



VIKINGTM
Enterprise Solutions

ONYX Series

VESq Software Guide

May 2023
Document CTC-DOC-003004, Rev1

Copyright

©2023 Viking Enterprise SolutionsTM All rights reserved.

Viking Enterprise Solutions has made every effort to ensure that the information contained in this document is accurate and reliable, but assumes no responsibility for errors or omissions. Information in this document is subject to change without notice.

This document contains copyrighted and proprietary information, which is protected by United States copyright laws and international treaty provisions.

No part of the document may be reproduced or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without express written permission from Viking Enterprise Solution.

Acknowledgments

Viking Enterprise Solutions and its logo are trademarks of Viking Enterprise Solutions™, which is a Sanmina Corporation company. All other trademarks are the properties of their respective owners.

Intel® and Xeon® are trademarks of Intel Corporation in the U.S. and/or other countries.

Phillips® is a registered trademark of Phillips Screw Company Corporation of Burlington, MA.

Notices

The information contained in this manual has been reviewed for accuracy. It may include typographical errors or technical inaccuracies. Changes are made to the document periodically. These changes will be incorporated in new editions of the publication. Viking Enterprise Solutions (VES) may make improvements or changes in the products. All features, functionality, and product specifications are subject to change without prior notice or obligation. All statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurements may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products.

All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Applicable Models

This manual is applicable to all ONYX series models.

Regulatory Statements

VES ONYX Series complies with different FCC/CE/VCCI/KCC compliance classes. Please refer to the classification and the corresponding statement below.

CE Class A Statement

This device has been shown to be in compliance with and was tested in accordance with the measurement procedures specified in the Standards and Specifications listed below.

Technical Standard: EMC DIRECTIVE 2014/30/EU

Class A (EN55032 /
EN55024)

CE Class B Statement

This device has been shown to be in compliance with and was tested in accordance with the measurement procedures specified in the Standards and Specifications listed below.

Technical Standard: EMC DIRECTIVE 2014/30/EU

Class B (EN55032 /
EN55024)

FCC Class A Statement

This device complies with Part 15 of the FCC Rules. The Operation is subject to the following two conditions:

1. This device may not cause harmful interference.
2. This device must accept any interference received, including interference that may cause undesired operation.

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and uses in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equivalent.

FCC Class B Statement

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

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

Notice: The changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equivalent.

VCCI Class A Statement

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

VCCI-A

VCCI Class B Statement

この装置は、クラス B 情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

取扱説明書に従って正しい取り扱いをして下さい。

VCCI - B

KCC Class A Statement*

A 급 기기 (업무용 방송통신기자재)

이 기기는 업무용 (A 급) 전자파적합기기로서 판매자 또는 사용자는 이 점을 주의 하시기
바라며, 가정 외의 지역에서 사용하는 것을 목적으로 합니다.

(This equipment has approved for EMC on purpose of business use and there is possible
for radio interference for home use.)

KCC Class B Statement*

B 급 기기 (가정용 방송통신기자재)

이 기기는 가정용 (B 급) 전자파적합기기로서 주로 가정에서 사용하는 것을 목적으로 하며,
모 든 지역에서 사용할 수 있습니다.

*KCC statement is only applicable for certain ONYX Series models. Please refer to the
product page on <https://www.vikingenterprisesolutions.com/onyx> for further information.

Safety Warnings

1. The ONYX Series can operate normally in the temperature of 0°C~40°C (31.99 ~ 103.99°F). Please make sure the environment is well-ventilated.
2. The power cord and devices connected to the ONYX Series must provide a correct supply voltage.
3. Do not place the ONYX Series in direct sunlight or near chemicals. Make sure the temperature and humidity of the environment are in the optimized level.
4. Place the product right side up at all times.
5. Unplug the power cord and all connected cables before cleaning. Wipe the ONYX Series with a dry towel. Do not use chemical or aerosol to clean the NAS.
6. Do not place any objects on the ONYX Series for the server's normal operation and to avoid overheat.
7. Use the screws provided in the product package to lock the hard disks in the ONYX Series when installing hard disks for proper operation.
8. Do not place the ONYX Series near any liquid.
9. Do not place the ONYX Series on any uneven surface to avoid falling off and damage.
10. Do no place the ONYX Series on the ground and do not step on the system to prevent any potential damages.
11. Make sure the voltage is correct in the location where the ONYX Series is installed. Contact the distributor or the local power supply company for the information.
12. Do not place any object on the power cord.

13. Do not attempt to repair the ONYX Series in any occasions. Improper disassembly of the product may expose the users to electric shock or other risks. For any inquiries, please contact the distributor.
14. Do not touch the fan inside the system to avoid serious injuries.
15. To remove all electrical current from the device, ensure that all power cords are disconnected from the power source.
16. The ONYX series should only be installed in restricted access location such as in the server room and maintained by the qualified service person. The server room is locked by key or keycard, or other means of security access and only a qualified service person is allowed to enter the server room.



CAUTION: (English)

Replacing incorrect type of battery will have the risk of explosion. Please replace the same or equivalent type battery use and dispose of used batteries appropriately.



INFORMATION:

VES provides a limited warranty for VES-branded hardware and peripheral product(s):

3 years limited warranty from date of original purchase.

Table of Contents

- Copyright 1
- Acknowledgments 2
- Notices 2
- Regulatory Statements 3
- Safety Warnings 5
- Preface 10
- About This Manual 10
- Related Documents 10
- Technical Support 10
- Information, Tip and Caution 10
- 1.0 Getting Started 11
 - 1.2. ONYX Series System Discovery 17
- 2.0 VESq Basics and Desktop 20
 - 2.1. About NAS 21
 - 2.3. Preference 22
 - 2.4. Desktop 25
 - 2.5. Monitor 31
 - 2.5.1. Resource 31
 - 2.5.2. Hardware 35
 - 2.5.3. Service 36
 - 2.5.4. Network 37
- 3.0 Control Panel 38
 - 3.1. System 38
 - 3.1.1. General Setting 38
 - 3.1.2. Network 42
 - 3.1.3. Security 50
 - 3.1.4. Connection 56
 - 3.1.5. Notification 59
 - 3.1.6. Power 65
 - 3.1.7. Log 68
 - 3.1.8. Maintenance 76
 - 3.2. Storage 81
 - 3.2.1. Overview 81
 - 3.2.2. Disk 83

- 3.2.3. Pool88
- 3.2.4. Volume.....97
- 3.2.5. Virtual Volume99
- 3.2.6. Block Storage102
- 3.2.7. SSD Cache110
- 3.2.8. Deduplication.....111
- 3.2.9. Performance Tuning.....113
- 3.3. File Sharing 114
 - 3.3.1. User.....114
 - 3.3.2. Group.....118
 - 3.3.3. Domain Security.....120
 - 3.3.4. Folder.....122
- 3.4. Network Service 135
 - 3.4.1. Service Binding135
 - 3.4.2. File Service136
 - 3.4.3. Bonjour143
 - 3.4.4. TimeMachine144
- 4.0 Backup..... 147
 - 4.2. Remote Backup 154
 - 4.3. Cloud Backup 159
 - 4.4. XMirror.....162
 - 4.5. USB Backup167
 - 4.6. Log.....170
- 5.0 File Manager.....172
 - 5.1. File Manager.....172
 - 5.2. Media Library Management178
 - 5.2.1. Media Library.....178
 - 5.2.2. Log179
- 6.0 VES Cloud Applications 180
 - 6.1. Cloud Sync180
- 7.0 Business Applications187
 - 7.1. Antivirus187
- 8.0 Support and Other Resources199
 - 8.1. Getting Technical Support.....199
 - 8.2. Documentation Feedback200

Appendix201
End-User License Agreement (EULA)201
Miscellaneous203

Preface

About This Manual

This manual provides technical guidance for how to setup VESq 3.0 with your ONYX Series, and it is intended for use by system administrators, storage consultants, or anyone who has purchased this product and is familiar with server and computer network, network administration, storage system installation and configuration, network attached storage management and relevant protocols.

Related Documents

There are related documents which can be downloaded from the website.

<https://www.vikingenterprisesolutions.com/onyx-series/>

Technical Support

Do you have any questions or need help troubleshooting a problem? Please contact VES Support, we will reply to you as soon as possible.

- Via the Web: <https://vikingenterprisesolutions.atlassian.net/servicedesk/customer/portal/6>
- Via Email: customersupport@vikingenterprise.com

Information, Tip and Caution

This manual uses the following symbols to draw attention to important safety and operational information.

**INFORMATION:**

INFORMATION provides useful knowledge, definition, or terminology for reference.

**TIP:**

TIP provides helpful suggestions for performing tasks more effectively.

**CAUTION:**

CAUTION indicates that failure to take a specified action could result in damage to the system.

1.0 Getting Started

Thank you for purchasing VES ONYX Series. The new users are advised to follow the steps below to complete the system installation.

1.1. Hardware Installation

After unpacking your ONYX Series, please refer to the following steps to install the ONYX Series system hardware:

1.1.1. Installing Disk Drive(s)

The detail instruction is illustrated in the Hardware Guide and the Quick Installation Guide (QIG). Both documents can be found on VES website

<https://www.vikingenterprisesolutions.com/support/> and the QIG can be found in the product package.

**CAUTION:**

If you are installing a used disk drive on the ONYX Series which contains other data, the data may be damaged or cleared during the installation or in future usage. Please make sure you back up the data before starting the installation.

**TIP:**

If you would like to maximize volume space with RAID being set, we recommend that all your installed drives be the same size.

1.1.2. Power On Your ONYX Series

Please follow the steps below to power on your ONYX Series system:

1. Connect at least one LAN cable to one of the LAN ports on your ONYX Series and the other end to your switch, router, or hub.
2. Connect the expansion mini-SAS HD and power cables
3. Connect your ONYX Series to the power and press the power button to start the installation process.
4. Checking the system status LEDs to make sure your ONYX Series is function properly.

System Status LED Indication


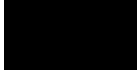
Description	Definition
USB One Touch Copy Button/ USB Status LED	<p>USB Copy Button</p> <ul style="list-style-type: none"> ▪ Press the button one time to start the action defined through UI <p>(Note: USB one touch copy function needs to be enabled through UI first)</p> <p>USB Status LED</p> <p>Blue: A front USB device is detected (after the device is mounted).</p> <p>Blue flashes every 0.5 sec:</p> <ol style="list-style-type: none"> 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. <p>OFF: No USB device is mounted.</p>
Solid State Drive (SSD) LED	<p>Blue: The hard disk is attached.</p> <p>Blue flashes: The disk data is being accessed.</p> <p>Amber: A hard drive read/write error occurs.</p> <p>Blue and Amber flashes alternatively: The hard disk is being rebuilt or identify a specific disk drive.</p> <p>OFF: No disk drive is inserted.</p>
Power Button/LED	<p>Power Button</p> <p>Press the button one time to turn ON or OFF the system power.</p> <p>Power LED</p> <p>White : power is ON.</p> <p>White flashes every 0.5 sec: the system is at the stage of starting up or shutting down, or the NAS is not configured.</p> <p>Amber:</p> <ol style="list-style-type: none"> 1) The system pool has reached its full capacity (100%). 2) The system pool is going to be full (95%).

	<p>3) The system fan is out of function.</p> <p>4) A bad sector is detected on the hard disk drive or hard disk failed.</p> <p>5) One of the pools is in degraded read-only mode.</p>
--	---

	<p>6) Hardware self-test error. e.g. abnormal voltage, the temperature is at critical high/low, any cooling fan module failed; any pool failed.</p> <p>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.</p> <p>Off: the system shutdown.</p>
LAN Status LED	<p>Blue: The NAS is connected to the network.</p> <p>Blue flashes: The disk data is being accessed from the network.</p>
Expansion Unit Status LED	<p>Blue: An expansion card is being accessed.</p> <p>OFF: No expansion card is being accessed.</p>
Disk Drive Status LED	<p>Blue: The hard disk is attached.</p> <p>Blue flashes: The disk data is being accessed.</p> <p>Amber: A hard drive read/write error occurs.</p> <p>Blue and Amber flashes alternatively: The hard disk is being rebuilt or identify a specific disk drive.</p> <p>OFF: No disk drive is inserted.</p>
LAN Port	<p>Activity/Link:</p> <p>Light OFF: No connection.</p> <p>Light ON: Connected to the internet</p> <p>Light flashes: when data is being accessed.</p> <p>Speed:</p> <p>Light OFF: Speed less than 10Mbps</p> <p>Light ON: Connected to the internet</p>

- System Status LED Indication

For ONYX Series XN5000R and XN8000R series.

Description	Definition
Enclosure Power Button/LED	<p>Power Button Press the button one time to turn ON or OFF the system power. Keep pressing for 4 seconds to force turn OFF the system power.</p> <p>Power LED  power is ON (at least one power supply unit is supplying power to the system).  flashes every 0.5 sec: the system is at the stage of starting up or shutting down, or the NAS is not configured. Off: the system is shutdown.</p>
Unit Identification (UID) Button/LED (front panel)	<p>UID (Unique Identity) button Press the button one time to turn it ON; press it again to turn it OFF.</p> <p>UID (Unique Identity) LED Blue: the system has been identified. Off: the system has not been identified.</p>
Enclosure Access LED	<p>(Indicate the host interface connectivity.) Blue flashes: the host interface activity is on-going. Off: no host interface activity.</p>
Enclosure Status LED	<p>(Indicate current health status of the system.) Amber: 1) The storage folder/pool has reached its full capacity (100%). 2) The storage folder/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. 5) One of the pool is in degraded read-only 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. Amber flashes every 0.5 sec: firmware is upgrading, or RAID rebuilding is in a process. Off: the system is healthy.</p>
Disk Drive Power LED	<p>Blue: the disk drive is inserted and no data access. Blue flashes: the disk data is being accessed. Blue flashes (interval of 0.5 sec): The hard disk is rebuilding or identify a specific disk drive. Off: no disk drive is inserted.</p>

Disk Drive Status LED	<p>Off: the disk drive is healthy.</p> <p>Amber: the disk drive is error.</p> <p>Amber flashes (interval of 0.5 sec): the disk drive is rebuilding or identify a specific disk drive.</p>
LAN Port	<p>Activity/Link:</p> <p>Light OFF: No connection.</p> <p>Light ON: Connected to the internet</p> <p>Light flashes: when data is being accessed.</p> <p>Speed:</p> <p>Light OFF: Speed less than 10Mbps</p> <p>Light ON: Connected to the internet</p>
Unit Identification (UID) LED (rear panel)	<p>Blue: the system has been identified.</p> <p>Off: the system has not been identified.</p>
PCIe Solid State Drive (SSD) System LED	<p>Blue: The SSD is attached.</p> <p>Blue flashes: The disk data is being accessed.</p> <p>Amber: A hard drive read/write error occurs.</p> <p>Blue and Amber flashes alternatively: The hard disk is being rebuilt or identify a specific disk drive.</p>
SATA Solid State Drive (SSD) System LED	<p>Blue: The SSD is attached.</p> <p>Blue flashes: The disk data is being accessed.</p> <p>Amber: A hard drive read/write error occurs.</p> <p>Blue and Amber flashes alternatively: The hard disk is being rebuilt or identify a specific disk drive.</p>
PSU LED	<p>OFF: No AC power to power supplies / AC present (only 5VSB on, PS off).</p> <p>Green: PSU is on and OK.</p> <p>Amber: Power supply failure for main output.</p>

4. Checking the system alarm buzzer to make sure your ONYX Series is function properly.

- System Alarm Buzzer Indication

No.	Beep Sound	No. of Times	Description
1	Short beep (0.5 sec)	1	<ul style="list-style-type: none"> • The ONYX Series is ready (finish start up). • The ONYX Series is being shut down (software shutdown). • The system firmware has been updated. • Front USB start copy [Note 3] • Front USB finish copy [Note 3] • USB drive is removed • The user starts hard drive rebuilding.
2	Short beep (0.5 sec)	3 times, interval of 0.5 sec	<ul style="list-style-type: none"> • 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	<ol style="list-style-type: none"> 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. degraded mode. 7) 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. 8) 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 VESQ. You can check the error messages through the **Notification Center** on VESQ.

Note 3: For ONYX series.

1.2. ONYX Series System Discovery

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

1. Power on the ONYX Series.
2. Access the ONYX Series storage management GUI using the below interfaces:

A. Ethernet Management port

The default setting for the management IP address is DHCP. Check the DHCP server for the ONYX Series leased IP address and you can go directly to the ONYX Series storage management interface using a web browser e.g. <http://192.168.1.x>.

Note: If the LAN doesn't have a DHCP server, the management port will be assigned a fix IP address: 169.254.1.234/16. So, you can configure the IP address of your management computer to the same subnet domain of the storage system, e.g.: 169.254.1.1/16. Then open a browser and enter <http://169.254.1.234> to go into the login page.

B. Serial Port – Access the ONYX Series system directly from a computer using the provided RS-232C serial cable

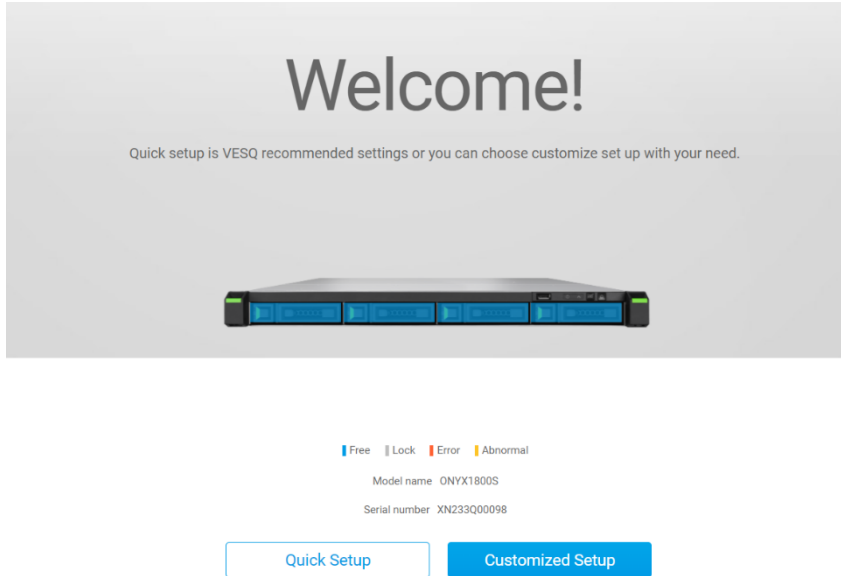
- a) Connect your computer to the ONYX Series system using the provided RS-232C serial port cable
- b) Launch a VT-100 terminal emulation application on your computer
- c) Configure the serial port as (8-N-1-115200)
- d) Login as admin/1234
- e) Enter "info" to see the ONYX Series storage management IP address(es)

```

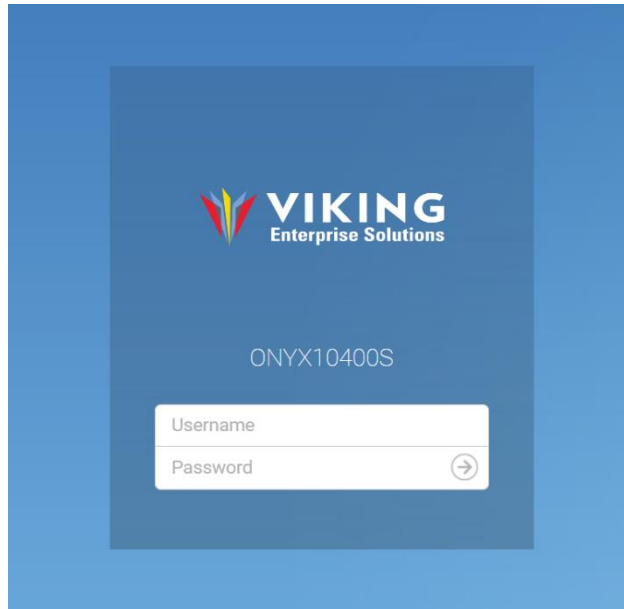
ONYX1800S login: admin
Password:
console> info
[System]
Product: ONYX1800S
Name: ONYX1800S
Version: 3.4.2 (build 202303291539)
Vendor: VESQ
[Network]
LAN1 => MAC: 00:A0:C9:00:00:00 IP: 172.30.12.165 Mask: 255.255.0.0
LAN2 => MAC: 00:A0:C9:00:00:00 IP: 169.254.1.235 Mask: 255.255.0.0
LAN3 => MAC: 00:A0:C9:00:00:00 IP: 169.254.1.236 Mask: 255.255.0.0
LAN4 => MAC: 00:A0:C9:00:00:00 IP: 169.254.1.237 Mask: 255.255.0.0
LAN5 => MAC: 00:00:00:00:01:03 IP: 172.30.12.118 Mask: 255.255.0.0
LAN6 => MAC: 00:00:00:00:01:02 IP: 169.254.1.239 Mask: 255.255.0.0
LAN7 => MAC: 00:00:00:00:01:01 IP: 169.254.1.240 Mask: 255.255.0.0
LAN8 => MAC: 00:00:00:00:01:00 IP: 169.254.1.241 Mask: 255.255.0.0
console>

```

3. Launch your web browser and point to the ONYX Series management IP address and the ONYX Series welcome wizard will launch



4. Click **Quick Setup** or **Custom Setup** to start the setup process and follow the onscreen instructions.
5. 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.
6. After quick setup is finished, login to the VESQ as “**admin**” (default account name) with the password you set on former instructions.





INFORMATION:

1. Both the ONYX Series and your PC must be on the same local network.
 2. If you cannot find your ONYX Series, the default IP address for LAN 1 is 169.254.1.234.
-

2.0 VESq Basics and Desktop

ONYX Series Storage Manager 3.0 (VESq 3.0) is an innovative storage operating system designed for VES ONYX series. Based on Linux and 128-bit ZFS, VESQ 3.0 not only inherits the amazing native features of ZFS but is also adjusted with several bespoke optimization enhancements that make the ONYX series a high-performance, efficient and superior network attached storage device.

VESQ 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.

VESQ 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 ONYX Series capable of storing beyond its raw storage capacity.

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

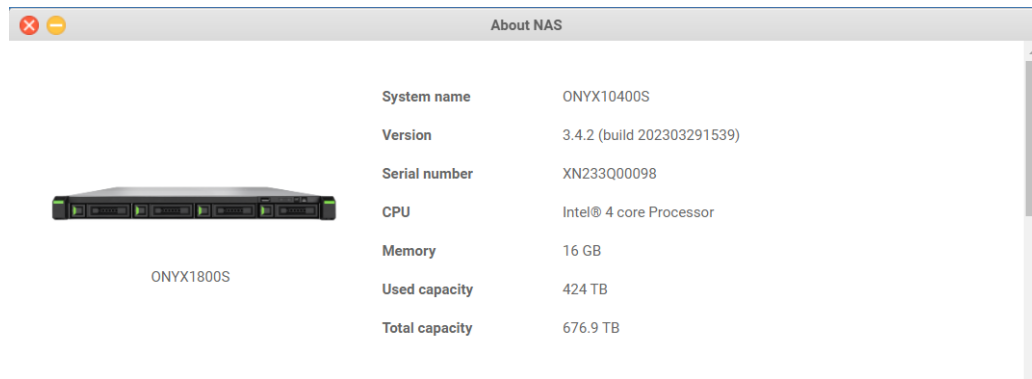
Value-added functionality's such as virtualization capability, multiple server center, centralized file station etc. are also provided making VESQ 3.0 robust and able to carry out dedicated applications.



In this manual, we will be introducing every feature of the VESQ 3.0. Once you have finished the basic setup and login to your ONYX Series, please check the topics below to learn more about VESQ 3.0.

2.1. About NAS

About NAS contains basic information about your ONYX Series, including firmware version, hardware information and your storage usage.



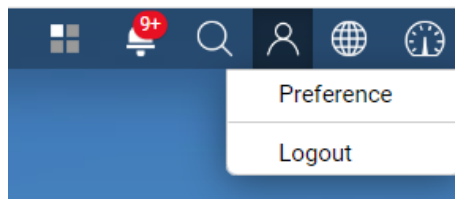
Checking information about you ONYX Series

Please follow the steps below to check the information of your ONYX Series:

1. Click the VES icon on the upper-left corner on VESQ 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 VESQ version.
 - **Serial number** : A unique, identifying number for your ONYX Series.
 - **CPU** : CPU specification for your ONYX Series.
 - **Memory** : Total memory capacity.
 - **Used capacity** : Current system capacity usage.
 - **Total capacity** : Total system capacity available.

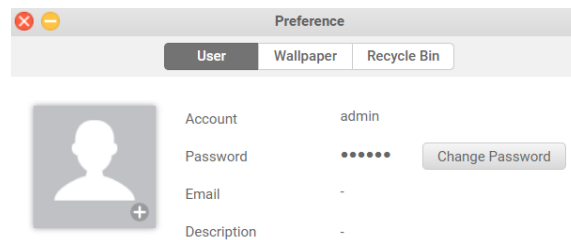
2.3. Preference

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.



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.

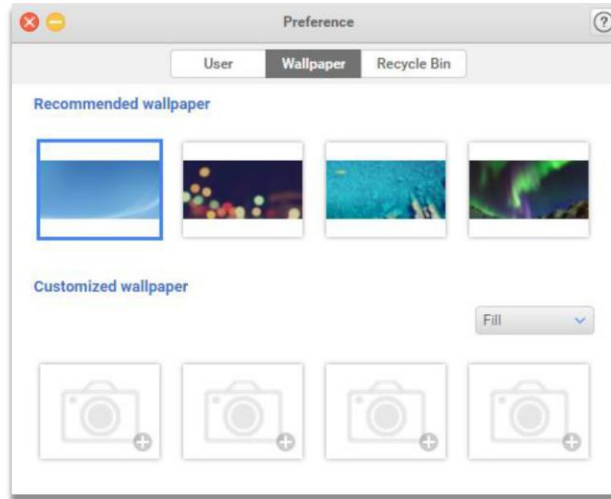


INFORMATION:

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.

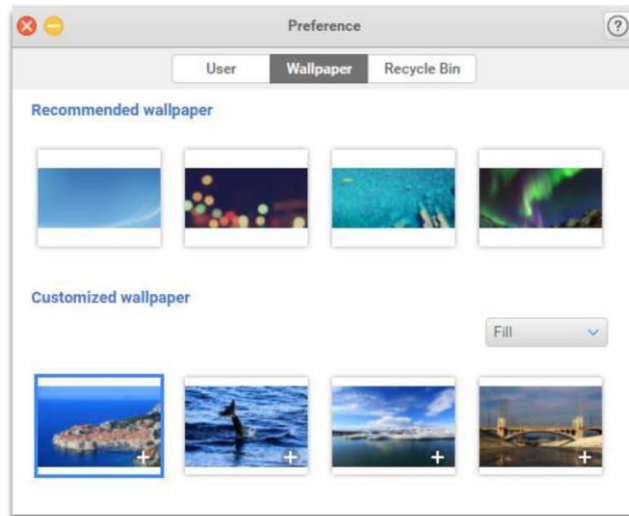


Change the background of your desktop:

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

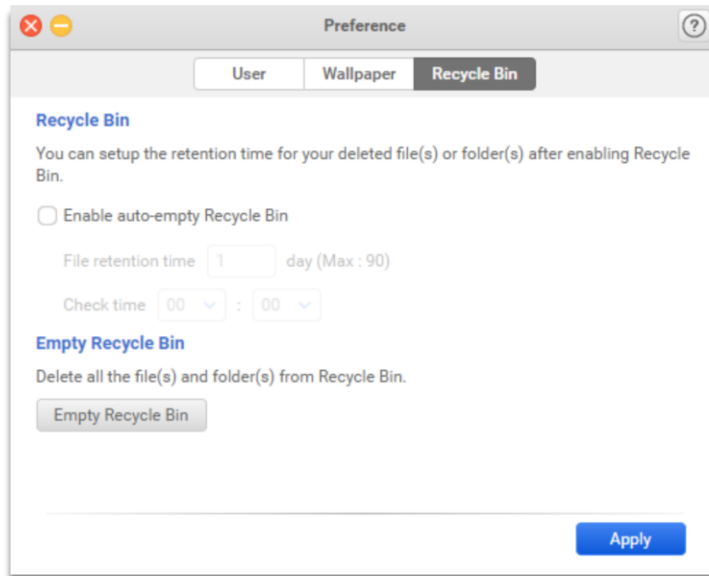
Upload a customized image that will be used as your desktop background:

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.

2.4. Desktop

VESQ'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. VES logo menu:

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

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

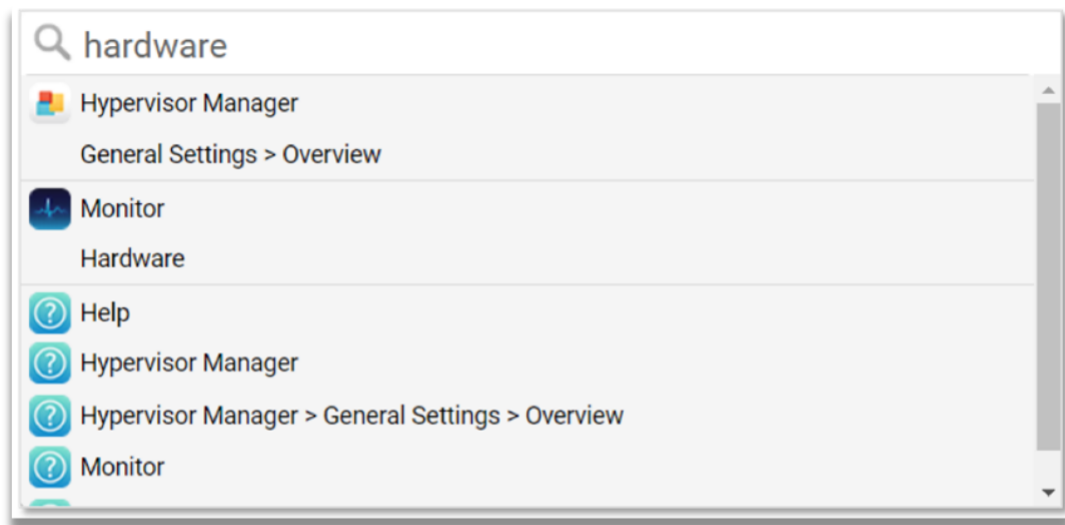
Apps : Contains all the applications in an area.

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

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

Shutdown: For admin, they can decide whether to shut down the VESQ 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.

**INFORMATION:**

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

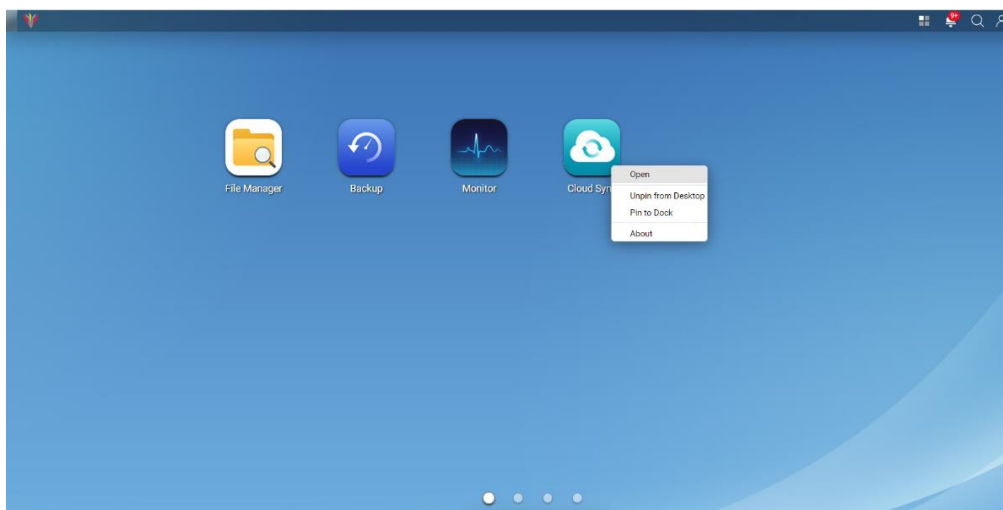
6. **Person-shaped icon:** Logout or modify your account, wallpaper and empty recycle bin.
7. **Language:** Choose your prefer language for the VESQ user interface. If you change the language successfully, the display language will be replaced immediately without having to log in VESQ again.
8. **Dashboard:** 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:



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.

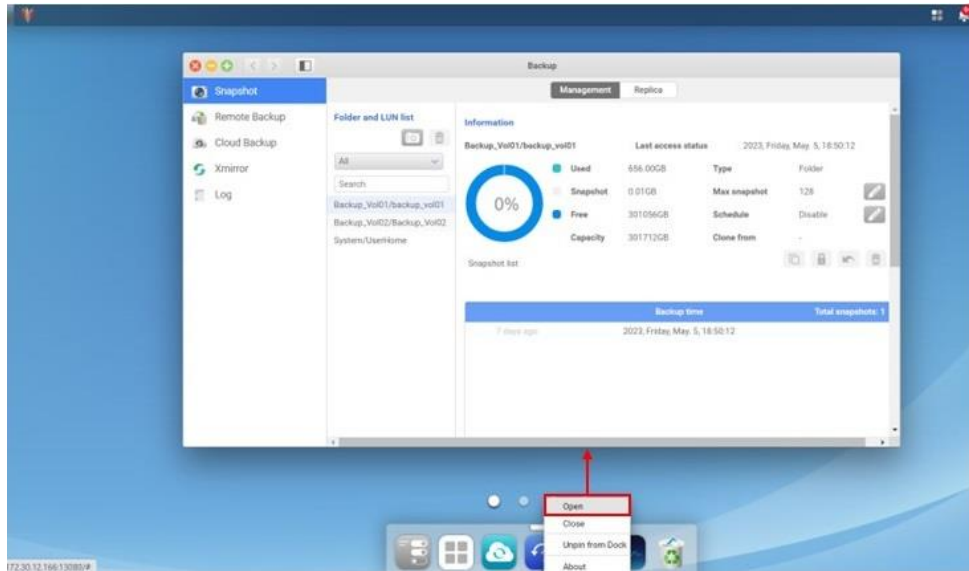
Dock

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.



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".

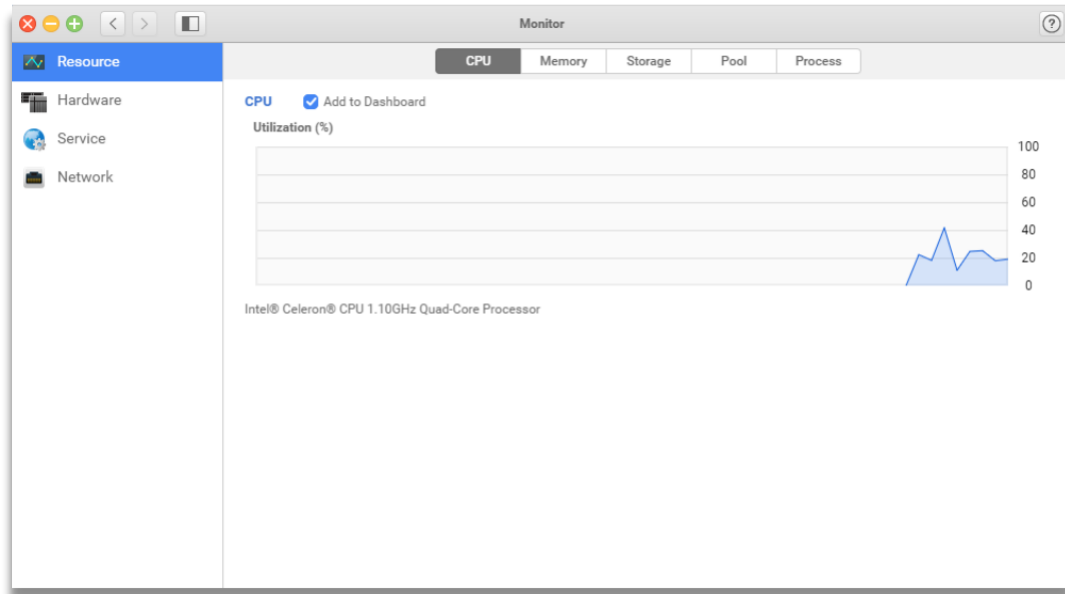
2.5. Monitor

2.5.1. Resource

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

CPU

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 Monitor is first launched, because the system needs to collect its resource data and load the UI page at the same time.

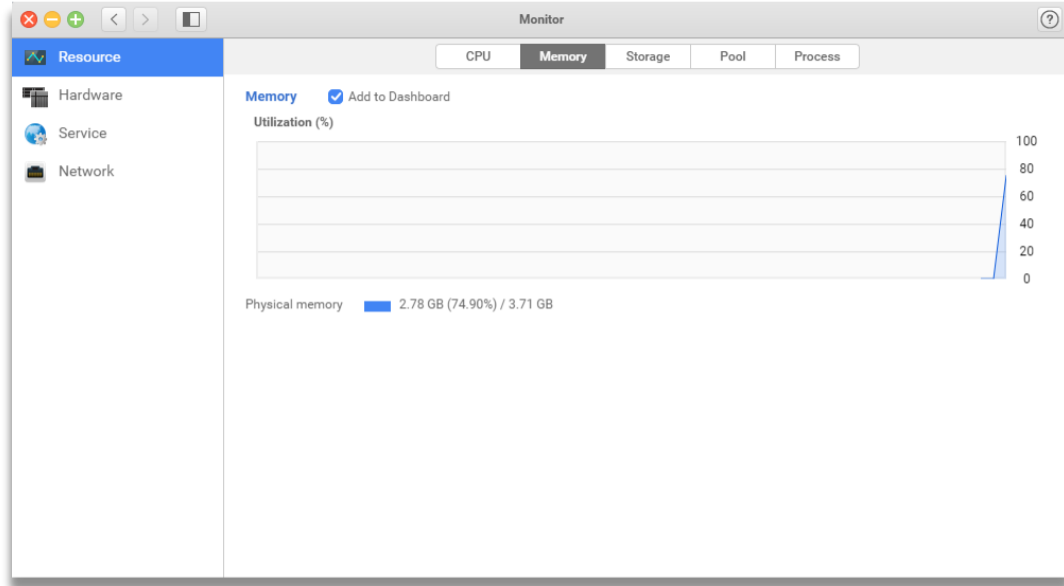


To show on Dashboard

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

Memory

This page shows the overall physical and expansion memory usage on your ONYX Series. 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.

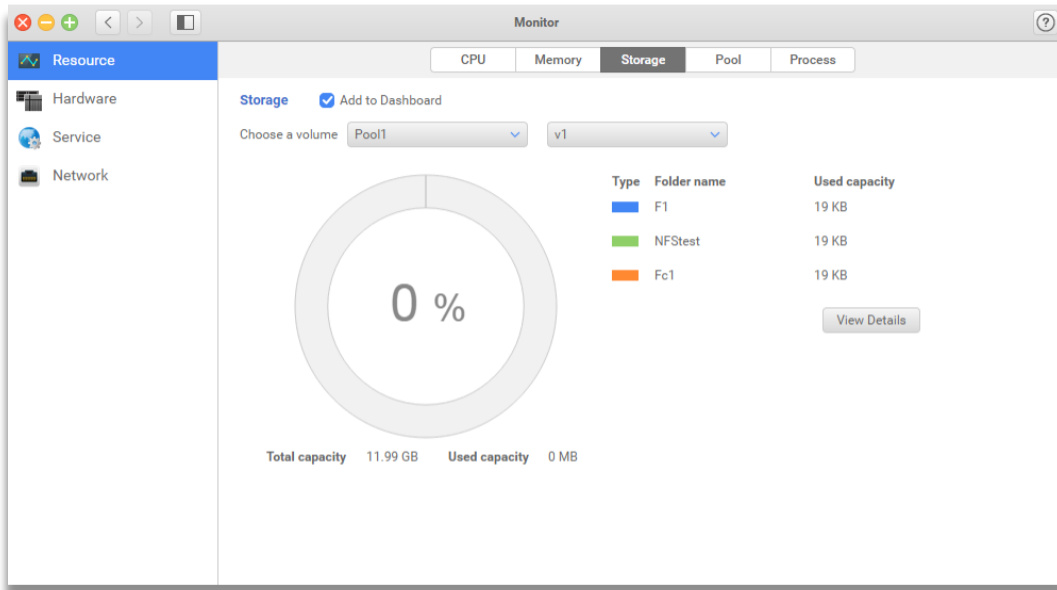


INFORMATION:

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 **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.

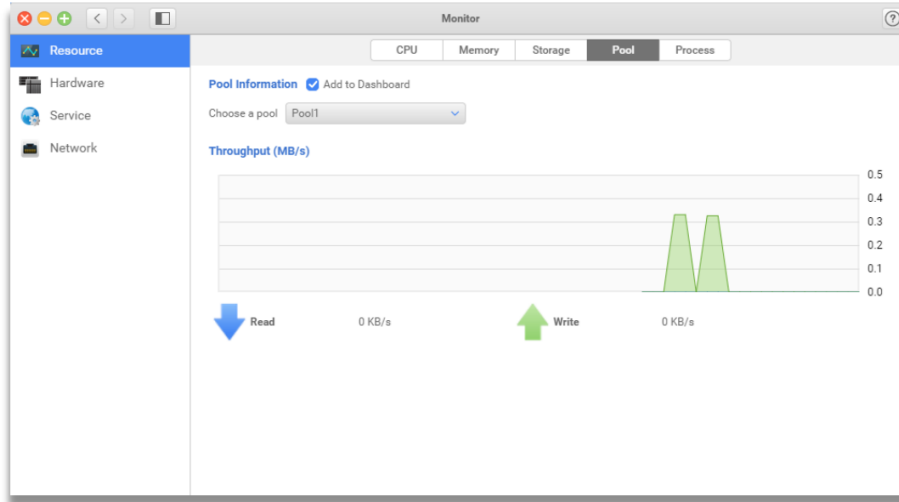


TIP:

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.

The screenshot shows the 'Monitor' application window with the 'Process' tab selected. At the top, there is a search bar labeled 'Search process name'. Below it is a table listing active processes. The table has the following columns: Process name, CPU usage (%), Memory usage (KB), PID, and User.

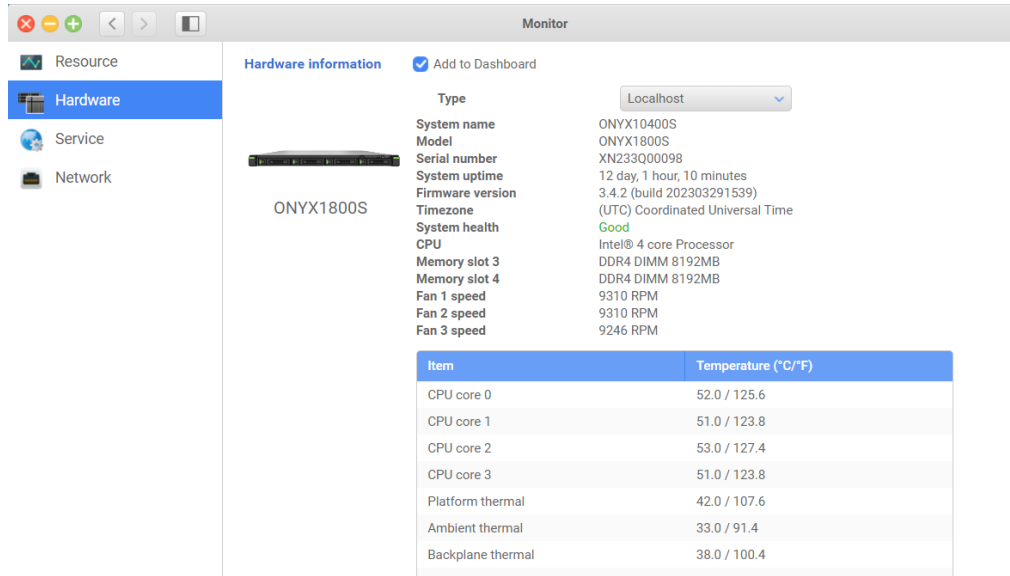
Process name	CPU usage (%)	Memory usage (KB)	PID	User
clamd	0%	687104	8878	admin
python	0%	503808	8157	admin
smbd	0%	254976	7002	admin
wireshark	0%	233472	7107	admin
nmbd	0%	180224	6964	admin
httpd	0%	153600	6742	admin
qbuzzed	0%	101376	6190	admin
qlogd	0%	94600	6140	admin
afpd	0%	94452	7035	admin
qureaddlogd	0%	88456	6207	admin
plp-cgi	0%	85676	8097	admin
bgtask_upd	0%	85424	4863	admin
xminor_notifyd	0%	85032	7220	admin
zqueryd	0%	84992	7827	admin
isnscd	0%	84708	5895	admin
index_notifyd	0%	84500	77517	admin

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.

2.5.2. 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.



TIP:

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 PSU status:

Yellow - The PSU is absent **Red**

- The PSU is not functioning.

- For temperature

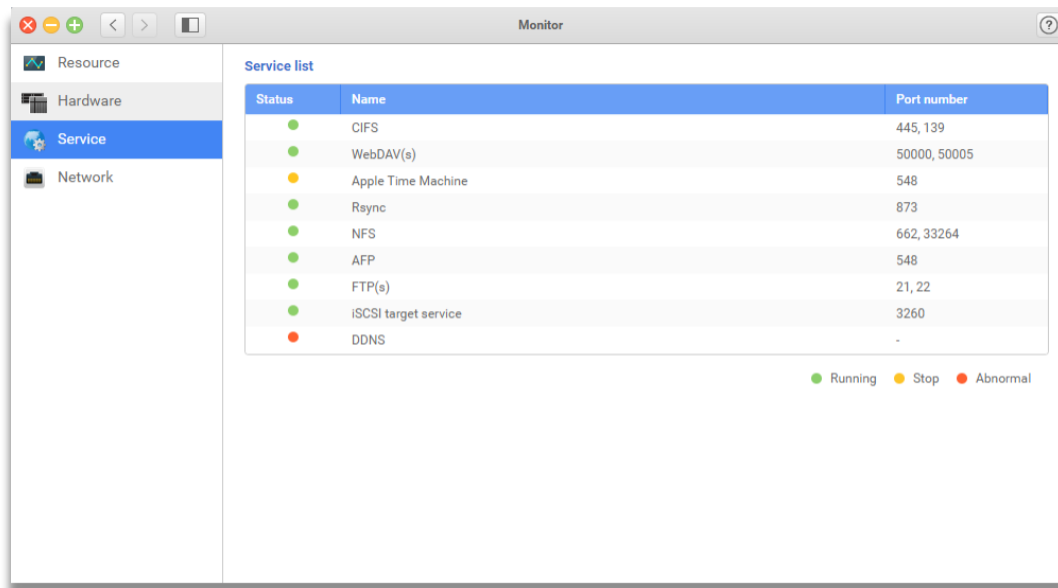
Green - The temperature is at normal level.

Yellow - The temperature is at abnormal

level. **Red** - The temperature is at critical level.

2.5.3. 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.



TIP:

The following are the possible service statuses:

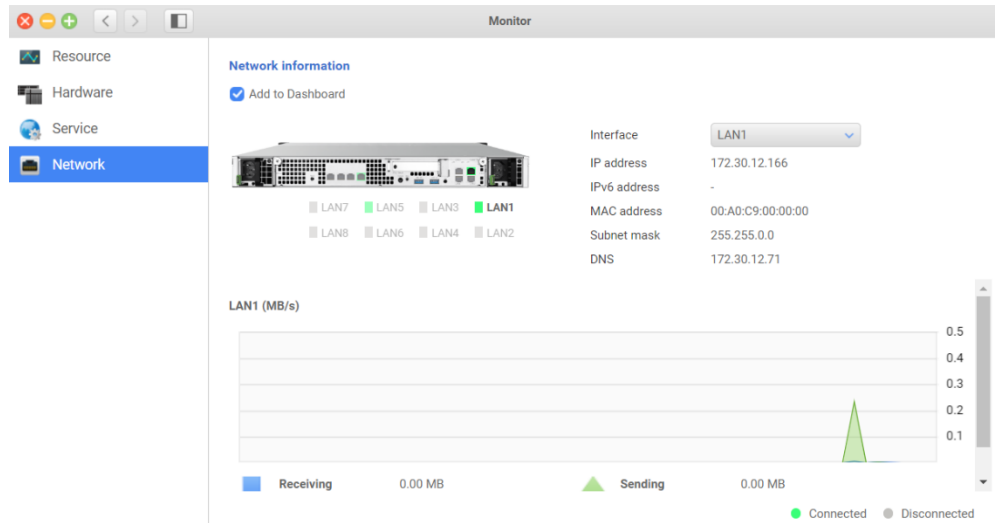
Green - Running.

Yellow - Stop.

Red - Abnormal.

2.5.4. 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.



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.



TIP:

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

following indication:

Green - Connected.

Grey - Disconnected.

3.0 Control Panel

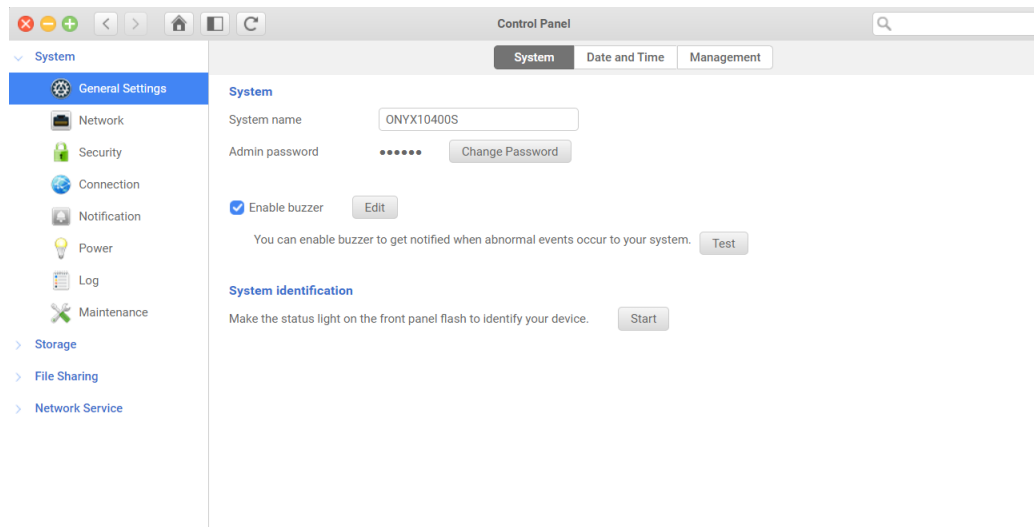
3.1. System

3.1.1. General Setting

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

System

In this page, you can setup the general setting, buzzer, and identify your ONYX Series. By naming and setting the password for the ONYX Series, it can help you recognize your device in your network and manage it.



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 admin's 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 ONYX Series start to notify administrators of the abnormal or error status by different type of sounds. At the same time, you can test the buzzer by simply click the **Test** button. To enable buzzer, please follow the steps below:

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

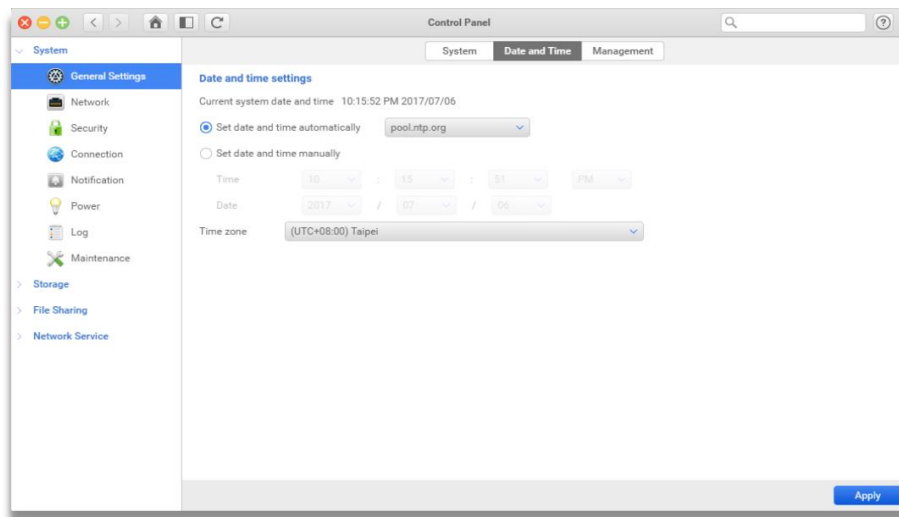
You can test the buzzer by simply click the Test button.

System identification

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

Date and Time

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



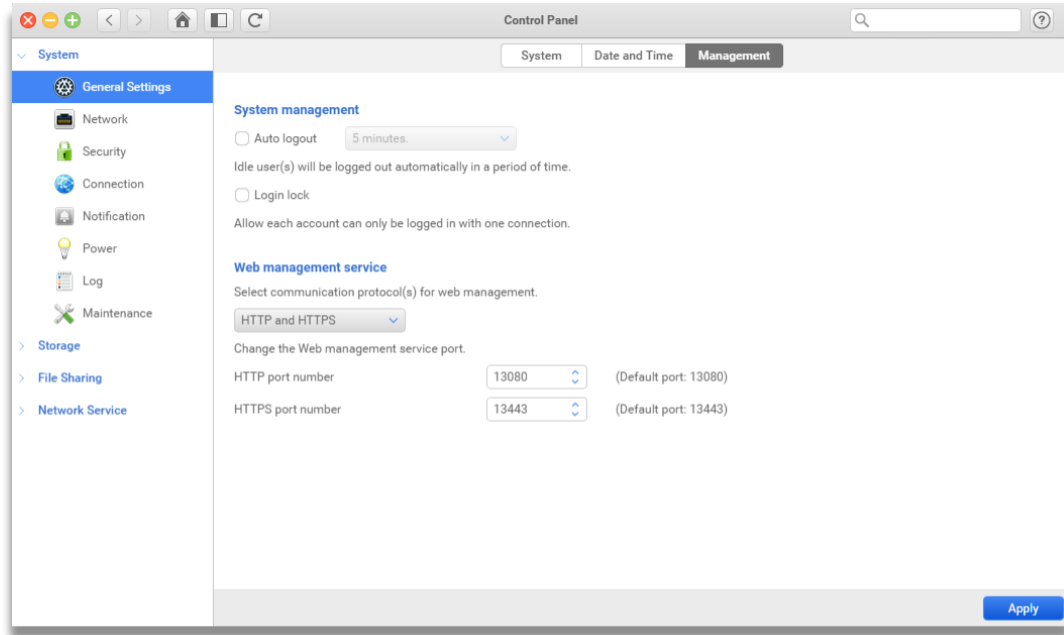
Date and Time settings

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 ONYX Series.



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: Enable the Login lock, one user account does not allow to create multisession to access ONYX Series.

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 ONYX Series 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 ONYX Series by TLS/SSL connection. Please setup the web management service by the following steps:

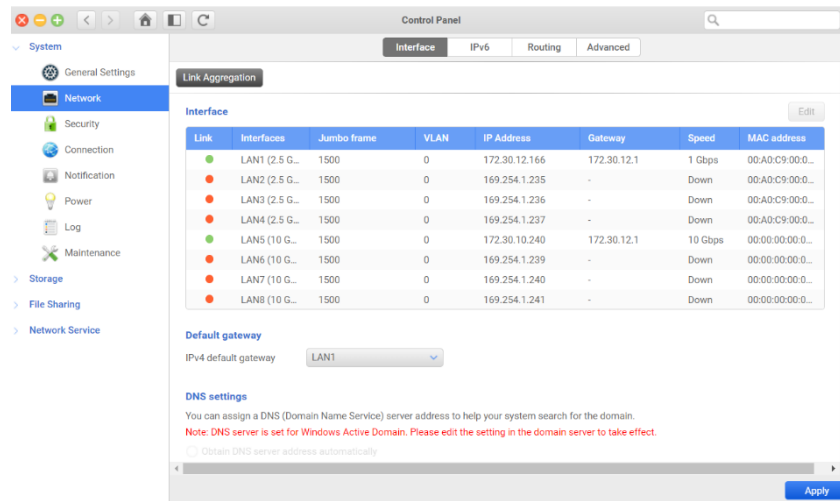
1. Choose web service communication protocol below from the drop-down menu:
 - **HTTP (Hypertext Transfer Protocol) only:** HTTP is a set of communication protocols which allows users to communicate and exchange information on the World Wide Web. The default port for an HTTP connection is 13080.
 - **HTTPS (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.

3.1.2. Network

In network page, you can view the status and config each Ethernet and Thunderbolt (Optional) interface. ONYX Series also provides the Link aggregation, IPv6, Routing table and some more advanced settings for administrators easy to control the Ethernet access of the device.

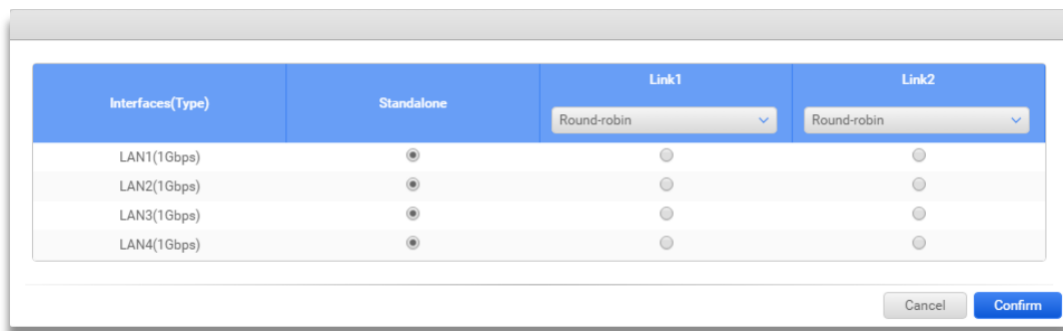
Interface

You can view the network circumstance and config each network interface. The default gateway and DNS service can also be setup over here. When Thunderbolt care is installed, the interface configuration can also be found on this page.



Link Aggregation

Link aggregation is the technology that can provide 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.



Please follow the steps below to setup link aggregation:

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.

Edit the specific network Interface

In different network circumstances, you may need the to set each network interface independently.

There are three ways help your ONYX Series to get an IP address, such as DHCP, BOOTP, and Static.

Moreover, you can set Jumbo frame and VLAN as well.

The screenshot shows a configuration window titled "LAN1". It contains the following fields and options:

- LAN1** (Section Header)
- Instruction: "You can select 'DHCP' or 'BOOTP' to acquire an IP address automatically. If you would like to specify an IP address, please select 'Static'."
- Radio buttons for **DHCP**, **BOOTP**, and **Static** (selected).
- IP address**: 192.168.153.180
- Subnet mask**: 255.255.128.0
- Gateway**: 192.168.128.254
- Jumbo frame**: 1500 (dropdown menu)
- Enable VLAN**
- VLAN ID**: 0
- Buttons: **Cancel** and **Confirm**

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 distribution 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 permanent number assigned to a computer by an Internet service provider (ISP). A static address is constant; systems with static IP addresses are vulnerable to data mining and increased security risks. A static IP address is also known as a fixed address, which means

that a computer with an assigned static IP address uses the same IP address when connecting to the Internet.

4. Setup jumbo frame: Select the MTU value of the jumbo frame for your network environment.



INFORMATION:

The Jumbo frame setting is valid if the ONYX Series 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.

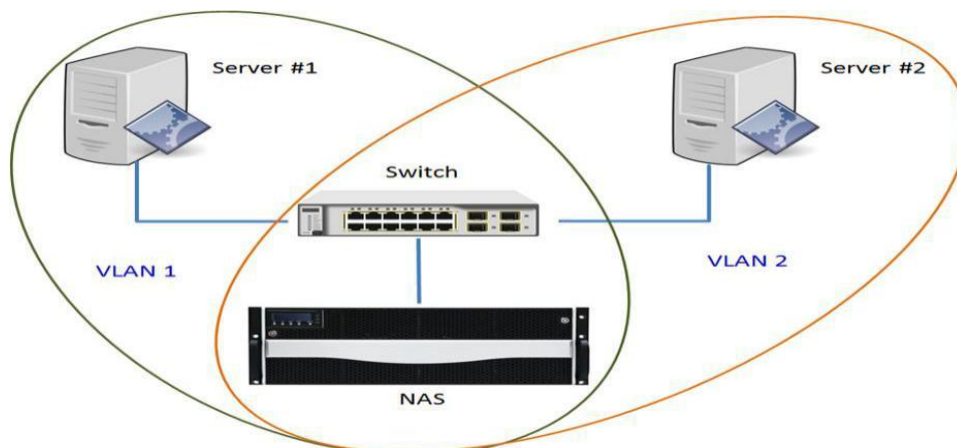


INFORMATION:

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, server) to integrate into the same logical network.
- ② Rapidly communicates information to each other.
- ③ Shares resource and isolate broadcast 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 ONYX Series, such as LAN1, LAN2, etc. Please set up by the following steps:

1. Choose the default gateway 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 have to enter primary or secondary DNS manually.
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. Choose the interface you want to modify, and click **Edit**.
3. Select one of the following types:
 - **Automatic:** Acquire an IP address automatically.

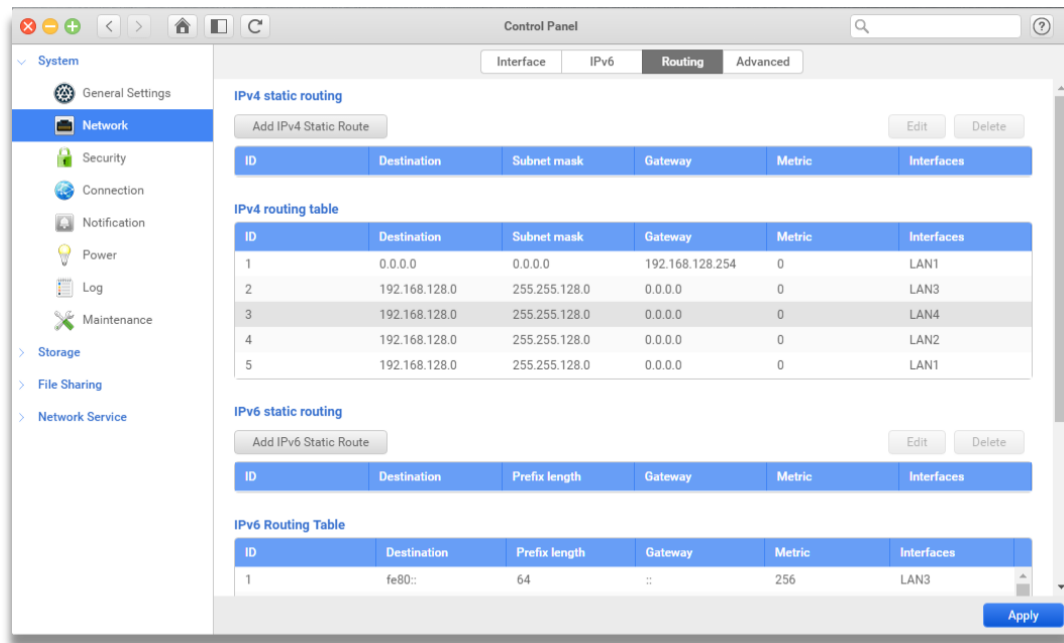
- **DHCP:** Use Dynamic Host Configuration Protocol (DHCP) to allocate an intellectual property address.
 - **Static:** Specify an IP address manually. If you choose Static, you have to set IPv6 address, prefix length (Valid range: 0~128) and gateway first.
4. Click **Confirm** to save the settings.

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 ONYX Series.

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:

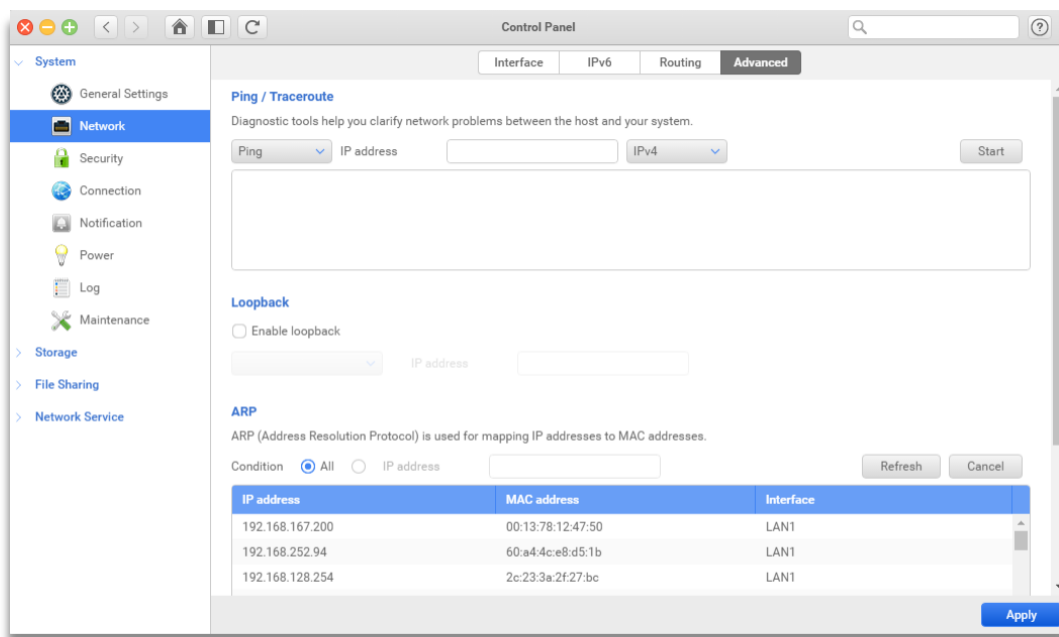
1. Choose the item you want to modify.
2. Click **Edit** and setup the form settings. (See the descriptions in **Add IPv4/IPv6 static route**)
3. Click **Confirm** to save the changes.

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

1. Choose the item you want to modify.
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.



The NAS system provides diagnostic tools such as Ping/Traceroute to diagnose what happens between the host and system. To start 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

Choose interface and enter the IP address of the other device to execute a loopback which checks the transmission performance between the NAS and other devices. 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 choose all or type the specific IP address for mapping. Check the steps Choose diagnostic tool including Ping or Traceroute.

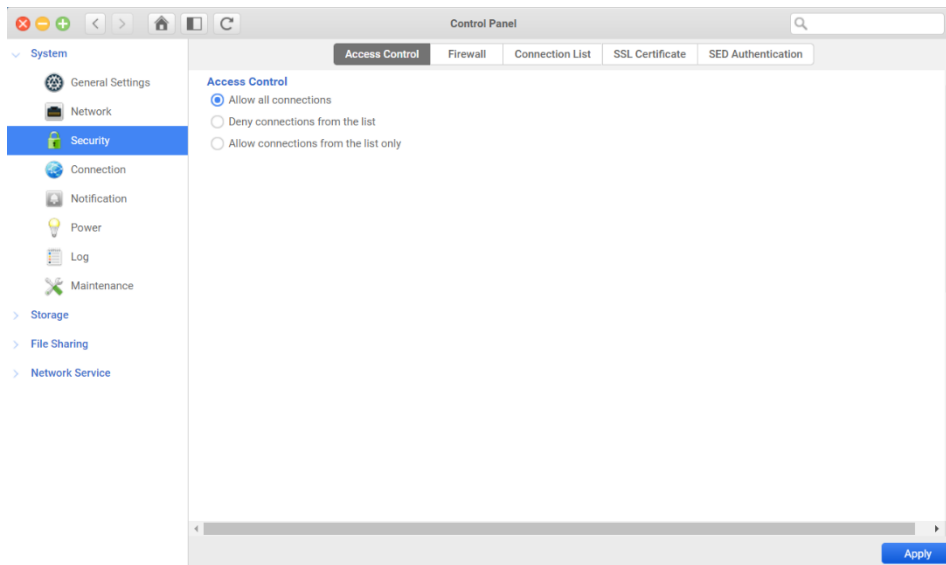
1. Select **All** or enter the specific IP address.
2. Click **Flush** to start mapping the addresses.
3. Click **Cancel** to stop mapping the addresses.

3.1.3. Security

In Security, you can make your ONYX Series 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 ONYX Series. 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:

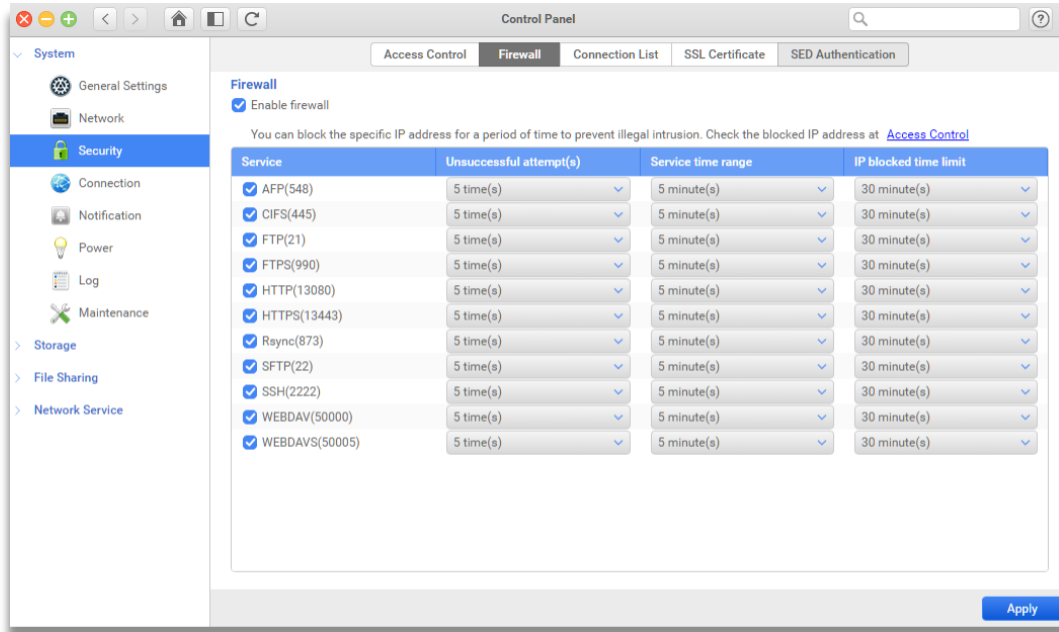
1. Select Allow connections from the list.
2. Click **Add** button.
3. Choose one of the following methods:
 - **Single IP address:**
 - ① Enter an IP address and setup the block time.
 - ② Click **Confirm** button.
 - ③ Click **Apply** button to finish the setting.
 - **Specify IP address of network 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.

**INFORMATION:**

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

Firewall

At this page, Firewall can prevent your ONYX Series from Internet attack for different data services by blocking the IP automatically. By setting up the unsuccessful attempts in the given time, the system will block the IP until the rules have passed.



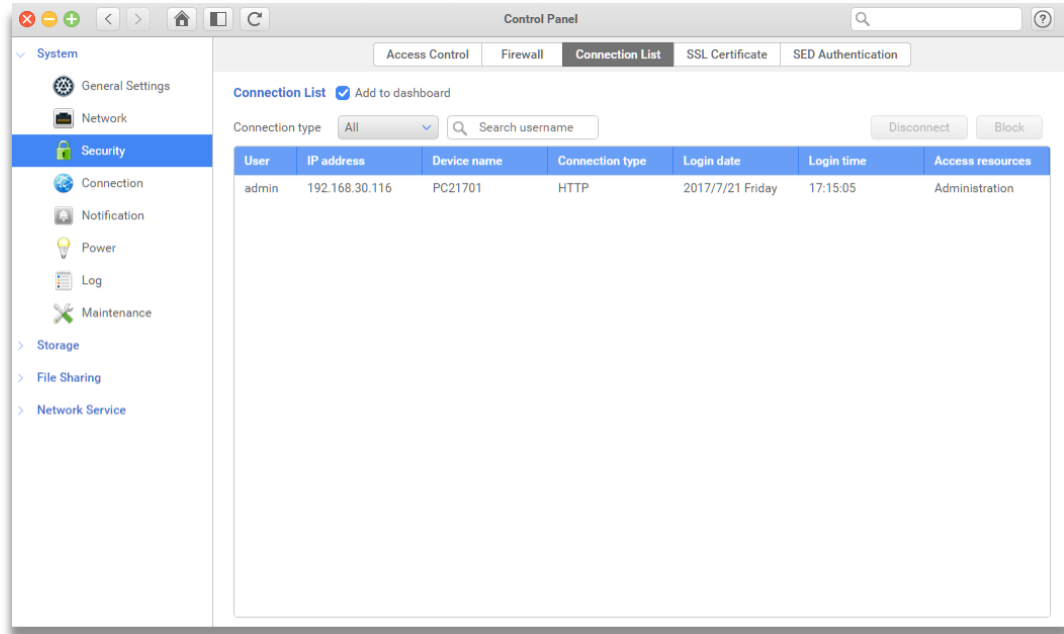
Enable Firewall

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 ONYX Series. 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 the particular file service, 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

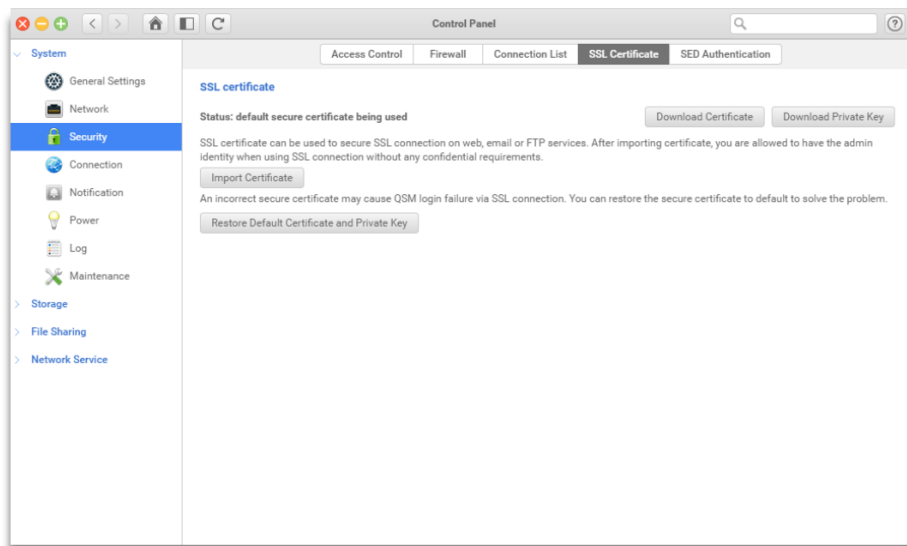
To block the user from the list, please follow the steps below:

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 ONYX Series, 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.

INFORMATION:

The certificate cannot be decrypted by the other private key pair.

Restore current certification

To restore the current certificates on ONYX Series, please follow the steps below:

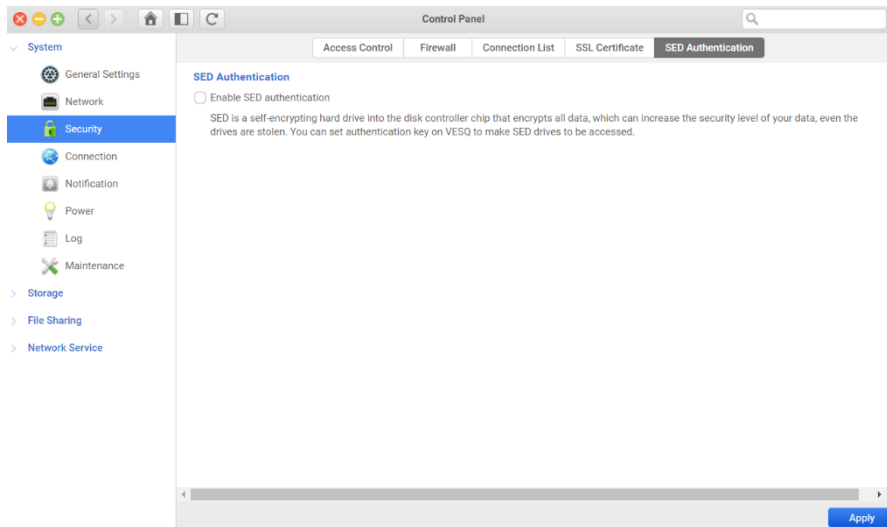
1. Click **Restore Default Certificate and Private Key**.
2. The certificate will be restored to default.

Download certificate

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

SED Authentication

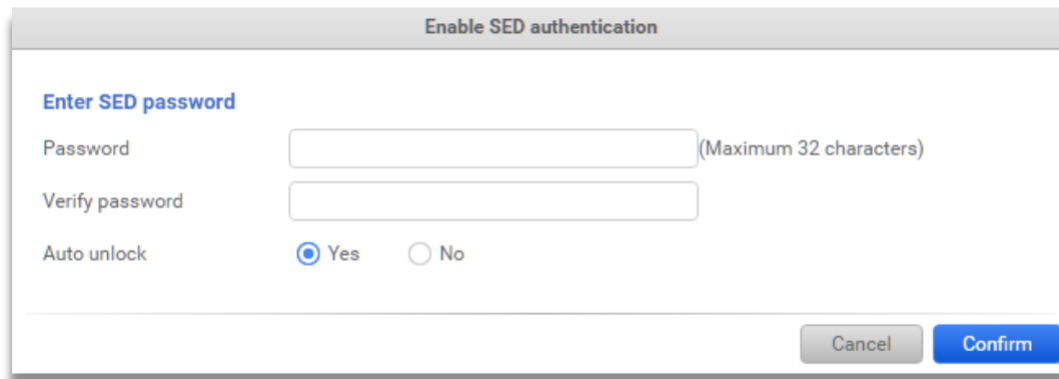
If you enable SED authentication, the system can generate the authentication key for SED protected disk(s) that even on the roaming process.



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**.

3.1.4. Connection

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

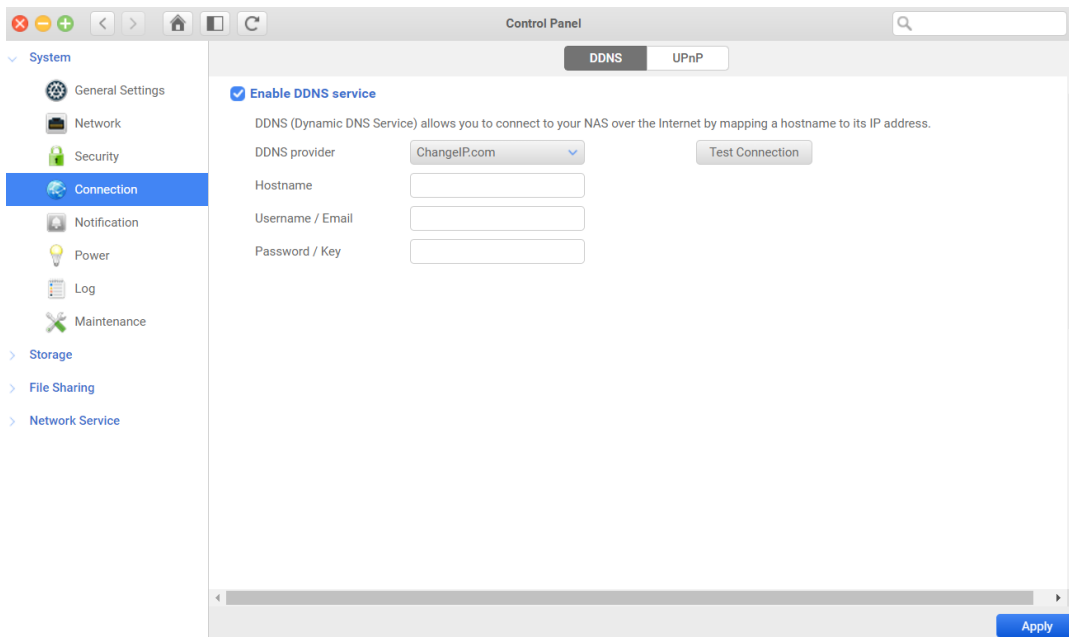
DDNS

In **DDNS**, you can register a VES dynamic domain name (VES Cloud) or log in a third-party dynamic domain name for your ONYX Series. Then you can easily connect to your ONYX Series with your public domain name (e.g. VES.VEScloud.net) 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 ONYX Series is able to connected to the internet.



Login a dynamic domain name for your ONYX Series

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



INFORMATION:

ONYX Series Software Guide

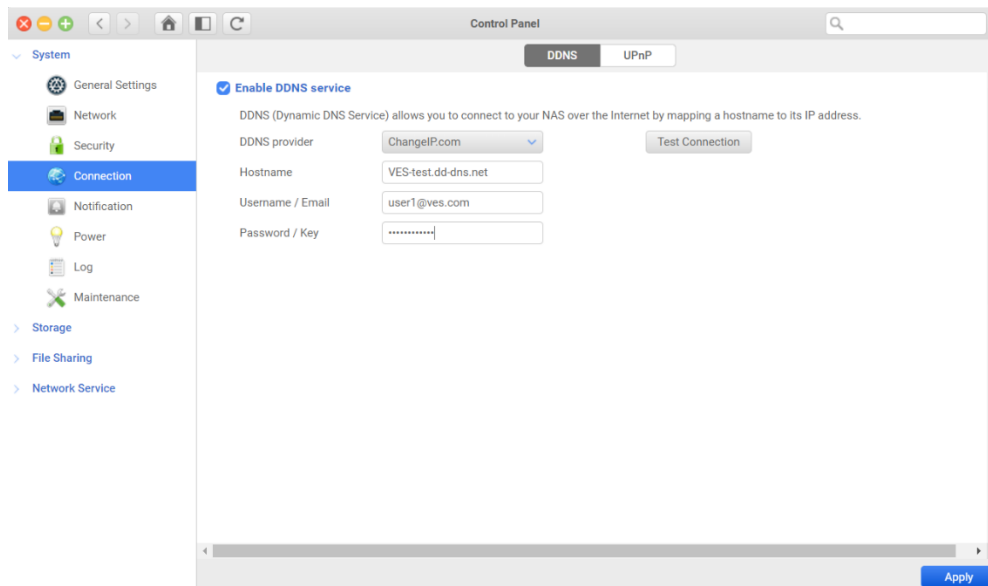
Document CTC-DOC-003004

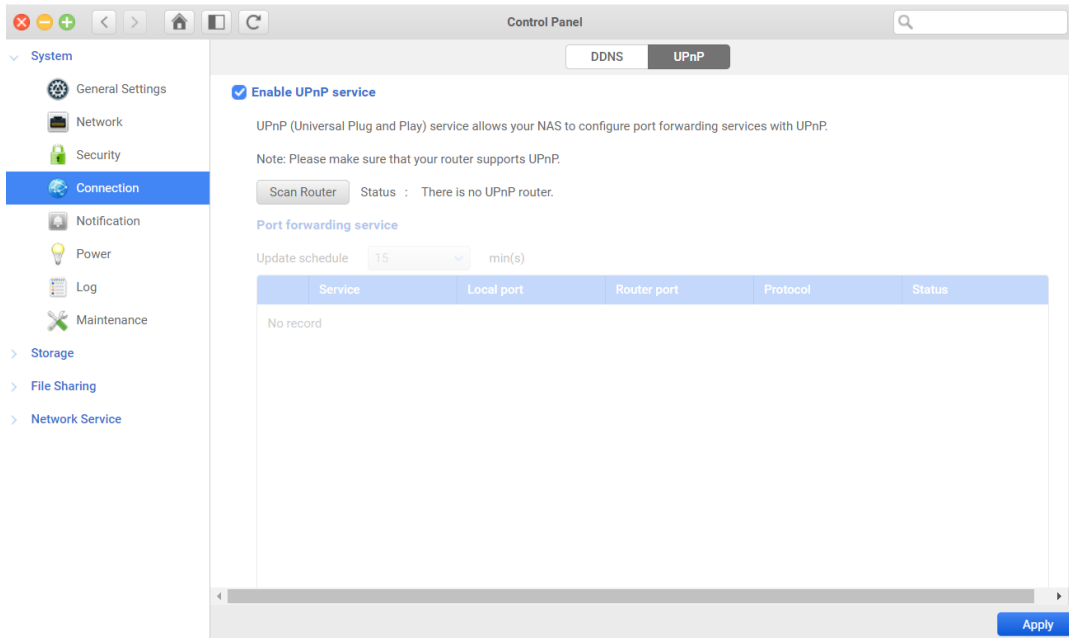
ONYX Series supports the following DDNS providers:

1. VES 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.





UPnP

In **UPnP**, you can set up the port forwarding table of your router to forward ONYX Series' service port number, to allow ONYX Series 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 VES compatibility list.
2. Your ONYX Series is connected with a 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.

**INFORMATION:**

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

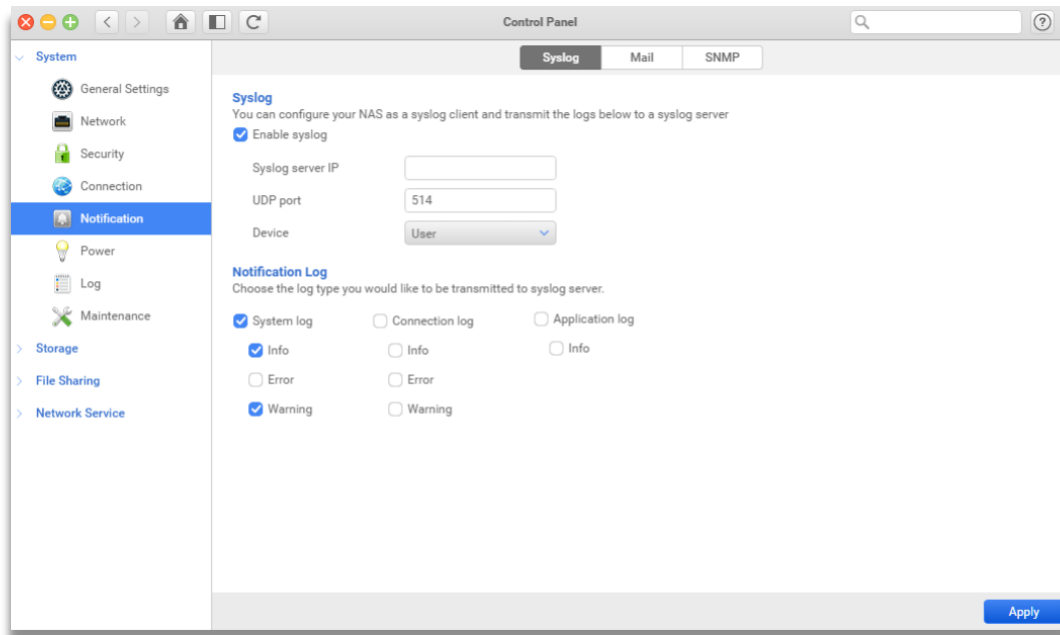
1. Xccess: 51000 ports
2. AFP: 548 ports
3. FTP: 21 ports
4. HTTP: 13080 ports
5. HTTPS: 13443 ports
6. Rsync: 873 ports
7. SFTP: 22 ports
8. SSH: 2222 ports
9. WebDAV: 50000 ports
10. WebDAVS: 50005 ports

3.1.5. 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:

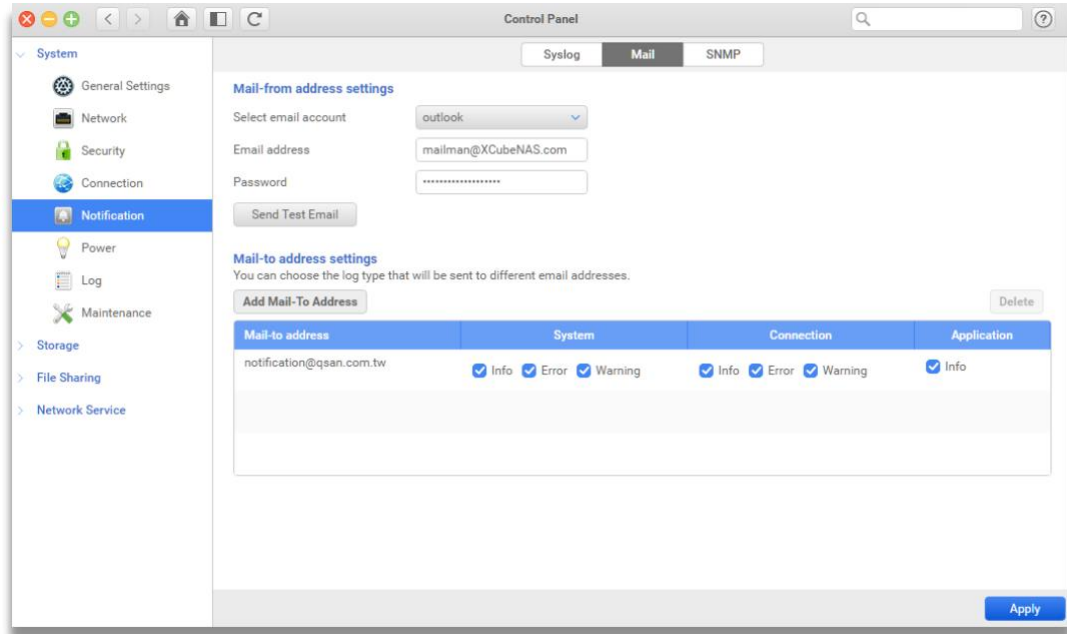
1. Select **Enable Syslog**.
2. Enter **Syslog server IP**.
3. Enter **UDP port**.
4. Select **Device**.
5. Select the events you want to send to the server.
6. Click **Apply** to save the settings.

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 ONYX Series 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 ONYX Series 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 on this server. (Please refer to your e-mail service provider for the SMTP settings.) (Custom mode)
3. Set up your port when you are log in. (Custom mode)
4. Enter your email address.
5. Type in your account & password
6. Click **Apply** to save the settings.
7. If you want to send a test email to the specified email account, click **Send test email**, and then check your email.

Mail-to address setting

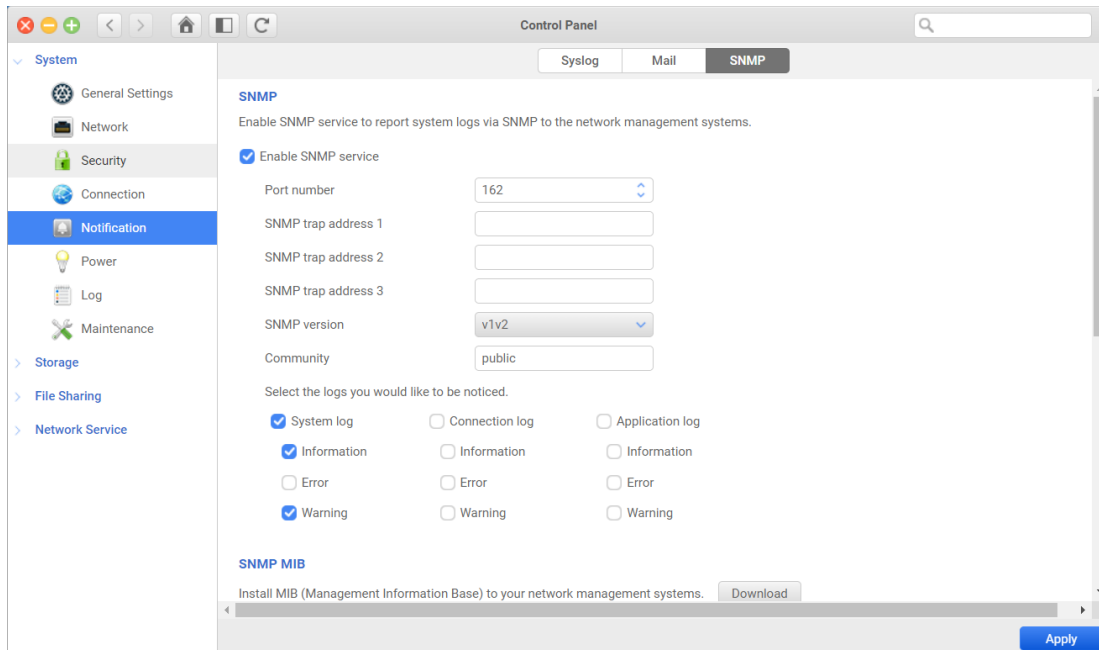
Enter a mail to address can help you receive the event occurred on your ONYX Series from your Mail-from address.

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 systems to monitor appliances attached to a network. Types include SNMPv1, SNMPv2 and SNMPv3 are supported.



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.



INFORMATION:

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

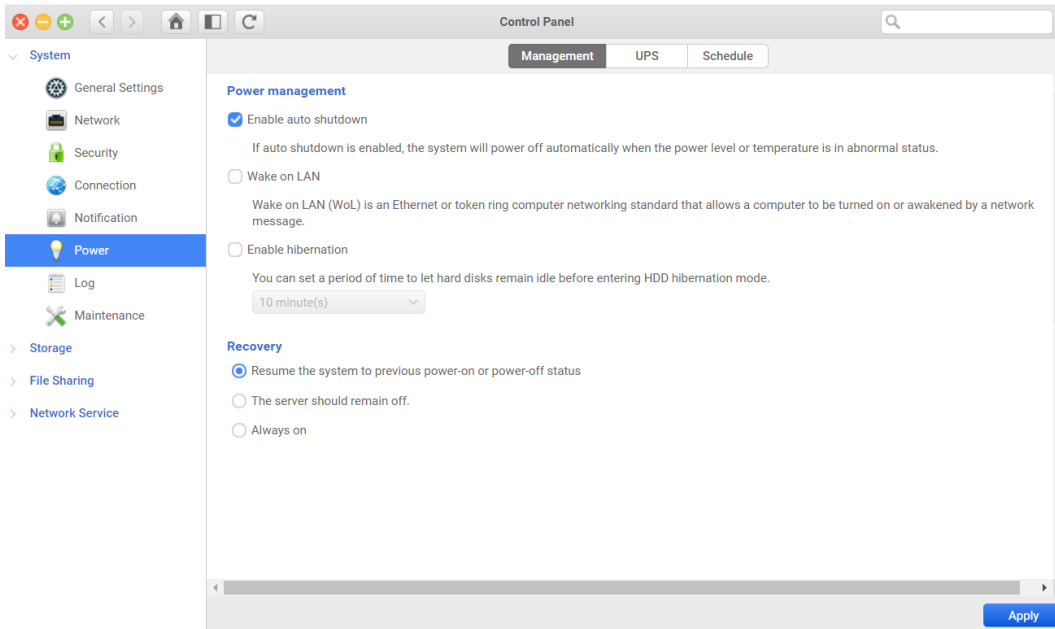
VES provides the ability to monitor the ONYX Series including system, disk, and the status of RAID volumes. Please click the **Download** button, if you want to install the MIB files into your managing system.

3.1.6. 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 ONYX Series can be powered on in LAN network. 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.

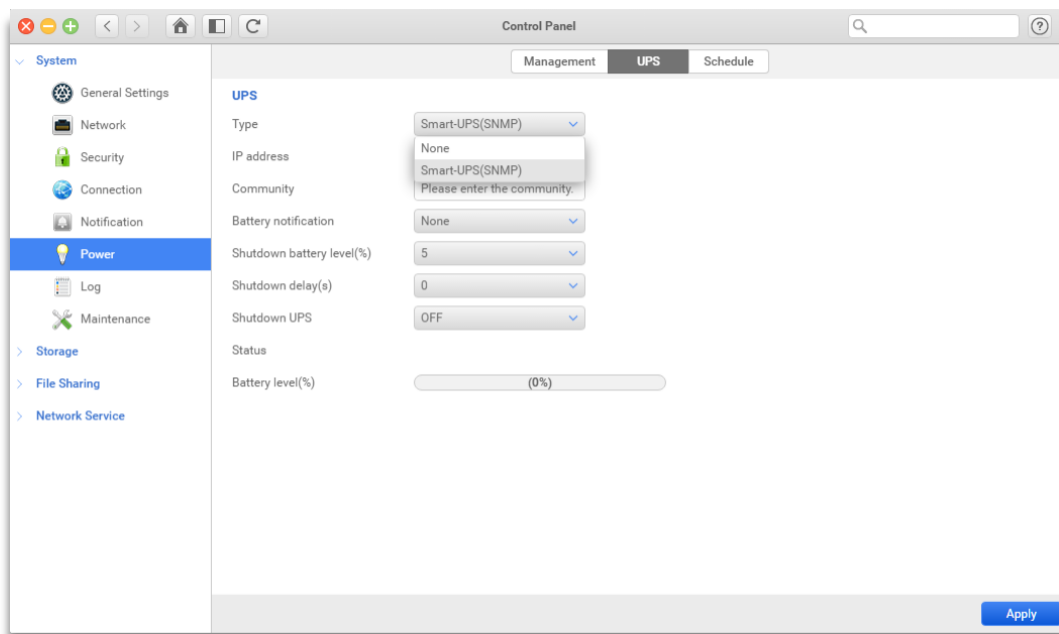
Recovery

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

1. Choose one of the following options:
 - Restored to the previous power-on or power-off status.
 - Left 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 ONYX Series if the power failure occurs or power outage.



Set up UPS

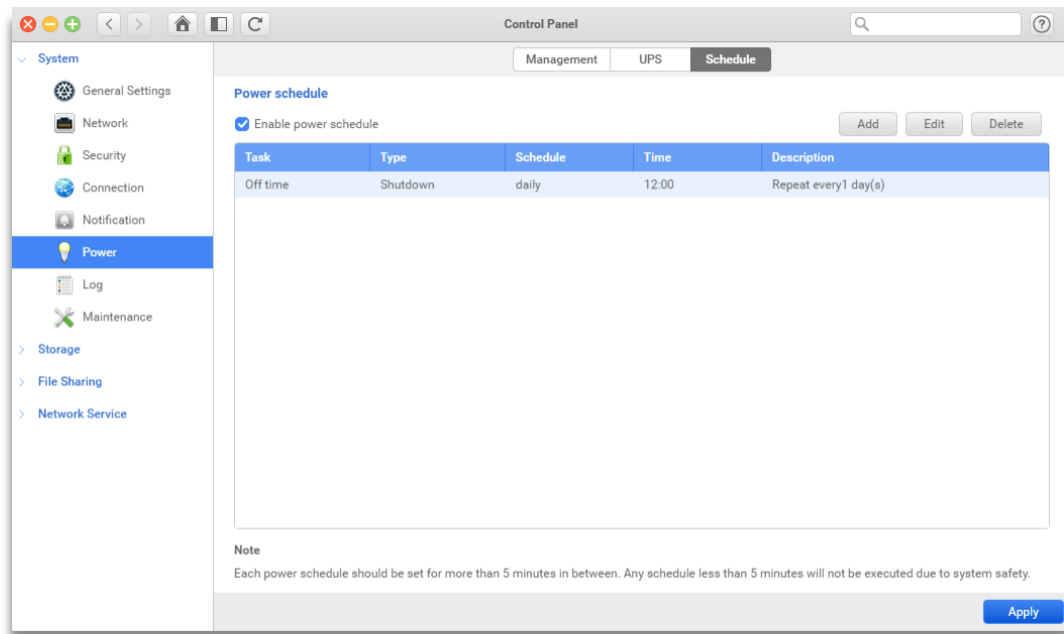
After installing the UPS, you can configure the UPS settings by the following steps:

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 ONYX Series 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:

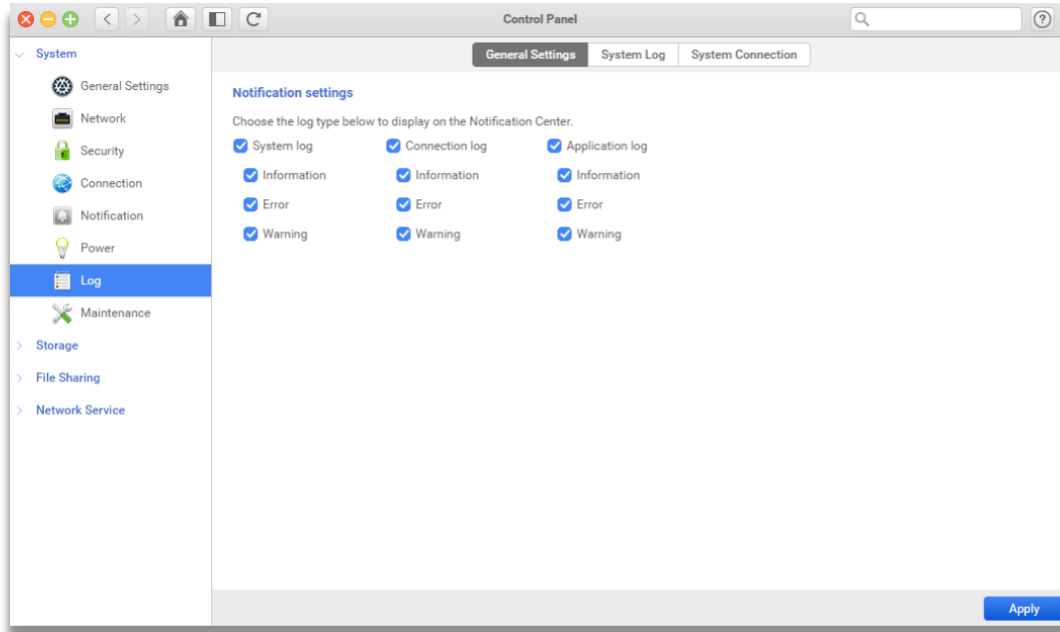
1. Select a schedule you want to remove.
2. Click **Delete**.
3. Click **Confirm** to save the settings.

3.1.7. 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.



INFORMATION:

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 types of log: 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.



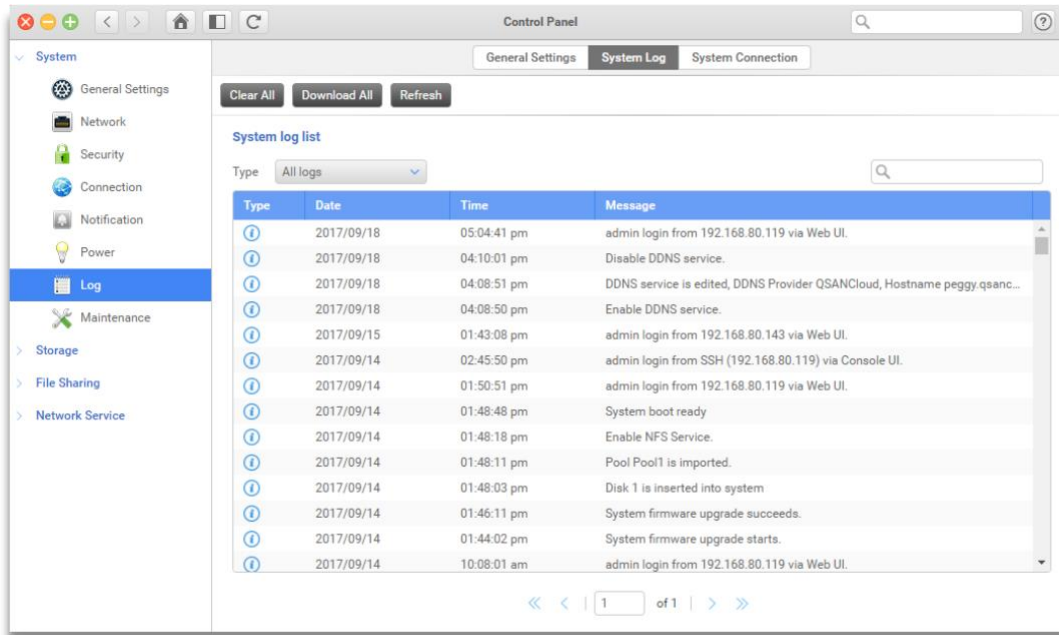
TIP

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 ONYX Series indicating errors may have occurred, you can refer to these event logs for troubleshooting.



INFORMATION:

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.



INFORMATION:

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.



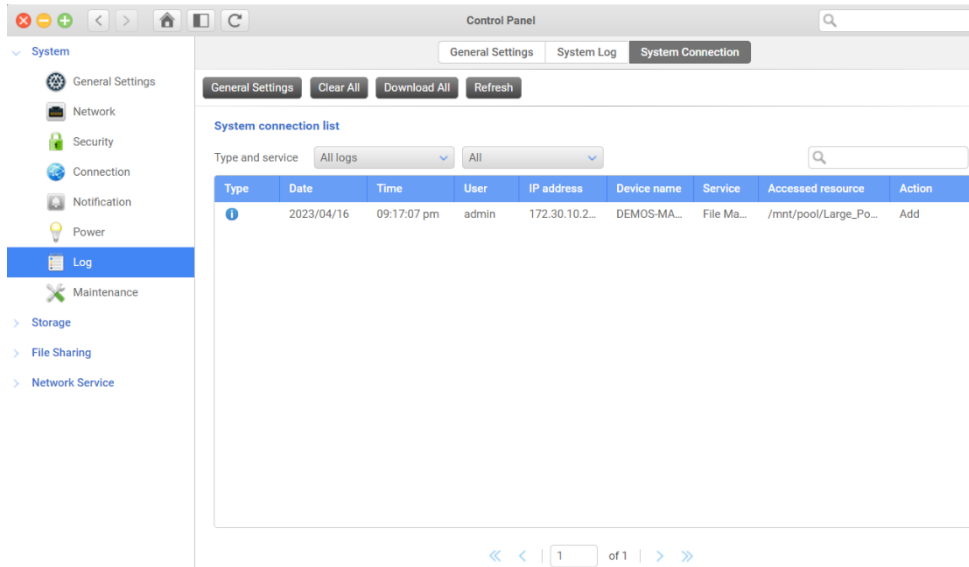
INFORMATION:

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.



INFORMATION:

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 and Xccess.

The file transfer performance might be slightly affected when the 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.



TIP:

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.



INFORMATION:

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.



INFORMATION:

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.

**INFORMATION:**

Valid characters: 【a-z A-Z 0-9】

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

**INFORMATION:**

Valid characters: 【0-9】

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

**INFORMATION:**

Valid characters: 【a-z A-Z 0-9】

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

3.1.8. Maintenance

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

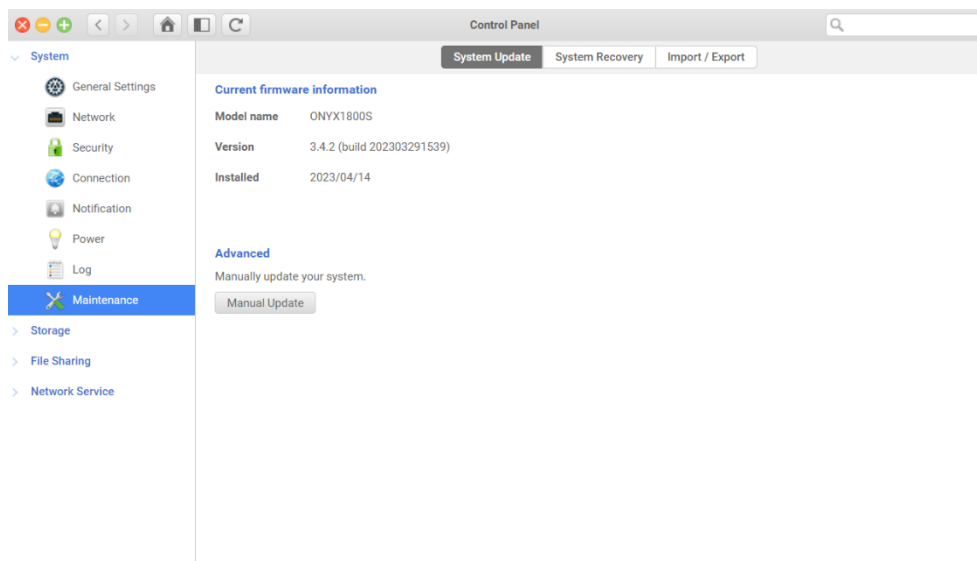
System Update

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



INFORMATION:

Updating firmware does not affect the data on ONYX Series, however, to ensure the data security, back up all your data before update is strongly recommended.



Current firmware information

It shows the model name, version and installed date of the current firmware on your ONYX Series.

Status

To make sure your ONYX Series 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.

Advanced

To update the firmware on ONYX Series manually, you can download the latest firmware on VES website (<http://www.VES.com>) and click Manual Update to upload the binary file (.bin) to your system.

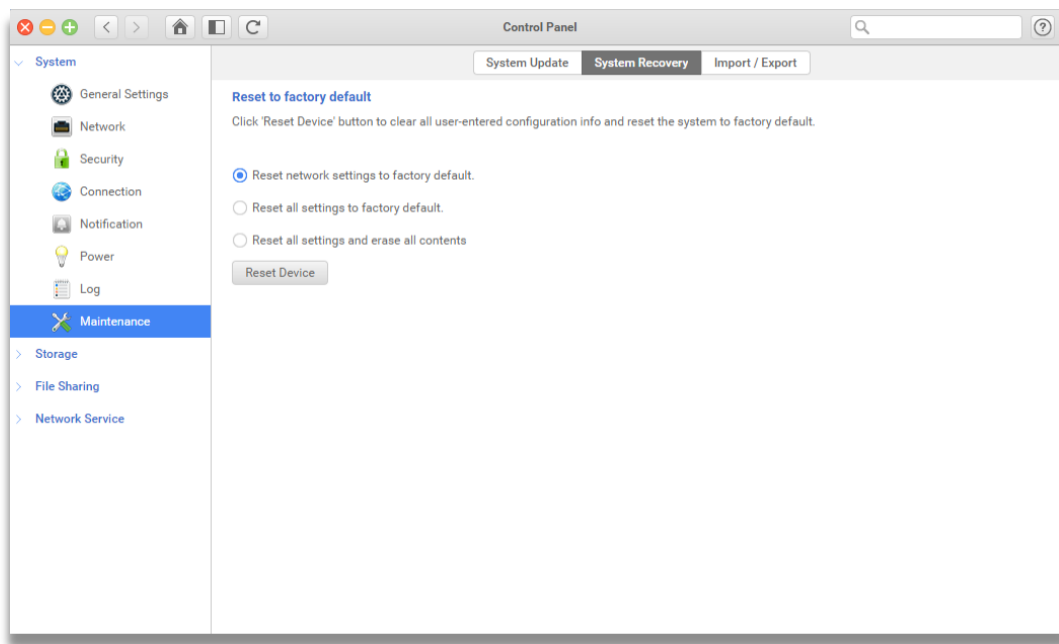


INFORMATION:

Firmware version cannot return to the previous version than currently installed one.

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 ONYX Series 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 Admin PWD to "1234".
- 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 delete.
 - ⑥ Port trunking will be disabling.
 - ⑦ After configs will be deleted, RESTART the NAS.
 - ⑧ Log out VES Cloud.
 - ⑨ DNS settings.
 - ⑩ DDNS and UPNP settings.



INFORMATION:

When system joined AD server, 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 All VPN settings will be deleted.
- ⑧ Web server setting set to default.
- ⑨ AntiVirus setting will be deleted.
- ⑩ SQL settings are set to default.

⑩ Media Library index will be deleted.
⑩ 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 contents.
- ③ After data and configurations are deleted, RESTART the NAS.

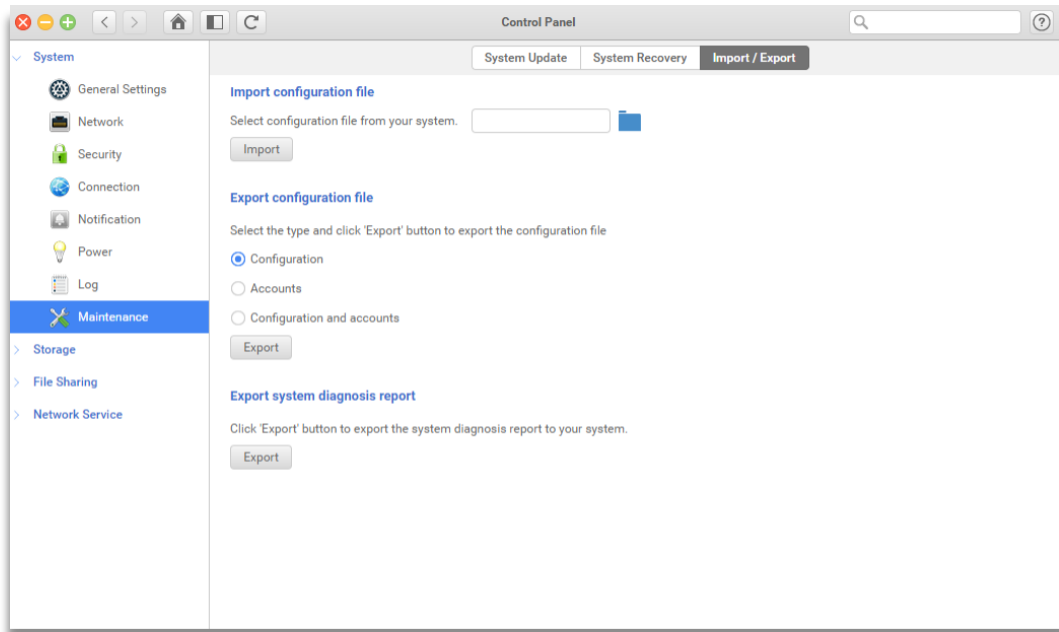


INFORMATION:

If WORN folder exists, this option will be gray out, So you will not be able to initiate your ONYX Series.

Import/ Export

You can use your ONYX Series settings on another ONYX Series. 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.



INFORMATION:

The import file (.bin) can only be the export configuration files from another ONYX Series.

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.



INFORMATION:

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 VES support and Engineers to diagnose the unexpected issues.

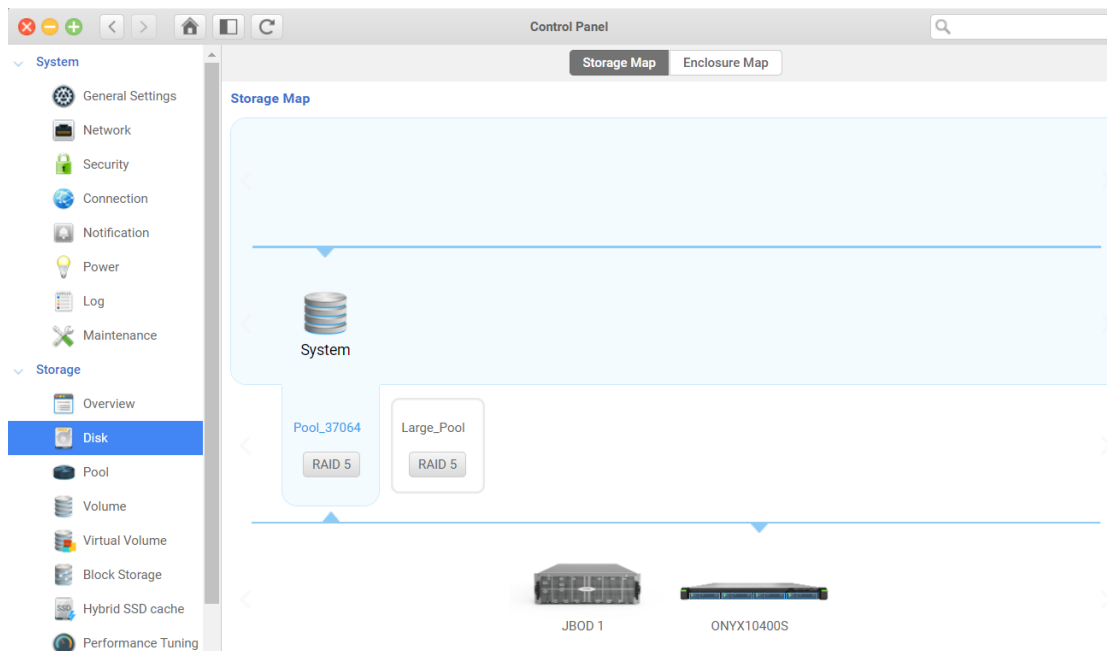
3.2. Storage

3.2.1. 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.



INFORMATION:

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

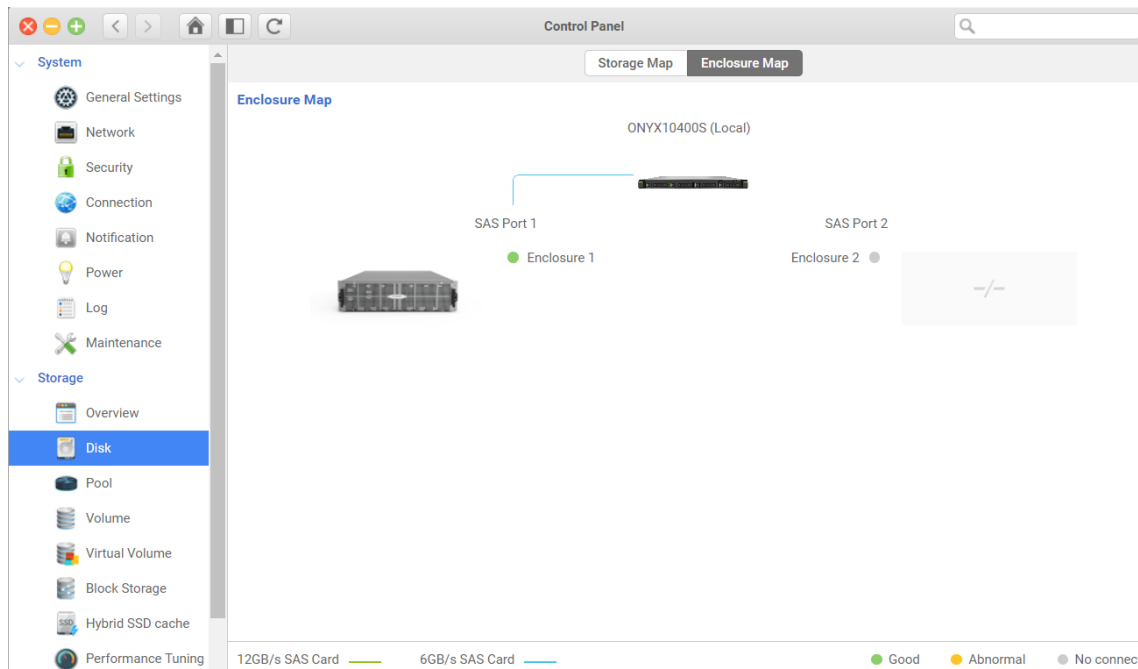
To make the management easier on each folder, you can simply click the folder icon showing on the page.

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.

Enclosure Map

In Enclosure Map, you can check all the enclosures which were connected via SAS 12G expansion card.



Check your expansions

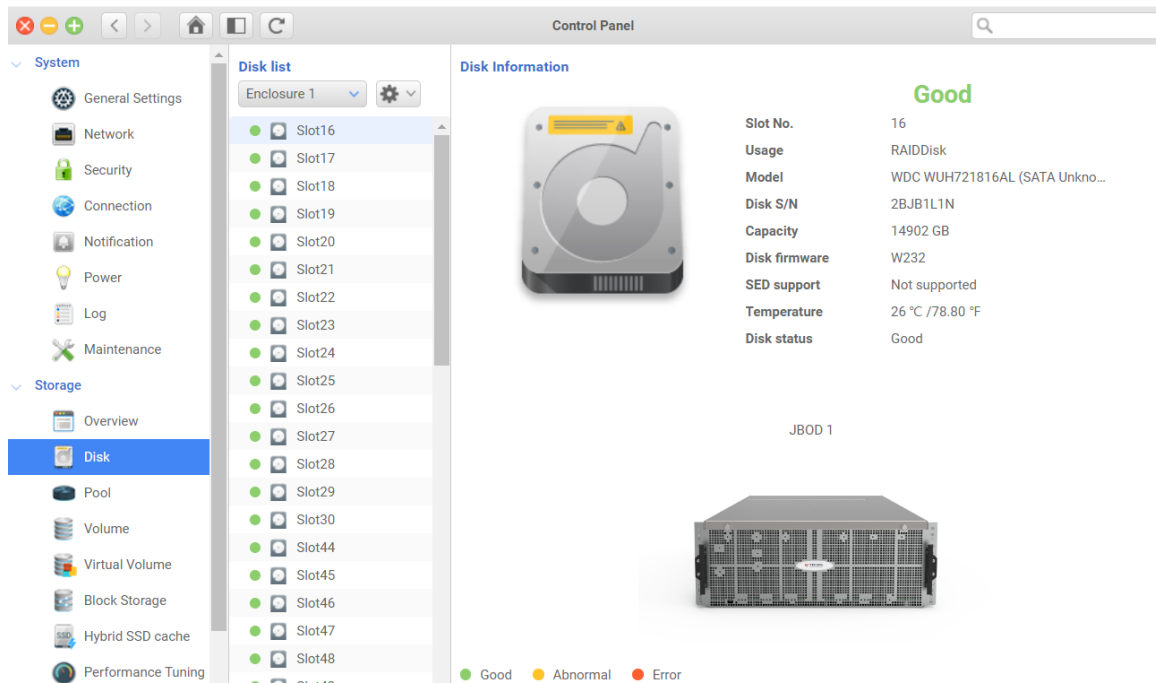
While connecting to expansion units, you can easily check the connecting speed or click it to view more information for the unit.

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.

3.2.2. Disk

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



Set global spare

The global spare disk is a redundant disk which helps the system automatically take over the failed disk in any pool.

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**.



INFORMATION:

You can only set the FreeDisk as the spare disk.

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



TIP:

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

Identify the disk

In some circumstances, system administrators need to find a physical disk in a bunch of the disks; this feature helps them to find disks in local and 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.

**TIP:**

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.

**TIP:**

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.

**TIP:**

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 ONYX Series.
-

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

Unlock a disk

Self-encrypting drive (SED) is a hardware 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**.

**TIP:**

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.

**INFORMATION:**

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.

**INFORMATION:**

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 administrators 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.

INFORMATION:

Not all of disks support S.M.A.R.T. test.

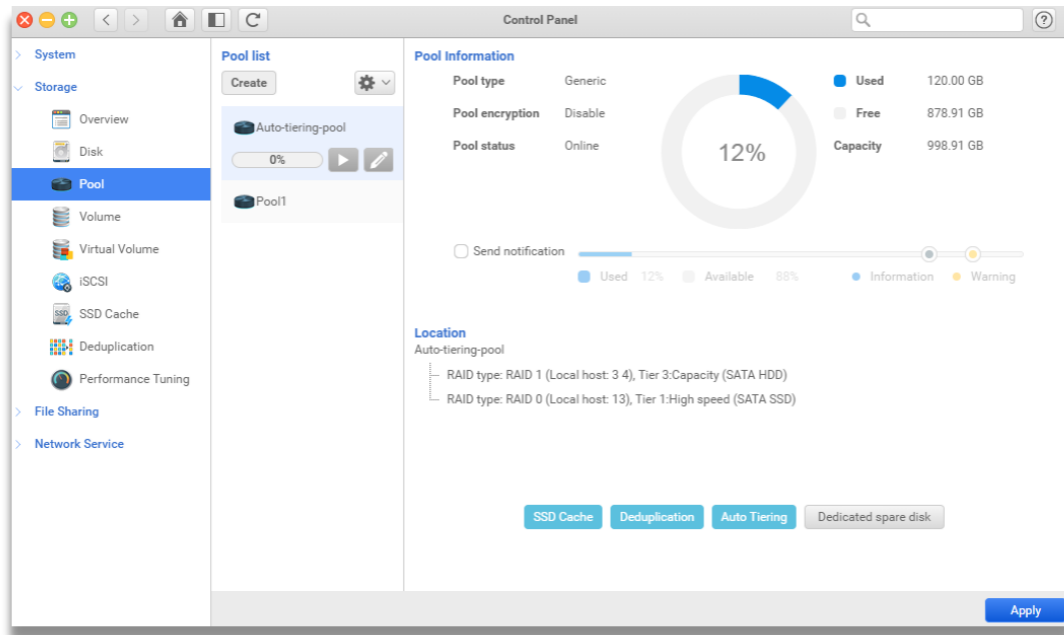
3.2.3. Pool

In **Pool**, you can check detail information about all pools on your ONYX Series, such as pool type, status, and capacity usage. You can also setup the **SSD Cache**, **Deduplication**, **Auto Tiering**, **Spare disks**, and **SED authentication**.



INFORMATION:

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

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 drivers on the systems, 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.

**INFORMATION:**

ONYX Series 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 ONYX Series.
-

**TIP:**

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.
-

**INFORMATION:**

1. Disk write cache: The cache is the disk built in cache.
 2. Pool encryption is a software-based encryption to improve the 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.

**INFORMATION:**

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. Select the dedicated spare disk for this particular RAID set.

**INFORMATION:**

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 the pool is short of storage capacity, the best way is the expand its capacity. In ONYX Series, it offers two ways to increase the pool capacity, expand it by **Adding a RAID set**, and **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.

**TIP:**

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 A online RAID expand window will pop out.

**INFORMATION:**

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.

**TIP:**

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. A 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 ONYX Series 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 decrypt 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.



INFORMATION:

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.

Delete

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



INFORMATION:

Before deleting the pool, please make sure all the data of the pool is erased.

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

VES 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 set which can be divided into different tiers, such as, Ultra-high speed (PCI-e SSD), High speed, High speed, and capacity.

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.

**TIP:**

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).

**TIP:**

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 bay schedule.

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

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

**TIP:**

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.

**TIP:**

During the data relocation, the system may be affected. You can set up a period of time to relocate the data or make it run until finished.

7. Set up the relocation rate.

**INFORMATION:**

Relocation rate is for how system performance resource to be allocated. Fast means use more resources to finish the data 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 Warning level notification.
4. Click **Apply** to finish the setting.

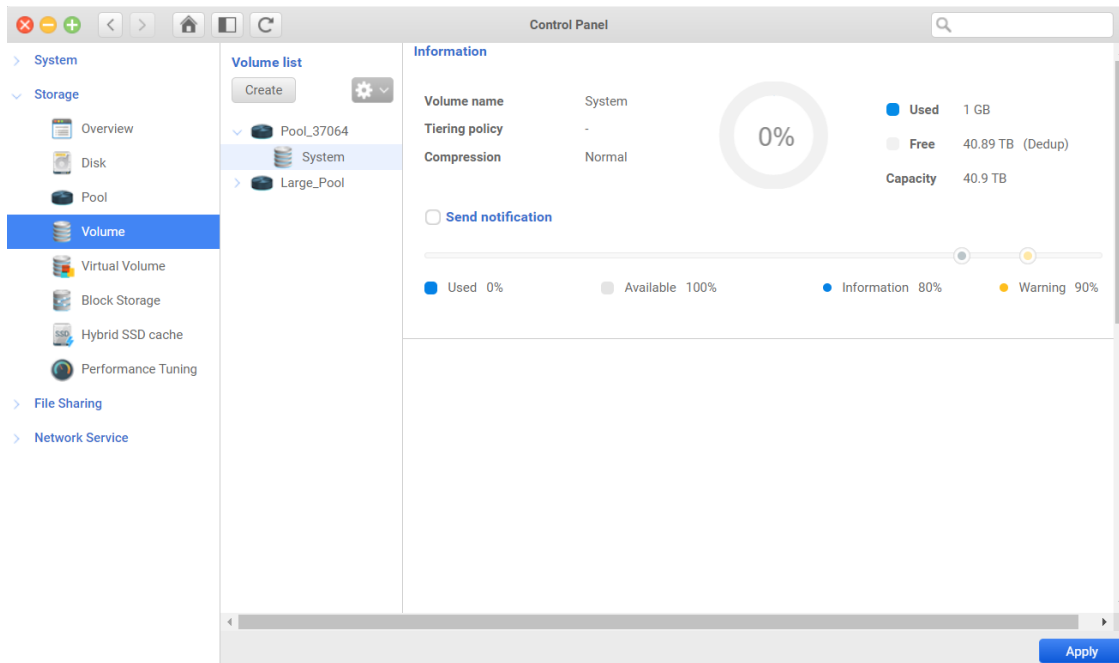
3.2.4. Volume

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



INFORMATION:

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

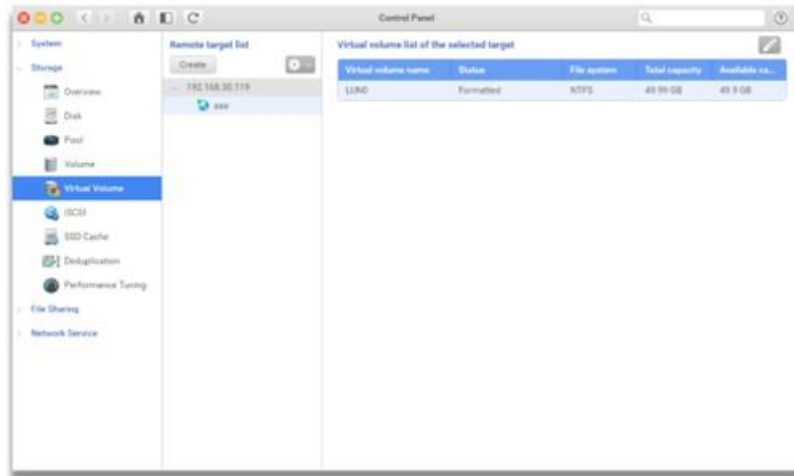
When the volume is no longer needed, you can delete the volume after all shared folder is deleted.

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.

3.2.5. 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 ONYX Series 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.



INFORMATION:

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 right away.

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 out.
5. Specify the CHAP authentication.
6. Click **Confirm** to finish the action.

IQN

For system administrators, we provide a convenience feature 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:

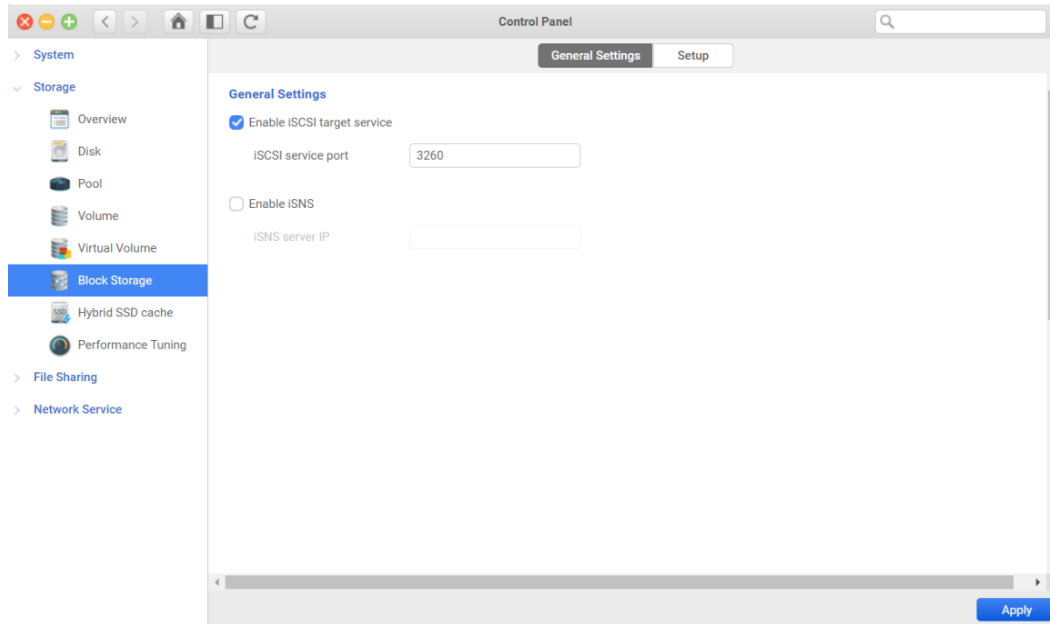
1. Select a virtual volume on the remote target list.
2. Click the function button on the top right-hand side of remote target list.
3. Click **Delete**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

3.2.6. Block Storage

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

General Settings

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



INFORMATION:

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 ONYX Series.

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



INFORMATION:

This target service is default on.

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



INFORMATION:
Default port is 3260.

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

Enable iSNS

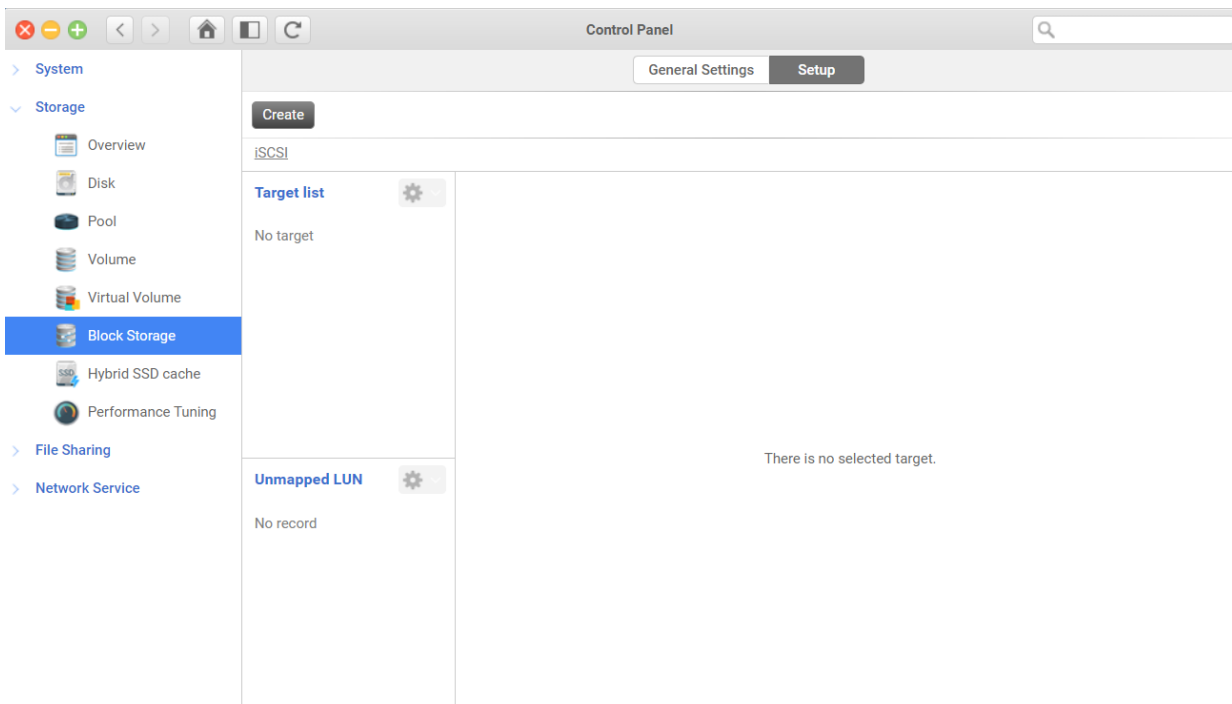
iSNS server provides intelligent storage discovery and management services comparable to those found in your networks.

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

1. Enter the IP address.
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

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 out.
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 automatically mapped to the LUN 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 a 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 Map an iSCSI target. In this create scenario, the LUN will be automatically mapped to the LUN you just created.
- ⑧ Click **Next**.
- ⑨ Check the creating summary.
- ⑩ Click **Confirm** to finish the action.



INFORMATION:

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. 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. Head 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. During an iSCSI session, it supports multiple sessions between different initiators.
-

Turn on/off the 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 switch button. When the target is off, it shows off.
3. After the button is clicked, the service 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 by just one click.

To delete the target, please follow the steps below:



TIP:

The target can only be deleted when there no LUN mapped on 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 a LUN

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

To edit a LUN, please follow the steps below:

1. Select a 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 **Confirm** to finish the action.

Take a snapshot for a LUN

Ensure the data security is the most important thing on ONYX Series. You can easily take a snapshot for your LUN.

To take a snapshot, please follow the steps below:

1. Select a 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 capacity.

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/unmap the LUN.
6. Check the summary for the editing.
7. Click **Confirm** to finish the action.

Delete a LUN

When the LUN is no longer needed, you can delete it just by one click.

To delete a LUN, please follow the steps below:

1. Select a 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.



INFORMATION:

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

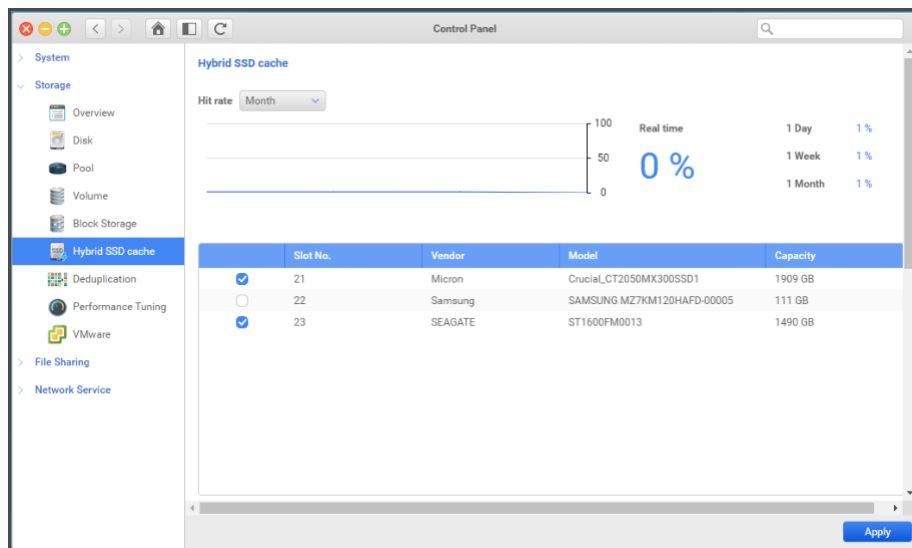
To add/edit/delete masking, please follow the steps below:

1. Select a 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.

3.2.7. SSD Cache

In **SSD Cache**, you can check and manage all your caches for your system. SSD cache can improve the random read performance. Meanwhile, one single SSD can provide both read and write cache to your storage.



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. Select the SSD.
2. Click Apply to finish the action.

Delete Cache

When the cache is no longer needed, you can delete the cache by simply one click.

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

1. Select the SSD from the SSD list.
2. Click out the checkbox.
3. Click **Apply** to finish the setting.

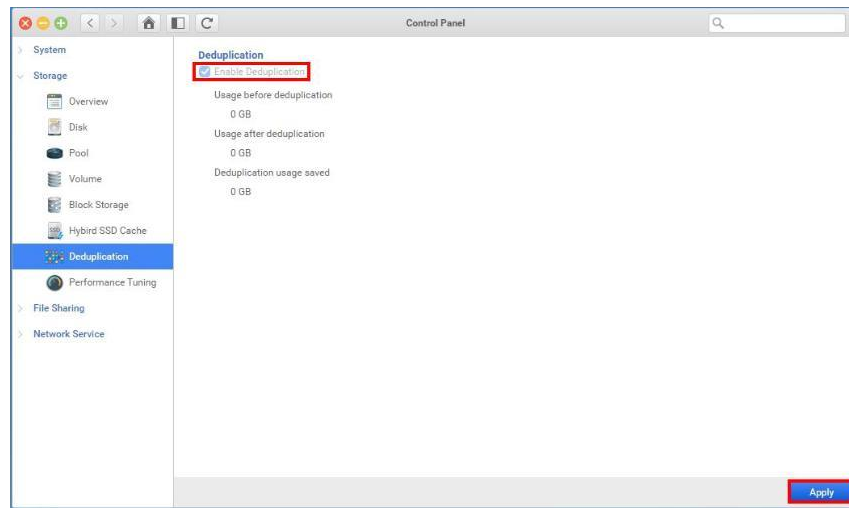
3.2.8. Deduplication

In **Deduplication**, you can check how this feature takes effect of you ONYX Series. It makes your storage capacity more efficiently and lowers the capacity requirement.

Enable the deduplication

To save more data capacity on your system, you can simply click one button to set it up.

To enable the deduplication, please follow the steps below:



TIP:

Before using deduplication, you have to assign at least two SSDs with minimum 480GB for Hybrid SSD cache.

1. Click **Enable**.
2. Click **Apply** to finish the action.



INFORMATION:

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



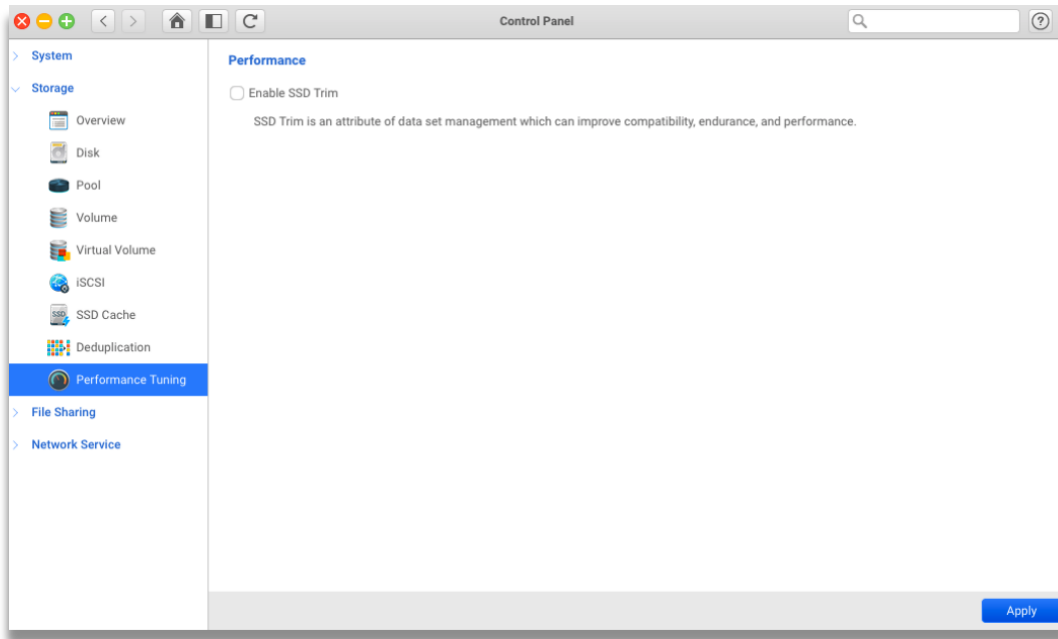
CAUTION:

Deduplication can't be disabled once its enabled, be sure when you try to enable it.

You need at least two SSDs for deduplication, and if two SSD fail, it will cause your pool fail, please be aware of your SSDs' endurance.

3.2.9. 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 improve the SSDs performance and compatibility on ONYX Series, 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 on the ONYX Series will be affected.

3.3. File Sharing

3.3.1. User

On **User** page, you can flexibly create and manage individual users when accessing ONYX Series.

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 VESQ.
 - **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.

**INFORMATION:**

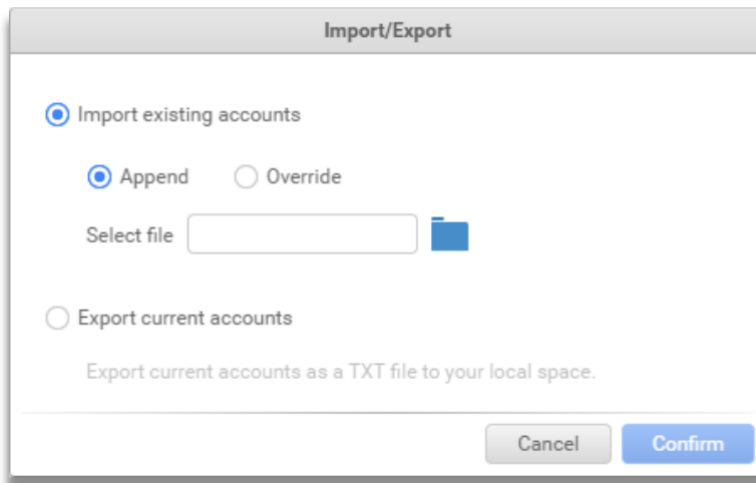
- The description is limited up to 512 characters.
- The maximum user number is 2048.

User Naming Rule:

1. Admin account is a special administrator account for managing ONYX Series. 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- _”.

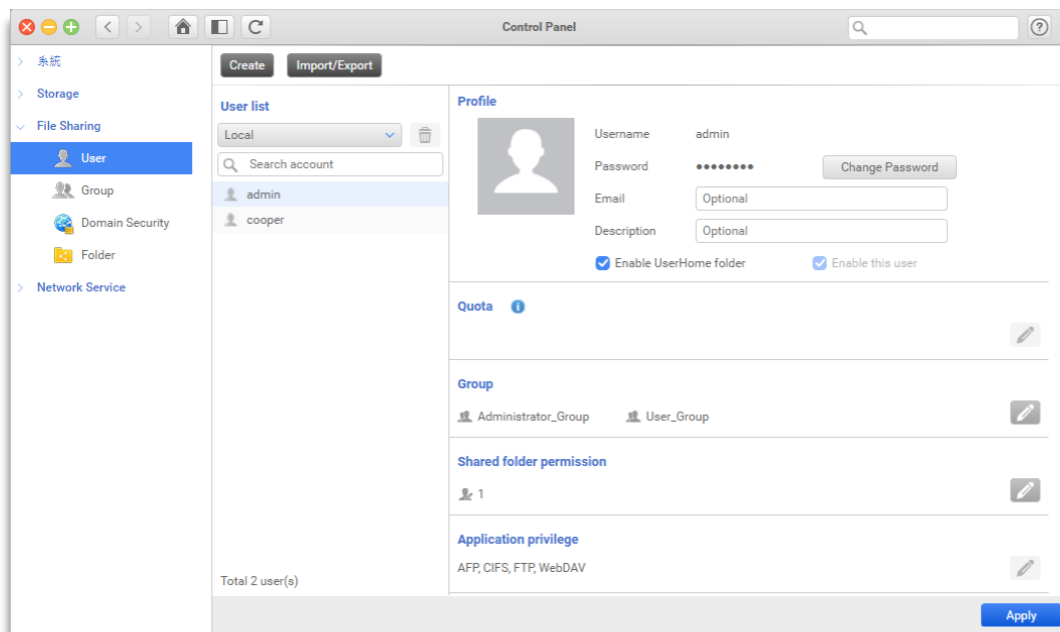
Import or Export Users and Groups

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

3.3.2. 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.

INFORMATION:



- 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.

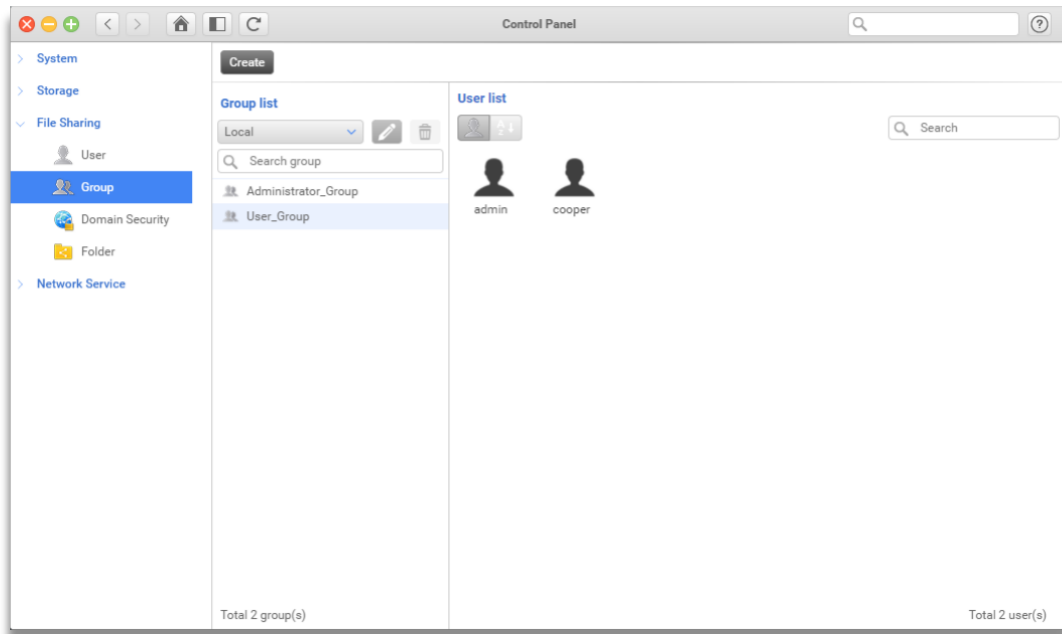
Group Naming Rule:

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 led 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.

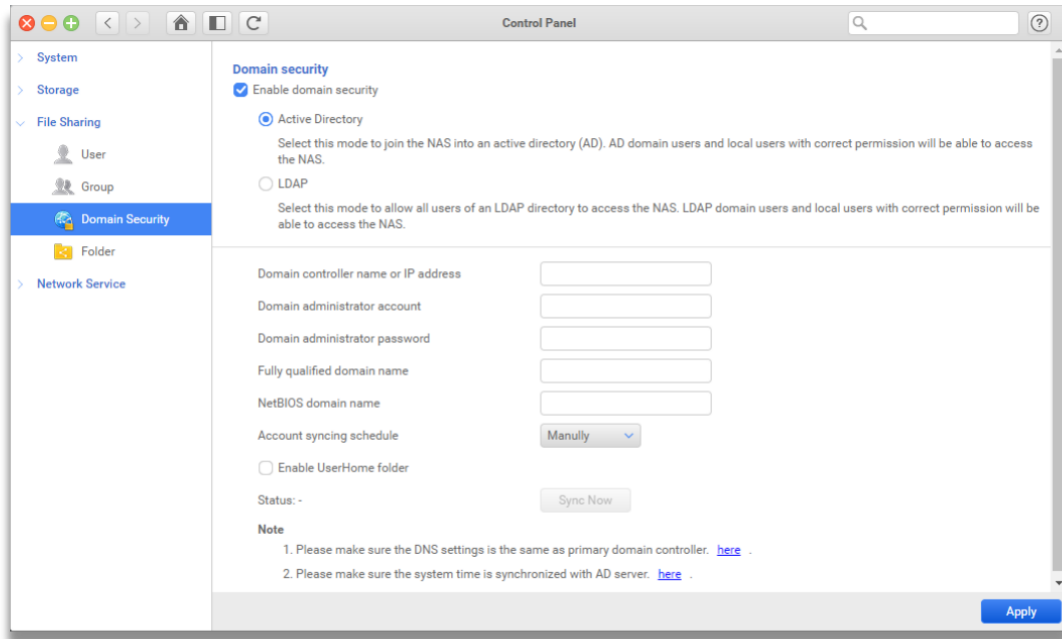
To delete a group, please follow steps below:

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

3.3.3. Domain Security

You can join your ONYX Series to a domain server and allow domain accounts to log in VESQ.

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.

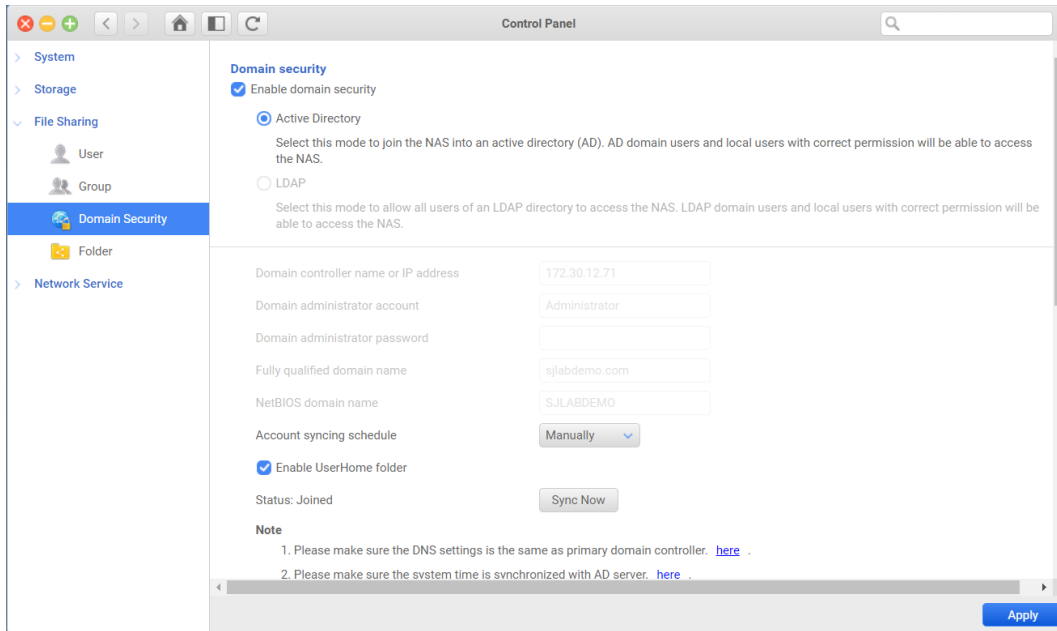
You can set **Account syncing schedule** to synchronize with AD server periodically. If you would like every AD user to have its own Home folder, select **Enable UserHome folder** .



TIP:

- 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 .



INFORMATION:

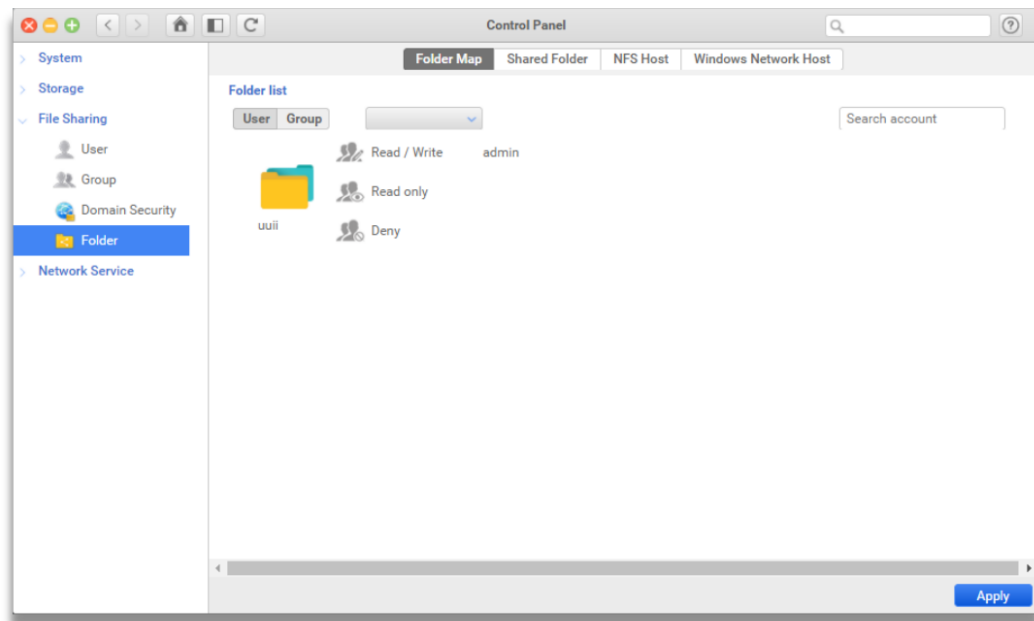
- After joining in LDAP, you cannot set Windows ACL permission from VESQ.
- Joining in LDAP server will cause local users cannot log in CIFS service.

3.3.4. Folder

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

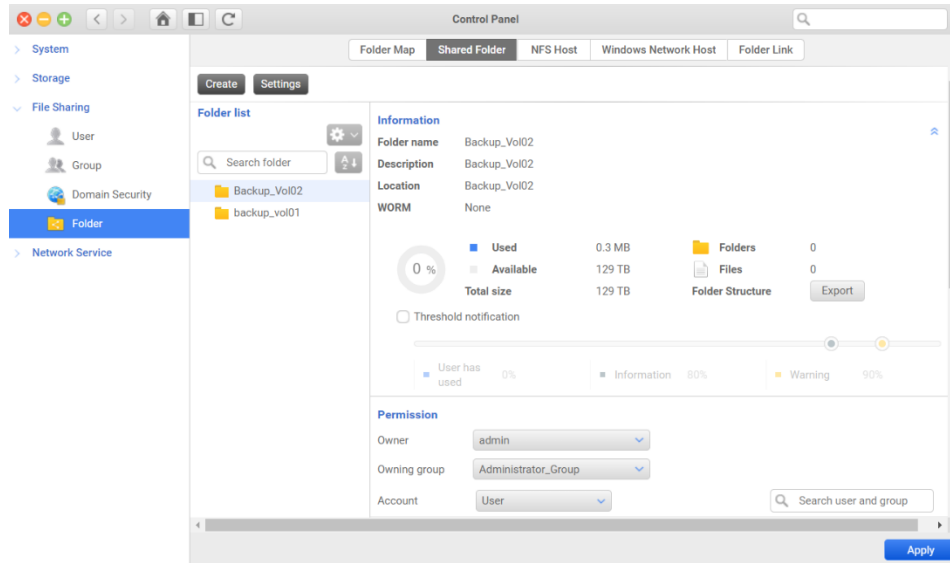
Folder Map

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 ONYX Series 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.



INFORMATION:

Requirement: A local data volume or a virtual volume.

Create Folder

Create Folder

Folder name

Description

Location Backup_Vol01 ▼

The folder will share the size of Backup_Vol01. You can also enable folder size and reserve capacity for the folder.

Folder size (Reserved capacity) GB

Hide Network Drive

Enable Access Based Share Enum

Enable Recycle Bin

Anonymous login Read only ▼

Enable File Retention Days delete files. Advance

When this feature is enabled, if the file has not been opened within the set time, it will be automatically deleted.

Cancel
Confirm

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.



INFORMATION:

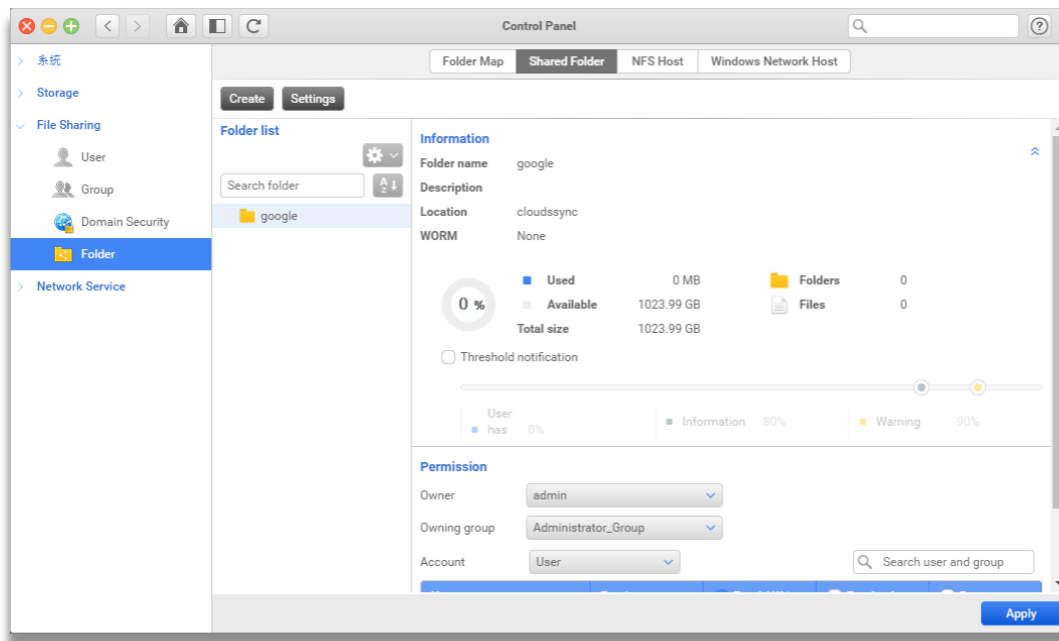
- The maximum shared folder number is 2048.
- Hiding a shared folder doesn’t affect its permission. A user who has proper access right can still access the shared folder by entering its path.

Shared Folder Naming Rule:

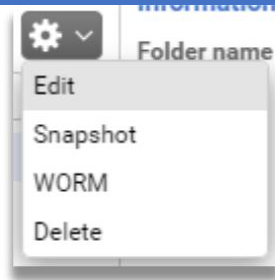
1. The maximum length of shared folder name is up to 128 characters.
2. A folder name can be alphabets, numbers but cannot contain following special characters: “ `~!@#\$%^&*()=+[]{}|\/;:” ’ , < > ? % ”.
3. The first character and the last character of a shared folder name cannot be “ . ”.
4. The character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

Shared Folder Management

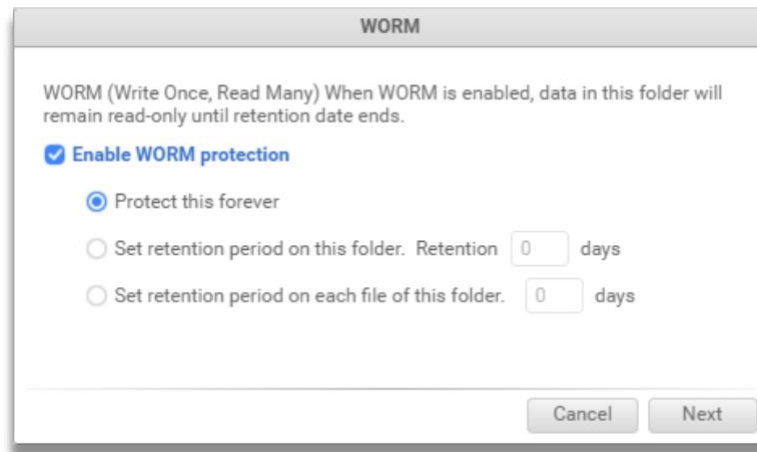
The **Information** section shows the basic settings and space utilization of the shared folder. You can check the status of the shared folder and whether WORM protection is enabled. The space usage is also presented for you to know how much space is available for storing data. You can set notification 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 led 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 remained 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:

- **Forever protection:** 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 counting from the time being added in.
4. **Delete:** Delete the shared folder.



INFORMATION:

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:

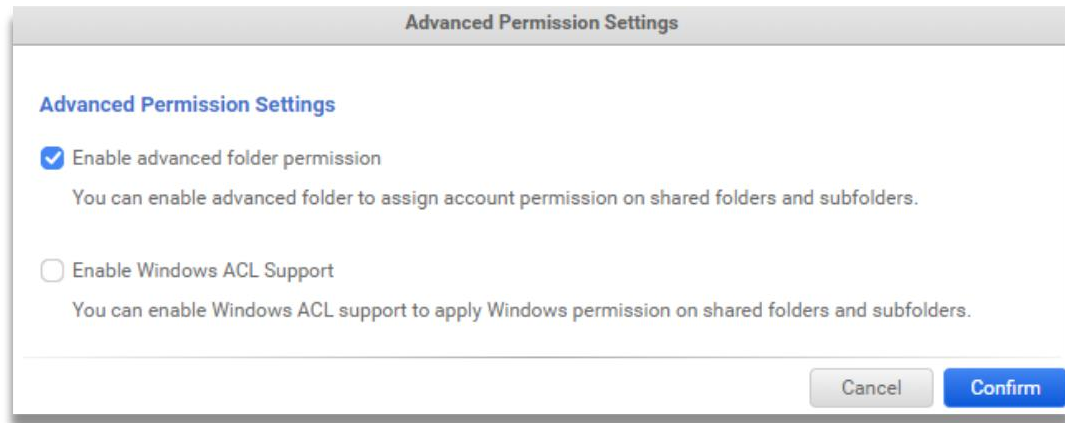
1. Change the user or account permission by selecting corresponding permission checkboxes.
2. Click **Apply** button and the new permission will take effect.

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.



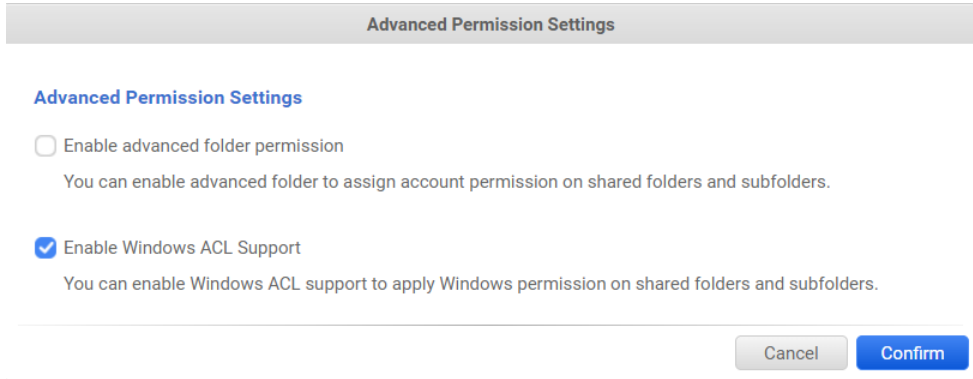
INFORMATION:

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 VESQ or Windows File Explorer to subfolders and files by steps below:

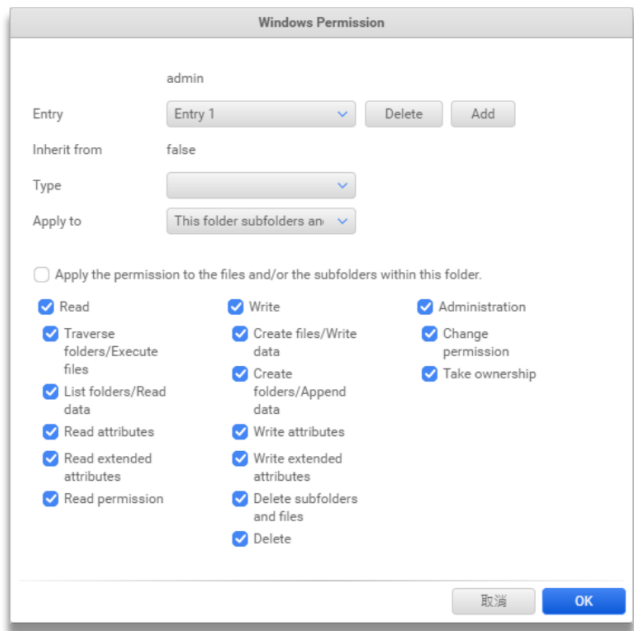
1. Click **Settings** button and **Advanced Permission Settings** Window will pop out.
2. Select **Windows ACL support** checkbox.
3. Click **Confirm** button.



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.

**INFORMATION:**

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

Permission Judgment

ONYX Series 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:

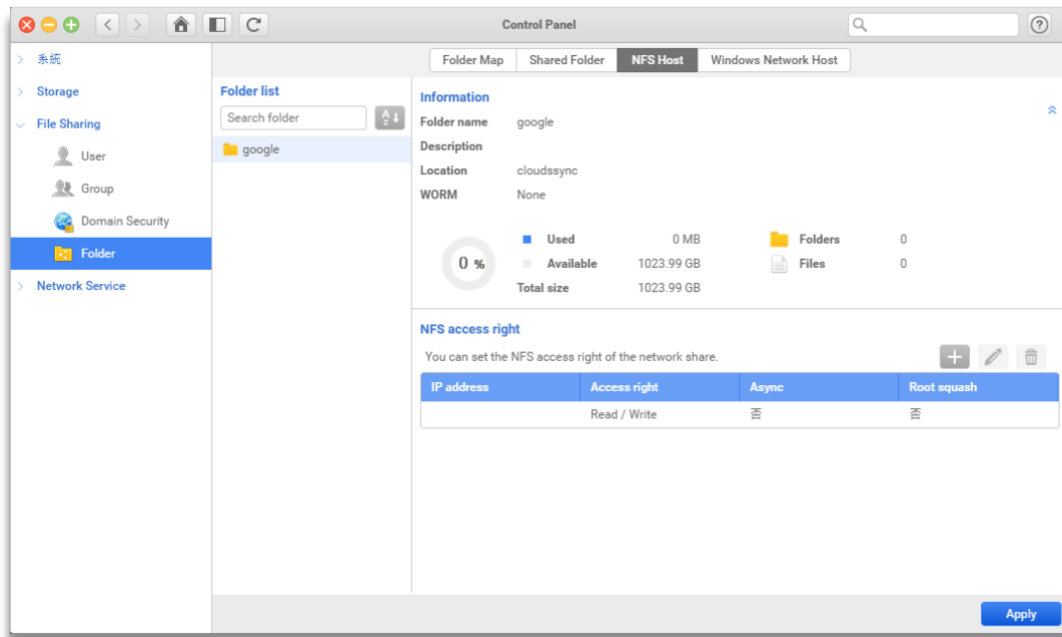
Shared folder permission	Subfolder permission	Behavior when accessing the subfolder
Read/Write	Read-only	Read-only
Read-only	Read/Write	Read-only
Not set	Read/Write	Denied
Read-only	Not set	Denied

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

VESQ 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 VESQ.

- **Async write:** Select this option if you don't want to execute write command immediately.
5. Click **Confirm** button.

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

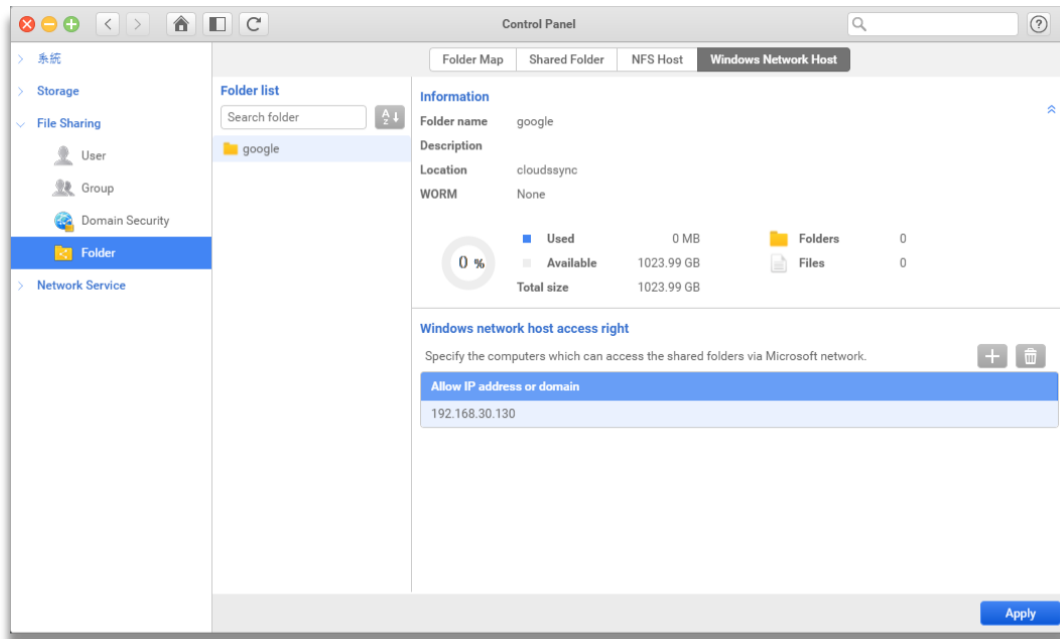
1. Select an access right and click **Edit** button. The **NFS Host Access Right** window will pop out.
2. You can change **IP address or domain**, **Access right**, **Root squash** or **Async write**.
3. Click **Confirm** button.

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 ONYX Series 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.

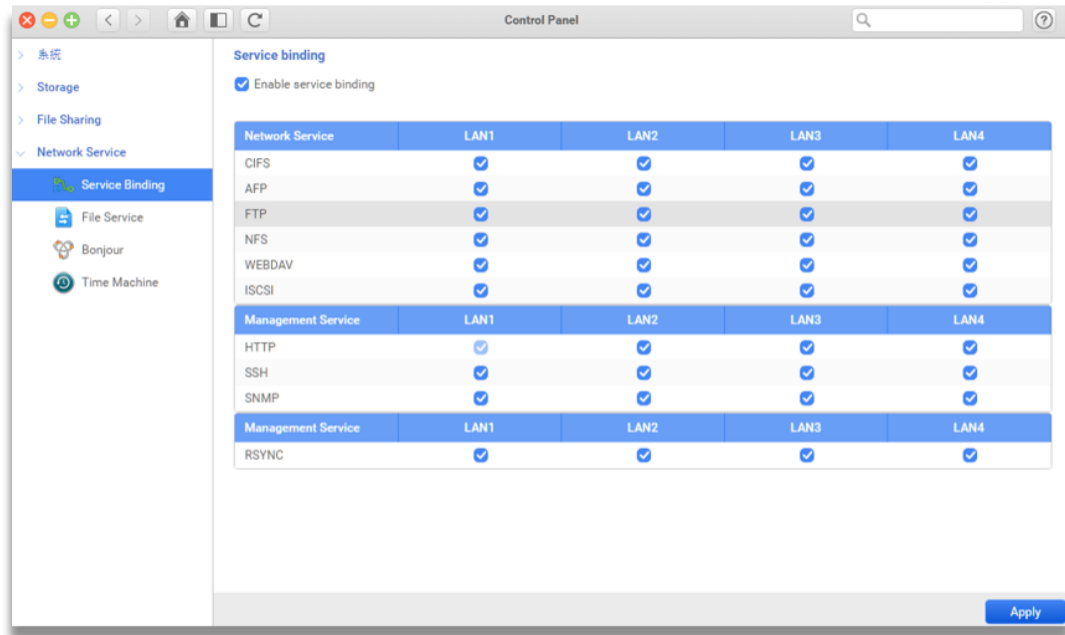
To delete a Windows network host access right, please follow steps below:

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

3.4. Network Service

3.4.1. Service Binding

The ONYX Series **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 ONYX Series.

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.



INFORMATION:

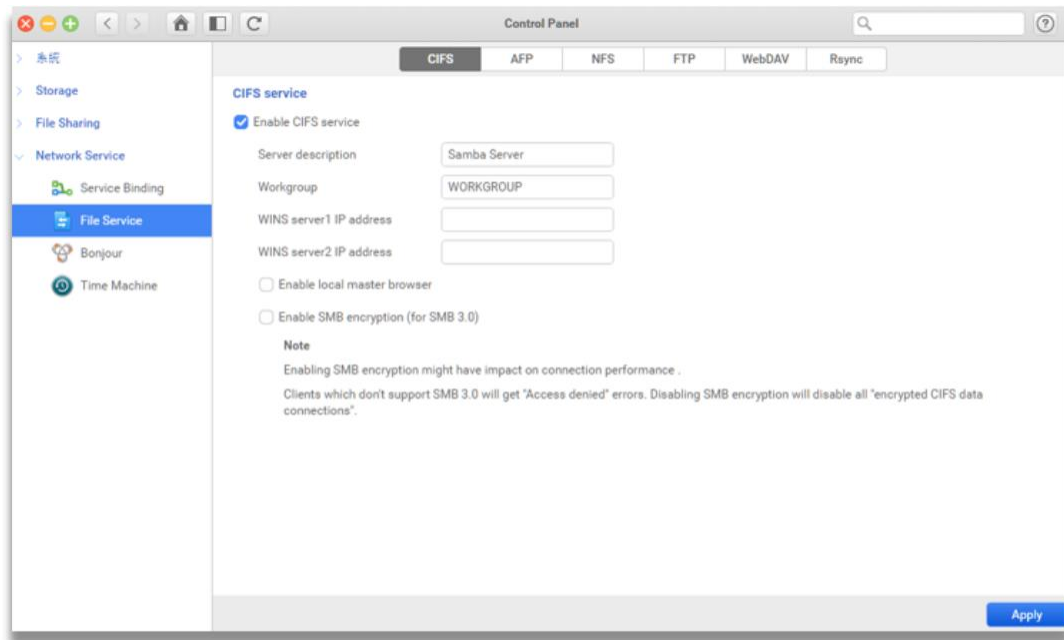
1. The currently connecting interface is not allowed to change on the service binding table. Location can be volumes or virtual volumes.
2. After clicking Apply button, all the data service will be restarted. All connected users need to reconnect to the ONYX Series via the selected interface(s).

3.4.2. File Service

With the multiple services supported, you can easily share files by ONYX Series.

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:

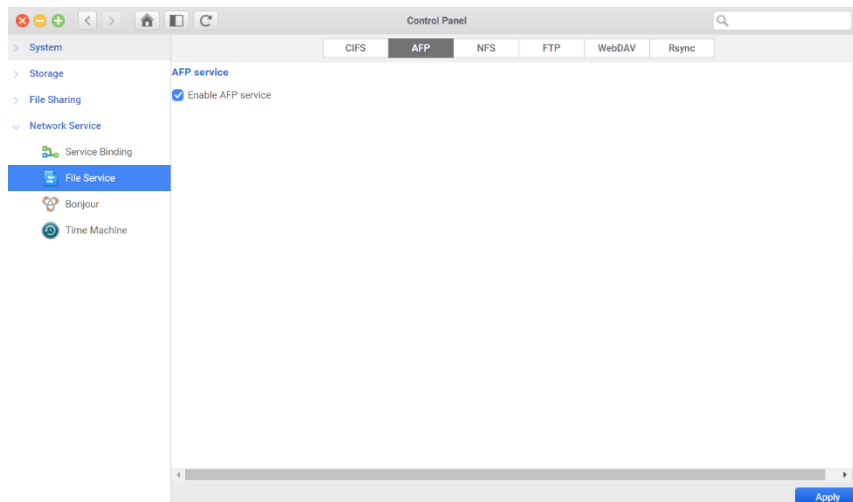
1. Select the **Enable CIFS service** checkbox.
2. In the **Server Description** text box, provide a name for the server.
3. In the **Workgroup** text box, provide a name for the workgroup.
4. In the **WINS Server IP Addresses** text box, provide the IP address for WINS server 1 and/or 2.
5. If you want 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.

**INFORMATION:**

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, that 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 ONYX Series 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 pier to pier 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:

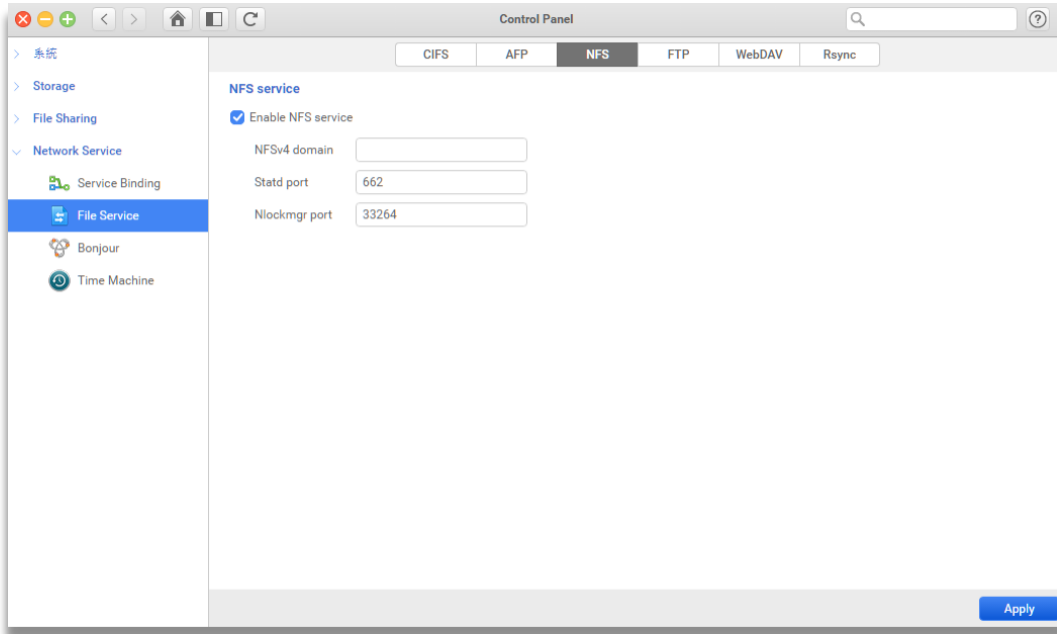
1. Select the **Enable AFP service** checkbox.
2. Click **Apply** button and finish the setting.

**TIP:**

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 ONYX Series.



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.

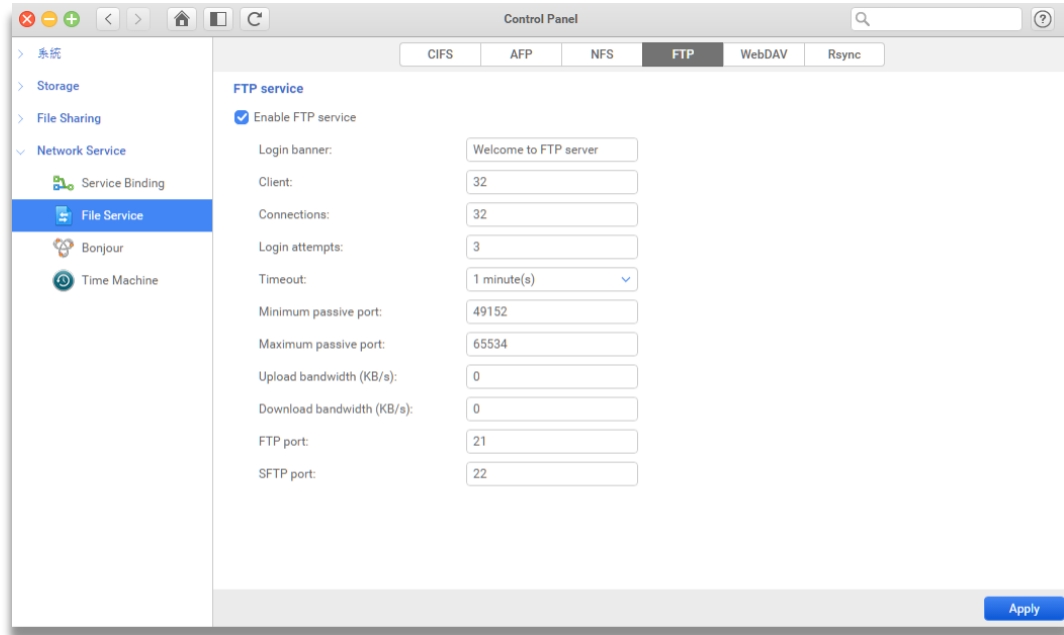


INFORMATION:

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 for a user can use FTP service before being automatically logged 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.

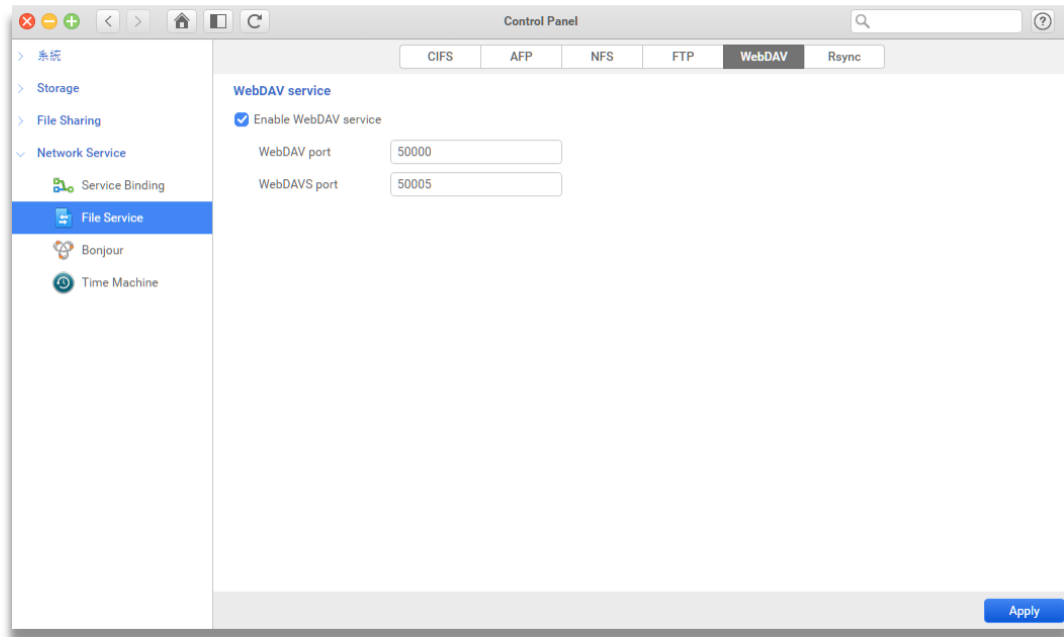
9. In the **Upload Bandwidth** text box, enter the maximum bandwidth when uploading data.
10. In the **Download Bandwidth** text box, enter the maximum bandwidth when downloading data.
11. In the **FTP port** text box, enter the port number that the FTP service used to communicate with other devices.
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.

**INFORMATION:**

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.

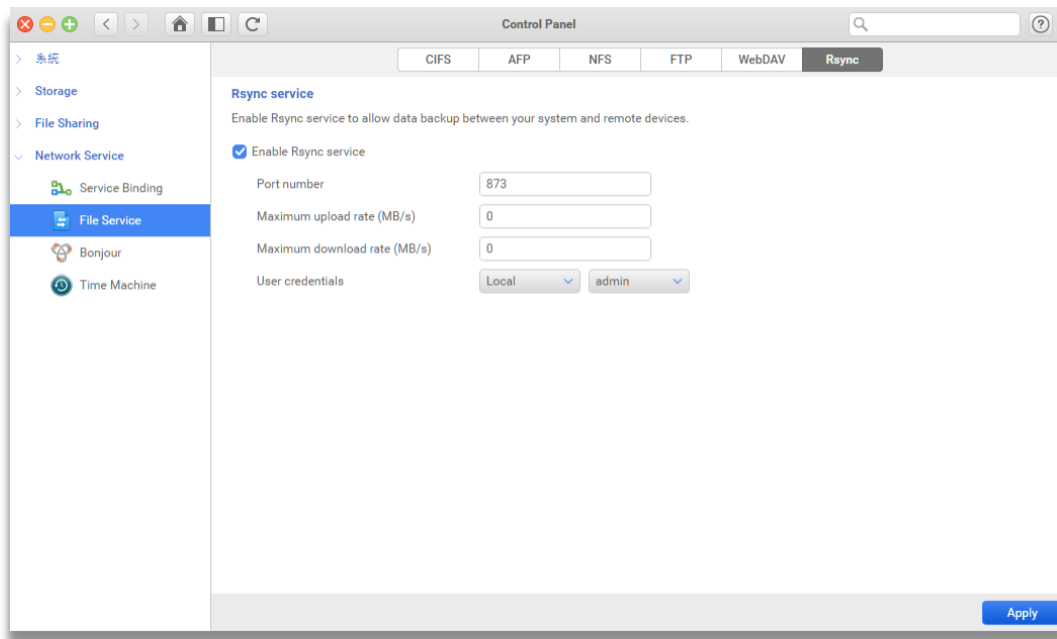


INFORMATION:

The default port for WebDAV and WebDAVS are 50000 and 50005.

Rsync

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



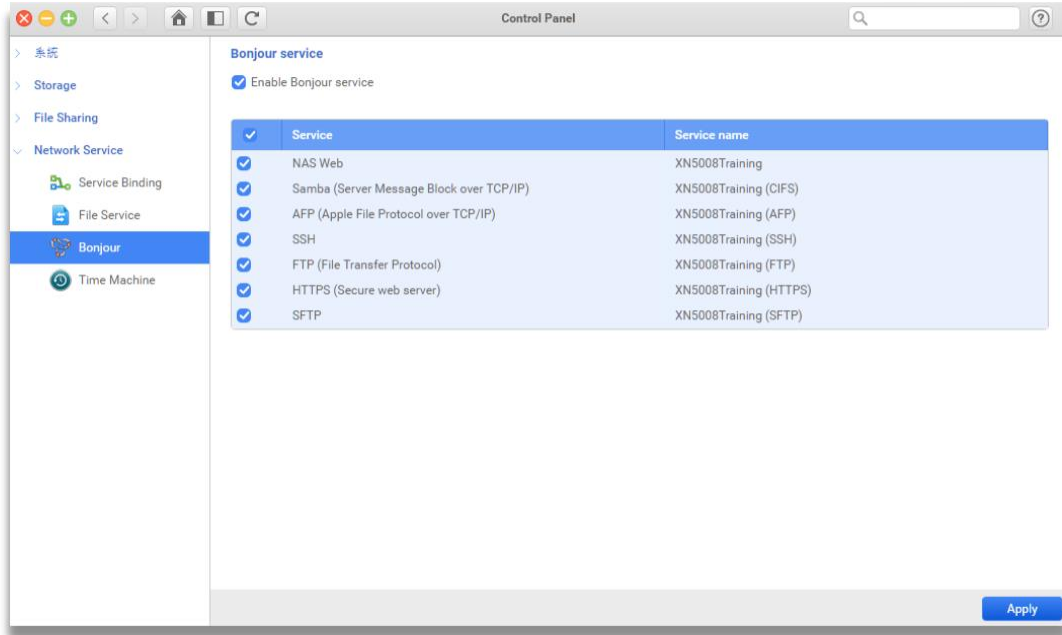
To enable Rsync

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.
4. In the **Maximum download rate** text box, enter the maximum download rate when downloading data.
5. In the **User Credentials** section, select the user credentials
6. Click **Apply** button and finish the setting.

3.4.3. Bonjour

The ONYX Series 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 ONYX Series 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.



INFORMATION:

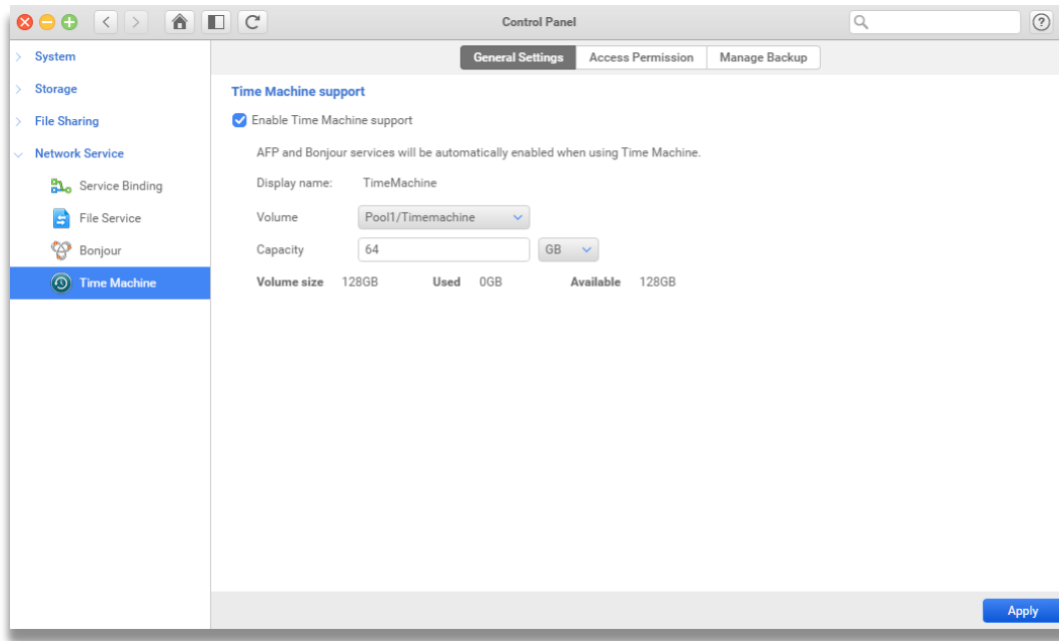
The service name is based on your device name.

3.4.4. TimeMachine

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 ONYX Series.



Time machine support

ONYX Series 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 ONYX Series.
3. Enter the **Capacity** to reserve the capacity for Time machine.
4. Click **Apply** button and finish the setting.

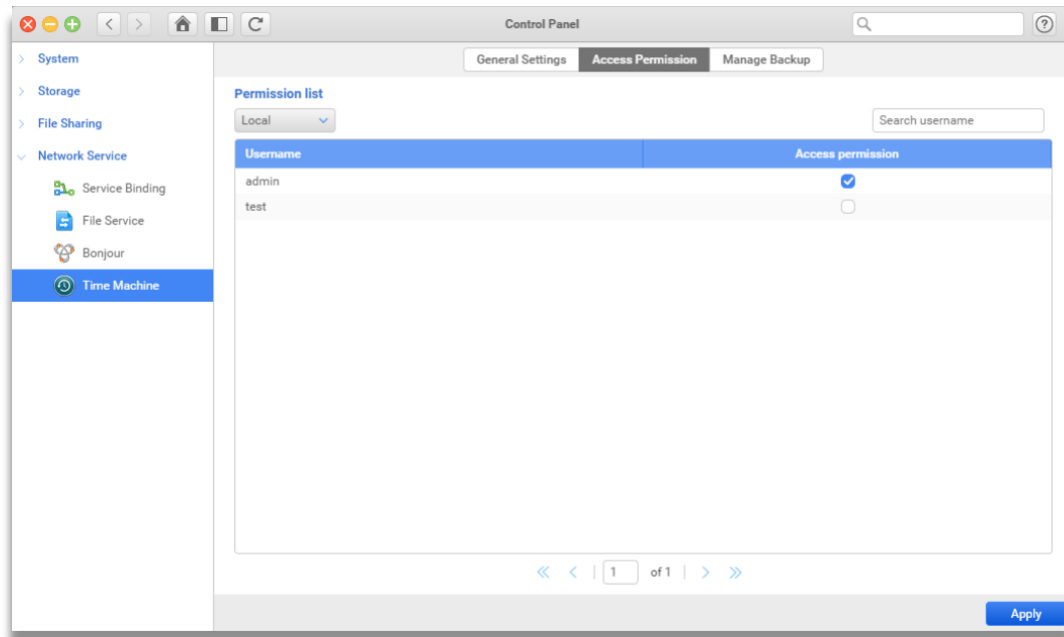


INFORMATION:

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

Access Permission

ONYX Series 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

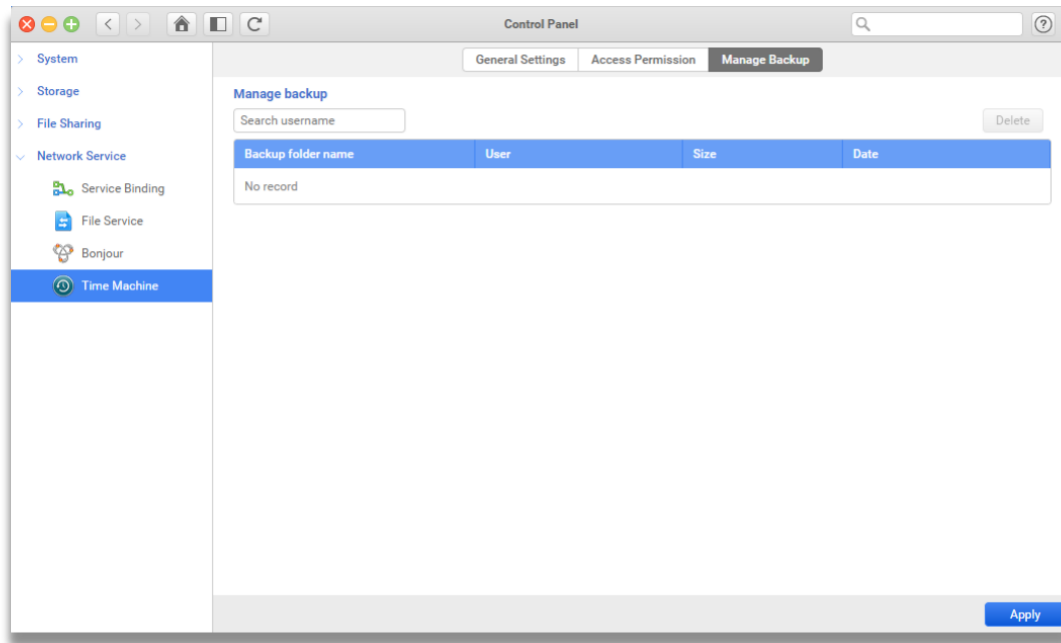
You can setup the user privilege of using Time Machine.

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.

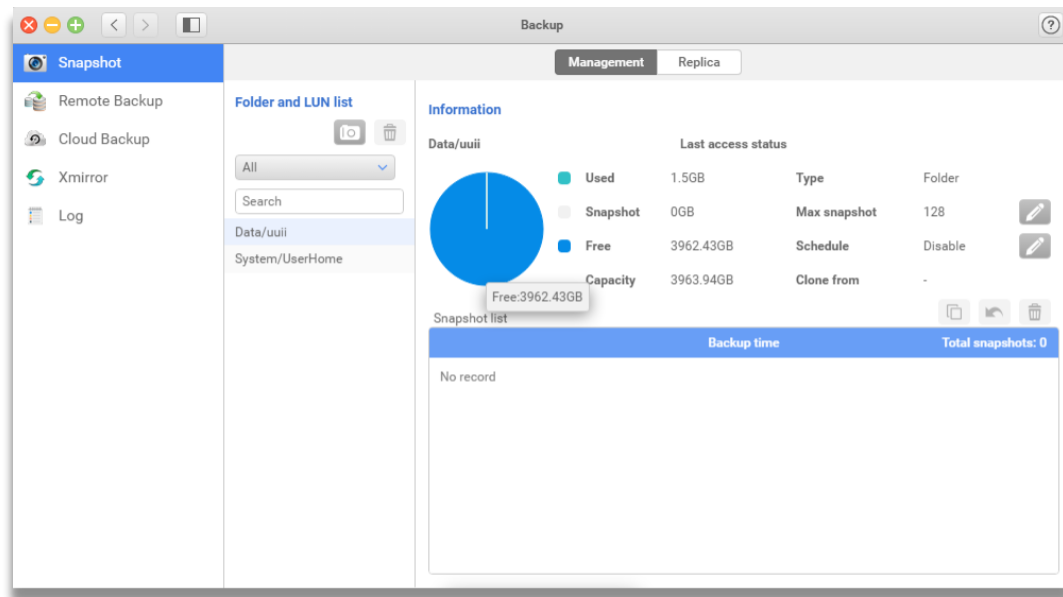
4.0 Backup

4.1. 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 folders or LUN, 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 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. 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.



INFORMATION:

1. Maximum snapshots for the entire system is 4096.
 2. Default snapshot amount for a shared folder or LUN is 8.
 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.



INFORMATION:

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.

**INFORMATION:**

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.

**INFORMATION:**

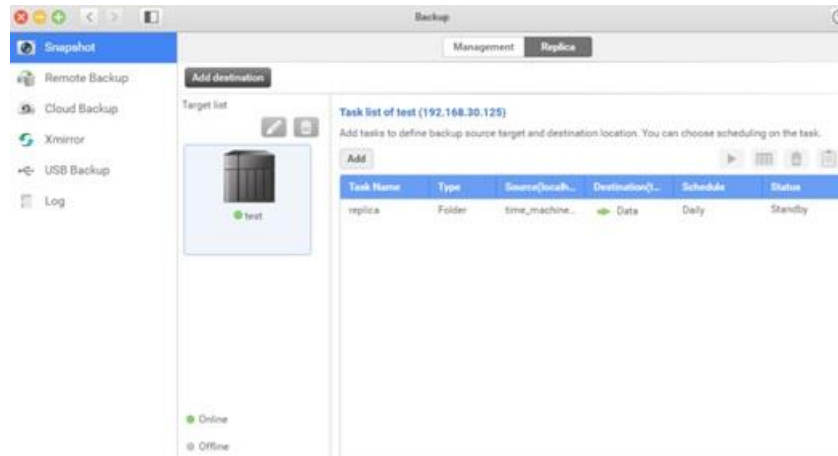
All data will back the date you select to roll back including snapshots.

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. Meanwhile, you can create, edit, delete, and schedule for a replica task.

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

1. Click **Add destination** button on the top left corner of the window.
2. Select the **Dedicated LAN** for your remote destination.



INFORMATION:

Default setting for dedicated LAN is Auto, which means, all interfaces including Thunderbolt 3 (Optional).

3. Enter the IP address / Host name of your remote destination.



TIP:

By clicking the drop-down menu, you can find all ONYX Series on the same network.

4. Enter a name for your Target.



INFORMATION: 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.

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 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**.



INFORMATION:

- 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.



INFORMATION:

- 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:

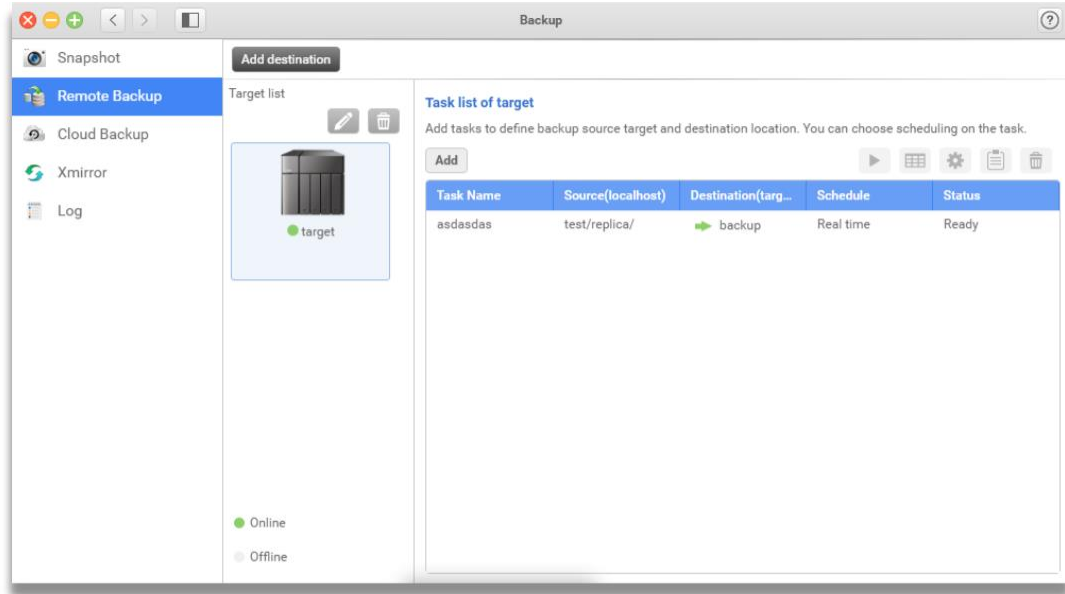
1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. The confirm window will pop out. Click **Confirm** button to delete the task.

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.

4.2. Remote Backup

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



How to add a destination

Before backing up your file to the remote site, you will need to add at least one destination to store your files. Meanwhile, you can create, edit, delete, set file backup policy and schedule for a remote backup task.



TIP:

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.



TIP:

By clicking the drop-down menu, you can find all ONYX Series on the same network.

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



INFORMATION: 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)



TIP:

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 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 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**.



INFORMATION:

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.



INFORMATION:

- 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:

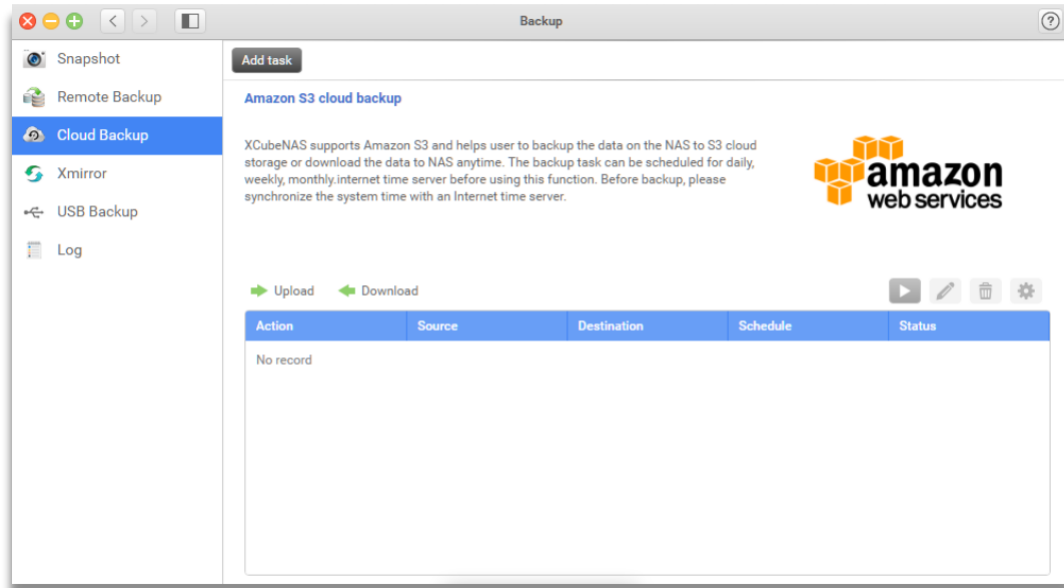
1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Log** button.
4. The detail information window will pop out. Click **OK** button to close the window.

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.

4.3. Cloud Backup

In **Cloud Backup**, ONYX Series supports the public cloud, Amazon web services (S3) and S3 compatible services, as the backup/restoration solutions to save your data with an additional off-site copy to prevent unexpected data loss from disks failures 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.



TIP:

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 ONYX Series 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.

**TIP:**

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 ONYX Series 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** on the confirmation window to delete the task.

To set the option for the task

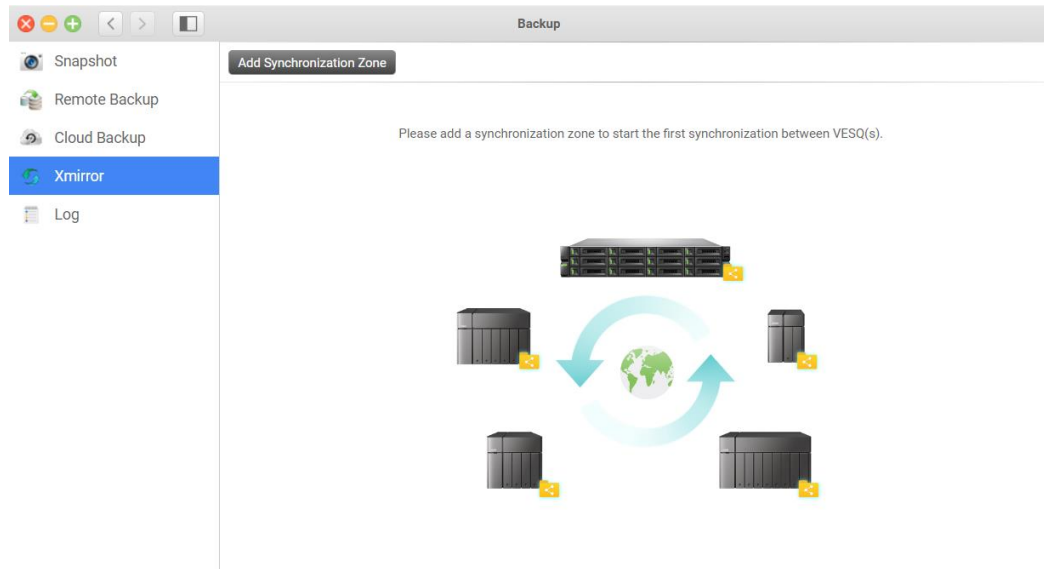
While backing up data, you can make your backup more secure.

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.

4.4. XMirror

In **Xmirror**, you can backup or synchronize your files between multiple ONYX Series over Internet or local network.



Sync your data in a zone

With our unique technology, Xmirror, you can easily sync files between different ONYX Series by joining an existing zone or create a new zone.



INFORMATION:

1. Before using Xmirror, you will need at least one shared folder on your ONYX Series.
2. Only one local folder in a zone.

To create a new zone or join an existing zoon, please follow the steps below:

1. Click **Add Synchronize 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 1-way zone or 2-way zone.

**INFORMATION:**

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 ONYX Series.
 - 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.

**TIP:**

You can click the dropdown menu to find all available ONYX Series.

- 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.

**INFORMATION:**

After the zone is created, the zone is default start to sync.

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 the zone, please follow the steps below:

**TIP:**

Before deleting the zone, you need to stop the synchronization first.

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.

**INFORMATION:**

The option is default on.

3. Specify the file filter while syncing. By clicking the checkbox, you can set the excluded file type or specify a particular file type.

**TIP:**

By setting up multiple file format, you can enter the words as following, *.abc, *.bbb and etc.

4. Set up the maximum previous versions for each file.

**INFORMATION:**

1. Default maximum previous versions is 1
 2. When you lower the maximum previous versions amounts, the 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 roll back 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.

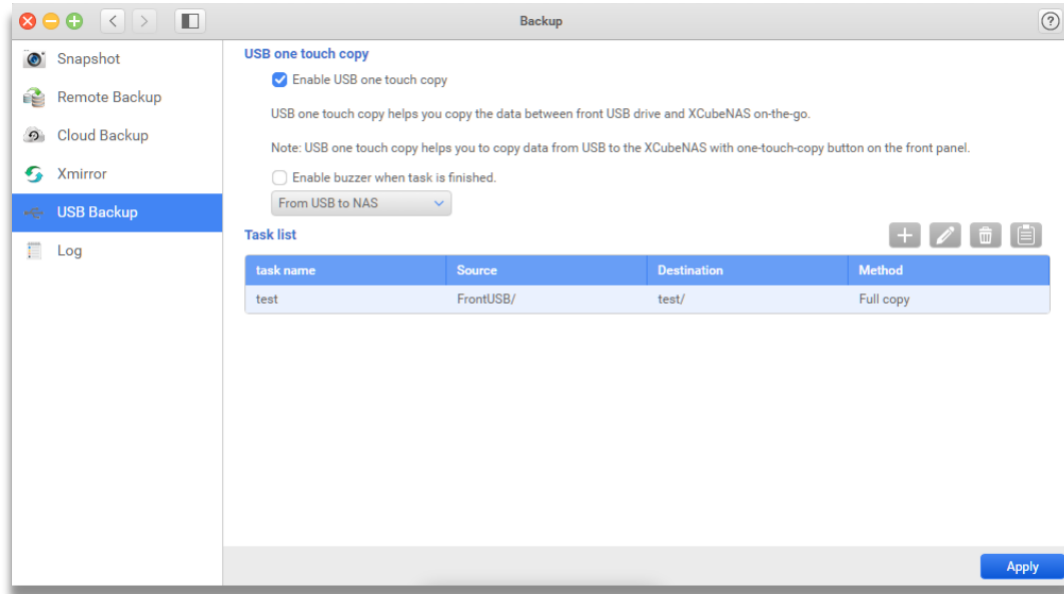


TIP:

When the folder is not able to sync, it is usually caused by the availability of the folder capacity. Please check its availability and edit its settings before clicking **Restart**.

4.5. USB Backup

In **USB Backup**, VESQ supports USB backup between the ONYX Series and external USB drives or storage devices by simply one touch on the front panel of ONYX Series.



In overview page, you can add, view the current task list, add a task, edit or delete a task and check the information of tasks. USB backup can be even more convenient. You can simply check the backup task completion by the buzzer if you click **Enable buzzer when task is finished**. Meanwhile, you can backup your sensitive data from a USB drive to ONYX Series or back it up in the opposite direction, ONYX Series to a USB drive.

Add a task

USB one touch backup is a task basis function. By adding the tasks, you can custom tasks for your USB devices.



TIP:

Before adding the task, you need to click enable USB one touch copy and 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**.

**TIP:**

Source and destination can be selected to up to folder-level.

5. Select the copy method, **Full copy**, **Incremental copy**, and **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. Edit the copy method.
5. Check the summary of the task.
6. 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** 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** on the confirmation window to delete the task.

View the information of the task

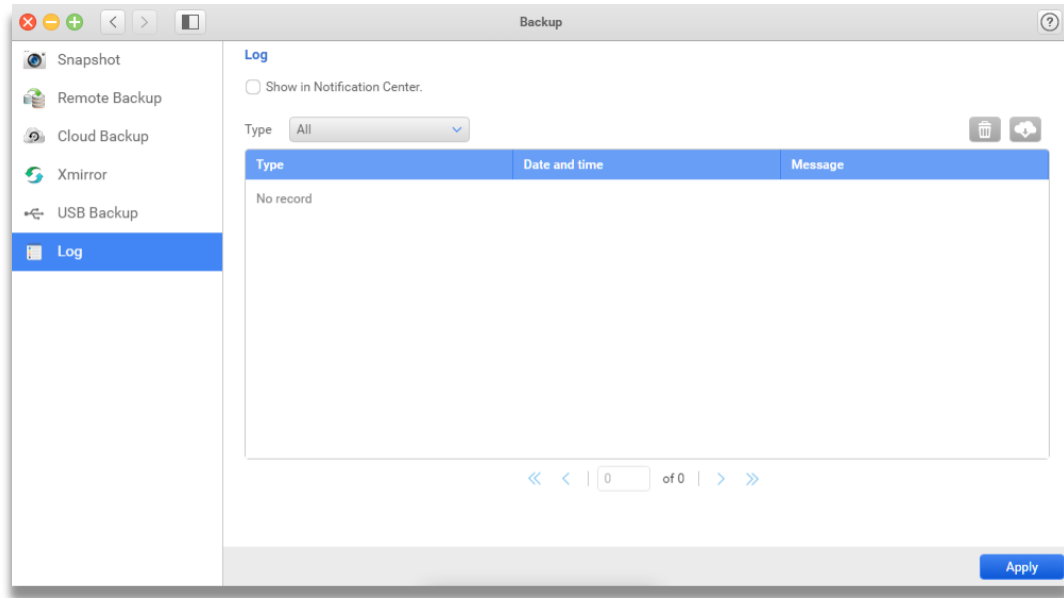
You can check the detail information of the task for its type, source, destination, create time, last access time, and last access status.

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.

4.6. 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 ONYX Series.



How to show events in notification center

Notification center is the desktop function which helps the administrator to monitor ONYX Series 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.



INFORMATION:

The log file will be shown as LOG-Host name-Date-Time.txt

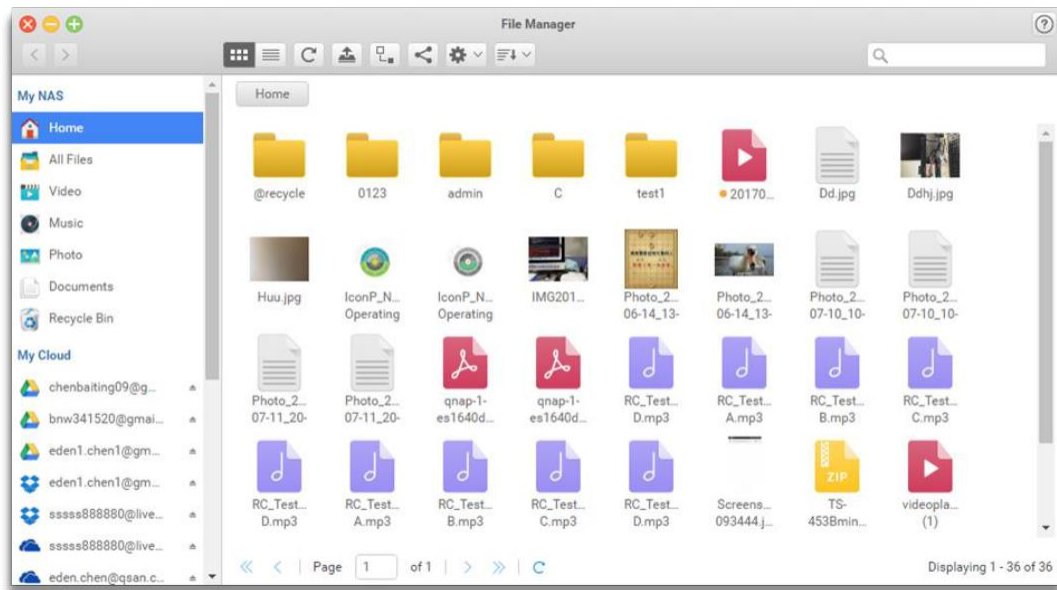
5.0 File Manager

5.1. File Manager

File Manager is a web-based file management center for ONYX Series. you can oragnize photo, music, video and document on File Manager when **Media Library** is enabled. Besides, 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:

If you want to have good experience in File Manager, please make sure your web browser is the newest version.



Start to use File Manager:

There are two operation areas of File Manager. Please refer to the introduction below before getting started:

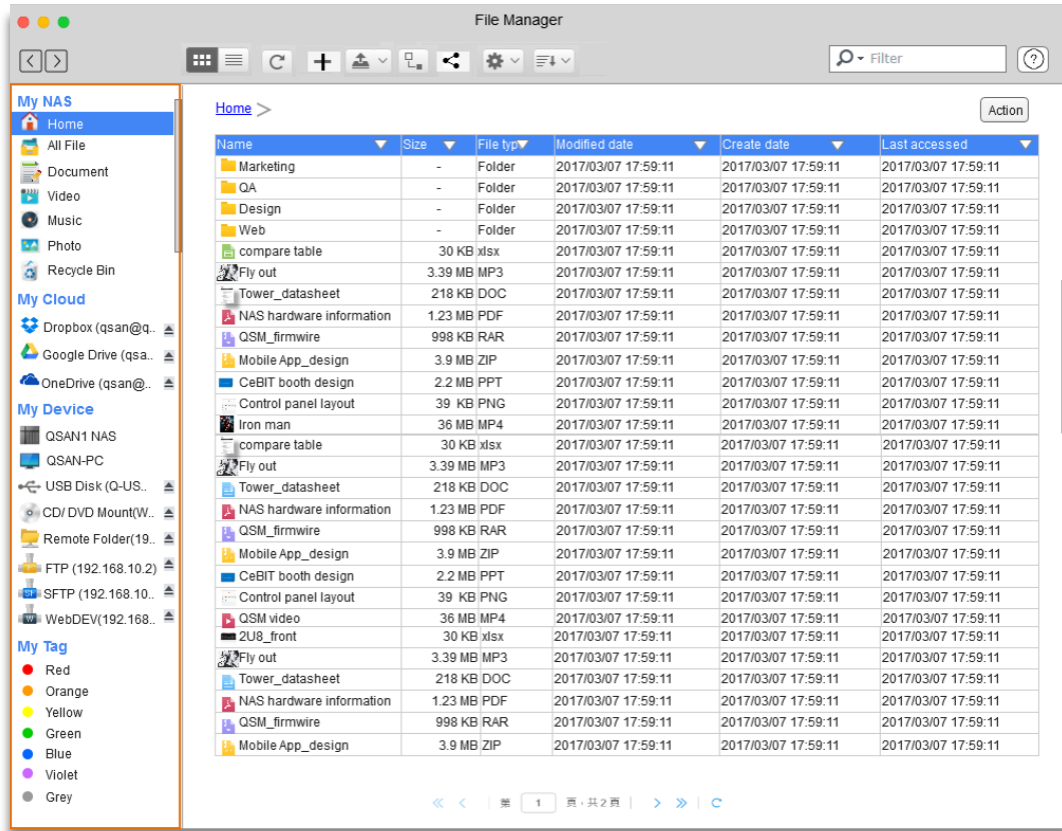
1. Toolbar



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

ONYX Series supports Google Drive, Dropbox, OneDrive to mount your public cloud drive on File Manager.

- My Device

My Device lists all the attached devices by ONYX Series. 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. ONYX Series 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:

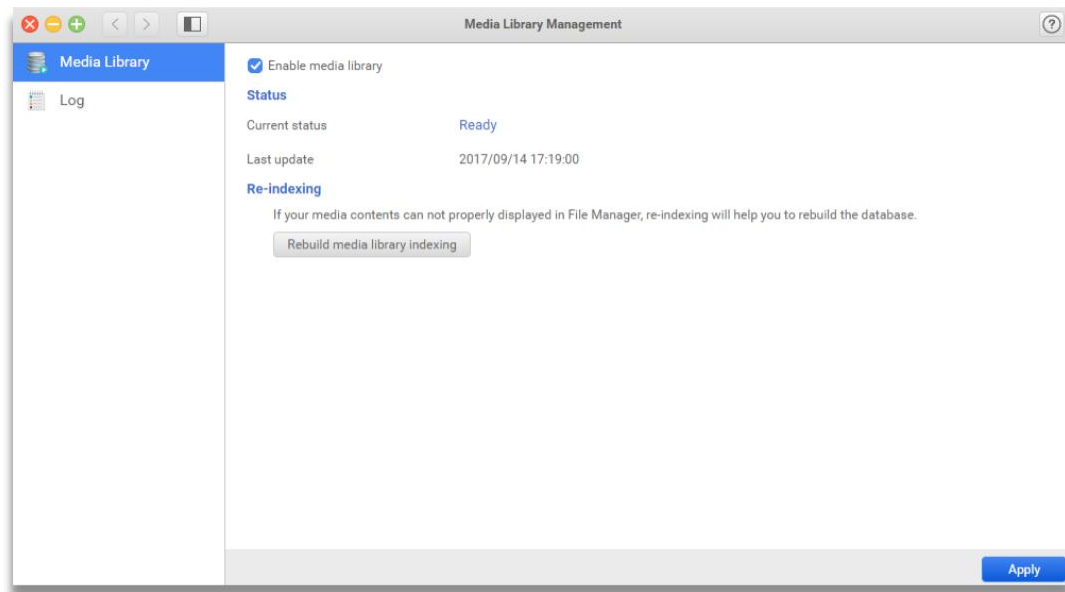


No.	Feature	Description
1	Menu	Show your play list.
2	Play / Pause button	Allows you to play and pause the video.
3	Seek bar	Control video progress.
4	Volume	Adjust the video and music volume.
5	Full screen	Switch your screen to full mode.

5.2. Media Library Management

5.2.1. Media Library

In Media Library, you can scan multimedia and documents such as, videos, music, videos, Microsoft office files, and Apple offices files, on ONYX Series 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

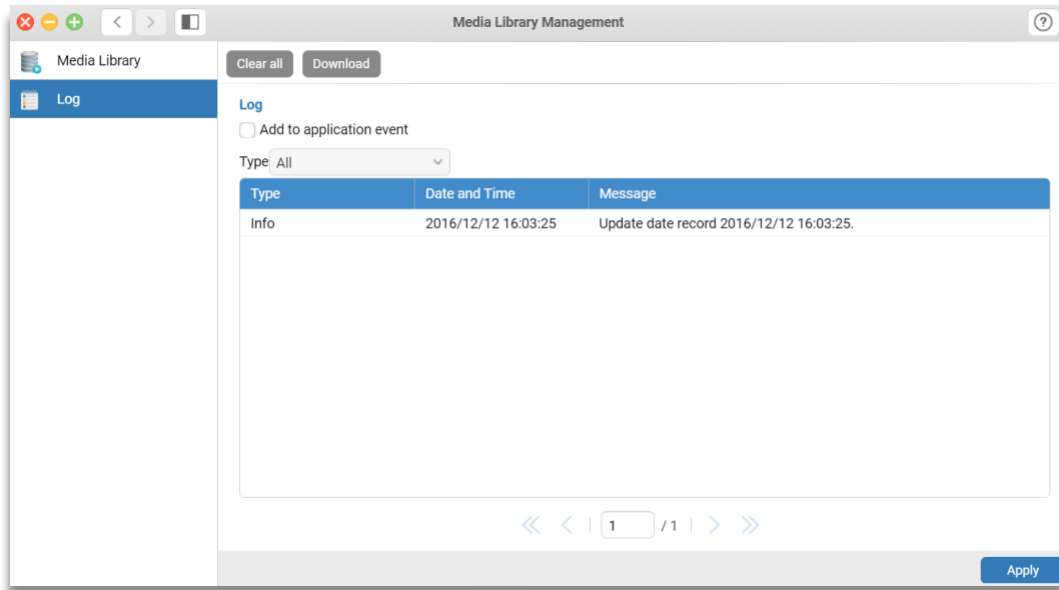
You can select which category by clicking the check box for Video, Music, Photo, and Documents.

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.

5.2.2. 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.



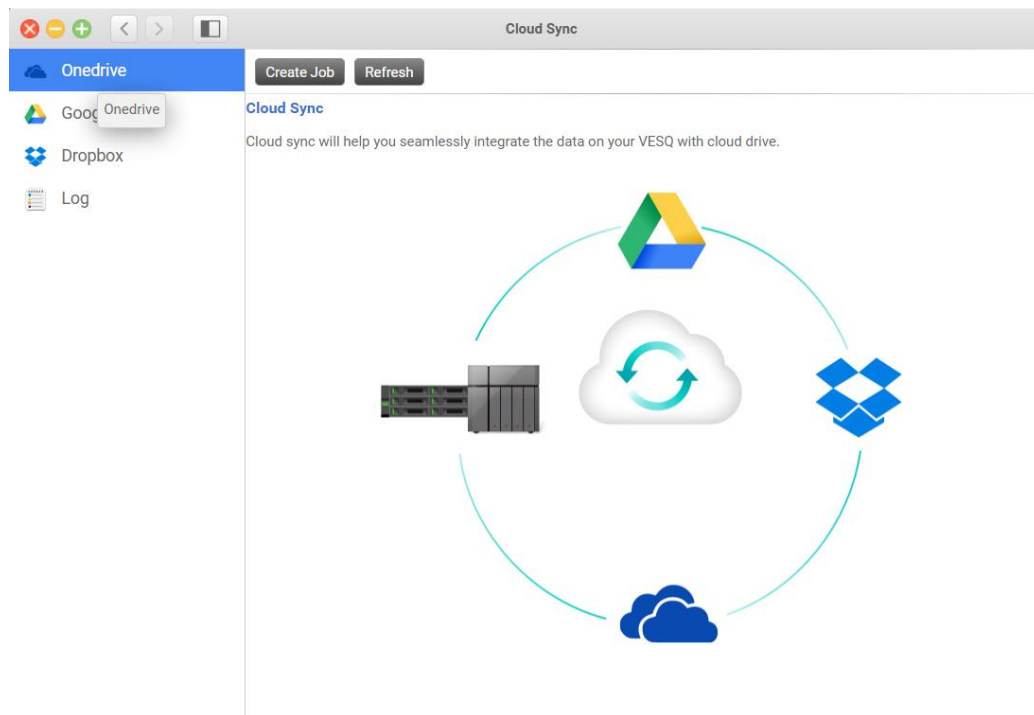
6.0 VES Cloud Applications

6.1. Cloud Sync

With **Cloud Sync**, you can seamlessly sync and share files between ONYX Series 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 ONYX Series is able to connect 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.

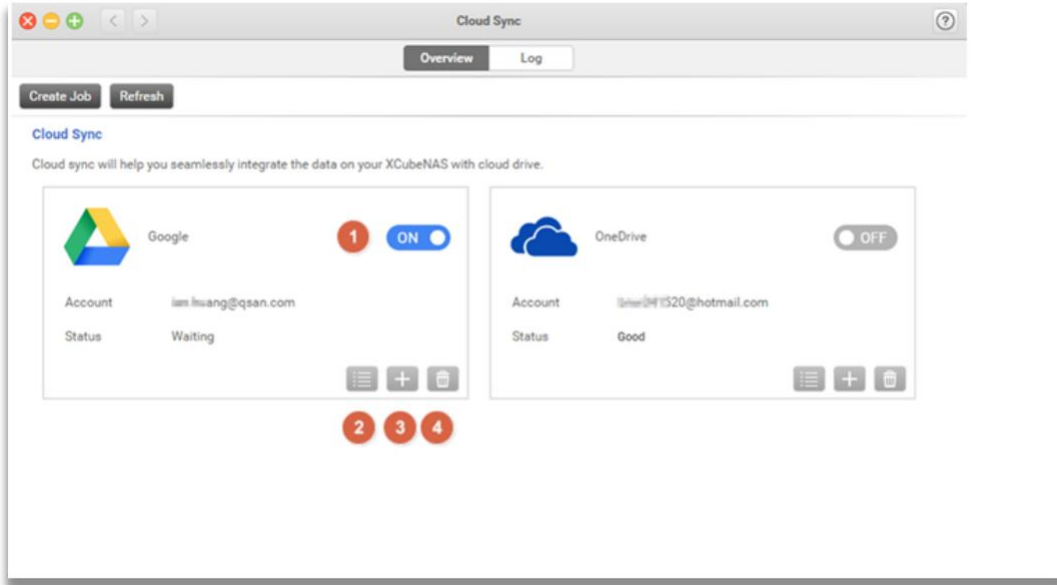
Your task will be shown on the overview page.

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. <ul style="list-style-type: none"> • Length: 1-128 characters • Invalid 【 `~!@#\$%^&*()=+[{} \ /;:"',<>?% 】 and space.
3	Local location	Select a ONYX Series 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 ONYX Series local folder.
5	Sync direction	There are three ways to manage your data. <ul style="list-style-type: none"> • 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 ONYX Series.
6	Schedule	There are two ways for the schedule settings. <ul style="list-style-type: none"> • Real Time – The data will always sync between your ONYX Series and cloud drive. • Periodically –You have four types to choose, Hourly, Daily, Weekly, and Monthly.
7	Advanced	<ul style="list-style-type: none"> • 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.

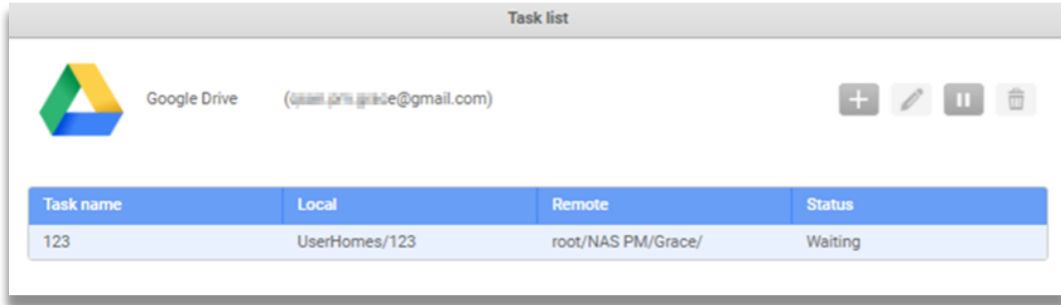


Job action button introduces:

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

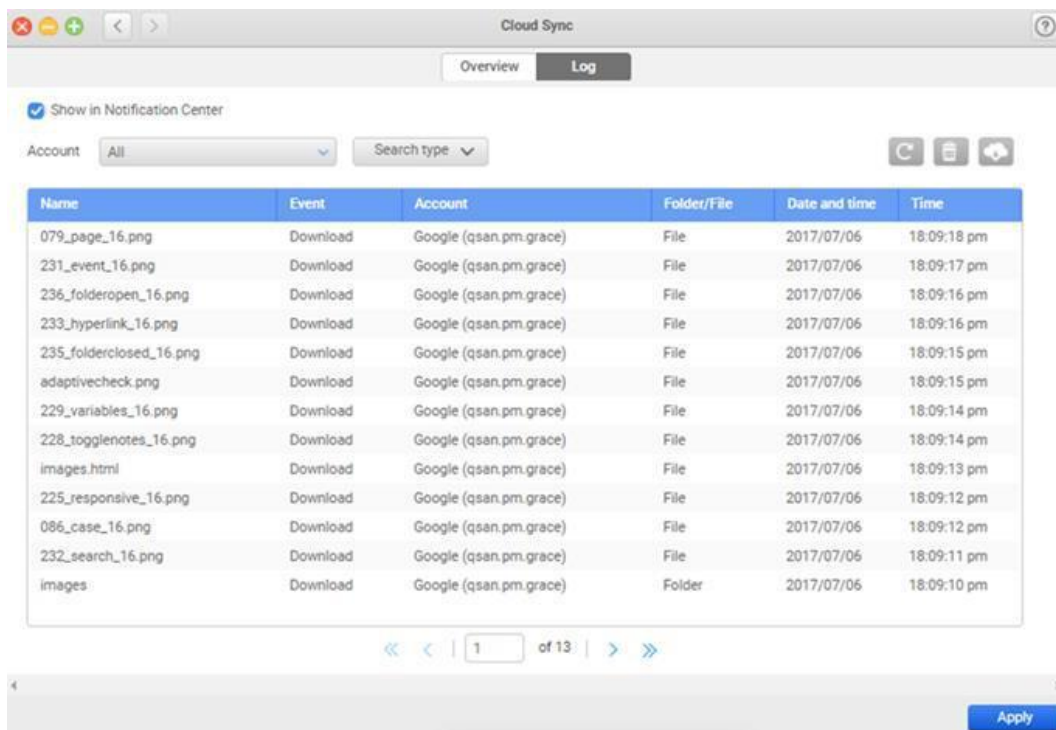
You can see all tasks of this cloud drive account and there are four actions on the task list page: **Add Task**, **Edit Task**, **Start/Pause**, and **Delete**.



- **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.

**TIP:**

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.



INFORMATION:

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

7.0 Business Applications

7.1. Antivirus

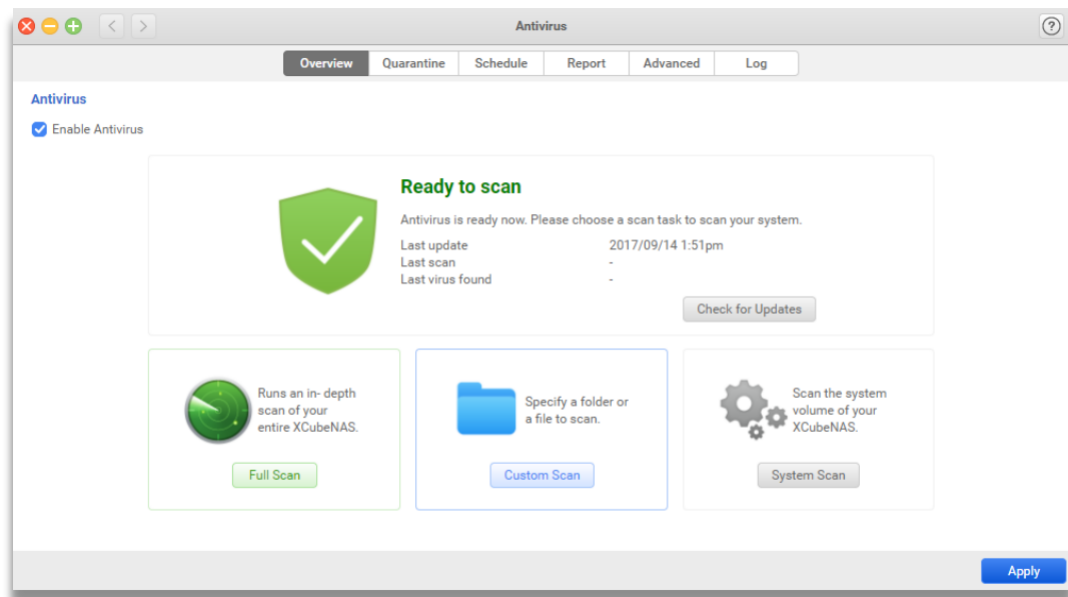
Antivirus is a full-featured security application which can protect your system. It will check the database update automatically and schedule a scan in the background.

Overview

You can check your current status, or prepare a scan for your ONYX Series.

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.



TIP:

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.



TIP:

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 VES 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 ONYX Series, 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 ONYX Series.
 - Custom scan: Only scan the selected folders or a specific folder on your ONYX Series.
 - 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 ONYX Series.
2. If you want to stop scanning during the process, please click the Stop button.

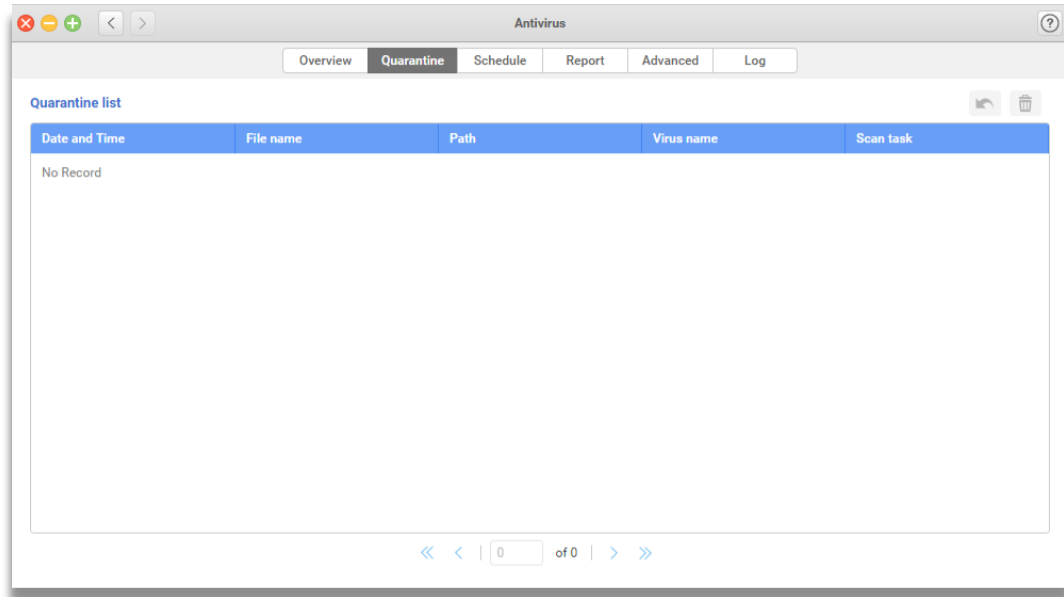


INFORMATION:

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 ONYX Series 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 put into potential threats if you restore the infected file(s) from the quarantine page. Please use this function carefully.

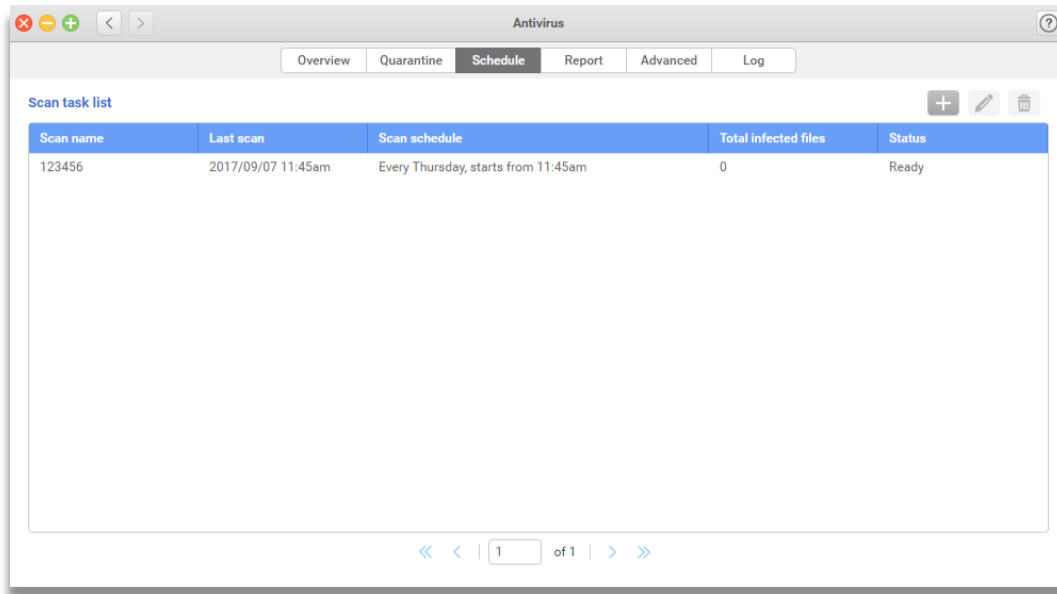
Delete the infected file(s)

To delete the 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 ONYX Series 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.

**INFORMATION:**

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.

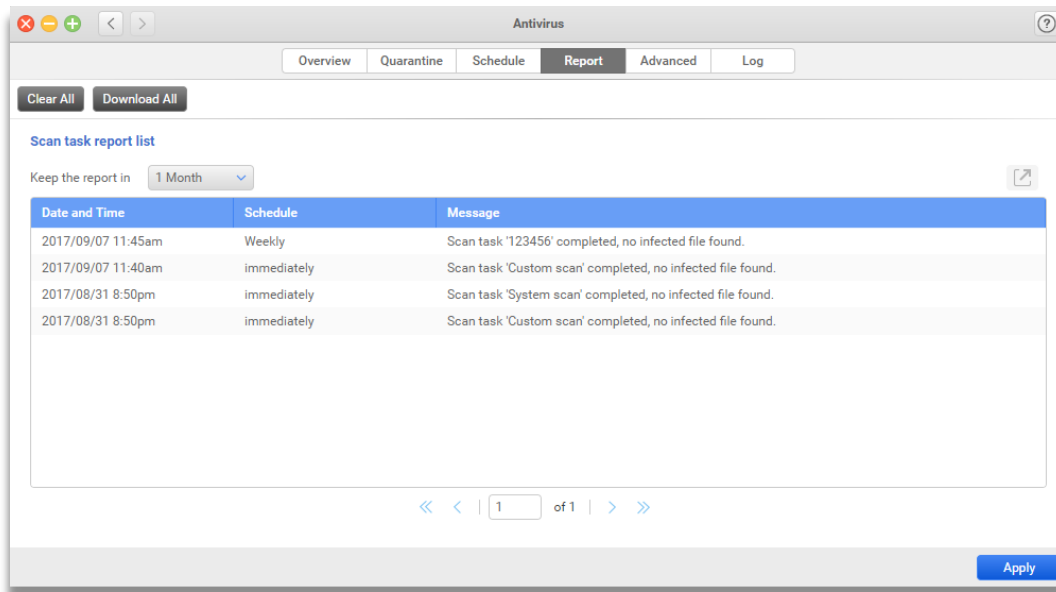
Delete a scan task

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, from 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:

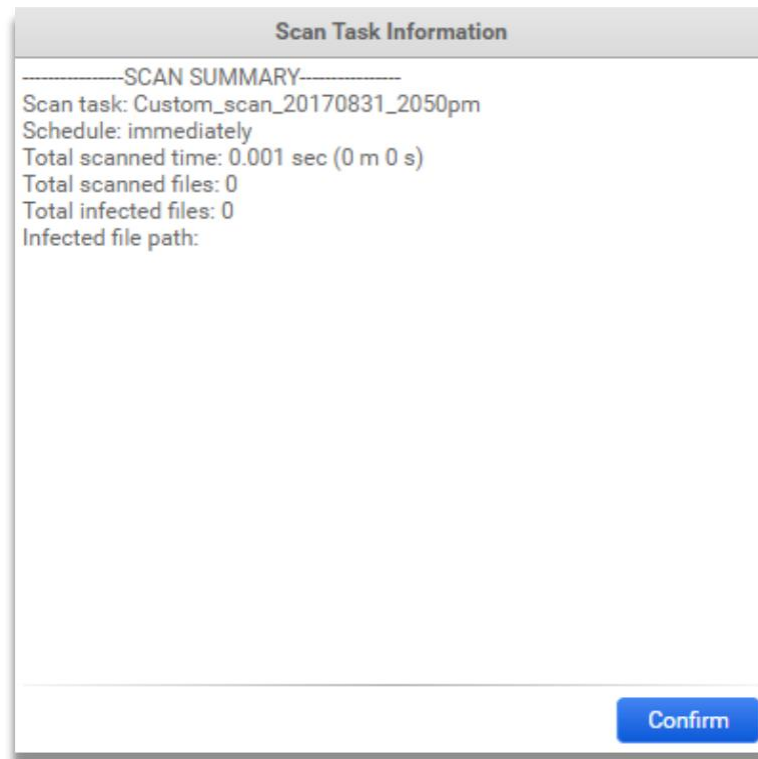
1. Select the number of days from the dropdown menu (10 Days/ 20 Days/ 1 Month/ 3 Month).

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:

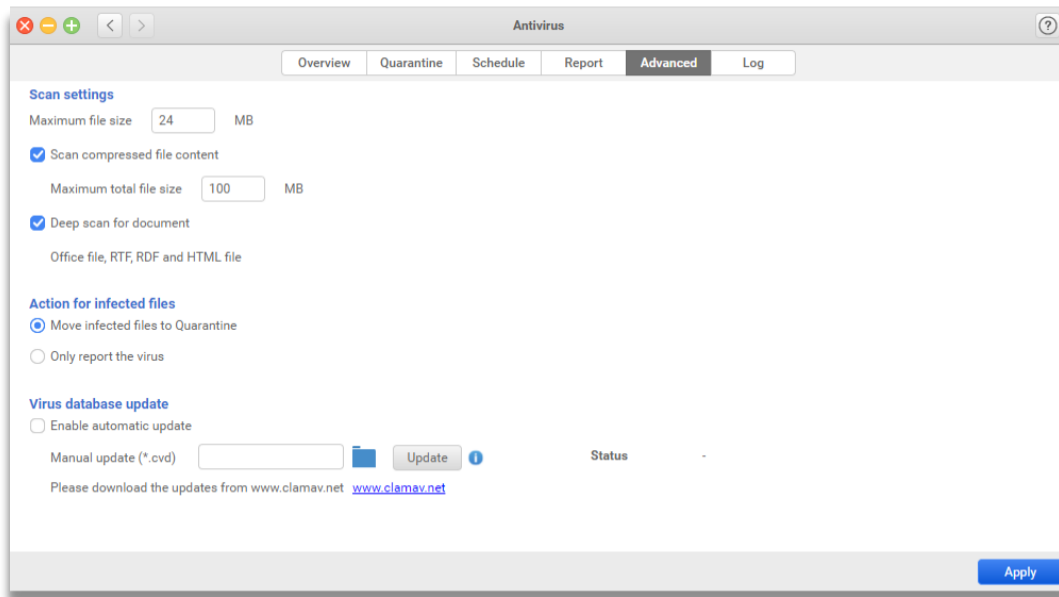
1. Choose a scanned result on report list.
2. Click **Open** button on top-right corner of the list.
3. The following information will be displayed on the popup window:



- 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.

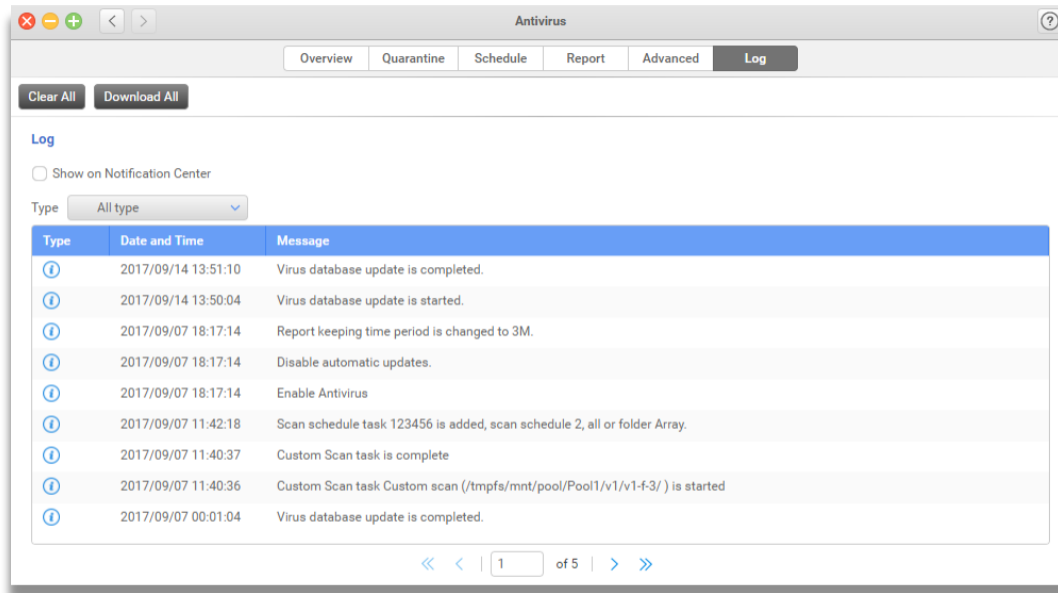
Update virus database

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.

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.



INFORMATION:

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.



TIP:

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.



INFORMATION:

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.
-

8.0 Support and Other Resources

8.1. Getting Technical Support

After installing your device, locate the serial number on the sticker located on the side of the chassis. To contact VES Support, please use the following information.

1. Via the Web: <https://www.vikingenterprisesolutions.com/support/customer-specific-support-portal/>
2. Via Email: support@vikingenterprise.com

Collect Information for Analysis

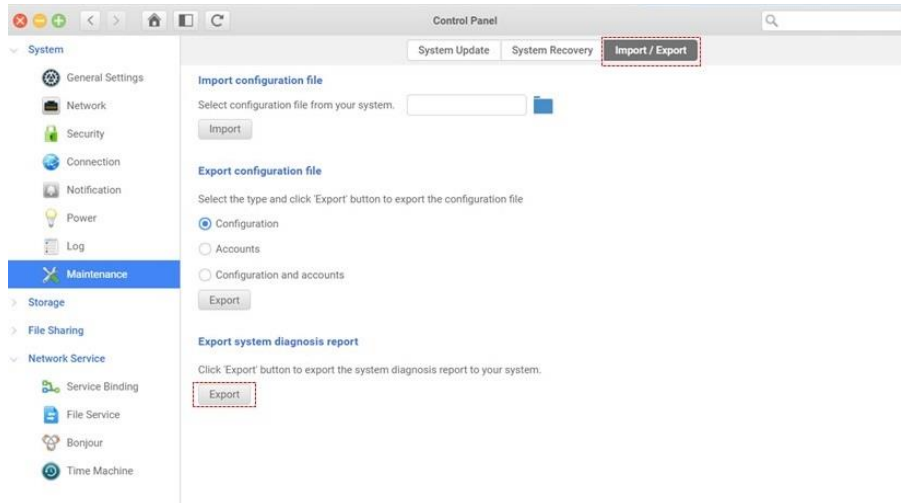
1. Product name, model or version, and serial number
2. Firmware version
3. Error messages or screenshot images
4. Product-specific reports and logs
5. Add-on products or components installed
6. Third-party products or components installed

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 ONYX Series model.

If the technical support requests you to download the service log, please navigate to the VESQ

UI → **Control Panel** → **System** → **Maintenance** → **Import/Export** → **Export system diagnosis report**, and then click the **Export** button.



8.2. Documentation Feedback

VES is committed to providing documentation that meets and exceeds your expectations. To help us improve the documentation, email any errors, suggestions, or comments to support@vikingenterprise.com.

When submitting your feedback, including the document title, part number, revision, and publication date located on the front cover of the document.

Appendix

End-User License Agreement (EULA)

Please read this document carefully before you use our product or open the package containing our product.

YOU AGREE TO ACCEPT TERMS OF THIS EULA BY USING OUR PRODUCT, OPENING THE PACKAGE CONTAINING OUR PRODUCT OR INSTALLING THE SOFTWARE INTO OUR PRODUCT. IF YOU DO NOT AGREE TO TERMS OF THIS EULA, YOU MAY RETURN THE PRODUCT TO THE RESELLER WHERE YOU PURCHASED IT FOR A REFUND IN ACCORDANCE WITH THE RESELLER'S APPLICABLE RETURN POLICY.

General

Viking Enterprise Solutions ("VES") is willing to grant you ("User") a license of software, firmware and/or other product sold, manufactured or offered by VES ("the Product") pursuant to this EULA.

License Grant

VES grants to User a personal, non-exclusive, non-transferable, non-distributable, non-assignable, non-sub-licensable license to install and use the Product pursuant to the terms of this EULA. Any right beyond this EULA will not be granted.

Intellectual Property Right

Intellectual property rights relative to the Product are the property of VES or its licensor(s). User will not acquire any intellectual property by this EULA.

License Limitations

The user may not, and may not authorize or permit any third party to (a) use the Product for any purpose other than in connection with the Product or in a manner inconsistent with the design or documentations of the Product; (b) license, distribute, lease, rent, lend, transfer, assign or otherwise dispose of the Product or use the Product in any commercial hosted or service bureau environment; (c) reverse engineer, decompile, disassemble or attempt to discover the source code for or any trade

secrets related to the Product, except and only to the extent that such activity is expressly permitted by applicable law notwithstanding this limitation; (d) adapt, modify, alter, translate or create any derivative works of the Licensed Software; (e) remove, alter or obscure any copyright notice or other proprietary rights notice on the Product; or (f) circumvent or attempt to circumvent any methods employed by VES to control access to the components, features or functions of the Product.

Disclaimer

VES DISCLAIMS ALL WARRANTIES OF PRODUCT, INCLUDING BUT NOT LIMITED TO ANY MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, WORKMANLIKE EFFORT, TITLE, AND NON-INFRINGEMENT. ALL PRODUCTS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. VES MAKES NO WARRANTY THAT THE PRODUCT WILL BE FREE OF BUGS, ERRORS, VIRUSES OR OTHER DEFECTS.

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

Limitation of Liability

IN ANY CASE, VES'S LIABILITY ARISING OUT OF OR IN CONNECTION WITH THIS EULA OR THE PRODUCT WILL BE LIMITED TO THE TOTAL AMOUNT ACTUALLY AND ORIGINALLY PAID BY CUSTOMER FOR THE PRODUCT. The foregoing Disclaimer and Limitation of Liability will apply to the maximum extent permitted by applicable law. Some jurisdictions do not allow the exclusion or limitation of incidental or consequential damages, so the exclusions and limitations set forth above may not apply.

Termination

If User breaches any of its obligations under this EULA, VES may terminate this EULA and take remedies available to VES immediately.

Miscellaneous

- Viking Enterprise Solutions reserves the right to modify this EULA.
- VES reserves the right to renew the software or firmware anytime.
- VES may assign its rights and obligations under this EULA to any third party without condition.
- This EULA will be binding upon and will inure to User's successors and permitted assigns.