iStorage®

DISKASHUR® M²



User Manual..... 2

Manuel de l'utilisateur..... 39

Benutzerhandbuch..... 76

Manuale d'uso..... 113

ユーザーガイド..... 150

Gebruikershandleiding..... 187

Manual del usuario..... 224

Εγχειρίδιο χρήστη 261

User Manual



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 diskAshur M² please contact our support team by email - support@istorage-uk.com or by phone on +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2020. All rights reserved.

Windows is a registered trademark of Microsoft Corporation.
All other trademarks and copyrights referred to are the property of their respective owners.

Distribution of modified versions of this document is prohibited without the explicit permission of the copyright holder.

Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID

RoHS Compliant

REACH COMPLIANCE

All trademarks and brand names are the property of their respective owners

Trade Agreements Act (TAA) Compliant

CITRIX® vmware®

Table of Contents

Introduction 5
Box contents 5
diskAshur M² Layout 5
1. LED indicators and their actions 6
2. LED States 6
3. First Time Use 7
4. Unlocking diskAshur M² 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 diskAshur M² with User PIN 14
14. Changing the User PIN in User Mode 14
15. Creating a One-Time User Recovery PIN 15
16. Deleting the One-Time User Recovery PIN 15
17. Activating Recovery Mode and Creating New User PIN 16
18. Set User Read-Only in Admin Mode 16
19. Enable User Read/Write in Admin Mode 17
20. Set Global Read-Only in Admin Mode 17
21. Enable Global Read/Write in Admin Mode 18
22. How to configure a Self-Destruct PIN 18
23. How to delete the Self-Destruct PIN 19
24. How to Unlock with the Self-Destruct PIN 19
25. How to Configure an Admin PIN after a Brute Force attack or Reset 20
26. Setting the Unattended Auto-Lock 20
27. Turn off the Unattended Auto-Lock 21
28. How to check the Unattended Auto-Lock 22
29. Set Read-Only in User Mode 22
30. Enable Read/Write in User Mode 23
31. Brute Force Hack Defence Mechanism 23
32. Admin PIN Brute Force Hack Defence Mechanism 24
33. How to set the User PIN Brute Force Limitation 24
34. How to check the User PIN Brute Force Limitation 25
35. How to perform a complete reset 26
36. How to configure diskAshur M² as Bootable 26
37. How to disable the diskAshur M² Bootable feature 27
38. How to check the Bootable setting 27
39. Initialising and formatting diskAshur M² for Windows 28
40. Initialising and formatting diskAshur M² in Mac OS 30
41. Initialising and formatting diskAshur M² in Linux OS 32
42. Hibernating, Suspending or Logging off from the Operating System 35
43. How to check Firmware in Admin Mode 35
44. How to check Firmware in User Mode 36
45. Technical Support 37
46. Warranty and RMA information 37

Introduction

Thank you for purchasing the new iStorage diskAshur M², an ultra-secure and easy to use, hardware encrypted, PIN authenticated portable Solid State Drive (SSD) with capacities of 120GB to 2TB and rising.

Designed to be FIPS 140-3 Level 3, the diskAshur M² encrypts data in transit and at rest using AES-XTS 256-bit full disk hardware encryption.

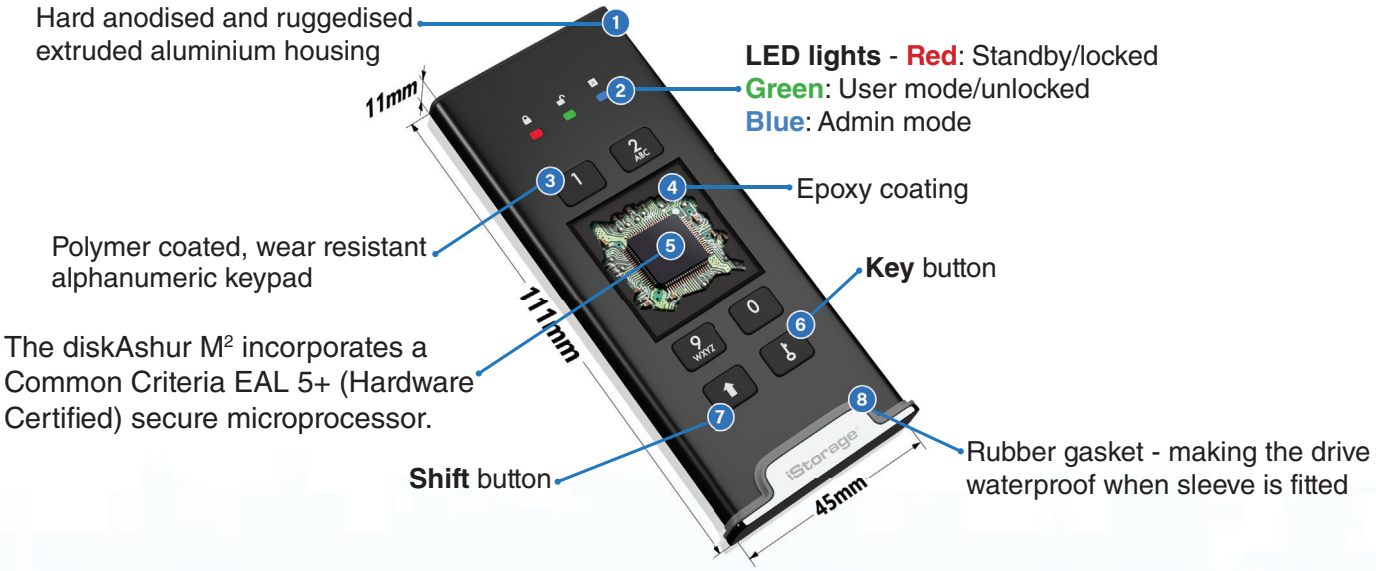
The diskAshur M² incorporates a Common Criteria EAL 5+ (Hardware Certified) secure microprocessor, which employs built-in physical protection mechanisms designed to defend against external tamper, bypass attacks and fault injections.

Unlike other solutions, the diskAshur M² 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

- diskAshur M² portable SSD & Protective Sleeve
- Protective carry case
- USB C & A Cables
- Quick start guide & Product disclaimer

diskAshur M² Layout



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		GREEN and BLUE Blinking alternately	Authentication in progress

2. LED States

Note: The normal function of the diskAshur M² may be disturbed by strong Electro-Magnetic Interference. If so, simply power cycle the product (power off then power on) to resume normal operation. If normal operation does not resume, please use the product in a different location.

To wake from Idle State

Idle state is defined as when diskAshur M² is not being used and all LEDs are off.

To wake diskAshur M² from the idle state do the following.

Connect the diskAshur M² to a powered USB port on your computer		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the drive is in Standby State

To enter Idle State

To force diskAshur M² to enter Idle State, execute either of the following operations:

- Disconnect the drive if connected to a USB port, all LEDs 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 or User PIN entry
Reset	RED Solid	×	×	Waiting for configuration of an Admin PIN

3. First Time Use

diskAshur M² is supplied in the **'Initial Shipment State' with no pre-set Admin PIN**. A **7-15** 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 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

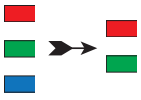
Password Tip: You can configure a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the button with the corresponding letters on it.

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 diskAshur M² for the first time, please follow the simple steps in the table below.

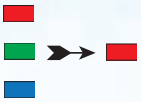
Instructions - First Time Use	LED	LED State
1. Connect the diskAshur M² to a powered USB port on your computer		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to solid RED and GREEN LEDs indicating the drive is in the Initial Shipment State
2. Press and hold down both **KEY (🔑) + 1** buttons		LEDs turn to blinking GREEN and solid BLUE
3. Enter a **New Admin PIN** (7-15 digits) and press the **KEY (🔑)** 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 **KEY (🔑)** button again		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 drive unlocked

Locking the diskAshur M²

To lock the drive, safely eject the diskAshur M² from your host operating system and then unplug from the USB port. If data is being written to the drive, unplugging the diskAshur M² will result in incomplete data transfer and possible data corruption.

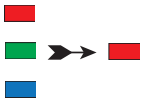
4. Unlocking diskAshur M² with the Admin PIN

To unlock the diskAshur M² with the Admin PIN, please follow the simple steps in the table below.

1. Connect the diskAshur M² to a USB port on your computer		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the drive is in Standby State
2. In Standby State (solid RED LED) press the **KEY (🔑)** button once		GREEN and BLUE LEDs blink together
3. With the GREEN and BLUE LEDs blinking together, enter the **Admin PIN** and press the **KEY (🔑)** button again		GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED and changing to a solid GREEN LED indicating the drive has been successfully unlocked as Admin

5. How to Enter Admin Mode

To Enter Admin Mode, do the following.

1. Connect the diskAshur M² to a powered USB port on your computer		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the drive is in Standby State
2. In Standby State (solid RED LED) Press and hold down both **KEY (🔑) + 1** buttons		GREEN and BLUE LEDs blink together
3. Enter your **Admin PIN** and press the **KEY (🔑)** button once		GREEN and BLUE LEDs will rapidly blink together several times and then switch to a solid GREEN LED and finally changing to a solid BLUE LED 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 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

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 **KEY (🔑) + 2** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **NEW Admin PIN** and then press the **KEY (🔑)** 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 **KEY (🔑)** 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 7 to 15 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 7-15 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 7-15 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 7-15 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 **KEY (🔑) + 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 **KEY (🔑) + 7** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **070** 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 **KEY (🔑)** 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 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (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 **KEY (🔑) + 3** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New User PIN** and press **KEY (🔑)** 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 **KEY (🔑)** 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 **KEY (🔑) + 3** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New User PIN** and press **KEY (🔑)** 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 **KEY (🔑)** 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.

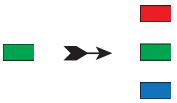
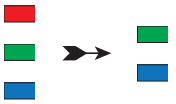
13. How to Unlock diskAshur M² with User PIN

To unlock the diskAshur M² with the **User PIN,** proceed with the following steps.

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

14. Changing the User PIN in User Mode

To change the **User PIN**, first unlock the diskAshur M² 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 **KEY (⚷) + 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 **KEY (⚷)** button once		GREEN and solid BLUE LEDs will alternate on and off and will then 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 **KEY (⚷)** 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 **KEY (⚷)** 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

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.

15. 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 diskAshur M².
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 7-15 digit User PIN.

To configure a One-Time 7-15 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 **KEY (🔑) + 4** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter a **One-Time Recovery PIN** and press **KEY (🔑)** 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 **KEY (🔑)** 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.

16. 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.

17. 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 diskAshur M².
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 7-15 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 **KEY (🔑) + 4** buttons		Solid RED LED will change to blinking RED and GREEN LEDs
2. Enter the One-Time **Recovery PIN** and press the **KEY (🔑)** 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 **KEY (🔑)** 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 **KEY (🔑)** 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.

18. 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 diskAshur M² 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 19. The User is restricted to Read-Only access and cannot write to the drive or change this setting in user mode.

To set the diskAshur M² 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 **KEY (🔑)** 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.

19. Enable User Read/Write in Admin Mode

To set the diskAshur M² 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.

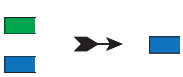
1. In Admin mode, press and hold down both "**7 + 9**" buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY (🔑)** button once		GREEN and BLUE LEDs change to a solid GREEN LED then to a solid BLUE LED indicating the drive is configured as Read/Write

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.

20. Set Global Read-Only in Admin Mode

When the Administrator configures the diskAshur M² 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 21.

To set the diskAshur M² 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 **KEY (🔑)** 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.

21. Enable Global Read/Write in Admin Mode

To set the diskAshur M² 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 **KEY (🔑)** 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.

22. 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 **KEY (🔑) + 6** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Configure and enter a 7-15 digit **Self-Destruct PIN** and press the **KEY (🔑)** 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 **KEY (🔑)** button		GREEN LED will rapidly blink for several seconds and then changes 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.

23. 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

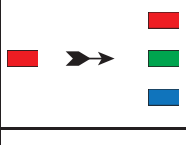
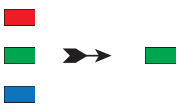
Note: To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED.

24. 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 diskAshur M² will need to be reset (see 'How to perform a complete reset' Section 35, on page 26) 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, 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 diskAshur M² 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** (⬆) + **KEY (🔑)** buttons		RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter the **Self-Destruct PIN** and press the **KEY (🔑)** button		RED, GREEN and BLUE blinking LEDs will change to GREEN and BLUE LEDs alternating on and off for a few seconds and finally shifts to a solid GREEN LED indicating the diskAshur M² has successfully self-destructed

25. 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 diskAshur M² has been reset to configure an Admin PIN before the drive can be used.

PIN Requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

If the diskAshur M² 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.

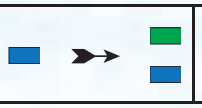
1. In Standby state (solid RED LED), press and hold down both **SHIFT** (⬆) **+ 1** buttons		Solid RED LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New Admin PIN** and press **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the **New Admin PIN** and press **KEY (🔑)** button		Blinking GREEN LED and solid BLUE LED change to BLUE LED rapidly blinking for a few seconds 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.

26. Setting the Unattended Auto-Lock

To protect against unauthorised access if the drive is unlocked and unattended, the diskAshur M² can be set to automatically lock after a pre-set amount of time. In its default state, the diskAshur M² Unattended Auto Lock time-out feature is turned off. The Unattended Auto Lock can be set to activate between 5 - 99 minutes.

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 **KEY (🔑) + 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.

27. 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 **KEY (🔑) + 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.

28. 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 **KEY** (🔑) 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.

29. Set Read-Only in User Mode

To set the diskAshur M² 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 **KEY** (🔑) 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.

30. Enable Read/Write in User Mode

To set the diskAshur M² 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 **KEY (🔑)** 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.

31. Brute Force Hack Defence Mechanism

The diskAshur M² incorporates a defence mechanism to protect the drive against Brute Force attacks. By default, the initial shipment state values of the brute force limitation (consecutive incorrect PIN entries) for both the Admin PIN and User PIN is **10** and **5** for the Recovery PIN. Three independent brute force counters are used to record the incorrect attempts for each PIN authorisation (Admin, User and Recovery) as set out below.

- 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.
- If an **incorrect Admin PIN** is entered 10 consecutive times, the drive will reset. All PINs and data are deleted and 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 of each individual PIN.

PIN used to unlock drive	Consecutive incorrect PIN enteries	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	10	• The diskAshur M² will reset. All PINs and data are deleted and lost forever.

Note: The brute force limitation is defaulted to initial shipment state values when the drive is completely reset, or self-destruct feature is activated, or brute forced. If Admin changes the User PIN, or a new User PIN is set when activating the recovery feature, the User PIN brute force counter is zeroed (0) but the brute force limitation is not affected. If Admin changes the Recovery PIN, the Recovery PIN brute force counter is zeroed.

Successful authorisation of a certain PIN will zero 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.

32. Admin PIN Brute Force Hack Defence Mechanism

The diskAshur M² Admin PIN is equipped with a more sophisticated defence mechanism in comparison to the User PIN or the Recovery PIN. This is meant to protect against accidentally entering an incorrect Admin PIN 10 consecutive times and subsequently losing all of your data. So after 5 consecutive incorrect Admin PIN entries, the diskAshur M² will lock and all LEDs light up and become solid.

WARNING: Do not attempt the following instructions if you unlock your diskAshur M² using the '**USER PIN**' only and you do not know the '**ADMIN PIN**'.

Refer to the instructions in the table below to enable further Admin PIN entries up to a maximum of 10.

Consecutive incorrect Admin PIN entries	Description of what happens to the diskAshur M²	Instructions
5	All LEDs, **RED**, **GREEN** & **BLUE** light up and become **solid**.	Enter the following PIN '**47867243'** and press the **KEY (🔑)** once, with both **GREEN** and **BLUE** LEDs alternately blinking on and off, the diskAshur M² is ready to accept a further **3 Admin PIN** entries.
8	All LEDs, **RED**, **GREEN** & **BLUE** alternately **blink on** and **off**.	Enter the following PIN '**47867243'** and press the **KEY (🔑)** once, with both **GREEN** and **BLUE** LEDs alternately blinking on and off, the diskAshur M² is ready to accept a further **2 Admin PIN** entries.
10	**RED** LED will light up and become solid.	After a total of 10 incorrect Admin PIN entries, the encryption key, all PINs and data will be deleted and lost forever.

33. 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 diskAshur M² 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.

34. 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 **KEY (🔑)** 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.

35. How to perform a complete reset

To perform a complete reset, the diskAshur M² 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 diskAshur M² 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 25 on page 20 on 'How to Configure an Admin PIN after a Brute Force attack or Reset', the diskAshur M² will also need to be formatted before any new data can be added to the drive.

36. How to configure diskAshur M² 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 diskAshur M2 is configured as non-bootable.

The diskAshur M² is equipped with a bootable feature to accommodate power cycling during a host boot process. When booting from the diskAshur M², you are running your computer with the operating system that is installed on the diskAshur M².

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 **KEY (🔑) + 8** 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.

37. How to disable the diskAshur M² Bootable feature

To disable the diskAshur M² 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 **KEY (🔑) + 8** 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.

38. 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** (⬆) **+ 8** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs

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

- **If diskAshur M² 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 diskAshur M² 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.

39. Initialising and formatting diskAshur M² for Windows

After a 'Brute Force Attack' or a complete reset the diskAshur M² will delete all PINs,data and the encryption key. You will need to initialise and format the diskAshur M² before it can be used.

To format your diskAshur M², do the following:

1. Configure a new Admin PIN - see page 20, section 25, 'How to configure an Admin PIN after a Brute Force attack or reset'.

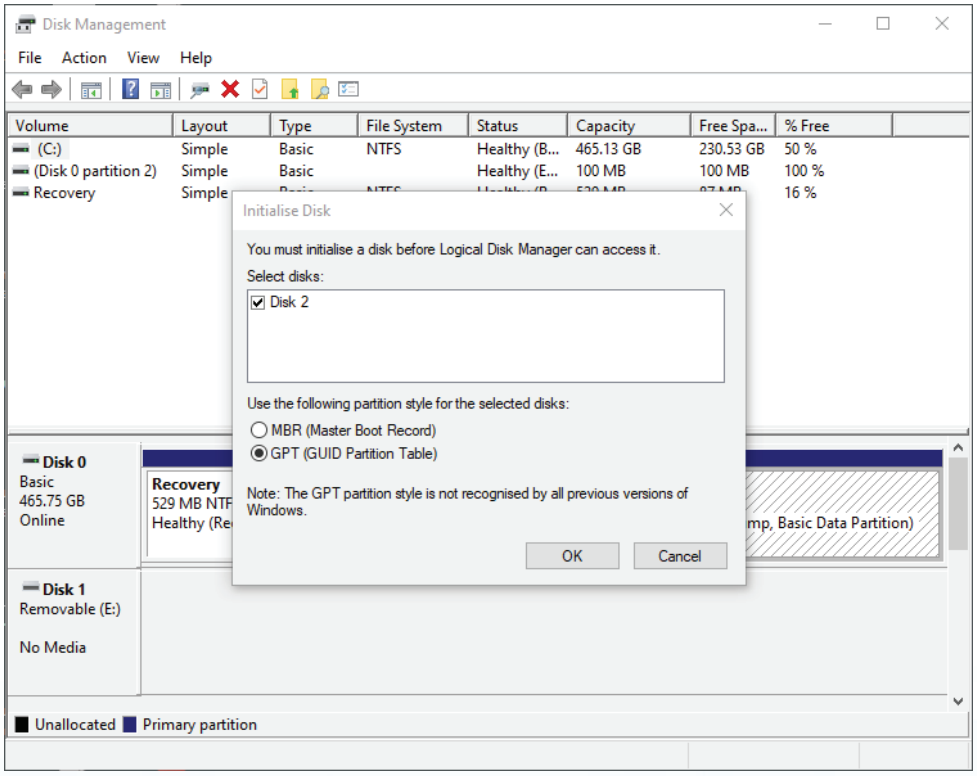
2. With the diskAshur M² in standby state (RED LED), press the **KEY (⚷)** button once and enter **New Admin PIN** to unlock (blinking GREEN LED).

3. Attach the diskAshur M² to the computer.

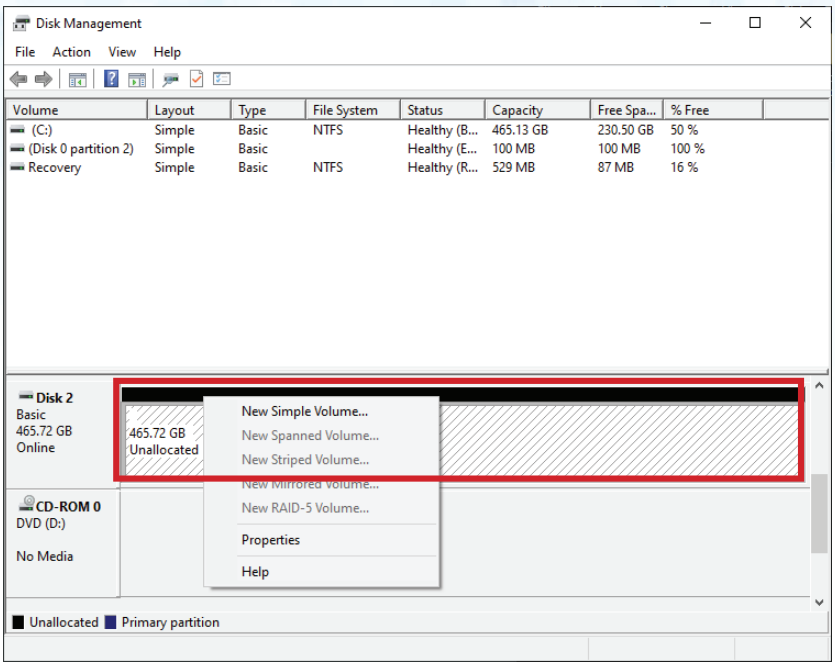
4. **Windows 7:** Right click **Computer** and then click **Manage** and then select **Disk Management**
   Windows 8: Right-click left corner of desktop and select **Disk Management**
   Windows 10: Right click on the start button and select **Disk Management**

5. In the Disk Management window, the diskAshur M² 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**.



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



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



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

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

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

11. Click **Finish**.

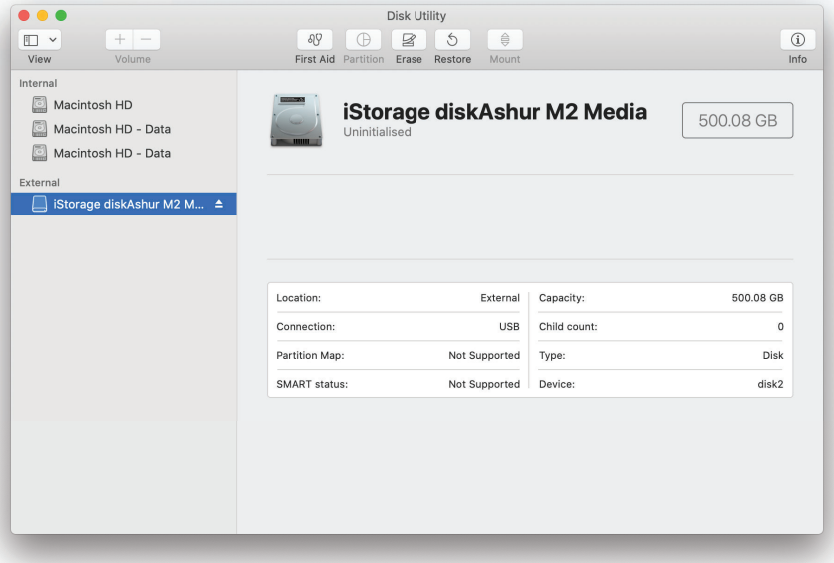
12. Wait until the format process is complete. The diskAshur M² will be recognised and it is available for use.

40. Initialising and formatting diskAshur M² in Mac OS

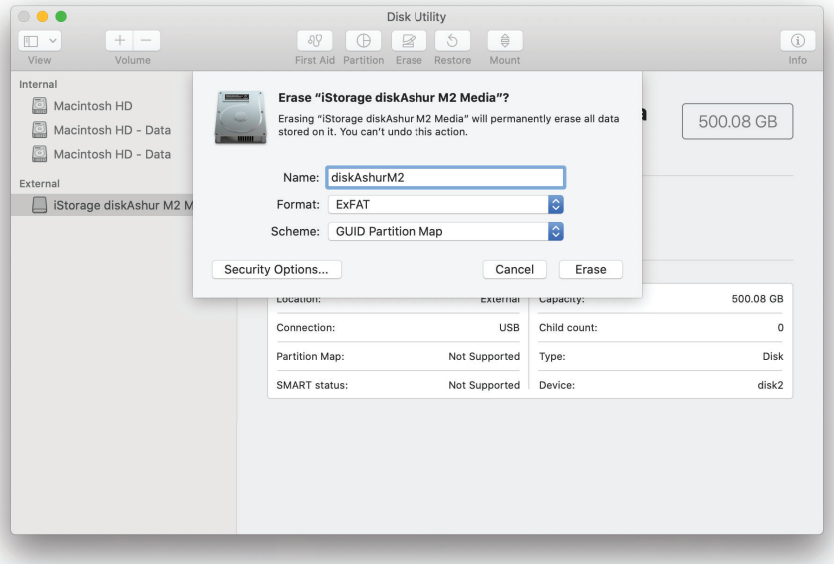
After a 'Brute Force Attack' or a complete reset the diskAshur M² will delete all PINs,data and the encryption key. You will need to initialise and format the diskAshur M² before it can be used.

To initialize and format the diskAshur M²:

1. Select diskAshur M² from the list of drives and volumes. Each drive in the list will display its capacity, manufacturer, and product name, such as '**iStorage diskAshur M² Media**'.



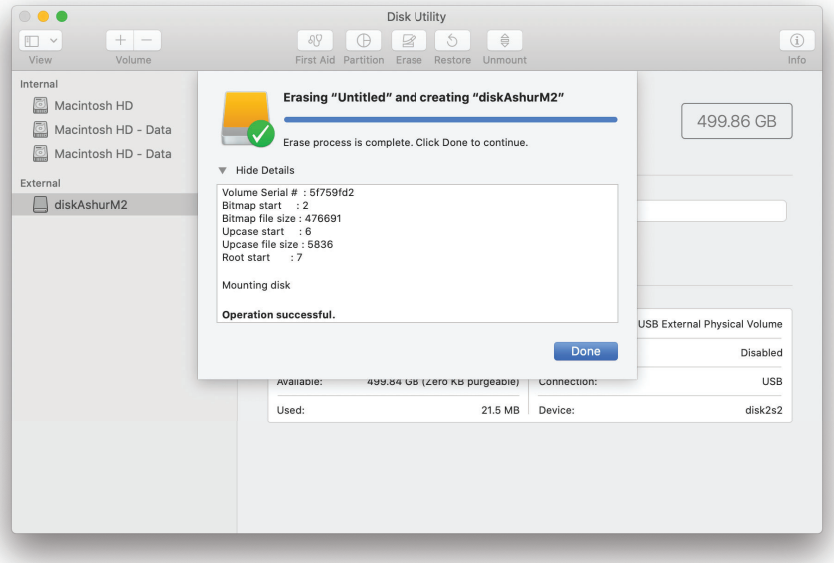
2. Click the '**Erase**' button under Disk Utility.
3. Enter a name for the drive. The default name is Untitled. The name of the drive will eventually appear on the desktop.



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.

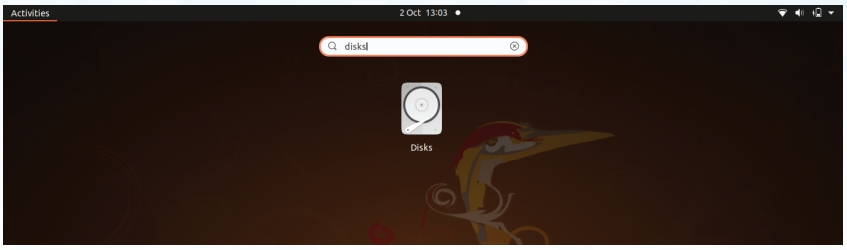


5. Click the 'Erase' button. Disk Utility will unmount the volume from the desktop, erase it, and then remount it on the desktop.

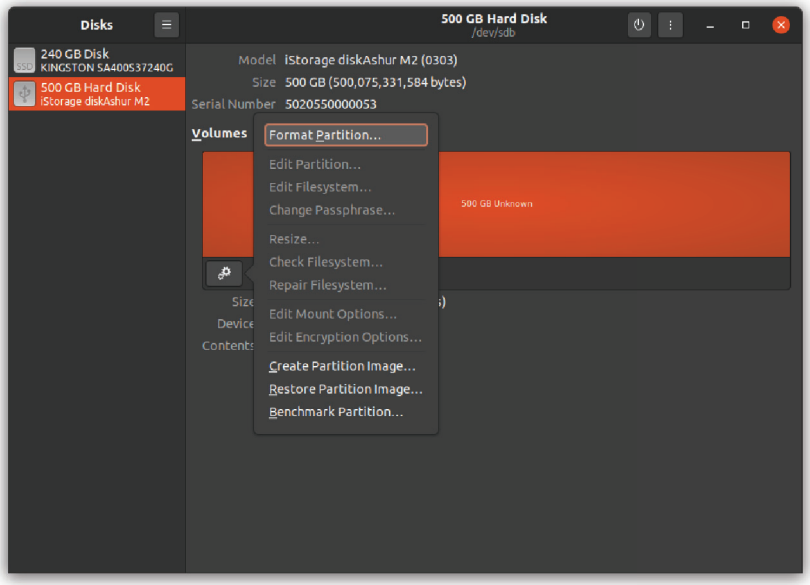


41. Initialising and formatting diskAshur M² in Linux OS

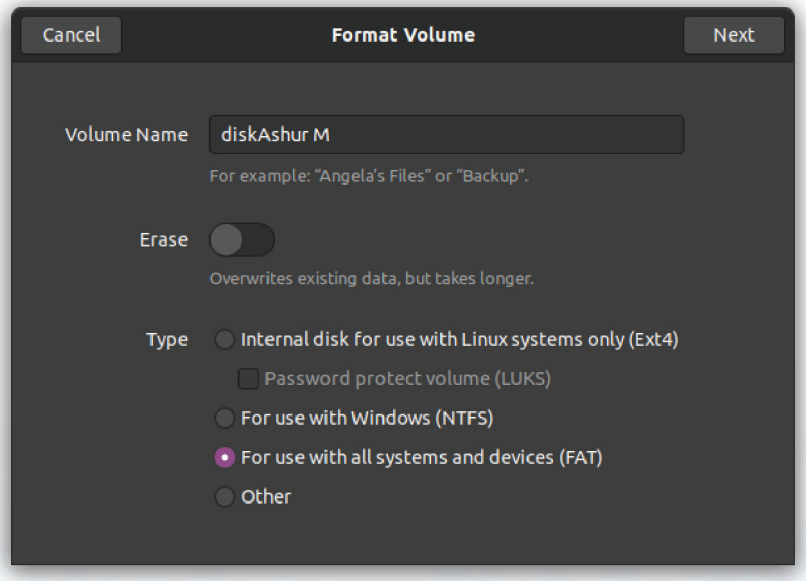
1. Open '**Show Application**' and type '**Disks**' in the search box. Click on the '**Disks**' utility when displayed.



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**'.

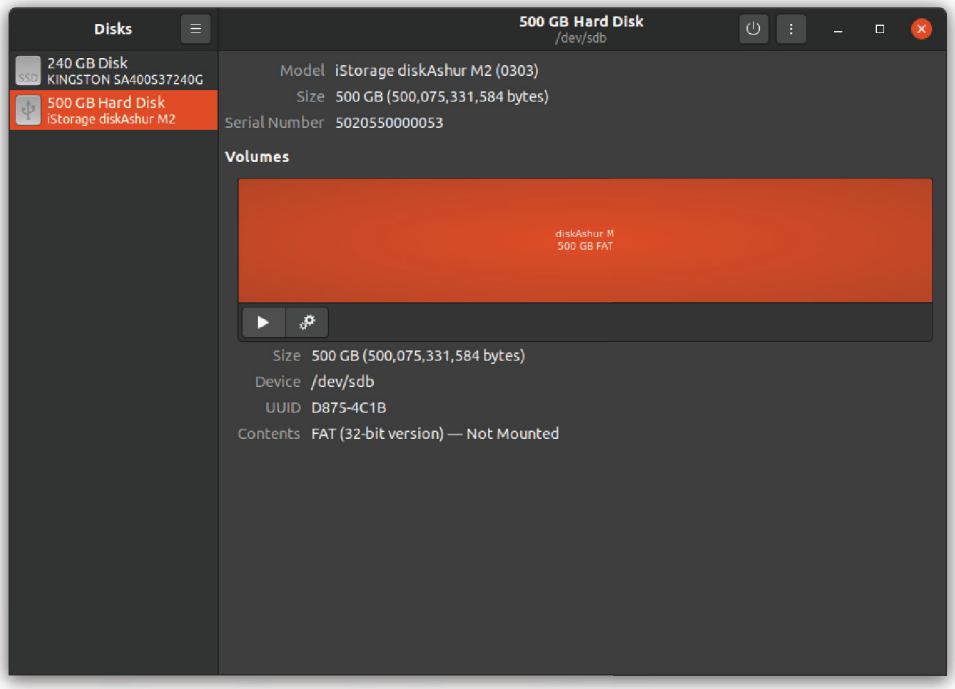


3. Select '**Compatible with all systems and devices (FAT)**' for the '**Type**' option. And enter a name for the drive, e.g: diskAshur M². Then, click the '**Format**' button.

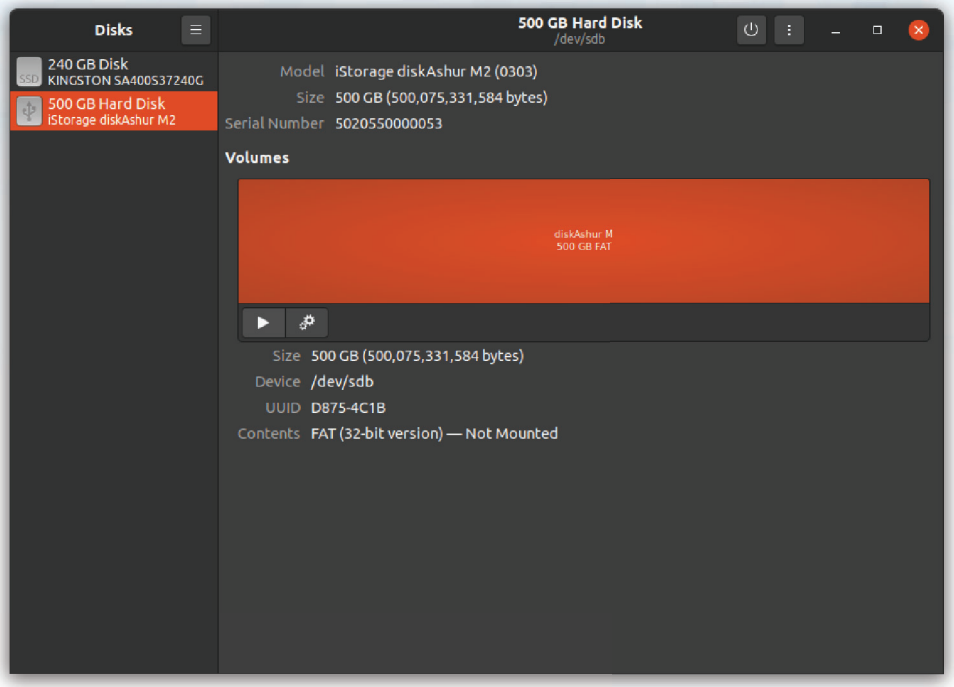




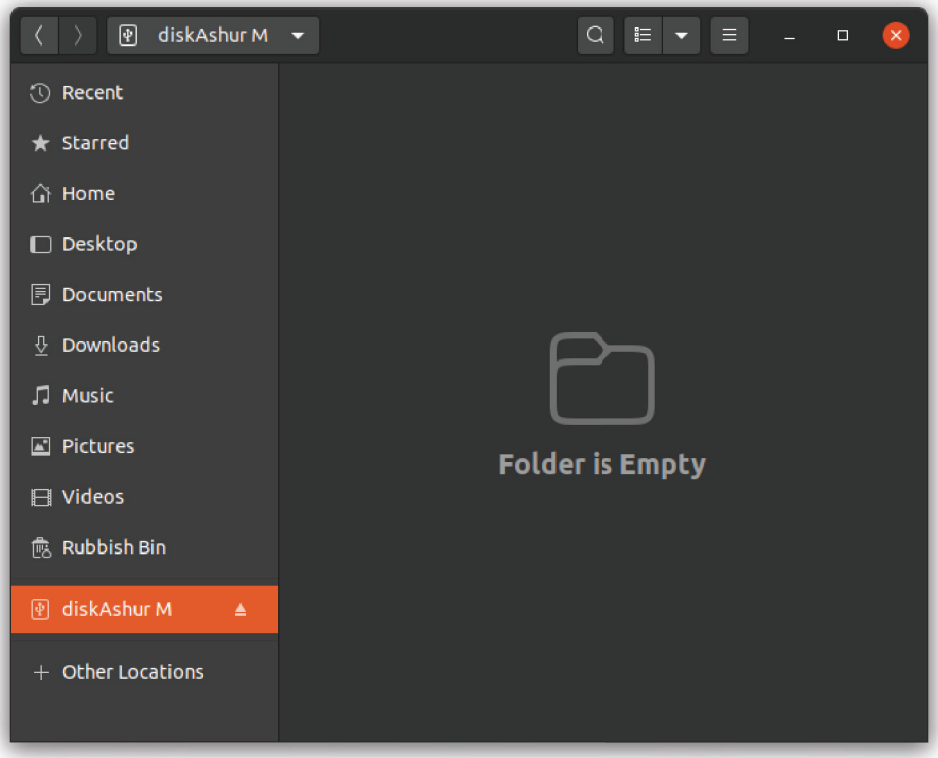
4. After the format process is finished, click Play button to mount the drive to Ubuntu.



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.



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

Be sure to save and close all the files on your diskAshur M² before hibernating, suspending, or logging off from the operating system.

It is recommended that you lock the diskAshur M² manually before hibernating, suspending, or logging off from your system.

To lock the drive, safely eject the diskAshur M² from your host operating system and then unplug from the USB port. If data is being written to the drive, unplugging the diskAshur M² will result in incomplete data transfer and possible data corruption.

⚠ **Attention:** To ensure your data is secure, be sure to lock your diskAshur M² if you are away from your computer.

43. 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 **KEY (♿)** 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 '**2.3**', the RED LED will blink twice (**2**) and the GREEN LED will blink three (**3**) 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.

44. 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 **KEY (🔑)** 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 BLUE LED		

For example, if the firmware revision number is '**2.3**', the RED LED will blink twice (**2**) and the GREEN LED will blink three (**3**) 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.

45. 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.

46. 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

Copyright © iStorage Limited 2020. All rights reserved.
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

Manuel de l'utilisateur



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 diskAshur M², veuillez contacter notre équipe clientèle par courriel - support@istorage-uk.com ou par téléphone au +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2020. Tous droits réservés.

Windows est une marque déposée de Microsoft Corporation.
Toutes les autres marques et droits d'auteur cités sont la propriété de leurs propriétaires respectifs.

La distribution de versions modifiées de ce document est interdite sans l'autorisation explicite du détenteur des droits d'auteur.

La distribution de l'ouvrage ou de ses dérivés sous forme de livre standard (papier) à des fins commerciales est interdite sans l'autorisation préalable du détenteur des droits d'auteur.

LA DOCUMENTATION EST FOURNIE TELLE QUELLE ET TOUTES LES CONDITIONS, DÉCLARATIONS ET GARANTIES EXPRESSES OU IMPLICITES, Y COMPRIS TOUTE GARANTIE IMPLICITE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE PARTICULIER OU DE NON-CONTREFAÇON, SONT REJETÉES, SAUF DANS LA MESURE OÙ CES REJETS SONT CONSIDÉRÉS COMME LÉGALEMENT INVALIDES

RoHS Compliant

REACH COMPLIANCE

Toutes les marques et noms de marque sont la propriété de leurs propriétaires respectifs

Conformité à la loi sur les accords commerciaux (TAA)

CITRIX® vmware®

Sommaire

Introduction 42
Contenu 42
Configuration diskAshur M² 42
1. Voyants LED et leurs actions 43
2. Statuts des LED 43
3. Première utilisation 44
4. Déverrouillage du diskAshur M² avec le code PIN de l'administrateur 45
5. Comment accéder au mode administrateur 45
6. Changer le code PIN administrateur 46
7. Définition d'une politique de code PIN utilisateur 47
8. Comment supprimer la politique de code PIN utilisateur 48
9. Comment vérifier la politique du code PIN utilisateur 48
10. Ajout d'un nouveau code PIN utilisateur en mode administrateur 49
11. Modification du code PIN utilisateur en mode administrateur 50
12. Suppression du code PIN utilisateur en mode administrateur 50
13. Comment déverrouiller le diskAshur M² avec le code PIN utilisateur 51
14. Modification du code PIN utilisateur en mode utilisateur 51
15. Création d'un code PIN utilisateur de récuperation à usage unique 52
16. Suppression d'un code PIN utilisateur de récuperation à usage unique 52
17. Activation du mode de récupération et création d'un nouveau code PIN utilisateur 53
18. Définir le mode lecture seule pour un utilisateur en mode administrateur 53
19. Activer le mode lecture/écriture pour l'utilisateur en mode administrateur 54
20. Définir le mode lecture seule en mode administrateur 54
21. Activer le mode lecture/écriture de manière générale en mode administrateur 55
22. Instructions pour configurer un code PIN d'autodestruction 55
23. Instructions pour supprimer un code PIN d'autodestruction 56
24. Comment déverrouiller le disque avec le code PIN d'autodestruction 56
25. Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation 57
26. Réglage du verrouillage automatique 57
27. Désactiver le verrouillage automatique 58
28. Comment vérifier le verrouillage automatique 59
29. Activer la fonction lecture seule en mode utilisateur 59
30. Activer le mode lecture/écriture en mode utilisateur 60
31. Protection contre les attaques par force brute 60
32. Mécanisme de défense contre le piratage du code PIN Administrateur 61
33. Comment définir la limitation de la force brute pour le code PIN de l'utilisateur 61
34. Comment vérifier la limitation de la force brute pour le code PIN de l'utilisateur 62
35. Comment effectuer une réinitialisation complète 63
36. Comment configurer le diskAshur M² comme bootable 63
37. Comment désactiver la fonction bootable du diskAshur M² 64
38. Comment vérifier le paramètre bootable 64
39. Initialisation et formatage du diskAshur M² pour Windows 65
40. Initialisation et formatage du diskAshur M² sous Mac OS 67
41. Initialisation et formatage du diskAshur M² sous Linux 69
42. Hibernation suspension ou déconnexion du système d'exploitation 72
43. Comment vérifier le firmware en mode administrateur 72
44. Comment vérifier le firmware en mode utilisateur 73
45. Support technique 74
46. Informations sur la garantie et le RMA 74

Introduction

Nous vous remercions d'avoir acheté le nouveau diskAshur M² d'iStorage, un disque SSD externe ultra-sécurisé et facile à utiliser, doté d'un chiffrement matériel et authentifié par un code PIN, d'une capacité de 120 Go à 2 To et plus.

Conçu pour être certifié FIPS 140-3 niveau 3, le diskAshur M² chiffre les données en transit et au repos en utilisant le chiffrement matériel AES-XTS 256 bits du disque complet.

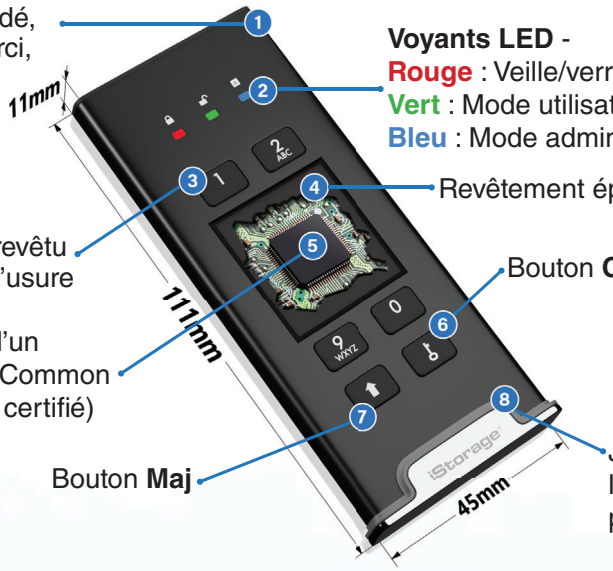
Le diskAshur M² dispose d'un microprocesseur sécurisé Common Criteria EAL5 + (hardware certifié), qui utilise des mécanismes de protection physique intégrés conçus pour se défendre contre les manipulations externes, les attaques de contournement et les injections de fautes.

Contrairement à d'autres solutions, le diskAshur M² réagit à une attaque automatisée en entrant dans un état de blocage, ce qui rend toutes ces attaques inutiles. En termes simples, sans le code PIN, il n'y a pas d'accès !

Contenu

- diskAshur M² portable SSD et housse de protection
- étui de protection
- câbles USB C & A
- guide de démarrage rapide et clause de non-responsabilité du produit

Configuration diskAshur M²



1. Voyants LED et leurs actions

LED	Statut du LED	Description	LED	Statut du LED	Description
	ROUGE fixe	Disque verrouillé (en état de **veille** ou de **réinitialisation**)		BLEU fixe	disque en **mode administrateur**
	Double clignotement ROUGE	Saisie incorrecte du code PIN		ROUGE, VERT et BLEU Clignotent ensemble	En attente de la saisie du code PIN de **l'utilisateur**
	VERT fixe	Disque **débloqué**		VERT et BLEU Clignotent ensemble	En attente de la saisie du code PIN de **l'administrateur**
	VERT clignotant	Transfert de données en cours		VERT et BLEU Clignotement alterné	Authentification en cours

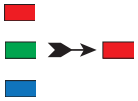
2. Statut de la LED

Remarque : Le fonctionnement normal du diskAshur M2 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.

Se remettre en marche depuis l'état d'inactivité

L'état d'inactivité est défini comme étant le moment où le diskAshur M² n'est pas utilisé et où toutes les LED sont éteintes.

Pour retirer le diskAshur M² de l'état de veille, procédez de la manière suivante.

Connectez le diskAhur M² à un port USB alimenté sur votre ordinateur		Les LED ROUGE, VERTE et BLEUE clignotent une fois de suite, puis la LED VERTE clignote deux fois et passe finalement à une LED ROUGE fixe indiquant que le disque est en état de veille

Pour être en état de veille

Pour forcer le diskAshur M² à entrer en état de veille, exécutez l'une des opérations suivantes :

- Débranchez le disque s'il est connecté à un port USB, toutes les LED s'éteignent (état de veille).

États de mise sous tension

Lorsque le disque se ranime à partir de l'état inactif, il se mettra dans l'un des états suivants indiqués dans le tableau ci-dessous.

État de mise sous tension	Indication LED	Clé 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 diskAshur M² est fourni dans « **l'État d'expédition initial** » **sans code PIN administrateur prédéfini**. Un code PIN administrateur de 7 à 15 chiffres doit être configuré avant que le disque puisse être utilisé. Lorsque le code PIN administrateur est configuré avec succès, il ne sera plus possible de remettre le disque dans l'état d'expédition initial.

Exigences relatives au code PIN :

- Doit comporter entre 7 et 15 chiffres
- Ne doit pas contenir uniquement des nombres répétitifs, par exemple (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)

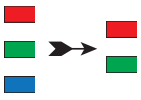
Mot de passe : Vous pouvez configurer un mot, un nom, une phrase ou toute autre combinaison de code PIN alphanumérique en appuyant simplement sur le bouton avec les lettres correspondantes.

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.

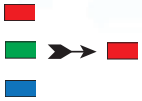
Pour configurer un code PIN administrateur et déverrouiller le diskAshur M² pour la première fois, suivez les étapes simples du tableau ci-dessous.

Instructions - Première utilisation	LED	Statut du LED
1. Connectez le diskAhur M² à un port USB alimenté sur votre ordinateur		Les LED ROUGE, VERTE et BLEUE clignotent une fois de suite puis la LED VERTE clignote deux fois et enfin passe à aux LED ROUGE et VERTE fixes indiquant que le disque est dans l'état d'expédition initial
2. Appuyez et maintenez enfoncés les deux boutons **CLÉ (🔑) + 1**		Les LED deviennent VERT clignotant et BLEU fixe
3. Saisissez un **nouveau code PIN administrateur** (7-15 chiffres) et appuyez sur la **CLÉ (🔑)** une seule fois		Les LED passeront du VERT clignotant au BLEU fixe pour revenir à une seule LED VERTE clignotante puis de retour VERT clignotant puis BLEU fixe
4. Ressaisissez ce **nouveau code PIN administrateur** et appuyez sur la **CLÉ (🔑)** de nouveau		La LED BLEUE clignote rapidement, puis passe à une LED BLEUE fixe et enfin à une LED VERTE fixe indiquant que le code PIN administrateur a été configuré avec succès et que le disque est déverrouillé.

Verrouillage du diskAshur M²
Pour verrouiller le disque, éjectez le diskAshur M² de votre ordinateur en toute sécurité, puis débranchez-le du port USB. Si des données sont en cours d'écriture sur le disque, la déconnexion du diskAshur M² entraînera un transfert de données incomplet et une éventuelle corruption des données.

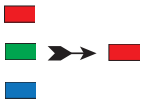
4. Déverrouillage du diskAshur M2 avec le code PIN de l'administrateur

Pour déverrouiller le diskAshur M² avec le code PIN de l'administrateur, veuillez suivre les étapes simples du tableau ci-dessous.

1. Connectez le diskAshur M² à un port USB sur votre ordinateur		Les LED ROUGE, VERTE et BLEUE clignotent une fois de suite puis la LED VERTE clignote deux fois et enfin passe à une LED ROUGE fixe indiquant que le disque est en état de veille
2. En état de veille (LED ROUGE fixe), appuyez sur la touche **CLÉ (🔑)** une seule fois		Les LED VERTE et BLEUE clignotent ensemble
3. Lorsque les LED VERTE et BLEUE clignotent ensemble, entrez le code **PIN administrateur** et appuyez à nouveau sur la **CLÉ (🔑)**		Les LED VERTE et BLEUE clignotent alternativement plusieurs fois, puis une LED BLEUE fixe et en passant à une LED VERTE fixe indiquant que le disque a été déb-loqué avec succès en tant qu'administrateur

5. Comment accéder au mode administrateur

Pour entrer en mode administrateur, procédez comme suit.

1. Connectez le diskAshur M² à un port USB sur votre ordinateur		Les LED ROUGE, VERTE et BLEUE clignotent une fois de suite puis la LED VERTE clignote deux fois et enfin passe à une LED ROUGE fixe indiquant que le disque est en état de veille
2. En état de veille (LED ROUGE fixe) appuyez et maintenez la **CLÉ (🔑) + le bouton 1** enfoncés		Les LED VERTE et BLEUE clignotent ensemble
3. Saisissez le **code PIN administrateur** et appuyer sur la **CLÉ (🔑)** une seule fois		Les LED VERTE et BLEUE clignotent rapidement ensemble plusieurs fois, puis passent à une LED VERTE fixe et enfin à une LED BLEUE fixe indiquant que le disque est en mode administrateur.

Pour sortir du mode administrateur

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

6. Changer le code PIN administrateur

Exigences relatives au code PIN :

- Doit comporter entre 7 et 15 chiffres
- Ne doit pas contenir uniquement des nombres répétitifs, par exemple (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)

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 **CLÉ (🔑) + 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 **CLÉ (🔑)** 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 **CLÉ (🔑)** 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 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

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 7 à 15 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 7 à 15 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 7 à 15 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 7 à 15 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 **CLÉ (🔑) + 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 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

8. Comment supprimer la politique sur le 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 **CLÉ (🔑) + 7** enfoncés		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Saisissez 070 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 **CLÉ (🔑)** 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. Ajout d'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 7 et 15 chiffres
- Ne doit pas contenir uniquement des nombres répétitifs, par exemple (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 **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 touches **CLÉ (🔑) + 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 **CLÉ (🔑)**		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 **CLÉ (🔑)**		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 **CLÉ (🔑) + 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 **CLÉ (🔑)** 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 **CLÉ (🔑)** 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

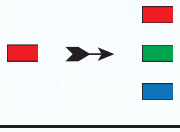
Pour supprimer un **code PIN utilisateur** existant, veuillez vous assurer d'être en « **mode administrateur** » comme décrit sous section 5. Lorsque le disque est en **mode administrateur** (LED BLEUE fixe) procédez aux étapes suivantes.

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

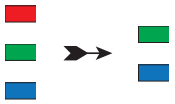
13. Comment déverrouiller le diskAshur M² avec le code PIN utilisateur

Pour déverrouiller le diskAshur M² avec le **code PIN utilisateur**, procédez comme suit.

1. En état de veille (LED ROUGE fixe) Appuyez et maintenez les deux touches **MAJ** (⬆) **+ CLÉ (🔑)** 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 **CLÉ (🔑)** une seule fois		Les LED clignotantes ROUGE, VERTE & BLEUE passent en alternance à des LED VERTE et BLEUE puis à une LED VERTE fixe indiquant que le disque est déverrouillé avec succès en mode utilisateur

14. Modification du code PIN utilisateur en mode utilisateur

Pour changer le code **PIN utilisateur**, déverrouillez en premier lieu le diskAshur M² avec le code PIN 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 (LED VERTE), appuyez et maintenez les touches **CLÉ (🔑) + 4** enfoncées		La LED VERTE fixe passe aux LED, ROUGE, VERTE et BLEUE qui s'allument et s'éteignent en alternance
2. Saisissez votre **code PIN utilisateur** existant et appuyez sur la **CLÉ (🔑)** une seule fois		Les LED VERTE et BLEUE s'allument et s'éteignent en alternance, puis passent à un seul clignotement de LED VERTE, puis reviennent à un clignotement de LED VERTE et BLEUE fixe
3. Saisissez un **nouveau code PIN utilisateur** et appuyez sur la **CLÉ (🔑)** 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
4. Ressaisissez ce **nouveau code PIN utilisateur** et appuyez sur la **CLÉ (🔑)** une seule fois		Les LED VERTE clignotante et BLEUE fixe passent à une LED VERTE clignotant rapidement, puis à une LED VERTE fixe indiquant que le code PIN de l'utilisateur a été modifié avec succès

Important : Le changement du code PIN utilisateur (LED VERTE) doit être conforme à la « Politique relative au 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.

15. Création d'un code PIN utilisateur de récuperation à usage unique

Le code PIN de récuperation à usage unique est extrêmement utile dans les situations où un utilisateur a oublié son code PIN pour déverrouiller le diskAshur M².
Pour activer le mode de récupération, l'utilisateur doit d'abord entrer le bon code PIN de récupération unique, si celui-ci a été configuré. Le processus de récupération du code PIN de l'utilisateur n'a aucune incidence sur les données, la clé de chiffrement et le code PIN de l'administrateur, mais l'utilisateur est obligé de configurer un nouveau code PIN utilisateur de 7 à 15 chiffres.

Pour configurer un code PIN utilisateur de récuperation à usage unique de 7 à 15 chiffres, 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 étap es suivantes.

1. En mode administrateur, appuyez et maintenez les touches **CLÉ (🔑) + 4** enfoncées		La LED BLEUE fixe se transforme en LED VERTE clignotante et BLEUE fixe
2. Saisissez le code **PIN de récupération** à usage unique et appuyez sur la **CLÉ (🔑)**		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 de récupération** à usage unique et appuyez sur la **CLÉ (🔑)** de nouveau		Les LED VERTE clignotante et BLEUE fixe passent à une LED VERTE clignotant rapidement et enfin à une LED BLEUE fixe indiquant que le code PIN unique de récupération 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

16. Suppression d'un code PIN utilisateur de récupération à usage unique

Pour supprimer le code PIN utilisateur de récupération à usage unique, 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** (⬆) **+ 4** enfoncées		La LED BLEUE fixe va passer à une LED ROUGE clignotant
2. Appuyez et maintenez enfoncées les touches **MAJ** (⬆) **+ 4** de nouveau		La LED ROUGE clignotante se transforme en LED ROUGE fixe et passe ensuite à une LED BLEUE fixe, indiquant que le code PIN unique de récupération 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

17. Activation du mode de récupération et création d'un nouveau code PIN utilisateur

Le code PIN utilisateur de récupération à usage unique est extrêmement utile dans les situations où un utilisateur a oublié son code PIN pour déverrouiller le diskAshur M².
Pour activer le mode de récupération, l'utilisateur doit d'abord entrer le bon code PIN de récupération à usage unique, si celui-ci a été configuré. Le processus de récupération du code PIN de l'utilisateur n'a aucune incidence sur les données, la clé de chiffrement et le code PIN de l'administrateur, mais l'utilisateur est obligé de configurer un nouveau PIN utilisateur de 7 à 15 chiffres.

Pour activer le processus de récupération et configurer un nouveau code PIN utilisateur, procédez de la manière suivante.

1. En mode veille (LED ROUGE) pressez et maintenez les touches **CLÉ (⚷) + chiffre 4** enfoncées		La LED ROUGE fixe se transforme en LED ROUGE et VERTE clignotante
2. Saisissez le code **PIN** de récupération à usage unique et appuyez sur la touche **CLÉ (⚷)**		Les LED VERTE et BLEUE s'allument et s'éteignent alternativement, puis passent à une LED VERTE fixe et enfin à des LED VERTE et BLEUE clignotantes.
3. Saisissez un **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (⚷)**		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. Ressaisissez ce **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (⚷)** de nouveau		La LED VERTE clignote rapidement puis devient VERTE fixe, indiquant que le processus de récupération a réussi et qu'un nouveau code PIN utilisateur a été configuré

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

18. Définir le mode lecture seule pour un utilisateur en mode administrateur

Avec autant de virus et de chevaux de Troie infectant les disques USB, la fonction en lecture seule est particulièrement utile si vous avez besoin d'accéder aux données sur le disque lorsqu'elle est utilisée dans un environnement public. C'est également une caractéristique essentielle à des fins judiciaires, où les données doivent être conservées dans leur état original et inchangé qui ne peut être modifié ou écrasé.

Lorsque l'administrateur configure le diskAshur M² et restreint l'accès de l'utilisateur à la lecture seule, alors seul l'administrateur peut écrire sur le disque ou modifier le réglage en lecture/écriture tel que cela est décrit dans la section 19. L'utilisateur est limité à l'accès en lecture seule et ne peut pas écrire sur le disque ou modifier ce paramètre en mode utilisateur.

Pour configurer le diskAshur M² et restreindre l'accès de l'utilisateur à la lecture seule, veuillez vous assurer d'être en « **mode administrateur** » tel que cela est décrit à la section 5. Lorsque le disque en **mode administrateur** (LED BLEUE fixe) procédez aux 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 **CLÉ (⚷)**		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

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

Pour configurer le diskAshur M² en mode lecture/écriture pour l'utilisateur en tant qu'administrateur, veuillez vous assurer d'être en « **mode administrateur** » tel que cela est décrit à la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE fixe), procédez aux étapes suivantes.

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 **CLÉ (🔑)**		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

20. Définir le mode lecture seule en mode administrateur

Lorsque l'administrateur configure le diskAshur M² et le limite en lecture seule de manière générale, ni l'administrateur ni l'utilisateur ne peuvent écrire sur le disque et tous deux sont limités à l'accès en lecture seule. Seul l'administrateur est en mesure de rétablir la configuration en lecture/écriture comme décrit dans la section 21.

Pour configurer le diskAshur M² et restreindre l'accès à la lecture seule, veuillez vous assurer d'être en « **mode administrateur** » tel que cela est 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 « **5+ 6** » enfoncés.		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **CLÉ (🔑)**		Les LED VERTE et BLEUE passeront en LED VERT fixe et ensuite à une LED BLEUE fixe indiquant que le disque a été configuré et que l'accès est limité à la fonction lecture uniquement

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 de manière générale en mode administrateur

Pour rétablir le diskAshur M² en lecture/écriture à partir du paramètre de lecture seule, veuillez vous assurer d'être en « **mode administrateur** » tel que cela est 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 « **5+ 9** » enfoncés.		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **CLÉ (🔑)**		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. Instructions pour configurer un code PIN d'autodestruction

Vous pouvez configurer un code PIN d'autodestruction qui, lorsqu'il est saisi, effectue un Crypto-Erase sur le disque (la clé de chiffrement est supprimée). Ce processus supprime tous les codes PIN configurés et rend toutes les données stockées sur le disque inaccessibles (perdues pour toujours), le disque se présentera ensuite comme déverrouillé avec une LED VERTE. En exécutant cette fonction, le code PIN autodestructeur 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 **CLÉS (🔑) + 6**		La LED BLEUE fixe se transforme en LED VERTE clignotante et BLEUE fixe
2. Configurez et entrez un **code PIN d'autodestruction** de 7 à 15 chiffres et appuyez sur la touche **CLÉ (🔑)**		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 **CLÉ (🔑)** 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

23. 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

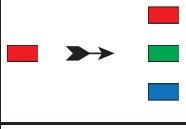
Remarque : Pour quitter immédiatement le **mode administrateur** (LED BLEUE fixe), appuyez sur le bouton **MAJ** (⬆) et maintenez-le enfoncé pendant une seconde - la LED BLEUE fixe passe à une LED ROUGE fixe

24. Comment déverrouiller le disque avec le code PIN d'autodestruction

Avertissement : 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**. Il n'existe plus de code PIN administrateur après l'activation du mécanisme d'autodestruction. Le diskAshur M² doit premièrement être réinitialisé (voir « Comment effectuer une réinitialisation complète », section 35, page 63) afin de configurer un code PIN administrateur avec tous les privilèges administrateur, y compris la possibilité de configurer un nouveau 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. L'activation de cette fonction fera du code **PIN d'autodestruction le nouveau code PIN utilisateur** et le diskAshur M² devra être formaté avant que de nouvelles données puissent être ajoutées au disque.

Pour activer le mécanisme d'auto-destruction, le disque doit être à l'état de veille (LED ROUGE fixe) et il est nécéssaire ensuite de procéder aux étapes suivantes.

1. En **mode veille** (LED ROUGE fixe), Appuyez et maintenez enfoncées les touches **MAJ** (⬆) + **CLÉ (⚷)**		La LED ROUGE s'allume et s'éteint, les LED ROUGE, VERTE & BLEUE clignotent
2. Saisissez le code **PIN** d'autodestruction et appuyez sur la **CLÉ (⚷)**		Les LED ROUGE, VERTE & BLEUE clignotantes se transforment en LED VERTE & BLEUE qui s'allument et s'éteignent alternativement pendant quelques secondes, puis passent finalement à une LED VERTE fixe indiquant que le diskAshur M² s'est autodétruit avec succès

25. 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 diskAshur M² 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 7 et 15 chiffres
- Ne doit pas contenir uniquement des nombres répétitifs, par exemple (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)

Si le diskAshur M² 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 **CLÉ (🔑)**		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 **CLÉ (🔑)** 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

26. Réglage du verrouillage automatique

Pour se protéger contre un accès non autorisé si le disque est déverrouillé et sans surveillance, le diskAshur M² peut être configuré pour se verrouiller. Dans son état par défaut, le verrouillage automatique du diskAshur M² 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 **CLÉS (🔑) + 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

27. 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 **CLÉ (🔑) + 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

28. 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 **CLÉ (🔑)** 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

29. Activer la fonction lecture seule en mode utilisateur

Pour configurer le diskAshur M² 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 BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la TOUCHE **(🔑)**		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.

30. Activer la lecture/écriture en mode utilisateur

Pour configurer le diskAshur M², 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 BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **TOUCHE** (☝)		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.

31. Protection contre les attaques par force brute

Le diskAshur M² intègre un mécanisme de défense pour protéger le disque contre les attaques par force brute. Par défaut, les valeurs de l'état d'expédition initial pour la limite d'attaque par force brute (nombre de saisies incorrectes consécutives du code PIN) pour le code PIN administrateur et le code PIN utilisateur sont fixées à 10 et 5 pour le code PIN de récupération. Trois compteurs indépendants de force brute sont utilisés pour enregistrer le nombre de tentatives incorrectes pour chaque autorisation de code PIN (administrateur, utilisateur et récupération) comme indiqué ci-dessous.

- Si un utilisateur saisit un **code PIN utilisateur incorrect** 10 fois de suite, 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 utilisateur saisit un **code PIN de récupération incorrect** 5 fois de suite, le code PIN de récupération est supprimé mais les données et le code PIN administrateur restent intacts et accessibles.
- Si un **code PIN administrateur incorrect** est saisi 10 fois de suite, le disque sera réinitialisé. Tous les codes PIN et les données sont supprimés et perdus définitivement.

Le tableau ci-dessous suppose que les trois codes PIN ont été configurés et met en évidence l'effet de déclenchement du mécanisme de défense par force brute de chaque code PIN.

Code PIN utilisé pour déverrouiller le disque	Saisies PIN incorrectes consécutives	Description de ce qui se passe
Code PIN utilisateur	10	• Le code PIN utilisateur est supprimé. • Le code PIN de récupération, le code PIN administrateur et toutes les données demeurent intacts et accessibles.
Code PIN de récupération	5	• Le code PIN de récupération est supprimé. • Le code PIN administrateur et toutes les données demeurent intacts et accessibles.
Code PIN administrateur	10	• Le diskAshur M² sera réinitialisé, tous les codes PIN et les données sont supprimés et perdus définitivement.

Remarque : La limitation de la force brute est fixée par défaut aux valeurs initiales de l'état d'expédition lorsque le disque est complètement réinitialisé,ou lorsque la fonction d'autodestruction est activée ou lorsque le mécanisme de défense contre attaque par force brute est déclenché. Dans le cas où l'administrateur modifie le code PIN de l'utilisateur, ou si un nouveau code PIN est défini lors de l'activation de la fonction de récupération, le compteur de force brute du code PIN de l'utilisateur est mis à zéro (0), cependant la limitation de la force brute n'est pas affectée. Si l'administrateur modifie le code PIN de récupération, le compteur de force brute du code PIN de récupération est réinitialisé.

L'autorisation réussie d'un certain code PIN mettra à zéro le compteur de force brute pour ce code PIN particulier, mais n'affectera pas le compteur de force brute des autres codes PIN. L'autorisation échouée d'un certain code PIN augmentera le compteur de force brute pour ce code PIN particulier, mais n'affectera pas le compteur de force brute des autres codes PIN.

32. Mécanisme de défense contre le piratage du code PIN Administrateur

Le code PIN Administrateur du diskAshur M² est équipé d'un mécanisme de défense plus sophistiqué que le code PIN utilisateur ou de récupération. Cela permet de le protéger contre la saisie accidentelle d'un code PIN Administrateur invalide 10 fois consécutives, suite à quoi, toutes vos données seraient perdues. Par conséquent, après 5 saisies d'un code PIN Administrateur invalide, le diskAshur M² se verrouillera, et tous les voyants resteront allumés.

ATTENTION : ne suivez pas les instructions suivantes si vous déverrouillez votre diskAshur M² à l'aide du **« CODE PIN UTILISATEUR »** uniquement, et que vous ne connaissez pas le **« CODE PIN ADMINISTRATEUR »**.

Référez-vous aux instructions dans le tableau ci-dessous, pour découvrir comment vous permettre de disposer d'un maximum de 10 saisies de code PIN Administrateur.

Saisies consécutives de codes PIN Administrateur invalides	Description de ce qui arrive au diskAshur M²	Instructions
5	Toutes les LED, **ROUGE**, **VERTE** & **BLEUE** s'allument et restent allumées.	Saisissez le code PIN suivant **« 47867243 »** puis appuyez sur **(key)** une fois. Les LED **VERTE** et **BLEUE** clignotent chacune leur tour, le diskAshur M2 est alors prêt à accepter **3 nouveaux essais de code PIN Administrateur**.
8	Toutes les LED, **ROUGE**, **VERTE** & **BLEUE** clignotent chacune leur tour.	Saisissez le code PIN suivant **«47867243 »** puis appuyez sur **(key)** une fois. Les LED **VERTE** et **BLEUE** clignotent chacune leur tour, le diskAshur M2 est alors prêt à accepter **2 nouveaux essais de code PIN Administrateur**.
10	La LED **ROUGE** s'allume et reste allumée.	Après un total de 10 saisies de code PIN administrateur invalide, la clé de chiffrement, tous les codes PIN ainsi que les données seront supprimés et définitivement perdus.

33. Comment définir la limitation de la force brute pour le code PIN de l'utilisateur

Remarque : Le paramètre de limitation de la force brute du code PIN de l'utilisateur est fixé par défaut à 10 entrées consécutives de code PIN incorrect lorsque le disque est soit complètement réinitialisé, soit le mécanisme de défense contre attaque par force brute est déclenché ou que le code PIN d'autodestruction est activé.

La limitation de la force brute pour le code PIN utilisateur du diskAshur M² peut être reprogrammée et définie par l'administrateur. Cette fonction peut être configurée pour autoriser de 1 à 10 tentatives consécutives d'entrée de code PIN incorrect.

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

1. En mode administrateur, appuyez et maintenez les deux touches **7 + 0** enfoncées		La LED BLEUE fixe se transforme en deux LED VERTE et BLEUE clignotant ensemble
2. Saisissez le nombre de tentatives pour la limitation de la force brute (entre 01-10), par exemple saisissez : • **01** pour 1 tentative • **10** pour 10 tentatives		
3. Appuyez une fois sur la touche (⬆) **MAJ**		Les LED VERTE et BLEUE clignotantes passent à une LED VERTE fixe pendant une seconde, puis à une LED BLEUE fixe indiquant que la limitation de la 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

34. Comment vérifier la limitation de la force brute pour le code PIN de l'utilisateur

L'administrateur est en mesure d'observer et de déterminer le nombre de fois consécutives où un code PIN utilisateur incorrect est autorisé à être saisi avant de déclencher le mécanisme de défense contre attaque par force brute en notant simplement la séquence de LED comme décrit ci-dessous.

Pour vérifier le réglage de la limitation de la force brute, 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 touches **2** + **0** enfoncées		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur la **CLÉ (🔑)** 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 le disque sur la force brute après **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

35. Comment effectuer une réinitialisation complète

Pour effectuer une réinitialisation complète, le diskAshur M² 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 diskAshur M², 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 25 page 57 sur Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation, le diskAshur M² devra également être formaté avant que de nouvelles données puissent être ajoutées au disque.

36. Comment configurer le diskAshur M² comme bootable

Remarque : Lorsque le disque est configuré comme bootable, l'éjection du disque du système d'exploitation ne forcera pas la LED à devenir ROUGE. Le disque reste bien VERT et doit être débranché pour la prochaine utilisation. Le réglage par défaut du diskAshur M² est configuré comme non bootable.

Le diskAshur M² est équipé d'une fonction bootable qui permet d'adapter le cycle d'alimentation pendant le processus de démarrage de l'hôte. Lorsque vous démarrez à partir du diskAshur M², vous utilisez votre ordinateur avec le système d'exploitation qui est installé sur le diskAshur M².

Pour définir le disque comme bootable, 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 enfoncées les touches CLÉ (🔑) **+ 8**		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur le « **0** » suivi de « **1** » (**01**)		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 le disque a été configuré avec succès comme bootable

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

37. Comment désactiver la fonction bootable du diskAshur M²

Pour désactiver la fonction bootable du diskAshur M², veuillez vous assurer d'être en « **mode administrateur** » tel que cela est 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 **CLÉ (⚷) + 8** enfoncées		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante
2. Appuyez sur le « **0** » suivi de « **0** » (**00**)		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 fonction bootable 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

38. Comment vérifier le paramètre bootable

Pour vérifier le paramètre bootable, 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 la touche **MAJ** (⬆) **+ 8** enfoncées		La LED BLEUE fixe se transforme en LED VERTE et BLEUE clignotante

2. Appuyez sur la **CLÉ (⚷)** et l'un des deux scénarios suivants se produira ;

- **Si diskAshur M² est configuré comme étant bootable, voici ce qui se passe ;**

a. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde.
b. La LED VERTE clignote une fois.
c. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde.
d. Les LED redeviennent BLEU fixe

- **Si diskAshur M² n'est PAS configuré comme étant bootable, voici ce qui se passe ;**

a. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde.
b. Toutes les LED sont éteintes
c. Toutes les LED (ROUGE, VERTE & BLEUE) deviennent fixes pour 1 seconde.
d. Les LED redeviennent BLEU fixe

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

39. Initialisation et formatage du diskAshur M² pour Windows

Après une attaque par force brute ou une réinitialisation complète, le diskAshur M² supprime tous les code PIN, les données et la clé de chiffrement. Vous devrez initialiser et formater le diskAshur M² avant qu'il ne puisse être utilisé.

Pour formater votre diskAshur M², procédez comme suit :

1. Configurez un nouveau code PIN administrateur - voir page 57, section 25, « Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation ».

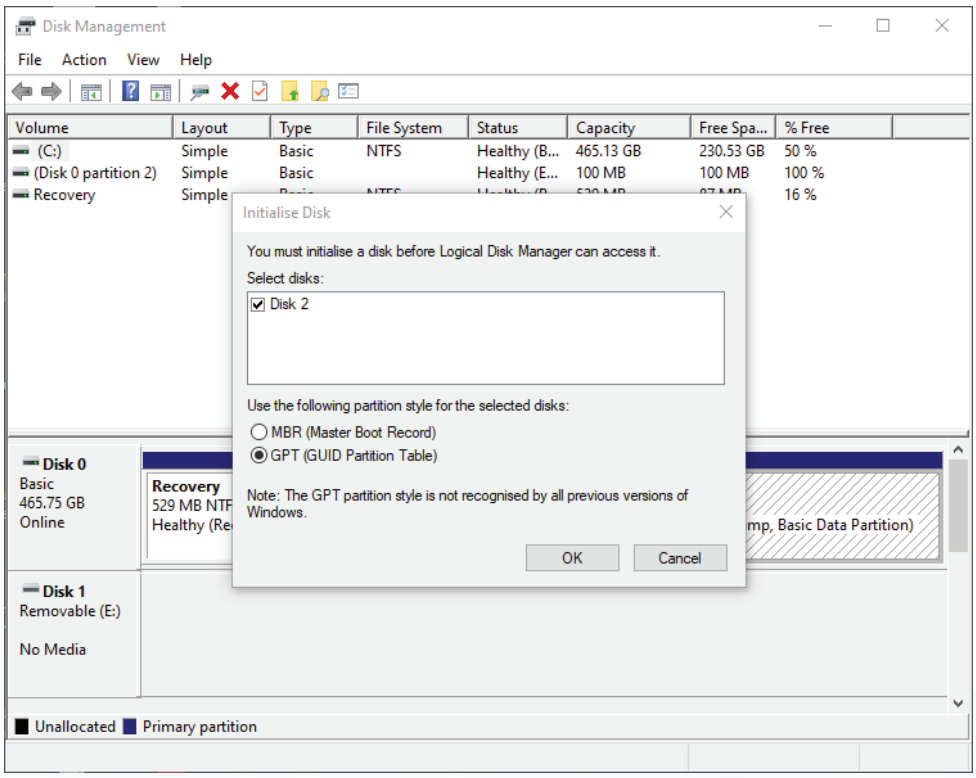
2. Lorsque le diskAshur M² est en veille (LED ROUGE), appuyez une fois sur la CLÉ **(ȣ)** et saisissez le nouveau code PIN administrateur pour le déverrouiller (LED VERTE clignotante).

3. Connectez le diskAshur M² à l'ordinateur.

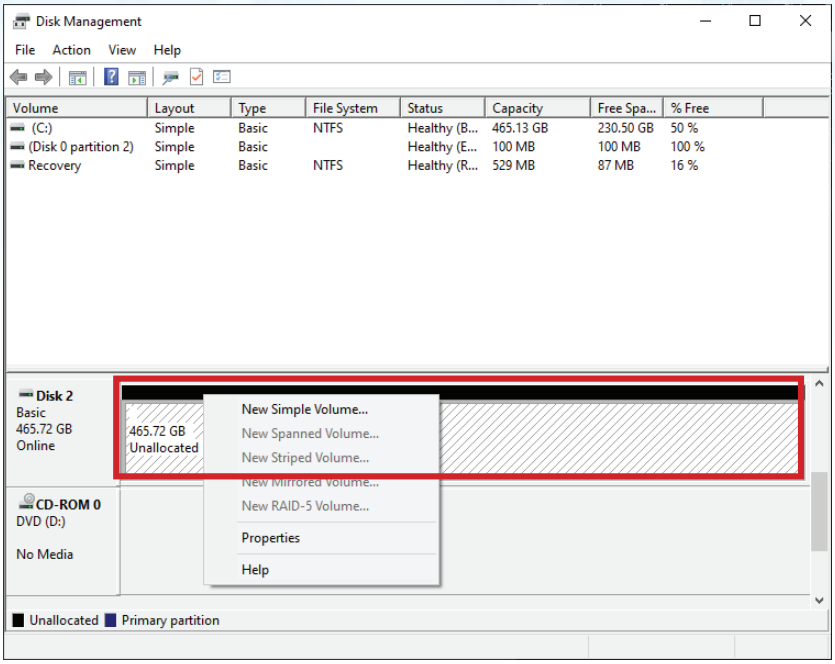
4. **Windows 7 :** Cliquez avec le bouton droit de la souris sur **Ordinateur**, puis cliquez sur **Gérer** et sélectionnez ensuite **Gestion des disques**
   Windows 8 : Cliquez avec le bouton droit de la souris dans le coin gauche du bureau et sélectionnez **Gestion des disques**
   Windows 10 : Cliquez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

5. Dans la fenêtre de gestion des disques, le diskAshur M² est reconnu comme un périphérique inconnu, non initialisé et non alloué. Une boîte de message devrait apparaître pour que vous puissiez choisir entre le style de partition MBR et GPT. GPT stocke plusieurs duplications 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 en un seul endroit.

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



6. Cliquez avec le bouton droit de la souris dans la zone vide sur la section **Non allouée**, puis sélectionnez **Nouveau volume simple.**



7. La fenêtre de bienvenue de l'assistant Nouveau volume simple s'ouvre. Cliquez sur suivant.



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

9. Attribuez une lettre de disque ou un chemin d'accès et cliquez sur **Suivant**.

10. Créez un label de volume, sélectionnez Effectuer un formatage rapide, puis cliquez sur **Suivant**.

11. Cliquez sur **Terminer**.

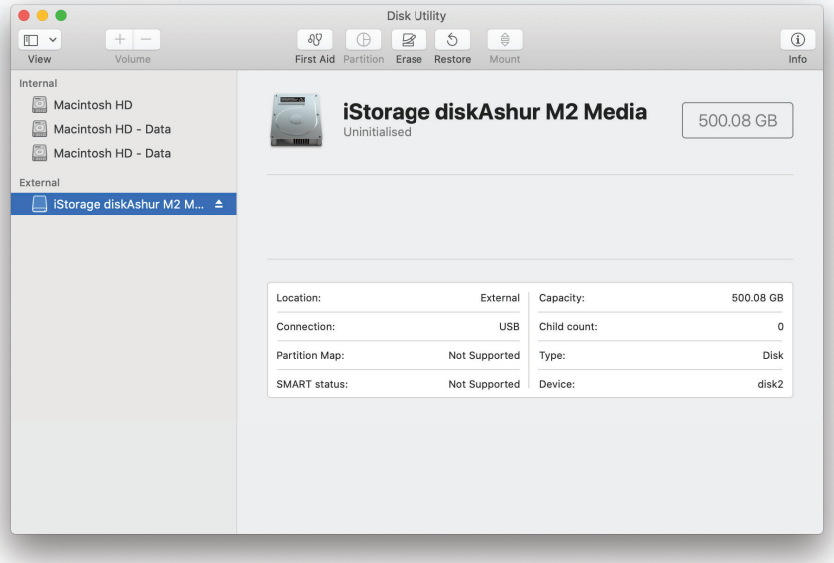
12. Attendez que le processus de formatage soit terminé. Le diskAshur M² sera reconnu et pourra être utilisé.

40. Initialisation et formatage du diskAshur M² sous Mac OS

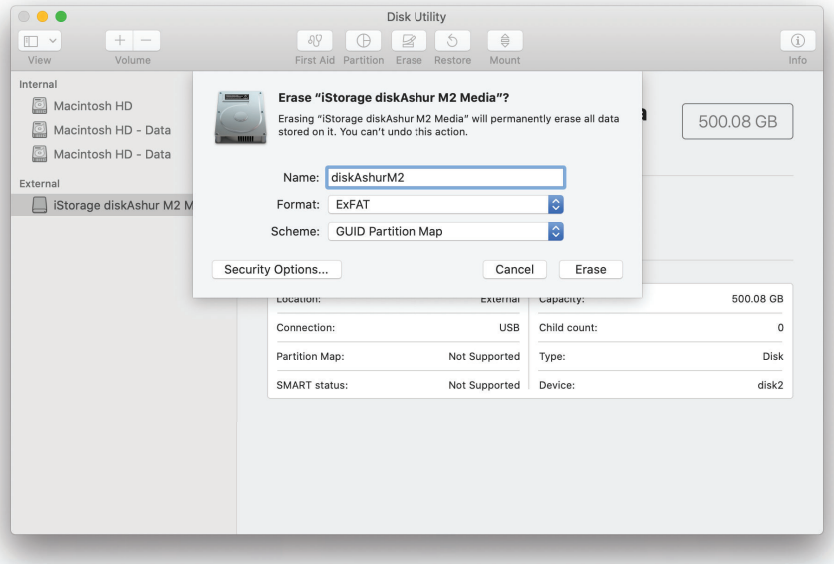
Après une attaque par force brute ou une réinitialisation complète, le diskAshur M² supprime tous les codes PIN, les données et la clé de chiffrement. Vous devrez initialiser et formater le diskAshur M² avant qu'il ne puisse être utilisé.

Pour initialiser et formater le diskAshur M² :

1. Sélectionnez diskAshur M² dans la liste des disques et des volumes. Chaque disque de la liste affichera sa capacité, son fabricant et le nom du produit, par exemple « **iStorage diskAshur M² Media** ».



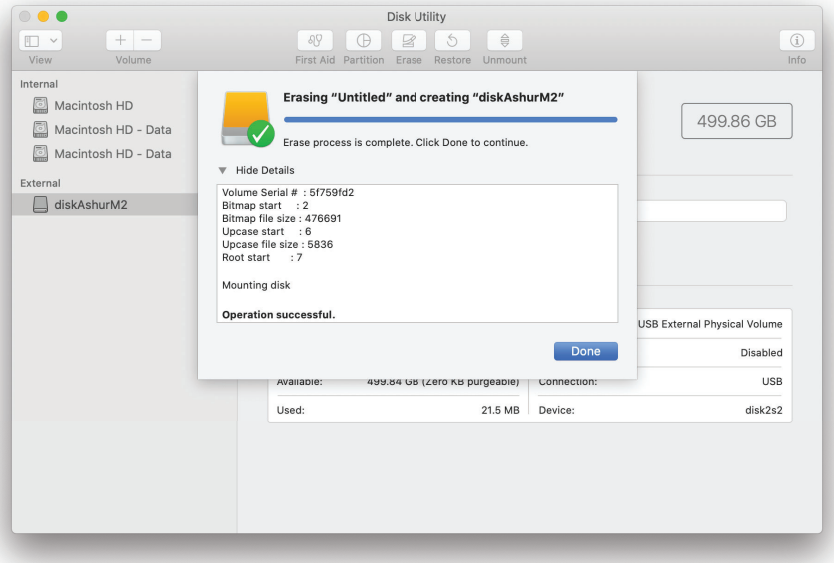
2. Cliquez sur le bouton « **Effacer** » sous Utilitaire de disque.
3. Saisissez un nom pour le disque. Le nom par défaut est Untitled. Le nom du disque apparaîtra éventuellement sur le bureau.



4. Sélectionnez un schéma et un format de volume à utiliser. Le menu déroulant Format de volume énumère les formats de disque disponibles que le Mac prend en charge. Le type de format recommandé est « Mac OS Extended (Journaled) ». Pour une utilisation multiplateforme, utilisez exFAT. Le menu déroulant « Scheme format » énumère les schémas disponibles à utiliser. Nous recommandons l'utilisation de « GUID Partition Map » pour les disques de plus de 2 To.

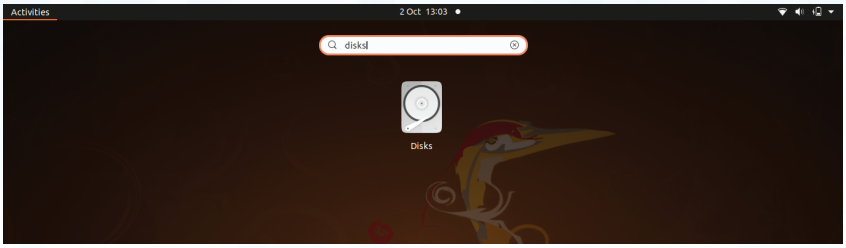


5. Cliquez sur le bouton « Effacer ». Disk Utility démontera le volume du bureau, l'effacera, puis le remontera sur le bureau.

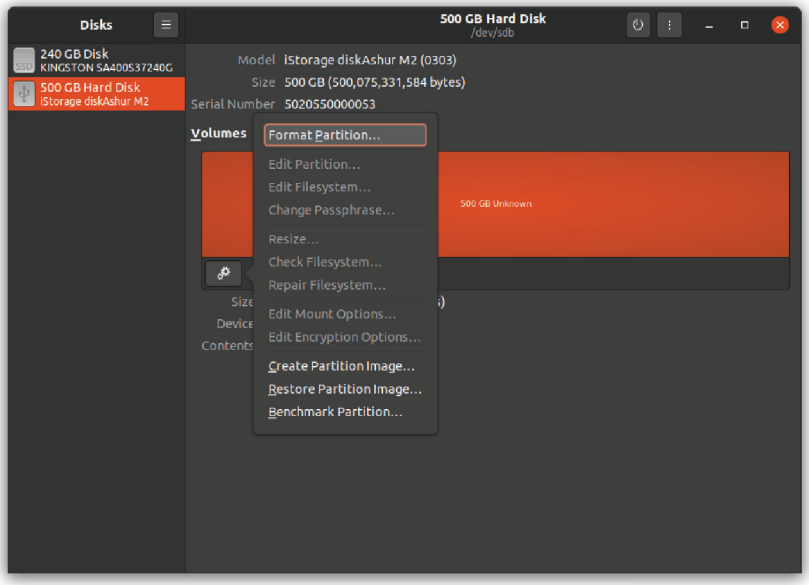


41. Initialisation et formatage du diskAshur M² sous Linux

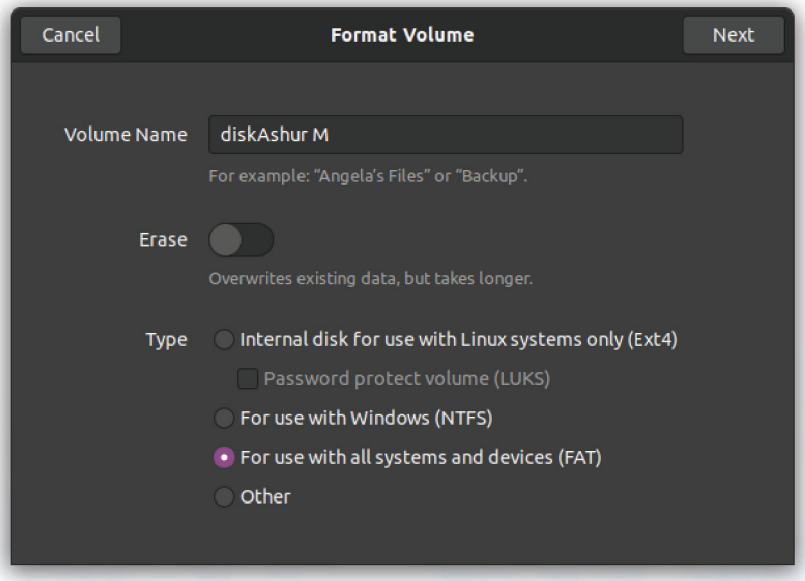
1. Ouvrez « **Afficher l'application** » et tapez « **Disques** » dans la boîte de recherche. Cliquez sur l'utilitaire « **Disques** » lorsqu'il s'affiche.



2. Cliquez pour sélectionner le disque (disque dur de 500 Go) sous « **Dispositifs** ». Ensuite, cliquez sur l'icône 'gestionnaire de périphériques' sous « **Volumes** », puis cliquez sur « **Format Partition** ».

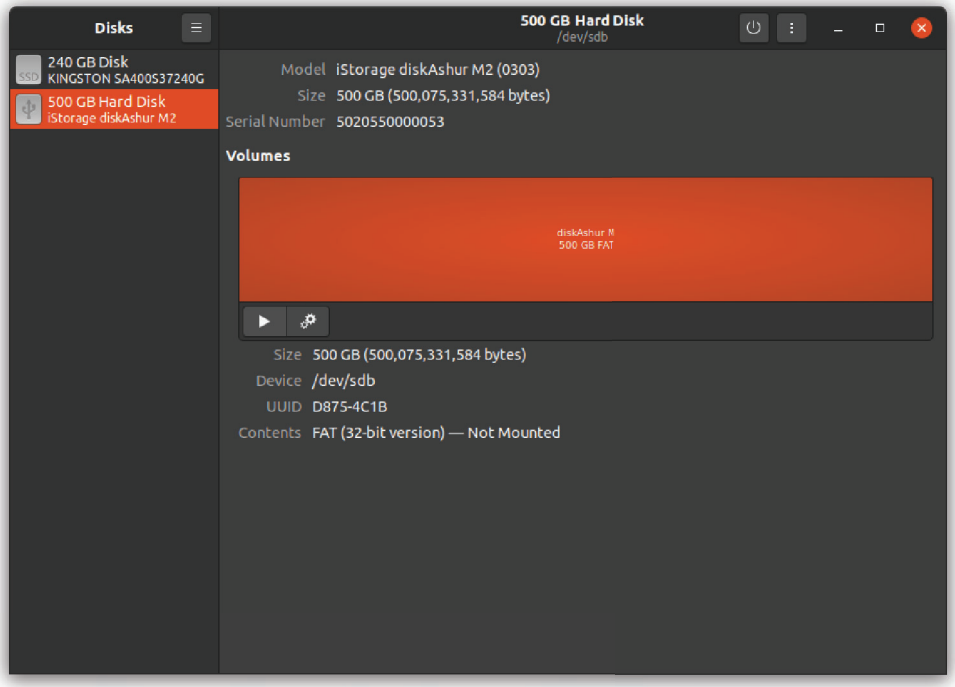


3. Sélectionnez « **Compatible avec tous les systèmes et périphériques (FAT)** » pour l'option « Type ». Et saisissez un nom pour le disque, par exemple : diskAshur M². Ensuite, cliquez sur le bouton « **Format** ».

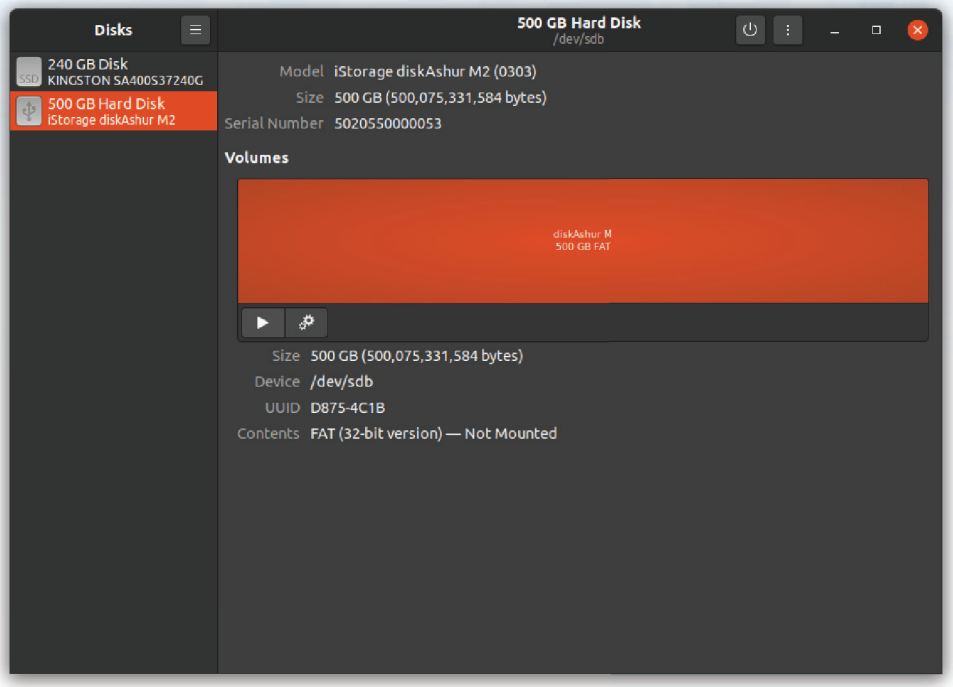




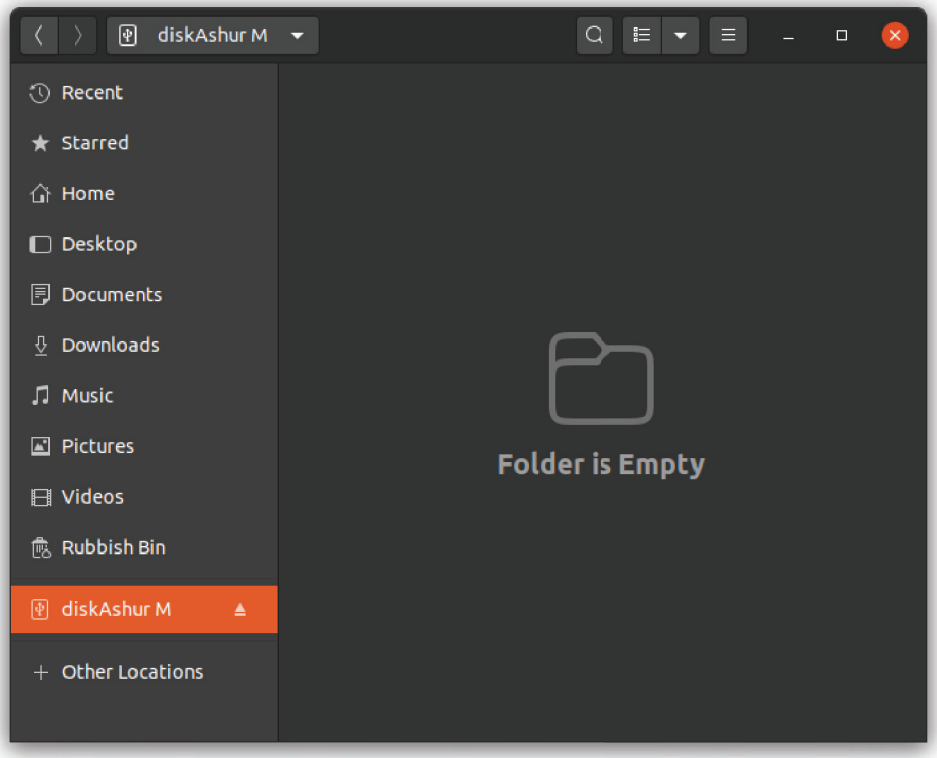
4. Lorsque le processus de formatage est terminé, cliquez sur le bouton Lecture pour monter le disque sur Ubuntu.



5. Le disque doit maintenant être monté sur Ubuntu et prêt à l'emploi.



6. Le disque sera montré comme dans l'image ci-dessous. Vous pouvez cliquer sur l'icône du disque pour ouvrir votre disque.



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

Veillez à sauvegarder et à fermer tous les fichiers de votre diskAshur M² avant d'hiberner, de suspendre ou de vous déconnecter du système d'exploitation.

Il est recommandé de verrouiller le diskAshur M² manuellement avant de le mettre en veilleuse, de le suspendre ou de le déconnecter du système.

Pour verrouiller le disque, éjectez le diskAshur M² 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 diskAshur M² 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 diskAshur M² si vous n'êtes pas sur votre ordinateur.

43. 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 **CLÉ (🔑)** 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.

44. 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 **CLÉ (🔑)** 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.

45. 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.

46. 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

Copyright © iStorage Limited 2020. Tous droits réservés.
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

Benutzerhandbuch



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 diskAshur M² haben, kontaktieren Sie bitte unser Support-Team per E-Mail – support@istorage-uk.com oder telefonisch unter +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2020. Alle Rechte vorbehalten.

Windows ist ein eingetragenes Warenzeichen der Microsoft Corporation.
Alle anderen genannten Marken und Urheberrechte sind Eigentum ihrer jeweiligen Inhaber.

Die Verbreitung von modifizierten Versionen dieses Dokuments ist ohne ausdrückliche Genehmigung des Copyright-Inhabers verboten.

Die Verbreitung des Werkes oder davon abgeleiteter Werke in einer Standardbuchform (Papier) für kommerzielle Zwecke ist ohne vorherige Genehmigung des Urheberrechtsinhabers verboten.

DIE DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR ZUR VERFÜGUNG GESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH JEDER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK
ODER DER NICHT-VERLETZUNG VON RECHTEN, SIND AUSGESCHLOSSEN, ES SEI DENN, SOLCHE AUSSCHLÜSSE WERDEN FÜR RECHTLICH UNGÜLTIG ERKLÄRT

RoHS Compliant

REACH COMPLIANCE

Alle Warenzeichen und Markennamen sind Eigentum ihrer jeweiligen Inhaber

Konform mit dem Trade Agreements Act (TAA)

CITRIX® vmware®

Inhaltsverzeichnis

Einführung 79
Verpackungsinhalt 79
Aufbau des diskAshur M² 79
1. LEDs und ihre Zustände 80
2. LED-Zustände 80
3. Erste Verwendung 81
4. Freischalten des diskAshur M² mit der Admin-PIN 82
5. Wechseln in den Admin-Modus 82
6. Ändern der Admin-PIN 83
7. Festlegen einer Benutzer-PIN-Richtlinie 84
8. Löschen der Benutzer-PIN-Richtlinie 85
9. Überprüfen der Benutzer-PIN-Richtlinie 85
10. Hinzufügen einer neuen Benutzer-PIN im Admin-Modus 86
11. Ändern der Benutzer-PIN im Admin-Modus 87
12. Löschen der Benutzer-PIN im Admin-Modus 87
13. Freischalten des diskAshur M² mit der Benutzer-PIN 88
14. Ändern der Benutzer-PIN im Benutzermodus 88
15. Erstellen einer einmaligen Benutzer-Wiederherstellungs-PIN 89
16. Löschen einer einmaligen Benutzer-Wiederherstellungs-PIN 89
17. Aktivieren des Wiederherstellungsmodus und Erstellen einer neuen Benutzer-PIN 90
18. Benutzer auf Schreibschutz im Admin-Modus einstellen 90
19. Benutzer auf Lese-/Schreibzugriff im Admin-Modus einstellen 91
20. Globalen Schreibschutz im Admin-Modus einstellen 91
21. Globalen Lese-/Schreibzugriff im Admin-Modus einstellen 92
22. Konfigurieren einer Selbstzerstörungs-PIN 92
23. Löschen der Selbstzerstörungs-PIN 93
24. Freischalten mit der Selbstzerstörungs-PIN 93
25. Erstellen einer Admin-PIN nach einem Brute-Force-Angriff oder nach dem Zurücksetzen 94
26. Einstellen der automatischen Sperre bei Abwesenheit 94
27. Deaktivieren der automatischen Sperre bei Abwesenheit 95
28. Überprüfen der automatischen Sperre bei Abwesenheit 96
29. Schreibschutz im Benutzermodus einstellen 96
30. Lese-/Schreibzugriff im Benutzermodus einstellen 97
31. Schutzmechanismus gegen Brute-Force-Hacking 97
32. Admin-PIN-Mechanismus zur Abwehr von Brute-Force-Hacker-Angriffen 98
33. Einstellen der Brute-Force-Begrenzung für die Benutzer-PIN 98
34. Überprüfen der Brute-Force-Begrenzung für die Benutzer-PIN 99
35. Vollständiges Zurücksetzen des Geräts 100
36. DiskAshur M² als bootfähiges Laufwerk konfigurieren 100
37. Bootfunktion des diskAshur M² deaktivieren 101
38. Bootfähigkeits-Einstellung überprüfen 101
39. Initialisieren und Formatieren des diskAshur M² für Windows 102
40. Initialisieren und Formatieren des diskAshur M² für Mac OS 104
41. Initialisieren und Formatieren des diskAshur M² für Linux 106
42. In den Ruhezustand versetzen, anhalten oder vom Betriebssystem abmelden 109
43. Überprüfen der Firmware im Admin-Modus 109
44. Überprüfen der Firmware im Benutzermodus 110
45. Technische Unterstützung 111
46. Garantie- und RMA-Informationen 111

Einführung

Vielen Dank, dass Sie sich für den neuen iStorage diskAshur M² entschieden haben, ein hochsicherer und einfach zu bedienender, hardwareverschlüsselter tragbarer Solid State Drive (SSD) mit PIN-Authentifizierung und Kapazitäten von 120 GB bis zu 2 TB und mehr.

Der diskAshur M² ist zertifiziert nach FIPS 140-3 Level 3, und verschlüsselt Daten während der Übertragung und im Ruhezustand mit AES-XTS 256-Bit Hardware-Vollverschlüsselung des gesamten Laufwerks.

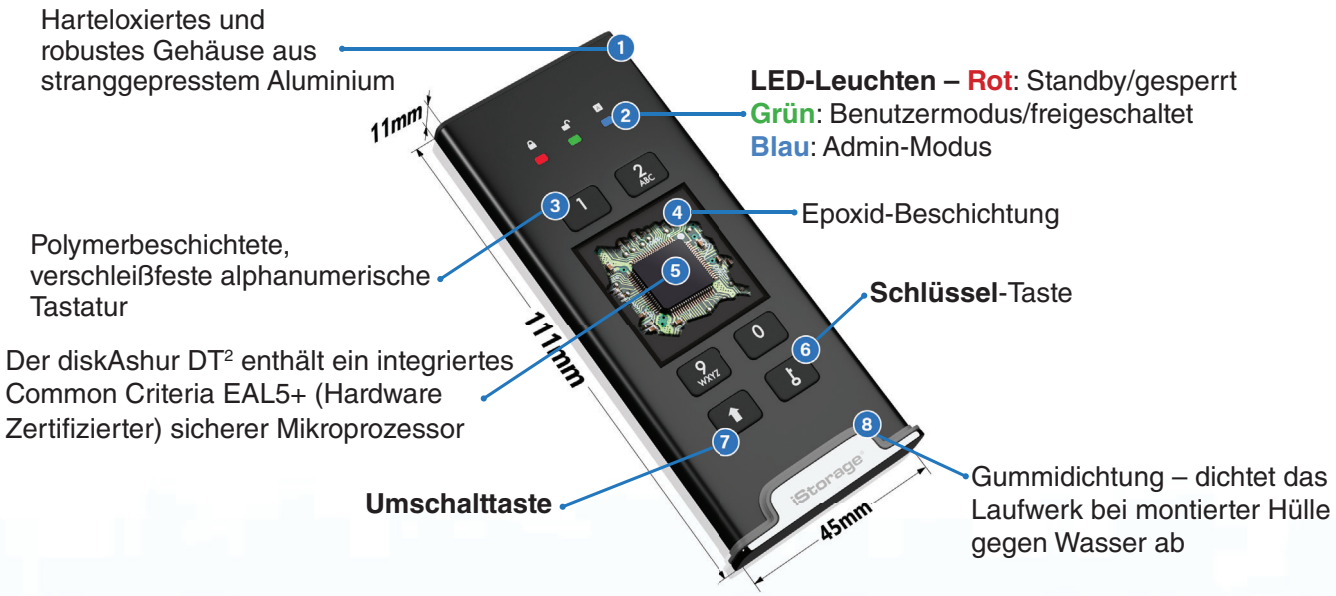
Der diskAshur DT² enthält ein integriertes Common Criteria EAL5+ (Hardware Zertifizierter) sicherer Mikroprozessor, der eingebaute physikalische Schutzmechanismen zur Abwehr von externen Manipulationen, Umgehungsangriffen und Fehlereinstreuungen verwendet.

Im Gegensatz zu anderen Lösungen reagiert der diskAshur M² auf einen automatisierten Angriff, indem er das Laufwerk in den absoluten Stillstand versetzt, was alle derartigen Angriffe nutzlos macht. Kurz gesagt: Ohne die PIN kommt man nicht an die Daten!

Verpackungsinhalt

- diskAshur M² tragbare SSD und Schutzhülle
- Schutztasche
- USB-C- und USB-A-Kabel
- Kurzanleitung und Produkthaftungsausschluss

Aufbau des diskAshur M²



1. LEDs und ihre Zustände

LED	LED-Zustand	Beschreibung	LED	LED-Zustand	Beschreibung
	ROT durchgehend	Gesperrtes Laufwerk (entweder im **Standby-** oder **Zurücksetzen-Zustand)**		BLAU durchgehend	Laufwerk im **Admin-Modus**
	ROT doppelt blinkend	Falsche PIN-Eingabe		ROT, GREEN und BLAU blinken zusammen	Warten auf Eingabe der **Benutzer**-PIN
	GRÜN durchgehend	Laufwerk **freigeschaltet**		GREEN und BLAU blinken zusammen	Warten auf Eingabe der **Admin**-PIN
	GRÜN blinkend	Datentransfer läuft		GREEN und BLAU blinken abwechselnd	Authentifizierung im Gange

2. LED-Zustände

Anmerkung: Starke elektromagnetische Strahlung kann die normale Funktion des diskAshur M2 beeinträchtigen. In diesem Fall schalten Sie das Produkt bitte aus und danach wieder ein. Sollte das Problem dadurch nicht beseitigt worden sein, setzen Sie die diskAshur M2 bitte an einem anderen Ort ein

Aus dem Ruhezustand aufwachen

Der Ruhezustand liegt vor, wenn der diskAshur M² nicht verwendet wird und alle LEDs deaktiviert sind.

Um den diskAshur M² aus dem Ruhezustand aufzuwecken, gehen Sie wie folgt vor.

Verbinden Sie den diskAshur M² mit einen USB-Anschluss an Ihrem Computer, der mit Strom versorgt wird		Es blinken hintereinander und der Reihe nach die ROTE, GRÜNE und BLAUE LED. Anschließend blinkt die GRÜNE LED zweimal und schließlich leuchtet die ROTE LED durchgehend und zeigt an, dass sich das Laufwerk im Standby-Zustand befindet

So versetzen Sie das Laufwerk in den Ruhezustand

Um den diskAshur M² in den Ruhezustand zu versetzen, führen Sie eine der folgenden Operationen aus:

- Trennen Sie das Laufwerk, wenn es an einen USB-Anschluss angeschlossen ist. Alle LEDs gehen aus (Ruhezustand).

Einschaltzustände

Nachdem das Laufwerk aus dem Ruhezustand aufgewacht ist, geht es in einen der Zustände über, die in der nachstehenden Tabelle dargestellt sind.

Einschaltzustand	LED-Anzeige	Schlüssel	Admin-PIN	Beschreibung
Lieferzustand	ROT und GRÜN durchgehend	✓	×	Warten auf die Einstellung einer Admin-PIN (Erste Verwendung)
Standby	ROT durchgehend	✓	✓	Warten auf Eingabe der Admin- oder Benutzer-PIN
Zurücksetzen	ROT durchgehend	×	×	Warten auf die Einstellung einer Admin-PIN

3. Erste Verwendung

Der diskAshur M² wird im **„Lieferzustand" ohne voreingestellte Admin-PIN** geliefert. Bevor das Laufwerk verwendet werden kann, muss eine **7–15-stellige** Admin-PIN eingestellt werden. Sobald eine Admin-PIN erfolgreich konfiguriert wurde, ist es nicht mehr möglich, das Laufwerk wieder in den „Lieferzustand" zu versetzen.

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern lang sein
- Darf nicht nur sich wiederholende Zahlen enthalten, z. B. (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)

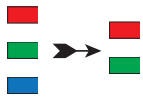
Passwort-Tipp: Sie können ein einprägsames Wort, einen Namen, einen Satz oder eine beliebige andere alphanumerische PIN-Kombination konfigurieren, indem Sie einfach die Taste mit den entsprechenden Buchstaben drücken.

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 eine Admin-PIN zu konfigurieren und den diskAshur M² zum ersten Mal freizuschalten, befolgen Sie bitte die einfachen Schritte in der folgenden Tabelle.

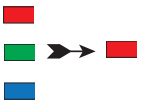
Anweisungen – Erste Verwendung	LED	LED-Zustand
1. Verbinden Sie den diskAshur M² mit einen USB-Anschluss an Ihrem Computer, der mit Strom versorgt wird		Die ROTE, GRÜNE und BLAUE LED blinken einmal der Reihe nach. Anschließend blinkt die GRÜNE LED zweimal und schließlich leuchten die ROTE und GRÜNE LED durchgehend und zeigen an, dass sich das Laufwerk im Lieferzustand befindet
2. Drücken und halten Sie die **SCHLÜSSEL-Taste (🔑)** und die **1**		Die GRÜNE LED blinkt und die BLAUE LED leuchtet durchgehend
3. Geben Sie eine **neue Admin-PIN** ein (7–15 Ziffern) und drücken Sie die Taste **SCHLÜSSEL (🔑)** 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
4. Geben Sie Ihre **neue Admin-PIN** erneut ein und drücken Sie die Taste **SCHLÜSSEL (🔑)** erneut		Die BLAUE LED blinkt schnell und wechselt dann zu einem durchgehenden BLAU und schließlich zu einer durchgehend GRÜN leuchtenden LED, die angibt, dass die Admin-PIN erfolgreich konfiguriert und das Laufwerk freigeschaltet wurde

Sperren des diskAshur M²

Um das Laufwerk zu sperren, werfen Sie den diskAshur M² 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 diskAshur M² zu unvollständiger Datenübertragung und möglicherweise zu Schäden an den Daten.

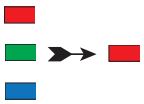
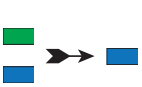
4. Freischalten des diskAshur M² mit der Admin-PIN

Um den diskAshur M² mit der Admin-PIN freizuschalten, befolgen Sie bitte die einfachen Schritte in der folgenden Tabelle.

1. Verbinden Sie den diskAshur M² mit einen USB-Anschluss an Ihrem Computer		Die ROTE, GRÜNE und BLAUE LED blinken einmal der Reihe nach. Anschließend blinkt die GRÜNE LED zweimalund schließlich leuchtet die ROTE LED durchgehend und zeigt an, dass sich das Laufwerk im Standby-Zustand befindet
2. Drücken Sie im Standby-Zustand (durchgehend ROT leuchtende LED) die **SCHLÜSSEL**-Taste **(🔑)** einmal		GRÜNE und BLAUE LEDs blinken zusammen
3. Während die GRÜNE und BLAUE LED zusammen blinken, geben Sie Ihre **Admin-PIN** ein und drücken Sie erneut die **SCHLÜSSEL**-Taste **(🔑)**		Die GRÜNE und BLAUE LED blinken abwechselnd mehrmals, dann leuchtet die BLAUE LED durchgehend und schließlich die GRÜNE LED, die anzeigt, dass das Laufwerk erfolgreich als Admin freigeschaltet wurde

5. Wechseln in den Admin-Modus

Gehen Sie wie folgt vor, um in den Admin-Modus zu wechseln.

1. Verbinden Sie den diskAshur M² mit einen USB-Anschluss an Ihrem Computer, der mit Strom versorgt wird		Die ROTE, GRÜNE und BLAUE LED blinken einmal der Reihe nach. Anschließend blinkt die GRÜNE LED zweimalund schließlich leuchtet die ROTE LED durchgehend und zeigt an, dass sich das Laufwerk im Standby-Zustand befindet
2. Drücken und halten Sie im Standby-Zustand (durchgehend leuchtende ROTE LED) die **SCHLÜSSEL**-Taste **(🔑)** und die **1**		GRÜNE und BLAUE LEDs blinken zusammen
3. Geben Sie Ihre **Admin-PIN** erneut ein und drücken Sie die Taste **SCHLÜSSEL (🔑)** einmal		Die GRÜNE und BLAUE LED blinken abwechselnd mehrmals, dann leuchtet die GRÜNE LED und schließlich die BLAUE LED durchgehend, die anzeigt, dass das Laufwerk im Admin-Modus ist

Beenden des Admin-Modus

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

6. Ändern der Admin-PIN

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern lang sein
- Darf nicht nur sich wiederholende Zahlen enthalten, z. B. (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)

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

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

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 (7 bis 15 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 7–15-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 7–15-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 7–15 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 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 **070** erneut ein und drücken Sie die **UMSCHALT**-Taste (⬆) einmal		Die blinkende GRÜNE und BLAUE LED wechseln zu einer durchgehend GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, 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: Die Erstellung einer neuen 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.

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern lang sein
- Darf nicht nur sich wiederholende Zahlen enthalten, z. B. (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.

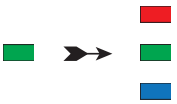
13. Freischalten des diskAshur M² mit der Benutzer-PIN

Um den diskAshur M² mit der **Benutzer-PIN** zu entsperren, fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im Standby-Zustand (durchgehend leuchtende ROTE LED) die **UMSCHALT**-Taste **(⬆)** und die SCHLÜSSEL-Taste **(🔑)** gedrückt		Von der leuchtenden ROTEN LED wechselt das Gerät zu drei blinkenden LEDs, ROT, GRÜN und BLAU
2. Geben Sie Ihre Benutzer-PIN erneut ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔑)** einmal		Die ROT, GRÜN und BLAU blinkenden LEDs wechseln zur abwechselnd blinkenden GRÜNEN und BLAUEN LED und dann zu einer durchgehend leuchtenden GRÜNEN LED, die anzeigt, dass das Laufwerk im Benutzermodus erfolgreich freigeschaltet wurde

14. Ändern der Benutzer-PIN im Benutzermodus

Um die **Benutzer-PIN** zu ändern, entsperren Sie zunächst den diskAshur M² mit der Benutzer-PIN, 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 (GRÜNE LED) die **SCHLÜSSEL**-Taste **(🔑)** und die 4 gedrückt.		Die durchgehend GRÜNE LED geht aus und alle LEDs fangen an zu blinken, ROT, GRÜN und BLAU.
2. Geben Sie Ihre **bestehende Benutzer-PIN** ein und drücken Sie die **SCHLÜSSEL**-Taste **(🔑)** einmal		Die GRÜNE und durchgehend BLAUE LED leuchten abwechselnd und schalten dann nur zur GRÜN blinkenden LED und anschließend wieder zur GRÜN blinkenden und durchgehend BLAUEN LED.
3. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie 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
4. Geben Sie die **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 GRÜNEN LED, die anzeigt, dass die Benutzer-PIN erfolgreich geändert wurde

Achtung: Das Ändern der Benutzer-PIN im Benutzermodus (GRÜNE LED) muss mit der „Benutzer-PIN-Richtlinie“ übereinstimmen, wenn diese wie in Abschnitt 7 beschrieben konfiguriert wurde. Darin wird die Mindestlänge der PIN und die Verwendung von „Sonderzeichen“ festgelegt.

15. Erstellen einer einmaligen Benutzer-Wiederherstellungs-PIN

Die Benutzer-Wiederherstellungs-PIN ist äußerst nützlich in Situationen, in denen ein Benutzer seine PIN zum Entsperren des diskAshur M² vergessen hat.
Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zunächst die einmalige Wiederherstellungs-PIN korrekt eingeben, falls diese konfiguriert wurde. Der Wiederherstellungsprozess der Benutzer-PIN hat keinen Einfluss auf die Daten, den Schlüssel oder die Admin-PIN. Allerdings muss der Benutzer dabei eine neue 7–15-stellige Benutzer-PIN konfigurieren.

Um eine einmalige Benutzer-Wiederherstellungs-PIN mit 7–15 Stellen zu konfigurieren, wechseln Sie zunächst 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 **SCHLÜSSEL- (🔑) und die 4**-Taste gleichzeitig gedrückt		Die durchgehend BLAUE LED schaltet zur blinkend GRÜNEN und durchgehend BLAUEN LEDs
2. Geben Sie eine **einmalige Wiederherstellungs-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 eine **einmalige Wiederherstellungs-PIN** erneut ein und drücken Sie erneut die **SCHLÜSSEL**-Taste **(🔑)**		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 einmalige Wiederherstellungs-PIN 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.

16. Löschen der einmaligen Benutzer-Wiederherstellungs-PIN

Um die einmalige Benutzer-Wiederherstellungs-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 **4** gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zur blinkend ROTEN LED
2. Drücken und halten Sie die **UMSCHALT**-Taste (⬆) und die **4** gleichzeitig gedrückt		Die blinkende ROTE LED leuchtet durchgehend ROT und wechselt dann zu einer durchgehend BLAUEN LED, die anzeigt, dass die einmalige Benutzer-Wiederherstellungs-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.

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

Die Benutzer-Wiederherstellungs-PIN ist äußerst nützlich in Situationen, in denen ein Benutzer seine PIN zum Entsperren des diskAshur M² vergessen hat.
Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zunächst die einmalige Wiederherstellungs-PIN korrekt eingeben, falls diese konfiguriert wurde. Der Wiederherstellungsprozess der Benutzer-PIN hat keinen Einfluss auf die Daten, den Schlüssel oder die Admin-PIN. Allerdings muss der Benutzer dabei eine neue 7–15-stellige Benutzer-PIN konfigurieren.
Um den Wiederherstellungsprozess zu aktivieren und eine neue Benutzer-PIN zu konfigurieren, fahren Sie mit den folgenden Schritten fort.

1. Drücken und halten Sie im **Standby-Zustand** (ROTE LED) die **SCHLÜSSEL-Taste (🔑)** und die **4** gleichzeitig		Die durchgehend ROTE LED wechselt zu ROT und GRÜN blinkenden LEDs
2. Geben Sie eine einmalige **Wiederherstellungs-PIN** ein und drücken Sie die Schlüssel-Taste **(🔑)**		Die GRÜNE und BLAUE LED leuchten abwechselnd auf und schalten dann zu einer durchgehend GRÜN leuchtenden LED und schließlich zu einer GRÜN blinkenden und durchgehend BLAUEN LED.
3. 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
4. Geben Sie Ihre **neue Benutzer-PIN** erneut ein und drücken Sie erneut die **SCHLÜSSEL**-Taste **(🔑)**		Die GRÜNE LED blinkt schnell, wird dann durchgehend GRÜN und zeigt so an, dass der Wiederherstellungsprozess erfolgreich war und eine neue Benutzer-PIN konfiguriert wurde

Wichtig: Die Erstellung einer neuen 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 wird beschrieben, wie die Einschränkungen der Benutzer-PIN überprüft werden können.

18. Benutzer auf Schreibschutz im Admin-Modus einstellen

Aufgrund der vielen Viren und Trojaner, die USB-Laufwerke infizieren, ist die Schreibschutzfunktion besonders nützlich, wenn Sie in einer öffentlichen Umgebung auf Daten auf dem USB-Laufwerk zugreifen möchten. Dies ist auch eine wichtige Funktion für forensische Zwecke, wenn Daten in ihrem ursprünglichen und unveränderten Zustand erhalten bleiben müssen, ohne dass dieser bearbeitet oder überschrieben wird.

Wenn der Administrator den diskAshur M² konfiguriert und den Benutzerzugriff auf Lesezugriff beschränkt, kann nur noch der Administrator auf das Laufwerk schreiben oder die Einstellung wieder auf Lese-/Schreibzugriff zurücksetzen, wie in Abschnitt 19 beschrieben. Der Benutzer ist auf den Lesezugriff beschränkt und kann im Benutzermodus nicht auf das Laufwerk schreiben oder diese Einstellung ändern.

Um den diskAshur M² so einzustellen, dass der Benutzerzugriff 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 „**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.

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

Um den diskAshur M² 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.

20. Globalen Schreibschutz im Admin-Modus einstellen

Wenn der Administrator den diskAshur M² 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 21 beschrieben.

Um den diskAshur M² 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.

21. Globalen Lese-/Schreibzugriff im Admin-Modus einstellen

Lesezugriff deaktiviert wird, 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 + 9“.**		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie die Schlüssel-Taste **(🔑)**		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. Konfigurieren einer Selbstzerstörungs-PIN

Sie können eine Selbstzerstörungs-PIN konfigurieren, die nach der Eingabe eine Krypto-Löschung auf dem Laufwerk durchführt (der Schlüssel wird gelöscht). Dieser Prozess löscht alle konfigurierten PINs und macht alle auf dem Laufwerk gespeicherten Daten unzugänglich (diese gehen dauerhaft verloren). Das Laufwerk zeigt dann eine freigeschaltete GRÜNE LED. Wenn diese Funktion ausgeführt wird, wird die Selbstzerstörungs-PIN zur neuen Benutzer-PIN, und das Laufwerk muss formatiert werden, bevor es wieder 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 7–15-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.

23. 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

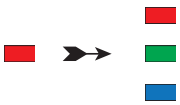
Anmerkung: Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu beenden, drücken Sie die **UMSCHALT**-Taste (⬆) und halten Sie sie eine Sekunde lang gedrückt – die durchgehend BLAUE LED schaltet zur durchgehend ROTEN LED um.

24. Freischalten mit der Selbstzerstörungs-PIN

Warnung: Wenn der Selbstzerstörungsmechanismus aktiviert wird, werden alle Daten, der Schlüssel sowie die Admin/Benutzer-PINs gelöscht. **Die Selbstzerstörungs-PIN wird zur Benutzer-PIN**. Nach Aktivierung des Selbstzerstörungsmechanismus existiert keine Admin-PIN mehr. Der diskAshur M² muss zuerst zurückgesetzt werden (siehe „Vollständiges Zurücksetzen“ in Abschnitt 35 auf Seite 100), um eine Admin-PIN mit vollen Admin-Rechten zu konfigurieren, einschließlich der Möglichkeit, eine neue Benutzer-PIN einzustellen.

Wenn die Selbstzerstörungs-PIN verwendet wird, **löscht sie ALLE Daten und Admin-/Benutzer-PINs** und schaltet dann das Laufwerk frei. Wenn diese Funktion aktiviert wird, **wird die Selbstzerstörungs-PIN zur neuen Benutzer-PIN**, und der diskAshur M² muss formatiert werden, bevor er wieder verwendet werden kann.

Um den Selbstzerstörungsmechanismus zu aktivieren, muss sich das Laufwerk im Standby-Zustand befinden (durchgehend leuchtende ROTE LED). Fahren Sie dann mit den folgenden Schritten fort.

1. Drücken und halten Sie im **Standby-Zustand** (durchgehend leuchtende ROTE LED) die **UMSCHALT**-Taste (⬆) und die **SCHLÜSSEL**-Taste **(🔑)** gleichzeitig gedrückt		Von der leuchtenden ROTEN LED wechselt das Gerät zu drei blinkenden LEDs, ROT, GRÜN und BLAU
2. Geben Sie die **Wiederherstellungs-PIN** ein und drücken Sie die **Schlüssel**-Taste **(🔑)**		Die ROT, GRÜN und BLAU blinkenden LEDs wechseln zu GRÜNEN und BLAUEN LEDs, die für einige Sekunden abwechselnd an und aus gehen. Schließlich leuchtet die GRÜNE LED durchgehend und zeigt an, dass der Selbstzerstörungsvorgang des diskAshur M² erfolgreich abgeschlossen wurde

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

Nach einem Brute-Force-Angriff oder wenn Sie den diskAshur M² zurückgesetzt haben, muss eine neue Admin-PIN erstellt werden, bevor das Laufwerk verwendet werden kann.

PIN-Anforderungen:

- Muss zwischen 7 und 15 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)

Wenn der diskAshur M² 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.

26. Einstellen der automatischen Sperre bei Abwesenheit

Zum Schutz vor unbefugtem Zugriff kann der diskAshur M² 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 diskAshur M² 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.

27. Deaktivieren der automatischen Sperre bei Abwesenheit

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 **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.

28. 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.

29. Schreibschutz im Benutzermodus einstellen

Um den diskAshur M² 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.

30. Lese-/Schreibzugriff im Benutzermodus einstellen

Um den diskAshur M² 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.

31. Schutzmechanismus gegen Brute-Force-Hacking

Der diskAshur M² verfügt über einen Abwehrmechanismus, um das Laufwerk vor Brute-Force-Angriffen zu schützen. Standardmäßig und im Lieferzustand betragen die Beschränkungen für Brute Force (aufeinanderfolgende Falscheingaben der PIN) sowohl für die Admin-PIN als auch für die Benutzer-PIN **10** Mal sowie **5** Mal für die Wiederherstellungs-PIN. Drei unabhängige Brute-Force-Zähler werden verwendet, um die fehlerhaften Versuche für jede PIN-Autorisierung (Admin, Benutzer und Wiederherstellung) aufzuzeichnen, wie unten beschrieben.

- Wenn ein Benutzer 10 Mal hintereinander eine **falsche Benutzer-PIN** eingibt, wird diese gelöscht. Die Daten, die Admin-PIN und die Wiederherstellungs-PIN bleiben jedoch intakt und zugänglich.
- Wenn ein Benutzer 5 Mal hintereinander eine **falsche Wiederherstellungs-PIN** eingibt, wird diese gelöscht. Die Daten, die Admin-PIN und die Wiederherstellungs-PIN bleiben jedoch intakt und zugänglich.
- Wenn die **Admin-PIN** 10 Mal hintereinander falsch eingegeben wird, wird das Laufwerk zurückgesetzt. Alle PINs und Daten werden gelöscht und gehen für immer verloren.

Die folgende Tabelle gilt für den Fall, dass alle drei PINs eingerichtet wurden, und verdeutlicht die Wirkung der Aktivierung des Brute-Force-Abwehrmechanismus für jede einzelne PIN.

Zum Entsperren des Laufwerks verwendete PIN	Aufeinanderfolgende falsche PIN-Eingaben	Beschreibung der Vorgänge
Benutzer-PIN	10	• Die Benutzer-PIN wird gelöscht. • Die Wiederherstellungs-PIN, die Admin-PIN und alle Daten bleiben intakt und zugänglich.
Wiederherstel-lungs-PIN	5	• Die Wiederherstellungs-PIN wird gelöscht. • Die Admin-PIN und alle Daten bleiben intakt und zugänglich.
Admin-PIN	10	• Der diskAshur M² wird zurückgesetzt. Alle PINs und Daten werden gelöscht und gehen für immer verloren.

Anmerkung: Die Brute-Force-Begrenzung wird auf die ursprünglichen Werte des Lieferzustands zurückgesetzt, wenn das Laufwerk vollständig zurückgesetzt, wenn die Selbstzerstörungsfunktion aktiviert wird oder wenn ein Brute-Force-Angriff erfolgt. Wenn der Admin die Benutzer-PIN ändert oder bei der Aktivierung der Wiederherstellungsfunktion eine neue Benutzer-PIN festgelegt wird, wird der Brute-Force-Zähler der Benutzer-PIN auf Null (0) gesetzt. Die Brute-Force-Beschränkung ist davon nicht betroffen. Wenn der Admin die Wiederherstellungs-PIN ändert, wird der Brute-Force-Zähler der Wiederherstellungs-PIN auf Null gesetzt.

Bei erfolgreicher Autorisierung mit einer bestimmten PIN wird der Brute-Force-Zähler für diese PIN auf Null gesetzt, die Brute-Force-Zähler der anderen PINs werden dadurch jedoch nicht beeinflusst. Bei fehlgeschlagener Autorisierung mit einer bestimmten PIN wird der Brute-Force-Zähler für diese PIN erhöht, die Brute-Force-Zähler der anderen PINs werden dadurch jedoch nicht beeinflusst.

32. Admin-PIN-Mechanismus zur Abwehr von Brute-Force-Hacker-Angriffen

Die diskAshur M²-Admin-PIN ist im Vergleich zur Benutzer- oder Wiederherstellungs-PIN mit einem ausgeklügelteren Abwehrmechanismus ausgestattet. Dadurch soll verhindert werden, dass Sie eine Admin-PIN versehentlich 10-mal hintereinander falsch eingeben und in der Folge alle Ihre Daten verlieren. Nach 5 aufeinanderfolgenden Eingaben einer falschen Admin-PIN wird die diskAshur M² gesperrt und alle LEDs leuchten auf und zeigen Dauerlicht.

WARNUNG: Benutzen Sie das folgende Verfahren nicht, wenn Sie Ihre diskAshur M² nur mit der „**BENUTZER-PIN**“ entsperren und die „**ADMIN-PIN**“ nicht kennen.

Informationen zur Erweiterung der Admin-PIN-Eingabe auf maximal 10 Versuche finden Sie in den Anweisungen.

Aufeinanderfolgende falsche Admin-PIN-Eingaben	Beschreibung der diskAshur M²-Vorgänge	Anweisungen
5	Alle LEDs – **ROT**, **GRÜN** und **BLAU** – leuchten auf und zeigen Dauerlicht	Geben Sie die PIN „**47867243**“ ein und drücken Sie einmal die **TASTE (⚷)**. Die **GRÜNE** und die **BLAUE** LED beginnen, abwechselnd zu blinken, d. h. die diskAshur M² akzeptiert jetzt **3 weitere Admin-PIN-Eingaben**.
8	Alle LEDs – **ROT**, **GRÜN** und **BLAU** – beginnen, abwechselnd zu blinken	Geben Sie die PIN „**47867243**“ ein und drücken Sie einmal die **TASTE (⚷)**. Die **GRÜNE** und **BLAUE** LED beginnen, abwechselnd zu blinken, d. h. die diskAshur M² akzeptiert jetzt **2 weitere Admin-PIN-Eingaben**.
10	Die **ROTE** LED leuchtet auf und zeigt Dauerlicht.	Nach insgesamt 10 falschen Admin-PIN-Eingaben werden der Verschlüsselungsschlüssel, alle PINs und die Daten unwiederbringlich gelöscht.

33. Einstellen der Brute-Force-Begrenzung für die Benutzer-PIN

Anmerkung: Die Einstellung für die Brute-Force-Begrenzung der Benutzer-PIN ist standardmäßig auf 10 aufeinanderfolgende falsche PIN-Eingaben eingestellt, wenn das Laufwerk vollständig zurückgesetzt wurde, einem Brute-Force-Angriff unterlag oder die Selbstzerstörungs-PIN aktiviert wurde.

Die Brute-Force-Begrenzung für die Benutzer-PIN des diskAshur M² kann vom Administrator umprogrammiert und eingestellt werden. Diese Funktion kann so eingestellt werden, dass von 1 bis 10 aufeinanderfolgende falsche PIN-Eingaben möglich sind.

Um die Brute-Force-Begrenzung für die Benutzer-PIN 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 Tasten **7 + 0** gleichzeitig gedrückt		Die durchgehend BLAUE LED schaltet um zu den GRÜN und BLAU blinkenden LEDs.
2. Geben Sie die Anzahl der Versuche für die Brute-Force-Begrenzung ein (zwischen 1 und 10), z. B.: • **01** für 1 Versuch • **10** für 10 Versuche		
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 Begrenzung für Brute-Force-Versuche erfolgreich konfiguriert wurden

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.

34. Überprüfen der Brute-Force-Begrenzung für die Benutzer-PIN

Der Administrator kann überprüfen und festlegen, wie oft hintereinander eine falsche Benutzer-PIN eingegeben werden darf, bevor der Brute-Force-Abwehrmechanismus ausgelöst wird, indem er oder sie einfach die LED-Sequenz wie unten beschrieben beobachtet.

Um die Brute-Force-Begrenzung 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 **2 + 0** 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) Falscheingaben in der Brute-Force-Begrenzung. c. Jedes Blinken der GRÜNEN LED entspricht einer (1) Falscheingabe in der Brute-Force-Begrenzung. 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 Einstellung der Brute-Force-Begrenzung. Wenn Sie z. B. das Laufwerk so eingestellt haben, dass es nach **5** aufeinanderfolgenden falschen PIN-Eingaben den Brute-Force-Abwehrmechanismus aktiviert, blinkt die GRÜNE LED fünf (**5**) Mal.

Einstellung der Brute-Force-Begrenzung	**ROT**	**GRÜN**
2 Versuche	0	2-faches Blinken
5 Versuche	0	5-faches Blinken
10 Versuche	1-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.

35. Vollständiges Zurücksetzen des Geräts

Um das Gerät vollständig zurückzusetzen, muss sich der diskAshur M² 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 diskAshur M² 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

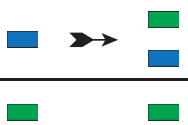
Wichtig: Wenn das Gerät vollständig zurückgesetzt wurde, muss eine neue Admin-PIN konfiguriert werden, siehe Abschnitt 25 auf Seite 94: „Erstellen einer Admin-PIN nach einem Brute-Force-Angriff oder nach dem Zurücksetzen“. Der diskAshur M² muss auch Formatiert werden, bevor neue Daten zum Laufwerk hinzugefügt werden können.

36. DiskAshur M² als bootfähiges Laufwerk konfigurieren

Anmerkung: Wenn das Laufwerk als bootfähiges Laufwerk konfiguriert ist, leuchtet die ROTE LED nicht, nachdem Sie das Laufwerk im Betriebssystem auswerfen. Das Gerät zeigt eine durchgehend GRÜN leuchtende LED und muss für den nächsten Gebrauch abgezogen werden. Standardmäßig ist der diskAshur M² als nicht bootfähig konfiguriert.

Der diskAshur M² ist mit Bootfunktion ausgestattet, um das Ein- und Ausschalten während des Bootvorgangs des Hosts zu ermöglichen. Wenn Sie vom diskAshur M² booten, führen Sie Ihren Computer mit dem Betriebssystem aus, das auf dem diskAshur M² installiert ist.

Um das Laufwerk als bootfähig 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 **8** gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie auf **„0“** gefolgt von einer **„1“** (**01**)		Die blinkenden GRÜNEN und BLAUEN LEDs blinken weiter
3. Drücken Sie die **UMSCHALT-Taste** (⬆) einmal		Die blinkende GRÜNE und BLAUE LED wechseln zu einer durchgehend GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, dass das Laufwerk erfolgreich als bootfähig 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.

37. Bootfunktion des diskAshur M² deaktivieren

Um die Bootfunktion des diskAshur M² zu deaktivieren, 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 **SCHLÜSSEL-Taste (🔑)** und die 8 gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs
2. Drücken Sie auf **„0“** gefolgt von einer weiteren **“0”** (**00**)		Die blinkenden GRÜNEN und BLAUEN LEDs blinken weiter
3. Drücken Sie die **UMSCHALT-Taste** (⬆) einmal		Die blinkende GRÜNE und BLAUE LED wechseln zu einer durchgehend GRÜNEN LED und schließlich zu einer durchgehend BLAUEN LED, die anzeigt, dass die Bootfunktion 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.

38. Bootfähigkeits-Einstellung überprüfen

Um den Status der Bootfunktion 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 8 gleichzeitig gedrückt		Die durchgehend BLAUE LED wechselt zu blinkend GRÜNEN und BLAUEN LEDs

2. Drücken Sie die **UMSCHALT**-Taste **(🔑)** und eines der beiden folgenden Szenarien wird eintreten;

- **Wenn der diskAshur M² als bootfähig konfiguriert ist, geschieht Folgendes;**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend.
b. Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend.
d. LEDs schalten zu einem durchgehenden BLAU zurück

- **Wenn der diskAshur M² <u>NICHT</u> als bootfähig konfiguriert ist, geschieht Folgendes;**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend.
b. Alle LEDs gehen aus
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten eine Sekunde lang durchgehend.
d. LEDs schalten zu einem durchgehenden BLAU zurück

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.

39. Initialisieren und Formatieren des diskAshur M² für Windows

Nach einem Brute-Force-Angriff oder einer vollständigen Zurücksetzung löscht der diskAshur M² alle PINs, Daten und den Schlüssel. Sie müssen den diskAshur M² initialisieren und formatieren, bevor er verwendet werden kann.

Um Ihren diskAshur M² zu formatieren, gehen Sie wie folgt vor:

1. Konfigurieren Sie eine neue Admin-PIN – siehe Seite 94, Abschnitt 25, „Erstellen einer Admin-PIN nach einem Brute-Force-Angriff oder nach dem Zurücksetzen“.

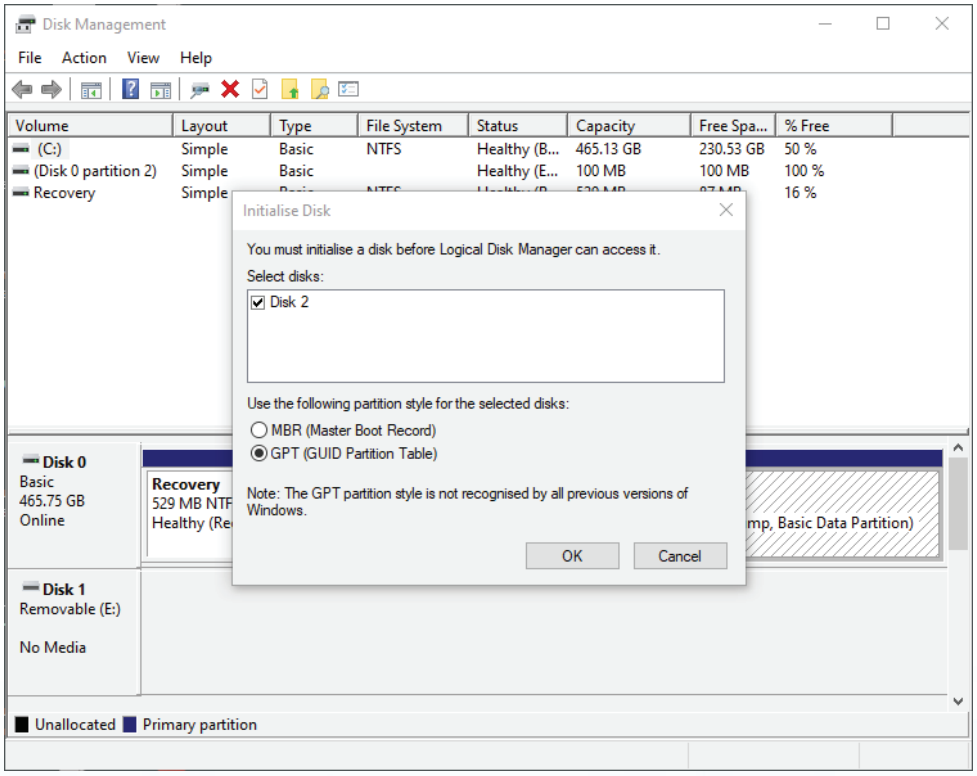
2. Drücken Sie, während der diskAshur M² im Standby-Zustand ist (ROTE LED), einmal auf die **SCHLÜSSEL**-Taste **(⚷)** und geben Sie die **neue Admin-PIN** zum Entsperren ein (GRÜN blinkende LED).

3. Schließen Sie den diskAshur M² an den Computer an.

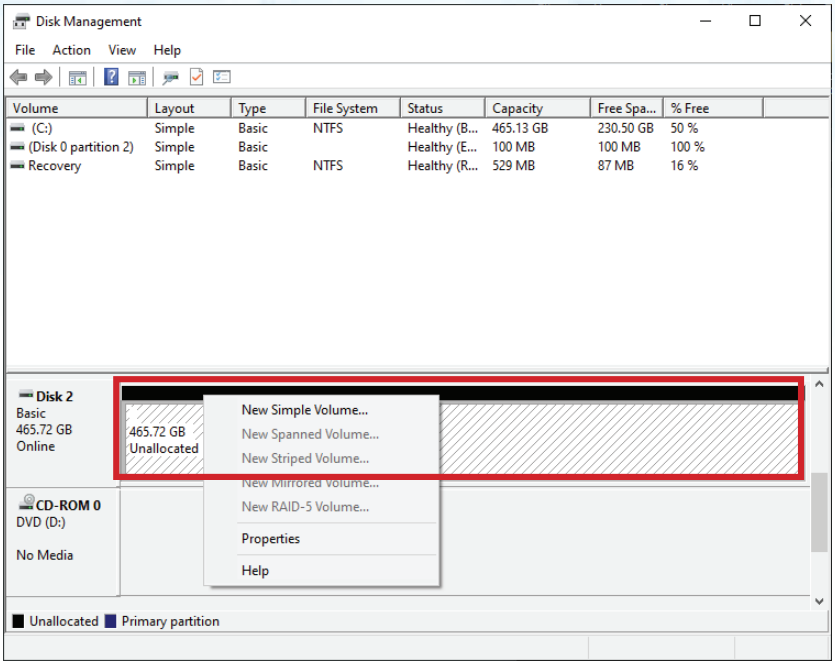
4. **Windows 7:** Klicken Sie mit der rechten Maustaste auf **Computer**, dann auf **Verwalten** und wählen Sie dann **Datenträgerverwaltung**
   Windows 8: Klicken Sie mit der rechten Maustaste auf die linke Ecke des Desktops und wählen Sie **Datenträgerverwaltung**
   Windows 10: Klicken Sie mit der rechten Maustaste auf die Start-Schaltfläche und wählen Sie **Datenträgerverwaltung**

5. Im Fenster Datenträgerverwaltung wird der diskAshur M² wird als unbekanntes Gerät erkannt, das nicht initialisiert und nicht zugewiesen ist. Es erscheint ein Meldungsfenster, in dem Sie zwischen MBR- und GPT-Partitionsstil wählen können. Mit GPT werden mehrere Duplikate dieser Daten über das Laufwerk verteilt gespeichert, wodurch die Datenspeicherung deutlich robuster ist. Auf einem MBR-Laufwerk werden die Partitionierungs- und Boot-Informationen an einem einzigen Ort gespeichert.

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



6. Klicken Sie mit der rechten Maustaste in den leeren Bereich über dem Bereich **Nicht zugewiesen** und wählen Sie dann **Neuer einfacher Datenträger.**



7. Das Fenster „Willkommen zum Assistenten für neue einfache Datenträger“ wird geöffnet. Klicken Sie auf „Weiter“.



8. Wenn Sie nur eine Partition benötigen, akzeptieren Sie die Standardpartitionsgröße und klicken Sie auf **Weiter**.

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

10. Erstellen Sie eine Datenträger-Bezeichnung, wählen Sie „Schnellformatierung durchführen“ und klicken Sie dann auf **Weiter**.

11. Klicken Sie auf **Fertigstellen**.

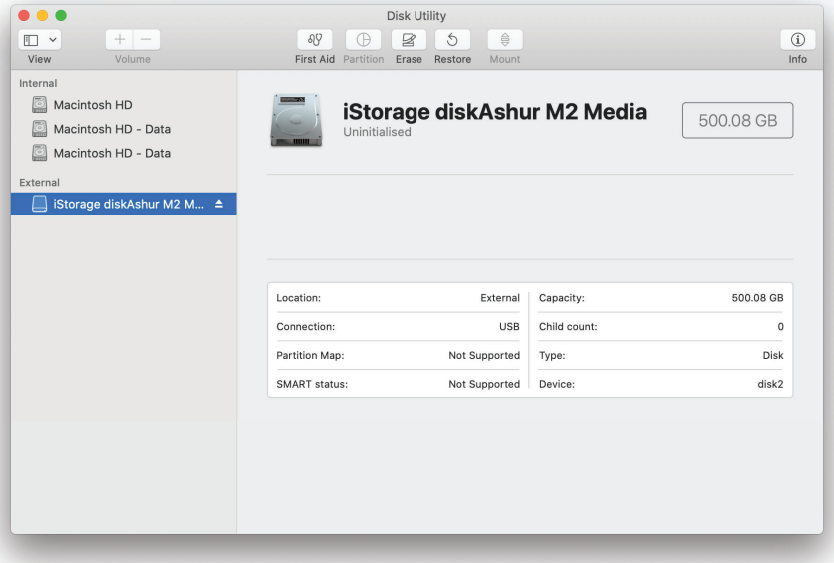
12. Warten Sie, bis der Formatierungsprozess abgeschlossen ist. Der diskAshur M² wird erkannt und kann nun benutzt werden.

40. Initialisieren und Formatieren des diskAshur M² unter Mac OS

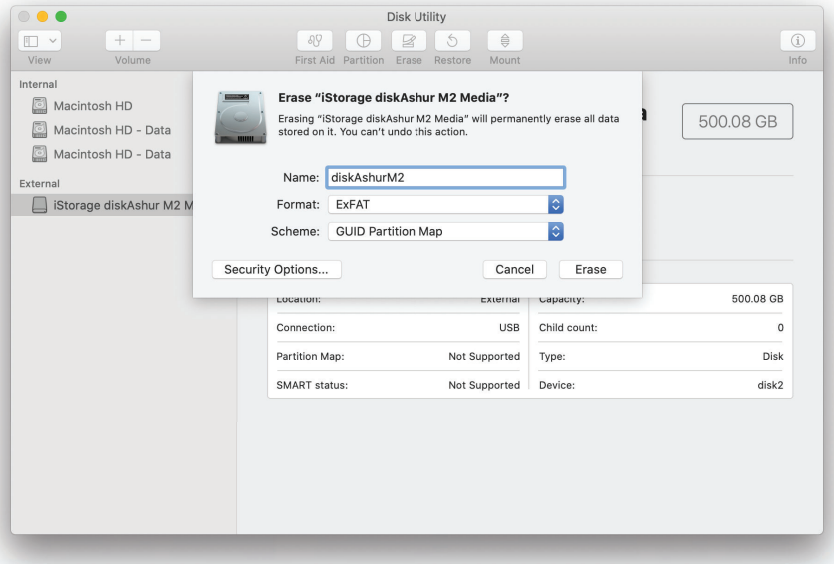
Nach einem Brute-Force-Angriff oder einer vollständigen Zurücksetzung löscht der diskAshur M² alle PINs, Daten und den Schlüssel. Sie müssen den diskAshur M² initialisieren und formatieren, bevor er verwendet werden kann.

Initialisieren und Formatieren des diskAshur M²:

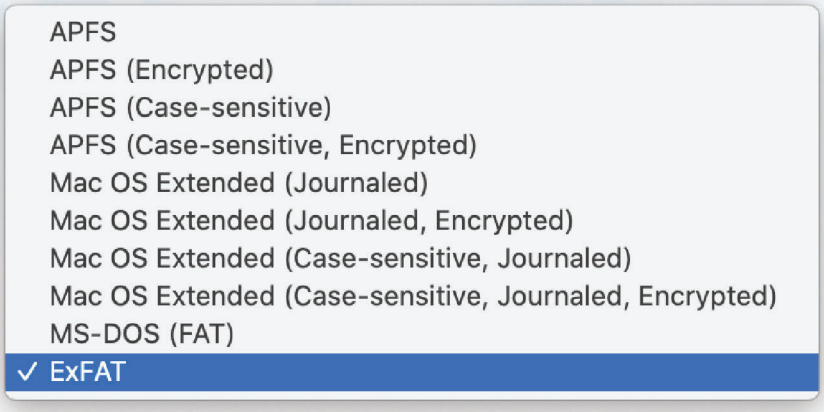
1. Wählen Sie den diskAshur M² aus der Liste der Laufwerke und Datenträger aus. Für jedes Laufwerk in der Liste wird die Kapazität, der Hersteller und der Produktname angezeigt, z. B. „**iStorage diskAshur M² Media**“.



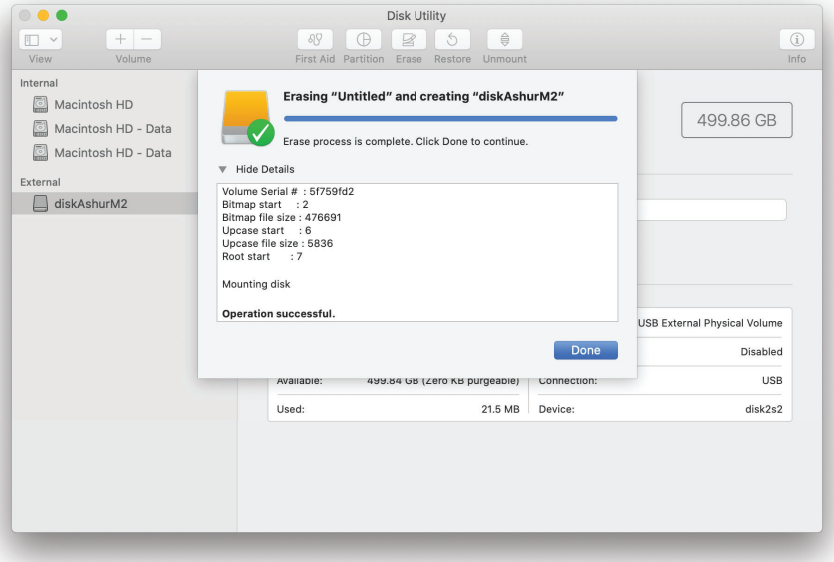
2. Klicken Sie im Festplattendienstprogramm auf die Schaltfläche „**Löschen**“.
3. Geben Sie einen Namen für das Laufwerk ein. Der Standardname ist „Unbenannt“. Der Name des Laufwerks erscheint anschließend auf dem Desktop.



4. Wählen Sie ein Schema und das zu verwendende Laufwerksformat aus. Das Dropdown-Menü „Laufwerksformat“ listet die verfügbaren Laufwerksformate auf, die der Mac unterstützt. Der empfohlene Formattyp ist „Mac OS Extended (Journaled)“. Für die plattformüber-greifende Verwendung sollten Sie „exFAT“ wählen. Das Dropdown-Menü „Schemaformat“ listet die verfügbaren Schemata auf, die verwendet werden können. Wir empfehlen die Verwendung von „GUID Partition Map“ auf Laufwerken mit mehr als 2 TB Kapazität.

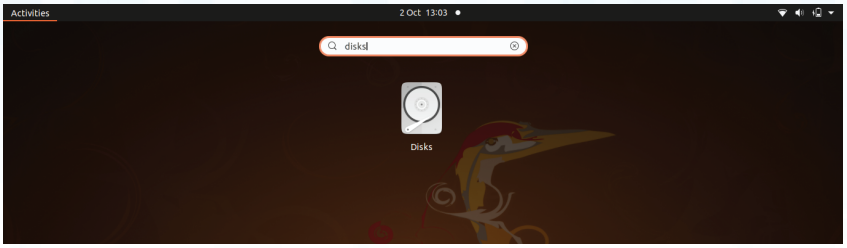


5. Klicken Sie auf die Schaltfläche „Löschen“. Das Festplattendienstprogramm wirft den Datenträger vom Desktop aus, löscht ihn zeigt ihn dann wieder auf dem Desktop an.

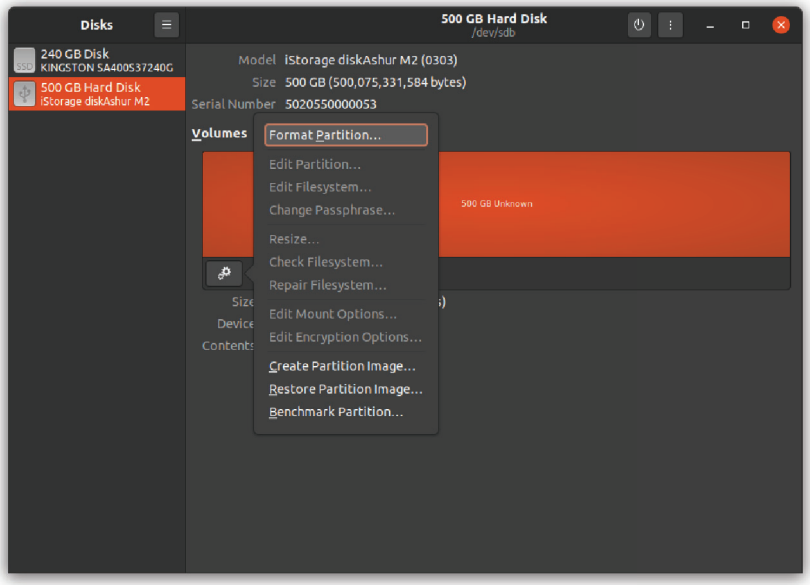


41. Initialisieren und Formatieren des diskAshur M² für Linux

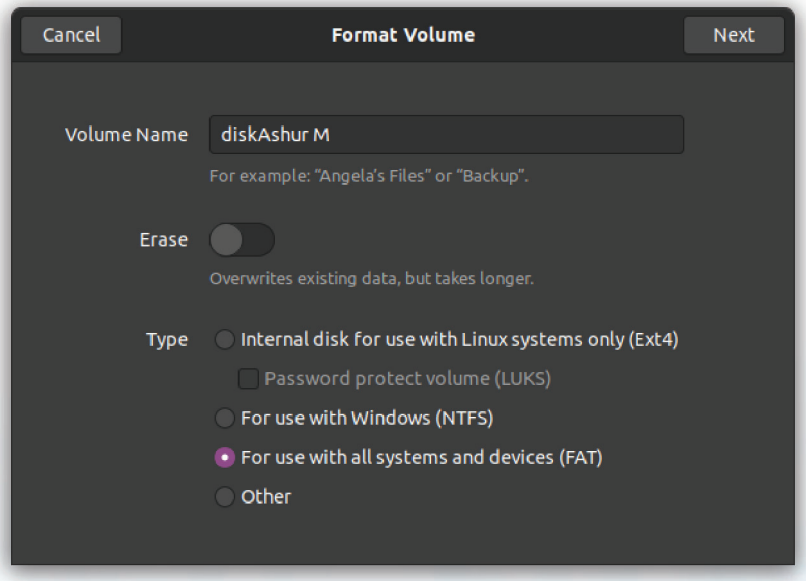
1. Öffnen Sie „**Anwendung anzeigen**“ und geben Sie „**Datenträger**“ in das Suchfeld ein. Klicken Sie auf das Dienstprogramm „**Datenträger**“, sobald es angezeigt wird.



2. Wählen Sie das Laufwerk (500 GB Festplatte) unter „**Geräte**“ aus. Klicken Sie als nächstes auf das Zahnradsymbol unter „**Datenträger**“ und dann auf „**Partitionen formatieren**“.

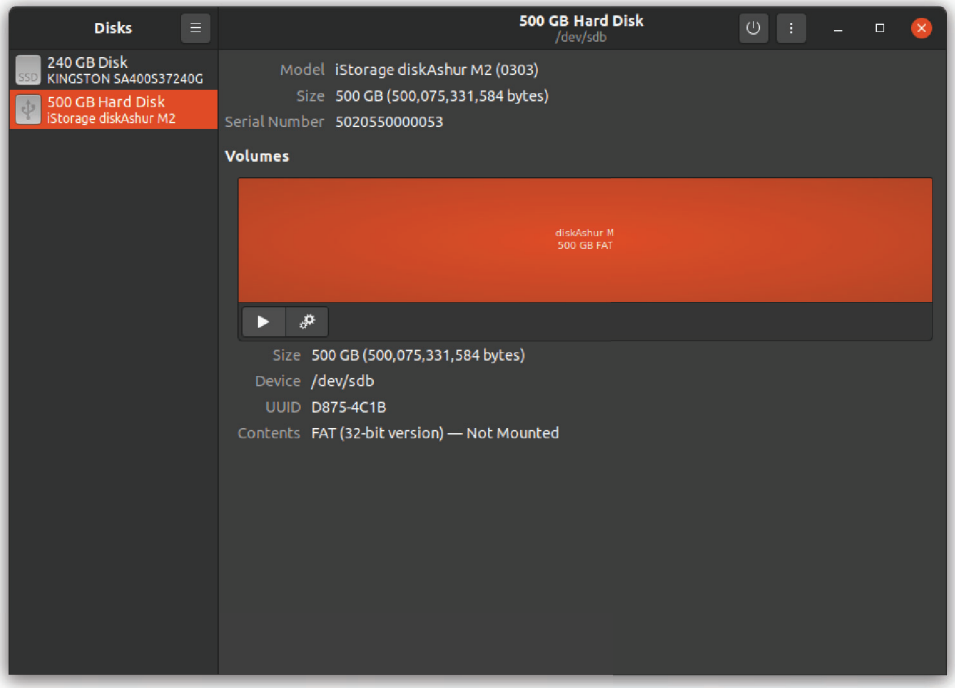


3. Wählen Sie „**Kompatibel mit allen Systemen und Geräten (FAT)**“ für die Option „**Typ**“. Und geben Sie einen Namen für das Laufwerk ein, z. B.: „diskAshur M²“. Klicken Sie dann auf die Schaltfläche „**Formatieren**“.

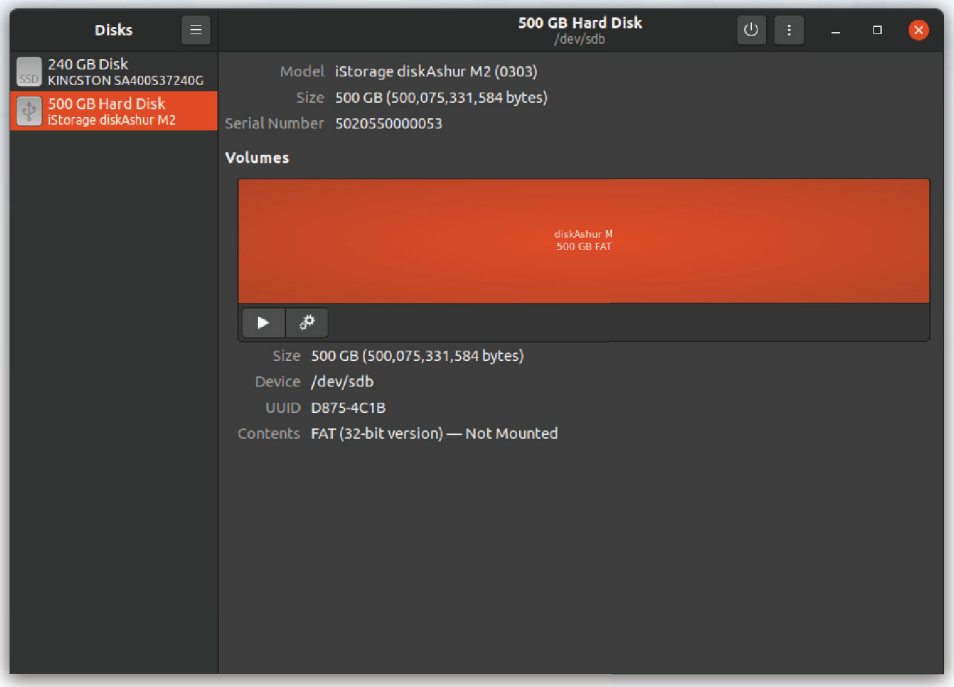




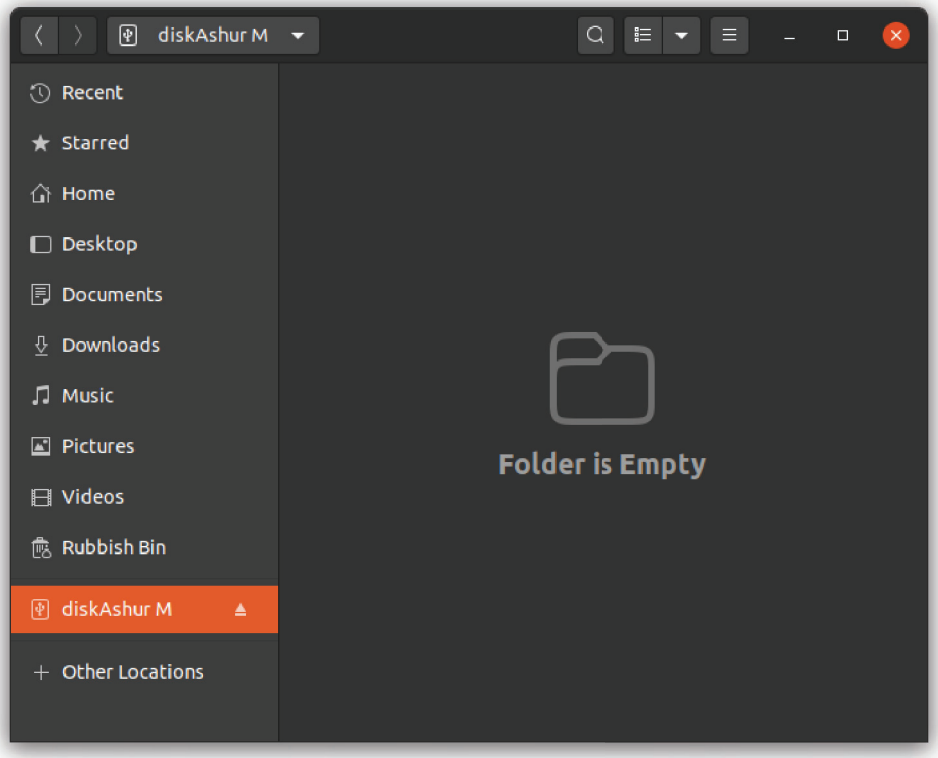
4. Nachdem der Formatierungsprozess abgeschlossen ist, klicken Sie auf die Schaltfläche „Wiedergeben“, um das Laufwerk in Ubuntu einzubinden.



5. Nun sollte das Laufwerk in Ubuntu eingebunden und einsatzbereit sein.



6. Das Laufwerk wird wie in der Abbildung unten gezeigt. Sie können auf das Laufwerkssymbol klicken, um Ihr Laufwerk zu öffnen.



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

Stellen Sie sicher, dass Sie alle Dateien auf Ihrem diskAshur M² speichern und schließen, bevor Sie es in den Ruhezustand versetzen, es anhalten oder sich vom Betriebssystem abmelden.

Es wird empfohlen, den diskAshur M² manuell zu sperren, bevor Sie den Ruhezustand aktivieren, ihn anhalten oder sich von Ihrem System abmelden.

Um das Laufwerk zu sperren, werfen Sie den diskAshur M² 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 diskAshur M² zu unvollständiger Datenübertragung und möglicherweise zu Schäden an den Daten.

⚠ **Achtung:** Damit Ihre Daten sicher sind, sollten Sie sicherstellen, dass Sie Ihren diskAshur M² sperren, wenn Sie sich nicht an Ihrem Computer befinden.

43. 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.

44. 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.

45. 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.

46. 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

Copyright © iStorage Limited 2020. Alle Rechte vorbehalten.
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

DISKASHUR® M²

iStorage®

Manuale d'uso



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 diskAshur M² si prega di contattare il nostro servizio assistenza via e-mail - support@istorage-uk.com o telefono al numero +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2020. Tutti i diritti riservati.

Windows è un marchio registrato di Microsoft Corporation.
Tutti gli altri marchi commerciali e i copyright a cui si fa riferimento sono proprietà dei rispettivi titolari.

La distribuzione di versioni modificate del presente documento è proibita senza il consenso esplicito del titolare di copyright.

La distribuzione dell'opera o derivate in qualsivoglia forma standard di libro (cartaceo) per scopi commerciali è proibita salvo espressa autorizzazione ottenuta dal titolare di copyright.

LA DOCUMENTAZIONE È FORNITA NELLA SUA VERSIONE DEFINITIVA E TUTTE LE CONDIZIONI, DICHIARAZIONI E GARANZIE, ESPRESSE O IMPLICITE, COMPRESE TUTTE LE GARANZIE IMPLICITE DI COMMERCIABILITÀ, IDONEITÀ PER UN PARTICOLARE SCOPO O GARANZIE DI NON VIOLAZIONE, SONO ESCLUSE, TRANNE NELLA MISURA IN CUI TALI ESCLUSIONI SONO RITENUTE NON VALIDE DAL PUNTO DI VISTA LEGALE

RoHS Compliant

REACH COMPLIANCE

Tutti i marchi commerciali e i copyright a cui si fa riferimento sono proprietà dei rispettivi titolari

Conforme al Trade Agreements Act (TAA)

CITRIX® vmware®

Indice

Introduzione 116
Contenuto della confezione 116
Layout DiskAshur M² 116
1. Indicatori LED e azioni corrispondenti 117
2. Stati LED 117
3. Primo utilizzo 118
4. Sblocco diskAshur M² con il PIN Amministratore 119
5. Come entrare in Modalità amministratore 119
6. Modifica del PIN Amministratore 120
7. Impostare una Politica Codice PIN Utente 121
8. Come cancellare la Politica Codice PIN Utente 122
9. Come verificare la Politica Codice PIN Utente 122
10. Aggiunta di un nuovo PIN utente in Modalità amministratore 123
11. Modifica del PIN Utente in Modalità amministratore 124
12. Cancellare il PIN utente in Modalità amministratore 124
13. Come sbloccare diskAshur M² con il PIN Utente 125
14. Modifica del PIN Utente in Modalità Utente 125
15. Creare un PIN Utente di recupero una tantum 126
16. Eliminare PIN Utente di recupero una tantum 126
17. Attivare la Modalità di Recupero e Creare un Nuovo PIN Utente 127
18. Impostare Sola Lettura Utente in Modalità amministratore 127
19. Abilitare Lettura/Scrittura Utente in Modalità amministratore 128
20. Impostare Sola Lettura Globale in Modalità amministratore 128
21. Attivare Lettura/Scrittura Utente Globale in Modalità amministratore 129
22. Come configurare un PIN Auto-Cancellabile 129
23. Come cancellare il PIN Auto-Cancellabile 130
24. Come sbloccare con il PIN Auto-Cancellabile 130
25. Come configurare un PIN Amministratore dopo un Attacco di Forza Bruta o un Reset 131
26. Impostare il Blocco Automatico Incustodito 131
27. Disattivare il Blocco Automatico Incustodito 132
28. Come verificare il Blocco Automatico Incustodito 133
29. Impostare Sola Lettura in Modalità Utente 133
30. Attivare Lettura/Scrittura in Modalità Utente 134
31. Meccanismo di Protezione da Attacco Hacker di Forza Bruta 134
32. Meccanismo di difesa contro l'hacking con forza bruta del PIN 135
33. Come impostare la Limitazione Forza Bruta del PIN Utente 135
34. Come verificare la Limitazione Forza Bruta del Pin Utente 136
35. Come eseguire un reset completo 137
36. Come configurare diskAshur M² come Avviabile 137
37. Come disabilitare la funzione Avviabile diskAshur M² 138
38. Come verificare l'impostazione Avviabile 138
39. Inizializzazione e formattazione di diskAshur M² per Windows 139
40. Inizializzazione e formattazione di diskAshur M² per Mac OS 141
41. Inizializzazione e formattazione di diskAshur M² per Linux OS 143
42. Ibernazione, Sospensione o Uscita dal Sistema Operativo 146
43. Come verificare il Firmware in Modalità amministratore 146
44. Come verificare il Firmware in Modalità Utente 147
45. Assistenza Tecnica 148
46. Garanzia e Informazioni RMA 148

Introduzione

Grazie per aver acquistato il nuovo iStorage diskAshur M², un'unità a stato solido portatile (SSD) ultra sicura e facile da usare, con hardware crittografato e autenticato con PIN, con capacità da 120GB fino a 2TB e oltre.

Progettato in base alle certificazioni FIPS 140-3 Livello 3, diskAshur M² cripta i dati in transito e a riposo, tramite la crittografia hardware AES-XTS 256-bit full disk.

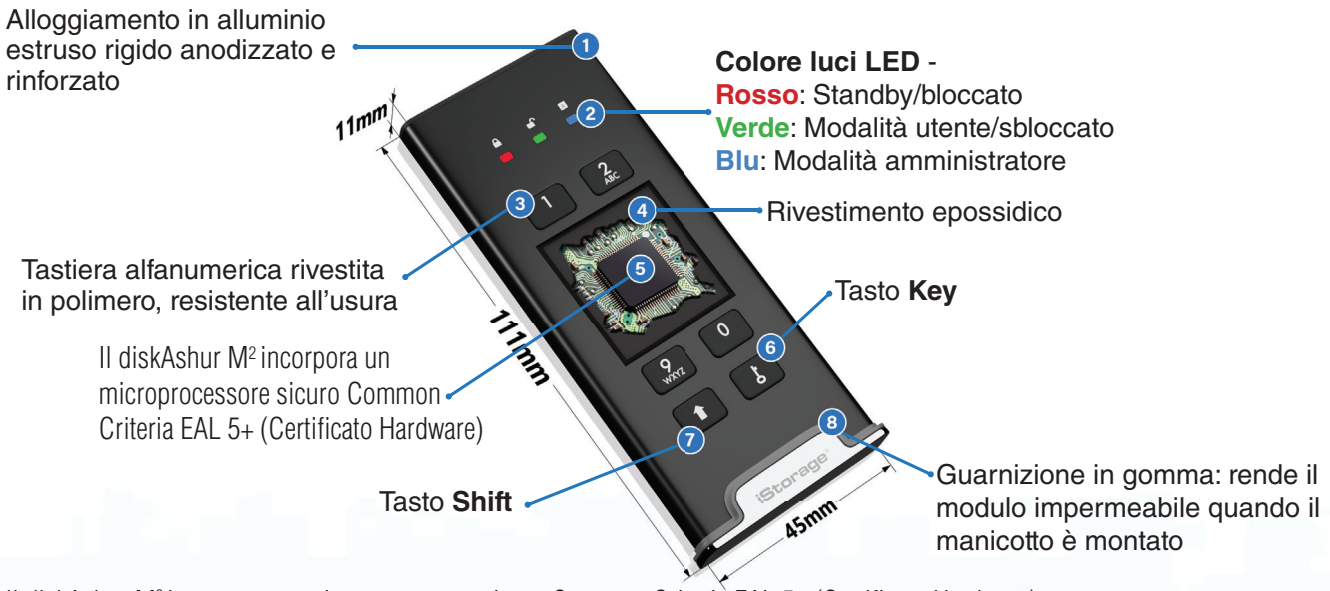
Il diskAshur M² incorpora un microprocessore sicuro Common Criteria EAL 5+ (Certificato Hardware), che impiega meccanismi di protezione fisica incorporati preposti alla difesa da manomissioni esterne, attacchi di bypass e iniezioni di guasti.

A differenza di altre soluzioni, diskAshur M² reagisce a un attacco automatico entrando nello stato di stallo congelato, che rende tutti questi attacchi inutili. In parole povere, senza il PIN non c'è modo di entrare!

Contenuto della confezione

- diskAshur M² iportatile SSD e manicotto protettivo
- custodia di trasporto
- cavi USB C e A
- guida rapida al prodotto e liberatoria

Layout diskAshur M²



Il diskAshur M² incorpora un microprocessore sicuro Common Criteria EAL 5+ (Certificato Hardware)

1. Indicatori LED e azioni corrispondenti

LED	Stato LED	Descrizione	LED	Stato LED	Descrizione
	ROSSO Fisso	Unità bloccata (in caso di stati di **Standby** o di **Reset**)		BLU Fisso	Unità in **Modalità amministratore**
	ROSSO Doppio lampeggio 	Immissione del PIN errato		LED ROSSO, VERDE e BLU che lampeggiano insieme 	In attesa dell'inserimento del PIN **Utente**
	VERDE Fisso	Unità **sbloccata**		VERDE e BLU che lampeggiano insieme 	In attesa dell'inserimento del PIN **Amministratore**
	VERDE Lampeggiante 	Trasferimento dati in corso		VERDE e BLU che lampeggiano alternativament e 	Autenticazione in corso

2. Stati LED

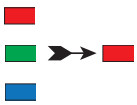


Nota: La normale funzione di diskAshur M2 può essere disturbata da forti interferenze elettromagnetiche. In questo caso, spegnere e poi accendere l'unità per riprendere il normale funzionamento. Se il normale funzionamento non riprende, utilizzare il dispositivo in una posizione diversa

Riattivare dallo Stato inattivo

Per Stato inattivo si intende lo stato in cui diskAshur M² non viene utilizzato e tutti i LED sono spenti.

Per riattivare diskAshur M² dallo stato inattivo, procedere come segue.

Collegare diskAshur M² ad una porta USB Alimentata dal computer		I LED ROSSO, VERDE e BLU lampeggiano una volta in sequenza, poi il LED VERDE lampeggia due volte e infine diventa ROSSO fisso, a indicare che l'unità è in stato di Standby

Per attivare lo Stato inattivo

Per forzare l'attivazione di diskAshur M², eseguire una delle seguenti operazioni:

- Scollegare l'unità se collegata ad una porta USB, tutti i LED si spegneranno (Stato inattivo).

Stati di accensione

Dopo che l'unità si riattiva dallo stato di inattività, entra in uno dei seguenti stati indicati nella tabella sottostante.

Stato di accensione	Indicazione LED	Chiave di crittografia	PIN Amministratore	Descrizione
Stato di spedizione iniziale	ROSSO e VERDE Fisso	✓	×	In attesa della configurazione di un PIN Amministratore (Primo utilizzo)
Standby	ROSSO Fisso	✓	✓	In attesa dell'inserimento del PIN Amministratore o PIN Utente
Reset	ROSSO Fisso	×	×	In attesa della configurazione di un PIN Amministratore

3. Primo utilizzo

diskAshur M² viene fornito nello **"Stato di spedizione iniziale", senza PIN Amministratore preimpostato**. Prima di poter utilizzare l'unità, è necessario configurare un PIN Amministratore di **7-15** cifre. Una volta che il PIN Amministratore è stato configurato con successo, non sarà più possibile riportare l'unità allo "Stato di spedizione iniziale".

Requisiti PIN:

- Deve essere di lunghezza compresa tra 7 e 15 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)

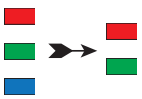
Suggerimento per la password: È possibile configurare una parola, un nome, una frase o qualsiasi altra combinazione di PIN alfanumerici facile da ricordare semplicemente premendo il pulsante con le lettere corrispondenti.

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 configurare un PIN Amministratore e sbloccare diskAshur M² per la prima volta, seguire i semplici passi illustrati nella tabella sottostante.

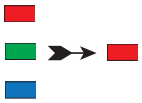
Istruzioni - Primo utilizzo	LED	Stato LED
1. Collegare diskAshur M² ad una porta USB alimentata del computer		I LED ROSSO, VERDE e BLU lampeggiano una volta in sequenza, poi il LED VERDE lampeggia due volte e infine i LED ROSSO e VERDE diventano fissi, ad indicare che l'unità è nello Stato di spedizione iniziale
2. Premere e tenere premuti entrambi i tasti **KEY (🔑) + 1**		I LED diventano VERDE lampeggiante e BLU fisso
3. Inserire un **Nuovo PIN Amministratore** (7-15 cifre) 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
4. Inserire un **Nuovo PIN Amministratore** e premere il tasto **KEY (🔑) nuovamente**		Il LED BLU lampeggia brevemente poi diventa BLU fisso e infine VERDE fisso, ad indicare che il PIN Amministratore è stato efficacemente configurato e l'unità è stata sbloccata

Blocco del diskAshur M²

Per bloccare l'unità, espellere in modo sicuro diskAshur M² dal sistema operativo host e quindi scollegarlo dalla porta USB. Se si stanno scrivendo dati sull'unità, scollegare il diskAshur M² comporterà un trasferimento di dati incompleto e una possibile corruzione dei dati.

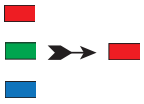
4. Sblocco diskAshur M² con il PIN Amministratore

Per sbloccare diskAshur M² con il PIN Amministratore, seguire i semplici passi illustrati nella tabella sottostante.

1. Collegare il diskAshur M² ad una porta USB sul computer		I LED ROSSO, VERDE e BLU lampeggiano una volta in sequenza, poi il LED VERDE lampeggia due volte e infine diventa ROSSO fisso, ad indicare che l'unità è in stato di Standby
2. Nello stato di Standby (LED ROSSO fisso) premere una volta il tasto **KEY (🔑)** button once		I LED VERDE e BLU lampeggiano insieme
3. Se i LED VERDE e BLU lampeggiano insieme, inserire il proprio **PIN Amministratore** e premere nuovamente il tasto **KEY (🔑)**		I LED VERDE e BLU lampeggiano più volte alternativamente poi diventano BLU fisso che diventa poi VERDE fisso, a indicare che l'unità è stata sbloccata con successo come Amministratore

5. Come entrare in Modalità amministratore

Per entrare in Modalità amministratore, procedere come segue.

1. Collegare diskAshur M² ad una porta USB alimentata del computer		I LED ROSSO, VERDE e BLU lampeggiano una volta in sequenza, poi il LED VERDE lampeggia due volte e infine diventa ROSSO fisso, ad indicare che l'unità è in stato di Standby
2. In stato di Standby (LED ROSSO fisso) Premere e tenere premuti entrambi i tasti **KEY (🔑) + 1**		I LED VERDE e BLU lampeggiano insieme
3. Inserire il **PIN Amministratore** e premere il tasto **KEY (🔑)** una volta		I LED VERDE e BLU lampeggiano insieme più volte e diventano VERDE fisso e infine BLU fisso, a indicare che l'unità è in Modalità amministratore

Per uscire dalla Modalità amministratore

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.

6. Modifica del PIN Amministratore

Requisiti PIN:

- Deve essere di lunghezza compresa tra 7 e 15 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)

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), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa 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 7 a 15 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 7-15 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 7-15 digit PIN.
- È possibile utilizzare più di un "Carattere speciale" e posizionarlo lungo il PIN a 7-15 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 7-15 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. Come cancellare la Politica Codice PIN Utente

Per cancellare 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 KEY **(🔑) + 7**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Inserire **070** e premere una volta il tasto **SHIFT** (⬆) button once		I LED VERDE e BLU lampeggianti diventano VERDE fisso e infine BLU fisso, a indicare che la Politica Codice PIN Utente è stata eliminata 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.

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

Importante: La creazione di un Nuovo 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.

Requisiti PIN:

- Deve essere di lunghezza compresa tra 7 e 15 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

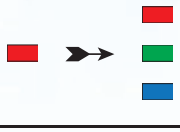
Per cancellare un PIN Utente esistente, occorre prima entrare in "**Modalità amministratore**" come descritto nella sezione 5. Una volta che l'unità è in **Modalità amministratore** (LED BLU fisso) procedere come segue.

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.

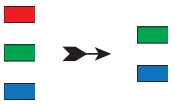
13. Come sbloccare diskAshur M² con il PIN Utente

Per sbloccare diskAshur M² con il PIN utente, procedere come segue.

1. In stato di Standby (LED ROSSO fisso) Premere e tenere premuti entrambi i tasti **SHIFT** (⬆) **+ KEY (⚷)**		Il LED ROSSO viene sostituito da tutti i LED ROSSO, VERDE & BLU che lampeggiano e si spengono
2. Inserire il **PIN Utente** e premere una volta il tasto **KEY (⚷)**		I LED ROSSO, VERDE e BLU lampeggianti diventano alternativamente VERDE e BLU e infine VERDE fisso, a indicare che l'unità è stata sbloccata con successo in Modalità utente

14. Modifica del PIN Utente in Modalità Utente

Per modificare il **PIN Utente**, sbloccare prima il diskAshur M² con il PIN 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 (LED VERDE fisso) Premere e tenere premuti entrambi i tasti **KEY (⚷) + 4**		Il LED VERDE fisso viene sostituito da tutti i LED ROSSO, VERDE & BLU che lampeggiano e si spengono
2. Inserire il PIN Utente Attuale e premere il tasto **KEY (⚷)** una volta		I LED VERDE e BLU fissi si attivano e disattivano alternativamente e poi lampeggiano una volta in VERDE prima di ridiventare VERDE lampeggiante e BLU fisso
3. Inserire il **Nuovo PIN Utente** e premere il tasto **KEY (⚷)** una volta		I LED VERDE lampeggiante e BLU fisso lampeggiano una volta in VERDE poi ridiventano VERDE lampeggiante e BLU fisso
4. 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 VERDE fisso, a indicare che il PIN Utente è stato modificato con successo

Importante: La modifica del PIN Utente in Modalità Utente (LED VERDE) 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".

15. Creare un PIN Utente di recupero una tantum

Il Pin Utente di recupero è estremamente utile in situazioni in cui l'utente ha dimenticato il proprio PIN per sbloccare diskAshur M². Per attivare la modalità di recupero, l'utente deve prima inserire il PIN Utente di recupero una tantum corretto, se è stato configurato. Il processo di recupero del PIN Utente non influisce sui dati, sulla chiave di cifratura e sul PIN Amministratore; tuttavia, l'utente è costretto a configurare un nuovo PIN utente di 7-15 cifre.

Per configurare un PIN Utente di recupero una tantum di 7-15 cifre, 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 (🔑) + 4**		Il LED BLU fisso sarà sostituito da LED VERDE lampeggiante e BLU fisso
2. Inserire un **PIN di recupero una tantum** 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 un **PIN di recupero una tantum** e premere nuovamente il tasto **KEY (🔑)**		I LED VERDE lampeggiante e BLU fisso diventano VERDE che lampeggia rapidamente e infine BLU fisso, a indicare che il PiN di recupero una tantum 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.

16. Eliminare PIN Utente di recupero una tantum

Per cancellare un PIN Utente di recupero una tantum, 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** (⬆) **+ 4**		Il LED BLU fisso diventa ROSSO lampeggiante
2. Premere e tenere premuti entrambi i tasti **SHIFT** (⬆) **+ 4** di nuovo		Il LED ROSSO lampeggiante diventa ROSSO fisso e poi BLU fisso , indicare che il PIN Utente di recupero è 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.

17. Attivare la Modalità di Recupero e Creare un Nuovo PIN

Il Pin Utente di recupero è estremamente utile in situazioni in cui l'utente ha dimenticato il proprio PIN per sbloccare diskAshur M². Per attivare la modalità di recupero, l'utente deve prima inserire il PIN Utente di recupero una tantum corretto, se è stato configurato. Il processo di recupero del PIN Utente non influisce sui dati, sulla chiave di cifratura e sul PIN Amministratore; tuttavia, l'utente è costretto a configurare un nuovo PIN utente di 7-15 cifre.

Per attivare il processo di ripristino e configurare un nuovo PIN Utente, procedere come segue.

1. In **Stato di standby** (LED ROSSO) premere e tenere premuti entrambi I tasti **KEY (🔑) + 4**		Il LED ROSSO fisso si trasformerà in LED ROSSO e VERDE lampeggianti
2. Inserire il **PIN di recupero una tantum** e premere il tasto **KEY (🔑)**		I LED VERDE e BLU si attivano e disattivano alternativamente per poi diventare VERDE fisso e infine a VERDE lampeggiante e BLU fisso
3. Inserire un **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
4. Reinserire il Nuovo **PIN Utente e premere** nuovamente il tasto **KEY (🔑)** button again		Il LED VERDE lampeggia rapidamente, poi diventa VERDE fisso, indicando che il processo di recupero è andato a buon fine e che è stato configurato un nuovo PIN utente

Importante: La creazione di un Nuovo 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. Fare riferimento alla sezione 9 per verificare le restrizioni del PIN Utente.

18. Impostare Sola Lettura Utente in Modalità

Poiché i virus e trojan che infettano le unità USB sono molti, la funzione di sola lettura è particolarmente utile se si necessita di accedere ai dati sull'unità USB mentre si è in un ambiente pubblico. Questa è una caratteristica essenziale anche a fini forensi, dove i dati devono essere conservati allo stato originale e inalterati, senza potere essere modificati e sovrascritti.

Quando l'Amministratore configura diskAshur M² e limita l'accesso dell'utente in modalità Sola Lettura Utente, allora solo

l'Amministratore può scrivere sull'unità o modificare l'impostazione in Lettura/Scrittura come descritto nella sezione 19. L'accesso Utente è limitato alla modalità Sola Lettura; l'Utente non può scrivere sull'unità o modificare questa impostazione in modalità utente.

Per impostare diskAshur M² e limitare l'accesso dell'Utente alla Sola Lettura 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 "**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.

19. Abilitare Lettura/Scrittura Utente in Modalità

Per reimpostare diskAshur M² 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.

20. Impostare Sola Lettura Globale in Modalità

Quando l'Amministratore configura diskAshur M² e lo limita alla Sola Lettura Globale, allora né l'Amministratore né l'Utente possono scrivere sull'unità e l'accesso di entrambi è limitato alla Sola Lettura. Solo l'Amministratore è in grado di reimpostare l'impostazione in Lettura/Scrittura come descritto nella sezione 21.

Per impostare diskAshur M² e limitare l'accesso globale alla Sola Lettura, 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 "**5 + 6**".		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. il tasto **KEY (🔑)**		I LED VERDE e BLU diventano VERDE fisso e poi BLU fisso che indica che l'unità è stata configurata e limita l'accesso globale alla 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.

21. Attivare Lettura/Scrittura Globale in Modalità

Per reimpostare diskAshur M² e consentire la Lettura/Scrittura a partire dalla Sola Lettura Globale, 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 "**5 + 9**".		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. 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. Come configurare un PIN Auto-Cancellabile

È possibile configurare un PIN auto.cancellabile che, una volta inserito, esegue una cripto-cancellazione sull'unità (la chiave di crittografia viene cancellata). Questo processo cancella tutti i PIN configurati e rende tutti i dati memorizzati sull'unità inaccessibili (persi per sempre); l'unità verrà quindi visualizzata come LED VERDE sbloccato. L'esecuzione di questa funzione fa sì che il PIN Auto-Cancellabile diventi il Nuovo PIN Utente e l'unità dovrà essere formattata prima di poter essere riutilizzata.

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 7-15 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.

23. 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.

24. Come Sbloccare con il PIN Auto-Cancellabile

Avvertenza: Quando il meccanismo di autocancellazione viene attivato, tutti i dati, la chiave di cifratura e i PIN dell'amministratore/utente vengono cancellati. **Il PIN Auto-Cancellabile diventa il PIN Utente**. Dopo l'attivazione del meccanismo di autodistruzione non esiste più alcun PIN Amministratore. DiskAshur M² dovrà essere precedentemente resettato (vedere 'Come eseguire un reset completo' Sezione 35, a pagina 137) per configurare un PIN Amministratore con tutti i privilegi di amministrazione, compresa la possibilità di configurare un Nuovo PIN Utente.

Quando viene utilizzato, il PIN Auto-Cancellabile **cancellerà TUTTI i dati, i PIN Amministratore/Utente**, e quindi sbloccherà l'unità. L'attivazione di questa funzione farà sì che il **PIN Auto-Cancellabile diventi il Nuovo PIN Utente** e diskAshur M² dovrà essere formattato prima di poter aggiungere nuovi dati all'unità.

Per attivare il meccanismo di Auto-Cancellazione, l'unità deve trovarsi in stato di standby (LED ROSSO fisso) e occorre poi procedere come segue.

1. In **Stato di standby** (LED ROSSO fisso), premere e tenere premuti entrambi i pulsanti **SHIFT** (⬆) + **KEY** (🔑)		Il LED ROSSO viene sostituito da tutti i LED ROSSO, VERDE & BLU che lampeggiano e si spengono
2. Inserire il **Pin Auto-Cancellabile** e premere il tasto **KEY** (🔑) button		I LED ROSSO, VERDE e BLU lampeggianti diventano VERDE e BLU alternandosi per alcuni secondi e diventano infine VERDE fisso, a indicare che diskAshur M² si è autodistrutto con successo.

25. Come configurare un PIN Amministratore dopo un Attacco

Dopo un Attacco di Forza Bruta o quando diskAshur M² è stato resettato occorre configurare un PIN Amministratore prima di potere utilizzare l'unità.

Requisiti PIN:

- Deve essere di lunghezza compresa tra 7 e 15 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)

Se diskAshur M² 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.

26. Impostare il Blocco Automatico Incustodito

Per proteggersi da accessi non autorizzati se l'unità è sbloccata e incustodita, diskAshur M² 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 diskAshur M² 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.

27. 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.

28. 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.

29. Impostare Sola Lettura in Modalità Utente

Per impostare diskAshur M² 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.

30. Attivare Lettura/Scrittura in Modalità Utente

Per impostare diskAshur M² 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.

31. Meccanismo di protezione da attacco di forza bruta

diskAshur M² incorpora un meccanismo di difesa per proteggere l'unità contro gli Attacchi di Forza Bruta. Di default, i valori dello stato di spedizione iniziale per la limitazione di forza bruta (immissione consecutiva di PIN errati) sia per il PIN di amministrazione che per il PIN Utente corrispondono a **10** e **5** per il PIN di recupero. Tre contatori indipendenti di forza bruta vengono utilizzati per registrare i tentativi non corretti per ogni autorizzazione PIN (Amministratore, Utente e di Recupero) come indicato di seguito.

- Se un utente inserisce un PIN Utente errato per 10 volte consecutive, il PIN Utente verrà cancellato, ma i dati, il PIN Amministratore e il PIN di recupero rimangono intatti e accessibili.
- Se un utente inserisce un PIN di recupero errato per 5 volte consecutive, il PIN di recupero verrà cancellato, ma i dati e il PIN Amministratore rimangono intatti e accessibili.
- Se viene immesso un PIN Amministratore errato per 10 volte consecutive, l'unità si resetta. Tutti i PIN e i dati vengono cancellati e persi per sempre.

La tabella seguente presuppone che tutti e tre i PIN siano stati impostati ed evidenzia l'effetto dell'attivazione del meccanismo di difesa dalla forza bruta di ogni singolo PIN.

PIN utilizzato per sbloccare l'unità	Immissioni errate consecutive di PIN	Descrizione di ciò che accade
PIN utente	10	• Il PIN utente viene cancellato. • Il PIN di recupero, il PIN Amministratore e tutti i dati rimangono intatti e accessibili.
Recupero PIN	5	• Il PIN di recupero viene cancellato. • Il PIN Amministratore e tutti i dati rimangono intatti e accessibili.
PIN Amministratore	10	• diskAshur M² si resetta. Tutti i PIN e i dati vengono cancellati e persi per sempre.

Nota: La limitazione della forza bruta viene impostata di default sui valori dello stato di spedizione iniziale quando l'unità viene completamente resettata, oppure se la funzione di auto-cancellazione è attivata o sottoposta ad attacco di forza bruta. Se l'Amministratore modifica il PIN Utente o viene impostato un Nuovo PIN Utente all'attivazione della funzione di recupero, il contatore della forza bruta del PIN Utente viene azzerato (0), senza che venga tuttavia alterata la limitazione della forza bruta. Se l'Amministratore modifica il PIN di recupero, il contatore di forza bruta del PIN di recupero viene azzerato.

L'autorizzazione riuscita di un determinato PIN azzererà il contatore di forza bruta per quel particolare PIN, ma non influirà sugli altri PIN del contatore di forza bruta. La mancata autorizzazione di un determinato PIN farà aumentare il conteggio del contatore di forza bruta per quel particolare PIN, ma non influirà sugli altri PIN del contatore di forza bruta.

32. Meccanismo di difesa contro l'hacking con forza bruta del PIN

Il PIN amministratore della diskAshur M² è dotato di un meccanismo di difesa più sofisticato rispetto al PIN utente o al PIN di ripristino; tale meccanismo ha lo scopo di proteggere dall'inserimento accidentale di un PIN amministratore errato per 10 volte consecutive e dalla conseguente perdita di tutti i dati. Pertanto, dopo 5 immissioni consecutive errate del PIN amministratore, la diskAshur M² si bloccherà e tutti i LED si accenderanno e le luci resteranno fisse.

AVVERTENZA: non seguire le seguenti istruzioni se intendi sbloccare la diskAshur M² utilizzando solo il **PIN UTENTE** e non conoscendo il **PIN AMMINISTRATORE**.

Fare riferimento alle istruzioni presenti nella tabella sottostante per abilitare ulteriori immissioni del PIN amministratore fino a un massimo di 10.

Inserimenti consecutivi errati del PIN amministratore	Descrizione di ciò che accade alla diskAshur M²	Istruzioni
5	I LED, **ROSSO**, **VERDE** e **BLU** si accendono e le luci restano fisse.	Inserire il seguente PIN '**47867243**' e premere il **TASTO (⚷)** una volta, quando entrambi i LED **VERDE** e **BLU** cominceranno a lampeggiare alternativamente, la diskAshur M² sarà pronta ad accettare l'immissione di altri **3 PIN amministratore** .
8	I LED, **ROSSO**, **VERDE** e **BLU** lampeggiano alternativamente.	Inserire il seguente PIN '**47867243**' e premere il **TASTO (⚷)** una volta, quando entrambi i LED **VERDE** e **BLU** cominceranno a lampeggiare alternativamente, la diskAshur M² sarà pronta ad accettare l'immissione di altri **2 PIN amministratore**.
10	Il LED **ROSSO** si accenderà e rimarrà fisso.	Dopo un totale di 10 immissioni errate del PIN amministratore, la chiave di crittografia, tutti i PIN e i dati verranno eliminati e persi per sempre.

33. Come impostare la Limitazione Forza Bruta del PIN

Nota: L'impostazione di limitazione della forza bruta del PIN Utente viene impostata di default su 10 immissioni errate consecutive del PIN quando l'unità viene sottoposta a reset completo, forzato con forza bruta o viene attivato il PIN Auto-Cancellabile.

La limitazione della forza bruta per il PIN Utente diskAshur M² può essere riprogrammata e impostata dall'amministratore. Questa funzione può essere impostata per consentire 1 a 10 tentativi errati di immissione del PIN consecutivi.

Per configurare la Limitazione Forza Bruta del 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 **7 + 0**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU che lampeggiano insieme
2. Inserire il numero di tentativi per la limitazione della forza bruta (tra 01 e 10); ad esempio inserire: • **01** per 1 tentativo • **10** per 10 tentativi		
3. Premere una volta il tasto **SHIFT** (⬆)		I LED VERDE e BLU lampeggianti diventano VERDE fisso per un secondo e poi BLU fisso, a indicare che la limitazione della forza bruta è stata configurata 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.

34. Come verificare la Limitazione Forza Bruta del Pin

L'Amministratore può osservare e determinare il numero di volte consecutive in cui è consentito l'inserimento di un PIN Utente errato prima di attivare il meccanismo di difesa della forza bruta, semplicemente annotando la sequenza di LED come descritto di seguito.

Per verificare la limitazione della Forza Bruta, 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 **2** + **0**		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 del numero di limitazioni della forza bruta. c. Ogni lampeggio del LED VERDE equivale ad una (1) singola unità di un numero di limitazione della forza bruta. d. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo. e. I LED ritornano al BLU fisso		

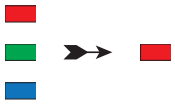
La tabella seguente descrive il comportamento dei LED durante il controllo dell'impostazione della limitazione della forza bruta; ad esempio se si è impostata l'unità in modo da attivare la forzatura con forza bruta dopo **5** immissioni errate consecutive del PIN, il LED VERDE lampeggerà cinque (**5**) volte.

Impostazione della limitazione della forza bruta	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), premere e tenere premuto il tasto **SHIFT** (⬆) per un secondo - il LED BLU fisso diventa ROSSO fisso.

35. Come eseguire un reset completo

Per eseguire un reset completo, diskAshur M² 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 diskAshur M², 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 25 a pagina 131 su "Come configurare un PIN Amministratore dopo un Attacco di Forza Bruta o un Reset". Inoltre, diskAshur M² dovrà essere formattato prima di poter aggiungere nuovi dati all'unità.

36. Come configurare diskAshur M² come Avviabile

Nota: Quando l'unità è impostata come avviabile, l'espulsione dell'unità stessa dal sistema operativo non farà diventare il LED ROSSO. L'unità rimane VERDE fissa e dovrà essere scollegata per l'utilizzo successivo. L'impostazione predefinita di diskAshur M² è configurata come non avviabile.

diskAshur M² è dotato di una funzione di avviabilità che consente di gestire i cicli di alimentazione durante i processi di avvio dell'host. Quando si avvia da diskAshur M², il computer è in esecuzione secondo il sistema operativo installato su diskAshur M².

Per impostare l'unità come avviabile, 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 (🔑) + 8**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premere **"0"** fseguito da un **"1"** (**01**)		I LED VERDE e BLU 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 l'unità è stata configurata come avviabile 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.

37. Come disattivare la funzione Avviabile di diskAshur M²

Per disattivare la funzione Avviabile di diskAshur M², 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 (🔑) + 8**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti
2. Premere **"0"** seguito da un altro **"0"** (**00**)		I LED VERDE e BLU 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 funzione avviabile è stata disattivata 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.

38. Come verificare l'impostazione Avviabile

Per verificare l'impostazione avviabile, 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** (⬆) **+ 8**		Il LED BLU fisso sarà sostituito da LED VERDE e BLU lampeggianti

2. Premere il tasto **KEY (🔑)** e si verificherà uno dei due scenari seguenti;

- **Se diskAshur M² è configurato come Avviabile, succede quanto segue;**

a. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo.
b. Il LED VERDE lampeggia una volta.
c. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo.
d. I LED ritornano al BLU fisso

- **Se diskAshur M² è configurato come Avviabile, succede quanto segue;**

a. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo.
b. Tutti i LED sono spenti
c. Tutti i LED (ROSSO, VERDE & BLU) diventano fissi per 1 secondo.
d. I LED ritornano al BLU 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.

39. Inizializzazione e formattazione di diskAshur M² per Windows

Dopo un a"Attacco di Forza Bruta" o un reset completo, diskAshur M² cancellerà tutti i PIN, i dati e la chiave di crittografia. È necessario inizializzare e formattare diskAshur M² prima di poterlo utilizzare.

Per formattare diskAshur M² procedere come segue:

1. Configurare un nuovo PIN Amministratore; vedi pagina 131, sezione 25, "Come configurare un PIN Amministratore dopo un Attacco di Forza Bruta o un Reset".

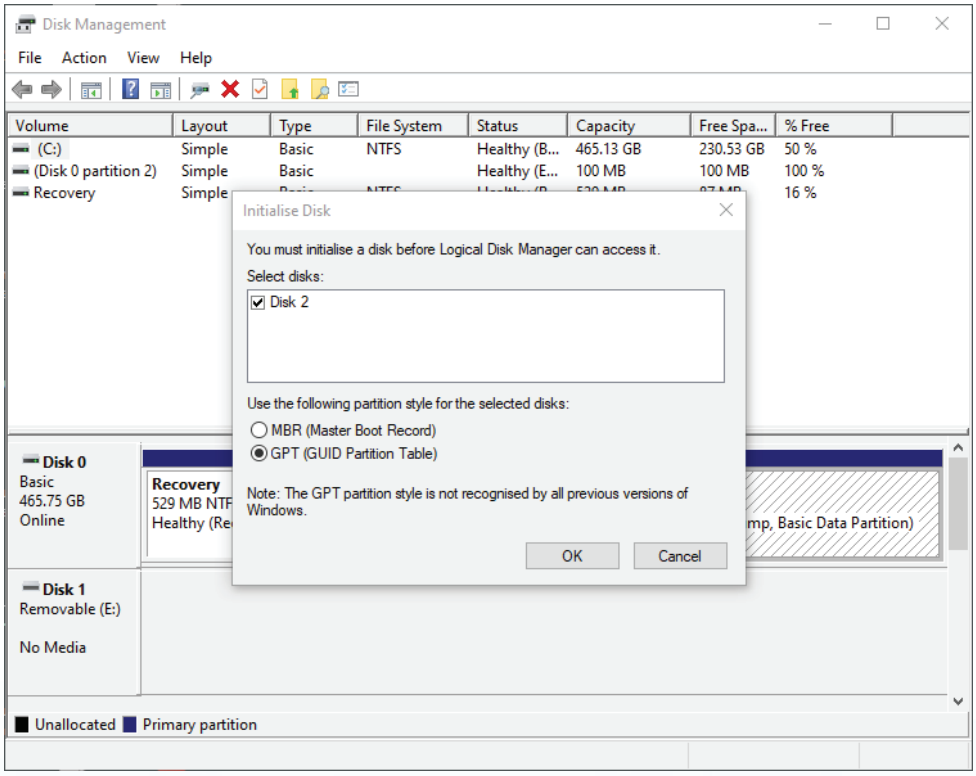
2. Con diskAshur M² in stato di standby (LED ROSSO), premere una volta il tasto **KEY (⚷)** e inserire il Nuovo PIN Amministratore per sbloccarlo (LED VERDE lampeggiante).

3. Collegare diskAshur M² al computer.

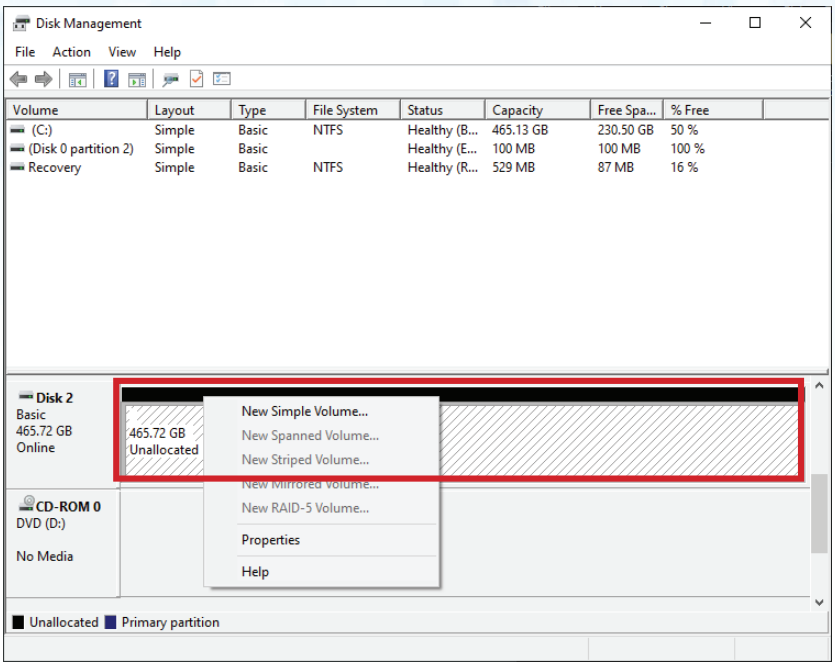
4. **Windows 7:** Fare clic con il tasto destro del mouse su **Computer**, quindi fare clic su **Gestisci** e quindi selezionare **Gestione disco**
   Windows 8: Cliccare con il tasto destro del mouse sull'angolo sinistro del desktop e selezionare **Gestione disco**
   Windows 10: Cliccare con il tasto destro del mouse sul tasto di avvio e selezionare **Gestione disco**

5. Nella finestra Gestione disco, diskAshur M² è riconosciuto come dispositivo sconosciuto, non inizializzato e non allocato. Dovrebbe apparire una finestra di dialogo che invita a scegliere lo stile di partizione MBR o GPT. GPT memorizza più duplicati di questi dati sul disco, di conseguenza è molto più robusto. Invece su un disco MBR, le informazioni di partizione e di avvio sono memorizzate in un'unica sede.

   Selezionare lo stile di partizione e fare clic su **OK**.



6. Cliccare con il tasto destro del mouse nell'area vuota sopra la sezione **Non Allocato**, quindi selezionare **Nuovo Volume Semplice.**



7. Si apre la finestra del Wizard di benvenuto in Nuovo Volume semplice. Fare clic su Avanti.



8. Se è necessaria una sola partizione, accettare la dimensione predefinita di partizione e fare clic su **Avanti**.

9. Assegnare una lettera di unità o un percorso e fare clic su **Avanti**.

10. Creare un'etichetta di volume, selezionare Esegui un formato rapido, quindi fare clic su **Avanti**.

11. Fare clic su **Fine**.

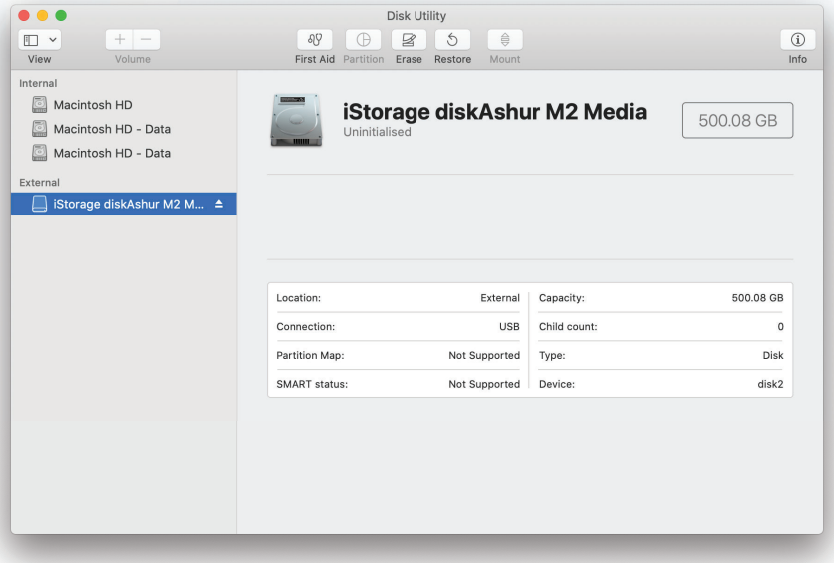
12. Attendere il completamento del processo di formattazione. diskAshur M² sarà riconosciuto ed è disponibile per l'uso.

40. Inizializzare e formattare diskAshur M² in Mac OS

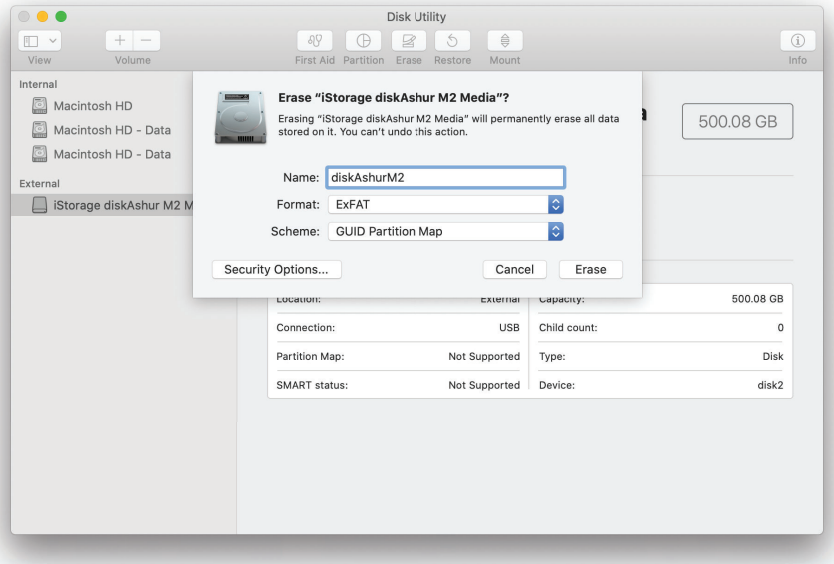
Dopo un "Attacco di Forza Bruta" o un reset completo, diskAshur M² cancellerà tutti i PIN, i dati e la chiave di crittografia. È necessario inizializzare e formattare diskAshur M² prima di poterlo utilizzare.

Per inizializzare e formattare diskAshur M²:

1. Selezionare diskAshur M² dall'elenco delle unità e dei volumi. In corrispondenza di ogni unità della lista verranno mostrati dati quali la capacità, il produttore e il nome del prodotto, come "**iStorage diskAshur M² Media**".



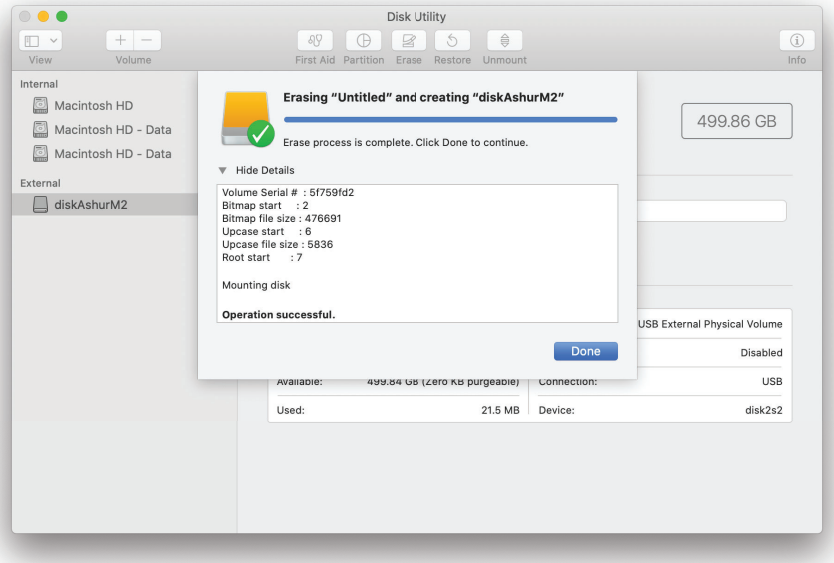
2. Fare clic sul pulsante "**Cancella**" alla voce utilità Disco.
3. Inserire un nome per l'unità. Il nome predefinito è Untitled. Il nome dell'unità apparirà infine sul desktop.



4. Selezionare uno schema e il formato del volume da utilizzare. Il menu a discesa Formato contiene un elenco di formati di unità disponibili supportati da Mac. Il tipo di formato raccomandato è “Mac OS Extended (Journaled)”. Per utilizzo su piattaforme trasversali selezionare exFAT. Il menu a discesa del formato dello schema contiene una lista degli schemi disponibili da utilizzare. Si consiglia di utilizzare la “Mappa partizione GUID” su unità di dimensioni superiori a 2 TB.

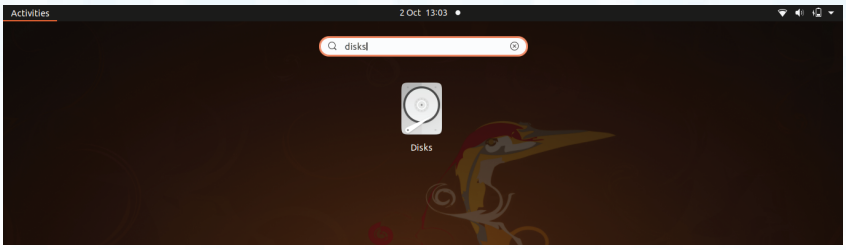


5. Fare clic sul pulsante “Cancella”. Utilità disco smonterà il volume dal desktop, lo cancellerà e poi lo rimonterà sul desktop.

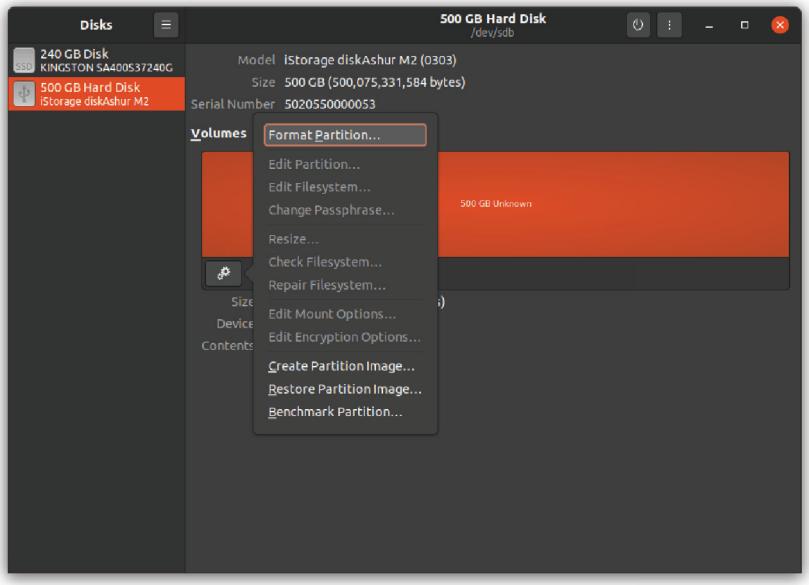


41. Inizializzazione e formattazione di diskAshur M² in Linux

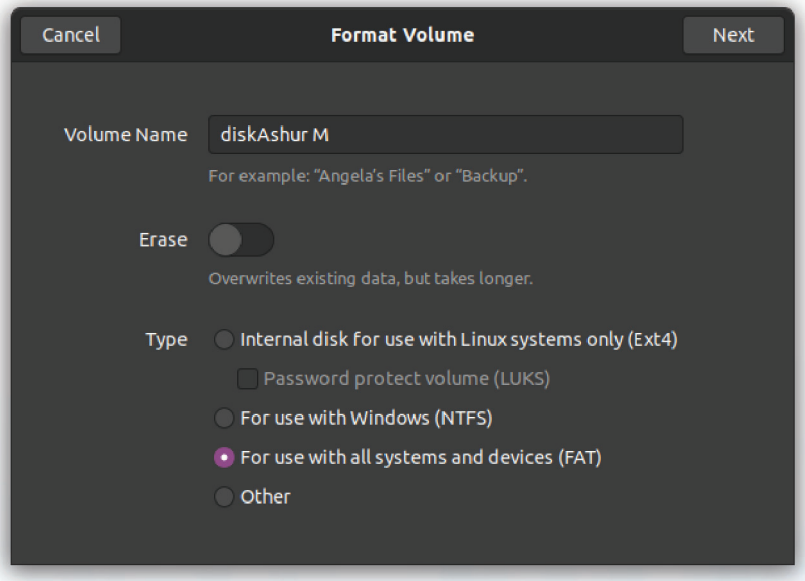
1. Aprire "**Mostra applicazione**" e digitare "**Dischi**""nella casella di ricerca. Fare clic sull'utilità "**Dischi**" quando viene visualizzata.



2. Fare clic per selezionare l'unità (Hard Disk da 500 GB) alla voce "**Dispositivi**". Fare clic poi sull'icona degli ingranaggi sotto "**Volumi**" e poi cliccare su "**Formato Partizioni**".

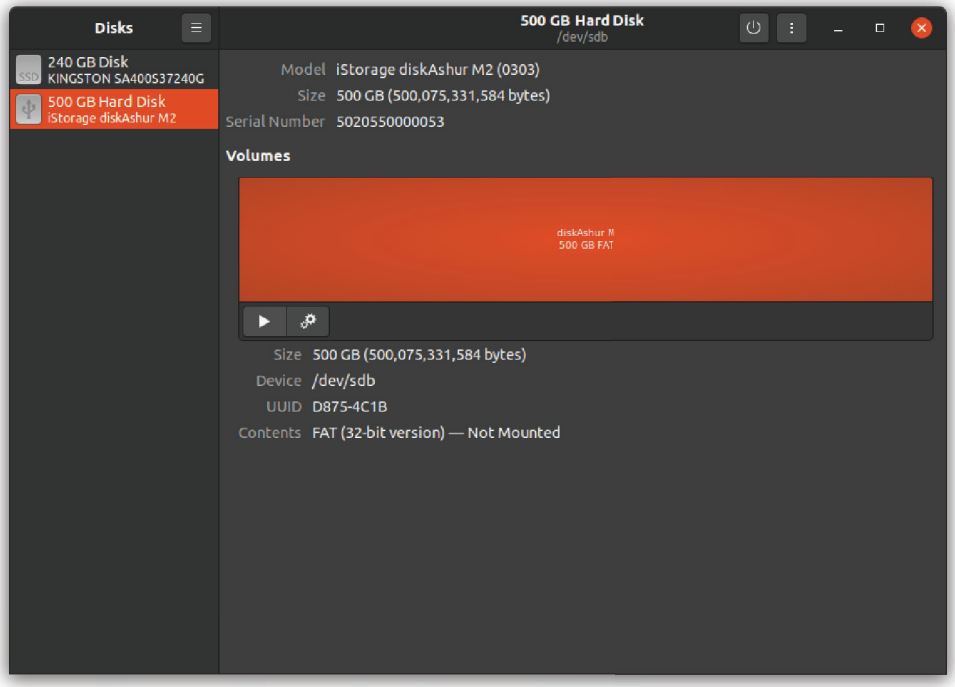


3. Selezionare "**Compatibile con tutti i sistemi e dispositivi (FAT)**" per l'opzione "**Tipo**". E inserire un nome per l'unità, ad esempio: diskAshur M². Quindi, fare clic sul pulsante "**Formato**".

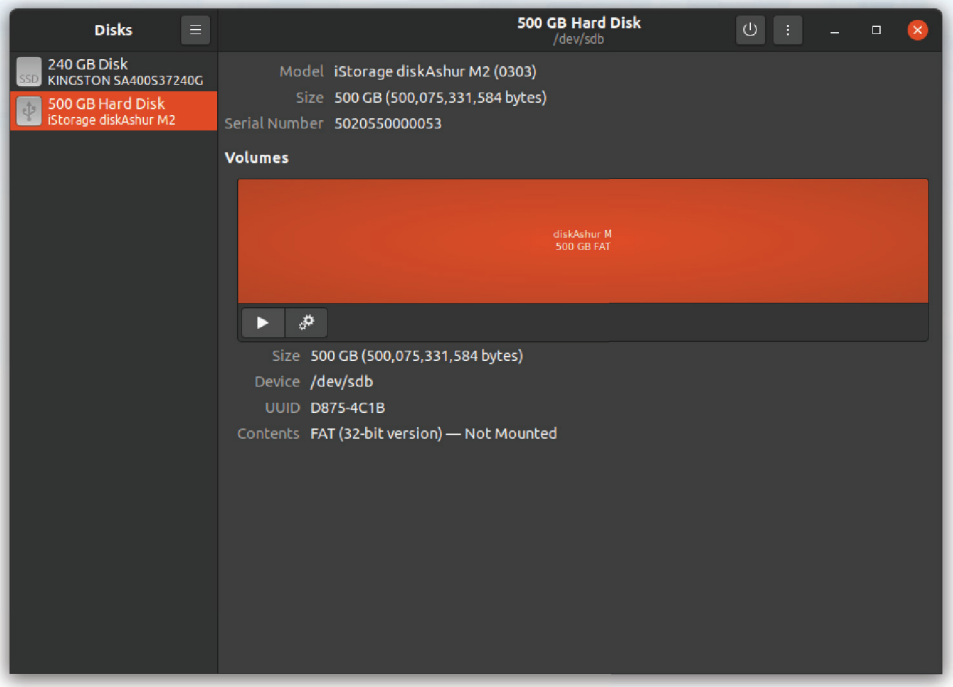




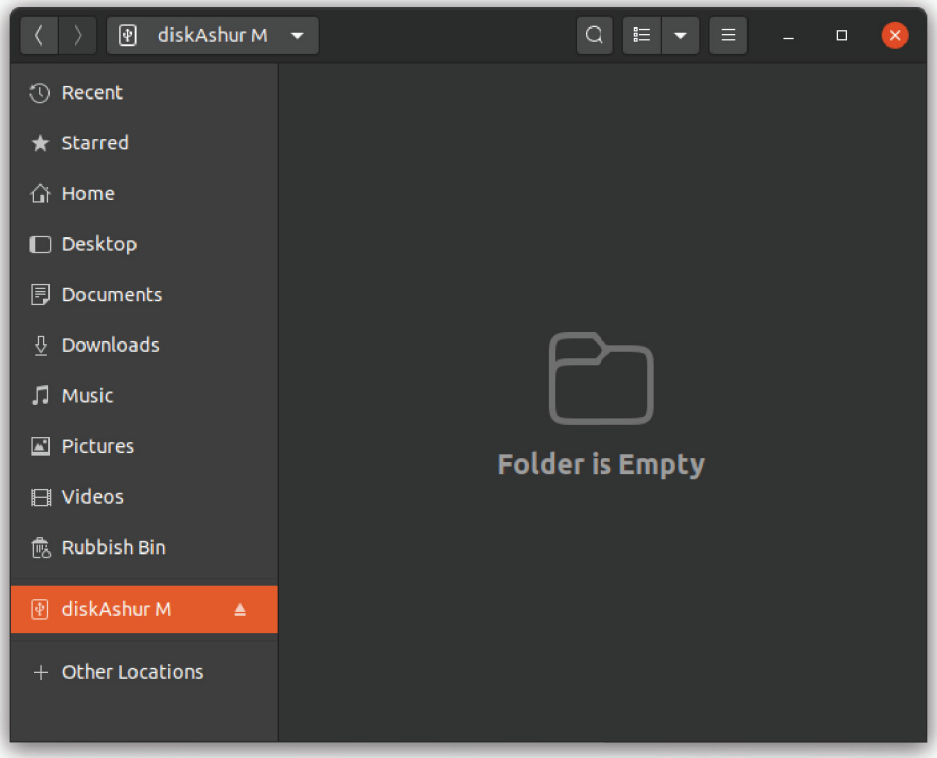
4. Al termine del processo di formattazione, fare clic sul pulsante Play per montare l'unità su Ubuntu.



5. Ora l'unità dovrebbe essere stata montata su Ubuntu e pronta all'uso.



6. Il disco verrà visualizzato come nell'immagine qui sotto. È possibile fare clic sull'icona del disco per aprire l'unità.



42. Ibernazione, Sospensione o Uscita dal Sistema Operativo

Accertarsi di salvare e chiudere tutti i file su diskAshur M² prima di ibernare, sospendere o uscire dal sistema operativo.

Si raccomanda di bloccare manualmente diskAshur M² prima di ibernare, sospendere o uscire dal sistema.

Per bloccare l'unità, espellere in modo sicuro diskAshur M² dal sistema operativo host e quindi scollegarlo dalla porta USB. Se si stanno scrivendo dati sull'unità, scollegare diskAshur M² comporterà un trasferimento di dati incompleto e una possibile corruzione dei dati.

⚠ **Attenzione:** Per garantire la sicurezza dei dati, accertarsi di bloccare diskAshur M² se ci si allontana dal proprio computer.

43. 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.

44. 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.

45. 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.

46. 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

Copyright © iStorage Limited 2020. Tutti i diritti riservati.
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

DISKASHUR® M²

iStorage®

ユーザーガイド



iStorage diskAshur® M² User Manual v3.0

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。

diskAshurM²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。

著作権©iStorageで、2020年株式会社.無断複写・転載を禁じます。
ウィンドウズは、マイクロソフトの登録商標です。
記載されているその他すべての商標および著作権は、それぞれの所有者に帰属します。
このドキュメントの変更されたバージョンの配布は、著作権所有者の明示的な許可なしに禁止されています。著作権者の事前の許可なしに、作品または派生物を標準的な本（紙）形式で商業目的で配布することは禁止されています。
ドキュメントは現状のまま提供され、すべての明示的または黙示的な条件、表現、および
商品性、特定への適合性の黙示の保証
これらの免責事項が法的に無効である場合を除き、目的または非侵害は否認されるものとします。。
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

RoHS Compliant

REACH COMPLIANCE

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 153
箱入り 153
diskAshur M²レイアウト 153
1. LEDインジケータとその動作 154
2. LEDの状態 154
3. 初めて 使用 155
4. 管理者ピンを使用してdiskAshurM²のロックを解除する 156
5. **管理者モードに入る方法** 156
6. 管理者ピンを変更する 157
7. ユーザーピンポリシーの設定 158
8. ユーザーピンポリシーを削除する方法 159
9. ユーザーピンポリシーの確認方法 159
10. 管理者モードでの新しいユーザーピンの追加 160
11. 管理者でユーザーピンを変更します 161
12. 管理者モードでのユーザーピンの削除 161
13. ユーザーピンを使用してdiskAshurM²のロックを解除する方法 162
14. ユーザーモードでのユーザーピンの変更 162
15. ワンタイムユーザーリカバリピンを作成する 163
16. ワンタイムユーザーリカバリピンの削除 163
17. 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 164
18. ユーザーを読み取り専用にする 管理者モード 164
19. **管理者モードでユーザーの読み取り/書き込みを有効にする** 165
20. 管理者モードでグローバルグローバル読み取り専用を設定 165
21. 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にします 166
22. 自己破壊ピンの設定方法 166
23. 自己破壊ピンを削除する方法 167
24. 自己破壊ピン（18）でロックを解除します 167
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設定する方法 168
26. 無人自動ロックの設定 168
27. 無人自動ロック（20）をオフにします。 169
28. 無人自動ロックの確認方法 170
29. ユーザーモードで読み取り専用に設定 170
30. ユーザーモードで読み取り/書き込みを有効にする 171
31. ブルートフォースハック防御メカニズム 171
32. 管理者PINブルートフォース攻撃防御機構 172
33. これは、ユーザーピンのブルートフォース制限を定義する方法です 172
34. ユーザーピンの強引な制限を確認する方法 173
35. フルリセットの実行方法 174
36. diskAshur M²を起動可能として構成する方法 174
37. 起動可能な機能diskAshurM²を無効にする方法 175
38. 起動可能な設定の確認方法 175
39. diskAshur M² for Windowsの初期化とフォーマット 176
40. MacOSでのdiskAshurM²の初期化とフォーマット 178
41. LinuxでのdiskAshurM²の初期化とフォーマット 180
42. 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す 183
43. 管理モードでファームウェアを確認する方法 183
44. ユーザーモードでファームウェアを確認する方法 184
45. テクニカルサポート 185
46. 保証およびRMA情報 185

前書き

新しいiStoragediskAshur M²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。

diskAshur M²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。

diskAshur M²には、Common Criteria EAL 5+（ハードウェア認定）に準拠した安全なマイクロプロセッサが含まれています。です。。外部操作、バイパス攻撃、およびフォールトインジェクションに対する防御のメカニズム。

他のソリューションとは対照的に、diskAshurM² 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

- diskAshur M²ポータブルSSD＆保護ケース
- 保護ケース
- USB C＆Aケーブル
- クイックスタートガイド＆製品免責事項

diskAshurM。² レイアウト



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		緑と青が交互に点滅	認証が進行中

2. LEDの状態

注意: '強い電磁波障害によりdiskAshur M²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、diskAshur M²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、diskAshurM²をスリープから復帰させます。

diskAshurM²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、diskAshurM²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	赤固定	✓	✓	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	赤固定	×	×	管理者ピンの設定を待っています

3. 初めての使用

diskAshur M²は、事前設定された管理者PINなしで「工場出荷時」状態で提供されます。ドライブを使用する前に、7～15桁の管理者PINを設定する必要があります。一度管理者PINが正常に設定されると、ドライブを「初期出荷」状態に戻すことはできなくなります。

ピンの要件：

- 7～15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）

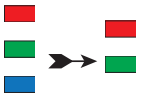
パスワードのヒント： 適切な文字でキーを押すだけで、覚えやすい単語、名前、フレーズ、またはその他の英数字のPINの組み合わせを構成できます。

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。

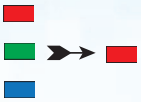
以下の表の簡単な手順に従って、管理者ピンを構成し、diskAshurM²のロックを初めて解除します。

手順-初めての使用	LED	LEDステータス
1. diskAshurM²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. キー（⚷）ボタンと**1**ボタンを両方押し続けてください。		LEDは緑と青で点滅します
3. 新しい管理者ピン（7～15桁）を入力し、キー（⚷）ボタンを1回押します		点滅する緑色LEDと点灯した青色LEDが、緑色の点滅に切り替わり、その後再び点滅する緑色LEDと点灯した青色LEDに戻ります。
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。

diskAshur M²のロック
ドライブをロックするには、ホストオペレーティングシステムから diskAshur M2 を安全に取り出し、その後 USB ポートから取り外してください。データがドライブに書き込まれている最中に diskAshur M² を取り外すと、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。

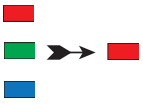
4. 管理者ピンを使用してdiskAshurM²のロックを解除する

管理者ピンを使用してdiskAshurM²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. diskAshurM²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. スタンバイ状態（赤色の連続LED）で、キー（🔑）ボタンを1回押してください。		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. 管理者モードに入る方法

管理者モードに入るには、次の手順に従います。

1. diskAshur M² をコンピュータの USB ポートに接続してください。		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LED）の状態で、キー（🔑）ボタンと**1**ボタンを両方押し続けてください。		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		緑色と青色のLEDが数回高速で点滅した後、緑色のLEDが点灯し、その後、青色のLEDが点灯して、ドライブが管理者モードにあることを示します。

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:

- 7〜15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 (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。

管理者PINを変更するには、まずセクション5に記載されているように「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)になったら、次の手順に進んでください。

1. 管理者モードで、キー(🔑) ボタンと**2**ボタンの両方を押し続ける。		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		点滅する緑色のLEDと点灯する青色のLEDは、単一の緑色LEDの点滅に切り替わり、その後、再び点滅する緑色のLEDと点灯する青色のLED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（7～15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7～15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:
- ユーザーピンの設定時に「特殊文字」が使用された場合（例えば、上記の「**B**」のように）、ドライブは設定された順序で「特殊文字」を正確に入力することによってのみ解除できます。例として、「**B**」の場合は次のように入力します: ('2', '4', 'シフト（⬆）+ **7**', '6', '8', '8', '3', '1', '4')。
- 複数の「特殊文字」を使用して、7～15桁のピンに配置することができます。
- ユーザーはピンを変更できますが、設定された「ユーザーピンポリシー」（制限）に従わなければなりません。該当する場合に適用されます。
- 新しいユーザーピンポリシーを設定すると、既存のユーザーピンが自動的に削除されます。
- このポリシーは「セルフデストラクトピン」には適用されません。セルフデストラクトピンと管理者ピンの複雑さ設定は常に7～15桁で、特殊文字は必要ありません。

ユーザPINポリシーを設定するには、まずセクション5に記載されているように「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）になったら、次の手順に進んでください。

1. 管理者モードで、キー（⚷）と**7**のボタンを両方押し続けてください。		青色のLEDが点灯状態から、緑色と青色のLEDが点滅する状態に変わります。
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（⬆）キーを一度押してください。		緑色と青色のLEDが点滅状態から、固体の緑色LEDに変わり、最終的に固体の青色LEDに変わって、ユーザーピンポリシーが正常に設定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

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。		点滅する緑色と青色のLEDが、固体の緑色LEDに変わり、最終的に固体の青色LEDに変わります。これにより、ユーザーピンポリシーが正常に削除されたことが示されます。

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

9. ユーザーピンポリシーを確認する方法

管理者は、ユーザーピンポリシーを確認でき、最小PIN長の制限や特殊文字の使用が設定されているかどうかを、以下に示すLEDシーケンスを確認することで識別できます。

ユーザーピンポリシーを確認するには、まずセクション5で説明されているように「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）になったら、次の手順を進めてください。

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：

- 7～15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、キー（🔑）ボタンと**3**ボタンを押し続けてください。		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		点滅する緑色LEDと点灯した青色LEDが、単一の緑色LEDの点滅に切り替わり、その後再び点滅する緑色LEDと点灯した青色LEDに戻ります。
3. 新しいユーザーピンを再入力し、もう一度キー（🔑）ボタンを押してください。		点滅する緑色LEDと点灯した青色LEDが、急速に点滅する緑色LEDに変わり、最終的に点灯した青色LEDに変わります。これにより、新しいユーザーピンが正常に設定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

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、キー (🔑) ボタンと**3**ボタンを押し続けてください。		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		点滅する緑色LEDと点灯した青色LEDが、単一の緑色LEDの点滅に切り替わり、その後再び点滅する緑色LEDと点灯した青色LEDに戻ります。
3. 新しいユーザーピンを再入力し、もう一度キー (🔑) ボタンを押してください。		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. 管理者モードで、シフト (⬆) + **3** ボタンを同時に押し続けてください。		点滅する赤色LEDが点灯した赤色LEDに変わり、その後、点灯した青色LEDに変わると、ユーザーPINが正常に削除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

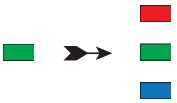
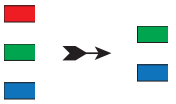
13. ユーザーピンを使用してdiskAshurM²のロックを解除する方法

以下の手順に従って、ユーザーピンでdiskAshurM²のロックを解除します。

1. 待機モード（赤色発光ダイオードが点灯）で、シフト（⬆）ボタンとキー（🔑）ボタンを両方押し続けてください。		赤色LEDがすべてのLED（赤、緑、青）の点滅に切り替わります。
2. ユーザー暗証番号（PIN）を入力し、キー（🔑）ボタンを一度押してください。		赤、緑、青の点滅LEDは、交互に点滅する緑と青のLEDに変わり、その後、緑のLEDが点灯して、ドライブがユーザーモードで正常にロック解除されたことを示します。

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diskAshurM²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（緑色LED）で、キー（🔑）ボタンと「4」ボタンの両方を押し続けてください。		緑のLEDの点灯が、赤、緑、青のすべてのLEDの点滅に変わります。
2. 既存のユーザー暗証番号（PIN）を入力し、キー（🔑）ボタンを一度押してください。		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. 新しいユーザー暗証番号（PIN）を入力し、キー（🔑）ボタンを一度押してください。		点滅する緑のLEDと点灯した青のLEDが、単独の緑のLEDの点滅に切り替わり、その後再び点滅する緑のLEDと点灯した青のLEDに戻ります。
4. 新しいユーザー暗証番号（PIN）を再入力し、キー（🔑）ボタンを一度押してください。		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. 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diskAshurM²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7～15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7～15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、キー（⚷）ボタンと「**4**」ボタンの両方を押し続けてください。		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. ワンタイム復旧用暗証番号（PIN）を入力し、キー（⚷）ボタンを押してください。		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. ワンタイム復旧用暗証番号 PIN を再入力し、キー（⚷）ボタンをもう一度押してください。		点滅する緑のLEDと点灯した青のLEDが、急速に点滅する緑のLEDに変わり、最終的に青のLEDが点灯して、ワンタイム復旧用暗証番号（PIN）が正常に設定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

16. 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、シフト（⬆）ボタンと「**4**」ボタンの両方を押し続けてください。		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（⬆）ボタンと「4」ボタンの両方をもう一度押し続けてください。		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

17. 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diskAshurM²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7〜15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. 待機モード（赤色LED点灯）で、キー（🔑）ボタンと「**4**」ボタンの両方を押し続けてください。		連続した赤いLEDが赤く点滅し、緑のLED
2. ワンタイム復旧用暗証番号（PIN）を入力し、キー（🔑）ボタンを押してください。		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. 新しいユーザー暗証番号（PIN）を入力し、キー（🔑）ボタンを押してください。		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。

18. 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diskAshurM²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。

diskAshur M²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		緑色と青色のLEDは、最初に緑色のLEDに、次に青色のLEDに変わり、これによりドライブが設定され、ユーザーアクセスが読み取り専用に制限されていることが示されます。

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

19. 管理者モードでユーザーの読み取り/書き込みを有効にする

diskAshur M²を読み取り/書き込みに戻すには、まずセクション5に記載された「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）になったら、次の手順に進んでください。

1. 管理者モードで両方のボタン「**7 + 9**」を押し続けます。		青色のLEDが点灯した後、緑色と青色のLEDが点滅に変わります。
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

20. 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diskAshurM²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。

diskAshur M²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。		青色のLEDが点灯した後、緑色と青色のLEDが点滅に変わります。
2. キー（🔑）ボタンを押してください。		緑色と青色のLEDは、最初に緑色のLEDに、次に青色のLEDに変わり、これによりドライブが設定され、グローバルアクセスが読み取り専用に制限されていることが示されます。

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. 管理者モードでグローバル読み取り/書き込みをアクティブ化する

diskAshur M²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。		青色のLEDが点灯した後、緑色と青色のLEDが点滅に変わります。
2. キー（🔑）ボタンを押してください。		緑色と青色のLEDが、最初に緑色のLEDに、次に青色のLEDに変わり、これによりドライブが読み取り/書き込みモードに設定されていることが示されます。

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. 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		点灯した青色LEDが点滅する緑色に変わり、点灯した青色LED
2. 7～15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

23. 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、シフト（⬆）ボタンと6ボタンを両方同時に押し続けてください。		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. もう一度、シフト（⬆）＋**6**ボタンを押し続けてくださ い。		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

24. 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、diskAshur M²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diskAshur M²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. 待機モード（赤色LEDが点灯している状態）で、シフト（⬆）ボタンとキー（🔑）ボタンを両方同時に押し続けてください。		赤色LEDがすべてのLED（赤、緑、青）が点滅する状態に切り替わります。
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、diskAshur M²が成功したことを示します 自己破壊

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設定する方法

ブルートフォース攻撃の後、またはdiskAshur M²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：

- 7～15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）

もしdiskAshur M²がブルートフォース攻撃を受けたか、リセットされた場合、ドライブは待機状態（赤色LEDが点灯）になります。管理者PINを設定するには、以下の手順に従ってください。

1. 待機モード（赤色LEDが点灯している状態）で、シフト（⬆）ボタンと**1**ボタンを同時に押し続けてください。		点灯した赤色LEDが点滅する緑色LEDと点灯した青色LEDに変わります。
2. 新しい管理者PINを入力し、キー（🔑）ボタンを押 してください。		点滅する緑色LEDと点灯した青色LEDが、単一の緑色LEDの点滅に切り替わり、その後再び点滅する緑色LEDと点灯した青色LEDに戻ります。
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		点滅する緑色LEDと点灯した青色LEDが、数秒間青色LEDが高速で点滅する状態に変わり、その後点灯した青色LEDに戻り、管理者PINが正常に設定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

26. 無人自動ロックを設定します

ドライブがロック解除された状態で放置されている場合、不正アクセスから保護するために、diskAshur M²は指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、diskAshur M²の未使用時自動ロック機能はオフになっています。未使用時自動ロックは、5～99分の間で設定することができます。

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、キー（⚷）ボタンと**5**ボタンを両方同時に押し続けてください。		点灯した青色LEDが点滅する緑色と青色LEDに変わります。
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

27. 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、キー（⚷）ボタンと**5**ボタンを同時に押し続けてください。		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

28. 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**		青色のLEDが点灯から緑色と青色のLEDが点滅する状態に変わります
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.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

29. ユーザーモードを読み取り専用に設定します

diskAshur M²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. キー（🔑）ボタンを押してください		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。

30. ユーザーモードで読み取り/書き込みを有効にする

diskAshur M²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が点灯から緑色と青色のLEDが点滅する状態に変わります
2. キー（⚷）ボタンを押す		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。

31. ブルートフォースハック防御メカニズム

diskAshur M²には、ブルートフォース攻撃からドライブを保護する防御メカニズムがあります。デフォルトでは、管理者ピンとユーザーピンの両方のブルートフォース制限（連続した誤ったピンエントリ）の初期送信ステータス値は、回復ピンの**10**と**5**です。以下に示すように、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、ピン認証（管理者、ユーザー、および回復）ごとに誤った試行を記録します。

- ユーザーが間違ったユーザーピンを10回続けて入力すると、ユーザーピンは削除されますが、データ、管理者ピン、および回復ピンはそのまま残り、アクセス可能です。
- 間違った回復ピンが5回続けて入力された場合、回復ピンは削除されますが、データと管理者ピンはそのまま残り、アクセス可能です。
- 間違った管理ピンが10回続けて入力された場合、ドライブはリセットされます。すべてのピンとデータは削除され、永久に失われます。

次の表は、3つのピンがすべて設定されていることを前提としており、各ピンの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。

ドライブのロックを解除するためのPIN	連続して間違っているピンエントリ	何が起こっているかの説明
ユーザーピン	10	• ユーザーピンが削除されます。 • リカバリピン、管理者ピン、およびすべてのデータはそのまま残り、アクセス可能です。
回復ピン	5	• リカバリピンは削除されます。 • 管理者ピンとすべてのデータは保持され、アクセス可能です。
管理者ピン	10	• diskAshur M²リセットされます。すべてのピンとデータは削除され、永久に失われます。

注意: 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場合、またはセルフデストラクション機能が有効化された場合、またはブルートフォース攻撃が行われた場合、出荷時の初期状態に戻されます。管理者がユーザーPINを変更した場合、またはリカバリ機能を有効化する際に新しいユーザーPINが設定された場合、ユーザーPINのブルートフォースカウンターはリセットされますが、ブルートフォース制限には影響しません。管理者がリカバリPINを変更した場合、リカバリPINのブルートフォースカウンターはリセットされます。

特定のPINの認証が成功すると、そのPINのブルートフォースカウンターはリセットされますが、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PINのブルートフォースカウンターが増加しますが、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。

32. 管理者PINブルートフォース攻撃防御機構

diskAshur M²の管理者PINは、ユーザーPINやリカバリPINと比較して、より高度な防御機構が備わっています。これは、管理者PINを10回連続で間違えて入力した場合に、誤ってデータを失うことを防ぐためのものです。したがって、管理者PINを5回連続で間違えて入力すると、diskAshur M²はロックされ、すべてのLEDが点灯して固定状態になります。

警告:「ユーザーPIN」のみでdiskAshur M²を解除し、「管理者PIN」を知らない場合は、以下の手順を試みないでください。

以下の表の指示に従って、最大10回までの管理者PIN入力を有効にする方法を参照してください。

管理者PINの不正な連続入力	diskAshur M² の動作説明	手順
5	すべてのLED（赤、緑、青）が点灯し、固定されます。	次のPIN '47867243' を入力し、キー (🔑)ボタンを1回押してください。緑色と青色のLEDが交互に点滅し、diskAshur M2は管理者PINの入力をあと3回試行できる状態になります。
8	すべてのLED（赤、緑、青）が交互に点滅します。	次のPIN「47867243」を入力して キー (🔑) を1回押すと、緑と青のLEDが交互に点滅し、diskAshur M² にさらに2回管理者PIN を入力できる状態になります。
10	赤のLEDが点灯し、固定されます。	管理者PINが不正に10回連続入力されると、暗号鍵、すべてのPIN、データが完全に削除され、復元することはできません。

33. これは、ユーザーピンのブルートフォース制限を設定する方法です。

注意: ドライブが完全にリセットされているか、残酷に強制されているか、または自己破壊PINが有効になっている場合、ユーザーPINのブルートフォース制限設定はデフォルトで10回の連続した不正なPINエントリに設定されます。

diskAshur M²のユーザーピンの強引な制限は、管理者が再プログラムして定義できます。この機能は、1～10回の連続した誤ったピン入力の試行が可能にな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		青色のLEDが点灯から緑色と青色のLEDが一緒に点滅する状態に変わります
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（⬆）ボタンを1回押してください。		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

34. 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

35. 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、diskAshur M²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、diskAshurM²をリセットします。

1. 待機状態（赤色のLEDが点灯している状態）で、「**0**」ボタンを押し続けてください。		赤色のLEDが点灯から、赤、緑、青のすべてのLEDが交互に点滅する状態に変わります。
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、diskAshurM²もフォーマットする必要があります。

36. diskAshurM²を起動可能として構成する方法

注意: ドライブがブータブルとして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外してもLEDは赤色にはなりません。ドライブは緑色のままで、次回使用するためには再度取り外す必要があります。diskAshur M2のデフォルト設定は非ブータブルとして構成されています。

diskAshur M2は、ホストのブートプロセス中に電源のサイクルを処理するためのブータブル機能を搭載しています。diskAshur M2からブートすると、diskAshur M2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ーを実行していることになります。

ドライブを起動可能にするには、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、キー(🔑) ボタンと**8**ボタンの両方を押し続けてください。		青色のLEDが点灯から緑色と青色のLEDが点滅する状態に変わります。
2.「**0**」を押してから「1」（**01**）を押します。		緑と青のLEDが点滅し続ける
3. シフト（⬆）ボタンを1回押してください。		緑色と青色のLEDが点滅から、緑色のLEDが点灯し、最終的に青色のLEDが点灯して、ドライブが正常にブータブルとして設定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

37. 起動機能diskAshurM²の無効化

起動可能な機能diskAshurM²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」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、キー(🔑)ボタンと**8**ボタンの両方を押し続けてください。		青色のLEDが点灯から緑色と青色のLEDが交互に点滅する状態に変わります。
2.「**0**」を押してから別の「**0**」(**00**) を押します。		緑と青のLEDが点滅し続ける
3. シフト (⬆) ボタンを1回押してください。		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が点灯します起動可能な機能が表示されました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

38. 起動可能な設定を確認する方法

起動可能な設定を確認するには、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、次の手順に進みます。

1. 管理者モードで、シフト (⬆) ボタンと8ボタンの両方を押し続けてください。		青色のLEDが点灯から緑色と青色のLEDが交互に点滅する状態に変わります。

2. キーボタンを押します。次の2つのシナリオのいずれかが発生します。

- **diskAshur M² が起動可能として構成されている場合、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が再び青色に点灯します

- **diskAshur M² が起動可能として構成されていない場合、以下が発生します。**

a. すべてのLED（赤、緑、青）が1秒間点灯します。
b. すべてのLEDがオフになっています
c. すべてのLED（赤、緑、青）が1秒間点灯します。
d. LEDが再び青色に点灯します

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

39. diskAshur M² 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、diskAshur M²はすべてのピン、データ、および暗号化キーを削除します。diskAshur M²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、diskAshurM²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。

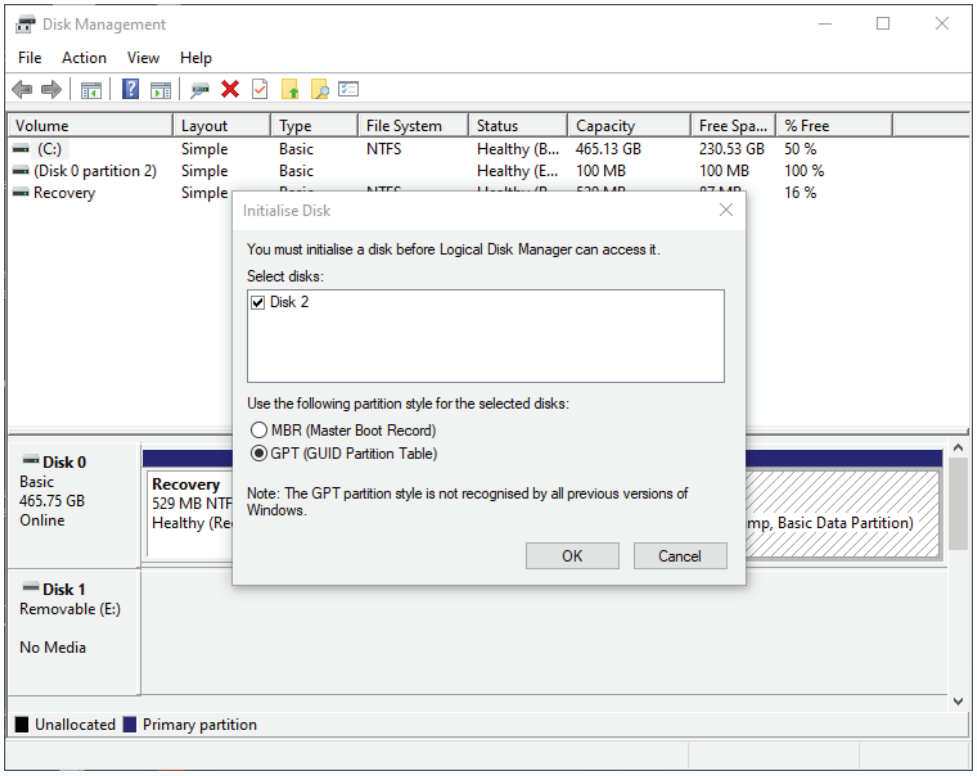
2. diskAshur M²がスタンバイモード（赤色のLED）の場合は、キーボタンを1回押し、新しい管理者ピンを入力してロックを解除します（緑色のLEDが点滅）。

3. diskAshurM²をコンピューターに接続します。

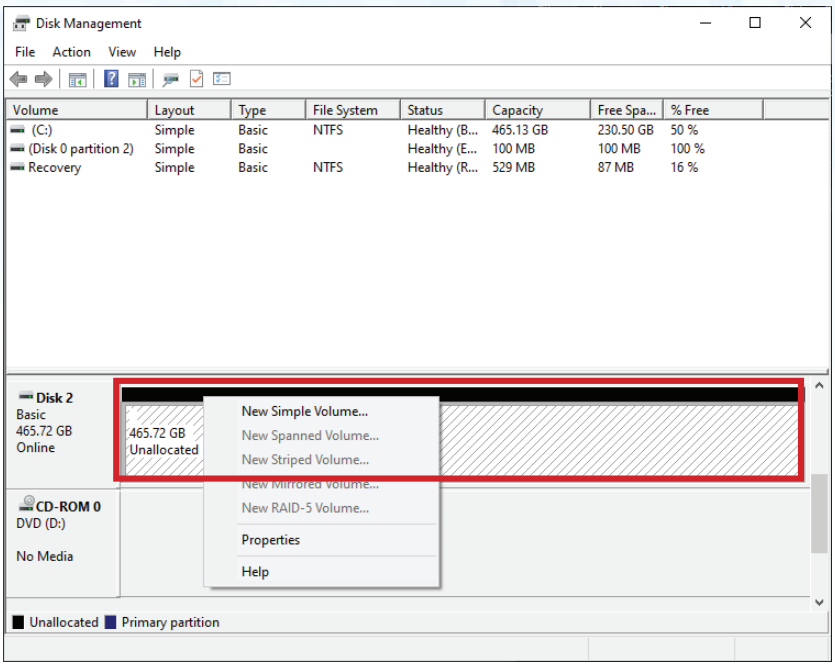
4. **ウィンドウズ 7:** [コンピューター]を右クリックし、[管理]をクリックして、[ディスクの管理]を選択します
   ウィンドウズ 8: デスクトップの左隅を右クリックして、[ディスクの管理]を選択します
   ウィンドウズ 10: [スタート]ボタンを右クリックして、[ディスクの管理]を選択します

5. [ディスクの管理]ウィンドウで、diskAshur M²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。

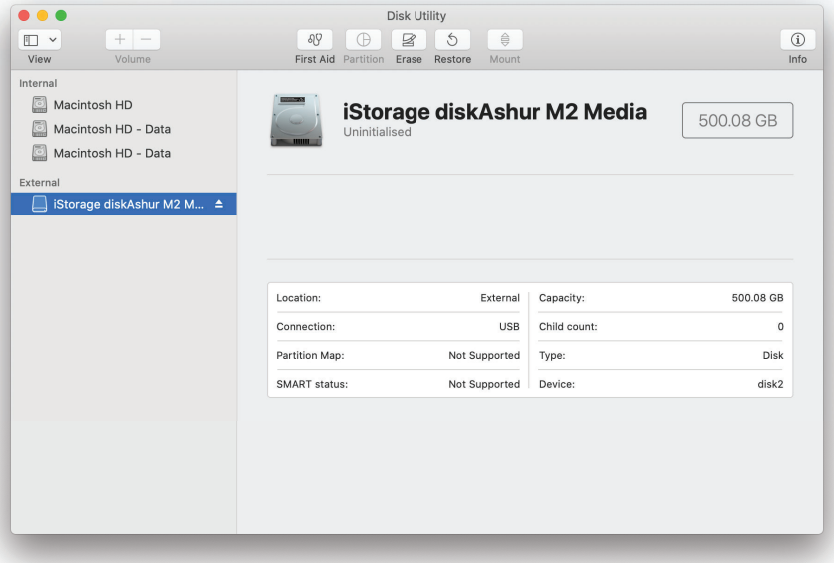
12. フォーマットプロセスが完了するのを待ちます。diskAshur M²が認識され、使用可能になります。

40. MacOSでのdiskAshurM²の初期化とフォーマット

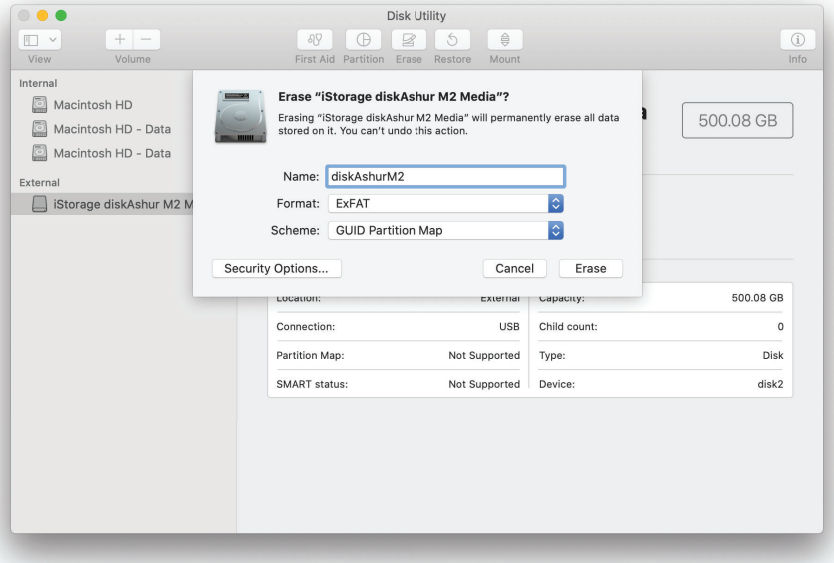
「ブルートフォース攻撃」または完全なリセットの後、diskAshur M²はすべてのピン、データ、および暗号化キーを削除します。diskAshur M²を使用する前に、初期化してフォーマットする必要があります。

diskAshurM²を初期化およびフォーマットする方法

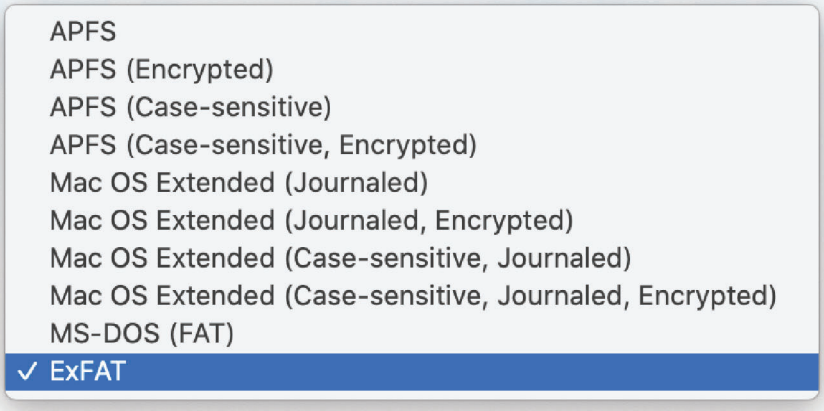
1. ドライブとボリュームのリストからdiskAshurM²を選択します。リスト内の各ドライブには、容量、製造元、製品名が表示されます（例：B。「**iStoragediskAshur M²Media**」）。



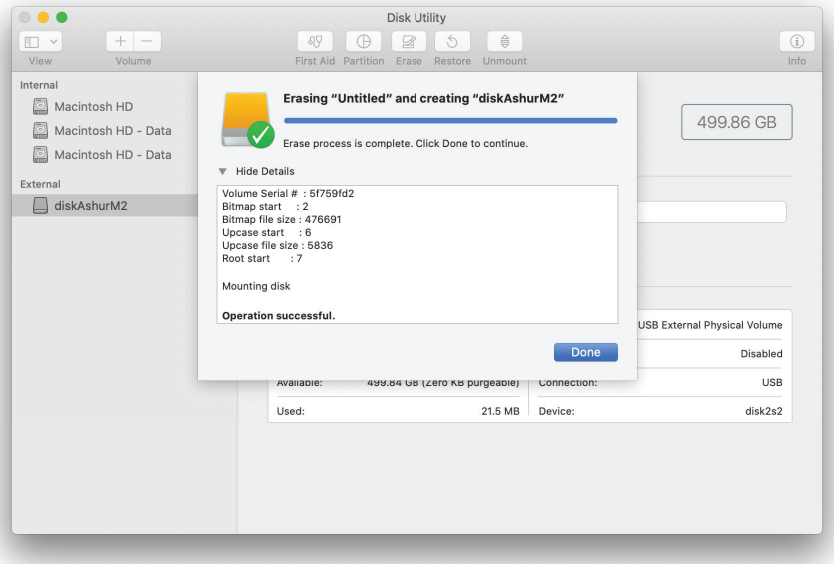
2. [ディスクユーティリティ]で、[消去]ボタンをクリックします。
3. ドライブの名前を入力します。デフォルトの名前は無題です。ドライブの名前は、最終的にデスクトップに表示されます。



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。

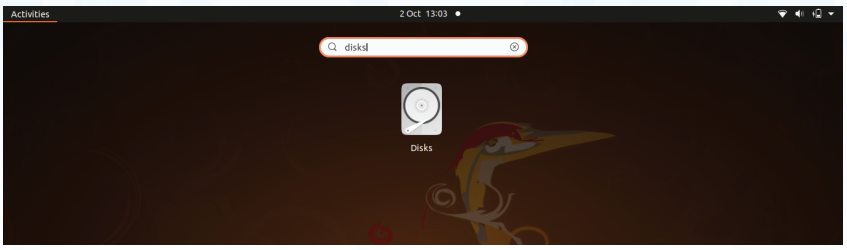


5. [削除]ボタンをクリックします。ディスクユーティリティは、ボリュームをデスクトップからアンマウントし、削除してから、デスクトップに再度マウントします。

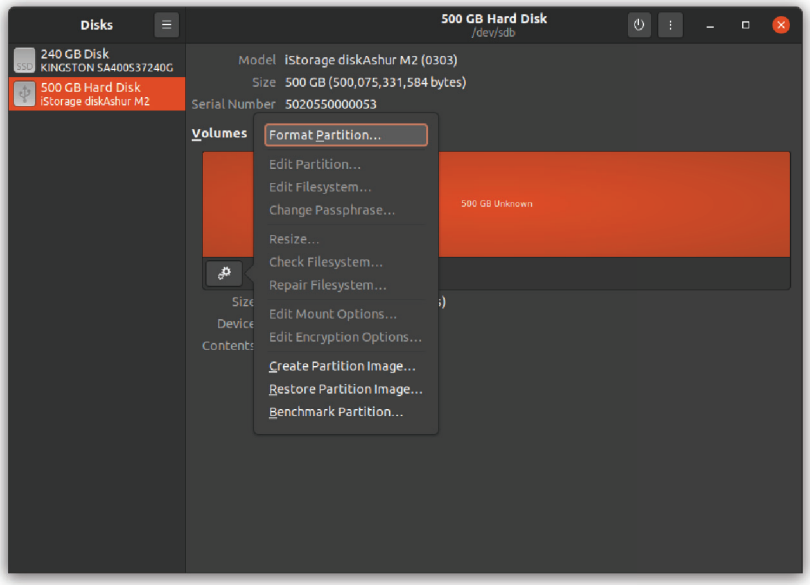


41. LinuxでのdiskAshurM²の初期化とフォーマット

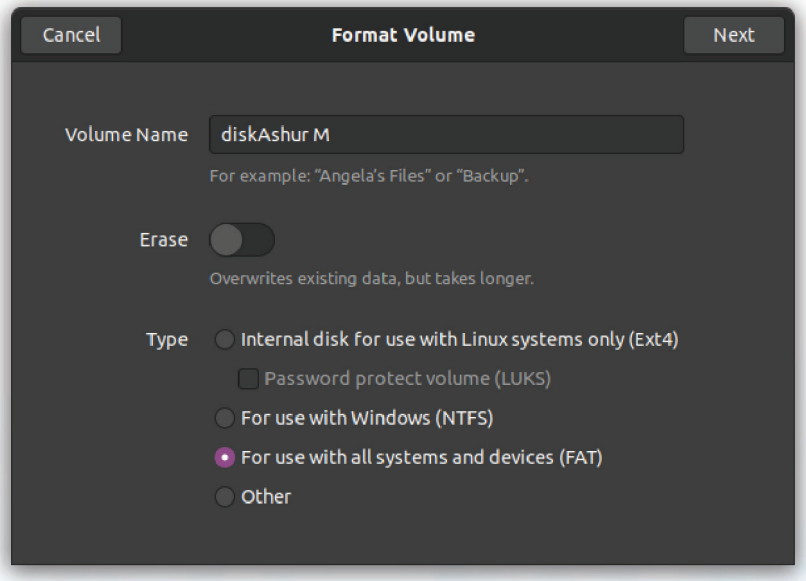
1. 「アプリケーションの表示」を開き、検索フィールドに「ディスク」と入力します。表示されたら、ハードディスクユーティリティをクリックします。



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。

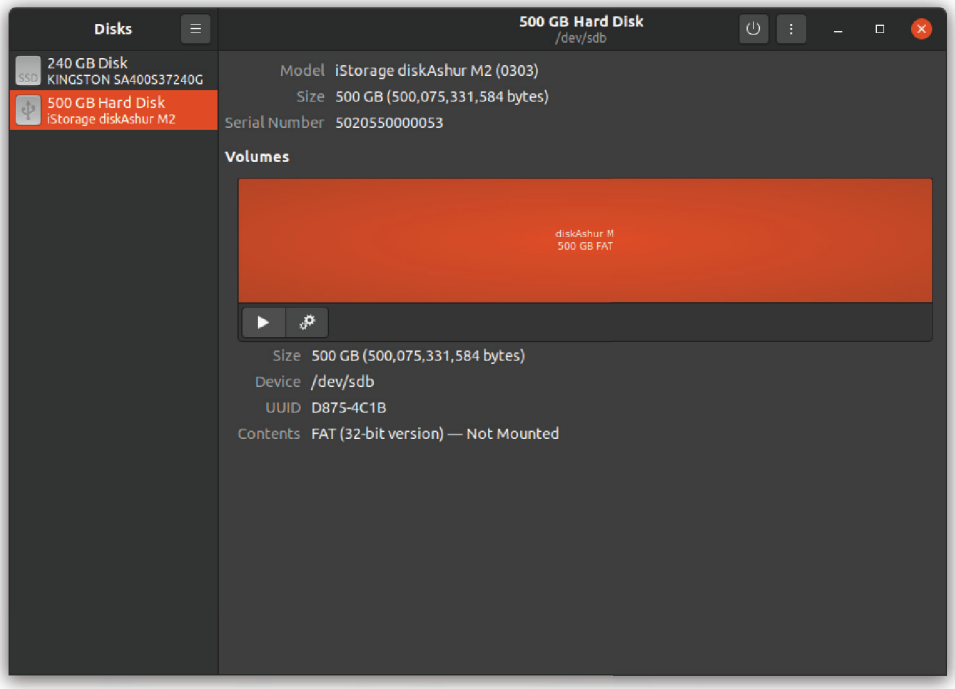


3. [タイプ]オプションで[すべてのシステムとデバイスと互換性がある（FAT）]を選択します。ドライブの名前を入力します（例：B。diskAshurM²）。次に、[フォーマット]ボタンをクリックします。

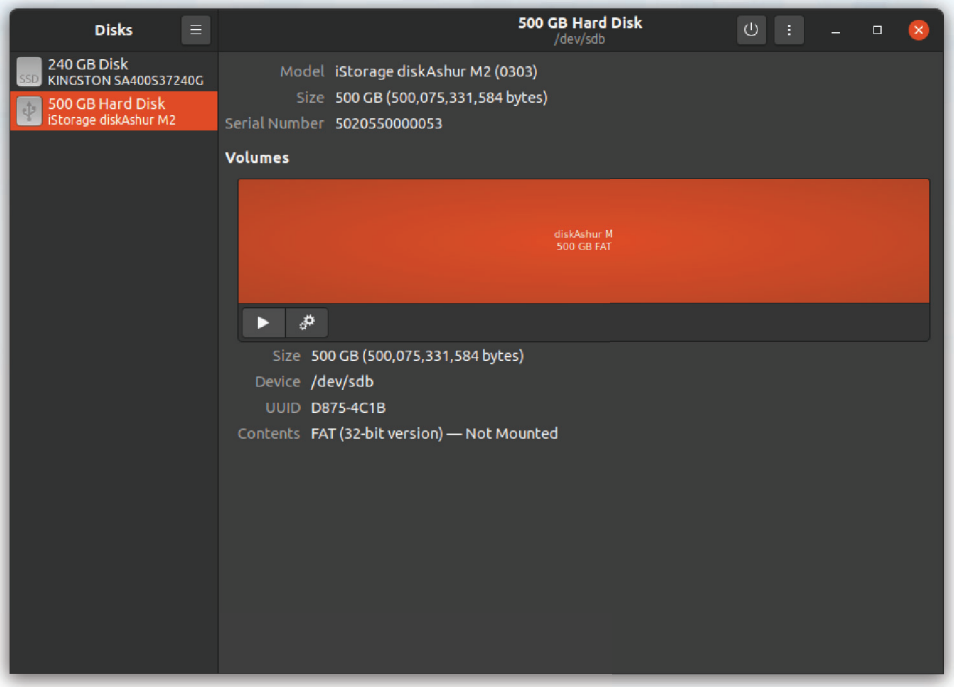




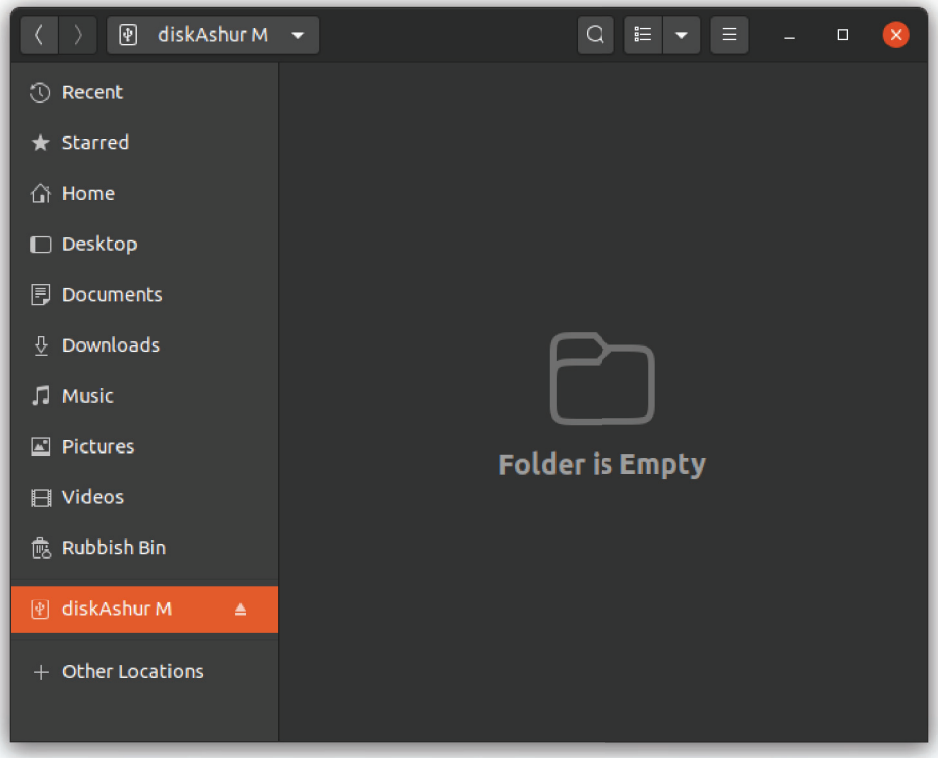
4. フォーマットプロセスが完了したら、[再生]ボタンをクリックしてドライブをUbuntuにマウントします。



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。



42. 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す

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diskAshurM²上のすべてのファイルを保存して閉じてください。

diskAshur M²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、diskAshur M²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、diskAshur M²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diskAshurM²をロックします。

43. 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		青色のLEDが点灯から緑色と青色のLEDが交互に点滅する状態に変わります。
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。

44. 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。

45. 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。

46. 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

DISKASHUR® M²

Copyright © iStorage Limited 2020。無断複写・転載を禁じます。
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

DISKASHUR® M²

iStorage®

Gebruikershandleiding



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 diskAshur M² neem dan contact op met ons ondersteuningsteam via e-mail - support@istorage-uk.com of per telefoon +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2020. Alle rechten voorbehouden.

Windows is een geregistreerd handelsmerk van Microsoft Corporation.
Alle andere handelsmerken en auteursrechten waarnaar wordt verwezen, zijn eigendom van hun respectievelijke eigenaren.

Verspreiding van gewijzigde versies van dit document is verboden zonder de uitdrukkelijke toestemming van de copyrighthouder.

Verspreiding van het werk of daarvan afgeleid werk in een standaard (papieren) boekvorm voor commerciële doeleinden is verboden tenzij hiervoor toestemming is verleend door de copyrighthouder.

DOCUMENTATIE WORDT IN DE HUIDIGE STAAT GELEVERD EN ALLE EXPLICIETE OF IMPLICIETE VOORWAARDEN, VERKLARINGEN EN GARANTIES, MET INBEGRIP VAN ELKE IMPLICIETE GARANTIE VAN VERKOOPBAARHEID, GESCHIKTHEID VOOR EEN BEPAALD DOEL OF NIET-INBREUK WORDEN AFGEWEZEN, BEHALVE VOOR ZOVER DERGELIJKE DISCLAIMERS WETTELIJK ONGELDIG WORDEN BESCHOUWD

RoHS Compliant

REACH COMPLIANCE

Alle handelsmerken en merknamen zijn eigendom van hun respectievelijke eigenaren

Voldoet aan de Handelswetgeving (Trade Agreements Act, TAA)

Table of Contents

Introductie 190
Inhoud van de doos 190
diskAshur M² Lay-out 190
1. LED-indicatoren en hun werking 191
2. LED-status 191
3. Eerste gebruik 192
4. DiskAshur M² ontgrendelen met de pincode van de beheerder 193
5. De beheerdersmodus openen 193
6. De pincode van de beheerder veranderen 194
7. Beleid voor pincode van de gebruiker instellen 195
8. Beleid van de gebruikerspincode verwijderen 196
9. Beleid van de gebruikerspincode controleren 196
10. Een nieuwe gebruikerspincode toevoegen in de beheerdersmodus 197
11. De gebruikerspincode veranderen in de beheerdersmodus 198
12. De gebruikerspincode verwijderen in de beheerdersmodus 198
13. De diskAshur M² ontgrendelen met pincode van de gebruiker 199
14. De pincode van de gebruiker in de gebruikersmodus wijzigen 199
15. Eenmalig herstel van gebruikerspincode aanmaken 200
16. Eenmalig herstel van gebruikerspincode verwijderen 200
17. Herstelmodus activeren en nieuwe gebruikerspincode aanmaken 201
18. Alleen-lezen toegang voor gebruiker instellen in de beheerdersmodus 201
19. Gebruiker lezen/schrijven in de beheerdersmodus inschakelen 202
20. Globale alleen-lezen toegang in de beheerdersmodus instellen 202
21. Globaal lezen/schrijven in de beheerdersmodus inschakelen 203
22. Zelfvernietigingspincode configureren 203
23. Zelfvernietigingspincode verwijderen 204
24. Zelfvernietigingspincode ontgrendelen 204
25. Beheerderspincode configureren of opnieuw instellen na een brute aanval 205
26. De onbeheerde automatische vergrendeling instellen 205
27. De onbeheerde automatische vergrendeling uitschakelen 206
28. De onbeheerde automatische vergrendeling controleren 207
29. Alleen-lezen in de gebruikersmodus instellen 207
30. Lezen/schrijven in gebruikersmodus inschakelen 208
31. Verdedigingsmechanisme tegen brute aanvallen 208
32. Admin PIN Brute Force Hack Verdedigingsmechanisme 209
33. De gebruikerspincode instellen om brute aanvallen te beperken 209
34. De gebruikerspincode tegen beperking van brute aanvallen controleren 210
35. Een volledige reset uitvoeren 211
36. diskAshur M² als opstartbaar configureren 211
37. De diskAshur M² opstartfunctie uitschakelen 212
38. De opstartinstelling controleren 212
39. Initialiseren en formatteren van diskAshur M² voor Windows 213
40. Initialiseren en formatteren van diskAshur M² in Mac OS 215
41. Initialiseren en formatteren van diskAshur M² in Linux OS 217
42. In slaapstand gaan, opschorten of afmelden bij het besturingssysteem 220
43. Firmware controleren in de beheerdersmodus 220
44. Firmware controleren in de gebruikersmodus 221
45. Technische ondersteuning 222
46. Garantie en RMA-informatie 222

Introductie

Dank u voor de aanschaf van de nieuwe iStorage diskAshur M², een ultraveilige en gebruiksvriendelijke draagbare Solid State Drive (SSD) met een capaciteit van 120 GB tot 2 TB en hoger geverifieerd met pincode en met hardware-encryptie.

Ontworpen om FIPS 140-3 Level 3, versleutelt de diskAshur M² gegevens tijdens verzending en in rust met behulp van AES-XTS 256-bit hardwareversleuteling op de volledige disk.

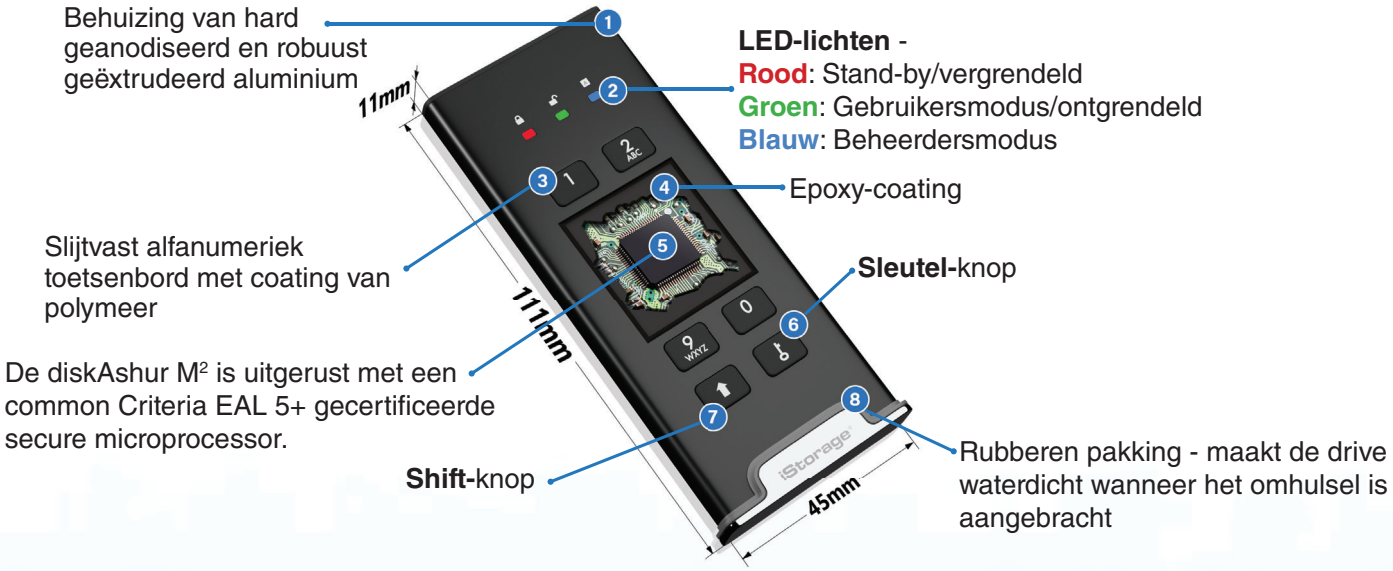
De diskAshur M² is uitgerust met een common Criteria EAL 5+ gecertificeerde secure microprocessor, die ingebouwde fysieke beschermings-mechanismen gebruikt die zijn ontworpen om te beschermen tegen externe sabotage, en om aanvallen en foutinjecties te omzeilen.

In tegenstelling tot andere oplossingen reageert de diskAshur M² op een geautomatiseerde aanval door de deadlock toestand in te gaan, waardoor al deze aanvallen nutteloos worden gemaakt. In duidelijke en eenvoudige bewoordingen: zonder de pincode is er geen toegang!

Inhoud van de doos

- diskAshur M² draagbare SSD & Beschermhoesje
- Beschermtasje
- USB C & USB A Kabels
- Snelstartgids & Product Disclaimer/Vrijwaringsclausule

diskAshur M² Lay-out



1. LED-indicatoren en hun werking

LED	LED-status	Beschrijving	LED	LED-status	Beschrijving
	ROOD ononderbroken	Vergrendelde drive (in hetzij **Stand-by** of **Reset** status)		BLAUW ononderbroken	Drive in **Beheerdersmodus**
	ROOD dubbele knippering	Onjuiste invoer pincode		ROOD, GROEN en BLAUW knipperen tegelijkertijd	Wachten op invoer pincode van **gebruiker**
	GROEN ononderbroken	Drive ontgrendeld		GROEN en BLAUW Knipperen tegelijkertijd	Wacht op invoer van **beheerders** pincode
	GROEN knippert	Gegevensoverdracht is bezig		GREEN en BLAUW Knipperen afwisselend	Authenticatie is bezig

2. LED-status

Opmerking: De normale werking van de diskAshur M² kan worden verstoord door sterke elektromagnetische interferentie. Als dit het geval is, schakelt u het product uit en weer in (uitschakelen en weer inschakelen) om de normale werking te hervatten. Als de normale werking niet wordt hervat, gebruik het product dan op een andere locatie.

Om uit de inactieve toestand te ontwaken

De inactieve toestand wordt gedefinieerd als het moment waarop diskAshur M² niet wordt gebruikt en alle LED's uit zijn.

Om diskAshur M² uit de inactieve toestand te halen doet u het volgende.

Sluit de diskAshur M² aan op een actieve USB-poort op uw computer	→	RODE, GROENE en BLAUWE LED's knipperen eenmaal achter elkaar en vervolgens knippert de GROENE LED tweemaal en schakelt uiteindelijk naar een ononderbroken RODE LED die aangeeft dat de drive in stand-by is

Om over te gaan tot de inactieve toestand

Om diskAshur M² te laten overgaan naar de inactieve toestand, voert u een van de volgende bewerkingen uit:

- Koppel de drive los als deze op een USB-poort is aangesloten, alle LED's gaan uit (inactieve toestand).

Inschakelstatus

Nadat de drive uit de inactieve status ontwaakt, gaat deze naar een van de volgende status die in de onderstaande tabel worden weergegeven.

Inschakelstatus	LED indicatie	Encryptiesleutel	Beheerderspincode	Beschrijving
Eerste verzendingsstatus	ROOD en GROEN Ononderbroken	✓	×	Wacht op configuratie van een beheerderspincode (eerste gebruik)
Stand-by	ROOD ononderbroken	✓	✓	Wacht op invoer van beheerders- of gebruikerspincode
Reset	ROOD ononderbroken	×	×	Wacht op configuratie van een beheerderspincode

3. Eerste gebruik

diskAshur M² is bij de 'Eerste verzendingsstatus' niet voorzien van een vooraf ingestelde beheerderspincode. Er moet een beheerderspincode met 7 tot 15 cijfers worden geconfigureerd voordat de drive kan worden gebruikt. Zodra een beheerderspincode met succes geconfigureerd is, zal het niet mogelijk zijn om de drive terug te veranderen in de 'Eerste verzendingsstatus'.

Vereisten voor pincode:

- Moet tussen de 7 en 15 cijfers lang zijn
- Mag niet alleen herhalende cijfers bevatten, bijv. (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)

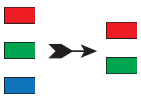
Tip voor wachtwoord: U kunt een gemakkelijk te onthouden woord, naam, zin of een andere alfanumerieke combinatie configureren door simpelweg op de knop met de bijbehorende letters te drukken.

Voorbeelden van dit soort alfanumerieke pincodes zijn:

- Druk voor "**Wachtwoord**" op de volgende toetsen:
  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)
- Druk voor "**iStorage**" op de volgende toetsen:
  4 (ghi) **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 pincodes worden geconfigureerd.

Om een beheerderspincode te configureren en de diskAshur M² voor de eerste keer te ontgrendelen volgt u de eenvoudige stappen in de onderstaande tabel.

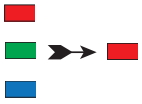
Instructies - Eerste gebruik	LED	LED-status
1. Sluit de diskAshur M² aan op een actieve USB-poort op uw computer		RODE, GROENE en BLAUWE LED's knipperen eenmaal achter elkaar en vervolgens knippert de GROENE LED tweemaal en gaat tenslotte over naar ononderbroken RODE en GROENE LED's die aangeven dat de drive in de Eerste verzendingsstatus is
2. Houd beide **SLEUTEL (🔑) + 1**-knoppen ingedrukt		LED's gaan GROENE knipperen en blijven ononderbroken BLAUW
3. Voer een **Nieuwe beheerderspincode** (7-15 cijfers) in en druk eenmaal op de **SLEUTEL (🔑)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's schakelen naar een GROENE knippering en dan terug naar knipperend GROEN en ononderbroken BLAUWE LED's
4. Voer opnieuw uw **nieuwe beheerderspincode** in en druk weer op de **SLEUTEL (🔑)**-knop		BLAUWE LED knippert snel en verandert dan in een ononderbroken BLAUWE LED en tenslotte naar een ononderbroken GROENE LED waarmee wordt aangeduid dat de beheerderspincode met succes werd geconfigureerd en de drive ontgrendeld

De diskAshur M² vergrendelen

Om de drive te vergrendelen, moet u de diskAshur M² 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 diskAshur M² resulteren in onvolledige datatransfer en mogelijke corruptie van gegevens.

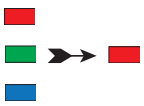
4. diskAshur M² ontgrendelen met de pincode van de beheerder

Om de diskAshur M² te ontgrendelen met de beheerderspincode volgt u de eenvoudige stappen in de onderstaande tabel.

1. Sluit de diskAshur M² aan op een 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) druk op de **SLEUTEL (🔑)** button once		GROENE en BLAUWE LED's knipperen tegelijkertijd
3. Met de GROENE en BLAUWE LED's die tegelijkertijd knipperen, voer de **Beheerderspincode** in en druk weer op de **SLEUTEL (🔑)**-knop		GROENE en BLAUWE LED's knipperen verschillende keren afwisselen en gaan dan over naar een ononderbroken BLAUWE LED en verandert naar een ononderbroken GROENE LED waarmee wordt aangeduid dat de drive met succes werd ontgrendeld als beheerder

5. De beheerdersmodus openen

Om de beheerdersmodus te openen doet u het volgende.

1. Sluit de diskAshur M² 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 **SLEUTEL (🔑) + 1** knoppen ingedrukt		GROENE en BLAUWE LED's knipperen tegelijkertijd
3. Voer uw beheerderspincode in en druk eenmaal op de **SLEUTEL (🔑)**-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. De pincode van de beheerder wijzigen

Vereisten voor pincode:

- Moet tussen de 7 en 15 cijfers lang zijn
- Mag niet alleen herhalende cijfers bevatten, bijv. (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)

Tip voor wachtwoord: U kunt een gemakkelijk te onthouden woord, naam, zin of een andere alfanumerieke combinatie configureren door simpelweg op de knop met de bijbehorende letters te drukken.

Voorbeelden van dit soort alfanumerieke pincodes zijn:

- Druk voor "**Wachtwoord**" op de volgende toetsen:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Druk voor "**iStorage**" op de volgende toetsen:
  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 pincodes worden geconfigureerd.

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 **SLEUTEL (🔑) + 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 **SLEUTEL (🔑)**-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 **SLEUTEL (🔑)**-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 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.

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 7 tot 15 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 7-15 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 7-15 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 7-15 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 **SLEUTEL** (🔑) **+ 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. Beleid van de gebruikerspincode verwijderen

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 **SLEUTEL (⚷) + 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 **SLEUTEL (⚷)**-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. Een nieuwe gebruikerspincode toevoegen in de beheerdersmodus

Belangrijk: De creatie van een nieuwe 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.

Vereisten voor pincode:

- Moet tussen de 7 en 15 cijfers lang zijn
- Mag niet alleen herhalende cijfers bevatten, bijv. (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 **SLEUTEL (🔑) + 3**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Voer **nieuwe gebruikerspincode** in en druk op **SLEUTEL (🔑)**-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 **SLEUTEL (🔑)**-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 **SLEUTEL (⚷)** + 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 **SLEUTEL (⚷)**-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 **SLEUTEL (⚷)**-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.

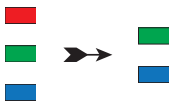
13. diskAshur M² ontgrendelen met gebruikerspincode

Om de diskAshur M² met de **gebruikerspincode** te ontgrendelen gaat u verder met de volgende stappen.

1. In stand-by status (ononderbroken RODE LED) houdt u beide **SHIFT (⬆) + KEY (⚷)**-knoppen ingedrukt		RODE LED wisselt naar alle LED's, ROOD, GROEN & BLAUW die aan en uit knipperen
2. Voer gebruikerspincode in en druk eenmaal op de **SLEUTEL (⚷)** -knop		RODE, GROENE en BLAUWE knipperen LED's zullen veranderen naar afwisselende GROENE en BLAUWE LED's en dan naar ononderbroken GROENE LED waarmee wordt aangeduid dat de drive met succes werd ontgrendeld in gebruikersmodus

14. De pincode van de gebruiker in de gebruikersmodus wijzigen

Om de **gebruikerspincode** te veranderen, ontgrendelt u eerst de diskAshur M² met de gebruikerspincode zoals beschreven in hoofdstuk 13. Zodra de drive in **gebruikersmodus** is (ononderbroken GROENE LED) ga verder met onderstaande stappen.

1. In stand-by status (ononderbroken GROENE LED) houdt u beide **SLEUTEL (⚷)** + 4-knoppen ingedrukt		Ononderbroken GROENE LED wisselt naar alle LED's, ROOD, GROEN & BLAUW die aan en uit knipperen
2. Voer uw **nieuwe gebruikerspincode** in en druk op de **SLEUTEL (⚷)**-knop		GROENE en ononderbroken BLAUWE LED's gaan aan en uit en zullen dan naar een enkele GROENE LED knippering overschakelen en vervolgens terug naar knipperende GROENE en ononderbroken BLAUWE LED's
3. Voer **nieuwe gebruikerspincode** in en druk eenmaal op de **SLEUTEL (⚷)**-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
4. Voer opnieuw **nieuwe gebruikerspincode** in en druk weer op de **SLEUTEL (⚷)**-knop		Knipperend GROENE en ononderbroken BLAUWE LED's veranderen in een snel knipperende GROENE LED en tenslotte naar een ononderbroken GROENE LED waarmee wordt aangeduid dat de gebruikerspincode met succes werd gewijzigd

Belangrijk: Het veranderen van een gebruikerspincode in de gebruikersmodus (GROENE LED) moet voldoen aan het 'gebruikerspincodebeleid' als er een is geconfigureerd zoals beschreven in hoofdstuk 7, die een minimale pincodelengte oplegt en of een 'speciaal teken' is gebruikt.

15. Eenmalig herstel van gebruikerspincode aanmaken

De herstelpincode voor gebruikers is uitermate nuttig in situaties waarin een gebruiker zijn pincode om de diskAshur M² te ontgrendelen, is vergeten.
Om de herstelmodus te activeren, moet de gebruiker eerst de juiste eenmalige herstelpincode invoeren, indien deze is geconfigureerd. Het herstelproces van de gebruikerspincode heeft geen invloed op de gegevens, de encryptiesleutel en de beheerderspincode, maar de gebruiker moet een nieuwe gebruikerspincode met 7-15 cijfers configureren.

Om een eenmalige 7-15 cijferige gebruikersherstelpincode te configureren, voert u eerst de "**beheerdersmodus**" in zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** (ononderbroken BLAUWE LED) ga verder met onderstaande stappen.

1. Houd in de beheerdersmodus beide **SLEUTEL (⚷) + 4**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. . Voer de **eenmalige herstelpincode** in en druk op de **SLEUTEL (⚷)**-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 **eenmalige herstelpincode** in en druk weer op de **SLEUTEL (⚷)**-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 eenmalige herstelpincode 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.

16. Eenmalig herstel van gebruikerspincode verwijderen

Om een eenmalige **gebruikersherstelpincode** te verwijderen, 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. Houd in de beheerdersmodus beide **SHIFT** (⬆) **+ 4**-knoppen ingedrukt		Ononderbroken BLAUWE LED zal veranderen naar een knipperende RODE LED
2. Houd beide **SHIFT (⬆) + 4**-knoppen ingedrukt		Knipperende RODE LED gaat naar ononderbroken ROOD en verandert vervolgens naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de Eenmalige herstelpincode met succes is 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.

17. Herstelmodus activeren en nieuwe gebruikerspincode aanmaken

De herstelpincode voor gebruikers is uitermate nuttig in situaties waarin een gebruiker zijn pincode om de diskAshur M² te ontgrendelen, is vergeten. Om de herstelmodus te activeren, moet de gebruiker eerst de juiste eenmalige herstelpincode invoeren, indien deze is geconfigureerd. Het herstelproces van de gebruikerspincode heeft geen invloed op de gegevens, de encryptiesleutel en de beheerderspincode, maar de gebruiker moet een nieuwe gebruikerspincode met 7-15 cijfers configureren.

Om het herstelproces te activeren en een nieuwe gebruikerspincode te configureren, gaat u verder met de volgende stappen.

1. In **Stand-by Status** (RODE LED) houdt u beide **SLEUTEL (⚷) + 4**-knoppen ingedrukt		Ononderbroken RODE LED verandert naar knipperende RODE en ononderbroken GROENE LED's
2. Voer de eenmalige **herstelpincode** in en druk op de **SLEUTEL (⚷)**-knop		GROENE en BLAUWE LED's gaan afwisselend aan en uit en dan naar een ononderbroken GROENE LED en tenslotte naar knipperende GROENE en ononderbroken BLAUWE LED's
3. Voer **nieuwe gebruikerspincode** in en druk op **SLEUTEL (⚷)**-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
4. Voer uw **nieuwe gebruikerspincode** opnieuw in en druk weer op de **SLEUTEL (⚷)**-knop		GROENE LED knippert snel en wordt ononderbroken GROENE waarmee wordt aangeduid dat het herstelproces is geslaagd en een nieuwe gebruikerspincode werd geconfigureerd

Belangrijk: De creatie van een nieuwe 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. Raadpleeg hoofdstuk 9 om beperkingen van de gebruikerspincode te controleren.

18. Alleen-lezen toegang voor gebruiker instellen in de beheerdersmodus

Met zoveel virussen en trojans die USB-drives infecteren, is de alleen-lezen-functie vooral handig als u toegang moet hebben tot gegevens op de USB-drive als hij gebruikt wordt in een openbare omgeving. Dit is ook een essentieel kenmerk voor forensische doeleinden, waarbij gegevens in de oorspronkelijke en ongewijzigde toestand moeten worden bewaard die niet kan worden aangepast of overschreven.

Wanneer de beheerder de diskAshur M² configureert en de gebruikerstoegang beperkt tot alleen-lezen, kan alleen de beheerder schrijven naar de drive of de instelling terug veranderen naar ezen/schrijven zoals beschreven in hoofdstuk 19. De gebruiker is beperkt tot alleen-lezen toegang en kan niet schrijven naar de drive of deze instelling wijzigen in de gebruikersmodus.

Om de diskAshur M² in te stellen en gebruikerstoegang beperken tot alleen-lezen, gaat u eerst naar de "**beheerdersmodus**" zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

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 **SLEUTEL (⚷)**-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.

19. Gebruiker lezen/schrijven in de beheerdersmodus inschakelen

Om de diskAshur M² 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 **SLEUTEL (🔑)**-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.

20. Globale alleen-lezen toegang in de beheerdersmodus instellen

Wanneer de beheerder de diskAshur M² configureert en het beperkt tot globaal alleen-lezen, kan noch de beheerder noch de gebruiker schrijven naar de drive en beiden zijn beperkt tot alleen-lezen toegang. Enkel de beheerder kan de instelling terug veranderen naar lezen/schrijven zoals beschreven in hoofdstuk 21.

Om de diskAshur M² in te stellen en globale toegang te beperken tot alleen-lezen, gaat u eerst naar de "**beheerdersmodus**" zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. In beheerdersmodus houdt u beide **"5 + 6"**-knoppen ingedrukt.		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk op de **SLEUTEL (🔑)**-knop		GROENE en BLAUWE LED's zullen veranderen naar een ononderbroken GROENE LED en dan naar een ononderbroken BLAUWE LED om aan te geven dat de drive is geconfigureerd en de globale 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.

21. Globaal lezen/schrijven in de beheerdersmodus inschakelen

Om de diskAshur M² terug in te stellen naar lezen/schrijven, vanuit de globale alleen-lezen instelling, gaat u eerst naar de "**beheerdersmodus**" zoals beschreven in hoofdstuk 5. Zodra de drive in **beheerdersmodus** is (ononderbroken BLAUWE LED) gaat u verder met de volgende stappen.

1. In beheerdersmodus houdt u beide "**5 + 9**"-knoppen ingedrukt.		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk op de **SLEUTEL (🔑)**-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. Zelfvernietigingspincode configureren

U kunt een zelfvernietigingspincode configureren die bij invoer een Crypto-Erase op de drive uitvoert (de encryptiesleutel wordt verwijderd). Dit proces verwijdert alle geconfigureerde pincodes en maakt alle gegevens die op de drive zijn opgeslagen ontoegankelijk (voor altijd verloren), de drive wordt dan weergegeven als ontgrendeld GROENE LED. Als u deze functie uitvoert, wordt de zelfvernietigingspincode de nieuwe gebruikerspincode en moet de drive worden geformatteerd voordat hij opnieuw gebruikt kan worden.

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 **SLEUTEL (🔑)** + 6-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Configureer en voer een 7-15-cijferige **zelfvernietigingspincode** in en druk op de **SLEUTEL (🔑)**-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 **SLEUTEL (🔑)**-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.

23. 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

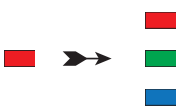
Opmerking: Om de beheerdersmodus onmiddellijk te verlaten (ononderbroken BLAUWE LED), houdt u de **SHIFT** (⬆)-knop een seconde ingedrukt - de ononderbroken BLAUWE LED schakelt over naar een ononderbroken RODE LED.

24. Zelfvernietigingspincode ontgrendelen

Waarschuwing: Als het zelfvernietigingsmechanisme is geactiveerd, worden alle gegevens, de coderingssleutel en de beheerders-/gebruikerspincodes verwijderd. **De zelfvernietigingspincode wordt de gebruikerspincode.** Er is geen beheerderspincode nadat het zelfvernietigingsmechanisme is geactiveerd. De diskAshur M² moet eerst worden gereset (zie 'Een volledige reset uitvoeren' hoofdstuk 35, op pagina 211) om een beheerderspincode met volledige beheerdersrechten te configureren, inclusief de mogelijkheid om een nieuwe gebruikerspincode te configureren.

Indien gebruikt, verwijdert de zelfvernietigingspincode **ALLE data, beheerders-/gebruikerspincodes** en ontgrendelt dan de drive. Het activeren van deze functie leidt ertoe dat de **zelfvernietigingspincode de nieuwe gebruikerspincode wordt** en de diskAshur M² moet worden geformatteerd voordat er nieuwe data aan de drive kunnen worden toegevoegd.

Om het zelfvernietigingsmechanisme te activeren, moet de drive in de stand-by positie staan (ononderbroken RODE LED) en vervolgens verder gaan met de volgende stappen.

1. Houd in **stand-by status** (ononderbroken RODE LED) de **SHIFT** (⬆) + **KEY (🔑)**-knoppen ingedrukt		RODE LED wisselt naar alle LED's, ROOD, GROEN & BLAUW die aan en uit knipperen
2. Voer de eenmalige **zelfvernietigingspincode** in en druk op de **SLEUTEL (🔑)**-knop		RODE, GROENE en BLAUWE knipperende LED's veranderen naar GROENE en BLAUWE LED's die gedurende enkele seconden afwisselend aan en uit gaan en dan uiteindelijk een ononderbroken GROENE LED worden, waarmee wordt aangeduid dat de diskAshur M² zichzelf met succes heeft vernietigd

25. Beheerderspincode configureren of opnieuw instellen na een brute aanval

Het is noodzakelijk om na een brute aanval of wanneer de diskAshur M² opnieuw is ingesteld om een beheerderspincode te configureren voordat de drive kan worden gebruikt.

Vereisten voor pincode:

- Moet tussen de 7 en 15 cijfers lang zijn
- Mag niet alleen herhalende cijfers bevatten, bijv. (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)

Als de diskAshur M² 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 **SLEUTEL** (⬆) **+ 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 **SLEUTEL (🔑)**-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 **SLEUTEL (🔑)**-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.

26. De onbeheerde automatische vergrendeling instellen

Als beveiliging tegen ongeautoriseerde toegang als de drive ontgrendeld en onbewaakt is, kan de diskAshur M² worden ingesteld naar automatische vergrendeling na een vooraf ingestelde tijdsduur. In de standaardstatus is de time-out functie van de diskAshur M² 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 **SLEUTEL (🔑) + 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.

27. 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 **SLEUTEL (🔑) + 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.

28. 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 **SLEUTEL (🔑)**-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.

29. Alleen-lezen in de gebruikersmodus instellen

Om de diskAshur M² 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 **SLEUTEL (🔑)**-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.

30. Lezen/schrijven in gebruikersmodus inschakelen

Om de diskAshur M² 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 **SLEUTEL (🔑)**-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.

31. Verdedigingsmechanisme tegen brute aanvallen

De diskAshur M² bevat een verdedigingsmechanisme om de drive te beschermen tegen brute aanvallen. De standaardwaarden van de eerste verzendingsstatus van de beperking van de brute aanvallen (opeenvolgende onjuiste pincode-invoer) voor zowel de beheerderspincode als de gebruikerspincode is 10 en 5 voor de herstelpincode. Er worden drie onafhankelijke tellers voor brute aanvallen gebruikt om de verkeerde pogingen voor elke pincode-autorisatie (beheerder, gebruiker en herstel) te registeren zoals hieronder uiteengezet.

- Als een gebruiker 10 opeenvolgende keren een **onjuiste gebruikerspincode** invoert, wordt de gebruikerspincode verwijderd, maar de gegevens, de beheerderspincode en herstelpincode blijven intact en toegankelijk.
- Als 5 opeenvolgende keren een **onjuiste herstelpincode** wordt ingevoerd, wordt de herstelpincode verwijderd, maar blijven de gegevens en de beheerderspincode intact en toegankelijk.
- Als een gebruiker 10 opeenvolgende keren een **onjuiste gebruikerspincode** invoert, wordt de drive opnieuw ingesteld. Alle pincodes en data worden verwijderd en zijn voor altijd verloren.

De onderstaande tabel gaat ervan uit dat de drie pincodes zijn ingesteld en benadrukt het effect van het activeren van het verdedigingsmechanisme tegen brute aanvallen van elke individuele pincode.

Pincode om de drive te ontgrendelen	Opeenvolgende onjuiste pincodes ingevoerd	Beschrijving wat er gebeurt
Gebruikerspincode	10	• De gebruikerspincode wordt verwijderd. • De herstelpincode, de beheerderspincode en alle data blijven intact en toegankelijk.
Herstelpincode	5	• De herstelpincode is verwijderd. • De beheerderspincode en alle data blijven intact en toegankelijk.
Beheerderspincode	10	• De diskAshur M² zal resetten. Alle pincodes en data worden verwijderd en zijn voor altijd verloren.

Opmerking: De beperking van brute aanvallen wordt standaard ingesteld op de oorspronkelijke waarden van de verzendingsstatus wanneer de drive volledig wordt gereset, of de zelfvernietigingsfunctie is geactiveerd, of gekraakt. Als de beheerder de gebruikerspincode wijzigt, of er wordt een nieuwe gebruikerspincode ingesteld als de herstelfunctie wordt ingesteld, zal de teller van brute aanvallen op de gebruikerspincode op nul worden gezet (0), maar de beperking van brute aanvallen wordt hierbij niet beïnvloed. Als de beheerder de herstelpincode verandert, wordt de teller van brute aanvallen van de herstelpincode op nul gezet.

Mislukte autorisatie van een bepaalde pincode zal de teller voor die specifieke pincode verhogen, maar heeft geen invloed op de teller van de andere pincodes. Mislukte autorisatie van een bepaalde pincode zal de teller voor die specifieke pincode verhogen, maar heeft geen invloed op de teller van de andere pincodes.

32. Admin PIN Brute Force Hack Verdedigingsmechanisme

De diskAshur M² Admin PIN is uitgerust met een geavanceerder verdedigingsmechanisme in vergelijking met de User PIN of de Recovery PIN. Dit is bedoeld om te voorkomen dat u per ongeluk 10 keer achter elkaar een verkeerde Admin PIN-code invoert en vervolgens al uw gegevens kwijtraakt. Dus na het 5x achter elkaar invoeren van een foutieve Admin PIN-code, zal de diskAshur M² vergrendelen en zullen alle LED-lampjes oplichten en blijven branden.

WAARSCHUWING: Probeer niet de instructies te volgen als u uw diskAshur M² heeft ontgrendeld met slechts de '**GEBRUIKERSPINCODE**' en u de '**ADMIN PINCODE**' niet weet.

Raadpleeg de instructies in de onderstaande tabel voor meer informatie over het instellen van de Admin PIN-code tot een maximum van 10.

Achter elkaar foutief ingevoerde Admin PIN-codes	Beschrijving van wat er gebeurt met de diskAshur M²	Instructies
5	Alle LED-lampjes, **ROOD**, **GROEN** & **BLAUW** gaan aan en blijven branden.	Voer de volgende PIN-code '**47867243**' in en druk eenmaal op de **TOETS** (), met zowel het **GROENE** als het **BLAUWE** LED-lampje afwisselend aan en uit knipperend, is de diskAshur M2 klaar om nog eens **3 Admin PIN-codes te accepteren**.
8	Alle LED-lampjes, **ROOD**, **GROEN** & **BLAUW** knipperen afwisselend aan en uit.	Voer de volgende PIN-code '**47867243**' in en druk eenmaal op de **TOETS** (), met zowel het **GROENE** als het **BLAUWE** LED-lampje afwisselend aan en uit knipperend, is de diskAshur M2 klaar om nog eens **2 Admin PIN-codes te accepteren**.
10	**RODE** LED-lampje gaat aan en blijft branden	Na in totaal 10x een foutieve invoer van de Admin PIN-code, worden de coderingssleutel, alle PIN-codes en gegevens gewist en gaan ze voorgoed verloren.

33. De gebruikerspincode instellen om brute aanvallen te beperken

Opmerking: De beperking van brute aanvallen op de gebruikerspincode is standaard ingesteld op 10 opeenvolgende onjuiste pogingen van de pincode als de drive hetzij geheel gereset is, gekraakt of de zelfvernietigingspincode is geactiveerd.

De beperking tegen brute aanvallen voor de gebruikerspincode van diskAshur M² kan geherprogrammeerd en ingesteld worden door de beheerder. Deze functie kan worden ingesteld om pogingen van 1 tot 10 opeenvolgende onjuiste pincodes toe te staan.

Om beperking van de brute aanvallen op de gebruikerspincode te configureren, 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 **7 + 0** knoppen		Ononderbroken BLAUWE LED verandert naar GROENE en BLAUWE LED's die tegelijkertijd knipperen
2. Voer het aantal pogingen in voor het beperken van brute aanvallen (tussen 01-10), voer bijvoorbeeld in: • **01** voor 1 poging • **10** voor 10 pogingen		
3. Druk eenmaal op de SHIFT (⬆)-knop		Knipperende GROENE en BLAUWE LED's veranderen gedurende een seconde naar een ononderbroken GROENE LED en tenslotte naar een ononderbroken BLAUWE LED waarmee wordt aangeduid dat de beperking van brute aanvallen met succes 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.

34. De gebruikerspincode tegen beperking van brute aanvallen controleren

De beheerder kan zien en bepalen hoe vaak een onjuiste gebruikerspincode mag worden ingevoerd voordat het verdedigingsmechanisme van brute aanvallen wordt geactiveerd door eenvoudig te letten op de LED volgorde zoals hieronder beschreven.

Om de beperking van brute aanvallen-instelling 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. Houd in de beheerdersmodus beide **2 + 0** knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en ononderbroken BLAUWE LED's
2. Druk op de **SLEUTEL (🔑)**-knop en het volgende gebeurt; a. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde. b. Elke knippering van de ROOD LED komt overeen met (10) eenheden van het aantal beperkingen van brute aanvallen. c. Elke knippering van de GROENE LED komt overeen met een (1) enkele eenheid van het aantal beperkingen van brute aanvallen. 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 instelling voor beperking van brute aanvallen, bijvoorbeeld als u de drive op brute aanval hebt ingesteld na **5** achtereenvolgende foute pogingen tot invoeren van de pincode, zal de GROENE LED vijf keer (**5**) knipperen.

Instelling voor beperking van brute aanvallen	ROOD	GROEN
2 pogingen	0	2 knipperingen
5 pogingen	0	5 knipperingen
10 pogingen	1 knippering	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.

35. Een volledige reset uitvoeren

Om een volledige reset uit te voeren moet diskAshur M² 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 diskAshur M² 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 25 op pagina 205 in 'Het configureren of opnieuw instellen na een brute aanval of reset', de diskAshur M² zal ook opnieuw moeten worden geformatteerd voordat er nieuwe data aan de drive kunnen worden toegevoegd.

36. diskAshur M² als opstartbaar configureren

Opmerking: Wanneer de drive is ingesteld als opstartbaar, zal het uitwerpen van de drive uit het besturingssysteem de LED niet forceren om ROOD te worden. De drive blijft ononderbroken GROEN en moet worden losgekoppeld voor het volgende gebruik. De standaardinstelling van de diskAshur M² wordt geconfigureerd als niet opstartbaar.

De diskAshur M² is uitgerust met een opstartfunctie om power cycling tijdens het opstarten van een host mogelijk te maken. Als u opstart vanuit de diskAshur M², draait u uw computer met het besturingssysteem dat is geïnstalleerd op de diskAshur M².

Om de drive als opstartbaar 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 **SLEUTEL (🔑) + 8**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk op "**0**" gevolgd door **"1"** (**01**)		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 en tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat de drive met succes werd geconfigureerd als opstartbaar

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.

37. De diskAshur M² opstartfunctie uitschakelen

Om de diskAshur M² opstartfunctie uit te schakelen, gaat u eerst naar de "**beheerdersmodus**" 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 **SLEUTEL (⚷) + 8**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's
2. Druk op **"0"** gevolgd door nog een **"0"** (**00**)		GROENE en BLAUWE LED's zullen blijven knipperen
3. Druk eenmaal op de **SHIFT** (⬆)-knop		Knipperend GROENE en BLAUWE LED's veranderen naar een ononderbroken GROENE LED en tenslotte naar een ononderbroken BLAUWE LED om aan te duiden dat de opstartfunctie 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.

38. De opstartinstelling controleren

Om de opstartinstelling 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** (⬆) **+ 8**-knoppen ingedrukt		Ononderbroken BLAUWE LED verandert naar knipperende GROENE en BLAUWE LED's

2. Druk op de **SLEUTEL (⚷)**-knop en een van de volgende scenario's zal plaatsvinden;

- **Als diskAshur M² is geconfigureerd als opstartbaar, gebeurt het volgende;**

a. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde.
b. GROENE LED knippert eenmaal.
c. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde.
d. LED's worden terug ononderbroken BLAUW

- **Als diskAshur M² <u>NIET</u> is geconfigureerd als opstartbaar, gebeurt het volgende;**

a. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde.
b. Alle LED's zijn uit
c. Alle LED's (ROOD, GROEN & BLAUW) branden ononderbroken gedurende 1 seconde.
d. LED's worden terug ononderbroken BLAUW

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.

39. Initialiseren en formatteren van diskAshur M² voor Windows

Na een 'brute aanval' of een volledige reset zal de diskAshur M² alle pincodes, gegevens en de encryptiesleutel verwijderen. U zult de diskAshur M² moeten initialiseren en formatteren voor hij gebruikt kan worden.

Om uw diskAshur M² te formatteren doet u het volgende:

1. Configureer een nieuwe beheerderspincode - zie pagina 205, hoofdstuk 25, 'Een beheerderspincode configureren na een brute aanval of reset'.

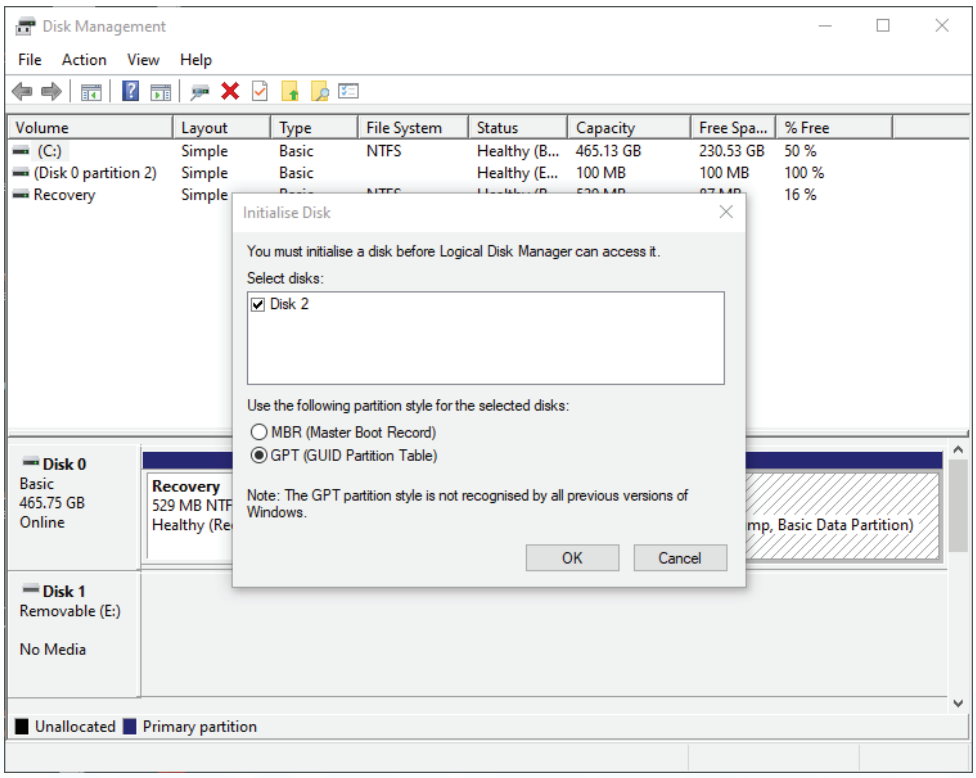
2. Met de diskAshur M² in stand-by status (RODE LED), drukt u eenmaal op de **SLEUTEL (🔑)**-knop en voert de **nieuwe beheerderspincode** in om te ontgrendelen (knipperende GROENE LED).

3. Sluit de diskAshur M² aan op de computer.

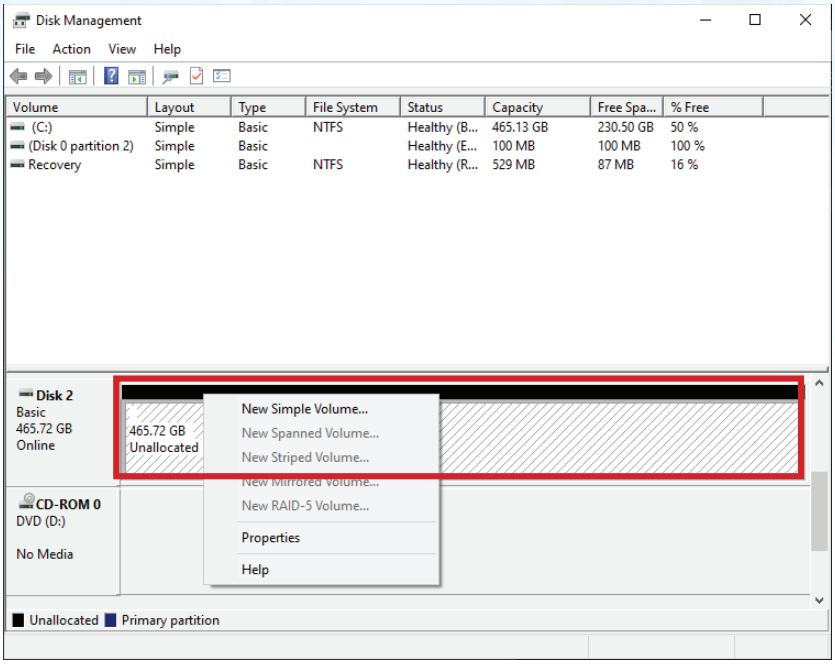
4. **Windows 7:** Klik met de rechtermuisknop op **Computer** en klik dan op **Manage (Beheer)** en selecteer **Disk Management (Schijfbeheer)**
   Windows 8: Klik met de rechtermuisknop op de linkerhoek van de desktop en selecteer **Disk Management (Schijfbeheer)**
   Windows 10: Klik met de rechtermuisknop op de startknop en kies **Disk Management (Schijfbeheer)**

5. In het venster Disk Management (Schijfbeheer) wordt de diskAshur M² herkend als een onbekend apparaat dat niet is geïnitialiseerd en niet is toegewezen. Er verschijnt een berichtvenster zodat u kunt kiezen tussen MBR- en GPT-partitiestijl. GPT slaat meerdere duplicaten van deze gegevens op over de disk, waardoor hij veel robuuster is. Op een MBR-disk worden de partitionerings- en opstartinformatie opgeslagen in een enkele locatie.

   Selecteer de partitiestijl en klik op **OK**.



6. Klik met de rechtermuisknop in het lege gebied boven de **Unallocated (Niet-toegewezen)** sectie, en kies dan **New Simple Volume (Nieuw, eenvoudig volume).**



7. Het venster Welcome to the New Simple Volume Wizard opent. Klik op volgende



8. Als u slecht een partitie nodig hebt, accepteer dan de standaard partitiegrootte en klik op **Volgende**.

9. Wijs een disk letter of pad toe en klik op **Volgende**.

10. Maak een volume label aan, selecteer snelle formattering uitvoeren en klik dan op **Volgende**.

11. Klik op **Finish (Klaar)**.

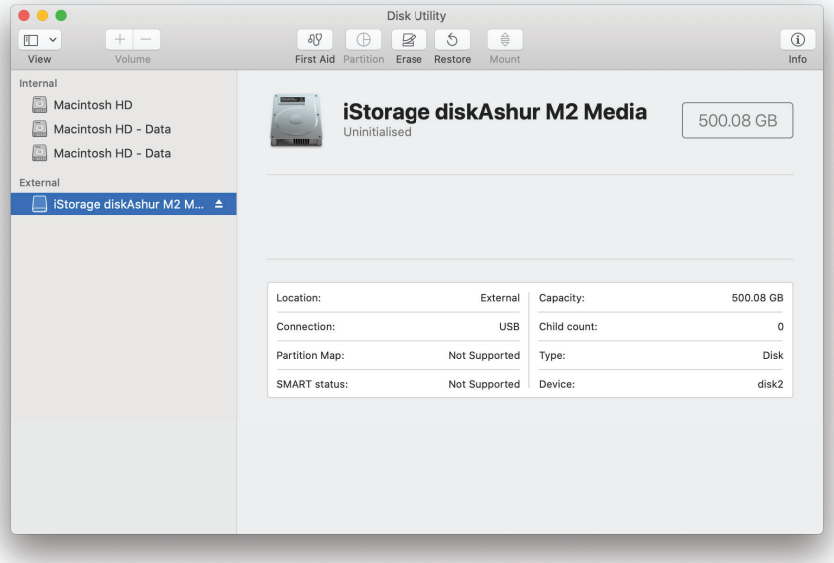
12. Wacht totdat het formatteringsproces volledig klaar is. De diskAshur M² zal worden herkend en is klaar voor gebruik.

40. Initialiseren en formatteren van diskAshur M² in Mac OS

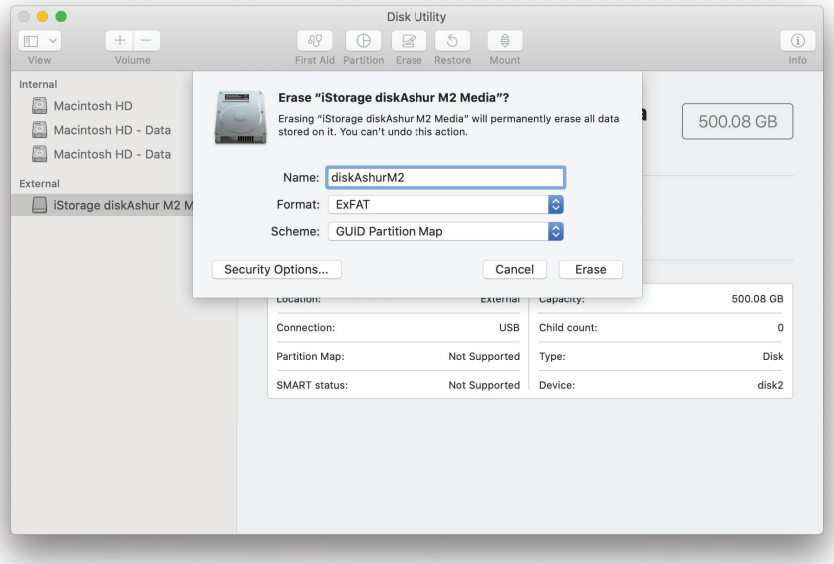
Na een 'brute aanval' of een volledige reset zal de diskAshur M² alle pincodes, gegevens en de encryptiesleutel verwijderen. U zult de diskAshur M² moeten initialiseren en formatteren voor hij gebruikt kan worden.

Om de diskAshur M² te initialiseren en formatteren:

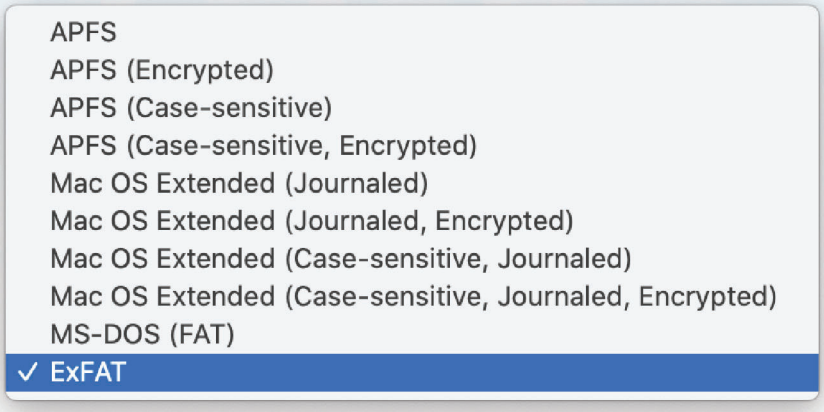
1. Selecteer diskAshur M² van de lijst van drives en volumes. Elke drive in de lijst geeft de capaciteit, fabrikant en productnaam weer, zoals '**iStorage diskAshur M² Media**'.



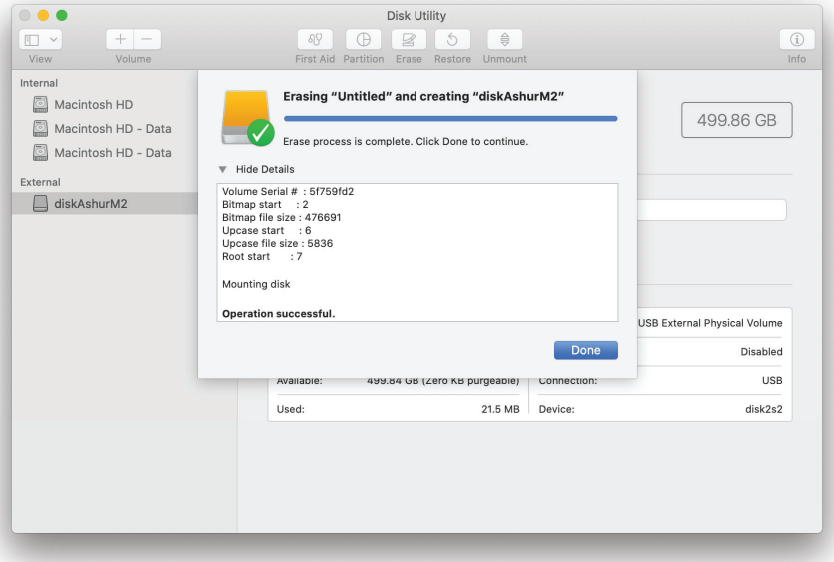
2. Klik op de '**wissen**'-knop onder Disk Utility (schijfhulpprogramma).
3. Voer een naam in voor de drive. De standaardnaam is Untitled (zonder titel). De naam van de drive zal dan op de desktop verschijnen.



4. Selecteer een schema en volumeformaat om te gebruiken. Het vervolgkeuzemenu volumeformaat geeft een overzicht van de beschikbare driveformaten die de Mac ondersteunt. Het aanbevolen formaattype is 'Mac OS Extended (Journaled)'. Gebruik exFAT over verschillende platformen. Het vervolgkeuzemenu voor schema-indeling geeft een overzicht van de beschikbare schema's die u kunt gebruiken. We raden aan om 'GUID Partition Map' te gebruiken voor schijven die groter zijn dan 2 TB.

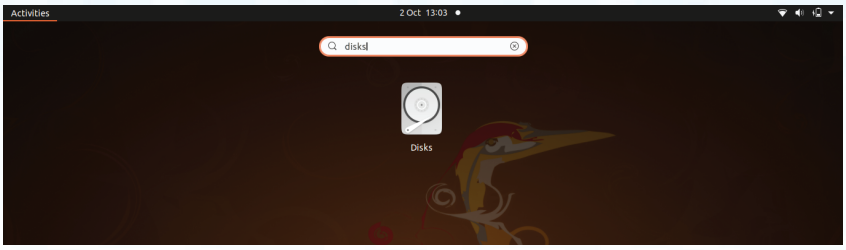


5. Klik op de 'wissen' -knop. Het schijfhulpprogramma ontkoppelt het volume van de desktop, wist het en plaatst het vervolgens opnieuw op de desktop.

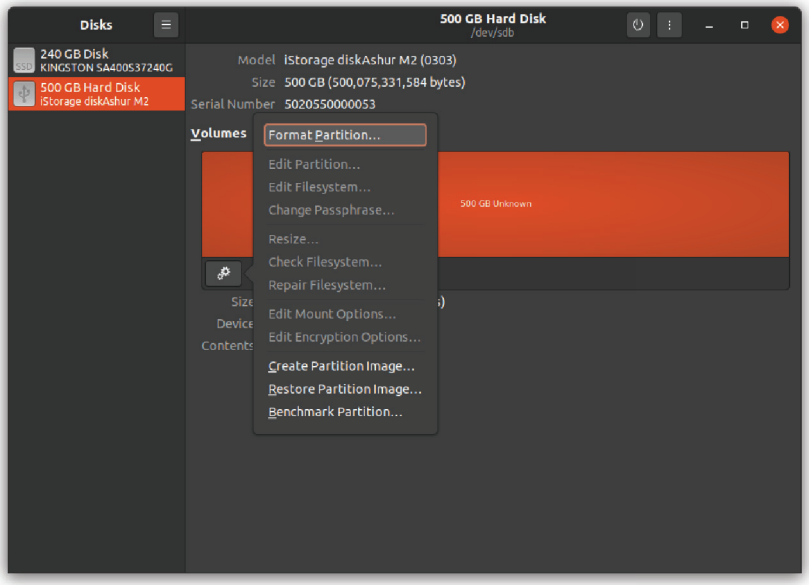


41. Initialiseren en formatteren van diskAshur M² in Linux OS

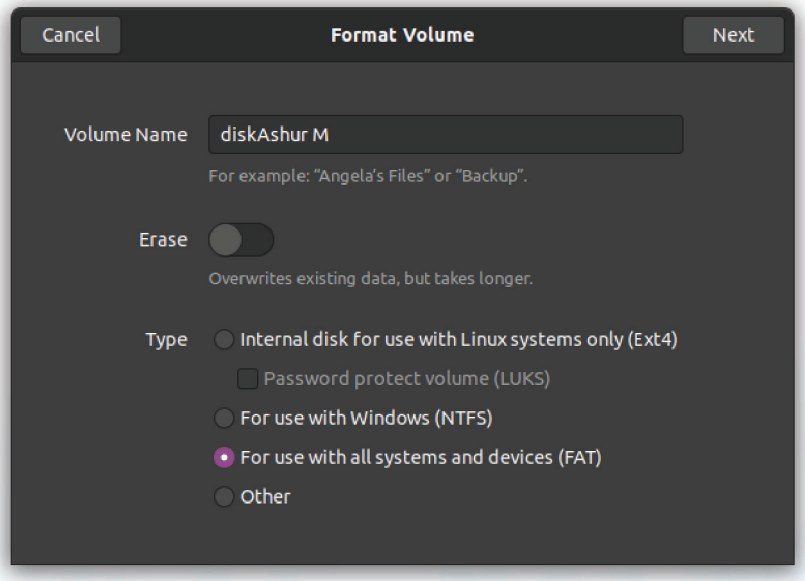
1. Open '**toon applicatie**' en type '**Disks**' in het zoekvak. Klik op het hulpprogramma '**Disks**' wanneer het wordt weergegeven.



2. Klik om de drive (500 GB harde schijf) te selecteren bij '**Apparaten**'. Klik vervolgens op het tandwielpictogram onder '**Volumes**' en klik dan op '**Partities formatteren**'.

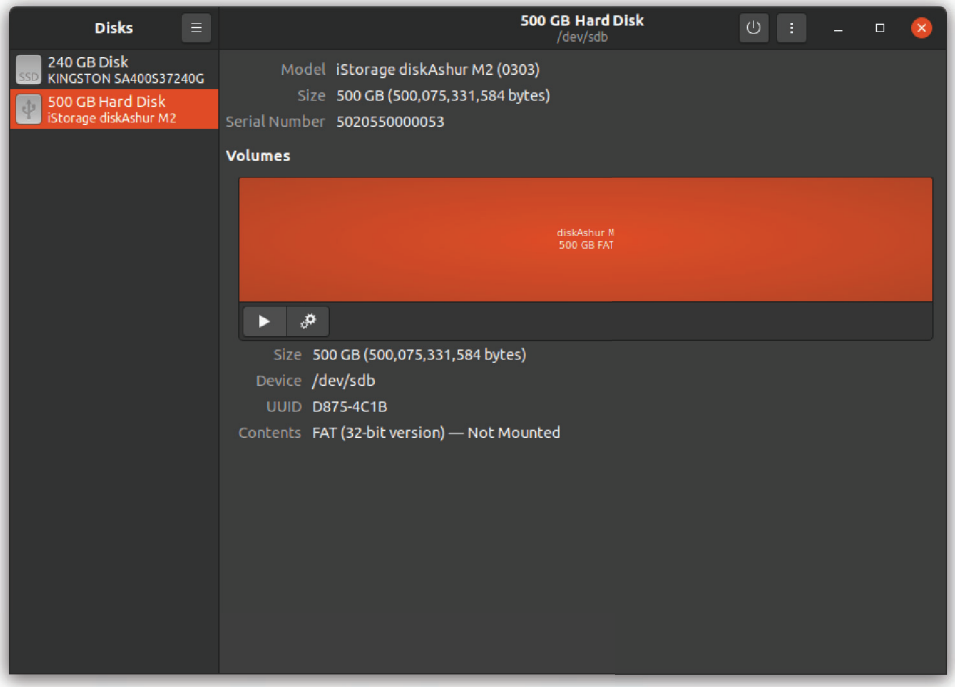


3. Selecteer '**Compatibel met alle systemen en apparaten (FAT)**' voor de '**Type**'-optie. En voer een naam in voor de drive, bijv. diskAshur M². Klik dan op de '**Format**'-knop.

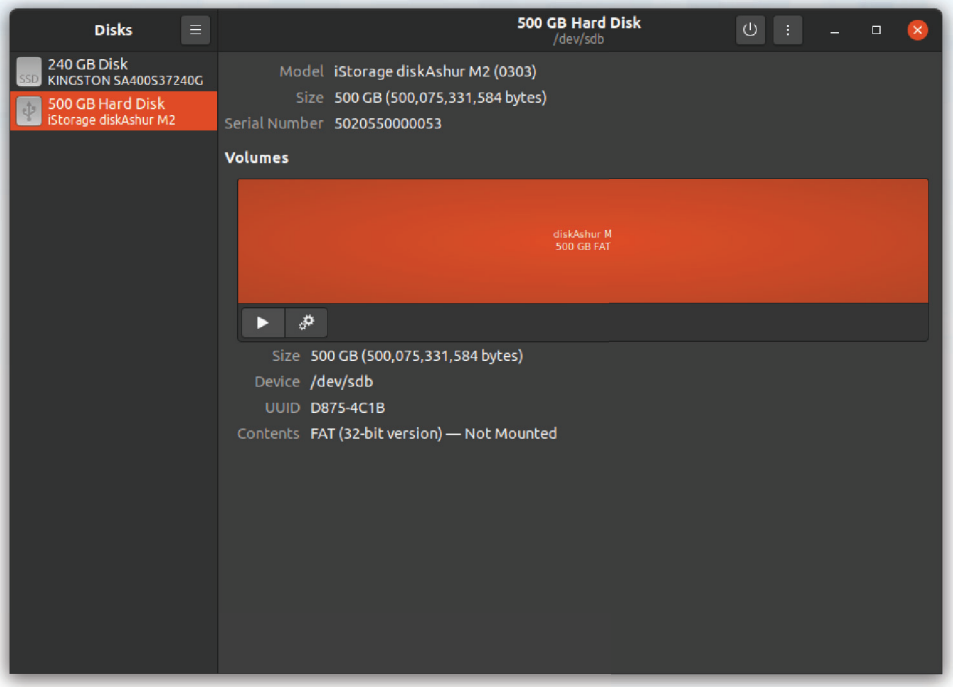




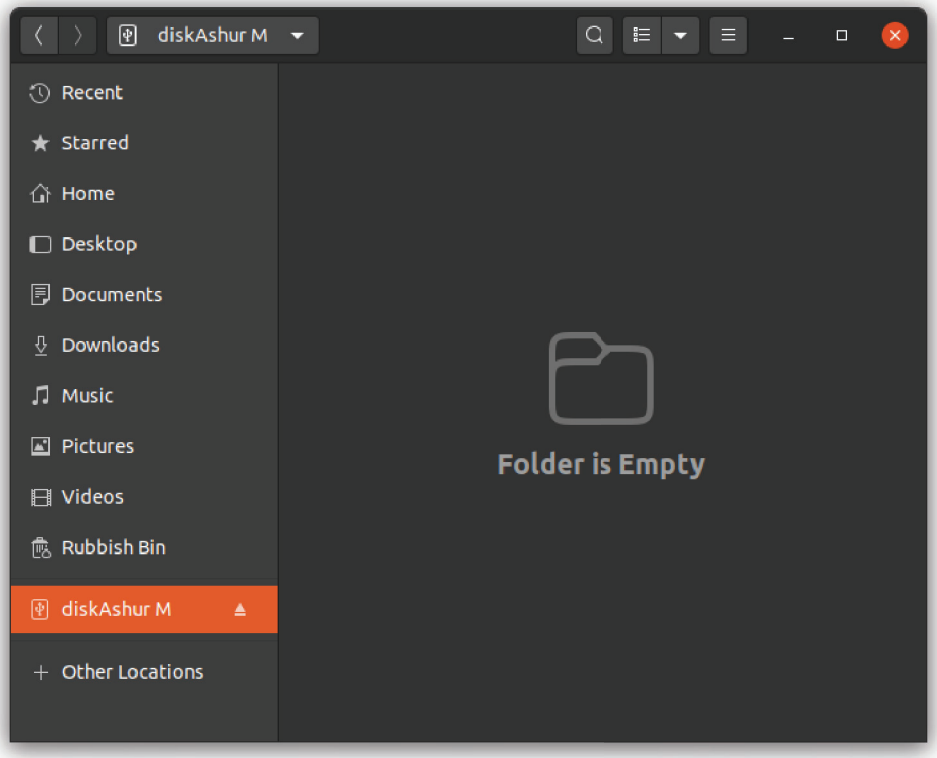
4. Nadat het formatteerproces is voltooid, klikt u op de afspeelknop om de drive aan Ubuntu te koppelen.



5. De drive moet aan Ubuntu worden gekoppeld en is klaar voor gebruik.



6. De disk wordt weergegeven zoals te zien in de onderstaande afbeelding. U kunt op het disk-pictogram klikken om uw drive te openen.



42. In slaapstand gaan, opschorten of afmelden bij het besturingssysteem

Zorg ervoor dat u alle bestanden op uw diskAshur M² opslaat en sluit voordat u in slaapstand gaat, opschort of uitlogt van het besturingssysteem.

Het is aanbevolen dat u de diskAshur M² handmatig vergrendelt voordat u in slaapstand gaat, opschort of uitlogt uit uw systeem.

Om de drive te vergrendelen, moet u de diskAshur M² 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 diskAshur M² resulteren in onvolledige datatransfer en mogelijke corruptie van gegevens.

⚠ **Opgelet:** Om ervoor te zorgen dat uw gegevens veilig zijn, moet u uw diskAshur M² vergrendelen als u niet achter uw computer zit.

43. 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 **SLEUTEL (♿)**-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.

44. 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 **SLEUTEL (⚷)**-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.

45. 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.

46. 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]

Copyright © iStorage Limited 2020. Alle rechten voorbehouden.
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

DISKASHUR® M²

iStorage®

Manual del usuario



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 diskAshur M², 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.

Copyright © iStorage Limited 2020. Todos los derechos reservados.

Windows es una marca registrada de Microsoft Corporation.
Todas las demás marcas comerciales y derechos de autor mencionados son propiedad de sus correspondientes dueños.

Está prohibida la distribución de versiones modificadas de este documento sin el permiso expreso del titular de los derechos de autor.

Está prohibida la distribución del trabajo o del trabajo derivado en cualquier formato de libro estándar (en papel) con fines comerciales, a menos que se obtenga el permiso previo del propietario de los derechos de autor.

LA DOCUMENTACIÓN SE PROPORCIONA TAL CUAL Y SE RENUNCIA A TODAS LAS CONDICIONES, DECLARACIONES Y GARANTÍAS EXPRESAS O IMPLÍCITAS, INCLUIDAS CUALESQUIERA GARANTÍAS IMPLÍCITAS DE COMERCIABILIDAD, DE ADECUACIÓN A UN FIN PARTICULAR O DE NO INFRACCIÓN, EXCEPTO EN LA MEDIDA EN QUE DICHAS EXENCIONES DE RESPONSABILIDAD SEAN CONSIDERADAS COMO LEGALMENTE NULAS

RoHS Compliant

REACH COMPLIANCE

Todas las marcas comerciales y nombres de marcas son propiedad de sus correspondientes dueños.

Cumple con la Ley de Acuerdos Comerciales (TAA)

CITRIX® vmware®

Índice

Introducción 227
Contenido de la caja 227
Diseño del diskAshur M² 227
1. Indicadores LED y sus acciones 228
2. Estados LED 228
3. Uso por primera vez 229
4. Desbloquear diskAshur M² con el PIN de administrador 230
5. Cómo acceder al modo administrador 230
6. Cambiar el PIN de administrador 231
7. Establecer una política de PIN de usuario 232
8. Cómo eliminar la política de PIN de usuario 233
9. Cómo verificar la política de PIN de usuario 233
10. Agregar un PIN de usuario nuevo en modo administrador 234
11. Cambiar el PIN de usuario en modo administrador 235
12. Eliminar el PIN de usuario en modo administradorr 235
13. Cómo desbloquear diskAshur M² con PIN de usuario 236
14. Cambiar el PIN de usuario en modo usuario 236
15. Crear un PIN único de recuperación de usuario 237
16. Eliminar el PIN único de recuperación de usuario 237
17. Activar el modo de recuperación y crear un PIN de usuario nuevo 238
18. Establecer usuario solo lectura en modo administrador 238
19. Permitir al usuario leer/escribir en modo administrador 239
20. Establecer en solo lectura general en modo administrador 239
21. Permitir lectura/escritura general en modo administrador 240
22. Cómo configurar un PIN de autodestrucción 240
23. Cómo eliminar el PIN de autodestrucción 241
24. Cómo eliminar el PIN de autodestrucción 241
25. Cómo configurar un PIN de administrador después de un ataque de fuerza bruta o un reseteo 242
26. Establecer el bloqueo automático desatendido 242
27. Desactivar el bloqueo automático desatendido 243
28. Cómo verificar el bloqueo automático desatendido 244
29. Establecer en solo lectura en modo usuario 244
30. Habilitar lectura/escritura en modo usuario 245
31. Mecanismo de defensa de ataque de fuerza bruta 245
32. Mecanismo de defensa contra ataques de fuerza bruta del PIN del administrador 246
33. Cómo establecer la limitación de fuerza bruta del PIN de usuario 246
34. Cómo verificar la limitación de fuerza bruta del PIN de usuario 247
35. Cómo realizar un reseteo completo 248
36. Cómo configurar diskAshur M² para su arranque 248
37. Cómo deshabilitar la función de arranque del diskAshur M² 249
38. Cómo verificar la configuración de arranque 249
39. Iniciar y formatear el disco Ashur M² para Windows 250
40. Iniciar y formatear el disco Ashur M² en Mac OS 252
41. Iniciar y formatear diskAshur M² en Linux OS 254
42. Hibernar, suspender o cerrar sesión del sistema operativo 257
43. Cómo verificar el firmware en modo administrador 257
44. Cómo verificar el firmware en modo usuario 258
45. Asistencia técnica 259
46. Información de garantía y autorización de devolución de material (RMA) 259

Introducción

Gracias por comprar el nuevo iStorage diskAshur M², una unidad de estado sólido (SSD) portátil ultrasegura y fácil de usar, cifrada por hardware, autenticada con PIN y con capacidad de 120 GB a 2 TB y en aumento.

Diseñado para ser certificado FIPS 140-3 Nivel 3, diskAshur M² cifra los datos en tránsito y en reposo utilizando cifrado de hardware de disco completo AES-XTS de 256 bits.

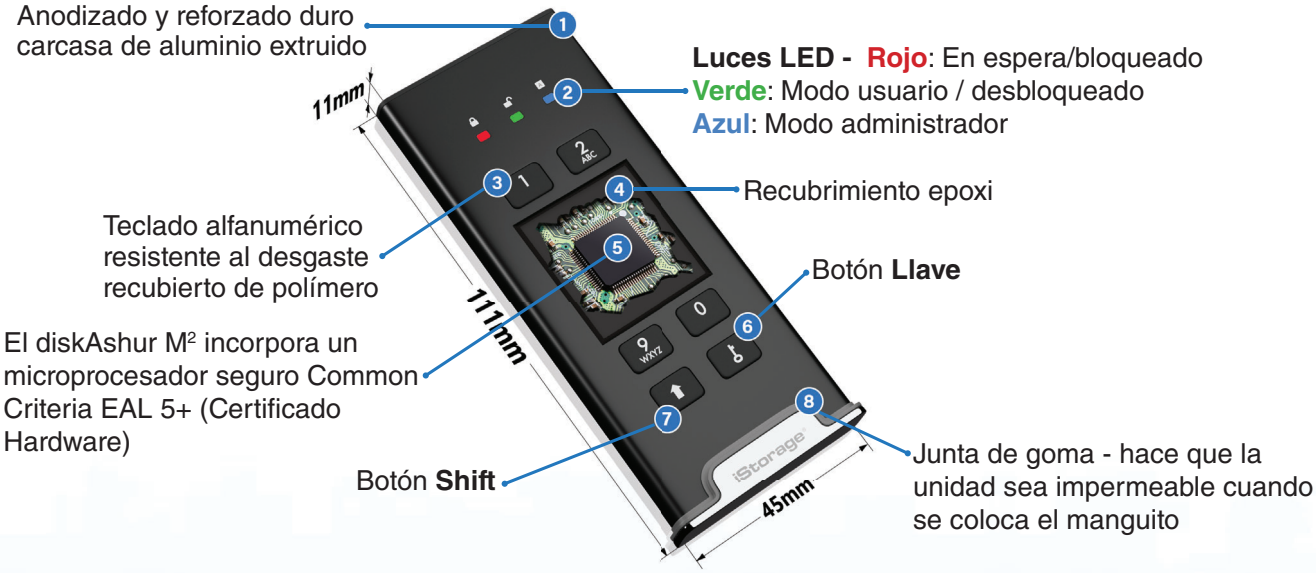
El diskAshur M2 incorpora un microprocesador seguro Common Criteria EAL 5+ (Certificado Hardware), que incorpora mecanismos de protección física diseñados para defenderse de manipulaciones externas, ataques bypass e inyecciones de fallos.

A diferencia de otras soluciones, el diskAshur M² reacciona a un ataque automatizado entrando en el estado congelado de punto muerto, lo que hace que todos esos ataques sean inútiles. Dicho de manera simple, sin el PIN no hay forma de entrar.

Contenido de la caja

- SSD portátil y funda protectora del diskAshur M²
- estuche
- cables USB C y A
- guía de inicio rápido y descargo de responsabilidad del product

Diseño del diskAshur M²



1. Indicadores LED y sus acciones

LED	Estado LED	Descripción	LED	Estado LED	Descripción
	ROJO fijo	Unidad bloqueada (en modo de **espera** o **reseteo**)		AZUL fijo	Unidad en **modo administrador**
	ROJO Parpadeo doble 	Introducción de PIN incorrecta		ROJO, VERDE y AZUL parpadeando juntos 	Esperando introducción del PIN de **usuario**
	VERDE fijo	Unidad **desbloqueada**		VERDE y AZUL parpadeando juntos 	Esperando introducción del PIN de **administrador**
	VERDE parpadeando 	Transferencia de datos en curso		VERDE y AZUL parpadeando alternativamente 	Autenticación en curso

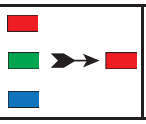
2. Estados LED

Nota: La función normal del diskAshur M2 puede ser perturbada por una fuerte interferencia electromagnética. Si esto ocurre, apague y luego encienda la unidad para reanudar el funcionamiento normal. Si el funcionamiento normal no se reanuda, utilice el dispositivo en un lugar diferente

Para despertar del estado de reposo

El estado de reposo se define como el momento en que diskAshur M² no se está utilizando y todos los LED están apagados.

Para reactivar diskAshur M² del estado de reposo, haga lo siguiente.

Conecte el diskAshur M² a un puerto USB con alimentación en su ordenador		Los LED ROJO, VERDE y AZUL parpadean una vez en secuencia, luego el LED VERDE parpadea dos veces y finalmente cambia a un LED ROJO fijo que indica que la unidad está en estado de espera

Para entrar en estado de reposo

Para forzar que diskAshur M² entre en estado de reposo, ejecute cualquiera de las siguientes operaciones:

- Desconecte la unidad si está conectada a un puerto USB, todos los LED se apagarán (estado de reposo).

Estados de encendido

Después de que la unidad haya salido del estado de reposo, entrará en uno de los siguientes estados que se muestran en la tabla de abajo.

Estado de encendido	Indicación LED	Clave de cifrado	PIN de administrador	Descripción
Estado de suministro inicial	ROJO y VERDE fijos	✓	×	Esperando la configuración de un PIN de administrador (uso por primera vez)
Espera	ROJO fijo	✓	✓	Esperando la introducción del PIN de administrador o usuario
Reseteo	ROJO fijo	×	×	Esperando la configuración de un PIN de administrador

3. Uso por primera vez

diskAshur M² se suministra en el '**estado de suministro inicial' sin un PIN de administrador preestablecido**. Se debe configurar un PIN de administrador de **7 a 15** dígitos antes de poder utilizar la unidad. Una vez que se haya configurado correctamente un PIN de administrador, no será posible volver a cambiar la unidad al 'estado de suministro inicial'.

Requisitos del PIN:

- Debe tener entre 7 y 15 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)

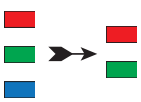
Consejo sobre la contraseña: Simplemente presionando el botón con las letras correspondientes, puede configurar una palabra de la que pueda acordarse, un nombre, una frase o cualquier otra combinación de PIN alfanumérico.

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 configurar un PIN de administrador y desbloquear el diskAshur M² por primera vez, siga los sencillos pasos de la siguiente tabla.

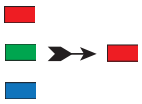
Instrucciones - Uso por primera vez	LED	Estado LED
1. Conecte el diskAshur M² a un puerto USB con alimentación en su ordenador		Los LED ROJO, VERDE y AZUL parpadean una vez en secuencia, el LED VERDE parpadea dos veces y finalmente cambia a LED ROJO y VERDE fijos que indican que la unidad está en el estado de suministro inicial
2. Mantenga presionados los botones **LLAVE (🔑) + 1**		Los LED cambian a VERDE parpadeante y a AZUL fijo
3. Introduzca un **PIN de administrador nuevo** (7-15 dígitos) y presione el botón **LLAVE (🔑)** una vez		Los LED VERDE parpadeante y AZUL fijo cambian a un parpadeo VERDE, luego de nuevo a LED VERDE parpadeante y AZUL fijo
4. Vuelva a introducir su **PIN de administrador nuevo** y presione nuevamente el botón **LLAVE (🔑)**		El LED AZUL parpadea rápidamente, luego cambia a LED AZUL fijo y finalmente a LED VERDE fijo, que indica que se ha configurado correctamente el PIN de administrador y se ha desbloqueado la unidad

Bloquear el diskAshur M²

Para bloquear la unidad, expulse de manera segura el diskAshur M² de su sistema operativo host y luego desconéctelo del puerto USB. Si se escriben datos en la unidad, desenchufar el diskAshur M² provocará una transferencia de datos incompleta y una posible corrupción de los datos.

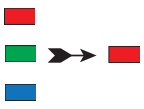
4. Desbloquear diskAshur M² con el PIN de administrador

Para desbloquear el diskAshur M² con el PIN de administrador, siga los sencillos pasos de la siguiente tabla.

1. Conecte el diskAshur M² a un puerto USB de su ordenador		Los LED ROJO, VERDE y AZUL parpadean una vez en secuencia, el LED VERDE parpadea luego dos veces y finalmente cambia a un LED ROJO fijo que indica que la unidad está en estado de espera
2. En estado de espera (LED ROJO fijo) presione el botón **LLAVE (⚷)** una vez		Los LED VERDE y AZUL parpadean juntos
3. Con los LED VERDE y AZUL parpadeando juntos, introduzca el **PIN de administrador** y presione nuevamente el botón **LLAVE (⚷)**		Los LED VERDE y AZUL parpadearán alternativamente varias veces y luego se quedarán en un LED AZUL fijo y cambiando a un LED VERDE fijo que indica que la unidad se ha desbloqueado correctamente en administrador

5. Cómo acceder al modo administrador

Para acceder al modo administrador, haga lo siguiente.

1. Conecte el diskAshur M² a un puerto USB con alimentación en su ordenador		Los LED ROJO, VERDE y AZUL parpadean una vez en secuencia, el LED VERDE parpadea luego dos veces y finalmente cambia a un LED ROJO fijo que indica que la unidad está en estado de espera
2. IEn estado de espera (LED ROJO fijo) mantenga presionados los botones **LLAVE (⚷) + 1**		Los LED VERDE y AZUL parpadean juntos
3. Introduzca su **PIN de administrador** y presione el botón **LLAVE (⚷)** una vez		Los LED VERDE y AZUL parpadearán juntos rápidamente varias veces, luego cambiarán a un LED VERDE fijo y finalmente a un LED AZUL fijo que indica que la unidad está en modo administrador

Para salir del modo administrador

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.

6. Cambiar el PIN de administrador

Requisitos del PIN:

- Debe tener entre 7 y 15 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)

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 **LLAVE (🔑) + 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 **LLAVE (🔑)** 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 **LLAVE (🔑)** 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 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.

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 7 a 15 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 '**SHIFT** (⬆) **+ 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 '**SHIFT** (⬆) + **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**' (**SHIFT** (⬆) **+ dígito** presionados juntos), esto se puede colocar en cualquier lugar a lo largo de su PIN de 7-15 dígitos durante el proceso de creación del PIN como se muestra en los ejemplos siguientes.

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:

- 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', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- Se puede utilizar más de un 'carácter especial' y colocarlo junto con su PIN de 7 a 15 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 7 a 15 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 **LLAVE (🔑) + 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 **SHIFT** (⬆) 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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

8. Cómo eliminar la política de PIN de usuario

Para eliminar 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 **LLAVE (🔑) + 7**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Introduzca **070** y presione el botón **SHIFT** (⬆) 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 eliminado 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.

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 **SHIFT** (⬆) **+ 7** buttons		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **LLAVE (🔑)** 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 PIN de usuario nuevo 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.

Requisitos del PIN:

- Debe tener entre 7 y 15 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 **SHIFT** (⬆) se puede usar para combinaciones de PIN adicionales, por ejemplo, **SHIFT** (⬆) **+ 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 **LLAVE (🔑) + 3**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca el **PIN de usuario nuevo** y presione el botón **LLAVE (🔑)** 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 **LLAVE (🔑)**		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 **LLAVE (🔑) + 3**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca el **PIN de usuario nuevo** y presione el botón **LLAVE (🔑)** 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 **LLAVE (🔑)** 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 **SHIFT** (⬆) 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 **SHIFT** (⬆) **+ 3**		El LED AZUL fijo cambiará a un LED ROJO parpadeante
2. Nuevamente mantenga presionados los botones **SHIFT** (⬆) **+ 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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

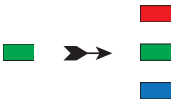
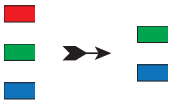
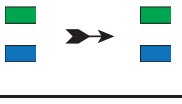
13. Cómo desbloquear diskAshur M² con PIN de usuario

Para desbloquear el diskAshur M² con el **PIN de usuario**, proceda con los siguientes pasos.

1. En un estado de espera (LED ROJO fijo), mantenga presionados los botones **SHIFT** (⬆) **+ LLAVE (🔑)**		El LED ROJO cambia a todos los LED ROJO, VERDE y AZUL alternando entre encendido y apagado
2. Introduzca el **PIN de usuario** y presione el botón **LLAVE (🔑)** una vez		Los LED parpadeantes ROJO, VERDE y AZUL cambiarán a LED VERDE y AZUL alternados y luego a un LED VERDE fijo que indica que la unidad se ha desbloqueado correctamente en modo usuario

14. Cambiar el PIN de usuario en modo usuario

Para cambiar el **PIN de usuario**, desbloquee primero el diskAshur M² con el PIN de 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 (LED VERDE) mantenga presionados los botones **LLAVE (🔑) + 4**		El LED VERDE fijo cambiará a todos los LED ROJO, VERDE y AZUL alternando entre encendido y apagado
2. Introduzca su **PIN de usuario existente** y presione el botón **LLAVE (🔑)** una vez		Los LED VERDE y AZUL fijo se encenderán y apagarán alternativamente y luego cambiarán a un solo parpadeo VERDE, después volverán a LED VERDE parpadeante y AZUL fijo
3. Introduzca el **PIN de usuario nuevo** y presione el botón **LLAVE (🔑)** 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
4. Vuelva a introducir el **PIN de usuario nuevo** y presione el botón **LLAVE (🔑)** una vez		Los LED VERDE parpadeante y AZUL fijo cambiarán a un LED VERDE que parpadea rápidamente y luego a un LED VERDE fijo que indica que el PIN de usuario se ha cambiado correctamente

Importante: El cambio del PIN de usuario en modo usuario (LED VERDE) 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 el uso de un 'carácter especial'.

15. Crear un PIN único de recuperación de usuario

El PIN de recuperación de usuario es extremadamente útil en situaciones en las que un usuario ha olvidado su PIN para desbloquear el diskAshur M².
Para activar el modo de recuperación, el usuario debe introducir primero el PIN de recuperación único correcto, si se ha configurado uno. El proceso de recuperación del PIN de usuario no afecta los datos, la clave de cifrado ni el PIN de administrador; no obstante, el usuario está obligado a configurar un PIN de usuario nuevo de 7 a 15 dígitos.

Para configurar un PIN único de recuperación de usuario de 7 a 15 dígitos, 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 **LLAVE (🔑) + 4**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca un **PIN de recuperación único** y presione el botón **LLAVE (🔑)**		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 recuperación único** y presione nuevamente el botón LLAVE **(🔑)**		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 recuperación único 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.

16. Eliminar el PIN único de recuperación de usuario

Para eliminar el PIN único de recuperación de usuario, 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 **SHIFT** (⬆) **+ 4**		El LED AZUL fijo cambiará a un LED ROJO parpadeante
2. Nuevamente mantenga presionados los botones **SHIFT** (⬆) **+ 4**		El LED ROJO parpadeante se volverá ROJO fijo y luego cambiará a un LED AZUL fijo que indica que el PIN único de recuperación de usuario se ha eliminado 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.

17. Activar el modo de recuperación y crear un PIN de usuario nuevo

El PIN de recuperación de usuario es extremadamente útil en situaciones en las que un usuario ha olvidado su PIN para desbloquear el diskAshur M².
Para activar el modo de recuperación, el usuario debe introducir primero el PIN de recuperación único correcto, si se ha configurado uno. El proceso de recuperación del PIN de usuario no afecta los datos, la clave de cifrado ni el PIN de administrador; no obstante, el usuario está obligado a configurar un PIN de usuario nuevo de 7 a 15 dígitos.

Para activar el proceso de recuperación y configurar un PIN de usuario nuevo, siga los siguientes pasos.

1. En **estado de espera** (LED ROJO) mantenga presionados los dos botones **LLAVE (🔑) + 4**		El LED ROJO fijo cambiará a LED ROJO y VERDE parpadeantes
2. Introduzca el **PIN de recuperación único** y presione el botón **LLAVE (🔑)**		Los LED VERDE y AZUL se encienden y apagan alternativamente, luego cambian a un LED VERDE fijo y finalmente a LED VERDE parpadeante y AZUL fijo
3. Introduzca un **PIN de usuario nuevo** y presione el botón **LLAVE (🔑)**		Los LED VERDE parpadeante y AZUL fijo cambian a un solo parpadeo LED VERDE y luego nuevamente a LED VERDE parpadeante y AZUL fijo
4. Vuelva a introducir su **PIN de usuario nuevo** y presione el botón **LLAVE (🔑)**		El LED VERDE parpadea rápidamente y luego se vuelve VERDE fijo, que indica que el proceso de recuperación se ha realizado correctamente y se ha configurado un PIN de usuario nuevo.

Importante: La creación de un PIN de usuario nuevo 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. Consulte la sección 9 para verificar las restricciones del PIN de usuario.

18. Establecer usuario solo lectura en modo administrador

Con tantos virus y troyanos que infectan las unidades USB, la función de solo lectura es especialmente útil si necesita acceder a los datos de la unidad USB cuando se utiliza en un entorno público. Esta es también una característica esencial para fines forenses, donde los datos deben conservarse en su estado original e inalterado, que no se puede modificar ni sobrescribir.

Cuando el administrador configura el diskAshur M² y limita el acceso del usuario a solo lectura, solo el administrador puede escribir en la unidad o volver a cambiar la configuración a lectura/escritura como se describe en la sección 19. El usuario está limitado al acceso de solo lectura y no puede escribir en la unidad o cambiar este ajuste en modo usuario.

Para ajustar el diskAshur M² y limitar el acceso del usuario a solo lectura, 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 + 6**"		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **LLAVE (🔑)**		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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

19. Permitir al usuario leer/escribir en modo administrador

Para volver a establecer el diskAshur M² 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 **LLAVE (🔑)** 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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

20. Establecer en solo lectura general en modo administrador

Cuando el administrador configura diskAshur M² y lo limita a solo lectura general, ni el administrador ni el usuario pueden escribir en la unidad y ambos están limitados al acceso de solo lectura. Solo el administrador puede volver a cambiar el ajuste a lectura/escritura como se describe en la sección 21.

Para establecer el diskAshur M² y limitar el acceso general a solo lectura, 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 **"5 + 6".**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **LLAVE (🔑)**		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 general a solo lectura.

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.

21. Permitir lectura/escritura general en modo administrador

Para volver a establecer el diskAshur M² en lectura/escritura desde la configuración de solo lectura general, 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 "**5 + 9**"		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **LLAVE (🔑)**		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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

22. Cómo configurar un PIN de autodestrucción

Puede configurar un PIN de autodestrucción que cuando se introduce realiza un criptoborrado en la unidad (se elimina la clave de cifrado). Este proceso elimina todos los PIN configurados y hace que todos los datos almacenados en la unidad sean inaccesibles (si pierden para siempre), la unidad luego se muestra como LED VERDE desbloqueado. Ejecutar esta función hará que el PIN de autodestrucción se convierta en el PIN de usuario nuevo y será necesario formatear la unidad antes de poder reutilizarla.

Para establecer 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 **LLAVE (🔑) + 6**		El LED AZUL fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Configure e introduzca un **PIN de autodestrucción** de 7 a 15 dígitos y presione el botón **LLAVE (🔑)**		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 **LLAVE (🔑)**		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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

23. 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 **SHIFT (⬆) + 6**		El LED AZUL fijo cambiará a un LED ROJO parpadeante
2. Mantenga presionados nuevamente los botones **SHIFT (⬆) + 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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

24. Cómo desbloquear con el PIN de autodestrucción

Advertencia: Cuando se activa el mecanismo de autodestrucción, se eliminan todos los datos, la clave de cifrado y los PIN de administrador/usuario. **El PIN de autodestrucción se convierte en el PIN de usuario**. No hay PIN de administrador después de activarse el mecanismo de autodestrucción. El diskAshur M² deberá restablecerse primero (véase 'Cómo realizar un reseteo completo' Sección 35, en la página 248) para configurar un PIN de administrador con privilegios de administrador totales, incluyendo la capacidad de configurar un PIN de usuario nuevo.

Cuando se use, el PIN de autodestrucción **eliminará TODOS los datos y los PIN de administrador/usuario** y luego desbloqueará la unidad. La activación de esta función hará que el **PIN de autodestrucción se convierta en el PIN de usuario nuevo** y deberá formatearse el diskAshur M² antes de que se puedan agregar nuevos datos a la unidad.

Para activar el mecanismo de autodestrucción, la unidad debe estar en estado de espera (LED ROJO fijo) y luego continuar con los siguientes pasos.

1. En **estado de espera** (LED ROJO fijo), mantenga presionados los botones **SHIFT** (⬆) + **LLAVE (🔑)**		El LED ROJO cambia a todos los LED ROJO, VERDE y AZUL alternando entre encendido y apagado
2. Introduzca el **PIN de autodestrucción** y presione el botón **LLAVE (🔑)**		Los LED parpadeantes ROJO, VERDE y AZUL cambiarán a LED VERDE y AZUL alternando entre encendido y apagado durante unos segundos y finalmente cambiarán a un LED VERDE fijo que indica que el diskAshur M² se ha autodestruido correctamente

25. 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 diskAshur M², será necesario configurar un PIN de administrador antes de que se pueda usar la unidad.

Requisitos del PIN:

- Debe tener entre 7 y 15 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)

Si el diskAshur M² 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 **SHIFT** (⬆) **+ 1**		El LED ROJO fijo cambiará a LED VERDE parpadeante y AZUL fijo
2. Introduzca el **PIN de administrador NUEVO** y presione el botón **LLAVE (🔑)**		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 **LLAVE (🔑)**		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.

26. Establecer el bloqueo automático desatendido

Para protegerse contra el acceso no autorizado si la unidad está desbloqueada y desatendida, el diskAshur M² 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 diskAshur M² 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 **LLAVE (🔑) + 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 **SHIFT** (⬆)		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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

27. 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 **LLAVE (🔑) + 5**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Introduzca **00** y presione el botón **SHIFT** (⬆)		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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

28. 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 **LLAVE (🔑)** 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 **SHIFT** (⬆) durante un segundo; el LED AZUL fijo cambia a un LED ROJO fijo.

29. Establecer en solo lectura en modo usuario

Para establecer el diskAshur M² 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 **LLAVE (🔑)**		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.

30. Habilitar lectura/escritura en modo usuario

Para establecer el diskAshur M² 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 **LLAVE (🔑)**		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.

31. Mecanismo de defensa de ataque de fuerza bruta

El diskAshur M² incorpora un mecanismo de defensa para proteger la unidad contra ataques de fuerza bruta. De forma predeterminada, los valores del estado de suministro inicial de la limitación de fuerza bruta (PIN incorrectos introducidos de manera consecutiva) son **10** tanto para el PIN de administrador como para el PIN de usuario y **5** para el PIN de recuperación. Se utilizan tres contadores de fuerza bruta independientes para registrar los intentos incorrectos para cada autorización de PIN (de administrador, usuario y recuperación) como se indica a continuación.

- Si un usuario introduce un **PIN de usuario incorrecto** 10 veces seguidas, el PIN de usuario se eliminará, pero los datos, el PIN de administrador y el PIN de recuperación permanecen intactos y accesibles.
- Si se introduce un **PIN de recuperación incorrecto** 5 veces seguidas, el PIN de recuperación se elimina, pero los datos y el PIN de administrador permanecen intactos y accesibles.
- Si se introduce un **PIN de administrador incorrecto** 10 veces seguidas, la unidad se restablecerá. Todos los PIN y los datos se eliminan y se pierden para siempre.

La siguiente tabla presume que se han configurado los tres PIN y destaca el efecto de activar el mecanismo de defensa de fuerza bruta de cada PIN concreto.

PIN utilizado para desbloquear la unidad	Introducciones incorrectas de PIN consecutivas	Descripción de lo que sucede
PIN de usuario	10	• Se elimina el PIN de usuario. • El PIN de recuperación, el PIN de administrador y todos los datos permanecen intactos y accesibles.
PIN de recuperación	5	• Se elimina el PIN de recuperación. • El PIN de administrador y todos los datos permanecen intactos y accesibles.
PIN de administrador	10	• El diskAshur M² se restablecerá. Todos los PIN y los datos se eliminan y se pierden para siempre.

Nota: La limitación de fuerza bruta se establece de forma predeterminada en los valores del estado de suministro inicial cuando la unidad se restablece totalmente, se activa la función de autodestrucción o es forzada brutalmente. Si el administrador cambia el PIN de usuario o se establece un PIN de usuario nuevo al activar la función de recuperación, el contador de fuerza bruta del PIN de usuario se pone a cero (0) pero la limitación de fuerza bruta no se ve afectada. Si el administrador cambia el PIN de recuperación, el contador de fuerza bruta del PIN de recuperación se pone a cero.

La autorización correcta de un determinado PIN pondrá a cero el contador de fuerza bruta para ese PIN concreto, pero no afectará al contador de fuerza bruta de los demás PIN. La autorización fallida de un determinado PIN aumentará el contador de fuerza bruta para ese PIN concreto, pero no afectará al contador de fuerza bruta de los demás PIN.

32. Mecanismo de defensa contra ataques de fuerza bruta del PIN del administrador

El PIN del administrador de la diskAshur M² está equipado con un mecanismo de defensa más sofisticado el PIN del usuario o el PIN de recuperación. Esto tiene como fin impedir que se introduzca de manera incorrecta el PIN del administrador 10 veces seguidas y se pierdan todos sus datos. Así pues, tras introducir 5 veces un PIN del administrador incorrecto, la diskAshur M² se boqueará y se encenderán todos los LED de manera continua.

ATENCIÓN: No intente seguir estas instrucciones si desbloquea su diskAshur M² utilizando solo el '**PIN DEL USUARIO**' y no conoce el '**PIN ADMINISTRADOR**'.

Consulte las instrucciones de la tabla de abajo para tener más intentos de introducir el PIN del administrador hasta un máximo de 10.

Intentos consecutivos de introducir un PIN del administrador incorrecto	Descripción de lo que le ocurre a la diskAshur M²	Instrucciones
5	Los LED **ROJO**, **VERDE** y **AZUL** se encienden de manera **continua**.	Introduzca el PIN '**47867243**' y pulse la **LLAVE** (⚷) una vez; los LED **VERDE** y **AZUL** se encenderán y apagarán de manera alterna, y la diskAshur M2 estará lista para aceptar **3 intentos más de introducir el PIN del administrador**.
8	Los LED **ROJO**, **VERDE** y **AZUL** **se encienden** y **se apagan** de forma alterna.	Introduzca el PIN '**47867243**' y pulse la **LLAVE** (⚷) una vez; los LED **VERDE** y **AZUL** se encenderán y apagarán de manera alterna y la diskAshur M2 estará lista para aceptar **2 intentos más de introducir el PIN del administrador**.
10	El LED **ROJO** se encenderá de manera continua.	Después de introducir el PIN del administrador de manera incorrecta 10 veces, la clave de cifrado, todos los PIN y los datos se borrarán y perderán para siempre.

33. Cómo establecer la limitación de fuerza bruta del PIN de usuario

Nota: El ajuste de limitación de fuerza bruta del PIN de usuario está fijado por defecto a introducir incorrectamente el PIN 10 veces seguidas cuando Hothwe drtivoe isseeithtertchomepleUtelsy reesret,PbrluNte foBrcerduotretheFseolf-rdcesetrucLt PilmN isiatcativtaiteodn.

El administrador puede reprogramar y establecer la limitación de fuerza bruta para el PIN de usuario del diskAshur M². Esta función se puede establecer para que permita de 1 a 10 intentos seguidos de introducir el PIN de manera incorrecta.

Para configurar la limitación de fuerza bruta del 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 **7 + 0**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeando juntos
2. Introduzca el número de intentos para la limitación de fuerza bruta (entre 01-10); por ejemplo, introduzca: • **01** para 1 intento • **10** para 10 intentos		
3. Presione el botón **SHIFT** (⬆) una vez		Los LED VERDE y AZUL parpadeantes cambiarán a un LED VERDE fijo durante un segundo y luego a un LED AZUL fijo que indica que la limitación de fuerza bruta 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.

34. Cómo verificar la limitación de fuerza bruta del PIN de usuario

El administrador puede observar y determinar el número de veces seguidas que se permite introducir un PIN de usuario incorrecto antes de activar el mecanismo de defensa de fuerza bruta simplemente observando la secuencia de LED como se describe a continuación.

Para verificar el ajuste de limitación de fuerza bruta, 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 **2** + **0**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione el botón **LLAVE (🔑)** 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) 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) permanecen fijos durante 1 segundo. e. Los LED vuelven a AZUL fijo		

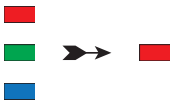
La siguiente tabla describe el comportamiento del LED mientras se verifica el ajuste de limitación de fuerza bruta; por ejemplo, si ha configurado la unidad en fuerza bruta después de **5** introducciones de PIN incorrectas seguidas, el LED VERDE parpadeará cinco (**5**) veces.

Ajuste 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 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.

35. Cómo realizar un reseteo completo

Para realizar un reseteo completo, el diskAshur M² 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 diskAshur M², 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 25 en la página 242 sobre 'Cómo configurar un PIN de administrador después de un ataque de fuerza bruta o un reseteo', el diskAshur M² también deberá ser formateado antes de que se puedan agregar nuevos datos a la unidad.

36. Cómo configurar diskAshur M² para su arranque

Nota: Cuando la unidad está establecida para su arranque, expulsar la unidad del sistema operativo no obligará al LED a ponerse ROJO. La unidad permanece en VERDE fijo y debe desenchufarse para la próxima vez que se use. El ajuste predeterminado del diskAshur M2 está configurado en no arranque.

El diskAshur M² está equipado con una función de arranque para acomodar el ciclo de energía durante un proceso de arranque del host. Al arrancar desde el diskAshur M², está ejecutando su ordenador con el sistema operativo que está instalado en el diskAshur M².

Para establecer la unidad para su arranque, 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 **LLAVE (🔑) + 8** buttons		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione **"0"** seguido de un **"1"** (**01**)		Los LED VERDE y AZUL seguirán parpadeando
3. Presione el botón **SHIFT** (⬆) 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 unidad se ha configurado correctamente para su arranque

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.

37. Cómo deshabilitar la función de arranque del diskAshur M²

Para deshabilitar la función de arranque del diskAshur M², 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 **LLAVE (🔑) + 8**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes
2. Presione **"0"** seguido de otro **"0"** (**00**)		Los LED VERDE y AZUL seguirán parpadeando
3. Presione el botón **SHIFT** (⬆) 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 función de arranque se ha desactivado 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.

38. Cómo verificar el ajuste de arranque

Para verificar el ajuste de arranque, 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 **SHIFT** (⬆) **+ 8**		El LED AZUL fijo cambiará a LED VERDE y AZUL parpadeantes

2. Presione el botón **LLAVE (🔑)** y ocurrirá una de las siguientes dos posibilidades;

- **Si diskAshur M² está configurado para su arranque, sucede lo siguiente;**

a. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo.
b. El LED VERDE parpadea una vez.
c. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo.
d. Los LED vuelven a AZUL fijo

- **Si diskAshur M² <u>NO</u> está configurado para su arranque, sucede lo siguiente;**

a. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo.
b. Todos los LED están apagados
c. Todos los LED (ROJO, VERDE y AZUL) permanecen fijos durante 1 segundo.
d. Los LED vuelven a AZUL fijo

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.

39. Iniciar y formatear el disco Ashur M² para Windows

Después de un 'ataque de fuerza bruta' o un reseteo completo, el diskAshur M² eliminará todos los PIN, los datos y la clave de cifrado. Debe iniciar y formatear el diskAshur M² antes de poder utilizarlo.

Para formatear su diskAshur M², haga lo siguiente:

1. Configure un PIN de administrador nuevo; véase la página 242, sección 25: 'Cómo configurar un PIN de administrador después de un ataque de fuerza bruta o un reseteo'.

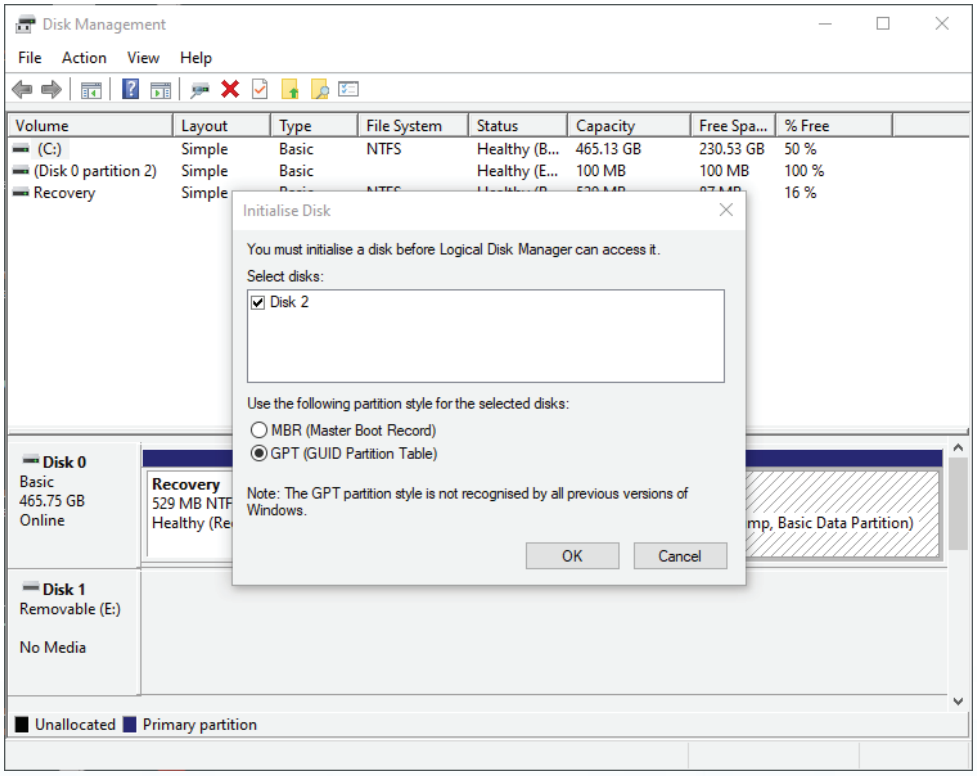
2. Con el diskAshur M² en estado de espera (LED ROJO), presione el botón **LLAVE (⚷)** una vez e introduzca el **PIN de administrador nuevo** para desbloquearlo (LED VERDE parpadeante).

3. Conecte el diskAshur M² al ordenador.

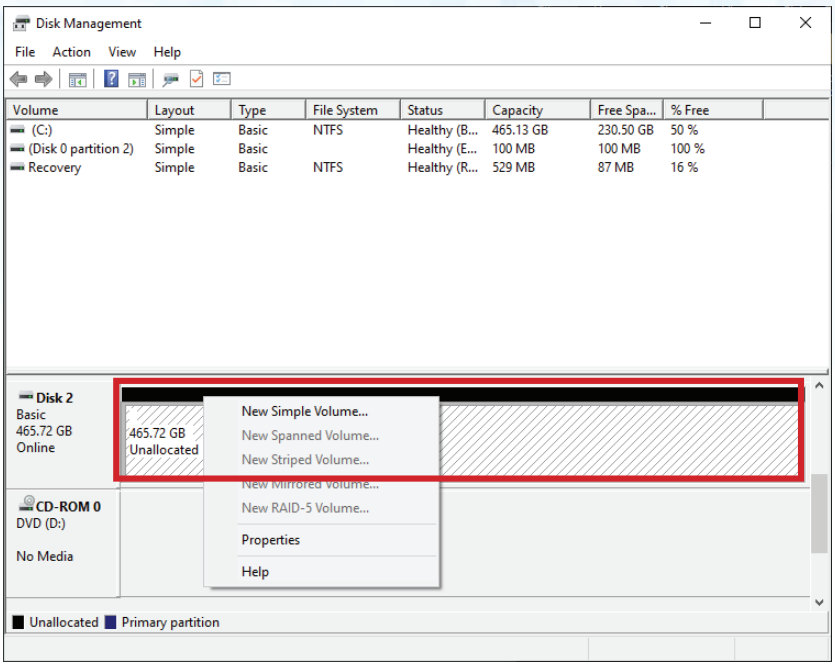
4. **Windows 7:** Haga clic derecho en **Ordenador**, después haga clic en Administrar y luego seleccione **Administración de discos**
   Windows 8: Haga clic con el botón derecho en la esquina izquierda del escritorio y seleccione **Administración de discos**
   Windows 10: Haga clic derecho en el botón de inicio y seleccione **Administración de discos**

5. En la ventana Administración de discos, diskAshur M² se reconoce como un dispositivo desconocido no iniciado ni asignado. Debería aparecer un cuadro de mensaje para que elija entre el estilo de partición MBR y GPT. GPT almacena múltiples duplicados de estos datos en el disco, lo que hace que sea mucho más robusto. En un disco MBR, la información de partición y arranque se almacena en un solo lugar.

   Seleccione el estilo de partición y haga **clic** en **Aceptar**.



6. Haga clic con el botón derecho en el área en blanco sobre la sección **No asignado** y luego seleccione **Nuevo volumen simple.**



7. Se abrirá la ventana de bienvenida al asistente del Nuevo volumen simple. Haga clic en Siguiente.



8. Si solo necesita una partición, acepte el tamaño de partición predeterminado y haga clic en **Siguiente**.

9. Asigne una letra de unidad o ruta y haga clic en **Siguiente**.

10. Cree una etiqueta de volumen, seleccione Realizar un formateo rápido y luego haga clic en **Siguiente**.

11. Haga clic en **Finalizar**.

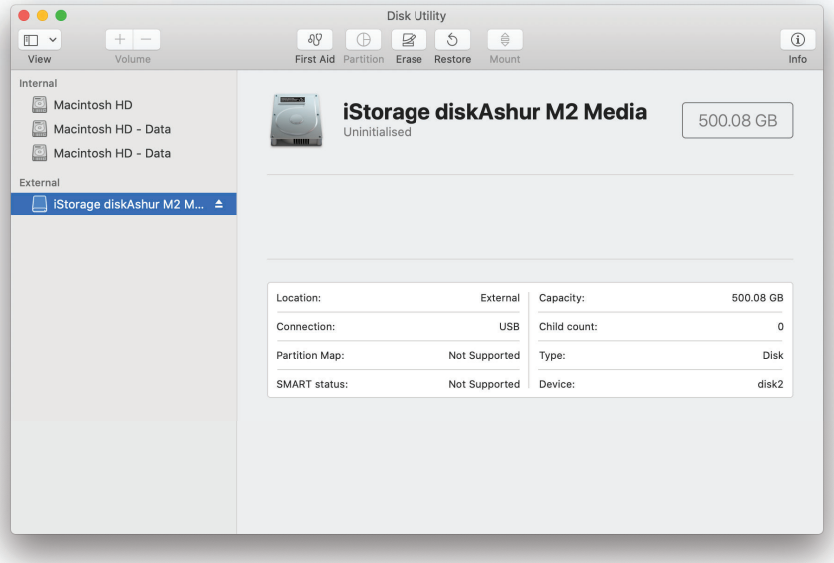
12. Espere hasta que haya finalizado el proceso de formateo. El diskAshur M² será reconocido y estará disponible para su uso.

40. Iniciar y formatear el disco Ashur M² en Mac OS

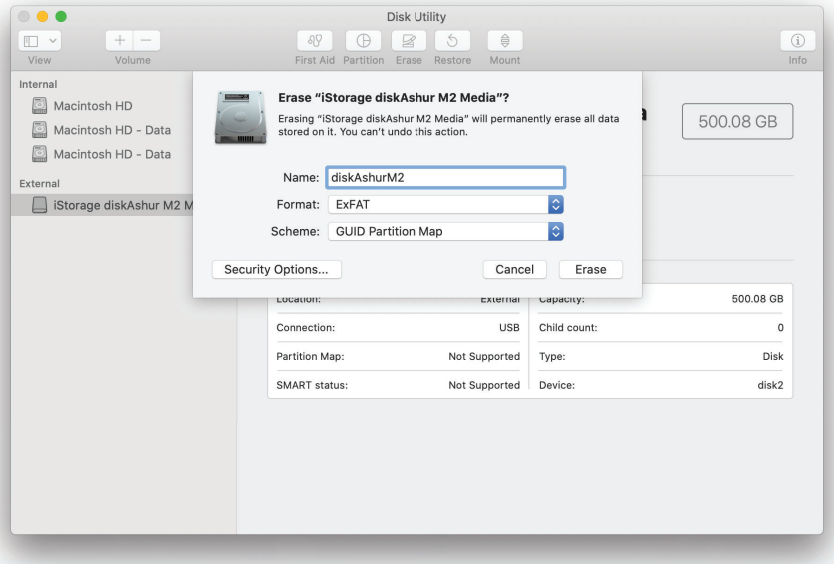
Después de un 'ataque de fuerza bruta' o un reseteo completo, el diskAshur M² eliminará todos los PIN, los datos y la clave de cifrado. Debe iniciar y formatear el diskAshur M² antes de poder utilizarlo.

Para iniciar y formatear el diskAshur M²:

1. Seleccione diskAshur M² de la lista de unidades y volúmenes. Cada unidad de la lista mostrará su capacidad, fabricante y nombre de producto, como, por ejemplo, '**iStorage diskAshur M² Media**'.



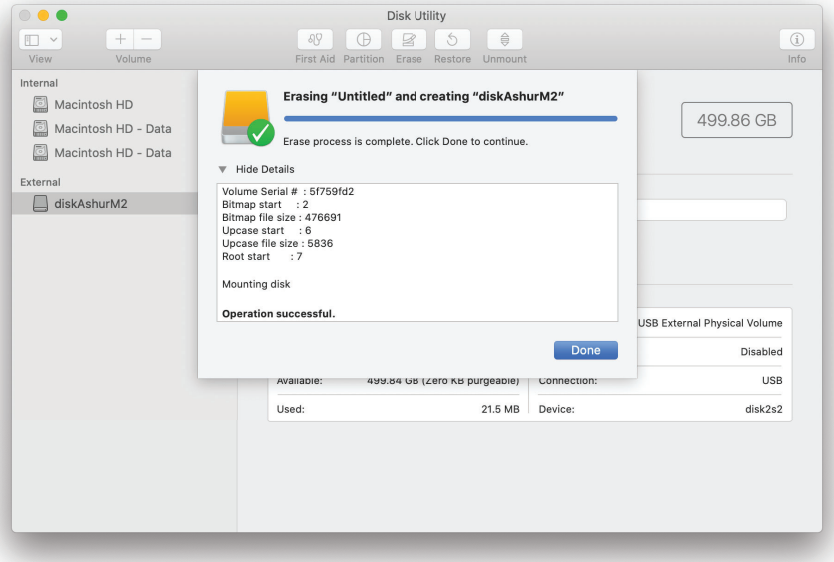
2. Haga clic en el botón '**Borrar**' en la utilidad de Disco.
3. Introduzca un nombre para la unidad. El nombre predeterminado es Sin título. El nombre de la unidad aparecerá después en el escritorio.



4. Seleccione una disposición y un formato de volumen a usar. El menú desplegable Formato de volumen enumera los formatos de unidad disponibles que admite Mac. El tipo de formato recomendado es 'Mac OS Extended (Journaled)'. Para multiplataforma, use exFAT. El menú desplegable de formato de disposiciones enumera las disposiciones disponibles para usar. Recomendamos utilizar 'Mapa de partición GUID' en unidades de más de 2 TB.

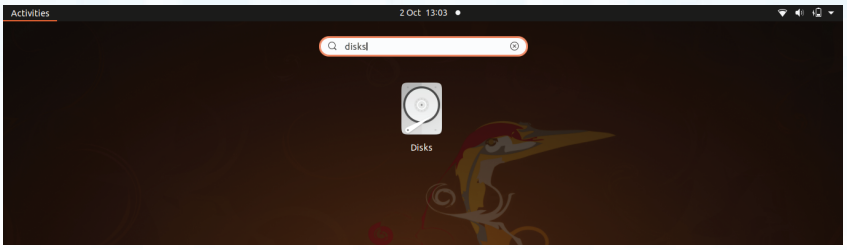


5. Haga clic en el botón 'Borrar'. La utilidad Disco desmontará el volumen del escritorio, lo borrará y luego lo volverá a montar en el escritorio.

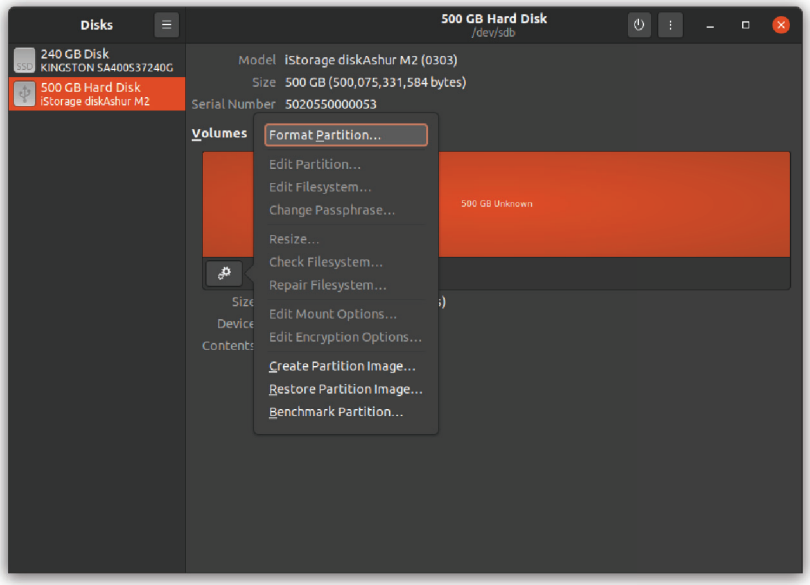


41. Iniciar y formatear diskAshur M² en Linux OS

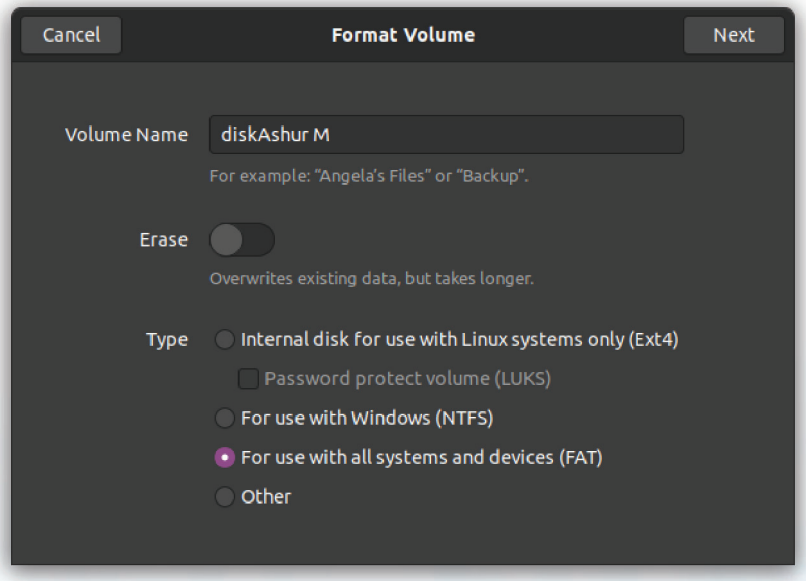
1. Abra '**Mostrar aplicación**' y escriba '**discos**' en el campo de búsqueda. Haga clic en la utilidad '**Discos**' cuando aparezca.



2. Haga clic para seleccionar la unidad (disco duro de 500 GB) en '**Dispositivos**'. A continuación, haga clic en el icono de engranajes en '**Volúmenes**' y en '**Formatear particiones**'.

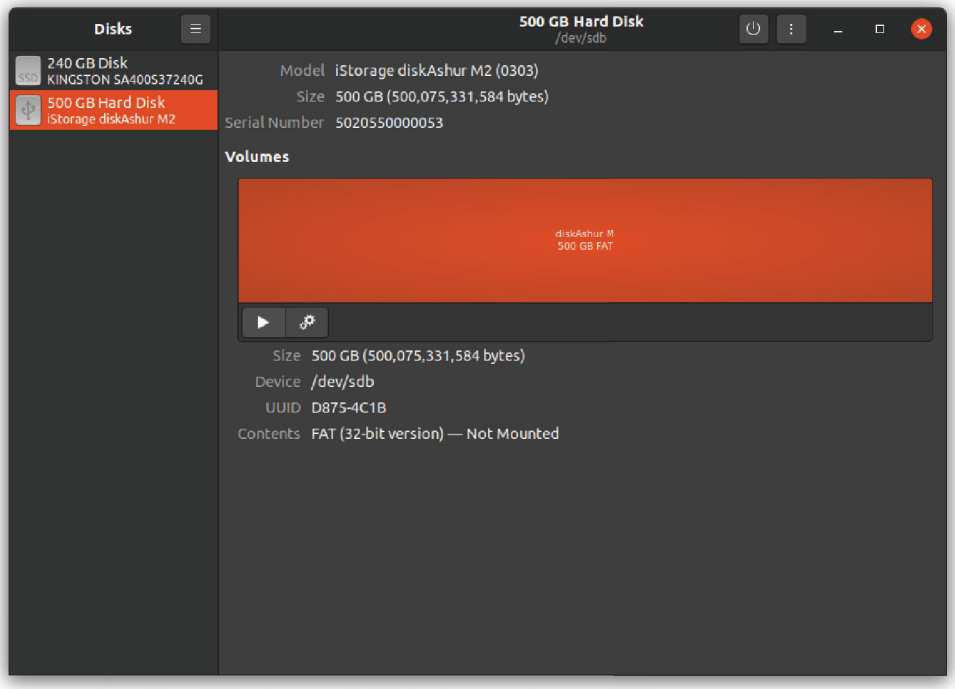


3. Seleccione '**Compatible con todos los sistemas y dispositivos (FAT)**' para la opción '**Tipo**'. E introduzca un nombre para la unidad, por ejemplo: diskAshur M². Luego, haga clic en el botón '**Formatear**'.

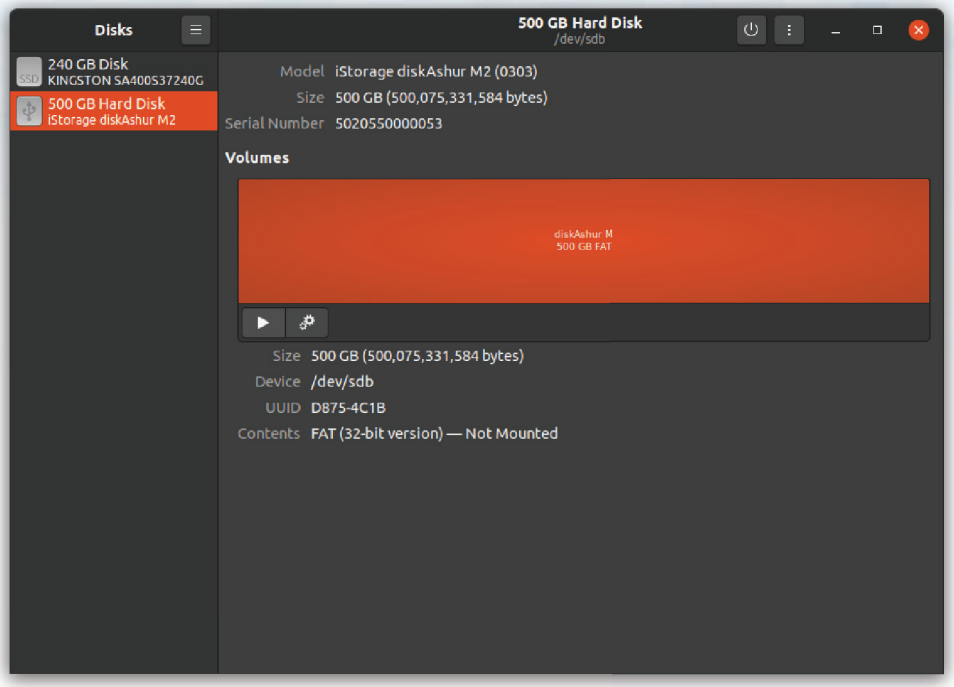




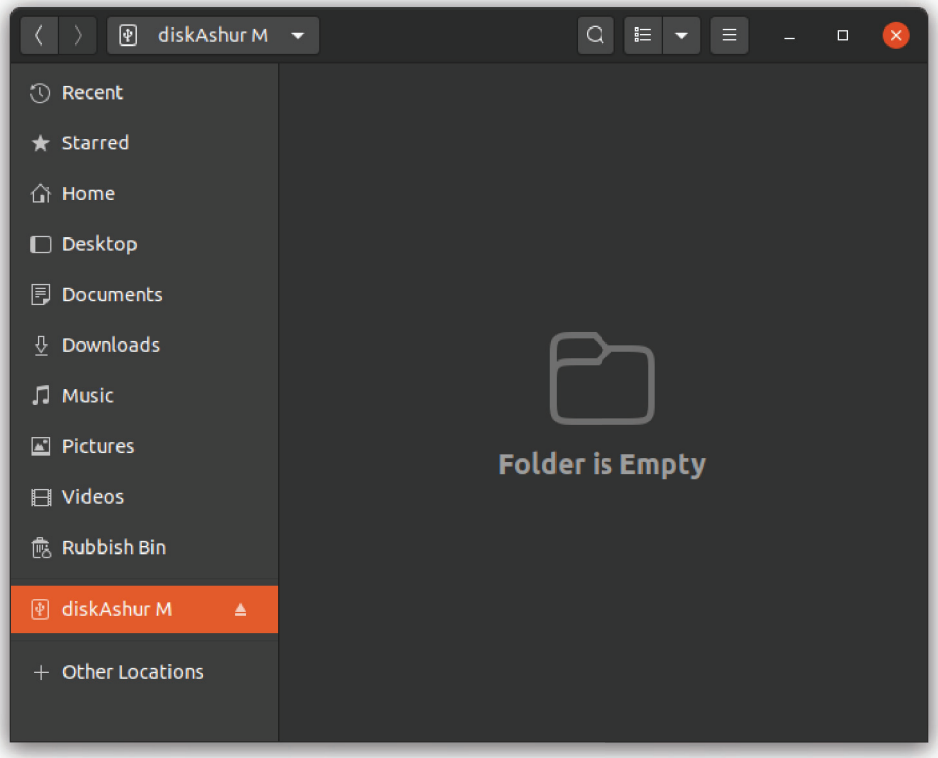
4. Una vez finalizado el proceso de formateo, haga clic en el botón Reproducir para montar la unidad en Ubuntu.



5. Ahora la unidad debería estar montada en Ubuntu y lista para usarse.



6. El disco se mostrará como se ve en la imagen a continuación. Puede hacer clic en el icono del disco para abrir su unidad.



42. Hibernar, suspender o cerrar sesión del sistema operativo

Asegúrese de guardar y cerrar todos los archivos en su diskAshur M² antes de hibernar, suspender o cerrar sesión en el sistema operativo.

Se recomienda que bloquee el diskAshur M² manualmente antes de hibernar, suspender o cerrar sesión en su sistema.

Para bloquear la unidad, expulse de manera segura el diskAshur M² de su sistema operativo host y luego desconéctelo del puerto USB. Si se escriben datos en la unidad, desenchufar el diskAshur M² 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 diskAshur M² si deja de usar su ordenador.

43. 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 **LLAVE (🔑)** 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.

44. 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 **LLAVE (🔑)** 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.

45. 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 viernes.

46. 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

DISKASHUR® M²

Copyright © iStorage Limited 2020. Todos los derechos reservados.
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

Εγχειρίδιο χρήστη



Βεβαιωθείτε ότι θυμάστε το PIN (κωδικός πρόσβασής σας), χωρίς αυτό δεν υπάρχει τρόπος πρόσβασης στα δεδομένα της μονάδας δίσκου.

Εάν αντιμετωπίζετε δυσκολίες με τη χρήση της μονάδας δίσκου diskAshur M², επικοινωνήστε με το τεχνικό μας τμήμα μέσω email- support@istorage-uk.com ή τηλεφωνικά στο +44 (0) 20 8991 6260.

Πνευματικά δικαιώματα © iStorage Limited 2020. Με την επιφύλαξη παντός δικαιώματος. Η ονομασία Windows είναι σήμα κατατεθέν της Microsoft Corporation.

Όλα τα άλλα εμπορικά σήματα και πνευματικά δικαιώματα που αναφέρονται είναι ιδιοκτησία των αντίστοιχων κατόχων τους. Η διανομή τροποποιημένων εκδόσεων αυτού του εγγράφου απαγορεύεται χωρίς τη ρητή άδεια του κατόχου των πνευματικών δικαιωμάτων.

Απαγορεύεται η διανομή του έργου ή του παράγωγου έργου σε οποιαδήποτε τυποποιημένη μορφή βιβλίου για εμπορικούς σκοπούς, εκτός εάν έχει ληφθεί προηγούμενη άδεια από τον κάτοχο των πνευματικών δικαιωμάτων.

Η ΤΕΚΜΗΡΙΩΣΗ ΠΑΡΕΧΕΤΑΙ ΩΣ ΕΧΕΙ ΚΑΙ ΟΛΕΣ ΟΙ ΡΗΤΕΣ Η ΣΙΩΠΗΡΕΣ ΠΡΟΫΠΟΘΕΣΕΙΣ, ΔΗΛΩΣΕΙΣ ΚΑΙ ΕΓΓΥΗΣΕΙΣ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΗΣ ΟΠΟΙΑΣΔΗΠΟΤΕ ΣΙΩΠΗΡΗΣ ΕΓΓΥΗΣΗΣ ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ, ΚΑΤΑΛΛΗΛΟΤΗΤΑΣ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΚΟΠΟΣ Η ΜΗ ΠΑΡΑΒΙΑΣΗ, ΑΠΟΠΟΙΟΥΝΤΑΙ, ΕΚΤΟΣ ΑΠΟ ΤΟ ΒΑΘΜΟ ΠΟΥ ΟΙ ΕΝ ΛΟΓΩ ΑΠΟΠΟΙΗΣΕΙΣ ΚΡΙΝΟΝΤΑΙ ΝΟΜΙΚΑ ΑΚΥΡΕΣ

Όλα τα εμπορικά σήματα και οι επωνυμίες είναι ιδιοκτησία των αντίστοιχων κατόχων τους

υμμόρφωση με τον νόμο περί εμπορικών συμφωνιών (TAA)

Πίνακας περιεχομένων

Εισαγωγή 264
Περιεχόμενα κουτιού 264
diskAshur M² Διάταξη 264
1. Ενδεικτικές λυχνίες LED και οι ενέργειές τους 265
2. Καταστάσεις LED 265
3. Πρώτη χρήση 266
4. Ξεκλείδωμα diskAshur M² με το PIN διαχειριστή 267
5. Πώς να εισέλθετε στη λειτουργία διαχειριστή 267
6. Αλλαγή του PIN διαχειριστή 268
7. Ορισμός πολιτικής PIN χρήστη 269
8. Τρόπος διαγραφής της πολιτικής PIN χρήστη 270
9. Πώς να ελέγξετε την Πολιτική PIN χρήστη 270
10. Προσθήκη νέου PIN χρήστη σε λειτουργία διαχειριστή 271
11. Αλλαγή του PIN χρήστη σε λειτουργία διαχειριστή 272
12. Διαγραφή του PIN χρήστη στη λειτουργία διαχειριστή 272
13. Πώς να ξεκλειδώσετε το diskAshur M² με PIN χρήστη 273
14. Αλλαγή του PIN χρήστη σε λειτουργία χρήστη 273
15. Δημιουργία PIN ανάκτησης χρήστη μίας χρήσης 274
16. Διαγραφή του PIN ανάκτησης χρήστη μίας χρήσης 274
17. Ενεργοποίηση λειτουργίας ανάκτησης και δημιουργία νέου PIN χρήστη 275
18. Ορισμός μόνο για ανάγνωση χρήστη σε λειτουργία διαχειριστή 275
19. Ενεργοποίηση ανάγνωσης/εγγραφής χρήστη σε λειτουργία διαχειριστή 276
20. Ορισμός καθολικής μόνο για ανάγνωση σε λειτουργία διαχειριστή 276
21. Ενεργοποίηση καθολικής ανάγνωσης/εγγραφής σε λειτουργία διαχειριστή 277
22. Πώς να ρυθμίσετε ένα PIN αυτοκαταστροφής 277
23. Πώς να διαγράψετε το PIN αυτοκαταστροφής 278
24. Πώς να ξεκλειδώσετε με το PIN αυτοκαταστροφής 278
25. Πώς να ρυθμίσετε ένα PIN διαχειριστή μετά από επίθεση ή επαναφορά ωμής βίας 279
26. Ρύθμιση του αυτόματου κλειδώματος χωρίς παρακολούθηση 279
27. Απενεργοποίηση του αυτόματου κλειδώματος χωρίς παρακολούθηση 280
28. Πώς να ελέγξετε το αυτόματο κλείδωμα χωρίς παρακολούθηση 281
29. Ορισμός μόνο για ανάγνωση σε λειτουργία χρήστη 281
30. Ενεργοποίηση ανάγνωσης/εγγραφής σε λειτουργία χρήστη 282
31. Brute Force Hack Μηχανισμός Άμυνας 282
32. Admin PIN ωμή δύναμη Hack Μηχανισμός Άμυνας 283
33. Τρόπος ορισμού του περιορισμού ωμής βίας PIN χρήστη 283
34. Πώς να ελέγξετε τον περιορισμό ωμής βίας PIN χρήστη 284
35. Πώς να εκτελέσετε μια πλήρη επαναφορά 285
36. Πώς να ρυθμίσετε το diskAshur M² ως Bootable 285
37. Πώς να απενεργοποιήσετε το diskAshur M² Δυνατότητα εκκίνησης 286
38. Πώς να ελέγξετε τη ρύθμιση Bootable 286
39. Αρχικοποίηση και διαμόρφωση diskAshur M² για Windows 287
40. Αρχικοποίηση και διαμόρφωση diskAshur M² σε Mac OS 289
41. Αρχικοποίηση και διαμόρφωση diskAshur M² σε λειτουργικό σύστημα Linux 291
42. Αδρανοποίηση, αναστολή ή αποσύνδεση από το λειτουργικό σύστημα 294
43. Πώς να ελέγξετε το υλικολογισμικό σε λειτουργία διαχειριστή 294
44. Πώς να ελέγξετε το υλικολογισμικό στη λειτουργία χρήστη 295
45. Τεχνική Υποστήριξη 296
46. Πληροφορίες εγγύησης και RMA 296

Εισαγωγή

Σας ευχαριστούμε που αγοράσατε το νέο δίσκο iStorage diskAshur M², ένα εξαιρετικά ασφαλές και εύκολο στη χρήση, κρυπτογραφημένο υλικό, φορητό δίσκο στερεάς κατάστασης (SSD) με πιστοποίηση PIN με χωρητικότητες από 120GB έως 2TB και αυξάνεται.

Σχεδιασμένος να είναι FIPS 140-3 Level 3, ο diskAshur M² κρυπτογραφεί δεδομένα κατά τη μεταφορά και την ηρεμία χρησιμοποιώντας κρυπτογράφηση υλικού πλήρους δίσκου AES-XTS 256-bit.

Ο δίσκος diskAshur M² ενσωματώνει έναν ασφαλή μικροεπεξεργαστή Common Criteria EAL 5+ (Hardware Certified), ο οποίος χρησιμοποιεί ενσωματωμένους μηχανισμούς φυσικής προστασίας σχεδιασμένους για προστασία από εξωτερική παραβίαση, επιθέσεις παράκαμψης και ενέσεις σφαλμάτων.

Σε αντίθεση με άλλες λύσεις, το diskAshur M² αντιδρά σε μια αυτοματοποιημένη επίθεση μπαίνοντας σε αδιέξοδο παγωμένη κατάσταση, γεγονός που καθιστά όλες αυτές τις επιθέσεις άχρηστες. Με απλά λόγια, χωρίς το PIN δεν υπάρχει τρόπος!

Περιεχόμενα κουτιού

- diskAshur M² φορητό SSD &; προστατευτικό μανίκι
- Προστατευτική θήκη μεταφοράς
- Καλώδια USB C &; A
- Οδηγός γρήγορης εκκίνησης &; Αποποίηση ευθυνών προϊόντος

diskAshur M² Διάταξη



1. Ενδεικτικές λυχνίες LED και οι ενέργειές τους

LED	LED State	Description	LED	LED State	Description
	ΚΟΚΚΙΝΟ στερεό	Κλειδωμένη μονάδα δίσκου (σε οποιοδήποτε από τα δύο **Κατάσταση αναμονής** ή **επαναφοράς**)		ΜΠΛΕ Στερεό	Οδηγήστε σε **λειτουργία διαχειριστή**
	ΚΟΚΚΙΝΟ Διπλή αναλαμπή	Εσφαλμένη καταχώρηση PIN		ΚΟΚΚΙΝΟ , ΠΡΑΣΙΝΟ και ΜΠΛΕ Αναβοσβήνει μαζί	Αναμονή για **εισαγωγή PIN** χρήστη
	ΠΡΑΣΙΝΟ Στερεό	Οδηγήστε **ξεκλείδωτη**		ΠΡΑΣΙΝΟ και ΜΠΛΕ Αναβοσβήνει μαζί	Αναμονή για **εισαγωγή PIN** διαχειριστή
	ΠΡΑΣΙΝΟ που αναβοσβήνει	Μεταφορά δεδομένων σε εξέλιξη		ΠΡΑΣΙΝΟ και ΜΠΛΕ Αναβοσβήνει εναλλάξ	Έλεγχος ταυτότητας σε εξέλιξη

2. Καταστάσεις LED

Σημείωση: Η κανονική λειτουργία του diskAshur M² μπορεί να διαταραχθεί από ισχυρές ηλεκτρομαγνητικές παρεμβολές. Εάν ναι, απλώς ενεργοποιήστε ξανά το προϊόν (απενεργοποιήστε και στη συνέχεια ενεργοποιήστε) για να συνεχίσετε την κανονική λειτουργία. Εάν η κανονική λειτουργία δεν συνεχιστεί, χρησιμοποιήστε το προϊόν σε διαφορετική τοποθεσία.

Για να ξυπνήσετε από την κατάσταση αδράνειας

Η κατάσταση αδράνειας ορίζεται ως όταν ο diskAshur M² δεν χρησιμοποιείται και όλες οι λυχνίες LED είναι απενεργοποιημένες.

να ξυπνήσετε το diskAshur M² από την κατάσταση αδράνειας, κάντε τα εξής.

Συνδέστε το diskAshur M² σε μια τροφοδοτούμενη θύρα USB στον υπολογιστή σας		Οι κόκκινες, πράσινες και μπλε λυχνίες LED αναβοσβήνουν μία φορά διαδοχικά, στη συνέχεια η πράσινη λυχνία LED αναβοσβήνει δύο φορές και τελικά αλλάζει σε μια σταθερή κόκκινη λυχνία LED που υποδεικνύει ότι η μονάδα βρίσκεται σε κατάσταση αναμονής

Για να εισέλθετε σε κατάσταση αδράνειας

Για να αναγκάσετε το diskAshur M2 να εισέλθει σε κατάσταση αδράνειας, εκτελέστε μία από τις ακόλουθες λειτουργίες:

- Αποσυνδέστε τη μονάδα δίσκου εάν είναι συνδεδεμένη σε θύρα USB, όλες οι λυχνίες LED θα σβήσουν (κατάσταση αδράνειας).

Καταστάσεις ενεργοποίησης

Μετά την επαναφορά της μονάδας δίσκου από την κατάσταση αδράνειας, θα εισέλθει σε μία από τις ακόλουθες καταστάσεις που εμφανίζονται στον παρακάτω πίνακα.

Κατάσταση ενεργοποίησης	Ένδειξη LED	Κλειδί κρυπτογράφησης	PIN διαχειριστή	Περιγραφή
Αρχική κατάσταση αποστολής	κόκκινη και πράσινες Στερεός	✓	×	Αναμονή για διαμόρφωση PIN διαχειριστή (πρώτη χρήση)
Εφεδρικός	κόκκινη στερεό	✓	✓	Αναμονή για καταχώρηση PIN διαχειριστή ή χρήστη
Επαναφορά	κόκκινη στερεό	×	×	Αναμονή για διαμόρφωση PIN διαχειριστή

3. Πρώτη χρήση

Το diskAshur M² παρέχεται στην «αρχική κατάσταση αποστολής» χωρίς προκαθορισμένο PIN διαχειριστή. Για να μπορέσετε να χρησιμοποιήσετε τη μονάδα δίσκου, πρέπει να ρυθμίσετε ένα PIN διαχειριστή 7-15 ψηφίων. Μόλις ολοκληρωθεί επιτυχώς η διαμόρφωση ενός PIN διαχειριστή, δεν θα είναι δυνατή η επαναφορά της μονάδας δίσκου στην «αρχική κατάσταση αποστολής».

Απαιτήσεις PIN:

- Πρέπει να έχει μήκος μεταξύ 7-15 ψηφίων
- Δεν πρέπει να περιέχει μόνο επαναλαμβανόμενους αριθμούς, π.χ. (3-3-3-3-3-3-3)
- Δεν πρέπει να περιέχει μόνο διαδοχικούς αριθμούς, π.χ. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

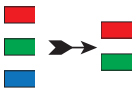
Συμβουλή κωδικού πρόσβασης: Μπορείτε να διαμορφώσετε μια αξέχαστη λέξη, όνομα, φράση ή οποιονδήποτε άλλο συνδυασμό αλφαριθμητικού PIN πατώντας απλώς το κουμπί με τα αντίστοιχα γράμματα πάνω του.

Παραδείγματα αυτών των τύπων αλφαριθμητικών PIN είναι:

- Για "Password" πατήστε τα ακόλουθα κουμπιά:
  7 (pqrs) 2 (abc) 7 (pqrs) 7 (pqrs) 9 (wxyz) 6 (mno) 7 (pqrs) 3 (def)
- Για "iStorage" πατήστε τα ακόλουθα κουμπιά:
  4 (ghi) 7 (pqrs) 8 (tuv) 6 (mno) 7 (pqrs) 2 (abc) 4 (ghi) 3 (def)

Χρησιμοποιώντας αυτήν τη μέθοδο, μπορούν να διαμορφωθούν μεγάλα και εύκολα στην απομνημόνευση PIN.

Για να διαμορφώσετε ένα PIN διαχειριστή και να ξεκλειδώσετε το diskAshur M² για πρώτη φορά, ακολουθήστε τα απλά βήματα στον παρακάτω πίνακα.





Οδηγίες - Πρώτη χρήση	LED	Κατάσταση LED
1. Συνδέστε το diskAshur M² σε μια τροφοδοτούμενη θύρα USB στον υπολογιστή σας		Οι κόκκινες, πράσινες και μπλε λυχνίες LED αναβοσβήνουν μία φορά ακολουθία τότε η ΠΡΑΣΙΝΗ λυχνία LED αναβοσβήνει δύο φορές και τελικά αλλάζει σε συμπαγείς ΚΟΚΚΙΝΕΣ και ΠΡΑΣΙΝΕΣ λυχνίες LED που υποδεικνύουν ότι η μονάδα βρίσκεται στην αρχική κατάσταση αποστολής
2. Πατήστε και κρατήστε πατημένα και τα δύο κουμπιά **πλήκτρο** (⚷) **+ 1**		Οι λυχνίες LED αναβοσβήνουν ΠΡΑΣΙΝΕΣ και συμπαγείς ΜΠΛΕ
3. Εισαγάγετε ένα **νέο PIN διαχειριστή** (7-15 ψηφία) και πατήστε το κουμπί **πλήκτρο** (⚷) μία φορά		Αναβοσβήνουν ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED αλλάζουν σε ΠΡΑΣΙΝΗ αναλαμπή και, στη συνέχεια, επιστρέφουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED
4. Εισαγάγετε ξανά το **νέο PIN διαχειριστή** και πατήστε το **πλήκτρο** (⚷) κουμπί ξανά		Το ΜΠΛΕ LED αναβοσβήνει γρήγορα, στη συνέχεια μεταβαίνει σε ένα συμπαγές ΜΠΛΕ LED και, τέλος, σε ένα συμπαγές ΠΡΑΣΙΝΟ LED που υποδεικνύει ότι το PIN διαχειριστή έχει ρυθμιστεί με επιτυχία και η μονάδα δίσκου ξεκλειδώνεται





Κλείδωμα του diskAshur M²

Για να κλειδώσετε τη μονάδα δίσκου, αφαιρέστε με ασφάλεια το diskAshur M² από το λειτουργικό σύστημα κεντρικού υπολογιστή και, στη συνέχεια, αποσυνδέστε το από τη θύρα USB. Εάν εγγράφονται δεδομένα στη μονάδα δίσκου, η αποσύνδεση του diskAshur M² θα έχει ως αποτέλεσμα την ελλιπή μεταφορά δεδομένων και πιθανή καταστροφή δεδομένων.

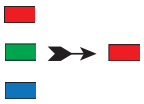
4. Ξεκλείδωμα diskAshur M² με το PIN διαχειριστή

Για να ξεκλειδώσετε το diskAshur M² με το PIN διαχειριστή, ακολουθήστε τα απλά βήματα στον παρακάτω πίνακα.

1. Συνδέστε το diskAshur M² σε μια θύρα USB στον υπολογιστή σας		Οι κόκκινες, πράσινες και μπλε λυχνίες LED αναβοσβήνουν μία φορά ακολουθία, στη συνέχεια, η ΠΡΑΣΙΝΗ λυχνία LED αναβοσβήνει δύο φορές και τελικά αλλάζει σε μια σταθερή κόκκινη λυχνία LED που υποδεικνύει ότι η μονάδα βρίσκεται σε κατάσταση αναμονής
2. Σε κατάσταση αναμονής (στερεά ΚΟΚΚΙΝΕΣ LED) πατήστε το κουμπί **Πλήκτρο** (⚷) μία φορά		Οι πράσινες και μπλε λυχνίες LED αναβοσβήνουν μαζί
3. Με τις πράσινες και μπλε λυχνίες LED να αναβοσβήνουν μαζί, εισαγάγετε το **PIN διαχειριστή** και πατήστε ξανά το κουμπί **Πλήκτρο** (⚷)		Τα πράσινα και μπλε LED θα αναβοσβήνουν εναλλάξ αρκετές φορές και στη συνέχεια σε ένα συμπαγές μπλε LED και αλλαγή σε σταθερή ΠΡΑΣΙΝΗ λυχνία LED που υποδεικνύει τη μονάδα δίσκου ξεκλειδώθηκε με επιτυχία ως διαχειριστής

5. Πώς να εισέλθετε στη λειτουργία διαχειριστή

Για να εισέλθετε στη λειτουργία διαχειριστή, κάντε τα εξής.

1. Συνδέστε το diskAshur M² σε μια τροφοδοτούμενη θύρα USB στον υπολογιστή σας		Οι κόκκινες, πράσινες και μπλε λυχνίες LED αναβοσβήνουν μία φορά ακολουθία, στη συνέχεια, η ΠΡΑΣΙΝΗ λυχνία LED αναβοσβήνει δύο φορές και τελικά αλλάζει σε μια σταθερή κόκκινη λυχνία LED που υποδεικνύει ότι η μονάδα βρίσκεται σε κατάσταση αναμονής
2. Σε κατάσταση αναμονής (στερεά ΚΟΚΚΙΝΕΣ LED) Πατήστε και κρατήστε πατημένο και τα δύο **Πλήκτρο** (⚷) **+ 1** κουμπιά		Οι πράσινες και μπλε λυχνίες LED αναβοσβήνουν μαζί
3. Εισαγάγετε το **PIN διαχειριστή** και πατήστε το κουμπί **Πλήκτρο** (⚷) μία φορά		Οι πράσινες και μπλε λυχνίες LED θα αναβοσβήνουν γρήγορα μαζί αρκετές φορές και στη συνέχεια θα μεταβούν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED και τελικά θα αλλάξουν σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι η μονάδα δίσκου βρίσκεται σε λειτουργία διαχειριστή

Για έξοδο από τη λειτουργία διαχειριστή

Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ.

6. Αλλαγή του PIN διαχειριστή

Απαιτήσεις PIN:

- Πρέπει να έχει μήκος μεταξύ 7-15 ψηφίων
- Δεν πρέπει να περιέχει μόνο επαναλαμβανόμενους αριθμούς, π.χ. (3-3-3-3-3-3-3)
- Δεν πρέπει να περιέχει μόνο διαδοχικούς αριθμούς, π.χ. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Συμβουλή κωδικού πρόσβασης: Μπορείτε να διαμορφώσετε μια αξέχαστη λέξη, όνομα, φράση ή οποιονδήποτε άλλο συνδυασμό αλφαριθμητικού PIN πατώντας απλώς το κουμπί με τα αντίστοιχα γράμματα πάνω του.

Παραδείγματα αυτών των τύπων αλφαριθμητικών PIN είναι:

- Για "Password" πατήστε τα ακόλουθα κουμπιά:
  7 (pqrs) 2 (abc) 7 (pqrs) 7 (pqrs) 9 (wxyz) 6 (mno) 7 (pqrs) 3 (def)
- Για "iStorage" πατήστε τα ακόλουθα κουμπιά:
  4 (ghi) 7 (pqrs) 8 (tuv) 6 (mno) 7 (pqrs) 2 (abc) 4 (ghi) 3 (def)

Χρησιμοποιώντας αυτήν τη μέθοδο, μπορούν να διαμορφωθούν μεγάλα και εύκολα στην απομνημόνευση PIN.

Για να αλλάξετε το PIN διαχειριστή, μεταβείτε πρώτα στη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή πατήστε και κρατήστε πατημένα και τα δύο κουμπιά **Πλήκτρο** (⚷) **+ 2**		Το συμπαγές μπλε LED θα αλλάξει σε αναβοσβήνει ΠΡΑΣΙΝΟ και συμπαγές LED
2. Εισαγάγετε **ΝΕΟ PIN διαχειριστή** και, στη συνέχεια, πατήστε το κουμπί **Πλήκτρο** (⚷) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα αλλάξουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέψουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε ξανά το **ΝΕΟ PIN διαχειριστή** και, στη συνέχεια, πατήστε το κουμπί **Πλήκτρο** (⚷) μία φορά		Αναβοσβήνουν ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED αλλάζουν σε ΜΠΛΕ LED που αναβοσβήνει γρήγορα και τελικά σε συμπαγή ΜΠΛΕ LED που υποδεικνύει ότι το PIN διαχειριστή έχει αλλάξει με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

7. Ορισμός πολιτικής PIN χρήστη

Ο διαχειριστής μπορεί να ορίσει μια πολιτική περιορισμού για το PIN χρήστη. Αυτή η πολιτική περιλαμβάνει τον καθορισμό του ελάχιστου μήκους του PIN (από 7 έως 15 ψηφία), καθώς και την απαίτηση ή μη εισαγωγής ενός ή περισσότερων «**Ειδικών χαρακτήρων**». Ο "Ειδικός χαρακτήρας" λειτουργεί ως κουμπιά "**ΒΑΡΔΙΑ** (⬆) + **ψηφίο**" πατημένα μαζί.

Για να ορίσετε μια Πολιτική PIN χρήστη (περιορισμοί), θα χρειαστεί να εισαγάγετε 3 ψηφία, για παράδειγμα «**091**», τα δύο πρώτα ψηφία (**09**) υποδεικνύουν το ελάχιστο μήκος PIN (σε αυτήν την περίπτωση, **9**) και το τελευταίο ψηφίο (**1**) υποδηλώνει ότι πρέπει να χρησιμοποιηθούν ένας ή περισσότεροι «Ειδικοί χαρακτήρες», σε άλλα λέξεις «**ΒΑΡΔΙΑ** (⬆)+ ψηφίο'. Με τον ίδιο τρόπο, μια πολιτική PIN χρήστη μπορεί να οριστεί χωρίς την ανάγκη ενός «ειδικού χαρακτήρα», για παράδειγμα «**120**», τα δύο πρώτα ψηφία (**12**) υποδεικνύουν το ελάχιστο μήκος PIN (στην περίπτωση αυτή,**12**) και το τελευταίο ψηφίο (**0**) που σημαίνει ότι δεν απαιτείται Ειδικός Χαρακτήρας.

Μόλις ο Διαχειριστής ορίσει την Πολιτική PIN χρήστη, για παράδειγμα '**091**', θα πρέπει να διαμορφωθεί ένα νέο PIN χρήστη- βλ. ενότητα 10, «Προσθήκη νέου PIN χρήστη σε λειτουργία διαχειριστή». Εάν ο διαχειριστής ρυθμίσει τις παραμέτρους του PIN χρήστη ως '**247688314**' με τη χρήση ενός '**Ειδικός χαρακτήρας**' (**ΒΑΡΔΙΑ** (⬆) + **ψηφίο** πιέζονται προς τα κάτω μαζί), αυτό μπορεί να τοποθετηθεί οπουδήποτε κατά μήκος του 7-15ψήφιου PIN σας κατά τη διαδικασία δημιουργίας του PIN χρήστη όπως φαίνεται στα παρακάτω παραδείγματα.

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

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

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

Σημείωση:

- Εάν χρησιμοποιήθηκε ένας «Ειδικός Χαρακτήρας» κατά τη διαμόρφωση του PIN χρήστη, για παράδειγμα, παράδειγμα «**Β**» παραπάνω, τότε η μονάδα δίσκου μπορεί να ξεκλειδωθεί μόνο εισάγοντας το PIN με τον «Ειδικό Χαρακτήρα» που εισάγεται ακριβώς με τη σειρά που έχει διαμορφωθεί, όπως στο παράδειγμα «**Β**» παραπάνω- ('2', '4', '**ΒΑΡΔΙΑ** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- Περισσότεροι από ένας «Ειδικοί Χαρακτήρες» μπορούν να χρησιμοποιηθούν και να τοποθετηθούν κατά μήκος του 7-15ψήφιου PIN σας.
- Οι χρήστες έχουν τη δυνατότητα να αλλάξουν το PIN τους, αλλά αναγκάζονται να συμμορφώνονται με την καθορισμένη «Πολιτική PIN χρήστη» (περιορισμοί), εάν και όταν ισχύει.
- Ο ορισμός μιας νέας πολιτικής PIN χρήστη θα διαγράψει αυτόματα το PIN χρήστη, εάν υπάρχει.
- Αυτή η πολιτική δεν ισχύει για το 'Self-Destruct PIN'. Η ρύθμιση πολυπλοκότητας για το PIN αυτοκαταστροφής και το PIN διαχειριστή είναι πάντα 7-15 ψηφία, χωρίς να απαιτείται ειδικός χαρακτήρας.

Για να ορίσετε μια **πολιτική PIN χρήστη**, μεταβείτε πρώτα στη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (ಕ) + **7** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Εισαγάγετε τα **3 ψηφία σας**, θυμηθείτε ότι τα δύο πρώτα ψηφία υποδηλώνουν ελάχιστο μήκος PIN και τελευταίο ψηφίο (0 ή 1) ανεξάρτητα από το αν έχει χρησιμοποιηθεί ειδικός χαρακτήρας ή όχι.		Οι πράσινες και μπλε λυχνίες LED που αναβοσβήνουν θα συνεχίσουν να αναβοσβήνουν
3. Πατήστε το κουμπί **ΒΑΡΔΙΑ** (⬆) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED θα αλλάξουν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED και τελικά σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι η Πολιτική PIN χρήστη έχει οριστεί με επιτυχία.

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

8. Τρόπος διαγραφής της πολιτικής PIN χρήστη

Για να διαγράψετε την Πολιτική PIN χρήστη, μεταβείτε πρώτα στη "Λειτουργία διαχειριστή" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε λειτουργία διαχειριστή (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (⚷) + **7** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πληκτρολογήστε 070 και πατήστε το κουμπί **ΒΑΡΔΙΑ** (🡅) μία φορά		Οι πράσινες και μπλε λυχνίες LED που αναβοσβήνουν θα αλλάξουν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED και τελικά σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι η πολιτική PIN χρήστη έχει διαγραφεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

9. Πώς να ελέγξετε την Πολιτική PIN χρήστη

Ο Διαχειριστής είναι σε θέση να ελέγξει την Πολιτική PIN χρήστη και μπορεί να προσδιορίσει τον ελάχιστο περιορισμό μήκους PIN και εάν έχει οριστεί ή όχι η χρήση ενός Ειδικού Χαρακτήρα σημειώνοντας την ακολουθία LED όπως περιγράφεται παρακάτω.

Για να ελέγξετε την Πολιτική PIN χρήστη, μεταβείτε πρώτα στη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **ΒΑΡΔΙΑ** (🡅) + **7** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν

2. Πατήστε το κουμπί **Πλήκτρο** (⚷) και συμβαίνουν τα εξής.

a. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
b. Μια κόκκινη λυχνία LED που αναβοσβήνει ισοδυναμεί με δέκα (10) μονάδες μιας καρφίτσας.
c. Κάθε ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει ισοδυναμεί με μία (1) μονάδα PIN
d. Μια ΜΠΛΕ αναλαμπή υποδεικνύει ότι χρησιμοποιήθηκε ένας «Ειδικός χαρακτήρας».
e. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
f. Οι λυχνίες LED επιστρέφουν στο συμπαγές ΜΠΛΕ

Ο παρακάτω πίνακας περιγράφει τη συμπεριφορά LED κατά τον έλεγχο της Πολιτικής PIN χρήστη, για παράδειγμα εάν έχετε ορίσει ένα 12ψήφιο PIN χρήστη με τη χρήση ενός ειδικού χαρακτήρα (**121**), το ΚΟΚΚΙΝΟ LED θα αναβοσβήσει μία (**1**) φορά και το ΠΡΑΣΙΝΟ LED θα αναβοσβήσει δύο (**2**) ακολουθούμενο από ένα μόνο (**1**) ΜΠΛΕ LED που αναβοσβήνει υποδεικνύοντας ότι **πρέπει να χρησιμοποιηθεί** ένας ειδικός χαρακτήρας.

Περιγραφή PIN	**3ψήφιο Setup**	**ΚΟΚΚΙΝΟΣ**	**ΠΡΑΣΙΝΟΣ**	**ΜΠΛΕ**
12ψήφιο PIN με χρήση ειδικού χαρακτήρα	121	1 Αναβοσβήνει	2 αναβοσβήνει	1 Αναβοσβήνει
12ψήφιο PIN χωρίς χρήση ειδικού χαρακτήρα	120	1 Αναβοσβήνει	2 αναβοσβήνει	0
9ψήφιο PIN με χρήση ειδικού χαρακτήρα	091	0	9 αναβοσβήνει	1 Αναβοσβήνει
9ψήφιο PIN χωρίς χρήση ειδικού χαρακτήρα	090	0	9 αναβοσβήνει	0

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

10. Προσθήκη νέου PIN χρήστη σε λειτουργία διαχειριστή

Σημαντικό: Η δημιουργία PIN νέου χρήστη πρέπει να συμμορφώνεται με την «Πολιτική PIN χρήστη» εάν έχει διαμορφωθεί όπως περιγράφεται στην ενότητα 7, η οποία επιβάλλει ελάχιστο μήκος PIN και εάν έχει χρησιμοποιηθεί «Ειδικός χαρακτήρας». Ο διαχειριστής μπορεί να ανατρέξει στην ενότητα 9 για να ελέγξει τους περιορισμούς PIN χρήστη.

Απαιτήσεις PIN:

- Πρέπει να έχει μήκος μεταξύ 7-15 ψηφίων
- Δεν πρέπει να περιέχει μόνο επαναλαμβανόμενους αριθμούς, π.χ. (3-3-3-3-3-3-3)
- Δεν πρέπει να περιέχει μόνο διαδοχικούς αριθμούς, π.χ. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- Ο **ΒΑΡΔΙΑ** (⬆) μπορεί να χρησιμοποιηθεί για πρόσθετους συνδυασμούς PIN- π.χ. **ΒΑΡΔΙΑ** (⬆) + **1** είναι διαφορετική τιμή από το 1. Ανατρέξτε στην ενότητα 7, «Ορισμός πολιτικής PIN χρήστη».

Για να προσθέσετε ένα **PIN νέου χρήστη**, μεταβείτε πρώτα στη «**Λειτουργία διαχειριστή**» όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (⚷) + **3** κουμπιά		Το συμπαγές μπλε LED θα αλλάξει σε αναβοσβήνει ΠΡΑΣΙΝΟ και συμπαγές μπλε LED
2. Εισαγάγετε **το PIN νέου χρήστη** και πατήστε το κουμπί **Πλήκτρο** (⚷)		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα αλλάξουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέψουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε ξανά το PIN νέου χρήστη και πατήστε **Πλήκτρο** (⚷) κουμπί ξανά		Αναβοσβήνοντας ΠΡΑΣΙΝΟ και συμπαγές ΜΠΛΕ LED αλλάζουν σε ένα ΠΡΑΣΙΝΟ LED που αναβοσβήνει γρήγορα και τελικά σε ένα συμπαγές ΜΠΛΕ LED που υποδεικνύει ότι ένα νέο PIN χρήστη έχει ρυθμιστεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

11. Αλλαγή του PIN χρήστη σε λειτουργία διαχειριστή

Σημαντικό: Η αλλαγή του PIN χρήστη πρέπει να συμμορφώνεται με την «Πολιτική PIN χρήστη» εάν έχει διαμορφωθεί όπως περιγράφεται στην ενότητα 7, η οποία επιβάλλει ελάχιστο μήκος PIN και εάν έχει χρησιμοποιηθεί «Ειδικός χαρακτήρας». Ο Διαχειριστής μπορεί να ανατρέξει στην ενότητα 9 για να ελέγξει τους περιορισμούς PIN χρήστη.

Για να αλλάξετε ένα υπάρχον **PIN χρήστη,** μεταβείτε πρώτα στη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (⚷) + **3** κουμπιά		Το συμπαγές μπλε LED θα αλλάξει σε αναβοσβήνει ΠΡΑΣΙΝΟ και συμπαγές μπλε LED
2. Εισαγάγετε **το PIN νέου χρήστη** και πατήστε το κουμπί **Πλήκτρο** (⚷) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα αλλάξουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέψουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε ξανά το **PIN νέου χρήστη** και πατήστε **Πλήκτρο** (⚷) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED αλλάζουν σε ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει γρήγορα και τελικά σε συμπαγή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι το PIN χρήστη έχει αλλάξει με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

12. Διαγραφή του PIN χρήστη στη λειτουργία διαχειριστή

Για να διαγράψετε ένα υπάρχον PIN χρήστη, μεταβείτε πρώτα στη "Λειτουργία διαχειριστή" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε λειτουργία διαχειριστή (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **ΒΑΡΔΙΑ** (⬆) + **3** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΚΟΚΚΙΝΗ λυχνία LED που αναβοσβήνει
2. Πατήστε και κρατήστε πατημένα και τα δύο **ΒΑΡΔΙΑ** (⬆) + **3** κουμπιά ξανά		Η κόκκινη λυχνία LED που αναβοσβήνει θα αλλάξει σε σταθερή ΚΟΚΚΙΝΗ λυχνία LED και, στη συνέχεια, σε σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι το PIN χρήστη έχει διαγραφεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

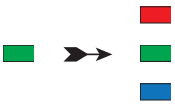
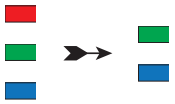
13. Πώς να ξεκλειδώσετε το diskAshur M² με PIN χρήστη

Για να ξεκλειδώσετε το diskAshur M² με το **PIN χρήστη**, ακολουθήστε τα παρακάτω βήματα.

1. Σε κατάσταση αναμονής (συμπαγές ΚΟΚΚΙΝΟΣ LED) Πατήστε και κρατήστε πατημένα και τα δύο κουμπιά **ΒΑΡΔΙΑ** (⬆) + **Πλήκτρο** (ಕ)		Οι διακόπτες ΚΟΚΚΙΝΟΣ LED σε όλα τα LED, ΚΟΚΚΙΝΟΣ, ΠΡΑΣΙΝΕΣ &; ΜΠΛΕ αναβοσβήνουν και σβήνουν
2. Εισαγάγετε **το PIN χρήστη** και πατήστε το κουμπί **Πλήκτρο** (ಕ) μία φορά		Οι λυχνίες LED που αναβοσβήνουν ΚΟΚΚΙΝΟΣ, ΠΡΑΣΙΝΕΣ και ΜΠΛΕ θα αλλάξουν σε εναλλασσόμενες ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED και στη συνέχεια σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED που υποδεικνύει ότι η μονάδα δίσκου ξεκλειδώθηκε επιτυχώς στη λειτουργία χρήστη

14. Αλλαγή του PIN χρήστη σε λειτουργία χρήστη

Για να αλλάξετε το **PIN χρήστη**, ξεκλειδώστε πρώτα το diskAshur M² με το PIN χρήστη όπως περιγράφεται στην ενότητα 13. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία χρήστη** (συμπαγές ΠΡΑΣΙΝΟ LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία χρήστη (GREEN LED) πατήστε και κρατήστε πατημένα και τα δύο κουμπιά **Πλήκτρο** (ಕ) + **4**		Η συμπαγής πράσινη λυχνία LED θα αλλάξει σε όλες τις λυχνίες LED, ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΟ &; ΜΠΛΕ που αναβοσβήνει και σβήνει
2. Εισαγάγετε το **υπάρχον PIN χρήστη** και πατήστε το **Πλήκτρο** (ಕ) μία φορά		Οι πράσινες και συμπαγείς μπλε λυχνίες LED θα ενεργοποιούνται και θα σβήνουν εναλλάξ και στη συνέχεια θα μεταβαίνουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέφουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε το νέο PIN χρήστη και πατήστε το **Πλήκτρο** (ಕ) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα αλλάξουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέψουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
4. Εισαγάγετε ξανά το PIN νέου χρήστη και πατήστε το **Πλήκτρο** (ಕ) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα μεταβούν σε μια ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει γρήγορα και, στη συνέχεια, σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED που υποδεικνύει ότι το PIN χρήστη έχει αλλάξει με επιτυχία

Σημαντικό: Η αλλαγή του PIN χρήστη σε λειτουργία χρήστη (ΠΡΑΣΙΝΟ LED) πρέπει να συμμορφώνεται με την «Πολιτική PIN χρήστη» εάν έχει διαμορφωθεί όπως περιγράφεται στην ενότητα 7, η οποία επιβάλλει ελάχιστο μήκος PIN και εάν έχει χρησιμοποιηθεί «Ειδικός χαρακτήρας».

15. Δημιουργία PIN ανάκτησης χρήστη μίας χρήσης

Το PIN ανάκτησης χρήστη είναι εξαιρετικά χρήσιμο σε περιπτώσεις όπου ένας χρήστης έχει ξεχάσει το PIN του για να ξεκλειδώσει το diskAshur M².
Για να ενεργοποιήσετε τη λειτουργία ανάκτησης, ο χρήστης πρέπει πρώτα να εισαγάγει το σωστό PIN ανάκτησης μίας χρήσης, εάν έχει ρυθμιστεί. Η διαδικασία ανάκτησης PIN χρήστη δεν επηρεάζει τα δεδομένα, το κλειδί κρυπτογράφησης και το PIN

διαχειριστή, ωστόσο ο χρήστης αναγκάζεται να διαμορφώσει ένα νέο 7-15ψήφιο PIN χρήστη.
Για να διαμορφώσετε ένα PIN ανάκτησης χρήστη μίας χρήσης 7-15 ψηφίων, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις εισέλθει η μονάδα δίσκου **Λειτουργία διαχειριστή** (συμπαγές μπλε LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (⚷) + **4** κουμπιά		Το συμπαγές μπλε LED θα αλλάξει σε αναβοσβήνει ΠΡΑΣΙΝΟ και συμπαγές μπλε LED
2. Εισαγάγετε ένα **PIN εφάπαξ ανάκτησης** και πατήστε Κουμπί **Πλήκτρο** (⚷)		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα αλλάξουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέψουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε ξανά το **PIN εφάπαξ ανάκτησης** και πατήστε **Πλήκτρο** (⚷) ξανά		Αναβοσβήνοντας ΠΡΑΣΙΝΟ και συμπαγές ΜΠΛΕ LED αλλάζουν σε ένα ΠΡΑΣΙΝΟ LED που αναβοσβήνει γρήγορα και τελικά σε ένα συμπαγές ΜΠΛΕ LED που υποδεικνύει ότι το PIN εφάπαξ ανάκτησης έχει ρυθμιστεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

16. Διαγραφή του PIN ανάκτησης χρήστη μίας χρήσης

Για να διαγράψετε το PIN ανάκτησης χρήστη μίας χρήσης, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **ΒΑΡΔΙΑ** (⬆) + **4** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΚΟΚΚΙΝΗ λυχνία LED που αναβοσβήνει
2. Πατήστε και κρατήστε πατημένα και τα δύο **ΒΑΡΔΙΑ** (⬆) + **4** κουμπιά ξανά		Αναβοσβήνει το ΚΟΚΚΙΝΗ LED θα γίνει σταθερό ΚΟΚΚΙΝΗ και στη συνέχεια θα μεταβεί σε ένα συμπαγές ΜΠΛΕ LED που δείχνει ότι το One-Ώρα PIN αποκατάστασης χρήστη έχει Διαγράφηκε με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

17. Ενεργοποίηση λειτουργίας ανάκτησης και δημιουργία νέου PIN χρήστη

Το PIN ανάκτησης χρήστη είναι εξαιρετικά χρήσιμο σε περιπτώσεις όπου ένας χρήστης έχει ξεχάσει το PIN του για να ξεκλειδώσει το diskAshur M².

Για να ενεργοποιήσετε τη λειτουργία ανάκτησης, ο χρήστης πρέπει πρώτα να εισαγάγει το σωστό PIN ανάκτησης μίας χρήσης, εάν έχει ρυθμιστεί. Η διαδικασία ανάκτησης PIN χρήστη δεν επηρεάζει τα δεδομένα, το κλειδί κρυπτογράφησης και το PIN διαχειριστή, ωστόσο ο χρήστης αναγκάζεται να διαμορφώσει ένα νέο 7-15ψήφιο PIN χρήστη.

Για να ενεργοποιήσετε τη διαδικασία ανάκτησης και να διαμορφώσετε ένα νέο PIN χρήστη, ακολουθήστε τα παρακάτω βήματα

1. **Σε κατάσταση αναμονής** (ΚΟΚΚΙΝΟΣ LED) πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (ಕ) + **4** κουμπιά		Η συμπαγής κόκκινη λυχνία LED θα αλλάξει σε ΚΟΚΚΙΝΕΣ και ΠΡΑΣΙΝΕΣ λυχνίες LED που αναβοσβήνουν
2. Εισαγάγετε το PIN εφάπαξ **ανάκτησης** και πατήστε το κουμπί **Πλήκτρο** (ಕ)		Οι πράσινες και μπλε λυχνίες LED εναλλάσσονται και σβήνουν, στη συνέχεια σε ένα συμπαγές ΠΡΑΣΙΝΟ LED και τέλος σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε ένα **νέο PIN χρήστη** και πατήστε το **Πλήκτρο** (ಕ) κουμπί		Αναβοσβήνουν ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED αλλάζουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED και στη συνέχεια επιστρέφουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
4. Εισαγάγετε ξανά το **νέο PIN χρήστη** και πατήστε το κουμπί **Πλήκτρο** (ಕ) ξανά		Η πράσινη λυχνία LED αναβοσβήνει γρήγορα και στη συνέχεια γίνεται σταθερή ΠΡΑΣΙΝΗ υποδεικνύοντας ότι η διαδικασία ανάκτησης ήταν επιτυχής και διαμορφώθηκε ένα νέο PIN χρήστη

Σημαντικό: Η δημιουργία PIN νέου χρήστη πρέπει να συμμορφώνεται με την «Πολιτική PIN χρήστη» εάν έχει διαμορφωθεί όπως περιγράφεται στην ενότητα 7, η οποία επιβάλλει ελάχιστο μήκος PIN και εάν έχει χρησιμοποιηθεί «Ειδικός χαρακτήρας». Ο διαχειριστής μπορεί να ανατρέξει στην ενότητα 9 για να ελέγξει τους περιορισμούς PIN χρήστη.

18. Ορισμός μόνο για ανάγνωση χρήστη σε λειτουργία διαχειριστή

Με τόσους πολλούς ιούς και δούρειους ίππους να μολύνουν μονάδες USB, η λειτουργία μόνο για ανάγνωση είναι ιδιαίτερα χρήσιμη εάν πρέπει να έχετε πρόσβαση σε δεδομένα στη μονάδα USB όταν χρησιμοποιείται σε δημόσιο περιβάλλον. Αυτό είναι επίσης ένα βασικό χαρακτηριστικό για εγκληματολογικούς σκοπούς, όπου τα δεδομένα πρέπει να διατηρούνται στην αρχική τους και αμετάβλητη κατάσταση που δεν μπορεί να τροποποιηθεί ή να αντικατασταθεί.

Όταν ο Διαχειριστής ρυθμίσει τις παραμέτρους του diskAshur M² και περιορίσει την πρόσβαση του Χρήστη σε Μόνο για ανάγνωση, τότε μόνο ο Διαχειριστής μπορεί να γράψει στη μονάδα δίσκου ή να αλλάξει τη ρύθμιση σε Ανάγνωση/Εγγραφή όπως περιγράφεται στην ενότητα 19. Ο χρήστης περιορίζεται στην πρόσβαση μόνο για ανάγνωση και δεν μπορεί να γράψει στη μονάδα δίσκου ή να αλλάξει αυτήν τη ρύθμιση σε κατάσταση λειτουργίας χρήστη.

Για να ρυθμίσετε το diskAshur M² και να περιορίσετε την πρόσβαση του χρήστη σε Μόνο για ανάγνωση, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο κουμπιά "**7 + 6**".		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πατήστε το κουμπί **Πλήκτρο** (ಕ) μία φορά		Οι πράσινες και μπλε λυχνίες LED θα αλλάξουν σε σταθερή ΠΡΑΣΙΝΗ λυχνία LED και, στη συνέχεια, σε σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι η μονάδα δίσκου έχει ρυθμιστεί και περιορίζει την πρόσβαση του χρήστη μόνο για ανάγνωση

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

19. Ενεργοποίηση ανάγνωσης/εγγραφής χρήστη σε λειτουργία διαχειριστή

Για να επαναφέρετε το diskAshur M2 σε Ανάγνωση/Εγγραφή, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις εισέλθει η μονάδα δίσκου **Λειτουργία διαχειριστή** (συμπαγές μπλε LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο κουμπιά "**7 + 9**".		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2.Πατήστε το κουμπί **Πλήκτρο** (ὃ) μία φορά		Τα πράσινα και μπλε LED αλλάζουν σε ένα συμπαγές ΠΡΑΣΙΝΟ LED και στη συνέχεια σε ένα συμπαγές ΜΠΛΕ LED υποδεικνύοντας ότι η μονάδα δίσκου έχει ρυθμιστεί ως ανάγνωση/εγγραφή

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

20. Ορισμός καθολικής μόνο για ανάγνωση σε λειτουργία διαχειριστή

Όταν ο διαχειριστής ρυθμίζει τις παραμέτρους του diskAshur M² και τον περιορίζει σε καθολικό μόνο για ανάγνωση, τότε ούτε ο διαχειριστής ούτε ο χρήστης μπορούν να γράψουν στη μονάδα δίσκου και αμφότεροι περιορίζονται στην πρόσβαση μόνο για ανάγνωση. Μόνο ο Διαχειριστής μπορεί να επαναφέρει τη ρύθμιση σε Ανάγνωση/Εγγραφή, όπως περιγράφεται στην ενότητα 21.

Για να ρυθμίσετε το diskAshur M² και να περιορίσετε την καθολική πρόσβαση σε Μόνο για ανάγνωση, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο κουμπιά "**5 + 6**"		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2.. Πατήστε το κουμπί **Πλήκτρο** (ὃ)		Οι πράσινες και μπλε λυχνίες LED θα αλλάξουν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED και, στη συνέχεια, σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι η μονάδα δίσκου έχει διαμορφωθεί και περιορίζει την καθολική πρόσβαση μόνο

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

21. Ενεργοποίηση καθολικής ανάγνωσης/εγγραφής σε λειτουργία διαχειριστή

Για να επαναφέρετε το diskAshur M² σε Ανάγνωση/Εγγραφή από τη ρύθμιση Global Read-Only, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο κουμπιά "**5 + 9**"		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πατήστε το κουμπί **Πλήκτρο** (ὃ)		Τα πράσινα και μπλε LED αλλάζουν σε ένα συμπαγές ΠΡΑΣΙΝΟ LED και στη συνέχεια σε ένα συμπαγές ΜΠΛΕ LED υποδεικνύοντας ότι η μονάδα δίσκου έχει ρυθμιστεί ως ανάγνωση/εγγραφή

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

22. Πώς να ρυθμίσετε ένα PIN αυτοκαταστροφής

Μπορείτε να διαμορφώσετε ένα PIN αυτοκαταστροφής το οποίο όταν εισάγεται εκτελεί Crypto-Erase στη μονάδα δίσκου (το κλειδί κρυπτογράφησης διαγράφεται). Αυτή η διαδικασία διαγράφει όλα τα διαμορφωμένα PIN και καθιστά όλα τα δεδομένα που είναι αποθηκευμένα στη μονάδα δίσκου ως απρόσιτα (χαμένα για πάντα), η μονάδα δίσκου θα εμφανιστεί στη συνέχεια ως ξεκλείδωτη ΠΡΑΣΙΝΗ λυχνία. Η εκτέλεση αυτής της δυνατότητας θα έχει ως αποτέλεσμα το PIN αυτοκαταστροφής να γίνει το PIN νέου χρήστη και η μονάδα δίσκου θα πρέπει να μορφοποιηθεί για να μπορέσει να χρησιμοποιηθεί ξανά.

Για να ορίσετε το PIN αυτοκαταστροφής, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (ὃ) + **6** κουμπιά		Το συμπαγές μπλε LED θα αλλάξει σε αναβοσβήνει ΠΡΑΣΙΝΟ και συμπαγές μπλε LED
2. Διαμορφώστε και εισαγάγετε ένα 7-15ψήφιο PIN αυτοκαταστροφής και πατήστε το κουμπί **Πλήκτρο** (ὃ)		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα αλλάξουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέψουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε ξανά το PIN αυτοκαταστροφής και πατήστε το κουμπί **Πλήκτρο** (ὃ)		Η ΠΡΑΣΙΝΗ λυχνία LED αναβοσβήνει γρήγορα για αρκετά δευτερόλεπτα και, στη συνέχεια, αλλάζει σε σταθερή ΜΠΛΕ λυχνία LED για να υποδείξει ότι το PIN αυτοκαταστροφής έχει ρυθμιστεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

23. Πώς να διαγράψετε το PIN αυτοκαταστροφής

Για να διαγράψετε το PIN αυτοκαταστροφής, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **ΒΑΡΔΙΑ** (⬆) + **6** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΚΟΚΚΙΝΗ λυχνία LED που αναβοσβήνει
2. Πατήστε και κρατήστε πατημένα τα κουμπιά **ΒΑΡΔΙΑ** (⬆) + **6** ξανά		Η κόκκινη λυχνία LED που αναβοσβήνει θα γίνει σταθερή και, στη συνέχεια, θα αλλάξει σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι το PIN αυτοκαταστροφής διαγράφηκε με επιτυχία

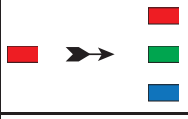
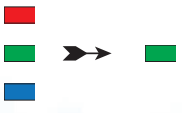
Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

24. Πώς να ξεκλειδώσετε με το PIN αυτοκαταστροφής

Προειδοποίηση: Όταν ενεργοποιηθεί ο μηχανισμός αυτοκαταστροφής, όλα τα δεδομένα, το κλειδί κρυπτογράφησης και τα PIN διαχειριστή/χρήστη διαγράφονται. **Το PIN αυτοκαταστροφής γίνεται το PIN χρήστη**. Δεν υπάρχει PIN διαχειριστή μετά την ενεργοποίηση του μηχανισμού αυτοκαταστροφής. Θα πρέπει πρώτα να γίνει επαναφορά του diskAshur M² (δείτε την ενότητα 35 «Πώς να εκτελέσετε πλήρη επαναφορά», στη σελίδα 25) προκειμένου να διαμορφώσετε ένα PIN διαχειριστή με πλήρη δικαιώματα διαχειριστή, συμπεριλαμβανομένης της δυνατότητας διαμόρφωσης ενός νέου PIN χρήστη.

Όταν χρησιμοποιείται, το PIN αυτοκαταστροφής θα διαγράψει ΟΛΑ τα δεδομένα, τα PIN διαχειριστή / χρήστη και στη συνέχεια θα ξεκλειδώσει τη μονάδα δίσκου. Η ενεργοποίηση αυτής της δυνατότητας θα έχει ως αποτέλεσμα το PIN αυτοκαταστροφής να γίνει το PIN νέου χρήστη και ο diskAshur M² θα πρέπει να μορφοποιηθεί πριν προστεθούν νέα δεδομένα στη μονάδα δίσκου.

Για να ενεργοποιήσετε το μηχανισμό αυτοκαταστροφής, η μονάδα δίσκου πρέπει να βρίσκεται σε κατάσταση αναμονής (στερεά κόκκινη λυχνία LED) και, στη συνέχεια, να προχωρήσετε στα παρακάτω βήματα.

1. Σε κατάσταση αναμονής (συμπαγές κόκκινο LED), πατήστε και κρατήστε πατημένα και τα δύο κουμπιά **ΒΑΡΔΙΑ** (⬆) + **Πλήκτρο** (⚷)		Οι διακόπτες ΚΟΚΚΙΝΗ LED σε όλα τα LED, ΚΟΚΚΙΝΗ, ΠΡΑΣΙΝΕΣ &; ΜΠΛΕ αναβοσβήνουν και σβήνουν
2. Εισαγάγετε το PIN Self-Destruct και πατήστε το κουμπί **Πλήκτρο** (⚷)		Τα ΚΟΚΚΙΝΑ, ΠΡΑΣΙΝΑ και ΜΠΛΕ LED που αναβοσβήνουν θα αλλάξουν σε ΠΡΑΣΙΝΑ και ΜΠΛΕ LED που εναλλάσσονται για λίγα δευτερόλεπτα και τελικά μετατοπίζονται σε ένα συμπαγές ΠΡΑΣΙΝΟ LED που δείχνει ότι ο diskAshur M² έχει αυτοκαταστραφεί με επιτυχία

25. Πώς να ρυθμίσετε ένα PIN διαχειριστή μετά από επίθεση ή επαναφορά ωμής βίας

Θα χρειαστεί μετά από μια επίθεση Brute Force ή όταν γίνει επαναφορά του diskAshur M² για να διαμορφώσετε ένα PIN διαχειριστή πριν από τη χρήση της μονάδας δίσκου.

Απαιτήσεις PIN:

- Πρέπει να έχει μήκος μεταξύ 7-15 ψηφίων
- Δεν πρέπει να περιέχει μόνο επαναλαμβανόμενους αριθμούς, π.χ. (3-3-3-3-3-3-3)
- Δεν πρέπει να περιέχει μόνο διαδοχικούς αριθμούς, π.χ. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Εάν ο diskAshur M² έχει εξαναγκαστεί ή επαναρυθμιστεί, η μονάδα δίσκου θα βρίσκεται σε κατάσταση αναμονής (στερεά κόκκινο LED). για να ρυθμίσετε τις παραμέτρους ενός PIN διαχειριστή, ακολουθήστε τα παρακάτω βήματα.

1. Σε κατάσταση αναμονής (συμπαγές κόκκινο LED), πατήστε και κρατήστε πατημένα και τα δύο κουμπιά **ΒΑΡΔΙΑ** (⬆) + **1**		Το στερεό κόκκινο LED θα αλλάξει σε αναβοσβήνει ΠΡΑΣΙΝΟ και συμπαγές μπλε LED
2. Εισαγάγετε **το νέο PIN διαχειριστή** και πατήστε **Πλήκτρο** (ꕥ) κουμπί		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED θα αλλάξουν σε μία μόνο ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει και στη συνέχεια θα επιστρέψουν σε ΠΡΑΣΙΝΕΣ και συμπαγείς μπλε λυχνίες LED που αναβοσβήνουν
3. Εισαγάγετε ξανά **το νέο PIN διαχειριστή** και πατήστε **Πλήκτρο** (ꕥ) Κουμπί		Αναβοσβήνει το ΠΡΑΣΙΝΟ LED και το συμπαγές ΜΠΛΕ LED αλλάζουν σε ΜΠΛΕ LED που αναβοσβήνουν γρήγορα για λίγα δευτερόλεπτα και στη συνέχεια σε ένα συμπαγές ΜΠΛΕ LED που υποδεικνύει ότι το PIN διαχειριστή έχει ρυθμιστεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

26. Ρύθμιση του αυτόματου κλειδώματος χωρίς παρακολούθηση

Για προστασία από μη εξουσιοδοτημένη πρόσβαση εάν η μονάδα δίσκου είναι ξεκλείδωτη και χωρίς επιτήρηση, ο diskAshur M² μπορεί να ρυθμιστεί ώστε να κλειδώνει αυτόματα μετά από ένα προκαθορισμένο χρονικό διάστημα. Στην προεπιλεγμένη του κατάσταση, η λειτουργία χρονικού ορίου αυτόματου κλειδώματος χωρίς παρακολούθηση diskAshur M² είναι απενεργοποιημένη. Το αυτόματο κλείδωμα χωρίς παρακολούθηση μπορεί να ρυθμιστεί ώστε να ενεργοποιείται μεταξύ 5- 99 λεπτών.

Για να ορίσετε τη λειτουργία χρονικού ορίου αυτόματου κλειδώματος χωρίς παρακολούθηση, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1.Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (ಕ) + **5** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Εισαγάγετε το χρονικό διάστημα για το οποίο θέλετε να ορίσετε τη λειτουργία χρονικού ορίου αυτόματου κλειδώματος, ο ελάχιστος χρόνος που μπορεί να οριστεί είναι 5 λεπτά και ο μέγιστος 99 λεπτά (5-99 λεπτά). Για παράδειγμα, ληκτρολογήστε: **05 για 5 λεπτά (πατήστε '0' ακολουθούμενο από '5')** **20 για 20 λεπτά (πατήστε '2' ακολουθούμενο από '0')** **99 για 99 λεπτά (πατήστε '9' ακολουθούμενο από άλλο '9')**		
3. Πατήστε το κουμπί **ΒΑΡΔΙΑ** (🡅)		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED θα αλλάξουν σε σταθερό ΠΡΑΣΙΝΟ για ένα δευτερόλεπτο και τελικά σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι το χρονικό όριο αυτόματου κλειδώματος έχει ρυθμιστεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

27. Απενεργοποίηση του αυτόματου κλειδώματος χωρίς παρακολούθηση

Για να απενεργοποιήσετε τη λειτουργία χρονικού ορίου αυτόματου κλειδώματος χωρίς παρακολούθηση, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις εισέλθει η μονάδα δίσκου **Λειτουργία διαχειριστή** (συμπαγές μπλε LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (ಕ) + **5** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πληκτρολογήστε **00** και πατήστε το κουμπί **ΒΑΡΔΙΑ** (🡅) button		Οι πράσινες και μπλε λυχνίες LED που αναβοσβήνουν θα αλλάξουν σε συμπαγές ΠΡΑΣΙΝΟ για ένα δευτερόλεπτο και τελικά σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι το χρονικό όριο αυτόματου κλειδώματος έχει απενεργοποιηθεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

28. Πώς να ελέγξετε το αυτόματο κλείδωμα χωρίς παρακολούθηση

Ο Διαχειριστής είναι σε θέση να ελέγξει και να καθορίσει το χρονικό διάστημα που έχει οριστεί για τη λειτουργία χρονικού ορίου αυτόματου κλειδώματος χωρίς παρακολούθηση σημειώνοντας απλώς την ακολουθία LED όπως περιγράφεται στον παρακάτω πίνακα.

Για να ελέγξετε το αυτόματο κλείδωμα χωρίς παρακολούθηση, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένο το πλήκτρο **ΒΑΡΔΙΑ** (⬆) + **5**		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πατήστε το κουμπί **Πλήκτρο** (⚷) και συμβαίνουν τα εξής. a. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ,) γίνονται σταθερά για 1 δευτερόλεπτο. b. Κάθε ΚΟΚΚΙΝΟ LED που αναβοσβήνει ισοδυναμεί με δέκα (10) λεπτά. c. Κάθε ΠΡΑΣΙΝΟ LED που αναβοσβήνει ισοδυναμεί με ένα (1) λεπτό. d. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο. e. Οι λυχνίες LED επιστρέφουν στο συμπαγές ΜΠΛΕ		

Ο παρακάτω πίνακας περιγράφει τη συμπεριφορά LED κατά τον έλεγχο του αυτόματου κλειδώματος χωρίς επιτήρηση, για παράδειγμα εάν έχετε ρυθμίσει τη μονάδα δίσκου να κλειδώνει αυτόματα μετά από **25** λεπτά, η ΚΟΚΚΙΝΗ λυχνία LED θα αναβοσβήνει δύο (**2**) φορές και η ΠΡΑΣΙΝΗ λυχνία LED θα αναβοσβήνει πέντε (**5**) φορές.

Αυτόματο κλείδωμα μέσα σε λίγα λεπτά	**ΚΟΚΚΙΝΟΣ**	**ΠΡΑΣΙΝΟΣ**
5 λεπτά	0	5 αναβοσβήνει
15 λεπτά	1 Αναβοσβήνει	5 αναβοσβήνει
25 λεπτά	2 αναβοσβήνει	5 αναβοσβήνει
40 λεπτά	4 αναβοσβήνει	0

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

29. Ορισμός μόνο για ανάγνωση σε λειτουργία χρήστη

Για να ρυθμίσετε το diskAshur M² σε Μόνο για ανάγνωση, εισαγάγετε πρώτα τη "**Λειτουργία χρήστη**" όπως περιγράφεται στην ενότητα 13. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία χρήστη** (συμπαγές ΠΡΑΣΙΝΟ LED), προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία χρήστη, πατήστε και κρατήστε πατημένα και τα δύο κουμπιά "**7 + 6**".		Το συμπαγές ΠΡΑΣΙΝΟ LED θα αλλάξει σε ΠΡΑΣΙΝΟ και ΜΠΛΕ LED που αναβοσβήνει
2. Πατήστε το κουμπί **Πλήκτρο** (⚷)		Οι πράσινες και μπλε λυχνίες LED θα αλλάξουν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED που υποδεικνύει ότι η μονάδα έχει διαμορφωθεί ως μόνο για ανάγνωση

Σημείωση: 1. Εάν ένας χρήστης ορίσει τη μονάδα δίσκου ως Μόνο για ανάγνωση, ο Διαχειριστής μπορεί να το παρακάμψει ορίζοντας τη μονάδα δίσκου ως Ανάγνωση/Εγγραφή σε λειτουργία διαχειριστή.

2. Εάν ο διαχειριστής ορίσει τη μονάδα δίσκου ως μόνο για ανάγνωση, ο χρήστης δεν μπορεί να ορίσει τη μονάδα δίσκου ως ανάγνωση/εγγραφή.

30. Ενεργοποίηση ανάγνωσης/εγγραφής σε λειτουργία χρήστη

Για να ρυθμίσετε το diskAshur M² σε ανάγνωση/εγγραφή, εισαγάγετε πρώτα τη "**Λειτουργία χρήστη**" όπως περιγράφεται στην ενότητα 13. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία χρήστη** (συμπαγές ΠΡΑΣΙΝΟ LED), προχωρήστε στα παρακάτω βήματα.



1.Στη λειτουργία χρήστη, πατήστε και κρατήστε πατημένα τα κουμπιά "**7 + 9**"		Το συμπαγές ΠΡΑΣΙΝΟ LED θα αλλάξει σε ΠΡΑΣΙΝΟ και ΜΠΛΕ LED που αναβοσβήνει
2. Πατήστε το κουμπί **Πλήκτρο** (♿)		Οι πράσινες και μπλε λυχνίες LED θα αλλάξουν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED που υποδεικνύει ότι η μονάδα δίσκου έχει διαμορφωθεί ως ανάγνωση/εγγραφή



Σημείωση: 1. Εάν ένας χρήστης ορίσει τη μονάδα δίσκου ως Μόνο για ανάγνωση, ο Διαχειριστής μπορεί να το παρακάμψει ορίζοντας τη μονάδα δίσκου ως Ανάγνωση/Εγγραφή σε λειτουργία διαχειριστή.

2. Εάν ο διαχειριστής ορίσει τη μονάδα δίσκου ως μόνο για ανάγνωση, ο χρήστης δεν μπορεί να ορίσει τη μονάδα δίσκου ως ανάγνωση/εγγραφή.

31. Brute Force Hack Μηχανισμός Άμυνας

Ο diskAshur M² ενσωματώνει έναν αμυντικό μηχανισμό για την προστασία της μονάδας από επιθέσεις Brute Force. Από προεπιλογή, οι αρχικές τιμές κατάστασης αποστολής του περιορισμού ωμής βίας (διαδοχικές εσφαλμένες καταχωρήσεις PIN) τόσο για το PIN διαχειριστή όσο και για το PIN χρήστη είναι **10** και **5** για το PIN ανάκτησης. Τρεις ανεξάρτητοι μετρητές ωμής βίας χρησιμοποιούνται για την καταγραφή των εσφαλμένων προσπαθειών για κάθε εξουσιοδότηση PIN (Διαχειριστής, Χρήστης και Ανάκτηση), όπως ορίζεται παρακάτω.

- Εάν ένας χρήστης εισαγάγει **εσφαλμένο PIN χρήστη** 10 συνεχόμενες φορές, το PIN χρήστη θα διαγραφεί, αλλά τα δεδομένα, το PIN διαχειριστή και το PIN ανάκτησης παραμένουν ανέπαφα και προσβάσιμα.
- Εάν εισαχθεί εσφαλμένο **PIN ανάκτησης** 5 συνεχόμενες φορές, το PIN ανάκτησης διαγράφεται, αλλά τα δεδομένα και το PIN διαχειριστή παραμένουν ανέπαφα και προσβάσιμα.
- Εάν εισαχθεί **εσφαλμένο PIN διαχειριστή** 10 συνεχόμενες φορές, θα γίνει επαναφορά της μονάδας δίσκου. Όλα τα PIN και τα δεδομένα διαγράφονται και χάνονται για πάντα.

Ο παρακάτω πίνακας υποθέτει ότι και τα τρία PIN έχουν ρυθμιστεί και επισημαίνει το αποτέλεσμα της ενεργοποίησης του μηχανισμού άμυνας ωμής βίας κάθε μεμονωμένου PIN.

PIN που χρησιμοποιείται για το ξεκλείδωμα της μονάδας δίσκου	Διαδοχικές εσφαλμένες καταχωρήσεις PIN	Περιγραφή του τι συμβαίνει
PIN χρήστη	10	• Το PIN χρήστη διαγράφεται. • Το PIN ανάκτησης, το PIN διαχειριστή και όλα τα δεδομένα παραμένουν ανέπαφα και προσβάσιμα.
PIN ανάκτησης	5	• Το PIN ανάκτησης διαγράφεται. • Το PIN διαχειριστή και όλα τα δεδομένα παραμένουν ανέπαφα και προσβάσιμα.
PIN διαχειριστή	10	• Θα γίνει επαναφορά του diskAshur M². Όλα τα PIN και τα δεδομένα.

Σημείωση: Ο περιορισμός ωμής βίας είναι προεπιλεγμένος στις αρχικές τιμές κατάστασης αποστολής όταν γίνει πλήρης επαναφορά της μονάδας δίσκου,ή η λειτουργία αυτοκαταστροφής είναι ενεργοποιημένη ή ωμή αναγκαστική. Εάν ο διαχειριστής αλλάξει το PIN χρήστη ή οριστεί νέο PIN χρήστη κατά την ενεργοποίηση της δυνατότητας ανάκτησης, ο μετρητής ωμής βίας PIN χρήστη μηδενίζεται (0), αλλά ο περιορισμός ωμής βίας δεν επηρεάζεται. Εάν ο διαχειριστής αλλάξει το PIN αποκατάστασης, ο μετρητής ωμής βίας PIN ανάκτησης μηδενίζεται.
Η επιτυχής εξουσιοδότηση ενός συγκεκριμένου PIN θα μηδενίσει τον μετρητή ωμής βίας για το συγκεκριμένο PIN, αλλά δεν θα επηρεάσει τον μετρητή ωμής βίας των άλλων PIN. Η αποτυχία εξουσιοδότησης ενός συγκεκριμένου PIN θα αυξήσει τον μετρητή ωμής βίας για το συγκεκριμένο PIN, αλλά δεν θα επηρεάσει τον μετρητή ωμής βίας των άλλων PIN.

32. Admin PIN ωμή δύναμη Hack Μηχανισμός Άμυνας

Το diskAshur M² Admin PIN είναι εξοπλισμένο με έναν πιο εξελιγμένο αμυντικό μηχανισμό σε σύγκριση με το PIN χρήστη ή το PIN ανάκτησης. Αυτό έχει σκοπό να προστατεύσει από την κατά λάθος εισαγωγή λανθασμένου PIN διαχειριστή 10 συνεχόμενες φορές και, στη συνέχεια, την απώλεια όλων των δεδομένων σας. Έτσι, μετά από 5 διαδοχικές λανθασμένες καταχωρήσεις PIN διαχειριστή, ο diskAshur M² θα κλειδώσει και όλα τα LED θα ανάψουν και θα γίνουν σταθερά.

ΠΡΟΕΙΔΟΠΟΙΗΣΗ: Μην επιχειρήσετε τις ακόλουθες οδηγίες εάν ξεκλειδώσετε το δίσκο diskAshur M² χρησιμοποιώντας μόνο το '**USER PIN**' και δεν γνωρίζετε το '**ADMIN PIN**'.

Ανατρέξτε στις οδηγίες στον παρακάτω πίνακα για να ενεργοποιήσετε περαιτέρω καταχωρήσεις PIN διαχειριστή έως και 10.

Διαδοχικές εσφαλμένες καταχωρήσεις PIN διαχειριστή	Περιγραφή του τι συμβαίνει με το diskAshur M²	Οδηγίες
5	Όλα τα LED, ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΟ &; ΜΠΛΕ ανάψτε και γίνετε σταθεροί.	Εισαγάγετε το ακόλουθο PIN '**47867243**' και πατήστε το **Πλήκτρο** (🔑) μία φορά, με τις ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED να αναβοσβήνουν εναλλάξ και να σβήνουν, το diskAshur M² είναι έτοιμο να δεχτεί άλλες **3 καταχωρήσεις PIN** διαχειριστή .
8	Όλα τα LED, ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΟ &; ΜΠΛΕ Αναβοσβήνει εναλλάξ και απενεργοποιείται.	Εισαγάγετε το ακόλουθο PIN '**47867243**' και πατήστε το **Πλήκτρο** (🔑) μία φορά, με τις ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED να αναβοσβήνουν εναλλάξ και να σβήνουν, το diskAshur M² είναι έτοιμο να δεχτεί άλλες **2 καταχωρήσεις PIN** διαχειριστή
10	Το ΚΟΚΚΙΝΟ LED θα ανάψει και θα γίνει σταθερό.	Μετά από συνολικά 10 λανθασμένες καταχωρήσεις PIN διαχειριστή, το κλειδί κρυπτογράφησης, όλα τα PIN και τα δεδομένα θα διαγραφούν και θα χαθούν για πάντα.

33. Τρόπος ορισμού του περιορισμού ωμής βίας PIN χρήστη

Σημείωση: Η ρύθμιση περιορισμού ωμής βίας PIN χρήστη είναι προεπιλεγμένη σε 10 διαδοχικές εσφαλμένες καταχωρήσεις PIN όταν γίνεται πλήρης επαναφορά της μονάδας δίσκου, αναγκαστική βία ή ενεργοποιείται το PIN αυτοκαταστροφής.

Ο περιορισμός ωμής δύναμης για το diskAshur M2 User PIN μπορεί να επαναπρογραμματιστεί και να οριστεί από το διαχειριστή. Αυτή η λειτουργία μπορεί να ρυθμιστεί ώστε να επιτρέπει προσπάθειες από 1 έως 10 διαδοχικές εσφαλμένες καταχωρήσεις PIN.

Για να ρυθμίσετε τον περιορισμό ωμής βίας του PIN χρήστη, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε παρατεταμένα και τα δύο **7 + 0** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε πράσινες και μπλε λυχνίες LED που αναβοσβήνουν μαζί
2. Εισαγάγετε τον αριθμό των προσπαθειών για τον περιορισμό της ωμής βίας (μεταξύ 01-10), για παράδειγμα πληκτρολογήστε: • **01** για 1 προσπάθεια • **10** για 10 προσπάθειες		
3. Πατήστε το κουμπί **ΒΑΡΔΙΑ** (🡅) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED θα μεταβούν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED για ένα δευτερόλεπτο και στη συνέχεια σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει ότι ο περιορισμός ωμής δύναμης διαμορφώθηκε με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

34. Πώς να ελέγξετε τον περιορισμό ωμής βίας PIN χρήστη

Ο Διαχειριστής είναι σε θέση να παρατηρήσει και να καθορίσει τον αριθμό των διαδοχικών φορών που επιτρέπεται να εισαχθεί εσφαλμένο PIN χρήστη πριν ενεργοποιήσει τον αμυντικό μηχανισμό Brute Force σημειώνοντας απλώς την ακολουθία LED όπως περιγράφεται παρακάτω.

Για να ελέγξετε τη ρύθμιση περιορισμού ωμής βίας, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **2 + 0** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πατήστε το κουμπί **Πλήκτρο** (ð) και συμβαίνουν τα εξής.		
a. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.		
b. Κάθε ΚΟΚΚΙΝΟ LED αναβοσβήνει ισοδυναμεί με δέκα (10) μονάδες ενός αριθμού περιορισμού ωμής βίας.		
c. Κάθε ΠΡΑΣΙΝΗ λυχνία LED που αναβοσβήνει ισοδυναμεί με μία (1) ενιαία μονάδα ενός αριθμού περιορισμού ωμής δύναμης.		
d. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.		
e. Οι λυχνίες LED επιστρέφουν στο συμπαγές ΜΠΛΕ		

Ο παρακάτω πίνακας περιγράφει τη συμπεριφορά LED κατά τον έλεγχο της ρύθμισης περιορισμού ωμής δύναμης, για παράδειγμα εάν έχετε ρυθμίσει τη μονάδα δίσκου σε ωμή δύναμη μετά από **5** διαδοχικές λανθασμένες καταχωρήσεις PIN, η ΠΡΑΣΙΝΗ λυχνία LED θα αναβοσβήσει πέντε (**5**) φορές.

Ρύθμιση περιορισμού ωμής βίας	**ΚΟΚΚΙΝΟΣ**	**ΠΡΑΣΙΝΟΣ**
2 attempts	0	2 αναβοσβήνει
5 attempts	0	5 αναβοσβήνει
10 attempts	1 Αναβοσβήνει	0

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (⬆) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

35. Πώς να εκτελέσετε μια πλήρη επαναφορά

Για να εκτελέσετε πλήρη επαναφορά, ο diskAshur M² πρέπει να βρίσκεται σε κατάσταση αναμονής (στερεά κόκκινη λυχνία LED). Μόλις γίνει επαναφορά της μονάδας δίσκου, τότε όλα

Τα PIN διαχειριστή/χρήστη, το κλειδί κρυπτογράφησης και όλα τα δεδομένα θα διαγραφούν και θα χαθούν για πάντα και η μονάδα δίσκου θα πρέπει να μορφοποιηθεί για να μπορέσει να επαναχρησιμοποιηθεί. Για να επαναφέρετε το diskAshur M², ακολουθήστε τα παρακάτω βήματα.

1. Σε κατάσταση αναμονής (στερεά κόκκινη λυχνία), πατήστε και κρατήστε πατημένο το κουμπί "**0**"		Το συμπαγές κόκκινο LED θα αλλάξει σε όλα τα LED, το κόκκινο, το πράσινο και το μπλε αναβοσβήνουν εναλλάξ και σβήνουν
2. Πατήστε και κρατήστε πατημένα και τα δύο κουμπιά **2 + 7**		Οι εναλλασσόμενες λυχνίες LED κόκκινο, ΠΡΑΣΙΝΕΣ και ΜΠΛΕ θα γίνουν σταθερές για ένα δευτερόλεπτο και στη συνέχεια σε μια σταθερή κόκκινη λυχνία LED που υποδεικνύει ότι η μονάδα δίσκου έχει μηδενιστεί

Σημαντικό: Μετά από μια πλήρη επαναφορά πρέπει να ρυθμιστεί ένα νέο PIN διαχειριστή, ανατρέξτε στην Ενότητα 25 στη σελίδα 19 σχετικά με τον «Τρόπο διαμόρφωσης ενός PIN διαχειριστή μετά από επίθεση ή επαναφορά ωμής βίας», ο diskAshur M² θα πρέπει επίσης να είναι Έχει διαμορφωθεί πριν από την προσθήκη νέων δεδομένων στη μονάδα δίσκου.

36. Πώς να ρυθμίσετε το diskAshur M² ως Bootable

Σημείωση: Όταν η μονάδα έχει οριστεί ως εκκινήσιμη, η εξαγωγή της μονάδας δίσκου από το λειτουργικό σύστημα δεν θα αναγκάσει τη λυχνία LED να γίνει κόκκινη. Ο δίσκος παραμένει σταθερός ΠΡΑΣΙΝΟΣ και πρέπει να αποσυνδεθεί από την πρίζα για την επόμενη χρήση. Η προεπιλεγμένη ρύθμιση του diskAshur M² έχει ρυθμιστεί ως μη εκκινήσιμη.

Ο diskAshur M² είναι εξοπλισμένος με μια δυνατότητα εκκίνησης για να φιλοξενήσει τον κύκλο ισχύος κατά τη διάρκεια μιας διαδικασίας εκκίνησης κεντρικού υπολογιστή. Κατά την εκκίνηση από το diskAshur M², εκτελείτε τον υπολογιστή σας με το λειτουργικό σύστημα που είναι εγκατεστημένο στο diskAshur M².

Για να ορίσετε τη μονάδα δίσκου ως εκκινήσιμη, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (⚷) + **8** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πατήστε "**0**" ακολουθούμενο από ένα "**1**" (**01**)		Οι πράσινες και μπλε λυχνίες LED θα συνεχίσουν να αναβοσβήνουν
3. Πατήστε το κουμπί **ΒΑΡΔΙΑ** (🡅) μία φορά		Αναβοσβήνοντας ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED θα αλλάξουν σε μια σταθερή ΠΡΑΣΙΝΗ λυχνία LED και τελικά σε μια σταθερή ΜΠΛΕ λυχνία LED που υποδεικνύει

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

37. Πώς να απενεργοποιήσετε το diskAshur M² Δυνατότητα εκκίνησης

Για να απενεργοποιήσετε τη λειτουργία εκκίνησης diskAshur M² , εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα

1.Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **Πλήκτρο** (ⓚ) + **8** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν
2. Πατήστε "**0**" ακολουθούμενο από ένα άλλο "**0**" (**00**)		Οι πράσινες και μπλε λυχνίες LED θα συνεχίσουν να αναβοσβήνουν
3. Πατήστε το κουμπί **ΒΑΡΔΙΑ** (🡅) μία φορά		Αναβοσβήνοντας τα κόκκινη και μπλε LED θα αλλάξουν σε ένα συμπαγές ΠΡΑΣΙΝΟ LED και τελικά σε ένα συμπαγές ΜΠΛΕ LED που υποδεικνύει ότι η λειτουργία εκκίνησης έχει απενεργοποιηθεί με επιτυχία

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

38. Πώς να ελέγξετε τη ρύθμιση Bootable

Για να ελέγξετε τη ρύθμιση εκκίνησης, εισαγάγετε πρώτα τη "**Λειτουργία διαχειριστή**" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία διαχειριστή** (συμπαγές μπλε LED), ακολουθήστε τα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο **ΒΑΡΔΙΑ** (🡅) + **8** κουμπιά		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν

2. Πατήστε το κουμπί **Πλήκτρο** (ⓚ) και θα συμβεί ένα από τα ακόλουθα δύο σενάρια.

- **Εάν το diskAshur M² έχει ρυθμιστεί ως Bootable, συμβαίνουν τα εξής.**

a. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
b. Η ΠΡΑΣΙΝΗ λυχνία LED αναβοσβήνει μία φορά.
c. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
d. Οι λυχνίες LED επιστρέφουν στο συμπαγές ΜΠΛΕ

- **Εάν το diskAshur M² ΔΕΝ έχει ρυθμιστεί ως Bootable, συμβαίνουν τα εξής.**

a. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
b. Όλες οι λυχνίες LED είναι σβηστές
c. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ γίνονται σταθερά για 1 δευτερόλεπτο.
d. Οι λυχνίες LED επιστρέφουν στο συμπαγές ΜΠΛΕ

Σημείωση: Για άμεση έξοδο από τη λειτουργία διαχειριστή (στερεό ΜΠΛΕ LED), πατήστε και κρατήστε πατημένο το κουμπί **ΒΑΡΔΙΑ** (🡅) κουμπί για ένα δευτερόλεπτο- το στερεό ΜΠΛΕ Η λυχνία LED αλλάζει σε στερεό ΚΟΚΚΙΝΟΣ ΟΔΗΓΗΜΕΝΟΣ

39. Αρχικοποίηση και διαμόρφωση diskAshur M² για Windows

Μετά από μια «Brute Force Attack» ή μια πλήρη επαναφορά, το diskAshur M² θα διαγράψει όλα τα PIN, τα δεδομένα και το κλειδί κρυπτογράφησης. Θα χρειαστεί να αρχικοποιήσετε και να διαμορφώσετε το diskAshur M² για να μπορέσετε να το χρησιμοποιήσετε.

Για να διαμορφώσετε το δίσκο diskAshur M², κάντε τα εξής

1. Διαμορφώστε ένα νέο PIN διαχειριστή- δείτε τη σελίδα 19, ενότητα 25, «Πώς να ρυθμίσετε ένα PIN διαχειριστή μετά από επίθεση ή επαναφορά ωμής βίας».

2. Με το diskAshur M² σε κατάσταση αναμονής (κόκκινη LED), πατήστε το κουμπί **Πλήκτρο** (ⓚ) μία φορά και πληκτρολογήστε New AdminPIN για ξεκλείδωμα (αναβοσβήνει πράσινες LED).

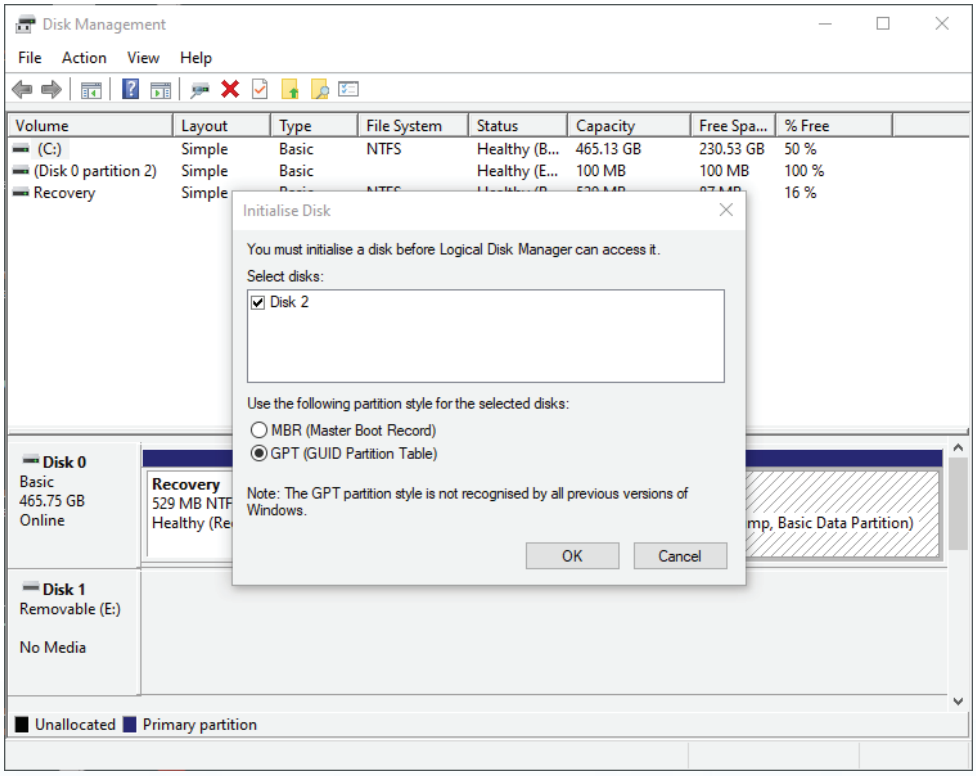
3. Συνδέστε το diskAshur M² στον υπολογιστή.

4. **Windows 7**: Κάντε δεξί κλικ στην **επιλογή Υπολογιστής** και, στη συνέχεια, κάντε κλικ στην επιλογή **Διαχείριση και**, στη συνέχεια, επιλέξτε **Διαχείριση δίσκων**

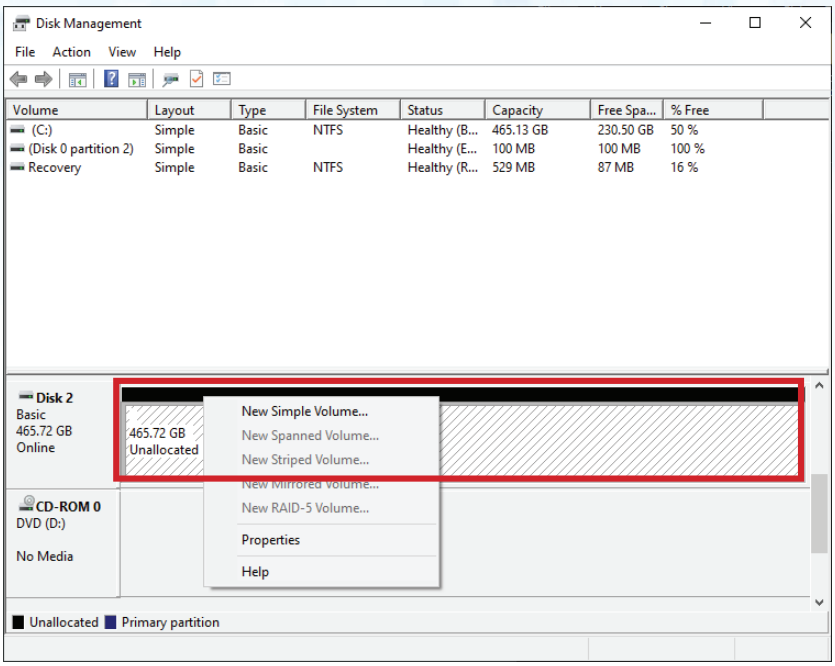
   Windows 8: Κάντε δεξί κλικ στην αριστερή γωνία της επιφάνειας εργασίας και επιλέξτε **Διαχείριση δίσκων**

   Windows 10: Κάντε δεξί κλικ στο κουμπί έναρξης και επιλέξτε **Διαχείριση δίσκων**

5. Στο παράθυρο Διαχείριση δίσκων (Disk Management), το diskAshur M² αναγνωρίζεται ως μια άγνωστη συσκευή που δεν έχει προετοιμαστεί και δεν έχει εκχωρηθεί. Θα πρέπει να εμφανιστεί ένα πλαίσιο μηνύματος για να επιλέξετε μεταξύ στυλ διαμερίσματος MBR και GPT. Το GPT αποθηκεύει πολλαπλά διπλότυπα αυτών των δεδομένων πάνω στο δίσκο, ως αποτέλεσμα είναι πολύ πιο ισχυρό. Σε ένα δίσκο MBR, οι πληροφορίες διαμέρισης και εκκίνησης αποθηκεύονται μέσα σε ένα μόνο μέρος Επιλέξτε το στυλ διαμερίσματος και κάντε κλικ στο **OK**.



6. Κάντε δεξιό κλικ στην κενή περιοχή πάνω από την **ενότητα Μη εκχωρημένο** και, στη συνέχεια, επιλέξτε **Νέος απλός τόμος**.



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



8. Εάν χρειάζεστε μόνο ένα διαμέρισμα, αποδεχτείτε το προεπιλεγμένο μέγεθος διαμερίσματος και κάντε κλικ στο κουμπί **Επόμενο**.

9. Αντιστοιχίστε ένα γράμμα μονάδας δίσκου ή μια διαδρομή και κάντε κλικ στο κουμπί Επόμενο.

10. Δημιουργία ετικέτας τόμου, επιλέξτε Εκτέλεση γρήγορης διαμόρφωσης και, στη συνέχεια, κάντε κλικ στο κουμπί Επόμενο.

11. Κάντε κλικ στο κουμπί **Τέλος**.

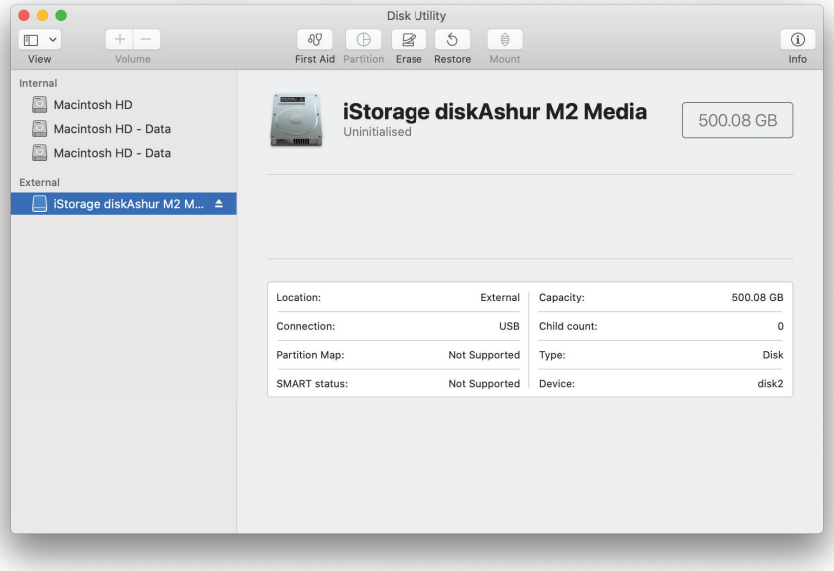
12. Περιμένετε μέχρι να ολοκληρωθεί η διαδικασία διαμόρφωσης. Ο diskAshur M² θα αναγνωριστεί και είναι διαθέσιμος για χρήση.

40. Αρχικοποίηση και διαμόρφωση diskAshur M² σε Mac OS

Μετά από μια «Brute Force Attack» ή μια πλήρη επαναφορά, το diskAshur M² θα διαγράψει όλα τα PIN, τα δεδομένα και το κλειδί κρυπτογράφησης. Θα χρειαστεί να αρχικοποιήσετε και να διαμορφώσετε το diskAshur M² για να μπορέσετε να το χρησιμοποιήσετε.

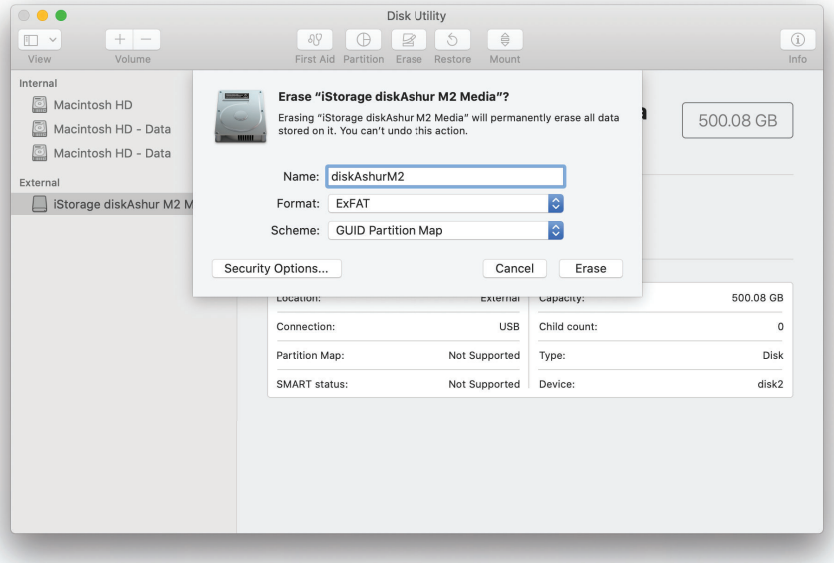
Για να αρχικοποιήσετε και να διαμορφώσετε το diskAshur M²:

1. Επιλέξτε diskAshur M² από τη λίστα μονάδων δίσκου και τόμων. Κάθε μονάδα δίσκου στη λίστα θα εμφανίζει τη χωρητικότητά της, τον κατασκευαστή και το όνομα προϊόντος, όπως "**iStorage diskAshur M² Media**".

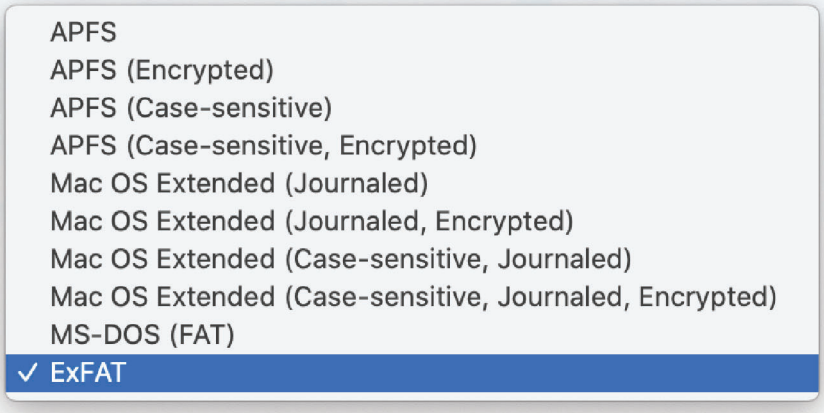


2. Κάντε κλικ στο κουμπί '**Διαγραφή**' κάτω από το Disk Utility.

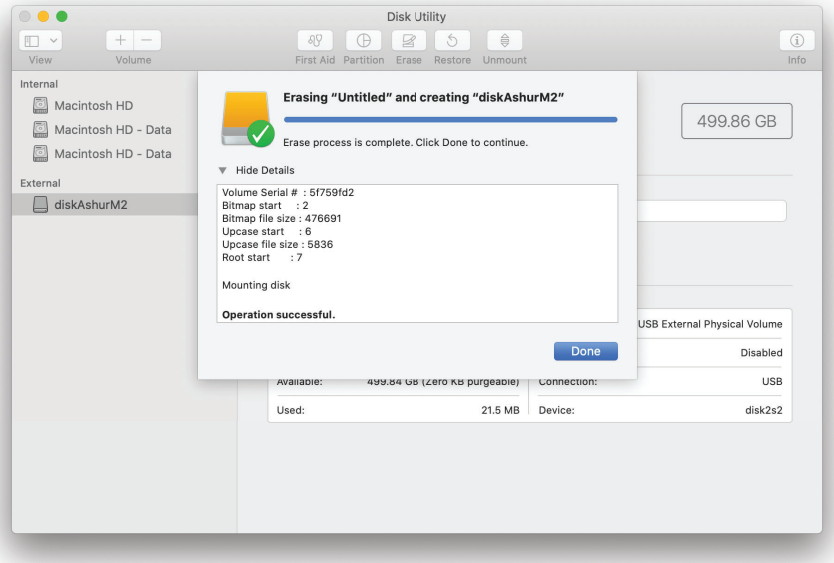
3. Εισαγάγετε ένα όνομα για τη μονάδα δίσκου. Το προεπιλεγμένο όνομα είναι Χωρίς τίτλο. Το όνομα της μονάδας δίσκου θα εμφανιστεί τελικά στην επιφάνεια εργασίας.



4. Επιλέξτε ένα σχήμα και μια μορφή τόμου για χρήση. ο Μορφή έντασης αναπτυσσόμενο μενού παραθέτει τις διαθέσιμες μορφές μονάδας δίσκου που υποστηρίζει το Mac. Ο προτεινόμενος τύπος μορφής είναι “Mac OS Extended (Journaled)”. Για cross-platform χρησιμοποιήστε το exFAT. Το αναπτυσσόμενο μενού μορφής συνδυασμού παραθέτει τους διαθέσιμους συνδυασμούς για χρήση. Συνιστούμε τη χρήση του “GUID Partition Map” σε μονάδες δίσκου μεγαλύτερες από 2TB.

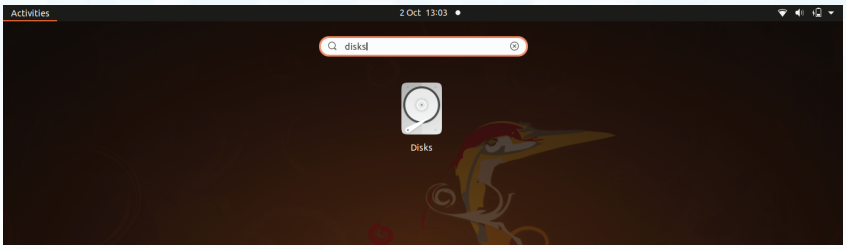


5. Κάντε κλικ στο κουμπί ‘Διαγραφή’. Το Βοήθημα δίσκων θα απομονώσει τον τόμο από την επιφάνεια εργασίας, θα τον διαγράψει και, στη συνέχεια, θα τον προσαρτήσει ξανά στην επιφάνεια εργασίας.

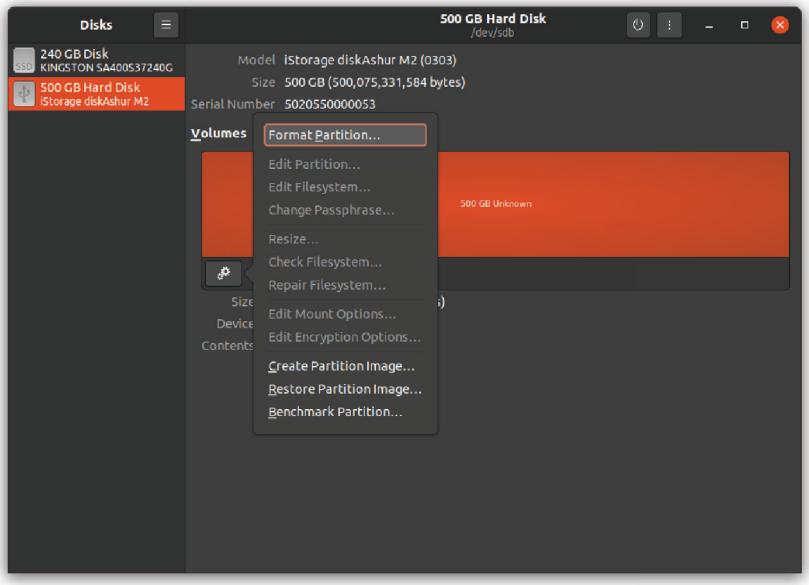


41. Αρχικοποίηση και διαμόρφωση diskAshur M² σε λειτουργικό σύστημα Linux

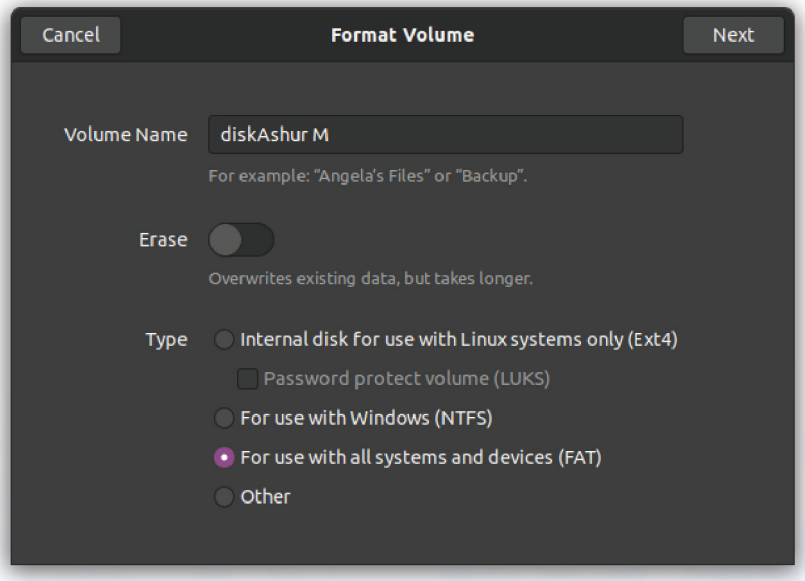
1. Ανοίξτε το "**Εμφάνιση εφαρμογής**" και πληκτρολογήστε "**Δίσκοι**" στο πλαίσιο αναζήτησης. Κάντε κλικ στο **βοηθητικό**



2. Κάντε κλικ για να επιλέξετε τη μονάδα δίσκου (σκληρός δίσκος 500 GB) στην ενότητα '**Συσκευές**'. Στη συνέχεια, κάντε κλικ στο εικονίδιο με τα γρανάζια κάτω από το '**Volumes**' και, στη συνέχεια, κάντε κλικ στο '**Format Partitons**'

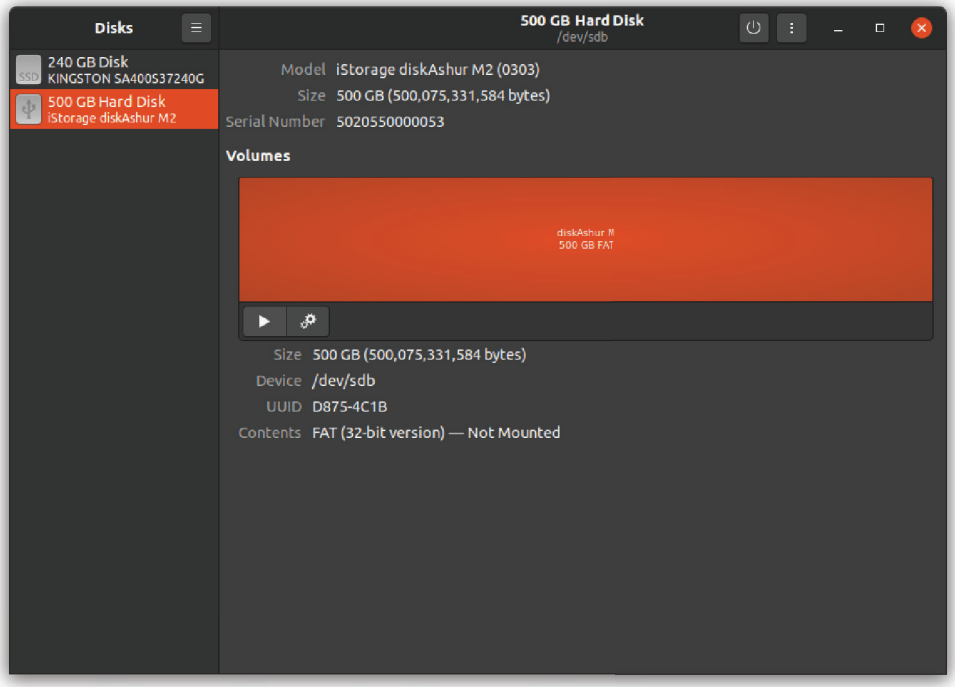


3. Επιλέξτε «**Συμβατό με όλα τα συστήματα και συσκευές (FAT)**» για την επιλογή «**Τύπος**». Και εισαγάγετε ένα όνομα για τη μονάδα δίσκου, π.χ.: diskAshur M². Στη συνέχεια, κάντε κλικ στο κουμπί 'Μορφοποίηση'.

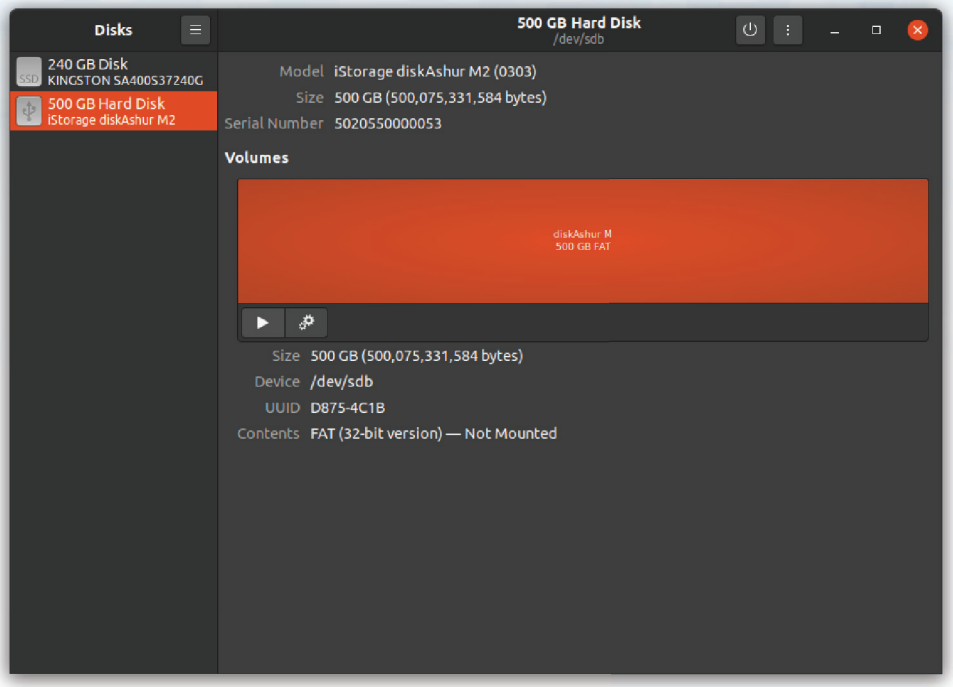




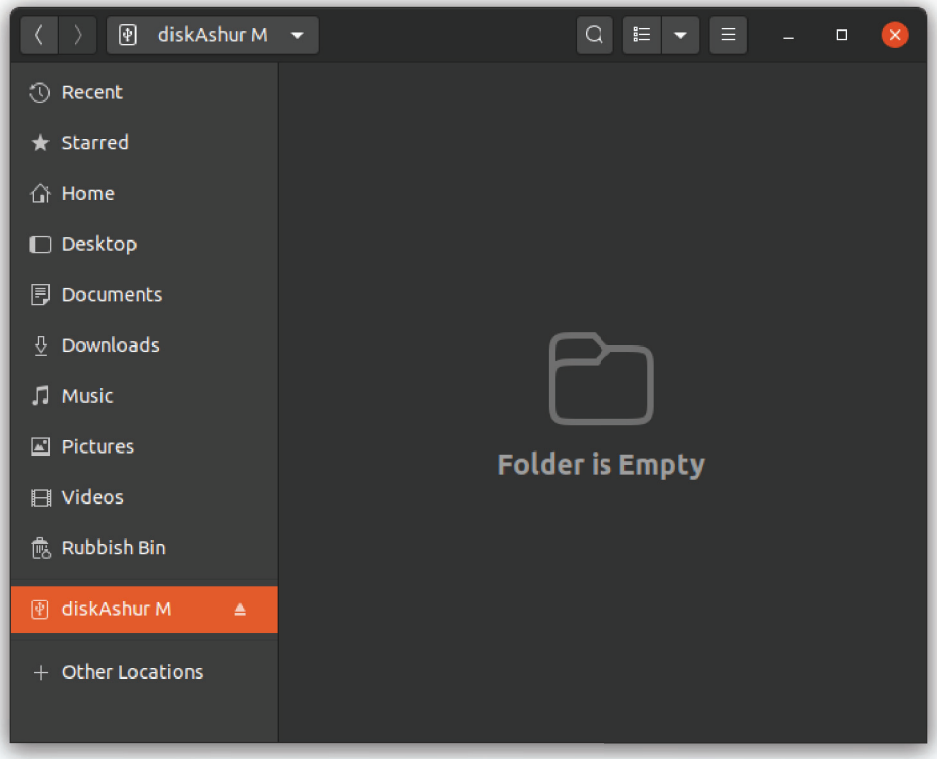
4. Αφού ολοκληρωθεί η διαδικασία μορφοποίησης, κάντε κλικ στο κουμπί Αναπαραγωγή για να προσαρτήσετε τη μονάδα δίσκου στο Ubuntu



5. Τώρα η μονάδα δίσκου θα πρέπει να τοποθετηθεί στο Ubuntu και να είναι έτοιμη για χρήση.



6. Ο δίσκος θα εμφανιστεί όπως φαίνεται στην παρακάτω εικόνα. Μπορείτε να κάνετε κλικ στο εικονίδιο του δίσκου για να ανοίξετε τη μονάδα δίσκου σας.



42. Αδρανοποίηση, αναστολή ή αποσύνδεση από το λειτουργικό σύστημα

Βεβαιωθείτε ότι έχετε αποθηκεύσει και κλείσει όλα τα αρχεία στο δίσκο diskAshur M² πριν από την αδρανοποίηση, την αναστολή ή την αποσύνδεση από το λειτουργικό σύστημα.

Συνιστάται να κλειδώσετε το diskAshur M² με μη αυτόματο τρόπο πριν από την αδρανοποίηση, την αναστολή ή την αποσύνδεση από το σύστημά σας.

Για να κλειδώσετε τη μονάδα δίσκου, αφαιρέστε με ασφάλεια το diskAshur M² από το λειτουργικό σύστημα κεντρικού υπολογιστή και, στη συνέχεια, αποσυνδέστε το από τη θύρα USB. Εάν εγγράφονται δεδομένα στη μονάδα δίσκου, η αποσύνδεση του diskAshur M² θα έχει ως αποτέλεσμα την ελλιπή μεταφορά δεδομένων και πιθανή καταστροφή δεδομένων.

⚠ Προσοχή: Για να διασφαλίσετε ότι τα δεδομένα σας είναι ασφαλή, φροντίστε να κλειδώσετε το δίσκο diskAshur M² εάν βρίσκεστε μακριά από τον υπολογιστή σας.

43. Πώς να ελέγξετε το υλικολογισμικό σε λειτουργία διαχειριστή

Για να ελέγξετε τον αριθμό αναθεώρησης υλικολογισμικού, εισαγάγετε πρώτα τη "Λειτουργία διαχειριστή" όπως περιγράφεται στην ενότητα 5. Μόλις η μονάδα δίσκου βρίσκεται σε λειτουργία διαχειριστή (συμπαγές BLUE LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία διαχειριστή, πατήστε και κρατήστε πατημένα και τα δύο κουμπιά "**3 + 8**"		Η συμπαγής μπλε λυχνία LED θα αλλάξει σε ΠΡΑΣΙΝΕΣ και ΜΠΛΕ λυχνίες LED που αναβοσβήνουν

2. Πατήστε το κουμπί **Πλήκτρο** (⚷) μία φορά και συμβαίνουν τα εξής.

a. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
b. Η λυχνία LED ΚΟΚΚΙΝΟ αναβοσβήνει υποδεικνύοντας το αναπόσπαστο μέρος του αριθμού αναθεώρησης υλικολογισμικού.
c. Η ΠΡΑΣΙΝΗ λυχνία LED αναβοσβήνει υποδεικνύοντας το κλασματικό τμήμα.
d ΜΠΛΕ LED αναβοσβήνει υποδεικνύοντας το τελευταίο ψηφίο του αριθμού αναθεώρησης υλικολογισμικού
e. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
f. Τα ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ LED αλλάζουν σε ένα συμπαγές μπλε LED

Για παράδειγμα, εάν ο αριθμός αναθεώρησης υλικολογισμικού είναι «**2.3**», η ΚΟΚΚΙΝΗ λυχνία LED θα αναβοσβήσει δύο (**2**) φορές και η ΠΡΑΣΙΝΗ λυχνία LED θα αναβοσβήσει τρεις (**3**) φορές. Μόλις τελειώσει η ακολουθία, τα ΚΟΚΚΙΝΟ, τα ΠΡΑΣΙΝΗ & ΜΠΛΕ LED θα αναβοσβήνουν μαζί μία φορά και στη συνέχεια θα επιστρέψουν στη λειτουργία Admin, ένα συμπαγές ΜΠΛΕ LED.

44. Πώς να ελέγξετε το υλικολογισμικό στη λειτουργία χρήστη

Για να ελέγξετε τον αριθμό αναθεώρησης υλικολογισμικού, εισαγάγετε πρώτα τη «**Λειτουργία χρήστη**» όπως περιγράφεται στην ενότητα 13. Μόλις η μονάδα δίσκου βρίσκεται σε **λειτουργία χρήστη** (συμπαγές ΠΡΑΣΙΝΟ LED) προχωρήστε στα παρακάτω βήματα.

1. Στη λειτουργία χρήστη πατήστε και κρατήστε πατημένα και τα δύο κουμπιά "**3 + 8**" έως ότου αναβοσβήνουν μαζί οι πράσινες και μπλε λυχνίες LED		Solid GREEN LED will change to blinking GREEN and BLUE LEDs

2. Πατήστε το κουμπί **Πλήκτρο** (🔑) μία φορά και συμβαίνουν τα εξής.

a. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
b. Η λυχνία LED ΚΟΚΚΙΝΟ αναβοσβήνει υποδεικνύοντας το αναπόσπαστο μέρος του αριθμού αναθεώρησης υλικολογισμικού.
c. Η ΠΡΑΣΙΝΗ λυχνία LED αναβοσβήνει υποδεικνύοντας το κλασματικό τμήμα.
d ΜΠΛΕ LED αναβοσβήνει υποδεικνύοντας το τελευταίο ψηφίο του αριθμού αναθεώρησης υλικολογισμικού
e. Όλα τα LED (ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ) γίνονται σταθερά για 1 δευτερόλεπτο.
f. Τα ΚΟΚΚΙΝΟ, ΠΡΑΣΙΝΗ & ΜΠΛΕ LED αλλάζουν σε ένα συμπαγές ΠΡΑΣΙΝΗ LED

Για παράδειγμα, εάν ο αριθμός αναθεώρησης υλικολογισμικού είναι «**2.3**», η ΚΟΚΚΙΝΗ λυχνία LED θα αναβοσβήσει δύο (**2**) φορές και η ΠΡΑΣΙΝΗ λυχνία LED θα αναβοσβήσει τρεις (**3**) φορές. Μόλις τελειώσει η ακολουθία, τα ΚΟΚΚΙΝΟ, τα ΠΡΑΣΙΝΗ & ΜΠΛΕ LED θα αναβοσβήνουν μαζί μία φορά και στη συνέχεια θα επιστρέψουν στη λειτουργία Admin, ένα συμπαγές ΜΠΛΕ LED.

45. Τεχνική Υποστήριξη

Το iStorage παρέχει τους παρακάτω χρήσιμους πόρους για εσάς:

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

Υποστήριξη μέσω e-mail:
support@istorage-uk.com

Τηλεφωνική υποστήριξη:
+44 (0) 20 8991-6260.

Οι ειδικοί τεχνικής υποστήριξης iStorage είναι διαθέσιμοι από τις 9:00 π.μ. έως τις 5:30 μ.μ. GMT- Δευτέρα έως Παρασκευή.

46. Πληροφορίες εγγύησης και RMA

ΑΠΟΠΟΙΗΣΗ ΠΡΟΪΟΝΤΟΣ ISTORAGE ΚΑΙ ΕΓΓΥΗΣΗ

Η iStorage εγγυάται ότι κατά την παράδοση και για περίοδο 36 μηνών από την παράδοση, τα Προϊόντα της θα είναι απαλλαγμένα από ελαττώματα υλικού. Ωστόσο, αυτή η εγγύηση δεν ισχύει στις περιπτώσεις που περιγράφονται παρακάτω. Η iStorage εγγυάται ότι τα Προϊόντα συμμορφώνονται με τα πρότυπα που αναφέρονται στο σχετικό φύλλο δεδομένων στον ιστότοπό μας τη στιγμή που κάνετε την παραγγελία σας.
Αυτές οι εγγυήσεις δεν ισχύουν για οποιοδήποτε ελάττωμα στα Προϊόντα που προκύπτει από:

- δίκαιη φθορά ·
- εσκεμμένη ζημιά, μη φυσιολογικές συνθήκες αποθήκευσης ή εργασίας, ατύχημα, αμέλεια από εσάς ή από οποιοδήποτε τρίτο μέρος.
- εάν εσείς ή ένα τρίτο μέρος αποτύχετε να λειτουργήσετε ή να χρησιμοποιήσετε τα Προϊόντα σύμφωνα με τις οδηγίες χρήσης,
- οποιαδήποτε αλλαγή ή επισκευή από εσάς ή από τρίτο μέρος που δεν είναι ένας από τους εξουσιοδοτημένους επισκευαστές μας, ή
- οποιαδήποτε προδιαγραφή παρέχεται από εσάς. Σύμφωνα με αυτές τις εγγυήσεις, κατά την επιλογή μας, είτε θα επισκευάσουμε, θα αντικαταστήσουμε ή θα σας επιστρέψουμε τα χρήματα για τυχόν Προϊόντα που βρέθηκαν να έχουν ουσιώδη ελαττώματα, υπό την προϋπόθεση ότι κατά την παράδοση:
- επιθεωρείτε τα Προϊόντα για να ελέγξετε εάν έχουν ελαττώματα υλικού, και
- δοκιμάζετε το μηχανισμό κρυπτογράφησης στα Προϊόντα.

Δεν θα είμαστε υπεύθυνοι για τυχόν ουσιώδη ελαττώματα ή ελαττώματα στον μηχανισμό κρυπτογράφησης των Προϊόντων που μπορούν να εξακριβωθούν κατά την επιθεώρηση κατά την παράδοση, εκτός εάν μας γνωστοποιήσετε τέτοια ελαττώματα εντός 30 ημερών από την παράδοση. Δεν θα είμαστε υπεύθυνοι για τυχόν ουσιώδη ελαττώματα ή ελαττώματα στον μηχανισμό κρυπτογράφησης των Προϊόντων, τα οποία δεν είναι αναγνωρίσιμα κατά την επιθεώρηση κατά την παράδοση, εκτός εάν μας γνωστοποιήσετε τέτοια ελαττώματα εντός 7 ημερών από τη στιγμή που ανακαλύπτετε ή θα έπρεπε να έχετε αντιληφθεί τέτοια ελαττώματα. Δεν θα είμαστε υπεύθυνοι βάσει αυτών των εγγυήσεων εάν κάνετε εσείς ή οποιοσδήποτε άλλος κάνει οποιαδήποτε περαιτέρω χρήση των Προϊόντων μετά την ανακάλυψη ενός ελαττώματος. Με την κοινοποίηση οποιουδήποτε ελαττώματος, θα πρέπει να μας επιστρέψετε το ελαττωματικό προϊόν. Εάν είστε επιχείρηση, θα είστε υπεύθυνοι για τα έξοδα μεταφοράς που προκύπτουν από την αποστολή οποιωνδήποτε Προϊόντων ή τμημάτων των Προϊόντων σε εμάς βάσει της εγγύησης και θα είμαστε υπεύθυνοι για τυχόν έξοδα μεταφοράς που προκύπτουν κατά την αποστολή ενός επισκευασμένου ή αντικατασταθέντος Προϊόντος. Εάν είστε καταναλωτής, ανατρέξτε στους όρους και τις προϋποθέσεις μας.
Τα προϊόντα που επιστρέφονται πρέπει να είναι στην αρχική τους συσκευασία και σε καθαρή κατάσταση. Τα προϊόντα που επιστρέφονται διαφορετικά θα απορρίπτονται, κατά την κρίση της Εταιρείας, είτε θα απορρίπτονται είτε θα χρεώνεται περαιτέρω πρόσθετη χρέωση για την κάλυψη του πρόσθετου κόστους που συνεπάγεται. Τα προϊόντα που επιστρέφονται για επισκευή βάσει εγγύησης πρέπει να συνοδεύονται από αντίγραφο του πρωτότυπου τιμολογίου ή πρέπει να αναφέρουν τον αρχικό αριθμό τιμολογίου και την ημερομηνία αγοράς.
Εάν είστε καταναλωτής, αυτή η εγγύηση είναι επιπλέον των νόμιμων δικαιωμάτων σας σε σχέση με Προϊόντα που είναι ελαττωματικά ή δεν είναι όπως περιγράφονται. Συμβουλές σχετικά με τα νόμιμα δικαιώματά σας διατίθενται από το τοπικό γραφείο παροχής συμβουλών στους πολίτες ή το γραφείο εμπορικών προτύπων.
Οι εγγυήσεις που ορίζονται στην παρούσα ρήτρα ισχύουν μόνο για τον αρχικό αγοραστή ενός Προϊόντος από την iStorage ή έναν εξουσιοδοτημένο μεταπωλητή ή διανομέα της iStorage. Αυτές οι εγγυήσεις δεν μεταβιβάζονται.
ΕΚΤΟΣ ΑΠΟ ΤΗΝ ΠΕΡΙΟΡΙΣΜΕΝΗ ΕΓΓΥΗΣΗ ΠΟΥ ΠΑΡΕΧΕΤΑΙ ΣΤΟ ΠΑΡΟΝ ΚΑΙ ΣΤΟ ΒΑΘΜΟ ΠΟΥ ΕΠΙΤΡΕΠΕΤΑΙ ΑΠΟ ΤΟ ΝΟΜΟ, Η ISTORAGE ΑΠΟΠΟΙΕΙΤΑΙ ΟΛΕΣ ΤΙΣ ΕΓΓΥΗΣΕΙΣ, ΡΗΤΕΣ Η ΣΙΩΠΗΡΕΣ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ ΟΛΩΝ ΤΩΝ ΕΓΓΥΗΣΕΩΝ ΕΜΠΟΡΕΥΣΙΜΟΤΗΤΑΣ. ΚΑΤΑΛΛΗΛΟΤΗΤΑ ΓΙΑ ΣΥΓΚΕΚΡΙΜΕΝΟ ΣΚΟΠΟ, ΜΗ ΠΡΟΣΒΟΛΗ. Η ISTORAGE ΔΕΝ ΕΓΓΥΑΤΑΙ ΟΤΙ ΤΟ ΠΡΟΪΟΝ ΘΑ ΛΕΙΤΟΥΡΓΕΙ ΧΩΡΙΣ ΣΦΑΛΜΑΤΑ. ΣΤΟ ΒΑΘΜΟ ΟΤΙ ΟΠΟΙΕΣΔΗΠΟΤΕ ΣΙΩΠΗΡΕΣ ΕΓΓΥΗΣΕΙΣ ΕΝΔΕΧΕΤΑΙ ΠΑΡ' ΟΤΙ ΝΑ ΥΠΑΡΧΟΥΝ ΑΠΟ ΤΟ ΝΟΜΟ, ΟΠΟΙΕΣΔΗΠΟΤΕ ΤΕΤΟΙΕΣ ΕΓΓΥΗΣΕΙΣ ΠΕΡΙΟΡΙΖΟΝΤΑΙ ΣΤΗ ΔΙΑΡΚΕΙΑ ΤΗΣ ΠΑΡΟΥΣΑΣ ΕΓΓΥΗΣΗΣ. Η ΕΠΙΣΚΕΥΗ Η ΑΝΤΙΚΑΤΑΣΤΑΣΗ ΑΥΤΟΥ ΤΟΥ ΠΡΟΪΟΝΤΟΣ, ΟΠΩΣ ΠΡΟΒΛΕΠΕΤΑΙ ΣΤΟ ΠΑΡΟΝ, ΕΙΝΑΙ Η ΑΠΟΚΛΕΙΣΤΙΚΗ ΣΑΣ ΑΠΟΖΗΜΙΩΣΗ.
ΣΕ ΚΑΜΙΑ ΠΕΡΙΠΤΩΣΗ Η ISTORAGE ΔΕΝ ΦΕΡΕΙ ΕΥΘΥΝΗ ΓΙΑ ΟΠΟΙΑΔΗΠΟΤΕ ΑΠΩΛΕΙΑ Η ΑΝΑΜΕΝΟΜΕΝΑ ΚΕΡΔΗ Η ΟΠΟΙΑΔΗΠΟΤΕ ΤΥΧΑΙΑ, ΠΟΙΝΙΚΗ, ΠΑΡΑΔΕΙΓΜΑΤΙΚΗ, ΕΙΔΙΚΗ, ΒΑΣΙΚΗ Η ΕΠΑΚΟΛΟΥΘΗ ΖΗΜΙΑ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΩΝ, ΕΝΔΕΙΚΤΙΚΑ, ΑΠΩΛΕΙΑΣ ΕΣΟΔΩΝ, ΔΙΑΦΥΓΟΝΤΩΝ ΚΕΡΔΩΝ, ΑΠΩΛΕΙΑΣ ΧΡΗΣΗΣ ΛΟΓΙΣΜΙΚΟΥ, ΑΠΩΛΕΙΑΣ ΔΕΔΟΜΕΝΩΝ, ΑΛΛΗΣ ΑΠΩΛΕΙΑΣ Η ΑΝΑΚΤΗΣΗΣ ΔΕΔΟΜΕΝΩΝ, ΖΗΜΙΑΣ ΣΕ ΙΔΙΟΚΤΗΣΙΑ ΚΑΙ ΑΞΙΩΣΕΩΝ ΤΡΙΤΩΝ, ΠΟΥ ΠΡΟΚΥΠΤΟΥΝ ΑΠΟ ΟΠΟΙΑΔΗΠΟΤΕ ΘΕΩΡΙΑ ΑΝΑΚΤΗΣΗΣ, ΣΥΜΠΕΡΙΛΑΜΒΑΝΟΜΕΝΗΣ ΤΗΣ ΕΓΓΥΗΣΗΣ, ΤΗΣ ΣΥΜΒΑΣΗΣ, ΤΟΥ ΝΟΜΟΥ Η ΤΗΣ ΑΔΙΚΟΠΡΑΞΙΑΣ, ΑΝΕΞΑΡΤΗΤΑ ΑΠΟ ΤΟ ΑΝ ΕΝΗΜΕΡΩΘΗΚΕ ΓΙΑ ΤΗΝ ΠΙΘΑΝΟΤΗΤΑ ΤΕΤΟΙΩΝ ΖΗΜΙΩΝ. ΑΝΕΞΑΡΤΗΤΑ ΑΠΟ ΤΗ ΔΙΑΡΚΕΙΑ ΟΠΟΙΑΣΔΗΠΟΤΕ ΠΕΡΙΟΡΙΣΜΕΝΗΣ ΕΓΓΥΗΣΗΣ Η ΟΠΟΙΑΣΔΗΠΟΤΕ ΕΓΓΥΗΣΗΣ ΠΟΥ ΥΠΟΝΟΕΙΤΑΙ ΑΠΟ ΤΟ ΝΟΜΟ Η ΣΕ ΠΕΡΙΠΤΩΣΗ ΠΟΥ ΟΠΟΙΑΔΗΠΟΤΕ ΠΕΡΙΟΡΙΣΜΕΝΗ ΕΓΓΥΗΣΗ ΑΠΟΤΥΧΕΙ ΤΟΥ ΟΥΣΙΑΣΤΙΚΟΥ ΣΚΟΠΟΥ ΤΗΣ, ΣΕ ΚΑΜΙΑ ΠΕΡΙΠΤΩΣΗ Η ΣΥΝΟΛΙΚΗ ΕΥΘΥΝΗ ΤΗΣ ISTORAGE ΔΕΝ ΘΑ ΥΠΕΡΒΑΙΝΕΙ ΤΗΝ ΤΙΜΗ ΑΓΟΡΑΣ ΑΥΤΟΥ ΤΟΥ ΠΡΟΪΟΝΤΟΣ. | 4823-2548-5683.3

DISKASHUR® M²

iStorage®

Πνευματικά δικαιώματα © iStorage Limited 2020.
Με την επιφύλαξη παντός δικαιώματος.
iStorage Limited, iStorage House, 13 Alperton Lane Perivale, Middlesex. UB6 8DH, Αγγλία
Τηλ: +44 (0) 20 8991 6260 | Φαξ: +44 (0) 20 8991 6277
e-mail: info@istorage-uk.com | web: www.istorage-uk.com