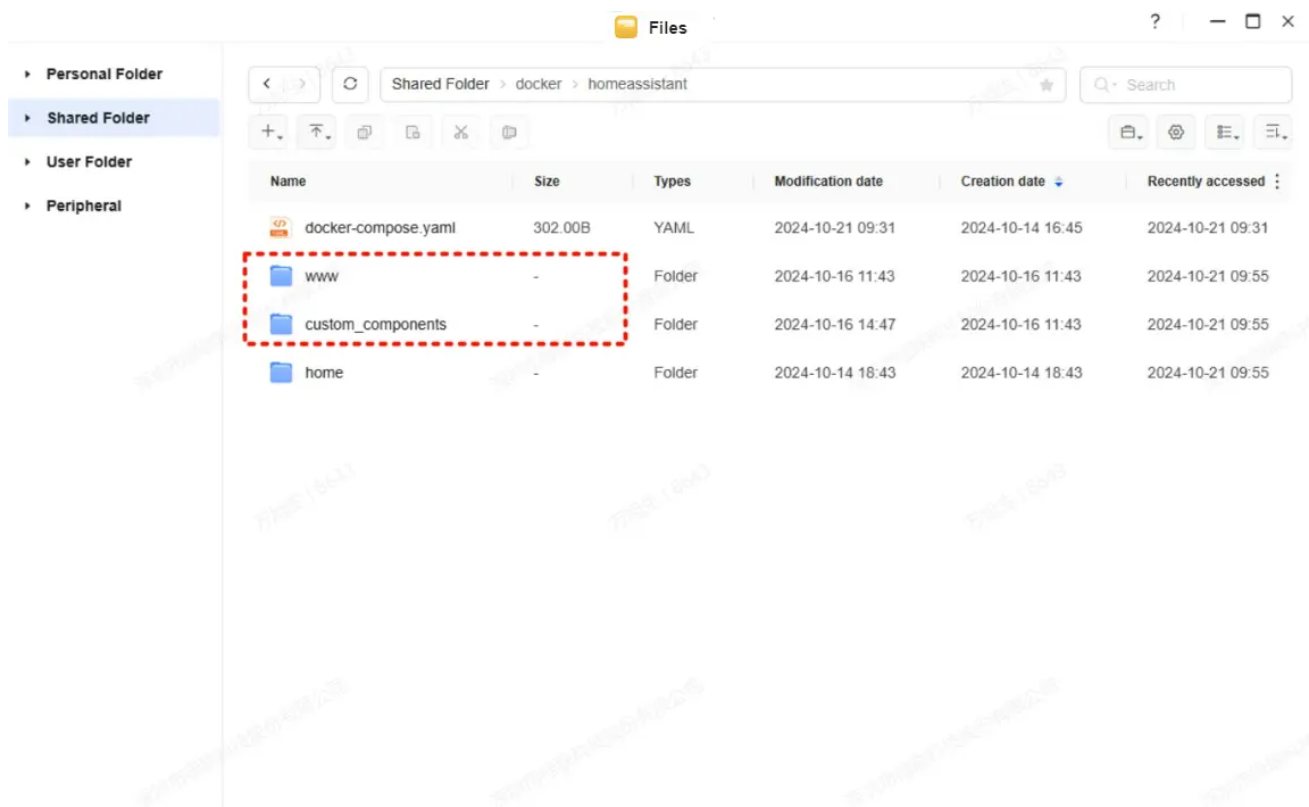
6. If you need to change the language, you can adjust the system language to one you are familiar with in "User settings".



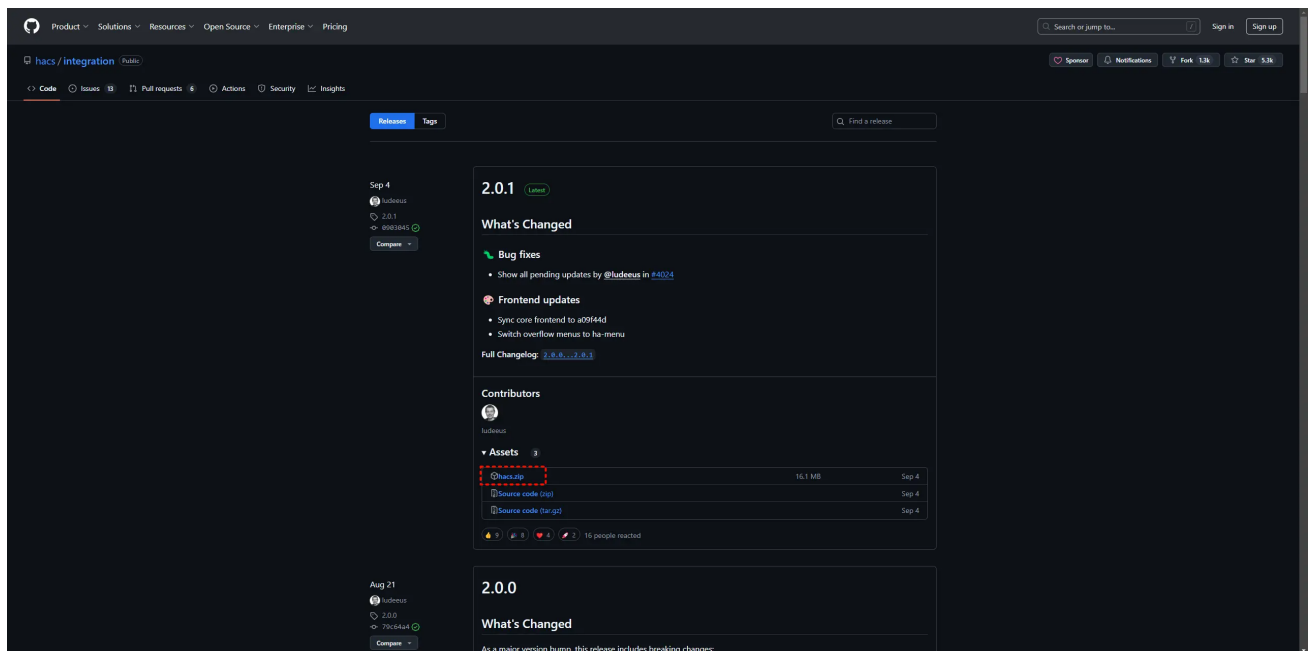
Install the HACS Plugin Store

HACS (Home Assistant Community Store) is a community-driven plugin store of Home Assistant, allowing users to install various integrations and plugins. Follow these steps to install HACS:

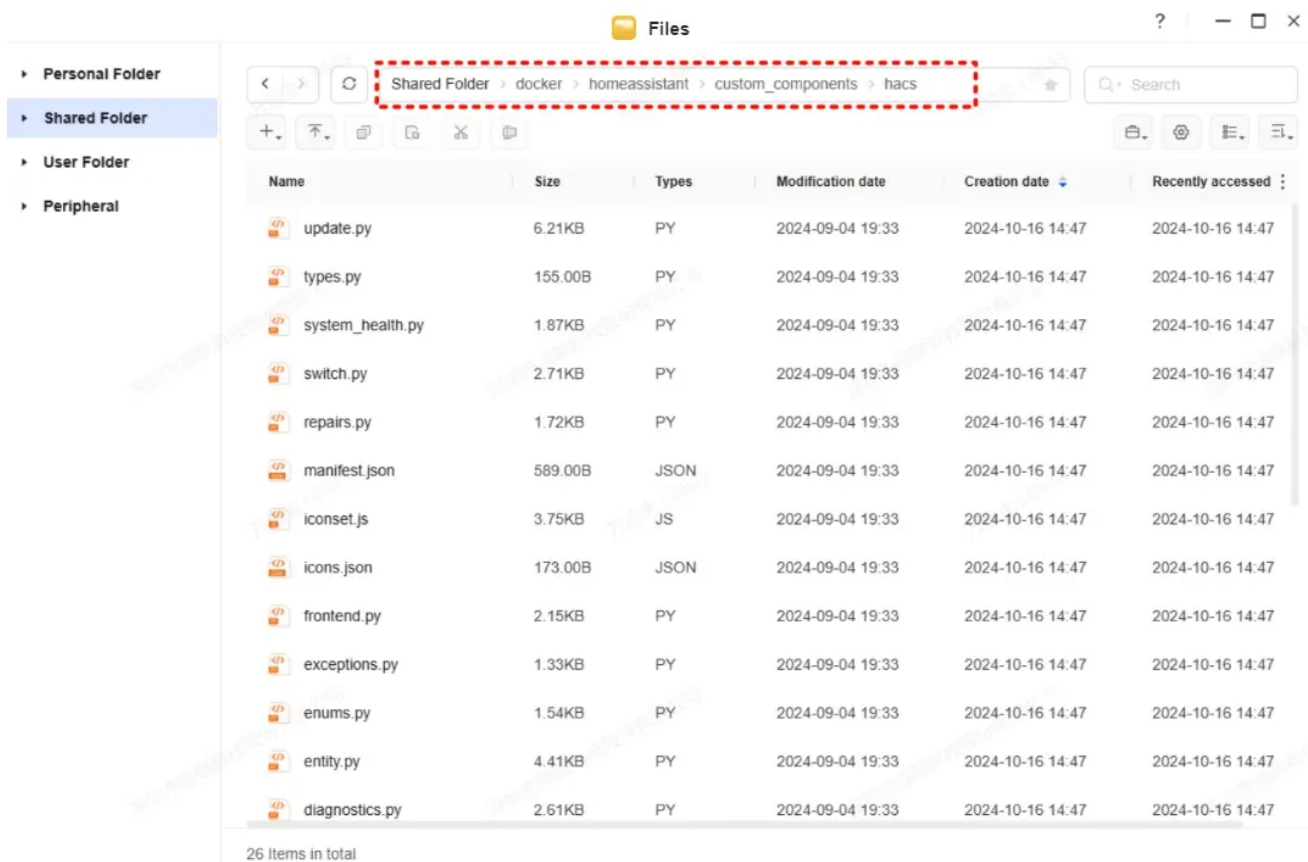
1. Open the file manager, create `www` and `custom_components` folders under the `homeassistant` directory, and then create a `hacs` folder inside the `custom_components` directory. **#**
custom_components is the plugin directory.



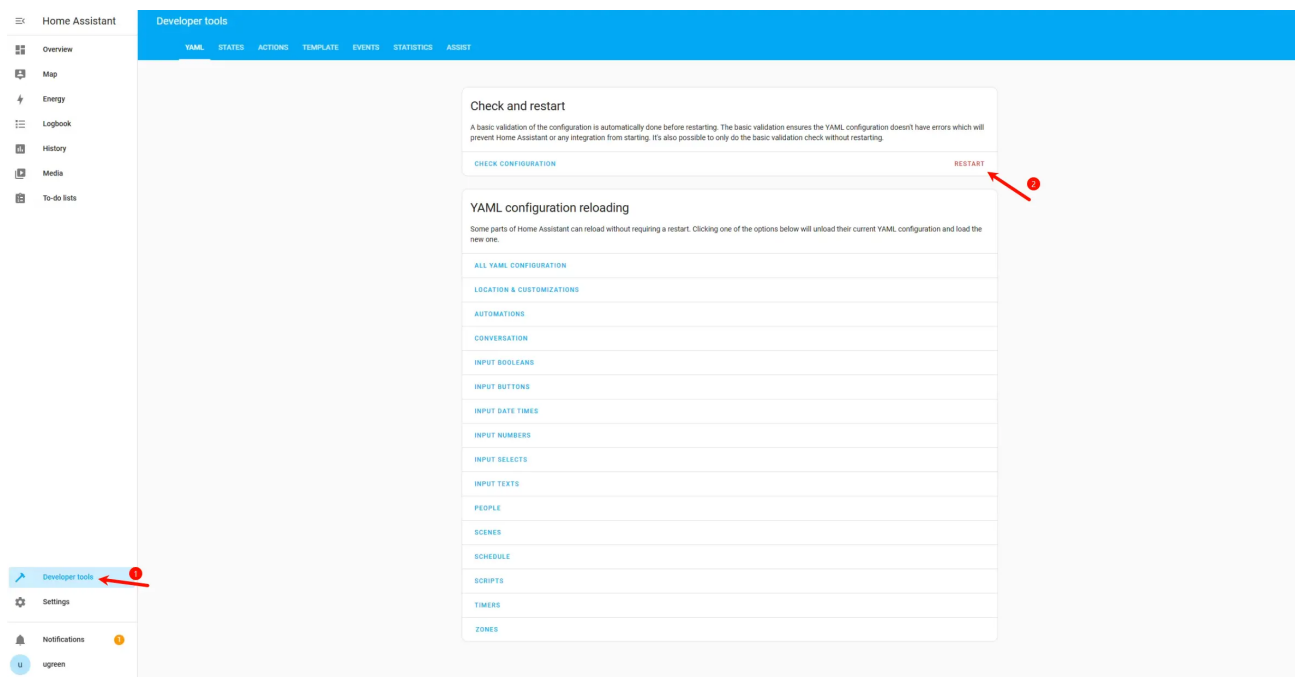
2. Go to GitHub to download the latest version of the HACS archive. If you don't have a GitHub account, you can register one first and then proceed with the download.



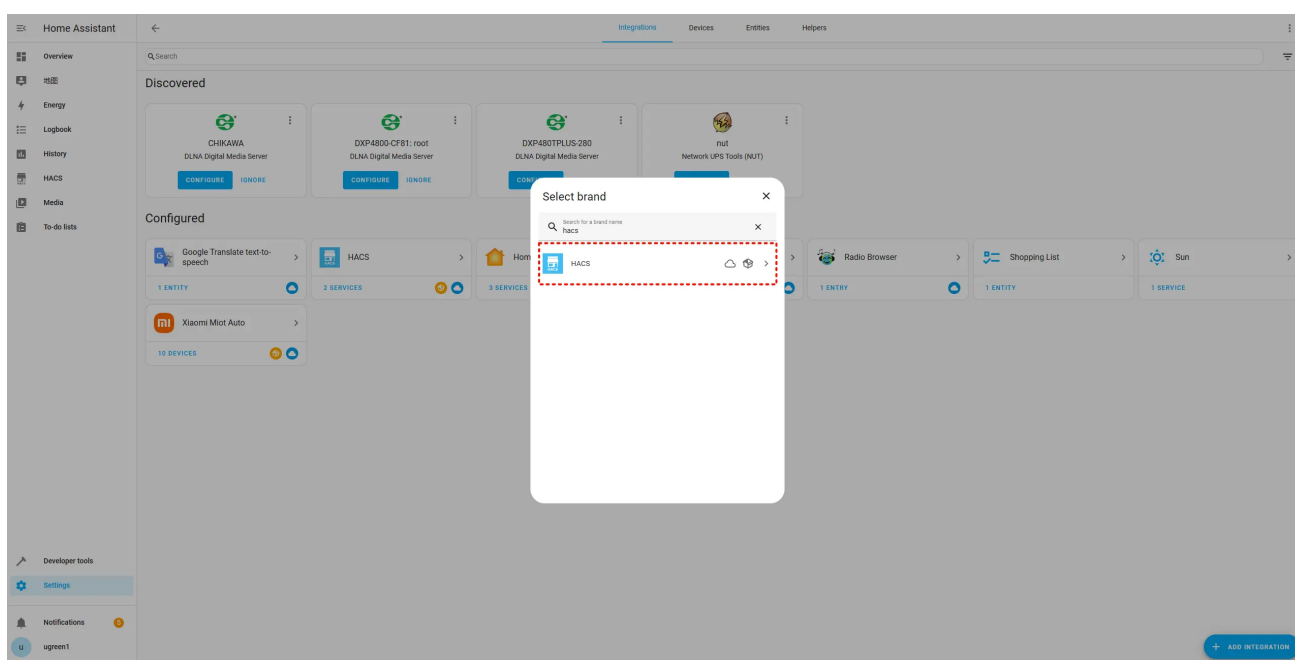
3. After downloading, extract the `hacs.zip` archive and upload the extracted files to the `custom_components/hacs` directory.



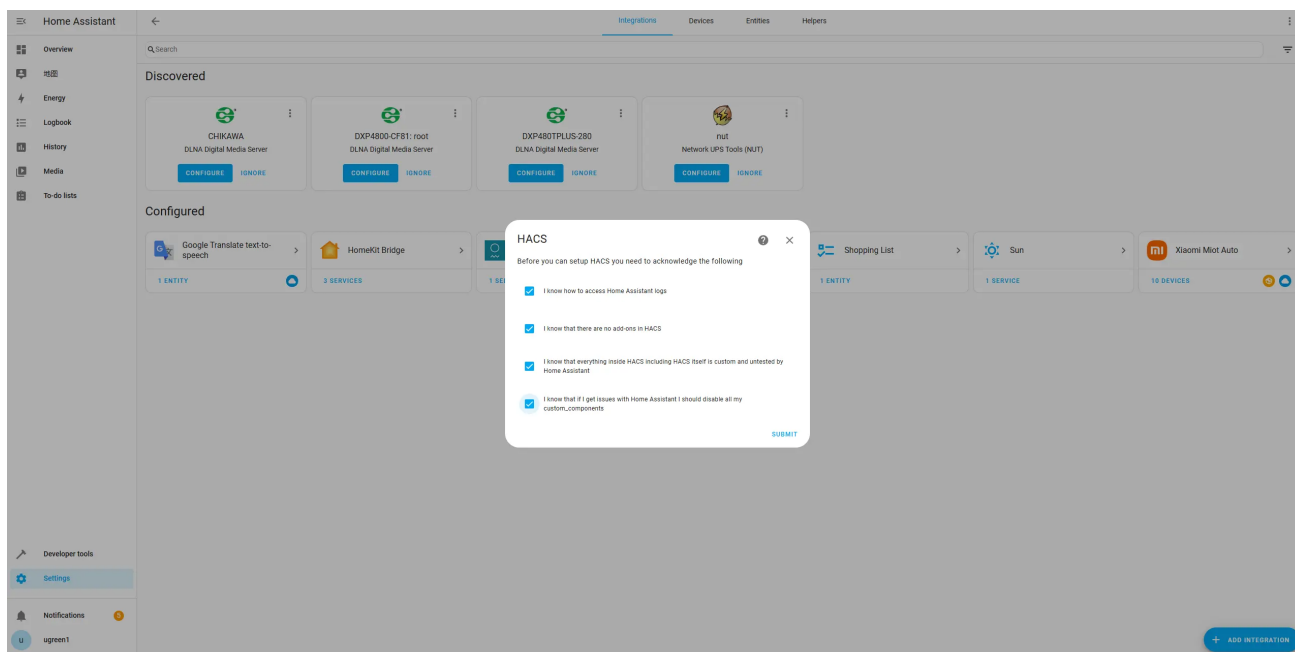
4. Restart the Home Assistant container through the [Docker] application or by using the [Developer Tools] on the Home Assistant page.



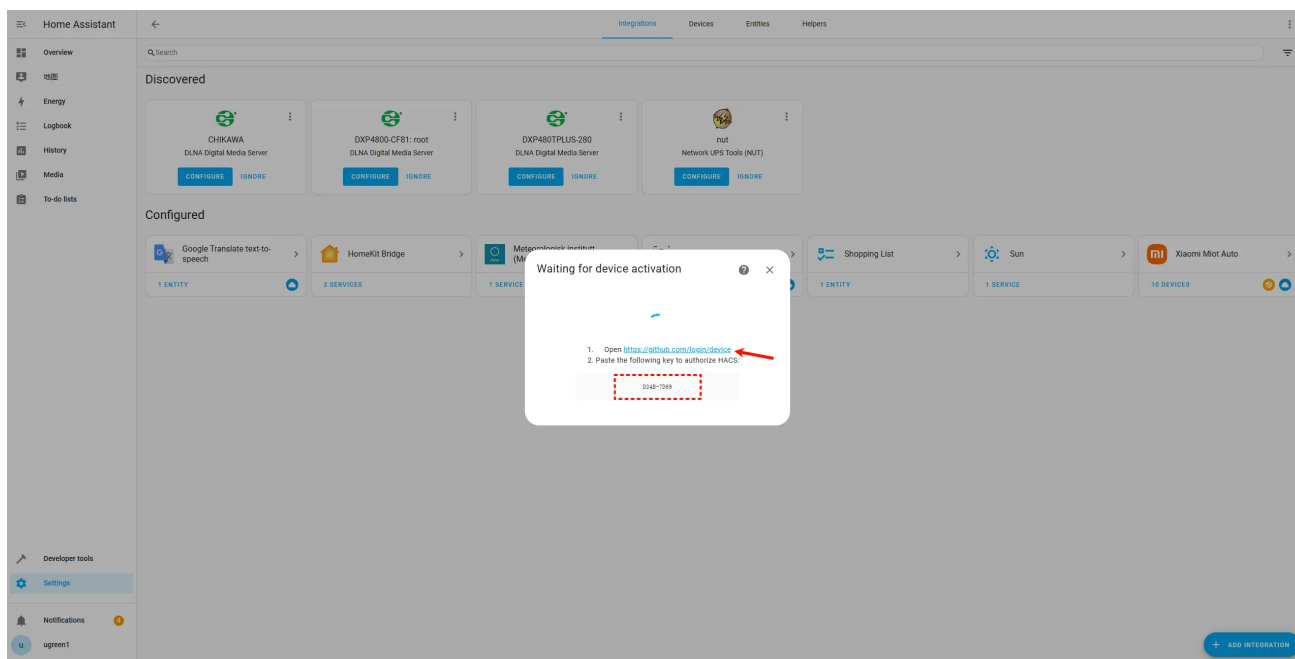
5. After the restart, go to the Home Assistant page, click [Settings > Devices & Services], select "Add Integration", search for and add HACS.



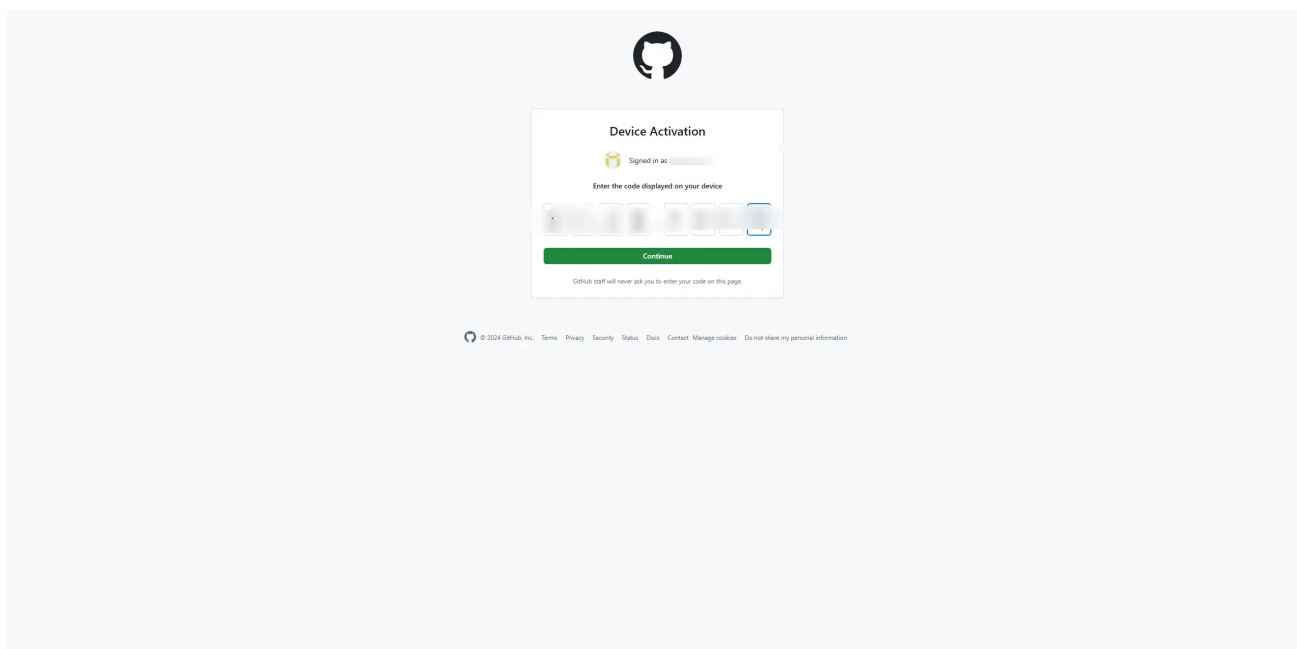
6. Check all the options and click "SUBMIT".



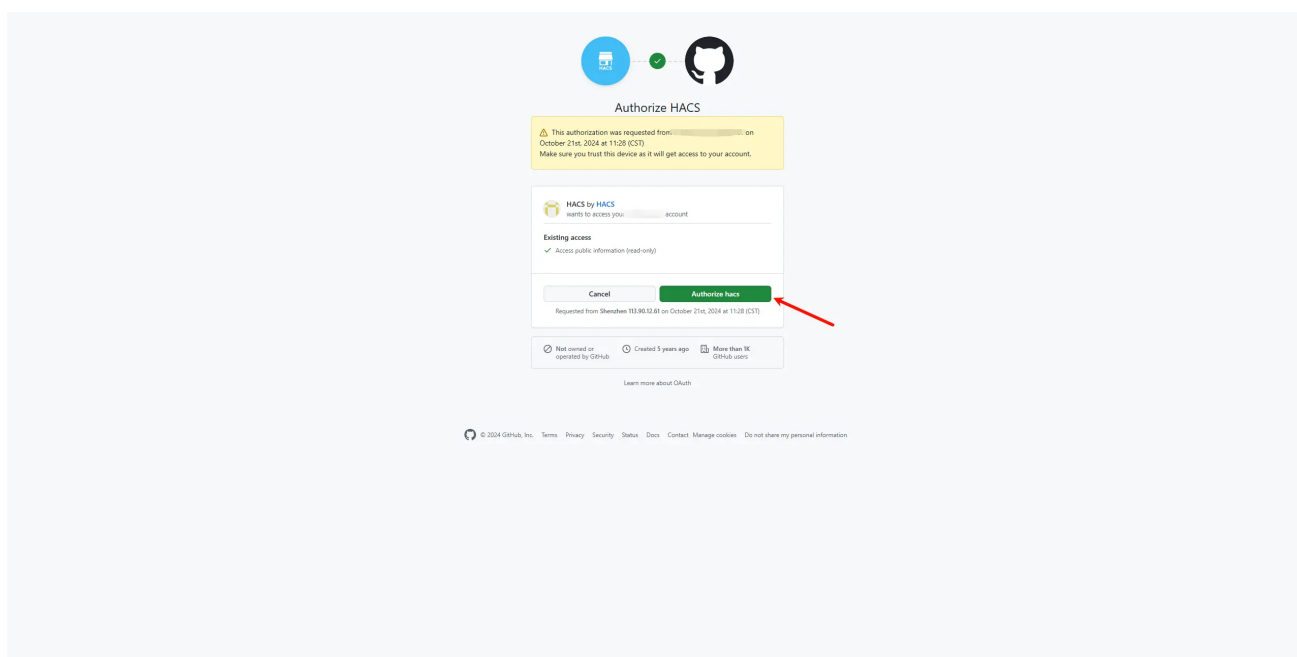
7. Copy the code, then click the GitHub link on the page to proceed with account binding. If you don't have a GitHub account, you can register one yourself and follow the prompts to complete the account binding process.



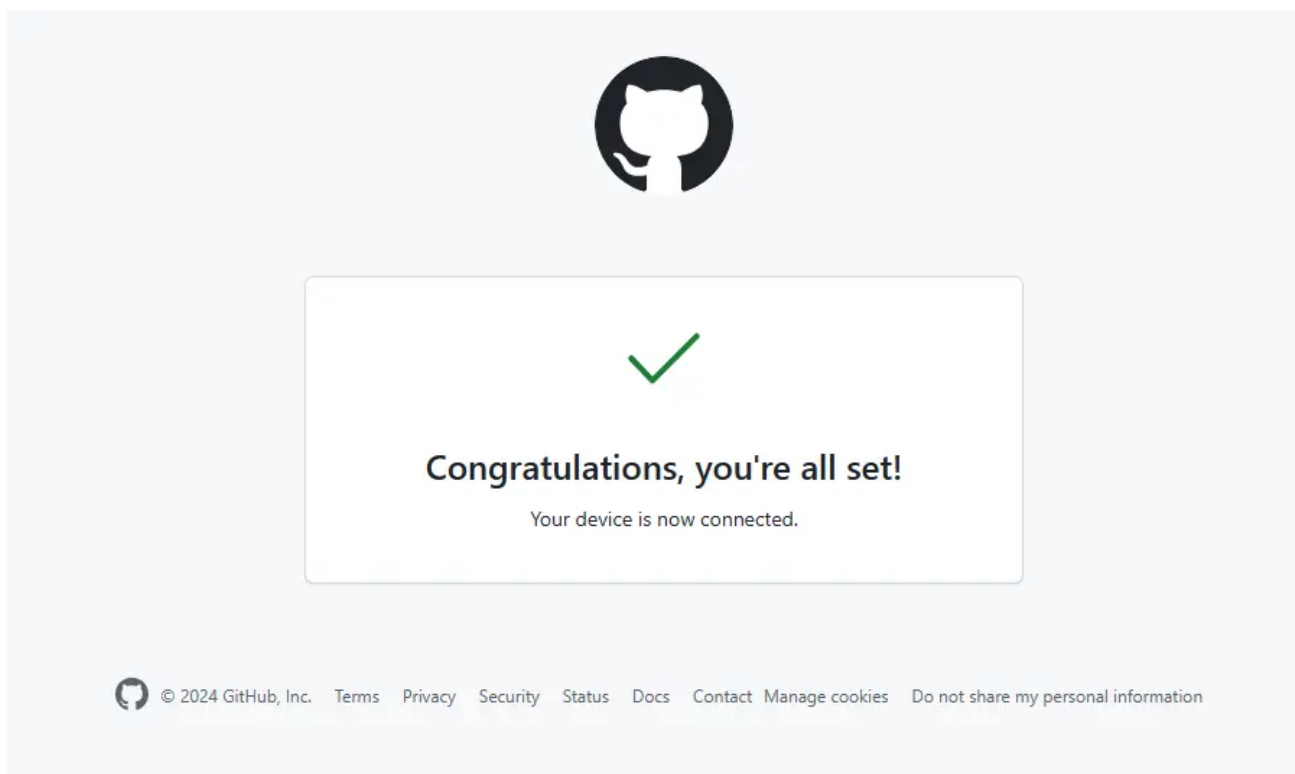
8. After entering the code, click "Continue".



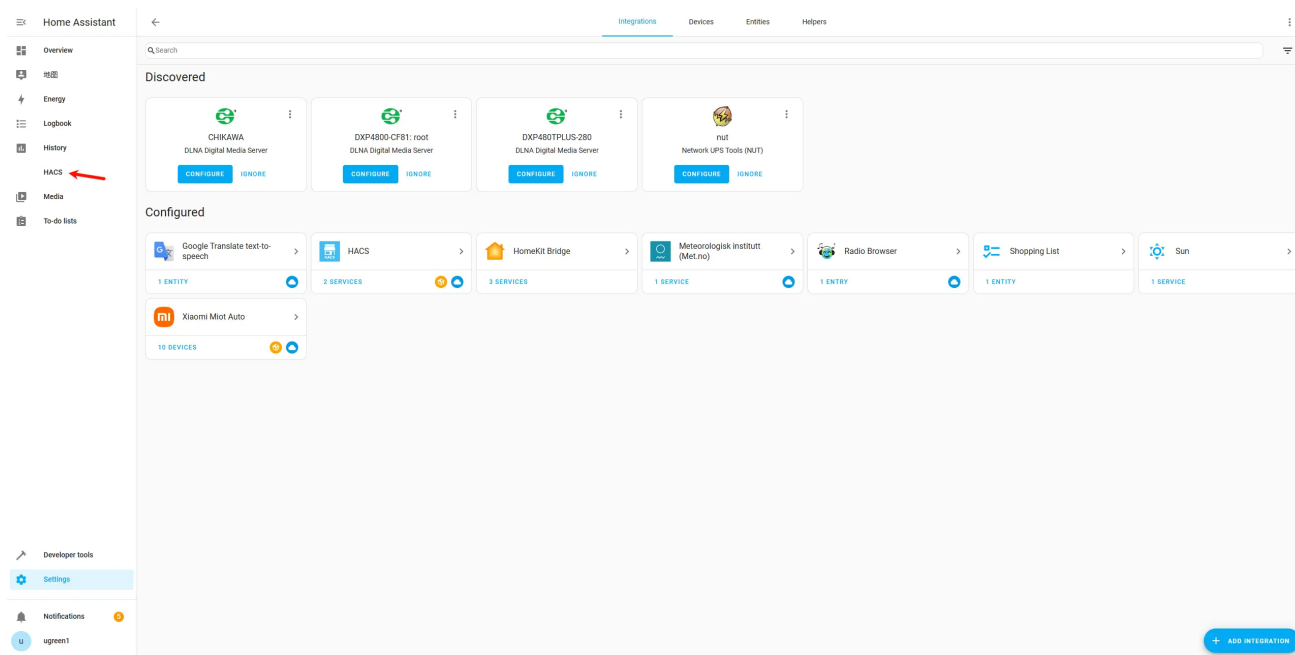
9. Click "Authorize hacs".



10. This screen indicates that the authorization was successful.



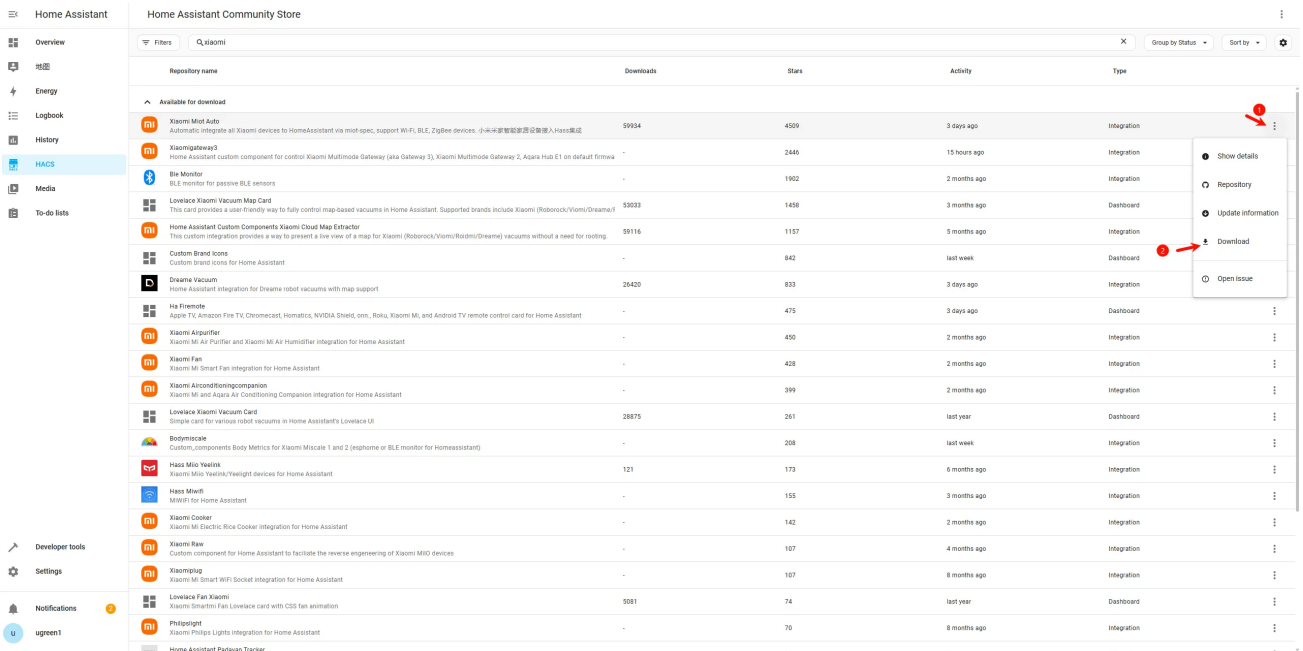
11. After completing the binding, you will see the HACS option in the sidebar of Home Assistant.



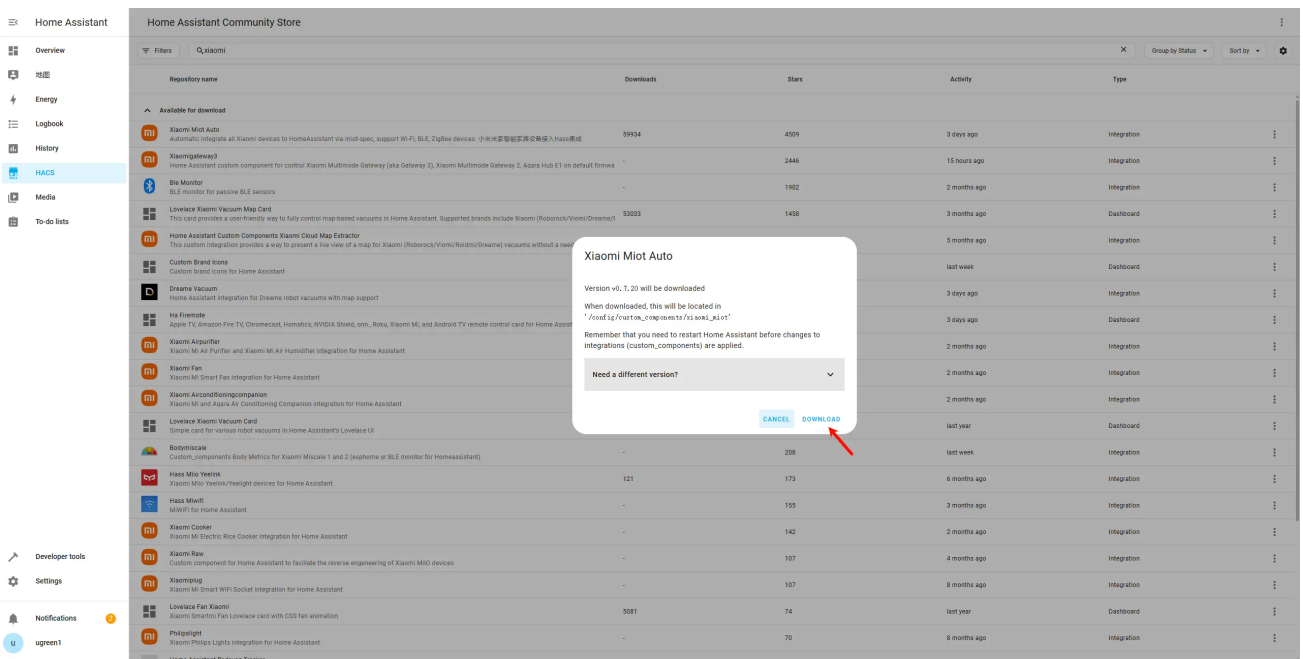
Install the Xiaomi-Miot Plugin

The Xiaomi-Miot plugin allows you to control Xiaomi smart devices through Home Assistant. Below are the steps to install Xiaomi-Miot via HACS:

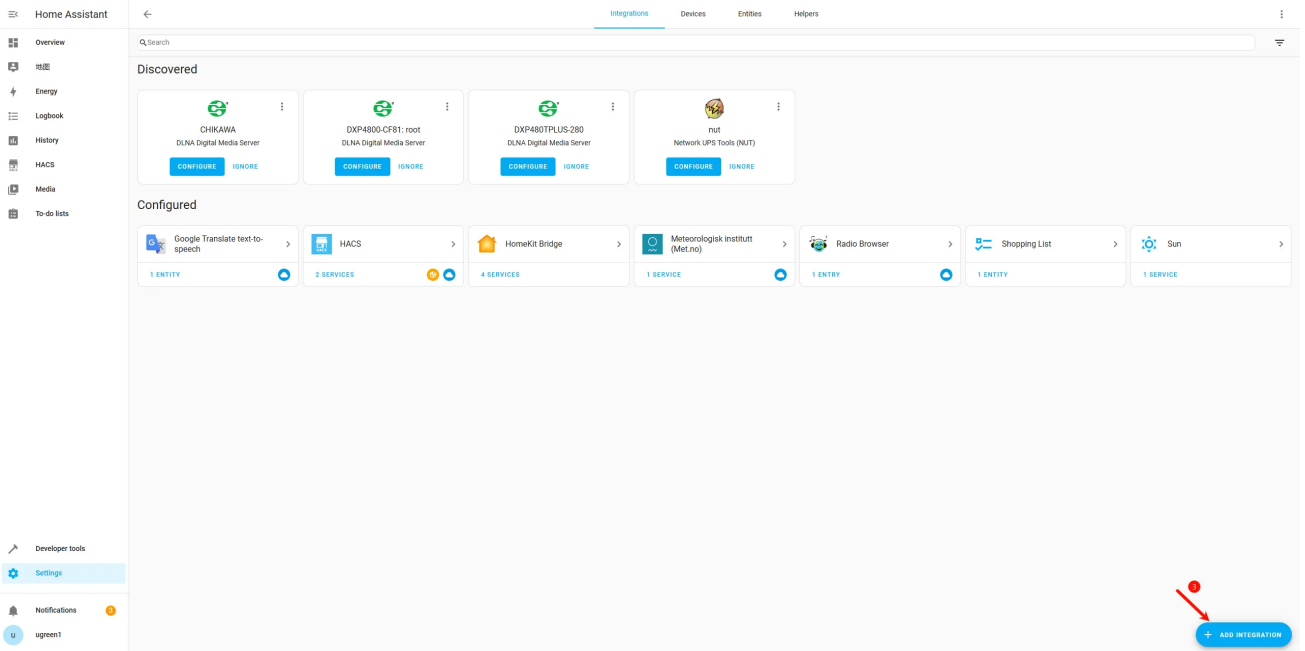
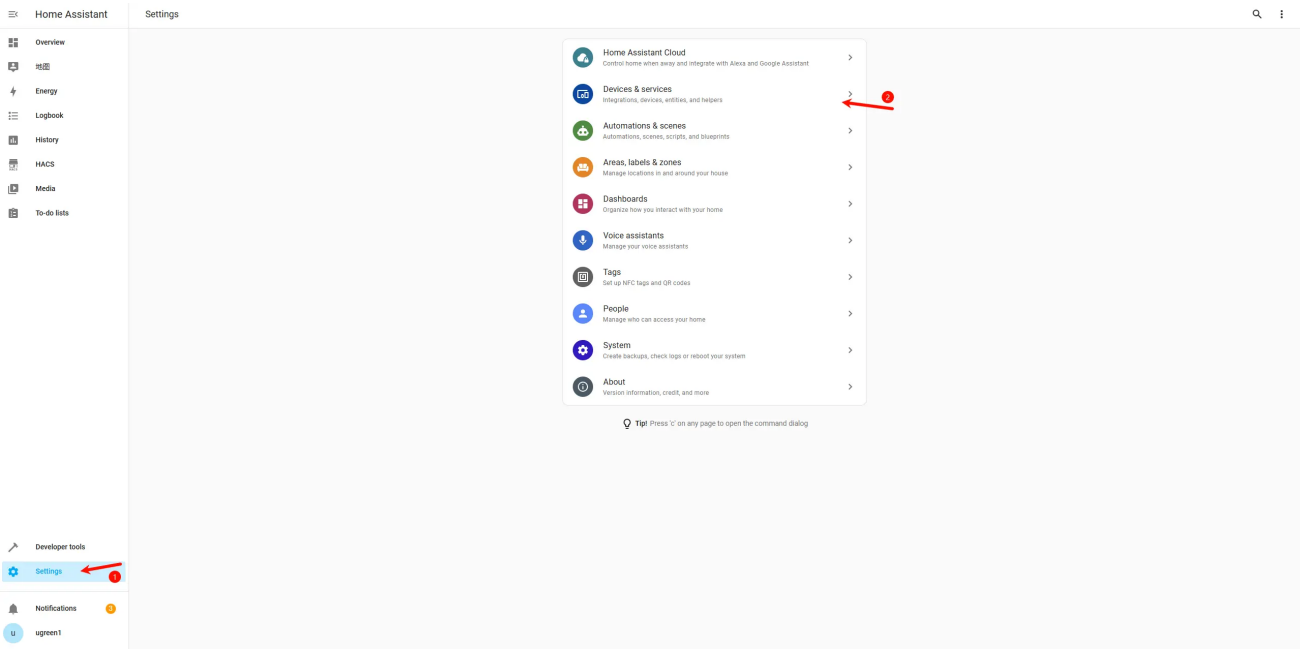
1. Search for "Xiaomi Miot Auto" in the HACS store and download the plugin.

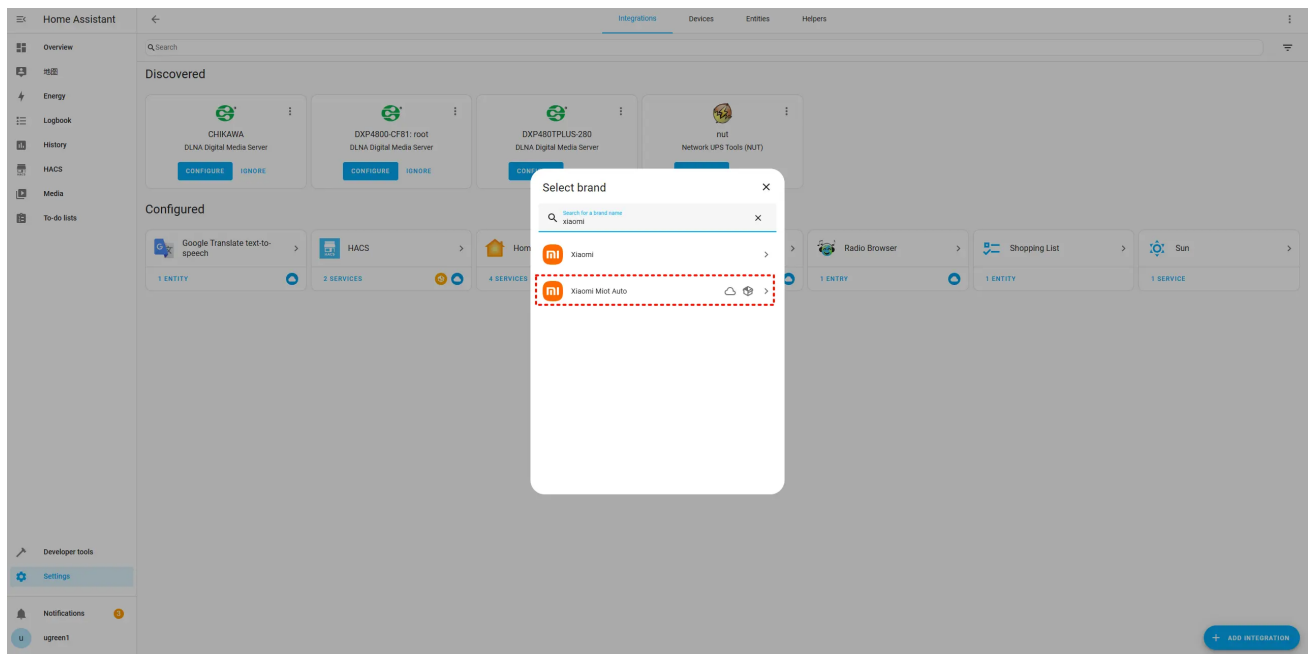


2. Click "Download" to begin the download. After the download is complete, restart the Home Assistant container. You can restart the container from the [Docker] app or by clicking "Restart" in the [Developer Tools] section on the Home Assistant page.

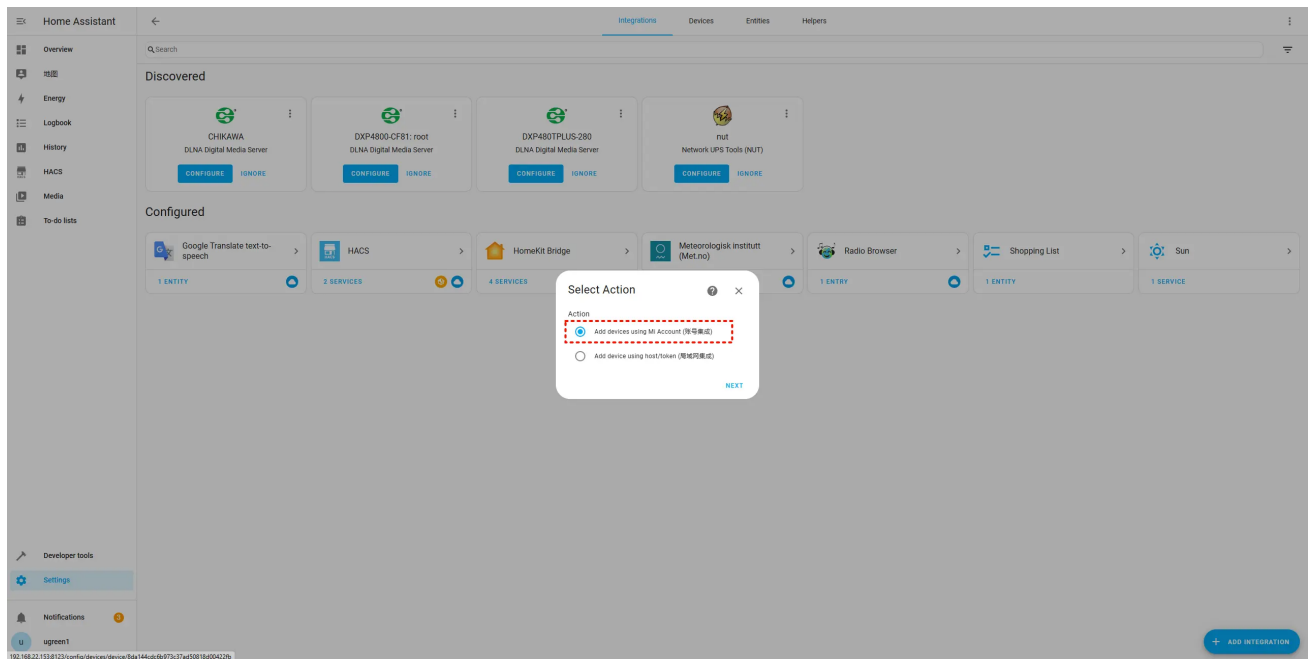


3. After restarting the container, go to [Settings > Devices & Services] in Home Assistant. Click "Add Integration" and search for "xiaomi miot auto." Once found, click the corresponding icon to complete the integration.





4. Select "Add devices using Mi Account" and click "NEXT".



5. Enter your Xiaomi ID and password, select "Automatic", and click "SUBMIT".

Xiaomi Miot Auto

?

×

Config xiaomi cloud account.

Xiaomi Account ID / Email*

Password*

.....

👁

Server location of MiCloud*

中国大陆

▼

Connection mode for device

☒ Automatic (自动模式)

☐ Local (本地模式)

☐ Cloud (云端模式)

☐ Filter devices via model/home/WiFi (Advanced)

SUBMIT

6. Based on your needs, select the devices to include or exclude, and complete the integration setup. Include mode allows you to manually select the devices you want to bind, while Exclude mode lets you manually choose devices you don't want to bind.

Filter cloud devices



You can include or exclude devices to integrate only the devices you want. In the exclude mode, if you do not check any option in the list, it is equivalent to including all options.

Filter Device



Exclude (排除)



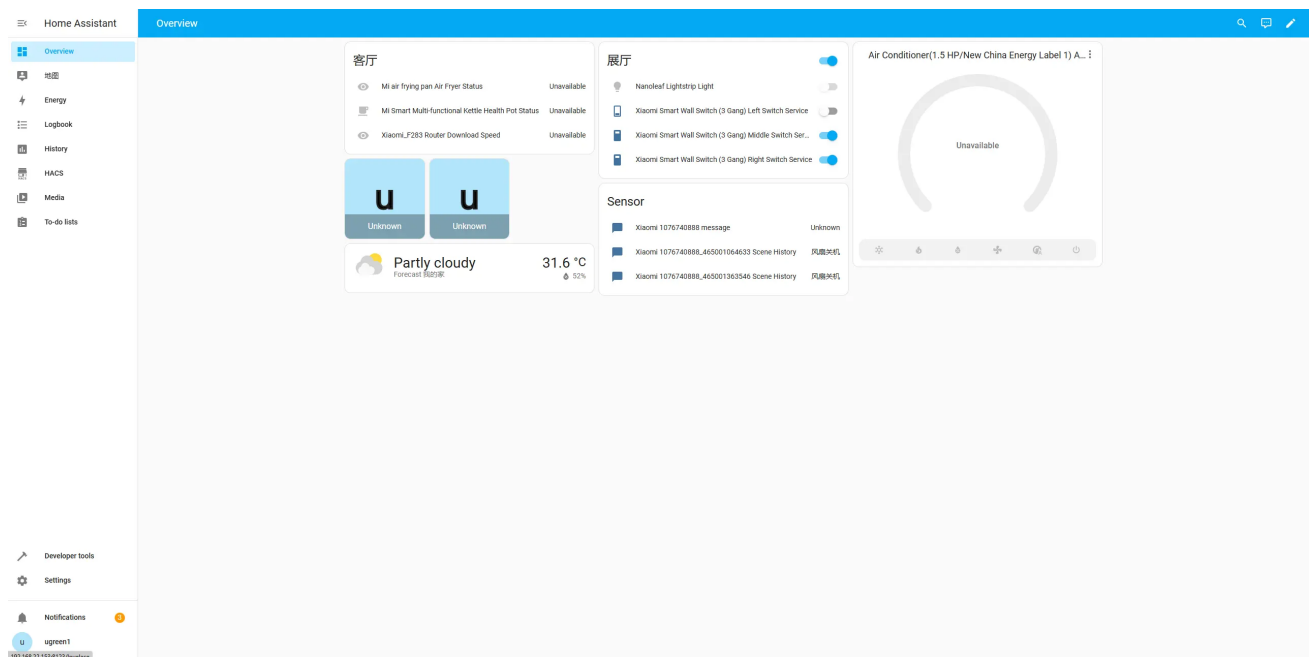
Include (包含)

Device List

Nanoleaf Lightstrip (nnleaf.light.strips), Mi air frying pan (careli.fryer.maf03), Xia...

SUBMIT

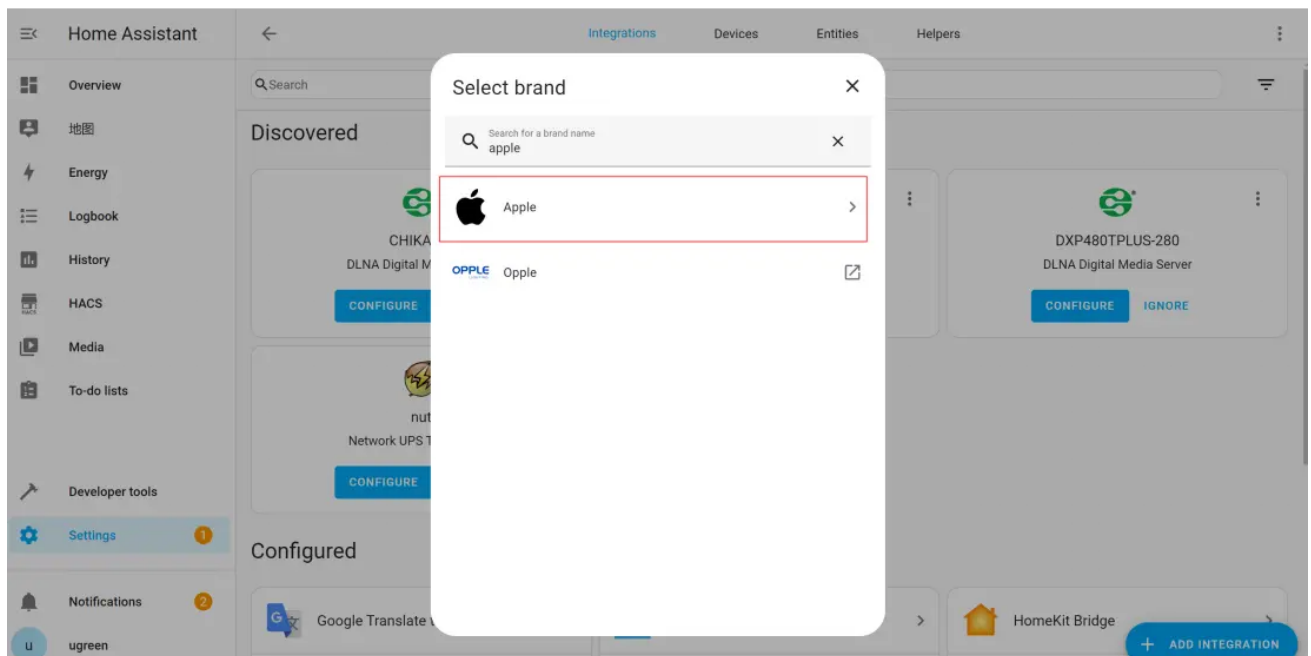
7. After completion, you can view the added devices on the [Overview] page. From here, you can use Home Assistant to control all Xiaomi devices integrated into the system.



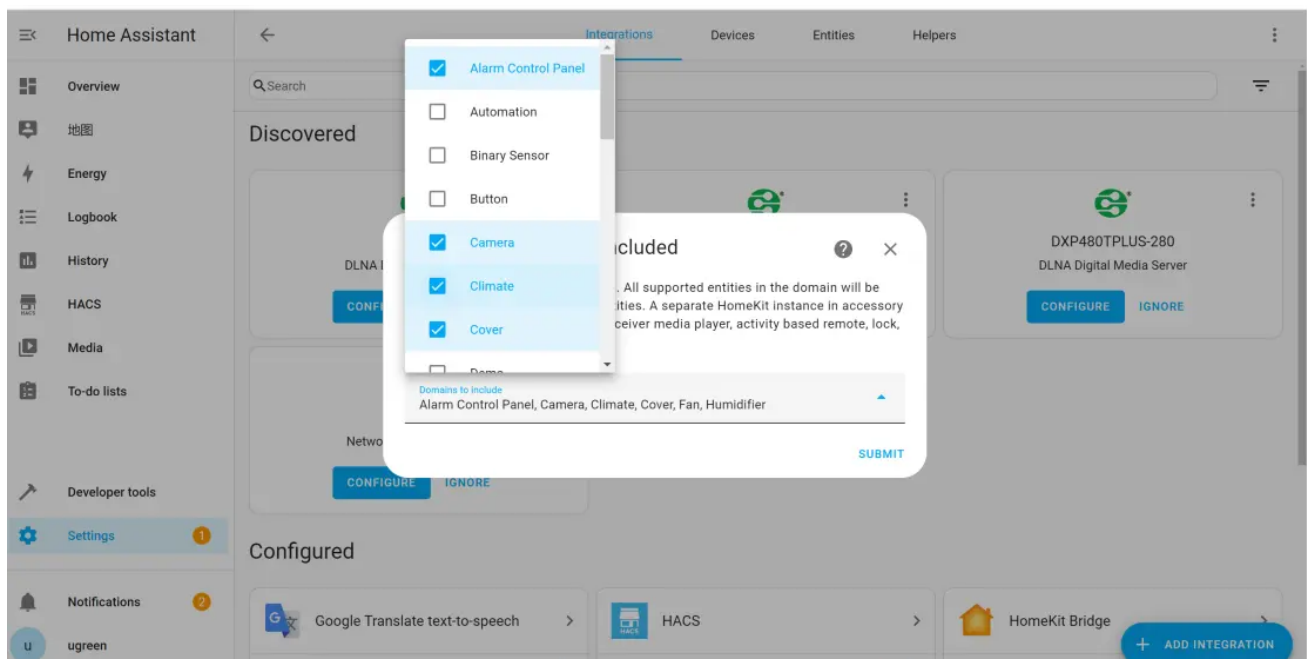
Configure Apple Homekit

If you want to add devices from Home Assistant to the Apple Home app, follow these steps:

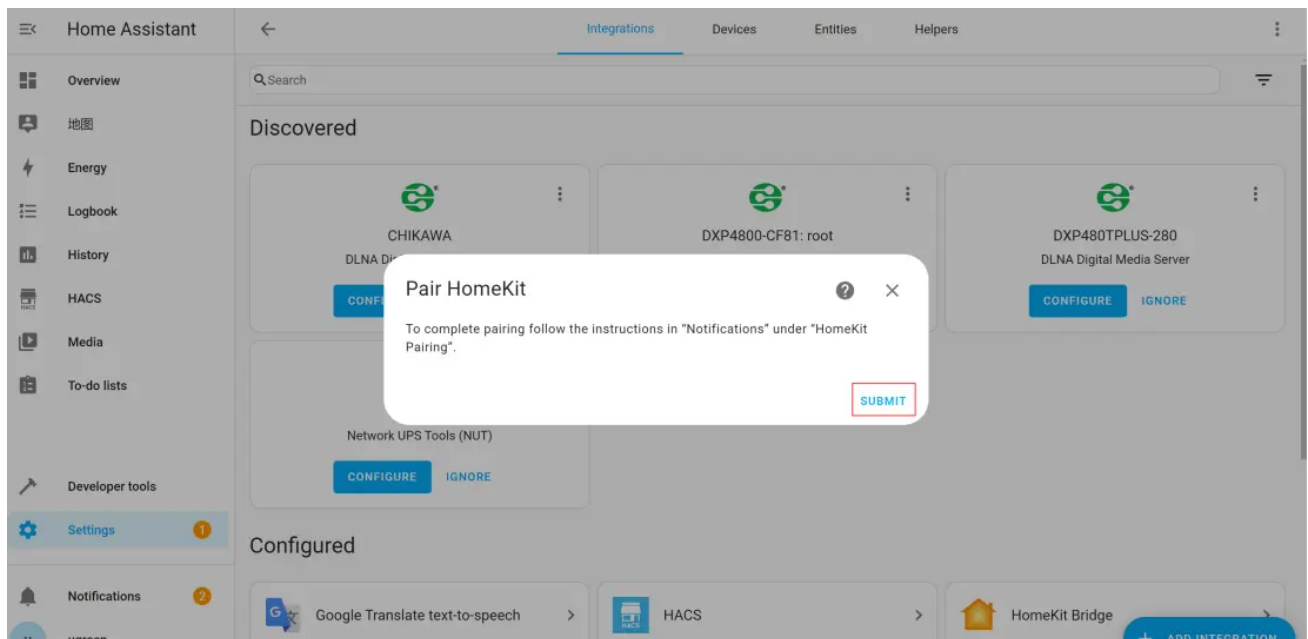
1. In Home Assistant, go to [Settings > Devices & Services], select "Add Integration", search for "apple", and click on the Apple icon to access the submenu.



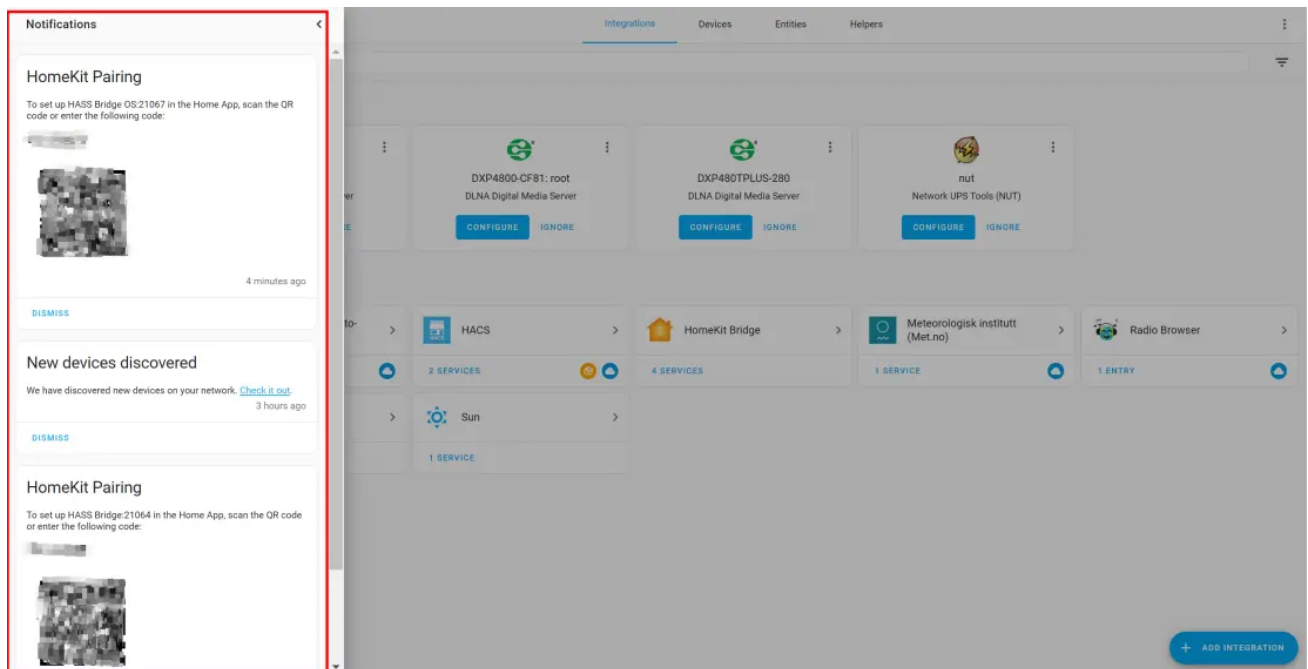
2. Then click "HomeKit Bridge". Based on your needs, select the domains you want to include, which can also be understood as different device types. After selecting, click "SUBMIT".



3. During the "Pair HomeKit" process, follow the guide to click "Submit" > "Finish".



4. Click [Notifications] on the sidebar, scan the QR codes with Apple Home and complete pairing.



Precautions

- **Container Storage Space:** The provided file or folder path configuration is for reference only. You can adjust it based on your needs.
- **Port Configuration:** Ensure that the server port matches the local port. In case of port conflicts, change to an unused port.
- **Local Port Conflicts between Containers:** Port conflicts may prevent containers from starting properly.

- Network Access: Gateway links for quick container access can be established via the bridge mode.
- Image Source Reliability: Use images from official or well-trusted sources, and consult relevant tutorials as needed.
- Third-Party Image Issues: For changes or bug fixes in third-party images, monitor the official announcements for updates.
- Recommended Storage Path: Store the Docker configuration directory on an SSD to avoid performance issues caused by the hard disk failing to enter sleep mode.

Screenshot of Home Assistant

