Atlas S8+
Software Manual

Version 1.0

Important data protection information
You should back up all data before installing any drive controller or storage peripheral. PROMISE Technology is not responsible for any loss of data resulting from the use, disuse or misuse of this or any other PROMISE Technology product.

Notice
Although PROMISE Technology has attempted to ensure the accuracy of the content of this document; it is possible that this document may contain technical inaccuracies, typographical, or other errors. PROMISE Technology assumes no liability for any error in this publication, and for damages, whether direct, indirect, incidental, consequential or otherwise, that may result from such error, including, but not limited to loss of data or profits.
PROMISE Technology provides this publication "as is" without warranty of any kind, either express or implied, including, but not limited to implied warranties of merchantability or fitness for a particular purpose. The published information in the manual is subject to change without notice. PROMISE Technology reserves the right to make changes in the product design, layout, and driver revisions without notification to its users. This version of this document supersedes all previous versions.

Recommendations

In this *Product Manual*, the appearance of products made by other companies, including but not limited to software, servers, and disk drives, is for the purpose of illustration and explanation only. PROMISE Technology does not recommend, endorse, prefer, or support any product made by another manufacturer.

About this guide

This *Product Manual* describes how to setup, use, and maintain the Atlas S8+ unit.

This manual includes a full table of contents, chapter task lists, and numerous cross-references to help you find the specific information you are looking for.

Four types of notices are used throughout the document:

Note
A *Note* provides helpful information such as hints or alternative ways of doing a task.

Important
An *Important* notice calls attention to an essential step or point required to complete a task. Important items include things often missed.

CAUTION

A *Caution* informs you of possible equipment damage or loss of data and how to avoid them.

WARNING
A ***Warning*** notifies you of probable equipment damage or loss of data, or the possibility of physical injury, and how to avoid them.

GETTING STARTED

Thank you for purchasing PROMISE Atlas S8+. The new users are advised to follow the steps below to complete the NAS Configuration.

Power On Your Atlas S8+

Please follow the steps below to power on your Atlas S8+:

1. Connect to the LAN1 port on your Atlas S8+ and the other end to your switch, router, or hub.
2. Connect your Atlas S8+ to the power and press the power button to start the Atlas S8+.
3. Checking the system status LEDs to make sure your Atlas S8+ is function properly.
    - System Status LED Indication

Description	Definition
USB Status LED	**USB Status LED** • Blue: A front USB device is detected (after the device is mounted). • Blue flashes every 0.5 sec: 1) The USB device (connected to the front USB port) is being accessed. 2) The data is being copied to or from the external USB or eSATA device. • OFF: No USB device is mounted.
Solid State Drive (SSD) LED	• Blue: The hard disk is attached. • Blue flashes: The disk data is being accessed. • Amber: A hard drive read/write error occurs. • Blue and Amber flashes alternatively: The hard disk is being rebuilt or identify a specific disk drive. • OFF: No disk drive is inserted.
Power Button/LED	**Power Button** • Press the button one time to turn ON or OFF the system power. **Power LED** • White: power is ON. • White flashes every 0.5 sec: the system is at the stage of starting up or shutting down, or the NAS is not configured. • Amber: 1) The system pool has reached its full capacity (100%). 2) The system pool is going to be full (95%). 3) The system fan is out of function. 4) A bad sector is detected on the

	hard disk drive or hard disk failed. 5) One of the pools is in degraded read-only mode. 6) Hardware self-test error. e.g. abnormal voltage, the temperature is at critical high/low, any cooling fan module failed, any pool failed. • White and Amber flash every 0.5 sec alternatively: 1) The system firmware is being updated. 2) RAID rebuilding is in a process. 3) Software control LED indicator. • Off: the system shutdown.
LAN Status LED	• Blue: The NAS is connected to the network. • Blue flashes: The disk data is being accessed from the network.
Expansion Unit Status LED	• Blue: An expansion card is being accessed. • OFF: No expansion card is being accessed.
Disk Drive Status LED	• Blue: The hard disk is attached. • Blue flashes: The disk data is being accessed. • Amber: A hard drive read/write error occurs. • Blue and Amber flashes alternatively: The hard disk is being rebuilt or identify a specific disk drive. • OFF: No disk drive is inserted.
LAN Port	**Activity/Link:** • Light OFF: No connection. • Light ON: Connected to the internet • Light flashes: when data is being accessed. **Speed:** • Light OFF: Speed less than 10Mbps • Light ON: Connected to the internet

4. Checking the system alarm buzzer to make sure your Atlas S8+ is function properly.

   - System Alarm Buzzer Indication

No.	Beep Sound	No. of Times	Description
1	Short beep (0.5 sec)	1	• The Atlas S8+ is ready (finish start up). • The Atlas S8+ is being shut down (software shutdown). • The system firmware has been updated. • Front USB start copy • Front USB finish copy • USB drive is removed • The user starts hard drive rebuilding.
2	Short beep (0.5 sec)	3 times, interval of 0.5 sec	• The NAS data cannot be copied to the external storage device from the front USB port.
3	Long beep (1.5 sec)	Beep until event finishes, interval of 0.5 sec	• 1) The system pool has reached its full capacity (100%). 2) The system pool is going to be full (95%). 3) The system fan is out of function. 4) A bad sector is detected on the hard disk drive or hard disk failed. 5) One of the pools is in degraded mode. 6) Hardware self-test error. *e.g.* PSU failed, abnormal voltage, the temperature is at critical high/low, any cooling fan module failed or removed, any pool failed. 7) Remove hard disk or solid state drive.

Note: If one event has triggered the beep sound, the next event will not trigger the beep sound until the previous event has finished.

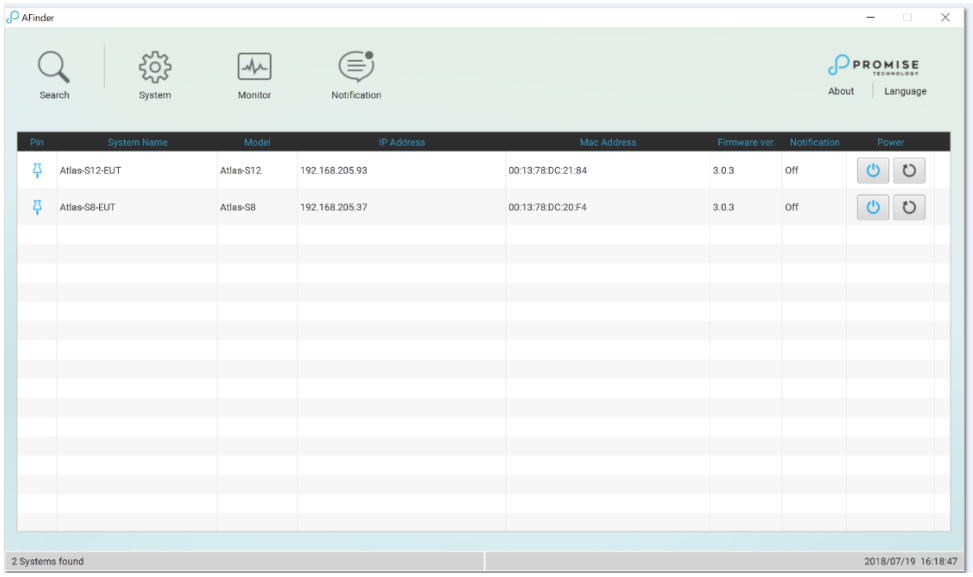
Note 2: The beep sound will not be triggered if buzzer function is disabled from the ASM. You can check the error messages through the **Notification Center** on ASM.

Initial Configuration

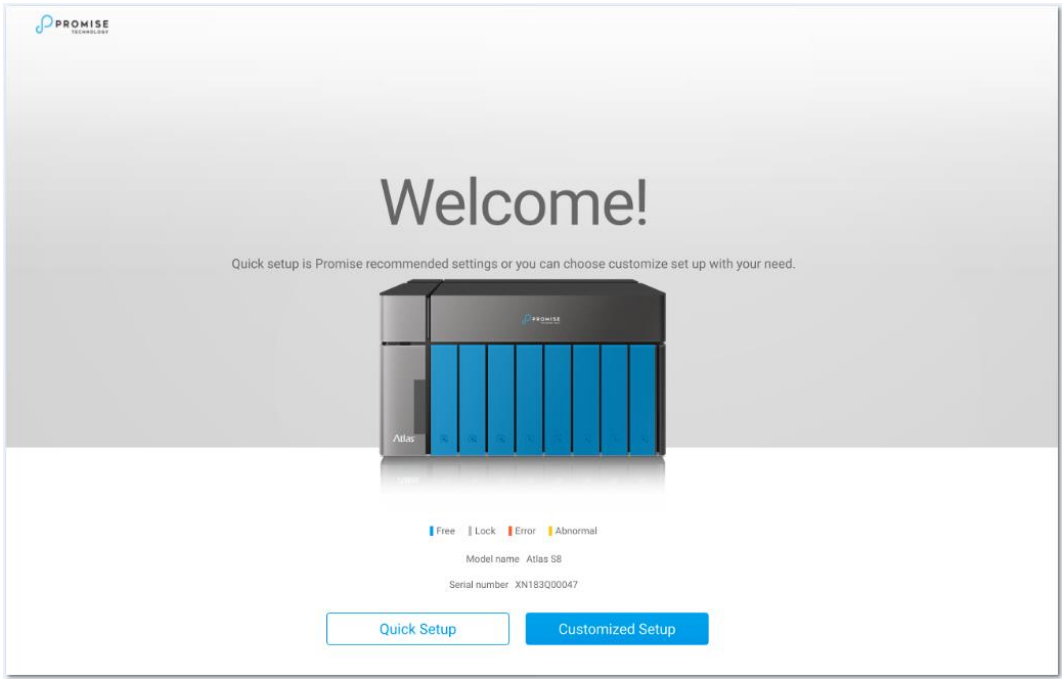
After hardware setup is finished, the next step is to discover the system on the network and start the initial configuration. To discover and run the Atlas Storage Manager (ASM), please follow the steps below:

1. Open a web browser on your computer connected to the same local area network as Atlas S8+, and use either of the following methods on the browser:
   a. Use Web Finder: atlas.promise.com (Please make sure the Atlas S8+ has internet access ability before using the Web Finder).

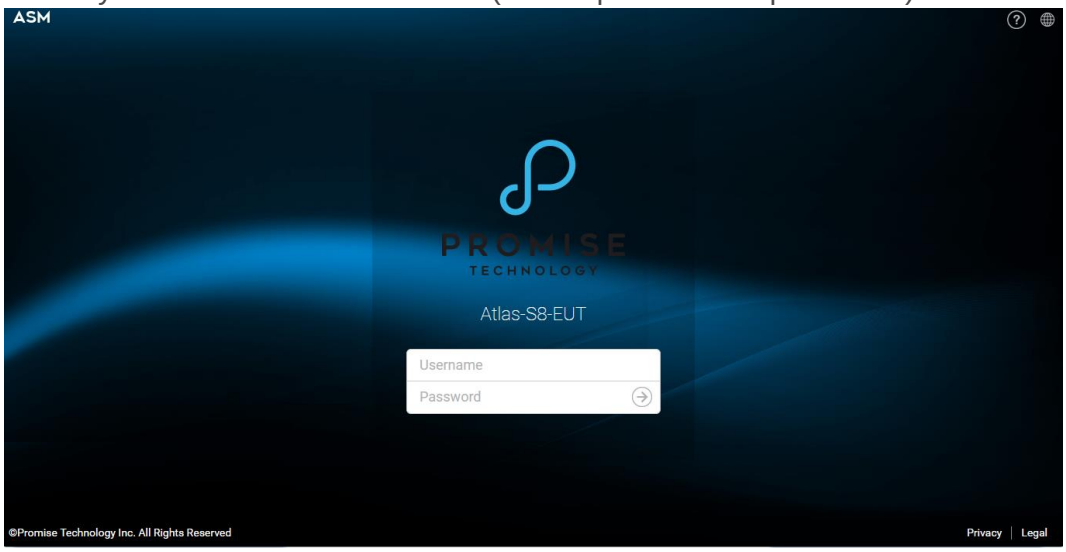
   b. If your Atlas S8+ cannot be connected to the internet, please try downloading and installing AFinder application from the PROMISE website to your PC: https://www.promise.com/Support/downloadcenter



2. Click “**Connect”** on the Web Finder or double click on your Atlas S8+ in the AFinder, the welcome page will be launched on your web browser.



3. Click **Quick Setup** or **Customized Setup** to start the setup process and follow the onscreen instructions.
4. If you accidentally leave the quick install page, you can always return to the setup page by go through the steps above from step 1 again.
5. After quick setup is finished, login to the ASM as “**admin”** (default account name) with the password you set on former instructions (default password is “password”).



NOTE:
1. The Atlas S8+ must be connected to the Internet to use the Web Finder.
2. Both the Atlas S8+ and your PC must be on the same local network.
3. If you expanded your memory before rebooting, you can now check to make sure the system recognizes the new memory capacity. You can check the status by following steps:

   a. Login to ASM as **admin** or a user belonging to the **administrator** group.
   b. Find the memory status in **About NAS**.

If your system cannot recognize the expanded memory or failed to start up, please check again and ensure the memory is properly installed.

Getting Utilities

All the Atlas S8+ related utilities can be found on PROMISE website. Please visit https://www.promise.com/Support/downloadcenter and choose the utilities you would like to download and install the utilities on your PC.

ASM Basics And Desktop

Atlas Storage Manager 3.0 (ASM 3.0) is an innovative storage operating system designed for PROMISE Atlas S8+ products. Based on Linux and 128-bit ZFS, ASM 3.0 not only inherits the amazing native features of ZFS but is also adjusted with several optimizations that make the Atlas S8+ a high-performance, efficient and superior network attached storage device.

ASM 3.0 guarantees data integrity, and security. The built in checksum mechanism can automatically correct corrupted data using file snapshots. A wide range of supported RAID types, file and block level snapshots and various backup solution support ensures that data always well-protected. AES-256 pool encryption, WORM and SED drive support prevent confidential data from being either stolen or modified.

ASM 3.0 utilizes every resource to achieve data efficiency. Data deduplication and compression technology reduce storing duplicate data blocks and files to maximize storage capacity, making the Atlas S8+ capable of storing beyond its raw storage capacity.

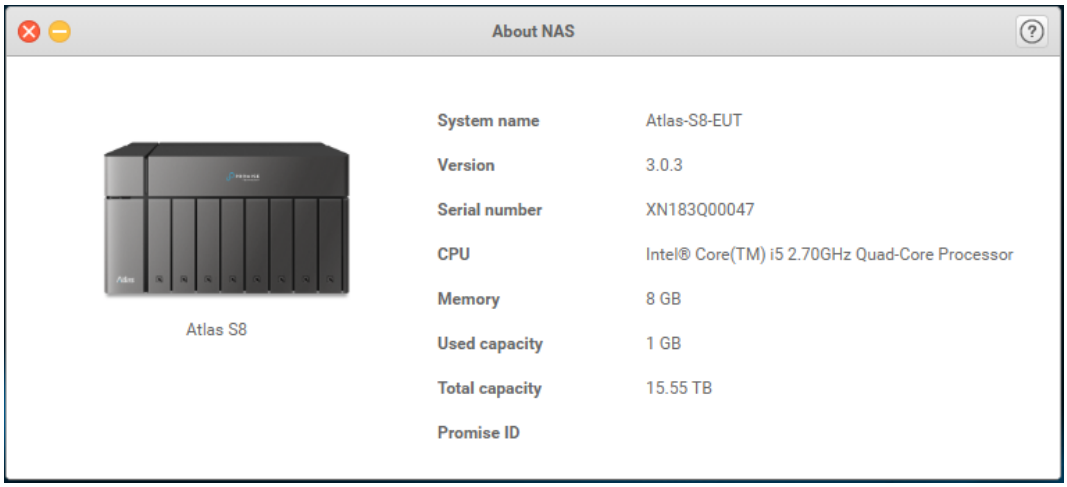
ASM 3.0 effectively addresses the performance demands of various applications. The SSD caching increases data access speed. And classifying data by access frequency lets auto-tiering help fetch frequently used files even faster.

Value-added functionalities such as virtualization capability, multiple server center, centralized file station etc. are also provided making ASM 3.0 robust and able to carry out dedicated applications.

In this manual, we will be introducing every features of the ASM 3.0. Once you have finished the basic setup and login to your Atlas S8+, please check the topics below to learn more about ASM 3.0.

About NAS

About NAS contains basic information about your Atlas S8+, including firmware version, hardware information and your storage usage.



Checking information about you Atlas S8+

Please follow the steps below to check the information of your Atlas S8+:

1. Click the PROMISE icon on the upper-left corner on ASM desktop to get to main menu.
2. Select **About NAS** on the menu.
3. The following information will be displayed on the popup window:
    - **Version** : The current ASM version.
    - **Serial number** : A unique identifying number for your Atlas S8+.
    - **CPU** : CPU specification for your Atlas S8+.
    - **Memory** : Total memory installed.
    - **Used capacity** : Current system capacity usage.
    - **Total capacity** : Total system capacity available.
    - **PROMISE ID** : PROMISE ID is the account you use to sign in to PROMISE services.

To learn more about how to register a PROMISE ID, please refer to PROMISE Cloud help page.

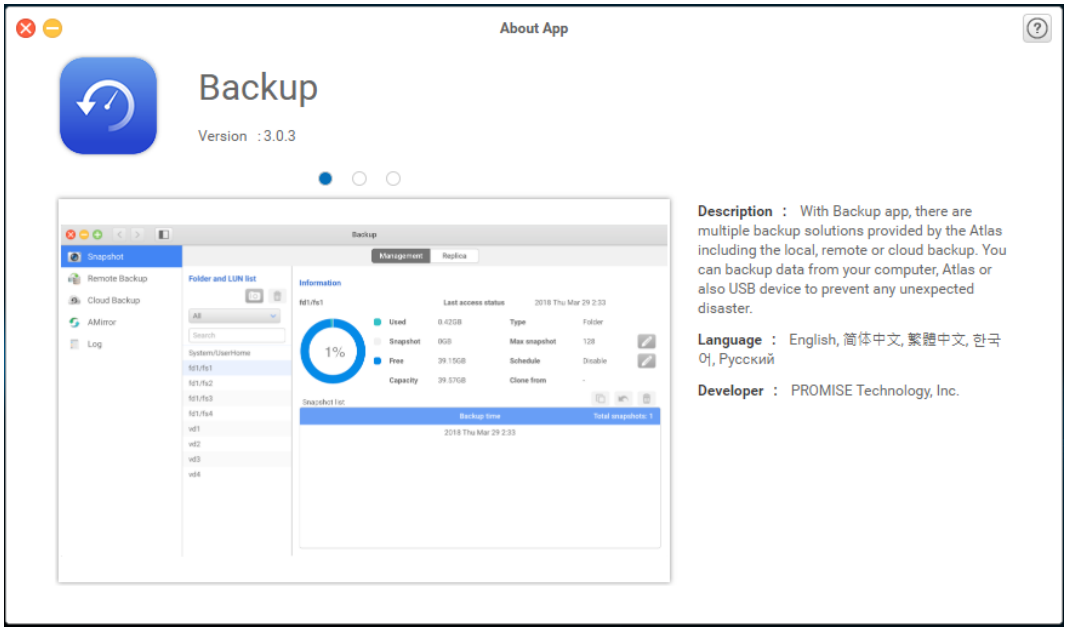
NOTE:
You only need one PROMISE ID. This ID can be used everywhere you sign in to ensure that your PROMISE services and devices work together seamlessly. If you have any questions, please contact PROMISE support team for more information.

About

In **About**, you can view the detailed information about each app or external devices, including its version, description, supported languages and more.

Checking information about a specific App

This page contains the detailed information of the selected app.



To check this page, please follow the steps below:

1. Right-click on a specific app icon.
2. Select **About** on the menu.
3. The following items will be displayed on the popup window:
    - **App name** : Selected App name.
    - **Version** : Firmware version or App version.

- **Description** : Brief introduction of this app.
- **Language** : The languages supported by this app.
- **Developer** : Developer of this app.
- **Picture** : Slideshow of this app.

Checking information about a specific Device

This page contains the detailed information of the selected external device.

To check this page, please follow the steps below:

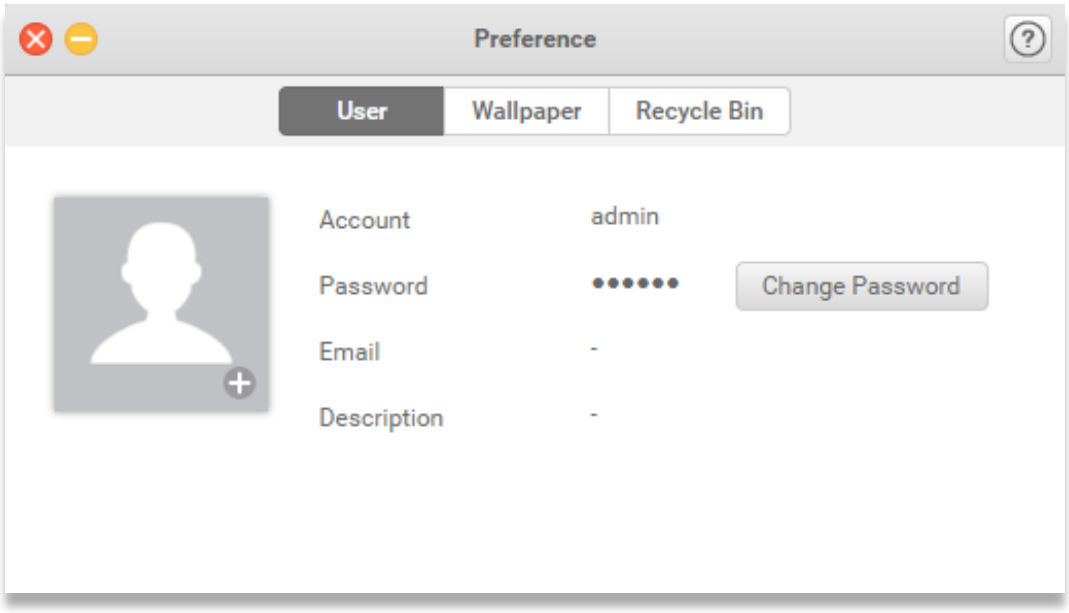
1. Right-click on a specific external device's icon on Dock.
2. Select **About** on the menu.
3. The following items will be displayed on the popup window:
   - **Device name** : Device name of the USB.
   - **Manufacturer** : The manufacturer of the USB.
   - **Type** : USB version.
   - **Used/Total capacity** : The capacity being used and its total capacity of the device.
   - **File system** : File system of the partition on USB.

Preference

The **Preference** page allows you to modify personal profile, setup wallpaper and empty your recycle bin. It can be found by clicking the person-shaped icon at the upper-right corner of the desktop.

User

This tab allows you to view your user profile and provides options to edit basic user account settings.



Upload profile picture:

You can change your profile picture by the following steps:

1. Click the **Upload** button on your profile picture.
2. Choose a picture from your computer.
3. Click **Open** on the upload window to save the setting. If it has been saved successfully, you can view your profile picture on both of the **User** page and **Control Panel** > **User** page.

Change user password:

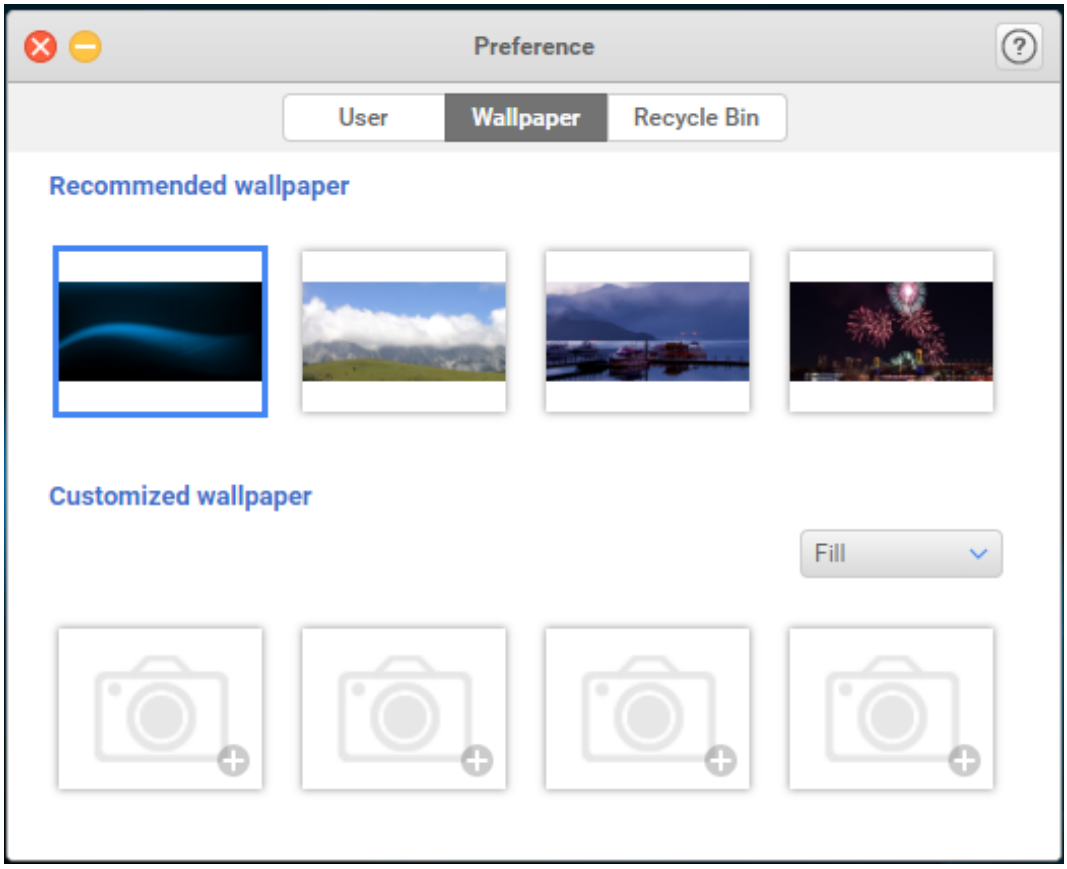
1. Click **Change Password** button.
2. Enter the new password in **New password** field.
3. Verity the new password in **Verify Password** field.

4. Click **Confirm** button to save the change.

NOTE:
Password can include up to 64 characters, only |a-z| |A-Z| |0-9-_| are valid.

Wallpaper

This page allows you to customize the appearance of your Desktop.



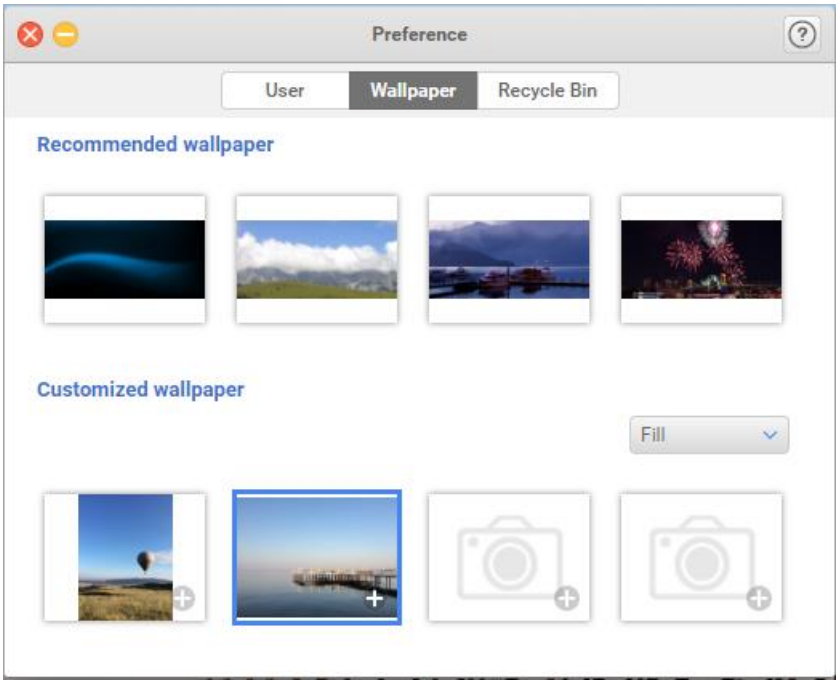
Change the background of your desktop:

You can choose one of the included wallpapers as your desktop wallpaper. If you select the picture, the desktop background will be changed at the same time.

Upload a customized image that will be used as your desktop background:

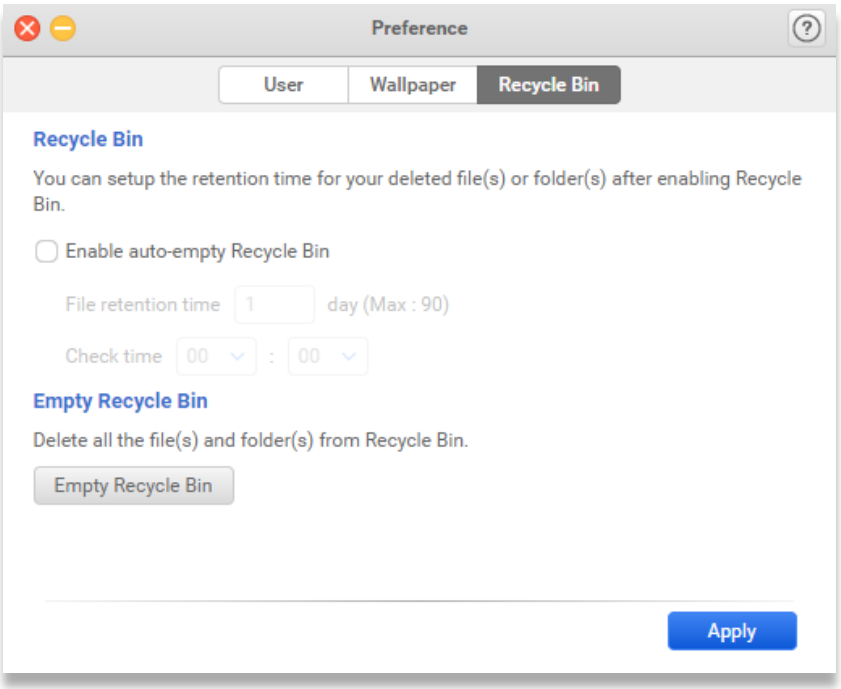
1. Click the lower right button of each customized wallpaper.

2. Choose the image from your computer.
3. Choose from the drop-down menu to decide how the background image will be arranged on your desktop, and the background will be changed in real time.



Recycle Bin

This page allows you to setup the retention time for all the deleted file(s) or folder(s) in Recycle Bin.



Enable Recycle Bin:

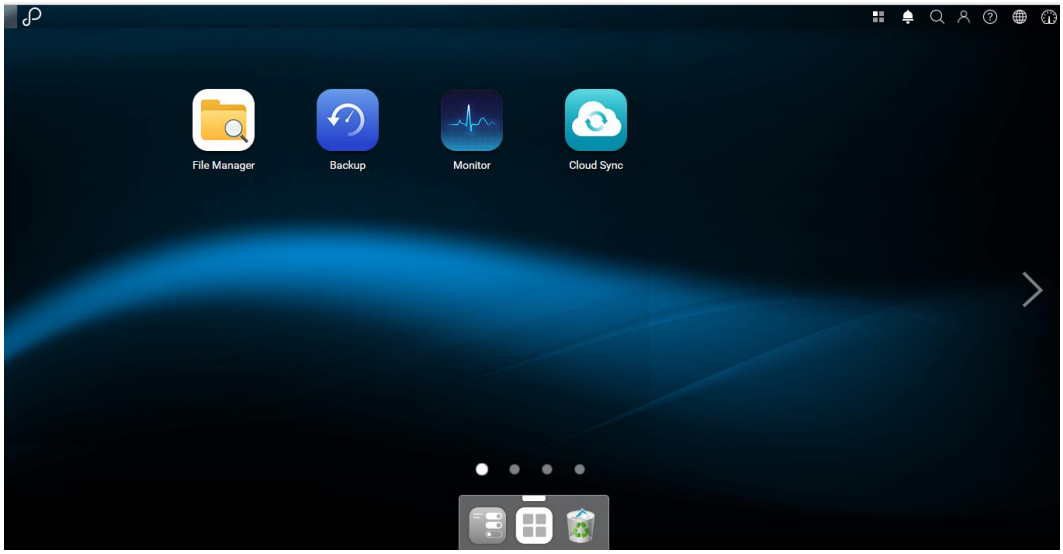
1. Click **Enable auto-empty Recycle Bin** checkbox.
2. Enter the retention time in **File retention time** textbox from 1 to 90 day(s) for your deleted file(s) or folder(s).
3. Choose the time which your system will check the recycle bin automatically from **Daily check time** drop-down menu.
4. Click **Apply** button to save the settings.

Empty Recycle Bin:

Click **Empty Recycle Bin** button to remove all the file(s) and folder(s) from recycle bin permanently.

Desktop

ASM's innovative desktop provides a simple, intuitive user interface where you can see folder, file and application windows. Learn more about your desktop at the following sections.



Status Bar

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

1. Display desktop: Minimize all open windows or restore them to original size.
2. PROMISE logo menu:

   About NAS : You can check the information about your NAS and register your PROMISE ID here. For more information, please see About NAS and PROMISE Cloud help documents.

   Control Panel : Manage all the system settings in a place. For more information, please see Control Panel help document.

   Apps : Contains all the applications in an area.

   Tutorial : Provide you several tips when first logging in ASM. For more information, please see Tutorial help document.

   Restart : For admin, they can decide whether to restart the ASM or not.

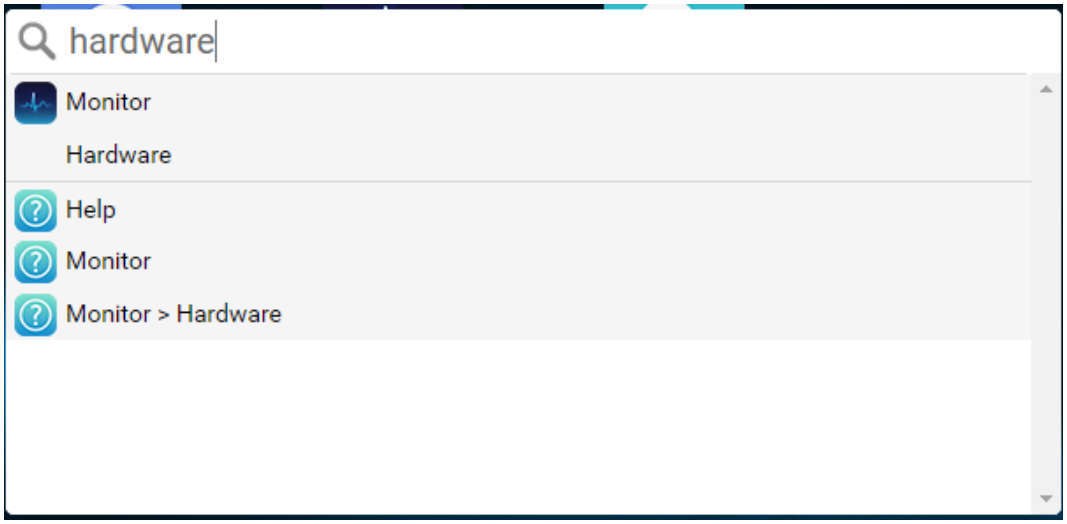
   Shutdown : For admin, they can decide whether to shut down the ASM or not.
3. Background tasks: Display currently running tasks.
4. **Notification Center** : Display event logs include information, warning and error.
5. **Spotlight** : Help you find the specific applications and help documents. You can follow these steps below to search for items:

   (1) Click **Spotlight** to open the search widget.

   (2) Enter keywords in search bar. (See valid characters on **Note**.)

   (3) Matched results will be displayed on the lower panel.

   (4) Click to open the needed item.

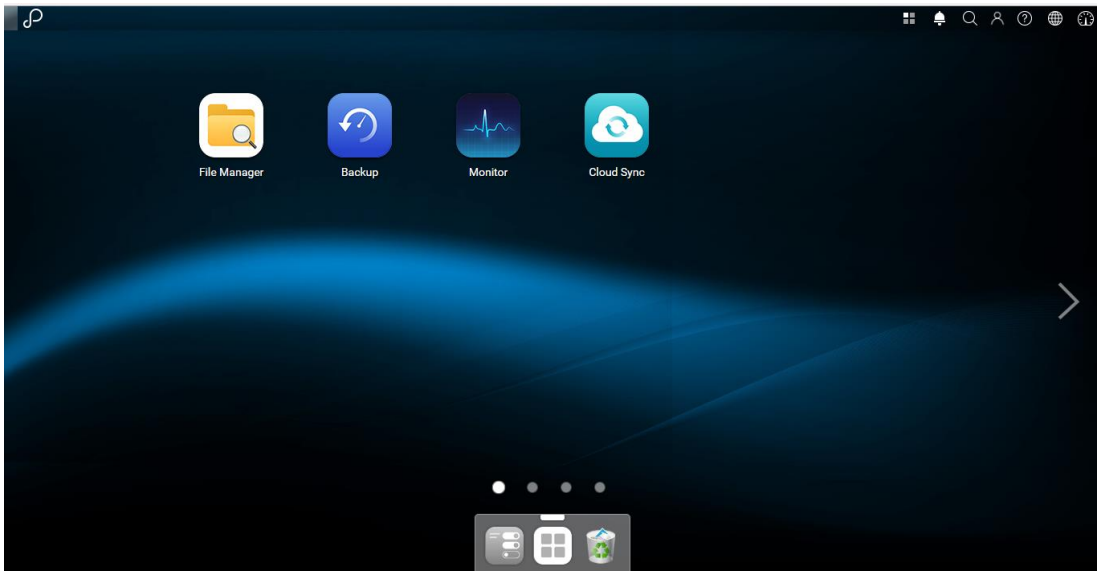


NOTE:
Characters which are allowed include: "a-z A-Z 0-9".

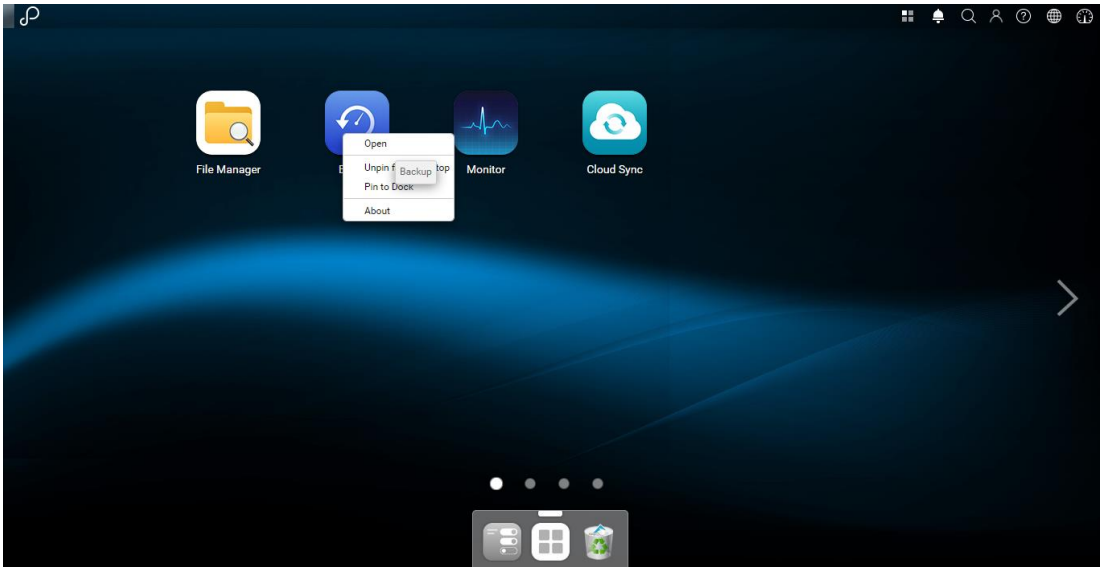
6. **Person-shaped icon** : Logout or modify your account, wallpaper and empty recycle bin.
7. **Help** : Click it to open help document. You can search keywords to filter the matched results.
8. **Language** : Choose your prefer language for the ASM user interface. If you change the language successfully, the display language will be replaced immediately without having to log in ASM again.
9. **Dashboard** : Display current system status such as CPU usage, memory usage, storage capacity usage, hardware status, network speed and connected users.

Desktop main screen

You can manage the app shortcut, Dock, and view the apps information on the desktop main screen.



You will see these functions below by using right mouse button on each app:



Open an app

1. Right-click the target app on desktop.
2. Choose **Open** on the menu.

Pin a shortcut to desktop/unpin from desktop

1. Open **Apps** button on the Dock.
2. Open **File Manager** app.
3. Click the right mouse button on the folder/file and select **Pin to Desktop** button, or drag the target folder/file and drop it on desktop.
4. Unpin: Right-click the folder/file that has pinned to desktop and select **Unpin from Desktop** on the menu.

Pin an app to Dock/Unpin an app from Dock

You can pin an app to Dock or unpin it by the following steps:

1. Right-click on each app.
2. Choose **Pin to Dock** on the menu.
3. Unpin: Right-click the target app on Dock and select **Unpin from Dock** on the menu.

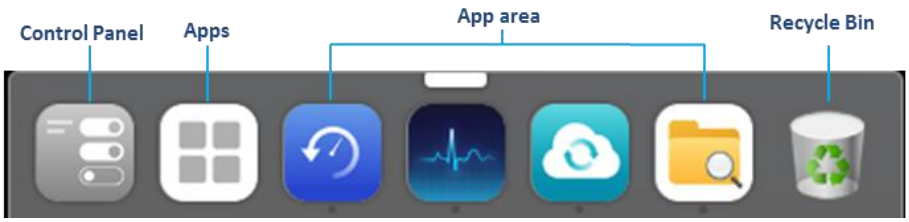
View app information

You can view the description, language and developer of the target app by the following steps:

1. Click the right mouse button on each app.
2. Choose **About** on the menu.

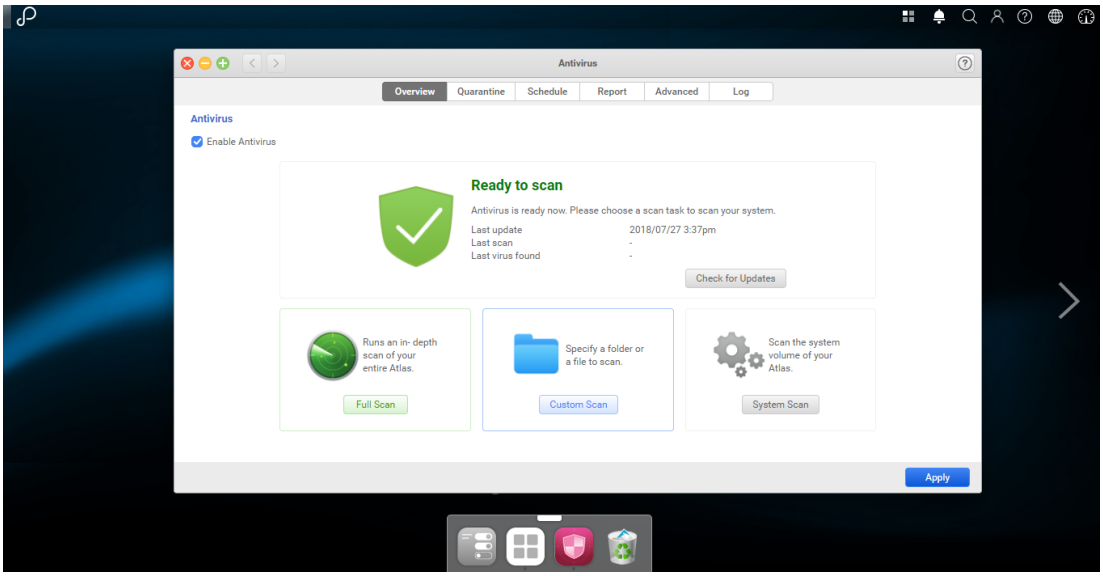
Dock

Dock is a convenient place to keep the objects you use frequently. You can add or remove objects from **Dock**. It is located at the bottom of desktop.



Open an object

Click an object on Dock, or you can choose **Open** on right-click menu of each object.



Move an object on Dock

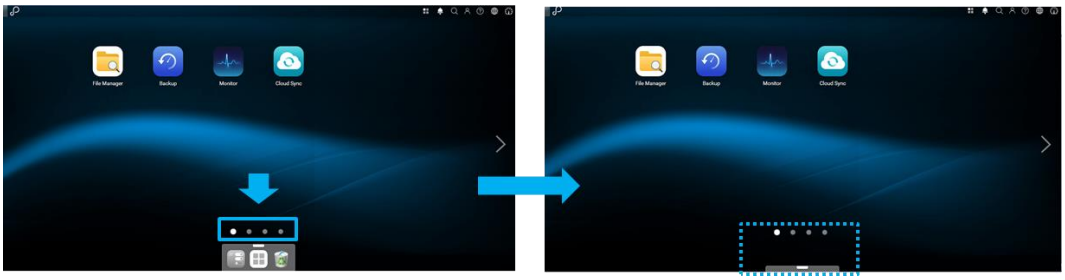
You can move an object by dragging it to the left of the Dock's separator.

Remove an object from Dock

You can remove the Dock's object by dragging it to recycle bin. When you drag an object to recycle bin at the end of the Dock, a hint text will be shown beside the icon and then you can move it successfully. (To empty the recycle bin, open the recycle bin and click Empty Recycle Bin button.)

Hide/Show Dock

You can hide or show the Dock by clicking the button on top of the Dock panel.



NOTE:

1. Default items: The default items include Control Panel, Apps and Recycle Bin will always be shown on Dock. You can't do remove or drag actions on these items.
2. Apps shortcut: The pinned shortcuts will be located between the Apps and Recycle Bin icon. If the app shortcut has been on the Dock, you can't pin this app again.
3. The maximum number of objects on Dock will be "24".

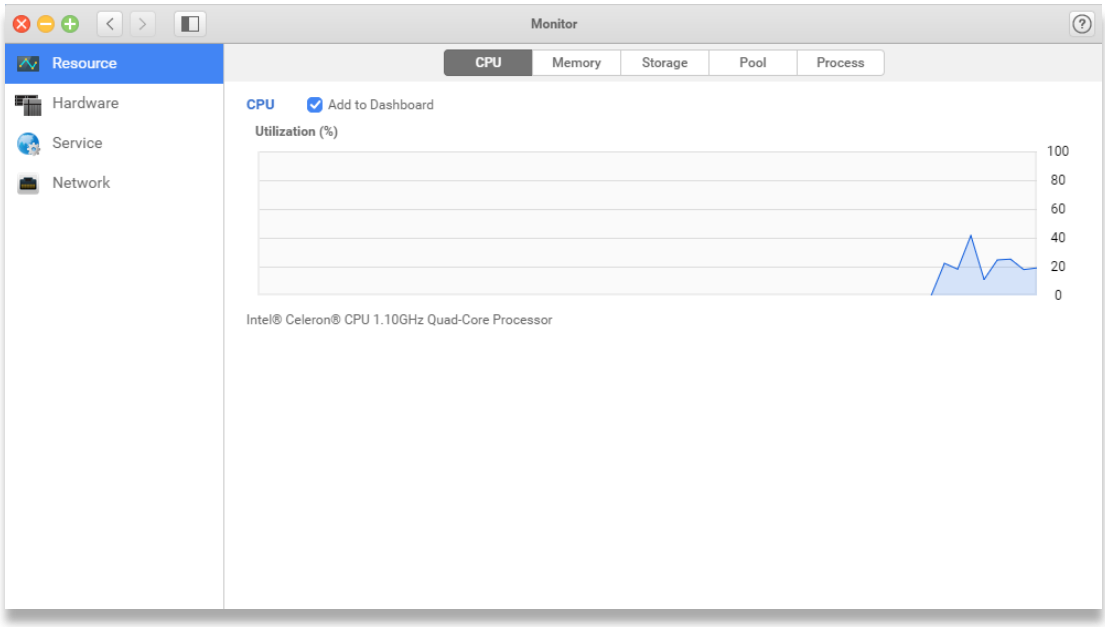
Monitor

Resource

This page allows you to monitor the CPU usage, memory usage, storage utilization, and pool throughput and network utilization.

CPU

You can check the status of CPU usage. The detailed information of each chart will be shown upon mouse over. CPU load can be high when the Monitor app is first launched, because the system needs to collect its resource data and load the UI page at the same time.

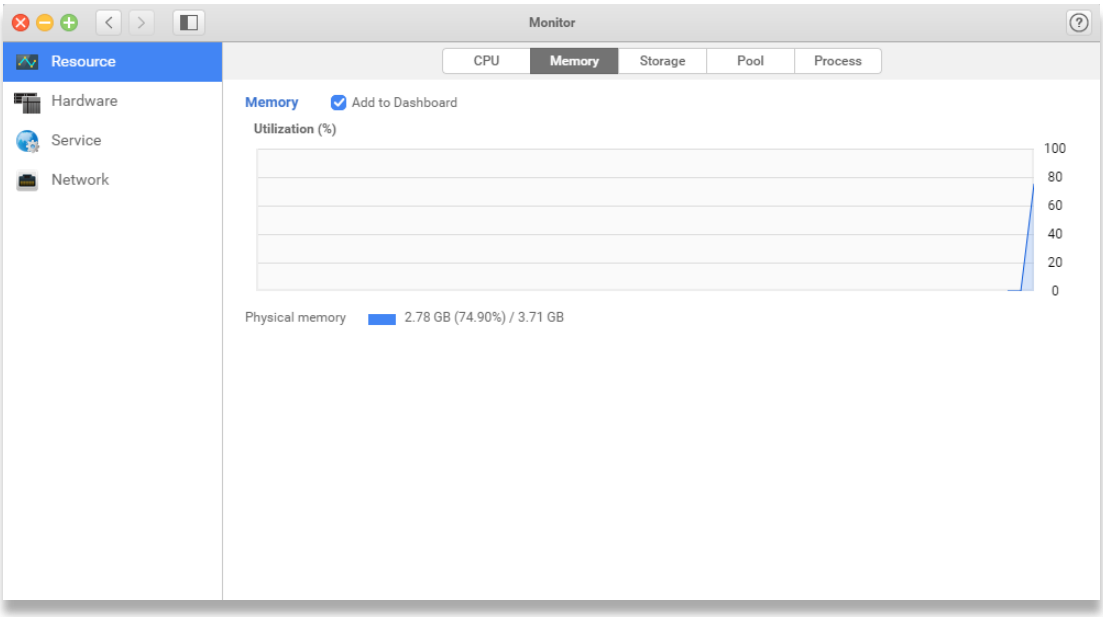


To show on Dashboard

If you want to view this status on Dashboard, click **Add to Dashboard** checkbox at the top of this page.

Memory

This page shows the overall physical and expansion memory usage on your Atlas S8+. Cache memory will be released when overall memory is insufficient.



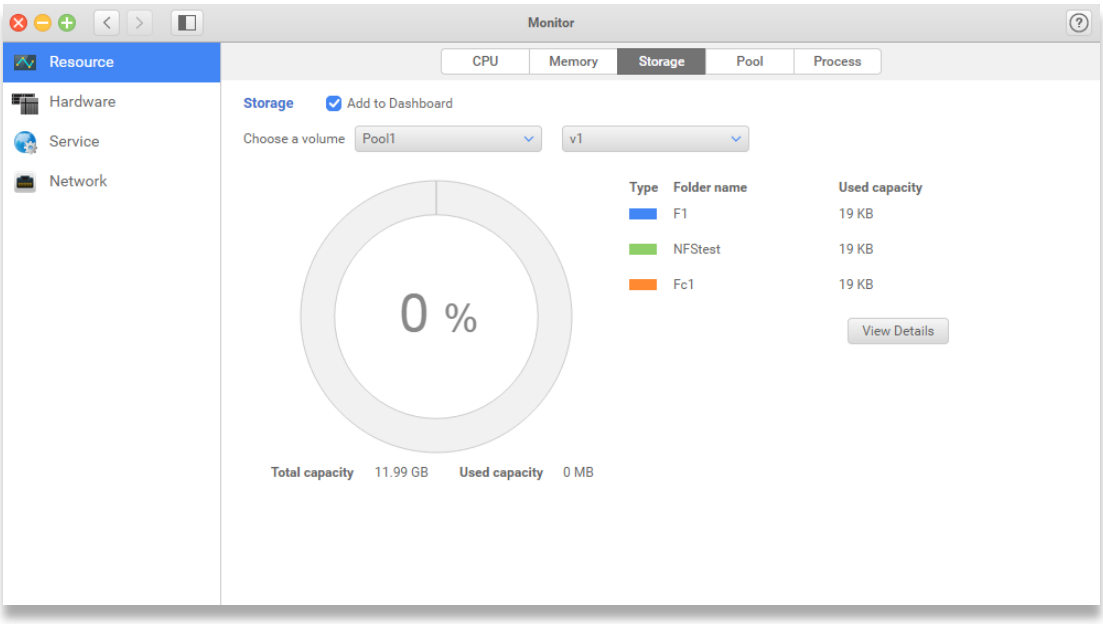
To show on Dashboard

If you want to view this status on Dashboard, click **Add to Dashboard** checkbox at the top of this page.

NOTE:
The percentage may be high if the system stores the frequently accessed data in cache, so the data can be quickly obtained by the system instead of from hard disks. The cache memory will be released when overall memory is insufficient.

Storage

This page shows the storage usage on each volume. The chart shows the percentage of used capacity on each volume and shared folders. You can view each volume specifically by clicking the drop-down menu at the top of the chart.



To view all folders

It will show at most eight folders in a volume. If you want to view the overall folders, click the **View Details** button to get more information.

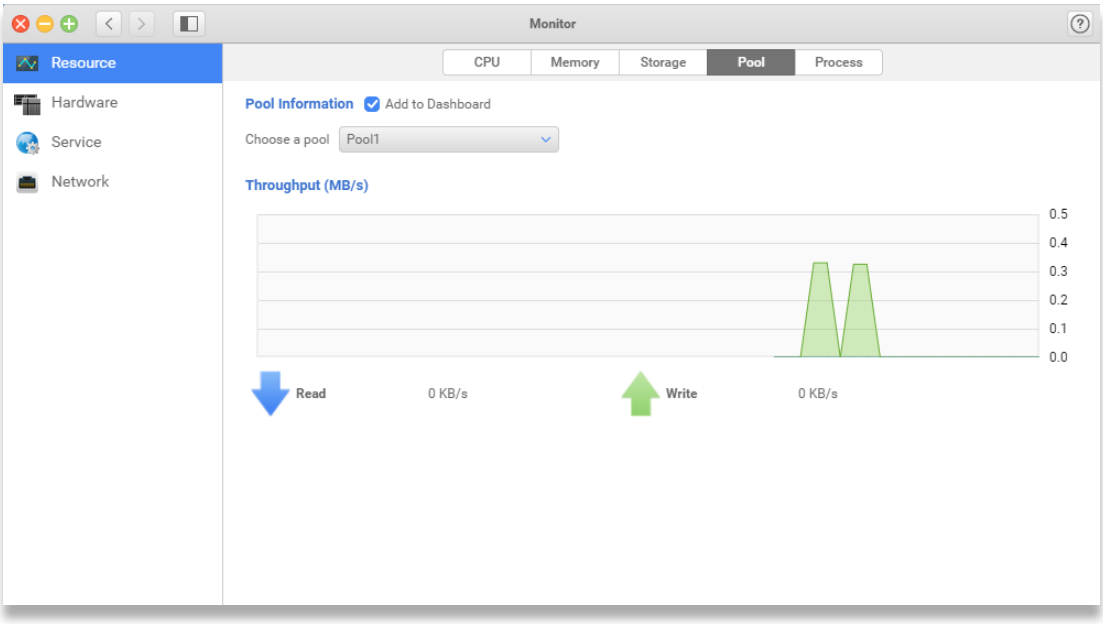
To show on Dashboard

If you want to view this status on Dashboard, click **Add to Dashboard** checkbox at the top of this page.

NOTE:
If you didn't reserve the size for your shared folder, it will show the same size as its volume on **Used capacity**.

Pool

This page displays the transfer status of each pool. The detailed information of each chart will be shown upon mouse over. You can check each pool status by clicking the drop-down menu at the top of the chart.

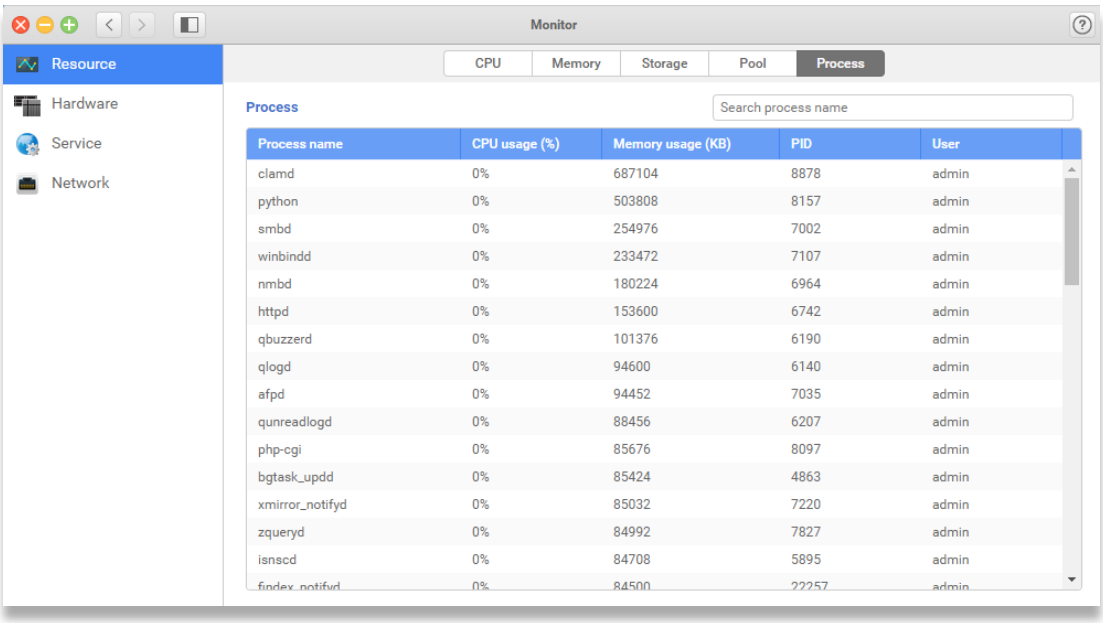


To show on Dashboard

If you want to view this status on Dashboard, click **Add to Dashboard** checkbox at the top of this page.

Process

Process allows you to check the CPU usage, memory usage, PID and user account of all the active processes in the order of CPU usage.

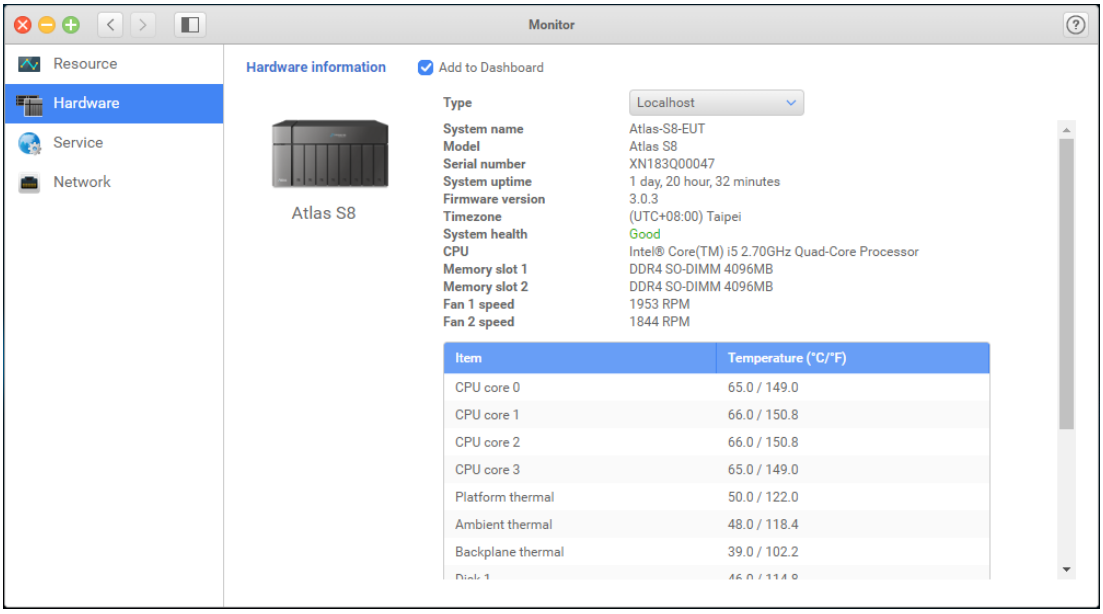


To search content

If you want to search processes on this table, enter the keyword and click **Search** button or Enter button on your keyboard.

Hardware

On this page, you can view the hardware information on localhost and all the enclosures by clicking the drop-down menu at the top of the page.



You can check the status of CPU usage. The detailed information of each chart will be shown upon mouse over. CPU load could be high when Resource Monitor is first launched, because the system needs to collect its resource data and load the UI page at the same time.

To show on Dashboard

If you want to view this status on Dashboard, click **Add to Dashboard** checkbox at the top of this page.

NOTE:
The following are the possible types of status of hardware information:

- For system health status:

Green - The system status is good.

Yellow - The system status is abnormal.

Red - The system status is error.

- For fan speed status

  Red - The fan speed is lower than the minimum level.

- For temperature

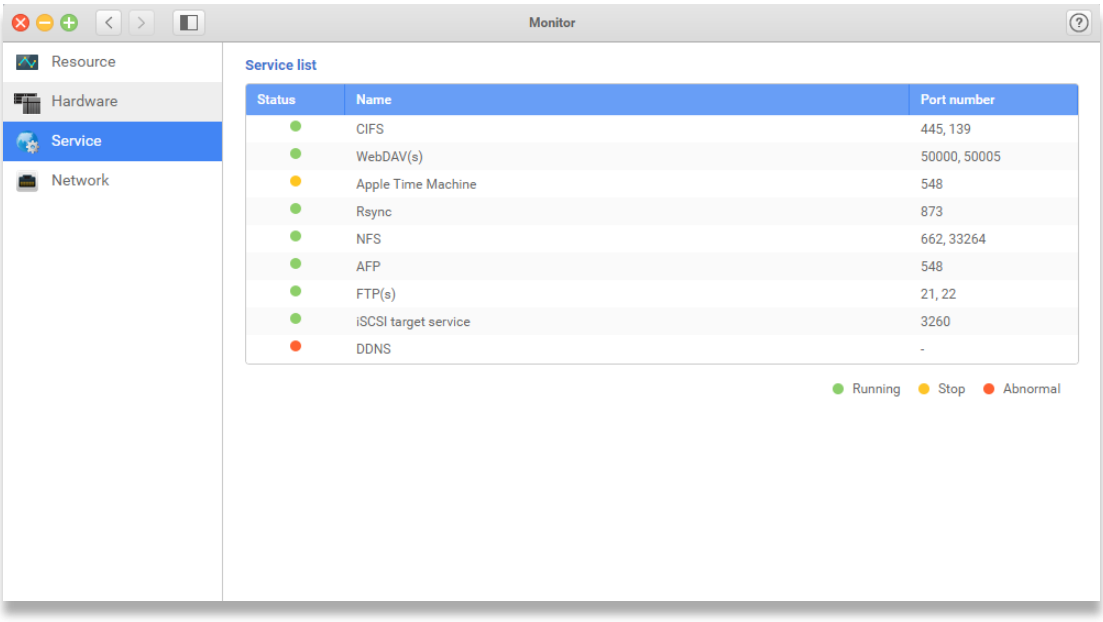
  Green - The temperature is at normal level.

  Yellow - The temperature is at abnormal level.

  Red - The temperature is at critical level.

Service

On this page, you can view the status and port number of all the network services.



To show on Dashboard

If you want to view this status on Dashboard, click **Add to Dashboard** checkbox at the top of this page.

NOTE:

The following are the possible service statuses:

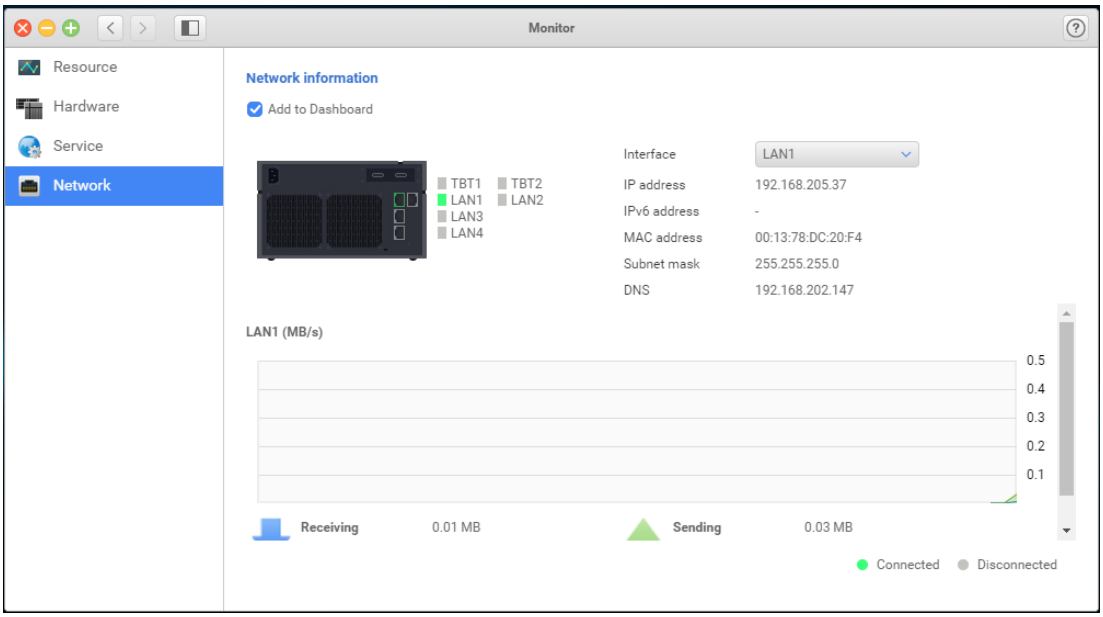
Green - Running.

Yellow - Stop.

Red - Abnormal.

Network

This page displays the sent and received data in MB every 3 seconds. If you create link aggregations or connect the Thunderbolt adapter card, the transfer speed will also show on this page.



View the network interface

You can view the overall network information including IP address, IPv6 address, MAC address, subnet mask and DNS by choosing the interface from Interface drop-down menu.

NOTE:

The status light shows the current status of each LAN port, please refer to the following indication:

Green - Connected.

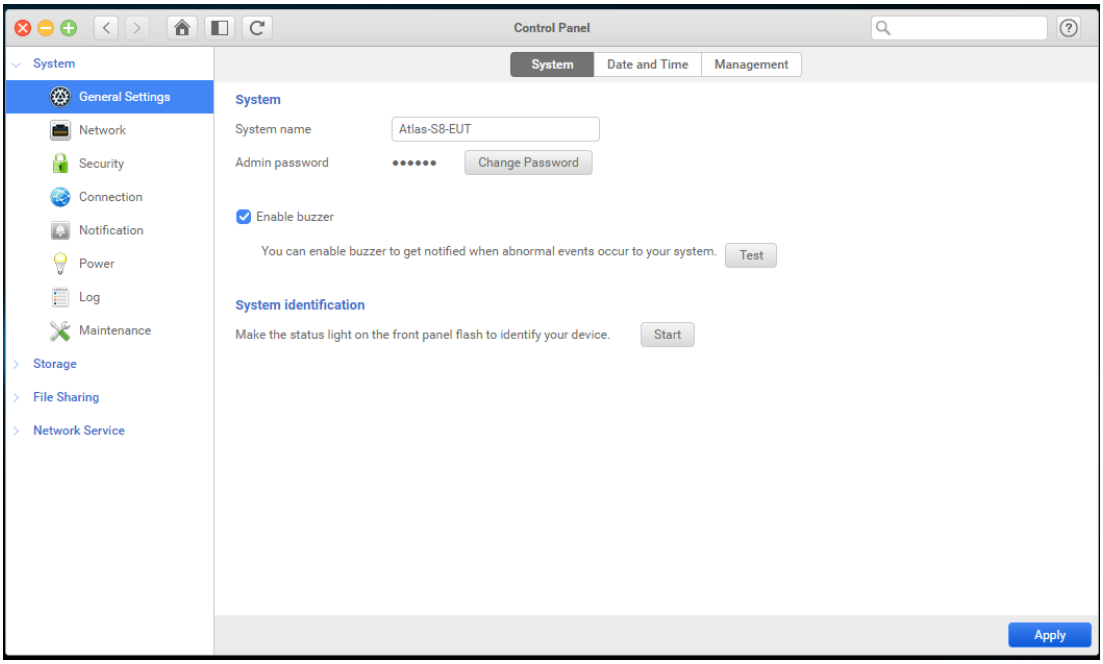
Grey - Disconnected.

Control Panel

System

General Setting

You can quickly set up the general system settings you want on this page, such as **System name**, **Time & Date**, and **Management**.



Naming your system

To name your system, please follow the steps below:

1. Enter the new name in **System name**.
2. Click **Apply** to save the changes.

Changing password

To change admins password, please follow the steps below:

1. Click **Change Password** button.
2. Enter the new password.
3. Retype the new password.

4. Click **Confirm** to save the change.

Buzzer

When the buzzer is enabled, your Atlas S8+ will audibly notify you of any error or abnormal status. Different errors have different sounds. You can test the buzzer by simply checking the **Test** button. To enable the buzzer, please follow the steps below:

1. Select **Enable buzzer**.
2. Click **Apply** to save the setting.

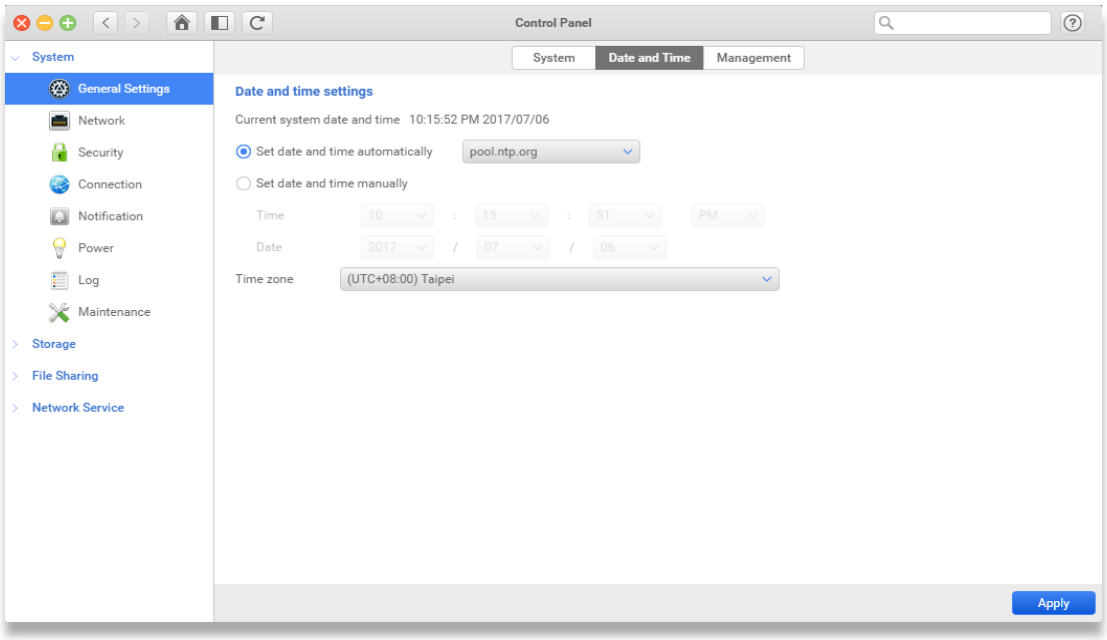
You can test the buzzer by simply click the Test button.

System identification

If you want to identify the Atlas S8+, click **Start** and then the UID (Unique Identify) LED on the front panel of Atlas S8+ will start blinking.

Date and Time

To change your **Date and Time** settings for you Atlas S8+. You can set the settings either as automatic or manual.



Date and Time settings

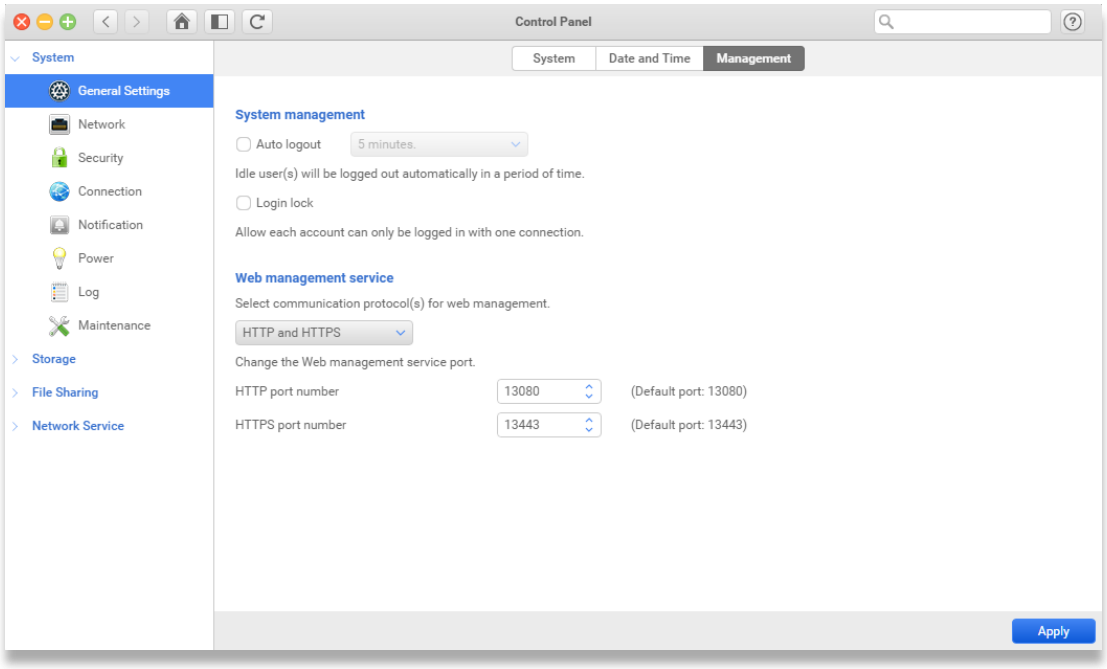
To setup the system time settings, please follow the steps and instructions below:

1. Setup time & date automatically: Select **Set date and time automatically** and choose time server from the drop-down menu for your preference.

2. Setup time & date manually: Select **Set day and time manually** and enter the time and date.
3. Choose a time zone from **Time zone** drop-down menu.
4. When you finish setting, click **Apply** to save the settings.

Management

You can configure the auto logout time and web managements for your Atlas S8+.



System Management

For the security, you can setup the Auto logout time and Login lock for you Administration's session.

- Auto logout: After in certain period of the time, the idle users will be logged out automatically if you enable “Auto Logout”.

  To enable the **Auto logout**, please follow the steps below:

  1. Click Auto log out checkbox.
  2. Choose the idle time for 5, 10, 15, or 30 minutes from the drop-down menu.
  3. Click **Apply** to save the settings.

- Login lock: Login Lock allows only one login per user account.

To enable the Login lock, please follow the steps below:

1. Select **Login Lock** checkbox.
2. Click **Apply** to save the settings.

Web Management Service

You can setup the data communication for Atlas S8+ WEB UI for HTTP, HTTPS or Both of them.

Moreover, you can set each protocol for a specific port. When the HTTPS is selected, you can access your Atlas S8+ by TLS/SSL connection. Please setup the web management service by the following steps:

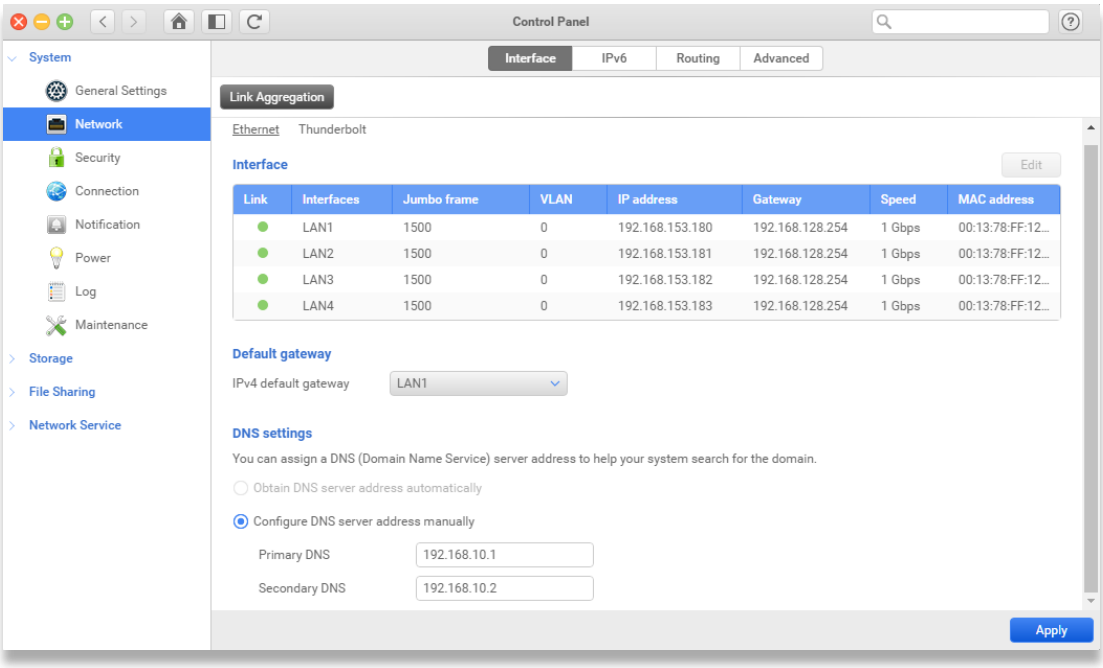
1. Choose web service communication protocol below from the drop-down menu:
   - **HTTP (Hypertext Transfer Protocol) only** : HTTP is a set of communication protocols which allows users to communicate and exchange information on the World Wide Web. The default port for an HTTP connection is 13080.
   - **HTTPS (Hypertext Transfer Protocol Secure) only** : HTTPS is a set of communication protocols which allows users to use HTTP as the connection encrypted by TLS/SSL. The default port for an HTTPS connection is 13443.
   - **HTTP and HTTPS** : Supports both HTTP and HTTPS protocols.
2. If you want to change the service port, please enter HTTP/HTTPS port number in the textbox.
3. Click **Apply** to save the settings.

Network

In network page, you can view the status and configuration of each Ethernet and Thunderbolt (Optional) interface. Atlas S8+ also supports link aggregation, IPv6, Routing table and more advanced settings for administrator accounts to monitor and control ethernet access to the device.

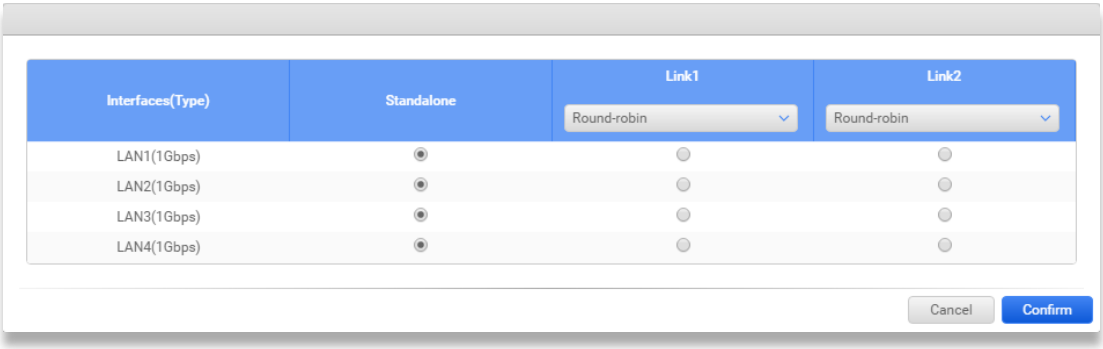
Interface

You can view the network circumstance and configure each network interface. The default gateway interface and DNS can be configured here. Also, for Atlases with Thunderbolt ports, the thunderbolt IP addresses can be configured.



Link Aggregation

Link aggregation is a technology that supports various methods of combining (aggregating) multiple network connections in parallel to increase throughput beyond what a single connection could sustain and to give redundancy in case one of the links should fail.



To use link aggregation select one of the following aggregation modes:

1. **Standalone** : Do not support link aggregation.
2. **Aggregation Link Driver Mode** :
    - **Round-Robin** : Round-robin driver mode transmits network packets in sequential order from the first available network interface to the last. This mode provides load balance, fault tolerance, and increases data transmission efficiency.
    - **Active-Backup** : In the active-backup mode, only one network interface in the

bond is active. If one adapter (interface) fails, it will switch to the second one automatically. The aggregated MAC address is externally visible on only one port (network adapter) to avoid confusing the switch. This mode provides fault tolerance.

- **XOR (Trunking Layer, Layer2, Layer2+3, Layer3+4)** : XOR mode balances network traffic by separating packets between different adapters. This mode selects the same network interface for each MAC address and also provides load balance and fault tolerance.
- **Broadcast** : Broadcast mode transmits network packets on all network interfaces. This mode provides fault tolerance.
- **LACP (Dynamic Link Aggregation, Layer 2, Layer 2+3, Layer 3+4, IEEE 802.3ad)** : LACP creates aggregation groups that share the same speed and duplex settings. This mode utilizes all network interfaces (adapters) in the active aggregator group according to the IEEE 802.3ad. This mode provides fault tolerance and load balance.
- **Transmit Load Balancing (balance-tlb)** : Transmit Load Balancing mode uses a bonding driver mode that does not require any particular network switch support. The outgoing network traffic is distributed according to the current load on each network interfaces. Incoming traffic is received by one currently designated slave network interface. If this receiving slave fails, another slave will take over the MAC address of the failed receiving slave. This mode provides fault tolerance.
- **Adaptive Load Balancing (balance-alb)** : Adaptive load balancing mode includes balance-tlb plus receives load balancing (rlb) for IPv4 traffic. Setup of this mode does not require any particular network switch support. ARP negotiation achieves the receive load balancing. This mode provides load balancing and fault tolerance.

3. Click **Confirm** to finish the settings.

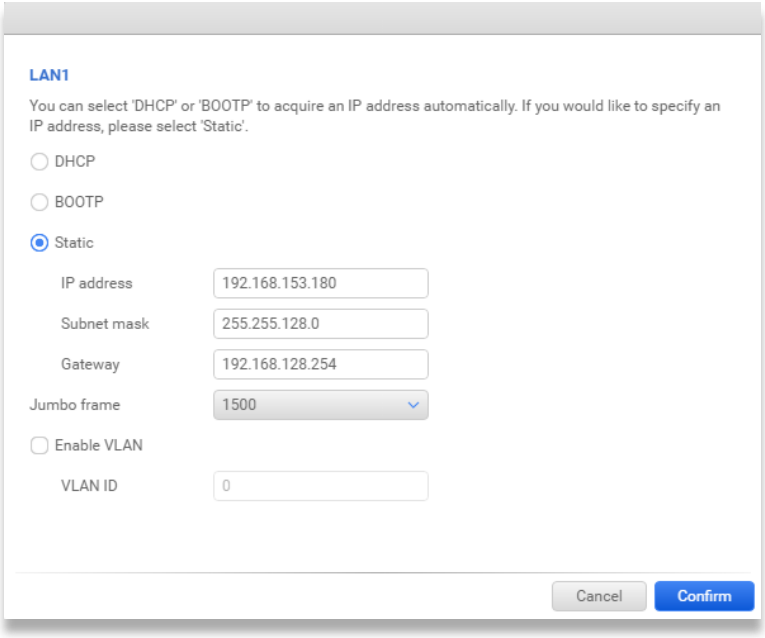
Thunderbolt (Optional)

On this page, you can set up the Thunderbolt Bridge Address for the each interface. Thunderbolt interfaces can also connect directly to another Atlas S8+ or MAC.

NOTE:
This function is only capable for the devices with Thunderbolt 3.0 interfaces.

Edit the specific network Interface

Every network interface requires an IP address, and the Network tab is where this is configured. There are three ways for your Atlas S8+ to get an IP address, DHCP, BOOTP, and by being assigned a Statis IP address. You can also configure jumbo frames and enter a VLAN tag for a port on this page.



To edit the network interface of the system, please check the instructions and follow the steps below:

1. Select the interface you want to modify.
2. Click **Edit**.
3. Choose one of the following interfaces:
    - **DHCP** : Dynamic Host Configuration Protocol which is a standardized network protocol used on IP network for dynamically distributed network configuration parameters, such as IP address for interfaces and services. With DHCP computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for an administrator or a user to configure their settings.
    - **BOOTP** : The Bootstrap Protocol is a computer networking protocol used in Internet protocol networks to automatically assign an IP address to network devices from a configuration server. This protocol is implemented by using the User Datagram Protocol (UDP) and operates only on IPv4 networks.
    - **Static** : A static Internet Protocol address is a fixed IP address assigned to a

computer or device by the network administrator

4. Setup jumbo frame: For Jumbo frames select an MTU of 9000, for standard frames select an MTU of 1500.

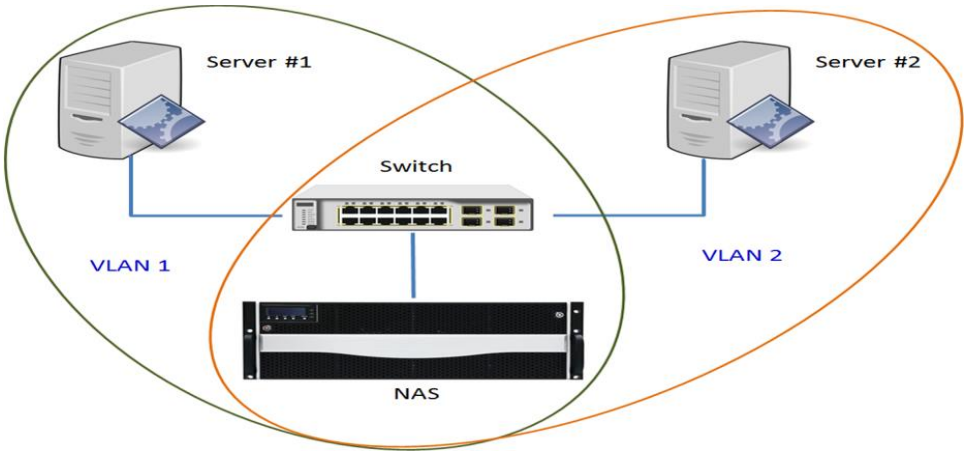
NOTE:
The Jumbo frame setting is valid if the Atlas S8+ is on a gigabit network environment and the other corresponding network devices support the same MTU value.

5. Enable VLAN: Select **Enable VLAN** and enter the VLAN ID.
6. Click **Apply** to finish the setting.

NOTE:
VLAN is a kind of “logical LAN,” in which a subnet can be planned and implemented based on logical connections, instead of physical location. You can divide a VLAN based on your requirements – it can be done in a single switch or across multiple switch environments. VLANs can be distributed by the network, your location, function, department, application, or Ethernet connection port.

- **Advantages of VLAN** :

① Allows different kind of devices (PC, workstation, and server) to integrate into the same logical network.
② Rapidly communicates information to each other.
③ Shares resources and isolates data traffic to increase the efficiency of the network data transmission.
④ The same VLAN will not change its access right due to physical location change.



- **VLAN ID** :

  VLAN ID is a number that used to identify those devices that are in the same network domain. Those devices with different VLAN IDs are not able to directly communicate with each other. The number for the VLAN ID number must be 0 to 4094. One physical network interface can be assigned with one VLAN ID.

Default Gateway

Configure the default gateway for your Atlas S8+, such as LAN1, LAN2, etc. Please set up by the following steps:

1. Choose the desired default gateway interface from the drop-down menu.
2. Click **Apply** to save the settings.

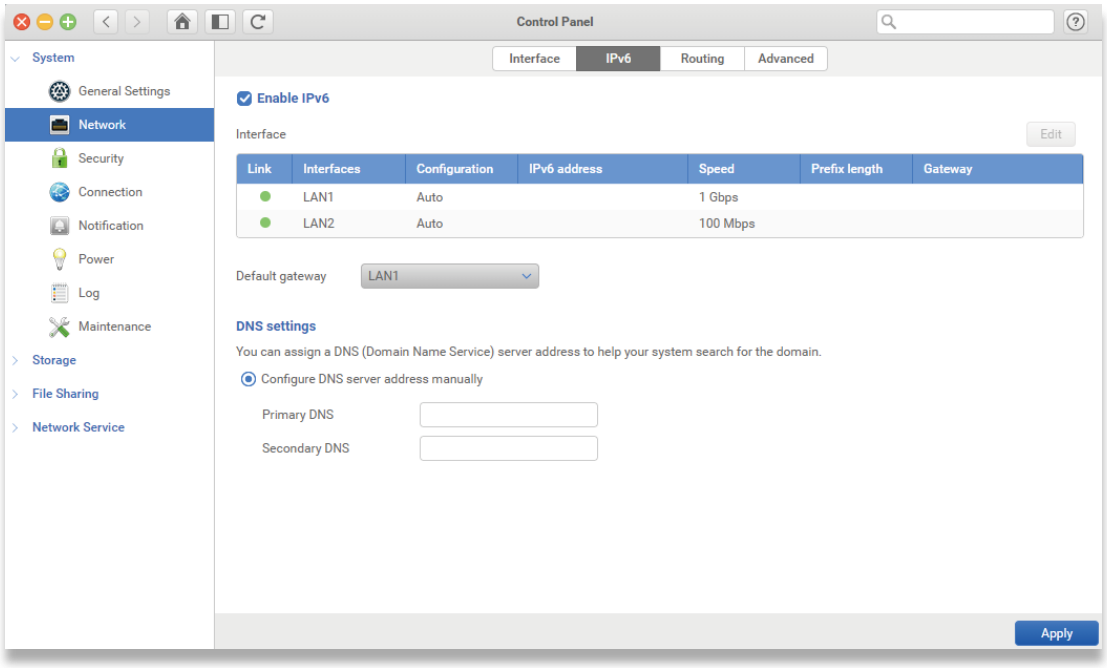
DNS Settings

DNS (Domain Name Service) provides a means to translate a host name into an IP address. You can obtain the DNS server address automatically from your DHCP server or manually input the DNS server address. Please follow the steps to setup the DNS settings:

1. Choose one of the items below for your need:
   - **Obtain DNS server address automatically** : If you choose this item, the system will automatically get the DNS IP address.
   - **Use the following DNS server address** : If you choose this item, you need to enter a primary and secondary DNS server’s IP address.
2. Click **Apply** to save the settings.

IPv6

IPv6 is short for "Internet Protocol Version 6". IPv6 is the Internet's next-generation protocol, designed to replace the current Internet Protocol, IP Version 4.



Set up IPv6 interface

To setup the IPv6 interface, please follow the steps below:

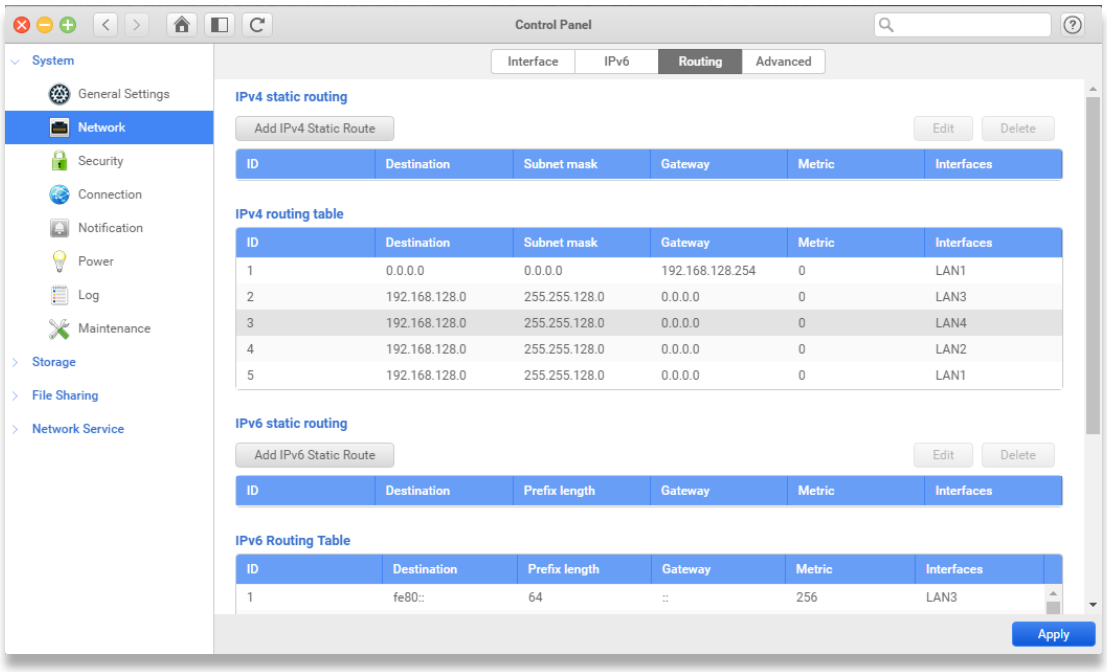
1. Select **Enable IPv6**.
2. You must click **Apply** after step1 or you won't be able to configure the LAN ports for ipv6.
3. Select one of the following types:
   - **Automatic** : Acquire an IP address automatically.
   - **DHCP** : Use Dynamic Host Configuration Protocol (DHCP) to allocate an intellectual property address.
   - **Static** : Specify an IP address manually. If you choose Static, you have to set IPv6 address, prefix length (Valid range: 0~128) and gateway first.
4. Click **Confirm** to save the settings.

DNS settings

You can assign the primary and secondary DNS server automatically or manually via IPv6 address.

Routing

This tab shows you the table for current **IPv4/ IPv6** routing status. You can add IPv4/IPv6 static route and manage them here.



IPv4 static routing/IPv6 static routing

In routing table, you can add, edit and delete a specific static route for your Atlas S8+.

To add an IPv4/IPv6 static route, please follow steps below:

1. Click **Add IPv4/IPv6 Static Route**.
2. In **Destination**, enter the IP address of your destination.
3. In **Subnet mask**, enter the subnet mask of your address
4. In **Gateway**, enter your destination's gateway address.
5. In **Metric**, setup the mask metric.
6. Choose default interface in **Interface**.
7. Set your IP address in **IP address**.
8. Click **Confirm** to save the changes.

To edit an IPv4/IPv6 static route, please follow steps below:

1. Choose the item you want to modify.
2. Click **Edit** and setup the form settings. (See the descriptions in **Add IPv4/IPv6**

static route)

3. Click **Confirm** to save the changes.

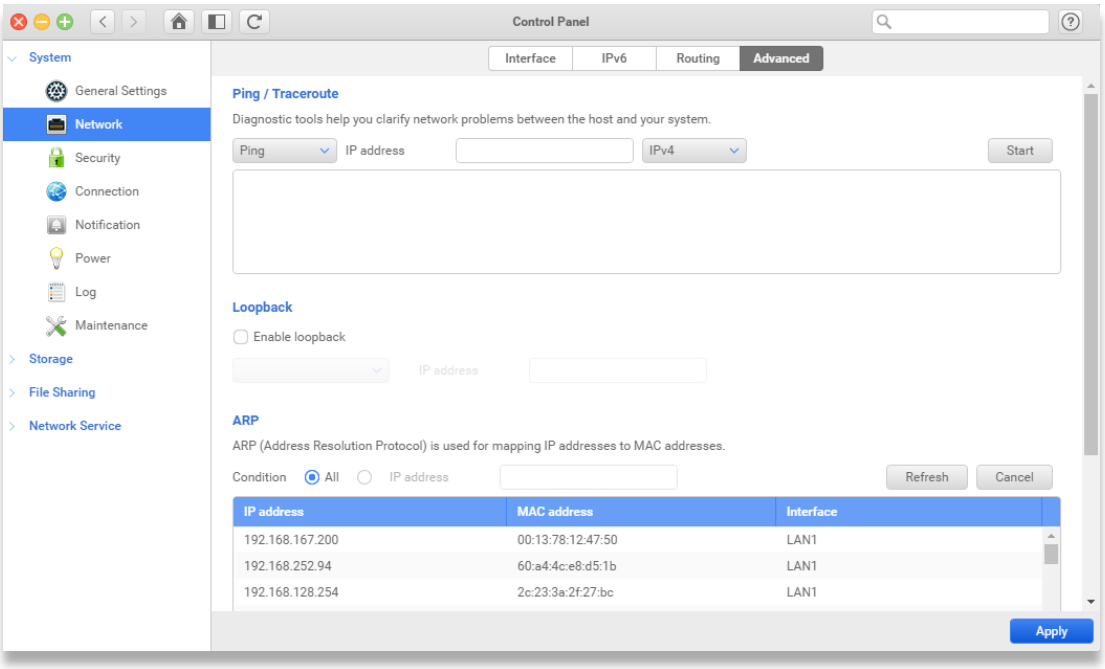
NOTE:
ipv6 needs to be enabled before you can modify ipv6 routing or delete ipv6 routes.

To remove an IPv4/IPv6 static route, please follow steps below:

1. Choose the item you want to delete.
2. Click **Delete** and setup the form settings. (See the descriptions in **Add an IPv4/IPv6 static route**)
3. Click **Confirm** to save the changes.

Advanced

With this page, you can find several Internet tools for administrators to solve Internet issues.



Ping / Traceroute

The NAS system provides diagnostic tools such as Ping/Traceroute to diagnose what happens between the Atlas S8+ and a client computer. To use the services, please follow the steps below:

1. Choose diagnostic tool including Ping or Traceroute.

2. Enter an IP address based on IPv4 or IPv6.
3. Click **Start** to diagnose.

Loopback

Loopback is used to test the ethernet interface itself. To enable the loopback service, please follow the steps below:

1. Select **Enable loopback**.
2. Click **Apply** to save the change.

ARP

ARP (Address Resolution Protocol) provides table mapping between IP addresses and MAC addresses. You can select All or enter a specific IP address and the table will display the MAC address of the selected IP address.

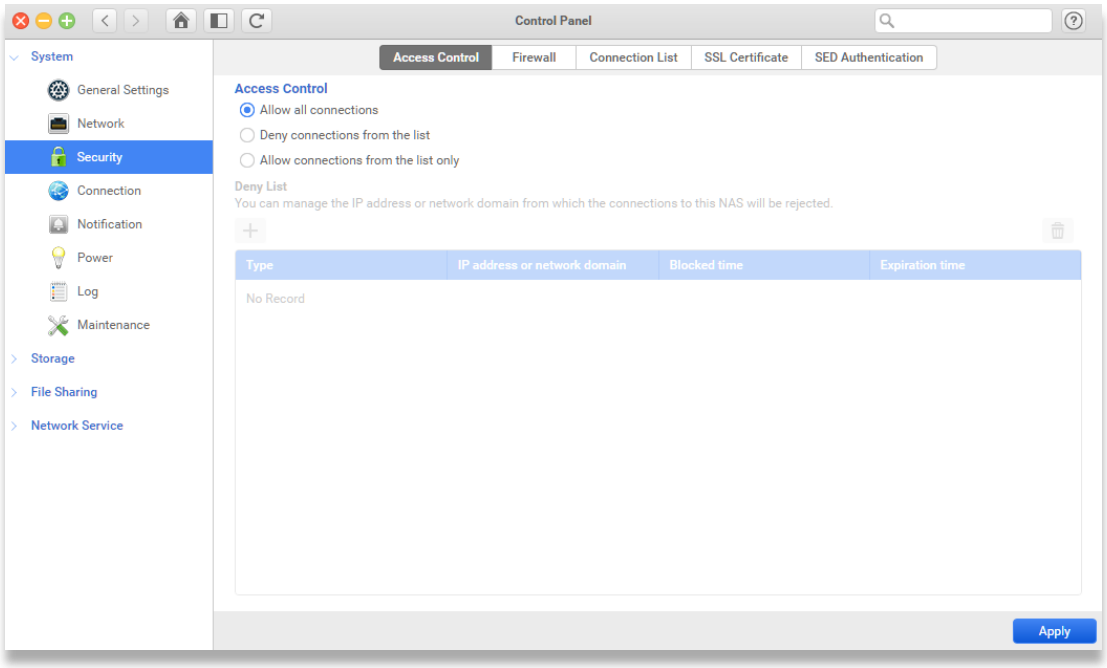
1. Select **All** or enter the specific IP address.
2. Click **Refresh** to update the table.
3. Click **Cancel** to stop mapping the addresses.

Security

In Security, you can make your Atlas S8+ even more secure with Access Control, Firewall, Connection List, SSL Certificate, and SED authentication.

Access Control

In this page, you can set up the access control for your Atlas S8+. You can allow all connections or a particular IP or IP ranges. Once the IP is set to deny, the host will not be capable of connecting to the device unless the setting is removed.



Add a deny connection list

To add a deny connection list, please follow steps below:

1. Select Deny connections from the list.
2. Click **Add** button.
3. Choose one of the following methods:

   - **Single IP address**

     ① Enter an IP address and setup the block time.
     ② Click **Confirm** button.
     ③ Click **Apply** button to finish the setting.

   - **Specify IP address of network by setting IP and netmask**

     ① Enter IP address and netmask.
     ② Setup the block time and click **Confirm** button.
     ③ Click **Apply** button to finish the setting.

   - **IP range**

     ① Enter the IP range in start/End IP text field.
     ② Setup the block time and click **Confirm** button.
     ③ Click **Apply** button to finish the setting.

Add an allow connection list

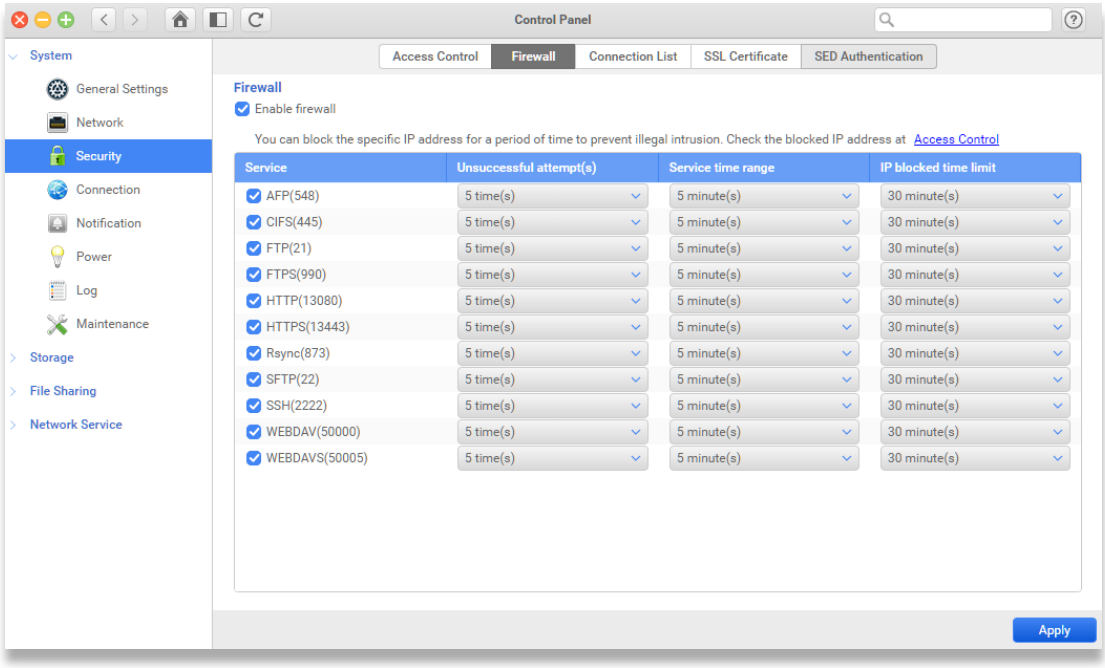
To add the allow connection list, please follow the steps below:

1. Select Allow connections from the list.
2. Click **Add** button.
3. Choose one of the following methods:
   - **Single IP address :**
     ① Enter an IP address and setup the block time.
     ② Click **Confirm** button.
     ③ Click **Apply** button to finish the setting.
   - **Specify IP address of network by setting IP and netmask**
     ① Enter IP address and netmask.
     ② Setup the **block time** and click **Confirm** button.
     ③ Click **Apply** button to finish the setting.
   - **IP range**
     ① Enter the IP range in start/End IP text field.
     ② Setup the **block time** and click **Confirm** button.
     ③ Click **Apply** button to finish the setting.

NOTE:
The current connection IP address will be automatically added to the allow list.

Firewall

The firewall can be configured to block the selected service's ports for a set period after a set number of unsuccessful login attempts.



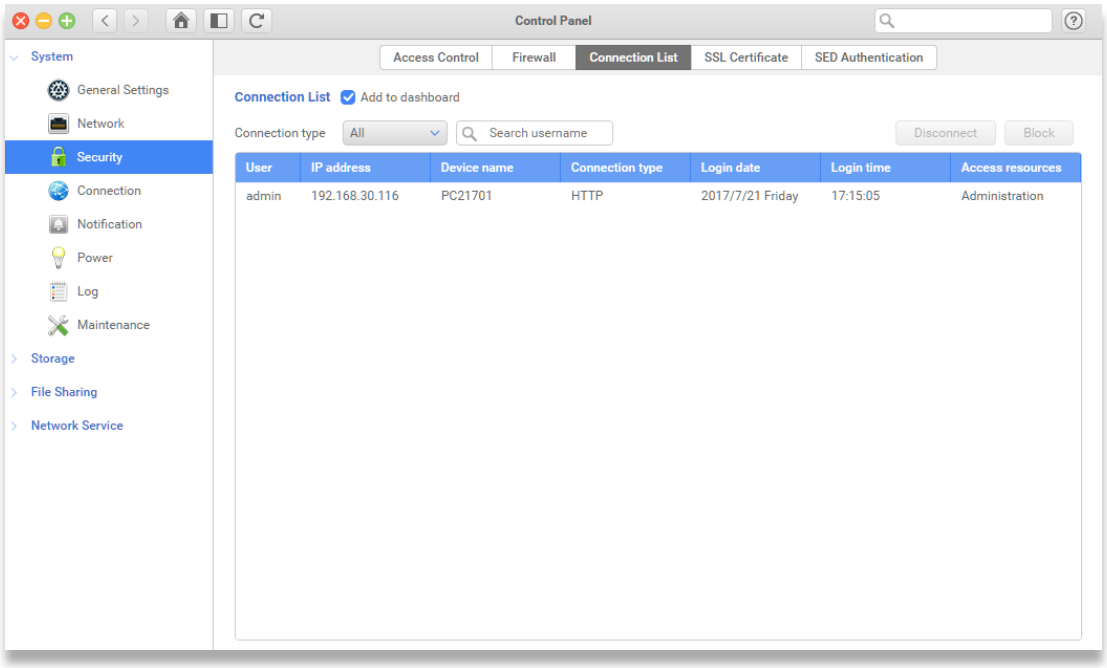
Enable Firewall

To enable Firewall and control the service permission, please follow the steps below:

1. Click **Enable firewall** checkbox.
2. Click **Service** checkbox which you want to set the restriction.
3. Set **Unsuccessful attempts** for 1/5/10/30 times.
4. Set **Service time range** for 5/10/20/30/100 minutes.
5. Set **Block the IP limited time** for 1 minute/30 minutes/1 hour/1 day.
6. Click **Apply** button and finish the setting.

Connection List

In this page, you can view and manage current connections of all data service for the Atlas S8+. You can check the particular user or file service as well. Moreover, by clicking check box “**Add to dashboard**”, you can see all the connection status on the desktop.



Viewing a particular file service

To view connections by a connection protocol, such as http or ftp, please follow the steps below:

1. Click the drop-down menu of connection type.
2. Select the file service you want to check.

Disconnect a user from the list

To disconnect the user from the list, please follow the steps below:

1. Choose the user you want to disconnect.
2. Click **Disconnect** button.
3. Click **Confirm** button to disconnect the user.
4. Click **Apply** button to save the change.

Block a user from the list

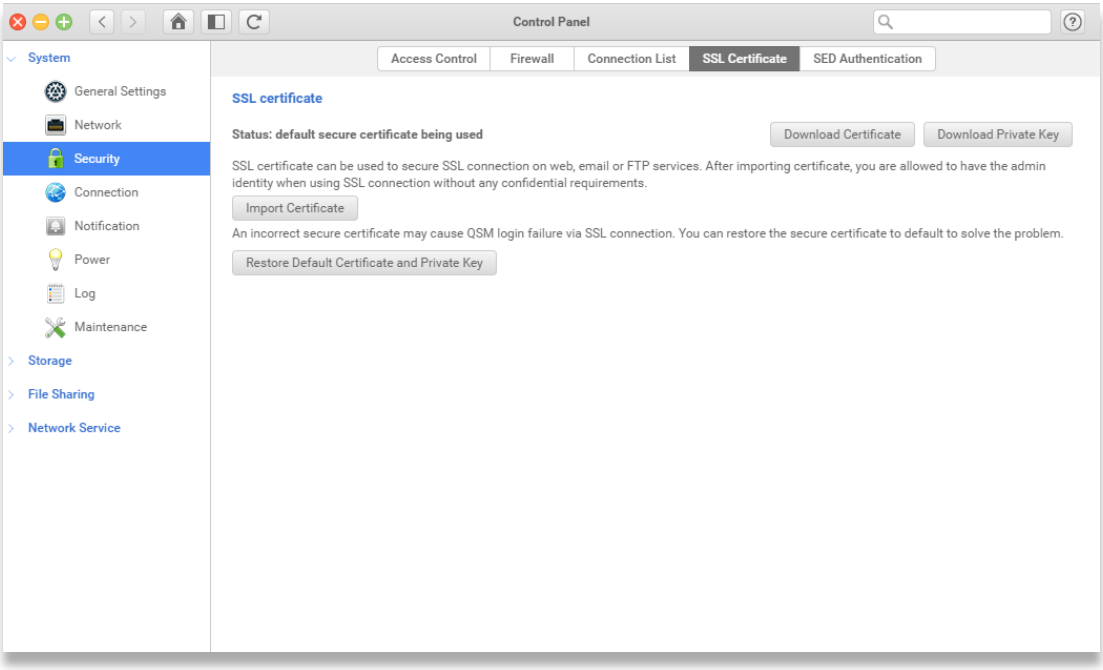
To block the user from the list, please follow the steps below:

1. Select the user you want to block.
2. Click **Block** button.
3. Choose the block time and click **Confirm** button.

4. Click the **Apply** button to save the change.

SSL Certificate

Certificates are used to ensure SSL services on your Atlas S8+, such as the web (all HTTP/HTTPS services), email, or FTP. It allows users to validate the identity of a server and the administrator before sending any confidential information.



Import certificate

To import certificates, please follow the steps below:

1. Click **Import Certificates** and the import window will pop out.
2. Upload **Certificate** and **Private Key** from your device.
3. Click **Confirm** to import the certificates.

NOTE:
The certificate can not be decrypted by the other private key pair.

Restore current certification

To restore the current certificates on Atlas S8+, please follow the steps below:

1. Click **Restore Default Certificate and Private Key**.

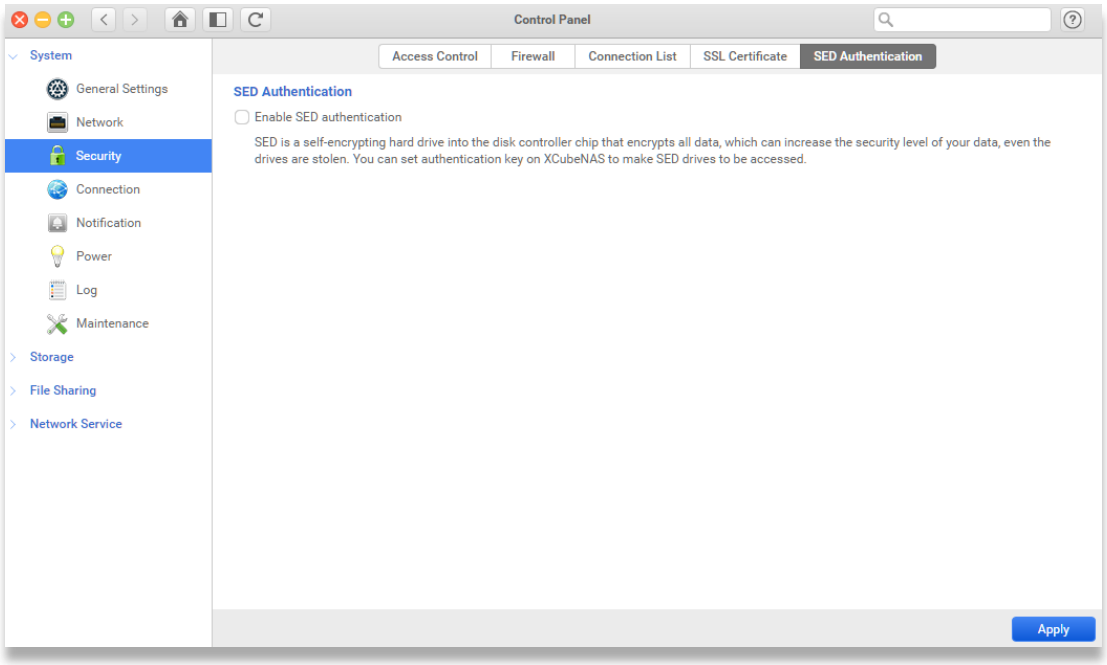
2. The certificate will be restored to default.

Download certificate

To download Certificate or Private Key to your computer, click on **Download Certificate** and **Download Private Key**.

SED Authentication

If you enable SED authentication, the system can generate the authentication key for SED protected disk(s) a period .



Enable SED authentication

To enable SED authentication, please follow the steps below:

1. Click **Enable SED authentication** check box.
2. Click **Apply** button.
3. The authentication setting window will pop out.

4. Click **Confirm**.

Connection

You can set up DDNS (Dynamic Domain Name Server) and UPnP (Universal Plug and Play) for your Atlas S8+ in **Connection** in order to connect to the Internet easily.

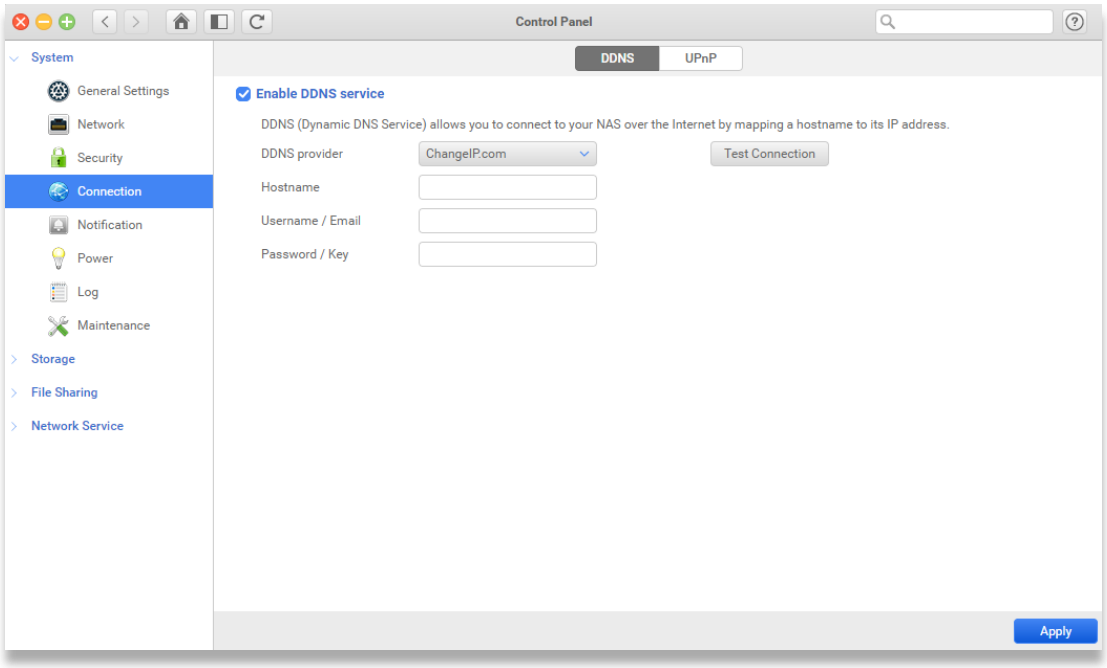
DDNS

In **DDNS**, you can register a PROMISE dynamic domain name (PROMISE Cloud) or log in a third party dynamic domain name for your Atlas S8+. Then you can easily connect to your Atlas S8+ with your public domain name (e.g. PROMISE.promisecs.com) instead of an IP address (e.g. 192.168.10.10).

Requirement:

Before you start setting up DDNS, please ensure the following items are ready:

1. Make sure the service of DDNS provider is working.
2. You have an active account on the DDNS provider.
3. The Atlas S8+ is able to connected to the internet.



Login a dynamic domain name for your Atlas S8+

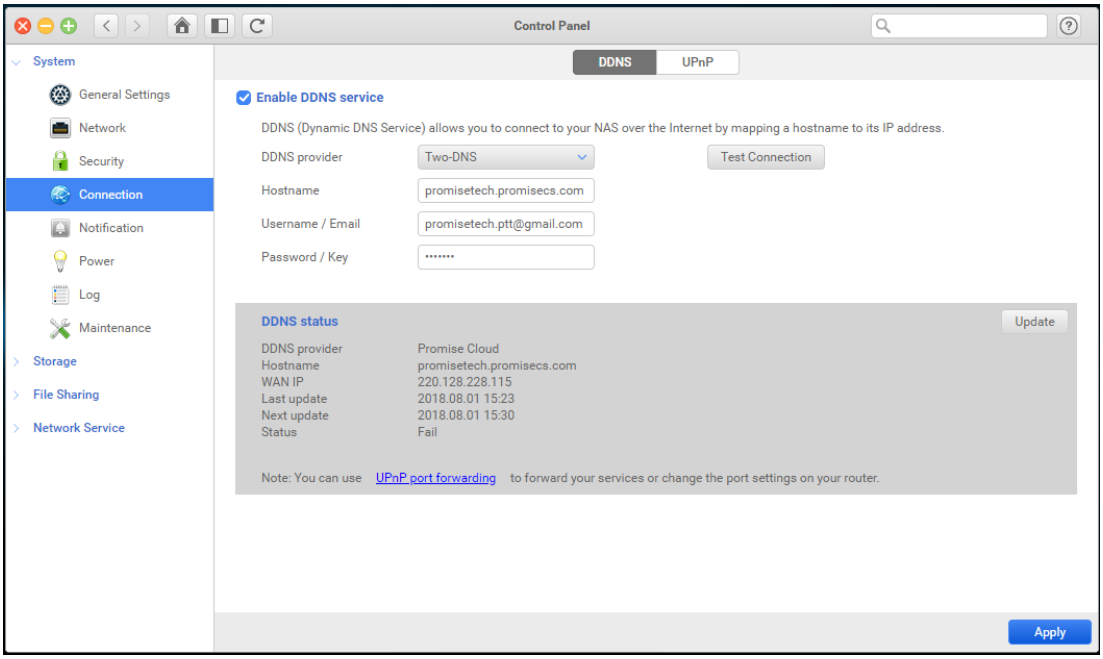
1. Click the checkbox to **Enable DDNS service**.
2. Select a DDNS Provider in the drop down menu.

NOTE:
Atlas S8+ supports the following DDNS providers:

1. PROMISE Cloud
2. Change IP
3. DNSEXIT
4. Dynamic DO! jp
5. FreeDNS
6. No-IP
7. Two-DNS

3. Enter your registered Hostname of your DDNS account.
4. Enter your Username or Email address of your DDNS account.
5. Enter your Password or Key.
6. Click **Test Connection** button to check if the setting is correct.
7. Click **Apply** to finish.

Once you have finished setting up, you can check and update your service status in the below dialog.



PROMISE Cloud

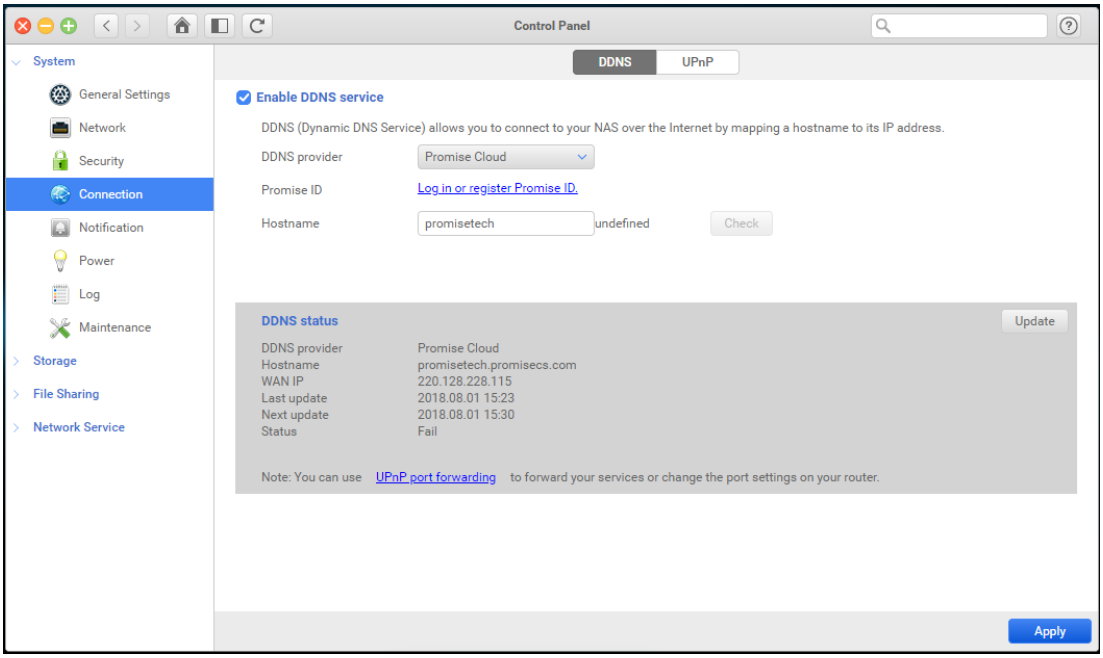
PROMISE Cloud is a PROMISE DDNS service to help your Atlas S8+ to have a public dynamic domain name for its internet access. To use PROMISE Cloud, please register a PROMISE ID first and then log in a PROMISE Cloud hostname.

Login or register a PROMISE ID

You only need one PROMISE ID to access PROMISE services. There are three ways to login or to create your PROMISE ID:

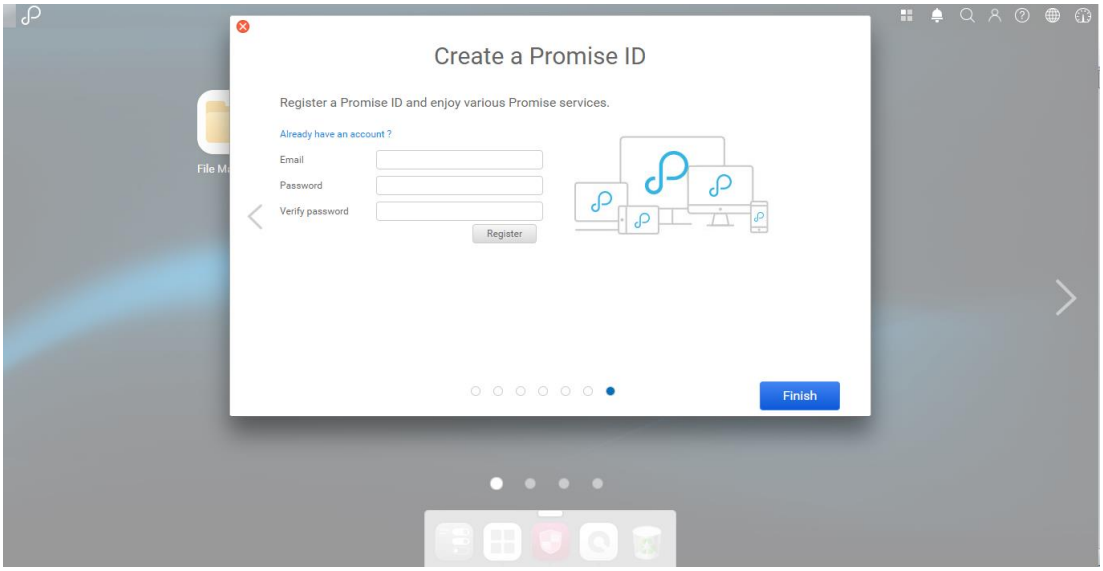
1. In **Connection** > **DDNS** page.

   Select PROMISE Cloud in **DDNS provider** dropdown menu. Then click **Log in or register PROMISE ID** hyperlink.



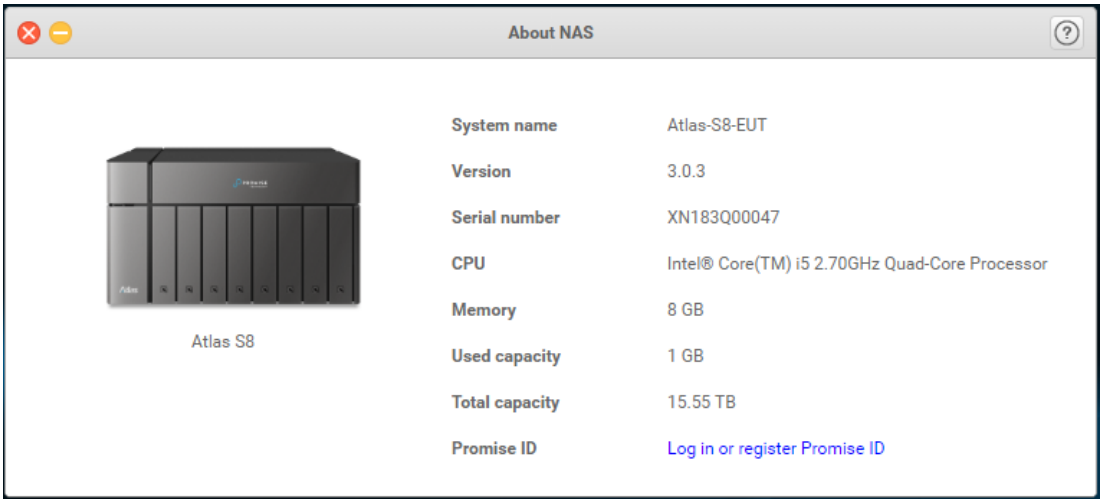
2. In **Tutorial** session.

   When you first start up your Atlas S8+, the tutorial session will automatically appear. You can also find **Tutorial** by clicking the PROMISE logo on the top-left corner on the desktop, then choose **Tutorial**. Click **Start** to go through the session and you will be able to log in by clicking **Already have an account?** hyperlink or to create a PROMISE ID.



3. In **About NAS** page.

   Click on the PROMISE logo on the top-left corner on the desktop, then choose **About NAS**. A pop up window will appear, then click **Log in or register PROMISE ID** hyperlink.



① Enter your PROMISE ID/ email address and your password, then click **Login** button. If you do not have a PROMISE ID, you can create one by following the steps below. Before you register a new PROMISE ID, consider whether it might be better to continue using one you already have. Click **Log in or register PROMISE ID** hyperlink, a pop up window will appear.

② Click **Register** hyperlink, another pop up window will appear.

③ Enter a PROMISE ID.

NOTE:
This field must be an email address. For example: user@example.com

④ Enter your password.

NOTE:
It must be between 6 to 16 characters.

⑤ Enter your password again to verify.

⑥ Choose a nickname you prefer.

NOTE:

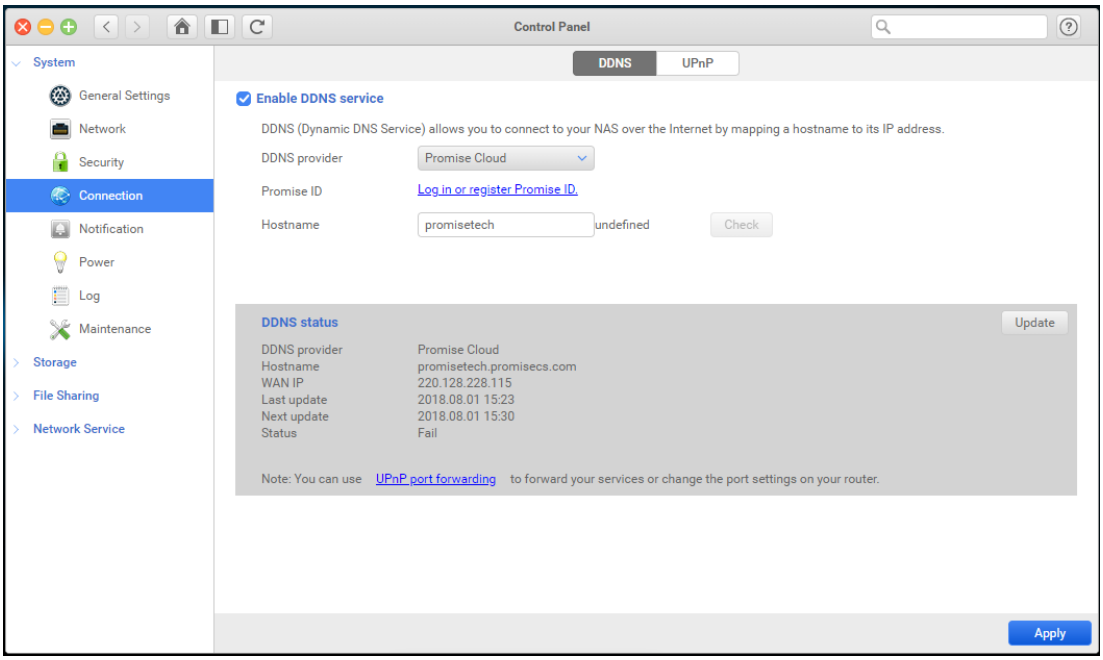
It must be between 1 to 32 characters.

Valid characters: 【a-z A-Z 0-9】

”.” can’t be placed either in the beginning nor the end.

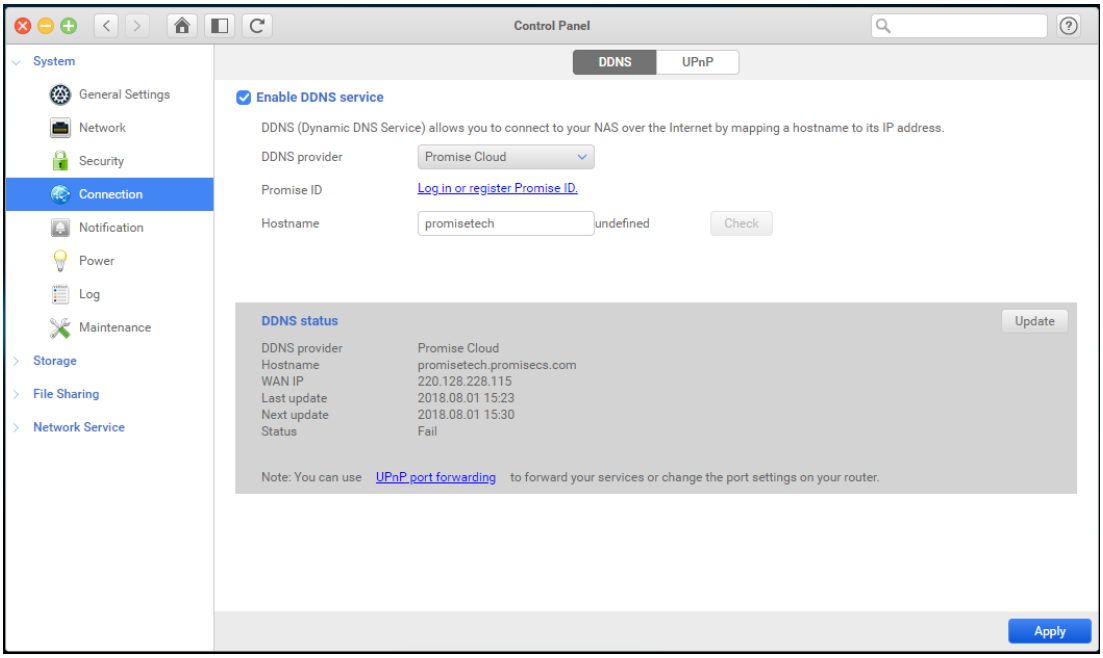
Enter PROMISE Cloud hostname

When you have logged in with your PROMISE ID, you can enter your hostname and click Check button to test if the hostname is available or not. The PROMISE Cloud hostname only allows A-Z, a-z, and numbers. Click Apply to finish the setting.



Check DDNS status

Besides DDNS, you also need to forward the Atlas S8+’s service port number on your router by clicking **UPnP port forwarding** hyperlink and use the UPnP feature to enable its internet access ability. Once you have finished the setting, return to DDNS page to check the DDNS status. Then you can simply click on the ASM web link to access ASM through internet.



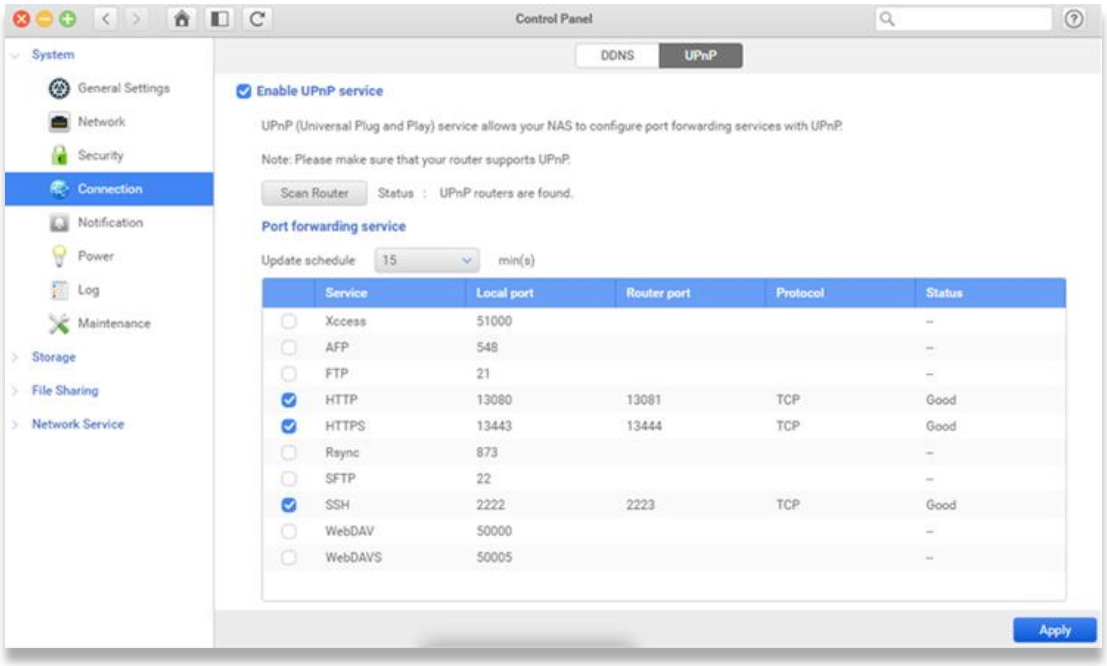
UPnP

In **UPnP**, you can set up the port forwarding table of your router to forward Atlas S8+'s service port number, to allow Atlas S8+ being accessed from the internet.

Requirement:

Before you start setting up UPnP, please ensure the following items are ready:

1. Your UPnP router is on the PROMISE compatibility list.
2. Your Atlas S8+ is connected with an UPnP router.



Set up UPnP

1. Click the checkbox to **Enable UPnP service**.
2. Click **Scan Router** button to check if your router supports UPnP or not.
3. Set up the UPnP **update schedule** the default value is 15 mins. You can choose other values (5, 10, 15, 30, 60 mins) from the drop down menu.
4. Check the service(s) to forward its port number.
5. Click **Apply** to finish the setting.

The UPnP service will forward the local port number of your service(s) on your router. When the port number is occupied by another device, the UPnP will try to assign a new port number on the router to forward.

NOTE:
Please refer to the following for the services and its associated port number:

1. AFP: port 548
2. FTP: port 21
3. HTTP: port 13080
4. HTTPS: port 13443
5. Rsync: port 873

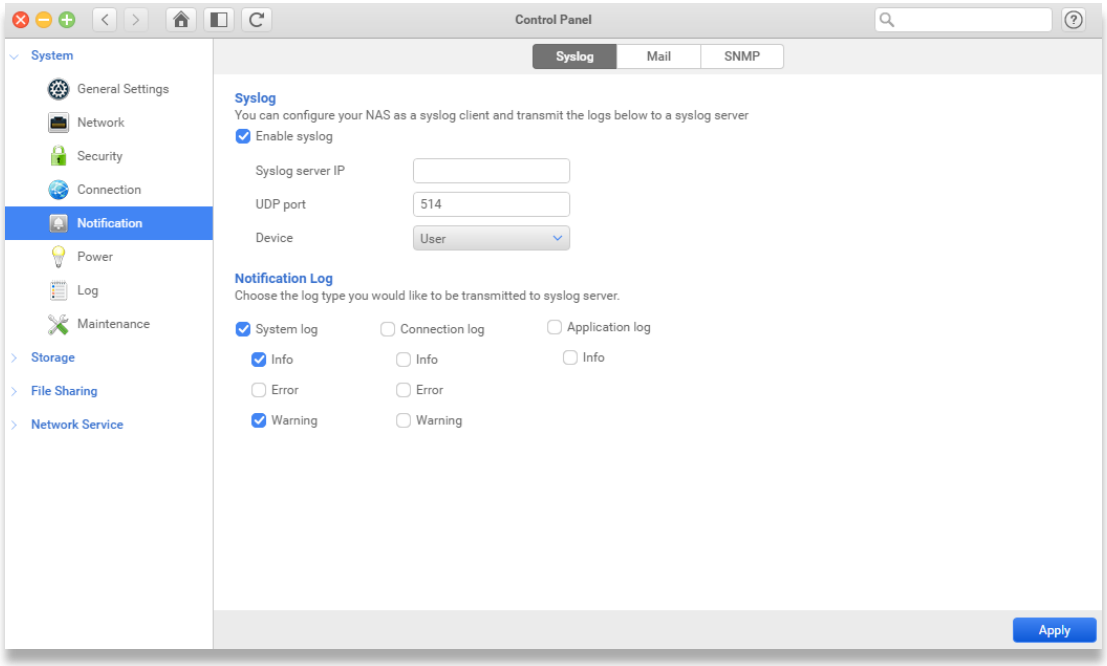
6. SFTP: port 22
7. SSH: port 2222
8. WebDAV: port 50000
9. WebDAVS: port 50005

Notification

In this page, you can setup the notification for the different system events occurred via different protocols, such as Syslog, Mail, and SNMP. Meanwhile, you can also set the event type for each account or protocols.

Syslog

When Syslog is enabled, all logs and connection logs can be saved to the remote Syslog server, and you can choose the event logs you would like to notice.



Syslog

To enable Syslog, please follow steps below:

1. Select **Enable Syslog**.

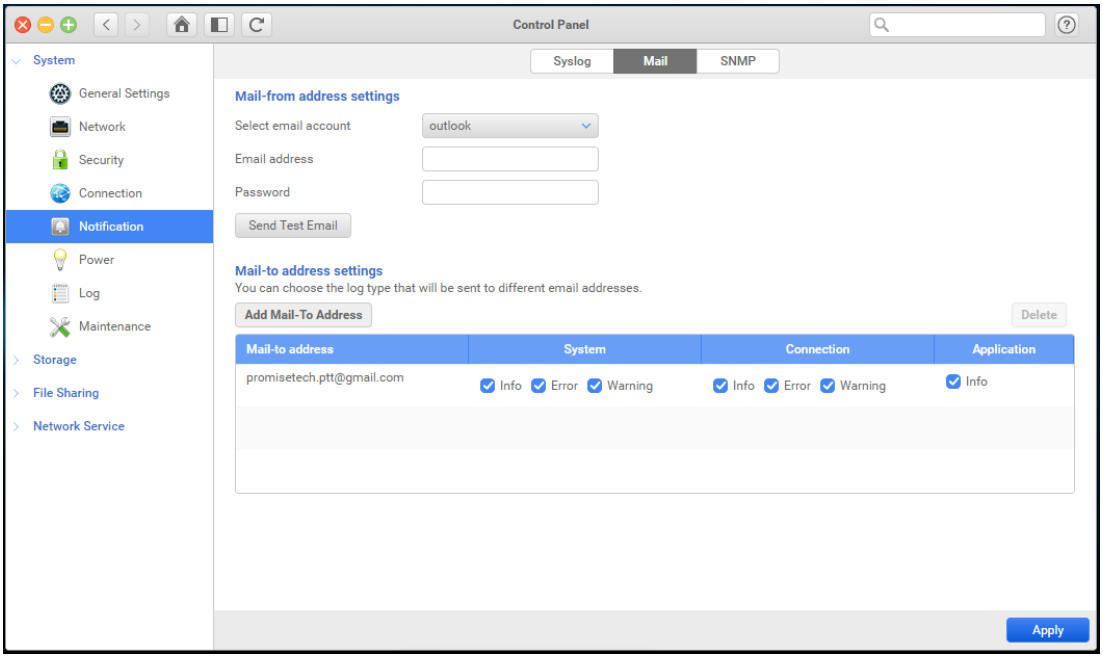
2. Enter **Syslog server IP**.
3. Enter **UDP port**.
4. Select **Device**.
5. Select the events you want to send to the server.
6. Click **Apply** to save the settings.

Notification Log

Choose the event occurred for the specific type of logs you want to be noticed via the protocol.

Mail

On this page, you can choose an e-mail service to save your logs. The Atlas S8+ offers Gmail, Yahoo Mail, Outlook, and the custom e-mail services.



Mail-from address setting

Enter a mail-from address can help you send out the event occurred on your Atlas S8+ to your specific mail account (Mail to address).

To add a mail-from address, please follow the steps below:

1. Select the email account host you would like to set as the mail-from account.

2. Configure the SMTP server for outgoing mails. (Please refer to your e-mail service provider for the SMTP settings.) (Custom mode)
3. Enter the email address to appear as the sender, example Atlas S8+@yourcompany.com.
4. Select authentication type in the “login using” pulldown menu and add account & password if necessary.
5. Click **Apply** to save the settings.
6. If you want to send a test email to the specified email account, you must first add a Mail-to destination to the Mail-to Address list. Then you can test your email configuration with the Send Test Email button.

Mail-to address setting

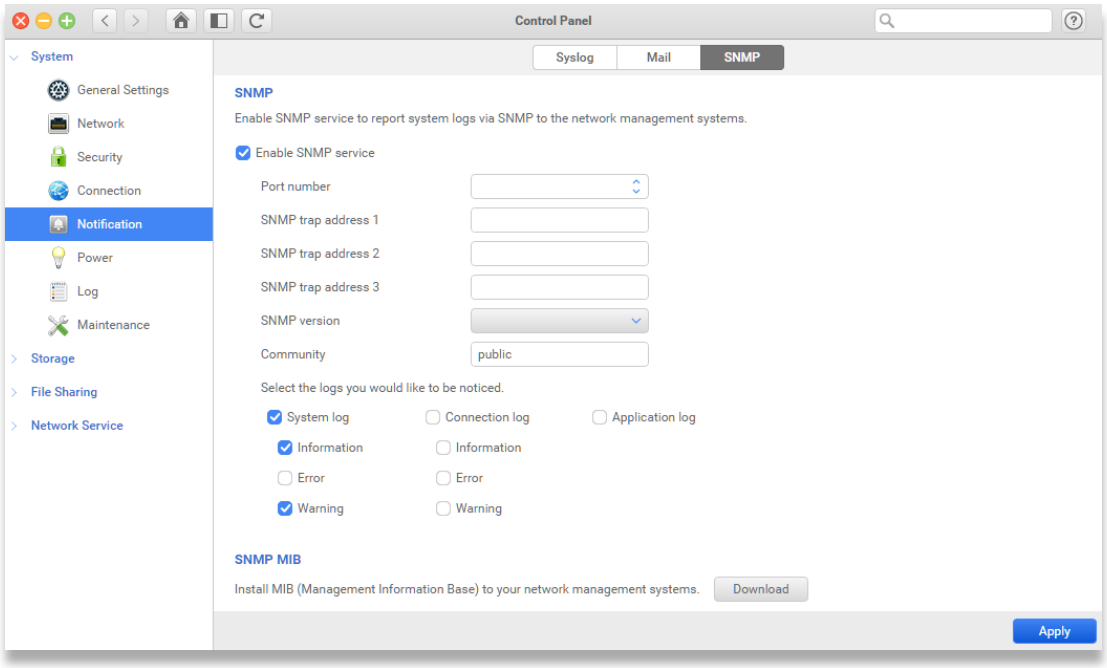
Enter email addresses where event messages are to be sent. The event emails will be from the email address entered in Mail-from above.

To add a mail-to address, please follow the steps below:

1. Click **Add Mail-To Address**.
2. Enter email address.
3. Choose the event occurred for the specific type of logs you want to be noticed
4. Click **Confirm** to save the settings.

SNMP

SNMP (Simple Network Management Protocol) is widely used in network management to monitor appliances attached to a network. The Atlas S8+ supports SNMPv1, SNMPv2 and SNMPv3.



To enable SNMPv1 and SNMPv2

To enable SNMPv1, SNMPv2, please follow the steps below:

1. Select **Enable SNMP service**.
2. Enter a port number.
3. Enter SNMP trap address 1~address 3.
4. Choose v1v2 in **SNMP version**.
5. Set up a **Community** name. (The default name is public.)
6. Select the events you want to be noticed.
7. Click **Apply** to save the settings.

To enable SNMPv3

To enable SNMPv3, please follow the steps below:

1. Select **Enable SNMP service**.
2. Enter a port number.
3. Enter SNMP trap address 1~address 3.
4. Choose v3 in **SNMP version**.
5. Pick a **protocol**.
6. Enter **Username** and **Password**.

7. Select **Enable encryption** if you want to encrypt the DES/AES protocol. (Optional)
8. Set up a **Community** name. (The default name is public.)
9. Select the events you want to be noticed.
10. Click **Apply** to save the settings.

NOTE:

1. SNMP service supports IPv4 and IPv6.
2. SNMPv1, SNMPv2, SNMPv3 community limitation: The community name must be in the range from 1 to 64 displayable characters. The following are not allowed: " ' \ and space.
3. SNMPv3 username limitation: The username must be in the range from 1 to 64 displayable characters. The following are not allowed: " ' \ and space.
4. SNMPv3 password limitation: The password is case sensitive and should be in the range from 8 to 127 displayable characters, including letters, numbers, and signs. The following are not allowed: " ' \ and space.

To enable SNMPv3

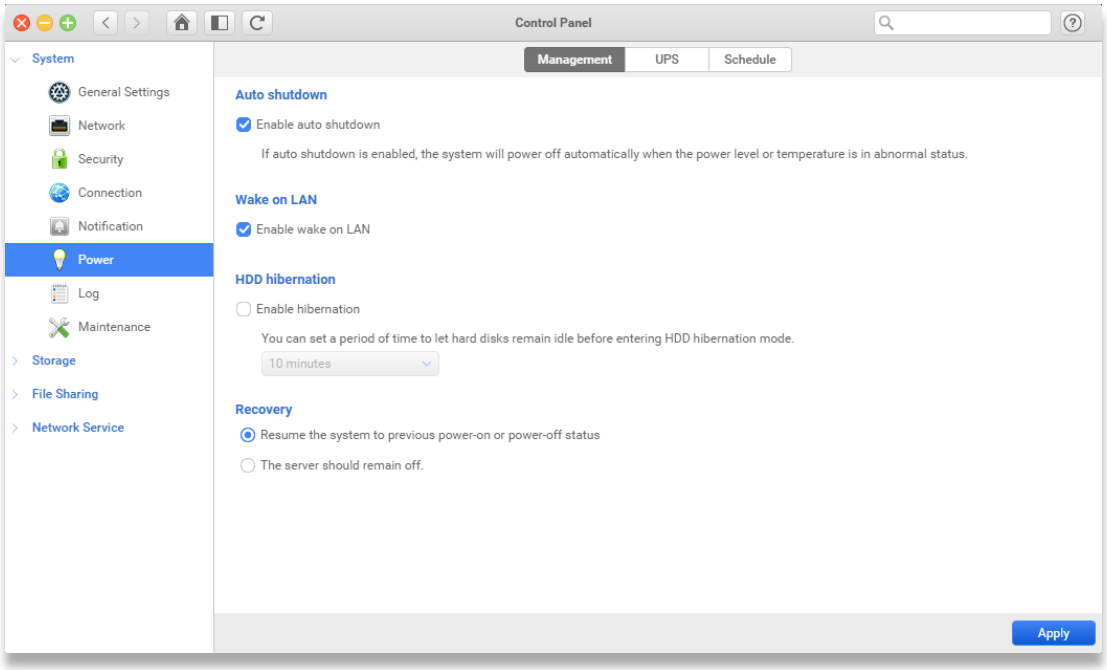
PROMISE provides the ability to monitor the Atlas S8+ including system, disk, and the status of RAID volumes. Please click the **Download** button, if you want to install the MIB files into your managing system.

Power

In this page, it can help you to increase the power efficacy, automatic mechanism configuration for the unexpected power outage.

Management

You can set Auto shutdown, Wake on LAN, HDD hibernation, and power recovery.



Auto Shutdown

When auto shutdown is enabled, the system will shut down automatically when internal power or temperature is in an abnormal status. To enable this function, please follow the steps below:

1. Select **Enable auto shutdown**.
2. Click **Apply** to save the settings.

Wake on LAN

Wake on LAN allows the Atlas S8+ to be powered on or woken from hibernation by an IP packet. To enable this function, please follow the steps below:

1. Select **Enable wake on LAN**.
2. Click **Apply** to save the settings.

HDD hibernation

The internal hard disk(s) and external SATA disk will hibernate after being inactive for a specified period. To enable this function, please follow the steps below:

1. Select **Enable HDD hibernation**.
2. Choose period from the drop-down menu.
3. Click **Apply** to save the settings.

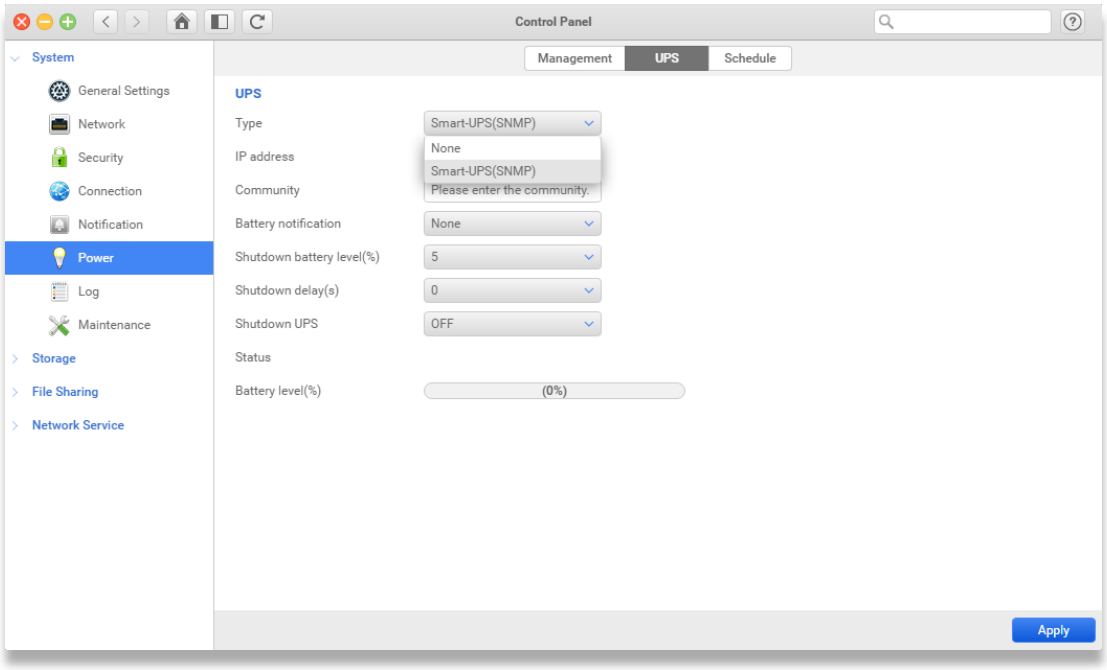
Recovery

To setup the recovery method when the power resume to work, please follow the steps below:

1. Choose one of the following options:
   - Just use restore-to the previous power-on or power-off state.
   - Leave in the powered off state in the power-off status.
2. Click **Apply** to save the settings.

UPS

The **UPS (Uninterruptible Power Supply)** is a backup power device for your Atlas S8+ if will maintain power to the Atlas S8+ if there is a power outage.



Set up UPS

After installing the UPS, you can configure the UPS settings by the following steps:

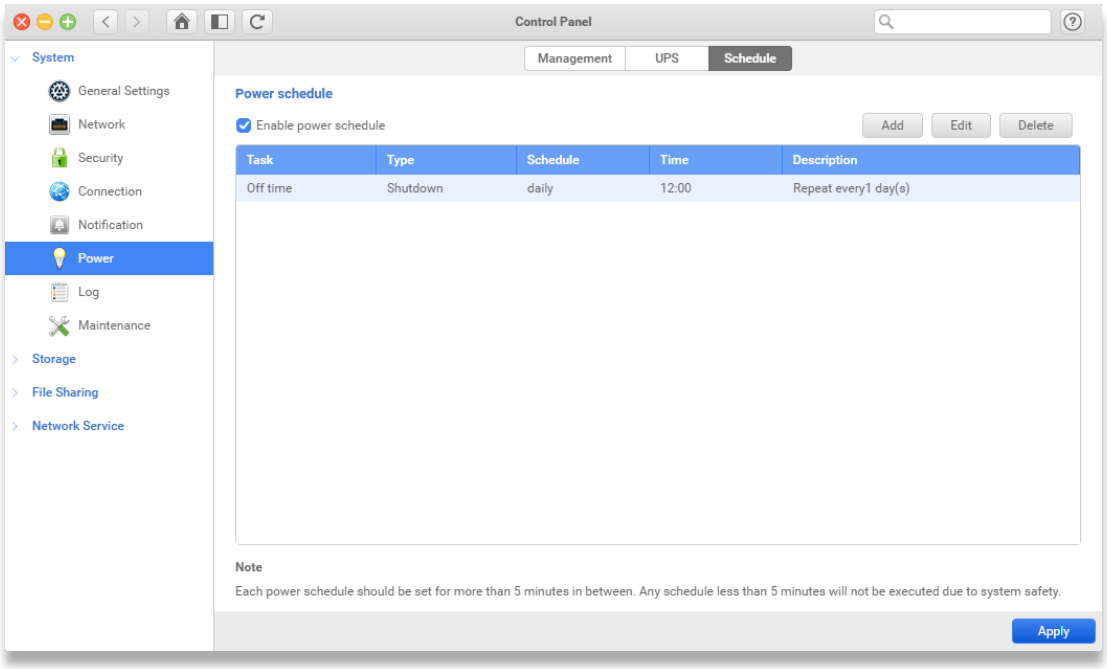
1. Choose UPS **type**.
2. Choose **battery notification** if the battery level is lower than 10~90(%).
3. Choose **shutdown battery level (%)**.
4. Choose **shutdown delay (s)**.

5. Choose on/off **shutdown UPS**.
6. Click **Apply** to save the settings.

In the UPS setting page, the system will show the UPS battery level (%) automatically.

Schedule

If you enable the power schedule, you can power on/ off, restart or hibernate the Atlas S8+ automatically. The power schedule can be a specified on a daily, weekly or dedicated monthly date basis.



To add a power schedule

To add a power schedule, please follow the steps below:

1. Click **Add Power Schedule**.
2. Choose shutdown, restart or turn on the server in **Task**.
3. Illustrate the task in **Description**.
4. Select the scheduled date in **Schedule**.
5. Choose the scheduled time in **Time**.
6. Click **Confirm** to save the settings.

To modify a power schedule

To modify the existing power schedule, please follow the steps below:

1. Select a schedule you want to modify.
2. Click **Edit**.
3. Follow the steps for schedule setup. (See **Add a power schedule**.)
4. Click **Confirm** to save the settings.

To delete a power schedule

To remove the power schedule, please follow the steps below:

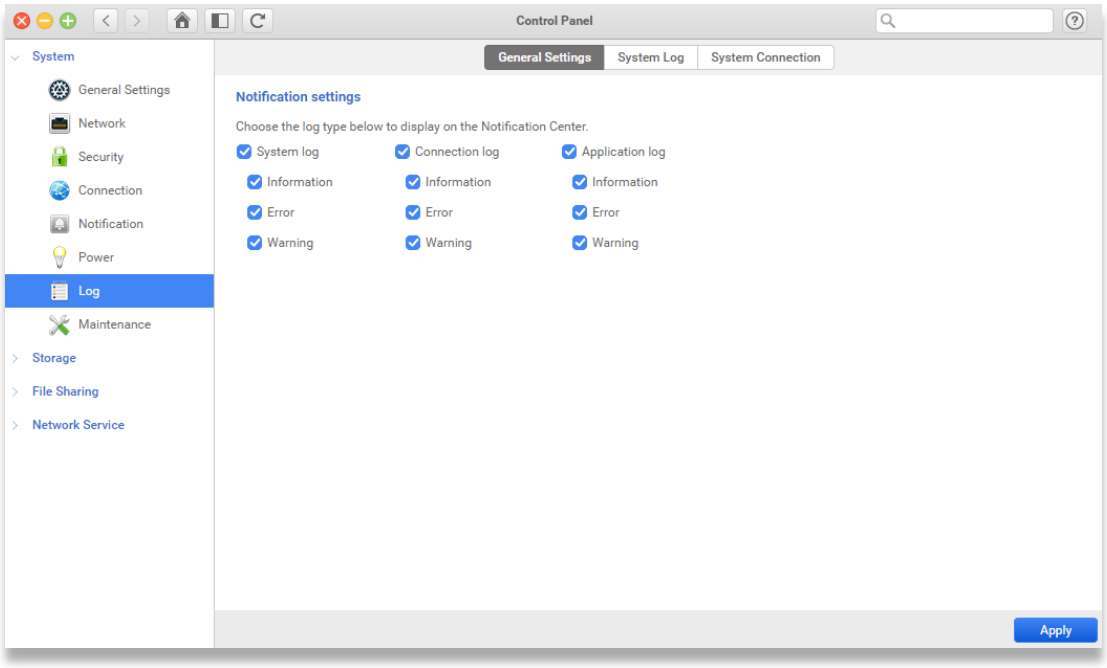
1. Select a schedule you want to remove.
2. Click **Delete**.
3. Click **Confirm** to save the settings.

Log

In Log, you can manage the types of log you would like to see in the Notification Center. You can also monitor the system and connection status easily and efficiently.

General Settings

In **General Settings**, you can choose the type(s) of event log you would like to see on the Notification Center. There are three types of log: Information, Error and Warning.



NOTE:

The classification of different log types:

- Information: Important information which should be recorded at all times, for example service starting, stopping, completed or settings being changed.
- Warning: Anything which can potentially cause damage to the system, but can be recovered automatically by the system, including operation failed, user login failed or system temperature abnormal.
- Error: Anything which is fatal to the system, including hardware malfunctioning, system temperature overheated or pool/volume created failed.

System log

System log includes all the functions under Control Panel, such as Storage, File Sharing and Network Service.

Connection log

Connection log includes all the access actions of the data services, such as login, logout, read, write, delete and more.

Application log

Application log includes logs from certain apps, such as File Manage, Backup, Cloud Sync, VPN Service and more.

Display logs in Notification Center

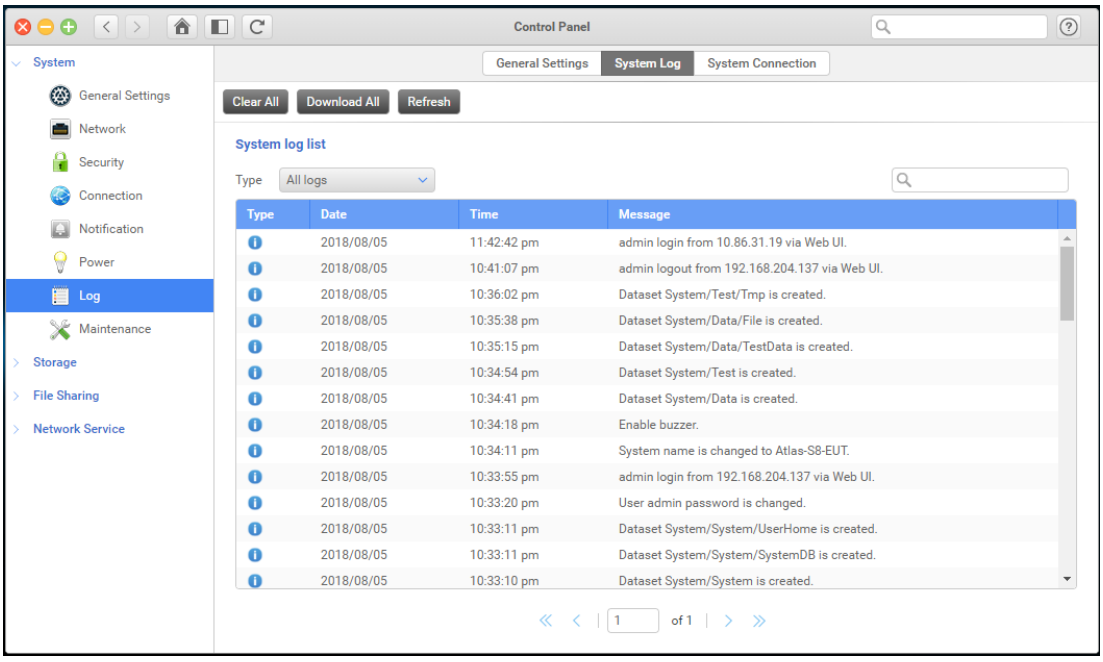
There are three levels of event severity: Information, Error and Warning.

1. To customize the events on the Notification Center, you can select the checkbox next to each log types.
2. Click **Apply** button to save the settings.

NOTE:
To make sure logs can be displayed in Notification Center successfully, please ensure that you have clicked the Show in Notification Center checkbox on the Log page of the app(s) you wish to display. For more information, please refer to the help page of the app interested.

System Log

In **System log**, you can view, download and search for logs related to the system. If you see an amber light showing on the front panel of your Atlas S8+ indicating errors may have occurred, you can refer to these event logs for troubleshooting.



NOTE:
The system can store up to 500 logs. If the numbers have reached the system limit, the earliest items will be deleted from the list automatically.

Clear all logs

To clear all the logs from your system, please follow the steps below:

1. Click **Clear All** button on the top of the page.
2. Click **Confirm** button to delete all logs.

Download all logs

To download all the logs from your system, please follow the steps below:

1. Click **Download All** button on the top of the page.
2. Choose the destination where you would like to store the logs in.

NOTE:
The downloaded file will be in .txt format, please open the file with software that supports .txt files.

Refresh the logs

By clicking **Refresh** button, the page will be reloaded and all the new event logs will be added to the list.

Filter the logs by its type

With the drop-down menu, you can choose to see all types of log or restricted to a specific type, such as Information, Warning and Error.

Search for logs

You can use the search bar to find logs quickly. To search the log history, please follow the steps below:

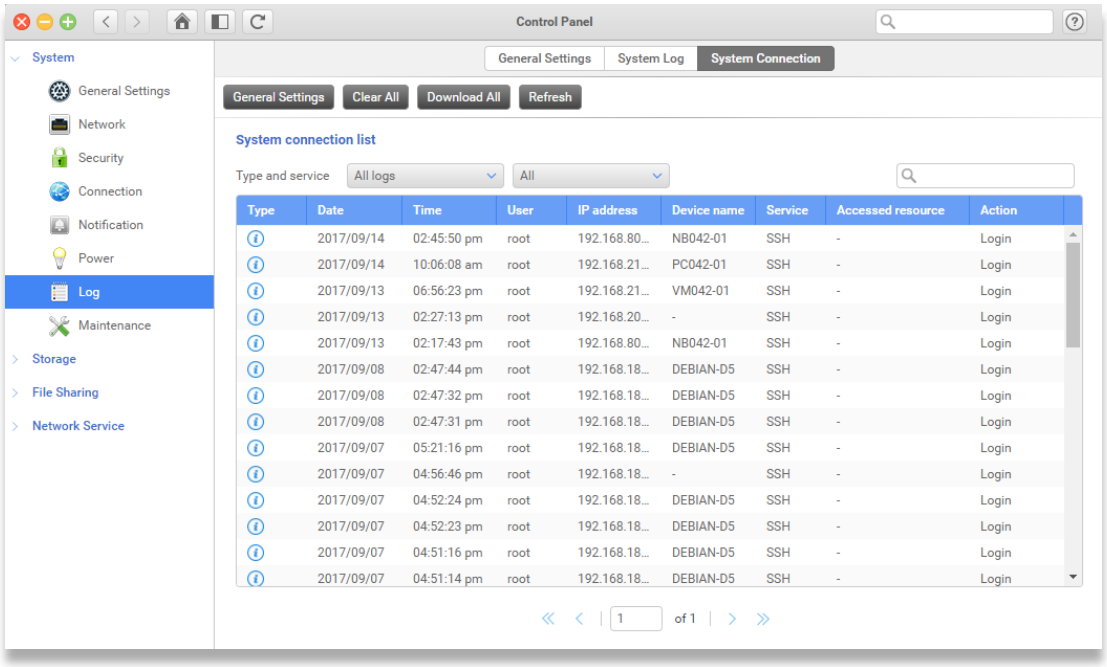
1. Enter the keyword in the search bar and press enter to search for logs with the matching keyword.

NOTE:
Valid characters: 【a-z A-Z 0-9】

2. To search the log history by its date and time, you can click the magnifying glass in the search bar on the top-right corner, the advanced search menu will appear.
3. Choose the date and time on the advanced search menu. Press **Search** to start searching for logs within the range.
4. Press **Reset** to return to the default setting.

System Connection

System connection contains connection history of how user's actions via each data service. Meanwhile, in overview page, you can download all logs or search particular events.



NOTE:

1. User actions: Login, log out, add, modify, delete, and move files.
2. Data service supported: CIFS, AFP, NFS, FTP(s)/SFTP, WebDAV(s), SSH, iSCSI, File Manager.

The file transfer performance might be slightly affected when logging is started.

Manage the log types to display

To choose the data services which you would like see on System connection list, please follow the steps below:

1. Click **General Settings** button.
2. Click the checkbox beside the services you would like to display.
3. Click **Confirm** button to save the settings.

NOTE:
Once you have chosen the service(s) you would like to display on the connection list and clicked the Confirm button, the selected service(s) will be restarted. Please make sure that you have finished all the task before confirmed.

Clear all logs

To clear all the logs from your system, please follow the steps below:

1. Click **Clear All** button on the top of the page.
2. Click **Confirm** button to delete all logs.

Download all logs

To download all the logs from your system, please follow the steps below:

1. Click **Download All** button on the top of the page.
2. Choose the destination where you would like to store the logs in.

NOTE:
The downloaded file will be in .txt format, please open the file with software that supports .txt files.

Refresh the logs by clicking the **Refresh** button, the page will be reloaded and all the new event logs will be added to the list.

Filter the logs by its type and action

With the drop-down menu, you can choose to see all types of log or restricted to a specific log type or data service.

Search for logs

You can use the search bar to find logs quickly. To search the log history, please follow the steps below:

1. Enter the keyword in the search bar and press enter to search for logs with the matching keyword.

NOTE:
Valid characters: 【a-z A-Z 0-9】

2. To use the advanced search tool, please click the magnifying glass in the search bar on the top-right corner.
3. Enter the criteria(s) you would like to search for on the advanced search menu. Press Search to start searching for logs within the range.
   - Date & Time range: Search for logs within the specific date and time range.
   - User: Search for logs by the specific user name.

NOTE:
Valid characters: 【a-z A-Z 0-9】

   - IP address: Search for logs by the specific IP address.

NOTE:
Valid characters: 【0-9】

   - Device name: Search for logs by the specific device name.

NOTE:
Valid characters: 【a-z A-Z 0-9】

4. Press **Reset** to return to the default setting.

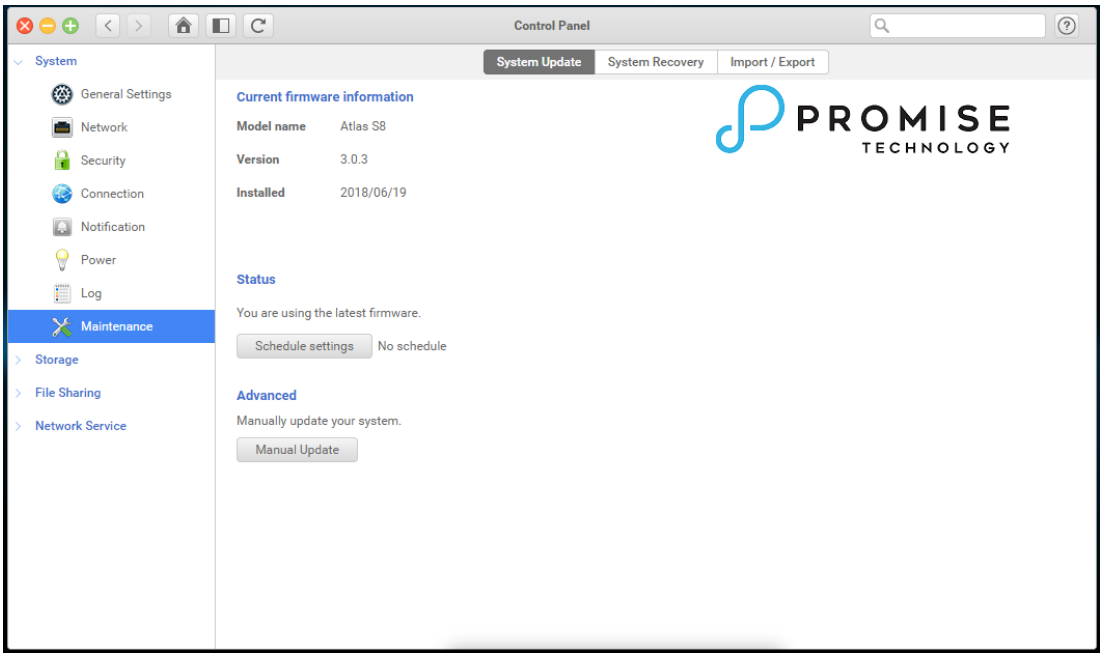
Maintenance

In this page, you can check and update firmware status, set the system back to factory default, and import or export system configuration.

System Update

This page shows current firmware information and firmware update schedule. PROMISE releases free ASM updates for new features, function improvement, and performance enhancements.

NOTE:
Updating firmware does not affect the data on Atlas S8+. But it is recommend to always back up of your data as a general principle.



Current firmware information

It shows the model name, version and installed date of the current firmware on your Atlas S8+.

Status

To make sure your Atlas S8+ is always up to date, you can setup the firmware update schedule by steps below:

1. Click **Schedule Setting**.
2. Choose one of the following options:
   - **Check update automatically** and set the schedule and time.

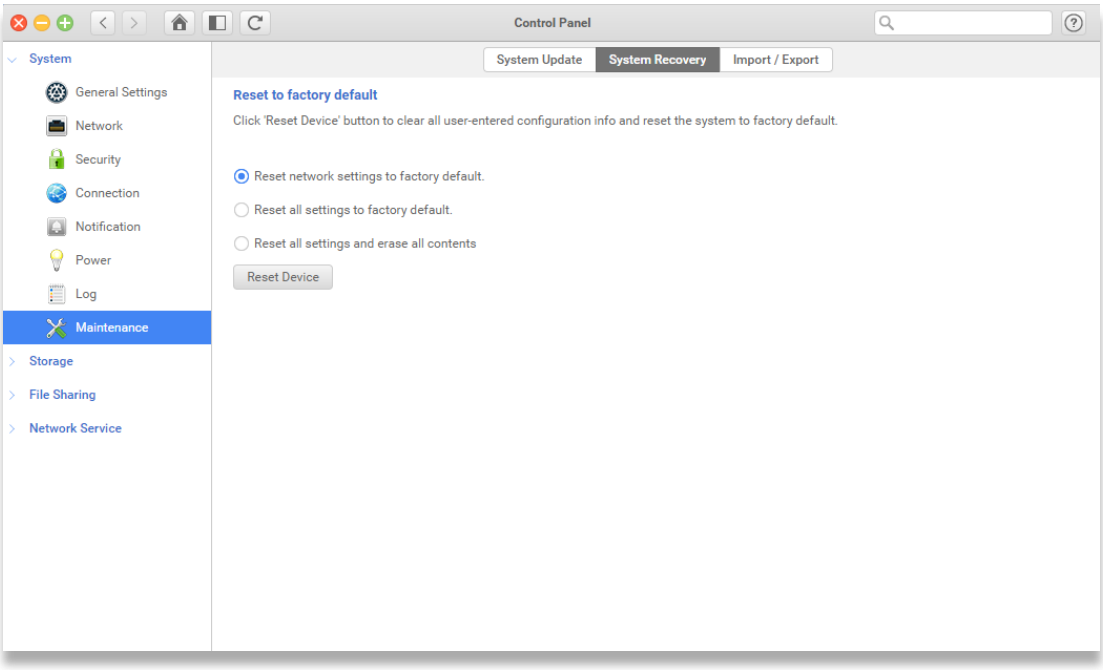
- **Never check update automatically**.

3. Click **Confirm** to save the settings.

NOTE:
Firmware cannot be rolled back to versions earlier than what is currently installed.

System Recovery

If the system has any issues due to the unexpected failure, the System Recovery setting allows the system to clear all user configuration, and the system will be restored to factory default.



Reset to factory default

The Atlas S8+ provides three methods below to reboot the system with faculty setting:

1. **Reset network setting to factory default** : If you choose reset network setting to factory default and click **Reset Device**, your system configuration will result in:

   ① Reset the “admin” password to "password".
   ② All networking set to "DHCP".
   ③ All data service ports set to the default setting (All data service enable and set to default port).
   ④ VLAN will be terminated.
   ⑤ Vswitch will be deleted.

⑥ Port trunking will be disabling.
⑦ After configs will be deleted, RESTART the NAS.
⑧ Log out PROMISE Cloud.
⑨ DNS settings.
⑩ DDNS and UPNP settings.

NOTE:
When joined to an AD domain, the DNS will not be reset.

2. **Reset all setting to factory default** : If you choose reset network setting to factory default and click **Reset Device**, your system configuration will result in:

   ① All **(1)** settings.
   ② System settings set to default.
   ③ All accounts, groups, folder permission, and ACL will be deleted.
   ④ All Access control lists will be deleted.
   ⑤ All backup tasks will be deleted.
   ⑥ All Cloud sync job will be deleted.
   ⑦ AntiVirus setting will be deleted.
   ⑧ Media Library index will be deleted.
   ⑨ After all configurations are deleted, RESTART the NAS.

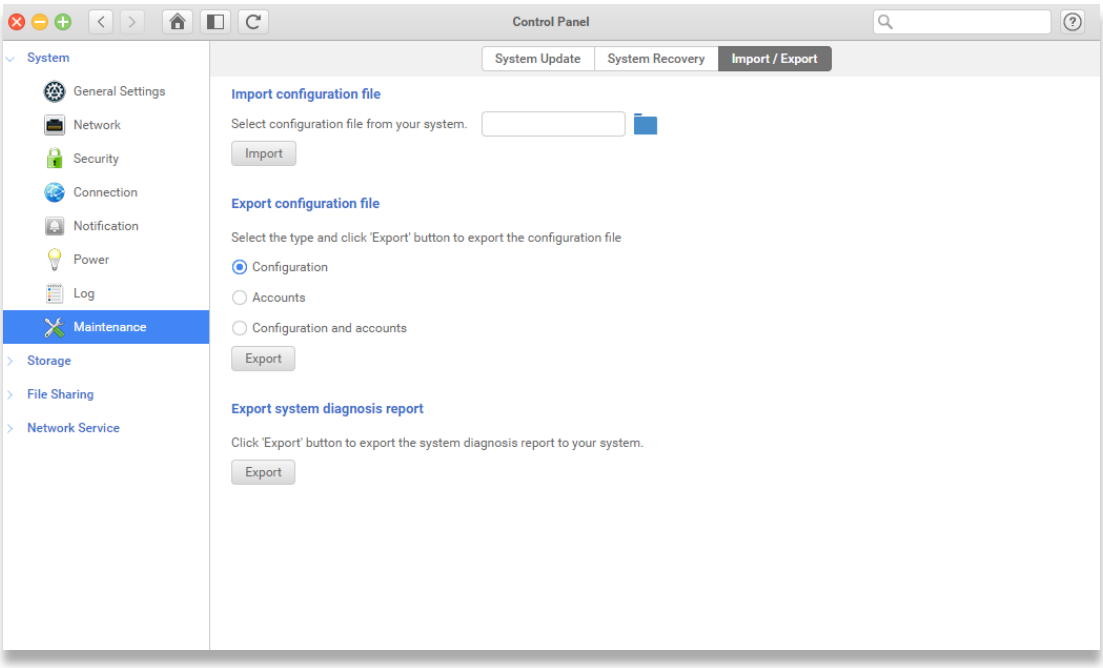
3. **Reset all settings and erase all contents** : If you choose to reset all settings to factory default and click **Reset Device**, your system configuration will result in:

   ① Include **(1)** and **(2)**.
   ② Erase all disk pools, sharedisks and iSCSI volumes.
   ③ After data and configurations are deleted, RESTART the NAS.

NOTE:
If a WORM folder exists, this option will be grayed out, So you will not be able to reset your Atlas S8+.

Import / Export

You can use your Atlas S8+ settings on another Atlas S8+. You will only need to setup once and Import/Export configuration file to another device. Every setting will be the same as your first setup one.



Import configuration file

To import the configuration file, please follow the steps below:

1. Click the “Folder symbol” to upload the configuration file that you would like to import.
2. Click **Import** to import the configuration file.

NOTE:
The import file (.bin) can only be the export configuration files from another Atlas S8+.

Export configuration file

To Export the configuration file, please follow the steps below:

1. Select the configuration you want to export.
2. Click **Export** to export the configuration file of this NAS.

NOTE:
The exported configuration will be named as “CONFIG-YOUR Device name-Date and time.bin”.

Export system diagnosis report

Click **Export** to export the system report for diagnosing. These files can help PROMISE support and Engineers to diagnose the unexpected issues.

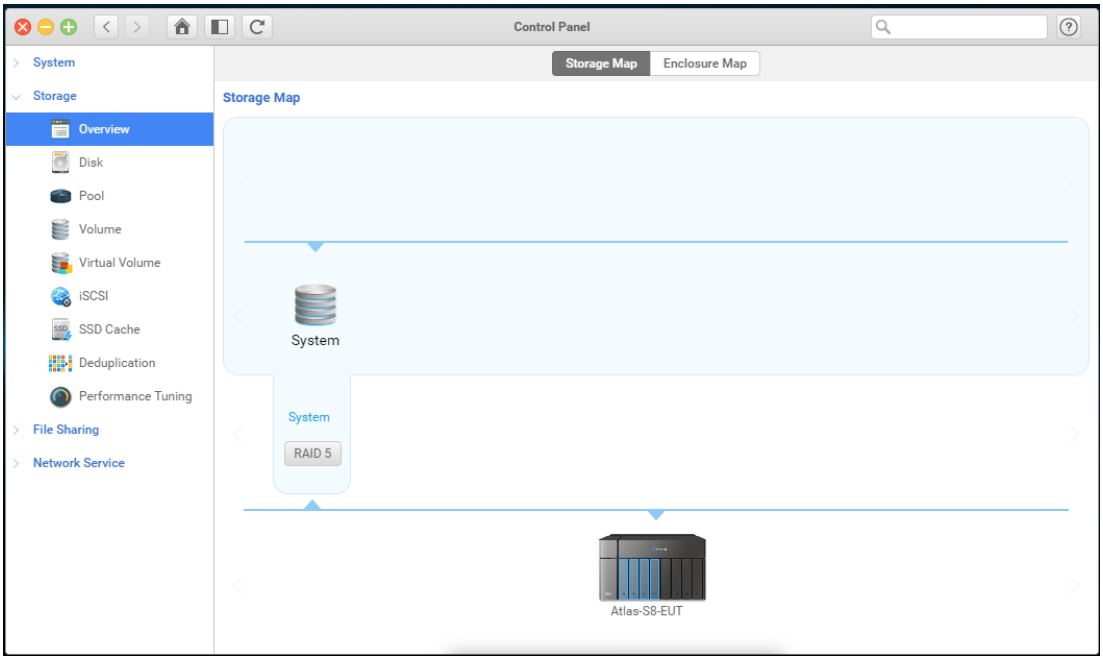
Storage

Overview

In **Overview**, you can check the structure of storage space and all connected enclosures.

Storage Map

In **Storage Map**, you can check the all pool structure, quick access to **Folder** setting page.



Check the pool structure

For administrators, it is always important to have a quick view of current storage space structure.

To check the pool structure, please follow the steps below:

1. Click a pool you want to check.
2. The page will show the information of the pool.

NOTE:

1. After selecting a pool, all disks in this pool will be highlighted on the machine.

2. While selecting a RAID group, all disks in the RAID group will be highlighted on the machine

Quick access to the setting page

To make the management easier on each folder, you can simply click the folder icon showing on the page.

To quickly access the folder, please follow the steps below:

1. Select the Folder on the top of the window.
2. Click the folder icon.
3. UI will direct you to the setting page of the selected folder.

Check your expansions

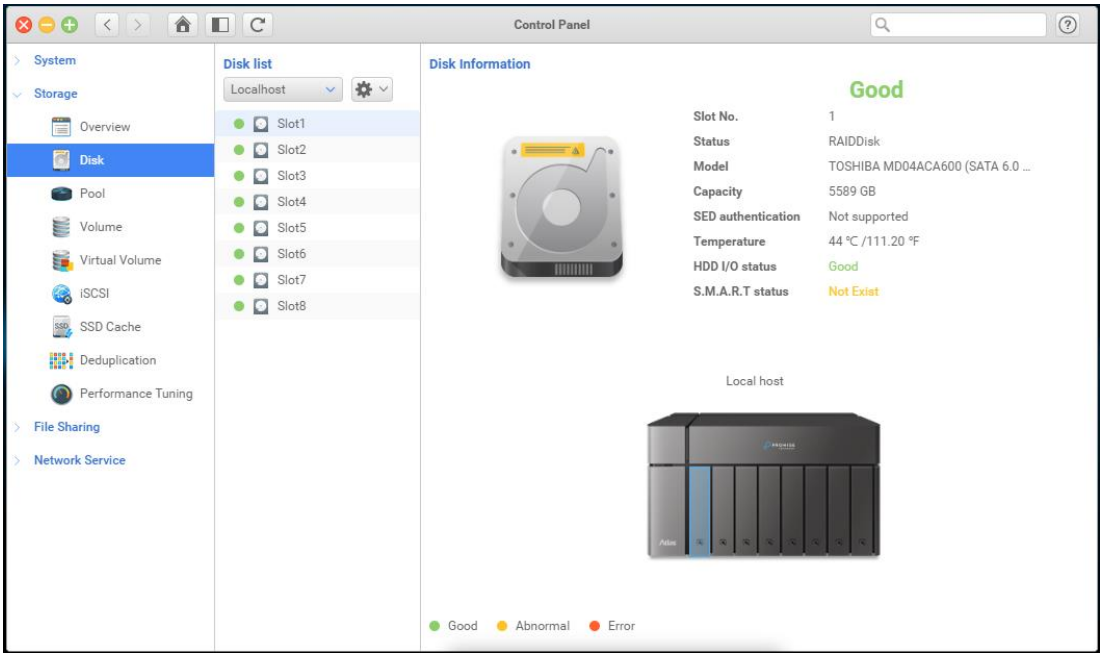
While connecting to expansion units, you can easily check the connecting speed or click it to view more information for the unit.

To view the status, please follow the steps below:

1. Select the **Enclosure** on the page.
2. One click the enclosure
3. UI will direct you to the monitor page to show more information.

Disk

In **Disk**, you can view the status, check the basic information and manage for each internal disk which was installed on your Atlas S8+ or expansion units.



Set global spare

If a pool is a redundant RAID such as RAID5 or RAID6 fails, it will automatically rebuild to a global spare if one is present in the system.

To set a **Global spare**, please follow the steps below:

1. Select a disk from the list.
2. Click the function button in the top right corner of the disk list.
3. Click **Global spare**.

NOTE:
You can only configure a FreeDisk as a global spare.

1. A confirmation window will pop out.
2. Click Confirm to finish the action.

NOTE:
To make the spare disk as free disk, please check Set free function.

Identify a disk

In some circumstances, system administrators need to locate a physical disk; this feature helps them to find disks locally and in enclosures.

To identify the disk, please the steps below:

1. Select a disk from the list.
2. Click the function button in the top right corner of the disk list.
3. Click **Identify disk**.
4. Disk blinking window will pop out.
5. Click **OK** to turn off the disk identification.

Self-encrypting drives

Self-encrypting drives (SEDs) designed using an open industry standard which developed by the Trusted Computing Group (TCG) provide protection for data at rest and in transit and meet criteria established by government agencies around the world. **Instant erase** and **Unlock** are the features only for SED supported disks.

Instant erase disks

This feature is designed to secure the data on the disk by setting the disk back to factory default and make the data instantly and permanently unreadable.

NOTE:
Enable SED protection on System > Security > SED, before performing this action.

To instant erase disks, please follow the steps below:

1. Select a disk from the disk list.

NOTE:
You can select only SED supported disks.

2. Click the function button in the top right corner of the disk list.
3. Click **Instant erase**.
4. Enter system administrator's password to ensure the security.
5. Select the disk you wish to instant erase.
6. Input the SED authentication code by entering the code, import the authentication key or PSID.

NOTE:
1. The disk manufacturer provides PSID, and it can be found on its label.

2. The SED authentication code or key to unlock the disk may not be as same as the authentication on your Atlas S8+.

7. Click **Confirm** to finish the action.

Unlock a disk

Self-encrypting drive (SED) is a hard basis encryption method by disk controller chips. For the data security, each access needs its authentication code, which means, before accessing the disk, you will need to unlock it.

To unlock the disks, please follow the steps below:

1. Select a disk from the disk list.
2. Click the function button in the top right corner of the disk list
3. Click **Unlock**.

NOTE:
Before unlocking the SED disk, you need to enable SED authentication in Control panel > Security > SED Authentication.

4. Select the disks you wish to unlock.
5. Enter the authentication password or import the authentication key.

NOTE:
The password or key may not be the current authentication on your system.

6. Click **Confirm** to finish the action.

Set free a disk

If you want to set your disk as a free disk, you can set it free and make it for another usage.

To set free a disk, please follow the steps below:

1. Select a disk from the disk list
2. Click the function button in the top right corner of the disk list.
3. Click **Set free**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

NOTE:
You can set free a disk from a mirror RAID set and the RAID will automatically change to RAID 0. You will lose RAID protection.

S.M.A.R.T. Test

S.M.A.R.T. stands for Self-Monitoring, Analysis, and Reporting Technology, which helps system administers to monitor and understand the disk status to prevent internally disk damage.

To do the S.M.A.R.T. test for a disk, please follow the steps below:

1. Select a disk from the list.
2. Click the function button in the top right corner of the disk list.
3. Click **S.M.A.R.T.** Test.

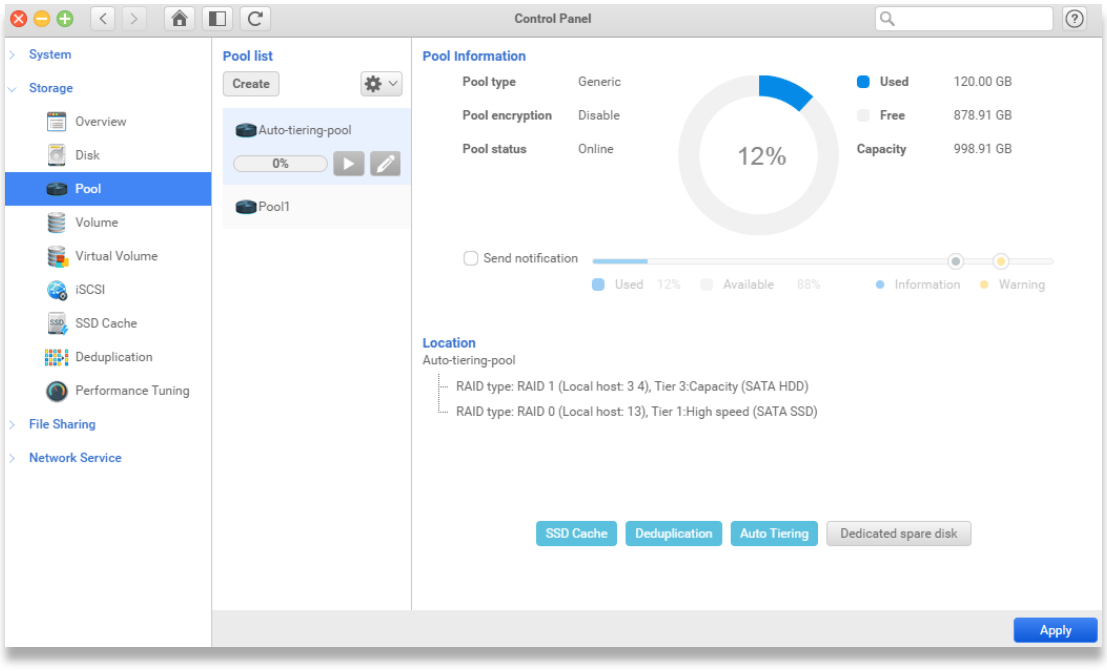
4. Select **Quick Test** or **Full Test** and click start.
5. The test result will be shown below.
6. Click **OK** to close the window.

NOTE:
Not all disks support the S.M.A.R.T. test.

Pool

In **Pool**, you can view detailed information about all pools on your Atlas S8+, such as pool type, status, and capacity usage. You can also setup the **SSD Cache**, **Deduplication**, **Auto Tiering**, **Spare disks**, and **SED authentication**.

NOTE:
A pool is a set of drives that provide specific storage characteristics for the resources that use them.



In this page, you can create a pool, expand or edit the existing pools, unlock the encrypted pool, export the pool encrypting key, scrub the pool and delete a pool. Meanwhile, you can also make quick settings by the button listed below. The button with gray background color

means the function is supported for the pool and the blue background color means the feature is enabled for the pool.

Create a pool

A pool provides optimized storage for a particular set of applications or conditions. When you create a storage resource for hosts to use, you must choose a pool with which to associate the storage resource. If there are multiple types of disk drivers in the system, you can define an auto tiering pool for more storage efficiency and performance. In physical deployment, each tier can be associated with a different RAID type.

NOTE:
Atlas S8+ supports RAID0, 1, 5, 6, 10, 50, 60 and JBOD.

To create a pool, please follow the step below:

1. Click the **Create** button at the top of the **Pool list**.
2. Specify the pool type for your purpose, **Generic**, **Media streaming**, **Data base**.
3. Enable or disable Auto tiering for the pool.
4. Enable or disable SED protection. If you choose to enable the SED protection, please enter the SED authentication for the Atlas S8+.

NOTE:
1. This feature supports only SED drives.

2. If your SED authentication has been created, you will not need to enter password again.

5. Specify the general settings for the pool, such as pool name, setting the disk write cache and pool encryption.

NOTE:
1. Disk write cache: The cache is the disk built in cache.
2. Pool encryption is a software based encryption to improve data security
3. Auto unlock is for the disk and system share the same password, it will unlock when the disks are inserted.
4. Pool name length: 1-32 characters.
5. Pool name allows only alphabet prefix.

6. “.” Can’t be placed neither in the beginning nor the end.
7. Valid characters: a-z, A-Z, 0-9, -_.
8. Pool encryption password: a-z, A-Z, 0-9, -_.!@#$%^&*()_+=?

6. Specify a RAID type to create the pool
7. Select the Tiering type if the pool is set for enabling Auto Tiering.
8. Select the disk from the local machine or connected enclosures.

NOTE:
The disk table shown on the screen shows only the select tier or enclosures.

9. Select a RAID type for the selected disks. The estimated capacity depends on the RAID type and selected disks.
10. If desired, select a dedicated spare disk for this particular RAID set.

NOTE:
1. A dedicated spare disk is based on its capacity and disk type.
2. The capacity of the spare disk needs to be greater or equal the largest capacity of the selected disks.
3. If the pool is set to auto tiering pool, the spare disk need to be the same type as the selected disks.

11. Check the create-pool summary.
12. Click **Confirm** to finish the action.

Expand the pool

When a pool is short of shortage capacity, the Atlas S8+ offers two ways to increase pool capacity, it can be expanded by adding more disks to the RAID with **Adding a RAID set**, or the capacity can be increased by swapping in large hard drives with **Increase RAID set Capacity**.

To expand the pool capacity, please follow the steps below:

1. Select a pool from the pool list.
2. Click the function button in the top right of the pool list.
3. Select an expanding method.

a. Adding a RAID Set.

① A create-window will pop out.
② Select the disk from the local machine or connected enclosures.

NOTE:
If the pool is auto tiering pool, you will need to choose a tier to create your RAID set.

③ Set the RAID type and dedicated spare disk and click Next when you finish setting.
④ Check expand pool summary/
⑤ Click Confirm to finish the action.

b. Increase RAID set capacity.

① An online RAID expand window will pop out.

NOTE:
Online expand does not support RAID 0.

② Select a RAID set to be expanded.
③ Select the disk you would like to replace and click the Change button at the top right corner.
④ After clicking the change button, you can find the disk LED identification light is blinking.

CAUTION:
Before next step, please take note of the following:

1. Do NOT turn off the power during the procedure.
2. Please remove the disk which was selected.
3. Please do NOT swap disks during rebuilding.

⑤ Remove the disk.
⑥ Insert a new disk that the capacity is larger or equal capacity than the disk you removed in step 5.
⑦ After the synchronizing finished, please repeat step 5 and 6 for the disk which were not replaced to finish online RAID expand.

NOTE:
If the disk has been used or locked, please set free or unlock the disk to finish the action.

⑧ When all disks are replaced, click **OK** to close the window.

Edit a pool

After the pool is created, the pool configuration can be setup afterward.

To edit a pool, please follow the steps below:

1. Select a pool from the pool list.
2. Click the function button at the top right corner of the pool list.
3. Click **Edit**.
4. An edit window will pop out.
5. Setup **Disk write cache**, **Pool encryption**, set **Dedicated spare disk** for each RAID set.
6. Click **Confirm** to finish setting.

Decrypt a pool

When pools are roaming from other Atlas S8+ and set for pool encryption, you need to unlock it before accessing.

To unlock a pool, please follow the steps below:

1. Select the locked pool from the pool list.
2. Click the function button at the top right corner of the pool list.
3. Click **Unlock**.
4. A decryption window will pop out.
5. You can either **Enter password** or **Import key** to decrytpe the encrypted pool.
6. Click **Confirm** to finish action.

Export Key

When the pool is encrypted, you can export the pool encryption key for you easy to manage the authentication.

To export the pool encryption key, please follow the steps below:

1. Select the pool with pool encryption from the pool list.
2. Click the function button at the top right corner of the pool list.
3. Click **Export**.
4. The encryption key will be downloaded immediately.

Scrub

This feature is for file system integrity. Scrub is for file system repair and system validation.

NOTE:
Pool scrubbing will be triggered by system while rebuilding the pool.

To manually start scrubbing the pool, please follow the steps below:

1. Select a pool from the pool list.
2. Click the function button at the top right corner of the pool list.
3. Click **Scrub**.
4. A confirmation window will pop out.
5. Click **Confirm** to start the action.
6. Click cancel to return to the pool menu

Delete

When the pool is no longer needed, you can always delete the pool.

NOTE:
A pool cannot be deleted unless all the volumes in the pool are deleted.

To delete the pool, please follow the steps below:

1. Select the pool from the pool list.
2. Click the function button at the top right corner of the pool list.
3. Click **Delete**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

Auto Tiering pool

PROMISE Auto Tiering cost-effectively and dynamically places hot data on SSD or faster hard drives and cold data on lower cost high-capacity drives, allowing you to optimize application performance without straining your budget or sacrificing capacity. When you are creating an auto-tiering pool, you can set different types of RAID sets which can be divided into different tiers, such as, a high speed tier or a high capacity tier.

When you first create a pool with Auto tiering feature enabled, you will need to expand the auto tiering pool to put another RAID set, to make the auto tiering pool, please follow the steps below:

1. Select an auto-tiering pool from the list.

NOTE
You can find the auto-tiering pool on the pool list that with start button and progress bar.

2. Click the function button at the top right corner of the pool list.
3. Click **Expand**.
4. Select **Expand the pool by adding another RAID set**.
5. Select the **Tier type**.
6. Select the disk location.
7. Select the disk(s).

NOTE
You can only use one type of disk for one tier.

8. Specify the RAID type.
9. Select the dedicated spare disk if needed.
10. Click **Next** to check the summary.
11. Click **Confirm** to finish the action.

After the auto tiering pool has been created, relocating the hot, warm, and cold data is the main factor for the auto-tiering pool. You can set the relocation manually or make it by schedule.

To start the data relocation manually, please follow the steps below:

1. Select an auto-tiering pool from the list.

NOTE
You can find the auto-tiering pool on the pool list that with start button and progress bar.

2. Click the start button on the bottom of the pool name.
3. The data relocation will start right away, and the progress will be shown below.

To start the data relocation by schedule, please follow the steps below:

1. Select an auto-tiering pool from the list.
2. Click the edit button on the bottom of the pool name.
3. A schedule setting window will pop out.
4. You can set the schedule as **Daily**, **Weekly**, **Monthly**, or **Repeat** in a period of time.
5. Set up the start time.
6. Set up the duration time.

NOTE
During the data relocation, the system performance may be affected. You can schedule the data relocation for a time when the Atlas S8+ is not heavily utilized.

7. Set up the relocation rate.

NOTE:
The relocation rate determines how Atlas S8+ resources are allocated, the Fast rate allocates more system resources to the relocation.

To check the detail information for auto tiering pool, please follow the steps below:

1. Select the auto-tiering pool from the pool list.
2. Click the **Auto Tiering** button on the bottom the right-hand side.
3. A detail information window will pop out.
4. You can check the current status or the history by clicking the tab on the top.

Monitor pool capacity usage

Storage space is a cost and resource sensitive object. For system administrators, we keep you updated of the usage of storage spaces by simply few clicks.

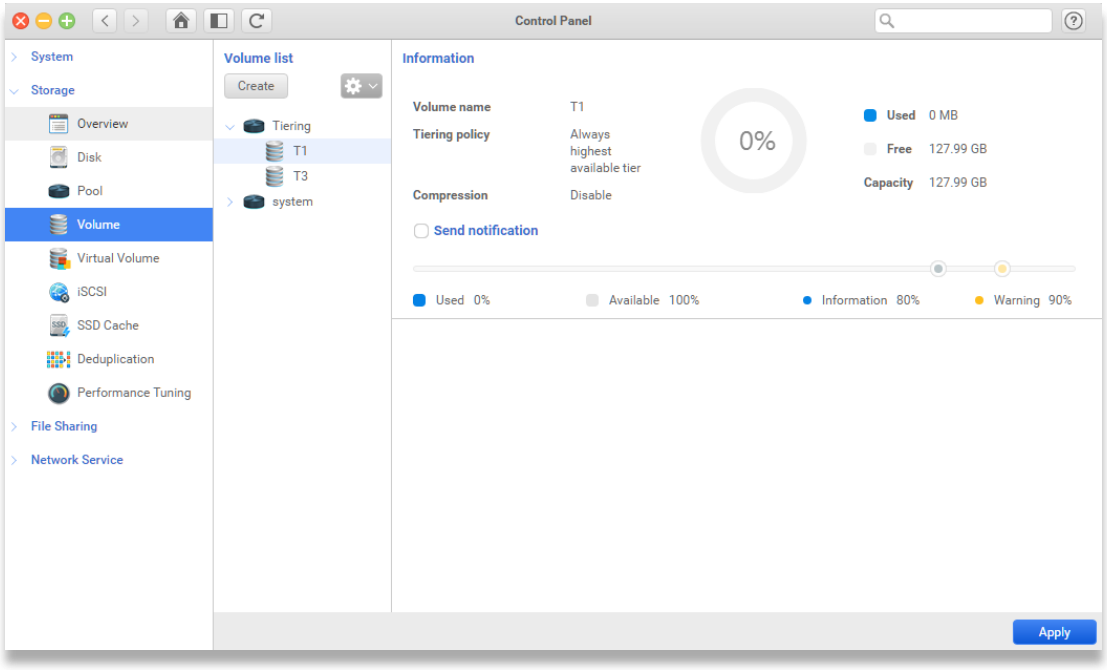
To set the notification of pool capacity usage, please follow the steps below,

1. Click the check box of **Send Notification**.
2. Scroll the blue spot to set the information level notification.
3. Scroll yellow spot to set the Warming level notification.
4. Click **Apply** to finish the setting.

Volume

In **Volume**, you can view the current status, edit volume properties and delete volumes.

NOTE:
A volume is a single accessible storage area with a single file system.



Create a volume

A volume is a single accessible storage area with a single file system, typically resident as a single partition of a hard disk.

To create a volume, please follow the steps below:

1. Click **Create** button on the top of the volume list.
2. Specify the name of the volume

3. Specify the location of the volume, such as pool1.
4. Specify the volume capacity or scroll the bar shown below.
5. Specify the tiering-policy if the pool is set to enable Auto tiering.
6. Click the checkbox and set the compression level.
7. Click **Next**.
8. Check the summary of the volume you are going to create.
9. Click **Confirm** to finish the action.

Edit a volume

After the volume has created, you can always increase its capacity, auto tiering policy and enable/disable compression level.

To edit the volume, please follow the step below:

1. Select a volume on the volume list. You can check the volume location on the list.
2. Click the function button on the top right of volume list.
3. A edit window will pop out.
4. Scroll the bar to increase the capacity.
5. Click the dropdown menu to set the auto tiering policy.
6. Click the check box to enable or disable of compression.
7. Click **Next**.
8. Check the summary of the volume.
9. Click **Confirm** to finish the action.

Delete a volume

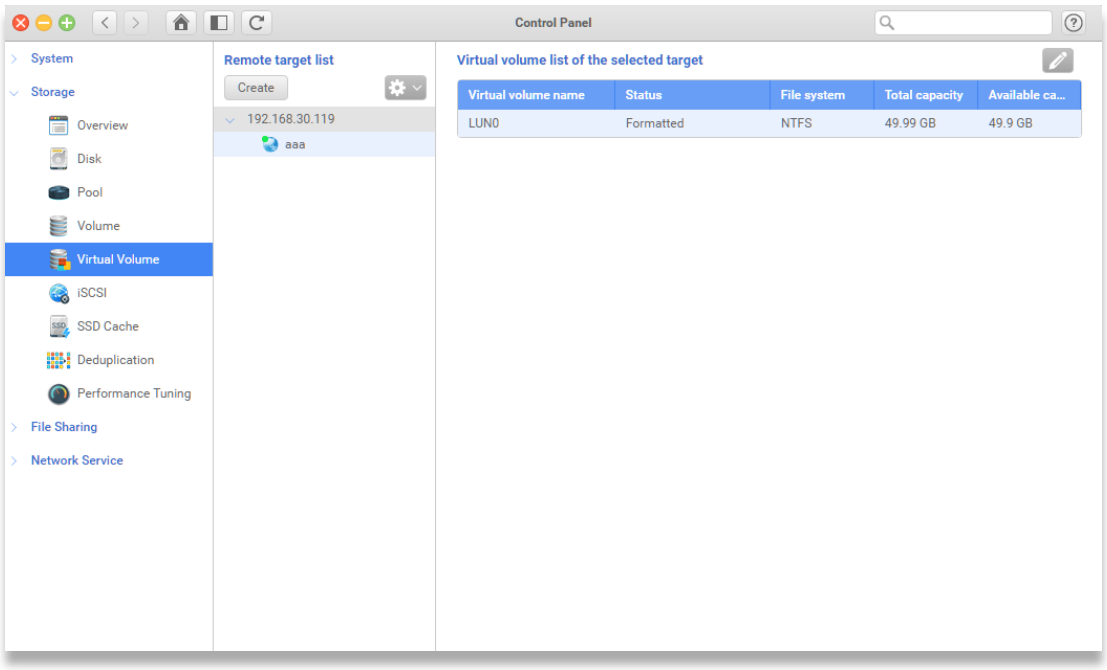
When the volume is no longer needed, you can delete the volume after all shared folder is deleted.

To delete the volume, please follow the steps below:

1. Select the volume on the volume list. You can check the volume location on the list.
2. Click the function button on the top right of volume list.
3. A confirmation window will pop out.
4. Click **Confirm** to finish the setting.

Virtual Volume

In **Virtual Volume**, you can create a target list to connect your remote target to extend your storage capacity. You can reconnect/disconnect, edit, copy the IQN and delete the target.



Create a remote target

By creating a remote target, you can see the volumes which you can use on your local Atlas S8+ or by other OS which supports virtual volumes. We support it connect via Ethernet and Thunderbolt 3 interfaces.

To create a remote target, please follow the steps below:

1. Click **Create** on the top of the remote target list.
2. Select the interface you prefer to connect your remote target or use **All** to auto-detect the target.
3. Enter the IP of the remote target or click the drop menu to broadcast all available remote target.
4. Specify the port for your remote target and its default value is 3260.
5. Click **Connect**.
6. Select the target on the remote destination.
7. Specify CHAP if needed.

8. Click **Confirm** to finish the action.

NOTE:
The target list will be shown as its IP address of the remote destination.

Edit the Virtual Volume

After connected to the remote target, you can check the virtual volume list on the right. You can see how many virtual volumes on the target, its status, file system, capacity, and its available capacity. At the same time, you can make an edit of the virtual volumes.

To edit the virtual volumes, please follow the steps below:

1. Select a virtual volume on the remote target list.
2. Click the **Edit** button on the top right-hand side of the virtual volume list of the selected target.
3. After clicked the checkbox of **Format now**, you can assign the file system of the virtual volume and change its name.
4. Click **Confirm** to finish the setting.

Disconnect a virtual volume

You can disconnect the online virtual volume, you can simply click the disconnect to finish the action.

To disconnect a virtual volume, please follow the steps below:

1. Select a virtual volume on the remote target list.
2. Click the function button on the top right-hand side of remote target list.
3. Click **Disconnect**.
4. The virtual volume will be disconnected.

Edit remote target

You can edit the CHAP authentication by clicking edit to finish the action.

To edit the remote target, please follow the steps below:

1. Select a virtual volume on the remote target list.
2. Click the function button on the top right-hand side of remote target list.
3. Click **Edit**.

4. The edit remote target window will pop up.
5. Specify the CHAP authentication.
6. Click **Confirm** to finish the action.

IQN

For system administrators, we provide a convenience features to help them finish settings faster, Copy the IQN.

To copy the IQN, please follow the steps below:

1. Select a virtual volume on the remote target list.
2. Click the function button on the top right-hand side of remote target list.
3. Click **IQN**.
4. The IQN window will pop out.
5. Click **Copy & Close**.
6. The IQN will be on the clipboard of your system.

Delete a remote target

When the remote target is no longer needed on the system, you can easily remove it by clicking one button.

To delete the remote target, please follow the steps below:

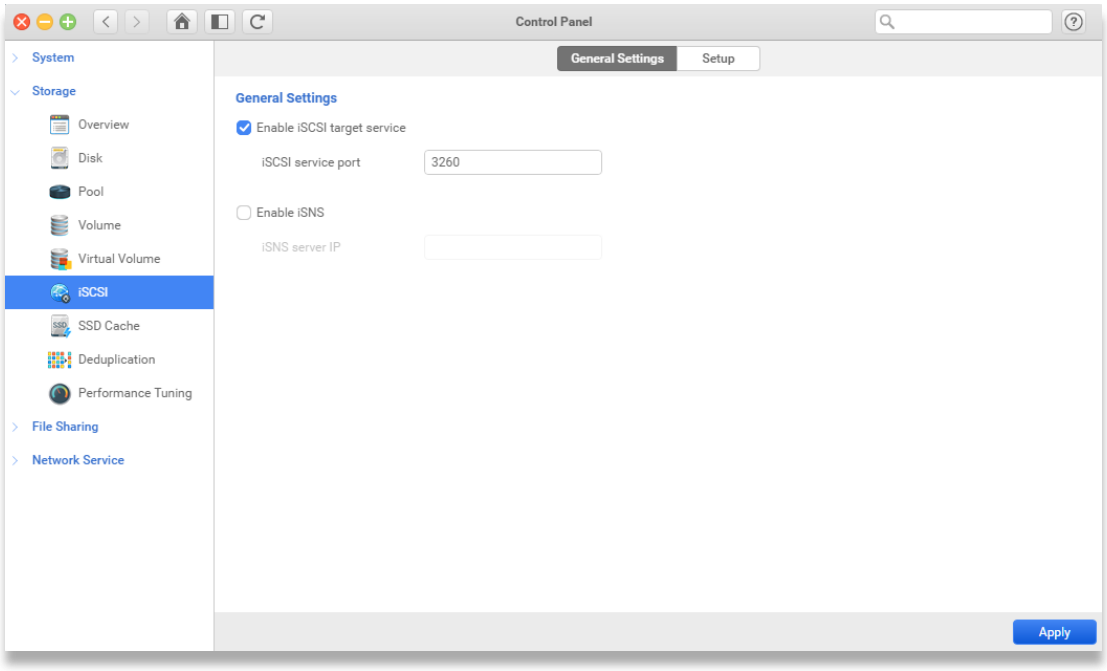
1. Select a virtual volume on the remote target list.
2. Click the function button on the top right-hand side of remote target list.
3. Click **Delete**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

iSCSI

In **iSCSI**, you can manage the **General settings**, **Target**, and **LUN** setups.

General Settings

In **General settings**, you can manage the iSCSI target service and configure its service port. Meanwhile, you can also setup the iSNS server IP address.



NOTE:

1. iSCSI Target service is an industry standard protocol allows sharing storage over the Ethernet. The server shares the storage called iSCSI Target. The server consumes the storage is called iSCSI initiator.

2. iSNS server is Internet storage name services protocol. This protocol is used for interaction between iSNS servers and iSNS clients.

Enable iSCSI target service

By enabling the iSCSI services, it can help the clients to connect the target on you Atlas S8+.

To enable the iSCSI target service, please follow the steps below:

NOTE:
By default the target service is enabled.

1. Click **Enable iSCSI target service**.
2. Specify the iSCSI service port numbers.

NOTE:
Default port is 3260.

3. Click **Apply** to finish the setting.

Enable iSNS

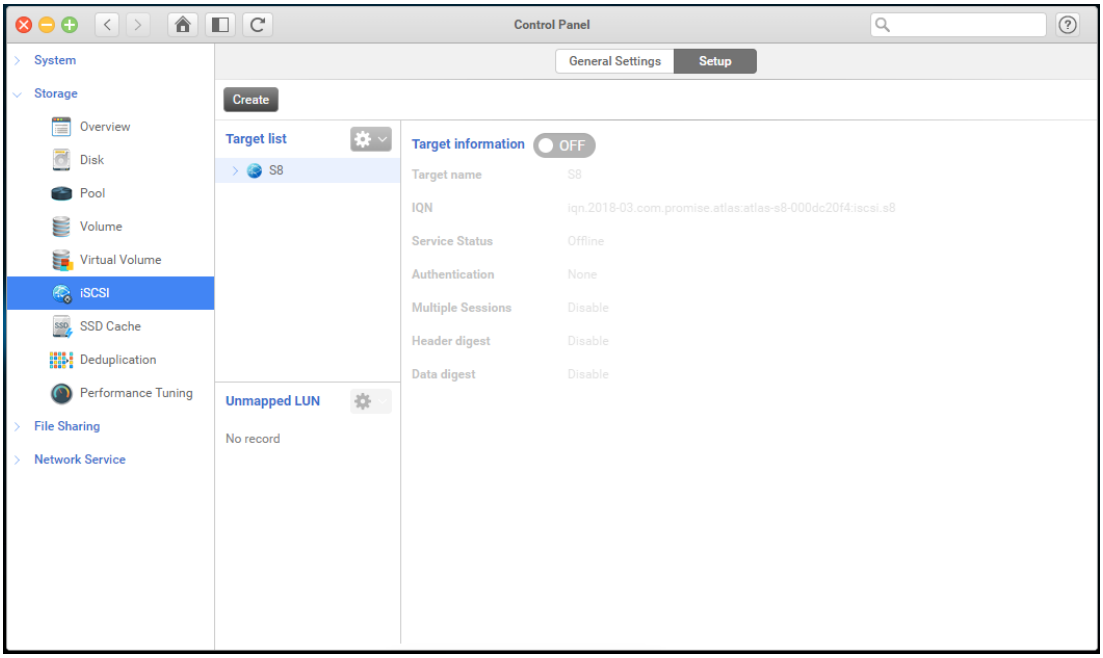
iSNS server provides intelligent storage discovery and management services comparable to those found in you networks.

To enable the iSNS service, please follow the steps below:

1. Enter the IP address of the iSNS server.
2. Click **Apply** to finish the setting.

Setup

In Setup page, we can create, edit, and modify Targets and LUNs .



Create target and map an LUN

An iSCSI LUN is a type of storage area networking service that provides additional storage capacities for another system to use. A target is an object which allows the iSCSI initiators to make the connection and a mapped LUN provides the storage capacities.

To create target and map a LUN, please follow the steps below:

1. Click **Create** button in the top right-hand corner of the window.
2. A create wizard will pop up.
3. Choose which way you want to use, **Create a target and map a LUN**, **Create a target**, **Create a LUN**, and click **Next**.

a. Create a target and map a LUN

① Specify the target name
② Choose to enable CHAP or not
③ If you choose to enable CHAP, you can enable Mutual CHAP.
④ Select the CRC checksum
⑤ Specify whether to allow multiple sessions or not.
⑥ Click **Next**.
⑦ Specify the LUN name.
⑧ Select its location. It should be located based on pool level.
⑨ Specify its allocation, Thin provision or Thick provision.
⑩ Specify its capacity by entering the number or scroll the bar.
⑪ Specify the tiering policy if it is located on an auto-tiering pool
⑫ Specify the compression.
⑬ Map an iSCSI target. In this create scenario, the LUN will be mapped to the iSCSI target you just created.
⑭ Click **Next**.
⑮ Check the creating summary.
⑯ Click **Confirm** to finish the action.

b. Create a target

① Specify the target name
② Choose to enable CHAP or not
③ If you choose to enable CHAP, you can enable Mutual CHAP.
④ Select the CRC checksum
⑤ Specify whether to allow multiple sessions or not.
⑥ Click **Next**.
⑦ Check the creating summary.

⑧ Click **Confirm** to finish the action.

c. Create an LUN

① Specify the LUN name.
② Select its location. It should be located based on the pool level.
③ Specify its allocation, Thin provision or Thick provision.
④ Specify its capacity by entering the number or scroll the bar.
⑤ Specify the tiering policy if it is located on an auto-tiering pool
⑥ Specify the compression.
⑦ Click **Next**.
⑧ Check the creating summary.
⑨ Click **Confirm** to finish the action.

NOTE:

1. CHAP is a protocol that is used to authenticate the peer of a connection and is based upon the peers sharing a security key.

2. With mutual CHAP, with this level of security, the target and the initiator authenticate each other.

3. CRC checksum is an error detection mechanism in which a special number is appended to a block of data to detect any changes introduced during transmission.

4. Header digest is to ensure the validity of the header portion of the protocol data unit.

5. Data digest is to validate the data segment of the PDU.

6. The Atlas S8+ supports multiple sessions between different initiators.

Enable or disable a target

After the target is created, the target is not yet connectable. You have to turn on the target so that can make initiators discover it.

To turn on the target, please follow the steps below:

1. Select a target from the target list.
2. Click the Target Information switch to enable the target.
3. After the button is clicked, the target is started.

Edit a target

You can always change the authentication, checksum setting and multisession settings afterwards.

To edit a target, please follow the steps below:

1. Select a target from the target list.
2. Click the function button on the top right-hand side of the target list.
3. An edit window will pop out.
4. You can edit the settings of the target.
5. Click **Next**.
6. Check the summary of the target.
7. Click **Confirm** to finish the action.

Delete a target

When a target is no longer needed, you can delete it.

To delect the target, please follow the steps below:

NOTE:
The target can only be deleted when there is no LUN mapped to it.

1. Select a target from the target list.
2. Click the function button on the top right-hand side of the target list.
3. Click **Delete**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

Edit an LUN

You can edit an LUN for the name, allocation, capacity, auto-tiering policy, and compression after an LUN is created.

To edit an LUN, please follow the steps below:

1. Select an LUN from a target or unmapped LUN list.
2. Click the function button on the top right-hand corner of the list.

3. Click **Edit**.
4. An edit window will pop out.
5. You can edit the settings of the LUN.
6. Click **Next**.
7. Check the summary of the LUN.
8. Click **Next**.
9. Click **Confirm** to finish the action.

Take a snapshot for an LUN

Ensure the data security is the most important thing on Atlas S8+. You can easily take a snapshot for your LUN.

To take a snapshot, please follow the steps below:

1. Select an LUN from a target or unmapped LUN list.
2. Click the function button on the top right-hand corner of the list.
3. Click **Take a snapshot**.
4. System will direct you the **Backup** page.
5. Click **Take Now** button to take a snapshot.
6. For more details, you can click Help button on the top right corner of the sub window.

LUN Mapping

After the LUN is created, you need to map it to a target so that it can be used for other device as a storage device.

To map or unmap an LUN, please follow the steps below:

1. Select an LUN from a target or unmapped LUN list.
2. Click the function button on the top right-hand corner of the list.
3. Click **LUN mapping**.
4. An edit window will pop out.
5. Use the drop-down menu to map the LUN.
6. Check the summary for the editing.
7. Click **Confirm** to finish the action.

Delete an LUN

When the LUN is no longer needed, you can delete it.

To delete an LUN, please follow the steps below:

1. Select an LUN from a target or unmapped LUN list.
2. Click the function button on the top right-hand corner of the list.
3. Click **Delete**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

LUN masking

LUN Masking is a level of security that makes a LUN available to only selected hosts and unavailable to all others. You can add, edit and delete the masking in the selected LUN.

NOTE:
Default policy is for all initiators and read/write permission.

To add/edit/delete masking, please follow the steps below:

1. Select an LUN from a target or unmapped LUN list.
2. In the LUN information, you can find out the masking information in the bottom of the window.

a. Add

① Click **Add** button at the top right corner of the table.
② An add window will pop out.
③ Specify the policy name
④ Enter the Initiator IQN
⑤ Specify the masking policy, Read only, Read/Write, and Deny Access.
⑥ Click **Confirm** to finish the action

b. Edit

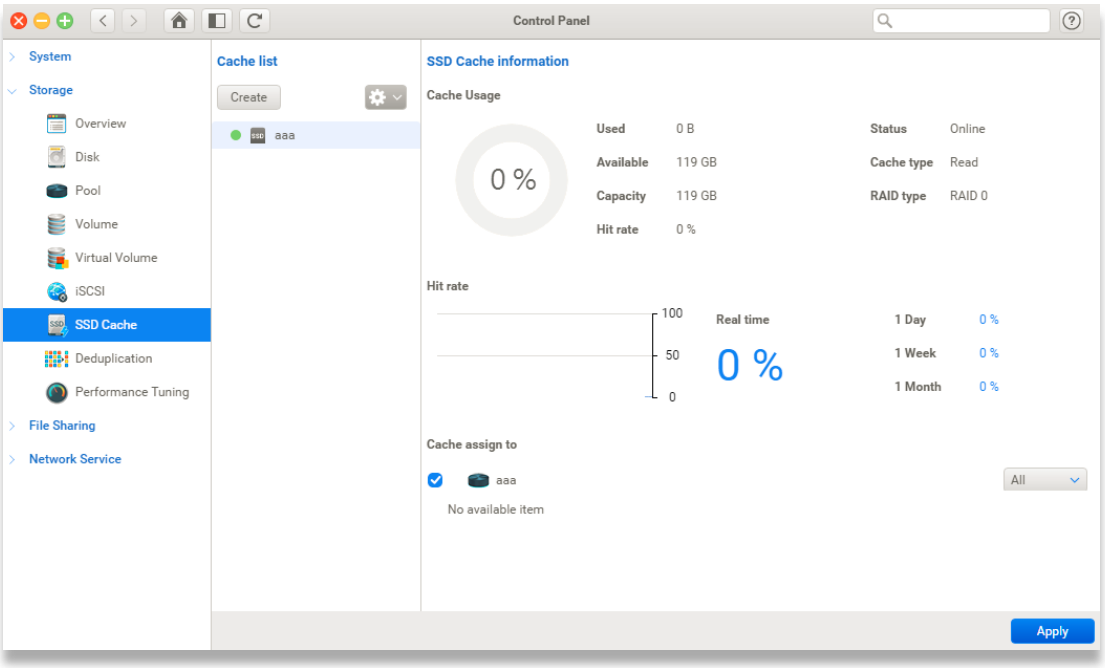
⑦ Select a masking policy on the list.
⑧ Click **Edit** button at the top right corner of the table.
⑨ Edit the masking policy, Read only, Read/Write, and Deny Access.
⑩ Click **Confirm** to finish the action.

c. Delete

⑪ Select a masking policy on the list.
⑫ Click **Delete** button at the top right corner of the table.
⑬ A confirmation window will pop out.
⑭ Click **Confirm** to finish the action.

SSD Cache

In **SSD Cache**, you can check and manage all your caches for each pool. SSD cache can improve the random read performance for a particular storage pool. Meanwhile, SSD cache can be mount on a volume or iSCSI LUN on the pool.



Create a SSD cache

To improve the performance of a particular pool, you can mount a SSD cache to the pool.

To create a SSD Cache, please follow the steps below:

1. Click **Create** button at the top of cache list.
2. Select the pool you want assign SSD cache.
3. Select the disk on Localhost or Enclosures.
4. Specify the cache type.
5. Select the disk.
6. Specify the RAID type for the Cache.

7. Click **Next**.
8. Check the summary.
9. Click **Confirm** to finish the action.

Assign SSD cache to a particular volume or LUN

After the SSD cache created, our system default settings is set to all volumes and LUNs on the pool. However, you can specify the SSD cache on each virtual storage spaces.

To set SSD cache on each virtual storage spaces, please follow the steps below:

1. Select the SSD cache from the cache list
2. On the information column, you can find **Cache assign to**.
3. Click on the volume or LUN to unmount the cache.
4. Click **Apply** to finish the action.

Edit Cache

You can add an additional SSD drive for an existing cache.

To edit the exist SSD cache, please follow the steps below:

1. Select the SSD cache from the cache list.
2. Click the function button on the top right corner of the cache list.
3. Click **Edit**.
4. An edit window will pop out.
5. Specify the disk(s) deploy.
6. Click **Confirm** to finish the action.

Delete Cache

When the cache is no longer needed, you can delete the cache

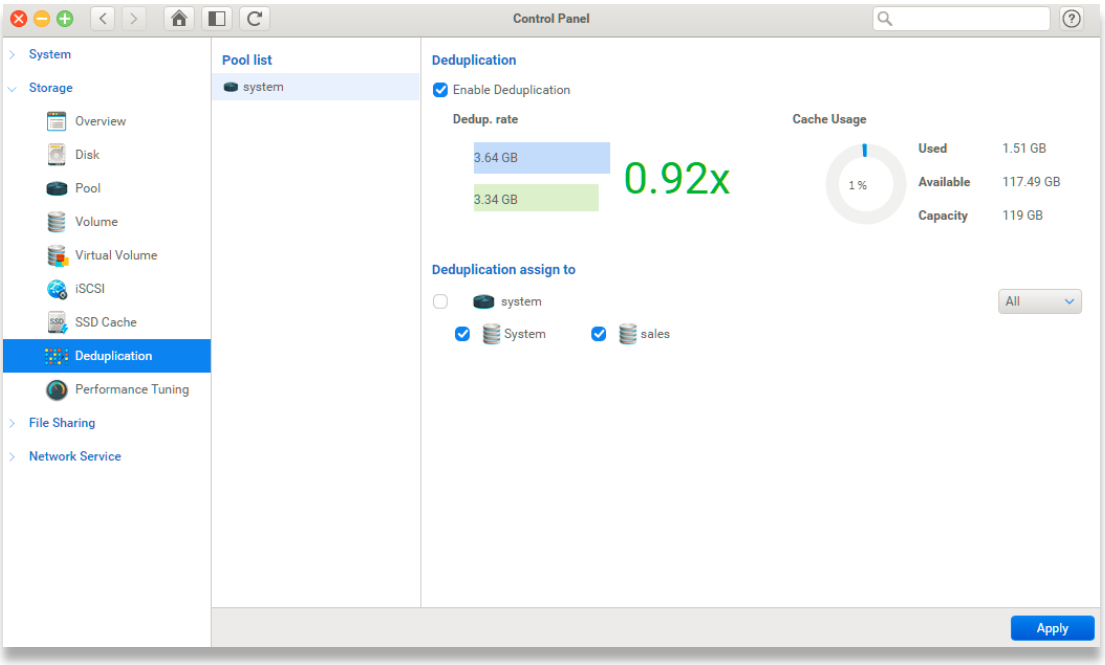
To delete an SSD cache, please follow the steps below:

1. Select the SSD cache from the cache list.
2. Click the function button on the top right corner of the cache list.
3. Click **Delete**.
4. A confirmation window will pop out.

5. Click **Confirm** to finish the setting.

Deduplication*

In **Deduplication**, you can check how this feature takes effect of you Atlas S8+. A pool with Read SSD cache, it makes your storage capacity more efficiently and lowers the capacity requirement.



Enable the deduplication

To save more data capacity on a selected pool, you can simply click one button to set it up.

To enable the deduplication, please follow the steps below:

NOTE:
Before using deduplication, you have to assign at least one SSD read cache to the pool.

1. Select a pool from the pool list.
2. Select Enable Deduplication for that pool.
3. Select the Volumes and LUNs that deduplication will be enabled on.
4. Click **Apply**.
5. Click **Confirm** to finish the action.

NOTE:
Deduplication can only take effect when the function is enabled. Files transferred to the NAS before deduplication was enabled will not be deduplicated.

Assign deduplication to a particular storage space

You can adjust the deduplication for different volumes and LUNs.

To assign deduplication for the particular storage space, please follow the steps below:

NOTE:
When you enable deduplication, all volumes and LUNs are assigned.

Select a pool from the pool list.

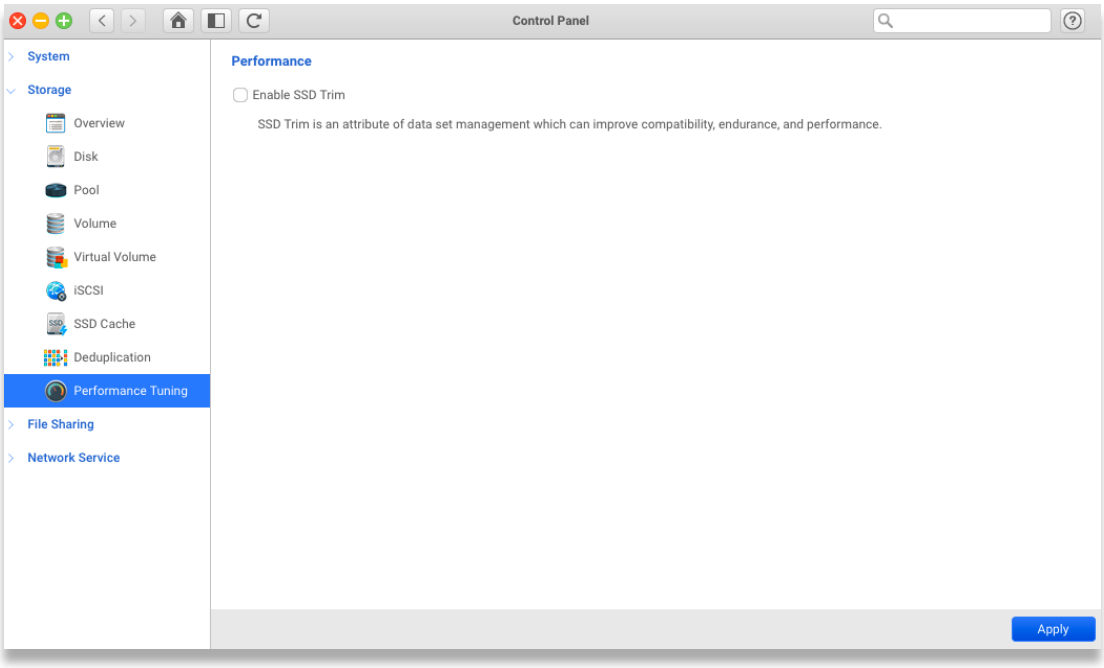
1. Untick the storage spaces you do not want to use deduplication.

NOTE:
When you have many volumes or LUNs, you can sort the type in the top right corner.

2. Click **Apply** to finish the settings.

Performance Tuning

In **performance tuning**, you can enable SSD trim to improve compatibility endurance and performance by allowing the drive to do garbage collection in the background.



Enable SSD Trim

To improved the SSDs performance and compatibility on Atlas S8+, you can enable SSD Trim.

To enable the SSD Trim, please follow the steps below:

1. Click the check box next to **Enable SSD Trim**.
2. Click **Apply** button to finish the setting.

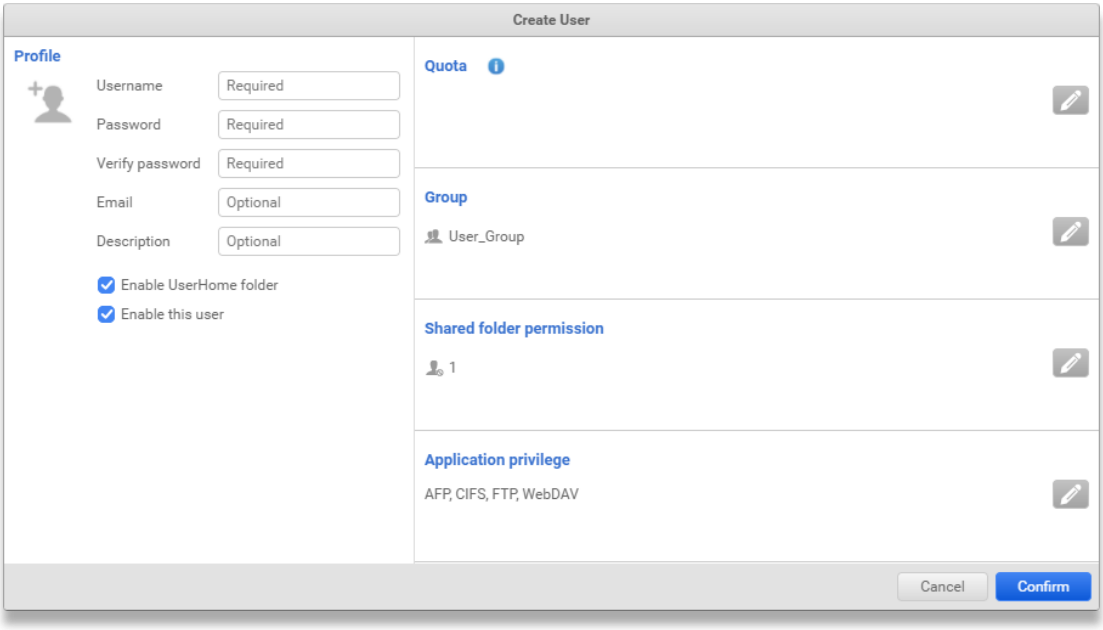
CAUTION:
While enabling the SSD Trim, all SSDs in the Atlas S8+ will be effected.

File Sharing

User

On **User** page, you can flexibly create and manage individual users when accessing Atlas S8+.

Create a User



To create a user, please follow steps below:

1. Click **Create** button and **Create User** window will pop out.
2. Fill in required information: **Username**, **Password** and **Verify password**.
3. You can also enter following optional values:
   - **Email** : User's email address.
   - **Description** : Brief description of the user.
   - **Enable this user** : With this option selected, the user can log into ASM.
   - **Enable UserHome folder** : With this option selected, the user would have a personal Home folder.
   - **Quota** : Limit the user's space usage of shared folders. The user quota is not limited to the total capacity of shared folder.
   - **Group** : Assign the user to groups. By default, the user will be a member of User_Group. A user should join at least a group.
   - **Shared folder permission** : Assign the user's permission when accessing shared folders.
   - **Application privilege** : Control the services that the user can use.
4. Click **Confirm** button. The user will be shown on the **User list** after it has been successfully created.

NOTE:

- The description is limited up to 512 characters.
- The maximum user number is 2048.

User Naming Rule:

1. Admin account is a special administrator account for managing Atlas S8+. It is created by default and cannot be deleted.

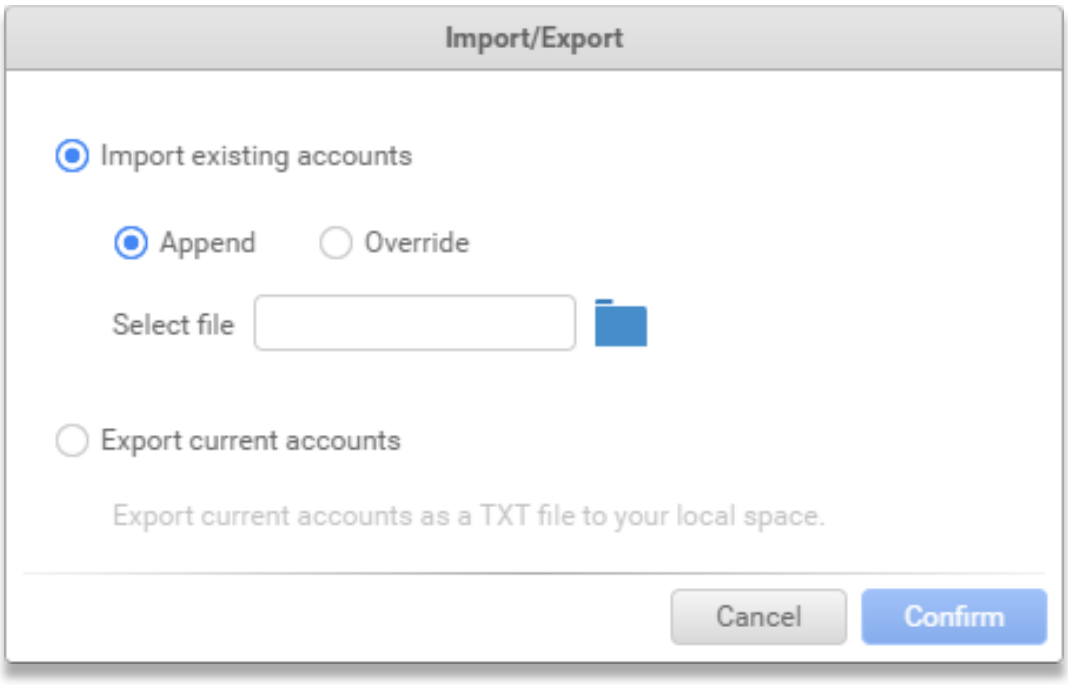
2. The username is case sensitive and should be from 1 to 128 characters, excluding the following symbols:
“ `~!@#$^&*()=+[]{}\|/;:'",<>?% ” and space.

3. The “.” cannot be placed either in the beginning nor the end.

4. The user password should be from 4 to 64 characters and be created with “a-zA-Z0-9-_”.

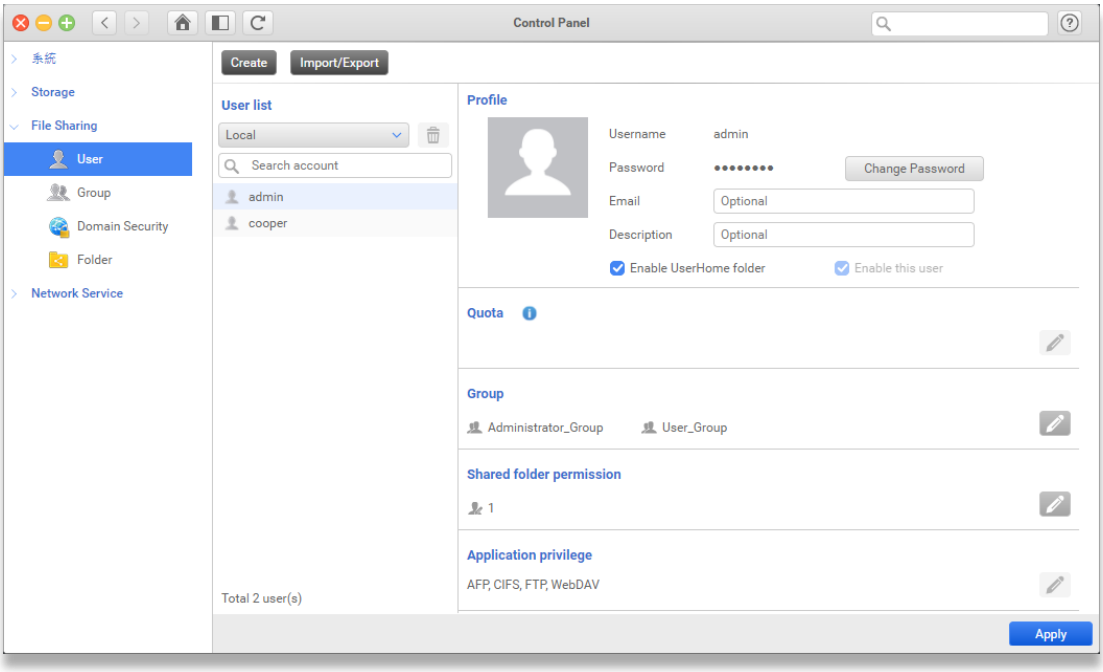
Import or Export Users and Groups

By clicking **Import/Export** button, the **Import/Export** window will pop out. Select **Export current accounts** to download all system accounts to your local device. If you want to import accounts backed up from the system previously, you can select **Import existing accounts** and choose whether to overwrite current accounts or append behind.



User Account Management

On **User** page, all system users are presented in **User list**. You can select a user and view its profile and detail settings.



You can directly edit the configuration of the user by clicking the Edit button on the right:

- In **Profile** area, the email address and the user description can be modified. You can also enable/disable the user and its Home folder. Click **Change Password** button if you want to change the user's password.
- In **Quota** area, you can restrict the user's space usage on shared folders.
- In **Group** area, the user can be assigned to different groups.
- In **Shared folder permission** area, the user's permission on shared folders can be assigned.
- In **Application privileges** area, you can decide which application service the user has right to use.

After finishing editing, click Apply button to save changes.

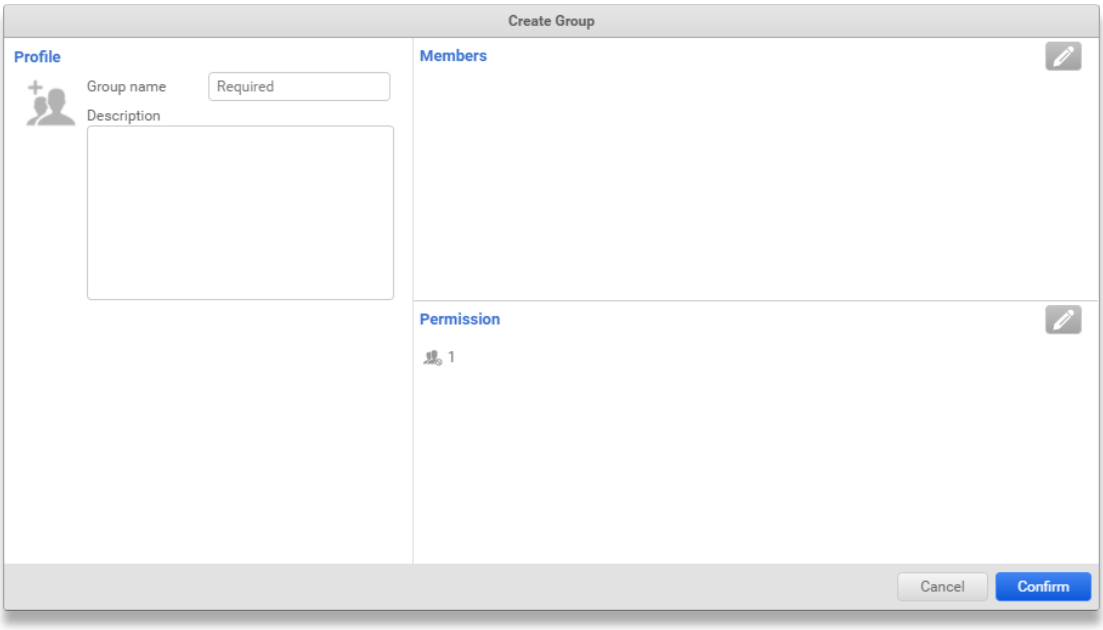
To delete a user, please follow steps below:

1. Select the user you want to delete.
2. Click **Delete** button.
3. Click **Confirm** button on the pop-up window.

Group

This page provides an overview of current system groups. You can categorize users into groups and assign group permissions on shared folders to simplify user permission control.

Create a Group



To create a group, please follow steps below:

1. Click **Create** button and **Create Group** window will pop out.
2. Fill in **Group name** and **Description**.
3. You can assign members or shared folder permission for the group.
4. Click **Confirm** button.

NOTE:

- The description is limited up to 512 characters.
- The maximum group number is 1024.
- **Administrator_Group** and **User_Group** are default groups which cannot be deleted.

Group Naming Rule:

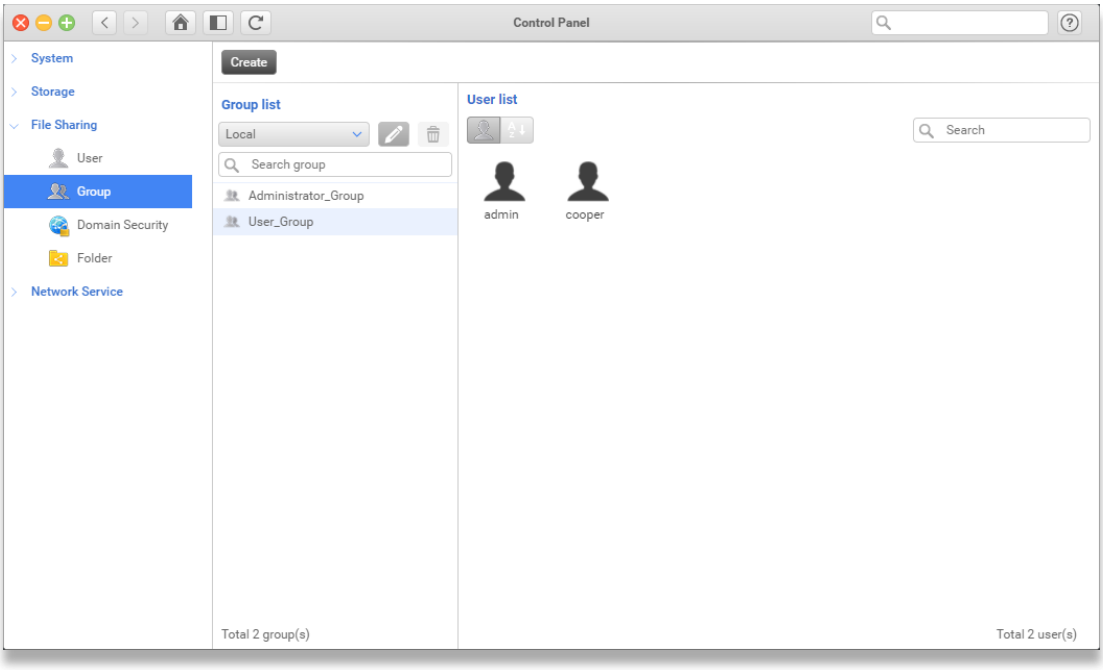
1. The group name is case sensitive and should be from 1 to 128 characters, excluding the following symbols:

“ `~!@#$^&*()=+[]{}\|/;:'",<>?% ”and space.

2. The “.” cannot be placed either in the beginning nor the end.

Group Management

The **Group** list shows all system groups. You can select a group and check its members. If you would like to manage the user further, simply click the user icon and you will be lead to its profile.



To edit a group, please follow steps below:

1. Select the group you want to edit.
2. Click **Edit** button and **Edit Group** window will pop out.
3. You can adjust group members and its shared folder permissions.
4. Click **Confirm** button to apply new settings.

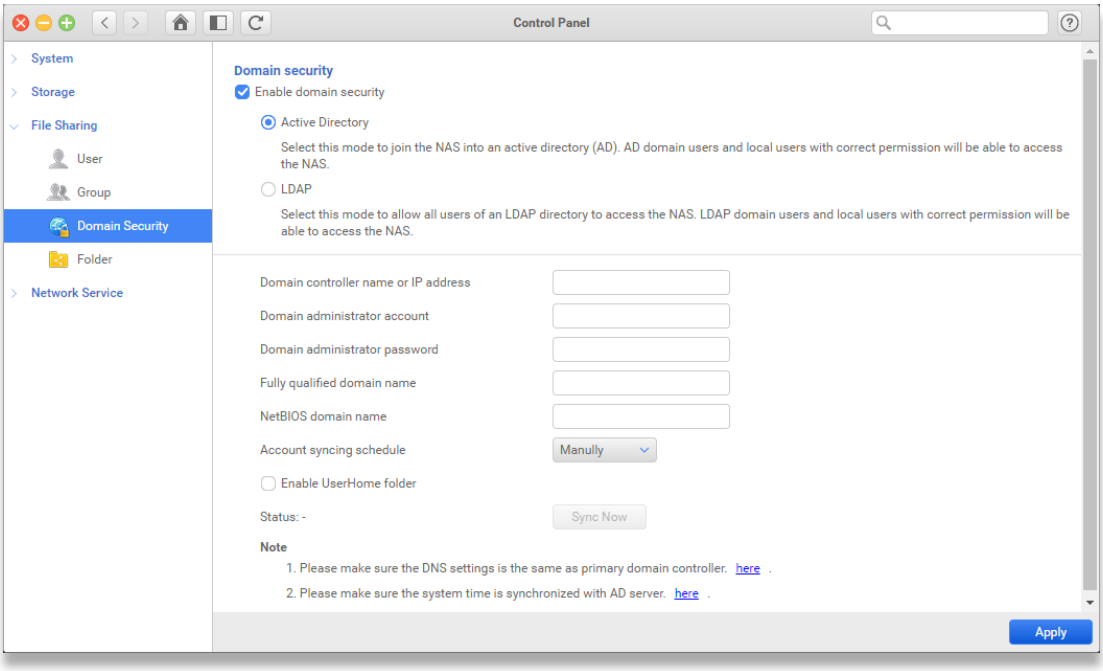
To delete a group, please follow steps below:

1. Select the group you want to delete.
2. Click **Delete** button.
3. Click **Confirm** button on the pop-up window.

Domain Security

You can join your Atlas S8+ to a domain server and allow domain accounts to log in ASM.

To join a Windows domain server



Select **Enable domain security** and click **Active Directory**, then fill in the required fields below:

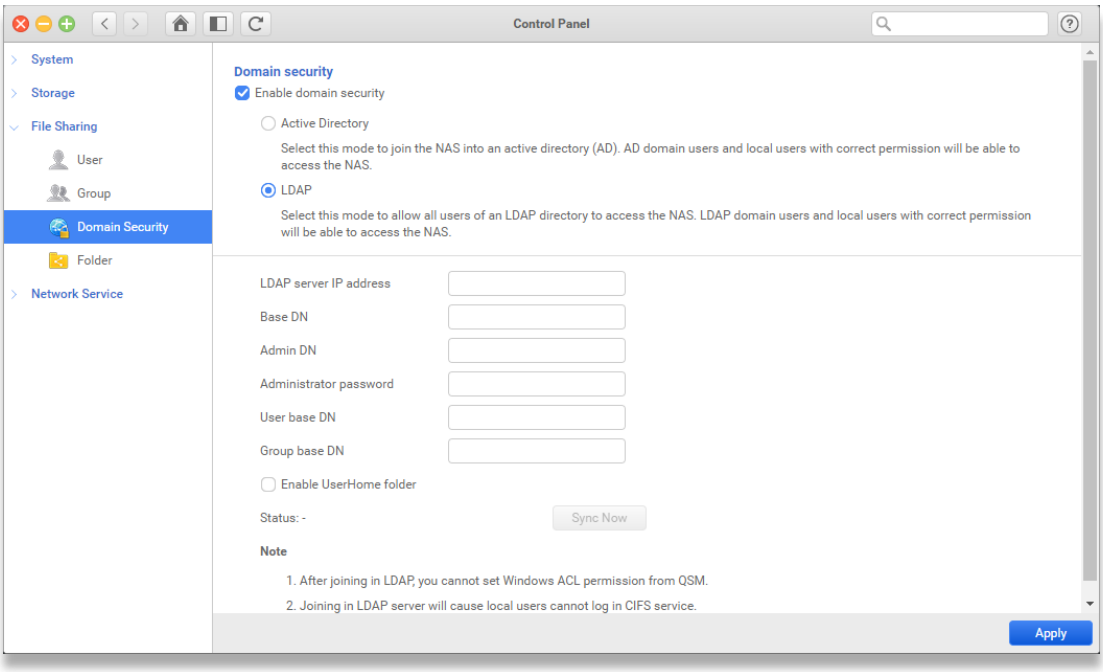
- **Domain controller name or IP address** : The name or address of the AD server.
- **Domain administrator account** : The admin account of the AD server.
- **Domain administrator password** : The admin password of the AD server.
- **Fully qualified domain name** : The DNS name of the domain.
- **NetBIOS domain name** : Microsoft domain name.

You can set **Account syncing schedule** to synchronize with AD server periodically. If you would like every AD user to have its own Home folder, select **Enable UserHome folder** .

NOTE:

- Please make sure that the DNS server can translate the AD server name.
- Please make sure that the system time is synchronized with AD server.

To join a LDAP domain server



Select Enable domain security and click LDAP , then fill in the required fields below:

- **LDAP server IP address** : The IP address of the LDAP server.
- **Base DN** : The domain of the LDAP server.
- **Admin DN** : The admin of the LDAP server.
- **Administrator password** : The password of the LDAP admin.
- **User base DN** : The organization unit (OU) in which users are stored.
- **Group base DN** : The organization unit (OU) in which groups are stored.

If you would like every LDAP user to have its own Home folder, select Enable UserHome folder .

NOTE:

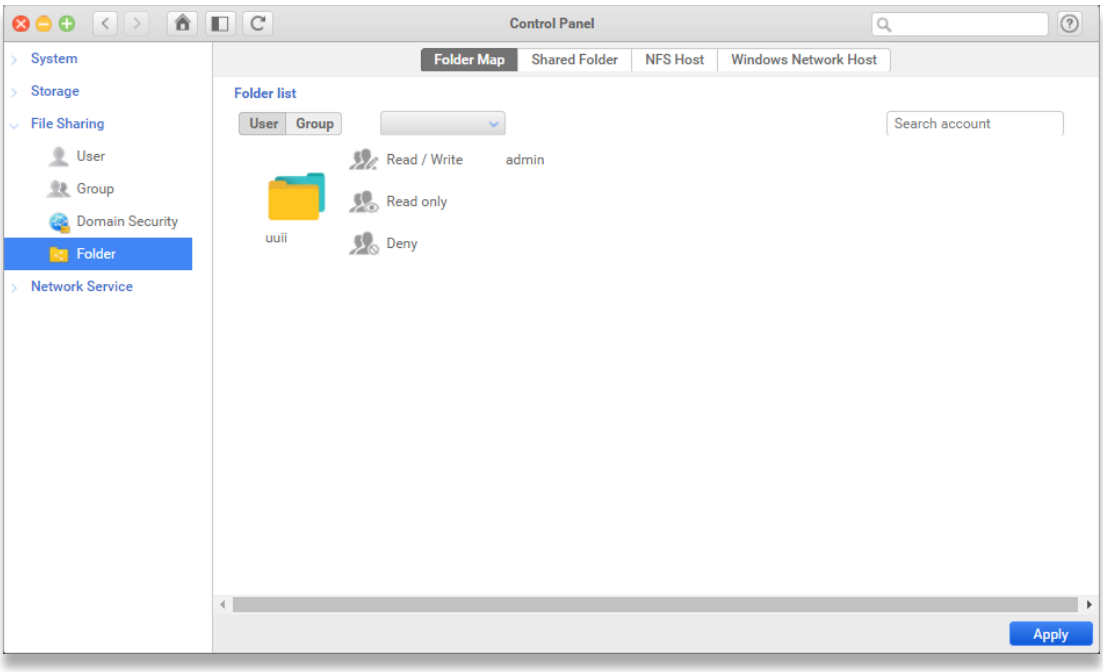
- After joining in LDAP, you cannot set Windows ACL permission from ASM.
- Local uses will not be able to use the CIFS service when joined to an LDAP domain.

Folder

You can create network shared folders for storing files or documents and share with other users. ASM brings you an intuitive interface to manage shared folders.

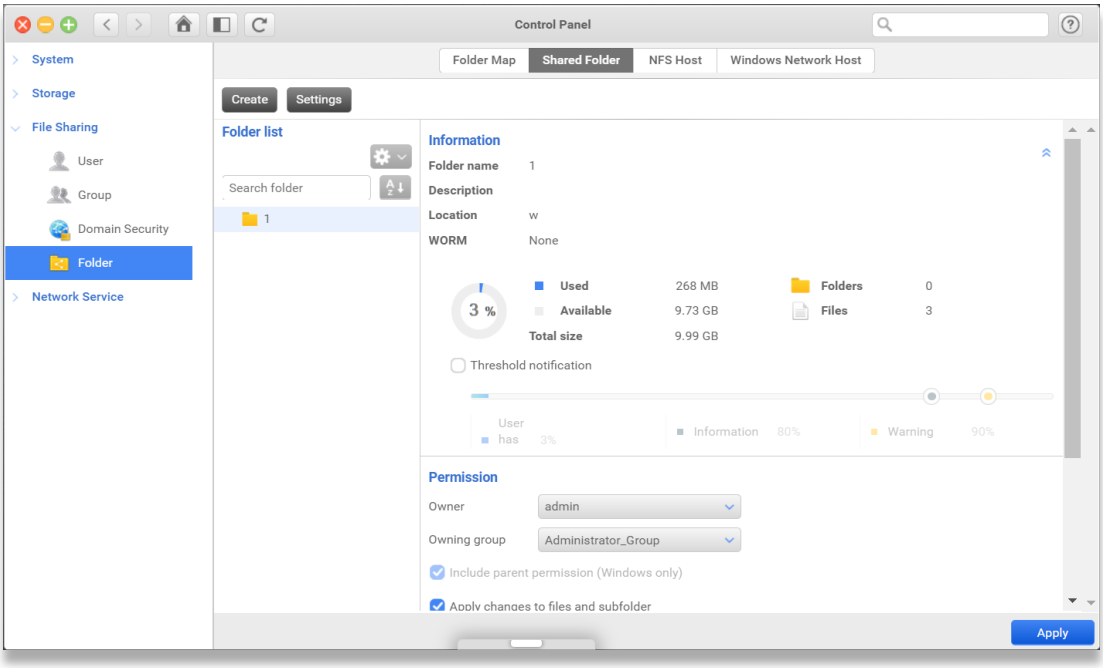
Folder Map

On **Folder Map**, you can easily view the permissions for each shared folder. By simply clicking the mode-switching buttons, you can check the user and group permissions on the Atlas S8+ or domain server. You can click the folder icon and jump to **Shared Folder** page to manage the shared folder. Clicking the account name will lead you to **User** or **Group** page to manage account settings.



Shared Folder

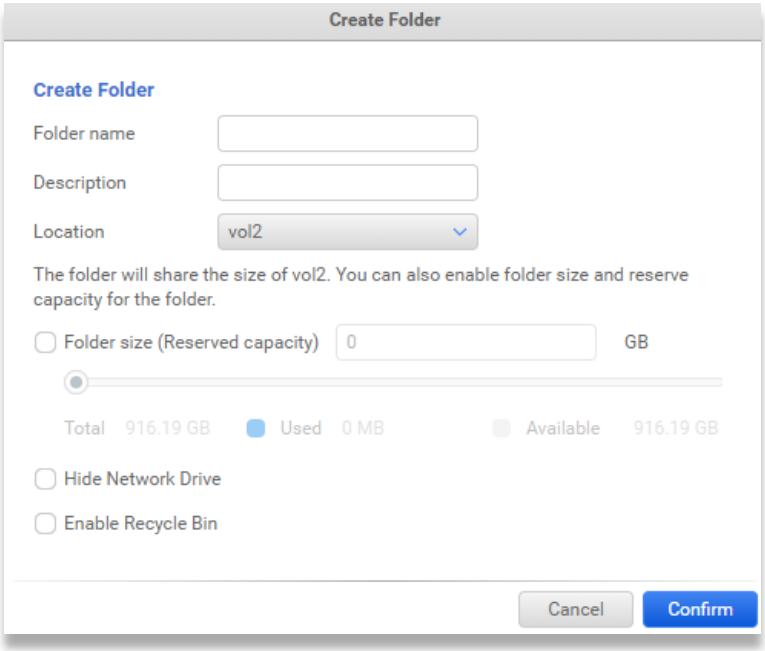
A shared folder is a root access point for storing data and sharing files via various file services. This page allows you to manage basic settings of shared folders and control access behaviors of users and groups.



Create a Shared Folder

Before creating a shared folder, please make sure that there is a local data volume or a virtual volume on the system.

NOTE:
Requirement: A local data volume or a virtual volume.



To create a shared folder, please follow steps below:

1. Click **Create** button and **Create Folder** window will pop out.
2. Fill in a name and description.
3. In **Location**, choose where to create the shared folder. It can be a local volume or a virtual volume.
4. By default, the shared folder will share the available size of the location. If the shared folder is created on a local data volume, you can reserve dedicated space for the shared folder by selecting **Folder size** checkbox and entering a capacity.
5. If you want to prevent the shared folder from being discovered under “Network” in Windows Files Explorer, select **Hide network drive** checkbox.
6. If you want to enable Recycle Bin, select the **Enable Recycle Bin** checkbox. When files in the shared folder are deleted, they will be moved to @**Recycle** folder.
7. Click **Confirm** button.

NOTE:

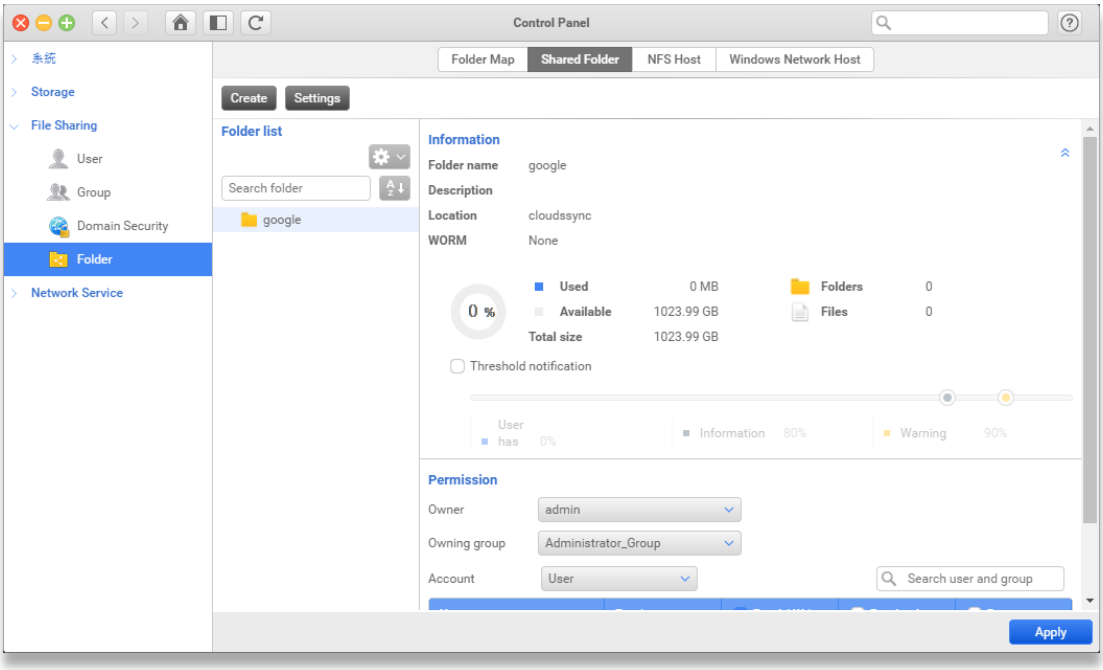
- The maximum shared folder number is 2048.
- Hiding a shared folder doesn’t affect its permission. A user who has proper access right can still access the shared folder by entering its path.

Shared Folder Naming Rule:

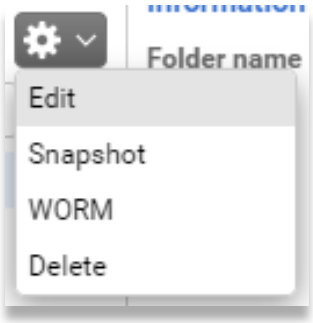
1. The maximum length of shared folder name is up to 128 characters.
2. A folder name can be alphabets, numbers but cannot contain following special characters: “ `~!@#$^&*()=+[]{}\|/;:'",<>?% ”.
3. The first character and the last character of a shared folder name cannot be “.” .
4. The character “.” cannot be used consecutively in the middle of a shared folder name.

Shared Folder Management

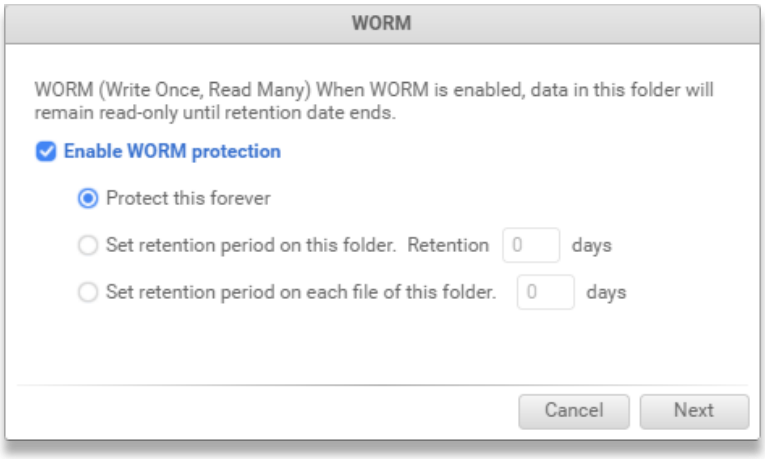
The **Information** section shows the basic settings and space utilization of the shared folder. You can check the status of the shared folder and whether WORM protection is enabled. The space usage is also presented for you to know how much space is available for storing data. You can set notification once data exceeds a specific amount by selecting **Threshold notification** checkbox.



There are 4 more actions that can be executed on a shared folder by clicking **Action** button:



1. **Edit** : Change shared folder settings except location.
2. **Snapshot** : By clicking this option, you will be lead to **Backup** app. You can then take snapshots on the selected shared folder.
3. **WORM** : By clicking this option, it will pop out **WORM** window. When WORM is set on the selected shared folder, all data under this folder would be read-only. Contents cannot be deleted, moved or modified by any user until the retention period expires.



There are 3 WORM options you can set on a shared folder:

- **Protect this forever** : guarantee a shared folder will never be modified.
- **Set retention period on this folder** : guarantee all files in this shared folder will not be modified.
- **Set retention period in each files of this folder** : guarantee files in this shared folder will not be modified for the retention period set.

4. **Delete** : Delete the shared folder.

NOTE:
If the selected shared folder has been reserved with a specific capacity, you cannot resize it smaller than original size.

Shared Folder Permission Assignment

The **Permission** section lists all permissions of the selected folder. You can designate who can access, view or modify the shared folder and its contents.

There are three types of permission can be set on an item:

Permission	Description
Read/Write	Allow the user or group to create, read, write and delete folders or files.
Read-only	Allow the user or group to access folders or files.
Deny	Prohibit the user or group from accessing folders or files.

Permissions set on a shared folder are simultaneously applied to connections via CIFS, FTP, AFP, WebDAV and NFS services.

To assign user or group permission, please follow steps below:

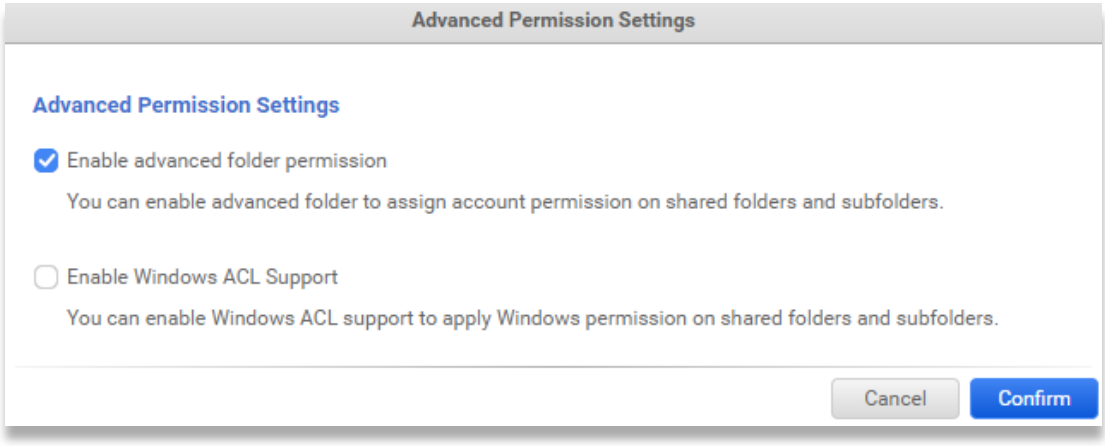
1. Change the user or account permission by selecting corresponding permission checkboxes.
2. Click **Apply** button and the new permission will take effect.

You can also change the owner or owning group of the selected folder by selecting accounts in **Owner** or **Owning group**.

Subfolders and Files Permission Assignment

By default, you can only set permissions on shared folders. To assign permissions on subfolders and files, please follow steps below:

1. Click **Settings** button and **Advanced Permission Settings** Window will pop out.
2. Select **Advanced folder permission** checkbox.
3. Click **Confirm** button.



After the option is enabled, subfolders would be listed under each shared folder.

There are two options:

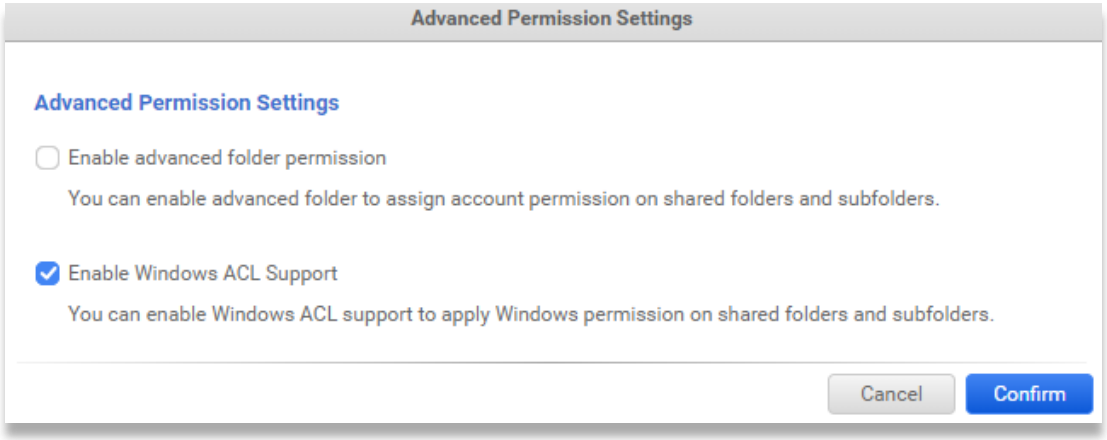
1. **Apply changes to subfolders and files** : This option is selected by default that the permissions of current folder would be applied to its subfolders and files.
2. **Replace child object permissions** : If you would like to replace the permissions of subfolders and files with current folder's permission, select this option.

NOTE:
If there are many shared folders containing multi-level folders and files, enabling / disabling advanced folder permission might take a long time.

Windows Permission Assignment

You can assign Windows permissions via ASM or Windows File Explorer to subfolders and files by steps below:

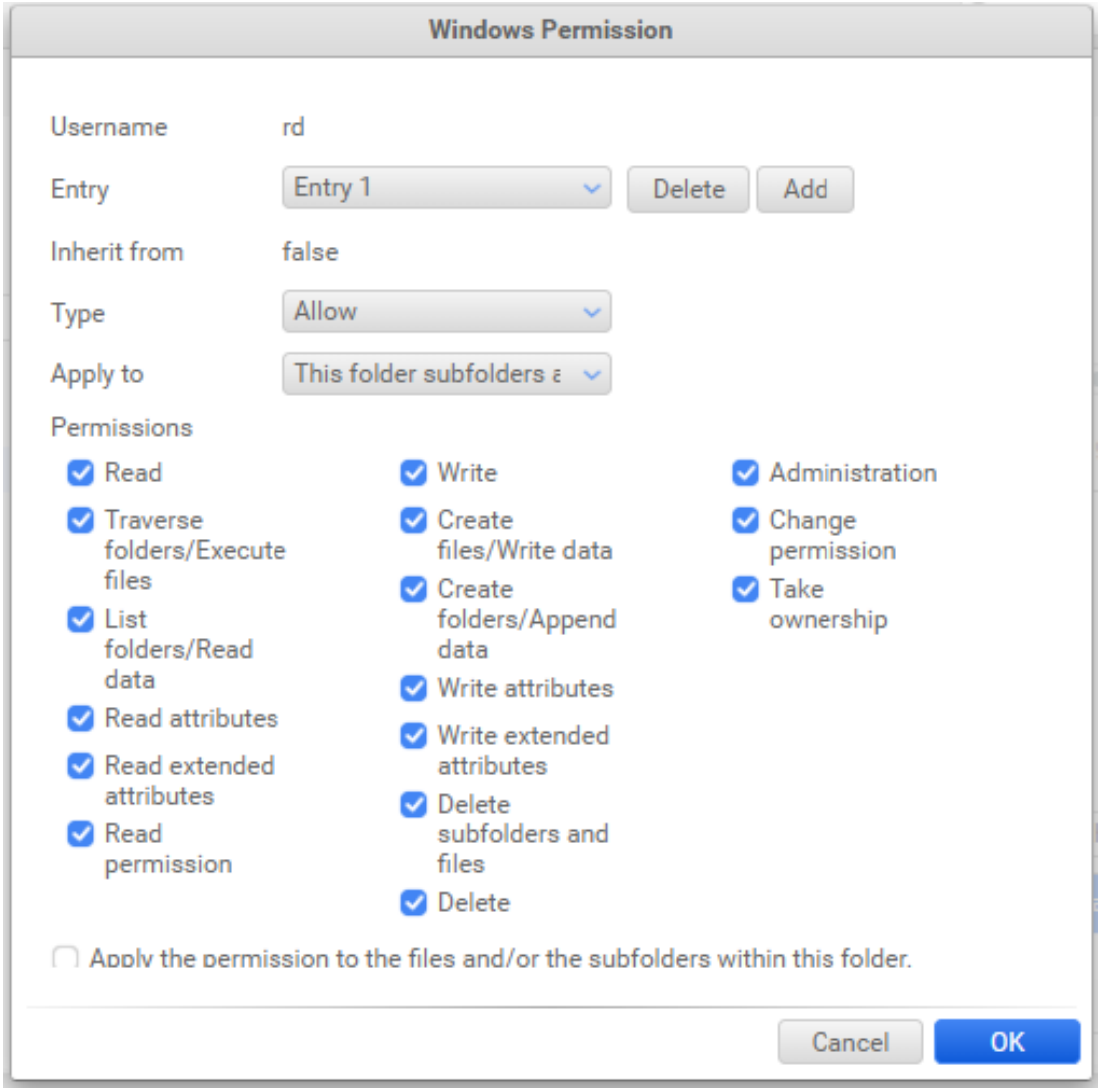
1. Click **Settings** button and **Advanced Permission Settings** Window will pop out.
2. Select **Windows ACL support** checkbox.
3. Click **Confirm** button.



After the option is enabled, the column **Windows** will appear in **Permission** section. And **Windows special** accounts will also appear in **Account**. An account which has been set with Windows permission will have its checkbox selected, otherwise unchecked.

To edit Windows ACL of the account, please follow steps below:

1. Click the account's checkbox under **Windows** column. And **Windows Permission** window will pop out.



2. In **Windows Permission** window, there are several fields:

- **Entry** : You can switch between all entries of the account. If you would like to add a new entry, click **Add** button. If you would like to delete current entry, click **Delete** button.
- **Inherit from** : Shows if the current entry is inherited from parent folders. The value would be “parent” if it is an inherited permission; otherwise, it would be “none”.
- **Type** : Shows the type of current entry.
- **Apply to** : Decide where this entry should be applied to. The default value is “This folder, subfolders and files”, meaning that the entry would be applied not only to the current folder but also its child objects.
- **Apply the permissions only on the objects and(or) the containers of this folder** : Select this option if you want the entry to be applied only one level the

subfolders of current folder.

- You can set 13 Windows permission options.

3. Click **OK** button to finish. And don't forget to click **Apply** button to take effect.

There are two options:

1. **Include parent permission (Windows only)** : Select this option if you would like to inherit parent Windows permissions.
2. **Replace child object permissions** : Select this option if you would like to replace the permissions of subfolders and files with current folder's permission.

NOTE:
If there are many shared folders containing multi-level folders and files, enabling / disabling Windows permission might take a long time.

Permission Judgment

Atlas S8+ adopts safety-first policy to guarantee shared folder security. You can view the actual access behavior of users and group in Preview column.

Permissions of a user would be judged as follows:

User permission	User's group permission	Actual behavior
Denied	Read/Write	Denied
Read-only	Denied	Denied
Not set	Read-only	Read-only
Read/Write	Read-only	Read-only

When accessing a subfolder under a shared folder, the actual behavior would be as follows:

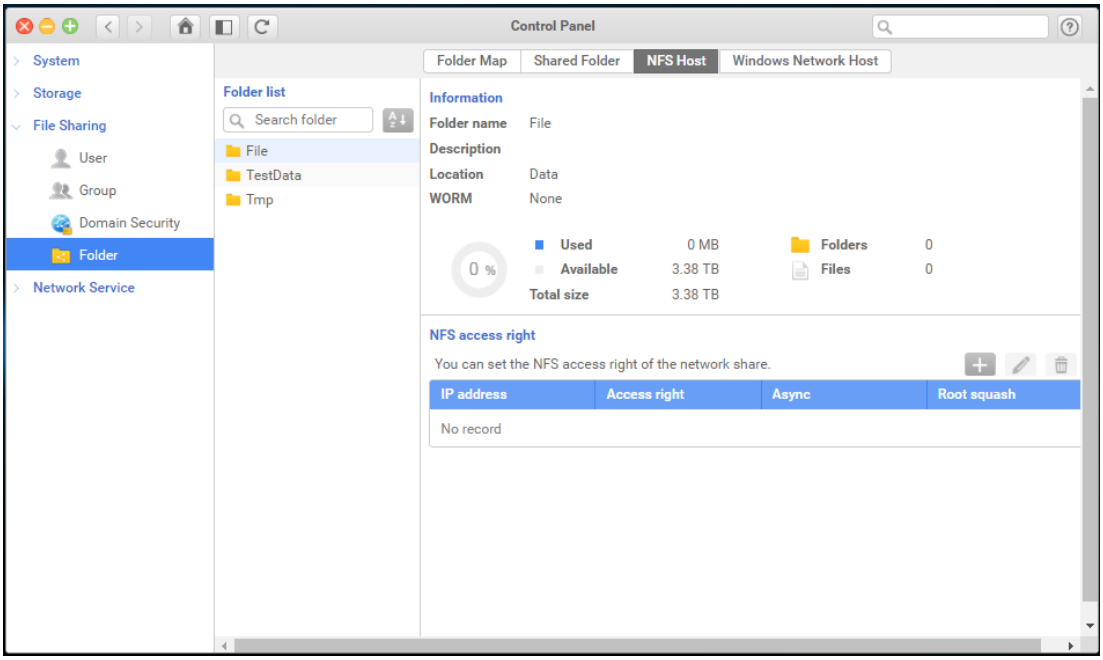
Shared folder permission	Subfolder permission	Behavior when accessing the subfolder
Read/Write	Read-only	Read-only
Read-only	Read/Write	Read-only
Not set	Read/Write	Denied
Read-only	Not set	Denied

If Windows permission support is enabled, the access behavior is as follows:

ASM permission	Windows permission	Actual behavior
Read/Write	Customized	Customized
Read-only	Full control	Read-only
Not set	Full Control	Denied
Read-only	Not set	Denied

NFS Host

You can set NFS permissions on shared folders to allow clients accessing from Linux.



Shared Folder Information

Folder list area lists all shared folders. You can select a shared folder and view its basic configuration as well as space utilization information in **Information** area.

Assign NFS Host Access Right

In **NFS access right**, you can assign access rights on the selected shared folder when clients connect from specific IP or domain using NFS service.

To add a NFS access right, please follow steps below:

1. Click **Add** button. The **NFS Host Access Right** window will pop out.
2. Enter a value in **IP address or domain**. Wildcard characters such as “*” and “?” is allowed.

3. In **Access right**, select “Read only” or “Read/Write”.
4. There are 2 more options you can choose:

- **Root squash** : Select this option to map root user on NFS client to guest account on ASM.
- **Async write** : Select this option if you don’t want to execute write command immediately.

5. Click **Confirm** button.

To edit a NFS access right, please follow steps below:

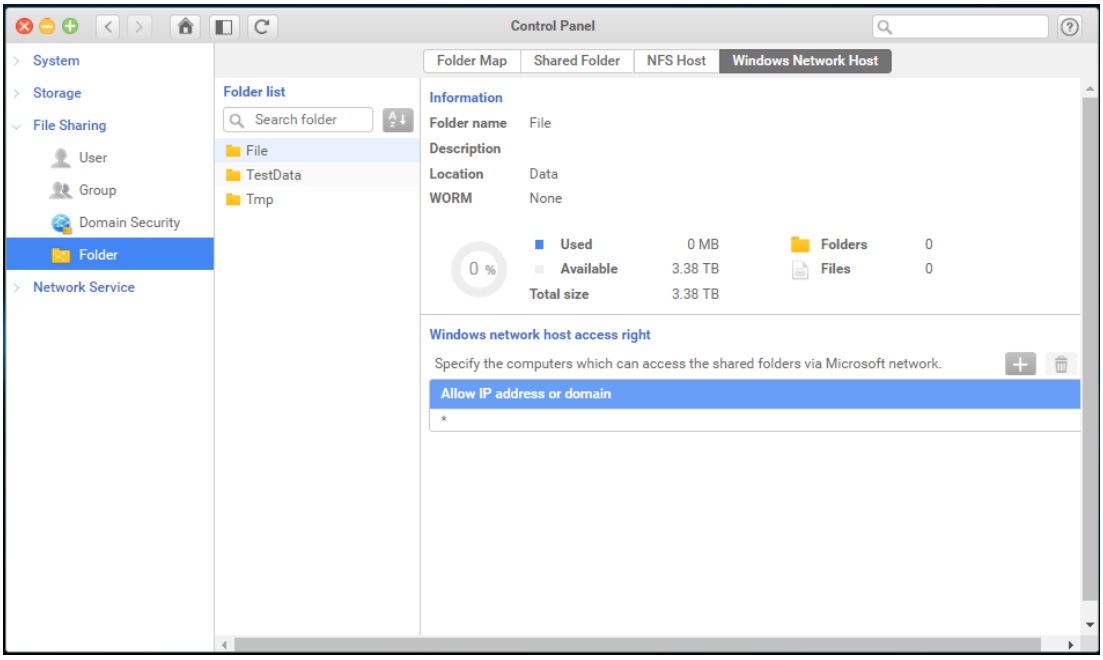
1. Select an access right and click **Edit** button. The **NFS Host Access Right** window will pop out.
2. You can change **IP address or domain**, **Access right**, **Root squash** or **Async write**.
3. Click **Confirm** button.

To delete a NFS access right, please follow steps below:

1. Select an access right and click **Delete** button. The **Delete NFS Host** window will pop out.
2. Click **Confirm** button.

Windows Network Host

You can set specific IP address, host or domain which is allowed to access the shared folders on Atlas S8+ via Microsoft Networking.



Shared Folder Information

Folder list area lists all shared folders. You can select a shared folder and view its basic configuration as well as space utilization information in **Information** area.

Assign Windows Network Host Access Right

In **Windows network access right**, you can assign access rights on the selected shared folder and the shared folder can be discovered under Windows network.

To add a Windows network host access right, please follow steps below:

1. Click **Add** button. The **Windows Network Host Access Right** window will pop out.
2. Enter a value in **IP address or domain**.
3. Click **Confirm** button.

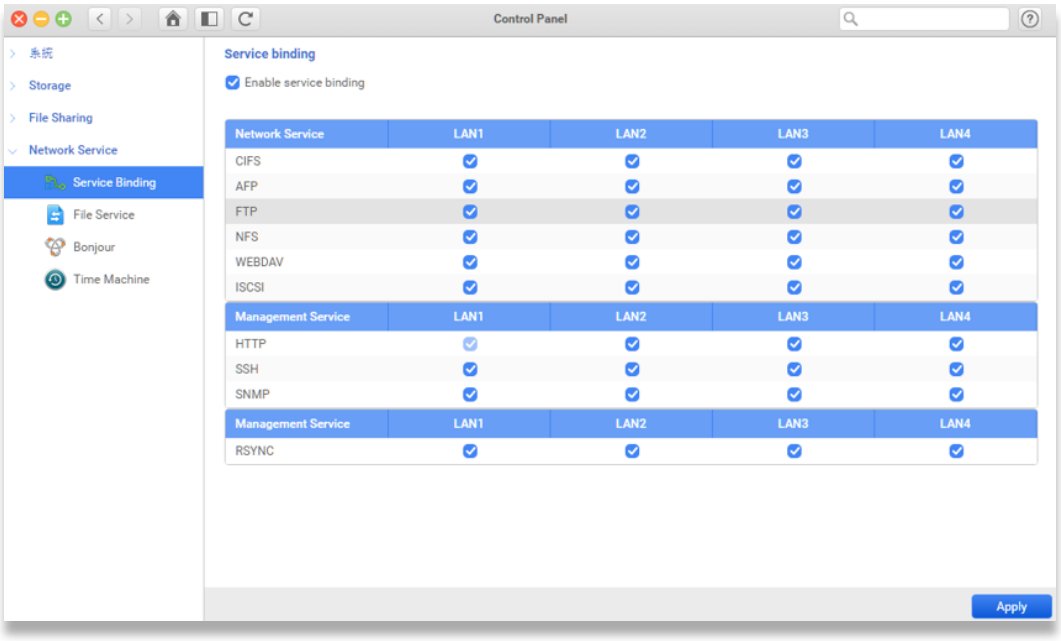
To delete a Windows network host access right, please follow steps below:

1. Select an access right and click **Delete** button. The **Delete Windows network host** window will pop out.
2. Click **Confirm** button.

Network Service

Service Binding

The Atlas S8+ **service binding** technology provides various methods of combining (aggregating) multiple network connections in parallel to increase throughput. This page shows you how to manage your data services.



Service binding

When the service binding is enabled, it links a specific or multiple available network interface on your Atlas S8+.

To enable the multiple services on the particular LAN or link, please follow the steps below:

1. Tick the **Enable service binding** checkbox.
2. Decide the particular service to a specific interface.
3. Click **Apply** button to finish the setting.

NOTE:

1. The currently connecting interface is not allowed to change on the service binding table. Location can be volumes or virtual volumes.

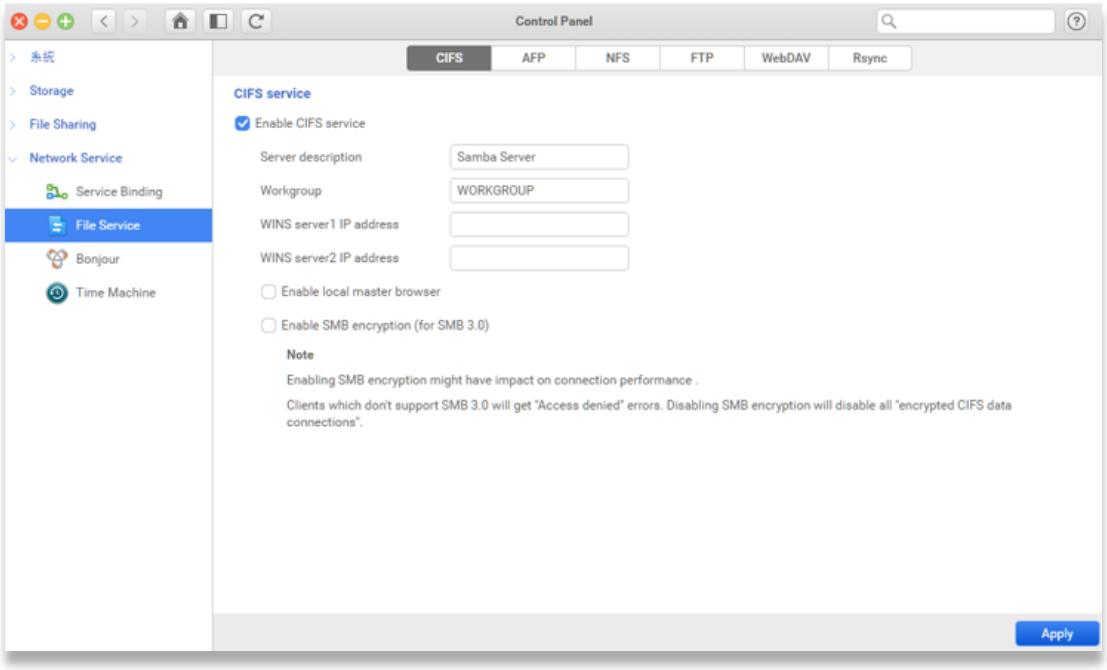
2. After clicking Apply button, all the data service will be restart. All connected users need to reconnect to the Atlas S8+ via the selected interface(s).

File Service

With the multiple services supported, you can easily share files by Atlas S8+.

CIFS

In Computer networking, the Server Message Block (SMB) is also as known as Common Internet File System (CIFS) . It is mainly used for providing shared access to files, printers, serial ports, and miscellaneous communication between nodes on a network. Most usage of CIFS involves computers running MS Windows.



To enable CIFS

To enable CIFS service, please follow the steps below:

1. Select the **Enable CIFS service** checkbox.
2. In the **Server Description** text box, provide a name for the server.
3. In the **Workgroup** text box, provide a name for the workgroup.
4. In the **WINS Server IP Addresses** text box, provide the IP address for WINS server 1 and or 2.
5. If you want to enable the **Local master browser***, please select the checkbox.
6. If you want to enable SMB encryption, please select the **Enable SMB encryption*** checkbox.

7. Click **Apply** button and finish the setting.

NOTE:

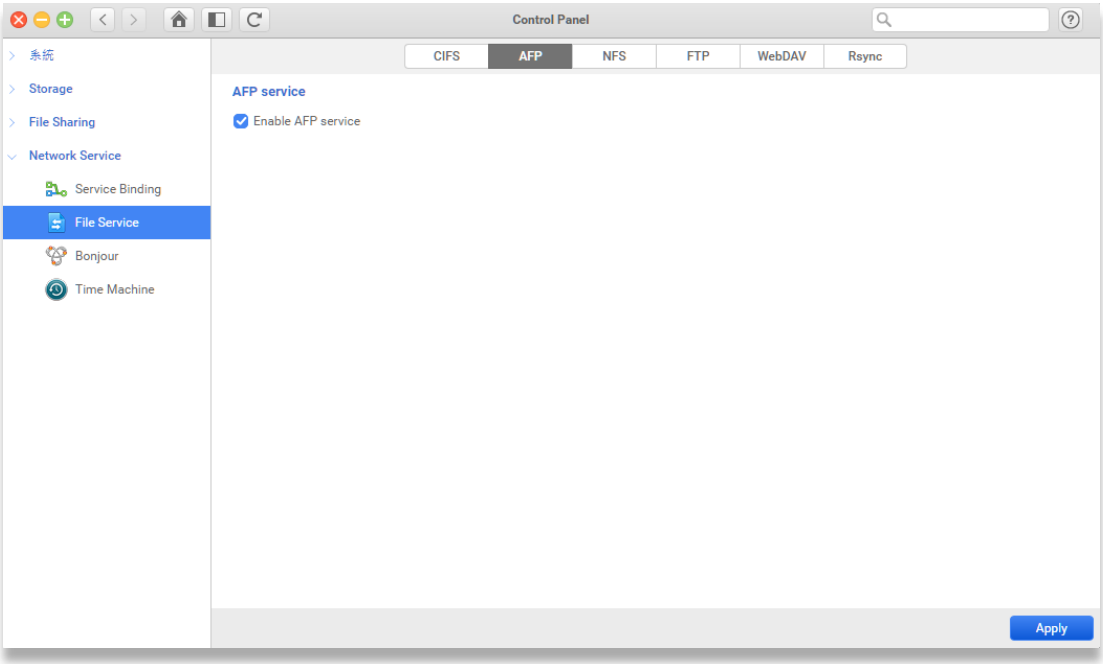
1. After enabling the CIFS service, mount the fully indexed folder to MacOS is fully supported.

2. Local master browser: When multiple Windows OS-based computers exist within the same subnet, those computers will choose one computer as the “Local master browser.” It maintains lists of others within the subnet and their shared resources and shares the lists to other computers. This option allows Atlas S8+ to be the role of the local master browser.

3. SMB encryption (for SMB 3.0): it supports AES-based file encryption transmission for improving the security of peer to peer transmission.

AFP

Apple Filing Protocol (AFP) is the proprietary network protocol that offers file service for Apple OSX and Mac OS users.



To enable AFP

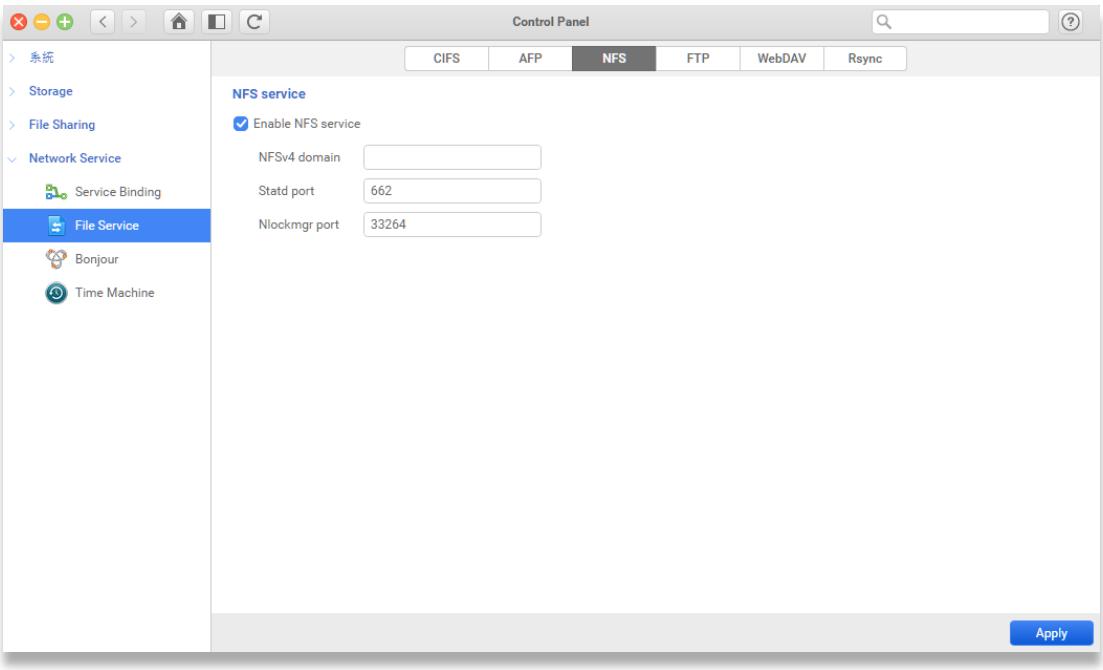
To enable AFP service, please follow the steps below:

1. Select the **Enable AFP service** checkbox.
2. Click **Apply** button and finish the setting.

NOTE:
You can set Time Machine backup service in Time Machine setting page if necessary. (Please refer to the Time Machine section for more information.)

NFS

Network File System (NFS) is the distributed file system protocol that allows Linux users to access files on the Atlas S8+.



To enable NFS

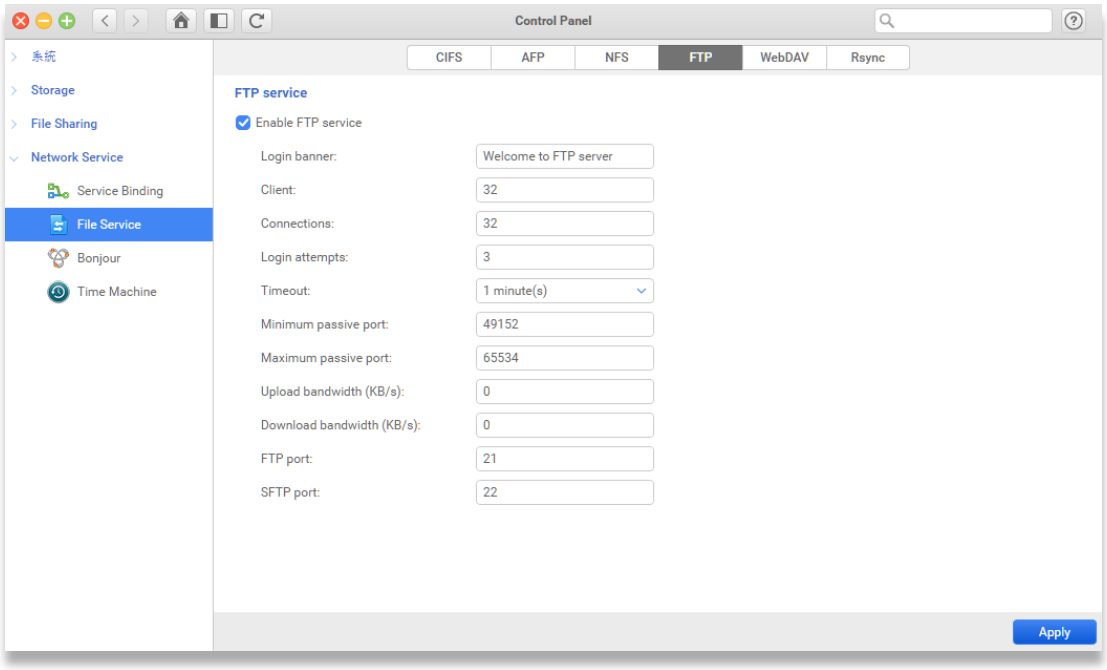
To enable NFS service, please follow the steps below:

1. Select the **Enable NFS service** checkbox.
2. In the **NFSv4 domain** text box, enter the NFSv4 domain.
3. In the **Statd port** text box, enter the Statd port number.
4. In the **Nlockmgr port** text box, enter the Nlockmgr port number.
5. Click **Apply** button and finish the setting.

NOTE:
The default port for Statd and Nlockmgr port are 662 and 33264.

FTP

The File Transfer Protocol (FTP) is the standard network protocol used to transfer files. It does not provide any encryption to protect information during transfer sessions, such as passwords, usernames, or files. The transfer speeds are faster and require fewer system resources.



To enable FTP

To enable FTP service, please follow the steps below:

1. Select **Enable FTP service** checkbox.
2. In the **Login Banner** text box, enter the banner when you log in FTP server (Optional).
3. In the **Client** text box, enter the port number that FTP used to communicate with other devices.
4. In the **Connections** text box, enter the number of concurrent connections that will be allowed for this FTP service.
5. In the **Login attempts** text box, enter the number that a user is authorized to log in before being locked out.
6. In the **Timeout** text box, enter the period of time an FTP connection can be idle before being automatically timed out.
7. In the **Minimum passive port** text box, enter the minimum port number that FTP used to communicate with other devices.

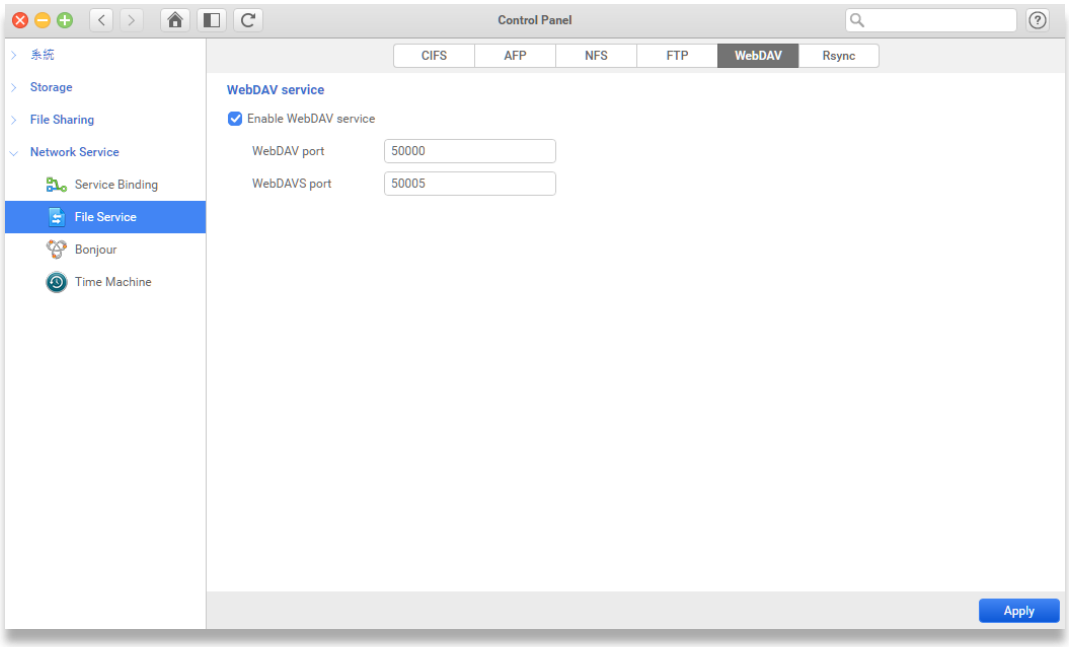
8. In the **Maximum passive port** text box, enter the maximum port number that FTP used to communicate with other devices.
9. In the **Upload Bandwidth** text box, enter the maximum bandwidth when uploading data. 0 (zero) means that the bandwidth is not limited.
10. In the **Download Bandwidth** text box, enter the maximum bandwidth when downloading data. 0 (zero) means that the bandwidth is not limited.
11. In the **FTP port** text box, enter the port number that the FTP service used to communicate with other devices.
12. In the **SFTP port** text box, enter the port number that SFTP used to communicate with other devices.
13. Click **Apply** button and finish the setting.

NOTE:
1. The default port for Minimum and Maximum passive ports are 49152 and 65534.

2. The default port for FTP and SFTP are 21 and 22.

WebDAV

Web Distributed Authoring and Versioning (WebDAV) allows users to perform remote Web content editing and authoring operations. The WebDAV protocol lets users create, change and move documents stored on remote server.



To enable WebDAV

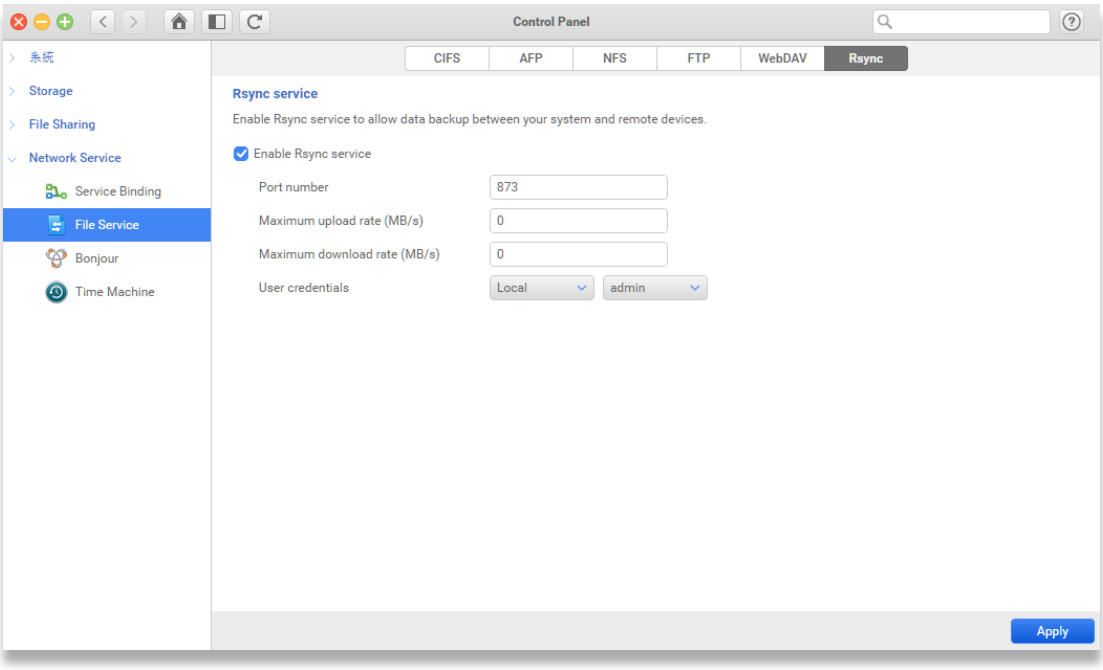
To enable WebDAV service, please follow the steps below:

1. By clicking **Enable WebDAV service** checkbox to enable the service.
2. In the **WebDAV port** text box, enter the WebDAV port number that WebDAV used to communicate with other devices.
3. In the **WebDAVS port** text box, enter the WebDAVS port number that WebDAVS used to communicate with other devices.
4. Click **Apply** button and finish the setting.

NOTE:
The default port for WebDAV ad WebDAVS are 50000 and 50005.

Rsync

Rsync service allows you to backup or restores data between the remote site and your local Atlas S8+ in real time. For more information about the backup configurations, please see the help page on **Backup** > **Remote Backup**.



To enable Rsync

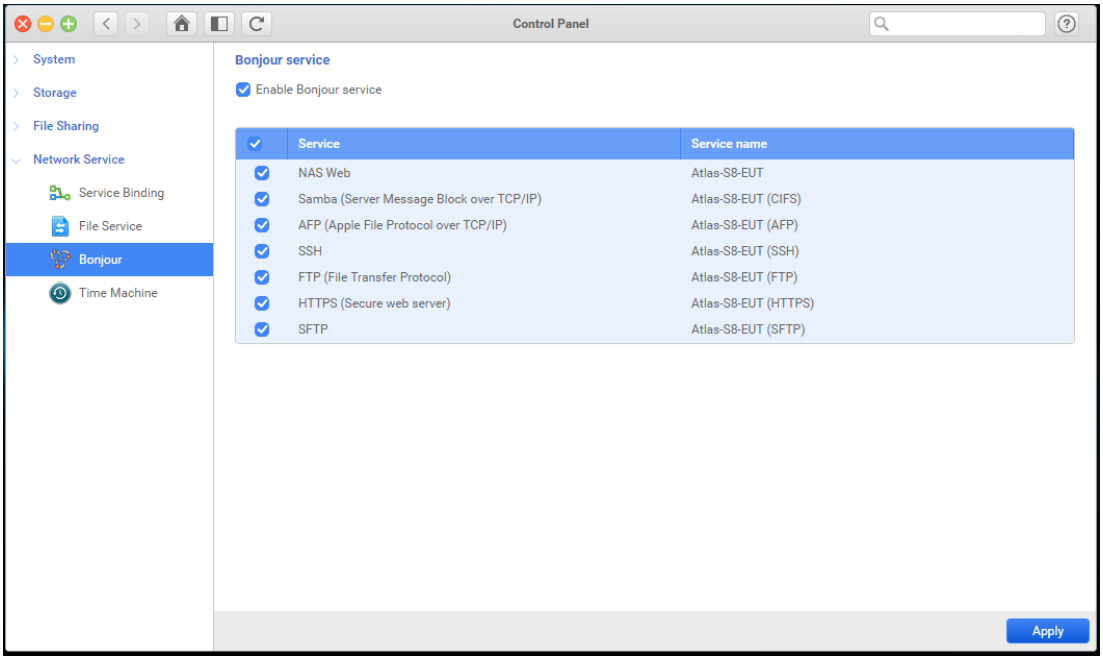
To enable Rsync service, please follow the steps below:

1. Click **Enable rsync service** checkbox.

2. In the **Port number** text box, enter the port number that rsync will use to communicate with other devices.
3. In the **Maximum upload rate** text box, enter the maximum upload rate when uploading data. a 0 (zero) means that the bandwidth is not limited.
4. In the **Maximum download rate** text box, enter the maximum download rate when downloading data. a 0 (zero) means that the bandwidth is not limited.
5. Click **Apply** button and finish the setting.

Bonjour

The Atlas S8+ provides the Apple Bonjour discovery service. In this page, you can set up discoverability for Bonjour.



Bonjour service

Enable this service allows **Bonjour** service to find your Atlas S8+ via different protocols.

To enable the Bonjour service, please follow the steps below:

1. Click **Enable Bonjour service** checkbox.
2. In the table shown below the check box, all supported data service will list on the table. Select the service that you want to use.
3. Click the **Apply** button and finish the setting.

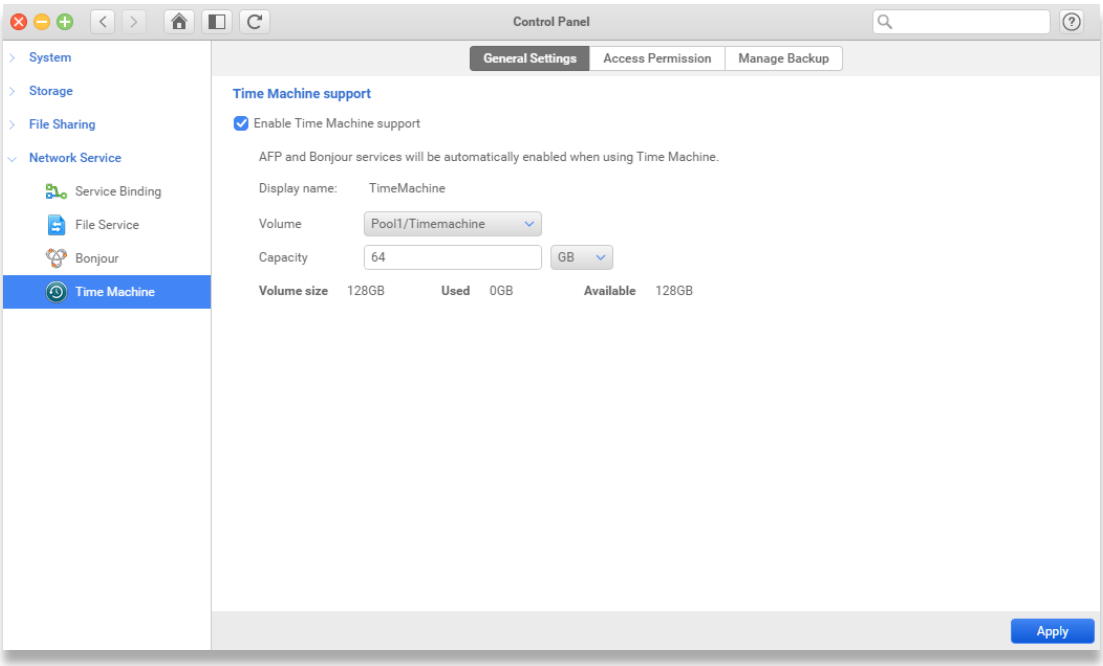
NOTE:
The service name is based on your device name.

Time Machine

Time Machine is a backup software application distributed by Apple INC, and it is particularly for the MAC OS users to backup their MAC machines.

General Settings

You can choose the location for your Time machine back files and set the maximum capacity on your Atlas S8+.



Time machine support

Atlas S8+ can help MAC users to backup their data by the application attributed by Apple.

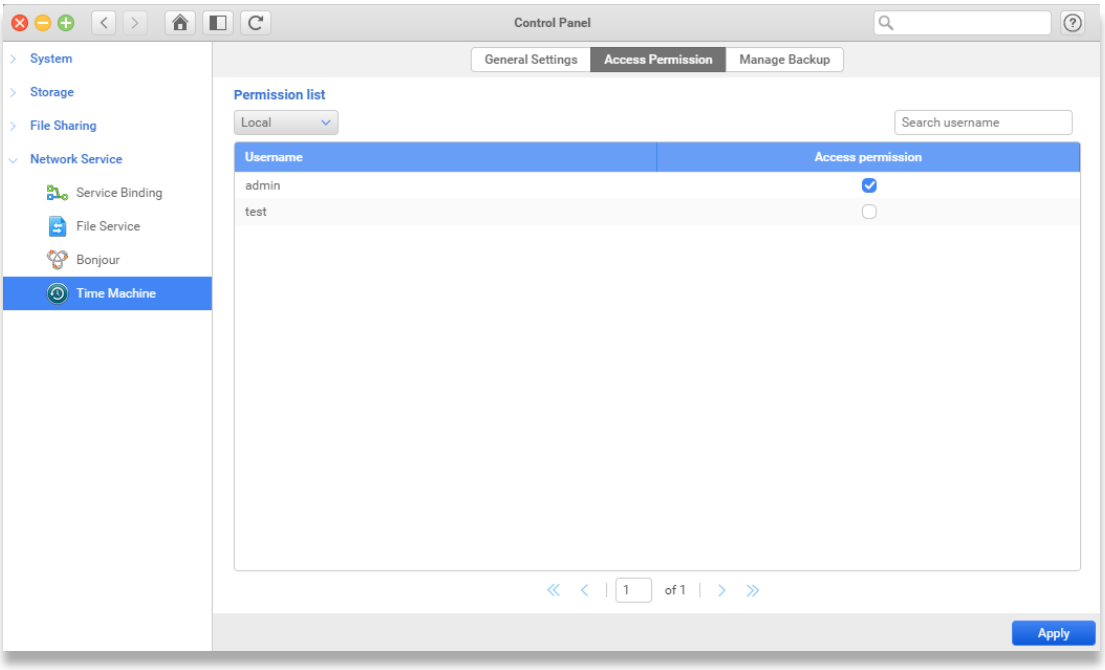
To enable Time Machine, please follow the steps below:

1. Select **Enable Time Machine support** checkbox.
2. Choose a **Volume** on your Atlas S8+.
3. Enter the **Capacity** to reserve the capacity for Time machine.
4. Click **Apply** button and finish the setting.

NOTE:
AFP and Bonjour service will be automatically enabled when Time Machine is enabled.

Access Permission

Atlas S8+ supports the multiple users to backup their Apple computers via Time Machine. You can setup the user's privilege for local or domain users.



Set up user privilege

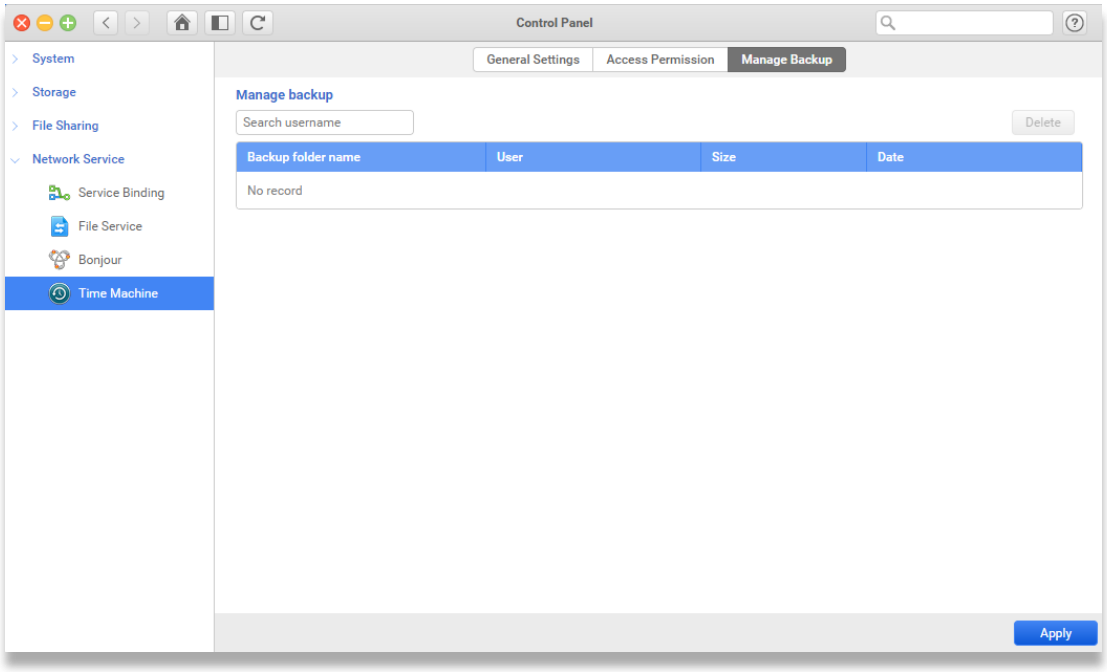
You can setup the user privilege of using Time Machine.

To set the Access Permissions, please follow the steps below:

1. Select your user list from either Local or Domain.
2. Choose the checkbox to decide each user's permission on using Time Machine service.
3. Click **Apply** button and finish the setting.

Manage Backup

In the page, you can check the list of all Time Machine backups. You can also delete a particular backup when you need more capacity.



Search for a particular user

To search a user, enter the keyword in the search column, the matching user(s) will be listed in the table.

To delete a backup

To delete your Time Machine backups, please follow the steps below:

1. Select the backup folder name you want to remove.
2. Click the **Delete** button.
3. Choose the **Confirm** button to remove the backup.

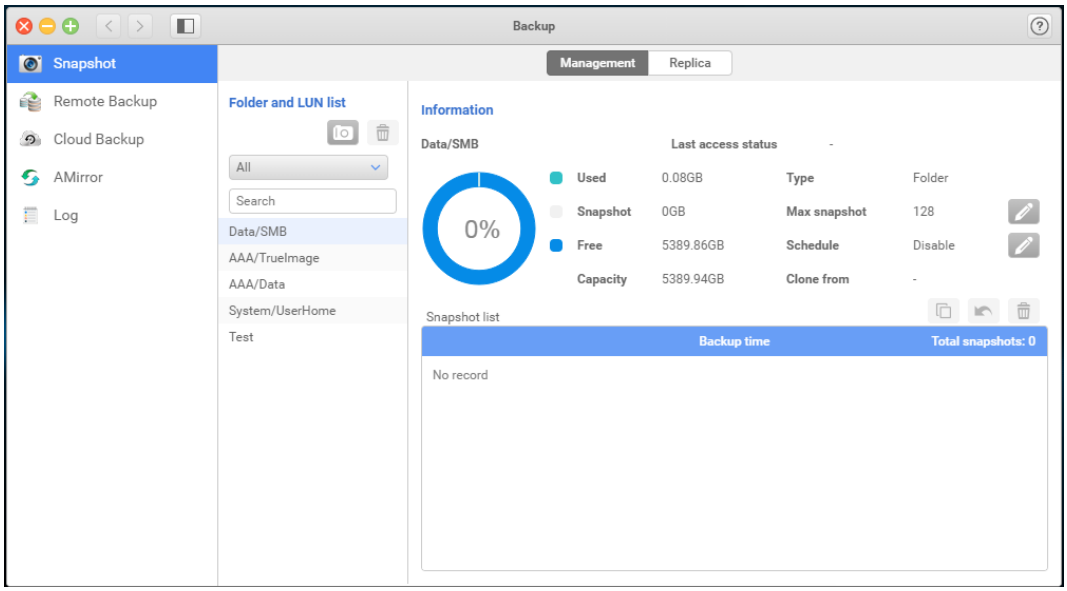
Backup

Snapshot

In **Snapshot**, you can backup and recover your data from a shared folder or LUN to prevent the data crash, corruption, and viruses. Snapshots can be stored on the local host or remote destinations.

Management

In **Management**, you can take a snapshot for the selected shared folders or LUNs, check the current backup and storage capacity usage, set up the maximum snapshot limit and schedule, clone the snapshot and convert to be a shared folder, and roll back to the specific time. Meanwhile, you can check the basic information of a selected folder or LUN.



Take Snapshots

Snapshots can help you capture the current status of your local shared folder and LUN.

To take a snapshot, please follow the steps below:

1. Select or Search a shared folder or LUN from **Folder and LUN list**.
2. Click the **Take Now** button on the top of the list.
3. Click the **CONFIRM** button to take the snapshot.
4. The name of the snapshot will be shown as the pleasant time in the **Backup time** table.

Manage Snapshots

You can set up the maximum snapshots for the folder or LUN, the schedule of taking snapshots, clone a snapshot from a shared folder or LUN, roll back to the data, and delete a snapshot.

To set the **Maximum snapshots**, please follow the steps below:

1. Click the edit button next to **Max snapshot**.
2. Select the snapshot rotation policy.
3. Enter the maximum snapshot amounts for the folder or LUN.
4. Click **Confirm** button to finish setting.

NOTE:

1. Maximum snapshots for the entire system is 4096.
2. Default snapshot amount for a shared folder or LUN is 128.
3. Default snapshot rotation policy is set to Stop when reaching the maximum amount.

To set the **Schedule** of taking snapshots, please follow the steps below:

1. Click the edit button next to **Schedule**.
2. You can set the snapshot schedule as **Manually only**, **Daily**, **Weekly**, **Monthly**, or **Repeat** in a period of the time.
3. You can also set the start time for the task.
4. Click **Confirm** button to finish settings.

NOTE:

The start time is based on the system time.

To **Clone** a snapshot from a shared folder or LUN, please follow the steps below:

1. Select the folder or LUN on the **Folder and LUN list**.
2. Select the Snapshot on the **Snapshot list** table.
3. Click the **Clone** icon in the first position on the top right side of snapshot list table.
4. Enter the new folder or the LUN name for the cloned folder or LUN.
5. Click **Confirm** button to finish the action.

NOTE:
1. If you clone this snapshot of folder/ LUN, it will be created a new "Clone Folder/ Clone LUN" and shown on the "Folder and LUN list.

2. If you clone the snapshot of folder, the Windows ACL permissions of each file that from parent share folder will be copied to the snapshot of the folder. However, the share permission of this snapshot of the folder is admin-use-only.

To **Roll back** data, please follow the steps below:

1. Select the folder or LUN on the **Folder and LUN list**.
2. Select the Snapshot on the **Snapshot list** table.
3. Click the **Roll back** icon in the second position on the top right side of snapshot list table.
4. Click **Confirm** button to finish the action.

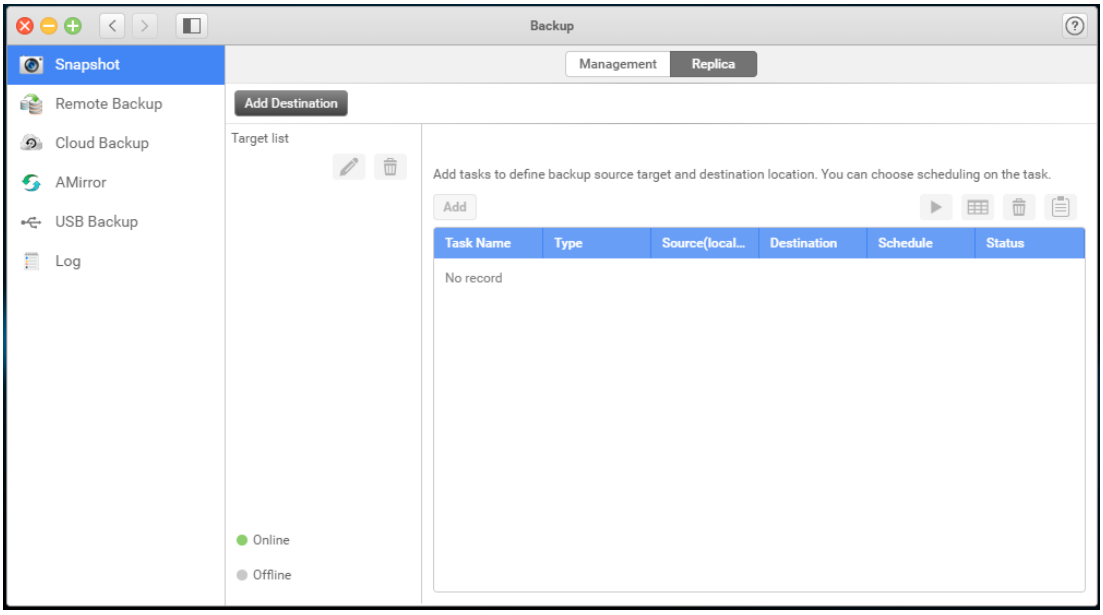
NOTE:
All data will back the date you select to roll back including snapshots.

To Delete a snapshot, please follow the steps below:

1. Select the folder or LUN on the **Folder and LUN list**.
2. Select the Snapshot on the **Snapshot list** table.
3. Click the **Delete** icon in the last position on the top right side of snapshot list table.
4. Click **Confirm** button to finish the action.

Replica

By replicating local snapshots to a remote site, it prevents data loss from hardware damage, accidental deletion, data corruption, and viruses. It also helps you to manage and monitor snapshots between different NAS via LAN or Thunderbolt3 (Optional) interface.



How to add a destination

Before replicating snapshots to the remote site, you will need to add at least one destination to store your snapshots. The destination must be a different Atlas S8+. After adding a destination target you will be able to create, edit, delete and schedule replication tasks.

To **Add destination**, please follow the steps below:

1. Click **Add destination** button on the top left corner of the window.
2. Enter the IP address / Host name of your remote destination.

NOTE:
By clicking the drop-down menu, you can find all Atlas S8+ on the same network.

3. Enter a name for your Target.

NOTE: Target name naming rule.

1. Length: 1-128 characters
2. Invalid 【 `~!@#$^&*()=+[]{}\|/;:'",<>?% 】and space.
3. It's not case sensitive.
4. "." can't be placed neither in the beginning nor the end.

4. Enter the **Username** and **Password**, which can access remote destination.
5. Click the **Test** button to test the connection ability between local host and remote destination.

6. Click **Confirm** button to finish the action.

How to edit or delete the destination

You can edit the destination for its dedicated LAN, IP address / Host name, Target name, user name, password and delete the target.

To edit the destination, please follow the steps below:

1. Select a destination on the **Target list**.
2. Click **Edit** button on the top of the list.
3. The edit window will pop out and select the item you want to edit.

CAUTION:

Changing the destination IP / Hostname may cause the backup task fail.

4. Click Confirm to finish the action.

To delete the destination, please follow the steps below:

1. Select a destination on the **Target list**.
2. Click **Delete** button on the top of the list.
3. The confirm window will pop out.
4. Click **Confirm** to finish the action.

How to create a task for a destination.

To **Add** a replica task, please follow the steps below:

1. Select a target on the target list.
2. Click **Add** button to add a task.
3. Select the **Folder**, **LUN** or **SRM** to be the backup target.
4. Enter a name for your **Task**.

NOTE: Task name naming rule.

1. Length: 1-128 characters
2. Invalid 【 `~!@#$^&*()=+[]{}\|/;:'",<>?% 】and space.
3. It’s not case sensitive.
4. "." can’t be placed neither in the beginning nor the end.

5. Enter a name for your replica Folder, LUN or SRM in the remote destination.

NOTE: Task name naming rule.

Replica Folder naming rule

1. Length: 1-128 characters.
2. Invalid 【 `~!@#$^&*()=+[]{}\|/;:'",<>?% 】
3. “.” Can’t be used consecutively in the middle of a folder name.
4. “.” can’t be placed neither in the beginning nor the end.

Replica LUN and SRM naming rule

1. Length: 1-32 characters.
2. “.” can’t be placed neither in the beginning nor the end.
3. Valid characters: 【a-zA-Z0-9-_.】

6. Select the source on local host by clicking the button on the right-hand side of the window.
7. Select a volume to create a new on the remote destination by clicking the button on the right hand side of the window.
8. Set a schedule for the task or back it up manually.
9. Click **Confirm** to finish this action.

How to start, schedule, delete a task and check detail information.

When you set a one time task, you can launch the task on the overview page, change the task to a scheduled one, delete the task, or view more information for the task.

To **Start** the one time task, please follow the steps below:

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Start** button, and the task starts right away.

To **Edit** the schedule of the task, please follow the steps below:

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Schedule** button.
4. Set the schedule for your task. You can set it as **Manually**, **Daily**, **Weekly**, **Monthly**,

or **Repeat** in a period of time of the time.

5. Set up the start time for your scheduled task.
6. Click **Confirm** to finish this setting.

To **Delete** a task, please follow the steps below:

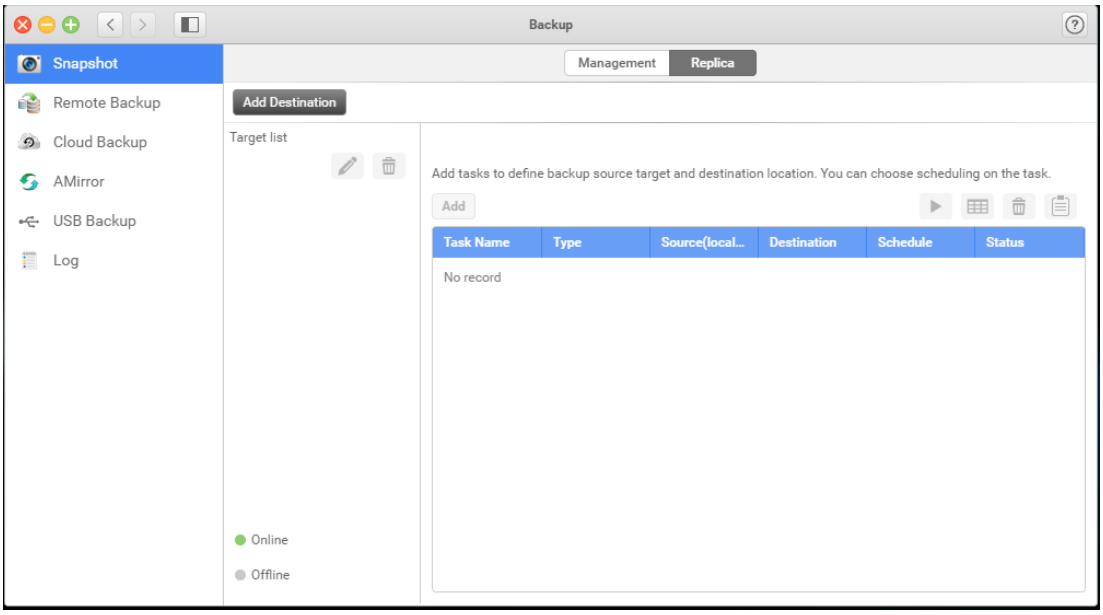
1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. The confirm window will pop out. Click **Confirm** button to delete the task.

To View more information for the task, please follow the steps below:

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Log** button.
4. The detail information window will pop out. Click **OK** button to close the window.

Remote Backup

In **Remote Backup**, you can backup your files across the network via rsync from an Atlas S8+ to another Atlas S8+ or rsync compatible destinations to prevent data loss. With this feature, data loss is no longer a disaster for system administrators.



How to add a destination

Before backing up your files to the remote site, you will need to add at least one destination to store your files.

NOTE

1. Make sure the Rsync service is enabled on your remote site.
2. Rsync is a file based backup protocol, which means, you will need at least one folder at your remote site.

To Add **Destination**, please follow the steps below:

1. Click **Add destination** button on the top left corner of the window.
2. Enter the **IP address / Host name** of your remote destination.

NOTE

By clicking the drop-down menu, you can find all Atlas S8+ on the same network.

3. Enter a name for your **Target**.

NOTE: Target name naming rule

1. Length: 1-128 characters
2. Invalid 【 `~!@#$^&*()=+[]{}\|/;:'",<>?% 】and space.
3. It’s not case sensitive.
4. "." can’t be placed neither in the beginning nor the end.

4. Enter the port number. (The default port is 873)

NOTE

Please make sure the port number is set as same as the remote rsync server.

5. Enter the **Username** and **Password**, which can access remote destination.
6. Click the **Test** button to test the connection ability between local host and remote destination.
7. Click **Confirm** button to finish the action.

How to edit or delete the destination

You can edit the destination for its IP address / Host name, port number, Target name, user name, password and delete the target.

To edit the destination, please follow the steps below:

1. Select a destination on the **Target list**.
2. Click **Edit** button on the top of the list.
3. The edit window will pop out and select the item you want to edit.

CAUTION:
Changing the destination IP / Hostname may cause a backup task to fail.

4. Click **Confirm** to finish the action.

To delete the destination, please follow the steps below:

1. Select a destination on the **Target list**.
2. Click **Delete** button on the top of the list.
3. The confirm window will pop out.
4. Click **Confirm** to finish the action.

How to create a task for a destination.

To **Add** a remote back task, please follow the steps below:

1. Select a target on the target list.
2. Click **Add** button to add a task.
3. Select the Replication or Restore for the task.
4. Enter a name for your **Task**.

NOTE:

Task name naming rule:
1. Length: 1-128 characters

2. Invalid 【 `~!@#$^&*()=+[]{}\|/;:'",<>?% 】and space.

3. It’s not case sensitive.

4. "." can’t be placed neither in the beginning nor the end.

5. Select a **Shared folder** or **Sub-folder** from your local host by clicking the button on the right hand side of the window.
6. Select a **Shared folder** or **Sub-folder** at your remote site by clicking the button on the right hand side of the window.
7. Set the schedule for your task. You can set it as **Manually**, **Real time**, **Daily**, **Weekly**, **Monthly**, or **Repeat** in a period of time of the time.
8. Set the start time for your scheduled task.
9. Check the summary of the task.
10. Click **Confirm** to finish the setting.

How to start, set option, schedule, delete a task and check detail information.

When you set a one time task, you can launch the task on the overview page, change the task to a scheduled one, delete the task, or view more information for the task.

To **Start** the one time task, please follow the steps below:

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Start** button, and the task starts right away.

To **Schedule** the schedule of the task, please follow the steps below:

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Schedule** button.
4. Set the schedule for your task. You can set it as **Manually**, **Daily**, **Weekly**, **Monthly**, or **Repeat** in a period of time of the time.
5. Set the start time for your scheduled task.
6. Click **Confirm** to finish this setting.

To **Set option** for the task, please follow the steps below:

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Option** button.

4. Set the policy and file filter for the task.

NOTE:

• You can setup policy for the task for the following policies,

1. the maximum transfer rate,
2. SSH encryption,
3. compressed file transmission,
4. Ignore symbolic link,
5. Replicate ACL and extended attribute,
6. remove excluded files from the destination.

• You can setup the filter for the following types

1. Maximum and or Minimum file size.
2. Last modified days.
3. File date and time for a period of the time.
4. Include or Excluded file type.
5. This file filter can be set only for replica task.

5. Click **Confirm** to finish the setting.

To View more information for the task, please follow the steps below:

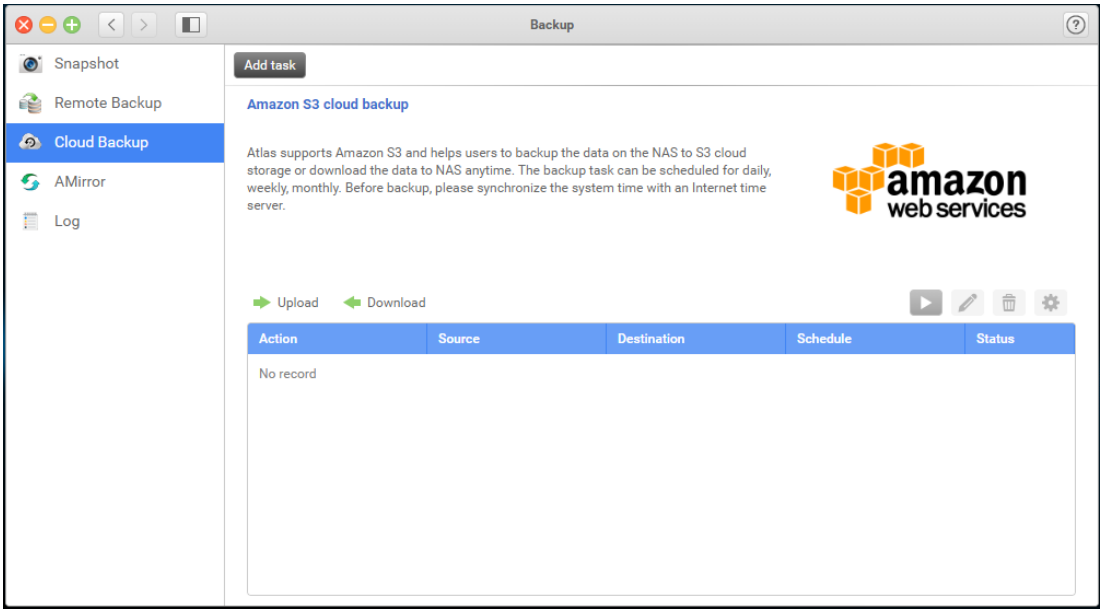
1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Log** button.
4. The detail information window will pop out. Click **OK** button to close the window.

To **Delete** a task, please follow the steps below:

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. The confirm window will pop out. Click **Confirm** button to delete the task.

Cloud Backup

In **Cloud Backup**, the Atlas S8+ supports the public cloud using Amazon web services (S3) as the backup/restoration solution. Your data will be backed up off-site to prevent unexpected data loss due to disk failure or physical system damage.



In overview page, you can add, view, start/stop, edit, delete or set the backup option for all your backup/restoration tasks.

How to add a task

By adding the task, you can backup or restore your data to the S3 compatible cloud storage.

To add a **Task**, please follow the steps below:

1. Click **Add task** in the top of the window.
2. Enter a name for the task.
3. Select the action of the task. It can be set as **Upload** or **Download**.
4. Select the destination on S3 by clicking the icon on the right-hand side of the window and click confirm when you finish setting.

NOTE
Before selecting the destination on S3, you will need the Access key, Secret key and setup the bucket in Amazon service.

5. Select a folder on your Atlas S8+ and click confirm when you finish setting.

6. Set the schedule for your task. You can set it as **Manually**, **Real time**, **Daily**, **Weekly**, **Monthly**, or **Repeat** in a period of time of the time.
7. Check the summary of the task.
8. Click **Confirm** to finish the setting.

How to Stop/Stop the task

After the task was created, you can Stop or Start the task manually.

To **Stop** or **Start** the task, please follow the steps below:

1. Select the task on the list shown below.
2. Click the **Stop** or **Start** button on the top right corner of the table.
3. The task will be stopped or started right away.

To edit the task

You can always edit the task afterward. You can change the backup action, destination, source and schedule of the task.

To edit the task, please follow the steps below:

1. Select the task on the list shown below
2. Click **Edit task** button on the top right corner on the table.
3. Edit the action of the task. It can be set as **Upload** or **Download**.
4. Edit the destination on S3 by clicking the icon on the right-hand side of the window and click confirm when you finish setting.

NOTE
Before selecting the destination on S3, you will need the Access key, Secret key and setup the bucket in Amazon service.

5. Edit a folder on your Atlas S8+ and click confirm when you finish setting.
6. Edit the schedule for your task. You can set it as **Manually**, **Real time**, **Daily**, **Weekly**, **Monthly**, or **Repeat in a period of time**.
7. Check the summary of the task.

8. Click **Confirm** to finish the editing.

To delete the task

Once if the task is no longer needed, you can just delete the task.

To **Delete** the task, please follow the steps below:

1. Select the task on the list shown below.
2. Click the **Delete** button at the top right corner.
3. Click **Confirm** in the confirmation window to delete the task.

To set the option for the task

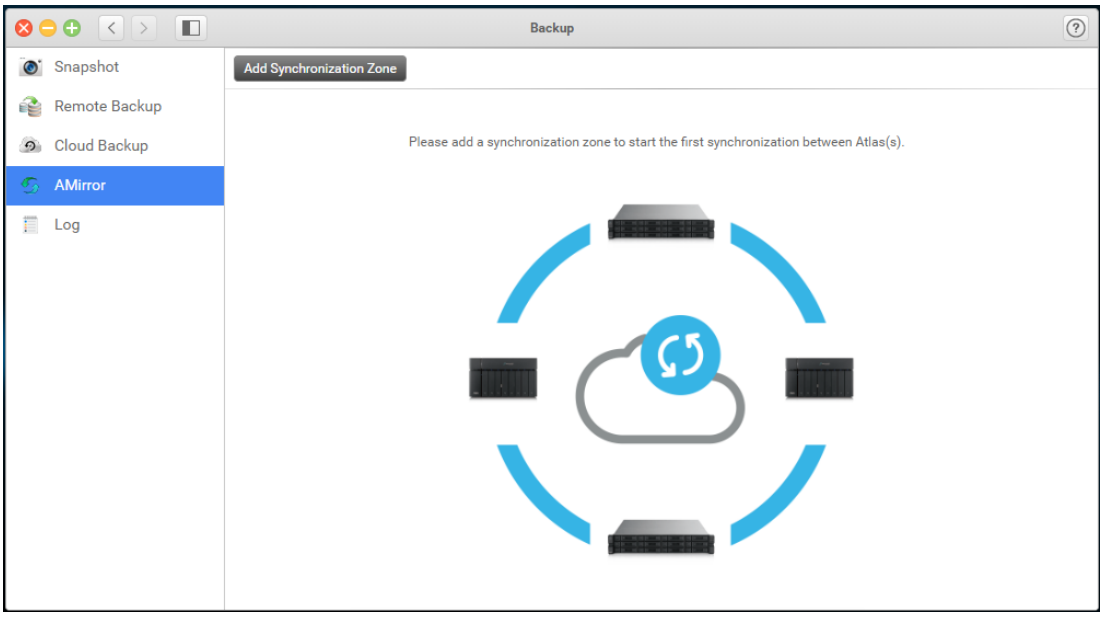
While backing up data, you can make your backup even more smarter or security.

To set up the **Option,** please follow the steps below:

1. Select the task on the list shown below
2. Click the **Option** button at the top right corner.
3. Click the option(s) you want to set and click **Confirm** to finish the setting.

AMirror

In **AMirror**, you can backup or synchronize your files between multiple Atlas S8+ over the Internet or local network.



Sync your data in a zone

With our unique technology, AMirror, you can easily sync files between different Atlas S8+ by joining an existing zone or create a new zone.

NOTE:
1. Before using AMirror, you will need at least one shared folder on your Atlas S8+.
2. There should be only one local folder in a zone.

To create a new zone or join an existing zone, please follow the steps below:

1. Click **Add Syncronize Zone** on the top of the window.
2. In create wizard, you can choose to **Create a new zone** or **Join another zone from another NAS.**
3. Select create a new zone.

   ① Specify the zone as a 1-way zone or 2-way zone.

NOTE:
1. 1-way zone means you send files to the master folder and sync to others.

2. 2-way zone means you can change files in each folder and the changes will sync to all folders in the zone.

② Specify the zone name and select one folder in your local Atlas S8+.
③ Check summary of the zone.
④ Click **Confirm** to finish the action.

4. Select join another zone from another NAS

① Select one local folder.
② Enter the remote destination information, IP, username, and password.

NOTE

You can click the dropdown menu to find all available Atlas S8+.

③ You can test the connection for authentication and performance between NAS.
④ Select a zone you want to join on the remote destination.
⑤ Check the summary of joining zone.
⑥ Click **Confirm** to finish the action.

Edit a zone

When the zone starts to sync, you can stop the syncing, delete the zone, edit the backup options, and check the detail information.

NOTE:
After a zone is created, it becomes the default zone. A sync will start when both a local and a remote zone has been added.

To stop the synchronization, please follow the steps below:

1. Select a zone.
2. Click the function button on the top right corner of the window.
3. Click **Stop** and the zone stop to sync right away.

To delete a zone, please follow the steps below:

NOTE
Before deleting a zone, any synchronization running must to be stopped.

1. Select a zone
2. Click **Delete** button.
3. A confirmation window will pop out.
4. Click **Confirm** to finish the action.

To edit the option of the zone, please follow the steps below:

1. Select a zone
2. Specify the policy for SSL encryption during transmission.

NOTE:
By default, ssl encryption is enabled.

3. Specify the file filter while syncing. By clicking the checkbox, you can set the excluded file type or specify a particular file type.

NOTE
By setting up multiple file format, you can enter the words as following, *.abc, *.bbb and etc.

4. Configure the maximum number of previous versions for a file.

NOTE:
1. Default maximum previous versions is 1

2. When you lower the maximum previous versions amounts, older files will be removed.

5. Click **Confirm** to finish the setting.

Edit a folder in the zone

After a folder is joined to the zone, you can disjoin it from the zone, change the local folder, rollback the file to the previous version, and restart the folder when it cannot be automatically be synced.

To disjoin the folder, please follow the steps below:

1. Select a domain folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Disjoin**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

To change local folder, please follow the steps below:

1. Select the local folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Change local folder**.
4. Select a new folder.
5. Check the summary.
6. Click **Confirm** to finish the action.

To rollback the file on the previous version, please follow the steps below:

1. Select the local folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Version rollback**.
4. Select the file you want to rollback.
5. Select the file version.
6. Check the summary
7. Click **Confirm** to finish the setting.

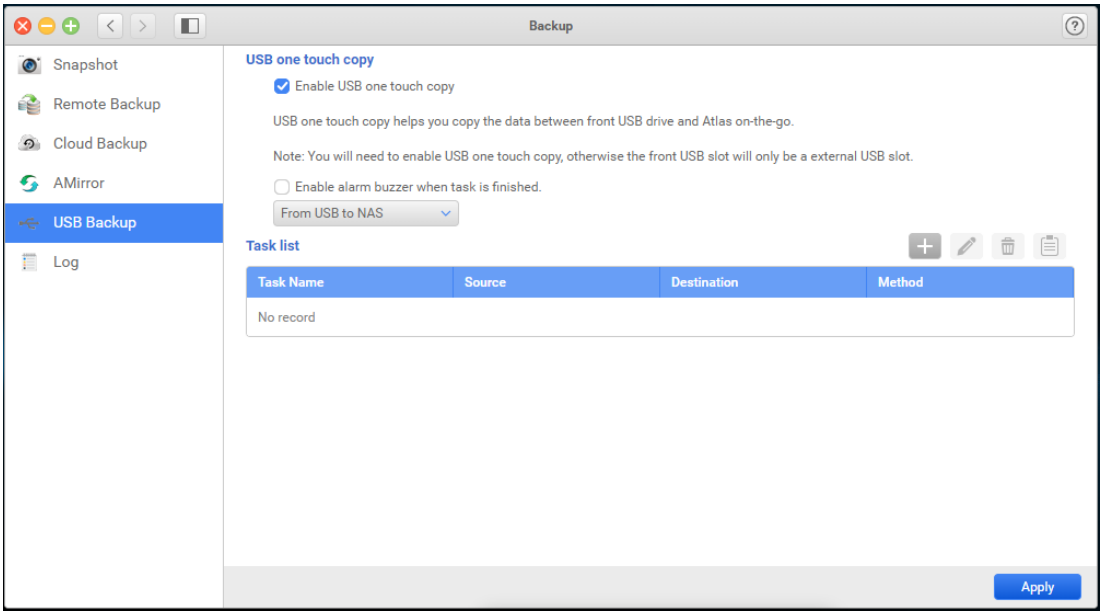
To restart the folder, please follow the steps below:

1. Select the folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Restart**.
4. System will try to recover the folder.

NOTE
When a folder is not able to sync, it is usually caused by lack of disk space at the sync target. After creating more space at the destination, the sync can be restarted manually by clicking **Restart**.

USB Backup

In **USB Backup**, ASM supports USB backup between the Atlas S8+ and external USB drives or storage devices by simply one touch on the front panel of Atlas S8+.



In overview page, you can view the current task list, add a task, edit or delete a task and check the information of tasks. USB backup can be made more convenient by informing you of task completion with the buzzer, simply click **Enable buzzer when task is finished**. You can backup your sensitive data from a USB drive to Atlas S8+ or back it up in the opposite direction, Atlas S8+ to a USB drive.

NOTE
USB Copy Button is located in upper left of Atlas S8+ and next to USB port. The USB Copy Button works only for USB devices plugged into the front USB port.

Add a task

USB one touch backup is task oriented allowing for multiple scheduled backup tasks to and from multiple USB devices nightly or whenever is required.

NOTE
Before adding tasks, you need to click Enable USB one touch copy and click the Apply button

To add a **Task**, please follow the steps below:

1. Select the direction of your USB one touch backup task.
2. Click **Add** in the top right of the task list.
3. Enter a name for the task.
4. Select the **Source** and **Destination**.

NOTE
Source and destination can be selected ~~to~~ up to folder-level.

5. Select the copy method, **Full copy**, **Incremental copy**, or **Synchronize**.
6. Check the summary of the task.
7. Click **Confirm** to finish the setting.

Edit the task

You can always edit the task afterward. You can change the task name, source, destination, and copy method.

To edit the task, please follow the steps below:

1. Select the task on the list shown below
2. Click **Edit task** button on the top right corner on the table.
3. Edit the task name, source, and destination.
4. Click Next.
5. Edit the copy method.
6. Click Next.
7. Check the summary of the task.

8. Click **Confirm** to finish the editing.

Delete the task

Once if the task is no longer needed, you can just delete the task.

To **Delete** a task, please follow the steps below:

1. Select the task on the list shown below.
2. Click the **Delete** button at the top right corner.
3. Click **Confirm** on the confirmation window to delete the task.

View the information of the task

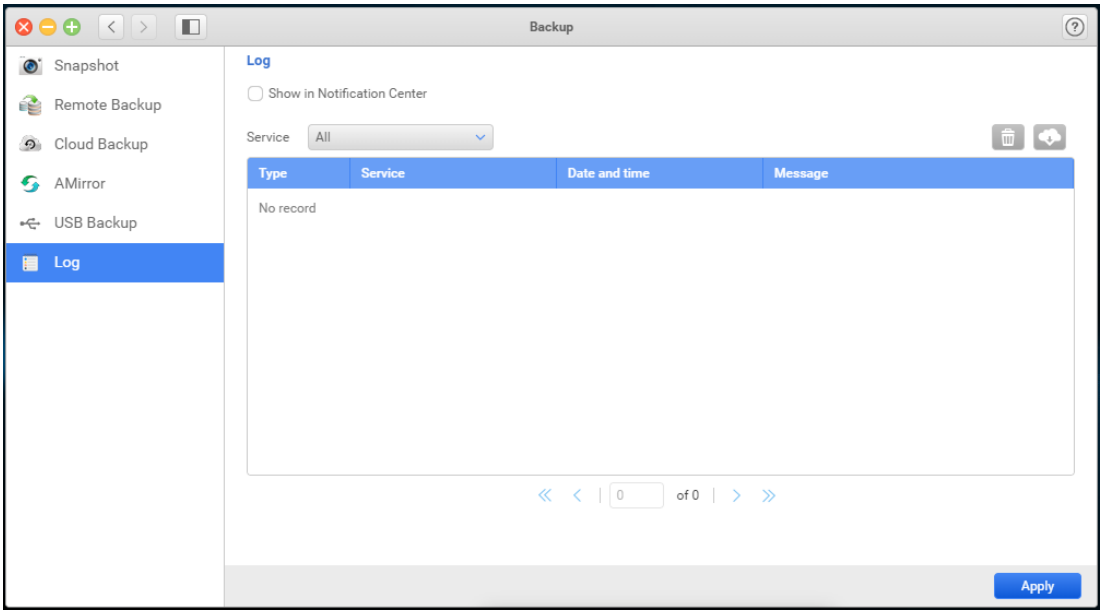
You can check the detail information of the task for its type, source, destination, create time, last access time, and last access status.

To check detail information, please follow the steps below:

1. Select the task on the list shown below
2. Click the **Log** button at the top right corner.
3. All details information will pop out and click **OK** to close the window.

Log

In **Log**, you can check and manage all the events occurred in the application. Meanwhile, you can show your events on the Notification Center for your easy management of Atlas S8+.



How to show events in notification center

Notification center is the desktop function which helps the administrator to monitor Atlas S8+ easier.

To **Show in Notification Center**, please follow the steps below:

1. Click the check box next to **Show in Notification Center** .
2. Click **Apply** to take effect.

How to manage the events

You can sort, delete and download the events occurred in the application.

To sort the events, please follow the steps below:

1. Click the drop-down menu.
2. Select the backup function you want to view, and the table will show the events you wish to check.

To delete the events, please follow the steps below:

1. Click the **Delete** button.
2. A confirmation window will pop out.
3. Click **Confirm** to take effect.

To download the events, please follow the steps below:

1. Click the **Download** button.
2. The log file will download immediately.

NOTE:
The log file will be shown as LOG-Host name-Date-Time.txt

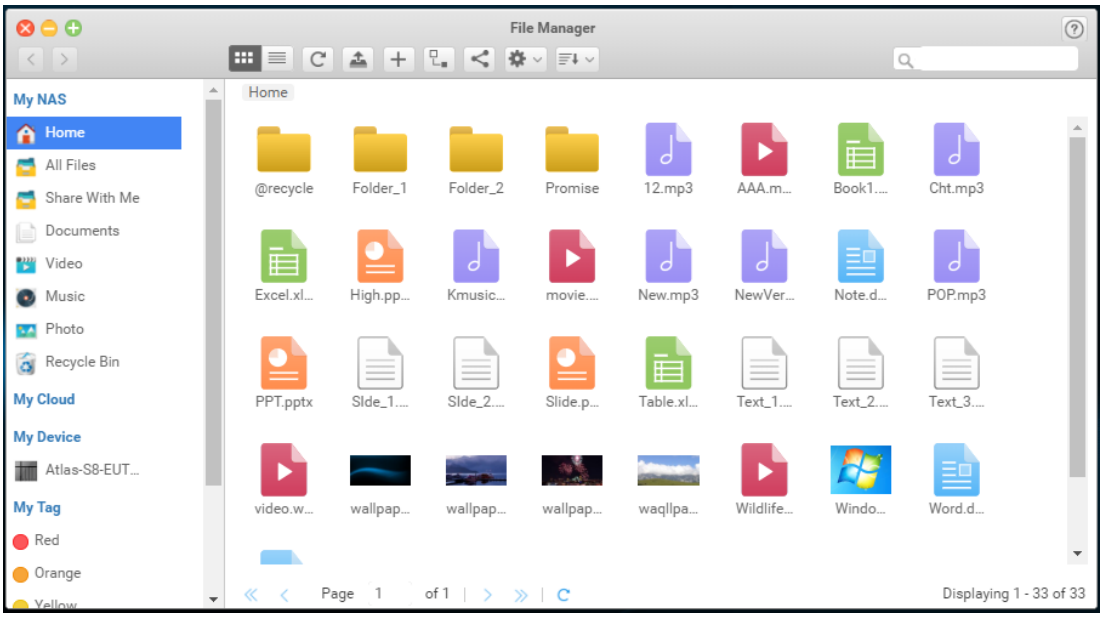
File Manager

File Manager

File Manager is a web based file management center for Atlas S8+. You can organize photo, music, video and document with the File Manager when the **Media Library** is enabled. File Manager helps easily upload, download and manage NAS files by using a web browser. With File Manager, you can mount your public cloud service (OneDrive, Google Drive, Dropbox) and remote network drive to File Manger to easily manage your private and public cloud together.

Requirement:

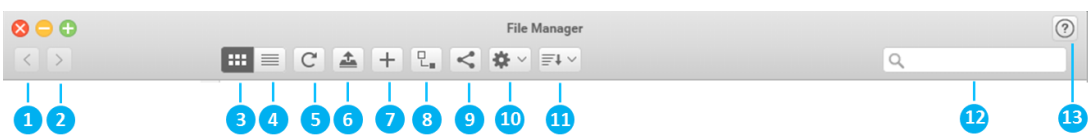
It is recommended that the web browser used be updated to the latest version.



Start to use File Manager:

There are two operation areas of File Manager. Please refer to the introduction below before getting started:

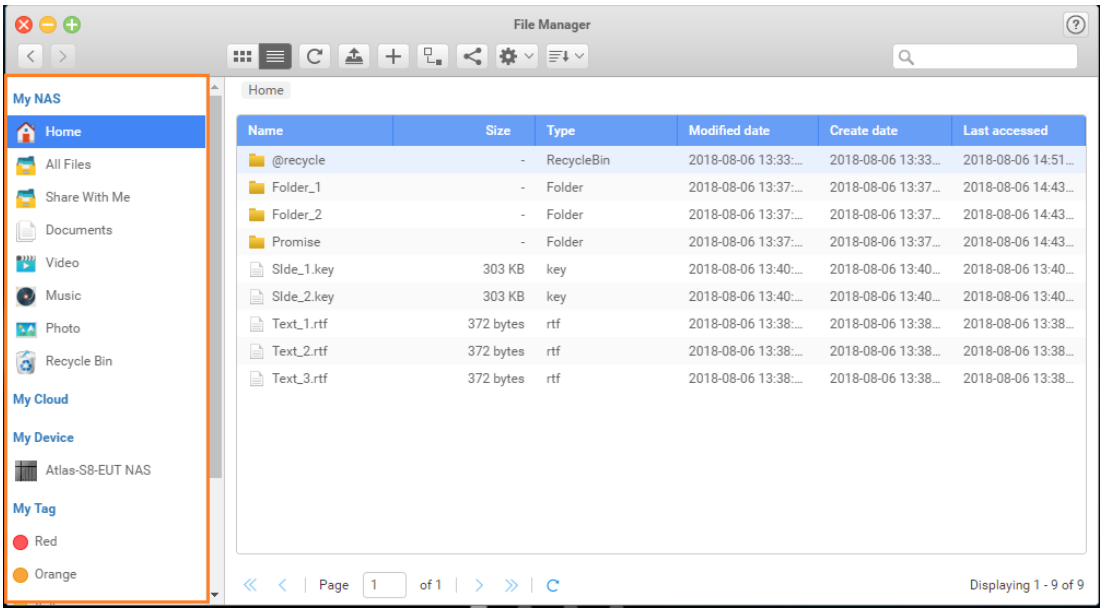
1. Toolbar



Tool bar functions introduction:

No.	Feature	Description
1	Previous page	Back to the previous page.
2	Next page	Go to next page.
3	Icon mode	Show the file and folder with icon and mouse over will display file's or folder's information such as name, size, type, time and path.
4	List mode	List file and folder in detail such as name, size, type, modified date, create date and last accessed.
5	Refresh	The data and service status will be up to date.
6	Create folder	Create folder on the current page.
7	Upload	Upload file or folder.
8	Mount	Mount cloud(Google Drive, OneDrive, Dropbox), remote network drive (CIFS, FTP, SFTP, WebDAV).
9	Share	Manage your share link, home share on this page.
10	Settings	Set user mount, share permission and conflict name policy(overwrite or skip).
11	Sort	Sort file and folder by name, type, create date, modified date, last access, and ascending, descending arrangement.
12	Search	Search file and folder by name, type.
13	Help	File Manager introduction.

2. Menu bar



- My NAS

  ① Home: The location of your home directory.
  ② All File: All the NAS file will be listed here.
  ③ Document:

  When **Media Library** is enabled, the document files will automatically be indexed on this page. Document files support “DOC”, “DOCX”, “PPT”, “PPTX”, “XLSX”, “XLS”, “PAGE”, “KEYNOTE”, “NUMBERS”, “PDF”, “TXT”, “ADE”(PowerPoint), “IGS”(Lotus Notes), “RTF”(Word), “WRI”

  ④ Video:

  When **Media Library** is enabled, the video will automatically be indexed on this page. Video support "3G2", "3GP", "ASF", "ASX", "AVI", "DIVX", "FLV", "M1V", "M2V", "M4V", "MKV", "MOD", "MOV", "MP4", "MPEG", "MPG", "MT2S", "MTD", "MTS", "RM", "RMVB", "SRT", "SWF", "TOD", "TRP", "TS", "VOB", "WMV", "MRW", "NEF", "OBJ", "ORF", "PEF", "PNG", "PS", "PSD", "PSPIMAGE", "PTX"

  ⑤ Music:

  When **Media Library** is enabled, the music will automatically be indexed on this page. Music support “AIF", "AIFF", "APE", "FLAC", "IFF", "M3U", "M4A", "MID", "MP3", "MPA", "OGG", "OGA", "RAW", "WAV", "WMA"

  ⑥ Photo:

  When **Media Library** is enabled, the photo will automatically be indexed on this page. Photo support "3DM", "3DS", "3FR", "AI", "ARW", "BMP", "CR2", "CRW", "DCR", "DDS", "DNG", "EPS", "ERF", "GIF", "JPE", "JPG", "JPEG", "K25", "KDC", "MAX", "MEF", "MOS", "MRW", "NEF", "OBJ", "ORF", "PEF", "PNG", "PS", "PSD", "PSPIMAGE", "PTX", "RAF", "RW2", "SR2", "SRF", "SVG", "TGA", "THM", "TIF", "TIFF", "X3F", "YUV"

  ⑦ Recycle Bin:

  Deleted file and folder will be listed on this page.

- My Cloud

  Atlas S8+ supports Google Drive, Dropbox, OneDrive to mount your public cloud drive on File Manager.

- My Device

My Device lists all the attached devices by Atlas S8+. You can click Mount bottom to mount your remote network drive (CIFS, FTP, SFTP, WebDAV) or attach an external device on your NAS

- My Tag

  With tag function, you can organize files by project or purpose, without having to move them into a specific folder. Your tags automatically show in the tag folder, so it's easy to manage tagged files no matter where they're located. And tag color is including Red, Orange, Yellow, Green, Blue, Violet, and Gray; you can use classification by your definition.

- Create folder

  Click **Create** button on the tool bar and enter your folder name then the new created folder will in the current folder.

- File Management

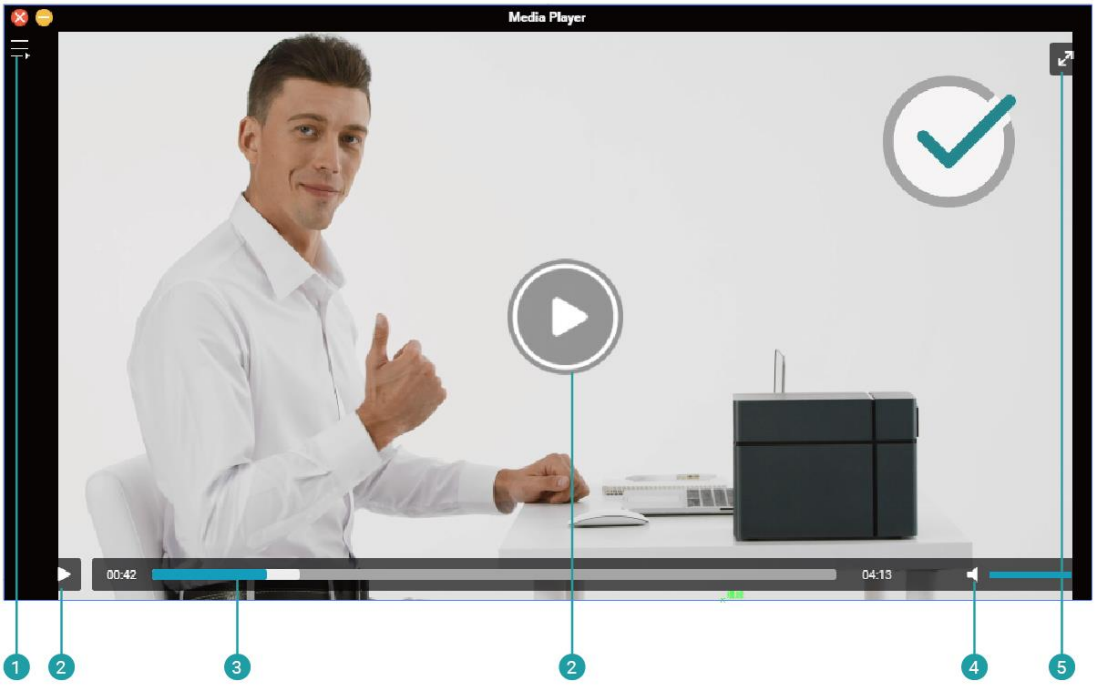
  You can select a file and manage it by mouse right click:

Operation	Description
Office Preview	If you select office file, The document will open via Google office online. Atlas S8+ supports preview PDF, powerpoint, excel and word. Before you preview, please install chrome extend first.
Transcode and streaming	If you select a media file, you can choose a resolution to transcode your media file.(240P, 360P, 480P, 720P, 1080p) and play immediately.
Transcode here	You can transcode your media file, and the file will be displayed on @transcode folder.(240P, 360P, 480P, 720P, 1080p).
Download	Download your file.
Extract	Extract your compressed file.
Compress	Compress your file.
Cut	Cut your file to another location.
Copy	Copy your file to another location.
Delete	Delete your file.
Rename	Rename your file.
Paste	Paste your file to another location.

Share file links	Create share link, and you can share via mail or share to social media.
Share to other NAS user	Share file with other NAS user.
Pin to Shortcut	The file will be pinned to desktop as a shortcut.
Properties	File detail information such as size, last modified date, and path.
Tags…	Tag your file by different categories.

Play a media file:

To play a media file with File Manager, double-click a media file (photo, music and video files) and the Media player (a built-in media player on the NAS) will appear to play the file:

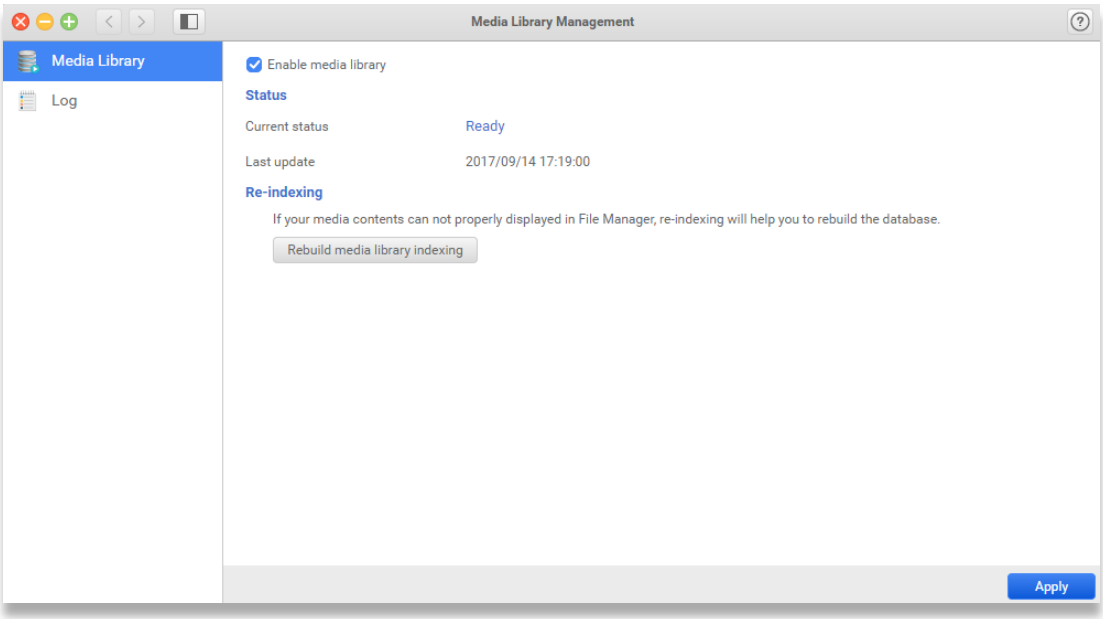


No.	Feature	Description
1	Menu	Show your play list.
2	Play / Pause button	Allows you to play and pause the video.
3	Seek bar	Control video progress.
4	Volume	Adjust the video and music volume.
5	Full screen	Switch your screen to full mode.

Media Library Management

Media Library

In Media Library, you can scan multimedia and documents such as, videos, music, videos, Microsoft office files, and Apple offices files, on Atlas S8+ and index them by categories in **File Manager**.



Status

Click **Enable media library** checkbox, you can see the current status and the last update time of the index.

Scan setting

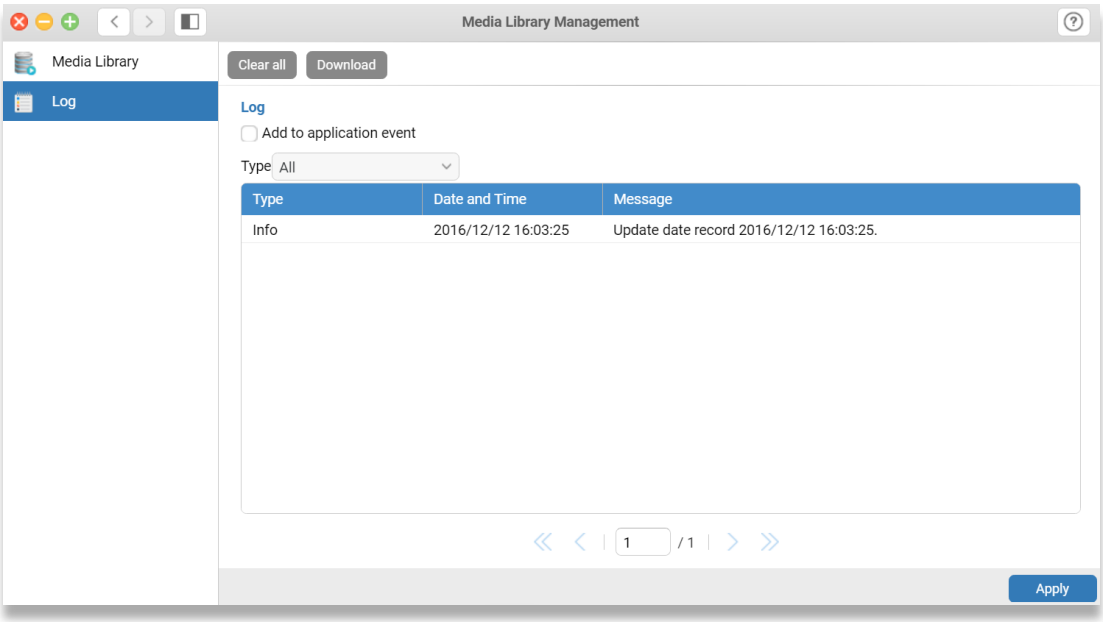
You can select which category by clicking the check box for Video, Music, Photo, and Documents.

Re-indexing

If your media content is displayed incorrect on File Manager, you can re-index it and create a new library. Click **Rebuild Media Library**Indexing button to rebuild the index.

Log

Here you can check the activities of media library. Choose the information type from **Type** drop-down menu to see the detail message. If you want to view the status in the application event, click **Show in Notification Center** checkbox.



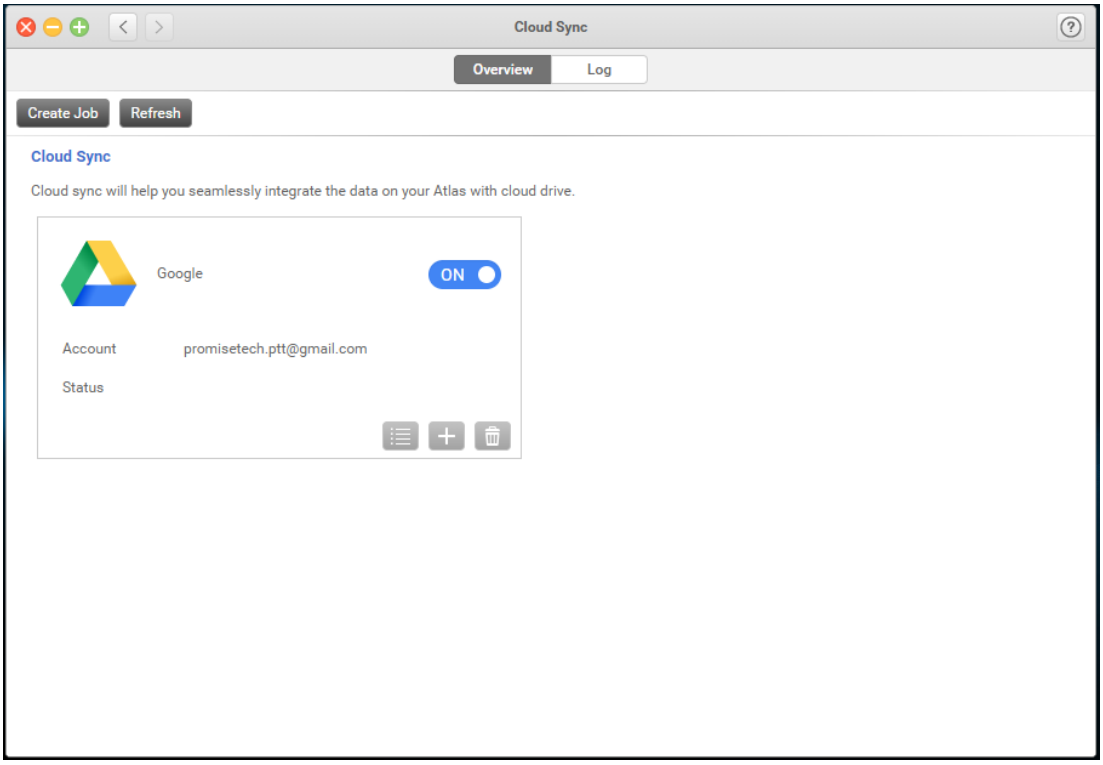
PROMISE CLOUD APPLICATIONS

Cloud Sync

With **Cloud Sync**, you can seamlessly sync and share files between Atlas S8+ and your cloud drive such as Google Drive, Dropbox and OneDrive.

Overview

In **Overview** , you can see all your job status and manage the jobs' setting on it.



Requirements:

Before setting Cloud Sync, please check the items below:

- The Atlas S8+ is connected to the internet.
- Cloud drive account is active by cloud drive provider.

Refresh this page

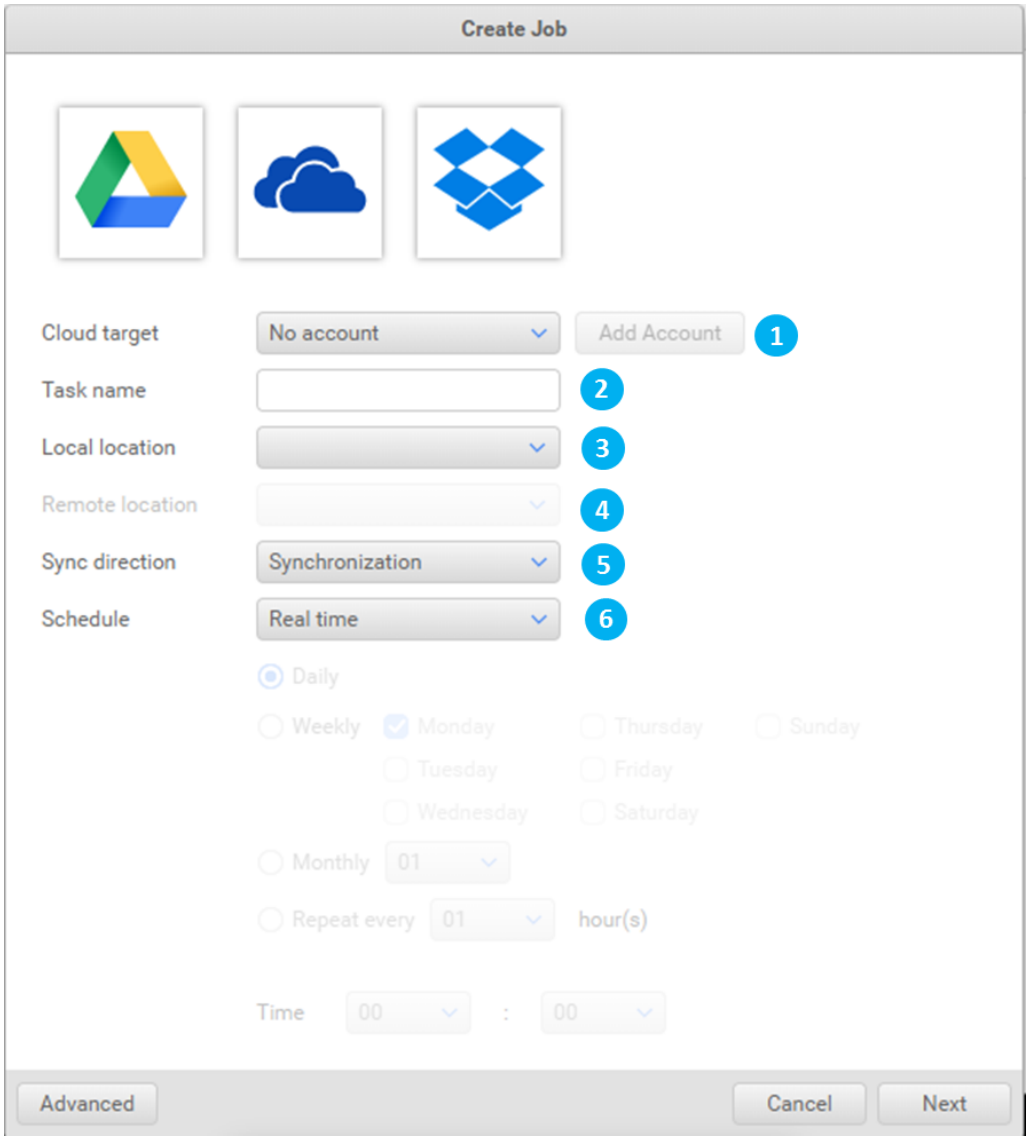
You can update all your data by clicking the **Refresh** button on this page.

Create a new job

To create a new job, please follow the steps below:

1. Click **Create Job** button and a create job window will appear.
2. On the top of the page, you can find the logos of cloud drive service. Choose service and click **Add account**. The cloud authentication page will be open on the browser with a new tab. Please log in and confirm your cloud permission.
3. Fill in all the job information.
4. Click **Next** button, and a **Job Confirmation** page will pop up.
5. Review the job summary, if everything is ok, please click **Confirm** button to finish.

Your task will be shown on the overview page.

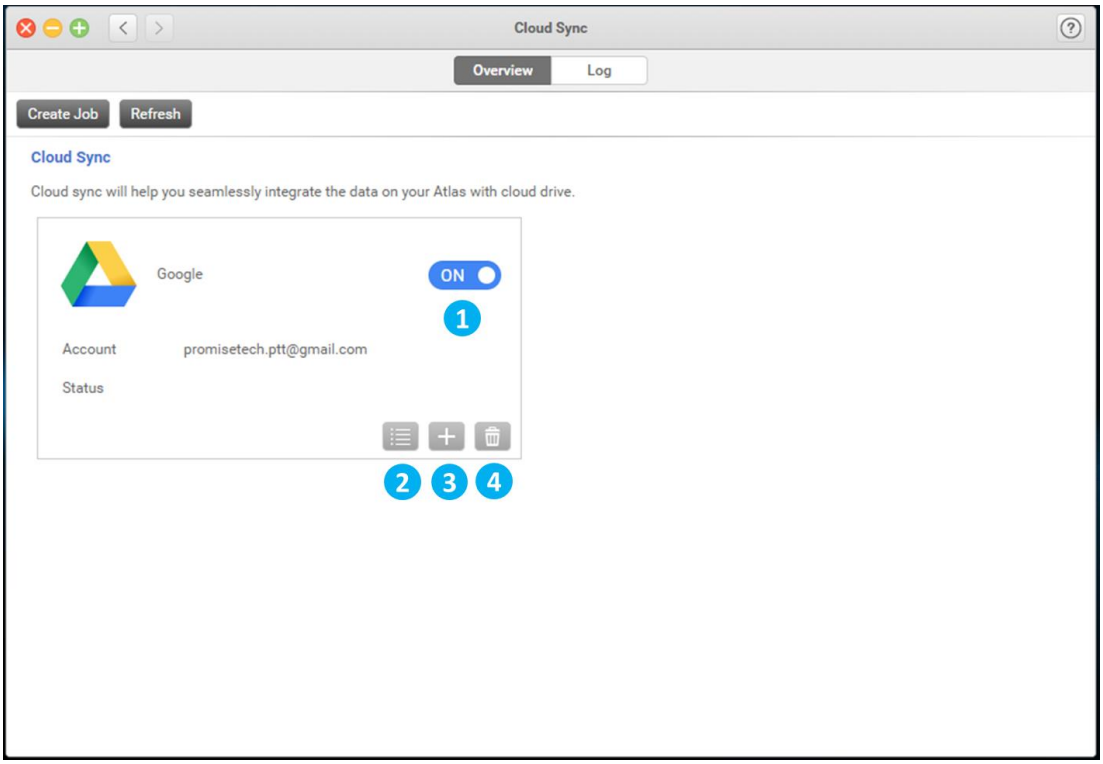


Create job setting items introduction:

No.	Button	Description
1	Add account	Support Google Drive, Dropbox and OneDrive.
2	Task name	The task name will show on the task list. And naming rule as below. • Length: 1-128 characters • Invalid 【 `~!@#$^&*()=+[]{}|/;:'",<>?% 】and space.
3	Local location	Select a Atlas S8+ local folder. All folders and files in this folder will be synced to the cloud drive.
4	Remote location	Select a remote folder on the cloud drive. All folders and files in this folder will be synced to the Atlas S8+ local folder.
5	Sync direction	There are three ways to manage your data. • Synchronize – The data in local folder and the remote folder will be synced. • NAS to Cloud – The data in local folder will back up to your cloud drive. • Cloud to NAS – The data in remote folder will back up to your Atlas S8+.
6	Schedule	There are two ways for the schedule settings. • Real Time – The data will always sync between your Atlas S8+ and cloud drive. • Periodically –You have four types to choose, Hourly, Daily, Weekly, and Monthly.
7	Advanced	• Filter by Size – You can set the max size limit and if the file is over this limit, it will not be synced. • Filter by Type – You can choose the file type you do not want to sync. • Conflict Policy –There are four ways to choose when file name is conflicted: Rename Local Files, Rename Remote Files, Overwrite Local Files, Overwrite Remote Files.

Manage Cloud Sync job

When the jobs are created, all of your jobs will be shown on the overview page. You can check the status, disable cloud drive, add the task or delete cloud account on the overview page.

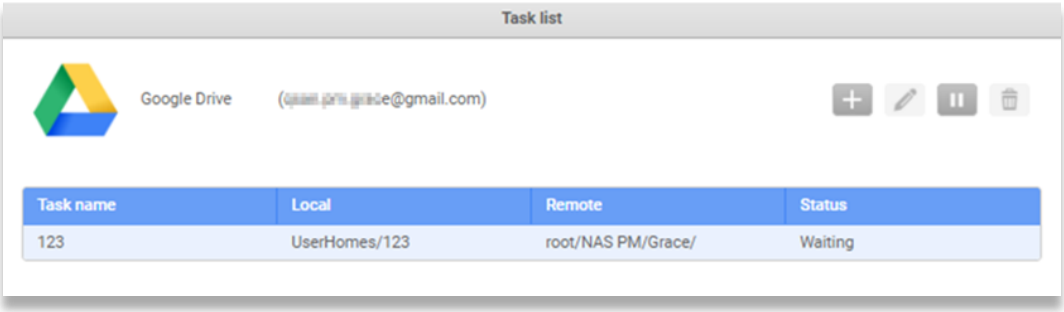


Job action button introduces:

No.	Button	Description
1	Enable/Disable account	Switch the on/off button, cloud account will be enabled / disabled. However, you can still check its tasks and delete the link of the cloud drive.
2	Task list	You can see the task all of this job.
3	Add task	You can add a task for this cloud drive.
4	Delete	Your cloud drive account will be deleted and all the tasks in the account will also be deleted.

Task list

You can see all tasks of this cloud drive account and there are four actions on the task list page: **Add Task**, **Edit Task**, **Start/Pause**, and **Delete**.

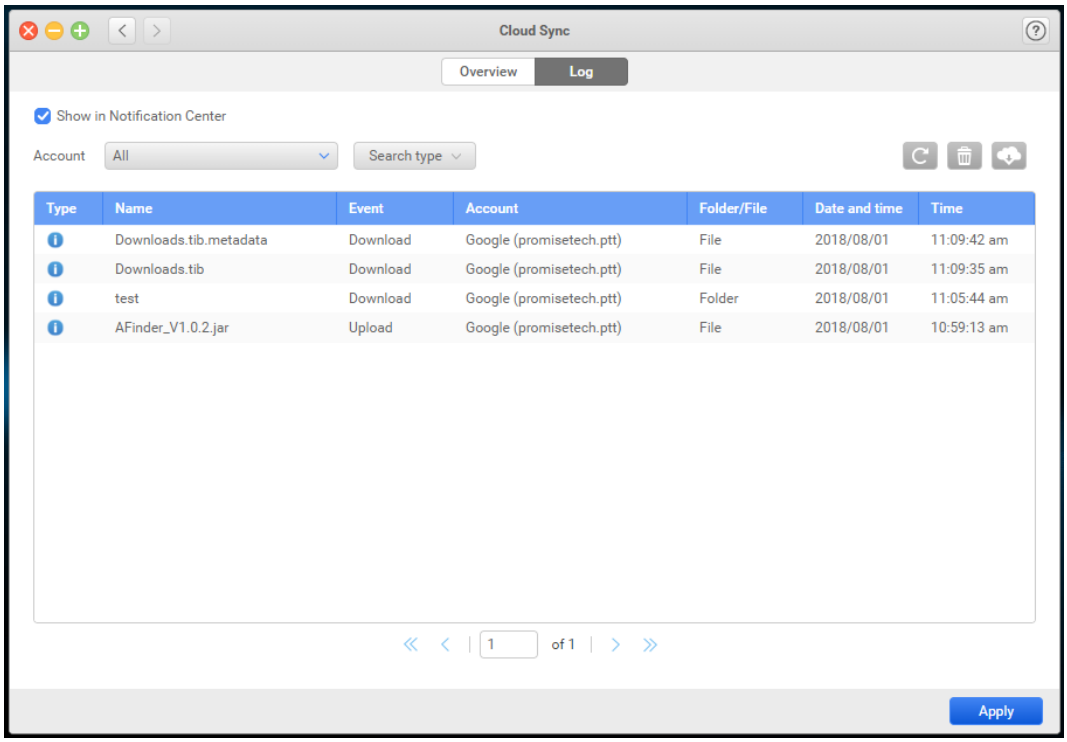


- **Add Task** : You can add a task for the job. The procedure is similar to the procedure of **Create job**. The only difference is you do not need to choose the cloud target.
- **Edit Task** : You can change the task name, sync direction, and schedule.
- **Start/Pause the Task** : By switch bottom, you can on/off the task.
- **Delete Task** : To delete a cloud sync task, please follow the steps below:

  ① Click the delete button; the confirm window will pop up.
  ② Click **Confirm** button to delete the job.

Log

In Log page, you can see all the events that happen in the Cloud Sync. You can choose a specific account from the left drop-down menu to check all the related logs.



Show logs in Notification Center

If you would like to display logs related to Cloud Sync in desktop > Notification Center , please select the Show in Notification Center checkbox.

NOTE
If you cannot view any Cloud Sync-related logs in the Notification Center, please go to Control Panel > Log > General Settings page to check if you have selected the application logs checkbox successfully.

Filter the logs by its account

With the drop-down menu, you can choose to see logs from all account or restricted to a specific account, such as OneDrive, Dropbox or Google Drive.

Search for logs

You can use the drop-down menu to search for logs quickly. To search the log history, please follow the steps below:

1. Enter the keyword in the search bar and press enter to search for logs with the matching keyword.
2. To search the log history by its date and time, you can choose the date and time on the calendar and the drop-down menu. Press **Search** to start searching for logs within the time range.
3. Press **Reset** to return to the default setting.

Refresh the logs

By clicking **Refresh** button, the page will be reloaded and all the new event logs will be added to the list.

Clear all logs

To clear all the logs from your system, please follow the steps below:

1. Click **Clear All** button on the top of the page.
2. Click **Confirm** button to delete all logs.

Download all logs

To download all the logs from your system, please follow the steps below:

1. Click Download button on the top of the page.
2. Choose the destination where you would like to store the logs in.

NOTE:
The downloaded file will be in .txt format, please open the file with software that supports .txt files.

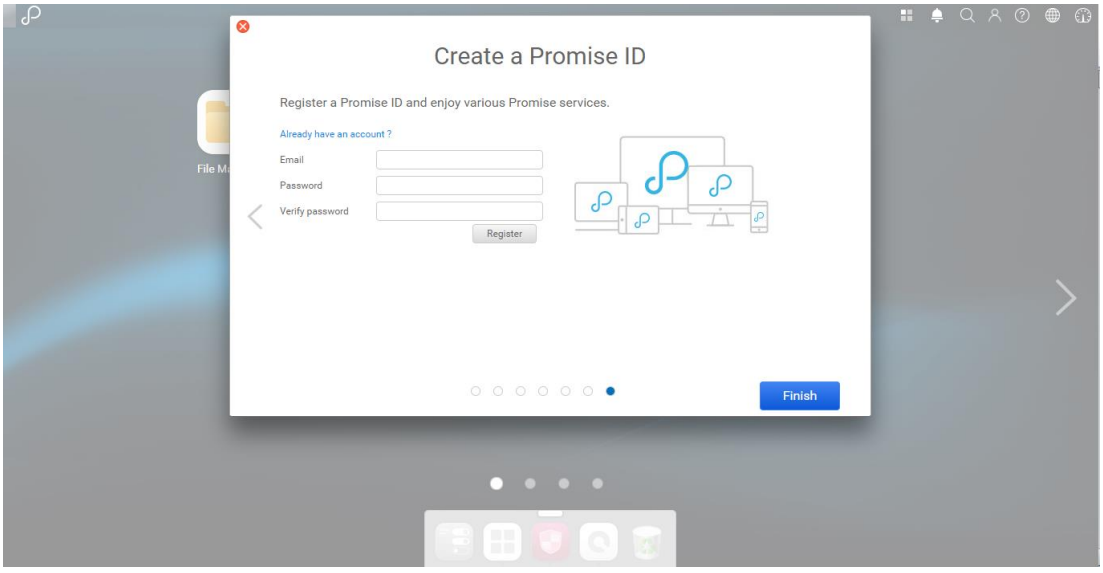
PROMISE Cloud

In PROMISE Cloud page, you can register PROMISE ID to use PROMISE Cloud DDNS service. You can pick your own PROMISE Cloud hostname and easily connect Atlas S8+ anywhere.

Requirement:

Before you use PROMISE Cloud, please check the item as below:

1. The Atlas S8+ is able to connected to the internet
2. Your Email address (PROMISE ID) is available.

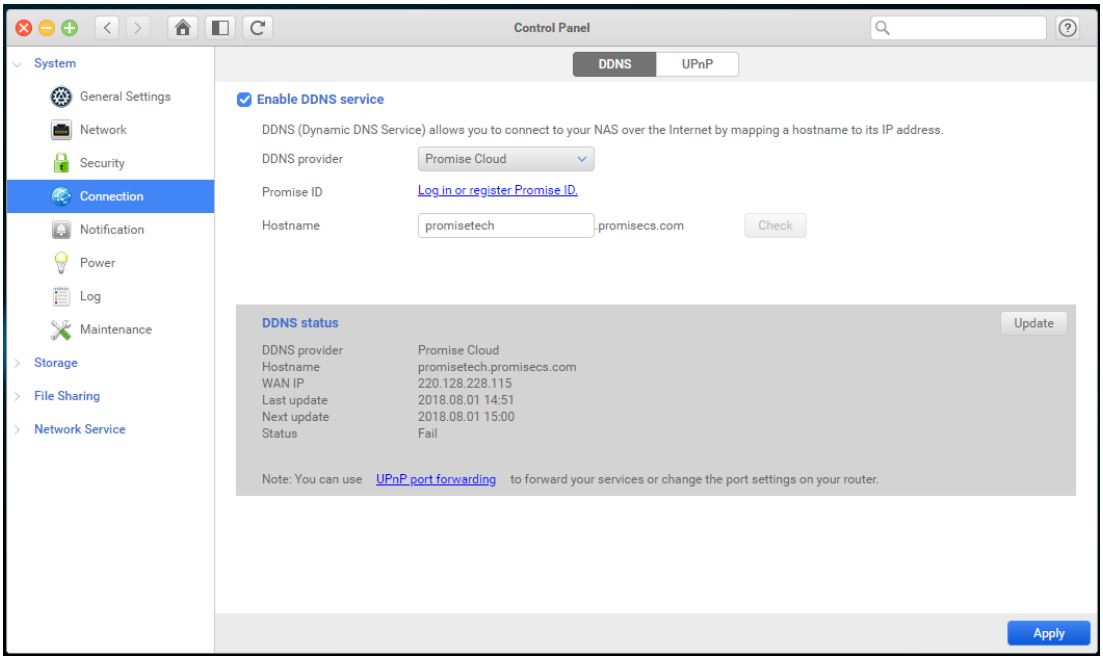


Login or register a PROMISE ID

You only need one PROMISE ID to access PROMISE services. There are three ways to login or to create your PROMISE ID:

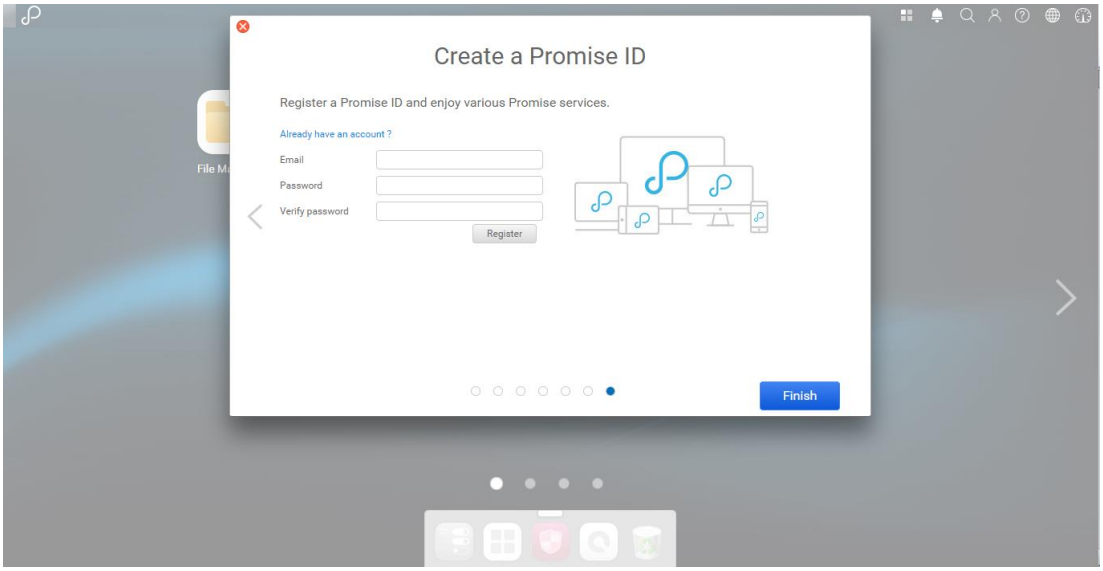
1. In **Connection** > **DDNS** page.

   Select PROMISE Cloud in **DDNS provider** dropdown menu. Then click **Log in or register PROMISE ID** hyperlink.



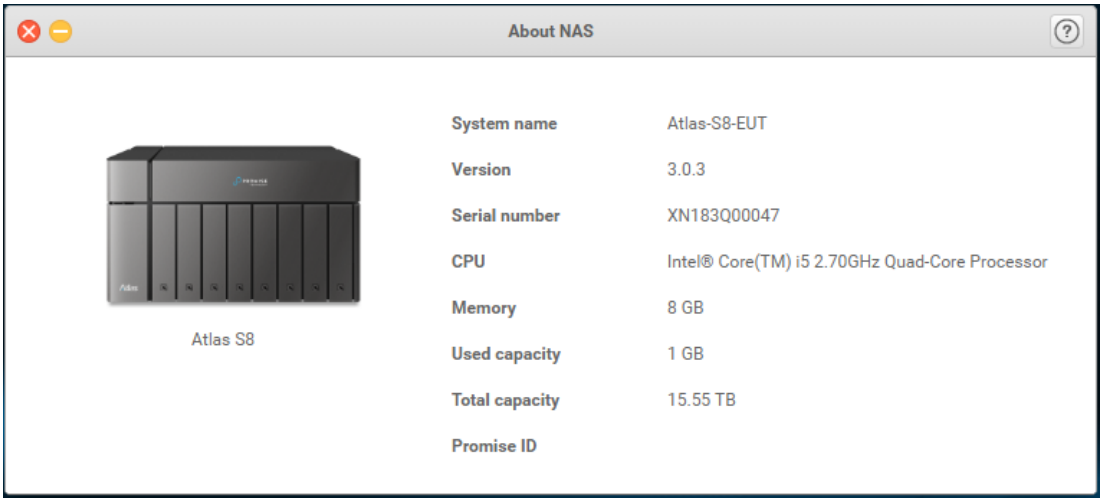
2. In **Tutorial** session.

   When you first start up your Atlas S8+, the tutorial session will automatically appear. You can also find **Tutorial** by clicking the PROMISE logo on the top-left corner on the desktop, then choose **Tutorial**. Click **Start** to go through the session and you will be able to log in by clicking **Already have an account?** hyperlink or to create a PROMISE ID.



3. In **About NAS** page.

   Click on the PROMISE logo on the top-left corner on the desktop, then choose **About NAS**. A pop up window will appear, then click **Log in or register PROMISE ID** hyperlink.



To login or to register, please follow the steps below:

1. Enter your PROMISE ID/ email address and your password, then click **Login** button. If you do not have a PROMISE ID, you can create one by following the steps below. Before you register a new PROMISE ID, consider whether it might be better to continue using one you already have. Click **Log in or register PROMISE ID** hyperlink, a pop up window will appear.
2. Click **Register** hyperlink, another pop up window will appear.

3. Choose a PROMISE ID.

NOTE:
This field must be an email address. For example: user@example.com

4. Enter your password.

NOTE:
It must be between 6 to 16 characters.

5. Enter your password again to verify.
6. Choose a nickname you prefer.

NOTE:
It must be between 1 to 32 characters.

Valid characters: 【a-z A-Z 0-9】

“.” can’t be placed either in the beginning nor the end.

To manage PROMISE ID

You can manage your nickname or password by following the steps below:

1. Click **Edit PROMISE ID** to change your password and nickname.
2. Enter your new password or nickname.
3. Click **Confirm** to save changes.

To change ID

There are two ways to change ID: Log out or Change ID , you can click log out and change ID to erase the binding relationship between your Atlas S8+ and PROMISE Cloud ID.

NOTE:
If you are connecting through PROMISE Cloud DDNS service, log out or change ID will terminate the connection.

Business Applications

Antivirus

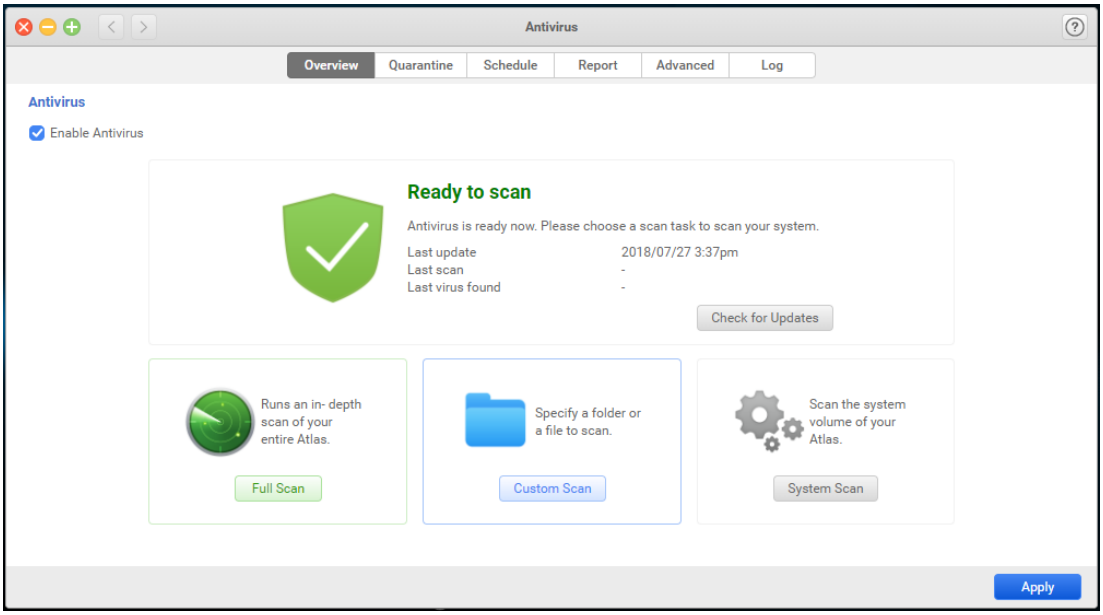
Antivirus is a full-featured security application which can protect your system. It will check the database update automatically and schedule a scan in the background.

Overview

You can check your current status, or prepare a scan for your Atlas S8+.

Requirement:

1. Please click the checkbox to enable Antivirus, then click **Apply** to confirm.
2. If you are using Antivirus for the first time, please click on **Check for Updates** on the **Overview** page, then select **Update Now** to download the virus database.
3. Make sure there are at least 512 MB of free storage space in your system volume before downloading virus database.
4. Check your network connection before downloading virus database.



Check the system status

The icon and the messages in the center of the page will display the current status of **Antivirus**. The status may appear as follows:

1. Inactive: Antivirus is disabled and cannot be used. If you would like to use this function, please click **Enable Antivirus** checkbox then click **Apply** button.
2. Ready to scan: Antivirus is ready, you can choose one of the scan tasks below and start to scan now.

NOTE
You can check if your database is the latest version by clicking Check for Updates button, then click **Update Now** button to update.

3. New version available: You can click **Update Now** button to get the latest version.

NOTE
This status will be shown if you disable automatic update. You can always change the update settings on Antivirus > Advanced page to ensure that your virus database is always the up- to-date version.

4. Checking network connections: It will be shown when downloading or updating the virus database.
5. Update failed: System pool abnormal: This is a system error message. If you see this status during the update process, please check if there is enough storage capacity on your system pool
6. Remote server error: This is a system error message. If you see this status, please check your network settings on **Control Panel** > **Network** > **Interface** or contact PROMISE support team for further information
7. Updating virus database: This status means the system is updating to the latest virus database now. Please note that the updates may fail if you disconnect the network connection on your system.
8. Scanning: The system is in the scanning process now. Please note that the process may fail if you disconnect the network connection on your system.
9. Protected: It will be shown after the scanning process if there are no viruses found on your system.
10. At risk: It will be shown when any viruses are found on your system. You can check

the infected file(s) on **Quarantine** page or on **Report** page to see more scanned results.

Scan your system

There are three types of scan: **Full Scan**, **Custom Scan** and **System Scan**. To scan your system, please follow these steps below:

1. Choose the scan type you would like to proceed:

   - Full scan: Scan all the data on your Atlas S8+, including your USB if mounted. It is recommended to select this option if you are not sure whether there are any potential threats on your Atlas S8+.
   - Custom scan: Only scan the selected folders or a specific folder on your Atlas S8+.

     ① Click **Custom Scan** button.
     ② Choose a folder you would like to scan.
     ③ Click **Confirm** button to scan.

   - System scan: To scan the system volume on the Atlas S8+.

2. If you want to stop scanning during the process, please click the Stop button.

NOTE:
1. The infected file(s) will be moved to Quarantine automatically and also shown on the Report page by default. If you only want to view the virus information on the Report page, please go to Antivirus > Advanced page for further settings.

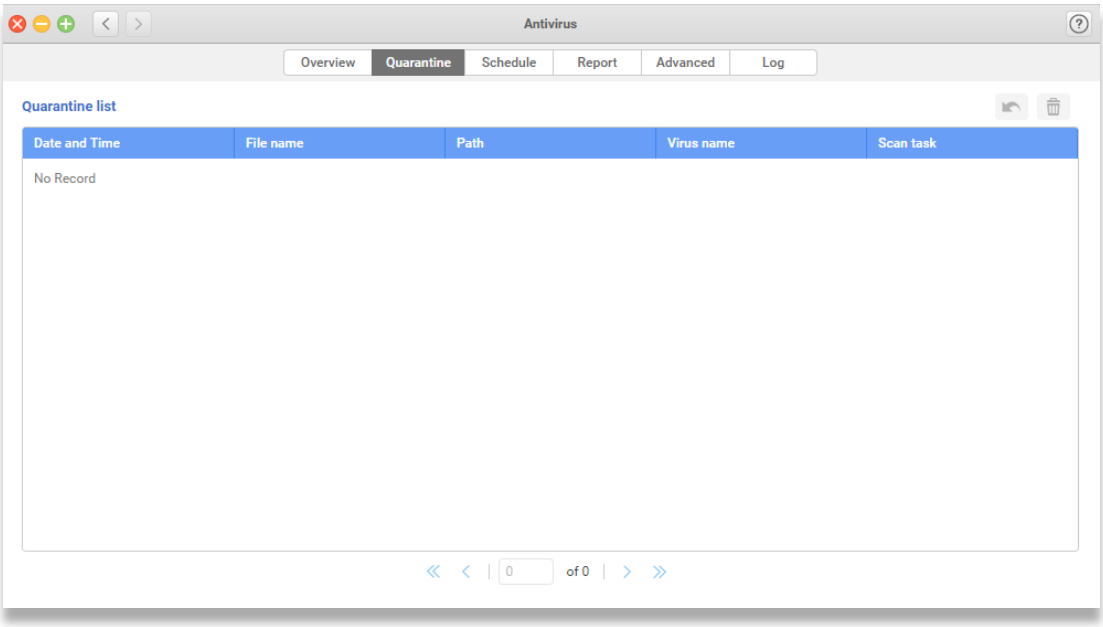
2. Remote folders (like CIFS/SMB, FTP, SFTP, WebDAV…etc.) mounted on your Atlas S8+ will not be scanned during full scan.

3. It is recommended not to scan files larger than 2048 MB or the system performance will be slightly influenced.

4. The probability of successfully finding viruses hidden in archive files (such as ZIP, RAR, ARJ, Tar, Gzip, Bzip2) will be slightly lower.

Quarantine

If the system has been infected, the target file(s) will be moved to **Quarantine**. You can check **Report** or **Log** page for more details.



Restore the infected file(s)

You can restore the infected files from quarantine. To restore, please follow these steps below:

1. Select the file(s) you would like to restore.
2. Click **Restore** button on the top right corner.
3. Click **Confirm** button and the file will be moved back to its originally location.

CAUTION:
Your system will be subject to potential threats if you restore the infected file(s) from the quarantine page. Please use this function carefully.

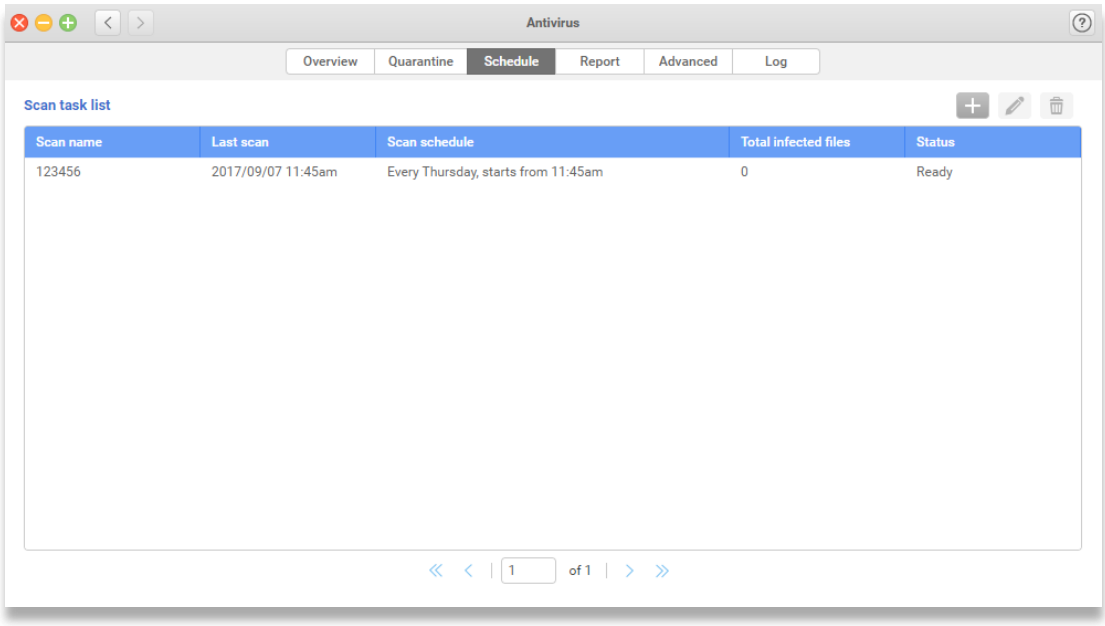
Delete the infected file(s)

To delete infected file(s), please follow these steps below:

1. Select the file(s) from the quarantine list.
2. Click **Delete** button.
3. Click **Confirm** button to proceed.

Schedule

Regularly scan your device can keep your Atlas S8+ safe. Your **Antivirus** gives you the possibility to schedule a scan at a time and frequency of your choice. You can define which folder(s) you would like to perform the scan regularly.



Add a scan task

To add a scan task to scan task list, please follow the steps below:

1. Click **Add** button on the top-right corner.
2. Enter your task name in **Scan task name** textbox.
3. Specified the folder(s) you would like to perform the scan on:
   - All folders:

     ① Select **All folders** button.
     ② Click **Next** button to set the scan frequency.

   - Specific folder(s):

     ① Select **Specific folder** button.
     ② Choose the folder(s) you would like to scan, then click **Add** button on the button-right corner.
     ③ Click **Next** button to set the scan frequency.
4. You can set the scan frequency as **Daily**, **Weekly**, **Monthly**, or **Repeat** in a period of the time. You can also set the start time for the task. Click **Confirm** to finish the setting.

NOTE:

1. The start time is based on the system time.
2. Only “one” task can be scanned at a time. If one scheduled task has started scanning, the second task will not start until the first task has finished.
3. Different status will be displayed on a scheduled task:
   - Ready: The task is ready and will start scanning at the set time.
   - Scanning: The task is on the scanning process.

Only “one” task can be scanned at a time. If one scheduled task has started scanning, the second task will not start until the first task has finished.

Edit a scan task

To edit a scan task, please follow the steps below:

1. Select the task you would like to edit from the Scan task list .
2. Click **Edit** button on the top-right corner.
3. Edit the folder(s) you would like to perform the scan on:
   - All folders:

     ① Select **All folders** button.
     ② Click **Next** button to edit the scan frequency..
   - Specific folder:

     ① Select **Specific folder** button.
     ② Choose the folder(s) you would like to scan, then click **Add** button on the button-right corner.
     ③ Click **Next** button to edit the scan frequency.
4. You can edit the scan frequency as **Daily**, **Weekly**, **Monthly** , or **Repeat** in a period of the time or the start time for the task. Click **Confirm** to finish the setting.

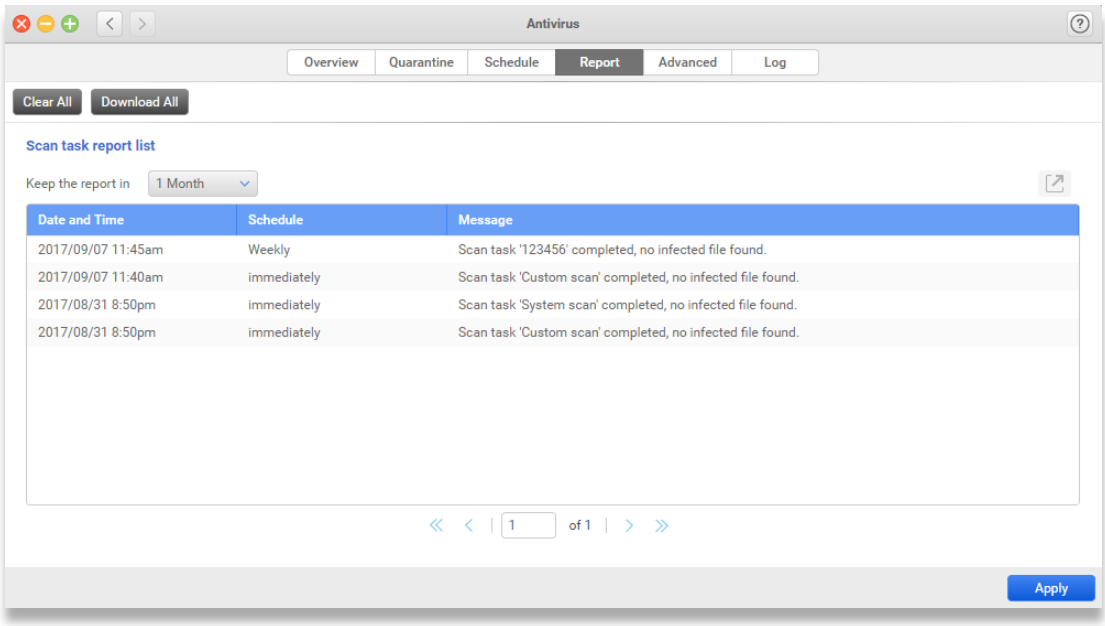
Delete a scan task

To delete a scan task from Scan task list , please follow the steps below:

5. Select the task you would like to delete.
6. Click **Delete** button on the top-right corner.
7. Click **Confirm** button to delete the task.

Report

You can view all the scan activities and results of your scan tasks on this page. You can keep the reports within a set period of time, and to download or delete them from your system.



Clear all reports

To clear all reports form the list, please follow the steps below:

1. Click **Clear All** button.
2. Click **Confirm** button to delete all reports.

Download all reports

To download all the reports, please follow the steps below:

1. Click **Download All** button.
2. Choose the location where you would like to store the reports, then click **Save**

button to download.

Keep the reports within a set time of your choice

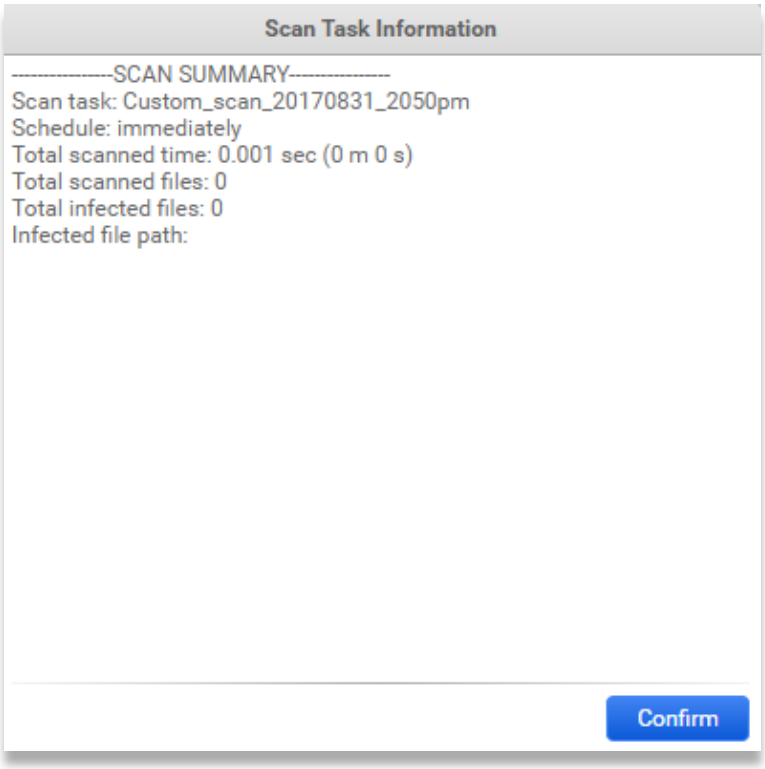
You can keep the reports within a certain period of time. To change the setting, please follow the steps below:

1. Select the number of days from the dropdown menu (10 Days/ 20 Days/ 1 Month/ 3 Month).
2. Click **Apply** button to save the setting.

View a scan report

You can open a scan task report to view its information. To view the scanned result, please follow the steps below:

1. Choose a scanned result on report list.
2. Click **Open** button on top-right corner of the list.
3. The following information will be displayed on the popup window:

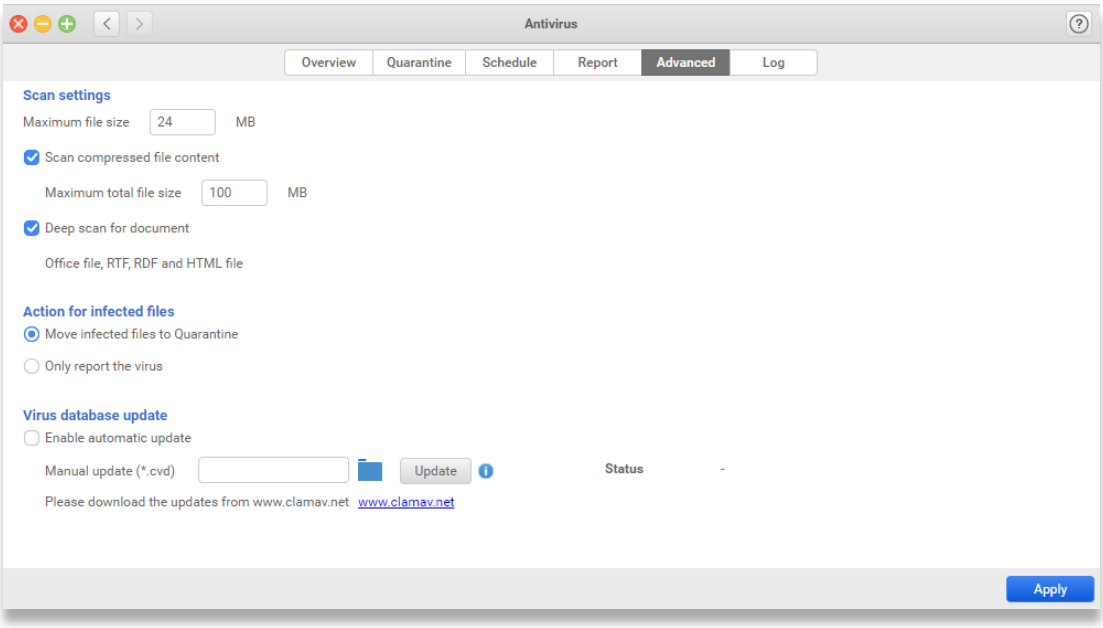


- Scan task: The task name and the date and time being scanned.
- Schedule: The scan frequency of the task.

- Total scanned time: The total amount of time spent on scanning.
- Total scanned files: The number of files being scanned.
- Total infected files: The number files being infected.
- Infected file path: The location of the viruses found on your system.

Advanced

You can change the settings of **Antivirus** application on this page.



Change the scan setting

You can change the maximum file size of which any files below this value will be scanned. There are also advance settings such as the following:

1. Scan compressed file content: If the checkbox is selected, compressed files will be scanned. Please note that the accumulative file size cannot exceed the maximum total file size which you have set, and only files smaller than the maximum file size will be scanned.
2. Deep scan for document: If the checkbox is selected, specific types of documents including office files, RTF, RDF and HTML files will be scanned in detail.

Choose an action when viruses are found

You can choose the action to proceed if infected file(s) are found on the system:

1. **Move infected files to Quarantine** : the files will be moved from its original location to Quarantine.

2. **Only report the virus: The result will be displayed on the Report** page.

   Once you have chosen the action, click **Apply** button to save the changes.

Update virus database

You can choose a method to update the virus database from the following:

1. Automatic update: The virus database will be updated twice a day at 12:00 a.m. and 12:00 p.m. automatically from websites. To enable automatic update, please follow the steps below:

   ① Click **Enable automatic update** checkbox.
   ② Click **Apply** button to save the settings.

2. Manual update: You can update the virus database manually by following the steps below:

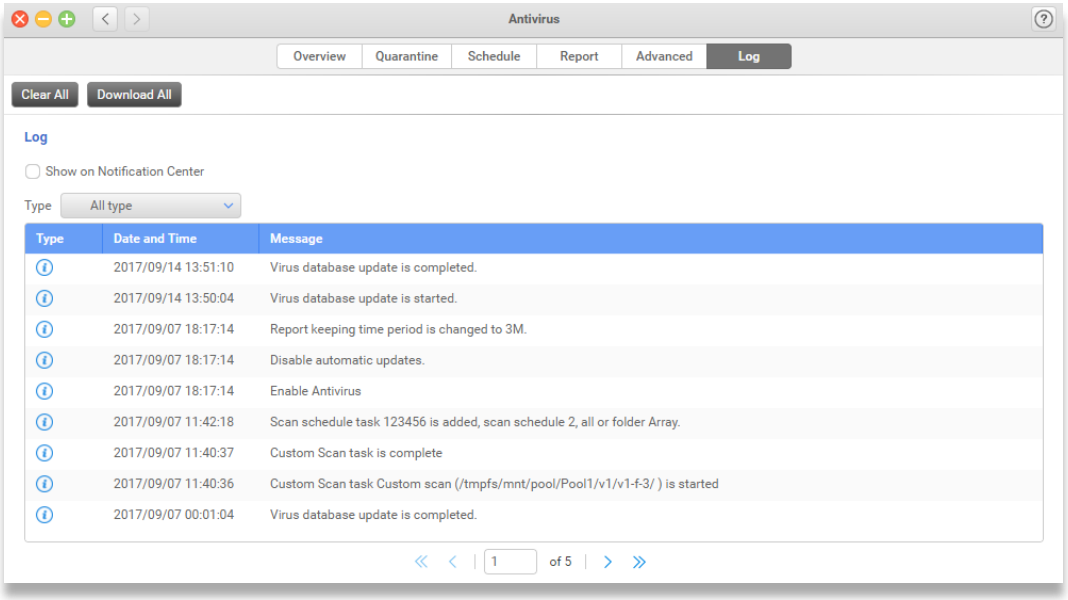
   ① Download all the files including “main.cvd”, “daily.cvd” and “bytecode.cvd” from www.clamav.net website.
   ② Choose those files from your local server and click **Update** button.
   ③ You can check the update status to see if the file has been uploaded successfully.

NOTE:

You cannot do a manual update until after you have disabled automatic update and clicked the Apply button.

Log

You can view different types of log related to **Antivirus** .



Clear all logs

To clear all the logs from your system, please follow the steps below:

1. Click **Clear All** button on the top of the page.
2. Click **Confirm** button to delete all logs.

Download all logs

To download all the logs from your system, please follow steps below:

1. Click **Download All** button on the top of the page.
2. Choose the destination where you would like to store the logs in, click **Save** button to download.

NOTE:

The downloaded file will be in .txt format, please open the file with software that supports .txt files.

Show logs in Notification Center

If you would like to display logs related to Antivirus in desktop > **Notification Center** , please select the **Show in Notification Center** checkbox.

NOTE

If you cannot view any Antivirus-related logs in the Notification Center, please go to Control Panel > Log > General Settings page to check if you have selected the application logs checkbox successfully.

View logs by type

There are three types of log: Information, Warning and Error. You can view the logs by its type by selecting from the drop-down menu, or select **All type** to view all logs.

NOTE:

The classification of different log types:

•Information: Important information which should be recorded at all times, for example service starting, stopping, completed or settings being changed.

•Warning: Anything which can potentially cause damage to the system, but can be recovered automatically by the system, including operation failed, user login failed or system temperature abnormal.

Conacting Technical And Resources

Getting Technical Support

PROMISE Technical Support provides several support options for PROMISE users to access information and updates. We encourage you to use one of our electronic services, which provide product information updates for the most efficient service and support.

PROMISE E-Support: https://support.promise.com

PROMISE web site: http://www.promise.com//

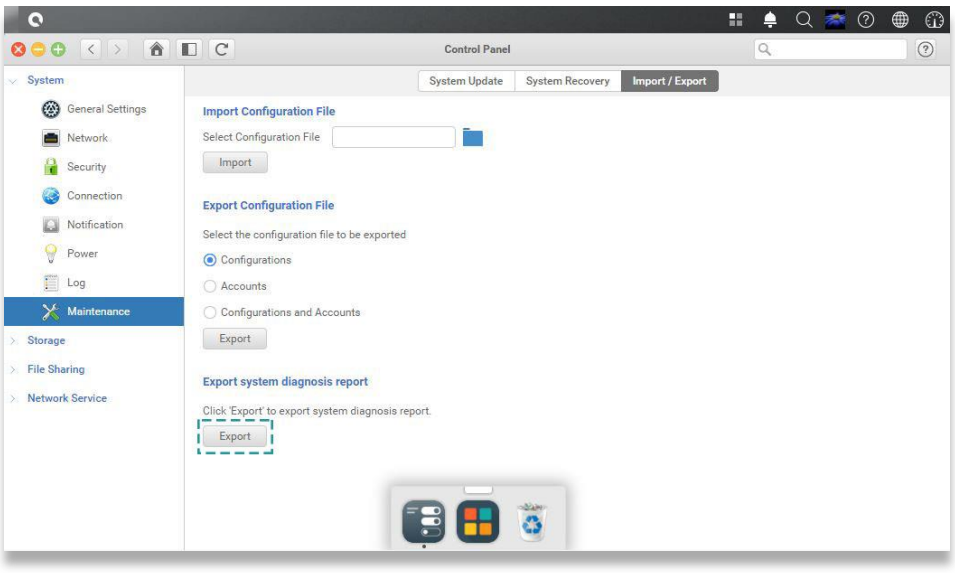
When you contact us, please have the following information available:

1. Firmware version
2. Error messages or screenshot images
3. Product-specific reports and logs
4. Add-on products or components installed
5. Third-party products or components installed

Information for Technical Support

The following system information is necessary for technical support, please refer to following for what and where to get the information of your Atlas S8+ model.

If the technical support requests you to download the service log, please navigate to the ASM UI → **Control Panel → System → Maintenance → Import/Export → Export system diagnosis report**, and then click the **Export** button.



Documentation Feedback

PROMISE is committed to providing documentation that meets and exceeds your expectations. To help us improve the documentation, email any errors, suggestions, or comments to https://support.promise.com

When submitting your feedback, including the document title, part number, revision, and publication date located on the front cover of the document.

Limited Warranty

PROMISE Technology, Inc. (“PROMISE”) warrants that this product, from the time of the delivery of the product to the original end user:

1. will conform to PROMISE’s specifications;
2. will be free from defects in material and workmanship under normal use and service.

This warranty:

1. applies only to products which are new and in cartons on the date of purchase;
2. is not transferable;
3. is valid only when accompanied by a copy of the original purchase invoice.
4. Is not valid on spare parts.

This warranty shall not apply to defects resulting from:

1. improper or inadequate maintenance, or unauthorized modification(s), performed by the end user;
2. operation outside the environmental specifications for the product;
3. accident, misuse, negligence, misapplication, abuse, natural or personal disaster, or maintenance by anyone other than a PROMISE or a PROMISE-authorized service center

Disclaimer of other warranties

This warranty covers only parts and labor, and excludes coverage on software items as expressly set above. Except as expressly set forth above, PROMISE disclaims any warranties, expressed or implied, by statute or otherwise, regarding the product, including, without limitation, any warranties for fitness for any purpose, quality, merchantability, non-infringement, or otherwise. PROMISE makes no warranty or representation concerning the suitability of any product for use with any other item. You assume full responsibility for selecting products and for ensuring that the products selected are compatible and appropriate for use with other goods with which they will be used.

PROMISE does not warrant that any product is free from errors or that it will interface without problems with your computer system. It is your responsibility to back up or otherwise save important data before installing any product and continue to back up your important data regularly. No other document, statement or representation may be relied on to vary the terms of this limited warranty. PROMISE's sole responsibility with respect to any product is to do one of the following:

1. replace the product with a conforming unit of the same or superior product;
2. repair the product.

PROMISE shall not be liable for the cost of procuring substitute goods, services, lost profits, unrealized savings, equipment damage, costs of recovering, reprogramming, or reproducing of programs or data stored in or used with the products, or for any other general, special, consequential, indirect, incidental, or punitive damages, whether in contract, tort, or otherwise, notwithstanding the failure of the essential purpose of the foregoing remedy and regardless of whether PROMISE has been advised of the possibility of such damages. PROMISE is not an insurer. If you desire insurance against such damage, you must obtain insurance from another party.

Some states do not allow the exclusion or limitation of incidental or consequential damages for consumer products, so the above limitation may not apply to you.

This warranty gives specific legal rights, and you may also have other rights that vary from state to state. This limited warranty is governed by the State of California.

Your Responsibilities

You are responsible for determining whether the product is appropriate for your use and will interface with your equipment without malfunction or damage. You are also responsible for backing up your data before installing any product and for regularly backing up your data after installing the product. PROMISE is not liable for any damage to equipment or data loss resulting from the use of any product.

Returning the Product For Repair

If you suspect a product is not working properly, or if you have any questions about your product, contact our Technical Support staff, and be ready to provide the following information:

1. Product model and serial number (required)
2. Return shipping address
3. Daytime phone number
4. Description of the problem

5. Copy of the original purchase invoice

The technician helps you determine whether the product requires repair. If the product needs repair, the technician issues an RMA (Return Merchandise Authorization) number.

Important Obtain an RMA number from Technical Support before you return the product and write the RMA number on the label. The RMA number is essential for tracking your product and providing the proper service.

Return ONLY the specific product covered by the warranty. Do not ship cables, manuals, CDs, etc.

USA and Canada:

PROMISE Technology, Inc. Customer Service Dept. Attn.: RMA # _____ 3241 Keller Street Santa Clara CA 95054

Other Countries:

Return the product to your dealer or retailer. Contact them for instructions before shipping the product.

You must follow the packaging guidelines for returning products:

1. Use the original shipping carton and packaging
2. Include a summary of the product's problem(s)
3. Write an attention line on the box with the RMA number
4. Include a copy of your proof of purchase

You are responsible for the cost of insurance and shipment of the product to PROMISE. Note that damage incurred due to improper transport or packaging is not covered under the Limited Warranty.

When repairing returned product(s), PROMISE may replace defective parts with new or reconditioned parts, or replace the entire unit with a new or reconditioned unit. In the event of a replacement, the replacement unit is under warranty for the remainder of the original warranty term from purchase date, or 30 days, whichever is longer.

PROMISE pays for standard return shipping charges only. You must pay for any additional shipping options, such as express shipping.

United States

580 Cottonwood Drive Milpitas, Ca 95035, USA
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Australia

Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

EMEA

Netherlands

Science Park Eindhoven 5228 5692 EG Son, The Netherlands
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Austria

Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

France

Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Germany

Europaplatz 9 44269 Dortmund, Germany
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Sweden

Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Switzerland ITF

Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Norway ITF
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Belgium
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Luxembourg
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

United Kingdom
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Taiwan
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

China
China Room 1108, West Wing, Shi Chuang Plaza, 22 Information Road Shangdi IT Park, Haidian District, Beijing 100085
Fax: 86-10-8857-8015
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Korea
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Hong Kong
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Singapore

Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//

Japan

3F, Mura Matsu Bldg, 3-8-5, Hongo Bunkyo-ku Tokyo 113-0033, Japan
Technical Support (E-Support): https://support.promise.com
Web site: http://www.promise.com//