



QSM Security Trilogy Application Note

Unified storage series



QSAN Technology, Inc.
www.QSAN.com



Copyright

© Copyright 2021 QSAN Technology, Inc. All rights reserved. No part of this document may be reproduced or transmitted without written permission from QSAN Technology, Inc.

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

Trademarks

All products and trade names used in this manual are trademarks or registered trademarks of their respective companies.

QSAN Technology, Inc

4F, No. 103, Ruei Hu, St. Neihu Dist, Taipei 114 Taiwan, ROC

Tel ; +886-2-7720-2118

Fax : +886-2-7720-0295

Email :

sales@qsantechonology.com

Website :

www.qsan.com

Notices

This Unified Storage series white paper is applicable to all Unified Storage models and QSM version 3.3.0 or above.

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

Notices	i
Overview	3
Security Configuration Setting	4
First part - External Protection	4
Access Control	5
Firewall	7
Connection List.....	7
Second Part - Core Data Protection	9
WORM	9
Pool Encryption	10
Snapshot Lock.....	11
Anti-Virus.....	11
Third Part - Backup Protection	15
Snapshot	15
Remote Backup.....	23
Cloud Backup.....	28
XMirror	31
QSAN Security Trilogy – Summary	36
Appendix	37
Related Documents	37
Technical Support.....	37

Overview

The importance of data is becoming more and more important in today's company. At the same time, cyber attacks are also emerging. Various targeted attacks will cause service suspension or further blackmail your company. In order to avoid all kinds of losses, QSM provides three ways quick security protection trilogy to help your business achieve the best data protection.

QSM data security trilogy include external protection, core data protection and data backup to strengthen the company's information security system.



In this application note, we will show you how to setup from external to backup protection in QSM and help you business data safe.

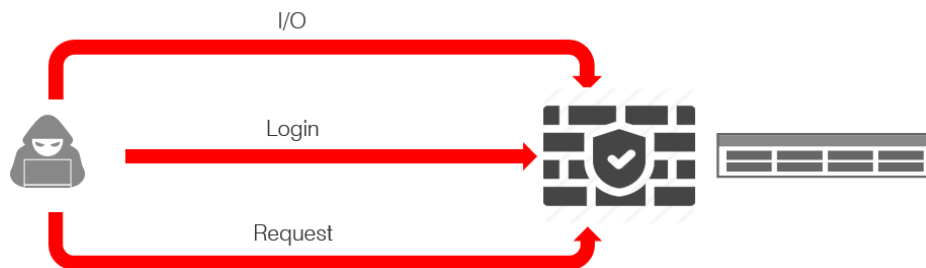
Security Configuration Setting

This chapter provides an overview of the settings available to ensure the secure operation of the product.

First part - External Protection

For external protection, many hackers will use various methods to attack your corporate data, such as DDOS or constantly log in to crack the password etc... and will try to enter your system to cause more serious damage.

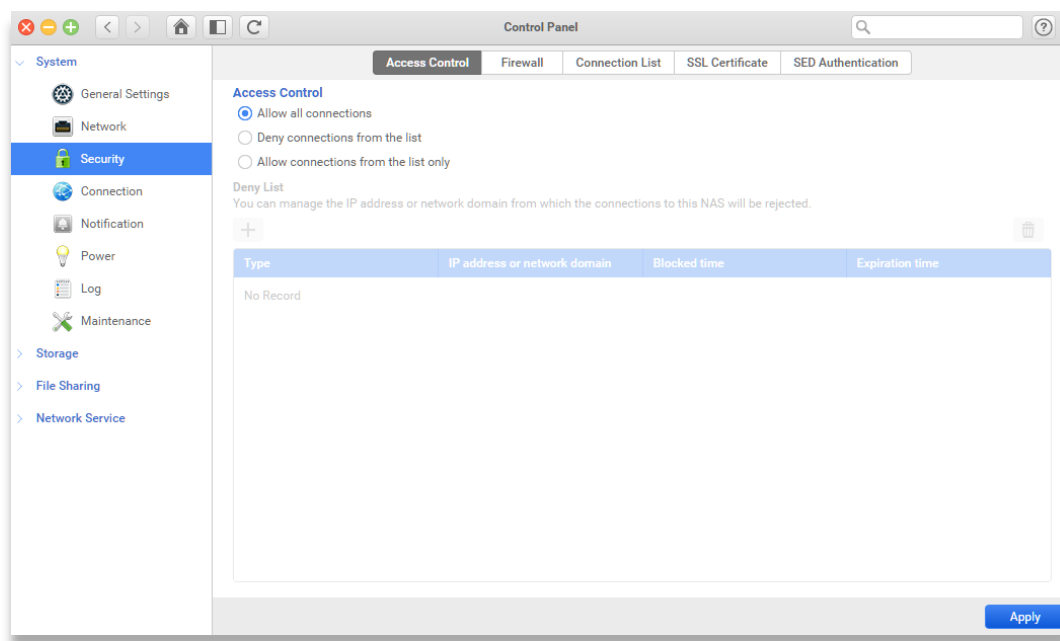
The first part of QSM security trilogy – External Protection allows you to prevent hackers from trying to invade or block corporate services from various protocols or networks through access control.



And we will show you how to set up all these function below.

Access Control

You can allow all connections or a particular IP or IP ranges. Once the IP is set to deny, the host will not be capable of connecting to the device unless the setting is removed. This can prevent all unfriendly access or attack that try to hurt your system.



Add a deny connection list

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

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

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

Add an allow connection list

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

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

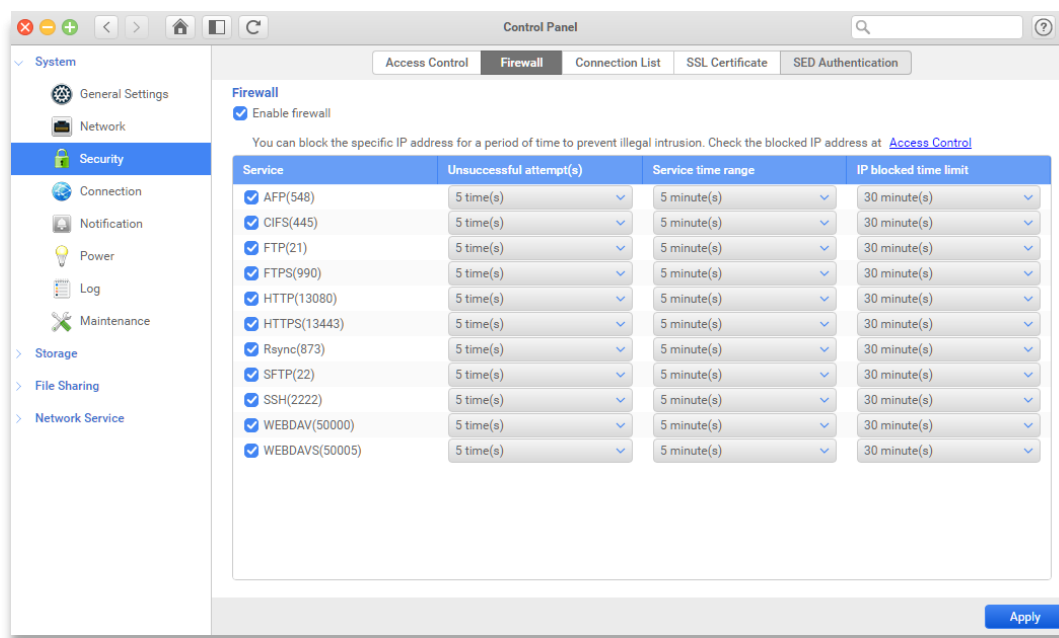


INFORMATION:

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

Firewall

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



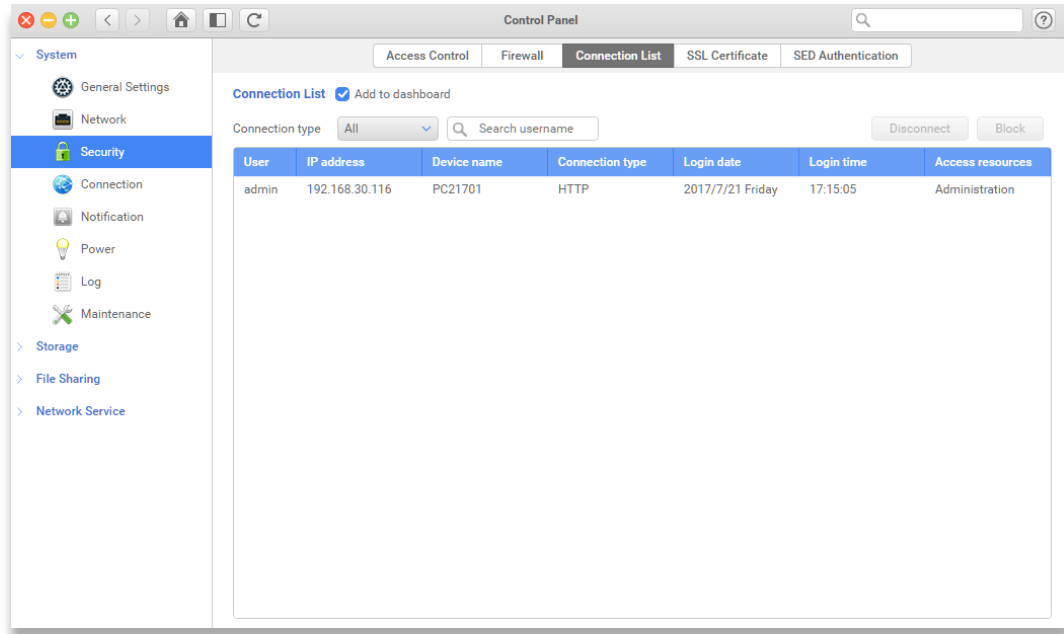
Enable Firewall

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

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

Connection List

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



Viewing a particular file service

To view the particular file service, please follow the steps below:

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

Disconnect a user from the list

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

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

Block a user from the list

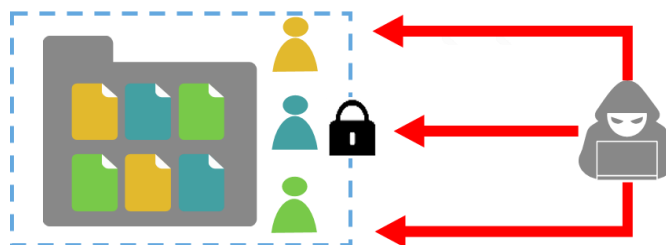
To block the user from the list, please follow the steps below:

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

Second Part - Core Data Protection

When hackers invade your system, they will try to steal your data or use ransomware to lock your system and ask you to pay to have your data restored. The most important treasure of your business is data, and data loss will cause huge impact to your business, so the protection of core data is very essential and important to your business.

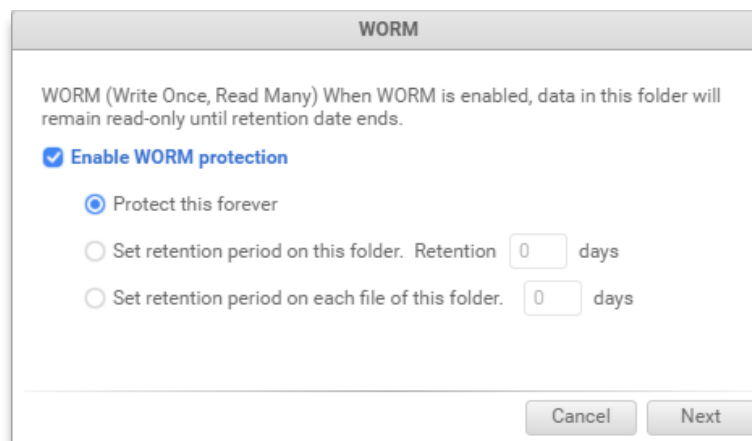
The second part of QSM security trilogy – Core data protection provides a variety of data protection, blocking data from being tampered or encrypted from the first line, and searching for malicious programs to prevent intrusion from backdoor.



And we will show you how to set up all these function to protect your data.

WORM

When WORM is set on the selected shared folder, all data under this folder would be remained read-only. Contents cannot be deleted, moved or modified by any user until the retention period expires. This can protect your data from being lock by ransomware.

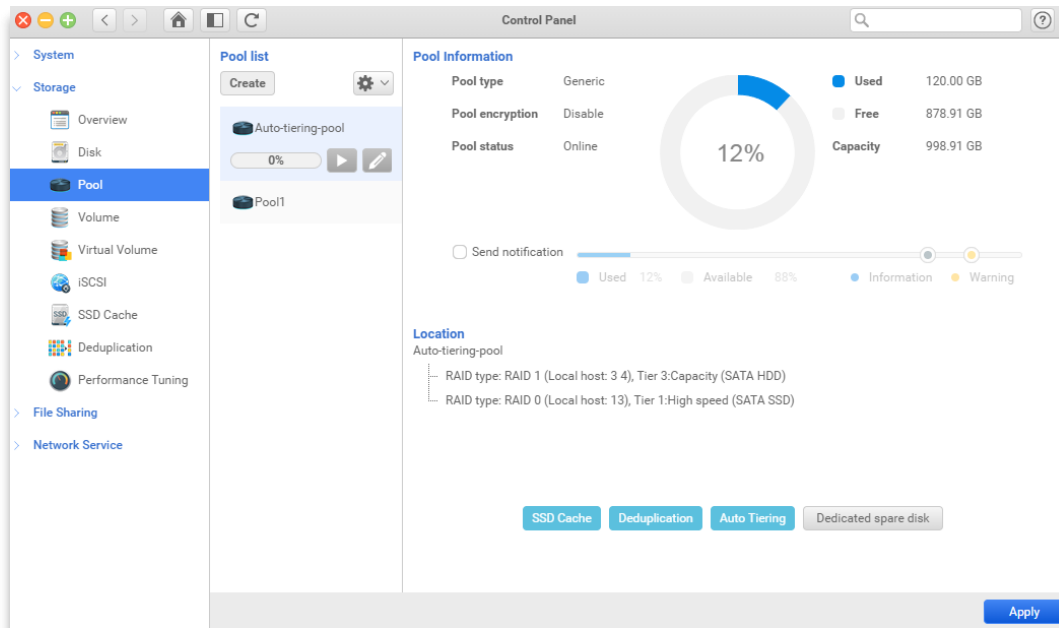


There are 3 WORM options you can set on a shared folder:

- **Forever protection** : guarantee a shared folder will never be modified.
- **Set retention period on this folder** : guarantee all files in this shared folder will not be modified.
- **Set retention period in each files of this folder** : guarantee files in this shared folder will not be modified counting from the time being added in.
- **Delete** : Delete the shared folder.

Pool Encryption

Pool encryption is a software based encryption to improve the data security and support highest level AES 256-bit encryption.



1. Click the **Create** button at the top of the **Pool list**.
2. After the setting of your pool, you will a checkbox for pool encryption, just click



TIP:

1. This feature supports only SED drives.
2. If your SED authentication has been created, you will not need to enter password again.

3. .Setup your password and finish the rest of the process.









INFORMATION:


1. Pool encryption password: a-z, A-Z, 0-9, -_!@#\$\$%^&*()_+=?

Snapshot Lock

Lock your snapshots from changes by any malware and any accidental deletion, providing a double protection to your data.

Last access status		2021, Tuesday, May. 18, 23:59:57	
<input checked="" type="checkbox"/> Used	0.00GB	Type	Folder
<input type="checkbox"/> Snapshot	0.00GB	Max snapshot	128 
<input checked="" type="checkbox"/> Free	383GB	Schedule	Disable 
Capacity	383GB	Clone from	-

Backup time	Total snapshots: 1
2021, Tuesday, May. 18, 23:59:57	

1. Take a snapshot.
2. Select the snapshot you want to lock, and click the lock icon.
3. Check your snapshot has a locked icon.

Anti-Virus

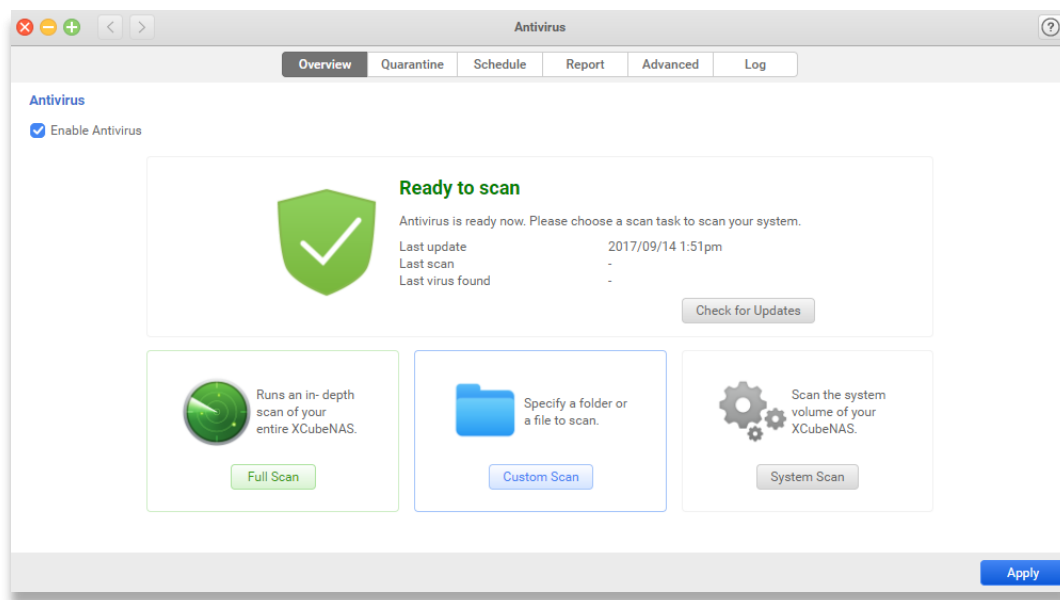
Antivirus is a full-featured security application which can protect your system. It will check the database update automatically and schedule a scan in the background.

You can check your current status, or prepare a scan for your Unified storage.

Requirement:

1. Please click the checkbox to enable Antivirus, then click **Apply** to confirm.

2. If you are using Antivirus for the first time, please click on **Check for Updates** on the **Overview** page, then select **Update Now** to download the virus database.
3. Make sure there are at least 512 MB of free storage space in your system volume before downloading virus database.
4. Check your network connection before downloading virus database.



Check the system status:

The icon and the messages in the center of the page will display the current status of **Antivirus**. The status may appear as follows:

1. Inactive: Antivirus is disabled and cannot be used. If you would like to use this function, please click **Enable Antivirus** checkbox then click **Apply** button.
2. Ready to scan: Antivirus is ready, you can choose one of the scan tasks below and start to scan now.



TIP:

You can check if your database is the latest version by clicking Check for Updates button, then click **Update Now** button to update.

3. New version available: You can click **Update Now** button to get the latest version.



TIP:

This status will be shown if you disable automatic update. You can always change the update settings on Antivirus > Advanced page to ensure that your virus database is always the up-to-date version.

4. Checking network connections: It will be shown when downloading or updating the virus database.
5. Update failed: System pool abnormal: This is a system error message. If you see this status during the update process, please check if there is enough storage capacity on your system pool
6. Remote server error: This is a system error message. If you see this status, please check your network settings on **Control Panel > Network > Interface** or contact QSAN support team for further information
7. Updating virus database: This status means the system is updating to the latest virus database now. Please note that the updates may fail if you disconnect the network connection on your system.
8. Scanning: The system is in the scanning process now. Please note that the process may fail if you disconnect the network connection on your system.
9. Protected: It will be shown after the scanning process if there are no viruses found on your system.
10. At risk: It will be shown when any viruses are found on your system. You can check the infected file(s) on **Quarantine** page or on **Report** page to see more scanned results.

Scan your system

There are three types of scan: **Full Scan**, **Custom Scan** and **System Scan**. To scan your system, please follow these steps below:

1. Choose the scan type you would like to proceed:
 - Full scan: Scan all the data on your Unified storage, including your USB if mounted. It is recommended to select this option if you are not sure whether there are any potential threats on your Unified storage.
 - Custom scan: Only scan the selected folders or a specific folder on your Unified storage.
- ① Click **Custom Scan** button.

- ② Choose a folder you would like to scan.
 - ③ Click **Confirm** button to scan.
 - System scan: To scan the system volume on the Unified storage.
2. If you want to stop scanning during the process, please click the Stop button.

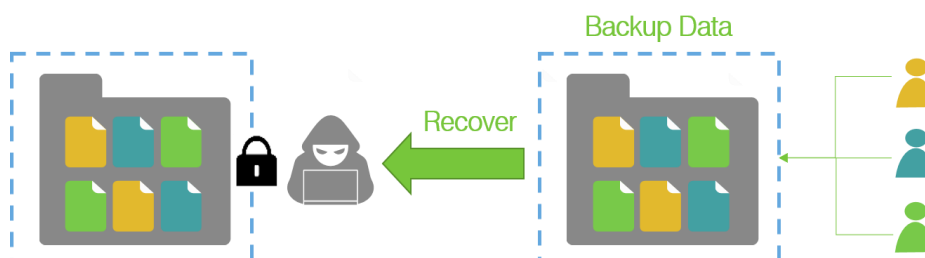
**INFORMATION:**

1. The infected file(s) will be moved to Quarantine automatically and also shown on the Report page by default. If you only want to view the virus information on the Report page, please go to Antivirus > Advanced page for further settings.
 2. Remote folders (like CIFS/SMB, FTP, SFTP, WebDAV...etc.) mounted on your Unified storage will not be scanned during full scan.
 3. It is recommended not to scan files larger than 2048 MB or the system performance will be slightly influenced.
 4. The probability of successfully finding viruses hidden in archive files (such as ZIP, RAR, ARJ, Tar, Gzip, Bzip2) will be slightly lower.
-

Third Part - Backup Protection

Data is the core competitiveness of enterprises, and data security has always been an important issue for enterprises. Whether it is hardware failure or cyber attack, data loss or theft and other disasters will directly affect the competitiveness of enterprises. Regular data backups can be used when data is accidentally damaged or deleted, and emergency disaster recovery can also be achieved.

The third part of QSM security trilogy – Backup protection provides various data backup methods to ensure immediate recovery when a disaster happens, minimizing service interruption.

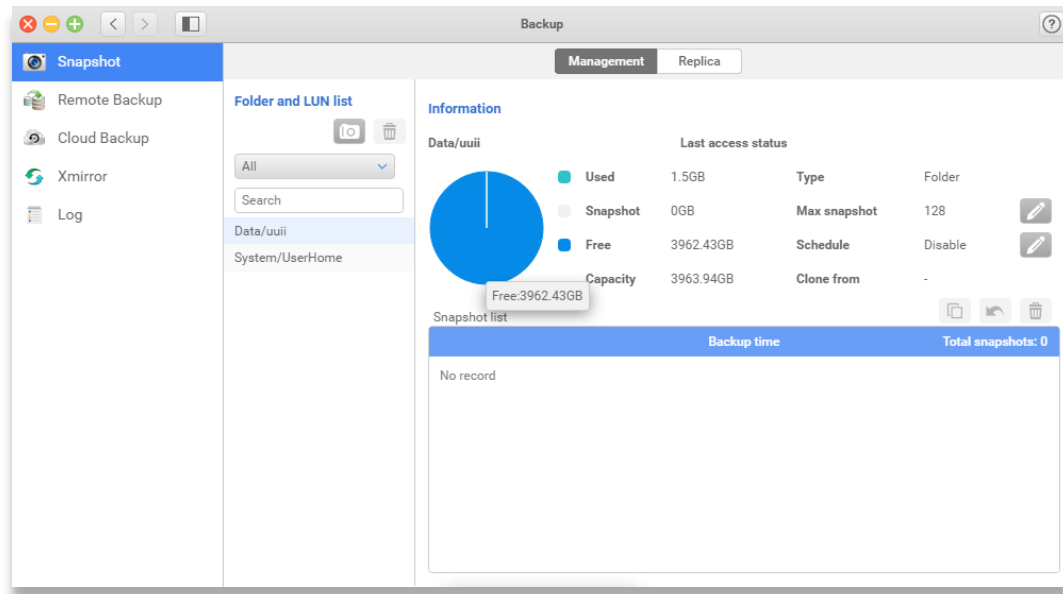


And we will show you how to set up all these function to backup your data and recover when accident happen.

Snapshot

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

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



Take Snapshots

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

To take a snapshot, please follow the steps below:

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

Manage Snapshots

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

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

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

**INFORMATION:**

1. Maximum snapshots for the entire system is 4096.
2. Default snapshot amount for a shared folder or LUN is 8.
3. Default snapshot rotation policy is set to Stop when reaching the maximum amount.

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

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

**INFORMATION:**

The start time is based on the system time.

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

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

**INFORMATION:**

1. If you clone this snapshot of folder/ LUN, it will be created a new "Clone Folder/ Clone LUN" and shown on the "Folder and LUN list."
2. If you clone the snapshot of folder, the Windows ACL permissions of each file that from parent share folder will be copied to the snapshot of the folder. However, the share permission of this snapshot of the folder is admin-use-only.

To Roll back data, please follow the steps below:

1. Select the folder or LUN on the **Folder and LUN list**.
2. Select the Snapshot on the **Snapshot list** table.

3. Click the **Roll back** icon in the second position on the top right side of snapshot list table.
4. Click **Confirm** button to finish the action.



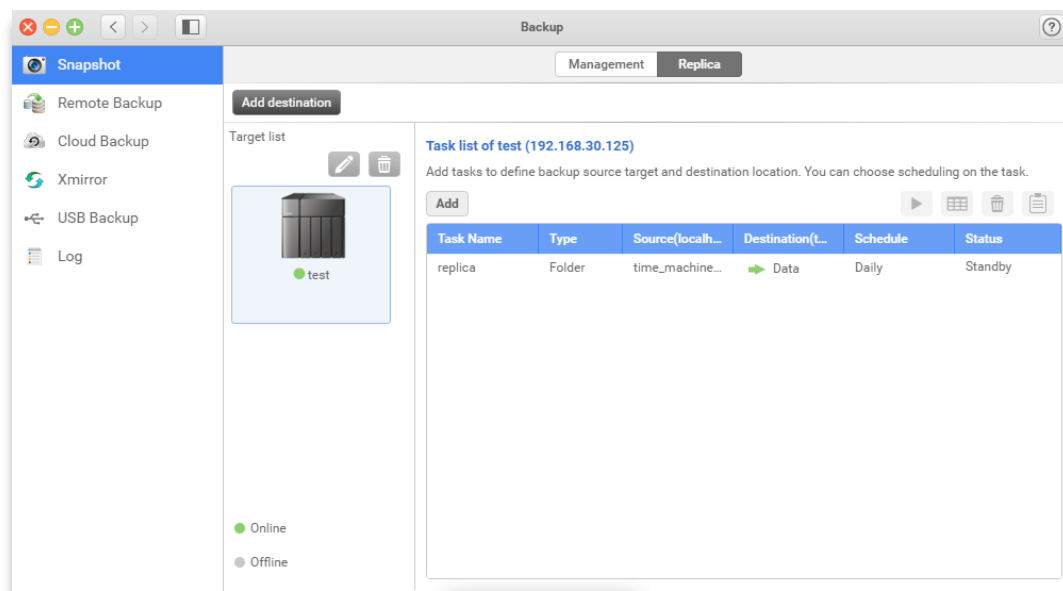
INFORMATION:

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

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

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

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



How to add a destination

Before replicating snapshots to the remote site, you will need to add at least one destination to store your snapshots. Meanwhile, you can create, edit, delete, and schedule for a replica task.

To Add destination, please follow the steps below:

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



INFORMATION:

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

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



TIP:

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

4. Enter a name for your Target.



INFORMATION: Target name naming rule.

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

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

How to edit or delete the destination

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

To edit the destination, please follow the steps below:

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



CAUTION:

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

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

To delete the destination, please follow the steps below:

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

How to create a task for a destination.

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

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



INFORMATION: Task name naming rule.

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

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



INFORMATION: Task name naming rule.

Replica Folder naming rule

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

Replica LUN and SRM naming rule

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

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

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

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

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

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

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

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.

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

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

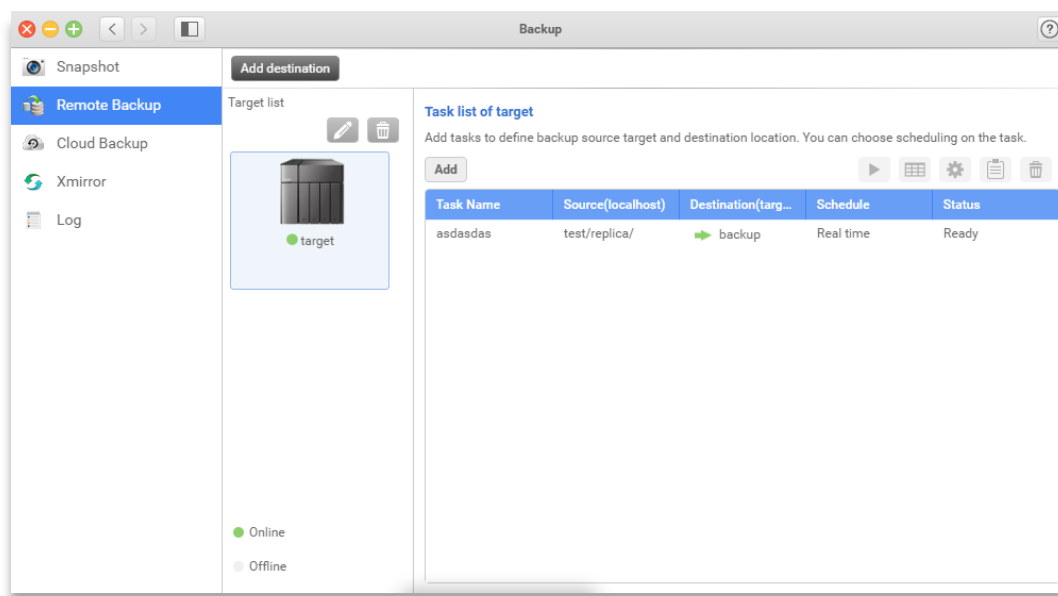
1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. The confirm window will pop out. Click **Confirm** button to delete the task.

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

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

Remote Backup

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



How to add a destination

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



TIP:

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

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

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



TIP:

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

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



INFORMATION: Target name naming rule

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

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



TIP:

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

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

How to edit or delete the destination

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

To edit the destination, please follow the steps below:

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



CAUTION:

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

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

To delete the destination, please follow the steps below:

1. Select a destination on the **Target list**.

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

How to create a task for a destination.

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

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



INFORMATION:

Task name naming rule:

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

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

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

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

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

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

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

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

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

1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Option** button.
4. Set the policy and file filter for the task.



INFORMATION:

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

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

-
- You can setup the filter for the following types

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

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

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

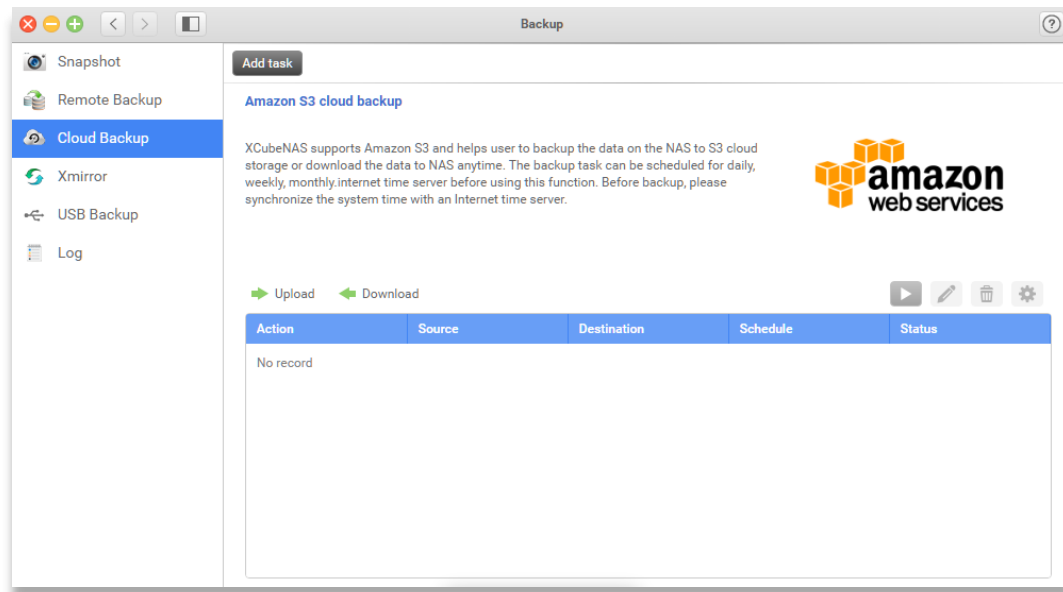
1. Select a **Target** on the **Target list**.
2. Select a task on the **Task list**.
3. Click the **Log** button.
4. The detail information window will pop out. Click **OK** button to close the window.

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

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

Cloud Backup

In Cloud Backup, QSM supports the public cloud, Amazon web services (S3), as the backup/restoration solutions to save your data with an additional off-site copy to prevent unexpected data loss from disks failures or physical system damage.



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

How to add a task

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

To add a Task, please follow the steps below:

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



TIP:

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

5. Select a folder on your Unified storage and click confirm when you finish setting.
6. Set the schedule for your task. You can set it as **Manually**, **Real time**, **Daily**, **Weekly**, **Monthly**, or **Repeat** in a period of time of the time.
7. Check the summary of the task.
8. Click **Confirm** to finish the setting.

How to Stop/Stop the task

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

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

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

To edit the task

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

To edit the task, please follow the steps below:

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



TIP:

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

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

7. Check the summary of the task.
8. Click **Confirm** to finish the editing.

To delete the task

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

To Delete the task, please follow the steps below:

1. Select the task on the list shown below.
2. Click the **Delete** button at the top right corner.
3. Click **Confirm** on the confirmation window to delete the task.

To set the option for the task

While backing up data, you can make your backup even more smarter or security.

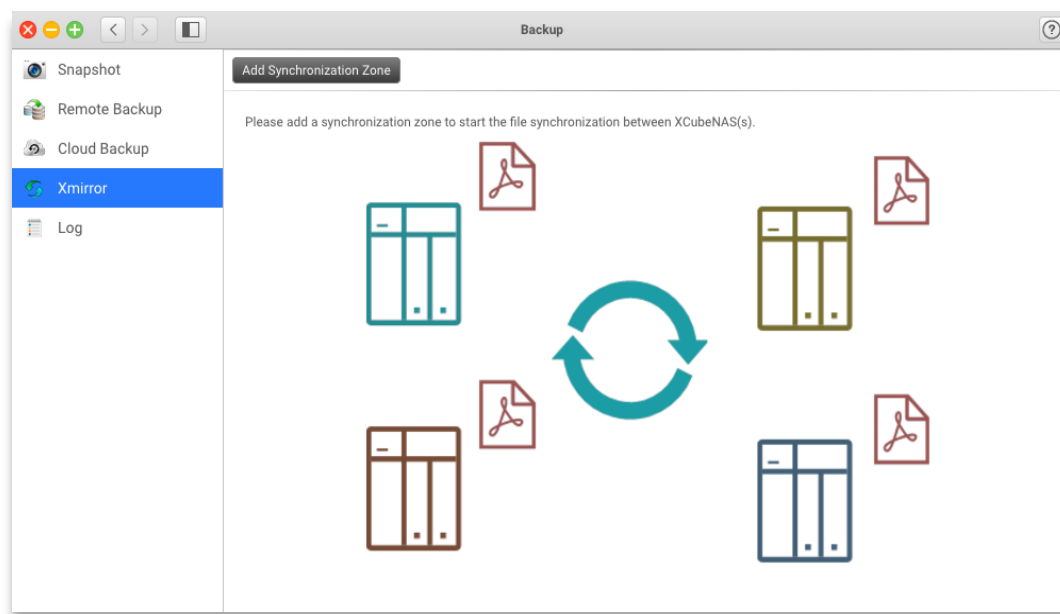
To set up the Option, please follow the steps below:

1. Select the task on the list shown below
2. Click the **Option** button at the top right corner.

Click the option(s) you want to set and click **Confirm** to finish the setting.

XMirror

In Xmirror, you can backup or synchronize your files between multiple Unified storage over Internet or local network.



Sync your data in a zone

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



INFORMATION:

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

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

1. Click **Add Synchronize Zone** on the top of the window.
2. In create wizard, you can choose to **Create a new zone** or **Join another zone from another NAS**.
3. Select create a new zone.
 - ① Specify the zone as 1-way zone or 2-way zone.

**INFORMATION:**

1. 1-way zone means you send files to the master folder and sync to others.
2. 2-way zone means you can change files in each folder and the changes will sync to all folders in the zone.

-
- ② Specify the zone name and select one folder in your local Unified storage.
 - ③ Check summary of the zone.
 - ④ Click **Confirm** to finish the action.
4. Select join another zone from another NAS
- ① Select one local folder.
 - ② Enter the remote destination information, IP, username, and password.

**TIP:**

You can click the dropdown menu to find all available Unified storage.

- ③ You can test the connection for authentication and performance between NAS.
- ④ Select a zone you want to join on the remote destination.
- ⑤ Check the summary of joining zone.
- ⑥ Click **Confirm** to finish the action.

Edit a zone

When the zone starts to sync, you can stop the syncing, delete the zone, edit the backup options, and check the detail information.

**INFORMATION:**

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

To stop the synchronization, please follow the steps below:

1. Select a zone.
2. Click the function button on the top right corner of the window.

3. Click **Stop** and the zone stop to sync right away.

To delete the zone, please follow the steps below:



TIP:

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

1. Select a zone
2. Click **Delete** button.
3. A confirmation window will pop out.
4. Click **Confirm** to finish the action.

To edit the option of the zone, please follow the steps below:

1. Select a zone
2. Specify the policy for SSL encryption during transmission.



INFORMATION:

The option is default on.

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



TIP:

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

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



INFORMATION:

1. Default maximum previous versions is 1
 2. When you lower the maximum previous versions amounts, the older files will be removed.
-

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

Edit a folder in the zone

After a folder is joined to the zone, you can disjoin it from the zone, change the local folder, rollback the file to the previous version, and restart the folder when it cannot be automatically be synced.

To disjoin the folder, please follow the steps below:

1. Select a domain folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Disjoin**.
4. A confirmation window will pop out.
5. Click **Confirm** to finish the action.

To change local folder, please follow the steps below:

1. Select the local folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Change local folder**.
4. Select a new folder.
5. Check the summary.
6. Click **Confirm** to finish the action.

To rollback the file on the previous version, please follow the steps below:

1. Select the local folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Version rollback**.
4. Select the file you want to rollback.
5. Select the file version.
6. Check the summary
7. Click **Confirm** to finish the setting.

To restart the folder, please follow the steps below:

1. Select the folder from the zone.
2. Click the function button in the top right corner of the zone.
3. Click **Restart**.
4. System will try to recover the folder.



TIP:

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

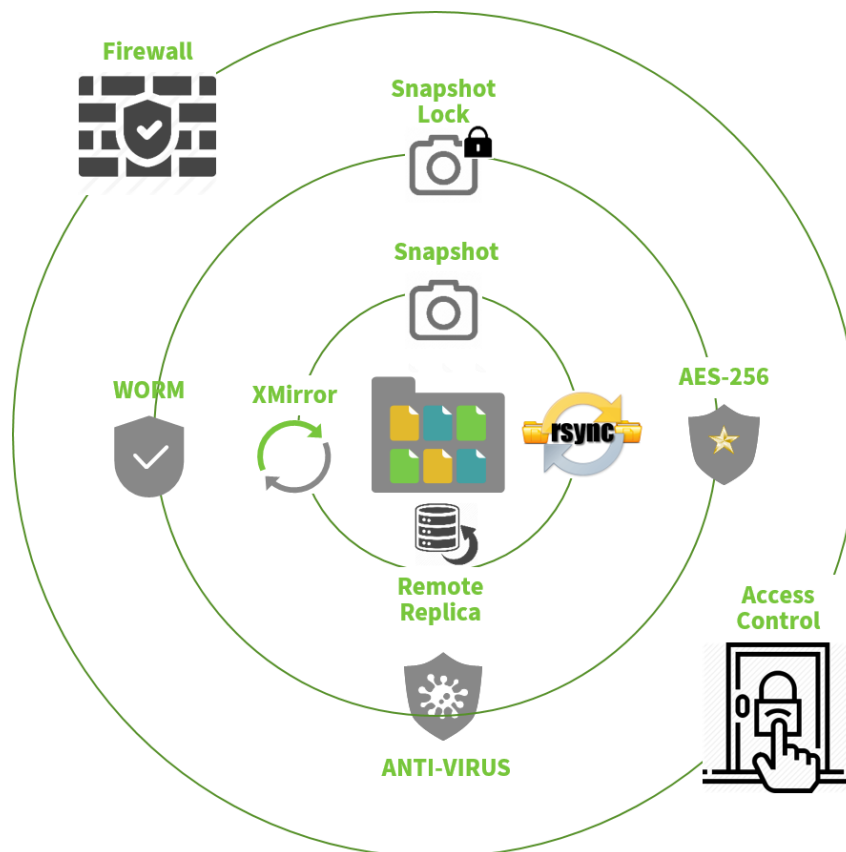
QSAN Security Trilogy – Summary

In the era of data explosion, the impacts of the cyber threats have been increased. For every business, the reliable data security solution is essential to protect the most important company's' assets for keeping business running.

With QSM we have three line to protect your data:

1. Access control and firewall to protect you from any unfriendly login.
2. All the encrypted and lock function to secure your core data.
3. All the backup function let you have second insurance.

Combine all three protection into QSAN security trilogy, and make sure your data is safe.



Appendix

Related Documents

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

- [All Unified Storage Documents](#)
- [Unified Storage QIG \(Quick Installation Guide\)](#)
- [Unified Storage Hardware Manual](#)
- [Unified Storage Configuration Worksheet](#)
- [QSM 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://qsan.com/support>
- Via Telephone: +886-2-7720-2118 extension 136
(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