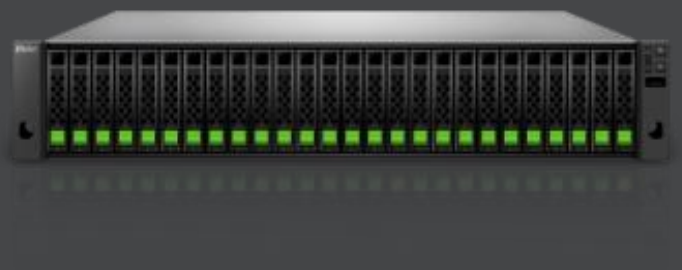
XCubeFAS XEVO 1.1 Software Manual

Applicable Models:
XF2026D



QSAN Technology, Inc.
www.QSAN.com

QSAN

August 2019

This edition applies to QSAN XCubeFAS XEVO (an all-flash array operating system). QSAN believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Notices

This XCubeFAS XEVO user's manual is applicable to the following XCubeFAS models:

XCubeFAS Storage System 2U 19" Rack Mount Model

Model Name	Controller Type	Form Factor, Bay Count, and Rack Unit
XF2026D	Dual Controller	SFF 26-disk 2U Chassis

Information contained in this manual has been reviewed for accuracy. But it could include typographical errors or technical inaccuracies. Changes are made to the document periodically. These changes will be incorporated in new editions of the publication. QSAN 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.

Table of Contents

Figures

Tables

Preface

About This Manual

This manual provides technical guidance for designing and implementing QSAN XCubeFAS series AFA (All-Flash Array) system, and it is intended for use by system administrators, SAN designers, storage consultants, or anyone who has purchased these products and is familiar with servers and computer networks, network administration, storage system installation and configuration, storage area network management, and relevant protocols.

Related Documents

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

- All XCubeFAS Documents
- XCubeFAS QIG (Quick Installation Guide)
- XCubeFAS Hardware Manual
- XCubeFAS XEVO Software Manual
- Compatibility Matrix
- White Papers
- Application Notes

Technical Support

Do you have any questions or need help trouble-shooting a problem? Please contact QSAN Support, we will reply to you as soon as possible.

- Via the Web: https://www.qsan.com/technical_support
- Via Telephone: +886-2-77206355
  (Service hours: 09:30 - 18:00, Monday - Friday, UTC+8)
- Via Skype Chat, Skype ID: qsan.support
  (Service hours: 09:30 - 02:00, Monday - Friday, UTC+8, Summer time: 09:30 - 01:00)
- Via Email: support@qsan.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.

Conventions

The following table describes the typographic conventions used in this manual.

Conventions	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels. Example: Click the **OK** button.
<*Italic*>	Indicates a variable, which is a placeholder for actual text provided by the user or system. Example: copy <*source-file*> <*target-file*>.
[ ] square brackets	Indicates optional values. Example: [a | b] indicates that you can choose a, b, or nothing.
{ } braces	Indicates required or expected values. Example: { a | b } indicates that you must choose either a or b.

| vertical bar	Indicates that you have a choice between two or more options or arguments.
/ Slash	Indicates all options or arguments.
underline	Indicates the default value. Example: [a | b]

1. XEVO Overview

XEVO is a QSAN specified OS for AFA (All-Flash Array). It can manage, monitor, and analyze the configuration and performance of the XCubeFAS series AFA storage system. This chapter provides an overview of the XEVO functionality and includes a brief explanation of storage terminology for you to be more familiar with the storage technologies used by the XCubeFAS system.

1.1. Introduction to XEVO

The QSAN XEVO is very user-friendly, it helps you manage your storage within just a few clicks, and if you are not available at your seat during the day, you may operate your AFA with your mobile device. It offers you the most superior storage services, available only to enterprise storage experts that can help you to analyze the status of your business usage, preventing accidental damages caused by human negligence.

In XEVO, all new UX (User Experience) was developed on a foundation of three simple concepts:

1. All-flash arrays should be user-friendly and operable by all.
2. Be able to be deployed or integrated into any environment.
3. Should be affordable for any size business.

You can gradually discover these ideas through the operation.

1.1.1. XEVO Software Architecture

XEVO supports Dual Active (Active/Active) controller system architecture with high availability. Figure 1-1 shows the XEVO software architecture. XEVO implements rich host applications and delivers enterprise data services that are founded upon QSAN core engines. These are the technologies that really care about your data, and also drive the high performance which QSAN is proud of.

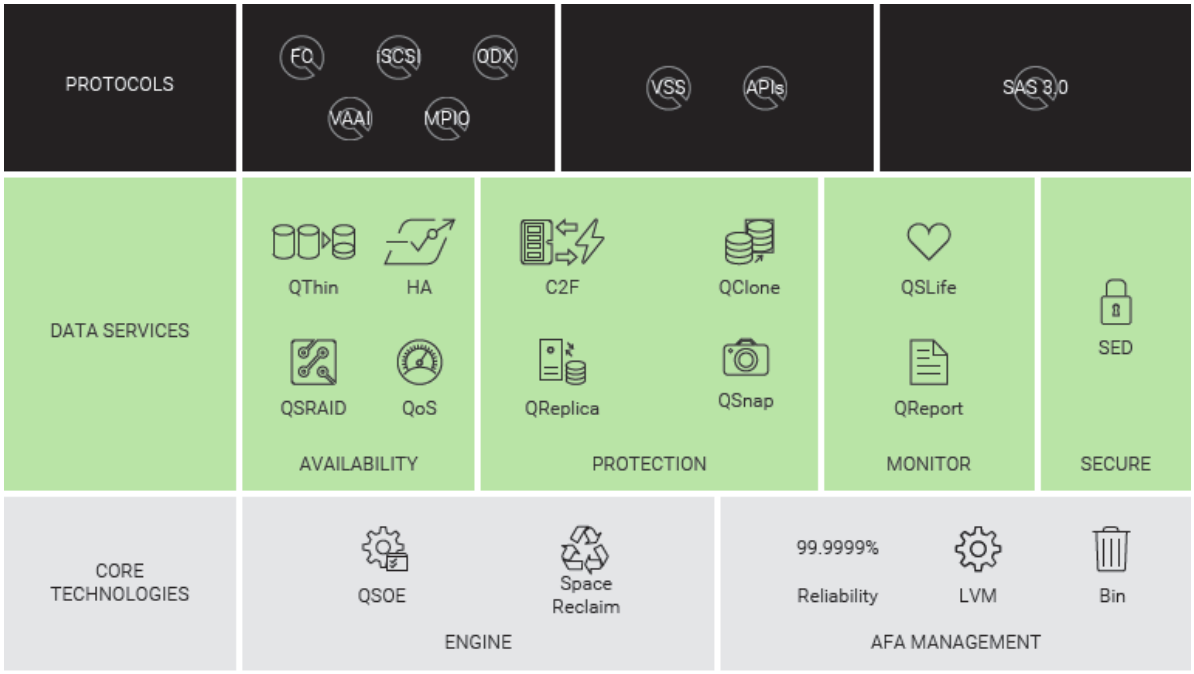


Figure 1-1 XEVO Software Architecture

The difference with SAN system is that XEVO focuses on and improves the operation and monitoring for flash drives. QSLife will monitor and analyze the activity of SSDs. It analyzes and decrypts SSD details, then turns into easy-to-understand information. The alert can be customized for SSD remaining life and health status when it approaches the threshold. In addition, it also can show the current and historical data of SSD usage.

QSRAID prevents all SSDs failure at the same time in one pool; we develop a specific algorithm for preventing pool failure due to SSD lifecycle. Due to the feature of SSD write endurance, the specific algorithm can provide that always aware user one SSD failure at one time. So you never forget to replace your SSDs before they fail.

1.1.2. XEVO 1.0 Functionality List

XEVO 1.0 provides the following functionality for administrator management.

Figure 1-2 XEVO 1.0 Dashboard Panel

Dashboard

- Provide hardware alert and system alert.
- Display array capacity information and storage overview.
- Monitor storage array performance by latency, IOPS, and throughput.
- Monitor and optimize SSD performance and longevity.
- Monitor SSD usage and learn SSD usage effectively with custom notifications.
- System reboot or shutdown.

Storage Management

- Support RAID pool with RAID level 0, 1, 3, 5, 6, 0+1, 10, 30, 50, 60, and N-way mirror.
- Also support RAID EE level 5EE, 6EE, 50EE, and 60EE.
- Support thick provisioning pool and online migrate RAID pool.
- Support thin provisioning pool with space reclamation.
- Support online storage pool capacity expansion and volume capacity extension.
- Configure disk properties with disk write cache, disk read-ahead, and command queuing.
- Configure volume properties with background I/O priority, volume write-back cache, and video editing mode for enhanced performance.
- Support global hot spares for pool.
- Support fast RAID rebuild.
- Support SSD life monitoring and S.M.A.R.T attributes.

- Support pool parity check.
- Support pool activated and deactivated for disk roaming.
- Support multiple volume creation.
- Support SED (Self-Encrypting Drive) and ISE (Instant Secure Erase) drives.
- Volume QoS (Quality of Service).

Host Management

- Support host groups to bind hosts and volumes.
- Obtain host connectivity information.
- Configure iSCSI target with CHAP (Challenge-Handshake Authentication Protocol) and mutual CHAP authentication.
- List iSCSI sessions.

Protection and Data Backup

- Support protection groups to protect volumes together.
- Enable snapshot space automatically.
- Support writable snapshot with manual or schedule tasks.
- Recycle snapshots.
- Support volume cloning for local replication.
- Easily deploy the local clone without doing configurations.
- Support remote replication with traffic shaping for dynamic bandwidth controller.
- Auto Replication, easily deploy the remote replication without doing configurations
- 1 step local-to-remote.

Performance and Capacity Analysis

- Monitor volume performance and history by latency, IOPS, and throughput.
- Monitor volume capacity and history usage.

System Management

- Monitor enclosure status of head and enclosure units.
- Monitor cache to flash memory protection status. BBM (Battery Backup Module), SCM (Super Capacitor Module), and flash module are optional add-ons.
- Blink UID (Unique Identifier) LEDs for locating the storage arrays.
- Configure login options.
- Change system name, date and time.
- Configuration export and import.

- Configure management IP address, DNS, and service ports.
- Configure data port settings.
- Configure iSCSI connectivity with IP address, link aggregation, VLAN (Virtual LAN) ID and jumbo frame.
- Setup entity name and iSNS (Internet Storage Name Service).
- Configure fibre channel connectivity with link speed and topology.
- Obtain system information and download service package.
- Update firmware of head unit or enclosure unit(s).
- Support disk firmware batch update.
- Support boot management including auto shutdown, wake-on-LAN, and wake-on-SAS.
- Support network UPS via SNMP.
- System reset to default and volume restoration for maintenance usage.
- Support RBAC (Role-Based Access Control).
- Support RESTful API (Application Programming Interface).
- Provide background task monitoring.

Message Management

- Configure alert notifications through email or SNMP traps.
- View event logs with different levels of event and download event logs.

1.2. Terminology

In this section, we introduce the terms that are used for the storage system throughout this manual.

RAID

RAID is the abbreviation of Redundant Array of Independent Disks. There are different RAID levels with different degrees of data protection, data availability, and performance to the host environment.

Pools

A storage pool is a collection of disk drives. One pool consists of a set of volumes and owns one RAID level attribute.

Volumes

Each pool can be divided into several volumes. The volumes from one pool have the same RAID level, but may have different volume capacity.

LUN

A LUN (Logical Unit Number) is a unique identifier for designating an individual or collection of physical or virtual storage devices that execute I/O commands with a host computer, as defined by the SCSI (Small Computer System Interface) standard.

iSCSI

iSCSI (Internet SCSI) is a protocol which encapsulates SCSI (Small Computer System Interface) commands and data in TCP/IP packets for linking storage devices with servers over common IP infrastructures.

Fibre Channel

Fibre channel is an extremely fast system interface. It was initially developed for use primarily in the supercomputing field, but has become the standard connection type for storage area networks (SAN) in enterprise storage.

SAS

Serial-attached SCSI offers advantages over older parallel technologies. The cables are thinner, and the connectors are less bulky. Serial data transfer allows the use of longer cables than parallel data connections.

SSD

An SSD (Solid-State Drive) is a solid-state storage device that uses integrated circuit assemblies as memory to store data persistently.

Thick Provisioning

Thick provisioning is allocated upon creation the physical disk drive space and is equal to the user capacity seen by the host server. It also called fat provisioning.

Thin Provisioning

Thin provisioning is allocated on-demand and can be less than the user capacity seen by the host server. It involves using virtualization technology to give the appearance of having more physical resources than are actually available.

Snapshot

A volume snapshot is the state of a system at a particular point in time.

Local Clone

Local clone function has another physical data copy as the original volume.

Remote Replication

Remote replication function prevents primary site failure by replicating data to the remote sites.

QoS (Quality of Service)

QoS has a control mechanism that provides different priorities to ensure that the performance of the data stream reaches a certain level according to the requirements of the application

2. Getting Started

After completing the configuration planning, it's time to power on the system, find your system and log into XEVO (AFA operating system). This chapter explains how to discover the AFA storage system and how to sign into XEVO.

2.1. Power on the Storage System

Before you power on the system, we assume that you have followed the following hardware installation document to finish the hardware installation.

- XCubeFAS QIG (Quick Installation Guide)
- XCubeFAS Hardware Owner's Manual

TIP:
Please double check all the cables (including power cords, Ethernet, fibre channel, and SAS cables) are connected properly, especially network cable connects to the management port. If everything is ready, now you can power on the system.

2.2. Discover the AFA Storage System

The default setting for the management IP address is DHCP. For users who are going to install at the first time, we provide the XFinder Java utility to search for QSAN products on the network and aid quick access to the login page of the XEVO web interface.

2.2.1. XFinder Utility

XFinder utility provides to search QSAN products on LAN. You can discover the management IP addresses of the storage systems via this utility. Please download XFinder utility from the following website.

https://www.qsan.com/download.php

In addition, XFinder is a java based program. It is also a highly portable utility. To execute this program, JRE (Java Runtime Environment) is required. You can visit the following websites to download and install JRE.

http://www.java.com/en/download/

After JRE is installed, run the **XFinder.jar** program. The AFA storage system in your network will be detected and listed in the table.

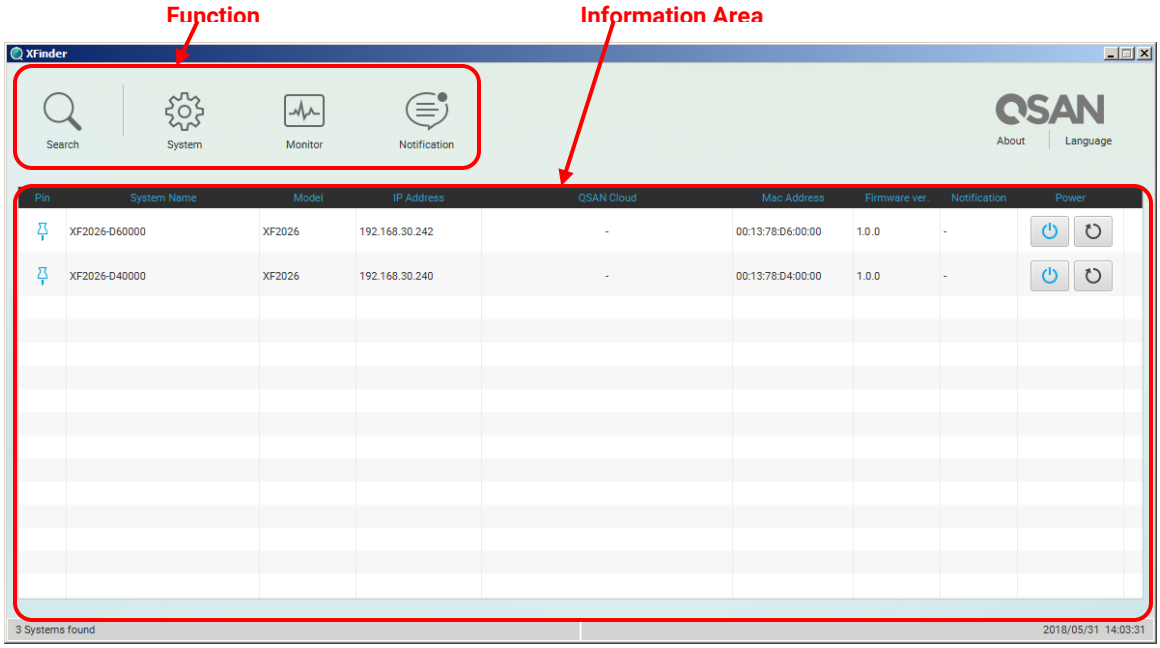


Figure 2-1 XFinder Utility

Take an example in Figure 2-1, Xfinder discovers two systems in LAN. The default setting of the management port IP address is gotten from the DHCP server, e.g., 192.168.30.242. The default system name is the model name plus the last 6 digits of the serial number, e.g., XF2026-D60000. Double-clicking the selected entry will automatically bring up the browser and display the login page.

INFORMATION:
XFinder utility works in the following network environments:

- Both the management port of the SAN storage system and the management computer are both on the same subnet domain of the LAN.
- The LAN works with or without DHCP server.
- If the LAN doesn't have a DHCP server, it still can work on zero-configuration networking. 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. For more information about zero configuration, please refer to: https://en.wikipedia.org/wiki/Zero-configuration_networking

2.3. Initial Setup

The Initial configuration wizard will guide the first time user to initialize and set up the system quickly. After discovering the storage system, please follow the steps to complete the initial configuration.

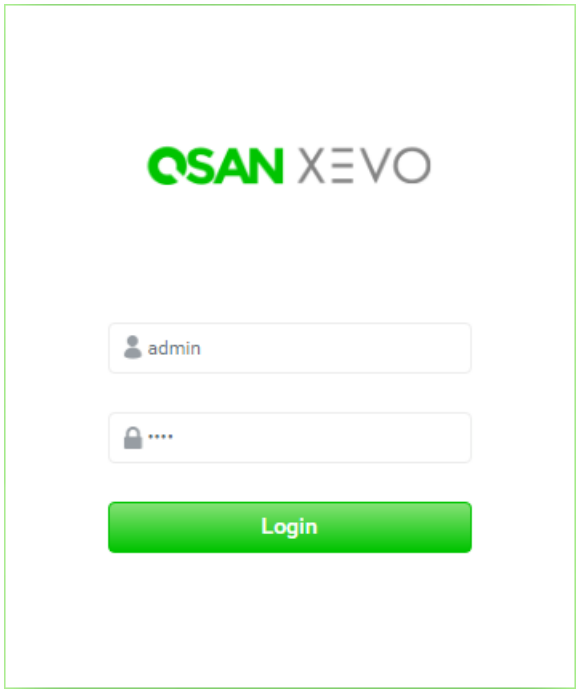


Figure 2-2 Login Page of web UI

1. To access the XEVO web interface, you have to enter a username and password. The initial defaults for administrator login are:
   - **Username**: admin
   - **Password**: 1234

TIP:
For existing users who are experienced, the Initial configuration wizard will not be shown again when you log in next time, unless the system is **Reset to Factory Defaults**. You may skip this section to start the operations of web UI in the next chapter.

You can execute **Reset to Factory Defaults** function in **System** -> **Maintenance** -> **Rescue** -> **Reset to Defaults**. Please refer to the chapter 9.4.5, Rescue section for more details.

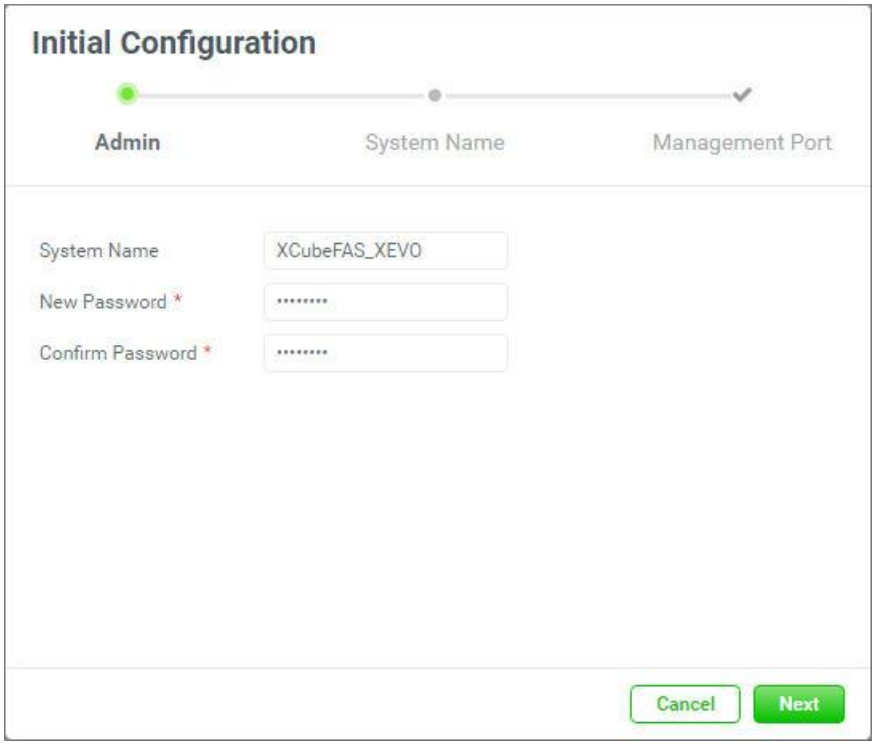


Figure 2-3 Initial Configuration Step 1

2. Enter a **System Name**, for security reason, it's highly recommended to change system name. The maximum length of the system name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_].
3. Change admin's password in **New Password** and reconfirm in **Confirm Password**, The maximum length of the password is 32 characters. Valid characters are [A~Z | a~z | 0~9 | ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/].
4. Click the **Next** button to proceed.

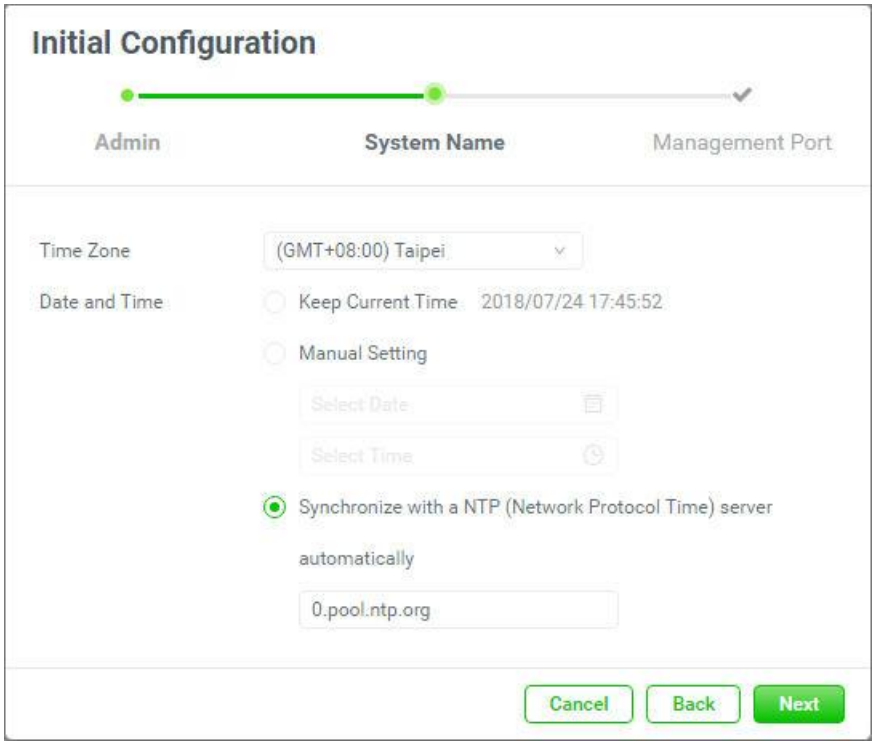


Figure 2-4 Initial Configuration Step 2

5. Select a **Time Zone** depending on your location.
6. Set the local **Date and Time**. Date and time can be set by manually or synchronized with a NTP (Network Time Protocol) server.
7. Click the **Next** button to proceed.

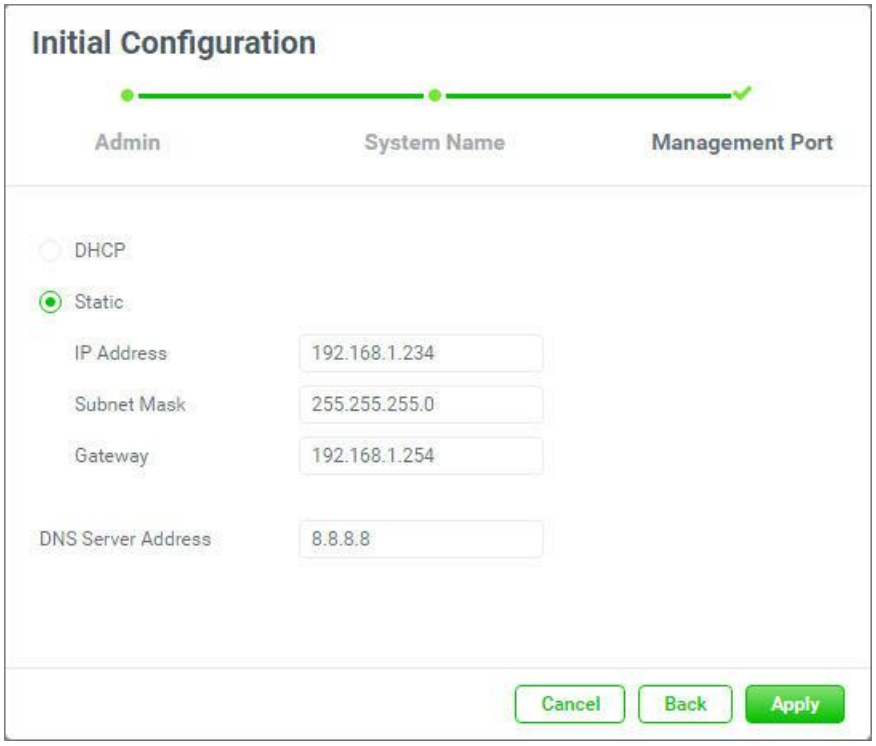


Figure 2-5 Initial Configuration Step 3

8. Assign an IP address for the management port by **DHCP** or **Static** IP Address.

INFORMATION:
DHCP: The Dynamic Host Configuration Protocol is a standardized network protocol used on IP (Internet Protocol) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

9. Assign a **DNS Server Address**. DNS (Domain Name System) provides a means to translate FQDN (Fully Qualified Domain Name) to IP address. Some notification services require DNS settings.
10. Click the **Apply** button to complete the initial configuration. You have to login with the new IP address of the management port and new admin password next time.

3. XEVO User Interface

This chapter illustrates the web user interface of XEVO and provides a brief introduction to the XEVO 1.0 desktop function menus.

3.1. Easy Deployment

XEVO simplifies itself – freeing you from complicated process of deploying your storage. Power it on and clicking your finger within just a few times (with our recommend configurations), then enjoy the convenience and focus on your business without paying too much attention to setting up your storage.

Figure 3-1 Easy Deployment

3.2. Accessing the Management Web UI

To access the management web user interface, open a supported web browser and enter the management IP address or Hostname of the system. The login panel is displayed, as shown in Figure 3-1.

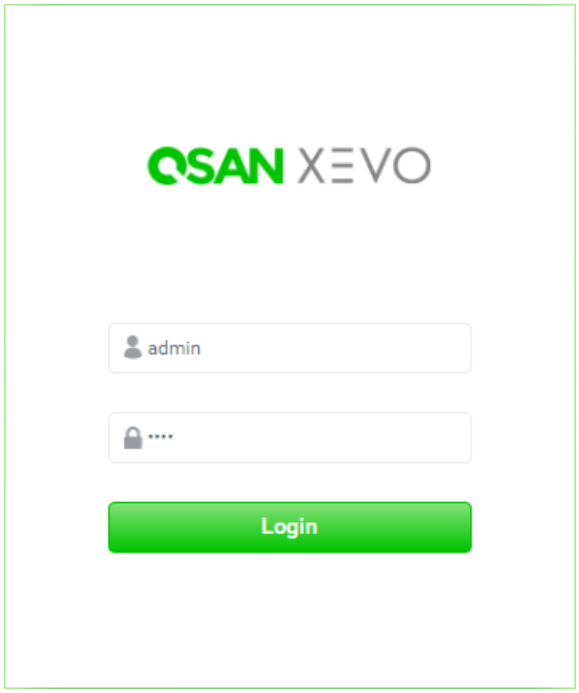


Figure 3-2 Login Page of web UI

To access the web user interface, you have to enter a username and password.

- **Username**: admin
- **Password**: <Your Password>

INFORMATION:
Supported web browsers:

- Google Chrome 45 or later.
- Mozilla Firefox 45 or later.
- Microsoft Internet Explorer 10 or later.
- Apple Safari 8 or later.

3.3. XEVO Web UI Overview

When the password has been verified, the dashboard is displayed as shown in Figure 3-2.

Figure 3-3 XEVO Dashboard

The XEVO Web UI contains the following tabs:

Dashboard

The **Dashboard** function tab represents a graphical overview of the array, including hardware alert, array capacity, system alerts, storage overview, and I/O (Input/Output) performance metrics. For more information, please refer to chapter 4.1, Dashboard Overview section.

Storage

Select the **Storage** function tab to display the storage pools on the array, including disk groups and volumes. View and operate the storage pools and their snapshots. For more information, please refer to chapter 5, Storage Tab.

Hosts

Select the **Hosts** function tab to display the host objects on the array, including host groups, host profile, connected volumes, and CHAP settings. View and operate the host objects and the connections between them. For more information, please refer to chapter 6, Hosts Tab.

Protection

Select the **Protection** function tab to display the protection groups on the array. View and operate the protection groups, their snapshot plan, and replication plan. For more information, please refer to chapter 7, Protection Tab.

Analysis

Select the **Analysis** function tab to display the historical array information, including I/O performance metrics and storage capacity, from various viewpoints. For more information, please refer to chapter 8, Analysis Tab.

System

Select the **System** function tab to display the system health and array-wide information. View and manage the array components, including user accounts, system general settings, management and data port interfaces, and maintenance functions. For more information, please refer to chapter 9, System Tab.

Messages

Select the **Messages** function tab to display the log events, and setup the notification methods. For more information, please refer to chapter 10, Messages Tab.

3.3.1. XEVO Web UI Navigation

The XEVO Web UI includes several tools to help you navigate around the interface efficiently. At the upper right corner of the XEVO Web UI is the header. The XEVO Web UI header includes the following links:

Help

Click the **Help** icon to display the like page of our presale FAQ. If they cannot solve your issues, you may use the contact us page to fill out your queries.

QSLife

Click the **QSLife** function icon to popup a QSLife window. It monitors and optimizes the SSD performance and longevity. For more information, please refer to the chapter 4.2, Introduce QSLife Functions section.

Hi, <Username>

Click the <Username> to drop down the functions that the user can perform. For example, admin can perform **Logout**, **Reboot**, and **Shutdown** the system.

The **Storage**, **Hosts**, **Protection**, and **Analysis** function tabs are divided into two main panes:

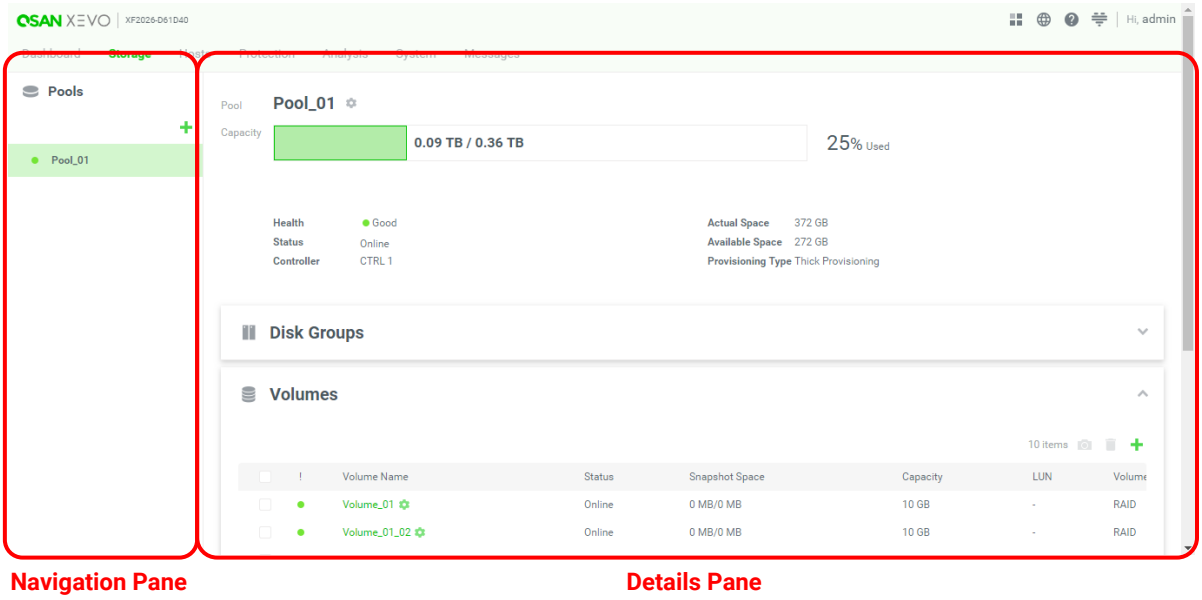


Figure 3-4 Function Tabs are Divided into Two Main Panes

Navigation Pane

The navigation pane displays the XEVO objects related to the selected function tab. Select an object to analyze or configure the information that appears in the details pane.

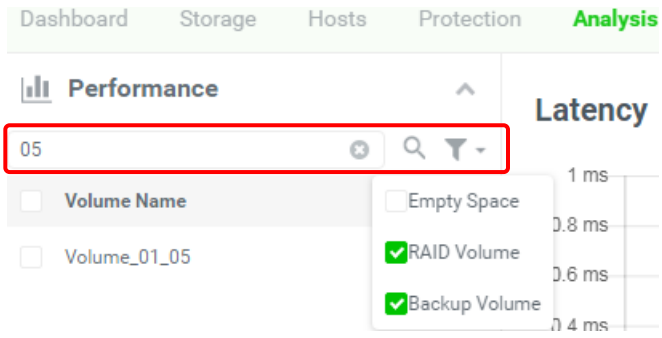


Figure 3-5 Filter in the Analysis Tab

In the navigation pane of the **Analysis** tab, click the filter icon to drop down the volume types, check or uncheck them to narrow the list of volume types. Or input the filter string in the field and click the search icon to narrow those that contain the filter string. Once you have narrowed down the list of items, select the actual item to view its details in the details pane.

Details Pane

The details pane contains information and configuration options for the selected object. Select an object in the navigation pane to analyze or configure the object details in the details pane. The details pane includes two types of icons:

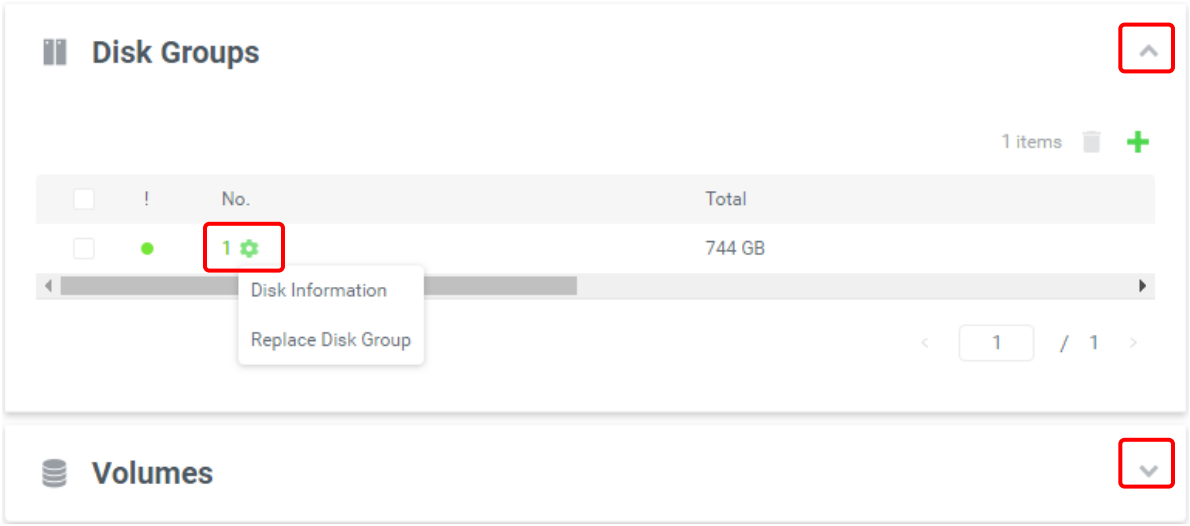


Figure 3-6 The Details Pane Includes Two Types of Icons

- Click the expand arrow or collapse arrow icon to upper-right corner in a sub pane to expand or collapse it.
- Click the working icon to the right of an object to pop up a drop down function menu. The function can be selected to execute.

3.4. Accessing the Management USB LCM

Optionally, we provide a portable USB LCM (LCD Control Module) for simple management. To access the management USB LCM, plug it into the USB port of the right ear in the front panel.

Figure 3-7 Portable USB LCM

INFORMATION:
For the USB port in front panel, please refer to the chapter 2, System Components Overview in the XCubeFAS Hardware Owner's Manual.

After plugging the USB LCM into the system, the LCD screen shows the management port IP address and the system model name.

```
192.168.1.234
QSAN XF2026D     ←
```

Figure 3-8 USB LCM Screen

To access the LCM options, use the **ENT** (Enter) button, **ESC** (Escape) button, ▲ (up) and ▼ (down) to scroll through the functions. **MUTE** button to mute the buzzer when the system alarms. If there are event logs occurred, events will be displayed on the first line of the LCM.

TIP:
The event alert settings can be changed, please refer to the chapter 10.2.2, Allert Settings section.

This table describes the function of each item.

Table 3-1 USB LCM Function List

Function	Description
System Info.	Display system information including firmware version and memory size.
Reset/Shutdown	Reset or shutdown the system.
View IP Setting	Display current IP address, subnet mask, and gateway.
Change IP Config	Set IP address, subnet mask, and gateway. There are three options of DHCP, BOOTP, or static IP address.
Enc. Management	Show the enclosure data of disk drive temperature, fan status, and power supply status.
Reset to Default	Reset the system to default settings. The default settings are: • Reset **Management Port** IP address to DHCP, and then fix IP address: 169.254.1.234/16. • Reset admin's **Password** to 1234. • Reset **System Name** to model name plus the last 6 digits of serial number. For example: XF2026-123456. • Reset IP addresses of all **iSCSI Ports** to 192.168.1.1, 192.168.2.1, … etc. • Reset link speed of all **Fibre Channel Ports** to Automatic. • Clear all access control settings of the host connectivity.

INFORMATION:

DHCP: The Dynamic Host Configuration Protocol is a standardized network protocol used on IP (Internet Protocol) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

BOOTP: Similar to DHCP, the Bootstrap Protocol is also a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. While some parts of BOOTP have been effectively superseded by the DHCP, which adds the feature of leases, parts of BOOTP are used to provide service to the DHCP protocol. DHCP servers also provide legacy BOOTP functionality.

This table displays the LCM menu hierarchy for your reference when you operate USB LCM.

Table 3-2 USB LCM Menu Hierarchy

Menu	L1	L2	L3	L4
<IP Addr> QSAN <Model> ▲▼	System Info.	Firmware Version <n.n.n>		
		RAM Size <nnnn> MB		
		▲Yes No▼		
	Reset / Shutdown	Reset	▲Yes No▼	
		Shutdown	▲Yes No▼	
	View IP Setting	IP Config <Static IP / DHCP / BOOTP>		
		IP Address <192.168.001.234>		
		IP Subnet Mask <255.255.255.0>		
		IP Gateway <xxx.xxx.xxx.xxx>		
	Change IP Config	DHCP		
		BOOTP		
		Static IP	IP Address	Adjust IP address
			IP Subnet Mask	Adjust Submask IP
			IP Gateway	Adjust Gateway IP
			Apply IP Setting	▲Yes No▼
	Enc. Management	Phy. Disk Temp.	Local Slot <*n*>: <*nn*> (C)	
		Cooling	Local FAN<*n*>: <*nnnnn*> RPM	
		Power Supply	Local	

			PSU<*n*>: <*status*>	
	Reset to Default	▲Yes No▼		

4. Dashboard Tab and QSLife

The **Dashboard** tab displays the hardware status and a running graphical overview of the array's storage capacity and performance. It helps the user to quickly view the basic information and system health. In addition, SSD plays an important role in the use of all-flash arrays. Therefore, we provide the **QSLife** function to monitor and analyze the activity of SSDs. This chapter describes the details of the **Dashboard** tab and the **QSLife** function.

4.1. Dashboard Overview

Select the **Dashboard** tab to show a summary of the overall system. It's divided into five blocks in the details pane. There are hardware alert, array capacity, system alert, storage overview, and performance graphs.

Figure 4-1 Dashboard

4.1.1. Hardware Alert

The **Hardware Alert** pane displays the disk health in the system. To drill down and analyze the array details, please select **System** -> **Arrays**.

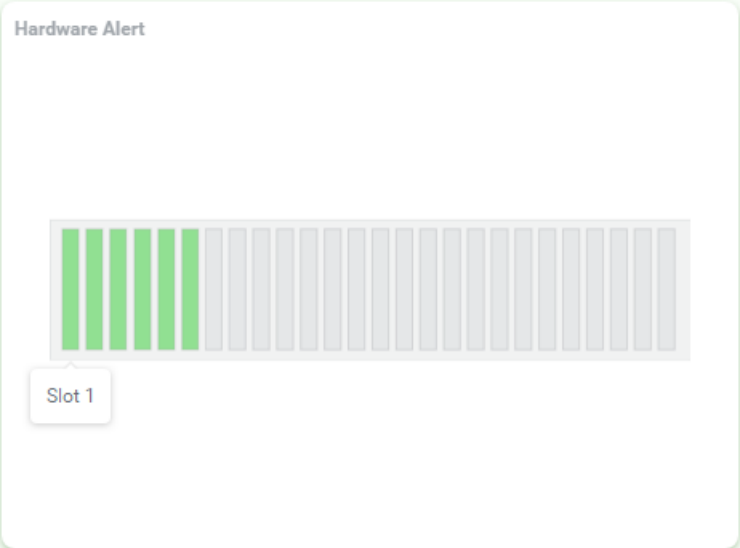


Figure 4-2 Hardware Alert in the Dashboard

Hovering over the slot will display the slot number. This table shows the hardware alert pane descriptions.

Table 4-1 Hardware Alert Pane Descriptions

Name	Description
Disk Health	The status of disk health: • Green Color / Normal: The disk drive is good. • Orange Color / Abnormal: The disk drive has unrecoverable read errors or S.M.A.R.T. error. • Red Color / Warning: The disk drive has failed.

4.1.2. Array Capacity

The **Array Capacity** pane contains a summary of the capacity usage including used, total, and the amount of storage occupied by provisioned volumes and snapshots.

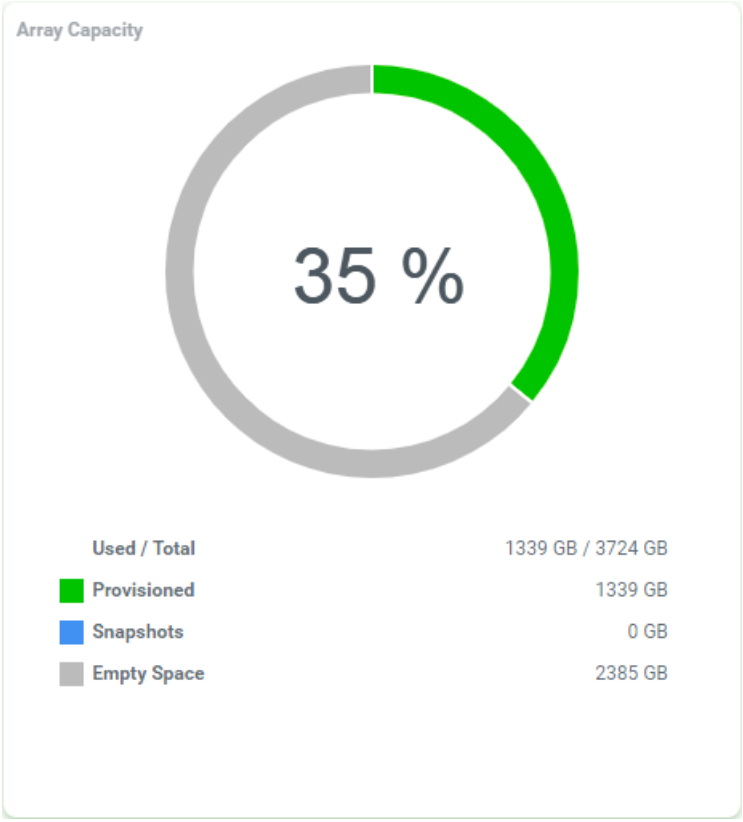


Figure 4-3 Array Capacity in the Dashboard

The pane includes the following items:

- **Percentage (%):** Percentage of the system's storage space occupied by provisioned volumes and snapshots. The percentage value is displayed in the circle of the pane.
- **Used:** Storage space occupied by volumes and snapshots.
- **Total:** Total physical usable space on the array.
- **Provisioned:** Total provisioned capacity of all volumes.
- **Snapshots:** Physical space occupied by data unique to one or more snapshots.
- **Empty Space:** Unused space available for allocation.

4.1.3. System Alert

The **System Alert** pane contains a summary of the abnormal and warning event messages. In addition, clicking the items or the numbers will jump to the **Messages** function tab.

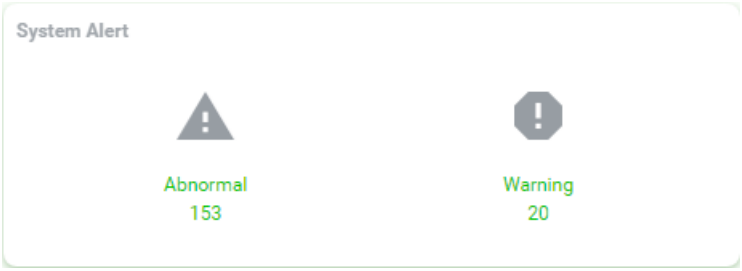


Figure 4-4 System Alert in the Dashboard

The pane includes the following items:

- **Abnormal:** The number under the item is the count of the abnormal messages.
- **Warning:** The number under the item is the count of the warning messages.

4.1.4. Storage Overview

The **Storage Overview** pane contains a summary of the abnormal and warning event messages. In addition, clicking the Array, Disk, Pool, or Volume or the numbers will jump to the **Storage** function tab. Clicking the Host or the number will jump to the **Hosts** function tab.

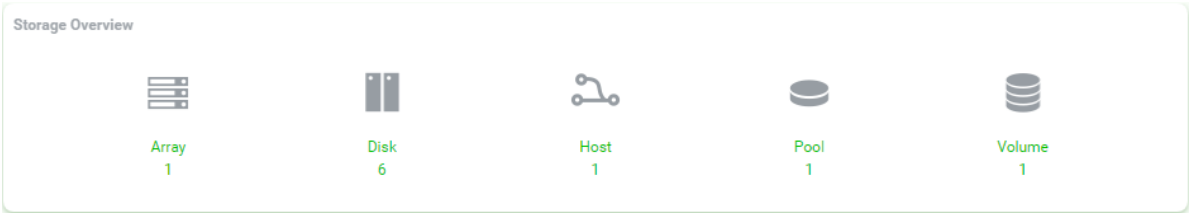


Figure 4-5 Storage Overview in the Dashboard

The pane includes the following items:

- **Array:** The number under the item is the count of total arrays including the head and the expansion units.
- **Disk:** The number under the item is the count of total disk drives in the system.
- **Host:** The number under the item is the count of total host groups in the system.
- **Pool:** The number under the item is the count of total pools in the system.
- **Volume:** The number under the item is the count of total volumes in the system.

4.1.5. Performance Graphs

The **Performance Graphs** pane displays the performance charts in real time.

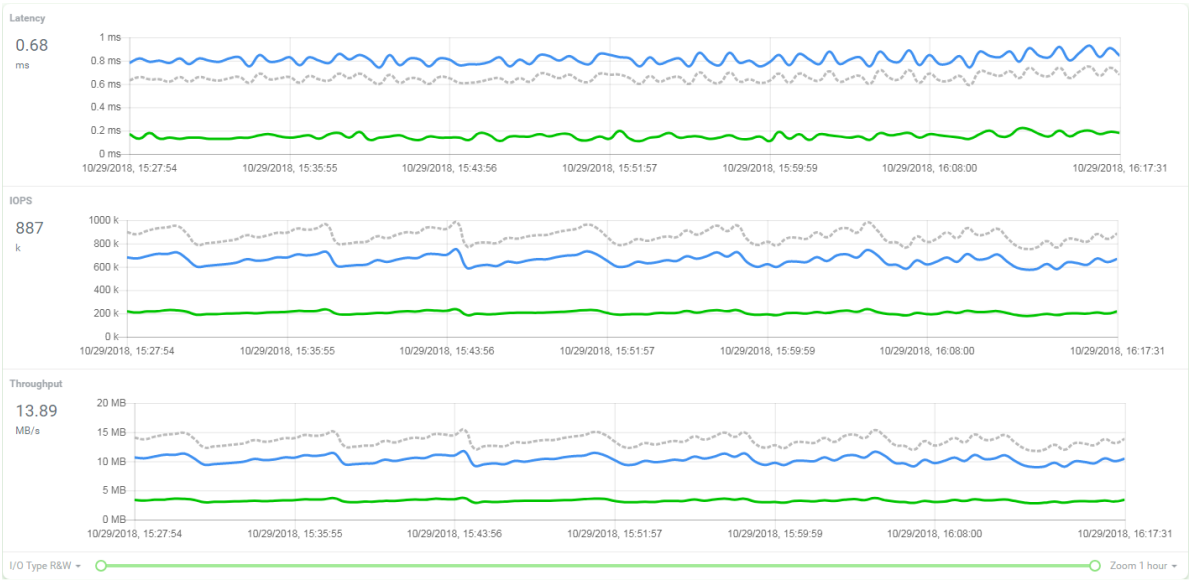


Figure 4-6 Performance Graphs in the Dashboard

The performance graphs include the Latency, IOPS, and Bandwidth graphs.

- **Latency:** The Latency graph displays the average time it takes the array to process a read, write, or read+write I/O request. The blue line represents the average read time, measured in milliseconds; it takes the array to perform a read I/O operation. The green line represents the average write time, measured in milliseconds; it takes the array to perform a write I/O operation. The dotted gray line represents the average read+write time, also measured in milliseconds; it takes the array to perform a read+write I/O operation.
- **IOPS:** The IOPS (Input/output Operations Per Second) graph displays host I/O requests processed per second by the array. The counts request per second, regardless of how much data is transferred in each. The blue line represents the number of read requests processed per second. The green line represents the number of write requests processed per second. The dotted gray line represents total read+write requests processed per second.
- **Bandwidth:** The Bandwidth graph displays the number of bytes transferred per second to and from all hosts. The data is counted to reflect what is transferred over the storage network. The blue line represents the number of bytes read per second. The green line

represents the number of bytes written per second. The dotted gray line represents the number of bytes read+written per second.

The performance graphs display the performance metrics in real time along with a scrolling graph; the incoming data appears along the right side of each graph as older numbers drop off the left side. Click the I/O Type drop-down arrow in the bottom-left corner of the window to filter the performance metrics of read, write, or read+write. By default, the performance graphs display performance metrics for the past 1 hour. Click the Zoom drop-down arrow in the bottom-right corner of the window to view performance metrics from as recent as 1 hour to as far back as 1 year. Drag the Range buttons to further narrow the view to a specific range of time.

Figure 4-7 Performance Indicator in the Dashboard

Hover your mouse over the line and click to display the point-in-time performance indicator. It shows the detailed number of read, write, and read+write. Clicking the "x" on the upper right corner will turn off the indicator.

INFORMATION:

The performance graphs present the information as the following.

- The performance graphs are updated once every 1 minute.
- The performance graphs display up to 1 year's worth of historical data.

4.1.6. Introduce the Upper Right Corner Icons

At the top right corner, there are four icons and one login name.

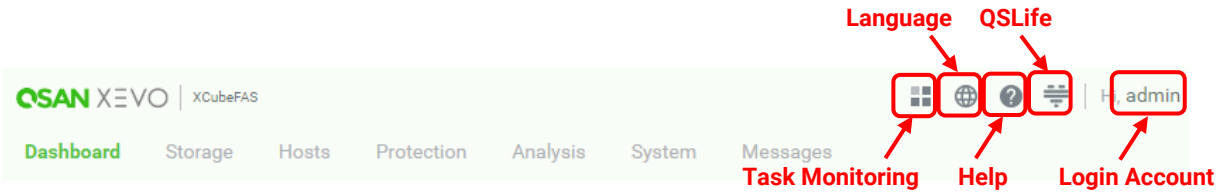


Figure 4-8 Upper Right Corner Icons

The options are available in these icons.

Task Monitoring

Click the icon at the top right corner to popup a window.

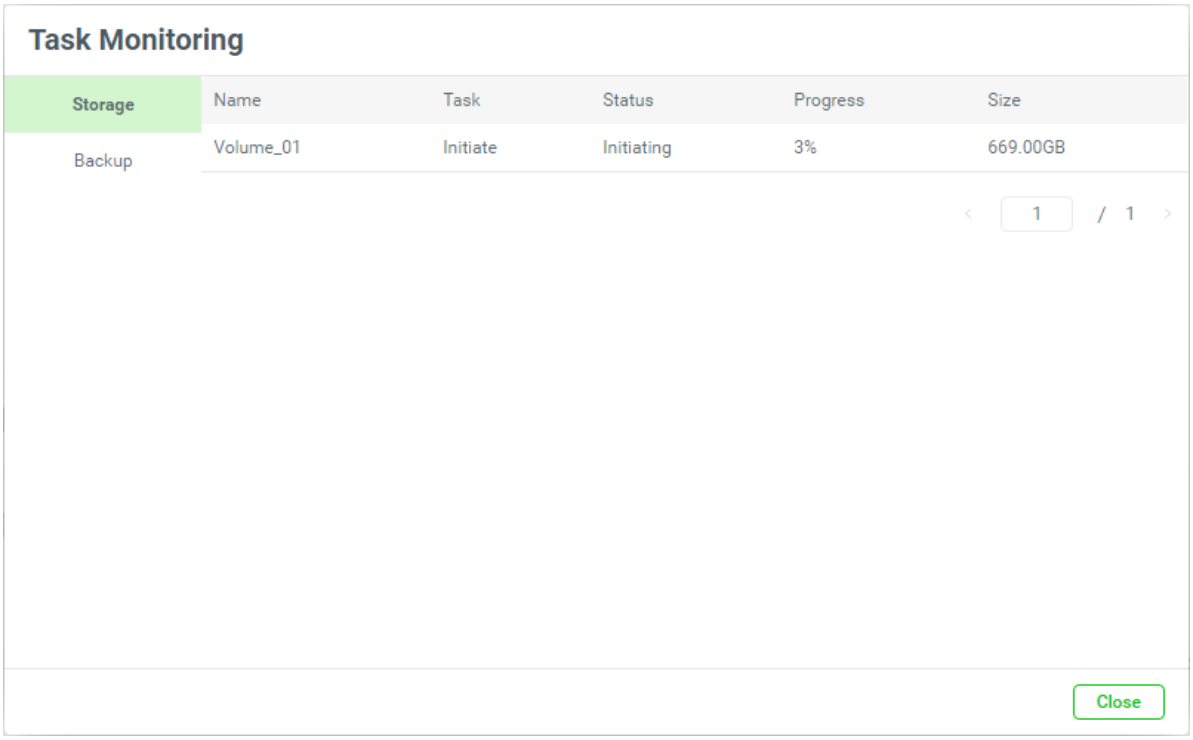


Figure 4-9 Task Monitoring

It displays the task monitoring of the system. The example shows that the Volume_01 is initialing at 3%. There are two tabs to choose from. **Storage** tab displays the process of storage tasks, and the other **Backup** tab displays the progress of backup tasks.

Language

Click the icon in the upper right corner to list the drop down options to change the language in the web UI.

Help

Click the icon in the upper right corner to popup the help information.

QSLife

Click the icon in the upper right corner to popup a window for QSLife functions. About the QSLife, please refer to the chapter 4.2, Introduct QSLife Functions for more details.

Login Account

Click the username in the upper right corner to list the drop down options to execute the system functions.

4.2. Introduce QSLife Functions

QSLife (QSAN SSD Life) is based on a specific algorithm to decrypt the attributes within the SSD to display detailed information. SSD has become the basic usage of the storage system as a mature and reliable data protection device. However, with the rapid growth in data storage capacity demand and the emergence of higher performance applications in recent years, SSDs have gradually exposed their flaws.

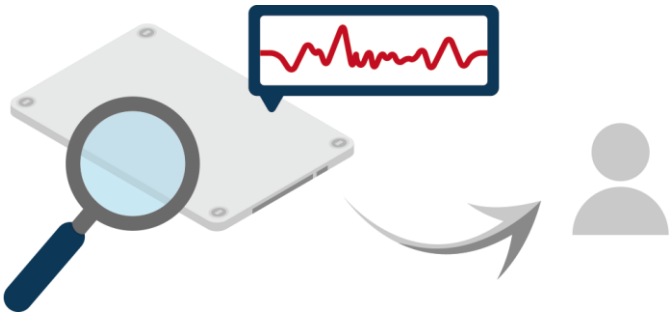


Figure 4-10 QSLife

SSDs today are almost universally comprised of NAND flash, which wears out with use. Each flash memory cell can only be written specific times before it becomes unreliable. As the number of I/O increases, the number of SSDs writes also increases significantly. This is one of the toughest issues in enterprise storage management today. In the past few days when SSDs were only written from 10GB to 100GB, the lifespan of SSDs was not a problem without special attention. However, as daily writes grow to hundreds of gigabytes or even terabytes, SSD's remaining life management will be one of the major issues in storage management.

This section will describe the operations of checking SSDs' status and the threshold settings. Click the **QSLife icon** to popup a window.

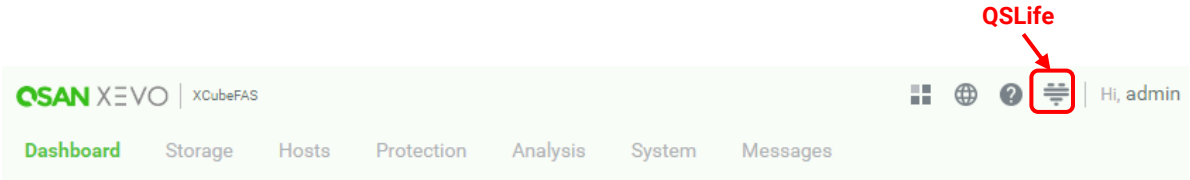


Figure 4-11 QSLife Icon

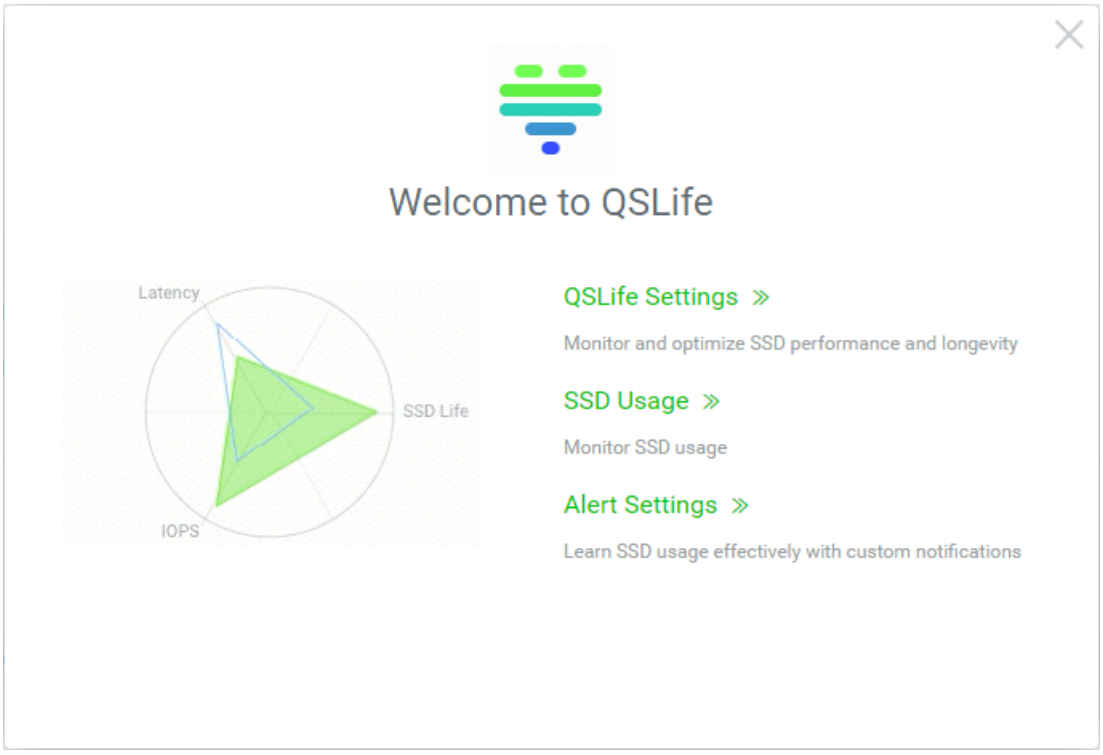


Figure 4-12 QSLife Popup Window

4.2.1. Check Life Remaining of SSD

Select the **QSLife Settings** function menu in the **QSLife** popup window. It will go to **QSLife Settings** function tab which is used to monitor and optimize SSD performance and longevity. Here is an example of checking the life remaining of the SSD.

1. Select a unit at the **Array** function submenu. It will scan and display all SSDs of this unit.

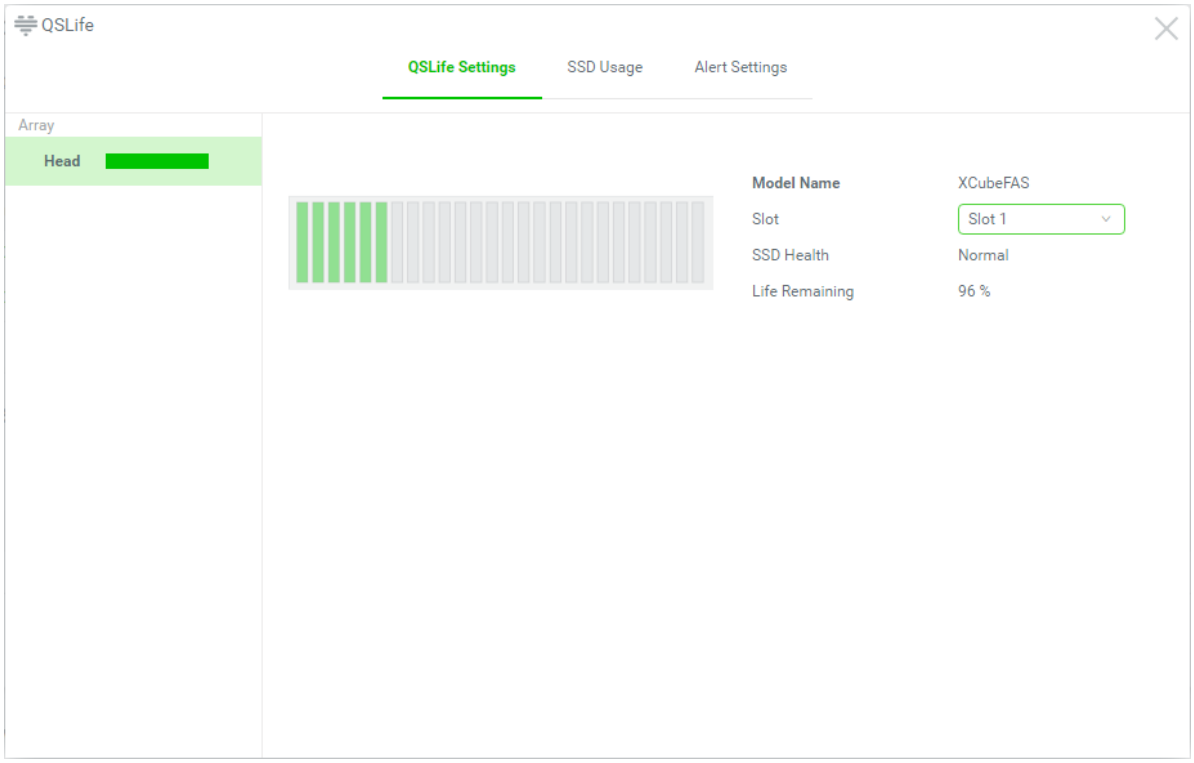


Figure 4-13 QSLife Settings

2. Select an SSD which you want to watch in **Slot,** the system will display the health status and the life remaining of the SSD. It is highly recommended to replace the SSD if the life remaining is under 10%.

4.2.2. Check SSD Usage

Select the **SSD Usage** function tab in the **QSLife** to be used to monitor the SSD usage status and history. With this information, we can easily estimate the actual DWPD required for a more accurate procurement strategy. Here is an example of checking the SSD usage.

1. Select a unit at the **Array** function submenu. It will scan and display all SSDs of this unit.

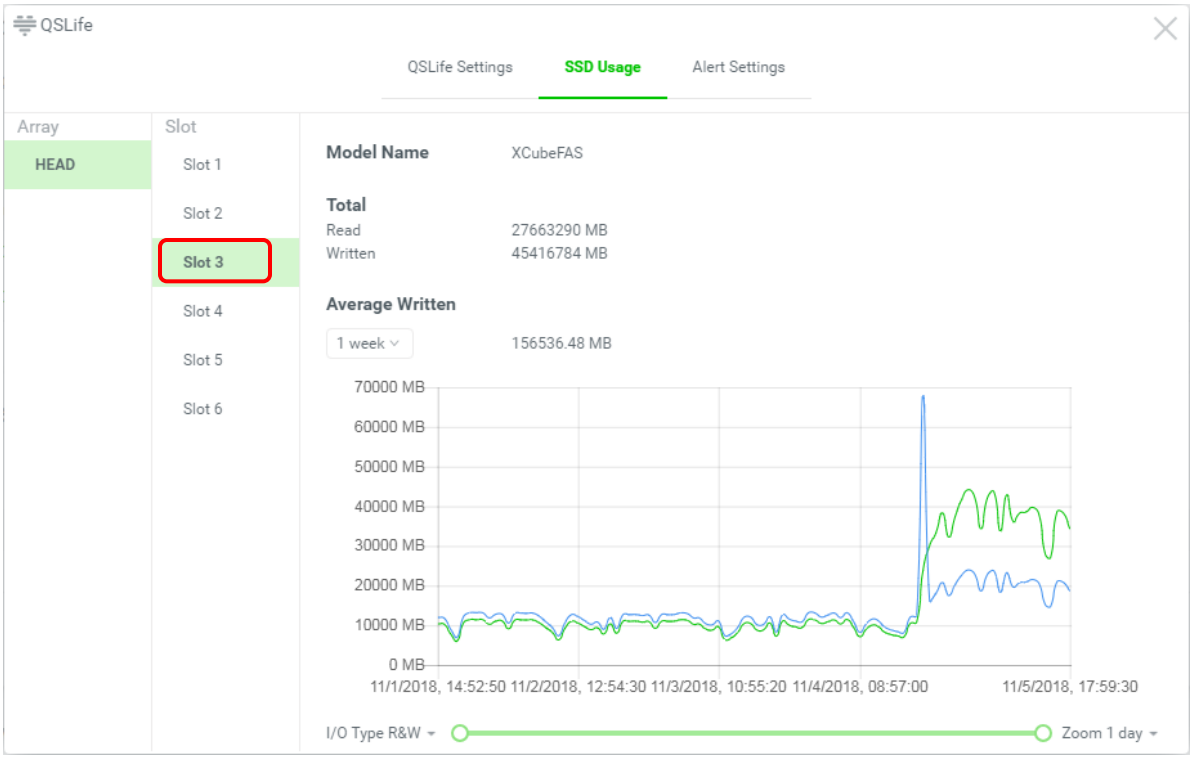


Figure 4-14 SSD Usage Step 1

2. Select an SSD which you want to watch in **Slot,** the system will display the SSD usage information. It includes a usage history of up to 1 year for analyzing the actual usage of your business.

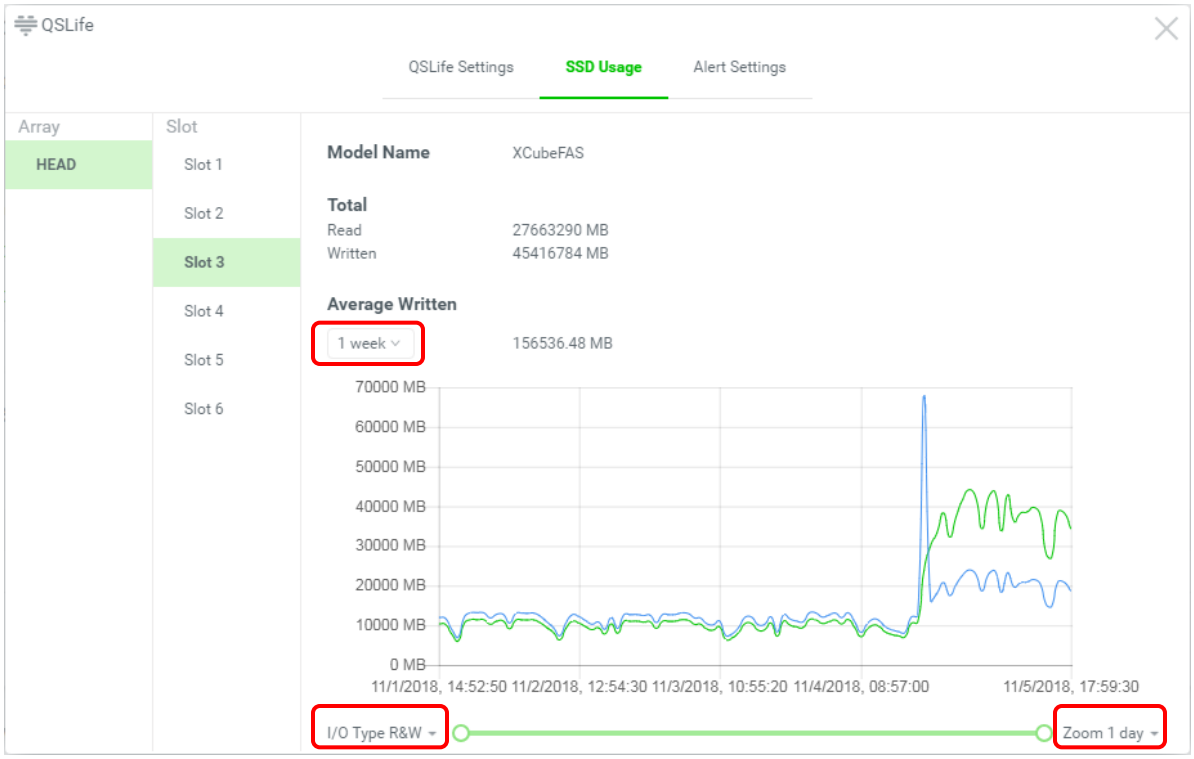


Figure 4-15 SSD Usage Step 2

3. It displays the **Total** read and written bytes of the SSD from the beginning.

Options on SSD Usage

- **Average Written:** The period of average written can be changed to display the current average written bytes. The options are average 1 week, 1 month, and 1 year.
- **I/O Type:** The I/O type of the SSD usage can be changed in the diagram for a different viewpoint. The options are Read, Written, and R&W (Read & Written).
- **Zoom:** The period of the SSD usage can be changed in the diagram to watch the usage in the different period. The options are 1 day, 1 week, 1 month, and 1 year.

4.2.3. Alert Settings

Select the **Alert Settings** function tab in the **QSLife** to be used to learn SSD usage effectively with custom notifications. User can customize the SSD endurance threshold settings at this page. Here is an example of setting the SSD alert.

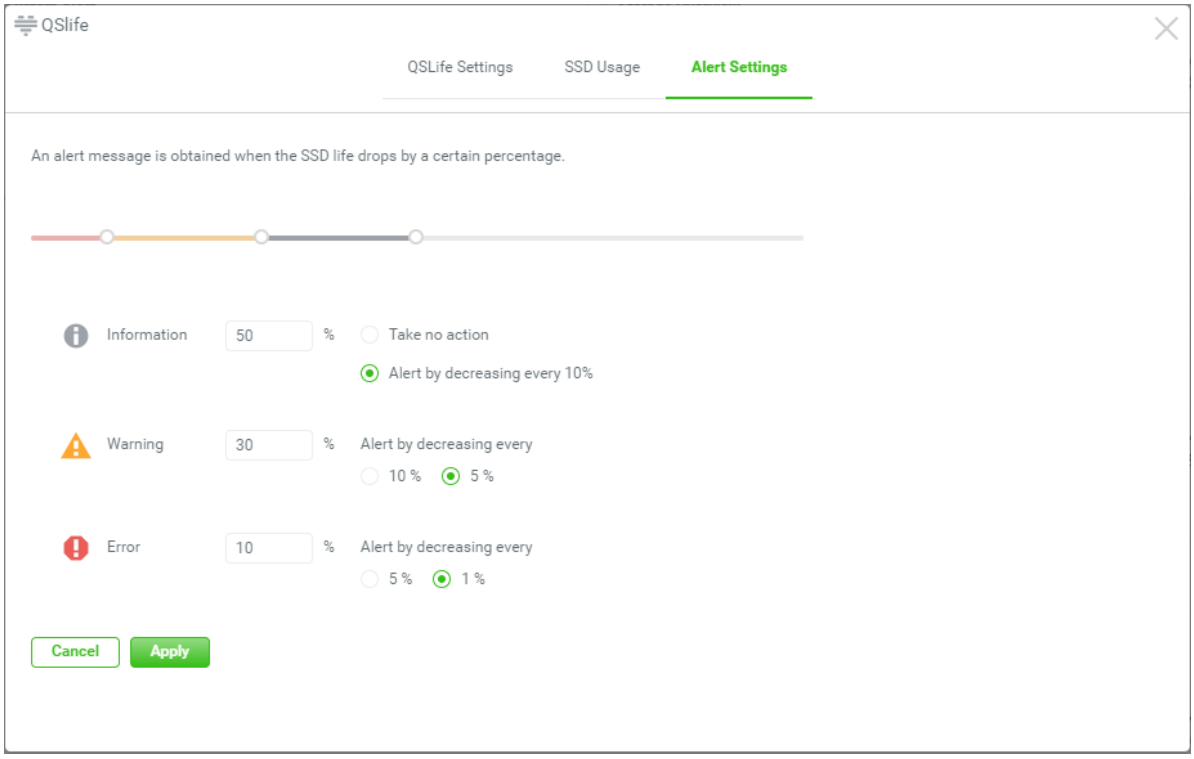


Figure 4-16 Alert Settings

1. There are three levels of the alert can be set. The options include **Information**, **Warning**, and **Error**. Drag the dot on the slide bar or enter the percentages of the SSD endurance thresholds. The actions can also be changed at every alert level.
2. Then press the **Apply** button to confirm your configurations.

If you use the default alert settings, the Information level sets 50% and the option sets **Alert by decreasing every 10%**, you will receive the notifications when the life remaining of every SSD reaches 50%, 40%, and 30% in the **Information** level. Alert by decreasing every **5%** during 30% to 10% in the **Warning** level. Finally, you may receive the notifications by decreasing every **1%** in the **Error** level. The purpose is to keep you informed that the SSD should be replaced during the life remaining counts down.

5. Storage Tab

The **Storage** tab manages the storage pools. It displays the storage pool status, configures the storage pool, and takes snapshots. This chapter describes the details of storage management operations and examples.

INFORMATION:
For the storage technologies of RAID, storage pool, volume, and LUN mapping, please refer to the chapter 8, Storage Management in the QSAN Software Manual SANOS 4.0.

5.1. Configure Storage Pools

Select the **Storage** tab to manage the storage pools. In this tab, you can create, modify, delete, or view the status of all pools.

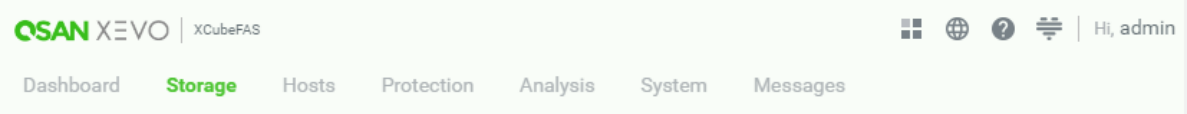


Figure 5-1 Storage Tab

5.1.1. Create a Pool

We design smart storage wizards for deployment in a few clicks, and also provide recommend configurations to set up quickly. Here is an example of creating a thick provisioning pool with 3 disks configured in RAID 5. At the first time of creating a thick provisioning pool, it contains a disk group and the maximum quantity of disk in a disk group is 64.

1. Click the + icon in the **Pools** pane to pop up a wizard.

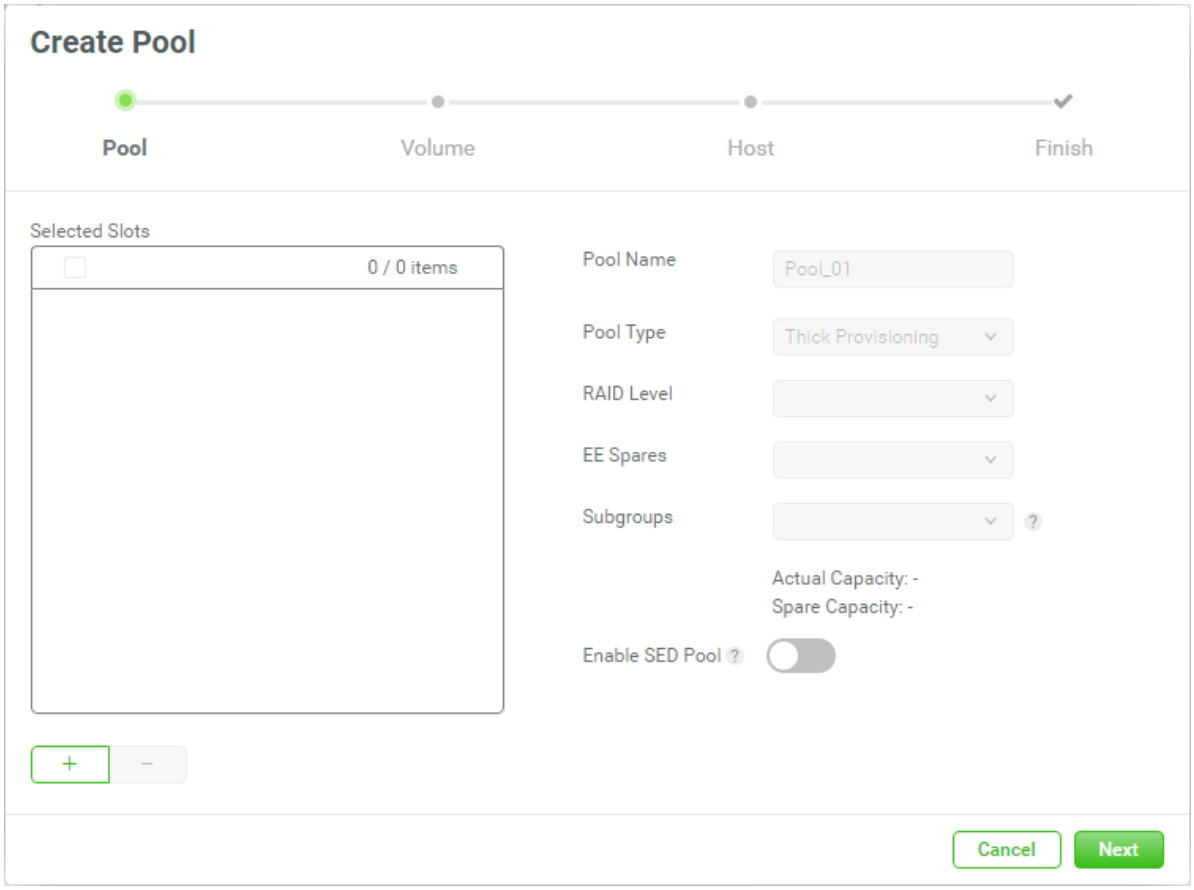


Figure 5-2 Create a Pool Step 1-1

2. Click the + icon to select disks to add into the pool.

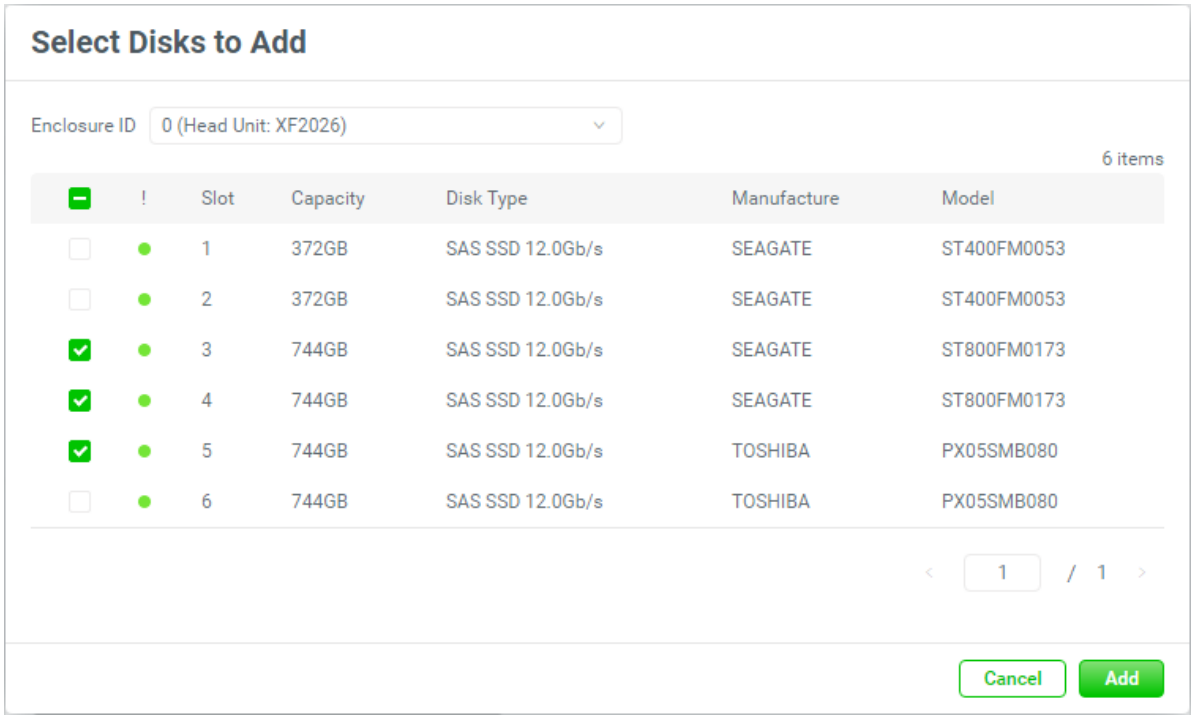


Figure 5-3 Select Disks to Add

3. Check disk slots which you want to add. The maximum quantity of disk in a disk group is 64. Select an **Enclosure ID** from the drop-down list to select disks from expansion enclosures. Then click the **Add** button to continue.

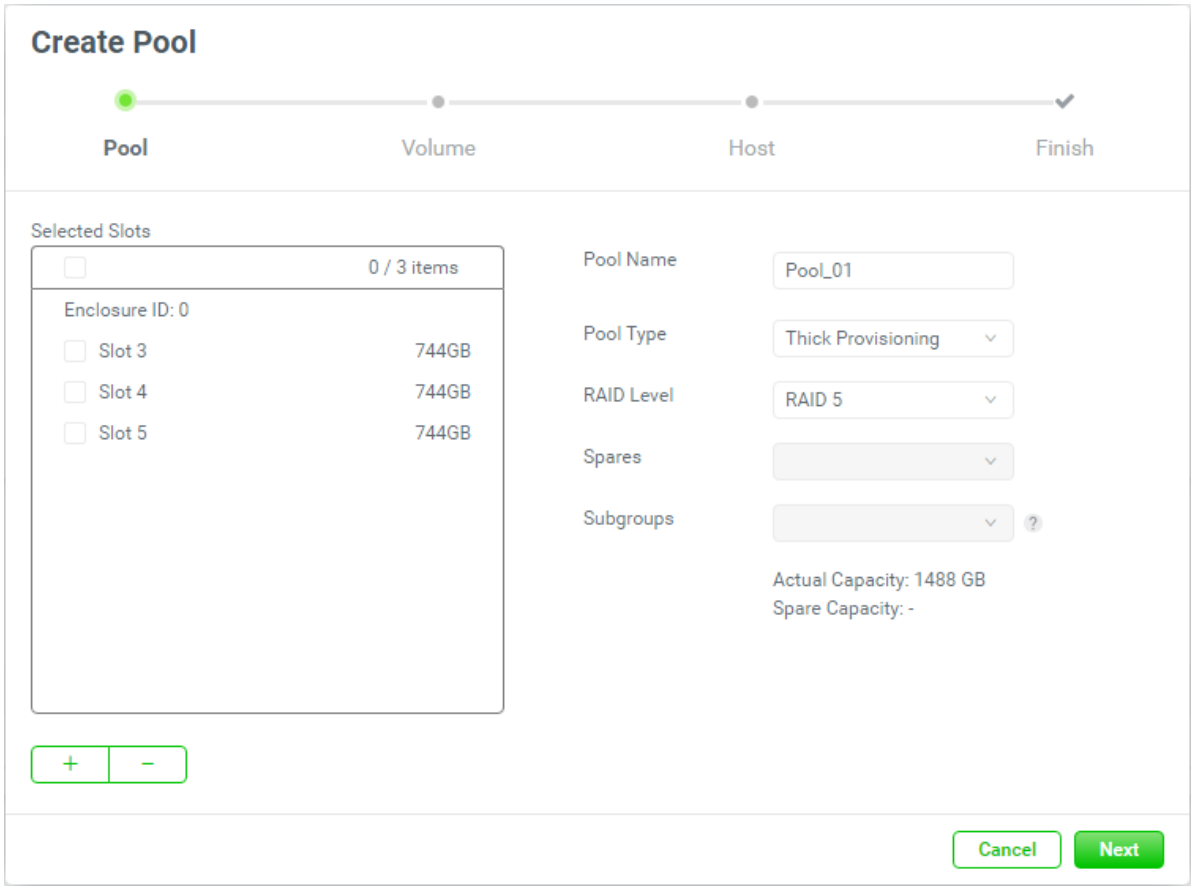


Figure 5-4 Create a Pool Step 1-2

4. The selected disk slots are listed in the box and can be removed. Check disk slots which you want to remove and then click the − button.
5. The recommended **Pool Name**, **Pool Type**, and **RAID Level** are provided. Enter a new **Pool Name** if necessary. The maximum length of the pool name is 16 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
6. Change the **Pool Type** with the drop down options. There are Thick Provisioning, and Thin Provisioning options.
7. The recommended **RAID Level** depends on the number of disks you select. The same, it can be changed with the drop down options.
8. Select the RAID EE **Spares** if you select the RAID EE level. Select the **Subgroups** if you select the compound RAID level.
9. Click the **Next** button to continue.

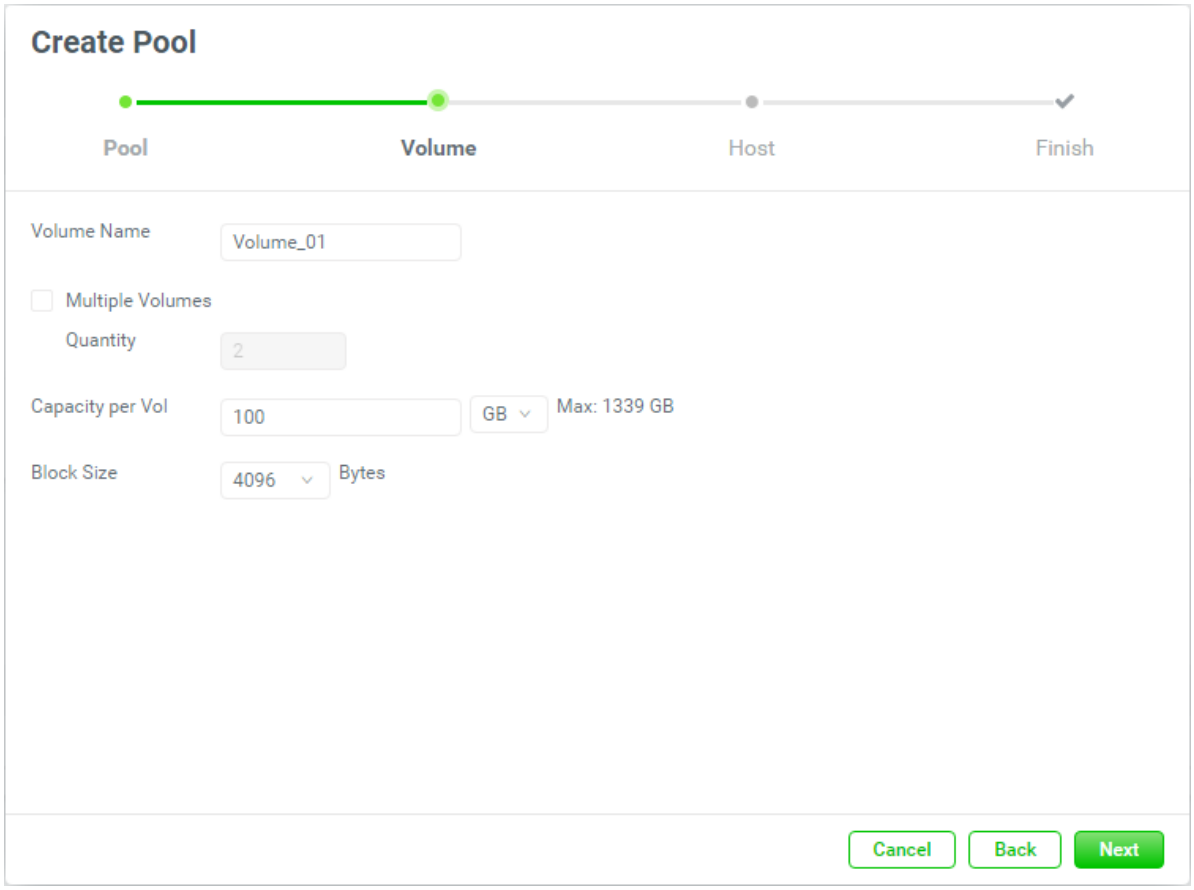


Figure 5-5 Create a Pool Step 2

10. The recommended **Volume Name**, **Capacity per Vol**, and **Block Size** are provided. Enter a new **Volume Name** if necessary. The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
11. Check the **Multiple Volumes** checkbox if you want to create multiple volumes at once. Then enter a number for **Quantity**. The maximum quantity is 64.
12. The recommended **Capacity per Vol** is the maximum capacity which can be created. Change it if necessary. At this time, change it to 100GB.
13. Change the **Block Size** with the drop down options. The options are 512 Bytes to 4,096 Bytes.
14. Click the **Next** button to continue.

TIP:
The system automatically reserves 10% of the pool capacity for snapshot space.

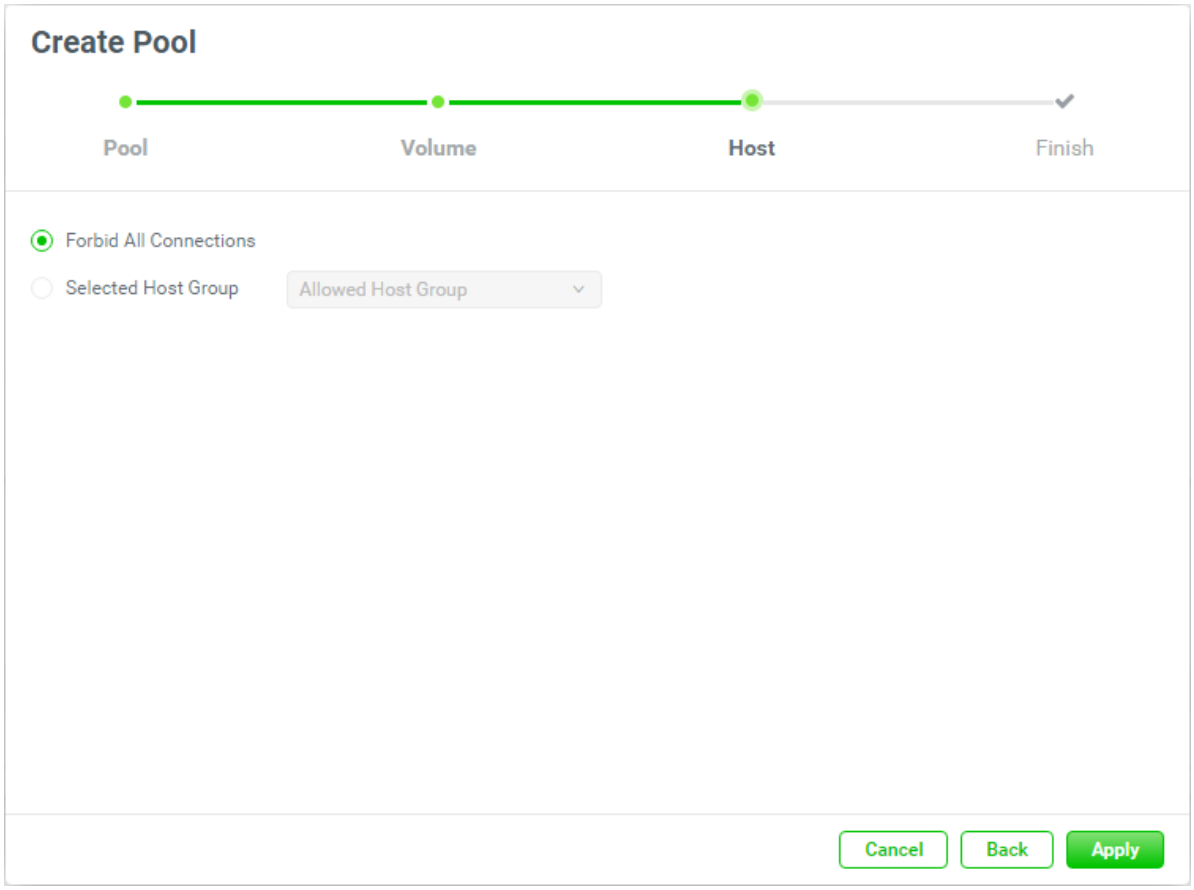


Figure 5-6 Create a Pool Step 3

15. If there are host groups which are created already, check the **Selected Host Group** checkbox and select a host group with the drop down options. Or keep it default as **Forbid All Connections** and change it later.
16. Click the **Apply** button to continue.

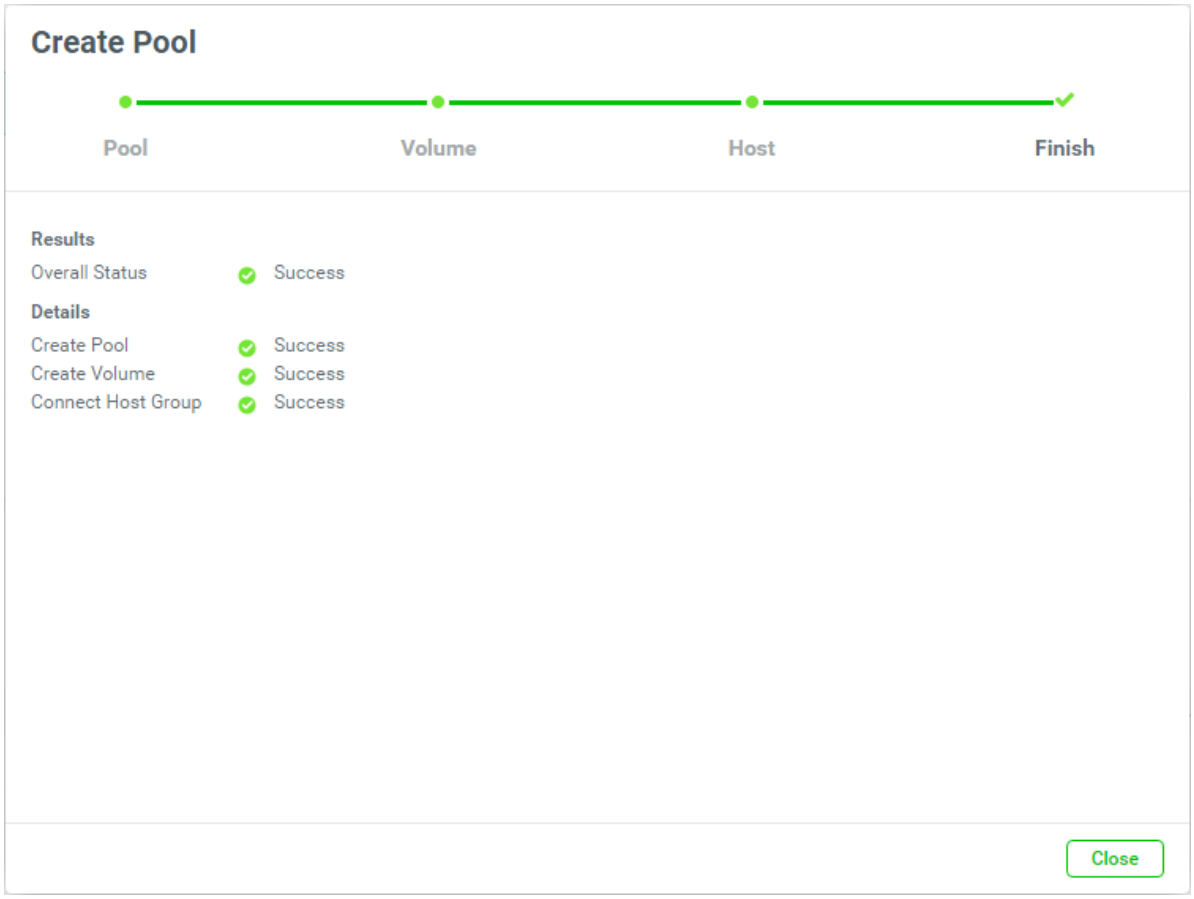


Figure 5-7 Create a Pool Step 4

17. There is a result page. Click the **Close** button to finish.

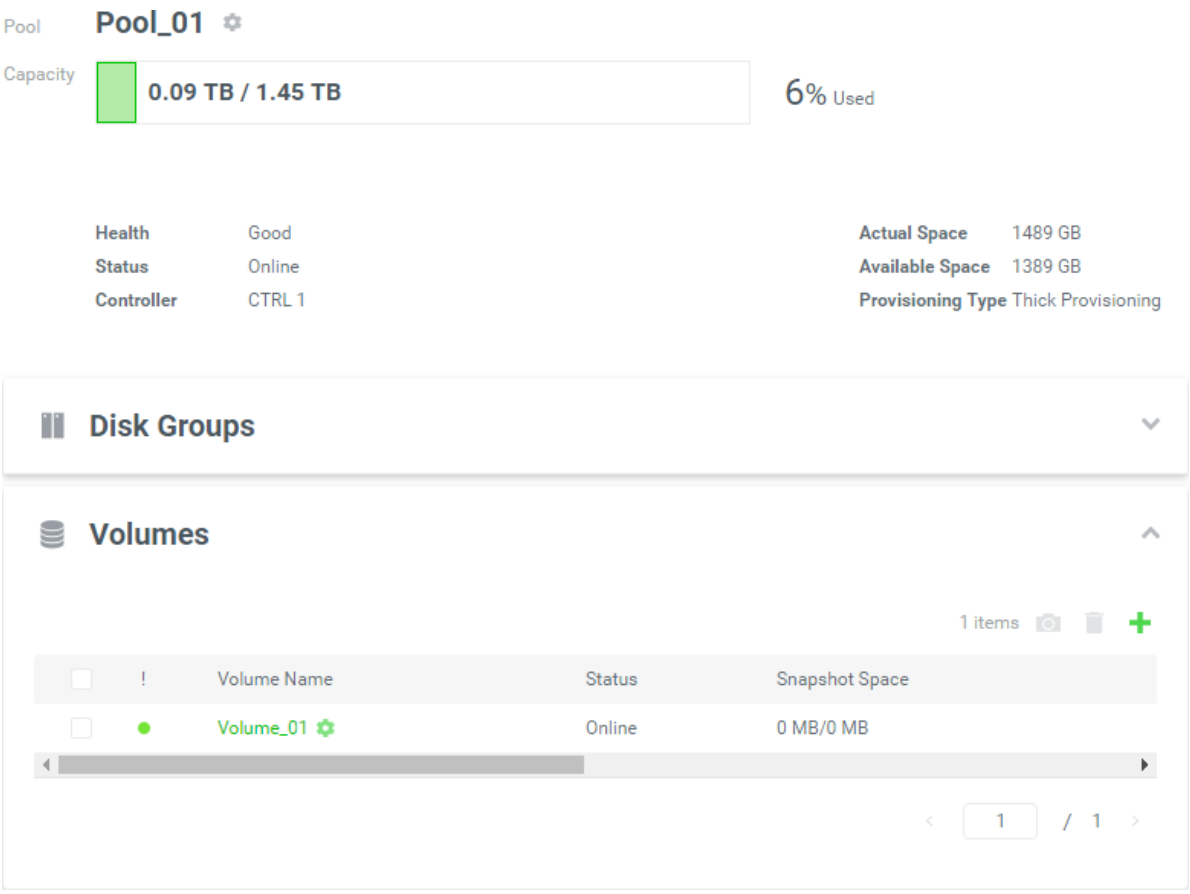


Figure 5-8 A Pool is Created

18. A pool with a volume has been created. If necessary, click the + icon in the **Pools** pane to create others.

5.1.2. List and Configure Pools

All pools are listed in the **Pools** pane. You can click one of them to display the details.

Figure 5-9 List All Pools

A thick provisioning pool and a thin provisioning pool are shown here.

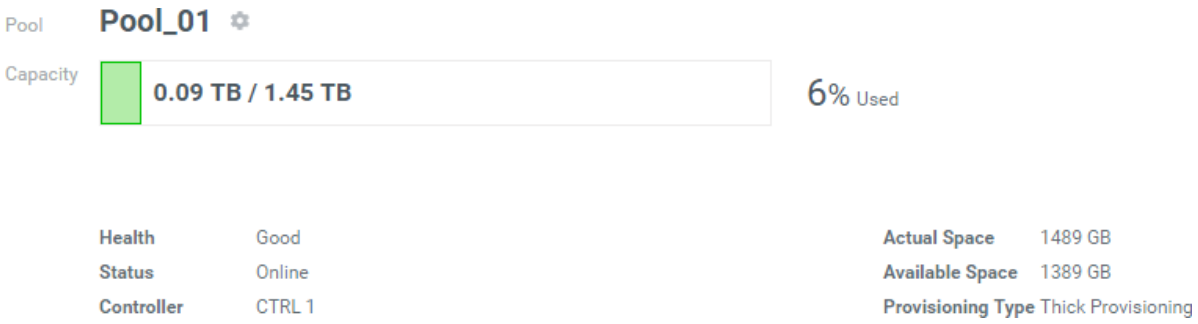


Figure 5-10 Thick Provisioning Pool Details

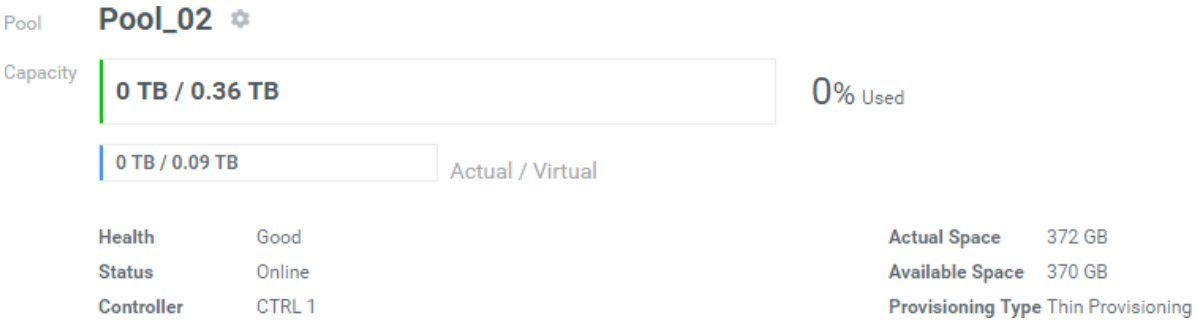


Figure 5-11 Thin Provisioning Pool Details

This table shows the pool descriptions.

Table 5-1 Pool Column Descriptions

Column Name	Description
Pool	The pool name.
Capacity	The bar color: • Green Bar: Fewer than 90% used space. • Orange Bar: 90% ~ 100% used space. • Red Bar: 100% used space. The number in the bar: • Used space / Actual space The 2nd bar is only visible when the pool type is thin provisioning: • Actual used space / Virtual space
Health	The health of the pool: • Good: The pool is good. • Abnormal: The pool is unhealthy and incomplete. The cause may

	be a disk loss or failure. • Warning: The pool has failed.
Status	The status of the pool: • Online: The pool is online. • Offline: The pool is offline. • Rebuilding: The pool is being rebuilt. • Migrating: The pool is being migrated. • Relocating: The pool is being relocated. • EE Rebuilding: The pool is being RAID EE rebuilt.
Controller	The current running controller of the pool.
Actual Space	Total capacity of the pool.
Available Space	Available capacity of the pool.
Virtual Space	Virtual capacity of the pool.
Provisioning Type	The provisioning type of the pool: • Thick Provisioning. • Thin Provisioning.

Click the icon beside the pool name to list the drop down options. These options are available in the pool.

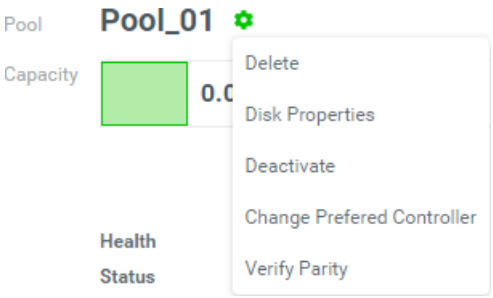


Figure 5-12 Pool Options

Delete

Click the **Delete** option to delete the pool. Click the **Apply** button to confirm and delete.

TIP:
The pool cannot be deleted when there are volumes in the pool.

Disk Properties

1. Click the **Disk Properties** option to change disk properties of the pool.

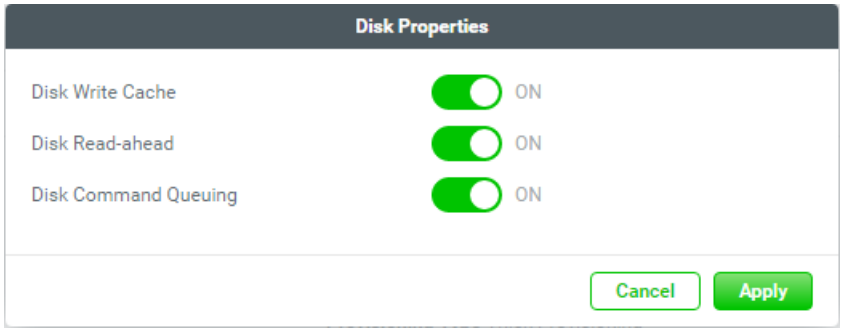


Figure 5-13 Change Disk Properties

2. Click the switch to turn ON (Enable) or OFF (Disable).
   - **Disk Write Cache**: Enabling the disk write cache will improve write I/O performance but have a risk of losing data when power failure.
   - **Disk Read-ahead**: When enabling the disk read-ahead, the system will preload data to disk buffer based on previously retrieved data. This feature will efficiently improve the performance of sequential data retrieved.
   - **Disk Command Queuing**: When enabling the disk command queuing, the system will send multiple commands to a disk at once to improve performance.
3. After change the disk properties, click the **Apply** button to take effect.

Activate or Deactivate

Click the **Activate** or **Deactivate** option to activate or deactivate the pool. Click the **Apply** button to confirm.

TIP:
These options are usually used for online disk roaming. Deactivate can be executed when the status is online. Conversely, activate can be executed when the pool status is offline.

Change Preferred Controller

1. Click the **Change Preferred Controller** option to change the pool ownership to the other controller.

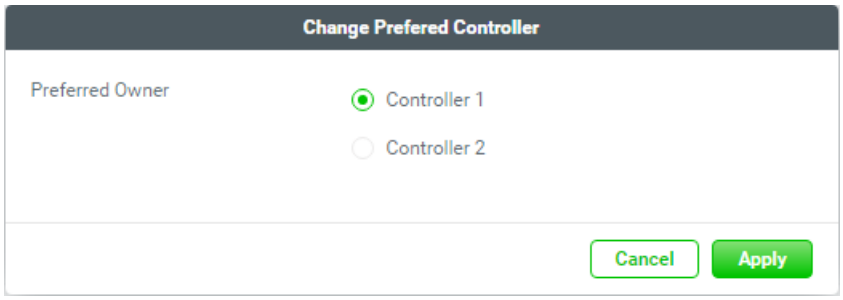


Figure 5-14 Change Preferred Controller

2. Select **Controller 1** or **Controller 2**, and then click the **Apply** button to take effect.

Thin Provisioning Policy *(Only visible when the pool type is thin provisioning)*

1. Click the **Thin Provisioning Policy** option to change policy of the thin provisioning pool.

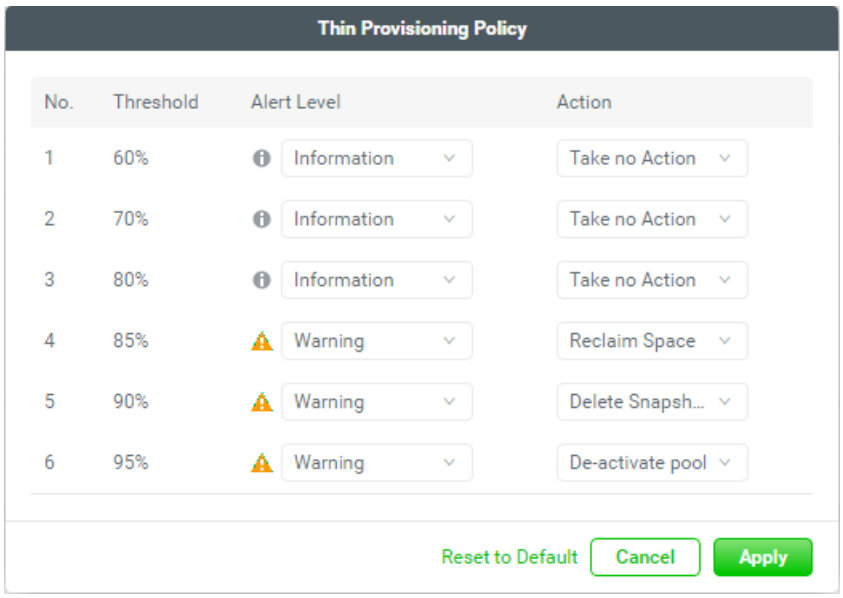


Figure 5-15 Change Thin Provisioning Policy

2. There are 6 levels of threshold percentage and the default values defined. The event log levels and actions can be changed when the usage of the pool capacity reaches the threshold.

3. After change the thin provisioning policies, click the **Apply** button to take effect.

Verify Parity

Click the **Verify Parity** option to regenerate parity for the pool. Click the **Apply** button to confirm and proceed.

INFORMATION:
It supports RAID level 3, 5, 6, 30, 50, 60 and RAID EE level 5EE, 6EE, 50EE, 60EE.

5.1.3. List and Configure Disk Groups

Click the **Disk Groups** pane to list all disk groups in the pool.

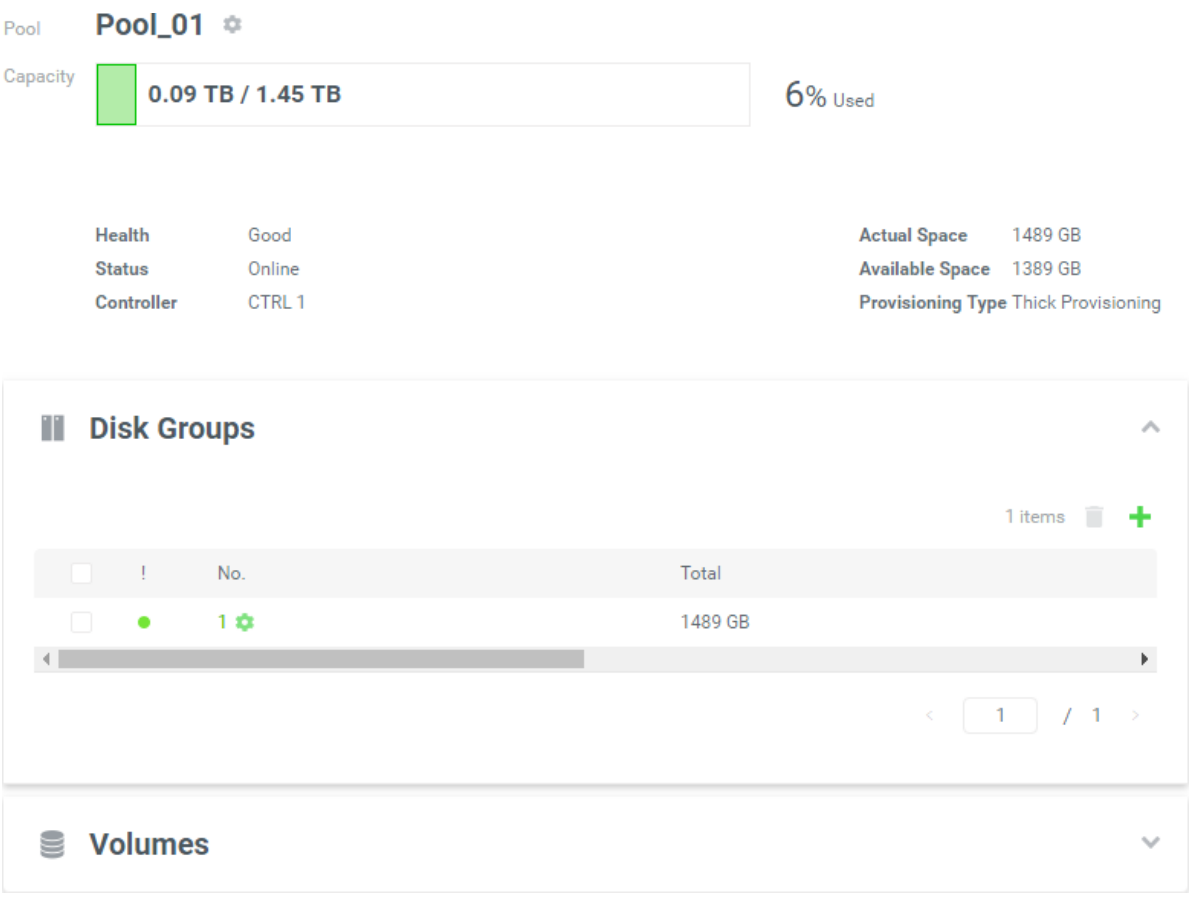


Figure 5-16 List Disk Groups

This table shows the disk group descriptions.

Table 5-2 Disk Group Column Descriptions

Column Name	Description
!	The status of the disk group: • Green Color / Normal: The disk group is good. • Orange Color / Abnormal: The pool is unhealthy and incomplete. The cause may be a disk loss or failure. • Red Light / Warning: The disk group has failed.
No.	The number of the disk group.
Total	Total capacity of the disk group.
Disks	The quantity of disk drives in the disk group.
RAID	The RAID level of the disk group.

The options are available in this pane.

Add a Disk Group

Here is an example to add a disk group.

1. Click the + icon in the **Disk Groups** pane to pop up a window.

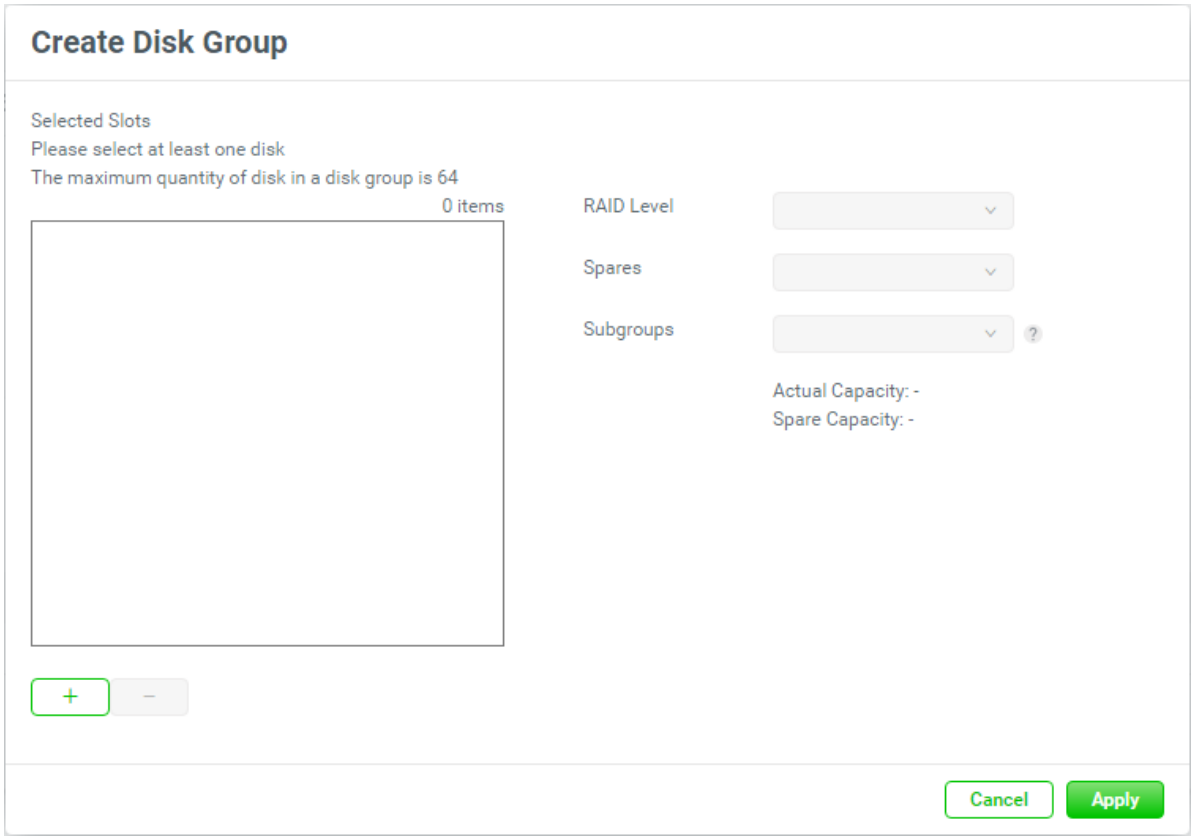


Figure 5-17 Create Disk Group

2. Click the + icon to select disks to add into the disk group

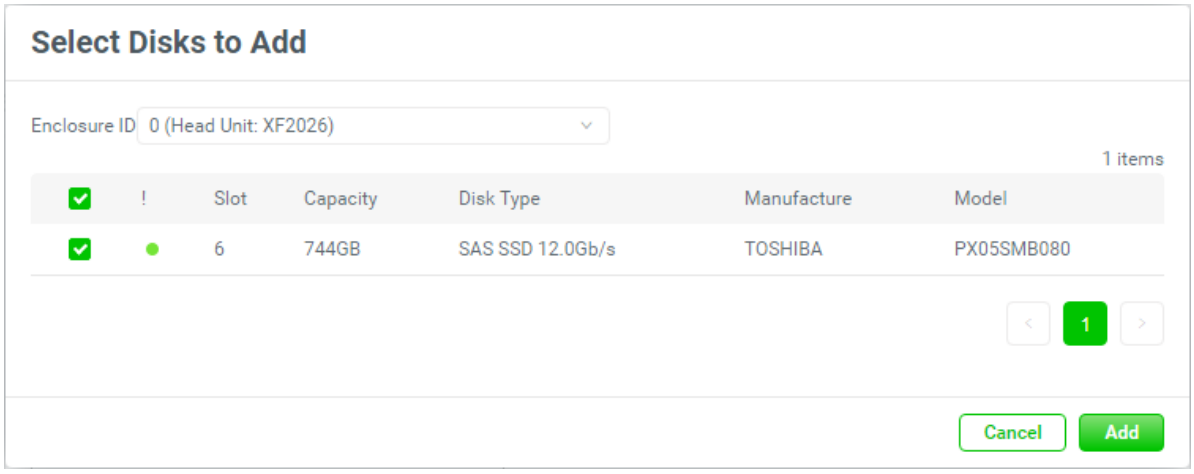


Figure 5-18 Select Disks to Add

3. Check disk slots which you want to add. The maximum quantity of disk in a disk group is 64. Select an **Enclosure ID** from the drop-down list to select disks from expansion enclosures. Then click the **Add** button to continue.

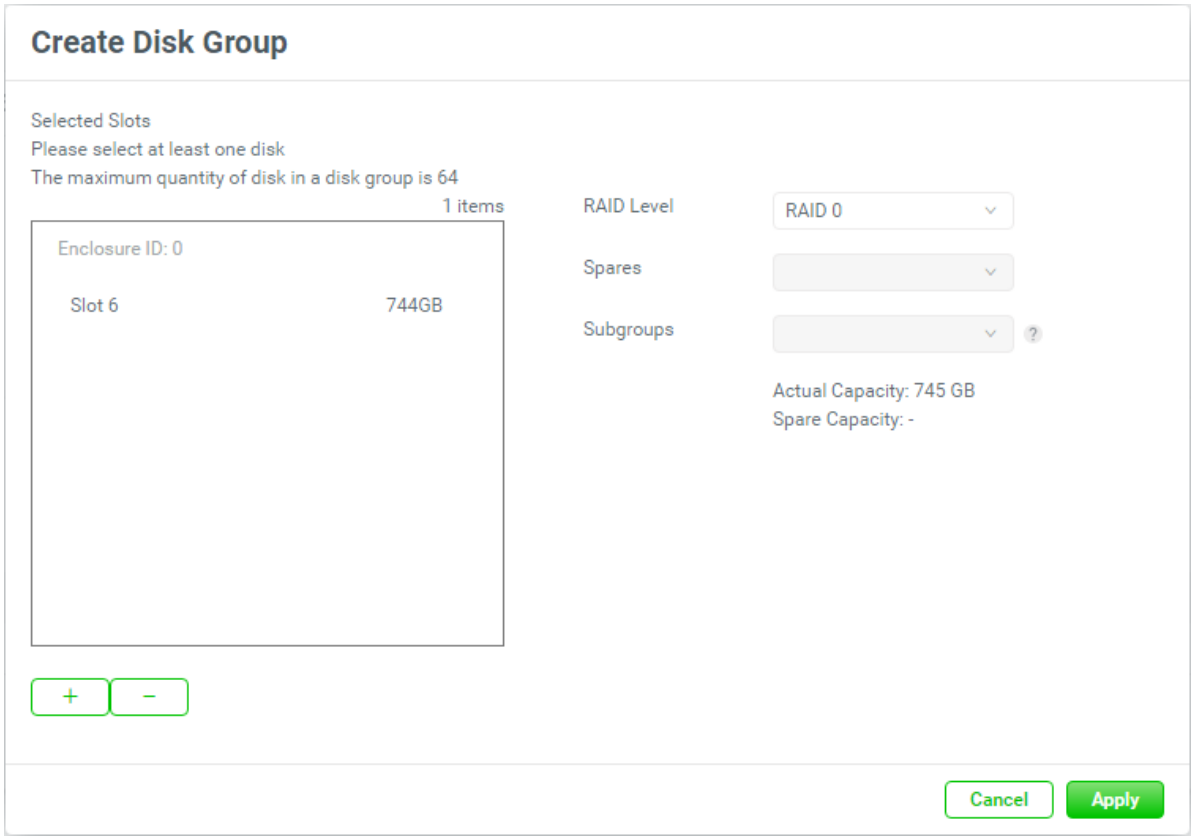


Figure 5-19 Create Disk Group

4. The selected disk slots are listed in the box and can be removed. Check disk slots which you want to remove and then click the − button.
5. The recommended **RAID Level** depends on the number of disks you select. It can be changed with the drop down options.
6. Select the RAID EE **Spares** if you select the RAID EE level. Select the **Subgroups** if you select the compound RAID level.
7. Click the **Apply** button to add a disk group.

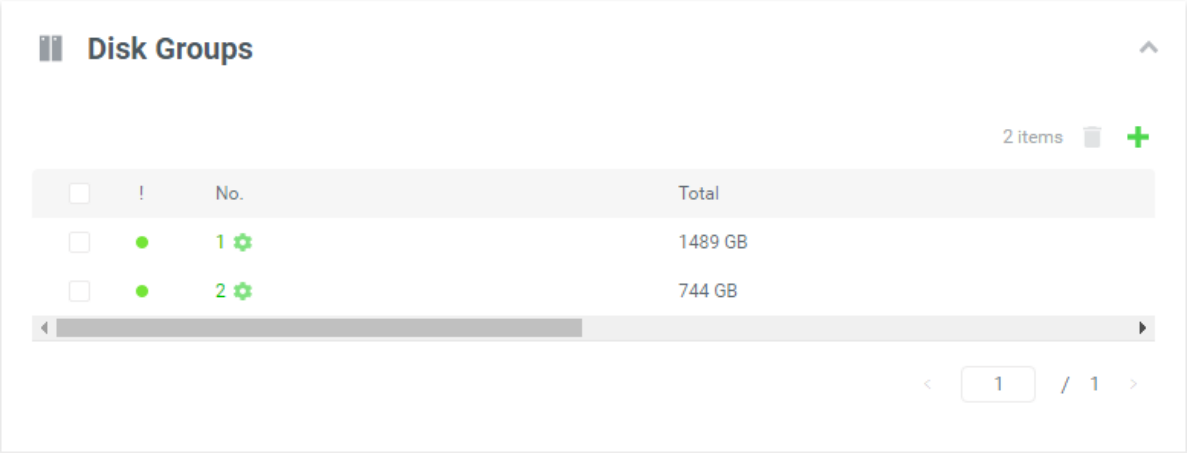


Figure 5-20 List Disk Groups

8. A disk group has been created. If necessary, click the + icon in the **Disk Groups** pane to create others.

Delete Disk Groups

1. Check the disk group checkboxes which you want to delete.

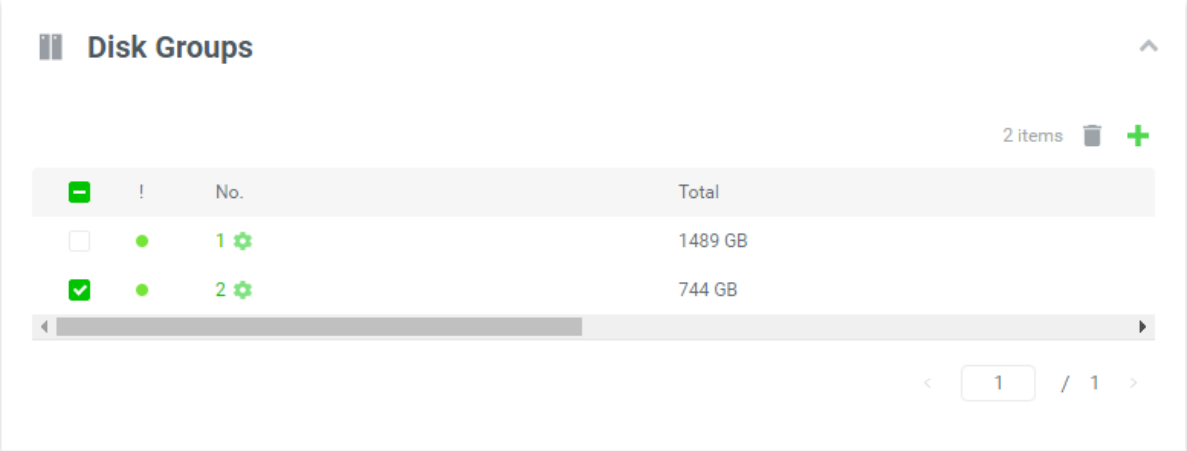


Figure 5-21 Delete Disk Groups

2. Click the icon to continue. Then click the **Apply** button to confirm and delete.

CAUTION:
If the pool contains only one disk group, it cannot be deleted. If the disk group is being used and not empty, it also cannot be deleted.

Click the icon beside the number of the disk group to list the drop down options. These options are available in the disk group.

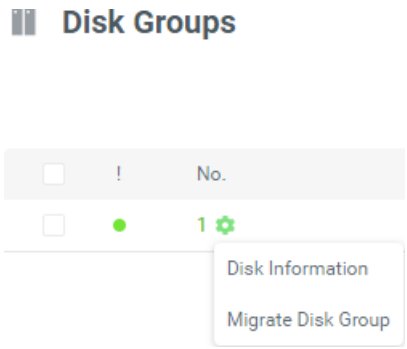


Figure 5-22 Disk Group Options

Disk Information

1. Click the **Disk Information** option to display the disk information in the disk group.

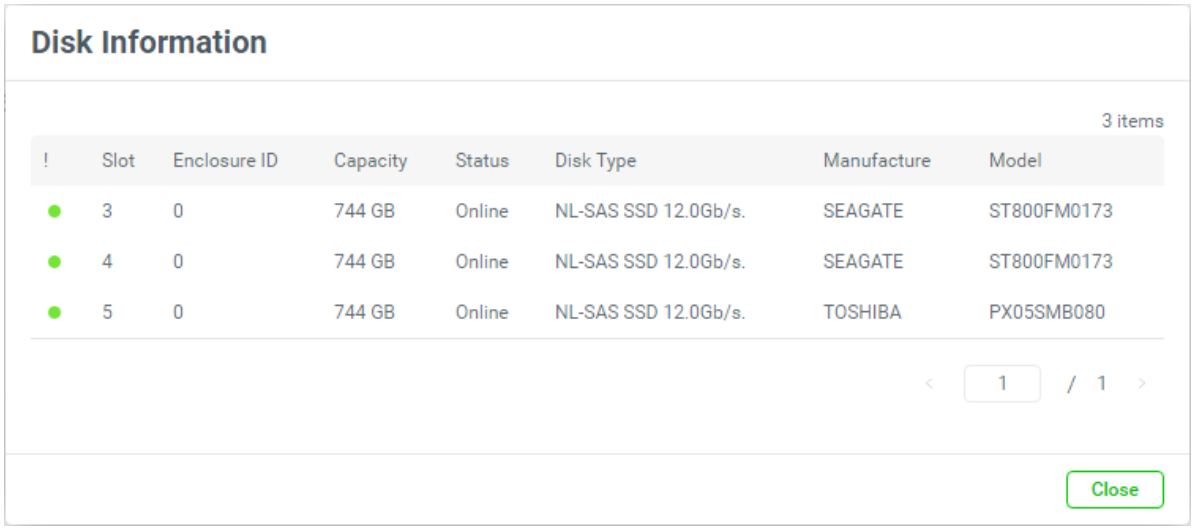


Figure 5-23 Disk Information

This table shows the disk descriptions.

Table 5-3 Disk Column Descriptions

Column Name	Description
!	The status of the disk: • Green Color / Normal: The disk drive is good. • Orange Color / Abnormal: S.M.A.R.T. error alerts or the disk drive has unrecoverable read errors. • Red Color / Warning: The disk drive has failed.
Slot	The position of the disk drive.
Enclosure ID	The enclosure ID.
Capacity	The capacity of the disk drive.
Status	The status of the disk drive: • Online: The disk drive is online. • Missing: The disk drive is missing in the pool. • Rebuilding: The disk drive is being rebuilt. • Transitioning: The disk drive is being migrated or is replaced by another disk when rebuilding occurs. • Scrubbing: The disk drive is being scrubbed. • Check Done: The disk drive has been checked the disk health. • Copying Back: The disk drive is being copied back.
Disk Type	The type of the disk drive: • [SAS HDD | NL-SAS HDD | SAS SSD | SATA SSD] • [12.0Gb/s | 6.0Gb/s | 3.0Gb/s | 1.5Gb/s]
Manufacturer	The manufacturer of the disk drive.
Model	The model name of disk drive.

2. Click the **Close** button to close the window.

Migrate Disk Group *(Only visible when the pool type is thick provisioning)*

Here is an example to migrate the disk group to RAID 6.

1. Click the **Migrate Disk Group** option to pop up a window.

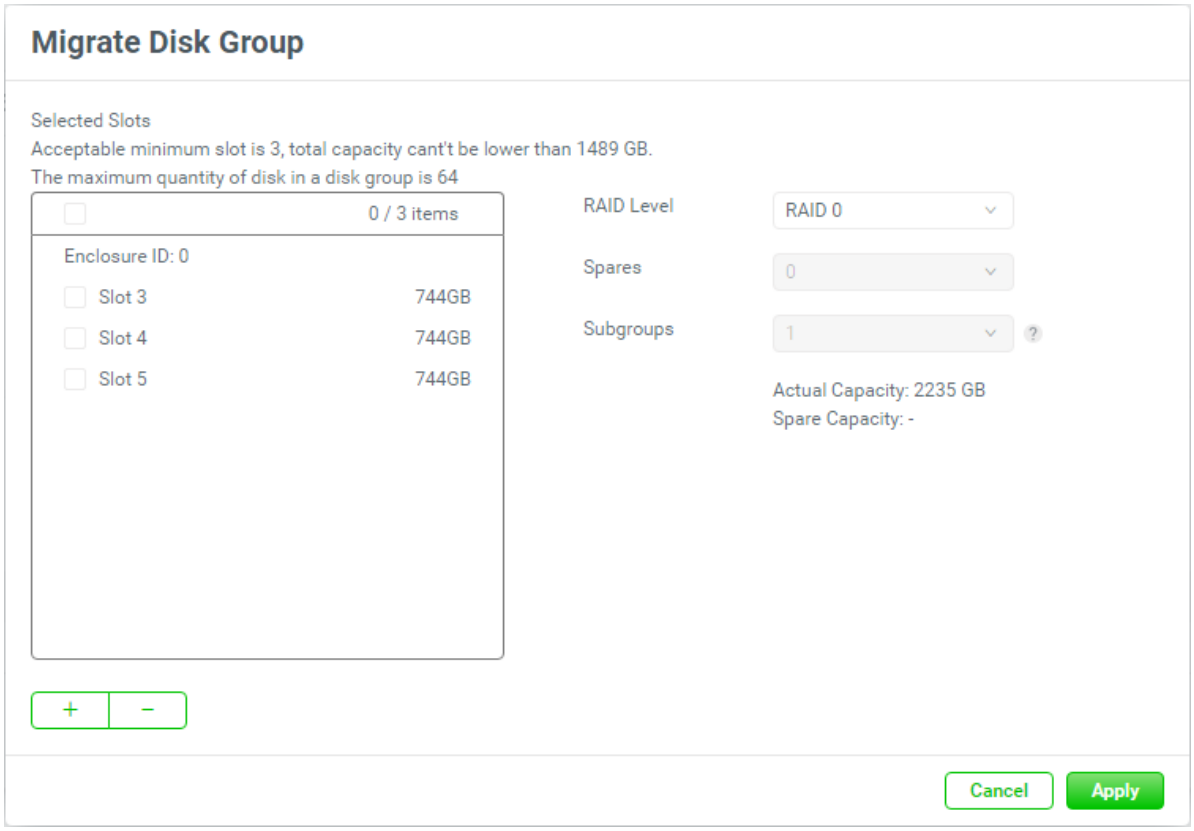


Figure 5-24 Migrate Disk Group

2. Click the + icon to select disks to add into the disk group

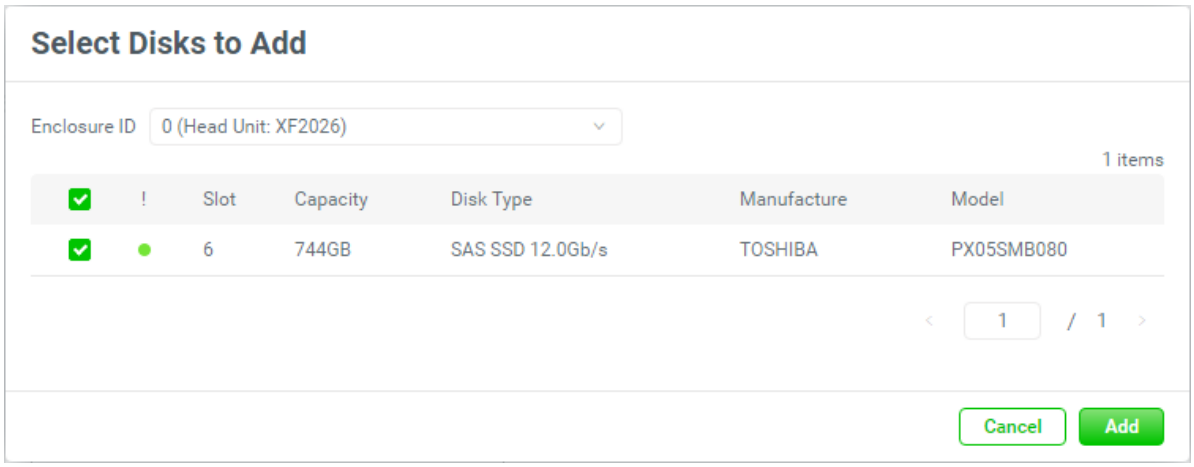


Figure 5-25 Select Disks to Add

3. Check disk slots which you want to add. The maximum quantity of disk in a disk group is 64. Select an **Enclosure ID** from the drop-down list to select disks from expansion enclosures. Then click the **Add** button to continue.

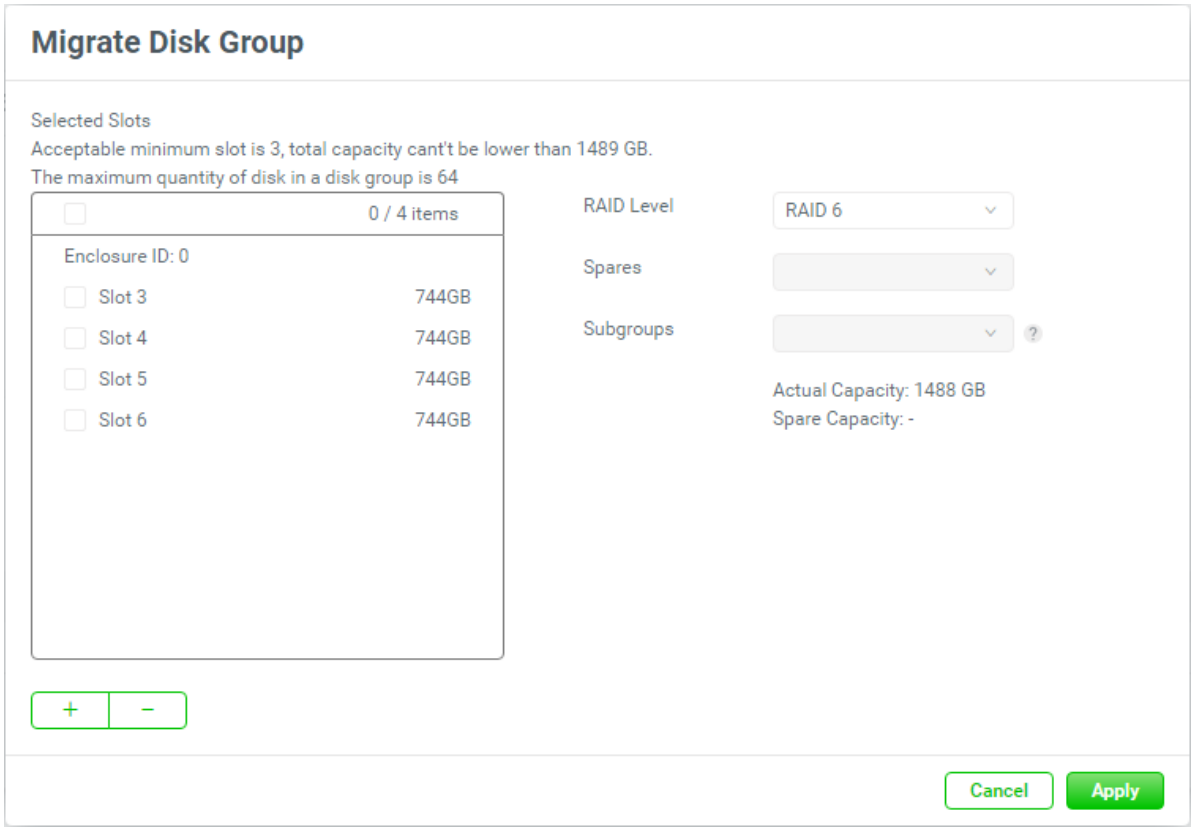


Figure 5-26 Migrate Disk Group

4. The selected disk slots are listed in the box and can be removed. Check disk slots which you want to remove and then click the − button.
5. Select the **RAID Level** which you want to migrate with the drop down options.
6. Select the RAID EE **Spares** if you select the RAID EE level. Select the **Subgroups** if you select the compound RAID level.
7. Click the **Apply** button to migrate the disk group.

TIP:
There are some operation limitations when a pool is being migrated.

- The capacity after migration must be larger than the current capacity.
- A traditional RAID level can be migrated to RAID EE level, but RAID EE level can be migrated to RAID EE level only.

TIP:
There are some operation limitations when a pool is being migrated. The System would reject these operations:

- Add dedicated spare.
- Remove a dedicated spare.
- Create a new volume.
- Delete a volume.
- Extend a volume.
- Scrub a volume.
- Perform another migration operation.
- Scrub entire pool.
- Take a snapshot.
- Delete a snapshot.
- Expose a snapshot.
- Rollback to a snapshot.

TIP:
Pool migration cannot be executed during rebuilding or volume extension.

Replace Disk Group *(Only visible when the pool type is thin provisioning)*
Here is an example to migrate the disk group to RAID 6.

1. Click the **Replace Disk Group** option to pop up a window.

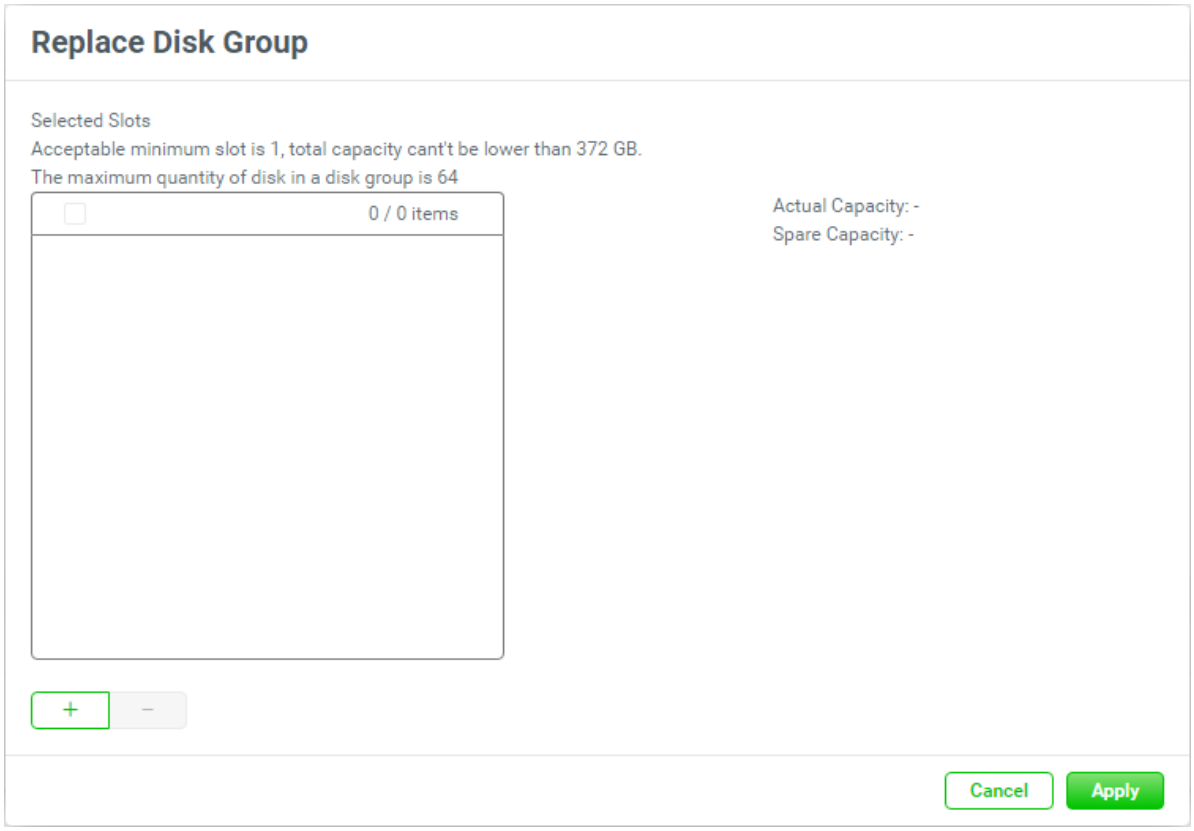


Figure 5-27 Replace Disk Group

2. Click the + icon to select disks to add into the disk group

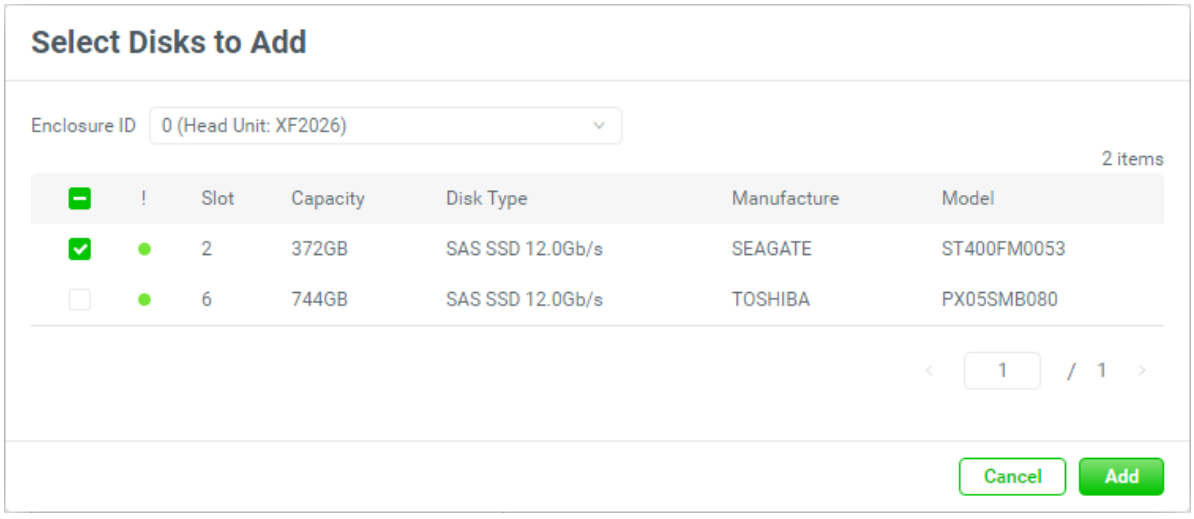


Figure 5-28 Select Disks to Add

3. Check disk slots which you want to add. The maximum quantity of disk in a disk group is 64. Select an **Enclosure ID** from the drop-down list to select disks from expansion enclosures. Then click the **Add** button to continue.

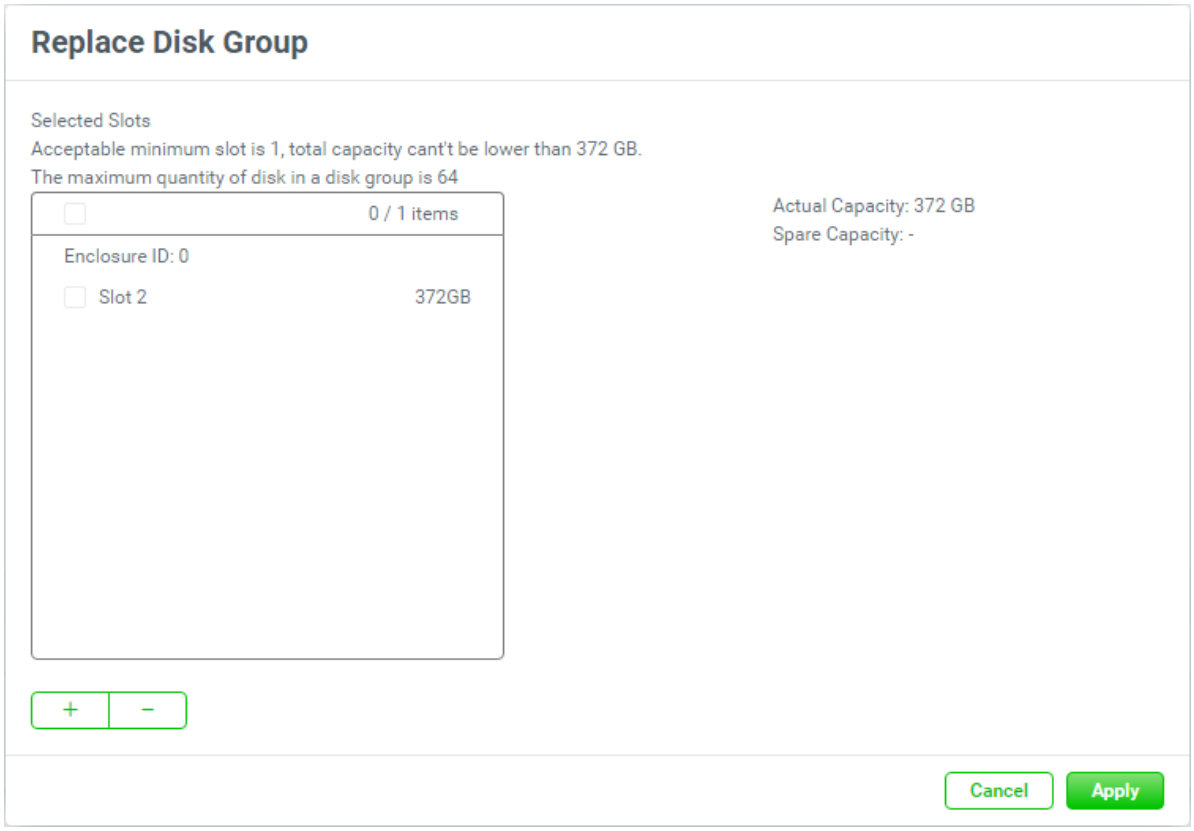


Figure 5-29 Replace Disk Group

4. The selected disk slots are listed in the box and can be removed. Check disk slots which you want to remove and then click the − button.
5. Click the **Apply** button to replace the disk group.

5.1.4. List and Configure Volumes

Click the **Volumes** pane to list all volumes in the pool.

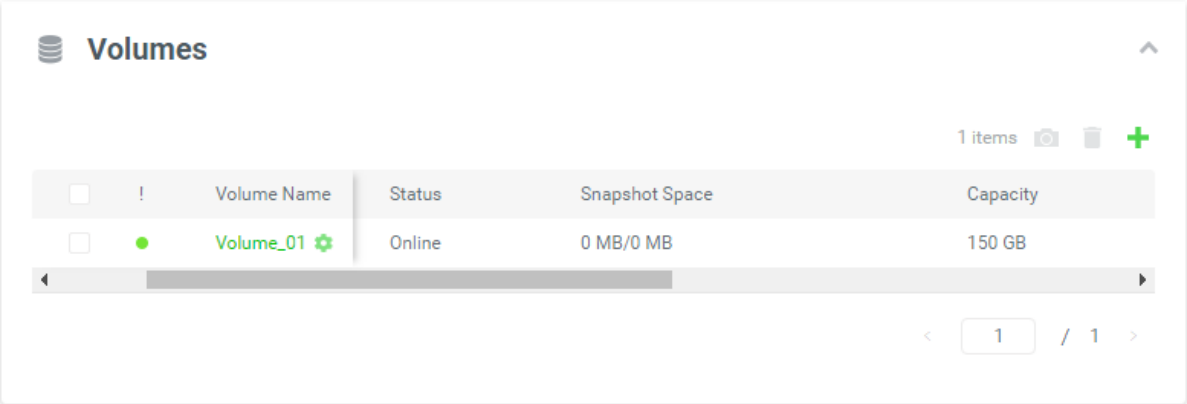


Figure 5-30 List Volumes

This table shows the volume descriptions.

Table 5-4 Volume Column Descriptions

Column Name	Description
!	The status of the disk group: • Green Color / Normal: The volume is good. • Orange Color / Abnormal: The pool is unhealthy and incomplete. The cause may be a disk loss or failure. • Red Light / Warning: The disk group has failed.
Volume Name	The volume name.
Status	The status of the volume: • Online: The volume is online. • Offline: The volume is offline. • Erasing: The volume is being erased. • Initiating: The volume is being initialized. • Rebuilding: The volume is being rebuilt. • Migrating: The volume is being migrated. • Rollback: The volume is being rolled back. • Parity Checking: The volume is being parity check. • Relocating: The volume is being relocated. • EE Rebuilding: The volume is being RAID EE rebuilt.
Snapshot space	Used snapshot space / Total snapshot space. The first capacity is current used snapshot space, and the second capacity is reserved total snapshot space.
Capacity	Total capacity of the volume.
Usage *(This*	Total usage of the volume.

option is only visible when the pool type is thin provisioning)	
Available *(This option is only visible when the pool type is thin provisioning)*	Total available space of the volume.
LUN	Display LUN (Logical Unit Number) or “-“ as none.
Volume Type	The type of the volume: • RAID Volume. • Backup Volume.
Clone	The target name of the clone volume or “-“ as none..
Permission	The access right of the volume: • WT: Write Through. • WB: Write Back. • RO: Read Only.

The options are available in this pane.

Create Volumes

Here is an example to create multiple volumes.

1. Click the ✚ icon in the **Volumes** pane to pop up a window.

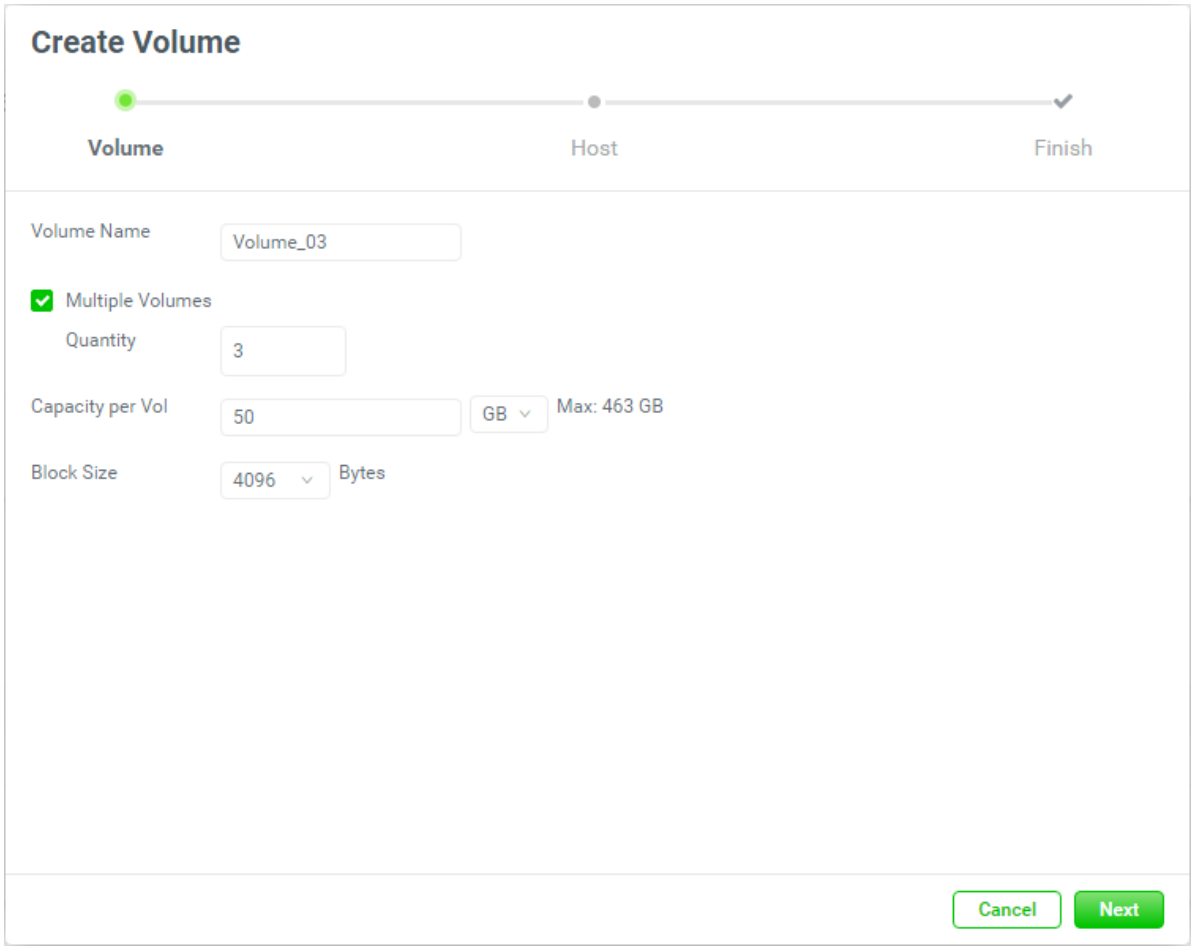


Figure 5-31 Create Volumes Step 1

2. The recommended **Volume Name**, **Capacity per Vol**, and **Block Size** are provided. Enter a new **Volume Name** if necessary. The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. Check the **Multiple Volumes** checkbox. Then enter a number for **Quantity**. The maximum quantity is 64. At this time, change it to 3.
4. The recommended **Capacity per Vol** is the maximum capacity which can be created. Change it if necessary. At this time, change it to 50GB.
5. Change the **Block Size** with the drop down options. The options are 512 Bytes to 4,096 Bytes.
6. Click the **Next** button to continue.

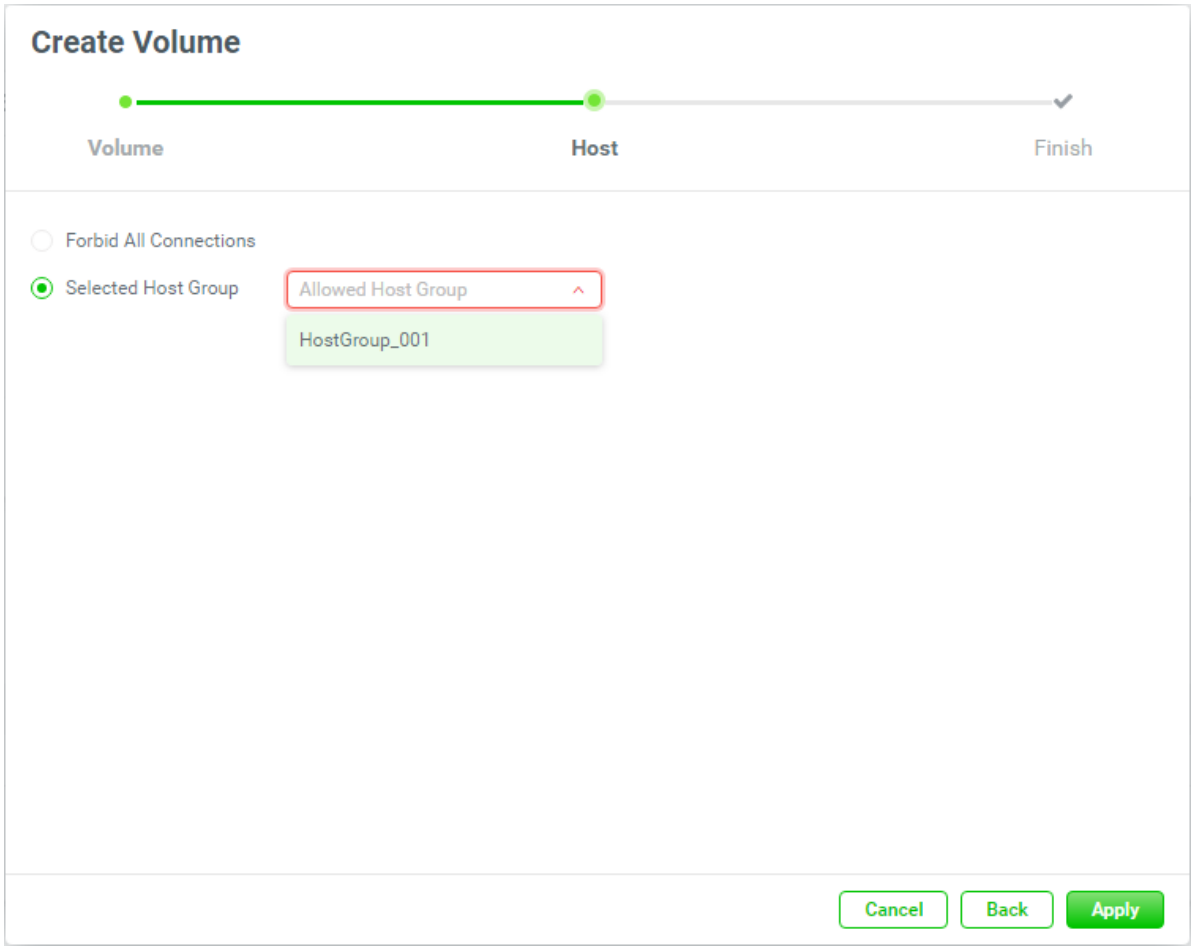


Figure 5-32 Create Volumes Step 2

7. Check the **Selected Host Group** checkbox and select a host group which is created already with the drop down options. Or keep it default as **Forbid All Connections** and change it later.
8. Click the **Apply** button to continue.

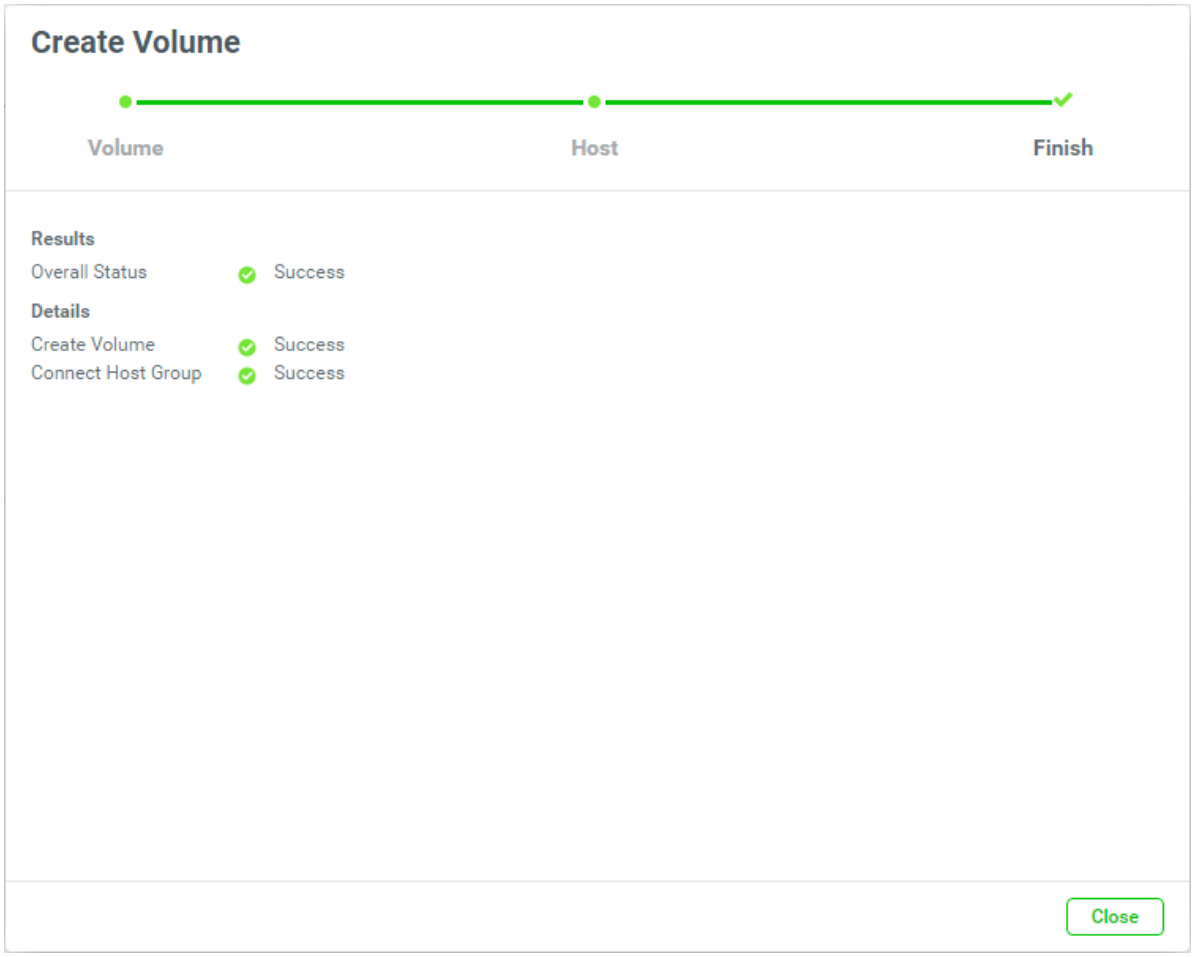


Figure 5-33 Create Volumes Step 3

9. There is a result page. Click the **Close** button to finish.

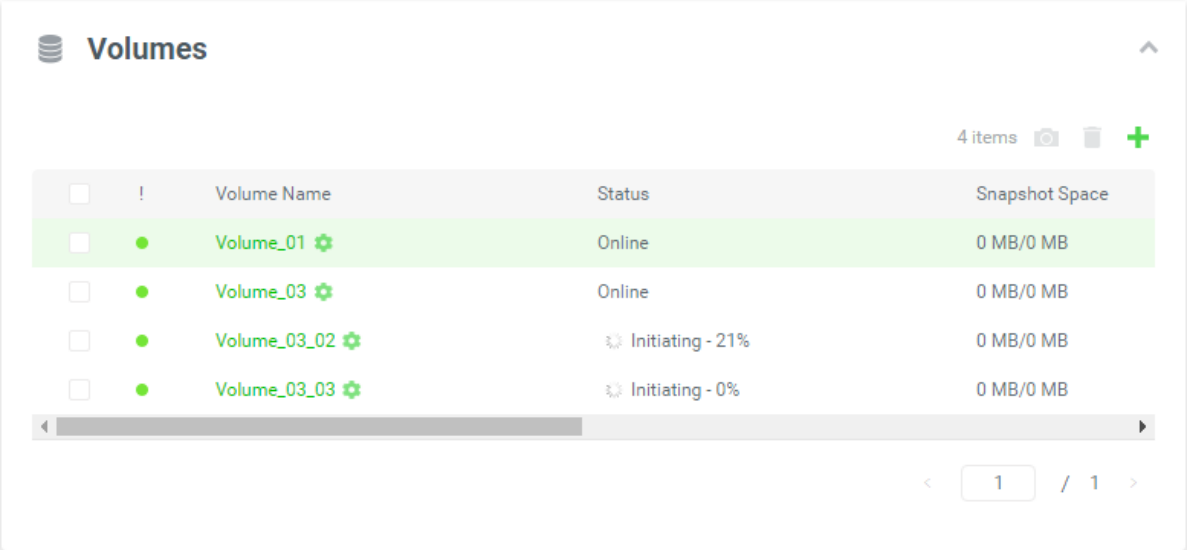


Figure 5-34 List Volumes

10. Multiple volumes have been created. If necessary, click the + icon in the **Volumes** pane to create others.

Delete Volumes

1. Check the volume checkboxes which you want to delete.

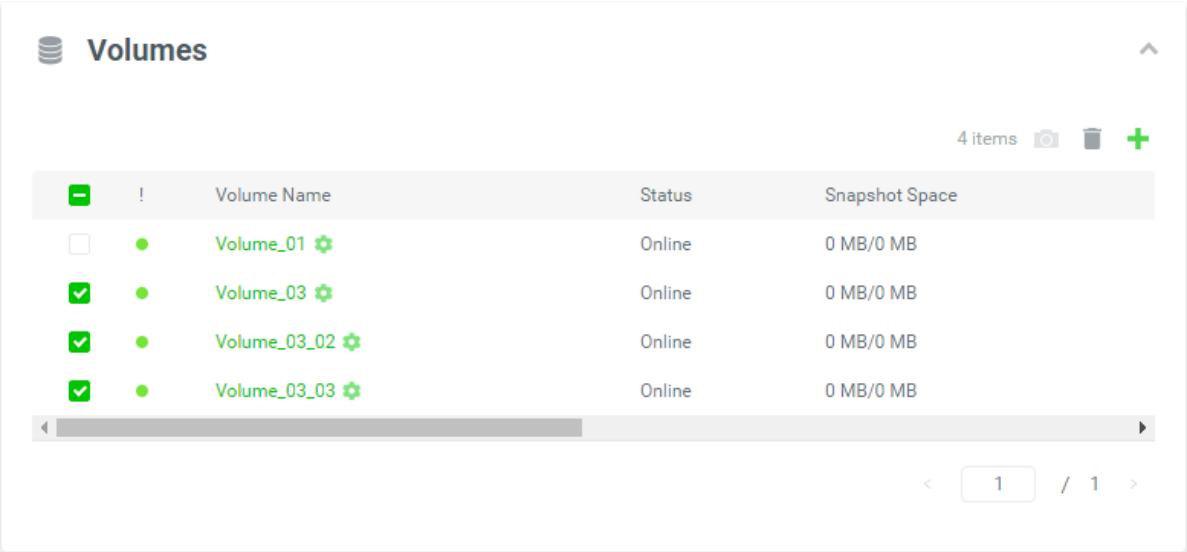


Figure 5-35 Delete Volumes

2. Click the icon to delete.

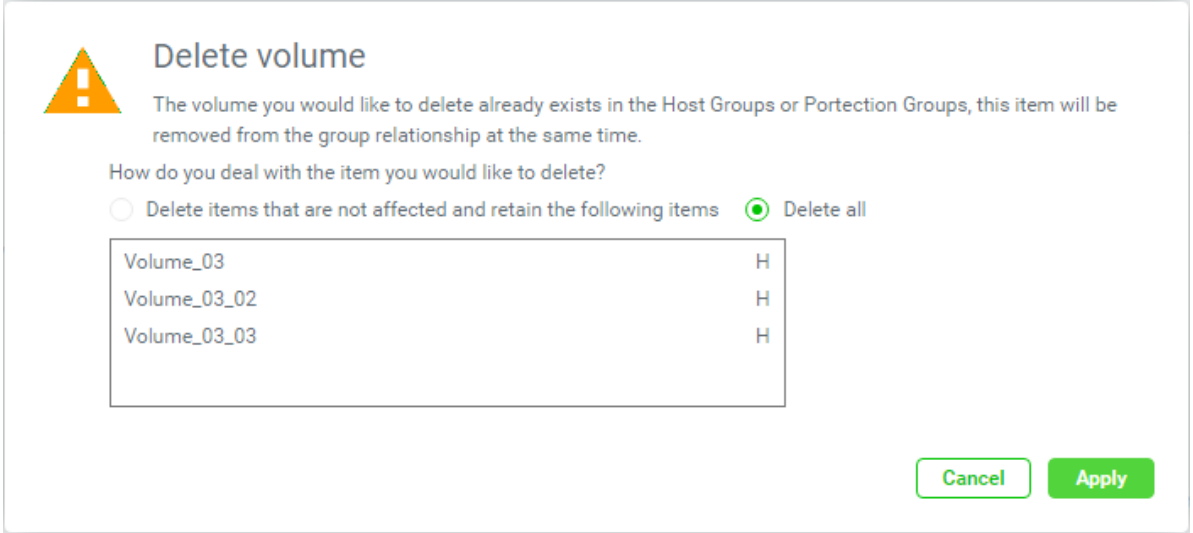


Figure 5-36 Delete Volumes

3. If the volumes are already exists in the **Host Groups** or **Protection Groups**, it will display the above dialog asking you how to handle the items you would like to delete.

INFORMATION:
There are four relationships shown after the volume name.

- none: The volume does not exist in the **Host Groups** nor **Protection Groups**.
- H: The volume exists in the **Host Groups**.
- P: The volume exists in the **Protection Groups**.
- P/H: The volume exists both in the **Host Groups** and **Protection Groups**.

Select the **Delete all** option will delete all volumes and remove them from the group relationships at the same time. Select the **Delete items that are not affected and retain the following items** option will delete the volumes which are “none” relationship only.

4. Click the **Apply** button to delete.

Take a Snapshot

1. Check the volume checkboxes which you want to take a snapshot.

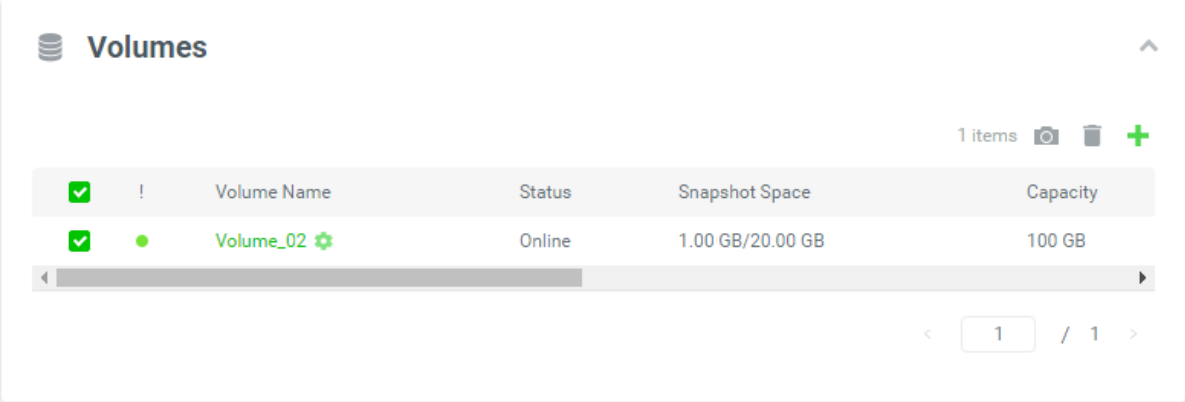


Figure 5-37 Take a Snapshot

2. Click the icon; it will pop up a window.

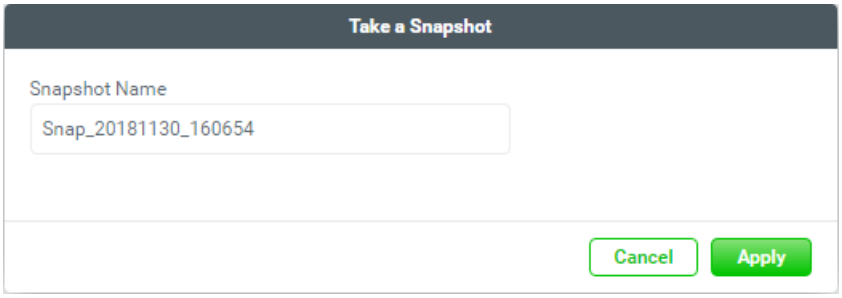


Figure 5-38 Take a Snapshot

3. The recommended **Snapshot Name** is provided. Enter a new **Snapshot Name** if necessary. The maximum length of the snapshot name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
4. Click the **Apply** button to take.

TIP:
If it failed to take a snapshot, you have to **Enable Snapshot Space** first in the **Snapshot Center**.

Click the icon beside the volume name to list the drop down options. These options are available in the volume.

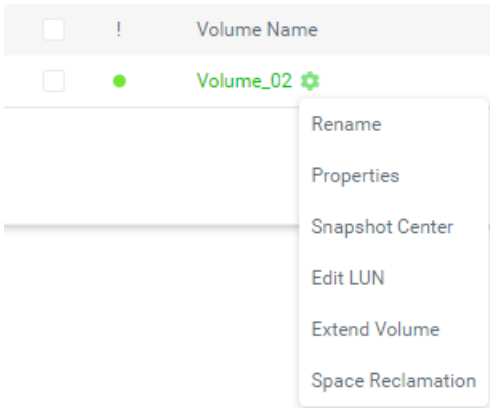


Figure 5-39 Volume Options

Rename

1. Click the **Rename** option to rename the volume.

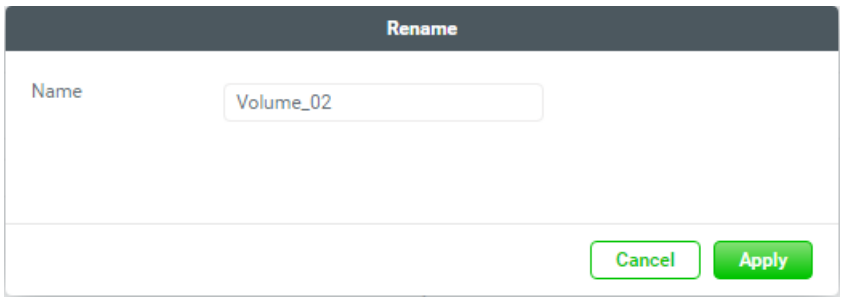


Figure 5-40 Rename Volume

2. Enter a new **Volume Name**. The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. Click the **Apply** button to rename.

Properties

1. Click the **Properties** option to change the volume properties.

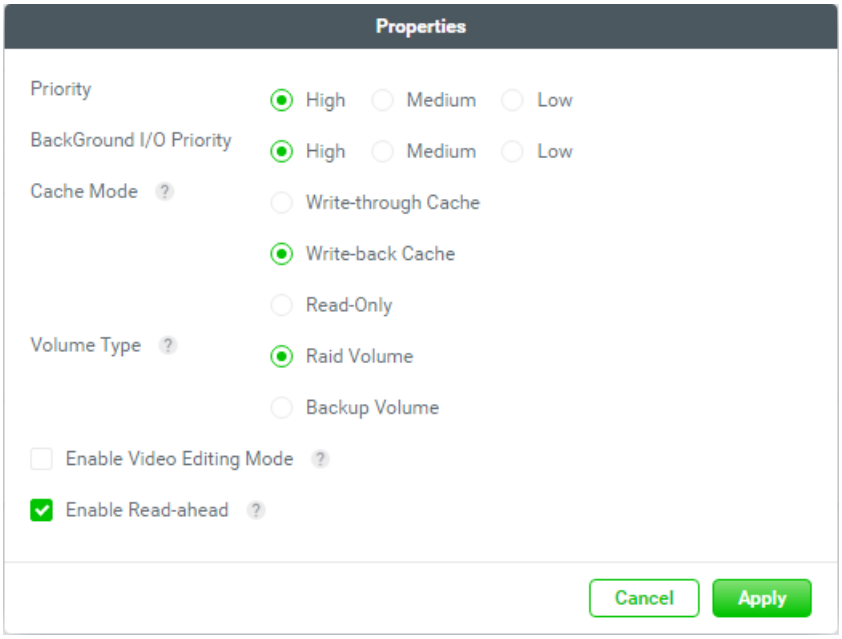


Figure 5-41 Change the Volume Properties

2. Volume advanced settings can be configured optionally.
    - **Priority**: The options are High, Medium, and Low. The priority compares to other volumes. Set it as High if the volume has many I/O.
    - **Background I/O Priority**: The options are High, Medium, and Low. It will influence volume initialization, rebuild, and migration.
    - **Cache Mode**: The options are Write-through Cache, Write-back Cache, and Read-only. Write-back optimizes the system speed but comes with the risk where the data may be inconsistent between cache and disks in one short time interval.
    - **Volume Type**: The options are RAID Volume and Backup Volume. RAID Volume is for general RAID usage and Backup Volume is for the target volume of local clone or remote replication.
    - **Enable Video Editing Mode**: Check to enable video editing mode function. It is optimized for video editing usage. Please enable it when your application is in video editing environment. This option provides a more stable performance figure without high and low peaks but slower in average.
    - **Enable Read-ahead**: Check to enable the read ahead function of volume. The system will discern what data will be needed next based on what was just retrieved from disk and then preload this data into the disk's buffer. This feature will improve performance when the data being retrieved is sequential.
3. After change the volume properties, click the **Apply** button to take effect.

Snapshot Center

About the snapshot center, please refer to the chapter 7.2.3, Snapshot Center section for more details.

Edit LUN

1. Click the **Edit LUN** option to change the LUN (Logical Unit Number).

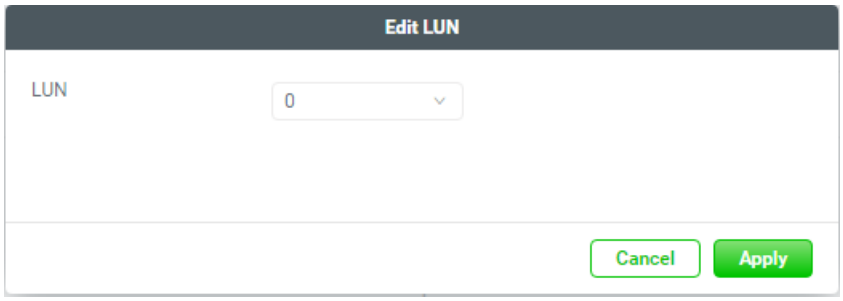


Figure 5-42 Edit LUN

2. Select the LUN with the drop down options. The options are LUN 0 to LUN 254 except the LUNs which are occupied.
3. Click the **Apply** button to take effect.

TIP:
If the LUN cannot be edited, the volume must first be assigned to a host group.

Extend Volume

1. Click the **Extend Volume** option to extend the volume capacity.

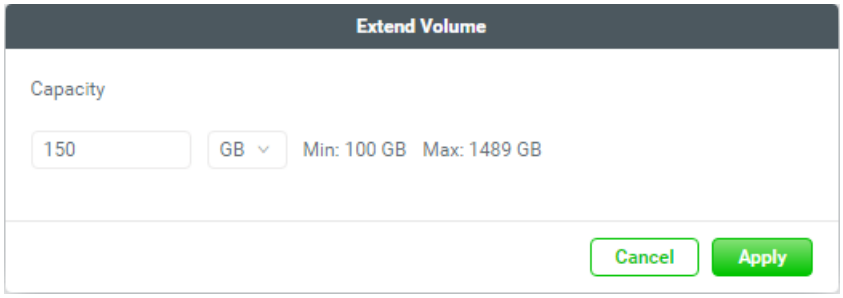


Figure 5-43 Extend Volume

2. Enter a new **Capacity** number which you want to extend. There are minimum and maximum capacity numbers after the **Capacity** field.
3. Click the **Apply** button to extend.

Space Reclamation *(Only visible when the pool type is thin provisioning)*
Click the **Space Reclamation** option to reclaim space from the volume when the volume is in a thin provisioning pool. Click the **Apply** button to confirm and proceed.

5.2. Hot Spares

The XEVO system sets all free disks as a global spare. If one disk drive of the pool fails or has been removed from any singly redundant RAID, the pool status will change to degraded mode. At the moment, the XEVO system will search the spare disk to execute pool/volume/data rebuild into a healthy RAID drive automatically.

5.3. Disk Roaming

Disks can be re-sequenced in the same system or move all member disks in the same pool from system-1 to system-2. This is called disk roaming. The system can execute disk roaming online. Please follow these steps.

1. Select the **Storage** tab, selects a pool. Click the ⚙ icon beside the pool name, and then click the **Deactivate** option.
2. Click the **Apply** button to apply. The Status changes to Offline.
3. Move all member disks of the pool to another system.
4. In the **Storage** tab, select the pool. Click the ⚙ icon beside the pool name, and then click the **Activate** option.
5. Click the **Apply** button to apply. The Status changes to Online.

Disk roaming has some constraints as described in the following.

1. Check the firmware version of two systems first. It is better for both systems to have the same firmware version or the firmware version of the system-2 is newer.
2. All physical disks of the pool should be moved from system-1 to system-2 together. The configuration of both pool and volume will be kept but LUN configuration will be cleared in order to avoid conflict with the current setting of the system-2.

CAUTION:
XCubeFAS series does NOT support disk roaming from XCbueSAN, AegisSAN LX, AegisSAN Q500, and AegisSAN V100.

6. Hosts Tab

The **Hosts** tab manages the host groups. It displays the host group status, configures the host profile and connected volumes. This chapter describes the details of host group management operations and examples.

6.1. Configure Host Groups

Select the **Hosts** tab to manage the host groups. In this tab, you can create, modify, delete, or view the status of all host groups.

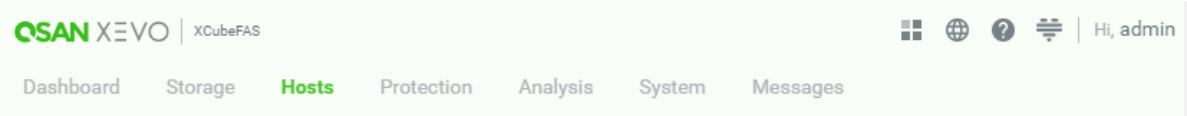


Figure 6-1 Hosts Tab

6.1.1. Create a Host Group

Here is an example of creating a host group and connecting a volume.

1. Click the + icon in the **Host Groups** pane to pop up a wizard.

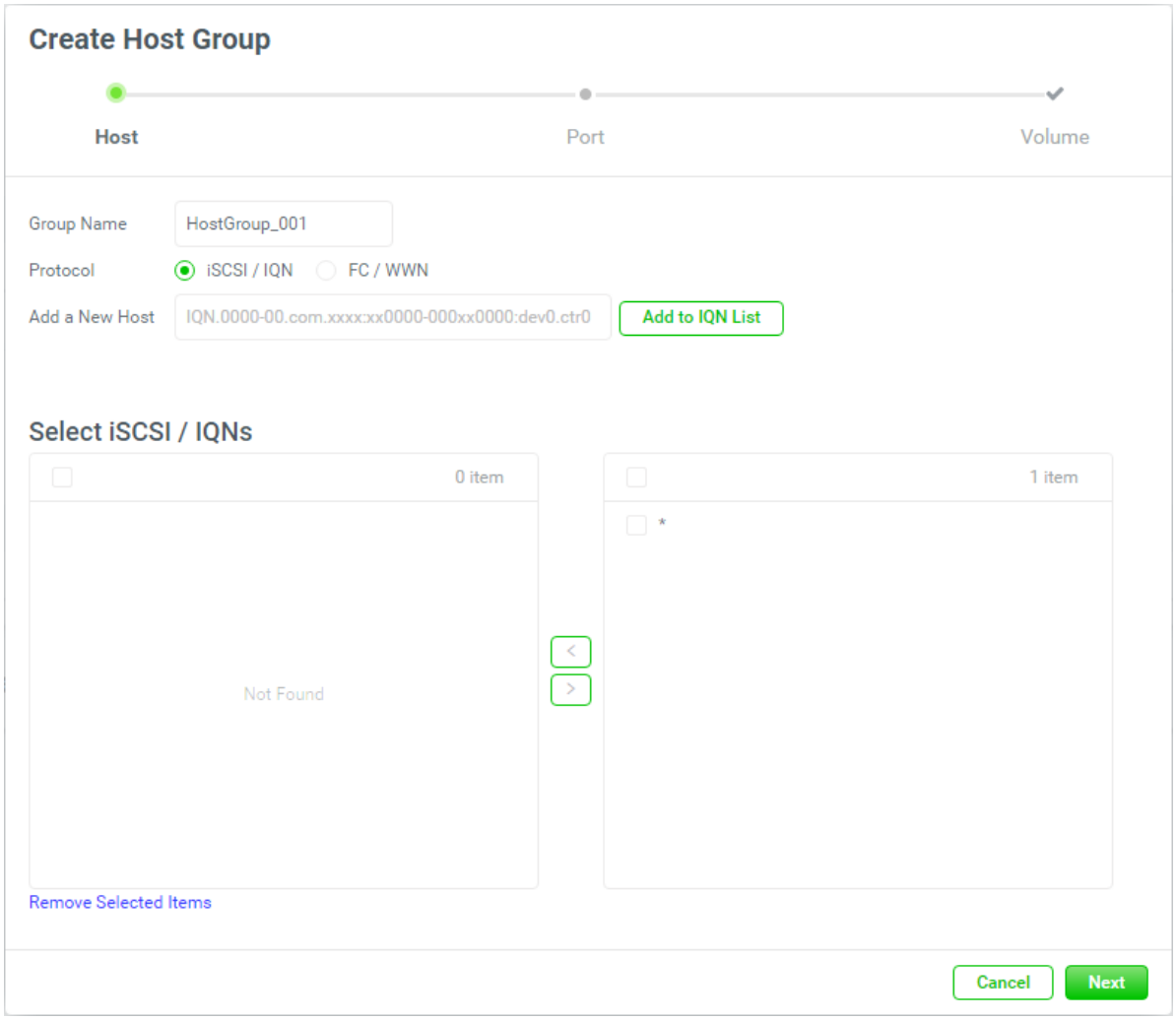


Figure 6-2 Create a Host Group Step 1-1

2. The recommended **Group Name** is provided. Enter a new **Group Name** if necessary. The maximum length of the pool name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. Select the **Protocol** for **iSCSI / IQN** or **FC / WWN**.

INFORMATION:
The **FC / WWN** will appear only when the system has a fibre channel host card installed.

4. If selecting the **iSCSI/ IQN** option, you can add an IQN for access control. Enter a host IQN in **Add a New Host**, and then click the **Add to IQN List** button. It will be added to the **Select iSCSI / IQNs** box.
5. If necessary, add another host IQN.

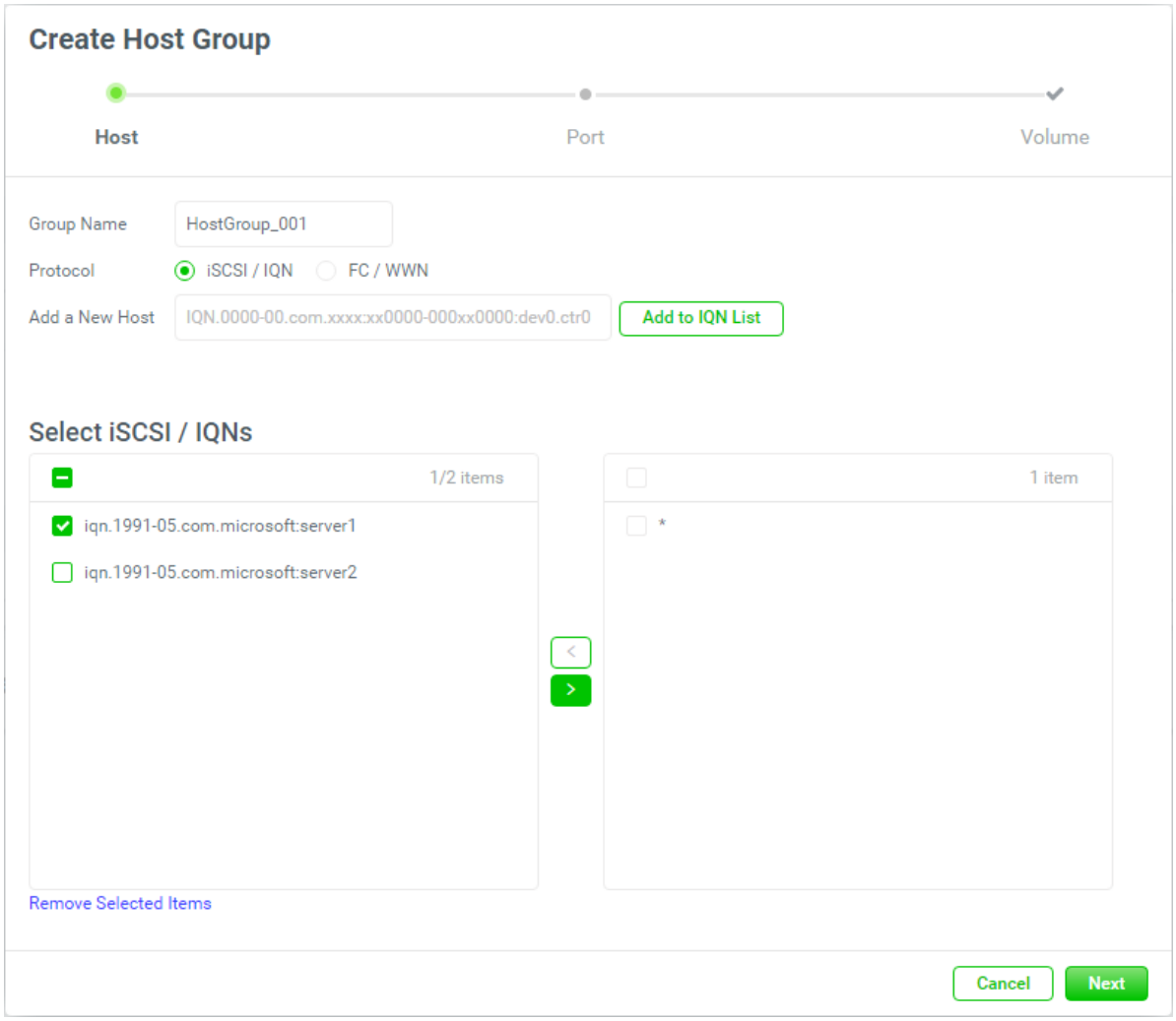


Figure 6-3 Create a Host Group Step 1-2

6. The **Select iSCSI / IQNs** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective.
7. Select the IQN and click the > button to move it from the left side to the right side.

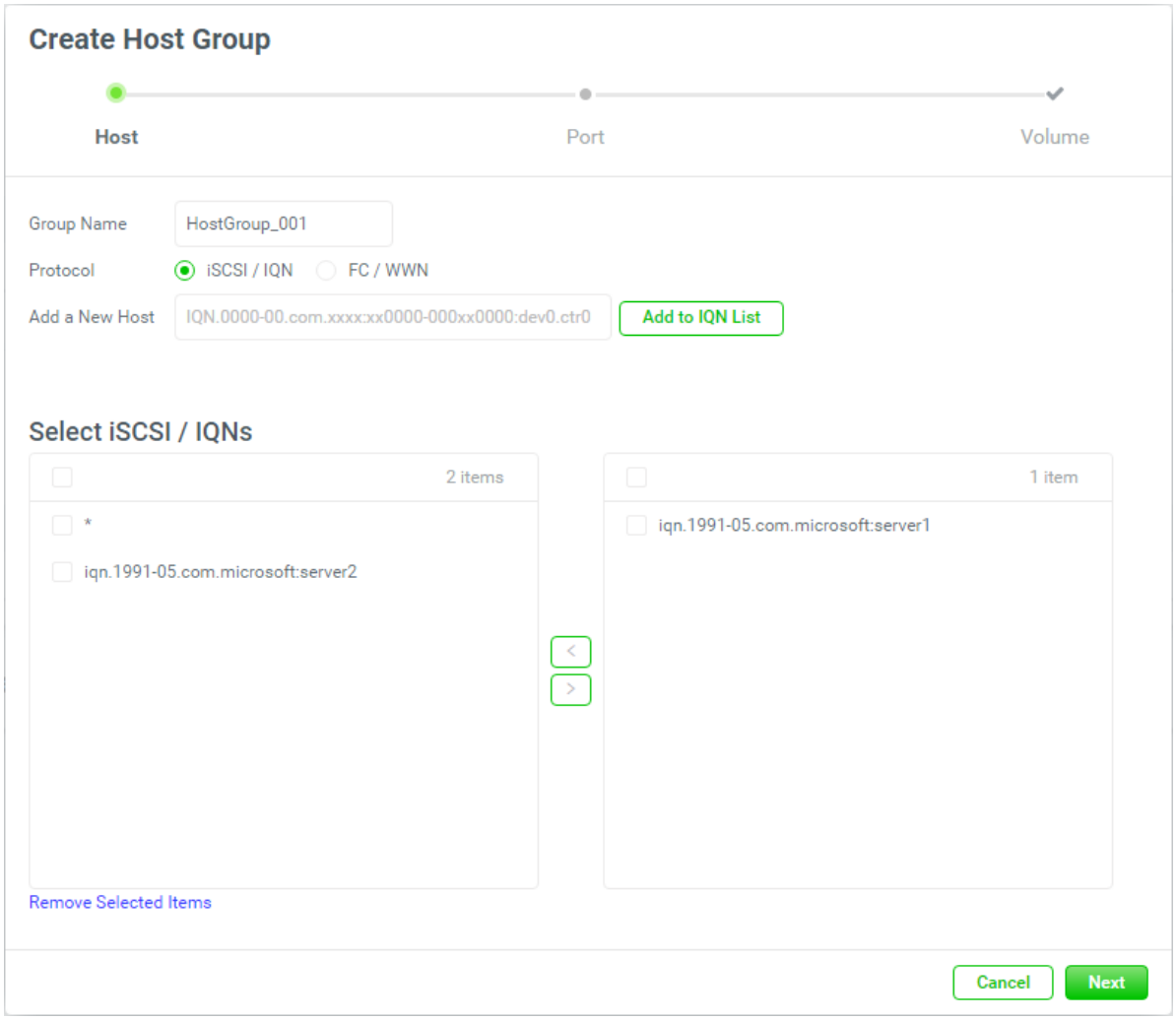


Figure 6-4 Create a Host Group 1-3

8. At the same time, the wide card “*” will be move to the left side automatically.

INFORMATION:
The wide card “*” means the host group can be accessed by all hosts without access control. A conflict occurs when a dedicated host or all hosts can access it.

9. If the created IQNs are wrong or unuseful, select the IQNs and click the **Remove Selected Items** to remove from the list.

10. If selecting the **FC / WWN** option, the automatically detected host FC / WWNs are listed in the **Select FC / WWN** box. Select the WWNs and click the > button or the < button to make them effective or not.

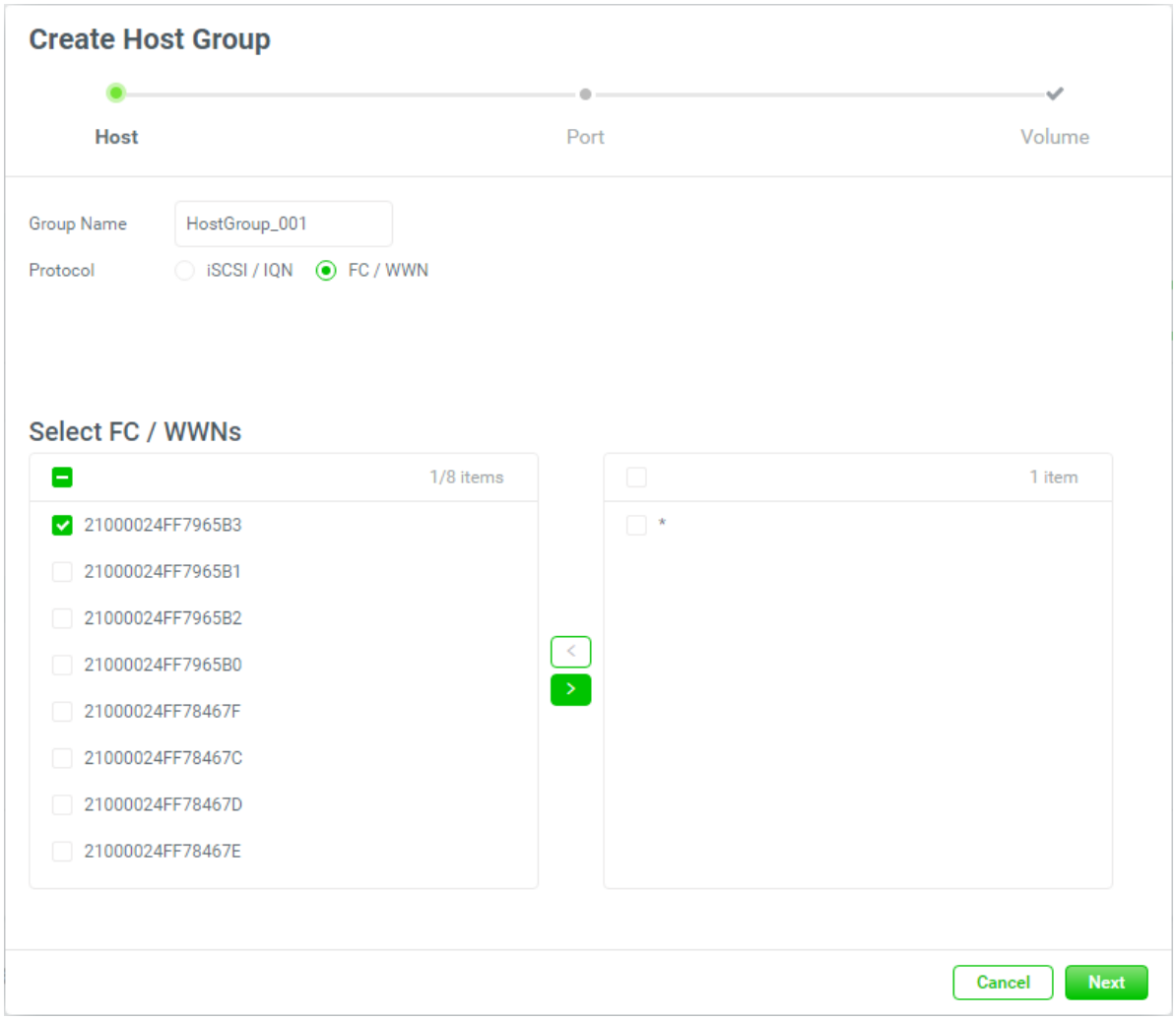


Figure 6-5 Create a Host Group 1-4

11. Click the **Next** button to continue.

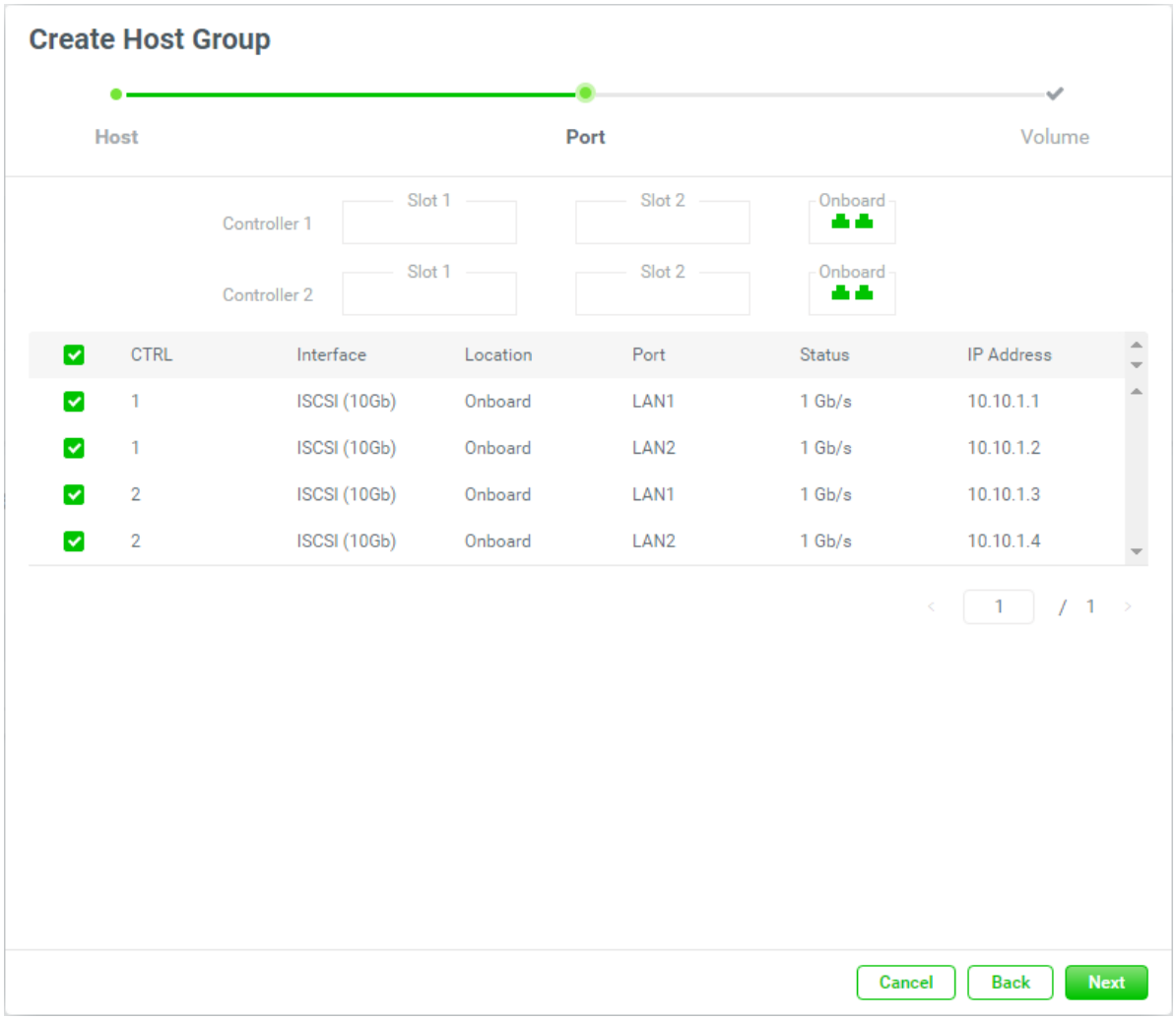


Figure 6-6 Create a Host Group Step 2

12. The all **Ports** (Network Portals) are enabled. If necessary, check the interfaces checkbox which you want to enable or disable.
13. Click the **Next** button to continue.

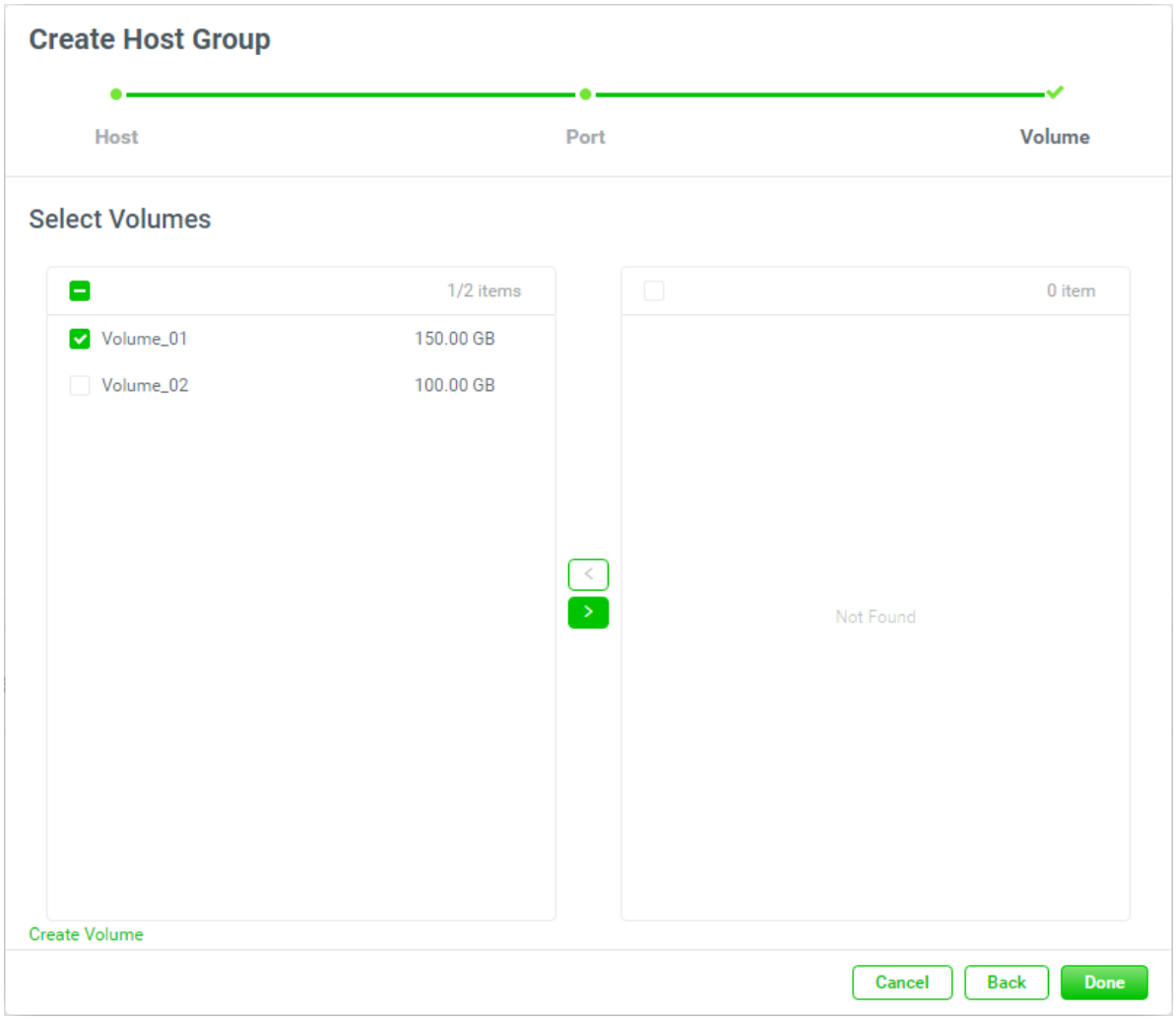


Figure 6-7 Create a Host Group Step 3-1

14. The **Select Volumes** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective.
15. Select volumes and click the > button to move it from the left side to the right side.

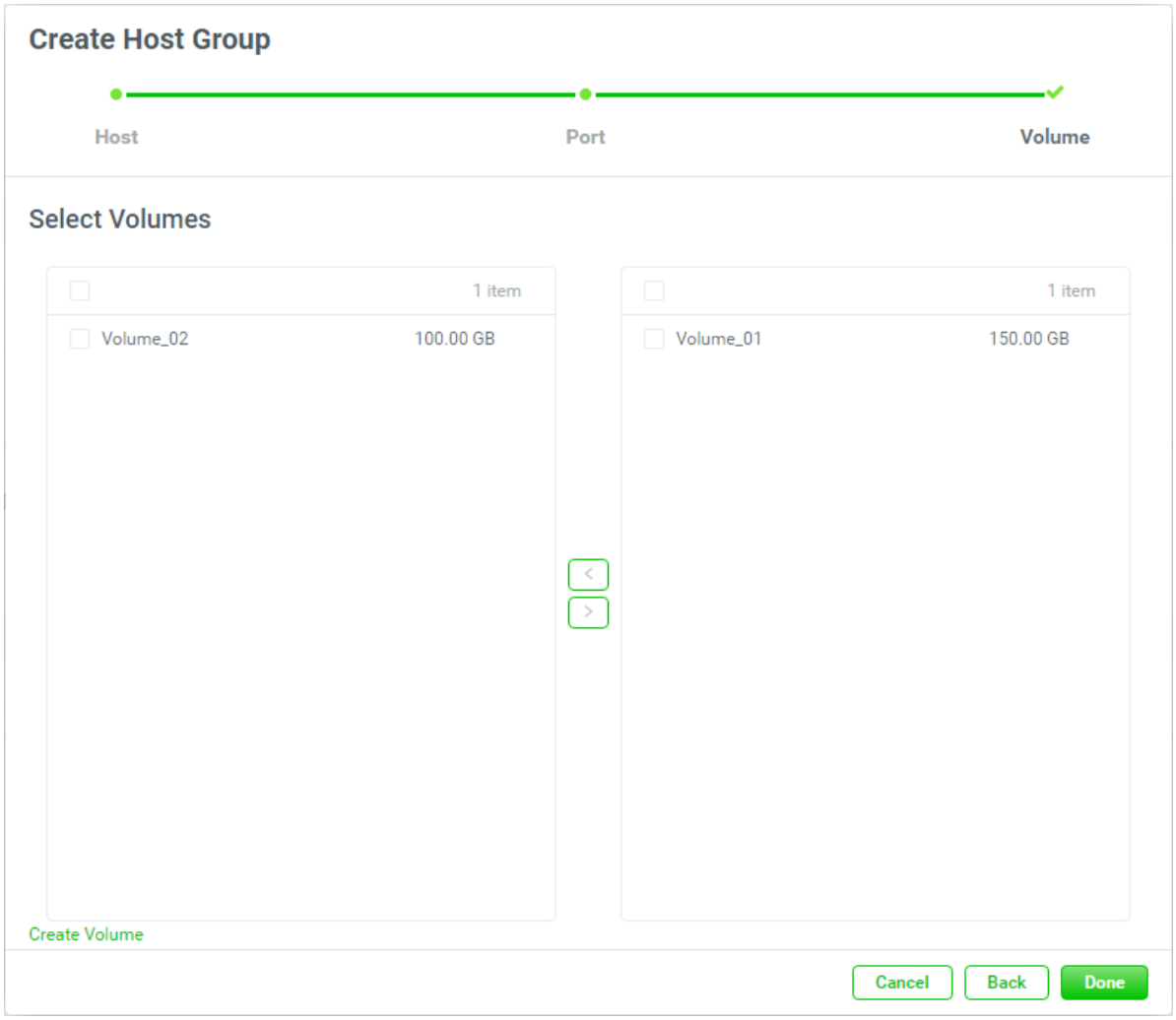


Figure 6-8 Create a Host Group Step 3-2

16. Click the **Done** button to finish.

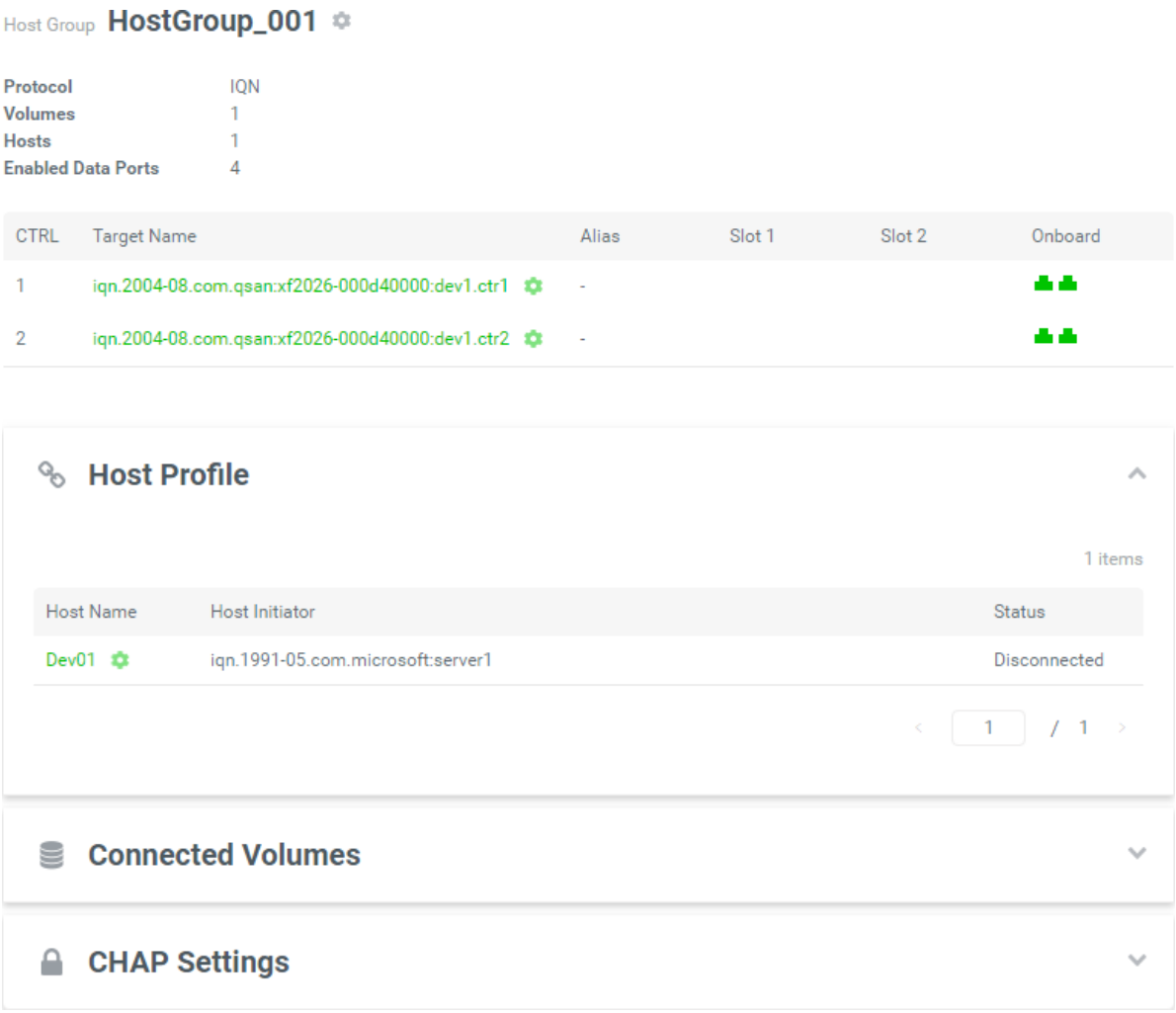


Figure 6-9 A Host Group is Created

17. A host group has been created. If necessary, click the ✚ icon in the **Host Groups** pane to create others.

6.1.2. List and Configure Host Groups

All host groups are listed in the **Host Groups** pane. You can click one of them to display the details.

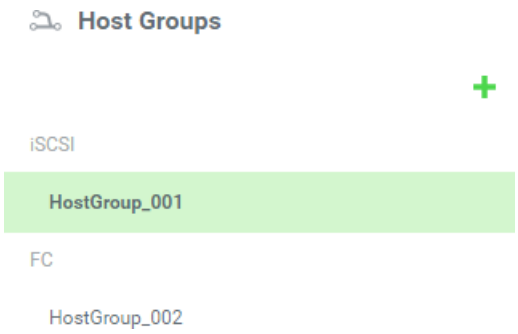


Figure 6-10 List All Host Groups

An iSCSI host group and a FC host group are shown here.

Figure 6-11 iSCSI Host Group Details

Figure 6-12 FC Host Group Details

This table shows the host group descriptions.

Table 6-1 Host Group Column Descriptions

Column Name	Description
Protocol	The protocol of the host group: • IQN: iSCSI protocol. • WWN: Fibre channel protocol.
Volumes	The quantity of the connected volumes.
Hosts	The quantity of the hosts.
Enabled Data Ports	The quantity of the enabled data ports.
CTRL	Controller 1 or 2.
Target Name	Target name of iSCSI or FC.
Alias	Alias name.
Slot 1	Port icons in slot 1.
Slot 2	Port icons in slot 2.
Onboard	Port icons onboard.

Click the ⚙ icon beside the host group name to list the drop down options. These options are available in the host group.

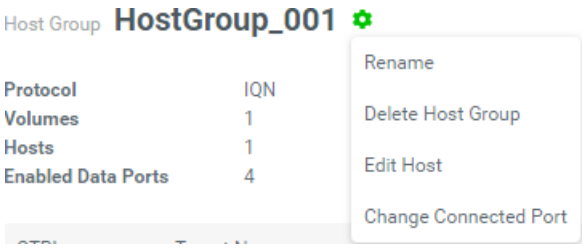


Figure 6-13 Host Group Options

Rename

1. Click the **Rename** option to rename the host group.

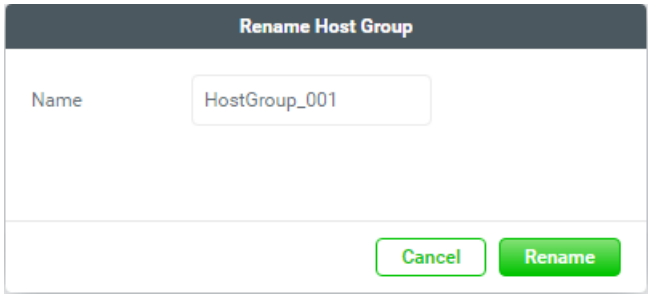


Figure 6-14 Rename Host Group

2. Enter a new **Group Name**. The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. Click the **Rename** button to rename.

Delete

Click the **Delete Host Group** option to delete the host group. Click the **Delete** button to confirm and delete.

Edit Host

1. Click the **Edit Host** option to edit the host group.

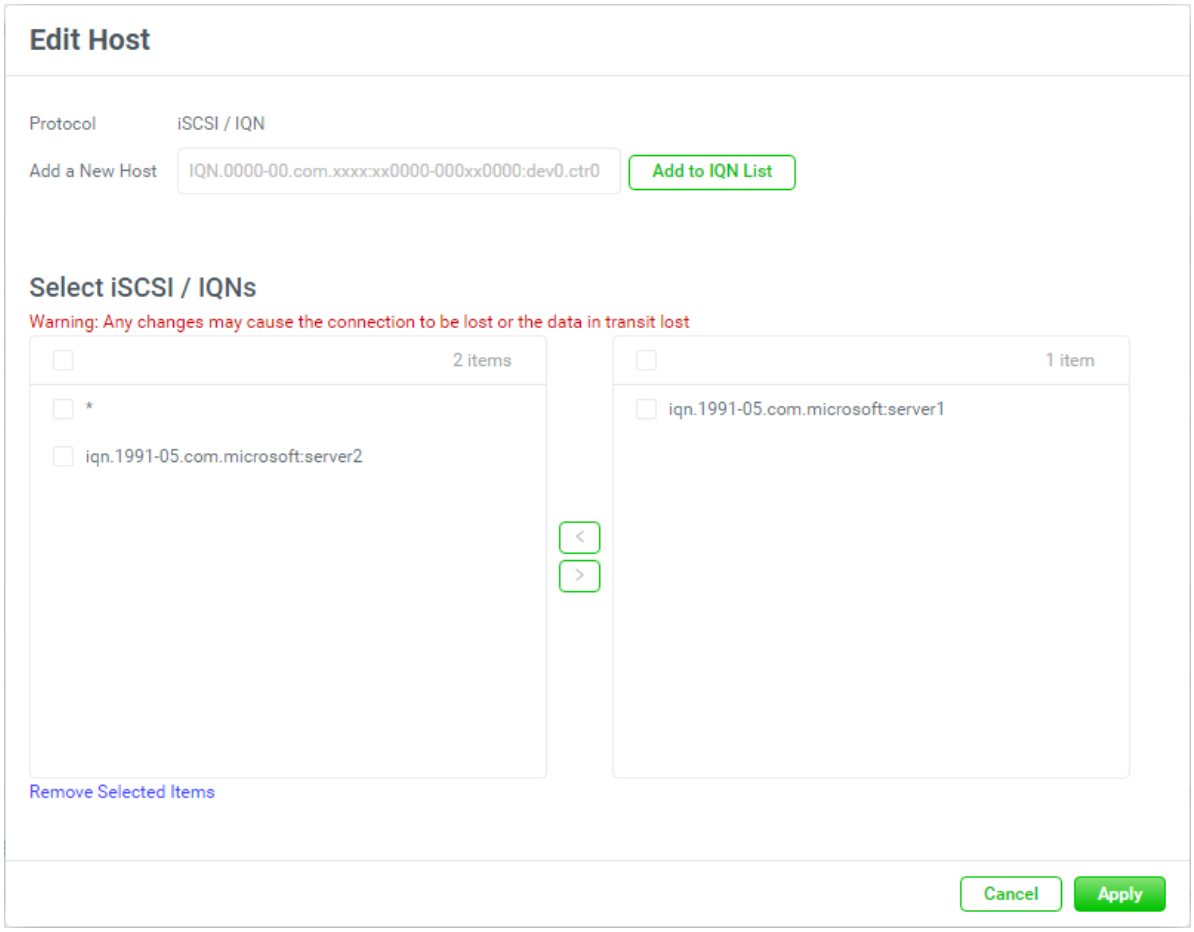


Figure 6-15 Edit Host for iSCSI

2. If editing the protocol of iSCSI / IQN, select the IQNs and click the > button or the < button to make them effective or not.
3. Click the **Apply** button to edit.

CAUTION:
Any changes may cause the connection to be lost or the data in transit lost.

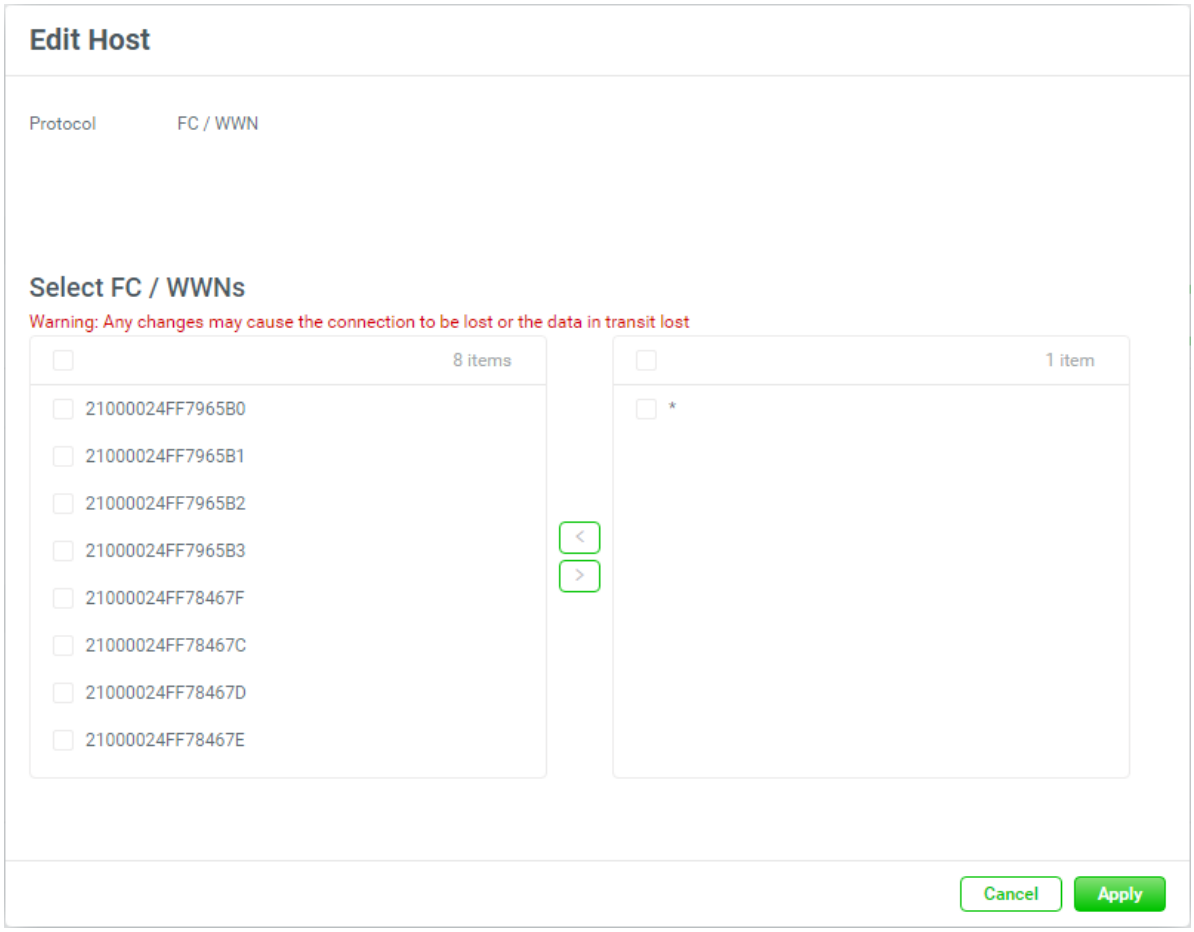


Figure 6-16 Edit Host for FC

4. If editing the protocol of FC / WWN, select the WWNs and click the > button or the < button to make them effective or not.
5. Click the **Apply** button to edit.

Change Connected Port

1. Click the **Change Connected Port** option to change the connected ports in the host group.

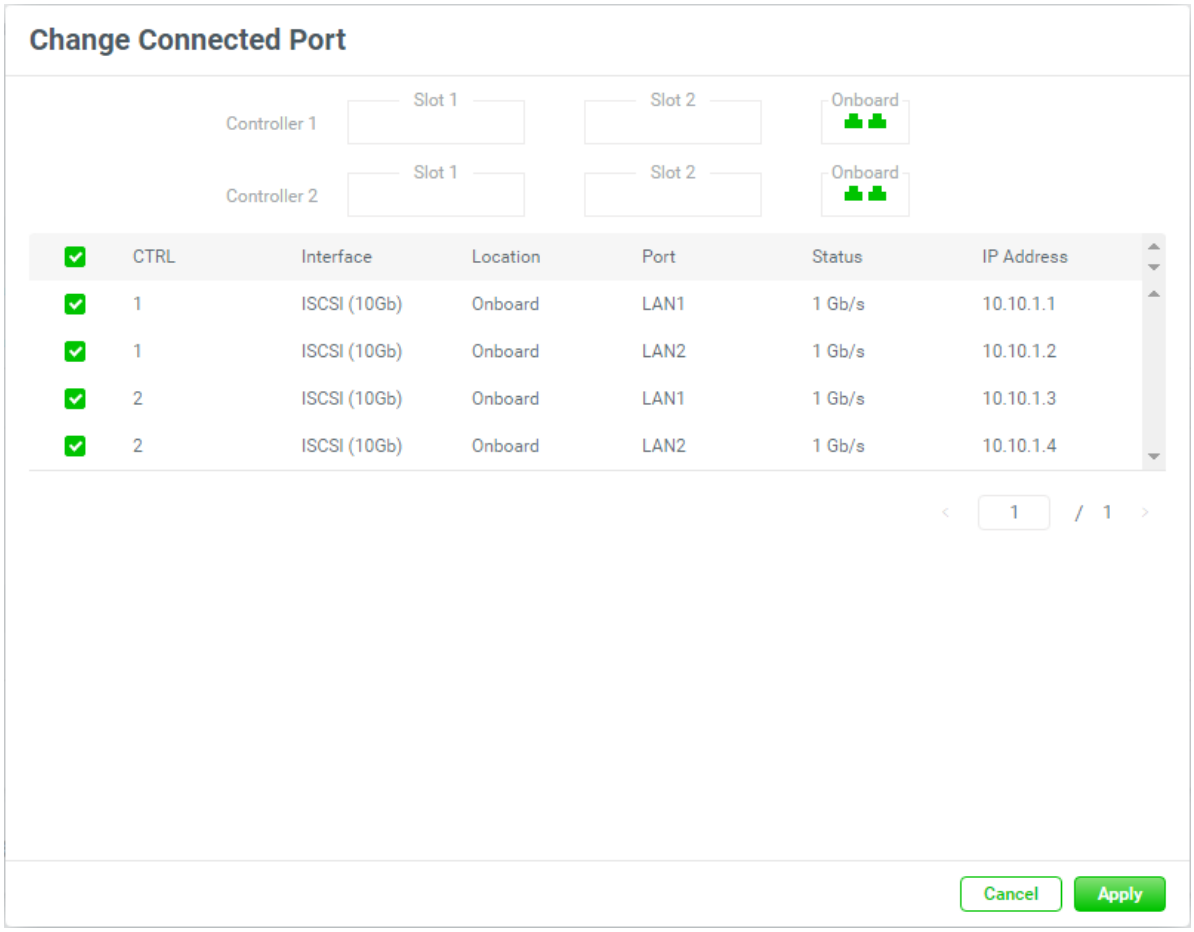


Figure 6-17 Change Connected Port

2. Check the interfaces checkbox which you want to enable or disable.
3. Click the **Apply** button to change.

Click the ⚙ icon beside the target name to list the drop down options. These options are available in the disk group.

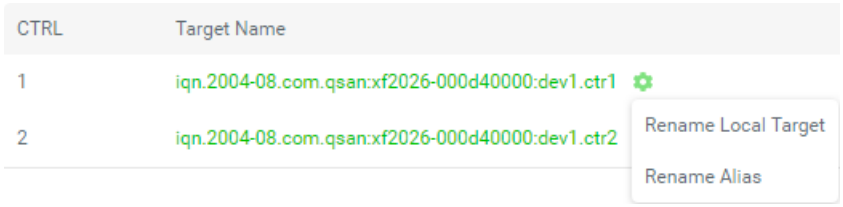


Figure 6-18 Host Target Options

Rename Local Target

1. Click the **Rename Local Target** option to rename the local target name.

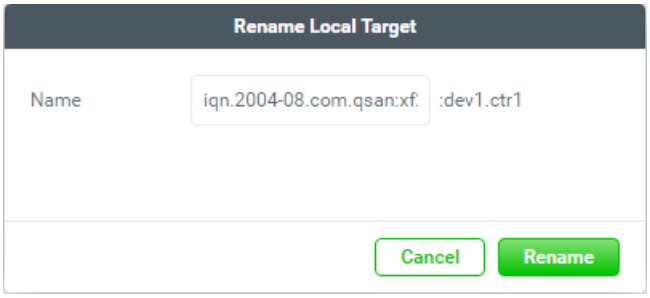


Figure 6-19 Rename Local Target Name

2. Enter a new **Local Target Name**. The maximum length of the volume name is 223 characters. Valid characters are [a~z | 0~9 | -.:].
3. Click the **Rename** button to rename.

Rename Alias

1. Click the **Rename Alias** option to add or change the alias.

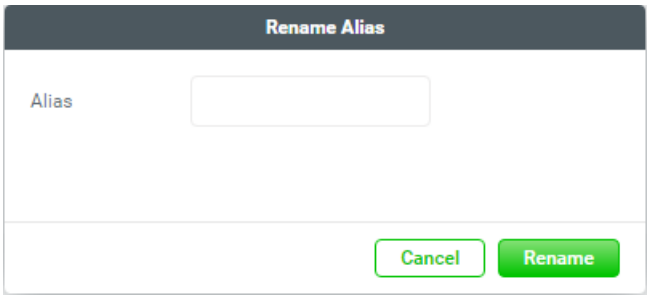


Figure 6-20 Rename Alias

2. Enter a new **Alias**. If you want to remove an alias, clear out the current name. The maximum length of the volume name is 223 characters. Valid characters are [a~z | 0~9 | -.:].
3. Click the **Rename** button to rename.

6.1.3. List and Configure Host Profile

Click the **Host Profile** pane to list all host profiles in the host group.

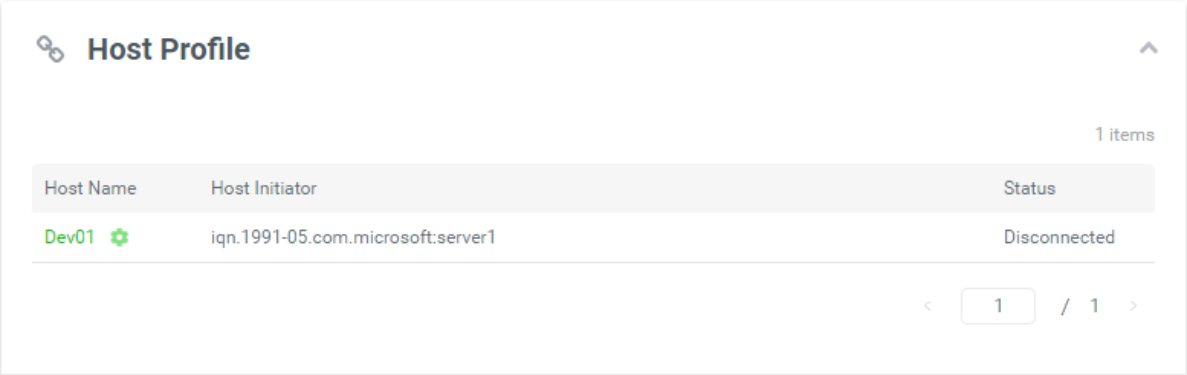


Figure 6-21 List Host Profile

Click the ⚙ icon beside the host name to list the drop down options. These options are available in the host profile.

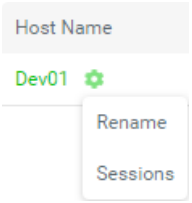


Figure 6-22 Host Profile Options

Rename

1. Click the **Rename** option to rename the host name.

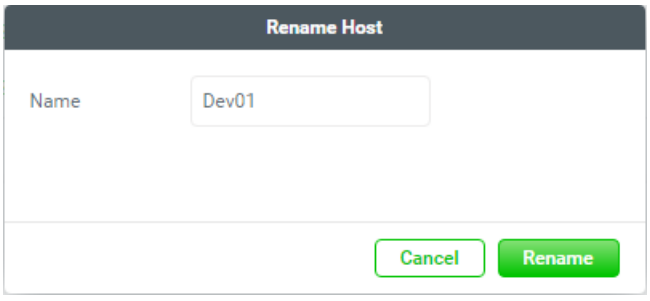


Figure 6-23 Rename Host Name

2. Enter a new **Host Name**. The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. Click the **Rename** button to rename.

Sessions

1. Click the **Sessions** option to display the host sessions in the host group.

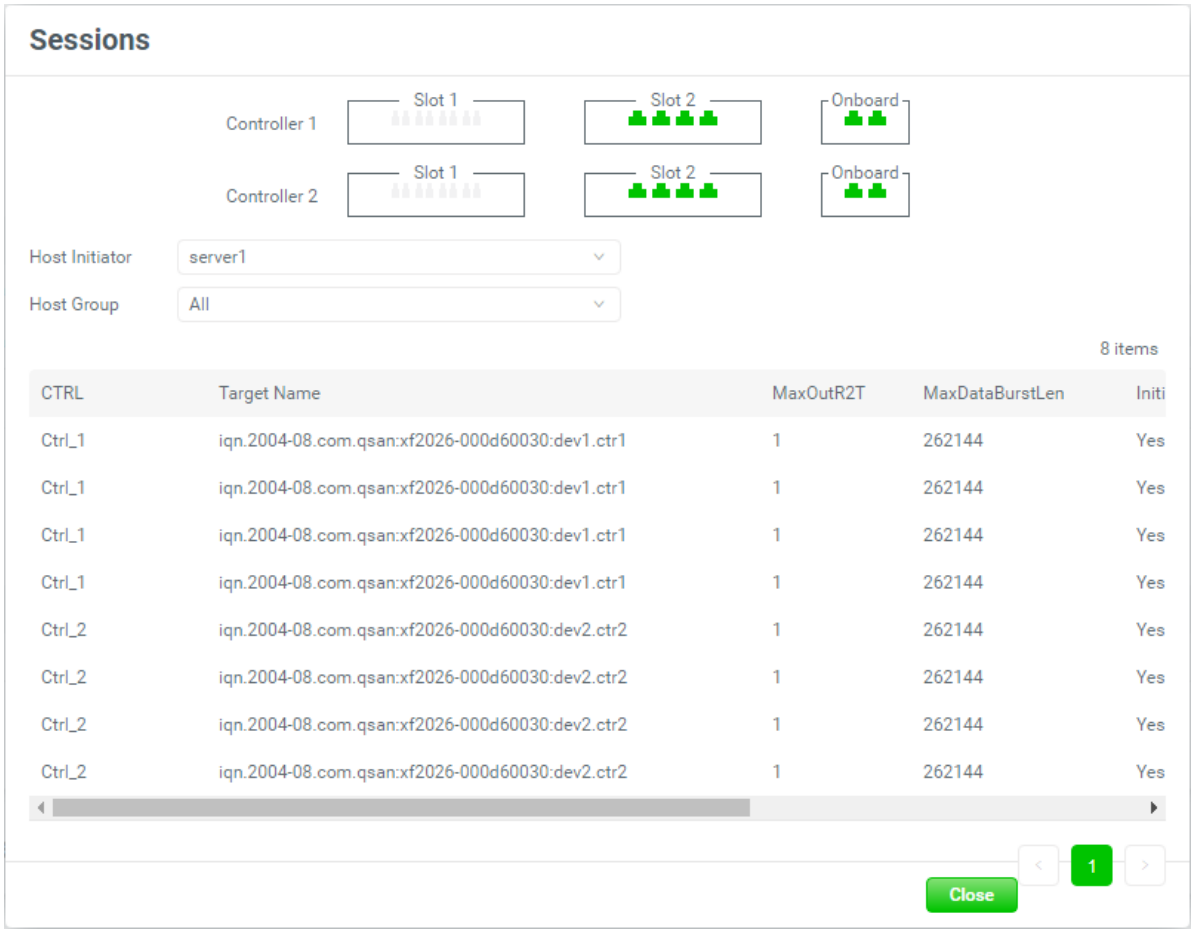


Figure 6-24 Display Sessions

This table shows the column descriptions.

Table 6-2 Active Sessions Column Descriptions

Column Name	Description
CTRL	Controller 1 or 2.
TSIH	TSIH (Target Session Identifying Handle) is used for this active session.
Target Name	It displays the controller name.
MaxOutR2T	MaxDataOutR2T (Maximum Data Outstanding Ready to Transfer) determines the maximum number of outstanding ready to transfer

	per task. The default value is 1.
MaxDataBurstLen	MaxDataBurstLen (Maximum Data Burst Length) determines the maximum SCSI data payload. The default value is 256kb.
InitialR2T	InitialR2T (Initial Ready to Transfer) is used to turn off either the use of a unidirectional R2T command or the output part of a bidirectional command. The default value is Yes.
Immed. data	Immed. data (Immediate Data) sets the support for immediate data between the initiator and the target. Both must be set to the same setting. The default value is Yes.
DataSeginOrder	DataSeginOrder (Data Sequence in Order) determines if the PDU (Protocol Data Units) are transferred in continuously non-decreasing sequence offsets. The default value is Yes.
DataPDU InOrder	DataPDU InOrder (Data PDU in Order) determines if the data PDUs within sequences are to be in order and overlays forbidden. The default value is Yes.

2. Click the **Close** button to close the window.

6.1.4. List and Configure Connected Volumes

Click the **Connected Volumes** pane to list all connected volumes in the host gorup.

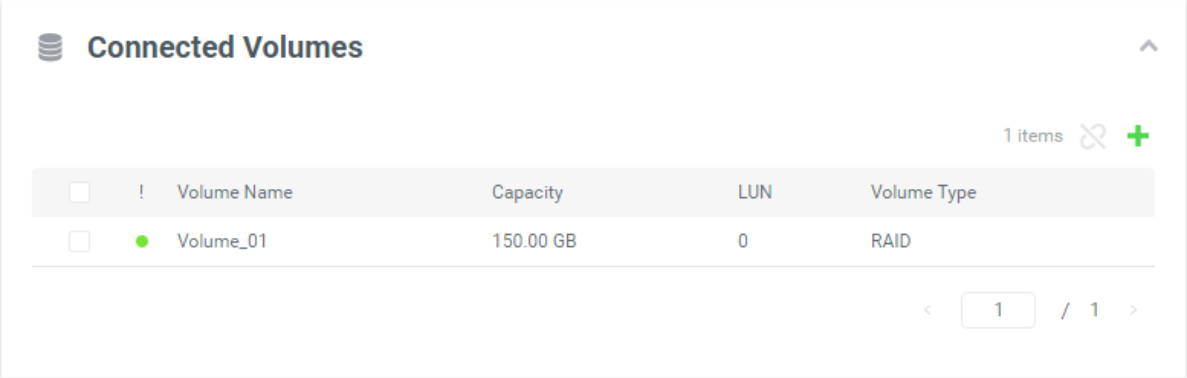


Figure 6-25 List Connected Volumes

This table shows the connected volume descriptions.

Table 6-3 Connected Volume Column Descriptions

Column Name	Description
!	The status of the disk group: • Green Color / Normal: The volume is good. • Orange Color / Abnormal: The pool is unhealthy and incomplete. The cause may be a disk loss or failure. • Red Light / Warning: The disk group has failed.
Volume Name	The volume name.
Capacity	Total capacity of the volume.
LUN	Display LUN (Logical Unit Number).
Volume Type	The type of the volume: • RAID Volume. • Backup Volume.

The options are available in this pane.

Connect Volumes

Here is an example to add volumes to the host group.

1. Click the + icon in the **Connected Volumes** pane to pop up a window.

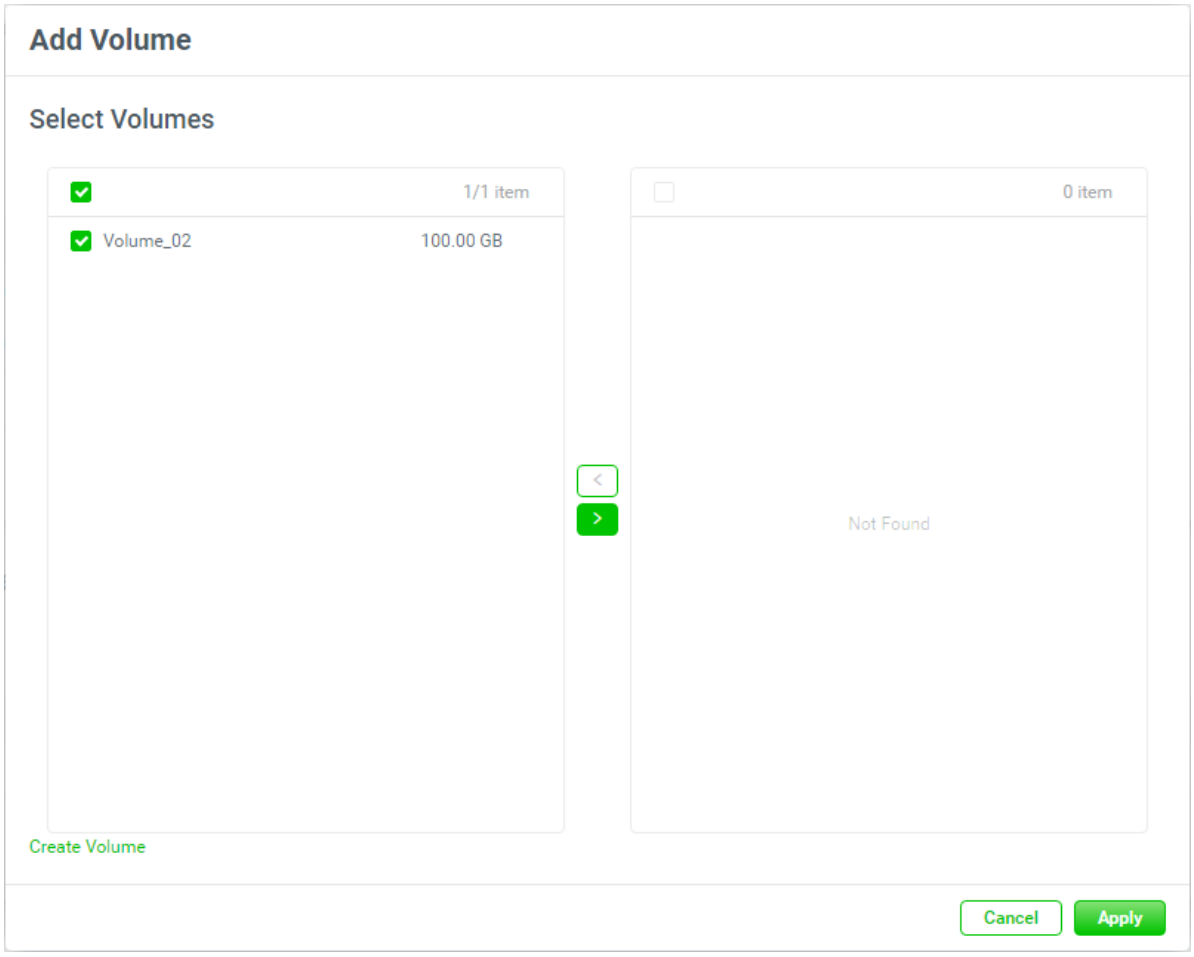


Figure 6-26 Add Volumes to the Host Group

2. The **Select Volumes** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective.
3. Select volumes and click the > button or the < button to make them effective or not.
4. Click the **Apply** button to add.

Disconnect Volumes

1. Check the volume checkboxes which you want to disconnect.

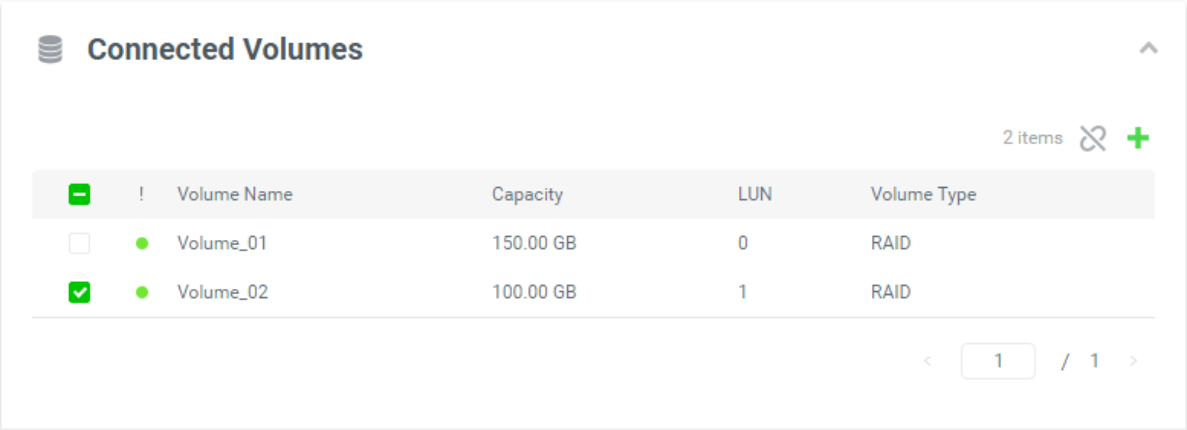


Figure 6-27 Disconnect Volumes

2. Click the icon to continue. Then click the **Disconnect** button to confirm and disconnect.

6.1.5. List and Configure CHAP Settings

Click the **CHAP Settings** pane to list all CHAP settings in the host group. This pane is only visible when the protocol of the host group is iSCSI. Here is an example to enable CHAP settings.

1. Check the **Select IQNs & WWNs** checkbox to enable CHAP.

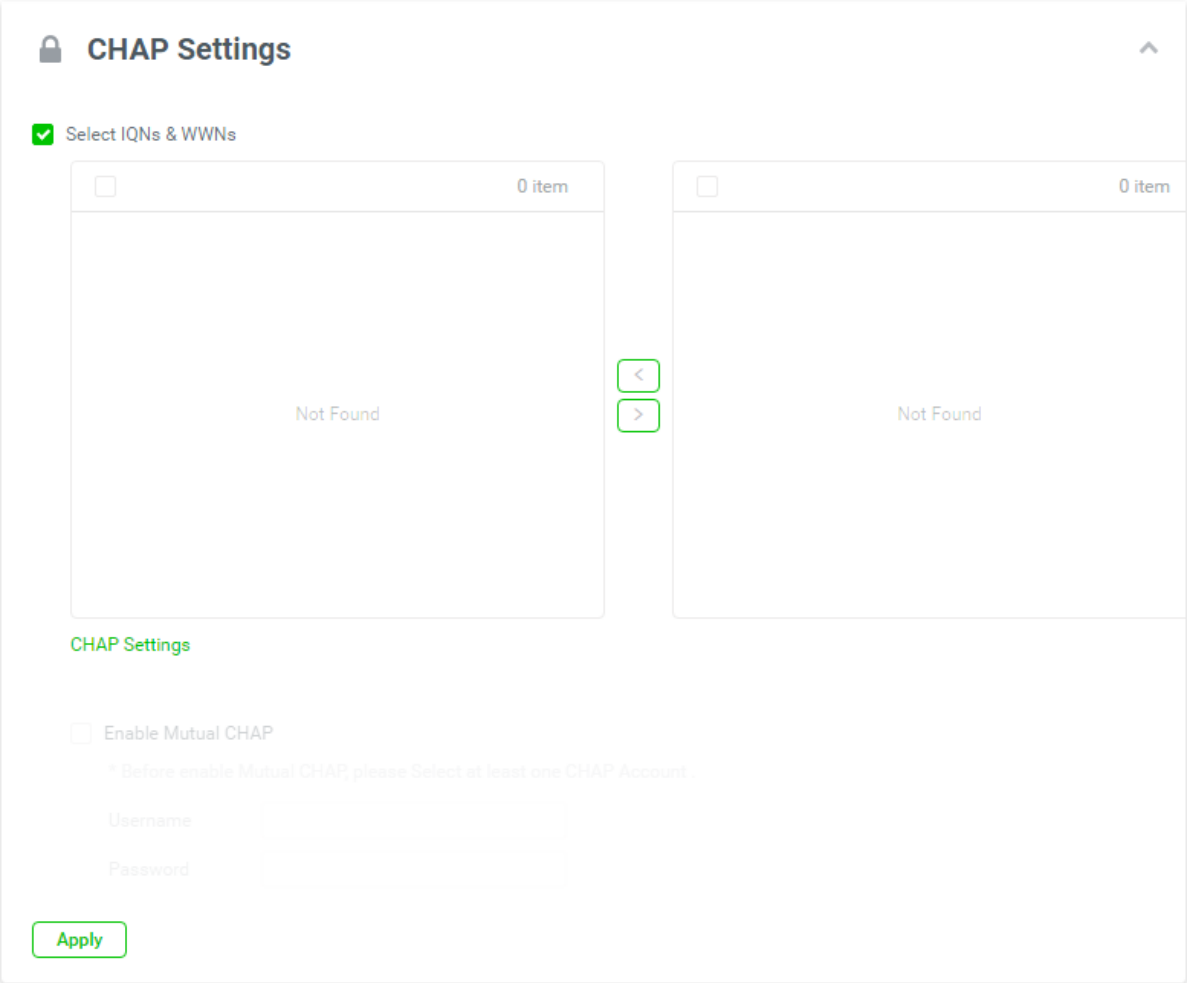


Figure 6-28 CHAP Settings 1

2. Click **CHAP Settings** to add CHAP accounts.

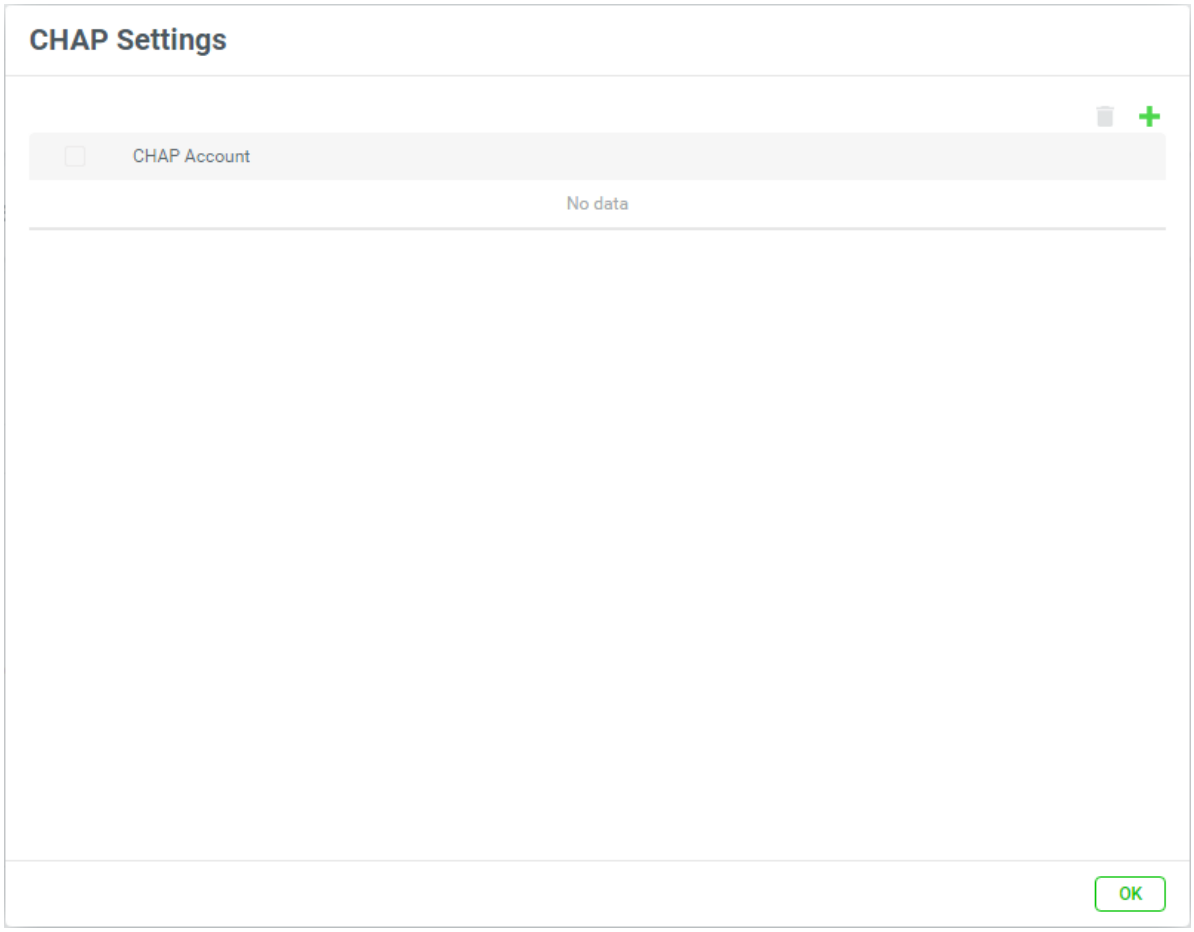


Figure 6-29 CHAP Accounts 1

3. Click the + icon in the **Volumes** pane to pop up a window.

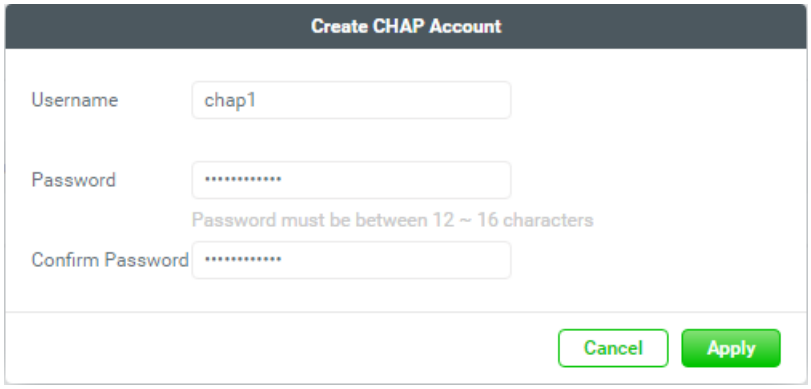


Figure 6-30 Create a CHAP Account

4. Enter **Username** of CHAP user. The maximum length of the username is 223 characters. Valid characters are [A~Z | a~z | 0~9 | ~!@#%^&*_-+=|(){}[]:;<>.?/].
5. Enter **Password** (CHAP secret) and **Confirm Password**. The length of the password is between 12 to 16 characters. Valid characters are [A~Z | a~z | 0~9 | ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/].
6. Click the **Apply** button to create a CHAP account.

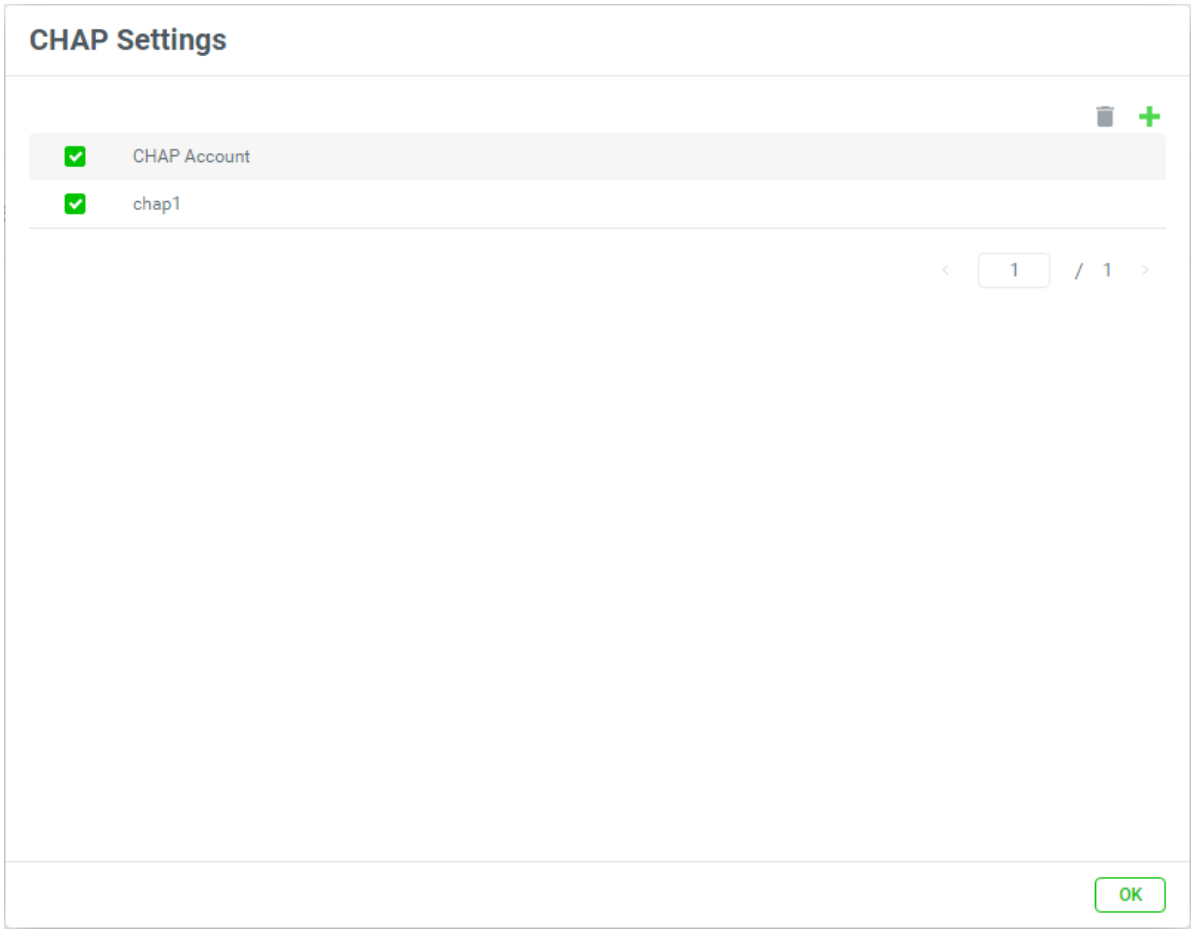


Figure 6-31 CHAP Account 2

7. A CHAP account has been created. If necessary, click the + icon to create others.
8. If the CHAP accounts are useless, check the account checkboxes which you want to delete, and then click the icon to delete.
9. Click the **OK** button to close the window.

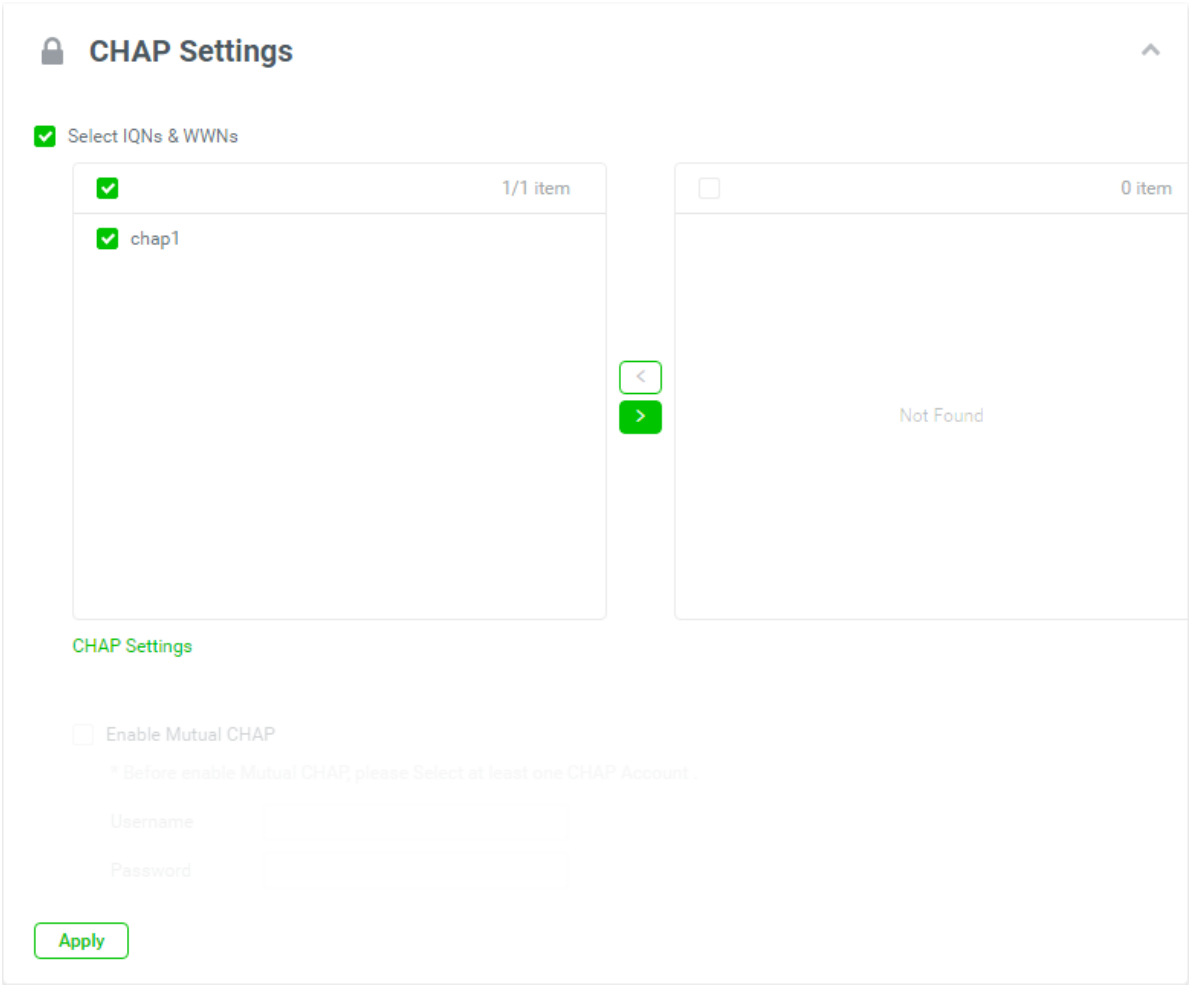


Figure 6-32 CHAP Settings 2

10. The **CHAP Settings** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective. Select the CHAP accounts and click the > button or the < button to make them effective or not.

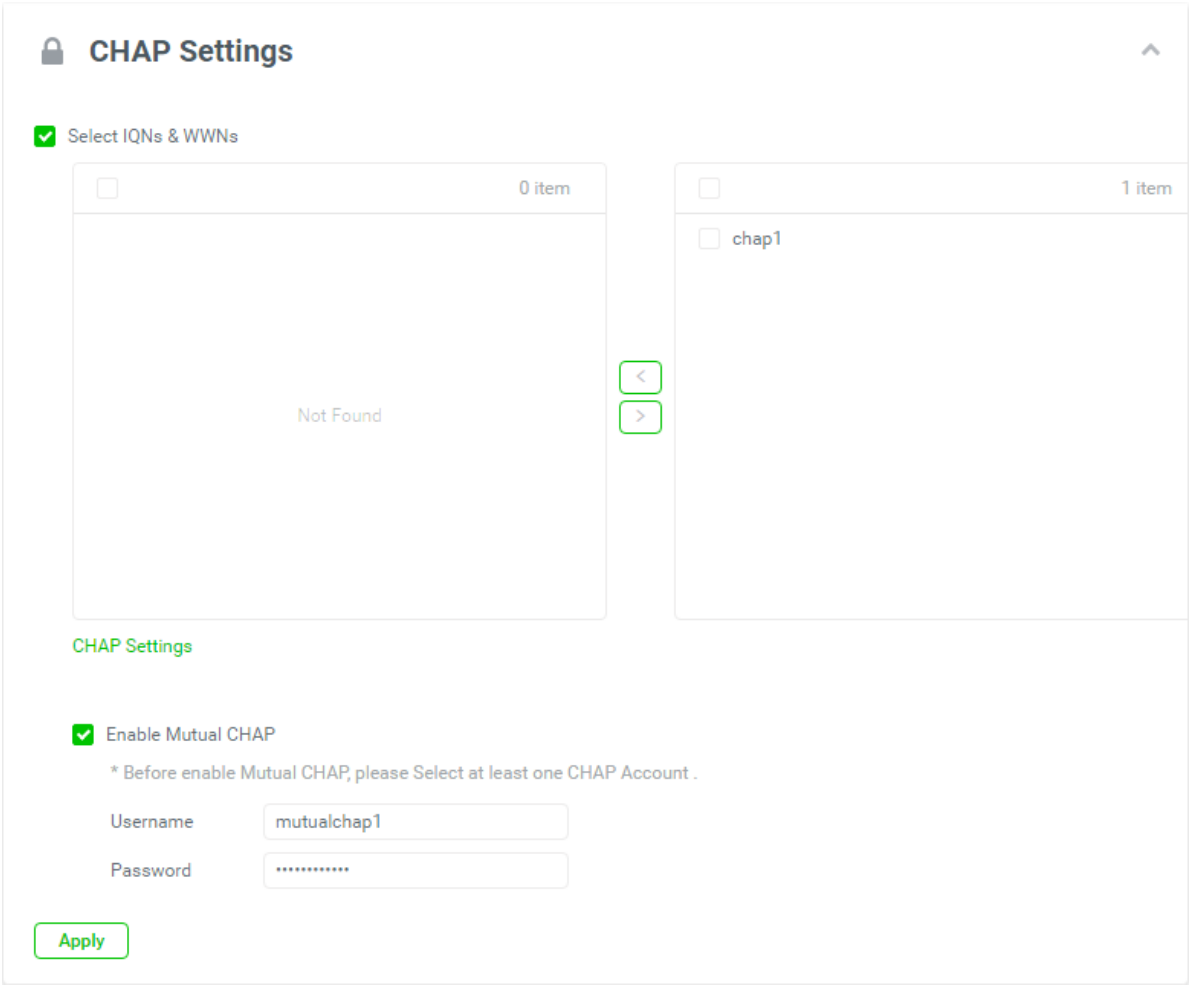


Figure 6-33 CHAP Settings 3

11. If necessary, check **Enable Mutual CHAP** to enable mutual CHAP authentication.
12. Enter **Username** of mutual CHAP user. The maximum length of the username is 223 characters. Valid characters are [A~Z | a~z | 0~9 | ~!@#%^&*_-+=|(){}[]:;<>.?/].
13. Enter **Password** (mutual CHAP secret). The length of the password is between 12 to 16 characters. Valid characters are [A~Z | a~z | 0~9 | ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/].
14. Click the **Apply** button to setup the CHAP settings.

7. Protection Tab

The **Protection** tab manages the protection groups. It displays the protection group status, configures the protection plan and protection volumes. This chapter describes the details of protection group management operations and examples.

7.1. Protection Features

XEVO provides protection group functionality for binding one or some volumes. These volumes can perform data backup services at the same time with some simple settings. In addition to the basic functions of snapshots, local cloning, and remote replication, there are new designs and are described below.

7.1.1. About Snapshot

Enable Snapshot Space Automatically

A volume snapshot is based on copy-on-write technology. Snapshots require more space to hold differential data. When the schedule function is enabled, all volumes belonging to the protection group will automatically enable snapshot space. The default snapshot space is 10% of the volume capacity. You can also enter the **Snapshot Center** of the volume and customize it.

Recycle Snapshots

Snapshot recycle bin can restore or permanently destroy the snapshots. It offers additional protection for backup from accidentally or deliberately deleting of a snapshot.

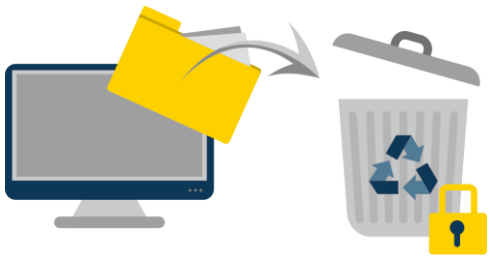


Figure 7-1 Recycle Snapshots

7.1.2. About Local Clone

It does easily deploy the local clone without doing configurations. In a protection group, select a new and empty target pool, the system will send the configurations of source volumes to the target pool. Then the target pool will generate the corresponding volumes.

Figure 7-2 Auto Local Clone

The limit is that the capacity of the target pool should be larger than the total capacity of all volumes in the protection group.

7.1.3. About Remote Replication

Auto Replication

It does easily deploy the remote replication without doing configurations. In a protection group, you only need to log in a remote system through management port. The source system will send the configurations of volumes to the remote system. The remote system will generate the corresponding volumes for the source system.

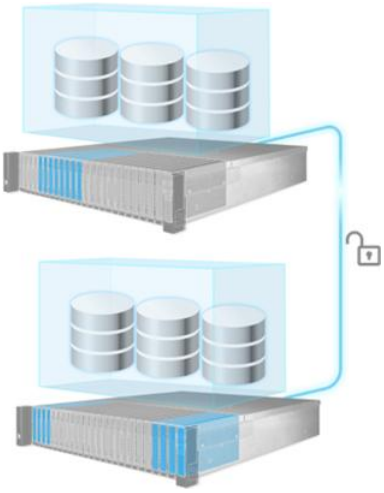


Figure 7-3 Auto Replication

The target system has to prepare at least 3 disk drives and the capacity of the target pool should be larger than the total capacity of all source volumes in the protection group.

1 Step Local-to-Remote

Through local-to-remote, transfer your local backup to remote sites without having to redo the full copy. On the remote side, you only need to insert all disk drives without any configurations. And then complete the local-to-remote process.

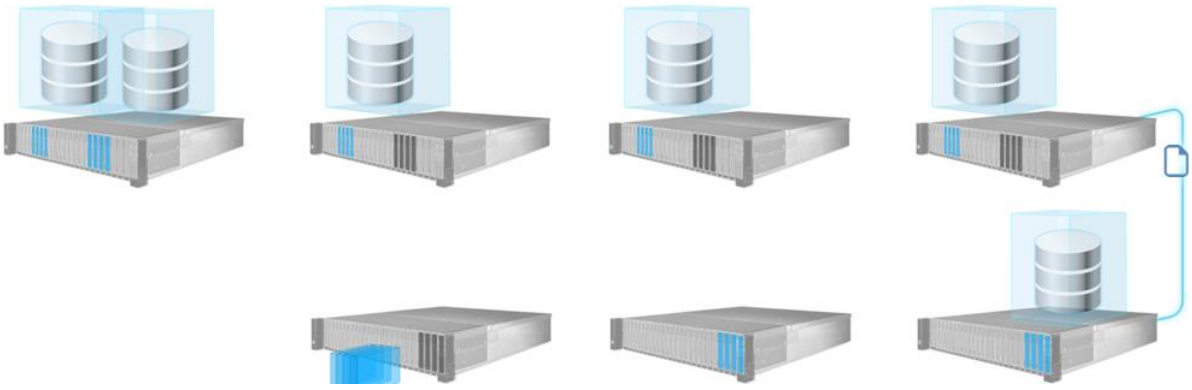


Figure 7-4 1 Step Local-to-Remote

INFORMATION:
The **Auto Replication** and **1 Step Local-to-Remote** features are supported by XEVO of XCubeFAS series only. It means that the source and target arrays are both running XEVO. In addition, The management ports and data ports of the source and target arrays must be connected to each other. Whether they are direct connections or through LAN switches.

CAUTION:
Snapshot function can only take the image of data which has been written into the corresponding volume, for the cached data that resides in the server's cache, that doesn't yet be flushed into the storage system, it is unable to protect, which means the taken snapshot might consist of inconsistent data/file/boot image, please make sure to take snapshot at the time point when there is no data I/O incoming to the storage system, to prevent the situation as much as possible. Any functionality that base on snapshot function to perform will have this kind of concern, e.g., local clone and remote replication.

SUGGESTION:
It is recommended to use native remote replication function upon the corresponding Operating System to prevent the situation, e.g., vSphere Replication (VR), so that the cached data can be seamlessly replicated to the target site.

7.2. Configure Protection Groups

Select the **Protection** tab to manage the protection groups. In this tab, you can create, modify, delete, or view the status of all protection groups.

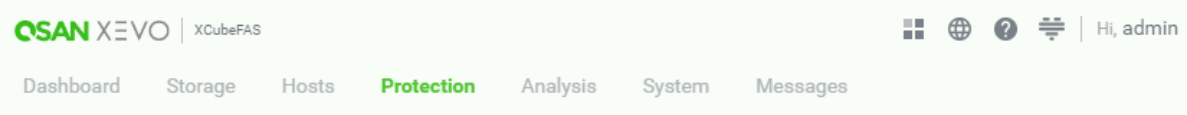


Figure 7-5 Protection Tab

INFORMATION:
A protection group includes one of a **Snapshot Plan** and/or either one of **Replication Plan** for Local or Remote.

7.2.1. Create a Protection Group

Here is an example of creating a protection group and connecting volumes.

1. Click the + icon in the **Protection Groups** pane to pop up a wizard.

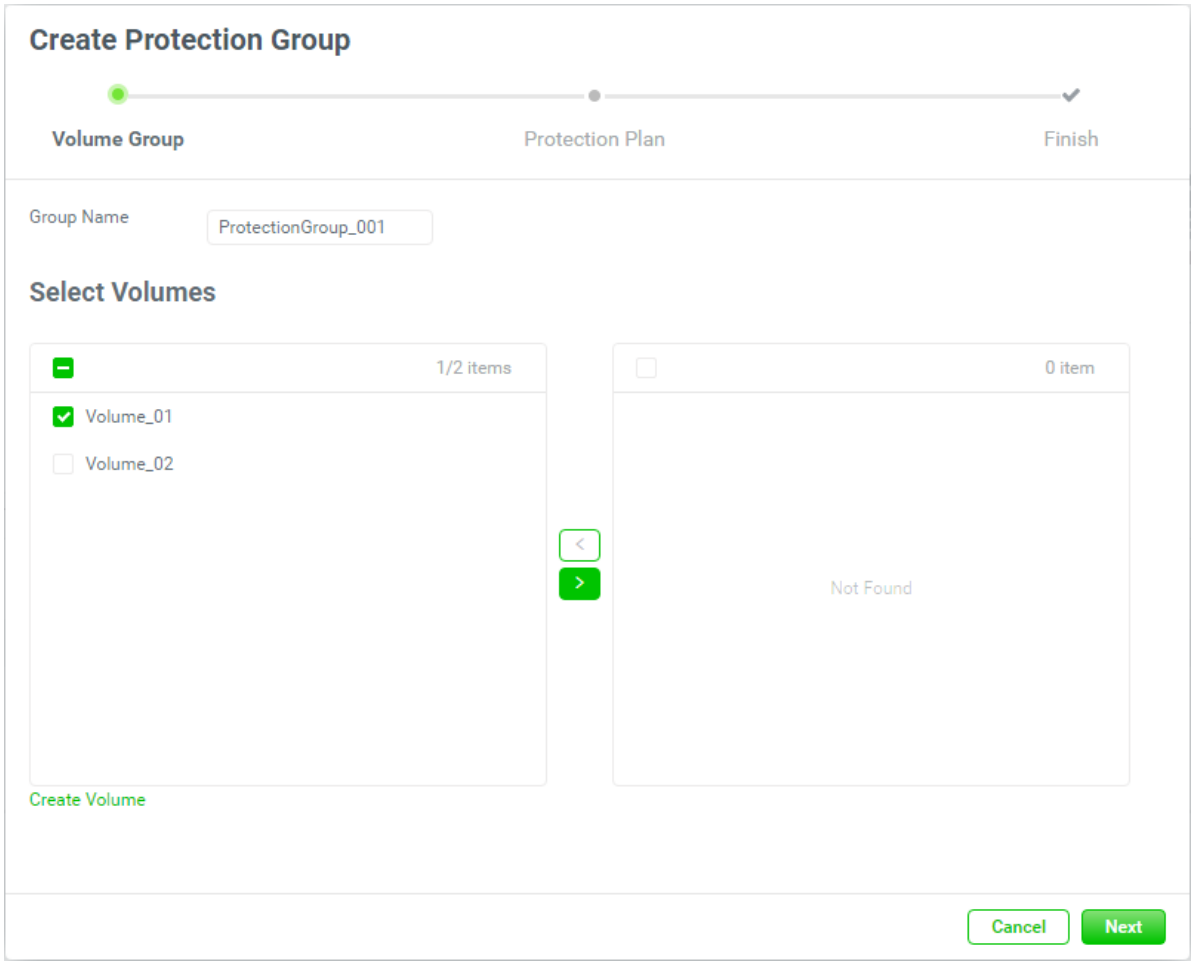


Figure 7-6 Create a Protection Group Step 1-1

2. The recommended **Group Name** is provided. Enter a new **Group Name** if necessary. The maximum length of the pool name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. The **Select Volumes** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective.
4. Select volumes and click the button to move it from the left side to the right side.

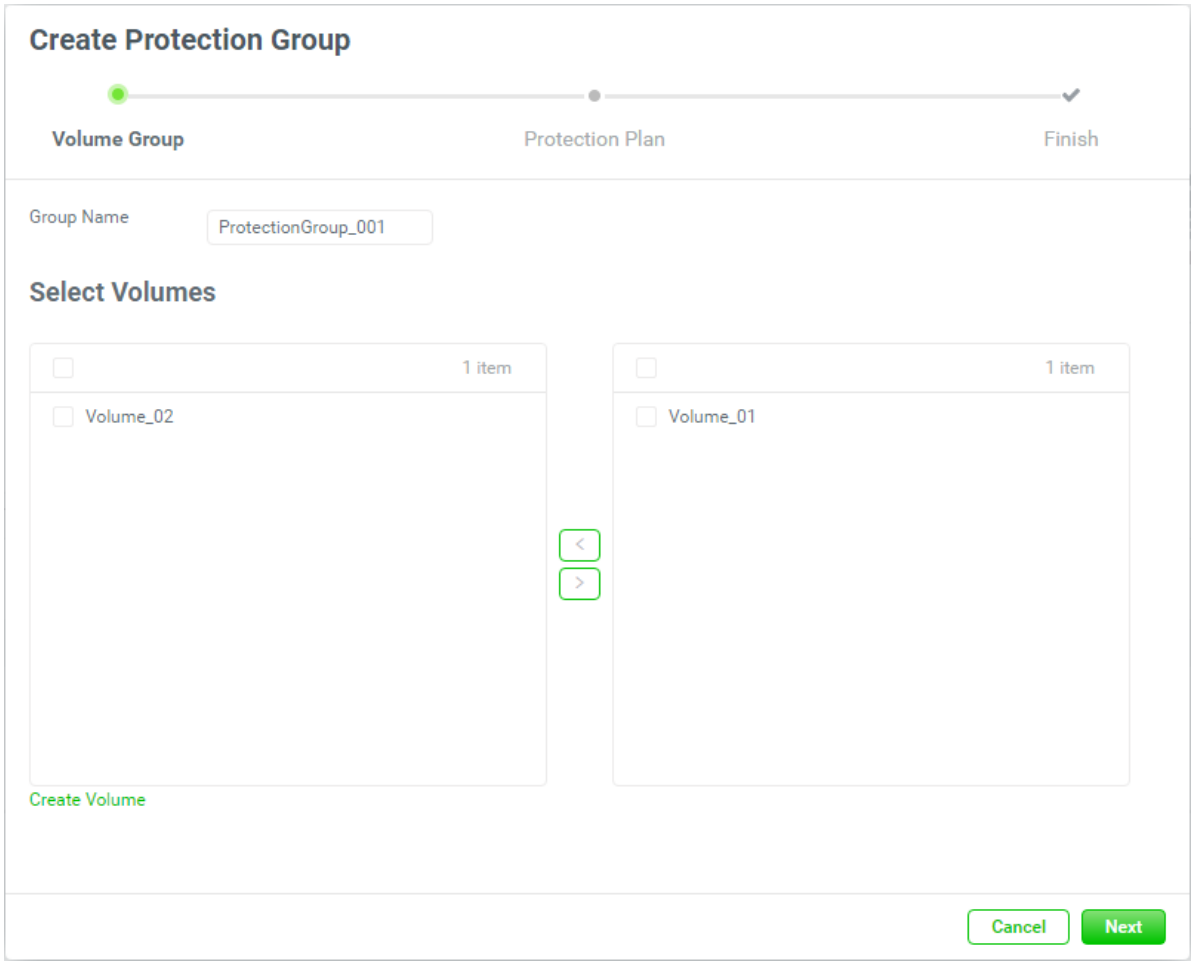


Figure 7-7 Create a Protection Group Step 1-2

5. Click the **Next** button to continue.

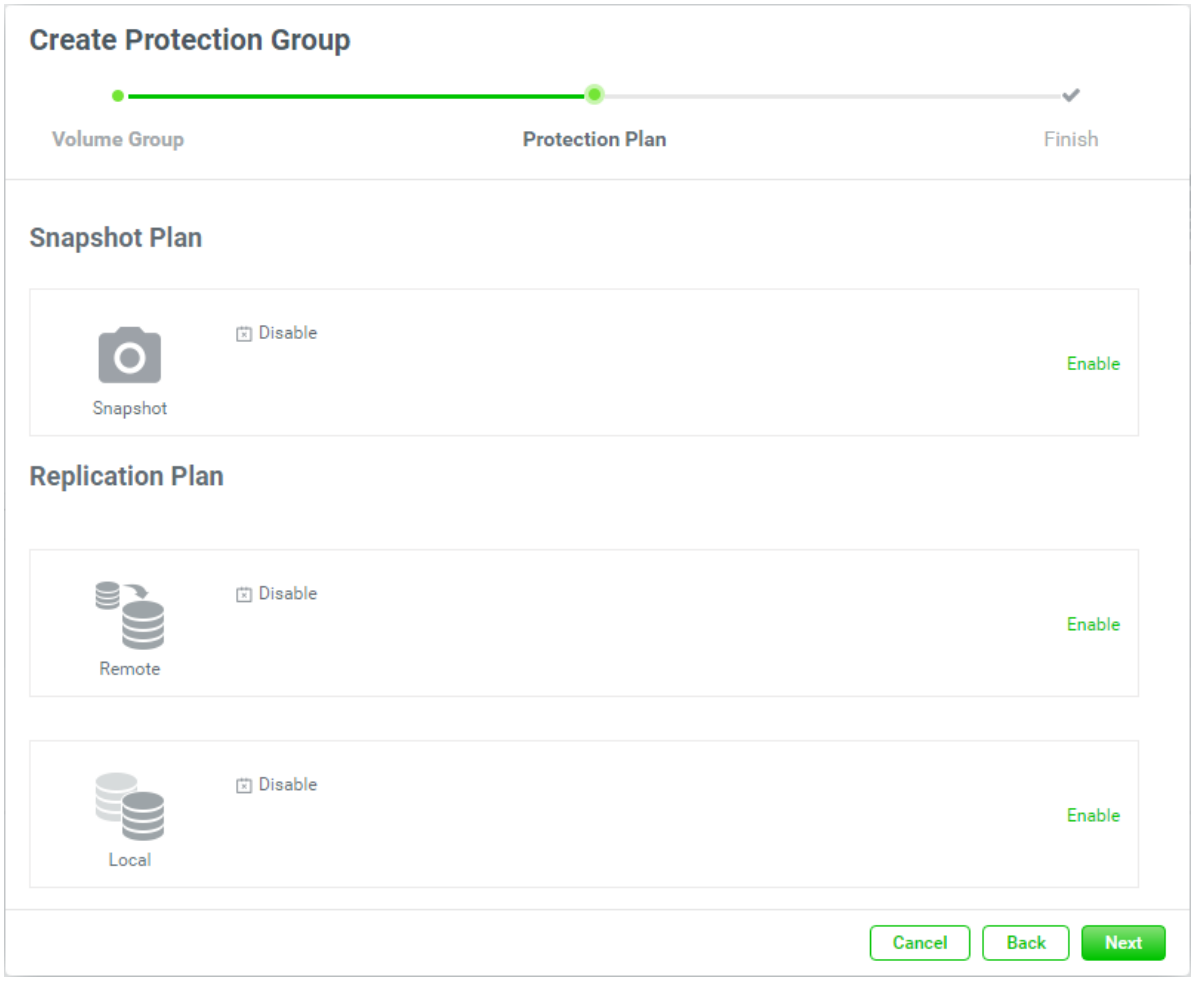


Figure 7-8 Create a Protection Group Step 2-1

Enable Snapshot Plan

6. Click the **Enable** text in the **Snapshot** pane to enable the **Snapshot Plan**.

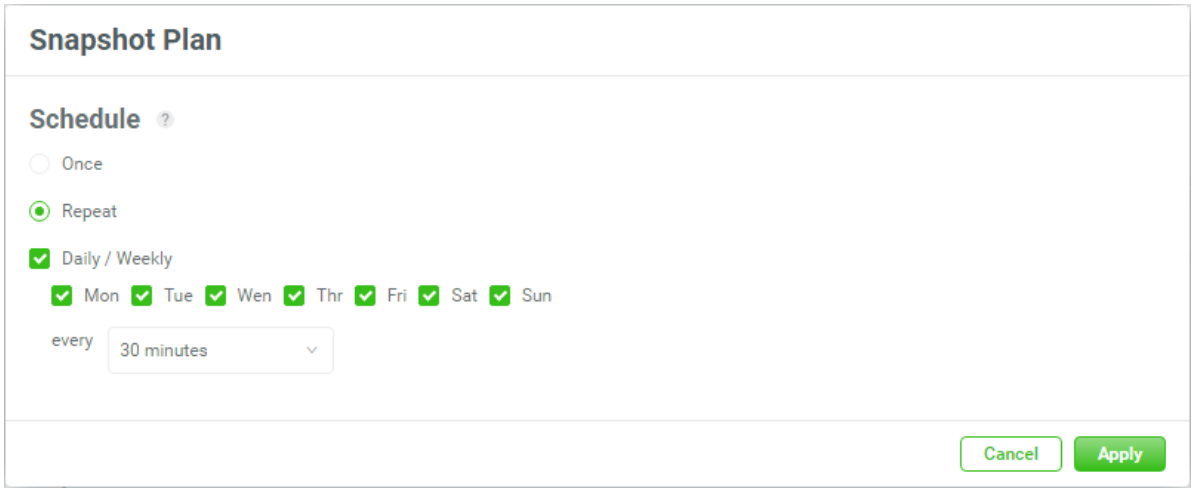


Figure 7-9 Enable Snapshot Plan

7. Select the **Once** option to execute the plan once. Or select the **Repeat** option to repeat the plan, and then check the repeat frequency.
8. Click the **Apply** button to continue.

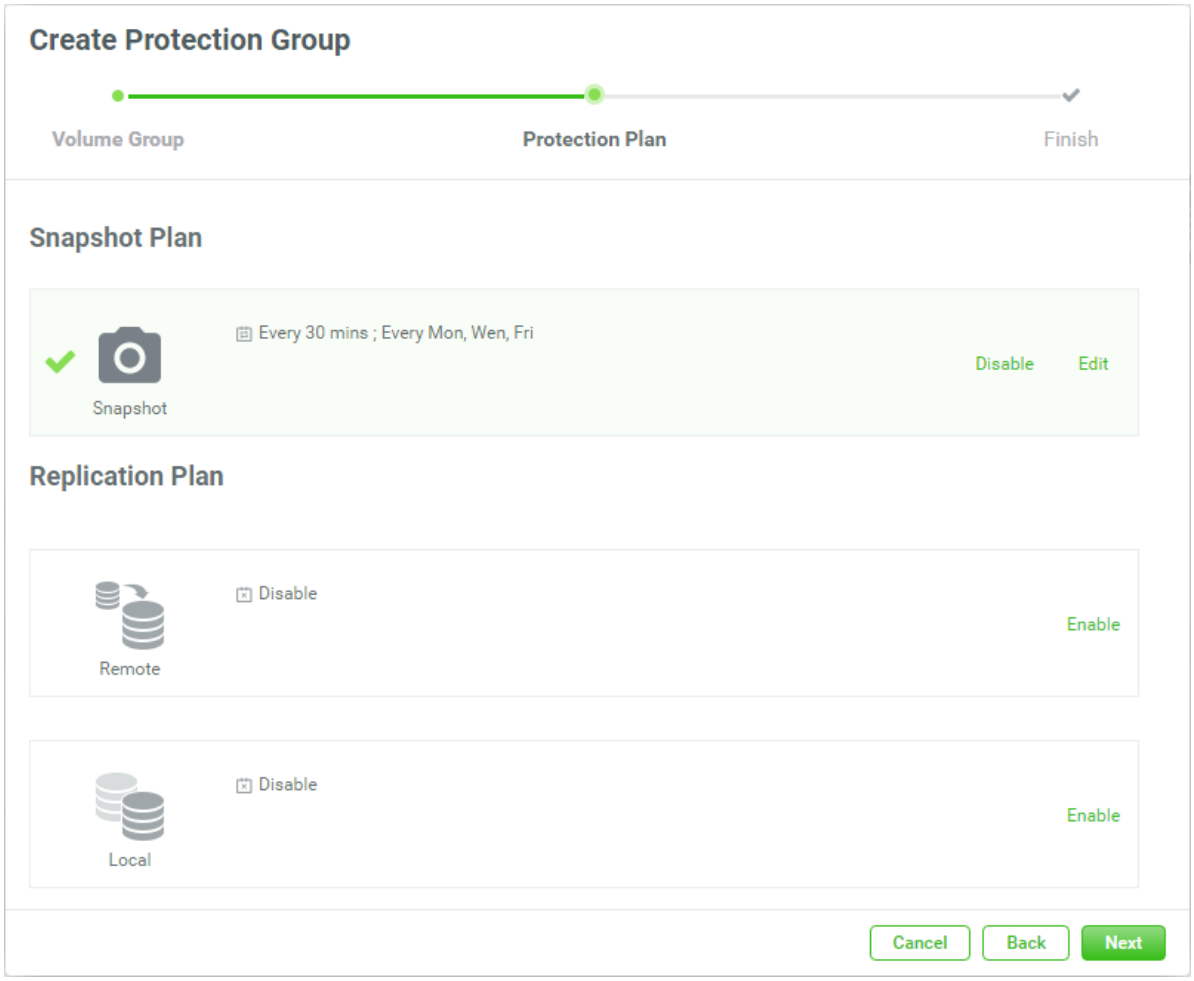


Figure 7-10 Create a Protection Group Step 2-2

INFORMATION:
A protection group can only be enabled one of the **Remote** or **Local** replication plan.

Enable Replication Plan - Remote

9. Click the **Enable** text in the **Remote** pane to enable the **Replication Plan - Remote**.

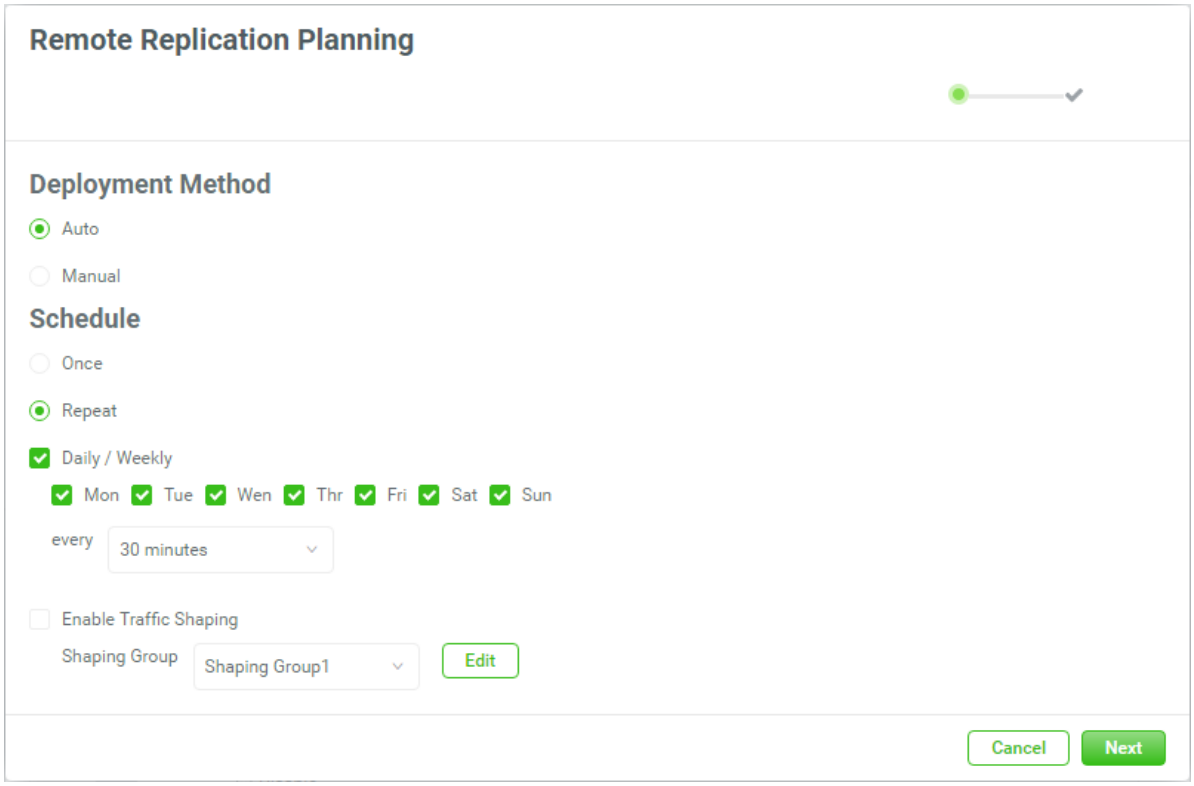


Figure 7-11 Enable Remote Replication Plan Step 1

10. Select the **Deployment Method** as **Auto** or **Manual**.

INFORMATION:
The **Auto** option of the **Deployment Method** supports **Auto Replication** feature described in the chapter 7.1.3 About Remote Replication.

11. Select the **Once** option to execute the plan once. Or select the **Repeat** option to repeat the plan, and then check the repeat frequency.
12. Check the **Enable Traffic Shaping** option if necessary and then click the **Edit** button to edit the shaping group.

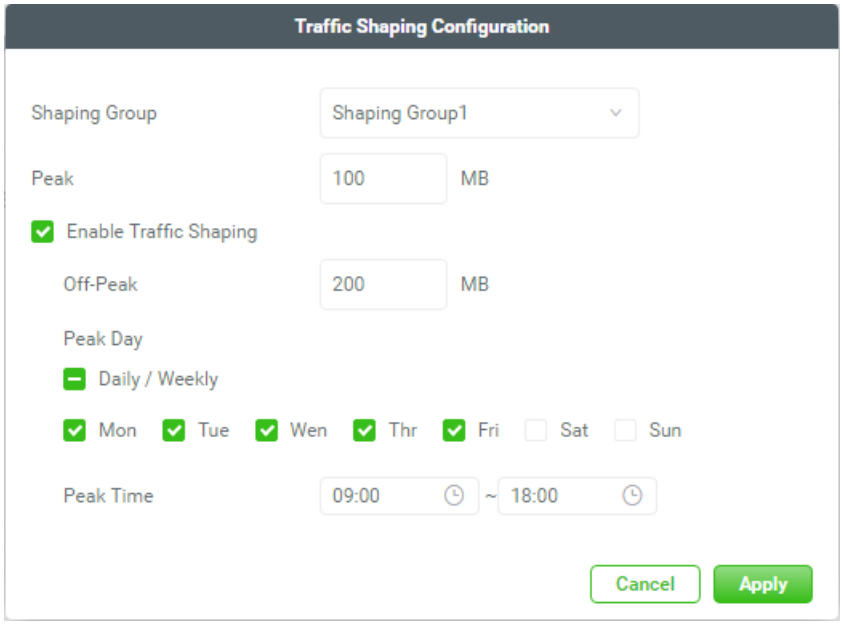


Figure 7-12 Traffic Shaping Configuration

13. Select a **Shaping Group** to be modified, enter a maximum throughput during **Peak** hours. Check the **Enable Traffic Shaping** option if necessary, and then enter a maximum throughput during **Off-Peak** hours and define the **Peak Day**.
14. Click the **Apply** button to continue.
15. Select the **Shaping Group** which you want.
16. Click the **Apply** button to continue.

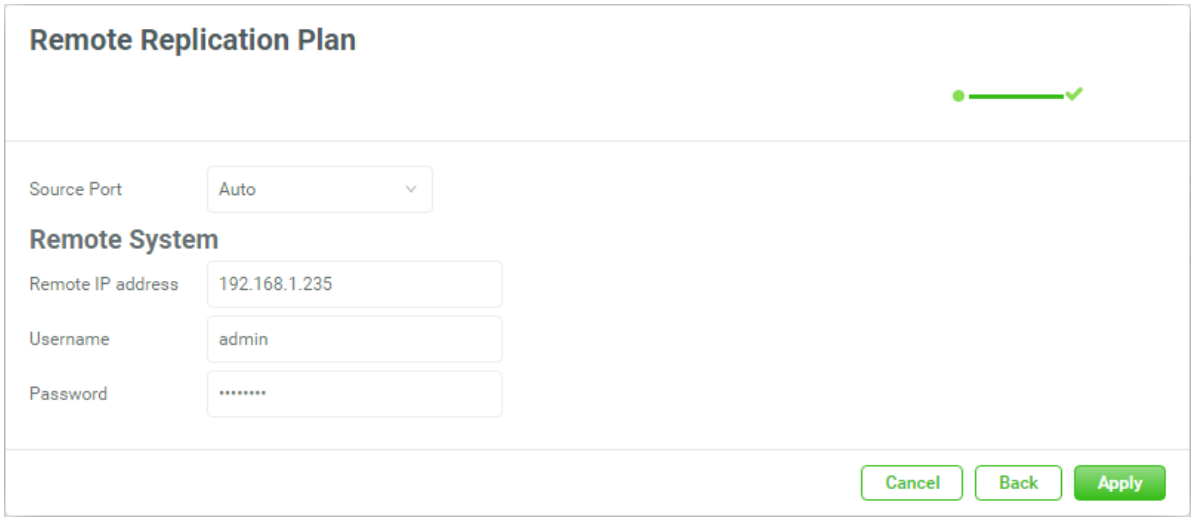


Figure 7-13 Enable Remote Replication Plan Step 2

17. Select the **Once** option to execute the plan once. Or select the **Repeat** option to repeat the plan, and then check the repeat frequency.
18. Click the **Apply** button to continue.

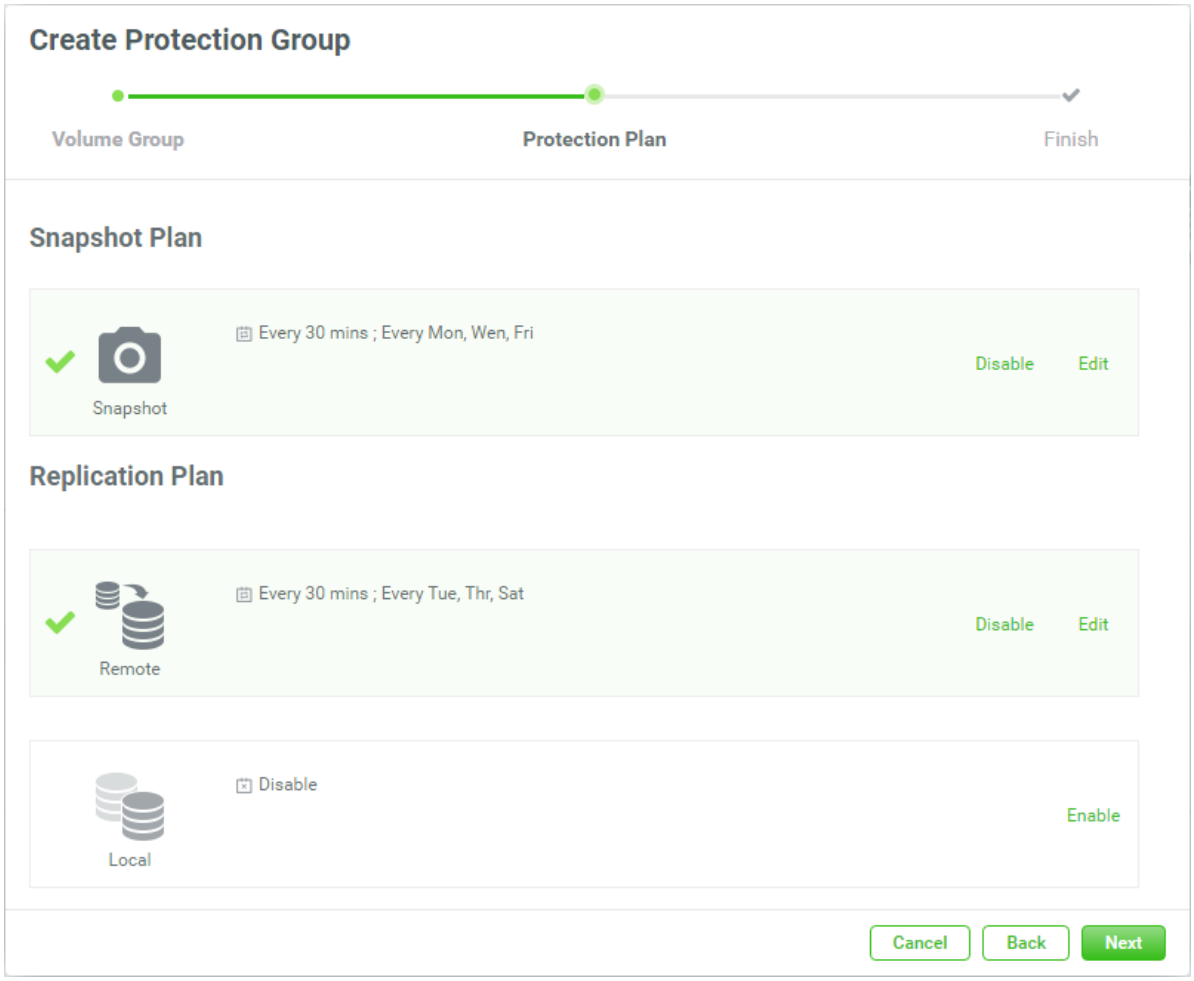


Figure 7-14 Create a Protection Group Step 2-3

INFORMATION:
A protection group can only be enabled one of the **Remote** or **Local** replication plan.

Enable Replication Plan - Local

19. Click the **Enable** text in the **Local** pane to enable the **Replication Plan - Local**.

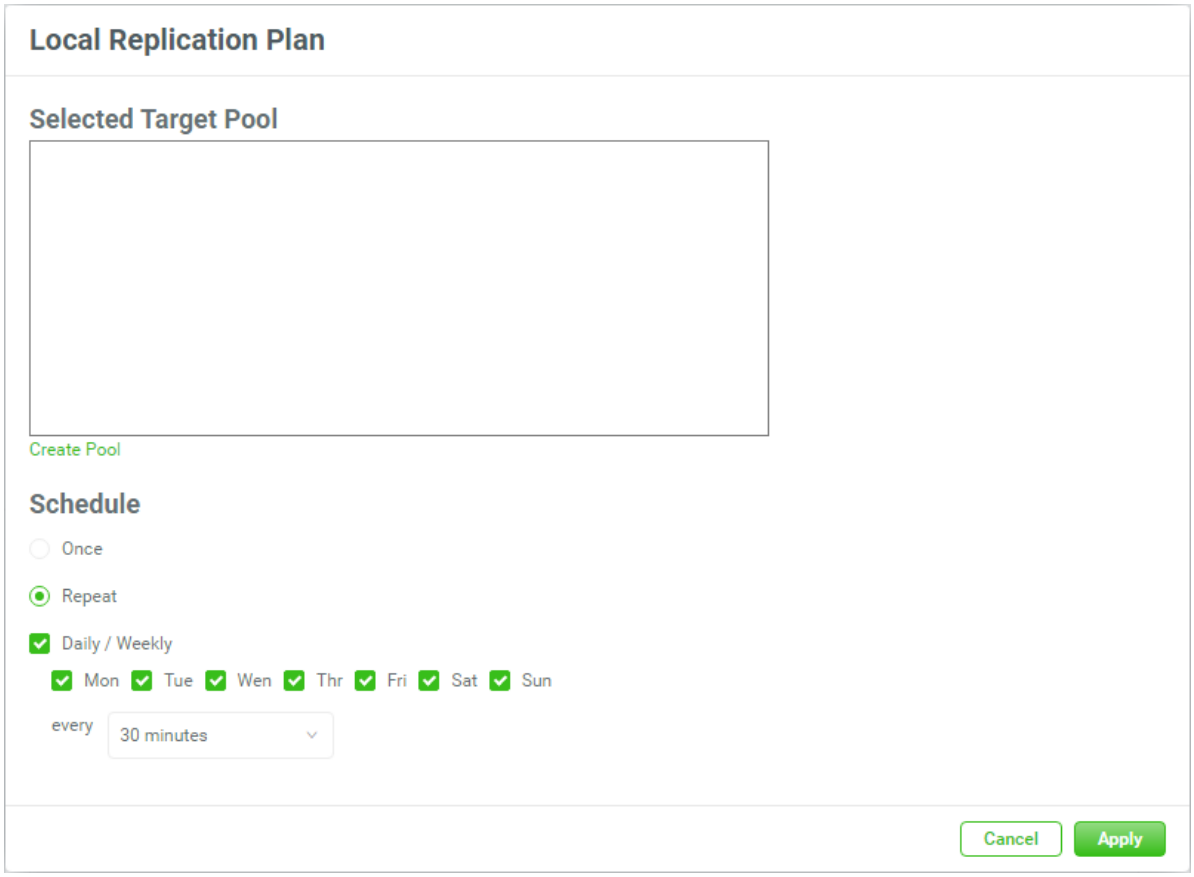


Figure 7-15 Local Replication Plan Step 1

20. Select a target pool, or click the **Create Pool** option to create one if it's empty.

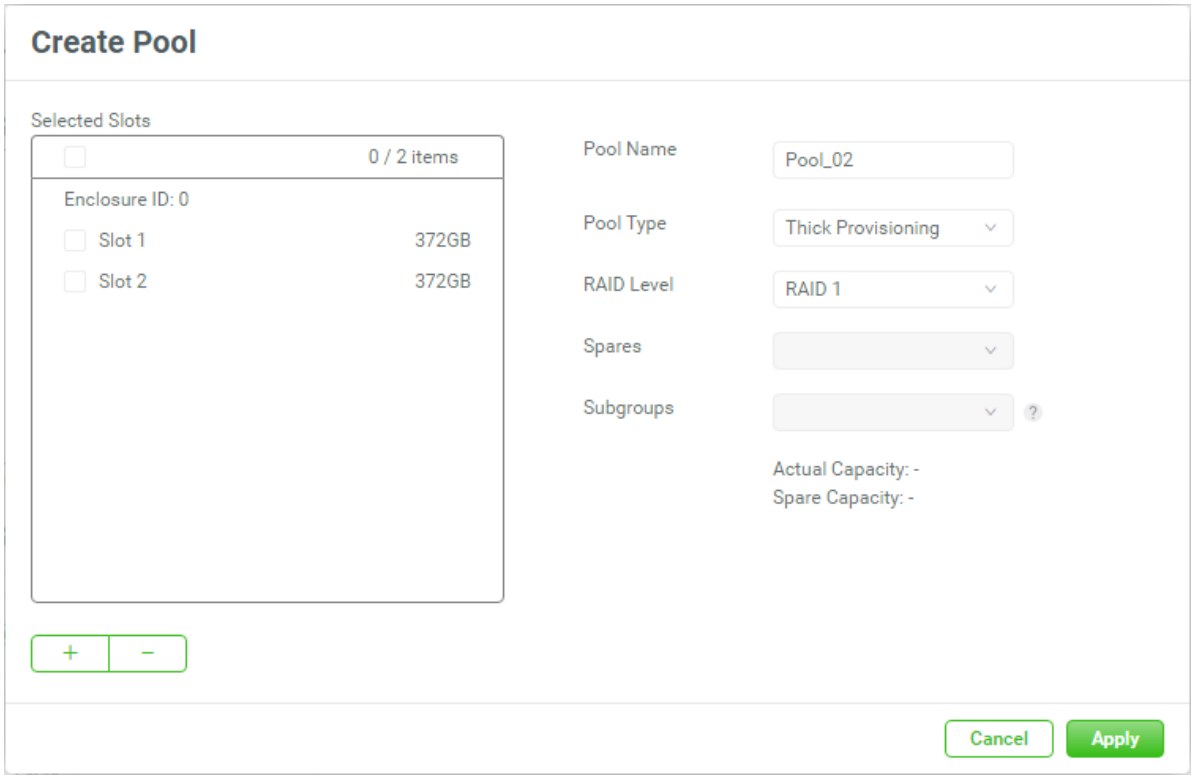


Figure 7-16 Create a Replication Target Pool

21. Please refer to the chapter 5.1.1 Create a Pool section for more details to create a pool.
22. Click the **Apply** button to continue.

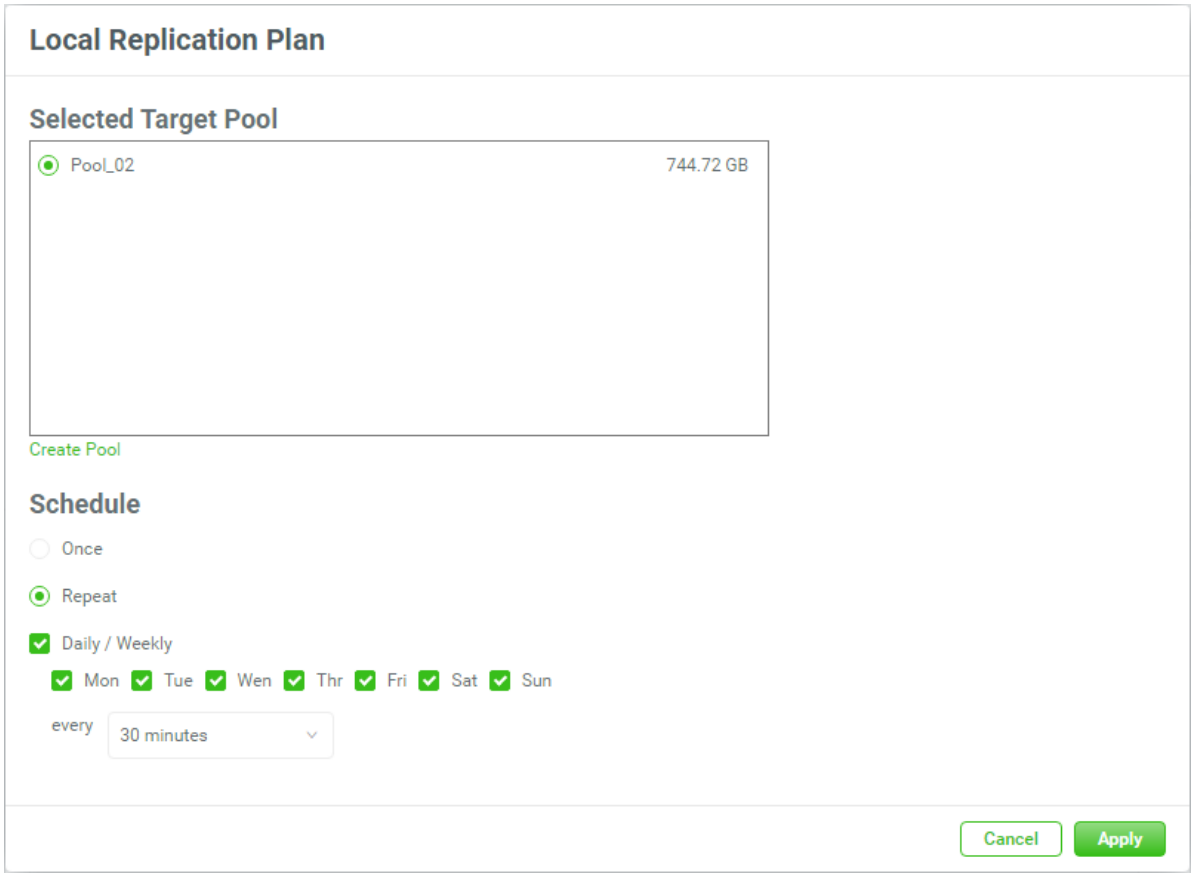


Figure 7-17 Local Replication Plan Step 2

23. Select a target pool, and select the **Once** option to execute the plan once. Or select the **Repeat** option to repeat the plan, and then check the repeat frequency.
24. Click the **Apply** button to continue.

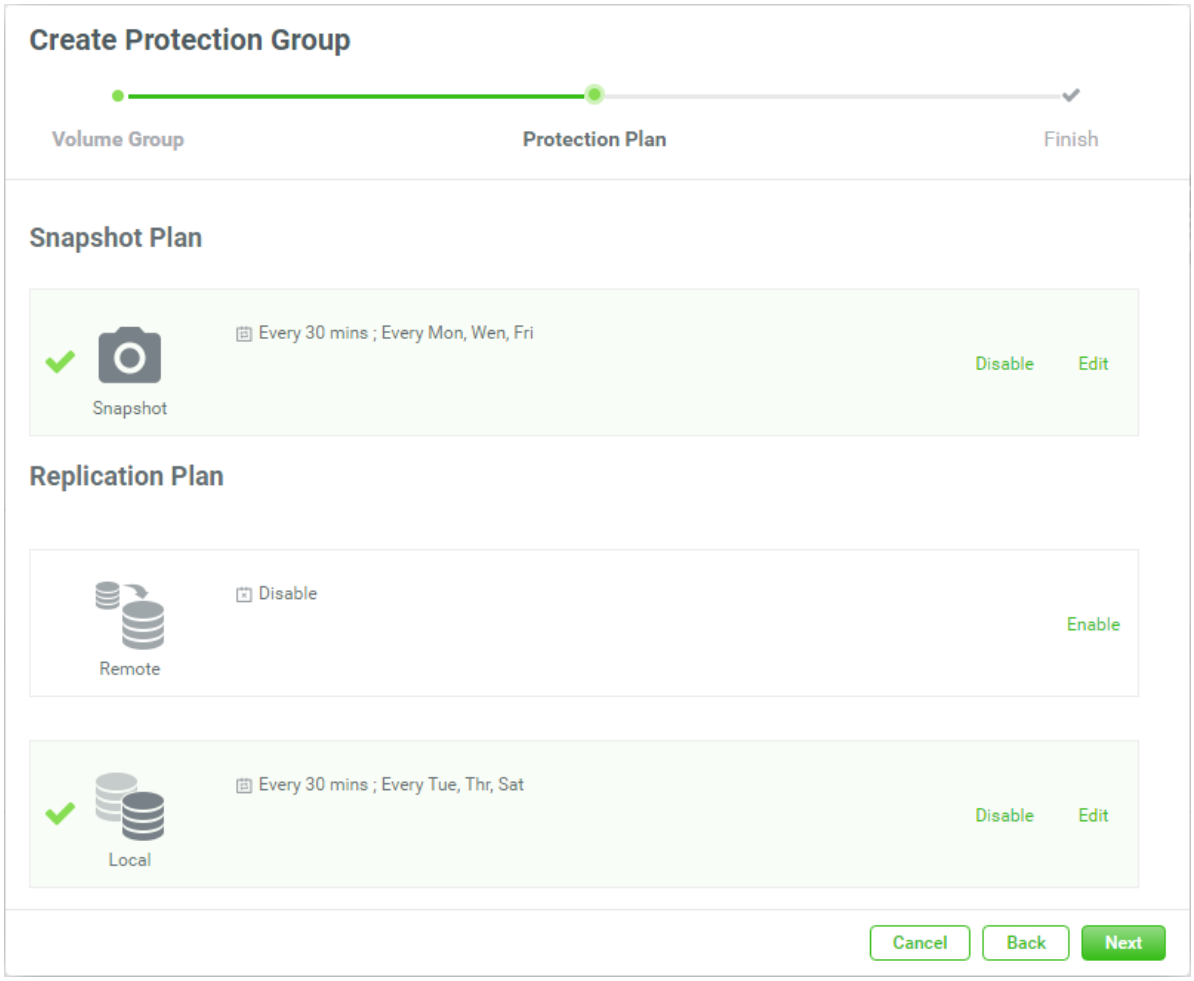


Figure 7-18 Create a Protection Group Step 2-4

25. Click the **Next** button to continue.

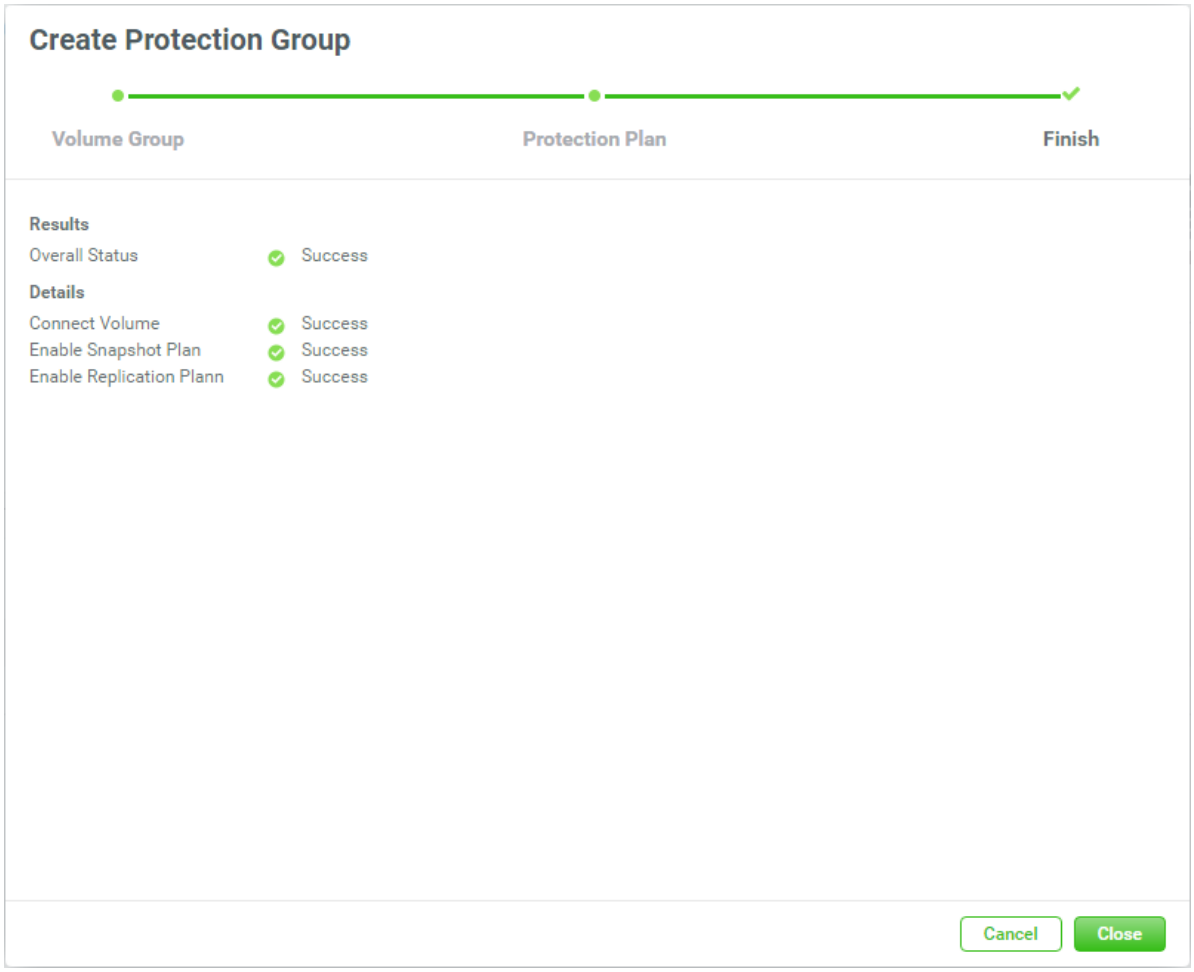


Figure 7-19 Local Replication Plan Step 3

26. There is a result page. Click the **Close** button to finish.

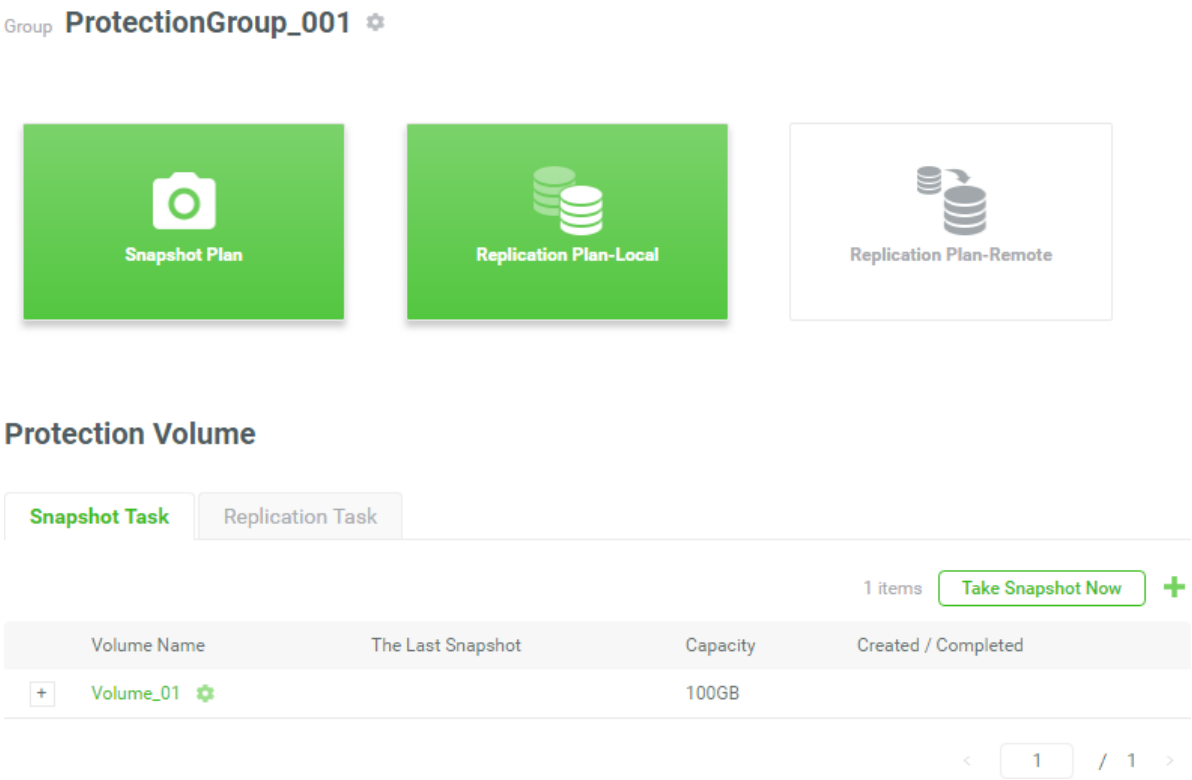


Figure 7-20 A Protection Group is Created

27. A protection group has been created. If necessary, click the + icon in the **Protection Groups** pane to create others.

7.2.2. List and Configure Snapshot Plan

All protection groups are listed in the **Protection Groups** pane. You can click one of them to display the details.

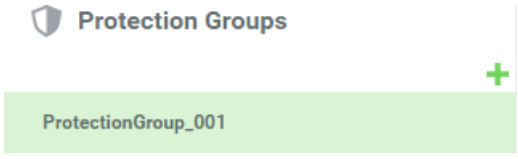


Figure 7-21 List All Protection Groups

A protection group is shown here.

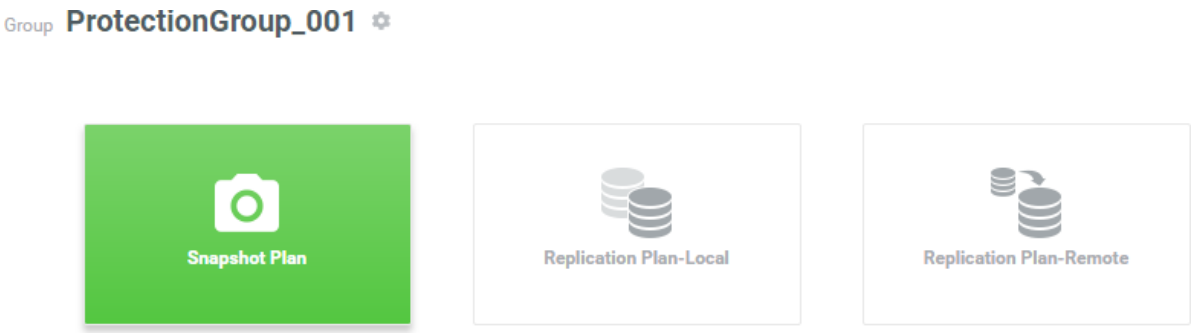


Figure 7-22 Protection Group with Snapshot Plan

The green box enables the service. The above figure enables the **Snapshot Plan** service. Clicking it will display the current snapshot plan.

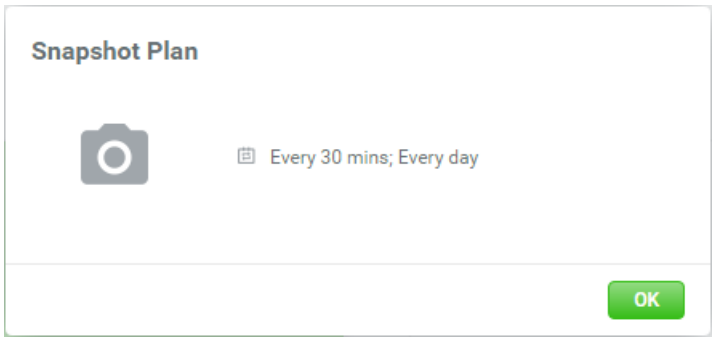


Figure 7-23 Snapshot Plan

Click the ⚙ icon beside the protection group name to list the drop down options.

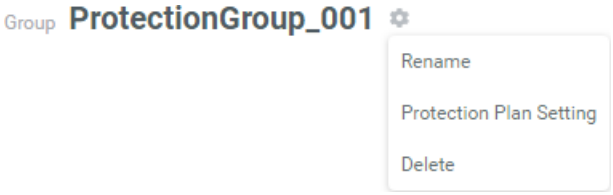


Figure 7-24 Protection Group Options with Snapshot Plan

These options are available in the protection group.

Rename

1. Click the **Rename** option to rename the host group.

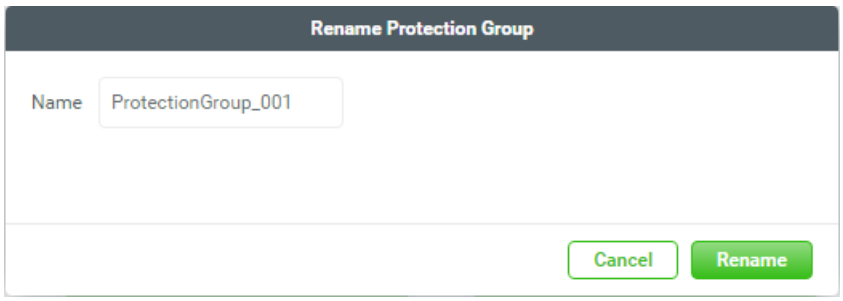


Figure 7-25 Rename Protection Group

2. Enter a new **Group Name**. The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. Click the **Rename** button to rename.

Protection Plan Setting

Click the **Protection Plan Setting** option to change the protection plan. Please refer to the chapter 7.2.1, Create a Protection Group section for more details.

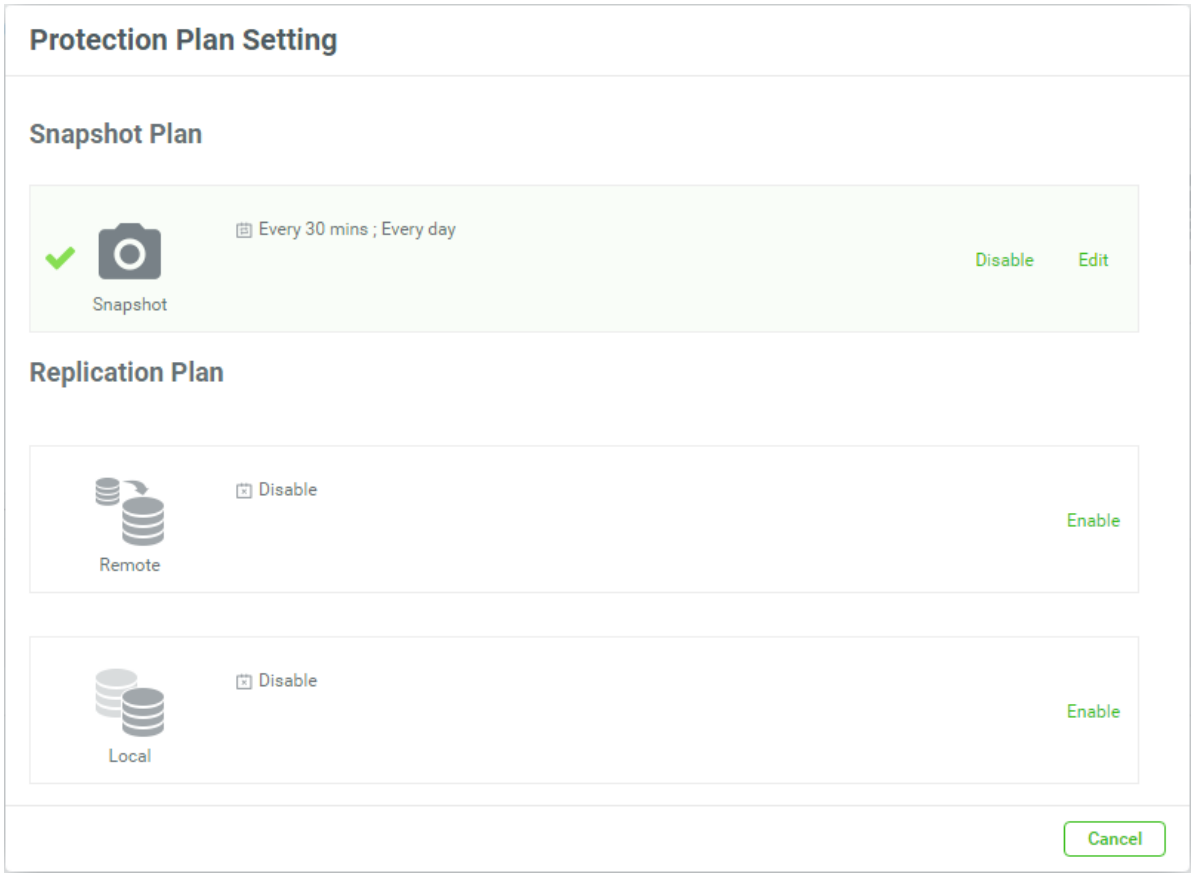


Figure 7-26 Protection Plan Setting

Delete

Click the **Delete** option to delete the protection group. Click the **Delete** button to confirm and delete.

At the **Protection Volume** pane, click the **Snapshot Task** tab to list all snapshot tasks.

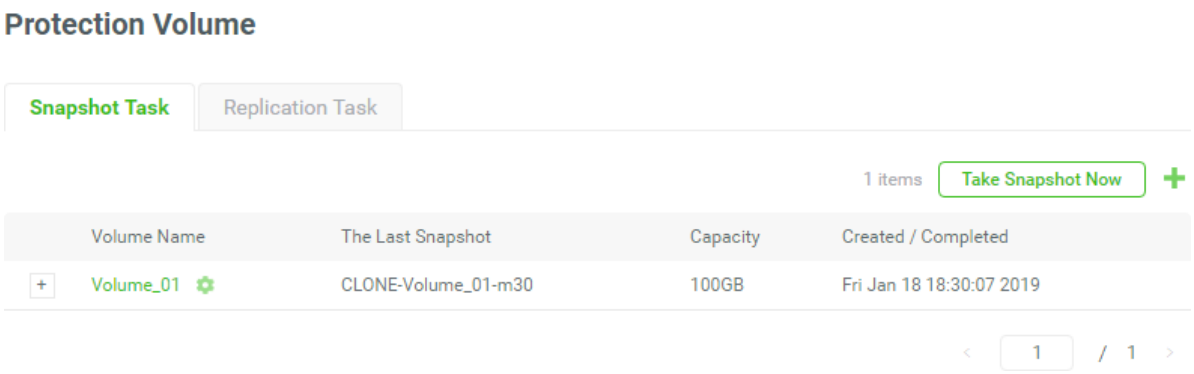


Figure 7-27 List Snapshot Tasks

The options are available in this tab.

Add Volumes

Here is an example to add volumes in the protection group.

1. Click the + icon in the **Snapshot Task** tab to pop up a window.

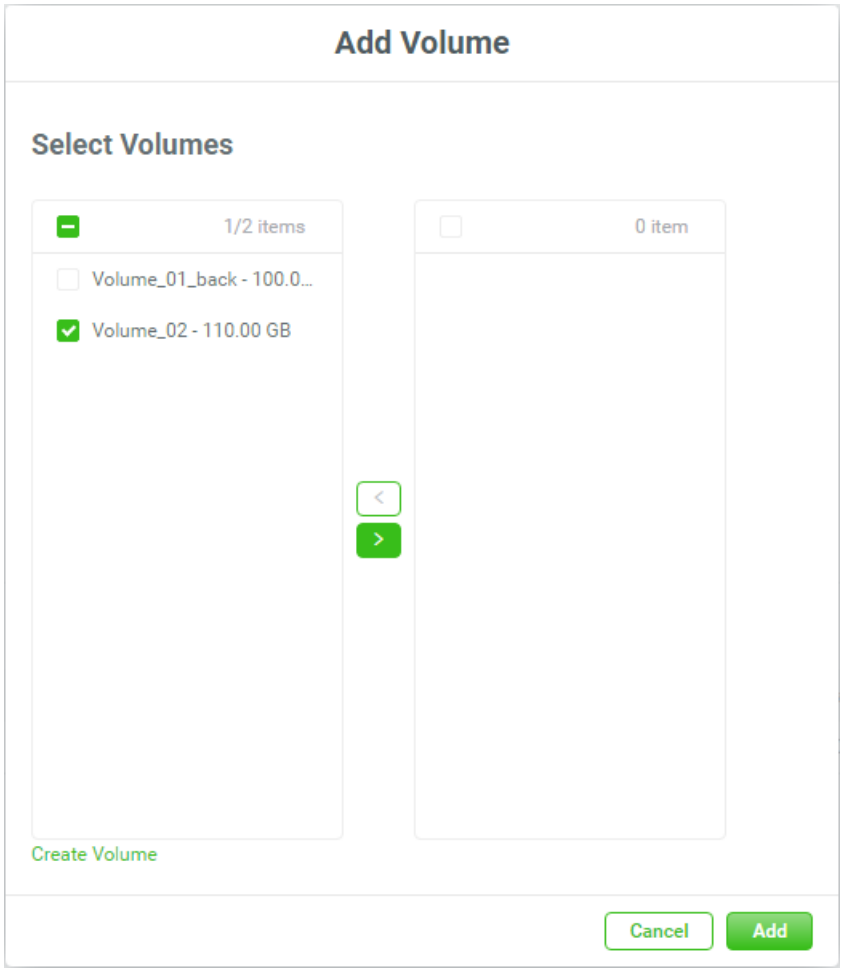


Figure 7-28 Add Volumes to the Protection Group

2. The **Select Volumes** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective.
3. Select volumes and click the > button or the < button to make them effective or not.
4. Click the **Add** button to add.

Take Snapshot Now

1. Click the **Take Snapshot Now** button to take a snapshot immediately.

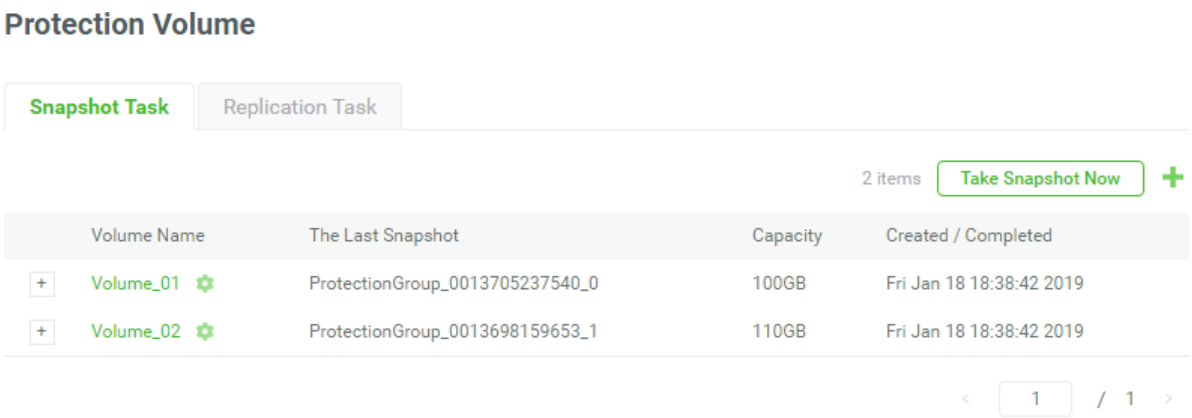


Figure 7-29 Take Snapshot Now

2. The snapshots are taken and displayed at **The Last Snapshot** field.

Click the ⚙ icon beside the volume name to list the drop down options. These options are available in the **Snapshot task** tab.

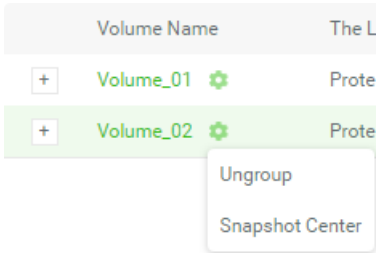


Figure 7-30 Snapshot Task Options

Ungroup

1. Click the **Ungroup** option to remove the volume from the protection group, and then pop up a confirm dialog box.
2. Click the **Ungroup** button to confirm.

Snapshot Center

About the snapshot center, please refer to the chapter 7.2.3, Snapshot Center section for more details.

7.2.3. Snapshot Center

Snapshot Center is a center for managing all snapshot functions. It can enable and expand the snapshot space. It also can take, rollback, or delete snapshots of the volume. In addition, the snapshot recycle bin can restore or permanently destroy the snapshots. Click the **Snapshot Center** option to pop up a window.

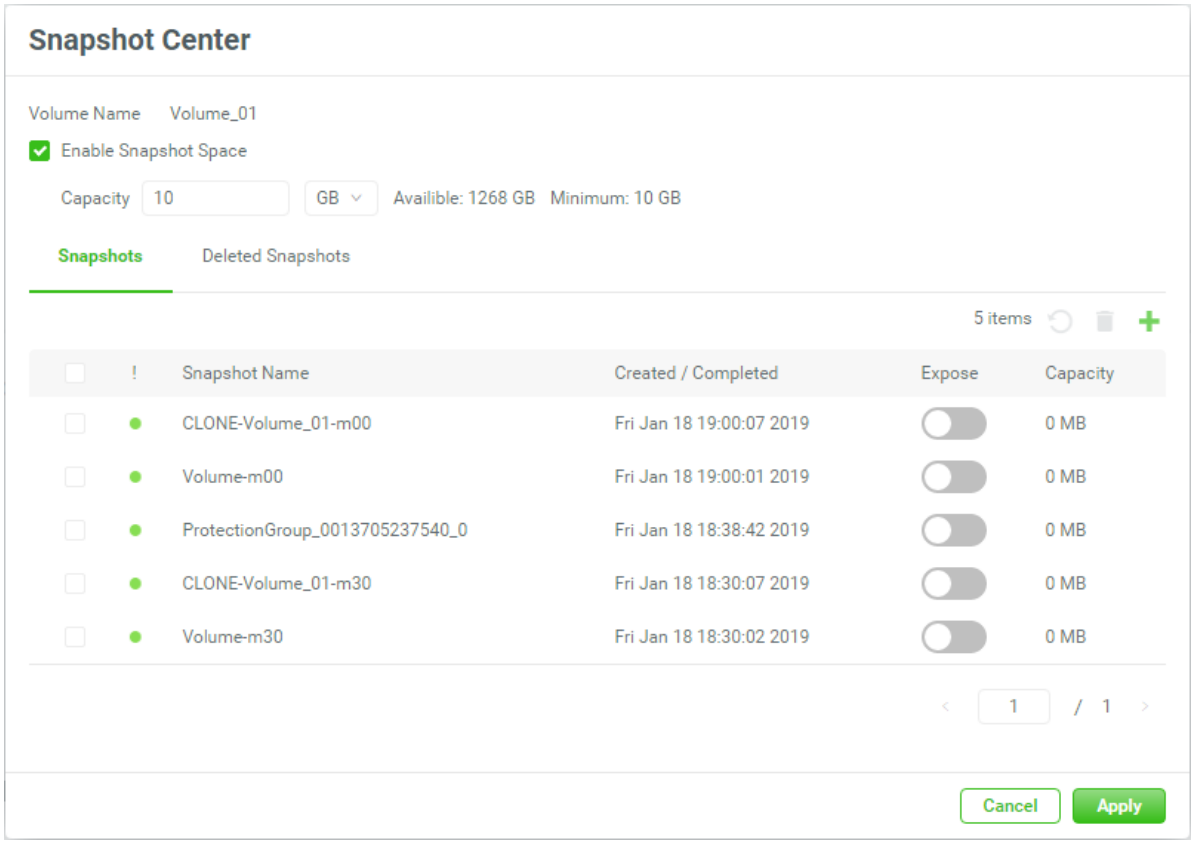


Figure 7-31 Snapshot Center

Snapshot Space

1. Check the **Enable Snapshot Space** checkbox and enter a new **Capacity** number which is reserved for the snapshot space.

TIP:
The recommended minimum capacity is set to 20% of the volume. Volumes in the thin provisioning pool will automatically reserve 20% of the capacity for the snapshot space. However, volumes in the thick provisioning pool are not preserved. You have to enable the snapshot space manually.

There are two tabs. One is the **Snapshots** tab to display all volume snapshots; the other is the **Deleted Snapshots** tab of the snapshot recycle bin. The options are available in the **Snapshots** tab.

Take a Snapshot

Here is an example to take a snapshot.

1. Click the + icon in the **Snapshots** tab to take a snapshot.

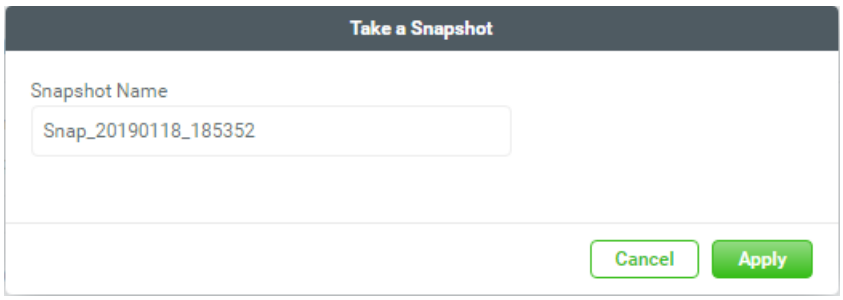


Figure 7-32 Take a Snapshot

2. The recommended **Snapshot Name** is provided. Enter a new **Snapshot Name** if necessary. The maximum length of the snapshot name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
3. Click the **Apply** button to take a snapshot.

TIP:
If it failed to take a snapshot, you have to **Enable Snapshot Space** first in the **Snapshot Center**.

Delete the Snapshot

1. In the **Snapshots** tab, check the snapshot checkbox which you want to delete.
2. Click the icon, and then pop up a confirm dialog box.
3. Click the **Delete** button to confirm to delete the snapshot.

Rollback the Snapshot

1. In the **Snapshots** tab, check the snapshot checkbox which you want to rollback.
2. Click the icon, and then pop up a confirm dialog box.
3. Click the **Apply** button to confirm to rollback the snapshot to the volume.

CAUTION:
Before executing rollback, it is better that the disk is unmounted on the host computer for flushing data from cache.

When a snapshot has been rolled-back, the related snapshots which are earlier than it will also be removed. But the rest snapshots will be kept after rollback.

Expose the Snapshot

1. In the **Snapshots** tab, click the switch to in the **Expose** to expose the snapshot volume.
2. The exposed snapshot is mapped a LUN automatically.

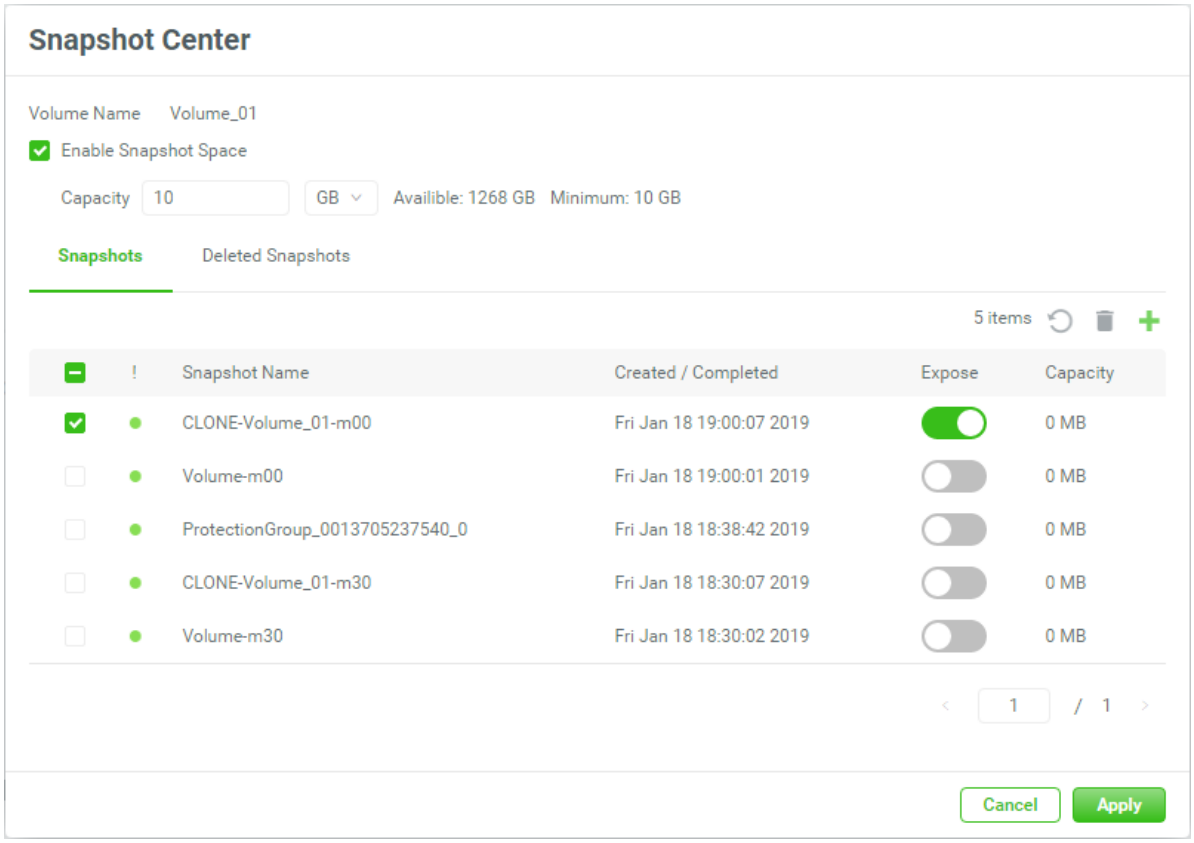


Figure 7-33 Expose the Snapshot

Unexpose the Snapshot

1. Click the switch to in the **Expose** to unexpose.

Click the **Deleted Snapshots** tab. It's a recycle bin of the deleted snapshots. The options are available in the **Deleted Snapshots** tab.

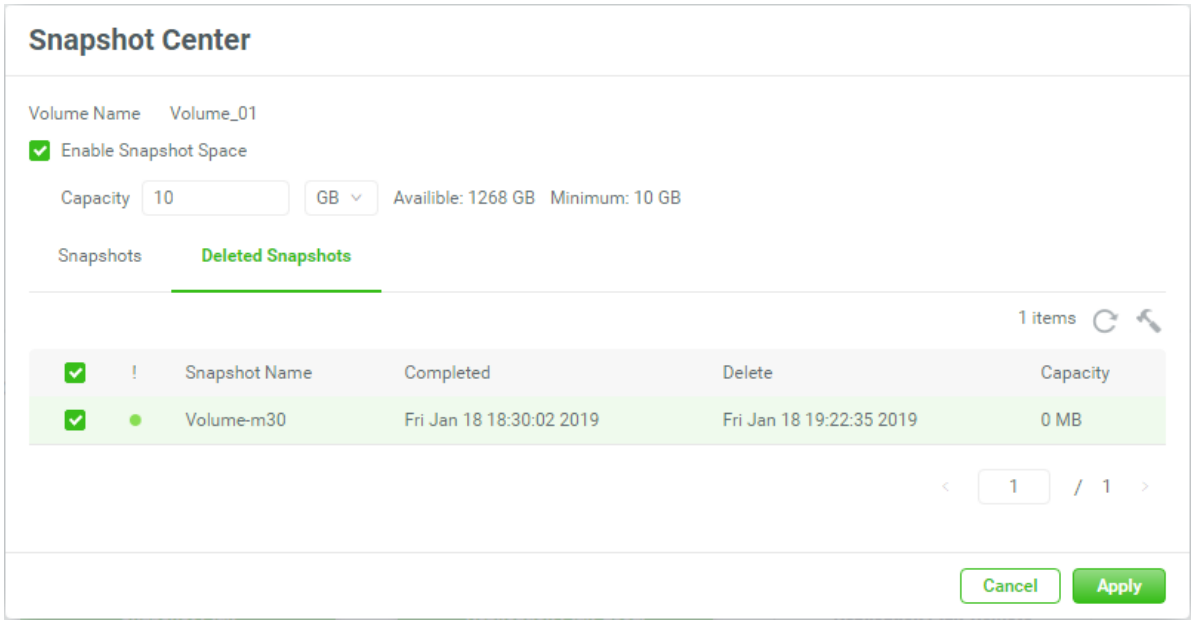


Figure 7-34 Deleted Snapshots

Rescue the Snapshot

1. In the **Deleted Snapshots** tab, check the snapshot checkbox which you want to rescue.
2. Click the icon, and then pop a confirm dialog box.
3. Click the **Rescue** button to rescue the deleted snapshot and it will be back to the snapshot volumes.

Destroy the Snapshot

1. In the **Deleted Snapshots** tab, check the snapshot checkbox which you want to destroy.
2. Click the icon, and then pop a confirm dialog box.
3. Click the **Destroy** button to destroy the deleted snapshot..

CAUTION:
If a snapshot has been deleted, the other snapshots which are earlier than it will also be deleted. The space occupied by these snapshots will be released after deleting.

7.2.4. List and Configure Replication Plan-Local

A protection group with replication plan-local is shown here.

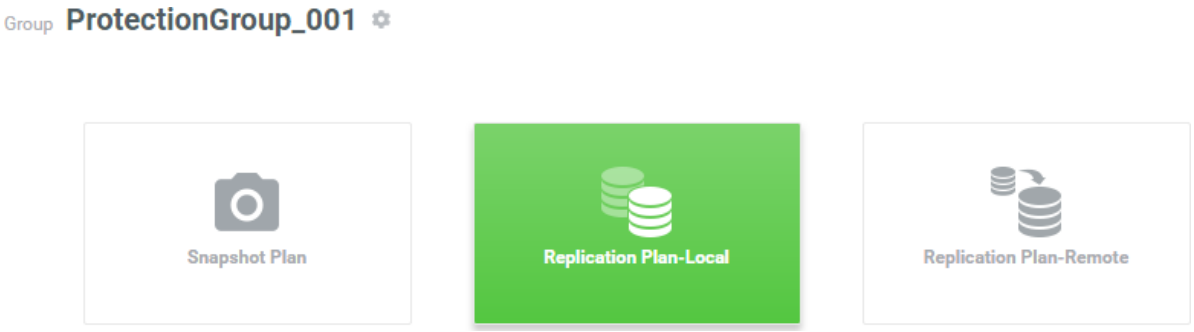


Figure 7-35 Protection Group with Replication Plan-Local

The green box enables the service. The above figure enables the **Replication Plan-Local** service. Clicking it will display the current snapshot plan.

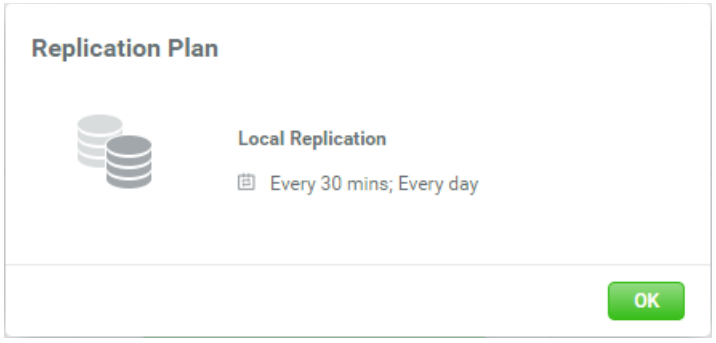


Figure 7-36 Replication Plan-Local

Click the ⚙ icon beside the protection group name to list the drop down options.

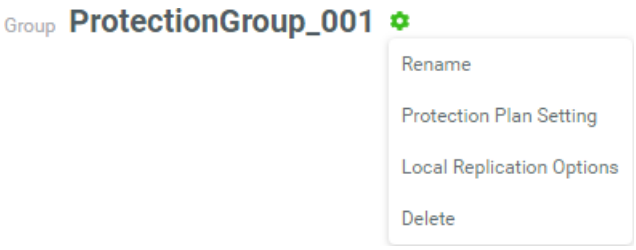


Figure 7-37 Protection Group Options with Replication Plan-Local

These options are available in the protection group.

Rename, Protection Plan Setting, Delete

About the Rename, Protection Plan Setting, and Delete functions, please refer to the chapter 7.2.2, List and Configure Snapshot Plan section for more details.

Local Replication Options

1. Click the **Local Replication Options** option to change the local replication settings.

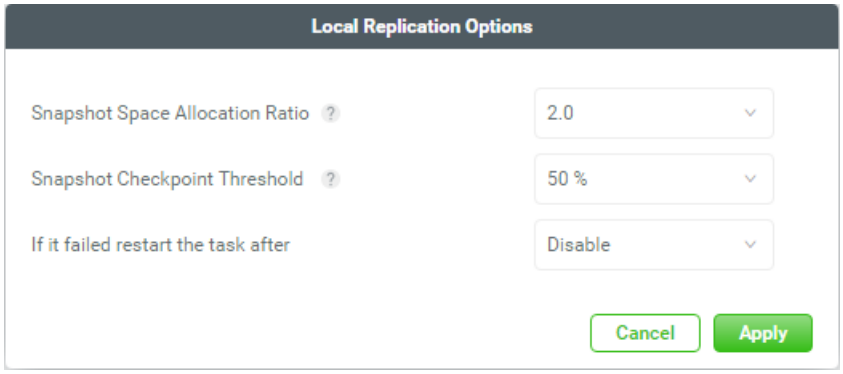


Figure 7-38 Local Replication Options

Three options are described in the following.

- **Snapshot Space Allocation Ratio:** This setting is the ratio of the source volume and snapshot space. If the ratio is set to 2, when there is no snapshot space assigned for the volume, the system will automatically reserve a free pool space to set as the snapshot space with twice capacity of the volume. The options are 0.5 ~ 3.
- **Snapshot Checkpoint Threshold:** The setting will be effective after enabling schedule clone. The threshold will monitor the usage amount of the snapshot space. When the used snapshot space achieves the threshold, system will take a snapshot and start clone process automatically. The purpose of threshold could prevent the incremental copy failure immediately when running out of the snapshot space. For example, the default threshold is 50%. The system will check the snapshot space every hour. When the snapshot space is used over 50%, the system will start the clone task automatically. And then continue monitoring the snapshot space. When the rest snapshot space has been used 50%, in other words, the total snapshot space has been used 75%, the system will start the clone task again.

- **If it failed to restart the task:** The setting will be effective after enabling a scheduled clone. When running out of snapshot space, the volume clone process will be stopped because there is no more available snapshot space. If this option is checked, the system will clear the snapshots of the clone in order to release snapshot space automatically, and the clone task will be restarted after an hour. This task will start a full copy.

2. Click the **Apply** button to change.

CAUTION:
The default snapshot space allocated by the system is two times the capacity of the source volume. That is the best value of our suggestion. If user sets snapshot space manually and lowers than the default value, understand that if the snapshot space is not enough, the clone task will fail.

At the **Protection Volume** pane, click the **Replication Task** tab to list all replication tasks.

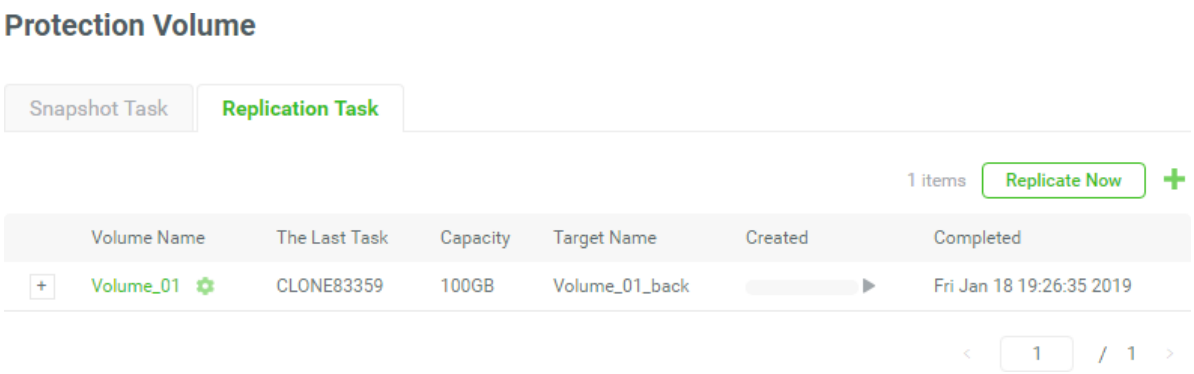


Figure 7-39 List Replication Tasks

The options are available in this tab.

Add Volumes

Here is an example to add volumes in the protection group.

1. Click the ✚ icon in the **Replication Task** tab to pop up a window.

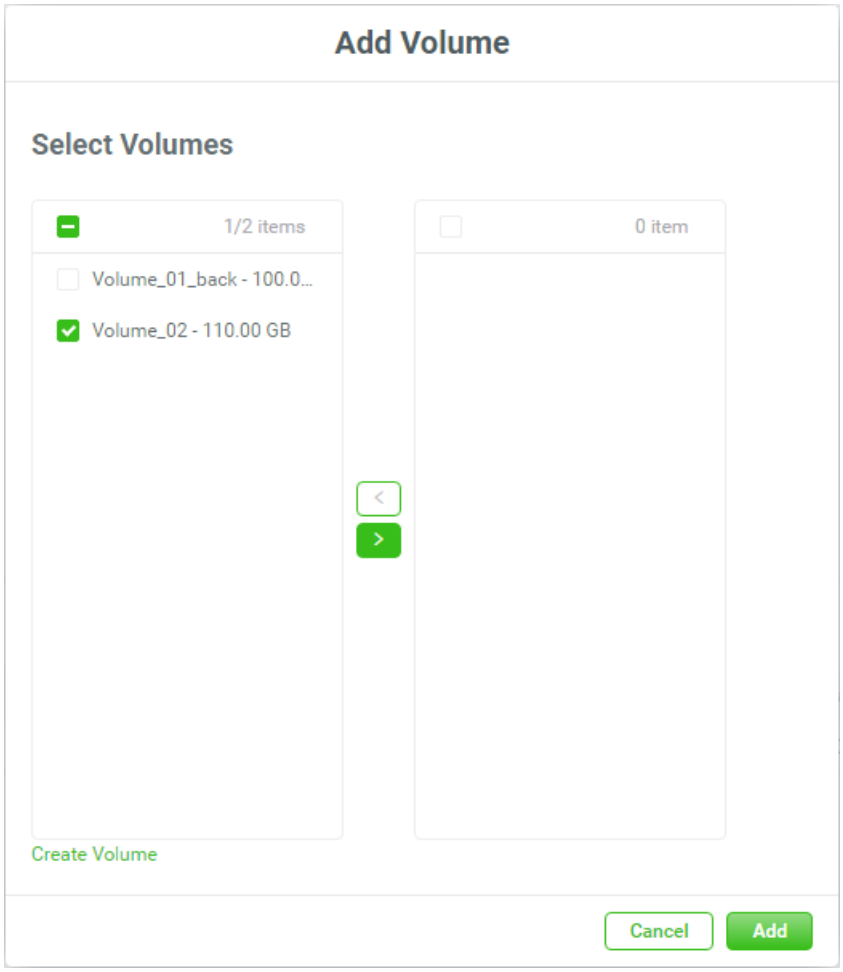


Figure 7-40 Add Volumes to the Protection Group

2. The **Select Volumes** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective.
3. Select volumes and click the > button or the < button to make them effective or not.
4. Click the **Add** button to add.

Replicate Now

1. Click the **Replicate Now** button to replicate all volumes immediately.

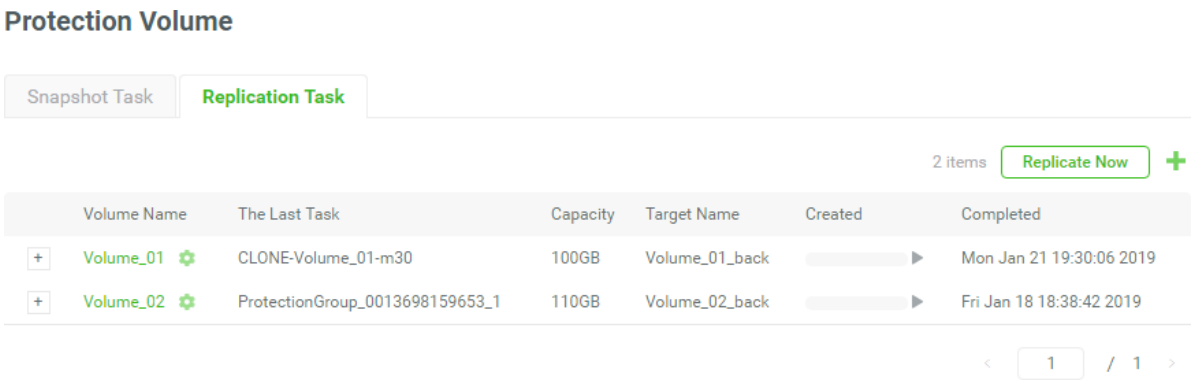


Figure 7-41 Replication Now

2. The volume is added into the replication task. And the snapshot is taken and displayed at **The Last Snapshot** field.

Start Task

1. Select a volume, and then click the ▶ icon to replicate the volume immediately.
2. The progress bar displays the current status.

Stop Task

1. Click the ○ icon of the volume to stop the replication task.

TIP:
The **Replicate Now** button will replicate all volumes in the protection group. And click the ▶ icon of the volume will replicate the volume only.

Click the ⚙ icon beside the volume name to list the drop down options.

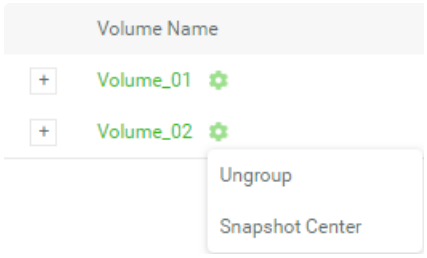


Figure 7-42 Replication Task Options

These options are available in the **Replication Task** tab.

Ungroup

1. Click the **Ungroup** option to remove the volume from the protection group.
2. Click the **Ungroup** button to confirm.

Snapshot Center

About the snapshot center, please refer to the chapter 7.2.3, Snapshot Center section for more details.

7.2.5. List and Configure Replication Plan-Remote

A protection group with replication plan-remote is shown here.

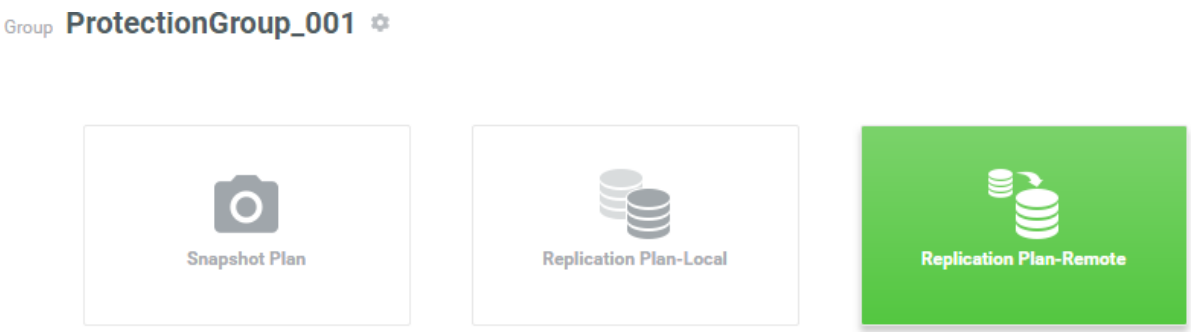


Figure 7-43 Protection Group with Replication Plan-Remote

The green box enables the service. The above figure enables the **Replication Plan-Remote** service. Clicking it will display the current snapshot plan.

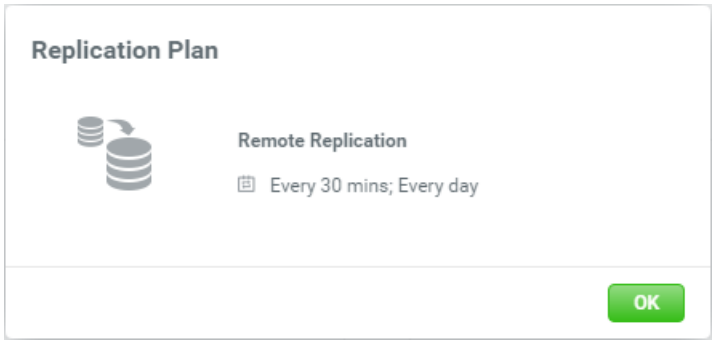


Figure 7-44 Replication Plan-Remote

Click the icon beside the protection group name to list the drop down options.

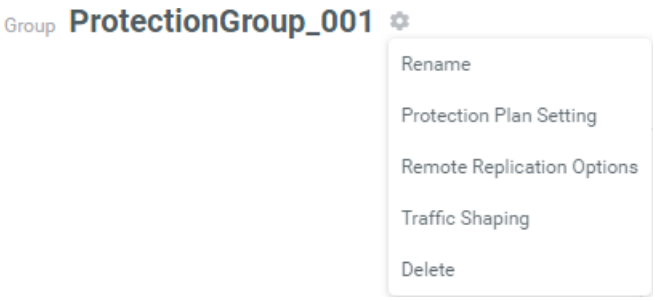


Figure 7-45 Protection Group Options with Replication Plan-Remote

These options are available in the protection group.

Rename, Protection Plan Setting, Delete

About the Rename, Protection Plan Setting, and Delete functions, please refer to the chapter 7.2.2, List and Configure Snapshot Plan section for more details.

Remote Replication Options

1. Click the **Remote Replication Options** option to change the remote replication settings.

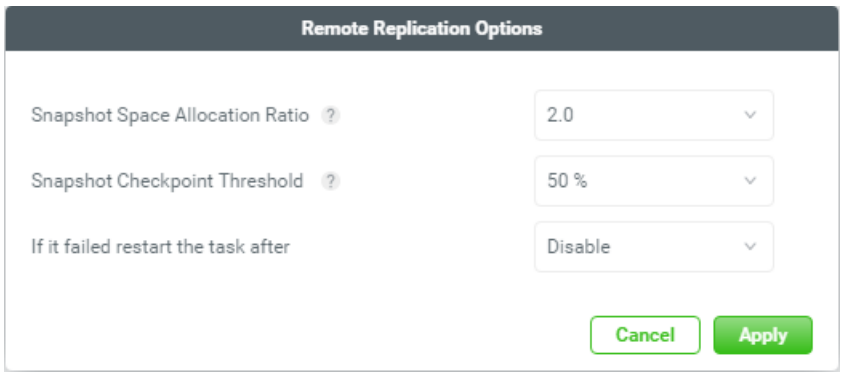


Figure 7-46 Remote Replication Options

Three options are described in the following.

- **Snapshot Space Allocation Ratio:** This setting is the ratio of the source volume and snapshot space. If the ratio is set to 2, when there is no snapshot space assigned for the volume, the system will automatically reserve a free pool space to set as the snapshot space with twice capacity of the volume. The options are 0.5 ~ 3.

- **Snapshot Checkpoint Threshold:** The setting will be effective after enabling schedule replication. The threshold will monitor the usage amount of the snapshot space. When the used snapshot space achieves the threshold, system will take a snapshot and start replication process automatically. The purpose of threshold could prevent the incremental copy failure immediately when running out of the snapshot space. For example, the default threshold is 50%. The system will check the snapshot space every hour. When the snapshot space is used over 50%, the system will start replication task automatically. And then continue monitoring the snapshot space. When the rest snapshot space has been used 50%, in other words, the total snapshot space has been used 75%, the system will start replication task again.
- **If it failed restart the task:** The setting will be effective after enabling schedule replication. When running out of snapshot space, the volume replication process will be stopped because there is no more available snapshot space. If this option is checked, the system will clear the snapshots of replication in order to release snapshot space automatically, and the replication task will be restarted after an hour. This task will start a full copy.

2. Click the **Apply** button to change.

CAUTION:
The default snapshot space allocated by the system is two times the capacity of source volume. That is the best value of our suggestion. If user sets snapshot space by manually and lower than the default value, user should take the risk if the snapshot space is not enough and the replication task will fail.

Traffic Shaping

1. Click the **Traffic Shaping** option to edit the traffic shaping configurations.

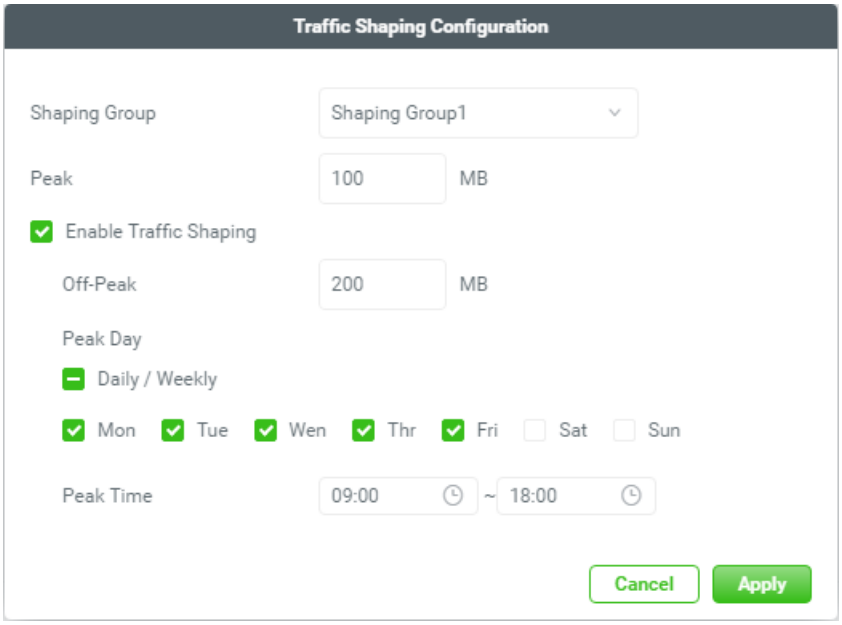


Figure 7-47 traffic shaping configurations

2. Select a **Shaping Group** to be modified, enter a maximum throughput during **Peak** hours. Check the **Enable Traffic Shaping** option if necessary, and then enter a maximum throughput during **Off-Peak** hours and define the **Peak Day**.
3. Click the **Apply** button to continue.

At the **Protection Volume** pane, click the **Replication Task** tab to list all replication tasks.

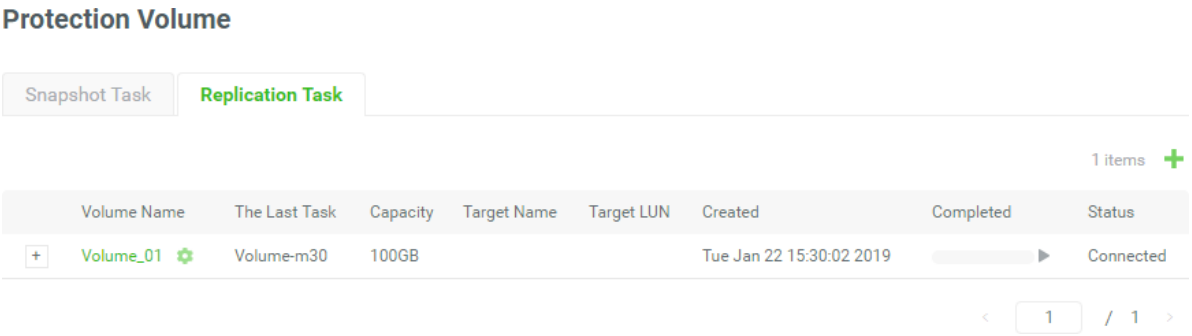


Figure 7-48 List Replication Tasks

The options are available in this tab.

Add Volumes

Here is an example to add volumes in the protection group.

1. Click the + icon in the **Replication Task** tab to pop up a window.

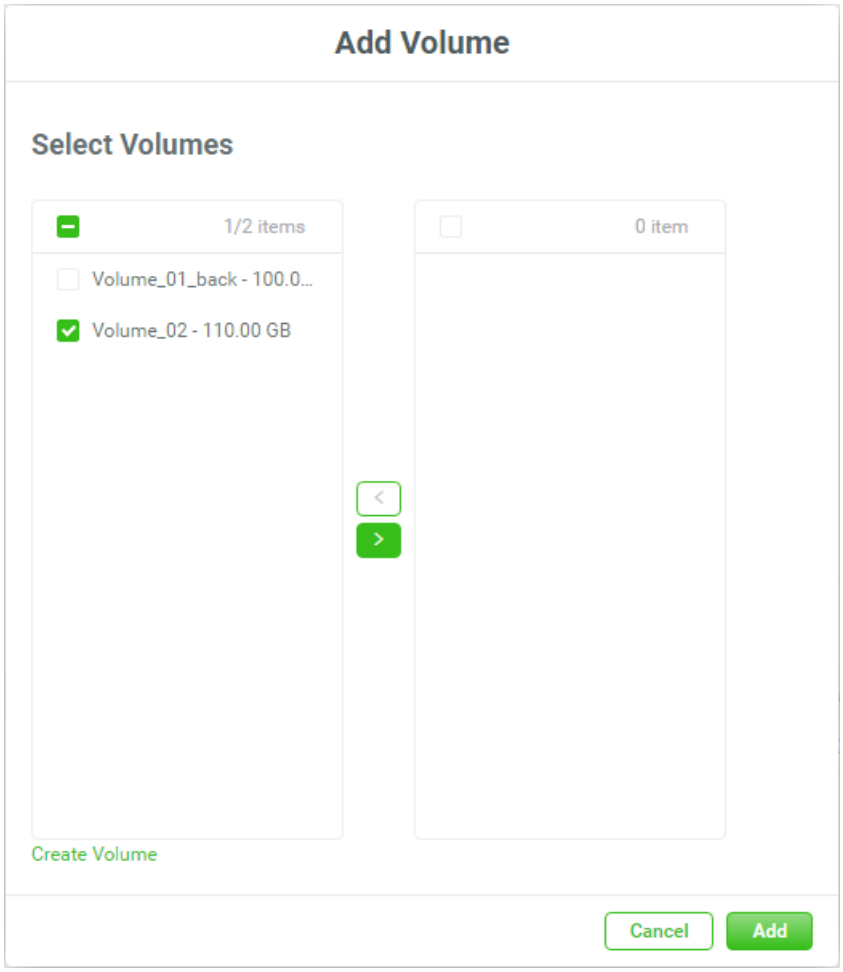


Figure 7-49 Add Volumes to the Protection Group

2. The **Select Volumes** boxes are divided into two sides. The left side is an ineffective list, and the right side is effective.
3. Select volumes and click the > button or the < button to make them effective or not.
4. Click the **Add** button to add.

Start Task

1. Select a volume, and then click the ▶ icon to replicate the volume immediately.
2. The progress bar displays the current status.

Stop Task

1. Click the icon of the volume to stop the replication task.

Click the icon beside the volume name to list the drop down options.

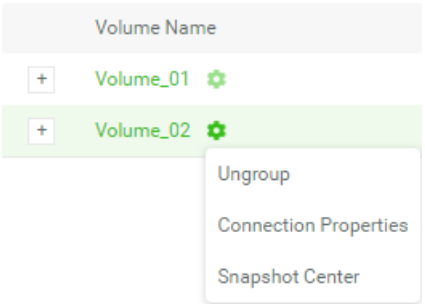


Figure 7-50 Replication Task Options

These options are available in the **Replication Task** tab.

Ungroup

1. Click the **Ungroup** option to remove the volume from the protection group.
2. Click the **Ungroup** button to confirm.

Connection Properties

1. Click the **Connection Properties** option to enable multipath and add connections.

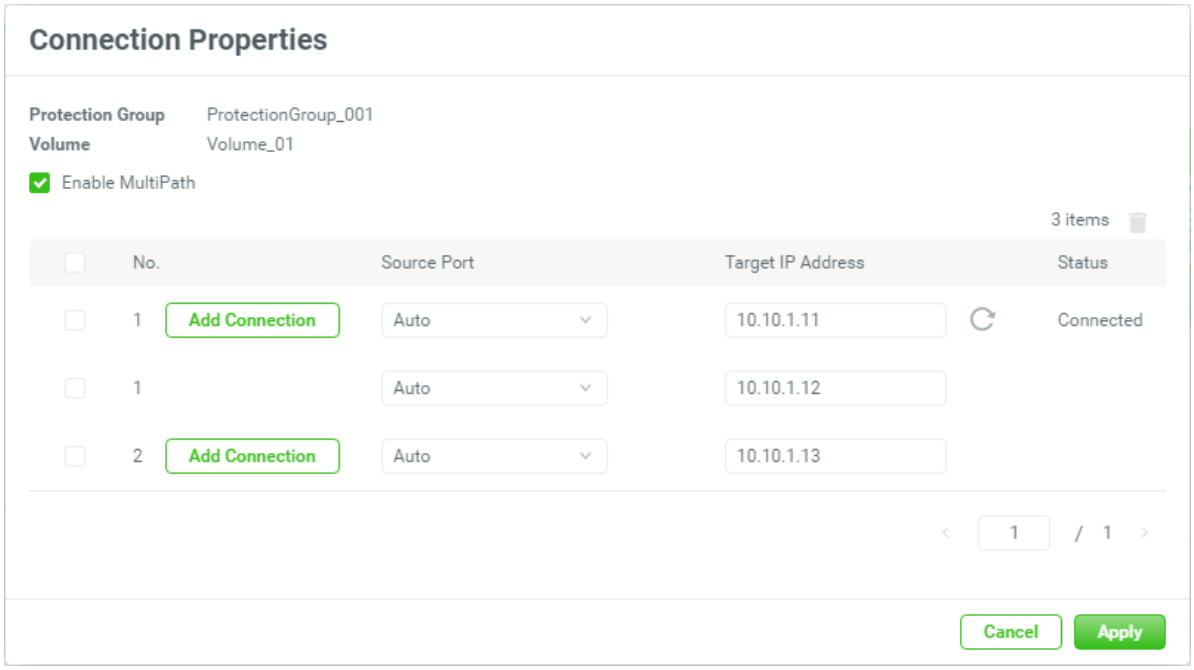


Figure 7-51 Connection Properties

2. Check the **Enable MultiPath** option if necessary, and then select the **Source Port** and enter a **Target IP Address**.
3. Or click the **Add Connection** button to add another connection. Select the **Source Port** and enter a **Target IP Address**.
4. If the connection is not stable, click the icon to reconnect the connection.
5. Click the **Apply** button to take effect.

Snapshot Center

About the snapshot center, please refer to the chapter 7.2.3, Snapshot Center section for more details.

7.2.6. Switch Local to Remote

Here is an example of switching a replication plan-local to replication plan-remote.

1. Click the **Protection Plan Setting** option to configure the switch local to remote.

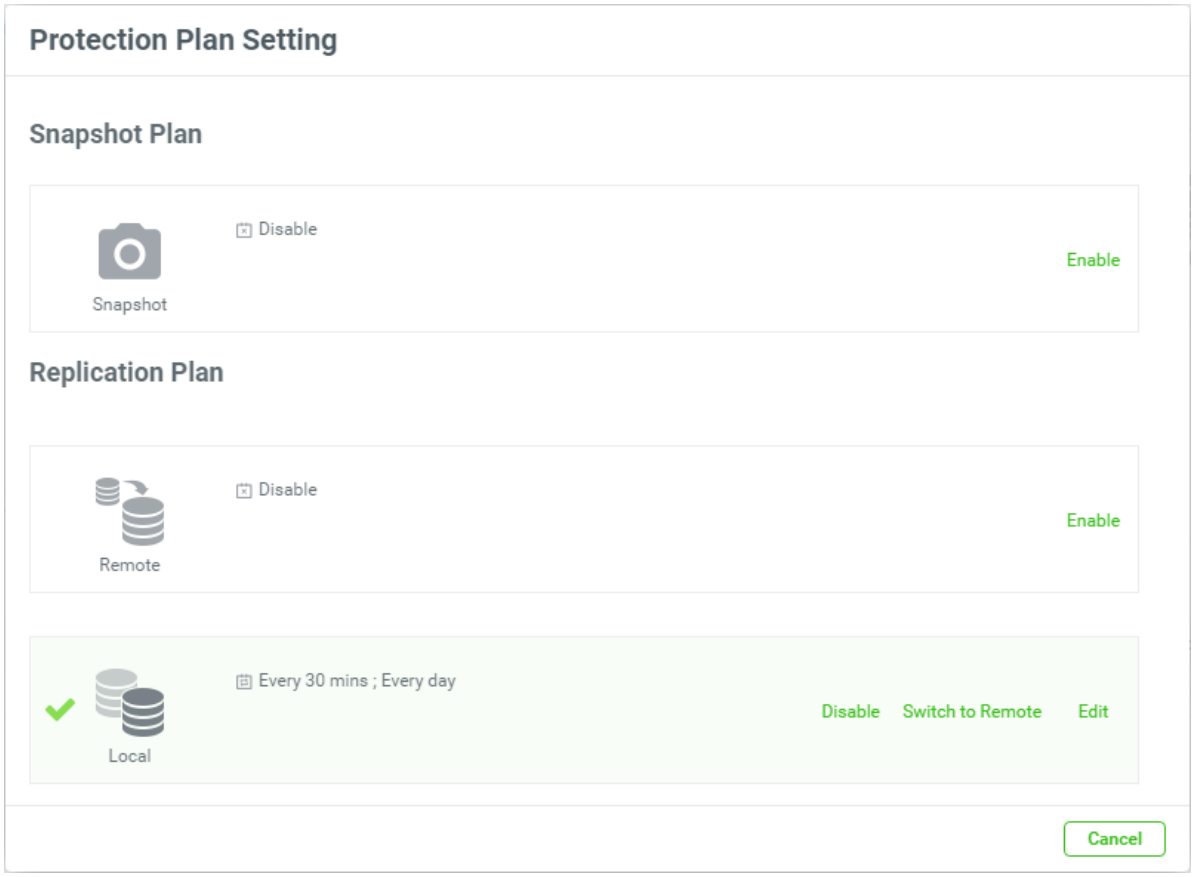


Figure 7-52 Switch to Remote

2. Click the **Switch to Remote** text to configure the replication plan.

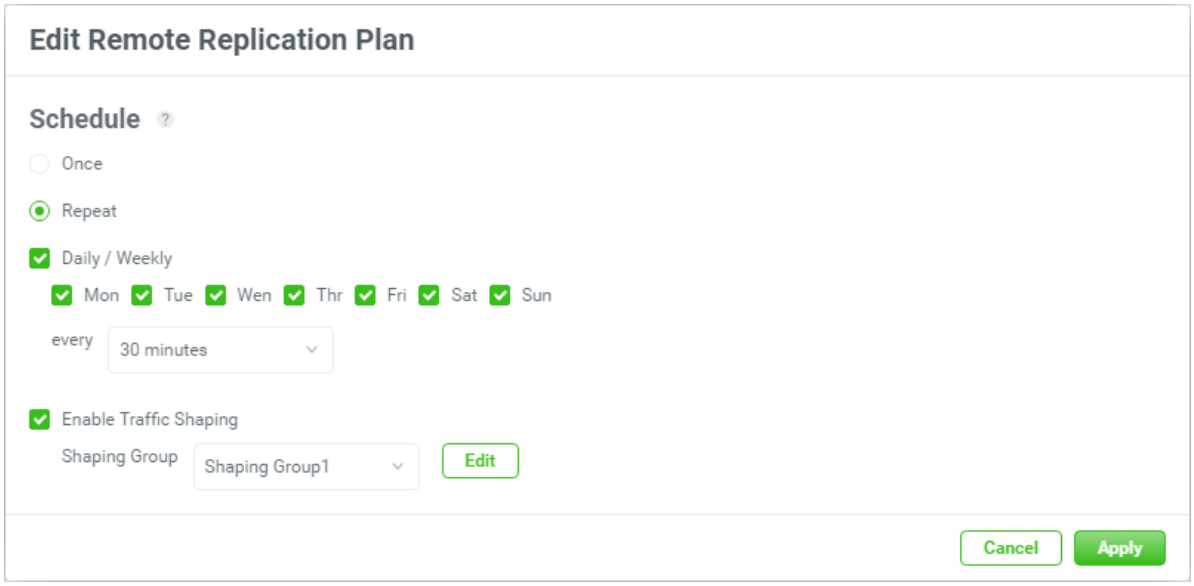


Figure 7-53 Edit Remote Replication Plan

3. Select the **Once** option to execute the plan once. Or select the **Repeat** option to repeat the plan, and then check the repeat frequency.
4. Check the **Enable Traffic Shaping** option if necessary and then click the **Edit** button to edit the shaping group.
5. Click the **Apply** button to continue.
6. Move all disk drives of the source pool to the target array.

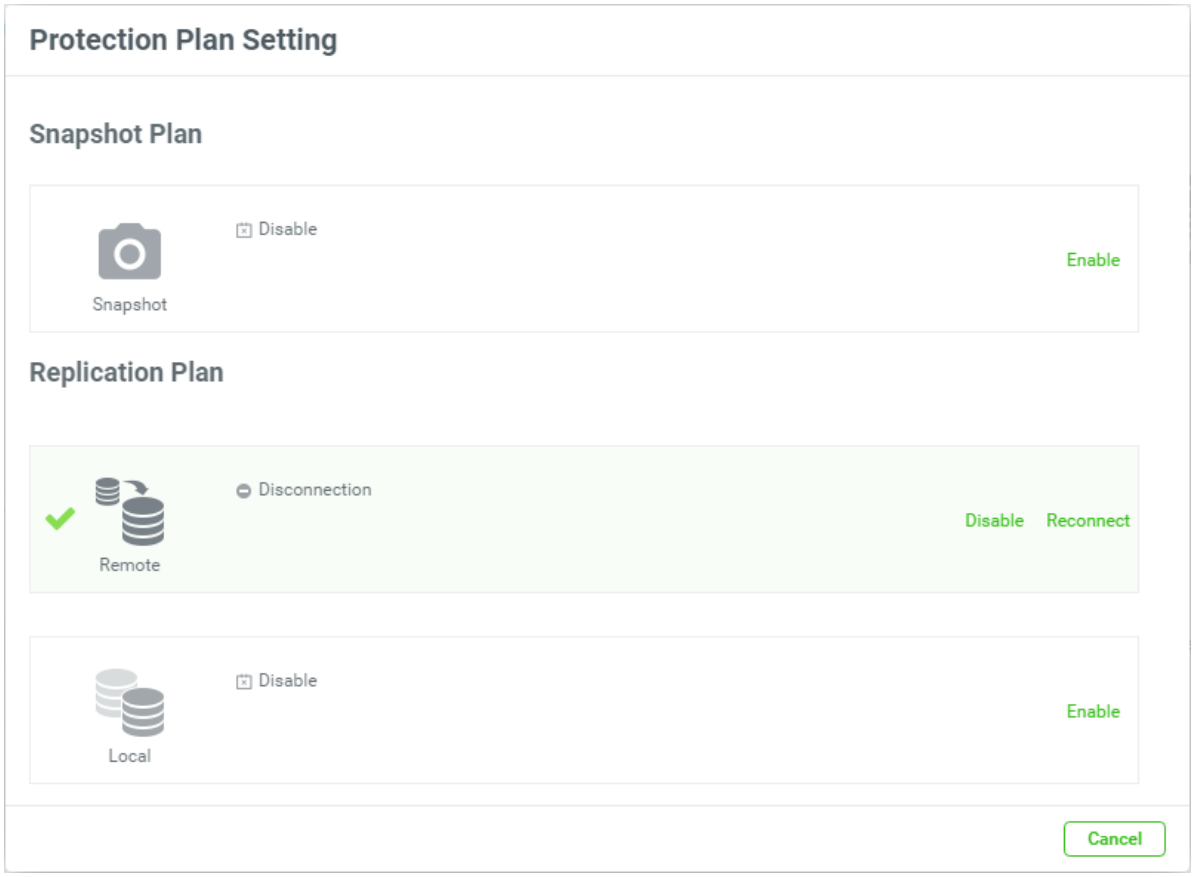


Figure 7-54 Remote Reconnect

7. Click the **Reconnect** text to reconnect.
8. Done.

8. Analysis Tab

The **Analysis** tab displays historical array data, including I/O performance trends across all volumes, storage capacity, and consumption on the array.

8.1. Analysis Features

XEVO provides QReport to help you analysis the status of your business usage. The system generates performance and capacity analytics as far back as 1 year. It eases the effort of IT managers by exporting a report to analyze the storage usage, and allows IT generalists to make a better resource arrangement faster than ever and easier.

Figure 8-1 Analysis Features

8.2. Array Analysis

Select the **Analysis** tab to view performance and capacity changes of the array.

Figure 8-2 Analysis Tab

8.2.1. Performance Monitoring

Select the **Performance** pane to monitor performance.

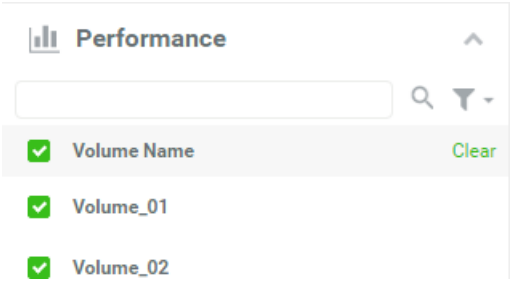


Figure 8-3 List All Volumes in the Performance Pane

All volumes are listed. You can select one or more volumes to view performance.

Figure 8-4 Performance Graph

The performance graph displays a series of rolling graphs consisting of real-time performance. The incoming data appears along the right side of each graph as older numbers drop off the left side. The curve in each graph consists of a series of individual data points.

The **I/O type** specified in the bottom-left corner of the performance graph pane determines the information. I/O types include Read, Write, and R & W. The **Zoom** specified in the bottom-right corner determines the performance interval. There is a time from 1 hour to 1 year.

INFORMATION:
XEVO maintains a rolling one-year history of data. The granularity of the historical data increases with age. Older data points are spaced further apart in time than the nearest data points.

Single Point Report

Click any part of the graph to display values for a specific point in time.

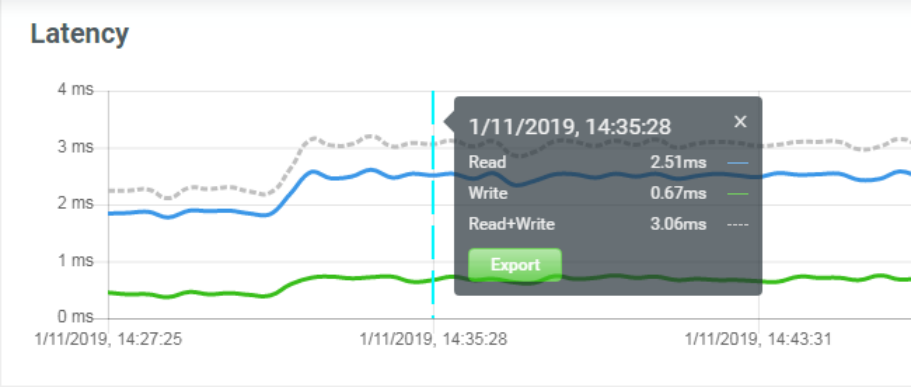


Figure 8-5 Single Point Report

Click the **Export** button to pop-up a window to display more details. Or click the **x** icon to unselect.

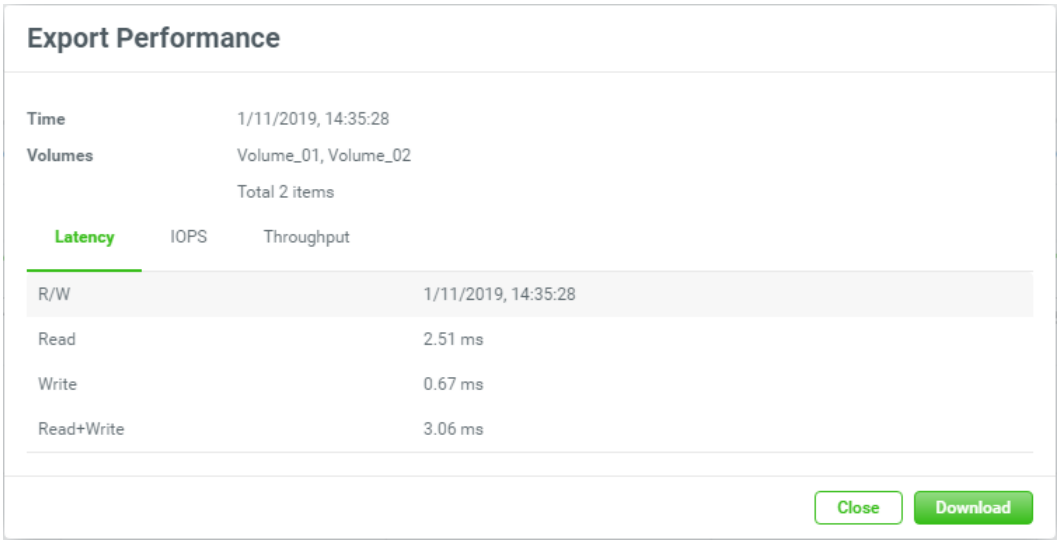


Figure 8-6 Export Performance of Single Point

Three tabs can be selected to observe **Latency**, **IOPS**, and **Throughput**. Click the **Download** button to download the performance report to a file. Or click the **Clear** button to close the window.

Two-point Interval Report

Click any two points of the graph to display values for two specific points in time.

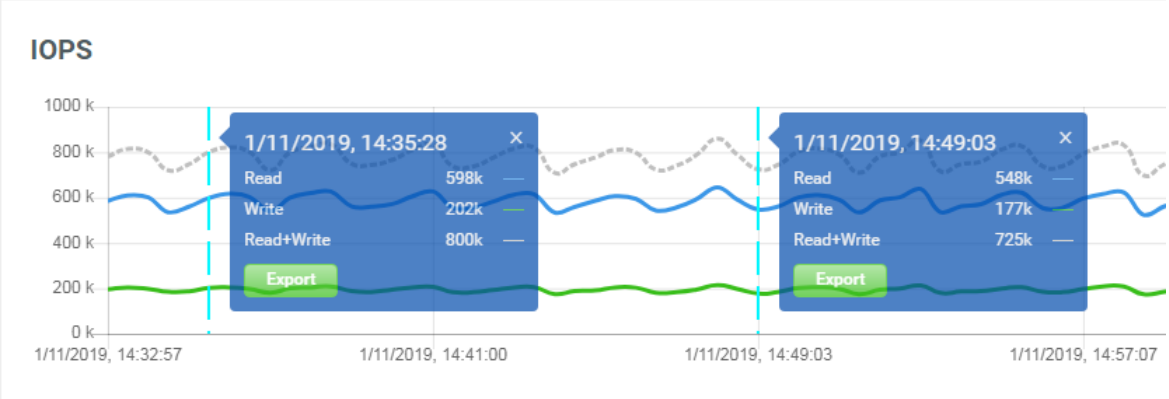


Figure 8-7 Two Points Report

Click the **Export** button to pop-up a window and display more details. Or click the **x** icon to unselect.

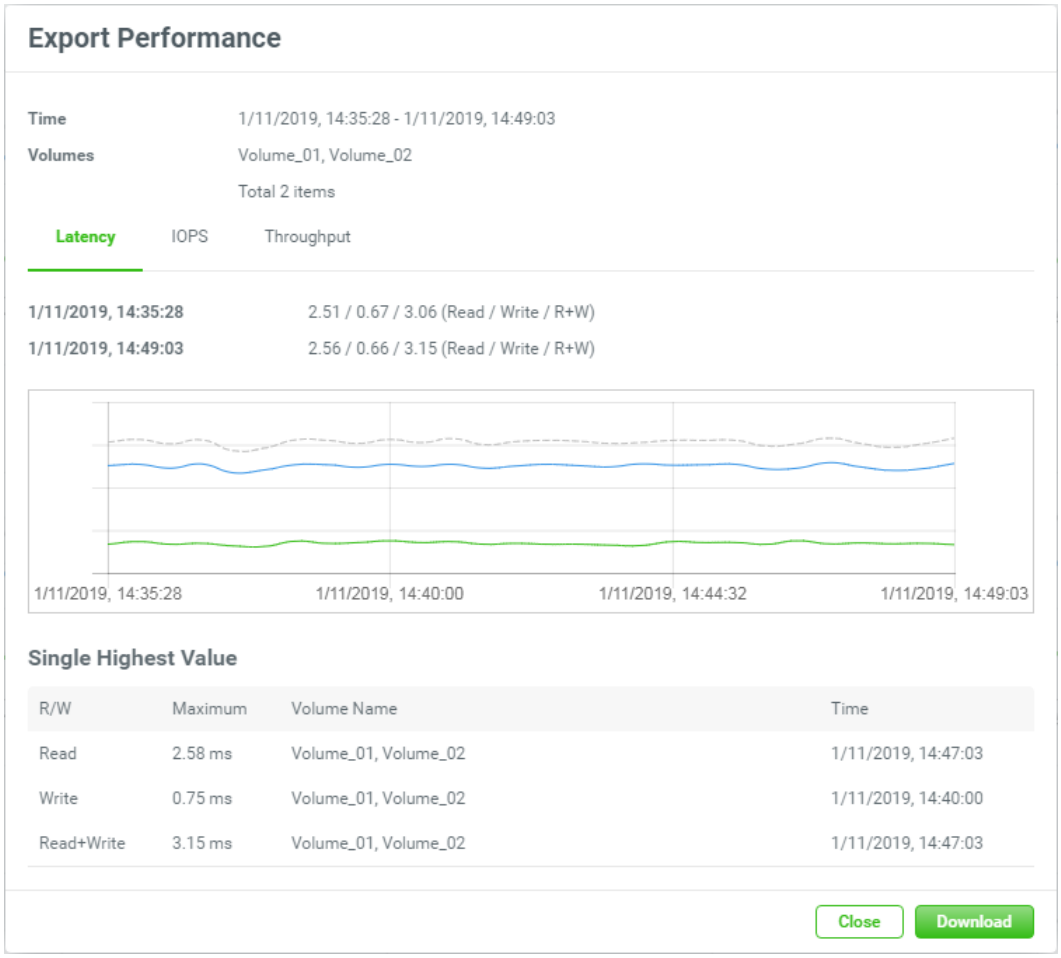


Figure 8-8 Export Performance of Two-point Interval

The same, three tabs can be selected to observe **Latency**, **IOPS**, and **Throughput**. Click the **Download** button to download the performance report to a file. Or click the **Clear** button to close the window.

8.2.2. Capacity Analysis

Select the **Capacity** pane to monitor array capacity.

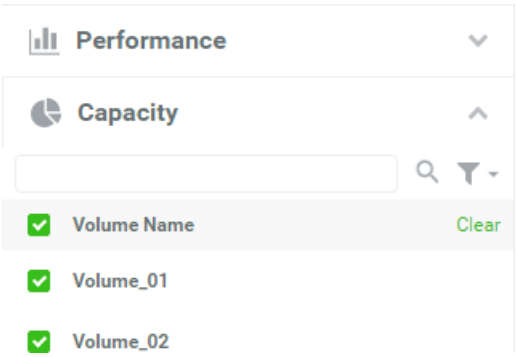


Figure 8-9 List All Volumes in the Capacity Pane

All volumes are listed. You can select one or more volumes to view capacity changes.

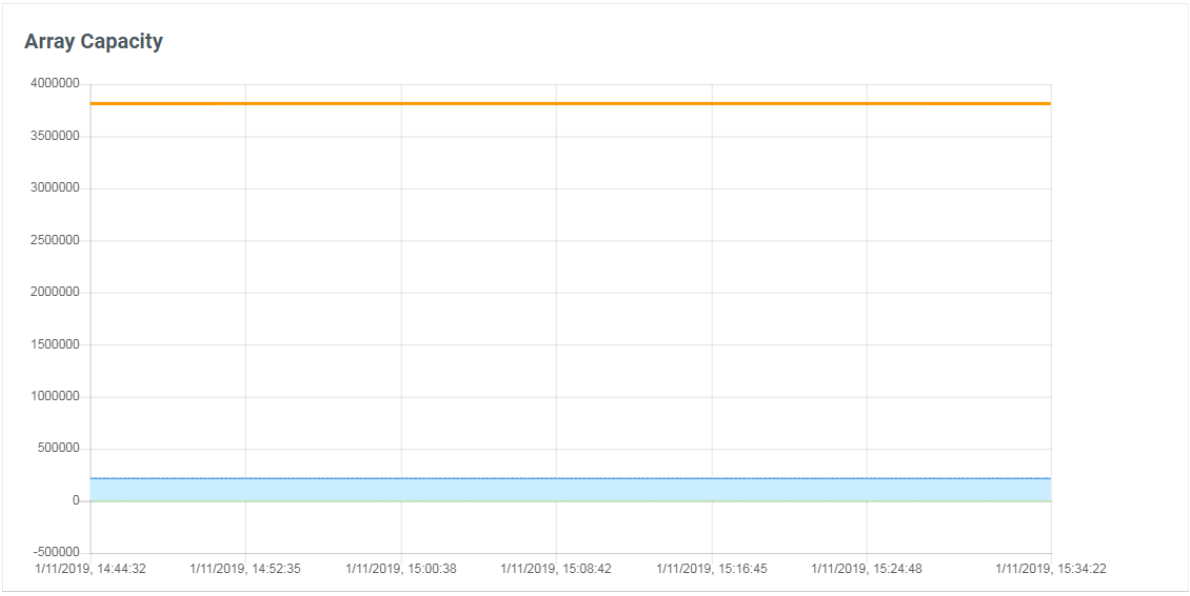


Figure 8-10 Array Capacity Graph

The capacity graph displays a series of rolling graphs consisting of real-time capacity.

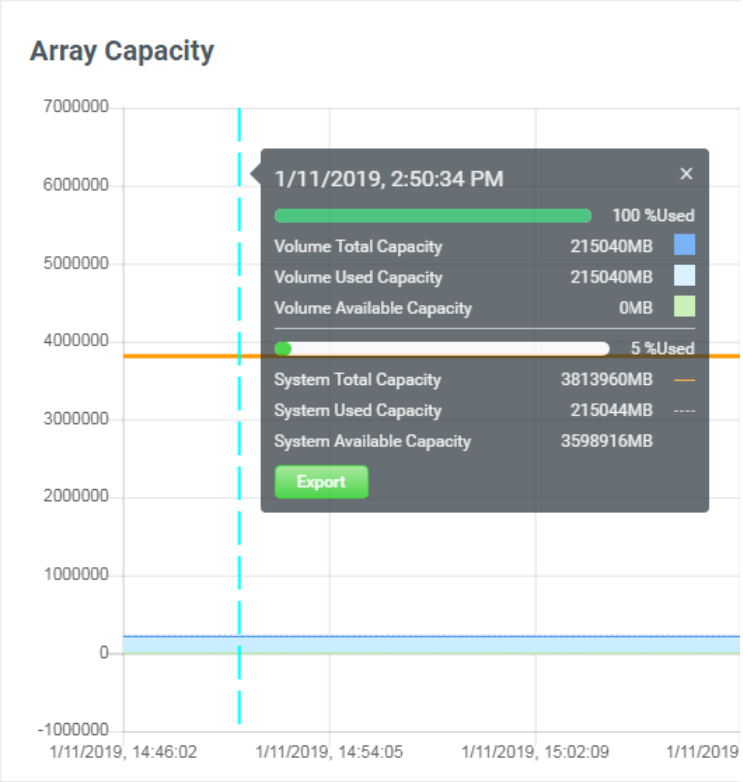


Figure 8-11 Array Capacity Report

Click the **Export** button to pop-up a window and display more details. Or click the **x** icon to unselect.

9. System Tab

The **System** tab manages the system settings. It displays array health status, and system information; configures general system settings, management and data ports; maintains system firmware, disks; rescues system setting or volume information. This chapter describes the details of system operations and examples.

9.1. Arrays Information

Select the **System** tab and the **Arrays** subtab to displays array health status.

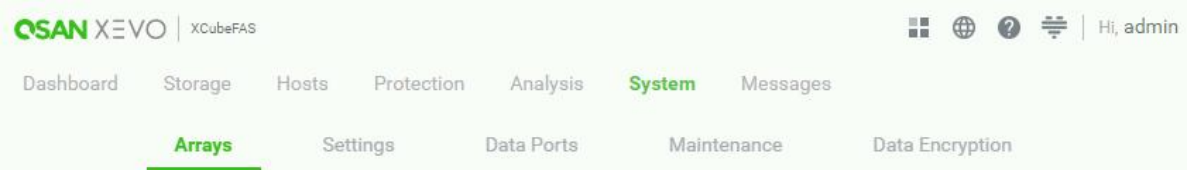


Figure 9-1 Arrays Subtab in the System Tab

9.1.1. List Arrays

All arrays including head and expansion units are listed in the left pane. You can click one of them to display the details.

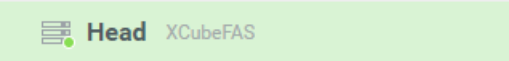


Figure 9-2 List All Arrays

There are front and rear pictures in the right pane. You can move your mouse over the system components and watch the status of disks, controllers, management ports, data ports, fan modules, power supply modules, and cache to flash modules.

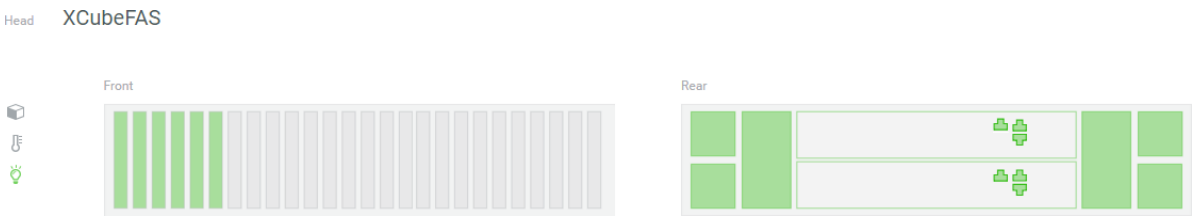


Figure 9-3 Front and Rear Pictures of the Array

9.1.2. Array Information

There are three icons at the left side. They are array information, temperatures, and identification.

Array Information

Click the first icon to display the array information.

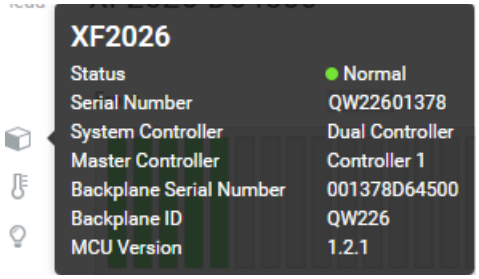


Figure 9-4 Array Information

This table shows the array descriptions.

Table 9-1 Array Descriptions

Row Name	Description
Model Name	The model name of the array.
Status	The status of array: • Green Color / Normal: Dual controllers and expansion units are in normal stage. • Orange Color / Abnormal: The configurations of two controllers are different, including the CPU model, memory capacity, host cards, and controller firmware version. Please check the hardware configurations of two controllers or execute firmware

	synchronization. • Red Color / Warning: In dual controller mode, one controller or one of expansion unit fails or they have been plugged out. Please replace or insert a good controller.
Serial Number	The seiral number of the array.
System Controller	The status of system availability: • Dual Controller, Active/Active: Dual controllers and expansion units are in normal stage. • Dual Controller, Degraded: In dual controller mode, one controller or one of expansion unit fails or they have been plugged out. Please replace or insert a good controller. • Dual Controller, Lockdown: In dual controller mode, the configurations of two controllers are different, including the memory capacity, host cards, and controller firmware version. Please check the hardware configurations of two controllers or execute firmware synchronization.
Master Controller	Current master controller.
Backplane Serial Number	The backplane serial number of the array.
Backplane ID	The backplane ID of the array.
MCU Version	The MCU version of the backplane.

Array Temperatures

Click the second icon to display the several temperatures of the array.

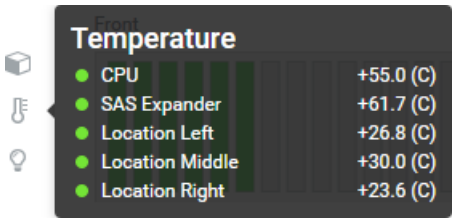


Figure 9-5 Array Temperatures

Array Identification

The UID (Unique Identifier) LEDs help users to easily identify the system location within the rack. Clicking on the third icon will turn on the UID LED control mechanism.

Figure 9-6 System Identification

When the UID LEDs are turn on, they are light blue color, located on the right panel of front view and both controllers of rear view. Click it again to turn off the UID LEDs.

INFORMATION:
For the front and rear view about the UID LEDs, please refer to chapter 2, System Components Overview in the QSAN Hardware Manual XF2026D.

9.1.3. Disk Information

Move your mouse over the disk and the disk information will appear in a popup box.

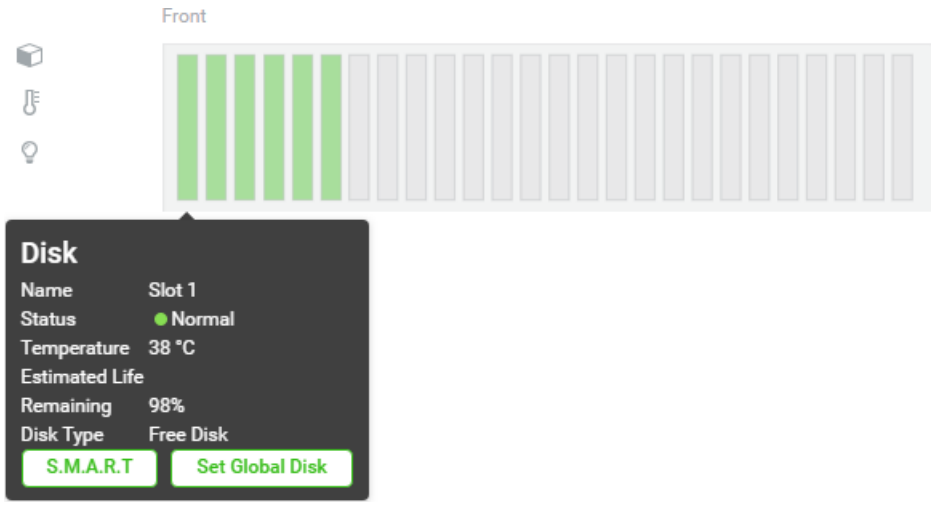


Figure 9-7 Disk Information

This table shows the disk descriptions.

Table 9-2 Disk Descriptions

Row Name	Description
Name	The position of the disk drive.
Status	The status of disk health: • Green Color / Normal: The disk drive is good. • Orange Color / Abnormal: The disk drive has unrecoverable read errors or S.M.A.R.T. error. • Red Color / Warning: The disk drive has failed.
Temperature	The temperature of the disk drive.
Estimated Life Remaining	The life remaining of the disk drive.
Disk Type	The type of the disk drive: • Free Disk: This disk drive is free for use • RAID Disk: This disk drive has been set to a pool. • Global Spare: This disk drive has been set as global spare of whole system.

The options are available in disk information.

S.M.A.R.T.

S.M.A.R.T. (Self-Monitoring Analysis and Reporting Technology) is a diagnostic tool for disk drives to deliver warning of drive failures in advance. It provides users a chance to take actions before a possible drive failure. Click the **S.M.A.R.T.** button to display S.M.A.R.T. information.

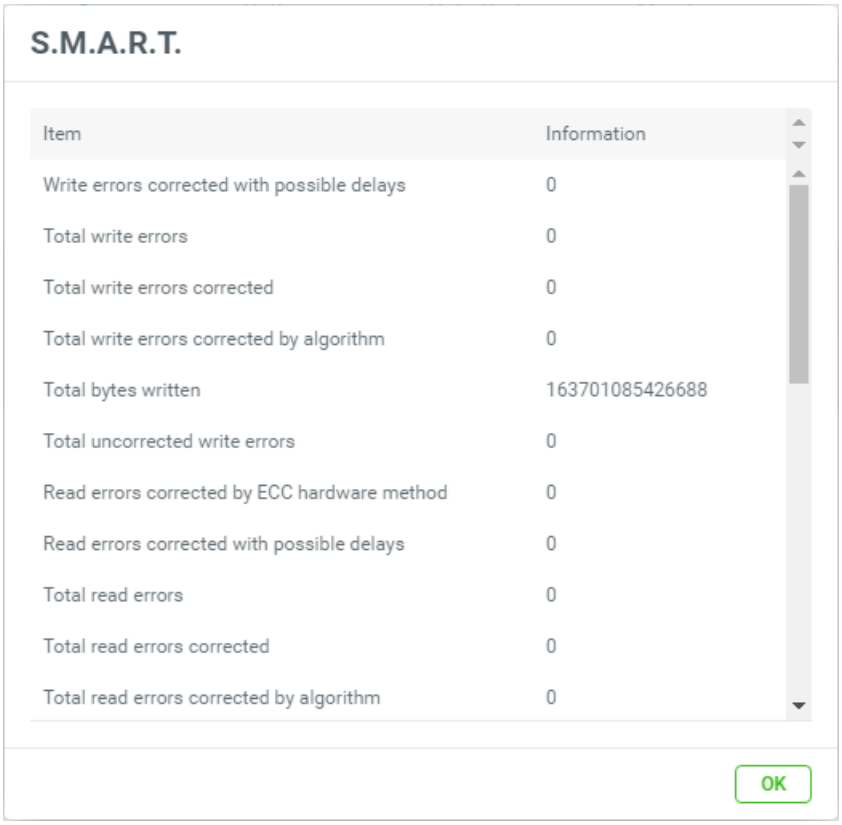


Figure 9-8 S.M.A.R.T. Information

Click the **OK** button to close the window.

Set Global Disk

Click the **Set Global Disk** button appears if the disk drive is free. You can set it as a global spare disk. Click the **Set Global Disk** button to set it up.

Set Free Disk

Click the **Set Free Disk** button appears if the disk drive is a global spare disk. You can set it as a free disk. Click the **Set Free Disk** button to set it up.

9.1.4. Rear Component Information

Move your mouse over the rear components in the array, the component information will appear in a popup box. You can watch the information of controllers, management ports, data ports, fan modules, power supply modules, and BBM, and flash module.

Controller Information

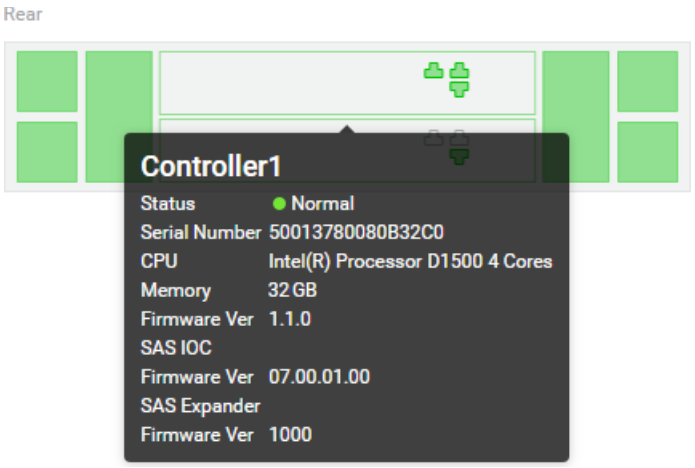


Figure 9-9 Controller Information

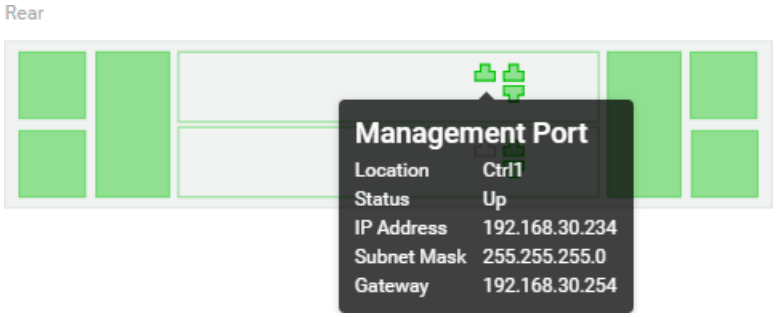


Figure 9-10 Management Port Information

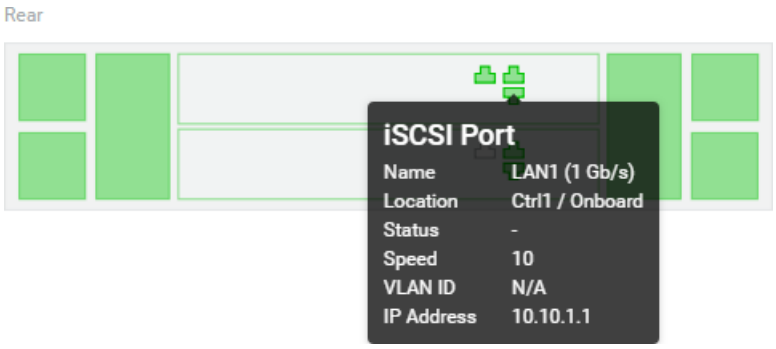


Figure 9-11 Data Port Information

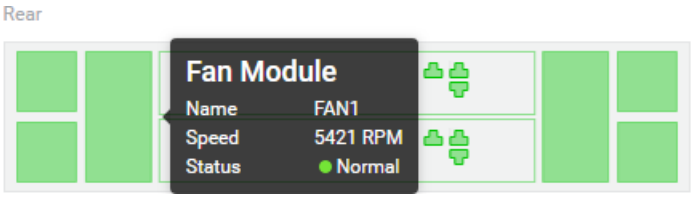


Figure 9-12 Fan Module Information

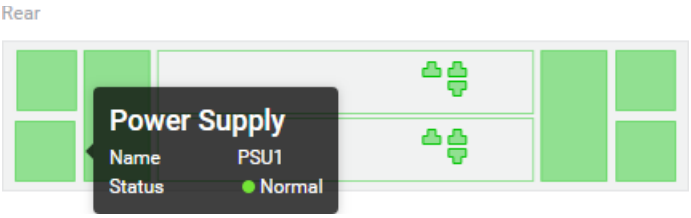


Figure 9-13 Power Supply Information

9.2. Configure System Settings

Select the **System** tab and the **Settings** subtab to configure system settings. There are four panes in this subtab. They are **Accounts**, **General Settings**, **Configuration Backup**, and **Management Port**.

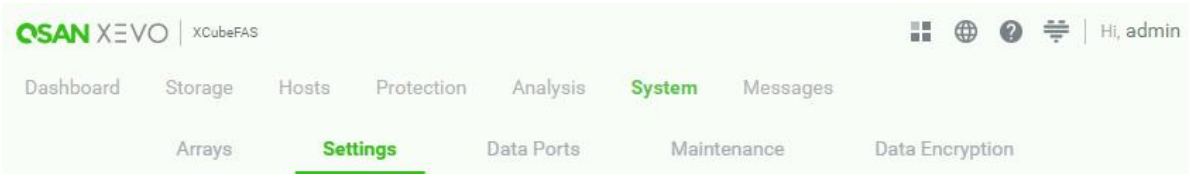


Figure 9-14 Settings Subtab in the System Tab

9.2.1. Account Settings

Click the **Accounts** pane to manage the user accounts.

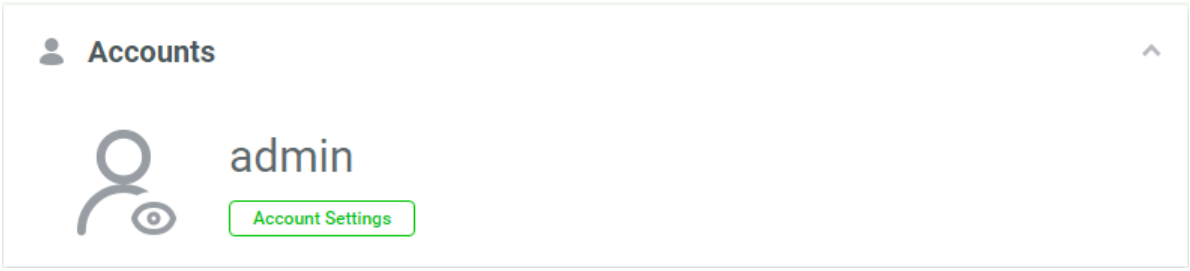


Figure 9-15 Accounts Pane

In this pane, it displays the current login name. For example in the figure, the current login name is **admin**. Click the **Account Settings** button to popup a window.

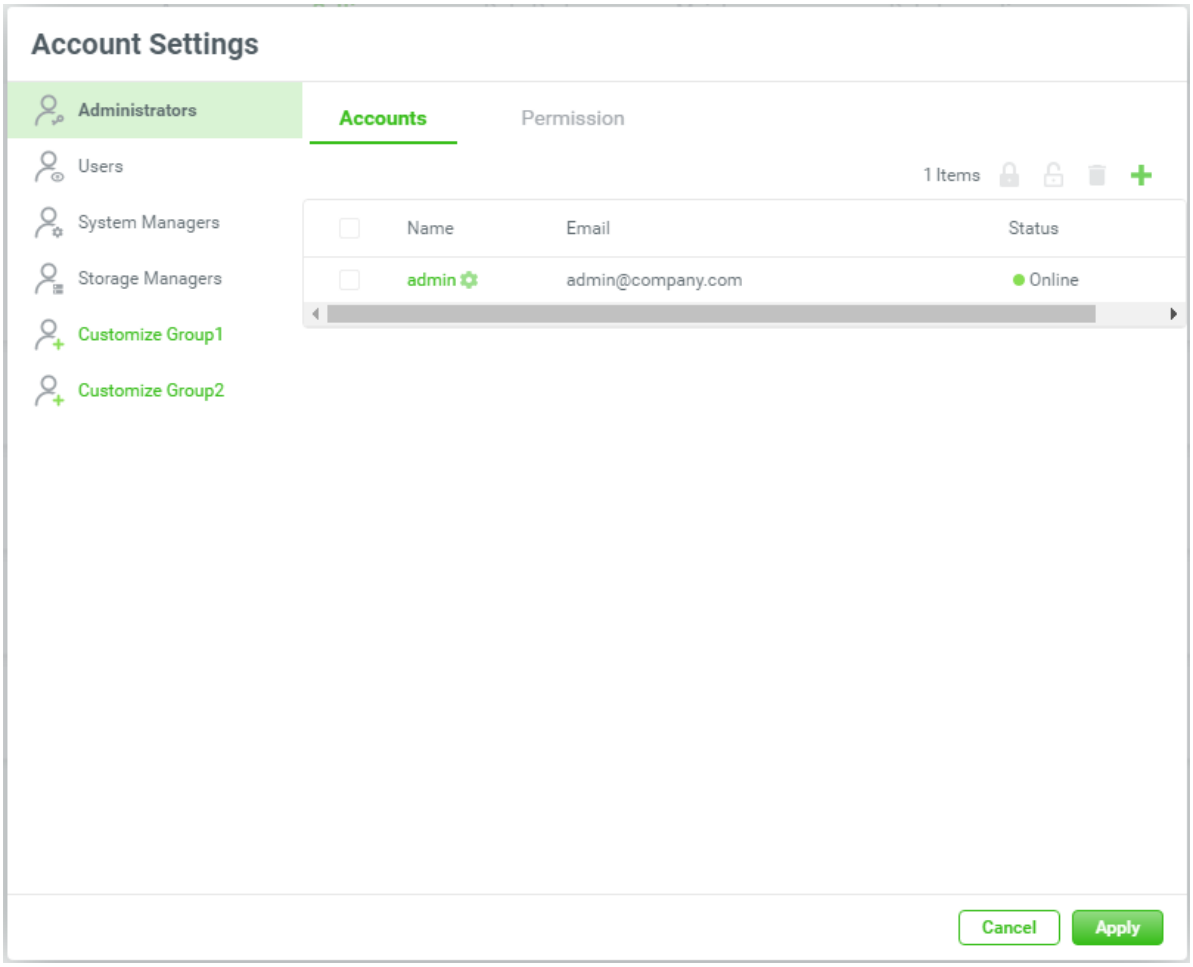


Figure 9-16 Account Settings

Six account groups displayed on the left. The first four have fixed permissions and the bottom two are customizable. Click the **Permission** tab to display the permissions in this group.

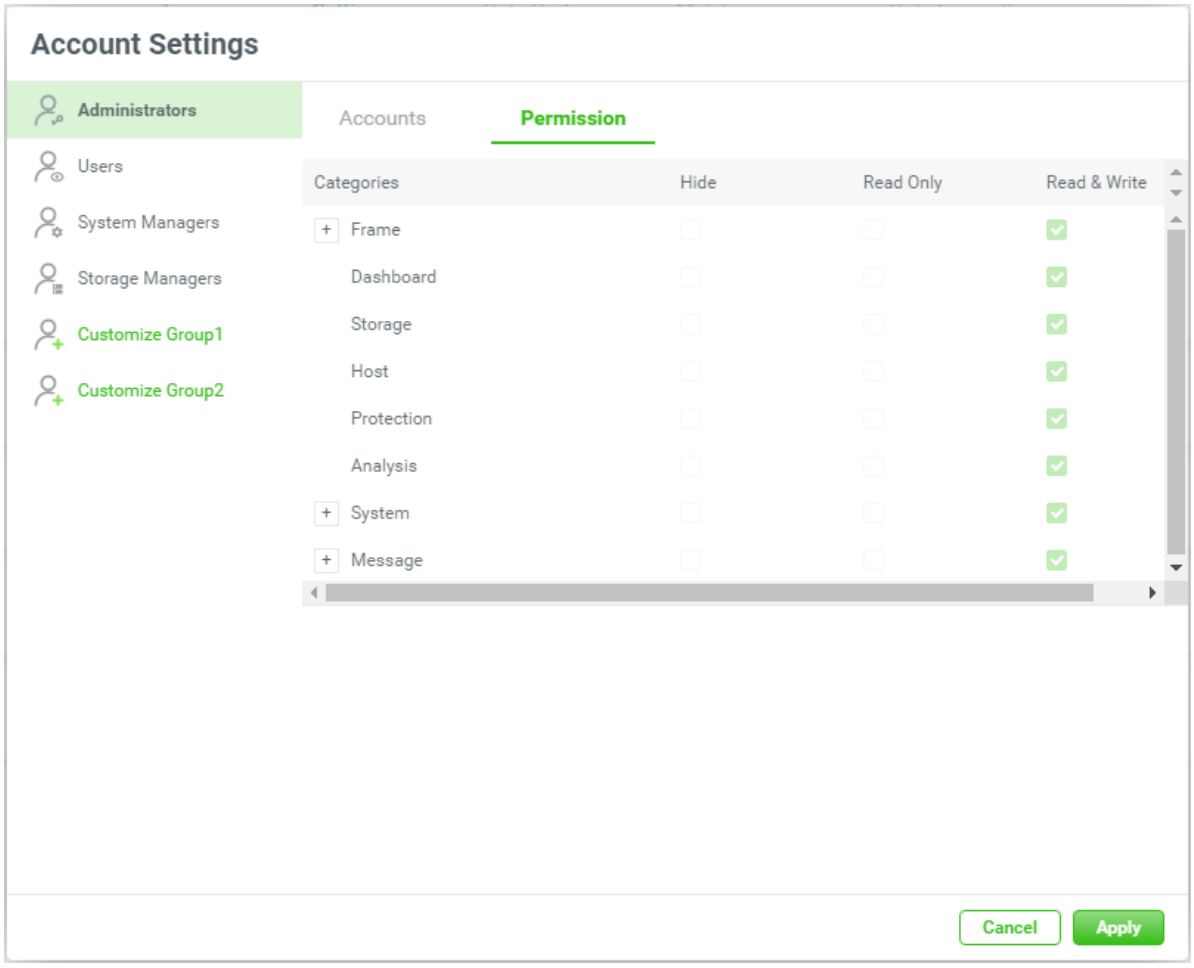


Figure 9-17 Account Permission

Account groups are describing on the following.

1. **Administrators:** This account group has full read and write permissions.
2. **Users:** Most functions are read only; functions on frame, system, and message are hidden.
3. **System Managers:** Functions about system management have read and write permissions, others are read only.
4. **Storage Managers:** Functions about storage management have read and write permissions, others are read only.

5. **Customize Group 1:** Permissions can be customized.
6. **Customize Group 2:** Permissions can be customized.

The options are available in this pane.

Create an Account

Here is an example to create an account.

1. Select an account group for which you want to create an account. Click the ✚ icon in the **Accounts** tab to pop up a window.

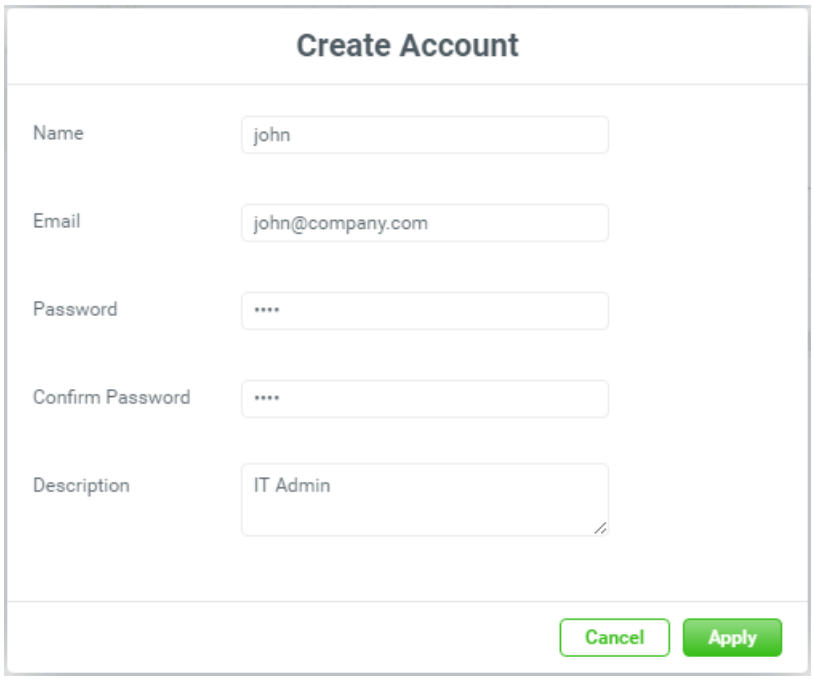


Figure 9-18 Create Account

2. Enter an account **Name.** The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | @].
3. Enter an **Email** address.
4. Enter a **Password**, and reconfirm in **Confirm Password.** The maximum length of the password is 32 characters. Valid characters are [A~Z | a~z | 0~9 | ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/].
5. If necessary, enter a **Description** to identify the account. The maximum length of the description is 20 characters.

6. Click the **Apply** button to take effect.

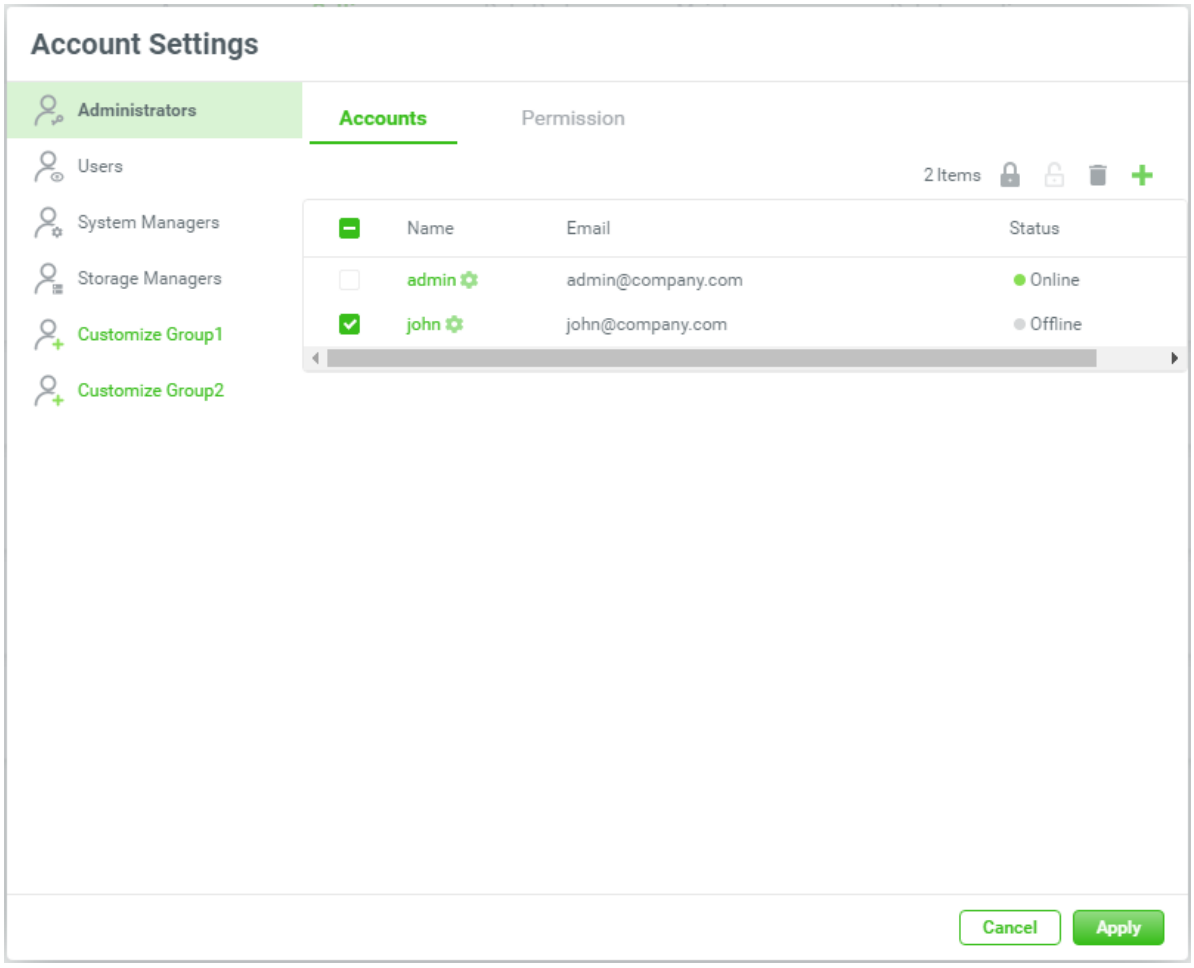


Figure 9-19 An Account is Created

Disable the Account

Here is an example to disable the account.

1. Select the account which you want to disable, and then click the icon.
2. Click the **OK** button to confirm.

Enable the Account

Here is an example to enable the account.

1. Select the account which you want to enable, and then click the icon.
2. Click the **OK** button to confirm.

Delete the Account

Here is an example to delete the account.

1. Select the account which you want to delete, and then click the icon.
2. Click the **OK** button to confirm.

INFORMATION:

There is a default account **admin** in the **Administrators** group. Account **user** in the **Users** group. Account **system** in the **System Managers** group. And account **storage** in the **Storage Managers** group. These default accounts cannot be deleted.

The **admin** account can be disabled only if the other account belongs to the **Administrators** group login.

Customize Permissions

Here is an example to have an account to customize the permissions.

1. Select the **Customize Group1** or **Customize Group2**; create an account in the group
2. Click the **Permission** tab to customize the permissions.

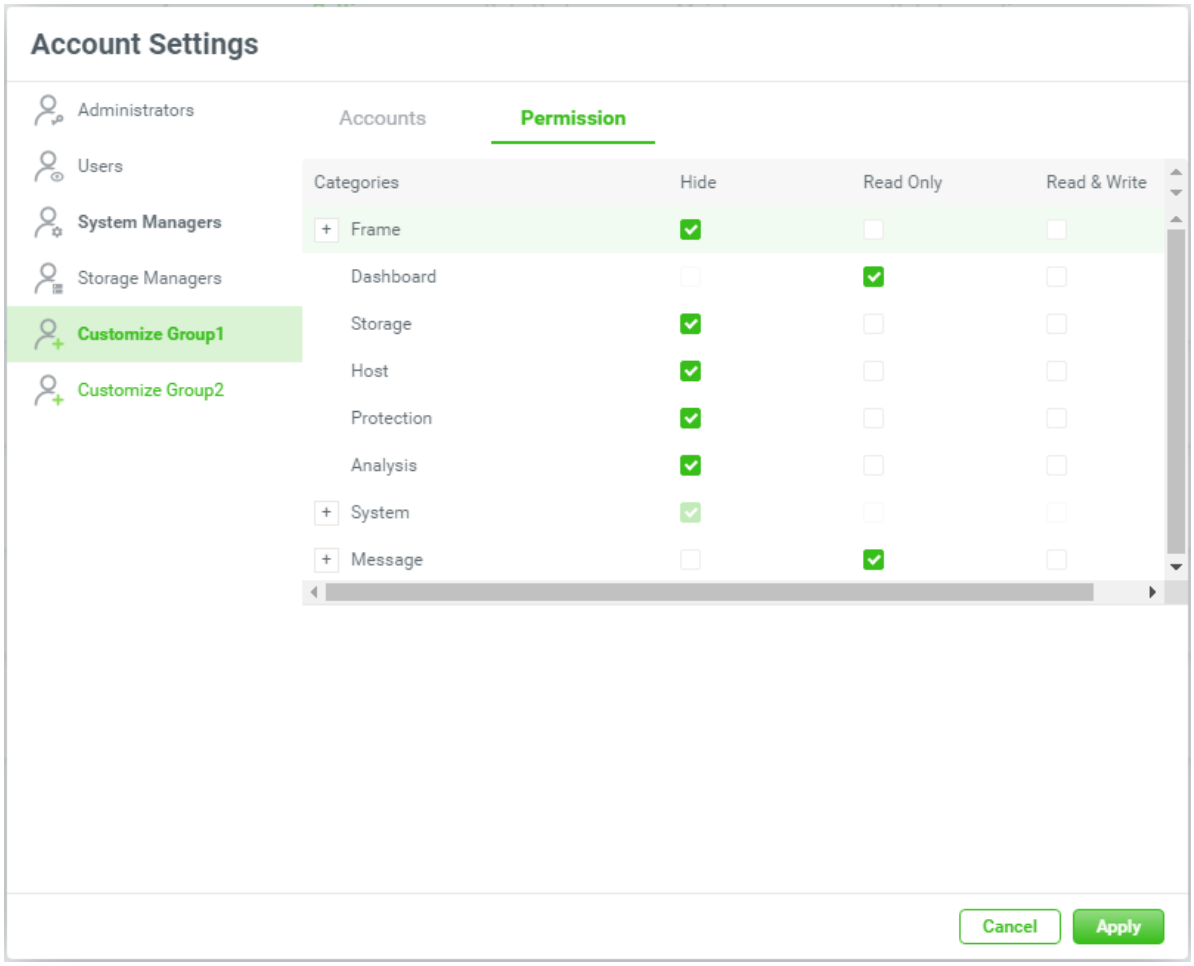


Figure 9-20 Permission Tab in Account Settings

3. According to the permission categories, change the permission to **Hide**, **Read Only**, or **Read & Write**.

When finished, click the **Apply** button to close the window.

9.2.2. General Settings

Click the **General Settings** pane to setup the system name, data and time, and configure the login options.

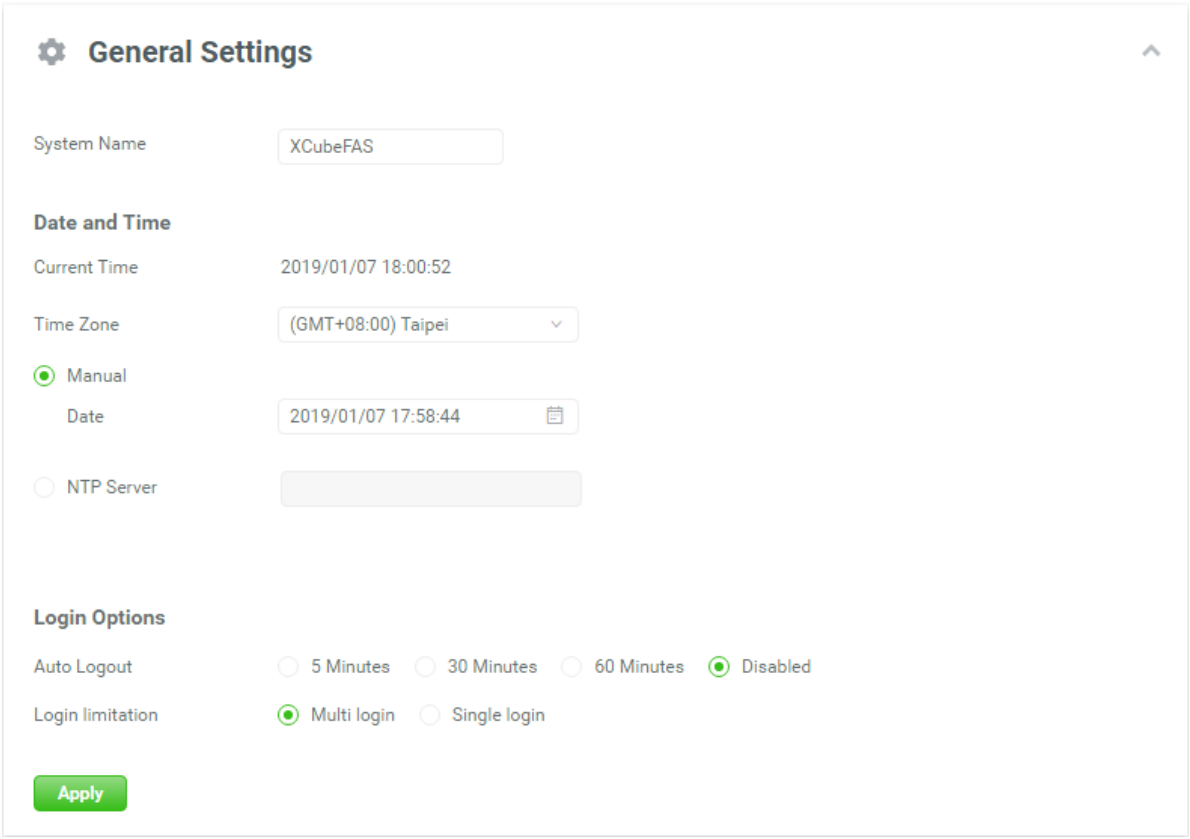


Figure 9-21 General Settings

The options are available in this pane.

System Name

Change the system name, highlight the old name and type in a new one. Maximum length of the system name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_].

Date and Time

Change the current date, time and time zone as required. Date and time can be set by manually or synchronized from a NTP (Network Time Protocol) server.

Login Options

- **Auto Logout:** When the auto logout option is enabled, you will be logged out of the admin interface after the time specified. There are Disabled (default), 5 minutes, 30 minutes, and 60 minutes options.
- **Login Lock:** When the login lock is enabled, the system allows only one user to login to the web UI at a time. There are Multi login (default) and Single login options.

When finished, click the **Apply** button to take effect.

9.2.3. Configuration Backup

Click the **Configuration Backup** pane to be used to either save system configuration (export) or apply a saved configuration (import).

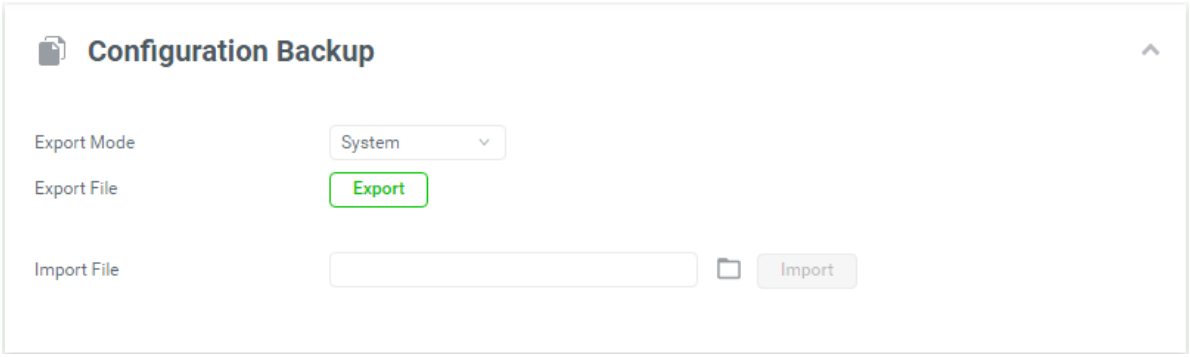


Figure 9-22 Configuration Backup

While the volume configuration settings are available for exporting, to prevent conflicts and overwriting existing data, they cannot be imported.

The options are available in this pane.

Export

Select the **Export Mode** for exporting system or volume configurations, then click the **Export** button to save a file.

Import

Import all system configurations excluding volume configuration.

CAUTION:
The Import option will import all system configurations excluding volume configuration. The current system configurations will be replaced.

9.2.4. Configure Management Port

Click the **Management Port** pane to show the information of the management ports. MAC address is displayed for reference and it is used on wake-on-LAN feature. IP address, DNS server, and service ports can be modified according to the management purpose.

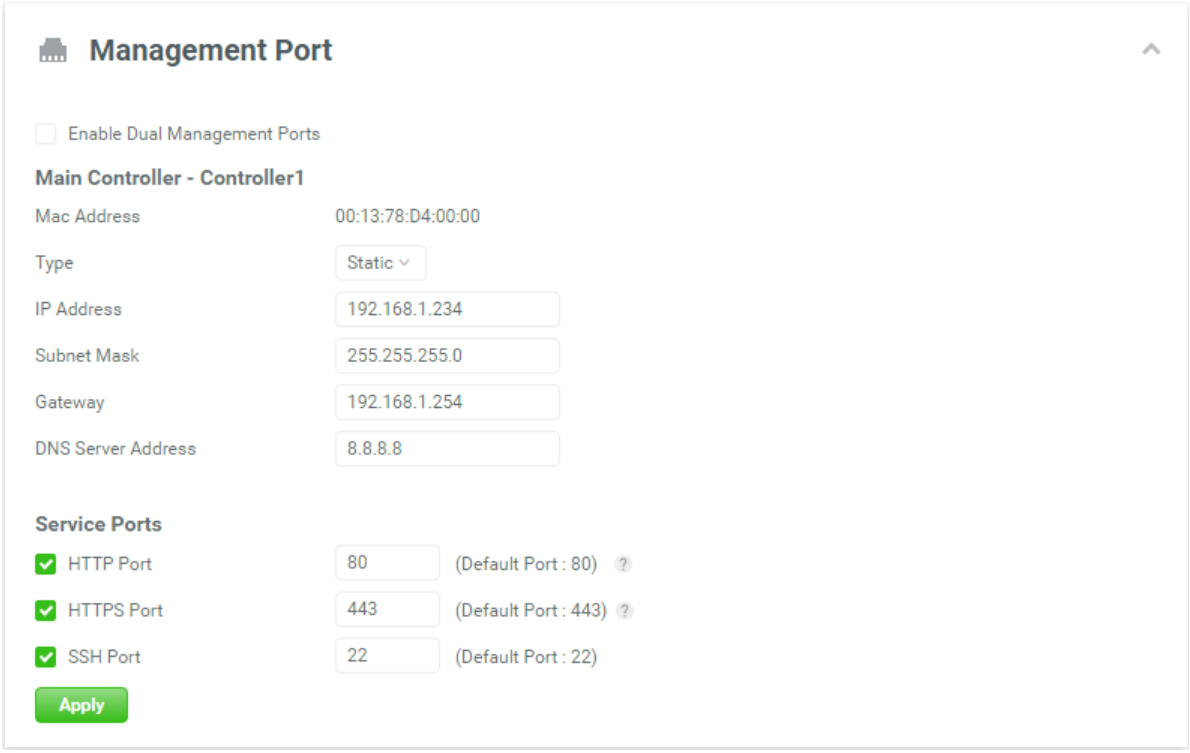


Figure 9-23 Configure Management Port

The options are available in this pane.

Enable Dual Management Ports
This is for dual controller models. When the setting is enabled, both management ports of the controllers have their own IP addresses and MAC addresses, and both are active. If the setting is disabled, only the management port of the master controller is active, the other one is on standby. Both controller management ports share the same IP address and MAC

address. The management port fails over to the slave controller when the master controller goes offline, either planned or unplanned.

INFORMATION:
For deployment of management ports, please refer to the chapter 4 Deployment Types and Cabling in the XCubeFAS Hardware Manual.

Main Controller

- **MAC Address:** Display the MAC address of the management port.
- **Type:** The option can change IP address for remote administration usage. There are three options for **DHCP**, **BOOTP**, or **Static IP Address**.

INFORMATION:
DHCP: The Dynamic Host Configuration Protocol is a standardized network protocol used on IP (Internet Protocol) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

BOOTP: Similar to DHCP, the Bootstrap Protocol is also a computer networking protocol used in Internet Protocol networks to automatically assign an IP address to network devices from a configuration server. While some parts of BOOTP have been effectively superseded by the DHCP, which adds the feature of leases, parts of BOOTP are used to provide service to the DHCP protocol. DHCP servers also provide legacy BOOTP functionality.

- **DNS Server Address:** DNS (Domain Name System) provides a means to translate FQDN (Fully Qualified Domain Name) to IP address. Some notification services need DNS setting. Enter an IP address of DNS server here.

Service Ports

- Uncheck to disable the service ports of **HTTP**, **HTTPS**, and **SSH**. If the default port numbers of the service ports are not allowed on your network environment, they can be changed here.

When finished, click the **Apply** button to take effect.

9.2.5. Configure QoS Settings

Click the **QoS Settings** pane to configure QoS (Quality of Service) settings. For more information, please refer to the chapter 12.1, Configure QoS Settings section.

9.3. Configure Data Port Settings

Select the **System** tab and the **Data Ports** subtab to configure iSCSI or fibre channel data ports.

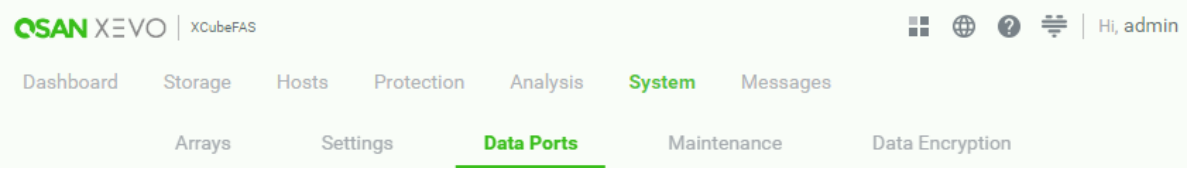


Figure 9-24 Data Ports Subtab in the System Tab

9.3.1. Data Port Overview

XCubeFAS provides different type of host connectivity according to the system configuration, it could be base system or host cards installed system. The base system has two 10GbE iSCSI ports onboard per controller. The host cards are installed the same type on both controllers. Currently host card has three types, 1GbE iSCSI (RJ45), 10GbE iSCSI (SFP+), and 16Gb FC (SFP+), for selection according to system infrastructure.

The **Data Port Overview** displays all the host connectivity in system. The icons show the data ports connected or disconnected.

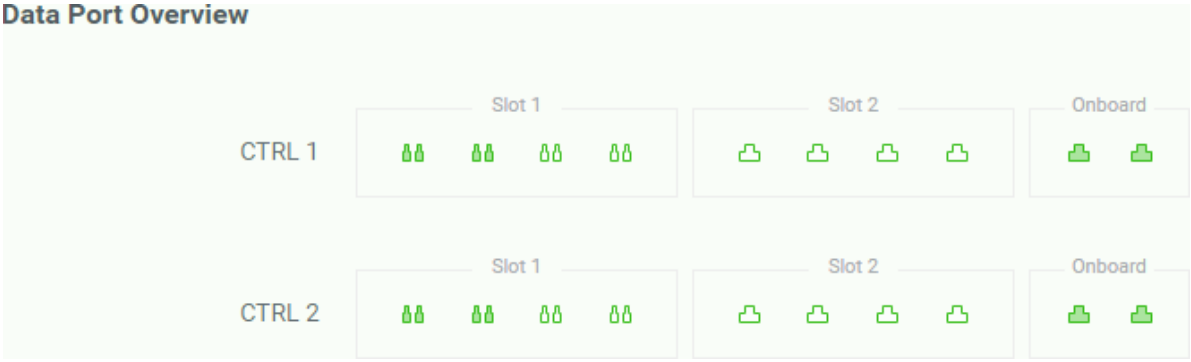


Figure 9-25 Data Port Overview

INFORMATION:
For hardware information about host cards, please refer to the chapter 3.3, Installing the Optional Host Cards section in the XCubeFAS Hardware Manual.

9.3.2. Configure iSCSI Data Ports

Click the **iSCSI Ports** pane to show information of iSCSI ports where they are located (onboard or host cards).

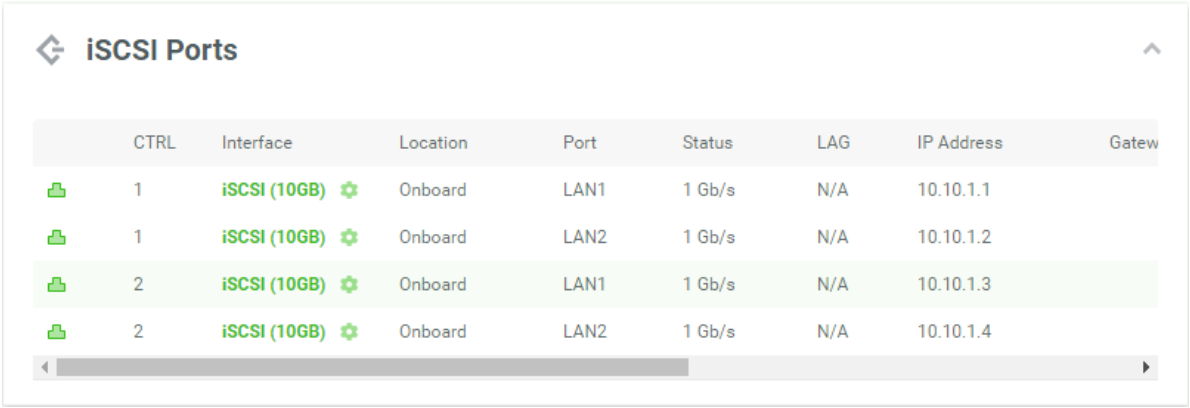


Figure 9-26 iSCSI Ports

The columns display information of an connected or disconnected icon, **CTRL** (Controller), **Interface** name, **Location**, **Port**, **Status**, **LAG** (Link Aggregation), **IP address**, **Gateway** IP address, **VLAN ID** (Virtual LAN ID), **Jumbo Frame** status, and **MAC address**.

Click the icon beside the interface to list the drop down options. These options are available in the iSCSI ports.

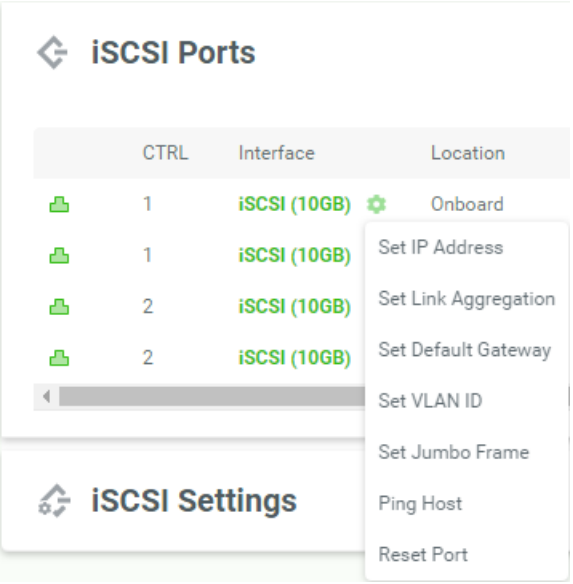


Figure 9-27 iSCSI Options

Set IP Address

Click the **Set IP Address** option to assign an iSCSI IP address of the iSCSI data port. There are two options: Use DHCP to acquire an IP address automatically or specify a Static IP Address to set the IP address manually.

INFORMATION:

DHCP: The Dynamic Host Configuration Protocol is a standardized network protocol used on IP (Internet Protocol) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

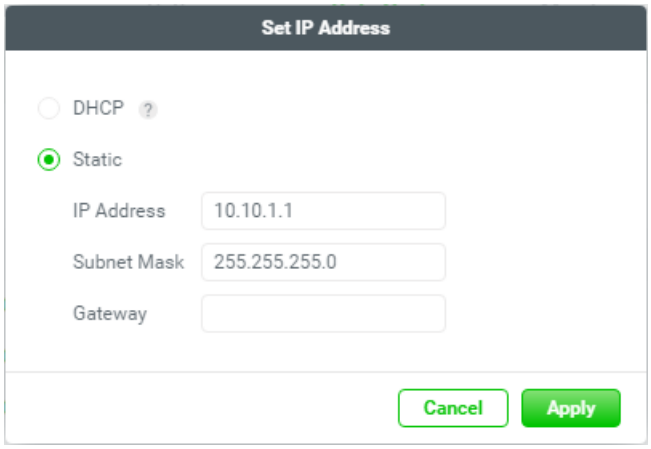


Figure 9-28 iSCSI IP Address Settings

Set Link Aggregation

Click the **Set Link Aggregation** option, the default mode of each iSCSI data port is connected without any bonding. Two bonding methods, Trunking and LACP (Link Aggregation Control Protocol), can be selected. At least two iSCSI data ports must be checked for iSCSI link aggregation.

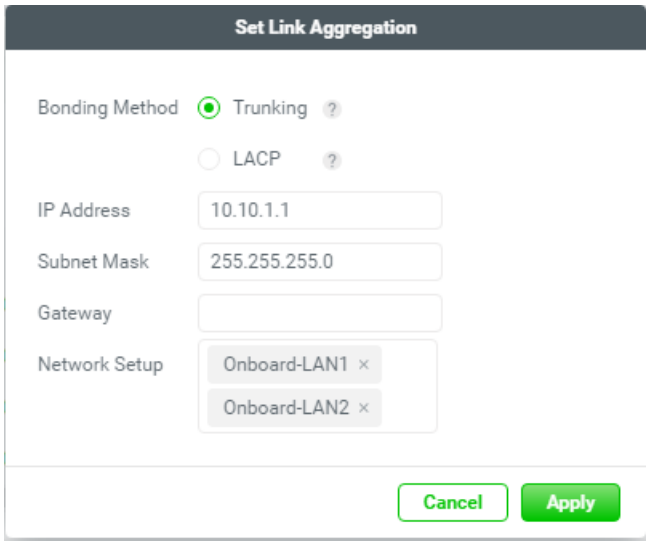


Figure 9-29 Set Link Aggregation

INFORMATION:

Trunking: Sometimes called “Port Trunking” configures multiple iSCSI ports to be grouped together into one in order to increase the connection speed beyond the limit of a single iSCSI port.

LACP: The Link Aggregation Control Protocol is part of IEEE 802.3ad that allows bonding several physical ports together to form a single logical channel. LACP allows a network switch to negotiate an automatic bundle by sending LACP packets to the peer. LACP can increase bandwidth usage and automatically perform failover when the link status fails on a port.

Set Default Gateway

Click the **Set Default Gateway** option to set the gateway of the IP address as default gateway. There can be only one default gateway.

Set VLAN ID

Click the **Set VLAN ID** option, VLAN (Virtual LAN) is a logical grouping mechanism implemented on switch device. VLANs are collections of switching ports that comprise a single broadcast domain. It allows network traffic to transfer more efficiently within these logical subgroups. Please consult your network switch user manual for VLAN setting instructions. Most of the work is done at the switch. Please make sure that your VLAN ID of iSCSI port matches that of switch port. If your network environment supports VLAN, you can use this function to change the configurations. Fill in VLAN ID and Priority settings to enable VLAN.

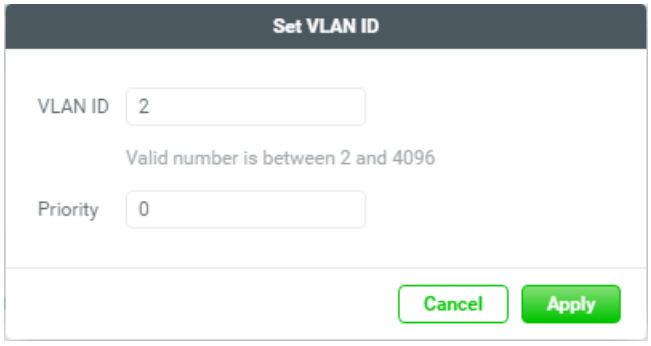


Figure 9-30 Set VLAN ID

INFORMATION:

VLAN ID: VLAN ID is a number ranges from 2 to 4094. Three numbers (0, 1, and 4095) are reserved for special purposes.

Priority: The PCP (Priority Code Point) is a number ranges from 0 to 7 and reserved for QoS (Quality of Service). The definition is compliant with IEEE 802.1p protocol and 0 is the default value. In normal cases, you don't need to set this value.

Remove Default Gateway

To remove the default gateway, click the **Remove Default Gateway** option.

Set Jumbo Frames

Click the **Set Jumbo Frames** option to set the MTU (Maximum Transmission Unit) size. The jumbo frame size could be set as 4000 or 9000 bytes. Jumbo Frame is disabled by default.

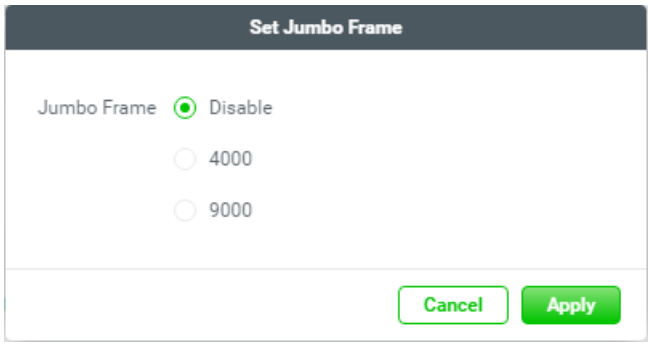


Figure 9-31 Set Jumbo Frame

CAUTION:

If the VLAN ID or jumbo frames are set, the related switching hub and HBA on host must be set, too. Otherwise, the LAN connection cannot work properly.

Ping Host

Click the **Ping Host** option to verify the port connection from a target to the corresponding host data port. Input the host's IP address and click **Start** button. The system will display the ping result. Click **Stop** button will stop ping activity.

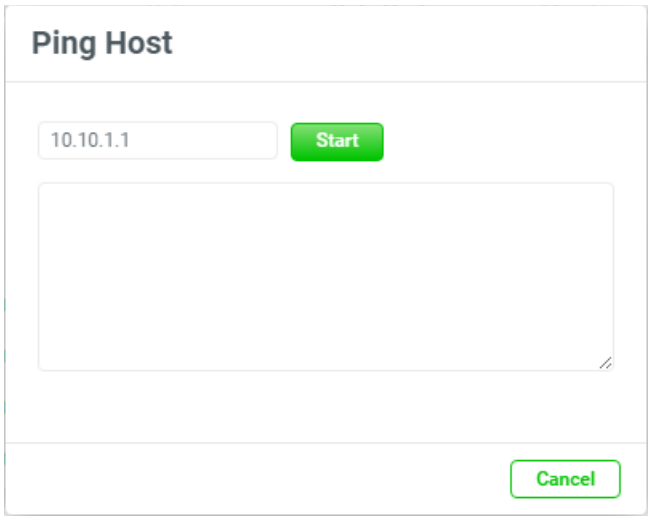


Figure 9-32 Ping Host

Reset Port

Click the **Reset Port** option to be generally used to recover from a port malfunction.

9.3.3. Configure iSCSI Settings

Click the **iSCSI Settings** pane to provide to set up entity name of the system and iSNS (Internet Storage Name Service) server. The entity name is default in IQN (iSCSI Qualified Name) format and could be modified for management purpose. The iSNS IP is used by iSNS protocol for automated discovery, management and configuration of iSCSI devices on a TCP/IP network. To use iSNS, an iSNS server must be added to the SAN. The iSNS server IP address must be added to the storage system for iSCSI initiator service to send queries.

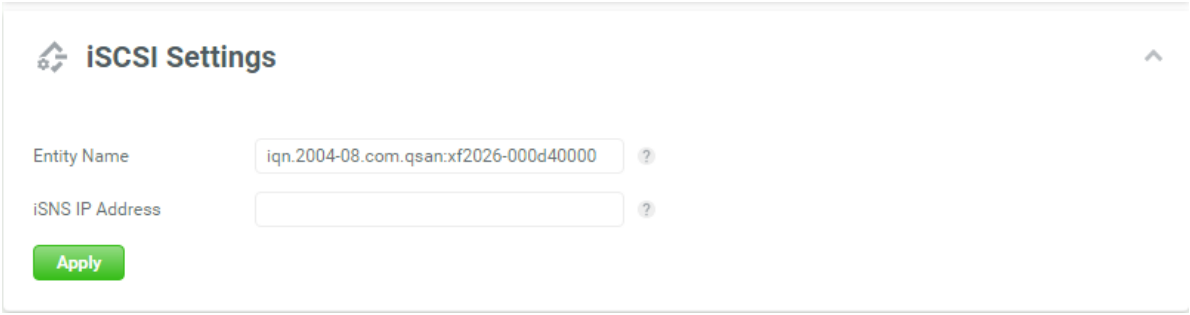


Figure 9-33 Entity Name and iSNS Settings

The options are available in this pane.

- **Entity Name:** Change the entity name; highlight the old name and type in a new one. The maximum length of entity name is 200 characters. Valid characters are [a~z | 0~9 | -.:].
- **iSNS IP Address:** The option can change iSNS IP address for internet storage name service.

When finished, click the **Apply** button to effect changes.

INFORMATION:
iSNS: The iSNS protocol allows automated discovery, management, and configuration of iSCSI devices on a network.

9.3.4. Configure Fibre Channel Ports

Click the **Fibre Channel Ports** pane to show information of fibre channel ports where they are located on the host cards.

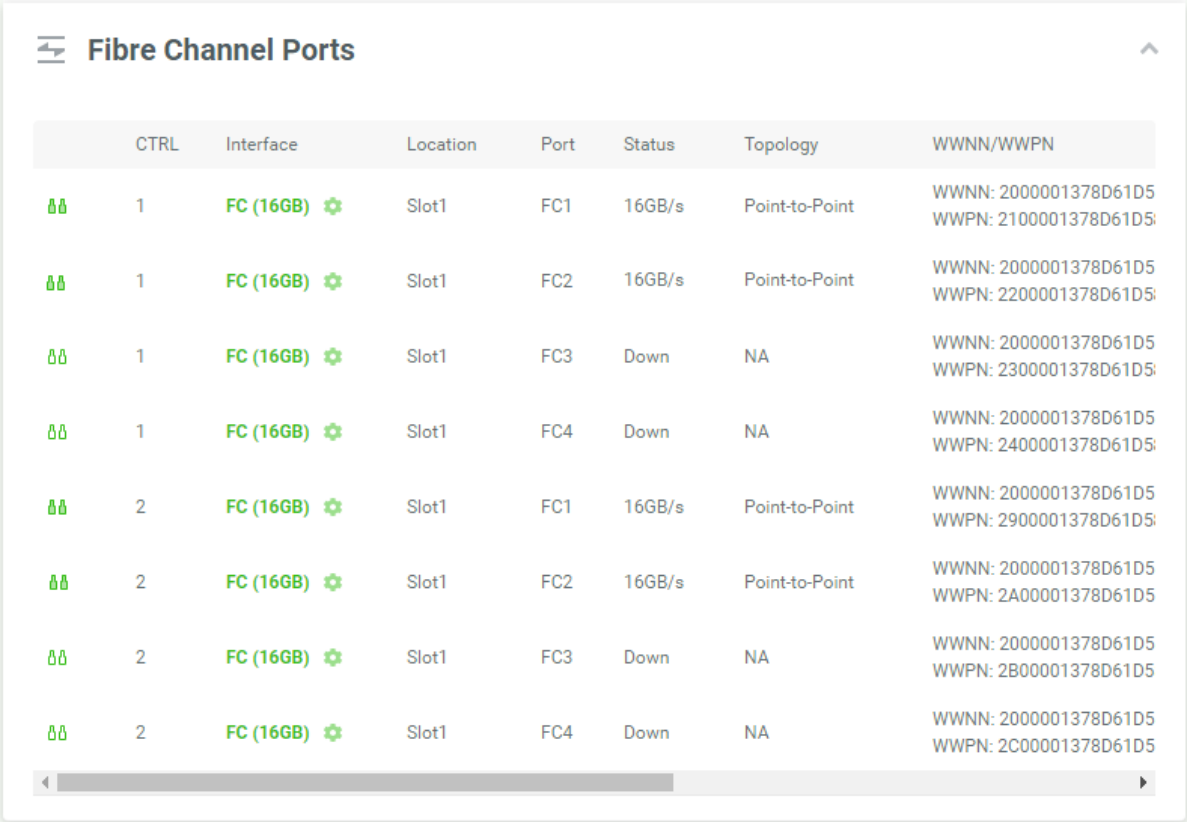


Figure 9-34 Fibre Channel Ports

The columns display information of an connected or disconnected icon, **CTRL** (Controller), **Interface** name, **Location**, **Port**, **Status**, **Topology**, **WWNN/WWPN** (World Wide Node Name / World Wide Port Name), **Loss of Signal**, **Loss of Sync**, **Link Failure**, and **Invalid CRC**.

Click the icon beside the interface to list the drop down options. These options are available in the Fibre Channel ports.

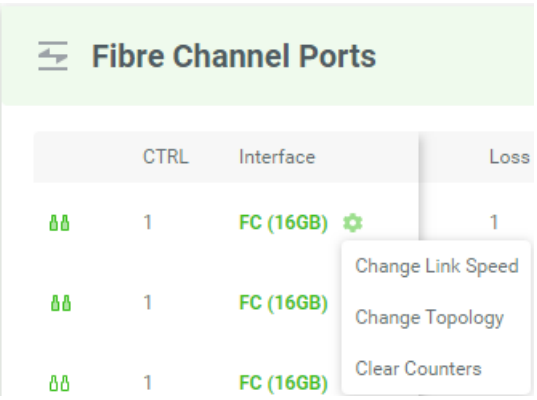


Figure 9-35 Fibre Channel Options

Change Link Speed

Click the **Change Link Speed** option to change the link speed of fibre channel. Set the link speed of fibre channel. The options are Automatic (default), 4 Gb/s, 8 Gb/s, and 16 Gb/s. Recommend to set it as Automatic to detect the data rate automatically.

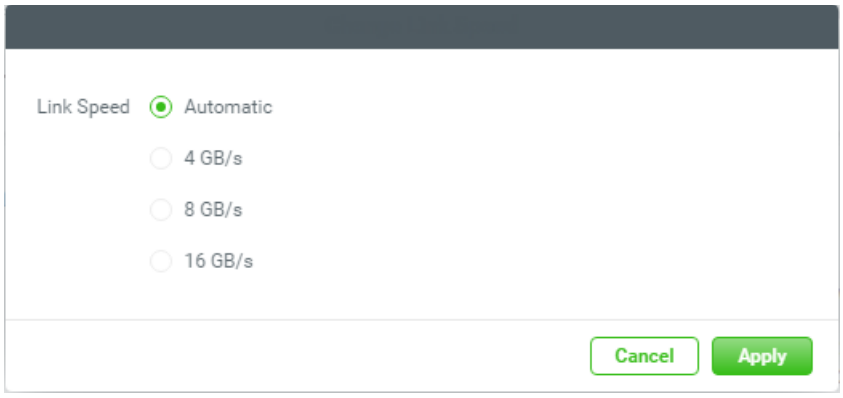


Figure 9-36 Change Link Speed

Change Topology

Click the **Change Topology** option to change the topology of fibre channel. Set the topology fibre channel. The option is Point-to-Point for 16 Gb/s fibre channel, Point-to-Point and Loop modes for 4 Gb/s, 8 Gb/s fibre channel. Set it appropriately according to your fibre channel environment.

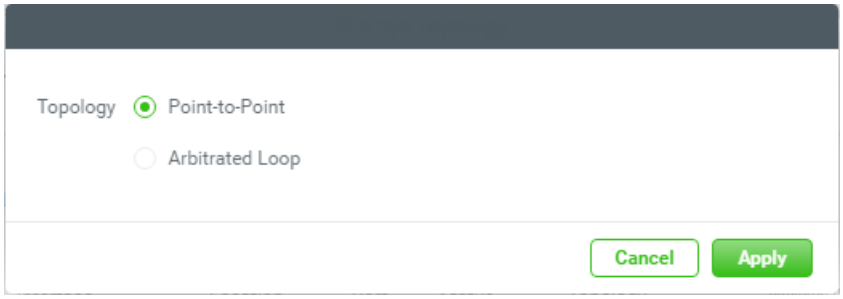


Figure 9-37 Change Topology

INFORMATION:

Point-to-Point (FC-P2P): Two devices are connected directly by FC interface. This is the simplest topology with limited connectivity and supports 4 Gb/s, 8 Gb/s, and 16 Gb/s fibre channel speed.

Loop (FC-AL, Arbitrated Loop): All devices are connection in loop or ring, similar to token ring networking. Add or remove any device will affect activities on the loop. The failure of any device will cause ring broken. Fibre Channel hub connects multiple devices together and may bypass the failed ports. A loop may also be made by cabling each port to the next in a ring. Loop mode supports 4 Gb/s and 8 Gb/s fibre channel speed only.

CAUTION:

If the link speed and topology are set, the related fibre channel switch and HBA on host must be set, too. Otherwise, the connection cannot work properly.

Clear Counters

Click the **Clear Counters** option to clear all counters of fibre channels. It will pop up a confirm dialog, and then click the **Apply** button to take effect.

9.4. Maintenance

Select the **System** tab and the **Maintenance** subtab to provide **System Information**, **Firmware**, **Disk Services**, **Power Settings**, and **Rescue** functions.

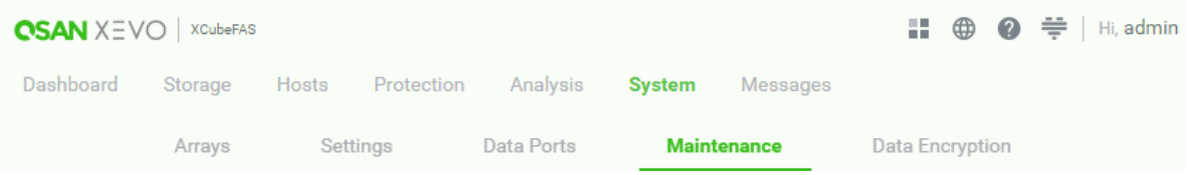


Figure 9-38 Maintenance Subtab in the System Tab

9.4.1. System Information

Click the **System Information** pane to display all system information.

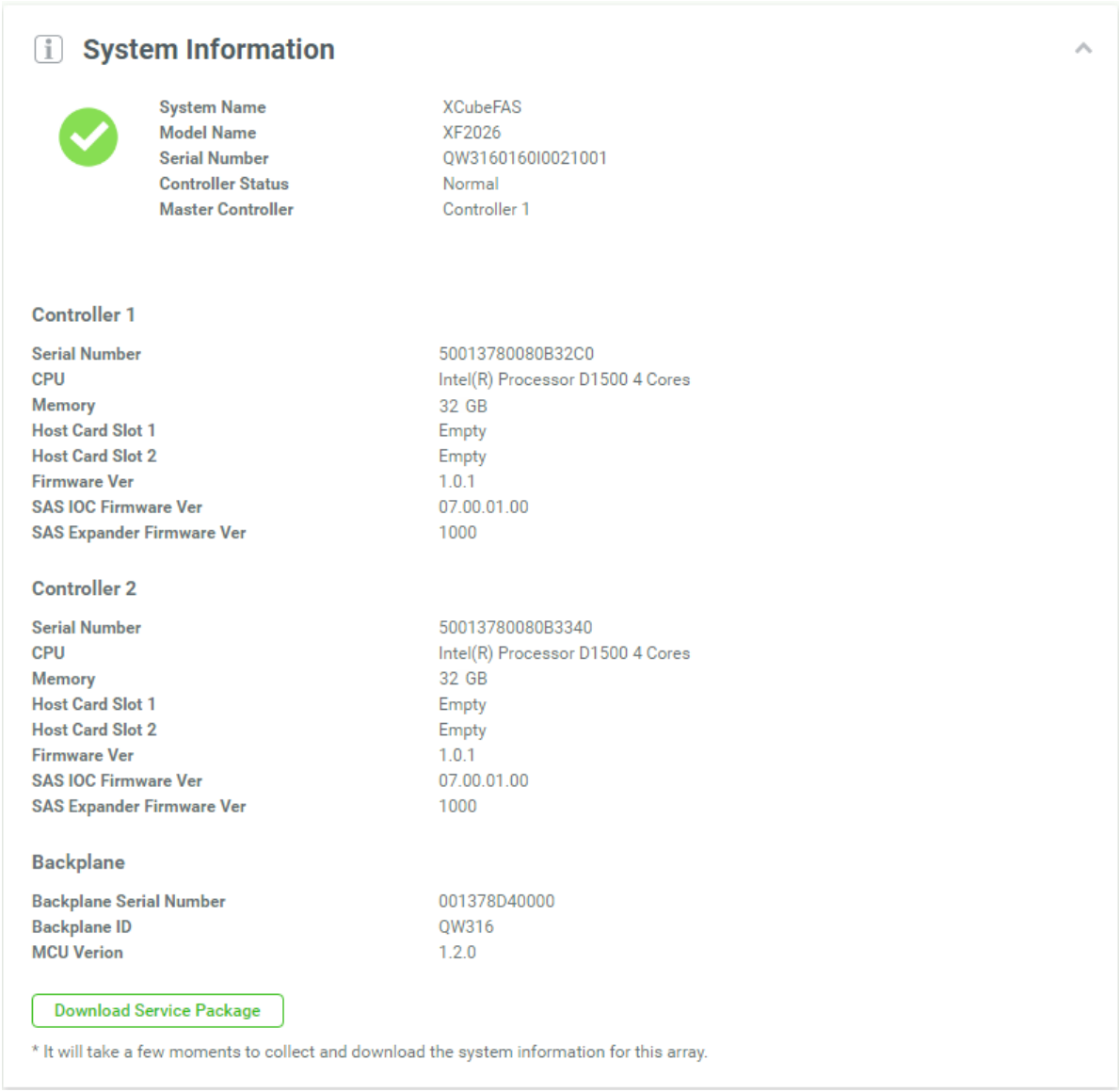


Figure 9-39 System Information

The options are available in this pane.

- **Download Service Package:** Click button to download system information for service.

CAUTION:
If you try to increase the system memory and running in dual controller mode, please make sure both controllers have the same DIMM on each corresponding memory slot. Failing to do so will result in controller malfunction, which will not be covered by warranty.

9.4.2. Firmware Update

Click the **Firmware** pane to be used to update controller firmware, expansion unit firmware.

TIP:
Before upgrading, we recommend you to export your system configurations first in the **Configuration Backup** function tab. Please refer to the chapter 9.2.3, Configuration Backup section for more details.

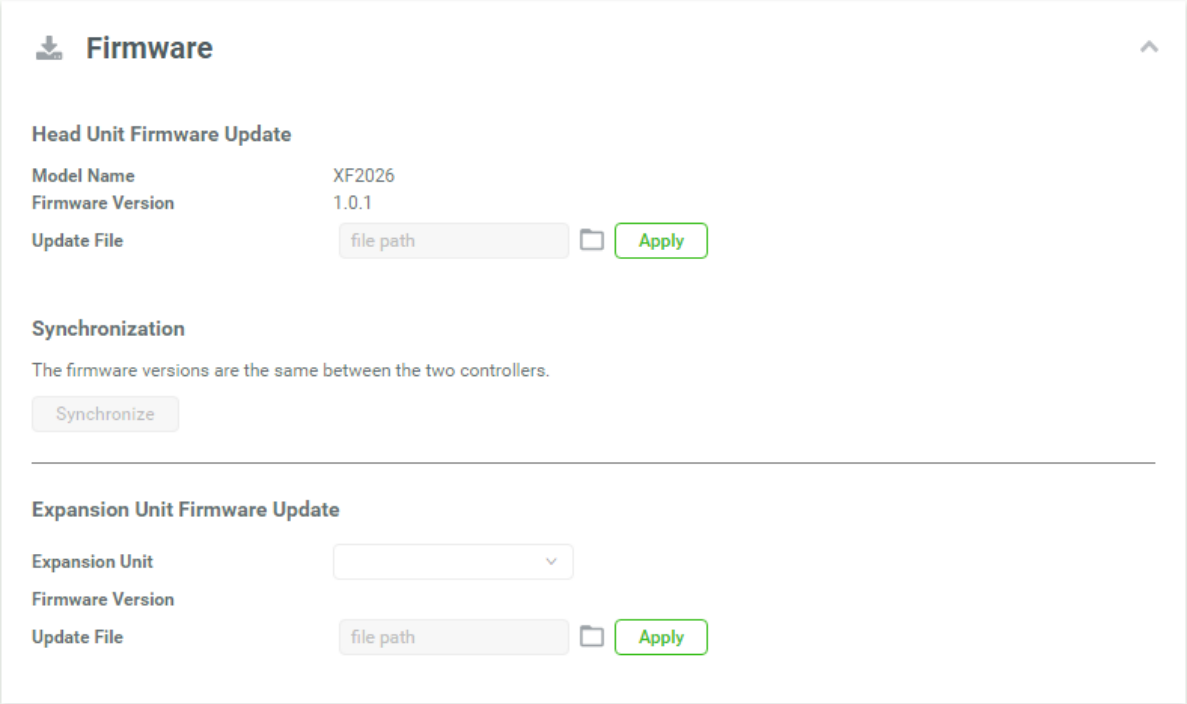


Figure 9-40 Firmware Update

The options are available in this pane.

Head Unit Firmware Update

Please prepare new controller firmware file named “xxxx.bin” in local hard drive, click the icon to select the firmware file. Then click the **Apply** button, it will pop up a warning message, click the **OK** button to start upgrading the firmware.

When upgrading, there is a progress bar running. After finished upgrading, the system must reboot manually to make the new firmware take effect.

TIP:

Firmware update can be done without downtime if the MPIO configuration is well-configured between the connected host / server and both controllers. A firmware update process will update both controllers at the same time. After finished updating, you have to reboot the system.

A system reboot will reboot the master controller first. At this point, the slave controller will take over all tasks (and becomes a new master controller). After the original master controller finishes the booting process (the original master controller is slave controller at this moment), the new master controller (the original slave controller) will reboot automatically, and so on for the original master controller to take over the tasks, once the original slave controller finishes the booting process, the firmware update procedure is completed.

Synchronization

If the firmware versions between two controllers are different, it will display a warning message. Click the **Synchronize** button to synchronize and force a reboot.

Expansion Unit Firmware Update

To upgrade expansion unit firmware, first select an expansion unit. Then other steps are the same as the head unit firmware update. After finished upgrading, the expansion unit must reboot manually to make the new firmware take effect.

9.4.3. Disk Services

Click the **Disk Services** pane to clear disk read error and update disk firmware.

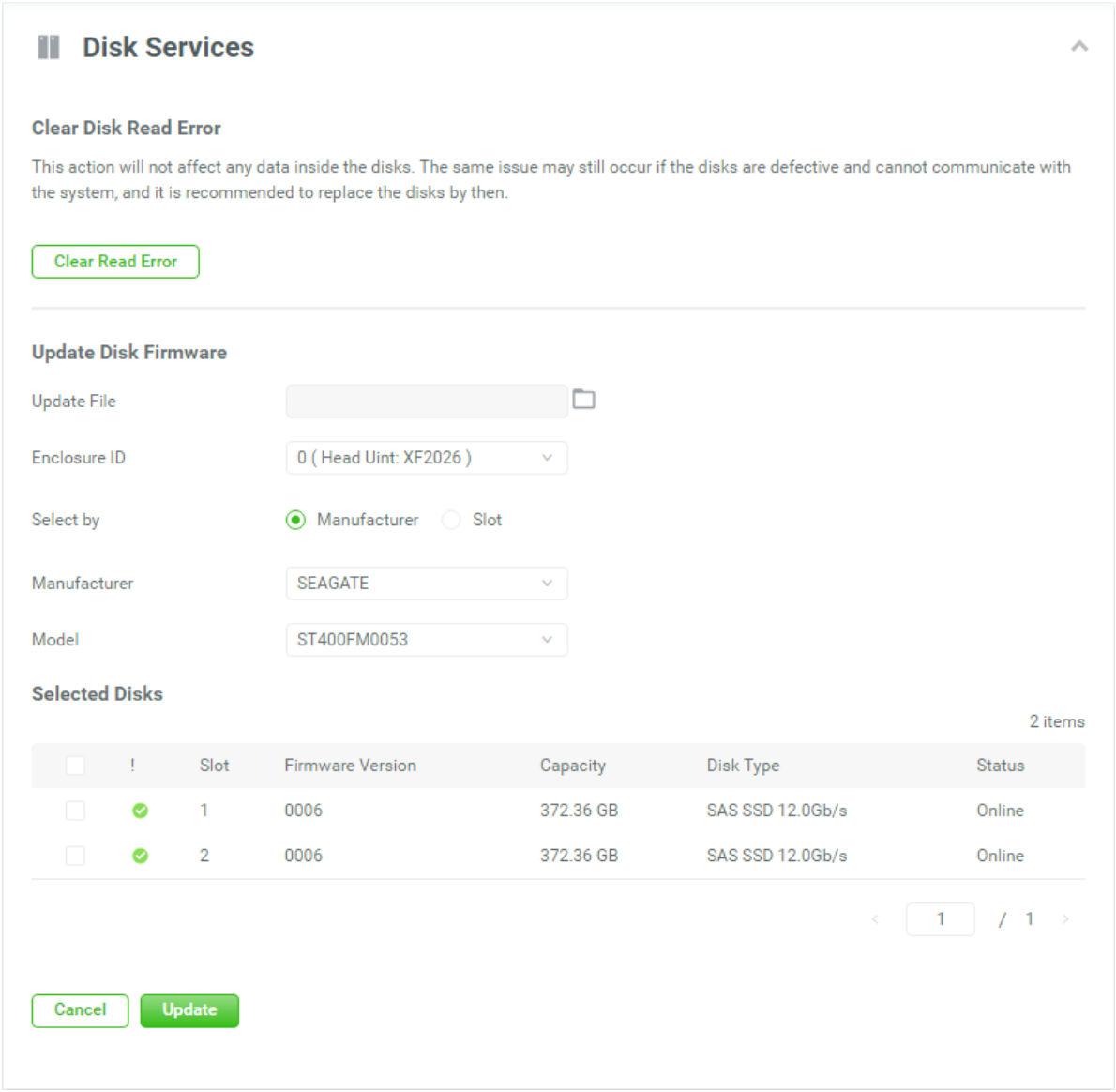


Figure 9-41 Disk Services

The options are available in this pane.

Clear Disk Read Error

Click the **Clear Read Error** button to clean the read error of the disk drive and reset the failed status.

Update Disk Firmware

Select disks by manufacturer or slot, and click the icon to select a firmware file, and then click the **Update** button to upgrade the firmware of the disk drive.

9.4.4. Power Settings

Click the **Power Settings** pane to configure the boot options and UPS (Uninterruptible Power Supply).

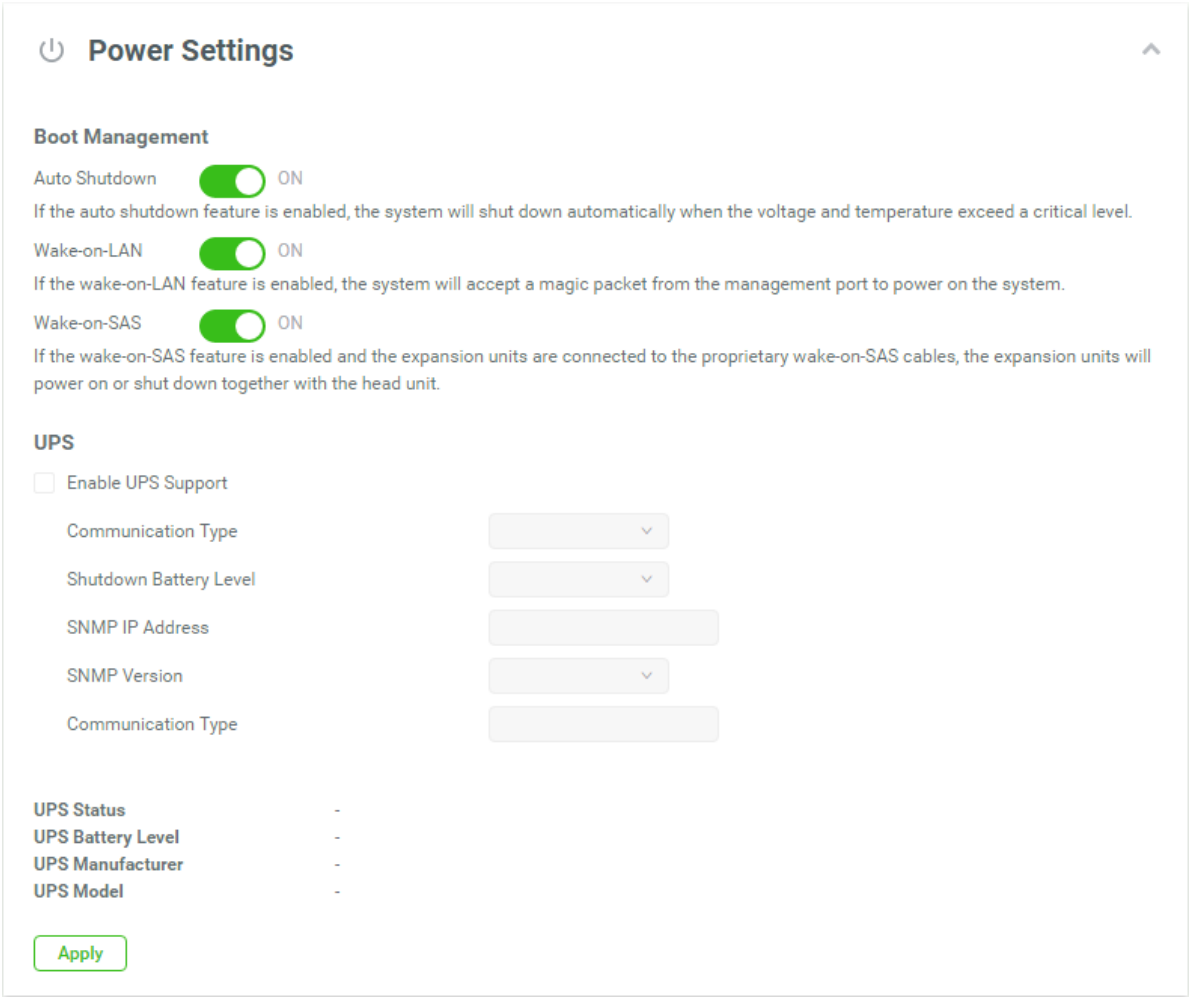


Figure 9-42 Power Settings

The options are available in this pane.

Boot Management

Click the switch to turn ON (Enable) or OFF (Disable).

- **Auto Shutdown:** Check to enable the auto shutdown feature. If it is enabled, the system will shut down automatically when the voltage and temperature exceed a critical level.

TIP:
For better protection and to avoid a single short period of abnormal voltage or temperature, enabling the setting could trigger an automatic shutdown. This is done using several sensors placed on key systems that the system checks every 30 seconds for present voltages or temperatures.

- **Enable Wake-on-LAN:** Check to enable the wake-on-LAN feature. If it is enabled, the system will accept a magic packet from the management port to power on the system.

TIP:
To execute wake-on-LAN function, MAC address of management port is needed. For the information of MAC address, please refer to the chapter 9.2.4, Configure Management Port page.

- **Enable Wake-on-SAS:** Check to enable the wake-on-SAS feature. If the wake-on-SAS feature is enabled and the expansion units (XD5300 series) are connected to the proprietary wake-on-SAS cables, the expansion units will power on or shut down together with the head unit.

INFORMATION:
For deployment of the head unit and expansion units, please refer to the chapter 4, Deployment Types and Cabling in the XCubeFAS Hardware Manual.

CAUTION:
Wake-on-SAS feature required QSAN proprietary expansion cables connected between the head unit and expansion units. Please contact local sales for this accessory.

UPS

Check the **Enable UPS Support** checkbox to enable UPS supported. Now we support network UPS via SNMP, Serial UPS with COM port, and USB UPS.

INFORMATION:
For deployment of UPS, please refer to the chapter 3, Installing the System Hardware in the XCubeFAS Hardware Manual.

- **Communication Type:** Now we support network UPS via SNMP, Serial UPS with COM port, and USB UPS.
- **Shutdown battery Level:** If the power is shortage, the system will execute shutdown process when reaching the UPS battery level.

If Communication Type selects SNMP:

- **SNMP IP Address:** Enter the IP address of the network UPS via SNMP.
- **SNMP Version:** Select SNMP supported versions: v1, v2c, or v3. Please enter community if select SNMP v1 or v2c. If select SNMP v3, it needs more options for authentication. Please enter a username, check to use authentication if necessary, select an authentication protocol and enter an authentication password, check to use privacy if necessary, the privacy protocol supports DES, and enter a privacy password.
- If Communication Type selects Serial:
- **UPS Manufacturer:** Select the UPS manufacture.
- **UPS Model:** Select the UPS model.

When finished, click the **Apply** button to take effect.

This table shows the UPS status.

Table 9-3 UPS Status Descriptions

Column Name	Description
UPS Status	The status of UPS: • On Line: The UPS is online. • On Battery: The UPS is on battery. • Low Battery: The voltage of the battery is low. • High Battery: The voltage of the battery is high. • Replace Battery: The battery needs to be replaced.

	• Charging: The battery is charging. • Discharging: The battery is discharging. • Bypass Mode: The power circuit bypasses the UPS battery, so no battery protection is available. It may happen to check if the UPS operates properly during a power loss. Or the UPS is offline for maintenance. • Offline: UPS is offline and is not supplying power to the load. • Overloaded: UPS is overloaded. You plugged more equipments into the UPS than it was designed to handle. • Forced Shutdown: Forced shutdown the UPS.
UPS Battery Level	The battery level of the UPS.
UPS Manufacturer	The manufacturer of the UPS.
UPS Model	The model of the UPS.

9.4.5. Rescue

Click the **Rescue** pane to allow users to reset the system configurations back to the factory default settings, clean all configurations of the expansion enclosure ID, and restore the volume configuration from the volume creation history.

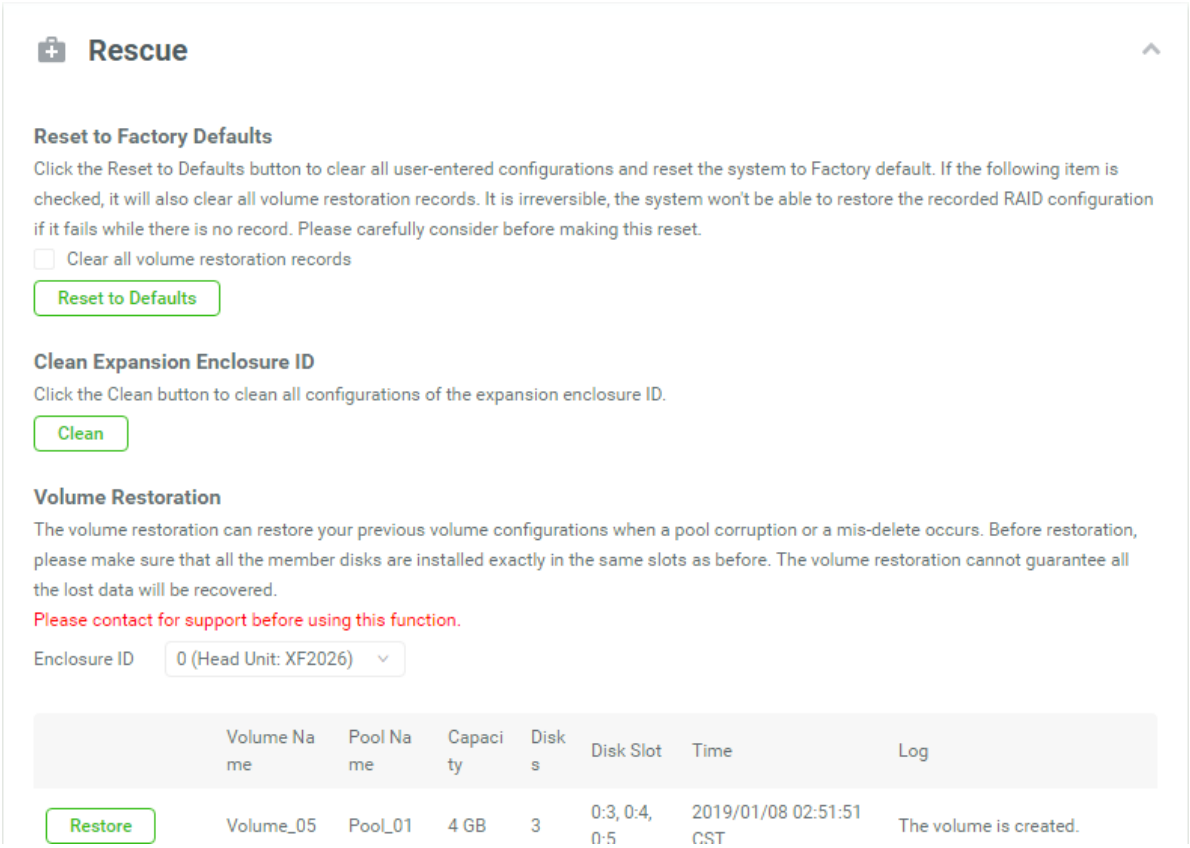


Figure 9-43 Rescue

The options are available in this pane.

Reset to Factory Defaults

Click the **Reset to Defaults** button to progress reset to defaults and force a reboot. The default settings are:

- Reset **Management Port** IP address to DHCP, and then fix IP address: 169.254.1.234/16.
- Reset admin's **Password** to 1234.
- Reset **System Name** to model name plus the last 6 digits of serial number. For example: XF2026-123456.
- Reset IP addresses of all **iSCSI Ports** to 192.168.1.1, 192.168.2.1, … etc.
- Reset link speed of all **Fibre Channel Ports** to Automatic.
- Clear all access control settings of the host connectivity.

Clear all volume restoration records

Check the **Clear all volume restoration records** to clear all volume restoration records.

CAUTION:
Process the **Reset to Defaults** function will force a reboot. To clear all volume restoration records is irreversible. The system won't be able to restore the recorded RAID configuration if it fails while there is no record. Please carefully consider before making this reset.

Clean Expansion Enclosure ID

Click the **Clean** button to clean all configurations of expansion enclosure ID. A clean will cause the system shutdown, and then you have to start manually.

INFORMATION:
The XCubeDAS XD5300 series features the seven-segment LED display for users to easily identify a specific XCubeDAS system. The enclosure ID is assigned by head unit (XCubeSAN series) automatically. The seven - segment LED display supports up to ten XCubeDAS systems, and the numbering rule will start from 1 to A. For dual controller models, both controllers will display the same enclosure ID. After the XD5300 had been assigned the enclosure ID, head unit will assign the same enclosure ID when the system reboots or goes shutdown. For hardware information enclosure ID, please refer to the chapter 2.7, Seven-segment LED Display section in the XCubeDAS Hardware Manual.

CAUTION:
Process the **Clean Expansion Enclosure ID** function will force the system shutdown to clean all configurations of expansion enclosure ID.

Volume Restoration

This function will restore the volume configuration from the volume creation history. It is used for pool corruption and tries to recreate the volume. When trying to do data recovery, the same volume configurations as original must be set and all member disks must be installed by the same sequence as the original. Otherwise, data recovery will fail. The volume restoration does not guarantee that the lost data can be restored. Please get help from an expert before executing this function.

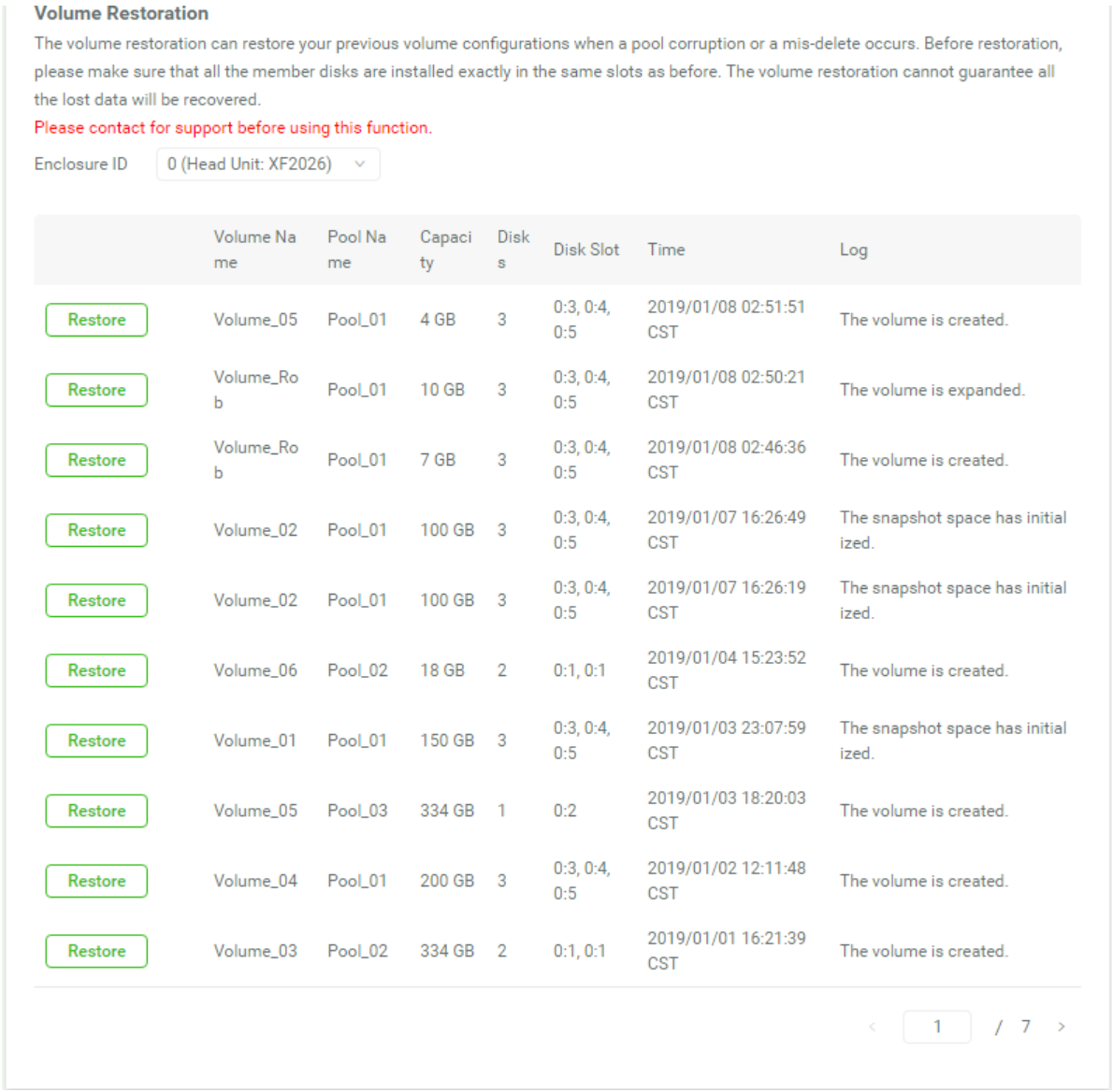


Figure 9-44 Volume Restoration

This table shows the column descriptions.

Table 9-4 Volume Restoration Column Descriptions

Column Name	Description
Volume Name	The original volume name.
Pool Name	The original pool name.
Capacity	The original capacity of the volume.
Disks	The original quantity of physical disk in the pool.
Disk Slot	The original physical disk locations.

Time	The last action time of the volume.
Logs	The last event of the volume.

TIP:
When attempting data recovery, the same volume configurations as the original must be set and all member disks must be installed by the same sequence as original. Otherwise, data recovery will fail.

CAUTION:
Performing data recovery does not guarantee that the lost data can be restored 100%. It depends on the real operation and the degree of physical damages on disks. Users assume all risk when attempting data recovery procedures.

Click the **Restore** button to restore the deleted volume in the pool. And then click the **Restore** button to proceed.

9.5. Data Encryption

Select the **System** tab and the **Data Encryption** subtab to provide **Data Encryption** and **SEDs** functions.

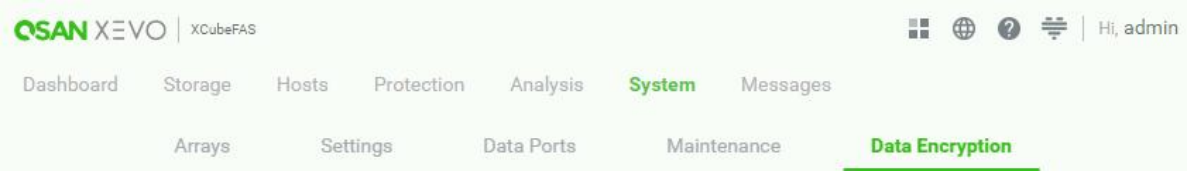


Figure 9-45 Data Encryption Subtab in the System Tab

For more information, please refer to the chapter 11.1, Configure Authentication Key section and chapter 11.2, Configure SEDs section.

10. Messages Tab

The **Messages** tab displays event logs and configures the notification settings. This chapter describes the details of message operations and examples.

10.1. Log Center

Select the **Messages** tab and the **Log** subtab to show event messages.

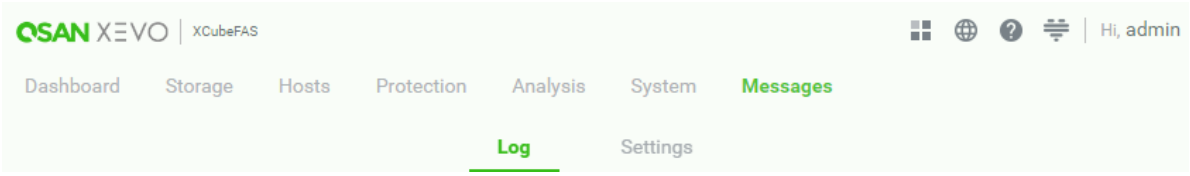


Figure 10-1 Log Subtab in the Messages Tab

Click All, or the icon (information), (warning), (error) to filter the event levels. The numbers next to the levels are the sum of the events.

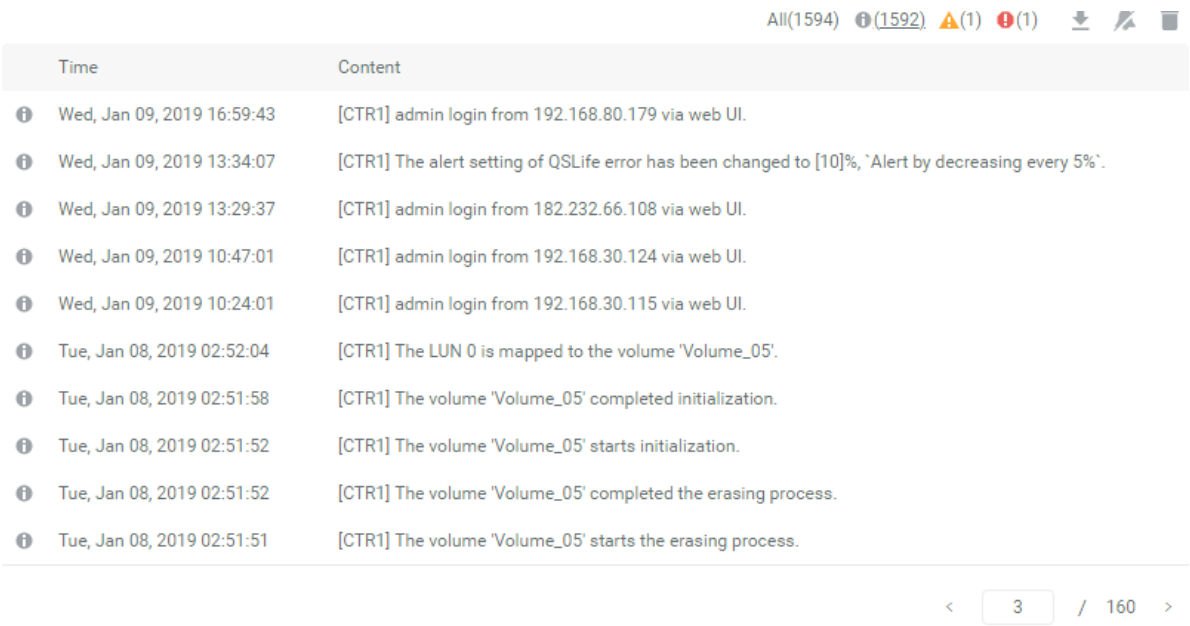


Figure 10-2 Event Logs

The event logs are displayed in reverse order which means the latest event log is on the first / top page. They are actually saved in the first four disk drives of the head unit, each disk drive has one copy of event log. For one system, there are four copies of event logs to make sure users can check event log any time when there are failed disks. If there are no disk drives in the first four slots, the event logs will keep in memory temporary and will disappear after system reboots.

The event logs record all system events. Each event has time frame that identifies the type of event that occurred, and has one of the following severities:

- **Error** : A failure occurred that may affect data integrity or system stability. Correct the problem as soon as possible.
- **Warning** : A problem occurred that may affect system stability, but not data integrity. Evaluate the problem and correct it if necessary.
- **Information** : An operation recorded that may help to debug.

The options are available in this pane.

Download Event Logs

Click the icon to save the event log as a file. It will pop up a filter dialog as the following.

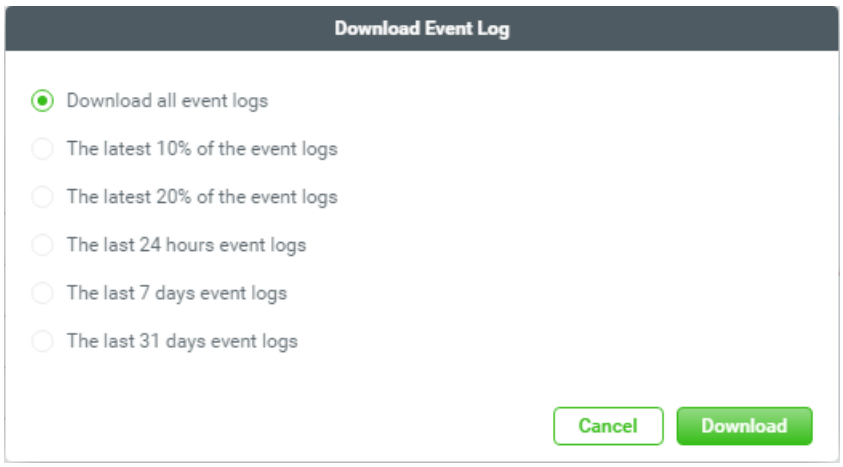


Figure 10-3 Download Event Logs

Select the options and then click the **Download** button to download event logs.

Mute Buzzer

Click the icon to stop alarm if the system alerts.

Clear Event Logs

Click the icon to clear all event logs.

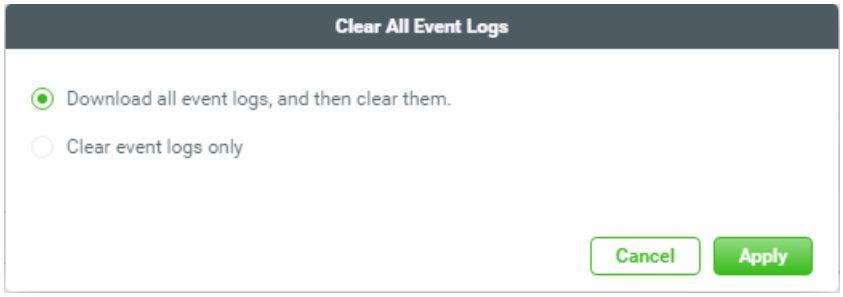


Figure 10-4 Clear All Event Logs

Select the options and then click the **Apply** button to clear event logs.

CAUTION:
Please plug-in any of the first four hard drives, then event logs can be saved and displayed in next system boot up. Otherwise, the event logs cannot be saved.

10.2. Configure Notification Settings

Select the **Messages** tab the **Settings** subtab to configure the notification settings via **Email**, **Alert** and **SNMP**.

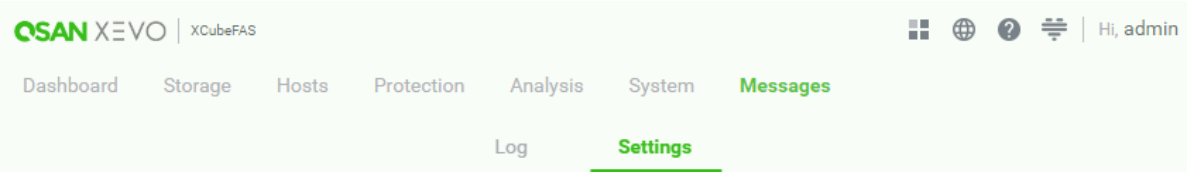


Figure 10-5 Settings Subtab in the Messages Tab

10.2.1. Email Settings

Click the **Email** pane to be used to enter up to three email addresses for receiving the event notifications.

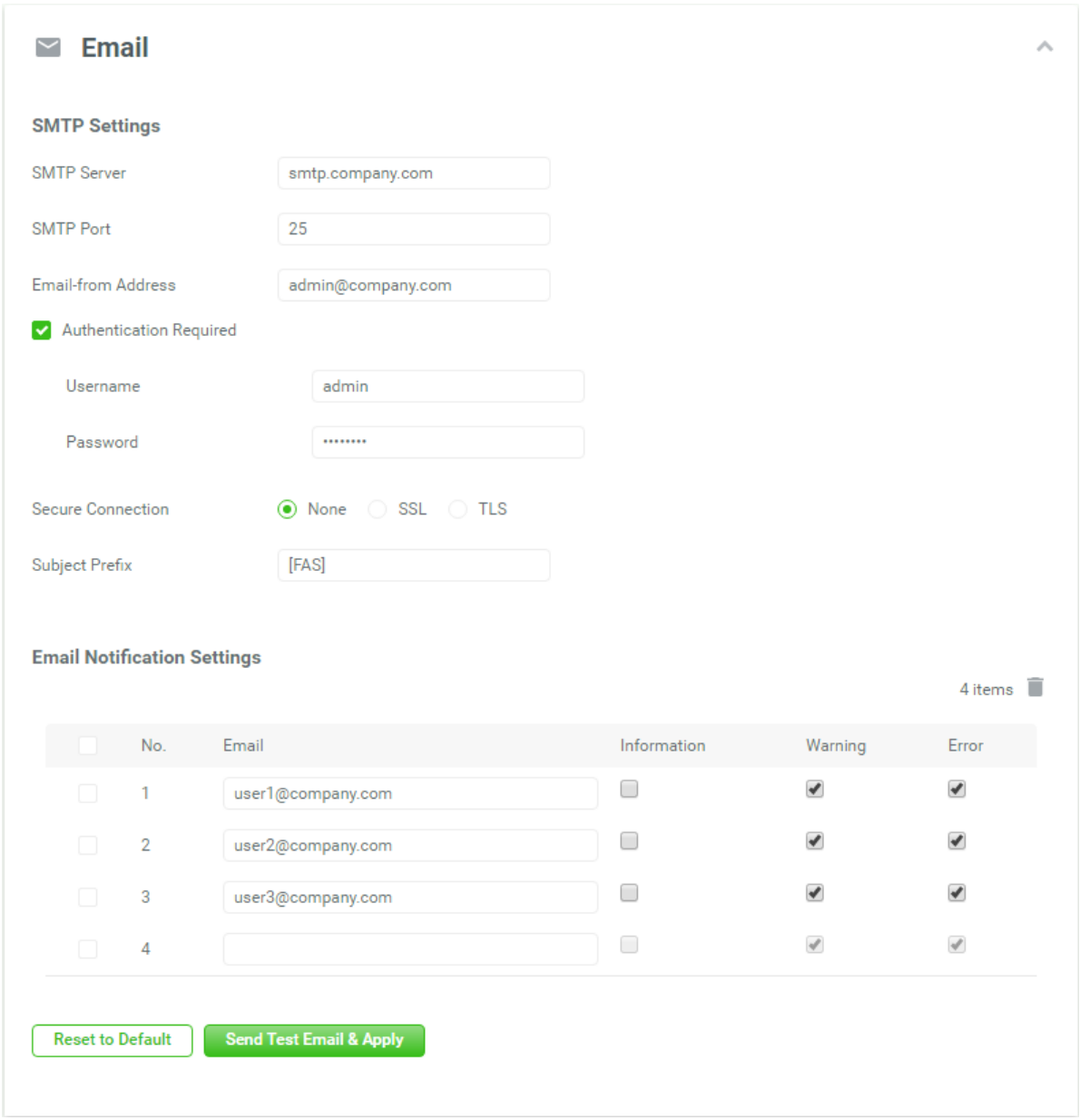


Figure 10-6 Email Settings

The options are available in this pane.

SMTP Settings

- **SMTP Server:** Enter the IP address or FQDN (Fully Qualified Domain Name) of SMTP server to deliver the notification mails.
- **SMTP Port:** Default is port 25. You can change the SMTP port here.
- **Email-from Address:** Enter the sender email address.
- **Authentication Required:** Some email servers require authentication for SMTP relay. Check to enable authentication and enter the **Username** and **Password**.
- **Secure Connection:** Using SSL (Secure Sockets Layer) or TLS (Transport Layer Security) for secure connection.
- **Subject Prefix:** The input string will be appended to the front of the email subject.

Email Notification Settings

- **Email-to-Address:** Enter the email address for receiving the event notifications. You can also select which levels of event logs which you would like to receive. The default setting only includes **Warning** and **Error** event logs.

TIP:
Please make sure the IP address of DNS server is well-setup in **Management Port**. So the event notification emails can be sent successfully. Please refer to the Confiture Management Port section for more details.

When finished, click the **Send Test Email & Apply** button to take effect. Or click the **Reset to Default** button to reset settings.

10.2.2. Alert Settings

Click the **Alert** pane to be used to setup alerts via alerts on the front display. The device buzzer is also managed here.

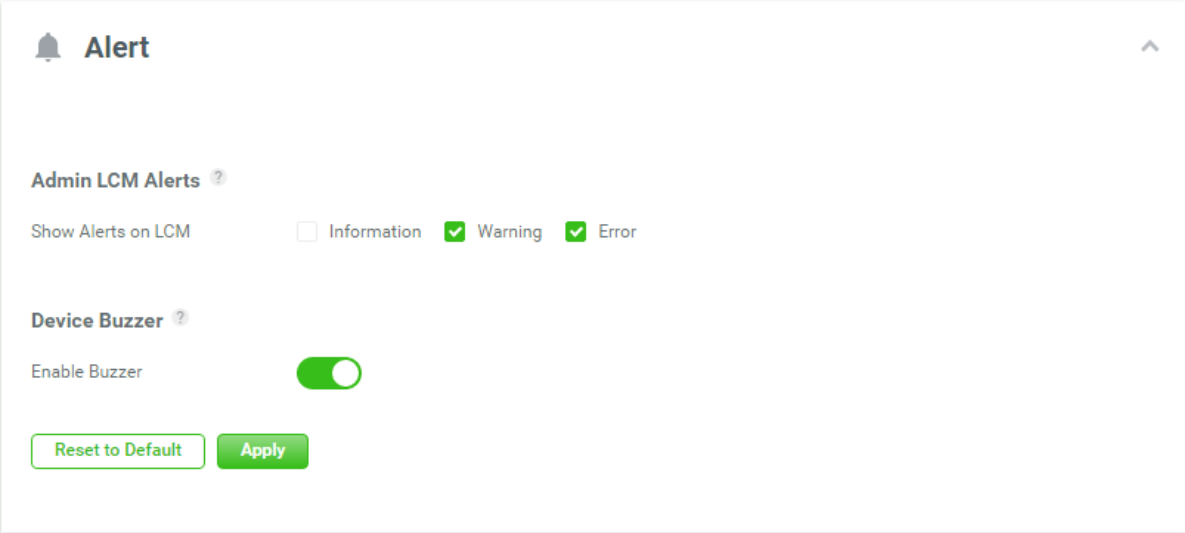


Figure 10-7 Alert Settings

The options are available in this pane.

Admin LCM Alerts

You can check or uncheck the alert levels which you would like to show on LCM.

Device Buzzer

Check it to enable the device buzzer. Uncheck it to disable device buzzer.

When finished, click the **Apply** button to tack effect. Or click the **Reset to Default** button to reset settings.

INFORMATION:

The device buzzer features are listed below:

- The buzzer alarms 1 second when system boots up successfully.
- The buzzer alarms continuously when there is error occurred. The alarm will be stopped after error resolved or be muted.
- The alarm will be muted automatically when the error is resolved. For example, when a RAID 5 pool is degraded and alarm rings immediately, user replaces one disk drive for rebuild. When the rebuild process is done, the alarm will be muted automatically.

10.2.3. SNMP Settings

Click the **SNMP** pane to be used to setup SNMP (Simple Network Management Protocol) traps for alerting with event logs and also setup SNMP server settings for client monitoring.

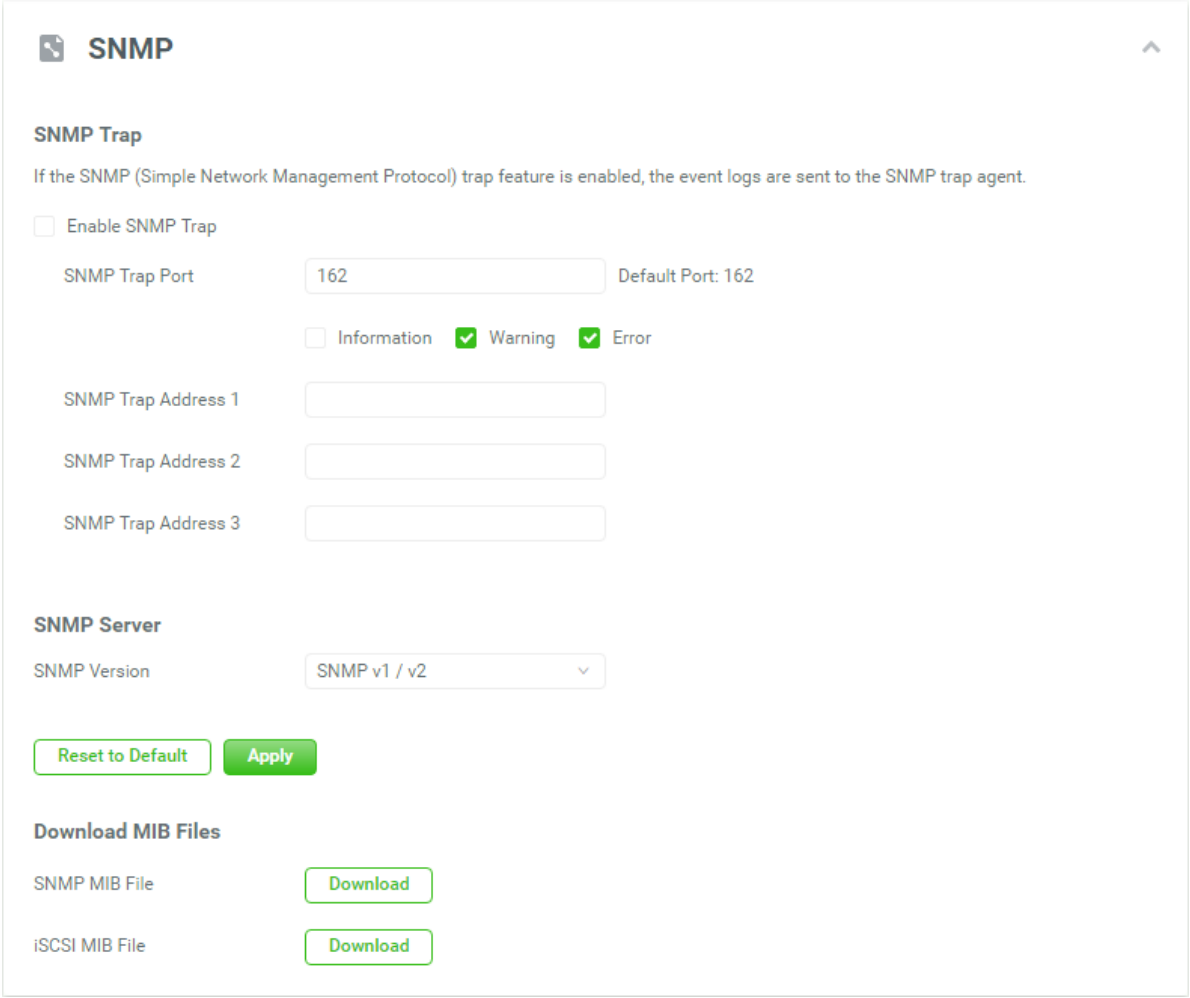


Figure 10-8 SNMP Settings

The options are available in this pane.

SNMP Trap

- **Enable SNMP Trap:** Check to enable SNMP trap to send system event logs to SNMP trap agent. The default SNMP trap port is 162. You can check or uncheck the alert levels which you would like to receive. And then fill in up to three SNMP trap addresses for receiving the event notifications.

SNMP Server

- **SNMP Version:** Select SNMP supported versions: v1/ v2, or v3. If select SNMP v3, it needs more options for authentication. Please enter a username, select an authentication protocol and enter an authentication password, check to use privacy if necessary, select a privacy protocol, and enter a privacy password.

When finished, click the **Apply** button to take effect. Or click the **Reset to Default** button to reset settings.

INFORMATION:
Authentication Protocol:

- **MD5:** The MD5 algorithm is a widely used hash function producing a 128-bit hash value. It can still be used as a checksum to verify data integrity, but only against unintentional corruption.
- **SHA:** SHA (Secure Hash Algorithm) is a cryptographic hash function which is a mathematical operation run on digital data; by comparing the computed "hash" (the output from execution of the algorithm) to a known and expected hash value, a person can determine the data's integrity.

Privacy Protocol:

- **DES:** The DES (Data Encryption Standard) is a symmetric-key algorithm for the encryption of electronic data.
- **AES:** The AES (Advanced Encryption Standard) is a specification for the encryption of electronic data. It supersedes the DES.

Download MIB Files

- **SNMP MIB File:** Click the **Download** button to save the SNMP MIB file which can be imported to the SNMP client tool to get system information. You can view fan, voltage, and system status via SNMP MIB.
- **iSCSI MIB File:** Click the **Download** button to save the iSCSI MIB file which can be imported to the SNMP client tool to get network information. You can view iSCSI traffic via iSCSI MIB.

11. SED and ISE Support

With data security issues at the time, the company places a high priority on ensuring that sensitive data is protected from unauthorized access. Whether it is due to internal policies or external compliance, access to data remains a matter of high importance for all organizations. These organizations will seek out storage manufacturers that provide a stored data protection method, SED (Self-Encrypting Drive), that has both authentication and encryption features.

In addition, ISE (Instant Secure Erase) drive is designed to protect data on hard disk drives by instantly resetting the drive back to factory settings and changing the encryption key so that any data remaining on the drive is cryptographically erased. This means all data on the drive is permanently and instantly unreadable, as needed.

INFORMATION:
SED (Self-Encryption Drive) and ISE (Instant Secure Erase) drive support is available in XEVO firmware 1.1.0.

11.1. Configure Authentication Key

This section will describe the operations of enabling an AK. Select the **System** tab and the **Data Encryption** subtab, and then click the **Disk Encryption** pane to configure the AK.

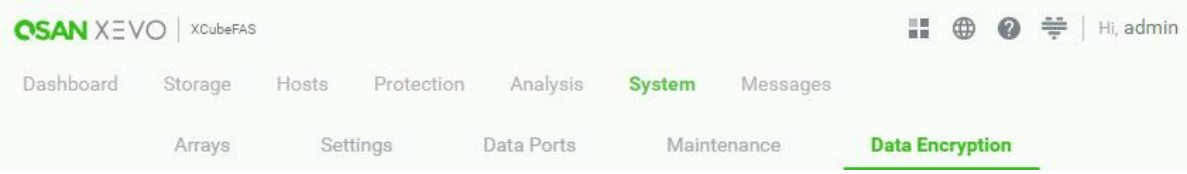


Figure 11-1 Disk Encryption Subtab in the System Tab

11.1.1. Operations on Authentication Key

The options are available in this pane.

Enable Authentication Key

Before using SED, you have to enable an AK. Note that all SEDs in the system use this AK. Here is an example of enabling an AK.

1. Click the **Disk Encryption** pane to enable an **Authentication Key**.

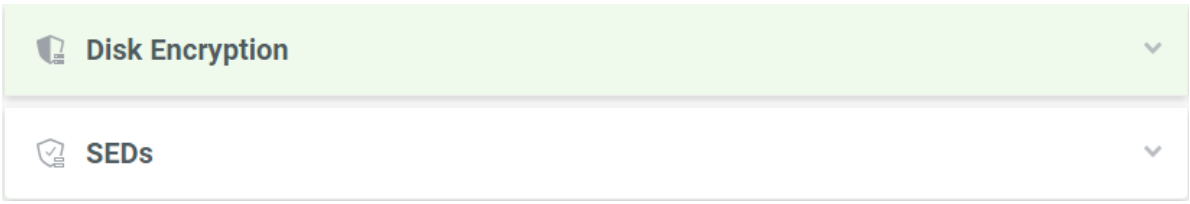


Figure 11-2 Disk Encryption Pane

2. Click the **Enable Authentication Key** switch to ON (Enable) to enable.

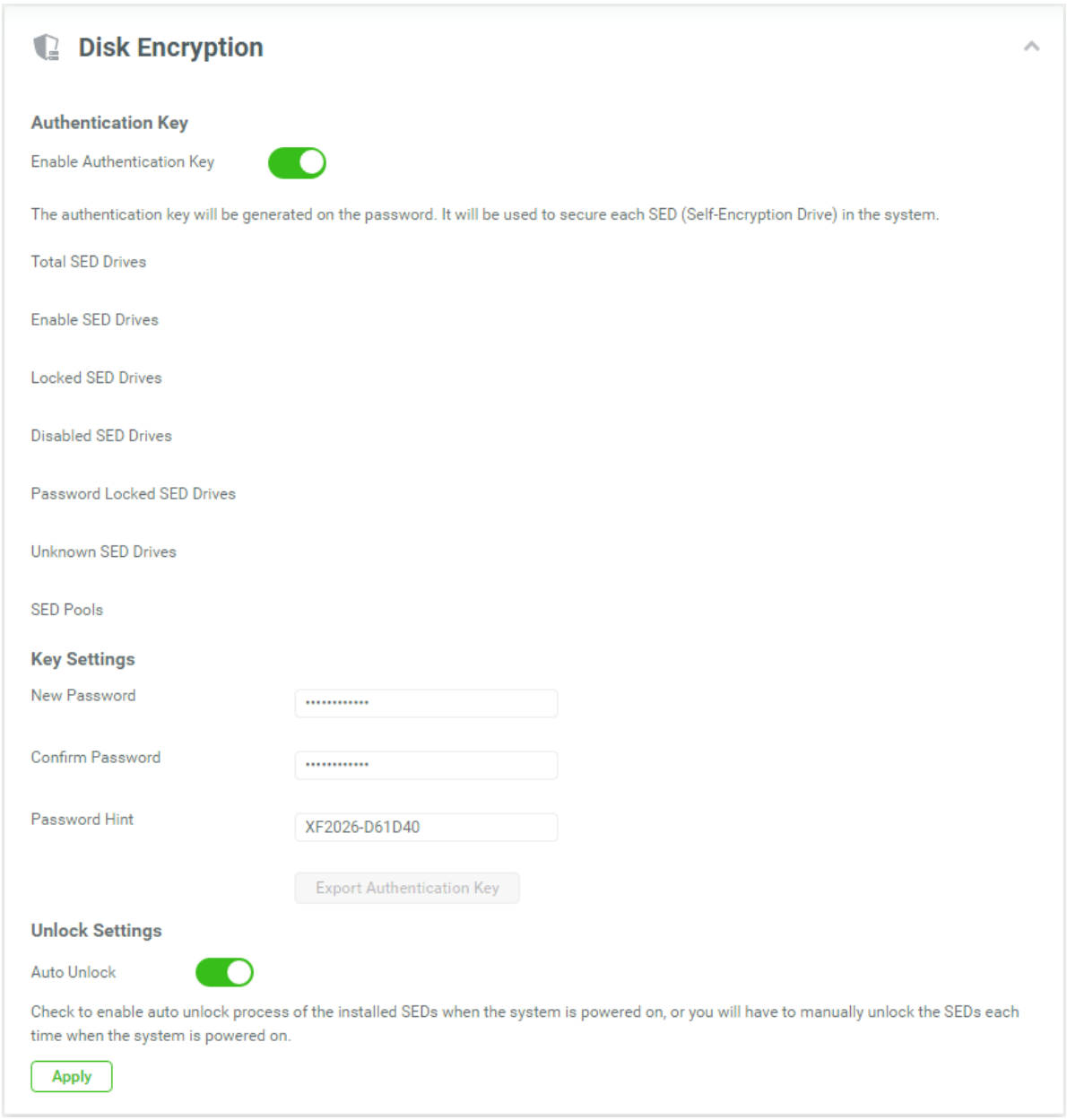


Figure 11-3 Enable Authentication Key

3. Enter a **Password** for generating the AK. The length of the password is between 4 to 12 characters. Valid characters are [A~Z | a~z | 0~9 | ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/]. And enter it again at **Confirm Password**.
4. Enter a **Password Hint**. It is the AK hint for recognizing the system. The default value is system name and can be changed. The maximum length of the password hint is 32 characters. Valid characters are [A~Z | a~z | 0~9 | _-].

5. Click the **Enable Auto Unlock** switch will enable auto unlock process of the installed SEDs when the system is powered on, or you will have to manually unlock the SEDs each time when the system is powered on. The default value is enabled.
6. Click the **Apply** button to enable.

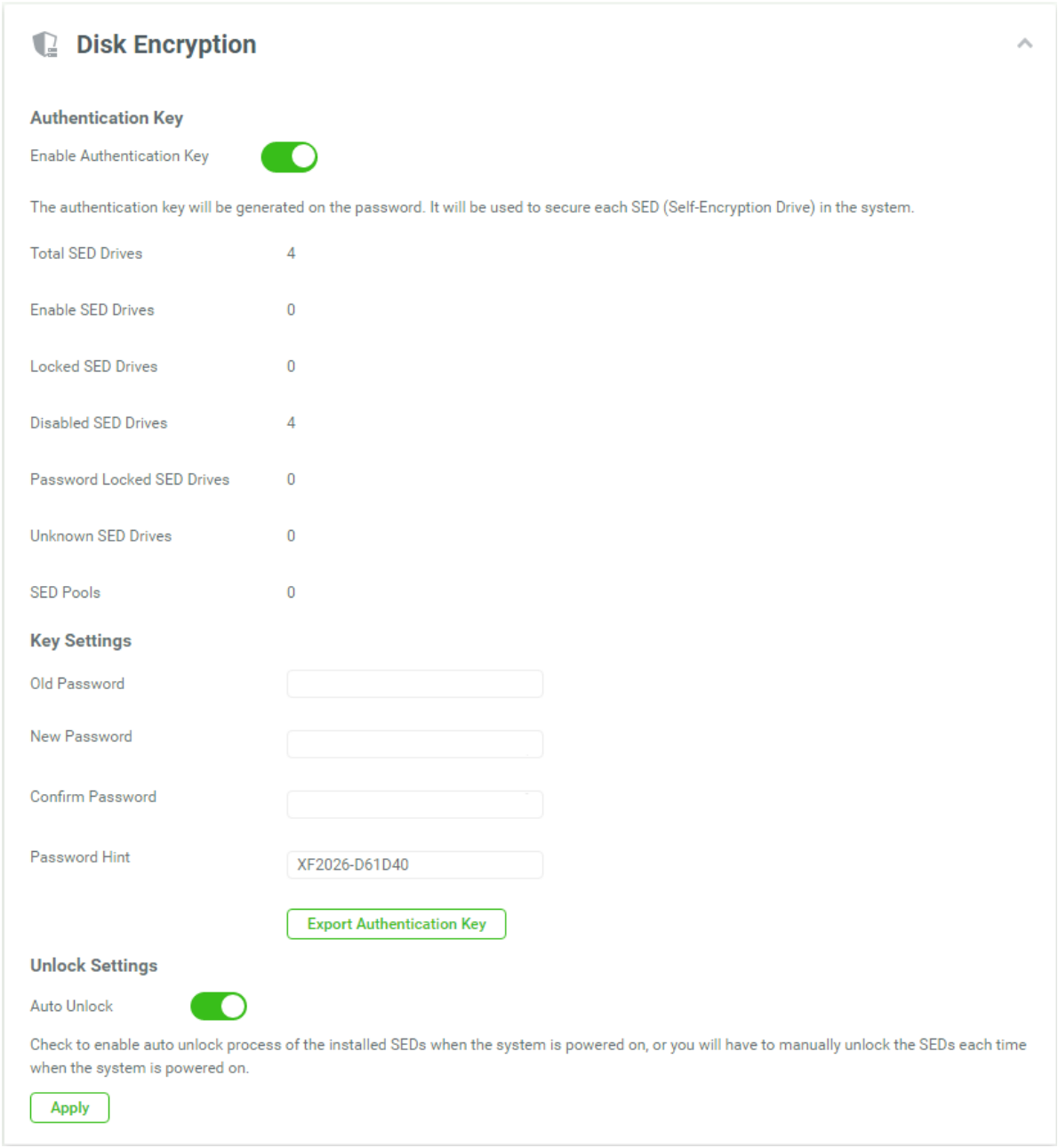


Figure 11-4 Authentication Key is Enabled

After the AK is enabled fully, there are SED summary displayed in the page. In addition, **Auto Unlock** option can also be changed here. You can click the **Enable Auto Unlock** switch and then click the **Apply** button to take effect.

Export Authentication Key

After enabling the AK successfully, please click the **Export Authentication Key** button to export the AK file to an external media (e.g.: external disk drive, USB drive, etc.) and store it in a safe location. You must be able to use the AK file to recover in case of an unforeseen event.

TIP:
Recommend backup the key, or you risk losing all data on the SEDs.

1. Enter a file name to export the AK file. The default vale is the password hint plus date and time.
2. Click the **Save** button to export.

Change Authentication Key

Enter the **Old Password**, **New Password**, **Confirm Password**, and click the **Apply** button to change the AK. Before changing the AK, please stop all I/O of the encryption pools within the SEDs. The new AK will be regenerated based on the new password and set the new authentication key to all enabled SEDs in the system. If the I/O are still running, it may risk losing data during changing the AK.

Disable Authentication Key

If you no longer use disk encryption and there are no encryption pools within the SEDs. The AK can be disabled. Click the **Enable Authentication Key** switch to  OFF (Disable), and then click the **Apply** button to disable.

TIP:
The **Disable Authentication Key** function can be operated when there is no encryption pools within the SEDs and the SED status of all SEDs is disabled or unknown.

11.2. Configure SEDs

The **SEDs** pane in the **Data Encryption** subtab is only active when the AK is enabled. Click the **SEDs** pane to display the status of SEDs, initiate SEDs, unlock SEDs, or erase SEDs.

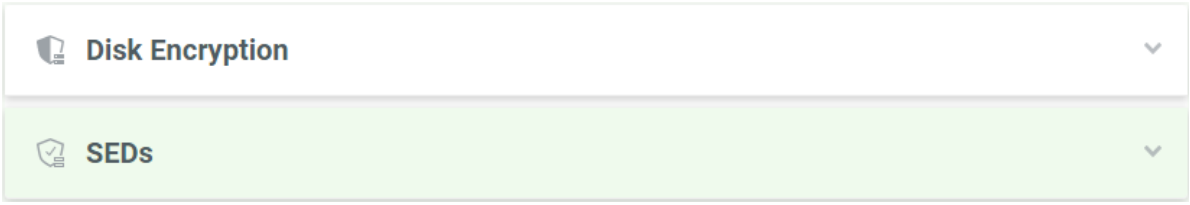


Figure 11-5 SEDs Pane

11.2.1. List SEDs

The drop-down lists at the top enable you to select the enclosure from head unit (FAS system) or expansion units (expansion enclosures).

TIP:
Enclosure format: Enclosure ID ([Head Unit | Expansion Unit]: Model Name). For example: 0 (Head Unit: XF2026), 1 (Expansion Unit: XD5326)

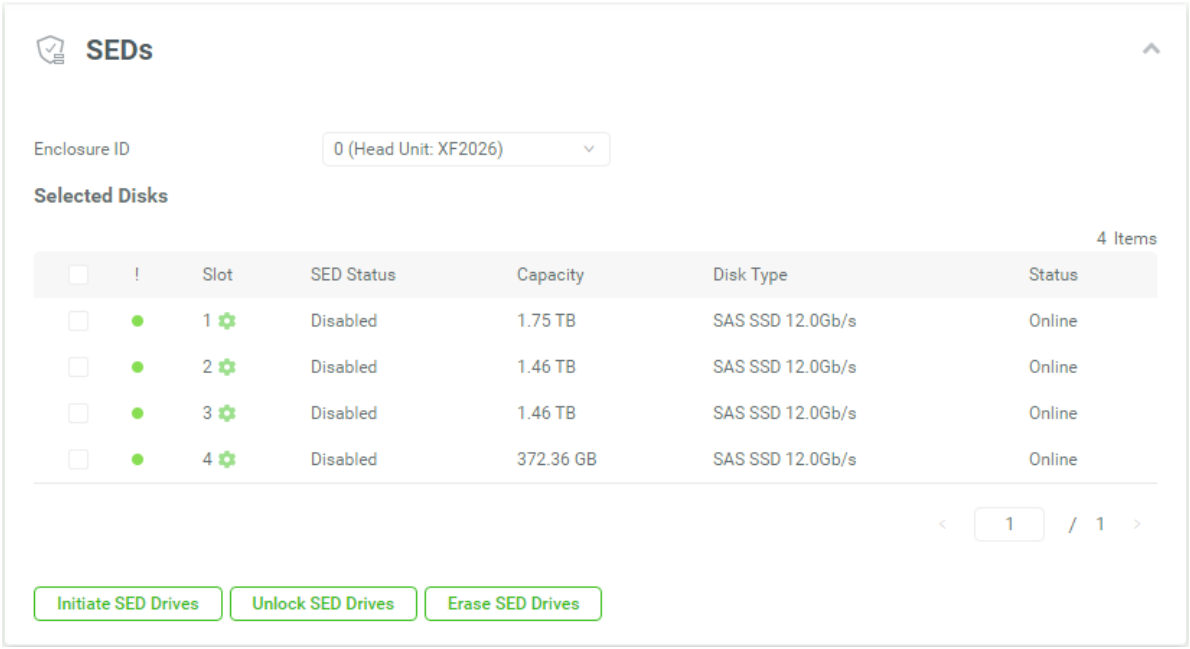


Figure 11-6 List SEDs

This table shows the column descriptions.

Table 11-1 Disk Column Descriptions

Column Name	Description
!	The status of disk health: • Green Color / Normal: The disk drive is good. • Orange Color / Abnormal: The disk drive has unrecoverable read errors or S.M.A.R.T. error. • Red Color / Warning: The disk drive has failed.
Slot	The position of the disk drive.
SED Status	The status of the SED: • Enabled: The SED is enabled. • Locked: The SED is locked. It must be unlocked by the correct AK before it can be used. • Disabled: The SED is disabled. It must be initiated before it can be used. • Password Locked: The SED is locked by entering the incorrect password too many times. • Unknown: The SED is unknown. • Initiating: The SED is being initiated.

	• Unlocking: The SED is being unlocked. • Erasing: The SED is being erased. • Changing Key: The SED is being changed the key.
Capacity	The capacity of the disk drive.
Disk Type	The type of the disk drive: • [SAS HDD | NL-SAS HDD | SAS SSD | SATA SSD] • [12.0Gb/s | 6.0Gb/s | 3.0Gb/s | 1.5Gb/s]
Status	The status of the disk drive: • Online: The disk drive is online. • Rebuilding: The disk drive is being rebuilt. • Transitioning: The disk drive is being migrated or is replaced by another disk when rebuilding occurs. • Scrubbing: The disk drive is being scrubbed. • Check Done: The disk drive has been checked the disk health.

11.2.2. Operations on SEDs

The options are available in this pane.

Initiate SEDs

Select SEDs and then click the **Initiate SED Drives** button to initiate the selected SEDs.

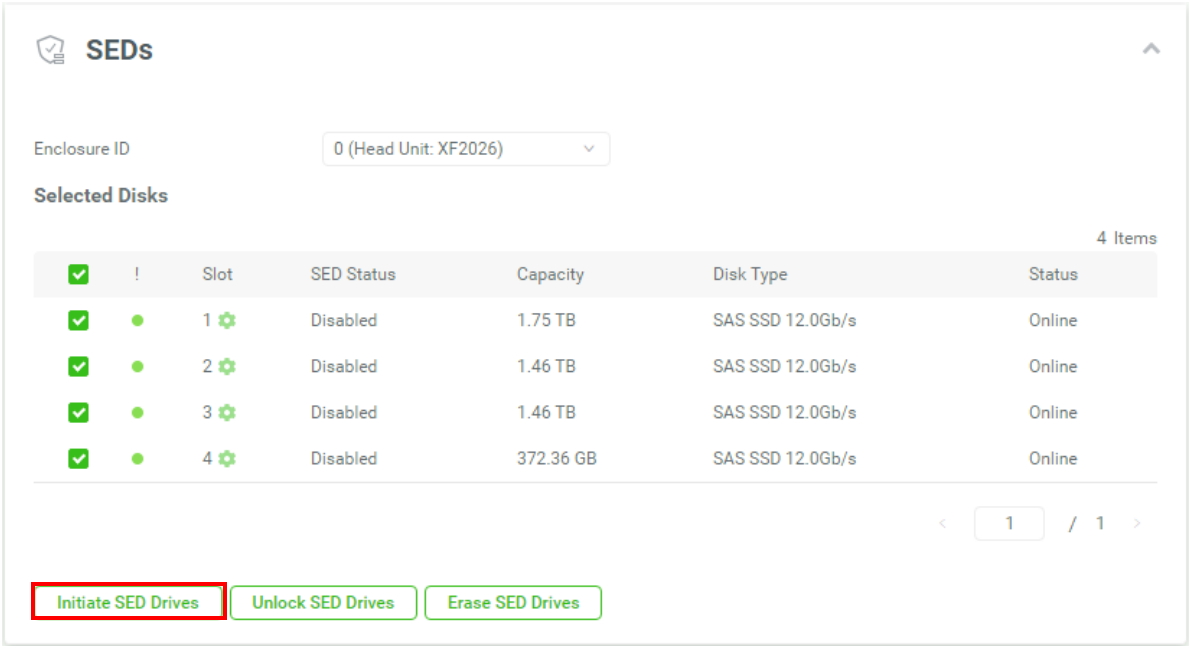


Figure 11-7 Initiate SEDs

After proceeding, it will pop up a dialog to display the results.

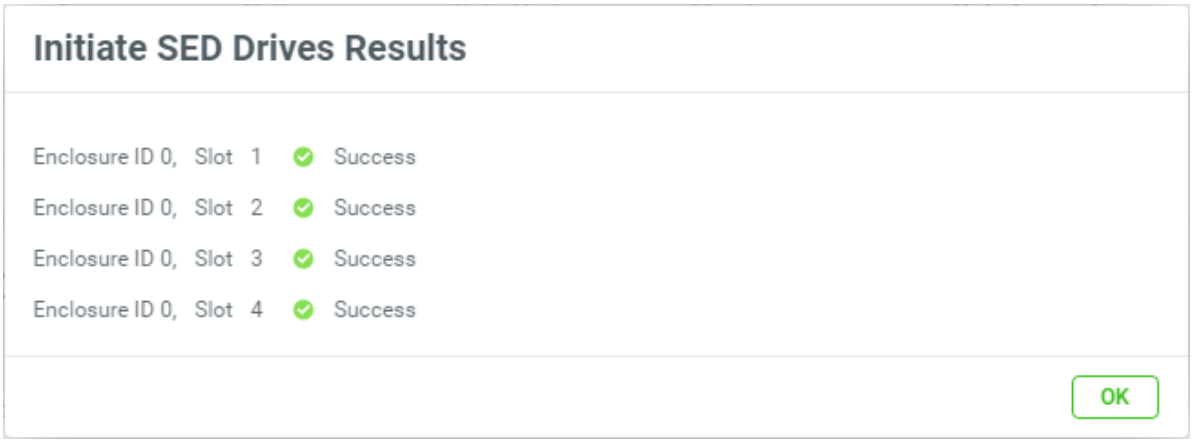


Figure 11-8 Initiate SED Results

If the results are successful, the SED status will become Enabled.

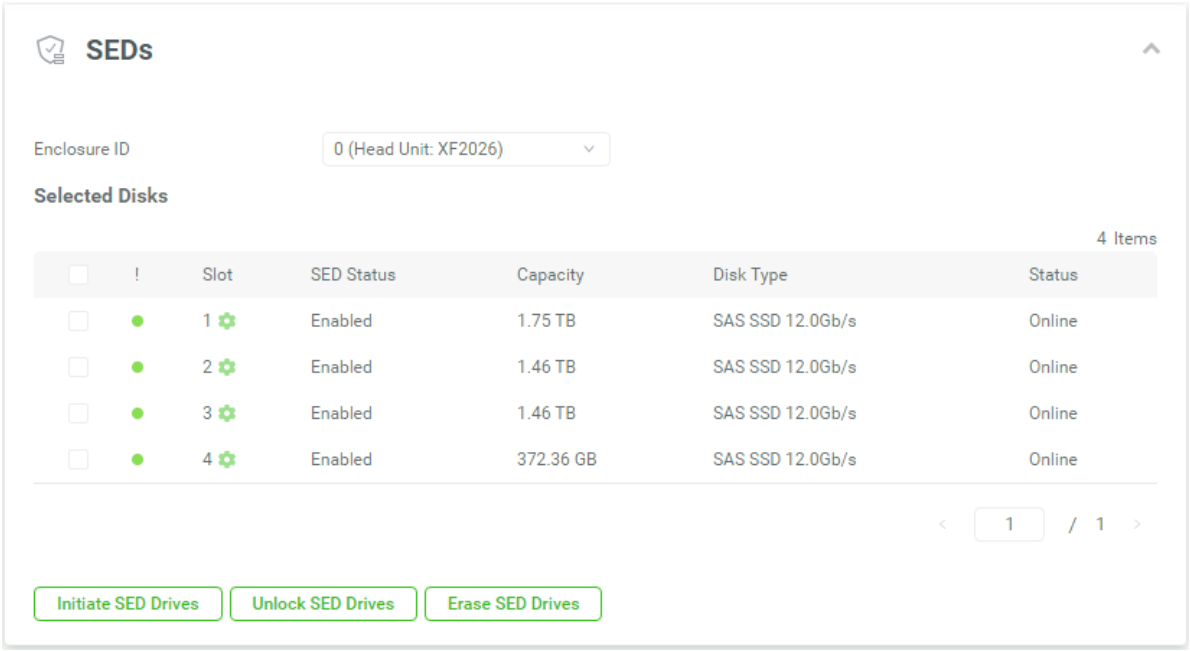


Figure 11-9 List SEDs

TIP:
The **Initiate SED Drives** function can be operated when the usage status of SEDs is free and the SED status is Disabled.

Unlock SEDs

Select SEDs and then click the **Unlock SED Drives** button to unlock the selected SEDs.

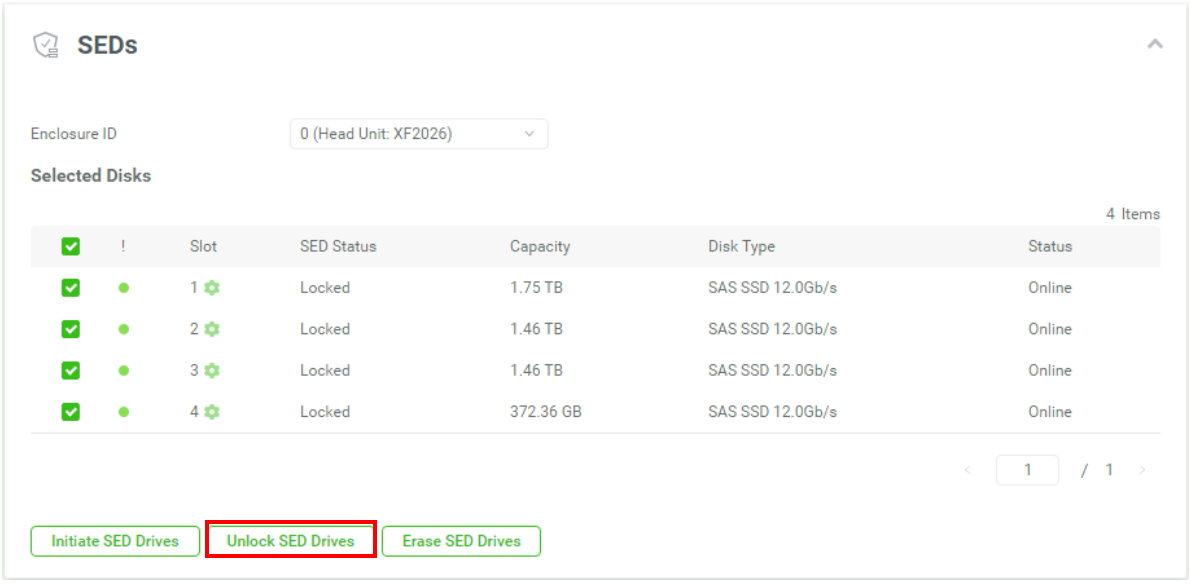


Figure 11-10 Unlock SEDs

You can select the **Use the Authentication Key of the Current System** to unlock the SEDs. Or if the SEDs are roamed from other systems, they will be unlocked with their AKs, and then being replaced by the AK of the current system. In this case, please select the **Enter an Authentication Key Password** or **Import and Authentication Key File** to unlock the SED.

TIP:
The **Unlock SED Drives** function can be operated when the SED status of SEDs is Locked.

Erase SEDs

If there are no encryption pools within the SEDs, these SEDs can be erased. Select SEDs and then click the **Erase SED Drives** button to erase the selected SEDs.

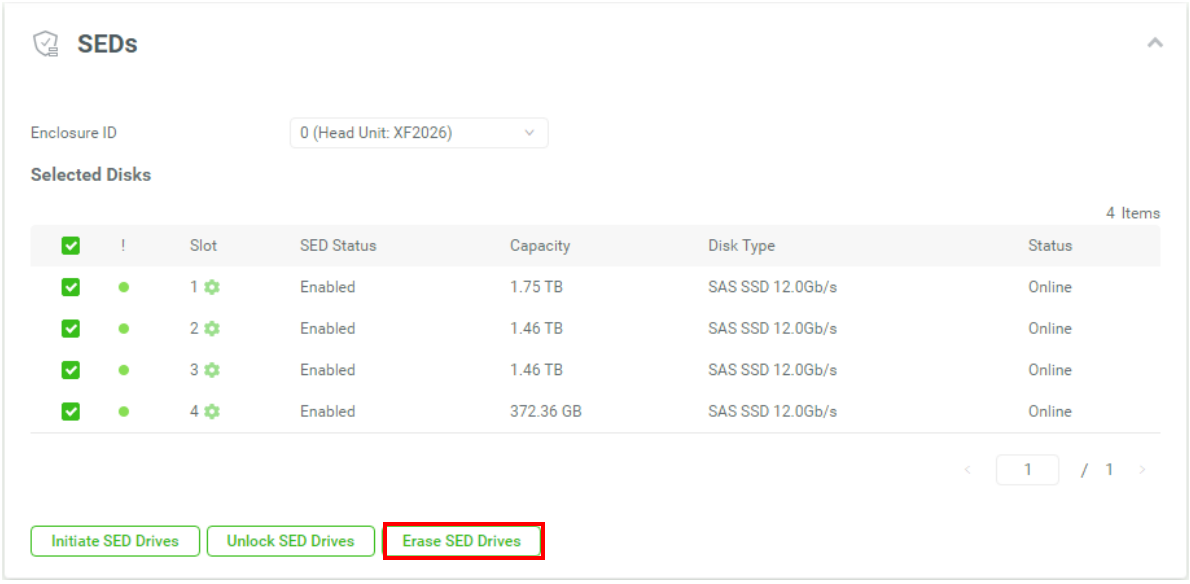


Figure 11-11 Erase SEDs

After proceeding, it will pop up a dialog to display the results. If the results are successful, the SED status will become Disabled.

TIP:
The **Erase SED Drives** function can be operated when the usage status of SEDs is free.

CAUTION:
Erasing the SEDs will change the DEK and delete all data on the SED. The data on SED can never be restored, please exercise caution.

Erase SED by PSID

If you don' know where the SED comes from, or the status of the SED is unknown and you don't know its password. The last method is to erase the SED by PSID (Physical Secure ID) which is on the label of the disk drive. Click the ⚙ icon beside the slot number of the specific disk drive and click the **Erase SED by PSID** option to erase the SED by PSID.

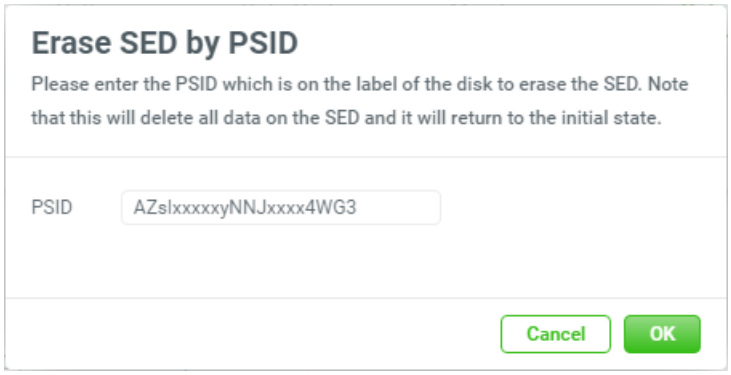


Figure 11-12 Erase SED by PSID

TIP:
The **Erase SED by PSID** function can be operated when the usage status of the SED is free.

CAUTION:
Erasing the SED by PSID will delete all data on the SED and it will return to the initial state. The data on SED can never be restored, please exercise caution.

11.3. Configure SED Pools

Select the **Storage** tab to manage the storage pools. In this tab, you can create, modify, delete, or view the status of all pools.

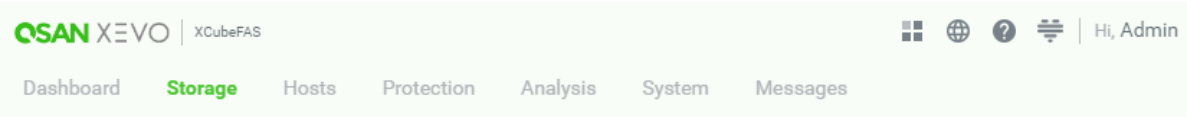


Figure 11-13 Storage Tab

11.3.1. Create an SED Pool

Here is an example of creating an SED pool with 3 SEDs configured in RAID 5. At the first time of creating a pool, it contains a disk group and the maximum quantity of disk in a disk group is 64.

1. Click the ✚ icon in the **Pools** pane to pop up a wizard. Switch the **Enable SED Pool** to ON (Enable).

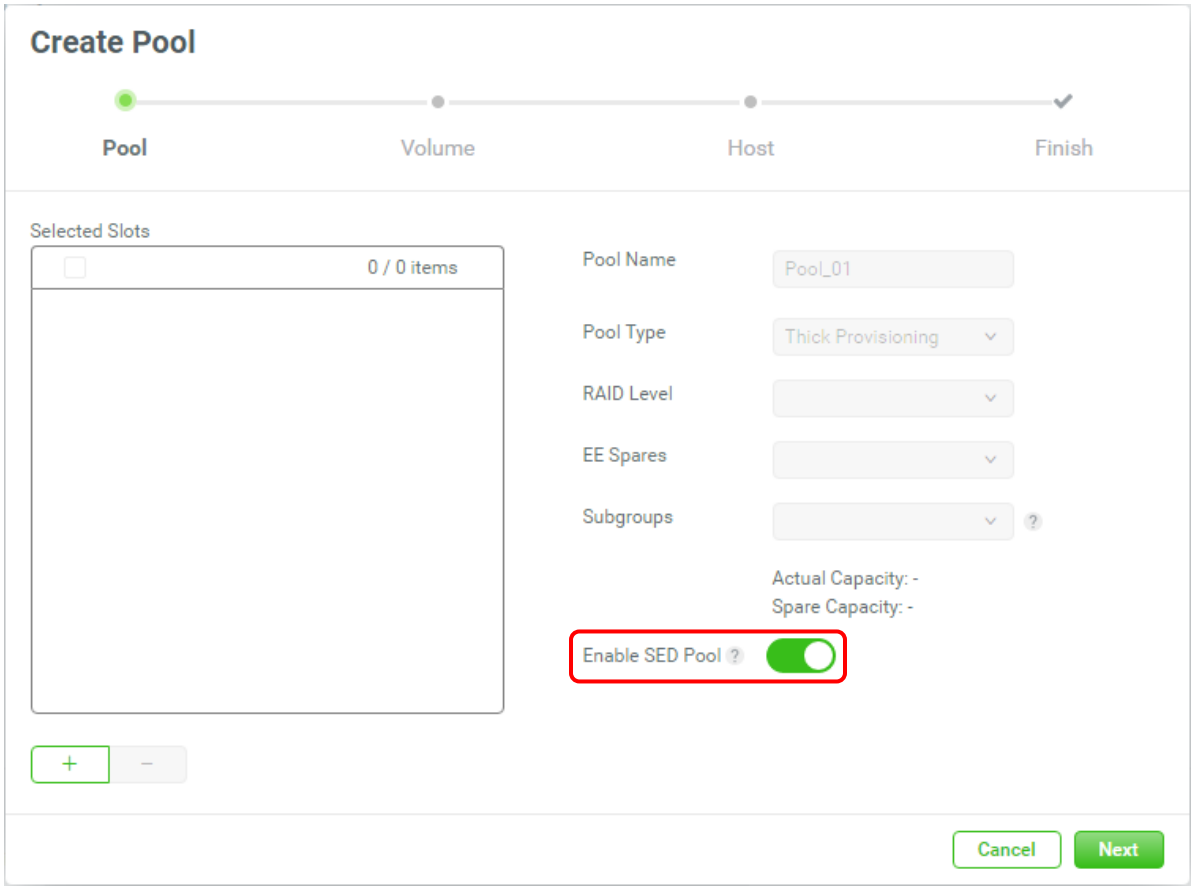


Figure 11-14 Create an SED Pool Step 1

2. Click the + icon to select disks to add into the pool.

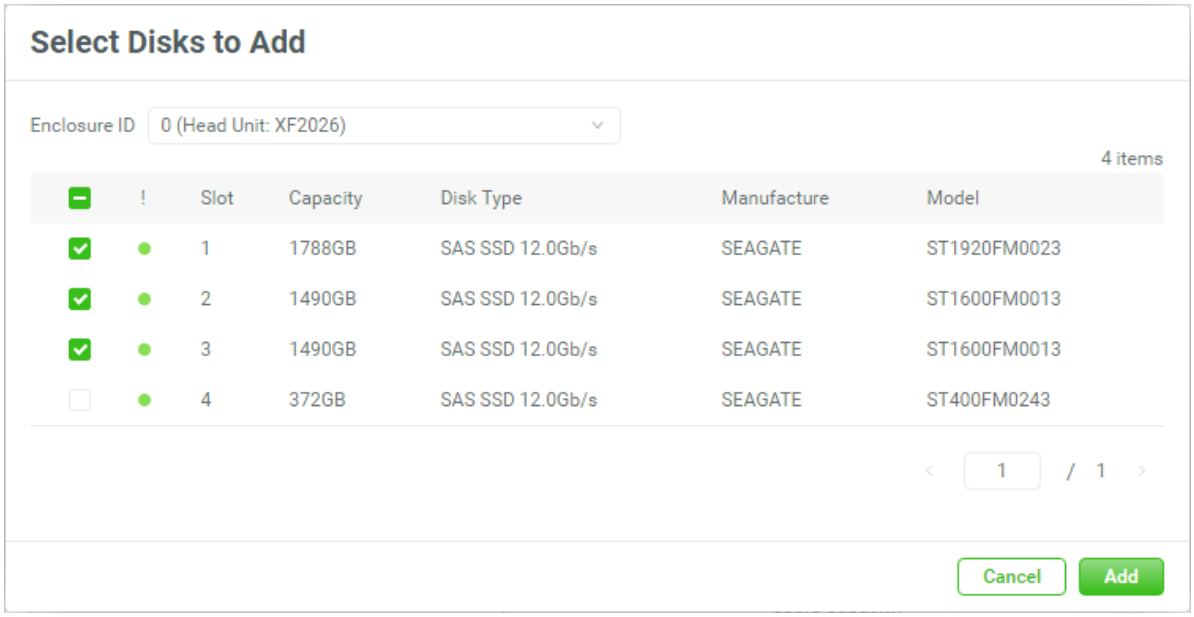


Figure 11-15 Select Disks to Add

3. Check disk slots which you want to add. The maximum quantity of disk in a disk group is 64. Select an **Enclosure ID** from the drop-down list to select disks from expansion enclosures. Then click the **Add** button to continue.

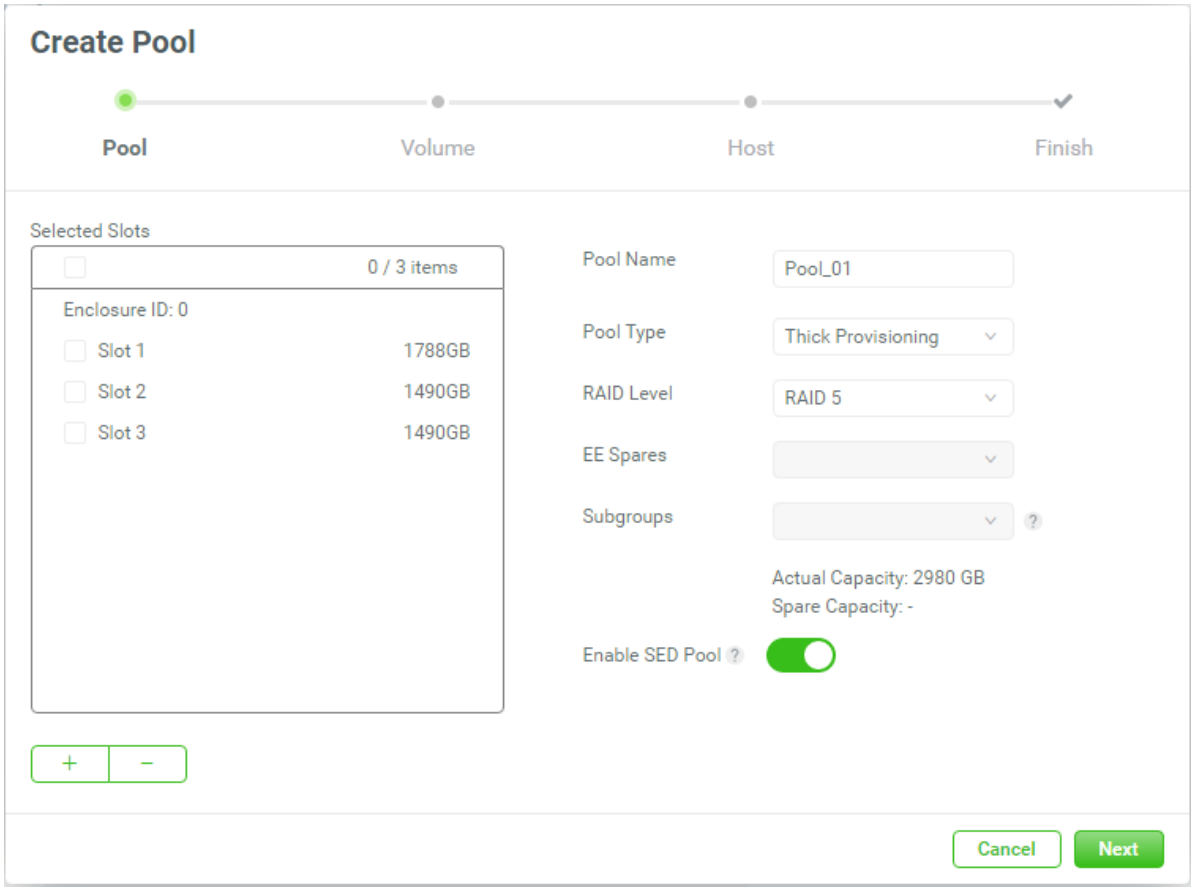


Figure 11-16 Create a Pool Step 1-2

4. The selected disk slots are listed in the box and can be removed. Check disk slots which you want to remove and then click the − button.
5. The recommended **Pool Name**, **Pool Type**, and **RAID Level** are provided. Enter a new **Pool Name** if necessary. The maximum length of the pool name is 16 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
6. Change the **Pool Type** with the drop down options. There are Thick Provisioning, and Thin Provisioning options.
7. The recommended **RAID Level** depends on the number of disks you select. The same, it can be changed with the drop down options.
8. Select the RAID EE **Spares** if you select the RAID EE level. Select the **Subgroups** if you select the compound RAID level.
9. Click the **Next** button to continue.

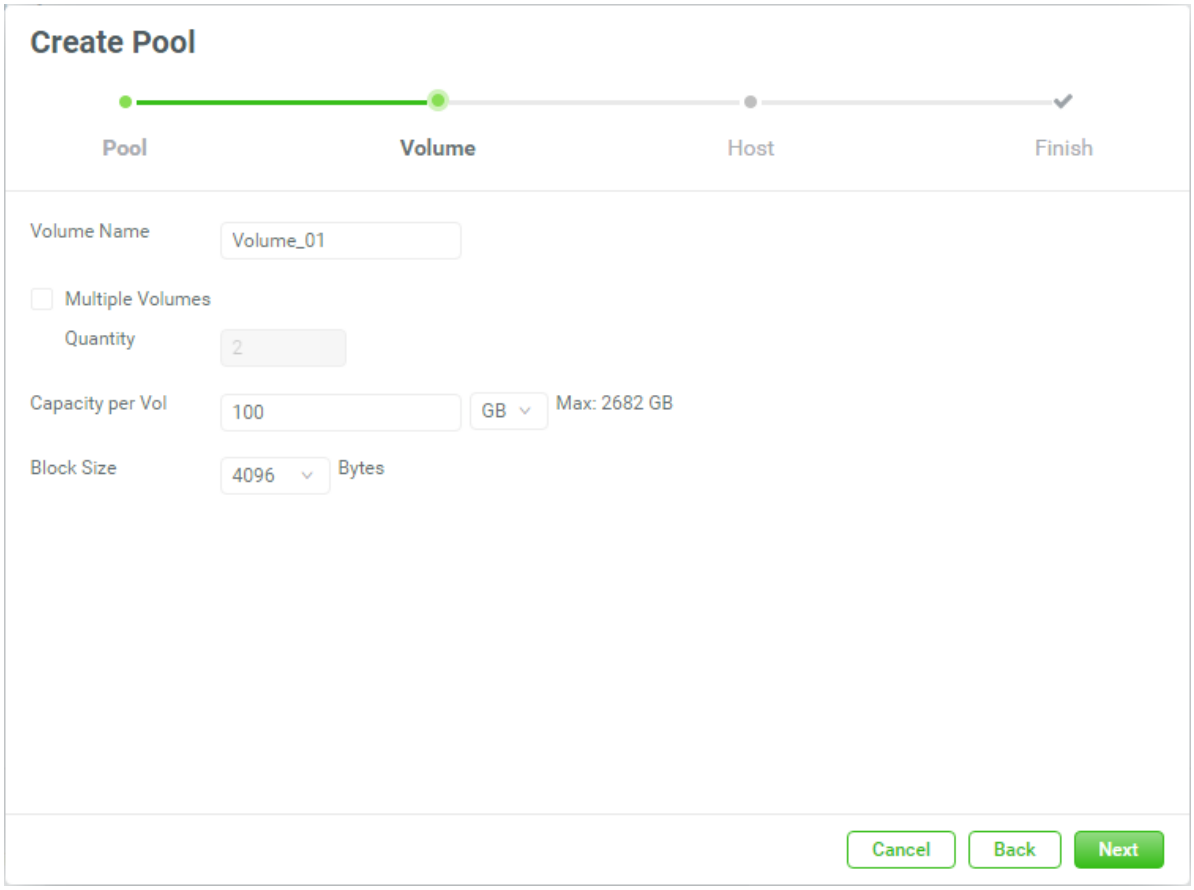


Figure 11-17 Create a Pool Step 2

10. The recommended **Volume Name**, **Capacity per Vol**, and **Block Size** are provided. Enter a new **Volume Name** if necessary. The maximum length of the volume name is 32 characters. Valid characters are [A~Z | a~z | 0~9 | -_<>].
11. Check the **Multiple Volumes** checkbox if you want to create multiple volumes at once. Then enter a number for **Quantity**. The maximum quantity is 64.
12. The recommended **Capacity per Vol** is the maximum capacity which can be created. Change it if necessary. At this time, change it to 100GB.
13. Change the **Block Size** with the drop down options. The options are 512 Bytes to 4,096 Bytes.
14. Click the **Next** button to continue.

TIP:
The system automatically reserves 10% of the pool capacity for snapshot space.

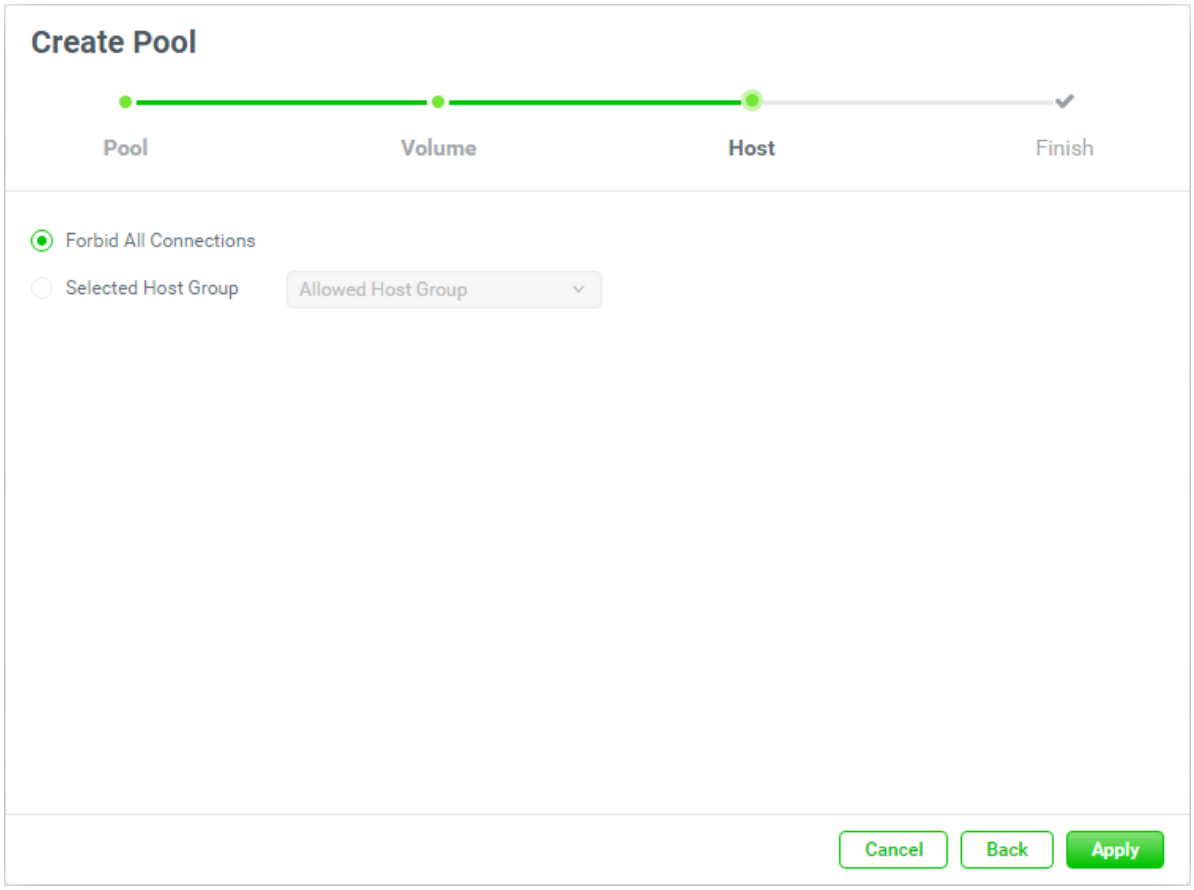


Figure 11-18 Create a Pool Step 3

15. If there are host groups which are created already, check the **Selected Host Group** checkbox and select a host group with the drop down options. Or keep it default as **Forbid All Connections** and change it later.
16. Click the **Apply** button to continue.

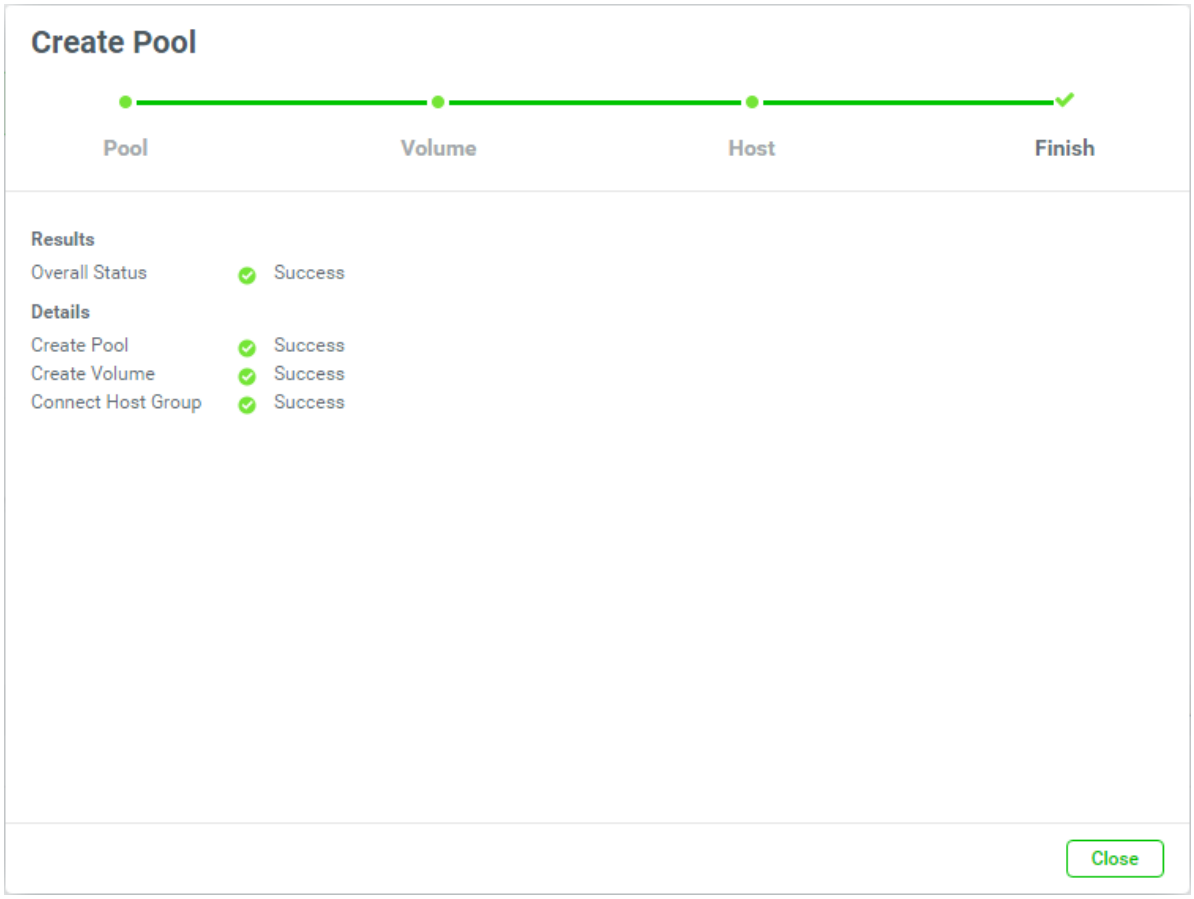


Figure 11-19 Create a Pool Step 4

17. There is a result page. Click the **Close** button to finish.

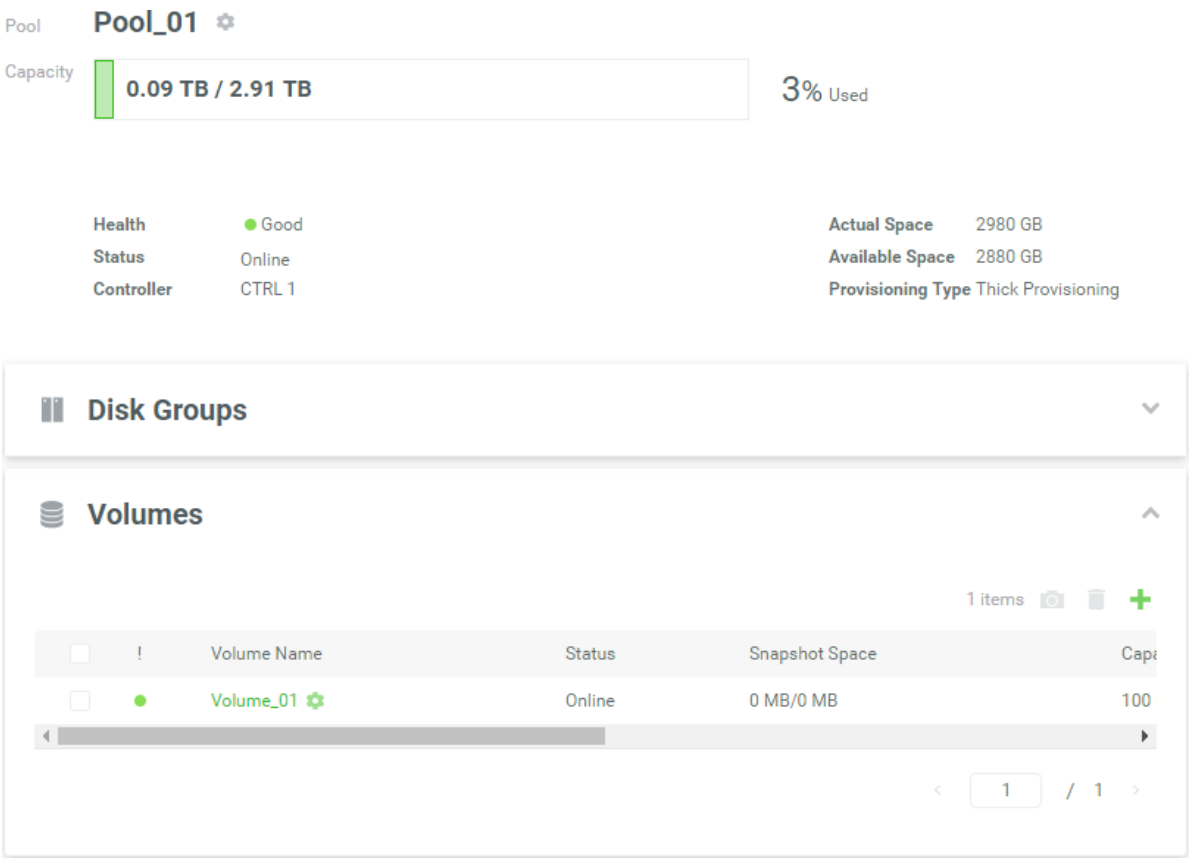


Figure 11-20 An SED Pool is Created

18. An SED pool with a volume has been created. If necessary, click the ✚ icon in the **Pools** pane to create others.

11.3.2. Operations on SED Pools

Most operations are described in the Configuring Storage Pools section in the XEVO Software Manual. We describe the restrictions about SED pool in the following.

Add a Disk Group

Click the ✚ icon in the **Disk Groups** pane to add a disk group. Disks can only choose SEDs. Select SEDs and then click the **Apply** button.

Migrate Disk Group *(Only visible when the pool type is thick provisioning)*
Click the ⚙ icon beside the slot number of the specific disk group and click the **Migrate Disk Group** option to migrate the disk group. Disks can only choose SEDs. Select SEDs and then click the **Apply** button.

Replace Disk Group *(Only visible when the pool type is thin provisioning)*
Click the ⚙ icon beside the slot number of the specific disk group and click the **Replace Disk Group** option to replace the disk group. Disks can only choose SEDs. Select SEDs and then click the **Apply** button.

11.3.3. Rebuild on SED Pools

Rebuilding an SED pool will use SED as spare disk.

11.3.4. Data Backup on Encrypted Volumes

Most operations are described in the Data Backup chapter in the XEVO Software Manual. We describe the tips about data backup on encrypted volumes in the following.

Local Clone on Encrypted Volume
If executing local clone from an encrypted volume to a non-encrypted volume, it will pop up a warning message.

Remote Replication on Encrypted Volume
If executing remote replication from an encrypted volume, It will pop up a warning message.

11.4. Configure ISE Drives

Click the **Disk Services** pane in the **Maintenance** subtab to display the status of the ISE drives.

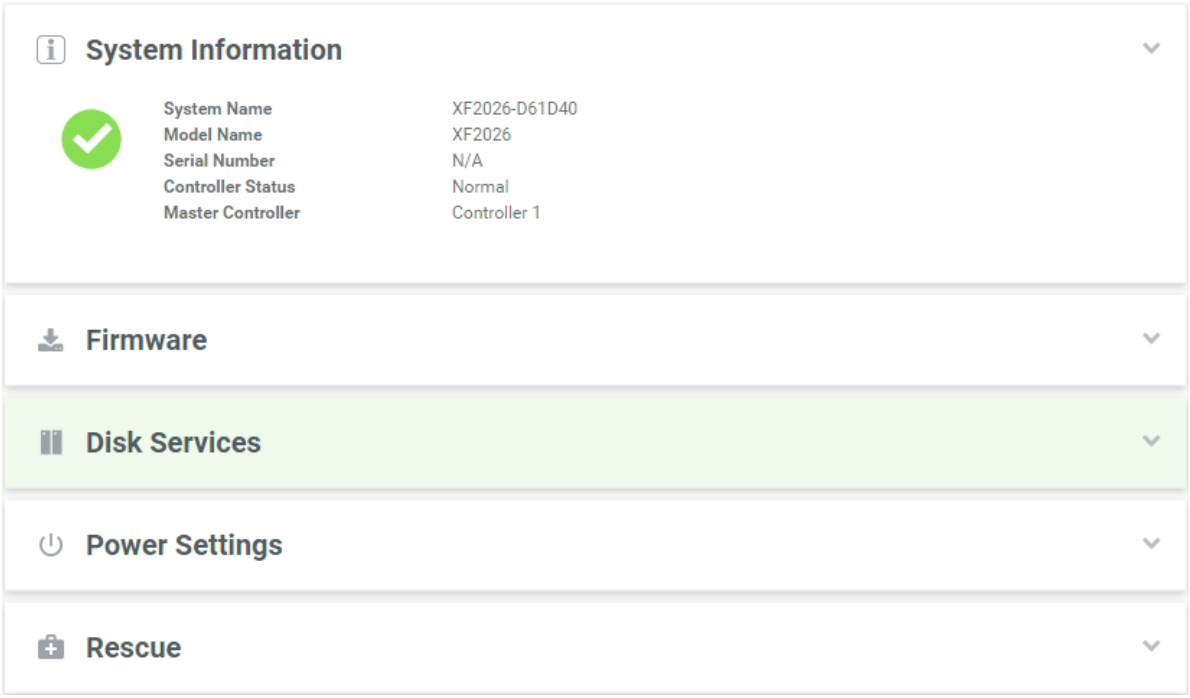


Figure 11-21 SEDs Pane

This section will describe the operations of configuring ISE drives. They can only be operated by instant erased.

11.4.1. List ISE Drives

The drop-down lists at the top enable you to select the enclosure from head unit (FAS system) or expansion units (expansion enclosures).

TIP:
Enclosure format: Enclosure ID ([Head Unit | Expansion Unit]: Model Name). For example: 0 (Head Unit: XF2026), 1 (Expansion Unit: XD5326)

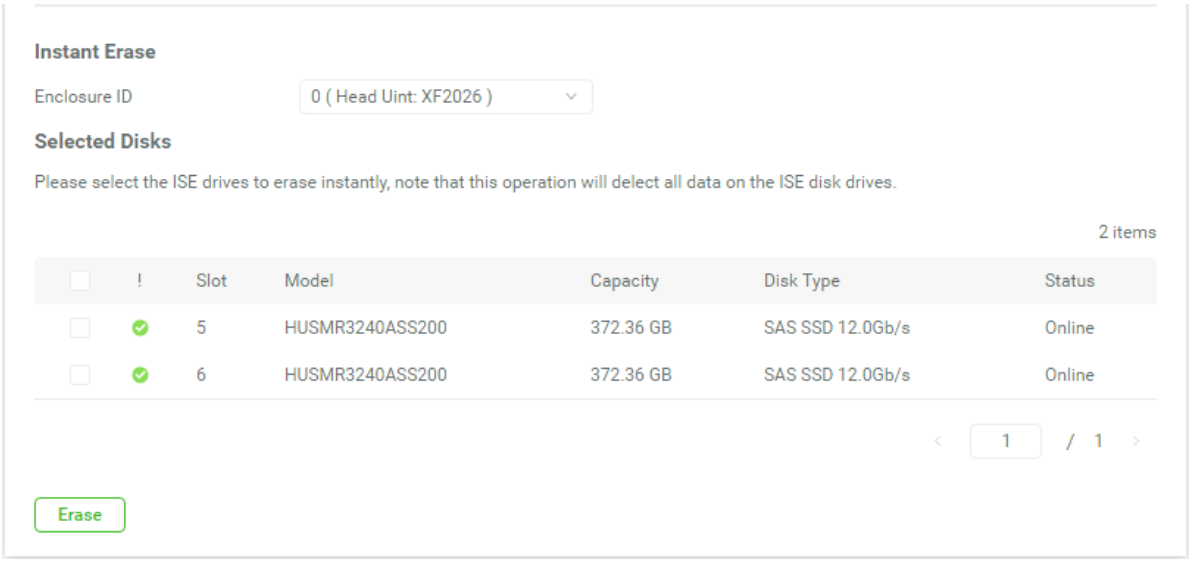


Figure 11-22 List ISE Drives

This table shows the column descriptions.

Table 11-2 Disk Column Descriptions

Column Name	Description
!	The status of disk health: • Green Color / Normal: The disk drive is good. • Orange Color / Abnormal: The disk drive has unrecoverable read errors or S.M.A.R.T. error. • Red Color / Warning: The disk drive has failed.
Slot	The position of the disk drive.
Model	The model name of disk drive.
Capacity	The capacity of the disk drive.
Disk Type	The type of the disk drive: • [SAS HDD | NL-SAS HDD | SAS SSD | SATA SSD] • [12.0Gb/s | 6.0Gb/s | 3.0Gb/s | 1.5Gb/s]
Status	The status of the disk drive: • Online: The disk drive is online. • Rebuilding: The disk drive is being rebuilt. • Transitioning: The disk drive is being migrated or is replaced by another disk when rebuilding occurs. • Scrubbing: The disk drive is being scrubbed. • Check Done: The disk drive has been checked the disk health.

11.4.2. Operations on ISE Drives

The options are available in this pane.

Instant Erase

If there are no pools within the ISE drives, these ISE drives can be erased. Select ISE drives and then click the **Erase** button to erase the selected ISEs.

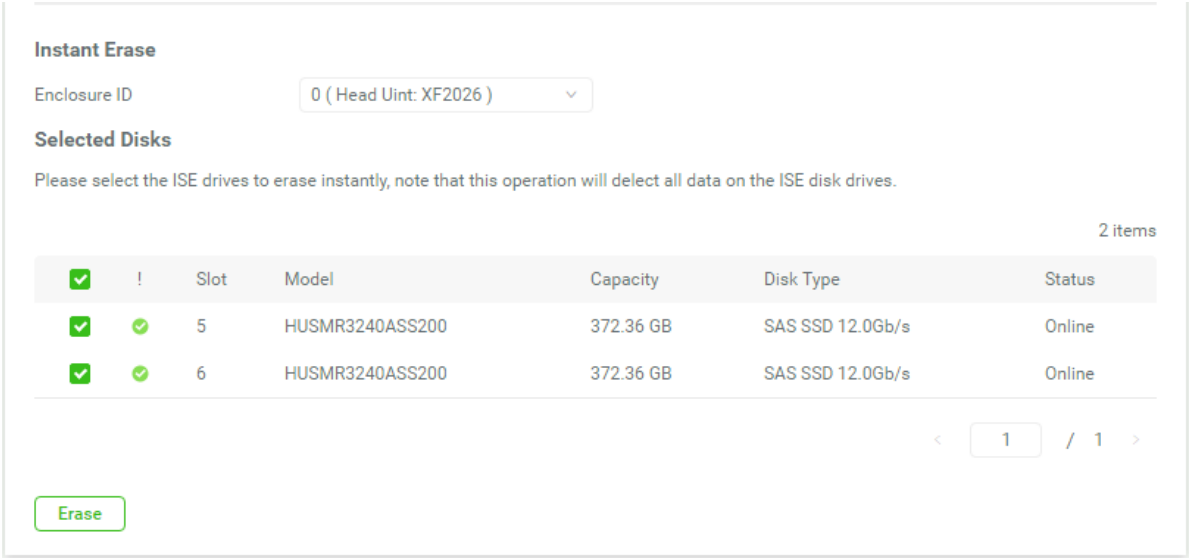


Figure 11-23 Instant Erase ISE drives

After proceeding, it will pop up a dialog to display the results.

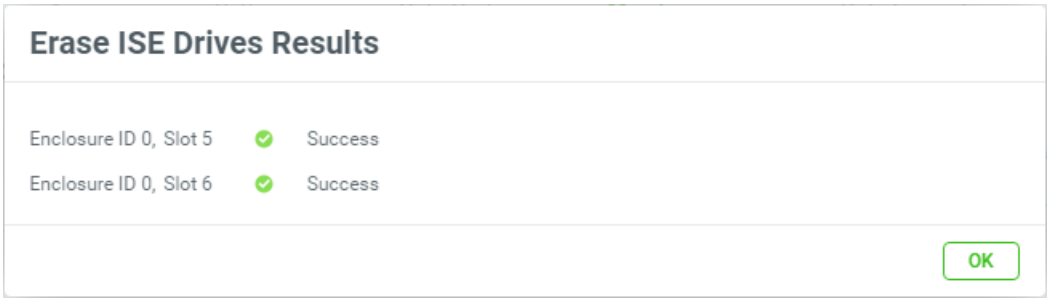


Figure 11-24 Instant Erase Results

TIP:
The **Instant Erase** function can be operated when the usage status of ISE drives is free.

CAUTION:
Erasing the ISE drives will change the DEK and delete all data on the ISE drive. The data on ISE drive can never be restored, please exercise caution.

12. QoS (Quality of Service)

QoS (Quality of Service) ensures that a particular application always gets a specific predefined performance level. Adjusting bandwidth and performing automatic tuning of the I/O performance makes sure the limitation of the throughput, IOPS per volume or required response time per application will be achieved.

INFORMATION:
QoS is available in XEVO firmware 1.1.0.

12.1. Configure QoS Settings

This section will describe the operations of enabling QoS. Select the **System** tab and the **Settings** subtab, and then click the **QoS Settings** pane to configure the QoS settings.

Figure 12-1 Settings Subtab in the System Tab

12.1.1. Operations on QoS Settings

The options are available in this pane.

Enable QoS Settings
Before using QoS, you have to enable the QoS settings.

1. Click the **QoS Settings** pane to configure the QoS settings

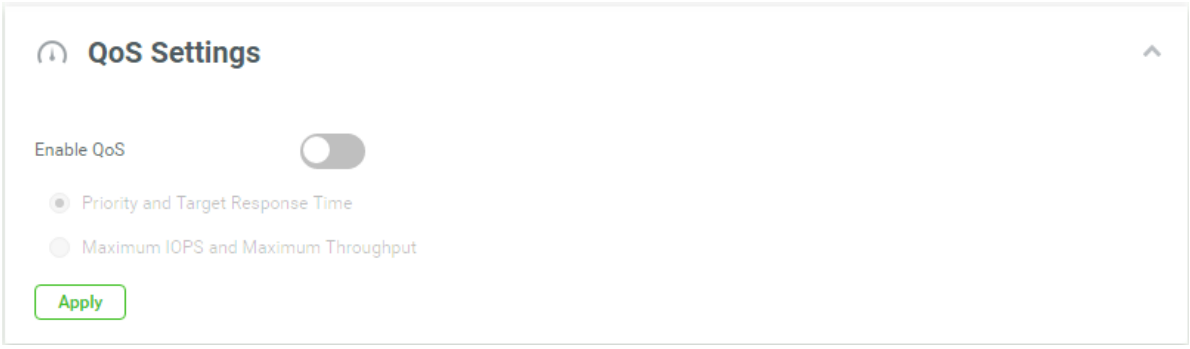


Figure 12-2 QoS Setting is Disabled

2. Click the **Enable QoS** switch to ON (Enable) to enable.
3. Select an option of **Priority and Target Response Time** or **Maximum IOPS and Maximum Throughput**.
4. Click the **Apply** button to enable.

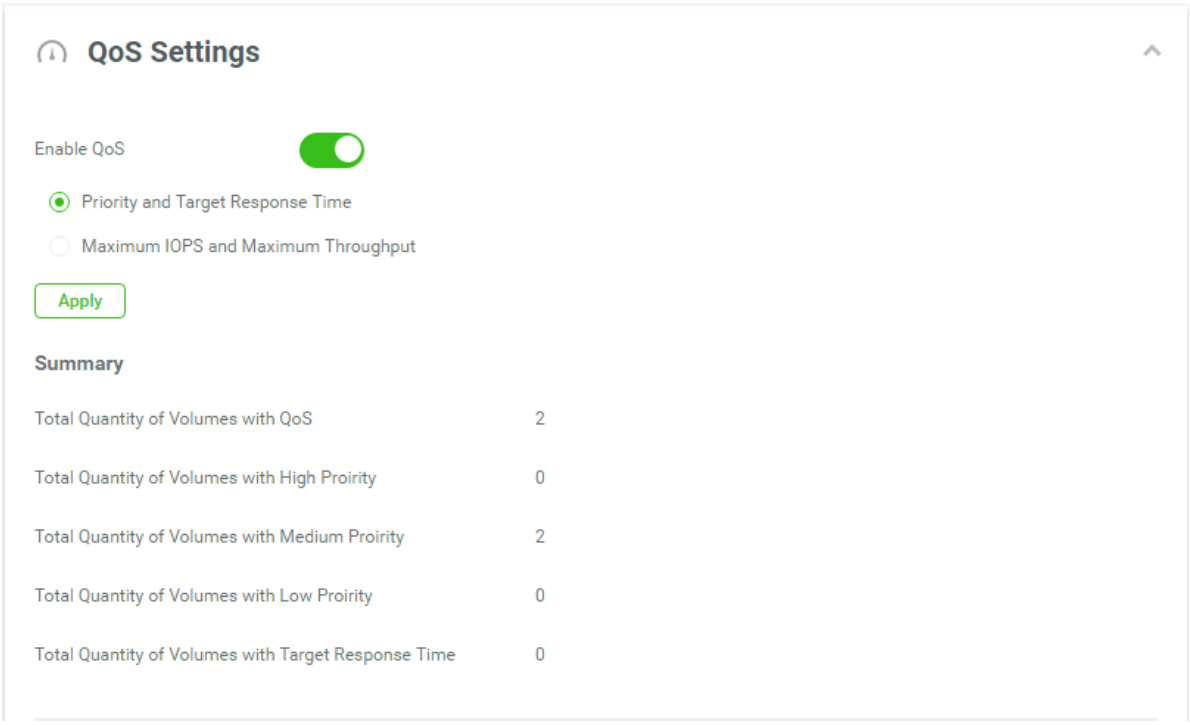


Figure 12-3 QoS Setting with Priority and Target Response

After the QoS setting is enabled, the relevant QoS summary is displayed in the page.

Change QoS Settings

The QoS settings can be changed dynamically.

1. Change the option of QoS setting.
2. Click the **Apply** button to change.

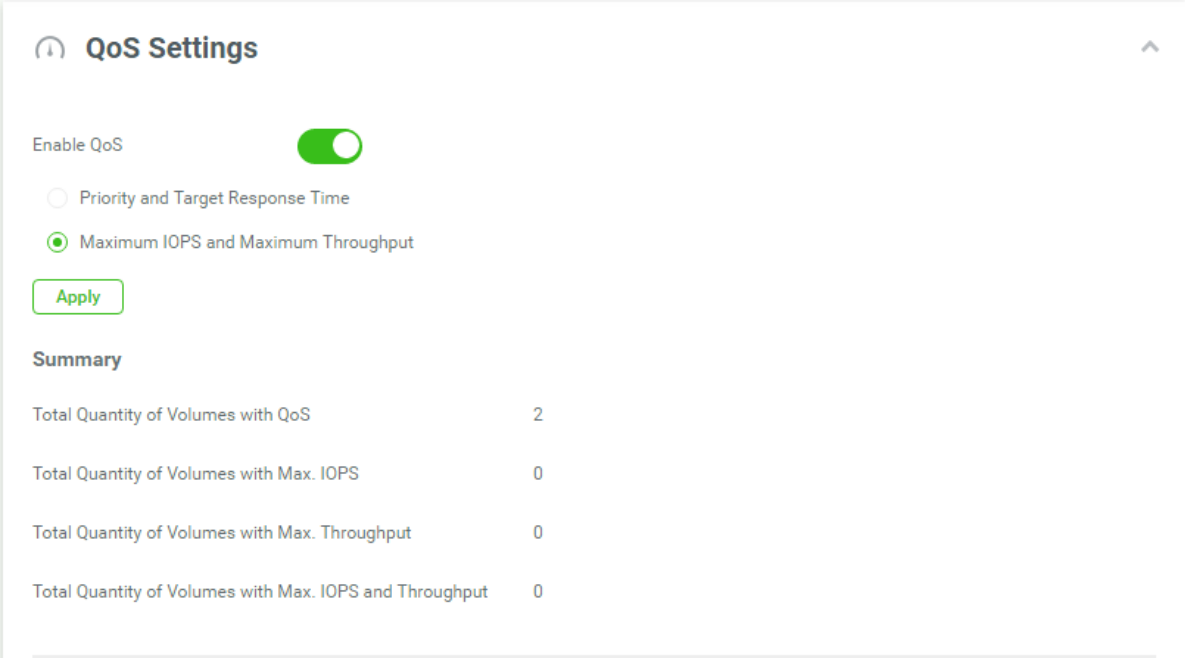


Figure 12-4 QoS Setting with Maximum IOPS and Maximum Throughput

The same, the relevant QoS summary is displayed in the page.

Disable QoS Settings

1. Click the **Enable QoS** switch to OFF (Disable) to disable.
2. Click the **Apply** button to disable.

12.2. Configure QoS Volumes

The **QoS Volumes** table is only visible when the QoS is enabled. It is displayed in the page below. In the **QoS Volumes** table, it can be displayed the status of QoS volumes, or configured the QoS volumes.

12.2.1. List QoS Volumes

The QoS settings can be configured by clicking the icon beside the volume name.

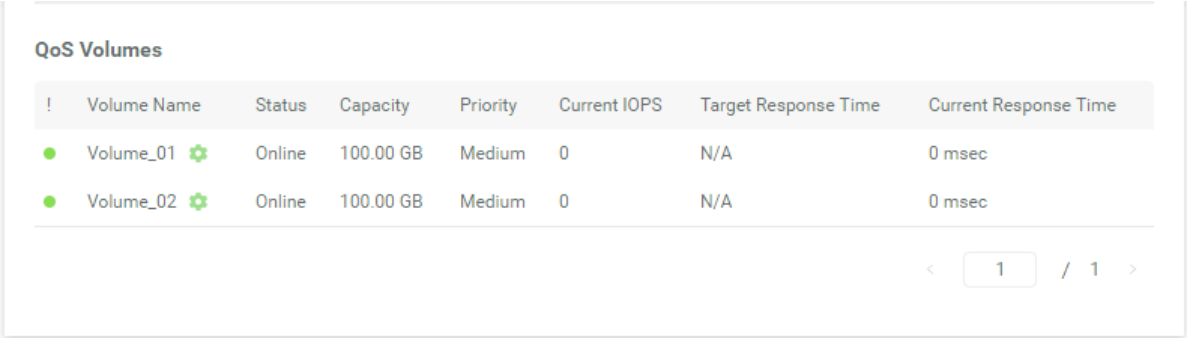


Figure 12-5 List QoS Volumes with Priority and Target Response

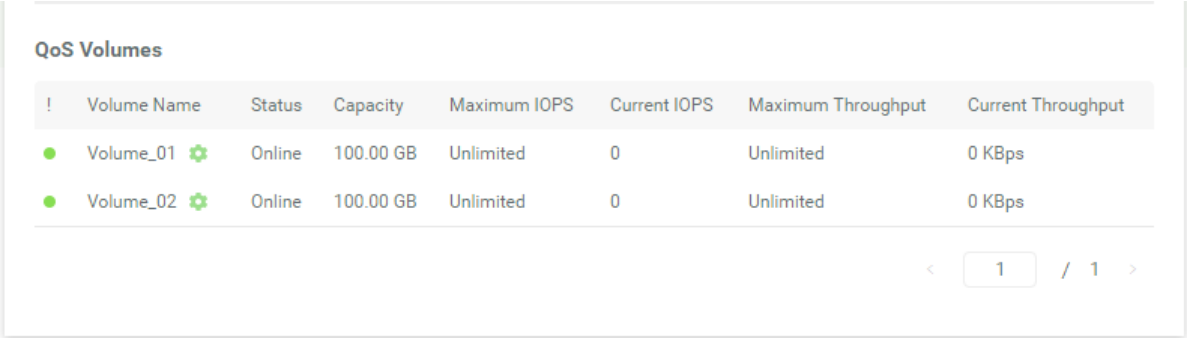


Figure 12-6 List QoS Volumes with Maximum IOPS and Maximum Throughput

This table shows the column descriptions.

Table 12-1 QoS Volume Descriptions

Column Name	Description
!	The status of the disk group: • Green Color / Normal: The volume is good. • Orange Color / Abnormal: The pool is unhealthy and incomplete. The cause may be a disk loss or failure. • Red Light / Warning: The disk group has failed.
Volume Name	The volume name.
Status	The status of the volume: • Online: The volume is online. • Offline: The volume is offline.

	• Erasing: The volume is being erased. • Initiating: The volume is being initialized. • Rebuilding: The volume is being rebuilt. • Migrating: The volume is being migrated. • Rollback: The volume is being rolled back. • Parity Checking: The volume is being parity check. • Relocating: The volume is being relocated. • EE Rebuilding: The volume is being RAID EE rebuilt.
Capacity	Total capacity of the volume.

Table 12-2 QoS Volume Descriptions with Priority and Target Response Time

Column Name	Description
Priority	The priority of the volume: • High • Middle • Low
Current IOPS	Current IOPS of the volume.
Target Response Time	Target response time setting, N/A is not configured.
Current Response Time	Current response time of the volume.

Table 12-3 QoS Volume Descriptions with Maximum IOPS and Maximum Throughput

Column Name	Description
Maximum IOPS	The maximum IOPS setting.
Current IOPS	Current IOPS of the volume.
Maximum Throughput	The maximum throughput setting.
Current Throughput	Current throughput of the volume.

12.2.2. Operations on QoS Volumes

Click the ⚙ icon beside the volume name to list the drop down options. These options are available in the QoS volume.

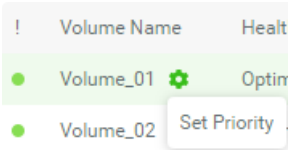


Figure 12-7 QoS Volume Options

Set Priority and Target Response Time

1. If the QoS setting is **Priority and Target Response Time**, select a volume, and then click **Set Priority** to configure.

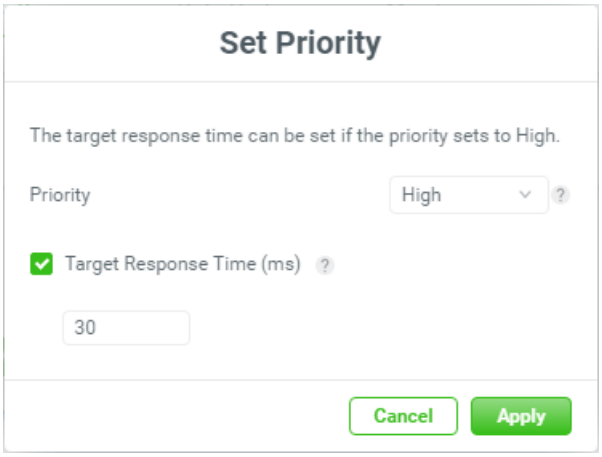


Figure 12-8 Set Priority

2. Select a **Priority** from the drop-down list. The default setting is **Middle**. The **Target Response Time** can be configured when the **Priority** is set to **High**.
3. If necessary, check the **Target Response Time** checkbox and enter a number. The number is between 1 and 10,000 milliseconds.
4. Click the **Apply** button to set.

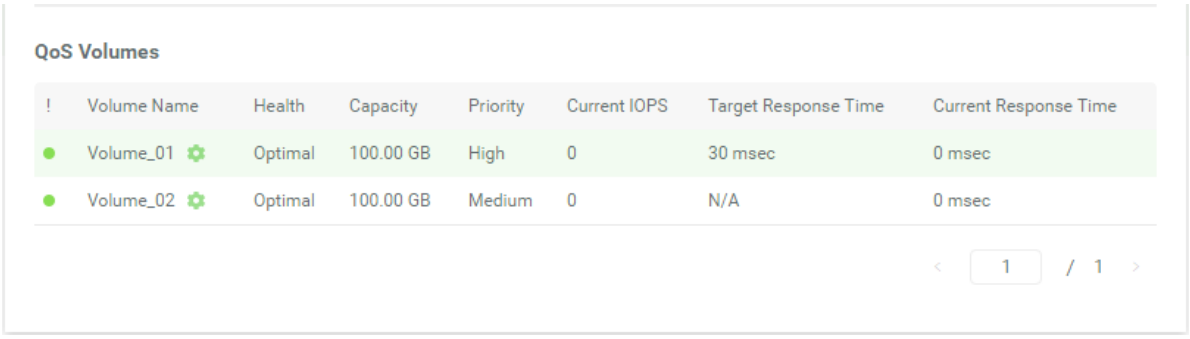


Figure 12-9 Priority and Target Response Time are Set

Set Maximum IOPS and Maximum Throughput

1. If the QoS setting is Maximum IOPS and Maximum Throughput, select a volume, and then click Set Maximum IOPS and Maximum Throughput to configure.

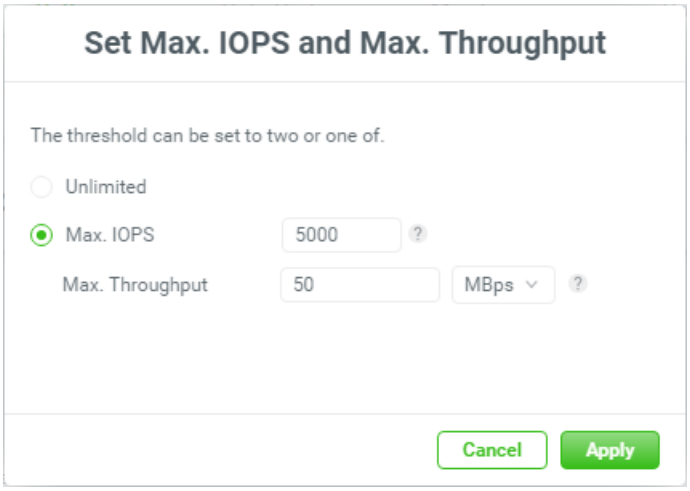


Figure 12-10 Set Maximum IOPS and Maximum Throughput

2. Select the Unlimited or Maximum IOPS and Maximum Throughput radio button.
3. If it is set to **Maximum IOPS and Maximum Throughput**, enter numbers for the maximum IOPS and/or the maximum throughput. The threshold can be set to two or one of. The maximum IOPS number is between 100 and 10,000,000. The maximum throughput number is between 50KBps and 100GBps.
4. Click the **Apply** button to set.

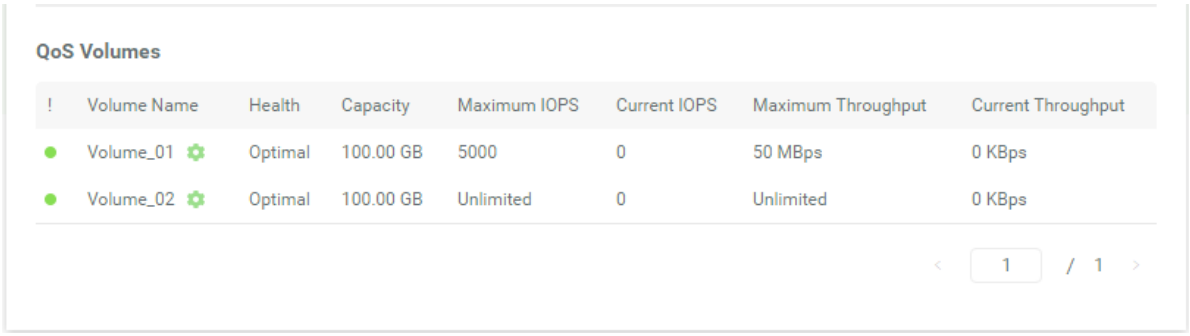


Figure 12-11 Maximum IOPS and Maximum Throughput are set

12.3. Volume Performance Monitoring

Select the **Performance** pane to monitor performance.

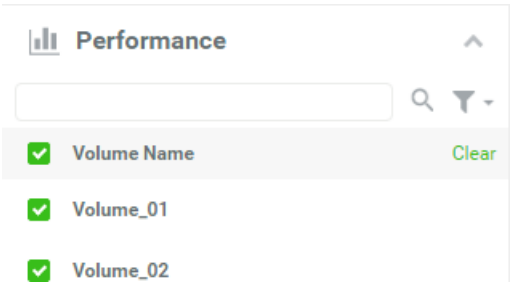


Figure 12-12 List All Volumes in the Performance Pane

All volumes are listed. You can select one or more volumes to view performance.

Figure 12-13 Performance Graph

13. Support and Other Resources

13.1. Getting Technical Support

After installing your device, locate the serial number on the sticker located on the side of the chassis or from the XEVO -> **System** -> **Maintenance** > **System Information** and use it to register your product at https://www.qsan.com/business_partnership. We recommend registering your product in QSAN partner website for firmware updates, document download, and latest news in eDM. To contact QSAN Support, please use the following information.

- Via the Web: https://www.qsan.com/technical_support
- Via Telephone: +886-2-77206355
  (Service hours: 09:30 - 18:00, Monday - Friday, UTC+8)
- Via Skype Chat, Skype ID: qsan.support
  (Service hours: 09:30 - 02:00, Monday - Friday, UTC+8, Summer time: 09:30 - 01:00)

1. SED and ISE Support

With data security issues at the time, the company places a high priority on ensuring that sensitive data is protected from unauthorized access. Whether it is due to internal policies or external compliance, access to data remains a matter of high importance for all organizations. These organizations will seek out storage manufacturers that provide a stored data protection method, SED (Self-Encrypting Drive), that has both authentication and encryption features.

In addition, ISE (Instant Secure Erase) drive is designed to protect data on hard disk drives by instantly resetting the drive back to factory settings and changing the encryption key so that any data remaining on the drive is cryptographically erased. This means all data on the drive is permanently and instantly unreadable, as needed.

INFORMATION:
SED (Self-Encryption Drive) and ISE (Instant Secure Erase) drive support is available in XEVO firmware 1.1.0.

1.1. Configure Authentication Key

- Via Email: support@qsan.com

Information to Collect

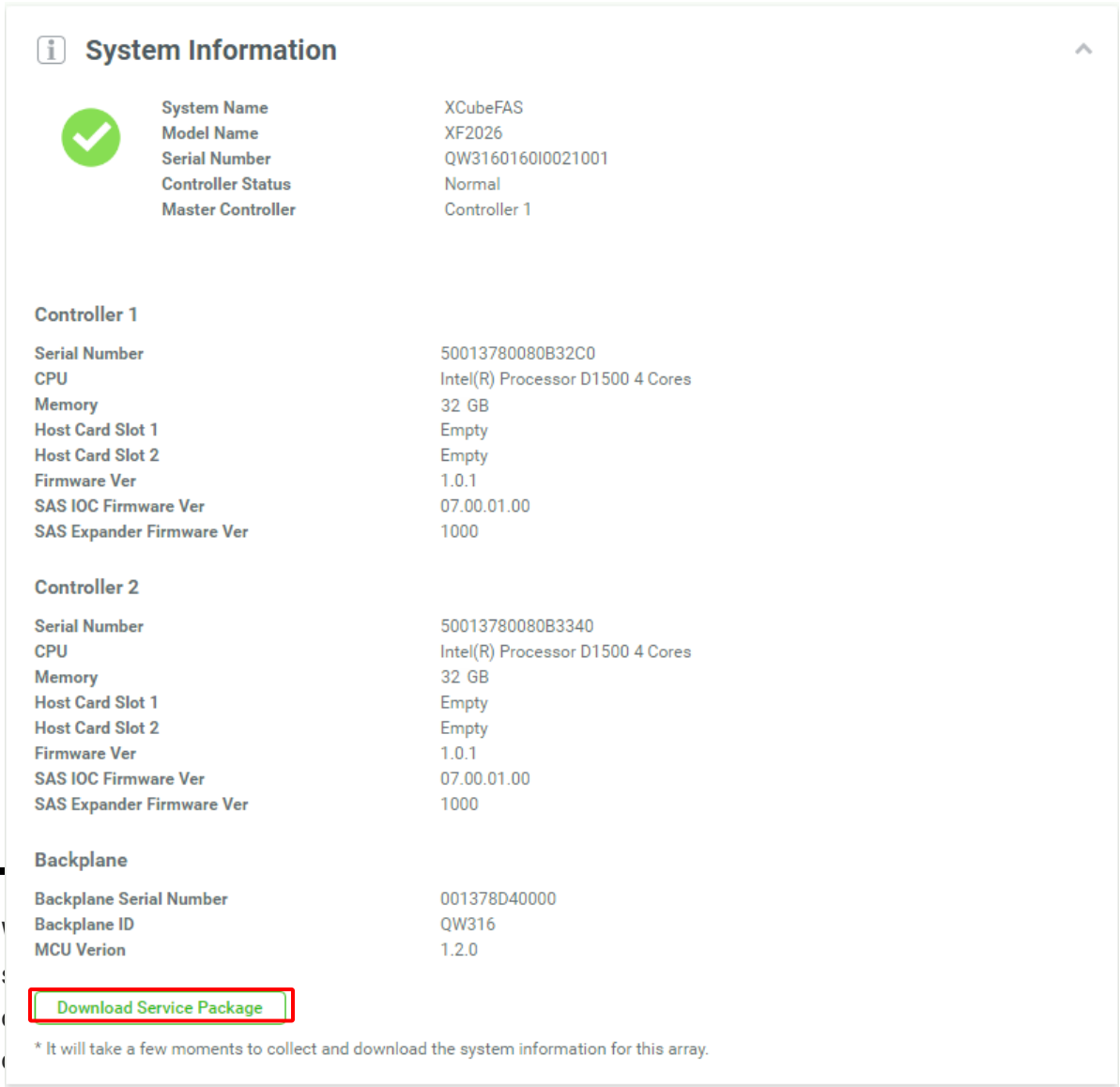
- Product name, model or version, and serial number
- Operating system name and version
- Firmware version
- Error messages or capture screenshots
- Product-specific reports and logs
- Add-on products or components installed
- Third-party products or components installed

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 XCubeFAS Series model.

If the technical support requests you to download the Service Package, please navigate in the XEVO -> **System** -> **Maintenance** > **System Information**, and then click the **Download Service Package** button to download. Then the system will automatically generate a zip file the default download location of your web browser.

1.



stored data protection method, SED (Self-Encrypting Drive), that has both authentication and encryption features.

In addition, ISE (Instant Secure Erase) drive is designed to protect data on hard disk drives by instantly resetting the drive back to factory settings and changing the encryption key so that any data remaining on the drive is cryptographically erased. This means all data on the drive is permanently and instantly unreadable, as needed.

INFORMATION:
SED (Self-Encryption Drive) and ISE (Instant Secure Erase) drive support is available in XEVO firmware 1.1.0.

1.1. Configure Authentication Key

Figure 13-1 Download Service Package

13.2. Online Customer Support

For better customer support, every XCubeFAS series models include the console cable (two for dual controller models), one for single controller models) for online support. Please follow the procedures below to setup the online help environment for QSAN support team.

The following procedure will help you to setup the serial console via the console cable that is enclosed in the shipping carton. The following image is the appearance of the console cable.

Figure 13-2 Appearance of a Console Cable

Procedures to Setup the Serial Console

1. Setup the serial cable between the controller and one server/host like in the below image.

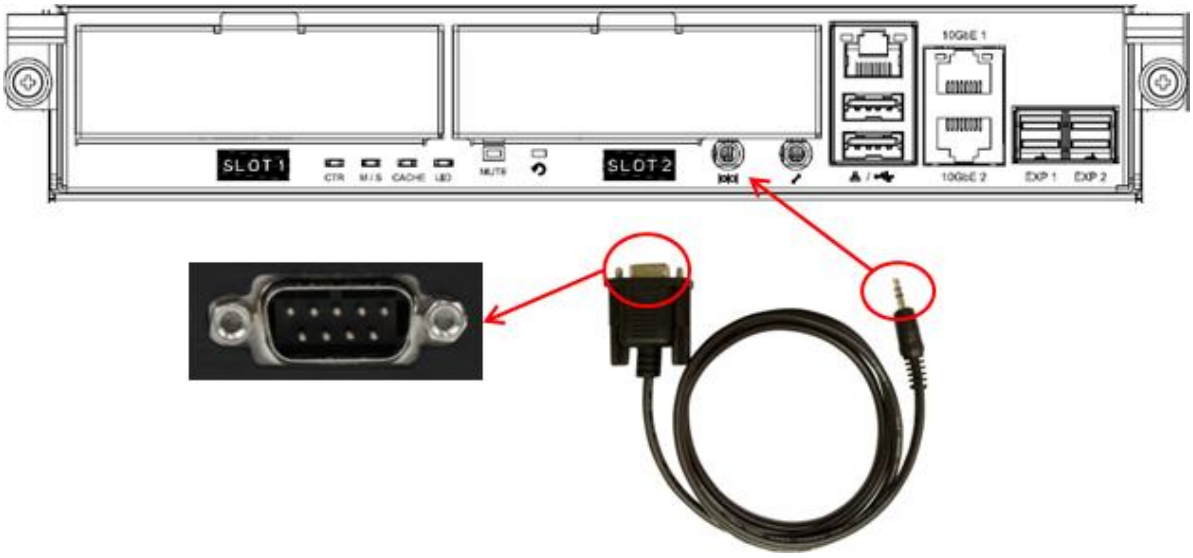


Figure 13-3 Connect the Console Cable

2. You must use terminal software such as HyperTerminal or Putty to open the console after the connection is made.

INFORMATION:
For more information about terminal software, please refer to

HyperTerminal: http://www.hilgraeve.com/hyperterminal/

PuTTY: http://www.putty.org/

3. Here we first demonstrate HyperTerminal. The console settings are on the following.

   Baud rate: 115200, 8 data bit, no parity, 1 stop bit, and no flow control

   Terminal type: vt100

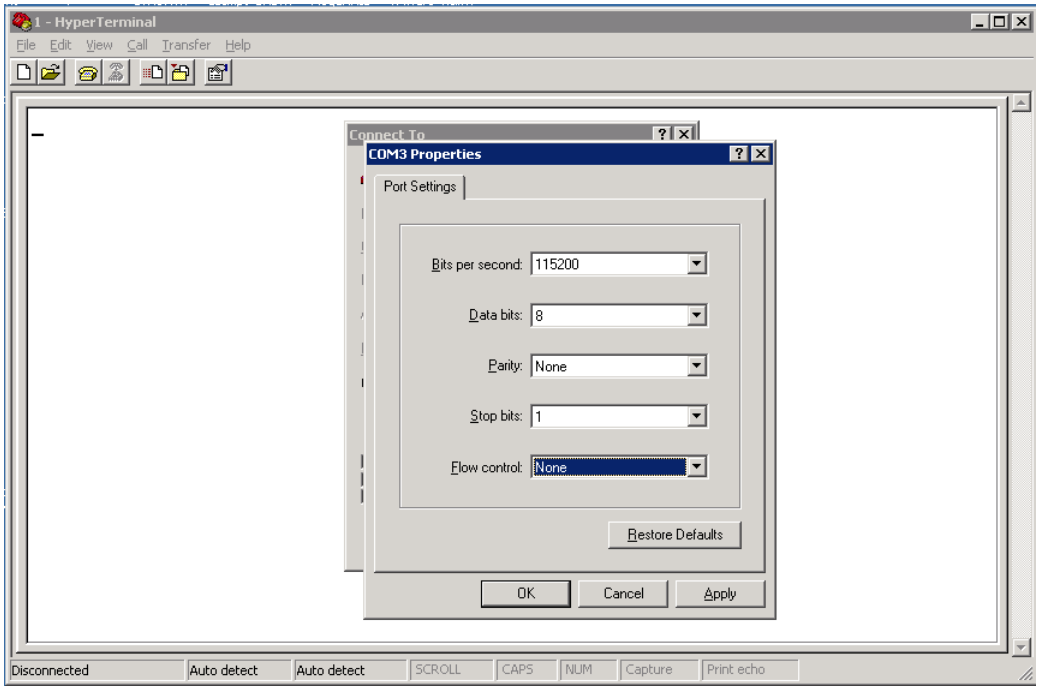
1. SED and ISE Support

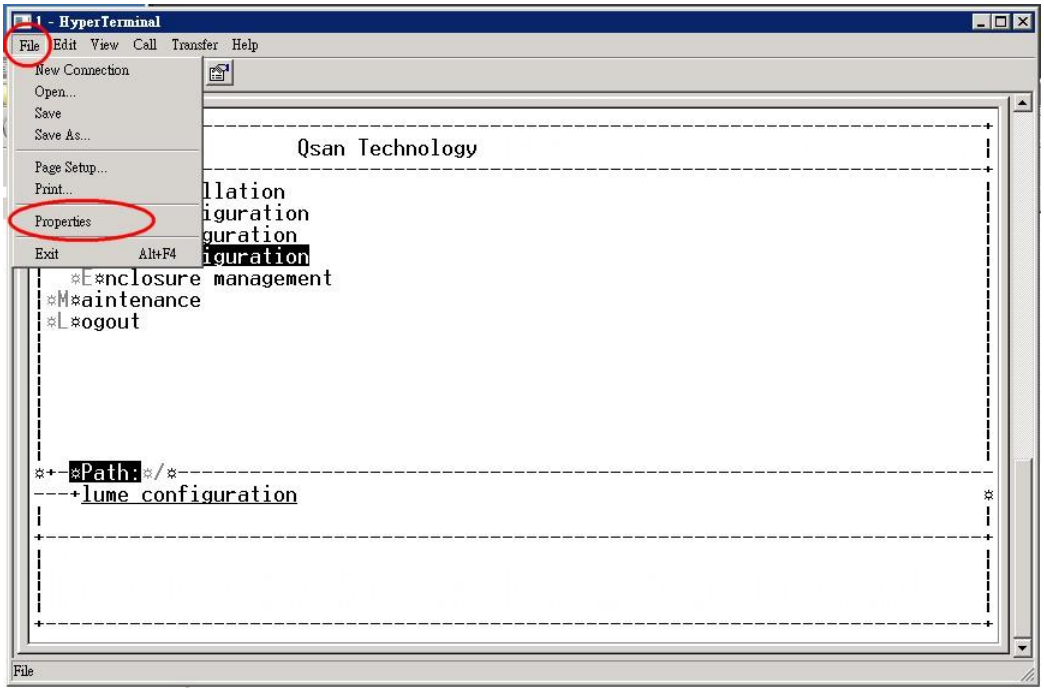
With data security issues at the time, the company places a high priority on ensuring that sensitive data is protected from unauthorized access. Whether it is due to internal policies or external compliance, access to data remains a matter of high importance for all organizations. These organizations will seek out storage manufacturers that provide a stored data protection method, SED (Self-Encrypting Drive), that has both authentication and encryption features.

In addition, ISE (Instant Secure Erase) drive is designed to protect data on hard disk drives by instantly resetting the drive back to factory settings and changing the encryption key so that any data remaining on the drive is cryptographically erased. This means all data on the drive is permanently and instantly unreadable, as needed.

INFORMATION:
SED (Self-Encryption Drive) and ISE (Instant Secure Erase) drive support is available in XEVO firmware 1.1.0.

1.1. Configure Authentication Key





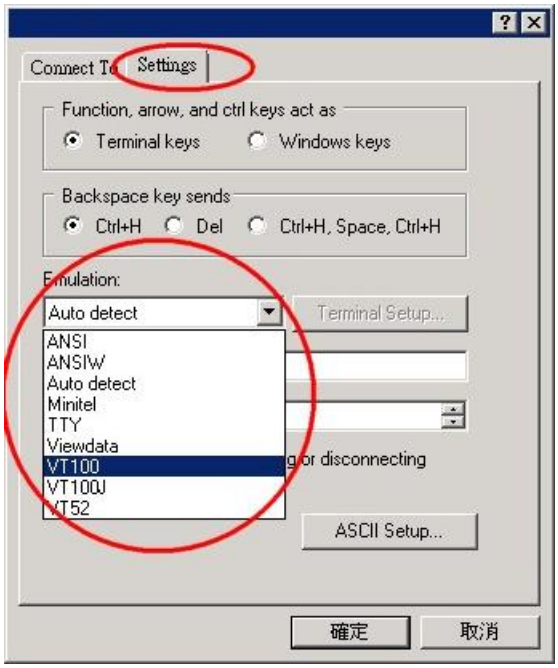


Figure 13-4 The Procedures of Setup Serial Console by HyperTerminal

1. SED and ISE Support

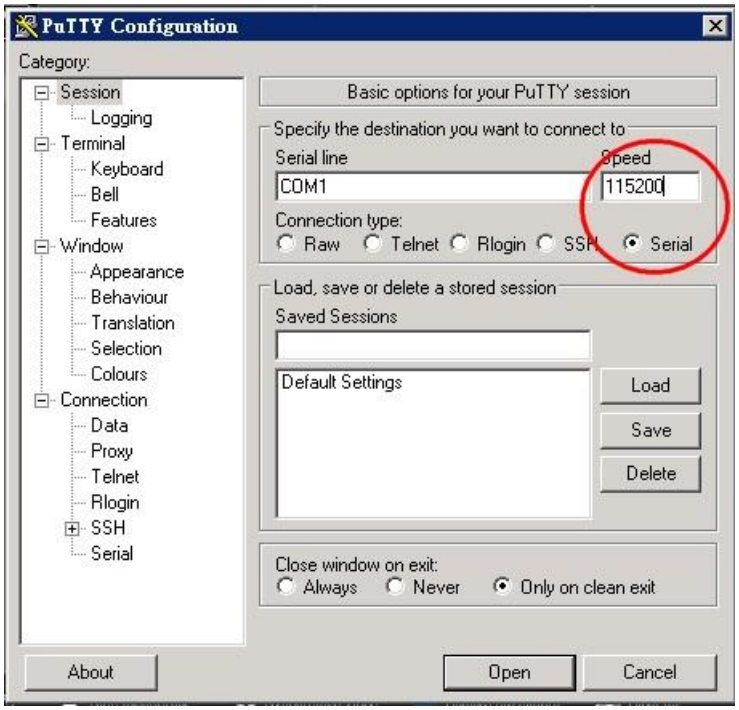
With data security issues at the time, the company places a high priority on ensuring that sensitive data is protected from unauthorized access. Whether it is due to internal policies or external compliance, access to data remains a matter of high importance for all organizations. These organizations will seek out storage manufacturers that provide a stored data protection method, SED (Self-Encrypting Drive), that has both authentication and encryption features.

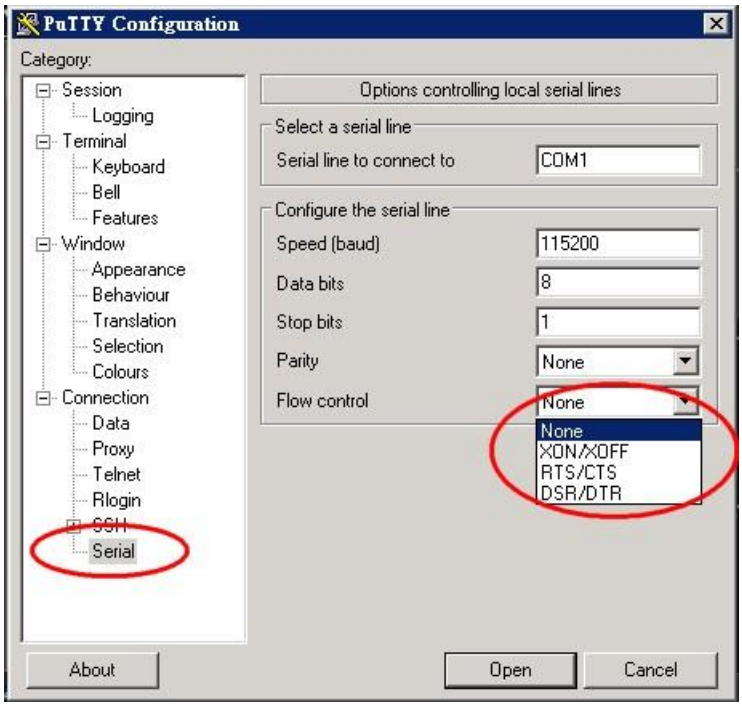
In addition, ISE (Instant Secure Erase) drive is designed to protect data on hard disk drives by instantly resetting the drive back to factory settings and changing the encryption key so that any data remaining on the drive is cryptographically erased. This means all data on the drive is permanently and instantly unreadable, as needed.

INFORMATION:
SED (Self-Encryption Drive) and ISE (Instant Secure Erase) drive support is available in XEVO firmware 1.1.0.

1.1. Configure Authentication Key

4. If you are using PuTTY instead, please refer to below





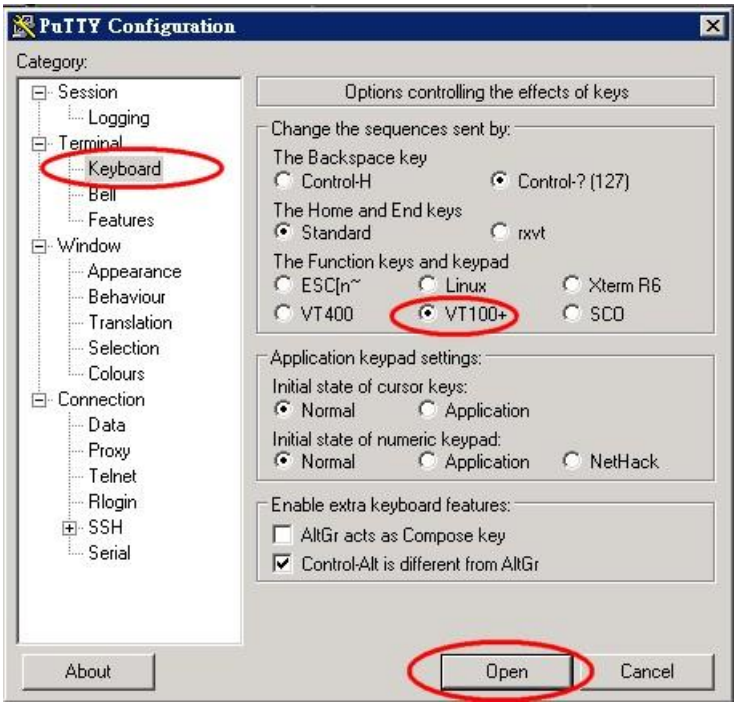


Figure 13-5 The Procedures of Setup Serial Console by PuTTY

1. SED and ISE Support

With data security issues at the time, the company places a high priority on ensuring that sensitive data is protected from unauthorized access. Whether it is due to internal policies or external compliance, access to data remains a matter of high importance for all organizations. These organizations will seek out storage manufacturers that provide a stored data protection method, SED (Self-Encrypting Drive), that has both authentication and encryption features.

In addition, ISE (Instant Secure Erase) drive is designed to protect data on hard disk drives by instantly resetting the drive back to factory settings and changing the encryption key so that any data remaining on the drive is cryptographically erased. This means all data on the drive is permanently and instantly unreadable, as needed.

INFORMATION:
SED (Self-Encryption Drive) and ISE (Instant Secure Erase) drive support is available in XEVO firmware 1.1.0.

1.1. Configure Authentication Key

5. Users should be able to login the controller system via console cable by following the procedures above.

Setup the Connection for Online Support

Following is the procedure to setup the connection for online support via TeamViewer:

1. Please download the TeamViewer from following hyper link: https://www.teamviewer.com/en/download/
2. Install TeamViewer.
3. Please provide the ID/password showed on the application to QSAN support team member to join the online support session.

13.3. Accessing Product Updates

To download product updates, please visit QSAN website:

https://www.qsan.com/download_center

13.4. Documentation Feedback

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

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

Appendix

Glossary and Acronym List

Common Terminology

Item	Description
RAID	Redundant Array of Independent Disks. There are different RAID levels with different degree of data protection, data availability, and performance to host environment.
Disk	The Physical Disk belongs to the member disk of one specific RAID group.
Pool	A collection of removable media. One pool consists of a set of volumes and owns one RAID level attribute.
Volume	Each pool could be divided into several volumes. The volumes from one pool have the same RAID level, but may have different volume capacity.
LUN	Logical Unit Number. A logical unit number (LUN) is a unique identifier which enables it to differentiate among separate devices (each one is a logical unit).
WebUI	Web User Interface.
WT	Write-Through cache-write policy. A cache technique in which the completion of a write request is not signaled until data is safely stored in non-volatile media. Each data is synchronized in both data cache and accessed physical disks.
WB	Write-Back cache-write policy. A cache technique in which the completion of a write request is signaled as soon as the data is in cache and actual writing to non-volatile media occurs at a later time. It speeds up system write performance but needs to bear the risk where data may be inconsistent between data cache and the physical disks in one short time interval.
RO	Set the volume to be Read-Only.
GS	Global Spare disks. It is shared for rebuilding purpose. If some RAID

	groups need to use the global spare disks for rebuilding, they could get the spare disks out from the common spare disks pool for such requirement.
DG	DeGraded mode. Not all of the array's member disks are functioning, but the array is able to respond to application read and write requests to its virtual disks.
SCSI	Small Computer System Interface
SAS	Serial Attached SCSI
S.M.A.R.T.	Self-Monitoring Analysis and Reporting Technology
WWN	World Wide Name
HBA	Host Bus Adapter
SES	SCSI Enclosure Services
NIC	Network Interface Card
BBM	Battery Backup Module

FC / iSCSI / SAS Terminology

Item	Description
FC	Fibre Channel
FC-P2P	Point-to-Point
FC-AL	Arbitrated Loop
FC-SW	Switched Fabric
iSCSI	Internet Small Computer Systems Interface
LACP	Link Aggregation Control Protocol
MPIO	Multipath Input/Output
MC/S	Multiple Connections per Session
MTU	Maximum Transmission Unit
CHAP	Challenge Handshake Authentication Protocol. An optional security mechanism to control access to an iSCSI storage system over the iSCSI data ports.
iSNS	Internet Storage Name Service
SAS	Serial Attached SCSI

Dual Controller Terminology

Item	Description
6G MUX	Bridge board is for SATA II disk to support dual controller mode.

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

QSAN Technology, Inc. ("QSAN") is willing to grant you (“User”) a license of software, firmware and/or other product sold, manufactured or offered by QSAN (“the Product”) pursuant to this EULA.

License Grant

QSAN 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 QSAN or its licensor(s). User will not acquire any intellectual property by this EULA.

License Limitations

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 QSAN to control access to the components, features or functions of the Product.

Disclaimer

QSAN 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 PROVIDE “AS IS” WITHOUT WARRANTY OF ANY KIND. QSAN MAKES NO WARRANTY THAT THE PRODUCT WILL BE FREE OF BUGS, ERRORS, VIRUSES OR OTHER DEFECTS.

IN NO EVENT WILL QSAN 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 QSAN HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Limitation of Liability

IN ANY CASE, QSAN’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, QSAN may terminate this EULA and take remedies available to QSAN immediately.

Miscellaneous

- QSAN reserves the right to modify this EULA.
- QSAN reserves the right to renew the software or firmware anytime.
- QSAN 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.

- This EULA shall be governed by and constructed according to the laws of R.O.C. Any disputes arising from or in connection with this EULA, User agree to submit to the jurisdiction of Taiwan Shilin district court as first instance trial.

