XCubeFAS Series White Paper

SED (Self-Encrypting Drive) and ISE (Instant Secure Erase) Support

QSAN Technology, Inc.
www.QSAN.com

Copyright

August 2019

This edition applies to QSAN XCubeFAS series. QSAN believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

Trademarks

Notices

This XCubeFAS series white paper 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 document 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

SED and ISE Support

Executive Summary

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.

Audience

This document is applicable for QSAN customers and partners who are interested in learning about SED and ISE drive for securing data on the storage systems. It assumes the reader is familiar with QSAN products and has general IT experience, including knowledge as a system or network administrator. If there is any question, please refer to the user manuals of products, or contact QSAN support for further assistance.

Overview

When disk drives are retired and moved outside from the data center into someone else's hands, the data on those drives is put at significant risk. IT administrators routinely retire drives for a variety of reasons, including:

- Returning drives for warranty, repair, maintenance, or expired lease agreements
- Removal and disposal of disk drives
- Repurposing drives to another storage

Through the study found that almost all drives eventually leave the enterprise or data center, but the corporate data resides on such drives, and when most leave the data center, the data they contain is still readable. Even data that has been striped across many drives in a RAID protection is vulnerable to data theft, because just a typical single stripe in today's high-capacity arrays is large enough to expose the sensitive and secured data.

Drive Control Challenges and Disposal Costs

In an effort to avoid data breaches, corporations have tried many ways to erase the data on retired drives before they leave the houses and potentially fall into the bad guy. Current retirement practices are all expensive and time-consuming, such as:

- Overwriting drive data
- Degaussing or physically shredding
- Hire professional disposal services

These designed to make data unreadable rely on significant human involvement in the process, and are thus subject to both technical and human failure.

The Solution

Every day, thousands of disk drives leave data centers as old systems are retired. But what if all those disk drives had been automatically and transparently encrypting that data, enabling it to be instantly and securely erased? SED comprehensively resolve these issues, making encryption for drive retirement both easy and affordable.

SED has build-in an encryption controller and an encryption key on the disk drive itself. It can provide instant secure erase (cryptographic erase or making the data no longer readable), and to enable auto-locking to secure active data if a drive is misplaced or stolen from a system while in use.

While ISE provides instant secure erase only. When it's time to retire or repurpose the drive, the owner sends a command to the drive to perform a cryptographic erase. Cryptographic erase simply replaces the encryption key inside the encrypted drive, making it impossible to ever decrypt the data encrypted with the deleted key.

Benefits

SED & ISE reduce IT operating expenses by freeing IT from both drive control headaches and disposal costs. By using SED & ISE, they are without hindering IT efficiency. Furthermore, SED & ISE simplify decommissioning and preserve hardware value for returns and repurposing by:

- Securing warranty and expired lease returns
- Eliminating the need to overwrite or destroy the drive
- Enabling drives to be repurposed securely

In addition, the drive owner may choose to employ the SED in the auto-lock mode to help secure active data against theft. Utilizing the SED in auto-lock mode simply requires securing the drive during its normal use with an authentication key. When secured in this manner, the drive's data encryption key is locked whenever the drive is powered down. In other words, the moment the SED is switched off or unplugged, it automatically locks down the drive's data.

When the SED is then powered back on, the SED requires authentication before being able to unlock its encryption key and read any data on the drive, thus protecting against misplacement and insider or external theft.

Theory of Operation

SED has two functions. There are authentication which is operated by AK (Authentication Key) and encryption data which is operated by DEK (Data Encryption Key). ISE drive has encryption data only by DEK but no authentication.

SED Operation Process

An AK is generated by a user entered password. After enabling authentication key successfully, recommend to export the key 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 authentication key file to recover in case of an unforeseen event.

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

A new clean SED is not locked; it has to be written an AK into the SED first. It's called initiate SED. The following describes the steps that occur during the authentication process of a secured drive.

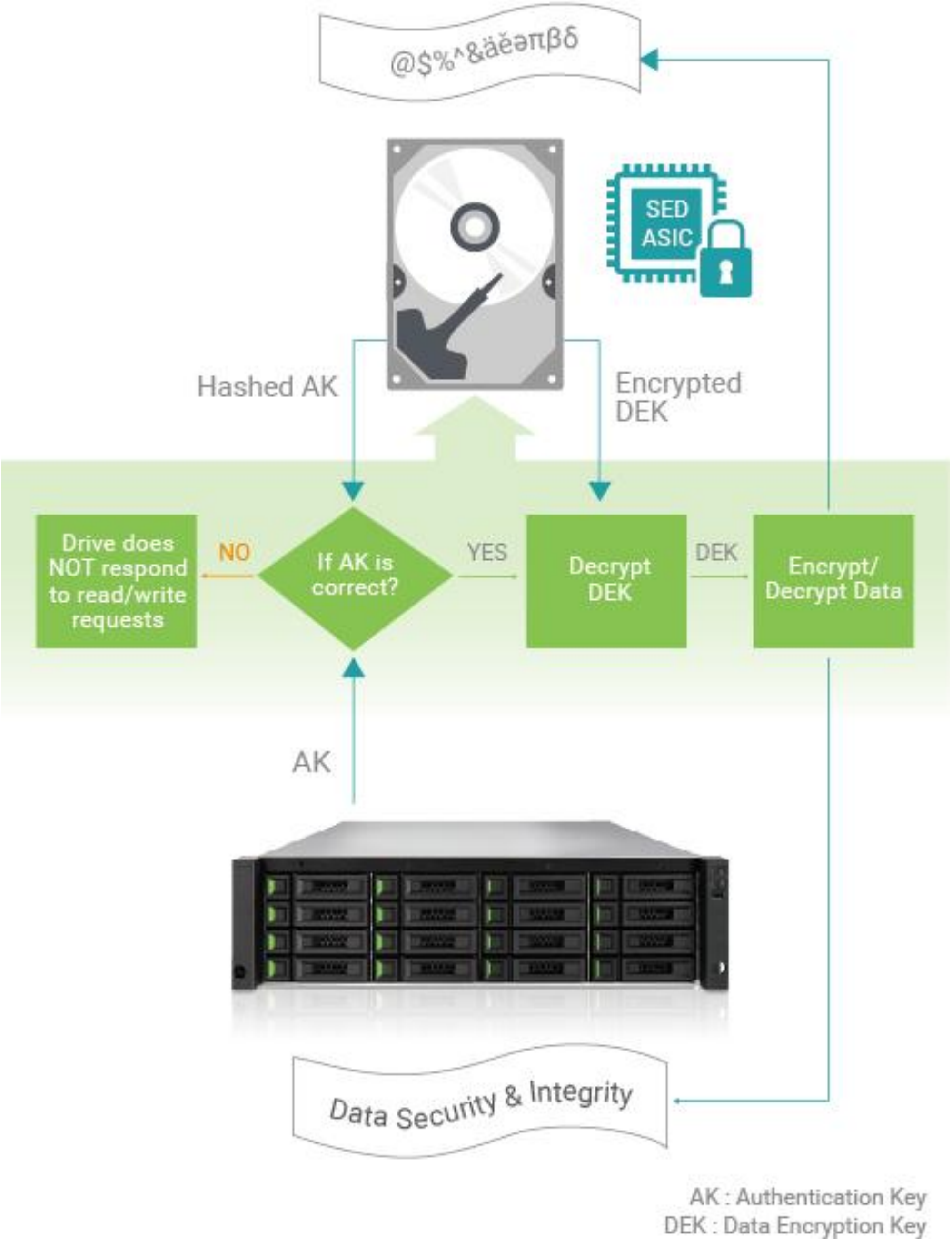


Figure 1 SED Operation Process

Authentication

The storage system gets the AK from user entered and sends it to the correct locked drive. The drive hashes the AK and compares the result with the hash of the AK that's stored in a secure area of the disk. If the two hashed AK values do not match, the authentication process ends, and the drive will not permit reading data from the disk. The drive remains locked.

Decrypt the DEK

If the two hashes match, the drive is then unlocked, and the drive uses the AK it received from the storage system to decrypt the DEK (which was previously encrypted with the AK) that's stored in a secure area of the disk. Once the authentication process is successfully completed, the drive is unlocked until the next time it is powered down. Note that this authentication process only occurs when the drive is first powered on. It does not repeat with each I/O.

The DEK Encrypts and Decrypts the Data

The DEK is then used to encrypt data to be written to the disk and to decrypt data that's being read from the disk. The drive now works in standard fashion during data transfers, with encryption and decryption transparently occurring in the background.

ISE Technology

Each ISE drive (SED as well) randomly generates an encryption key in the factory that is embedded on the drive. The ISE automatically performs full disk encryption; when a write is performed; clear text enters the drive and is first encrypted (using the DEK embedded within the drive) before being written to the disk. When a read is performed, the encrypted data on the disk is decrypted before leaving the drive. During normal operation an ISE is completely transparent to the system, appearing to be the same as a non-encrypting drive. The self-encrypting is constantly encrypting, encryption cannot be accidentally turned off.

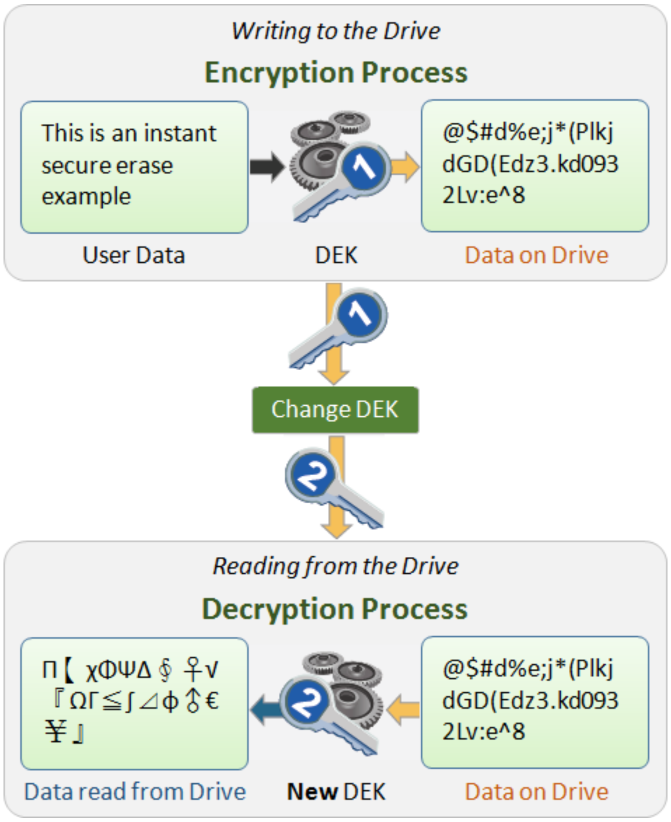


Figure 2 ISE Technology

ISE technology greatly simplifies repurposing of the drive and disposal. An owner wishing to repurpose a drive simply performs a key erase to replace the encryption key. The drive deletes the encryption key and replaces it with a new encryption key generated randomly within the drive. After key erase, any data that had been written to the disk is unreadable; data that was encrypted with the previous key is unintelligible when decrypted with the new encryption key. The drive is left as it was delivered from the factory.

Instant Erase Limitation

If ISEs are free and not be used as any pool member, they can be performed instant erase. The same limitation as SEDs, however SEDs can be erased by the AK is enabled. Another case is that the unknown SED is put in lock mode, the way to erase it is to perform erase SED by PSID which is a unique number in each drive, printed on the disk label, and visible to anyone with physical access to the SED. The owner would simply perform a secure erase to replace the encryption key.

TIP:
SEDs or ISE drives can be erased only if their usage status is free.

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.

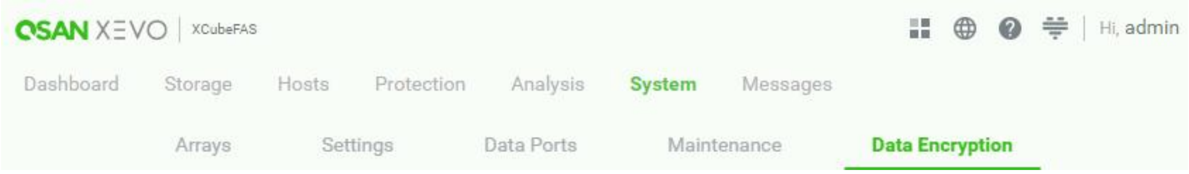


Figure 3 Disk Encryption Subtab in the System Tab

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**.

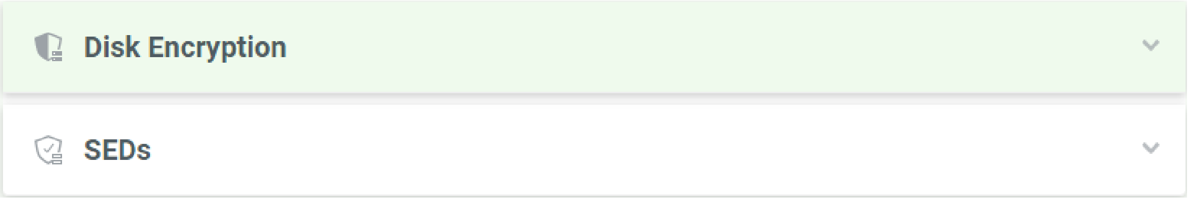
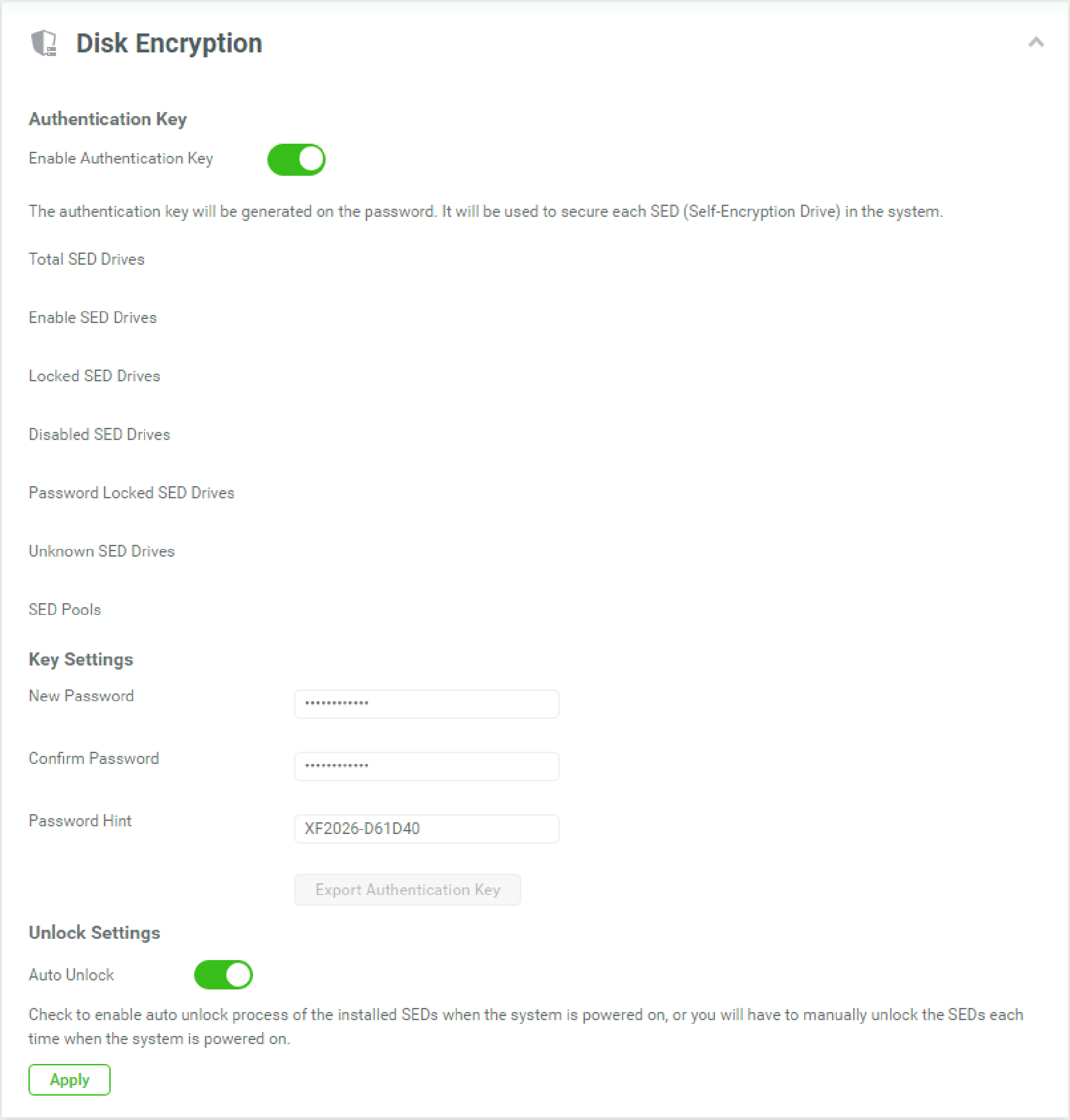


Figure 4 Disk Encryption Pane

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



Authentication Key

Enable Authentication Key ●

The authentication key will be generated on the password. It will be used to secure each SED (Self-Encryption Drive) in the system.

Total SED Drives

Enable SED Drives

Locked SED Drives

Disabled SED Drives

Password Locked SED Drives

Unknown SED Drives

SED Pools

Key Settings

New Password	············
Confirm Password	············
Password Hint	XF2026-D61D40

Unlock Settings

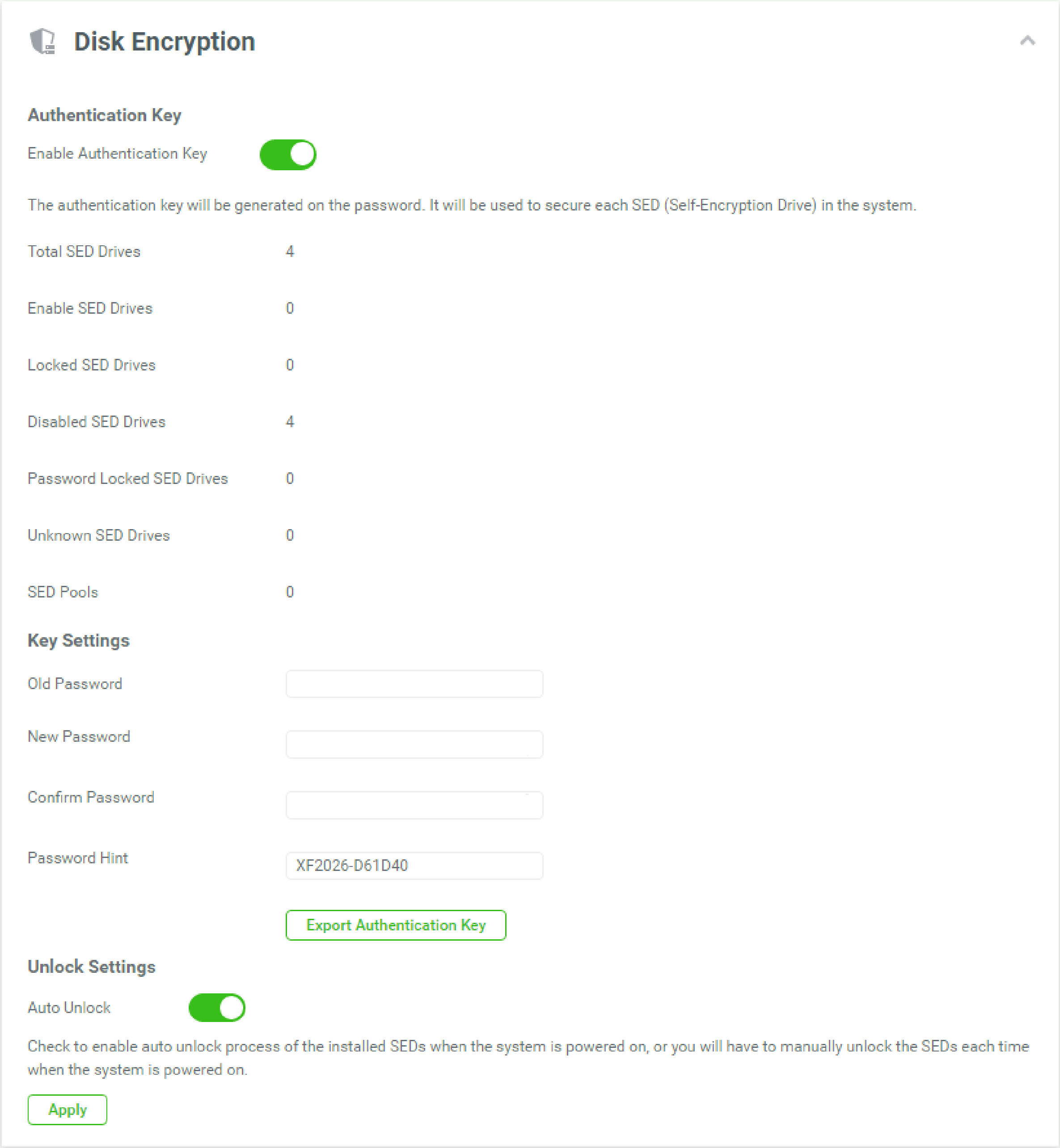
Auto Unlock ●

Check to 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.

Figure 5 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.



Disk Encryption

Authentication Key

Enable Authentication Key

The authentication key will be generated on the password. It will be used to secure each SED (Self-Encryption Drive) in the system.

Total SED Drives	4
Enable SED Drives	0
Locked SED Drives	0
Disabled SED Drives	4
Password Locked SED Drives	0
Unknown SED Drives	0
SED Pools	0

Key Settings

Old Password

New Password

Confirm Password

Password Hint: XF2026-D61D40

Unlock Settings

Auto Unlock

Check to 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.

Figure 6 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.

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.

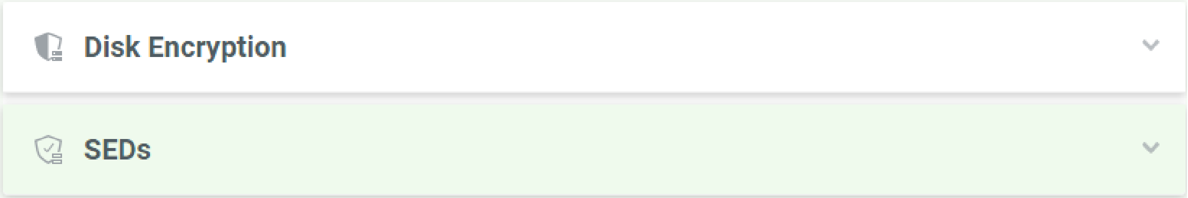
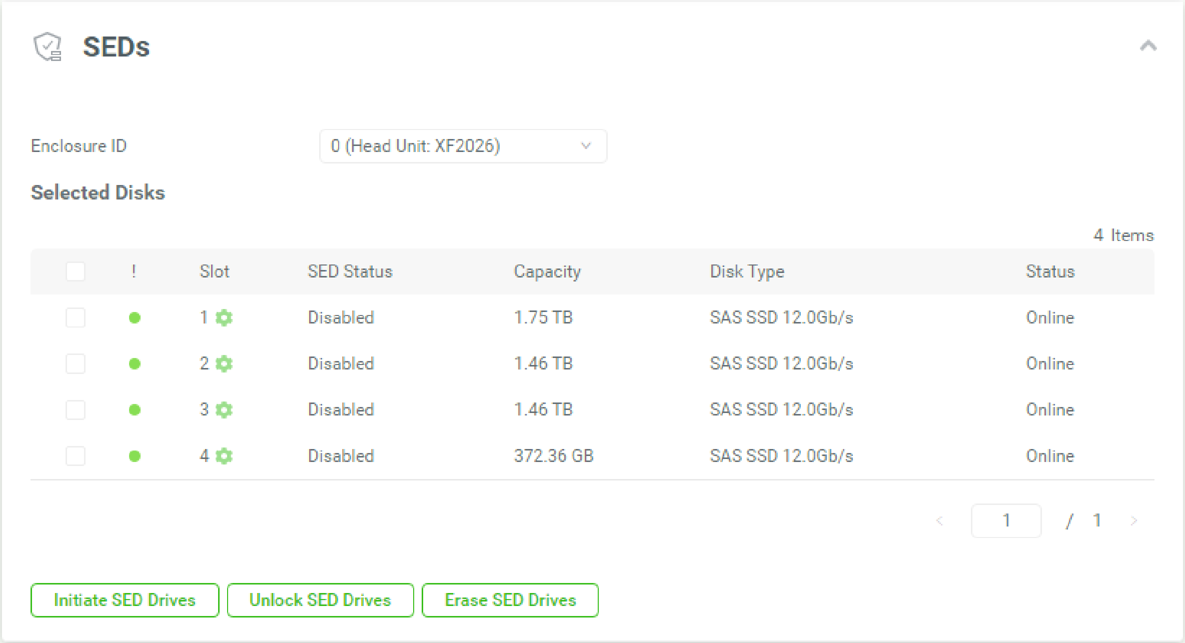


Figure 7 SEDs Pane

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)



SEDs

Enclosure ID: 0 (Head Unit: XF2026)

Selected Disks

4 Items

□	!	Slot	SED Status	Capacity	Disk Type	Status
□	●	1 ⚙	Disabled	1.75 TB	SAS SSD 12.0Gb/s	Online
□	●	2 ⚙	Disabled	1.46 TB	SAS SSD 12.0Gb/s	Online
□	●	3 ⚙	Disabled	1.46 TB	SAS SSD 12.0Gb/s	Online
□	●	4 ⚙	Disabled	372.36 GB	SAS SSD 12.0Gb/s	Online

Figure 8 List SEDs

This table shows the column descriptions.

Table 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.

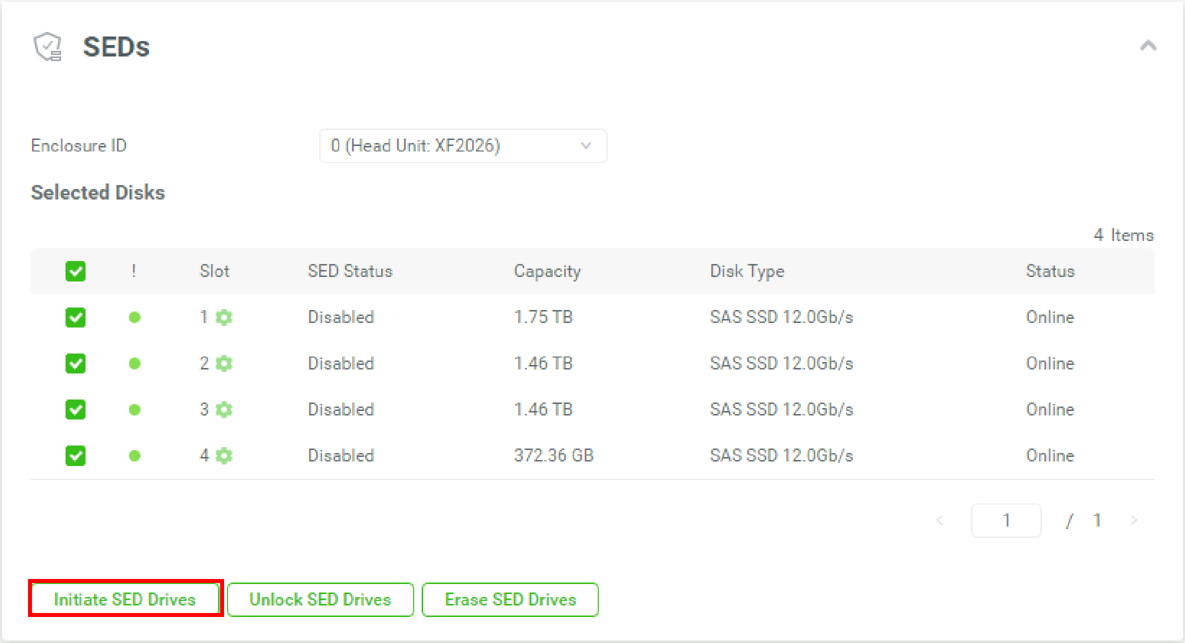
	• Unlocking: The SED is being unlocked. • Erasing: The SED is being erased. • Changing Key: The SED is being changed the key.
Capacity	The capacity of the disk drive.
Disk Type	The type of the disk drive: • [SAS HDD | NL-SAS HDD | SAS SSD | SATA SSD] • [12.0Gb/s | 6.0Gb/s | 3.0Gb/s | 1.5Gb/s]
Status	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.

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.



SEDs

Enclosure ID: 0 (Head Unit: XF2026)

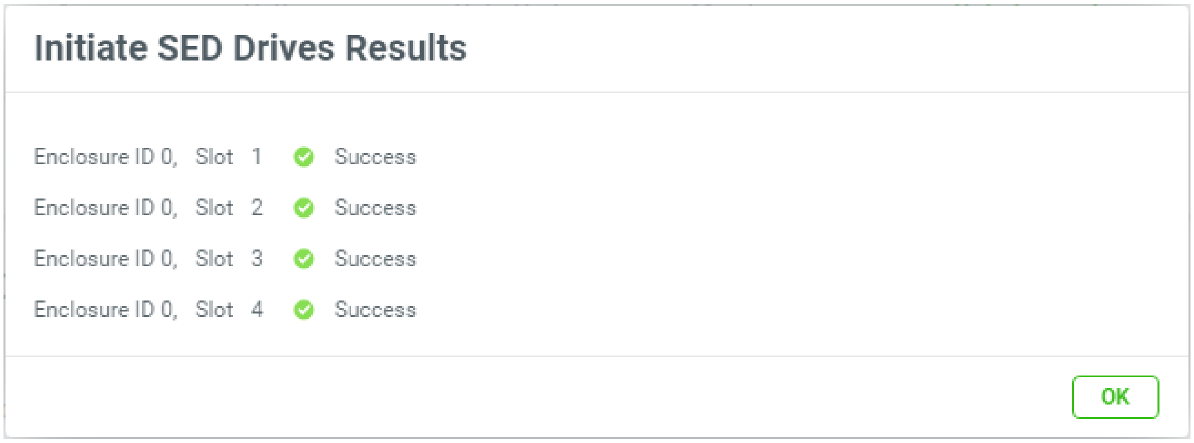
Selected Disks

4 Items

☑	!	Slot	SED Status	Capacity	Disk Type	Status
☑	●	1	Disabled	1.75 TB	SAS SSD 12.0Gb/s	Online
☑	●	2	Disabled	1.46 TB	SAS SSD 12.0Gb/s	Online
☑	●	3	Disabled	1.46 TB	SAS SSD 12.0Gb/s	Online
☑	●	4	Disabled	372.36 GB	SAS SSD 12.0Gb/s	Online

Figure 9 Initiate SEDs

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



Initiate SED Drives Results

Enclosure ID 0, Slot 1 ✓ Success

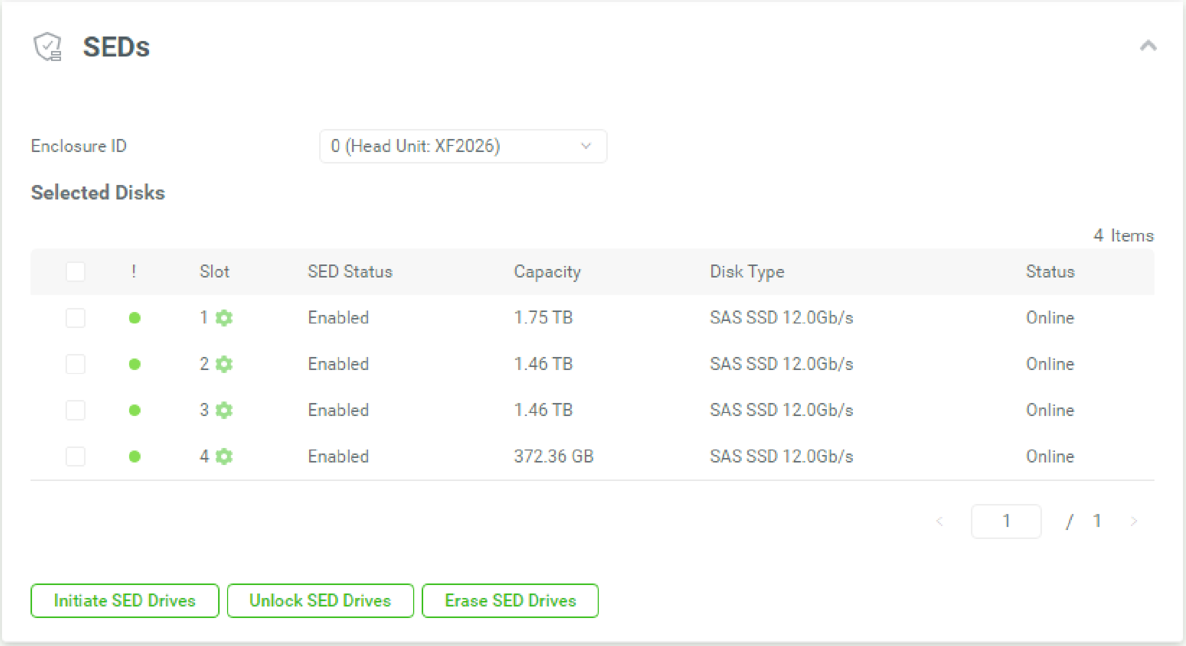
Enclosure ID 0, Slot 2 ✓ Success

Enclosure ID 0, Slot 3 ✓ Success

Enclosure ID 0, Slot 4 ✓ Success

Figure 10 Initiate SED Results

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



SEDs

Enclosure ID: 0 (Head Unit: XF2026)

Selected Disks

4 Items

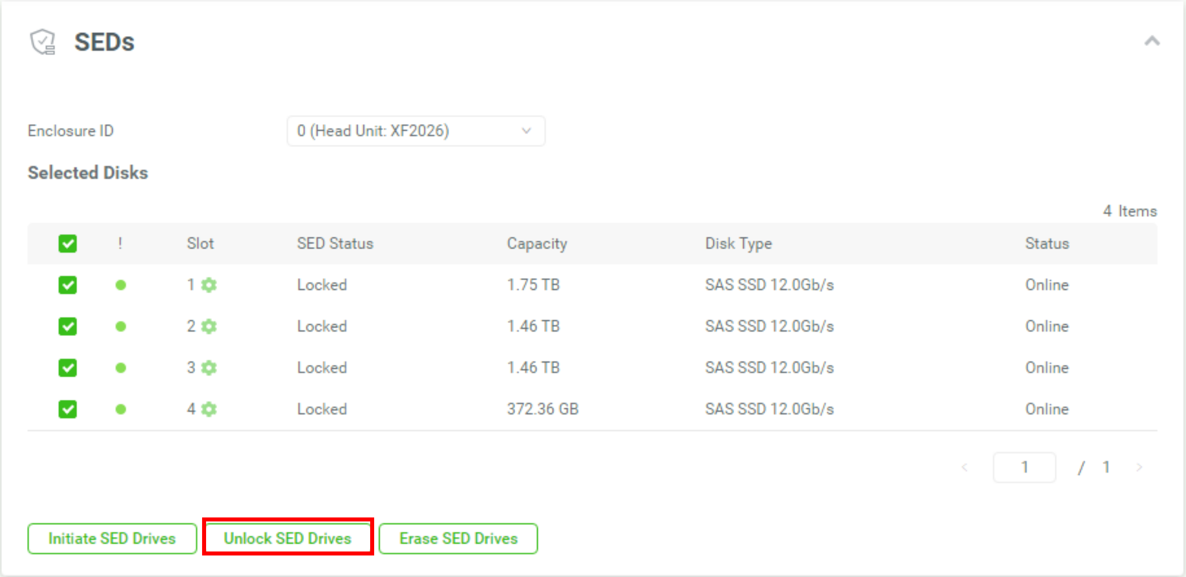
□	!	Slot	SED Status	Capacity	Disk Type	Status
□	●	1 ⚙	Enabled	1.75 TB	SAS SSD 12.0Gb/s	Online
□	●	2 ⚙	Enabled	1.46 TB	SAS SSD 12.0Gb/s	Online
□	●	3 ⚙	Enabled	1.46 TB	SAS SSD 12.0Gb/s	Online
□	●	4 ⚙	Enabled	372.36 GB	SAS SSD 12.0Gb/s	Online

Figure 11 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.



Enclosure ID: 0 (Head Unit: XF2026)

Selected Disks

4 Items

☑	!	Slot	SED Status	Capacity	Disk Type	Status
☑	●	1	Locked	1.75 TB	SAS SSD 12.0Gb/s	Online
☑	●	2	Locked	1.46 TB	SAS SSD 12.0Gb/s	Online
☑	●	3	Locked	1.46 TB	SAS SSD 12.0Gb/s	Online
☑	●	4	Locked	372.36 GB	SAS SSD 12.0Gb/s	Online

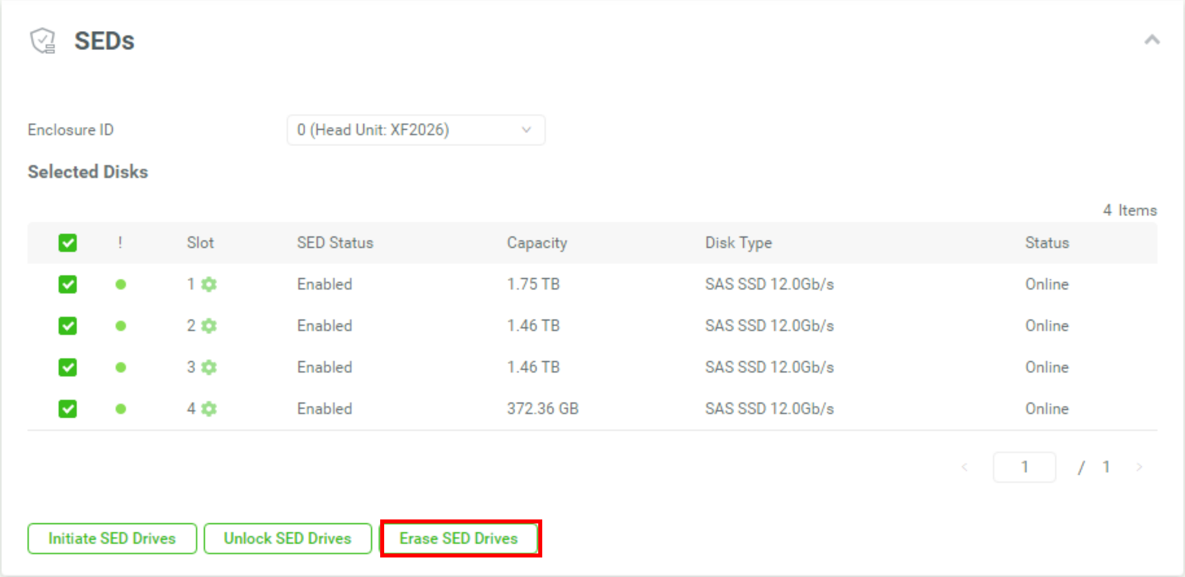
Figure 12 Unlock SEDs

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.



SEDs

Enclosure ID: 0 (Head Unit: XF2026)

Selected Disks

4 Items

☑	!	Slot	SED Status	Capacity	Disk Type	Status
☑	●	1 ⚙	Enabled	1.75 TB	SAS SSD 12.0Gb/s	Online
☑	●	2 ⚙	Enabled	1.46 TB	SAS SSD 12.0Gb/s	Online
☑	●	3 ⚙	Enabled	1.46 TB	SAS SSD 12.0Gb/s	Online
☑	●	4 ⚙	Enabled	372.36 GB	SAS SSD 12.0Gb/s	Online

Figure 13 Erase SEDs

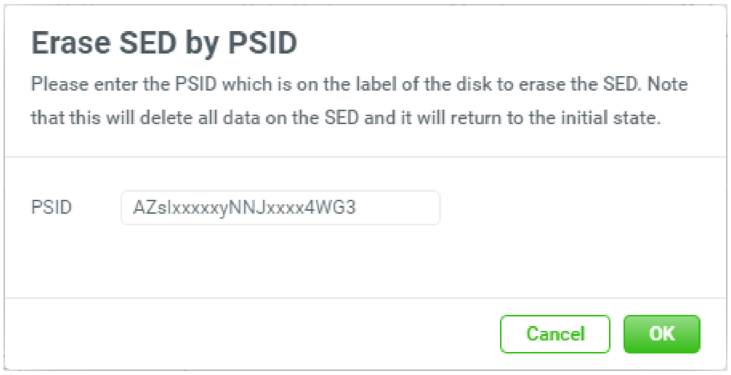
After proceeding, it will pop up a dialog to display the results. If the results are successful, the SED status will become Disabled.

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.



Erase SED by PSID

Please enter the PSID which is on the label of the disk to erase the SED. Note that this will delete all data on the SED and it will return to the initial state.

PSID: AZslxxxxxyNNJxxxx4WG3

Figure 14 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.

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.

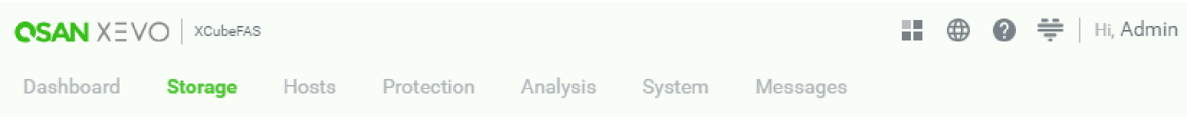
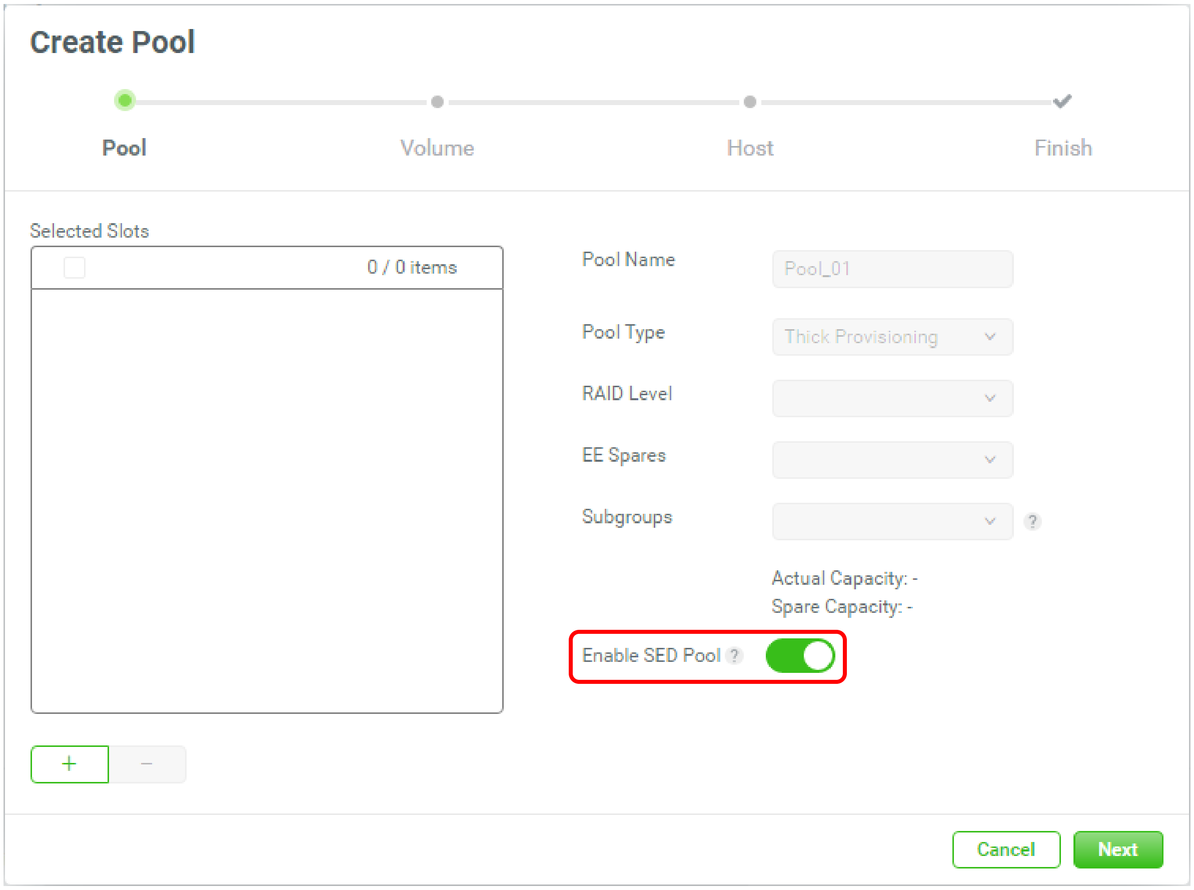


Figure 15 Storage Tab

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).



Create Pool

Selected Slots

0 / 0 items

Pool Name: Pool_01

Pool Type: Thick Provisioning

RAID Level

EE Spares

Subgroups

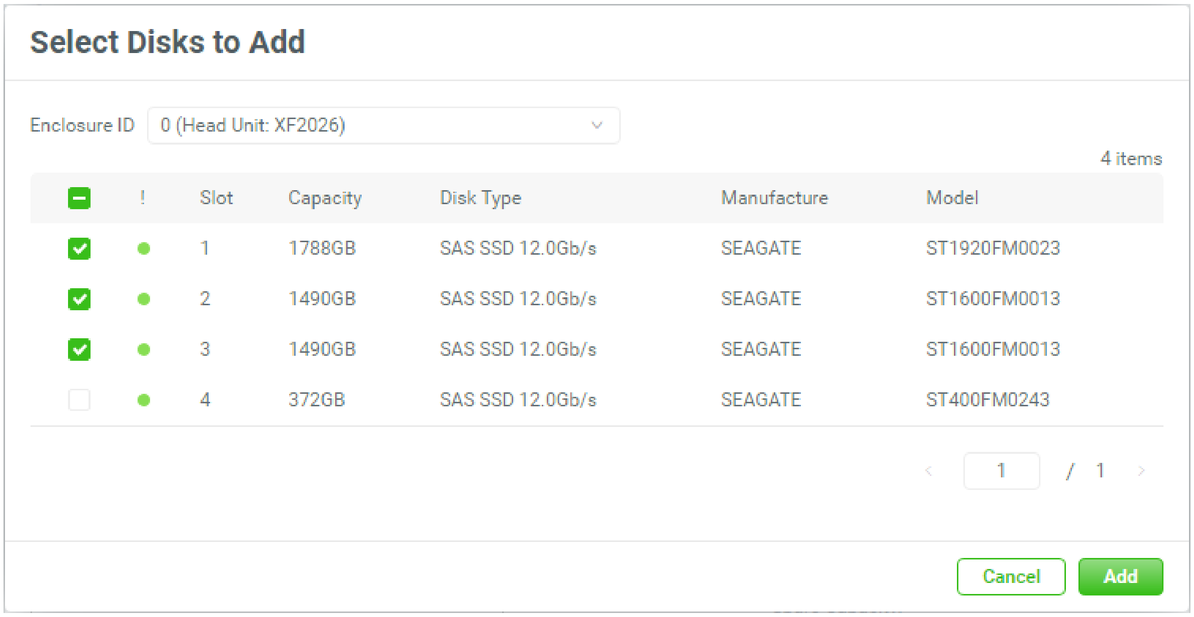
Actual Capacity: -

Spare Capacity: -

Enable SED Pool

Figure 16 Create an SED Pool Step 1

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



Select Disks to Add

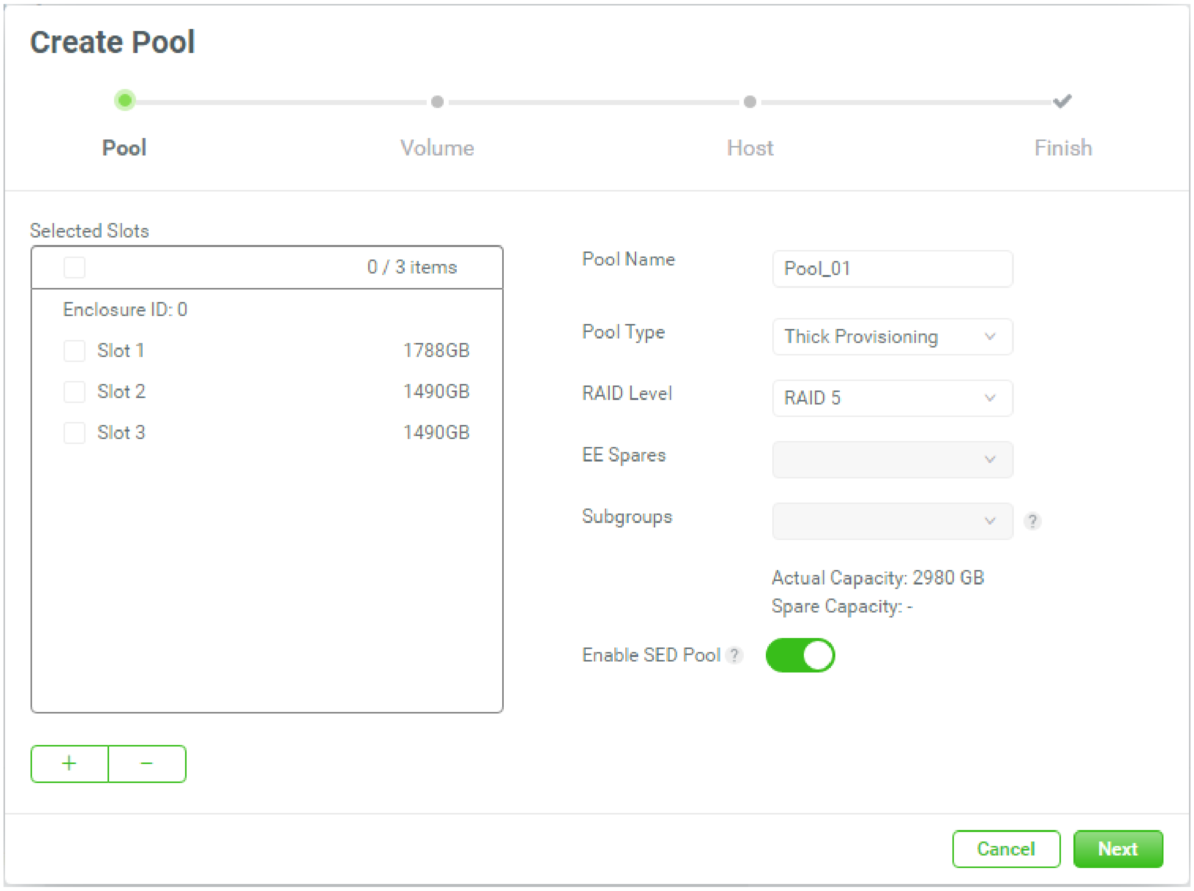
Enclosure ID: 0 (Head Unit: XF2026)

4 items

☐	!	Slot	Capacity	Disk Type	Manufacture	Model
☑	●	1	1788GB	SAS SSD 12.0Gb/s	SEAGATE	ST1920FM0023
☑	●	2	1490GB	SAS SSD 12.0Gb/s	SEAGATE	ST1600FM0013
☑	●	3	1490GB	SAS SSD 12.0Gb/s	SEAGATE	ST1600FM0013
☐	●	4	372GB	SAS SSD 12.0Gb/s	SEAGATE	ST400FM0243

Figure 17   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.



Create Pool

Selected Slots

□ 0 / 3 items

Enclosure ID: 0

□ Slot 1	1788GB
□ Slot 2	1490GB
□ Slot 3	1490GB

Pool Name: Pool_01

Pool Type: Thick Provisioning

RAID Level: RAID 5

EE Spares:

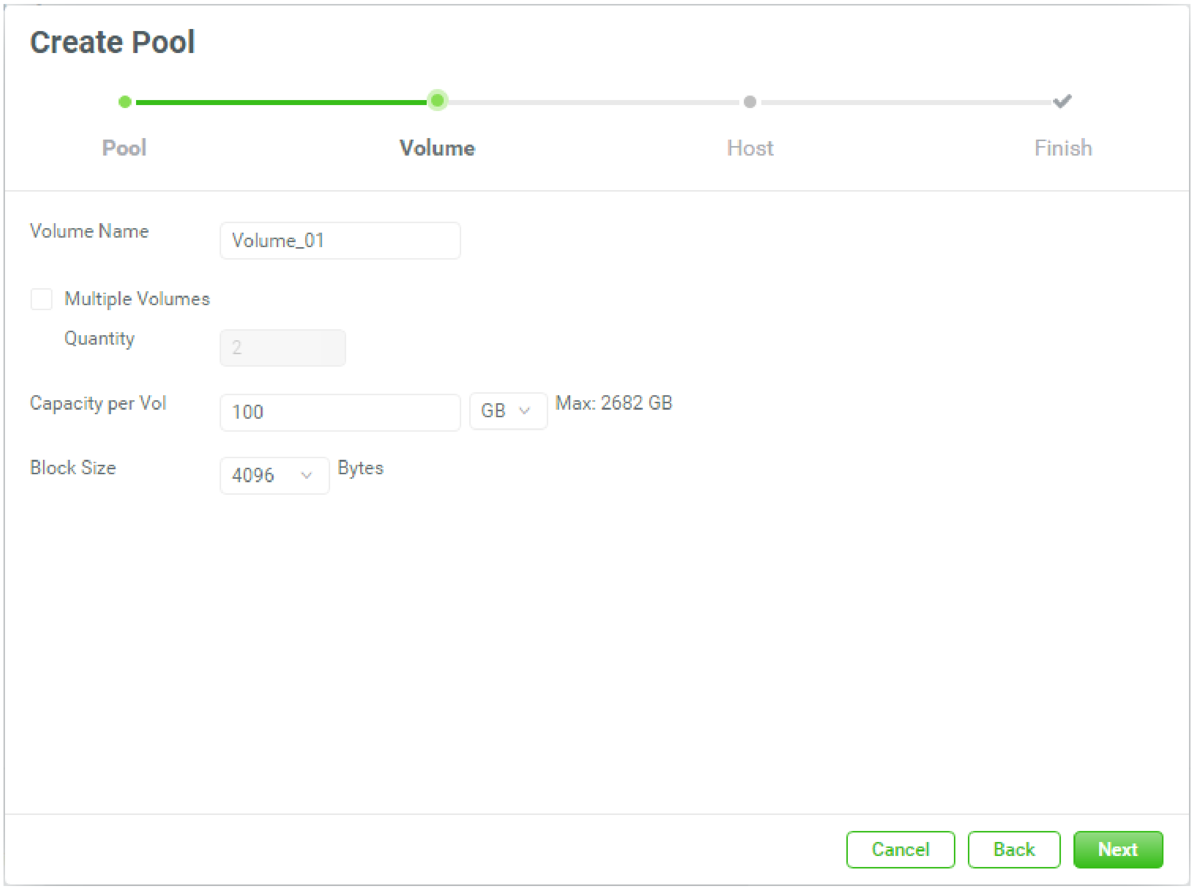
Subgroups:

Actual Capacity: 2980 GB
Spare Capacity: -

Enable SED Pool: On

Figure 18 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.



Volume Name: Volume_01

□ Multiple Volumes

Quantity: 2

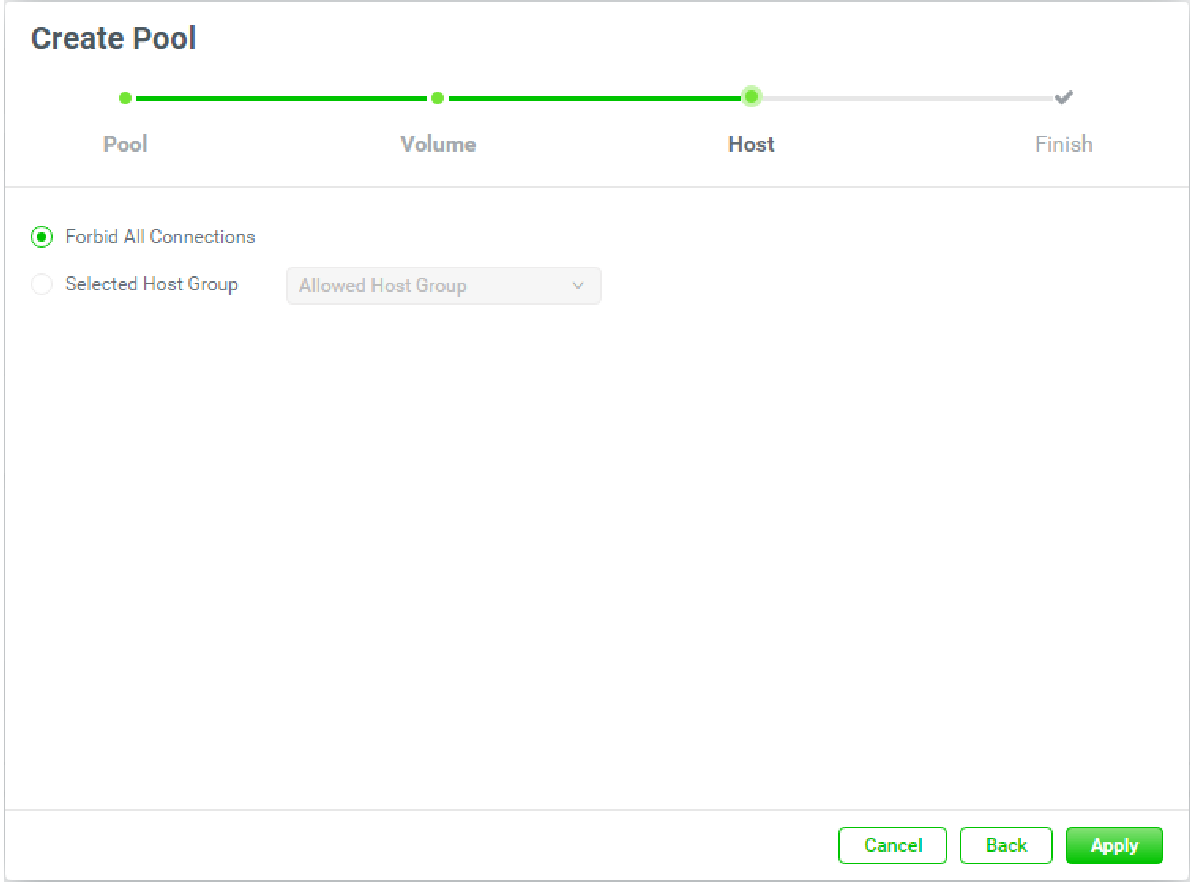
Capacity per Vol: 100 GB Max: 2682 GB

Block Size: 4096 Bytes

Figure 19 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.



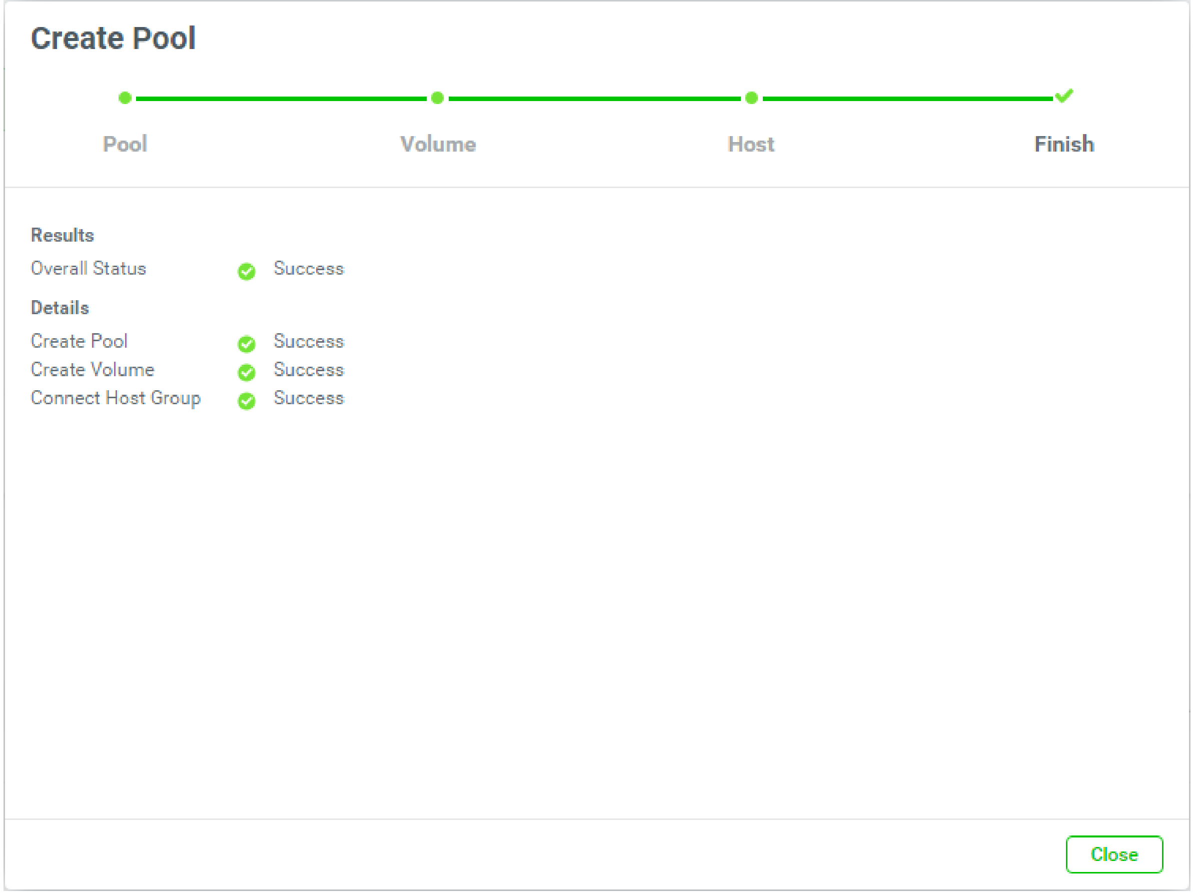
Create Pool

● Forbid All Connections

○ Selected Host Group — Allowed Host Group

Figure 20 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.



Results

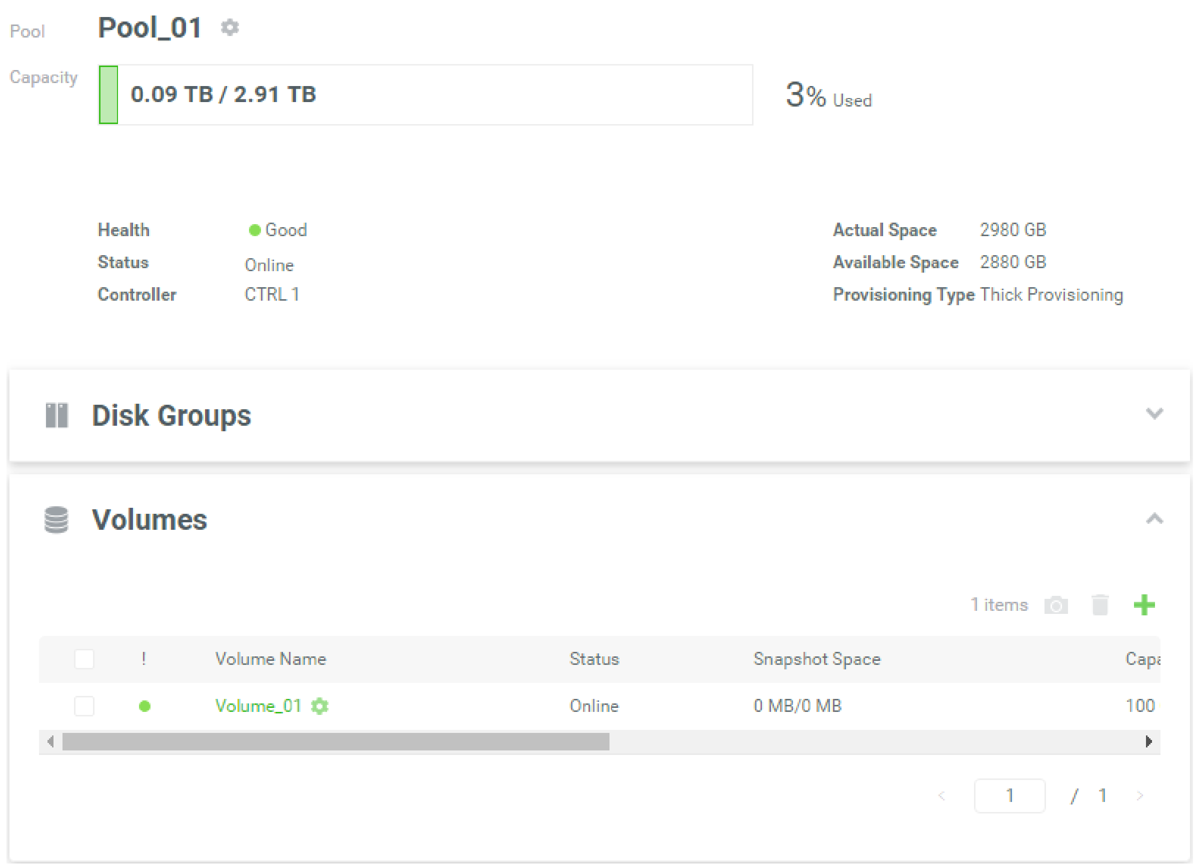
Overall Status	✓	Success

Details

Create Pool	✓	Success
Create Volume	✓	Success
Connect Host Group	✓	Success

Figure 21 Create a Pool Step 4

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



Pool Pool_01

Capacity 0.09 TB / 2.91 TB

3% Used

Health	● Good	Actual Space	2980 GB
Status	Online	Available Space	2880 GB
Controller	CTRL 1	Provisioning Type	Thick Provisioning

Disk Groups

Volumes

1 items

□	!	Volume Name	Status	Snapshot Space	Capa
□	●	Volume_01	Online	0 MB/0 MB	100

1 / 1

Figure 22 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.

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.

Rebuild on SED Pools

Rebuilding an SED pool will use SED as spare disk.

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

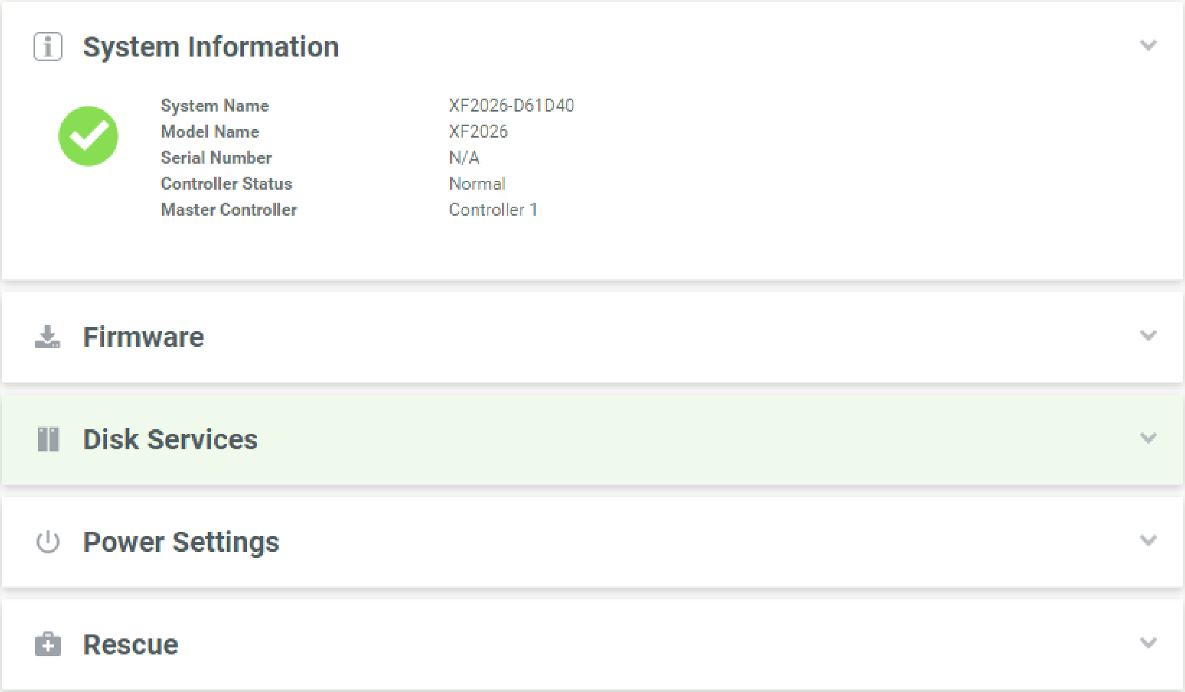
If executing local clone from an encrypted volume to a non-encrypted volume, it will pop up a warning message.

Remote Replication on Encrypted Volume

If executing remote replication from an encrypted volume, It will pop up a warning message.

Configure ISE Drives

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



System Name XF2026-D61D40
Model Name XF2026
Serial Number N/A
Controller Status Normal
Master Controller Controller 1

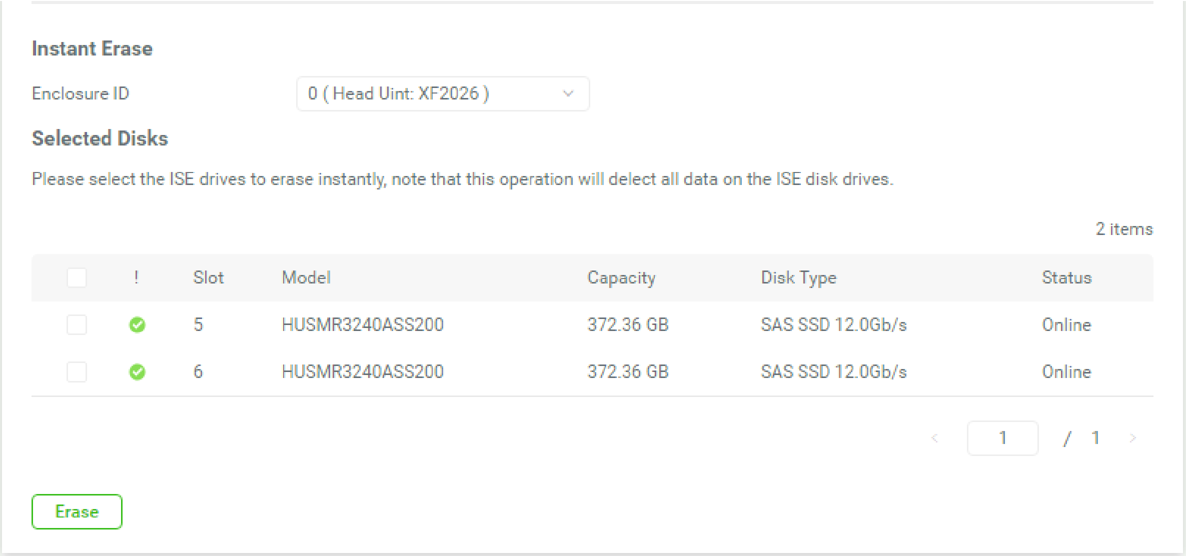
Figure 23 SEDs Pane

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

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)



Instant Erase

Enclosure ID: 0 (Head Uint: XF2026)

Selected Disks

Please select the ISE drives to erase instantly, note that this operation will delect all data on the ISE disk drives.

2 items

□	!	Slot	Model	Capacity	Disk Type	Status
□	✓	5	HUSMR3240ASS200	372.36 GB	SAS SSD 12.0Gb/s	Online
□	✓	6	HUSMR3240ASS200	372.36 GB	SAS SSD 12.0Gb/s	Online

Figure 24 List ISE Drives

This table shows the column descriptions.

Table 2 Disk Column Descriptions

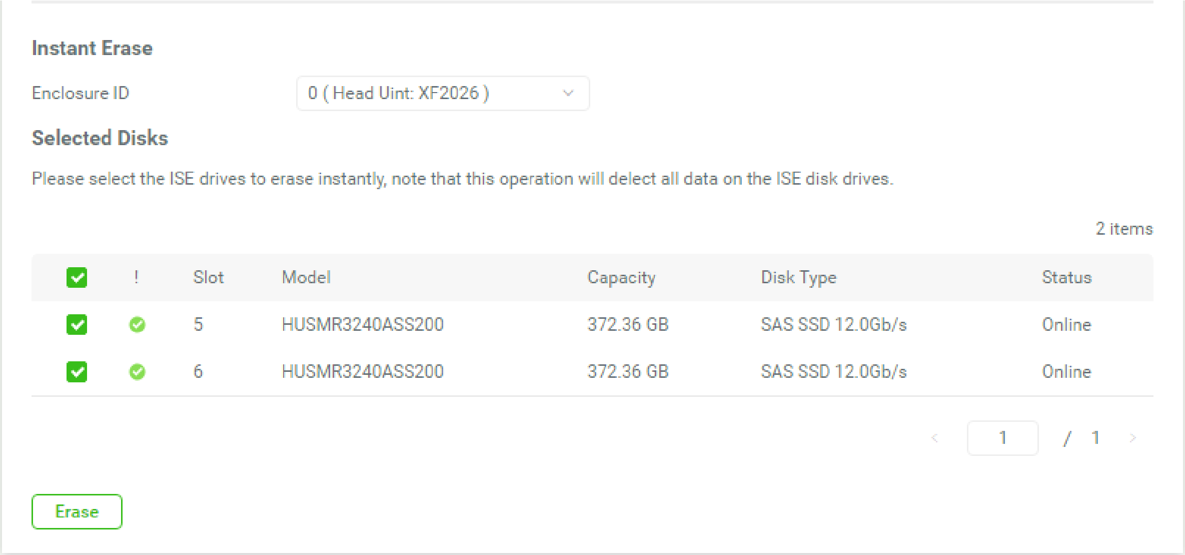
Column Name	Description
!	The status of disk health: • Green Color / Normal: The disk drive is good. • Orange Color / Abnormal: The disk drive has unrecoverable read errors or S.M.A.R.T. error. • Red Color / Warning: The disk drive has failed.
Slot	The position of the disk drive.
Model	The model name 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.

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.



Instant Erase

Enclosure ID 0 (Head Uint: XF2026)

Selected Disks

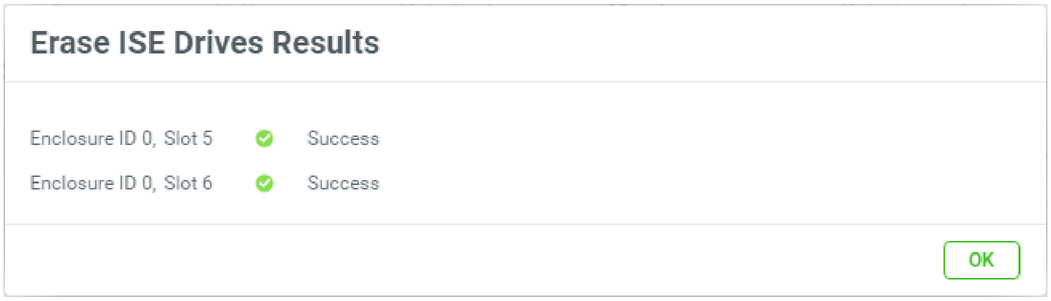
Please select the ISE drives to erase instantly, note that this operation will delect all data on the ISE disk drives.

2 items

☑	!	Slot	Model	Capacity	Disk Type	Status
☑	✓	5	HUSMR3240ASS200	372.36 GB	SAS SSD 12.0Gb/s	Online
☑	✓	6	HUSMR3240ASS200	372.36 GB	SAS SSD 12.0Gb/s	Online

Figure 25 Instant Erase ISE drives

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



Erase ISE Drives Results

Enclosure ID 0, Slot 5 ✓ Success

Enclosure ID 0, Slot 6 ✓ Success

Figure 26 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.

Conclusion

As data security becomes more popular, storage systems need to provide secure data to ensure the peace of mind, compliance, and general security use cases that cared by companies. Regardless of disk drives are lost, stolen, or failed, unauthorized persons cannot compromise the security of the organization by accessing any sensitive data.

Data encryption ensures that all sensitive user data stored on the array is encrypted as it is written to disk, so that private data does not fall into the bad guys. With SED & ISE technology support, it is a simple and useful function for protecting your data. Therefore, organizations can be assured that their data is always safe and secure when stored on the QSAN storage systems.

Apply To

- XCubeFAS XF2026 FW 1.1.0 and later

Reference

XCubeFAS XEVO Software Manual

- XCubeFAS XEVO Software Manual

Appendix

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