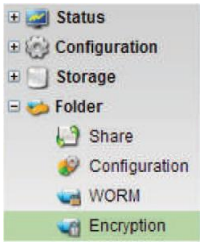
Managing Encrypted Folders

View the list of encrypted folders and add, delete, or edit an encrypted folder.

Go to

Folder > Encryption



What is Encryption?

An encrypted folder is password-protected with 256-bit AES encryption. The encrypted folder can only be used for normal read/ write access with the authorized password. The encryption protects the confidential data from unauthorized access even if the hard drives or the entire server were stolen.

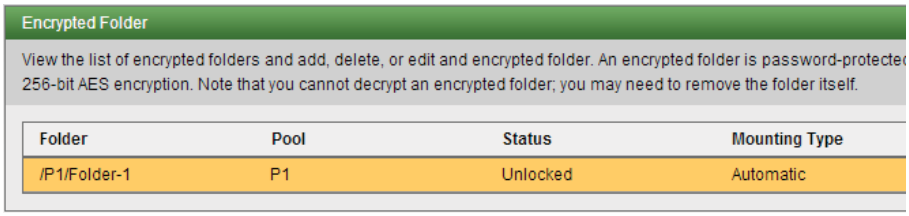
If the Encryption option has been enabled in a folder, the contents will not be retrieved. Using this function protects critical information from being leaked to external environment.

Notes

- The folder unmount function is only enabled when you enable the encryption function.
- You cannot decrypt an encrypted folder; you may need to remove the folder itself.
- To change the encryption password after a folder has been encrypted, you must first mount the folder and select the "Password" option and enter the new password.
- You do not need to enter a password when you copy data into a folder in which the Encryption option has been enabled. You only need to enter the password when you mount the folder.
- Once the Encryption option is enabled, users cannot disable it.

Viewing the List of Encrypted Folders

The list of existing encrypted folders will appear in a list. View their pool, status, and mounting type.

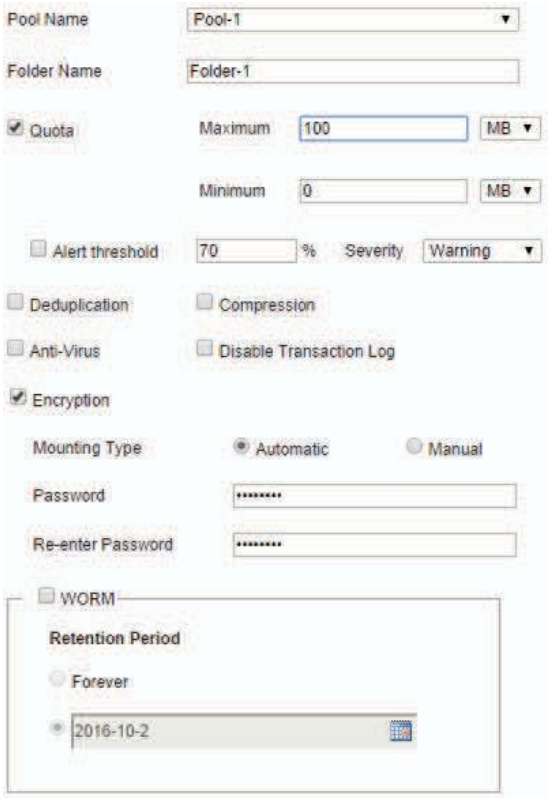


- To add a new encrypted folder, click Add.
- To edit an encrypted folder, click Edit or double-click a folder.

- To delete an encrypted folder, click Delete.

Creating a New Encrypted Folder

Click Add. Configure the parameters.



The new folder will appear in the list.

Parameters

Folder Name

Enter the name of the new folder.

Quota

Quota represents the maximum disk capacity allocated for the folder.

> The default minimum amount (0 GB) actually means “unlimited size.”

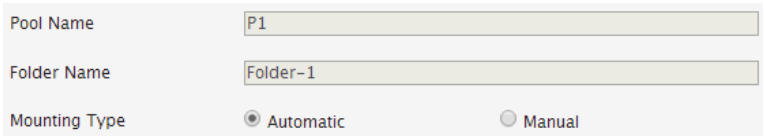
Quota/ Alert threshold

Quota represents the maximum disk capacity allocated for the folder.

> The default minimum amount (0 GB) actually means “unlimited size.”

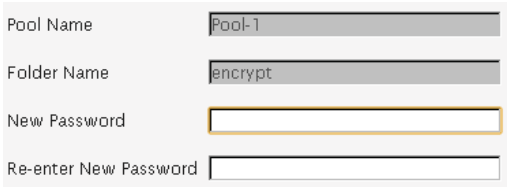
Once the quota setting is enabled, you can click Alert threshold, and then enter a value to set the usage percentage that will trigger a notification event when the value is reached. Choose from the Severity drop-down

	menu to set the severity of the event.
Deduplication	Reduces the amount of space for new data by integrating identical copies of data blocks. Deduplication does not change the size of the original data. Block deduplication takes more CPU processing power, but optimizes the use of storage space very effectively.
Antivirus	Enables antivirus scanning on the folder. This option will be disabled if no antivirus software is found on the computer.
Compression	Enables data compression for new data on the folder. Data compression uses LZJB algorithm, a lossless data compression algorithm, which does not consume much power compared to other algorithms. Compression does not change the size of the original data.
Disable Transaction Log	During data writes, NAS by default writes transaction log into the ZIL (ZFS Intent Log) in parallel. This design improves data integrity because the transaction log can be used to replay data writes after sudden interruption. To ensure the log can be kept safe during power outages, the log is stored in disk drives. By disabling this feature, you can improve performance since the host application no longer needs to wait until transaction log is written to the disk drives. Host application can continue new writes as long as the issued writes reach cache. When this feature is disabled, we recommend you to connect your NAS system to a UPS (Uninterrupted Power Supply) unit to ensure stable power supply.
Encryption	Enables folder encryption.
Mounting Type	Specifies how the encrypted folder will be mounted (unlocked). The following describes the mounting type and its status.

		Status/Mounting Type • Unlocked/Automatic: The folder will be mounted automatically when the system boots up. Currently, the folder is mounted. • Locked/Automatic: The folder will be mounted automatically when the system boots up. Currently, the folder is unmounted. • Unlocked/Manual: The folder will not be mounted until the user actively mounts it. Currently, the folder is mounted. • Locked/Manual: The folder will not be mounted until the user actively mounts it. Currently, the folder is unmounted.
	Encryption Password	Specifies the password for accessing the encrypted folder. The password must be 8 to 32 characters length.
	WORM	WORM stands for Write Once, Read Many. When this option is enabled, the files and sub-folders in the folder cannot be modified or deleted until the retention period expires. To activate the WORM option, follow these steps. Check the WORM checkbox. Set the retention period. If the retention period has been set to forever, the folder cannot be deleted unless the pool is destroyed. To view the list of WORM-enabled folders, go to the Folder > WORM menu.
Editing an Encrypted Folder	Select a folder and click Edit in the menu. The Editing screen will appear.  This option allows you to configure only the encryption aspect of the folder. To configure other parameters, you may do so from the Explorer menu.	
Parameters	**Mounting Type**	You may change the mounting type between Automatic and Manual.

Changing the Password

Highlight a folder and click the Password button.



Enter the new password and click OK.

Mounting/Unmounting an Encrypted Folder

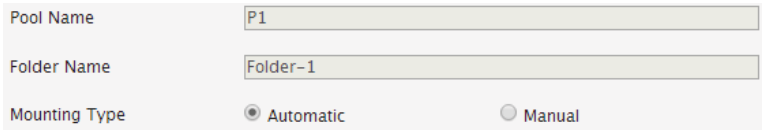
Unmounting a Folder

Select a folder and click Unmount in the menu. The Status of the folder should change accordingly.

- Locked = Unmounted

Mounting a Folder

Select a folder and click Mount in the menu.



The Status of the folder should change accordingly.

- Unlocked = Mounted

When Using Encrypted Folders for Remote Replication

An encrypted folder can be used as the source or target folder of remote replication, but there are some limitations, as described here.

If the source encrypted folder is unmounted

Replication will fail.

If the target encrypted folder is unmounted

A new target directory with the same name as the encrypted folder will be created.

Example:

- Rsync source: “/Pool-1/FolderA/SourceData/”
- Rsync target: “/Pool-2/FolderB/TargetData/”
- Folder “Pool-2/FolderB” is an encrypted folder and unmounted.

When remote replication starts, a new directory “TargetData” under “/Pool-2/FolderB/” will be created with replicated data from the source site.

When the user wants to mount the encrypted target folder later, a warning message will appear, indicating that a target directory already exists.

A folder with the same name as the encrypted target folder already exists in the target directory. If you mount the encrypted target folder, the existing folder and its files will be deleted.

- If the user chooses to proceed, the existing target folder and its data will be deleted, and the encrypted folder will be mounted.
- If the user chooses not to proceed, the encrypted folder will not be mounted until the existing target folder and its data are deleted.