iStorage®

# diskAshur PRO² ®




CESG Certified Product
Foundation Grade
HME1433053936-1257

NCSC CPA CERTIFIED

FIPS VALIDATED 140-2™

FIPS 140-2 LEVEL 2 CERTIFIED

Algemene Inlichtingen- en Veiligheidsdienst
*Ministerie van Binnenlandse Zaken en Koninkrijksrelaties*

NLNCSA BSPA CERTIFIED


**English** User Manual - Table of Contents .....4

**Deutsch** Benutzerhandbuch - Inhaltsverzeichnis .....42

**Français** Manuel d'utilisation - Table des matières .....80

diskAshur PRO²®

iStorage®

# User Manual




diskAshur PRO²®

## HDD & SSD Range

**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 PRO² drive please contact our technical department by email - support@istorage-uk.com or by phone on +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2017. 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

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

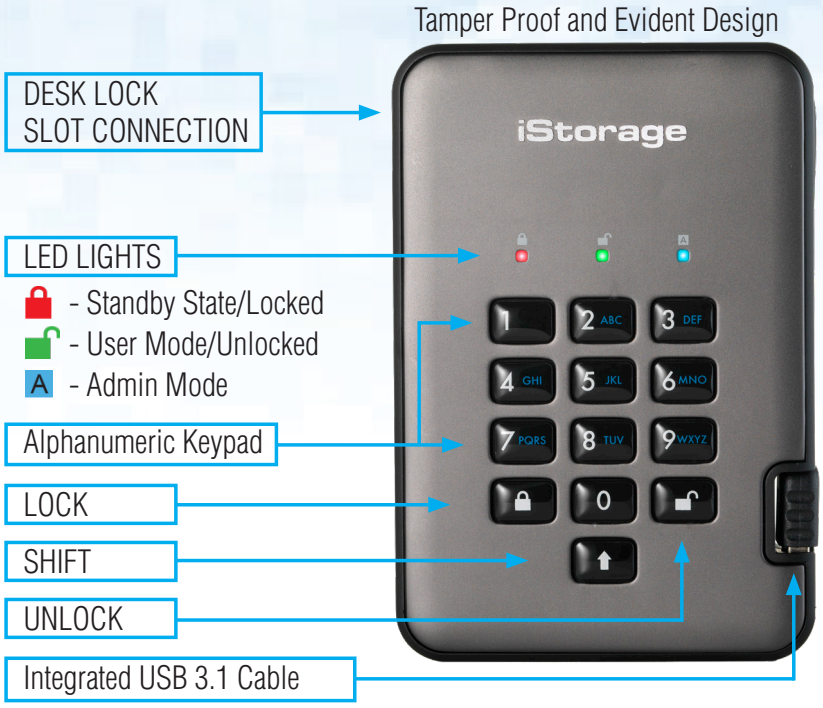
Trade Agreements Act (TAA) Compliant

# Table of Contents

Introduction ..... 5
Box contents ..... 5
1. diskAshur PRO² LED States ..... 6
2. How to use the diskAshur PRO² for the first time ..... 6
3. Unlocking the diskAshur PRO² ..... 7
4. Locking the diskAshur PRO² ..... 7
5. Entering Admin Mode ..... 7
6. Changing the Admin PIN ..... 8
7. Setting a User PIN Policy ..... 9
8. How to check the User PIN Policy ..... 10
9. Adding a new User PIN in Admin Mode ..... 11
10. Changing the User PIN in Admin Mode ..... 11
11. Deleting the User PIN in Admin Mode ..... 11
12. Set Read-Only in Admin Mode ..... 12
13. Enable Read/Write in Admin Mode ..... 12
14. How to create a Self-Destruct PIN ..... 12
15. How to delete the Self-Destruct PIN ..... 13
16. How to Unlock with the Self-Destruct PIN ..... 13
17. How to Create an Admin PIN after a Brute Force attack or Reset ..... 14
18. Setting the Unattended Auto-Lock Clock ..... 14
19. Turn off the Unattended Auto-Lock Clock ..... 15
20. How to check the Unattended Auto-Lock Clock ..... 15
21. How to Unlock diskAshur PRO² with User PIN ..... 16
22. Changing the User PIN in User Mode ..... 16
23. Set Read-Only in User Mode ..... 17
24. Enable Read/Write in User Mode ..... 17
25. Brute Force Protection ..... 18
26. How to perform a complete reset ..... 18
27. Initialising and formatting the diskAshur PRO² ..... 19
28. diskAshur PRO² Setup for Mac OS ..... 21
29. diskAshur PRO² Setup for Linux (Ubuntu 17.10) ..... 23
30. Hibernating, Suspending or Logging off from the Operating System ..... 26
31. How to check Firmware in Admin Mode ..... 26
32. How to check Firmware in User Mode ..... 27
33. Technical Support ..... 28
34. Warranty and RMA information ..... 28

**Appendices**

A. iStorage Security Directive #1 – Secure Handling ..... 29
B. iStorage Security Directive #2 – Sanitisation and Secure Disposal ..... 34




## Introduction

The diskAshur PRO² is an easy to use, ultra-secure, hardware encrypted portable drive with capacities of up to 5TB. Simply connect the integrated USB 3.1 cable to any computer and enter a 7-15 digit PIN, if the correct PIN is entered, all data stored on the drive will be decrypted and accessible. To lock the drive and encrypt all data, simply eject the diskAshur PRO² from the host computer and the entire contents of the drive will be encrypted (full disk encryption) using military grade AES 256-bit hardware encryption (XTS mode). If the drive is lost or stolen and an incorrect PIN is entered 15 consecutive times, the drive will reset, the encryption key will be deleted and all data previously stored on the drive will be lost forever.

One of the unique and underlying security features of the GDPR compliant diskAshur PRO² is the dedicated hardware based secure microprocessor (Common Criteria EAL4+ ready), which employs built-in physical protection mechanisms designed to defend against external tamper, bypass attacks and fault injections. Unlike other solutions, the diskAshur PRO² 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

1. diskAshur PRO² Drive with integrated USB Cable
2. Elegant Travel Case
3. Quick Start Guide

## Caution! Please Read:

**For security reasons, iStorage recommend that upon first use of the diskAshur PRO², you take one of the following actions:**

1. Change the default Admin PIN (11223344) immediately as described in '**Section 6: Changing the Admin PIN**' then proceed to '**Create a New User PIN**' as described in '**Section 9: Adding a New User PIN in Admin Mode**'.

**- or -**

2. Reset your diskAshur PRO² as described in '**Section 26: How to perform a complete reset**' and then '**Create a New Admin PIN**' as described in '**Section 17: How to Create an Admin PIN after a Brute Force attack or Reset**'.

# 1. diskAshur PRO² LED States

When the diskAshur PRO² is plugged in, there are three possible behaviours for the LED indicators as shown in the table below.

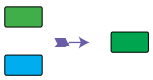
| RED | GREEN | BLUE | diskAshur PRO² State |
|---|---|---|---|
| Solid | Off | Off | Factory Reset [1] |
| Solid | Solid | Solid | Brute Force [2] |
| Solid | Off | Off | Standby [3] |

1. In Factory Reset State, the drive is waiting for the operation to set up an Admin PIN.
2. In Brute Force state, the drive is waiting for an operation to get more PIN entry attempts.
3. In Standby state, the drive is waiting for an operation to unlock the drive, or enter Admin mode, or reset the drive.

# 2. How to use the diskAshur PRO² for the first time

The diskAshur PRO² is shipped with a default Admin PIN of **11223344** and although it can be used straight out of the box with the default Admin PIN, for security reasons we **highly recommend a new Admin PIN be created immediately** by following the instructions under section 6 'Changing the Admin PIN'.

Please follow the 3 simple steps in the table below to unlock the diskAshur PRO² for the first time with the default Admin PIN.

| Instructions - first time use | LED | LED State |
|---|---|---|
| 1. Connect the diskAshur PRO² to a USB port |  | RED LED will be solid awaiting PIN entry |
| 2. Enter Admin PIN (default - 11223344) |  | RED LED remains solid |
| 3. Within 10 seconds press the "**UNLOCK**" button once to unlock diskAshur PRO² |  | GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED changing to a blinking GREEN and finally solid GREEN LED |

**Note**: Once the diskAshur PRO² has been successfully unlocked, the GREEN LED will remain on and in a solid state. It can be locked down immediately by pressing the "**LOCK**" button once or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system. To ensure no data is corrupted, we recommend using 'Safely Remove Hardware/Eject'.

## 3. Unlocking the diskAshur PRO²

The diskAshur PRO² can be unlocked with either an Admin or User PIN whilst in standby state (solid RED LED).

1. To unlock as the Administrator, enter the **Admin** PIN and press the "**UNLOCK**" button.

2. To unlock as a **User**, first press the "**UNLOCK**" button (all LEDs,  blink on and off) and then enter the **User** PIN and press the "**UNLOCK**" button again.

3. If correct User PIN is entered, both GREEN and BLUE LEDs will blink alternately and then return to a solid GREEN LED.

4. If correct Admin PIN is entered, both GREEN and BLUE LEDs will blink alternately, then to a solid BLUE for 1 second and then to the unlocked state, a solid GREEN LED.

5. If correct PIN is entered, the drive displays as "iStorage diskAshur PRO² USB Device" under "Computer Management/ Device Manager".

In an unlocked state (GREEN LED), there are two possible behaviours for the LED indicators, shown in the table below.

| RED | GREEN | BLUE | diskAshur PRO² |
|---|---|---|---|
| Off | Solid | Off | No data transfer |
| Off | Blink | Off | Data transfer in progress |

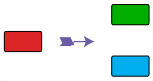
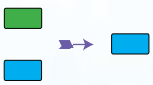
## 4. Locking the diskAshur PRO²

To lock the drive, press the "**LOCK**" button once or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system. If data is still being written to the drive, please wait until all data has been written to the drive before pressing the 'LOCK' button or safely ejecting from the Operating System. When the unattended Auto-Lock timeout is activated, the drive will automatically lock after a predetermined amount of time.

**Note:** The diskAshur PRO² cannot be recognized by the operating system in standby state.

## 5. Entering Admin Mode

To enter the Admin Mode, do the following:

| | | |
|---|---|---|
| 1. In standby state (solid RED LED), press and hold down "**UNLOCK + 1**" buttons |  | Solid RED LED will change to blinking GREEN and BLUE LEDs |
| 2. Enter the Admin PIN (default - 11223344) and press "**UNLOCK**" button |  | GREEN and BLUE LEDs blink rapidly together for a few seconds then to a solid GREEN and finally a solid BLUE LED indicating the diskAshur PRO² is in "Admin Mode" |

To exit Admin mode, press the "**LOCK**" button.

# 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 create a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the key with the corresponding letters on it.

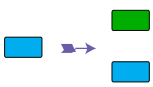
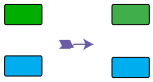
**Examples of these types of Alphanumerical PINs are:**

- For "**Password**" you would press the following keys:
  **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)
- For "**iStorage**" you would press:
  **4** (gh**i**) **7** (pqr**s**) **8** (**t**uv) **6** (mn**o**) **7** (pq**r**s) **2** (**a**bc) **4** (**g**hi) **3** (d**e**f)

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

**Note:** The **SHIFT** key can be used for additional combinations. **SHIFT** + 1 is a separate value than just 1. To create a PIN using additional combinations, press and hold down the **SHIFT** button whilst entering your 7-15 digit PIN. e.g. **SHIFT** + **26756498**.

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 "**UNLOCK + 2**" buttons |  | Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs |
| 2. Enter NEW Admin PIN and press "**UNLOCK**" button |  | Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs |
| 3. Re-enter the NEW Admin PIN and press "**UNLOCK**" button |  | Blinking GREEN 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 |

# 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 a '**Special Character**'. The "Special Character" functions as '**Shift** + **digit**'.

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 a 'Special Character' 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 created. If the Administrator creates the User PIN as '**247688314**' with the use of a '**Special Character**' (Shift+digit), 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:**

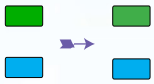
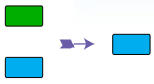
- If a 'Special Character' was used during the creation of the User PIN, for instance, example '**B**' above, then the drive can only be unlocked by entering the PIN with the 'Special Character' entered precisely in the order created, as per example '**B**' above - ('2', '4', '**Shift + 7**', '6', '8', '8', '3', '1', '4').

- 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 "**UNLOCK + 7**" buttons |  | Solid BLUE LED will change to blinking GREEN and solid 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 solid BLUE LEDs will continue to blink |
| 3. Press the "**SHIFT**" button ( ⬆ ) once |  | Blinking GREEN and Solid BLUE will change to a solid GREEN LED and finally to a solid BLUE LED indicating the User PIN Policy has been successfully set. |

## 8. 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.

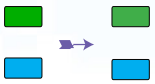
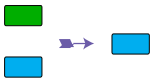
| | | |
|---|---|---|
| 1. In Admin mode press and hold down **SHIFT** ( ⬆ ) + **7** |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs |
| 2. Press the "**UNLOCK**" button and the following happens;<br><br>a. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>b. A RED LED blink equates to ten (10) units of a PIN.<br>c. Every GREEN LED blink equates to a single (1) unit of a PIN<br>d. A BLUE blink indicates that a 'Special Character' was used.<br>e. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>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, the RED LED will blink once (**1**) and the GREEN will blink twice (**2**) followed by a single 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 |

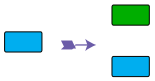
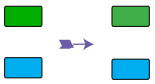
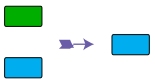
## 9. Adding a new User PIN in Admin Mode

To add a **New User**, 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 "**UNLOCK + 3**" buttons |  | Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs |
| 2. Enter New User PIN and press "**UNLOCK**" button |  | Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs |
| 3. Re-enter the New User PIN and press "**UNLOCK**" button |  | GREEN LED rapidly blinks for a few seconds then changes to a solid BLUE LED indicating the User PIN has been successfully created |

## 10. Changing the User PIN in Admin Mode

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 "**UNLOCK + 3**" buttons |  | Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs |
| 2. Enter New User PIN and press "**UNLOCK**" button |  | Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs |
| 3. Re-enter the New User PIN and press "**UNLOCK**" button |  | GREEN LED rapidly blinks for a few seconds then changes to a solid BLUE LED indicating the User PIN has been successfully changed |

## 11. Deleting the User PIN in Admin Mode

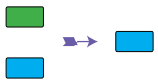
To delete a **User PIN**, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

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

## 12. Set Read-Only in Admin Mode

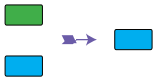
**Important:** If data has just been copied to the diskAshur PRO², make sure to properly disconnect the drive first by clicking 'Safely Remove Hardware/Eject' the diskAshur PRO² from the Operating System before reconnecting and setting the diskAshur PRO² as 'Read-Only/Write-Protect'.

When Admin writes content to the diskAshur PRO² and restricts access to read-only, the User cannot change this setting in User mode. To set the diskAshur PRO² 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 "**7 + 6**" buttons. (7=**R**ead + 6=**O**nly) |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs |
| 2. Release 7+6 buttons and press "**UNLOCK**" |  | GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating the drive is configured as Read-Only |

## 13. Enable Read/Write in Admin Mode

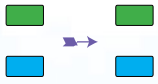
To set the diskAshur PRO² to Read/Write, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

| | | |
|---|---|---|
| 1. In Admin mode, press and hold down "**7 + 9**" buttons. (7=**R**ead + 9=**W**rite) |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs |
| 2. Release 7+9 buttons and press "**UNLOCK**" |  | GREEN and BLUE LEDs change to a solid GREEN LED then to a solid BLUE LED indicating the drive is configured as Read/Write |

## 14. How to create a Self-Destruct PIN

The self-destruct feature allows you to set a PIN which can be used to perform a crypto-erase on the entire drive. 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 PRO² will need to be partitioned and formatted before any new data can be added to the drive.

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 "**UNLOCK + 6**" buttons |  | Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs |
| 2. Create a 7-15 digit Self-Destruct PIN and press the "**UNLOCK**" button |  | Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs |
| 3. Re-enter the PIN and press the "**UNLOCK**" 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 |

## 15. How to Delete the Self-Destruct PIN

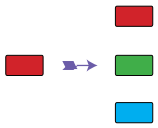
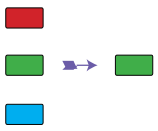
To delete the Self-Destruct PIN, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

| | | |
|---|---|---|
| 1. In Admin mode, press and hold down "**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 |

## 16. How to Unlock with the Self-Destruct 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 PRO² will need to be partitioned and 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, press the "**UNLOCK**" button |  | RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off |
| 2. Enter the Self-Destruct PIN and press the "**UNLOCK**" button |  | RED, GREEN and BLUE blinking LEDs will change to GREEN and BLUE LEDs alternating on and off for approximately 15 seconds and finally shifts to a solid GREEN LED |

**Important:** 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 PRO² will need to be reset (see 'How to perform a complete reset' Section 26, on page 18) first in order to create an Admin PIN with full Admin privileges including the ability to create a User PIN.

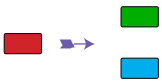
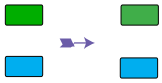
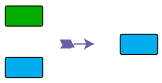
## 17. How to Create an Admin PIN after a Brute Force attack or Reset

It will be necessary after a Brute Force attack or when the diskAshur PRO² has been reset to create an Admin PIN before the drive can be used. If the drive has been brute forced or reset, the drive will be in a standby state (solid RED LED). to create an Admin PIN proceed with the following steps.

**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)

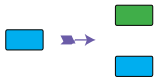
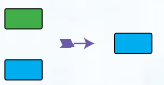
**Note:** The **SHIFT** key can be used for additional combinations. **SHIFT** + 1 is a separate value than just 1. To create a PIN using additional combinations, press and hold down the **SHIFT** button whilst entering your 7-15 digit PIN. e.g. **SHIFT** + **26756498**.

| | | |
|---|---|---|
| 1. In Standby state, press and hold down "**Shift + 1**" buttons |  | Solid RED LED will change to blinking GREEN and solid BLUE LEDs |
| 2. Enter NEW Admin PIN and press "**UNLOCK**" button |  | Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs |
| 3. Re-enter the NEW Admin PIN and press "**UNLOCK**" button |  | Blinking GREEN LED and solid BLUE LED change to BLUE LED rapidly blinking for a few seconds and then to a solid BLUE LED indicating the Admin PIN was successfully configured. |

## 18. Setting the Unattended Auto-Lock Clock

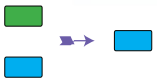
To protect against unauthorised access if the drive is unlocked and unattended, the diskAshur PRO² can be set to automatically lock after a pre-set amount of time. In its default state, the diskAshur PRO² Unattended Auto Lock feature is turned off. The Unattended Auto Lock can be set to activate between 5 - 99 minutes.

To set 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 "**UNLOCK + 5**" buttons |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs |
| 2. Enter the amount of time that you would like to set the Auto-Lock timeout feature for, the minimum time that can be set is 5 minutes and the maximum being 99 minutes (5-99 minutes). For example enter:<br>**05 for 5 minutes**<br>**20 for 20 minutes**<br>**99 for 99 minutes** | | |
| 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 |

## 19. Turn off the Unattended Auto-Lock Clock

To turn off 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 "**UNLOCK + 5**" buttons |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs |
| 2. Enter "**00**" and press the "**SHIFT**" ( ⬆ ) button |  | Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto-Lock time out has been successfully switched off |

## 20. How to check the Unattended Auto-Lock Clock

The Administrator is able to check and determine the length of time set for the unattended auto-lock clock by simply noting the LED sequence as described on the table at the bottom of this page.

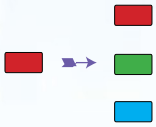
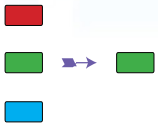
To check the unattended auto-lock, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

| | | |
|---|---|---|
| 1. In Admin mode press and hold down **SHIFT** ( ⬆ ) + **5** |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs |
| 2. Press the "**UNLOCK**" button and the following happens;<br><br>a. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>b. Each RED LED blink equates to ten (10) minutes.<br>c. Every GREEN LED blink equates to one (1) minute.<br>d. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>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 **26** minutes, the RED LED will blink twice (**2**) and the GREEN LED will blink six (**6**) times.

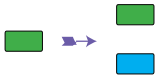
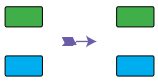
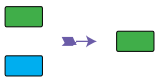
| Auto-Lock in minutes | RED | GREEN |
|---|---|---|
| 8 minutes | 0 | 8 Blinks |
| 15 minutes | 1 Blink | 5 Blinks |
| 26 minutes | 2 Blinks | 6 Blinks |
| 40 minutes | 4 Blinks | 0 |

## 21. How to Unlock diskAshur PRO² with User PIN

| | | |
|---|---|---|
| 1. In a standby state (solid RED LED) Press the "**UNLOCK**" button |  | RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off |
| 2. Enter User PIN and press the "**UNLOCK**" button |  | RED, GREEN and BLUE blinking LEDs will change to alternating GREEN and BLUE LEDs then to a rapidly blinking GREEN LED and finally shifts to a solid Green LED indicating drive successfully unlocked in User mode |

## 22. Changing the User PIN in User Mode

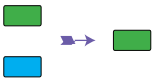
To change the **User PIN**, first unlock the diskAshur PRO² with a User PIN as described above in section 21. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

| | | |
|---|---|---|
| 1. In User mode press and hold down "**UNLOCK + 4**" |  | Solid GREEN LED will change to a blinking GREEN LED and a solid BLUE LED |
| 2. Enter New User PIN and press the "**UNLOCK**" button |  | Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs |
| 3. Re-enter New User PIN and press the "**UNLOCK**" button |  | Blinking GREEN and solid BLUE LEDs will switch to a rapidly blinking GREEN LED and then to a solid GREEN LED indicating successful User PIN change |

## 23. Set Read-Only in User Mode

**Important:** If data has just been copied to the diskAshur PRO², make sure to properly disconnect the drive first by clicking 'Safely Remove Hardware/Eject' the diskAshur PRO² from the Operating System before reconnecting and setting the diskAshur PRO² as 'Read-Only/Write-Protect'.

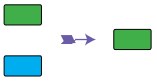
To set the diskAshur PRO² to Read-Only, first enter the "**User Mode**" as described in section 21. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

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

**Note:** 1. This setting is activated the next time the drive is unlocked.
2. If a User set the drive as Read-Only, Admin can override it by setting the drive as Read/Write in Admin mode.
3. If Admin set the drive as Read-Only, the User cannot set the drive as Read/Write

## 24. Enable Read/Write in User Mode

To set the diskAshur PRO² to Read/Write, first enter the "**User Mode**" as described in section 21. 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. Release 7+9 buttons and press "**UNLOCK**" |  | GREEN and BLUE LEDs will change to a solid GREEN LED indicating the drive is configured as Read/Write |

**Note:** 1. This setting is activated the next time the drive is unlocked.
2. If a User set the drive as Read-Only, Admin can override it by setting the drive as Read/Write in Admin mode.
3. If Admin set the drive as Read-Only, the User cannot set the drive as Read/Write

## 25. Brute Force Protection

If an incorrect PIN is entered 15 (3 x 5 PIN clusters) consecutive times, then all Admin/User PINs, the encryption key and all data will be deleted and lost forever. The diskAshur PRO² will then need to be formatted and partitioned before it can be reused.

**1.** If a PIN is entered incorrectly 5 (five) consecutive times, all LEDs - RED, GREEN, BLUE will light up and become solid.

**2.** Unplug the drive and re-plug it into the host to get five more PIN attempts. If PIN is incorrectly entered 5 more times, (10 in total - 5 from step 1 and 5 from step 2) all LEDs - RED, GREEN, BLUE will light up and become solid again.

**3**. Unplug the drive, hold down the "**SHIFT**" button and replug it into the host, all LEDs - RED, GREEN, BLUE will light up and blink together.

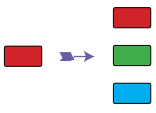
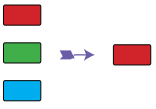
**4**. With all LEDs blinking, enter "**47867243**" and press the "**UNLOCK**" button to get 5 final attempts.

**Caution:** After 15 consecutive incorrect PIN entries the Brute Force Defence Mechanism activates and deletes all Admin/User PINs, the encryption key and data. A new Admin PIN must be created, refer to Section 17 on page 14 on 'How to Create an Admin PIN after a Brute Force attack or Reset', the diskAshur PRO² will also need to be partitioned and formatted before any new data can be added to the drive.

## 26. How to perform a complete reset

To perform a complete reset, the diskAshur PRO² must be in a 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 and partitioned before it can be reused.

To reset the diskAshur PRO² proceed with the following steps.

| | | |
|---|---|---|
| 1. In standby state, press and hold down "**0**" button until all LEDs blink alternately on and off |  | Solid RED LED will change to all LEDs, RED, GREEN and BLUE blinking alternately on and off |
| 2. Press and hold down "**2 + 7**" buttons until all LEDs become solid for a second and then to a solid RED LED |  | RED, GREEN and BLUE alternating LEDs will change to all 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 created, refer to Section 17 on page 14 on 'How to Create an Admin PIN after a Brute Force attack or Reset', the diskAshur PRO² will also need to be partitioned and formatted before any new data can be added to the drive.

# 27. Initialising and formatting the diskAshur PRO²

After a 'Brute Force Attack' or a complete reset of the diskAshur PRO² will delete all data, encryption key and partition settings. You will need to initialise and format the diskAshur PRO² before it can be used.

To initialise your diskAshur PRO², do the following:

1. Attach the diskAshur PRO² to the computer.

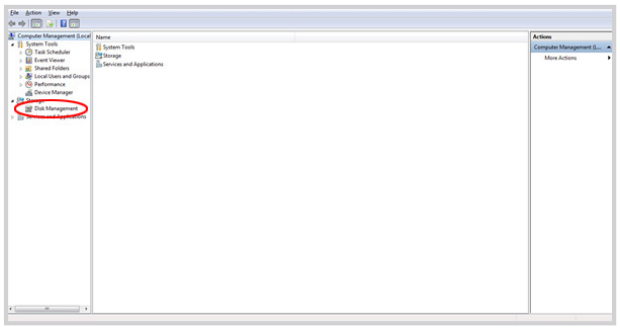
2. Create a new Admin PIN - see page 14, section 17, 'How to create an Admin PIN after a Brute Force attack or reset'.

3. With the diskAshur PRO² in standby state (RED LED) enter New Admin PIN to unlock (GREEN LED).

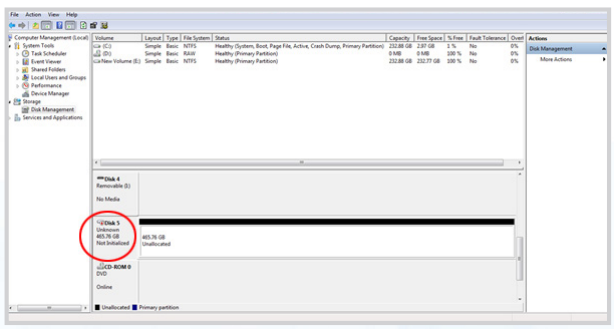
4. **Windows 7:** Right click **Computer** and then click **Manage** and then select **Disk Management**
   **Windows 8**: Right-click left corner of desktop and select **Disk Management**
   **Windows 10:** Right click on the start button and select **Disk Management**

5. In the Computer Manage window, click **Disk Management**. In the Disk Management window, the diskAshur PRO² is recognised as an unknown device that is uninitialised and unallocated.

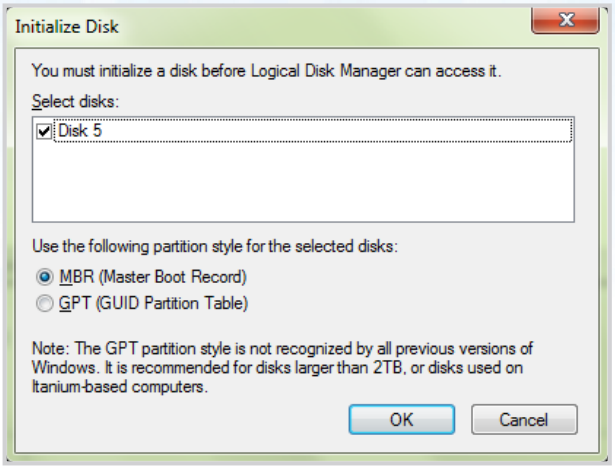
**Note:** If the Initialise Disk Wizard window opens, click **Cancel.**



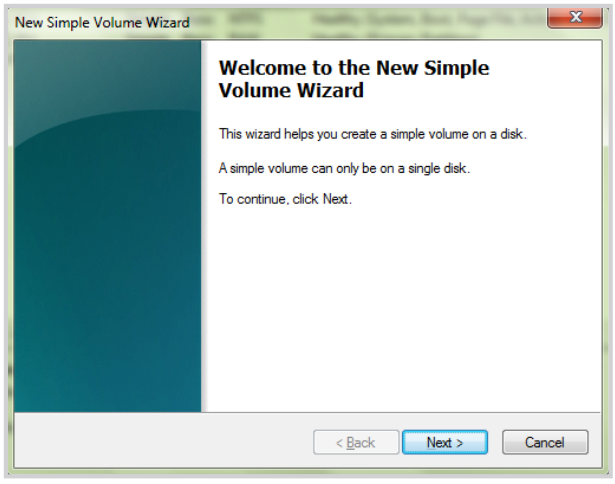
6. Right-click Unknown Disk, and then select Initialise Disk.



7. In the Initialise Disk window, click **OK**.




8. Right-click in the blank area under the Unallocated section, and then select New Simple Volume. The Welcome to the New Simple Volume Wizard window opens.




9. Click **Next**.

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

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

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

13. Click **Finish**.

14. Wait until the format process is complete. The diskAshur PRO² will be recognised and it is available for use.

# 28. diskAshur PRO² Setup for Mac OS

Your diskAshur PRO² is preformatted exFAT. To reformat the drive to a Mac compatible format please read below.

Once the drive is unlocked, open Disk Utility from Applications/Utilities/Disk Utilities.

**To format the diskAshur PRO²:**

1. Select diskAshur PRO² from the list of drives and volumes. Each drive in the list will display its capacity, manufacturer, and product name, such as 'iStorage diskAshur PRO² Media' or 232.9 diskAshur PRO².




2. Click the 'Erase' button (figure 1).




figure 1

3. Enter a name for the drive (figure 2). The default name is Untitled. The name of the drive will eventually appear on the desktop.

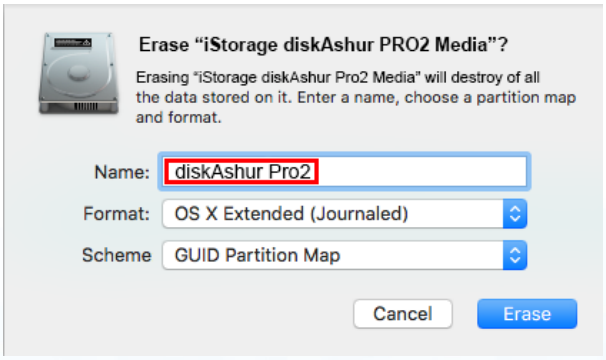



figure 2

4. Select a scheme and volume format to use. The Volume Format dropdown menu (figure 3) lists the available drive formats that the Mac supports. The recommended format type is 'Mac OS Extended (Journaled).' The scheme format dropdown menu lists the available schemes to use (figure 4). We recommend using 'GUID Partition Map' on drives larger than 2TB.

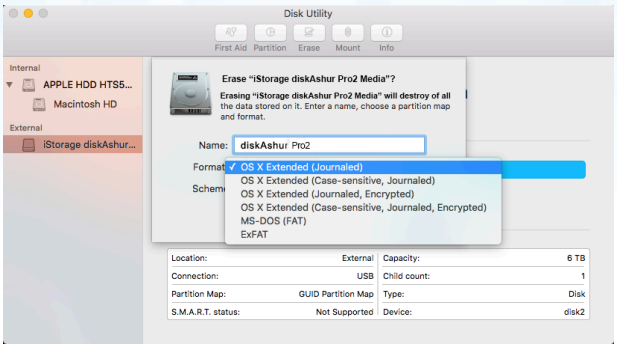


figure 3

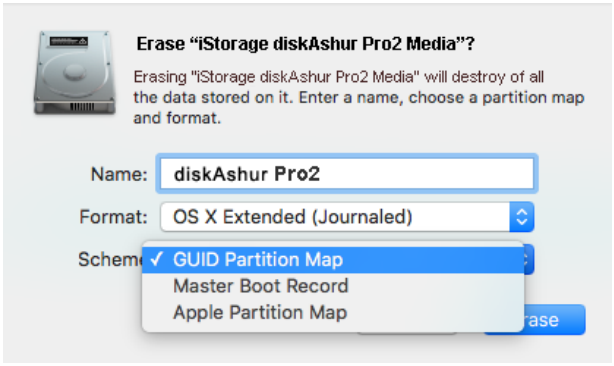


figure 4

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

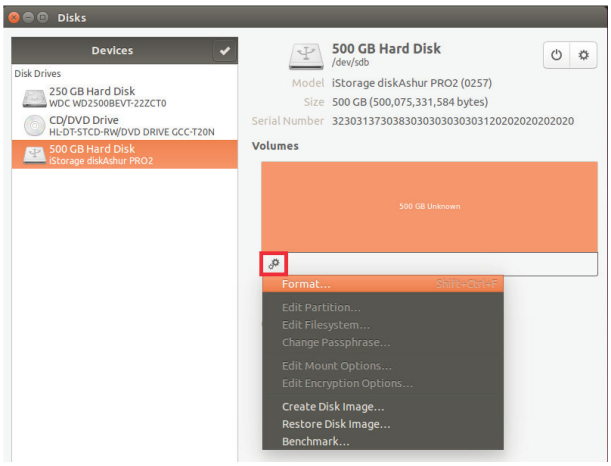
# 29. diskAshur PRO² Setup for Linux (Ubuntu 17.10)

If your diskAshur PRO² has been initialised and formatted exFAT, you can directly use the drive on Ubuntu.
If not, please read below.
To format the diskAshur PRO² as FAT filesystem:

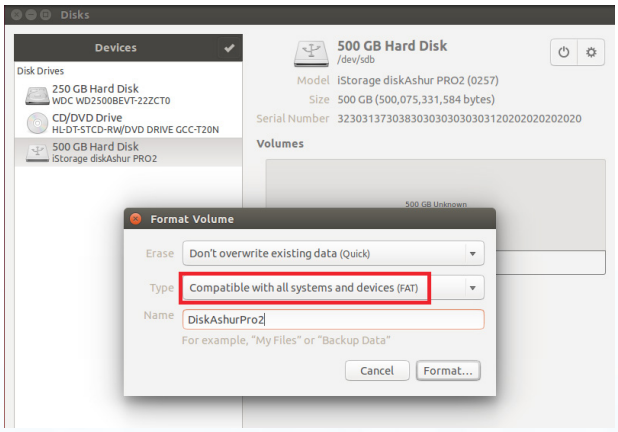
1. Open '**Show Application**' and type '**Disks**' in the search box. Click on the '**Disks**' utility when displayed.



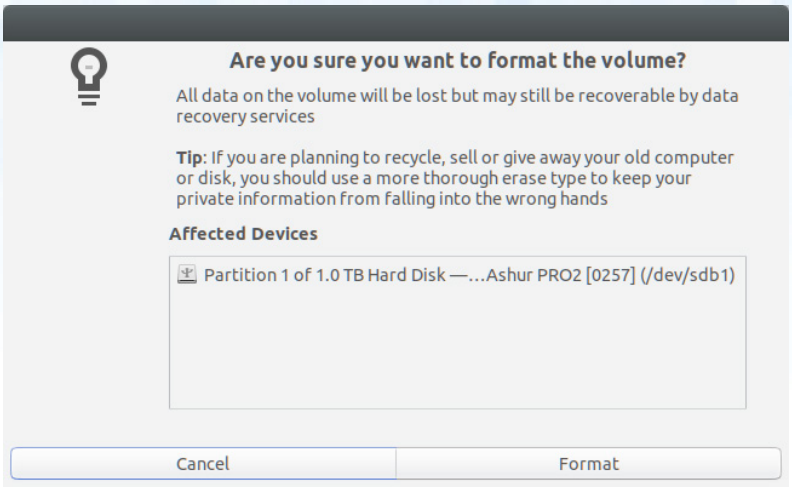

2. Click to select the drive (500 GB Hard Disk) under '**Devices**'. Next click on the gears icon under '**Volumes**' and then click on '**Format**'.



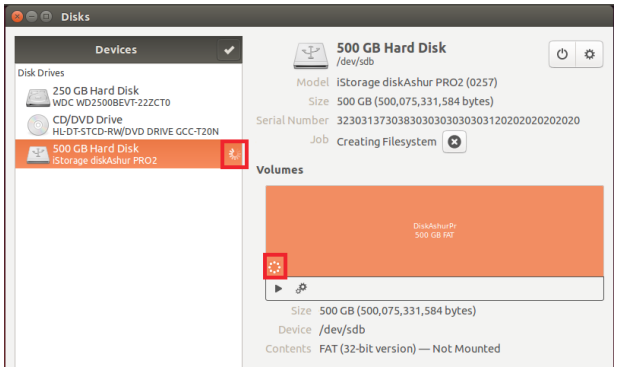

3. Select '**Compatible with all systems and devices (FAT)**' for the '**Type**' option. And enter a name for the drive, e.g: diskAshur PRO². Then, click the '**Format**' button.



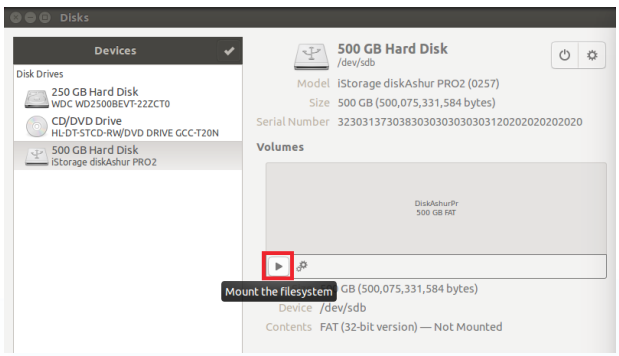
4. Click '**Format**' again.



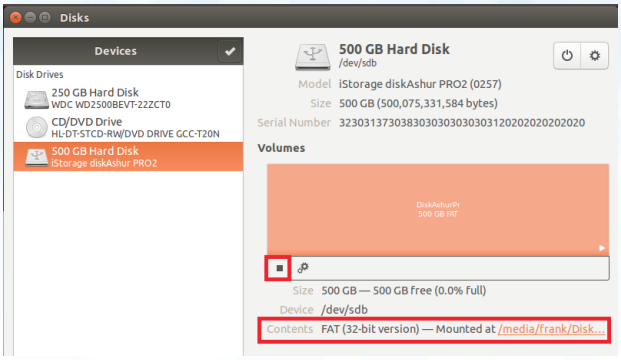

5. The drive will start to be formatted.



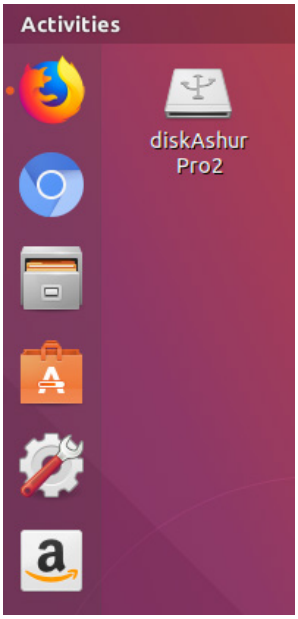

6. After the format process is finished, click ▶ to mount the drive to Ubuntu.



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

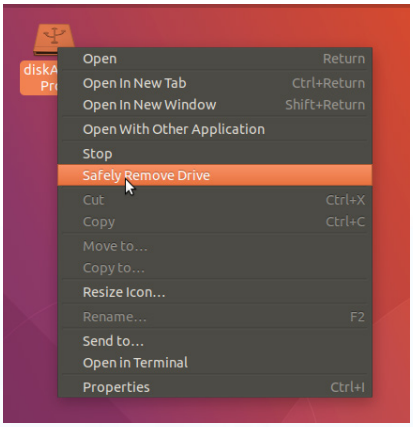



8. A disk icon will be shown as seen in the image below. You can click the disk icon to open your drive.




## Lock diskAshur PRO² for Linux (Ubuntu 17.10)

It is strongly recommended to right click your drive icon and then click '**Safely Remove**' in the OS to eject (lock) your diskAshur PRO², especially after data has been copied or deleted from the drive.



## 30. Hibernating, Suspending, or Logging off from the Operating System

Be sure to save and close all the files on your diskAshur PRO² before hibernating, suspending, or logging off from the operating system.

It is recommended that you lock the diskAshur PRO² manually before hibernating, suspending, or logging off from your system.

To lock, simply press the 'LOCK' button on the diskAshur PRO² or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system.

**Attention:** To ensure your data is secure, be sure to lock your diskAshur PRO² if you are away from your computer.

## 31. 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 "3 + 8" until GREEN and BLUE LEDs blink together |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs |
| 2. Press the "**UNLOCK**" button and the following happens;<br><br>a. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>b. RED LED blinks indicating the integral part of the firmware revision number.<br>c. GREEN LED blinks indicating the fractional part.<br>d. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>e. LEDs return to solid BLUE | | |

For example, if the firmware revision number is '1.2', the RED LED will blink once (1) and the GREEN LED will blink two (2) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to a solid BLUE LED.

## 32. How to check Firmware in User Mode

To check the firmware revision number, first enter the "**User Mode**" as described in section 21. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

| | | |
|---|---|---|
| 1. In User mode press and hold down "3 + 8" until GREEN and BLUE LEDs blink together |  | Solid GREEN LED will change to blinking GREEN and BLUE LEDs |
| 2. Press the "**UNLOCK**" button and the following happens;<br><br>a. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>b. RED LED blinks indicating the integral part of the firmware revision number.<br>c. GREEN LED blinks indicating the fractional part.<br>d. All LED's (RED, GREEN & BLUE) become solid for 1 second.<br>e. LEDs return to solid GREEN | | |

For example, if the firmware revision number is '1.2', the RED LED will blink once (1) and the GREEN LED will blink two (2) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to a solid BLUE LED.

## 33. Technical Support

iStorage provides the following helpful resources for you:

iStorage's Website
https://www.istorage-uk.com

E-mail correspondence
support@istorage-uk.com

Telephone support with our Technical Support Department on **+44 (0) 20 8991-6260**.
iStorage's Technical Support Specialists are available from 9:00 a.m. to 5:30 p.m.
GMT - Monday through Friday

## 34. Warranty and RMA information

**Three Year Warranty:**

iStorage offers a 3-year warranty on the iStorage diskAshur PRO² against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from iStorage or an authorised reseller.

**Disclaimer and terms of warranty:**

THE WARRANTY BECOMES EFFECTIVE ON THE DATE OF PURCHASE AND MUST BE VERIFIED WITH YOUR SALES RECEIPT OR INVOICE DISPLAYING THE DATE OF PRODUCT PURCHASE.
ISTORAGE WILL, AT NO ADDITIONAL CHARGE, REPAIR OR REPLACE DEFECTIVE PARTS WITH NEW PARTS OR SERVICEABLE USED PARTS THAT ARE EQUIVALENT TO NEW IN PERFORMANCE. ALL EXCHANGED PARTS AND PRODUCTS REPLACED UNDER THIS WARRANTY WILL BECOME THE PROPERTY OF ISTORAGE.
THIS WARRANTY DOES NOT EXTEND TO ANY PRODUCT NOT PURCHASED DIRECTLY FROM ISTORAGE OR AN AUTHORISED RESELLER OR TO ANY PRODUCT THAT HAS BEEN DAMAGED OR RENDERED DEFECTIVE: 1. AS A RESULT OF ACCIDENT, MISUSE, NEGLECT, ABUSE OR FAILURE AND/OR INABILITY TO FOLLOW THE WRITTEN INSTRUCTIONS PROVIDED IN THIS INSTRUCTION GUIDE: 2. BY THE USE OF PARTS NOT MANUFACTURED OR SOLD BY ISTORAGE; 3. BY MODIFICATION OF THE PRODUCT; OR 4. AS A RESULT OF SERVICE, ALTERNATION OR REPAIR BY ANYONE OTHER THAN ISTORAGE AND SHALL BE VOID. THIS WARRANTY DOES NOT COVER NORMAL WEAR AND TEAR.
NO OTHER WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING ANY WARRANTY OR MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, HAS BEEN OR WILL BE MADE BY OR ON BEHALF OF ISTORAGE OR BY OPERATION OF LAW WITH RESPECT TO THE PRODUCT OR ITS INSTALLATION, USE, OPERATION, REPLACEMENT OR REPAIR.
ISTORAGE SHALL NOT BE LIABLE BY VIRTUE OF THIS WARRANTY, OR OTHERWISE, FOR ANY INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGE INCLUDING ANY LOSS OF DATA RESULTING FROM THE USE OR OPERATION OF THE PRODUCT, WHETHER OR NOT ISTORAGE WAS APPRISED OF THE POSSIBILITY OF SUCH DAMAGES.

# Appendix A

## iStorage Security Directive #1 – Product Security Features & Secure Handling

This iStorage directive provides product support for use by **commercial, public service**, and **government** agencies alike of iStorage secure drive products, and applies the direction of the NCSC CESG document:

CPA Security Characteristic Hardware Media Encryption Version 1.2 Dated April 2012

This iStorage Directive #1 advises the security features supported by iStorage secure drive products, along with best security practices to be employed when using iStorage secure devices to protect sensitive and protectively marked information assets both in on-site accommodation and when away from the operational premises; or when the iStorage secure drives are in transit.

Together, the secure drive supported features and best practice advice accommodates robust mitigations against the risk of **physical attack, theft**, or the **opportunity to compromise data assets** stored on iStorage secure drives to deny the opportunity of unauthorised access to the protected content.

**The Risk:** iStorage secure drives are classified as valuable and attractive items, which may contain sensitive business, government related, or personal/protected data assets (GDPR related) and as such they represent a target for both physical and logical attack in the form of theft or compromise if:

- Left unattended
- Visible in public places
- When left in an open logical state (authenticated)
- When not secured correctly when in transit
- When commensurate controls are not applied to the sensitivity of the stored data asset
- Misplaced or lost

Within this iStorage Security Directive **#**1 we provide best advice, and pragmatic, workable mitigation to reduce the surface of attack.

**Mitigations:** The device security features and mitigations provided in the below document are the recommended and best security practices which should be applied when handling iStorage secure drives and are shown in **Table 1** below. This approach has the security objective to preserve the security mantra of **C**I**A**+**A** (**C**onfidentiality, **I**ntegrity, and **A**vailability + **A**ccountability) and applies relevant security controls as outlined within the ISO/IEC 27001, and the referenced NCSC CESG document:

### Table 1 – Mitigations – Product Features - Secure Handling

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| 1<br>Integrity<br>Availability<br>Accountability | DEP.M311<br>DEP.1.M26 | In Transit | Never leave an iStorage drive insecure in a vehicle, or on display when in transit;<br>If the secure drive must be left unattended, ensure that it is not in view, and that the vehicle is locked between loading and unloading of the media;<br>If an iStorage drive is operational, and contains data assets, always send via a tracked and trusted courier service;<br>iStorage secure drives are issued in a tamper proofed box which is secured by a security seal – if upon receipt the security seal is broken, or showing indications of tampering the drive should be considered compromised. Thus, immediately report this to the iStorage support line on:<br>+44 (0) 20 8991-6260<br>Or send an email to: support@istorage-uk.com |

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| 2<br>Confidentiality<br>Integrity<br>Availability | DEP.M1<br>DEP.M701 | Unauthorised Access | To mitigate and minimize the threat of compromise to data assets stored on an iStorage secure drive:<br><br>Never leave the iStorage secure drive unattended in an authenticated open session;<br><br>To avoid the potential of unauthorised access, place the drive in locked mode when not in operational use;<br><br>Configure the iStorage Unattended Auto-Lock Clock to secure the drive after a prescribed time (Refer to the iStorage User Manual);<br><br>When the iStorage secure drive is not required, ensure it is removed, and secured under appropriate physical security controls.<br><br>Always ensure that the stored data assets on the iStorage drive have been backed up, and are available should a loss of the iStorage secure drive occur. |
| 3<br>Confidentiality<br>Accountability | DEP.M703 | Loss, Theft, Compromise | Ensure that a process exists to support notification to management of theft, loss, or compromise of the iStorage secure drive – for example:<br><br>i. Report the loss or theft to the Police – and obtain a Crime Reference Number<br><br>ii. If a Corporate owned device, take steps to notify the Security Department as soon as possible<br><br>iii. In cases where UK Government (or other Government) assets are stored, report the incident to the appropriate Departmental IAO (Information Asset Owner) without delay<br><br>iv. In the case of Government Classified materials, consider the Privacy, Protective Marking, or any associated Caveats and their associated implications to National Security |

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| | | | v. On occasions where Commercial Data is concerned, assess the impact of the loss and potential compromise of the assets stored on the lost/stolen media<br><br>vi. If the asset is retuned, consider it compromised and take steps to ensure it is reformatted and initialised before it is reissued<br><br>Where Protectively Marked or Government data assets are stored on the iStorage drive, seek advice from the appropriate agency or authority;<br><br>Confirm that data was encrypted at time of theft or loss (drive was not in an authenticated open session) - clarifying it will not compromise sensitive data assets, or other forms of related information. |
| 4<br><br>Integrity | DEP.1.M26 | Tamper Proofing | The iStorage drives are protected by tamper proofing.<br><br>Conduct regular checks of the iStorage secure drive outer casing for indications of tampering or direct physical attack.<br><br>In the rare event that our product needs an update, software or firmware updates (either online or on CD or other media) are not provided, but we provide a Recall and Replacement service, which will inform you by email 2 working days in advance of the dispatch of the new product, including its serial number, which can be verified on receipt by your organisation. However, please be aware, at all times, of the potential risk of receiving a tampered or fake iStorage product from third parties, by ensuring that your organisation delivers appropriate Security Education and Awareness Training to users to make them aware of the potential risks.<br><br>**Note 1:** If there are any actual or suspected indications of product tampering or falsification, immediately report this to the iStorage support line on: +44 (0) 20 8991-6260 Alternatively, you can send an email to: support@istorage-uk.com |

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| 5<br>Confidentiality<br>Integrity | DEP.2.M12<br>DEP.2.M283<br>DEP.2.M285<br>DEP.2.M617 | Robust Password Management | The Password is never displayed whilst being entered.<br><br>Always set a complex password for both Admin, and User accounts on the iStorage secure drive to mitigate the potential ease of logical attack, and/or compromise;<br><br>Although the device accepts passwords of minimum 7 characters in length, we strongly recommend for the user to set up a password with higher complexity, e.g. no less than 8 characters and using **SHIFT** key with digits;<br><br>Choose a password construction which cannot be easily guessed;<br><br>Avoid multiple uses of the password on multiple systems of differing security sensitivities;<br><br>Never write down a password on paper;<br><br>Never share a password;<br><br>Be aware of overlooking when entering a password into the iStorage device in public places;<br><br>If it is suspected that the password has been subject to compromise, it must be subject to change at the earliest opportunity;<br><br>Where there is an operational reason to document a password in hard-copy, this must be done by secure means, or via the company Exception Process.<br><br>**Note 2:** Secure storage of a password may be facilitated by a secure password locker application, or by use of a sealed envelope which is subject to robust physical access control and secured within a high-grade combination lock safe. |
| 6<br>Confidentiality<br>Integrity | DEP.2.M281 | Administrator Password Management | The iStorage secure drive supports the functionality for an Administrator to be provisioned with a level of privileged access to manage the device.<br><br>Only authorised and authenticated Administrators can add, or revoke any assigned accounts. |

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| **7**<br>Confidentiality | **DEP.2.M277** | **Social Engineering** | Be aware of the potential of direct and indirect threat of Social Engineering attacks which may attempt to discover your user id, password and other business related, or personal credentials by means of social engineering techniques.<br><br>Ensure that the organisation delivers Security Education and Awareness to make users aware of the potential threats posed by:<br><br>i. Unsolicited email seeking to entice the user into exchanging communications with the sender<br><br>ii. Opening URL's which are embodied within an unexpected email, which has been received from an unknown user<br><br>iii. Opening attachments without consideration – they could be carrying a Malware Payload<br><br>iv. Accepting requests on Social Networking sites from people you don't know or recognise<br><br>v. Being enticed by on-line offers – if they look to good to be true, they probably are and most certainly are fake |
| **8**<br>Confidentiality<br>Integrity | **DEP.2.M280** | **Credential Distribution** | Never communicate or issue any form of security credentials via the same channel, or which are packaged with an iStorage secure drive.<br><br>**Note 3:** Where operational necessity dictates the requirement for distributing credentials, this should be achieved out-of-band (e.g. by voice, text, secured email). |
| **9**<br>Integrity | **DEP.4.M348**<br>**DEP.1.M348** | **Authorised Updates** | No automated process exists. Only approved updates which applicable to the iStorage products will be distributed as part of an upgrade or replacement process under the internal iStorage SDLC (Security Development Lifecycle) and their Vulnerability Management Policy/Process. |
| **10**<br>Confidentiality<br>Accountability | | **Data Classification** | Ensure that the value of data assets stored on the iStorage secure drive are classified, or protectively marked as is appropriate for their use, and/or custodianship. |
| **11**<br>Confidentiality | | **Cleared Staff/ Access** | Ensure that those who are provisioned access to the data assets stored on an iStorage secure drive possess a clear need-to-know and are suitably cleared as appropriate to the level of data asset, or protectively marked materials stored thereon. |

# Appendix B

## iStorage Security Directive #2 – Sanitisation and Secure Disposal

This iStorage directive provides product support for use by **commercial, public service** and **government** agencies alike of iStorage products. This iStorage Directive #2 advises the best security practices to be employed for sanitisation and secure disposal of iStorage secure drives which is aligned to the UK Government Directive **IS5** concerning secure disposal and reference – **DEP.M.137** which outlines the requirement for secure disposal.

This directive also advises on the reissue of secure drives to mitigate the risk of object reuse, or compromise of data assets stored on such iStorage secure drives.

**The Risk:** If any data assets stored on an iStorage secure drive are not subject to security controls when the drives are reissued, or disposed of at operational end-of-life, they could be subject to compromise implicating organisational security and data protection mandated controls, such as GDPR. For example:

- Exfiltration and circulation of sensitive data to unauthorised external actors
- Accidental disclosure
- Disclosure of Protectively Marked or Government Classified data assets

**Objective:** Whilst iStorage secure drives enforce protection over their stored data assets by means of robust encryption, it is nevertheless best security practice to ensure that on occasions when iStorage secure drives are reissued to other parties, custodians, department, or when they reach their operational end-of-life, the drives are subject to robust processes to ensure that any remanence of previously stored data assets are securely deleted and purged from that drive to mitigate the likelihood of compromise of such data assets.

Within this iStorage Security Directive #2 we provide best advice and pragmatic, workable mitigations to counter this threat.

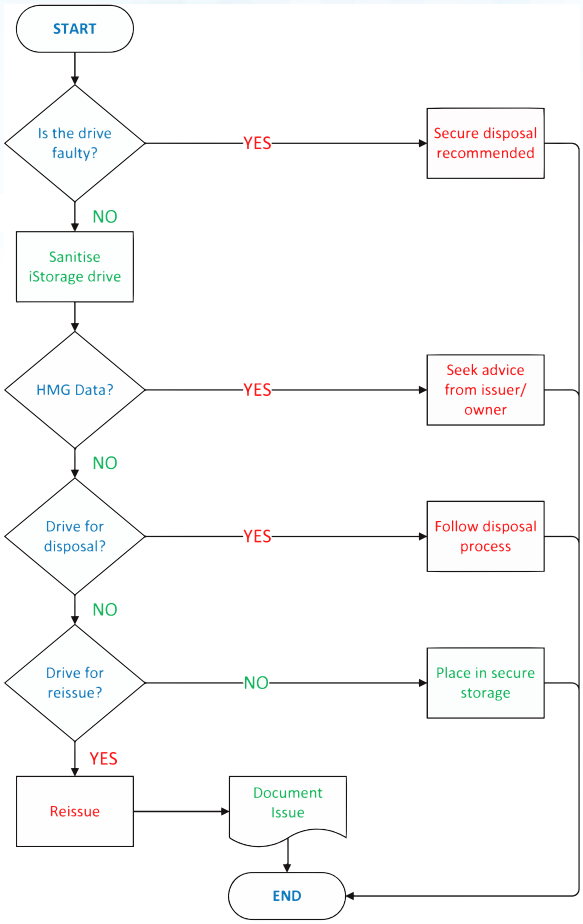
**Mitigations:** The mitigations provided below are the recommended and best security practices which should be applied when handling iStorage secure drives and are shown in **Table 1** below. This approach has the objective to preserve the security mantra of **CIA+A** (**C**onfidentiality, **I**ntegrity, and **A**vailability + **A**ccountability) and applies relevant security controls as outlined within the ISO/IEC 27001 and applies the direction of the NCSC (CESG) document.

CPA Security Characteristic Hardware Media Encryption Version 1.2 Dated April 2012

**Process:** **Fig 1** below is a representation of the high-level data flow which relates to:

- Secure disposal
- Sanitisation
- Protectively Marked and Government Security Classified data assets
- Reissue of iStorage secure drives

## Fig 1 – Sanitisation/Disposal Process




## Table 1 - Mitigations - Sanitisation and Secure Disposal

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| 1<br>Confidentiality<br>Accountability | DEP.M1 | Storage | Ensure that all iStorage secure drives awaiting sanitisation, or secure disposal are fully documented and accounted for;<br><br>That they are stored in a secure facility provisioned with robust physical and access control security mechanisms and procedures.<br><br>**Note 1:** Dependent on the amount awaiting processing, this could be a locked room, or a security cabinet. |
| 2<br>Confidentiality<br>Accountability | DEP.M311 | In Transit | When in transit to secure a disposal facility, never leave a drive insecure in a vehicle, or on display when in transit;<br><br>If the drives must be left unattended, ensure the iStorage secure drives are not in view, and that the vehicle is locked between loading and unloading of the media; |

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| | | | All iStorage secure drives destined for processing by a secure destruction facility should be tracked and handled only by a trusted vendor, or courier service;<br><br>Where iStorage secure drives have stored Protectively Marked and Government Classified information assets, advice should be sought from the relevant department, or agency to confirm if a requirement exists to apply additional controls (e.g. in transit communications, contact with the emergency services, or a stand-by vehicle) |
| **3**<br>**C**onfidentiality<br>**A**ccountability | | **Protective Marking** | Where iStorage secure drives have stored Protectively Marked, Government Classified data assets, guidance should be sought from the owner department or agency as to the requirements for recording and secure disposal of secure drives |
| **4**<br>**C**onfidentiality<br>**A**ccountability | | **Accountability** | All iStorage secure drives awaiting sanitisation, or secure disposal should be fully accounted for in a register, recording:<br><br>• Serial number<br>• Owner/department<br>• Date received<br>• Data asset classification, or protective marking<br>• Any special handling caveats<br>• Dispatch date for processing<br><br>**Note 2:** In circumstances where the iStorage drive has been sanitised for reissue, it should be then documented in a separate register awaiting distribution to a new owner/custodian/department. |
| **5**<br>**A**vailability | | **Business Continuity** | Prior to any iStorage secure drive being subject to sanitisation, or secure disposal, confirmation should be sought to assure that any data assets held thereon are accounted for, and backed up as required to avoid unintentional disposal of the stored operational data assets. |

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| 6<br>Confidentiality<br>Accountability | DEP.M137 | Sanitisation Methods | The sanitisation methods which are employed to process any iStorage secure drive should be supported by documented sanitisation procedures and Security Operating Procedures (SyOps);<br>Such procedures should follow appropriate processes relevant to the media type and any Protective Marking, or other Government Classification of the data asset being sanitised to meet as a minimum HMG Standards.<br>The selected Service Provider must demonstrate that these procedures are followed in practice.<br>NCSC (part of GCHQ) advice available at the following URL: https://www.ncsc.gov.uk/index/topic/164 |
| 7<br>Integrity | DEP.M137 | Sanitisation and Disposal | All Sanitisation/Destruction iStorage secure drives products should be conducted in line with Manufacturer's documented operating procedures, user guides and any published Security Procedures;<br>The personnel or teams who are conducting the sanitisation, or secure disposal process should be trained in the correct usage of such equipment;<br>Processes must be in place to verify that equipment is being used correctly and in accordance with the manufacturers recommendations. |
| 8<br>Confidentiality<br>Accountability | | Reissue of Media | On occasions where the iStorage secure drive has been subjected to sanitisation and is required for reissue to a new user, custodian, or department, checks should be conducted prior to issue to assure that the media is fully blank;<br>An iStorage secure drive user manual should be issued to the recipient user, with clear instructions of secure operational use;<br>The issue of the iStorage secure drive should be fully accounted for and entered in an asset register. |
| 9<br>Confidentiality<br>Accountability | DEP.M703 | Loss, Theft, Compromise | Ensure that a process exists to support notification to management of theft, loss, or compromise of the iStorage secure drive awaiting processing;<br>Where Protectively Marked or Government data assets are stored on the iStorage, seek advice from the appropriate authority of agency; |

| Mitigation | NCSC (CESG) CPA | Risk | Best Practice |
|---|---|---|---|
| | | | Confirm that data was encrypted at time of theft or loss - clarifying it will not compromise sensitive data assets, or other forms of related information. |
| 10<br>Confidentiality | MIT003 | Cleared Staff/ Access | Ensure that those who are provisioned access to the data assets stored on an iStorage secure drive possess a clear need-to-know and are suitably cleared as appropriate to the level of data asset, or Protectively Marked, Government Classified data assets and materials stored thereon. |

diskAshur PRO²®

iStorage®

Copyright © iStorage Limited 2017 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

# Benutzerhandbuch




diskAshur PRO²®

**Vergessen Sie Ihre PIN (Ihr Passwort) nicht, da Sie ohne PIN/Passwort nicht auf die Daten auf der Festplatte zugreifen können.**

Wenn Sie Probleme mit Ihrer diskAshur PRO²-Festplatte haben, wenden Sie sich per E-Mail oder telefonisch an unsere Technical Support-Abteilung: support@istorage-uk.com oder +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2017. Alle Rechte vorbehalten.
Windows ist eine eingetragene Marke der Microsoft Corporation.
Alle anderen erwähnten Marken und Copyrights sind Eigentum der jeweiligen Besitzer.
Die Verteilung modifizierter Versionen dieses Dokuments ist ohne die explizite Zustimmung des Urheberrechtsinhabers nicht zulässig.
Die Verteilung des Dokuments oder abgeleiteter Versionen in standardmäßiger Papierform zu kommerziellen Zwecken ist nur mit vorheriger Zustimmung des Urheberrechtsinhabers zulässig.
DIE DOKUMENTATION WIRD "WIE VORLIEGEND" ZUR VERFÜGUNG GESTELLT UND ALLE AUSDRÜCKLICHEN ODER IMPLIZITEN BEDINGUNGEN, ZUSAGEN UND GARANTIEN, EINSCHLIESSLICH JEGLICHER IMPLIZITER GARANTIE DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHTVERLETZUNG, SIND AUSGESCHLOSSEN, AUSSER WENN EIN DERARTIGER GEWÄHRLEISTUNGSAUSSCHLUSS RECHTLICH ALS UNGÜLTIG ANGESEHEN WIRD.

FC CE RoHS

Alle Marken und Markennamen sind Eigentum der jeweiligen Besitzer.

Konform mit Trade Agreements Act (TAA)

# Inhaltsverzeichnis

Einführung ..... 43
Lieferumfang ..... 43
1. diskAshur PRO²-LED-Zustände ..... 44
2. Erstmalige Verwendung der diskAshur PRO² ..... 44
3. Entsperren der diskAshur PRO² ..... 45
4. Sperren der diskAshur PRO² ..... 45
5. Zugreifen im Admin-Modus ..... 45
6. Ändern der Admin-PIN ..... 46
7. Festlegen einer Benutzer-PIN-Richtlinie ..... 47
8. So überprüfen Sie die Benutzer-PIN-Richtlinie ..... 48
9. Hinzufügen einer neuen Benutzer-PIN im Admin-Modus ..... 49
10. Ändern der Benutzer-PIN im Admin-Modus ..... 49
11. Löschen der Benutzer-PIN im Admin-Modus ..... 49
12. Festlegen des schreibgeschützten Zugriffs im Admin-Modus ..... 50
13. Aktivieren des Lese-/Schreibzugriffs im Admin-Modus ..... 50
14. Erstellen einer Selbstzerstörungs-PIN ..... 50
15. Löschen der Selbstzerstörungs-PIN ..... 51
16. Entsperren mit der Selbstzerstörungs-PIN ..... 51
17. Erstellen einer Admin-PIN nach einem Brute Force-Angriff oder dem Zurücksetzen ..... 52
18. Festlegen der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“ ..... 52
19. Deaktivieren der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“ ..... 53
20. Überprüfen der automatischen Sperre ..... 53
21. Entsperren der diskAshur PRO² mit Benutzer-PIN ..... 54
22. Ändern der Benutzer-PIN im Benutzermodus ..... 54
23. Festlegen des schreibgeschützten Zugriffs im Benutzermodus ..... 55
24. Aktivieren des Lese-/Schreibzugriffs im Benutzermodus ..... 55
25. Brute Force-Schutz ..... 56
26. Komplettes Zurücksetzen ..... 56
27. Initialisieren und Formatieren der diskAshur PRO² ..... 57
28. diskAshur PRO²-Einrichtung für Mac OS ..... 59
29. diskAshur PRO² Einrichtung für Linux (Ubuntu 17.10) ..... 61
30. Ruhezustand, Sperre oder Abmeldung beim Betriebssystem ..... 64
31. Prüfen von Firmware im Admin-Modus ..... 64
32. Prüfen von Firmware im Benutzermodus ..... 65
33. Technical Support ..... 66
34. Garantie- und RMA-Informationen ..... 66

**Anhänge**

A. iStorage Sicherheitsrichtlinie Nr. 1 – Produkt-Sicherheitsmerkmale und sicherer Umgang ..... 67
B. iStorage Sicherheitsrichtlinie Nr. 2 – Säuberung und sichere Entsorgung ..... 72




## Einführung

Eine benutzerfreundliche ultrasichere, hardwareverschlüsselte, Desktop-Festplatte mit Kapazitäten von bis zu 2 TB. Schließen Sie einfach das integrierte USB 3.1-Kabel an einen Computer an, und geben Sie eine 7- bis 15-stellige PIN ein. Wenn die korrekte PIN eingegeben wird, sind alle Daten auf der Festplatte zugänglich. Um die Festplatte zu sperren und alle Daten zu verschlüsseln, drücken Sie die Taste SPERREN auf der diskAshur PRO², oder entfernen Sie sie sicher vom Hostcomputer. Die gesamten Inhalte der Festplatte werden mit AES 256-Bit-Hardwareverschlüsselung (XTS-Modus) nach Militärstandard verschlüsselt. Wenn die Festplatte verloren geht oder gestohlen und 15 Mal hintereinander eine falsche PIN eingegeben wird, wird die Festplatte zurückgesetzt, und die Daten können nicht wiederhergestellt werden.

Eine der einzigartigen zugrundeliegenden Sicherheitsfunktionen der GDPR-kompatiblen diskAshur PRO² ist der dedizierte hardwarebasierte sichere Mikroprozessor (Common Criteria EAL4+-fähig), der integrierte physische Schutzmechanismen nutzt, um Schutz gegen externe Manipulationen, Bypass-Angriffe und Fault Injections zu bieten. Im Gegensatz zu anderen Lösungen reagiert die diskAshur PRO² auf einen automatischen Angriff, indem sie in den Deadlock-Zustand wechselt (einfriert), sodass sich alle diese Angriffe als vergeblich erweisen. Einfach ausgedrückt: Ohne PIN ist kein Zugriff möglich!

## Lieferumfang

1. diskAshur PRO²-Festplatte mit integriertem USB-Kabel
2. Eleganter Transportbehälter
3. Schnellstartanleitung

**ACHTUNG: Unbedingt vor Inbetriebnahme lesen:**
iStorage empfiehlt aus Sicherheitsgründen, dass Sie vor der ersten Benutzung des diskAshur PRO² eine der folgenden Aktionen durchführen:

1. Ändern Sie die vorbelegte Admin PIN (11223344) umgehend, wie in Kapitel 6 "**Ändern der Admin-Pin**" beschrieben. Im Anschluss legen Sie bitte eine neue User PIN an, wie in Kapitel 9 "**Hinzufügen einer neuen Benutzer-PIN im Admin Modus**" erklärt.

**ODER**

2. Setzen Sie den diskAshur PRO² zurück, wie in Kapitel 26 "**Komplettes Zurücksetzen**" beschrieben. Im Anschluss legen Sie bitte eine neue Admin PIN an, wie in Kapitel 17 "**Erstellen einer Admin-PIN nach einem Brute Force-Angriff oder dem Zurücksetzen**" erläutert.

## 1. diskAshur PRO²-LED-Zustände

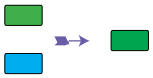
Wenn die diskAshur PRO² angeschlossen wird, gibt es drei mögliche Anzeigevarianten der LEDs (siehe Tabelle unten).

| ROT | GRÜN | BLAU | diskAshur PRO²-Zustand |
|---|---|---|---|
| Leuchtet | Aus | Aus | Factory Reset [1] |
| Leuchtet | Leuchtet | Leuchtet | Brute Force [2] |
| Leuchtet | Aus | Aus | Standby [3] |

1. Im Factory Reset-Zustand wartet die Festplatte darauf, dass eine Admin-PIN eingerichtet wird.
2. Im Brute Force-Zustand wartet die Festplatte auf weitere PIN-Eingabeversuche.
3. Im Standby-Zustand wartet die Festplatte auf das Entsperren der Festplatte, das Wechseln in den Admin-Modus oder das Zurücksetzen der Festplatte.

## 2. Erstmalige Verwendung der diskAshur PRO²

Ihre diskAshur PRO² wird mit der standardmäßigen Admin-PIN **11223344** ausgeliefert. Obwohl die Festplatte direkt mit der standardmäßigen Admin-PIN verwendet werden kann, **empfehlen wird aus Sicherheitsgründen dringend die umgehende Erstellung einer neuen Admin-PIN**. Befolgen Sie dabei die Anweisungen unter Abschnitt 6 „Ändern der Admin-PIN".
Um die diskAshur PRO² zum ersten Mal mit der standardmäßigen Admin-PIN zu entsperren, befolgen Sie die 3 einfachen Schritte in der Tabelle unten.

| Anweisungen – erstmalige Verwendung | LED | LED-Zustand |
|---|---|---|
| 1. Schließen Sie die diskAshur PRO² an einen USB-Port an. |  | ROTE LED leuchtet und wartet auf PIN-Eingabe |
| 2. Geben Sie die Admin-PIN ein (Standard: 11223344). |  | ROTE LED leuchtet |
| 3. Drücken Sie innerhalb von 10 Sekunden einmal die Taste **ENTSPERREN**, um die diskAshur PRO² zu entsperren. |  | Die GRÜNE und BLAUE LED blinken abwechselnd mehrere Male. Anschließend sollte die Anzeige wie folgt sein: BLAUE LED leuchtet, GRÜNE LED blinkt, GRÜNE LED leuchtet. |

**Hinweis**: Nachdem die diskAshur PRO² erfolgreich entsperrt wurde, leuchtet die GRÜNE LED weiter. Die Festplatte kann umgehend gesperrt werden, indem Sie einmal die Taste **SPERREN** drücken oder auf das Symbol „Hardware sicher entfernen/Auswerfen" Ihres Betriebssystems klicken. Um sicherzustellen, dass keine Daten beschädigt werden, empfehlen wir die Verwendung von „Hardware sicher entfernen/Auswerfen".

## 3. Entsperren der diskAshur PRO²

Die diskAshur PRO² kann mit der Admin- oder Benutzer-PIN im Standby-Zustand (ROTE LED leuchtet) entsperrt werden.

1. Um sie als Administrator zu entsperren, geben Sie die **Admin**-PIN ein, und drücken Sie die Taste **ENTSPERREN**.
2. Um sie als **Benutzer** zu entsperren, drücken Sie die Taste **ENTSPERREN** (alle LEDs  blinken), geben Sie die **Benutzer**-PIN ein, und drücken Sie erneut die Taste **ENTSPERREN**.
3. Wenn die korrekte Benutzer-PIN eingegeben wird, blinken die GRÜNE und BLAUE LED abwechselnd und dann leuchtet die GRÜNE LED.
4. Wenn die korrekte Admin-PIN eingegeben wird, blinken die GRÜNE und BLAUE LED abwechselnd. Dann leuchtet die BLAUE LED 1 Sekunde, bevor der Entsperrt-Zustand angezeigt wird und die GRÜNE LED leuchtet.
5. Wenn die korrekte PIN eingegeben wird, wird die Festplatte als „iStorage diskAshur PRO²-USB-Gerät“ unter „Computer-verwaltung/Geräte-Manager“ angezeigt.

Im Entsperrt-Zustand (GRÜNE LED) gibt es zwei mögliche Anzeigevarianten der LEDs (siehe Tabelle unten).

| ROT | GRÜN | BLAU | diskAshur PRO² |
|---|---|---|---|
| Aus | Leuchtet | Aus | Keine Datenübertragung |
| Aus | Blinkt | Aus | Datenübertragung |

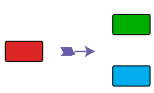
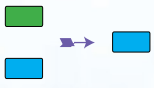
## 4. Sperren der diskAshur PRO²

Die Festplatte kann gesperrt werden, indem Sie einmal die Taste **SPERREN** drücken oder auf das Symbol „Hardware sicher entfernen/Auswerfen“ Ihres Betriebssystems klicken. Wenn Daten weiter auf die Festplatte geschrieben werden, warten Sie, bis alle Daten auf die Festplatte geschrieben wurden, bevor Sie die Taste SPERREN drücken oder die Hardware sicher vom Betriebssystem entfernen. Wenn das Timeout für „Automatische Sperre, wenn unbeaufsichtigt“ aktiviert ist, wird die Festplatte automatisch nach einem vorab festgelegten Zeitraum gesperrt.

**Hinweis:** Die diskAshur PRO² kann vom Betriebssystem im Standby-Zustand nicht erkannt werden.

## 5. Zugreifen im Admin-Modus

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

| | | |
|---|---|---|
| 1. Halten Sie im Standby-Zustand (ROTE LED leuchtet) die Tasten **ENTSPERREN + 1** gedrückt. |  | Statt der leuchtenden ROTEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt. |
| 2. Geben Sie die Admin-PIN (Standard: 11223344) ein, und drücken Sie die Taste **ENTSPERREN**. |  | Die GRÜNE und BLAUE LED blinken einige Sekunden schnell. Anschließend leuchtet die GRÜNE LED und dann die BLAUE LED. Dies gibt an, dass sich die diskAshur PRO² im Admin-Modus befindet. |

Um den Admin-Modus zu verlassen, drücken Sie die Taste **SPERREN**.

# 6. Ändern der Admin-PIN

PIN – Anforderungen:

- Muss zwischen 7 und 15 Ziffern aufweisen
- Darf nicht nur gleiche Ziffern enthalten, z. B. (3-3-3-3-3-3-3)
- Darf nicht nur sequenzielle Ziffern 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 Wort, einen Namen, eine Phrase oder eine andere alphanumerische PIN-Kombination erstellen, die aussagekräftig ist, indem Sie einfach die Taste mit den entsprechenden Buchstaben drücken.

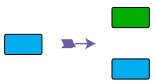
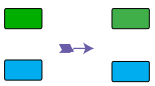
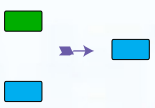
**Beispiele für alphanumerische PINs sind:**

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

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

**Hinweis:** Die Taste **SHIFT** kann für zusätzliche Kombinationen verwendet werden. **SHIFT** + 1 ist ein separater Wert zu 1. Um eine PIN mit zusätzlichen Kombinationen zu erstellen, halten Sie die Taste **SHIFT** während der Eingabe Ihrer 7- bis 15-stelligen PIN gedrückt. Z. B. **SHIFT** + **26756498**.

Um die Admin-PIN zu ändern, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **ENTSPERREN + 2** gedrückt. |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 2. Geben Sie die NEUE Admin-PIN ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der blinkenden GRÜNEN LED und der leuchtenden BLAUEN LED wird eine einzelne blinkende GRÜNE LED angezeigt. Dann werden wieder eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 3. Geben Sie die NEUE Admin-PIN erneut ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der blinkenden GRÜNEN und leuchtenden BLAUEN LED wird eine schnell blinkende BLAUE LED und dann eine leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Admin-PIN erfolgreich geändert wurde. |

# 7. Festlegen einer Benutzer-PIN-Richtlinie

Der Administrator kann eine Einschränkungsrichtlinie für die Benutzer-PIN festlegen. Diese Richtlinie umfasst das Festlegen der PIN-Mindestlänge (7 bis 15 Zeichen) sowie, ob '**Sonderzeichen**' gefordert werden oder nicht. "Sonderzeichen" lassen sich eingeben mithilfe von '**Shift + Ziffer**'

Um eine Benutzer-PIN-Richtlinie festzulegen (Einschränkungen), müssen Sie 3 Ziffern eingeben, etwa '**091**'. Die ersten beiden Ziffern (**09**) geben die Mindest-PIN-Länge an (in diesem Fall **9**) und die letzte Ziffer (**1**) kennzeichnet, dass ein „Sonderzeichen" verwendet werden muss, anders gesagt '**Shift + Ziffer**'. Gleichermaßen kann eine Benutzer-PIN-Richtlinie ohne „Sonderzeichen" festgelegt werden, etwa: '**120**'. Hier geben die ersten beiden Ziffern (**12**) die Mindest-PIN-Länge an (in diesem Fall **12**), während die letzte Ziffer (**0**) angibt, dass kein Sonderzeichen erforderlich ist.

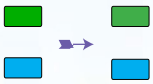
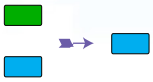
Wenn der Administrator die Benutzer-PIN-Richtlinie festgelegt hat, etwa „091", muss eine neue Benutzer-PIN erstellt werden. Wenn der Administrator die Benutzer-PIN als '**247688314**' festlegt, unter Verwendung eines '**Sonderzeichens**' (Shift+Ziffer), kann dieses Sonderzeichen bei der Erstellung der Benutzer-PIN an beliebiger Stelle in der 7-15-stelligen PIN platziert werden, wie in folgenden Beispielen gezeigt.

**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**',

**Hinweis:**

- Wenn ein „Sonderzeichen" bei der Erstellung der Benutzer-PIN verwendet wurde, etwa '**B**' wie oben, kann das Laufwerk nur durch Eingabe der PIN mit dem „Sonderzeichen" in genau der gleichen Reihenfolge entsperrt werden, wie bei '**B**' oben - also ('2', '4', '**Shift + 7**', '6', '8', '8', '3', '1', '4').
- Benutzer können ihre PIN ändern, müssen sich aber (falls zutreffend) an die festgelegten PIN-Einschränkungen halten.
- Das Festlegen einer neuen Benutzer-PIN-Richtlinie löscht automatisch eine vorhandene Richtlinie.
- Diese Richtlinie gilt nicht für die „Selbstzerstörungs-PIN". Die Komplexitätseinstellung für die Selbstzerstörungs-und Administrator-PIN sieht stets 7-15 Zeichen ohne Sonderzeichen vor.

Um eine **Benutzer-PIN-Richtlinie** festzulegen, rufen Sie zunächst den "**Administratormodus**" wie in Abschnitt 5 beschrieben auf. Befindet sich das Laufwerk im **Administratormodus** (durchgehend BLAUE LED), gehen Sie wie folgt vor.

| | | |
|---|---|---|
| 1. Drücken und halten Sie im Administratormodus die Tasten "**ENTSPERREN + 7**" |  | Die durchgehend BLAUEN LEDs blinken jetzt GRÜN und BLAU |
| 2. Geben Sie Ihre **3 Ziffern** ein. Die ersten zwei Ziffern geben die Mindest-PIN-Länge an, die letzte Ziffer (0 oder 1) gibt an, ob ein Sonderzeichen verwendet wird. |  | Die blinkende GRÜNE und durchgehend BLAUE LED blinken weiter |
| 3. Drücken Sie einmal die Taste **SHIFT** ( ⬆ ) |  | Die GRÜN blinkende und durchgehend BLAUE LED wechseln zu durchgehend GRÜN und schließlich durchgehend BLAU und zeigen so an, dass die Benutzer-PIN-Richtlinie erfolgreich festgelegt wurde. |

## 8. So überprüfen Sie die Benutzer-PIN-Richtlinie

Der Administrator kann die Benutzer-PIN-Richtlinie überprüfen und die Mindest-PIN-Länge sowie die Notwendigkeit eines Sonderzeichens ermitteln, indem er die nachfolgend beschriebene LED-Sequenz notiert.

Um eine Benutzer-PIN-Richtlinie zu ermitteln, rufen Sie zunächst den "**Administratormodus**" wie in Abschnitt 5 beschrieben auf. Befindet sich das Laufwerk im **Administratormodus** (durchgehend BLAUE LED), gehen Sie wie folgt vor.

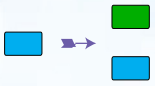
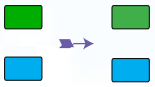
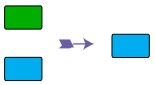
| | | |
|---|---|---|
| 1. Drücken und halten Sie im Administratormodus die Tasten **SHIFT** ( ⬆ ) + **7** |  | Die durchgehend BLAUEN LEDs blinken jetzt GRÜN und BLAU |
| 2. Drücken Sie die Taste „**ENTSPERREN**" und Folgendes geschieht:<br><br>a. Alle LEDs (ROT, GRÜN UND BLAU) leuchten 1 Sekunde durchgehend.<br>b. Ein ROTES LED-Blinken entspricht zehn (10) Einheiten einer PIN.<br>c. Ein GRÜNES LED-Blinken entspricht einer (1) Einheit einer PIN<br>d. Ein BLAUES Blinken zeigt an, dass ein „Sonderzeichen" verwendet wurde.<br>e. Alle LEDs (ROT, GRÜN UND BLAU) leuchten 1 Sekunde durchgehend.<br>f. Die LEDs leuchten wieder durchgehend BLAU | | |

Die nachfolgende Tabelle beschreibt das LED-Verhalten beim Prüfen der Benutzer-PIN-Richtlinie. Wenn Sie etwa eine 12-stellige Benutzer-PIN mit Sonderzeichen konfiguriert haben, blinkt die ROTE LED einmal (**1**) und die GRÜNE LED blinkt zweimal (**2**), gefolgt von einer einmal blinkenden BLAUEN LED, die kennzeichnet, dass ein **Sonderzeichen** verwendet wurde.

| PIN-Beschreibung | 3-Ziffern- | ROT | GRÜN | BLAU |
|---|---|---|---|---|
| 12-stellige PIN mit Sonderzeichen | 121 | 1 x Blinken | 2 x Blinken | 1 x Blinken |
| 112-stellige PIN OHNE Sonderzeichen | 120 | 1 x Blinken | 2 x Blinken | 0 |
| 9-stellige PIN mit Sonderzeichen | 091 | 0 | 9 x Blinken | 1 x Blinken |
| 9-stellige PIN OHNE Sonderzeichen | 090 | 0 | 9 x Blinken | 0 |

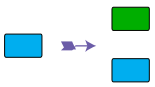
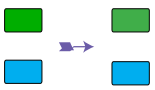
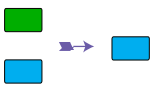
## 9. Hinzufügen einer neuen Benutzer-PIN im Admin-Modus

Um einen **neuen Benutzer** hinzuzufügen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **ENTSPERREN + 3** gedrückt. |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 2. Geben Sie Ihre neue Benutzer-PIN ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der blinkenden GRÜNEN LED und der leuchtenden BLAUEN LED wird eine einzelne blinkende GRÜNE LED angezeigt. Dann werden wieder eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 3. Geben Sie die neue Benutzer-PIN erneut ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der einige Sekunden schnell blinkenden GRÜNEN LED wird eine leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Benutzer-PIN erfolgreich erstellt wurde. |

## 10. Ändern der Benutzer-PIN im Admin-Modus

Um eine vorhandene **Benutzer-PIN** zu ändern, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **ENTSPERREN + 3** gedrückt. |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 2. Geben Sie Ihre neue Benutzer-PIN ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der blinkenden GRÜNEN LED und der leuchtenden BLAUEN LED wird eine einzelne blinkende GRÜNE LED angezeigt. Dann werden wieder eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 3. Geben Sie die neue Benutzer-PIN erneut ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der einige Sekunden schnell blinkenden GRÜNEN LED wird eine leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Benutzer-PIN erfolgreich geändert wurde. |

## 11. Löschen der Benutzer-PIN im Admin-Modus

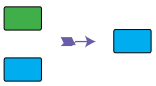
Um eine **Benutzer-PIN** zu löschen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **SHIFT** ( ⬆ ) **+ 3** gedrückt. |  | Statt der leuchtenden BLAUEN LED wird eine blinkende ROTE LED angezeigt. |
| 2. Halten Sie die Tasten **SHIFT** ( ⬆ ) **+ 3** erneut gedrückt. |  | Statt der blinkenden ROTEN LED wird eine leuchtende ROTE LED und dann eine leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Benutzer-PIN erfolgreich gelöscht wurde. |

## 12. Festlegen des schreibgeschützten Zugriffs im Admin-Modus

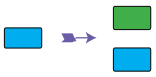
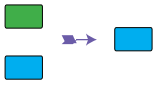
**Wichtig:** Wenn Daten gerade auf die diskAshur PRO² kopiert wurden, trennen Sie die Festplatte zunächst ordnungsgemäß, indem Sie auf „Hardware sicher entfernen/Auswerfen“ für die diskAshur PRO² im Betriebssystem klicken, bevor Sie sie erneut anschließen und die diskAshur PRO² als „Schreibgeschützt“ festlegen.

Wenn der Admin Inhalte auf die diskAshur PRO² schreibt und den Zugriff auf „Schreibgeschützt“ festlegt, kann der Benutzer diese Einstellung nicht im Benutzermodus ändern. Um die diskAshur PRO² auf „Schreibgeschützt“ festzulegen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **7 + 6** gedrückt. (7=**R**ead + 6=**O**nly) |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt. |
| 2. Lassen Sie die Tasten „7 + 6“ los, und drücken Sie **ENTSPERREN**. |  | Die GRÜNE und BLAUE LED ändern sich in eine leuchtende GRÜNE LED und dann in eine leuchtende BLAUE LED. Dies gibt an, dass die Festplatte als „Schreibgeschützt“ konfiguriert ist. |

## 13. Aktivieren des Lese-/Schreibzugriffs im Admin-Modus

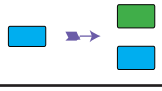
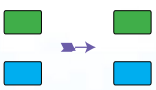
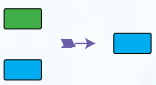
Um die diskAshur PRO² auf „Lesen/Schreiben“ festzulegen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **7 + 9** gedrückt . (7=**R**ead + 9=**W**rite) |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt. |
| 2. Lassen Sie die Tasten „7 + 9“ los, und drücken Sie **ENTSPERREN**. |  | Die GRÜNE und BLAUE LED ändern sich in eine leuchtende GRÜNE LED und dann in eine leuchtende BLAUE LED. Dies gibt an, dass die Festplatte als „Lesen/Schreiben“ konfiguriert ist. |

## 14. Erstellen einer Selbstzerstörungs-PIN

Die Selbstzerstörungsfunktion ermöglicht es Ihnen, eine PIN festzulegen, mit der Sie einen Crypto-Erase für die gesamte Festplatte durchführen können. Die Selbstzerstörungs-PIN **löscht ALLE Daten und Admin/Benutzer-PINs** und entsperrt die Festplatte dann. Die Aktivierung dieser Funktion führt dazu, dass die Selbstzerstörungs-PIN die neue Benutzer-PIN wird und die diskAshur PRO² partitioniert und formatiert werden muss, bevor neue Daten zur Festplatte hinzugefügt werden können.

Um die Selbstzerstörungs-PIN festzulegen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **ENTSPERREN + 6** gedrückt. |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 2. Erstellen Sie eine 7- bis 15-stellige Selbstzerstörungs-PIN, und drücken Sie die Taste **ENTSPERREN** . |  | Statt der blinkenden GRÜNEN LED und der leuchtenden BLAUEN LED wird eine einzelne blinkende GRÜNE LED angezeigt. Dann werden wieder eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 3. Geben Sie die PIN erneut ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der einige Sekunden schnell blinkenden GRÜNEN LED wird eine leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Selbstzerstörungs-PIN erfolgreich konfiguriert wurde. |

## 15. Löschen der Selbstzerstörungs-PIN

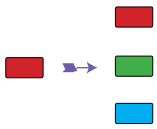
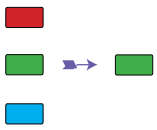
Um die Selbstzerstörungs-PIN zu löschen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **SHIFT** ( ⬆ ) **+ 6** gedrückt. |  | Statt der leuchtenden BLAUEN LED wird eine blinkende ROTE LED angezeigt. |
| 2. Halten Sie die Tasten **SHIFT** ( ⬆ ) **+ 6** erneut gedrückt. |  | Statt der blinkenden ROTEN LED wird eine leuchtende ROTE LED und dann eine leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Selbstzerstörungs-PIN erfolgreich gelöscht wurde. |

## 16. Entsperren mit der Selbstzerstörungs-PIN

Die Selbstzerstörungs-PIN **löscht den Verschlüsselungsschlüssel, ALLE Daten und Admin/Benutzer-PINs** und entsperrt die Festplatte dann. Die Aktivierung dieser Funktion führt dazu, dass die **Selbstzerstörungs-PIN die neue Benutzer-PIN wird** und die diskAshur PRO² partitioniert und formatiert werden muss, bevor neue Daten zur Festplatte hinzugefügt werden können.

Um den Selbstzerstörungsmechanismus zu aktivieren, muss sich die Festplatte im Standby-Zustand (ROTE LED leuchtet) befinden. Führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Drücken Sie im Standby-Zustand die Taste **ENTSPERREN**. |  | Statt der ROTEN LED werden alle LEDs angezeigt (ROT, GRÜN und BLAU) und blinken. |
| 2. Geben Sie die Selbstzerstörungs-PIN ein, und drücken Sie die Taste **ENTSPERREN**. |  | Die blinkenden ROTEN, GRÜNEN und BLAUEN LEDs ändern sich in ca. 15 Sekunden blinkende GRÜNE und BLAUE LEDs und dann in eine GRÜN leuchtende LED. |

**Wichtig:** Wenn der Selbstzerstörungsmechanismus aktiviert ist, werden alle Daten, der Verschlüsselungsschlüssel und die Admin-/Benutzer-PINs gelöscht. **Die Selbstzerstörungs-PIN wird zur Benutzer-PIN.** Nach der Aktivierung des Selbstzerstörungsmechanismus ist keine Admin-PIN vorhanden. Die diskAshur PRO² muss zunächst zurückgesetzt werden (siehe Komplettes Zurücksetzen in Abschnitt 26 auf Seite 56), um eine Admin-PIN mit umfassenden Admin-Privilegien (einschließlich Erstellung einer Benutzer-PIN) zu erstellen.

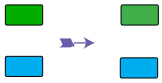
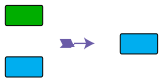
## 17. Erstellen einer Admin-PIN nach einem Brute Force-Angriff oder dem Zurücksetzen

Nach einem Brute Force-Angriff oder dem Zurücksetzen der diskAshur PRO² muss eine Admin-PIN erstellt werden, bevor die Festplatte verwendet werden kann. Nach einem Brute Force-Angriff oder dem Zurücksetzen befindet sich die Festplatte im Standby-Zustand (ROTE LED leuchtet). Um eine Admin-PIN zu erstellen, gehen Sie wie folgt vor.

**PIN – Anforderungen:**

- Muss zwischen 7 und 15 Ziffern aufweisen
- Darf nicht nur gleiche Ziffern enthalten, z. B. (3-3-3-3-3-3-3)
- Darf nicht nur sequenzielle Ziffern 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)

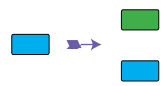
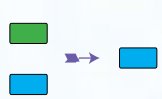
**Hinweis:** Die Taste **SHIFT** kann für zusätzliche Kombinationen verwendet werden. **SHIFT** + 1 ist ein separater Wert zu 1. Um eine PIN mit zusätzlichen Kombinationen zu erstellen, halten Sie die Taste **SHIFT** während der Eingabe Ihrer 7- bis 15-stelligen PIN gedrückt. Z. B. **SHIFT** + **26756498**.

| | | |
|---|---|---|
| 1. Halten Sie im Standby-Zustand die Tasten **Shift** ( ⬆ ) + **1** gedrückt. |  | Statt der leuchtenden ROTEN LED werden eine blinkende GRÜNE und eine leuchtende BLAUE LED angezeigt. |
| 2. Geben Sie die NEUE Admin-PIN ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der blinkenden GRÜNEN LED und der leuchtenden BLAUEN LED wird eine einzelne blinkende GRÜNE LED angezeigt. Dann werden wieder eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 3. Geben Sie die NEUE Admin-PIN erneut ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der blinkenden GRÜNEN und leuchtenden BLAUEN LED wird eine einige Sekunden schnell blinkende BLAUE LED und dann eine leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Admin-PIN erfolgreich konfiguriert wurde. |

## 18. Festlegen der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“

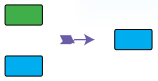
Um die Festplatte vor nicht autorisiertem Zugriff zu schützen, wenn sie entsperrt und unbeaufsichtigt ist, kann festgelegt werden, dass die diskAshur PRO² automatisch nach einem vorab ausgewählten Zeitraum gesperrt wird. Standardmäßig ist die Funktion „Automatische Sperre, wenn unbeaufsichtigt“ der diskAshur PRO² deaktiviert. „Automatische Sperre, wenn unbeaufsichtigt“ kann auf 5 bis 99 Minuten festgelegt werden.

Um „Automatische Sperre, wenn unbeaufsichtigt“ festzulegen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **ENTSPERREN + 5** gedrückt. |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt. |
| 2. Geben Sie den Zeitraum für „Automatische Sperre, wenn unbeaufsichtigt“ ein, mindestens 5 Minuten und maximal 99 Minuten (5 bis 99 Minuten). Geben Sie beispielsweise Folgendes ein:<br>**05 für 5 Minuten**<br>**20 für 20 Minuten**<br>**99 für 99 Minuten** | | |
| 3. Drücken Sie die Taste **SHIFT** ( ⬆ ). |  | Die blinkende GRÜNE und blinkende BLAUE LED ändern sich eine Sekunde in eine leuchtende GRÜNE LED und dann in eine leuchtende BLAUE LED. Dies gibt an, dass das Timeout für die automatische Sperre erfolgreich konfiguriert wurde. |

## 19. Deaktivieren der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“

Um „Automatische Sperre, wenn unbeaufsichtigt“ zu deaktivieren, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten **ENTSPERREN + 5** gedrückt. |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt. |
| 2. Geben Sie **00** ein, und drücken Sie die Taste **SHIFT** ( ⬆ ). |  | Die blinkende GRÜNE und blinkende BLAUE LED ändern sich eine Sekunde in eine leuchtende GRÜNE LED und dann in eine leuchtende BLAUE LED. Dies gibt an, dass das Timeout für die automatische Sperre erfolgreich deaktiviert wurde. |

## 20. Überprüfen der automatischen Sperre

Der Administrator kann die festgelegte Länge für die automatische Sperre ermitteln, indem er die LED-Sequenz der nachstehenden Tabelle notiert.

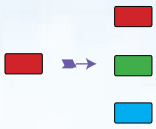
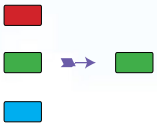
Um die automatische Sperre zu ermitteln, rufen Sie zunächst den “**Administratormodus**” wie in Abschnitt 5 beschrieben auf. Befindet sich das Laufwerk im **Administratormodus** (durchgehend BLAUE LED), gehen Sie wie folgt vor.

| | | |
|---|---|---|
| 1. Drücken und halten Sie im Administratormodus die Tasten **SHIFT** ( ⬆ ) + **5** |  | Die durchgehend BLAUEN LEDs blinken jetzt GRÜN und BLAU |
| 2. Drücken Sie die Taste „**ENTSPERREN**” und Folgendes geschieht:<br><br>a. Alle LEDs (ROT, GRÜN UND BLAU) leuchten 1 Sekunde durchgehend.<br>b. Ein ROTES LED-Blinken entspricht zehn (10) Minuten.<br>c. Ein GEÜNES LED-Blinken entspricht einer (1) Minute.<br>d. Alle LEDs (ROT, GRÜN UND BLAU) leuchten 1 Sekunde durchgehend.<br>e. Die LEDs leuchten wieder durchgehend BLAU | | |

Die nachstehende Tabelle beschreibt das LED-Verhalten beim Überprüfen der automatischen Sperre. Wenn Sie das Laufwerk beispielsweise auf eine Sperrung nach **26** Minuten konfiguriert haben, blinkt die ROTE LED zweimal (**2**) und die GRÜNE LED sechsmal (**6**).

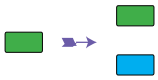
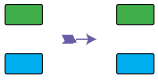
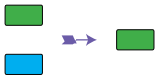
| Autom. Sperre in Minuten | ROT | GRÜN |
|---|---|---|
| 8 minutes | 0 | 8 x Blinken |
| 15 minutes | 1 x Blinken | 5 x Blinken |
| 26 minutes | 2 x Blinken | 6 x Blinken |
| 40 minutes | 4 x Blinken | 0 |

## 21. Entsperren der diskAshur PRO² mit Benutzer-PIN

| | | |
|---|---|---|
| 1. Drücken Sie im Standby-Zustand (ROTE LED leuchtet) die Taste **ENTSPERREN**. |  | Statt der ROTEN LED werden alle LEDs angezeigt (ROT, GRÜN und BLAU) und blinken. |
| 2. Geben Sie die Benutzer-PIN ein, und drücken Sie die Taste **ENTSPERREN**. |  | Die blinkenden ROTEN, GRÜNEN und BLAUEN LEDs ändern sich in blinkende GRÜNE und BLAUE LEDs, dann in eine schnell blinkende GRÜNE LED und schließlich in eine leuchtende GRÜNE LED. Dies gibt an, dass die Festplatte erfolgreich im Benutzermodus entsperrt wurde. |

## 22. Ändern der Benutzer-PIN im Benutzermodus

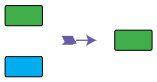
Um die **Benutzer-PIN** zu ändern, entsperren Sie zunächst die diskAshur PRO² mit einer Benutzer-PIN, wie oben in Abschnitt 21 beschrieben. Wenn sich die Festplatte im **Benutzermodus** befindet (GRÜNE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Benutzermodus die Tasten **ENTSPERREN + 4** gedrückt. |  | Statt der leuchtenden GRÜNEN LED werden eine blinkende GRÜNE und eine leuchtende BLAUE LED angezeigt. |
| 2. Geben Sie die neue Benutzer-PIN ein, und drücken Sie die Taste **ENTSPERREN**. |  | Statt der blinkenden GRÜNEN LED und der leuchtenden BLAUEN LED wird eine einzelne blinkende GRÜNE LED angezeigt. Dann werden wieder eine blinkende GRÜNE LED und eine leuchtende BLAUE LED angezeigt. |
| 3. Geben Sie die neue Benutzer-PIN erneut ein, und drücken Sie die Taste **ENTSPERREN**. |  | Die blinkende GRÜNE und die leuchtende BLAUE LED ändern sich in eine schnell blinkende GRÜNE LED und dann in eine leuchtende GRÜNE LED. Dies gibt eine erfolgreiche Änderung der Benutzer-PIN an. |

## 23. Festlegen des schreibgeschützten Zugriffs im Benutzermodus

**Wichtig:** Wenn Daten gerade auf die diskAshur PRO² kopiert wurden, trennen Sie die Festplatte zunächst ordnungsgemäß, indem Sie auf „Hardware sicher entfernen/Auswerfen“ für die diskAshur PRO² im Betriebssystem klicken, bevor Sie sie erneut anschließen und die diskAshur PRO² als „Schreibgeschützt“ festlegen.

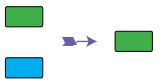
Um die diskAshur PRO² auf „Schreibgeschützt“ festzulegen, wechseln Sie zuerst in den **Benutzermodus** wie in Abschnitt 21 beschrieben. Wenn sich die Festplatte im **Benutzermodus** befindet (GRÜNE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Benutzermodus die Tasten **7 + 6** gedrückt . (7=**R**ead + 6=**O**nly) |  | Die leuchtende GRÜNE LED ändert sich in eine blinkende GRÜNE und eine blinkende BLAUE LED. |
| 2. Lassen Sie die Tasten „7 + 6“ los, und drücken Sie **ENTSPERREN**. |  | Die GRÜNE und BLAUE LED ändern sich in eine leuchtende GRÜNE LED. Dies gibt an, dass die Festplatte als „Schreibgeschützt“ konfiguriert ist. |

**Hinweis:**
1. Diese Einstellung wird aktiviert, wenn die Festplatte das nächste Mal entsperrt wird.
2. Wenn ein Benutzer die Festplatte als „Schreibgeschützt“ festgelegt hat, kann der Admin dies durch Festlegen der Festplatte als „Lesen/Schreiben“ im Admin-Modus überschreiben.
3. Wenn ein Admin die Festplatte als „Schreibgeschützt“ festgelegt hat, kann der Benutzer die Festplatte nicht als „Lesen/Schreiben“ festlegen.

## 24. Aktivieren des Lese-/Schreibzugriffs im Benutzermodus

Um die diskAshur PRO² auf „Lesen/Schreiben“ festzulegen, wechseln Sie zuerst in den **Benutzermodus** wie in Abschnitt 21 beschrieben. Wenn sich die Festplatte im **Benutzermodus** befindet (GRÜNE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Benutzermodus die Tasten **7 + 9** gedrückt . (7=**R**ead + 9=**W**rite) |  | Die leuchtende GRÜNE LED ändert sich in eine blinkende GRÜNE und eine blinkende BLAUE LED. |
| 2. Lassen Sie die Tasten „7 + 9“ los, und drücken Sie **ENTSPERREN**. |  | Die GRÜNE und BLAUE LED ändern sich in eine leuchtende GRÜNE LED. Dies gibt an, dass die Festplatte als „Lesen/Schreiben“ konfiguriert ist. |

**Hinweis:**
1. Diese Einstellung wird aktiviert, wenn die Festplatte das nächste Mal entsperrt wird.
2. Wenn ein Benutzer die Festplatte als „Schreibgeschützt“ festgelegt hat, kann der Admin dies durch Festlegen der Festplatte als „Lesen/Schreiben“ im Admin-Modus überschreiben.
3. Wenn ein Admin die Festplatte als „Schreibgeschützt“ festgelegt hat, kann der Benutzer die Festplatte nicht als „Lesen/Schreiben“ festlegen.

## 25. Brute Force-Schutz

Wenn eine PIN 15 Mal (3 x 5 PIN-Gruppen) falsch eingegeben wird, werden alle Admin/Benutzer-PINs, der Verschlüsselungsschlüssel und alle Daten gelöscht und können nicht wiederhergestellt werden. Die diskAshur PRO² muss dann formatiert und partitioniert werden, bevor sie wiederverwendet werden kann.

**1.** Wenn eine PIN 5 Mal hintereinander falsch eingegeben wird, leuchten alle LEDs (ROT, GRÜN und BLAU).

**2.** Trennen Sie die Festplatte, und schließen Sie sie erneut an den Host an, um weitere 5 PIN-Versuche zu erhalten. Wenn eine PIN 5 Mal hintereinander falsch eingegeben wird (10 Mal insgesamt – 5 Mal in Schritt 1 und 5 Mal in Schritt 2), leuchten alle LEDs (ROT, GRÜN und BLAU).

**3**. Trennen Sie die Festplatte, halten Sie die Taste **SHIFT** gedrückt, und schließen Sie die Festplatte wieder an den Host an. Alle LEDs (ROT, GRÜN und BLAU )werden angezeigt und blinken.

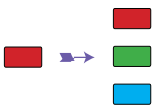
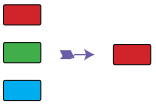
**4**. Wenn alle LEDs blinken, geben Sie **47867243** ein, und drücken Sie die Taste **ENTSPERREN**, um 5 letzte Versuche zu erhalten.

**Achtung:** Nach 15 aufeinanderfolgenden falschen PIN-Eingaben wird der Brute Force Defence-Mechanismus aktiviert. Alle Admin/Benutzer-PINs, der Verschlüsselungsschlüssel und alle Daten werden gelöscht. Eine neue Admin-PIN muss erstellt werden (siehe Abschnitt 17 auf Seite 52 Erstellen einer Admin-PIN nach einem Brute Force-Angriff oder dem Zurücksetzen). Die diskAshur PRO² muss partitioniert und formatiert werden, bevor neue Daten zur Festplatte hinzugefügt werden können.

## 26. Komplettes Zurücksetzen

Für komplettes Zurücksetzen muss sich die diskAshur PRO² im Standby-Zustand befinden (ROTE LED leuchtet). Wenn die Festplatte zurückgesetzt wird, werden alle Admin/Benutzer-PINs, der Verschlüsselungsschlüssel und alle Daten gelöscht und können nicht wiederhergestellt werden. Die Festplatte muss formatiert und partitioniert werden, bevor sie wiederverwendet werden kann.

Um die diskAshur PRO² zurückzusetzen, gehen Sie wie folgt vor.

| | | |
|---|---|---|
| 1. Halten Sie im Standby-Zustand die Taste **0** gedrückt, bis alle LEDs abwechselnd blinken. |  | Statt der leuchtenden ROTEN LED werden alle LEDs angezeigt (ROT, GRÜN und BLAU) und blinken. |
| 2. Halten Sie die Tasten **2 + 7** gedrückt, bis alle LEDs eine Sekunde leuchten und dann eine leuchtende ROTE LED angezeigt wird. |  | Die blinkende ROTE, GRÜNE und BLAUE LED ändern sich eine Sekunde in leuchtende LEDs und dann in eine leuchtende ROTE LED. Dies gibt an, dass die Festplatte zurückgesetzt wurde. |

**Wichtig:** Nach dem kompletten Zurücksetzen muss eine neue Admin-PIN erstellt werden (siehe Abschnitt 17 auf Seite 52 Erstellen einer Admin-PIN nach einem Brute Force-Angriff oder dem Zurücksetzen). Die diskAshur PRO² muss partitioniert und formatiert werden, bevor neue Daten zur Festplatte hinzugefügt werden können.

# 27. Initialisieren und Formatieren der diskAshur PRO²

Nach einem Brute Force-Angriff oder dem kompletten Zurücksetzen der diskAshur PRO² werden alle Daten, der Verschlüsselungsschlüssel und die Partitionseinstellungen gelöscht.

Sie müssen die diskAshur PRO² initialisieren und formatieren, bevor sie verwendet werden kann.

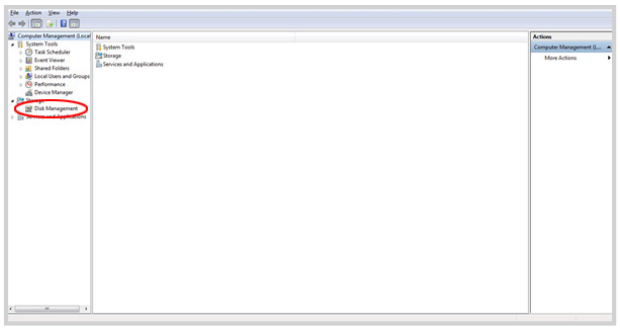
Um Ihre diskAshur PRO² zu initialisieren, gehen Sie wie folgt vor:

1. Schließen Sie die diskAshur PRO² an den Computer an.
2. Erstellen Sie eine neue Admin-PIN (siehe Seite 52, Abschnitt 17 „Erstellen einer Admin-PIN nach einem Brute Force-Angriff oder dem Zurücksetzen“).
3. Geben Sie mit der diskAshur PRO² im Standby-Zustand (ROTE LED) eine neue Admin-PIN zum Entsperren ein (GRÜNE LED).
4. **Windows 7:** Klicken Sie mit der rechten Maustaste auf **Computer** und dann auf **Verwalten** und **Datenträgerverwaltung**.

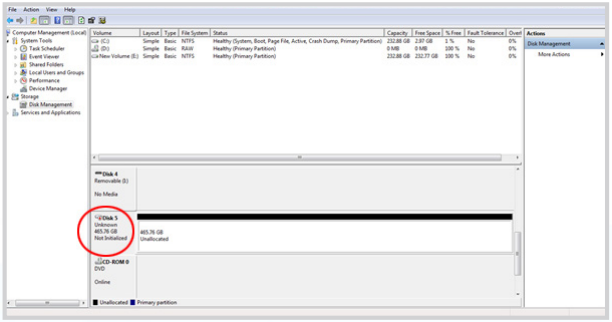
   **Windows 8**: Klicken Sie mit der rechten Maustaste in die linke Ecke des Desktops, und wählen Sie **Datenträgerverwaltung**

   **Windows 10:** Klicken Sie mit der rechten Maustaste auf die Schaltfläche „Start“, und wählen Sie **Datenträgerverwaltung**.
5. Klicken Sie im Fenster „Computerverwaltung“ auf **Datenträgerverwaltung**. Im Fenster „Datenträgerverwaltung“ wird die diskAshur PRO² als unbekanntes Gerät erkannt, das nicht initialisiert und nicht zugeordnet ist.

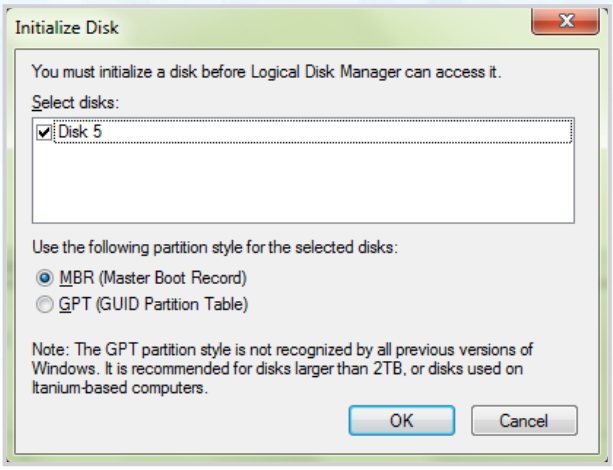
**Hinweis:** Wenn das Fenster mit dem Assistenten für die Datenträgerinitialisierung geöffnet wird, klicken Sie auf **Abbrechen**.



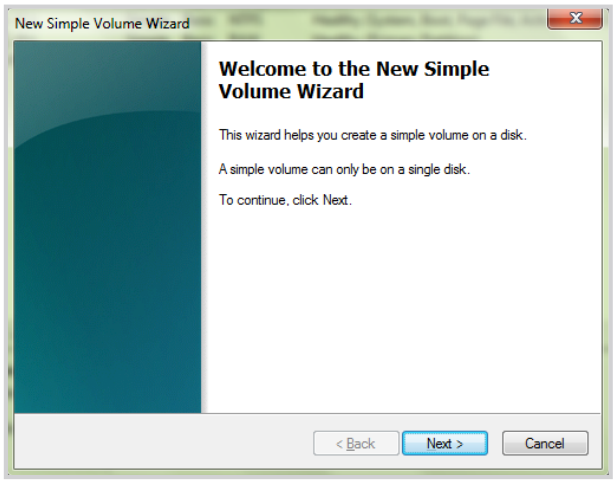
6. Klicken Sie mit der rechten Maustaste auf „Unbekannter Datenträger“, und wählen Sie dann „Datenträger initialisieren“.



7. Klicken Sie im Fenster „Datenträger initialisieren“ auf **OK**.




8. Klicken Sie mit der rechten Maustaste in den leeren Bereich unter dem Bereich „Nicht zugeordnet“, und wählen Sie dann „Neues einfaches Volume“. Das Fenster „Willkommen“ wird geöffnet.




9. Klicken Sie auf **Weiter**.

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

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

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

13. Klicken Sie auf **Fertig stellen**.

14. Warten Sie, bis der Formatierungsprozess abgeschlossen ist. Die diskAshur PRO² wird erkannt und kann verwendet werden.

# 28. diskAshur PRO²-Einrichtung für Mac OS

Ihre diskAshur PRO² ist exFAT vorformatiert. Um die Festplatte in ein Mac-kompatibles Format neu zu formatieren, lesen Sie die Anweisungen unten.

Öffnen Sie nach dem Entsperren der Festplatte das Datenträger-Dienstprogramm bei Anwendungen/Dienstprogramme/Datenträger-Dienstprogramme.

### So formatieren Sie die diskAshur PRO²:

1. Wählen Sie diskAshur PRO² aus der Liste der Laufwerke und Volumes aus. Für jedes Laufwerk in der Liste werden Kapazität, Hersteller und Produktname angezeigt, wie „iStorage diskAshur PRO²-Datenträger“ oder 232.9 diskAshur PRO².




2. Klicken Sie auf die Schaltfläche „Löschen“ (Abbildung 1).




Abbildung 1

3. Geben Sie einen Namen für das Laufwerk ein (Abbildung 2). Der Standardname ist „Unbenannt“. Der Name des Laufwerks wird schließlich auf dem Desktop angezeigt.

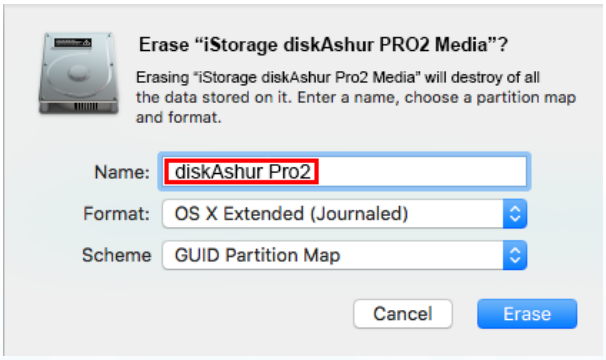



Abbildung 2

4. Wählen Sie ein Schema- und Volume-Format aus. Das Drop-down-Menü „Volume-Format“ (Abbildung 3) listet die verfügbaren Laufwerkformate auf, die der Mac unterstützt. Der empfohlene Formattyp ist „Mac OS Extended (Journaled).“ Das Drop-down-Menü „Schemaformat“ listet die verfügbaren Schemas auf (Abbildung 4). Wir empfehlen „GUID Partition Map“ auf Laufwerken größer als 2 TB.

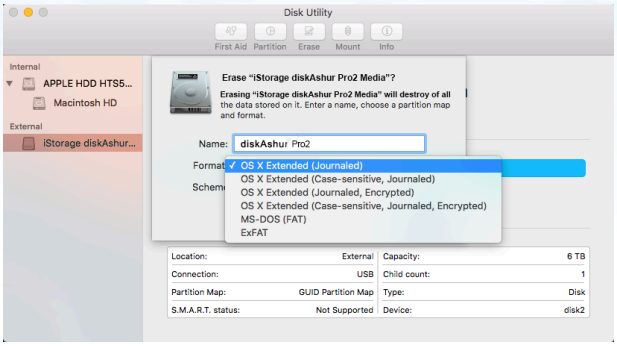


Abbildung 3

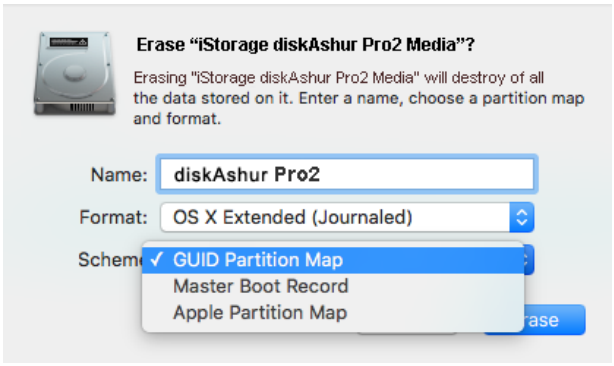


Abbildung 4

5. Klicken Sie auf die Schaltfläche „Löschen“. Das Datenträger-Dienstprogramm hebt die Bereitstellung des Volume auf dem Desktop auf, löscht es und stellt es dann wieder auf dem Desktop bereit.

# 29. diskAshur PRO² Einrichtung für Linux (Ubuntu 17.10)

Wenn Ihr iStorage diskAshur PRO² initialisiert wurde und formatiert exFAT wurde, können Sie das Laufwerk direkt auf Ubuntu verwenden.

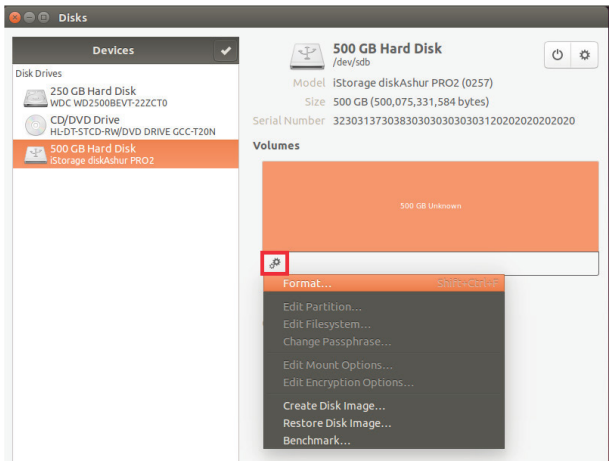
Wenn es nicht funktioniert lessen sie bitte unten weiter.

Um das iStorage diskAshur PRO² zu formatisiern als FAT 'Dateisystem'

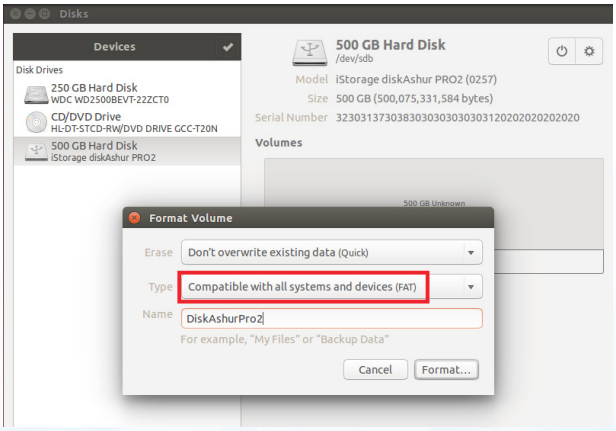
1. Öffnen sie '**Applikation anzeigen**' und schreiben sie '**Platten**' in die such taste. Klicken die dann auf das **Platte** zeichen wenn es angezeigt wird.



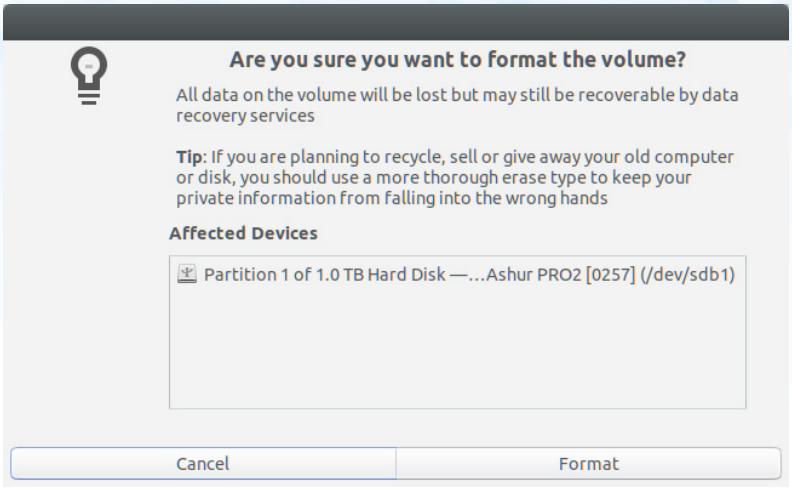

2. Klicken sie um das Laufwerk auszuwählen (500 GB Festplatte) unter "**Geräten"**. Dann drücken sie auf das zahnrad symbol unter "**Volumen"** und dann klicken sie "**Format".**



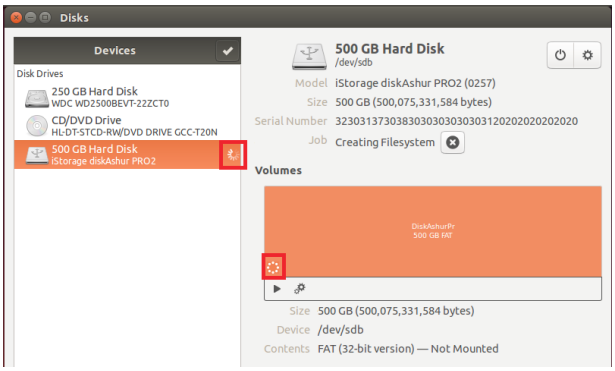

3. Wählen Sie "**Kompatibel mit allen Systemen und Geräten (FAT)**" für die Option "**Typ**". Geben Sie einen Namen für das Laufwerk ein, z. B. diskAshur PRO². Klicken Sie dann auf die Schaltfläche "**Formatieren**".



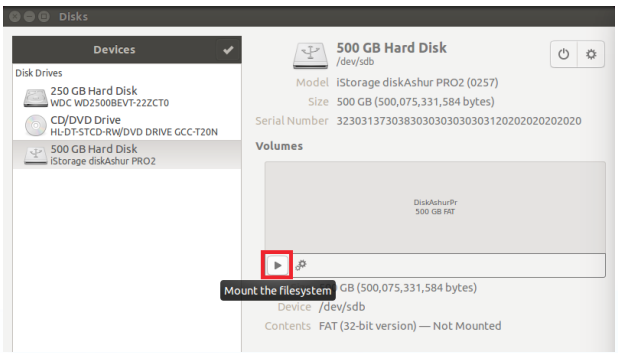
4. Klicken Sie nochmal auf “**Format**”.



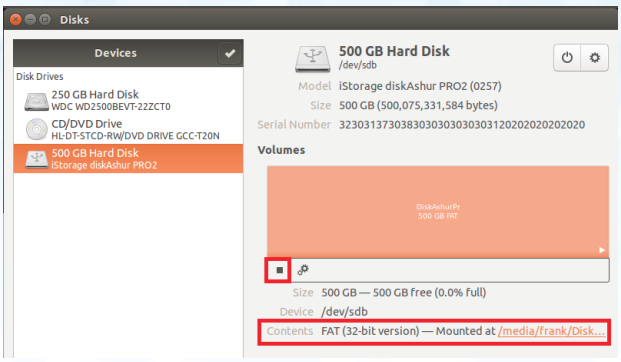

5. Das Laufwerk beginnt mit der Formatierung.



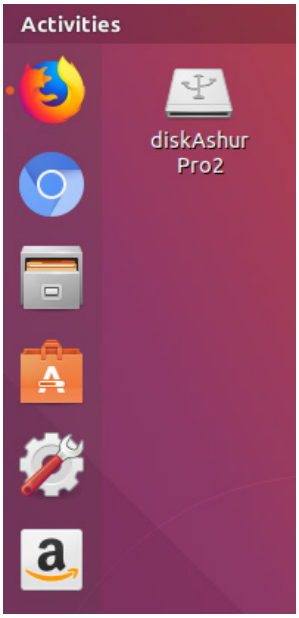

6. Nachdem der Formatierungsprozess abgeschlossen ist, klicken Sie ▶ um das Laufwerk auf Ubuntu zu mounten.



7. Nun sollte das Laufwerk auf Ubuntu gemountet und betriebsbereit sein.

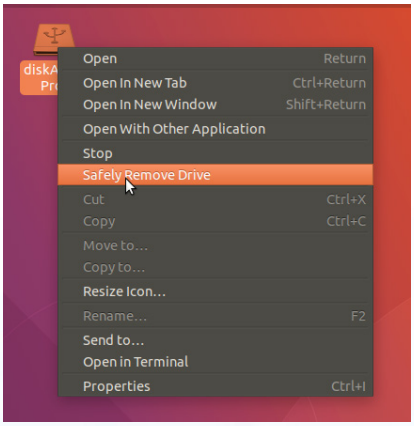



8. Ein Diskettensymbol wird angezeigt, wie im Bild unten zu sehen ist. Sie können auf das Diskettensymbol klicken, um das Laufwerk zu öffnen.




**Verschlüssel sie das iStorage diskAshur PRO² für Linux (Ubuntu 17.10)**

Es wird **dringend empfohlen, mit der rechten Maustaste auf das Laufwerkssymbol zu klicken und dann im Betriebssystem auf "Sicher entfernen" zu klicken**, um den diskAshur PRO² auszuwerfen (zu sperren), insbesondere nachdem Daten vom Laufwerk kopiert oder gelöscht wurden.



## 30. Ruhezustand, Sperre oder Abmeldung beim Betriebssystem

Speichern und schließen Sie alle Dateien auf der diskAshur PRO² vor Ruhezustand, Sperre oder Abmeldung beim Betriebssystem.

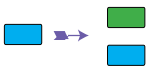
Es wird empfohlen, die diskAshur PRO² vor Ruhezustand, Sperre oder Abmeldung vom System manuell zu sperren.

Die Festplatte kann gesperrt werden, indem Sie einmal die Taste „SPERREN“ auf der diskAshur PRO² drücken oder auf das Symbol „Hardware sicher entfernen/Auswerfen“ Ihres Betriebssystems klicken.

**Achtung:** Um dafür zu sorgen, dass Ihre Daten sicher sind, sperren Sie Ihre diskAshur PRO², wenn Sie nicht an Ihrem Computer arbeiten.

## 31. Prüfen von Firmware im Admin-Modus

Um die Firmware-Revisionsnummer zu prüfen, wechseln Sie zuerst in den **Admin-Modus** wie in Abschnitt 5 beschrieben. Wenn sich die Festplatte im **Admin-Modus** befindet (BLAUE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Admin-Modus die Tasten „3 + 8“ gedrückt, bis die GRÜNE und BLAUE LED blinken. |  | Statt der leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt. |
| 2. Drücken Sie die Taste **ENTSPERREN**. Folgendes geschieht:<br><br>a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde.<br>b. Die ROTE LED blinkt. Dies gibt den 1. Bestandteil der Firmware-Revisionsnummer an.<br>c. Die GRÜNE LED blinkt. Dies gibt den 2. Bestandteil an.<br>d. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde.<br>e. Nur die BLAUE LED leuchtet. | | |

Wenn die Firmware-Revisionsnummer beispielsweise 1.2 ist, blinkt die ROTE LED einmal (1) und die GRÜNE LED zweimal (2). Nach der Sequenz blinken die ROTE, GRÜNE und BLAUE LED einmal, und dann wird eine leuchtende BLAUE LED angezeigt.

## 32. Prüfen von Firmware im Benutzermodus

Um die Firmware-Revisionsnummer zu prüfen, wechseln Sie zuerst in den **Benutzermodus** wie in Abschnitt 21 beschrieben. Wenn sich die Festplatte im **Benutzermodus** befindet (GRÜNE LED leuchtet), führen Sie die folgenden Schritte durch.

| | | |
|---|---|---|
| 1. Halten Sie im Benutzermodus die Tasten „3 + 8“ gedrückt, bis die GRÜNE und BLAUE LED blinken. |  | Die leuchtende GRÜNE LED ändert sich in eine blinkende GRÜNE und eine blinkende BLAUE LED. |
| 2. Drücken Sie die Taste **ENTSPERREN**. Folgendes geschieht:<br><br>a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde.<br>b. Die ROTE LED blinkt. Dies gibt den 1. Bestandteil der Firmware-Revisionsnummer an.<br>c. Die GRÜNE LED blinkt. Dies gibt den 2. Bestandteil an.<br>d. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde.<br>e. Nur die GRÜNE LED leuchtet. | | |

Wenn die Firmware-Revisionsnummer beispielsweise 1.2 ist, blinkt die ROTE LED einmal (1) und die GRÜNE LED zweimal (2). Nach der Sequenz blinken die ROTE, GRÜNE und BLAUE LED einmal, und dann wird eine leuchtende BLAUE LED angezeigt.

# 33. Technical Support

iStorage bietet die folgenden nützlichen Ressourcen:

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

E-Mail-Korrespondenz
support@istorage-uk.com

Telefonsupport unserer Technical Support-Abteilung: **+44 (0) 20 8991-6260**.
Die Technical Support-Spezialisten von iStorage sind Montag bis Freitag von 9:00 bis 17:30 Uhr GMT erreichbar.

# 34. Garantie- und RMA-Informationen

**3-Jahres-Garantie:**

iStorage bietet eine 3-Jahres-Garantie auf die iStorage diskAshur PRO², die Material- und Herstellungsmängel bei normaler Verwendung umfasst. Der Garantiezeitraum gilt ab dem Datum des Kaufs entweder direkt bei iStorage oder einem autorisierten Reseller.

**Haftungsausschluss und Garantiebedingungen:**

DIE GARANTIE WIRD AM DATUM DES KAUFS WIRKSAM UND MUSS DURCH IHREN KASSENBON ODER IHRE RECHNUNG VERIFIZIERT WERDEN.
ISTORAGE REPARIERT DEFEKTE TEILE ODER ERSETZT SIE DURCH NEUE ODER FUNKTIONSFÄHIGE GEBRAUCHTE TEILE, DIE HINSICHTLICH IHRER LEISTUNG NEUEN TEILEN ENTSPRECHEN. ES FALLEN KEINE ZUSÄTZLICHEN KOSTEN AN. ALLE IM RAHMEN DIESER GARANTIE AUSGETAUSCHTEN TEILE UND PRODUKTE SIND EIGENTUM VON ISTORAGE.
DIESE GARANTIE GILT NICHT FÜR PRODUKTE, DIE NICHT DIREKT BEI ISTORAGE ODER EINEM AUTORISIERTEN RESELLER ERWORBEN WURDEN, ODER PRODUKTE, DIE AUS FOLGENDEN GRÜNDEN BESCHÄDIGT WURDEN ODER DEFEKT SIND: 1. ALS RESULTAT EINES UNFALLS ODER FEHLGEBRAUCHS SOWIE DER MISSACHTUNG ODER NICHTEINHALTUNG DER SCHRIFTLICHEN ANWEISUNGEN IM ANWEISUNGSHANDBUCH: 2. DURCH DIE VERWENDUNG VON TEILEN, DIE NICHT VON ISTORAGE HERGESTELLT ODER VERKAUFT WURDEN 3. DURCH DIE MODIFIZIERUNG DES PRODUKTS ODER 4. ALS RESULTAT
EINES SERVICE, EINER ÄNDERUNG ODER EINER REPARATUR DURCH EINE ANDERE PARTEI ALS ISTORAGE. IN DIESEN FÄLLEN IST DIE GARANTIE HINFÄLLIG. DIESE GARANTIE DECKT NICHT NATÜRLICHE ABNUTZUNG AB.
ES WURDE UND WIRD KEINE ANDERE GARANTIE, WEDER AUSDRÜCKLICH NOCH IMPLIZIT, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF EINE BELIEBIGE GARANTIE ODER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DURCH ODER IM NAMEN VON ISTORAGE ODER KRAFT GESETZES IM HINBLICK AUF DAS PRODUKT ODER INSTALLATION, VERWENDUNG, BETRIEB, AUSTAUSCH ODER REPARATUR GEGEBEN.
ISTORAGE KANN AUFGRUND DIESER GARANTIE ODER ANDERWEITIG NICHT FÜR ETWAIGE ZUFALLS-, SONDER- ODER FOLGESCHÄDEN HAFTBAR GEMACHT WERDEN, EINSCHLIESSLICH AUS DER VERWENDUNG ODER DEM BETRIEB DES PRODUKTS RESULTIERENDER DATENVERLUST, UNABHÄNGIG DAVON, OB ISTORAGE ÜBER DIE MÖGLICHKEIT DERARTIGER SCHÄDEN INFORMIERT WURDE.

# Anhang A

## iStorage Sicherheitsrichtlinie Nr. 1 – Produkt-Sicherheitsmerkmale und sicherer Umgang

Diese iStorage Richtlinie bietet Produktunterstützung für die Verwendung von iStorage Sicherheitslaufwerk-Produkten durch private und staatliche Unternehmen gleichermaßen und orientiert sich an den Anweisungen des folgenden NCSC CESG-Dokuments:

CPA Security Characteristic Hardware Media Encryption Version 1.2 vom April 2012

Diese iStorage Richtlinie Nr.1 erläutert die von iStorage Sicherheitslaufwerk-Produkten unterstützten Sicherheitsmerkmale, zusammen mit den empfehlenswertesten Sicherheitspraktiken, um empfindliche und mit Schutzkennzeichnung versehene Informationen sowohl vor Ort, standortextern und beim Laufwerkstransport zu schützen.

Zusammen bieten die Sicherheitsmerkmale und Best Practices einen robusten Schutz vor dem Risiko physischer Angriffe, vor Diebstahl oder der Chance, dass Daten auf iStorage Sicherheitslaufwerken offengelegt werden, sodass ein unbefugter Zugriff auf die geschützten Inhalte nicht möglich ist.

**Das Risiko:** iStorage Sicherheitslaufwerke werden als wertvolle und attraktive Gegenstände eingestuft, die empfindliche geschäftliche, staatliche oder persönliche Daten (DSGV-bezogen) enthalten können. Daher stellen sie ein Ziel für physische und logische Angriffe (in Form von Diebstahl oder Zugriff) dar, wenn:

- Sie unbeaufsichtigt zurückgelassen werden
- An öffentlichen Orten sichtbar sind
- In einem offenen logischen Zustand belassen werden (authentifiziert)
- Beim Transport nicht korrekt gesichert wurden
- Keine für die Empfindlichkeit der Daten angemessene Kontrollen angewandt wurden
- Sie verlegt oder verloren wurden

Im Rahmen dieser iStorage Sicherheitsrichtlinie Nr.1 bieten wir Best Practices und praxisorientierte Maßnahmen, um das Angriffsrisiko zu reduzieren.

**Maßnahmen:** Die Geräte-Sicherheitsmerkmale und Maßnahmen im nachfolgenden Dokument sind die empfohlenen und besten Sicherheitspraktiken, die beim Umgang mit iStorage Sicherheitslaufwerken angewandt werden sollten. Sie werden in **Tabelle 1** aufgeführt. Dieser Ansatz befolgt die Sicherheitsphilosophie von **C**I**A**+**A** (**C**onfidentiality (Vertraulichkeit), **I**ntegrity (Integrität) und **A**vailability (Verfügbarkeit) + **A**ccountability (Verantwortlichkeit) und wendet relevante Sicherheitskontrollen aus ISO/IEC 27001 und dem erwähnten NCSC CESG-Dokument an:

### Tabelle 1 – Maßnahmen – Produktmerkmale - Sicherer Umgang

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| 1<br>**I**ntegrity (Integrität) **A**vailability (Verfügbarkeit) **A**ccountability (Verantwortlichkeit) | DEP.M311<br>DEP.1.M26 | Beim Transport | Lassen Sie ein iStorage Laufwerk beim Transport nie ungesichert in einem Laufwerk oder sichtbar zurück.<br>Wenn das Sicherheitslaufwerk unbeaufsichtigt zurückgelassen werden muss, stellen Sie sicher, dass es nicht sichtbar ist und das Fahrzeug beim Ein- und Ausladen der Medien abgeschlossen wird.<br>Wird ein iStorage Laufwerk verwendet und enthält es Daten, verschicken Sie es stets mit einem nachverfolgbaren und vertrauenswürdigen Kurierdienst.<br>iStorage Sicherheitslaufwerke werden in einer manipulationssicheren Hülle geliefert, die durch ein Sicherheitssiegel geschützt ist. Ist das Sicherheitssiegel bei der Lieferung gebrochen oder gibt es Hinweise auf Manipulation, sollte das Laufwerk als gefährdet gelten. Melden Sie dies umgehend dem iStorage Kundendienst unter:<br><br>+44 (0) 20 8991-6260<br>Oder senden Sie eine E-Mail an: support@istorage-uk.com |

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| **2**<br>**C**onfidentiality (Vertraulichkeit) **I**ntegrity (Integrität) **A**vailability (Verfügbarkeit) | **DEP.M1**<br>**DEP.M701** | **Unbefugter Zugriff** | Um die Gefahr kompromittierter Daten auf einem iStorage Sicherheitslaufwerk zu minimieren:<br><br>Lassen Sie das iStorage Sicherheitslaufwerk nie in einer authentifizierten, offenen Sitzung zurück.<br><br>Um das Risiko von unbefugtem Zugriff zu vermeiden, wechseln Sie das Laufwerk in den gesperrten Modus, wenn es nicht verwendet wird.<br><br>Konfigurieren Sie die automatische Sperre für das iStorage Laufwerk, damit das Laufwerk nach einer bestimmten Zeit gesichert wird (weitere Informationen finden Sie im Benutzerhandbuch).<br><br>Wird das iStorage Sicherheitslaufwerk nicht gebraucht, entfernen Sie und sichern Sie es unter Einhaltung angemessener physischer Sicherheitskontrollen.<br><br>Stellen Sie stets sicher, dass für auf dem iStorage Laufwerk gespeicherte Daten eine Sicherheitskopie angefertigt wurde, die bei einem Verlust des iStorage Sicherheitslaufwerks verfügbar ist. |
| **3**<br>**C**onfidentiality (Vertraulichkeit) **A**ccountability (Verantwortlichkeit) | **DEP.M703** | **Verlust, Diebstahl, Offenlegung** | Stellen Sie sicher, dass ein Prozess zur Benachrichtigung des Vorstands im Falle von Diebstahl, Verlust oder Offenlegung des iStorage Sicherheitslaufwerks besteht. Zum Beispiel:<br><br>i. Melden Sie den Verlust oder Diebstahl der Polizei und fordern Sie eine Fallreferenznummer an<br><br>ii. Unternehmen Sie bei einem Unternehmensgerät die notwendigen Schritte, um so schnell wie möglich die Sicherheitsabteilung zu benachrichtigen<br><br>iii. Für den Fall, dass auf dem Laufwerk Daten der Regierung des Vereinigten Königreichs (oder einer anderen Regierung) gespeichert wurden, melden Sie den Vorfall unverzüglich dem zuständigen Eigentümer (Information Asset Owner, IAO).<br><br>iv. Erwägen Sie im Falle von vertraulichen Regierungsmaterialien die Vorbehalte hinsichtlich Datenschutz, Schutzkennzeichnung usw. und die damit verbundenen Auswirkungen auf die nationale Sicherheit. |

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| | | | v. Beurteilen Sie bei Daten von Privatunternehmen die Auswirkungen des Verlusts und die mögliche Offenlegung der Informationen auf den gestohlenen Medien<br><br>vi. Sollten Sie das Laufwerk zurückerhalten, behandeln Sie es als kompromittiert und unternehmen Sie die nötigen Schritte zur Neuformatierung und Initialisierung, bevor es erneut eingesetzt wird.<br><br>Wenn mit Schutzkennzeichnung versehene oder Regierungsdaten auf dem iStorage Laufwerk gespeichert werden, fragen Sie bei den zuständigen Behörden nach.<br><br>Vergewissern Sie sich, dass die Daten zum Zeitpunkt des Diebstahls oder Verlusts verschlüsselt waren (das Laufwerk befand sich nicht in einer authentifizierten, offenen Sitzung). Die Klarstellung dieses Sachverhaltes führt nicht zur Kompromittierung empfindlicher Daten oder anderer Informationen. |
| **4**<br><br>Integrity<br>(Integrität) | **DEP.1.M26** | **Manipulationsschutz** | Die iStorage Laufwerke verfügen über einen Manipulationsschutz.<br><br>Führen Sie eine regelmäßige Prüfung des Außengehäuses des iStorage Sicherheitslaufwerks auf Anzeichen von Manipulation oder direkten physischen Angriffen durch.<br><br>Im seltenen Fall, dass unser Produkt eine Aktualisierung erfordert, werden keine Software- oder Firmware-Aktualisierungen (weder online noch auf CDs oder anderen Medien) bereitgestellt. Stattdessen bieten wir einen Rückruf- und Austauschservice, der Sie zwei Werktage vor dem Versand des neuen Produkts per E-Mail u. a. über die Seriennummer informiert, die von Ihrer Organisation nach dem Empfang verifiziert werden kann. Berücksichtigen Sie jedoch stets das Risiko, ein manipuliertes oder gefälschtes iStorage Produkt von Dritten zu erhalten. Stellen Sie dafür sicher, dass Ihre Organisation angemessene Sicherheits- und Aufklärungsschulungen durchführt, damit Mitarbeiter sich der Risiken bewusst sind.<br><br>**Hinweis 1:** Sollte es tatsächliche oder vermutete Anzeichen von Produktmanipulation oder -fälschung geben, melden Sie dies unverzüglich dem iStorage Kundendienst unter:<br>+44 (0) 20 8991-6260<br>Alternativ können Sie eine E-Mail senden an:<br>support@istorage-uk.com |

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| 5<br>Confidentiality<br>(Vertraulichkeit)<br>Integrity<br>(Integrität) | DEP.2.M12<br>DEP.2.M283<br>DEP.2.M285<br>DEP.2.M617 | Robustes Kennwortmanagement | Das Kennwort wird bei der Eingabe nie angezeigt.<br><br>Legen Sie stets ein komplexes Kennwort für das Administrator- und die Benutzerkonten auf dem iStorage Sicherheitslaufwerk fest, um das Risiko logischer Angriffe und/oder von Offenlegung zu mindern.<br><br>Obwohl das Gerät Kennwörter mit mindestens 7 Zeichen akzeptiert, empfehlen wir für Benutzer ein Kennwort mit höherer Komplexität, d. h. nicht weniger als 8 Zeichen und die Nutzung der **SHIFT**-Taste mit Ziffern.<br><br>Wählen Sie ein Kennwort, das nicht leicht erraten werden kann.<br><br>Vermeiden Sie die Nutzung des gleichen Kennworts bei mehreren Systemen mit unterschiedlichen Sicherheitseinstufungen.<br><br>Schreiben Sie Kennwörter nie auf und geben Sie nie weiter. Achten Sie bei der Eingabe eines Kennworts an einem iStorage Gerät an öffentlichen Orten darauf, dass Ihnen niemand dabei zusieht.<br><br>Sollten Sie den Verdacht haben, dass das Kennwort offengelegt wurde, muss es so schnell wie möglich geändert werden.<br><br>Gibt es betriebliche Gründe zur Dokumentierung eines Kennworts in gedruckten Unterlagen, muss dies auf sichere Art und Weise oder über den Unternehmensausnahmeprozess erfolgen.<br><br>**Hinweis 2:** Die sichere Aufbewahrung eines Kennworts kann durch eine sichere Kennwortspeicher-Anwendung oder durch einen sicheren Umschlag erfolgen, der durch physische Zugriffskontrollen und in einem hochwertigen Kombinationssafe geschützt wird. |
| 6<br>Confidentiality<br>(Vertraulichkeit)<br>Integrity<br>(Integrität) | DEP.2.M281 | Administrator kennwort-Management | Das iStorage Sicherheitslaufwerk bietet die Möglichkeit, erweiterten Zugriff für Administratoren zur Verwaltung des Geräts bereitzustellen.<br><br>Nur autorisierte und authentifizierte Administratoren können zugeordnete Konten hinzufügen oder entfernen. |

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| **7**<br>Confidentiality (Vertraulichkeit) | DEP.2.M277 | **Social Engineering** | Seien Sie sich der Gefahr direkter und indirekter Social-Engineering-Angriffe bewusst. Diese können benutzt werden, um Benutzer-ID, Kennwort und andere Unternehmens- oder private Benutzerdaten durch Social-Engineering-Techniken zu stehlen.<br><br>Stellen Sie sicher, dass die Organisation eine Sicherheits- und Aufklärungsschulung durchführt, damit Benutzer sich folgender Gefahren bewusst sind:<br><br>i. Unaufgeforderte E-Mails, die Benutzer zum Austausch von Mitteilungen verleiten sollen<br><br>ii. Das Öffnen von URLs in nicht erwarteten E-Mails, die von unbekannten Benutzern versandt wurden<br><br>iii. Das unvorsichtige Öffnen von Anhängen, die mit Malware infiziert sein können<br><br>iv. Die Annahme von Freundschaftsanfragen in sozialen Netzwerken von Personen, die Sie nicht kennen<br><br>v. Verlockende Online-Angebote – wenn sie zu schön sind, um wahr zu sein, sind sie das wahrscheinlich auch und in der Regel gefälscht. |
| **8**<br>Confidentiality (Vertraulichkeit)<br>Integrity (Integrität) | DEP.2.M280 | **Verteilung von Benutzerdaten** | Übermitteln Sie Sicherheitsbenutzerdaten nie über den gleichen Kanal und nutzen Sie keine Benutzerdaten, die mit einem iStorage Sicherheitslaufwerk geliefert werden.<br><br>**Hinweis 3:** Gibt es betriebliche Vorgaben zur Verteilung von Benutzerdaten, sollte dies außerhalb der Hauptkommunikationsformen erfolgen (z. B. mündlich, per SMS oder gesicherte E-Mail). |
| **9**<br>Integrity (Integrität) | DEP.4.M348<br>DEP.1.M348 | **Autorisierte Aktualisierungen** | Es gibt keinen automatisierten Vorgang. Nur genehmigte Aktualisierungen, die für iStorage Produkte gelten, warden im Rahmen des internen iStorage SDLC (Security Development Lifecycle) und der Prozesse für Schwachstellenmanagement als Teil eines Upgrade- oder Austauschprozesses vertrieben. |
| **10**<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | | **Daten-Klassifizierung** | Stellen Sie sicher, dass der Wert der auf dem iStorage Sicherheitslaufwerk gespeicherten Daten als vertraulich klassifiziert, mit Schutzkennzeichnung versehen oder unter Verwahrung gestellt wird. |
| **11**<br>Confidentiality (Vertraulichkeit) | | **Freigegebener Zugriff** | Stellen Sie sicher, dass der Zugriff auf die Daten oder mit Schutzkennzeichnung versehenen Materialien auf einem iStorage Sicherheitslaufwerk nur bei Bedarf und der Vertraulichkeitsstufe entsprechend gewährt wird. |

# Anhang B

## iStorage Sicherheitsrichtlinie Nr. 2 – Säuberung und sichere Entsorgung

Diese iStorage Richtlinie bietet Informationen für die Nutzung von iStorage Produkten durch private und staatliche Unternehmen. Die Richtlinie Nr. 2 erläutert die besten Sicherheitsmaßnahmen für die Säuberung und sichere Entsorgung von iStorage Sicherheitslaufwerken entsprechend der Direktive **IS5** der Regierung des Vereinigten Königreichs zur sicheren Entsorgung und unter Bezugnahme auf **DEP.M.137**, das die Anforderungen für die sichere Entsorgung beschreibt.

Diese Richtlinie enthält auch Informationen zur Neuausgabe von sicheren Laufwerken, um das Risiko einer erneuten Nutzung oder Kompromittierung von Daten auf iStorage Sicherheitslaufwerken zu mindern.

**Das Risiko:** Wenn auf einem iStorage Sicherheitslaufwerk gespeicherte Daten bei der Neuausgabe oder Entsorgung von Laufwerken keinen Sicherheitskontrollen unterliegen, können sie kompromittiert werden und organisatorische Auflagen zu Sicherheit und Datenschutz (wie DSGV) beeinträchtigen. Zum Beispiel:

- Exfiltrierung und Vertrieb empfindlicher Daten durch unbefugte externe Akteure
- Versehentliche Offenlegung
- Offenlegung von Schutzkennzeichnung versehenen oder vertraulichen Regierungsdaten

**Ziel:** Obwohl iStorage Sicherheitslaufwerke mithilfe von robuster Verschlüsselung den Schutz der gespeicherten Daten ermöglichen, ist es dennoch empfehlenswert, iStorage Sicherheitslaufwerke bei der Neuausgabe an Dritte, Verwahrer, Abteilungen oder am Ende ihres Lebenszyklus robusten Prozessen zu unterziehen, damit zurückgebliebene gespeicherte Daten sicher gelöscht und nicht kompromittiert werden können.

Im Rahmen dieser iStorage Sicherheitsrichtlinie Nr. 2 bieten wir Best Practices und praxisorientierte Maßnhmen, um diese Bedrohung zu mindern.

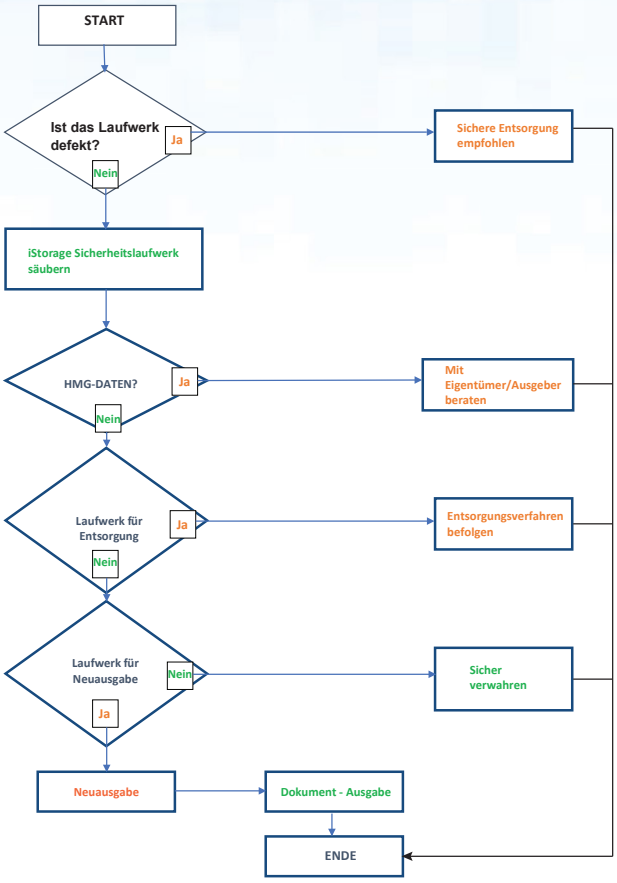
**Maßnahmen:** Die nachfolgenden Maßnahmen sind die empfohlenen und besten Sicherheitspraktiken, die beim Umgang mit iStorage Sicherheitslaufwerken angewandt werden sollten. Sie werden in Tabelle 1 aufgeführt. Dieser Ansatz befolgt die Sicherheitsphilosophie von **C**I**A**+**A** (**C**onfidentiality (Vertraulichkeit) **I**ntegrity (Integrität) und **A**vailability (Verfügbarkeit) + **A**ccountability (Verantwortlichkeit) und wendet relevante Sicherheitskontrollen aus ISO/IEC 27001 und dem erwähnten NCSC (CESG-Dokument an.

CPA Security Characteristic Hardware Media Encryption Version 1.2 vom April 2012

**Prozess:** **Abb. 1** unten zeigt den Datenfluss auf hoher Ebene im Bezug auf:

- Sichere Entsorgung
- Säuberung
- Mit Schutzkennzeichnung versehene und vertrauliche Regierungsdaten
- Neuausgabe von iStorage Sicherheitslaufwerken

## Abb. 1 – Säuberungs-/Entsorgungsprozess




## Tabelle 1 - Maßnahmen - Säuberung und sichere Entsorgung

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| 1<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | DEP.M1 | Aufbewahrung | Stellen Sie sicher, dass alle iStorage Sicherheitslaufwerke, für die Säuberung oder sichere Entsorgung vorgesehen ist, voll dokumentiert und erfasst sind,<br><br>dass sie an einem sicheren Standort mit robusten physischen und Zugriffskontrollmechanismen und -verfahren aufbewahrt werden.<br><br>**Hinweis 1:** Abhängig von der zu verarbeitenden Anzahl an Laufwerken kann es sich dabei um einen abgeschlossenen Raum oder einen Sicherheitsschrank handeln. |
| 2<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | DEP.M311 | Beim Transport | Lassen Sie beim Transport zu einer Entsorgungsanlage Laufwerke nie ungesichert in einem Fahrzeug oder sichtbar zurück.<br><br>Wenn Laufwerke unbeaufsichtigt zurückgelassen werden müssen, stellen Sie sicher, dass diese nicht sichtbar sind und das Fahrzeug beim Ein- und Ausladen der Medien abgeschlossen wird. |

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| | | | Alle iStorage Sicherheitslaufwerke, die zur Verarbeitung durch eine sichere Entsorgungsanlage vorgesehen sind, sollten nur von einem vertrauenswürdigen Anbieter oder Kurierdienst gehandhabt werden.<br><br>Wenn auf den iStorage Sicherheitslaufwerken mit Schutzkennzeichnung versehene oder vertrauliche Regierungsdaten gespeichert sind, sollten Sie sich mit den relevanten Abteilungen oder Behörden beraten, um zu erfahren, ob zusätzliche Kontrollen implementiert werden müssen (z. B. Kommunikation während des Transports, Kontakt zu Notfalldiensten oder ein Bereitschaftsfahrzeug). |
| **3**<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | | **Schutzkennzeichnung** | Wenn auf iStorage Sicherheitslaufwerken mit Schutzkennzeichnung versehene, empfindliche Regierungsdaten gespeichert sind, sollten Sie sich mit den relevanten Abteilungen oder Behörden hinsichtlich der Anforderungen für die Aufzeichnung und sichere Entsorgung von Sicherheitslaufwerken beraten. |
| **4**<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | | **Verantwortlichkeit** | Alle iStorage Sicherheitslaufwerke, die für die Säuberung oder sichere Entsorgung vorgesehen sind, sollten in einem Verzeichnis dokumentiert werden, u. a. mit:<br><br>• Seriennummer<br>• Eigentümer/Abteilung<br>• Empfangsdatum<br>• Einstufung oder Schutzkennzeichnung der Daten<br>• Besondere Handhabungsauflagen<br>• Versanddatum zur Verarbeitung<br><br>**Hinweis 2:** In Fällen, in denen das iStorage Laufwerk zur Neuausgabe gesäubert wurde, sollte es in einem neuen Verzeichnis dokumentiert werden, bevor es an einen neuen Eigentümer/Verwahrer/eine neue Abteilung gesandt wird. |
| **5**<br>Availability (Verfügbarkeit) | | **Geschäftskontinuität** | Bevor ein iStorage Sicherheitslaufwerk einer Säuberung oder sicheren Entsorgung unterzogen wird, sollten Sie sicherstellen, dass sämtliche darauf gespeicherten Daten erfasst und bei Bedarf gesichert wrden, um eine unbeabsichtigte Entsorgung der gespeicherten Betriebsdaten zu vermeiden. |

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| **6**<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | **DEP.M137** | **Säuberungsmethoden** | Die zur Verarbeitung von iStorage Sicherheitslaufwerken verwendeten Säuberungsmethoden sollten durch dokumentierte Säuberungsverfahren und Sicherheitsbetriebsprozeduren (Security Operating Procedures, SysOps) gestützt werden.<br><br>Derartige Prozeduren sollten die für Medientyp, Schutzkennzeichnung oder Regierungseinstufung relevanten Prozesse befolgen, um mindestens die HMG-Standards zu erfüllen.<br><br>Der ausgewählte Dienstanbieter muss nachweisen können, dass die Prozeduren tatsächlich durchgeführt wurden.<br><br>Hinweise zu NCSC (Teil von GCHQ) finden Sie unter folgender URL: https://www.ncsc.gov.uk/index/topic/164 |
| **7**<br>Integrity (Integrität) | **DEP.M137** | **Säuberung und Entsorgung** | Die Säuberung oder Entsorgung von iStorage Sicherheitslaufwerken sollte gemäß der dokumentierten Betriebsverfahren des Herstellers, der Benutzerhandbücher und veröffentlichter Sicherheitsverfahren erfolgen.<br><br>Die für die Säuberung oder sichere Entsorgung verantwortlichen Mitarbeiter oder Teams sollten in der richtigen Nutzung der dafür notwendigen Geräte geschult sein.<br><br>Es müssen Verfahren bestehen, um die richtige Verwendung der Geräte unter Befolgung der Herstellerempfehlungen sicherzustellen. |
| **8**<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | | **Erneute Medienausgabe** | In Fällen, in denen ein iStorage Sicherheitslaufwerk gesäubert und an einen neuen Benutzer, Verwahrer oder eine neue Abteilung ausgegeben werden soll, sollte in einer vorherigen Prüfung sichergestellt werden, dass das Medium vollständig leer ist.<br><br>Ein Benutzerhandbuch für das iStorage Sicherheitslaufwerk mit klaren Anweisungen zur sicheren Verwendung sollte zusammen mit dem Laufwerk ausgegeben werden.<br><br>Die Neuausgabe des iStorage Sicherheitslaufwerks sollte vollständig dokumentiert und in einem Verzeichnis erfasst werden. |
| **9**<br>Confidentiality (Vertraulichkeit)<br>Accountability (Verantwortlichkeit) | **DEP.M703** | **Verlust, Diebstahl, Offenlegung** | Stellen Sie sicher, dass ein Prozess zur Benachrichtigung des Vorstands im Falle von Diebstahl, Verlust oder Offenlegung des zu verarbeitenden iStorage Sicherheitslaufwerks besteht.<br><br>Wenn mit Schutzkennzeichnung versehene oder Regierungsdaten auf dem iStorage Laufwerk gespeichert werden, fragen Sie bei den zuständigen Behörden nach. |

| Maßnahmen | NCSC (CESG) CPA | Risiko | Beste Vorgehensweise |
|---|---|---|---|
| | | | Vergewissern Sie sich, dass die Daten zum Zeitpunkt des Diebstahls oder Verlusts verschlüsselt waren. Die Klarstellung dieses Sachverhaltes führt nicht zur Kompromittierung empfindlicher Daten oder anderer Informationen. |
| **10** Confidentiality (Vertraulichkeit) | MIT003 | Freigegebener Zugriff | Stellen Sie sicher, dass der Zugriff auf die Daten, mit Schutzkennzeichnung versehenen Materialien oder Regierungsdaten auf einem iStorage Sicherheitslaufwerk nur bei Bedarf und der Vertraulichkeitsstufe entsprechend gewährt wird. |

diskAshur PRO²®

iStorage®

Copyright © iStorage Limited 2017. 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

iStorage®

# Manuel d'utilisation




diskAshur PRO²®



**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 rencontrez des difficultés à utiliser le disque diskAshur PRO², merci de contacter notre service technique par courriel à l'adresse support@istorage-uk.com ou par téléphone au +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2017. Tous droits réservés.
Windows est une marque déposée de Microsoft Corporation.

L'ensemble des autres marques déposées et droits d'auteur auquel il est fait référence est la propriété de leurs fabricants respectifs.

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

La distribution du travail ou d'une variante sous forme imprimée (papier) standard à des fins commerciales est interdite sans l'autorisation préalable du détenteur des droits d'auteur.

LA DOCUMENTATION EST FOURNIE EN L'ÉTAT ET TOUTES CONDITIONS, DÉCLARATIONS ET GARANTIES, IMPLICITES OU EXPLICITES,

Y COMPRIS TOUTE GARANTIE IMPLICITE DE CONFORMITÉ D'USAGE POUR UN EMPLOI PARTICULIER OU DE NON-TRANSGRESSION, SONT DÉNIÉES, SOUS RÉSERVE QUE CES DÉNIS DE RESPONSABILITÉ NE SOIENT PAS LÉGALEMENT TENUS POUR NULS.

RoHS

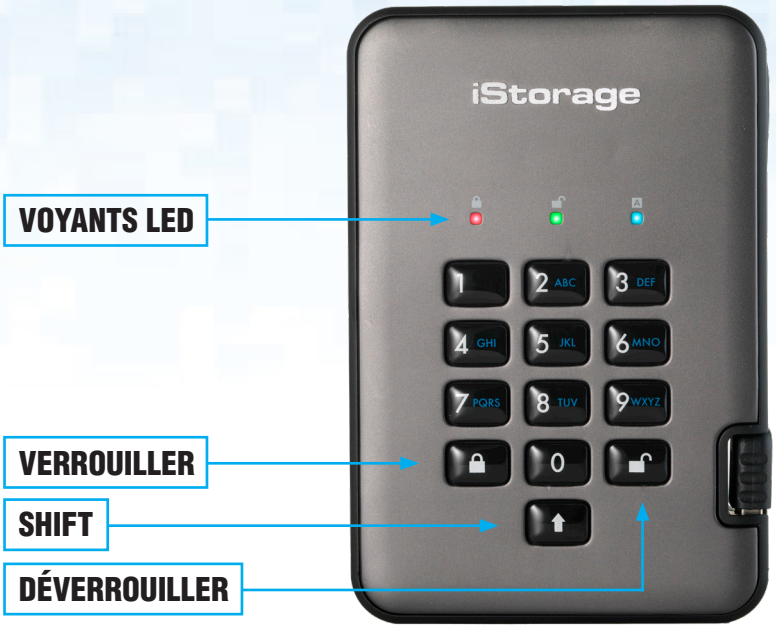
Toutes les marques déposées et les noms de marque sont la propriété de leurs fabricants respectifs
Conforme au Trade Agreements Act (TAA)

# Table des matières

Introduction ..... 81
Contenu de la boîte ..... 81
1. États des LED du diskAshur PRO² ..... 82
2. Comment utiliser le diskAshur PRO² pour la première fois ..... 82
3. Déverrouiller le diskAshur PRO² ..... 83
4. Verrouiller le diskAshur PRO² ..... 83
5. Accéder au mode administrateur ..... 83
6. Modifier le code PIN administrateur ..... 84
7. Définir une politique en matière de code PIN utilisateur ..... 85
8. Comment vérifier la politique de code PIN utilisateur ..... 86
9. Ajouter un nouveau code PIN utilisateur en mode administrateur ..... 87
10. Modifier le code PIN utilisateur en mode administrateur ..... 87
11. Supprimer le code PIN utilisateur en mode administrateur ..... 87
12. Définir le mode de lecture seule en mode administrateur ..... 88
13. Activer le mode lecture/écriture en mode administrateur ..... 88
14. Comment créer un code PIN d'autodestruction ..... 88
15. Comment supprimer le code PIN d'autodestruction ..... 89
16. Comment déverrouiller avec le code PIN d'autodestruction ..... 89
17. Comment créer un code PIN administrateur après une attaque par force brute ou une réinitialisation ..... 90
18. Programmer la fonction de verrouillage automatique ..... 90
19. Désactiver le verrouillage automatique ..... 91
20. Comment vérifier la minuterie de verrouillage ..... 91
21. Comment déverrouiller le diskAshur PRO² avec le code PIN utilisateur ..... 92
22. Modifier le code PIN utilisateur en mode utilisateur ..... 92
23. Définir le mode de lecture seule en mode utilisateur ..... 93
24. Activer le mode lecture/écriture en mode utilisateur ..... 93
25. Protection contre les attaques par force brute ..... 94
26. Comment effectuer une réinitialisation complète ..... 94
27. Initialiser et formater le diskAshur PRO² ..... 95
28. Configuration du diskAshur PRO² pour Mac OS ..... 97
29. Configuration du diskAshur PRO² pour Linux (Ubuntu 17.10) ..... 99
30. Mettre en veille prolongée, suspendre ou se déconnecter du système d'exploitation ..... 102
31. Comment vérifier la version du firmware en mode administrateur ..... 102
32. Comment vérifier la version du firmware en mode utilisateur ..... 103
33. Assistance technique ..... 104
34. Informations de garantie et de service après-vente (SAV) ..... 104

**Annexes**

A. Directive de sécurité iStorage n° 1 - Fonctionnalités de sécurité et manipulation sécurisée ..... 105
B. Directive de sécurité iStorage n° 2 - Procédure d'effacement et ..... 110




## Introduction

Disque dur portable avec cryptage matériel très sécurisé et facile à utiliser doté d'une capacité de stockage pouvant atteindre 2 To. Il vous suffit de connecter le câble USB 3.1 intégré à un ordinateur et de saisir un code PIN de 7 à 15 chiffres. Si le code PIN saisi est correct, toutes les données stockées sur le disque sont accessibles. Pour verrouiller le disque et chiffrer toutes les données, appuyez simplement sur le bouton de verrouillage situé sur le diskAshur PRO² ou supprimez-le en toute sécurité/éjectez-le de l'ordinateur hôte. L'intégralité du contenu du disque est chiffré à l'aide du chiffrement matériel AES 256 bits de classe militaire (mode XTS). Si le disque est perdu ou volé et que le code PIN est saisi 15 fois consécutives de manière incorrecte, le disque se réinitialise et toutes les données sont perdues à jamais.

Conforme au règlement général sur la protection des données, l'une des fonctionnalités de sécurité fondamentales et uniques du diskAshur PRO² est le microprocesseur sécurisé intégré (conforme aux Critères Communs EAL4+), équipé de mécanismes de protection physiques intégrés conçus pour protéger contre la falsification externe, les attaques et les injections d'erreurs. Contrairement à d'autres solutions, le diskAshur PRO² réagit aux attaques automatisées en entrant dans un état de blocage et en rendant toutes ces attaques inutiles. Autrement dit, sans le code PIN, il est impossible de se connecter !

## Contenu de la boîte

1. Disque diskAshur PRO² avec câble USB intégré
2. Étui de transport élégant
3. Guide de démarrage rapide

diskAshur PRO²®

iStorage®

**Attention! veuillez lire attentivement:**

Pour des raisons de sécurité, iStorage vous conseille de procéder à l'une des actions suivantes avant toute première utilisation de votre diskAshur PRO²:

1. Changez immédiatement le code PIN Administrateur par défaut (11223344), tel que décrit sous section 6: '**Modifier le code PIN administrateur**', puis procéder à la création d'un nouveau code PIN utilisateur tel qu'indiqué sous section 9, '**Ajouter un nouveau code PIN utilisateur en mode administrateur**'.

**Ou –**

2. Réinitialisez votre diskAshur PRO² tel que décrit sous section 26: '**Comment effectuer une réinitialisation complète**', procédez ensuite à la création d'un nouveau code PIN administrateur comme decrit sous section 17: '**Comment créer un code PIN administrateur après une attaque par force brute ou une réinitialisation**'.

## 1. États des LED du diskAshur PRO²

Lorsque le diskAshur PRO² est connecté, il existe trois comportements possibles pour les témoins LED tel qu'indiqué dans le tableau ci-dessous.

| ROUGE | VERT | BLEU | État du diskAshur PRO² |
|---|---|---|---|
| Continu | Éteint | Éteint | Réinitialisation [1] |
| Continu | Continu | Continu | Force brute [2] |
| Continu | Éteint | Éteint | Veille [3] |

1. En état de réinitialisation, le disque attend que l'opérateur saisisse un code PIN administrateur.
2. En état de force brute, le disque attend que l'opérateur effectue d'autres tentatives de saisie de code PIN.
3. En état de veille, le disque attend que l'opérateur déverrouille le disque, passe en mode administrateur ou réinitialise le disque.

## 2. Comment utiliser le diskAshur PRO² pour la première fois

Le diskAshur PRO² est livré avec le code PIN administrateur par défaut de **11223344**. Même s'il est directement prêt à l'emploi avec le code PIN administrateur par défaut, nous vous **recommandons fortement, pour des raisons de sécurité, de créer immédiatement un nouveau code PIN administrateur** en suivant les instructions indiquées sous la section 6 « Modifier le code PIN administrateur ».

Merci de suivre les 3 étapes simples indiquées dans le tableau ci-dessous pour déverrouiller le diskAshur PRO² pour la première fois avec le code PIN administrateur par défaut.

| Instructions (première utilisation) | LED | État de la LED |
|---|---|---|
| 1. Connectez le diskAshur PRO² à un port USB. |  | La LED ROUGE est continue en attente de la saisie du code PIN. |
| 2. Saisissez le code PIN administrateur (par défaut : 11223344) |  | La LED ROUGE reste continue. |
| 3. Dans les 10 secondes qui suivent, appuyez une fois sur le bouton « **UNLOCK** » (Déverrouiller) pour déverrouiller le diskAshur PRO². |  | Les LED VERTE et BLEUE clignotent plusieurs fois en alternance, puis la LED BLEUE devient continue avant d'être remplacée par la LED VERTE clignotante, puis continue. |

**Remarque** : une fois que vous avez correctement déverrouillé le diskAshur PRO², la LED VERTE reste allumée en continu. Vous pouvez le verrouiller immédiatement en appuyant une fois sur le bouton « **LOCK** » (Verrouiller) ou en cliquant sur l'icône « Safely Remove Hardware/Eject » (Supprimer le périphérique en toute sécurité/Éjecter) dans votre système d'exploitation. Pour vous assurer que les données ne sont pas corrompues, nous vous recommandons d'utiliser l'option « Supprimer le périphérique en toute sécurité/Éjecter ».

## 3. Déverrouiller le diskAshur PRO²

Vous pouvez déverrouiller le diskAshur PRO² avec un code PIN administrateur ou utilisateur en état de veille (LED ROUGE continue).

1. Pour déverrouiller en tant qu'administrateur, saisissez le code PIN **administrateur** et appuyez sur le bouton « **DÉVERROUILLER** ».
2. Pour déverrouiller en tant qu'**utilisateur**, appuyez d'abord sur le bouton « **DÉVERROUILLER** » (toutes les LED, ▬ ▬ ▬ se mettent à clignoter), puis saisissez le code PIN **utilisateur** et appuyez à nouveau sur le bouton « **DÉVERROUILLER** ».
3. Si le code PIN utilisateur saisi est correct, les LED VERTE et BLEUE clignotent en alternance, puis sont remplacées par la LED VERTE continue.
4. Si le code PIN administrateur saisi est correct, les LED VERTE et BLEUE clignotent en alternance avant d'être remplacées par la LED BLEUE continue pendant 1 seconde puis, à l'état déverrouillé, par la LED VERTE continue.
5. Si le code PIN saisi est correct, le disque apparaît en tant que « Périphérique USB iStorage diskAshur PRO² » sous « Computer Management/Device Manager » (Gestion de l'ordinateur/Gestionnaire de périphériques).

À l'état déverrouillé (LED VERTE), il existe deux comportements possibles pour les témoins LED, indiqués dans le tableau ci-dessous.

| ROUGE | VERT | BLEU | diskAshur PRO² |
|---|---|---|---|
| Éteint | Continu | Éteint | Aucun transfert de données |
| Éteint | Clignote | Éteint | Transfert de données en cours |

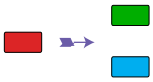
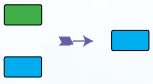
## 4. Verrouiller le diskAshur PRO²

Pour verrouiller le disque, appuyez une fois sur le bouton « **DÉVERROUILLER** » ou cliquez sur l'icône « Supprimer le périphérique en toute sécurité/Éjecter » dans votre système d'exploitation. Si les données sont en cours d'écriture sur le disque, patientez jusqu'à la fin de l'écriture de toutes les données avant d'appuyer sur le bouton « VERROUILLER » ou d'éjecter le disque en toute sécurité du système d'exploitation. Lorsque le délai de verrouillage automatique est activé, le disque se verrouille automatiquement au bout d'un intervalle de temps prédéterminé.

⚠ **Remarque :** le diskAshur PRO² ne peut pas être reconnu par le système d'exploitation en état de veille.

## 5. Accéder au mode administrateur

Pour accéder au mode administrateur, effectuez les étapes suivantes :

| | | |
|---|---|---|
| 1. En mode veille (LED ROUGE continue), appuyez sur les boutons « **DÉVERROUILLER + 1** » et maintenez-les enfoncés. |  | La LED ROUGE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Saisissez le code PIN administrateur (par défaut : 11223344) et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE et BLEUE clignotent rapidement simultanément pendant quelques secondes avant d'être remplacées par la LED VERTE continue et enfin par la LED BLEUE continue, indiquant que le diskAshur PRO² est en mode administrateur. |

Pour quitter le mode administrateur, appuyez sur le bouton « **VERROUILLER** ».

# 6. Modifier le code PIN administrateur

Exigences pour le code PIN :

- Doit être composé de 7 à 15 chiffres.
- Ne doit pas contenir que des nombres répétitifs (c.-à-d. 3-3-3-3-3-3-3-3).
- Ne doit pas contenir que des nombres consécutifs (c.-à-d. 1-2-3-4-5-6-7 ; 7-8-9-0-1-2-3-4 ; 7-6-5-4-3-2-1).

**Conseil pour le mot de passe** : vous pouvez créer un mot, un nom, une phrase ou toute autre combinaison de code PIN alphanumérique facile à mémoriser en appuyant simplement sur la touche de la lettre correspondante.

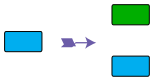
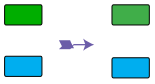
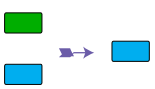
**Voici des exemples de ces types de codes PIN alphanumériques :**

- Pour le terme « **Password** », vous appuieriez sur les touches suivantes :
  **7** (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Pour le terme « **iStorage** », vous appuieriez sur :
  **4** (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

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

**Remarque :** la touche **SHIFT** peut être utilisée pour d'autres combinaisons. **SHIFT** + 1 est une valeur différente de 1. Pour créer un code PIN utilisant d'autres combinaisons, appuyez sur le bouton **SHIFT** et maintenez-le enfoncé pendant la saisie de votre code PIN de 7 à 15 chiffres (c.-à-d. **SHIFT** + **26756498**).

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

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 2** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue. |
| 2. Saisissez le NOUVEAU code PIN administrateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE continue. |
| 3. Ressaisissez le NOUVEAU code PIN administrateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED BLEUE qui se met à clignoter rapidement avant d'être continue, indiquant que le code PIN administrateur a été correctement modifié. |

# 7. Définir une politique en matière de code PIN utilisateur

L'administrateur peut définir une politique de restriction pour le code PIN utilisateur. Cette politique consiste à définir la longueur minimum du code PIN (de 7 à 15 chiffres), ainsi que la saisie ou non d'un « caractère spécial ». Le « **caractère spécial** » fonctionne à l'aide de « **SHIFT + chiffre** ».

Pour définir une politique (restrictions) en matière de code PIN d'utilisateur, vous devez saisir 3 chiffres, par exemple « **091** », les deux premiers chiffres (**09**) indiquent la longueur minimale du PIN (dans ce cas, **9**) et le dernier chiffre (1) indique qu'un « caractère spécial » doit être utilisé, en d'autres termes « **SHIFT + chiffre**. » De la même manière, une politique de code PIN utilisateur peut être définie sans recourir à un « caractère spécial », par exemple « **120** », les deux premiers chiffres (**12**) indiquent la longueur minimale du PIN (dans ce cas, 12) et le dernier chiffre (**0**), qui indique qu'aucun caractère spécial
n'est requis.

Une fois que l'administrateur a défini la politique de code PIN utilisateur, par exemple « 091 », un nouveau code PIN utilisateur doit être créé. Si l'administrateur crée le code PIN utilisateur « **247688314** » avec l'utilisation d'un « **caractère spécial** » (shift+chiffre), celui-ci peut être placé n'importe où dans votre code PIN de 7 à 15 chiffres durant le processus de création du code PIN utilisateur, comme montré dans les exemples ci-dessous.

**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**',

**Remarque :**

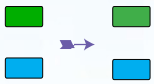
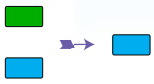
- Si un « caractère spécial » a été utilisé durant la création du code PIN utilisateur, par exemple, l'exemple « **B** » ci-dessus, ce disque ne peut être déverrouillé qu'en saisissant le code PIN avec le « caractère spécial » précisément dans l'ordre créé soit, dans l'exemple « **B** » ci-dessus - (« 2 », « 4 », « **SHIFT + 7** » , « 6 », « 8 », « 8 », « 3 », « 1 », « 4 »).

- Les utilisateurs peuvent changer leur code PIN mais sont contraints de respecter la « politique de code PIN utilisateur » définie (restrictions), si et quand elle est applicable.

- Le fait de définir une nouvelle politique en matière de code PIN utilisateur supprimera automatiquement le code PIN utilisateur s'il en existe un.

- Celle politique ne s'applique pas au « code PIN d'autodestruction ». Le paramètre de complexité pour le code PIN d'autodestruction et le code PIN admin est toujours de 7 à 15 chiffres, sans caractère spécial requis.

**Pour définir une politique de code PIN utilisateur**, accédez d'abord au mode administrateur tel que décrit dans la section 5. **Une fois que le disque est en mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 7** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue |
| 2.Saisissez vos **3 chiffres**, n'oubliez pas que les deux premiers chiffres représentent la longueur minimale du code PIN et que le dernier chiffre (0 ou 1) indique si un caractère spécial a été utilisé ou non. |  | Blinking GREEN and solid BLUE LEDs will continue to blink |
| 3. Appuyez une fois sur le bouton «**SHIFT**» ( ⬆ ) |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE continue, puis une LED BLEUE continue, indiquant que le code PIN utilisateur a été correctement défini. |

## 8. Comment vérifier la politique de code PIN utilisateur

L'administrateur peut vérifier la politique de code PIN utilisateur et peut identifier la règle de longueur minimale du code PIN et si l'utilisation d'un caractère spéciale a été définie ou non en notant la séquence de LED décrite ci-dessous.

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

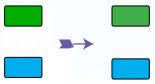
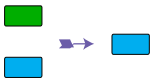
| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons «**SHIFT**» ( ⬆ ) + **7** |  | La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes |
| 2. Appuyez sur le bouton « **DÉVERROUILLER** » et vous observerez ce qui suit :<br><br>a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>b. Un clignotement de la LED ROUGE est égal à dix (10) unités d'un code PIN.<br>c. Chaque clignotement de la LED VERTE est égal à une (1) unité d'un code PIN.<br>d. Un clignotement BLEU indique l'utilisation d'un caractère spécial.<br>e. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>f. Les LED reviennent au BLEU continu. | | |

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

| **Description du PIN** | **Configuration à 3 chiffres** | **ROUGE** | **VERT** | **BLEU** |
|---|---|---|---|---|
| Code PIN de 12 chiffres avec utilisation d'un caractère spécial | 121 | 1 clignotement | 2 clignotements | 1 clignotement |
| Code PIN de 12 chiffres SANS utilisation d'un caractère spécial | 120 | 1 clignotement | 2 clignotements | 0 |
| Code PIN de 9 chiffres avec utilisation d'un caractère spécial | 091 | 0 | 9 clignotements | 1 clignotement |
| Code PIN de 9 chiffres SANS utilisation d'un caractère spécial | 090 | 0 | 9 clignotements | 0 |

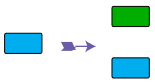
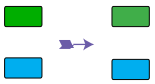
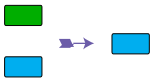
## 9. Ajouter un nouveau code PIN utilisateur en mode administrateur

Pour ajouter un **nouvel utilisateur**, accédez d'abord au **mode administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 3** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue. |
| 2. Saisissez le nouveau code PIN utilisateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE continue. |
| 3. Ressaisissez le nouveau code PIN utilisateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | La LED VERTE clignote rapidement pendant quelques secondes, puis est remplacée par la LED BLEUE continue, indiquant que le code PIN utilisateur a été correctement créé. |

## 10. Modifier le code PIN utilisateur en mode administrateur

Pour modifier un **code PIN utilisateur** existant, accédez d'abord au **mode administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 3** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue. |
| 2. Saisissez le nouveau code PIN utilisateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE continue. |
| 3. Ressaisissez le nouveau code PIN utilisateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | La LED VERTE clignote rapidement pendant quelques secondes, puis est remplacée par la LED BLEUE continue, indiquant que le code PIN utilisateur a été correctement modifié. |

## 11. Supprimer le code PIN utilisateur en mode administrateur

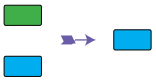
Pour supprimer un **code PIN utilisateur**, accédez d'abord au **mode administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **SHIFT** (⬆) **+ 3** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par la LED ROUGE clignotante. |
| 2. Appuyez à nouveau sur les boutons « **SHIFT** (⬆) **+ 3** » et maintenez-les enfoncés. |  | La LED ROUGE clignotante est remplacée par la LED ROUGE continue, puis par la LED BLEUE continue, indiquant que le code PIN utilisateur a été correctement supprimé. |

## 12. Définir le mode de lecture seule en mode administrateur

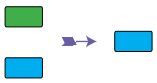
**Important :** si les données viennent d'être copiées sur le diskAshur PRO², veillez d'abord à déconnecter correctement le disque en cliquant sur Supprimer le périphérique en toute sécurité/Éjecter le diskAshur PRO² du système d'exploitation avant de reconnecter et de définir le diskAshur PRO² sur « Lecture seule/Protection en écriture ».

Quand l'administrateur écrit du contenu sur le diskAshur PRO² et limite l'accès au mode lecture seule, l'utilisateur ne peut pas modifier ce paramètre en mode utilisateur. Pour configurer le diskAshur PRO² en mode lecture seule, accédez d'abord au **mode administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **7 + 6** » et maintenez-les enfoncés. (7 = **R**ead (lecture) + 6 = **O**nly (seule)) |  | La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Relâchez les boutons 7 + 6 et appuyez sur « **DÉVERROUILLER** ». |  | Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue, puis par la LED BLEUE continue, indiquant que le disque est configuré en mode lecture seule. |

## 13. Activer le mode lecture/écriture en mode administrateur

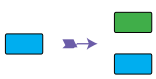
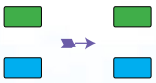
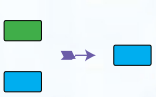
Pour configurer le diskAshur PRO² en mode lecture/écriture, accédez d'abord au **mode administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **7 + 9** » et maintenez-les enfoncés. (7 = **R**ead (lecture) + 9 = **W**rite (écriture)) |  | La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Relâchez les boutons 7 + 9 et appuyez sur « **DÉVERROUILLER** ». |  | Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue, puis par la LED BLEUE continue, indiquant que le disque est configuré en mode lecture/écriture. |

## 14. Comment créer un code PIN d'autodestruction

Avec la fonctionnalité d'autodestruction, vous définissez un code PIN permettant d'effacer les données chiffrées sur le disque entier. Lorsqu'il est utilisé, le code PIN d'autodestruction **supprime TOUTES les données, les codes PIN administrateur/utilisateur,** et déverrouille le disque. L'activation de cette fonctionnalité définit le code PIN d'autodestruction comme le nouveau code PIN utilisateur, et le diskAshur PRO² doit être partitionné et formaté avant que toute nouvelle donnée puisse être ajoutée au disque.

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

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 6** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue. |
| 2. Créez un code PIN d'autodestruction de 7 à 15 chiffres et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE continue. |
| 3. Ressaisissez le code PIN et appuyez sur le bouton « **DÉVERROUILLER** ». |  | La LED VERTE clignote rapidement pendant plusieurs secondes, puis est remplacée par la LED BLEUE continue pour indiquer que le code PIN d'autodestruction a été correctement configuré. |

## 15. Comment supprimer le code PIN d'autodestruction

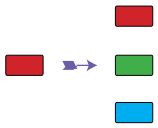
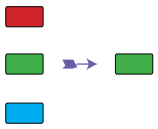
Pour supprimer le code PIN d'autodestruction, accédez d'abord au **mode administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 6** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par la LED ROUGE clignotante. |
| 2. Appuyez à nouveau sur les boutons « **SHIFT** ( ⬆ ) **+ 6** » et maintenez-les enfoncés. |  | La LED ROUGE clignotante devient continue, puis est remplacée par la LED BLEUE continue, indiquant que le code PIN d'autodestruction a été correctement supprimé. |

## 16. Comment déverrouiller avec le code PIN d'autodestruction

Lorsqu'il est utilisé, le code PIN d'autodestruction **supprime la clé de chiffrement, TOUTES les données, les codes PIN administrateur/utilisateur,** puis déverrouille le disque. Activer cette fonctionnalité définit le **code PIN d'autodestruction comme le nouveau code PIN utilisateur**, et le diskAshur Pro² doit être partitionné et formaté avant que toute nouvelle donnée puisse être ajoutée au disque.

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

| | | |
|---|---|---|
| 1. En état de veille, appuyez sur le bouton « **DÉVERROUILLER** ». |  | La LED ROUGE est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter. |
| 2. Saisissez le code PIN d'autodestruction et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED ROUGE, VERTE et BLEUE clignotantes sont remplacées par les LED VERTE et BLEUE qui clignotent en alternance pendant environ 15 secondes avant d'être remplacées par la LED VERTE continue. |

**Important :** quand le mécanisme d'autodestruction est activé, toutes les données, la clé de chiffrement et les codes PIN administrateur/utilisateur sont supprimés. **Le code PIN d'autodestruction devient le code PIN utilisateur.** Aucun code PIN administrateur n'existe après l'activation du mécanisme d'autodestruction. Le diskAshur PRO² doit d'abord être réinitialisé (voir la section 26 « Comment effectuer une réinitialisation complète » à la page 94) afin de créer un code PIN administrateur avec les pleins privilèges administrateur, notamment la possibilité de créer un code PIN utilisateur.

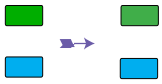
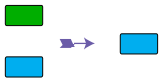
## 17. Comment créer un code PIN administrateur après une attaque par force brute ou une réinitialisation

Après une attaque par force brute ou quand le diskAshur PRO² a été réinitialisé, vous devez créer un code PIN administrateur avant de pouvoir utiliser le disque. Si le disque a été attaqué par force brute ou réinitialisé, il se met en état de veille (LED ROUGE continue). Pour créer un code PIN administrateur, effectuez les étapes suivantes.

**Exigences pour le code PIN :**

- Doit être composé de 7 à 15 chiffres.
- Ne doit pas contenir que des nombres répétitifs (c.-à-d. 3-3-3-3-3-3-3-3).
- Ne doit pas contenir que des nombres consécutifs (c.-à-d. 1-2-3-4-5-6-7 ; 7-8-9-0-1-2-3-4 ; 7-6-5-4-3-2-1).

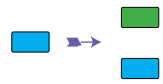
**Remarque :** la touche **SHIFT** peut être utilisée pour d'autres combinaisons. **SHIFT** + **1** est une valeur différente de 1. Pour créer un code PIN utilisant d'autres combinaisons, appuyez sur le bouton **SHIFT** et maintenez-le enfoncé pendant la saisie de votre code PIN de 7 à 15 chiffres (c.-à-d. **SHIFT** + **26756498**).

| | | |
|---|---|---|
| 1. En état de veille, appuyez sur les boutons « **SHIFT** ( ⬆ ) **+ 1** » et maintenez-les enfoncés. |  | La LED ROUGE continue est remplacée par les LED VERTE clignotante et BLEUE continue. |
| 2. Saisissez le NOUVEAU code PIN administrateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE continue. |
| 3. Ressaisissez le NOUVEAU code PIN administrateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | La LED VERTE clignotante et la LED BLEUE continue sont remplacées par la LED BLEUE qui se met à clignoter rapidement avant d'être continue, indiquant que le code PIN administrateur a été correctement configuré. |

## 18. Programmer la fonction de verrouillage automatique

Pour protéger le disque contre les accès non autorisés s'il est déverrouillé et laissé sans surveillance, il est possible de configurer le diskAshur PRO² de façon à ce qu'il se verrouille automatiquement au bout d'un intervalle de temps prédéfini. Par défaut, la fonctionnalité de verrouillage automatique du diskAshur PRO² est désactivée. Le verrouillage automatique peut être défini de façon à se déclencher au bout de 5 à 99 minutes.

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

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 5** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Saisissez la durée sur laquelle vous souhaitez définir le délai de verrouillage automatique, le délai minimal possible étant de 5 minutes et le maximal étant de 99 minutes (de 5 à 99 minutes). Par exemple, saisissez :<br>**05 pour 5 minutes ;**<br>**20 pour 20 minutes ;**<br>**99 pour 99 minutes.** | | |
| 3. Appuyez sur le bouton « **SHIFT** ( ⬆ ) ». |  | Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE continue pendant une seconde, puis enfin par la LED BLEUE continue, indiquant que le délai du verrouillage automatique a été correctement configuré. |

## 19. Désactiver le verrouillage automatique

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

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **DÉVERROUILLER + 5** » et maintenez-les enfoncés. |  | La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Saisissez « **00** » et appuyez sur le bouton « **SHIFT** ( ⬆ ) ». |  | Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE continue pendant une seconde, puis enfin par la LED BLEUE continue, indiquant que le délai du verrouillage automatique a été correctement désactivé. |

## 20. Comment vérifier la minuterie de verrouillage

L'administrateur est en mesure de vérifier et de déterminer la durée de temps définie pour la minuterie de verrouillage automatique en notant simplement la séquence des LED décrite dans le tableau en bas de cette page.

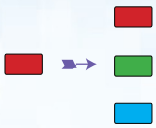
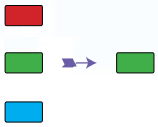
Pour vérifier le verrouillage automatique pour non utilisation, accédez d'abord au « mode administrateur » tel que décrit dans la section 5. Une fois que le lecteur est en mode administrateur (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « **SHIFT** » ( ⬆ ) + **5** |  | La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes |
| 2. Appuyez sur le bouton « **DÉVERROUILLER** » et vous observerez ce qui suit :<br><br>a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>b. Chaque clignotement de la LED ROUGE est égal à dix (10) minutes.<br>c. Chaque clignotement de la LED VERTE est égal à une (1) minute.<br>d. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>e. Les LED reviennent au BLEU continu. | | |

Le tableau ci-dessous décrit le comportement des LED lorsque vous vérifiez la minuterie de verrouillage automatique, par exemple si vous avez programmé le lecteur pour se verrouiller automatiquement au bout de **26** minutes, la LED ROUGE clignotera deux (**2**) fois et la LED VERTE clignotera six (**6**) fois.

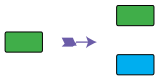
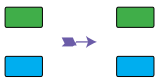
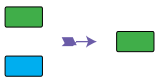
| **Verrouillage automatique en minutes** | **ROUGE** | **VERT** |
|---|---|---|
| 8 minutes | 0 | 8 clignotements |
| 15 minutes | 1 clignotement | 5 clignotements |
| 26 minutes | 2 clignotements | 6 clignotements |
| 40 minutes | 4 clignotements | 0 |

## 21. Comment déverrouiller le diskAshur PRO² avec le code PIN utilisateur

| | | |
|---|---|---|
| 1. En état de veille (LED ROUGE continue), appuyez sur le bouton « **DÉVERROUILLER** ». |  | La LED ROUGE est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter. |
| 2. Saisissez le code PIN utilisateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED clignotant en ROUGE, VERT et BLEU sont remplacées pour alterner entre les LED VERTE et BLEUE, puis par une LED VERTE qui se met à clignoter rapidement avant d'être continue, indiquant que le disque a été correctement déverrouillé en mode utilisateur. |

## 22. Modifier le code PIN utilisateur en mode utilisateur

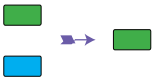
Pour modifier le **code PIN utilisateur**, déverrouillez d'abord le diskAshur PRO² avec un code PIN utilisateur tel que décrit dans la section 21. Une fois que le disque est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode utilisateur, appuyez sur les boutons « **DÉVERROUILLER + 4** » et maintenez-les enfoncés. |  | La LED VERTE continue est remplacée par les LED VERTE clignotante et BLEUE continue. |
| 2. Saisissez le nouveau code PIN utilisateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE continue. |
| 3. Ressaisissez le nouveau code PIN utilisateur et appuyez sur le bouton « **DÉVERROUILLER** ». |  | Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui se met à clignoter rapidement avant d'être continue, indiquant que le code PIN utilisateur a été correctement modifié. |

## 23. Définir le mode de lecture seule en mode utilisateur

**Important :** si les données viennent d'être copiées sur le diskAshur PRO², veillez d'abord à déconnecter correctement le disque en cliquant sur Supprimer le périphérique en toute sécurité/Éjecter le diskAshur PRO² du système d'exploitation avant de reconnecter et de définir le diskAshur PRO² sur « Lecture seule/Protection en écriture ».

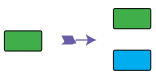
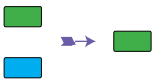
Pour configurer le diskAshur PRO² en mode lecture seule, accédez d'abord au **mode utilisateur** tel que décrit dans la section 21. Une fois que le disque est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode utilisateur, appuyez sur les boutons « **7 + 6** » et maintenez-les enfoncés. (7 = **R**ead (lecture) + 6 = **O**nly (seule)) |  | La LED VERTE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Relâchez les boutons 7 + 6 et appuyez sur « **DÉVERROUILLER** ». |  | Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue indiquant que le disque est configuré en mode lecture seule. |

**Remarque :**
1. Ce paramètre sera activé la prochaine fois que le disque sera déverrouillé.
2. Si un utilisateur configure le disque en mode lecture seule, l'administrateur peut modifier ce paramètre par le mode lecture/écriture en mode administrateur.
3. Si l'administrateur configure le disque en mode lecture seule, l'utilisateur ne peut pas configurer le disque en mode lecture/écriture.

## 24. Activer le mode lecture/écriture en mode utilisateur

Pour configurer le diskAshur PRO² en mode lecture/écriture, accédez d'abord au **mode utilisateur** tel que décrit dans la section 21. Une fois que le disque est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode utilisateur, appuyez sur les boutons « **7 + 9** » et maintenez-les enfoncés. (7 = **R**ead (lecture) + 9 = **W**rite (écriture)) |  | La LED VERTE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Relâchez les boutons 7 + 9 et appuyez sur « **DÉVERROUILLER** ». |  | Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue indiquant que le disque est configuré en mode lecture/écriture. |

**Remarque :**
1. Ce paramètre sera activé la prochaine fois que le disque sera déverrouillé.
2. Si un utilisateur configure le disque en mode lecture seule, l'administrateur peut modifier ce paramètre par le mode lecture/écriture en mode administrateur.
3. Si l'administrateur configure le disque en mode lecture seule, l'utilisateur ne peut pas configurer le disque en mode lecture/écriture.

## 25. Protection contre les attaques par force brute

Si un code PIN incorrect est saisi 15 fois consécutives (3 x 5 groupes de codes PIN), tous les codes PIN administrateur/utilisateur, la clé de chiffrement et toutes les données sont supprimés et perdus à jamais. Le diskAshur PRO² doit ensuite être formaté et partitionné avant de pouvoir être réutilisé.

**1.** Si un code PIN incorrect est saisi 5 (cinq) fois consécutives, toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu.

**2.** Déconnectez le disque et reconnectez-le à l'hôte afin de disposer de cinq tentatives supplémentaires pour saisir le code de PIN. Si le code PIN saisi est incorrect 5 fois de plus (10 fois au total : 5 fois à l'étape 1 et 5 fois à l'étape 2), toutes les LED (ROUGE, VERTE et BLEUE) s'allument à nouveau en continu.

**3**. Déconnectez le disque, maintenez le bouton « **SHIFT** » enfoncé et reconnectez-le à l'hôte : toutes les LED (ROUGE, VERTE et BLEUE) s'allument et clignotent simultanément.

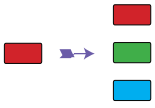
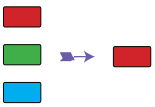
**4**. Pendant que les LED clignotent, saisissez « **47867243** » et appuyez sur le bouton « **DÉVERROUILLER** » pour disposer de 5 dernières tentatives.

**Attention :** À l'issue de 15 saisies incorrectes consécutives du code PIN, le mécanisme de défense contre la force brute se déclenche et supprime tous les codes PIN administrateur/utilisateur, la clé de chiffrement et les données. Un nouveau code PIN administrateur doit être créé : consultez la section 17 de la page 90 intitulée « Comment créer un code PIN administrateur après une attaque par force brute ou une réinitialisation ». Le diskAshur PRO² doit aussi être partitionné et formaté avant que toute nouvelle donnée puisse être ajoutée au disque.

## 26. Comment effectuer une réinitialisation complète

Pour effectuer une réinitialisation complète, le diskAshur PRO² doit être en état de veille (LED ROUGE continue). Une fois que le disque est réinitialisé, tous les codes PIN administrateur/utilisateur, la clé de chiffrement et toutes les données sont supprimés et perdus à jamais, et le disque doit être formaté et partitionné avant de pouvoir être réutilisé.

Pour réinitialiser le diskAshur PRO², effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En état de veille, appuyez sur le bouton « **0** » et maintenez-le enfoncé jusqu'à ce que toutes les LED se mettent à clignoter en alternance. |  | La LED ROUGE continue est remplacée par toutes les LED, ROUGE, VERTE et BLEUE, qui se mettent à clignoter en alternance. |
| 2. Appuyez sur les boutons « **2 + 7** » et maintenez-les enfoncés jusqu'à ce que toutes les LED deviennent continues pendant une seconde, puis soient remplacées par la LED ROUGE continue. |  | Les LED ROUGE, VERTE et BLEUE qui clignotaient en alternance s'allument toutes en continu pendant une seconde, puis sont remplacées par une LED ROUGE continue indiquant que le disque a été réinitialisé. |

**Important :** après une réinitialisation complète, un nouveau code PIN administrateur doit être créé : consultez la section 17, page 90 intitulée « Comment créer un code PIN administrateur après une attaque par force brute ou une réinitialisation ». Le diskAshur PRO² doit aussi être partitionné et formaté avant que toute nouvelle donnée puisse être ajoutée au disque.

# 27. Initialiser et formater le diskAshur PRO²

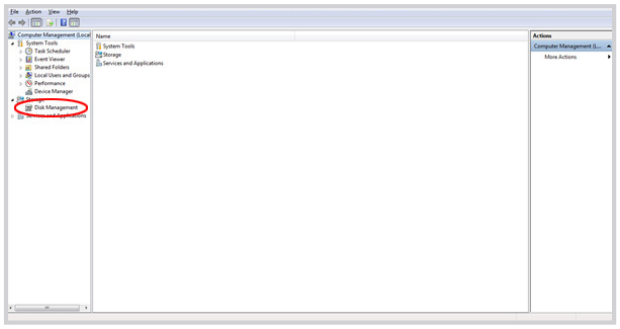
Après une « attaque par force brute » ou une réinitialisation complète du diskAshur PRO², toutes les données, la clé de chiffrement et les paramètres de partition sont supprimés.

Vous devez initialiser et formater le diskAshur PRO² avant de pouvoir l'utiliser.

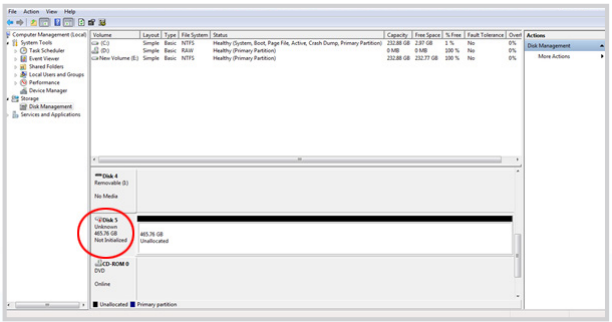
Pour initialiser le diskAshur PRO², effectuez les étapes suivantes :

1. Branchez le diskAshur PRO² à l'ordinateur.
2. Créez un nouveau code PIN administrateur : voir page 90, section 17 « Comment créer un code PIN administrateur après une attaque par force brute ou une réinitialisation ».
3. Lorsque le diskAshur PRO² est en état de veille (LED ROUGE), saisissez le nouveau code PIN administrateur afin de le déverrouiller (LED VERTE).
4. **Windows 7 :** Faites un clic droit sur **Ordinateur**, cliquez sur **Gérer**, puis sélectionnez **Gestion des disques**.
   **Windows 8** : Faites un clic droit dans le coin gauche du bureau et sélectionnez **Gestion des disques**.
   **Windows 10 :** Faites un clic droit sur le bouton Démarrer et sélectionnez **Gestion des disques**.
5. Dans la fenêtre Gestion de l'ordinateur, cliquez sur **Gestion des disques**. Dans la fenêtre Gestion des disques, le diskAshur PRO² est reconnu comme périphérique inconnu non initialisé et non alloué.

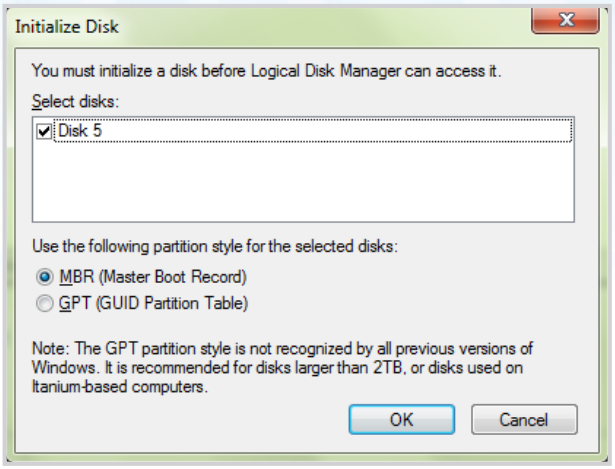
**Remarque :** si la fenêtre Initialiser l'assistant de disque s'ouvre, cliquez sur **Annuler.**



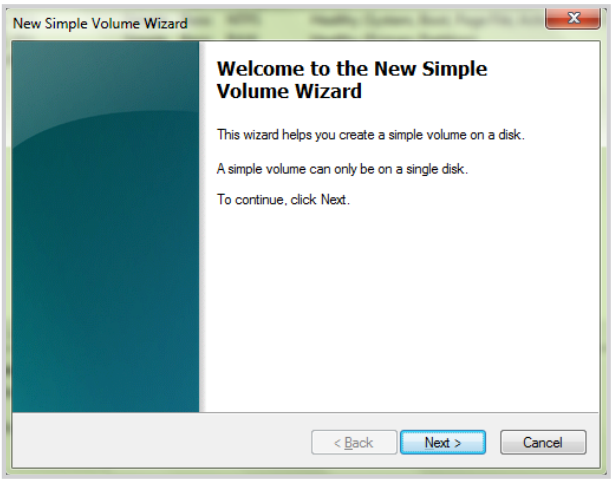
6. Faites un clic droit sur Disque inconnu, puis sélectionnez Initialiser le disque.



7. Dans la fenêtre Initialiser le disque, cliquez sur **OK**.




8. Faites un clic droit dans la zone vide située sous la section Non alloué, puis sélectionnez Nouveau volume simple. La fenêtre de bienvenue dans l'Assistant Création d'un volume simple s'ouvre.




9. Cliquez sur **Suivant**.
10. Si vous avez besoin d'une seule partition, acceptez la taille de partition par défaut et cliquez sur **Suivant**.
11. Affectez une lettre ou un chemin de disque et cliquez sur **Suivant**.
12. Créez un libellé de volume, sélectionnez Effectuer un formatage rapide, puis cliquez sur **Suivant**.
13. Cliquez sur **Terminer**.
14. Patientez jusqu'à la fin du formatage. Le diskAshur PRO² est reconnu et peut être utilisé.

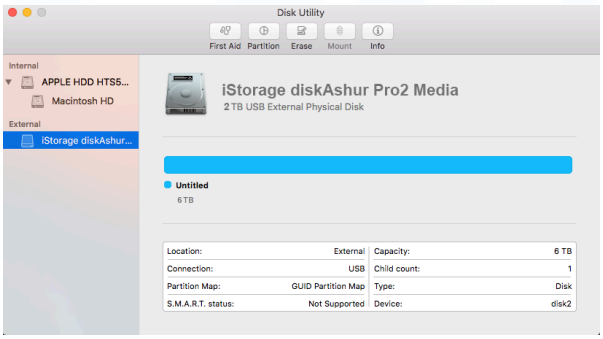
# 28. Configuration du diskAshur PRO² pour Mac OS

Le diskAshur PRO² est préformaté exFAT. Pour reformater le disque en un format compatible Mac, lisez les informations indiquées ci-après.

Une fois que le disque est déverrouillé, ouvrez Utilitaire de disque dans Applications/Utilitaires/Utilitaires de disque.

**Pour formater le diskAshur PRO² :**

1. Sélectionnez diskAshur PRO² dans la liste des disques et des volumes. Chaque disque de la liste affiche sa capacité, son fabricant et le nom de produit, tel que « iStorage diskAshur PRO² Media » ou 232.9 diskAshur PRO².




2. Cliquez sur le bouton « Erase » (Effacer) (figure 1).




figure 1

3. Saisissez un nom pour le disque (figure 2). Le nom par défaut est Sans titre. Le nom du disque finit par apparaître sur le bureau.

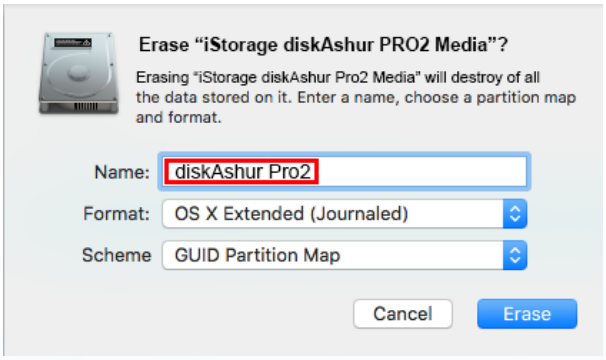



figure 2

4. Sélectionnez un format de modèle et de volume à utiliser. Le menu déroulant Volume Format (Format de volume) (figure 3) répertorie les formats de disque disponibles pris en charge par Mac. Le type de format recommandé est « Mac OS Extended (Journaled) ». Le menu déroulant du format de modèle répertorie les modèles disponibles à utiliser (figure 4). Nous vous recommandons d'utiliser « GUID Partition Map » sur les disques d'une capacité supérieure à 2 To.

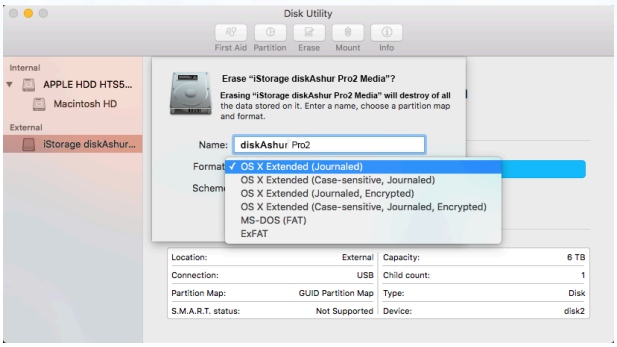


figure 3

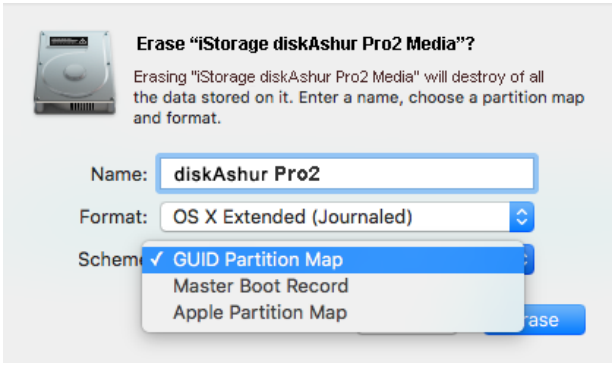


figure 4

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

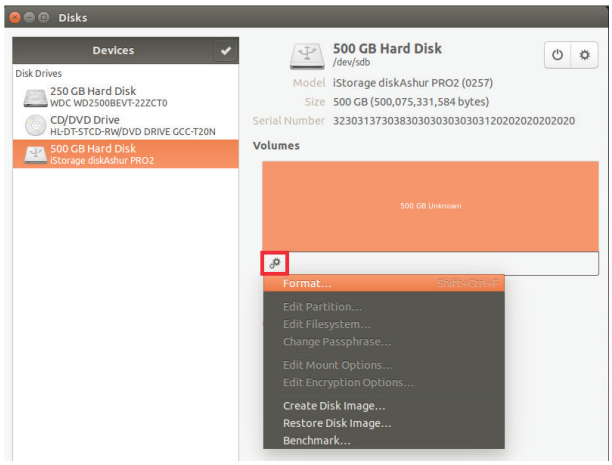
# 29. Configuration du diskAshur PRO² pour Linux (Ubuntu 17.10)

Si votre diskAshur PRO² a été initialisé et formaté exFAT, vous pouvez utiliser votre disque sous Ubuntu.
Si ce n'est pas le cas, veuillez suivre les instructions ci-dessous.
Pour formater le diskAshur PRO² sous système de fichier FAT:

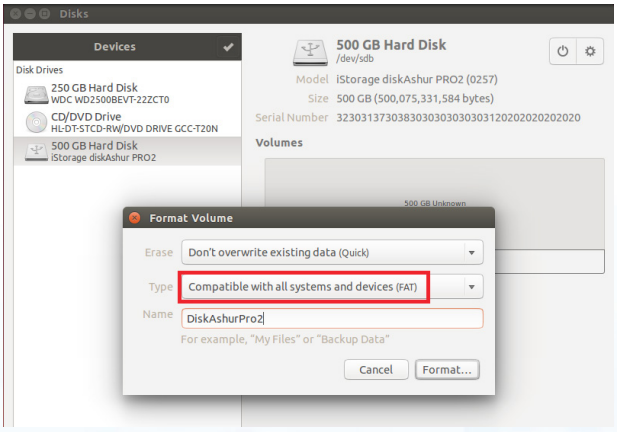
1. Ouvrir '**Toutes les applications**' et tapez le mot-clé '**Disques**' dans le champ de recherche. Cliquez sur l'utilitaire '**Disques**' lorsqu'il s'affiche.



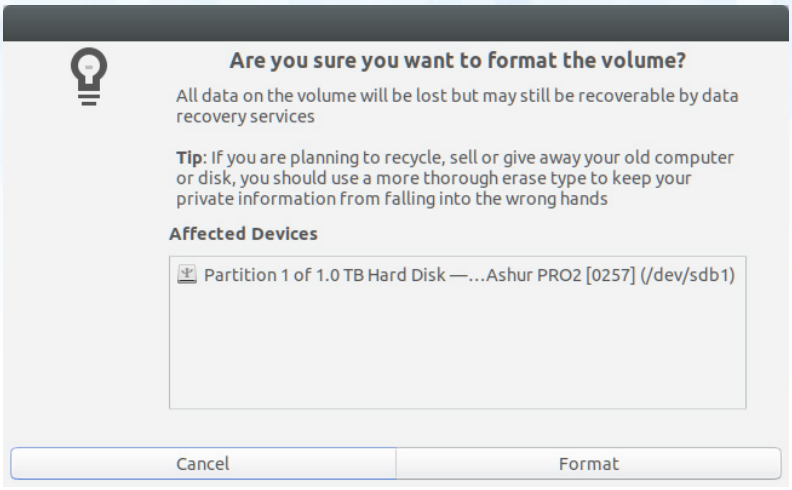

2. Sélectionnez le disque (Disque dur de 500Go) que vous souhaitez formater sous le '**gestionnaire de périphériques**'. Ensuite, cliquez dans le menu d'actions sous l'onglet '**Volumes**' et sélectionnez '**Formater**'



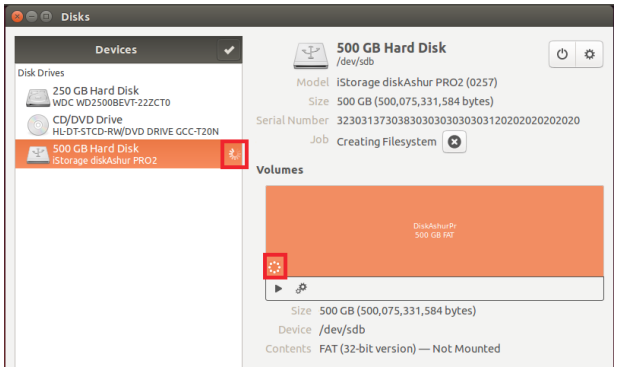

3. Sélectionnez '**Compatible avec tous les systèmes et périphériques (FAT)**' pour l'option '**Type**' de fichier. Et entrez un nom pour le disque, par exemple: diskAshur PRO². Ensuite, cliquez sur le bouton '**Formater**'.



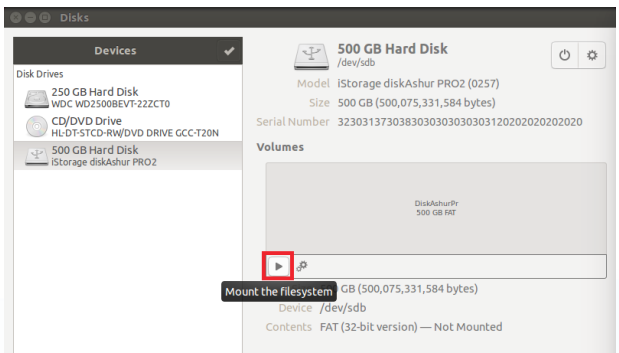
4. Cliquez de nouveau sur '**Formater**'



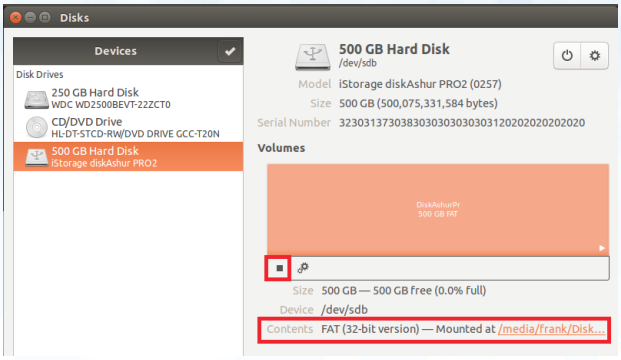

5. Le formatage du disque commence.



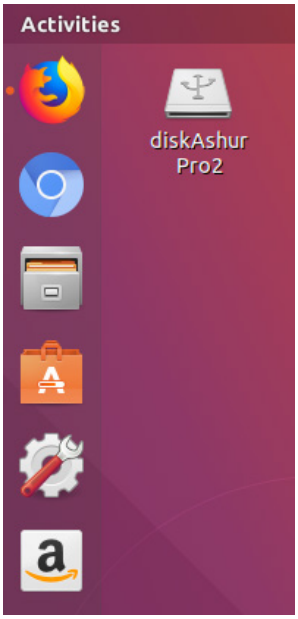

6. Une fois le processus de formatage terminé, cliquez ▶ pour monter le disque sous Ubuntu.



7. Le disque est maintenant monté et prêt à l'emploi.

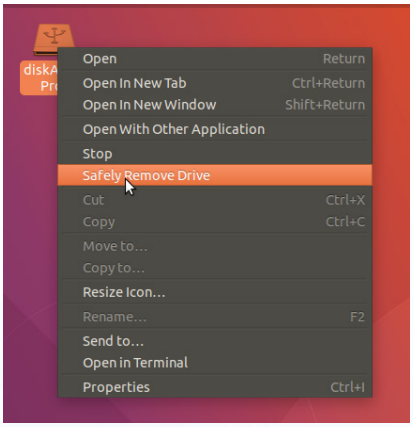



8. Un icône disque devrait être visible comme dans l'exemple ci-dessous. Vous pouvez cliquer sur l'icône disque pour ouvrir votre disque.




## Déconnecter votre diskAshur PRO² pour Linux (Ubuntu 17.10)

Il est **vivement recommandé de faire un clic droit sur l'icône du disque et de sélectionner 'éjecter'** pour retirer votre diskAshur PRO² en toute sécurité depuis , surtout si des données ont été copiées ou supprimées sur le disque.



## 30. Mettre en veille prolongée, suspendre ou se déconnecter du système d'exploitation

Veillez à sauvegarder et à fermer tous les fichiers sur le diskAshur PRO² avant de le mettre en veille prolongée, de le suspendre ou de le déconnecter du système d'exploitation.

Il est recommandé de verrouiller le diskAshur PRO² manuellement avant de le mettre en veille prolongée, de le suspendre ou de le déconnecter de votre système.

Pour verrouiller le disque, appuyez simplement sur le bouton « VERROUILLER » sur le diskAshur PRO² ou en cliquant sur l'icône « Supprimer le périphérique en toute sécurité/Éjecter » dans votre système d'exploitation.

**Attention :** pour vous assurer que vos données sont sécurisées, veillez à verrouiller le diskAshur PRO² si vous vous éloignez de votre ordinateur.

## 31. Comment vérifier la version du firmware en mode administrateur

Pour vérifier le numéro de la version du firmware, accédez d'abord au **mode administrateur** tel que décrit dans la section 5. Une fois que le disque est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode administrateur, appuyez sur les boutons « 3 + 8 » et maintenez-les enfoncés jusqu'à ce que les LED VERTE et BLEUE clignotent simultanément. |  | La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Appuyez sur le bouton « **DÉVERROUILLER** » et vous observerez ce qui suit :<br><br>a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>b. La LED ROUGE clignote, indiquant la partie intégrante du numéro de révision la version du firmware.<br>c. La LED VERTE clignote, indiquant la partie fractionnaire du numéro.<br>d. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>e. Les LED reviennent au BLEU continu. | | |

Par exemple, si le numéro de de la version du firmware est « 1.2 », la LED ROUGE clignote une (1) fois et la LED VERTE clignote deux (2) fois. Une fois la séquence terminée, les LED ROUGE, VERTE et BLEUE clignotent une fois simultanément, puis sont remplacées par la LED BLEUE continue.

## 32. Comment vérifier la version du firmware en mode utilisateur

Pour vérifier le numéro de la version du firmware, accédez d'abord au **mode utilisateur** tel que décrit dans la section 21. Une fois que le disque est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

| | | |
|---|---|---|
| 1. En mode utilisateur, appuyez sur les boutons « 3 + 8 » et maintenez-les enfoncés jusqu'à ce que les LED VERTE et BLEUE clignotent simultanément. |  | La LED VERTE continue est remplacée par les LED VERTE et BLEUE clignotantes. |
| 2. Appuyez sur le bouton « **DÉVERROUILLER** » et vous observerez ce qui suit :<br><br>a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>b. La LED ROUGE clignote, indiquant la partie intégrante du numéro de la version du firmware.<br>c. La LED VERTE clignote, indiquant la partie fractionnaire du numéro.<br>d. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.<br>e. Les LED reviennent au BLEU continu. | | |

Par exemple, si le numéro de la version du firmware est « 1.2 », la LED ROUGE clignote une (1) fois et la LED VERTE clignote deux (2) fois. Une fois la séquence terminée, les LED ROUGE, VERTE et BLEUE clignotent une fois simultanément, puis sont remplacées par la LED BLEUE continue.

# 33. Assistance technique

iStorage vous fournit les ressources utiles suivantes :

Site Web d'iStorage
https://www.istorage-uk.com

Correspondance par courriel
support@istorage-uk.com

Assistance téléphonique avec notre service d'assistance technique au **+44 (0) 20 8991 6260**.
Les spécialistes de l'assistance technique d'iStorage sont disponibles de 9 h 00 à 17 h 30 GMT, du lundi au vendredi

# 34. Informations de garantie et du service après-vente (SAV)

**Garantie de trois ans :**

iStorage offre une garantie de 3 ans sur le iStorage diskAshur PRO² contre les vices de fabrication et de main-d'œuvre dans des conditions d'utilisation normales. La période de garantie prend effet à la date de l'achat, effectué directement auprès d'iStorage ou d'un revendeur autorisé.

**Clause et conditions de non-responsabilité :**

LA GARANTIE PREND EFFET À LA DATE D'ACHAT ET DOIT ÊTRE VÉRIFIÉE À L'AIDE DE VOTRE TICKET DE CAISSE OU FACTURE MENTIONNANT LA DATE D'ACHAT DU PRODUIT. ISTORAGE RÉPARERA OU REMPLACERA, SANS FRAIS SUPPLÉMENTAIRES, LES PIÈCES DÉFECTUEUSES PAR DE NOUVELLES PIÈCES OU DES PIÈCES D'OCCASION UTILISABLES COMPARABLES AUX NEUVES EN MATIÈRE DE PERFORMANCE. TOUTES LES PIÈCES ÉCHANGÉES ET LES PRODUITS REMPLACÉS AU TITRE DE CETTE GARANTIE DEVIENNENT LA PROPRIÉTÉ D'ISTORAGE.
CETTE GARANTIE NE COUVRE PAS LES PRODUITS NON ACHETÉS DIRECTEMENT AUPRÈS D'ISTORAGE OU D'UN REVENDEUR AUTORISÉ, NI LES PRODUITS ENDOMMAGÉS OU RENDUS DÉFECTUEUX : 1. À LA SUITE D'UN ACCIDENT, D'UN USAGE NON CONFORME, DE NÉGLIGENCE, D'ABUS, DE MANQUEMENT OU D'INCAPACITÉ DE SUIVRE LES INSTRUCTIONS ÉCRITES FOURNIES DANS LE GUIDE D'INSTRUCTIONS ; 2. PAR L'UTILISATION DE PIÈCES NON FABRIQUÉES OU VENDUES PAR ISTORAGE ; 3. PAR LA MODIFICATION DU PRODUIT ; 4. À LA SUITE
D'UN SERVICE, D'UNE ALTÉRATION OU D'UNE RÉPARATION EFFECTUÉE PAR QUICONQUE AUTRE QU'ISTORAGE, ET SERA NULLE. CETTE GARANTIE NE COUVRE PAS L'USURE NORMALE.
AUCUNE AUTRE GARANTIE, EXPRESSE OU IMPLICITE, Y COMPRIS TOUTE GARANTIE IMPLICITE DE CONFORMITÉ D'USAGE POUR UN EMPLOI PARTICULIER, N'A ÉTÉ OU NE SERA FAITE PAR ISTORAGE, EN SON NOM OU EN VERTU DE LA LOI EN CE QUI CONCERNE LE PRODUIT OU SON INSTALLATION, UTILISATION, FONCTIONNEMENT, REMPLACEMENT OU RÉPARATION.
ISTORAGE N'EST PAS RESPONSABLE EN VERTU DE CETTE GARANTIE, OU AUTREMENT, POUR TOUT DOMMAGE ACCESSOIRE, SPÉCIAL OU CONSÉQUENSIEL, Y COMPRIS TOUTE PERTE DE DONNÉES DÉCOULANT DE L'UTILISATION OU DU FONCTIONNEMENT DU PRODUIT, QU'ISTORAGE AIT EU CONNAISSANCE OU NON DE LA POSSIBILITÉ DE TELS DOMMAGES.

# Annexe A

## Directive de sécurité iStorage n° 1 - Fonctionnalités de sécurité et manipulation sécurisée

Cette directive iStorage fournit une assistance produit dans le cadre d'une utilisation par des agences commerciales, de service public et gouvernementales des disques sécurisés iStorage et applique les consignes du document du NCSC (CESG):

Caractéristiques de sécurité CPA pour le chiffrement des supports matériels, version 1.2, en date d'avril 2012

La directive iStorage n°1 détaille les fonctionnalités de sécurité prises en charge par les disques sécurisés iStorage, ainsi que les bonnes pratiques de sécurité à employer lors de l'utilisation de périphériques sécurisés iStorage pour protéger les actifs informationnels confidentiels et marqués d'un niveau de sécurité tant sur site qu'à l'extérieur des locaux opérationnels, ou lorsque les disques sécurisés iStorage sont en transit.

Associées aux bonnes pratiques, les fonctionnalités de sécurité des disques offrent des mesures robustes d'atténuation des risques d'attaque physique, de vol, ou l'opportunité de compromettre les actifs de données stockés sur les disques sécurisés iStorage, afin de refuser l'opportunité d'accès non autorisé aux contenus protégés.

**Le risque :** les disques sécurisés d'iStorage sont catégorisés comme des objets de valeur attrayants, susceptibles de contenir des actifs de données confidentiels d'entreprise, gouvernementaux ou personnels/protégés (en lien avec le GDPR ou RGPD) et représentent à ce titre une cible pour les attaques physiques comme logiques sous forme de vol ou de compromission, s'ils sont :

- Laissés sans surveillance
- Visibles dans des lieux publics
- Laissés dans un état logique ouvert (utilisateur authentifié)
- Laissés dans un état non sécurisé en transit
- Lorsque les mesures de protection utilisées ne sont pas adaptées au niveau de confidentialité des actifs de données qu'ils contiennent
- Égarés ou perdus

Dans cette directive de sécurité iStorage n°1, nous fournissons les meilleurs conseils disponibles ainsi que des mesures d'atténuation pragmatiques et pratiques permettant de réduire la surface d'attaque.

**Mesures d'atténuation :** les fonctionnalités de sécurité du périphérique et les mesures d'atténuation mentionnées dans le document ci-dessous constituent les pratiques de sécurité optimales recommandées à mettre en œuvre lors de toute manipulation des disques sécurisés iStorage et sont présentées dans le **Tableau 1** ci-dessous. Cette approche a pour objectif de préserver le principe de sécurité **DIC+T** (**D**isponibilité, **I**ntégrité et **C**onfidentialité + **T**ransparence) et met en application les contrôles de sécurité exposés dans la norme ISO/IEC 27001 et le document NCSC (CESG) désigné :

### Tableau 1 - Mesures d'atténuation - Fonctionnalités produit - Manipulation sécurisée

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| **1**<br>Intégrité<br>Disponibilité<br>Transparence | **DEP.M311**<br>**DEP.1.M26** | **En transit** | Ne jamais laissez un disque iStorage sans surveillance dans un véhicule ou dans une situation visible en transit ;<br>Si le disque sécurisé doit être laissé sans surveillance, veillez à ce qu'il ne soit pas visible et fermez le véhicule entre le chargement et le déchargement du média ;<br>Si un disque iStorage est opérationnel et contient des actifs de données, il doit toujours être envoyé par l'entremise d'un service de livraison de confiance, avec suivi.<br>Les disques sécurisés iStorage sont fournis dans un emballage inviolable doté d'un sceau de sécurité. Si, lors de la réception, le sceau de sécurité est brisé ou montre des traces d'altération, le disque doit être considéré comme compromis. Signalez-le immédiatement auprès du service d'assistance technique d' iStorage au :<br>+44 (0) 20 8991-6260<br>Ou envoyez un e-mail à : support@istorage-uk.com |

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| 2<br>Disponibilité<br>Intégrité Confiidentialité | DEP.M1<br>DEP.M701 | Accès non autorisé | Pour atténuer et minimiser le risque de compromission des actifs de données stockés sur un disque sécurisé iStorage :<br><br>Ne laissez le disque sécurisé iStorage sans surveillance au milieu d'une session ouverte authentifiée ;<br><br>Pour éviter le risque d'accès non autorisé, placez le disque en mode verrouillé lorsqu'il n'est pas en cours d'utilisation ;<br><br>Configurez la minuterie de verrouillage automatique iStorage en cas de non-utilisation au bout d'un délai déterminé (consultez le manuel d'utilisation iStorage) ;<br><br>Lorsque vous n'utilisez pas le disque sécurisé iStorage, veillez à le retirer et à le placer en sécurité, avec les contrôles de sécurité physique adaptés.<br><br>Veillez toujours à ce que les actifs de données stockés sur le disque iStorage soient sauvegardés et disponibles en cas de perte du disque sécurisé iStorage. |
| 3<br>Confiidentialité<br>Transparence | DEP.M703 | Perte, vol, compromission | Veillez à disposer d'un processus prenant en charge le signalement à la direction de tout vol, perte ou compromission du disque sécurisé iStorage - par exemple :<br><br>i. Signalez la perte ou le vol à la police - et obtenez un numéro de procès-verbal<br><br>ii. Si l'appareil appartient à une entreprise, faites le nécessaire pour en aviser<br>le service Sécurité dans les plus brefs délais<br><br>iii. Au cas où l'appareil contient des données appartenant à une instance gouvernementale, signalez sans attendre l'incident au responsable des actifs d'information du service concerné.<br><br>iv. S'il s'agit de documents gouvernementaux classés secrets, prenez en compte les aspects liés à la confidentialité, au marquage de protection ou à toute autre restriction ainsi que les conséquences pour la sécurité nationale. |

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| | | | v. S'il s'agit de données commerciales, évaluez l'impact d'une perte ou d'une compromission po-tentielle des actifs stockés sur le support per-du/volé.<br><br>vi. Si l'actif est restitué, traitez-le comme compro-mis et prenez les mesures nécessaires pour le reformater et le réinitialiser avant de le réutiliser.<br><br>Si des actifs comportant un marquage de protection ou des données gouvernementales sont stockés sur le disque iStorage, demandez conseil à l'agence ou autorité concernée ;<br><br>Confirmez que les données étaient chiffrées au moment du vol ou de la perte (le disque n'était pas dans une ses-sion ouverte authen-tifiée) - afin d'établir que des actifs de données confidentielles ou autres formes d'information connexes ne seront pas compromises. |
| **4**<br>Intégrité | **DEP.1.M26** | **Dispositifs anti-violation** | Les disques iStorage sont protégés par des dispositifs anti-viola-tion.<br><br>Réalisez des contrôles réguliers du boîtier externe du disque sécurisé iStorage afin d'y trouver des indications de violation ou d'attaque physique directe.<br><br>Au cas peu probable où notre produit nécessiterait une mise à jour, nous ne fournissons pas de mises à jour de logiciel ou de firmware (ni en ligne, ni sur CD ou autre support), mais nous proposons un service de rappel et de remplacement, qui vous informera par e-mail dans un délai de 2 jours ouvrés avant l'expédition du nouveau produit, en précisant son numéro de série, lequel peut être vérifié à la réception par votre organisation. Cependant, protégez-vous contre la possibilité de recevoir un disque iStorage trafiqué ou contrefait par une tierce partie, en veillant à ce que votre organisation fournisse une formation et une sensibilisation adéquate en matière de sécurité afin d'informer les utilisateurs des risques potentiels.<br><br>**Remarque 1 :** Si vous constatez des signes avérés de falsification ou de contrefaçon de produit, veuillez immédiatement contacter le service d'assistance technique d'iStorage au :<br>+44 (0) 20 8991-6260<br>Ou envoyez un e-mail à :<br>support@istorage-uk.com |

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| 5<br>Confiidentialité<br>Intégrité | DEP.2.M12<br>DEP.2.M283<br>DEP.2.M285<br>DEP.2.M617 | Gestion de mot de passe robuste | Le mot de passe n'est jamais affiché durant la saisie.<br><br>Configurez toujours un mot de passe complexe pour les comptes d'administrateur et d'utilisateur sur le disque sécurisé iStorage afin d'atténuer la facilité des attaques et/ou compromissions logiques ;<br><br>Bien que l'appareil accepte des mots de passe com-portant au moins 7 chiffres de longueur, nous recom-mandons fortement à l'utilisateur de définir un mot de passe de complexité supérieure, par ex. pas moins de 8 chiffres, en utilisant la touche SHIFT en combinaison avec des chiffres ;<br><br>Choisissez une structure de mot de passe qui ne peut pas être devinée facilement ;<br><br>Évitez la réutilisation du mot de passe sur plusieurs sys-tèmes présentant des exigences de sécurité diffé-rentes ;<br><br>N'écrivez jamais un mot de passe sur une feuille de papier ; ne partagez jamais un mot de passe ;<br>Veillez à éviter que quiconque puisse lire votre mot de passe iStor-age lorsque vous le saisissez dans un endroit public ;<br><br>Si vous soupçonnez que le mot de passe a poten-tiellement été compris, il doit être modifié dans les plus brefs délais ;<br><br>Lorsqu'il existe une raison opérationnelle de documenter un mot de passe sous forme de copie papier, ceci doit être accompli de manière sécurisée ou en respectant le processus d'exemption de l'entreprise.<br><br>**Remarque 2 :** la consignation sécurisée d'un mot de passe peut être facilitée par un gestionnaire de mots de passe sécurisé, ou grâce à l'utilisation d'une enveloppe scellée sujette à des mesures de contrôle d'accès ro-bustes et protégée par un coffre-fort à com-binaison de haute qualité. |
| 6<br>Confiidentialité<br>Intégrité | DEP.2.M281 | Gestion du mot de passe administrateur | Le disque sécurisé iStorage prend en charge une fonctionnalité per-mettant à un administrateur d'obtenir un niveau d'accès privilégié pour gérer l'appareil.<br><br>Seuls les administrateurs autorisés et authentifiés peuvent ajouter ou révoquer des comptes attribués. |

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| **7**<br>Confiidentialité | **DEP.2.M277** | **Ingénierie sociale** | Soyez conscient de la menace potentielle représentée par des attaques d'ingénierie sociale directes ou indirectes visant à découvrir votre identifiant, votre mot de passe ou toute autre information personnelle ou professionnelle par le biais de techniques d'ingénierie sociale.<br><br>Veillez à ce que votre organisation fournisse une formation et une sensibilisation à la sécurité afin d'informer les utilisateurs des menaces potentielles que constituent :<br><br>i. Les courriers électroniques non sollicités qui incitent l'utilisateur à échanger des communications avec l'expéditeur<br><br>ii. Le fait d'ouvrir des liens intégrés à un e-mail inattendu, reçu d'un utilisateur inconnu<br><br>iii. Ouvrir des pièces jointes sans y prêter attention - elles pourraient contenir un logiciel malveillant<br><br>iv. Accepter des requêtes sur des sites de réseaux sociaux émanant de personnes que vous ne connaissez ou ne reconnaissez pas<br><br>v. Se laisser appâter par des offres en ligne - si elles ont l'air trop belles pour être vraies, c'est certainement le cas |
| **8**<br>Confiidentialité<br>Intégrité | **DEP.2.M280** | **Identifiants Distribution** | Ne transmettez ou ne fournissez jamais aucune forme d'identifiant de sécurité via le même canal, ou dans le même conditionnement qu'un disque sécurisé iStorage.<br><br>**Remarque 3 :** Lorsque les exigences opérationnelles nécessitent la distribution d'identifiants, ceci doit être réalisé hors réseau (par ex. par voix, texto, courrier électronique sécurisé). |
| **9**<br>Intégrité | **DEP.4.M348**<br>**DEP.1.M348** | **Mises à jour autorisées** | Il n'existe aucun processus automatisé. Seules les mises à jour approuvées qui s'appliquent aux produits iStorage seront distribuées dans le cadre d'un processus de mise à jour ou de remplacement conforme à la politique/processus de cycle de vie de sécurité et de gestion des vulnérabilités d'iStorage. |
| **10**<br>Confiidentialité<br>Transparence | | **Classification des données** | Veillez à ce que la valeur des actifs de données stockés sur le disque sécurisé iStorage soit classifiée, ou qu'ils portent un marquage de protection adapté à leur utilisation et/ou administration. |
| **11**<br>Confiidentialité | | **Personnel / accès autorisé** | Veillez à ce que les personnes qui obtiennent un accès aux actifs de données stockés sur un disque sécurisé iStorage puissent justifier d'un « besoin de savoir » clair et des autorisations adéquates en fonction de la classification de l'actif de données, ou des documents portant un marquage de protection qui y sont stockés |

# Annexe B

## Directive de sécurité iStorage n° 2 - Procédure d'effacement et

Cette directive iStorage fournit une assistance produit dans le cadre d'une utilisation des disques sécurisés iStorage par des agences commerciales, de service public et gouvernementales. Cette directive iStorage n°2 expose les bonnes pratiques de sécurité à employer pour l'effacement et l'élimination sécurisée des disques sécurisés iStorage, conformément à la directive **IS5** du gouvernement britannique relative à l'élimination sécurisée et fait référence à la **DEP.M.137** qui détaille les exigences en matière d'élimination sécurisée.

Cette directive aborde également la question de la remise en service de disques sécurisés afin de minimiser le risque de réutilisation d'un objet, ou la compromissions d'actifs de données stockés sur ces disques sécurisés iStorage.

**Le risque :** si les actifs de données stockés sur un disque sécurisé iStorage ne sont pas soumis à des contrôles de sécurité lors de la remise en service des disques ou de leur élimination au moment de leur fin de vie d'exploitation, ils pourraient être soumis à des risques en relation avec des contrôles obligatoires de sécurité organisationnelle et de protection des données, comme le GDPR ou RGPD. Par exemple :

- Exfiltration et transmission de données sensibles à des acteurs externes non autorisés
- Divulgation accidentelle
- Divulgation d'actifs de données portant un marquage de protection ou classés secrets par un gouvernement

**Objectif :** bien que les disques iStorage sécurisés assurent la protection des actifs de données qui y sont stockés grâce à un chiffrement robuste, une bonne pratique de sécurité consiste néanmoins à s'assurer que lorsque les disques sécurisés iStorage sont remis à d'autres parties, responsables, services, ou lorsqu'ils atteignent leur fin de vie d'exploitation, les disques doivent être soumis à des processus robustes afin de s'assurer que tout éventuel actif de données résiduel soit effacé et purgé du disque de manière sécurisée afin de réduire les chances de compromission de ces actifs de données.

Dans cette directive de sécurité iStorage n°2, nous fournissons les meilleurs conseils disponibles ainsi que des mesures d'atténuation pragmatiques et pratiques pour contrer cette menace.

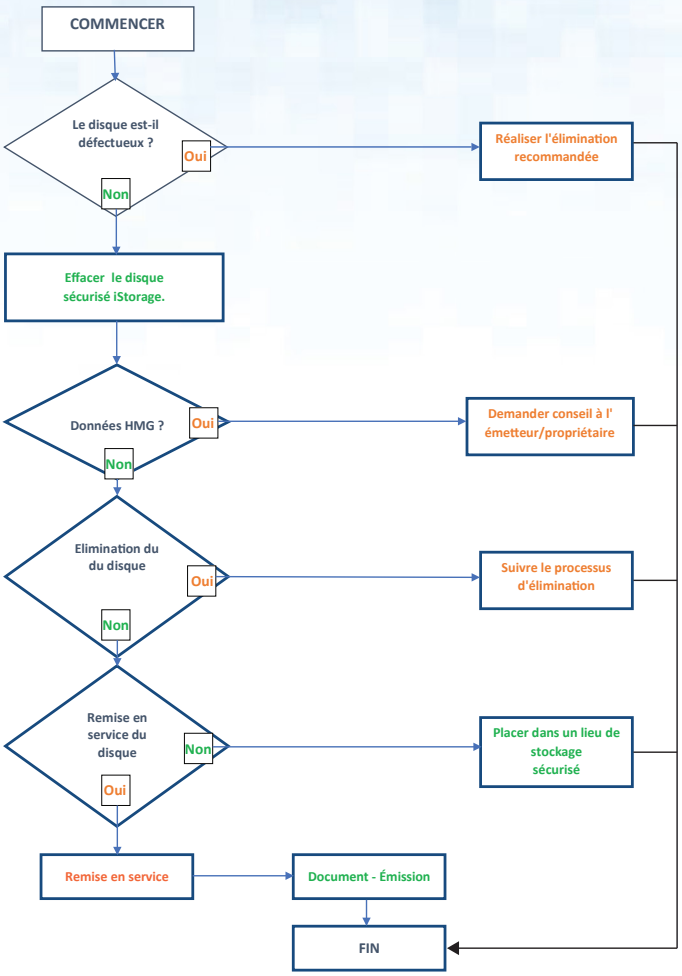
**Mesures d'atténuation :** les mesures d'atténuation mentionnées ci-dessous constituent les pratiques de sécurité optimales recommandées à mettre en œuvre lors de toute manipulation des disques sécurisés iStorage et sont présentées dans le **Tableau 1** ci-dessous. Cette approche a pour objectif de préserver le principe de sécurité **DIC+T** (**D**isponibilité, **I**ntégrité et **C**onfidentialité + **T**ransparence) et met en application les contrôles de sécurité pertinents exposés dans la norme ISO/IEC 27001 et le document NCSC (CESG).

Caractéristiques de sécurité CPA pour le chiffrement des supports matériels, version 1.2, en date d'avril 2012

**Processus :** La **fig. 1** ci-dessous est une représentation du flux de données de haut niveau qui se rapporte à :

- L'élimination sécurisée
- L'effacement sécurisé
- Actifs de données portant un marquage de protection et gouvernementaux classés secret
- Remise en service de disques sécurisés iStorage

## Fig. 1 – Processus d'effacement/élimination




## Tableau 1 - Mesures d'atténuation - Effacement et élimination sécurisés

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| 1<br>Confiidentialité<br>Transparence | DEP.M1 | Stockage | Vérifiez que tous les disques sécurisés iStorage en attente d'effacement ou d'élimination sécurisés sont tous recensés et comptabilisés ;<br><br>Qu'ils soient stockés dans un endroit sécurisé comportant des mécanismes et procédures de sécurité pour le contrôle physique et des accès.<br><br>**Remarque 1 :** Selon la quantité en attente de traitement, il pourrait s'agir d'une salle fermée ou d'une armoire de sécurité. |
| 2<br>Confiidentialité<br>Transparence | DEP.M311 | En transit | Durant le transport vers un centre d'élimination, ne jamais laissez un disque iStorage sans surveillance dans un véhicule ou dans une situation visible en transit ;<br><br>Si les disques sécurisés doivent être laissés sans surveillance, veillez à ce qu'ils ne soient pas visibles et fermez le véhicule entre le chargement et le déchargement du média ; |

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| | | | Tous les disques sécurisés iStorage destinés à être traités par un centre d'élimination sécurisée ne doivent être suivis et pris en charge que par un prestataire ou service de li-vraison de confiance.<br><br>Lorsque les disques sécurisés iStorage contiennent des actifs in-formationnels portant un marquage de protection et des documents gouvernementaux classés secrets, le service ou l'agence concernés doivent être consultés afin de confirmer l'obligation éventuelle de réaliser des con-trôles supplémentaires (par ex. communications en transit, contact avec les services d'urgence, ou véhicule en stand-by) |
| **3**<br>Confiidentialité<br>Transparence | | **Marquage de protection** | Lorsque les disques sécurisés iStorage contiennent des actifs informationnels portant un marquage de protection et des doc-uments gouvernementaux classés secret, le service ou l'agence propriétaires doivent être consultés afin de confirmer les exigences d'enregistrement et d'élimination sécurisés des disques sécurisés |
| **4**<br>Confiidentialité<br>Transparence | | **Transparence** | Tous les disques sécurisés iStorage en attente d'effacement ou d'élimination sécurisés sont tous recensés dans un registre qui consigne :<br><br>• Numéro de série<br>• Propriétaire/service<br>• Date de réception<br>• Classification ou marquage de protection de l'actif de données<br>• Toute mise en garde spécifique liée à la manipulation<br>• Date d'expédition pour traitement<br><br>**Remarque 2:** Si le disque iStorage a été effacé pour une remise en service, cela doit être consigné dans un registre indépendant en attendant la distribution à un nouveau propriétaire/responsable/service. |
| **5**<br>Disponibilité | | **Continuité des opérations** | Avant tout effacement ou élimination sécurisés d'un disque sécurisé iStorage, on doit obtenir la confirmation que tous les actifs de données qu'il contient sont recensés et sauvegardés de manière adéquate afin d'éviter l'élimination accidentelle d'actifs de données opérationnelles. |

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| 6<br>Confiidentialité<br>Transparence | DEP.M137 | Méthodes d'effacement | Les méthodes d'effacement qui sont employées pour traiter un disque sécurisé iStorage doivent être prises en charge par les procédures d'effacement et les procédures opérationnelles de sécurité (SyOps) documentées ;<br><br>Ces procédures doivent suivre des processus adaptés au type de média et à tout type de marquage de protection ou autre classification gouvernementale de l'actif de données à effacer, conformément (a minima) aux normes HMG.<br><br>Le prestataire de service sélectionné doit démontrer que ces procédures sont suivies en pratique.<br><br>Les conseils du NCSC (une divison du GCHQ) sont disponibles à l'adresse suivante : https://www.ncsc.gov.uk/index/topic/164 |
| 7<br>Intégrité | DEP.M137 | Effacement et élimination | Tout effacement/élimination de disques sécurisés iStorage doit être réalisé conformément aux procédures opérationnelles documentées du fabricant, aux guides d'utilisation et à toutes procédures de sécurité publiées ;<br>Le personnel ou les équipes qui réalisent les processus d'effacement ou d'élimination sécurisés doivent être formés à l'utilisation correcte de ces équipements.<br>Des processus doivent être en place pour vérifier que l'équipement est utilisé correctement et conformément aux recommandations des fabricants. |
| 8<br>Confiidentialité<br>Transparence | | Remise en service des supports | Lorsque le disque sécurisé iStorage a subi un effacement et doit être remis à un nouvel utilisateur, responsable ou service, des vérifications doivent être réalisées avant<br>sa remise en service afin de s'assurer que le support est totalement vierge ;<br><br>Un manuel d'utilisation de disque sécurisé iStorage contenant des instructions claires pour une utilisation en toute sécurité doit être remis au destinataire.<br><br>L'attribution du disque sécurisé iStorage doit être recensée et consignée dans un registre d'actifs. |
| 9<br>Confiidentialité<br>Transparence | DEP.M703 | Perte, vol, compromission | Veillez à disposer d'un processus prenant en charge le signalement à la direction de tout vol, perte ou compromission du disque sécurisé iStorage en attente de traitement ;<br><br>Si des actifs de données comportant un marquage de protection ou des données gouvernementales sont stockés sur le disque iStorage, demandez conseil à l'agence ou autorité concernée ; |

| Mesures d'atténuation | NCSC (CESG) CPA | Risque | Bonne pratique |
|---|---|---|---|
| | | | Confirmez que les données étaient chiffrées au moment du vol ou de la perte - afin d'établir que des actifs de données confidentielles ou autres formes d'information connexes ne seront pas compromises. |
| 10<br>Confiidentialité | MIT003 | Personnel / accès autorisé | Veillez à ce que les personnes qui obtiennent un accès aux actifs de données stockés sur un disque sécurisé iStorage disposent d'un besoin de savoir clair et des autorisations adéquates en fonction du niveau de l'actif de données, ou des documents gouvernementaux classés secrets et portant un marquage de protection qui y sont stockés. |

diskAshur PRO²®

iStorage®

Copyright © iStorage Limited 2017 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
Courriel : info@istorage-uk.com | Site Web : www.istorage-uk.com