DATASHUR® PRO²

iStorage®

iStorage datAshur PRO²® User Manual v2.1

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.

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

Table of Contents

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 (**p**qrs) **2** (**a**bc) **7** (pqr**s**) **7** (pqr**s**) **9** (**w**xyz) **6** (mn**o**) **7** (pq**r**s) **3** (**d**ef)
- For "**iStorage**" press the following buttons:
  4 (gh**i**) **7** (pqr**s**) **8** (**t**uv) **6** (mn**o**) **7** (pq**r**s) **2** (**a**bc) **4** (**g**hi) **3** (d**e**f)

Using this method, long and easy to remember PINs can be 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 PRO^2 has been successfully unlocked, the GREEN LED will remain blinking for 30 seconds only, during which time the datAshur PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 (**p**qrs) **2** (**a**bc) **7** (pqr**s**) **7** (pqr**s**) **9** (**w**xyz) **6** (mn**o**) **7** (pq**r**s) **3** (**d**ef)
- For "**iStorage**" press the following buttons:
  4 (gh**i**) **7** (pqr**s**) **8** (**t**uv) **6** (mn**o**) **7** (pq**r**s) **2** (**a**bc) **4** (**g**hi) **3** (d**e**f)

Using this method, long and easy to remember PINs can be 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

14. How to Unlock datAshur PRO^2 with User PIN

To unlock with the **User PIN,** the datAshur PRO^2 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 PRO^2 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 PRO^2. 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2. 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 successfully configured

Note: When the datAshur PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 can be set to automatically lock after a pre-set amount of time. In its default state, the datAshur PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 incorporates a defence mechanism to protect the drive against Brute Force attacks. By default, the initial shipment state values of the brute force limitation (consecutive incorrect PIN entries) for both the Admin PIN and User PIN is **10** and **5** for the Recovery PIN. Three independent brute force counters are used to record the incorrect attempts for each PIN authorisation (Admin, User and Recovery) as set out below.

- If a user enters an **incorrect User PIN** 10 consecutive times, the User PIN will be deleted but the data, Admin PIN and Recovery PIN remain intact and accessible.
- If an **incorrect Recovery PIN** is entered 5 consecutive times, the Recovery PIN is deleted but the data and Admin PIN remain intact and accessible.
- If an **incorrect Admin PIN** is entered 10 consecutive times, the drive will reset. All PINs and data are deleted and lost forever.

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

PIN used to unlock drive	Consecutive incorrect PIN enteries	Description of what happens
User PIN	10	• The User PIN is deleted. • The Recovery PIN, the Admin PIN and all data remain intact and accessible.
Recovery PIN	5	• The Recovery PIN is deleted. • The Admin PIN and all data remain intact and accessible.
Admin PIN	10	• The datAshur PRO^2 will reset. All PINs and data are deleted and lost forever.

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

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

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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 will also need to be formatted before any new data can be added to the drive.

36. How to configure datAshur PRO^2 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 PRO^2 is configured as non-bootable.

iStorage datAshur PRO^2 USB drives are equipped with a bootable feature to accommodate power cycling during a host boot process. When booting from the datAshur PRO^2, you are running your computer with the operating system that is installed on the datAshur PRO^2.

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 PRO^2 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 PRO^2 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 PRO^2 must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

37. How to disable the datAshur PRO^2 Bootable feature

To disable the datAshur PRO^2 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 PRO^2 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 PRO^2 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 PRO^2 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.

<table>
<tr><td>1. In Admin mode press and hold down both <b>SHIFT</b> (⬆) + <b>8</b> buttons</td><td>▲ ➾ ▼▲</td><td>Solid BLUE LED will change to blinking GREEN and BLUE LEDs</td></tr>
<tr><td colspan="3">2. Press the <b>KEY (⚷)</b> button and one of the following two scenarios will happen;
• <b>If datAshur PRO² is configured as Bootable, the following happens;</b>
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
• <b>If datAshur PRO² is <u>NOT</u> configured as Bootable, the following happens;</b>
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</td></tr>
</table>

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. How to configure the Drive as Removable or Local Disk

iStorage datAshur PRO² USB drives can be configured as either "Removable Disk" or "Local Disk" whilst the default setting of the datAshur PRO² is configured as a Removable Disk. To configure the drive, 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 (⚷)** + **1** buttons	▲ ➝ ▼▲	Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter one of the following indication numbers for disk enumeration type: • "**00**" for "**Removable Disk**" • "**01**" for "**Local Disk**"		
3. Press **SHIFT** (🡅) button once	▼▲ ➝ ▲	Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the disk enumeration 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.

40. How to check whether the Drive is Removable or Local Disk

To check the disk enumeration 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** (🡅) + **1** buttons	▲ ⇢ ▼ ▲	Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY** (⚷) button and the following happens; • **If datAshur PRO² is configured as Local Disk, 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 configured as Removable Disk, 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.

41. Formatting the datAshur PRO^2 for Windows

After a 'Brute Force Attack' or a complete reset the datAshur PRO^2 will delete all data and the encryption key.
You will need to format the datAshur PRO^2 before it can be used.

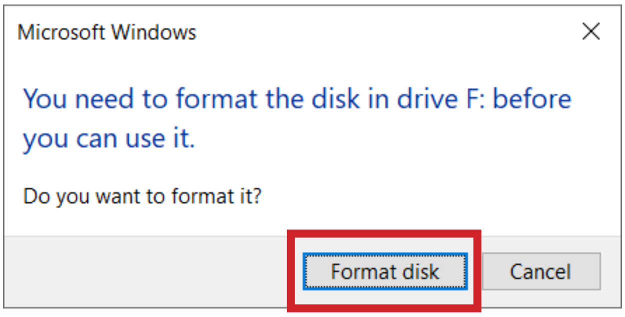
To format your datAshur PRO^2, do the following:

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

3. Attach the datAshur PRO^2 to the computer.

4. Click on 'Format Disk'

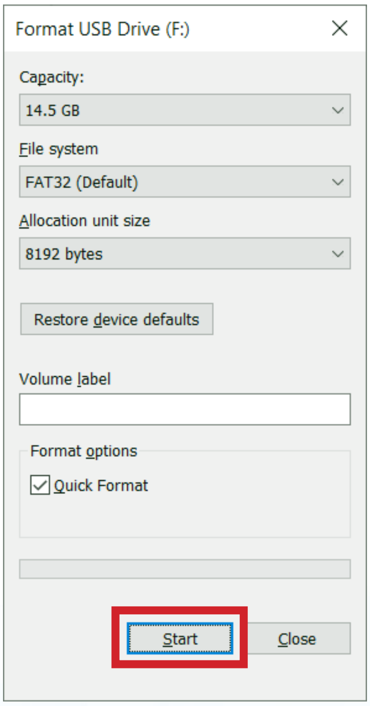


Microsoft Windows

You need to format the disk in drive F: before you can use it.

Do you want to format it?

5. Click 'Start'.



Format USB Drive (F:)

Capacity: 14.5 GB

File system: FAT32 (Default)

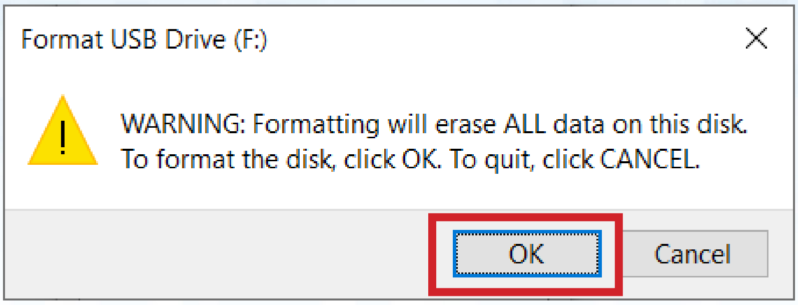
Allocation unit size: 8192 bytes

Volume label:

Format options

☑ Quick Format

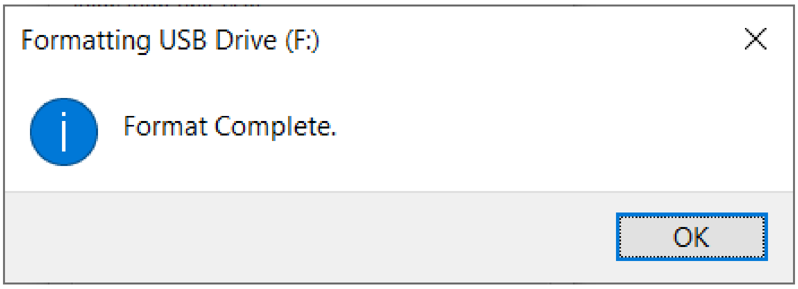
6. Click 'OK'.



Format USB Drive (F:)

WARNING: Formatting will erase ALL data on this disk.
To format the disk, click OK. To quit, click CANCEL.

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



Formatting USB Drive (F:)

Format Complete.

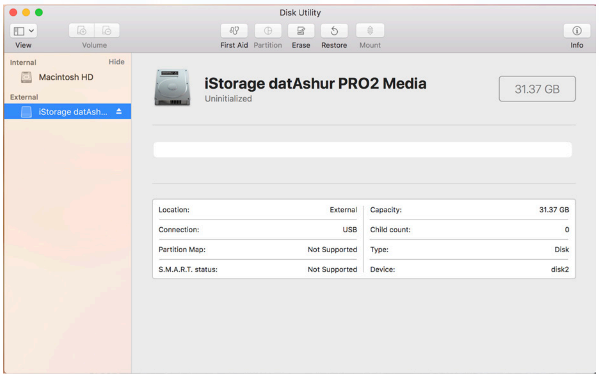
42. datAshur PRO² Setup for Mac OS

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.



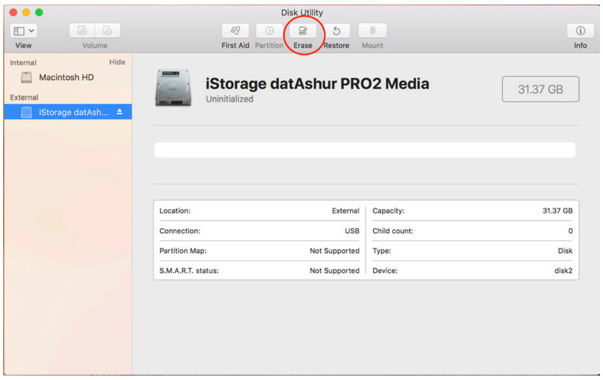
iStorage datAshur PRO2 Media

Uninitialized

31.37 GB

Location:	External	Capacity:	31.37 GB
Connection:	USB	Child count:	0
Partition Map:	Not Supported	Type:	Disk
S.M.A.R.T. status:	Not Supported	Device:	disk2

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



iStorage datAshur PRO2 Media

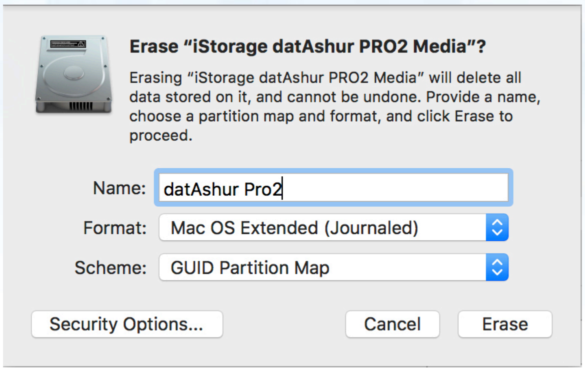
Uninitialized

31.37 GB

Location:	External	Capacity:	31.37 GB
Connection:	USB	Child count:	0
Partition Map:	Not Supported	Type:	Disk
S.M.A.R.T. status:	Not Supported	Device:	disk2

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.



Erase "iStorage datAshur PRO2 Media"?

Erasing "iStorage datAshur PRO2 Media" will delete all data stored on it, and cannot be undone. Provide a name, choose a partition map and format, and click Erase to proceed.

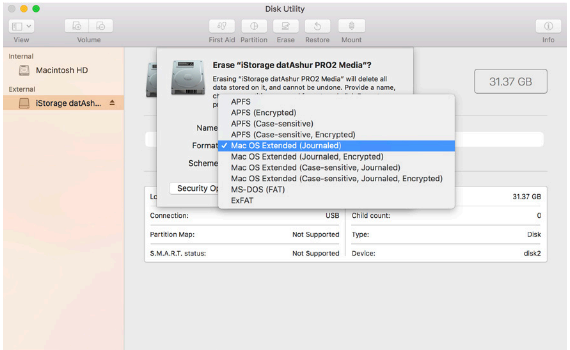
Name: datAshur Pro2

Format: Mac OS Extended (Journaled)

Scheme: GUID Partition Map

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).



Erase "iStorage datAshur PRO2 Media"?

Erasing "iStorage datAshur PRO2 Media" will delete all data stored on it, and cannot be undone. Provide a name,

Name
Format
Scheme
Security Op
APFS
APFS (Encrypted)
APFS (Case-sensitive)
APFS (Case-sensitive, Encrypted)
✓ Mac OS Extended (Journaled)
Mac OS Extended (Journaled, Encrypted)
Mac OS Extended (Case-sensitive, Journaled)
Mac OS Extended (Case-sensitive, Journaled, Encrypted)
MS-DOS (FAT)
ExFAT

31.37 GB

Connection: USB

Child count: 0

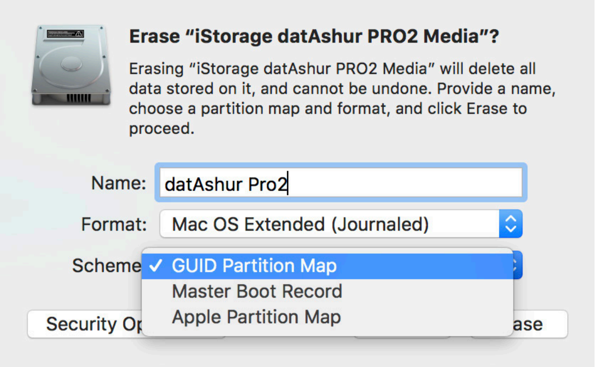
Partition Map: Not Supported

Type: Disk

S.M.A.R.T. status: Not Supported

Device: disk2

figure 3



Erase "iStorage datAshur PRO2 Media"?

Erasing "iStorage datAshur PRO2 Media" will delete all data stored on it, and cannot be undone. Provide a name, choose a partition map and format, and click Erase to proceed.

Name: datAshur Pro2

Format: Mac OS Extended (Journaled)

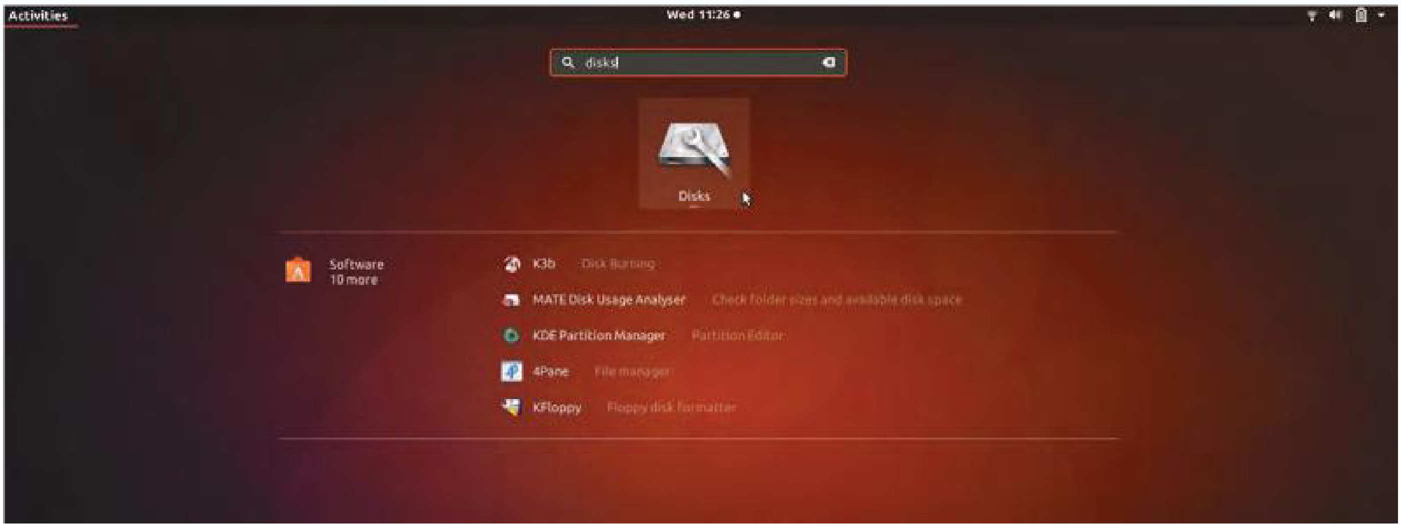
figure 4

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

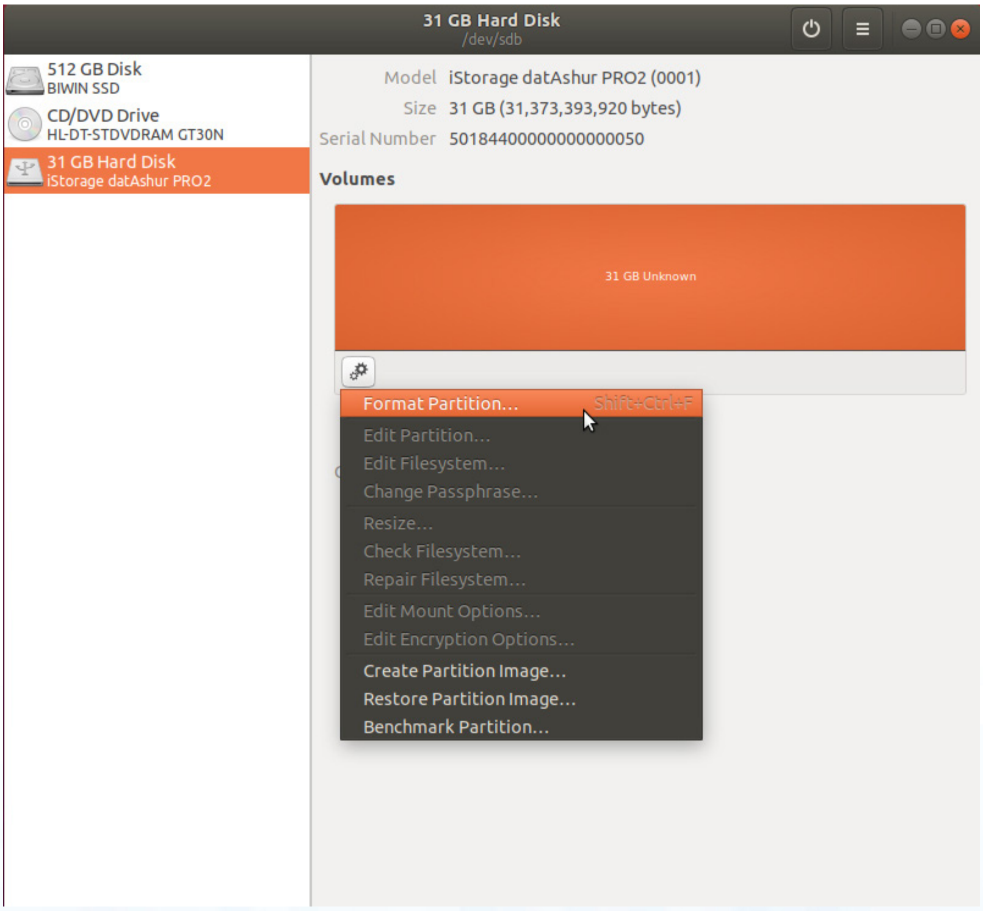
43. datAshur PRO² Setup for Linux (Ubuntu 18.04 LTS)

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.



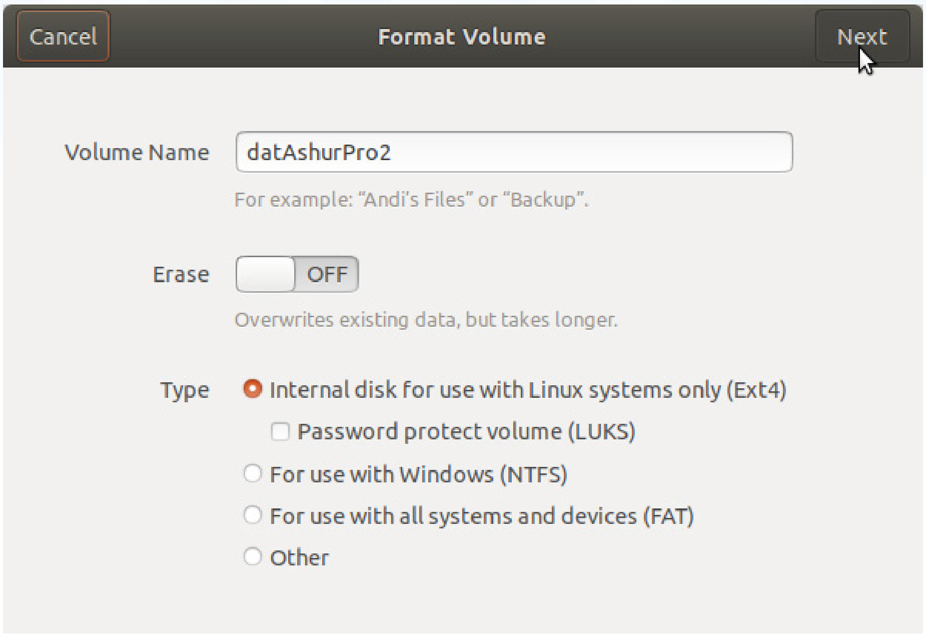
2. Select the datAshur PRO² under 'Devices'. Click on the gears icon and choose 'Format Partition'


31 GB Hard Disk
/dev/sdb

Model iStorage datAshur PRO2 (0001)
Size 31 GB (31,373,393,920 bytes)
Serial Number 5018440000000000050

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'



Volume Name: datAshurPro2

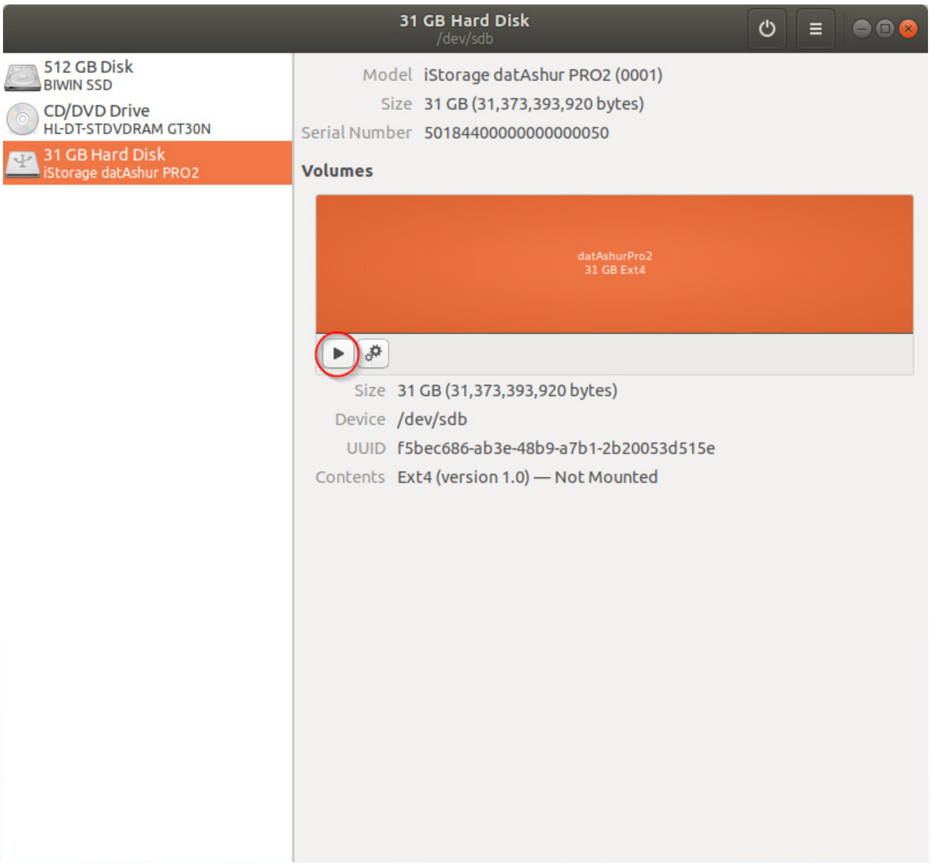
For example: "Andi's Files" or "Backup".

Erase: OFF

Overwrites existing data, but takes longer.

Type:
- ● Internal disk for use with Linux systems only (Ext4)
  - □ Password protect volume (LUKS)
- ○ For use with Windows (NTFS)
- ○ For use with all systems and devices (FAT)
- ○ Other

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

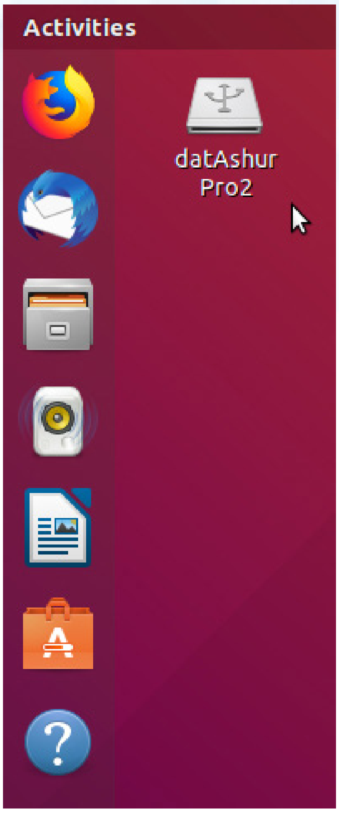


Model: iStorage datAshur PRO2 (0001)
Size: 31 GB (31,373,393,920 bytes)
Serial Number: 50184400000000000050

Volumes

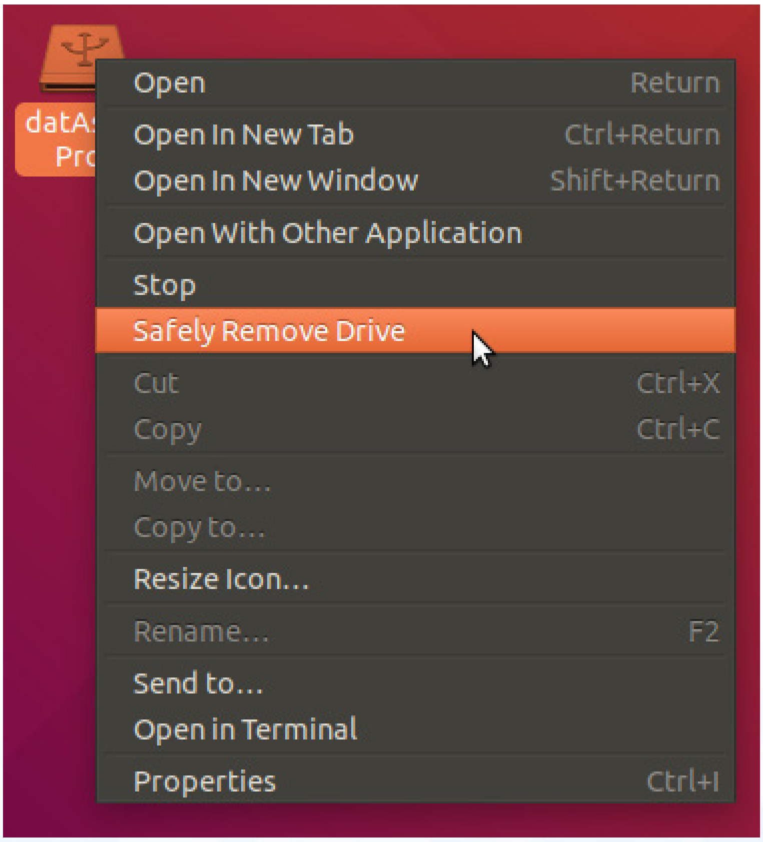
Size: 31 GB (31,373,393,920 bytes)
Device: /dev/sdb
UUID: f5bec686-ab3e-48b9-a7b1-2b20053d515e
Contents: Ext4 (version 1.0) — Not Mounted

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.



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

Be sure to save and close all the files on your datAshur PRO^2 before hibernating, suspending, or logging off from the operating system.

It is recommended that you lock the datAshur PRO^2 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 PRO^2.

Attention: To ensure your data is secure, be sure to lock your datAshur PRO^2 if you are away from your computer.

45. How to check Firmware in Admin mode

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

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

For example, if the firmware revision number is '**2.3**', the RED LED will blink twice (**2**) and the GREEN LED will blink three (**3**) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to Admin mode, a solid BLUE LED.

46. 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 '**2.3**', the RED LED will blink twice (**2**) and the GREEN LED will blink three (**3**) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to the User mode, a solid GREEN LED.

47. 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.

48. Warranty and RMA information

Three Year Warranty:

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

Disclaimer and terms of warranty:

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

iStorage®

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