iStorage®

DATASHUR® PRO²



English User Manual - Table of Contents 4

Deutsch Benutzerhandbuch - Inhaltsverzeichnis 45

Français Manuel d'utilisation - Table des matières 86

User Manual



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

If you are having difficulty using your datAshur PRO² please contact our support team by email - support@istorage-uk.com or by phone on +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2019. All rights reserved.

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

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

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

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

RoHS Compliant

REACH COMPLIANCE

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

Trade Agreements Act (TAA) Compliant

CITRIX® vmware®

Table of Contents

Introduction 5
Box contents 5
1. LED indicators and their actions 6
2. Battery and LED States 6
3. First Time Use 7
4. Unlocking datAshur PRO² with the Admin PIN 8
5. To Enter Admin Mode 9
6. To Exit Admin Mode 9
7. Changing the Admin PIN 10
8. Setting a User PIN Policy 11
9. How to delete the User PIN Policy 12
10. How to check the User PIN Policy 13
11. Adding a New User PIN in Admin Mode 14
12. Changing the User PIN in Admin Mode 15
13. Deleting the User PIN in Admin Mode 15
14. How to Unlock datAshur PRO² with User PIN 16
15. Changing the User PIN in User Mode 16
16. Creating a One-Time User Recovery PIN 17
17. Deleting the One-Time User Recovery PIN 17
18. Activating Recovery Mode and Creating New User PIN 18
19. Set User Read-Only in Admin Mode 19
20. Enable User Read/Write in Admin Mode 19
21. Set Global Read-Only in Admin Mode 20
22. Enable Global Read/Write in Admin Mode 20
23. How to configure a Self-Destruct PIN 21
24. How to delete the Self-Destruct PIN 22
25. How to Unlock with the Self-Destruct PIN 22
26. How to Configure an Admin PIN after a Brute Force attack or Reset 23
27. Setting the Unattended Auto-Lock Clock 23
28. Turn off the Unattended Auto-Lock Clock 24
29. How to check the Unattended Auto-Lock Clock 25
30. Set Read-Only in User Mode 25
31. Enable Read/Write in User Mode 26
32. Brute Force Hack Defence Mechanism 26
33. How to set the User PIN Brute Force Limitation 28
34. How to check the User PIN Brute Force Limitation 29
35. How to perform a complete reset 30
36. How to configure datAshur PRO² as Bootable 30
37. How to disable the datAshur PRO² Bootable feature 31
38. How to check the Bootable setting 31
39. Formatting the datAshur PRO² for Windows 32
40. datAshur PRO² Setup for Mac OS 34
41. datAshur PRO² Setup for Linux (Ubuntu 18.04 LTS) 36
42. Hibernating, Suspending or Logging off from the Operating System 39
43. How to check Firmware in Admin Mode 39
44. How to check Firmware in User Mode 40
45. Technical Support 41
46. Warranty and RMA information 41

Introduction



Note: The datAshur PRO² rechargeable battery is not fully charged, we recommend the battery be charged prior to first use. Please plug in the datAshur PRO² to a powered USB port for 30-60 minutes to fully charge the battery.

Thank you for purchasing the iStorage datAshur® PRO², an ultra-secure and easy to use, hardware encrypted USB 3.2 Gen 1 PIN authenticated flash drive with capacities up to 512GB and rising.

The datAshur PRO² incorporates a rechargeable battery allowing the user to enter a 7-15 digit PIN (Personal Identification Number) onto the on-board keypad to unlock the drive before connecting to a USB port. To lock the drive and encrypt all data, simply eject the datAshur PRO² from the host computer and the entire contents of the drive will be encrypted (full disk encryption) using military grade AES-XTS 256-bit hardware encryption. If the drive is lost or stolen and an incorrect PIN is entered 10 consecutive times (default setting), the datAshur PRO² defence mechanism will be triggered to protect against unathorised access.

The datAshur PRO² can be configured with both User and Admin PINs and can also be programmed to include a 'User Recovery PIN' making it perfect for corporate and government deployment. As the datAshur PRO² is unlocked via the on-board keypad and not a host computer, it is not vulnerable to software/hardware based key-loggers or brute force attacks.

One of the unique and underlying security features of the GDPR compliant datAshur 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 datAshur 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

- iStorage datAshur PRO²
- Extruded Aluminium Sleeve
- QSG - Quick Start Guide

1. LED indicators and their actions

LED	LED State	Description	LED	LED State	Description
▲	RED Solid	Locked device (in either **Standby** or **Reset** states)	▲▼▲	RED, GREEN and BLUE Blinking	Waiting for **User** PIN entry
▲	RED - Fade Out	Device Turning off to the **Idle State**	▼▲	GREEN and BLUE Blinking together	Waiting for **Admin** PIN entry
▼	GREEN Blinking	**Unlocked** device as **Admin** (not connected to USB port)	▼▲	GREEN and BLUE Blinking alternately	Authentication in progress
▼	GREEN Solid	**Unlocked** device as **User** (not connected to USB port) or device in User mode	▲	BLUE blinking every 5 seconds	Battery starts charging after 30 seconds when device is locked and connected to a USB port
▲	BLUE Solid	Device in **Admin mode**			

2. Battery and LED States

Note: The normal function of the datAshur PRO² may be disturbed by strong Electro-Magnetic Interference. If so, simply power cycle the product (power off then power on) to resume normal operation. If normal operation does not resume, please use the product in a different location.

Low Battery Sensor

The datAshur PRO² incorporates voltage detection circuitry that monitors the battery output when the device is powered on. When battery output drops to 3.3V or below, the RED LED flashes three times and fades out. At this point, the User should connect the datAshur PRO² to a powered USB port and charge for 15-30minutes. Once recharged, the datAshur PRO² will resume normal function.

To wake from Idle State

Idle state is defined as when datAshur PRO² is not being used and all LEDs are off.

To wake datAshur PRO² from the idle state do the following.

Press and hold down the **SHIFT** (⬆) button for one second or connect the device to a powered USB port	▲ ▼ ▲ ▲	RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the device is in Standby State

To enter Idle State

To force datAshur PRO² to enter Idle State, execute either of the following operations:

- If the device is connected to a USB port, disconnect it.
- If the device is not connected to a USB port, press and hold down the **SHIFT** (⬆) button for a second until the LED turns solid RED and fades out to the Idle State (off).

Note: When datAshur PRO² is unlocked and not connected to a USB port and no operations are performed within 30 seconds, the device will enter Idle State automatically. The LED turns to solid RED and then fades out to the idle state.

When datAshur PRO² is connected to a USB port, the **SHIFT** (⬆) button does not function.

When connected to a powered USB port, a locked datAshur PRO² will start charging after 30 seconds, indicated by the BLUE LED blinking every 5 seconds.

Power-on States

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

Power-on State	LED indication	Encryption Key	Admin PIN	Description
Standby	RED Solid	✓	✓	Waiting for Admin or User PIN entry
Reset	RED Solid	×	×	Waiting for configuration of an Admin PIN
Low Battery Level	RED Blinks 3 Times	✓	✓	Charge on a powered USB port for 15-30 minutes
Initial Shipment State	RED and GREEN Solid	✓	×	Waiting for configuration of an Admin PIN

3. First Time Use

datAshur PRO² is supplied in the **'Initial Shipment State' with no pre-set Admin PIN**. A **7-15** digit Admin PIN must be configured before the drive can be used. Once an Admin PIN has been successfully configured, it is then not possible to switch the drive back to the 'Initial Shipment State'.

PIN Requirements:

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

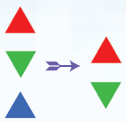
Password Tip: You can configure a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the button with the corresponding letters on it.

Examples of these types of Alphanumerical PINs are:

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

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

To configure an Admin PIN and unlock the datAshur PRO² for the first time, please follow the simple steps in the table below.

Instructions - First Time Use	LED	LED State
1. Press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to solid RED and GREEN LEDs indicating the drive is in the Initial Shipment State
2. Press and hold down both **KEY (🔑) + 1** buttons		LEDs turn to blinking GREEN and solid BLUE
3. Enter **New Admin PIN** and press the **KEY (🔑)** button once		Blinking GREEN and solid BLUE LEDs switch to a GREEN blink then back to Blinking GREEN and solid BLUE LEDs
4. Re-enter **New Admin PIN** and press the **KEY (🔑)** button again		BLUE LED rapidly blinks then switches to a solid BLUE LED and finally to a blinking GREEN LED indicating the Admin PIN has been successfully configured and drive unlocked

Note: Once datAshur PRO² has been successfully unlocked, the GREEN LED will remain blinking for 30 seconds only, during which time the datAshur PRO² needs to be connected to a powered USB port. It can be locked down immediately (if not connected to a USB port) by pressing and holding down the **SHIFT** (⬆) button for a second or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system when connected to a USB port.

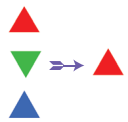
When the datAshur PRO² is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

Locking datAshur PRO²

To lock the drive, safely eject the datAshur PRO² from your host operating system and unplug from the USB port. If data is being written to the drive, unplugging the datAshur PRO² will result in incomplete data transfer and possible data corruption.

4. Unlocking datAshur PRO² with the Admin PIN

To unlock the datAshur PRO² with the Admin PIN, please follow the simple steps in the table below.

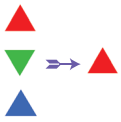
1. Press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the drive is in Standby State
2. In Standby State (solid RED LED) press the **KEY (🔑)** button once		GREEN and BLUE LEDs blink together
3. With the GREEN and BLUE LEDs blinking together, enter the **Admin PIN** and press the **KEY (🔑)** button again		GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED and changing to a blinking GREEN LED indicating the drive has been successfully unlocked as Admin

Note: Once datAshur PRO² has been successfully unlocked, the GREEN LED will remain blinking for 30 seconds only, during which time the datAshur PRO² needs to be connected to a powered USB port. It can be locked down immediately (if not connected to a USB port) by pressing and holding down the **SHIFT** (⬆) button for a second or by clicking the 'Safely Remove Hardware/Eject' icon within your operating system when connected to a USB port.

When the datAshur PRO² is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

5. To Enter Admin Mode

To Enter Admin Mode, do the following.

1. Press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the device is in Standby State
2. In Standby State (solid RED LED) press the **KEY (⚷)** button once		GREEN and BLUE LEDs blink together
3. With the GREEN and BLUE LEDs blinking together, enter the **Admin PIN** and press the **KEY (⚷)** button again		GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED changing to a blinking GREEN LED indicating the device is unlocked
4. Press the **KEY (⚷)** button **Three** times within 2 seconds (**KEY (⚷)** x **3**)		Blinking GREEN LED will change to a solid BLUE LED indicating the device is in Admin mode

6. To Exit Admin Mode

When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

7. Changing the Admin PIN

PIN Requirements:

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

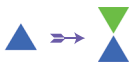
Password Tip: You can configure a memorable word, name, phrase or any other Alphanumerical PIN combination by simply pressing the button with the corresponding letters on it.

Examples of these types of Alphanumerical PINs are:

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

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

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

8. Setting a User PIN Policy

The Administrator can set a restriction policy for the User PIN. This policy includes setting the minimum length of the PIN (from 7 to 15 digits), as well as requiring or not the input of one or more '**Special Characters**'. The "Special Character" functions as both the '**SHIFT** (⬆) + **digit**' buttons pressed down together.

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

Once the Administrator has set the User PIN Policy, for instance '091', a new User PIN will need to be configured - see section 11, 'Adding a New User PIN in Admin Mode'. If the Administrator configures the User PIN as '**247688314**' with the use of a '**Special Character**' (**SHIFT** (⬆) **+ digit** pressed down together), this can be placed anywhere along your 7-15 digit PIN during the process of creating the User PIN as shown in the examples below.

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

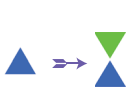
B. '2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4',

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

Note:

- If a 'Special Character' was used during the configuration of the User PIN, for instance, example '**B**' above, then the drive can only be unlocked by entering the PIN with the 'Special Character' entered precisely in the order configured, as per example '**B**' above - ('2', '4', '**SHIFT** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4').
- More than one 'Special Character' can be used and placed along your 7-15 digit PIN.
- Users are able to change their PIN but are forced to comply with the set 'User PIN Policy' (restrictions), if and when applicable.
- Setting a new User PIN Policy will automatically delete the User PIN if one exists.
- This policy does not apply to the 'Self-Destruct PIN'. The complexity setting for the Self-Destruct PIN and Admin PIN is always 7-15 digits, with no special character required.

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

9. How to delete the User PIN Policy

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

1. In Admin mode, press and hold down both **KEY (🔑) + 7** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **070** and press **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will change to a solid GREEN LED and finally to a solid BLUE LED indicating the User PIN Policy has been successfully deleted

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

10. How to check the User PIN Policy

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

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

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

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

11. Adding a New User PIN in Admin Mode

Important: The creation of a new User PIN must comply with the 'User PIN Policy' if one has been configured as described in section 8, which imposes a minimum PIN length and whether a 'Special Character' has been used. Refer to section 10 to check the user PIN restrictions.

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- Must not contain only consecutive numbers, e.g. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- The **SHIFT** (⬆) button can be used for additional PIN combinations - e.g. **SHIFT** (⬆) **+ 1** is a different value than just 1. See section 8, 'Setting a User PIN Policy'.

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

12. Changing the User PIN in Admin Mode

Important: Changing the User PIN must comply with the 'User PIN Policy' if one has been configured as described in section 8, which imposes a minimum PIN length and whether a 'Special Character' has been used. Refer to section 10 to check the user PIN restrictions.

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

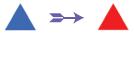
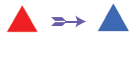
1. In Admin mode press and hold down both **KEY (🔑) + 3** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New User PIN** and press **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

13. Deleting the User PIN in Admin Mode

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

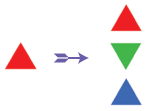
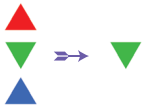
1. In Admin mode press and hold down both **SHIFT** (⬆) **+ 3** buttons		Solid BLUE LED will change to a blinking RED LED
2. Press and hold down both **SHIFT** (⬆) **+ 3** buttons again		Blinking RED LED will change to a solid RED LED and then to a solid BLUE LED indicating the User PIN has been successfully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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

14. How to Unlock datAshur PRO² with User PIN

To unlock with the **User PIN,** the datAshur PRO² must first be in Standby State (solid RED LED) by pressing and holding down the **SHIFT** (⬆) button for one second.

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

15. Changing the User PIN in User Mode

To change the **User PIN**, first unlock the datAshur PRO² with a User PIN as described above in section 14. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

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

Important: Changing the User PIN must comply with the 'User PIN Policy' if one has been configured as described in section 8, which imposes a minimum PIN length and whether a 'Special Character' has been used. The administrator can refer to section 10 to check the user PIN restrictions.

16. Creating a One-Time User Recovery PIN

The User Recovery PIN is extremely useful in situations where a user has forgotten their PIN to unlock the datAshur PRO². To activate the recovery mode, the user must first enter the correct One-Time Recovery PIN, if one has been configured. The user PIN recovery process does not impact the data, encryption key and Admin PIN, however the user is forced to configure a new 7-15 digit User PIN.

To configure a One-Time 7-15 digit User Recovery PIN, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

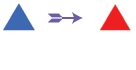
1. In Admin mode press and hold down both **KEY (🔑) + 4** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **a One-Time Recovery PIN** and press **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

17. Deleting the One-Time User Recovery PIN

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

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

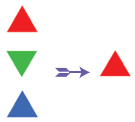
Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

18. Activating Recovery Mode and Creating New User PIN

The User Recovery PIN is extremely useful in situations where a user has forgotten their PIN to unlock the datAshur PRO².
To activate the recovery mode, the user must first enter the correct One-Time Recovery PIN, if one has been configured. The user PIN recovery process does not impact the data, encryption key and Admin PIN, however the user is forced to configure a new 7-15 digit User PIN.

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

1. With the drive in **Idle State** press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the drive is in Standby State
2. In **Standby State** press and hold down both **KEY (🔑) + 4** buttons		Solid RED LED will change to blinking RED and GREEN LEDs
3. Enter the One-Time **Recovery PIN** and press the **KEY (🔑)** button		GREEN and BLUE LEDs alternate on and off then to a solid GREEN LED and finally to blinking GREEN and solid BLUE LEDs
4. Enter the **New User PIN** and press the **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs change to a single GREEN LED blink then back to blinking GREEN and solid BLUE LEDs
5. Re-enter the **New User PIN** and press the **KEY (🔑)** button again		GREEN LED blinks rapidly then becomes solid GREEN indicating the recovery process has been successful and a new user PIN configured

Important: The creation of a new User PIN must comply with the 'User PIN Policy' if one has been configured as described in section 8, which imposes a minimum PIN length and whether a special character has been used. Refer to section 10 to check the user PIN restrictions.

19. Set User Read-Only in Admin Mode

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

When the Administrator configures the datAshur PRO² and restricts User access to Read-Only, then only the Administrator can write to the drive or change the setting back to Read/Write as described in section 20. The User is restricted to Read-Only access and cannot write to the drive or change this setting in user mode.

To set the datAshur PRO² and restrict User access to Read-Only, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

20. Enable User Read/Write in Admin Mode

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

21. Set Global Read-Only in Admin Mode

When the Administrator configures the datAshur PRO² and restricts it to Global Read-Only, then neither the Administrator nor the User can write to the drive and both are restricted to Read-Only access. Only the Administrator is able to change the setting back to Read/Write as described in section 22.

To set the datAshur PRO² and restrict Global access to Read-Only, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

22. Enable Global Read/Write in Admin Mode

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

23. How to configure a Self-Destruct PIN

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

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

1. In Admin mode, press and hold down both **KEY (🔑) + 6** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Configure a 7-15 digit **Self-Destruct PIN** and press the **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter the **Self-Destruct PIN** and press the **KEY (🔑)** button		GREEN LED will rapidly blink for several seconds and then changes to a solid BLUE LED to indicate the Self-Destruct PIN has been success-fully configured

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

24. How to Delete the Self-Destruct PIN

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

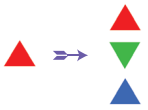
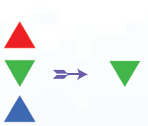
To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

25. How to Unlock with the Self-Destruct PIN

Warning: When the Self-Destruct mechanism is activated, all data, the encryption key and the Admin/User PINs are deleted. **The Self-Destruct PIN becomes the User PIN.** No Admin PIN exists after the Self-Destruct mechanism is activated. The datAshur PRO² will need to be reset (see 'How to perform a complete reset' Section 35, on page 28) first in order to configure an Admin PIN with full Admin privileges including the ability to configure a User PIN.

When used, the self-destruct PIN will **delete ALL data, Admin/User PINs** and then unlock the drive. Activating this feature will cause the **Self-Destruct PIN to become the New User PIN** and the datAshur PRO² will need to be formatted before any new data can be added to the drive.

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

1. In standby state (solid RED LED), press and hold down both the **SHIFT** (⬆) + **KEY (🔑)** buttons		RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter the **Self-Destruct PIN** and press the **KEY (🔑)** button		RED, GREEN and BLUE blinking LEDs will change to GREEN and BLUE LEDs alternating on and off for a few seconds and finally shifts to a solid GREEN LED indicating the datAshur PRO² has successfully self-destructed

26. How to Configure an Admin PIN after a Brute Force attack or Reset

It will be necessary after a Brute Force attack or when the datAshur PRO² has been reset to configure an Admin PIN before the drive can be used.

PIN Requirements:

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

If the datAshur PRO² has been brute forced or reset, the drive will be in standby state (solid RED LED). to configure an Admin PIN proceed with the following steps.

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

27. Setting the Unattended Auto-Lock Clock

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

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

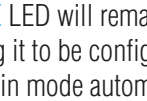
1. In Admin mode, press and hold down both **KEY (🔑) + 5** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter the amount of time that you would like to set the Auto-Lock time-out feature for, the minimum time that can be set is 5 minutes and the maximum being 99 minutes (5-99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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

28. 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 both **KEY (🔑) + 5** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **00** and press the **SHIFT** (⬆) button		Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto-Lock time out has been successfully disabled

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

29. 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 **KEY** (🔑) button and the following happens; a. All LED's (RED, GREEN & BLUE) become solid for 1 second. b. Each RED LED blink equates to ten (10) minutes. c. Every GREEN LED blink equates to one (1) minute. d. All LED's (RED, GREEN & BLUE) become solid for 1 second. e. LEDs return to solid BLUE		

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

30. Set Read-Only in User Mode

To set the datAshur PRO² to Read-Only, first enter the "**User Mode**" as described in section 14. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

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

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

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

31. Enable Read/Write in User Mode

To set the datAshur PRO² to Read/Write, first enter the "**User Mode**" as described in section 14. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

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

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

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

32. Brute Force Hack Defence Mechanism

The datAshur PRO² incorporates a defence mechanism to protect the drive against a Brute Force attack. By default, the brute force limitation for Admin PIN and User PIN is set to 10, for the Recovery PIN is 5. Three independent brute force counters are used to record the incorrect attempts for each PIN authorisation. If user enters an incorrect Admin PIN ten consecutive times, (broken down into 5,3,2, clusters as described below) the drive will be reset and all data will be lost forever. If user enters incorrect Recovery PIN or User PIN and exceed the respective brute force limitation, the corresponding PINs will be cleared but the data will still exist on the drive.

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

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

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

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

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

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

Important: A new Admin PIN must be configured if the pre-existing Admin PIN was brute forced, refer to Section 26 on page 23 on 'How to Configure an Admin PIN after a Brute Force attack or Reset', the datAshur PRO² will also need to be formatted before any new data can be added to the drive.

33. How to set the User PIN Brute Force Limitation

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

The brute force limitation for datAshur PRO² User PIN can be reprogrammed and set by the administrator. This feature can be set to allow attempts from 1 to 10 consecutive incorrect PIN entries.

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

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

34. How to check the User PIN Brute Force Limitation

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

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

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

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

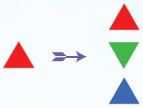
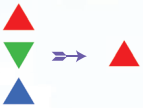
Brute Force Limitation Setting	RED	GREEN
2 attempts	0	2 Blinks
5 attempts	0	5 Blinks
10 attempts	1 Blink	0

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

35. How to perform a complete reset

To perform a complete reset, the datAshur PRO² must be in standby state (solid RED LED). Once the drive is reset then all Admin/User PINs, the encryption key and all data will be deleted and lost forever and the drive will need to be formatted before it can be reused. To reset the datAshur PRO² proceed with the following steps.

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

Important: After a complete reset a new Admin PIN must be configured, refer to Section 26 on page 22 on 'How to Configure an Admin PIN after a Brute Force attack or Reset', the datAshur PRO² will also need to be formatted before any new data can be added to the drive.

36. How to configure datAshur PRO² as Bootable

Note: When the drive is set as bootable, ejecting the drive from Operating System will not force the LED to turn RED. The drive stays solid GREEN and needs to be unplugged for next time use. The default setting of the datAshur PRO² is configured as non-bootable.

iStorage datAshur PRO² USB drives are equipped with a bootable feature to accommodate power cycling during a host boot process. When booting from the datAshur PRO², you are running your computer with the operating system that is installed on the datAshur PRO².

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

1. In Admin mode, press and hold down both **KEY (🔑) + 8** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **"0"** followed by a **"1"** (**01**)		GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will change to a solid GREEN LED and finally to a solid BLUE LED indicating the drive has been successfully configured as bootable

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

37. How to disable the datAshur PRO² Bootable feature

To disable the datAshur PRO² Bootable Feature, first enter the "**Admin Mode**" as described in section 5. Once the drive is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **KEY (🔑) + 8** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press **"0"** followed by another **"0"** (**00**)		GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will change to a solid GREEN LED and finally to a solid BLUE LED indicating the bootable feature has been successfully disabled

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

38. How to check the Bootable setting

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

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

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

- **If datAshur PRO² is configured as Bootable, the following happens;**

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

- **If datAshur PRO² is <u>NOT</u> configured as Bootable, the following happens;**

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

Note: When the datAshur PRO² is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur PRO² will exit Admin mode automatically - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state (all LEDs off).

To immediately exit Admin Mode (solid BLUE LED), press and hold down the **SHIFT** (⬆) button for a second - the solid BLUE LED switches to a solid RED LED which then fades out to the Idle state. To access the drive contents (data), the datAshur PRO² must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

39. Formatting the datAshur PRO² for Windows

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

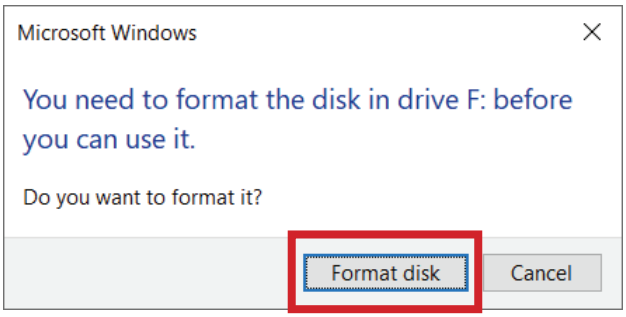
To format your datAshur PRO², do the following:

1. Configure a new Admin PIN - see page 22, section 26, 'How to configure an Admin PIN after a Brute Force attack or reset'.

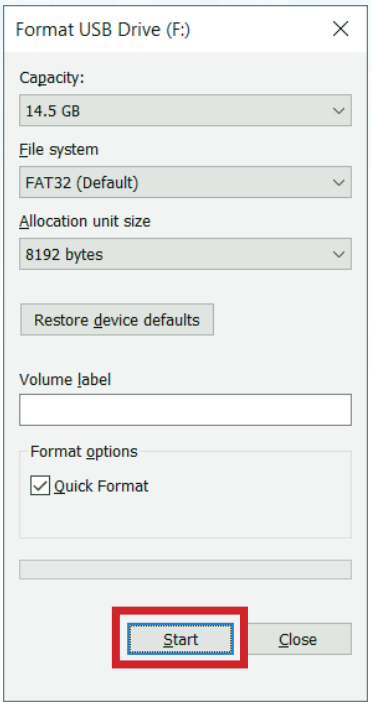
2. With the datAshur PRO² in standby state (RED LED), press the **KEY (🔑)** button once and enter **New Admin PIN** to unlock (blinking GREEN LED).

3. Attach the datAshur PRO² to the computer.

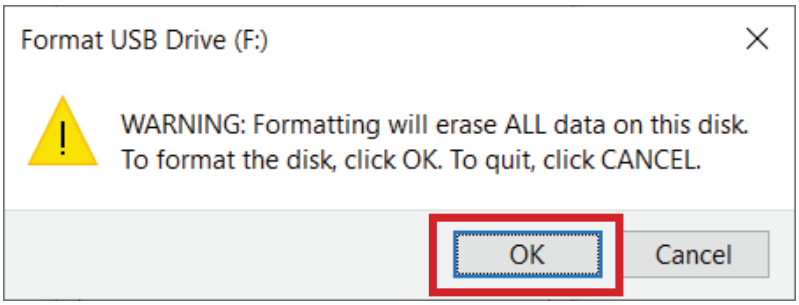
4. Click on 'Format Disk'



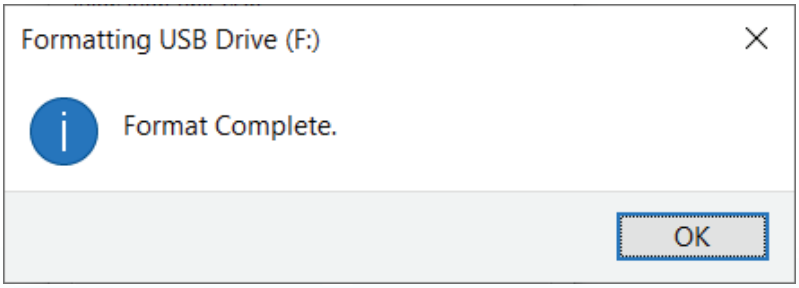
5. Click 'Start'.



6. Click 'OK'.



7. Wait until the formatting process is complete. The datAshur PRO² will be recognised and it is available for use.



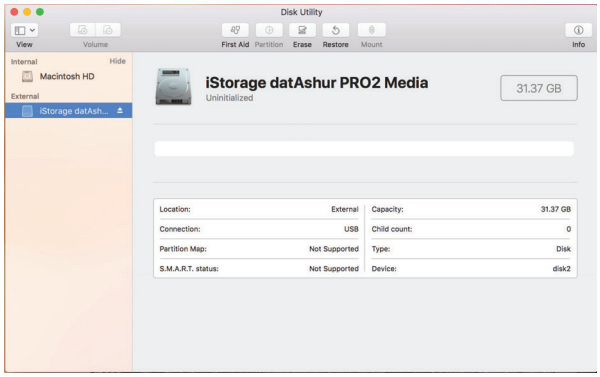
40. datAshur PRO² Setup for Mac OS

Your datAshur 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 datAshur PRO²:

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



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

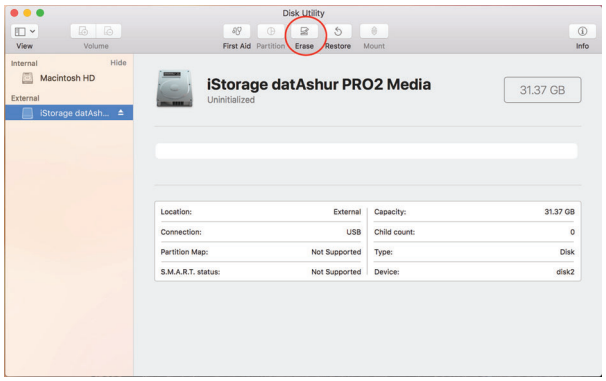


figure 1

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.

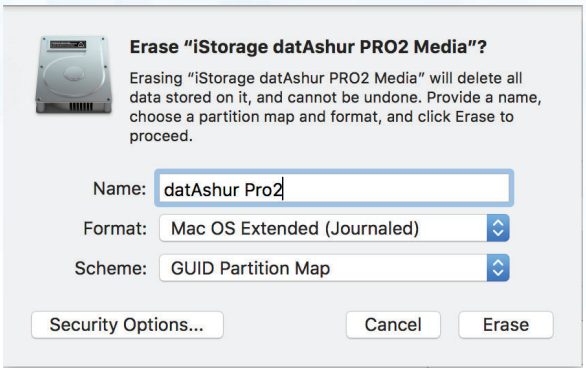


figure 2

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).

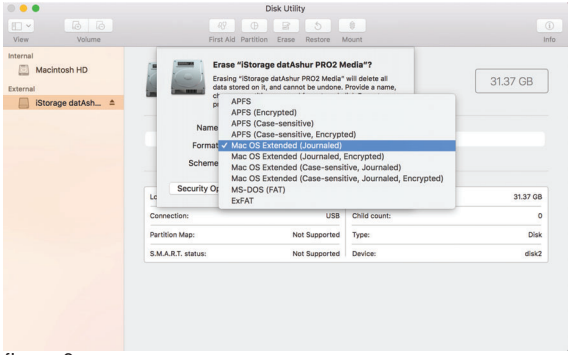


figure 3

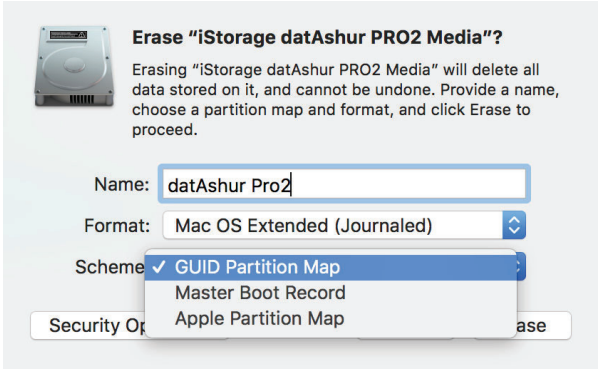


figure 4

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

41. datAshur PRO² Setup for Linux (Ubuntu 18.04 LTS)

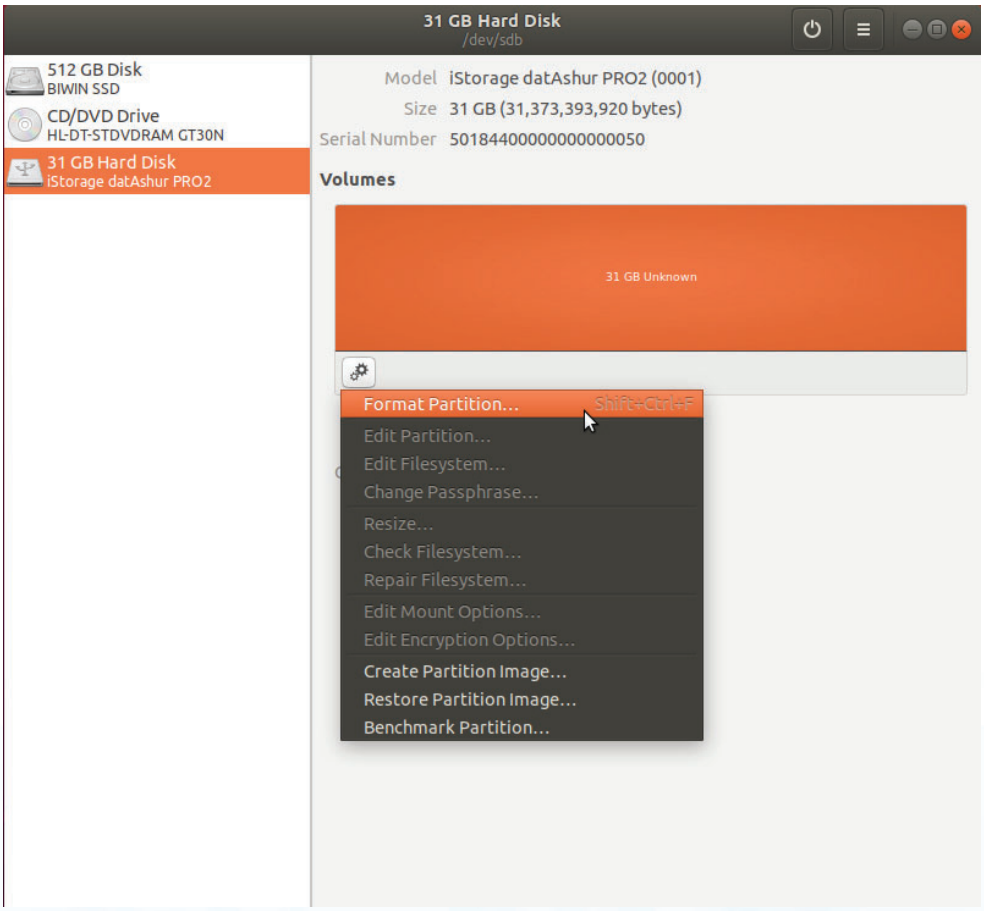
If your datAshur PRO² has been initialised and formatted in NTFS/FAT32/exFAT for Windows, you can directly use the drive on Ubuntu. If not, please read below.

To format the datAshur PRO² as EXT4 or other filesystem:

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

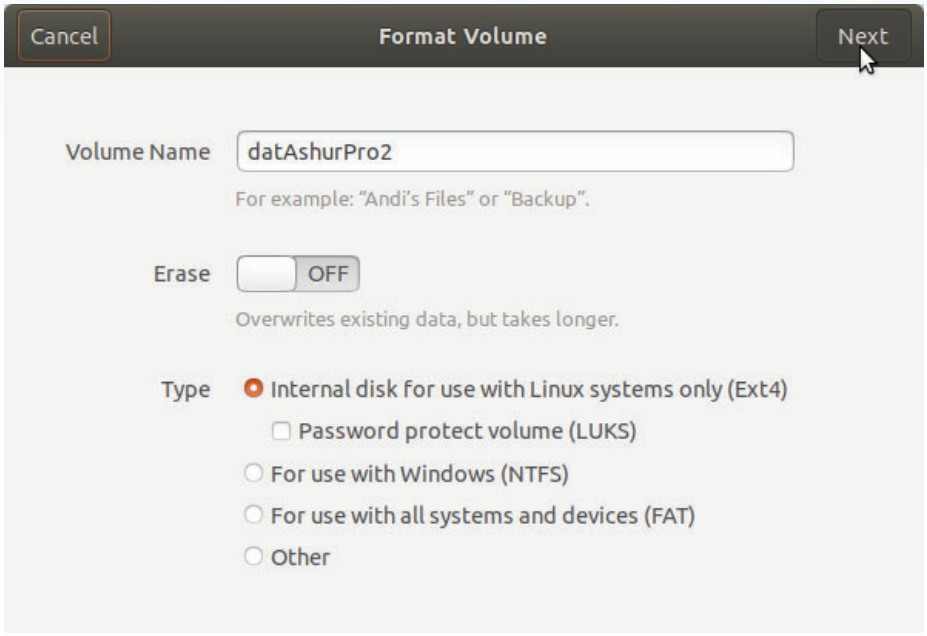


2. Select the datAshur PRO² under 'Devices'. Click on the gears icon and choose 'Format Partition'

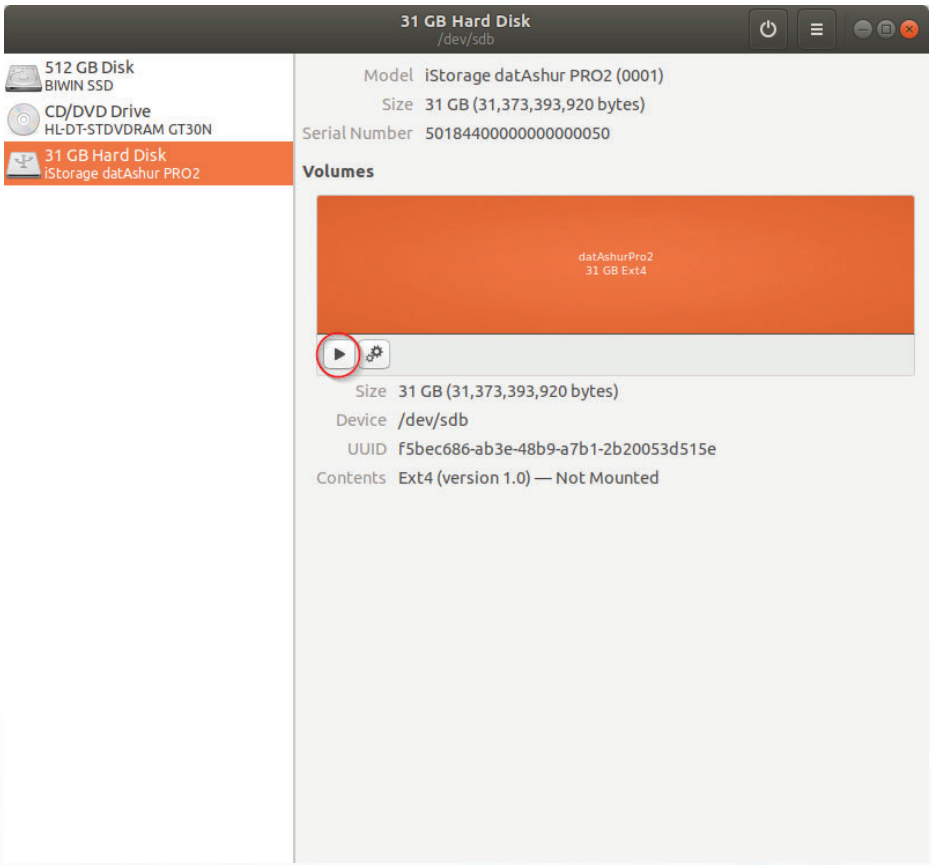


3. Configure a Volume Name and then select type of formatting you wish to use.
   EXT4 – compatible with Linux
   NTFS – Windows Only
   FAT – compatible with all Operating Systems

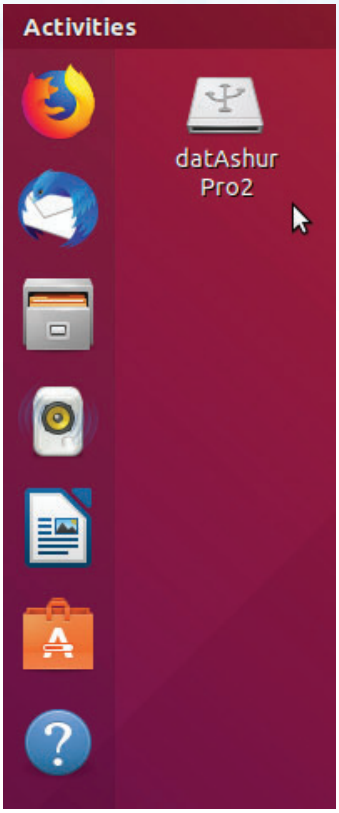
   And then press 'Next' and then 'FORMAT'



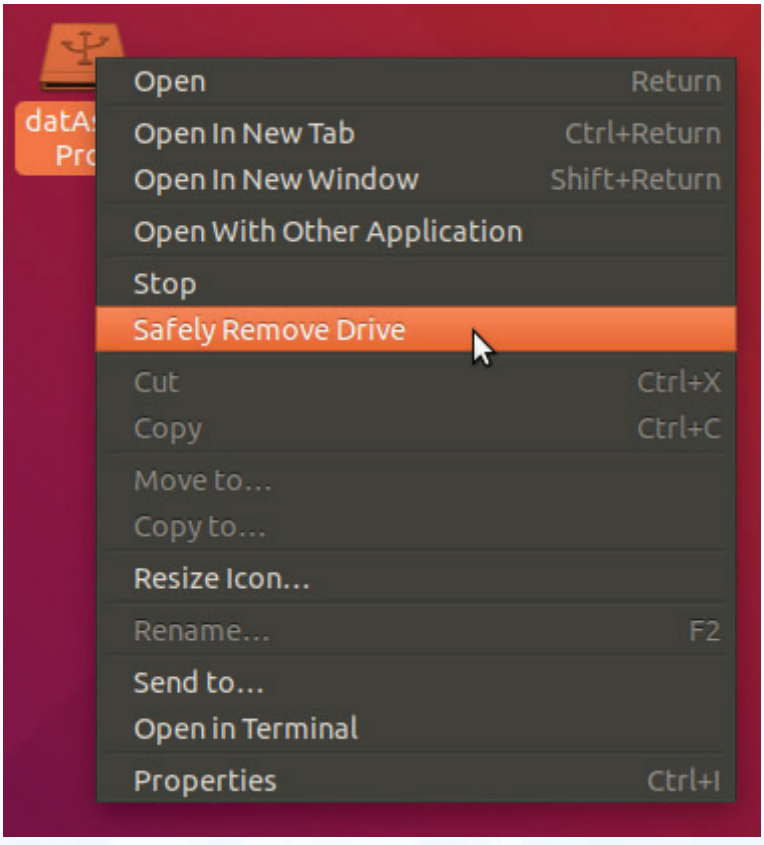
4. After the format process is finished, click  to mount the drive to Ubuntu.



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



Lock datAshur PRO² for Linux (Ubuntu 18.04 LTS)
It is strongly recommended to right click your drive icon and then click 'Safely Remove' in the OS to eject (lock) your datAshur PRO², especially after data has been copied or deleted from the drive.



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

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

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

To lock, simply click the 'Safely Remove Hardware/Eject' icon within your operating system and unplug the datAshur PRO².

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

43. How to check Firmware in Admin mode

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

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

For example, if the firmware revision number is '**2.5**', the RED LED will blink twice (**2**) and the GREEN LED will blink five (**5**) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to Admin mode, a solid BLUE LED.

44. How to check Firmware in User Mode

To check the firmware revision number, first enter the "**User Mode**" as described in section 14. Once the drive is in **User Mode** (solid GREEN LED) proceed with the following steps.

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

For example, if the firmware revision number is '**2.5**', the RED LED will blink twice (**2**) and the GREEN LED will blink five (**5**) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to Admin mode, a solid BLUE LED.

45. Technical Support

iStorage provides the following helpful resources for you:

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

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

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

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

46. Warranty and RMA information

ISTORAGE PRODUCT DISCLAIMER AND WARRANTY

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

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

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

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

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

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

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

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

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

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

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

iStorage datAshur PRO²® Manual / Handbuch / Manuel v3.3

iStorage®

Copyright © iStorage Limited 2019. 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



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 Ihrem datAshur PRO² haben, wenden Sie sich per E-Mail oder telefonisch an unser Support-Team: support@istorage-uk.com oder +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2019. Alle Rechte vorbehalten.
Windows ist eine eingetragene Marke der Microsoft Corporation.
Alle anderen genannten Marken und Urheberrechte sind Eigentum ihrer jeweiligen Inhaber.
Die Verteilung geänderter Versionen dieses Dokuments ohne die ausdrückliche Genehmigung des Urheberrechtsinhabers ist verboten.
Die Verteilung des Dokuments oder abgeleiteter Versionen in standardmäßiger Papierform zu kommerziellen Zwecken ist nur mit vorheriger Zustimmung des Urheberrechtsinhabers zulässig.
DIE DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN BEDINGUNGEN, ZUSICHERUNGEN UND GARANTIEN, EINSCHLIESSLICH STILLSCHWEIGENDER GARANTIE DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHTVERLETZUNG, SIND, SOFERN DIESER HAFTUNGSAUSSCHLUSS NICHT FÜR RECHTLICH UNGÜLTIG BEFUNDENWIRD, AUSGESCHLOSSEN.

RoHS Compliant

REACH COMPLIANCE

Alle Marken und Markennamen sind Eigentum ihrer jeweiligen Inhaber.

Konform mit Trade Agreements Act (TAA)

CITRIX® vmware®

Inhaltsverzeichnis

Einführung 46
Verpackungsinhalt 46
1. LED-Anzeigen und ihre Funktionen 47
2. Batterie- und LED-Status 47
3. Erstmalige Verwendung 48
4. Entsperren des datAshur PRO² mit der Admin-PIN 49
5. In den Admin-Modus gehen 50
6. Admin-Modus beenden 50
7. Ändern der Admin-PIN 51
8. Einstellen einer Benutzer-PIN-Richtlinie 52
9. So löschen Sie die Benutzer-PIN-Richtlinie 53
10. So prüfen Sie die Benutzer-PIN-Richtlinie 54
11. Hinzufügen einer neuen Benutzer-PIN im Admin-Modus 55
12. Ändern der Benutzer-PIN im Admin-Modus 56
13. Löschen der Benutzer-PIN im Admin-Modus 56
14. So entsperren Sie datAshur PRO² mit Benutzer-PIN 57
15. Ändern der Benutzer-PIN im Benutzermodus 57
16. Erstellen einer einmaligen Benutzerwiederherstellungs-PIN 58
17. Löschen der einmaligen Benutzerwiederherstellungs-PIN 58
18. Aktivieren des Wiederherstellungsmodus und Erstellen einer neuen Benutzer-PIN 59
19. Einstellen des schreibgeschützten Benutzerzugriffs im Admin-Modus 60
20. Aktivieren des Lese-/Schreibzugriffs für Benutzer im Admin-Modus 60
21. Einstellen des globalen Lese-/Schreibzugriffs im Admin-Modus 61
22. Aktivieren des globalen Lese-/Schreibzugriffs im Admin-Modus 61
23. So konfigurieren Sie eine Selbstzerstörungs-PIN 62
24. So löschen Sie die Selbstzerstörungs-PIN 63
25. So entsperren Sie mit der Selbstzerstörungs-PIN 63
26. So konfigurieren Sie eine Admin-PIN nach einem Brute-Force-Angriff oder dem Zurücksetzen 64
27. Einstellen der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“ 64
28. Deaktivieren der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“ 65
29. So prüfen Sie die Uhr für „Automatische Sperre, wenn unbeaufsichtigt“ 66
30. Einstellen des schreibgeschützten Zugriffs im Benutzermodus 66
31. Aktivieren des Lese-/Schreibzugriffs im Benutzermodus 67
32. Abwehrmechanismus gegen Brute-Force-Hacker-Angriffe 67
33. So stellen Sie die Brute-Force-Beschränkung für die Benutzer-PIN ein 69
34. So prüfen Sie die Brute-Force-Beschränkung für die Benutzer-PIN 70
35. So führen Sie ein komplettes Zurücksetzen durch 71
36. So konfigurieren Sie datAshur PRO² als bootfähig 71
37. So deaktivieren Sie die Funktion Bootfähig von datAshur PRO² 72
38. So prüfen Sie die Bootfähig-Einstellung 72
39. Formatieren von datAshur PRO² für Windows 73
40. datAshur PRO² Setup für Mac OS 75
41. datAshur PRO² Setup für Linux (Ubuntu 18.04 LTS) 77
42. Ruhezustand, Anhalten oder Abmelden vom Betriebssystem 80
43. So prüfen Sie Firmware im Admin-Modus 80
44. So prüfen Sie Firmware im Benutzermodus 81
45. Technischer Support 82
46. Garantie- und RMA-Informationen 82

Einführung



Hinweis: Der wiederaufladbare Akku des datAshur PRO² ist nicht vollständig geladen. Wir empfehlen, den Akku vor der ersten Verwendung aufzuladen. Schließen Sie das datAshur PRO² bitte 30 - 60 Minuten lang an einen eingeschalteten USB-Anschluss an, um den Akku vollständig aufzuladen.

Vielen Dank für den Kauf des iStorage datAshur® PRO², eines ultra-sicheren und einfach zu verwendenden USB-Speichersticks 3.2 Gen 1 mit Hardwareverschlüsselung und PIN-Authentifizierung und einer Kapazität von 512 GB, Tendenz steigend.

Das datAshur PRO² verfügt über einen wiederaufladbaren Akku, der dem Benutzer ermöglicht, über die integrierte Tastatur eine 7- bis 15-stellige PIN (Personal Identification Number, persönliche Identifikationsnummer) einzugeben, um den Datenträger vor dem Anschließen an einen USB-Anschluss zu entsperren. Um den Datenträger zu sperren und alle Daten zu verschlüsseln, entfernen Sie das datAshur PRO² einfach vom Hostcomputer. Die gesamten Inhalte auf dem Datenträger werden mit AES-XTS 256-bit Hardwareverschlüsselung im Militärstandard verschlüsselt (vollständige Festplattenverschüsselung). Wenn der Datenträger verloren geht oder gestohlen wird und zehnmal hintereinander (Standardeinstellung) eine falsche PIN eingegeben wird, wird der Abwehrmechanismus des datAshur PRO² ausgelöst, um vor unbefugtem Zugriff zu schützen.

Das datAshur PRO² kann mit sowohl Benutzer- als auch Admin-PIN konfiguriert und für eine „Benutzer-Wiederherstellungs-PIN“ programmiert werden, was für den Einsatz in Unternehmen und Behörden die perfekte Wahl ist. Da das datAshur PRO² über die integrierte Tastatur und nicht über einen Hostcomputer entsperrt wird, ist es nichtanfällig für software-/hardwarebasierte Key-Logger oder Brute-Force-Angriffe.

Eine der einzigartigen zugrundeliegenden Sicherheitsfunktionen des DSGVO-konformen datAshur 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 das datAshur PRO² auf einen automatischen Angriff, indem es in den Deadlock-Status wechselt (einfriert), sodass sich alle diese Angriffe als vergeblich erweisen. Einfach ausgedrückt: Ohne PIN ist kein Zugriff möglich!

Paketinhalt

- iStorage datAshur PRO²
- Hülle aus stranggepresstem Aluminium
- Schnellanleitung

1. LED-Anzeigen und ihre Aktionen

LED	LED-Status	Beschreibung	LED	LED-Status	Beschreibung
▲	ROT leuchtet durchgehend	Gesperrtes Gerät (entweder im **Standby-** oder **Zurücksetz-**Status)	▲▼▲	ROT, GRÜN und BLAU blinkt	Wartet auf die Eingabe der **Benutzer-**PIN
▲	ROT erlischt langsam	Gerät schaltet sich in den **Leerlauf ab**	▼▲	GRÜN und BLAU blinken zusammen	Wartet auf die Eingabe der **Admin-**PIN
▼	GRÜN blinkt	**Entsperrtes** Gerät als **Admin** (nicht an den USB-Anschluss angeschlossen)	▼▲	GRÜN und BLAU blinken abwechselnd	Authentifizierung läuft
▼	GRÜN leuchtet durchgehend	**Entsperrtes** Gerät als **Benutzer** (nicht an den USB-Anschluss angeschlossen) oder Gerät im Benutzermodus	▲	BLAU blinkt alle 5 Sekunden	Der Akku beginnt nach 30 Sekunden, sich aufzuladen, wenn das Gerät gesperrt und an einen USB-Anschluss angeschlossen ist
▲	BLAU leuchtet durchgehend	Gerät im **Admin-Modus**			

2. Akku- und LED-Status

Hinweis: Die normale Funktion des datAshur PRO² kann durch starke elektromagnetische Einwirkung gestört werden. Wenn dies der Fall ist, führen Sie einfach eine Aus- und Wiedereinschaltung für das Produkt durch (das Produkt ausschalten und anschließend wieder einschalten), um den normalen Betrieb wieder aufzunehmen. Wenn der normale Betrieb nicht wieder aufgenommen wird, verwenden Sie das Produkt bitte an einem anderen Ort.

Sensor für niedrigen Akkustand

Das datAshur PRO² enthält einen Spannungserfassungskreis, der die Akkuausgangsleistung überwacht, wenn das Gerät eingeschaltet ist. Wenn die Akkuausgangsleistung auf oder unter 3,3 V abfällt, blinkt die ROTE LED dreimal auf und erlischt langsam. An diesem Punkt sollte der Benutzer das datAshur PRO² an einen eingeschalteten USB-Anschluss anschließen und 15 - 30 Minuten lang aufladen. Sobald es aufgeladen ist, nimmt das datAshur PRO² die normale Funktion wieder auf.

Zur Aktivierung aus dem Leerlauf

ist der Leerlauf als der Status definiert, in dem das datAshur PRO² nicht verwendet wird und alle LEDs ausgeschaltet sind.

Zum Aktivieren des datAshur PRO² aus dem Leerlauf führen Sie Folgendes aus.

Halten Sie die **UMSCHALTTASTE** (⬆) für eine Sekunde gedrückt oder schließen Sie das Gerät an einen mit Strom versorgten USB-Port an.	▲ ▼ ▲	Die ROTE, GRÜNE und BLAUE LED blinken einmal in Folge, danach blinkt die GRÜNE LED zweimal und wechselt schließlich auf eine durchgehend leuchtende ROTE LED, was angibt, dass sich das Gerät im Standby befindet

Zum Wechseln in den Leerlauf

Um den Wechsel des datAshur PRO² in den Leerlauf zu erzwingen, führen Sie einen der folgenden Abläufe durch:

- Wenn das Gerät an einen USB-Anschluss angeschlossen ist, trennen Sie es.
- Wenn das Gerät nicht an einen USB-Anschluss angeschlossen ist, drücken Sie die **UMSCHALTTASTE** (⬆) und halten Sie sie 1 Sekunde lang gedrückt, bis die LED auf durchgehendes ROT wechselt und langsam in den Leerlauf (Aus) erlischt.

Hinweis: Wenn das datAshur PRO² entsperrt und nicht an einen USB-Anschluss angeschlossen ist und wenn 30 Sekunden lang keine Aktionen ausgeführt werden, wechselt das Gerät automatisch in den Leerlauf. Die LED wechselt auf durchgehend leuchtendes ROT und erlischt danach langsam in den Leerlauf.

Wenn das datAshur PRO² an einen USB-Anschluss angeschlossen ist, funktioniert die **UMSCHALTTASTE** (⬆) nicht.

Wenn es an einen aktivierten USB-Anschluss angeschlossen ist, beginnt ein gesperrtes datAshur PRO² sich nach 30 aufzuladen, was dadurch angegeben wird, dass die BLAUE LED alle 5 Sekunden blinkt.

Eingeschalteter Status

Nach dem Aktivieren aus dem Leerlauf geht das Gerät in einen der folgenden, in der Tabelle unten gezeigten Status.

Eingeschalteter Status	LED-Anzeige	Verschlüsselungsschlüssel	Admin -PIN	Beschreibung
Standby	ROT leuchtet durchgehend	✓	✓	Bus wartet auf die Eingabe der Admin- oder Benutzer-PIN
Zurücksetzen	ROT leuchtet durchgehend	×	×	Wartet auf die Konfiguration einer Admin-PIN
Niedriger Akkustand	ROT blinkt dreimal	✓	✓	Aufladen an einem aktivierten USB-Anschluss für 15 - 30 Minuten
Ursprünglicher Versandstatus	ROT und GRÜN leuchten durchgehend	✓	×	Wartet auf die Konfiguration einer Admin-PIN

3. Erstmalige Verwendung

Das datAshur PRO² wird im **„ursprünglichen Versandstatus“ und ohne voreingestellte Admin-PIN** geliefert. Es muss eine **7- bis 15-**stellige Admin-PIN konfiguriert werden, bevor der Datenträger verwendet werden kann. Sobald eine Admin-PIN erfolgreich konfiguriert wurde, ist es nicht möglich, den Datenträger zurück auf den „ursprünglichen Versandstatus“ zu setzen.

PIN-Anforderungen:

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

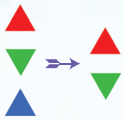
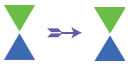
Passwort-Tipp: Sie können einen einprägsamen Begriff, Namen, Ausdruck oder eine andere alphanumerische PIN-Kombination konfigurieren, indem Sie einfach die Tasten mit den entsprechenden Buchstaben drücken.

Beispiele für alphanumerische PINs sind:

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

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

Um eine Admin-PIN zu konfigurieren und das datAshur PRO² erstmalig zu entsperren, befolgen Sie bitte die einfachen Schritte in der Tabelle unten.

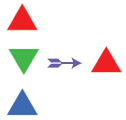
Anweisungen – erstmalige Verwendung	LED	LED-Status
1. Drücken Sie die **UMSCHALTTASTE** (⇧) und halten Sie sie 1 Sekunde lang gedrückt		Die ROTE, GRÜNE und BLAUE LED blinken einmal in Folge, danach blinkt die GRÜNE LED zweimal und wechselt schließlich zu durchgehend leuchtender ROTER und GRÜNER LED, was angibt, dass sich der Datenträger im ursprünglichen Versandstatus befindet
2. Drücken Sie die Tasten **SCHLÜSSEL (🔑) + 1** und halten Sie sie gedrückt		Die LEDs wechseln auf blinkendes GRÜN und durchgehend leuchtendes BLAU
3. Geben Sie die **neue Admin- PIN** ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)** einmal		Die blinkende GRÜNE und durchgehend leuchtende BLAUE LED wechseln auf ein GRÜNES BLINKEN und danach wieder auf eine blinkende GRÜNE und durchgehend leuchtende BLAUE LED
4. Geben Sie die **neue Admin-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)** erneut		Die BLAUE LED blinkt schnell und wechselt danach auf eine durchgehend leuchtende BLAUE LED und schließlich zu einer blinkenden GRÜNEN LED, was angibt, dass die Admin-PIN erfolgreich konfiguriert wurde und dass der Datenträger entsperrt ist

Hinweis: Sobald das datAshur PRO² erfolgreich entsperrt wurde, blinkt die GRÜNE LED nur für 30 Sekunden. Während dieser Zeit muss das datAshur PRO² über einen stromführenden USB-Anschluss angeschlossen sein. Es kann sofort gesperrt werden (wenn es nicht an einen USB-Anschluss angeschlossen ist), indem Sie die **UMSCHALTTASTE** (⇧) drücken und 1 Sekunde lang halten oder indem Sie auf das Symbol „Hardware sicher entfernen/auswerfen" Ihres Betriebssystems klicken, wenn es an einen USB-Anschluss angeschlossen ist.
Wenn das datAshur PRO² entsperrt und an einen USB-Anschluss angeschlossen ist, akzeptiert es keine weiteren Anweisungen über die Tastatur.

Sperren des datAshur PRO²
Um den Datenträger zu sperren, werfen Sie das datAshur PRO² sicher aus Ihrem Hostbetriebssystem aus und trennen Sie es vom USB-Anschluss. Wenn gerade Daten auf den Datenträger geschrieben werden, führt das Trennen des datAshur PRO² zu unvollständiger Datenübertragung und möglicher Datenbeschädigung.

4. Entsperren des datAshur PRO² mit der Admin-PIN

Um das datAshur PRO² mit der Admin-PIN zu entsperren, befolgen Sie bitte die einfachen Schritte in der Tabelle unten.

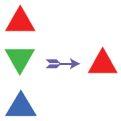
1. Drücken Sie die **UMSCHALTTASTE** (⇧) und halten Sie sie kunde lang gedrückt		Die ROTE, GRÜNE und BLAUE LED blinken einmal in Folge, danach blinkt die GRÜNE LED zweimal und wechselt schließlich auf eine durchgehend leuchtende ROTE LED, was angibt, dass sich der Datenträger im Standby befindet
2. Drücken Sie im Standby (durchgehend leuchtende ROTE LED) einmal auf die **SCHLÜSSEL-Taste (🔑)**		Die GRÜNE und BLAUE LED blinken zusammen.
3. Geben Sie mit zusammen blinkender GRÜNER und BLAUER LED die **Admin-PIN** ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)** erneut		Die GRÜNE und BLAUE LED blinken abwechselnd mehrere Male und danach eine durchgehend leuchtende BLAUE LED und Wechsel auf eine blinkende GRÜNE LED, was angibt, dass der Datenträger erfolgreich als Admin entsperrt wurde

Hinweis: Sobald das datAshur PRO² erfolgreich entsperrt wurde, blinkt die GRÜNE LED nur für 30 Sekunden. Während dieser Zeit muss das datAshur PRO² über einen stromführenden USB-Anschluss angeschlossen sein. Es kann sofort gesperrt werden (wenn es nicht an einen USB-Anschluss angeschlossen ist), indem Sie die **UMSCHALTTASTE** (⬆) drücken und 1 Sekunde lang halten oder indem Sie auf das Symbol „Hardware sicher entfernen/auswerfen“ Ihres Betriebssystems klicken, wenn es an einen USB-Anschluss angeschlossen ist.

Wenn das datAshur PRO² entsperrt und an einen USB-Anschluss angeschlossen ist, akzeptiert es keine weiteren Anweisungen über die Tastatur.

5. In den Admin-Modus gehen

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

1. Drücken Sie die **UMSCHALTTASTE** (⬆) und halten Sie sie 1 Sekunde lang gedrückt		Die ROTE, GRÜNE und BLAUE LED blinken einmal in Folge, danach blinkt die GRÜNE LED zweimal und wechselt schließlich auf eine durchgehend leuchtende ROTE LED, was angibt, dass sich das Gerät im Standby befindet
2. Drücken Sie im Standby (durchgehend leuchtende ROTE LED) einmal auf die **SCHLÜSSEL-Taste (🔑)**		Die GRÜNE und BLAUE LED blinken zusammen.
3. Geben Sie mit gemeinsam blinkender GRÜNER und BLAUER LED die **Admin-PIN** ein und drücken Sie die **SCHLÜSSEL**-Taste (🔑) erneut		Die GRÜNE und BLAUE LED blinken abwechselnd mehrere Male und danach eine durchgehend leuchtende BLAUE LED mit Wechsel zu einer blinkenden GRÜNEN LED, die angibt, dass das Gerät entsperrt ist
4. Drücken Sie die **SCHLÜSSEL-Taste (🔑)** innerhalb von 2 Sekunden **dreimal** (**SCHLÜSSEL-Taste (🔑)** x **3**)		Die blinkende GRÜN LED wird zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass sich das Gerät im Admin-Modus befindet

6. Admin-Modus beenden

Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

7. Ändern der Admin-PIN

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern aufweisen
- Darf nicht nur gleiche Ziffern enthalten, z. B. (3-3-3-3-3-3-3-3)
- 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 einen einprägsamen Begriff, Namen, Ausdruck oder eine andere alphanumerische PIN-Kombination erstellen, indem Sie einfach die Tasten mit den entsprechenden Buchstaben drücken.

Beispiele für alphanumerische PINs sind:

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

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

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

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (⚷) + 2**		Die durchgehend BLAU leuchtende LED wird zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED
2. Geben Sie die **NEUE Admin-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**		Die blinkende GRÜNE LED und durchgehend BLAU leuchtende LED werden zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
3. Geben Sie die **NEUE Admin-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (⚷)**		Statt der blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED werden eine schnell blinkende BLAUE LED und schließlich eine durchgehend leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Admin-PIN erfolgreich geändert wurde

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

8. Einstellen einer Benutzer-PIN-Richtlinie

Der Administrator kann eine Einschränkungsrichtlinie für die Benutzer-PIN einstellen. Diese Richtlinie umfasst das Einstellen der PIN-Mindestlänge (7 bis 15 Zeichen) sowie, ob ein oder mehrere „**Sonderzeichen**“ gefordert werden oder nicht. Die Funktionen „Sonderzeichen“, wenn die Tasten „**UMSCHALTTASTE** (⬆) + **Zeichen**“ gleichzeitig gedrückt werden.

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 oder mehrere „Sonderzeichen“ verwendet werden müssen, anders gesagt „**UMSCHALTTASTE (⬆)+ Zeichen**“. In der gleichen Weise kann eine Benutzer-PIN-Richtlinie ohne die Notwendigkeit eines „Sonderzeichen“ eingestellt werden. Bei „**120**“ zum Beispiel geben die ersten beiden Ziffern (**12**) die Mindestlänge der PIN an (in diesem Fall **12**) und die letzte Ziffer (**0**) bedeutet, dass kein Sonderzeichen erforderlich ist.

Sobald der Administrator die Benutzer-PIN-Richtlinie eingestellt hat, zum Beispiel „091“, muss eine neue Benutzer-PIN konfiguriert werden - siehe Abschnitt 11, „Neue Benutzer-PIN im Admin-Modus hinzufügen“. Wenn der Administrator die Benutzer-PIN als „**247688314**“ unter Verwendung eines „**Sonderzeichens**“ (**UMSCHALTTASTE** (⬆) **+ Zeichen** gemeinsam gedrückt) konfiguriert, kann dieses Sonderzeichen bei der Erstellung der Benutzer-PIN an beliebiger Stelle in der 7- bis 15-stelligen PIN platziert werden, wie in folgenden Beispielen gezeigt.

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

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

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

Hinweis:

- Wenn bei der Konfiguration der Benutzer-PIN ein „Sonderzeichen“ verwendet wurde, zum Beispiel „**B**“ oben, kann der Datenträger nur durch Eingabe der PIN unter Eingabe des „Sonderzeichens“ in genau der konfigurierten Reihenfolge entsperrt werden, wie zum Beispiel „**B**“ oben - („2“, „4“, „**UMSCHALTTASTE** (⬆) **+ 7**“, „6“, „8“, „8“, „3“, „1“, „4’).
- Es kann mehr als ein „Sonderzeichen“ verwendet und entlang Ihrer 7- bis 15-stelligen PIN platziert werden.
- Die Benutzer können ihre PIN ändern, werden jedoch gezwungen, die eingestellte „Benutzer-PIN-Richtlinie“ (Beschränkungen) einzuhalten, wenn und wann diese gilt.
- Das Einstellen einer neuen Benutzer-PIN-Richtlinie löscht automatisch eine vorhandene Richtlinie.
- Diese Richtlinie gilt nicht für die „Selbstzerstörungs-PIN“. Die Einstellung der Komplexität für die Selbstzerstörungs-PIN und Admin-PIN lautet immer 7 - 15 Ziffern ohne erforderliches Sonderzeichen.

Um eine **Benutzer-PIN-Richtlinie** festzulegen, rufen Sie zunächst den „**Administratormodus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (⚷) + 7**.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
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 wurde oder nicht.		Die blinkende GRÜNE und BLAUE LED blinken weiter
3. Drücken Sie einmal die **UMSCHALTTASTE** (⬆)		Die blinkende GRÜNE und blinkende BLAUE LED wechseln zu durchgehend GRÜN und schließlich durchgehend BLAU und zeigen so an, dass die Benutzer-PIN-Richtlinie erfolgreich festgelegt wurde.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALT-TASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

9. So löschen Sie die Benutzer-PIN-Richtlinie

Um eine **Benutzer-PIN-Richtlinie** zu löschen, rufen Sie zunächst den „**Administratormodus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑 + 7**.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Geben Sie **070** ein und drücken Sie einmal auf die **UM-SCHALTTASTE** (⬆)		Die blinkende GRÜNE und blinkende BLAUE LED wechseln zu durchgehend GRÜN und schließlich durchgehend BLAU und zeigen so an, dass die Benutzer-PIN-Richtlinie erfolgreich gelöscht wurde.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALT-TASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

10. So prüfen 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 prüfen, rufen Sie zunächst den „**Admin-Modus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALT-TASTE** (⬆) **+ 7** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die „**SCHLÜSSEL-Taste (🔑)**“ und Folgendes geschieht: a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend. b. Ein ROTES LED-Blinken entspricht zehn (10) Einheiten einer PIN. c. Ein GRÜNES LED-Blinken entspricht einer (1) Einheit einer PIN d. Ein BLAUES Blinken zeigt an, dass ein „Sonderzeichen“ verwendet wurde. e. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend. 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 (**121**) eingestellt haben, blinkt die ROTE LED einmal (**1**) und die GRÜNE LED blinkt zweimal (**2**) gefolgt von einer einmal blinkenden (**1**) BLAUEN LED, die angibt, dass ein **Sonderzeichen** verwendet werden muss.

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

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALT-TASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

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

Wichtig: Eine neue Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ erstellt werden, wenn eine wie in Abschnitt 8 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie schreibt eine Mindest-PIN-Länge vor und ob ein „Sonderzeichen“ verwendet wurde. Siehe Abschnitt 10, um die Benutzer-PIN-Beschränkungen zu prüfen.

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern aufweisen
- Darf nicht nur gleiche Ziffern enthalten, z. B. (3-3-3-3-3-3-3-3)
- 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)
- Die **UMSCHALTTASTE** (⬆) kann für zusätzliche PIN-Kombinationen verwendet werden - z. B. **UMSCHALTTASTE** (⬆) **+ 1** entspricht einem anderen Wert als 1. Siehe Abschnitt 8, „Benutzer-PIN-Richtlinie einstellen“.

Um einen **neue Benutzer-PIN** hinzuzufügen, wechseln Sie zuerst in den Admin-Modus wie in Abschnitt 5 beschrieben. Wenn sich der Datenträger im **Admin-Modus** befindet (durchgehend leuchtende BLAUE LED), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 3**.		Die durchgehend BLAU leuchtende LED wird zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED
2. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)**		Die blinkende GRÜNE LED und durchgehend BLAU leuchtende LED werden zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
3. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)** erneut.		Statt der blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED werden eine schnell blinkende GRÜNE LED und dann eine durchgehend leuchtende BLAUE LED angezeigt. Dies gibt an, dass eine neue Benutzer-PIN erfolgreich konfiguriert wurde.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

12. Ändern der Benutzer-PIN im Admin-Modus

Wichtig: Die Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ geändert werden, wenn eine wie in Abschnitt 8 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie schreibt eine Mindest-PIN-Länge vor und ob ein „Sonderzeichen“ verwendet wurde. Siehe Abschnitt 10, um die Benutzer-PIN-Beschränkungen zu prüfen.

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

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (ಠ) + 3**.		Die durchgehend BLAU leuchtende LED wird zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED
2. Geben Sie die neue **Benutzer-PIN** ein und drücken Sie die **SCHLÜSSEL-Taste (ಠ)**		Die blinkende GRÜNE LED und durchgehend BLAU leuchtende LED werden zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
3. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (ಠ)** erneut.		Statt der blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED werden eine schnell blinkende GRÜNE LED und dann eine durchgehend leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Benutzer-PIN erfolgreich geändert wurde.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

13. Löschen der Benutzer-PIN im Admin-Modus

Um eine bestehende Benutzer-PIN zu löschen , gehen Sie zunächst in den „**Admin-Modus**“ wie in Abschnitt 5 beschrieben. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

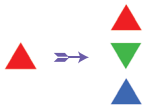
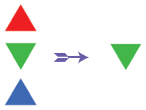
1. Halten Sie im Admin-Modus die beiden Tasten **UMSCHALTTASTE** (⬆) **+ 3** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED wird eine blinkende ROTE LED angezeigt.
2. Halten Sie die Tasten **UMSCHALTTASTE** (⬆) **+ 3** erneut gedrückt		Statt der blinkenden ROTEN LED werden eine durchgehend leuchtende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

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALT-TASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

14. So entsperren Sie das datAshur PRO¹² mit Benutzer-PIN

Um mit der **Benutzer-PIN zu entsperren,** muss sich das datAshur PRO² zunächst im Standby befinden (durchgehend leuchtende ROTE LED), in dem Sie die **UMSCHALTTASTE** (⬆) 1 Sekunde lang gedrückt halten.

1. Halten Sie im Standby (durchgehend leuchtende ROTE LED) die Tasten **UMSCHALTTASTE** (⬆) **+ SCHLÜSSEL (🔑)** gedrückt		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 **SCHLÜSSEL(🔑)-Taste**.		Die blinkende ROTE, GRÜNE und BLAUE LED werden zu abwechselnd GRÜNER und BLAUER LED, danach zu einer durchgehend leuchtenden GRÜNEN LED, was angibt, dass der Datenträger im Benutzermodus erfolgreich entsperrt wurde

15. Ändern der Benutzer-PIN im Benutzermodus

Um die **Benutzer-PIN** zu ändern, entsperren Sie zunächst das datAshur PRO² mit einer Benutzer-PIN, wie oben in Abschnitt 14 beschrieben. Wenn sich der Datenträger im **Benutzermodus** befindet (GRÜNE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Benutzermodus die Tasten **SCHLÜSSEL (🔑) + 4**		Die durchgehend leuchtende GRÜNE LED ändert sich in eine blinkende GRÜNE und eine durchgehend leuchtende BLAUE LED.
2. e die **SCHLÜSSEL-Taste (🔑)**		Die blinkende GRÜNE LED und durchgehend BLAU leuchtende LED werden zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
3. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)**		Die blinkende GRÜNE und die durchgehend leuchtende BLAUE LED ändern sich in eine schnell blinkende GRÜNE LED und dann in eine leuchtende GRÜNE LED, was eine erfolgreiche Änderung der Benutzer-PIN anzeigt.

Wichtig: Die Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ geändert werden, wenn eine wie in Abschnitt 8 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie schreibt eine Mindest-PIN-Länge vor und ob ein „Sonderzeichen“
verwendet wurde. Der Administrator kann Abschnitt 10 heranziehen, um die Benutzer-PIN-Beschränkungen zu prüfen.

16. Erstellen einer einmaligen Benutzerwiederherstellungs-PIN

Die Benutzerwiederherstellungs-PIN ist sehr nützlich in Situationen, in denen ein Benutzer seine PIN vergessen hat, um das datAshur PRO² zu entsperren. Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zunächst die richtige einmalige Wiederherstellungs-PIN eingeben, wenn eine konfiguriert wurde. Der Wiederherstellungsprozess für die Benutzer-PIN wirkt sich nicht auf die Daten, den Verschlüsselungsschlüssel und die Admin-PIN aus, der Benutzer wird jedoch gezwungen, eine neue 7- bis 15-stellige Benutzer-PIN zu konfigurieren. Um eine 7- bis 15-stellige Benutzerwiederherstellungs-PIN zu konfigurieren, gehen Sie zunächst in den „**Admin-Modus**“ wie in Abschnitt 5 beschrieben. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 4**.		Die durchgehend BLAU leuchtende LED wird zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED
2. Geben Sie **eine einmalige Wiederherstellungs-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**		Die blinkende GRÜNE LED und durchgehend BLAU leuchtende LED werden zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
3. Geben Sie **eine einmalige Wiederherstellungs-PIN** erneut ein und drücken Sie erneut auf die **SCHLÜSSEL-Taste (🔑)**		Statt der blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED wird eine schnell blinkende GRÜNE LED und dann eine durchgehend leuchtende BLAUE LED angezeigt. Dies gibt an, dass die einmalige Wiederherstellungs-PIN erfolgreich konfiguriert wurde.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

17. Löschen der einmaligen Benutzerwiederherstellungs-PIN

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

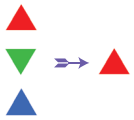
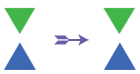
1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE (⬆) + 4** gedrückt		Statt der durchgehend leuchtenden BLAUEN LED wird eine blinkende ROTE LED angezeigt
2. Halten Sie die **UMSCHALTTASTE (⬆) + 4** erneut gedrückt		Die blinkende ROTE LED wird zu durchgehend ROT leuchtend und danach zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass die einmalige Benutzerwiederherstellungs-PIN erfolgreich gelöscht wurde

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

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

Die Benutzerwiederherstellungs-PIN ist sehr nützlich in Situationen, in denen ein Benutzer seine PIN vergessen hat, um das datAshur PRO² zu entsperren. Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zunächst die richtige einmalige Wiederherstellungs-PIN eingeben, wenn eine konfiguriert wurde. Der Wiederherstellungsprozess für die Benutzer-PIN wirkt sich nicht auf die Daten, den Verschlüsselungsschlüssel und die Admin-PIN aus, der Benutzer wird jedoch gezwungen, eine neue 7- bis 15-stellige Benutzer-PIN zu konfigurieren. Zum Aktivieren des Wiederherstellungsprozesses und zum Konfigurieren einer neuen Benutzer-PIN führen Sie die folgenden Schritte durch.

1. Mit dem Datenträger im **Leerlauf** halten Sie die **UMSCHALTTASTE** (⬆) 1 Sekunde lang gedrückt		Die ROTE, GRÜNE und BLAUE LED blinken einmal in Folge, danach blinkt die GRÜNE LED zweimal und wechselt schließlich auf eine durchgehend leuchtende ROTE LED, was angibt, dass sich der Datenträger im Standby befindet
2. Drücken und halten Sie im **Standby** die Tasten **SCHLÜSSEL (🔑) + 4**		Statt der durchgehend ROT leuchtenden LED werden blinkende ROTE und GRÜNE LEDs angezeigt
3. Geben Sie die einmalige **Wiederherstellungs-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**		Die GRÜNE und BLAUE LED wechselt zwischen Ein und Aus und wird danach zu einer durchgehend leuchtenden GRÜNEN LED und schließlich zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
4. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)**		Statt der blinkenden GRÜNEN LED und der durchgehend leuchtenden BLAUEN LED wird eine einzelne blinkende GRÜNE LED angezeigt. Dann werden wieder eine blinkende GRÜNE LED und eine durchgehend leuchtende BLAUE LED angezeigt.
5. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)** erneut		Die GRÜNE LED blinkt schnell und wird danach zu durchgehend GRÜN leuchtend, was angibt, dass der Wiederherstellungsprozess erfolgreich war und dass eine neue Benutzer-PIN konfiguriert wurde

Wichtig: Eine neue Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ erstellt werden, wenn eine wie in Abschnitt 8 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie schreibt eine Mindest-PIN-Länge vor und ob ein Sonderzeichen verwendet wurde. Siehe Abschnitt 10, um die Benutzer-PIN-Beschränkungen zu prüfen.

19. Einstellen des Lesezugriffs für Benutzer im Admin-Modus

Mit zahlreichen Viren und Trojanern, die USB-Datenträger infizieren, ist die Schreibschutzfunktion besonders nützlich, wenn Sie in einem öffentlichen Raum auf die Daten auf dem USB-Datenträger zugreifen müssen. Das ist auch eine grundlegende Funktion zu forensischen Zwecken, wenn die Daten in ihrem ursprünglichen und unveränderten Zustand, der nicht geändert oder überschrieben werden kann, bewahrt werden müssen.

Wenn der Administrator das datAshur PRO² konfiguriert und den Benutzerzugriff auf den Lesezugriff beschränkt, kann nur der Administrator auf den Datenträger schreiben oder die Einstellung wie in Abschnitt 20 beschrieben wieder auf Lesen/Schreiben setzen. Der Benutzer hat auf den Lesezugriff beschränkten Zugriff und kann weder auf den Datenträger schreiben noch diese Einstellung im Benutzermodus ändern.

Um das datAshur PRO² einzurichten und den Benutzerzugriff auf den Lesezugriff zu beschränken, gehen Sie zunächst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten „**7 + 6**“.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden GRÜNEN LED und danach zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass der Datenträger konfiguriert wurde und den Benutzerzugriff auf den Lesezugriff beschränkt

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet). Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

20. Aktivieren des Lese-/Schreibzugriffs für Benutzer im Admin-Modus

Um das datAshur PRO² wieder auf Lesen/Schreiben zurückzusetzen, gehen Sie zunächst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten „**7 + 9**“.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden GRÜNEN LED, danach zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass der Datenträger als Lesen/Schreiben konfiguriert ist

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

21. Einstellen des globalen Lesezugriffs im Admin-Modus

Wenn der Administrator das datAshur PRO² konfiguriert und den Zugriff auf den globalen Lesezugriff beschränkt, können weder der Administrator noch der Benutzer auf den Datenträger schreiben und beide verfügen lediglich über auf den Lesezugriff beschränkten Zugriff. Nur der Administrator kann die Einstellung wie in Abschnitt 22 beschrieben wieder auf Lesen/Schreiben setzen. Um das datAshur PRO² einzurichten und den globalen Zugriff auf den Lesezugriff zu beschränken, gehen Sie zunächst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten „**5 + 6**“.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden GRÜNEN LED und danach zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass der Datenträger konfiguriert wurde und den globalen Zugriff auf den Lesezugriff beschränkt

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

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

Um das datAshur PRO² wieder auf Lesen/Schreiben zu setzen, gehen Sie zunächst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten „**5 + 9**“.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden GRÜNEN LED, danach zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass der Datenträger als Lesen/Schreiben konfiguriert ist

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALT-TASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

23. So konfigurieren Sie eine Selbstzerstörungs-PIN

Sie können eine Selbstzerstörungs-PIN konfigurieren, die, wenn sie eingegeben wird, ein Crypto-Erase auf dem Datenträger ausführt (der Verschlüsselungsschlüssel wird gelöscht). Dieser Prozess löscht alle konfigurierten PINs und macht alle auf dem Datenträger gespeicherten Daten unzugänglich (für immer verloren), der Datenträger wird daraufhin mit einer GRÜNEN LED als entsperrt angezeigt. Die Ausführung dieser Funktion führt dazu, dass die Selbstzerstörungs-PIN die neue Benutzer-PIN wird und dass der Datenträger formatiert werden muss, bevor er wieder verwendet werden kann.

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

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 6**.		Die durchgehend BLAU leuchtende LED wird zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED
2. Konfigurieren Sie eine 7- bis 15-stellige **Selbstzerstörungs-PIN** und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**		Die blinkende GRÜNE LED und durchgehend BLAU leuchtende LED werden zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
3. Geben Sie die **Selbstzerstörungs-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)**		Die GRÜNE LED blinkt einige Sekunden lang schnell und wird dann zu einer durchgehend leuchtenden BLAUEN LED, um anzugeben, dass die Selbstzerstörungs-PIN erfolgreich konfiguriert wurde

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

24. So löschen Sie die Selbstzerstörungs-PIN

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

1. Halten Sie im Admin-Modus die Tasten **UMSCHALT-TASTE + 6** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED wird eine blinkende ROTE LED angezeigt.
2. Drücken und halten Sie die Tasten **UMSCHALTTASTE + 6** erneut		Statt der blinkenden ROTEN LED wird eine durchgehend leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Selbstzerstörungs-PIN erfolgreich gelöscht wurde.

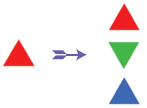
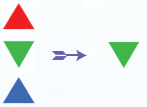
Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

25. So entsperren Sie mit der Selbstzerstörungs-PIN

Warnung: Wenn der Selbstzerstörungsmechanismus aktiviert ist, werden alle Daten, der Verschlüsselungsschlüssel und die Admin-/Benutzer-PINs gelöscht. **Die Selbstzerstörungs-PIN wird die Benutzer-PIN.** Nach der Aktivierung der Selbstzerstörungsmechanismus ist keine Admin-PIN vorhanden. Das datAshur PRO² muss zunächst zurückgesetzt werden (siehe Komplettes Zurücksetzen in Abschnitt 35 auf Seite 28), um eine Admin-PIN mit vollen Admin-Privilegien, einschließlich Konfigurieren einer Benutzer-PIN, zu erstellen.

Wenn verwendet, **löscht die Selbstzerstörungs-PIN 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 dass das datAshur PRO² partitioniert und formatiert werden muss, bevor neue Daten zum Datenträger hinzugefügt werden können. Um den Selbstzerstörungsmechanismus zu aktivieren, muss sich der Datenträger im Standby-Status (ROTE LED leuchtet durchgehend) befinden. Führen Sie die folgenden Schritte durch.

1. Halten Sie im Standby (durchgehend leuchtende ROTE LED), die Tasten **UMSCHALTTASTE** (⬆) **+ SCHLÜSSEL** (🔑) gedrückt		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 **SCHLÜSSEL-Taste** (🔑)		Die ROT, GRÜN und BLAU blinkende LED werden zu einer GRÜNEN und BLAUEN LED, die einige Sekunden lang zwischen Ein und Aus wechseln und schließlich zu einer durchgehend leuchtenden GRÜNEN LED werden, was angibt, dass die Selbstzerstörung des datAshur PRO² erfolgreich durchgeführt wurde

26. So konfigurieren Sie eine Admin-PIN nach einem Brute-Force-Angriff oder dem Zurücksetzen

Nach einem Brute Force-Angriff oder dem Zurücksetzen des datAshur PRO² muss eine Admin-PIN erstellt werden, bevor der Datenträger verwendet werden kann.

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)

Nach einem Brute-Force-Angriff oder dem Zurücksetzen des datAshur PRO² befindet sich der Datenträger im Standby-Status (ROTE LED leuchtet). Um eine Admin-PIN zu konfigurieren, gehen Sie wie folgt vor.

1. Halten Sie im Standby (durchgehend leuchtende ROTE LED), die beiden Tasten **UMSCHALTTASTE (⬆) + 1** gedrückt		Die durchgehend ROT leuchtende LED wird zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED
2. Geben Sie die **neue Admin-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**		Die blinkende GRÜNE LED und durchgehend BLAU leuchtende LED werden zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und durchgehend leuchtenden BLAUEN LED
3. Geben Sie die **neue Admin-PIN** erneut ein und drücken Sie die **SCHLÜSSEL-Taste (🔑)**		Statt der blinkenden GRÜNEN und leuchtenden BLAUEN LED werden eine einige Sekunden schnell blinkende BLAUE LED und dann eine durchgehend leuchtende BLAUE LED angezeigt. Dies gibt an, dass die Admin-PIN erfolgreich konfiguriert wurde.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

27. Einstellen der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“

Um den Datenträger vor unbefugtem Zugriff zu schützen, wenn er entsperrt und unbeaufsichtigt ist, kann festgelegt werden, dass das datAshur PRO² automatisch nach einem vorab ausgewählten Zeitraum gesperrt wird. In diesem Standardstatus ist das Timeout der Funktion „Automatische Sperre, wenn unbeaufsichtigt“ des datAshur PRO² deaktiviert. „Automatische Sperre, wenn unbeaufsichtigt“ kann auf 5 bis 99 Minuten festgelegt werden.

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

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 5**.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Geben Sie den von Ihnen gewünschten Zeitraum für „Automatische Sperre, wenn unbeaufsichtigt“ ein, mindestens 5 Minuten und maximal 99 Minuten (5 bis 99 Minuten). Geben Sie beispielsweise Folgendes ein: **05 für 5 Minuten (drücken Sie auf „0“ gefolgt von einer „5“)** **20 für 20 Minuten (drücken Sie auf „2“ gefolgt von einer „0“)** **99 für 99 Minuten (drücken Sie auf „9“ gefolgt von einer weiteren „9“)**		
3. Drücken Sie einmal auf die **UMSCHALTTASTE (⬆)**		Die blinkende GRÜNE und blinkende BLAUE LED ändern sich eine Sekunde lang in eine durchgehend leuchtende GRÜNE LED und dann in eine durchgehend leuchtende BLAUE LED. Dies gibt an, dass das Timeout für die automatische Sperre erfolgreich konfiguriert ist.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet). Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE (⬆)** für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

28. 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 der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 5**.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Geben Sie **00** und drücken Sie die **UMSCHALTTASTE (⬆)**		Die blinkende GRÜNE und blinkende BLAUE LED ändern sich eine Sekunde lang in eine durchgehend leuchtende GRÜNE LED und dann in eine durchgehend leuchtende BLAUE LED. Dies gibt an, dass das Timeout für die automatische Sperre erfolgreich deaktiviert wurde.

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).
Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE (⬆)** für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

29. So überprüfen Sie die Uhr für „Automatische Sperre, wenn unbeaufsichtigt“

Der Administrator kann die Uhr für „Automatische Sperre, wenn unbeaufsichtigt“ prüfen und bestimmen, indem er einfach die LED-Sequenz wie auf der Tabelle unten auf dieser Seite beschrieben notiert.
Um „Automatische Sperre, wenn unbeaufsichtigt“ zu prüfen, rufen Sie zunächst den „**Administratormodus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALT-TASTE (⬆) + 5** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die „**SCHLÜSSEL-Taste (🔑)**“ und Folgendes geschieht: a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend. b. Jedes ROTE LED-Blinken entspricht zehn (10) Minuten. c. Jedes GRÜNE LED-Blinken entspricht einer (1) Minute. d. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend. e. Die LEDs leuchten wieder durchgehend BLAU		

Die nachstehende Tabelle beschreibt das LED-Verhalten bei „Automatische Sperre, wenn unbeaufsichtigt“. Wenn Sie den Datenträger beispielsweise auf eine automatische Sperrung nach **25** Minuten konfiguriert haben, blinkt die ROTE LED zweimal (**2**) und die GRÜNE LED fünfmal (**5**).

Autom. Sperre in Minuten	**ROT**	**GRÜN**
5 Minuten	0	5x Blinken
15 Minuten	1x Blinken	5x Blinken
25 Minuten	2x Blinken	5x Blinken
40 Minuten	4x Blinken	0

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).
Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

30. Einstellen des Lesezugriffs im Benutzermodus

Um das datAshur PRO² auf den Lesezugriff zu setzen, gehen Sie zunächst wie in Abschnitt 14 beschrieben in den „**Benutzermodus**“. Wenn sich der Datenträger im **Benutzermodus** befindet (GRÜNE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Benutzermodus die Tasten „**7 + 6**“. (7=**R**ead (Lese) + 6=**O**nly (Zugriff))		Statt der durchgehend leuchtenden GRÜNEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und BLAUE LED ändern sich in eine durchgehend leuchtende GRÜNE LED. Dies gibt an, dass die Festplatte als schreibgeschützt konfiguriert ist.

Hinweis:

1. Wenn ein Benutzer den Datenträger als „Schreibgeschützt“ festgelegt hat, kann der Admin dies durch Einstellen des Datenträgers als „Lesen/Schreiben“ im dmin-Modus überschreiben.
2. Wenn ein Admin den Datenträger als „Schreibgeschützt“ einstellt, kann der Benutzer den Datenträger nicht als „Lesen/Schreiben“ einstellen.

31. Aktivieren des Lese-/Schreibzugriffs im Benutzermodus

Um das datAshur PRO² auf Lesen/Schreiben zu setzen, gehen Sie zunächst wie in Abschnitt 14 beschrieben in den „**Benutzermodus**“. Wenn sich der Datenträger im **Benutzermodus** befindet (GRÜNE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Benutzermodus die Tasten „**7 + 9**“. (7=**R**ead (Lese) + 9=**W**rite (Schreiben))		Statt der durchgehend leuchtenden GRÜNEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und BLAUE LED ändern sich in eine durchgehend leuchtende GRÜNE LED. Dies gibt an, dass die Festplatte als Lesen/Schreiben konfiguriert ist.

Hinweis:

1. Wenn ein Benutzer den Datenträger als „Schreibgeschützt“ festgelegt hat, kann der Admin dies durch Einstellen des Datenträgers als „Lesen/Schreiben“ im Admin-Modus überschreiben.
2. Wenn ein Admin den Datenträger als „Schreibgeschützt“ einstellt, kann der Benutzer den Datenträger nicht als „Lesen/Schreiben“ einstellen.

32. Abwehrmechanismus gegen Brute-Force-Hacker-Angriffe

Das datAshur PRO² beinhaltet einen Abwehrmechanismus zum Schutz der Festplatte gegen Brute-Force-Angriffe. Die Brute-Force-Einschränkung ist für die Admin-PIN und für die User-PIN auf 10 und für die Wiederherstellungs-PIN auf 5 voreingestellt. Es werden drei unabhängige Brute-Force-Zähler verwendet, um die inkorrekten Versuche für jede PIN-Autorisierung zu protokollieren. Gibt ein User eine inkorrekte Admin-PIN 10-mal in Folge (gemäß nachfolgender Beschreibung in 5-, 3-, 2-Cluster aufgeschlüsselt) ein, wird die Festplatte resettet und sämtliche Daten sind für immer verloren. Gibt ein User eine inkorrekte Wiederherstellung-PIN oder User-PIN ein und überschreitet die jeweilige Brute-Force-Einschränkung, werden die entsprechenden PINs gelöscht. Aber die Daten sind weiterhin auf der Festplatte vorhanden.

Anmerkung: Die Brute-Force-Einschränkung ist auf Anfangswerte programmiert, wenn die Festplatte komplett resettet oder die Selbstzerstörungsfunktion aktiviert wurde. Ändert der Admin die User-PIN oder wird bei Aktivierung der Wiederherstellungsfunktion eine neue User-PIN eingerichtet, wird der User-PIN-Brute-Force-Zähler gelöscht. Die Brute-Force-Einschränkung wird jedoch nicht tangiert. Ändert der Admin die Wiederherstellungs-PIN, wird der Brute-Force-Zähler für den Wiederherstellungs-PIN gelöscht.

Durch eine erfolgreiche Autorisierung einer bestimmten PIN wird der Brute-Force-Zähler für diese bestimmte PIN gelöscht. Der Brute-Force-Zähler für die anderen PINs wird jedoch nicht tangiert. Eine fehlgeschlagene Autorisierung einer bestimmten PIN erhöht den Brute-Force-Zähler für diese bestimmte PIN. Der Brute-Force-Zähler für die anderen PINs wird jedoch nicht tangiert.

- Wenn ein Benutzer 10 Mal hintereinander eine falsche Benutzer-PIN eingibt, wird die Benutzer-PIN gelöscht, aber die Daten, die Admin-PIN und die Wiederherstellungs-PIN bleiben intakt und zugänglich.
- Wenn 5 Mal hintereinander eine falsche Wiederherstellungs-PIN eingegeben wird, wird die Wiederherstellungs-PIN gelöscht, aber die Daten und die Admin-PIN bleiben intakt und zugänglich.
- Für die Admin-PIN wird im Vergleich zu den User- und Wiederherstellungs-PINs ein anspruchsvollerer Abwehrmechanismus verwendet. Die Festplatte wird, sofern 5-mal in Folge eine falsche Admin-PIN eingegeben wird, entsprechend gesperrt. Dann sind die LEDs in **ROT**, **GRÜN** und **BLAU** dauerhaft an. An dieser Stelle müssen folgende Schritte durchgeführt werden, damit der User wiederum dreimal eine PIN eingeben kann.

- Bitte die PIN „**47867243**“ eingeben und die Taste **SCHLÜSSEL-Taste (🔑)** betätigen. Die LEDs in GRÜN und BLAU blinken. Die Festplatte akzeptiert jetzt **drei** weitere Eingaben einer Admin-PIN.
- Die Festplatte wird, wird insgesamt 8-mal in Folge eine falsche Admin-PIN eingegeben, gesperrt. Die LEDs in ROT, GRÜN und BLAU blinken dann abwechselnd. An dieser Stelle müssen folgende Schritte durchgeführt werden, damit die letzten 2 PINs (insgesamt 10) eingeben können.
- Bitte die PIN „**47867243**“ eingeben und die Taste **SCHLÜSSEL-Taste (🔑)** betätigen. Die LEDs in GRÜN und BLAU blinken. Die Festplatte akzeptiert jetzt letzten zwei PIN-Eingaben (insgesamt 10).
- Nach insgesamt 10 falschen Admin-PIN-Versuchen wird der Verschlüsselungscode gelöscht. Dann sind sämtliche auf der Festplatte gespeicherten Daten und PINs für immer verloren.

Für die nachfolgende Tabelle wurde angenommen, dass alle drei PINs eingerichtet wurden. Es wird hierbei der Effekt, den Brute-Force-Abwehrmechanismus für jede einzelne PIN anzusteuern, hervorgehoben.

PIN zum Entsperren des Laufwerks	Aufeinanderfolgende falsche PIN-Eingaben (insgesamt)	Beschreibung der Ereignisse
User-PIN	10	• Die User-PIN wird gelöscht. • Die Wiederherstellungs-PIN, die Admin-PIN und alle Daten sind weiterhin intakt und zugänglich.
Wiederherstel-lungs-PIN	5	• Die Wiederherstellungs-PIN wird gelöscht. • Die Admin-PIN und alle Daten sind weiterhin intakt und zugänglich.
Admin-PIN	5 3 2 (10 insgesamt)	• Die Festplatte wird, wird **5**-mal in Folge eine falsche Admin-PIN eingegeben, gesperrt. Dann sind alle LEDs dauerhaft an. • Bitte die PIN „**47867243**“ eingeben und die Taste **SCHLÜSSEL-Taste (🔑)** betätigen, um **3** weitere PINs eingeben zu können. • Die Festplatte wird, wird insgesamt 8-mal (5 + 3) in Folge eine falsche Admin-PIN eingegeben, gesperrt. Die LEDs blinken dann abwechselnd. • Bitte die PIN „**47867243**“ eingeben und die Taste **SCHLÜSSEL-Taste (🔑)** betätigen, um die letzten **2** PINs (10 insgesamt) eingeben zu können. • Nach insgesamt 10 falschen Admin-PIN-Eingaben wird der Verschlüs-selungscode gelöscht.



Wichtig: Eine neue Admin-PIN muss, wenn die bereits vorhandene Admin-PIN brachial geknackt wurde, konfiguriert werden. Siehe Abschnitt 26 über „Wie man eine Admin-PIN nach einem Brute-Force-Angriff oder Reset konfiguriert“. Darüber hinaus muss das datAshur PRO² formatiert werden, bevor der Festplatte neue Daten hinzugefügt werden können.

33. So stellen Sie die Brute-Force-Beschränkung für die Benutzer-PIN ein

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

Die Brute-Force-Beschränkung für die Benutzer-PIN des datAshur PRO² kann vom Administrator vorprogrammiert und eingestellt werden. Diese Funktion kann dafür eingestellt werden, 1 bis 10 Versuche der Eingabe einer falschen PIN zuzulassen.
Um eine Brute-Force-Beschränkung für die Benutzer-PIN zu konfigurieren, rufen Sie zunächst den „**Administratormodus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten **7 + 0** .		Statt der durchgehend leuchtenden BLAUEN LED werden eine zusammen blinkende GRÜNE und BLAUE LED angezeigt.
2. Geben Sie die Anzahl der Versuche für die Brute-Force-Beschränkung ein (von 01 - 10), zum Beispiel: • **01** für 1 Versuch • **10** für 10 Versuche		
3. Drücken Sie einmal die **UMSCHALTTASTE (⬆)**		Die blinkende GRÜNE und BLAU LED werden 1 Sekunde lang zu einer durchgehend leuchtenden GRÜNEN LED und danach zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass die Brute-Force-Beschränkung erfolgreich konfiguriert wurde

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).
Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

34. So prüfen Sie die Brute-Force-Beschränkung für die Benutzer-PIN

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

Um die Einstellung der Brute-Force-Beschränkung zu prüfen, rufen Sie zunächst den „**Administratormodus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **2 + 0** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die „**SCHLÜSSEL-Taste (🔑)**“ und Folgendes geschieht: a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend. b. Jedes ROTE LED-Blinken entspricht zehn (10) Einheiten einer Brute-Force-Beschränkungsanzahl. c. Jedes GRÜNE LED-Blinken entspricht einer (1) einzelnen Einheit einer Brute-Force-Beschränkungsanzahl. d. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend. e. Die LEDs leuchten wieder durchgehend BLAU		

Die nachstehende Tabelle beschreibt das LED-Verhalten bei der Prüfung der Brute-Force-Beschränkungseinstellung. Wenn Sie den Datenträger beispielsweise auf Brute Force nach **5**-maliger aufeinanderfolgender Eingabe einer falschen PIN eingestellt haben, blinkt die GRÜNE LED fünfmal (**5**).

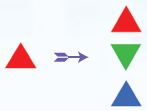
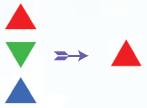
Brute-Force-Beschränkungseinstellung	**ROT**	**GRÜN**
2 Versuche	0	2x Blinken
5 Versuche	0	5x Blinken
10 Versuche	1x Blinken	0

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALT-TASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

35. So führen Sie ein komplettes Zurücksetzen durch

Für komplettes Zurücksetzen muss sich das datAshur PRO² im Standby-Status befinden (ROTE LED leuchtet durchgehend). Wenn der Datenträger zurückgesetzt wird, werden alle Admin-/Benutzer-PINs, der Verschlüsselungsschlüssel und alle Daten gelöscht und sind für immer verloren. Der Datenträger muss formatiert werden, bevor er wieder verwendet werden kann. Um das datAshur PRO² zurückzusetzen, gehen Sie wie folgt vor.

1. Halten Sie im Standby (durchgehend leuchtende ROTE LED) die Taste „**0**“ gedrückt		Statt der durchgehend leuchtenden ROTEN LED blinken alle LEDs, ROT, GRÜN und BLAU, abwechselnd Ein und Aus
2. Halten Sie die Tasten **2 + 7** gedrückt		Die zwischen ROT, GRÜN und BLAU wechselnden LEDs leuchten 1 Sekunde lang durchgehend und werden danach zu einer durchgehend blinkenden ROTEN LED, was angibt, dass der Datenträger zurückgesetzt wurde

Wichtig: Nach dem kompletten Zurücksetzen muss eine neue Admin-PIN konfiguriert werden, siehe Abschnitt 26 auf Seite 22, „So konfigurieren Sie eine Admin-PIN nach einem Brute-Force-Angriff oder dem Zurücksetzen“. Das datAshur PRO² muss zudem formatiert werden, bevor neue Daten zum Datenträger hinzugefügt werden können.

36. So konfigurieren Sie datAshur PRO² als bootfähig

Hinweis: Wenn der Datenträger als bootfähig eingestellt ist, wird durch das Auswerfen des Datenträgers durch das Betriebssystem nicht erzwungen, dass die LED auf ROT wechselt. Der Datenträger bleibt durchgehend GRÜN leuchtend und muss für die nächste Verwendung getrennt werden. Das datAshur PRO² ist standardmäßig als nicht-bootfähig konfiguriert.

Die USB-Datenträger des iStorage datAshur PRO² sind mit einer Funktion Bootfähig ausgestattet, um das Aus- und Wiedereinschalten bei einem Hostbootprozess zu ermöglichen. Beim Booten vom datAshur PRO² aus wird Ihr Computer mit dem auf dem datAshur PRO² installierten Betriebssystem ausgeführt.
Um den Datenträger als bootfähig einzustellen, rufen Sie zunächst den „**Admin-Modus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (⚷) + 8** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie auf **„0“** gefolgt von einer **„1“** (**01**)		Die GRÜNE und BLAUE LED blinken weiter
3. Drücken Sie einmal die **UMSCHALTTASTE (⬆)**		Die blinkende GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass der Datenträger erfolgreich als bootfähig konfiguriert wurde

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).
Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

37. So deaktivieren Sie die Funktion Bootfähig von datAshur PRO²

Um die Funktion Bootfähig des datAshur PRO² zu deaktivieren, gehen Sie zunächst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (⚷) + 8** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie auf **„0“** gefolgt von einer weiteren **„0“** (**00**)		Die GRÜNE und BLAUE LED blinken weiter
3. Drücken Sie einmal die **UMSCHALTTASTE (⬆)**		Die blinkende GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED, was angibt, dass die Funktion Bootfähig erfolgreich deaktiviert wurde

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).

Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALTTASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

38. So prüfen Sie die Bootfähig-Einstellung

Um die Bootfähig-Einstellung zu prüfen, rufen Sie zunächst den „**Administratormodus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE (⬆) + 8** gedrückt.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.

2. Drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**. Daraufhin tritt eines der folgenden zwei Szenarien ein.

- **Wenn das datAshur PRO² als bootfähig konfiguriert ist, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend.
b. Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend.
d. Die LEDs leuchten wieder durchgehend BLAU

- **Wenn das datAshur PRO² <u>NICHT</u> als bootfähig konfiguriert ist, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend.
b. Alle LEDs sind ausgeschaltet
c. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend.
d. Die LEDs leuchten wieder durchgehend BLAU

Hinweis: Wenn sich das datAshur PRO² im Admin-Modus befindet, bleibt die BLAUE LED eingeschaltet und leuchtet nur 30 Sekunden lang durchgehend. Während dieser Zeit kann der Datenträger Anweisungen über die Tastatur annehmen, womit er mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden kann. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt das datAshur PRO² den Admin-Modus automatisch - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt (alle LEDs ausgeschaltet).
Um den Admin-Modus (durchgehend leuchtende BLAUE LED) sofort zu verlassen, drücken und halten Sie die **UMSCHALT-TASTE** (⬆) für 1 Sekunde gedrückt - die durchgehend leuchtende BLAUE LED wird zu einer durchgehend leuchtenden ROTEN LED, die danach langsam in den Leerlauf erlischt. Um auf die Inhalte auf dem Datenträger (Daten) zuzugreifen, muss sich das datAshur PRO² zunächst im Leerlauf befinden (alle LEDs ausgeschaltet), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

39. Formatieren von datAshur PRO² für Windows

Nach einem „Brute-Force-Angriff“ oder dem kompletten Zurücksetzen löscht das datAshur PRO² alle Daten und den Verschlüsselungsschlüssel.
Sie müssen das datAshur PRO² formatieren, bevor es verwendet werden kann.

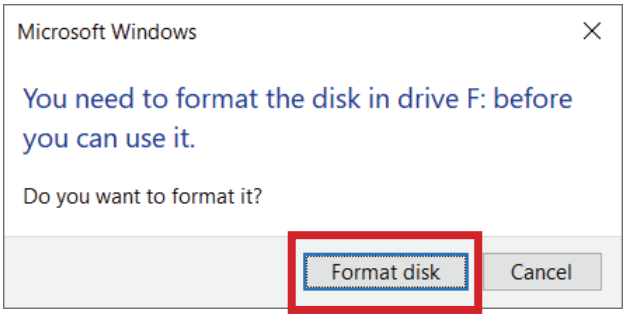
Führen Sie zum Formatieren Ihres datAshur PRO² Folgendes durch:

1. Konfigurieren Sie eine neue Admin-PIN - siehe Seite 22, Abschnitt 26 „So konfigurieren Sie eine Admin-PIN nach einem Brute-Force-Angriff oder dem Zurücksetzen“.

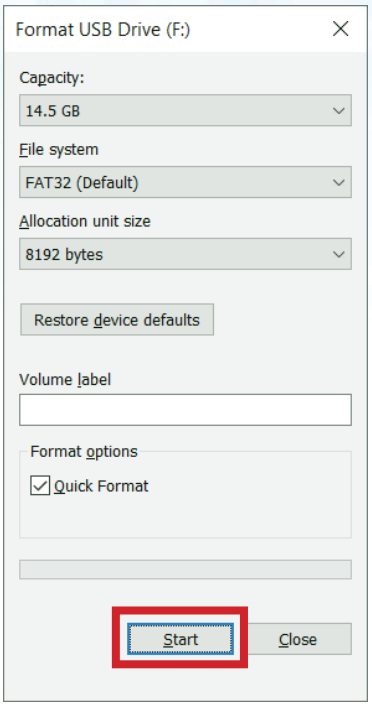
2. Mit dem datAshur PRO² im Standby (ROTE LED) drücken Sie einmal auf die **SCHLÜSSEL-Taste (🔑)** und geben Sie eine **neue Admin-PIN** ein, um zu entsperren (blinkende GRÜNE LED).

3. Schließen Sie das datAshur PRO² an den Computer an.

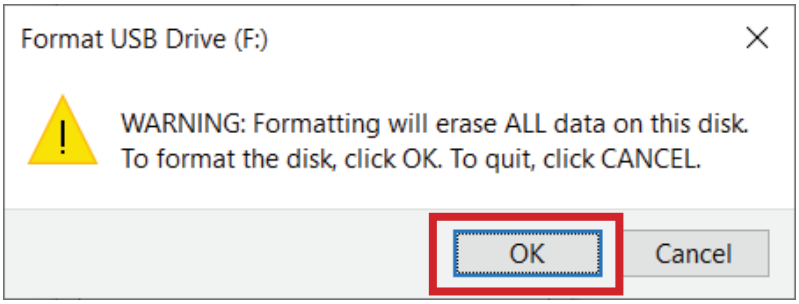
4. Klicken Sie auf „Datenträger formatieren“



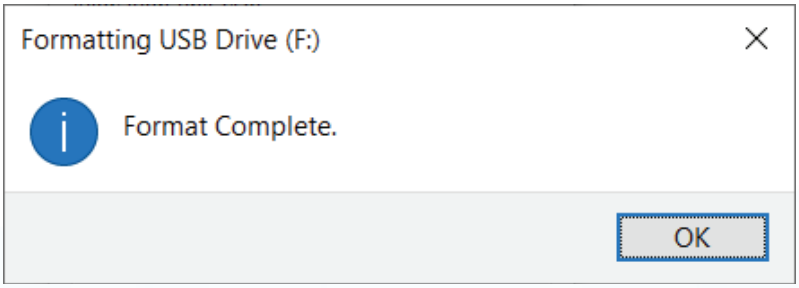
5. Klicken Sie auf „Start“.



6. Klicken Sie auf „OK“.



7. Warten Sie, bis der Formatierungsprozess abgeschlossen ist. Das datAshur PRO² wird erkannt und kann verwendet werden.



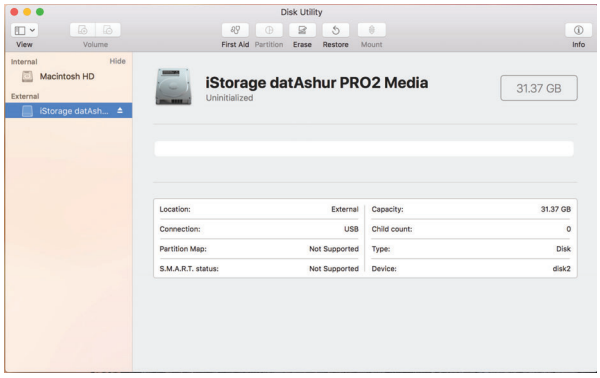
40. datAshur PRO² Setup für Mac OS

Ihr datAshur PRO² ist als exFAT vorformatiert. Um den Datenträger auf ein Mac-kompatibles Format neu zu formatieren, lesen Sie bitte nachfolgend weiter.

Öffnen Sie nach dem Entsperren des Datenträgers das Datenträger-Hilfsprogramm unter Anwendungen/Hilfsprogramme/Datenträger-Hilfsprogramme.

So formatieren Sie das datAshur PRO²:

1. Wählen Sie das datAshur PRO² aus der Liste der Datenträger und Volumes aus. Für die einzelnen Datenträger in der Liste werden dessen Kapazität, Hersteller und Produktname wie „Medium iStorage datAshur PRO²“ oder 232.9 datAshur PRO² angezeigt.



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

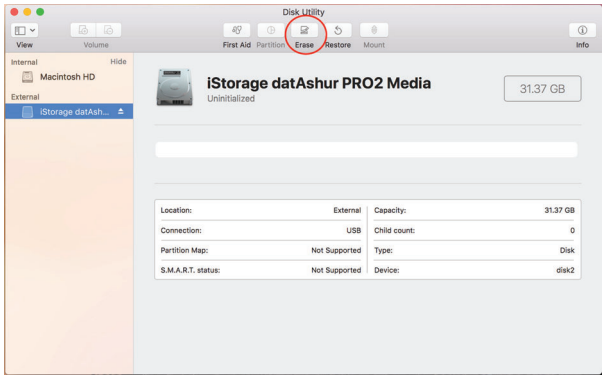


Abbildung 1

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

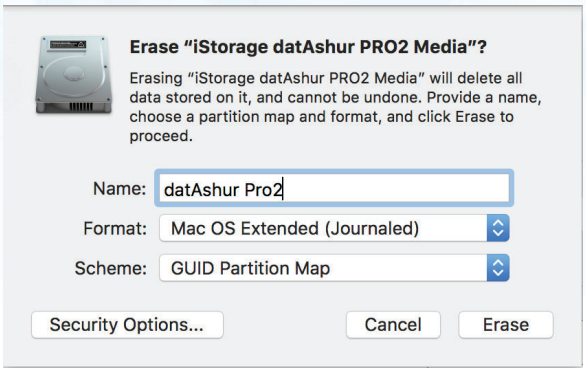


Abbildung 2

4. Wählen Sie ein Schema- und Volume-Format aus. Im Dropdownmenü des Volume-Formats (Abbildung 3) werden die verfügbaren Datenträgerformate angezeigt, die vom Mac unterstützt werden. Der empfohlene Formattyp ist „Mac OS Extended (Journaled)“. Im Dropdownmenü des Schemaformats werden die zur Verwendung verfügbaren Schemata aufgelistet (Abbildung 4).

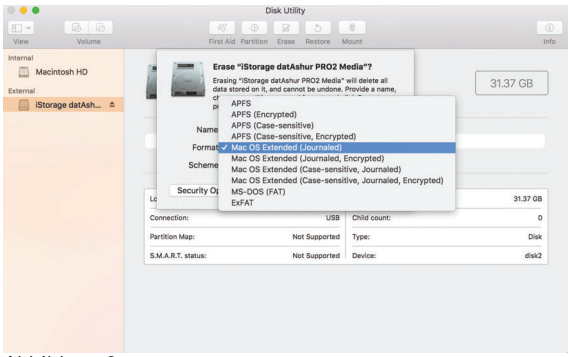


Abbildung 3

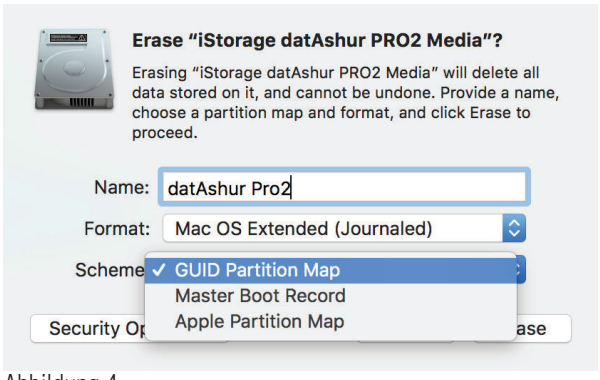


Abbildung 4

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

41. datAshur PRO² Setup für Linux (Ubuntu 18.04 LTS)

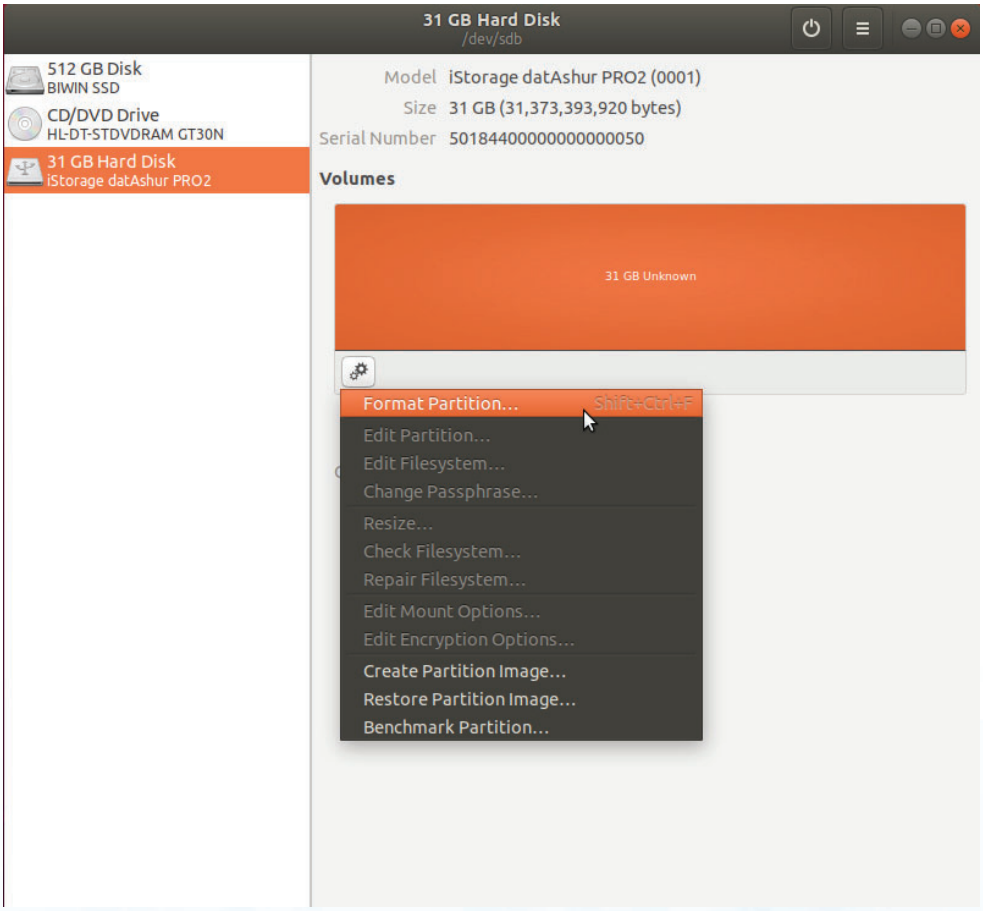
Wenn Ihr datAshur PRO² in NTFS/FAT32/exFAT für Windows initialisiert und formatiert wurde, können Sie den Datenträger direkt in Ubuntu verwenden. Wenn nicht, lesen Sie bitte weiter unten nach.

So formatieren Sie das datAshur PRO² als EXT4 oder andere Dateisysteme:

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

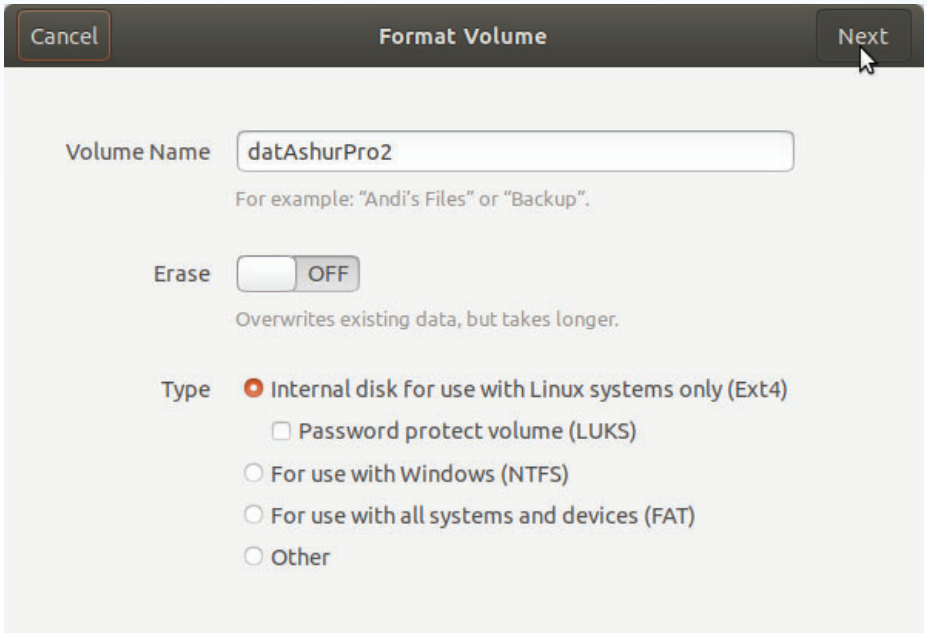


2. Wählen Sie datAshur PRO² unter „Geräte“ aus. Klicken Sie auf das Zahnradsymbol und wählen Sie „Partition formatieren“ aus

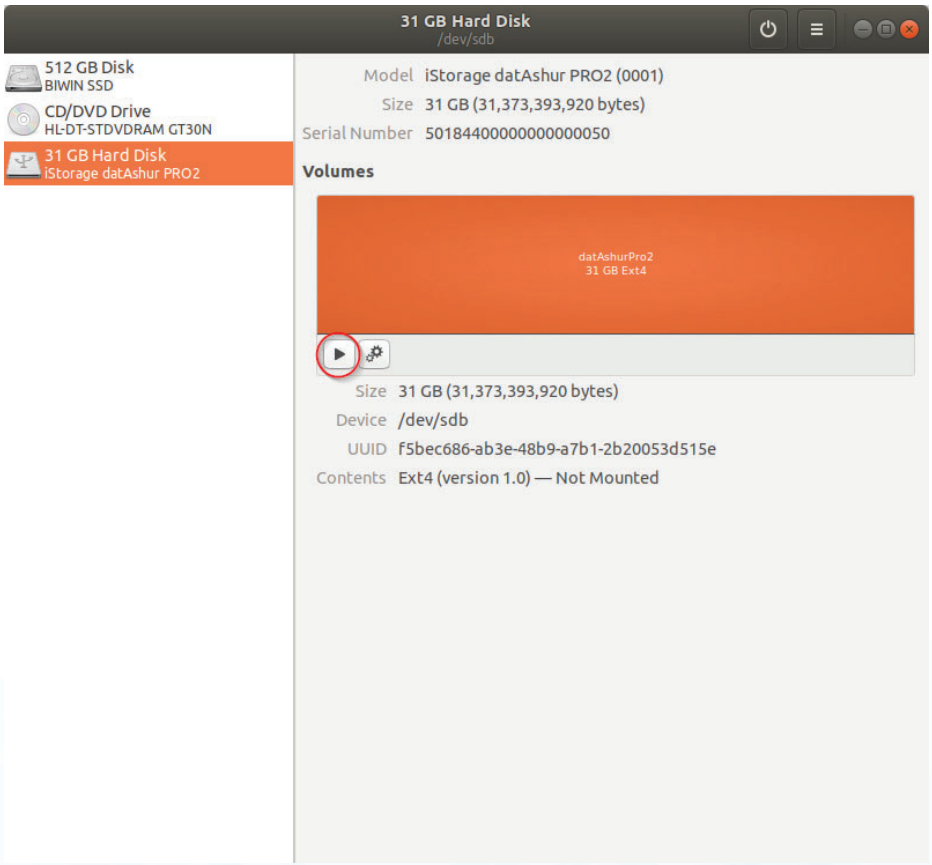


3. Konfigurieren Sie einen Volume-Namen und wählen Sie anschließend die von Ihnen gewünschte Formatierungsart aus.
   EXT4 – kompatibel mit Linux
   NTFS – nur Windows
   FAT – kompatibel mit allen Betriebssystemen

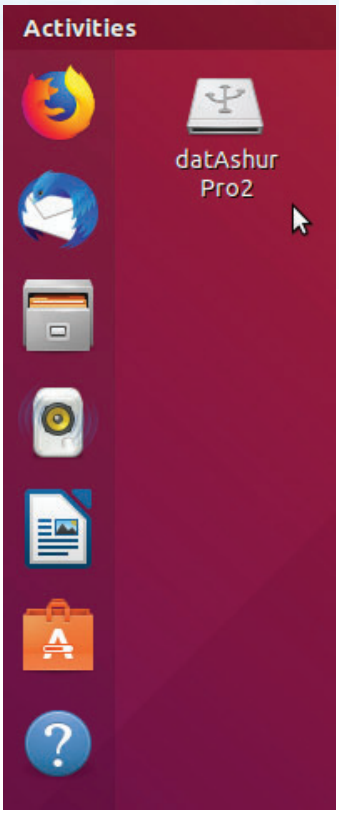
   Und drücken Sie danach auf „Weiter“ und anschließend auf „FORMATIEREN“



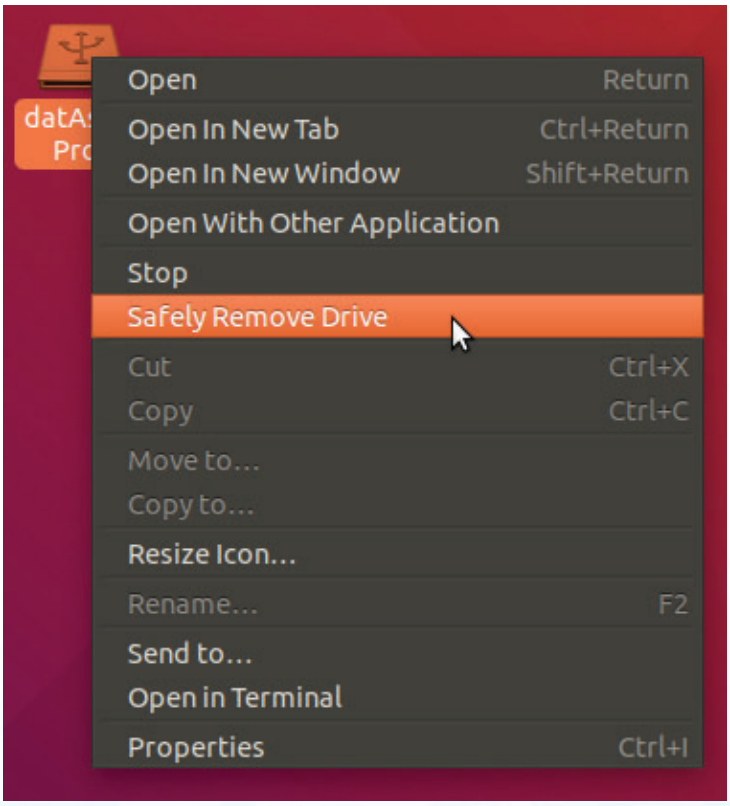
4. Nach Abschluss der Formatierung klicken Sie , um den Datenträger in Ubuntu zu installieren.



5. Es wird ein Datenträgersymbol wie auf der Abbildung unten angezeigt. Sie können auf das Datenträgersymbol klicken, um Ihren Datenträger zu öffnen.



Sperren des datAshur PRO² für Linux (Ubuntu 18.04 LTS)
Es wird dringend empfohlen, mit der rechten Maustaste auf das Symbol Ihres Datenträgers zu klicken und anschließend auf „Sicher entfernen“ im Betriebssystem zu klicken, um Ihr datAshur PRO² auszuwerfen (zu sperren), insbesondere, nachdem Daten auf dem Datenträger kopiert oder gelöscht wurden.



42. Ruhezustand, Anhalten oder Abmelden vom Betriebssystem

Stellen Sie vor dem Ruhezustand, Anhalten oder Abmelden vom Betriebssystem sicher, dass alle Dateien auf Ihrem datAshur PRO² gespeichert und geschlossen werden.

Es wird empfohlen, das datAshur PRO² vor dem Ruhezustand, Anhalten oder Abmelden von Ihrem System manuell zu sperren.

Klicken Sie zum Sperren einfach auf das Symbol „Hardware sicher entfernen/auswerfen“ in Ihrem Betriebssystem und trennen Sie das datAshur PRO².

Achtung: Um die Sicherheit Ihrer Daten sicherzustellen, achten Sie darauf, Ihr datAshur PRO² zu sperren, wenn Sie nicht an Ihrem Computer sind.

43. So prüfen Sie Firmware im Admin-Modus

Um die Firmwareversionsnummer zu prüfen, rufen Sie zunächst den „**Admin-Modus**“ wie in Abschnitt 5 beschrieben auf. Wenn sich der Datenträger im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Drücken und halten Sie im Admin-Modus die Tasten „**3 + 8**“.		Statt der durchgehend leuchtenden BLAUEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.
2. Drücken Sie die „**SCHLÜSSEL-Taste (🔑)**“ einmal und Folgendes geschieht: a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend. b. Die ROTE LED blinkt. Dies gibt den ganzzahligen Teil der Firmware-Versionsnummer an. c. Die GRÜNE LED blinkt. Dies gibt die Dezimalstellen an. d Die BLAUE LED blinkt. Dies gibt die letzte Ziffer der Nummer der Firmwareversion an e. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend. f. Die ROTE, GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden BLAUEN LED		

Wenn die Firmwareversionsnummer beispielsweise „**2.5**“ lautet, blinkt die ROTE LED zweimal (**2**) und die GRÜNE LED blinkt fünf (**5**). Nachdem die Sequenz beendet wurde, blinken die ROTE, GRÜNE und BLAUE LED zusammen einmal und kehren danach in den Admin-Modus zurück, zu einer durchgehend leuchtenden BLAUEN LED.

44. So prüfen Sie Firmware im Benutzermodus

Um die Firmwareversionsnummer zu prüfen, rufen Sie zunächst den „**Benutzermodus**“ wie in Abschnitt 14 beschrieben auf. Wenn sich der Datenträger im **Benutzermodus** befindet (GRÜNE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Benutzermodus die beiden Tasten „**3 + 8**“ gedrückt, bis die GRÜNE und BLAUE LED zusammen blinken.		Statt der durchgehend leuchtenden GRÜNEN LED werden eine blinkende GRÜNE und eine blinkende BLAUE LED angezeigt.

2. Drücken Sie die „**SCHLÜSSEL-Taste (🔑)**“ und Folgendes geschieht:

a. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde durchgehend.
b. Die ROTE LED blinkt. Dies gibt den ganzzahligen Teil der Firmware-Versionsnummer an.
c. Die GRÜNE LED blinkt. Dies gibt die Dezimalstellen an.
d. Die BLAUE LED blinkt. Dies gibt die letzte Ziffer der Nummer der Firmwareversion an
e. Alle LEDs (ROT, GRÜN und BLAU) leuchten 1 Sekunde lang durchgehend.
f. Die ROTE, GRÜNE und BLAUE LED werden zu einer durchgehend leuchtenden BLAUEN LED

Wenn die Firmwareversionsnummer beispielsweise „**2.5**“ lautet, blinkt die ROTE LED zweimal (**2**) und die GRÜNE LED blinkt fünf (**5**). Nachdem die Sequenz beendet wurde, blinken die ROTE, GRÜNE und BLAUE LED zusammen einmal und kehren danach in den Admin-Modus zurück, zu einer durchgehend leuchtenden BLAUEN LED.

45. Technischer Support

iStorage stellt Ihnen die folgenden nützlichen Ressourcen bereit:

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

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

Telefonsupport:
+44 (0) 20 8991-6260.

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

46. Garantie- und RMA-Informationen

HAFTUNGSAUSSCHLUSS UND GARANTIE FÜR PRODUKTE VON ISTORAGE

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

Garantien gelten nicht für Mängel an Produkten, die zurückzuführen sind auf:

- normale Abnutzung und Verschleiß,
- vorsätzliche Beschädigung, unsachgemäße Lager- oder Einsatzsbedingungen, Unfall, Fahrlässigkeit durch Sie oder Dritte,
- unsachgemäße Bedienung oder Nutzung der Produkte durch Sie oder Dritte entgegen der Benutzeranweisungen,
- jegliche Änderung oder Reparatur durch Sie oder Dritte, die nicht zu unseren autorisierten Reparaturbetrieben gehören, oder
- jegliche von Ihnen bereitgestellte Spezifikation.

Im Rahmen dieser Garantien reparieren, ersetzen oder erstatten wir nach eigenem Ermessen jedes Produkt, bei dem Materialfehler festgestellt wurden, sofern Sie bei der Lieferung:

- die Produkte geprüft haben, um festzustellen, ob sie Materialfehler aufweisen, und
- Sie den Verschlüsselungsmechanismus der Produkte getestet haben.

Wir haften nur für Materialfehler oder Mängel am Verschlüsselungsmechanismus der Produkte, die durch Prüfung bei Lieferung festgestellt und uns innerhalb von 30 Tagen nach Lieferung mitgeteilt werden. Sofern Materialfehler oder Mängel am Verschlüsselungsmechanismus nicht durch Prüfung der Produkte bei Lieferung festgestellt wurden, haften wir nur für Mängel, die Sie uns innerhalb von 7 Tagen mitteilen, nachdem Sie sie entdeckt haben oder hätten erkennen müssen. Wir haften im Rahmen dieser Garantie nicht, wenn Sie oder andere Personen die Produkte nach Feststellung eines Mangels weiter verwenden. Wenn Sie einen Mangel feststellen, senden Sie das defekte Produkt bitte an uns zurück. Wenn Sie ein Unternehmen sind, tragen Sie die Transportkosten für die Rücksendung von Produkten oder Produktteilen an uns im Rahmen der Garantie; wir tragen alle Transportkosten für das Versenden von reparierten oder ersetzten Produkten an Sie. Wenn Sie privater Verbraucher sind, lesen Sie bitte unsere Allgemeinen Geschäftsbedingungen.

Zurückgesandte Produkte müssen in Originalverpackung und in sauberem Zustand sein. Anderenfalls werden zurückgesandte Produkte nach Ermessen des Unternehmens entweder abgelehnt oder für entstehende Kosten zusätzliche Gebühren berechnet. Wenn Produkte im Rahmen der Garantie zur Reparatur zurückgesandt werden, müssen Kopien der Originalrechnungen beigelegt oder die Originalrechnungsnummer mit Kaufdatum angegeben werden.

Wenn Sie privater Verbraucher sind, gilt diese Garantie zusätzlich zu Ihren gesetzlichen Rechten für Produkte, die fehlerhaft oder nicht wie beschrieben sind. Informationen zu diesen Rechten erhalten Sie von Ihrer örtlichen Beratungsstelle für Privatverbraucher.

Die in dieser Klausel aufgeführten Garantien gelten nur für Erstkäufer, von iStorage autorisierte Wiederverkäufer oder Händler der Produkte von iStorage. Diese Garantien sind nicht übertragbar.

MIT AUSNAHME DER HIER GEWÄHRTEN BESCHRÄNKTEN GARANTIE UND IM GESETZLICH ZULÄSSIGEN UMFANG LEHNT ISTORAGE ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN AB, EINSCHLIEßLICH DER MARKTGÄNGIGKEIT, EIGNUNG FÜR BESTIMMTE ZWECKE UND NICHTVERLETZUNG. ISTORAGE GARANTIERT NICHT, DASS DAS PRODUKT FEHLERFREI FUNKTIONIERT. SOWEIT IMPLIZITE GARANTIEN GESETZLICH ZULÄSSIG SIND, SIND DIESE AUF DIE DAUER IHRER GÜLTIGKEIT BESCHRÄNKT. IHR RECHT UMFASST AUSSCHLIEßLICH REPARATUR ODER ERSATZ DES PRODUKTS WIE HIER ANGEGEBEN.

IN KEINEM FALL HAFTET ISTORAGE FÜR VERLUSTE, ERWARTETE GEWINNE ODER ZUFÄLLIGE, STRAFRECHTLICHE, BEISPIELHAFTE, SPEZIELLE, VERTRAUENS- ODER FOLGESCHÄDEN, U. A. EINSCHLIEßLICH ENTGANGENER UMSÄTZE, GEWINNE, NUTZUNGSVERLUSTE FÜR SOFTWARE, DATENVERLUSTE, SONSTIGE VERLUSTE ODER WIEDERHERSTELLUNG VON DATEN, SACHSCHÄDEN UND ANSPRÜCHE DRITTER, DIE SICH AUS EINER WIEDERHERSTELLUNG THEORETISCH ERGEBEN, EINSCHLIEßLICH GARANTIEN, VERTRÄGEN, UNGESETZLICHEN ODER UNERLAUBTEN HANDLUNGEN, UNABHÄNGIG DAVON, OB AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE. UNGEACHTET DER LAUFZEIT EINER BESCHRÄNKTEN GARANTIE ODER EINER GESETZLICH FESTGELEGTEN GARANTIE, ODER FALLS EINE BESCHRÄNKTE GARANTIE IHREN HAUPTZWECK VERFEHLT, ÜBERSTEIGT DIE GESAMTE HAFTUNG VON ISTORAGE IN KEINEM FALL DEN KAUFPREIS DES PRODUKTS. | 4823-2548-5683.3

Copyright © iStorage Limited 2019. 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

Manuel d'utilisation



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

Si vous rencontrez des difficultés pour utiliser la clé datAshur PRO2, merci de contacter notre équipe d'assistance par courriel à l'adresse support@istorage-uk.com ou par téléphone au +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2019. 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, DONT TOUTE
GARANTIE IMPLICITE DE QUALITÉ MARCHANDE, D'ADÉQUATION À UN USAGE
DONNÉ OU DE NON-TRANSGRESSION, SONT DÉNIÉES, SOUS RÉSERVE QUE CES DÉNIS DE RESPONSABILITÉ NE SOIENT PAS LÉGALEMENT TENUS POUR NULS.

RoHS Compliant

REACH COMPLIANCE

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

Conforme au Trade Agreements Act (TAA)

Table des matières

Introduction 87
Contenu de la boîte 87
1. Indicateurs LED et leur signification 88
2. États de la batterie et des LED 88
3. Première utilisation 89
4. Déverrouillage de la datAshur PRO² à l'aide du code PIN administrateur 90
5. Pour passer en mode administrateur 91
6. Pour quitter le mode administrateur 91
7. Modifier le code PIN administrateur 92
8. Définir une politique de code PIN utilisateur 93
9. Comment supprimer la politique de code PIN utilisateur 94
10. Comment vérifier la politique de code PIN utilisateur 95
11. Ajouter un nouveau code PIN utilisateur en mode administrateur 96
12. Modifier le code PIN utilisateur en mode administrateur 97
13. Supprimer le code PIN utilisateur en mode administrateur 97
14. Comment déverrouiller la datAshur PRO² avec le code PIN utilisateur 98
15. Modifier le code PIN utilisateur en mode utilisateur 98
16. Créer un code PIN utilisateur de récupération à usage unique 99
17. Supprimer le code PIN utilisateur de récupération à usage unique 99
18. Activer le mode récupération et créer un nouveau code PIN utilisateur 100
19. Définir le mode lecture seule pour l'utilisateur en mode administrateur 100
20. Activer le mode lecture/écriture pour l'utilisateur en mode administrateur 101
21. Définir le mode lecture seule globale en mode administrateur 102
22. Activer le mode lecture/écriture globale en mode administrateur 102
23. Comment configurer un code PIN d'autodestruction 103
24. Comment supprimer le code PIN d'autodestruction 104
25. Comment déverrouiller avec le code PIN d'autodestruction 104
26. Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation 105
27. Définir la minuterie de verrouillage automatique en cas de non-utilisation 105
28. Désactiver la minuterie de verrouillage automatique en cas de non-utilisation 106
29. Comment vérifier la minuterie de verrouillage automatique en cas de non-utilisation 107
30. Définir le mode lecture seule en mode utilisateur 107
31. Activer le mode lecture/écriture en mode utilisateur 108
32. Mécanisme de défense contre les tentatives de piratage par force brute 108
33. Comment définir la limite d'attaque par force brute du code PIN utilisateur 110
34. Comment vérifier la limite d'attaque par force brute du code PIN utilisateur 111
35. Comment effectuer une réinitialisation complète 112
36. Comment configurer la datAshur PRO² comme une clé bootable 112
37. Comment désactiver la fonctionnalité bootable de la datAshur PRO² 113
38. Comment vérifier le paramètre clé bootable 113
39. Formater la datAshur PRO² pour Windows 114
40. Configuration de la datAshur PRO² pour Mac OS 116
41. Configuration de la datAshur PRO² pour Linux (Ubuntu 18.04 LTS) 118
42. Mettre en veille prolongée, suspendre ou se déconnecter du système d'exploitation 121
43. Comment vérifier la version du firmware en mode administrateur 121
44. Comment vérifier la version du firmware en mode utilisateur 122
45. Assistance technique 123
46. Informations de garantie et de renvoi de matériel 123

Introduction

Remarque : La batterie rechargeable de la datAshur PRO² ne sera pas entièrement chargée. Nous recommandons de charger la batterie avant la première utilisation. Veuillez brancher la datAshur PRO² à un port USB alimenté pendant 30-60 minutes pour charger totalement la batterie.

Merci d'avoir acheté la datAshur® PRO² d'iStorage, une clé USB 3.2 Gen 1 avec authentification par code PIN ultra-sécurisée et facile d'utilisation, avec chiffrement matériel, et capacité allant jusqu'à 512 Go et au-delà.

La datAshur PRO² contient une batterie rechargeable qui permet à l'utilisateur de saisir un code PIN (numéro d'identification personnel) de 7 à 15 chiffres sur le clavier intégré afin de déverrouiller la clé avant de connecter celle-ci à un port USB. Pour verrouiller la clé et chiffrer toutes les données, déconnectez simplement la datAshur PRO² de l'ordinateur hôte et l'intégralité du contenu de la clé sera chiffré à l'aide d'un chiffrement matériel AES-XTS 256 bits de classe militaire. Si la clé est perdue ou volée et que le code PIN est saisi 10 fois consécutives de manière incorrecte (paramètre par défaut), le mécanisme de défense de la datAshur PRO² sera activé afin de la protéger contre tout accès non autorisé.

La datAshur PRO² peut être configurée avec des codes PIN utilisateur et administrateur et peut également être programmée de manière à ajouter un « Code PIN de récupération », ce qui en fait une solution idéale pour le déploiement dans un contexte d'entreprise ou gouvernemental. La datAshur PRO² étant déverrouillée à l'aide du clavier intégré, et non d'un ordinateur hôte, elle n'est pas vulnérable contre les attaques par force brute ou 'keyloggers' logiciels/matériels.

L'une des fonctionnalités de sécurité fondamentales et uniques de la datAshur PRO² qui est conforme au règlement général sur la protection des données (RGPD) est le microprocesseur matériel sécurisé et dédié (conforme aux critères communs EAL4+) équipé de mécanismes de protection physiques intégrés conçus pour protéger contre les altérations externes, les attaques par contournement et les injections d'erreurs. Contrairement à d'autres solutions, la datAshur PRO² réagit aux attaques automatisées en entrant dans un état de blocage, qui rend toutes ces attaques inutiles. Autrement dit, sans le code PIN, il est impossible de se connecter !

Contenu de la boîte

- iStorage datAshur PRO²
- Etui en aluminium extrudé
- GDR - Guide de démarrage rapide

1. Les indicateurs LED et leur signification

LED	État de la LED	Description	LED	État de la LED	Description
▲	ROUGE continue	Périphérique verrouillé (à l'état de **Veille** ou de **Réinitialisation**)	▲▼▲	ROUGE, VERTE et BLEUE clignotantes	En attente de saisie du code PIN **utilisateur**
▲	ROUGE - s'affaiblit graduellement	Le périphérique s'éteint et passe à **l'état Inactif**	▼▲	VERTE et BLEUE clignotent simultanément	En attente de saisie du code PIN **administrateur**
▼	VERTE clignotante	**Périphérique déverrouillé** en tant qu'**administrateur** (non connecté au port USB)	▼▲	VERTE et BLEUE clignotent alternativement	Authentification en cours
▼	VERTE continue	**Périphérique déverrouillé** en tant qu'**utilisateur** (non connecté au port USB) ou périphérique en mode utilisateur	▲	BLEUE clignotante toutes les 5 secondes	La batterie commence à se charger au bout de 30 secondes lorsque le périphérique est verrouillé et relié à un port USB
▲	BLEUE continue	Périphérique en **mode administrateur**			

2. États de la batterie et des LED

Remarque : Le fonctionnement normal de la datAshur PRO² peut être perturbé par les interférences électromagnétiques intenses. Si tel est le cas, éteignez puis rallumez le produit afin de rétablir le fonctionnement normal. Si le fonctionnement normal n'est pas rétabli, veuillez utiliser le produit à un endroit différent.

Capteur de batterie faible

La datAshur PRO² comprend un circuit de détection de la tension qui analyse la tension en sortie de batterie lorsque l'appareil est allumé. Lorsque la tension de la batterie chute pour atteindre 3,3 V ou moins, la LED ROUGE s'affiche trois fois et s'éteint. Dans cette situation, l'utilisateur devrait connecter la datAshur PRO² à un port USB alimenté et la charger pendant 15-30 minutes. Une fois rechargée, la datAshur PRO² reprendra son fonctionnement normal.

Pour se réveiller de l'état Inactif

La datAshur PRO² est à l'état inactif lorsqu'elle n'est pas en cours d'utilisation et que toutes les LED sont éteintes. Pour réveiller la datAshur PRO² de l'état Inactif, procédez comme suit.

Appuyez et maintenez enfoncée la touche **Maj** (⬆) pendant une seconde pour connecter le périphérique à un port USB alimenté	▲ ▼ ▲	Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, et cède la place à une LED ROUGE continue, ce qui indique que l'appareil est en mode Veille

Pour passer à l'état Inactif

Pour forcer la datAshur PRO² à passer à l'état Inactif, exécutez l'une des opérations suivantes :

- Si l'appareil est connecté à un port USB, déconnectez-le.
- Si l'appareil n'est pas connecté à un port USB, appuyez et maintenez enfoncée la touche **Maj** (⬆) pendant une seconde jusqu'à ce que la LED passe en ROUGE continu et s'éteigne en passant en mode inactif (éteint).

Remarque : Lorsque la datAshur PRO² est déverrouillée et n'est pas connectée à un port USB et qu'aucune opéra-tion n'est effectuée dans un délai de 30 secondes, l'appareil passera automatiquement à l'état Inactif. La LED passe en ROUGE continu, puis s'éteint et passe en mode Inactif.

Lorsque la datAshur PRO² est connectée à un port USB, la touche **Maj** (⬆) ne fonctionne pas.
Lorsqu'elle est connecté à un port USB alimenté, une datAshur PRO² commence à se charger au bout de 30 secondes, ce qui est indiqué par la LED BLEUE qui clignote toutes les 5 secondes.

États sous tension
Lorsque l'appareil sort de l'état Inactif, il passe à l'un des états suivants présentés dans le tableau ci-dessous.

État sous tension	Indication de la LED	Clé de chif-frement	Code PIN Administrateur	Description
Veille	ROUGE continue	✓	✓	En attente de saisie du code PIN administrateur ou utilisateur
Réinitialiser	ROUGE continue	×	×	Attente de configuration d'un code PIN administrateur
Niveau de batterie faible	ROUGE clignote 3 fois	✓	✓	Charger sur un port USB alimenté pendant 15-30 minutes
État d'expédition initial	ROUGE et VERTE continues	✓	×	Attente de configuration d'un code PIN administrateur

3. Première utilisation

La datAshur PRO² est fournie à l'**« état d'expédition initial » sans code PIN administrateur prédéfini**. Un code PIN administrateur de 7 à 15 chiffres peut être configuré avant que la clé ne puisse être utilisée. Une fois qu'un code PIN administrateur a été configuré correctement, il n'est plus possible de rétablir la clé à son « état d'expédition d'origine »

Exigences pour le code PIN :

- Doit comprendre de 7 à 15 chiffres
- Ne doit contenir aucune répétition de chiffre, par ex. (3-3-3-3-3-3-3)
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

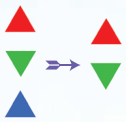
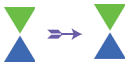
Conseil pour le mot de passe : Pour votre code PIN, vous pouvez créer une phrase, un nom ou un mot mémorables, ou toute autre combinaison alphanumérique en appuyant simplement sur les touches indiquant les lettres correspondantes.

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 « **iStorage** » vous appuieriez sur :
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

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

Pour configurer un code PIN administrateur et déverrouiller la datAshur PRO² pour la première fois, veuillez suivre les étapes simples décrites dans le tableau ci-dessous.

Instructions (première utilisation)	LED	État de la LED
1. Appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde.		Les LED ROUGE, VERTE et BLEUE clignotent une fois l'une après l'autre, puis la LED VERTE clignote deux fois, et cède la place aux LED ROUGE et VERTE continues, ce qui indique que le lecteur est à l'état d'expédition initial
2. Appuyez sur les touches **CLÉ (🔑) + 1** et maintenez-les enfoncées.		Les LED sont remplacées par les LED VERTE clignotante et BLEUE continue.
3. Saisissez votre **nouveau code PIN** administrateur et appuyez une fois sur la touche **CLÉ (🔑) .**		Les LED VERTE clignotante et BLEUE continue sont remplacées par un clignotement rapide de la LED VERTE, puis repassent en mode LED VERTE clignotante et BLEUE continue.
4. Saisissez à nouveau votre **nouveau code PIN** administrateur et appuyez à nouveau sur la touche **CLÉ (🔑).**		La LED BLEUE clignote rapidement avant de céder la place à la LED BLEUE continue, puis est finalement remplacée par une LED VERTE clignotante, ce qui indique que le code PIN administrateur a été correctement configuré et la clé déverrouillée

Remarque : : Une fois que la datAshur PRO² a bien été déverrouillée, la LED VERTE reste allumée pendant seulement 30 secondes, pendant lesquelles la datAshur PRO² doit être connectée à un port USB alimenté. Elle peut être verrouillé immédiatement (si elle n'est pas connectée à un port USB) en appuyant et en maintenant enfoncée la touche **Maj** (⬆) pendant une seconde ou en cliquant sur l'icône « Retirer/éjecter le matériel en toute sécurité » de votre système d'exploitation lorsqu'il est connecté à un port USB.

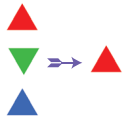
Une fois la datAshur PRO² déverrouillée et connectée à un port USB, elle n'accepte plus d'instructions via le clavier.

Verrouiller le datAshur PRO²

Pour verrouiller la clé, éjectez en toute sécurité la datAshur PRO2 de votre système d'exploitation hôte, puis débranchez-la du port USB. Si des données sont en cours d'écriture sur la clé, le fait de débrancher la datAshur PRO2 se soldera par un transfert de données incomplet et entraînera potentiellement une corruption de données..

4. Déverrouillage de la datAshur PRO² à l'aide du code PIN administrateur

Pour déverrouiller la datAshur PRO² avec le code PIN administrateur, veuillez suivre les simples étapes présentées dans le tableau ci-dessous.

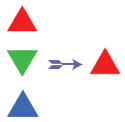
1. Appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde.		Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, et cède la place à une LED ROUGE continue, ce qui indique que le lecteur est en mode Veille
2. En état de veille (LED ROUGE continue), appuyez une fois sur la touche **CLÉ (🔑)**.		Les LED de couleur VERTE et BLEUE se mettent à clignoter simultanément.
3. Alors que les LED de couleur VERTE et BLEUE clignotent simultanément, saisissez le **code PIN administrateur** et appuyez à nouveau sur la touche **CLÉ (🔑)**.		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, qui indique que la clé a été déverrouillée en tant qu'administrateur.

Remarque : : Une fois que la datAshur PRO² a bien été déverrouillée, la LED VERTE reste allumée pendant seulement 30 secondes, pendant lesquelles la datAshur PRO² doit être connectée à un port USB alimenté. Elle peut être verrouilleé immédiatement (si elle n'est pas connectée à un port USB) en appuyant et en maintenant enfoncée la touche **Maj** (⬆) pendant une seconde ou en cliquant sur l'icône « Retirer/éjecter le matériel en toute sécurité » de votre système d'exploitation lorsqu'il est connecté à un port USB.

Une fois la datAshur PRO² déverrouillée et connectée à un port USB, elle n'accepte plus d'instructions via le clavier.

5. Pour accéder au mode administrateur

Pour accéder au mode administrateur, effectuez les étapes suivantes :

1. Appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde.		Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, et cède la place à une LED ROUGE continue, ce qui indique que l'appareil est en mode Veille
2. En état de veille (LED ROUGE continue), appuyez une fois sur la touche **CLÉ (🔑)**.		Les LED de couleur VERTE et BLEUE se mettent à clignoter simultanément.
3. Alors que les LED de couleur VERTE et BLEUE clignotent simultanément, saisissez le **code PIN administrateur** et appuyez à nouveau sur la touche **CLÉ (🔑)**.		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, ce qui indique que l'appareil est déverrouillé
4. Appuyez sur la touche **CLÉ (🔑) trois** fois en l'espace de 2 secondes **CLÉ (🔑) x 3**		La LED VERTE clignotante est remplacée par une LED BLEUE continue, ce qui indique que l'appareil est en mode administrateur

6. Pour quitter le mode administrateur

Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur - la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

7. Modifier le code PIN administrateur

Exigences pour le code PIN :

- Doit comprendre de 7 à 15 chiffres
- Ne peut contenir qu'une répétition de chiffres, par ex. (3-3-3-3-3-3-3)
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

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

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 « **iStorage** » vous appuieriez sur :
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

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

Pour modifier le code PIN administrateur, 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 les touches **CLÉ (🔑) + 2** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue.
2. Saisissez votre **NOUVEAU code PIN administrateur** et appuyez une fois sur la touche **CLÉ (🔑)**.		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 la touche **CLÉ (🔑)**		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.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

8. Définir une politique 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 ou plusieurs « **caractères spéciaux** ». Le « caractère spécial » fonctionne comme une pression simultanée sur les deux touches « **Maj** (⬆) + **chiffre** ».

Pour définir une politique (restrictions) en matière de code PIN utilisateur, vous devez saisir 3 chiffres, par exemple « **091** », les deux premiers chiffres (**09**) indiquent la longueur minimale du code PIN (dans ce cas, **9**) et le dernier chiffre (**1**) indique qu'un « caractère spécial » doit être utilisé, en d'autres termes « **Maj** (⬆) + **chiffre**. » De même, 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 configuré - voir section 11 « Ajouter un nouveau code PIN utilisateur en mode administrateur ». Si l'administrateur configure le code PIN utilisateur « **247688314** » avec l'utilisation d'un « **caractère spécial** » (**Maj** (⬆) + **chiffre** en même temps), 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. '**Maj** (⬆) **+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',

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

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

Remarque :

- Si un « caractère spécial » a été utilisé durant la configuration du code PIN utilisateur, par exemple, l'exemple « **B** » ci-dessus, cette clé ne peut être déverrouillée qu'en saisissant le code PIN avec le « caractère spécial » précisément dans l'ordre configuré soit, dans l'exemple « **B** » ci-dessus - (« 2 », « 4 », « **Maj** (⬆) **+ 7** » , « 6 », « 8 », « 8 », « 3 », « 1 », « 4 »).
- Plus d'un « caractère spécial » peut être utilisé à n'importe quel emplacement dans votre code PIN de 7 à 15 chiffres
- 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 administrateur comporte 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 la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches **CLÉ (🔑) + 7** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
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.		Les LED VERTE et BLEUE clignotantes continueront de clignoter
3. Appuyez une fois sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE continue, puis une LED BLEUE continue, indiquant que la politique en matière de code PIN utilisateur a été correctement définie.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

9. Comment supprimer la politique de code PIN utilisateur

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

1. En mode administrateur, appuyez sur les touches **CLÉ (🔑) + 7** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez **070** et appuyez une fois sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE continue, puis une LED BLEUE continue, indiquant que la politique de code PIN utilisateur a été correctement supprimée.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

10. 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 spécial a été définie ou non en notant la séquence de LED décrite ci-dessous.

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

1. En mode administrateur, appuyez sur les touches **Maj** (⬆) **+ 7** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche « **CLÉ** (🔑) » et vous observerez ce qui suit : a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. b. Un clignotement de la LED ROUGE est égal à dix (10) unités d'un code PIN. c. Chaque clignotement de la LED VERTE est égal à une (1) unité d'un code PIN. d. Un clignotement BLEU indique l'utilisation d'un caractère spécial. e. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. 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 (**121**), la LED ROUGE clignotera une fois (**1**) et la LED VERTE clignotera deux fois (**2**), suivie d'un seul (**1**) clignotement de la LED BLEUE 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

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

11. Ajouter un nouveau code PIN utilisateur en mode administrateur

Important : La création d'un nouveau code PIN utilisateur doit se conformer à la « Politique de code PIN utilisateur », si cette dernière a été configurée tel que décrit dans la section 8, qui impose une longueur minimale du code PIN et spécifie si un caractère spécial doit être utilisé. Reportez-vous à la section 10 pour vérifier les restrictions en matière de code PIN utilisateur.

Exigences pour le code PIN :

- Doit comprendre de 7 à 15 chiffres
- Ne doit contenir aucune répétition de chiffre, par ex. (3-3-3-3-3-3-3)
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- La touche **Maj** (⬆) peut être utilisée pour d'autres combinaisons de PIN - par ex. **Maj** (⬆) **+ 1** produit une valeur différente de 1. Voir la section 8. « Définir une politique de code PIN utilisateur »

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

1. En mode administrateur appuyez sur les touches **CLÉ (🔑) + 3** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue
2. Saisissez le **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)**.		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. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez à nouveau sur la touche **CLÉ (🔑)**.		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 utilisateur a été correctement configuré.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

12. Modifier le code PIN utilisateur en mode administrateur

Important : La modification du code PIN utilisateur doit se conformer à la « Politique de code PIN utilisateur », si cette dernière a été configurée tel que décrit dans la section 8, qui impose une longueur minimale du code PIN et spécifie si un caractère spécial doit être utilisé. Reportez-vous à la section 10 pour vérifier les restrictions en matière de code PIN utilisateur.

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

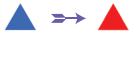
1. En mode administrateur, appuyez sur les touches **CLÉ (🔑) + 3** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue
2. Saisissez le **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)**.		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE continue.
3. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez à nouveau sur la touche **CLÉ (🔑)**.		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui se met à clignoter rapidement avant d'être continue et BLEUE, indiquant que le code PIN utilisateur a été correctement modifié.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

13. Supprimer le code PIN utilisateur en mode administrateur

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

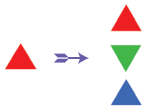
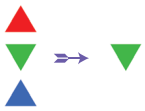
1. En mode administrateur, appuyez sur les touches **Maj** (⬆) **+ 3** et maintenez-les enfoncées.		La LED BLEUE continue est remplacée par la LED ROUGE clignotante.
2. Appuyez sur les touches **Maj** (⬆) **+ 3** et maintenez-les enfoncées.		La LED ROUGE clignotante est remplacée par la LED ROUGE continue, puis par la LED BLEUE continue, indiquant que le code PIN utilisateur a été correctement supprimé.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

14. Comment déverrouiller la datAshur PRO² avec le code PIN utilisateur

Pour déverrouiller à l'aide du **code PIN utilisateur**, le datAshur PRO² doit d'abord être en mode Veille (LED ROUGE continue) en appuyant sur la touche **Maj** (⬆) pendant une seconde.

1. En état de veille (LED ROUGE continue), appuyez sur les touches **Maj** (⬆) **+ CLÉ** (⚷) et maintenez-les enfoncées		La LED ROUGE est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter.
2. Saisissez le **code PIN utilisateur** et appuyez sur la touche **CLÉ** (⚷).		Les LED ROUGE, VERTE et BLEUE clignotantes seront remplacées par des LED VERTE et BLEUE en alternance, puis par une LED VERTE continue qui indique un déverrouillage réussi du lecteur en mode Utilisateur.

15. Modifier le code PIN utilisateur en mode utilisateur

Pour modifier le **code PIN utilisateur**, déverrouillez d'abord le datAshur PRO² avec un code PIN utilisateur tel que décrit dans la section 14. Une fois que la clé est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

1. En mode utilisateur, appuyez sur les touches **CLÉ** (⚷) **+ 4** et maintenez-les enfoncées		La LED VERTE continue est remplacée par les LED VERTE clignotante et BLEUE continue.
2. Saisissez le **nouveau code PIN utilisateur** et appuyez sur la touche « **CLÉ** (⚷) ».		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. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez sur la touche « **CLÉ** (⚷) ».		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui se met à clignoter rapidement avant d'être continue, indiquant une modification réussie du code PIN utilisateur.

Important : La modification du code PIN utilisateur doit se conformer à la « Politique de code PIN utilisateur », si cette dernière a été configurée tel que décrit dans la section 8, et qui impose une longueur minimale du code PIN et spécifie si un caractère spécial doit être utilisé. L'administrateur peut se reporter à la section 10 pour vérifier les restrictions en matière de code PIN utilisateur.

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

Le code PIN de récupération utilisateur est extrêmement utile dans les situations où un utilisateur a oublié son code PIN, afin de déverrouiller le datAshur PRO².
Pour activer le mode récupération, l'utilisateur doit d'abord saisir le code PIN de récupération à usage unique, si ce dernier a été configuré. Le processus de récupération du code PIN n'affecte pas les données, la clé de chiffrement et le code PIN administrateur. Cependant, l'utilisateur est contraint de configurer un nouveau code PIN utilisateur de 7 à 15 chiffres.
Pour configurer un code PIN utilisateur de récupération à usage unique de 7 à 15 chiffres, accédez d'abord au **« mode administrateur »** tel que décrit dans la section 5. Une fois que la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches **CLÉ (⚷) + 4** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue
2. Saisissez **un code PIN de récupération à usage unique** et appuyez sur la touche **CLÉ (⚷)**.		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. Saisissez à nouveau **un code PIN de récupération à usage unique** et appuyez à nouveau sur la touche **CLÉ (⚷)**		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui se met à clignoter rapidement avant d'être continue en BLEU indiquant que le code PIN de récupération à usage unique a été correctement configuré.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

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

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

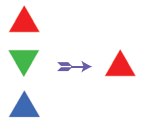
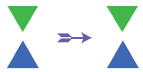
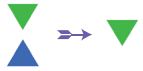
1. En mode administrateur, appuyez sur les touches **Maj** (⬆) **+ 4** et maintenez-les enfoncées.		La LED BLEUE continue est remplacée par la LED ROUGE clignotante.
2. Appuyez sur les touches **Maj** (⬆) **+ 4** et maintenez-les enfoncées.		La LED ROUGE clignotante s'allumera en ROUGE continu, puis sera remplacée par une LED BLEUE continue, ce qui indique que le code PIN utilisateur de récupération à usage unique a été supprimé avec succès

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

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

Le code PIN de récupération utilisateur est extrêmement utile dans les situations où un utilisateur a oublié son code PIN, afin de déverrouiller la datAshur PRO².
Pour activer le mode récupération, l'utilisateur doit d'abord saisir le code PIN de récupération à usage unique, si ce dernier a été configuré. Le processus de récupération du code PIN n'affecte pas les données, la clé de chiffrement et le code PIN administrateur. Cependant, l'utilisateur est contraint de configurer un nouveau code PIN utilisateur de 7 à 15 chiffres.
Pour activer le processus de récupération et configurer un nouveau code PIN utilisateur, effectuez les étapes suivantes :

1. Lorsque la clé est à l'**état Inactif**, appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde		Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, et cède la place à une LED ROUGE continue, ce qui indique que la clé est en mode Veille
2. En **mode Veille**, appuyez sur les touches **CLÉ (🔑) + 4** et maintenez-les enfoncées		La LED ROUGE continue est remplacée par les LED ROUGE et VERTE clignotantes
3. Saisissez le **code PIN de récupération** à usage unique et appuyez sur la touche **CLÉ (🔑)**.		Les LED VERTE et BLEUE clignotent en alternance, puis sont remplacées par une LED VERTE continue, puis par les LED VERTE clignotante et BLEUE continue.
4. Saisissez le **Nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)**		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.
5. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez à nouveau sur la touche **CLÉ (🔑)**		La LED VERTE clignote rapidement, puis devient VERTE continue, ce qui indique que le processus de récupération est réussi et qu'un nouveau code PIN utilisateur a été configuré

Important : La création d'un nouveau code PIN utilisateur doit se conformer à la « Politique de code PIN utilisateur »,si une telle politique a été configurée, tel que décrit dans la section 8, qui impose une longueur minimale du code PIN et spécifie si un caractère spécial doit être utilisé. Reportez-vous à la section 10 pour vérifier les restrictions en matière de code PIN utilisateur.

19. Définir le mode de lecture seule en mode administrateur

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

Lorsque l'administrateur configure la datAshur PRO² et limite l'accès utilisateur au mode Lecture seule, seul l'administrateur peut écrire sur la clé ou rétablir le paramètre en Lecture/écriture, tel que décrit dans la section 20. L'utilisateur est limité à un accès en Lecture seule et ne peut pas écrire sur la clé ni modifier ce paramètre en mode utilisateur.

Pour configurer la datAshur PRO² en mode lecture seule pour l'accès utilisateur, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. Une fois que la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches « **7 + 6** » et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ (⚷)**		Les LED VERTE et BLEUE sont remplacées par une LED VERTE continue, puis par une LED BLEUE continue, ce qui indique que la clé a été configurée et limite l'accès utilisateur en Lecture seule

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

20. Activer le mode lecture/écriture en mode administrateur

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

1. En mode administrateur, appuyez sur les touches « **7 + 9** » et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ (⚷)**		Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue, puis par la LED BLEUE continue, indiquant que le lecteur est configuré en mode lecture/écriture.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

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

Lorsque l'administrateur configure la datAshur PRO² et la configure en mode Lecture seule global, ni l'administrateur ni l'utilisateur ne peuvent écrire sur la clé et tous deux sont limités à un accès en lecture seule. Seul l'administrateur peut modifier ce paramètre et le rétablir en mode Lecture/écriture, tel que décrit dans la section 22.

Pour configurer la datAshur PRO² en mode lecture seule global, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. Une fois que la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

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

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

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

Pour configurer la datAshur PRO² en mode lecture/écriture depuis le paramètre Lecture seule global, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. Une fois que la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches « **5 + 9** » et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ (⚷)**		Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue, puis par la LED BLEUE continue, indiquant que la clé est configurée en mode lecture/écriture.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

23. Comment configurer un code PIN d'autodestruction

Vous pouvez configurer un code PIN d'autodestruction qui, une fois saisi, réalise un effacement cryptographique de la clé (la clé de déchiffrement est effacée). Ce processus supprime tous les codes PIN configurés et rend toutes les données stockées sur la clé inaccessibles (perdues à tout jamais). La clé apparaîtra alors comme déverrouillée (LED VERTE). Activer cette fonctionnalité définit le code PIN d'autodestruction comme le nouveau code PIN utilisateur, et la clé devra être formatée avant de pouvoir être réutilisée.

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

1. En mode administrateur, appuyez sur les touches **CLÉ (🔑) + 6** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE clignotante et BLEUE continue.
2. Configurez un **code PIN d'autodestruction** de 7 à 15 chiffres et appuyez sur la touche « **CLÉ (🔑)** ».		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. Saisissez à nouveau le **code PIN d'autodestruction** et appuyez sur la touche **CLÉ (🔑)**		La LED VERTE clignote rapidement pendant plusieurs secondes, puis est remplacée par la LED BLEUE continue, ce qui indique que le code PIN d'autodestruction a été correctement configuré.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

24. 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 la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches **Maj + 6** et maintenez-les enfoncées.		La LED BLEUE continue est remplacée par la LED ROUGE clignotante.
2. Appuyez à nouveau sur les touches « **Maj + 6** » et maintenez-les enfoncées.		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.

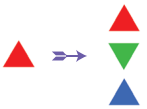
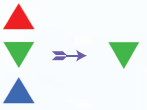
Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

25. Comment déverrouiller avec le code PIN d'autodestruction

Avertissement : 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. La datAshur PRO² doit d'abord être réinitialisée (voir la section 35 « Comment effectuer une réinitialisation complète » à la page 28) afin de configurer un code PIN administrateur avec les pleins privilèges administrateur, notamment la possibilité de configurer un code PIN utilisateur.

Lorsqu'il est utilisé, le code PIN d'autodestruction supprime TOUTES les données, les codes PIN administrateur/utilisateur, et déverrouille le lecteur.
Activer cette fonctionnalité définit le code PIN d'autodestruction comme le nouveau code PIN utilisateur, et la datAshur PRO 2 doit être formatée avant que toute nouvelle donnée puisse être ajoutée sur la clé.
Pour activer le mécanisme d'autodestruction, la clé doit être en état de veille (LED ROUGE continue), puis effectuez les étapes suivantes.

1. En état de Veille (LED ROUGE continue), appuyez sur les touches **Maj** (⬆) **+ CLÉ (⚷)** et maintenez-les enfoncées		La LED ROUGE est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter.
2. Saisissez le **code PIN d'autodestruction** et appuyez sur la touche « **CLÉ (⚷)** ».		Les LED ROUGE, VERTE et BLEUE clignotantes sont remplacées par les LED VERTE et BLEUE qui s'allument en alternance pendant quelques secondes, avant de céder la place à la LED VERTE, ce qui indique que la datAshur PRO² s'est autodétruit avec succès.

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

Après une attaque par force brute ou quand la datAshur PRO² a été réinitialisée, vous devez configurer un code PIN administrateur avant de pouvoir utiliser la clé.

Exigences pour le code PIN :

- Doit comprendre de 7 à 15 chiffres
- Ne doit contenir aucune répétition de chiffre, par ex. (3-3-3-3-3-3-3)
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Si la datAshur PRO² a été attaquée par force brute ou réinitialisé, la clé se met en état de veille (LED ROUGE continue). Pour configurer un PIN administrateur, effectuez les étapes suivantes.

1. En mode Veille (LED ROUGE continue), appuyez sur les touches « **Maj** (⬆) **+ 1** » et maintenez-les enfoncées.		La LED ROUGE continue est remplacée par les LED VERTE clignotante et BLEUE continue.
2. Saisissez le **nouveau code PIN administrateur** et appuyez une fois sur la touche **CLÉ (🔑)**.		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. Saisissez à nouveau le **nouveau code PIN administrateur** et appuyez sur la touche « **CLÉ (🔑)** ».		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.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

27. Définir la minuterie de verrouillage automatique en cas de non-utilisation

Pour protéger la clé contre les accès non autorisés si elle est déverrouillée et laissée sans surveillance, il est possible de configurer la datAshur PRO² de façon à ce qu'elle se verrouille automatiquement au bout d'un intervalle prédéfini.

Dans son état par défaut, la fonctionnalité de verrouillage automatique pour non-utilisation de la datAshur PRO² est désactivée. Le verrouillage automatique en cas de non-utilisation peut être défini de façon à se déclencher au bout de 5 à 99 minutes.

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

1. En mode administrateur, appuyez sur les touches **CLÉ (⚷) + 5** et maintenez-les enfoncées		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 : **05 pour 5 minutes (appuyez sur « 0 », suivi d'un « 5 »)** **20 pour 20 minutes (appuyez sur « 2 » suivi de « 0 »)** **99 pour 99 minutes (appuyez sur « 9 » suivi d'un autre « 9 »)**		
3. Appuyez sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE continue pendant une seconde, puis enfin p ar la LED BLEUE continue, indiquant que le délai du verrouillage automatique a été correctement configuré.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

28. Désactiver la minuterie de verrouillage automatique en cas de non-utilisation

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

1. En mode administrateur, appuyez sur les touches **CLÉ (⚷) + 5** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez « **00** » et appuyez sur la touche « **Maj** (⬆) ».		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.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

29. Comment vérifier la minuterie de verrouillage automatique en cas de non-utilisation

L'administrateur est en mesure de vérifier et de déterminer la durée définie pour la minuterie de verrouillage automatique en cas de non-utilisation en notant simplement la séquence des LED décrite dans le tableau en bas de cette page.
Pour vérifier le verrouillage automatique en cas de non-utilisation, accédez d'abord au « **mode administrateur** » tel que décrit dans la section 5. Une fois que la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

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

Le tableau ci-dessous décrit le comportement des LED lorsque vous vérifiez la minuterie de verrouillage automatique en cas de non-utilisation, par exemple si vous avez programmé la clé pour se verrouiller automatiquement au bout de **25** minutes, la LED ROUGE clignotera deux (**2**) fois et la LED VERTE clignotera cinq (**5**) fois.

Verrouillage automatique en minutes	ROUGE	VERT
5 minutes	0	5 clignotements
15 minutes	1 clignotement	5 clignotements
25 minutes	2 clignotements	5 clignotements
40 minutes	4 clignotements	0

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

30. Définir le mode de lecture seule en mode utilisateur

Pour configurer la datAshur PRO² en mode lecture seule, accédez d'abord au **mode utilisateur** tel que décrit dans la section 14. Une fois que la clé est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

1. En mode utilisateur, appuyez sur les touches « **7 + 6** » et maintenez-les enfoncées (7 = **R**ead (lecture) + 6 = **O**nly (seule))		La LED VERTE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur **CLÉ** (🔑)		Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue? indiquant que la clé est configurée en mode lecture seule.

Remarque : 1. Si un utilisateur configure la clé en mode lecture seule, l'administrateur peut passer outre en paramétrant la clé en lecture/écriture en mode administrateur.
2. Si l'administrateur configure la clé en mode lecture seule, l'utilisateur ne peut pas configurer la clé en mode lecture/écriture.

31. Activer le mode lecture/écriture en mode utilisateur

Pour configurer la datAshur PRO² en mode lecture/écriture, accédez d'abord au **mode utilisateur** tel que décrit dans la section 14. Une fois que la clé est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches « **7 + 9** » et maintenez-les enfoncées (7 = **R**ead (lecture) + 9 = **W**rite (écriture))		La LED VERTE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ** (🔑)		Les LED VERTE et BLEUE sont remplacées par la LED VERTE continue, indiquant que la clé est configuré en mode lecture/écriture.

Remarque : 1. Si un utilisateur configure la clé en mode lecture seule, l'administrateur peut passer outre en paramétrant la clé en lecture/écriture en mode administrateur.
2. Si l'administrateur configure la clé en mode lecture seule, l'utilisateur ne peut pas configurer la clé en mode lecture/écriture.

32. Mécanisme de défense contre les tentatives de piratage par la force brute

La datAshur PRO² intègre un mécanisme de défense visant à protéger la clé contre les attaques par force brute. Par défaut, les valeurs de l'état d'expédition initial pour la limite d'attaque par force brute utilisateur sont fixées à 10 essais pour le code PIN administrateur et le code PIN utilisateur et 5 essais pour le code PIN de récuperation. Trois compteurs d'attaques par force brute indépendants sont utilisés pour enregistrer le nombre de tentatives infructueuses pour chaque validation de code PIN. Si un code PIN administrateur incorrect est saisi 10 fois consécutivement (décomposé en 3 groupes de 5, 3 et 2 essais comme décrit ci-dessous), la clé sera réinitialisée et toutes les données seront perdues à jamais. Si un utilisateur saisit un code PIN de récuperation ou un code PIN utilisateur incorrect qui excède le nombre d'essais de leur compteur respectif, les codes PIN correspondants seront supprimés mais les données restent intactes.

Remarque : La limite d'attaque par force brute est définie par défaut sur les valeurs de l'état d'expédition initial lorsque la clé est complètement réinitialisée ou que la fonctionnalité d'autodestruction est active. Si l'administrateur modifie le code PIN utilisateur ou qu'un nouveau code PIN utilisateur est configuré lors de l'activation de la fonctionnalité de récupération, le compteur d'attaque par force brute du code PIN utilisateur est remis à zéro (0), mais la limite d'attaque par force brute n'est pas affectée. Si l'administrateur modifie le code PIN de récupération, le compteur d'attaques par force brute du code PIN de récupération est remis à zéro.

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

- Si un utilisateur saisit un code PIN **utilisateur** incorrect 10 fois consécutives, le code PIN utilisateur sera supprimé mais les données, le code PIN administrateur et le code PIN de récupération resteront intacts et accessibles.
- Si un code **PIN de récupération incorrect** est saisi 5 fois consécutives, le code PIN de récupération est supprimé mais les données et le code PIN admin restent intacts et accessibles.
- Le code PIN Administrateur du datAshur PRO² est équipé d'un mécanisme de défense plus sophistiqué que le code PIN utilisateur ou de récupération. Après 5 saisies d'un code PIN Administrateur invalide, la clé se verrouillera, et toutes les LED, ROUGE, VERTE & BLEUE s'allumeront et resteront allumées. Référez-vous aux instructions ci-dessous pour disposer de 3 essais supplémentaires de code PIN Administrateur.

- Saisissez le code PIN « **47867243** » puis appuyez sur le bouton **CLÉ (⚷)** une fois. les LED VERTE et BLEUE clignotent chacune leur tour, la clé est alors prête à accepter **3** nouveaux essais de code PIN Administrateur.
- Au bout de 8 essais invalides du code PIN Administrateur, la clé se verrouillera et toutes les LED ROUGE, VERTE & BLEUE clignoteront en alternance. Référez-vous ensuite aux instructions ci-dessous pour disposer de **2** essais supplémentaires de code PIN Administrateur (10 en tout).
- Saisissez le code PIN « **47867243** » puis appuyez sur le bouton **CLÉ (⚷)** une fois. les LED VERTE et BLEUE clignotent chacune leur tour, la clé est alors prête à accepter 2 derniers essais de code PIN Administrateur (10 en tout).
- Au bout de 10 saisies de code PIN administrateur invalide, la clé de chiffrement, tous les codes PIN ainsi que toutes les données seront supprimés et définitivement perdus.

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

Code PIN utilisé pour déverrouiller la clé	Saisies consécutives de code PIN erroné (au total)	Description de ce qui se produit
Code PIN Utilisateur	10	• Le code PIN Utilisateur est supprimé. • Les codes PIN de récupération et Administrateur restent intactes et accessibles.
Code PIN de Récupération	5	• Le code PIN de récupération est supprimé. • Le code PIN Administrateur et toutes les données restent intactes et accessibles.
Code PIN Administrateur	5 3 2 (10 au total)	• Au bout de **5** saisies consécutives de code PIN Administrateur erroné, la clé se verrouillera, et toutes les LED, ROUGE, VERTE & BLEUE s'allumeront et resteront allumées. • Saisissez le code PIN « **47867243** » puis appuyez sur le bouton **CLÉ (⚷)** une fois pour disposer de **3** saisies de code supplémentaires. • Au bout de **8** (5+3) saisies consecutives de code PIN Administrateur invalide, la clé se verrouillera, et toutes les LED cligneront en alternance. • Saisissez le code PIN « **47867243** » puis appuyez sur le bouton **CLÉ (⚷)** une fois pour disposer de **2** dernières saisies de code PIN (10 au total). • Au bout de 10 saisies consecutives de code PIN Administrateur invalide, la clé de chiffrement, tous les codes PIN ainsi que toutes les données seront supprimés et définitivement perdus.

Important: Un nouveau code PIN Administrateur doit être configuré enc as d'attaque par force brute d'un code PIN Administrateur pré-existant. Consultez la section 26 pour 'Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation', la datAshur PRO² devra être également formatée avant de stocker toutes données sur la clé.

33. Comment définir la limite d'attaque par force brute du code PIN utilisateur

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

La limite d'attaque par force brute du code PIN utilisateur de la datAshur PRO² peut être reprogrammée et définie par l'administrateur. Cette fonctionnalité peut être configurée de manière à permettre de 1 à 10 tentatives de saisie de code PIN erroné.

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

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

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur - la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

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

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

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

1. En mode administrateur, appuyez sur les touches **2** + **0** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche « **CLÉ (🔑)** » et vous observerez ce qui suit : a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. b. Chaque clignotement de la LED ROUGE est égal à dix (10) unités d'un chiffre de limite d'attaque par force brute. c. Chaque clignotement de la LED VERTE est égal à une (1) unité d'un chiffre de limite d'attaque par force brute. d. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. e. Les LED reviennent au BLEU continu.		

Le tableau ci-dessous décrit le comportement des LED lorsque vous vérifiez la limite d'attaque par force brute, par exemple si vous avez programmé la clé pour détecter une attaque par force brute au bout de **5** saisies consécutives d'un code PIN erroné, la LED VERTE clignotera cinq (**5**) fois.

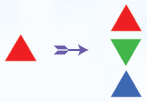
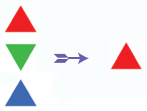
Paramètre de limite d'attaque par force brute	ROUGE	VERT
2 tentatives	0	2 clignotements
5 tentatives	0	5 clignotements
10 tentatives	1 clignotement	0

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

35. Comment effectuer une réinitialisation complète

Pour effectuer une réinitialisation complète, la datAshur PRO² doit être en état de veille (LED ROUGE continue). Une fois que la clé est réinitialisée, tous les codes PIN administrateur/utilisateur, la clé de chiffrement et toutes les données sont supprimés et perdus à jamais, et la clé doit être formatée avant de pouvoir être réutilisée. Pour réinitialiser la datAshur PRO², effectuez les étapes suivantes.

1. En mode veille (LED ROUGE continue), appuyez sur la touche "**0**" et maintenez-le enfoncé		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 touches **2 + 7** et maintenez-les enfoncées.		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 la clé a été réinitialisée.

Important: après une réinitialisation complète, un nouveau code PIN administrateur doit être configuré : consultez la section 26 de la page 22 intitulée « Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation », la datAshur PRO² doit aussi être formatée avant que toute nouvelle donnée puisse être ajoutée à la clé.

36. Comment configurer la datAshur PRO² comme une clé bootable

Remarque : Lorsque la clé est définié comme bootable, l'éjection de la clé du système d'exploitation ne forcera pas la LED à passer au ROUGE. La clé conserve la LED VERTE continue et doit être débranchée pour être réutilisée. Le paramètre par défaut de la datAshur PRO² est configuré comme non bootable.

Les clés USB datAshur PRO² d'iStorage sont équipées d'une fonctionnalité « clé bootable » qui permet la mise hors tension durant un processus de démarrage de l'hôte. Lorsque vous exécutez le démarrage à partir de la datAshur PRO², vous faites fonctionner votre ordinateur avec le système d'exploitation installé sur la datAshur PRO².

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

1. En mode administrateur, appuyez sur les touches **CLÉ (🔑) + 8** et maintenez-les enfoncées.		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur **« 0 »** suivi d'un **« 1 »** (**01**)		Les LED VERTE et BLEUE continueront de clignoter
3. Appuyez une fois sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE continue, puis une LED BLEUE continue, indiquant que la fonctionnalité clé bootable a été configurée avec succès.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

37. Comment désactiver la fonctionnalité bootable de la datAshur PRO²

Pour désactiver la fonctionnalité clé bootable de la datAshur PRO², accédez d'abord au **« mode administrateur »** tel que décrit dans la section 5. Une fois que la clé est en **mode administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode administrateur, appuyez sur les touches **CLÉ (⚷) + 8** et maintenez-les enfoncées.		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur **« 0 »** suivi d'un autre **« 0 »** (**00**)		Les LED VERTE et BLEUE continueront de clignoter
3. Appuyez une fois sur la touche **Maj** (⬆)		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE continue, puis une LED BLEUE continue, indiquant que la fonctionnalité clé bootable a été désactivée avec succès.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

38. Comment vérifier le paramètre clé bootable

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

1. En mode administrateur appuyez, sur les touches **Maj** (⬆) **+ 8** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.

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

- **Si la datAshur PRO² est configurée comme bootable, vous observerez ce qui suit :**
  a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
  b. La LED VERTE clignote une fois.
  c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
  d. Les LED reviennent au BLEU continu.

- **Si la datAshur PRO² n'est <u>PAS</u> configurée comme bootable, vous observerez ce qui suit :**
  a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
  b. Toutes les LED s'éteignent
  c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
  d. Les LED reviennent au BLEU continu.

Remarque : Lorsque la datAshur PRO² est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles la clé peut accepter des instructions via le clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, la datAshur PRO² quitte automatiquement le mode administrateur la LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez la enfoncée pendant une seconde - La LED BLEUE continue est remplacée par une LED ROUGE continue qui s'éteint ensuite et passe en mode Inactif. Pour accéder au contenu de la clé (données), la datAshur PRO² doit d'abord être en état Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

39. Formater la datAshur PRO² pour Windows

Après une « attaque par force brute » ou une réinitialisation complète de la datAshur PRO², toutes les données et la clé de chiffrement sont supprimés.
Vous devez formater la datAshur PRO² avant de pouvoir l'utiliser.

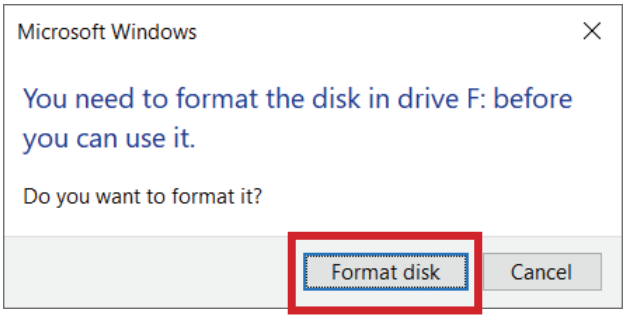
Pour formater votre datAshur PRO², effectuez les étapes suivantes :

1. Configurez un nouveau code PIN administrateur : voir page 22, section 26 « Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation ».

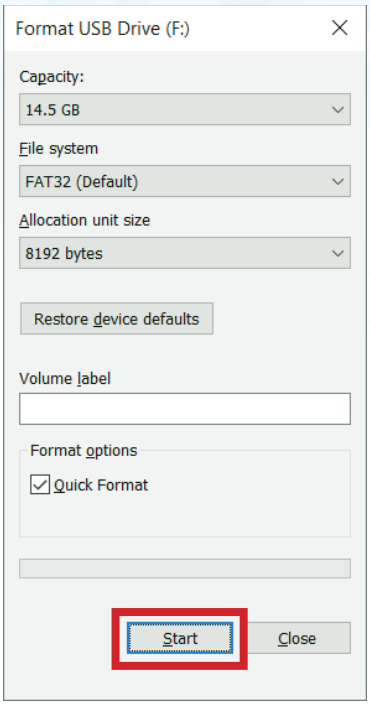
2. Lorsque la datAshur PRO² est en état de veille (LED ROUGE), appuyez une fois sur la touche **CLÉ (🔑)** et saisissez le **nouveau code PIN administrateur** pour le déverrouiller (LED VERTE clignotante).

3. Connectez la datAshur PRO² à l'ordinateur.

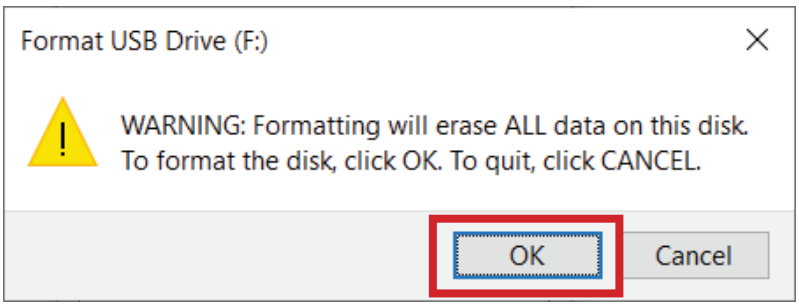
4. Cliquez sur « Formater le disque »



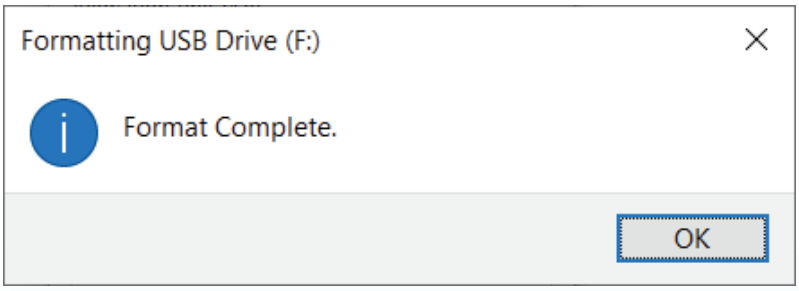
5. Cliquez sur « Commencer ».



6. Cliquez sur « OK ».



7. Patientez jusqu'à la fin du formatage. La datAshur PRO² est reconnue et peut être utilisée.



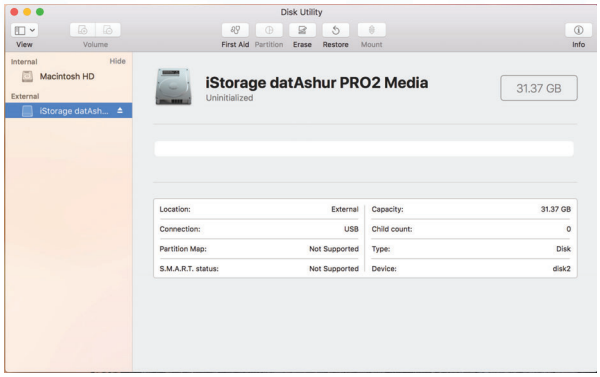
40. Configuration de la datAshur PRO² pour Mac OS

Votre datAshur PRO² est préformatée au format exFAT. Pour reformater la clé en un format compatible Mac, lisez les informations ci-dessous.

Une fois que la clé est déverrouillée, ouvrez Utilitaire de disque dans Applications/Utilitaires/Utilitaires de disque.

Pour formater la datAshur PRO² :

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



2. Cliquez sur la touche « Effacer » (figure 1).

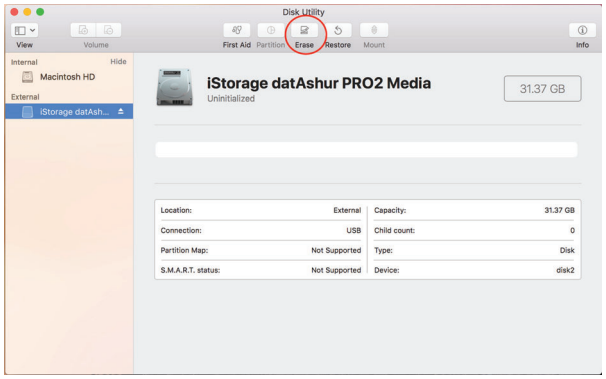


figure 1

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

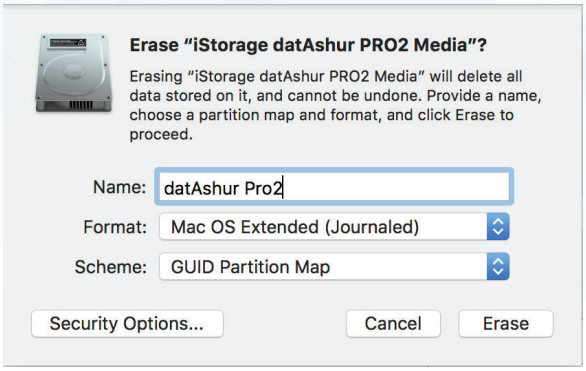


figure 2

4. Sélectionnez un format de modèle et de volume à utiliser. Le menu déroulant Volume Format (Format du volume) (figure 3) répertorie les formats de disque pris en charge par le Mac. Le type de format recommandé est « Mac OS Extended (Journaled) ». Le menu déroulant Scheme format (format du système) répertorie les systèmes disponibles à l'utilisation (figure 4).

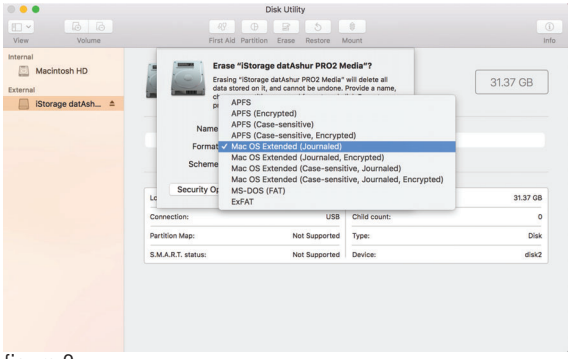


figure 3

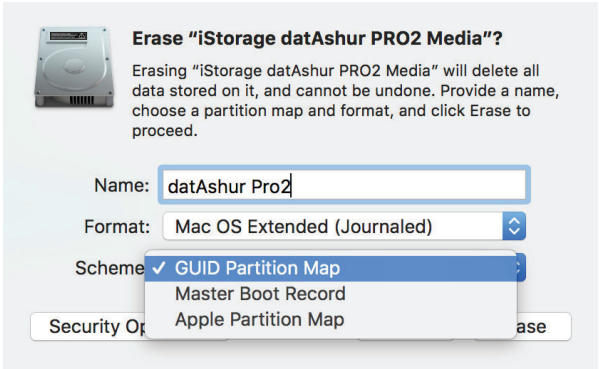


figure 4

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

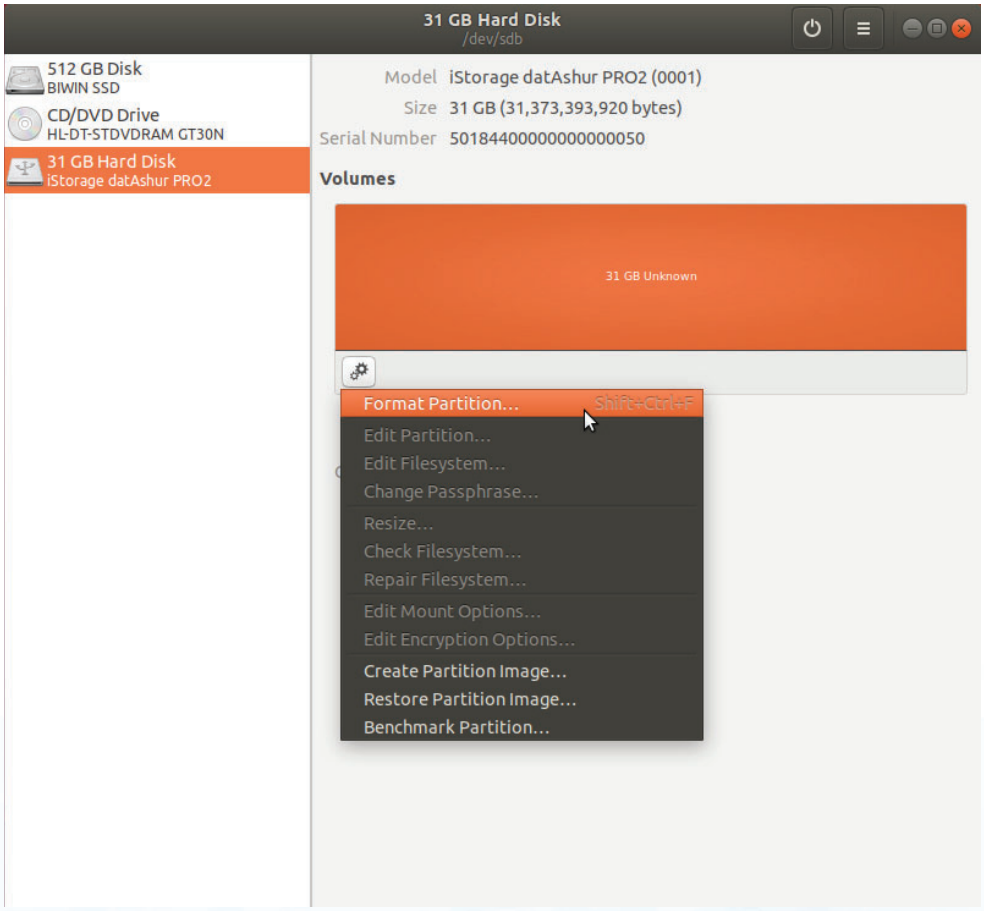
41. Configuration de la datAshur PRO² pour Linux (Ubuntu 18.04 LTS)

Si votre datAshur PRO² a été initialisée et formatée en NTFS/FAT32/exFAT pour Windows, vous pouvez utiliser directement la clé dans Ubuntu. Dans le cas contraire, veuillez lire les instructions ci-dessous.
Pour formater la datAshur PRO² au format EXT4 ou autre système de fichier :

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

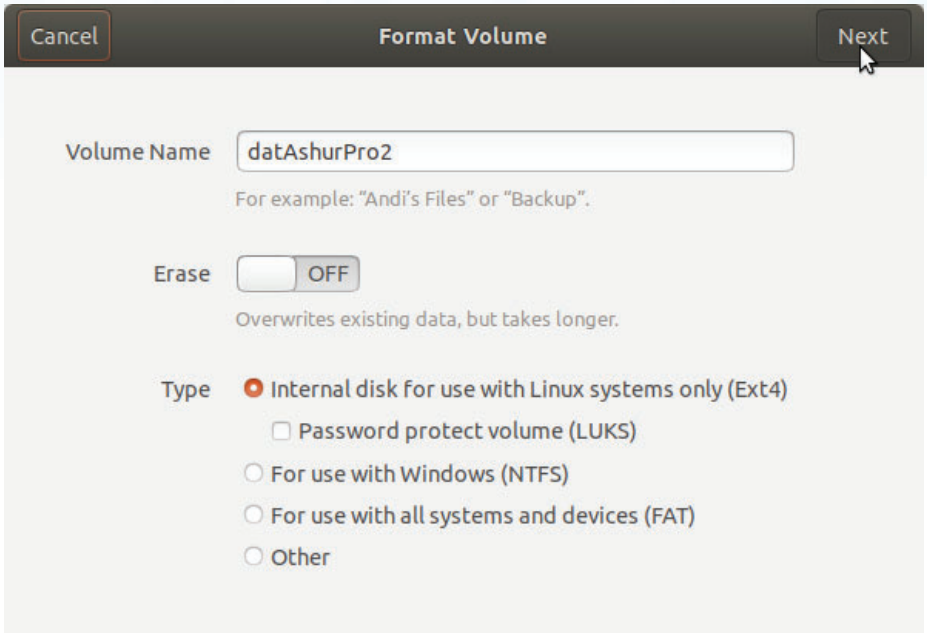


2. Choisissez la datAshur PRO² dans « Périphériques ». Cliquez sur l'icône en forme d'engrenage et choisissez « Formater la partition »

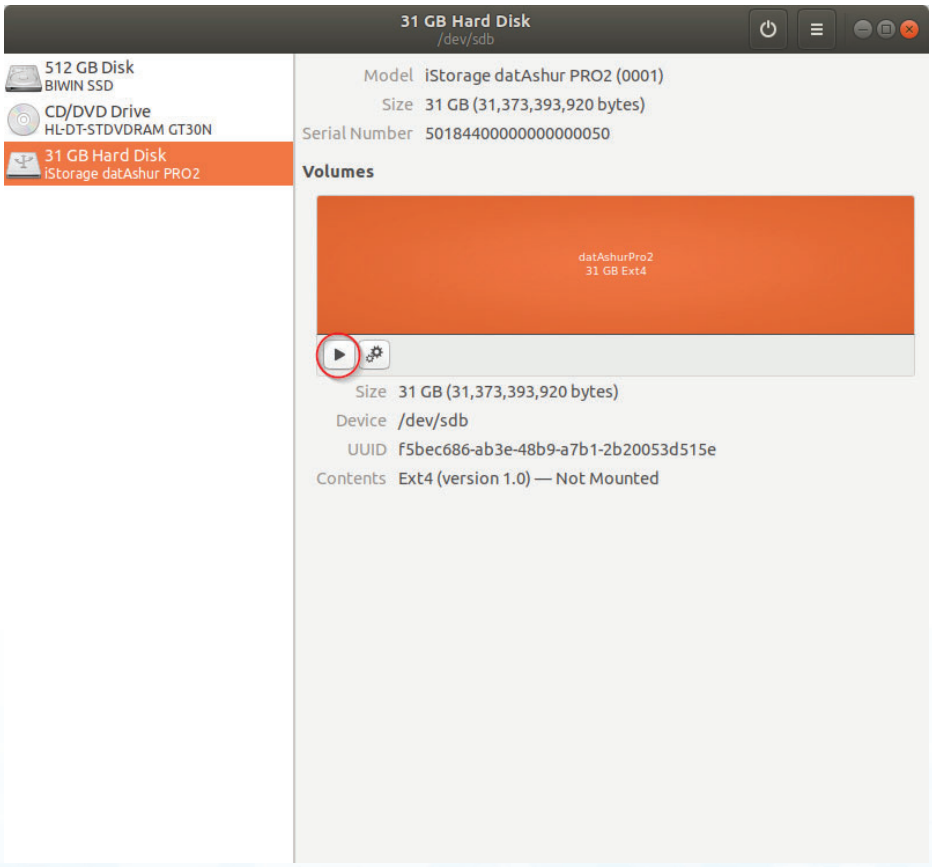


3. Configurez un Nom de volume, puis choisissez le type de formatage que vous souhaitez utiliser.
   EXT4 – Compatible avec Linux
   NTFS – Windows seulement
   FAT – Compatible avec tous les systèmes d'exploitation

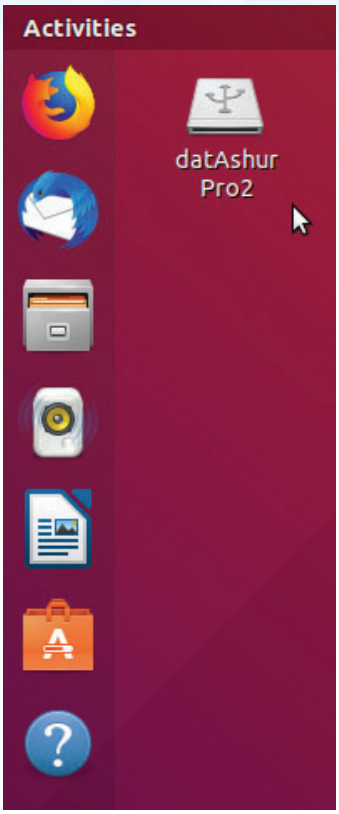
   Ensuite, appuyez sur « Suivant » puis sur « FORMATER »



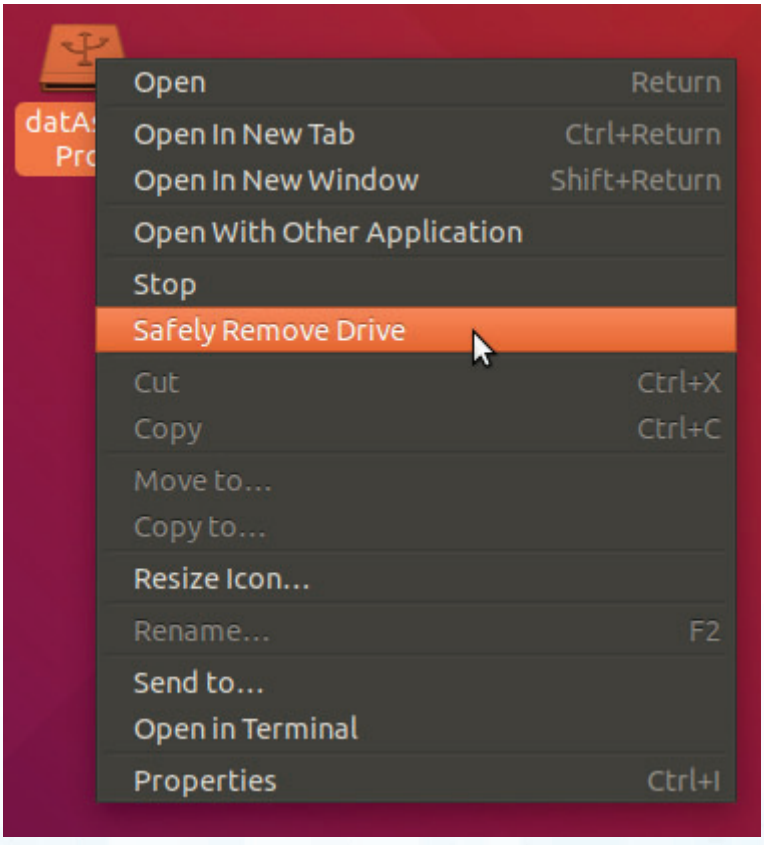
4. Une fois le processus de formatage terminé, cliquez sur ▶ pour monter la clé dans Ubuntu.



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



Verrouiller la datAshur PRO² pour Linux (Ubuntu 18.04 LTS) Il est fortement recommandé de faire un clic droit sur l'icône en forme de disque, puis de cliquer sur « Retirer en toute sécurité » dans le système d'exploitation pour éjecter (verrouiller) votre datAshur PRO², particulièrement une fois que les données ont été copiées ou supprimées de la clé.



42. Mise en veille prolongée, mise en veille ou déconnexion du système d'exploitation

Veillez bien à enregistrer et à fermer tous les fichiers qui se trouvent sur votre datAshur PRO² avant de mettre en veille prolongée, en veille ou de vous déconnecter du système d'exploitation.

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

Pour la verrouiller, cliquez simplement sur l'icône « Supprimer le périphérique en toute sécurité » de votre système d'exploitation et débranchez la datAshur PRO².

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

43. Comment vérifier la version du firmware en mode administrateur

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

1. En mode administrateur, appuyez sur les touches « **3** + **8** » et maintenez-les enfoncées		La LED BLEUE continue est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez une fois sur la touche **CLÉ (🔑)** et vous observerez ce qui suit : a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. b. La LED ROUGE clignote, indiquant la partie entière du numéro de révision du firmware. c. La LED VERTE clignote, ce qui indique la partie fractionnaire. d. La LED BLEUE clignote, indiquant le dernier chiffre du numéro de révision du firmware. e. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. f. Les LED ROUGE, VERTE et BLEUE sont remplacées par une LED BLEUE continue		

Par exemple, si le numéro de révision du firmware est « **2.3** », la LED ROUGE clignote une (**2**) fois et la LED VERTE clignote trois (**3**) fois. Une fois la séquence terminée, les LED ROUGE, VERTE et BLEUE clignotent une fois simultanément, puis sont remplacées par la LED BLEUE continue.

44. Comment vérifier la version du firmware en mode utilisateur

Pour vérifier le numéro de révision du firmware, accédez d'abord au **mode utilisateur** tel que décrit dans la section 14.
Une fois que la clé est en **mode utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

1. En mode utilisateur, appuyez sur les touches « **3 + 8** » et maintenez-les enfoncées 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 la touche **CLÉ (🔑)** et vous observerez ce qui suit :

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED ROUGE clignote, indiquant la partie intégrante du numéro de révision du firmware.
c. La LED VERTE clignote, ce qui indique la partie fractionnaire.
d. La LED BLEUE clignote, indiquant le dernier chiffre du numéro de révision du firmware
e. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde
f. Les LED ROUGE, VERTE et BLEUE sont remplacées par une LED BLEUE continue

Par exemple, si le numéro de révision du firmware est « **2.3** », la LED ROUGE clignote une (**2**) fois et la LED VERTE clignote trois (**3**) fois. Une fois la séquence terminée, les LED ROUGE, VERTE et BLEUE clignotent une fois simultanément, puis sont remplacées par la LED BLEUE continue.

45. Assistance technique

iStorage vous fournit les ressources utiles suivantes :

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

E-mail du support technique :
support@istorage-uk.com

Téléphone du support technique :
+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.

46. Informations de garantie et de renvoi de matériel

GARANTIE ET LIMITATION DE GARANTIE POUR LE PRODUIT ISTORAGE

iStorage garantit qu'à la livraison et pour la période de 36 mois qui la suit, ses produits ne présenteront aucun défaut matériel. Toutefois, cette garantie ne concerne pas les cas décrits ci-dessous. iStorage garantit que les produits sont conformes aux normes listées dans la fiche de données correspondante qui se trouvait sur notre site web au moment où vous avez passé votre commande.

Ces garanties ne couvrent aucun défaut des produits découlant de :

- une usure normale ;
- un dommage volontaire, stockage ou conditions de fonctionnement anormaux, accident, négligence de votre part ou de celle de toute tierce partie ;
- si un tiers ou vous manquez à faire fonctionner ou utiliser les produits conformément aux instructions de l'utilisateur ;
- toute modification ou réparation effectuée par vous ou un tiers n'étant pas l'un de nos réparateurs autorisés ; ou
- toute caractéristique fournie par vous.

Dans le cadre de ces garanties et à notre seule discrétion, nous réparerons, remplacerons ou vous rembourserons tout produit présentant un défaut matériel, à condition qu'à la livraison :

- vous ayez inspecté les produits afin de vérifier qu'ils ne comportaient aucun défaut matériel ; et
- vous ayez testé le mécanisme d'encodage des produits.

Nous ne serons tenus responsable d'aucun défaut matériel ou défaut du mécanisme d'encodage des produits qui aurait pu être vérifié à la livraison, sauf si vous déclarez ce défaut auprès de nous dans un délai de 30 jours après la livraison. Nous ne serons tenu responsables d'aucun défaut matériel ou défaut du mécanisme d'encodage des produits n'étant pas détectable lors d'une inspection réalisée à la livraison, sauf si vous nous signalez ce défaut dans un délai de 7 jours après l'avoir découvert ou après le jour où vous auriez dû le remarquer. Dans le cadre des présentes garanties, nous ne serons en aucun tenus responsable si vous ou qui que ce soit d'autre continuez à utiliser les produits après avoir découvert le défaut. Après le signalement d'un défaut, vous devez nous renvoyer le produit. Si vous êtes une entreprise, les frais de port liés au renvoi du produit ou des pièces du produit concernées à notre adresse dans le cadre de cette garantie, seront à votre charge, et nous prendrons en charge les frais de port liés au renvoi d'un produit réparé ou remplacé à votre adresse. Si vous êtes un particulier, merci de consulter nos conditions générales.

Les produits renvoyés doivent l'être dans leur emballage d'origine et dan un état propre. Les produits retournés autrement seront, à la seule discrétion de l'entreprise, refusés, ou des frais supplémentaires vous seront facturés pour couvrir les coûts additionnels. Les produits renvoyés à des fins de réparation dans le cadre de la garantie, doivent être accompagnés d'une copie de la facture originale, ou d'une feuille de papier libre contenant le numéro de facture originale ainsi que la date d'achat.

Si vous êtes un particulier, la présente garantie s'ajoute à vos droits légaux concernant les produits défectueux, ou ne correspondant pas à la description qui en est faite. Vous pouvez recueillir des conseils sur vos droits auprès de votre Bureau local de conseils aux citoyens, ou du Bureau des normes commerciales.

Les garanties présentées dans la présente clause s'appliquent uniquement à l'acheteur original d'un produit iStorage, ou au distributeur ou revendeur autorisé iStorage. Ces garanties sont non cessibles.

À L'EXCEPTION DE LA GARANTIE LIMITÉE OFFERTE ICI, ET DANS LA MESURE MAXIMALE AUTORISÉE PAR LA LOI, ISTORAGE DÉCLINE TOUTE GARANTIE, EXPRESSE OU TACITE, NOTAMMENT TOUTES LES GARANTIES DE CONFORMITÉ ET D'USAGE NORMAL, ET NON INFRACTION. ISTORAGE NE GARANTIT EN AUCUN CAS QUE LE PRODUIT FONCTIONNERA PARFAITEMENT. DANS LA MESURE OÙ TOUTE GARANTIE TACITE PUISSE NÉANMOINS EXISTER PAR APPLICATION DE LA LOI, TOUTE GARANTIE DE CE TYPE EST LIMITÉE À LA DURÉE DE LA PRÉSENTE GARANTIE. LA RÉPARATION OU LE REMPLACEMENT DE CE PRODUIT, TEL QU'INDIQUÉ ICI, CONSTITUE VOTRE RECOURS EXCLUSIF.

EN AUCUN CAS ISTORAGE NE SERA TENU RESPONSABLE D'UNE PERTE OU DE PROFITS ANTICIPÉS, NI AUCUN DOMMAGE FORTUIT, PUNITIF, TYPIQUE, SPÉCIAL, DÉPENDANT OU ULTÉRIEUR, INCLUANT SANS POUR AUTANT S'Y LIMITER, LA PERTE DE CHIFFRE D'AFFAIRES, LA PERTE DE RECETTES, LA PERTE DE L'UTILISATION D'UN LOGICIEL, LA PERTE DE DONNÉES, TOUTE AUTRE PERTE OU RÉCUPÉRATION DE DONNÉES, TOUT DOMMAGE AUX BIENS ET RÉCLAMATION DE TIERS, DÉCOULANT DE TOUTE THÉORIE DE RÉCUPÉRATION, COMPRENANT LA GARANTIE, TOUT ACTE CONTRACTUEL, STATUTAIRE OU DÉLICTUEL, QU'IL EST ÉTÉ OU NON INDIQUÉ LA POSSIBILITÉ DE SURVENUE DE CES DOMMAGES, NONOBSTANT LA DURÉE DE TOUTE GARANTIE LIMITÉE, OU DE TOUTE GARANTIE IMPLIQUÉE PAR LA LOI, OU DANS LE CAS OÚ TOUTE GARANTIE LIMITÉE MANQUE À SATISFAIRE SON OBJECTIF PRINCIPAL, EN AUCUN CAS LA RESPONSABILITÉ TOTALE D'ISTORAGE N'EXCÉDERA LE PRIX D'ACHAT DE CE PRODUIT. | 4823-2548-5683.3

Copyright © iStorage Limited 2019. Tous droits réservés.
iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, Angleterre
Tél. : +44 (0) 20 8991 6260 | Fax : +44 (0) 20 8991 6277
e-mail : info@istorage-uk.com | web : www.istorage-uk.com