Synology®

User's Guide for

Synology Router Manager 1.3

Table of Contents

Chapter 1: Introduction 01

Chapter 2: Get started with SRM 02

2.1 Install SRM with Web Assistant

2.2 Install SRM with DS router

2.3 Navigate your SRM desktop

2.4 Sign up for a Synology Account

2.5 Register a QuickConnect ID

Chapter 3: Select an operation mode 08

3.1 Wireless router

3.2 Wireless AP (access point)

Chapter 4: Set up Wi-Fi connections 10

4.1 Manage the primary Wi-Fi network

4.2 Activate the guest Wi-Fi network

4.3 Create custom Wi-Fi networks

4.4 Configure MAC filtering

4.5 Connect to Wi-Fi via WPS

Chapter 5: Build a mesh Wi-Fi network 13

5.1 Add Wi-Fi points

5.2 Manage Wi-Fi points

Chapter 6: Manage client devices 15

6.1 Monitor device status

6.2 Apply traffic control

6.3 Apply Wake on LAN

Chapter 7: Fortify network security 17

7.1 Leverage Security Advisor

7.2 Activate the firewall

7.3 Enforce auto block

7.4 Enable DoS protection

7.5 Access SRM via HTTPS

7.6 Create certificates

7.7 Implement additional security measures

Chapter 8: Update, restore, and reset your SRM 20

8.1 Update SRM and packages

8.2 Back up and restore SRM

8.3 Reset SRM

Chapter 9: Manage Internet connections 22

9.1 Select an Internet connection type

9.2 Configure ISP, VPN client, and IPv6 settings

9.3 Set up Smart WAN

9.4 Set up QuickConnect & DDNS

9.5 Set up DMZ

9.6 Enable port forwarding

9.7 Enable port triggering

Chapter 10: Manage local network connections 26

10.1 Manage local networks

10.2 Create additional local networks

10.3 Manage DHCP services

10.4 Set up static routes

10.5 Set up IPTV & VoIP

Chapter 11: Manage external device and permissions 29

11.1 Manage storage devices

11.2 Define folder permissions

11.3 Manage mobile network dongles

Chapter 12: Configure system settings 31

12.1 Manage hardware settings

12.2 Check system databases
12.3 Modify time and regions
12.4 Customize login styles

Chapter 13: Discover SRM packages 33
13.1 Safe Access
13.2 VPN Plus Server
13.3 Threat Prevention
13.4 DNS Server
13.5 Media Server
13.6 RADIUS Server

Chapter 14: Discover SRM mobile apps 36
14.1 DS router
14.2 VPN Plus
14.3 DS file

Chapter 15: Utilize diagnosis tools 38
15.1 Check connection status
15.2 Set up notifications
15.3 Audit logs in Log Center
15.4 Ping
15.5 Traceroute

Chapter 16: Troubleshooting & FAQ 40

Find your information

Synology publishes a wide range of supporting documentation.

In **Knowledge Center**, you will find useful Help and FAQ articles, as well as video tutorials breaking up processes into handy steps. You can also find User's Guides, Solution Guides, brochures, and White Papers. Experienced users and administrators will find answers and guidance in technical Administrator's Guides and Developer Guides.

Got a problem and unable to find the solution in our official documentation? Search hundreds of answers by users and support staff in **Synology Community** or reach **Synology Support** through the web form, email or telephone.

Chapter 1: Introduction

Synology Router Manager (SRM) is a dedicated web-based operating system for your Synology Router, designed to help you manage and protect your network.

SRM main features and functionalities include:

- **Connectivity management**: Easy-to-use and powerful connectivity management tools ensure smooth operation for your network. Effortlessly configure the Internet, VLAN, dual WAN, and other settings.
- **Smart Wi-Fi & mesh network**: Smart Connect with band steering technology intelligently points your device to the better of the 2.4 GHz and 5 GHz bands, ensuring the best signal and speed. You can efficiently manage multiple Wi-Fi networks from a single web portal.
- **Monitoring of network traffic**: SRM provides detailed information about each application's and device's traffic, allowing administrators to easily discover potential threats or compromised devices using device control and network discovery tools.
- **VLAN configuration**: Use advanced VLAN features to improve network security and flexibility; you can create a network specifically for wired or wireless devices. Isolate devices from other network segments or isolate devices between two networks (e.g., primary network and IoT network).
- **Multiple SSIDs**: Pair Wi-Fi names (SSIDs) with VLANs, set multiple SSIDs (up to 15 for models that support tri-band frequencies), and customize schedules and MAC filters for each SSID.
- **Add-on packages**: Easily expand network management functionalities with VPN Plus Server, Safe Access, Threat Prevention, and others according to your needs.
- **Mobile application DS router**: Do the initial installation of a Synology Router, configure its Internet connection, manage multiple SSIDs, manage device connectivity with Safe Access, remind users of relevant activity that require their attention, and see all contents within a glance in the all-new overview page.

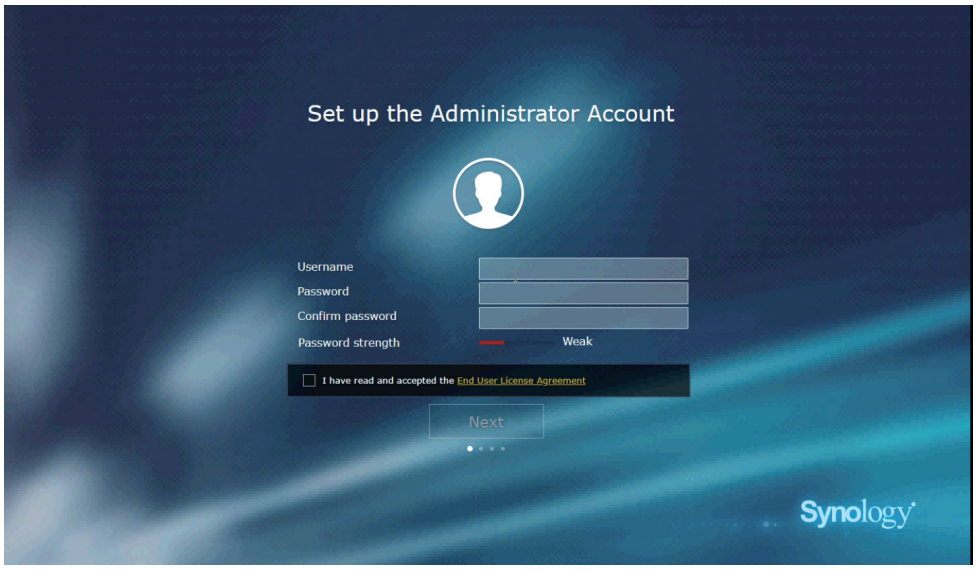
Chapter 2: Get started with SRM

This chapter provides an overview of the initial configurations of Synology Router Manager (SRM). To help you get started with your Synology Router, the following instructions include initial installation and desktop navigation.

2.1 Install SRM with Web Assistant

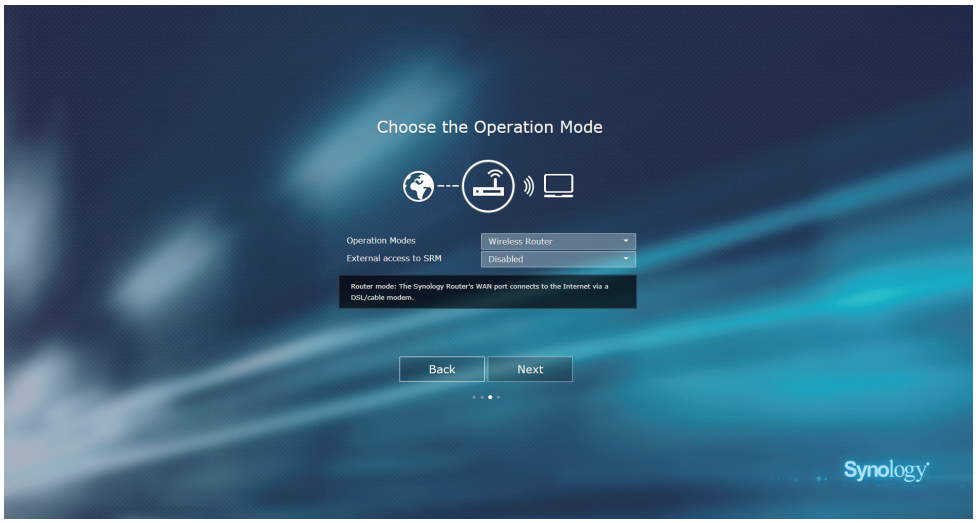
Follow the steps below to install SRM with Web Assistant:

1. Follow the instructions in the Quick Installation Guide included with your Synology Router to install your device.
2. Use a computer or wireless device connected to the Synology Router's local network. If you use a wireless device, join the Wi-Fi network (SSID: SynologyRouter; Password: synology).
3. Open a web browser, and enter either URL into the address bar:
   - **http://router.synology.com**
   - **http://192.168.1.1:8000**
4. Once connected, click **Start** to launch the SRM Setup Wizard.
5. Fill in the information to set up the administrator account. Click **Next** to continue.



6. Fill in the information to set up the Wi-Fi network. Click **Next** to continue.

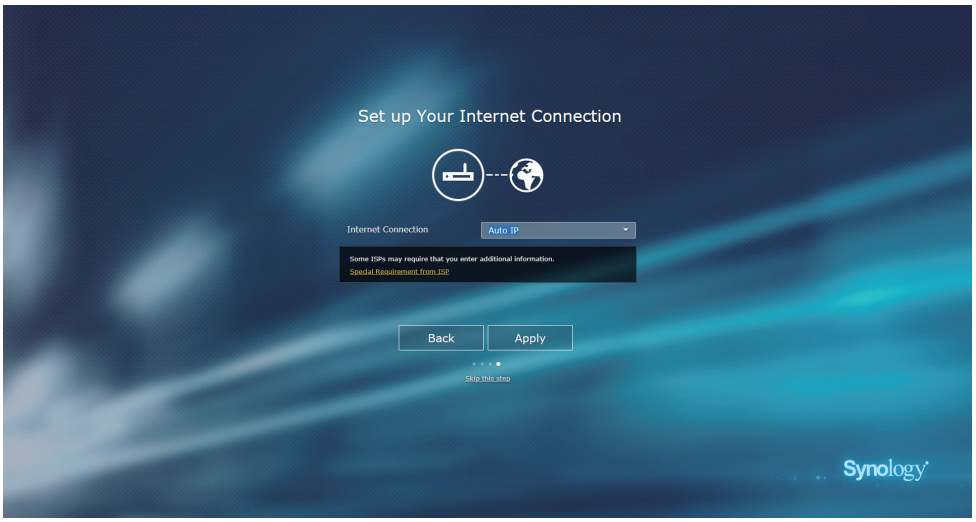
7. Set up the operation mode.



Notes:

- If **Wireless Router** mode is chosen, you can also enable **External access to SRM**. This option restricts external access to SRM via the HTTP(S) port (e.g., 8000/8001).
- For more information about operation modes, please refer to **chapter 3**.

8. Choose an Internet connection type:
   - **PPPoE:** Choose this option if your ISP has provided you with PPPoE credentials.
   - **Manual IP**: Choose this option if you have an available IP address for use.
   - **Auto IP**: Choose this option if you rely on an ISP modem for automatic IP assignment.
   - **DS-Lite**: Choose this option if your ISP has provided you with a DS-Lite service request.



9. The wizard will continue to set up your SRM, and it may take up to three minutes to complete the setup.
10. After the setup is complete, click **Start managing now** to enjoy SRM and its various features.

2.2 Install SRM with DS router

Synology's mobile application DS router allows you to quickly set up and manage your Synology Router. Follow the steps below to install SRM with DS router.

1. Follow the instructions in the Quick Installation Guide included with your Synology Router to install SRM.
2. Download and install DS router on your wireless device.

Download on the App Store

GET IT ON Google Play

3. On your wireless device, join the Wi-Fi network (SSID: SynologyRouter; Password: synology).
4. Follow the instructions in the Quick Installation Guide included with your Synology Router to install the device.

2.3 Navigate your SRM desktop

Sign in to SRM

Follow the steps below to sign in via a web browser:

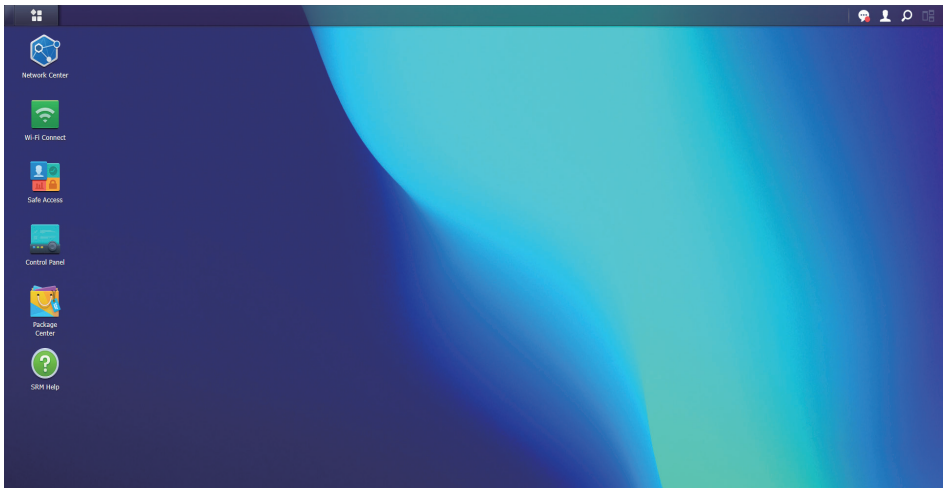
1. Make sure that your computer and Synology Router are connected to the same local network or the Internet.
2. Open a browser on your computer and enter one of the following in the address bar:
   - **Over the local network**: When your device and the Synology Router are connected to the same local network, type one of the following:

Address	Example
Private IP address of Synology Router:8000	192.168.1.1:8000
router.synology.com	

   - **Over the Internet**: When your device and the Synology Router are connected to the Internet, type one of the following:

Address	Example
Private IP address of Synology Router:8000	66.249.7x.1xx:8000
QuickConnect address	quickconnect.to/your QuickConnect ID
DDNS address	yourSynoRouter.synology.me

3. Enter your username and password and click **Sign in**.



Notes:

- The SRM desktop is customizable; please refer to **this article** for more information.

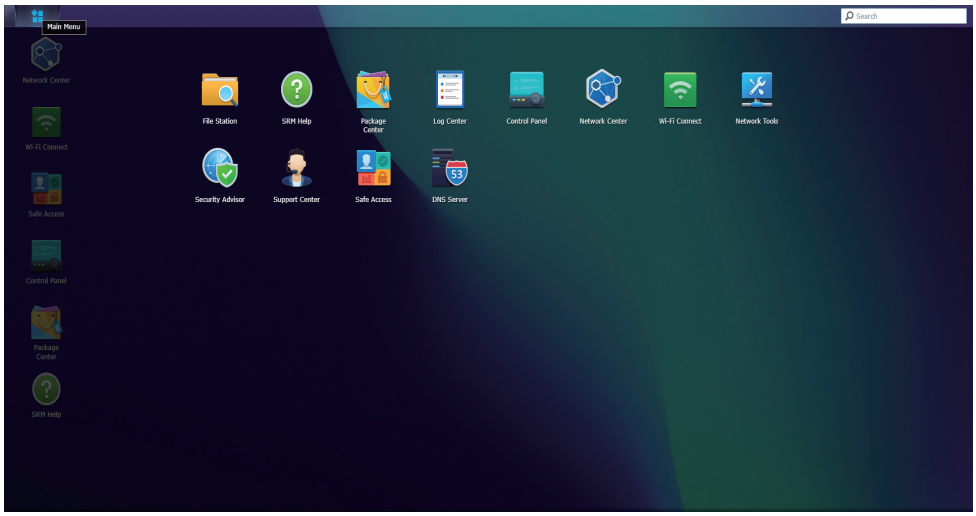
Visit the taskbar

The taskbar is located at the top of the screen and includes the following items:

1. **Show Desktop**: Minimizes all open applications and package windows.
2. **Main Menu**: Views and opens applications and packages installed on your Synology Router. You can also click and drag to create desktop shortcuts.
3. **Open Applications**: Displays currently open applications and packages. You can right-click and pin packages to the taskbar for faster access in the future.
4. **Upload Queue**: Appears when you start uploading files to your Synology Router. Click on the icon to see more details, like progress and upload speed.
5. **Notifications**: Displays notifications, like errors, status updates, and package installation notifications.
6. **Options**: Allows you to modify your personal account options, restart, or sign out of your Synology Router.
7. **Search**: Quickly finds specific applications, packages, or SRM Help articles here.
8. **Pilot View**: Offers a preview of all open application and package windows.

Visit the main menu

You will find a list of applications and packages installed on your Synology Router here.



Notes:

- You can create desktop shortcuts for your own convenience; please refer to **this article** for more information.

Restart, and signing out

Click the **Options** menu (the person icon on the upper right) to restart or sign out of your Synology Router.

2.4 Sign up for a Synology Account

Synology Account is an all-in-one web platform for Synology's online services. With a Synology Account, you can register a QuickConnect ID for your Synology Router, which helps you to securely configure and manage your Synology Router from anywhere, anytime. Other Synology services such as Synology's support services, the latest product updates, software license management and your purchase history of Synology products are also available.

To register/access your Synology Account, go to **Control Panel** > **System** > **Synology Account**, or go to Synology Account's **official website**.

2.5 Register a QuickConnect ID

QuickConnect allows you to connect to your Synology Router via the Internet without creating port forwarding rules. Simply enter your QuickConnect ID in Synology client applications (e.g., DS router) or visit "quickconnect.to/***your QuickConnect ID***" in any browser to access your Synology Router.

Activate the service at any time by following the steps below:

1. Go to **Network Center** > **Internet** > **QuickConnect & DDNS**.
2. Check **Enable QuickConnect**.
3. If you are not signed in to your Synology Account, a login window will pop up. Enter your existing Synology Account information or create a new account in the window.
4. Specify a new QuickConnect ID.
5. Click **Apply**.

Notes:

- A custom QuickConnect ID can only include English letters, numbers, and dashes (-). It must start with a letter and cannot end with a dash.
- For more information on QuickConnect, please refer to **this article**.

Chapter 3: Select an operation mode

This chapter introduces the wireless operation modes available to your Synology Router to suit your networking needs. Operation modes can be found by going to **Network Center** > **Operation Modes**.

3.1 Wireless router

The **wireless router** mode is the default operation mode. Your Synology Router in this mode transfers data from one network to another (e.g., your local network and the Internet) and finds optimized paths using a routing table.

With this mode, you can also ensure that all data are forwarded through NAT (Network Address Translation). For example, if a packet traverses outside the local network, your Synology Router translates the private IP address of its source (e.g., 192.168.1.1) into a public IP address.

This mode is recommended under the following circumstances:

- Your local network requires extra security, e.g., firewall, NAT, and DMZ.
- You need to create several subnets within a local network.

Notes:

- To use the **wireless router** mode, make sure your Synology Router is connected through one of the following methods:
  - **With an ISP modem**: Connect the WAN port of your Synology Router to the LAN port of an ISP (Internet Service Provider) modem with an Ethernet cable.
  - **Without an ISP modem**: Connect the WAN port of your Synology Router to the Internet port on the wall/ground with an Ethernet cable.
- NAT is enabled by default in the wireless router mode.

3.2 Wireless AP (access point)

The **wireless AP** mode (also called the bridge mode) turns your Synology Router into a network switch and extends Wi-Fi coverage. In this mode, your Synology Router provides wired/wireless access but cannot select routes for data transmission. Assigning IP addresses to clients in the local network is not available either.

This mode is recommended under the following circumstances:

- Your Synology Router is already connected to an ISP modem or router for Internet access with an Ethernet cable.

Notes:

- There are several limitations on the **wireless AP** mode:
  - Features at the **Port Forwarding** and **Traffic Control** tabs in **Network Center** are not available.
  - DHCP for the local network is disabled, but your Synology Router can still assign IP addresses to clients in the guest network.
  - To ensure that SRM packages (e.g., Safe Access) can function properly, make sure the Ethernet cable connected to the parent router is plugged into the WAN port of your Synology Router.

Chapter 4: Set up Wi-Fi connections

This chapter introduces how to set up and manage Wi-Fi networks, define MAC filters, and configure WPS options in Wi-Fi Connect.

4.1 Manage the primary Wi-Fi network

By default, a Wi-Fi name (SSID) will be created for you as part of the primary local network.

The following additional options are available to configure at **Wi-Fi Connect** > **Wi-Fi Settings** > **Wi-Fi Network** > **Primary Network (System default)**, then selecting **Edit**:

- **Enable Smart Connect**: Smart Connect is a combination of 2.4 GHz and 5 GHz bands. This feature automatically steers connected devices towards the band that gives them the strongest speed and signal.
- **Configure security settings**: Settings such as the password and security level can be configured here.
- **Apply MAC filter**: Control whether specific MAC addresses (or devices) have access to the wireless network.
- **Configure a schedule**: Set days and times that your Wi-Fi network turns off automatically.

For more information about managing your primary Wi-Fi network, please refer to **this article**.

4.2 Activate the guest Wi-Fi network

A guest Wi-Fi network is typically a time-limited network created by businesses for visitors/ non-regular users. To prevent unauthorized access to the host network, guests can only connect to the guest network and not the host one.

By default, a deactivated guest Wi-Fi network will be created for you. The guest Wi-Fi network can be activated at **Wi-Fi Connect** > **Wi-Fi Settings** > **Wi-Fi Network** > **Guest Network (System default)**.

In addition to the options available in the primary Wi-Fi network, the following additional options are available for configuration:

- **Configure guest portal**: Customize a web page where you can display a welcome message with various types of information which the user must interact with before being granted access to the network.
- **Configure client isolation**: This is a security feature that prevents wireless clients from communicating with one another.
- **Configure a schedule**: Set days and times that your Wi-Fi network turns off automatically. You can also specify a period after which the guest network will be disabled.

4.3 Create custom Wi-Fi networks

You can quickly create a custom Wi-Fi network by clicking **Create** at **Wi-Fi Connect** > **Wi-Fi Settings** > **Wi-Fi Network**. You can join an existing local network, or a local network with the same name will be created.

The following additional options are available for configuration:

- **Enable Smart Connect**: Smart Connect is a combination of 2.4 GHz and 5 GHz bands. This feature automatically steers connected devices towards the band that gives them the strongest speed and signal.
- **Configure security settings**: Settings such as the password and security level can be configured here.
- **Apply a MAC filter**: Control whether specific MAC addresses (or devices) have access to the wireless network.
- **Configure a schedule**: Set days and times that your Wi-Fi network turns off automatically.

Notes:

- At **Wi-Fi Connect** > **Wi-Fi Settings** > **Radio**, you can edit the radio settings that apply to all your Wi-Fi networks as well as configure wireless uplink.
- Further settings such as VLAN tagging and network isolation can be configured in **Network Center**.
- You can also create custom Wi-Fi networks using the mobile app **DS router**.

For more information about managing custom Wi-Fi networks, please refer to **this article**.

4.4 Configure MAC filtering

MAC address filtering allows you to block traffic from known machines or devices or only allow known devices to connect. The MAC address of a computer or device is used by your Synology Router to identify it and to block or allow access.

By default, the system block list will be created for you using MAC addresses containing devices blocked automatically by broadcast storm prevention. It will prevent devices from sending a large number of broadcast packets in a short time (and consequently affect the normal operation of other devices). This list applies to all Wi-Fi names (SSIDs) and takes precedence over all custom MAC filters.

To edit devices on the system block list or to enable broadcast storm prevention, go to **Wi-Fi Connect** > **Wi-Fi Settings** > **MAC Filter** > **System Block List**.

Additional filters can also be created, generally for organizational or administrative purposes. For example, in complex networks with multiple gateways and Wi-Fi points, you can use MAC filters to limit user access to specific networks.

To create custom MAC filters, go to **Wi-Fi Connect** > **Wi-Fi Settings** > **MAC Filter** and click **Create**.

For more information about configuring MAC filtering, please refer to **this article**.

4.5 Connect to Wi-Fi via WPS

WPS (Wi-Fi Protected Setup) is a wireless security standard that allows you to easily connect devices to a wireless network.

To enable WPS, go to **Wi-Fi Connect** > **Wi-Fi Settings** > **WPS** and tick **Enable WPS**.

There are two WPS methods in which users can connect to a wireless network hosted by your Synology Router:

- **Push button**: Press the **WPS** button located on your Synology Router or click the WPS button at **WPS** > **By push button**.
- **PIN code**: Enter an AP PIN code on the client device or enter the client PIN code.

For more information about connecting to Wi-Fi via WPS, please refer to **this article**.

Notes:

- Adding additional Wi-Fi points using WPS is not supported.

Chapter 5: Build a mesh Wi-Fi network

This chapter introduces various features to manage Wi-Fi points and build a mesh Wi-Fi system.

5.1 Add Wi-Fi points

This section shows how to add Wi-Fi points to deploy a mesh Wi-Fi system. For more detailed instructions, please refer to **this article**.

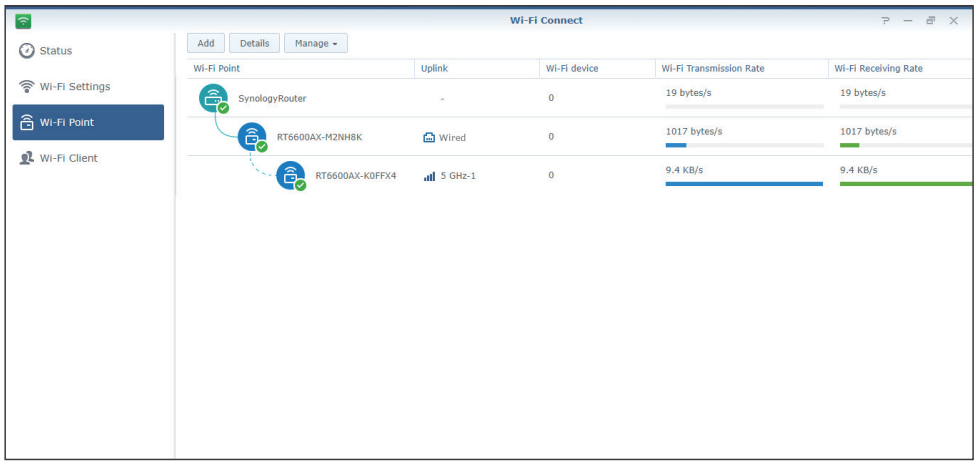
1. On your primary router, go to **Wi-Fi Connect** > **Wi-Fi Point**.
2. Click **Add**.
3. Follow the on-screen instructions to place your additional Wi-Fi points, power them on, and wait until their LED indicators start blinking.
4. The wizard will start scanning available Wi-Fi points. When the scan is complete, name the Wi-Fi points and click **Next**. The Wi-Fi points will be added to your mesh Wi-Fi system in a few minutes.

Notes:

- For a specific model's LED behavior, please refer to its **hardware installation guide**.
- Wi-Fi points might fail to connect to the primary router if the primary router is reset to default. To rebuild your mesh Wi-Fi system, reset all Wi-Fi points and follow the instructions provided by the Mesh Wi-Fi System Setup Wizard.
- For more information about mesh Wi-Fi systems, please refer to **this article**.

5.2 Manage Wi-Fi points

At **Wi-Fi Connect** > **Wi-Fi Point**, you can add new Wi-Fi points, manage existing Wi-Fi points, and view the current status of your Wi-Fi system by topology. All your devices and their connection types are listed on this page — a solid line means the Wi-Fi point is connected by an Ethernet cable, and a dotted line means it is connected via Wi-Fi.



- **Details**: Name your Wi-Fi points for easy recognition. You can find the general information, network status, and the connected list from the pop-up window.
- **Manage**: Change the status of all Wi-Fi points.
  - **Turn off LED**: Turn off the LED indicator of the selected Wi-Fi point.
  - **Blink to find**: Use the blinking LED indicator of the selected Wi-Fi point to assist you in finding its location.
  - **Restart now**: Restart the selected Wi-Fi point immediately.
  - **Delete & Reset**: Remove the selected Wi-Fi point from the mesh Wi-Fi system, and reset to factory default.

For more information about configuring Wi-Fi points, please refer to **this article**.

Chapter 6: Manage client devices

This chapter introduces various features to manage client devices.

6.1 Monitor device status

Go to **Network Center** > **Status** to monitor the wired/wireless network status of Synology Router and its network, CPU, and memory usage in real-time. You can also monitor the devices connected to your Synology Router and their specific network usage.

For more information about monitoring the devices connected to your Synology Router and their specific network usage, please refer to **this article**.

6.2 Apply traffic control

Traffic control manages the upload and download of Internet traffic running on your Synology Router networks. An overview of current traffic control rules and QoS (Quality of Service) settings applied to devices can be seen at **Network Center** > **Traffic Control** > **General**.

Manage bandwidth

You can quickly apply traffic control rules to connected devices at **Network Center** > **Traffic Control** > **General** (refer to **this article** for more information).

Configure the following:

- **Ban**: Blocks the transmission between a device and your Synology Router. Banned devices will still be able to access other devices within the same local area network while access to the Internet or the SRM is paused until you sign in to SRM using another device and cancel the ban.
- **High/low priority**: Defines which devices should be given higher or lower priority when sending or receiving data between local networks and the Internet. You can at most designate three devices with higher priority and three with lower priority.
- **Guaranteed Bandwidth**: Defines the outgoing traffic guaranteed to be served to a device or application when the whole system bandwidth is sufficient.

- **Maximum Bandwidth**: Defines the maximum outgoing traffic a device or application can utilize when the whole system bandwidth is sufficient, and there is System Remaining Bandwidth.

At **Network Center > Traffic Control > Advanced**, you can apply more defined traffic control rules to additional devices based on their MAC addresses, as well as set the bandwidth allowed for applications running on each device (refer to **this article** for more information).

Traffic control formula:

- We suggest calculating **System Output Bandwidth** first. Then, make sure the sum of **Guaranteed Bandwidth** for every device and application is not greater than **System Output Bandwidth**, or the setting may not work properly.
  - Total **Guaranteed Bandwidth** of all devices and applications + **System Remaining Bandwidth** ≤ **System Output Bandwidth**
  - **Guaranteed Bandwidth** for each device or application ≤ **Maximum Bandwidth** for each device or application

Monitor network usage

You can monitor the network usage history by device and by application. To access the usage log, go to **Network Center** > **Traffic Control** > **Monitor**. You can identify the source of usage anomalies, such as malicious software/websites, or identify users that misuse network resources.

At **Network Center** > **Traffic Control** > **Report**, you can create a report task to generate a reader-friendly traffic report. This report will give you an overview of your Synology Router's network traffic statistics over a certain period of time. You can also set up schedules and email notifications for traffic reports.

6.3 Apply Wake on LAN

With Wake on LAN (WOL), you can remotely wake up wired devices from shutdown. The devices joined to the WOL service can be woken up via the MAC addresses or the connection list.

If you have a Synology NAS (e.g., DiskStation or RackStation) joined to a Synology Router's local network, you can simply wake it up with its QuickConnect ID, without using its MAC address or the connection list.

To use the WOL-related service, go to **Network Tools** > **Wake on LAN** (refer to **this article** more detailed instructions).

Chapter 7: Fortify network security

This chapter introduces various security features designed to protect your Synology Router and connected client devices from cyber threats.

7.1 Leverage Security Advisor

Highly recommended is the Security Advisor, an SRM security application that scans your SRM settings and Synology Router. Security Advisor will check your settings and recommend changes that help keep your Synology Router secure.

To launch Security Advisor, go to **Main Menu** > **Security Advisor** (refer to **this article** for more information).

7.2 Activate the firewall

By default, firewall rules filter external IPv4 and IPv6 access to your Synology Router based on specified conditions (e.g., ports and source IP addresses). You can fine-tune security policies for better protection of your Synology Router using firewall rules.

Default firewall rules are already enabled for you. To fine-tune your firewall, you can create custom firewall rules on general traffic by going to **Network Center** > **Security** > **Firewall** (refer to **this article** for more information).

To modify Internet access policies on SRM services/packages, go to **Network Center** > **Security** > **Service** (refer to **this article** for more information).

Notes:

- Firewall rules can be applied to traffic from LAN to LAN, WAN to LAN, or from WAN to SRM.

Enable external access

This function allows external access to SRM via the HTTP/HTTPS ports (e.g., 8000/8001). External access via other ports will be denied.

To enable this function:

1. Go to **Control Panel** > **System** > **SRM Settings**.
2. Select **Allow external access to SRM**.

Notes:

- If this option is deactivated, access to your Synology Router will only be available through LAN.

7.3 Enforce auto block

Auto block automatically blocks IP addresses with a high number of failed login attempts. Such IP addresses will be identified as a potential source of malicious attacks attempting to uncover the passwords.

To enable this function, go to **Network Center** > **Security** > **Auto Block** (refer to **this article** for more information).

7.4 Enable DoS protection

DoS (Denial of Service) attacks bombard a computer system with numerous requests exceeding the target's capability. The attacked computer may miss important data/service requests (e.g., email messages) from outside and suffer from limited Internet bandwidth and system resources.

To enable DoS protection, go to **Network Center** > **Security** > **General**.

7.5 Access SRM via HTTPS

HTTPS (Hypertext Transfer Protocol Secure) is the secure version of HTTP, which is the common protocol for web browsers to communicate with web servers. HTTPS safeguards your Synology Router and client devices against cyber threats and unauthorized access.

You can configure HTTPS settings at **Control Panel** > **System** > **SRM Settings**. To avoid malicious attacks you can do the following:

- **Change the HTTP/HTTPS ports**: By default, the HTTP/HTTPS ports are 8000/8001 respectively, and you can re-specify the HTTP/HTTPS ports to suit your needs.
- **Automatically redirect HTTP connections to HTTPS**: All Internet connections via HTTP will be switched to HTTPS to access SRM. (Both HTTP and HTTPS connections are supported by default.)

- **Enable HSTS**: Only web browsers using HTTPS connection can access SRM, while HTTP-using browsers are denied access.

To access SRM via HTTPS, enter the following in your web browser:

Address	Example
https://IP address of Synology Router:https port number	https://192.168.1.1:8001

7.6 Create certificates

Creating a certificate from your Synology Router is much like issuing a certified ID. If a client device (e.g., a mobile phone) imports the certificate (a .crt file), your Synology Router will be able to identify and communicate with that device via a secure connection (e.g., HTTPS or SSL).

You can also import a certificate from a certificate authority to your Synology Router so that it can access another server.

To create or manage a certificate, go to **Control Panel** > **Services** > **Certificate** (refer to **this article** for more information).

7.7 Implement additional security measures

Additional security measures for strengthening SRM security policies are available in **Network Center**. There, you can set a logout timer, assist your browser in bypassing IP checking, and do much more.

To configure additional security measures for your Synology Router, go to **Network Center** > **Security** > **General** (refer to **this article** for more information).

Chapter 8: Update, restore, and reset your SRM

This chapter introduces how to update SRM and its packages, as well as how to back up and restore SRM's configuration.

8.1 Update SRM and packages

Synology periodically releases free SRM updates and package updates to fix reported issues, enhance system and package performance and offer whole new features.

Update SRM

The system will display the current SRM version and check if a newer SRM update is available. To update SRM and modify update preferences, go to **Control Panel** > **System** > **Update & Restore**.

If you wish to run a manual SRM update, a .pat update file is necessary. This can be found at Synology's **Download Center**.

For more information about updating SRM, please refer to **this article**.

Notes:

- You cannot downgrade SRM using a version older than the current version running on your Synology Router.

Update packages

In **Package Center**, the system will display packages that have any updates for download. Here you can update packages and customize update settings. You can also manually update packages with a .spk update file.

For more information about updating SRM packages, please refer to **this article**.

Notes:

- You cannot downgrade packages using a version older than the current version running on your Synology Router.

8.2 Back up and restore SRM

By backing up and restoring SRM, you can preserve important settings for future use. We suggest you regularly back up SRM configurations and store the configuration file (.dss) on your Synology NAS or local computer.

You can back up current SRM configurations or restore previous configurations by importing the .dss file at **Control Panel** > **System** > **Update & Restore**.

For more information on backup and restore, please refer to **this article**.

8.3 Reset SRM

There are times when you may want to reset all or a portion of the settings on your Synology Router to their factory defaults. SRM offers the following two methods:

Perform a partial reset

You can restore part of your Synology Router settings to their original settings, also called a "soft reset". Only passwords of the administrator and other accounts with equal privileges will be reset.

To perform a soft reset, hold and press the **RESET** button on your Synology Router for 4 seconds.

Restore to factory default settings

You can reset your Synology Router's entire SRM through a "hard reset." All user data stored will be erased, and the entire system will be restored to default settings.

There are two ways to do a hard reset:

- **Method 1**: Go to **Control Panel** > **System** > **Update & Restore** and click **Restore Factory Default Settings**.
- **Method 2**: Hold and press the **RESET** button for 10 seconds.

Notes:

- If you click **Restore Factory Default Settings**, all user data stored on any attached external storage devices will also be erased and the entire system will be restored to default settings.

For more information about restoring to factory default settings, please refer to **this article**.

Chapter 9: Manage Internet connections

This chapter introduces various features for easy and safe access to the Internet.

9.1 Select an Internet connection type

At **Network Center** > **Internet** > **Connection** > **Primary Interface**, you can choose how to connect your Synology Router to the Internet:

- **Auto**: Choose this option if you rely on an ISP (Internet Service Provider) modem for automatic IP assignment.
- **PPPoE**: Choose this option if you have obtained PPPoE credentials from the ISP.
- **Manual**: Choose this option if you have obtained an available IP address for use.
- **DS-Lite**: Choose this option if you have obtained a DS-Lite service request from the ISP.

You can enable a secondary interface to operate in failover or load-balancing mode. Go to **Network Center** > **Internet** > **Connection** > **Secondary Interface (LAN 1)** to enable this interface.

For more information on selecting an Internet connection type, please refer to **this article**.

9.2 Configure ISP, VPN client, and IPv6 settings

You can manage ISP settings, VPN client settings, and IPv6 settings of your Synology Router.

For more information about these settings respectively, please refer to **this article**.

Configure ISP settings

Some ISPs require additional configurations for successful registration. These settings allow you to configure MAC cloning and extra DHCP options (12/60/61) to suit the needs of these ISPs.

To configure, go to **Network Center** > **Internet** > **Connection** > **Primary Interface** > **ISP settings**.

Configure VPN settings

A VPN (Virtual Private Network) helps you securely access resources to another private network from the Internet. SRM currently supports the following protocols: L2TP/IPSec, OpenVPN, and PPTP.

To use your Synology Router as a VPN client, go to **Network Center** > **Internet** > **Connection** > **Primary Interface** > **VPN Settings** to modify the settings.

Further reading:

- **Frequently asked questions regarding using Synology Router as a VPN client**

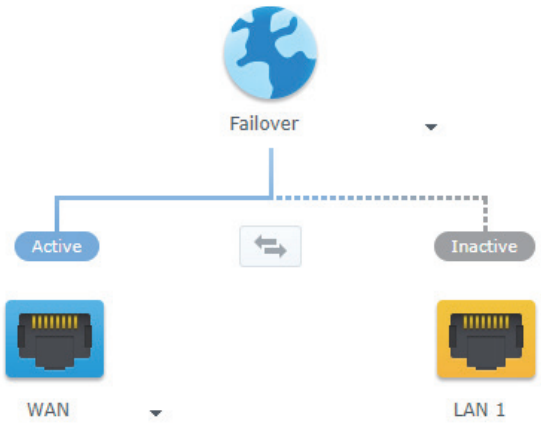
Configure IPv6 settings

To set up IPv6 on your Synology Router, please go to **Network Center** > **Internet** > **Connection** > **Primary Interface** > **IPv6 Setup**. The supported IPv6 types include Auto, Manual, 6in4, 6to4, 6rd, DHCPv6-PD, IPv6 relay (pass-through), and FLET's IPv6.

9.3 Set up Smart WAN

At **Network Center** > **Internet** > **Smart WAN**, you can configure network access plans for two defined outward-facing internet interfaces (e.g., PPPoE, WAN, VPN, and mobile networks). You can choose either mode to determine their roles in network connectivity:

- **Failover**: When one of the interfaces is down, the other will be responsible for all the network connectivity to ensure stable connection at all times.
- **Load Balancing + Failover**: When both interfaces are well-functioning, this mode allows you to distribute network traffic to the interfaces for optimal network traffic flow; when one of the interfaces is down, the other will be responsible for all the network connectivity to ensure stable connection at all times.



Apart from failover and load balancing, you can also configure the following additional options for Smart WAN:

- **Interface priority:** This mode allows you to determine the priority order of WAN interfaces. The interface of the highest priority will act as the default interface. If its gateway fails, it will connect to the gateway of the next interface.
- **Policy routing**: This mode specifies WAN interfaces to forward outbound traffic based on customized criteria. If a network packet matches a policy routing rule, it will be routed to the network interface specified in the same rule.
- **Interface checks**: Test the connectivity of network interfaces by pinging external IP addresses. By default, your Synology Router periodically checks if its external IP address can be pinged.

For more information about setting up Smart WAN, please refer to **this article**.

Further reading:

- **How do I configure Smart WAN for my Synology Router?**
- **How do I connect devices to the Internet via specific network interfaces?**

9.4 Set up QuickConnect & DDNS

You can enable the services for QuickConnect or DDNS for easy connection to your Synology Router at **Network Center** > **Internet** > **QuickConnect & DDNS**.

QuickConnect

QuickConnect is a connection technology developed by Synology that helps you effortlessly access your Synology Router from everywhere, using only your QuickConnect ID. A Synology Account is required to set up QuickConnect.

For more information on setting up and utilizing QuickConnect with your Synology Router, please refer to **Chapter 2**.

Further reading:

- **QuickConnect white paper**

DDNS

DDNS (Dynamic Domain Name Service) matches the hostname and the IP address of your Synology Router for quick access. If you don't have a DDNS hostname, you can register one from Synology or another DDNS provider. Enter the registered hostname in the web browser to find your Synology Router with its DDNS hostname (e.g., morgan.synology.me).

For more information about setting up QuickConnect and DDNS, please refer to **this article**.

9.5 Set up DMZ

A DMZ (also known as a "demilitarized zone") is a section of a network that is directly connected to the Internet or other untrusted networks. All external access will be directed to the DMZ host device. The DMZ host can connect to the Internet directly and is not restricted by firewall restrictions or protection.

At times it may be useful to configure servers as the DMZ host. Some examples include:

- Open a random port for certain applications.
- Host a home-based webserver.
- Use the DMZ host for gaming consoles.

To set up DMZ, go to **Network Center** > **Port Forwarding** > **DMZ**.

Notes:

- To connect to a host in the DMZ from an external network, you need the host's external IP address retrieved by your Synology Router.

9.6 Enable port forwarding

Port forwarding redirects data flow between different ports and has the following advantages:

- Improves performance for applications that might otherwise rely on a relay service.
- Protects the ports used by services/client devices from direct exposure to cyber threats.
- Offers open ports to resolve port conflicts between multiple services/client devices.

To set up port forwarding rules, go to **Network Center** > **Port Forwarding** > **Port Forwarding**.

For more information about configuring port forwarding, please refer to **this article**.

9.7 Enable port triggering

Port triggering requires the configuration of one static port (the trigger port) and one dynamic port (the incoming port) for data transmission used by a service/device in the local network. Once the data come out to an external host through the trigger port, the incoming port is then triggered and opened to receive data from the host. If no data come out, the incoming port turns off, shutting down a possible opening for malicious attacks.

To set up port triggering rules, go to **Network Center** > **Port Forwarding** > **Port Triggering**.

For more information about enabling port triggering, please refer to **this article**.

Chapter 10: Manage local network connections

The chapter introduces various features to flexibly manage LANs (Local Area Networks).

10.1 Manage local networks

At **Network Center** > **Local Network**, you can manage your local networks. Local networks can be configured with independent Wi-Fi and a variety of LAN settings. There are three types of local networks:

- **Primary network**: The main local network is set up by default. It is the only network whose Ethernet ports can be configured as trunk ports. Client devices can connect to it via Ethernet cables or wireless signals.
- **Guest network**: A completely wireless local network set up by default. It allows you to provide visitors with Internet connectivity without granting them access to your private networks.
- **Custom network**: Additional local networks that you can set up. It can be assigned both Ethernet ports or Wi-Fi names (SSIDs).

Detailed network configurations settings for each local network can be managed by going to **Network Center** > **Local Network** > **Network** > **Specify a network** > **Edit**.

Assign Ethernet ports

Once an Ethernet port is assigned to a local network, devices connected to this port directly or indirectly (i.e., through a switch) will belong to this network. By default, Ethernet ports that are not assigned to custom networks will belong to the primary network.

To assign Ethernet ports to your local network, go to **Network Center** > **Local Network** > **Network** > **Specify a network** > **Edit** > **Ethernet**.

Assign VLAN tags

VLANs (Virtual Local Area Networks) enable networks to be segmented and formed into logical groups of users, regardless of the user's physical location or LAN connection. Networks can be assigned a VLAN ID (VID) to differentiate a network from others.

To assign a VLAN ID for a local network, go to **Network Center** > **Local Network** > **Network** > **Specify a network** > **Edit** > **General**.

At **Network Center** > **Local Network** > **Network** > **VLAN Tag**, you can see how traffic from each port is tagged with VLAN IDs (VIDs), allowing you to configure managed switches or other devices that require VLAN tags.

For more information about managing your primary local network, please refer to **this article**.

10.2 Create additional local networks

Other than the primary network and guest network, you can create additional local networks for greater flexibility. Local networks can consist of entirely wired clients, entirely wireless clients, or a mix of both.

To create a new local network, go to **Network Center** > **Local Network** > **Network** > **Add**, and follow the directions provided by the wizard.

For more information about creating local networks, please refer to **this article**.

10.3 Manage DHCP services

As a DHCP (Dynamic Host Configuration Protocol) server, your Synology Router can assign dynamic IP addresses to DHCP clients (i.e., your computer) within your local network.

You can enable DHCP services for both IPv4 and IPv6 networks. To do so, go to **Network Center** > **Local Network** > **Network** > **Specify local network** > **IPv4 DHCP** or **IPv6 DHCP**.

You can also view a list of DHCP clients and their properties (e.g., MAC and IP addresses) at **Network Center** > **Local Network** > **DHCP Client**.

To reserve the assigned IP addresses for the clients, go to **Network Center** > **Local Network** > **DHCP Reservation**.

For more information about managing DHCP services, please refer to **this article**.

10.4 Set up static routes

A static route is a routing path manually configured to pass data to a specific destination service/device.

Setting up static routes can benefit you in the following scenarios:

- When the network (e.g., a home local network) is small and may not expand quickly into a complex network.
- When you do not wish to share routing information (e.g., IP addresses and network configuration) with other routers for security reasons.

To set up static routes, go to **Network Center** > **Local Network** > **Static Route**.

For more information about configuring static routes, please refer to **this article**.

Notes:

- Static routes do not automatically change their routing settings to fit any network configuration changes.
- It is recommended not to use static routes when the network is large and complex because maintaining static routes in this environment can be time-consuming.
- You can set up IPv6 static routes after enabling the IPv6 function on your Synology Router.

10.5 Set up IPTV & VoIP

The IPTV & VoIP services allow you to connect an STB (set-top box) or VoIP phone to your Synology Router for your ISP's multimedia services or phone communication services. Before using these services, you need to have a VLAN ID provided by your ISP.

To set up the IPTV & VoIP services, go to **Network Center** > **Local Network** > **IPTV & VoIP**.

For more information about configuring IPTV & VoIP, please refer to **this article**.

Chapter 11: Manage external device and permissions

This chapter introduces features to manage external devices that can be plugged into your Synology Router.

11.1 Manage storage devices

With USB/SD storage, your Synology Router can turn into a storage device for personal data and multimedia files. Attach the storage to the corresponding slot to install external USB/SD storage to your Synology Router.

At **Control Panel** > **Storage** > **Storage**, you can view the total available external storage (e.g., USB drives & SD cards) on your Synology Router. There you can also format and manage the storage to suit your needs.

For more information on managing external storage devices, please refer to **this article**.

Notes:

- Please refer to the **compatibility list** for approved USB/SD storage.
- Some system services and packages may create temporary files on USB/SD storage devices. To safely eject a USB/SD storage device for system stability and prevent accidental data loss, press the **EJECT** button on your Synology Router or eject the storage at **Control Panel** > **Storage** > **Storage**.

11.2 Define folder permissions

After external storage is established on your Synology Router, you can create shared folders for public use and home folders for individual users.

To create shared folders and assign access privileges to users, go to **Control Panel** > **Storage** > **Shared Folder** (refer to **this article** for more information).

To create users and assign them access privileges to shared folders, go to **Control Panel** > **User** > **User**.

11.3 Manage mobile network dongles

With a mobile broadband dongle, your Synology Router will be able to provide Internet access to client devices via a mobile broadband network. The dongle can transform your Synology Router into a Wi-Fi hotspot. To install a mobile broadband dongle to your Synology Router, please plug it into the USB slot. The dongle will be available immediately. If not, please check your settings.

To manage the dongle settings, go to **Network Center** > **Internet** > **Mobile Network** (refer to **this article** for more information).

Notes:

- Please refer to the **compatibility list** for approved mobile broadband dongles.

Chapter 12: Configure system settings

This chapter introduces various system settings such as hardware settings, system databases, regional options, and customizing login styles.

12.1 Manage hardware settings

Go to **Control Panel** > **Device** to view the following hardware information and manage their settings :

- **System settings**: View basic information regarding your Synology Router.
- **LED**: Customize the LED behavior of your Synology Router.
- **Printer**: Configure your Synology Router as a print server.
- **Reboot Schedule**: Set up a one-time or recurring schedule for your Synology Router to reboot.

For more information about managing your router's hardware settings, please refer to **this article**.

12.2 Check system databases

System database contains information used by various APIs such as DoH server and Threat Intelligence.

Go to **Control Panel** > **System Database** to enable or disable the function of **Automatically check for and install updates** for the system databases on your SRM.

12.3 Modify time and regions

Go to **Control Panel** > **System** > **Regional Options** to the below time and region settings:

- **Current Time**: Configure your SRM system time settings. You can check the current time, set the date and time of your Synology Router, or synchronize system time automatically using a network time server.
- **Location**: Select your current location to ensure the full functionality of your Synology Router.

- **Language**: Set the language for display, notification, and code pages.

For more information about modifying time and regions, please refer to **this article**.

12.4 Customize login styles

Go to **Control Panel** > **System** > **Login Style** to customize the appearance of the SRM login screen by choosing from a variety of templates, changing the background image, or adding a logo.

For more information about customizing login styles, please refer to **this article**.

Chapter 13: Discover SRM packages

This chapter introduces various Synology-developed packages to go with your Synology Router. Featured packages are available via **Package Center** or Synology's **Download Center**.

13.1 Safe Access

Safe Access shields your network and makes it simple to manage devices connected to your Synology Router. You can create profiles and assign devices to safeguard their Internet behavior, specify how long and when to block or allow their Internet access, and create web filters to manage what websites profile owners can visit. Safe Access functions can also be managed via the **DS router** mobile app for added convenience.

Safe Access also includes the pause, reward, and access request features to help you manage your profiles effectively. Furthermore, by blocking dangerous websites, the Network Protection function of the package also gives comprehensive protection to all the devices in your local networks.

For more information about configuring Safe Access, please refer to **this article**.

Further reading:

- **Frequently asked questions about Safe Access**

13.2 VPN Plus Server

VPN Plus Server turns your Synology Router into a powerful VPN server. This package provides secure VPN access via a web browser or client. A variety of VPN services such as WebVPN, SSL VPN, SSTP, OpenVPN, L2TP/IPSec, and PPTP is supported. Its Remote Desktop also enables employees to easily and securely access remote internal network resources through a web browser.

With Site-to-Site VPN, VPN Plus Server allows multiple networks in different locations to establish secure connections between each other over the Internet. Moreover, with built-in management tools, this package can help network administrators regulate and monitor VPN traffic at all times.

For more information about configuring VPN Plus Server, please refer to **this article**.

Further reading:

- **Frequently asked questions regarding VPN Plus Server on Synology Router**
- **Frequently asked questions about Site-to-Site VPN**

13.3 Threat Prevention

Threat Prevention protects the network security of your Synology Router and subordinate devices by detecting/dropping malicious packets. This package offers various features to help you keep track of potential malicious threats.

For more information about configuring Threat Prevention, please refer to **this article.**

Further reading:

- **How do I monitor Threat Prevention to avoid attacks?**

13.4 DNS Server

The Domain Name System (DNS) is an address book of the Internet. It maps meaningful names (i.e., domain names such as "www.synology.com") into IP addresses (e.g., "210.61.203.220"), allowing users to easily access web pages, computers, or other resources across networks.

DNS service can be set up via **DNS Server** in SRM. It has the following features:

- **Master and slave zones**: The DNS boundaries that allow granular control of DNS components. You can store DNS information in one master zone (containing a read/write copy of data) and multiple slave zones (containing read-only copies of data) to ensure high availability of DNS service.
- **DNS forwarding**: An alternative method of DNS resolution that will be used when the DNS Server cannot find matching IP addresses in your zones.
- **TSIG keys**: Safeguard the synchronization of your DNS files with encryption.
- **Split-horizon DNS**: A function that provides each client with customized DNS information; this can help improve the security and privacy management of DNS zone records.

For more information about configuring DNS Server, please refer to **this article**.

13.5 Media Server

Turn your Synology Router into a multimedia server. With Media Server, you can stream multimedia content from your Synology Router to DLNA/UPnP-compliant DMAs (e.g., stereo systems, TV sets, or gaming consoles). By connecting these devices to your home network, you can view photos, listen to music, and watch videos without installing any applications or devices on them.

Manage Media Server with the following options for enhanced DMA compatibility and a smooth streaming experience:

- Custom MIME types that help individual devices identify file formats.
- Device lists to restrict the access of newly detected devices on LAN and to apply the settings of predefined profiles.

For more information about Media Server, please refer to **this article**.

13.6 RADIUS Server

RADIUS Server is an add-on package that offers centralized authentication, authorization, and accounting (AAA) for wired and wireless network connections via the Remote Authentication Dial-In User Service (RADIUS) protocol. RADIUS Server allows you to:

- Flexibly deploy wireless routers, VPN servers, and network switches with RADIUS support on your network.
- Unify the security regulation process of different connection types.
- Choose between various authentication methods, e.g., PAP, MS-CHAP, PEAP, EAP-MSCHAPv2, or EAP-TTLS.
- Import existing local SRM, domain, or LDAP user lists.
- Configure detailed restrictions for users and groups.
- Keep track of the access statuses with detailed reports.

For more information about RADIUS Server, please refer to **this article**.

Further reading:

- **How do I set up a WPA2-Enterprise wireless network with RADIUS Server on Synology Router?**

Chapter 14: Discover SRM mobile apps

This chapter introduces useful Synology mobile applications to go with your Synology Router.

14.1 DS router

DS router enables you to easily access your Synology Router from a mobile device. From the initial setup of your Synology Router to managing QoS and adjusting security settings, DS router makes network management easy, intuitive, and mobile.

The overview page allows you to quickly view relevant information such as the link rate between your mobile device and the Synology Router, the number of connected clients, the Internet status, and other relevant activities. In addition, you can quickly monitor and manage connected clients, monior connection status and resource usage, configure Wi-Fi settings, and update your Synology Router.

Moreover, integration with Safe Access allows you to create profiles and manage devices, set time quotas, and apply web filters to protect certain users and supervise Internet access directly from.

DS router is available for both **Android** and **iOS**.

To learn more about DS router, please refer to the articles for **Android** and **iOS**.

14.2 VPN Plus

VPN Plus provides convenient access to local network resources via Synology SSL VPN service powered by the Synology Router. This mobile application provides you with fast connection speeds, enhanced security, and the capability of passing network traffic through firewalls.

VPN Plus is available for **Android** and **iOS**.

To learn more about VPN Plus, please refer to the articles for **Android** and **iOS**.

Notes:

- If your mobile device requires a VPN connection via another protocol other than SSL vpn or web vpn, you can use a third-party app (either built-in or downloaded from your mobile device's app store). For more information, please refer to the user guide of your mobile device.

14.3 DS file

DS file is ideal for managing files stored on your Synology Router. It can upload or download files between your Synology Router and your wireless device, as well as perform basic editing tasks. Besides file management, DS file is also a useful tool for doing things like browsing pictures, watching videos, and checking work documents while on the go.

DS file is available for **Android** and **iOS**.

For more information about using DS file, please refer to **this article**.

Chapter 15: Utilize diagnosis tools

This chapter introduces features on your Synology Router helpful for diagnosing system and connection problems.

15.1 Check connection status

To grasp Synology Router's current status and pin down the possible causes of a down connection, you can get a quick, well-rounded view of all wired and Wi-Fi connections at **Network Center** > **Status** (refer to **this article** for more information). There you can also view the router's network, CPU, and memory usage in real-time.

You can also view a detailed traffic log (up to one month long) of devices and applications by going to **Network Center** > **Traffic Control** > **Monitor** (refer to **this article** for more information).

15.2 Set up notifications

Synology Router sends instant notifications to keep you informed of system/connection errors via various media (e.g., SRM desktop, SMS, and emails). You can immediately identify and fix issues.

To customize the notification service, go to **Control Panel** > **Notification** (refer to **this article** for more information).

15.3 Audit logs in Log Center

Router logs tell you a lot about your networks and can be an important source of information when diagnosing network problems. Synology Router logs can be found in **Log Center**, a centralized log management application. It includes comprehensive tools to help you conveniently and efficiently complete the following tasks:

- Send and receive logs from other network devices via syslog logging standard.
- Monitor log volume according to device and time.
- Specify log archival destination and create rules to automatically trigger log archival.

- Search for and filter local logs and logs received from other network devices.
- Send notifications to administrators when specified events occur.

Log Center can be found in the Main Menu (refer to **this article** for more information).

15.4 Ping

Ping is a utility used to test and verify if a particular destination IP address exists and can accept requests in computer network administration. It can also be used to diagnose if a connection is being throttled. Ping works by sending out a request packet to a target website or IP address and calculating the time it takes for the target to respond.

- **Normal connection**: The response packet comes from the target instantly.
- **Slow connection**: The response packet comes from the target with significant delay.

Delayed packet transmission may occur in the suggested scenarios below:

- The target is busy dealing with huge traffic to and from other hosts/clients.
- The target website/IP address is down/not working.
- The Internet/local network connection of your Synology Router is not properly configured.
- The ISP service is down.

If the problem is identified as extraneous to your Synology Router, you may consult your ISP or other relevant service providers for assistance.

To diagnose connection problems with Ping, please go to **Network Tools** > **Ping** (refer to **this article** for more information).

15.5 Traceroute

Traceroute is a utility used to examine the Internet pathways taken to reach specific destinations. The physical route will be displayed on Google Maps, along with the time-lapse spent between two adjacent route points.

With Traceroute, you can better understand how your traffic is routed.

To diagnose connection problems with Traceroute, please go to **Network Tools** > **Traceroute** (refer to **this article** for more information).

Chapter 16: Troubleshooting & FAQ

This section contains solutions to common issues that you may encounter. Follow the steps provided in the link to solve your problem.

Connection issues

- **Why can't I find my Synology Router via router.synology.com**
- **Why can't I access the Internet after setting up my Synology Router?**
- **I can't connect to the L2TP VPN of VPN Plus Server. What can I do?**
- **My guest network is not functioning properly when the mesh Wi-Fi system has been set up. What can I do?**
- **My Internet is slow. What can I do?**
- **I can't access my Synology Router. What can I do?**

Setup issues

- **How do I deploy my Synology Wi-Fi system to achieve the best connection?**
- **I can't set up a Site-to-Site VPN connection. What can I do?**
- **My Wi-Fi signal is weak. What can I do to improve it?**
- **What should I do if my Wi-Fi is unstable, disconnected, or has a low transmission speed?**

Hardware issues

- **How do I reset my Synology Router?**
- **Why can't I block some mobile apps using Safe Access?**
- **Log Center says my 5 GHz-1 Wi-Fi has "run out of DFS channels." What does that mean?**

SYNOLOGY, INC.
END USER LICENSE AGREEMENT

IMPORTANT–READ CAREFULLY: THIS END USER LICENSE AGREEMENT ("EULA") IS A LEGAL AGREEMENT BETWEEN YOU (EITHER AN INDIVIDUAL OR A LEGAL ENTITY) AND SYNOLOGY, INC. ("SYNOLOGY") FOR THE SYNOLOGY SOFTWARE INSTALLED ONTO THE SYNOLOGY PRODUCT PURCHASED BY YOU (THE "PRODUCT"), OR LEGALLY DOWNLOADED FROM WWW.SYNOLOGY.COM, OR ANY OTHER CHANNEL PROVIDED BY SYNOLOGY ("SOFTWARE").

YOU AGREE TO BE BOUND BY THE TERMS OF THIS EULA BY USING THE PRODUCTS CONTAINING THE SOFTWARE, INSTALLING THE SOFTWARE ONTO THE PRODUCTS OR DEVICE CONNECTED TO THE PRODUCTS. IF YOU DO NOT AGREE TO THE TERMS OF THIS EULA, DO NOT USETHE PRODUCTS CONTAINING THE SOFTWAREOR DOWNLOAD THE SOFTWARE FROM WWW.SYNOLOGY.COM, OR ANY OTHER CHANNEL PROVIDED BY SYNOLOGY.INSTEAD, YOU MAY RETURN THE PRODUCT TO THE RESELLER WHERE YOU PURCHASED IT FOR A REFUND IN ACCORDANCE WITH THE RESELLER'S APPLICABLE RETURN POLICY.

Section 1. Limited Software License. Subject to the terms and conditions of this EULA, Synology grants you a limited, non-exclusive, non-transferable, personal license to install, run and use one copy of the Software loaded on the Product or on your device connected to the Product solely relating to your authorized use of the Product.

Section 2. Documentation. You may make and use a reasonable number of copies of any documentation provided with the Software; provided that such copies will only be used for internal business purposes and are not to be republished or redistributed (either in hard copy or electronic form) to any third party.

Section 3. Backup. You may make a reasonable number of copies of the Software for backup and archival purposes only.

Section 4. Updates. Any software provided to you by Synology or made available on the Synology website at www.synology.com ("Website") or any other channel provided by Synology that updates or supplements the original Software is governed by this EULA unless separate license terms are provided with such updates or supplements, in which case, such separate terms will govern.

Section 5. License Limitations. The license set forth in Sections 1, 2 and 3 applies only to the extent that you have ordered and paid for the Product and states the entirety of your rights with respect to the Software. Synology reserves all rights not expressly granted to you in this EULA. Without limiting the foregoing, you shall not authorize or permit any third party to: (a) use the Software for any purpose other than that in connection with the Product; (b) license, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Software; (c) reverse engineer, decompile, disassemble or attempt to discover the source code of or any trade secrets related to the Software, except and only to the extent that such conduct is expressly permitted by applicable law notwithstanding this limitation; (d) adapt, modify, alter, translate or create any derivative works of the Software; (e) remove, alter or obscure any copyright notice or other proprietary rights notice on the Software or Product; or (f) circumvent or attempt to circumvent any methods employed by Synology to control access to the components, features or functions of the Product or Software. Subject to the limitations specified in this Section 5, you are not prohibited from providing any services hosted by Synology NAS server to any third party for commercial purpose.

Section 6. Open Source. The Software may contain components licensed to Synology under the GNU General Public License ("GPL Components"), currently available at http://www.gnu.org/licenses/gpl.html. The terms of the GPL will control solely with respect to the GPL Components to the extent that this EULA conflicts with the requirements of the GPL with respect to your use of the GPL Components, and, in such event, you agree to be bound by the GPL with respect to your use of such components.

Section 7. Audit. Synology will have the right to audit your compliance with the terms of this EULA. You agree to grant Synology a right to access to your facilities, equipment, books, records and documents and to otherwise reasonably cooperate with Synology in order to facilitate any such audit by Synology or its agent authorized by Synology.

Section 8. Ownership. The Software is a valuable property of Synology and its licensors, protected by copyright and other intellectual property laws and treaties. Synology or its licensors own all rights, titles and interests in and to the Software, including but not limited to copyright and any other intellectual property rights.

Section 9. Limited Warranty. Synology provides a limited warrant that the Software will substantially conform to Synology's published specifications for the Software, if any, or otherwise set forth on the Website, for a period required by your local law. Synology will use commercially reasonable efforts to, in Synology's sole discretion, either correct any such nonconformity in the Software or replace any Software that fails to comply with the foregoing warranty, provided that you give Synology written notice of such noncompliance within the warranty period. The foregoing warranty does not apply to any noncompliance resulting from any: (w) use, reproduction, distribution or disclosure not in accordance with this EULA; (x) any customization, modification or other alteration of the Software by anyone other than Synology; (y) combination of the Software with any product, services or other items provided by anyone other than Synology; or (z) your failure to comply with this EULA.

Section 10. Support. During the period specified in the Section 9, Synology will make available to you the support services. Following the expiration of the applicable period, support for Software may be available from Synology upon written

request.

Section 11. Disclaimer of Warranties. EXCEPT AS EXPRESSLY SET FORTH ABOVE, THE SOFTWARE IS PROVIDED "AS IS" AND WITH ALL FAULTS. SYNOLOGY AND ITS SUPPLIERS HEREBY DISCLAIM ALL OTHER WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, ARISING BY LAW OR OTHERWISE, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR USE, TITLE AND NONINFRINGEMENT, WITH REGARD TO THE SOFTWARE. WITHOUT LIMITING THE FOREGOING, SYNOLOGY DOES NOT WARRANT THAT THE SOFTWARE WILL BE FREE OF BUGS, ERRORS, VIRUSES OR OTHER DEFECTS.

Section 12. Disclaimer of Certain Damages. IN NO EVENT WILL SYNOLOGY OR ITS LICENSORS BE LIABLE FOR ANY INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, CONSEQUENTIAL OR SIMILAR DAMAGES OR LIABILITIES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO LOSS OF DATA, INFORMATION, REVENUE, PROFIT OR BUSINESS) ARISING OUT OF OR RELATING TO THE USE OF OR INABILITY TO USE THE SOFTWARE OR OTHERWISE UNDER OR IN CONNECTION WITH THIS EULA OR THE SOFTWARE, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHER THEORY EVEN IF SYNOLOGY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Section 13. Limitation of Liability. SYNOLOGY'S AND ITS SUPPLIERS' LIABILITY ARISING OUT OF OR RELATING TO THE USE OF OR INABILITY TO USE THE SOFTWARE OR OTHERWISE UNDER OR IN CONNECTION WITH THIS EULA OR THE SOFTWARE IS LIMITED TO THE AMOUNT ACTUALLY PAID BY YOU FOR THE PRODUCT REGARDLESS OF THE AMOUNT OF DAMAGES YOU MAY INCUR AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHER THEORY. The foregoing disclaimer of warranties, disclaimer of certain damages and limitation of liability will apply to the maximum extent permitted by applicable law. The laws of some states/jurisdictions do not allow the exclusion of implied warranties or the exclusion or limitation of certain damages. To the extent that those laws apply to this EULA, the exclusions and limitations set forth above may not apply to you.

Section 14. Export Restrictions. You acknowledge that the Software is subject to U.S. export restrictions. You agree to comply with all applicable laws and regulations that apply to the Software, including without limitation the U.S. Export Administration Regulations.

Section 15. Termination. Without prejudice to any other rights, Synology may terminate this EULA if you do not abide by the terms and conditions contained herein. In such event, you must cease use of the Software and destroy all copies of the Software and all of its component parts.

Section 16. Assignment. You may not transfer or assign your rights under this EULA to any third party, except for that pre-installed in the Products. Any such transfer or assignment in violation of the foregoing restriction will be void.

Section 17. Applicable Law. Unless expressly prohibited by local law, this EULA is governed by and construed in accordance with the laws of the country, in accordance with which Synology Inc. was organized without regard to any conflict of law principles to the contrary.

Section 18. Dispute Resolution. Any dispute, controversy or claim arising out of or relating to this EULA will be resolved exclusively and finally by arbitration conducted by three neutral arbitrators in accordance with the procedures of the Arbitration Law and related enforcement rules of the country in which Synology Inc. was organized. In such cases, the arbitration will be limited solely to the dispute between you and Synology. The arbitration, or any portion of it, will not be consolidated with any other arbitration and will not be conducted on a class-wide or class action basis. The arbitration shall take place in Taipei and the arbitration proceedings shall be conducted in English or, if both parties so agree, in Mandarin Chinese. The arbitration award shall be final and binding on the parties and may be enforced in any court having jurisdiction. You understand that, in the absence of this provision, you would have had a right to litigate any such dispute, controversy or claim in a court, including the right to litigate claims on a class-wide or class-action basis, and you expressly and knowingly waive those rights and agree to resolve any disputes through binding arbitration in accordance with the provisions of this Section 18. Nothing in this Section shall be deemed to prohibit or restrict Synology from seeking injunctive relief or seeking such other rights and remedies as it may have at law or equity for any actual or threatened breach of any provision of this EULA relating to Synology's intellectual property rights.

Section 19. Attorneys' Fees. In any arbitration, mediation, or other legal action or proceeding to enforce rights or remedies under this EULA, the prevailing party will be entitled to recover, in addition to any other relief to which it may be entitled, costs and reasonable attorneys' fees.

Section 20. Severability. If any provision of this EULA is held by a court of competent jurisdiction to be invalid, illegal, or unenforceable, the remainder of this EULA will remain in full force and effect.

Section 21. Entire Agreement. This EULA sets forth the entire agreement of Synology and you with respect to the Software and the subject matter hereof and supersedes all prior and contemporaneous understandings and agreements whether written or oral. No amendment, modification or waiver of any of the provisions of this EULA will be valid unless set forth in a written instrument signed by the party to be bound thereby.

SYNOLOGY, INC.
LIMITED PRODUCT WARRANTY

THIS LIMITED WARRANTY ("WARRANTY") APPLIES TO THE PRODUCTS (AS DEFINED BELOW) OF SYNOLOGY, INC. AND ITS AFFILIATES, INCLUDING SYNOLOGY AMERICA CORP, (COLLECTIVELY, "SYNOLOGY"). YOU ACCEPT AND AGREE TO BE BOUND BY THE TERMS OF THIS WARRANTY BY OPENING THE PACKAGE CONTAINING AND/OR USING THE PRODUCT. PLEASE BE ADVISED THAT THIS LIMITED WARRANTY DOES NOT APPLY TO THE SOFTWARE CONTAINED IN THE PRODUCTS WHICH SHALL BE SUBJECT TO ITS END USER LICENSE AGREEMENT, AND THAT SYNOLOGY RESERVES THE RIGHT TO MAKE ADJUSTMENTS AND/OR MODIFICATION TO THIS PRODUCT WARRANTY FROM TIME TO TIME WITHOUT PROVIDING PRIOR NOTICE TO YOU. IF YOU DO NOT AGREE TO THE TERMS OF THIS WARRANTY, DO NOT USE THE PRODUCT. INSTEAD, YOU MAY RETURN THE PRODUCT TO THE RESELLER WHERE YOU PURCHASED IT FOR A REFUND IN ACCORDANCE WITH THE RESELLER'S APPLICABLE RETURN POLICY.
PLEASE NOTE THAT SYNOLOGY'S WARRANTY SUPPORTS ARE NOT AVAILABLE IN EVERY COUNTRY, AND THAT SYNOLOGY MAY REFUSE TO PROVIDE THIS LIMITED WARRANTY SUPPORTS TO YOU IF YOU REQUEST SUCH SUPPORTS NOT AT THE COUNTRY AT WHICH THE PRODUCT WAS ORIGINALLY PURCHASED. THE COUNTRY AT WHICH THE PRODUCT WAS ORIGINALLY PURCHASED SHALL BE DETERMINED BASED ON THE SYNOLOGY'S INTERNAL RECORDS.

Section 1. Products

(a) "Products" refer to New Products or Refurbished Products.
(b) "New Product" means the Synology-branded hardware product and Synology-branded accessories contained in the original packaging Customer bought from an authorized Synology distributor or reseller. You may see our "New Product" at Product Support Status.
(c) "Refurbished Product" means all Synology products which have been refurbished by Synology's affiliate or an authorized Synology distributor or reseller, not including those sold as "as is" or with "no warranty" by anyone.
(d) Other definition: "Customer" means the original person or entity purchasing the Product from Synology or an authorized Synology distributor or reseller; "Online Store" means an online shop operated by Synology or Synology's affiliate; "Software" means the Synology proprietary software that accompanies the Product when purchased by Customer, is downloaded by Customer from the Web Site, or is pre-installed on the Product by Synology, and includes any firmware, associated media, images, animations, video, audio, text and applets incorporated into the software or Product and any updates or upgrades to such software.

Section 2. Warranty Period

(a) "Warranty Period": The warranty period commences on the purchase date is shown on the purchase receipt or invoice to be presented by Customer and ending at the day after the end of the Warranty Period for each New Product. You may see the Warranty Period for each New Product at Product Support Status. For the Refurbished Product or repaired parts, it's the remainder of the warranty period of the product they are replacing, or ninety (90) days from the date the product was replaced or repaired, whichever is longer; except for those sold as "as is" or with "no warranty" by any stores. Without presenting such purchase receipt or invoice, the warranty period shall commence on the date of manufacture based on our internal record.
(b) "Extended Warranty Period": For Customer purchasing EW201/ EW202 optional service for applicable Products specified in Section 1 (b), the Warranty Period specified in Section 2 (a) of the applicable Product registered with EW201/EW202 optional service will be extended by two years. You may see the applied model at Extended Warranty.
(c) "Immediate termination of Warranty Period": As to the Synology drive product, its warrant period will terminate immediately upon either of following situations occurs: (a) for solid-state drive, its lifespan wear-out indicator is equal to or exceeds the limit specified in the "product specifications" of the drive attached with the purchased product; (b) for all drive products, its temperature record is equal to or exceeds the operating temperature limit of the drive, which is specified in the "product specifications" attached with the purchased product.

Section 3. Limited Warranty and Remedies

3.1 Limited Warranty. Subject to Section 3.2, Synology warrants to the Customer that each Product (a) will be free of material defects in workmanship and (b) under normal use will perform substantially in accordance with Synology's published specifications for the Product during the Warranty Period. Such limited warranty does not apply to the Software contained in the product or purchased by Customer which shall be subject to the accompanying end user license agreement provided with the Product. Synology provides no warranty to Refurbished Product sold as "as is" or with "no warranty". (c) This Limited Warranty is NOT transferable and applies only to the customers who directly purchase products from Synology's affiliate, the resellers, and distributor that Synology authorized. The warranty set forth in Section 3 will terminate upon Customer's sale or transfer of the Product to a third party.

3.2 Exclusions. The foregoing warranties and warranty obligations do not apply to any Product that (a) has been installed or used in a manner not specified or described in the Product, specifications, or its related documents, or in any way misused, abused, or damaged; (b) has been damaged caused by accident, fire, liquid contact, earthquake, other external factor or product use in improper environment; (c) has been disassembled without authorization from Synology; or (d) with cosmetic damage caused by normal wear and tear or otherwise due to the normal aging of the Product, including but not limited to scratches, dents and broken plastic on ports unless failure has occurred due to a defect in materials or

workmanship; (e) serial number has been removed or defaced from Product, resulting in not able to identify; (f) has been damaged or out of order because Customer fails to implement any correction, modification, enhancement, improvement or other update made available to Customer by Synology, or because Customer implements, installs or uses any correction, modification, enhancement, improvement or other update made available by any third party; (g) has been damaged, out-of-order, or incompatible due to installation or use with items not provided by Synology other than the hardware, software or other accessory for which the Product is designed.

Please note that each of the above situations shall be subject to the inspection and verification of the product's appearance and functions by Synology.

3.3 Warranty Support and Exclusive Remedy. If Customer gives notice of noncompliance with any of the warranties set forth in Section 3.1 within the applicable Warranty Period in the manner set forth below, then, upon verification of the noncompliance by Synology, Synology will, at Synology's option: (a) use commercially reasonable efforts to repair the Product, (b) provide technical support, or (c) replace the noncomplying Product or part thereof upon return of the complete Product in accordance with Section 3.4 The foregoing sets forth Synology's entire liability and Customer's sole and exclusive remedy for any breach of warranty under Section 3.1 or any other defect or deficiency in the Product. Customer will reasonably assist Synology to diagnose and validate any nonconformity with the Product. Please note that the warranty support does not apply to rescue of the data stored in Synology Product or its backup. Customer shall make a backup copy of the stored data before it returns the Product to Synology, Synology may weed up all information or data in the Product while it performs the warranty services and shall not be responsible or liable for any data loss therein.

3.4 Return. Any Product return by Customer under Section 3.3 must be made in accordance with Synology's then-current return procedures with the purchase receipt or invoice. You may see more information about the return procedure at How do I make a warranty claim for my Synology product? For warranty claims, the Customer must return the complete Product to Synology in accordance with this Section 3.4. Any returned Product that (a) has been disassembled (except under the direction of Synology); or (b) serial number has been removed or defaced from Product, resulting in not able to identify, or (c) was damaged on the way of return due to improper packaging (including but not limited to scratches and deformation), will be refused and returned to Customer at Customer's expense. Any Product must be returned in the same condition as it was received from Synology to the address designated by Synology, freight pre-paid, in packaging sufficient to protect the contents thereof. Customer is responsible for insurance and risk of loss/damage with respect to returned items until they are properly received by Synology.

3.5 Replacement of New Product or Refurbished Product by Synology. If Synology elects to replace any Product under this Warranty set forth in Section 3.1, then Synology will ship a replacement Product at Synology's expense via the shipping method selected by Synology after receipt of the nonconforming Product returned in accordance with Section 3.4 and validation by Synology that the Product does not conform to the warranty. Before the shipment of the Refurbished Product to the Customers, they have been verified to strictly comply with Synology's quality standard. Please note that part of the Refurbished Products would be with certain stain, scratches, or other minor wear and tear. In some countries, Synology may at its own discretion apply the Synology Replacement Service to certain Products, through which Synology will ship a replacement Product to Customer before its receipt of the nonconforming Product returned by Customer ("Synology Replacement Service").

3.6 Disclaimer of Warranties. THE WARRANTIES, OBLIGATIONS, AND LIABILITIES OF SYNOLOGY AND THE REMEDIES OF CUSTOMER SET FORTH IN THIS WARRANTY ARE EXCLUSIVE AND IN SUBSTITUTION FOR, AND CUSTOMER HEREBY WAIVES, RELEASES AND DISCLAIMS, ALL OTHER WARRANTIES, OBLIGATIONS AND LIABILITIES OF SYNOLOGY AND ALL OTHER RIGHTS, CLAIMS AND REMEDIES OF CUSTOMER AGAINST SYNOLOGY, EXPRESS OR IMPLIED, ARISING BY LAW OR OTHERWISE, WITH RESPECT TO THE PRODUCT, ACCOMPANYING DOCUMENTATION OR SOFTWARE AND ANY OTHER GOODS OR SERVICES DELIVERED UNDER THIS WARRANTY, INCLUDING, BUT NOT LIMITED TO ANY: (A) IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE; (B) IMPLIED WARRANTY ARISING FROM COURSE OF PERFORMANCE, COURSE OF DEALING, OR USAGE OF TRADE; (C) CLAIM OF INFRINGEMENT OR MISAPPROPRIATION; OR (D) CLAIM IN TORT (WHETHER BASED ON NEGLIGENCE, STRICT LIABILITY, PRODUCT LIABILITY OR OTHER THEORY). SYNOLOGY MAKES NO GUARANTEE AND SPECIFICALLY DISCLAIMS ANY WARRANTY THAT THE DATA OR INFORMATION STORED ON ANY SYNOLOGY PRODUCT WILL BE SECURE AND WITHOUT RISK OF DATA LOSS. SYNOLOGY RECOMMENDS THAT CUSTOMER TAKES APPROPRIATE MEASURES TO BACK UP THE DATA STORED ON THE PRODUCT. SOME STATES/JURISDICTIONS DO NOT ALLOW LIMITATIONS ON IMPLIED WARRANTIES, SO THE ABOVE LIMITATION MAY NOT APPLY TO CUSTOMER.

Section 4. Limitations of Liability

4.1 Force Majeure. Synology will not be liable for, or be considered to be in breach of or default under this Warranty on account of, any delay or failure to perform as required by this Warranty as a result of any cause or condition beyond its reasonable control (including, without limitation, any act or failure to act by Customer).

4.2 Disclaimer of Certain Damages. IN NO EVENT WILL SYNOLOGY OR ITS SUPPLIERS BE LIABLE FOR THE COST OF COVER OR FOR ANY INCIDENTAL, INDIRECT, SPECIAL, PUNITIVE, CONSEQUENTIAL OR SIMILAR DAMAGES OR LIABILITIES WHATSOEVER (INCLUDING, BUT NOT LIMITED TO LOSS OF DATA, INFORMATION, REVENUE,

PROFIT OR BUSINESS) ARISING OUT OF OR RELATING TO THE USE OR INABILITY TO USE THE PRODUCT, ANY ACCOMPANYING DOCUMENTATION OR SOFTWARE AND ANY OTHER GOODS OR SERVICES PROVIDED UNDER THIS WARRANTY, WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHER THEORY EVEN IF SYNOLOGY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

4.3 Limitation of Liability. SYNOLOGY'S AND ITS SUPPLIERS' LIABILITY ARISING OUT OF OR RELATING TO THE USE OR INABILITY TO USE THE PRODUCT, ANY ACCOMPANYING DOCUMENTATION OR SOFTWARE AND ANY OTHER GOODS OR SERVICES PROVIDED UNDER THIS WARRANTY IS LIMITED TO THE AMOUNT ACTUALLY PAID BY CUSTOMER FOR THE PRODUCT REGARDLESS OF THE AMOUNT OF DAMAGES CUSTOMER MAY INCUR AND WHETHER BASED ON CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY OR OTHER THEORY. The foregoing disclaimer of certain damages and limitation of liability will apply to the maximum extent permitted by applicable law. The laws of some states/jurisdictions do not allow exclusion or limitation of certain damages. To the extent that those laws apply to the Product, the exclusions and limitations set forth above may not apply to Customer.

Section 5. Miscellaneous

5.1 Proprietary Rights. The Product and any accompanying Software and documentation provided with the Product include proprietary and intellectual property rights of Synology and its third party suppliers and licensors. Synology retains and reserves all right, title, and interest in the intellectual property rights of the Product, and no title to or ownership of any intellectual property rights in or to the Product, any accompanying Software or documentation and any other goods provided under this Warranty is transferred to Customer under this Warranty. Customer will (a) comply with the terms and conditions of the Synology end user license agreement accompanying any Software furnished by Synology or an authorized Synology distributor or reseller; and (b) not attempt to reverse engineer any Product or component thereof or accompanying Software or otherwise misappropriate, circumvent or violate any of Synology's intellectual property rights.

5.2 Assignment. Customer will not assign any of its rights under this Warranty directly, by operation of law or otherwise, without the prior written consent of Synology.

5.3 No Additional Terms. Except as expressly permitted by this Warranty, neither party will be bound by, and each party specifically objects to, any term, condition or other provision that conflicts with the provisions of this Warranty that is made by the other party in any purchase order, receipt, acceptance, confirmation, correspondence or otherwise, unless each party specifically agrees to such provision in writing. Further, if this Warranty conflicts with any terms or conditions of any other agreement entered into by the parties with respect to the Product, this Warranty will prevail unless the other agreement specifically references the sections of this Warranty that it supersedes.

5.4 Applicable Law. Unless explicitly prohibited by local law, this Warranty is governed by the laws of the State of Washington, U.S.A. for the Customers residing within the United States; and by the laws of the Republic of China (Taiwan) for Customers not residing within the United States, without regard to any conflict of law principles to the contrary. The 1980 U.N. Convention on Contracts for the International Sale of Goods or any successor thereto does not apply.

5.5 Dispute Resolution. Any dispute, controversy or claim arising out of or relating to this Warranty, the Product or services provided by Synology with respect to the Product or the relationship between Customers residing within the United States and Synology will be resolved exclusively and finally by arbitration under the current commercial rules of the American Arbitration Association, except as otherwise provided below. The arbitration will be conducted before a single arbitrator, and will be limited solely to the dispute between Customer and Synology. The arbitration, or any portion of it, will not be consolidated with any other arbitration and will not be conducted on a class-wide or class action basis. The arbitration shall be held in King County, Washington, U.S.A. by submission of documents, by telephone, online or in person as determined by the arbitrator at the request of the parties. The prevailing party in any arbitration or legal action occurring within the United States or otherwise shall receive all costs and reasonable attorneys’ fees, including any arbitration fee paid by the prevailing party. Any decision rendered in such arbitration proceedings will be final and binding on the parties, and judgment may be entered thereon in any court of competent jurisdiction. Customer understands that, in the absence of this provision, Customer would have had a right to litigate any such dispute, controversy or claim in a court, including the right to litigate claims on a class-wide or class-action basis, and Customer expressly and knowingly waives those rights and agrees to resolve any disputes through binding arbitration in accordance with the provisions of this Section 5.5. For Customers not residing within the United States, any dispute, controversy or claim described in this section shall be finally resolved by arbitration conducted by three neutral arbitrators in accordance with the procedures of the R.O.C. Arbitration Law and related enforcement rules. The arbitration shall take place in Taipei, Taiwan, R.O.C., and the arbitration proceedings shall be conducted in English or, if both parties so agree, in Mandarin Chinese. The arbitration award shall be final and binding on the parties and may be enforced in any court having jurisdiction. Nothing in this Section shall be deemed to prohibit or restrict Synology from seeking injunctive relief or seeking such other rights and remedies as it may have at law or equity for any actual or threatened breach of any provision of this Warranty relating to Synology's intellectual property rights.

5.6 Attorneys' Fees. In any arbitration, mediation, or other legal action or proceeding to enforce rights or remedies under

this Warranty, the prevailing party will be entitled to recover, in addition to any other relief to which it may be entitled, costs and reasonable attorneys' fees.

5.7 Export Restrictions. You acknowledge that the Product may be subject to U.S. export restrictions. You will comply with all applicable laws and regulations that apply to the Product, including without limitation the U.S. Export Administration Regulations.

5.8 Severability. If any provision of this Warranty is held by a court of competent jurisdiction to be invalid, illegal, or unenforceable, the remainder of this Warranty will remain in full force and effect.

5.9 Entire Agreement. This Warranty constitutes the entire agreement, and supersedes any and all prior agreements, between Synology and Customer related to the subject matter hereof. No amendment, modification or waiver of any of the provisions of this Warranty will be valid unless set forth in a written instrument signed by the party to be bound thereby.

FCC Declaration of Conformity

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Federal Communication Commission Interference Statement

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this equipment.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Operations in the 5.15-5.25GHz band are restricted to indoor usage only.

This device meets all the other requirements specified in Part 15E, Section 15.407 of the FCC Rules.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 23cm between the radiator & your body.

Note: The country code selection is for non-US model only and is not available to all US model. Per FCC regulation, all WiFi product marketed in US must fixed to US operation channels only.

FCC regulations restrict the operation of this device to indoor use only.

Industry Canada statement:

This device complies with ISED's licence-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Caution :

(i) the device for operation in the band 5150-5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems;

(ii) where applicable, antenna type(s), antenna models(s), and worst-case tilt angle(s) necessary to remain compliant with the e.i.r.p. elevation mask requirement set forth in section 6.2.2.3 shall be clearly indicated.

Avertissement:

Le guide d'utilisation des dispositifs pour réseaux locaux doit inclure des instructions précises sur les restrictions susmentionnées, notamment :

(i) les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux;

(ii) lorsqu'il y a lieu, les types d'antennes (s'il y en a plusieurs), les numéros de modèle de l'antenne et les pires angles d'inclinaison nécessaires pour rester conforme à l'exigence de la p.i.r.e. applicable au masque d'élévation, énoncée à la section 6.2.2.3, doivent être clairement indiqués

Radiation Exposure Statement:
This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with greater than 20cm between the radiator & your body.

Déclaration d'exposition aux radiations:
Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à plus de 20 cm entre le radiateur et votre corps.

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。
低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

應避免影響附近雷達系統之操作。

「本產品電磁波曝露量(MPE)標準值1mW/cm^2，送測產品實測值為 0.358 mW/cm^2，建議使用時至少距離人體 21 cm」

設備名稱：802.11ax無線路由器，型號（型式）：RT6600ax
Equipment name　　Type designation (Type)

單元Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞 Mercury (Hg)	鎘 Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
上下蓋	○	○	○	○	○	○
印刷電路板及電子組件	—	○	○	○	○	○
天線	○	○	○	○	○	○
電源供應器	—	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。
Note 1：“Exceeding 0.1 wt %” and “exceeding 0.01 wt %” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.
備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。
Note 2：“○” indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.
備考3. 〝—〞係指該項限用物質為排除項目。
Note 3：The “–” indicates that the restricted substance corresponds to the exemption.

RED Compliance Statement

Compliance with 2014/53/EU Radio Equipment Directive (RED)

In accordance with Article 10.8(a) and 10.8(b) of the RED, the following table provides information on the frequency bands used and the maximum RF transmit power of the product for sale in the EU:

Frequency Range (MHz)	Max. Transmit Power (dBm) EIRP
2412 ~ 2472	19.86 dBm
5180 ~ 5240	22.80 dBm
5250 ~ 5320	22.94 dBm
5500 ~ 5700	29.87 dBm

This equipment should be installed and operated with minimum distance 20cm between the radiator & your body.

	AT	BE	BG	HR	CY	CZ	DK	
	EE	FI	FR	DE	EL	HU	IE	
	IT	LV	LT	LU	MT	NL	PL	
	PT	RO	SK	SI	ES	SE	UK	UK(NI)

This device is restricted to indoor use

SYNOLOGY INC.

9F, No. 1, Yuandong Rd.
Banqiao Dist., New Taipei City 220545
Taiwan
Tel: +886 2 2955 1814

SYNOLOGY AMERICA CORP.

3535 Factoria Blvd SE, Suite #200,
Bellevue, WA 98006
USA
Tel: +1 425 818 1587

SYNOLOGY UK LTD.

Unit 5 Danbury Court, Linford Wood,
Milton Keynes, MK14 6PL
United Kingdom
Tel.: +44 (0)1908048029

SYNOLOGY FRANCE

102 Terrasse Boieldieu (TOUR W)
92800 Puteaux
France
Tel: +33 147 176288

SYNOLOGY GMBH

Grafenberger Allee 295
40237 Düsseldorf
Deutschland
Tel: +49 211 9666 9666

SYNOLOGY SHANGHAI

200070, Room 201,
No. 511 Tianmu W. Rd.,
Jingan Dist., Shanghai,
China

SYNOLOGY JAPAN CO., LTD.

4F, No. 3-1-2, Higashikanda,
Chiyoda-ku, Tokyo, 101-0031
Japan

Synology®

synology.com