iStorage®

DISKASHUR® 3 & DISKASHUR® PRO3

User Manual..... 2

Manuel de l'utilisateur..... 43

Benutzerhandbuch..... 84

Manuale utente..... 125

ユーザーガイド..... 166

Gebruikershandleiding..... 207

Manual del usuario..... 248

iStorage®

DISKASHUR® 3 & DISKASHUR® PRO 3

User Manual

This user manual is applicable to both diskAshur³ and diskAshur PRO³ and shall hereinafter be referred to as diskAshur³

Please make sure you remember your PIN (password), without it, there is no way to access the data on the drive.

If you are having difficulty using your diskAshur³ please contact our support team by email - support@istorage-uk.com or by phone on +44 (0) 20 8991 6260.

RoHS Compliant

REACH COMPLIANCE

Trade Agreements Act (TAA) Compliant

Table of Contents

Introduction 5
Box contents 5
diskAshur³ Layout 5
1. LED indicators and their actions 6
2. LED States 6
3. First Time Use 7
4. Unlocking diskAshur³ with the Admin PIN 8
5. How to enter Admin Mode 8
6. Changing the Admin PIN 9
7. Setting a User PIN Policy 10
8. How to delete the User PIN Policy 11
9. How to check the User PIN Policy 11
10. Adding a New User PIN in Admin Mode 12
11. Changing the User PIN in Admin Mode 13
12. Deleting the User PIN in Admin Mode 13
13. How to unlock diskAshur³ with User PIN 14
14. Changing the User PIN in User Mode 14
15. Switching on the backlit LED keypad 15
16. Switching off the backlit LED keypad 15
17. Creating a One-Time User Recovery PIN 16
18. Deleting the One-Time User Recovery PIN 16
19. Activating Recovery Mode and Creating New User PIN 17
20. Set User Read-Only in Admin Mode 17
21. Enable User Read/Write in Admin Mode 18
22. Set Global Read-Only in Admin Mode 18
23. Enable Global Read/Write in Admin Mode 19
24. How to configure a Self-Destruct PIN 19
25. How to delete the Self-Destruct PIN 20
26. How to Unlock with the Self-Destruct PIN 20
27. How to configure an Admin PIN after a Brute Force attack or Reset 21
28. Setting the unattended Auto-Lock 21
29. Turn off the unattended Auto-Lock 22
30. How to check the unattended Auto-Lock 23
31. Set Read-Only in User Mode 23
32. Enable Read/Write in User Mode 24
33. Brute Force Hack Defence Mechanism 24
34. How to set the User PIN Brute Force Limitation 25
35. How to check the User PIN Brute Force Limitation 26
36. How to perform a complete reset 27
37. How to configure diskAshur³ as Bootable 27
38. How to disable the diskAshur³ Bootable feature 28
39. How to check the Bootable setting 28
40. How to configure the Encryption Mode 29
41. How to check the Encryption Mode 30
42. How to configure the Disk type 31
43. How to check the Disk type setting 31
44. Initialising and formatting diskAshur³ for Windows 32
45. Initialising and formatting diskAshur³ in Mac OS 34
46. Initialising and formatting diskAshur³ in Linux OS 36
47. Hibernating, Suspending or Logging off from the Operating System 39
48. How to check Firmware in Admin Mode 39
49. How to check Firmware in User Mode 40
50. Technical Support 41
51. Warranty and RMA information 41

Introduction

Thank you for purchasing the new iStorage diskAshur³/ diskAshur PRO³ drive, hereinafter referred to as diskAshur³.

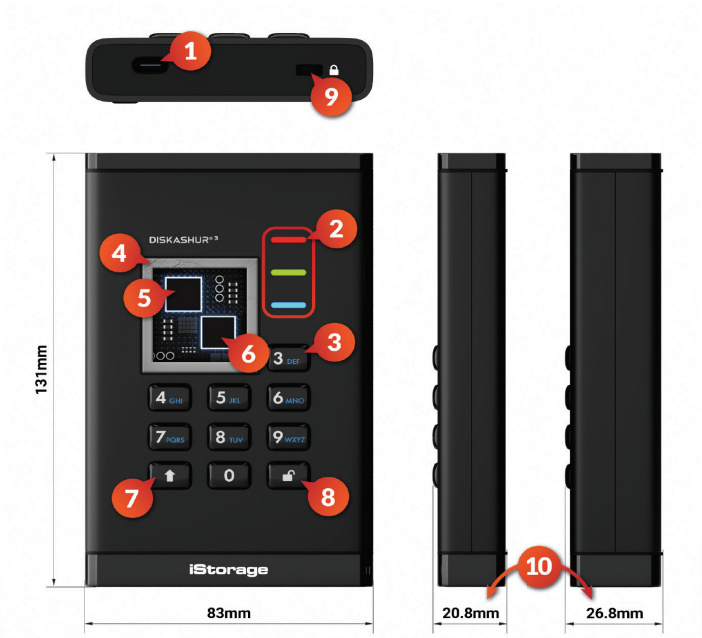
The diskAshur³ is an easy to use, ultra-secure, password protected, hardware encrypted portable HDD/SSD drive with capacities of up to 5TB (HDD) and up to 16TB (SSD) and rising. The diskAshur³ encrypts data in transit and at rest using 256-bit full disk hardware encryption.

The diskAshur³ incorporates a Common Criteria EAL 5+ Certified secure microprocessor, which employs built-in physical protection mechanisms designed to defend against external tamper, bypass attacks and fault injections. Unlike other solutions, the diskAshur³ reacts to an automated attack by entering the deadlock frozen state, which renders all such attacks as useless. In plain and simple terms, without the PIN there's no way in!

Box Contents

- iStorage diskAshur³
- Protective carry case
- USB C & A Cables
- Free 1 year license of Nero BackItUp and iStorage DriveSecurity
- QSG - Quick Start Guide

diskAshur³ Layout



1. USB 3.2 (Gen 1) Type-C Interface
   USB Type C & A cables included
2. LED lights
   RED - Locked/Standby mode. SOLID GREEN - Unlocked. FLASHING GREEN - Data transfer.
   BLUE - Admin mode.
3. Epoxy coated, wear resistant, backlit (user selectable), alphanumeric keypad.
4. Tamper proof and tamper evident design
   All critical components are covered by a layer of super tough epoxy resin.
5. On-device crypto chip
6. On-device Common Criteria EAL-5+ Certified Secure Microprocessor
7. SHIFT button.
8. UNLOCK button.
9. Desk Lock Slot.
10. The depth of the 4TB & 5TB HDD drive is 26.8mm instead of 20.8mm.

1. LED indicators and their actions

LED	LED State	Description	LED	LED State	Description
	RED Solid	Locked drive (in either **Standby** or **Reset** states)		BLUE Solid	Drive in **Admin mode**
	RED Double blink	Incorrect PIN entry		RED, GREEN and BLUE Blinking together	Waiting for **User** PIN entry
	GREEN Solid	Drive **unlocked**		GREEN and BLUE Blinking together	Waiting for **Admin** PIN entry
	GREEN Blinking	Data transfer in progress			

2. LED States

To wake from Idle State

Idle state is defined as when the drive is not being used and all LEDs are off.

To wake diskAshur³ from the idle state do the following.

Connect the drive to a powered USB port on your computer		A solid RED LED switches on indicating the drive is in Standby State

To enter Idle State

To force diskAshur³ to enter Idle State, execute either of the following operations:

- Safely eject and disconnect drive from your computer, RED LED will switch off (idle state).

Power-on States

After the drive wakes from the Idle State, it will enter one of the following states shown in the table below.

Power-on State	LED indication	Encryption Key	Admin PIN	Description
Initial Shipment State	RED and GREEN Solid	✓	×	Waiting for configuration of an Admin PIN (First Time Use)
Standby	RED Solid	✓	✓	Waiting for Admin, User or Recovery PIN entry
Reset	RED Solid	×	×	Waiting for configuration of an Admin PIN

3. First Time Use

The iStorage diskAshur³ is supplied in the **'Initial Shipment State' with no pre-set Admin PIN**. A **8-64** digit Admin PIN must be configured before the drive can be used. Once an Admin PIN has been successfully configured, it will then not be possible to switch the drive back to the 'Initial Shipment State'.

PIN Requirements:

- Must be between 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- The SHIFT key can be used for additional combinations e.g. (**SHIFT (🔓) +1** is a separate value to just 1).

Password Tip: You can configure a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the button with the corresponding letters on it.

Examples of these types of Alphanumerical PINs are:

- For "**Password**" press the following buttons:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- For "**iStorage**" press the following buttons:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Using this method, long and easy to remember PINs can be configured.

To configure an Admin PIN and unlock the diskAshur³ for the first time, please follow the simple steps in the table below.

Instructions - First Time Use	LED	LED State
1. Connect the diskAshur³ to a powered USB port on your computer		Solid RED and GREEN LEDs switch on indicating the drive is in the Initial Shipment State
2. Press and hold down both **Unlock (🔓) + 1** buttons		LEDs turn to blinking GREEN and solid BLUE
3. Enter a **New Admin PIN** (8-64 digits) and press the **Unlock (🔓)** button once		Blinking GREEN and solid BLUE LEDs switch to a GREEN blink then back to Blinking GREEN and solid BLUE LEDs
4. Re-enter your **New Admin PIN** and press the **Unlock (🔓)** button once		BLUE LED rapidly blinks then switches to a solid BLUE LED and finally to a solid GREEN LED indicating the Admin PIN has been successfully configured and the drive is unlocked and ready to be used

Locking the diskAshur³
To lock the drive, safely eject from your host operating system and then unplug from the USB port. If data is being written to the drive, ejecting the diskAshur³ will result in incomplete data transfer and possible data corruption.

4. Unlocking diskAshur³ with the Admin PIN

To unlock the diskAshur³ with the Admin PIN, please follow the simple steps in the table below.

1. Connect the diskAshur³ to a USB port on your computer		A solid RED LED switches on indicating the drive is in Standby State
2. In Standby State (solid RED LED) press the **Unlock (🔓)** button once		GREEN and BLUE LEDs blink together
3. With the GREEN and BLUE LEDs blinking together, enter the **Admin PIN** and then press the **Unlock (🔓)** button once		The GREEN LED blinks several times and then switches to a solid GREEN LED indicating the drive has been successfully unlocked as Admin and is ready to be used

5. How to enter Admin Mode

To Enter Admin Mode, do the following.

1. Connect the diskAshur³ to a powered USB port on your computer		A solid RED LED switches on indicating the drive is in Standby State
2. In Standby State (solid RED LED) Press and hold down both **Unlock (🔓) + 1** buttons		GREEN and BLUE LEDs blink together
3. Enter your **Admin PIN** and press the **Unlock (🔓)** button once		A solid BLUE LED switches on indicating the drive is in Admin mode

To Exit Admin Mode

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

6. Changing the Admin PIN

PIN Requirements:

- Must be between 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- The SHIFT key can be used for additional combinations e.g. (**SHIFT** (⬆)**+1** is a separate value to just 1).

Password Tip: You can configure a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the button with the corresponding letters on it.

Examples of these types of Alphanumerical PINs are:

- For "**Password**" press the following buttons:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- For "**iStorage**" press the following buttons:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Using this method, long and easy to remember PINs can be configured.

To change the Admin PIN, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both the **Unlock (🔓) + 2** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **NEW Admin PIN** and then press the **Unlock (🔓)** button once		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the **NEW Admin PIN** and then press the **Unlock (🔓)** button once		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking BLUE LED and finally to a solid BLUE LED indicating the Admin PIN has been successfully changed

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

7. Setting a User PIN Policy

The Administrator can set a restriction policy for the User PIN. This policy includes setting the minimum length of the PIN (from 8 to 64 digits), as well as requiring or not the input of one or more '**Special Characters**'. The "Special Character" functions as both the '**SHIFT** (⬆) + **digit**' buttons pressed down together.

To set a User PIN Policy (restrictions), you will need to enter 3 digits, for instance '**091**', the first two digits (**09**) indicate the minimum PIN length (in this case, **9**) and the last digit (**1**) denotes that one or more 'Special Characters' must be used, in other words '**SHIFT** (⬆) + **digit**'. In the same way, a User PIN Policy can be set without the need of a 'Special Character', for instance '**120**', the first two digits (**12**) indicate the minimum PIN length (in this case,**12**) and the last digit (**0**) meaning no Special Character is required.

Once the Administrator has set the User PIN Policy, for instance '**091**', a new User PIN will need to be configured - see section 10, 'Adding a New User PIN in Admin Mode'. If the Administrator configures the User PIN as '**247688314**' with the use of a '**Special Character**' (**SHIFT** (⬆) **+ digit** pressed down together), this can be placed anywhere along your 8-64 digit PIN during the process of creating the User PIN as shown in the examples below.

A. '**SHIFT** (⬆) **+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',

B. '2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4',

C. '2', '4', '7', '6', '8', '8', '3', '1', '**SHIFT** (⬆) **+ 4**',

Note:

- If a 'Special Character' was used during the configuration of the User PIN, for instance, example '**B**' above, then the drive can only be unlocked by entering the PIN with the 'Special Character' entered precisely in the order configured, as per example '**B**' above - ('2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- More than one 'Special Character' can be used and placed along your 8-64 digit PIN.
- Users are able to change their PIN but are forced to comply with the set 'User PIN Policy' (restrictions), if and when applicable.
- Setting a new User PIN Policy will automatically delete the User PIN if one exists.
- This policy does not apply to the 'Self-Destruct PIN'. The complexity setting for the Self-Destruct PIN and Admin PIN is always 8-64 digits, with no special character required.

To set a **User PIN Policy**, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **Unlock (🔓) + 7** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter your **3 digits**, remember the first two digits denote minimum PIN length and last digit (0 or 1) whether or not a special character has been used.		Blinking GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will change to a solid GREEN LED and finally to a solid BLUE LED indicating the User PIN Policy has been successfully set.

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

8. How to delete the User PIN Policy

To delete the **User PIN Policy**, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **Unlock (🔓) + 7** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **080** and press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will change to a solid GREEN LED and finally to a solid BLUE LED indicating the User PIN Policy has been successfully deleted

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

9. How to check the User PIN Policy

The Administrator is able to check the User PIN Policy and can identify the minimum PIN length restriction and whether or not the use of a Special Character has been set by noting the LED sequence as described below.

To check the User PIN Policy, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **SHIFT** (⬆) **+ 7** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **Unlock (🔓)** button and the following happens; a. All LED's (RED, GREEN & BLUE) become solid for 1 second. b. A RED LED blink equates to ten (10) units of a PIN. c. Every GREEN LED blink equates to a single (1) unit of a PIN d. A BLUE blink indicates that a 'Special Character' was used. e. All LED's (RED, GREEN & BLUE) become solid for 1 second. f. LEDs return to solid BLUE		

The table below describes the LED behaviour whilst checking the User PIN Policy, for instance if you have set a 12 digit User PIN with the use of a Special Character (**121**), the RED LED will blink once (**1**) and the GREEN LED will blink twice (**2**) followed by a single (**1**) BLUE LED blink indicating that a **Special Character** must be used.

PIN Description	3 digit Setup	RED	GREEN	BLUE
12 digit PIN with use of a Special Character	121	1 Blink	2 Blinks	1 Blink
12 digit PIN with NO Special Character used	120	1 Blink	2 Blinks	0
9 digit PIN with use of a Special Character	091	0	9 Blinks	1 Blink
9 digit PIN with NO Special Character used	090	0	9 Blinks	0

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

10. Adding a New User PIN in Admin Mode

Important: The creation of a New User PIN must comply with the 'User PIN Policy' if one has been configured as described in section 7, which imposes a minimum PIN length and whether a 'Special Character' has been used. The Administrator can Refer to section 9 to check the user PIN restrictions.

PIN requirements:

- Must be between 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- The **SHIFT** (⬆) button can be used for additional PIN combinations - e.g. (**SHIFT** (⬆) **+ 1** is a different value than just 1). See section 7, 'Setting a User PIN Policy'.

To add a **New User PIN**, first enter "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **Unlock (🔓) + 3** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New User PIN** and press **Unlock (🔓)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the **New User PIN** and press **Unlock (🔓)** button again		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking GREEN LED and finally to a solid BLUE LED indicating a New User PIN has been successfully configured

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

11. Changing the User PIN in Admin Mode

Important: Changing the User PIN must comply with the 'User PIN Policy' if one has been configured as described in section 7, which imposes a minimum PIN length and whether a 'Special Character' has been used. The Administrator can refer to section 9 to check the user PIN restrictions.

To change an existing **User PIN**, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **Unlock (🔓) + 3** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New User PIN** and press **Unlock (🔓)** button once		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the **New User PIN** and press **Unlock (🔓)** button once		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking GREEN LED and finally to a solid BLUE LED indicating the User PIN has been successfully changed

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

12. Deleting the User PIN in Admin Mode

To delete an existing **User PIN**, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **SHIFT** (⬆) **+ 3** buttons		Solid BLUE LED will change to a blinking RED LED
2. Press and hold down both **SHIFT** (⬆) **+ 3** buttons again		Blinking RED LED will change to a solid RED LED and then to a solid BLUE LED indicating the User PIN has been successfully deleted

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

13. How to unlock diskAshur³ with User PIN

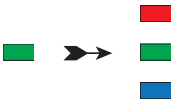
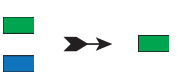
To unlock the diskAshur³ with the **User PIN,** proceed with the following steps.

1. In a standby state (solid RED LED) Press and hold down both the **SHIFT** (⬆) **+ Unlock (🔓)** buttons		RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter **User PIN** and press the **Unlock (🔓)** button once		RED, GREEN and BLUE blinking LEDs will change to a blinking GREEN LED then to a solid GREEN LED indicating drive successfully unlocked in User Mode

14. Changing the User PIN in User Mode

Important: Changing the User PIN in User mode (GREEN LED) must comply with the 'User PIN Policy' if one has been configured as described in section 7, which imposes a minimum PIN length and whether a 'Special Character' has been used.

To change the **User PIN**, first unlock the diskAshur³ with the User PIN as described in section 13. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

1. In User mode (GREEN LED) press and hold down both **Unlock (🔓) + 4** buttons		Solid GREEN LED will change to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter your **Existing User PIN** and press the **Unlock (🔓)** button once		LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Enter **New User PIN** and press the **Unlock (🔓)** button once		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
4. Re-enter **New User PIN** and press the **Unlock (🔓)** button once		Blinking GREEN and solid BLUE LEDs will switch to a rapidly blinking GREEN LED and then to a solid GREEN LED indicating the User PIN has been successfully changed

15. Switching on the backlit LED keypad

To aid with low-light visibility, the diskAshur³ is equipped with an LED backlit keypad. To switch on the LED backlit keypad, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **2 & 6** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **Unlock (🔓)** button		Blinking GREEN and BLUE LEDs will switch to a solid GREEN LED and then to a solid BLUE LED indicating the backlit keypad has been activated and will switch on the next time the drive is plugged in to a powered USB port.

Note: After setting the diskAshur³ to switch ON the LED backlit keypad, the drive must be first unplugged from the powered USB port and then plugged back in again to activate. To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

16. Switching off the backlit LED keypad

To switch off the LED backlit keypad, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **2 & 3** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **Unlock (🔓)** button		Blinking GREEN and BLUE LEDs will switch to a solid GREEN LED and then to a solid BLUE LED indicating the backlit keypad has been deactivated and will switch off the next time the drive is plugged in to a powered USB port.

Note: After setting the diskAshur³ to switch OFF the LED backlit keypad, the drive must be first unplugged from the powered USB port and then plugged back in again to activate. To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

17. Creating a One-Time User Recovery PIN

The User Recovery PIN is extremely useful in situations where a user has forgotten their PIN to unlock the diskAshur³.
To activate the recovery mode, the user must first enter the correct One-Time Recovery PIN, if one has been configured. The user PIN recovery process does not impact the data, encryption key and Admin PIN, however the user is forced to configure a new 8-64 digit User PIN.

To configure a One-Time 8-64 digit User Recovery PIN, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **Unlock (🔓) + 4** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter a **One-Time Recovery PIN** and press **Unlock (🔓)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter your **One-Time Recovery PIN** and press **Unlock (🔓)** button again		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking GREEN LED and finally to a solid BLUE LED indicating the One-Time Recovery PIN has been successfully configured

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

18. Deleting the One-Time User Recovery PIN

To delete the One-Time User Recovery PIN, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **SHIFT** (⬆) **+ 4** buttons		Solid BLUE LED will change to blinking RED LED
2. Press and hold down both **SHIFT** (⬆) **+ 4** buttons again		Blinking RED LED will become solid RED and then switch to a solid BLUE LED indicating that the One-Time User Recovery PIN has been successfully deleted

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

19. Activating Recovery Mode and Creating New User PIN

The User Recovery PIN is extremely useful in situations where a user has forgotten their PIN to unlock the diskAshur³.
To activate the recovery mode, the user must first enter the correct One-Time Recovery PIN, if one has been configured. The user PIN recovery process does not impact the data, encryption key and Admin PIN, however the user is forced to configure a new 8-64 digit User PIN.

To activate the Recovery process and configure a new User PIN, proceed with the following steps.

1. In **Standby State** (RED LED) press and hold down both **Unlock (🔓) + 4** buttons		Solid RED LED will change to blinking RED and GREEN LEDs
2. Enter the One-Time **Recovery PIN** and press the **Unlock (🔓)** button		GREEN and BLUE LEDs alternate on and off then to a solid GREEN LED and finally to blinking GREEN and solid BLUE LEDs
3. Enter a **New User PIN** and press the **Unlock (🔓)** button		Blinking GREEN and solid BLUE LEDs change to a single GREEN LED blink then back to blinking GREEN and solid BLUE LEDs
4. Re-enter your **New User PIN** and press the **Unlock (🔓)** button again		GREEN LED blinks rapidly then becomes solid GREEN indicating the recovery process has been successful and a new user PIN configured

Important: The creation of a new User PIN must comply with the 'User PIN Policy' if one has been configured as described in section 7, which imposes a minimum PIN length and whether a special character has been used. Refer to section 9 to check the user PIN restrictions.

20. Set User Read-Only in Admin Mode

With so many viruses and Trojans infecting USB drives, the Read-Only feature is especially useful if you need to access data on the USB drive when used in a public setting. This is also an essential feature for forensic purposes, where data must be preserved in its original and unaltered state that cannot be modified or overwritten.

When the Administrator configures the diskAshur³ and restricts User access to Read-Only, then only the Administrator can write to the drive or change the setting back to Read/Write as described in section 21. The User is restricted to Read-Only access and cannot write to the drive or change this setting in user mode.

To set the diskAshur³ and restrict User access to Read-Only, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both "**7 + 6**" buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **Unlock (🔓)** button once		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating the drive has been configured and restricts User access to Read-Only

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

21. Enable User Read/Write in Admin Mode

To set the diskAshur³ back to Read/Write, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

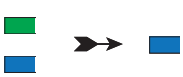
1. In Admin mode, press and hold down both "**7 + 9**" buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **Unlock (🔓)** button once		GREEN and BLUE LEDs change to a solid GREEN LED then to a solid BLUE LED indicating the drive is configured as Read/Write

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

22. Set Global Read-Only in Admin Mode

When the Administrator configures the diskAshur³ and restricts it to Global Read-Only, then neither the Administrator nor the User can write to the drive and both are restricted to Read-Only access. Only the Administrator is able to change the setting back to Read/Write as described in section 23.

To set the diskAshur³ and restrict Global access to Read-Only, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both "**5 + 6**" buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **Unlock (🔓)** button		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating the drive has been configured and restricts Global access to Read-Only

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

23. Enable Global Read/Write in Admin Mode

To set the diskAshur³ back to Read/Write from the Global Read-Only setting, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both "**5 + 9**" buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **Unlock (🔓)** button		GREEN and BLUE LEDs change to a solid GREEN LED then to a solid BLUE LED indicating the drive is configured as Read/Write

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

24. How to configure a Self-Destruct PIN

You can configure a self-destruct PIN which when entered performs a Crypto-Erase on the drive (encryption key is deleted).This process deletes all configured PINs and renders all data stored on the drive as inaccessible (lost forever), the drive will then show as unlocked GREEN LED. Running this feature will cause the self-destruct PIN to become the New User PIN and the drive will need to be formatted before it can be reused.

To set the Self-Destruct PIN, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **Unlock (🔓) + 6** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Configure and enter a 8-64 digit **Self-Destruct PIN** and press the **Unlock (🔓)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter your **Self-Destruct PIN** and press the **Unlock (🔓)** button		GREEN LED will rapidly blink and then change to a solid BLUE LED to indicate the Self-Destruct PIN has been successfully configured

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

25. How to Delete the Self-Destruct PIN

To delete the Self-Destruct PIN, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **SHIFT (⬆) + 6** buttons		Solid BLUE LED will change to a blinking RED LED
2. Press and hold down **SHIFT (⬆) + 6** buttons again		Blinking RED LED will become solid and then change to a solid BLUE LED indicating the Self-Destruct PIN was successfully deleted

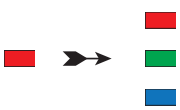
Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

26. How to unlock with the Self-Destruct PIN

Warning: When the Self-Destruct mechanism is activated, all data, the encryption key and the Admin/User PINs are deleted. **The Self-Destruct PIN becomes the User PIN.** No Admin PIN exists after the Self-Destruct mechanism is activated. The diskAshur³ will need to be reset (see 'How to perform a complete reset' Section 36, on page 27) first in order to configure an Admin PIN with full Admin privileges including the ability to configure a new User PIN.

When used, the self-destruct PIN will **delete ALL data, the encryption key, Admin/User PINs** and then unlock the drive. Activating this feature will cause the **Self-Destruct PIN to become the New User PIN** and the diskAshur³ will need to be formatted before any new data can be added to the drive.

To activate the Self-Destruct mechanism, the drive needs to be in the standby state (solid RED LED) and then proceed with the following steps.

1. In **Standby State** (solid RED LED), press and hold down both the **SHIFT** (⬆) + **Unlock (🔓)** buttons		RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter the **Self-Destruct PIN** and press the **Unlock (🔓)** button		RED, GREEN and BLUE blinking LEDs will change to a blinking GREEN LED and then to a solid GREEN LED indicating the diskAshur³ has successfully self-destructed

27. How to configure an Admin PIN after a Brute Force attack or Reset

It will be necessary after a Brute Force attack or when the diskAshur³ has been reset to configure an Admin PIN before the drive can be used.

PIN Requirements:

- Must be between 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- The SHIFT key can be used for additional combinations e.g. (**SHIFT** (⬆)**+1** is a separate value to just 1).

If the diskAshur³ has been brute forced or reset, the drive will be in standby state (solid RED LED). to configure an Admin PIN proceed with the following steps.

1. In Standby state (solid RED LED), press and hold down both **SHIFT** (⬆) **+ 1** buttons		Solid RED LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New Admin PIN** and press **Unlock (🔓)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the **New Admin PIN** and press **Unlock (🔓)** button		Blinking GREEN LED and solid BLUE LED change to a blinking BLUE LED and then to a solid BLUE LED indicating the Admin PIN was successfully configured.

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

28. Setting the unattended Auto-Lock

To protect against unauthorised access if the drive is unlocked and unattended, the diskAshur³ can be set to automatically lock after a pre-set amount of time. In its default state, the diskAshur³ unattended Auto Lock time-out feature is turned off. The unattended Auto Lock can be set to activate between 5 - 99 minutes if and when the drive is inactive (no data being written/read).

To set the unattended Auto Lock time-out feature, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **Unlock (🔓) + 5** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter the amount of time that you would like to set the Auto Lock time-out feature for, the minimum time that can be set is 5 minutes and the maximum being 99 minutes (5-99 minutes). For example enter: **05 for 5 minutes (press '0' followed by a '5')** **20 for 20 minutes (press '2' followed by a '0')** **99 for 99 minutes (press '9' followed by another '9')**		
3. Press the **SHIFT** (⬆) button		Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto Lock time-out is successfully configured

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

29. Turn off the unattended Auto-Lock

To turn off the unattended Auto Lock time-out feature, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **Unlock (🔓) + 5** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **00** and press the **SHIFT** (⬆) button		Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto Lock time-out has been successfully disabled

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

30. How to check the unattended Auto-Lock

The Administrator is able to check and determine the length of time set for the unattended Auto Lock time-out feature by simply noting the LED sequence as described in the table below.

To check the unattended auto-lock, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down **SHIFT** (⬆) + **5**		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **Unlock (🔓)** button and the following happens; a. All LED's (RED, GREEN & BLUE) become solid for 1 second. b. Each RED LED blink equates to ten (10) minutes. c. Every GREEN LED blink equates to one (1) minute. d. All LED's (RED, GREEN & BLUE) become solid for 1 second. e. LEDs return to solid BLUE		

The table below describes the LED behaviour whilst checking the unattended auto-lock, for instance if you have set the drive to automatically lock after **25** minutes, the RED LED will blink twice (**2**) and the GREEN LED will blink five (**5**) times.

Auto-Lock in minutes	**RED**	**GREEN**
5 minutes	0	5 Blinks
15 minutes	1 Blink	5 Blinks
25 minutes	2 Blinks	5 Blinks
40 minutes	4 Blinks	0

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

31. Set Read-Only in User Mode

To set the diskAshur³ to Read-Only, first enter the "**User Mode**" as described in section 13. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

1. In User mode, press and hold down both "**7 + 6**" buttons. (7=**R**ead + 6=**O**nly)		Solid GREEN LED will change to blinking GREEN and BLUE LEDs
2. Press **Unlock (🔓)** button		GREEN and BLUE LEDs will change to a solid GREEN LED indicating the drive is configured as Read-Only

Note: 1. If a User set the drive as Read-Only, Admin can override this by setting the drive as Read/Write in Admin mode.

2. If Admin set the drive as Read-Only, the User cannot set the drive as Read/Write.

32. Enable Read/Write in User Mode

To set the diskAshur³ to Read/Write, first enter the "**User Mode**" as described in section 13. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

1. In User mode, press and hold down "**7 + 9**" buttons. (7=**R**ead + 9=**W**rite)		Solid GREEN LED will change to blinking GREEN and BLUE LEDs
2. Press **Unlock (🔓)** button		GREEN and BLUE LEDs will change to a solid GREEN LED indicating the drive is configured as Read/Write

Note: 1. If a User set the drive as Read-Only, Admin can override this by setting the drive as Read/Write in Admin mode.

2. If Admin set the drive as Read-Only, the User cannot set the drive as Read/Write.

33. Brute Force Hack Defence Mechanism

The diskAshur³ incorporates a defence mechanism to protect the drive against a Brute Force attack. By default, the brute force limitation for **Admin PIN** and **User PIN** is set to **10** consecutive incorrect PIN entries, for the **Recovery PIN** it is **5**. Three independent brute force counters are used to record the incorrect attempts for each PIN authorisation. If a user enters an incorrect Admin PIN ten consecutive times, (broken down into 5,3,2, clusters as described below) the drive will be reset and all data will be lost forever. If a user enters an incorrect Recovery PIN or User PIN and exceed the respective brute force limitation, the corresponding PINs will be cleared but the data will still exist on the drive.

Note: The brute force limitation is programmed to initial values when the drive is completely reset or self-destruct feature is activated. If Admin changes the User PIN, or a new User PIN is set when activating recovery feature, the User PIN brute force counter is cleared but the brute force limitation is not affected. If Admin changes the Recovery PIN, the Recovery PIN brute force counter is cleared.

Successful authorisation of a certain PIN will clear the brute force counter for that particular PIN, but not affect the other PINs brute force counter. Failed authorisation of a certain PIN will increase the brute force counter for that particular PIN, but not affect the other PINs brute force counter.

- If a user enters an **incorrect User PIN** 10 consecutive times, the User PIN will be deleted but the data, Admin PIN and Recovery PIN remain intact and accessible.
- If an **incorrect Recovery PIN** is entered 5 consecutive times, the Recovery PIN is deleted but the data and Admin PIN remain intact and accessible.
- The **Admin PIN** uses a more sophisticated defence mechanism in comparison to the User and Recovery PINs. After **5 consecutive incorrect Admin PIN entries**, the drive will lock and the **RED**, **GREEN** and **BLUE** LEDs will light up solid. At this point the following steps need to be taken in order to allow the User a further **3** PIN entries.

- Enter PIN "**47867243**" and press the **Unlock (🔓)** button, **GREEN** and **BLUE** LEDs blink together. The drive is now ready to accept a further **3** Admin PIN entries
- After a total of 8 consecutive incorrect Admin PIN entries, the drive will lock and the **RED**, **GREEN** and **BLUE** LEDs will blink alternately. At this point the following steps need to be taken in order to get the final **2** PIN entries (10 in total).
- Enter PIN "**47867243**" and press the **Unlock (🔓)** button, **GREEN** and **BLUE** LEDs blink together, the drive is now ready to accept the final **2** PIN entries (10 in total).
- After a total of 10 incorrect Admin PIN attempts, the encryption key will be deleted and all data and PINs stored on the drive will be lost forever.

The table below assumes that all three PINs have been set up and highlights the effect of triggering the brute force defence mechanism for each individual PIN.

PIN used to unlock drive	Consecutive incorrect PIN entries	Description of what happens
User PIN	10	• The User PIN is deleted. • The Recovery PIN, the Admin PIN and all data remain intact and accessible.
Recovery PIN	5	• The Recovery PIN is deleted. • The Admin PIN and all data remain intact and accessible.
Admin PIN	5 3 2 (10 in total)	• After **5** consecutive incorrect Admin PIN entries, the drive will lock and all LEDs light up solid. • Enter PIN "**47867243**" and press the **Unlock (🔓)** button to get **3** further PIN entries. • After a total of **8** (5+3) consecutive incorrect Admin PIN entries, the drive will lock and the LEDs blink alternately. • Enter PIN "**47867243**" and press the **Unlock (🔓)** button to get the final **2** PIN entries (10 in total). • After a total of 10 consecutive incorrect Admin PIN entries, the encryption key will be deleted and all data and PINs stored on the drive will be lost forever.

Important: A new Admin PIN must be configured if the pre-existing Admin PIN was brute forced, refer to Section 27 on page 21 on 'How to Configure an Admin PIN after a Brute Force attack or Reset', the diskAshur³ will also need to be formatted before any new data can be added to the drive.

34. How to set the User PIN Brute Force Limitation

Note: The User PIN brute force limitation setting is defaulted to 10 consecutive incorrect PIN entries when the drive is either completely reset, brute forced or the self-destruct PIN is activated.

The brute force limitation for diskAshur³ User PIN can be reprogrammed and set by the administrator. This feature can be set to allow attempts from 1 to 10 consecutive incorrect PIN entries.

To configure the User PIN brute force limitation, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

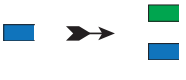
1. In Admin mode, press and hold down both **7 + 0** buttons		Solid BLUE LED will change to GREEN and BLUE LEDs blinking together
2. Enter the number of attempts for the brute force limitation (between 01-10), for example enter: • **01** for 1 attempt • **10** for 10 attempts		
3. Press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will switch to a solid GREEN LED for a second and then to a solid BLUE LED indicating the brute force limitation was successfully configured

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

35. How to check the User PIN Brute Force Limitation

The Administrator is able to observe and determine the number of consecutive times an incorrect User PIN is allowed to be entered before triggering the Brute Force defence mechanism by simply noting the LED sequence as described below.

To check the brute force limitation setting, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **2** + **0** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **Unlock (🔓)** button and the following happens; a. All LED's (RED, GREEN & BLUE) become solid for 1 second. b. Each RED LED blink equates to ten (10) units of a brute force limitation number. c. Every GREEN LED blink equates to one (1) single unit of a brute force limitation number. d. All LED's (RED, GREEN & BLUE) become solid for 1 second. e. LEDs return to solid BLUE		

The table below describes the LED behaviour whilst checking the brute force limitation setting, for instance if you have set the drive to brute force after **5** consecutive incorrect PIN entries, the GREEN LED will blink five (**5**) times.

Brute Force Limitation Setting	RED	GREEN
2 attempts	0	2 Blinks
5 attempts	0	5 Blinks
10 attempts	1 Blink	0

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

36. How to perform a complete reset

To perform a complete reset, the diskAshur³ must be in standby state (solid RED LED). Once the drive is reset then all Admin/User PINs, the encryption key and all data will be deleted and lost forever and the drive will need to be formatted before it can be reused. To reset the diskAshur³ proceed with the following steps.

1. In standby state (solid RED LED) , press and hold down "**0**" button		Solid RED LED will change to all LEDs, RED, GREEN and BLUE blinking alternately on and off
2. Press and hold down both **2 + 7** buttons		RED, GREEN and BLUE alternating LEDs will become solid for a second and then to a solid RED LED indicating the drive has been reset

Important: After a complete reset a new Admin PIN must be configured, refer to Section 27 on page 21 on 'How to Configure an Admin PIN after a Brute Force attack or Reset', the diskAshur³ will also need to be formatted before any new data can be added to the drive.

37. How to configure diskAshur³ as Bootable

Note: When the drive is set as bootable, ejecting the drive from Operating System will not force the LED to turn RED. The drive stays solid GREEN and needs to be unplugged for next time use. The default setting of the diskAshur³ is configured as non-bootable.

The diskAshur³ is equipped with a bootable feature to accommodate power cycling during a host boot process. When booting from the diskAshur³, you are running your computer with the operating system that is installed on the diskAshur³.

To set the drive as bootable, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **Unlock (🔓) + 9** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **"0"** followed by a **"1"** (**01**)		GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will change to a solid GREEN LED and finally to a solid BLUE LED indicating the drive has been successfully configured as bootable

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

38. How to disable the diskAshur³ Bootable feature

To disable the diskAshur³ Bootable Feature, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **Unlock (🔓) + 9** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **"0"** followed by another **"0"** (**00**)		GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will change to a solid GREEN LED and finally to a solid BLUE LED indicating the bootable feature has been successfully disabled

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

39. How to check the Bootable setting

To check the bootable setting, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **SHIFT** (⬆) **+ 9** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs

2. Press the **Unlock (🔓)** button and one of the following two scenarios will happen;

- **If diskAshur³ is configured as Bootable, the following happens;**

a. All LED's (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks once.
c. All LED's (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

- **If diskAshur³ is <u>NOT</u> configured as Bootable, the following happens;**

a. All LED's (RED, GREEN & BLUE) become solid for 1 second.
b. All LEDs are off
c. All LED's (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

40. How to configure the Encryption Mode

WARNING: Changing the encryption mode from AES-XTS (default state) to AES-ECB or AES-CBC will delete the encryption key and cause the diskAshur³ to reset and render all data as inaccessible and lost forever!

Perform the following steps to configure the diskAshur³ encryption mode to either **AES-ECB** indicated by the number **'01'**, or **AES-XTS** indicated by the number **'02',**or **AES-CBC** indicated by the number **'03'**. This feature is set as AES-XTS (02) by default. Please note all critical parameters will be deleted when switching to a different encryption mode and will cause the drive to reset.

To set the diskAshur³ encryption mode, first enter the A**dmin Mode** as described in section 5. Once the diskAshur³ is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin Mode, press and hold down both '**Unlock (🔓) + 1**' buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **01** to set as **AES-ECB** Enter **02** to set as **AES-XTS (default state)** Enter **03** to set as **AES-CBC**		GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once.		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid RED LED (**Reset State**) indicating the encryption mode was successfully changed

Important: After configuring the encryption mode, the diskAshur³ completely resets and a new Admin PIN must be configured, refer to Section 27 on page 21 on 'How to Configure an Admin PIN after a Brute Force attack or Reset'.

41. How to check the encryption mode

To check the diskAshur³ encryption mode, first enter the **Admin Mode** as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin Mode press and hold down both **'SHIFT** (⬆) + **1'** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs

2. Press the **Unlock (🔓)** button and the following happens:

- **If the encryption mode is configured as AES-ECB, the following happens:**

a. All LED's (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks once.
c. All LED's (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

- **If the encryption mode is configured as AES-XTS, the following happens:**

a. All LED's (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks twice.
c. All LED's (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

- **If the encryption mode is configured as AES-CBC, the following happens:**

a. All LED's (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks three times.
c. All LED's (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

42. How to configure the Disk type

The diskAshur³ can be configured as either a 'Removable Disk' or 'Local Disk (default state)'. All critical parameters will be erased when switching to a different disk type, deleting all PINs, the encryption key and data and causing the drive to enter the reset state.

WARNING: Changing the disk type as either a 'Removable Disk' or 'Local Disk (default state)' will delete the encryption key and cause the diskAshur³ to reset and render all data as inaccessible and lost forever!

Perform the following steps to configure the diskAshur³ disk type to either a Removable Disk (**00**) or Local Disk (**01**)This feature is set as Local Disk (**01**) by default. Please note all critical parameters will be erased when switching to a different disk type causing the drive to reset.

To set the diskAshur³ disk type, first enter the **Admin Mode** as described in section 5. Once the diskAshur³ is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin Mode, press and hold down both '**Unlock (🔓) + 8**' buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **00** to set as **Removable Disk** Enter **01** to set as **Local Disk (default state)**		GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once.		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid RED LED (**Reset State**) indicating the disk type was successfully changed

Important: After changing the disk type, the diskAshur³ completely resets and a new Admin PIN must be configured, refer to Section 27 on page 21 on 'How to Configure an Admin PIN after a Brute Force attack or Reset'.

43. How to check the Disk type setting

To check the diskAshur³ disk type setting, first enter the **Admin Mode** as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin Mode press and hold down both '**SHIFT** (⬆) + **8**' buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs

2. Press the **Unlock (🔓)** button and the following happens:

- **If the disk type is configured as 'Removable', the following happens:**

a. All LED's (RED, GREEN & BLUE) become solid for 1 second and then switch off.
b. All LED's (RED, GREEN & BLUE) become solid for 1 second again and then switch off.
d. LEDs return to solid BLUE

- **If the disk type is configured as 'Local', the following happens:**

a. All LED's (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks once.
c. All LED's (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

44. Initialising and formatting diskAshur³ for Windows

After a 'Brute Force Attack' or a complete reset the diskAshur³ will delete all PINs, data and the encryption key. You will need to initialise and format the diskAshur³ before it can be used.

To format your diskAshur³, do the following:

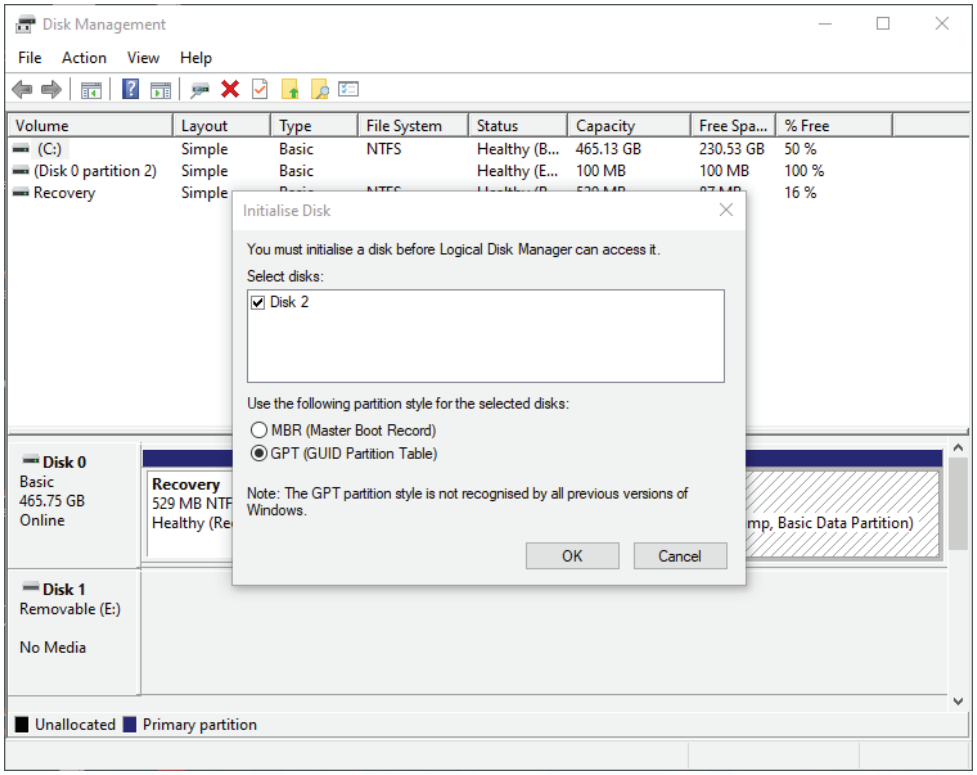
1. Configure a new Admin PIN - see page 21, section 27, 'How to configure an Admin PIN after a Brute Force attack or reset'.

2. With the diskAshur³ in standby state (RED LED), press the **Unlock (🔓)** button once and enter **New Admin PIN** to unlock (blinking GREEN LED).

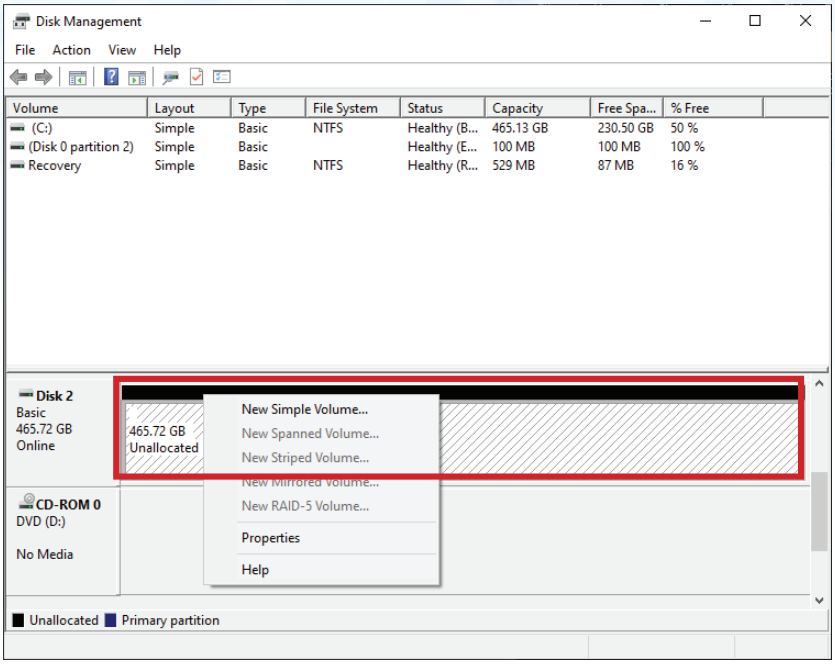
3. **Windows 7:** Right click **Computer** and then click **Manage** and then select **Disk Management**
   Windows 8: Right-click left corner of desktop and select **Disk Management**
   Windows 10: Right click on the start button and select **Disk Management**

4. In the Disk Management window, the diskAshur³ is recognised as an unknown device that is uninitialized and unallocated. A message box should appear for you to choose between MBR and GPT partition style. GPT stores multiple duplicates of this data over the disk, as a result it's much more robust. On an MBR disk, the partitioning and boot information is stored inside single place.

   Select the partition style and click **OK**.



5. Right-click in the blank area over the **Unallocated** section, and then select **New Simple Volume**.



6. The Welcome to the New Simple Volume Wizard window opens. Click Next.

7. If you need only one partition, accept the default partition size and click **Next**.

8. Assign a drive letter or path and click **Next**.

9. Create a volume label, select Perform a quick format, and then click **Next**.

10. Click **Finish**.

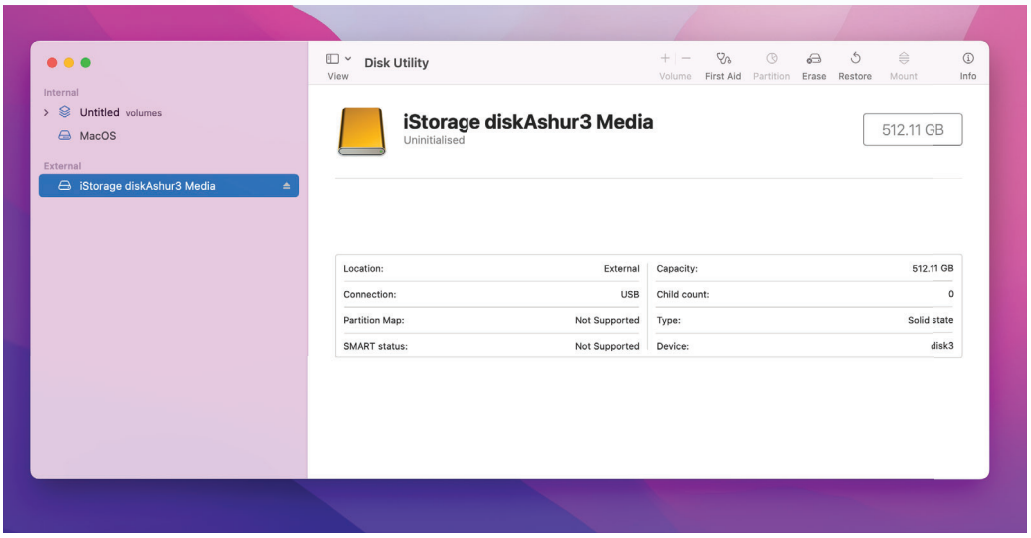
11. Wait until the format process is complete. The diskAshur³ will be recognised and it is available for use.

45. Initialising and formatting diskAshur³ in Mac OS

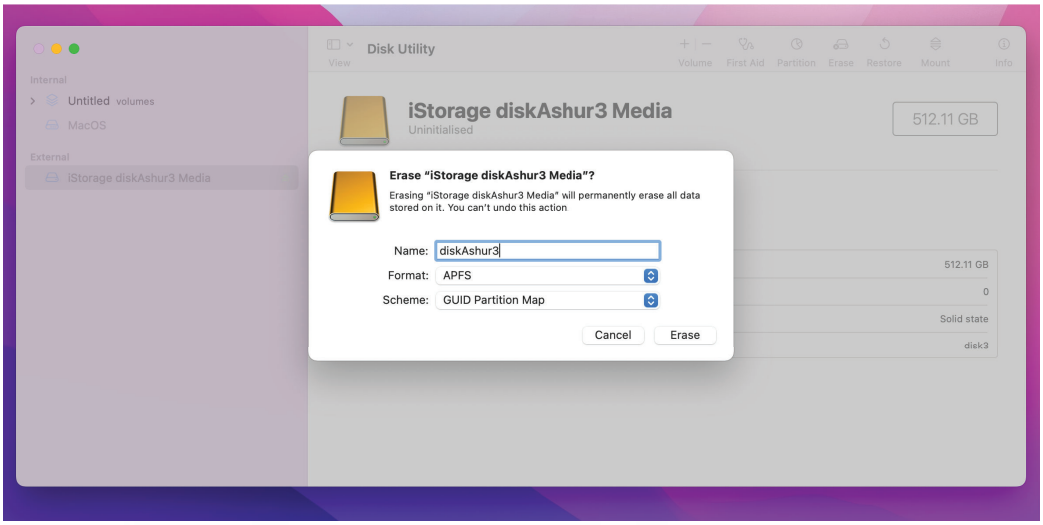
After a 'Brute Force Attack' or a complete reset the diskAshur³ will delete all PINs,data and the encryption key. You will need to initialise and format the diskAshur³ before it can be used.

To initialize and format the diskAshur³:

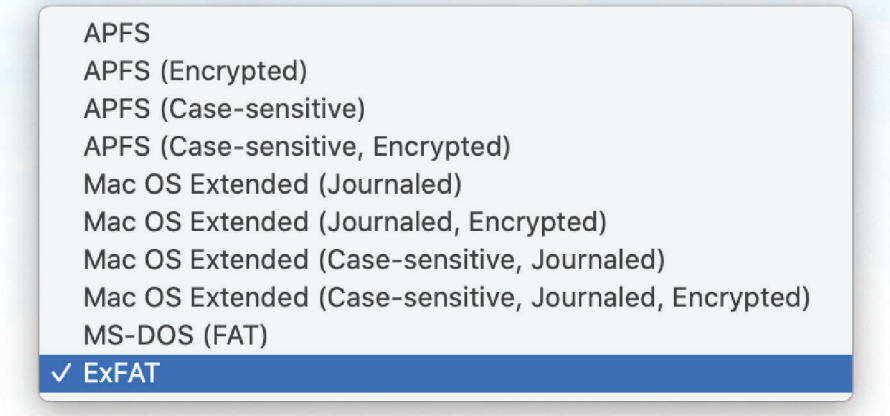
1. Select diskAshur³ from the list of drives and volumes. Each drive in the list will display its capacity, manufacturer, and product name, such as '**iStorage diskAshur³ Media**'.



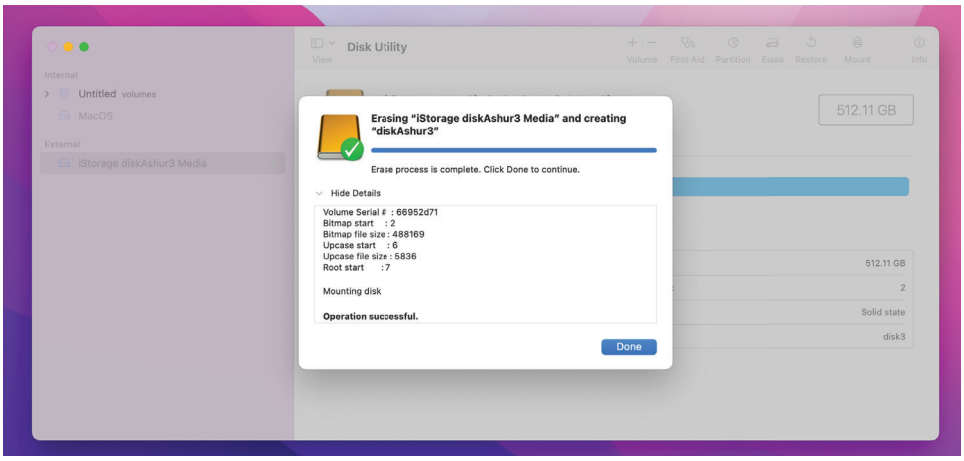
2. Click the '**Erase**' button under Disk Utility.
3. Enter a name for the drive. The default name is Untitled. The name of the drive will eventually appear on the desktop.



4. Select a scheme and volume format to use. The Volume Format dropdown menu lists the available drive formats that the Mac supports. The recommended format type is 'Mac OS Extended (Journaled).' For cross platform use exFAT. The scheme format dropdown menu lists the available schemes to use. We recommend using 'GUID Partition Map' on drives larger than 2TB.

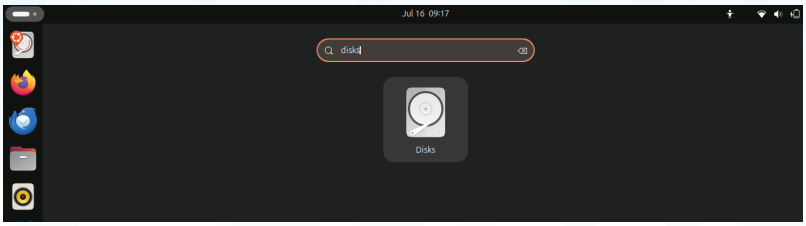


5. Click the 'Erase' button. Disk Utility will unmount the volume from the desktop, erase it, and then remount it on the desktop.

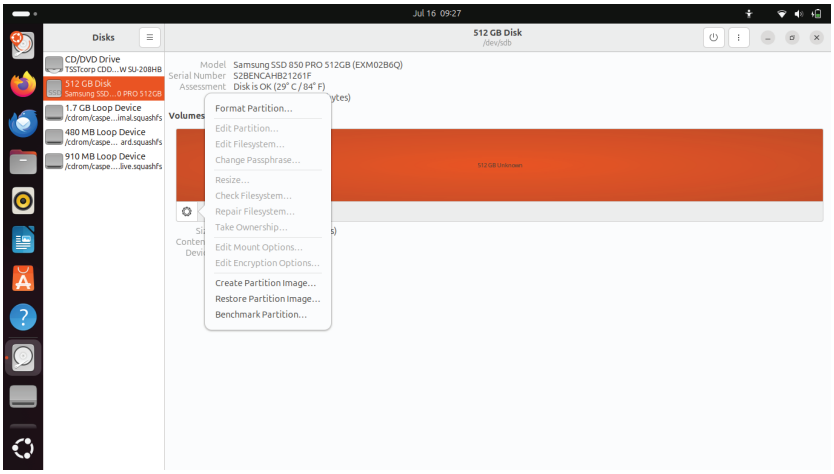


46. Initialising and formatting diskAshur³ in Linux OS

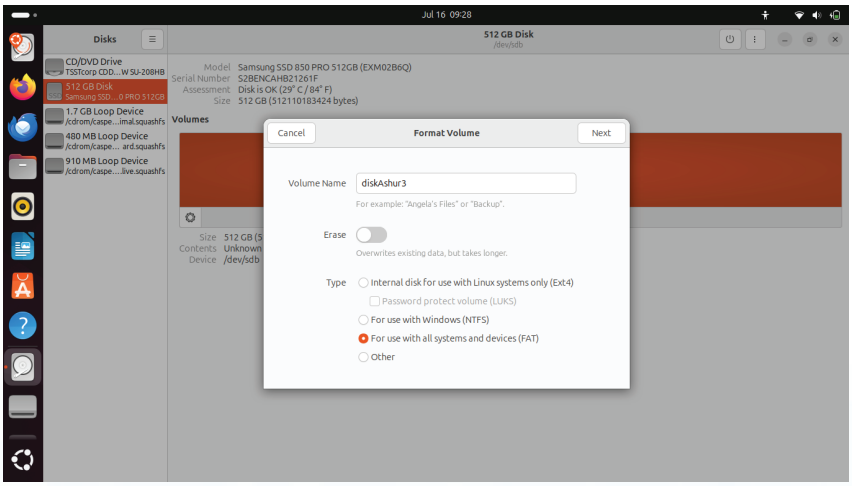
1. Open '**Show Application**' and type '**Disks**' in the search box. Click on the '**Disks**' utility when displayed.

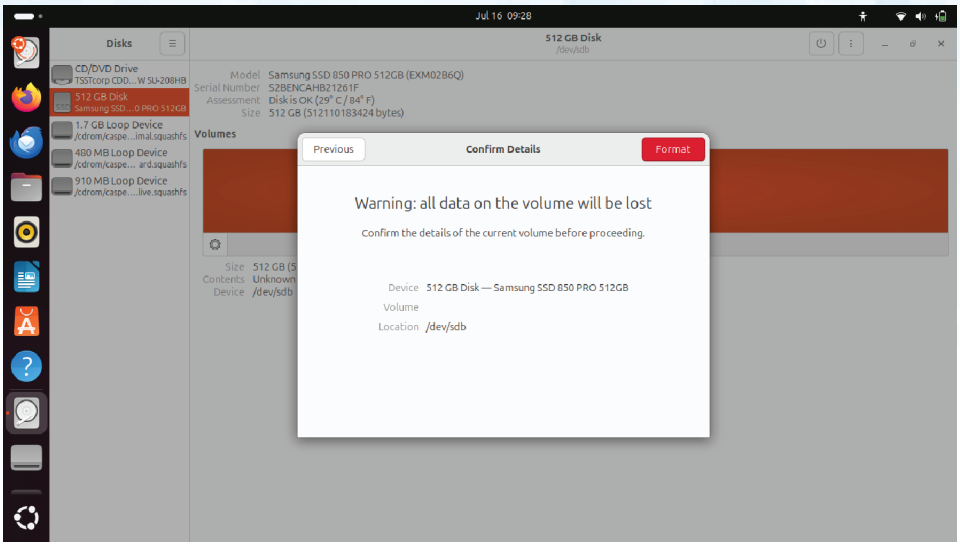


2. Click to select the drive (500 GB Hard Disk) under '**Devices**'. Next click on the gears icon under '**Volumes**' and then click on '**Format Partitons**'.

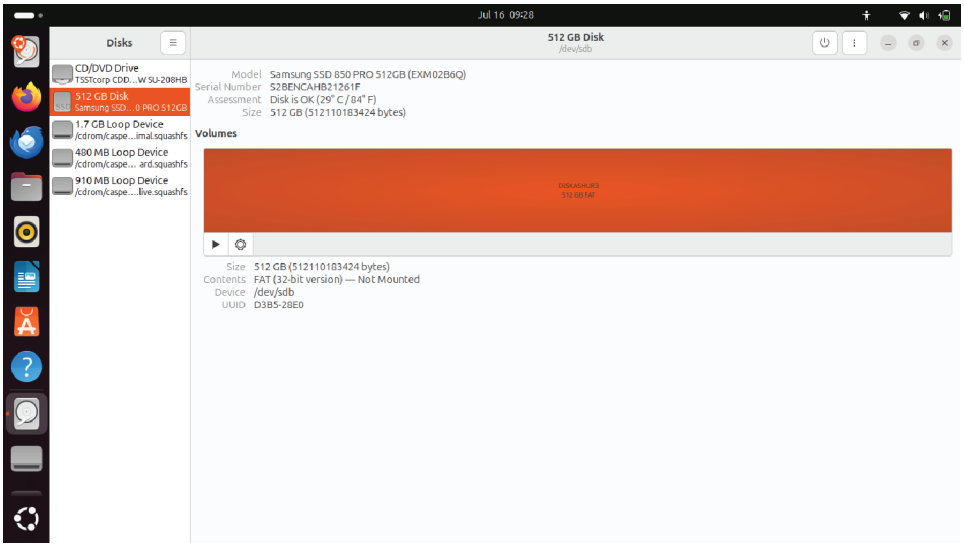


3. Select '**Compatible with all systems and devices (FAT)**' for the '**Type**' option. And enter a name for the drive, e.g: diskAshur³. Then, click the '**Format**' button.

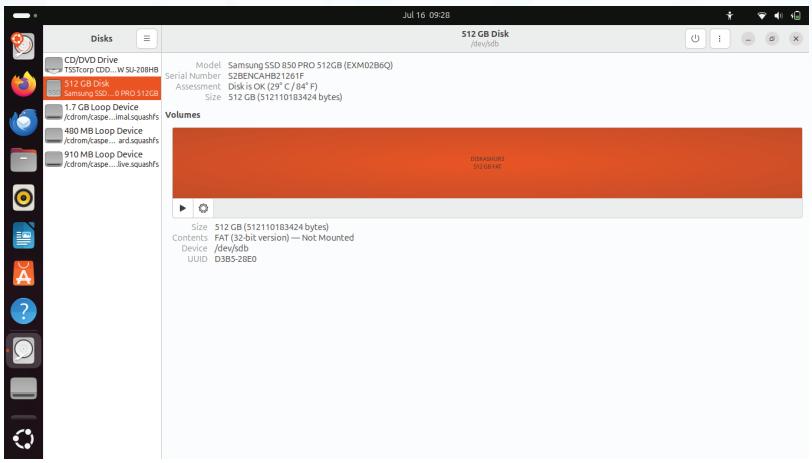




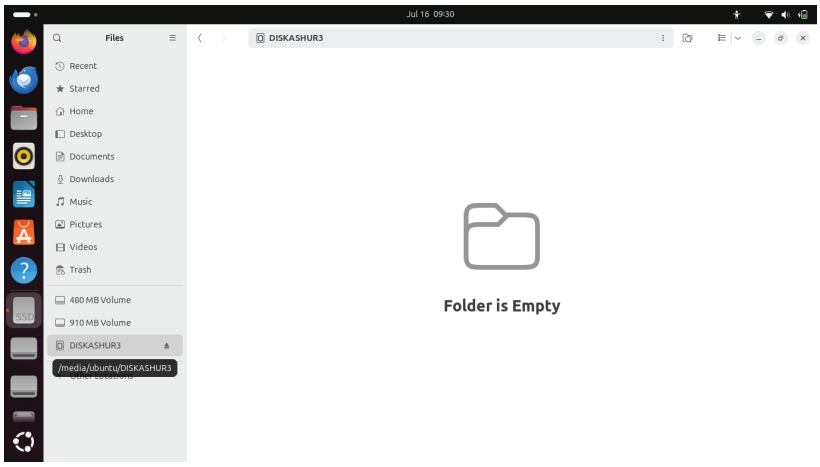
4. After the format process is finished, click Play button to mount the drive to Ubuntu.



5. Now the drive should be mounted to Ubuntu and ready to use.



6. The disk will be shown as seen in the image below. You can click the disk icon to open your drive.



47. Hibernating, Suspending, or Logging off from the Operating System

Be sure to save and close all the files on your diskAshur³ before hibernating, suspending, or logging off from the operating system.

It is recommended that you lock the diskAshur³ manually before hibernating, suspending, or logging off from your system.

To lock the drive, safely eject the diskAshur³ from your host operating system and then unplug from the USB port. If data is being written to the drive, safely ejecting and unplugging the diskAshur³ will result in incomplete data transfer and possible data corruption.

Attention: To ensure your data is secure, be sure to lock your diskAshur³ if you are away from your computer.

48. How to check Firmware in Admin mode

To check the firmware revision number, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both "**3 + 8**" buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **Unlock (🔓)** button once and the following happens; a. All LED's (RED, GREEN & BLUE) become solid for 1 second. b. RED LED blinks indicating the integral part of the firmware revision number. c. GREEN LED blinks indicating the fractional part. d BLUE LED blinks indicating the last digit of the firmware revision number e. All LED's (RED, GREEN & BLUE) become solid for 1 second. f. RED, GREEN & BLUE LEDs switch to a solid BLUE LED		

For example, if the firmware revision number is '**1.9**', the RED LED will blink once (**1**) and the GREEN LED will blink nine (**9**) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to Admin mode, a solid BLUE LED.

49. How to check Firmware in User Mode

To check the firmware revision number, first enter the "**User Mode**" as described in section 13. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

1. In User mode press and hold down both "**3 + 8**" buttons until GREEN and BLUE LEDs blink together		Solid GREEN LED will change to blinking GREEN and BLUE LEDs

2. Press the **Unlock (🔓)** button and the following happens;

a. All LED's (RED, GREEN & BLUE) become solid for 1 second.
b. RED LED blinks indicating the integral part of the firmware revision number.
c. GREEN LED blinks indicating the fractional part.
d. BLUE LED blinks indicating the last digit of the firmware revision number
e. All LED's (RED, GREEN & BLUE) become solid for 1 second.
f. RED, GREEN & BLUE LEDs switch to a solid GREEN LED

For example, if the firmware revision number is '**1.9**', the RED LED will blink once (**1**) and the GREEN LED will blink nine (**9**) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to the User mode, a solid GREEN LED.

50. Technical Support

iStorage provides the following helpful resources for you:

Website:
https://www.istorage-uk.com

E-mail Support:
support@istorage-uk.com

Telephone Support:
+44 (0) 20 8991-6260.

iStorage Technical Support Specialists are available from 9:00 a.m. to 5:30 p.m. GMT - Monday through Friday.

51. Warranty and RMA information

ISTORAGE PRODUCT DISCLAIMER AND WARRANTY

iStorage warrants that on delivery and for a period of 36 months from delivery, its Products shall be free from material defects. However, this warranty does not apply in the circumstances described below. iStorage warrants that the Products comply with the standards listed in the relevant data sheet on our website at the time you place your order.

These warranties do not apply to any defect in the Products arising from:

- fair wear and tear;
- wilful damage, abnormal storage or working conditions, accident, negligence by you or by any third party;
- if you or a third party fail(s) to operate or use the Products in accordance with the user instructions;
- any alteration or repair by you or by a third party who is not one of our authorised repairers; or
- any specification provided by you.

Under these warranties we will, at our option, either repair, replace, or refund you for, any Products found to have material defects, provided that upon delivery:

- you inspect the Products to check whether they have any material defects; and
- you test the encryption mechanism in the Products.

We shall not be liable for any material defects or defects in the encryption mechanism of the Products ascertainable upon inspection on delivery unless you notify such defects to us within 30 days of delivery. We shall not be liable for any material defects or defects in the encryption mechanism of the Products which are not ascertainable upon inspection on delivery unless you notify such defects to us within 7 days of the time when you discover or ought to have become aware of such defects. We shall not be liable under these warranties if you make or anyone else makes any further use of the Products after discovering a defect. Upon notification of any defect, you should return the defective product to us. If you are a business, you will be responsible for the transportation costs incurred by you in sending any Products or parts of the Products to us under the warranty, and we will be responsible for any transportation costs we incur in sending you a repaired or replacement Product. If you are a consumer, please see our terms and conditions.

Products returned must be in the original packaging and in clean condition. Products returned otherwise will, at the Company's discretion, either be refused or a further additional fee charged to cover the additional costs involved. Products returned for repair under warranty must be accompanied by a copy of the original invoice, or must quote the original invoice number and date of purchase.

If you are a consumer, this warranty is in addition to your legal rights in relation to Products that are faulty or not as described. Advice about your legal rights is available from your local Citizens' Advice Bureau or Trading Standards office.

The warranties set out in this clause apply only to the original purchaser of a Product from iStorage or an iStorage authorized reseller or distributor. These warranties are non-transferable.

EXCEPT FOR THE LIMITED WARRANTY PROVIDED HEREIN, AND TO THE EXTENT PERMITTED BY LAW, ISTORAGE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ALL WARRANTIES OF MERCHANTABILITY; FITNESS FOR A PARTICULAR PURPOSE, NONINFRINGEMENT. ISTORAGE DOES NOT WARRANT THAT THE PRODUCT WILL OPERATE ERROR-FREE. TO THE EXTENT THAT ANY IMPLIED WARRANTIES MAY NONETHELESS EXIST BY OPERATION OF LAW, ANY SUCH WARRANTIES ARE LIMITED TO THE DURATION OF THIS WARRANTY. REPAIR OR REPLACEMENT OF THIS PRODUCT, AS PROVIDED HEREIN, IS YOUR EXCLUSIVE REMEDY.

IN NO EVENT SHALL ISTORAGE BE LIABLE FOR ANY LOSS OR ANTICIPATED PROFITS, OR ANY INCIDENTAL, PUNITIVE, EXEMPLARY, SPECIAL, RELIANCE OR CONSEQUENTIAL DAMAGES, INCLUDING, BUT NOT LIMITED TO, LOST REVENUES, LOST PROFITS, LOSS OF USE OF SOFTWARE, DATA LOSS, OTHER LOSS OR RECOVERY OF DATA, DAMAGE TO PROPERTY, AND THIRD-PARTY CLAIMS, ARISING OUT OF ANY THEORY OF RECOVERY, INCLUDING WARRANTY, CONTRACT, STATUTORY OR TORT, REGARDLESS OF WHETHER IT WAS ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. NOTWITHSTANDING THE TERM OF ANY LIMITED WARRANTY OR ANY WARRANTY IMPLIED BY LAW, OR IN THE EVENT THAT ANY LIMITED WARRANTY FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL ISTORAGE'S ENTIRE LIABILITY EXCEED THE PURCHASE PRICE OF THIS PRODUCT. | 4823-2548-5683.3

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, England
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com

iStorage®

DISKASHUR® 3 & DISKASHUR® PRO3

Manuel d'utilisation

Ce manuel d'utilisation est applicable aux diskAshur³ et diskAshur PRO³ qui seront nommé ici diskAshur³

Assurez-vous de vous souvenir de votre code PIN (mot de passe), sans lequel il est impossible d'accéder aux données du disque.

Si vous avez des difficultés à utiliser votre diskAshur³, veuillez contacter notre service client par courriel - support@istorage-uk.com ou par téléphone au +44 (0) 20 8991 6260.

RoHS Compliant

REACH COMPLIANCE

Conformité à la loi sur les accords commerciaux (TAA)

CITRIX vmware

Table des matières

Introduction 46
Contenu de la boîte 46
Disposition du diskAshur³ 46
1. Indicateurs LED et leur signification 47
2. États des LED 47
3. Première utilisation 48
4. Déverrouillage du diskAshur³ à l'aide du code PIN administrateur 49
5. Comment passer en mode Administrateur 49
6. Modifier le code PIN administrateur 50
7. Définir une politique de code PIN utilisateur 51
8. Comment supprimer la politique de code PIN utilisateur 52
9. Comment vérifier la politique de code PIN utilisateur 52
10. Ajouter un nouveau code PIN utilisateur en mode Administrateur 53
11. Modifier le code PIN utilisateur en mode Administrateur 54
12. Supprimer le code PIN utilisateur en mode Administrateur 54
13. Comment déverrouiller le diskAshur³ avec le code PIN utilisateur 55
14. Modifier le code PIN utilisateur en mode Utilisateur 55
15. Mise en marche du clavier à LED rétroéclairé 56
16. Mise à l'arrêt du clavier à LED rétroéclairé 56
17. Créer un code PIN utilisateur de récupération à usage unique 57
18. Supprimer le code PIN utilisateur de récupération à usage unique 57
19. Activer le mode récupération et créer un nouveau code PIN utilisateur 58
20. Définir le mode lecture seule pour l'utilisateur en mode administrateur 58
21. Activer le mode lecture/écriture pour l'utilisateur en mode administrateur 59
22. Définir le mode lecture seule globale en mode administrateur 59
23. Activer le mode lecture/écriture globale en mode administrateur 60
24. Comment configurer un code PIN d'autodestruction 60
25. Comment supprimer le code PIN d'autodestruction 61
26. Comment déverrouiller avec le code PIN d'autodestruction 61
27. Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation 62
28. Régler le verrouillage automatique 62
29. Désactiver le verrouillage automatique en cas de non-utilisation 63
30. Comment vérifier le verrouillage automatique en cas de non-utilisation 64
31. Définir le mode lecture seule en mode utilisateur 64
32. Activer le mode lecture/écriture en mode utilisateur 65
33. Mécanisme de défense contre les tentatives de piratage par force brute 65
34. Comment définir la limite d'attaque par force brute du code PIN utilisateur 66
35. Comment vérifier la limite d'attaque par force brute du code PIN utilisateur 67
36. Comment effectuer une réinitialisation complète 68
37. Comment configurer diskAshur³ comme lecteur bootable 68
38. Comment désactiver la fonctionnalité bootable du diskAshur³ 69
39. Comment vérifier le paramètre disque bootable 69
40. Comment configurer le mode de chiffrement sur le diskAshur³ 70
41. Comment vérifier le mode de chiffrement 71
42. Comment configurer le type de disque 72
43. Comment vérifier le paramètre du type de disque 72
44. Initialiser et formater diskAshur³ pour Windows 73
45. Initialiser et formater diskAshur³ dans Mac OS 75
46. Initialiser et formater diskAshur³ dans Linux OS 77
47. Mettre en veille prolongée, suspendre ou se déconnecter du système d'exploitation 80
48. Comment vérifier le firmware en mode Administrateur 80
49. Comment vérifier le firmware en mode Utilisateur 81
50. Assistance technique 82
51. Informations de garantie et de renvoi de matériel 82

Introduction

Merci d'avoir acheté le nouveau disque diskAshur³ / diskAshur PRO³ d'iStorage, nommé ici diskAshur³.

Le diskAshur³ est un disque portable HDD/SSD facile à utiliser, ultra-sécurisé, protégé par mot de passe et chiffré matériellement, avec des capacités allant jusqu'à 5 To (HDD) et jusqu'à 16 To (SSD), voire plus. Le diskAshur³ chiffre les données en transit et au repos à l'aide d'un chiffrement matériel de 256 bits sur l'ensemble du disque.

Le diskAshur³ intègre un microprocesseur sécurisé certifié aux normes Critères Communs EAL 5+, qui utilise des mécanismes de protection physique intégrés conçus pour empêcher toute altération externe, attaque par contournement et injection de défauts. Contrairement à d'autres solutions, le diskAshur³ réagit aux attaques automatisées en entrant dans un état de blocage, qui rend toutes ces attaques inutiles. Autrement dit, sans le code PIN, il est impossible d'accéder aux données !

Contenu de la boîte

- iStorage diskAshur³
- Pochette de protection
- Câble C & A USB
- Licence gratuite de Nero BackItUp et iStorageDriveSecurity valable un an
- GDR - Guide de démarrage rapide

Disposition du diskAshur³

1. Interface USB 3,2 (Gen 1) Type-C
   Câbles USB Type C et A inclus.
2. Lumières LED -
   ROUGES - mode verrouillé/en veille. VERT FIXE - déverrouillé. VERT CLIGNOTANT - transfert de données. BLEU : mode administrateur.
3. Clavier alphanumérique rétroéclairé (sélectionnable par l'utilisateur), résistant à l'usure avec revêtement époxy.
4. Inviolable, avec témoins d'ouverture non autorisée
   Tous les composants critiques sont recouverts d'une couche de résine époxy super résistante..
5. Puce de chiffrement embarquée
6. Microprocesseur sécurisé dédié certifié Common Criteria EAL 5+
7. Touche MAJ.
8. Touche DÉVERROUILLAGE.
9. Fente pour câble antivol de bureau
10. L' épaisseur du disque de 4-5 To HDD est de 26,8 mm au lieu de 20,8 mm

1. Indicateurs LED et leur signification

LED	Statut du LED	Description	LED	Statut du LED	Description
	ROUGE fixe	Disque verrouillé (à l'état de Veille **ou de** Réinitialisation**)**		La LED bleue est fixe	Disque en **mode administrateur**
	Double clignotement ROUGE	Saisie incorrecte du code PIN		ROUGE, VERT et BLEU Clignotent simultanément	En attente de saisie du code PIN **utilisateur**
	VERT fixe	Disque **déverrouillé**		VERT et BLEU Clignotent ensemble	En attente de saisie du code PIN **administrateur**
	VERT clignotant	Transfert de données en cours		VERT et BLEU Clignotement alterné	Authentification en cours

2. États des LED

Remarque : Le fonctionnement normal du diskAshur³ peut être perturbé par de fortes interférences électromagnétiques. Si tel est le cas, redémarrez simplement le produit (éteindre/mettre hors tension puis sous tension) pour reprendre son fonctionnement normal. Si le fonctionnement normal du disque ne reprend pas, veuillez utiliser le produit dans un autre endroit.

Pour se réveiller de l'état Inactif

Le disque est à l'état inactif lorsqu'il n'est pas en cours d'utilisation et que toutes les LED sont éteintes.

Pour réveiller le diskAshur³ de l'état inactif, faites ce qui suit :

Insérez le disque dans le port USB connecté à votre ordinateur.		Une LED ROUGE continue s'allume indiquant que le disque est en mode Veille

Pour entrer en état Inactif

pour forcer le diskAshur³ à entrer en état inactif, exécutez l'une ou l'autre des opérations suivantes :

- Éjectez et déconnectez le disque de votre ordinateur en toute sécurité, le voyant ROUGE s'éteint (état inactif).

États sous tension

Lorsque le disque sort de l'état Inactif, il passe à l'un des trois états possibles suivants présentés dans le tableau ci-dessous.

État de mise sous tension	Indication LED	Déverrouiller de chiffrement	PIN administrateur	Description
État d'expédition initial	ROUGE et VERT fixe	✓	×	Attente de la configuration d'un code PIN administrateur (première utilisation)
Veille	ROUGE fixe	✓	✓	En attente de la saisie du code PIN administrateur ou utilisateur
Réinitialisation	ROUGE fixe	×	×	Attente de la configuration d'un code PIN administrateur

3. Première utilisation

Le diskAshur³ est fourni dans son **« état initial de livraison », sans code PIN administrateur prédéfini**. Un code PIN Administrateur composé de **8 à 64** chiffres doit être configuré avant de pouvoir utiliser le disque. Après avoir correctement configuré le code PIN administrateur, il n'est plus possible de remettre le disque en « état initial de livraison ».

Exigences relatives au code PIN :

- Doit comprendre de 8 à 64 chiffres.
- Ne doit contenir aucune répétition de chiffres, par ex. (3-3-3-3-3-3-3-3).
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- La touche Maj peut être utilisée pour d'autres combinaisons par ex. (**MAJ** (⬆)**+ 1** produit une valeur différente de 1**).**

Conseil pour le mot de passe : Pour votre code PIN, vous pouvez utiliser une phrase, un nom ou un mot mémorables, ou toute autre combinaison alphanumérique en appuyant simplement sur les boutons indiquant les lettres correspondantes.

Voici des exemples de ces types de codes PIN alphanumériques :

- Pour « **password** » appuyez sur les boutons suivants :
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Pour « **iStorage** » appuyez sur les boutons suivants :
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Cette méthode permet de configurer des codes PIN longs et faciles à mémoriser.

Pour configurer un code PIN d'administrateur et déverrouiller le diskAshur³ pour la première fois, veuillez suivre les étapes simples décrites dans le tableau ci-dessous.

Instructions - Première utilisation	LED	Statut du LED
1. Connectez le diskAshur³ à un port USB branché sur votre ordinateur.		Les LED ROUGE et VERTES s'allument en continu pour indiquer que le lecteur est en état d'expédition initial
2. Appuyez sur les boutons **Déverrouiller (🔓) + 1 et maintenez-les enfoncés.**		Les LED passent au VERT clignotant et BLEU fixe
3. Saisissez votre **nouveau code** PIN **administrateur** (de 8 à 64 chiffres) et appuyez une fois **sur le bouton Déverrouiller (🔓)**		Les LED VERTE clignotante et BLEUE fixe sont remplacées par une LED VERTE qui clignote, puis par les LED VERTE clignotante et BLEUE fixe.
4. Veuillez saisir à nouveau votre **nouveau code PIN** administrateur et appuyez sur le bouton **Déverrouiller (🔓)** une fois		La LED BLEUE clignote rapidement avant de céder la place à la LED BLEUE continue, puis est finalement remplacée par une LED VERTE continue, ce qui indique que le code PIN administrateur a été correctement configuré, que le lecteur est déverrouillé et prêt à être utilisé

Verrouiller le diskAshur³

Pour verrouiller le disque, éjectez-le en toute sécurité de votre système d'exploitation hôte, puis débranchez-le du port USB. Si des données sont en cours d'écriture sur le disque, le fait d'éjecter le diskAshur³ se soldera par un transfert de données incomplet et entraînera potentiellement une corruption de données.

4. Déverrouillage du diskAshur³ à l'aide du code PIN Administrateur

Pour déverrouiller le diskAshur³ à l'aide du code PIN administrateur, suivez les étapes simples détaillées dans le tableau suivant.

1. Branchez le diskAshur³ à un port USB sur votre ordinateur		Une LED ROUGE continue s'allume indiquant que le disque est en mode Veille
2. En état de veille (LED ROUGE allumée), appuyez une fois sur le bouton **Déverrouiller (🔓)**		Les LED VERT et BLEUE se mettent à clignoter simultanément.
3. Alors que les LED de couleur VERTE et BLEUE clignotent simultanément, saisissez votre code PIN administrateur et appuyez sur la touche **Déverrouiller (🔓)** une fois		La LED VERTE clignote plusieurs fois, puis passe à une lumière VERTE continue indiquant que le disque a bien été déverrouillé en tant qu'Administrateur et prêt à être utilisé

5. Comment accéder au mode administrateur

Pour accéder au mode Administrateur, effectuez les étapes suivantes :

1. Branchez le diskAshur³ à un port USB sur votre ordinateur		Une LED ROUGE continue s'allume indiquant que le disque est en mode Veille
2. En mode Veille (LED ROUGE continue), appuyez à la fois sur les boutons **Déverrouiller (🔓) + 1** et maintenez-les enfoncés		Les LED VERTE et BLEUE se mettent à clignoter simultanément
3. Saisissez votre code PIN administrateur et appuyez une fois sur le bouton **Déverrouiller (🔓)** une seule fois		Une LED BLEUE continue s'allume indiquant que le disque est en mode administrateur

Pour quitter le mode Administrateur

Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la LED BLEUE continue passe au ROUGE continu.

6. Changer le code PIN administrateur

Exigences relatives au code PIN :

- Doit comporter entre 8 et 64 chiffres
- Ne doit pas contenir uniquement des nombres répétitifs, par exemple (3-3-3-3-3-3-3-3)
- Ne doit pas contenir uniquement des numéros consécutifs, par exemple (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- La touche Maj peut être utilisée pour d'autres combinaisons par ex. (**MAJ** (⬆)**+ 1** produit une valeur différente de 1**).**

Mot de passe : Vous pouvez configurer un mot, un nom, une phrase ou toute autre combinaison de code PIN alphanumérique en appuyant simplement sur le bouton avec les lettres correspondantes.

Voici des exemples de ces types de codes PIN alphanumériques :

- Pour « **password** » appuyez sur les boutons suivants :
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Pour « **iStorage** » appuyez sur les boutons suivants :
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

En utilisant cette méthode, les codes PIN longs et faciles à mémoriser peuvent être configurés.

Pour modifier le code PIN administrateur, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEU fixe), procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les touches **Déverrouiller (🔓) + 2** enfoncées		La LED BLEUE fixe se transforme en LED VERTE clignotante et BLEUE fixe
2. Saisissez le **NOUVEAU code PIN administrateur**, puis appuyez sur la **Déverrouiller (🔓)** une seule fois		Les LED passeront du VERT clignotant au BLEU fixe pour revenir à une seule LED VERTE clignotante puis de retour à VERT clignotant puis BLEU fixe
3. Ressaisissez ce **NOUVEAU code PIN administrateur**, puis appuyez sur la **Déverrouiller (🔓)** une seule fois		Les LED VERTE clignotante et BLEUE fixe passent à une LED BLEUE clignotant rapidement et enfin à une LED BLEUE fixe indiquant que le code PIN d'administrateur a été modifié avec succès.

Remarque : Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la **LED** BLEUE continue passe au ROUGE continu

7. Définition d'une politique de code PIN utilisateur

L'administrateur peut définir une politique de restriction pour le code PIN utilisateur. Cette politique comprend le réglage de la longueur minimale du code PIN (de 8 à 64 chiffres), ainsi que l'obligation ou non de saisir un ou plusieurs « **caractères spéciaux** ».
Le « caractère spécial » fonctionne comme si les deux touches « **MAJ** (⬆) + chiffre » étaient enfoncées ensemble.

Pour définir une politique de code PIN utilisateur (restrictions), vous devrez saisir trois chiffres, par exemple « **091** », les deux premiers chiffres (**09**) indiquent la longueur minimale du code PIN (dans ce cas, 9) et le dernier chiffre (**1**) indique qu'un ou plusieurs « caractères spéciaux » doivent être utilisés, en d'autres termes « **MAJ** (⬆) + **chiffre** ». De la même manière, une politique de code PIN utilisateur peut être définie sans avoir besoin d'un « caractère spécial », par exemple « **120** », les deux premiers chiffres (**12**) indiquent la longueur minimale du code PIN (dans ce cas, 12) et le dernier chiffre (0) signifie qu'aucun caractère spécial n'est requis.

Lorsque l'administrateur a défini la politique en matière de code PIN utilisateur, par exemple « **091** », un nouveau code PIN utilisateur devra être configuré - pour cela consultez la section 10, « Ajout d'un nouveau code PIN utilisateur en mode administrateur ». Si l'administrateur configure le code PIN de utilisateur comme étant « **247688314** » en utilisant un « **caractère spécial** » (**MAJ** (⬆) + chiffre enfoncé), celui-ci peut être placé n'importe où le long de votre code PIN de 8 à 64 chiffres pendant le processus de création du code PIN de utilisateur, comme indiqué dans les exemples ci-dessous.

A. '**MAJ** (⬆) **+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',
B. '2', '4', '**MAJ** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4',
C. '2', '4', '7', '6', '8', '8', '3', '1', '**MAJ** (⬆) **+ 4**',

Remarque :

- Si un caractère spécial a été utilisé lors de la configuration du code PIN de l'utilisateur, par exemple « B » ci-dessus, alors le disque ne peut être déverrouillé qu'en entrant le code PIN avec le caractère spécial entré précisément dans l'ordre configuré, comme par exemple « B » ci-dessus - (« 2 », « 4 », « **MAJ** » (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- Vous pouvez utiliser plus d'un caractère spécial et le placer le long de votre code PIN de 8 à 64 chiffres.
- Les utilisateurs peuvent changer leur code PIN, mais ils sont obligés de se conformer à l'ensemble de la « Politique relative au code PIN des utilisateurs » (restrictions), si une telle politique est définie.
- La définition d'une nouvelle politique de code PIN utilisateur supprimera automatiquement le code PIN utilisateur s'il existe.
- Cette politique ne s'applique pas au « code PIN d'auto-destruction ». Le réglage de complexité pour le code PIN d'auto-destruction et le code PIN administrateur se compose toujours de 8 à 64 chiffres, sans caractère spécial requis.

Pour définir une **politique de code PIN utilisateur**, veuillez vous assurer d'être en « **mode administrateur** » comme décrit sous section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les boutons **Déverrouiller (🔓) + chiffre 7** enfoncés		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Saisissez vos **3 chiffres**, n'oubliez pas que les deux premiers chiffres indiquent la longueur minimale du code PIN et le dernier chiffre (0 ou 1) qu'un caractère spécial ait été utilisé ou non.		Les LED VERTE et BLEUE clignotent toujours
3. Appuyez une fois sur la touche (⬆) **MAJ**		Les LED VERTE et BLEUE passeront à une LED VERTE fixe puis à une LED BLEUE fixe indiquant que la politique de PIN utilisateur a été activée avec succès.

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

8. Comment supprimer la politique de code PIN utilisateur

Pour supprimer une **politique de code PIN utilisateur**, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les deux boutons **Déverrouiller (🔓) + 7** enfoncés		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Saisissez **080** et appuyez une fois sur le bouton **MAJ** (⬆)		Les LED VERTE et BLEUE passeront à une LED VERTE fixe puis à une LED BLEUE fixe indiquant que la politique du code PIN utilisateur e a été désactivée avec succès

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

9. Comment vérifier la politique du code PIN utilisateur

L'administrateur est en mesure de vérifier la politique de code PIN de l'utilisateur et peut identifier la restriction minimale de longueur du code PIN et si oui ou non l'utilisation d'un caractère spécial a été définie en notant la séquence de LED comme décrit ci-dessous.

Pour vérifier la **politique du code PIN utilisateur**, veuillez vous assurer d'être en « **mode administrateur** » comme décrit sous section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les touches **MAJ** (⬆) **+ 7** enfoncées		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur le bouton **Déverrouiller (🔓)** et voici ce qui se passe; a. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. b. Le clignotement d'une LED ROUGE équivaut à dix (10) unités d'un PIN. c. Chaque clignotement d'une LED VERTE équivaut à une (1) unité d'un PIN d. Un clignotement BLEU indique qu'un caractère spécial a été utilisé. e. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. f. Les LED redeviennent BLEU fixe		

Le tableau ci-dessous décrit le comportement de la LED lors de la vérification de la politique du code PIN utilisateur, par exemple si vous avez défini un code PIN utilisateur à 12 chiffres avec l'utilisation d'un caractère spécial (**121**), la LED ROUGE clignotera une fois (**1**) et la LED VERTE clignotera deux fois (**2**) suivie d'un seul (**1**) clignotement de la LED BLEUE pour indiquer qu'un **caractère spécial** doit être utilisé.

Description du PIN	Configuration à 3 chiffres	ROUGE	VERT	BLEU
Code PIN à 12 chiffres avec utilisation d'un caractère spécial	121	1 Clignotant	2 Clignotants	1 Clignotant
Code PIN à 12 chiffres sans caractère spécial utilisé	120	1 Clignotant	2 Clignotants	0
Code PIN à 9 chiffres avec utilisation d'un caractère spécial	091	0	9 Clignotants	1 Clignotant
Code PIN à 9 chiffres sans caractère spécial utilisé	090	0	9 Clignote	0

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

10. Ajouter un nouveau code PIN utilisateur en mode Administrateur

Important : La création d'un nouveau code PIN utilisateur doit être conforme à la « politique du code PIN utilisateur » définie, si celle-ci a bien été configurée comme décrit sous section 7, qui impose une longueur minimale du code PIN et détermine si un « caractère spécial » a été utilisé. L'administrateur peut se référer à la section 9 pour vérifier les restrictions relatives au code PIN de l'utilisateur.

Exigences relatives au code PIN :

- Doit comporter entre 8 et 64 chiffres
- Ne doit pas contenir uniquement des nombres répétitifs, par exemple (3-3-3-3-3-3-3-3)
- Ne doit pas contenir uniquement des numéros consécutifs, par exemple (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- Le bouton **MAJ** (⬆) peut être utilisé pour d'autres combinaisons de code PIN - par exemple **MAJ** (⬆) + 1 est une valeur différente de 1. Voir la section 7, « Définition d'une politique d'utilisation du code PIN ».

Pour ajouter un nouveau **PIN utilisateur**, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEU fixe), procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les touches **Déverrouiller (🔓) + chiffre 3** enfoncées		La LED BLEUE fixe se transforme en LED VERTE clignotante et BLEUE fixe
2. Saisissez le **nouveau code PIN utilisateur** et appuyer sur le bouton **Déverrouiller (🔓)**		Les LED passeront du VERT clignotant au BLEU fixe pour revenir à une seule LED VERTE clignotante puis de retour à VERT clignotant puis BLEU fixe
3. Ressaisissez ce **nouveau code PIN utilisateur** et appuyez sur le bouton **Déverrouiller (🔓)**		Les LED VERTE clignotante et BLEUE fixe passeront à une LED VERTE fixe puis à une LED BLEUE fixe indiquant qu'un nouveau code PIN utilisateur a été configuré avec succès

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

11. Modification du code PIN utilisateur en mode administrateur

Important : La création d'un nouveau code PIN utilisateur doit être conforme à la « politique du code PIN utilisateur » définie, si celle-ci a bien été configurée comme décrit dans sous section 7, qui impose une longueur minimale du code PIN et détermine si un « caractère spécial » a été utilisé. L'administrateur peut se référer à la section 9 pour vérifier les restrictions relatives au code PIN de l'utilisateur.

Pour modifier un **code PIN utilisateur** existant, veuillez vous assurer d'être en « **mode administrateur** » comme décrit sous section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les touches **Déverrouiller (🔓) + 3** enfoncées		La LED BLEUE fixe se transforme en LED VERTE clignotante et BLEUE fixe
2. Saisissez un **nouveau code PIN utilisateur** et appuyer sur la touche **Déverrouiller (🔓)** une seule fois		Les LED passeront du VERT clignotant au BLEU fixe pour revenir à une seule LED VERTE clignotante puis de retour à VERT clignotant puis BLEU fixe
3. Ressaisissez ce **nouveau code PIN utilisateur** et appuyez sur la touche **Déverrouiller (🔓)** une seule fois		Les LED VERTE et BLEUE passeront à une LED VERTE clignotante puis à une LED BLEUE fixe indiquant que le code PIN utilisateur a été modifié avec succès

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

12. Suppression du code PIN utilisateur en mode administrateur

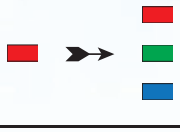
Pour supprimer un **code PIN utilisateur** existant, veuillez vous assurer d'être en « **mode administrateur** » comme décrit sous section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les deux touches **MAJ** (⬆) **+ 3** enfoncées		La LED BLEUE fixe va passer à une LED ROUGE clignotant
2. Pressez et maintenez enfoncées les deux touches **MAJ** (⬆) **+ 3** à nouveau		La LED ROUGE clignotante se transforme en LED ROUGE fixe, puis en LED BLEUE fixe, indiquant que le code PIN de l'utilisateur a été supprimé avec succès

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

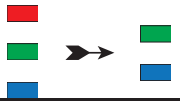
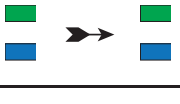
13. Comment déverrouiller le diskAshur³ avec le code PIN utilisateur

Pour déverrouiller le diskAshur³ avec le **code PIN Utilisateur**, effectuez les étapes suivantes.

1. En état de veille (LED ROUGE fixe) Appuyez et maintenez les deux touches **MAJ** (⬆) **+ Déverrouiller (🔓)** enfoncées		La LED ROUGE s'allume et s'éteint, les LED ROUGE, VERTE & BLEUE clignotent
2. Saisissez le **code PIN utilisateur** et appuyer sur la **Déverrouiller (🔓)** une seule fois		Les LED clignotantes ROUGE, VERTE et BLEUE se mettront à clignoter en VERT puis au VERT fixe pour indiquer que le disque a bien été déverrouillé en mode Utilisateur

14. Modifier le code PIN utilisateur en mode utilisateur

Important : le changement du code PIN utilisateur en mode utilisateur (LED VERTE) doit se conformer avec la « Politique de code PIN utilisateur » si elle a été établie telle que décrite à la section 7, ce qui impose une longueur minimum de PIN et si un « caractère spécial » a été utilisé.

1. En mode Utilisateur (LED VERTE), appuyez et maintenez enfoncées les touches **Déverrouiller (🔓) + 4**		La LED VERTE continue est remplacée par toutes les LED, ROUGE, VERTE et BLEUE, qui se mettent à clignoter
2. Saisissez votre PIN utilisateur existant et appuyez une fois sur le bouton **Déverrouiller (🔓)**		Les LED passeront à une LED VERTE clignotante, puis de retour aux LED VERTE clignotante et BLEUE fixe
3. Saisissez le nouveau code PIN utilisateur et appuyez sur le bouton **Déverrouiller (🔓)** une fois		Les LED VERTE clignotante et BLEUE fixe sont remplacées par une LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe
4. Saisissez à nouveau ce nouveau code PIN utilisateur et appuyez sur la touche **Déverrouiller (🔓)** une fois		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui se met à clignoter rapidement avant d'être continue et VERTE, indiquant que le code PIN utilisateur a été correctement modifié

Important : le changement du code PIN utilisateur en mode utilisateur (LED VERTE) doit se conformer avec la « Politique de code PIN utilisateur » si elle a été établie telle que décrite à la section 7, ce qui impose une longueur minimum de PIN et si un « caractère spécial » a été utilisé.

15. Mise en marche du clavier rétroéclairé à LED

Pour une meilleure visibilité en cas de faible luminosité, le diskAshur³ est équipé d'un clavier rétroéclairé par LED. Pour activer le clavier rétroéclairé par LED, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **2 & 6** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **Déverrouiller (🔓)**		Les LED VERTE et BLEUE clignotantes passeront à une LED VERTE puis à un LED BLEUE fixe indiquant que le clavier rétroéclairé par LED a été activé. Il s'allumera la prochaine fois que le disque est branché à un port USB alimenté.

Remarque : Après avoir configuré le diskAshur³ de manière à activer le clavier rétroéclairé par LED, le disque doit d'abord être débranché du port USB alimenté, puis rebranché pour être activé.Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la LED BLEUE continue passe au ROUGE continu.

16. Désactiver le clavier rétroéclairé par LED

Pour désactiver le clavier rétroéclairé par LED, accédez d'abord au **mode Administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **2 & 3** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **Déverrouiller (🔓)**		Les LED VERTE et BLEUE clignotantes passent à une LED VERTE fixe, puis à une LED BLEUE fixe, indiquant que le clavier rétroéclairé a été désactivé et qu'il s'éteindra la prochaine fois que le disque sera branché sur un port USB alimenté.

Remarque : Après avoir configuré le diskAshur³ afin d'éteindre le clavier rétroéclairé par LED, le disque doit tout d'abord être débranché du port USB alimenté, puis rebranché afin d'être activé. Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la LED BLEUE continue passe au ROUGE continu.

17. Créer un code PIN utilisateur de récupération à usage unique.

Le code PIN de récupération utilisateur à usage unique est extrêmement utile dans les situations où un utilisateur a oublié son code PIN, afin de déverrouiller le diskAshur³. Pour activer le mode Récupération, l'utilisateur doit d'abord saisir le code PIN de récupération à usage unique, si ce dernier a été configuré. Le processus de récupération du code PIN n'affecte pas les données, la clé de chiffrement et le code PIN administrateur. Cependant, l'utilisateur est contraint de configurer un nouveau code PIN utilisateur de 8 à 64 chiffres.

Pour configurer un code PIN utilisateur de récupération à usage unique de 8 à 64 chiffres, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. Appuyez à la fois sur les boutons **Déverrouiller (🔓) + 4** et maintenez-les enfoncés.		La LED BLEUE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe
2 Saisissez un code PIN de récupération à usage unique et appuyez sur la touche **Déverrouiller (🔓)**		Les LED VERTE clignotante et BLEUE fixe sont remplacées par une LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe
3. Ressaisissez votre code PIN de récupération à usage unique et appuyez à nouveau sur la touche **Déverrouiller (🔓)**		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui se met à clignoter rapidement avant de se fixer en BLEU indiquant que le code PIN de récupération à usage unique a été correctement configuré

Remarque : Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la **LED** BLEUE continue passe au ROUGE continu.

18. Supprimer le code PIN utilisateur de récupération à usage unique

Pour supprimer la code PIN utilisateur de récupération à usage unique, accédez d'abord au **« mode administrateur »** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. Appuyez sur les boutons **MAJ** (⬆) **+ 4** et maintenez-les enfoncés		La LED BLEUE continue est remplacée par une LED ROUGE clignotante
2. Appuyez sur les boutons **MAJ** (⬆) **+ 4** et maintenez-les enfoncés		La LED ROUGE clignotante devient ROUGE fixe, puis passe à une LED BLEUE fixe, indiquant que le code PIN de récupération à usage unique a été supprimé avec succès

Remarque : Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la **LED** BLEUE continue passe au ROUGE continu.

19. Activer le mode récupération et créer un nouveau code PIN utilisateur

Le code PIN de récupération utilisateur à usage unique est extrêmement utile dans les situations où un utilisateur a oublié son code PIN, afin de déverrouiller le diskAshur³.
Pour activer le mode Récupération, l'utilisateur doit d'abord saisir le code PIN de récupération à usage unique, si ce dernier a été configuré. Le processus de récupération du code PIN utilisateur n'a pas d'impact sur les données, la clé de chiffrement et le code PIN administrateur. Cependant, l'utilisateur est contraint de configurer un nouveau code PIN utilisateur de 8 à 64 chiffres.

Pour activer le processus de récupération et configurer un nouveau code PIN utilisateur, effectuez les étapes suivantes :

1. En mode Veille (LED ROUGE), appuyez sur les boutons **Déverrouiller (🔓) + 4** et maintenez-les enfoncés		La LED ROUGE fixe est remplacée par des LED ROUGE et VERTE clignotante
2. Saisissez le code PIN de récupération à usage unique et appuyez sur la touche **Déverrouiller (🔓)**		Les LED VERTE et BLEUE s'allument et s'éteignent en alternance, passent ensuite à une LED VERTE fixe, puis enfin à une LED clignotante VERTE et une LED BLEUE fixe
3. Saisissez le nouveau code PIN utilisateur et appuyez sur le bouton **Déverrouiller (🔓)**		Les LED passeront du VERT clignotant au BLEU fixe pour revenir à une seule LED VERTE clignotante puis de retour à VERT clignotant puis BLEU fixe
4. Veuillez saisir à nouveau votre code PIN utilisateur et appuyez à nouveau sur le bouton **Déverrouiller (🔓)**		Les LED VERTES clignotent rapidement, puis se fixent en VERT pour indiquer que le processus de récupération s'est correctement déroulé et qu'un nouveau code PIN utilisateur a été configuré

Important : La création d'un code PIN utilisateur doit se conformer à la « Politique de code PIN utilisateur », si cette dernière a été configurée de la manière décrite à la section 7, et qui impose une longueur minimale du code PIN et spécifie si un caractère spécial doit être utilisé. Reportez-vous à la section 9 pour vérifier les restrictions en matière de code PIN utilisateur.

20. Définir le mode de lecture seule utilisateur en mode administrateur

Étant donné le nombre de virus et de chevaux de Troie qui infectent les périphériques USB, la fonctionnalité Lecture seule est particulièrement utile si vous devez accéder au contenu du disque utilisé dans un environnement public. Cette fonctionnalité est également particulièrement utile dans le cadre d'opérations d'investigation/police scientifique, qui nécessitent que les données soient préservées dans leur état initial, sans altération, d'une manière qui empêche toute modification ou écrasement.

Lorsque l'administrateur configure le diskAshur³ et limite l'accès utilisateur au mode Lecture seule, seul l'administrateur peut écrire sur le disque ou rétablir le paramètre en Lecture/écriture, tel que décrit dans la section 21. L'utilisateur est limité à un accès en Lecture seule et ne peut pas écrire sur le disque ni modifier ce paramètre en mode utilisateur.

Pour configurer le diskAshur³ en mode lecture seule global, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez et maintenez les deux boutons enfoncés « **7+ 6** ».		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez une fois sur la **Déverrouiller (🔓)**		Les LED VERTE et BLEUE passeront à une LED VERTE fixe puis à une LED BLEUE fixe indiquant que le disque a été configuré et qu'il limite l'accès de l'utilisateur à la lecture seule

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

21. Activer le mode lecture/écriture pour l'utilisateur en mode administrateur

1. En mode administrateur, appuyez et maintenez les deux boutons « **7+ 9** » enfoncés.		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez une fois sur la **Déverrouiller (🔓)**		Les LED VERTE et BLEUE passent à une LED VERTE fixe puis à une LED BLEUE fixe indiquant que le disque est configuré en lecture/écriture

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

22. Définir le mode de lecture seule global en mode administrateur

Pour configurer le diskAshur³ en mode lecture seule global, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches « **5 + 6** » et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes
2. Appuyez sur la touche **Déverrouiller (🔓)**		Les LED VERTE et BLEUE sont remplacées par une LED VERTE continue, puis par une LED BLEUE fixe , ce qui indique que le disque a été configuré et limite l'accès global en Lecture seule

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

23. Activer le mode lecture/écriture global en mode administrateur

Pour configurer le diskAshur³ en mode lecture/écriture depuis le paramètre Lecture seule global, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez à la fois sur les touches « **5 + 9** » et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes
2. Appuyez sur la touche **Déverrouiller (🔓)**		Les LED VERTE et BLEUE sont remplacées par une LED VERTE continue, puis par une LED BLEUE continue, indiquant que le disque est configuré en mode lecture/écriture

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

24. Instructions pour configurer un code PIN d'autodestruction

Vous pouvez configurer un code PIN d'autodestruction qui, une fois saisi, réalise un effacement cryptographique du disque (la clé de chiffrement est effacée). Ce processus supprime tous les codes PIN configurés et rend toutes les données stockées sur le disque inaccessibles (perdues à tout jamais). Le disque fera apparaître une LED VERTE déverrouillée. L'exécution de cette fonctionnalité engendrera l'auto-destruction du code PIN qui deviendra le nouveau code PIN utilisateur et le disque devra être formaté avant de pouvoir être réutilisé.

Pour configurer un code PIN d'autodestruction, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez enfoncés les boutons **Déverrouiller (🔓) + 6**		La LED BLEUE fixe se transforme en LED VERTE clignotante et BLEUE fixe
2. Configurez et entrez un **code PIN d'autodestruction** de 8 à 64 chiffres et appuyez sur la touche **Déverrouiller (🔓)**		Les LED passeront du VERT clignotant au BLEU fixe pour revenir à une seule LED VERTE clignotante puis de retour à VERT clignotant puis BLEU fixe
3. Ressaisissez ce **code PIN d'autodestruction** et appuyez sur la **Déverrouiller (🔓)** button		La LED VERTE clignote rapidement pendant plusieurs secondes, puis passe à une LED BLEUE fixe pour indiquer que le code PIN d'autodestruction a été configuré avec succès

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

25. Instructions pour supprimer un code PIN d'autodestruction

Pour supprimer un code PIN d'autodestruction existant, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les touches **MAJ (⬆) + 6** enfoncées		La LED BLEUE fixe va passer à une LED ROUGE clignotante
2. Appuyez et maintenez enfoncées les touches **MAJ (⬆) + 6** de nouveau		La LED ROUGE clignote rapidement pendant plusieurs secondes, puis passe à une LED BLEUE fixe pour indiquer que le code PIN d'autodestruction a été configuré avec succès

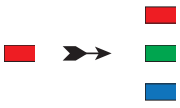
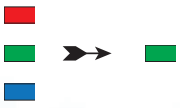
Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

26. Comment déverrouiller avec le code PIN d'autodestruction

Attention :lorsque le mécanisme d'autodestruction est activé, toutes les données, la clé de chiffrement et les codes PIN administrateur/utilisateur sont supprimés.**Le code PIN d'autodestruction devient le code PIN utilisateur.** Aucun code PIN administrateur n'existe après l'activation du mécanisme d'autodestruction. Le diskAshur³ doit d'abord être réinitialisé (voir la section 36 « Comment effectuer une réinitialisation complète » à la page 68) afin de créer un code PIN administrateur avec les pleins privilèges administrateur, notamment la possibilité de créer un code PIN utilisateur.

Lorsqu'il est utilisé, le code PIN d'autodestruction **supprime TOUTES les données, les codes PIN administrateur/utilisateur,** puis déverrouille le disque.
Activer cette fonctionnalité définit le **code PIN d'autodestruction comme le nouveau code PIN utilisateur**, et le diskAshur³ doit être formaté avant que toute nouvelle donnée puisse être ajoutée au lecteur.

Pour activer le mécanisme d'autodestruction, le disque doit être en état de veille (LED ROUGE continue), puis effectuez les étapes suivantes.

1. En état de Veille (LED ROUGE continue), appuyez sur les touches **MAJ** (⬆) + **Déverrouiller (🔓)** et maintenez-les enfoncées		La LED ROUGE est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter
2. Saisissez le code PIN d'autodestruction et appuyez sur le bouton **Déverrouiller (🔓)**		Les LED ROUGE, VERTE et BLEUE clignotantes seront remplacées par une LED VERTE fixe, puis une LED VERTE fixe indiquant que l'auto-destruction du diskAshur³ s'est correctement déroulée

27. Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation

Cette étape sera nécessaire après une attaque par force brute ou lorsque le diskAshur³ a été réinitialisé pour configurer un code PIN administrateur avant que le disque puisse être utilisé de nouveau.

Exigences relatives au code PIN :

- Doit comporter entre 8 et 64 chiffres
- Ne doit pas contenir uniquement des nombres répétitifs, par exemple (3-3-3-3-3-3-3-3)
- Ne doit pas contenir uniquement des numéros consécutifs, par exemple (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- La touche Maj peut être utilisée pour d'autres combinaisons par ex. (**MAJ + 1** produit une valeur différente de 1**).**

Si le diskAshur³ a été brutalement forcé ou réinitialisé, le disque sera en état de veille (LED ROUGE fixe). pour réinitialiser le code PIN administrateur, suivez les étapes suivantes.

1. En état de veille (LED ROUGE), appuyez et maintenez les boutons **MAJ** (⬆) **+ 1** enfoncés		La LED ROUGE fixe se transforme en LED VERTE clignotante et BLEUE fixe
2. Saisissez un **nouveau code PIN administrateur** et appuyez sur la **Déverrouiller (🔓)**		Les LED passeront du VERT clignotant au BLEU fixe pour revenir à une seule LED VERTE clignotante puis de retour à VERT clignotant puis BLEU fixe
3. Ressaisissez ce **nouveau code PIN administrateur** et appuyez sur la **Déverrouiller (🔓)** button		La LED VERTE clignotante et la LED BLEUE fixe passent à la LED BLEUE en clignotant rapidement pendant quelques secondes, puis à une LED BLEUE fixe indiquant que le code PIN administrateur a été configuré avec succès.

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

28. Réglage du verrouillage automatique

Pour se protéger contre un accès non autorisé si le disque est déverrouillé et sans surveillance, le diskAshur³ peut être configuré pour se verrouiller. Dans son état par défaut, le verrouillage automatique du diskAshur³ est désactivé. Celui-ci peut être réglé pour s'activer entre 5 - 99 minutes.

Pour établir un verrouillage automatique , veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les deux boutons **Déverrouiller (🔓) + 5** enfoncés		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Saisissez la durée pendant laquelle vous souhaitez définir la fonction d'autoverrouillage, la durée minimale qui peut être réglée est de 5 minutes et la durée maximale est de 99 minutes (5 à 99 minutes). Par exemple saisissez : **05 pour 5 minutes (appuyez sur « 0 » suivi d'un « 5 »)** **20 pour 20 minutes (appuyez sur « 2 » suivi d'un « 0 »)** **99 pour 99 minutes (appuyez sur « 9 » suivi d'un « 9 »)**		
3. Appuyez sur la touche (⬆) **MAJ**		Les LED VERTE et BLEUE clignotantes passent en VERT fixe pendant une seconde, puis en BLEU fixe pour indiquer que le délai de verrouillage automatique a été configuré avec succès.

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

29. Désactiver le verrouillage automatique

Pour désactiver un verrouillage automatique, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe), procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les deux boutons **Déverrouiller (🔓) + 5** enfoncés		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Saisissez **00** et appuyez sur le bouton **MAJ** (⬆)		Les LED VERTE et BLEUE passeront à une LED VERTE fixe puis à une LED BLEUE fixe indiquant que la fonction de verrouillage automatique a été désactivée avec succès

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

30. Comment vérifier le verrouillage automatique

L'administrateur est en mesure de vérifier et de déterminer la durée de la fonction de verrouillage automatique en notant simplement la séquence des LED comme décrit dans le tableau ci-dessous.

Pour vérifier le verrouillage automatique, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

1. En mode administrateur, appuyez et maintenez les boutons **MAJ** (⬆) **+ 5** enfoncés		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur le bouton **Déverrouiller (🔓)** et voici ce qui se passe ; a. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. b. Le clignotement d'une LED ROUGE équivaut à dix (10) minutes. c. Le clignotement d'une LED VERTE équivaut à une (1) minute. d. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. e. Les LED redeviennent BLEU fixe		

Le tableau ci-dessous décrit le comportement de la LED lors de la vérification du verrouillage automatique. Par exemple, si vous avez réglé le disque pour qu'il se verrouille automatiquement après **25** minutes, la LED ROUGE clignotera deux fois (**2**) et la LED VERTE clignotera cinq (**5**) fois.

Auto-verrouillage en quelques minutes	**ROUGE**	**VERT**
5 minutes	0	5 clignotements
15 minutes	1 clignotement	5 clignotements
25 minutes	2 clignotements	5 clignotements
40 minutes	4 clignotements	0

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

31. Activer la fonction lecture seule en mode utilisateur

Pour configurer le diskAshur³ en lecture seule, veuillez vous assurer d'être en « **mode utilisateur** » tel que cela est décrit à la section 13. Lorsque le disque est en **mode utilisateur** (LED VERTE fixe) procédez aux étapes suivantes.

1. En mode utilisateur, appuyez et maintenez les deux boutons « **7 + 6** » enfoncés. (7=**R**ead (lecture) + 6=**O**nly (**S**eule)		La LED VERTE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **Déverrouiller (🔓)**		Les LED VERTE et BLEUE se transforment en une LED VERTE fixe indiquant que le disque est configuré en lecture seule

Remarque : 1. Si un utilisateur définit le disque en lecture seule, l'administrateur peut changer cela en définissant le disque en lecture/écriture en mode administrateur.

2. Si l'administrateur définit le disque en lecture seule, l'utilisateur ne peut pas définir le disque en lecture/écriture.

32. Activer la lecture/écriture en mode utilisateur

Pour configurer le diskAshur³, en mode lecture/écriture pour utilisateur, veuillez vous assurer d'être en « **mode utilisateur** » tel que cela est décrit à la section 13. Lorsque le disque est en **mode Utilisateur** (LED VERTE fixe) procédez aux étapes suivantes.

1. . En mode utilisateur, appuyez et maintenez les deux boutons « **7+ 9** » enfoncés. (**7**=**R**ead (lecture) + **9**=**W**rite) (écriture)		La LED VERTE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **Déverrouiller (🔓)**		Les LED VERTE et BLEUE se transforment en une LED VERTE fixe indiquant que le disque est configuré en lecture seule

Remarque : 1. Si un utilisateur définit le disque en lecture seule, l'administrateur peut changer cela en définissant le disque en lecture/écriture en mode administrateur.

2. Si l'administrateur définit le disque en lecture seule, l'utilisateur ne peut pas définir le disque en lecture/écriture.

33. Mécanisme de défense contre les tentatives de piratage par force brute

Le diskAshur³ intègre un mécanisme de défense visant à protéger le disque contre les attaque par force brute. Par défaut, la limitation par force brute du **code PIN administrateur** et du **code PIN utilisateur** est configurée à **10** saisies consécutives de code PIN incorrectes. Pour le **code PIN de récupération**, ce chiffre passe à **5**. Trois compteurs de force brute indépendants permettent d'enregistrer les tentatives incorrectes pour chaque autorisation de code PIN. Si un utilisateur saisit un code PIN administrateur incorrect dix fois de suite (réparti en groupes de 5, 3, 2 comme décrit ci-dessous), le disque sera réinitialisé et toutes les données seront perdues à jamais. Si un utilisateur saisit un code PIN de récupération ou un code PIN d'utilisateur incorrect et dépasse les limites d'attaque par force brute respectives, les codes PIN correspondants seront effacés, toutefois les données seront toujours présentes sur le disque.

Remarque : la limitation d'attaque par force brute reprend ses valeurs initiales après réinitialisation complète du disque ou activation de la fonction d'autodestruction. Si l'administrateur modifie le code PIN de l'utilisateur ou qu'un nouveau code PIN est configuré lors de l'activation de la fonction de récupération, le compteur d'attaque par force brute du code PIN utilisateur est effacé, sans que la limitation d'attaques par force brute ne soit affectée. Si l'administrateur modifie le code PIN de récupération, le compteur d'attaques par force brute du code PIN de récupération est réinitialisé.

L'autorisation réussie d'un code PIN donné provoque une réinitialisation du compteur d'attaques par force brute pour ce code PIN, mais n'affecte pas le compteur de force brute des autres codes PIN. L'échec de l'autorisation d'un certain code PIN provoquera une incrémentation du compteur pour ce code PIN, mais n'affectera pas le compteur d'attaques par force brute des autres codes PIN.

- Si un utilisateur saisit un code **PIN utilisateur incorrect** 10 fois consécutives, le code PIN utilisateur sera supprimé mais les données, le code PIN administrateur et le code PIN de récupération resteront intacts et accessibles.
- Si un **code PIN de récupération incorrect** est saisi 5 fois consécutives, le code PIN de récupération est supprimé mais les données et le code PIN administrateur restent intacts et accessibles.
- Le **code PIN administrateur** utilise un mécanisme de défense sophistiqué par rapport aux codes PIN utilisateur et de récupération. Après **5 saisies consécutives incorrectes du code PIN administrateur**, le disque se verrouillera et des LED **ROUGE**, **VERTE** et **BLEUE** fixes s'allumeront. À ce stade, les étapes suivantes doivent être suivies pour permettre à l'utilisateur de saisir **3** codes PIN supplémentaires.

- Saisissez le code PIN « 47867243 » et appuyez sur la touche **Déverrouiller (🔓)**, les LED VERTE et BLEUE se mettent à clignoter en même temps. Le disque est maintenant prêt à accepter 3 autres saisies de PIN administrateur Après un total de 8 saisies consécutives incorrectes du code PIN administrateur, le disque se verrouille et les LED ROUGE, VERTE et BLEUE se mettent à clignoter alternativement.
- À ce stade, les étapes suivantes doivent être suivies afin d'obtenir les **2** derniers codes PIN (10 au total).
- Saisissez le code PIN « **47867243** » et appuyez sur la **touche Déverrouiller (🔓),** les les LED de couleur **VERTE** et **BLEUE** clignotent simultanément, le disque est maintenant prêt à accepter les **2** dernières saisies de code PIN (10 au total).
- Après un total de 10 tentatives de saisie d'un code PIN erroné, la clé de chiffrement sera effacée et toutes les données et les codes PIN stockés sur le disque seront perdus à jamais.

Le tableau ci-dessous suppose que les trois codes PIN ont été configurés et souligne les effets produits par le déclenchement du mécanisme de défense contre les attaques de force brute de chaque type de code PIN.

Code PIN utilisé pour déverrouiller le disque	Saisies consécutives d'un code PIN erroné	Description des conséquences
Code PIN Utilisateur	10	• Le code PIN utilisateur est supprimé. • Le code PIN de récupération, le code PIN administrateur et toutes les données restent intacts et accessibles.
Code PIN de récupération	5	• Le code PIN de récupération est supprimé. • Le code PIN administrateur et toutes les données restent intacts et accessibles.
Code PIN Administrateur	5 3 2 (10 au total)	• Après **5** saisies consécutives de code PIN administrateur erronées, le disque se verrouillera et toutes les LED s'allumeront en continu. • Entrez le code PIN « **47867243** » et appuyez sur la touche **Déverrouiller (🔓)** pour obtenir **3** tentatives supplémentaires de saisie du code PIN. • Après un total de **8** (5+3) saisies consécutives du code PIN d'administration erronées, le disque est verrouillé et les LED clignotent en alternance • Saisissez le code PIN « **47867243** » et appuyez sur la touche **Déverrouiller (🔓)** pour obtenir les deux derniers codes PIN (10 au total). • Après un total de 10 saisies consécutives du code PIN Admin erronées, la clé de chiffrement sera supprimée et toutes les données et les codes PIN stockés sur le disque seront définitivement perdus.

Important : un nouveau code PIN administrateur doit être configuré si le code PIN administrateur préexistant a fait l'objet d'une attaque par force brute. Se reporter à la section 27 à la page 62 « Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation », le diskAshur³ devra également être formaté avant que de nouvelles données ne puissent être ajoutées au disque.

34. Comment définir la limite d'attaques par force brute du code PIN utilisateur

Remarque : la limite d'attaques par force brute du code PIN utilisateur est définie par défaut sur 10 saisies de code PIN erroné, lorsque le disque est complètement réinitialisé, subit une attaque par force brute ou que le code PIN d'autodestruction est activé.

La limite d'attaques par force brute du code PIN utilisateur du diskAshur³ peut être reprogrammée et définie par l'administrateur. Cette fonctionnalité peut être configurée de manière à permettre de 1 à 10 tentatives de saisie de code PIN erroné.

Pour configurer le nombre limite d'attaques par force brute du code PIN utilisateur, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le lecteur est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **7 + 0** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE qui clignotent simultanément
2. Saisissez le nombre de tentatives pour la limite d'attaques par force brute (entre 01 et 10). Par exemple, saisissez : • **01** pour 1 tentative • **10 pour** 10 tentatives		
3. Appuyez une fois sur le bouton « **MAJ** » (⬆)		Les LED VERTE et BLEUE clignotantes seront remplacée par une LED VERTE fixe pendant une seconde, puis par une LED BLEUE qui indique que la limite d'attaques par force brute a été configurée avec succès

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

35. Comment vérifier la limite d'attaque par force brute du code PIN utilisateur

L'administrateur peut observer et déterminer le nombre de saisies consécutives autorisées d'un code PIN utilisateur erroné avant de déclencher le mécanisme de défense contre l'attaque par force brute en notant simplement la séquence LED décrite ci-dessous.

Pour vérifier le paramètre de limite d'attaque par force brute, accédez d'abord au **« mode administrateur »** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez et maintenez les deux touches **2** + **0** enfoncées		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **Déverrouiller (🔓)** et voici ce qui se passe ; a. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. b. Le clignotement d'une LED ROUGE équivaut à dix (10) unités d'une limite de force brute. c. Chaque clignotement d'une LED VERTE équivaut à une (1) unité de limitation de force brute. d. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. e. Les LED redeviennent BLEU fixe		

Le tableau ci-dessous décrit le comportement de la LED lors de la vérification du réglage de la limitation de la force brute. Par exemple, si vous avez réglé la limitation par force brute au bout de **5** entrées consécutives de code PIN incorrect, la LED VERTE clignotera cinq (**5**) fois.

Limitation de la force brute	**ROUGE**	**VERT**
2 tentatives	0	2 clignotements
5 tentatives	0	5 clignotements
10 tentatives	1 clignotement	0

Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

36. Comment effectuer une réinitialisation complète

Pour effectuer une réinitialisation complète, le diskAshur³ doit être en état de veille (LED ROUGE fixe). Lorsque le disque est réinitialisé, tous les codes PIN administrateur/utilisateur, la clé de chiffrement et toutes les données seront supprimés et perdus à jamais et le disque devra être formaté avant de pouvoir être réutilisé. Pour réinitialiser le diskAshur³, suivez les étapes suivantes.

1. En état de veille (LED ROUGE fixe), appuyez sur le bouton « **0** » et maintenez-le enfoncé		La LED ROUGE fixe passe aux LED, ROUGE, VERTE et BLEUE en clignotant en alternance
2. Appuyez et maintenez enfoncés les deux boutons **2 + 7**		Les LED alternantes ROUGE, VERTE et BLEUE deviennent fixes pendant une seconde, puis une LED ROUGE fixe indique que le disque a été réinitialisé.

Important : Après une réinitialisation complète, un nouveau code PIN administrateur doit être configuré, voir section 27 page 62 sur Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation, le diskAshur³ devra également être formaté avant que de nouvelles données puissent être ajoutées au disque.

37. Comment configurer le diskAshur³ en tant que disque Bootable

Remarque : Lorsque le disque est configuré comme étant bootable, l'éjection du disque du système d'exploitation ne force pas le LED à devenir ROUGE. Le disque reste en VERT fixe et doit être débranché pour la prochaine utilisation. Par défaut, diskAshur³ est configuré comme non bootable

Le disque diskAshur³ est équipé d'une fonctionnalité « disque bootable » qui permet la mise hors tension durant un processus de démarrage de l'hôte. Lorsque vous exécutez le démarrage à partir du diskAshur³, vous faites fonctionner votre ordinateur avec le système d'exploitation installé sur le diskAshur³.

Pour définir le disque comme bootable, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. **Une fois que le disque est en** mode administrateur (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches **Déverrouiller (🔓) + 9** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur **« 0 »** suivi par un **« 1 »** (**01**)		Les LED VERTE et BLEUE continueront de clignoter
3. Appuyez une fois sur le bouton **MAJ** (⬆)		Les LED VERTE et BLEUE clignotantes se transforment en LED VERTE fixe, puis en LED BLEUE fixe, ce qui indique que le disque a été configuré avec succès en tant que disque bootable

Remarque : Pour quitter la mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la **LED** BLEUE continue passe au ROUGE continu

38. Comment désactiver la fonctionnalité bootable du diskAshur³

Pour désactiver la fonctionnalité disque bootable du diskAshur³, accédez d'abord au « mode administrateur » **tel que décrit dans la section 5.** Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches **Déverrouiller (🔓) + 9** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes
2. Appuyer sur **« 0 »** suivi d'un autre **« 0 »** (**00**)		Les LED VERTE et BLEUE continueront de clignoter
3. Appuyez une fois sur le bouton **MAJ** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE fixe, puis une LED BLEUE fixe, indiquant que la fonctionnalité bootable a été correctement désactivée

Remarque : Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la **LED** BLEUE continue passe au ROUGE continu

39. Comment vérifier le paramètre disque bootable

Pour vérifier le paramètre bootable, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. **Une fois que le lecteur est en** mode administrateur (LED BLEUE continue), effectuez les étapes suivantes.

1. Appuyez sur les boutons **MAJ** (⬆) **+** 9 et maintenez-les enfoncés.		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante

2. Appuyez sur le bouton **Déverrouiller (🔓)** et vous observerez l'un des deux scénarios suivants :

- **Si diskAshur³ est configuré comme étant bootable, il se passe ce qui suit :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote une fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU continu.

- **Si diskAshur³ n'est <u>PAS</u> configuré comme étant bootable, il se produit ce qui suit ;**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. Toutes les LED s'éteignent
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU continu.

Remarque : Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la LED BLEUE continue passe au ROUGE continu.

40. Comment configurer le mode de chiffrement

ATTENTION : Passer du mode de chiffrement AES-XTS (par défaut) aux modes AES-ECB ou AES-CBC ou vice versa, supprimera la clé de chiffrement se réinitialisera et rendra vos données inaccessibles et définitivement perdues !

Effectuez les étapes suivantes pour configurer le mode de chiffrement du diskAshur³ sur **AES-ECB** indiqué par le numéro **« 01 »**, ou **AES-XTS** indiqué par le numéro **« 02 »,** ou **AES-CBC** indiqué par le numéro **« 03 ».** Cette fonctionnalité est paramétrée comme AES-XTS (02) par défaut. Veuillez noter que tous les paramètres critiques seront supprimés lorsqu'on passe à un autre mode de chiffrement et que cela entraînera une réinitialisation du disque.

Pour configurer le mode de chiffrement du diskAshur³ accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le diskAshur³ est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **Déverrouiller (🔓) + 1** et maintenez-les enfoncées		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotantes
2. Saisissez **01** pour choisir **AES-ECB** Saisissez **02** pour choisir **AES-XTS (par défaut)** Saisissez **03** pour choisir **AES-CBC**		Les LED VERTE et BLEUE continueront de clignoter
3. Appuyez une fois sur le bouton « **MAJ** » (⬆)		Les LED VERTE et BLEUE clignotantes se transforment en LED VERTE fixe, puis en LED ROUGE fixe (état de réinitialisation) ce qui indique que le mode de chiffrement a été changé avec succès

Important : Après avoir configuré le mode de chiffrement, le diskAshur³ se réinitialise totalement, et un nouveau code PIN Administrateur doit être configuré. Référez-vous à la Section 27 de la page 62 : « Comment configurer un code PIN Administrateur après une attaque brutale ou une réinitialisation ».

41. Comment vérifier le mode de chiffrement

Pour vérifier le mode de chiffrement diskAshur³ accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le disque est en mode administrateur (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode Administrateur appuyez sur les touches « **MAJ** (⬆) + **1**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.

2. Appuyez sur le bouton **Déverrouiller (🔓)** et vous observerez ce qui suit :

- **Si le mode de chiffrement est configuré AES-ECB :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote une fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU continu.

- **Si le mode est configuré AES-XTS :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote deux fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU continu.

- **Si le mode est configuré AES-CBC :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote trois fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU continu.

Remarque : Pour quitter le mode Administrateur (LED BLEUE continue) immédiatement, appuyez et maintenez enfoncée la touche **MAJ** (⬆) pendant une seconde - la **LED** BLEUE continue passe au ROUGE continu.

42. Comment configurer le type de disque

Le diskAshur³ peut être configuré en tant que « disque amovible » ou « disque local (état par défaut) ». Le passage à un autre type de disque efface tous les paramètres critiques, supprime tous les codes PIN, la clé de chiffrement et les données, et entraîne la réinitialisation du disque.

ATTENTION : Changer le type de disque en « Disque amovible » ou « Disque local (état par défaut) » supprimera la clé de chiffrement et provoquera la réinitialisation du diskAshur³ et rendra toutes les données inaccessibles et perdues à jamais !

Suivez les étapes suivantes pour configurer le type de disque diskAshur³ en disque amovible (**00**) ou disque local (**01**). Par défaut, cette fonction est définie comme disque local (**01**). Veuillez noter que, lors du passage à un autre type de disque, tous les paramètres critiques seront effacés, ce qui entraînera une réinitialisation du disque.

Pour configurer le type de disque diskAshur³ accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le diskAshur³ est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**Déverrouiller (🔓) + 8**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes
2. Saisissez **00** pour choisir **Disque amovible** Saisissez **01** pour choisir **Disque local (par défaut)**		Les LED VERTE et BLEUE continueront de clignoter
3. Appuyez une fois sur le bouton « **MAJ** »(⬆)		Les LED VERTE et BLEUE seront remplacées par une LED VERTE fixe, puis une LED ROUGE fixe (**État de Réinitialisation**) indique que le type de disque a bien été changé

Important : après avoir changé le type de disque, le diskAshur³ se réinitialise complètement et un nouveau code PIN administrateur doit être configuré, reportez-vous à la section 27 à la page 62 sur « Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation »

43. Comment contrôler le paramètre de type de disque

Pour vérifier le paramètre de type de disque du diskAshur³, accédez d'abord au « mode administrateur » tel que décrit dans la section 5. Une fois que le disque est en mode administrateur (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode Administrateur appuyez, sur les touches « **MAJ** (⬆) + **8**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes

2. Appuyez sur le bouton **Déverrouiller (🔓)** et vous observerez ce qui suit :

- **Si le type de disque est configuré comme « amovible », il se produit ce qui suit :**

a. Toutes les LED (ROUGE, VERTE & BLEUE) s'allument pendant 1 seconde puis s'éteignent.
b. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument à nouveau pendant 1 seconde, puis s'éteignent.
d. Les LED reviennent au BLEU continu.

- **Si le type de disque est configuré comme « local », il se produit ce qui suit :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote une fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU continu.

44. Initialisation et formatage du diskAshur³ pour Windows

Après une « attaque par force brute » ou une réinitialisation complète du diskAshur³, toutes les données, les données et la clé de chiffrement sont supprimés. Vous devez initialiser et formater le diskAshur³ avant de pouvoir l'utiliser.

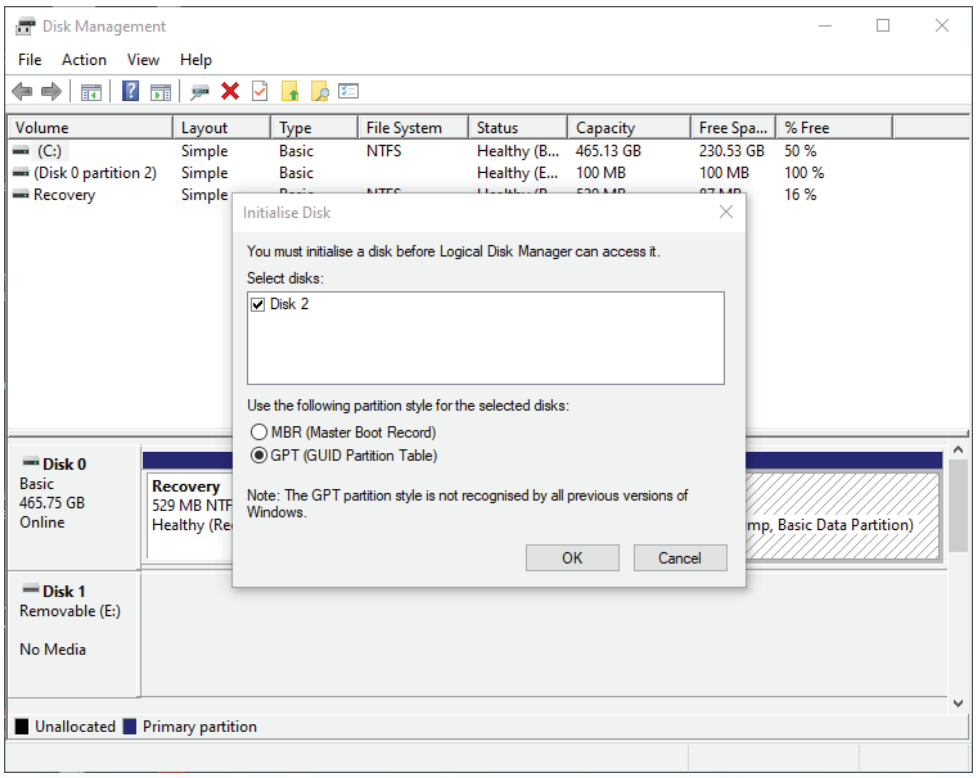
Pour formater votre diskAshur³, procédez comme suit :

1. Configurez un nouveau code PIN administrateur : voir page 62, section 27 « Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation »
2. Lorsque le diskAshur³ est en état de veille (LED ROUGE), appuyez une fois sur la touche Déverrouiller **(🔓)** et saisissez le nouveau code PIN administrateur pour le déverrouiller (LED VERTE clignotante).

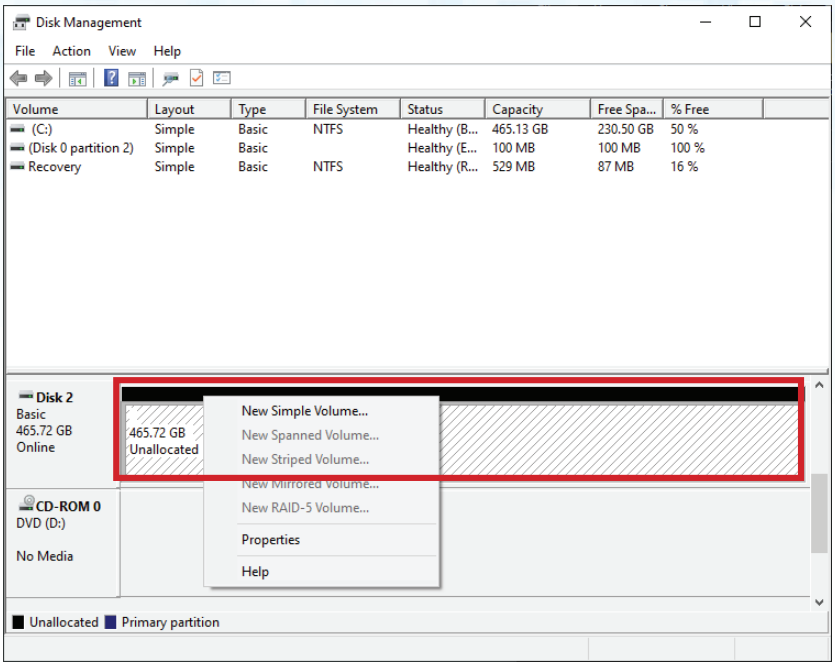
3. **Windows 7 :** Cliquez avec le bouton droit de la souris sur **Ordinateur**, puis cliquez sur **Gestion** et sélectionnez **Gestion des disques**
   Windows 8 : Cliquez avec le bouton droit de la souris sur le coin gauche du bureau et sélectionnez **Gestion des disques**
   Windows 10 : Cliquez avec le bouton droit de la souris sur le bouton Démarrer et sélectionnez **Gestion des disques**

4. Dans la fenêtre de gestion des disques, le diskAshur³ est reconnu comme un périphérique inconnu, non initialisé et non alloué. Une fenêtre de message s'affiche pour vous permettre de choisir entre le style de partition MBR et le style de partition GPT. GPT stocke plusieurs copies de ces données sur le disque, ce qui le rend beaucoup plus robuste. Sur un disque MBR, les informations de partitionnement et de démarrage sont stockées au même endroit.

   Sélectionnez le style de partition et cliquez sur **OK**.



5. Faites un clic droit dans la zone vide située sur la section **Non alloué**, puis sélectionnez **Nouveau volume simple**.



6. La fenêtre Bienvenue de l'assistant Nouveau volume simple s'ouvre. Cliquez sur Suivant.

7. Si vous avez besoin d'une seule partition, acceptez la taille de partition par défaut et cliquez sur **Suivant**.

8. Affectez une lettre ou un chemin de lecteur et cliquez sur **Suivant**.

9. Créez un libellé de volume, sélectionnez Effectuer un formatage rapide, puis cliquez sur Suivant.

10. Cliquez sur Terminer.

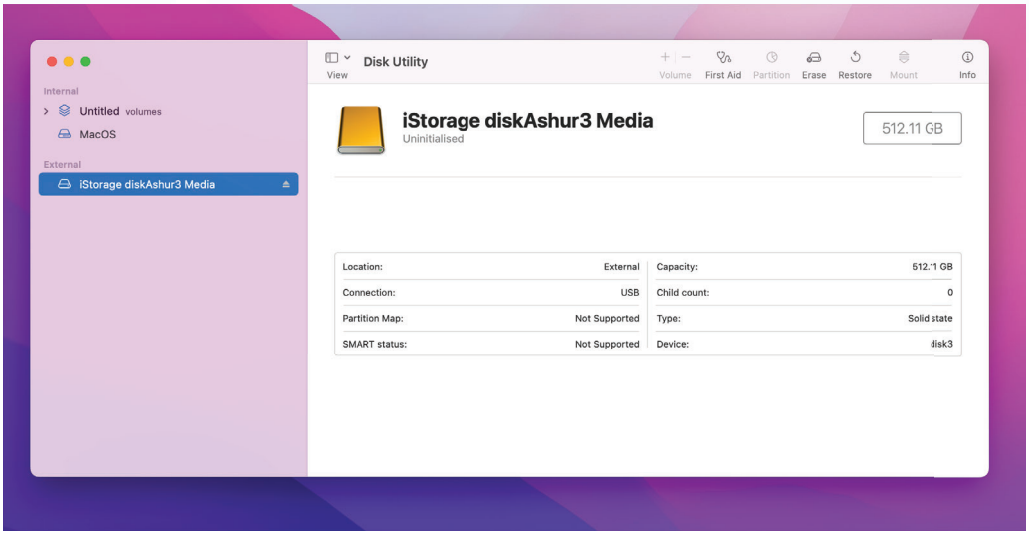
11. Patientez jusqu'à la fin du formatage. Le diskAshur³ est reconnu et peut être utilisé.

45. Initialisation et formatage du diskAshur³ sous Mac OS

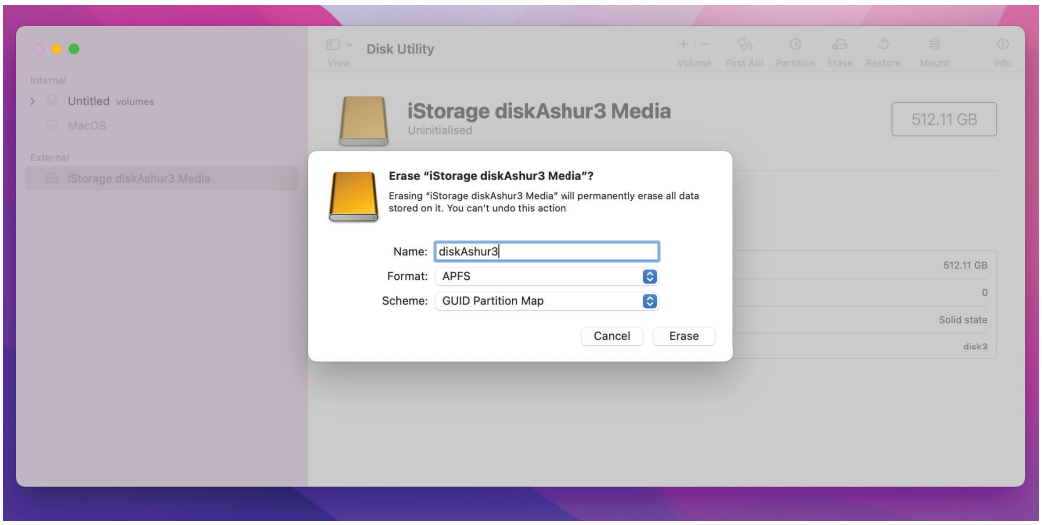
Après une « attaque par force brute » ou une réinitialisation complète du diskAshur³ toutes les données, les données et la clé de chiffrement sont supprimés. Vous devez initialiser et formater le diskAshur³ avant de pouvoir l'utiliser.

Pour initialiser et formater le diskAshur³ :

1. Sélectionnez diskAshur³ dans la liste des disques et des volumes. Chaque disque de la liste affiche sa capacité, son fabricant et le nom du produit, par exemple « **iStorage diskAshur³ Media** ».

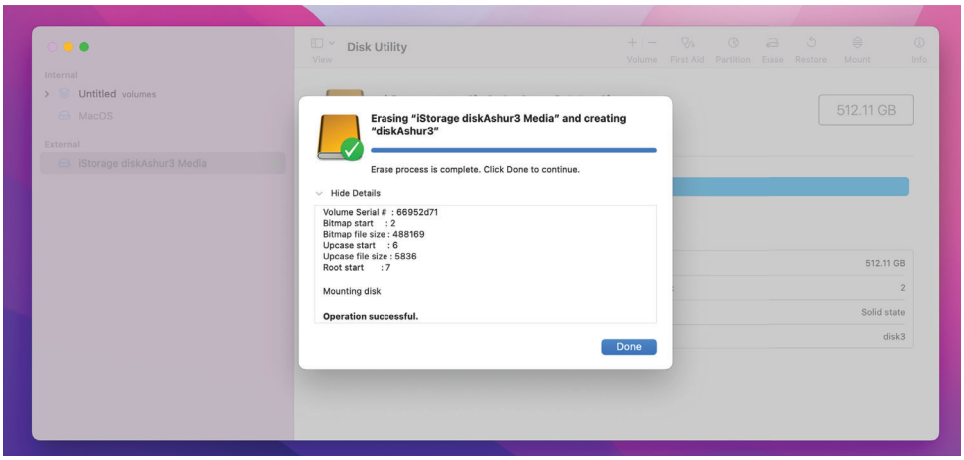


2. Cliquez sur la touche « **Effacer** » de l'Utilitaire de disque.
3. Saisissez un nom pour le disque. Le nom par défaut est Sans titre. Le nom du disque finit par apparaître sur le bureau.



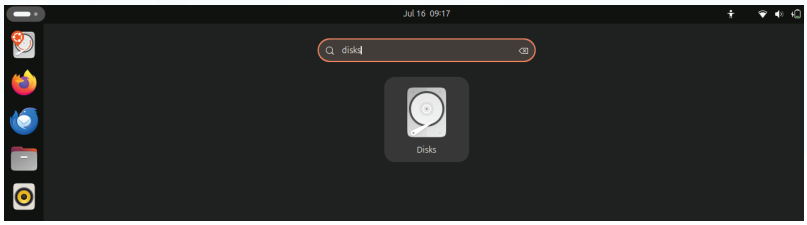
4. Sélectionnez un format de modèle et de volume à utiliser. Le menu déroulant Volume Format (Format du volume) (répertorie les formats de lecteur pris en charge par le Mac. Le type de format recommandé est « Mac OS Extended (Journaled) ». Pour les plates-formes multiples, utilisez exFAT. Le menu déroulant du format de schéma répertorie les schémas disponibles à utiliser. Nous vous recommandons d'utiliser « GUID Partition Map » sur les disques d'une capacité supérieure à 2 To.

5. Cliquez sur le bouton « Effacer ». L'utilitaire de disque démonte le volume du bureau, l'efface et le remonte sur le bureau.

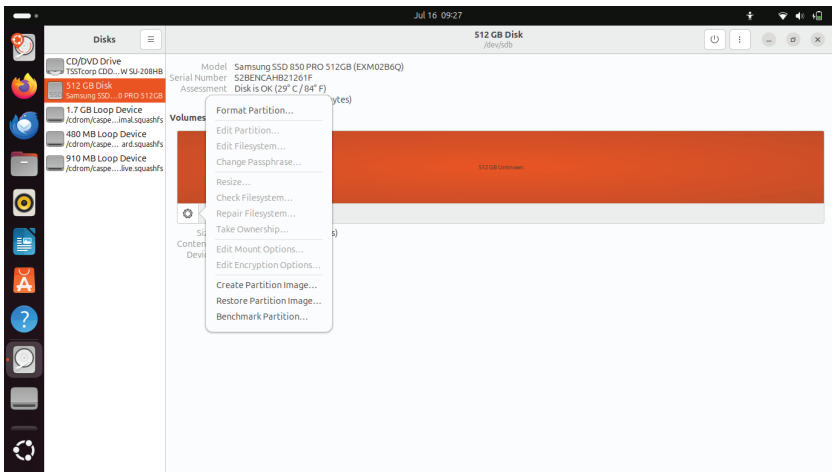


46. Initialisation et formatage de diskAshur³ sous Linux OS

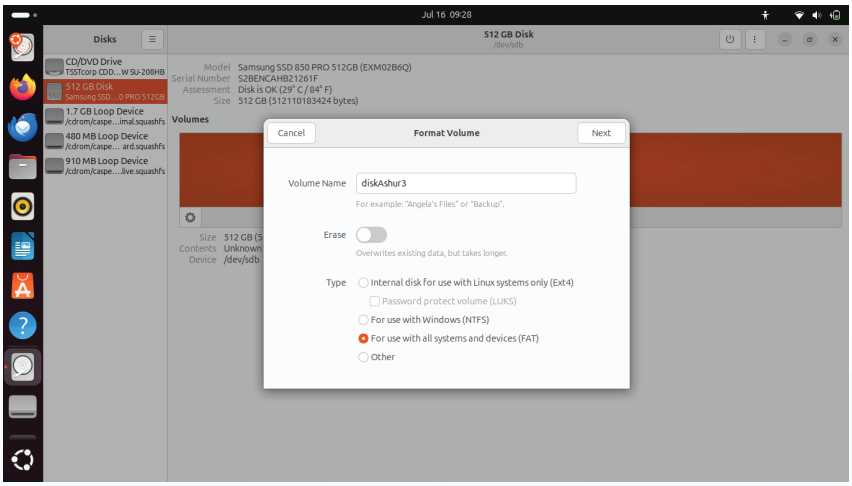
1. Ouvrez « **Afficher application** » et tapez « **Disques** » dans la case de recherche. Cliquez sur l'utilitaire Disques lorsqu'il est affiché.

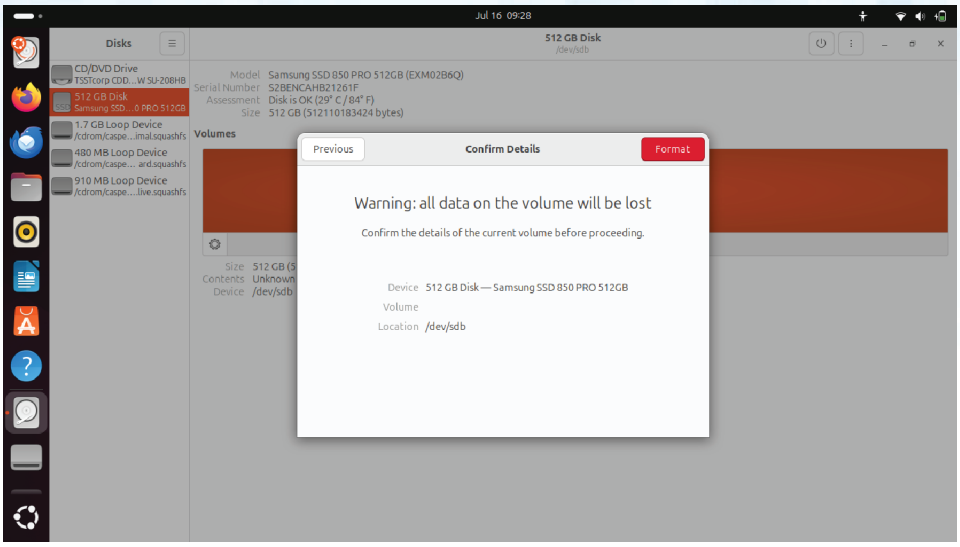


2. Cliquez pour sélectionner le disque (disque dur de 500 Go) sous « **Périphériques** ». Ensuite, cliquez sur l'icône d'engrenage sous Volumes, puis cliquez sur Formater des partitions.

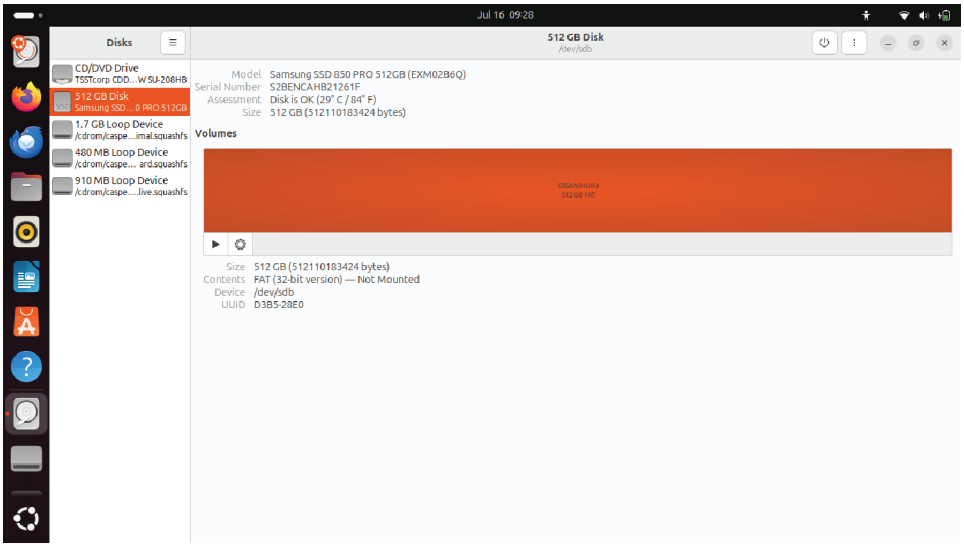


3. Sélectionnez « **Compatible avec tous les systèmes et appareils (FAT)** » dans l'option « **Type** ». Saisissez un nom pour le disque, par exemple : diskAshur³. Ensuite, cliquez sur la touche « **Formater** ».

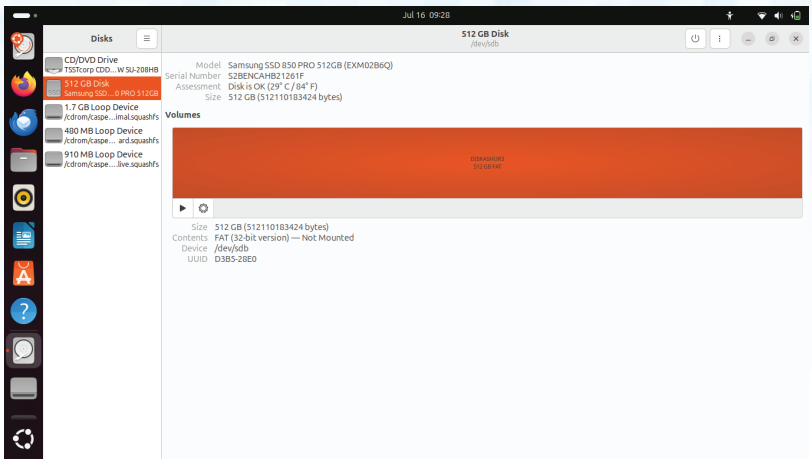




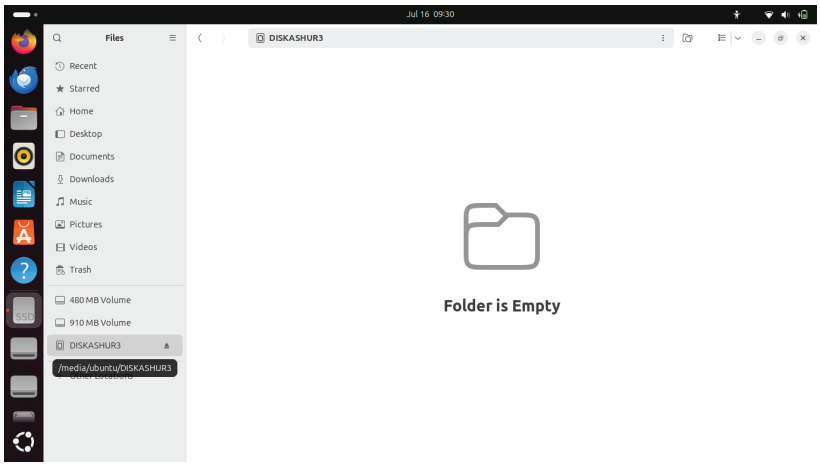
4. Une fois le processus de formatage terminé, cliquez sur le bouton Lancer le montage du disque dans Ubuntu.



5. Maintenant, le disque est monté sous Ubuntu et prêt à être utilisé.



6. 'icône en forme de disque s'affichera, comme illustré dans l'image ci-dessous. Vous pouvez cliquer sur l'icône en forme de disque pour ouvrir votre lecteur.



47. Hibernation, suspension ou déconnexion du système d'exploitation

Veillez à sauvegarder et à fermer tous les fichiers de votre diskAshur³ avant d'hiberner, de suspendre ou de vous déconnecter du système d'exploitation.

Il est recommandé de verrouiller le diskAshur³ manuellement avant de le mettre en veilleuse, de le suspendre ou de le déconnecter du système.

Pour verrouiller le disque, éjectez le diskAshur³ de votre système d'exploitation hôte en toute sécurité, puis débranchez-le du port USB. Si des données sont en cours d'écriture sur le disque, la déconnexion du diskAshur³ entraînera un transfert de données incomplet et une éventuelle corruption des données.

⚠ **Attention:** Pour garantir la sécurité de vos données, assurez-vous de verrouiller votre diskAshur³ si vous n'êtes pas sur votre ordinateur.

48. Comment vérifier le firmware en mode administrateur

Pour vérifier la version du firmware, veuillez vous assurer d'être en « **mode administrateur** » comme décrit à la section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe), procédez aux étapes suivantes.

1. En mode administrateur et maintenez les deux boutons « **3 + 8** » enfoncés		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **Déverrouiller (🔓)** et voici ce qui se passe : a. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. b. La LED ROUGE clignote, indiquant la partie intégrante du numéro de la version du firmware. c. La LED VERTE clignote pour indiquer la partie fractionnaire. d. La LED BLEUE clignote, indiquant la partie intégrante du numéro de la version du firmware e. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde. f. Les LED ROUGE, VERTE & BLEUE passent à une LED BLEUE fixe		

Par exemple, si la version du firmware est « **2.3** », la LED ROUGE clignotera deux (**2**) fois et la LED VERTE trois (**3**) fois. Une fois la séquence terminée, les ROUGE, VERTE & BLEUE clignotent ensemble une fois, puis reviennent en mode administrateur, une LED BLEUE fixe apparaît alors.

49. Comment vérifier le firmware en mode utilisateur

Pour vérifier la version du firmware, veuillez vous assurer d'être en « **mode utilisateur** » comme décrit à la section 13. Lorsque le disque est en **mode utilisateur** (LED VERTE fixe), procédez aux étapes suivantes.

1. En mode utilisateur, appuyez sur les deux boutons « **3 + 8** » et maintenez-les enfoncés jusqu'à ce que les LED VERTE et BLEUE clignotent ensemble		La LED VERTE fixe se transforme en LED VERTE et BLEUE clignotante

2. Appuyez sur la **Déverrouiller (🔓)** et voici ce qui se passe :

a. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde.
b. La LED ROUGE clignote, indiquant la partie intégrante du numéro de la version du firmware.
c. La LED VERTE clignote pour indiquer la partie fractionnaire.
d. La LED BLEUE clignote, indiquant la partie intégrante du numéro de la version du firmware
e. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde.
f. Les LED ROUGE, VERTE & BLEUE passent à une LED BLEUE fixe

Par exemple, si la version du firmware est « **2.3** », la LED ROUGE clignotera deux (**2**) fois et la LED VERTE trois (**3**) fois. Une fois la séquence terminée, les LED ROUGE, VERTE & BLEUE clignotent ensemble une fois, puis reviennent au mode utilisateur avec une LED VERTE fixe.

50. Support technique

iStorage met à votre disposition les ressources utiles suivantes :

Site internet :
https://www.istorage-uk.com

Support e-mail :
support@istorage-uk.com

Support téléphonique :
+44 (0) 20 8991-6260.

Les spécialistes du support technique d'iStorage sont disponibles de 9h00 à 17h30 GMT - du lundi au vendredi.

51. Informations sur la garantie et le RMA

ISTORAGE CLAUSE DE NON-RESPONSABILITÉ ET GARANTIE DU PRODUIT

iStorage garantit qu'à la livraison et pendant une période de 36 mois à compter de la livraison, ses produits sont exempts de défauts matériels. Toutefois, cette garantie ne s'applique pas dans les circonstances décrites ci-dessous. iStorage garantit que les produits sont conformes aux normes énumérées dans la fiche technique correspondante sur notre site web au moment où vous passez votre commande.

Ces garanties ne s'appliquent pas à tout défaut des produits découlant de :

- de l'usure normale ;
- d'un dommage intentionnel, de conditions de stockage ou de travail anormales, d'un accident, d'une négligence de votre part ou de la part d'un tiers ;
- si vous ou un tiers ne faites pas fonctionner ou n'utilisez pas les produits conformément aux instructions d'utilisation ;
- toute modification ou réparation effectuée par vous ou par un tiers qui n'est pas un de nos réparateurs agréés ; ou
- toute spécification fournie par vous.

Dans le cadre de ces garanties, nous nous engageons, à notre choix, à réparer, remplacer ou rembourser tout produit présentant un défaut matériel, à condition que lors de la livraison :

- vous inspectiez les produits pour vérifier s'ils présentent des défauts matériels ; et
- vous testez le mécanisme de cryptage dans les produits.

Nous ne sommes pas responsables des défauts matériels ou des défauts du mécanisme de cryptage des produits constatés lors de l'inspection à la livraison, sauf si vous nous les signalez dans les 30 jours suivant la livraison. Nous ne sommes pas responsables des défauts matériels ou des défauts du mécanisme de cryptage des produits qui ne peuvent être constatés lors de l'inspection à la livraison, sauf si vous nous les signalez dans les 7 jours suivant le moment où vous les avez découverts ou auriez dû en prendre connaissance. Nous ne sommes pas responsables au titre de ces garanties si vous ou toute autre personne utilisez les produits après avoir découvert un défaut. Dès la notification d'un défaut, vous devez nous retourner le produit défectueux. Si vous êtes une entreprise, vous serez responsable des frais de transport que vous aurez engagés pour nous envoyer tout produit ou partie de produit au titre de la garantie, et nous serons responsables de tous les frais de transport que nous aurons engagés pour vous envoyer un produit réparé ou de remplacement. Si vous êtes un consommateur, veuillez consulter nos conditions générales.

Les produits retournés doivent être dans l'emballage d'origine et en bon état de propreté. Les produits retournés autrement seront, à la discrétion de la société, soit refusés, soit des frais supplémentaires seront facturés pour couvrir les coûts supplémentaires impliqués. Les produits retournés pour réparation sous garantie doivent être accompagnés d'une copie de la facture originale, ou doivent mentionner le numéro de la facture originale et la date d'achat.

Si vous êtes un consommateur, cette garantie s'ajoute à vos droits légaux en ce qui concerne les produits défectueux ou non conformes à la description. Des conseils sur vos droits légaux sont disponibles auprès de votre bureau local de conseil aux citoyens ou de votre bureau des normes commerciales.

Les garanties énoncées dans la présente clause s'appliquent uniquement à l'acheteur initial d'un produit d'iStorage ou d'un revendeur ou distributeur agréé par iStorage. Ces garanties ne sont pas transférables.

À L'EXCEPTION DE LA GARANTIE LIMITÉE PRÉVUE DANS LE PRÉSENT DOCUMENT, ET DANS LA MESURE OÙ LA LOI LE PERMET, ISTORAGE DÉCLINE TOUTE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER, DE NON-CONTREFAÇON. ISTORAGE NE GARANTIT PAS QUE LE PRODUIT FONCTIONNERA SANS ERREUR. DANS LA MESURE OÙ DES GARANTIES IMPLICITES PEUVENT NÉANMOINS EXISTER EN VERTU DE LA LOI, CES GARANTIES SONT LIMITÉES À LA DURÉE DE LA PRÉSENTE GARANTIE. LA RÉPARATION OU LE REMPLACEMENT DE CE PRODUIT, TEL QUE PRÉVU DANS LE PRÉSENT DOCUMENT, EST VOTRE SEUL RECOURS.

EN AUCUN CAS ISTORAGE NE POURRA ÊTRE TENU RESPONSABLE DE TOUTE PERTE OU DE TOUT PROFIT ANTICIPÉ, OU DE TOUT DOMMAGE ACCESSOIRE, PUNITIF, EXEMPLAIRE, SPÉCIAL, DE CONFIANCE OU CONSÉCUTIF, Y COMPRIS, MAIS SANS S'Y LIMITER, LES PERTES DE REVENUS, DE PROFITS, D'UTILISATION DE LOGICIELS, DE DONNÉES, TOUTE AUTRE PERTE OU RÉCUPÉRATION DE DONNÉES, LES DOMMAGES AUX BIENS ET LES RÉCLAMATIONS DE TIERS, DÉCOULANT DE TOUTE THÉORIE DE RÉCUPÉRATION, Y COMPRIS LA GARANTIE, LE CONTRAT, LA LOI OU LE DÉLIT, QU'IL AIT ÉTÉ OU NON INFORMÉ DE LA POSSIBILITÉ DE TELS DOMMAGES. NONOBSTANT LA DURÉE DE TOUTE GARANTIE LIMITÉE OU DE TOUTE GARANTIE IMPLICITE PRÉVUE PAR LA LOI, OU DANS LE CAS OÙ UNE GARANTIE LIMITÉE NE REMPLIRAIT PAS SON OBJECTIF ESSENTIEL, LA RESPONSABILITÉ TOTALE D'ISTORAGE NE DÉPASSERA EN AUCUN CAS LE PRIX D'ACHAT DU PRÉSENT
PRODUIT. | 4823-2548-5683.3

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, Angleterre
Tél. : +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com

iStorage®

DISKASHUR® 3 und DISKASHUR® PRO 3

Benutzerhandbuch

Dieses Benutzerhandbuch gilt sowohl für den diskAshur³ als auch für den diskAshur PRO³. Beide Produkte werden im Folgenden als diskAshur³ bezeichnet.

Bitte stellen Sie sicher, dass Sie sich Ihre PIN (Passwort) merken. Ohne die PIN gibt es keine Möglichkeit, auf die Daten auf dem Laufwerk zuzugreifen.

Wenn Sie Probleme bei der Verwendung Ihres diskAshur³ haben, kontaktieren Sie bitte unser Support-Team per E-Mail – support@istorage-uk.com oder telefonisch unter +44 (0) 20 8991 6260.

RoHS Compliant

REACH COMPLIANCE

Konform mit dem Trade Agreements Act (TAA)

Inhaltsverzeichnis

Einführung 87
Verpackungsinhalt 87
diskAshur³-Layout 87
1. LED-Anzeigen und ihre Funktionen 88
2. LED-Zustände 88
3. Erstmalige Verwendung 89
4. Entsperren des diskAshur³ mit der Admin-PIN 90
5. Wechsel in den Admin-Modus 90
6. Ändern der Admin-PIN 91
7. Einstellen einer Benutzer-PIN-Richtlinie 92
8. Löschen der Benutzer-PIN-Richtlinie 93
9. Überprüfen der Benutzer-PIN-Richtlinie 93
10. Hinzufügen einer neuen Benutzer-PIN im Admin-Modus 94
11. Ändern der Benutzer-PIN im Admin-Modus 95
12. Löschen der Benutzer-PIN im Admin-Modus 95
13. Entsperren des diskAshur³ mit der Benutzer-PIN 96
14. Ändern der Benutzer-PIN im Benutzermodus 96
15. Einschalten des beleuchteten LED-Tastenfelds 97
16. Ausschalten des beleuchteten LED-Tastenfelds 97
17. Erstellen einer einmaligen Benutzerwiederherstellungs-PIN 98
18. Löschen der einmaligen Benutzerwiederherstellungs-PIN 98
19. Aktivieren des Wiederherstellungsmodus und Erstellen einer neuen Benutzer-PIN 99
20. Einstellen des schreibgeschützten Benutzerzugriffs im Admin-Modus 99
21. Aktivieren des Lese-/Schreibzugriffs für Benutzer im Admin-Modus 100
22. Einstellen des globalen Lese-/Schreibzugriffs im Admin-Modus 100
23. Aktivieren des globalen Lese-/Schreibzugriffs im Admin-Modus 101
24. Konfigurieren einer Selbstzerstörungs-PIN 101
25. Löschen der Selbstzerstörungs-PIN 102
26. Entsperren mit der Selbstzerstörungs-PIN 102
27. Konfigurieren einer Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung 103
28. Einstellen von „Automatische Sperre, wenn unbeaufsichtigt“ 103
29. Deaktivieren von „Automatische Sperre, wenn unbeaufsichtigt“ 104
30. Überprüfen von „Automatische Sperre, wenn unbeaufsichtigt“ 105
31. Einstellen des schreibgeschützten Zugriffs im Benutzermodus 105
32. Aktivieren des Lese-/Schreibzugriffs im Benutzermodus 106
33. Abwehrmechanismus gegen Brute-Force-Hacker-Angriffe 106
34. Einstellen der Brute-Force-Beschränkung für die Benutzer-PIN 107
35. Überprüfen der Brute-Force-Beschränkung für die Benutzer-PIN 108
36. Durchführen einer kompletten Rücksetzung 109
37. Konfigurieren der Bootfähigkeitsfunktion des diskAshur³ 109
38. Deaktivieren der Bootfähigkeitsfunktion des diskAshur³ 110
39. Überprüfen der Bootfähigkeitseinstellung 110
40. Konfigurieren des Verschlüsselungsmodus 111
41. Überprüfen des Verschlüsselungsmodus 112
42. Konfigurieren des Datenträgertyps 113
43. Überprüfen der Datenträgertyp-Einstellung 113
44. Initialisierung und Formatierung des diskAshur³ für Windows 114
45. Initialisierung und Formatierung des diskAshur³ unter Mac OS 116
46. Initialisierung und Formatierung des diskAshur³ unter Linux OS 118
47. Ruhezustand, Anhalten oder Abmelden vom Betriebssystem 121
48. Überprüfen der Firmware im Admin-Modus 121
49. Überprüfen der Firmware im Benutzermodus 122
50. Technischer Support 123
51. Garantie- und RMA-Informationen 123

Einführung

Vielen Dank, dass Sie sich für den Kauf des neuen iStorage diskAshur³/ diskAshur PRO³ entschieden haben. Beide Produkte werden im Folgenden als „diskAshur³“ bezeichnet.

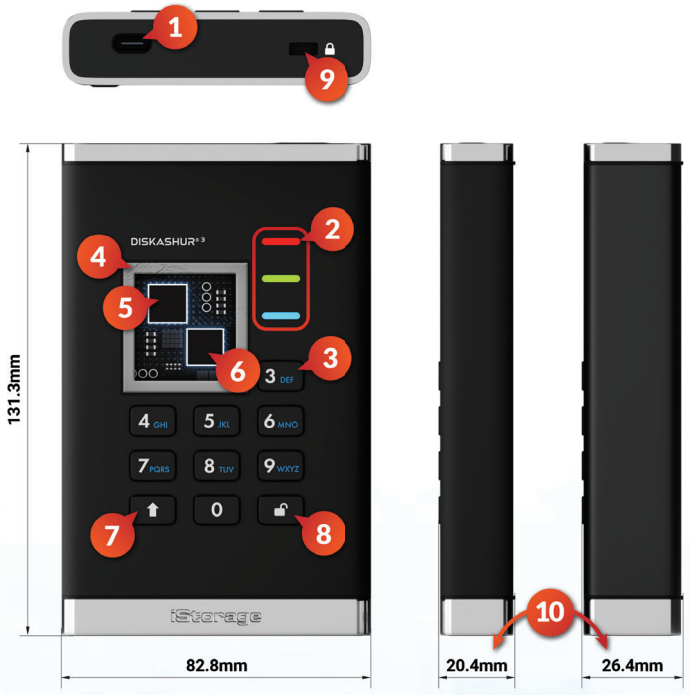
Der diskAshur³ ist eine einfach zu verwendende, ultrasichere, passwortgeschützte und tragbare HDD/SSD-Festplatte mit Hardwareverschlüsselung und Kapazitäten von bis zu 5 TB (HDD) bzw. bis zu 16 TB (SSD) und mehr. Der diskAshur³ verschlüsselt Daten während der Übertragung und im Ruhezustand mit einer 256-Bit-Hardwareverschlüsselung.

Der diskAshur3 verfügt über einen nach Common Criteria EAL 5+ zertifizierten sicheren Mikroprozessor mit integrierten physischen Schutzmechanismen, die vor externen Manipulationen, Umgehungsangriffen und Fehlerinjektionen schützen. Im Gegensatz zu anderen Lösungen reagiert der diskAshur³ auf einen automatisierten Angriff, indem er in den Deadlock-Zustand wechselt (einfriert), sodass alle derartigen Angriffe vergeblich sind. Einfach ausgedrückt: Ohne PIN ist kein Zugriff möglich!

Verpackungsinhalt

- iStorage diskAshur³
- Schutztragetasche
- USB-Kabel (Typ C und A)
- Kostenlose 1-jährige Lizenz für Nero BackIt-Up und iStorage DriveSecurity
- Schnellanleitung

Aufbau des diskAshur³



1. USB 3,2 (Gen 1) Typ-C-Schnittstelle
   USB-Kabel des Typs C und des Typs A sind enthalten.
2. LED-Leuchten
   ROT - Gesperrt/Standby-Modus. DURCHGEHEND GRÜN– Entsperrt BLINKT GRÜN – Datenübertragung BLAU – Admin-Modus
3. Epoxidbeschichtetes, verschleißfestes, hintergrundbeleuchtetes (vom Benutzer wählbar), alphanumerisches Tastenfeld.
4. Manipulationsgeschütztes Design, das zudem Manipulationsversuche sichtbar macht *Alle wichtigen Komponenten sind mit äußerst widerstandsfähigem Epoxidharz beschichtet.*
5. Crypto-Chip im Gerät
6. Geräteinterner, nach Common Criteria EAL 5+ zertifizierter sicherer Mikroprozessor
7. UMSCHALT-Taste
8. ENTSPERREN-Taste
9. Anschluss für Kensington-Schloss
10. Die Tiefe des 4TB&5TB HDD-Laufwerks beträgt 26,8 mm anstatt 20,8 mm.

1. LED-Anzeigen und ihre Aktionen

LED	LED-Zustand	Beschreibung	LED	LED-Zustand	Beschreibung
	ROT Dauerlicht	Gesperrter Datenträger (entweder im **Standby-** oder im **Zurücksetz-**Status)		BLAU Dauerlicht	Datenträger im **Admin-Modus**
	ROT Doppelblinken	Falsche PIN-Eingabe		ROT, GREEN und BLAU blinken gleichzeitig	Wartet auf die Eingabe der **Benutzer-**PIN
	GRÜN leuchtet durchgehend	Datenträger **entsperrt**		GREEN und BLAU blinken gleichzeitig	Warten auf Eingabe der **Admin**-PIN
	GRÜN blinkt	Datenübertragung erfolgt			

2. LED-Zustände

Aktivieren aus dem Ruhezustand

Der Ruhezustand ist als der Zustand definiert, in dem der Datenträger nicht verwendet wird und alle LEDs erloschen sind.

Um den diskAshur³ aus dem Ruhezustand zu aktivieren, gehen Sie wie folgt vor:

Verbinden Sie den Datenträger mit einem stromführenden USB-Anschluss an Ihrem Computer		Eine durchgehend ROT leuchtende LED zeigt an, dass sich der Datenträger im Standby-Modus befindet.

Wechseln in den Ruhezustand

Um den diskAshur³ in den Ruhezustand zu versetzen, führen Sie eine der folgenden Aktionen aus:

- Werfen Sie den Datenträger aus und trennen Sie ihn von Ihrem Computer. Die ROTE LED erlischt (Ruhezustand).

Eingeschaltete Zustände

Nach dem Aktivieren aus dem Ruhezustand wechselt der Datenträger in einen in der nachstehenden Tabelle aufgeführten Zustand.

Eingeschalteter Zustand	LED-Anzeige	Verschlüsselungsschlüssel	Admin-PIN	Beschreibung
Auslieferungsstatus	ROT und GRÜN – Dauerlicht	✓	×	Wartet auf die Konfiguration einer Admin-PIN (erstmalige Verwendung)
Standby	ROT – Dauerlicht	✓	✓	Wartet auf die Eingabe der Admin-, Benutzer- oder Wiederherstellungs-PIN
Rücksetzung	ROT – Dauerlicht	×	×	Wartet auf die Konfiguration einer Admin-PIN

3. Erstmalige Verwendung

Der iStorage diskAshur³ wird im Auslieferungszustand ohne voreingestellte **Admin-PIN** geliefert. Bevor der Datenträger verwendet werden kann, muss eine **8–64**-stellige Admin-PIN konfiguriert werden. Sobald eine Admin-PIN erfolgreich konfiguriert wurde, kann der Datenträger nicht mehr in den „Auslieferungszustand“ versetzt werden.

PIN-Anforderungen:

- Muss zwischen 8 und 64 Stellen lang sein
- Darf nicht ausschließlich sich wiederholende Ziffern enthalten, wie z. B. (3-3-3-3-3-3-3-3)
- Darf nicht ausschließlich sequenzielle Ziffern enthalten, z. B. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- Die UMSCHALT-Taste kann für zusätzliche Kombinationen verwendet werden z. B.(**UMSCHALTEN** (⬆) **+ 1** ergibt einen anderen Wert als nur 1.

Passwort-Tipp: Sie können einen einprägsamen Begriff, Namen, Ausdruck oder eine andere alphanumerische PIN-Kombination erstellen, indem Sie einfach die Tasten mit den entsprechenden Buchstaben drücken.

Beispiele für alphanumerische PINs sind:

- Für „**Password**“ drücken Sie die folgenden Tasten:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Für „**iStorage**“ drücken Sie die folgenden Tasten:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Mit dieser Methode können lange und einfach zu merkende PINs konfiguriert werden.

Um eine Admin-PIN zu konfigurieren und den diskAshur³ erstmalig zu entsperren, befolgen Sie bitte die einfachen Schritte in der nachstehenden Tabelle.

Anweisungen – erstmalige Verwendung	LED	LED-Status
1. Schließen Sie den diskAshur³ an einen stromführenden USB-Anschluss Ihres Computers an.		Die ROTE und die GRÜNE LED leuchten durchgehend und zeigen an, dass sich der Datenträger im Auslieferungszustand befindet.
2. Halten Sie die Tasten **Entsperren (🔓) und 1** gedrückt.		Die GRÜNE LED blinkt und die BLAUE LED leuchtet durchgehend.
3. Geben Sie eine **neue Admin-PIN** (8–64 Ziffern) ein und drücken Sie einmal die Taste **Entsperren (🔓)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED zuerst zu einer blinkenden GRÜNEN LED und dann wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
4. Geben Sie Ihre **neue Admin-PIN** erneut ein und drücken Sie einmal die Taste **Entsperren (🔓)**		Die BLAUE LED blinkt schnell. Die Anzeige wechselt dann zu einer durchgehend leuchtenden BLAUEN und schließlich zu einer durchgehend leuchtenden GRÜNEN LED. Damit wird angezeigt, dass die Admin-PIN erfolgreich konfiguriert wurde und der Datenträger entsperrt und einsatzbereit ist.

Sperren des diskAshur³

Um den Datenträger zu sperren, werfen Sie ihn sicher aus Ihrem Host-Betriebssystem aus und ziehen Sie dann den Stecker vom USB-Anschluss ab. Wenn gerade Daten auf den Datenträger geschrieben werden, führt das Auswerfen des diskAshur³ zu einer unvollständigen Datenübertragung und zu einer möglichen Datenbeschädigung.

4.Entsperren des diskAshur³ mit der Admin-PIN

Um den diskAshur³ mit der Admin-PIN zu entsperren, befolgen Sie bitte die einfachen Schritte in der nachstehenden Tabelle.

1. Schließen Sie den diskAshur³ an einen USB-Anschluss Ihres Computers an.		Eine durchgehend ROT leuchtende LED zeigt an, dass sich der Datenträger im Standby-Modus befindet.
2. Drücken Sie im Standby-Modus ROTE LED leuchtet durchgehend) einmal die Taste **Entsperren (🔓)**		Die GRÜNE und die BLAUE LED blinken gleichzeitig.
3. Wenn die GRÜNE und die BLAUE LED gleichzeitig blinken, geben Sie Ihre Admin-PIN ein und drücken Sie einmal die Taste **Entsperren (🔓)**		Die GRÜNE LED blinkt mehrmals und leuchtet dann durchgehend GRÜN. Damit wird angezeigt, dass der Datenträger erfolgreich mit der Admin-PIN entsperrt wurde und betriebsbereit ist.

5. Wechsel in den Admin-Modus

Um in den Admin-Modus zu wechseln, gehen Sie wie folgt vor:

1. Schließen Sie den diskAshur³ an einen stromführenden USB-Anschluss Ihres Computers an.		Eine durchgehend ROT leuchtende LED zeigt an, dass sich der Datenträger im Standby-Modus befindet.
2. Halten Sie im Standby-Modus (ROTE LED leuchtet durchgehend) die Tasten **Entsperren (🔓) und 1** gedrückt.		Die GRÜNE und die BLAUE LED blinken gleichzeitig.
3. Geben Sie Ihre Admin-PIN ein und drücken Sie einmal die Taste Entsperren **(🔓)**		Die BLAUELED leuchtet durchgehend. Damit wird angezeigt, dass sich der Datenträger im Admin-Modus befindet.

Beenden des Admin-Modus

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

6. Ändern der Admin-PIN

PIN-Anforderungen:

- Muss zwischen 8 und 64 Ziffern lang sein
- Darf nicht nur sich wiederholende Zahlen enthalten, z. B. (3-3-3-3-3-3-3-3)
- Darf nicht nur aufeinanderfolgende Zahlen enthalten, z. B. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- Die UMSCHALT-Taste kann für zusätzliche Kombinationen verwendet werden z. B.(**UMSCHALTEN** (⬆) **+ 1** ergibt einen anderen Wert als nur 1.

Passwort-Tipp: Sie können ein einprägsames Wort, einen Namen, einen Satz oder eine beliebige andere alphanumerische PIN-Kombination konfigurieren, indem Sie einfach die Taste mit den entsprechenden Buchstaben drücken.

Beispiele für solche alphanumerischen PINs sind:

- Drücken Sie für **„Passwort“** die folgenden Tasten:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **8** (tuv)
- Drücken Sie für **„iStorage“** die folgenden Tasten:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Mit dieser Methode können Sie lange PINs konfigurieren, die man sich dennoch leicht merken kann.

Um die Admin-PIN zu ändern, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **SCHLÜSSEL-Taste (🔓)** und die **2**		Die durchgehend BLAUE LED schaltet zur blinkend GRÜNEN und durchgehend BLAUEN LEDs
2. Geben Sie die **NEUE Admin-PIN** ein und drücken Sie dann die **SCHLÜSSEL**-Taste **(🔓)** einmal		Die blinkende GRÜNE und durchgehend BLAUE LED schalten zu einer GRÜN blinkenden LED und schließlich wieder zu einer blinkenden GRÜNEN und einer durchgehend BLAUEN LED
3. Geben Sie die **NEUE Admin-PIN** erneut ein und drücken Sie dann die **SCHLÜSSEL**-Taste **(🔓)** einmal		Die blinkend GRÜNE und durchgehend BLAUE LED wechseln zu einer schnell blinkenden BLAUEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, dass die Admin-PIN erfolgreich geändert wurde

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

7. Festlegen einer Benutzer-PIN-Richtlinie

Der Administrator kann eine einschränkende Richtlinie für die Benutzer-PIN festlegen. Diese Richtlinie umfasst die Festlegung der Mindestlänge der PIN (8 bis 64 Ziffern) sowie die Anforderung, ein oder mehrere **„Sonderzeichen“** einzugeben bzw. nicht. Das „Sonderzeichen“ steht für eine der **Zifferntasten**, die zusammen mit der **UMSCHALT**-Taste (⬆) gedrückt werden.

Um eine Benutzer-PIN-Richtlinie (Einschränkungen) festzulegen, müssen Sie 3 Ziffern eingeben. In der Ziffernfolge **„091“** geben zum Beispiel die ersten beiden Ziffern (**09**) die Mindestlänge der PIN an (in diesem Fall 9) und die letzte Ziffer (**1**) gibt an, dass ein oder mehrere „Sonderzeichen“ verwendet werden müssen, also: **„UMSCHALT (⬆) + Ziffer“**. Ganz ähnlich kann eine Benutzer-PIN-Richtlinie so festgelegt werden, dass kein „Sonderzeichen“ erforderlich ist. Bei **„120“** geben etwa die ersten beiden Ziffern (**12**) die Mindestlänge der PIN an (in diesem Fall **12**) und die letzte Ziffer (**0**) gibt an, dass kein Sonderzeichen erforderlich ist.

Sobald der Administrator die Benutzer-PIN-Richtlinie festgelegt hat, zum Beispiel „**091**“, muss eine neue Benutzer-PIN konfiguriert werden – siehe Abschnitt 10, „Hinzufügen einer neuen Benutzer-PIN im Admin-Modus“ Wenn der Administrator die Benutzer-PIN als **„247688314“** unter Verwendung eines **„Sonderzeichens“ (UMSCHALT-Taste (⬆) +** gleichzeitig gedrückte **Ziffern-**Taste) konfiguriert, kann dies während des Erstellungsprozesses der Benutzer-PIN an einer beliebigen Stelle Ihrer 8-64-stelligen PIN platziert werden, wie in den folgenden Beispielen gezeigt.

A. „**UMSCHALT** (⬆) **+ 2**“, „4“, „7“, „6“, „8“, „8“, „3“, „1“, „4“,

B. „2“, „4“, „**UMSCHALT** (⬆) **+ 7**“, „6“, „8“, „8“, „3“, „1“, „4“,

C. „2“, „4“, „7“, „6“, „8“, „8“, „3“, „1“, „**UMSCHALT** (⬆) **+ 4**“,

Anmerkung:

- Wenn bei der Konfiguration der Benutzer-PIN ein „Sonderzeichen“ verwendet wurde, z. B. Option „**B**“ oben, dann kann das Laufwerk nur durch Eingabe der PIN mit dem „Sonderzeichen“ entriegelt werden, und zwar genau in der konfigurierten Reihenfolge des obigen Beispiels „**B**“ – („2“, „4“, „**SHIFT** (⬆) **+ 7**“, „6“, „8“, „8“, „3“, „1“, „4“).
- Es kann mehr als ein „Sonderzeichen“ verwendet und in Ihrer 8-64-stelligen PIN platziert werden.
- Benutzer können ihre PIN ändern, sind aber gezwungen, die festgelegten „Benutzer-PIN-Richtlinie“ (Einschränkungen) einzuhalten, falls und soweit zutreffend.
- Das Einstellen einer neuen Benutzer-PIN-Richtlinie löscht automatisch die Benutzer-PIN, falls diese existiert.
- Diese Richtlinie gilt nicht für die „Selbstzerstörungs-PIN“. Die Komplexitätseinstellung für die Selbstzerstörungs-PIN und die Admin-PIN beträgt immer 8-64 Ziffern, wobei kein Sonderzeichen erforderlich ist.

Um die Benutzer-PIN-Richtlinie zu ändern, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **SCHLÜSSEL- (🔓) und die 7-**Taste gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Geben Sie Ihre **3 Ziffern** ein und bedenken Sie daran, dass die ersten beiden Ziffern die Mindestlänge der PIN angibt und die letzte Ziffer (0 oder 1) festlegt, ob ein Sonderzeichen verwendet wird.		Die blinkende GRÜNE und BLAUE LED blinkt weiter
3. Drücken Sie die **UMSCHALT-Taste** (⬆) einmal		Die blinkende GRÜNE und BLAUE LED wechselt zu einer durchgehend GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, dass die Benutzer-PIN-Richtlinie erfolgreich eingestellt wurde.

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

8. Löschen der Benutzer-PIN-Richtlinie

Um die **Benutzer-PIN-Richtlinie** zu löschen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus**befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **Entsperren (🔓) und 7** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **080** ein und drücken Sie einmal die **UM SCHALT**-Taste (⬆)		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass die Benutzer-PIN-Richtlinie erfolgreich gelöscht wurde.

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

9. Überprüfen der Benutzer-PIN-Richtlinie

Der Administrator hat die Möglichkeit, die Benutzer-PIN-Richtlinie zu überprüfen und kann abfragen, welche minimale Länge die PIN haben muss, und ob die Verwendung eines Sonderzeichens festgelegt wurde oder nicht, indem er oder sie die LED-Sequenz wie unten beschrieben beobachtet.

Um die Benutzer-PIN-Richtlinie zu überprüfen, wechseln Sie zunächst in den **„Admin-Modus“**, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **UMSCHALT-Taste (⬆) und die 7** gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** und Folgendes geschieht; a. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend. b. Jedes Blinken der ROTEN LED entspricht zehn (10) Stellen einer PIN. c. Jedes Blinken der GRÜNEN LED entspricht einer (1) Stelle einer PIN d. Ein Blinken der BLAUEN LED zeigt an, dass ein „Sonderzeichen“ verwendet wurde. e. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend. f. LEDs schalten zu einem durchgehenden BLAU zurück		

Die folgende Tabelle beschreibt die Signale der LED bei der Überprüfung der Benutzer-PIN-Richtlinie. Wenn Sie z. B. eine 12-stellige Benutzer-PIN mit einem Sonderzeichen (**121**), festgelegt haben, blinkt die ROTE LED einmal (**1**), die GRÜNE LED blinkt zweimal (**2**) und die BLAUE LED blinkt einmal (**1**), um anzuzeigen, dass ein **Sonderzeichen** verwendet werden muss.

PIN-Beschreibung	3-Ziffern-Wert	ROT	GRÜN	BLAU
12-stellige PIN mit einem Sonderzeichen	121	1-faches Blinken	2-faches Blinken	1-faches Blinken
12-stellige PIN OHNE Sonderzeichen	120	1-faches Blinken	2-faches Blinken	0
9-stellige PIN mit einem Sonderzeichen	091	0	9-faches Blinken	1-faches Blinken
9-stellige PIN OHNE Sonderzeichen	090	0	9-faches Blinken	0

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

10. Hinzufügen einer neuen Benutzer-PIN im Admin-Modus

Wichtig: Eine neue Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ erstellt werden, wenn eine solche Richtlinie wie in Abschnitt 7 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie legt die PIN-Mindestlänge fest und ob ein „Sonderzeichen“ verwendet wurde. Der Administrator kann zur Überprüfung der Benutzer-PIN-Beschränkungen Abschnitt 9 zu Rate ziehen.

PIN-Anforderungen:

- Muss zwischen 8 und 64 Ziffern lang sein
- Darf nicht nur sich wiederholende Zahlen enthalten, z. B. (3-3-3-3-3-3-3-3)
- Darf nicht nur aufeinanderfolgende Zahlen enthalten, z. B. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- Die **UMSCHALT**-Taste (⬆) kann für zusätzliche PIN-Kombinationen verwendet werden – z. B. ist **UMSCHALT** (⬆) **+ 1** ein anderer Wert als einfach nur 1. Siehe Abschnitt 7, „Festlegen einer Benutzer-PIN-Richtlinie“.

Um eine **neue Benutzer-PIN** hinzuzufügen, wechseln Sie zunächst in den **„Admin-Modus“**, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **SCHLÜSSEL**- **(🔓)** und die 3-Taste gleichzeitig gedrückt		Die durchgehend BLAUE LED schaltet zur blinkend GRÜNEN und durchgehend BLAUEN LEDs
2. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔓)**		Die blinkende GRÜNE und durchgehend BLAUE LED schalten zu einer GRÜN blinkenden LED und schließlich wieder zu einer blinkenden GRÜNEN und einer durchgehend BLAUEEN LED
3. Geben Sie Ihre **neue Benutzer-PIN** erneut ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** erneut		Die blinkend GRÜNE und durchgehend BLAUE LED wechseln zu einer schnell blinkenden GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED, die angeben, dass erfolgreich eine neue Benutzer-PIN eingestellt wurde

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

11. Ändern der Benutzer-PIN im Admin-Modus

Wichtig: Das Ändern der Benutzer-PIN muss mit der „Benutzer-PIN-Richtlinie“ übereinstimmen, wenn eine solche wie in Abschnitt 7 beschrieben konfiguriert wurde. Darin wird die Mindestlänge der PIN und die Verwendung von „Sonderzeichen“ festgelegt. In Abschnitt 9 kann der Administrator erfahren, wie die Einschränkungen der Benutzer-PIN überprüft werden können.

Um eine bestehende **Benutzer-PIN** zu ändern, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **SCHLÜSSEL**- **(🔓) und die 3**-Taste gleichzeitig gedrückt		Die durchgehend BLAUE LED schaltet zur blinkend GRÜNEN und durchgehend BLAUEN LEDs
2. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔓)**		Die blinkende GRÜNE und durchgehend BLAUE LED schalten zu einer GRÜN blinkenden LED und schließlich wieder zu einer blinkenden GRÜNEN und einer durchgehend BLAUEN LED
3. Geben Sie Ihre **neue Benutzer-PIN** erneut ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** einmal		Die blinkend GRÜNE und durchgehend BLAUE LED wechseln zu einer schnell blinkenden GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, dass die Benutzer-PIN erfolgreich geändert wurde

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

12. Löschen der Benutzer-PIN im Admin-Modus

Um eine bestehende **Benutzer-PIN** zu löschen, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **UMSCHALT-Taste** (⬆) und die **3** gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zur blinkenden ROTEN LED
2. Drücken und halten Sie die **UMSCHALT**-Taste (⬆) und die **3** gleichzeitig gedrückt		Die blinkende ROTE LED wechselt zu einer durchgehend ROTEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, dass die Benutzer-PIN erfolgreich gelöscht wurde

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

13. Entsperren des diskAshur³ mit der Benutzer-PIN

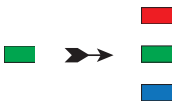
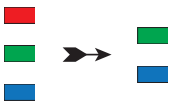
Um den diskAshur³ mit der **Benutzer-PIN** zu entsperren, führen Sie die folgenden Schritte aus:

1. Halten Sie im Standby-Modus (ROTE LED leuchtet durchgehend) die Tasten **UMSCHALTEN (🔓)und Entsperren (🔓)** gedrückt.		Anstatt der ROTEN LED leuchten alle LEDs auf (ROT, GRÜN und BLAU) und blinken abwechselnd.
2. Geben Sie die **Benutzer-PIN** ein und drücken Sie einmal die Taste **Entsperren (🔓)**		Die Anzeige wechselt von einer blinkenden ROTEN, einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zuerst zu einer blinkenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden GRÜNEN LED. Damit wird angezeigt, dass der Datenträger erfolgreich im Benutzermodus entsperrt wurde.

14. Ändern der Benutzer-PIN im Benutzermodus

Wichtig: Wenn die Benutzer-PIN im Benutzermodus (GRÜNE LED) geändert wird, muss diese Änderung mit der „Benutzer-PIN-Richtlinie" übereinstimmen, falls eine solche wie in Abschnitt 7 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie legt die PIN-Mindestlänge fest und ob ein „Sonderzeichen" verwendet wurde.

Um die **Benutzer-PIN** zu ändern, entsperren Sie zuerst den diskAshur³ mit der Benutzer-PIN wie in Abschnitt 13 beschrieben. Wenn sich der Datenträger im **Benutzermodus** befindet (GRÜNE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Benutzermodus (GRÜNE LED) die Tasten **Entsperren (🔓) und 4** gedrückt.		Anstatt der durchgehend leuchtenden GRÜNEN LED leuchten alle LEDs auf (ROT, GRÜN und BLAU) und blinken abwechselnd.
2. Geben Sie Ihre **bestehende Benutzer-PIN** ein und drücken Sie einmal die **Taste** Entsperren **(🔓)** .		Die LED-Anzeige wechselt zu einer blinkenden GRÜNEN LED und dann wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie einmal **die Taste** Entsperren **(🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN LED und dann wieder zurück zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
4. Geben Sie die neue Benutzer-PIN erneut ein und drücken Sie einmal die Taste Entsperren **(🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zuerst zu einer schnell blinkenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden GRÜNEN LED. Damit wird angezeigt, dass die Benutzer-PIN erfolgreich geändert wurde.

15. Einschalten des beleuchteten LED-Tastenfelds

Für eine bessere Sichtbarkeit bei schlechten Lichtverhältnissen wurde der diskAshur³ mit einem beleuchteten LED-Tastenfeld ausgestattet.Um das beleuchtete LED-Tastenfeld einzuschalten, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **2 und 6** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie die Taste Entsperren **(🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und dann zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass das beleuchtete Tastenfeld aktiviert wurde. Es wird eingeschaltet, sobald der Datenträger das nächste Mal an einen stromführenden USB-Anschluss angeschlossen wird.

Hinweis: Nachdem Sie den diskAshur³ so eingestellt haben, dass die Beleuchtung des LED-Tastenfelds eingeschaltet ist, müssen Sie den Datenträger zur Aktivierung zuerst vom stromführenden USB-Anschluss trennen und dann wieder anschließen. Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

16. Ausschalten des beleuchteten LED-Tastenfelds

Um das beleuchtete LED-Tastenfeld auszuschalten, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus**befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **2 und 3** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie die Taste Entsperren **(🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und dann zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass das beleuchtete Tastenfeld deaktiviert wurde. Es wird ausgeschaltet, sobald der Datenträger das nächste Mal an einen stromführenden USB-Anschluss angeschlossen wird.

Hinweis: Nachdem Sie den diskAshur³ so eingestellt haben, dass die Beleuchtung des LED-Tastenfelds ausgeschaltet ist, müssen Sie den Datenträger zur Aktivierung zuerst vom stromführenden USB-Anschluss trennen und dann wieder anschließen. Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

17. Erstellen einer einmaligen Benutzerwiederherstellungs-PIN

Die Benutzerwiederherstellungs-PIN ist sehr nützlich in Situationen, in denen ein Benutzer seine PIN zum Entsperren des diskAshur³ vergessen hat. Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zuerst die richtige einmalige Wiederherstellungs-PIN eingeben, sofern eine solche konfiguriert wurde. Der Benutzer-PIN-Wiederherstellungsprozess hat keine Auswirkungen auf die Daten, den Verschlüsselungsschlüssel und die Admin-PIN. Allerdings muss der Benutzer eine neue 8–64-stellige Benutzer-PIN konfigurieren.

Um eine einmalige 8–64-stellige Benutzerwiederherstellungs-PIN zu konfigurieren, müssen Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“ wechseln. Wenn sich der Datenträger im **Admin-Modus**befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **Entsperren (🔓) und 4** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
2. Geben Sie eine **einmalige Wiederherstellungs-PIN** ein und drücken Sie die Taste **Entsperren (🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN LED und dann wieder zurück zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie Ihre **einmalige Wiederherstellungs-PIN** erneut ein und drücken Sie erneut die Taste **Entsperren (🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED zu einer schnell blinkenden GRÜNEN und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass die einmalige Wiederherstellungs-PIN erfolgreich konfiguriert wurde.

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste **(🔓)** eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

18. Löschen der einmaligen Benutzerwiederherstellungs-PIN

Um die einmalige Benutzerwiederherstellungs-PIN zu löschen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus**befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTEN** (⬆) **und 4** gedrückt		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden ROTEN LED.
2. Halten Sie erneut die Tasten **UMSCHALTEN** (⬆) **und 4** gedrückt		Die Anzeige wechselt von einer blinkenden ROTEN LED zuerst zu einer durchgehend leuchtenden ROTEN LED und dann zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass die einmalige Benutzerwiederherstellungs-PIN erfolgreich gelöscht wurde.

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste **(🔓)** eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

19. Aktivieren des Wiederherstellungsmodus und Erstellen einer neuen Benutzer-PIN

Die Benutzerwiederherstellungs-PIN ist sehr nützlich in Situationen, in denen ein Benutzer seine PIN zum Entsperren des diskAshur³ vergessen hat. Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zuerst die richtige einmalige Wiederherstellungs-PIN eingeben, sofern eine solche konfiguriert wurde. Der Benutzer-PIN-Wiederherstellungsprozess hat keine Auswirkungen auf die Daten, den Verschlüsselungsschlüssel und die Admin-PIN. Allerdings muss der Benutzer eine neue 8–64-stellige Benutzer-PIN konfigurieren.

Führen Sie zum Aktivieren des Wiederherstellungsprozesses und zum Konfigurieren einer neuen Benutzer-PIN die folgenden Schritte aus:

1. Halten Sie im **Standby-Modus** (ROTE LED) die Tasten **Entsperren (🔓) und 4** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden ROTEN LED zu einer blinkenden ROTEN und einer blinkenden GRÜNENLED.
2. Geben Sie die einmalige **Wiederherstellungs-PIN** ein und drücken Sie die Taste **Entsperren (🔓)**		Die GRÜNEund BLAUE LED blinken abwechseln. Dann wechselt die Anzeige zuerst zu einer durchgehend leuchtenden GRÜNEN LED und schließlich zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie eine neue Benutzer-PIN ein und drücken Sie die Taste Entsperren **(🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED zunächst zu einer blinkenden GRÜNEN LED und dann wieder zu einer blinkendenGRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
4. Geben Sie Ihre neue Benutzer-PIN erneut ein und drücken Sie erneut die Taste Entsperren **(🔓)**		Die GRÜNE LED blinkt schnell und leuchtet dann durchgehend GRÜN. Damit wird angezeigt, dass der Wiederherstellungsprozess erfolgreich durchgeführt und eine neue Benutzer-PIN konfiguriert wurde.

Wichtig: Eine neue Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ erstellt werden, wenn eine wie in Abschnitt 7 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie legt die PIN-Mindestlänge fest und ob ein „Sonderzeichen“ verwendet wurde. Siehe Abschnitt 9 für die Überprüfung von Benutzer-PIN-Beschränkungen.

20. Einstellen des schreibgeschützten Benutzerzugriffs im Admin-Modus

Es gibt unzählige Viren und Trojaner, mit denen USB-Datenträger infiziert werden können. Deshalb ist die Schreibschutzfunktion besonders nützlich, wenn Sie in einem öffentlichen Raum auf die Daten auf dem USB-Datenträger zugreifen müssen. Es ist auch eine grundlegende Funktion für forensische Zwecke, wenn die Daten in ihrem ursprünglichen und unveränderten Zustand, der nicht modifiziert oder überschrieben werden darf, bewahrt werden müssen.

Wenn der Administrator den diskAshur³ konfiguriert und den Benutzerzugriff auf den schreibgeschützten Zugriff beschränkt, kann nur der Administrator auf den Datenträger schreiben oder die Einstellung wie in Abschnitt 21 beschrieben wieder in „Lesen/Schreiben“ ändern. Der Benutzer ist auf den schreibgeschützten Zugriff beschränkt und kann weder auf den Datenträger schreiben noch diese Einstellung im Benutzermodus ändern.

Um den diskAshur³ entsprechend einzustellen und den Benutzerzugriff auf den schreibgeschützten Zugriff zu beschränken, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus**befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Drücken und halten Sie im Admin-Modus die Tasten „**7 + 6**“.		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** einmal		Die GRÜNE und BLAUE LED schalten auf eine durchgehend GRÜNE LED und dann zu einer durchgehend BLAUEN LED, die anzeigt, dass das Laufwerk konfiguriert wurde und den Benutzerzugriff auf Lesezugriff einschränkt

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

21. Benutzer auf Lese-/Schreibzugriff im Admin-Modus einstellen

Um den diskAshur³ so einzustellen, dass der Benutzerzugriff als Lese-/Schreibzugriff aktiviert ist, gehen Sie zuerst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald das Laufwerk im **Admin-Modus** (durchgehend BLAUE LED) ist, fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die Tasten „**7 + 9**“.		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** einmal		Die GRÜNE und BLAUE LED wechseln zu einer durchgehend GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED. So wird angezeigt, dass das Laufwerk für Lese-/Schreibzugriff konfiguriert ist

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

22. Globalen Schreibschutz im Admin-Modus einstellen

Wenn der Administrator den diskAshur³ konfiguriert und auf globalen Lesezugriff beschränkt, dann können weder der Administrator noch der Benutzer auf das Laufwerk schreiben und beide sind auf den Lesezugriff beschränkt. Nur der Administrator ist in der Lage, die Einstellung wieder auf Lese-/Schreibzugriff zurückzusetzen, wie in Abschnitt 23 beschrieben.

Um den diskAshur³ so einzustellen, dass der globale Zugriff auf Lesezugriff beschränkt ist, gehen Sie zuerst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die Tasten „**5 + 6**“.		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie die **Schlüssel**-Taste **(🔓)**		Die GRÜNE und BLAUE LED schalten auf eine durchgehend GRÜNE LED und dann zu einer durchgehend BLAUEN LED, die anzeigt, dass das Laufwerk konfiguriert wurde und der globale Zugriff auf Lesezugriff eingeschränkt ist

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

23. Aktivieren des globalen Lese-/Schreibzugriffs im Admin-Modus

Um die Einstellung des diskAshur³ vom globalen schreibgeschützen Zugriff wieder in „Lesen/Schreiben“ zu ändern, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus**befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten „**5 und 9**“ gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie die Taste **Entsperren (🔓)**		Die Anzeige wechselt von einer blinkenden GRÜNEN und blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN und dann zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass für den Datenträger die Einstellung „Lesen/Schreiben“ konfiguriert wurde.

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

24. Konfigurieren einer Selbstzerstörungs-PIN

Sie können eine Selbstzerstörungs-PIN konfigurieren, bei deren Eingabe ein Crypto-Erase auf dem Datenträger ausgeführt wird (der Verschlüsselungsschlüssel wird gelöscht). Dieser Prozess löscht alle konfigurierten PINs und macht alle auf dem Datenträger gespeicherten Daten unzugänglich (für immer verloren). Der Datenträger wird daraufhin als entsperrt angezeigt (GRÜNE LED). Wenn diese Funktion ausgeführt wird, wird die Selbstzerstörungs-PIN zur neuen Benutzer-PIN und der Datenträger muss neu formatiert werden, bevor er erneut verwendet werden kann.

Um die Selbstzerstörungs-PIN zu ändern, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **SCHLÜSSEL-Taste (🔓)** und die **6** gleichzeitig gedrückt		Die durchgehend BLAUE LED schaltet zur blinkend GRÜNEN und durchgehend BLAUEN LEDs
2. Konfigurieren Sie eine 8-64-stellige **Selbstzerstörungs-PIN**, geben Sie diese ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔓)**		Die blinkende GRÜNE und durchgehend BLAUE LED schalten zu einer GRÜN blinkenden LED und schließlich wieder zu einer blinkenden GRÜNEN und einer durchgehend BLAUEN LED
3. Geben Sie Ihre **Selbstzerstörungs-PIN** erneut ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔓)**		Die GRÜNE LED blinkt schnell einige Sekunden lang und anschließend leuchtet die BLAUE LED durchgehend und zeigt so an, dass die Selbstzerstörungs-PIN erfolgreich konfiguriert wurde

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

25. Löschen der Selbstzerstörungs-PIN

Um die Selbstzerstörungs-PIN zu ändern, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **UMSCHALT**-Taste und die 6 gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zur blinkenden ROTEN LED
2. Drücken und halten Sie die **UMSCHALT-Taste (⬆)** und die **6** gleichzeitig gedrückt		Die ROTE LED blinkt und leuchtet dann durchgehend, anschließend leuchtet die BLAUE LED durchgehend und zeigt so an, dass die Selbstzerstörungs-PIN erfolgreich gelöscht wurde

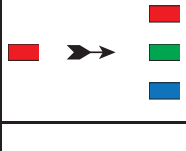
Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

26. Entsperren mit der Selbstzerstörungs-PIN

Warnung: Wenn der Selbstzerstörungsmechanismus aktiviert wird, werden alle Daten, der Verschlüsselungsschlüssel und die Admin-/Benutzer-PINs gelöscht. **Die Selbstzerstörungs-PIN wird zur neuen Benutzer-PIN.** Nach Aktivierung des Selbstzerstörungsmechanismus ist keine Admin-PIN mehr vorhanden. Der diskAshur³ muss zuerst zurückgesetzt werden (siehe Abschnitt 36 „Durchführen einer kompletten Rücksetzung“ auf Seite 109), damit eine Admin-PIN mit umfassenden Admin-Privilegien (einschließlich der Erstellung einer neuen Benutzer-PIN) konfiguiert werden kann.

Die Selbstzerstörungs-PIN **löscht ALLE Daten, den Verschlüsselungsschlüssel und die Admin-/Benutzer-PINs** und entsperrt anschließend den Datenträger. Die Aktivierung dieser Funktion führt dazu, dass die **Selbstzerstörungs-PIN zur neuen Benutzer-PIN** wird. Der diskAshur³ muss neu formatiert werden, bevor neue Daten zum Datenträger hinzugefügt werden können.

Damit der Selbstzerstörungsmechanismus aktiviert werden kann, muss sich der Datenträger im Standby-Modus (ROTE LED leuchtet durchgehend) befinden. Führen Sie dann die folgenden Schritte aus:

1. Halten Sie im **Standby-Modus** (ROTE LED leuchtet durchgehend) die Tasten **UMSCHALTEN** (⬆) und **Entsperren(🔓)** gedrückt.		Anstatt der ROTEN LED leuchten alle LEDs auf (ROT, GRÜN und BLAU) und blinken abwechselnd.
2. Geben Sie die **Selbstzerstörungs-PIN** ein und drücken Sie die Taste **Entsperren (🔓)**		Die Anzeige wechselt von einer blinkenden ROTEN, GRÜNEN und BLAUEN LED zu einer blinkenden GRÜNEN und dann zu einer durchgehend leuchtenden GRÜNEN LED. Damit wird angezeigt, dass der Selbstzerstörungsprozess für den diskAshur³ erfolgreich durchgeführt wurde.

27. Erstellen einer Admin-PIN nach einem Brute-Force-Angriff oder nach dem Zurücksetzen

Nach einem Brute-Force-Angriff oder wenn Sie den diskAshur³ zurückgesetzt haben, muss eine neue Admin-PIN erstellt werden, bevor das Laufwerk verwendet werden kann.

PIN-Anforderungen:

- Muss zwischen8 und 64 Ziffern lang sein
- Darf nicht nur sich wiederholende Zahlen enthalten, z. B. (3-3-3-3-3-3-3-3)
- Darf nicht nur aufeinanderfolgende Zahlen enthalten, z. B. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- Die UMSCHALT-Taste kann für zusätzliche Kombinationen verwendet werden (z. B.**UMSCHALTEN** (⬆) **+ 1** ergibt einen anderen Wert als nur 1.

Wenn der diskAshur³ per Brute-Force angegriffen oder zurückgesetzt wurde, befindet sich das Laufwerk im Standby-Zustand (durchgehend ROTE LED). Um eine Admin-PIN zu konfigurieren, fahren Sie mit den folgenden Schritten fort.

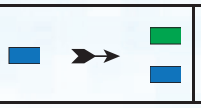
1. Drücken und halten Sie im Standby-Zustand (durchgehend leuchtende ROTE LED) die **UMSCHALT**-Taste (⬆) und die **1** gedrückt		Die durchgehend ROTE LED schaltet zur GRÜN blinkenden und durchgehend BLAUEN LED
2. Geben Sie die **neue Admin-PIN** ein und drücken Sie die SCHLÜSSEL-Taste **(🔓)**		Die GRÜN blinkende und durchgehend BLAUE LED schalten auf eine ein Mal GRÜN aufleuchtende LED um, und anschließend wieder auf eine GRÜN blinkende und durchgehend BLAUE LED
3. Geben Sie die **neue Admin-PIN** erneut ein und drücken Sie dann die **Schlüssel**-Taste **(🔓)**		Die GRÜN blinkende LED und die durchgehend BLAUE LED wechseln für einige Sekunden zu einer schnell blinkenden BLAUEN LED. Schließlich leuchtet wieder die BLAUE LED durchgehend und zeigt an, dass die Admin-PIN erfolgreich konfiguriert wurde.

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

28. Einstellen der automatischen Sperre bei Abwesenheit

Zum Schutz vor unbefugtem Zugriff kann der diskAshur³ so eingestellt werden, dass er nach einer voreingestellten Zeitspanne automatisch gesperrt wird, wenn er freigeschaltet und unbeaufsichtigt ist. In der Standardeinstellung ist die automatische Sperre des diskAshur³ deaktiviert. Die automatische Sperre bei Abwesenheit kann so eingestellt werden, dass sie zwischen 5 und 99 Minuten aktiviert wird.

Um die automatische Sperre bei Abwesenheit einzustellen, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die SCHLÜSSEL-Taste **(🔓)** und die 5 gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Geben Sie die Zeitspanne ein, auf die die automatische Sperre eingestellt werden soll. Die minimale Zeitspanne beträgt 5 Minuten und die maximale Zeitspanne 99 Minuten (5–99 Minuten). Sie können zum Beispiel Folgendes eingeben: **05 für 5 Minuten (drücken Sie „0“ und anschließend „5“)** **20 für 20 Minuten (drücken Sie „2“ und anschließend „0“)** **99 für 99 Minuten (drücken Sie „9“ und anschließend „9“)**		
3. Drücken Sie die **UMSCHALT**-Taste (⬆)		Die blinkende GRÜNE und BLAUE LED wechseln für eine Sekunde zu einer durchgehend GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, dass die Zeitspanne für die automatische Sperrung erfolgreich konfiguriert wurde

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

29. Deaktivieren der automatischen Sperre bei Abwesenheit

Um die unbeaufsichtigte Zeitüberschreitungsfunktion für die automatische Sperre zu deaktivieren, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend leuchtende BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **SCHLÜSSEL-Taste (🔓)** und die 5 gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Geben Sie **00** erneut ein und drücken Sie die **UMSCHALT**-Taste (⬆)		Die GRÜN und BLAU blinkenden LEDs werden auf für eine Sekunde auf durchgehend GRÜN geschaltet, und anschließend auf durchgehend BLAU LED, wodurch angezeigt wird, dass die Zeitspanne für die automatische Sperre erfolgreich deaktiviert wurde

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

30. Überprüfen der automatischen Sperre bei Abwesenheit

Der Administrator kann die Zeitspanne, die für die automatische Sperre bei Abwesenheit eingestellt wurde, überprüfen und ermitteln, indem er oder sie einfach die LED-Sequenz beobachtet, wie in der nachstehenden Tabelle beschrieben.

Um die automatische Sperre bei Abwesenheit zu überprüfen, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die **UMSCHALT**-Taste (⬆) und die 5 gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** und Folgendes geschieht; a. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend. b. Jedes Blinken der ROTEN LED entspricht zehn (10) Minuten. c. Jedes Blinken der GRÜNEN LED entspricht zehn (1) Minuten. d. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend. e. LEDs schalten zu einem durchgehenden BLAU zurück		

Die folgende Tabelle beschreibt die Signale der LEDs bei der Überprüfung der automatischen Sperre. Wenn Sie z. B. das Laufwerk so eingestellt haben, dass es sich nach **25** Minuten automatisch sperrt, wird die ROTE LED zweimal (**2**) blinken und die GRÜNE LED fünf (**5**) Mal.

Automatische Sperre in Minuten	ROT	GRÜN
5 Minuten	0	5-faches Blinken
15 Minuten	1-faches Blinken	5-faches Blinken
25 Minuten	2-faches Blinken	5-faches Blinken
40 Minuten	4-faches Blinken	0

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

31. Schreibschutz im Benutzermodus einstellen

Um den diskAshur³ ausschließlich auf Lesezugriff einzustellen, gehen Sie zuerst in den „**Benutzermodus**“, wie in Abschnitt 13 beschrieben. Sobald sich das Laufwerk im **Benutzermodus** befindet (durchgehend GRÜNE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Benutzermodus die Tasten „**7 + 6**“ gedrückt. (7=**R**ead + 6=**O**nly)		Die GRÜNE LED schaltet zu blinkend GRÜN, und die BLAUE LEDs ebenfalls
2. Drücken Sie die **Schlüssel**-Taste **(🔓)**		Die GRÜNE und BLAUE LED wechseln zu einer durchgehenden GRÜNEN LED, die anzeigt, dass das Laufwerk als schreibgeschützt konfiguriert ist

Anmerkung: 1. Wenn ein Benutzer das Laufwerk als schreibgeschützt festgelegt hat, kann der Admin dies außer Kraft setzen, indem er das Laufwerk im Admin-Modus auf Lese-/Schreibzugriff stellt.

2. Wenn der Administrator das Laufwerk als schreibgeschützt festgelegt hat, kann der Benutzer das Laufwerk nicht für den Lese-/Schreibzugriff aktivieren.

32. Lese-/Schreibzugriff im Benutzermodus einstellen

Um den diskAshur³ auf Lese-/Schreibzugriff einzustellen, gehen Sie zuerst in den „**Benutzermodus**“, wie in Abschnitt 13 beschrieben. Sobald sich das Laufwerk im **Benutzermodus** befindet (durchgehend GRÜNE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Benutzermodus die Tasten „**7 + 9**“ gedrückt. (7=**R**ead + 9=**W**rite)		Die GRÜNE LED schaltet zu blinkend GRÜN, und die BLAUE LEDs ebenfalls
2. Drücken Sie die Schlüssel-Taste **(🔓)**		Die GRÜNE und BLAUE LED wechseln zu einer durchgehenden GRÜNEN LED, die anzeigt, dass das Laufwerk für Lese-/Schreibzugriff konfiguriert ist

Anmerkung: 1. Wenn ein Benutzer das Laufwerk als schreibgeschützt festgelegt hat, kann der Admin dies außer Kraft setzen, indem er das Laufwerk im Admin-Modus auf Lese-/Schreibzugriff stellt.

2. Wenn der Administrator das Laufwerk als schreibgeschützt festgelegt hat, kann der Benutzer das Laufwerk nicht für den Lese-/Schreibzugriff aktivieren.

33. Abwehrmechanismus gegen Brute-Force-Hacker-Angriffe

Der diskAshur³ verfügt über einen Abwehrmechanismus, der den Datenträger vor Brute-Force-Angriffen schützt. Standardmäßig ist die Brute-Force-Beschränkung für die **Admin-PIN** und die **Benutzer-PIN** auf **10** aufeinanderfolgende falsche PIN-Eingaben eingestellt. Die Anzahl für die **Wiederherstellungs-PIN** beträgt **5**. Drei voneinander unabhängige Brute-Force-Zähler werden verwendet, um die Fehlversuche für jede PIN-Autorisierung aufzuzeichnen. Wenn ein Benutzer zehnmal hintereinander eine falsche Admin-PIN eingibt (wie nachstehend beschrieben aufgeteilt in Gruppen von 5, 3 und 2), wird der Datenträger zurückgesetzt und alle Daten gehen für immer verloren. Wenn ein Benutzer eine falsche Wiederherstellungs-PIN oder Benutzer-PIN eingibt und die jeweilige Brute-Force-Beschränkung überschreitet, werden die entsprechenden PINs gelöscht, aber die Daten sind weiterhin auf dem Datenträger vorhanden.

Hinweis: Für die Brute-Force-Beschränkung werden die Anfangswerte wiederhergestellt, wenn der Datenträger vollständig zurückgesetzt oder die Selbstzerstörungsfunktion aktiviert wird. Wenn der Administrator die Benutzer-PIN ändert oder wenn bei Aktivierung der Wiederherstellungsfunktion eine neue Benutzer-PIN eingestellt wird, wird der Brute-Force-Zähler der Benutzer-PIN gelöscht. Das hat jedoch keine Auswirkung auf die Brute-Force-Beschränkung. Wenn der Administrator die Wiederherstellungs-PIN ändert, wird der Brute-Force-Zähler der Wiederherstellungs-PIN gelöscht.

Durch die erfolgreiche Autorisierung einer bestimmten PIN wird der Brute-Force-Zähler für die betreffende PIN gelöscht. Das hat jedoch keine Auswirkung auf den Brute-Force-Zähler der anderen PINs. Durch die fehlgeschlagene Autorisierung einer bestimmten PIN erhöht sich der Brute-Force-Zähler für die betreffende PIN. Das hat jedoch keine Auswirkung auf den Brute-Force-Zähler der anderen PINs.

- Wenn ein Benutzer zehnmal hintereinander eine **falsche Benutzer-PIN** eingibt, wird die Benutzer-PIN gelöscht. Die Daten sowie die Admin-PIN und die Wiederherstellungs-PIN bleiben jedoch intakt und zugänglich.
- Wenn fünfmal hintereinander eine **falsche Wiederherstellungs-PIN** eingegeben wird, wird die Wiederherstellungs-PIN gelöscht. Die Daten und die Admin-PIN bleiben jedoch intakt und zugänglich.
- Die **Admin-PIN** verwendet einen ausgefeilteren Schutzmechanismus als die Benutzer- und Wiederherstellungs-PINs. Nach **5 aufeinanderfolgenden falschen Admin-PIN-Eingaben** wird der Datenträger gesperrt und die **ROTE**, **GRÜNE** und **BLAUE** LED leuchten durchgehend. Jetzt müssen Sie die folgenden Schritte ausführen, um dem Benutzer **3** weitere PIN-Eingaben zu ermöglichen.

- Geben Sie die PIN „**47867243**“ ein und drücken Sie die Taste **SCHLÜSSEL (🔓)**. Die **GRÜNE** und die **BLAUE** LED blinken gleichzeitig. Der Datenträger akzeptiert jetzt **3** weitere Admin-PIN-Eingaben.
- Nach insgesamt 8 aufeinanderfolgenden falschen Admin-PIN-Eingaben wird der Datenträger gesperrt und die **ROTE**, **GRÜNE** und **BLAUE** LED blinken abwechselnd. Nun müssen Sie die folgenden Schritte ausführen, um die letzten **2** PIN-Eingaben zu ermöglichen (insgesamt 10).
- Geben Sie die PIN „**47867243**“ ein und drücken Sie die Taste **SCHLÜSSEL (🔓)**. Die **GRÜNE** und **BLAUE** LED blinken gleichzeitig. Der Datenträger ist jetzt bereit für die letzten **2** PIN-Eingaben (insgesamt 10).
- Nach insgesamt 10 falschen Admin-PIN-Eingaben wird der Verschlüsselungsschlüssel gelöscht und alle Daten und PINs auf dem Laufwerk gehen unwiderruflich verloren.

In der nachfolgenden Tabelle wird davon ausgegangen, dass alle drei PINs eingerichtet wurden. Es werden die Auswirkungen eines ausgelösten Brute-Force-Abwehrmechanismus für jede einzelne PIN beschrieben.

Zum Entsperren des Datenträgers verwendete PIN	Aufeinanderfolgende falsche PIN-Eingaben	Beschreibung der Auswirkungen
Benutzer-PIN	10	• Die Benutzer-PIN wird gelöscht. • Die Wiederherstellungs-PIN, die Admin-PIN und alle Daten bleiben intakt und zugänglich.
Wiederherstellungs-PIN	5	• Die Wiederherstellungs-PIN wird gelöscht. • Die Admin-PIN und alle Daten bleiben intakt und zugänglich.
Admin-PIN	5 3 2 (insgesamt 10)	• Nach **5** aufeinanderfolgenden falschen Admin-PIN-Eingaben wird der Datenträger gesperrt und alle LEDs leuchten durchgehend. • Geben Sie die PIN „**47867243**“ ein und drücken Sie die Taste **SCHLÜSSEL (🔓)**, um **3** weitere PIN-Eingaben zu ermöglichen. • Nach insgesamt **8** (5 + 3) aufeinanderfolgenden falschen Admin-PIN-Eingaben wird der Datenträger gesperrt und die LEDs blinken abwechselnd. • Geben Sie die PIN „**47867243**“ ein und drücken Sie die Taste **SCHLÜSSEL (🔓)**, um die letzten **2** PIN-Eingaben zu ermöglichen (insgesamt 10). • Nach insgesamt 10 aufeinanderfolgenden falschen Admin-PIN-Eingaben wird der Verschlüsselungsschlüssel gelöscht und alle Daten und PINs auf dem Datenträger gehen unwiderruflich verloren.

Wichtig: Es muss eine neue Admin-PIN konfiguriert werden, wenn auf die vorherige Admin-PIN ein Brute-Force-Angriff erfolgt ist. Lesen Sie dazu Abschnitt 27 „Konfigurieren einer Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung“ auf Seite 103 Der diskAshur³ muss außerdem formatiert werden, bevor neue Daten zum Datenträger hinzugefügt werden können.

34. Einstellen der Brute-Force-Beschränkung für die Benutzer-PIN

Hinweis: Die Brute-Force-Beschränkung für die Benutzer-PIN ist standardmäßig auf 10 aufeinanderfolgende falsche PIN-Eingaben eingestellt, wenn der Datenträger vollständig zurückgesetzt wird, ein Brute-Force-Angriff erfolgt oder die Selbstzerstörungs-PIN aktiviert wird.

Die Brute-Force-Beschränkung für die Benutzer-PIN des diskAshur³ kann vom Administrator neu programmiert und eingestellt werden. Diese Funktion kann so eingestellt werden, dass 1 bis 10 aufeinanderfolgende Versuche für die Eingabe einer falschen PIN zulässig sind.

Um eine Brute-Force-Beschränkung für die Benutzer-PIN zu konfigurieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **7 und 0** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einerGRÜNEN und BLAUEN LED, die gleichzeitig blinken.
2. Geben Sie die Anzahl der zulässigen Versuche für die Brute-Force-Beschränkung (zwischen 01 und 10) ein – zum Beispiel: • **01** für 1 Versuch • **10** für 10 Versuche		
3. Drücken Sie einmal die **UMSCHALT**-Taste (⬆)		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zuerst zu einer GRÜNEN LED, die eine Sekunde lang durchgehend leuchtet, und dann zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass die Brute-Force-Begrenzung erfolgreich konfiguriert wurde.

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

35. Überprüfen der Brute-Force-Beschränkung für die Benutzer-PIN

Der Administrator kann die Anzahl der zulässigen aufeinanderfolgenden Eingaben einer falschen Benutzer-PIN vor dem Auslösen des Brute-Force-Abwehrmechanismus beobachten und bestimmen, indem er einfach die LED-Sequenz wie nachfolgend beschrieben notiert.

Um die Einstellung der Brute-Force-Beschränkung zu überprüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „ **Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus**befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **2** und **0 gedrückt.**		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie die Taste **Entsperren (🔓)** Es geschieht Folgendes: a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend. b. Jedes Blinken einer ROTEN LED entspricht zehn (10) Einheiten einer Brute-Force-Beschränkungsanzahl. c. Jedes Blinken einer GRÜNEN LED entspricht einer (1) einzelnen Einheit einer Brute-Force-Beschränkungsanzahl. d. Alle LEDs (ROT, GRÜN UND BLAU) leuchten 1 Sekunde durchgehend. e. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.		

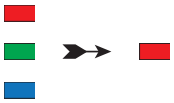
In der nachstehenden Tabelle wird das LED-Verhalten bei der Überprüfung der Brute-Force-Beschränkungseinstellung beschrieben. Wenn Sie den Datenträger beispielsweise auf eine Brute-Force-Reaktion nach **5** aufeinanderfolgenden falschen PIN-Eingaben eingestellt haben, blinkt die GRÜNE LED fünfmal (**5**).

Brute-Force-Beschränkungseinstellung	**ROT**	**GRÜN**
2 Versuche	0	2 Blinkzeichen
5 Versuche	0	5 Blinkzeichen
10 Versuche	1 Blinkzeichen	0

Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

36. Vollständiges Zurücksetzen des Geräts

Um das Gerät vollständig zurückzusetzen, muss sich der diskAshur³ im Standby-Zustand befinden (durchgehend ROTE LED). Sobald das Laufwerk zurückgesetzt wurde, werden die Admin-/Benutzer-PINs, der Schlüssel und alle Daten gelöscht und gehen für immer verloren. Das Laufwerk muss formatiert werden, bevor er wieder verwendet werden kann. Um den diskAshur³ zurückzusetzen, fahren Sie mit den folgenden Schritten fort.

1. Im Standby-Zustand (durchgehend ROTE LED), drücken und halten Sie die Taste „**0**“ gedrückt		Die durchgehend ROTE LED geht aus und alle LEDs fangen an, abwechselnd zu blinken, ROT, GRÜN und BLAU.
2. Drücken und halten Sie die **Tasten 2** und **7**		Die ROT, GRÜN und BLAU blinkenden LEDs leuchten eine Sekunde lang durchgehend und anschließend leuchtet die ROTE LED durchgehend und zeigt an, dass das Laufwerk zurückgesetzt wurde

Wichtig: Wenn das Gerät vollständig zurückgesetzt wurde, muss eine neue Admin-PIN konfiguriert werden, siehe Abschnitt 27 auf Seite 103: „Erstellen einer Admin-PIN nach einem Brute-Force-Angriff oder nach dem Zurücksetzen“. Der diskAshur³ muss auch Formatiert werden, bevor neue Daten zum Laufwerk hinzugefügt werden können.

37. Konfigurieren der Bootfähigkeitsfunktion des diskAshur³

Hinweis: Bei aktivierter Bootfähigkeitsfunktion des Datenträgers leuchtet die LED nicht ROT, wenn Sie den Datenträger aus dem Betriebssystem auswerfen. Stattdessen leuchtet die GRÜNE LED durchgehend, und der Datenträger muss zuersvom Computer getrennt werden, bevor er wieder verwendet werden kann. Standardmäßig ist der diskAshur³ als nicht bootfähig konfiguriert.

Der diskAshur³ verfügt über eine Bootfähigkeitsfunktion, mit der ein Neustart während eines Host-Bootprozesses überbrückt werden kann. Beim Booten vom diskAshur³ wird Ihr Computer mit dem Betriebssystem ausgeführt, das auf dem diskAshur³ installiert ist.

Um den Datenträger als bootfähig zu konfigurieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **Entsperren (🔓) und 9** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie zuerst auf **„0“** und dann auf **„1“** (**01**).		Die GRÜNE und die BLAUE LED blinken weiter.
3. Drücken Sie einmal die UMSCHALT-Taste (⬆)		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zuerst zu einer durchgehend leuchtenden GRÜNEN und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass der Datenträger erfolgreich als bootfähig konfiguriert wurde.

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

38. Deaktivieren der Bootfähigkeitsfunktion des diskAshur³

Um die Bootfähigkeitsfunktion des diskAshur³ zu deaktivieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten **Entsperren (🔓) und 9** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie zuerst auf **„0“** und dann erneut auf **„0“** (**00**).		Die GRÜNE und die BLAUE LED blinken weiter.
3. Drücken Sie einmal die UMSCHALT-Taste (⬆)		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Damit wird angezeigt, dass die Bootfähigkeitsfunktion erfolgreich deaktiviert wurde.

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

39. Überprüfen der Bootfähigkeitseinstellung

Um die Bootfähigkeitseinstellung zu überprüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „Admin-Modus**“.** Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die **Tasten UMSCHALTEN** (⬆) **und 9** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie die Taste **Entsperren (🔓)** und eines der beiden folgenden Szenarien tritt ein:

- **Wenn der diskAshur³ als bootfähig konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
b. Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
d. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.

- **Wenn der diskAshur³ <u>NICHT</u> als bootfähig konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
b. Alle LEDs erlöschen.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
d. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste **(🔓)** eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

40. Konfigurieren des Verschlüsselungsmodus

WARNUNG: Wenn der Verschlüsselungsmodus von AES-XTS (Standardeinstellung) in AES-ECB oder AES-CBC geändert wird, wird der Verschlüsselungsschlüssel gelöscht. Außerdem wird der diskAshur³ zurückgesetzt und alle Daten werden unzugänglich und sind für immer verloren!

Führen Sie die folgenden Schritte aus, um für den Verschlüsselungsmodus des diskAshur³ entweder die Option **AES-ECB**, angegeben durch die Nummer **„01“**, oder die Option **AES-XTS**, angegeben durch die Nummer **„02“**, oder die Option **AES-CBC**, angegeben durch die Nummer **„03“**, zu konfigurieren. Die Standardeinstellung dieser Funktion lautet „AES-XTS“ (02). Bitte beachten Sie, dass beim Wechsel zu einem anderen Verschlüsselungsmodus alle wichtigen Parameter gelöscht werden und der Datenträger zurückgesetzt wird.

Um den Verschlüsselungsmodus des diskAshur³ einzustellen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den **Admin-Modus** . Wenn sich der diskAshur³ im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten „ **SCHLÜSSEL (🔓) und 1**“ gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **01** ein, um **AES-ECB** einzustellen. Geben Sie **02** ein, um **AES-XTS** einzustellen (Standardeinstel lung). Geben Sie **03** ein, um **AES-CBC** einzustellen		Die GRÜNE und die BLAUE LED blinken weiter.
3. Drücken Sie einmal die **UMSCHALT**-Taste (⬆)		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und dann zu einer durchgehend leuchtenden ROTEN LED (Zurücksetz-Status**). Damit wird angezeigt, dass der Verschlüsselungsmodus erfolgreich geändert wurde.**

Wichtig: Nach der Konfiguration des Verschlüsselungsmodus wird der diskAshur³ vollständig zurückgesetzt, und es muss eine neue Admin-PIN konfiguriert werden. Siehe hierzu Abschnitt 27 „Konfigurieren einer Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung“ auf Seite 103.

41. Überprüfen des Verschlüsselungsmodus

Um den Verschlüsselungsmodus des diskAshur³ zu überprüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den **Admin-Modus**. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus **die Tasten „**UMSCHALTEN (⬆) und **1**“ gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie die Taste **SCHLÜSSEL (🔓)** und Folgendes geschieht:

- **Wenn für den Verschlüsselungsmodus die Option „AES-ECB“ konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
b. Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
d. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.

- **Wenn für den Verschlüsselungsmodus die Option „AES-XTS“ konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
b. Die GRÜNE LED blinkt zweimal.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
d. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.

- **Wenn für den Verschlüsselungsmodus die Option „AES-CBC“ konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
b. Die GRÜNE LED blinkt dreimal.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
d. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.

Hinweis: Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALT**-Taste (⬆) eine Sekunde lang gedrückt – die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED.

42. Konfigurieren das Datenträgertyps

Der diskAshur³ kann entweder als „Wechseldatenträger“ oder als „Lokaler Datenträger (Standardeinstellung)“ konfiguriert werden. Beim Wechsel zu einem anderen Datenträgertyp werden alle wichtigen Parameter – alle PINs, der Verschlüsselungsschlüssel und die Daten – gelöscht und der Datenträger wird zurückgesetzt.

WARNUNG: Wenn die Datenträgertyp-Einstellung – entweder „Wechseldatenträger“ oder „Lokaler Datenträger (Standardeinstellung)“ – geändert wird, wird der Verschlüsselungsschlüssel gelöscht. Außerdem wird der diskAshur³ zurückgesetzt und alle Daten werden unzugänglich und sind für immer verloren!

Führen Sie die folgenden Schritte aus, um den Datenträgertyp des diskAshur³ entweder als „Wechseldatenträger“ (**00**) oder als „Lokaler Datenträger“ (**01**) zu konfigurieren. Diese Funktion ist standardmäßig auf „Lokaler Datenträger“ (**01**) eingestellt. Bitte beachten Sie, dass beim Wechsel zu einem Datenträgertyp anderen alle wichtigen Parameter gelöscht werden und der Datenträger zurückgesetzt wird.

Um den Datenträgertyp des diskAshur3 einzustellen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den **Admin-Modus** . Wenn sich der diskAshur³ im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus die Tasten „ **SCHLÜSSEL(🔓) und 8**“ gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **00** ein, um die Option **Wechseldatenträger** einzustellen. Geben Sie **01** ein, um die Option **Lokaler Datenträger (Standardeinstellung) einzustellen.**		Die GRÜNE und die BLAUE LED blinken weiter.
3. Drücken Sie einmal die **UMSCHALT**-Taste (⬆)		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN und dann zu einer durchgehend leuchtenden ROTEN LED (Zurücksetz-Status). Damit wird angezeigt, dass der Datenträgertyp **erfolgreich geändert wurde.**

Wichtig: Nach der Änderung des Datenträgertyps wird der diskAshur³ vollständig zurückgesetzt, und es muss eine neue Admin-PIN konfiguriert werden. Siehe hierzu Abschnitt 27 „Konfigurieren einer Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung“ auf Seite 103.

43. Überprüfen der Datenträgertyp-Einstellung

Um die Datenträgertyp-Einstellung des diskAshur³ zu überprüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den **Admin-Modus**. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte aus:

1. Halten Sie im Admin-Modus **die Tasten „**SCHLÜSSEL (⬆) und **8**“ gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie die Taste **SCHLÜSSEL (🔓)** und Folgendes geschieht:

- **Wenn der Datenträgertyp als „Wechseldatenträger“ konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend und erlöschen dann.
b. Alle LEDs (ROT, GRÜN und BLAU) leuchten erneut 1 Sekunde lang durchgehend und erlöschen dann.
d. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.

- **Wenn der Datenträgertyp als „Lokal“ konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
b Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
d. Die Anzeige wechselt wieder zu einer durchgehend leuchtenden BLAUEN LED.

44. Initialisieren und Formatieren des diskAshur³ für Windows

Nach einem „Brute-Force-Angriff“ oder einer kompletten Rücksetzung löscht der diskAshur³ alle PINs und Daten sowie den Verschlüsselungsschlüssel. Sie müssen den diskAshur³ initialisieren und formatieren, bevor er wieder verwendet werden kann.

Um Ihren diskAshur³ zu formatieren, gehen Sie wie folgt vor:

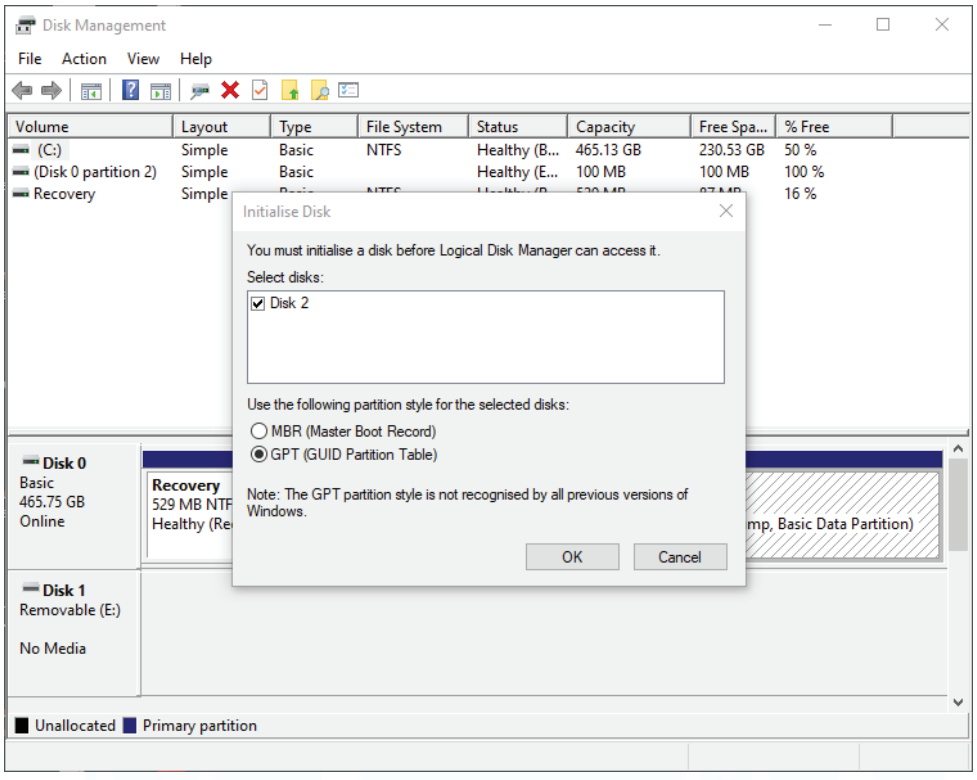
1. Konfigurieren Sie eine neue Admin-PIN – siehe Seite 103, Abschnitt 27 „Konfigurieren einer Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung“.

2. Versetzen Sie den diskAshur³ in den Standby-Modus (ROTE LED). Drücken Sie einmal die Taste **Entsperren (🔓)** und geben Sie zum Entsperren die **neue Admin-PIN** ein (GRÜNE LED blinkt).

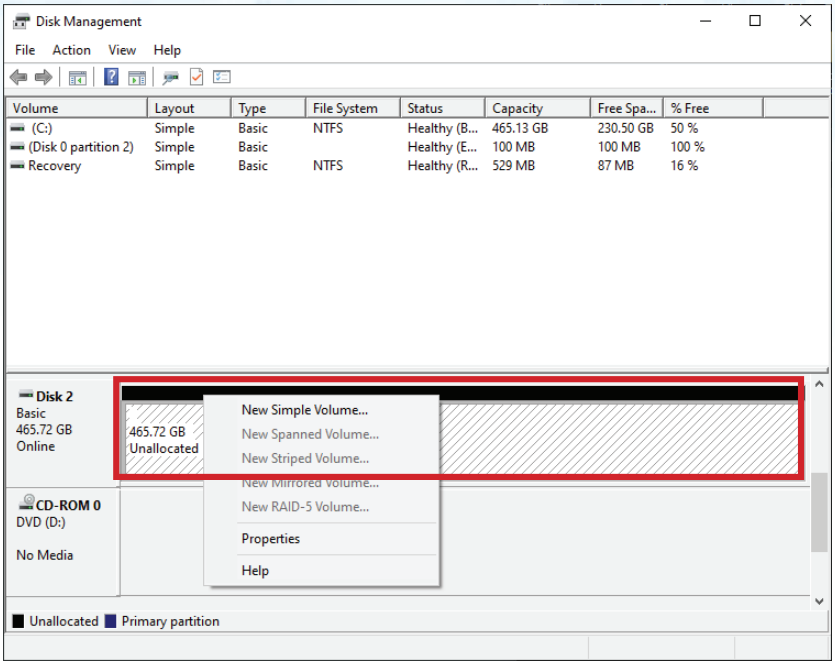
3. **Windows 7:** Rechtsklicken Sie auf **Computer**. Klicken Sie dann auf **Verwalten** und wählen Sie **Datenträgerverwaltung aus.**
   Windows 8: Rechtsklicken Sie auf die linke Ecke des Desktops und wählen Sie **Datenträgerverwaltung aus**.
   Windows 10: Rechtsklicken Sie auf die Start-Schaltfläche und wählen Sie **Datenträgerverwaltung aus.**

4. Im Fenster Datenträgerverwaltung wird der diskAshur³ als ein unbekanntes Gerät erkannt, das nicht initialisiert und nicht zugewiesen ist. Es erscheint ein Meldungsfenster, in dem Sie zwischen MBR- und GPT-Partitionen wählen können. GPT speichert mehrere Duplikate dieser Daten auf dem Datenträger und ist daher viel robuster. Auf einem MBR-Datenträger werden die Partitionierungs- und Bootinformationen an einem einzigen Ort gespeichert.

Wählen Sie den Partitionsstil aus und klicken Sie auf **OK**.



5. Rechtsklicken Sie in den leeren Bereich über dem Bereich **Nicht zugeordnet** und wählen Sie dann **Neues einfaches Volume** aus.



6. Das Fenster „Willkommen“ des Assistenten zum Erstellen neuer einfacher Volumes wird geöffnet. Klicken Sie auf „Weiter“.

7. Wenn Sie nur eine Partition benötigen, übernehmen Sie die Standardpartitionsgröße und klicken Sie auf **Weiter**.

8. Weisen Sie einen Laufwerksbuchstaben oder Pfad zu und klicken Sie auf **Weiter**.

9. Erstellen Sie eine Volumebezeichnung, wählen Sie „Schnellformatierung durchführen“ aus und klicken Sie dann auf **Weiter**.

10. Klicken Sie auf **Fertig stellen**.

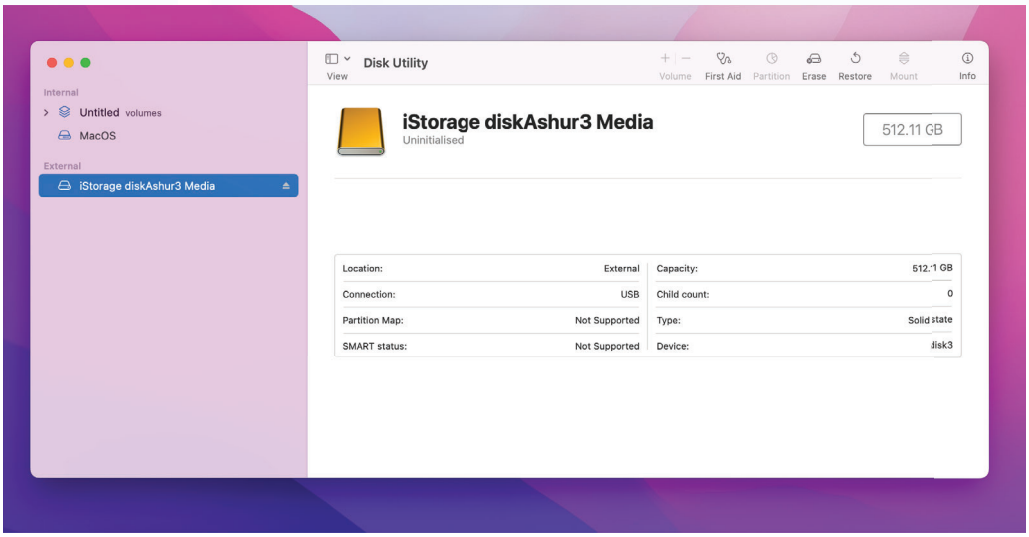
11. Warten Sie, bis der Formatierungsprozess abgeschlossen ist. Der diskAshur³ wird erkannt und kann verwendet werden.

45. Initialisieren und Formatieren des diskAshur³ unter Mac OS

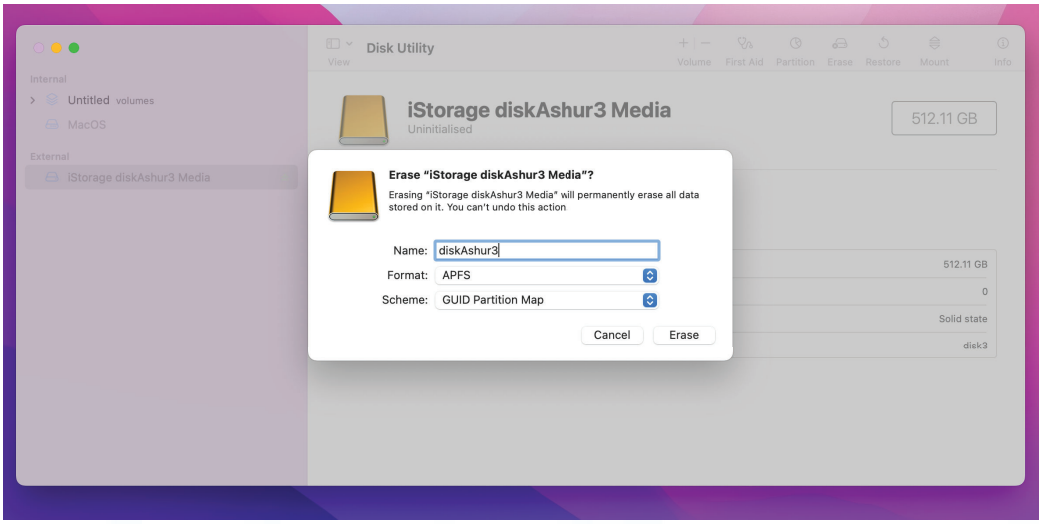
Nach einem „Brute-Force-Angriff“ oder einer kompletten Rücksetzung löscht der diskAshur³ alle PINs und Daten sowie den Verschlüsselungsschlüssel. Sie müssen den diskAshur³ initialisieren und formatieren, bevor er wieder verwendet werden kann.

Initialisieren und Formatieren des diskAshur³:

1. Wählen Sie den diskAshur³ aus der Liste der Laufwerke und Volumes aus. Für jedes Laufwerk in der Liste werden die Kapazität, der Hersteller und der Produktname angezeigt, wie z. B. „**iStorage diskAshur³ Media**“.

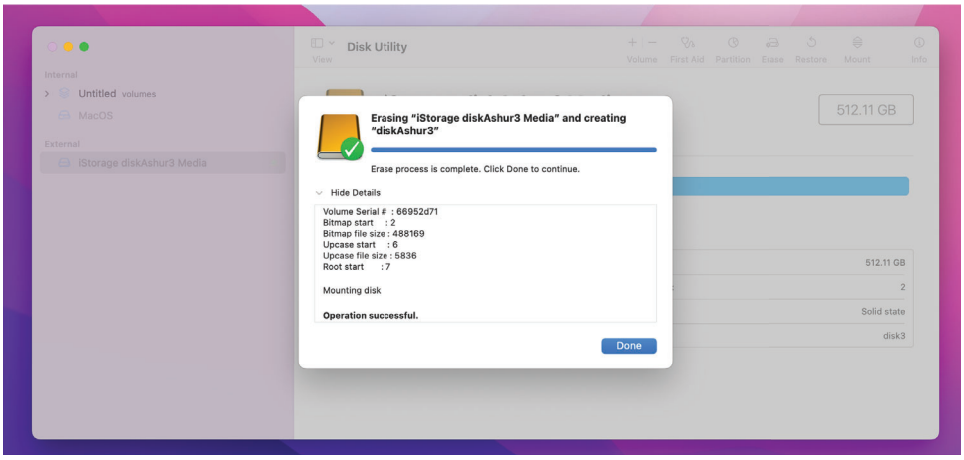


2. Klicken Sie im Datenträgern-Dienstprogramm auf die Schaltfläche „**Löschen**“.
3. Geben Sie einen Namen für das Laufwerk ein. Der Standardname ist „Unbenannt“. Der Name des Laufwerks wird schließlich auf dem Desktop angezeigt.



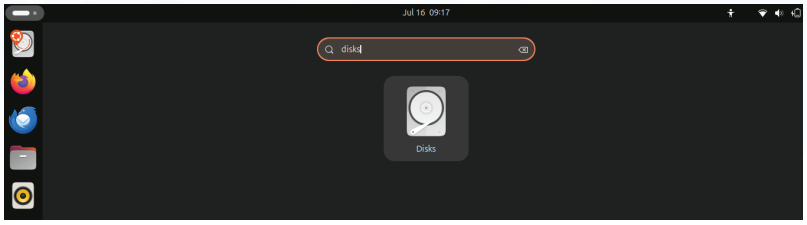
4. Wählen Sie ein Schema- und Volume-Format aus. Im Dropdown-Menü „Volumeformat“ werden alle vom Mac unterstützten Laufwerkformate angezeigt. Der empfohlene Formattyp ist „Mac OS Extended (Journaled)“. Für plattformübergreifende Anwendungen verwenden Sie „exFAT“. Im Dropdown-Menü „Schema“ werden die verfügbaren Schemata aufgelistet. Für Laufwerke, die größer als 2 TB sind, empfehlen wir die Option „GUID-Partitionstabelle“.

5. Klicken Sie auf die Schaltfläche „Löschen“. Das Datenträger-Dienstprogramm deinstalliert das Volume vom Desktop, löscht es und installiert es dann wieder auf dem Desktop.

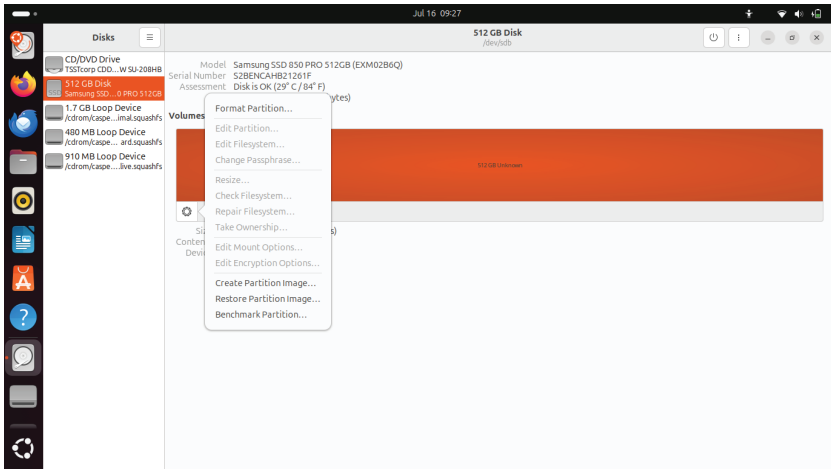


46. Initialisieren und Formatieren des diskAshur³ unter Linux OS

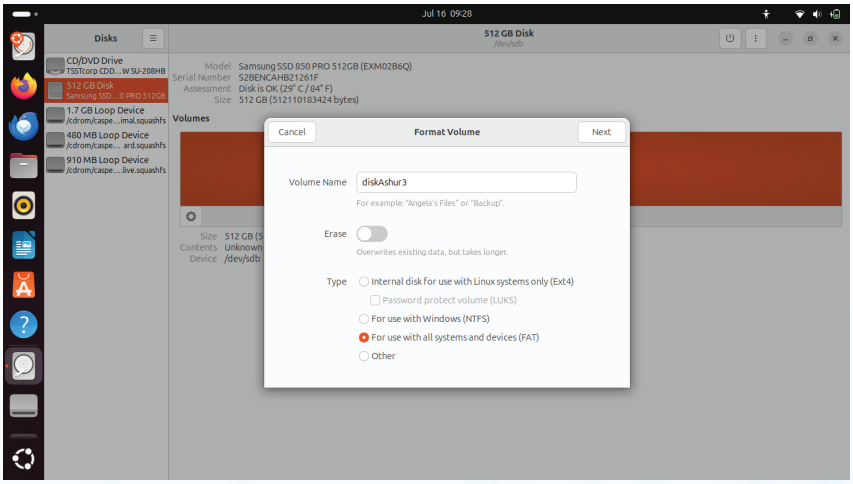
1. Öffnen Sie „**Show Application**“ (Anwendung anzeigen) und geben Sie „**Disks**“ (Datenträger) in das Suchfeld ein. Klicken Sie auf das Dienstprogramm „**Disks**“ (Datenträger), wenn es angezeigt wird.

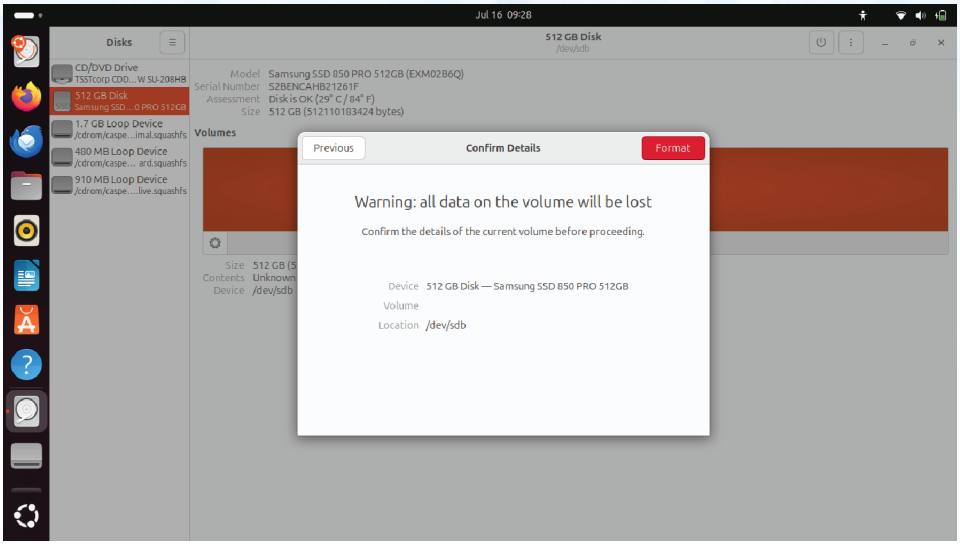


2. Wählen Sie unter „**Devices**“ (Geräte) das Laufwerk (500 GB Hard Disk) mit einem Mausklick aus. Klicken Sie als Nächstes unter „**Volumes**“ (Volumen) auf das Zahnrad-Symbol und dann auf „**Format Partitions**“ (Partitionen formatieren).

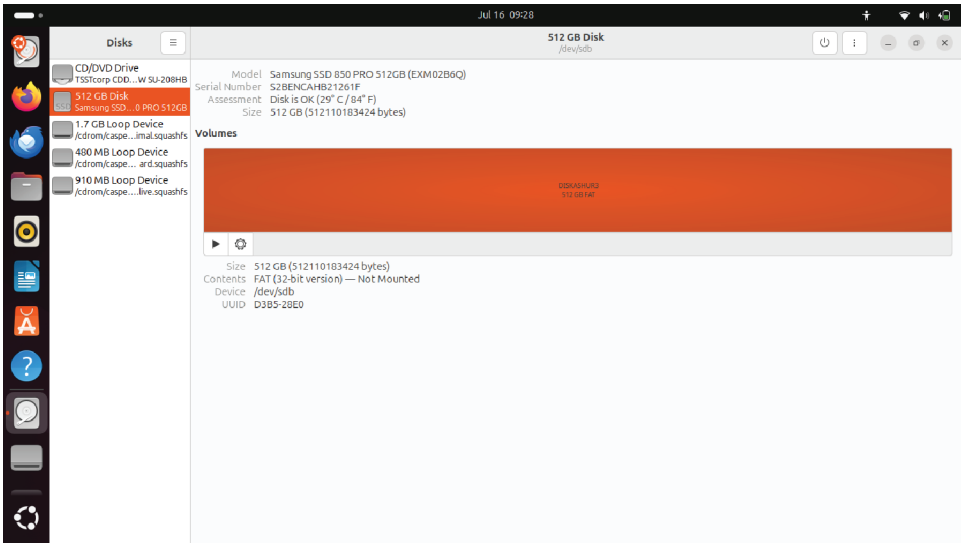


3. Wählen Sie für „**Type**“ (Typ) die Option „Compatible with all systems and devices (FAT)“ (Kompatibel mit allen Systemen und Geräten [FAT]) aus. Und geben Sie einen Namen für den Datenträger ein, wie z. B.: diskAshur³. Klicken Sie dann auf die Schaltfläche „**Format**“ (Formatieren).

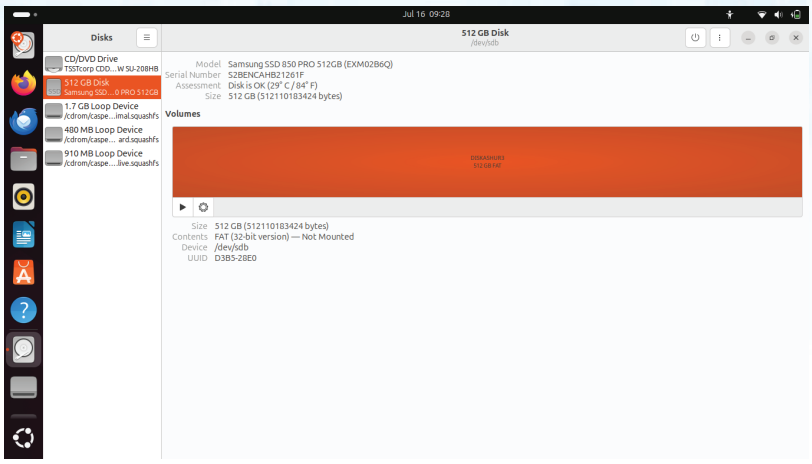




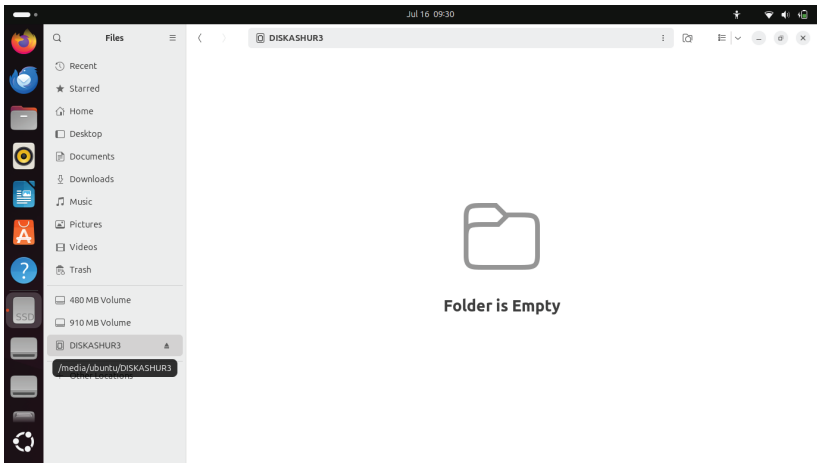
4. Wenn der Formatierungsvorgang abgeschlossen ist, klicken Sie auf die Wiedergabe-Schaltfläche, um den Datenträger in Ubuntu einzubinden.



5. Jetzt sollte der Datenträger in Ubuntu eingebunden und betriebsbereit sein.



6. Der Datenträger wird wie in der nachstehenden Abbildung zu sehen ist angezeigt. Sie können auf das Datenträgersymbol klicken, um Ihren Datenträger zu öffnen.



47. In den Ruhezustand versetzen, anhalten oder vom Betriebssystem abmelden

Stellen Sie sicher, dass Sie alle Dateien auf Ihrem diskAshur³ speichern und schließen, bevor Sie es in den Ruhezustand versetzen, es anhalten oder sich vom Betriebssystem abmelden.

Es wird empfohlen, den diskAshur³ manuell zu sperren, bevor Sie den Ruhezustand aktivieren, ihn anhalten oder sich von Ihrem System abmelden.

Um das Laufwerk zu sperren, werfen Sie den diskAshur³ sicher von Ihrem Host-Betriebssystem aus und ziehen Sie das Laufwerk aus dem USB-Anschluss. Wenn Daten auf das Laufwerk geschrieben werden, führt das Abziehen des diskAshur³ zu unvollständiger Datenübertragung und möglicherweise zu Schäden an den Daten.

⚠ **Achtung:** Damit Ihre Daten sicher sind, sollten Sie sicherstellen, dass Sie Ihren diskAshur³ sperren, wenn Sie sich nicht an Ihrem Computer befinden.

48. Überprüfen der Firmware im Admin-Modus

Um die Firmware-Revisionsnummer zu überprüfen, wechseln Sie zunächst in den „**Admin-Modus**“, wie in Abschnitt 5 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend BLAUE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Admin-Modus die Tasten **„3 + 8“** gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** einmal und Folgendes geschieht; a. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend. b. Die ROTE LED blinkt und zeigt den ganzzahligen Teil der Firmware-Revisionsnummer an. c. Die GRÜNE LED blinkt und zeigt den Dezimalteil an. d. Die BLAUE LED blinkt und zeigt die letzte Ziffer der Firmware-Revisionsnummer an e. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend. f. Die ROTE, GRÜNE und BLAUE LEDs wechseln zu einer durchgehend BLAUEN LED		

Wenn zum Beispiel die Firmware-Revisionsnummer „**2.3**“ ist, blinkt die ROTE LED zwei Mal (**2**) und die GRÜNE LED drei Mal (**3**). Sobald die Sequenz beendet ist, blinken die ROTE, GRÜNE und BLAUE LED einmal zusammen und kehren dann in den Admin-Modus zurück, also zur durchgehend BLAUEN LED.

49. Überprüfen der Firmware im Benutzermodus

Um die Firmware-Revisionsnummer zu überprüfen, wechseln Sie zunächst in den „**Benutzermodus**“, wie in Abschnitt 13 beschrieben. Sobald sich das Laufwerk im **Admin-Modus** befindet (durchgehend leuchtende GRÜNE LED), fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Benutzermodus die Tasten **„3 + 8“** gleichzeitig gedrückt, bis die GRÜNE und BLAUE LED gleichzeitig blinken		Die GRÜNE LED schaltet zu blinkend GRÜN, und die BLAUE LEDs ebenfalls

2. Drücken Sie die **SCHLÜSSEL**-Taste **(🔓)** und Folgendes geschieht;

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend.
b. Die ROTE LED blinkt und zeigt den ganzzahligen Teil der Firmware-Revisionsnummer an.
c. Die GRÜNE LED blinkt und zeigt den Dezimalteil an.
d. Die BLAUE LED blinkt und zeigt die letzte Ziffer der Firmware-Revisionsnummer an
e. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend.
f. Die ROTE, GRÜNE und BLAUE LEDs wechseln zu einer durchgehend BLAUEN LED

Wenn zum Beispiel die Firmware-Revisionsnummer „**2.3**“ ist, blinkt die ROTE LED zwei Mal (**2**) und die GRÜNE LED drei Mal (**3**). Sobald die Sequenz beendet ist, blinken die ROTE, GRÜNE und BLAUE LED einmal zusammen und kehren dann in den Benutzermodus zurück, also zur durchgehend GRÜNEN LED.

50. Technische Unterstützung

iStorage stellt die folgenden nützlichen Ressourcen für Sie bereit:

Website:
https://www.istorage-uk.com

E-Mail-Support:
support@istorage-uk.com

Telefonischer Support:
+44 (0) 20 8991-6260.

Die Spezialisten des technischen Supports von iStorage sind von 9:00 bis 17:30 Uhr GMT verfügbar, von Montag bis Freitag.

51. Garantie- und RMA-Informationen

ISTORAGE-PRODUKTHAFTUNG UND -GARANTIE

iStorage garantiert, dass seine Produkte bei Lieferung und für einen Zeitraum von 36 Monaten ab Lieferung frei von Materialfehlern sind. Diese Garantie gilt jedoch nicht unter den nachfolgend beschriebenen Umständen. iStorage garantiert, dass die Produkte den Standards entsprechen, die im entsprechenden Datenblatt auf unserer Website zum Zeitpunkt Ihrer Bestellung aufgeführt sind.

Diese Garantien gelten nicht für Mängel an den Produkten, die sich aus Folgendem ergeben:

- angemessene Abnutzung;
- mutwillige Beschädigung, anormale Lagerungs- oder Arbeitsbedingungen, Unfall, Fahrlässigkeit Ihrerseits oder durch Dritte;
- wenn Sie oder eine Drittpartei die Produkte nicht in Übereinstimmung mit der Bedienungsanleitung betreiben oder verwenden;
- jede Änderung oder Reparatur durch Sie oder durch einen Dritten, der nicht zu unseren autorisierten Reparaturdienstleistern gehört; oder
- jede von Ihnen zur Verfügung gestellte Spezifikation.

Im Rahmen dieser Garantien reparieren, ersetzen oder erstatten wir Ihnen nach unserem Ermessen alle Produkte, bei denen Materialfehler festgestellt wurden, vorausgesetzt, dass Sie bei der Lieferung folgende Maßnahmen durchführen:

- Sie inspizieren die Produkte, um zu prüfen, ob sie Materialfehler aufweisen; und
- Sie testen den Verschlüsselungsmechanismus in den Produkten.

Wir haften nicht für Sachmängel oder Mängel im Verschlüsselungsmechanismus der Produkte, die bei der Prüfung bei Lieferung feststellbar sind, sofern Sie uns diese Mängel nicht innerhalb von 30 Tagen nach Lieferung mitteilen. Wir haften nicht für Sachmängel oder Mängel im Verschlüsselungsmechanismus der Produkte, die nicht bei der Prüfung bei Lieferung feststellbar sind, sofern Sie uns diese Mängel nicht innerhalb von 7 Tagen mitteilen, nachdem Sie diese Mängel feststellen oder feststellen sollten. Wir sind im Rahmen dieser Garantien nicht haftbar, wenn Sie oder eine andere Person die Produkte weiterhin verwendet, nachdem ein Mangel festgestellt wurde. Nach der Mitteilung eines Defekts sollten Sie das defekte Produkt an uns zurücksenden. Wenn Sie ein Unternehmen sind, sind Sie für die Transportkosten verantwortlich, die Ihnen entstehen, wenn Sie Produkte oder Teile der Produkte im Rahmen der Garantie an uns senden, und wir sind für alle Transportkosten verantwortlich, die uns entstehen, wenn wir Ihnen ein repariertes oder Ersatzprodukt schicken. Wenn Sie eine Privatperson sind, lesen Sie bitte unsere Allgemeinen Geschäftsbedingungen.

Produkte, die zurückgegeben werden, müssen in der Originalverpackung und in sauberem Zustand sein. Zurückgegebene Produkte, die diesen Anforderungen nicht entsprechen, werden nach Ermessen des Unternehmens entweder abgelehnt oder es wird eine weitere zusätzliche Gebühr zur Deckung der zusätzlichen Kosten erhoben. Produkten, die zur Reparatur im Rahmen der Garantie zurückgesandt werden, muss eine Kopie der Originalrechnung beiliegen, oder es müssen die Originalrechnungsnummer und das Kaufdatum angegeben werden.

Wenn Sie eine Privatperson sind, gilt diese Garantie zusätzlich zu Ihren gesetzlichen Rechten in Bezug auf Produkte, die fehlerhaft sind oder nicht der Beschreibung entsprechen. Beratung über Ihre gesetzlichen Rechte erhalten Sie bei Ihrem örtlichen Bürgerberatungsbüro oder bei Ihrem Gewerbeaufsichtsamt

Die in diesem Abschnitt dargelegten Garantien gelten nur für den ursprünglichen Käufer eines Produkts von iStorage oder einem von iStorage autorisierten Wiederverkäufer oder Vertreiber. Diese Gewährleistungen sind nicht übertragbar.

MIT AUSNAHME DER HIERIN ENTHALTENEN BESCHRÄNKTEN GEWÄHRLEISTUNG UND SOWEIT GESETZLICH ZULÄSSIG, LEHNT ISTORAGE ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN AB, EINSCHLIESSLICH ALLER GEWÄHRLEISTUNGEN DER HANDELSÜBLICHEN QUALITÄT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER. ISTORAGE GARANTIERT NICHT, DASS DAS PRODUKT FEHLERFREI FUNKTIONIERT. SOWEIT VON RECHTS WEGEN DENNOCH STILLSCHWEIGENDE GEWÄHRLEISTUNGEN BESTEHEN, SIND DIESE GEWÄHRLEISTUNGEN AUF DIE DAUER DIESER GARANTIE BESCHRÄNKT. DIE REPARATUR ODER DER ERSATZ DIESES PRODUKTS, WIE HIERIN VORGESEHEN, IST IHR AUSSCHLIESSLICHES RECHTSMITTEL.

IN KEINEM FALL IST ISTORAGE HAFTBAR FÜR VERLUSTE ODER ERWARTETE GEWINNE ODER FÜR MITTELBARE, STRAF-, BEISPIELHAFTE, BESONDERE, VERTRAUENS- ODER FOLGESCHÄDEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE, NUTZUNGSAUSFALL VON SOFTWARE, DATENVERLUST, ANDERWEITIGEN DATENVERLUST ODER -WIEDERHERSTELLUNG, SACHSCHÄDEN UND ANSPRÜCHE DRITTER, DIE SICH AUS EINER BELIEBIGEN WIEDERHERSTELLUNGSTHEORIE ERGEBEN, EINSCHLIESSLICH GARANTIE, VERTRAG, GESETZ ODER UNERLAUBTER HANDLUNG, UNABHÄNGIG DAVON, OB AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE. UNGEACHTET DER LAUFZEIT EINER BESCHRÄNKTEN GARANTIE ODER EINER GESETZLICH IMPLIZIERTEN GARANTIE ODER FÜR DEN FALL, DASS EINE BESCHRÄNKTE GARANTIE IHREN WESENTLICHEN ZWECK VERFEHLT, ÜBERSTEIGT DIE GESAMTE HAFTUNG VON ISTORAGE IN KEINEM FALL DEN KAUFPREIS DIESES PRODUKTS. | 4823-2548-5683.3

iStorage®

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, England
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
E-Mail: info@istorage-uk.com | Web: www.istorage-uk.com

iStorage®

DISKASHUR® 3 & DISKASHUR® PRO3

Manuale utente

Questo manuale d'uso è relativo a diskAshur³ e diskAshur PRO³, d'ora in poi indicati con il termine "diskAshur³"

Tenere a mente il proprio PIN (password): senza di esso non è possibile accedere ai dati sul disco.

Se si riscontrano difficoltà nell'uso di diskAshur³ si prega di contattare il nostro servizio assistenza via e-mail - support@istorage-uk.com o telefono al numero +44 (0) 20 8991 6260.

DISKASHUR® 3

iStorage®

RoHS Compliant

REACH COMPLIANCE

Conforme al Trade Agreements Act (TAA)

CITRIX® vmware®

Sommario

Introduzione 128
Contenuto della confezione 128
diskAshur³ Layout 128
1. LED e azioni relative 129
2. Stati dei LED 129
3. Primo utilizzo 130
4. Sbloccare diskAshur³ con il PIN amministratore 131
5. Accedere alla modalità amministratore 131
6. Cambiare il PIN amministratore 132
7. Impostazione di un criterio del PIN utente 133
8. Eliminare il criterio del PIN utente 134
9. Verificare il criterio del PIN utente 134
10. Aggiungere un nuovo PIN utente in modalità amministratore 135
11. Cambiare il PIN utente in modalità amministratore 136
12. Eliminare il PIN utente in modalità amministratore 136
13. Sbloccare diskAshur³ con il PIN utente 137
14. Cambiare il PIN utente in modalità utente 137
15. Accendere la tastiera a LED retroilluminata 138
16. Spegnere la tastiera LED retroilluminata 138
17. Creazione di un PIN di ripristino utente una tantum 139
18. Eliminazione del PIN di ripristino utente una tantum 139
19. Attivazione della modalità di ripristino e creazione di un nuovo PIN utente 140
20. Impostare la sola lettura per un utente in modalità amministratore 140
21. Abilitare la lettura/scrittura per un utente in modalità amministratore 141
22. Impostare la sola lettura globale in modalità amministratore 141
23. Abilitare la lettura/scrittura globale in modalità amministratore 142
24. Configurare il PIN di autodistruzione 142
25. Eliminare il PIN di autodistruzione 143
26. Eseguire lo sblocco con il PIN di autodistruzione 143
27. Configurare un PIN amministratore dopo un attacco "brute force" o un reset 144
28. Impostare il blocco automatico non presidiato 144
29. Disattivare il blocco automatico non presidiato 145
30. Verificare il blocco automatico non presidiato 146
31. Impostare la sola lettura nella modalità utente 146
32. Abilitare la lettura/scrittura in modalità utente 147
33. Meccanismo di difesa dagli attacchi "brute force" 147
34. Impostare il limite per gli attacchi "brute force" del PIN utente 148
35. Verificare il limite per gli attacchi "brute force" del PIN utente 149
36. Eseguire una reimpostazione completa 150
37. Configurare diskAshur³ come unità di avvio 150
38. Disattivare la funzione di avvio di diskAshur³ 151
39. Verificare l'impostazione di avvio 151
40. Configurare la modalità di crittografia 152
41. Verificare la modalità di crittografia 153
42. Configurare il tipo di disco 154
43. Controllare l'impostazione del tipo di disco 154
44. Inizializzazione e formattazione di diskAshur³ su Windows 155
45. Inizializzazione e formattazione di diskAshur³ su Mac OS 157
46. Inizializzare e formattare diskAshur³ su Linux 159
47. Ibernazione, sospensione o disconnessione dal sistema operativo 162
48. Verificare il firmware in modalità amministratore 162
49. Verificare il firmware in modalità utente 163
50. Supporto tecnico 164
51. Garanzia e informazioni sul reso 164

Introduzione

Grazie per aver acquistato la nuova unità iStorage diskAshur³/ diskAshur PRO³, di seguito denominata "diskAshur³".

diskAshur³ è un'unità portatile HDD/SSD facile da usare, ultra-sicura, protetta da password, con crittografia hardware e capacità fino a 5 TB (HDD) e 16 TB (SSD) e oltre. diskAshur³ esegue la crittografia dei dati in transito e di quelli inutilizzati mediante una procedura hardware a 256 bit.

diskAshur3 dispone di un microprocessore sicuro certificato Common Criteria EAL 5+ , che utilizza meccanismi di protezione fisica incorporati in grado di prevenire manomissioni esterne, attacchi di bypass e iniezioni di errore. A differenza delle altre soluzioni, diskAshur³ reagisce agli eventuali attacchi automatizzati attivando lo stato di blocco, che rende vano qualsiasi attacco. In parole chiare e semplici, senza PIN non è possibile accedere al disco.

Contenuto della confezione

- iStorage diskAshur³
- Custodia protettiva per il trasporto
- Cavi USB C e A
- Licenza gratuita di 1 anno di Nero BackItUp e iStorage DriveSecurity
- Guida rapida

Layout diskAshur3

1. Interfaccia USB 3,2 (Gen 1) Type-C
   Cavi USB Type C e A inclusi.
2. Luci LED
   ROSSO: modalità bloccata/standby. VERDE FISSO: sbloccato. VERDE LAMPEGGIANTE: trasferimento dati. BLU: modalità amministratore
3. Tastierino alfanumerico con rivestimento epossidico, resistente all'usura e con retroilluminazione selezionabile dall'utente.
4. Design a prova di manomissione e in grado di evidenziare gli eventuali tentativi di manomissione
   Tutti i componenti critici sono ricoperti da uno strato di resina epossidica super resistente.
5. Chip crittografico sul dispositivo.
6. Microprocessore sicuro con certificazione Common Criteria EAL 5+.
7. Pulsante SHIFT (Maiuscole)
8. Pulsante UNLOCK (Sblocca).
9. Slot per l'alloggiamento del dispositivo
10. La profondità dell'unità HDD da 4&5 TB è di 26,8 mm invece che di 20,8 mm.

1.LED e azioni relative

LED	Stato dei LED	Descrizione	LED	Stato dei LED	Descrizione
	ROSSO Fisso	Unità bloccata (negli stati di **standby** o **reset**)		BLU Fisso	Unità in **Modalità amministratore**
	ROSSO Doppio lampeggio	Inserimento del PIN errato		LED ROSSO, VERDE e BLU ampeggianti insieme	In attesa dell'inserimento del PIN **Utente**
	VERDE Fisso	Unità **sbloccata**		VERDE e BLU ampeggianti insieme	IIn attesa di inserimento del PIN **amministratore**
	VERDE Lampeggiante	Trasferimento dati in corso			

2. Stati dei LED

Ripristinare l'unità dallo stato di inattività

Lo stato di inattività si verifica quando l'unità è inutilizzata e tutti i LED sono spenti.

Per ripristinare diskAshur³ dallo stato di inattività, procedere come segue:

Collegare l'unità a una porta USB alimentata del computer in uso		Il LED diventa ROSSO fisso, a indicare che l'unità è in stato di standby

Entrare nello stato di inattività

Per collocare manualmente diskAshur³ nello stato di inattività, effettuare una delle seguenti operazioni:

- Espellere e scollegare in modo sicuro l'unità dal computer. Il LED ROSSO si spegnerà (stato di inattività).

Stati di accensione

Quando l'unità è stata ripristinata dallo stato di inattività, entrerà in uno degli stati indicati nella tabella seguente.

Stato di accensione	Indicazione LED	Chiave di crittografia	PIN amministratore	Descrizione
Stato di fabbrica	ROSSO e VERDE fisso	✓	×	Attesa della configurazione di un PIN amministratore (primo utilizzo)
Standby	ROSSO fisso	✓	✓	Attesa per l'inserimento del PIN amministratore, utente o di ripristino
Reset	ROSSO fisso	×	×	Attesa per la configurazione di un PIN amministratore

3.Primo utilizzo

iStorage diskAshur³ viene fornito nello **"Stato iniziale" senza alcun PIN amministratore preimpostato**. Configurare un PIN amministratore di **8-64** cifre prima di usare l'unità. Una volta configurato correttamente il PIN amministratore, non sarà possibile riportare l'unità allo "stato di fabbrica".

Requisiti del PIN:

- Deve essere lungo tra 8 e 64 cifre
- Non deve contenere solo numeri ripetitivi, es. (3-3-3-3-3-3-3-3)
- Non deve contenere solo numeri consecutivi, es. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- È possibile usare il tasto SHIFT (Maiuscole) per inserire combinazioni aggiuntive es.(**SHIFT** (⬆) **e 1** è un valore diverso dal solo 1).

Suggerimento per la password: è possibile inserire una parola, un nome, una frase facile da ricordare o qualsiasi altra combinazione alfanumerica da usare come PIN premendo il tasto dotato delle lettere corrispondenti.

Alcuni esempi di questo tipo di PIN alfanumerici:

- Per "**Password**" premere i seguenti pulsanti
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Per "**iStorage**" premere i seguenti pulsanti:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Utilizzando questo metodo è possibile creare PIN lunghi e facili da ricordare.

Per configurare un PIN amministratore e sbloccare diskAshur³ per la prima volta, attenersi ai semplici passi descritti nella tabella seguente.

Istruzioni per il primo utilizzo	LED	Stato dei LED
1. Collegare diskAshur³ a una porta USB alimentata del computer in uso		I LED ROSSO e VERDE fisso si accendono in modo fisso, a indicare che l'unità si trova nello stato di fabbrica
2. Tenere premuti entrambi i pulsanti **Unlock (Sblocca) (🔓) e1**		I LED diventano VERDE lampeggiante e BLU fisso
3. Inserire un **nuovo PIN** amministratore (8-64 cifre) e premere una volta il pulsante **Unlock (Sblocca) (🔓)**		Il LED VERDE lampeggiante e BLU fisso diventeranno un LED VERDE lampeggiante e quindi di nuovo uno VERDE lampeggiante e uno BLU fisso
4. Reinserire il **nuovo PIN** amministratore e premere il pulsante **Unlock (Sblocca) (🔓)** per una volta		Il LED BLU lampeggia rapidamente, quindi diventa BLU fisso e infine VERDE fisso, a indicare che il PIN amministratore è stato configurato correttamente e che l'unità è sbloccata e pronta per l'uso

Bloccare diskAshur³

Per bloccare il disco, espellerlo in modo sicuro dal sistema operativo e scollegarlo dalla porta USB. Se è in corso la scrittura di dati sull'unità, l'espulsione di diskAshur³ comporterà un trasferimento incompleto dei dati e il possibile danneggiamento degli stessi.

4. Sblocco di diskAshur³ con il PIN amministratore

Per sbloccare diskAshur³ con il PIN amministratore, attenersi ai semplici passaggi riportati nella tabella seguente:

1. Collegare diskAshur³ a una porta USB del computer in uso		Il LED diventa ROSSO fisso, a indicare che l'unità è in stato di standby
2. In stato di standby (LED ROSSO fisso), premere il pulsante **Unlock (Sblocca) (🔓)** per una volta		I LED VERDE e BLU lampeggiano insieme
3. Con i LED VERDE e BLU lampeggianti insieme, inserire il PIN amministratore e premere per una volta il pulsante **Unlock (Sblocca) (🔓)** per una volta		Il LED VERDE lampeggia più volte e quindi diventa VERDE fisso, a indicare che l'unità è stata sbloccata correttamente dall'amministratore ed è pronta per l'uso

5. Accedere alla modalità amministratore

Per entrare in modalità amministratore, procedere come segue.

1. Collegare diskAshur³ a una porta USB alimentata del computer in uso		Il LED diventa ROSSO fisso, a indicare che l'unità è in stato di standby
2. In stato di standby (LED ROSSO fisso), tenere premuti entrambi i pulsanti **Unlock (Sblocca) (🔓) e 1**		I LED VERDE e BLU lampeggiano insieme
3. Inserire il PIN amministratore e premere di nuovo il pulsante **Unlock (Sblocca) (🔓)**		Il LED BLU fisso si accende a indicare che l'unità è in modalità amministratore

Per uscire dalla modalità amministratore

Per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

6. Modifica del PIN amministratore

Requisiti del PIN:

- Deve essere lungo tra 8 e 64 cifre
- Non deve contenere solo numeri ripetitivi, es. (3-3-3-3-3-3-3-3)
- Non deve contenere solo numeri consecutivi, es. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- È possibile usare il tasto SHIFT (Maiuscole) per inserire combinazioni aggiuntive es.(**SHIFT** (⬆) **e 1** è un valore diverso dal solo 1).

Suggerimento per la password: È possibile configurare una parola, un nome, una frase o qualsiasi altra combinazione di PIN alfanumerici facile da ricordare semplicemente premendo il pulsante con le lettere corrispondenti.

Esempi di questi tipi di PIN alfanumerici sono i seguenti:

- Per "**Password**" premere i seguenti tasti:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Per "**iStorage**" premere i seguenti tasti:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Con questo metodo si possono configurare PIN lunghi e facili da ricordare.

Per modificare il PIN Amministratore, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLUE fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **KEY (🔓) + 2** buttons		Il LED BLU fisso sarà sostituito da LED VERDE lampeggiante e BLU fisso
2. Inserire il **Nuovo PIN Amministratore** e premere una volta il tasto **KEY (🔓)** button once		I LED VERDE lampeggiante e BLU fisso lampeggiano una volta in VERDE poi ridiventano VERDE lampeggiante e BLU fisso
3. Inserire il **Nuovo PIN Amministratore** e premere una volta il tasto **KEY (🔓)** button once		I LED VERDE lampeggiante e BLU fisso diventano BLU che lampeggia rapidamente e infine BLU fisso, a indicare che il PIN Amministratore è stato modificato con successo

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

7. Impostare una Politica Codice PIN Utente

L'amministratore può impostare regole restrittive per il PIN Utente Questa politica include l'impostazione di una lunghezza minima del PIN (da 8 a 64 cifre) e la possibilità di richiedere l'inserimento di uno o più "**Caratteri speciali**". Il "Carattere speciale" si ha quando entrambi i pulsanti "**SHIFT** (⬆) + **cifra**" vengono premuti insieme.

Per impostare una politica di PIN Utente (con restrizioni), è necessario inserire 3 cifre, ad esempio "**091**", le prime due cifre (**09**) indicano la lunghezza minima del PIN (in questo caso, **9**) e l'ultima cifra (**1**) indica che uno o più 'Caratteri speciali' devono essere utilizzati, in altre parole "**MAIUSCOLO (⬆) + cifra**". Allo stesso modo, è possibile impostare una Politica Codice PIN Utente senza richiedere alcun "Carattere speciale"; ad esempio in "**120**", le prime due cifre (**12**) indicano la lunghezza minima del PIN (in questo caso,**12**) e l'ultima cifra (**0**), il che significa che non è richiesto alcun Carattere speciale.

Una volta che l'amministratore ha impostato la Politica Codice PIN Utente, ad esempio "**091**", sarà necessario configurare un nuovo PIN utente - vedi Sezione 10 "Aggiunta di un Nuovo PIN Utente in Modalità amministratore". Se l'amministratore configura il PIN utente come "**247688314**" con l'uso di un "**Carattere speciale" (SHIFT (⬆) + cifra** premuti insieme), questo può essere posizionato in qualsiasi punto del PIN a 8-64 cifre durante il processo di creazione del PIN utente, come mostrato negli esempi seguenti.

A. '**SHIFT** (⬆) **+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',

B. '2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4',

C. '2', '4', '7', '6', '8', '8', '3', '1', '**SHIFT** (⬆) **+ 4**',

Nota:

- Se durante la configurazione del PIN Utente è stato utilizzato un "Carattere speciale", come nell'esempio "**B**" di cui sopra, l'unità può essere sbloccata solo inserendo il PIN con il "Carattere speciale" inserito esattamente nell'ordine configurato, come nell'esempio "**B**" di cui sopra - ('2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- More than one 'Special Character' can be used and placed along your 8-64 digit PIN.
- È possibile utilizzare più di un "Carattere speciale" e posizionarlo lungo il PIN a 8-64 cifre.
- Gli utenti possono modificare il proprio PIN, ma devono rispettare la "Politica Codice PIN Utente" (restrizioni), se e quando applicabile.
- L'impostazione di un nuovo codice PIN Utente cancella automaticamente il PIN Utente precedente se attivo.
- Questa politica non si applica al "PiN Auto-Cancellabile" L'impostazione della complessità per il PIN Auto-Cancellabile e il PIN Amministratore è sempre di 8-64 cifre, senza bisogno di caratteri speciali.

Per impostare una **Politica Codice PIN Utente**, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **KEY (🔓) + 7** buttons		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Inserire le proprie **3 cifre**, ricordando che le prime due cifre indicano la lunghezza minima del PIN e l'ultima cifra (0 o 1) se è stato utilizzato o meno un carattere speciale.		I LED VERDE e BLU lampeggianti continueranno a lampeggiare
3. Premere una volta il tasto **SHIFT** (⬆)		I LED VERDE e BLU lampeggianti diventano VERDE fisso e infine BLU fisso, a indicare che la Politica Codice PIN Utente è stata impostata con successo.

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

8. Eliminare il criterio del PIN utente

Per eliminare il **criterio del PIN utente**, entrare in "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **Unlock (Sblocca) (🔓) e 7**		Il LED BLU fisso diventerà VERDE e BLU lampeggiante
2. Inserire **080** e premere una volta il tasto **SHIFT (Maiuscole)** (⬆)		I LED VERDE e BLU lampeggianti diventeranno VERDE fisso e infine BLU fisso, a indicare la corretta eliminazione del criterio del PIN utente

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

9. Come verificare la Politica Codice PIN Utente

L'amministratore può verificare la Politica Codice PIN Utente, individuare la restrizione di lunghezza minima del PIN e se l'uso di un Carattere speciale è stato impostato o meno, annotando la sequenza di LED come descritto di seguito.

Per verificare la Politica Codice PIN Utente, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **SHIFT** (⬆) **+ 7**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premendo il tasto **KEY (🔓)** accade quanto segue; a. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. b. Un lampeggio del LED ROSSO equivale a dieci (10) unità di un PIN. c. Ogni lampeggio del LED VERDE equivale a dieci (1) unità di un PIN. d. Un lampeggio BLU indica che è stato utilizzato un 'Carattere speciale'. e. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. f. I LED ritornano al BLU fisso		

La tabella seguente descrive il comportamento del LED durante la verifica della Politica Codice PIN Utente; ad esempio se si è impostato un PIN Utente a 12 cifre con l'uso di un Carattere speciale (**121**), il LED ROSSO lampeggerà una volta (**1**) e il LED VERDE lampeggerà due volte (**2**) seguito da un singolo (**1**) lampeggio BLU che indica che è necessario utilizzare un **Carattere speciale**.

Descrizione PIN	**Configurazione a 3 cifre**	**ROSSO**	**VERDE**	**BLU**
PIN a 12 cifre con l'utilizzo di un Carattere speciale	121	1 Lampeggio	2 Lampeggi	1 Lampeggio
PIN a 12 cifre SENZA Caratteri speciali	120	1 Lampeggio	2 Lampeggi	0
PIN a 9 cifre con l'utilizzo di un Carattere speciale	091	0	9 Lampeggi	1 Lampeggio
PIN a 9 cifre SENZA Caratteri speciali	090	0	9 Lampeggi	0

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

10. Aggiunta di un nuovo PIN utente in modalità amministratore

Importante: la creazione di un nuovo PIN utente deve essere conforme al "criterio del PIN utente", se configurato come descritto nella sezione 7, aspetto che impone una lunghezza minima del PIN e l'utilizzo di un "carattere speciale". L'amministratore può consultare la sezione 9 per verificare le restrizioni del PIN utente.

Requisiti PIN:

- Deve essere di lunghezza compresa tra 8 e 64 cifre
- Non deve contenere solo numeri ripetitivi, ad esempio (3-3-3-3-3-3-3-3-3)
- Non deve contenere solo numeri consecutivi, ad esempio (1-2-3-4-4-5-6-7), (7-8-9-0-0-1-2-2-3-4), (7-6-5-4-3-2-1)
- Il tasto **SHIFT** (⬆) può essere utilizzato per ulteriori combinazioni - es. **SHIFT** (⬆) **+ 1** iè un valore diverso da solo 1. Vedere la sezione 7, “Impostare una Politica Codice PIN Utente”.

Per impostare un **Nuovo PIN Utente**, occorre prima entrare in “**Modalità amministratore**” come descritto nella sezione 5. Una volta che l’unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **KEY (🔓) + 3**		Il LED BLU fisso sarà sostituito da LED VERDE lampeggiante e BLU fisso
2. Inserire il **Nuovo PIN Utente** e premere il tasto **KEY (🔓)**		I LED VERDE lampeggiante e BLU fisso lampeggiano una volta in VERDE poi ridiventano VERDE lampeggiante e BLU fisso
3. Reinserire il **Nuovo PIN Utente** e premere il tasto **KEY (🔓)** nuovamente		I LED VERDE lampeggiante e BLU fisso diventano VERDE che lampeggia rapidamente e infine BLU fisso, a indicare che il Nuovo PIN Utente è stato configurato con successo

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

11. Modifica del PIN Utente in Modalità amministratore

Importante: La modifica del PIN Utente deve essere conforme alla "Politica Codice PIN Utente", se configurata come descritto nella sezione 7, che impone una lunghezza minima del PIN e l'eventuale richiesta di un "Carattere speciale". L'amministratore può fare riferimento alla sezione 9 per verificare le restrizioni del PIN Utente.

Per modificare un **PIN Utente esistente**, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **KEY (🔓) + 3**		Il LED BLU fisso sarà sostituito da LED VERDE lampeggiante e BLU fisso
2. Inserire il **Nuovo PIN Utente** e premere una volta il tasto **KEY (🔓)**		I LED VERDE lampeggiante e BLU fisso lampeggiano una volta in VERDE poi ridiventano VERDE lampeggiante e BLU fisso
3. Reinserire il **Nuovo PIN Utente** e premere il tasto **KEY (🔓)** una volta		I LED VERDE lampeggiante e BLU fisso diventano VERDE che lampeggia rapidamente e infine BLU fisso, a indicare il NPIN Utente è stato modificato con successo

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

12. Cancellare il PIN utente in Modalità amministratore

Per cancellare un PIN Utente esistente, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **SHIFT** (⬆) **+ 3**		Il LED BLU fisso diventa ROSSO lampeggiante
2. Premere e tenere premuti entrambi **SHIFT** (⬆) **+ 3** di nuovo		Il LED ROSSO lampeggiante diventa ROSSO fisso e infine BLU fisso, a indicare che il PIN Utente è stato eliminato con successo

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

13. Sbloccare diskAshur³ con il PIN utente

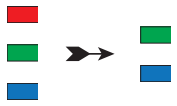
Per sbloccare diskAshur³ con il **PIN utente,** procedere come segue:

1. Nello stato di standby (LED ROSSO fisso), tenere premuti entrambi i pulsanti SHIFT (Maiuscole) (⬆) e **Unlock (Sblocca) (🔓)**		Il LED ROSSO lascerà il posto a tutti i LED, ROSSO, VERDE e BLU, lampeggianti
2. Inserire il **PIN utente** e premere una volta il pulsante **Unlock (Sblocca) (🔓)**		I LED ROSSO, VERDE e BLU lampeggianti diventeranno VERDE lampeggiante e quindi VERDE fisso, a indicare lo sblocco dell'unità in modalità utente

14. Cambiare il PIN utente in modalità utente

Importante:la modifica del PIN utente in modalità utente (LED VERDE) deve essere conforme al "criterio del PIN utente", se configurato come descritto nella sezione 7, che impone una lunghezza minima del PIN e l'utilizzo di un "carattere speciale".

Per modificare il **PIN utente**, sbloccare prima diskAshur³ usando il PIN utente come descritto nella sezione 13. Quando l'unità si trova in **modalità utente** (LED VERDE fisso) procedere con i seguenti passaggi:

1. In modalità utente (LED VERDE), tenere premuti entrambi i pulsanti **Unlock (Sblocca) (🔓) e 4**		Il LED VERDE fisso diventeràROSSO, VERDE e BLU lampeggiante
2. Immettere il proprio **PIN utente esistente** e premere una volta il pulsante **Unlock (Sblocca) (🔓)**		I LED diventeranno un solo LED VERDE lampeggiante e quindi un LED VERDE lampeggiante e uno BLU fisso
3. Inserire il **nuovo PIN utente** e premere una volta il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE lampeggiante e BLU fisso diventeranno un LED VERDE lampeggiante e quindi un LED VERDE lampeggiante e uno BLU fisso
4. Reinserire il nuovo PIN utente e premere il pulsante **Unlock (Sblocca)(🔓)** per una volta		I LED VERDE lampeggiante e BLU fisso si spegneranno, quindi si accenderà un LED VERDE lampeggiante rapidamente e quindi VERDE fisso, a indicare la corretta modifica del PIN utente

15. Accensione della tastiera a LED retroilluminata

Per migliorare la visibilità in condizioni di scarsa illuminazione, diskAshur³ è dotato di una tastiera retroilluminata a LED.Per accendere la tastiera retroilluminata a LED, attivare la "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **2 e 6**		Il LEDBLU fisso diventerà VERDE e BLU lampeggiante
2. Premere il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE e BLU lampeggianti diventeranno un LED VERDE fisso e quindi uno BLU fisso, a indicare l'attivazione della tastiera retroilluminata, che si accenderà alla prossima connessione dell'unità a una porta USB alimentata.

Nota: per eseguire l'attivazione, una volta configurato diskAshur³per accendere la tastiera retroilluminata a LED, scollegare e ricollegare l'unità dalla porta USB alimentata.Per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

16.Spegnimento della tastiera a LED retroilluminata

Per spegnere la tastiera retroilluminata a LED, accedere prima alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **2 e 3**		Il LEDBLU fisso diventerà VERDE e BLU lampeggiante
2. Premere il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE e BLU lampeggianti diventeranno un LED VERDE fisso e quindi uno BLU fisso, a indicare la disattivazione della tastiera retroilluminata, che si spegnerà alla prossima connessione dell'unità a una porta USB alimentata.

Nota: una volta configurato lo spegnimento della tastiera retroilluminata a LED di diskAshur³, per eseguire l'attivazione scollegare l'unità dalla porta USB alimentata, quindi ricollegarla.Per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

17. Creazione di un PIN di ripristino utente una tantum

Il PIN di ripristino utente è utile nelle situazioni in cui un utente dimentica il PIN necessario per sbloccare diskAshur³.
Per attivare la modalità di ripristino, inserire prima il corretto PIN di ripristino, se configurato. Il processo di ripristino del PIN utente non influisce sui dati, sulla chiave di crittografia e sul PIN amministratore, ma richiede la configurazione di un nuovo PIN utente di 8-64 cifre.

Per configurare il PIN di ripristino utente una tantum, lungo da 8 a 64 cifre, accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **Unlock (Sblocca) (🔓) e 4**		Il LEDBLU fisso diventerà VERDE lampeggiante e BLU fisso
2. Inserire il **PIN di ripristino una tantum** e premere il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE lampeggiante e BLU fisso diventeranno un LED VERDE lampeggiante e quindi un LED VERDE lampeggiante e uno BLU fisso
3. Reinserire il **PIN di ripristino una tantum** e premere nuovamente il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE lampeggiante e BLU fisso diventeranno un LED VERDE lampeggiante rapidamente e infine un LED BLU fisso, a indicare la corretta configurazione del PIN di ripristino una tantum

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)**(⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

18. Eliminare il PIN di ripristino utente una tantum

Per eliminare il PIN di ripristino utente una tantum, accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **SHIFT (Maiuscole)** (⬆) e **4**.		Il LED BLU fisso diventerà ROSSO lampeggiante
2. Tenere premuti entrambi i pulsanti **SHIFT (Maiuscole)** (⬆) **e** 4 ancora una volta		Il LED ROSSO lampeggiantediventerà ROSSO fisso e quindi BLU fisso, a indicare la corretta eliminazione del PIN di ripristino utente una tantum

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

19. Attivazione della modalità di ripristino e creazione di un nuovo PIN utente

Il PIN di ripristino utente è utile nelle situazioni in cui un utente dimentica il PIN necessario per sbloccare diskAshur³.
Per attivare la modalità di ripristino, inserire prima il corretto PIN di ripristino, se configurato. Il processo di ripristino del PIN utente non influisce sui dati, sulla chiave di crittografia e sul PIN amministratore, ma richiede la configurazione di un nuovo PIN utente di 8-64 cifre.

Per attivare il processo di ripristino e configurare un nuovo PIN utente, procedere come indicato di seguito.

1. Nello **stato di standby** (LED ROSSO), tenere premuti i pulsanti **Unlock (Sblocca) (🔓) e 4**		Il LED ROSSO fisso cambierà in ROSSO e VERDE lampeggiante
2. Inserire il **PIN di ripristino una tantum** e premere il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE e BLU lampeggeranno, per poi diventare VERDE fisso e infine VERDE lampeggiante e BLU fisso
3. Inserire un nuovo PIN utente e premere il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE lampeggiante e BLU fisso diventeranno un LED VERDE lampeggiante e quindi un LED VERDE lampeggiante e uno BLU fisso
4. Reinserire il nuovo PIN utente e premere nuovamente il pulsante **Unlock (Sblocca) (🔓)**		Il LED VERDE lampeggerà rapidamente, per poi diventare VERDE fisso, a indicare che il processo di ripristino è andato a buon fine e che è avvenuta la configurazione di un nuovo PIN utente

Importante: la creazione di un nuovo PIN utente deve essere conforme al "criterio del PIN utente", se configurato come descritto nella sezione 7, che impone una lunghezza minima del PIN e l'utilizzo di un carattere speciale. Consultare la sezione 9 per le restrizioni del PIN utente.

20. Impostare la sola lettura per un utente in modalità amministratore

Alla luce della grande quantità di virus e trojan in grado di colpire le unità USB, la funzione di sola lettura consente di accedere ai dati contenuti nell'unità USB negli ambienti pubblici. Si tratta di una funzionalità importante anche per scopi forensi, che richiedono la conservazione dei dati nello stato originario e inalterato, senza possibilità di modifica o sovrascrittura.

Quando l'amministratore configura diskAshur³ limitando l'accesso dell'utente in sola lettura, solo l'amministratore potrà scrivere sull'unità o modificare l'impostazione in "lettura/scrittura" come descritto nella sezione 21. L'utente potrà accedere solo in lettura senza la possibilità di scrivere sull'unità o modificare l'impostazione in modalità utente.

Per impostare diskAshur³ in modo da limitare l'accesso dell'utente in sola lettura, accedere prima alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In Modalità amministratore premere e tenere premuti entrambi i tasti "**7 + 6**".		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premere una volta il tasto **KEY (🔓)**		I LED VERDE e BLU saranno sostituiti da LED VERDE fisso e poi BLU fisso, a indicare che l'unità è stata configurata e limita l'accesso dell'Utente alla Sola Lettura Utente.

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

21. Abilitare Lettura/Scrittura Utente in Modalità

Per reimpostare diskAshur3 e consentire la Lettura/Scrittura, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti "**7 + 9**".		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premere una volta il tasto **KEY (🔓)**		I LED VERDE e BLU diventano VERDE fisso e poi BLU fisso che indica che l'unità è configurata per la Lettura/Scrittura

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

22. Impostare la sola lettura globale in modalità amministratore

Quando l'amministratore configura diskAshur³ in sola lettura a livello globale, l'amministratore e l'utente non potranno scrivere sull'unità, ma solo accedervi in lettura. Solo l'amministratore può modificare l'impostazione in lettura/scrittura, come descritto nella sezione 23.

Per impostare diskAshur³ in modo da limitare l'accesso in sola lettura globale, accedere prima alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti "**5 e 6**" .		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti
2. Premere il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE e BLU diventeranno VERDE fisso e quindi BLU fisso, a indicare l'avvenuta configurazione dell'unità con accesso globale in sola lettura

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

23. Abilitare la lettura/scrittura globale in modalità amministratore

Per riportare diskAshur³ in modalità lettura/scrittura dopo l'impostazione globale della modalità di sola lettura, accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti "**5 e 9**" .		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti
2. Premere il pulsante **Unlock (Sblocca) (🔓)**		I LED VERDE e BLU diventeranno VERDE fisso e quindi BLU fisso, a indicare che l'unità è configurata in lettura/scrittura

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

24. Configurare il PIN di autodistruzione

È possibile configurare un PIN di autodistruzione che, una volta inserito, esegua una cancellazione crittografica dell'unità, compresa la chiave di crittografia e tutti i PIN configurati, rendendo inaccessibili tutti i dati memorizzati sull'unità per sempre. Quindi, l'unità viene visualizzata come sbloccata (LED VERDE). Eseguendo questa funzione, il PIN di autodistruzione diventerà il nuovo PIN utente e occorrerà formattare l'unità prima di poterla riutilizzare.

Per impostare il PIN Auto-Cancellabile, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti i tasti **KEY (🔓) + 6**		Il LED BLU fisso sarà sostituito da LED VERDE lampeggiante e BLU fisso
2. Configurare e inserire un **PIN Auto-Cancellabile** di 8-64 cifre e premere il tasto **KEY (🔓)**		I LED VERDE lampeggiante e BLU fisso lampeggiano una volta in VERDE poi ridiventano VERDE lampeggiante e BLU fisso
3. Inserire nuovamente il **PIN Auto-Cancellabile** e premere il tasto **KEY (🔓)**		Il LED VERDE lampeggia rapidamente per diversi secondi e poi diventa BLU fisso, a indicare che il PIN Auto-Cancellabile è stato configurato con successo

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

25. Come cancellare il PIN Auto-Cancellabile

Per cancellare il PIN Auto-Cancellabile, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **SHIFT (⬆) + 6**		Il LED BLU fisso diventa ROSSO lampeggiante
2. Premere e tenere premuti entrambi i tasti **SHIFT (⬆) + 6**		Il LED ROSSO lampeggiante diventa fisso e diventa BLU fisso, indicando che il PIN Auto-Cancellabile è stato cancellato con successo

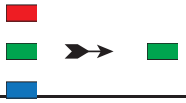
Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

26. Eseguire lo sblocco con il PIN di autodistruzione

Attenzione: attivando il meccanismo di autodistruzione, tutti i dati, la chiave di crittografia e i PIN amministratore/utente verranno eliminati.**Il PIN di autodistruzione diventerà il PIN utente.** Dopo l'attivazione del meccanismo di autodistruzione non sarà presente alcun PIN amministratore. Occorrerà reimpostare diskAshur³ (vedi "Eseguire una reimpostazione completa", sezione 36, pagina 150) per configurare un PIN amministratore dotato di tutti i privilegi amministrativi, compresa la possibilità di configurare un nuovo PIN utente.

Se utilizzato, il PIN di autodistruzione **eliminerà TUTTI i dati, la chiave di crittografia, i PIN amministratore/utente** e quindi sbloccherà l'unità. Attivando questa funzione, il PIN di autodistruzione **diventerà il nuovo PIN utente** e occorrerà formattare diskAshur³ per aggiungere nuovi dati all'unità.

Per attivare il meccanismo di autodistruzione, l'unità deve trovarsi nello stato di standby (LED ROSSO fisso). Quindi, sarà possibile procedere con i seguenti passaggi:

1. In **stato di standby** (LED ROSSO fisso), tenere premuti entrambi i pulsanti **SHIFT (Maiuscole)** (⬆) e **Unlock (Sblocca) (🔓)**		Il LED ROSSO lascerà il posto a tutti i LED, ROSSO, VERDE e BLU, lampeggianti
2. Inserire il **PIN di autodistruzione** e premere il pulsante **Unlock (Sblocca) (🔓)**		I LED ROSSO, VERDE e BLU lampeggiante diventeranno VERDE lampeggiante e quindi VERDE fisso, a indicare l'avvenuta autodistruzione di diskAshur³

27. Come configurare un PIN Amministratore dopo un Attacco

Dopo un Attacco di Forza Bruta o quando diskAshur³ è stato resettato occorre configurare un PIN Amministratore prima di potere utilizzare l'unità.

Requisiti PIN:

- Deve essere di lunghezza compresa tra 8 e 64 cifre
- Non deve contenere solo numeri ripetitivi, ad esempio (3-3-3-3-3-3-3-3-3)
- Non deve contenere solo numeri consecutivi, ad esempio (1-2-3-4-4-5-6-7), (7-8-9-0-0-1-2-2-3-4), (7-6-5-4-3-2-1)
- Il tasto **SHIFT** (⬆) può essere utilizzato per ulteriori combinazioni - es. **SHIFT** (⬆) **+ 1** iè un valore diverso da solo 1. Vedere la sezione 7, "Impostare una Politica Codice PIN Utente".

Se diskAshur³ è stato sottoposto a un Attacco di Forza Bruta o a reset, l'unità si troverà in Stato di standby (LED ROSSO fisso).
Per configurare un PIN Amministratore, procedere come segue.

1. In Stato di Standby (LED ROSSO fisso), premere e tenere premuti entrambi i tasti **SHIFT** (⬆) **+ 1**		Il LED ROSSO fisso sarà sostituito da LED VERDE lampeggiante e BLU fisso
2. Inserire il Nuovo PIN Amministratore e premere il tasto **KEY (🔓)**		I LED VERDE lampeggiante e BLU fisso lampeggiano una volta in VERDE poi ridiventano VERDE lampeggiante e BLUfisso
3. Inserire il Nuovo PIN Amministratore e premere il tasto **KEY (🔓)**		Il LED VERDE lampeggiante e BLU fisso diventano un BLU che lampeggia rapidamente per alcuni secondi infine e poi BLU fisso, a indicare che il PIN Amministratore è stato configurato con successo.

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

28. Impostare il Blocco Automatico Incustodito

Per proteggersi da accessi non autorizzati se l'unità è sbloccata e incustodita, diskAshur³ può essere impostato in modo da bloccarsi automaticamente dopo un periodo di tempo prestabilito. Nel suo stato predefinito, la funzione di time-out del Blocco Automatico Incustodito di diskAshur³ è disattivata. È possibile impostare il Blocco Automatico Incustodito perché si attivi dopo un lasso di tempo compreso tra i 5 e i 99 minuti.

Per impostare la funzione di time-out del Blocco Automatico Incustodito, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti **KEY (🔓) + 5**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Inserire il lasso di tempo desiderato per la funzione di time-out del Blocco Automatico: il tempo minimo impostabile è di 5 minuti, quello massimo di 99 minuti (5-99 minuti). Ad esempio, inserire: **05 per 5 minuti (premere '0' seguito da un '5')** **20 per 20 minuti (premere '2' seguito da uno '0')** **99 per 99 minuti (premere '9' seguito da un altro '9')**		
3. Premere il tasto **SHIFT** (⬆)		I LED VERDE e BLU lampeggianti diventano VERDE fisso per un secondo e infine BLU fisso, a indicare che il timeout del Blocco Automatico è stato configurato con successo.

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

29. Disattivare il Blocco Automatico Incustodito

Per disattivare la funzione di time-out del Blocco Automatico Incustodito, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti entrambi i tasti i tasti **KEY (🔓) + 5**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Inserire **00** e premere una volta il tasto **SHIFT** (⬆)		I LED VERDE e BLU lampeggianti diventeranno VERDE fisso per un secondo e infine BLU fisso, a indicare che il time-out del Blocco Automatico è stato disattivato con successo.

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

30. Come verificare il Blocco Automatico Incustodito

L'Amministratore può controllare e determinare la durata impostata della funzione di time-out del Blocco Automatico Incustodito semplicemente annotando la sequenza di LED come descritto nella tabella sottostante.

Per verificare il Blocco Automatico Incustodito, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità amministratore premere e tenere premuti **SHIFT** (⬆) **+ 5**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premendo il tasto **KEY (🔓)** accade quanto segue; a. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. b. Un lampeggio del LED ROSSO equivale a dieci (10) minuti. c. Un lampeggio del LED VERDE equivale a un (1) minuto. d. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. e. I LED ritornano al BLU fisso		

La tabella seguente descrive il comportamento dei LED durante la verifica del Blocco Automatico Incustodito, ad esempio se si è impostata l'unità in modo che si blocchi automaticamente dopo **25** minuti, il LED ROSSO lampeggerà due volte (**2**) e il LED VERDE lampeggerà cinque (**5**) volte.

Blocco Automatico in minuti	ROSSO	VERDE
5 minuti	0	5 Lampeggi
15 minuti	1 Lampeggio	5 Lampeggi
25 minuti	2 Lampeggi	5 Lampeggi
40 minuti	4 Lampeggi	0

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

31. Impostare Sola Lettura in Modalità Utente

Per impostare diskAshur3 in modalità Sola Lettura, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 13. Una volta che l'unità è in modalità utente (LED VERDE fisso) procedere come segue.

1. In Modalità Utente, premere e tenere premuti entrambi i tasti "**7 + 6**" (7=**R**ead + 6=**O**nly) (sola lettura)		Il LED VERDE fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premere il tasto **KEY (🔓)**		I LED VERDE e BLU diventeranno VERDE fisso, a indicare che l'unità è configurata come Sola Lettura

Nota: 1. Se un Utente ha impostato l'unità come Sola Lettura, l'Amministratore può annullare questa impostazione impostando l'unità come Lettura/Scrittura in Modalità amministratore.

2. Se l'Amministratore ha impostato l'unità come Sola Lettura, l'Utente non può impostare l'unità come Lettura/Scrittura.

32. Attivare Lettura/Scrittura in Modalità Utente

Per impostare diskAshur3 in modalità Lettura/Scrittura, occorre prima entrare in "Modalità utente" come descritto nella sezione 13. Una volta che l'unità è in Modalità utente (LED VERDE fisso) procedere come segue.

1. In Modalità Utente, premere e tenere premuti entrambi i tasti "**7 + 9**" (7=**R**ead + 9=**W**rite) (7=lettura + 9 = scrittura)		Il LED VERDE fisso si trasformerà in LED VERDE e BLU lampeggianti
2. Premere il tasto **KEY (🔓)**		I LED VERDE e BLU diventerà VERDE fisso, a indicare che l'unità è configurata come Lettura/Scrittura

Nota: 1. Se un Utente ha impostato l'unità come Sola Lettura, l'Amministratore può annullare questa impostazione impostando l'unità come Lettura/Scrittura in Modalità amministratore.

2. Se l'Amministratore ha impostato l'unità come Sola Lettura, l'Utente non può impostare l'unità come Lettura/Scrittura.

33. Meccanismo di difesa dagli attacchi "brute force"

diskAshur³ dispone di un meccanismo di difesa che protegge l'unità da un attacco "brute force". Per impostazione predefinita, il limite per gli attacchi "brute force" per il **PIN amministratore** e il **PIN utente** è impostato su **10** inserimenti consecutivi di un PIN errato, mentre per il **PIN di ripristino** è pari a **5** tentativi. Tre contatori "brute force" indipendenti registrano i tentativi errati per ciascuna autorizzazione del PIN. Se un utente inserisce un PIN amministratore errato per dieci volte consecutive (suddivise in gruppi di 5, 3 e 2, come descritto di seguito) l'unità verrà reimpostata e tutti i dati andranno perduti per sempre. Se un utente inserisce un PIN di ripristino o un PIN utente errato superando il limite per gli attacchi "brute force" corrispondente, i PIN corrispondenti verranno eliminati, ma i dati resteranno presenti sull'unità.

Nota: il limite per gli attacchi "brute force" viene riportato sui valori iniziali quando l'unità viene completamente reimpostata o viene attivata la funzione di autodistruzione. Se l'amministratore modifica il PIN utente o ne imposta uno nuovo attivando la funzione di ripristino, il contatore del PIN utente per gli attacchi "brute force" viene azzerato, ma il limite per gli attacchi "brute force" non viene interessato in alcun modo. Se l'amministratore modifica il PIN di ripristino, il contatore degli attacchi "brute force" del PIN di ripristino viene azzerato.

L'autorizzazione di un determinato PIN azzera il contatore "brute force" per tale PIN, ma non influisce su quello degli altri PIN. La mancata autorizzazione di un determinato PIN incrementerà il contatore "brute force" per tale PIN specifico, ma non influirà su quello degli altri PIN.

- Se un utente inserisce un **PIN utenteerrato** per 10 volte consecutive, tale PIN utente verrà eliminato, ma i dati, il PIN amministratore e quello di ripristino resteranno intatti e accessibili.
- Se viene immesso un **PIN di ripristino** erroneo per 5 volte consecutive, il PIN di ripristino verrà eliminato, ma i dati e il PIN amministratore resteranno intatti e accessibili.
- Il **PIN amministratore** utilizza un meccanismo di difesa più sofisticato rispetto ai PIN utente e di ripristino. Dopo **5 inserimenti consecutivi del PIN amministratore errato**, l'unità verrà bloccata e i LED **ROSSO**, **VERDE** e **BLU** si accenderanno, restando fissi. A questo punto occorrerà procedere come segue per consentire all'utente di inserire altri **3** PIN.

- Inserire il PIN "**47867243**" e premere il tasto **KEY (Chiave) (🔓)** : i LED **VERDE** e **BLU** lampeggeranno entrambi. L'unità è pronta ad accettare altri **3** tentativi di immissione del PIN amministore
- Dopo un totale di 8 tentativi consecutivi di immissione del PIN amministratore errato, l'unità si bloccherà e i LED **ROSSO**, **VERDE** e **BLU** lampeggeranno alternativamente. A questo punto, per ottenere gli ultimi **2** tentativi di inserimento del PIN (per un totale di 10), eseguire i seguenti passaggi.
- Inserire il PIN "**47867243**" e premere il tasto **KEY (Chiave) (🔓)** . I LED **VERDE** e **BLU** lampeggeranno assieme, indicando che l'unità è pronta ad accettare gli ultimi **2** tentativi di inserimento del PIN (per un totale di 10).
- Dopo un totale di 10 tentativi errati di immissione del PIN amministratore, la chiave di crittografia verrà eliminata e tutti i dati e PIN memorizzati sull'unitàandranno perduti per sempre.

La tabella seguente ipotizza l'impostazione di tutti i tre PIN ed evidenzia l'effetto dell'attivazione del meccanismo di difesa dagli attacchi "brute force" per ciascun singolo PIN.

PIN per lo sblocco dell'unità	Inserimento consecutivo di un PIN errato	Descrizione dell'azione eseguita dal prodotto
PIN utente	10	• Il PIN utente viene eliminato. • Il PIN di ripristino, il PIN amministratore e tutti i dati resteranno intatti e accessibili.
PIN di ripristino	5	• Il PIN di ripristino viene eliminato. • Il PIN amministratore e tutti i dati resteranno intatti e accessibili.
PIN amministratore	5 3 2 (10 in totale)	• Dopo **5** inserimenti consecutivi del PIN amministratore errato, l'unità si bloccherà e tutti i LED si accenderanno in modo fisso. • Immettere il PIN "**47867243**" e premere il tasto **KEY (Chiave) (🔓)** per ottenere altri **3** tentativi per l'inserimento del PIN. • Dopo un totale di **8** (5+3) inserimenti consecutivi di un PIN amministratore errato, l'unità viene bloccata e i LED lampeggiano in modo alternato. • Immettere il PIN "**47867243**" e premere il tasto **KEY (Chiave) (🔓)** per ottenere gli ultimi **2** tentativi di immissione del PIN (per un totale di 10). • Dopo un totale di 10 tentativi di inserimento consecutivi del PIN amministratore errato, la chiave di crittografia verrà eliminata e tutti i dati e PIN memorizzati sull'unità andranno perduti per sempre.

Importante: configurare un nuovo PIN amministratore se quello preesistente è stato sottoposto a un attacco "brute force". Fare riferimento alla sezione 27, pagina 144, "Configurare un PIN amministratore dopo un attacco brute force o un reset". Inoltre, occorrerà formattare diskAshur³ prima di aggiungere nuovi dati all'unità.

34. Impostare il limite per gli attacchi "brute force" del PIN utente

Nota: l'impostazione del limite per gli attacchi "brute force" del PIN utente è predefinita a 10 inserimenti consecutivi di un PIN errato quando l'unità viene completamente reimpostata, sottoposta a un attacco "brute force" o nel caso in cui venga attivato il PIN di autodistruzione.

L'amministratore può riprogrammare e impostare il limite per gli attacchi "brute force" per il PIN utente di diskAshur³. È possibile impostare questa funzione per consentire da 1 a 10 inserimenti consecutivi dei PIN errati.

Per configurare il limite per gli attacchi "brute force" per il PIN utente, accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **7 e 0**		Il LED BLU fisso lascerà il passo ai LED VERDE e BLU lampeggianti insieme
2. Inserire il numero di tentativi per il limite per gli attacchi "brute force" (01-10), ad esempio: • **01** per 1 tentativo • **10** per 10 tentativi		
3. Premere il pulsante **SHIFT (Maiuscole)** (⬆) per una volta.		I LED VERDE e BLU lampeggianti diventeranno VERDE fisso per un secondo e quindi BLU fisso, a indicare la corretta configurazione del limite per gli attacchi "brute force"

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

35. Verificare il limite per gli attacchi "brute force" del PIN utente

L'amministratore può osservare e determinare il numero di volte consecutive in cui è consentito inserire un PIN utente errato prima di attivare il meccanismo di difesa dagli attacchi "brute force" osservando la sequenza di LED descritta di seguito:

Per verificare l'impostazione del limite per gli attacchi "brute force", accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **Modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **2** e **0**		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti
2. Premere il pulsante **Unlock (Sblocca) ()** per eseguire quanto segue. a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo. b. Ciascun lampeggio del LED ROSSO equivale a dieci (10) unità del numero limite per gli attacchi "brute force". c. Ogni lampeggio del LED VERDE equivale a una (1) singola unità del numero limite per gli attacchi "brute force". d. Tutti i LED (ROSSO, VERDE e BLU) diventeranno fissi per 1 secondo. e. I LED tornano BLU fisso		

La tabella seguente descrive il comportamento dei LED durante il controllo dell'impostazione del limite per gli attacchi "brute force". Ad esempio, se tale limite è stato impostato su **5** inserimenti consecutivi di un PIN errato, il LED VERDE lampeggerà cinque (**5**) volte.

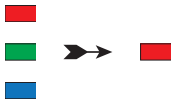
Impostazione del limite per gli attacchi "brute force"	**ROSSO**	**VERDE**
2 tentativi	0	2 lampeggi
5 tentativi	0	5 lampeggi
10 tentativi	1 lampeggio	0

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

Nota: Per uscire immediatamente dalla Modalità amministratore (LED BLU fisso), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

36. Come eseguire un reset completo

Per eseguire un reset completo, diskAshur³ deve essere in stato di standby (LED ROSSO fisso). Una volta che l'unità è stata resettata, allora tutti i PIN Amministratore/Utente, la chiave di crittografia e tutti i dati saranno cancellati e persi per sempre e l'unità dovrà essere formattata prima di poter essere riutilizzata. Per resettare diskAshur³, procedere come segue.

1. In stato di standby (LED ROSSO fisso) , premere e tenere premuto il tasto "**0**"		Il LED ROSSO fisso sarà sostituito dai LED ROSSO, VERDE e BLU che si attivano e disattivano
2. Premere e tenere premuti entrambi i tasti **2 + 7**		I LED ROSSO, VERDE e BLU alternati diventeranno fissi per un secondo, per essere sostituiti da un ROSSO fisso a indicare che l'unità è stata resettata

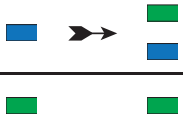
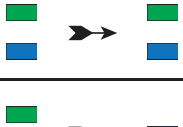
Importante: ADopo un reset completo occorre configurare un Nuovo PIN Amministratore; fare riferimento alla Sezione 27 a pagina 144 su "Come configurare un PIN Amministratore dopo un Attacco di Forza Bruta o un Reset". Inoltre, diskAshur³ dovrà essere formattato prima di poter aggiungere nuovi dati all'unità.

37. Configurare diskAshur³ come unità di avvio

Nota: quando l'unità è impostata come avviabile, l'espulsione della stessa dal sistema operativo non farà diventare il LED ROSSO. L'unità resterà VERDE fisso e occorrerà scollegarla per l'uso successivo. L'impostazione predefinita di diskAshur³ è "non di avvio".

diskAshur³ è dotato di una funzione di avvio, che consente di accendere e spegnere il sistema durante il processo di avvio dell'host. Quando si esegue l'avvio da diskAshur³, il computer caricherà il sistema operativo installato su diskAshur³.

Per configurare l'unità come di avvio, accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **Unlock (Sblocca) e 9**		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti
2. Premere **"0"** e quindi **"1"** (**01**)		I LED VERDE e BLU continueranno a lampeggiare
3. Premere il pulsante **SHIFT (Maiuscole)** (⬆) per una volta.		I LED VERDE e BLU lampeggianti diventeranno VERDE fisso e infine BLU fisso, a indicare la corretta configurazione dell'unità come di avvio

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

38. Disattivare la funzione di avvio di diskAshur³

Per disabilitare la funzione di avvio di diskAshur³, accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **Unlock (Sblocca) e 9**		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti
2. Premere **"0"** e quindi **"0"** (**00**)		I LED VERDE e BLU continueranno a lampeggiare
3. Premere il pulsante **SHIFT (Maiuscole)** (⬆) per una volta.		I LED VERDE e BLU lampeggianti diventeranno VERDE fisso e infine BLU fisso, a indicare la corretta disabilitazione della funzione di avvio dell'unità

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

39. Verificare l'impostazione di avvio

Per verificare l'impostazione di avvio, accedere alla "**modalità amministratore**" come descritto nella sezione 5. Quando l'unità si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **SHIFT (Maiuscole)** (⬆) **e 9**		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti

2. Premere il pulsante **Unlock (Sblocca) (🔓)** per attivare uno dei due scenari seguenti:

- **Se diskAshur³ è configurato come di avvio, si verifica quanto segue:**

a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
b. Il LED VERDE lampeggia una volta.
c. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
f. I LED tornano BLU fisso

- **Se diskAshur³ <u>NON</u> è configurato come di avvio, si verifica quanto segue:**

a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
b. Tutti i LED si spengono
c. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
f. I LED tornano BLU fisso

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

40. Configurare la modalità di crittografia

ATTENZIONE: la modifica della modalità di crittografia da AES-XTS (predefinita) a AES-ECB o AES-CBC eliminerà la chiave crittografica causando la reimpostazione di diskAshur³, che renderà tutti i dati inaccessibili e perduti per sempre.

Eseguire i seguenti passaggi per configurare la modalità di crittografia di diskAshur³ su **AES-ECB**, indicata dal numero **"01"**, su **AES-XTS**, indicata da **"02",** o **AES-CBC**, indicata da **"03"**. Per impostazione predefinita, questa funzione è AES-XTS (02). Attivando una diversa modalità di crittografia, tutti i parametri critici verranno eliminati e l'unità verrà reimpostata.

Per impostare la modalità della crittografia di diskAshur³, entrare in **modalità amministratore** come descritto nella sezione 5. Quando diskAshur³ si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **KEY (Chiave) (🔓) e 1**.		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti
2. Digitare **01** per impostare **AES-ECB** Digitare **02** per impostare **AES-XTS (predefinito)** Digitare **03** per impostare **AES-CBC**		I LED VERDE e BLU continueranno a lampeggiare
3. Premere il pulsante **SHIFT (Maiuscole)** (⬆) per una volta.		I LED VERDE e BLU diventeranno VERDE fisso e quindi ROSSO fisso (**stato di reimpostazione**) a indicare che la modalità di crittografia è stata modificata correttamente

Importante: dopo aver configurato la modalità di crittografia, diskAshur³ viene reimpostato completamente e occorrerà configurare un nuovo PIN amministratore (fare riferimento alla Sezione 27 a pagina 144 su "Configurare un PIN amministratore dopo un attacco brute force o un reset").

41. Verificare la modalità di crittografia

Per verificare la modalità di crittografia di diskAshur³, accedere prima alla **modalità amministratore** come descritto nella sezione 5. Quando l'unità si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **SHIFT (Maiuscole)** (⬆) e **1**		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti

2. Premere il pulsante **KEY (Chiave) (🔓)** per eseguire quanto segue:

- **Se la modalità di crittografia è configurata su AES-ECB, si verifica quanto segue:**

a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
b. Il LED VERDE lampeggia una volta.
c. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
f. I LED tornano BLU fisso

- **Se la modalità di crittografia è configurata su AES-XTS, si verifica quanto segue:**

a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
b. Il LED VERDE lampeggia due volte.
c. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
f. I LED tornano BLU fisso

- **Se la modalità di crittografia è configurata su AES-CBC, si verifica quanto segue:**

a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
b. Il LED VERDE lampeggia tre volte.
c. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
f. I LED tornano BLU fisso

Nota: per uscire immediatamente dalla modalità amministratore (LED BLU fisso), tenere premuto il pulsante **SHIFT (Maiuscole)** (⬆) per un secondo: il LED BLU fisso diventerà ROSSO fisso.

42. Configurare il tipo di disco

È possibile configurare diskAshur³ come "Removable Disk" (disco removibile) o "Disco locale (stato predefinito)". Scegliendo un altro tipo di disco, tutti i parametri critici verranno eliminati, così come tutti i PIN, la chiave di crittografia e i dati, collocando l'unità nello stato di reimpostazione.

ATTENZIONE: la modifica del tipo di disco da "Removable Disk" (disco removibile) o "Local Disk" (disco locale, predefinita) eliminerà la chiave crittografica e causerà la reimpostazione di diskAshur³, rendendo tutti i dati inaccessibili e perduti per sempre.

Eseguire i seguenti passaggi per configurare il tipo di disco di diskAshur³ come Removable Disk (disco removibile) (**00**) o Local Disk (disco locale) (**01**). Questa funzione è Local Disk (disco locale) (**01**) per impostazione predefinita. Passando a una tipo di disco diversa, tutti i parametri critici verranno eliminati causando la reimpostazione dell'unità.

Per impostare la tipo di disco di diskAshur³, entrare in **modalità amministratore** come descritto nella sezione 5. Quando diskAshur³ si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **KEY (Chiave) (🔓) e 8**.		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti
2. Digitare **00** per impostare **"Removable Disk" (disco removibile)** Digitare **01** per impostare **"Local Disk" (disco locale, predefinita)**		I LED VERDE e BLU continueranno a lampeggiare
3. Premere il pulsante **SHIFT (Maiuscole)** (⬆) per una volta.		I LED VERDE e BLU diventeranno VERDE fisso e quindi ROSSO fisso (**stato di reimpostazione**) a indicare la corretta modifica del tipo di disco

Importante: dopo aver modificato il tipo di disco, diskAshur³ verrà reimpostato completamente e occorrerà configurare un nuovo PIN amministratore (fare riferimento alla sezione 27 a pagina 144 "Configurare un PIN amministratore dopo un attacco "brute force" o un reset").

43. Controllare l'impostazione del tipo di disco

Per verificare l'impostazione del tipo di disco di diskAshur³, accedere prima alla **modalità amministratore** come descritto nella sezione 5. Quando l'unità si trova in **modalità amministratore** (LED BLU fisso) procedere con i seguenti passaggi:

1. In modalità amministratore, tenere premuti entrambi i pulsanti **SHIFT (Maiuscole)** (⬆) e **8**		Il LED BLU fisso cederà il passo ai LED VERDE e BLU lampeggianti

2. Premere il pulsante **KEY (Chiave) (🔓)** per eseguire quanto segue:

- **Se il tipo di disco è configurato come "Removable" (Removibile), si verifica quanto segue:**

a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo e quindi si spengono.
b. Tutti i LED (ROSSO, VERDE e BLU) diventano di nuovo fissi per 1 secondo e quindi si spengono.
d. I LED tornano BLU fisso

- **Se il tipo di disco è configurato come "Local" (Locale), si verifica quanto segue:**

a. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
b. Il LED VERDE lampeggia una volta.
c. Tutti i LED (ROSSO, VERDE e BLU) diventano fissi per 1 secondo.
f. I LED tornano BLU fisso

44. Inizializzazione e formattazione di diskAshur³ su Windows

Dopo un attacco "brute force" o una reimpostazione completa, diskAshur³ eliminerà tutti i PIN, i dati e la chiave di crittografia. Occorrerà inizializzare e formattare diskAshur³ prima di poterlo utilizzare.

Per formattare diskAshur³, procedere come segue:

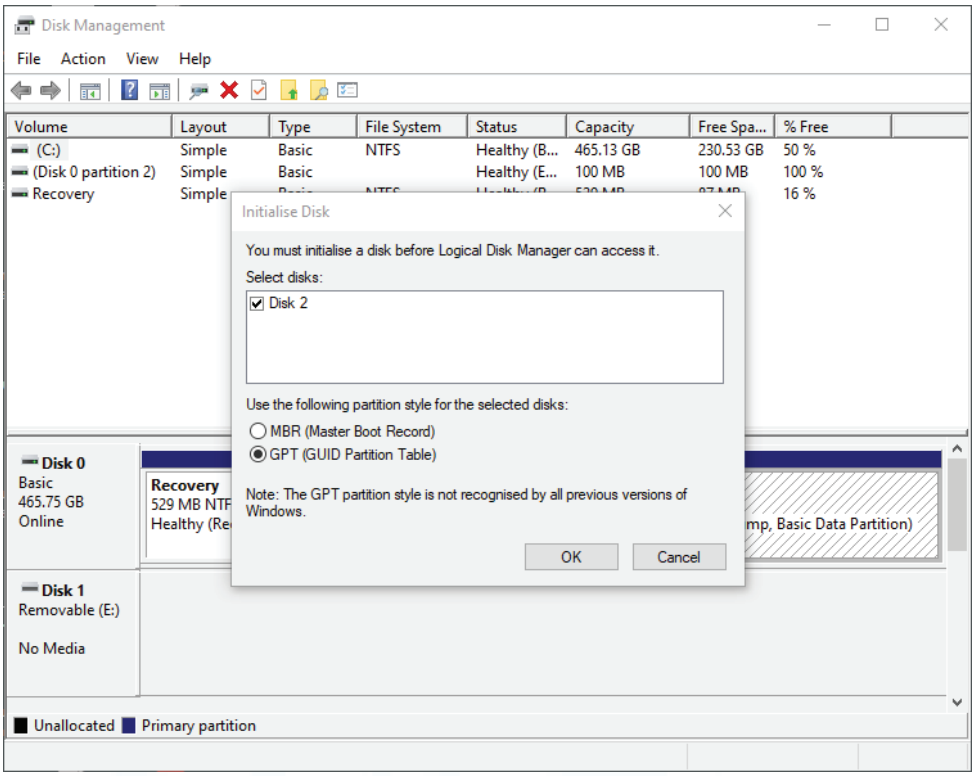
1. Configurare un nuovo PIN amministratore, vedere a pagina 144, sezione 27 "Configurare un PIN amministratore dopo un attacco "brute force" o un reset".

2. Quando diskAshur³ è in stato di standby (LED ROSSO), premere una volta il pulsante **Unlock (Sblocca) ()** e digitare il **nuovo PIN amministratore** per eseguire lo sblocco (LED VERDE lampeggiante).

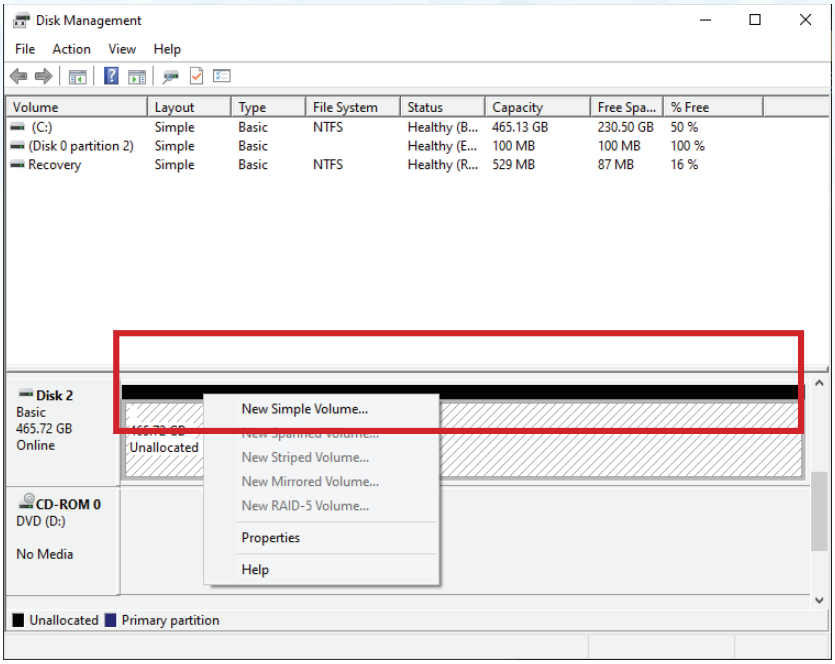
3. **Windows 7:** fare clic con il tasto destro del mouse su **Computre** e quindi su **Gestione**. Infine, selezionare **Gestione disco**
   Windows 8: fare clic con il tasto destro del mouse sull'angolo sinistro del desktop e selezionare **Gestione disco**
   Windows 10: fare clic con il tasto destro del mouse sul pulsante Start e selezionare **Gestione disco**

4. Nella finestra Gestione disco, diskAshur³ viene riconosciuto come un dispositivo sconosciuto, non inizializzato e non allocato. Dovrebbe essere visualizzata una finestra in cui è possibile scegliere tra una partizione MBR e GPT. GPT consente di memorizzare duplicati dei dati sul disco ed è quindi più sicuro. In un disco MBR, le informazioni di partizionamento e avvio vengono memorizzate in un unico luogo.

Selezionare il tipo di partizione e fare clic su **OK**.



5. Fare clic con il tasto destro del mouse nell'area vuota posta sopra la sezione **Non allocato** e quindi selezionare **Nuovo volume semplice**.



6. Viene visualizzata la finestra di benvenuto della procedura guidata per la creazione di un nuovo volume semplice. Fare clic su Avanti.

7. Per creare una singola partizione, accettare le dimensioni predefinite della partizione e fare clic su **Avanti**.

8. Assegnare una lettera di unità o un percorso e fare clic su **Avanti**.

9. Creare un'etichetta di volume, selezionare Formattazione rapida e quindi fare clic su **Avanti**.

10. Fare clic su **Fine**.

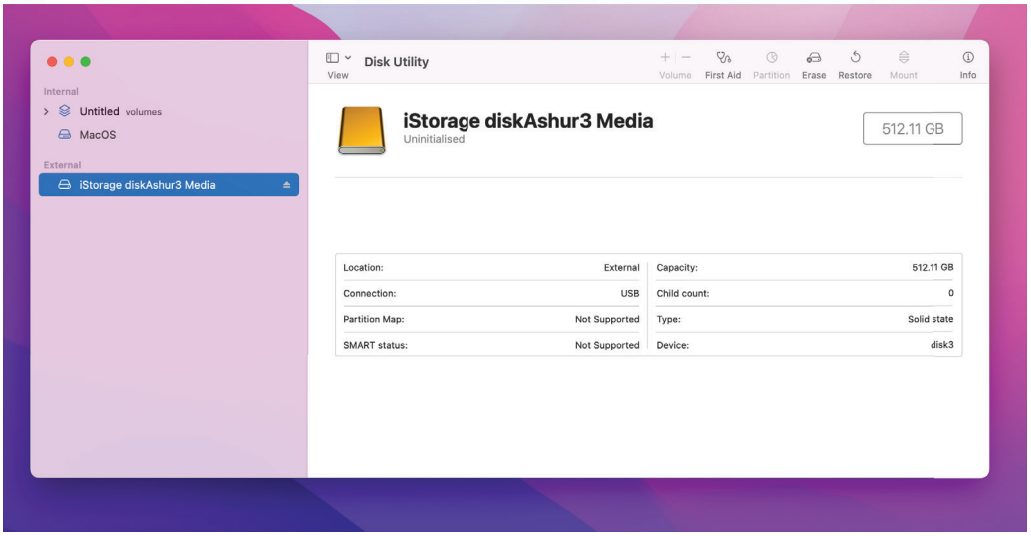
11. Attendere il completamento del processo di formattazione. diskAshur³ verrà riconosciuto dal sistema e sarà disponibile per l'uso.

45. Inizializzazione e formattazione di diskAshur³ su Mac OS

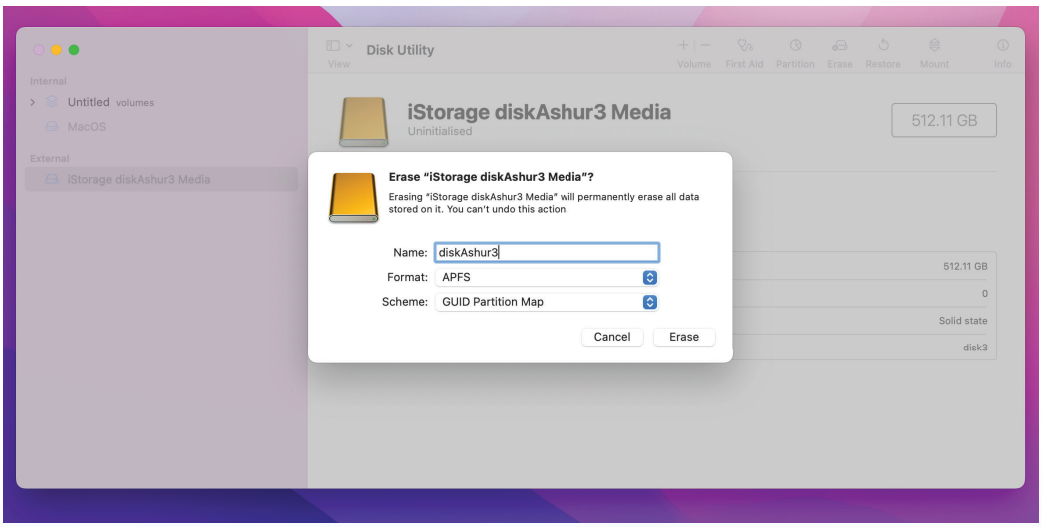
Dopo un attacco "brute force" o una reimpostazione completa, diskAshur³ eliminerà tutti i PIN, i dati e la chiave di crittografia. Occorrerà inizializzare e formattare diskAshur³ prima di poterlo utilizzare.

Per inizializzare e formattare diskAshur³:

1. Selezionare diskAshur³ dall'elenco delle unità e dei volumi. Ciascuna unità nell'elenco indicherà informazioni sulla capacità, sul produttore e sul nome del prodotto, ad esempio "**iStorage diskAshur³ Media**".

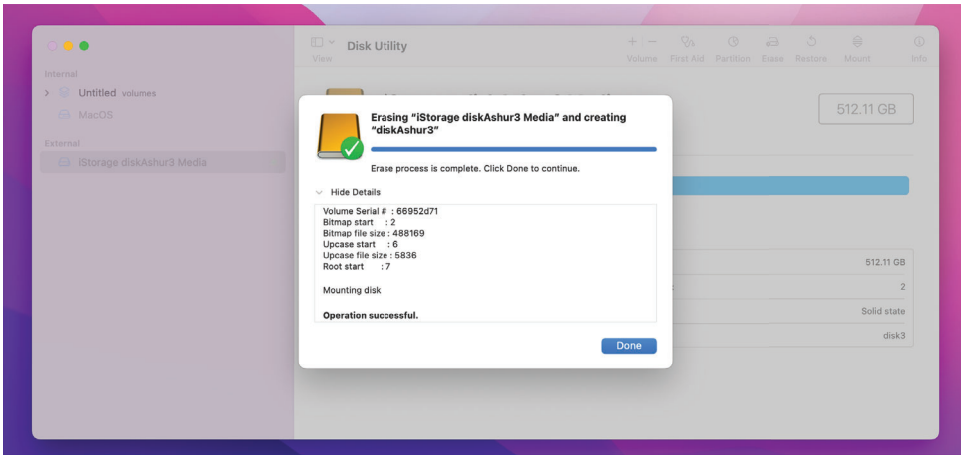


2. Fare clic sul pulsante "**Cancella**" in Utility Disco.
3. Inserire un nome per l'unità. Il nome predefinito è "Senza titolo". Il nome dell'unità verrà visualizzato sul desktop alla fine del processo.



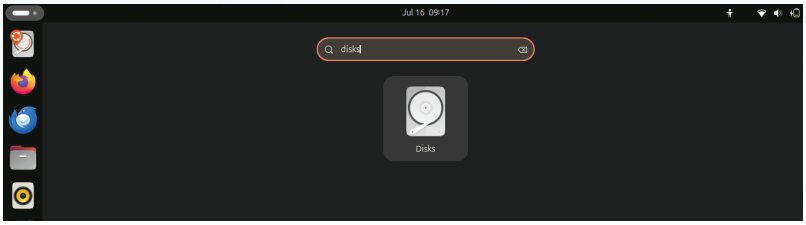
4. Selezionare uno schema e un formato per il volume da utilizzare. Il menu a discesa "Formato volume" elenca i formati di unità supportati da Mac . Il formato consigliato è "Mac OS esteso, journaled" Se si intende usare il prodotto su più piattaforme, sceglierei l formato exFAT. Il menu a discesa del formato elenca gli schemi disponibili. Consigliamo di utilizzare "Mappa partizione GUID" per le unità di dimensioni superiori a 2 TB.

5. Fare clic sul pulsante "Cancella". Utility Disco smonterà il volume dal desktop, lo cancellerà e lo rimonterà sul desktop.

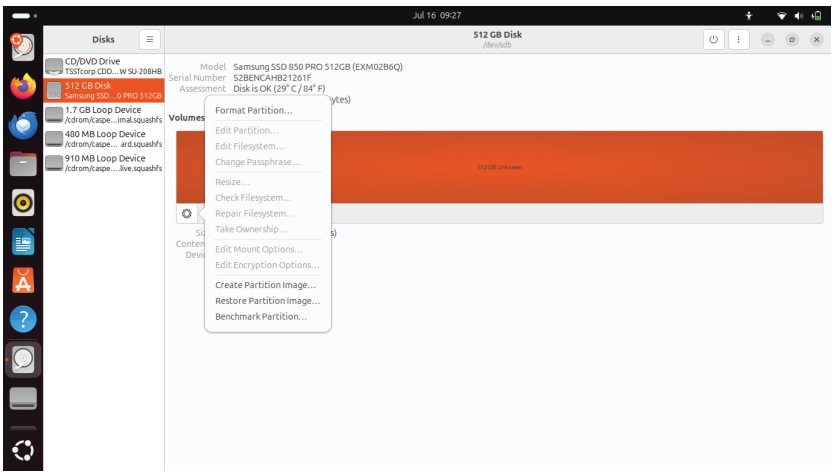


46. Inizializzare e formattare diskAshur³ su Linux

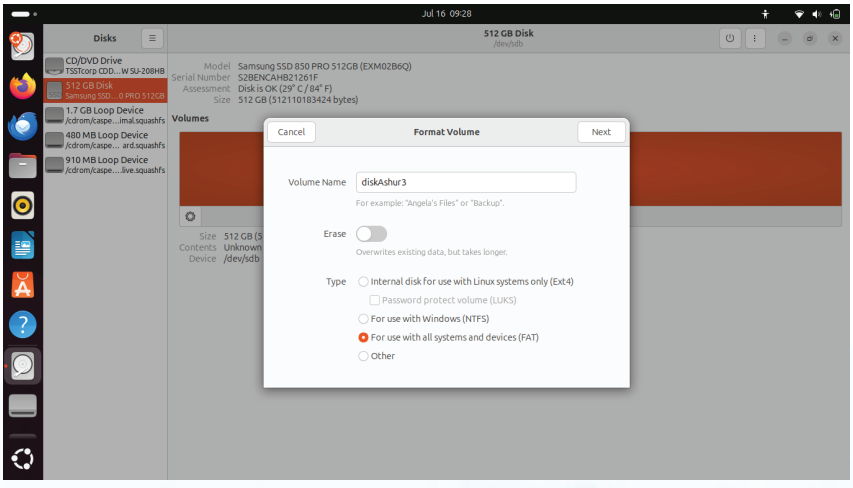
1. Aprire **Visualizza applicazione** e digitare "**Dischi**" nella casella di ricerca. Fare clic sul programma "**Dischi**" una volta visualizzata.

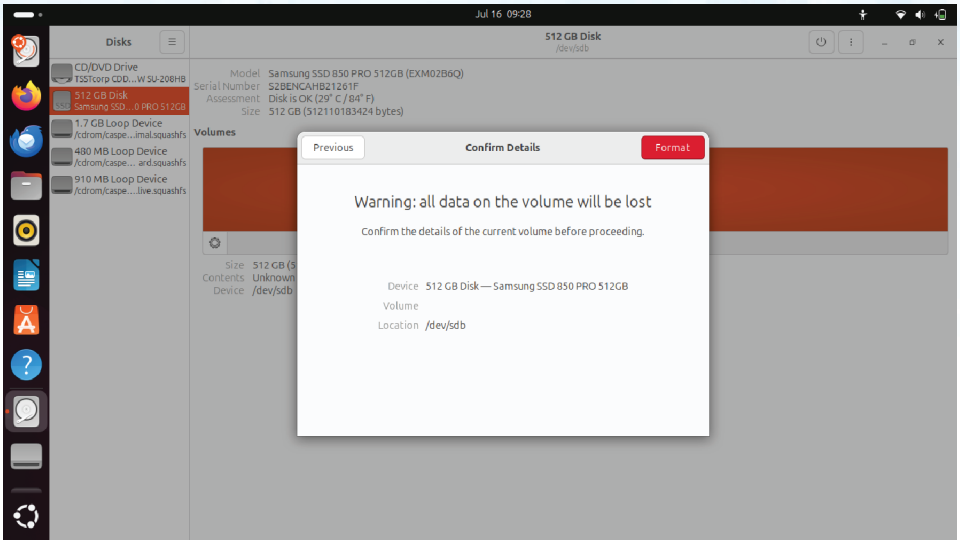


2. Fare clic per selezionare l'unità (hard disk da 500 GB) in "**Dispositivi**". In seguito, fare clic sull'icona a forma di ingranaggio sotto "**Volumi**" e quindi su "**Formatta partizioni**".

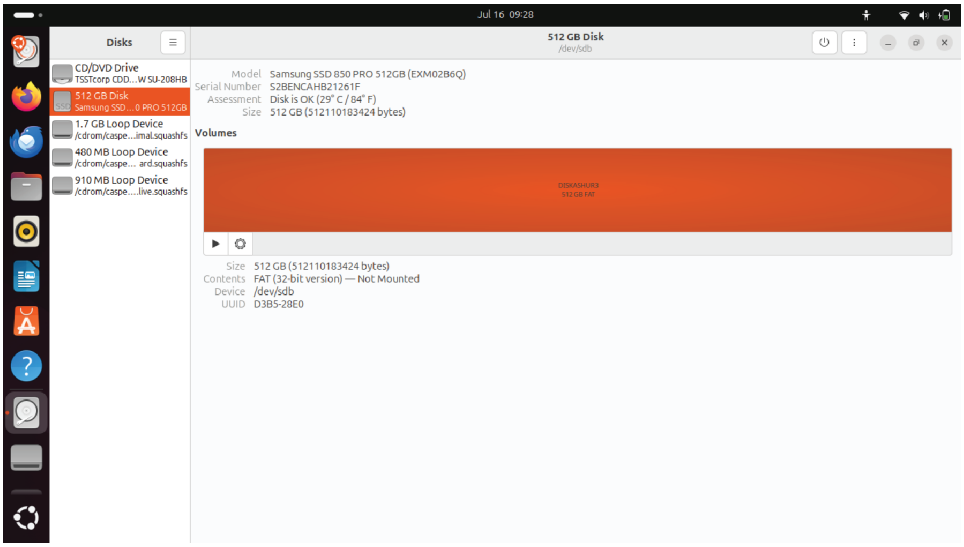


3. Selezionare "**Compatibile con tutti i sistemi e dispositivi, FAT**" per l'opzione "**Tipo**". Inserire un nome per l'unità, ad esempio: diskAshur³. Quindi, fare clic sul pulsante **"Formatta".**

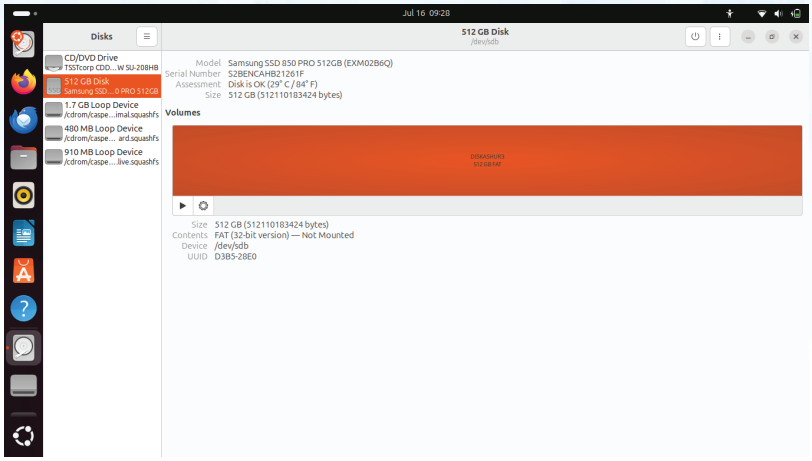




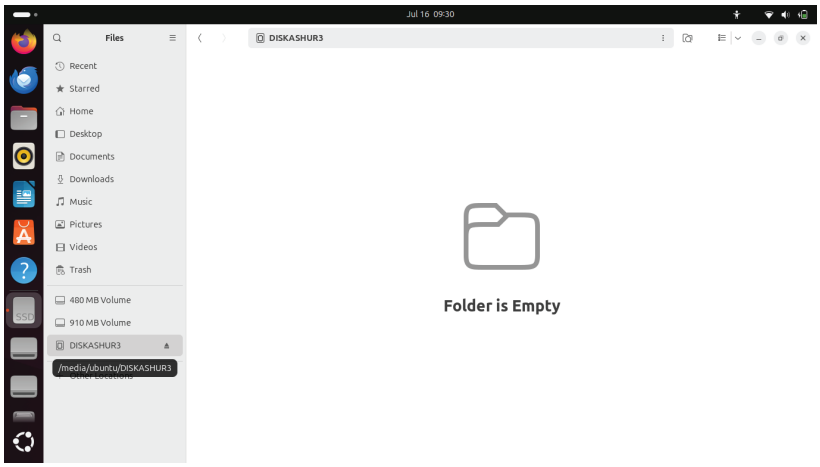
4. Al termine del processo di formattazione, fare clic sul pulsante Play per montare l'unità su Ubuntu.



5. L'unità verrà montata su Ubuntu e sarà pronta per l'uso.



6. Il disco verrà visualizzato come indicato nell'immagine seguente. Per aprire l'unità, fare clic sull'icona del disco.



47. Ibernazione, Sospensione o Uscita dal Sistema Operativo

Accertarsi di salvare e chiudere tutti i file su diskAshur³ prima di ibernare, sospendere o uscire dal sistema operativo.

Si raccomanda di bloccare manualmente diskAshur³ prima di ibernare, sospendere o uscire dal sistema.

Per bloccare l'unità, espellere in modo sicuro diskAshur³ dal sistema operativo host e quindi scollegarlo dalla porta USB. Se si stanno scrivendo dati sull'unità, scollegare diskAshur³ comporterà un trasferimento di dati incompleto e una possibile corruzione dei dati.

⚠ **Attenzione:** Per garantire la sicurezza dei dati, accertarsi di bloccare diskAshur³ se ci si allontana dal proprio computer.

48. Come verificare il Firmware in Modalità amministratore

Per verificare il numero di revisione del firmware, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

1. In Modalità Amministratore, premere e tenere premuti entrambi i tasti "**3 + 8**"		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premendo una volta il tasto **KEY (🔓)** accade quanto segue; a. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. b. Il LED ROSSO lampeggia indicando la parte totale del numero di revisione del firmware. c. Il LED VERDE lampeggia indicando la parte parziale. d. Il LED BLU lampeggia indicando l'ultima cifra del numero di revisione del firmware e. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. f. I LED ROSSO, VERDE e BLU si trasformano in BLU fisso		

Ad esempio, se il numero di revisione del firmware è '**2.3**', il LED ROSSO lampeggerà due volte (**2**) e il LED VERDE tre (**3**) volte. Una volta terminata la sequenza, i LED ROSSO, VERDE e BLU lampeggeranno insieme una volta e poi torneranno in Modalità amministratore, un LED BLU fisso.

49. Come verificare il Firmware in Modalità Utente

Per verificare il numero di revisione del firmware, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 13. Una volta che l'unità è in Modalità utente (LED VERDE fisso) procedere come segue.

1. In Modalità Utente, premere e tenere premuti entrambi i pulsanti "3 + 8" fino a quando i LED VERDE e BLU lampeggiano insieme		Il LED VERDE fisso si trasformerà in LED VERDE e BLU lampeggianti
2. Premendo il tasto **KEY (🔓)** accade quanto segue; a. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. b. Il LED ROSSO lampeggia indicando la parte totale del numero di revisione del firmware. c. Il LED VERDE lampeggia indicando la parte parziale. d. Il LED BLU lampeggia indicando l'ultima cifra del numero di revisione del firmware e. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. f. I LED ROSSO, VERDE e BLU si trasformano in un LED BLU fisso		

Ad esempio, se il numero di revisione del firmware è "**2.3**", il LED ROSSO lampeggerà due volte (**2**) e il LED VERDE tre (**3**) volte. Una volta terminata la sequenza, i LED ROSSO, VERDE e BLU lampeggeranno insieme una volta e poi torneranno in Modalità Utente, un LED VERDE fisso.

50. Assistenza Tecnica

iStorage mette a disposizione le seguenti utili risorse:

Sito web:
https://www.istorage-uk.com

Assistenza via e-mail:
support@istorage-uk.com

Assistenza telefonica:
+44 (0) 20 8991-6260.

Gli specialisti dell'Assistenza Tecnica iStorage sono disponibili dalle 9:00 alle 17:30 GMT - dal lunedì al venerdì.

51. Garanzia e Informazioni RMA

LIBERATORIA E GARANZIA DEL PRODOTTO ISTORAGE

iStorage garantisce che i propri Prodotti sono esenti da difetti materiali, alla consegna e per un periodo di 36 mesi successivi alla consegna. Tuttavia, questa garanzia non si applica nelle circostanze descritte di seguito. iStorage garantisce che i Prodotti sono conformi agli standard elencati nella relativa scheda tecnica sul nostro sito web al momento dell'ordine.

Queste garanzie non si applicano a qualsiasi difetto dei Prodotti derivante da:

- una discreta usura;
- danni intenzionali, condizioni anomale di conservazione o funzionamento, incidenti, negligenza da parte del cliente o di terzi;
- se il cliente o terzi non riescono a far funzionare o a utilizzare i Prodotti in conformità con le istruzioni per l'uso;
- qualsiasi modifica o riparazione da parte del cliente o di terzi che non siano nostri riparatori autorizzati; oppure
- qualsiasi specifica fornita da dal cliente.

In base a queste garanzie, ci riserviamo di riparare, sostituire o rimborsare a nostra discrezione i Prodotti che risultino avere difetti materiali, a condizione che alla consegna:

- i Prodotti vengano ispezionati per verificare se presentano difetti materiali; e
- si sottoponga a una prova il meccanismo di crittografia nei Prodotti.

Non saremo responsabili di eventuali difetti materiali o difetti nel meccanismo di crittografia dei Prodotti verificabili al momento dell'ispezione alla consegna, a meno che tali difetti non ci vengano notificati entro 30 giorni dalla consegna. Non saremo responsabili di eventuali difetti materiali o difetti nel meccanismo di crittografia dei Prodotti non verificabili al momento dell'ispezione alla consegna, a meno che tali difetti non ci vengano notificati entro 7 giorni dal momento in cui vengono riscontrati o il cliente dovrebbe avere riscontrato tali difetti. Ai sensi di tali garanzie, non saremo responsabili dell'eventuale uso ulteriore dei Prodotti dopo che il cliente o terzi hanno riscontrato eventuali difetti. Al momento della notifica di qualsiasi difetto, è necessario restituirci il prodotto difettoso. Se il cliente è un'azienda, sarà responsabile dei costi di trasporto sostenuti per l'invio di qualsiasi Prodotto o parte dei Prodotti in garanzia, e noi saremo responsabili di qualsiasi costo di trasporto sostenuto per l'invio di un Prodotto riparato o sostitutivo. Se il cliente è un consumatore, si prega di consultare i nostri termini e condizioni.

I prodotti restituiti devono essere nella confezione originale e puliti. In caso contrario, i prodotti restituiti, a discrezione della Società, potranno essere rifiutati o sottoposti ad addebito di ulteriore costo per coprire le spese aggiuntive. I prodotti restituiti per la riparazione in garanzia devono essere accompagnati da una copia della fattura originale, oppure riportare il numero di fattura originale e la data di acquisto.

Se il cliente è un consumatore, questa garanzia si aggiunge ai diritti legali in relazione ai Prodotti che risultano difettosi o diversi da come descritto. È possibile ricevere una consulenza in merito ai diritti legali del cliente presso l'Ufficio di Consulenza per i cittadini o l'Ufficio per gli Standard Commerciali.

Le garanzie di cui alla presente clausola si applicano solo agli acquirenti originali dei Prodotti iStorage o a rivenditori o distributori autorizzati iStorage. Queste garanzie non sono trasferibili.

FATTA ECCEZIONE PER LA GARANZIA LIMITATA IVI PREVISTA, E NELLA MISURA CONSENTITA DALLA LEGGE, ISTORAGE DECLINA OGNI GARANZIA, ESPRESSA O IMPLICITA, INCLUSE TUTTE LE GARANZIE DI COMMERCIABILITÀ; IDONEITÀ A SCOPI PARTICOLARI, NON VIOLAZIONE. ISTORAGE DECLINA QUALSIASI GARANZIA IN MERITO AL FUNZIONAMENTO SENZA ERRORI DEL PRODOTTO. NELLA MISURA IN CUI EVENTUALI GARANZIE IMPLICITE POSSONO COMUNQUE SUSSISTERE PER EFFETTO DI LEGGE, ESSE SONO LIMITATE ALLA DURATA DELLA PRESENTE GARANZIA. LA RIPARAZIONE O LA SOSTITUZIONE DI QUESTO PRODOTTO, COME QUI PREVISTO, È RIMEDIO ESCLUSIVO DEL CLIENTE.

IN NESSUN CASO ISTORAGE SARÀ RESPONSABILE DI QUALSIVOGLIA PERDITA, MANCATO GUADAGNO PREVISTO, DANNO ACCIDENTALE, PUNITIVO, ESEMPLARE, SPECIALE, DI FIDUCIA O CONSEQUENZIALE, INCLUSI, MA NON LIMITATAMENTE A, MANCATI RICAVI, MANCATI PROFITTI, PERDITA DI UTILIZZO DEL SOFTWARE, PERDITA DI DATI, ALTRE PERDITE O RECUPERO DI DATI, DANNI ALLA PROPRIETÀ, E RECLAMI DI TERZI, DERIVANTI DA QUALSIASI IPOTESI DI COMPENSAZIONE, INCLUSA LA GARANZIA, IL 44. Assistenza Tecnica CONTRATTO, LA LEGGE O L'ILLECITO CIVILE, INDIPENDENTEMENTE DAL FATTO DI ESSERE STATA AVVISATA DELLA POSSIBILITÀ DI TALI DANNI. NONOSTANTE LA DURATA DI QUALSIASI GARANZIA LIMITATA O COMUNQUE IMPLICITA PER LEGGE, O NEL CASO IN CUI UNA GARANZIA LIMITATA NON RAGGIUNGA IL SUO SCOPO ESSENZIALE, IN NESSUN CASO L'INTERA RESPONSABILITÀ DI ISTORAGE SUPERERÀ IL PREZZO DI ACQUISTO DI QUESTO
PRODOTTO. | 4823-2548-5683.3

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, Inghilterra
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 89916277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com

iStorage®

DISKASHUR® 3 & DISKASHUR® PRO3

ユーザーガイド

本ユーザー マニュアルは diskAshur³ および diskAshur PRO³ の両方に対応しています。以下では、どちらの製品も「diskAshur³」と呼びます。

それなしであなたのピン（パスワード）をメモしてくださいIドライブ上のデータにアクセスする方法はありません。

diskAshurMの使用に問題がある場合。[2]メール（support@istorage-uk.com）または電話（+44 (0) 20 8991 6260）でサポートチームに連絡してください。

すべての商標およびブランド名は、それぞれの所有者に帰属します

貿易協定法（TAA）に準拠

目次

はじめに 169
梱包内容 169
diskAshur³ のレイアウト 169
1. LED インジケータおよび動作 170
2. LED の状態 170
3. 使用開始 171
4. diskAshur ³ を管理者 PIN を使ってアンロックする 172
5. 管理者モードに入る方法 172
6. 管理者 PIN の変更 173
7. ユーザー PIN ポリシーの設定 174
8. ユーザー PIN ポリシーの削除方法 175
9. ユーザー PIN ポリシーの確認方法 175
10. 管理者モードでの新しいユーザー PIN の追加 176
11. 管理者モードでのユーザー PIN の変更 177
12. 管理者モードでのユーザー PIN の削除 177
13. ユーザー PIN を使った diskAshur³ のアンロック方法 178
14. ユーザー モードでのユーザー PIN の変更 178
15. LED バックライト付きキーパッドのスイッチ オン 179
16. LED バックライト付きキーパッドのスイッチ オフ 179
17. ワンタイム ユーザー回復 PIN の作成 180
18. ワンタイム ユーザー回復 PIN の削除 180
19. 回復モードのアクティブ化と新しいユーザー PIN の作成 181
20. 管理者モードでのユーザーの読み取り専用設定 181
21. 管理者モードでのユーザーの読み取り/書き込みの有効化 182
22. 管理者モードでのグローバル読み取り専用設定 182
23. 管理者モードでのグローバル読み取り/書き込みの有効化 183
24. 自己破壊 PIN の設定方法 183
25. 自己破壊 PIN の削除方法 184
26. 自己破壊 PIN を使ったアンロック方法 184
27. ブルートフォース攻撃またはリセット後の管理者 PIN の設定方法 185
28. 無人自動ロックの設定 185
29. 無人自動ロックをオフにする 186
30. 無人自動ロックの確認方法 187
31. ユーザー モードでの読み取り専用設定 187
32. ユーザー モードでの読み取り/書き込みの有効化 188
33. ブルートフォース ハックの防御メカニズム 188
34. ユーザー PIN ブルートフォース制限の設定方法 189
35. ユーザー PIN ブルートフォース制限の確認方法 190
36. 完全なリセットの実行方法 191
37. diskAshur³ を起動可能に設定する方法 191
38. diskAshur³ の起動可能機能を無効にする方法 192
39. 起動可能設定の確認方法 192
40. 暗号化モードの設定方法 193
41. 暗号化モードの確認方法 194
42. ディスクの種類の設定方法 195
43. ディスクの種類設定の確認方法 195
44.Windows 用 diskAshur³ の初期化とフォーマット 196
45.Mac OS での diskAshur³ の初期化とフォーマット 198
46. Linux OS での diskAshur³ の初期化とフォーマット 200
47. 休止状態、サスペンド、またはオペレーティングシステムからのログオフ 203
48. 管理者モードでのファームウェアの確認方法 203
49. ユーザー モードでのファームウェアの確認方法 204
50. テクニカル サポート 205
51. 保証と RMA 情報 205

前書き

新しいiStoragediskAshur3をお買い上げいただき、ありがとうございます。これは、120GBから2TB以上の容量を備えた、安全性が高く使いやすい、ハードウェア暗号化、ピン認証済みのポータブルソリッドステートドライブ（SSD）です。

diskAshur3は、FIPS 140-3レベル3になるように設計されており、AES-XTS 256ビットフルディスクハードウェア暗号化を使用して、転送中および保存中のデータを暗号化します。

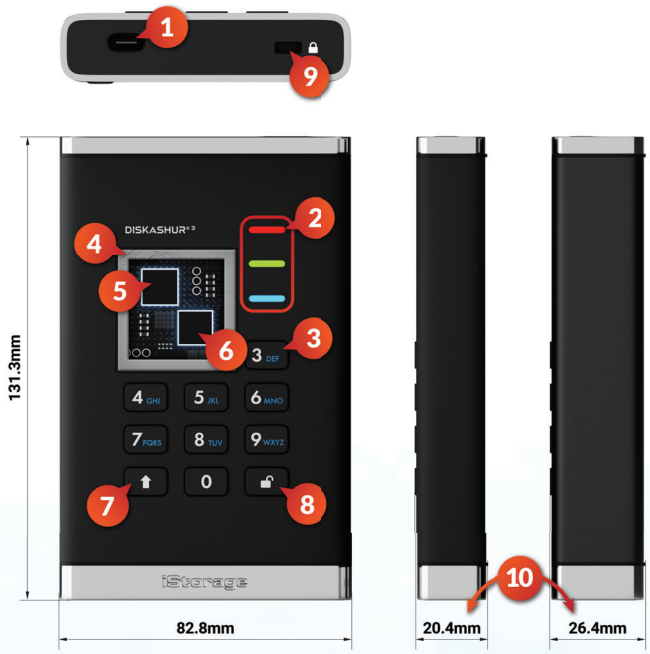
diskAshur3 には、Common Criteria EAL 5+ 認定のセキュア マイクロプロセッサが組み込まれており、外部からの改ざん、バイパス攻撃、障害挿入を防ぐように設計された組み込みの物理保護メカニズムが採用されています。

他のソリューションとは対照的に、diskAshurM。2 自動化された攻撃に応答して、デッドロック凍結状態に入り、そのような攻撃をすべて使用できなくします。簡単に言えば、ピンなしでは方法はありません!

ボックスの内容

- diskAshur³ポータブルSSD＆保護ケース
- 保護ケース
- USB C＆Aケーブル
- Nero BackItUpの1年間無料ライセンスおよびiStorage DriveSecurity
- クイックスタートガイド＆製品免責事項

diskAshur³ レイアウト



1. USB 3.2 (Gen 1) Type-C インターフェース
   USB Type C & A ケーブル付属。
2. LED ライト
   赤 - ロック／スタンバイモード。緑の点灯 - アンロックされています。緑の点滅
   - データ転送。青 - 動作モード
3. エポキシ樹脂コーティング、耐摩耗性、バックライト付き（ユーザーによる選択が可能）、英数字キーパッド。
4. 改ざん防止機能と改ざん検出設計
   すべての重要コンポーネントは、超強靭エポキシ樹脂層で覆われています。
5. オンデバイス暗号化チップ。
6. On-device Common Criteria EAL 5+ 認証済みの安全なマイクロプロセッサ。
7. シフトボタン
8. アンロックボタン
9. デスク ロック スロット
10. 4TB&5TBのHDDドライブの奥行きは、従来の20.8mmから26.8mmに変更。

1. LEDディスプレイとその動作

LED	ステータス	説明	LED	ステータス	説明
	赤ソリッド 	ロックされたドライブ（両方で スタンバイまたはリセットステータス）		ブルーソリッド 	管理者モードで続行します
	赤のダブルフラッシュ 	間違ったピン入力		赤、緑、青が点滅 一緒 	ユーザーピンが入力されるのを待ちます
	緑の固体 	ドライブのロックが解除されました		緑と青 一緒に点滅 	管理者ピンが入力されるのを待ちます
	グリーンフラッシュ 	データ転送が実行されています		緑と青 認証が進行中です 	交互に点滅

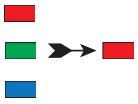
2. LEDの状態

注意: '強い電磁波障害によりdiskAshur³の通常の機能に不具合が生じる場合があります。そのような場合、商品の電源操作（電源をオフにしてからオンすること）を行うと通常に稼働するようになります。それでも通常に稼働しない場合、本商品を違う場所で使ってみてください。'

睡眠から目覚める

ハイバネーションは、diskAshur³が使用されておらず、すべてのLEDがオフの場合と定義されます。

次の手順に従って、diskAshur³をスリープから復帰させます。

diskAshur³をコンピューターのUSBポートに接続します		赤、緑、青LEDが連続して1回点滅し、次に緑LEDが2回点滅し、最後に赤色のLEDに変わり、ドライブがスタンバイ状態であることを示します。

アイドル状態に切り替えます

次のいずれかを実行して、diskAshur³をスリープ状態にします。

- ドライブがUSBポートに接続されている場合は、取り外します。すべてのLEDが消灯します（アイドル状態）。

スイッチオン状態

ドライブが休止状態から復帰した後、次の表にリストされている次のいずれかの状態になります。

電源投入時の状態	LEDディスプレイ	暗号化キー	管理者ピン	説明
初期出荷状況	赤と緑の固体	✓	×	管理者ピンの設定を待っています（初回使用）
待機する	REDソリッド	✓	✓	管理者またはユーザーのピンが入力されるのを待っています
デフォルトにリセット	REDソリッド	×	×	管理者ピンの設定を待っています

3. 初めての使用

diskAshur³は、事前設定された管理者ピンなしでステータス「初期出荷」で提供されます。ドライブを使用する前に、8～64桁の管理ピンを設定する必要があります。管理者ピンが正常に構成されると、ドライブを「初期出荷」ステータスにリセットできなくなります。

ピンの要件：

- 8～64文字の長さである必要があります
- 繰り返し番号のみを含めることはできません（例：B）。（3-3-3-3-3-3-3）
- 連続した数字だけを含めることはできません。例：B。（1-2-3-4-5-6-7）、（7-8-9-0-1-2-3-4）、（7-6-5 -4）-3-2- 1）

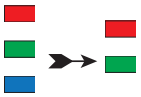
パスワードのヒント： 適切な文字でキーを押すだけで、覚えやすい単語、名前、フレーズ、またはその他の英数字のPINの組み合わせを構成できます。

これらのタイプの英数字ピンの例は次のとおりです。

- 「パスワード」の場合は、次のキーを押します。
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- 「iStorage」の場合は、次のキーを押します。
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

この方法は、長くて覚えやすいピンを構成するために使用できます。

以下の表の簡単な手順に従って、管理者ピンを構成し、diskAshur³のロックを初めて解除します。

手順-初めての使用	LED	LEDステータス
1. diskAshur³を接続します の電源付きUSBポートに コンピューター		赤、緑、青のLEDが1回点滅します 次に、緑色のLEDが2回点滅し、最後に赤色と緑色に変わり、ドライブが初期状態にあることを示します。
2. 両方のキー + 1ボタンを押し続けます		LEDは緑と青で点滅します
3. 新しい管理者ピン（8～64桁）を入力し、キーボタンを1回押します		緑の点滅と青のLEDの点灯が 次に、緑色が点滅して緑色に点滅し、青色のLEDが点灯します。
4. 新しい管理者ピンをもう一度入力し、キーボタンをもう一度押します		青いLEDがすばやく点滅してから、青色に点灯し、最後に緑色に点灯して、管理者ピンが正常に構成され、ドライブのロックが解除されたことを示します。

diskAshur³のロック
ロックドライブをロックするには、diskAshur³をホストオペレーティングシステムから安全に取り出し、電源コードを電源コンセントから抜きます。データがドライブに書き込まれている場合、diskAshur³のプラグを抜くと、データ転送が不完全になり、データが破損する可能性があります。

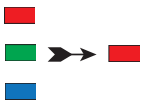
4. 管理者ピンを使用してdiskAshur³のロックを解除する

管理者ピンを使用してdiskAshur³のロックを解除するには、以下の表の簡単な手順に従ってください。

1. diskAshur³をコンピューターのUSBポートに接続します		赤、緑、青のLEDが1回点滅します 次に、緑色のLEDが2回点滅し、最後に赤色のLEDが点灯して、ドライブがスタンバイ状態にあることを示します。
2. スタンバイモード（赤色の連続LED）でボタンを押します**キー ( )** ボタンを1回		緑と青のLEDが一緒に点滅します
3. LEDが緑と青で一緒に点滅すると、管理者ピンを入力し、キー ( ) ボタンを押します もう一度		緑と青のLEDが交互に点滅します 数回、次に点灯した青色LED ドライブが管理者として正常にロック解除されたことを示す緑色のLEDに変わります

5. 管理者モードを呼び出す方法

管理者モードに入るには、次の手順に従います。

1. diskAshur³を接続します の電源付きUSBポートに コンピューター		赤、緑、青のLEDが1回点滅します 赤、緑、青のLEDが1回点滅します次に、緑色のLEDが2回点滅し、最後に赤色のLEDが点灯して、ドライブがスタンバイ状態にあることを示します。
2. スタンバイモード（赤色の連続LED）で、両方のキー +1ボタンを押し続けます		緑と青のLEDが一緒に点滅します
3. 管理者ピンを入力し、キーボタンを1回押します		数回押してから、緑色のLEDに切り替え、最 後に青色のLEDに切り替えて、ドライブが管理モードになっていることを示します。

管理モードを終了する方法

（管理者モードをすぐに終了するには（青色のLEDが点灯）、シフトキー ( ) を1秒間押し続けます。青色のLEDが赤色の点灯に変わります。

6. 管理者ピンを変更します

ピンの要件:

- 8〜64文字の長さである必要があります
- 繰り返し番号のみを含めることはできません(例:B)。(3-3-3-3-3-3-3)
- 連続した数字だけを含めることはできません。例:B。(1-2-3-4-5-6-7)、(7-8-9-0-1-2-3-4)、(7-6-5 -4) -3-2- 1)

パスワードのヒント: 対応する文字のキーを押すだけで、覚えやすい単語、名前、フレーズ、またはその他の英数字のピンの組み合わせを構成できます。

これらのタイプの英数字ピンの例は次のとおりです。

- パスワード」の場合は、次のキーを押します。
  7 (**p**qrs) **2** (**a**bc) **7** (pqr**s**) **7** (pqr**s**) **9** (**w**xyz) **6** (mn**o**) **7** (pq**r**s) **3** (**d**ef)
- i**Storage**」の場合は、次のキーを押します。
  4 (gh**i**) **7** (pqr**s**) **8** (**t**uv) **6** (mn**o**) **7** (pq**r**s) **2** (**a**bc) **4** (**g**hi) **3** (d**e**f)

この方法は、長くて覚えやすいピンを構成するために使用できます。

管理者ピンを変更するには、最初にセクション5の説明に従って「管理者モード」に移動します。ドライブが管理者モード(青色のLEDが点灯)の場合は、以下の手順に従います。

1. 管理者モードで、両方を押し続けますキーキー **+ 2**		点灯している青色LEDが点滅している緑色と点灯している青色LEDに変わります
2. 新しい管理者ピンを入力し、ボタンを押しますキーボタンを1回		緑と青のLEDの点滅は、緑のLEDの1回の点滅と交互になり、その後、緑と青のLEDの点滅に戻ります。
3. 新しい管理者ピンをもう一度入力し、キーボタンを1回押します		緑の点滅と青のLEDの点灯がに変わります急速に点滅する青色LED、そして最後に点灯するLED 青色のLEDは、管理者ピンが 正常に変更されました

注意: 管理モードをすぐに終了するには(青色のLEDが点灯)、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

7. ユーザーピンポリシーを設定します

管理者は、ユーザーピンの制限ポリシーを設定できます。このポリシーには、ピンの最小長（8～64桁）の指定、および1つ以上の「特殊文字」の入力を要求するかどうかの指定が含まれます。特殊文字は、両方のキー「シフト＋数字」を同時に押すと機能します。

ユーザーピンポリシー（制限）を設定するには、B。'091'のように3桁の数字を入力する必要があります。最初の2桁（09）は、ピンの最小長（この場合は9）と最後の桁（1）を示します。1つ以上の「特殊文字」、つまり「シフト＋数字」を使用する必要があることを意味します。同様に、B。"120"などの特殊文字を使用せずに、ユーザーピンポリシーを設定できます。最初の2桁（12）は最小ピン長（この場合は12）を示し、最後の桁（0）は特殊文字が不要であることを意味します。

管理者がユーザーピンポリシー（B. '091'など）を設定した後、新しいユーザーピンを構成する必要があります。セクション10「管理者モードでの新しいユーザーピンの追加」を参照してください。管理者が特殊文字を使用してユーザーピンを「247688314」として構成する場合（シフト＋数字を同時に押す）、以下に示すユーザーピンを作成するときに、これを8～64桁のピンのどこにでも配置できます。

A. '**シフト**＋2'、'4'、'7'、'6'、'8'、'8'、'3'、'1'、'4'、

B. '2'、'4'、'**シフト**＋7'、'6'、'8'、'8'、'3'、'1'、'4'、

C. '2'、'4'、'7'、'6'、'8'、'8'、'3'、'1'、'**シフト＋4**'、

注意:

- ユーザーPINの構成時に「特殊文字」が使用された場合（例：B）。上記の例「B」では、PINを入力することによってのみドライブのロックを解除できます。これにより、「特殊文字」は例のように構成された順序で正確に入力されました上記の「B」-（「2」、「4」、「シフト（）＋7」、「6」、「8」、「8」、「3」、「1」、「4」）。
- 複数の特殊文字を使用して、8～64桁のPINの横に配置できます。
- ユーザーはPINを変更できますが、設定されている「ユーザーPINガイドライン」（制限）に準拠する必要がある場合があります。
- 新しいユーザーPINポリシーを設定すると、ユーザーPINが存在する場合は自動的に削除されます。
- このポリシーは、自己破壊PINには適用されません。SelfDestruct PINとAdminPINの複雑さの設定は、特殊文字を必要とせずに、常に8～64桁です。

ユーザーピンポリシーを設定するには、最初にセクション5の説明に従って「管理者モード」に移動します。ドライブが管理者モード（青色のLEDが点灯）の場合は、次の手順に進みます。

1. 管理者モードで、両方を押し続けますキー+7キー		点灯している青色LEDは緑色に点滅し、青色LED
2. 3桁を入力し、最初の2桁を覚えておいてくださいピンの最小長と最後の桁（0または1）を示します特殊文字が使用されたかどうか		点滅している緑と青のLEDが点滅し続けます
3. シフトキーを1回押します		LEDの緑と青の点滅がに変わります緑色のLEDが点灯し、最後に青色のLEDが点灯しますユーザーピンポリシーが成功したことの表示合わせる。

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

8. ユーザーピンポリシーを削除する方法

ユーザーピンポリシーを削除するには、最初にセクション5の説明に従って「管理者モード」に移動します。ドライブが管理者モード（青色のLEDが点灯）の場合は、次の手順に進みます。

1. 管理者モードで、両方を押し続けますキー+7キー		点灯している青色LEDが点滅する緑色と青色LEDに変わります
2. **070**と入力し、シフトキーを1回押します。		LEDの緑と青の点滅がに変わります緑色のLEDが点灯し、最後に青色のLEDが点灯しますユーザーピンポリシーが成功したことの表示削除

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

9. ユーザーピンポリシーを確認する方法

管理者は、ユーザーのピンポリシーを確認し、ピンの長さの最小制限を決定し、以下に説明するLEDシーケンスに注意することで、特殊文字の使用が指定されているかどうかを判断できます。

ユーザーピンポリシーを確認するには、セクション5の説明に従って、最初にオプション「管理者モード」を入力します。ドライブが管理者モード（青色のLEDが点灯）になったら、次の手順に進みます。

1. 管理者モードで、両方を押し続けますシフト +7キー		点灯している青色LEDが点滅する緑色と青色LEDに変わります
2. キーボタンを押すと、次のようになります。 a) すべてのLED（赤、緑、青）が1秒間点灯します。 b) 1回の赤色LEDの点滅は、10ユニットのピンに対応します。 c) 各緑色のLEDの点滅は、ピンの単一のユニットに対応します d) 青い点滅は、特殊文字が使用されたことを示します。 e) すべてのLED（赤、緑、青）が1秒間点灯します。 f) LEDが再び青色に点灯します		

次の表に、ユーザーピンポリシーを確認するときのLEDの動作を示します。たとえば、特殊文字（**121**）を使用して12桁のユーザーピンを設定した場合、赤のLEDが1回点滅し（**1**）、緑のLEDが2回点滅し（**2**）、その後に青みがかったLEDが1回点滅します。特殊文字を使用する必要があることを示します。

ピンの説明	3桁のセットアップ	赤	緑	青い
特殊文字を使用した12桁のピン	121	1回点滅	2回点滅	1回点滅
特殊文字なしの12桁のピン	120	1回点滅	2回点滅	0
特殊文字を使用した9桁のピン	091	0	9回点滅	1回点滅
特殊文字なしの9桁のピン	090	0	9回点滅	0

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

10. 管理者モードで新しいユーザーピンを追加する

重要: 新しいユーザーピンの作成は、ピンの最小長を規定するセクション7に従って説明されている場合、および「特殊文字」が使用されている場合は、「ユーザーピンポリシー」に準拠する必要があります。管理者は、セクション9でユーザーピンの制限を確認できます。

ピンの要件：

- 8～64文字の長さである必要があります
- 繰り返し番号のみを含めることはできません（例：B）。（3-3-3-3-3-3-3）
- 連続した数字だけを含めることはできません。例：B。（1-2-3-4-5-6-7）、（7-8-9-0-1-2-3-4）、（7-6-5 -4）-3-2- 1）
- シフトボタン（⬆）は、追加のピンの組み合わせに使用できます（例：B）。シフト（⬆）+ 1は、1以外の値です。セクション7「ユーザーピンポリシーの設定」を参照してください。

新しいユーザーピンを追加するには、セクション5の説明に従って、最初に「管理者モード」を呼び出します。ドライブが管理者モード（青色のLEDが点灯）の場合は、次の手順に進みます。

1. 管理者モードで、両方を押し続けますキー**+3**キー		点灯している青色LEDが点滅している緑色と点灯している青色LEDに変わります
2. 新規ユーザーのピンを入力し、キーを押します		緑と青のLEDの点滅は、緑のLEDの1回の点滅と交互になり、その後、緑と青のLEDの点滅に戻ります。
3. 新しいユーザーピンをもう一度入力し、ボタンをもう一度押します		緑の点滅と青のLEDの点灯が緑のLEDが急速に点滅し、最後に点灯します青色のLEDは、新しいユーザーピンが利用可能であることを示します正常に構成されました

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

11. 管理者モードでユーザーピンを変更します

重要: ユーザーピンの変更は、セクション7で説明されているように構成されている場合、および「特殊文字」が使用されている場合は、「ユーザーピンポリシー」に準拠する必要があります。管理者は、セクション9でユーザーPINの制限を確認できます。

既存のユーザーピンを変更するには、最初にセクション5の説明に従って「管理者モード」を呼び出します。ドライブが管理者モード（青色のLEDが点灯）の場合は、次の手順に進みます。

1. 管理者モードで、両方を押し続けますキー（🔓）+3キー		点灯している青色LEDが点滅している緑色と点灯している青色LEDに変わります
2. 新しいユーザーのピンを入力し、キー（🔓）ボタンを1回押します		緑と青のLEDの点滅は、緑のLEDの1回の点滅と交互になり、その後、緑と青のLEDの点滅に戻ります。
3. 新しいユーザーピンをもう一度入力し、キー（🔓）を押します。		緑の点滅と青のLEDの点灯が緑のLEDが急速に点滅し、最後に点灯します青色のLEDは、ユーザーピンが正常に変更されました

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

12. 管理者モードでユーザーピンを削除します

既存のユーザーピンを削除するには、最初にセクション5で説明されている「管理者モード」を呼び出します。ドライブが管理者モード（青色のLEDが点灯）の場合は、以下の手順に従います。

1. 管理者モードで両方のシフト **+ 3**キーを押し続けます		点灯している青色LEDが点滅している赤色LEDに変わります
2. 両方のシフト **+ 3**キーをもう一度押し続けます		点滅している赤色のLEDが赤色のLEDに変わります次に、ユーザーを示す青色のLEDが点灯しますピンは正常に削除されました

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

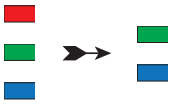
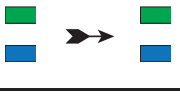
13. ユーザーピンを使用してdiskAshur³のロックを解除する方法

以下の手順に従って、ユーザーピンでdiskAshur³のロックを解除します。

1. スタンバイモード（赤色のLEDが点灯）で、シフトキーとキーの両方を押し続けます		赤LEDは、赤、緑、およびすべてのLEDに切り替わります。BLUEが点滅します
2. ユーザーピンを入力し、ボタンを1回押します		点滅するLEDの赤、緑、青が変化します緑と青のLEDを交互に使用し、次に緑色のLEDが点灯し、ドライブが成功したことを示しますユーザーモードでロック解除

14. ユーザーモードでユーザーピンを変更します

ユーザーピンを変更するには、セクション13の説明に従って、最初にユーザーピンを使用してdiskAshur³のロックを解除します。ドライブがユーザーモード（緑色のLEDが点灯）になったら、次の手順を実行します。

1. ユーザーモードで、（緑色のLED）を押し続けます両方のボタン（🔓）+4つのボタン		連続した緑のLEDがすべてのLED、赤、グリーン＆ブルーフラッシュのオンとオフ
2. 既存のユーザーピンを入力し、ボタンを押します1回押す		緑と青のLEDが交互にオンとオフになりますオフにしてから、単一の緑色のLEDに切り替えます点滅してから、緑色の点滅に戻ります。青色LED
3. 新しいユーザーピンを入力し、ボタンを押します1回押す		緑と青のLEDの点滅は、緑のLEDの1回の点滅と交互になり、その後、緑と青のLEDの点滅に戻ります。
4. 新しいユーザーピンをもう一度入力し、ボタンを押します 1回押す		緑の点滅と青のLEDの点灯が切り替わります急速に点滅する緑色のLEDに、次に緑色のLEDが点灯している場合は、ユーザーピンが正常に変更されたことを示しています。

重要: ユーザーモード（緑色のLED）でのユーザーPINの変更は、セクション7で説明されているように構成されており、最小のPIN長が必要であり、「特殊文字」が使用されている場合は、「ユーザーPINポリシー」に準拠する必要があります。

15. LED バックライト付きキーパッドのスイッチ オン

暗い場所での視認性を高めるため、diskAshur³ には LED バックライト付きキーパッドが装備されています。LED バックライト付きキーパッドをオンにするには、セクション 5 の説明に従って、まず「管理者モード」に入ります。ドライブが管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1.管理者モードで 2 & 6 の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。
2.アンロック () ボタンを押します。		点滅中の緑と青の LED は、緑の LED の点灯に切り替わり、その後、青の LED が点灯して、バックライト付きキーパッドがアクティブになったことを示し、次回ドライブを電源付き USB ポートに接続した時にオンになります。

注記:LED バックライト付きキーパッドをオンにするように diskAshur³ を設定した後、まず、電源付き USB ポートからドライブのプラグを抜き取ってから再度接続して、アクティブにする必要があります。管理者モード (青の LED 点灯) をすぐに終了するには、シフト ( ) ボタンを 1 秒間押し続けます - 青の LED 点灯が赤の LED 点灯に切り替わります。

16. LED バックライト付きキーパッドのスイッチ オフ

LED バックライト付きキーパッドをオフにするには、セクション 5 の説明に従って、まず「管理者モード」に入ります。ドライブが管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1.管理者モードで 2 + 3 の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。
2.アンロック () ボタンを押します。		点滅中の緑と青の LED は、緑の LED の点灯に切り替わり、その後、青の LED が点灯して、バックライト付きキーパッドが非アクティブになったことを示し、次回ドライブを電源付き USB ポートに接続した時にオフになります。

注記:LED バックライト付きキーパッドをオフにするように diskAshur³ を設定した後、まず、電源付き USB ポートからドライブのプラグを抜き取ってから再度接続して、アクティブにする必要があります。管理者モード (青の LED 点灯) をすぐに終了するには、シフト ( ) ボタンを 1 秒間押し続けます - 青の LED 点灯が赤の LED 点灯に切り替わります。

17. ワンタイムユーザーリカバリピンを作成します

ユーザー回復ピンは、ユーザーがdiskAshur³のロックを解除するためにピンを忘れた場合に非常に役立ちます。リカバリモードをアクティブにするには、設定されている場合、ユーザーは最初に正しいワンタイムリカバリピンを入力する必要があります。ユーザーピンを復元するプロセスは、データ、暗号化キー、および管理者ピンには影響しません。ただし、ユーザーは新しい8～64桁のユーザーピンを構成する必要があります。

1回限りの8～64桁のユーザーリカバリピンを設定するには、セクション5の説明に従って、最初に「管理者モード」に入ります。ドライブが管理者モード（青色のLEDが点灯）の場合は、次の手順に進みます。

1. 管理者モードで、両方を押し続けますキー+4キー		点灯している青色LEDが点滅している緑色と点灯している青色LEDに変わります
2. ワンタイムリカバリピンを入力し、を押しますキーボタン		緑と青のLEDの点滅は、緑のLEDの1回の点滅と交互になり、その後、緑と青のLEDの点滅に戻ります。
3. ワンタイムリカバリピンをもう一度入力し、ボタンをもう一度押します		緑の点滅と青のLEDの点灯が緑のLEDが急速に点滅し、最後に点灯します青色のLEDは、1回限りの回復ピンを示します正常に構成されました

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

18. ワンタイムユーザーリカバリピンを削除します

1回限りのユーザー回復のためにピンを削除するには、最初にセクション5で説明されている「管理者モード」を呼び出します。ドライブが管理者モード（青色のLEDが点灯）になったらすぐに次の手順を実行します。

1. 管理者モードで両方のシフト + 4キーを押し続けます		点灯している青色LEDが点滅している赤色LEDに変わります
2. 両方のシフト + 4キーをもう一度押し続けます		点滅する赤いLEDが赤く点灯してから赤く点灯します点灯している青色LEDに切り替えて、One-ユーザー回復ピンが正常に削除された時間

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

19. リカバリモードをアクティブにして、新しいユーザーピンを作成します

ユーザー回復ピンは、ユーザーがdiskAshur³のロックを解除するためにピンを忘れた場合に非常に役立ちます。リカバリモードをアクティブにするには、設定されている場合、ユーザーは最初に正しいワンタイムリカバリピンを入力する必要があります。ユーザーピンを復元するプロセスは、データ、暗号化キー、および管理者ピンには影響しません。ただし、ユーザーは新しい8～64桁のユーザーピンを構成する必要があります。

以下の手順に従って、回復プロセスをアクティブにし、新しいユーザーピンを構成します。

1. スタンバイ状態（赤色LED）で、両方のボタン+4を押し続けます		連続した赤いLEDが赤く点滅し、緑のLED
2. ワンタイムリカバリピンを入力し、ボタンを押しますキーボタン		緑と青のLEDが交互になり、次に緑のLEDが点灯し、最後に緑と青のLEDが点滅します。
3. 新しいユーザーピンを入力し、ボタンを押しますボタン		緑の点滅と青のLEDの点灯がに変わります1つの緑色のLEDが点滅してから、再び点滅します緑と青のLED
4. 新しいユーザーピンをもう一度入力し、ボタンを押しますもう一度キーボタン		緑のLEDがすばやく点滅した後、継続的に点灯します緑は、回復プロセスが完了したことを示します成功し、新しいユーザーピンが構成されました

重要: 新しいユーザーピンの作成は、次のように構成されている場合は「ユーザーピンポリシー」に準拠する必要があります。セクション7で説明されており、最小PIN長が指定されており、特殊文字が使用されているかどうかが示されています。参照するセクション9で、ユーザーのPIN制限を確認します。

20. 管理者モードでユーザーを書き込み禁止として設定します

USBドライブに感染するウイルスやトロイの木馬が非常に多いため、読み取り専用機能は、公共の環境でUSBドライブ上のデータにアクセスする必要がある場合に特に役立ちます。これは、データを変更または上書きできない元の変更されていない状態で保存する必要があるフォレンジック目的にも不可欠な機能です。

管理者がdiskAshur³を構成し、ユーザーアクセスを読み取り専用に制限した場合、セクション19で説明されているように、管理者のみがドライブへの書き込みまたは設定を読み取り専用に戻すことができます。ユーザーは読み取り専用アクセスに制限され、ドライブに書き込んだり、ユーザーモードでこの設定を変更したりすることはできません。

diskAshur³をセットアップし、ユーザーアクセスを書き込み禁止に制限するには、最初にセクション5で説明されている「管理モード」を呼び出します。ドライブが管理モード（青色のLEDが点灯）になったらすぐに次の手順を実行します。

1. 管理者モードで両方のボタン「**7 + 6**」を押し続けます。		点灯している青色LEDが点滅する緑色と青色LEDに変わります
2. キーボタンを1回押します		緑と青のLEDが連続して点灯します緑のLED、次に青のLEDに点灯ドライブが構成されていることを示し、ユーザーアクセスを読み取り専用に制限します

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

21. 管理者モードでユーザーによる読み取り/書き込みを有効にする

diskAshur³を再度読み取り/書き込みに設定するには、最初にセクション5の説明に従って「管理モード」を呼び出します。ドライブが管理モード（青色のLEDが点灯）になったら、次の手順に進みます。

1. 管理者モードで両方のボタン「**7 + 9**」を押し続けます。		点灯している青色LEDは緑色に点滅し、青色LED
2. キーボタンを1回押します		緑と青のLEDが緑色に変わりますLEDを点灯してから青色のLEDに点灯ドライブが読み取り/書き込みとして構成されていることを示します

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

22. 管理者モードでグローバル読み取り専用を設定する

管理者がdiskAshur³を構成し、それをグローバル読み取り専用に制限すると、管理者もユーザーもドライブに書き込むことができず、両方とも読み取り専用アクセスに制限されます。セクション21で説明されているように、管理者のみが設定を読み取り/書き込みに戻すことができます。

diskAshur³をセットアップし、グローバルアクセスを書き込み禁止に制限するには、最初にセクション5で説明されている「管理モード」に移動します。ドライブが管理モード（青色のLEDが点灯）になったら、次の手順に従います。

1. 管理者モードで両方のボタン「5 + 6」を押し続けます。		点灯している青色LEDは緑色に点滅し、青色LED
2. ボタンを押します		緑と青のLEDが連続して点灯します緑のLED、次に青のLEDに点灯ドライブが構成されていることを示し、グローバルアクセスを読み取り専用に制限します

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

23. 管理者モードでグローバル読み取り/書き込みをアクティブ化する

diskAshur³をグローバルな書き込み保護設定から読み取り/書き込みにリセットするには、最初にセクション5で説明されている「管理モード」を呼び出します。ドライブが管理モード（青色のLEDが点灯）の場合は、以下の手順に従います。

1. 管理者モードで両方のボタン「**5 + 9**」を押し続けます。		点灯している青色LEDは緑色に点滅し、青色LED
2. ボタンを押します		緑と青のLEDが緑色に変わります次に、LEDが青色のLEDに変わり、ドライブが読み取り/書き込み用に構成されていることを示します。

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

24. 自己破壊ピンを構成する方法

入力すると、ドライブで暗号化削除を実行する（暗号化キーが削除される）自己破壊ピンを構成できます。このプロセス中に、構成されたすべてのピンが削除され、ドライブに保存されているすべてのデータがアクセス不能（永久に失われる）として表示され、ロック解除された緑色のLEDとして表示されます。この機能を実行すると、自己破壊ピンが新しいユーザーピンになり、ドライブを再利用する前にフォーマットする必要があります。

自己破壊ピンを設定するには、最初にセクション5の説明に従って「管理者モード」に移動します。ドライブが管理者モード（継続的に青信号）になったら、次の手順に進みます。

1. 管理者モードで、両方を押し続けますキー+6キー		点灯している青色LEDは緑色に点滅し、青色のLEDが点灯
2. 8～64桁の自己破壊ピンを設定して入力し、キー（🔓）ボタンを押します。		緑の点滅と青のLEDの点灯がに変わります1つの緑色のLEDが点滅してから、再び点滅します緑と青のLED
3. 自己破壊ピンをもう一度入力して、を押します。キーボタン		緑のLEDが数回すばやく点滅します数秒後、青色のLEDに変わります自己破壊ピンが正常に構成されました

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

25. 自己破壊ピンを削除する方法

自己破壊ピンを削除するには、最初にセクション5の説明に従って「管理者モード」に移動します。ドライブが管理者モード（青色のLEDが点灯）になったら、以下の手順に従います。

1. 管理者モードで、両方を押し続けます シフト +6キー		点灯している青色LEDが点滅している赤色LEDに変わります
2. シフト +6キーをもう一度押し続けます		点滅する赤いLEDが継続的に点灯しますインジケータを示す青色のLEDに切り替えます自己破壊ピンは正常に削除されました

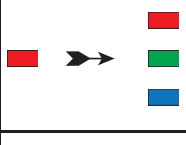
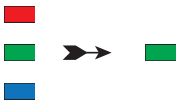
注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

26. 自己破壊ピンでロックを解除します

警告: 自己破壊メカニズムがアクティブになると、すべてのデータ、暗号化キー、および管理者/ユーザーピンが削除されます。自己破壊ピンがユーザーピンになります。自己破壊メカニズムをアクティブにした後、管理者ピンは使用できません。新しいユーザーピンを構成するオプションを含め、完全な管理者権限で管理者ピンを構成するには、diskAshur³を最初にリセットする必要があります（「完全なリセットを実行する方法」、セクション35、（174ページ）を参照）。

使用すると、自己破壊ピンはすべてのデータ、管理者/ユーザーピンを消去してから、ドライブのロックを解除します。この機能を有効にすると、自己破壊ピンが新しいユーザーピンになり、新しいデータをドライブに追加する前にdiskAshur³をフォーマットする必要があります。

自己破壊メカニズムをアクティブにするには、ドライブをスタンバイ状態（赤色のLEDが点灯）にしてから、次の手順に進む必要があります。

1. スタンバイモードで、長押しします（赤色のLEDが点灯）シフトキーとキーの両方を押します		赤LEDは、赤、緑、およびすべてのLEDに切り替わります。BLUEが点滅します
2. 自己破壊ピンを入力し、ボタンを押しますキーボタン		点滅するLEDの赤、緑、青が変化します交互にオンとオフを切り替える緑色と青色のLED数秒後、最終的に緑色に変わりますLEDは、diskAshur³が成功したことを示します 自己破壊

27. ブルートフォース攻撃またはリセット後に管理者ピンを設定する方法

ブルートフォース攻撃の後、またはdiskAshur³がリセットされた場合は、ドライブを使用する前に管理者ピンを構成する必要があります。

ピンの要件：

- 8～64文字の長さである必要があります
- 繰り返し番号のみを含めることはできません（例：B）。（3-3-3-3-3-3-3）
- 連続した数字だけを含めることはできません。例：B。（1-2-3-4-5-6-7）、（7-8-9-0-1-2-3-4）、（7-6-5 -4- 3-2-1）

diskAshur³が残酷に強制またはリセットされた場合、ドライブはスタンバイ状態になります（赤色のLEDが点灯）。以下の手順に従って、管理者ピンを構成します。

1. スタンバイモードで、長押しします（赤色のLEDが点灯）両方のシフト + 1キーを押します		連続した赤色LEDが緑色に点滅し、青色のLEDが点灯
2. 新しい管理者ピンを入力し、ボタンを押します		緑の点滅と青のLEDの点灯がに変わります1つの緑色のLEDが点滅してから、再び点滅します緑と青のLED
3. 新しい管理者ピンをもう一度入力して、を押しますキーボタン		交互に点滅する緑色のLEDと青色のLEDが点灯青のLEDが数秒間すばやく点滅し、次に、管理者ピンを示す青色のLEDが点灯します正常に構成されました。

注意： 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

28. 無人自動ロックを設定します

ドライブのロックが解除されていないときに不正アクセスから保護するために、diskAshur³は、事前設定された時間後に自動的にロックするように設定できます。デフォルトの状態では、diskAshur³の無人自動ロックのタイムアウト機能は無効になっています。無人自動ロックは、5～99分でアクティブになるように設定できます。

無人自動ロックのタイムアウト機能を設定するには、最初にセクション5の説明に従って「管理者モード」に移動します。ドライブが管理者モード（青色のLEDが点灯）の場合は、以下の手順に従います。

1. 管理者モードで、両方を押し続けますキー+5キー		点灯している青色LEDが緑色に点滅しますおよび青色LED
2. 自動ロックをタイムアウトする時間を入力します。最小時間は5分、最大時間は99分（5～99分）です。たとえば、次のように入力します。 • **05を5分間（「0」を押してから「5」を押す）** • **20を20分間（「2」を押してから「0」を押す）** • **99を99分間（「9」を押してから別の「9」を押す）**		
3. シフトキーを押します		LEDの緑と青の点滅がに変わりますソリッドグリーンを1秒間、最後にソリッドに自動ロックタイムアウトがオンになっていることを示す青色LED正常に構成されました

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

29. 無人自動ロックをオフにします

無人自動ロックのタイムアウト機能を無効にするには、最初にセクション5で説明されている「管理モード」に移動します。ドライブが管理モード（青色のLEDが点灯）になったらすぐに次の手順を実行します。

1. 管理者モードで、両方を押し続けますキー+5キー		点灯している青色LEDが緑色に点滅しますおよび青色LED
2. **00**と入力し、シフトキーを押します		LEDの緑と青の点滅がに変わりますソリッドグリーンを1秒間、最後にソリッドにオートロックの制限時間を示す青色LED正常に非アクティブ化されました

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

30. 無人自動ロックの確認方法

管理者は、次の表に記載されているLEDシーケンスに注意するだけで、無人自動ロックタイムアウト機能に設定されている時間の長さを確認および決定できます。

無人自動ロックを確認するには、最初にセクション5の説明に従って「管理者モード」に移動します。ドライブが管理者モード（青色のLEDが点灯）の場合は、次の手順に進みます。

1. 管理者モードで、長押ししますシフト **+ 5**		点灯している青色LEDは緑色に点滅し、青色LED
2. キー（🔓）ボタンを押すと、次のようになります。 a. すべてのLED（赤、緑、青）が1秒間点灯します。 b.赤色LEDの各点滅は10分に対応します。 c. 緑のLEDが点滅するたびに、1分に相当します。 d. すべてのLED（赤、緑、青）が1秒間点灯します。 e. LEDが再び青色に点灯します		

次の表は、無人自動ロックをチェックするときのLEDの動作を示しています。たとえば、**25**分後に自動的にロックするようにドライブを設定すると、赤色のLEDが**2**回点滅し、緑色のLEDが**5**回点滅します。

数分で自動ロック	**赤**	**緑**
5分	0	5回点滅
15分	1回点滅	5回点滅
25分	2回点滅	5回点滅
40分	4回点滅	0

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

31. ユーザーモードを読み取り専用に設定します

diskAshur³を書き込み禁止に設定するには、最初にセクション13で説明されている「ユーザーモード」を呼び出します。ドライブがユーザーモード（緑色のLEDが点灯）になったら、次の手順を実行します。

1. ユーザーモードで、「7 +6」の両方を押し続けます。キー。（7 =読み取り+6 =のみ）		緑色のLEDが緑色に点滅しますおよび青色LED
2. ボタンを押します		緑と青のLEDが連続して点灯します緑のLEDは、ドライブが次のように構成されていることを示します読み取り専用

注意: 1. 1.ユーザーがドライブを読み取り専用に設定した場合、管理者は、管理者モードでドライブを読み取り専用/書き込みに設定することにより、これを上書きできます。

2. 管理者がドライブを読み取り専用に設定した場合、ユーザーはドライブを読み取り専用に設定できません。

32. ユーザーモードで読み取り/書き込みを有効にする

diskAshur³を読み取り/書き込みに設定するには、最初にセクション13の説明に従って「ユーザーモード」を呼び出します。ドライブがユーザーモード（緑色のLEDが点灯）の場合は、次の手順に進みます。

1. ユーザーモードで、**7 +9**を押し続けます。キー。（7 =**読**み取り+9 =**書**き込み）		緑色のLEDが緑色に点滅します
2. ボタンを押します		緑と青のLEDが連続して点灯します緑のLEDは、ドライブが次のように構成されていることを示します読み書き

注意: 1. ユーザーがドライブを読み取り専用に設定した場合、管理者は、管理者モードでドライブを読み取り専用/書き込みに設定することにより、これを上書きできます。

2. 管理者がドライブを読み取り専用に設定した場合、ユーザーはドライブを読み取り専用に設定できません。

33. ブルートフォース ハックの防御メカニズム

diskAshur³ には、ブルートフォース攻撃からドライブを保護するための防御メカニズムが組み込まれています。デフォルトでは、管理者 PIN とユーザー PIN ではブルートフォース制限は連続 10 回の誤った PIN 入力に設定され、回復 PIN の場合は 5 回に設定されています。3 つ
の独立したブルートフォース カウンターを使用して、各 PIN 認証の誤った試行を記録します。ユーザーが間違った
管理者 PIN を10 回連続して入力すると (以下で説明するように 5回、3回、2 回の試行に分割)、ドライブがリセットされ、すべてのデータが永久に失われます
。ユーザーが間違った回復 PIN またはユーザー PIN を入力し、それぞれのブルートフォース制限を超えた場合、対応する PIN はクリアされますが、データはドライブに残ります。

注記：ブルートフォース制限は、ドライブが完全にリセットされたとき、または自己破壊機能がアクティブになったときに、初期値にプログラムされます。管理者がユーザー PIN を変更した場合、または回復機能をアクティブにするときに新しいユーザー PIN を設定した場合、ユーザー PIN のブルートフォース
カウンターはクリアされますが、ブルートフォース制限は影響を受けません。管理者が回復 PIN を変更した場合、回復 PIN のブルートフォース カウンターはクリアされます。
特定の PIN の認証に成功すると、その特定の PIN のブルートフォース カウンターはクリアされますが、他の PIN のブルートフォース カウンターには影響しません。特定の PIN の認証に失敗すると、その特定の PIN のブルートフォース カウンターは増加しますが、他の PIN のブルートフォース カウンターには影響しません。

- ユーザーが間違ったユーザー PIN を10 回連続して入力すると、そのユーザー PIN は削除されますが、データ、管理者 PIN、回復 PIN はそのまま残り、アクセス可能です。
- 間違った回復 PIN を 5 回連続して入力すると、回復 PIN は削除されますが、データと管理者 PIN はそのまま残り、アクセス可能です。
- 管理者 PIN は、ユーザー PIN や回復 PIN と比較して、より高度な防御メカニズムを使用します。 管理者 PIN を 5 回
連続して間違えて入力すると、ドライブがロックされ、赤、緑、青の LED が点灯します。この時点で、ユーザーがさらに 3 回の PIN 入力ができるようにするためには、次の手順を実行する必要があります。

- PIN「47867243」を入力し、キー () ボタンを押します。緑と青の LED が一緒に点滅します。これでドライブはさらに 3 回の管理者 PIN 入力を受け入れる準備が整いました。
- 合計 8 回連続して誤った管理者 PIN を入力すると、ドライブがロックされ、赤、緑、青の LED が交互に点滅します。この時点で、さらに最後の 2 回の PIN 入力の機会 (合計 10 回) を取得するには、次の手順を実行する必要があります。
- PIN「47867243」を入力し、KEY () ボタンを押します。緑と青の LED が一緒に点滅します。これでドライブは最後の 2 回の管理者 PIN 入力 (合計 10 回) を受け入れる準備が整いました。
- 管理者 PIN を合計 10 回連続して間違って入力すると、暗号化キーが削除され、ドライブに保存されているすべてのデータと PIN が永久に失われます。

次の表は、3 つの PIN がすべて設定されていることを前提とし、個々の PIN に対してブルートフォース防御メカニズムをトリガーした場合の影響を示しています。

ドライブのアンロックに使用される PIN	誤った PIN の連続入力	何が起こるかの説明
ユーザー PIN	10	• ユーザー PIN が削除されます。 • 回復 PIN、管理者 PIN、およびすべてのデータはそのまま維持され、アクセス可能です。
回復 PIN	5 5 3	• 回復 PIN が削除されます。 • 管理者PINとすべてのデータはそのまま残り、アクセス可能です。
管理者 PIN	2 (合計 10 回)	• 管理者 PIN を 5 回連続して間違えて入力すると、ドライブがロックされ、すべての LED が点灯します。 • PIN「47867243」を入力し、KEY () ボタンを押すと、さらに 3 回 PIN を入力できます。 • 管理者 PIN を合計 8 回 (5 回 + 3 回) 連続して間違って入力すると、ドライブがロックされ、LED が交互に点滅します。 • PIN「47867243」を入力し、KEY () ボタンを押して、最後の 2 回の PIN 入力 の機会 (合計 10 回) を取得します。 • 管理者 PIN を合計 10 回連続して間違って入力すると、暗号化キーが削除され、ドライブに保存されているすべてのデータと PIN が永久に失われます。

重要：既存の管理者 PIN がブルートフォース攻撃された場合は、新しい管理者 PIN を設定する必要があります (20 ページのセクション 27「ブルートフォース攻撃またはリセット後の管理者 PIN の設定方法」を参照)。新しいデータをドライブに追加する前に diskAshur³ もフォーマットする必要があります。

34. ユーザー PIN ブルートフォース制限の設定方法

注記：ドライブが完全にリセットされた場合、ブルートフォース攻撃された場合、または自己破壊 PIN がアクティブになった場合、ユーザー PIN ブルートフォース制限のデフォルト設定は、誤った PIN 連続入力回数が 10 回になります。

diskAshur³ のユーザー PIN のブルートフォース制限は、管理者が再プログラムして設定できます。この機能は、誤った PIN 入力を 1 回から 10 回まで連続して試行することができるように設定できます。

ユーザーピンのブルートフォース制限を構成するには、セクション5の説明に従って、最初に「管理者モード」を呼び出します。ドライブが管理者モード（青色のLEDが点灯）になったら、以下の手順に従います。

1. 管理者モードで、両方を押し続けます7 +0ボタン		点灯している青色LEDが緑色に変わり、青色LEDが一緒に点滅します
2. ブルートフォース制限の試行回数を入力します（01から10の間）。たとえば、次のように入力します。 • 1回の試行で**01** • 10回の試行で**10**		
3. シフトキーを1回押します		点滅する緑色と青色のLEDが1秒間緑色に点灯し、次に青色に点灯して、ブルートフォース制限が正常に構成されたことを示します。

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色

35. ユーザーピンのブルートフォース制限を確認する方法

管理者は、以下に説明するようにLEDシーケンスに注意するだけで、ブルートフォース防御メカニズムがトリガーされる前に、間違ったユーザーピンが連続して入力される頻度を監視および判断できます。

ブルートフォース制限の設定を確認するには、最初にセクション5の説明に従って「管理モード」を呼び出します。ドライブが管理モード（青色のLEDが点灯）の場合は、以下の手順に従います。

1. 管理者モードで、両方を押し続けます2 +0ボタン		点灯している青色LEDが点滅する緑色と青色LEDに変わります
2. キーボタンを押すと、次のようになります。 a. すべてのLED（赤、緑、青）が1秒間点灯します。 b. 各赤色LEDの点滅は、ブルートフォース制限数の10単位に対応します。 c. 各緑色のLEDの点滅は、ブルートフォース制限数の1つの単一ユニットに対応します。 d. すべてのLED（赤、緑、青）が1秒間点灯します。 e. LEDが再び青色に点灯します		

次の表に、ブルートフォース制限設定を確認するときのLEDの動作を示します。たとえば、5つの誤ったピンエントリが連続して発生した後、ドライブをブルートフォースに設定すると、緑色のLEDが5回点滅します。

ブルートフォース制限設定	赤	緑
2回の試行	0	2回点滅
5回の試行	0	5回点滅
10回の試行	1回点滅	0

注意: 管理モードをすぐに終了するには（青色のLEDが点灯）、シフトキーを1秒間押し続けます。点灯している青色LEDが点灯している赤色LEDに変わります。

36. フルリセットを行う方法

完全なリセットを実行するには、diskAshur3がスタンバイモード（赤色のLEDが点灯）になっている必要があります。ドライブがリセットされると、すべての管理者/ユーザーピン、暗号化キー、およびすべてのデータが消去され、永久に失われます。ドライブは、再利用する前にフォーマットする必要があります。以下の手順に従って、diskAshur³をリセットします。

1. スタンバイモード（赤色のLEDが点灯）で、を押して「**0**」キーを押したままにします		赤色のLEDがすべてのLEDに変わります。緑と青が交互に点滅します
2. **2 +7**ボタンの両方を押し続けます		赤、緑、青の交互のLEDが点灯します少し固まってから赤く固まるLEDはドライブがリセットされたことを示します

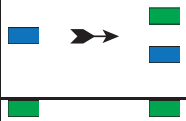
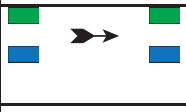
重要: 完全にリセットした後、新しい管理ピンを構成する必要があります（168ページの「ブルートフォース攻撃またはリセット後の管理ピンの構成」のセクション25を参照）。新しいデータをドライブに追加する前に、diskAshur³もフォーマットする必要があります。

37. diskAshur³ を起動可能に設定する方法

注記：ドライブが起動可能に設定されている場合、オペレーティング システムからドライブを取り出しても、LED は 強制的に赤には変わりません。ドライブは緑に点灯したままなので、次回使用するためにプラグを抜く必要があります。diskAshur³ のデフォルト設定では起動不可に設定されています。

diskAshur³ には、ホストの起動プロセス中の電源の入れ直しに対応するため、起動可能な機能が備わっています。diskAshur³ から起動する場合、diskAshur³ にインストールされているオペレーティング システムでコンピュータを実行しています。

ドライブを起動可能に設定するには、セクション 5 の説明に従って、まず「管理者モード」に入ります。ドライブが管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1. 管理者モードで、 アンロック () + 9 の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。
2.「0」を押してから「1」(01) を押します。		緑と青の LED が点滅を続けます。
3.シフト ( ) ボタンを 1 回押します		点滅中の緑と青の LED が緑の LED の点灯に変わり、最後に青の LED が点灯して、ドライブが正常に起動可能に設定されたことを示します。

注記：管理者モード (青の LED 点灯) をすぐに終了するには、シフト ( ) ボタンを 1 秒間押し続けます - 青の LED 点灯が赤の LED 点灯に切り替わります。

38. diskAshur³ の起動可能機能を無効にする方法

diskAshur³ 起動可能機能を無効にするには、セクション 5 の説明に従って、まず「管理者モード」に入ります。ドライブが管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1. 管理者モードで アンロック () + 9 の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。
2.「0」を押してから、もう一度「0」(00) を押します。		緑と青の LED が点滅を続けます。
3.シフト ( ) ボタンを 1 回押します。		点滅中の緑と青の LED が緑の LED の点灯に変わり、最後に青の LED が点灯して、起動可能機能が 正常に無効にされたことを示します。

注記：管理者モード (青の LED 点灯) をすぐに終了するには、シフト ( ) ボタンを 1 秒間押し続けます - 青の LED 点灯が赤の LED 点灯に切り替わります。

39. 起動可能設定の確認方法

起動可能の設定を確認するには、セクション 5 の説明に従って、まず「管理者モード」に入ります。ドライブが管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1. 管理者モードで シフト ( ) + 9 の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。
2. アンロック () ボタンを押すと、次の 2 つのいずれかが起きます。 • diskAshur³ が起動可能に設定されている場合、次のようになります。 a. すべての LED (赤、緑、青) が 1 秒間点灯します。 b.緑の LED が 1 回点滅します。 c. すべての LED (赤、緑、青) が 1 秒間点灯します。 d. LED が青の点灯状態に戻ります。 • diskAshur³ が起動可能に設定されていない場合、次のようになります。 a. すべての LED (赤、緑、青) が 1 秒間点灯します。 b. すべての LED が消灯します。 c. すべての LED (赤、緑、青) が 1 秒間点灯します。 d. LED が青の点灯状態に戻ります。		

注記：管理者モード (青の LED 点灯) をすぐに終了するには、シフト ( ) ボタンを 1 秒間押し続けます - 青の LED 点灯が赤の LED 点灯に切り替わります。

40. 暗号化モードの設定方法

警告：暗号化モードを AES-XTS (デフォルト状態) から AES-ECB または AES-CBC に変更すると、暗号化キーが削除され、diskAshur³ がリセットされ、すべてのデータがアクセスできなくなり、永久に失われます。

diskAshur³ の暗号化モードを、番号「01」で示される AES-ECB、番号「02」で示される AES-XTS、または番号「03」で示される AES-CBC のいずれかに設定するには、次の手順を実行します。この機能は、デフォルトでは AES-XTS (02) として設定されています。別の暗号化モードに切り替えると、すべての重要なパラメータが削除され、ドライブがリセットされることに注意してください。

diskAshur³ を暗号化モードに設定するには、セクション 5 の説明に従って、まず「管理者モード」に入ります。diskAshur³が管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1. 管理者モードで 「キー () + 1」の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。
2.01 を入力して AES-ECB として設定します。02 を入力して AES-XTSとして設定します (デフォルトの状態)。 03 を入力して AES-CBC として設定します。		緑と青の LED が点滅を続けます。
3. シフト ( ) ボタンを 1 回押します。		緑と青の LED が緑の LED の点灯に変わってから、赤の LED が点灯して (リセット状態)、暗号化モードが正常に変更されたことを示します。

重要：暗号化モードを設定した後、diskAshur³ は完全にリセットされ、新しい管理者 PIN を設定する必要があります (20ページのセクション27「ブルートフォース攻撃またはリセット後の管理者 PIN の設定方法」を参照してください)。

41. 暗号化モードの確認方法

diskAshur³ の暗号化モードを確認するには、セクション 5 の説明に従って、まず「管理者モード」に入ります。ドライブが管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1. 管理者モードで「シフト ( ) + 1」の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。

2. キー () ボタンを押すと、次のようになります。

- 暗号化モードが AES-ECB として設定されている場合、次のことが起こります。

a. すべての LED (赤、緑、青) が 1 秒間点灯します。
b. 緑の LED が 1 回点滅します。
c. すべての LED (赤、緑、青) が 1 秒間点灯します。
d. LED が青の点灯状態に戻ります。

- 暗号化モードが AES-XTS として設定されている場合、次のことが起こります。

a. すべての LED (赤、緑、青) が 1 秒間点灯します。
b. 緑の LED が 2 回点滅します。
c. すべての LED (赤、緑、青) が 1 秒間点灯します。
d. LED が青の点灯状態に戻ります。

- 暗号化モードが AES-CBC として設定されている場合、次のことが起こります。

a. すべての LED (赤、緑、青) が 1 秒間点灯します。
b. 緑の LED が 3 回点滅します。
c. すべての LED (赤、緑、青) が 1 秒間点灯します。
d. LED が青の点灯状態に戻ります。

注記：管理者モード (青の LED 点灯) をすぐに終了するには、シフト ( ) ボタンを 1 秒間押し続けます - 青の LED 点灯が赤の LED 点灯に切り替わります。

42. ディスクの種類の設定方法

diskAshur³ は、「リムーバブル ディスク」または「ローカル ディスク (デフォルトの状態)」として設定できます。ディスクの種類を変更すると、すべての重要なパラメータが消去され、すべての PIN、暗号化キー、データが削除され、ドライブがリセット状態に入ります。

警告：ディスクの種類を「リムーバブル ディスク」または「ローカル ディスク (デフォルト状態)」に変更すると、暗号化キーが削除され、diskAshur³ がリセットされ、すべてのデータがアクセスできなくなり、永久に失われます。

diskAshur³ ディスクの種類をリムーバブルディスク (00) またはローカルディスク (01) に設定するには、次の手順を実行します。この機能は、デフォルトではローカルディスク (01) として設定されています。別の暗号化モードに切り替えると、すべての重要なパラメータが削除され、ドライブがリセットされることに注意してください。
diskAshur³ の暗号化モードを設定するには、セクション 5 の説明に従って、まず「管理者モード」に入ります。
diskAshur³が管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1. 管理者モードで「キー () + 8」の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。
2.リムーバブルディスクとして設定するには 00 を入力します。ローカルディスク (デフォルトの状態) として設定するには 01 を入力します。		緑と青の LED が点滅を続けます。
3. シフト ( ) ボタンを 1 回押します。		緑と青の LED が緑の LED の点灯に変わってから、赤の LED が点灯して (リセット状態)、ディスクの種類が正常に変更されたことを示します。

重要：ディスクの種類を変更した後、diskAshur³ は完全にリセットされ、新しい管理者 PIN を設定する必要があります (20ページのセクション27「ブルートフォース攻撃またはリセット後の管理者 PIN の設定方法」を参照してください)。

43. ディスクの種類設定の確認方法

diskAshur³ のディスクの種類を確認するには、セクション 5 の説明に従って、まず「管理者モード」に入ります。ドライブが管理者モード (青の LED 点灯) になったら、次の手順に進みます。

1. 管理者モードで「シフト ( ) + 8」の両方のボタンを押したままにします。		点灯中の青の LED が緑と青の LED の点滅に変わります。

2. キー () ボタンを押すと、次のようになります。

- ディスクの種類が「リムーバブル」として設定されている場合、次のことが起こります。

a. すべての LED (赤、緑、青) が 1 秒間点灯してから消灯します。
b. すべての LED (赤、緑、青) がもう一度 1 秒間点灯してから消灯します。
b. LED が青の点灯状態に戻ります。

- ディスクの種類が「ローカル」として設定されている場合、次のことが起こります。

a. すべての LED (赤、緑、青) が 1 秒間点灯します。
b.緑の LED が 1 回点滅します。
c. すべての LED (赤、緑、青) が 1 秒間点灯します。
d. LED が青の点灯状態に戻ります。

44. DiskAshur³ Windows用を初期化してフォーマットします

「ブルートフォース攻撃」または完全なリセットの後、diskAshur³はすべてのピン、データ、および暗号化キーを削除します。diskAshur³を使用する前に、初期化してフォーマットする必要があります。

以下の手順に従って、diskAshur³をフォーマットします：

1. 新しい管理者ピンの構成-168ページのセクション25「ブルートフォース攻撃またはリセット後に管理者ピンを構成する方法」を参照してください。

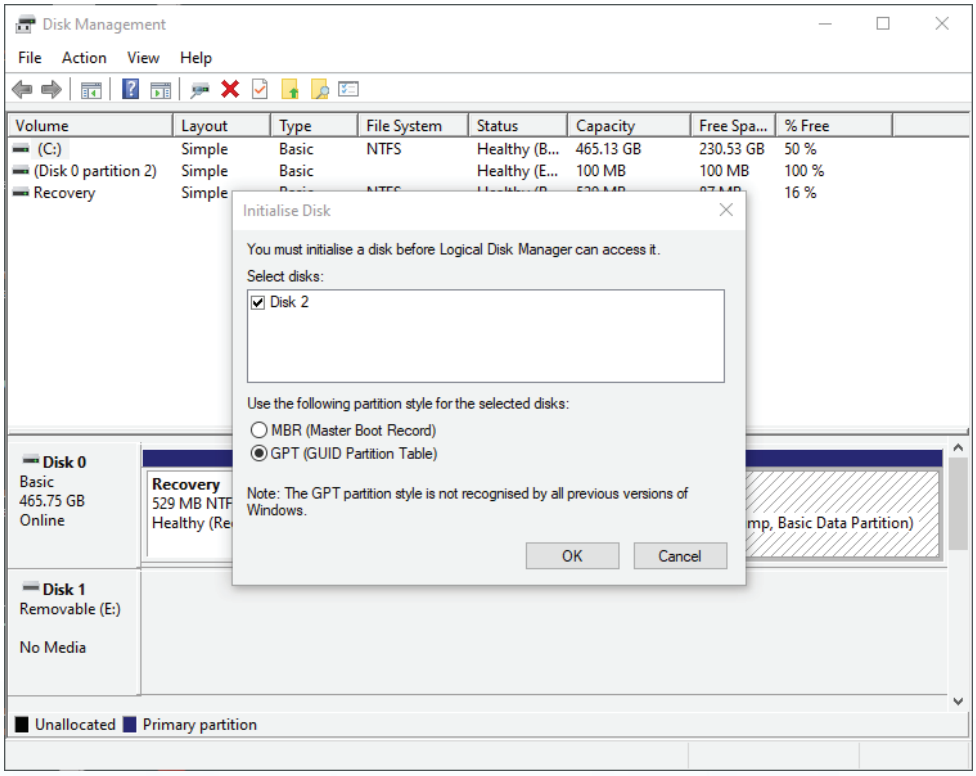
2. diskAshur³がスタンバイモード（赤色のLED）の場合は、キーボタンを1回押し、新しい管理者ピンを入力してロックを解除します（緑色のLEDが点滅）。

3. diskAshur³をコンピューターに接続します。

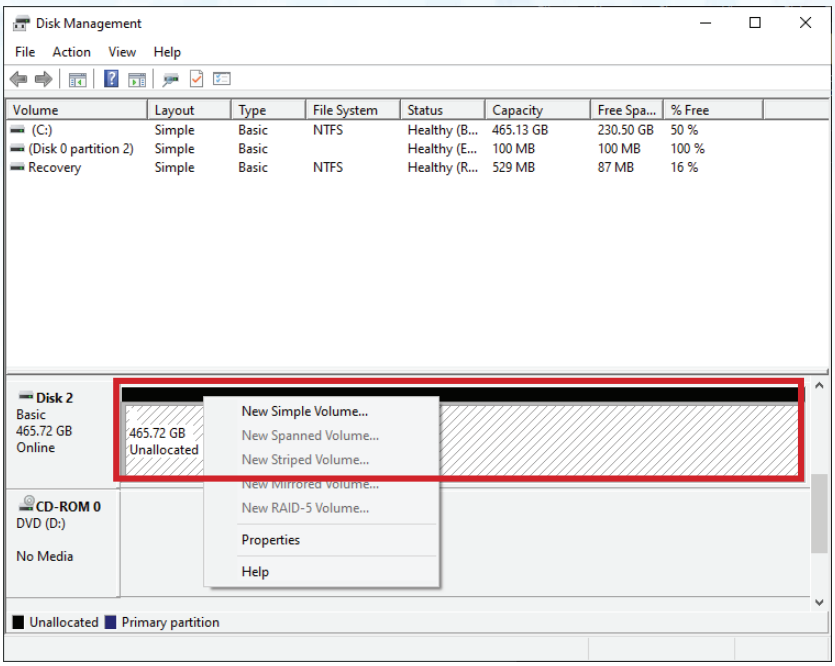
4. **ウィンドウズ 7:** [コンピューター]を右クリックし、[管理]をクリックして、[ディスクの管理]を選択します
   ウィンドウズ 8: デスクトップの左隅を右クリックして、[ディスクの管理]を選択します
   ウィンドウズ 10: [スタート]ボタンを右クリックして、[ディスクの管理]を選択します

5. [ディスクの管理]ウィンドウで、diskAshur³は、初期化されておらず、割り当てられていない不明なデバイスとして認識されます。メッセージボックスが表示され、MBRとGPTのパーティションスタイルを選択できます。GPTは、このデータの複数の複製をディスクに保存するため、はるかに堅牢になります。MBRハードドライブは、パーティションとブート情報を1か所に保存します。

   パーティションスタイルを選択し、[OK]をクリックします。



6. [未割り当て]セクションの上の空白の領域を右クリックして、[新しいシンプルボリューム]を選択します。



7. [新しいシンプルボリュームウィザードへようこそ]ウィンドウが開きます。[次へ]をクリックします。

8. 必要なパーティションが1つだけの場合は、デフォルトのパーティションサイズを受け入れて、[次へ]をクリックします。

9. ドライブ文字またはパスを割り当て、[次へ]をクリックします。

10. ボリュームラベルを作成し、[クイックフォーマットを実行する]を選択して、[次へ]をクリックします。

11. [完了]をクリックします。

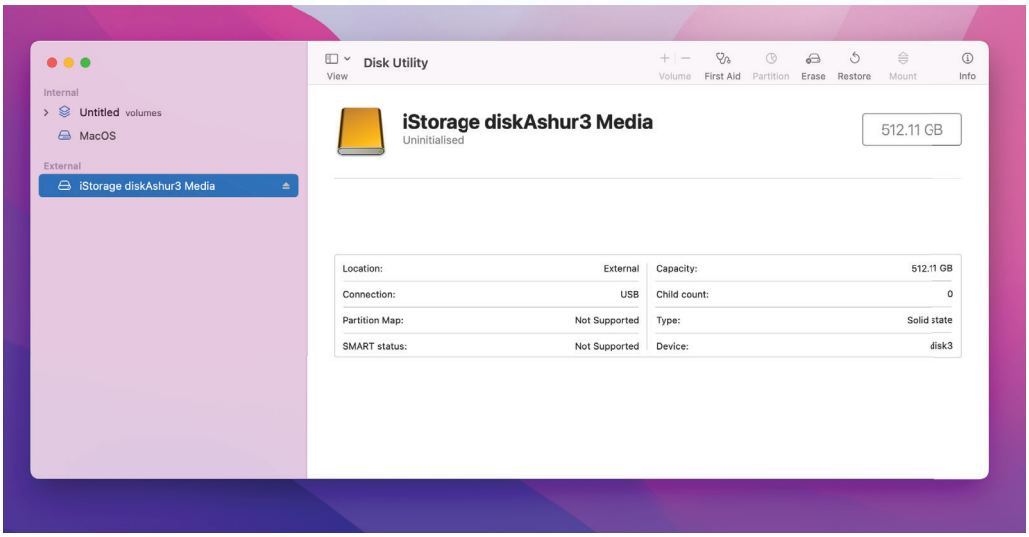
12. フォーマットプロセスが完了するのを待ちます。diskAshur³が認識され、使用可能になります。

45. MacOSでのdiskAshur³の初期化とフォーマット

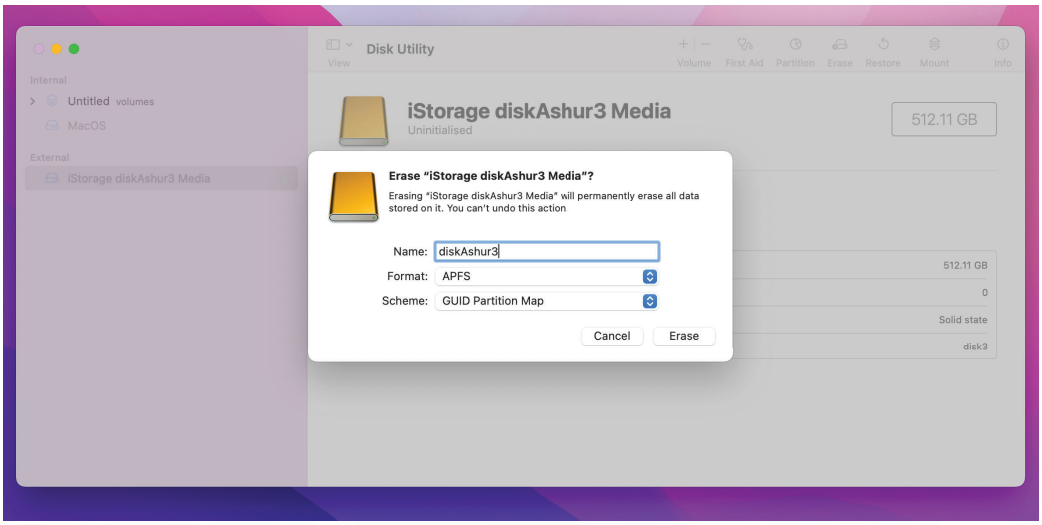
「ブルートフォース攻撃」または完全なリセットの後、diskAshur³はすべてのピン、データ、および暗号化キーを削除します。diskAshur³を使用する前に、初期化してフォーマットする必要があります。

diskAshur³を初期化およびフォーマットする方法

1. ドライブとボリュームのリストからdiskAshur³を選択します。リスト内の各ドライブには、容量、製造元、製品名が表示されます（例：B。「**iStoragediskAshur3Media**」）。

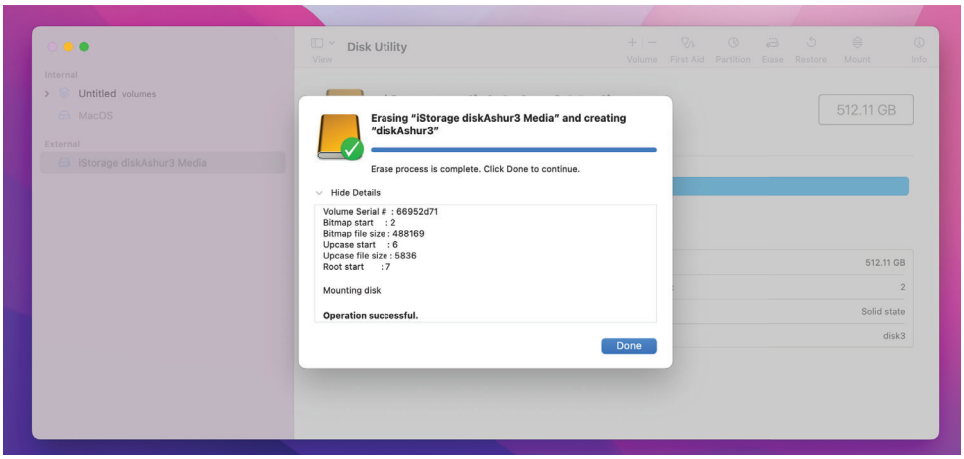


2. [ディスクユーティリティ]で、[消去]ボタンをクリックします。
3. ドライブの名前を入力します。デフォルトの名前は無題です。ドライブの名前は、最終的にデスクトップに表示されます。



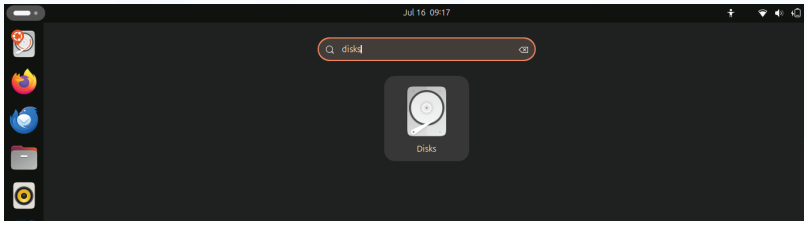
4. スキームとボリュームフォーマットを選択します。[ボリュームフォーマット]ドロップダウンメニューには、Macがサポートする利用可能なドライブフォーマットが一覧表示されます。推奨されるフォーマットタイプはMacOS 拡張（ジャーナリング）です。クロスプラットフォームアプリケーションにはexFATを使用します。[スキーマ形式]ドロップダウンメニューには、使用可能なスキーマが一覧表示されます。2TBを超えるドライブでは「GUIDパーティションマップ」を使用することをお勧めします。

5. [削除]ボタンをクリックします。ディスクユーティリティは、ボリュームをデスクトップからアンマウントし、削除してから、デスクトップに再度マウントします。

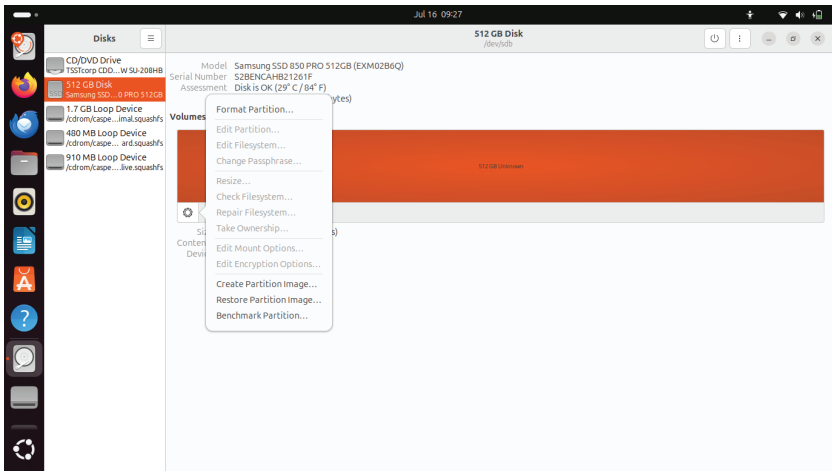


46. LinuxでのdiskAshur³の初期化とフォーマット

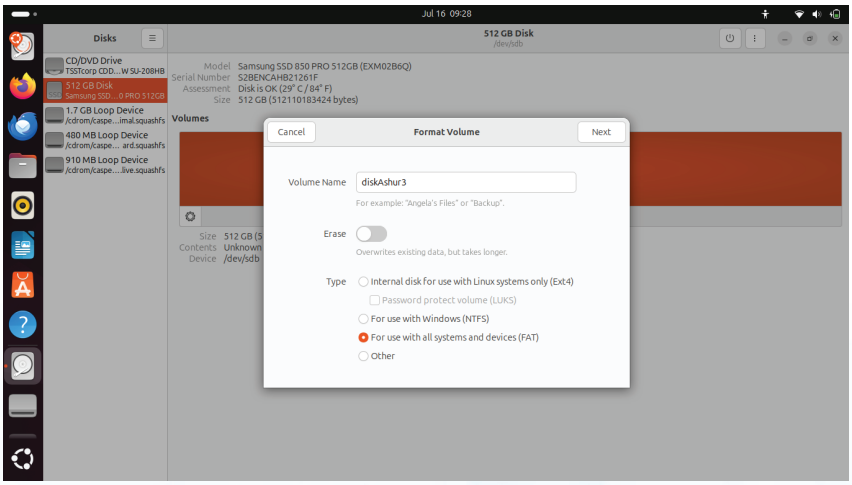
1. 「アプリケーションの表示」を開き、検索フィールドに「ディスク」と入力します。表示されたら、ハードディスクユーティリティをクリックします。

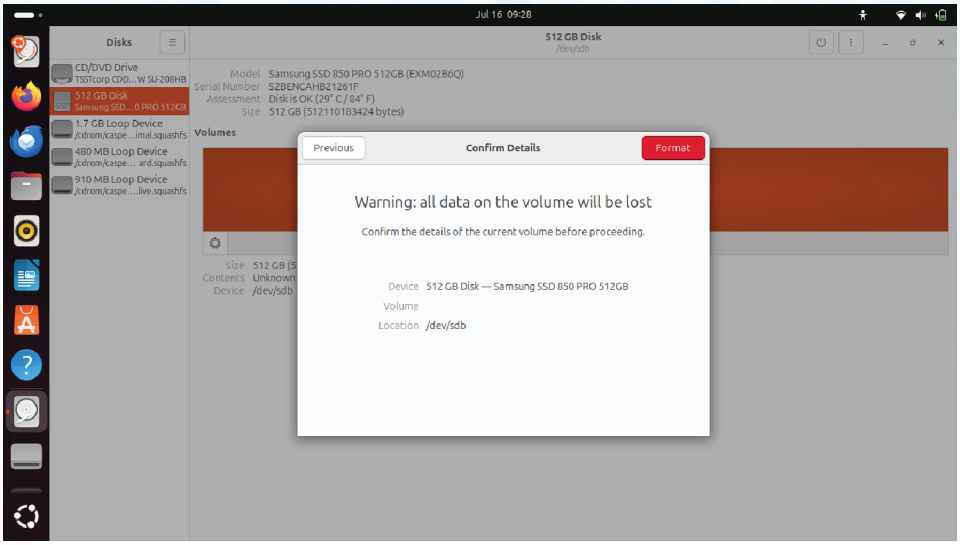


2. [デバイス]の下のドライブ（500 GBハードドライブ）をクリックして選択します。次に、[ボリューム]の下の歯車アイコンをクリックし、[パーティションのフォーマット]をクリックします。

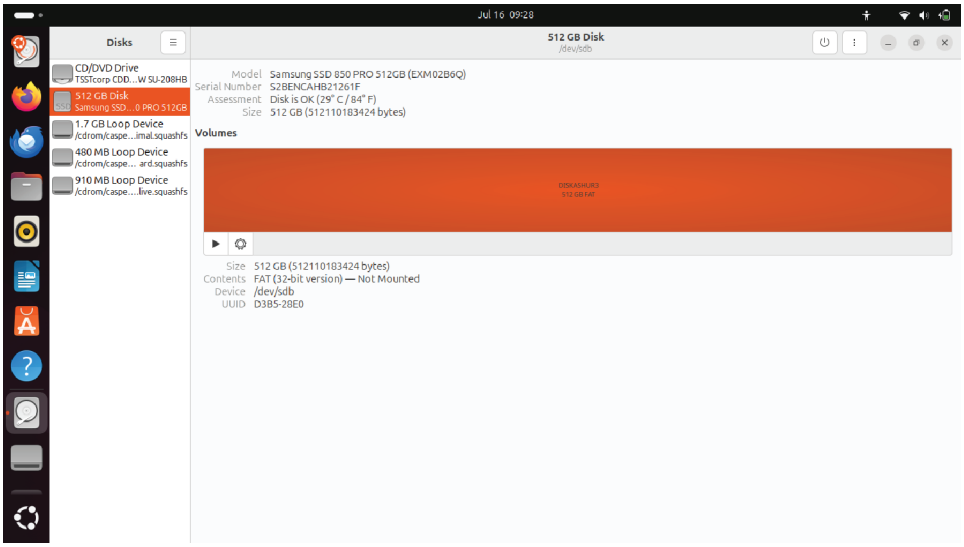


3. [タイプ]オプションで[すべてのシステムとデバイスと互換性がある（FAT）]を選択します。ドライブの名前を入力します（例：B。diskAshur³）。次に、[フォーマット]ボタンをクリックします。

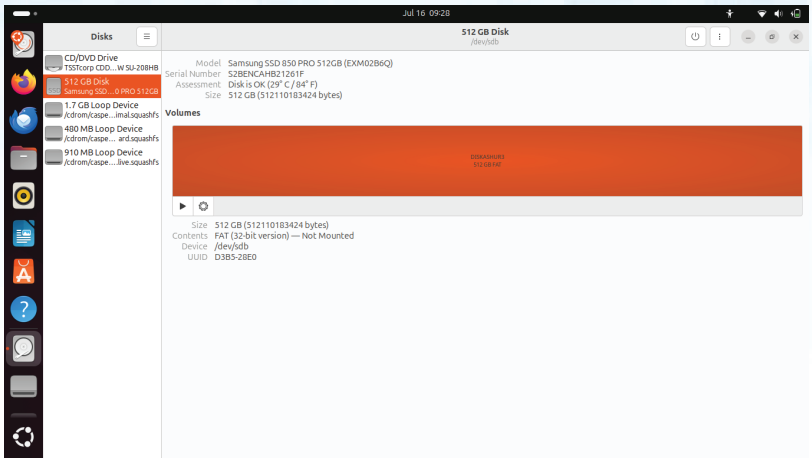




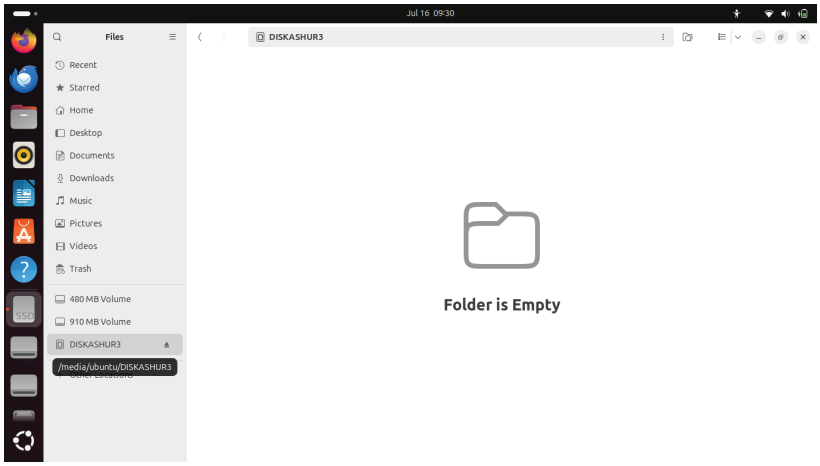
4. フォーマットプロセスが完了したら、[再生]ボタンをクリックしてドライブをUbuntuにマウントします。



5. これで、ドライブがUbuntuにマウントされ、使用できるようになります。



6. 次の図に示すように、ハードドライブが表示されます。ハードドライブのアイコンをクリックして、ドライブを開くことができます。



47. オペレーティングシステムを休止、一時停止、またはログオフしま

オペレーティングシステムをスリープ、一時停止、またはログアウトする前に、必ずdiskAshur³上のすべてのファイルを保存して閉じてください。

diskAshur³をスリープ状態にする、一時停止する、またはシステムからログアウトする前に、手動でロックすることをお勧めします。

ドライブをロックするには、diskAshur³をホストオペレーティングシステムから安全に取り出し、電源コードをソケットから抜きます。データがドライブに書き込まれている場合、diskAshur³のプラグを抜くと、データ転送が不完全になり、データが破損する可能性があります。

⚠ **注意:** データが安全であることを確認するには、コンピューターから離れているときにdiskAshur³をロックします。

48. 管理モードでファームウェアを確認する方法

ファームウェアのバージョン番号を確認するには、セクション5の説明に従って、最初に「管理者モード」に移動します。ドライブが管理者モード（青色のLEDが点灯）の場合は、以下の手順に従います。

1. 管理モードで両方のボタン「3 + 8」を押し続けます		点灯している青色LEDは緑色に点滅し、青色LED
2. キーボタンを1回押すと、次のようになります。 a) すべてのLED（赤、緑、青）が1秒間点灯します。 b) 赤いLEDが点滅し、ファームウェアのバージョン番号の不可欠な部分を示します。 c) 緑のLEDが点滅し、端数を示します。 d) 青LEDが点滅し、ファームウェアバージョン番号の最後の桁を示します e) すべてのLED（赤、緑、青）が1秒間点灯します。 f) 赤、緑、青のLEDが青一色のLEDに変わります		

たとえば、ファームウェアのバージョン番号が「**2.3**」の場合、赤色のLEDが2回点滅し（**2**）、緑色のLEDが3回点滅します（**3**）。シーケンスが終了するとすぐに、赤、緑、青のLEDが1回点滅し、その後、連続した青のLEDである管理モードに戻ります。

49. ユーザーモードでファームウェアを確認する方法

ファームウェアのバージョン番号を確認するには、セクション13の説明に従って、最初に「ユーザーモード」に入ります。ドライブがユーザーモード（緑色のLEDが点灯）になったら、次の手順に進みます。

1. ユーザーモードで、「3 +8」の両方を押し続けます。LEDの緑と青が一緒に点滅するまでボタンを押します		緑色のLEDが緑色に点滅しますおよび青色LED
2. キー () ボタンを押します。次のことが起こります。 a) すべてのLED（赤、緑、青）が1秒間点灯します。 b) 赤いLEDが点滅し、ファームウェアのバージョン番号の不可欠な部分を示します。 c) 緑のLEDが点滅し、端数を示します。 d) 青LEDが点滅し、ファームウェアバージョン番号の最後の桁を示します e) すべてのLED（赤、緑、青）が1秒間点灯します。 f) 赤、緑、青のLEDが青一色のLEDに変わります		

たとえば、ファームウェアのバージョン番号が「**2.3**」の場合、赤色のLEDが2回点滅し（**2**）、緑色のLEDが3回点滅します（**3**）。シーケンスが終了すると、赤、緑、青のLEDが1回点滅し、ユーザーモードに戻ります。緑のLEDが点灯します。

50. テクニカルサポート

iStorageには、次の役立つリソースがあります。

ウェブサイト：
https://www.istorage-uk.com

メールサポート：
support@istorage-uk.com

電話サポート：
+44 (0) 20 8991-6260.

IStorageのテクニカルサポートスペシャリストは、月曜日から金曜日の午前9時から午後5時30分（GMT）までご利用いただけます。

51. 保証およびRMA情報

製品の免責事項と保証の保管

iStorageは、その製品が納品時および納品から36か月間、重大な欠陥がないことを保証します。ただし、この保証は以下の場合には適用されません。iStorageは、ご注文時に当社のウェブサイトの関連データシートに記載されている基準を製品が満たしていることを保証します。

これらの保証は、以下に起因する製品の欠陥には適用されません。
- 通常の損耗;
- 故意の損傷、異常な保管または労働条件、事故、お客様または第三者による過失。
- お客様または第三者がユーザーの指示に従って製品を操作または使用しない場合
- 認定修理業者の一部ではない、お客様または第三者による変更または修理。
- またはあなたが提供する仕様。

これらの保証に基づき、納品時に以下の場合に限り、欠陥が見つかった製品については、当社の選択により、修理、交換、または払い戻しを行います。
- 彼らは製品に重大な欠陥があるかどうかを確認します。そして
- 製品の暗号化メカニズムをテストします。

納品後30日以内にご連絡いただけない限り、納品時の検査で発見された製品の暗号化メカニズムの重大な欠陥や欠陥については責任を負いません。納品時の検査で判断できない製品の暗号化メカニズムの重大な欠陥や欠陥については、発見した時点または気付いたはずの時間から7日以内に報告しない限り、当社は責任を負いません。お客様または他の誰かが欠陥を発見した後も製品を使用し続けた場合、当社はこれらの保証の下で責任を負いません。欠陥の通知後、欠陥のある製品を当社に返送する必要があります。あなたが会社である場合、あなたは輸送費に対して責任があります、あなたは保証の下で私たちに製品または製品の一部を出荷する際に負担します、また、修理または交換した製品の発送にかかるすべての送料は当社が負担します。あなたが消費者であるならば、我々の利用規約を読んでください。

返品される製品は、元のパッケージに入れられ、清潔な状態である必要があります。それ以外の場合、返品された製品は拒否されるか、会社の裁量により、関連する追加費用をカバーするために追加料金が請求されます。保証期間中に修理のために返品される製品には、元の請求書のコピーを添付するか、元の請求書番号と購入日を含める必要があります。

あなたが消費者である場合、この保証は、欠陥があるか、説明されていない製品に関するあなたの法定権利に追加されます。法的権利については、最寄りの市民相談局または貿易基準局にお問い合わせください。

この条項に記載されている保証は、iStorage製品の最初の購入者またはiStorage認定再販業者またはディーラーにのみ適用されます。これらの保証は譲渡できません。

ここに記載されている限定保証を除き、ISTORAGEは、商品性のすべての保証を含む、明示または黙示を問わず、すべての保証を否認します。侵害ではなく、特定の目的への適合性。ISTORAGEは、製品がエラーなしで動作することを保証しません。法的規定により暗黙の保証が単純に存在できない限り、そのような保証はこの保証の期間に限定されます。ここに記載されているように、この製品を修理または交換することが唯一の救済策です。
いかなる場合も、損失または将来の利益、または偶発的、罰則、例、特別、信頼性、または結果的損害に対する保管責任を負わないものとします。これには、収入、損失、または損失、損失、損失、第三者の損失が含まれますが、これらに限定されません。保証、契約、法定規制を含む、回復理論に起因する請求。この損害の可能性について通知を受けたかどうかを考慮に入れます。限定保証または法的に義務付けられた保証の期間にかかわらず、または限定保証がその本質的な目的を達成できない場合でも、ISTORAGEはその購入価格の全責任を超えることはありません。| 4823-2548-5683.3

iStorageでリミテッド、iStorageでハウス、13 Alpertonレーン
ペリベール、ミドルセックス。UB6 8DH、イギリス
電話：+44 (0) 20 8991 6260 | ファックス：+44 (0) 20 8991 6277
Eメール：info@istorage-uk.com | ウェブ：www.istorage-uk.com

iStorage®

Gebruikershandleiding

DISKASHUR® 3 & DISKASHUR® PRO3

Deze gebruikershandleiding geldt voor zowel de diskAshur³ als de diskAhur PRO³ en zal hierna diskAshur³ worden genoemd

Zorg ervoor dat u uw pincode (wachtwoord) onthoudt, zonder deze is er geen manier om toegang te krijgen tot de gegevens op de drive.

Als u problemen ondervindt bij het gebruik van uw diskAshur³ neem dan contact op met ons ondersteuningsteam via e-mail - support@istorage-uk.com of per telefoon +44 (0) 20 8991 6260.

Inhoudsopgave

Introductie....210
Inhoud verpakking....210
diskAshur³ Ontwerp....210
1. LED indicatoren en bijbehorende acties....211
2. LED-standen....211
3. Eerste Gebruik....212
4. Ontgrendelen van de diskAshur³ met de Admin pincode....213
5. Admin modus benaderen....213
6. Wijzigen van de Admin pincode....214
7. Instellen van gebruikerspincodebeleid....215
8. Verwijderen van gebruikerspincodebeleid....216
9. Controleren van gebruikerspincodebeleid....216
10. Toevoegen van een nieuwe gebruikerspincode in Admin modus....217
11. Wijzigen van de gebruikerspincode in Admin modus....218
12. Verwijderen van de gebruikerspincode in Admin modus....218
13. Ontgrendelen van de diskAshur³ met de gebruikerspincode....219
14. Gebruikerspincode wijzigen in gebruikersmodus....219
15. Inschakelen LED-achtergrondverlichting van het toetsenbord....220
16. Uitschakelen LED-achtergrondverlichting van het toetsenbord....220
17. Aanmaken van eenmalige gebruikersherstelpincode....221
18. Verwijderen van de eenmalige gebruikersherstelpincode....221
19. Herstelmodus activeren en aanmaken van nieuwe gebruikerspincode....222
20. Instellen van alleen-lezen voor gebruikers in Admin modus....222
21. Inschakelen van lezen-schrijven voor gebruikers in Admin modus....223
22. Instellen van algemeen alleen-lezen in Admin modus....223
23. Inschakelen van algemeen lezen-schrijven in Admin modus....224
24. Zelfvernietigingspincode instellen....224
25. Zelfvernietigingspincode verwijderen....225
26. Ontgrendelen met de zelfvernietigingspincode....225
27. Admin pincode instellen na een Brute Force aanval of reset....226
28. Onbeheerde automatische vergrendeling instellen....226
29. Uitschakelen van onbeheerde automatische vergrendeling....227
30. Controleren van onbeheerde automatische vergrendeling....228
31. Instellen alleen-lezen in gebruikersmodus....228
32. Inschakelen alleen-lezen in gebruikersmodus....229
33. Brute Force Hack verdedigingsmechanisme....229
34. Instellen van de gebruikerspincode Brute Force beperking....230
35. Controleren van de gebruikerspincode Brute Force beperking....231
36. Complete reset uitvoeren....232
37. diskAshur³ instellen als opstartbaar....232
38. Uitschakelen van de diskAshur³ opstartbare functionaliteit....233
39. Controleren van de opstartbare instelling....233
40. Encryptiemodus instellen....234
41. Encryptiemodus controleren....235
42. Schijftype instellen....236
43. Controleren van schijftype instelling....236
44. Initialiseren en formatteren van de diskAshur³ voor Windows....237
45. Initialiseren en formatteren van de diskAshur³ in Mac OS....239
46. Initialiseren en formatteren van de diskAshur³ in Linux OS....241
47. Slaapstand of uitloggen van het besturingssysteem....244
48. Firmware controleren in Admin modus....244
49. Firmware controleren in gebruikersmodus....245
50. Technische Ondersteuning....246
51. Garantie en RMA informatie....246

Introductie

Bedankt voor uw aankoop van de nieuwe iStorage diskAshur³/ diskAshur PRO³ schijf, ofwel diskAshur³.

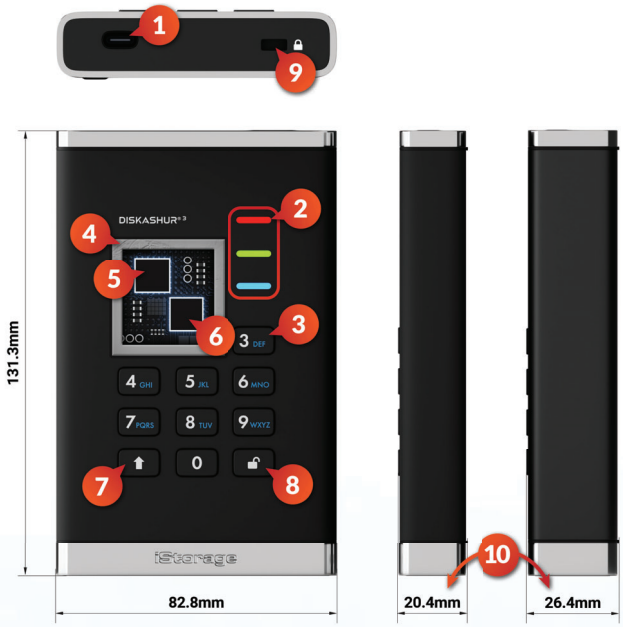
De diskAshur³ is een gebruiksvriendelijke, ultra-veilige, wachtwoord beveiligde, hardware gecodeerde, draagbare HDD/SSD harde schijf met capaciteiten tot wel 5TB (HDD) en tot 16TB (SSD) en oplopend. De diskAshur³ codeert data onderweg en in ruste middels een 256-bit full disk hardware encryptie.

De diskAshur3 bevat een Common Criteria EAL 5+ gecertificeerde veilige microprocessor, met ingebouwde fysieke beschermingsmechanismen die zijn ontworpen om te beschermen tegen externe sabotage, bypass aanvallen en foutieve invoer. In tegenstelling tot andere oplossingen, reageert de diskAshur³ op een geautomatiseerde aanval door in muurvaste blokkeerstand te gaan, waardoor al dit soort aanvallen nutteloos zijn. Simpel gezegd, zonder PIN komt niemand erin!

Inhoud van de doos

- iStorage diskAshur³
- Beschermende draagtas
- USB C & A kabels
- Gratis 1 jaar licentie van Nero BackItUp en iStorage DriveSecurity
- Snelstartgids

diskAshur³ Ontwerp



1. USB 3.2 (Gen 1) Type-C interface
   USB Type C & A kabels inclusief.
2. LED lampjes
   ROOD – *Vergrendeld/Stand-by stand.* CONSTANT GROEN – Ontgrendeld. KNIPPEREND GROEN – Bestandsoverdacht. BLAUW – Admin modus.
3. Epoxyhars gecoat, slijtvast, achtergrondverlicht (door gebruiker te selecteren), alfanumeriek toetsenbord.
4. Fraudebestendig en anti-manipulatief ontwerp
   Alle essentiële componenten zijn omhuld met een laag van zeer sterk en duurzaam epoxyhars.
5. Ingebouwde crypto chip.
6. Ingebouwde Common Criteria EAL 5+ Gecertificeerde Veilige Microprocessor.
7. SHIFT toets.
8. ONTGRENDEL toets.
9. Sleuf voor bureauslot.
10. De diepte van de 4TB&5TB HDD schijf is 26.8mm in plaats van 20.8mm.

1. LED indicatoren en bijbehorende acties

LED	LED Stand	Omschrijving	LED	LED Stand	Omschrijving
	ROOD Constant	Vergrendelde schijf (in **Stand-by** of **Reset** stand)		BLAUW Constant	Schijf in **Admin modus**
	ROOD dubbele knipper	Foutieve invoer pincode		ROOD, GROEN en BLAUW knipperen samen	In afwachting van invoer **Gebruikerspincode**
	GROEN Constant	Schijf ontgrendeld		GROEN en BLAUW Knipperen samen	In afwachting van invoer **Admin** pincode
	GROEN knipperend	Data overdracht actief			

2. LED-status

Inschakelen vanuit inactieve stand

Inactieve stand betekent dat de schijf niet wordt gebruikt en alle LED-lampjes zijn uitgeschakeld. Doe het volgende om de diskAshur3 vanuit inactieve stand in te schakelen

Sluit de schijf aan op een actieve USB-poort van uw computer		Een constant RODE LED gaat aan om aan te geven dat de schijf in Stand-by stand staat.

In inactieve stand zetten

Voer onderstaande acties uit om de diskAshur³ in inactieve stand te zetten;

- Werp de schijf veilig uit en koppel deze af van uw computer, RODE LED gaat nu uit (inactieve stand).

Ingeschakelde Standen

Nadat de schijf 'wakker' is geworden vanuit inactieve stand, zal deze in één van de volgende standen komen te staan, zoals in onderstaande tabel wordt getoond.

Ingeschakelde Stand	LED indicatie	Encryptie Sleutel	Admin pincode	Omschrijving
Oorspronkelijke Verzendstatus	RED and GREEN Constant	✓	×	Wacht op instellen van een Admin pincode (Eerste Gebruik)
Stand-by	RED Constant	✓	✓	Wacht op invoer van Admin, Gebruikers- of Herstelpincode
Reset	RED Constant	×	×	Wacht op instellen van een Admin pincode

3. Eerste Gebruik

De iStorage diskAshur³ wordt geleverd in de '**Oorspronkelijke Verzendstatus' zonder vooraf ingestelde Admin pincode**. Een **8 tot 64**-cijferige Admin pincode dient te worden ingesteld alvorens de schijf kan worden gebruikt. Zodra een Admin pincode succesvol is ingesteld, is het niet meer mogelijk om de schijf terug te zetten in de oorspronkelijke verzendstatus.

Pincode vereisten:

- Moet tussen de 8 en 64 cijfers lang zijn
- Mag niet alleen dezelfde nummers bevatten, bijv. (3-3-3-3-3-3-3-3)
- Mag niet alleen uit opeenvolgende nummers bestaand, bijv. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- De SHIFT toets kan voor additionele combinaties worden gebruikt bijv. (SHIFT (⬆) +1 is een andere waarde dan alleen 1).

Wachtwoordtip: U kunt een herkenbaar woord, naam, zin of elke andere alfanumerieke pincodecombinatie invoeren door de toetsen met corresponderende letters in te drukken.

Voorbeelden van dergelijke alfanumerieke pincodes:

- Voor "**Password**" drukt u de volgende toetsen in:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Voor "**iStorage**" drukt u de volgende toetsen in:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Met deze methode kunnen lange en gemakkelijk te onthouden wachtwoorden worden ingesteld.

Volg de eenvoudige stappen in onderstaande tabel om een Admin pincode in te stellen en de diskAshur³ voor de eerste keer te ontgrendelen.

Instructies - Eerste gebruik	LED	LED-status
1. Sluit de diskAshur³ aan op een actieve USB-poort op uw computer		Constant RODE en GROENE LED's gaan aan om aan te geven dat de schijf in Oorspronkelijke Verzendstatus staat
2. Druk de **Ontgrendel (🔓) + 1** toetsen in en houd deze allebei ingedrukt		LED's worden knipperend GROEN en constant BLAUW
3. Voer een **Nieuwe Admin pincode** (8 tot 64 cijfer) in en druk de **Ontgrendel (🔓)** toets een keer in		Knipperend GROENE en constant BLAUWE LED's verspringen naar een GROENE knipper en dan terug naar knipperend GROENE en constant BLAUWE LED's
4. Voer uw **Nieuwe Admin pincode** opnieuw in en druk de **Ontgrendel (🔓)** toets een keer in		BLAUWE LED knippert snel en verspringt dan naar een constant BLAUWE LED en uiteindelijke naar een constant GROENE LED om aan te geven dat de Admin pincode succesvol is ingesteld en de schijf ontgrendeld en klaar voor gebruik is

Vergrendelen van de diskAshur³
Werp de schijf veilig uit en ontkoppel uit de USB-poort om de schijf te vergrendelen. Als er tegelijkertijd data op de schijf wordt geschreven zal het uitwerpen van de diskAshur³ resulteren in incomplete dataoverdracht en mogelijke beschadiging van data.

4. Ontgrendelen van de diskAshur³ met de Admin pincode

Volg de eenvoudige stappen in onderstaande tabel om de diskAshur³ met de Admin pincode te ontgrendelen.

1. Sluit de diskAshur³ aan op een USB-poort van uw computer		Een constant RODE LED gaat aan om aan te geven dat de schijf in stand-by stand staat.
2. Druk in stand-by stand (constant RODE LED) de **Ontgrendel (🔓)** toets een keer in		GROENE en BLAUWE LED's knipperen samen
3. Voer de **Admin pincode** in terwijl de GROENE en BLAUWE LED's samen knipperen en druk dan de **Ontgrendel (🔓)** toets een keer in		De GROENE LED knippert een paar keer en verspringt dan naar een constant GROENE LED om aan te geven dat de schijf succesvol als Admin is ontgrendeld en klaar is voor gebruik.

5. Admin modus benaderen

Om de beheerdersmodus te openen doet u het volgende.

1. Sluit de diskAshur³ aan op een actieve USB-poort op uw computer		RODE, GROENE en BLAUWE LED's knipperen eenmaal achter elkaar en dan knippert de GROENE LED tweemaal en schakelt uiteindelijk naar een ononderbroken RODE LED die aangeeft dat de drive in stand-by is
2. In stand-by status (ononderbroken RODE LED) houd beide **Ontgrendel (🔓) + 1** knoppen ingedrukt		GROENE en BLAUWE LED's knipperen tegelijkertijd
3. Voer uw beheerderspincode in en druk eenmaal op de **Ontgrendel** (🔓)-knop		GROENE en BLAUWE LED's knipperen verschillende keren snel en tegelijkertijd en gaan dan naar een ononderbroken GROENE LED en verandert tenslotte naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de drive in beheerdersmodus is

De beheerdersmodus verlaten

Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED

6. Wijzigen van de Admin pincode

Pincode vereisten:

- Moet tussen de 8 en 64 cijfers lang zijn
- Mag niet alleen dezelfde nummers bevatten, bijv. (3-3-3-3-3-3-3-3)
- Mag niet alleen uit opeenvolgende nummers bestaand, bijv. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- De SHIFT toets kan voor additionele combinaties worden gebruikt bijv. (SHIFT (⬆) +1 is een andere waarde dan alleen 1).

Wachtwoordtip: U kunt een herkenbaar woord, naam, zin of elke andere alfanumerieke pincodecombinatie invoeren door de toetsen met corresponderende letters in te drukken.

Voorbeelden van dergelijke alfanumerieke pincodes:

- Voor "**Password**" drukt u de volgende toetsen in:
  7 (**p**qrs) **2** (**a**bc) **7** (pqr**s**) **7** (pqr**s**) **9** (**w**xyz) **6** (mn**o**) **7** (pq**r**s) **3** (**d**ef)
- Voor "**iStorage**" drukt u de volgende toetsen in:
  4 (gh**i**) **7** (pqr**s**) **8** (**t**uv) **6** (mn**o**) **7** (pq**r**s) **2** (**a**bc) **4** (**g**hi) **3** (d**e**f)

Met deze methode kunnen lange en gemakkelijk te onthouden wachtwoorden worden ingesteld.

Om de beheerderspincode te veranderen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) ga verder met onderstaande stappen.

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓) + 2**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Voer de **NIEUWE beheerderspincode** in en druk dan eenmaal op de **Ontgrendel (🔓)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's schakelen naar een enkele GROENE knippering en dan terug naar knipperend GROEN en ononderbroken BLAUWE LED's
3. Voer de **NIEUWE beheerderspincode** opnieuw in en druk dan eenmaal op de **Ontgrendel (🔓)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's schakelen naar een snel knipperende BLAUWE LED tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat de beheerderspincode met succes werd gewijzigd

Opmerking: Om de Admin modus onmiddellijk te verlaten (constant BLAUWE LED), druk de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt - de constant BLAUWE LED verspringt nu naar een constant RODE LED.

7. Beleid voor pincode van de gebruiker instellen

De beheerder kan een beperkingsbeleid instellen voor de gebruikerspincode. Dit beleid omvat het instellen van de minimumlengte van de pincode (van 8 tot 64 cijfers), evenals het al dan niet invoeren van een of meer '**Speciale tekens**'. Het 'Speciale teken' functioneert als beide '**SHIFT (⬆) + cijfer**'-knoppen tegelijkertijd worden ingedrukt.

Om een gebruikerspincodebeleid (beperkingen) in te stellen, moet u 3 cijfers invoeren, bijvoorbeeld '**091**', de eerste twee cijfers (**09**) geven de minimumlengte van de pincode aan (in dit geval 9) en het laatste cijfer (**1**) geeft aan dat een of meer 'speciale tekens' moeten worden gebruikt, met andere woorden '**SHIFT (⬆) + cijfer**'. Op dezelfde manier kan een gebruikerspincodebeleid worden ingesteld zonder dat er een 'speciaal teken' nodig is, bijvoorbeeld '**120**', de eerste twee cijfers (**12**) geven de minimumlengte van de pincode aan (**12**) en het laatste cijfer (**0**) betekent dat er geen speciaal teken is vereist.

Als de beheerder eenmaal het gebruikerspincodebeleid ingesteld heeft, bijvoorbeeld '**091**', een nieuwe gebruikerspincode moet worden geconfigureerd - zie hoofdstuk 10, 'Een nieuwe gebruikerspincode toevoegen in de beheerdersmodus'. Als de beheerder de gebruikerspincode configureert als '**247688314**' met een '**speciaal teken' (SHIFT (⬆) + cijfer** samen ingedrukt), kan dit overal in uw 8-64 cijferige pincode worden geplaatst tijdens het proces voor het aanmaken van de gebruikerspincode zoals weergegeven in de onderstaande voorbeelden.

A. '**SHIFT** (⬆) **+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',

B. '2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4',

C. '2', '4', '7', '6', '8', '8', '3', '1', '**SHIFT** (⬆) **+ 4**',

Opmerking:

- Als er bijvoorbeeld een 'speciaal teken' is gebruikt tijdens de configuratie van de gebruikerspincode, bijvoorbeeld '**B**' boven, dan kan de drive alleen worden ontgrendeld door de pincode met het 'speciale teken' in te voeren in precies dezelfde geconfigureerde volgorde als in het bovenstaande '**B**' voorbeeld: ('2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- Er kan meer dan één 'speciaal teken' worden gebruikt en in uw 8-64 cijferige pincode worden toegevoegd.
- Gebruikers kunnen hun pincode wijzigen, maar worden gedwongen zich te houden aan het ingestelde 'gebruikerspincodebeleid' (beperkingen), indien en waar van toepassing
- Als u een nieuwe gebruikerspincode instelt, wordt de gebruikerspincode automatisch verwijderd, indien deze bestaat.
- Dit beleid is niet van toepassing op de 'zelfvernietigingspincode'. De complexiteitsinstelling voor de zelfvernietigingspincode en de beheerderspincode is altijd 8-64 cijfers, zonder vereiste voor een speciaal teken.

Om het **gebruikerspincodebeleid** in te stellen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓) + 7**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Voer uw **3 cijfers** in, onthoud de eerste twee cijfers geef de minimale lengte van de pincode en het laatste cijfer (0 of 1) aan of er al dan niet een speciaal teken is gebruikt.		Knipperende GROENE en BLAUWE LED's zullen blijven knipperen
3. Druk eenmaal op de SHIFT (⬆)-knop		Knipperend GROENE en BLAUWE LED's schakelen naar een ononderbroken GROENE LED tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat de beheerderspincode met succes werd ingesteld.

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

8. Verwijderen van Gebruikerspincodebeleid

Ga eerst naar de "**Admin Modus**" zoals beschreven in hoofdstuk 5 om het **gebruikerspincodebeleid** te verwijderen. Ga verder met de volgende stappen zodra de schijf in **Admin Mode** staat (constant BLAUWE LED).

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓) + 7** buttons		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Voer 070 in en druk eenmaal op de **SHIFT** (⬆)-knop		Knipperend GROENE en BLAUWE LED's schakelen naar een ononderbroken GROENE LED en tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat het beheerderspincodebeleid met succes werd verwijderd.

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

9. Beleid van de gebruikerspincode controleren

De beheerder is in staat het gebruikerspincodebeleid te controleren en kan de minimale pincodelengtebeperking identificeren en of er al dan niet een speciaal teken is ingesteld door op de volgorde van de LED te letten zoals hieronder beschreven.

Om het gebruikerspincodebeleid in te controleren, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **SHIFT** (⬆) **+ 7**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk op de **Ontgrendel (🔓)**-knop en het volgende gebeurt;; a. All LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde. b. Elke knippering van een RODE LED komt overeen met (10) eenheden van een pincode. c. Elke knippering van de GROENE LED komt overeen met een (1) enkele eenheid van een pincode d. Een BLAUWE knippering geeft aan dat er een 'speciaal teken' werd gebruikt. e. All LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde. f. LED's worden terug ononderbroken BLAUW		

De onderstaande tabel beschrijft het LED-gedrag tijdens het controleren van het gebruikerspincodebeleid, bijvoorbeeld als u een 12-cijferige gebruikerspincode heeft ingesteld met het gebruik van een speciaal teken (**121**), de RODE LED knippert eenmaal (**1**) en de GROENE LED knippert tweemaal (**2**) gevolgd door een enkele (**1**) BLAUWE LED knippering waarmee wordt aangeduid dat een Speciaal teken moet worden gebruikt.

Beschrijving van pincode	3-cijferige instelling	ROOD	GROEN	BLAUW
12-cijferige pincode met gebruik van een speciaal teken	121	1 knippering	2 knipperingen	1 knippering
12-cijferige pincode ZONDER speciaal teken	120	1 knippering	2 knipperingen	0
9-cijferige pincode met gebruik van een speciaal teken	091	0	9 knipperingen	1 knippering
9-cijferige pincode ZONDER speciaal teken	090	0	9 knipperingen	0

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

10. Toevoegen van nieuwe gebruikerspincode in Admin modus

Belangrijk: Creatie van een nieuwe gebruikerspincode moet voldoen aan het 'gebruikerspincodebeleid' als deze is ingesteld zoals beschreven in hoofdstuk 7. Dit betekent een minimale lengte van de pincode en gebruik van een 'speciaal karakter'. De Administrator kan hoofdstuk 9 raadplegen om beperkingen van de gebruikerspincode te controleren.

Vereisten voor pincode:

- Moet tussen de 8 en 64 cijfers lang zijn
- Mag niet alleen herhalende cijfers bevatten, bijv. (3-3-3-3-3-3-3-3)
- Mag niet alleen opeenvolgende cijfers bevatten, bijv. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- De **SHIFT** (⬆) -knop kan gebruikt worden voor bijkomende combinaties van pincodes - bijv. **SHIFT (⬆) + 1** is een andere waarde dan 1. Zie hoofdstuk 7, 'Beleid voor pincode van de gebruiker instellen'. .

Om een nieuwe **gebruikerspincode** in te stellen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) ga verder met onderstaande stappen.

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓) + 3**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Voer **nieuwe gebruikerspincode** in en druk op **Ontgrendel (🔓)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's schakelen naar een enkele GROENE knippering en dan terug naar knipperend GROEN en ononderbroken BLAUWE LED's
3. Voer de **nieuwe gebruikerspincode** in en druk weer op **Ontgrendel (🔓)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's veranderen in een snel knipperende GROENE LED en tenslotte naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de nieuwe gebruikerspincode met succes werd geconfigureerd

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

11. De gebruikerspincode veranderen in de beheerdersmodus

Belangrijk: Het veranderen van de gebruikerspincode moet voldoen aan het 'gebruikerspincodebeleid' als er een is geconfigureerd zoals beschreven in hoofdstuk 7, die een minimumlengte van de pincode oplegt en of er een 'speciaal teken' wordt gebruikt. De beheerder kan hoofdstuk 9 raadplegen om de beperkingen van de gebruikerspincode te controleren.

Om een bestaande gebruikerspincode te veranderen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓)** + **3**-knoppen ingedrukt		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Voer **nieuwe gebruikerspincode** in en druk eenmaal op de **Ontgrendel (🔓)**-knop		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Voer de **nieuwe gebruikerspincode** in en druk op **Ontgrendel (🔓)**-knop		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking GREEN LED and finally to a solid BLUE LED indicating the User PIN has been successfully changed

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

12. De gebruikerspincode verwijderen in de beheerdersmodus

Om een bestaande **gebruikerspincode** te verwijderen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **SHIFT** (⬆) **+ 3**-knoppen ingedrukt		Ononderbroken BLAUWE LED zal veranderen naar een knipperende RODE LED
2. Houd beide **SHIFT** (⬆) **+ 3** -knoppen opnieuw ingedrukt		Knipperend RODE LED zal veranderen naar een ononderbroken RODE LED en tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat het gebruikerspincode met succes werd verwijderd.

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

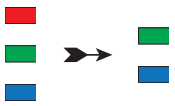
13. Ontgrendelen van diskAshur³ met gebruikerspincode

Ga verder met de volgende stappen om de diskAshur³ met de gebruikerspincode te ontgrendelen.

1. Druk in stand-by stand (constant RODE LED) de **SHIFT (⬆)** en **+ Ontgrendel (🔓)** toetsen in en houd deze allebei ingedrukt		RODE LED verspringt nu naar alle LED's, ROOD, GROEN & BLAUW knipperen tegelijkertijd aan en uit
2. Voer de gebruikerspincode in en druk de **Ontgrendel (🔓)** toets een keer in		ROOD, GROEN en BLAUW knipperende LED's veranderen in een knipperende GROENE LED en dan in een constant GROENE LED om aan te geven dat de schijf succesvol is ontgrendeld in gebruikersmodus

14. Gebruikerspincode wijzigen in gebruikersmodus

Om de gebruikerspincode te wijzigen, ontgrendelt u eerst de diskAshur³ met de gebruikerspincode zoals beschreven in hoofdstuk 13. Ga verder met de volgende stappen zodra de schijf in gebruikersmodus staat (constant GROENE LED).

1. Druk in gebruikersmodus (GROENE LED) de **Ontgrendel (🔓)** + **4** toetsen in en houd deze allebei ingedrukt		Constant GROENE LED verandert in alle LED's, ROOD, GROEN & BLAUW knipperen tegelijkertijd aan en uit
2. Voer uw **bestaande gebruikerspincode** in en d\uk de **Ontgrendel (🔓)** toets een keer in		LED's verspringen naar een enkele GROENE LED knipper en dan terug naar knipperend GROENE en constant BLAUWE LED's
3. Voer de nieuwe gebruikerspincode in en druk de **Ontgrendel (🔓)** toets een keer in		Knipperend GROENE en constante BLAUWE LED's verspringen naar een enkele GROENE LED knipper en dan terug naar knipperend GROENE en constant BLAUWE LED's
4. Voer nogmaals de **nieuwe gebruikerspincode** in en druk de **Ontgrendel (🔓)** toets een keer in		Knipperend GROENE en constant BLAUWE LED's verspringen naar een snel knipperende GROENE LED en dan naar een constant GROENE LED om aan te geven dat de gebruikerspincode succesvol is gewijzigd

Belangrijk: Wijziging van de gebruikerspincode in gebruikersmodus (GROENE LED) moet voldoen aan het 'gebruikerspincodebeleid' als deze is ingesteld zoals beschreven in hoofdstuk 7. Dit betekent een minimale lengte van de pincode en gebruik van een 'speciaal karakter'.

15. Inschakelen LED-achtergrondverlichting van het toetsenbord

De diskAshur³ is voorzien van een toetsenbord met LED-achtergrondverlichting ter ondersteuning van de zichtbaarheid bij weinig licht. Ga eerst naar de Admin modus om de LED-achtergrondverlichting in te schakelen, zoals beschreven in hoofdstuk 5. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **2 & 6** toetsen in en houd deze allebei ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Druk op de **Ontgrendel (🔓)** toets		Knipperend GROENE en BLAUWE LED's verspringen naar een constant GROENE LED en dan naar een constant BLAUWE LED om aan te geven dat het achtergrondverlichte toetsenbord is geactiveerd en deze, de eerstvolgende keer dat de schijf op een USB-poort wordt aangesloten, aan zal gaan

Opmerking: Nadat de diskAshur³ is ingesteld op ingeschakeld LED-achtergrondverlicht toetsenbord, dient de schijf eerst uit de actieve USB-poort te worden verwijderd en dan opnieuw te worden aangesloten om deze instelling te activeren. Druk de **SHIFT** (⬆) Nadat de diskAshur³ is ingesteld op ingeschakeld LED-achtergrondverlicht toetsenbord, dient de schijf eerst uit de actieve USB-poort te worden verwijderd en dan opnieuw te worden aangesloten om deze instelling te activeren.

16. Uitschakelen LED-achtergrondverlichting van het toetsenbord

Ga eerst naar de **Admin Modus** om de LED-achtergrondverlichting uit te schakelen zoals beschreven in hoofdstuk 5. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **2 & 3** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Druk de **Ontgrendel (🔓)** toets in		Knipperend GROENE en BLAUWE LED's verspringen naar een constant GROENE LED en dan naar een constant BLAUWE LED om aan te geven dat het achtergrondverlichte toetsenbord is gedeactiveerd en deze, de eerstvolgende keer dat de schijf op een USB-poort wordt aangesloten, uit zal schakelen

Opmerking: Nadat de diskAshur³ is ingesteld op uitgeschakeld LED-achtergrondverlicht toetsenbord, dient de schijf eerst uit een actieve USB-poort te worden verwijderd en dan opnieuw te worden aangesloten om deze instelling te activeren. Druk de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt om de Admin Modus onmiddellijk te verlaten (constant BLAUWE LED), - de constant BLAUWE LED verspringt nu naar een constant RODE LED.

17. Eenmalig herstel van gebruikerspincode aanmaken

De gebruikersherstelpincode is zeer nuttig in situaties wanneer de gebruiker zijn of haar pincode is vergeten om de diskAshur³ te ontgrendelen.

Om de herstelmodus te activeren dient de gebruiker eerst de correcte eenmalige herstelpincode in te voeren, mits deze is ingesteld. Het gebruikerspincode-herstelproces heeft geen invloed op de data, encryptiesleutel noch op de Admin pincode, maar de gebruiker moet wel een nieuwe 8 tot 64-cijferige pincode instellen.

Ga eerst naar de "**Admin Modus**" om een eenmalige 8 tot 64-cijferige gebruikersherstelpincode in te stellen, zoals beschreven in hoofdstuk 5. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **Ontgrendel (🔓) + 4** toetsen in en houd deze allebei ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en constante BLAUWE LED's
2. Voer een **Eenmalige Herstelpincode** in en druk op de **Ontgrendel (🔓)** toets		Knipperend GROENE en constante BLAUWE LED's verspringen naar een enkele GROENE LED knipper en dan terug naar knipperend GROENE en constant BLAUWE LED's
3. Voer nogmaals uw **Eenmalige Herstelpincode** in en druk de **Ontgrendel (🔓)** toets opnieuw in		Knipperend GROENE en constant BLAUWE LED's veranderen in snel knipperend GROENE LED en uiteindelijk in een constant BLAUWE LED om aan te geven dat de eenmalige herstelpincode succesvol is ingesteld

Opmerking: Druk de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt om de Admin Modus onmiddellijk te verlaten (constant BLAUWE LED), - de constant BLAUWE LED verspringt nu naar een constant RODE LED.

18. Eenmalig herstel van gebruikerspincode verwijderen

Ga eerst naar de "**Admin Modus**" om een eenmalige gebruikersherstelpincode in te stellen, zoals beschreven in hoofdstuk 5. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **SHIFT** (⬆) **+ 4** toetsen in en houd deze allebei ingedrukt		Constant BLAUWE LED verandert in een knipperend RODE LED
2. Druk de **SHIFT (⬆) + 4** opnieuw in en houd deze allebei ingedrukt		Knipperend RODE LED wordt constant ROOD en verspringt dan naar een constant BLAUWE LED om aan te geven dat de eenmalige gebruikersherstelpincode succesvol is verwijderd

Opmerking: Druk de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt om de Admin Modus onmiddellijk te verlaten (constant BLAUWE LED), - de constant BLAUWE LED verspringt nu naar een constant RODE LED.

19. Aanmaken van eenmalige gebruikersherstelpincode

De gebruikersherstelpincode is zeer nuttig in situaties wanneer de gebruiker zijn of haar pincode is vergeten om de diskAshur³ te ontgrendelen.

Om de herstelmodus te activeren dient de gebruiker eerst de correcte eenmalige herstelpincode in te voeren, mits deze is ingesteld. Het gebruikerspincode-herstelproces heeft geen invloed op de data, encryptiesleutel noch op de Admin pincode, maar de gebruiker moet wel een nieuwe 8 tot 64-cijferige pincode instellen.

Ga verder met de volgende stappen om het herstelproces te activeren en een nieuwe gebruikerspincode in te stellen.

1. Druk in **Stand-by stand** (RODE LED) de **Ontgrendel (🔓) + 4** toetsen in en houd deze ingedrukt		Constant RODE LED verandert in knipperend RODE en GROENE LED's
2. Voer de eenmalige **Herstelpincode** in en druk op de **Ontgrendel (🔓)** toets		GROENE en BLAUWE LED's gaan afwisselend aan en uit, worden dan constant GROEN en uiteindelijk knipperend GROENE en constante BLAUWE LED's
3. Voer een **Nieuwe Gebruikerspincode** in en druk op de **Ontgrendel (🔓)** toets		Knipperend GROENE en constant BLAUWE LED's veranderen in een enkele GROENE LED knipper en vervolgens terug in knipperend GROENE en constant BLAUWE LED's
4. Voer nogmaals uw **Gebruikerspincode** in en druk de **Ontgrendel (🔓)** toets opnieuw in		GROENE LED knippert snel en wordt dan constant GROEN om aan te geven dat het herstelproces gereed is en een nieuwe gebruikerspincode is ingesteld

Belangrijk: Een nieuwe gebruikerspincode moet voldoen aan het 'gebruikerspincodebeleid' als deze is ingesteld zoals beschreven in hoofdstuk 7. Dit betekent een minimale pincode lengte en het gebruik van een speciaal karakter. Raadpleeg hoofdstuk 9 om de beperkingen van de gebruikerspincode na te gaan.

20. Alleen-lezen toegang voor gebruiker instellen in de beheerdersmodus

Met zoveel virussen en trojans die USB-schijven infecteren is de alleen-lezen functionaliteit extra handig wanneer u in een publieke omgeving data op USB-schijven wilt benaderen. Dit is ook een essentiële functionaliteit voor forensische doeleinden, wanneer data in originele en onveranderde staat moet worden bewaard en niet aangepast of overschreven mag worden.

Wanneer de Administrator de diskAshur³ configureert en de gebruikerstoegang tot alleen-lezen beperkt, kan alleen de Administrator op de schijf schrijven of de instelling terugzetten naar lezen/schrijven zoals beschreven in hoofdstuk 21. De gebruiker is beperkt tot alleen-lezen toegang en kan niet op de schijf schrijven of deze instelling wijzigen in gebruikersmodus.

Ga eerst naar de "**Admin Modus**" zoals beschreven in hoofdstuk 5 om de diskAshur³ in te stellen en gebruikerstoegang te beperken tot alleen-lezen. Ga verder met de volgende stappen zodra de schijf in Admin Modus (constant BLAUWE LED) staat.

1. In beheerdersmodus houdt u beide **"7 + 6"**-knoppen ingedrukt.		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk eenmaal op de **Ontgrendel (🔓)** knop		GROENE en BLAUWE LED's zullen veranderen naar een ononderbroken GROENE LED en dan naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de drive werd geconfigureerd en het beperkt de toegang voor de gebruiker tot alleen-lezen

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

21. Gebruiker lezen/schrijven in de beheerdersmodus inschakelen

Om de diskAshur³ terug in te stellen naar lezen/schrijven, gaat u eerst naar de "**beheerdersmodus**" zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** (ononderbroken BLAUWE LED) is, ga verder met de volgende stappen.

1. In beheerdersmodus houdt u beide "**7 + 9**" knoppen ingedrukt.		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk eenmaal op de **Ontgrendel (🔓)** knop		GROENE en BLAUWE LED's veranderen naar een GROENE LED en dan naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de drive als lezen/schrijven is geconfigureerd

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

22. Instellen van algemeen alleen-lezen in Admin modus

Wanneer de administrator de diskAshur³ configureert en beperkt tot alleen-lezen in het algemeen, dan kan de administrator noch de gebruiker op de schijf schrijven en zijn beiden beperkt tot alleen-lezen toegang. Alleen de administrator is in staat om de instelling terug te zetten naar lezen/schrijven zoals beschreven in hoofdstuk 23.

Ga eerst naar de "**Admin Mode**" om de diskAshur³ in te stellen en te beperken tot algemene toegang met alleen-lezen, zoals beschreven in hoofdstuk 5. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** (constant BLAUWE LED) staat.

1. Druk in de Admin modus de "**5 + 6**" toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Druk op de **Ontgrendel (🔓)** toets		GROENE en BLAUWE LED's veranderen in een constant GROENE LED en dan in een constant BLAUWE LED om aan te geven dat de schijf is ingesteld en algemene toegang beperkt tot alleen-lezen.

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

23. Globaal lezen/schrijven in de beheerdersmodus inschakelen

Ga eerst naar de "**Admin Modus**" om de diskAshur³ vanuit de algemene alleen-lezen instelling terug te zetten naar lezen/schrijven, zoals beschreven in hoofdstuk 5. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** (constant BLAUWE LED) staat.

1. Druk in de Admin modus de "**5 + 9**" toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Druk de **Ontgrendel (🔓)** toets in		GROENE en BLAUWE LED's veranderen in een constant GROENE LED en dan in een constant BLAUWE LED om aan te geven dat de schijf op lezen/schrijven is ingesteld

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

24. Zelfvernietigingspincode configureren

U kunt een zelfvernietigingspincode instellen die, wanneer deze wordt ingevoerd, een Crypto-Erase op de schijf uitvoert (encryptiesleutel wordt verwijderd). Dit proces verwijdert alle ingestelde pincodes en maakt alle opgeslagen data op de schijf ontoegankelijk (voor altijd verloren). De schijf toont zich dan als onvergrendeld; GROENE LED. Het uitvoeren van deze functionaliteit maakt de zelfvernietigingspincode de nieuwe gebruikerspincode. De schijf moet dan wel worden geformatteerd alvorens deze opnieuw kan worden gebruikt.

Om de zelfvernietigingspincode in te stellen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓)** + 6-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Configureer en voer een 8.64-cijferige **zelfvernietigingspincode** in en druk op de **Ontgrendel (🔓)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's schakelen naar een enkele GROENE knippering en dan terug naar knipperend GROEN en ononderbroken BLAUWE LED's
3. Voer opnieuw uw **zelfvernietigingspincode** in en druk weer op de **Ontgrendel (🔓)**-knop		GROENE LED zal gedurende enkele seconden snel knipperen en verandert dan naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de zelfvernietigingspincode met succes werd geconfigureerd

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

25. Zelfvernietigingspincode verwijderen

Om de zelfvernietigingspincode in te verwijderen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **SHIFT (⬆) + 6**-knoppen ingedrukt		Ononderbroken BLAUWE LED zal veranderen naar een knipperende RODE LED
2. Houd weer de **SHIFT (⬆) + 6**-knoppen ingedrukt		Knipperende RODE LED zal overgaan naar ononderbroken en verandert dan naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de zelfvernietigingspincode met succes werd verwijderd

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

26. Ontgrendelen met de zelfvernietigingspincode

Waarschuwing: Wanneer het zelfvernietigingsmechanisme is geactiveerd, worden alle data, encryptiesleutel en de Admin- en gebruikerspincodes verwijderd. **De Zelfvernietigingspincode wordt de Gebruikerspincode**. Er bestaat geen Admin pincode meer nadat het zelfvernietigingsmechanisme is geactiveerd. De diskAshur³ zal gereset moeten worden (raadpleeg eerst 'complete reset uitvoeren' in hoofdstuk 36,op pagina 232) om een Admin pincode met volledige Admin privileges in te stellen inclusief de mogelijkheid tot het instellen van een nieuwe gebruikerspincode.

De zelfvernietigingspincode zal, wanneer deze wordt gebruikt, **alle data, encryptiesleutel, Admin- en gebruikerspincodes verwijderen** en de schijf vervolgens ontgrendelen. Door het activeren van deze functionaliteit wordt de **zelfvernietigingspincode de nieuwe gebruikerspincode**. De diskAshur³ zal moeten worden geformatteerd alvorens nieuwe data op de schijf kan worden gezet.

Om het zelfvernietigingsmechanisme te activeren, dient de schijf in stand-by stand te staan (constant RODE LED). Ga vervolgens verder met de volgende stappen.

1. . Druk in **Stand-by stand** (constant RODE LED) de **SHIFT (⬆) + Ontgrendel (🔓)** toetsen in en houd deze ingedrukt		RODE LED verspringt naar alle LED's, ROOD, GROEN & BLAUW knipperen aan en uit
2. Voer de Zelfvernietigingspincode in en druk de **Ontgrendel (🔓)** toets in		ROOD, GROEN en BLAUW knipperende LED's veranderen in een knipperend GROENE LED en dan in een constant GROENE LED om aan te geven dat de diskAshur³ zichzelf succesvol heeft vernietigd

27. Beheerderspincode configureren of opnieuw instellen na een brute aanval

Het is noodzakelijk om na een brute aanval of wanneer de diskAshur³ opnieuw is ingesteld om een beheerderspincode te configureren voordat de drive kan worden gebruikt.

Pincode vereisten:

- Moet tussen de 8 en 64 cijfers lang zijn
- Mag niet alleen dezelfde nummers bevatten, bijv. (3-3-3-3-3-3-3-3)
- Mag niet alleen uit opeenvolgende nummers bestaand, bijv. (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- De SHIFT toets kan voor additionele combinaties worden gebruikt bijv. (SHIFT (⬆) +1 is een andere waarde dan alleen 1).

Als de diskAshur³ werd aangevallen of opnieuw werd ingesteld, zal de drive in stand-by status zijn (ononderbroken RODE LED). Om een beheerderspincode te configureren, ga verder met de volgende stappen.

1. In stand-by status (ononderbroken RODE LED) houdt u beide **SHIFT** (⬆) **+ 1**-knoppen ingedrukt		Ononderbroken RODE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Voer uw nieuwe beheerderspincode in en druk weer op de **Ontgrendel (🔓)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's schakelen naar een enkele GROENE knippering en dan terug naar knipperend GROEN en ononderbroken BLAUWE LED's
3. Voer de NIEUWE beheerderspincode opnieuw in en druk dan op de **Ontgrendel (🔓)**-knop		Knipperend GROENE LED en ononderbroken BLAUWE LED schakelen gedurende enkele seconden naar een snel knipperende BLAUWE LED en tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat de beheerderspincode met succes werd geconfigureerd.

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

28. De onbeheerde automatische vergrendeling instellen

Als beveiliging tegen ongeautoriseerde toegang als de drive ontgrendeld en onbewaakt is, kan de diskAshur³ worden ingesteld naar automatische vergrendeling na een vooraf ingestelde tijdsduur. In de standaardstatus is de time-out functie van de diskAshur³ onbeheerde automatische vergrendeling uitgeschakeld. De onbeheerde automatische vergrendeling kan worden ingesteld om te activeren tussen 5 - 99 minuten.

Om de time-out functie voor onbeheerde automatische vergrendeling in te stellen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓) + 5**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Voer de tijdsperiode in waarvoor u de time-out functie voor de automatische vergrendeling wilt instellen, de minimale tijd die kan worden ingesteld is 5 minuten en het maximum is 99 minuten (5-99 minuten). Voer bijvoorbeeld in: **05 voor 5 minuten (druk op '0' gevolgd door een '5')** **20 voor 20 minuten (druk op '2' gevolgd door een '0')** **99 voor 99 minuten (druk op '9' gevolgd door een '9')**		
3. Druk op de **SHIFT** (⬆)-knop		Knipperend GROENE en BLAUWE LED's schakelen naar een ononderbroken GROENE LED gedurende een seconde en tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat de time-out van de automatische vergrendeling met succes werd geconfigureerd.

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

29. De onbeheerde automatische vergrendeling uitschakelen

Om de time-out functie voor onbeheerde automatische vergrendeling uit te schakelen, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** (ononderbroken BLAUWE LED) is, ga verder met de volgende stappen.

1. Houd in de beheerdersmodus beide **Ontgrendel (🔓) + 5**-knoppen ingedrukt		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Voer **00** in en druk op de **SHIFT** (⬆)-knop		Knipperend GROENE en BLAUWE LED's veranderen naar een ononderbroken GROENE LED gedurende een seconde en tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat de time-out van de automatische vergrendeling met succes werd uitgeschakeld.

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

30. De onbeheerde automatische vergrendeling controleren

De beheerder kan de tijdsduur die is ingesteld voor de time-out functie voor de onbeheerde automatische vergrendeling controleren en bepalen door eenvoudig te letten op de LED-volgorde zoals beschreven in onderstaande tabel.

Om de onbeheerde automatisch vergrendeling te controleren, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. Houd in beheerdersmodus de **SHIFT** (⬆) **+ 5** ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Druk op de **Ontgrendel (🔓)**-knop en het volgende gebeurt; a. All LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde. b. Elke knippering van de RODE LED komt overeen met (10) minuten. c. Elke knippering van de GROENE LED komt overeen met een (1) minuut. d. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde. e. LED's worden terug ononderbroken BLAUW		

De onderstaande tabel beschrijft het LED-gedrag tijdens het controleren van de onbeheerde automatische vergrendeling, bijvoorbeeld als u de drive heeft ingesteld om automatisch te vergrendelen na **25** minuten, zal de RODE LED tweemaal (**2**) knipperen en de GROENE LED vijf (**5**) keer.

Automatisch vergrendelen in enkele minuten	**ROOD**	**GROEN**
5 minuten	0	5 knipperingen
15 minuten	1 knippering	5 knipperingen
25 minuten	2 knipperingen	5 knipperingen
40 minuten	4 knipperingen	0

Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

31. Alleen-lezen in de gebruikersmodus instellen

Om de diskAshur³ in te stellen op alleen-lezen, gaat u eerst naar de "**gebruikersmodus**" zoals beschreven in hoofdstuk 13. Zodra de drive in **gebruikersmodus** (ononderbroken GROENE LED) is, gaat u verder met de volgende stappen.

1. In gebruikersmodus houdt u beide "**7 + 6**"-knoppen ingedrukt. (7=**R**ead + 6=**O**nly)		Ononderbroken GROENE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Druk op de **Ontgrendel (🔓)**-knop		GROENE en BLAUWE LED's veranderen naar een ononderbroken GROENE LED waarmee wordt aangeduid dat de drive als alleen-lezen is geconfigureerd

Opmerking: 1. Als een gebruiker de drive instelt als alleen-lezen, kan de beheerder dit negeren door de drive in te stellen als lezen/schrijven in de beheerdersmodus.

2. Als de beheerder de drive instelt als alleen-lezen, kan de gebruiker de drive niet instellen als lezen/schrijven.

32. Lezen/schrijven in gebruikersmodus inschakelen

Om de diskAshur³ in te stellen in lezen/schrijven, gaat u eerst naar de "**gebruikersmodus**" zoals beschreven in hoofdstuk 13. Zodra de drive in **gebruikersmodus** (ononderbroken GROENE LED) is, gaat u verder met de volgende stappen.

1. In gebruikersmodus houdt u knoppen "**7 + 9**" ingedrukt. (7=**R**ead + 9=**W**rite)		Ononderbroken GROENE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Druk op de **Ontgrendel (🔓)**-knop		GROENE en BLAUWE LED's veranderen naar een ononderbroken GROENE LED waarmee wordt aangeduid dat de drive als lezen/schrijven is geconfigureerd

Opmerking: 1. Als een gebruiker de drive instelt als alleen-lezen, kan de beheerder dit negeren door de drive in te stellen als lezen/schrijven in de beheerdersmodus.

2. Als de beheerder de drive instelt als alleen-lezen, kan de gebruiker de drive niet instellen als lezen/schrijven.

33. Brute Force Hack verdedigingsmechanisme

De diskAshur³ bevat een verdedigingsmechanisme om te beschermen tegen een Brute Force aanval. De brute force beperking voor **Admin en Gebruikerspincodes** staat standaard ingesteld op **10** opeenvolgende foutieve pincode invoerpogingen en op **5** voor de **Herstelpincode**. Er worden drie onafhankelijke brute force tellers gebruikt om de foutieve pincode invoerpogingen voor elke pincode autorisatie op te nemen. Wanneer een gebruiker tien keer achter elkaar een foutieve Admin pincode invoert (onderverdeeld in 5,3,2, clusters zoals hieronder beschreven) zal de schijf worden gereset en gaat alle data voor altijd verloren. Wanneer een gebruiker een herstelpincode of gebruikerspincode invoert en de respectievelijke brute force beperking overschrijdt, worden deze pincodes gewist maar blijft de data wel op de schijf staan.

Opmerking: De brute force beperking wordt op initiële waarden geprogrammeerd wanneer de schijf compleet is gereset of wanneer de zelfvernietigingsfunctionaliteit is geactiveerd. Als de Admin de gebruikerspincode wijzigt of er een nieuwe gebruikerspincode wordt ingesteld na activatie van de herstelfunctionaliteit, wordt de gebruikerspincode brute force teller gewist maar heeft dit geen invloed op de brute force beperking. Wanneer de Admin de herstelpincode wijzigt, wordt de herstelpincode brute force teller gewist. Succesvolle autorisatie van een bepaalde pincode zal de brute force teller van deze specifieke pincode wissen, maar de brute force teller van de andere pincodes niet beïnvloeden. Mislukte autorisatie van een bepaalde pincode verhoogt de brute force teller van die specifieke pincode maar heeft geen invloed op de brute force teller van andere pincodes.

- Wanneer een gebruiker een **foutieve gebruikerspincode** 10 keer achtereenvolgens invoert, zal de gebruikerspincode worden gewist maar blijven de data, Admin pincodes en herstelpincodes intact en toegankelijk.
- Wanneer een **foutieve herstelpincode** 5 keer achtereenvolgens wordt ingevoerd, wordt de herstelpincode gewist maar blijven de data en Admin pincode intact en toegankelijk.
- De **Admin pincode** maakt gebruikt van een meer verfijnd verdedigingsmechanisme vergeleken met gebruikers- en herstelpincodes. Na **5 opeenvolgende foutieve Admin pincode invoerpogingen,** gaat de schijf op slot en lichten de RODE, GROENE en BLAUWE LED's constant op. Vanaf dit moment dienen de volgende stappen te worden genomen om de gebruiker nog 3 pincode invoerpogingen toe te staan.

- Voer pincode "**47867243**" in en druk de **Ontgrendel (🔓)** toets in, GROENE en BLAUWE LED's knipperen samen. De schijf is nu klaar om invoer van de volgende extra **3** Admin pincodes te accepteren
- Na totaal 8 opeenvolgende foutieve pincode invoerpogingen gaat de schijf op slot en knipperen de RODE, GROENE en BLAUWE LED's afwisselend. Vanaf dit moment dienen de volgende stappen te worden genomen om de laatste **2** pincode invoerpogingen te krijgen (10 in totaal).
- Voer pincode "**47867243**" in en druk de c toets in, GROENE en BLAUWE LED's knipperen samen en de schijf is nu klaar om de laatste **2** pincode invoerpogingen te accepteren (10 in totaal).
- Na totaal 10 foutieve invoerpogingen van de Admin pincode, wordt de encryptiesleutel verwijderd en gaan alle data en pincodes die op de schijf zijn opgeslagen, voor altijd verloren.

Onderstaande tabel gaat er vanuit dat alle drie pincodes zijn ingesteld en onderstreept het effect van het triggeren van het brute force verdedigingsmechanisme voor elke afzonderlijke pincode.

Pincode om schijf te ontgrendelen	Opeenvolgende foutieve pincode invoerpogingen	Beschrijving van wat er gebeurt
Gebruikerspincode	10	• De Gebruikerspincode wordt verwijderd. • De Herstelpincode, de Admin pincode en alle data blijven intact en toegankelijk.
Herstelpincode	5	• De Herstelpincode wordt verwijderd. • De Admin pincode en alle data blijven intact en toegankelijk.
Admin pincode	5 3 2 (10 in total)	• Na **5** opeenvolgende foutieve invoerpogingen van de Admin pincode, gaat de schijf op slot en lichten alle LED's constant op. • Voer pincode "**47867243**" in en druk de **Ontgrendel (🔓)** toets in om **3** extra pincode invoerpogingen te krijgen. • Na totaal **8** (5+3) opeenvolgende foutieve invoerpogingen van de Admin pincode, gaat de schijf op slot en knipperen de LED's afwisselend. • Voer pincode "**47867243**" in en druk de **Ontgrendel (🔓)** toets in om de laatste **2** pincode invoerpogingen te krijgen (10 in totaal). • Na totaal 10 opeenvolgende foutieve invoerpogingen van de Admin pincode, wordt de encryptiesleutel verwijderd en gaan alle data en pincodes op de schijf voor altijd verloren.

Belangrijk: Een nieuwe Admin pincode dient te worden ingesteld als de vooringestelde Admin pincode is gecompromitteerd door brute force. Raadpleeg Hoofdstuk 27 op pagina 226 voor 'Admin pincode instellen na een Brute Force aanval of Reset'. De diskAshur³ zal ook moeten worden geformatteerd alvorens nieuwe data op de schijf kan worden gezet.

34. De gebruikerspincode instellen om brute aanvallen te beperken

Opmerking: De brute force beperking van de gebruikerspincode is standaard ingesteld op 10 opeenvolgende foutieve pincode invoerpogingen wanneer de schijf ofwel compleet wordt gereset, met brute force wordt aangevallen of de zelfvernietigingspincode wordt geactiveerd

De brute force beperking voor de diskAshur³ gebruikerspincode kan door de Administrator her geprogrammeerd en ingesteld worden. Deze functionaliteit kan worden ingesteld om 1 tot 10 opeenvolgende foutieve pincode invoerpogingen toe te staan.

Ga eerst naar de "**Admin Modus**" zoals beschreven in hoofdstuk 5, om de brute force beperking voor de gebruikerspincode in te stellen. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **7 + 0** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in GROENE en BLAUWE LED's die samen knipperen
2. Voer het aantal pogingen in voor de brute force beperking (tussen 01 en 10), voer bijvoorbeeld in: • **01** voor 1 poging • **10** voor 10 pogingen		
3. Druk de SHIFT (⬆) toets een keer in		Knipperend GROENE en BLAUWE LED's verspringen gedurende een seconde naar een constant GROENE LED en dan naar een constant BLAUWE LED om aan te geven dat de brute force beperking succesvol is geconfigureerd

Opmerking: Druk om de Admin Modus (constant BLAUWE LED) onmiddellijk te verlaten, de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt, - constant BLAUWE LED wordt nu een constant RODE LED.

35. De gebruikerspincode tegen beperking van brute aanvallen controleren

De Administrator is in staat om te observeren en het aantal opeenvolgende foutieve invoerpogingen van de gebruikerspincodes te bepalen dat mag worden ingevoerd voordat het Brute Force verdedigingsmechanisme wordt getriggerd, door eenvoudigweg de volgorde van de LED's te noteren, zoals hieronder wordt beschreven.

Ga eerst naar de "Admin Modus" zoals beschreven in hoofdstuk 5 om de instelling van de brute beperking te controleren. Ga verder met de volgende stappen zodra de schijf in Admin Modus staat (constant BLAUWE LED).

1. Druk in Admin modus de **2 + 0** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Druk de **Ontgrendel (🔓)** toets in en het volgende gebeurt: a. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende 1 seconde constant. b. Elke RODE LED knipper staat gelijk aan tien (10) eenheden van een brute force beperkingsnummer. c. Iedere GROENE LED knipper staat gelijk aan een (1) enkele eenheid van een brute force beperkingsnummer. d. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende 1 seconde constant. e. LED's worden weer constant BLAUW		

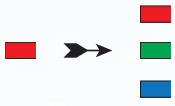
Onderstaande tabel beschrijft het LED-gedrag terwijl de instelling van de brute force beperking wordt gecontroleerd. Wanneer u bijvoorbeeld de schijf hebt ingesteld om te 'brute forcen' na **5** opeenvolgende foutieve pincode invoerpogingen. De GROENE LED zal vijf (**5**) keer knipperen.

Brute Force Beperking Instelling	ROOD	GROEN
2 pogingen	0	2 knippers
5 pogingen	0	5 knippers
10 pogingen	1 knipper	0

Opmerking: Druk om de Admin Modus (constant BLAUWE LED) onmiddellijk te verlaten, de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt, - constant BLAUWE LED wordt nu een constant RODE LED.

36. Een volledige reset uitvoeren

Om een volledige reset uit te voeren moet diskAshur³ in stand-by status (ononderbroken RODE LED) zijn. Zodra de drive opnieuw is ingesteld zullen alle beheerders-/gebruikerspincodes, encryptiesleutel en alle gegevens worden verwijderd en voor altijd verdwijnen en de drive moet worden geformatteerd voordat hij opnieuw kan worden gebruikt. Om de diskAshur³ te resetten gaat u verder met de volgende stappen.

1. In stand-by status (ononderbroken RODE LED) houdt u de "**0**"-knop ingedrukt		Ononderbroken RODE LED wisselt naar alle LED's, ROOD, GROEN & BLAUW die aan en uit knipperen
2. Houd beide **2 + 7**-knoppen ingedrukt		RODE, GROENE en BLAUWE afwisselende LED's blijven gedurende een seconde ononderbroken en gaan dan naar een ononderbroken RODE LED waarmee wordt aangeduid dat de drive werd gereset

Belangrijk: Na een volledige reset moet een nieuwe beheerderspincode worden geconfigureerd, zie hoofdstuk 27 op pagina 226 in 'Het configureren of opnieuw instellen na een brute aanval of reset', de diskAshur³ zal ook opnieuw moeten worden geformatteerd voordat er nieuwe data aan de drive kunnen worden toegevoegd.

37. diskAshur³ instellen als opstartbaar

Opmerking: Wanneer de schijf is ingesteld als opstartbaar (bootable), zal het uitwerpen van de schijf uit het besturingssysteem de LED niet forceren ROOD te worden. De schijf blijft constant GROEN en moet worden afgekoppeld voor volgend gebruik. De diskAshur³ is standaard ingesteld als niet-opstartbaar (non-bootable).

De diskAshur³ is uitgerust met een opstartbare functionaliteit om power cycling mogelijk te maken tijdens het opstartproces van de host. Wanneer er vanaf de diskAshur³, wordt opgestart, bestuurt u uw computer met het besturingssysteem dat op de diskAshur³ staat geïnstalleerd.

Ga eerst naar de "**Admin Modus**" zoals beschreven in hoofdstuk 5 om de schijf als opstartbaar in te stellen.
Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **Ontgrendel (🔓) + 9** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Druk "**0**" in gevolgd door een **"1"** (**01**)		GROENE en BLAUWE LED's zullen blijven knipperen
3. Druk de **SHIFT** (⬆) toets een keer in		Knipperend GROENE en BLAUWE LED's veranderen in een constant GROENE LED en uiteindelijk in een constant BLAUWE LED om aan te geven dat de schijf succesvol is ingesteld als opstartbaar (bootable)

Opmerking: Druk om de Admin Modus (constant BLAUWE LED) onmiddellijk te verlaten, de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt, - constant BLAUWE LED wordt nu een constant RODE LED

38. De diskAshur³ opstartfunctie uitschakelen

Ga eerst naar de "**Admin Modus**" zoals beschreven in hoofdstuk 5 om de diskAshur³ opstartbare functionaliteit uit te schakelen. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **Ontgrendel (🔓) + 9** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Toets de **"0"** in gevolgd door nog een **"0"** (**00**)		GROENE en BLAUWE LED's zullen blijven knipperen
3. Druk de **SHIFT** (⬆) toets een keer in		Knipperend GROENE en BLAUWE LED's veranderen in een constante GROENE LED en uiteindelijk in een constant BLAUWE LED om aan te geven dat de opstartbare functionaliteit succesvol is uitgeschakeld

Opmerking: Druk om de Admin Modus (constant BLAUWE LED) onmiddellijk te verlaten, de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt, - constant BLAUWE LED wordt nu een constant RODE LED

39. De opstartinstelling controleren

Ga eerst naar de "**Admin Modus**" zoals beschreven in hoofdstuk 5 om de opstartbare functionaliteit te controleren. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **SHIFT** (⬆) **+ 9** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's

2. Druk de **Ontgrendel (🔓)** toets in en dan ziet u één van de twee onderstaande scenario's gebeuren;

- **Als de diskAshur³ als opstartbaar is ingesteld, gebeurt het volgende;**

a. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
b. GROENE LED knippert één keer.
c. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
d. LED's worden weer constant BLAUW

- **Als de diskAshur³ NIET als opstartbaar is ingesteld, gebeurt het volgende;**

a. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
b. Alle LED's gaan uit.
c. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
d. LED's worden weer constant BLAUW

Opmerking: Druk om de Admin Modus (constant BLAUWE LED) onmiddellijk te verlaten, de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt, - constant BLAUWE LED wordt nu een constant RODE LED

.

40. Encryptiemodus instellen

WAARSCHUWING: Wijziging van de encryptiemodus van AES-XTS (standaard instelling) naar AES-ECB of AES-CBC zal de encryptiesleutel verwijderen en de diskAshur³ resetten en alle data ontoegankelijk maken en voor altijd verloren doen gaan!

Voer de volgende stappen uit om de diskAshur³ encryptiemodus te configureren als **AES-ECB** aangegeven door nummer '**01**', of **AES-XTS** aangegeven door nummer '**02**', of **AES-CBC** aangegeven door nummer '**03**'. Deze functionaliteit is standaard als AES-XTS (02) ingesteld. Houd er rekening mee dat wanneer er naar een andere encryptiemodus wordt overgegaan alle kritische parameters worden verwijderd en de schijf wordt gereset.

Ga eerst naar de **Admin Modus** zoals beschreven in hoofdstuk 5 (constant BLAUWE LED) om de diskAshur³ encryptiemodus in te stellen en ga verder met de volgende stappen:

1. Druk in Admin Modus de **Ontgrendel (🔓) + 1** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Voer **01** in om als **AES-ECB** Voer **02** in om als **AES-XTS (standaard)** in te stellen Voer **03** in om als **AES-CBC**		GROENE en BLAUWE LED's zullen blijven knipperen
3. Druk de (⬆) toets een keer in		GROENE en BLAUWE LED's veranderen in een constant GROENE LED en dan in een constant RODE LED (Reset stand) om aan te geven dat de encryptiemodus succesvol is gewijzigd

Belangrijk: Na het configureren van de encryptiemodus wordt de diskAshur³ volledig gereset en wordt er een nieuwe Admin pincode moet worden geconfigureerd. Raadpleeg Paragraaf 27 op pagina 226 over 'Een beheerderspincode configureren na een brute force-aanval of reset'.

41. Encryptiemodus controleren

Ga eerst naar de **Admin Modus** zoals beschreven in hoofdstuk 5 om de diskAshur³ encryptiemodus te controleren. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **SHIFT** (⬆) **+ 1** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's

2. Druk de **Ontgrendel (🔓)** toets in en het volgende gebeurt:

- **Als de encryptiemodus is geconfigureerd als AES-ECB, gebeurt het volgende:**

a. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
b. GROENE LED knippert één keer.
c. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
d. LED's worden weer constant BLAUW

- **Als de encryptiemodus is geconfigureerd als AES-XTS, gebeurt het volgende:**

a. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
b. GROENE LED knippert twee keer.
c. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
d. LED's worden weer constant BLAUW

- **Als de encryptiemodus is geconfigureerd als AES-CBC, gebeurt het volgende:**

a. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
b. GROENE LED knippert drie keer.
c. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
d. LED's worden weer constant BLAUW

Opmerking: Druk om de Admin Modus (constant BLAUWE LED) onmiddellijk te verlaten, de **SHIFT** (⬆) toets in en houd deze gedurende een seconde ingedrukt, - constant BLAUWE LED wordt nu een constant RODE LED

42. Schijftype configureren

De diskAshur³ kan worden geconfigureerd als ofwel 'Verwijderbare Schijf' of als 'Lokale Schijf (standaard)'. Alle kritische parameters worden gewist wanneer er wordt overgegaan naar een ander schijftype. Alle pincodes, de encryptiesleutel en data worden verwijderd en de schijf zal in de resetstand gaan.

WAARSHUWING: Wijziging van schijftype in een 'Verwijderbare Schijf' of 'Lokale Schijf (standaard)' zal de enryptiesleutel verwijderen en de diskAshur³ doen resetten en alle data ontoegankelijk maken en voor altijd verloren doen gaan!

Voer de volgende stappen uit om het diskAshur³ schijftype in te stellen als een Verwijderbare Schijf (**00**) of Lokale Schijf (**01**). Deze functionaliteit is standaard ingesteld als Lokale Schijf (**01**). Houd er rekening mee dat alle kritische parameters worden gewist wanneer er naar een ander schijftype wordt overgegaan. De schijf zal dan resetten.

Ga eerst naar de **Admin Modus** zoals beschreven in hoofdstuk 5 om de diskAshur³ encryptiemodus in te stellen. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED)

1. Druk in Admin Modus de **Ontgrendel (🔓) + 8** toetsen in en houd deze ingedrukt.		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's
2. Voer **00** in om als **Verwijderbare Schijf** in te stellen Voer **01** om als **Lokale Disk (standaard)** in te stellen		GROENE en BLAUWE LED's zullen blijven knipperen
3. . Druk de **SHIFT** (⬆) toets een keer in		GROENE en BLAUWE LED's veranderen in een constant GROENE LED en dan in een constant RODE LED (Reset stand) om een te geven dat het schijftype succesvol is gewijzigd.

Belangrijk: Na wijziging van het schijftype, zal de diskAshur³ volledig resetten en dient er een nieuwe Admin pincode te worden ingesteld. Raadpleeg Hoofdstuk 27 op pagina 226 voor 'Admin PIN instellen na een Brute Force aanval of Reset'.

43. How to check the Disk type setting

Ga eerst naar de **Admin Modus** zoals beschreven in hoofdstuk 5 om de diskAshur³ schijftype instelling te controleren. Ga verder met de volgende stappen zodra de schijf in **Admin Modus** staat (constant BLAUWE LED).

1. Druk in Admin modus de **'SHIFT** (⬆) + **8'** toetsen in en houd deze ingedrukt		Constant BLAUWE LED verandert in knipperend GROENE en BLAUWE LED's

2. Druk de **Ontgrendel (🔓)** toets in en het volgende gebeurt;

- **Als het schijftype als 'Verwijderbaar' is geconfigureerd, gebeurt het volgende:**

a. Alle LED's ROOD, GROEN & BLAUWE) worden gedurende een seconde constant en gaan dan uit.
b. Alle LED's (ROOD, GROEN & BLAUW) worden opnieuw gedurende een seconde constant en gaan dan uit.
d. LED's worden weer constant BLAUW

- **Als het schijftype als 'Lokaal' is geconfigureerd, gebeurt het volgende:**

a. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
b. GROENE LED knippert een keer.
c. Alle LED's (ROOD, GROEN & BLAUW) worden gedurende een seconde constant.
d. LED's weer constant BLAUW

44. Initialiseren en formatteren van diskAshur³ voor Windows

Na een 'Brute Force Aanval' of een volledige reset zal de diskAshur³ alle pincodes, data en de encryptiesleutel wissen. U zult de diskAshur³ voor gebruik moeten initialiseren en formatteren.

Doe het volgende om uw diskAshur³ te resetten:

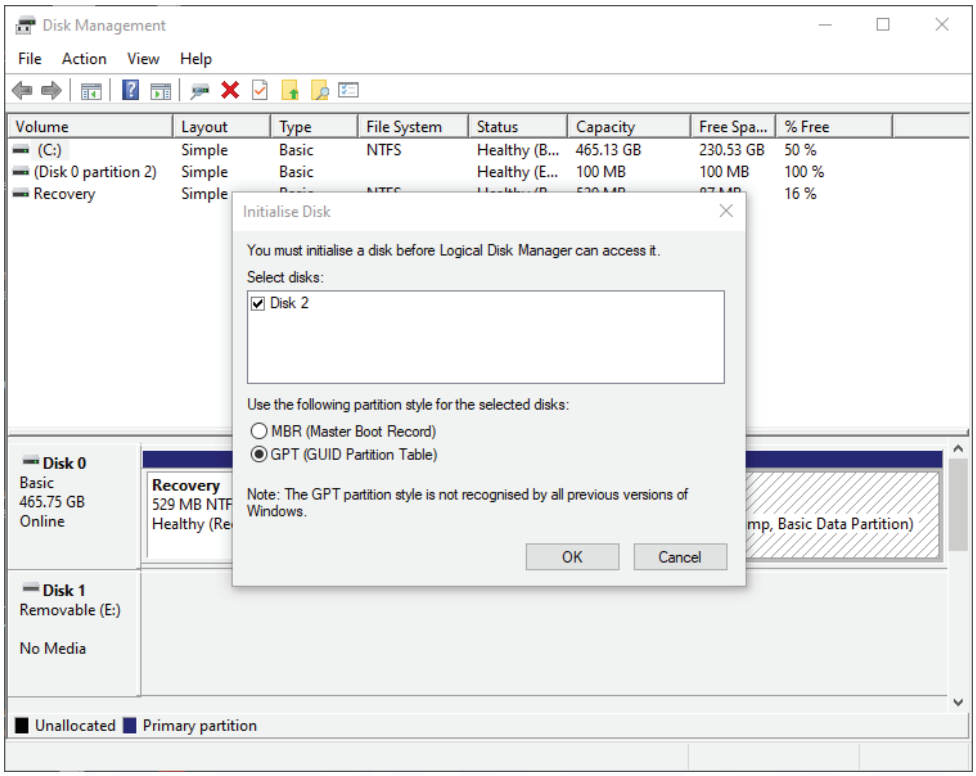
1. Stel een nieuwe Admin pincode in – zie pagina 226, hoofdstuk 27, 'Admin pincode instellen na een Brute Force aanval of reset'.

2. Druk, terwijl de diskAshur³ in stand-by stand staat (RODE LED), de **Ontgrendel (🔓)** toets een keer in en voer een **Nieuwe Admin pincode** in om te ontgrendelen (GROENE LED).

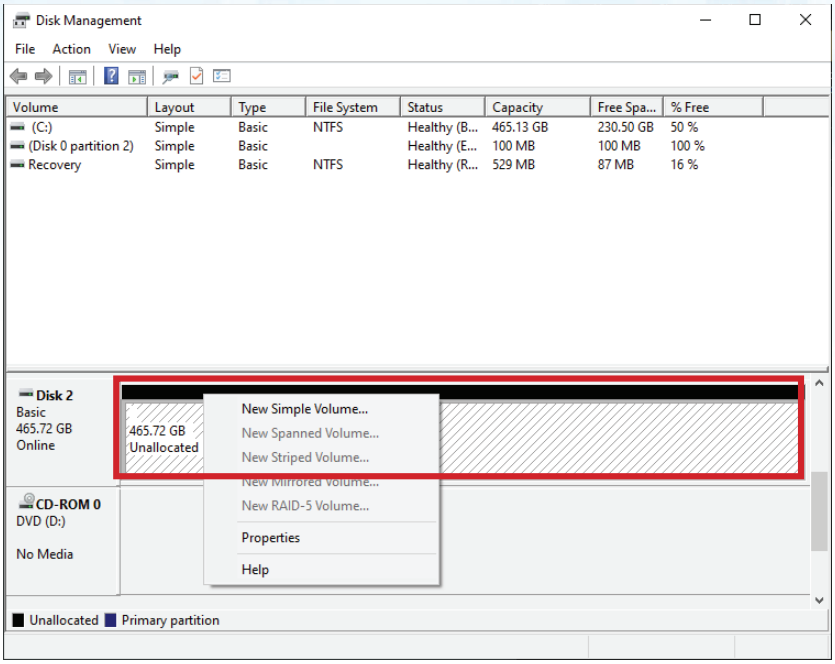
3. **Windows 7:** Klik met de rechtermuisknop op **Computer** en klik dan op **Manage (Beheer)** en selecteer **Disk Management (Schijfbeheer)**
   Windows 8: Klik met de rechtermuisknop op de linkerhoek van de desktop en selecteer **Disk Management (Schijfbeheer)**
   Windows 10: Klik met de rechtermuisknop op de startknop en kies **Disk Management (Schijfbeheer)**

4. In het Disk Management window, wordt de diskAshur³ als een onbekend apparaat herkend dat niet is geïnitialiseerd en niet is gealloceerd. Er verschijnt een berichtenvenster waarin u kunt kiezen uit een MBR of GPT partitiestijl. GPT slaat meerdere kopieën van deze data op over de schijf en is dientengevolge meer robuust. Op een MBR schijf, worden de partitie en opstart (boot) informatie op een enkele plaats opgeslagen.

Selecteer de partitiestijl en kik op **OK**



5. Rechtermuisklik in het blanco veld over het **Ongealloceerde** gedeelte, en selecteer dan **New Simple Volume**.



6. De Welcome to the New Simple Volume Wizard window opent. Klik op Next.

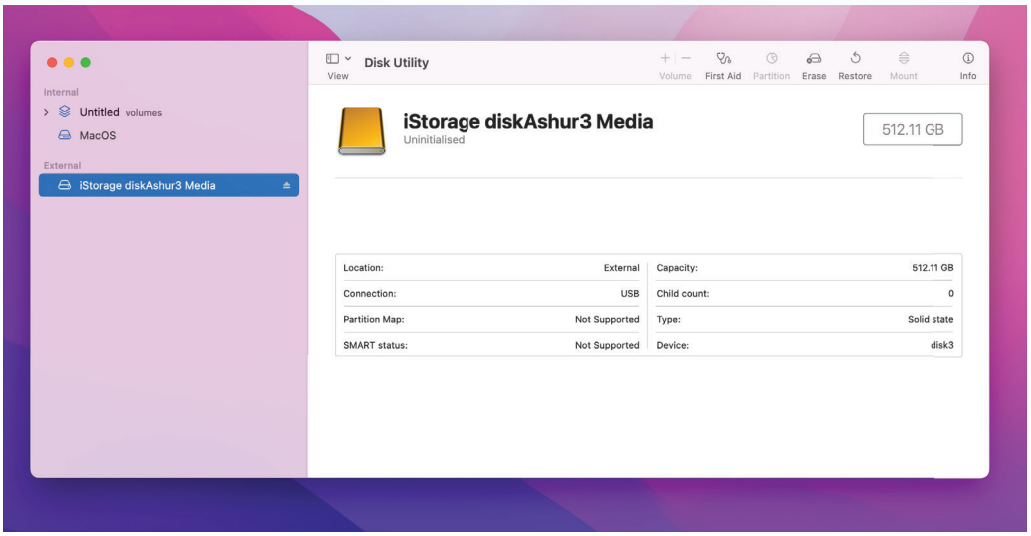
7. Als u slechts één partitie nodig hebt, accepteer de standaard partitiegrootte en klik op Next.
8. Wijs een schijfletter of pad toe en klik op Next.
9. Creëer een volume label, selecteer Perform a quick format, and then click Next.
10. Klik op Finish.
11. Wacht totdat het formatteerproces is voltooid. De diskAshur³ wordt herkend en is beschikbaar voor gebruik.

45. Initialiseren en formatteren van de diskAshur³ in Mac OS

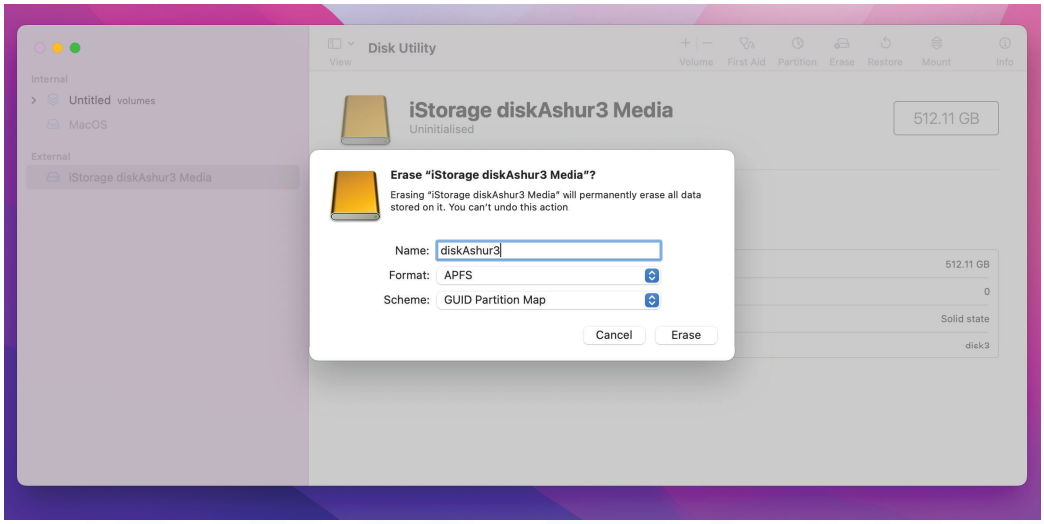
Na een 'Brute Force Aanval' of complete reset zal de diskAshur³ alle pincodes, alle data en de encryptiesleutel verwijderen. U moet de diskAshur³ initialiseren en formatteren voor gebruik.

Om de diskAshur³ te initialiseren en te formatteren:

1. Selecteer diskAshur³ uit de lijst van schijven en volumes. Elke schijf in de lijst toont de capaciteit, fabrikant, en productnaam, zoals '**iStorage diskAshur³ Media**'.

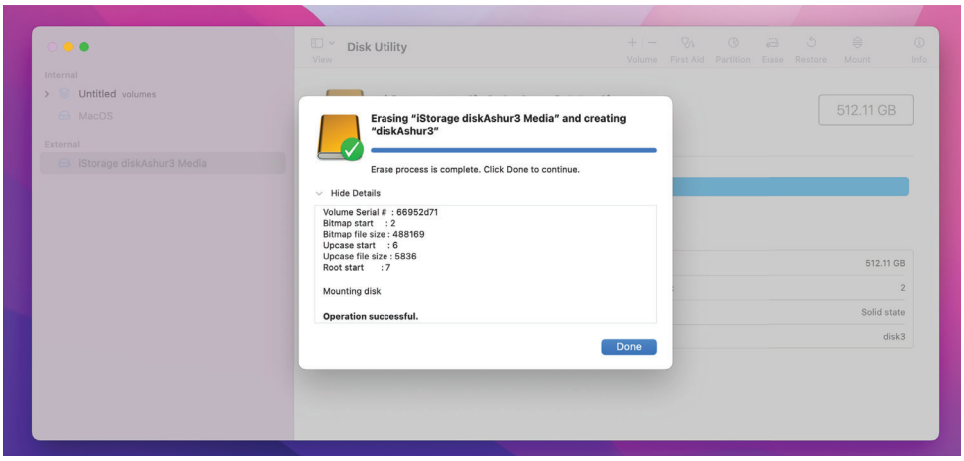


2. Klik op de '**Erase**' button onder Disk Utility.
3. Voer een naam in voor de schijf. De standaard naam is Untitled. De naam van de schijf zal uiteindelijk op de desktop verschijnen.



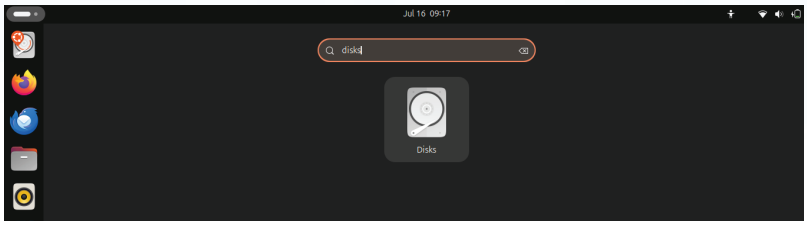
4. Selecteer een schema en volume format om te gebruiken. Het Volume Format dropdown menu somt de beschikbare schijfformaten op die door de Mac worden ondersteund. Het aanbevolen format type is Mac OS Extended (Journaled).' Gebruik exFAT voor cross platform. Het schema format dropdown menu somt de beschikbare schema's op die kunnen worden gebruikt. We raden 'GUID Partition Map' aan om te gebruiken op schijven groter dan 2TB.

5. Klik op de 'Erase' button. Disk Utility zal het volume van de desktop afhalen (unmount), het wissen vervolgens opnieuw op de desktop plaatsen (mounten).

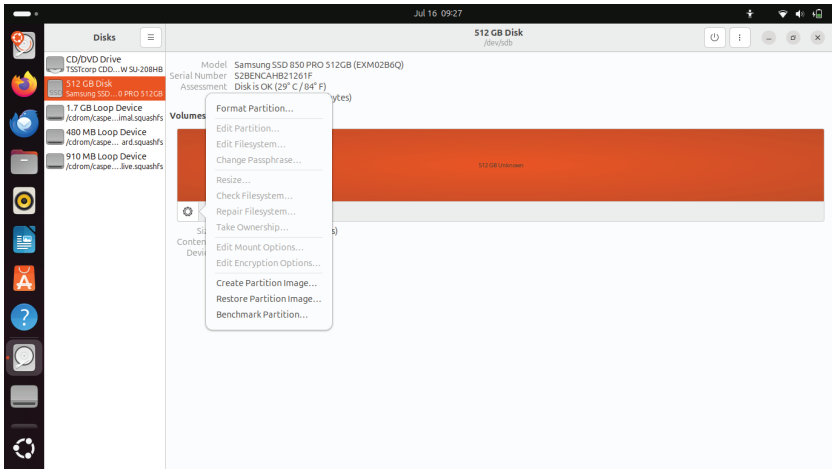


46. Initialiseren en formatteren van de diskAshur³ in Linux OS

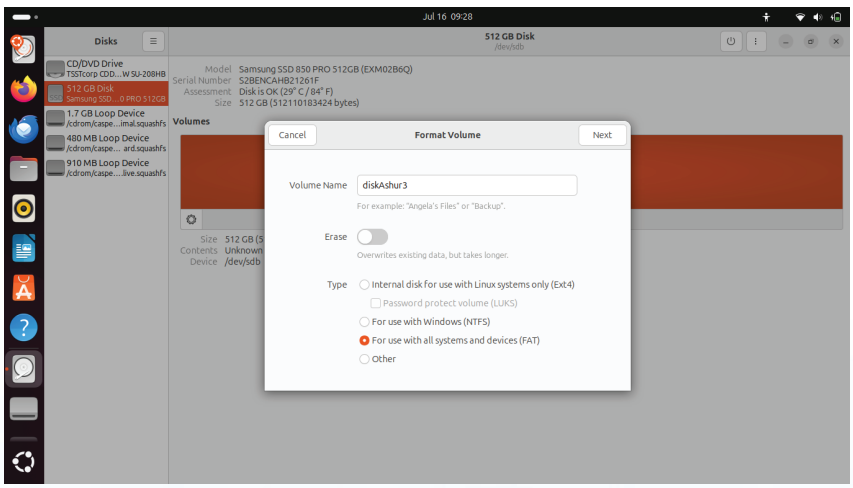
1. Open '**Show Application**' en typ '**Disks**' in het zoekveld. Klik op '**Disks**' wanneer dit wordt getoond.

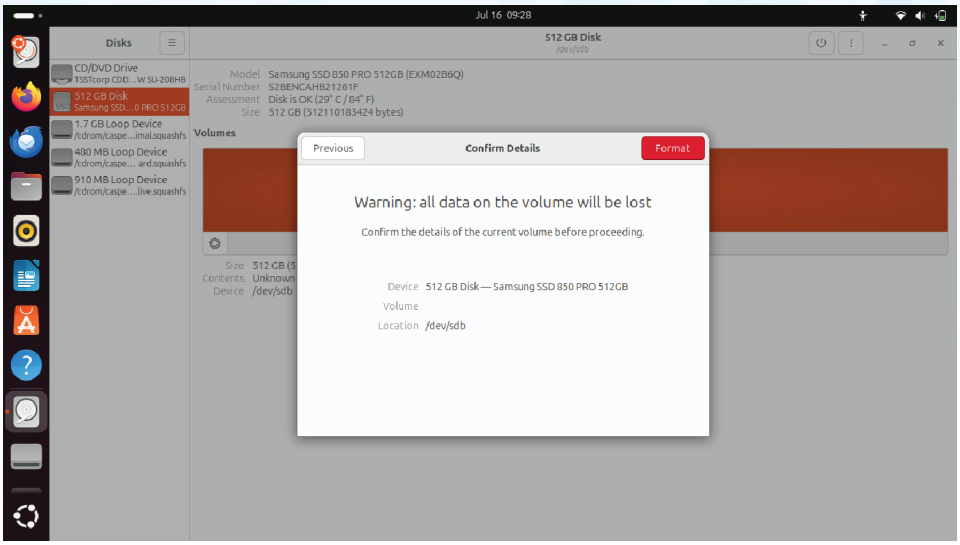


2. Klik om de schijf te selecteren (500 GB Hard Disk) onder '**Devices**'. Klik daarna op het tandwiel-icoontje onder '**Volumes**' en klik tot slot op '**Format Partitions**'.

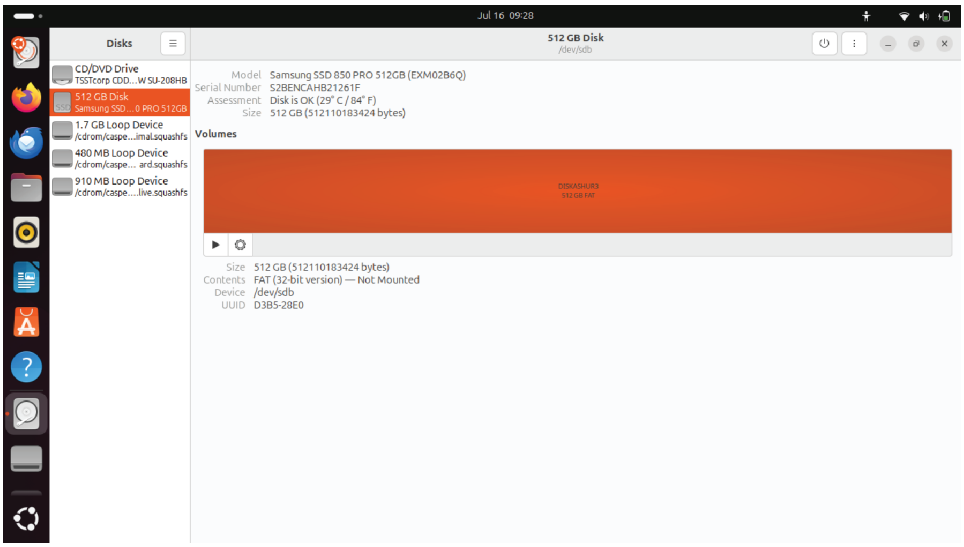


3. Selecteer '**For use with all systems and devices (FAT)**' bij de '**Type**' optie. Voer een naam in voor de schijf bijvoorbeeld: diskAshur³. Klik daarna op de '**Format**' button.

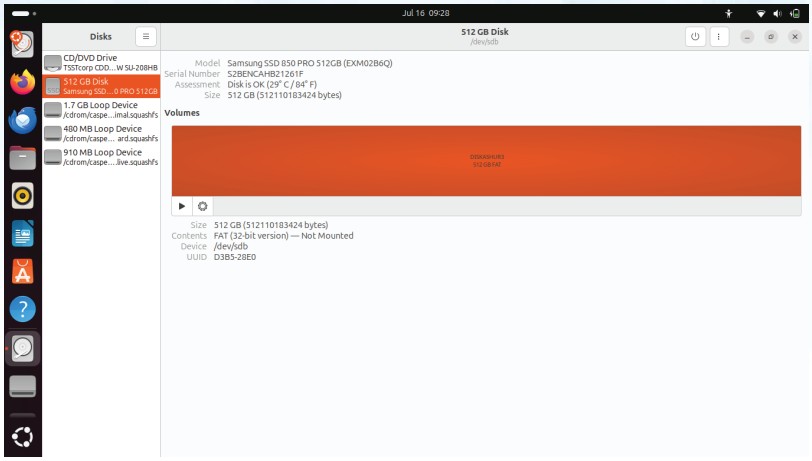




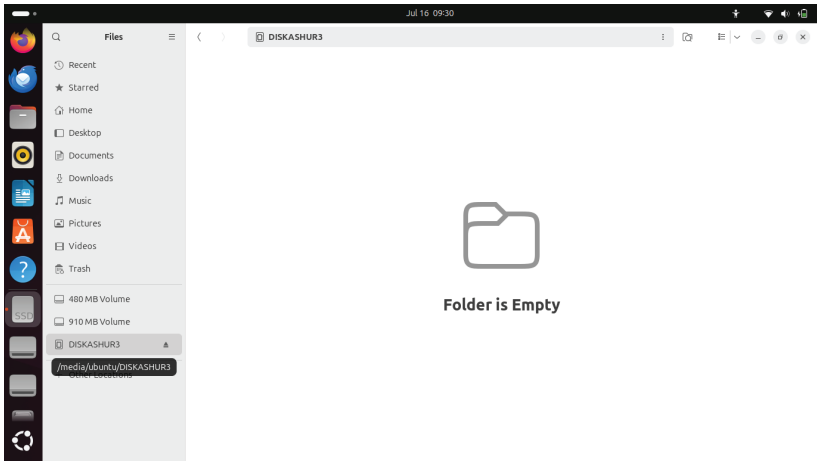
4. Nadat het formatteerproces is voltooid, klikt u op de Play button om de schijf in Ubuntu te plaatsen.



5. Nu zou de schijf in Ubuntu moeten zijn geplaatst en klaar zijn voor gebruik.



6. De schijf wordt getoond zoals te zien in onderstaande afbeelding. U kunt het diskicoontje aanklikken om uw schijf te openen.



47. In slaapstand gaan, opschorten of afmelden bij het besturingssysteem

Zorg ervoor dat u alle bestanden op uw diskAshur³ opslaat en sluit voordat u in slaapstand gaat, opschort of uitlogt van het besturingssysteem.

Het is aanbevolen dat u de diskAshur³ handmatig vergrendelt voordat u in slaapstand gaat, opschort of uitlogt uit uw systeem.

Om de drive te vergrendelen, moet u de diskAshur³ veilig uit uw hostbesturingssysteem verwijderen en vervolgens loskoppelen van de USB-poort. Als er data wordt overgeschreven naar de drive zal het loskoppelen van de diskAshur³ resulteren in onvolledige datatransfer en mogelijke corruptie van gegevens.

⚠ **Opgelet:** Om ervoor te zorgen dat uw gegevens veilig zijn, moet u uw diskAshur³ vergrendelen als u niet achter uw computer zit.

48. Firmware controleren in de beheerdersmodus

Om het firmwarerevisienummer te controleren, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) ga verder met de volgende stappen.

1. In beheerdersmodus houdt u beide "**3 + 8**"-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk eenmaal op de **Ontgrendel (🔓)**-knop en het volgende gebeurt; a. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde. b. RODE LED knippert en geeft het integrale deel van het firmwarerevisienummer aan. c. GROENE LED knippert en geeft het fractionele deel aan. d. BLAUWE LED knippert en duidt het laatste cijfer van het firmwarerevisienummer aan e. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde. f. RODE, GROENE & BLAUWE LED's schakelen naar een ononderbroken BLAUWE LED		

Als het firmwarerevisienummer bijvoorbeeld '**2.3**' is, dan zal de RODE LED tweemaal (**2**) knipperen en de GROENE LED knippert drie (**3**) keer. Zodra de reeks is beëindigd, knipperen de RODE, GROENE & BLAUWE LED's eenmaal tegelijkertijd en keren dan terug naar de beheerdersmodus, een ononderbroken GROENE LED.

49. Firmware controleren in de gebruikersmodus

Om het firmwarerevisienummer te controleren, voert u eerst de "**gebruikersmodus**" in zoals beschreven in hoofdstuk 13. Zodra de drive in **beheerdersmodus** ononderbroken (GROENE LED) is, ga door met de volgende stappen.

1. In gebruikersmodus houdt u beide "**3 + 8**"-knoppen ingedrukt totdat de GROENE en BLAUWE LED's tegelijkertijd knipperen		Ononderbroken GROENE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's

2. Druk eenmaal op de **Ontgrendel (🔓)**-knop en het volgende gebeurt;

a. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde.
b. RODE LED knippert en geeft het integrale deel van het firmwarerevisienummer aan.
c. GROENE LED knippert en geeft het fractionele deel aan.
d. BLAUWE LED knippert en duidt het laatste cijfer van het firmwarerevisienummer aan
e. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde.
f. RODE, GROENE & BLAUWE LED's schakelen naar een ononderbroken BLAUWE LED

Als het firmwarerevisienummer bijvoorbeeld '**2.3**' is, dan zal de RODE LED tweemaal (**2**) knipperen en de GROENE LED knippert drie (**3**) keer. Zodra de reeks is beëindigd, knipperen de RODE, GROENE & BLAUWE LED's eenmaal tegelijkertijd en keren dan terug naar de beheerdersmodus, een ononderbroken GROENE LED.

50. Technische ondersteuning

iStorage biedt u de onderstaande nuttige hulpmiddelen:

Website:
https://www.istorage-uk.com

Technische ondersteuning e-mail:
support@istorage-uk.com

Telefonische ondersteuning:
+44 (0) 20 8991-6260.

iStorage Technical Support specialisten zijn beschikbaar tussen 9.00 en 17.30 uur GMT - maandag tot en met vrijdag.

51. Garantie en RMA-informatie

DISCLAIMER EN GARANTIE VAN ISTORAGE PRODUCT

iStorage garandeert dat haar producten bij levering en gedurende een periode van 36 maanden vanaf levering vrij zijn van materiële gebreken. Deze garantie is echter niet van toepassing in de hieronder beschreven omstandigheden. iStorage garandeert dat de producten voldoen aan de normen die worden vermeld in het relevante gegevensblad op onze website op het moment dat u uw bestelling plaatst.

Deze garanties zijn niet van toepassing op defecten in de producten die het gevolg zijn van:

- normale slijtage;
- opzettelijke schade, abnormale opslag- of werkomstandigheden, ongeval, nalatigheid door u of door een derde partij;
- als u of een derde partij er niet in slaagt de producten te bedienen of te gebruiken in overeenstemming met de gebruikersinstructies;
- elke wijziging of reparatie door u of door een derde partij, maar die geen erkende reparateur is; of
- een door u verstrekte specificatie.

Onder deze garanties zullen we, naar eigen goeddunken, alle producten die materiële gebreken vertonen, repareren, vervangen of terugbetalen, op voorwaarde dat bij levering:

- u de producten inspecteert om na te gaan of ze materiële gebreken vertonen; en
- u het versleutelingsmechanisme test in de producten.

Wij zijn niet aansprakelijk voor materiële defecten of defecten in het versleutelingsmechanisme van de producten die bij inspectie bij levering kunnen worden vastgesteld, tenzij u dergelijke defecten aan ons meldt binnen 30 dagen na aflevering. Wij zijn niet aansprakelijk voor materiële defecten of defecten in het versleutelingsmechanisme van de producten die bij inspectie bij levering niet kunnen worden vastgesteld, tenzij u dergelijke defecten aan ons meldt binnen 7 dagen vanaf het moment dat u deze ontdekt of u op de hoogte zou moeten zijn van dergelijke defecten. Wij zijn onder deze garantie niet aansprakelijk als u of iemand anders de producten verder gebruikt na het ontdekken van een defect. Na de melding van een defect, dient u het defecte product naar ons terug te sturen. Als u een bedrijf bent, bent u verantwoordelijk voor de transportkosten die u maakt bij het verzenden van producten of onderdelen van de producten naar ons onder de garantie, en wij zijn verantwoordelijk voor alle transportkosten wanneer we u het herstelde product of een vervangingsproduct sturen. Als u een consument bent, raadpleeg dan onze algemene voorwaarden.

Geretourneerde producten moeten in de originele verpakking en in schone staat zijn. Op een andere manier geretourneerde producten worden, naar goeddunken van het bedrijf, geweigerd of er wordt een extra vergoeding voor in rekening gebracht om de extra kosten te dekken. Producten die voor reparatie onder garantie worden geretourneerd, moeten vergezeld gaan van een kopie van de originele factuur of moeten het originele factuurnummer en datum van aankoop vermelden.

Als u een consument bent, is deze garantie een aanvulling op uw wettelijke rechten met betrekking tot producten die defect zijn of niet zoals beschreven. Advies over uw wettelijke rechten is verkrijgbaar bij uw plaatselijke adviesbureau (Citizens 'Advice Bureau of Trading Standards Office).

De garanties die in deze clausule worden uiteengezet, zijn alleen van toepassing op de oorspronkelijke koper van een product van iStorage of een door iStorage geautoriseerde wederverkoper of distributeur. Deze garanties zijn niet overdraagbaar.

MET UITZONDERING VAN DE BEPERKTE GARANTIE DIE HIERIN WORDT VERSTREKT, EN VOOR ZOVER TOEGESTAAN DOOR DE WET, WIJST ISTORAGE ALLE GARANTIES, EXPLICIET OF IMPLICIET, INCLUSIEF ALLE GARANTIES VAN VERKOOPBAARHEID; GESCHIKTHEID VOOR EEN BEPAALD DOEL, NIET-INBREUK. ISTORAGE BIEDT GEEN GARANTIE DAT HET PRODUCT FOUTLOOS WERKT. VOOR ZOVER ENIGE IMPLICIETE GARANTIE NIET EVENWEL KAN BESTAAN BIJ WETGEVING, ZIJN DERGELIJKE GARANTIES BEPERKT TOT DE DUUR VAN DEZE GARANTIE. REPARATIE OF VERVANGING VAN DIT PRODUCT, ZOALS HIERIN AANGEBODEN, IS UW ENIGE RECHTSMIDDEL.

ISTORAGE IS IN GEEN GEVA{2}[3}L AANSPRAKELIJK VOOR ENIG VERLIES OF VERWACHTE WINST, OF ENIGE INCIDENTELE, PUNITIEVE, SPECIALE, VERTROUWELIJKE SCHADE OF OORZAKELIJKE SCHADES, MET INBEGRIP VAN, MAAR NIET BEPERKT TOT, GEDERFDE INKOMSTEN, GEDERFDE WINST, VERLIES VAN GEBRUIK VAN SOFTWARE, GEGEVENSVERLIES, ANDER VERLIES OF HERSTEL VAN GEGEVENS, SCHADE AAN EIGENDOM EN CLAIMS VAN DERDEN DIE VOORTVLOEIEN UIT EEN VERWACHTING VAN HERSTEL, MET INBEGRIP VAN GARANTIE, CONTRACT, WETTELIJK OF ONRECHTMATIG, ONGEACHT OF DIT WERD GEADVISEERD BIJ DE MOGELIJKHEID VAN DERGELIJKE SCHADE. ONGEACHT DE DUUR VAN BEPERKTE GARANTIE OF GARANTIE DIE DOOR DE WET IS GEIMPLICEERD, OF IN HET GEVAL DAT DE BEPERKTE GARANTIE NIET VOLDOET AAN ZIJN ESSENTIËLE DOEL, ZAL DE VOLLEDIGE AANSPRAKELIJKHEID VAN ISTORAGE IN GEEN GEVAL DE AANKOOPPRIJS VAN DIT PRODUCT OVERSCHRIJDEN. | 4823-2548-5683.3{2]

iStorage®

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, Engeland
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | website: www.istorage-uk.com

iStorage®

Manual del usuario

DISKASHUR® 3 & DISKASHUR® PRO3

Este manual de usuario es aplicable tanto a la diskAshur³ como a la diskAshur PRO³, por lo que, de ahora en adelante, nos referiremos a la unidad como diskAshur³

Asegúrese de recordar su PIN (contraseña); sin él, no hay forma de acceder a los datos guardados en la unidad.

Si tiene dificultades para utilizar su diskAshur³, póngase en contacto con nuestro equipo de soporte en el correo electrónico support@istorage-uk.com o por teléfono al +44 (0) 20 8991 6260.

RoHS Compliant

REACH COMPLIANCE

Cumple con la Ley de Acuerdos Comerciales (TAA)

CITRIX® vmware®

Índice

Introducción 251
Contenido de la caja 251
Distribución de diskAshur³ 251
1. Indicadores LED y sus acciones 252
2. Estados LED 252
3. Primer uso 253
4. Desbloqueo de la diskAshur³ con el PIN de administración 254
5. Cómo acceder al modo de administración 254
6. Cómo cambiar el PIN de administración 255
7. Cómo configurar una política de PIN de usuario 256
8. Cómo eliminar la política de PIN de usuario 257
9. Cómo comprobar la política de PIN de usuario 257
10. Cómo añadir un nuevo PIN de usuario en el modo de administración 258
11. Cómo cambiar el PIN de usuario en el modo de administración 259
12. Cómo eliminar el PIN de usuario en el modo de administración 259
13. Cómo desbloquear la diskAshur³ con el PIN de usuario 260
14. Cómo cambiar el PIN de usuario en el modo de usuario 260
15. Cómo encender el teclado LED retroiluminado 261
16. Cómo apagar el teclado LED retroiluminado 261
17. Cómo crear un PIN de recuperación de usuario de un solo uso 262
18. Cómo eliminar el PIN de recuperación de usuario de un solo uso 262
19. Cómo activar el modo de recuperación y crear un nuevo PIN de usuario 263
20. Configurar solo lectura para el usuario en el modo de administración 263
21. Habilitar la lectura/escritura para el usuario en el modo de administración 264
22. Establecer solo lectura global en el modo de administración 264
23. Habilitar la lectura/escritura global en el modo de administración 265
24. Cómo configurar un PIN con autodestrucción 265
25. Cómo eliminar el PIN con autodestrucción 266
26. Cómo desbloquear con el PIN con autodestrucción 266
27. Cómo configurar un PIN de administración después de un ataque por fuerza bruta o restablecimiento 267
28. Cómo configurar el autobloqueo sin supervisión 267
29. Desactivar el autobloqueo sin supervisión 268
30. Cómo comprobar el autobloqueo sin supervisión 269
31. Configurar solo lectura en el modo de usuario 269
32. Habilitar lectura/escritura en el modo de usuario 270
33. Mecanismo de defensa ante ataque por fuerza bruta 270
34. Cómo configurar la limitación de fuerza bruta del PIN de usuario 271
35. Cómo comprobar la limitación de fuerza bruta del PIN de usuario 272
36. Cómo realizar un restablecimiento completo 273
37. Cómo configurar diskAshur³ como un dispositivo de inicio 273
38. Cómo deshabilitar la función de inicio de diskAshur³ 274
39. Cómo comprobar la configuración de inicio 274
40. Cómo configurar el modo de cifrado 275
41. Cómo comprobar el modo de cifrado 276
42. Cómo configurar el tipo de disco 277
43. Cómo comprobar la configuración del tipo de disco 277
44. Cómo inicializar y formatear la diskAshur³ para Windows 278
45. Cómo inicializar y formatear diskAshur³ en Mac OS 280
46. Cómo inicializar y formatear diskAshur³ en Linux OS 282
47. Cómo poner en hibernación, suspender o cerrar la sesión del sistema operativo 285
48. Cómo comprobar el firmware en el modo de administración 285
49. Cómo comprobar el firmware en el modo de usuario 286
50. Soporte técnico 287
51. Garantía e información RMA 287

Introducción

Gracias por comprar la nueva unidad iStorage diskAshur³/ diskAshur PRO³, en adelante, “diskAshur³”.

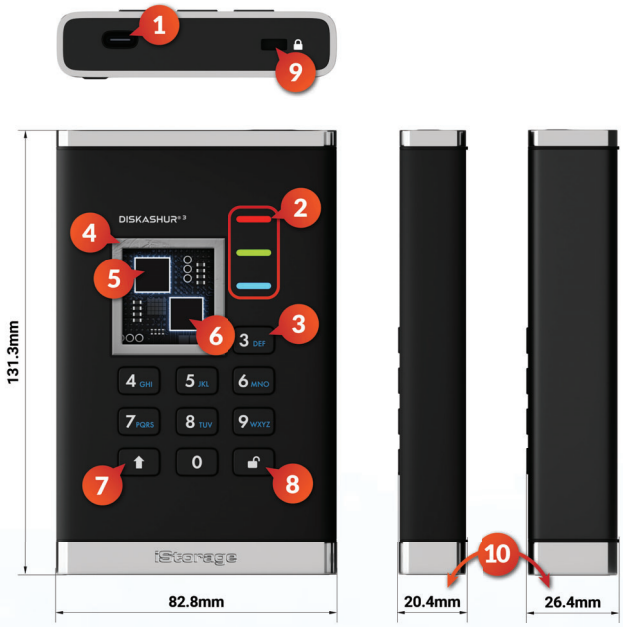
La diskAshur³ es una unidad HDD/SSD portátil fácil de usar, ultrasegura y con protección de contraseña y cifrado de hardware que cuenta con capacidades de hasta 5 TB (HDD) y hasta 16 TB (SSD), con nuevas capacidades próximamente. La diskAshur³ cifra datos en tránsito y en reposo por medio de un cifrado de hardware de disco completo de 256 bits.

La diskAshur3 incorpora un microprocesador seguro con certificación de Common Criteria EAL 5+, el cual emplea mecanismos de protección físicos incorporados diseñados para proteger el dispositivo de manipulación externa, ataques de bypass e inyección de fallos. A diferencia de otras soluciones, diskAshur³ reacciona a un ataque automatizado pasando a un estado de bloqueo que anula todos los intentos de acceso no autorizado. En pocas palabras, sin el PIN no hay forma alguna de entrar.

Contenido de la caja

- iStorage diskAshur³
- Estuche protector
- Cables C y A de entrada USB
- Licencia gratuita de 1 año de Nero BackItUp y iStorage DriveSecurity
- QSG - Quick Start Guide (guía de inicio rápido)

Distribución de diskAshur³



1. Interfaz USB 3,2 (Gen 1) de tipo C
   Se incluyen los cables USB de tipo C y A.
2. Indicadores LED
   ROJOS -modo de bloqueo o standby. Indicador VERDE FIJO - Desbloqueo. Indicador VERDE INTERMITENTE - Transferencia de datos. AZUL - Modo de administración
3. Teclado alfanumérico con revestimiento epoxi, resistente al desgaste, con iluminación de fondo (seleccionable por el usuario).
4. Diseño a prueba de manipulaciones:
   Todos los componentes críticos están revestidos con una capa de resina epoxídica extremadamente resistente.
5. Chip criptográfico integrado.
6. Microprocesador seguro certificado Common Criteria EAL 5+ integrado en el dispositivo.
7. Tecla Mayús
8. Tecla UNLOCK
9. Ranura de bloqueo de escritorio
10. La profundidad de la unidad de disco duro de 4 TB&5 TB es de 26,8 mm en lugar de 20,8 mm.

1. Indicadores LED y sus acciones

LED	Estado del LED	Descripción	LED	Estado del LED	Descripción
	ROJO fijo	Unidad bloqueada (en modo **en espera** o **restablecimiento**)		AZUL fijo	Unidad en **modo de administración**
	ROJO Parpadeo doble	Entrada incorrecta del PIN		ROJO, VERDE y AZUL parpadeando a la vez	Esperando a que el **usuario** escriba el PIN
	VERDE continuo	Unidad **desbloqueada**		VERDE y AZUL parpadeando a la vez	Esperando a que el se escriba el PIN **de administración**
	VERDE intermitente	Transferencia de datos en curso			

2. Estados LED

Para activar la unidad tras un modo en reposo

El modo en reposo se define como un estado en el que la unidad no se está utilizando y todos los indicadores LED están apagados.

Para activar la diskAshur³ desde el modo en reposo, siga los pasos que indicamos a continuación.

Conecte la unidad a un puerto USB activo en su ordenador		Se encenderá un LED ROJO fijo para indicar que la unidad está en modo en espera

Para entrar en modo en reposo

Para forzar la diskAshur³ de forma que entre en un modo en reposo, puede realizar una de las operaciones siguientes:

- Extraiga y desconecte la unidad de forma segura del ordenador; el LEDROJO se apagará (modo en reposo).

Estados de unidad encendida

Al activar la unidad desde el modo en reposo, esta entrará en uno de los estados que se indican en la tabla siguiente.

Estado de unidad encendida	Indicación LED	Tecla de cifrado	PIN de ad-minis-tración	Descripción
Estado inicial de entrega	ROJO y VERDE fijos	✓	×	Esperando configuración de un PIN de administración (primer uso)
En espera	ROJO fijo	✓	✓	Esperando entrada de PIN de administración, usuario o recuperación
Restablecimiento	ROJO fijo	×	×	Esperando configuración de un PIN de administración

3.Primer uso

La unidad iStorage diskAshur³ se suministra en el **"estado inicial de entrega" sin PIN de administración predefinido**. Para poder usar la unidad es necesario configurar un PIN de administración de entre **8 y 64** dígitos. Una vez que se haya configurado un PIN de administración de forma correcta, ya no será posible revertir la unidad al estado inicial de entrega.

Requisitos del PIN:

- Debe ser de entre 8-64 dígitos de longitud
- No puede incluir únicamente números repetidos, por ejemplo: (3-3-3-3-3-3-3-3)
- No deberá contener únicamente números consecutivos, por ejemplo: (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- Se puede usar la tecla Mayús para otras combinaciones p. ej.,(**Mayús** (⬆)**+1** es un valor distinto a solo "1").

Consejo sobre contraseñas: el usuario puede configurar una palabra, nombre o frase fácil de recordar, o cualquier otra combi nación de PIN alfanumérico presionando simplemente el botón con las letras correspondientes sobre ellas.

Algunos ejemplos de estos tipos de PIN alfanuméricos son:

- Para "**Password**" el usuario presionaría las siguientes teclas:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Para "**iStorage**" el usuario presionaría:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Usando este método, pueden configurarse PIN largos y fáciles de recordar.

Para configurar un PIN de administración y desbloquear la diskAshur³ por primera vez, solo tiene que seguir los pasos que aparecen en la tabla de abajo.

Instrucciones: primer uso	LED	Estado del LED
1. Conecte la unidad diskAshur³ a un puerto USB activo en su ordenador		Se encenderán los LED ROJO y VERDE fijos para indicar que la unidad está en estado inicial de entrega
2. Mantenga pulsadas las teclas **Unlock (🔓) +1**		Los LED cambiarán a VERDE intermitente y AZUL fijo
3. Introduzca un **nuevo PIN deadministración** (8-64 dígitos) y pulse la tecla **Unlock (🔓)** una vez		Los indicadores LED de color VERDE intermitente y AZUL fijo cambiarán a VERDE de un solo parpadeo y después de nuevo a VERDE intermitente y AZUL fijo
4. Vuelva a escribir el **nuevo PIN deadministración** y pulse la tecla **Unlock (🔓)** una vez		El indicador LED AZUL parpadeará rápidamente y cambiará a un AZUL fijo y, finalmente, a un VERDE fijo para indicar que el PIN de administración se ha configurado correctamente y que la unidad está desbloqueada y lista para su uso

Cómo bloquear la diskAshur³

Para bloquear la unidad, extráigala de forma segura del sistema operativo anfitrión y, a continuación, desenchúfela del puerto USB. Si desconecta la diskAshur³ mientras se están escribiendo datos en la unidad, se interrumpirá la transferencia de datos y es posible que estos se corrompan.

4. Desbloqueo de la diskAshur³ con el PIN de administración

Para desbloquear la diskAshur³ con el PIN de administración, siga los sencillos pasos que se indican en la tabla a continuación.

1. Conecte la diskAshur³ a un puerto USB de su ordenador		Se encenderá un LED ROJO fijo para indicar que la unidad está en modo en espera
2. Mientras la unidad está en el modo de espera (LED ROJO fijo), pulse la tecla **Unlock (🔓)** una vez		Los LED VERDE y AZUL empezarán a parpadear al mismo tiempo
3. Con los LED VERDE y AZUL parpadeando al mismo tiempo, escriba el PIN de administración y, a continuación, pulse el botón **Unlock (🔓)** una vez		El indicador LED VERDE parpadeará varias veces y cambiará a VERDE fijo para indicar que la unidad se ha desbloqueado correctamente en modo administración y está lista para su uso

5. Cómo acceder al modo administración

Para acceder al modo administración, siga estos pasos.

1. Conecte la unidad diskAshur³ a un puerto USB activo en su ordenador		Se encenderá un LED ROJO fijo para indicar que la unidad está en modo en espera
2. En el estado de espera (LED ROJO fijo), mantenga pulsados el botón **Unlock (🔓) +1**		Los LED VERDE y AZUL empezarán a parpadear al mismo tiempo
3. Introduzca su PIN de administración y pulse la tecla **Unlock (🔓)** una vez		Se encenderá un LED AZUL fijo para indicar que la unidad está en modo administración

Para salir del modo administración

Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

6. Cambiar el PIN de administrador

Requisitos del PIN:

- Debe ser de entre 8-64 dígitos de longitud
- No puede incluir únicamente números repetidos, por ejemplo: (3-3-3-3-3-3-3-3)
- No deberá contener únicamente números consecutivos, por ejemplo: (1-2-3-4-5-6-7-8), (7-8-9-0-1-2-3-4), (8-7-6-5-4-3-2-1)
- Se puede usar la tecla Mayús para otras combinaciones p. ej.,(**Mayús** (⬆)**+1** es un valor distinto a solo "1").

Consejo sobre la contraseña: Simplemente presionando el botón con las letras correspondientes, puede configurar una palabra de la que pueda acordarse, un nombre, una frase o cualquier otra combinación de PIN alfanumérico.

Ejemplos de estos tipos de PIN alfanuméricos son:

- Para "**Contraseña**" presione los siguientes botones:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Para "**iStorage**" presione los siguientes botones:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Usando este método, largo y fácil de recordar, se pueden configurar los PIN.

Para cambiar el PIN de administrador, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad está en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Unlock (🔓) + 2**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca el **PIN de administrador NUEVO** y luego presione el botón **Unlock (🔓)** una vez		Los LED VERDE parpadeante y AZUL fijo cambiarán a un solo parpadeo LED VERDE y luego nuevamente a LED VERDE parpadeante y AZUL fijo
3. Introduzca de nuevo el **PIN de administrador NUEVO** y luego presione el botón **Unlock (🔓)** una vez		Los LED VERDE parpadeante y AZUL fijo cambian a un LED AZUL que parpada rápidamente y finalmente a un LED AZUL fijo que indica que el PIN de administrador se ha cambiado correctamente

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

7. Establecer una política de PIN de usuario

El administrador puede establecer una política de limitación para el PIN de usuario. Esta política incluye establecer la longitud mínima del PIN (de 8 a 64 dígitos), así como requerir o no la introducción de uno o más '**caracteres especiales**'. El "carácter especial" funciona al presionar a la vez los dos botones '**Mayús** (⬆) **+ dígito'**.

Para establecer una política de PIN de usuario (restricciones), deberá introducir 3 dígitos, por ejemplo '**091**', los dos primeros dígitos (**09**) indican la longitud mínima del PIN (en este caso, **9**) y el último dígito (**1**) indica que se deben utilizar uno o más 'caracteres especiales'; en otras palabras '**Mayús** (⬆) + **dígito'**. De la misma manera, se puede establecer una política de PIN de usuario sin la necesidad de un 'carácter especial'; por ejemplo en '**120**', los dos primeros dígitos (**12**) indican la longitud mínima del PIN (en este caso, **12**) y el último dígito (**0**) significa que no se requieren caracteres especiales.

Una vez que el administrador ha establecido la política de PIN de usuario, por ejemplo, '**091**', se deberá configurar un PIN de usuario nuevo; véase la sección 10: 'Agregar un PIN de usuario nuevo en modo administrador'. Si el administrador configura el PIN de usuario como '**247688314**' usando un '**carácter especial**' (**Mayús** (⬆) **+ dígito** presionados juntos), esto se puede colocar en cualquier lugar a lo largo de su PIN de 8.64 dígitos durante el proceso de creación del PIN como se muestra en los ejemplos siguientes.

A. '**Mayús** (⬆) **+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',

B. '2', '4', '**Mayús** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4',

C. '2', '4', '7', '6', '8', '8', '3', '1', '**Mayús** (⬆) **+ 4**',

Nota:

- Si se ha utilizado un 'carácter especial' durante la configuración del PIN de usuario, como el ejemplo '**B**' anterior, la unidad solo se puede desbloquear introduciendo el PIN con el 'carácter especial' introducido exactamente en el orden configurado, como por ejemplo '**B**' arriba - ('2', '4', '**Mayús** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- Se puede utilizar más de un 'carácter especial' y colocarlo junto con su PIN de 8 a 64 dígitos.
- Los usuarios pueden cambiar su PIN, pero están obligados a cumplir con la 'política de PIN de usuario' (restricciones) establecida, si corresponde.
- Al establecer una nueva política de PIN de usuario, eliminará automáticamente el PIN de usuario en caso de haber uno.
- Esta política no se aplica al 'PIN de autodestrucción'. La configuración de complejidad para el PIN de autodestrucción y el PIN de administrador es siempre de 8 a 64 dígitos, sin necesidad de ningún carácter especial.

Para establecer una **política de PIN de usuario**, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Unlock (🔓) + 7**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Introduzca sus 3 **dígitos**, recuerde que los dos primeros dígitos indican la longitud mínima del PIN y el último dígito (0 o 1) independientemente de que se haya utilizado o no un carácter especial.		Los LED VERDE y AZUL parpadeantes seguirán parpadeando
3. Presione el botón **Mayús** (⬆) una vez		Los LED VERDE y AZUL parpadeantes cambiarán a un LED VERDE fijo y finalmente a un LED AZUL fijo que indica que la política de PIN de usuario se ha establecido correctamente.

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

8. Cómo eliminar la política del PIN de usuario

Para eliminar la **política del PIN de usuario**, en primer lugar, acceda al **modo de administración** según se indica en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Unlock (🔓)** y **7**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Introduzca **"080"** y pulse una vez la tecla **Mayús** (⬆)		Los LED VERDE y AZUL intermitentes cambiarán a un LED VERDE fijo y, finalmente, a un AZUL fijo para indicar que la política del PIN de usuario se ha eliminado correctamente

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayus** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

9. Cómo verificar la política de PIN de usuario

El administrador puede verificar la política de PIN de usuario e identificar la restricción de longitud mínima del PIN y si se ha establecido o no el uso de un carácter especial al anotar la secuencia de LED como se describe a continuación.

Para verificar la política de PIN de usuario, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Mayús** (⬆) **+ 7** buttons		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)** y sucederá lo siguiente; a. Todos los LED (ROJO , VERDE y AZUL) permanecen fijos durante 1 segundo. b. Un parpadeo del LED ROJO equivale a diez (10) unidades de un PIN. c. Cada parpadeo del LED VERDE equivale a una (1) sola unidad de un PIN d. Un parpadeo AZUL indica que se ha usado un 'carácter especial'. e. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo. f. Los LED vuelven a AZUL fijo		

La siguiente tabla describe el comportamiento de los LED mientras verifica la política de PIN de usuario, por ejemplo, si ha establecido un PIN de usuario de 12 dígitos usando un carácter especial (**121**), el LED ROJO parpadeará una (**1**) vez y el LED VERDE parpadeará dos (**2**) veces, a lo que seguirá un (**1**) único parpadeo de LED AZUL que indica que se debe usar un **carácter especial**.

Descripción del PIN	**Configuración de 3 dígitos**	**ROJO**	**VERDE**	**AZUL**
PIN de 12 dígitos usando un carácter especial	121	1 parpadeo	2 parpadeos	1 parpadeo
PIN de 12 dígitos SIN usar carácter especial	120	1 parpadeo	2 parpadeos	0
PIN de 9 dígitos usando un carácter especial	091	0	9 parpadeos	1 parpadeo
PIN de 9 dígitos SIN usar caracteres especiales	090	0	9 parpadeos	0

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

10. Agregar un PIN de usuario nuevo en modo administrador

Importante: La creación de un nuevo PIN de usuario debe cumplir con la política correspondiente (si se ha configurado una tal y como se describe en la sección 7), la cual impone una longitud mínima para el PIN y si se utilizará o no un carácter especial. Para conocer las restricciones del PIN de usuario, el administrador puede consultar la sección 9.

Requisitos del PIN:

- Debe tener entre 8 y 64 dígitos de longitud
- No debe contener solo números repetitivos, p. ej. (3-3-3-3-3-3-3)
- No debe contener solo números consecutivos, p. ej. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5- 4-3-2-1)
- El botón **Mayús** (⬆) se puede usar para combinaciones de PIN adicionales, por ejemplo, **Mayús** (⬆) **+ 1** es un valor diferente que solo 1. Consulte la sección 7: "Establecer una política de PIN de usuario".

Para agregar un PIN de usuario nuevo, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad está en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Unlock (🔓) + 3**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca el **PIN de usuario nuevo** y presione el botón **Unlock (🔓)** button		Los LED VERDE parpadeante y AZUL fijo cambiarán a un solo parpadeo LED VERDE y luego nuevamente a LED VERDE parpadeante y AZUL fijo
3. Vuelva a introducir el PIN de usuario nuevo y presione nuevamente el botón **Unlock (🔓)**		Los LED VERDE parpadeante y AZUL fijo cambian a un LED VERDE que parpadea rápidamente y finalmente a un LED AZUL fijo que indica que se ha configurado correctamente un PIN de usuario nuevo

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

11. Cambiar el PIN de usuario en modo administrador

Importante: El cambio del PIN de usuario debe cumplir con la 'política de PIN de usuario' si se ha configurado una como se describe en la sección 7, que impone una longitud mínima de PIN y si se ha usado un 'carácter especial'. El administrador puede consultar la sección 9 para verificar las restricciones del PIN de usuario.

Para cambiar un **PIN de usuario** existente, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Unlock (🔓) + 3**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca el **PIN de usuario nuevo** y presione el botón **Unlock (🔓)** una vez		Los LED VERDE parpadeante y AZUL fijo cambiarán a un solo parpadeo LED VERDE y luego nuevamente a LED VERDE parpadeante y AZUL fijo
3. Vuelva a introducir el **PIN de usuario nuevo** y presione nuevamente el botón **Unlock (🔓)** una vez		Los LED VERDE parpadeante y AZUL fijo cambian a un LED VERDE que parpadea rápidamente y finalmente a un LED AZUL fijo que indica que el PIN de usuario se ha cambiado correctamente

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

12. Eliminar el PIN de usuario en modo administrador

Para eliminar un **PIN de usuario** existente, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Mayús** (⬆) **+ 3**		El LED AZUL fijo cambiará a un LED ROJO parpadeante
2. Nuevamente mantenga presionados los botones **Mayús** (⬆) **+ 3**		El LED ROJO parpadeante cambiará a un LED ROJO fijo y luego a un LED AZUL fijo que indica que el PIN de usuario se ha eliminado correctamente

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

13. Cómo desbloquear la diskAshur³ con un PIN de usuario

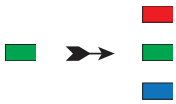
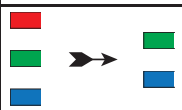
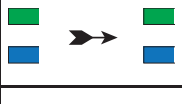
Para desbloquear la diskAshur³ con el **PIN de usuario,** lleve a cabo los pasos siguientes.

1. En estado en espera (LED ROJO fijo), mantenga pulsadas las teclas **Mayús** (⬆) **+ Unlock (🔓)**		El LED ROJO cambiará a todos los LED, es decir, ROJO, VERDE y AZUL parpadeando al mismo tiempo
2. Introduzca el PIN de usuario y pulse una vez la tecla **Unlock (🔓)**		Los LED ROJO, VERDE y AZUL intermitentes cambiarán a un VERDE intermitente y, a continuación, a un VERDE fijo para indicar que la unidad se ha desbloqueado con éxito en el modo de usuario

14. Modificación del PIN de usuario en el modo de usuario

Importante: La modificación del PIN de usuario en el modo de usuario (LED VERDE) debe cumplir con la política correspondiente en caso de que se haya configurado una según se detalla en la sección 7, la cual impone una longitud mínima para el PIN y si se utilizará o no un carácter especial.

Para cambiar el **PIN de usuario**, en primer lugar, desbloquee la diskAshur³ con el PIN de usuario según se describe en la sección 13. Una vez que la unidad esté en **modo de usuario** (VERDE fijo) continúe con los pasos siguientes.

1. En el modo de usuario (LED VERDE), mantenga pulsadas las teclas **Unlock (🔓) + 4**		El LED VERDE fijo cambiará a todos los LED, es decir, ROJO, VERDE y AZUL parpadeando al mismo tiempo
2. Escriba el PIN de usuario existente y pulse una vez la tecla **Unlock (🔓)**		Los LED cambiarán a VERDE intermitente y, a continuación, de nuevo a VERDEintermitente y AZUL fijo
3. Escriba el nuevo PIN de usuario y pulse la tecla **Unlock (🔓)** una vez		Los indicadores LED VERDE intermitente y AZUL fijo cambiarán a VERDE intermitente y, de nuevo, a VERDE intermitente y AZUL fijo
4. Vuelva a escribir el nuevo PIN de usuario y pulse la tecla **Unlock (🔓)** una vez		Los indicadores LED VERDEintermitente y AZUL fijo cambiarán a un VERDE intermitente rápido y, después, a un VERDE fijo para indicar que el PIN de usuario se ha cambiado correctamente

15. Cómo encender el teclado LED retroiluminado

Para ayudar al usuario en condiciones de baja visibilidad, la diskAshur³ viene equipada con un teclado LED retroiluminado.Para encender el teclado, en primer lugar, acceda al **modo de administración** tal y como se detalla en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **2 y 6**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse la tecla **Unlock (🔓)**		Los LED VERDE y AZUL intermitentes cambiarán a un VERDE fijo y, a continuación, a un AZUL fijo para indicar que el teclado retroiluminado se ha activado y se encenderá la próxima vez que la unidad se conecte a un puerto USB activo.

Nota: Tras configurar la diskAshur³ para encender el teclado LED retroiluminado, es preciso desconectar primero la unidad del puerto USB activo y, a continuación, volver a conectarla para que se active.Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

16. Cómo apagar el teclado LED retroiluminado

Para apagar el teclado LED retroiluminado, en primer lugar, acceda al **modo de administración** tal y como se detalla en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **2 y 3**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse la tecla **Unlock (🔓)**		Los LED VERDE y AZUL intermitentes cambiarán a un VERDE fijo y, a continuación, a un AZUL fijo para indicar que el teclado retroiluminado se ha desactivado y se apagará la próxima vez que la unidad se conecte a un puerto USB activo.

Nota: Tras configurar la diskAshur³ para que apague el teclado LED retroiluminado, es preciso desconectar primero la unidad del puerto USB activo y, a continuación, volver a conectarla para que se active.Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

17. Cómo crear un PIN de recuperación de usuario de un solo uso

El PIN de recuperación del usuario es extremadamente útil en los casos en los que el usuario ha olvidado el PIN para desbloquear la diskAshur³.
Para activar el modo de recuperación, en primer lugar, el usuario debe escribir el PIN de recuperación de un solo uso, en caso de que se haya configurado uno. El proceso de recuperación del PIN de usuario no afecta a los datos, la clave de cifrado y el PIN de administración; no obstante, el usuario tendrá que configurar un nuevo PIN de usuario de entre 8 y 64 dígitos.

Para configurar un PIN de recuperación de usuario de un solo uso de entre 8 y 64 dígitos, en primer lugar, acceda al **modo de administración** tal y como se describe en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Unlock (🔓) + 4**		El indicador LED AZUL fijo cambiará a un VERDE intermitente y un AZUL fijo
2. Escriba un PIN de recuperación de un solo uso y pulse la tecla **Unlock (🔓)**		Los indicadores LED VERDE intermitente y AZUL fijo cambiarán a VERDE intermitente y, de nuevo, a VERDE intermitente y AZUL fijo
3. Vuelva a escribir el PIN de recuperación de un solo uso y pulse de nuevo la tecla **Unlock (🔓)**		Los LED VERDE intermitente y AZUL fijo cambiarán a un VERDE intermitente rápido y, finalmente, a un AZUL fijo para indicar que el PIN de recuperación de un solo uso se ha configurado correctamente

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** ( ) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

18. Cómo eliminar el PIN de recuperación de usuario de un solo uso

Para eliminar el PIN de recuperación de usuario de un solo uso, en primer lugar, acceda al **modo de administración** tal y como se describe en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Mayús** (⬆) **+ 4**		El LEDAZUL fijo cambiará a LED ROJO intermitente
2. Mantenga pulsadas de nuevo las teclas **Mayús** (⬆) **+ 4**		El LED ROJO intermitentecambiará a ROJO fijo y, después, a AZUL fijo para indicar que el PIN de recuperación de usuario de un solo uso se ha eliminado correctamente

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

19. Cómo activar el modo de recuperación y crear un nuevo PIN de usuario

El PIN de recuperación del usuario es extremadamente útil en los casos en los que el usuario ha olvidado el PIN para desbloquear la diskAshur³.
Para activar el modo de recuperación, en primer lugar, el usuario debe escribir el PIN de recuperación de un solo uso, en caso de que se haya configurado uno. El proceso de recuperación del PIN de usuario no afecta a los datos, la clave de cifrado y el PIN de administración; no obstante, el usuario tendrá que configurar un nuevo PIN de usuario de entre 8 y 64 dígitos.

Para activar el proceso de recuperación y configurar un nuevo PIN de usuario, continúe con los pasos siguientes.

1. En el **estado en espera** (LED ROJO), mantenga pulsadas las teclas **Unlock (🔓) y 4**		El indicador LED ROJO fijo cambiará a ROJO y VERDE intermitentes
2. Escriba el **PIN de recuperación** de un solo uso y pulse la tecla **Unlock (🔓)**		Los LED VERDE y AZUL se apagan y encienden alternativamente y, después, cambian a un LED VERDE fijo hasta que, finalmente, pasan a VERDE intermitente y AZUL fijo
3. Escriba un nuevo PIN de usuario y pulse la tecla **Unlock (🔓)**		Los indicadores LED VERDE intermitente y AZUL fijo cambian a un VERDE intermitente y, de nuevo, a VERDE intermitente y AZUL fijo
4. Vuelva a introducir su PIN de administración nuevo y pulse otra vez la tecla **Unlock (🔓)**		El LED VERDE parpadea rápidamente y, después, se convierte en VERDE fijo para indicar que el proceso de recuperación ha tenido éxito y se ha configurado un nuevo PIN de usuario

Importante: La creación de un nuevo PIN de usuario debe cumplir con la política correspondiente en caso de que se haya configurado una tal y como se detalla en la sección 7, la cual impone una longitud mínima para el PIN y si se utilizará o no un carácter especial. Consulte la sección 9 para conocer las restricciones del PIN de usuario.

20. Configurar solo lectura de usuario en el modo de administración

Existen muchos virus y troyanos que pueden infectar las unidades USB, por lo que la función de solo lectura es especialmente útil si necesita acceder a los datos en la unidad USB en un entorno público. También es una función esencial para fines forenses en los que es necesario conservar los datos en su estado original inalterado de forma que no se puedan modificar o sobrescribir.

Cuando el administrador configura la diskAshur³ y restringe el acceso del usuario a solo lectura, únicamente el administrador podrá escribir en la unidad o cambiar la configuración a lectura/escritura, tal y como se describe en la sección 21. El usuario únicamente podrá acceder a la unidad en solo lectura y no podrá escribir en la unidad ni cambiar esta configuración desde el modo de usuario.

Para configurar la diskAshur³ y restringir el acceso del usuario a solo lectura, en primer lugar debe acceder al **modo de administración** tal y como se describe en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En modo administrador, mantenga presionados los botones "**7 + 6**"		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)**		Los LED VERDE y AZUL cambiarán a un LED VERDE fijo y luego a un LED AZUL fijo que indica que la unidad se ha configurado y limita el acceso del usuario a solo lectura.

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

21. Permitir al usuario leer/escribir en modo administrador

Para volver a establecer el diskAshur³ en lectura/escritura, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo) proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones "**7 + 9**"		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)** una vez		Los LED VERDE y AZUL cambian a un LED VERDE fijo y luego a un LED AZUL fijo que indica que la unidad está configurada en lectura/escritura

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

22. Configurar solo lectura global en el modo de administración

Cuando el administrador configure la diskAshur³ y la restrinja el acceso a solo lectura global, ni el administrador ni el usuario podrán escribir en la unidad y solo podrán acceder en modo solo lectura. Solo el administrador podrá cambiar la configuración de nuevo a lectura/escritura según se describe en la sección 23.

Para configurar la diskAshur³ y restringir el acceso global a solo lectura, en primer lugar, debe acceder al **modo de administración** según se indica en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **5 y 6** .		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse la tecla **Unlock (🔓)**		Los indicadores LED VERDE y AZUL cambiarán a VERDE fijo y, después, a AZUL fijo para indicar que la unidad se ha configurado para restringir el acceso global al modo de solo lectura

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

23. Habilitar la lectura/escritura global en el modo de administración

Para configurar la diskAshur³ a un acceso lectura/escritura desde la configuración de solo lectura global, primero hay que acceder al **modo de administración** tal y como se indica en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **5 y 9** .		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse la tecla **Unlock (🔓)**		Los indicadores LED VERDE y AZUL cambiarán a un VERDE fijo y, a continuación, a un AZUL fijo para indicar que la unidad se ha configurado como lectura/escritura

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

24. Cómo configurar un PIN con autodestrucción

Es posible configurar un PIN con autodestrucción que realice un borrado criptográfico en la unidad, es decir, se borrará la clave de cifrado. El proceso elimina todos los PIN que se hayan configurado y prohibirá el acceso a todos los datos almacenados en la unidad (con lo que se perderán de manera definitiva). A continuación, la unidad se mostrará como desbloqueada con un LED VERDE. Al ejecutar esta función, el PIN con autodestrucción se convertirá en el nuevo PIN de usuario y será preciso formatear la unidad para poder volver a utilizarla.

1. En modo administrador, mantenga presionados los botones **Unlock (🔓) + 6**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Configure e introduzca un **PIN de autodestrucción** de 8 a 64 dígitos y presione el botón **Unlock (🔓)**		Los LED VERDE parpadeante y AZUL fijo cambiarán a un solo parpadeo LED VERDE y luego nuevamente a LED VERDE parpadeante y AZUL fijo
3. Vuelva a introducir su **PIN de autodestrucción** y presione el botón **Unlock (🔓)**		El LED VERDE parpadeará rápidamente durante varios segundos y luego cambiará a un AZUL fijo que indica que el PIN de autodestrucción se ha configurado correctamente

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

25. Cómo eliminar el PIN de autodestrucción

Para eliminar el PIN de autodestrucción, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Mayús (⬆) + 6**		El LED AZUL fijo cambiará a un LED ROJO parpadeante
2. Mantenga presionados nuevamente los botones **Mayús (⬆) + 6**		El LED ROJO parpadeante se volverá fijo y luego cambiará a un LED AZUL fijo que indica que el PIN de autodestrucción se ha eliminado correctamente

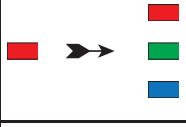
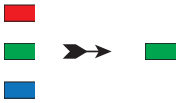
Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

26. Cómo desbloquear la unidad con el PIN con autodestrucción

Advertencia: Cuando se activa la autodestrucción, se eliminan todos los datos, la clave de cifrado y los PIN de administración y usuario. **El PIN de autodestrucción se convertirá en el PIN de usuario.** No habrá PIN de administración después de activar el mecanismo de autodestrucción. Será necesario restablecer primero la diskAshur³ (consulte "Cómo realizar un restablecimiento completo", en la sección 36, página 273) para poder configurar un PIN de administración con privilegios completos, incluida la capacidad de configurar un nuevo PIN de usuario.

Si se utiliza, el PIN con autodestrucción **eliminará TODOS los datos, la clave de cifrado y los PIN de administración y usuario** y, después, desbloqueará la unidad. Activar esta función hará que el **PIN con autodestrucción se convierta en el nuevo PIN de usuario** y será preciso formatear la diskAshur³ para poder añadirle datos nuevos.

Para activar el mecanismo de autodestrucción, la unidad debe estar en estado en espera (LED ROJO fijo). A continuación, proceda con los pasos siguientes.

1. En el estado en espera (LED ROJO fijo), mantenga pulsadas las **teclas Mayús (⬆) y Unlock (🔓)**		El LED ROJO cambiará a todos los LED, es decir, ROJO, VERDE y AZUL parpadeando al mismo tiempo
2. Escriba el **PIN con autodestrucción** y pulse la tecla **Unlock (🔓)**		Los indicadores LED ROJO, VERDE y AZUL intermitentes cambiarán a un VERDE intermitente y, después, a un VERDE fijo para indicar que la diskAshur³ se ha autodestruido con éxito

27. Cómo configurar un PIN de administrador después de un ataque de fuerza bruta o un reseteo

Después de un ataque de fuerza bruta o cuando se haya reiniciado el diskAshur³, será necesario configurar un PIN de administrador antes de que se pueda usar la unidad.

Requisitos del PIN:

- Debe tener entre 8 y 64 dígitos de longitud
- No debe contener solo números repetitivos, p. ej. (3-3-3-3-3-3-3-3)
- No debe contener solo números consecutivos, p. ej. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5- 4-3-2-1)
- El botón **Mayús** (⬆) se puede usar para combinaciones de PIN adicionales, por ejemplo, **Mayús** (⬆) **+ 1** es un valor diferente que solo 1. Consulte la sección 7: “Establecer una política de PIN de usuario”.

Si el diskAshur³ ha sido forzado o restablecido, la unidad estará en estado de espera (LED ROJO fijo). Para configurar un PIN de administrador, proceda con los siguientes pasos.

1. En estado de espera (LED ROJO fijo), mantenga presionados los botones **Mayús** (⬆) **+ 1**		El LED ROJO fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca el **PIN de administrador NUEVO** y presione el botón **Unlock (🔓)**		Los LED VERDE parpadeante y AZUL fijo cambiarán a un solo parpadeo LED VERDE y luego nuevamente a LED VERDE parpadeante y AZUL fijo
3. Vuelva a introducir el **PIN de administrador nuevo** y presione el botón **Unlock (🔓)**		El LED VERDE parpadeante y el LED AZUL fijo cambian a LED AZUL parpadeando rápidamente durante unos segundos y luego a un LED AZUL fijo que indica que el PIN de administrador se ha configurado correctamente.

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

28. Establecer el bloqueo automático desatendido

Para protegerse contra el acceso no autorizado si la unidad está desbloqueada y desatendida, el diskAshur³ se puede ajustar para que se bloquee automáticamente después de un período de tiempo preestablecido. En su estado predeterminado, la función de tiempo de espera de bloqueo automático desatendido del diskAshur³ está desactivada. El bloqueo automático desatendido se puede establecer para que se active entre 5 y 99 minutos.

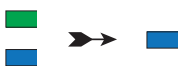
Para configurar la función de tiempo de espera de bloqueo automático desatendido, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Unlock (🔓) + 5**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Introduzca la cantidad de tiempo en que le gustaría establecer la función de tiempo de espera de bloqueo automático; el tiempo mínimo que se puede establecer es de 5 minutos y el máximo, de 99 minutos (5-99 minutos). Por ejemplo, introduzca: **05 durante 5 minutos (presione '0' seguido de un '5')** **20 durante 20 minutos (presione '2' seguido de un '0')** **99 durante 99 minutos (presione '9' seguido de otro '9')**		
3. Presione el botón **Mayús** (⬆)		Los LED VERDE y AZUL parpadeantes cambiarán a VERDE fijo durante un segundo y, finalmente, a un LED AZUL fijo que indica que el tiempo de espera de bloqueo automático se ha configurado correctamente

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

29. Desactivar el bloqueo automático desatendido

Para desactivar la función de tiempo de espera de bloqueo automático desatendido, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en modo administrador (LED AZUL fijo) proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones **Unlock (🔓) + 5**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Introduzca **00** y presione el botón **Mayús** (⬆)		Los LED VERDE y AZUL parpadeantes cambiarán a un VERDE fijo durante un segundo y luego, finalmente, a un LED AZUL fijo que indica que el tiempo de espera de bloqueo automático se ha desactivado correctamente

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

30. Cómo verificar el bloqueo automático desatendido

El administrador puede verificar y determinar el período de tiempo establecido para la función de tiempo de espera de bloqueo automático desatendido simplemente observando la secuencia de LED como se describe en la siguiente tabla.

Para verificar el bloqueo automático desatendido, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad esté en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionado **MAYÚS** (⬆) + **5**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)** y sucederá lo siguiente; a. Todos los LED (ROJO , VERDE y AZUL) permanecen fijos durante 1 segundo. b. Cada parpadeo del LED ROJO equivale a diez (10) minutos. c. Cada parpadeo del LED VERDE equivale a un (1) minuto. d. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo. e. Los LED vuelven a AZUL fijo		

La siguiente tabla describe el comportamiento del LED mientras se verifica el bloqueo automático desatendido; por ejemplo, si ha establecido la unidad para que se bloquee automáticamente después de **25** minutos, el LED ROJO parpadeará dos (**2**) veces y el LED VERDE parpadeará cinco (**5**) veces.

Bloqueo automático en minutos	**ROJO**	**VERDE**
5 minutos	0	5 parpadeos
15 minutos	1 parpadeo	5 parpadeos
25 minutos	2 parpadeos	5 parpadeos
40 minutos	4 parpadeos	0

Nota: Para salir inmediatamente del modo administrador (LED AZUL fijo), mantenga presionado el botón **MAYÚS** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

31. Establecer en solo lectura en modo usuario

Para establecer el diskAshur³ en solo lectura, acceda primero al "**modo usuario**" como se describe en la sección 13. Una vez que la unidad esté en **modo usuario** (LED VERDE fijo), proceda con los siguientes pasos.

1. En modo usuario, mantenga presionados los botones "**7 + 6**" (7=**L**ectura + 6=**S**olo)		El LED VERDE fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)**		Los LED VERDE y AZUL cambiarán a un LED VERDE fijo que indica que la unidad está configurada en solo lectura

Nota: 1. Si un usuario establece la unidad en solo lectura, el administrador puede anular esto configurando la unidad en lectura/escritura en modo administrador.

2. Si el administrador establece la unidad en solo lectura, el usuario no puede establecer la unidad en lectura/escritura.

32. Habilitar lectura/escritura en modo usuario

Para establecer el diskAshur³ en lectura/escritura, acceda primero al "**modo usuario**" como se describe en la sección 13. Una vez que la unidad esté en **modo usuario** (LED VERDE fijo), proceda con los siguientes pasos.

1. En modo usuario, mantenga presionados los botones "**7 + 9**" (7=**L**ectura + 9=**E**scritura)		El LED VERDE fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)**		Los LED VERDE y AZUL cambiarán a un LED VERDE fijo que indica que la unidad está configurada en lectura/escritura

Nota: 1. Si un usuario establece la unidad en solo lectura, el administrador puede anular esto configurando la unidad en lectura/escritura en modo administrador.

2. Si el administrador establece la unidad en solo lectura, el usuario no puede establecer la unidad en lectura/escritura.

33. Mecanismo de defensa frente a ataques por fuerza bruta

La diskAshur³ incorpora un mecanismo de defensa para protegerse frente a un ataque por fuerza bruta. De forma predeterminada, la limitación de fuerza bruta para el **PIN de administración** y el **PIN de usuario** se establece en **10** intentos fallidos de entrada del PIN consecutivos; para el **PIN de recuperación**, la limitación es de **5 intentos**. Se utilizan tres contadores de fuerza bruta independientes para registrar los intentos fallidos por cada autorización de PIN Si un usuario escribe un PIN de administración incorrecto diez veces seguidas, (divididas en 5, 3 o 2 agrupaciones, tal y como se indica a continuación) la unidad se restablecerá y se perderán todos los datos permanentemente. Si un usuario escribe un PIN de recuperación o un PIN de usuario incorrecto y supera la limitación de fuerza bruta correspondiente, los PIN implicados se borrarán, pero los datos seguirán almacenados en la unidad.

Nota: La limitación de fuerza bruta se programa con valores de fábrica cuando la unidad se restablece por completo o se activa la función de autodestrucción. Si el administrador cambia el PIN de usuario o bien se establece un PIN de usuario nuevo al activar la función de recuperación, el contador de fuerza bruta de dicho PIN de usuario se borrará, pero la limitación de la fuerza bruta no se verá afectada. Si el administrador cambia el PIN de recuperación, se borrará el contador de fuerza bruta de dicho PIN.

La autorización correcta de un PIN determinado hará que se borre el contador de ese PIN, pero no afectará a los contadores de otros PIN. Un fallo en la autorización de un PIN determinado aumentará el contador de fuerza bruta para ese PIN, pero no afectará a los contadores de otros PIN.

- Si un usuario introduce un **PIN de usuario incorrecto** 10 veces consecutivas, se eliminará dicho PIN de usuario, pero los datos, el PIN de administración y el PIN de recuperación se mantendrán intactos y accesibles.
- Si se introduce un **PIN de recuperación incorrecto** 5 veces consecutivas, dicho PIN se eliminará, pero los datos y el PIN de administración se mantendrán intactos y accesibles.
- El **PIN de administración** utiliza un mecanismo de defensa más sofisticado que los PIN de usuario y recuperación. Tras **5 intentos fallidos de entrada del PIN de administración consecutivos**, la unidad se bloqueará y los LED **ROJO**, **VERDE** y **AZUL** se encenderán sin parpadear. En ese momento, será preciso realizar los pasos siguientes para poder volver a introducir el PIN **3** veces.

- Escriba el PIN "47867243" y pulse la tecla **Unlock (🔓)**; los LED VERDE y AZUL parpadearán al mismo tiempo. La unidad ya está lista para aceptar otros **3** intentos de introducir el PIN de administración.
- Tras un total de 8 intentos fallidos seguidos, la unidad se bloqueará y los LED **ROJO**, **VERDE** y **AZUL** parpadearán de forma alterna. En este punto, se deben seguir los pasos que enumeramos a continuación para poder obtener los últimos **2** intentos de entrada de PIN (10 en total).
- Introduzca el PIN "**47867243**" y pulse la tecla **Unlock (🔓)**; los LED **VERDE** y **AZUL** parpadearán al mismo tiempo para indicar que la unidad está lista para aceptar los últimos **2** intentos de entrada de PIN (10 en total).
- Tras un total de 10 intentos de entrada de PIN de administración fallidos, la clave de cifrado se eliminará y se perderán para siempre todos los datos y los PIN almacenados en la unidad.

En la tabla siguiente se asume que se han configurado los tres PIN y se describe el efecto de activar el mecanismo de defensa por fuerza bruta para cada PIN individual.

PIN utilizado para desbloquear la unidad	Intentos fallidos consecutivos	Descripción de lo que ocurre
PIN de usuario	10	• El PIN de usuario se elimina. • El PIN de recuperación, el PIN de administración y todos los datos permanecen intactos y accesibles.
PIN de recuperación	5	• El PIN de recuperación se elimina. • El PIN de administración y todos los datos permanecen intactos y accesibles.
PIN de administración	5 3 2 (10 en totales)	• Así pues, tras introducir **5** veces un PIN del administrador incorrecto, la unidad se boqueará y se encenderán todos los LED de manera continua. • Introduzca el PIN "**47867243**" y pulse la tecla **Unlock (🔓)** para obtener **3** intentos más de entrada de PIN. • Tras un total de **8** (5+3) intentos consecutivos de entrada de PIN de administración fallidos, la unidad se bloqueará y los LED parpadearán de forma alterna. • Introduzca el PIN "**47867243**" y pulse la **Unlock (🔓)** para obtener los últimos **2** intentos de entrada de PIN (10 en total). • Tras un total de 10 intentos consecutivos de entrada de PIN de administración fallidos, la clave de cifrado se eliminará y se perderán para siempre todos los datos y los PIN almacenados en la unidad.

Importante: Es preciso configurar un nuevo PIN de administración si se ha aplicado fuerza bruta sobre el PIN anterior. Para ello, consulte "Cómo configurar un PIN de administración tras un ataque de fuerza bruta o un restablecimiento", en la sección 27, ———————— 267. También se deberá formatear la diskAshur³ para poder añadir datos nuevos a la unidad.

34. Cómo establecer la limitación de fuerza bruta del PIN de usuario

Nota: La configuración de la limitación de fuerza bruta para el PIN de usuario se establece de form predeterminada en 10 intentos consecutivos cuando la unidad se restablece por completo, se ha aplicado fuerza bruta o se ha activado el PIN de autodestrucción.

El administrador puede volver a programar la limitación de fuerza bruta para el PIN de usuario de la diskAshur³. Esta función se puede configurar para permitir entre 1 y 10 intentos fallidos consecutivos.

Para configurar la limitación de fuerza bruta del PIN de usuario, primero debe acceder al "**modo de administración**" tal y como se detalla en la sección 5. Una vez que la unidad esté en el**modo de administración** (LED AZUL fijo) continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **7 y 0**		El indicador LEDAZUL fijo cambiará a VERDE y AZUL parpadeando al mismo tiempo
2. Escriba el número de intentos para la limitación de fuerza bruta (entre 01 y 10); por ejemplo: • **01** para 1 intento • **10** para 10 intentos		
3. Pulse la tecla **Mayús** (⬆) una vez		Los indicadores LED VERDEy AZUL intermitentes cambiarán a VERDE fijo durante un segundo y, a continuación, a AZUL fijo para indicar que la limitación de fuerza bruta se ha configurado con éxito

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

35. Cómo comprobar la limitación de fuerza bruta del PIN de usuario

El administrador puede observar y averiguar el número de veces consecutivas que se permite la entrada incorrecta del PIN de usuario antes de que se active el mecanismo de defensa por fuerza bruta fijándose en la secuencia de los LED que se describe a continuación.

Para comprobar la configuración de la limitación de fuerza bruta, acceda primero al "**modo de administración**" según se describe en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **2** y **0**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse la tecla Unlock () y sucederá lo siguiente;**a.** Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo. b. Cada parpadeo del LED ROJO equivale a diez (10) unidades de un número de limitación de fuerza bruta. c. Cada parpadeo del LED VERDE equivale a una (1) única unidad de un número de limitación de fuerza bruta. d. Todos los LED (ROJO, VERDE y AZUL) se vuelven fijos durante 1 segundo. e. Los LED volverán a un AZUL fijo		

La tabla siguiente describe el comportamiento de los LED al verificar la configuración de la limitación de fuerza bruta. Por ejemplo, si ha configurado la fuerza bruta tras **5** intentos fallidos consecutivos, el LED VERDE parpadeará cinco (**5**) veces.

Configuración de limitación de fuerza bruta	ROJO	VERDE
2 intentos	0	2 parpadeos
5 intentos	0	5 parpadeos
10 intentos	1 parpadeo	0

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

36. Cómo realizar un reseteo completo

Para realizar un reseteo completo, el diskAshur³ debe estar en estado de espera (LED ROJO fijo). Una vez que se restablece la unidad, todos los PIN de administrador/usuario, la clave de cifrado y todos los datos se eliminarán y perderán para siempre, y la unidad deberá formatearse antes de poder ser reutilizada. Para restablecer el diskAshur³, proceda con los siguientes pasos.

1. En estado de espera (LED ROJO fijo), mantenga presionado el botón "**0**"		El LED ROJO fijo cambiará a todos los LED ROJO, VERDE y AZUL parpadeando alternativamente entre encendido y apagado
2. Mantenga presionados los botones **2 + 7**		Los LED alternantes ROJO, VERDE y AZUL se volverán fijos durante un segundo y luego cambiarán a un LED ROJO fijo que indica que la unidad se ha restablecido

Importante: Después de un reseteo completo, se debe configurar un PIN de administrador nuevo; consulte la sección 27 en la página 267 sobre 'Cómo configurar un PIN de administrador después de un ataque de fuerza bruta o un reseteo', el diskAshur³ también deberá ser formateado antes de que se puedan agregar nuevos datos a la unidad.

37. Cómo configurar la diskAshur³ como dispositivo de inicio

Nota: Cuando la unidad se configura como de inicio, al extraerla desde el sistema operativo, no se encenderá el LED ROJO. En su lugar, la unidad permanecerá en VERDE fijo y deberá desconectarse para el siguiente uso. La configuración predeterminada de la diskAshur³ no es la de encendido.

La diskAshur³ está equipada con una función de inicio para admitir un ciclo de encendido durante un proceso de arranque del host. Al encender desde la diskAshur³, su ordenador se ejecutará con el sistema operativo que se haya instalado en la diskAshur³.

Para configurar la unidad como dispositivo de encendido, primero debe acceder al "**modo de administración**" tal y como se detalla en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Unlock (🔓) y 9**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse **"0"** seguido de un **"1"** (**01**)		Los LED VERDE y AZUL continuarán intermitentes
3. Pulse la tecla **Mayús** (⬆) una vez.		Los indicadores LED VERDE y AZUL intermitentes cambiarán a un VERDE fijo y, finalmente, a un AZUL fijo para indicar que la unidad se ha configurado como dispositivo de inicio correctamente

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

38. Cómo deshabilitar la función de dispositivo de inicio de la diskAshur³

Para deshabilitar la función de dispositivo de inicio de la diskAshur³, primero debe acceder al "**modo de administración**" tal y como se detalla en la sección 5. Una vez que la unidad esté en el**modo de administración** (LED AZUL fijo) continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Unlock (🔓) y 9**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse **"0"** seguido de otro **"0"** (**00**)		Los LED VERDE y AZUL continuarán intermitentes
3. Pulse la tecla **Mayús** (⬆) una vez.		Los indicadores LED VERDEy AZUL intermitentes cambiarán a un VERDE fijo y, finalmente, a un AZUL fijo para indicar que la función de dispositivo de inicio se ha deshabilitado correctamente

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

39. Cómo comprobar la configuración de dispositivo de inicio

Para comprobar la configuración de dispositivo de inicio, primero debe acceder al "**modo de administración**" según se detalla en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Mayús** (⬆) **y 9**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes

2. Pulse la tecla **Unlock (🔓)** y se producirán una de estas dos situaciones;

- **Si la diskAshur³ se ha configurado como dispositivo de inicio, sucederá lo siguiente;**

a. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo.
b.El LED VERDE parpadeará una vez.
c. Todos los LED (ROJO, VERDE y AZUL) se vuelven fijos durante 1 segundo.
d. Los LED volverán a un AZUL fijo

- **Si la diskAshur³ NO <u>se ha configurado</u> como dispositivo de inicio, sucederá lo siguiente;**

a. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo.
b. Todos los LED se apagarán
c. Todos los LED (ROJO, VERDE y AZUL) se vuelven fijos durante 1 segundo.
d. Los LED volverán a un AZUL fijo

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

40. Cómo configurar el modo de cifrado

ADVERTENCIA: Cambiar el modo de cifrado de AES-XTS (valor predeterminado) a AES-ECB o AES-CBC hará que se elimine la clave de cifrado y que se restablezca la diskAshur³, por lo que los datos quedarán inaccesibles y se perderán definitivamente.

Siga estos pasos para configurar el modo de cifrado de la unidad diskAshur³ **AES-ECB**, indicado por el número **"01"**, o **AES-XTS**, indicado por el número **"02",** o bien **AES-CBC**, indicado por el número **"03"**. Esta función viene configurada como AES-XTS (02) de forma predeterminada. Tenga en cuenta que, al cambiar a un modo de cifrado diferente, todos los parámetros críticos se eliminarán y la unidad se restablecerá.

Para configurar el modo de cifrado de la diskAshur³, primero debe acceder al **modo de administración** tal y como se detalla en la sección 5. Una vez que la unidad diskAshur³ esté en el **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Unlock (🔓) y 1**.		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Escriba **01** para cambiar al cifrado **AES-ECB**; escriba **02** para cambiar al cifrado **AES-XTS (valor predeterminado)**; escriba **03** para cambiar al cifrado **AES-CBC**		Los LED Verde y Azul continuarán intermitentes
3. Pulse la tecla **Mayús** (⬆) una vez.		Los LED VERDE y AZUL cambiarán a un VERDE fijo y, a continuación, a un ROJO fijo (**estado de restablecimiento**) para indicar que el modo de cifrado se ha cambiado con éxito

Importante: Tras configurar el modo de cifrado, la diskAshur³ se restablece por completo y se debe configurar un nuevo PIN de administración. Consulte la sección 7 "Cómo configurar un PIN de administración después de un ataque por fuerza bruta o un restablecimiento".

41. Cómo comprobar el modo de cifrado

Para comprobar el modo de cifrado de la unidad de la diskAshur³, primero debe acceder al **modo de administración** tal y como se detalla en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Mayús** (⬆) y 1		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes

2. Pulse la tecla **Unlock (🔓)** y sucederá lo siguiente:

- **Si el modo de cifrado está configurado como AES-ECB, ocurrirá lo siguiente:**

a. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo.
b. El LED VERDE parpadeará una vez.
c. Todos los LED (ROJO, VERDE y AZUL) se vuelven fijos durante 1 segundo.
d. Los LED volverán a un AZUL fijo

- **Si el modo de cifrado está configurado como AES-XTS, ocurrirá lo siguiente:**

a. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo.
b .El LED VERDE parpadeará dos veces.
c. Todos los LED (ROJO, VERDE y AZUL) se vuelven fijos durante 1 segundo.
d. Los LED volverán a un AZUL fijo

- **Si el modo de cifrado está configurado como AES-CBC, ocurrirá lo siguiente:**

a. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo.
b .El indicador LED VERDE parpadeará tres veces.
c. Todos los LED (ROJO, VERDE y AZUL) se vuelven fijos durante 1 segundo.
d. Los LED volverán a un AZUL fijo

Nota: Para salir de inmediato del modo administración (LED AZUL fijo), mantenga pulsada la tecla **Mayús** (⬆) durante un segundo; el LED AZUL fijo cambiará a un LED ROJO fijo.

42. Cómo configurar el tipo de disco

La diskAshur³ se puede configurar como disco extraíble o como disco local (estado predeterminado). Al cambiar a un tipo de disco diferente, se borrarán los parámetros críticos y se eliminarán también todos los PIN, la clave de cifrado y los datos, con lo que la unidad entrará en estado de restablecimiento.

ADVERTENCIA: Cambiar el tipo de disco a extraíble o local (estado predeterminado) borrará la clave de cifrado y hará que la diskAshur³ se restablezca, por lo que todos los datos quedarán inaccesibles y se perderán definitivamente

Siga estos pasos para configurar el tipo de disco de la diskAshur³ como disco extraíble (**00**) o disco local (**01**). Esta función viene configurada como disco local (**01**) de forma predeterminada. Tenga en cuenta que, si cambia a un modo de cifrado diferente, todos los parámetros críticos se borrarán y la unidad se restablecerá.

Para configurar el tipo de disco de la diskAshur³, primero debe acceder al **modo de administración** tal y como se detalla en la sección 5. Una vez que la unidad diskAshur³ esté en el **modo de administración** (LEDAZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, mantenga pulsadas las teclas **Unlock (🔓) y 8**.		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Escriba **00** para configurar la unidad como **disco extraíble**; escriba **01** para configurar la unidad como **disco local (estado predeterminado)**		Los LED Verde y Azul continuarán intermitentes
3. Pulse la tecla **Mayús** (⬆) una vez.		Los indicadores LED VERDE y AZUL cambiarán a un VERDE fijo y, a continuación, a un LED ROJO (**estado de restablecimiento**) para indicar que el tipo de disco se ha cambiado con éxito

Importante: Tras cambiar el tipo de disco, la diskAshur³ se restablecerá por completo y será necesario configurar un nuevo PIN de administración. Consulte la sección 27 "Cómo configurar un PIN de administración tras un ataque por fuerza bruta o un restablecimiento'.

43. Cómo comprobar la configuración del tipo de disco

Para comprobar el tipo de disco de la diskAshur³, primero debe acceder al "**modo de administración**" tal y como se detalla en la sección 5. Una vez que la unidad esté en **modo de administración** (LED AZUL fijo), continúe con los pasos siguientes.

1. En el modo de administración, pulse las teclas **Mayús** (⬆) **y 8**		El indicador LED AZUL fijo cambiará a VERDE y AZUL intermitentes
2. Pulse la tecla **Unlock (🔓)** y sucederá lo siguiente: • **Si el tipo de disco se configura como extraíble, sucederá lo siguiente:** a. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo y luego se apagarán. b. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo otra vez y después se apagarán. d. Los LED volverán a un AZUL fijo • **Si el tipo de disco se configura como local, ocurrirá lo siguiente:** a. Todos los LED (ROJO, VERDE y AZUL) se volverán fijos durante 1 segundo. b. El LED VERDE parpadeará una vez. c. Todos los LED (ROJO, VERDE y AZUL) se vuelven fijos durante 1 segundo. d. Los LED volverán a un AZUL fijo		

44. Como inicializar y formatear la diskAshur³ para Windows

Después de un ataque por fuerza bruta o de un restablecimiento completo, la unidad diskAshur³ eliminará todos los PIN, los datos y la clave de cifrado. Deberá inicializar y formatear la diskAshur³ para volver a usarla.

Para formatear la diskAshur³, haga lo siguiente:

1. Configure un nuevo PIN de administración. Para ello, consulte "Cómo configurar un PIN de administración tras un ataque de fuerza bruta o un restablecimiento" en la sección 27.

2. Con la diskAshur³ en estado en espera (LED ROJO), pulse la tecla Unlock () una vez y escriba un nuevo PIN de administración para desbloquear la unidad (LED VERDE intermitente).

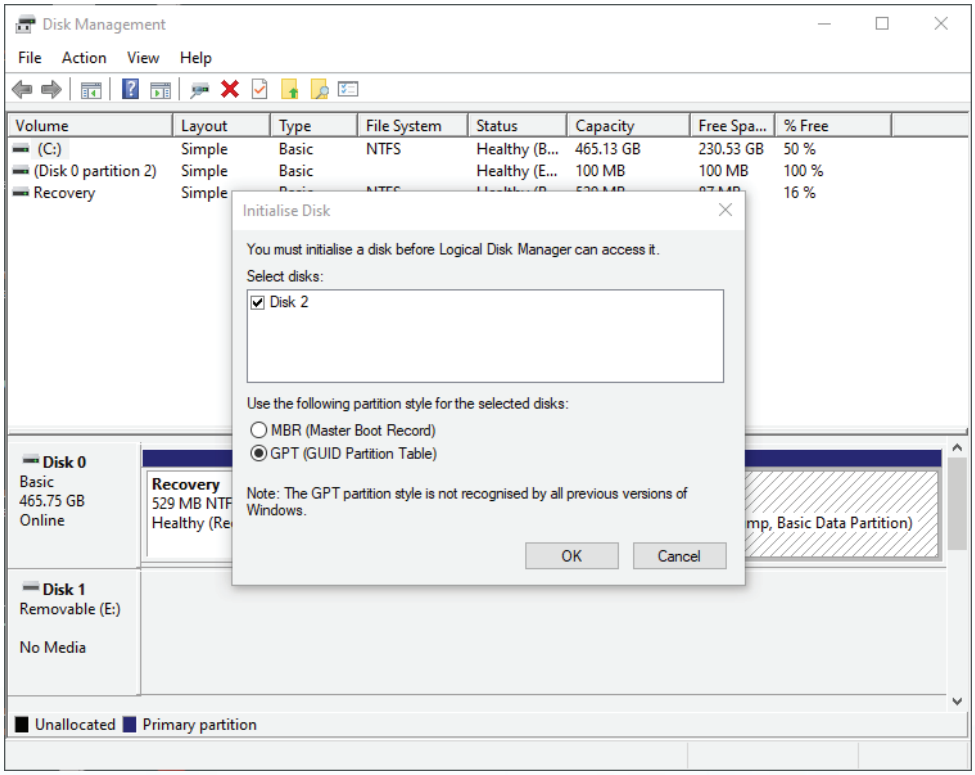
3. **Windows 7:** Haga clic con el botón de derecho en **Equipo** y, a continuación, seleccione **Administrar**y **Administración de discos**

   Windows 8: Haga clic con el botón derecho en la esquina izquierda del escritorio y seleccione **Administración de discos**

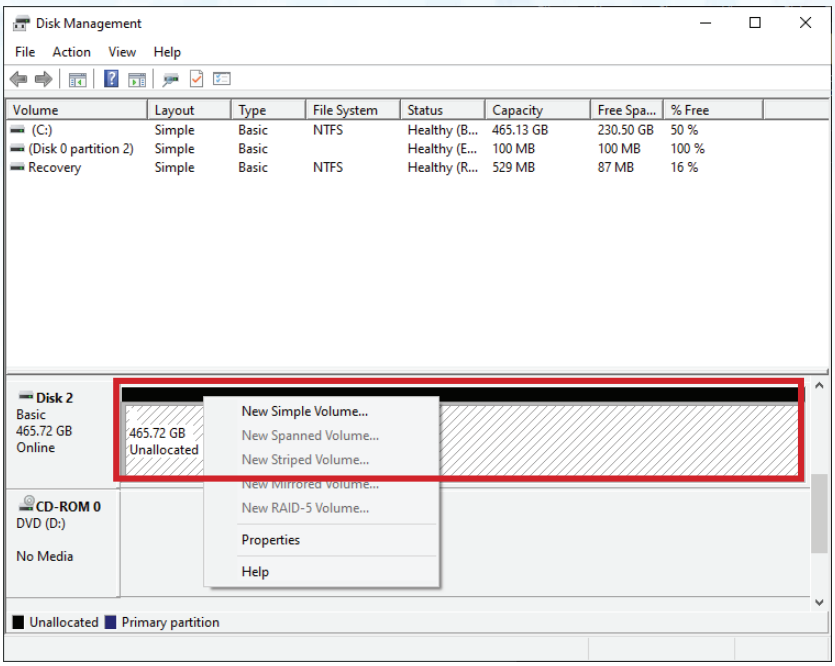
   Windows 10: Haga clic con el botón derecho en el botón de inicio y seleccione **Administración de discos**

4. En la ventana Administración de discos, la diskAshur³ se reconoce como dispositivo desconocido que no se ha inicializado ni se ha asignado. Debería aparecer un mensaje para que pueda elegir entre un estilo de partición MBR o GPT. GPT almacena múltiples duplicados de estos datos en el disco y, por lo tanto, es mucho más potente. En un disco MBR, la información de partición y de arranque se almacena en un único lugar.

Seleccione el estilo de partición y haga clic en **Aceptar**.



5. Haga clic con el botón de derecho en una región **sin asignar** del disco y, a continuación, haga clic en **Nuevo volumen simple**



6. Se abrirá la ventana de bienvenida al asistente del Nuevo volumen simple. Haga clic en Siguiente.

7. Si solo necesita una partición, acepte el tamaño predeterminado y haga clic en **Siguiente**.

8. Asigne una letra o ruta para la unidad y haga clic en **Siguiente**.

9. Cree una etiqueta de volumen, seleccione Formato rápido y, a continuación, haga clic en **Siguiente**.

10. Haga clic en **Finalizar**.

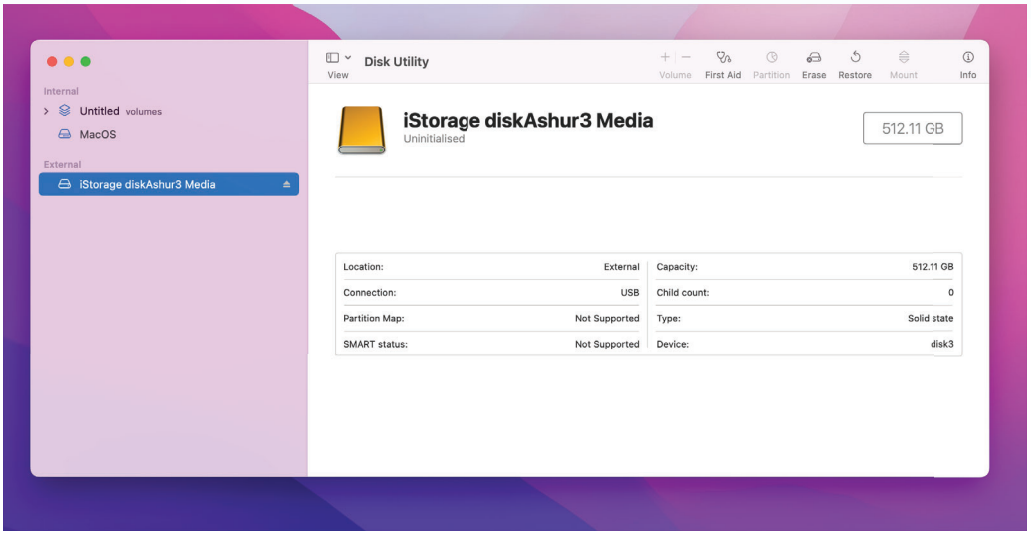
11. Espere hasta que se complete el proceso de formateo. La diskAshur³ se reconocerá debidamente y estará disponible para su uso.

45. Cómo inicializar y formatear la diskAshur³ en Mac OS

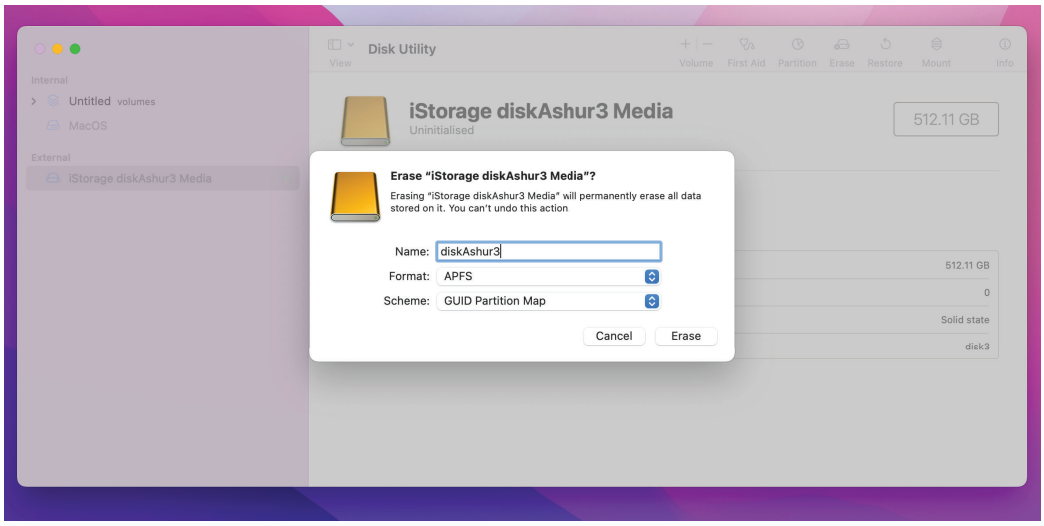
Después de un ataque por fuerza bruta o de un restablecimiento completo, la unidad diskAshur³ eliminará todos los PIN, los datos y la clave de cifrado. Deberá inicializar y formatear la diskAshur³ para poder empezar a usarla.

Para inicializar y formatear la diskAshur³:

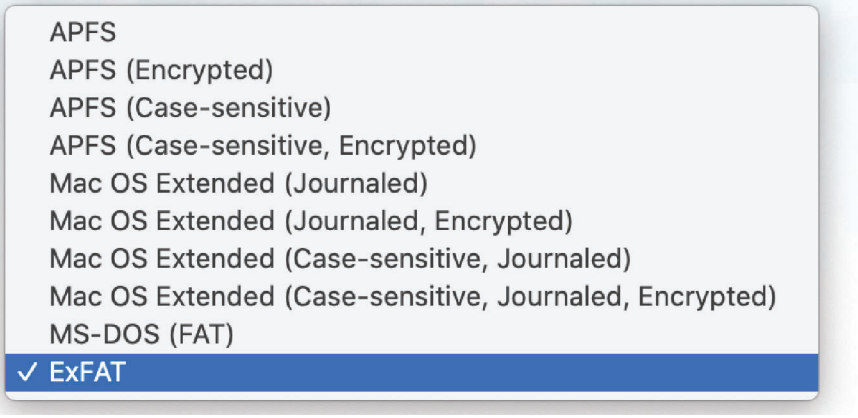
1. Seleccione diskAshur³ de la lista de unidades y volúmenes. Para cada unidad de la lista se mostrará su capacidad, fabricante y nombre de producto, como "**iStorage diskAshur³ Media**".



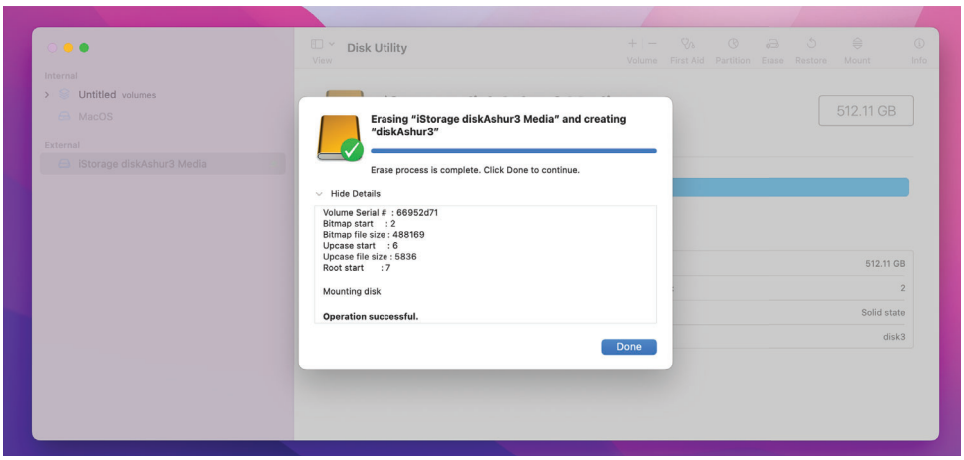
2. Haga clic en el botón "**Borrar**" bajo Utilidad de discos.
3. Introduzca un nombre para la unidad. El nombre predeterminado es "Sin título". El nombre de la unidad aparecerá finalmente en el escritorio.



4. Seleccione el esquema y el formato de volumen que desea usar. El menú desplegable Formatear volumen enumera los formatos de unidad disponibles compatibles con Mac. El tipo de formato recomendado es “Mac OS Extended (Journaled)”. En caso de utilizar una plataforma cruzada, utilice exFAT. El menú desplegable de formatos de esquemas enumera los esquemas disponibles. Recomendamos emplear “Mapa de particiones GUID” en unidades con una capacidad superior a 2 TB.

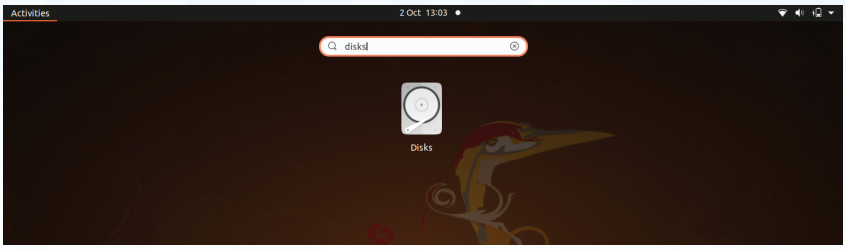


5. Haga clic en el botón “Borrar”. La Utilidad de discos desmontará el volumen del escritorio, lo borrará y lo volverá al montar después.

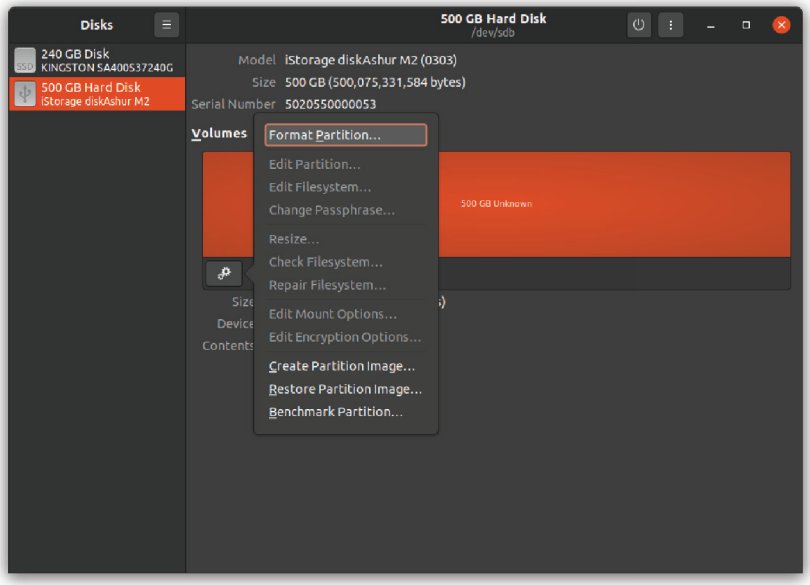


46. Cómo inicializar y formatear la diskAshur³ en Linux OS

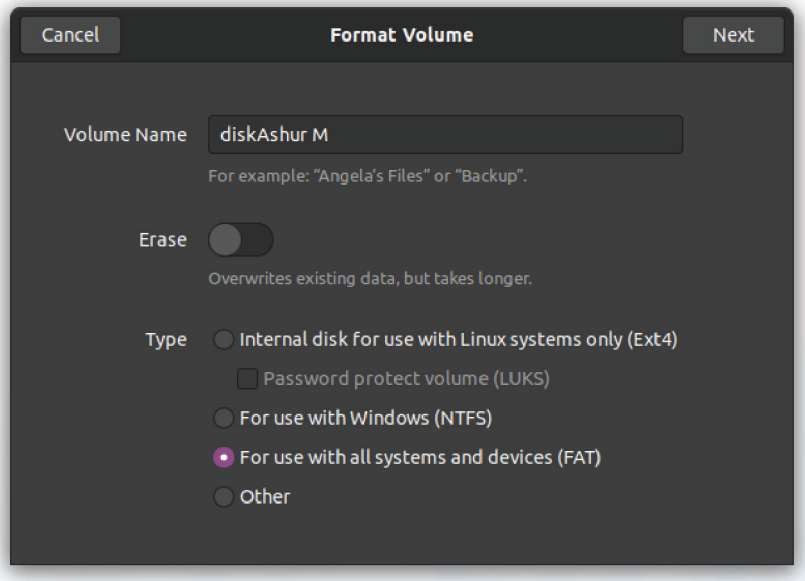
1. Abra **Show Application** y escriba **Disks** en el cuadro de búsqueda. Haga clic en la utilidad **Disks** cuando esta se visualice.



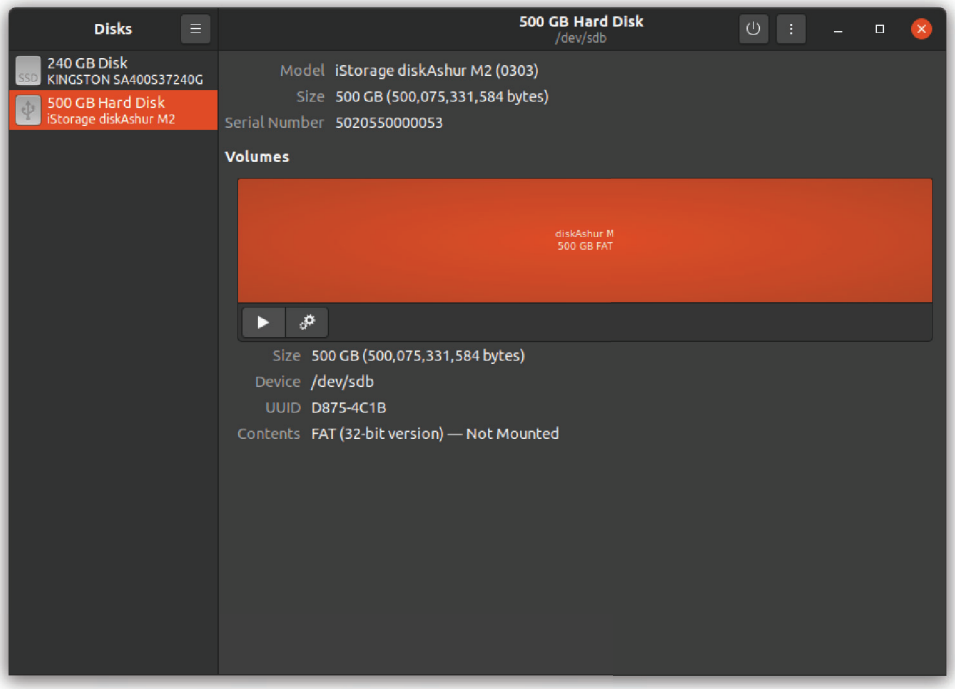
2. Haga clic para seleccionar la unidad (500 GB Hard Disk) en la sección **Devices**. A continuación, haga clic en el icono de engranajes bajo **Volumes** y después haga clic n **Format Partitions**.



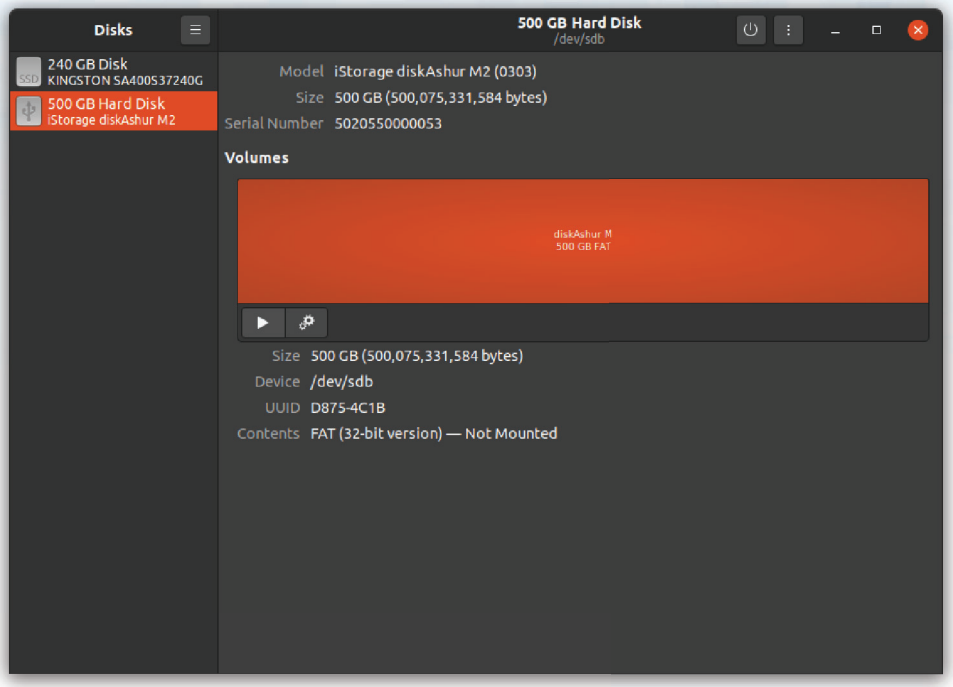
3. Seleccione **Compatible with all systems and devices (FAT)** para la opción **Type**. Escriba un nombre para la unidad, como, por ejemplo: diskAshur³. Luego haga clic sobre el botón **Format**.



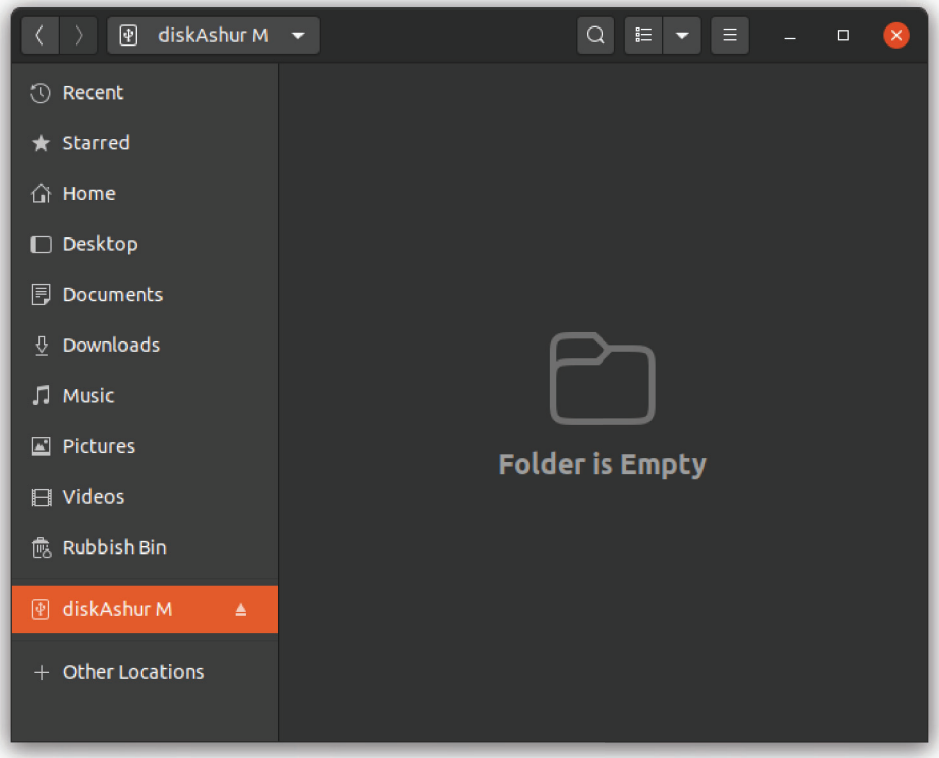
4. Cuando finalice el proceso de formateo, haga clic en el botón Play para montar la unidad en Ubuntu.



5. Ahora la unidad deberá estar montada en Linux y lista para su uso.



6. El disco se mostrará tal y como puede verse en la imagen a continuación. Puede hacer clic en el icono del disco para abrir la unidad.



47. Hibernar, suspender o cerrar sesión del sistema operativo

Asegúrese de guardar y cerrar todos los archivos en su diskAshur³ antes de hibernar, suspender o cerrar sesión en el sistema operativo.

Se recomienda que bloquee el diskAshur³ manualmente antes de hibernar, suspender o cerrar sesión en su sistema.

Para bloquear la unidad, expulse de manera segura el diskAshur³ de su sistema operativo host y luego desconéctelo del puerto USB. Si se escriben datos en la unidad, desenchufar el diskAshur³ provocará una transferencia de datos incompleta y una posible corrupción de los datos.

Atención: Para asegurarse de que sus datos estén seguros, no se olvide de bloquear su diskAshur³ si deja de usar su ordenador.

48. Cómo verificar el firmware en modo administrador

Para verificar el número de revisión del firmware, acceda primero al "**modo administrador**" como se describe en la sección 5. Una vez que la unidad está en **modo administrador** (LED AZUL fijo), proceda con los siguientes pasos.

1. En modo administrador, mantenga presionados los botones "**3 + 8**"		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)** una vez y ocurrirá lo siguiente; a. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo. b. El LED ROJO parpadea indicando la parte integral del número de revisión del firmware. c. El LED VERDE parpadea indicando la parte fraccionaria. d El LED AZUL parpadea indicando el último dígito del número de revisión del firmware e. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo. f. Los LED ROJO, VERDE y AZUL cambian a un LED AZUL fijo		

Por ejemplo, si el número de revisión del firmware es '**2.3**', el LED ROJO parpadeará dos (**2**) veces y el LED VERDE parpadeará tres (**3**) veces. Una vez que la secuencia ha terminado, los LED ROJO, VERDE y AZUL parpadearán juntos una vez y luego regresarán al modo administrador, un LED AZUL fijo.

49. Cómo verificar el firmware en modo usuario

Para verificar el número de revisión del firmware, introduzca primero el "**modo usuario**" como se describe en la sección 13. Una vez que la unidad está en **modo usuario** (LED VERDE fijo), proceda con los siguientes pasos.

1. En modo usuario, mantenga presionados los botones **"3 + 8"** hasta que los LED VERDE y AZUL parpadeen juntos		El LED VERDE fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **Unlock (🔓)** y sucederá lo siguiente; a. Todos los LED (ROJO , VERDE y AZUL) permanecen fijos durante 1 segundo. b. El LED ROJO parpadea indicando la parte integral del número de revisión del firmware. c. El LED VERDE parpadea indicando la parte fraccionaria. d. El LED AZUL parpadea indicando el último dígito del número de revisión del firmware e. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo. f. Los LED ROJO, VERDE y AZUL cambian a un LED AZUL fijo		

Por ejemplo, si el número de revisión del firmware es '**2.3**', el LED ROJO parpadeará dos (**2**) veces y el LED VERDE parpadeará tres (**3**) veces. Una vez que la secuencia haya terminado, los LED ROJO, VERDE y AZUL parpadearán juntos una vez y luego regresarán al modo usuario, un LED VERDE fijo.

50. Asistencia técnica

iStorage le ofrece los siguientes recursos útiles:

Sitio web:
https://www.istorage-uk.com

Asistencia de correo electrónico:
support@istorage-uk.com

Asistencia telefónica:
+44 (0) 20 8991-6260.

Los especialistas de asistencia técnica de iStorage están disponibles de 9:00 a 17:30 GMT, de lunes a vierne.

51. Información de garantía y autorización de devolución de material (RMA)

DESCARGO DE RESPONSABILIDAD Y GARANTÍA DEL PRODUCTO DE ISTORAGE

iStorage garantiza que en el momento de la entrega y durante un período de 36 meses a partir de la misma, sus productos carecerán de defectos materiales. Sin embargo, esta garantía no se aplica en las circunstancias que se describen a continuación. iStorage garantiza que los productos cumplen con los estándares enumerados en la ficha técnica correspondiente en nuestro sitio web en el momento en que realiza su pedido.

Estas garantías no se aplican a ningún defecto en los productos que originado por:

- desgaste normal por el uso;
- daños intencionales, almacenamiento o condiciones de funcionamiento anormales, accidente, negligencia por su parte o por parte de un tercero;
- una ejecución o un uso de los productos por su parte o por parte de un tercero no conforme con las instrucciones del usuario;
- cualquier alteración o reparación por usted o por un tercero que no sea uno de nuestros reparadores autorizados; o
- cualquier especificación proporcionada por usted.

En virtud de estas garantías, decidiremos, a nuestra discreción, reparar, sustituir o reembolsar cualquier producto que tenga defectos materiales, siempre que los tenga en el momento de la entrega:

- deberá inspeccionar los productos para verificar si tienen algún defecto material, además de
- probar el mecanismo de cifrado en los productos.

No seremos responsables de ningún defecto material o defecto en el mecanismo de cifrado de los productos que se pueda determinar en una inspección en el momento de la entrega, a menos que nos notifique dichos defectos en un plazo de 30 días posteriores a la entrega. No seremos responsables de ningún defecto material o defecto en el mecanismo de cifrado de los productos que no se pueda determinar en una inspección en el momento de la entrega, a menos que nos notifique dichos defectos en un plazo de 30 días desde el momento en que descubrió o debió tener conocimiento de dichos defectos. No seremos responsables en virtud de estas garantías si usted o cualquier otra persona hiciera uso de los productos después de descubrir un defecto. Después de notificar cualquier defecto, debe devolvernos el producto defectuoso. Si usted como cliente es una empresa, su empresa será responsable de los costes de transporte en los que incurra al enviarnos los productos o partes de los productos en garantía, y nosotros seremos responsables de los costes de transporte en los que incurramos al enviarle un producto reparado o de sustitución. Si es un consumidor, consulte nuestros términos y condiciones.

Los productos devueltos deben estar en su embalaje original y limpios. Los productos devueltos de otra manera podrán ser rechazados o se cobrará una tarifa adicional por los mismos para cubrir los costes añadidos, a la entera discreción de la compañía. Los productos devueltos para su reparación en garantía deben ir acompañados de una copia de la factura original o bien indicar el número de la factura original y la fecha de compra.

Si usted es un consumidor, esta garantía es complementaria a sus derechos legales en relación con los productos defectuosos o que no se corresponden con la descripción. Puede obtener asesoramiento sobre sus derechos legales en su oficina de Citizens Advice o en la oficina del consumidor.

Las garantías establecidas en esta cláusula se aplican únicamente al comprador original de un producto de iStorage o al revendedor o distribuidor autorizado de iStorage. Estas garantías no son transferibles.

EXCEPTO POR LA GARANTÍA LIMITADA QUE SE PROPORCIONA EN LA PRESENTE Y EN LA MEDIDA EN QUE LA LEY LO PERMITA, ISTORAGE NIEGA CUALESQUIERA OTRAS GARANTÍAS, EXPRESAS O IMPLÍCITAS, INCLUIDAS TODAS LAS GARANTÍAS DE COMERCIABILIDAD, IDONEIDAD PARA UN PROPÓSITO PARTICULAR o NO INFRACCIÓN. ISTORAGE NO GARANTIZA QUE EL PRODUCTO VAYA A FUNCIONAR SIN ERRORES. EN LA MEDIDA EN QUE PUEDA EXISTIR CUALQUIER GARANTÍA IMPLÍCITA EN VIRTUD DE LA LEY, DICHA GARANTÍA SE LIMITARÁ A LA DURACIÓN DE LA MISMA. LA REPARACIÓN O SUSTITUCIÓN DEL PRESENTE PRODUCTO, COMO SE INDICA AQUÍ, ES SU ÚNICO RECURSO.

EN NINGÚN CASO ISTORAGE SERÁ RESPONSABLE DE PÉRDIDAS O GANANCIAS PREVISTAS, NI DE CUALESQUIERA DAÑOS INCIDENTALES, PUNITIVOS, EJEMPLARES, ESPECIALES, DE CONFIANZA O CONSECUENTES, INCLUYENDO, ENTRE OTROS, LAS PÉRDIDAS DE INGRESOS, DE BENEFICIOS, DE USO DE SOFTWARE, OTRAS PÉRDIDAS Y LA RECUPERACIÓN DE DATOS, LOS DAÑOS A LA PROPIEDAD Y LAS RECLAMACIONES DE TERCEROS QUE DERIVEN DE CUALQUIER TEORÍA DE RECUPERACIÓN, INCLUYENDO GARANTÍA, CONTRATO, RECURSO LEGAL O AGRAVIO, INDEPENDIENTEMENTE DE QUE SE HUBIESE INFORMADO DE LA POSIBILIDAD DE TALES DAÑOS. NO OBSTANTE EL PLAZO DE CUALQUIER GARANTÍA LIMITADA O IMPLÍCITA POR LEY, O EN EL SUPUESTO DE QUE ALGUNA GARANTÍA LIMITADA NO CUMPLA SU FINALIDAD ESENCIAL, LA RESPONSABILIDAD TOTAL DE ISTORAGE NO SUPERARÁ EN NINGÚN CASO EL PRECIO DE COMPRA DEL PRESENTE PRODUCTO. | 4823-2548-5683.3

iStorage®

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, Inglaterra
Tel: +44 (0) 20 8991 6260 | Fax: +44 (0) 20 8991 6277
correo electrónico: info@istorage-uk.com | web: www.istorage-uk.com