User Manual

diskashur® PRO

FIPS
Level 2 Certified
140-2
Certificate number 1970

Remember to save your PIN in a safe place. If lost or forgotten, there is no way to access the drive.

If you are having difficulty please refer to this complete user manual which is loaded on your diskAshur PRO drive and is also available at iStorage's website: www.istorage-uk.com/support

N30732

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

iStorage diskAshur PRO® Manual – v 2.1

Table of Contents

iStorage diskAshur PRO® Manual – v 2.1

Introduction

Looking for an effortless way to secure your data?

Looking for the highest level of security for your data while utilizing the fastest USB 3.0 speeds?

Look no further than the diskAshur PRO, certified and tested to NIST FIPS 140-2 Level 2 requirements. Sporting an easy-to-use keypad design that is impervious to dust, grit and water. With a software free setup and operation, the diskAshur PRO enables you to access the drive simply and easily with your own unique PIN. And with a super fast integrated USB 3.0 cable, you can access your data faster and more secure than ever before.

Box Contents

- **iStorage diskAshur PRO drive with integrated USB 3.0 cable**
- **Travel Pouch**
- **USB Y-cable**
- **Quick Start Guide**

1. Connecting the diskAshur PRO

Be sure to review the following information before you begin to use the diskAshur PRO.

> ⚠️ **Attention:** Use only the included cables with your diskAshur PRO. You might damage the drive if you use a cable not included with the diskAshur PRO.

diskAshur PRO is designed for portable use without an AC power adapter and in most cases will be able to power on a single USB port. In the event that diskAshur PRO is unable to power on a single USB connection, use the included USB Y-cable. The diskAshur PRO is not self-powered and requires connection to a USB port to perform all operations.

1. Attach the integrated USB cable of the diskAshur PRO drive to an available USB port on your computer, as shown below.

   Note: While diskAshur PRO will work with any USB port, for the fastest speeds connect to a USB 3.0 port on your computer.

2. At least one of the diskAshur PRO LEDs should turn on, indicating that it is receiving power.
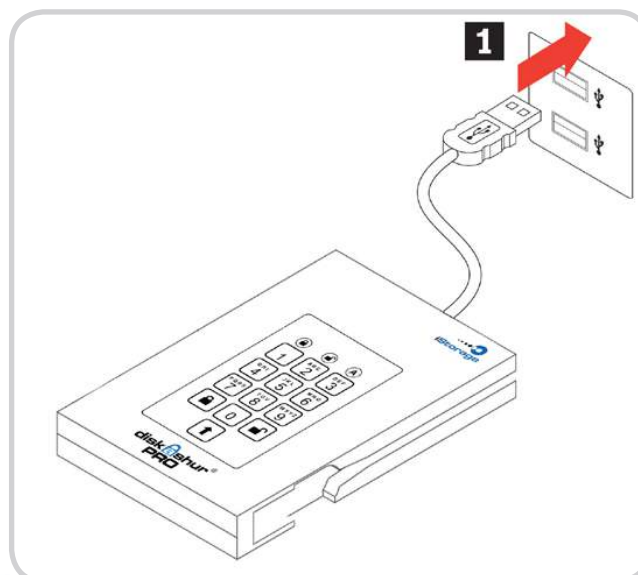
> ⚠️ **Note:** If none of the LED indicator lights turn on or the drive locks when writing to the disk, use the included USB Y-cable.
> Refer to directions on the following page.

2. Connecting with the USB Y-cable

If none of the diskAshur PRO LED indicator lights power on a single USB connection, use the included USB Y-cable.

1. Attach diskAshur PRO's integrated USB cable to the female connector of the USB Y-cable.

2. Connect the two male USB connectors to two available USB ports on your computer.

3. At least one of the diskAshur PRO's LED indicator lights should turn on, indicating that the diskAshur PRO is powered.

iStorage diskAshur PRO® Manual – v 2.1
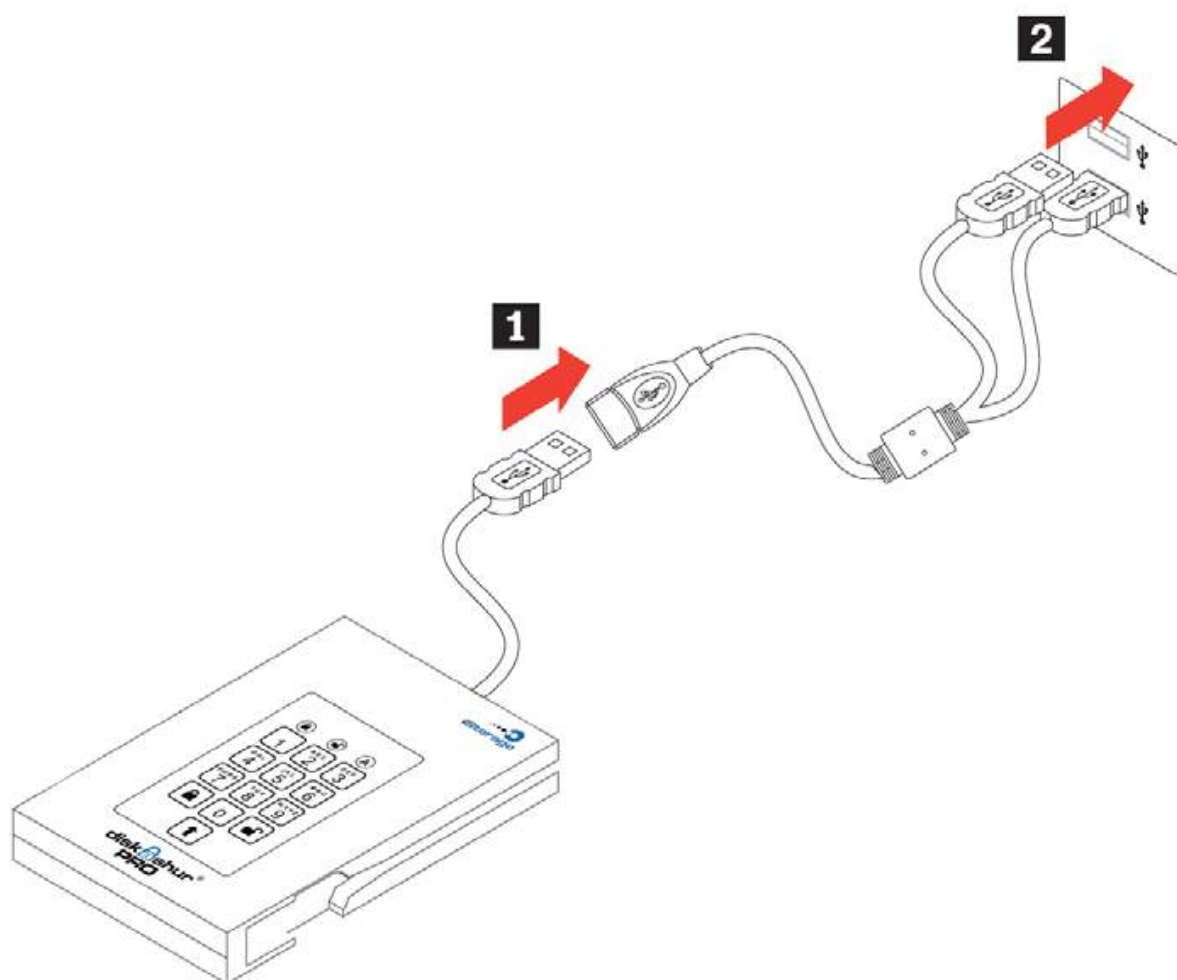
3. diskAshur PRO Layout
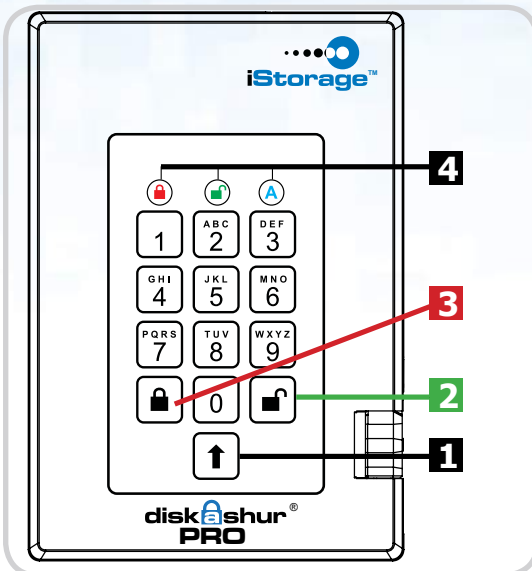
1	⬆	**SHIFT** button
2	🔓	**UNLOCK** button
3	🔒	**LOCK** button
4		**LED** Indicator lights

When you first plug in the FIPS diskAshur PRO drive, the unit will do a self-test to verify all security components are working properly. The LEDs will go through 3 test stages **RED**, **GREEN**, and **BLUE**. This will be followed by three **GREEN** flashes on a successful test. Any test failure will leave the unit in an interoperable state with the **RED** LED flashing.

4. First Time Use

Before diskAshur PRO can be used, the Admin PIN MUST be set. The LED will display Solid **BLUE** and Solid **GREEN** to indicate diskAshur PRO is waiting for a PIN to be set.

To Set-up the Admin PIN:

1. Press **UNLOCK + 9**. The LED will change to Solid **BLUE** and Blinking **GREEN**.
2. Enter the new Admin PIN and press **UNLOCK** key. If accepted the **GREEN** LED will flash for 3 short blinks, then return to Solid **BLUE** and Blinking **GREEN**.
3. Re-enter the Admin PIN and press the **UNLOCK** key. If accepted the **GREEN** LED will be Solid for 3 seconds.
4. LED will then turn **BLUE** and remain in Admin mode for 30 seconds or if the **LOCK** key is pressed, will return the drive to a standby state.
5. The Admin PIN is now set and will allow access to the drive or the Admin features.
6. To **UNLOCK** the drive, exit Admin by pressing the **LOCK** button. Then enter the new PIN and press **UNLOCK**.

Requirements for Admin, User and Self-Destruct PIN:

PINs must be a minimum length of 7 maximum 16 digits.
Cannot contain all consecutive numbers (2345678 or 9876543)
Cannot contain all same number (1111111)
The **SHIFT** key can be used for additional combinations.
SHIFT + **1** are a separate value than just 1.

5. Locking the diskAshur PRO

To lock the drive, press the **LOCK** button.

If data is still being written to the drive, diskAshur PRO will wait until all data has been written to the drive and then it will lock automatically.

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

6. Unlocking the diskAshur PRO

To unlock the drive:

Enter either a User PIN or Admin PIN and press the **UNLOCK** button.

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

7. Admin Mode

To enter the Admin Mode, do the following:

1. Attach the USB cable to an available USB port on your computer. The diskAshur PRO goes into the Standby Mode after the self-check, and the LED turns **RED**.
2. Press and hold **UNLOCK + 0** buttons for five seconds until the LED flashes **RED**. This indicates that you can enter the Admin PIN.
3. Enter the Admin PIN and press the **UNLOCK** button.
4. The drive is in Admin Mode when the LED has changed to **BLUE**.

8. Changing the Admin PIN

You can change the Admin PIN by doing the following:

1. Enter Admin Mode (**UNLOCK + 0** buttons for five seconds. Enter Admin PIN and press **UNLOCK**).
2. Press and hold **UNLOCK + 9** buttons until the LED turns to Solid **BLUE** and Blinking **GREEN**.
3. Enter the new PIN and press **UNLOCK** (The PIN must be a minimum of 7 digits and a maximum of 16 digits). The LED flashes **GREEN** three times, then returns to Solid **BLUE** and Blinking **GREEN**.
4. Re-enter the new Admin PIN and press **UNLOCK**. The LED stays solid **GREEN** for two seconds and then solid **BLUE** indicating that the Admin PIN has been changed successfully.

9.   Adding a new User PIN

1. Enter the Admin Mode (**UNLOCK + 0** buttons for five seconds. Enter Admin PIN and press **UNLOCK**).
2. Press and hold **UNLOCK + 1** buttons until the LED turns to Solid **BLUE** and Blinking **GREEN**.
3. Enter a User PIN and press **UNLOCK** (a minimum of 7 digits and a maximum of 16 digits).
   The LED flashes **GREEN** three times, then returns to Solid **BLUE** and Blinking **GREEN**.
4. Re-enter the new User PIN and press **UNLOCK**. If the LED stays solid **GREEN** for two
   seconds and then solid **BLUE**, the User PIN was successfully added.

10. Deleting the User PINs

You can delete ALL User PINs by doing the following:

1. Enter the Admin Mode (**UNLOCK + 0** buttons for five seconds. Enter Admin PIN and press **UNLOCK**).
2. Press and hold **7 + 8 + UNLOCK** buttons for five seconds until the LED flashes **GREEN** three
   times and then changes to **BLUE** / **RED** alternating.
3. Press and hold **7 + 8 + UNLOCK buttons** a second time for five seconds until the LED goes on
   solid **GREEN** for two seconds and then back to solid **BLUE**, this indicates that the User
   PINs were deleted successfully.

11. Changing the User PIN

You can change the User PIN by doing the following:

1. Unlock the drive by inputting your User PIN and pressing the **UNLOCK** button.
2. Press and hold **UNLOCK + 1** buttons until the LED flashes **RED**.
3. Enter your current PIN and press **UNLOCK**.
   The LED will be Solid **BLUE** and Solid **GREEN**.
4. Enter the new PIN and press **UNLOCK** (The PIN must be a minimum of 7 digits and
   a maximum of 16 digits). The LED will flash **GREEN** three times, then returns to Solid
   BLUE and Blinking **GREEN**.
5. Re-enter the new User PIN and press **UNLOCK**. The LED stays solid **GREEN**
   indicating that the User PIN has been changed successfully.

12. Setting the Unattended Auto Lock Feature

To protect against unauthorized access if the drive is unlocked and unattended, diskAshur PRO can be set to automatically lock after a pre-set amount of time. In its default state, the diskAshur PRO Unattended Auto Lock feature is turned off. The Unattended Auto Lock can be set to activate after 5, 10 or 20 minutes.

To set the Unattended Auto Lock please uses the following steps:

1. Enter the Admin mode by pressing and holding **UNLOCK + 0** buttons for five seconds until the LED flashes **RED**. This indicates that you can enter the Admin PIN.

2. Enter the Admin PIN and press **UNLOCK**. The drive is in Admin Mode when the LED has changed to solid **BLUE**.

3. Once in Admin mode, press **UNLOCK + 6** buttons. The LED should start flashing **RED** and **BLUE** intermittently.

4. Press one of the numbers below that corresponds to amount of time you would like the drive to lock after no activity:

> **Auto Lock Timeout Table:**
>
> 1 = 5 minutes
> 2 = 10 minutes
> 3 = 20 minutes
> 0 = OFF
>
> The Default is **OFF** for this feature.

5. After you have input the number, the LED should flash **GREEN** 3 times to indicate that you have successfully set the Unattended Auto Lock feature.

13. Brute Force Protection

What is Brute Force Attack?

A brute force attack is a method of defeating a cryptographic scheme by systematically trying a large number of possibilities; for example, a large number of the possible keys in a key space in order to decrypt a message. In most schemes, the theoretical possibility of a brute force attack is recognized, but it is set up in such a way that it would be computationally infeasible to carry out. Accordingly, one definition of "breaking" a cryptographic scheme is to find a method faster than a brute force attack.

Brute Force Feature

After FIVE consecutive incorrect User or Admin PIN entries, the keypad will not respond and LED will turn off. The drive will need to be unplugged from the USB port and re-plugged.

If the user, unsuccessfully tries to **UNLOCK** the drive on the 10th try the keypad will lock and the LED will begin blinking **RED** quickly. Even after unplugging and re-plugging in the unit, the drive will remain locked and the LED will continue to blink rapidly.

Here are the steps to allow the user to unlock the keypad for 10 more attempts to unlock this drive.

1. Unplug the device from the computer

2. Push and hold the number five key and plug-in the drive

3. The LED will be blinking alternating **RED** and **GREEN** rapidly

4. Enter the PIN 5278879 and press **UNLOCK**.

5. The keypad will unlock and will be in the standby state with the LED solid **RED**, this will allow only 10 more attempts

6. After a total of 20 Attempts the drive will remain locked with the LED flashing **RED** quickly. You must now go through the reset process and reformat the drive to be able to use the drive again.

14. Setting a Self-Destruct PIN

1. Enter the Admin mode by pressing and holding **UNLOCK + 0** buttons for five seconds until the LED flashes **RED**. This indicates that you can enter the Admin PIN.

2. Enter the Admin PIN and press **UNLOCK**. The drive is in Admin Mode when the LED has changed to **BLUE**.

3. Once in Admin mode, press **UNLOCK + 3** buttons. LED will be alternating **BLUE** / **RED**.

4. Input in the PIN that you would like to use as the Self Destruct PIN and press **UNLOCK**.

5. If the Self Destruct PIN is accepted the LED flashes **GREEN**.

6. Immediately re-enter the new PIN and press **UNLOCK**. If the LED stays solid **GREEN** for two seconds and then goes to solid **BLUE**, the Self Destruct PIN was added successfully.

7. To delete the Self Destruct PIN, you will need to delete all of the User PINs. Disconnect and re-connect the drive, then refer to the instructions on the previous page - Deleting User PINs.

The self-destruct feature allows you to set a PIN which can be used to perform a crypto-erase on the entire drive. When used, the self-destruct PIN will **delete ALL data, Admin/User PINs** and then unlock the drive. Activating this feature will cause the Self-Destruct PIN to become the new Admin PIN and the diskAshur PRO will need to be partitioned and formatted before any new data can be added to the drive.

Once the Self-Destruct PIN is set, the feature can be activated by plugging the drive into a USB port, entering the self-destruct PIN and then press the unlock button.

15. Performing a Complete Reset

To perform a complete reset of the drive, do the following:

1. Press and hold the **LOCK** button while you attach the diskAshur PRO to an available USB port on your computer. The LED will flash **RED**, **GREEN** and **BLUE** alternately.

2. Release the **LOCK** button.

3. Press and hold **LOCK + UNLOCK + 2 buttons** for 10 seconds until the LED turns Solid **GREEN** for two seconds, followed by Solid **BLUE** and Solid **GREEN**. You have successfully reset the diskAshur PRO.

16. Initializing and formatting the diskAshur PRO after a complete reset

A complete reset of the diskAshur PRO will erase all information and partition settings. You will need to initialize and format the diskAshur PRO.

To initialize your diskAshur PRO, do the following:

1. After a complete reset, attach the diskAshur PRO to the computer.
2. Press **UNLOCK + 9 buttons**. The LED will change to Solid **BLUE** / Blinking **GREEN**.
3. Enter the new Admin PIN and press **UNLOCK** key. If accepted the LED will
   flash 3 short blinks of the **GREEN** LED, then return to Solid **BLUE** and Blinking
   GREEN.
4. Re-enter the Admin PIN and press the **UNLOCK** key. If accepted the **GREEN**
   LED will be Solid for 3 seconds.
5. LED will then turn **BLUE** and remain in Admin mode for 30 seconds or if the
   LOCK key is pressed, will return the drive to a standby state.
6. The Admin PIN is now set and will allow access to the drive or the Admin
   features.
7. To **UNLOCK** the drive, enter the new PIN and press **UNLOCK**.
8. **Windows 7** and earlier: Right-click **My Computer**, and then click **Manage** from
   the Windows desktop.
   Windows 8: Right click left corner of desktop and select **Disk Management**.

9. In the Computer Manage window, click **Disk Management**. In the Disk Management window, the diskAshur PRO is
   recognized as an unknown device that is uninitialized and unallocated.
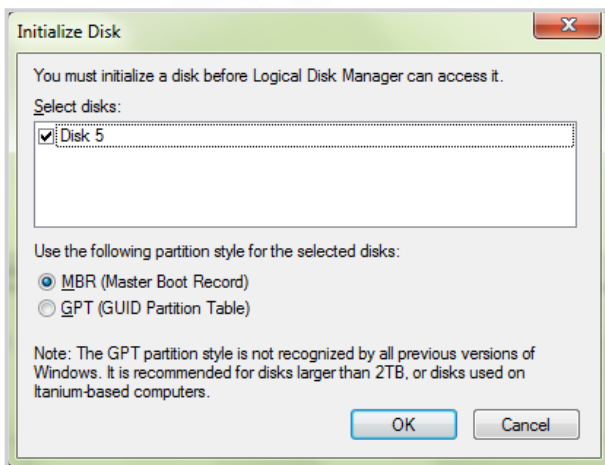
> ⚠️   **Note:** If the Initialize Disk Wizard window opens, click **Cancel.**
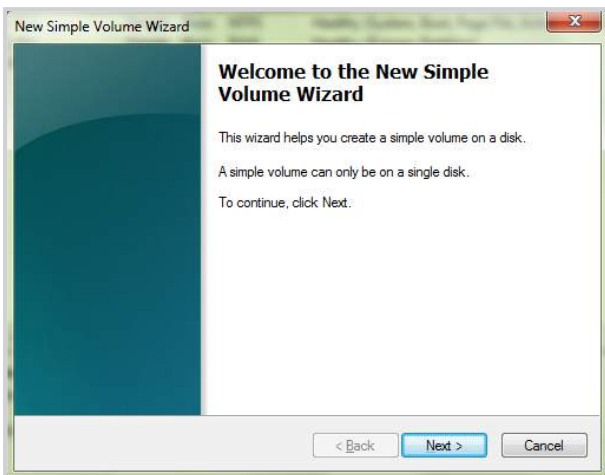
10. Right-click Unknown Disk, and then select Initialize Disk.
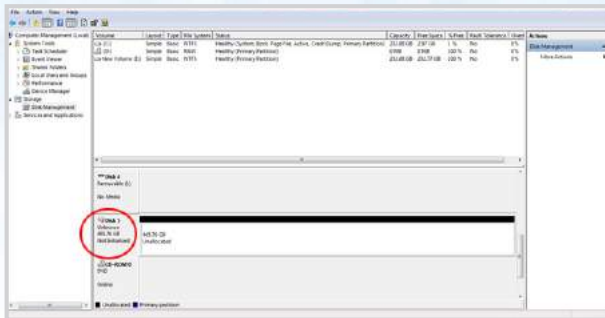
11. In the Initialize Disk window, click **OK**.

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

9. Click **Next**.

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

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

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

13. Click **Finish**.

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

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

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

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

To log off the diskAshur PRO, double-click Safely Remove Hardware on the Windows desktop and remove the diskAshur PRO from your computer.

Attention: To ensure the data integrity of your diskAshur PRO, be sure to lock or log off diskAshur PRO if you are:

- Away from your computer.
- Using the switching user function by sharing a computer with others.

18. diskAshur PRO Setup for Mac OS

Your diskAshur PRO is preformatted in NTFS for Windows. To reformat the drive to a Mac compatible format please read below.

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

To format the diskAshur PRO:

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

2. Click the 'Erase' tab.

3. Enter a name for the drive. The default name is Untitled. The drive's name will eventually appear on the desktop.

4. Select a volume format to use. The Volume Format dropdown menu lists the available drive formats that the Mac supports. The recommended format type is 'Mac OS Extended (Journaled).'

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

19. Troubleshooting

This section contains troubleshooting information for the diskAshur PRO. If you encounter any of the following problems when using diskAshur PRO, refer to the corresponding answers.

Q: What can I do if I forget the User PIN?

A: Use your Admin PIN to enter Admin Mode, and then create another User PIN in Admin Mode.

Q: What can I do if I forget the Admin PIN?

A: There is no other way to retrieve the Admin PIN except a complete reset of diskAshur PRO. After a complete reset, all data will be lost and you will need to initialize, allocate and format the diskAshur PRO manually.

Q: Why did the operating system not recognize the diskAshur PRO after I enter the User Mode and completely reset the computer?

A: You need to initialize, allocate and format the diskAshur PRO manually. For more information, refer to Initializing and formatting the diskAshur PRO after a complete reset in this manual.

Q: How do I use the diskAshur PRO without a PIN?

A: As a full disk encryption product, the diskAshur PRO can never be used without a PIN.

Q: What encryption algorithm is used in this product?

A: The diskAshur PRO uses AES 256-bit algorithm.

Q: Why could I not initialize, partition or format the diskAshur PRO?

A: Ensure that you have administrator privileges. You will need Admin privileges to use the Disk Management Utility.

Q: The LED is blinking RED and I can't enter a code. Why?

A: Somebody has tried to access the drive and the code has been entered 10 times incorrectly (see Brute Force section of this manual).

Q: Do I require 'Admin Rights' for the diskAshur PRO to work?

A: No, since the diskAshur PRO does not require any software to be installed and the encryption/decryption is performed in Hardware on the drive itself, "Admin Rights" are not required.

Q: Why do the LEDs blink BLUE, RED and GREEN after I plug the drive in?

A: When you first plug the drive in, it does a self-test on the encryption components of the drive. If any component fails the test, the LED will stop on RED and the drive will not function.

Q: What is FIPS 140-2?

A: This is a government standard to accredit cryptographic modules. The government regulates certain industries that collect, store and/or transfer sensitive data to use security that meets this standard. For a general explanation: http://en.wikipedia.org/wiki/FIPS_140-2

Q: What kind of speed can be expected out of this drive?

A: USB speed will be affected by a variety of factors (USB type – 1, 2 or 3, Host controller, Driver version, hard drive read/write speeds, Operating System). On average, if using a USB 3.0 port, speeds should be from 80+ MB/s for a newer rotating drive and 250+ MB/s for a newer SSD version. If you are experiencing lower than expected speeds, check to make sure you have the latest host controller driver available. If you are getting considerably less, make sure that you are plugged into a USB 3 port. USB 3 ports use a blue center contact.

Q: Is there any way to recover my data if I forget the PIN?

A: If an Admin PIN has been previously set, the Admin PIN can be used to unlock the drive and recover the data. If you forget the PIN and do not have an Admin PIN, the drive can be re-set so it can be used again, but the data cannot be recovered.

Q: Why does the LED indicate an error when I try to change the PIN?

A: PIN requirements for this drive must meet a minimum security level. There are several combinations that are not allowed, such as, all repeating numbers, sequential number going up or down. The PIN must also be a minimum of **7** digits and cannot be longer than **16** digits.

Q: My diskAshur PRO locks for no reason when connected to my computer whilst I'm using it, what is causing this?

A: The issue you are having is being caused by power saving settings on your PC or Laptop so please see below and make the appropriate changes to your computer and this will stop the diskAshur PRO from locking as when your computer is power saving it switches off data to the USB ports and our products see that as `Disconnect` and are designed to lock when this is detected.

Microsoft Windows
Doing the following will prevent Windows from switching off the diskAshur PRO, go to **'Control Panel'** & **'Power Options'** , the easier option is to disable power saving which means stopping the computer from `Sleeping` see below;
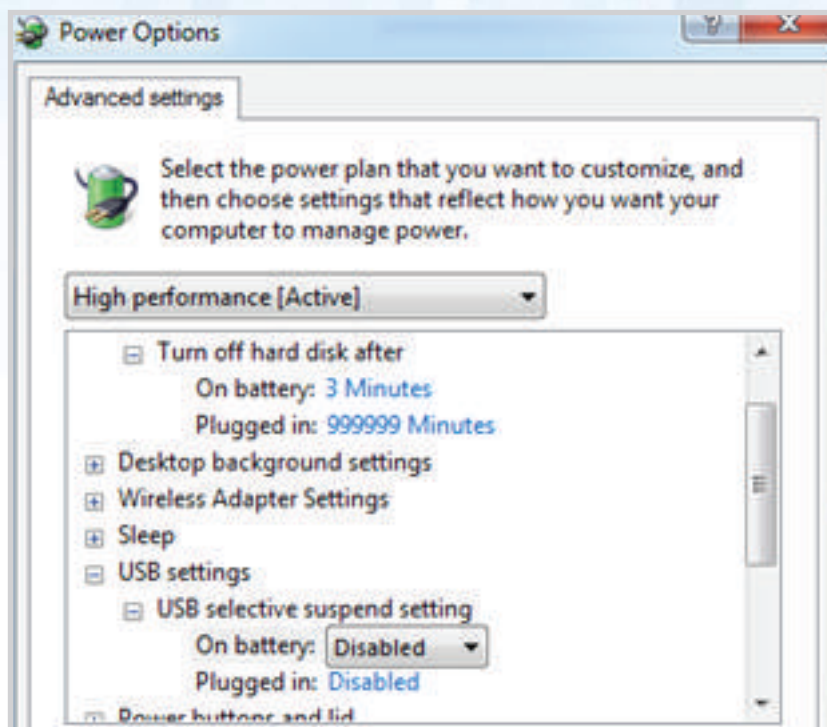

In addition go into `Advanced Settings` in `Power Option` to disable the following:

- Ensure the computer is set to sleep: Never (as above)
- Turn off hard disk after: 999999 Minutes
- USB selective suspend setting: Disabled

This will keep the diskAshur PRO connected to the computer continuously on.

Apple Mac

The diskAshur PRO keeps locking after 5-10 minutes on the Macs – This will be due the Mac's power saving as there is a setting to switch off hard drives that are idle after a fix period of time see below;

The settings in Energy Saver preferences affect what happens when your Mac is left unattended for a period of time that you specify. Disable `Put the hard disk(s) to sleep when possible` to prevent the diskAshur PRO going to sleep and so not locking. You will also need to stop the computer from sleeping to prevent the diskAshur PRO from locking.
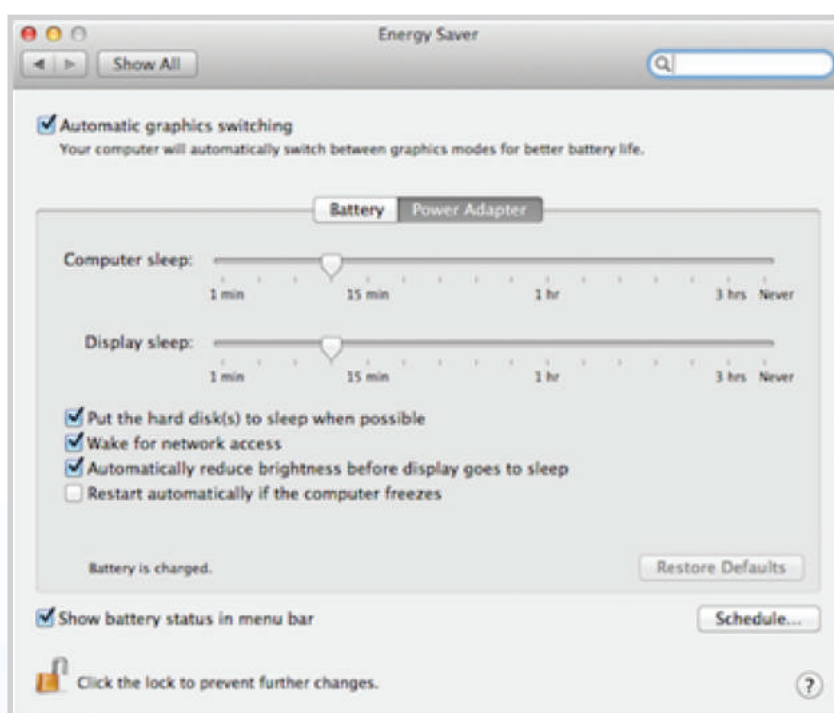
Note For Windows 8.1 users; You will need to install a Windows update (KB2919355) as well as follow the steps on pages 18 &19. Please go to this link and choose Method 2; http://support.microsoft.com/kb/2919355. Once the download option appears select KB2919355 and then download and install.

Q: My diskAshur PRO locks when my computer sleeps/hibernates how can I stop this?

A: The only way to prevent this is by changing the power settings (Windows computers) of the computer so that it only switches of the monitor on hibernation/sleep and keeps power to hard drives and USB. On Apple MAC computers going to the power settings in `System Preferences` and clicking the do not suspend USB will keep the drive alive even if the MAC goes into full hibernation.

Q: The diskAshur PRO will not power on when connected to my computer?

A: This only happens when the computer the diskAshur PRO is connected to cannot provide enough power from the USB port to power the drive. This issue only appears on much older computers and/or imbedded systems like USB enabled medical equipment. It can be resolved by either trying all the USB ports on the computer or system as some ports can have less power than others or failing that use the USB Y-Power cable supplied with the diskAshur PRO to ensure the correct power.

Q: I want to use my diskAshur PRO with different Operating Systems how can that be done?

A: To make the diskAshur PRO universally compatible with all the most common Operating Systems and embedded systems like USB enabled medical equipment, requires the drive to be formatted using the FAT file system. This is done by using `Disk Management` in Windows, `Disk Utility` on MAC OS/x or MKFS in Linux.

Q: How many unique User ID's can I create?

A: The Administrator feature allows enrollment of up to five (5) unique User ID's and one (1) Administrator. If a user forgets their PIN, the diskAshur PRO can be unlocked using the Admin PIN.

20. Technical Support

iStorage provides the following helpful resources for you:

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

E-mail correspondence
support@istorage-uk.com

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

21. Warranty and RMA information

Two Year Warranty:

iStorage offers a 2-year warranty on the iStorage diskAshur PRO against defects in materials and workmanship under normal use. The warranty period is effective from the date of purchase either directly from iStorage or an authorised reseller.

Disclaimer and terms of warranty:

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

iStorage diskAshur PRO® Manual – v 2.1