



## DATASHUR® SD

**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 SD please contact our support team by email, [support@istorage-uk.com](mailto:support@istorage-uk.com) or by phone on +44 (0) 20 8991 6260.

Copyright © iStorage Limited 2021. 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

iStorage datAshur SD® User Manual v1.0.8



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

Trade Agreements Act (TAA) Compliant



## Table of Contents

|   |    |
|---|----|
| Introduction .....  | 4  |
| Box contents .....  | 4  |
| 1. LED indicators and their actions .....                                   | 5  |
| 2. Battery and LED States .....   | 5  |
| 3. First Time Use.....  | 6  |
| 4. Unlocking datAshur SD with the Admin PIN .....                           | 7  |
| 5. To enter Admin Mode .....  | 8  |
| 6. To exit Admin Mode .....   | 8  |
| 7. Changing the Admin PIN .....   | 9  |
| 8. Setting a User PIN Policy .....  | 10 |
| 9. How to delete the User PIN Policy .....                                  | 11 |
| 10. How to check the User PIN Policy .....                                  | 12 |
| 11. Adding a new User PIN in Admin Mode .....                               | 13 |
| 12. Changing the User PIN in Admin Mode .....                               | 14 |
| 13. Deleting the User PIN in Admin Mode .....                               | 14 |
| 14. How to unlock datAshur SD with User PIN .....                           | 15 |
| 15. Changing the User PIN in User Mode .....                                | 15 |
| 16. Creating a One-Time User Recovery PIN .....                             | 16 |
| 17. Deleting the One-Time User Recovery PIN .....                           | 16 |
| 18. Activating Recovery Mode and Creating New User PIN .....                | 17 |
| 19. Set User Read-Only in Admin Mode .....                                  | 18 |
| 20. Enable User Read/Write in Admin Mode .....                              | 18 |
| 21. Set Global Read-Only in Admin Mode .....                                | 19 |
| 22. Enable Global Read/Write in Admin Mode .....                            | 19 |
| 23. How to configure a Self-Destruct PIN .....                              | 20 |
| 24. How to delete the Self-Destruct PIN .....                               | 21 |
| 25. How to unlock with the Self-Destruct PIN .....                          | 21 |
| 26. How to configure an Admin PIN after a Brute Force attack or Reset ..... | 22 |
| 27. Setting the Unattended Auto-Lock Clock .....                            | 22 |
| 28. Turn off the Unattended Auto-Lock Clock .....                           | 23 |
| 29. How to check the Unattended Auto-Lock Clock.....                        | 24 |
| 30. Set Read-Only in User Mode .....  | 24 |
| 31. Enable Read/Write in User Mode .....                                    | 25 |
| 32. Brute Force Hack Defence Mechanism .....                                | 25 |
| 33. How to set the User PIN Brute Force Limitation .....                    | 26 |
| 34. How to check the User PIN Brute Force Limitation .....                  | 27 |
| 35. How to perform a complete reset .....                                   | 28 |
| 36. How to configure datAshur SD as Bootable .....                          | 28 |
| 37. How to disable the datAshur SD Bootable feature .....                   | 29 |
| 38. How to check the Bootable setting .....                                 | 29 |
| 39. How to set your datAshur SD to enable KeyWriter cloning .....           | 30 |
| 40. How to disable KeyWriter cloning .....                                  | 30 |
| 41. How to check KeyWriter cloning configuration .....                      | 31 |
| 42. How to configure datAshur SD Encryption Mode .....                      | 31 |
| 43. How to check datAshur SD Encryption Mode .....                          | 32 |
| 44. Formatting the datAshur SD (microSD card) for Windows .....             | 33 |
| 45. Formatting the datAshur SD (microSD card) for macOS .....               | 34 |
| 46. Formatting the datAshur SD (microSD card) for Linux OS .....            | 36 |
| 47. Hibernating, suspending or logging off from the operating system .....  | 38 |
| 48. How to check Firmware in Admin Mode .....                               | 38 |
| 49. How to check Firmware in User Mode .....                                | 39 |
| 50. Technical Support .....   | 40 |
| 51. Warranty and RMA information .....                                      | 40 |

## Introduction



**Note:** The datAshur SD rechargeable battery is not fully charged, we recommend the battery be charged prior to first use. Please plug in the datAshur SD to a powered USB port for 20-30 minutes to fully charge the battery.

Only genuine iStorage microSD Cards are compatible with the datAshur SD drive.

The iStorage datAshur SD is a PIN authenticated, hardware encrypted, USB Type-C flash drive designed to incorporate removable iStorage microSD Cards with a range of different capacities.

Rather than incorporating fixed memory, the datAshur SD is designed with an integrated microSD Card Slot making it a unique, ultra-secure and cost-effective solution that enables users to use one drive with as many iStorage microSD Cards as required, in varying capacities, offering unlimited encrypted data storage.

Furthermore, the patented iStorage datAshur SD KeyWriter application clones datAshur SD flash drives with the same encrypted encryption key enabling a secondary drive (or more) to be cloned as a backup and also enables organisations to share encrypted iStorage microSD Cards with as many authorised users of cloned datAshur SD drives as required, without compromising on data security.

All data stored on iStorage microSD Cards is encrypted (full disk encryption) using FIPS PUB 197 validated AES-XTS 256-bit hardware encryption, the encryption mode can also be changed to either AES-ECB or AES-CBC. In addition to the datAshur PRO<sup>2</sup> (Common Criteria EAL 5+ hardware certified), the datAshur SD is the world's only encrypted USB flash drive to incorporate a secure microprocessor that is Common Criteria EAL 5+ certified, which enhances security through true random number generation and built-in cryptography. The data encryption key is protected by FIPS and Common Criteria validated wrapping algorithms and is securely stored on the secure microprocessor, separate from the data.

For more information on the datAshur SD KeyWriter application, please refer to our website <https://istorage-uk.com>.

## Box Contents

- iStorage datAshur SD
- Extruded Aluminium Sleeve
- Type C to Type A USB Adapter
- Quick Start Guide

**iStorage microSD cards are sold separately**

## 1. LED indicators and their actions

| LED | LED State          | Description  | LED | LED State                            | Description  |
|-----|--------------------|--|-----|--------------------------------------|--|
|     | RED Solid<br>      | Locked device (in either <b>Standby</b> or <b>Reset</b> states)                          |     | RED, GREEN and BLUE Blinking<br>     | Waiting for <b>User</b> PIN entry  |
|     | RED - Fade Out<br> | Device Turning off to the <b>Idle State</b>  |     | GREEN and BLUE Blinking together<br> | Waiting for <b>Admin</b> PIN entry   |
|     | GREEN Blinking<br> | <b>Unlocked</b> device as <b>Admin</b> (not connected to USB port)                       |     | RED and GREEN Blinking together<br>  | Waiting for <b>Recovery</b> PIN entry  |
|     | GREEN Solid<br>    | <b>Unlocked</b> device as <b>User</b> (not connected to USB port) or device in User Mode |     | BLUE blinking every 5 seconds<br>    | Battery starts charging after 30 seconds when device is locked and connected to a USB port |
|     | BLUE Solid<br>     | Device in <b>Admin Mode</b>  |     | Rapidly Blinking GREEN<br>           | Data transfer in progress  |

## 2. Battery and LED States



**Note:** The normal function of the datAshur SD 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 SD 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 SD to a powered USB port and charge for 20-30 minutes. Once recharged, the datAshur SD will resume normal function.

### To wake from Idle State

Idle State is defined as when datAshur SD is not being used and all LEDs are off.

To wake datAshur SD from the Idle State do the following.

|  |  |   |
|--|--|---|
| Press and hold down the <b>SHIFT</b> (↑) button for one second or connect the device to a powered USB port |  | RED LED lights on indicating the device is in Standby State |
|--|--|---|

### To enter Idle State

To force datAshur SD 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 SD 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 SD is connected to a USB port, the **SHIFT (↑)** button does not function.

When connected to a powered USB port, a locked datAshur SD 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 20-30 minutes |
| Initial Shipment State | RED and GREEN Solid | ✓              | ✗         | Waiting for configuration of an Admin PIN      |

## 3. First Time Use



**Important:** datAshur SD is supplied in the ‘Initial Shipment State’ with no pre-set Admin PIN. A **8-64** digit Admin PIN must be configured before the drive can be used. Once an Admin PIN has been successfully configured, it is then not possible to switch the drive back to the ‘Initial Shipment State’.

### PIN Requirements:

- Must be between 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3)
- 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)

### Special Characters:

- The Admin PIN can be configured with the use of one or more ‘Special Characters’ (**SHIFT (↑) + digit** pressed down together), this can be placed once or several times anywhere along your 8-64 digit Admin PIN.

**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.



**Important microSD Card Information:** Only genuine iStorage microSD Cards are compatible with the datAshur SD drive. If the datAshur SD drive is unlocked and connected to a host computer using a non iStorage microSD card, all LEDs, **RED**, **GREEN** & **BLUE** blink on and off twice and will then change to a solid **RED** LED, indicating that the microSD card is not compatible with the datAshur SD drive.

To configure an 8-64 digit Admin PIN and unlock the datAshur SD for the first time, please follow the simple steps in the table below.

| Instructions - First Time Use  | LED            | LED State   |
|--|----------------|---|
| 1. Insert a genuine iStorage microSD card into the datAshur SD card slot   |                |   |
| 2. Press and hold down the <b>SHIFT</b> (↑) button for one second          | ▲<br>▼         | Solid <b>RED</b> and <b>GREEN</b> LEDs light up indicating the drive is in the Initial Shipment State   |
| 3. Press and hold down both <b>KEY</b> (⌘) + <b>1</b> buttons              | ▲ - ▼<br>▼ - ▲ | LEDs turn to blinking <b>GREEN</b> and solid <b>BLUE</b>  |
| 4. Enter <b>New Admin PIN</b> and press the <b>KEY</b> (⌘) button once     | ▼ → ▼<br>▲ → ▲ | Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs switch to a <b>GREEN</b> blink then back to Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs   |
| 5. Re-enter <b>New Admin PIN</b> and press the <b>KEY</b> (⌘) button again | ▼ → ▼<br>▲ → ▼ | Blinking <b>GREEN</b> and solid <b>BLUE</b> LED switches to a solid <b>BLUE</b> LED and finally to a blinking <b>GREEN</b> LED indicating the Admin PIN has been successfully configured and drive unlocked |



**Note:** Once datAshur SD has been successfully unlocked, the **GREEN** LED will remain blinking for 30 seconds only, during which time the datAshur SD needs to be connected to a powered USB port and formatted. Please refer to one of the following formats:

- Formatting the datAshur SD for Windows - Section 44 on page 33
- datAshur SD setup for macOS - Section 45 on page 34
- Initialising and formatting datAshur SD in Linux OS - Section 46 on page 36

### Locking datAshur SD

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

## 4. Unlocking datAshur SD with the Admin PIN

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

|   |  |  |
|---|--|--|
| 1. Press and hold down the <b>SHIFT (↑)</b> button for one second   |  | A solid <b>RED</b> LED switches on indicating the drive is in Standby State  |
| 2. In Standby State (solid <b>RED</b> LED) press the <b>KEY (⌘)</b> button once   |  | <b>GREEN</b> and <b>BLUE</b> LEDs blink together   |
| 3. With the <b>GREEN</b> and <b>BLUE</b> LEDs blinking together, enter the <b>Admin PIN</b> and press the <b>KEY (⌘)</b> button again |  | <b>GREEN</b> and <b>BLUE</b> LEDs change to a blinking <b>GREEN</b> LED indicating the drive has been successfully unlocked as Admin |



**Note:** Once datAshur SD has been successfully unlocked, the **GREEN** LED will remain blinking for 30 seconds only, during which time the datAshur SD 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 SD is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

## 5. To enter Admin Mode

The Admin PIN can be used to setup the datAshur SD with a host of security features including the creation of a secondary User PIN by first entering the Admin Mode indicated by a solid **BLUE** LED.

**Note:** The datAshur SD must not be connected to a USB port when accessing Admin Mode.

To Enter Admin Mode, do the following.

|   |  |  |
|---|--|--|
| 1. Press and hold down the <b>SHIFT (↑)</b> button for one second   |  | A solid <b>RED</b> LED switches on indicating the drive is in Standby State  |
| 2. In Standby State (solid <b>RED</b> LED) press the <b>KEY (⌘)</b> button once   |  | <b>GREEN</b> and <b>BLUE</b> LEDs blink together   |
| 3. With the <b>GREEN</b> and <b>BLUE</b> LEDs blinking together, enter the <b>Admin PIN</b> and press the <b>KEY (⌘)</b> button again |  | <b>GREEN</b> and <b>BLUE</b> LEDs will alternately blink several times and then to a solid <b>BLUE</b> LED changing to a blinking <b>GREEN</b> LED indicating the device is unlocked |
| 4. Press the <b>KEY (⌘)</b> button <b>three</b> times within 2 seconds ( <b>KEY (⌘) x 3</b> )   |  | Blinking <b>GREEN</b> LED will change to a solid <b>BLUE</b> LED indicating the device is in Admin Mode  |

When the datAshur SD 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 SD 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).

## 6. To exit Admin Mode

To immediately exit Admin Mode (solid **BLUE** LED), press and hold down the **SHIFT (↑)** button for a second - the solid **BLUE** LED switches to a solid **RED** LED which then fades out to the Idle State. To access the drive contents (data), the datAshur SD 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 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (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)

### Special Characters:

- The Admin PIN can be configured with the use of one or more ‘**Special Characters**’ (**SHIFT** (↑) + **digit** pressed down together), this can be placed once or several times anywhere along your 8-64 digit Admin PIN.




**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 <b>KEY</b> (⌘) + <b>2</b> buttons |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs   |
| 2. Enter <b>NEW Admin PIN</b> and press <b>KEY</b> (⌘) button                   |  | Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs will switch to a single <b>GREEN</b> LED blink and then back to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs                       |
| 3. Re-enter the <b>NEW Admin PIN</b> and press <b>KEY</b> (⌘) button            |  | Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs change to a double blink <b>BLUE</b> LED and finally to a solid <b>BLUE</b> LED indicating the Admin PIN has been successfully changed |

**Note:** When the datAshur SD 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 SD 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 SD 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 8 to 64 digits), as well as requiring or not the input of one or more 'Special Characters'. The "Special Character" functions as both the 'SHIFT (↑) + digit' buttons pressed down together.

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

Once the Administrator has set the User PIN Policy, for instance '091', a new User PIN will need to be configured - see section 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 8-64 digit PIN during the process of creating the User PIN as shown in the examples below.

- A. 'SHIFT (↑) + 2', '4', '7', '6', '8', '8', '3', '1', '4',
- B. '2', '4', 'SHIFT (↑) + 7', '6', '8', '8', '3', '1', '4',
- C. '2', '4', '7', '6', '8', '8', '3', '1', 'SHIFT (↑) + 4',



**Note:**

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

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



|  |  |   |
|--|--|---|
| 1. In Admin Mode, press and hold down both <b>KEY (Ⓟ) + 7</b> buttons  |  | Solid BLUE LED will change to blinking GREEN and BLUE LEDs  |
| 2. Enter your <b>3 digits</b> , remember the first two digits denote minimum PIN length and last digit (0 or 1) whether or not a special character has to be used. |  | Blinking GREEN and BLUE LEDs will continue to blink   |
| 3. Press the <b>SHIFT (↑)</b> 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 SD 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 SD 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 SD 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.

|  |   |   |
|--|---|---|
| <p>1. In Admin Mode, press and hold down both <b>KEY (5) + 7</b> buttons</p> |   | <p>Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs</p>  |
| <p>2. Enter <b>080</b> and press <b>SHIFT (↑)</b> button once</p>            |  | <p>Blinking <b>GREEN</b> and <b>BLUE</b> LEDs will change to a solid <b>GREEN</b> LED and finally to a solid <b>BLUE</b> LED indicating the User PIN Policy has been successfully deleted</p> |


**Note:** When the datAshur SD 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 SD 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 SD 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.

|  |   |  |
|--|---|--|
| <p>1. In Admin Mode press and hold down both <b>SHIFT (↑) + 7</b> buttons</p>  |  | <p>Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs</p> |
| <p>2. Press the <b>KEY (Ⓟ)</b> button and the following happens:</p> <ol style="list-style-type: none"> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>A <b>RED</b> LED blink equates to ten (10) units of a PIN.</li> <li>Every <b>GREEN</b> LED blink equates to a single (1) unit of a PIN</li> <li>A <b>BLUE</b> blink indicates that a 'Special Character' was set.</li> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>LEDs return to solid <b>BLUE</b></li> </ol> |   |  |

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 required | 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 required  | 090           | 0       | 9 Blinks | 0       |

**Note:** When the datAshur SD 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 SD 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 SD 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 to be used. Refer to section 10 to check the user PIN restrictions.

PIN requirements:

- Must be between 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3)
- 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 <b>KEY (⌘) + 3</b> buttons      |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs   |
| 2. Enter <b>New User PIN</b> and press <b>KEY (⌘)</b> button              |  | Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs will switch to a single <b>GREEN</b> LED blink and then back to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs |
| 3. Re-enter the <b>New User PIN</b> and press <b>KEY (⌘)</b> button again |  | <b>GREEN</b> LED will rapidly blink three times before it changes to a solid <b>BLUE</b> LED indicating a New User PIN has been successfully configured           |

**Note:** When the datAshur SD 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 SD 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 SD 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 to be 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 <b>KEY (Ⓝ) + 3</b> buttons      |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs   |
| 2. Enter <b>New User PIN</b> and press <b>KEY (Ⓝ)</b> button              |  | Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs will switch to a single <b>GREEN</b> LED blink and then back to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs |
| 3. Re-enter the <b>New User PIN</b> and press <b>KEY (Ⓝ)</b> button again |  | <b>GREEN</b> LED will rapidly blink three times before it changes to a solid <b>BLUE</b> LED indicating a New User PIN has been successfully configured           |

**Note:** When the datAshur SD 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 SD 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 SD 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 <b>SHIFT (↑) + 3</b> buttons |  | Solid <b>BLUE</b> LED will change to a blinking <b>RED</b> LED  |
| 2. Press and hold down both <b>SHIFT (↑) + 3</b> buttons again         |  | Blinking <b>RED</b> LED will change to a solid <b>RED</b> LED and then to a solid <b>BLUE</b> LED indicating the User PIN has been successfully deleted |

**Note:** When the datAshur SD 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 SD 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 SD must first be in the Idle State (all LEDs off) before an Admin/User PIN can be entered.

## 14. How to unlock datAshur SD with User PIN

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

|  |  |   |
|--|--|---|
| <p>1. In a standby state (solid <b>RED</b> LED) Press and hold down both the <b>SHIFT</b> (↑) + <b>KEY</b> (⌘) buttons</p> |  | <p><b>RED</b> LED switches to all LEDs, <b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b> blinking on and off</p>  |
| <p>2. Enter <b>User PIN</b> and press the <b>KEY</b> (⌘) button</p>  |  | <p><b>RED</b>, <b>GREEN</b> and <b>BLUE</b> blinking LEDs will switch to a solid <b>GREEN</b> LED indicating drive was successfully unlocked in User Mode</p> |

## 15. Changing the User PIN in User Mode

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

|  |  |  |
|--|--|--|
| <p>1. In User Mode press and hold down both <b>KEY</b> (⌘) + <b>4</b></p>  |  | <p>Solid <b>GREEN</b> LED will change to a blinking <b>GREEN</b> LED and a solid <b>BLUE</b> LED</p>   |
| <p>2. Enter <b>New User PIN</b> and press the <b>KEY</b> (⌘) button</p>    |  | <p>Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs will switch to a single <b>GREEN</b> LED blink and then back to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs</p> |
| <p>3. Re-enter <b>New User PIN</b> and press the <b>KEY</b> (⌘) button</p> |  | <p><b>GREEN</b> LED will rapidly blink three times and will then change to a solid <b>GREEN</b> LED indicating a successful User PIN change</p>                          |






**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 to be 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 SD. To activate the recovery mode, the user must first enter the correct One-Time Recovery PIN, if one has been configured. The user PIN recovery process does not impact the data, encryption key and Admin PIN, however the user is forced to configure a new 8-64 digit User PIN.

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



|   |   |   |
|---|---|---|
| <p>1. In Admin Mode press and hold down both <b>KEY (Ⓝ) + 4</b> buttons</p>             |  | <p>Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs</p>   |
| <p>2. Enter a <b>One-Time Recovery PIN</b> and press <b>KEY (Ⓝ)</b> button</p>          |  | <p>Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs</p>                       |
| <p>3. Re-enter a <b>One-Time Recovery PIN</b> and press <b>KEY (Ⓝ)</b> button again</p> |  | <p>GREEN LED will rapidly blink three times before it changes to a solid BLUE LED indicating the One-Time Recovery PIN has been successfully configured</p> |

**Note:** When the datAshur SD 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 SD 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 SD 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.

|   |   |  |
|---|---|--|
| <p>1. In Admin Mode press and hold down both <b>SHIFT (↑) + 4</b> buttons</p> |  | <p>Solid BLUE LED will change to blinking RED LED</p>  |
| <p>2. Press and hold down both <b>SHIFT (↑) + 4</b> buttons again</p>         |  | <p>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</p> |








**Note:** When the datAshur SD 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 SD 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 SD 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 SD. To activate the recovery mode, the user must first enter the correct One-Time Recovery PIN, if one has been configured. The user PIN recovery process does not impact the data, encryption key and Admin PIN, however the user is forced to configure a new 8-64 digit User PIN.

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

|   |   |  |
|---|---|--|
| 1. With the drive in <b>Idle State</b> press and hold down the <b>SHIFT</b> (↑) button for one second |  | A solid RED LED switches on indicating the drive is in Standby State   |
| 2. In <b>Standby State</b> press and hold down both <b>KEY</b> (Ⓝ) + <b>4</b> buttons                 |  | Solid RED LED will change to blinking RED and GREEN LEDs   |
| 3. Enter the One-Time <b>Recovery PIN</b> and press the <b>KEY</b> (Ⓝ) 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 <b>New User PIN</b> and press the <b>KEY</b> (Ⓝ) 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 <b>New User PIN</b> and press the <b>KEY</b> (Ⓝ) button again                         |  | GREEN LED will rapidly blink three times and will then change to a solid GREEN LED 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 SD 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 SD 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 SD 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 SD 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 SD 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 SD 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 SD 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 SD 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 SD 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 SD 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 SD 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 “ <b>5 + 6</b> ” buttons. |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs   |
| 2. Press <b>KEY (b)</b> button                                       |  | <b>GREEN</b> and <b>BLUE</b> LEDs will change to a solid <b>GREEN</b> LED and then to a solid <b>BLUE</b> LED indicating the drive has been configured and restricts Global access to Read-Only |

**Note:** When the datAshur SD 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 SD 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 SD 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 SD 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 “ <b>5 + 9</b> ” buttons. |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs   |
| 2. Press <b>KEY (b)</b> button                                       |  | <b>GREEN</b> and <b>BLUE</b> LEDs change to a solid <b>GREEN</b> LED then to a solid <b>BLUE</b> LED indicating the drive is configured as Read/Write |

**Note:** When the datAshur SD 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 SD 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 SD 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



**Warning:** 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 microSD card as inaccessible (lost forever), the drive will then show as unlocked **GREEN** LED. Unless you have cloned another datAshur SD as a backup drive, self-destructing this drive will also render data on other microSD cards that have been encrypted by this drive as inaccessible and lost forever. 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 <b>KEY (Ⓝ) + 6</b> buttons                  |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs   |
| 2. Configure a 8-64 digit <b>Self-Destruct PIN</b> and press the <b>KEY (Ⓝ)</b> button |  | Blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs will switch to a single <b>GREEN</b> LED blink and then back to blinking <b>GREEN</b> and solid <b>BLUE</b> LEDs |
| 3. Re-enter the <b>Self-Destruct PIN</b> and press the <b>KEY (Ⓝ)</b> button           |  | <b>GREEN</b> LED will rapidly blink three times before it changes to a solid <b>BLUE</b> LED to indicate the Self-Destruct PIN has been successfully configured   |

**Note:** When the datAshur SD 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 SD 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 SD 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 <b>SHIFT (↑) + 6</b> buttons |  | Solid <b>BLUE</b> LED will change to a blinking <b>RED</b> LED   |
| 2. Press and hold down <b>SHIFT (↑) + 6</b> buttons again               |  | Blinking <b>RED</b> LED will become solid and then change to a solid <b>BLUE</b> LED indicating the Self-Destruct PIN was successfully deleted |

**Note:** When the datAshur SD 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 SD 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 SD must first be in the Idle State (all LEDs off) before an Admin/User PIN can be entered.

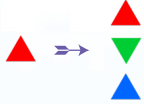
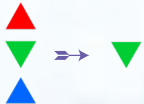
## 25. How to unlock with the Self-Destruct PIN



**Warning:** When the Self-Destruct mechanism is activated, the encryption key, the Admin/User PINs and all data are deleted and lost forever. Unless you have cloned another datAshur SD as a backup drive, self-destructing this drive will also render data on other microSD cards that have been encrypted by this drive as inaccessible and lost forever too. **The Self-Destruct PIN becomes the User PIN.** No Admin PIN exists after the Self-Destruct mechanism is activated. The datAshur SD 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 the encryption key, ALL data, Admin/User PINs** and then unlock the drive. Unless you have cloned another datAshur SD as a backup drive, self-destructing this drive will also render data on other microSD cards that have been encrypted by this drive as inaccessible and lost forever. Activating this feature will cause the **Self-Destruct PIN to become the New User PIN** and the datAshur SD 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 <b>RED</b> LED), press and hold down both the <b>SHIFT (↑) + KEY (Ⓟ)</b> buttons |  | <b>RED</b> LED switches to all LEDs, <b>RED, GREEN &amp; BLUE</b> blinking on and off   |
| 2. Enter the <b>Self-Destruct PIN</b> and press the <b>KEY (Ⓟ)</b> button                                   |  | <b>RED, GREEN</b> and <b>BLUE</b> blinking LEDs will change to a solid <b>GREEN</b> LED indicating the datAshur SD 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 SD has been reset to configure an Admin PIN before the drive can be used.




### PIN Requirements:

- Must be between 8-64 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3)
- 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)

### Special Characters:

- The Admin PIN can be configured with the use of one or more 'Special Characters' (**SHIFT (↑) + digit** pressed down together), this can be placed once or several times anywhere along your 8-64 digit Admin PIN.

If the datAshur SD 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 <b>SHIFT (↑) + 1</b> buttons |  | Solid RED LED will change to blinking GREEN and solid BLUE LEDs  |
| 2. Enter <b>New Admin PIN</b> and press <b>KEY (⌂)</b> 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 <b>New Admin PIN</b> and press <b>KEY (⌂)</b> button                       |  | Blinking GREEN LED and solid BLUE LED change to a solid BLUE LED indicating the Admin PIN was successfully configured.         |

**Note:** When the datAshur SD 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 SD 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 SD 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 SD can be set to automatically lock after a pre-set amount of time. In its default state, the datAshur SD 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 <b>KEY (Ⓝ) + 5</b> buttons   |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> 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:<br><b>05 for 5 minutes (press '0' followed by a '5')</b><br><b>20 for 20 minutes (press '2' followed by a '0')</b><br><b>99 for 99 minutes (press '9' followed by another '9')</b> |  |  |
| 3. Press the <b>SHIFT (↑)</b> button  |  | Blinking <b>GREEN</b> and <b>BLUE</b> LEDs will change to a solid <b>GREEN</b> for a second and then finally to a solid <b>BLUE</b> LED indicating the Auto-Lock time out is successfully configured |

**Note:** When the datAshur SD 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 SD 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 SD 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 <b>KEY (Ⓝ) + 5</b> buttons |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs  |
| 2. Enter <b>00</b> and press the <b>SHIFT (↑)</b> button              |  | Blinking <b>GREEN</b> and <b>BLUE</b> LEDs will change to a solid <b>GREEN</b> for a second and then finally to a solid <b>BLUE</b> LED indicating the Auto-Lock time out has been successfully disabled |


**Note:** When the datAshur SD 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 SD 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 SD 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.

|  |   |   |
|--|---|---|
| <p>1. In Admin Mode press and hold down <b>SHIFT (↑) + 5</b></p>   |  | <p>Solid BLUE LED will change to blinking GREEN and BLUE LEDs</p> |
| <p>2. Press the <b>KEY (Ⓟ)</b> button and the following happens:</p> <ul style="list-style-type: none"> <li>a. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>b. Each RED LED blink equates to ten (10) minutes.</li> <li>c. Every GREEN LED blink equates to one (1) minute.</li> <li>d. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>e. LEDs return to solid BLUE</li> </ul> |   |   |

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 SD 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 SD 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 SD 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 SD 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.

|  |   |   |
|--|---|---|
| <p>1. In User Mode, press and hold down both "<b>7 + 6</b>" buttons.</p> |  | <p>Solid GREEN LED will change to blinking GREEN and BLUE LEDs</p>  |
| <p>2. Press <b>KEY (Ⓟ)</b> button</p>                                    |  | <p>GREEN and BLUE LEDs will change to a solid GREEN LED indicating the drive is configured as Read-Only</p> |





**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 SD 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. |  | Solid GREEN LED will change to blinking GREEN and BLUE LEDs   |
| 2. Press <b>KEY (b)</b> 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 SD 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.

Successfully 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. Unless you have cloned another datAshur SD as a backup drive, this will also render data on other microSD cards that have been encrypted by this drive as inaccessible and lost forever too.

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

| PIN used to unlock drive | Consecutive incorrect PIN entries | Description of what happens  |
|--------------------------|-----------------------------------|--|
| User PIN                 | 10                                | <ul style="list-style-type: none"> <li>• The User PIN is deleted.</li> <li>• The Recovery PIN, the Admin PIN and all data remain intact and accessible.</li> </ul>   |
| Recovery PIN             | 5                                 | <ul style="list-style-type: none"> <li>• The Recovery PIN is deleted.</li> <li>• The Admin PIN and all data remain intact and accessible.</li> </ul>   |
| Admin PIN                | 5<br>3<br>2<br>(10 in total)      | <ul style="list-style-type: none"> <li>• After <b>5</b> consecutive incorrect Admin PIN entries, the drive will lock and all LEDs light up solid.</li> <li>• Enter PIN “<b>47867243</b>” and press the <b>KEY (⏏)</b> button to get <b>3</b> further PIN entries.</li> <li>• After a total of <b>8</b> (5+3) consecutive incorrect Admin PIN entries, the drive will lock and the LEDs blink alternately.</li> <li>• Enter PIN “<b>47867243</b>” and press the <b>KEY (⏏)</b> button to get the final <b>2</b> PIN entries (10 in total).</li> <li>• 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 (microSD card) will be lost forever.</li> </ul> |





**Important:** A new Admin PIN must be configured if the pre-existing Admin PIN was brute forced, refer to Section 26 on page 22 on ‘**How to Configure an Admin PIN after a Brute Force attack or Reset**’, the datAshur SD 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 SD 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.

|  |   |  |
|--|---|--|
| <p>1. In Admin Mode, press and hold down both <b>7 + 0</b> buttons</p>   |  | <p>Solid <b>BLUE</b> LED will change to <b>GREEN</b> and <b>BLUE</b> LEDs blinking together</p>  |
| <p>2. Enter the number of attempts for the brute force limitation (between 01-10), for example enter:</p> <ul style="list-style-type: none"> <li>• <b>01</b> for 1 attempt</li> <li>• <b>10</b> for 10 attempts</li> </ul> |   |  |
| <p>3. Press the <b>SHIFT (↑)</b> button once</p>   |  | <p>Blinking <b>GREEN</b> and <b>BLUE</b> LEDs will switch to a solid <b>GREEN</b> LED for a second and then to a solid <b>BLUE</b> LED indicating the brute force limitation was successfully configured</p> |

### 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.

|   |   |  |
|---|---|--|
| <p>1. In Admin Mode press and hold down both <b>2 + 0</b> buttons</p>   |  | <p>Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs</p> |
| <p>2. Press the <b>KEY (Ⓝ)</b> button and the following happens:</p> <ol style="list-style-type: none"> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>Each <b>RED</b> LED blink equates to ten (10) units of a brute force limitation number.</li> <li>Every <b>GREEN</b> LED blink equates to one (1) single unit of a brute force limitation number.</li> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>LEDs return to solid <b>BLUE</b></li> </ol> |   |  |

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 SD 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 SD 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 SD 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 SD 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 the drive will need to be formatted before it can be reused. Unless you have cloned another datAshur SD as a backup drive, resetting this drive will also render data on other microSD cards that have been encrypted by this drive as inaccessible and lost forever. To reset the datAshur SD 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 SD (microSD card) will also need to be formatted before any new data can be added to the drive, refer to Section 44, 45 or 46 depending on the operating system.

## 36. How to configure datAshur SD 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 SD is configured as non-bootable.

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

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 <b>KEY (5) + 9</b> 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 <b>SHIFT (↑)</b> 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 SD 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 SD 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 SD must first be in the Idle State (all LEDs off) before an Admin/User PIN can be entered.

## 37. How to disable the datAshur SD Bootable feature

To disable the datAshur SD 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 <b>KEY (⌘) + 9</b> buttons |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs  |
| 2. Press “ <b>0</b> ” followed by another “ <b>0</b> ” ( <b>00</b> )  |  | <b>GREEN</b> and <b>BLUE</b> LEDs will continue to blink   |
| 3. Press the <b>SHIFT (↑)</b> button once                             |  | Blinking <b>GREEN</b> and <b>BLUE</b> LEDs will change to a solid <b>GREEN</b> LED and finally to a solid <b>BLUE</b> LED indicating the bootable feature has been successfully disabled |

**Note:** When the datAshur SD 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 SD 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 SD 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 <b>SHIFT (↑) + 9</b> buttons  |  | Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs |
| 2. Press the <b>KEY (⌘)</b> button and one of the following two scenarios will happen:  |  |   |
| <ul style="list-style-type: none"> <li>• <b>If datAshur SD is configured as Bootable, the following happens:</b> <ol style="list-style-type: none"> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li><b>GREEN</b> LED blinks once.</li> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>LEDs return to solid <b>BLUE</b></li> </ol> </li> <li>• <b>If datAshur SD is NOT configured as Bootable, the following happens:</b> <ol style="list-style-type: none"> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>All LEDs are off</li> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>LEDs return to solid <b>BLUE</b></li> </ol> </li> </ul> |  |   |

## 39. How to set your datAshur SD to enable KeyWriter cloning



**Note:** The datAshur SD is set as default to enable KeyWriter cloning.

The datAshur SD can be used in conjunction with the iStorage KeyWriter application to enable cloning of up to 9 devices at a time. To set the datAshur SD to enable KeyWriter cloning, first enter the **Admin Mode** as described in section 5. Once the datAshur SD 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 <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs   |
| 2. Enter '11' and press the 'SHIFT (↑)' button once.              |  | <b>GREEN</b> and <b>BLUE</b> LEDs will change to a solid <b>GREEN</b> LED and then to a solid <b>BLUE</b> LED indicating the datAshur SD has been set to enable KeyWriter cloning |

**Note:** When the datAshur SD 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 SD 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 SD must first be in the Idle State (all LEDs off) before an Admin/User PIN can be entered.

## 40. How to disable KeyWriter cloning

To disable KeyWriter cloning, first enter the **Admin Mode** as described in section 5. Once the datAshur SD 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 <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs  |
| 2. Enter '44' and press the 'SHIFT (↑)' button once.              |  | <b>GREEN</b> and <b>BLUE</b> LEDs will change to a solid <b>GREEN</b> LED and then to a solid <b>BLUE</b> LED indicating the KeyWriter cloning feature has been disabled |

**Note:** When the datAshur SD 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 SD 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 SD must first be in the Idle State (all LEDs off) before an Admin/User PIN can be entered.

## 41. How to check KeyWriter cloning configuration

To check the datAshur SD KeyWriter configuration, first enter the **Admin Mode** as described in section 5. Once the datAshur SD is in **Admin Mode** (solid **BLUE** LED) proceed with the following steps.

|   |  |  |
|---|--|--|
| <p>1. In Admin Mode press and hold down both 'SHIFT (↑) + 8' buttons</p>  |  | <p>Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs</p> |
| <p>2. Press the <b>KEY (⌘)</b> button and the following happens:</p> <ul style="list-style-type: none"> <li>• <b>If datAshur SD is set to enable KeyWriter cloning, the following happens:</b> <ol style="list-style-type: none"> <li>a. All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>b. <b>GREEN</b> LED blinks once.</li> <li>c. All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>d. LEDs return to solid <b>BLUE</b></li> </ol> </li> <li>• <b>If KeyWriter cloning is disabled, the following happens:</b> <ol style="list-style-type: none"> <li>a. All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>b. All LEDs are off</li> <li>c. All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li>d. LEDs return to solid <b>BLUE</b></li> </ol> </li> </ul> |  |  |

## 42. How to Configure datAshur SD Encryption Mode



**WARNING:** Changing the encryption mode from AES-XTS (default state) to AES-ECB or AES-CBC will delete the encryption key and cause the datAshur SD to reset and render all data as inaccessible and lost forever! Unless you have cloned another datAshur SD as a backup drive, changing the encryption mode will also render data on other microSD cards that have been encrypted by this drive as inaccessible and lost forever too!

Perform the following steps to configure the datAshur SD encryption mode to either **AES-ECB** indicated by the number **'01'**, or **AES-XTS** indicated by the number **'02'**, or **AES-CBC** indicated by the number **'03'**. This feature is set as AES-XTS (02) by default. Please note all critical parameters will be sanitised when switching to a different encryption mode, therefore the user will not be able to unlock the drive with old PINs. The drive will be enter reset state at the next boot.

To set the datAshur SD encryption mode, first enter the **Admin Mode** as described in section 5. Once the datAshur SD 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 <b>01</b> to set as <b>AES-ECB</b><br>Enter <b>02</b> to set as <b>AES-XTS (default state)</b><br>Enter <b>03</b> to set as <b>AES-CBC</b> |  | GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating the client application registration is disabled                                |
| 3. Press the <b>SHIFT (↑)</b> button once.  |  | GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid RED LED ( <b>Reset State</b> ) indicating the datAshur SD encryption mode was successfully changed |

**Important:** After configuring the encryption mode, the datAshur SD completely resets and 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'.

## 43. How to check datAshur SD encryption mode

To check the datAshur SD encryption mode, first enter the **Admin Mode** as described in section 5. Once the datAshur SD 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 |
| <p>2. Press the <b>KEY (⌘)</b> button and the following happens:</p> <ul style="list-style-type: none"> <li>• <b>If the encryption mode is configured as AES-ECB, the following happens:</b> <ol style="list-style-type: none"> <li>a. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>b. GREEN LED blinks once.</li> <li>c. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>d. LEDs return to solid BLUE</li> </ol> </li> <li>• <b>If the encryption mode is configured as AES-XTS, the following happens:</b> <ol style="list-style-type: none"> <li>a. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>b. GREEN LED blinks twice.</li> <li>c. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>d. LEDs return to solid BLUE</li> </ol> </li> <li>• <b>If the encryption mode is configured as AES-CBC, the following happens:</b> <ol style="list-style-type: none"> <li>a. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>b. GREEN LED blinks three times.</li> <li>c. All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>d. LEDs return to solid BLUE</li> </ol> </li> </ul> |  |  |



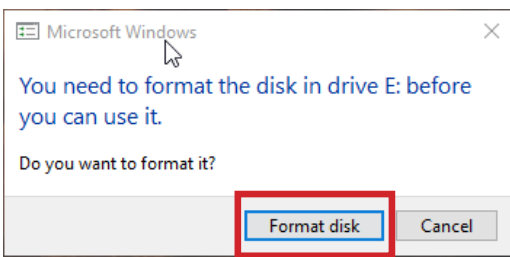
**Note:** When the datAshur SD is in Admin Mode, the **BLUE** LED will remain on and solid for 30 seconds only, during which time the drive can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the datAshur SD 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 SD must first be in the Idle State (all LEDs off) before an Admin/User PIN can be entered.

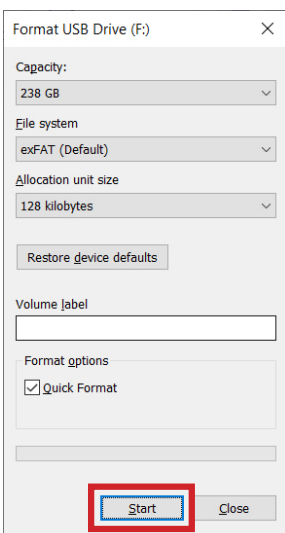
## 44. Formatting the datAshur SD (microSD card) for Windows

To format your datAshur SD on Windows, please follow the below steps:

1. Insert the microSD card in the datAshur SD, unlock the drive and attach the to the Windows machine.
2. The system will prompt you with the Format window.

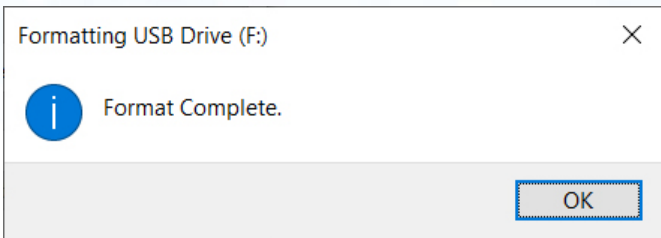
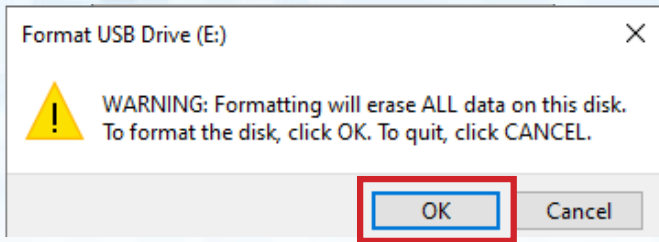


3. Click **Format disk** and Format USB drive window will open.



4. Enter a name for the drive on the Volume label. This name of the drive will eventually appear on the Desktop. The File System dropdown menu lists the available drive formats supported in Windows. Select NTFS for Windows or select FAT32 or exFAT for cross-platform compatibility, which includes macOS.
5. Click **Start** to continue with formatting the drive.

6. Click **OK** and the procedure will finish formatting the drive and will then confirm that formatting has been completed.



## 45. Formatting the datAshur SD (microSD card) for macOS

To format your datAshur SD on macOS, please follow the below steps:

1. Insert the microSD card in the datAshur SD, unlock the drive and attach the to the macOS machine.
2. A warning message will pop up (Image 1). Press **“Initialise”**.

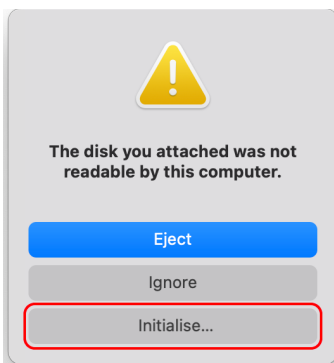


Image 1

3. Select the external volume (Image 2) labelled “iStorage datAshur SD M...” and press **“Erase”**.

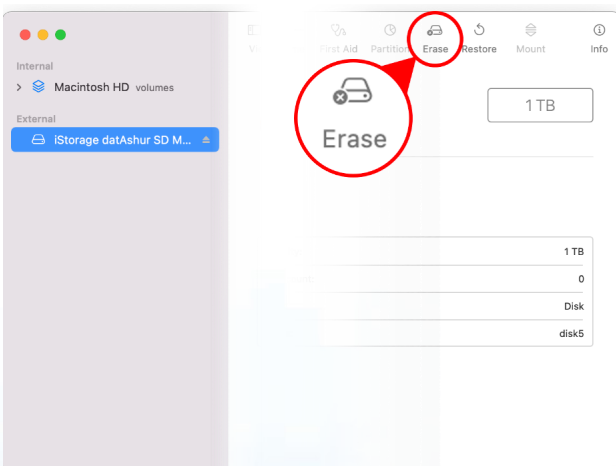


Image 2

4. Enter a name for the drive (Image 3). The name of the drive will eventually appear on the Desktop. The Volume Format dropdown menu lists the available drive formats that the Mac supports. The recommended format type is macOS Extended for macOS and MS-DOS or exFAT for cross platform including windows. Select Scheme as GUID Partition Map.
5. Click Erase.

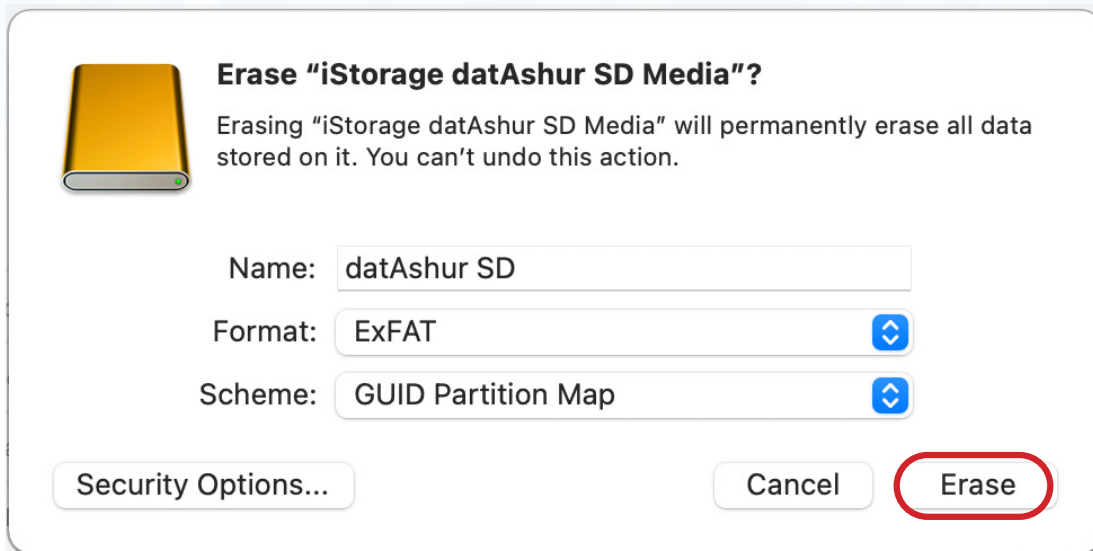


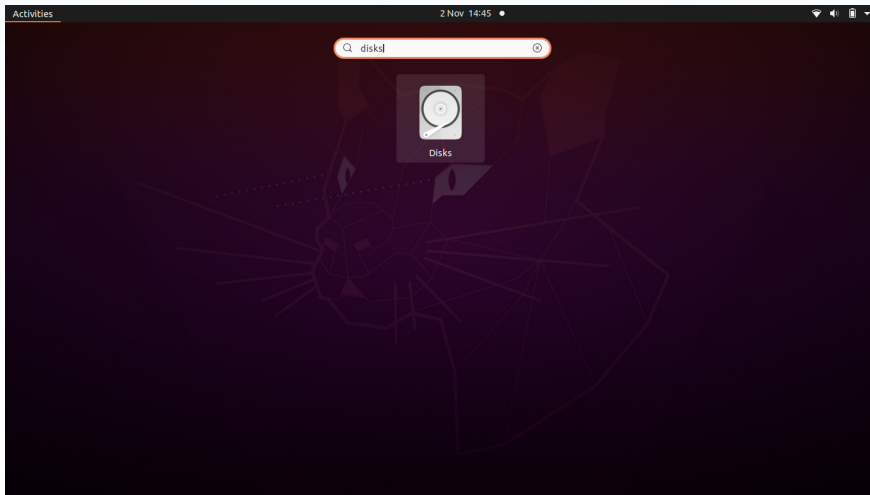
Image 3

6. The formatted datAshur SD (microSD card) will appear in the Disk Utility window and will mount onto the desktop.

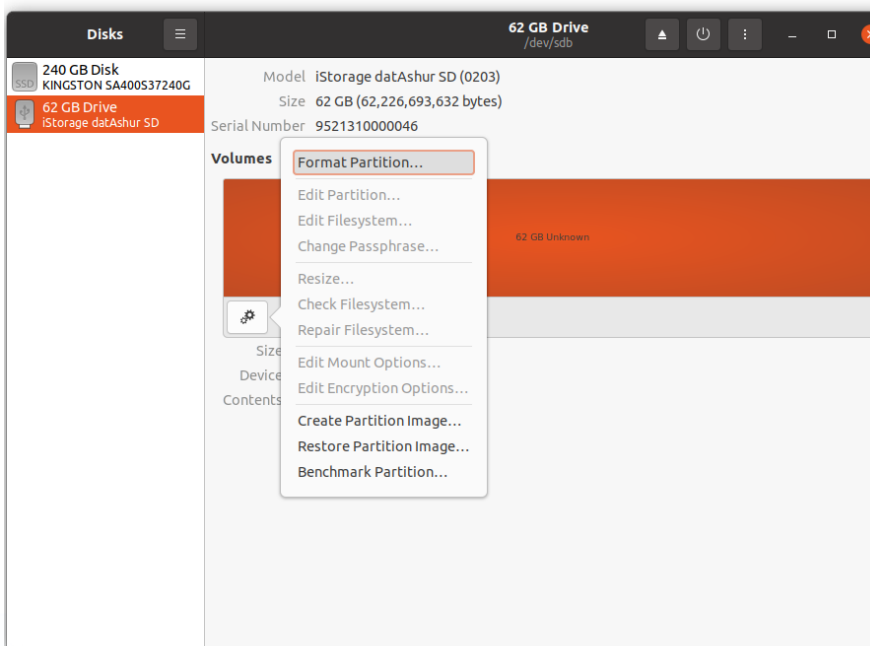
## 46. Formatting the datAshur SD (microSD card) for Linux

To format your datAshur SD on Linux, please follow the below steps:

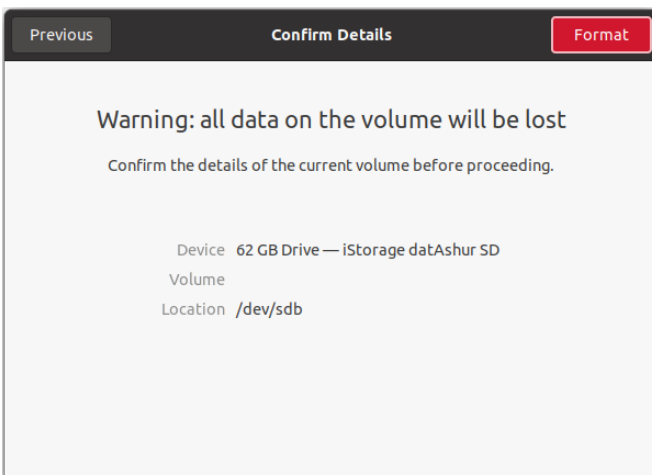
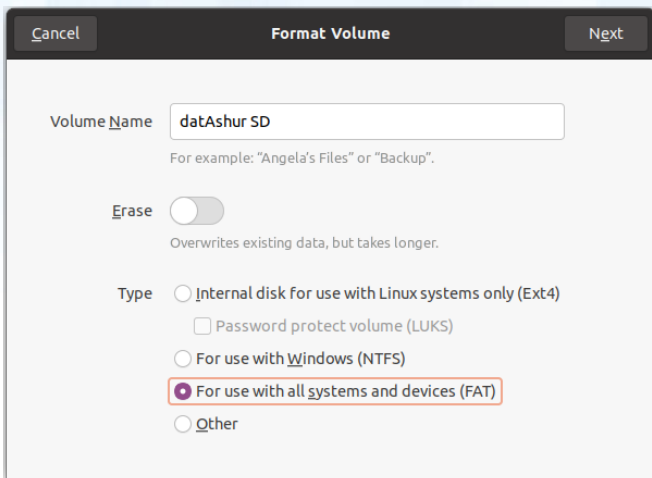
1. Insert the micro SD card in the datAshur SD drive and unlock and attach the drive to the Linux machine.
2. Open 'Show Application' and type 'Disks' in the search box. Click on the 'Disks' utility when displayed.



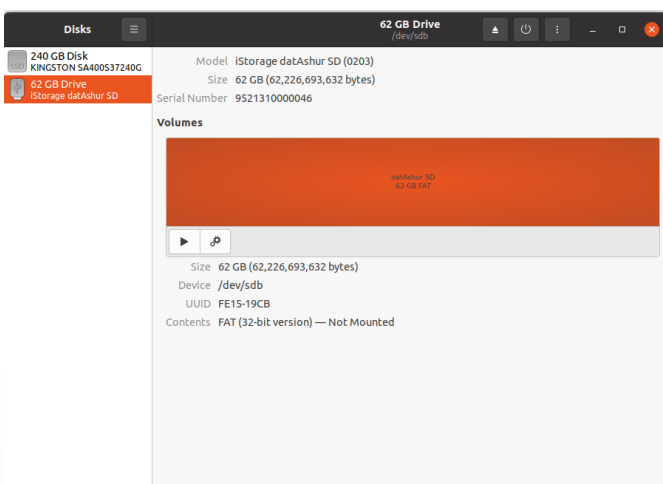
3. Click to select the drive under '**Devices**'. Next click on the gear icon under '**Volumes**' and then click on '**Format Partitions**'.



4. Enter a name for the drive and select 'For use in all systems and devices (FAT)' for the 'Type' option. e.g.: datAshur SD. Then, click the **'Format'** button.



5. After the format process is finished, click  to mount the drive to Linux.



6. Now the drive should be mounted to Linux and ready to use.

## 47. Hibernating, suspending, or logging off from the operating system

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

It is recommended that you lock the datAshur SD 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 SD.



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

## 48. How to check Firmware in Admin Mode


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

|   |  |  |
|---|--|--|
| <p>1. In Admin Mode press and hold down both “<b>3 + 8</b>” buttons</p>   |  | <p>Solid <b>BLUE</b> LED will change to blinking <b>GREEN</b> and <b>BLUE</b> LEDs</p> |
| <p>2. Press the <b>KEY (5)</b> button once and the following happens:</p> <ol style="list-style-type: none"> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li><b>RED</b> LED blinks indicating the integral part of the firmware revision number.</li> <li><b>GREEN</b> LED blinks indicating the fractional part.</li> <li><b>BLUE</b> LED blinks indicating the last digit of the firmware revision number</li> <li>All LED's (<b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b>) become solid for 1 second.</li> <li><b>RED</b>, <b>GREEN</b> &amp; <b>BLUE</b> LEDs switch to a solid <b>BLUE</b> LED</li> </ol> |  |  |

For example, if the firmware revision number is '**6.2**', the **RED** LED will blink twice (**6**) and the **GREEN** LED will blink three (**2**) times. Once the sequence has ended the **RED**, **GREEN** & **BLUE** LED's will blink together once and then return to Admin Mode, a solid **BLUE** LED.

## 49. How to check Firmware in User Mode

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

|   |   |  |
|---|---|--|
| <p>1. In User Mode press and hold down both “<b>3 + 8</b>” buttons until GREEN and BLUE LEDs blink together</p>   |  | <p>Solid GREEN LED will change to blinking GREEN and BLUE LEDs</p> |
| <p>2. Press the <b>KEY (b)</b> button and the following happens:</p> <ol style="list-style-type: none"> <li>All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>RED LED blinks indicating the integral part of the firmware revision number.</li> <li>GREEN LED blinks indicating the fractional part.</li> <li>BLUE LED blinks indicating the last digit of the firmware revision number</li> <li>All LED's (RED, GREEN &amp; BLUE) become solid for 1 second.</li> <li>RED, GREEN &amp; BLUE LEDs switch to a solid BLUE LED</li> </ol> |   |  |

For example, if the firmware revision number is ‘**6.2**’, the RED LED will blink twice (**6**) and the GREEN LED will blink three (**2**) times. Once the sequence has ended the RED, GREEN & BLUE LED's will blink together once and then return to the User Mode, a solid GREEN LED.

## 50. Technical Support

iStorage provides the following helpful resources for you:

Website:

<https://www.istorage-uk.com>

E-mail Support:

[support@istorage-uk.com](mailto:support@istorage-uk.com)

Telephone Support:

**+44 (0) 20 8991-6260.**

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

## 51. Warranty and RMA information

### ISTORAGE PRODUCT DISCLAIMER AND WARRANTY

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

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

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

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

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

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

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

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

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

EXCEPT FOR THE LIMITED WARRANTY PROVIDED HEREIN, AND TO THE EXTENT PERMITTED BY LAW, ISTORAGE DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ALL WARRANTIES OF MERCHANTABILITY; FITNESS FOR A PARTICULAR PURPOSE, NON-INFRINGEMENT. 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®

Copyright © iStorage Limited 2021. 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](mailto:info@istorage-uk.com) | web: [www.istorage-uk.com](http://www.istorage-uk.com)