

datAshur[®]



User Guide

Copyright © iStorage Limited, 2011, 2012. 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 substantively 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 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 use or operation of the product, whether or not iStorage was apprised of the possibility of such damages



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



iStorage datashur is developed and manufactured by iStorage Ltd. and is based on DataLock® technology licensed from ClevX, LLC

OS and Host Independent



Table of Contents

Introduction	4
LED Indicators	4
How to change User PIN	5
How to create a new User Pin	6
How to configure the datAshur with Windows after a Complete reset	6-7
How to unlock drive with User PIN	8
How to lock the iStorage datAshur	8
How to create an Admin PIN	8-10
How to unlock with Admin PIN	10
How to change Admin PIN	11
How to reset the drive	12
Frequently asked questions	13-14



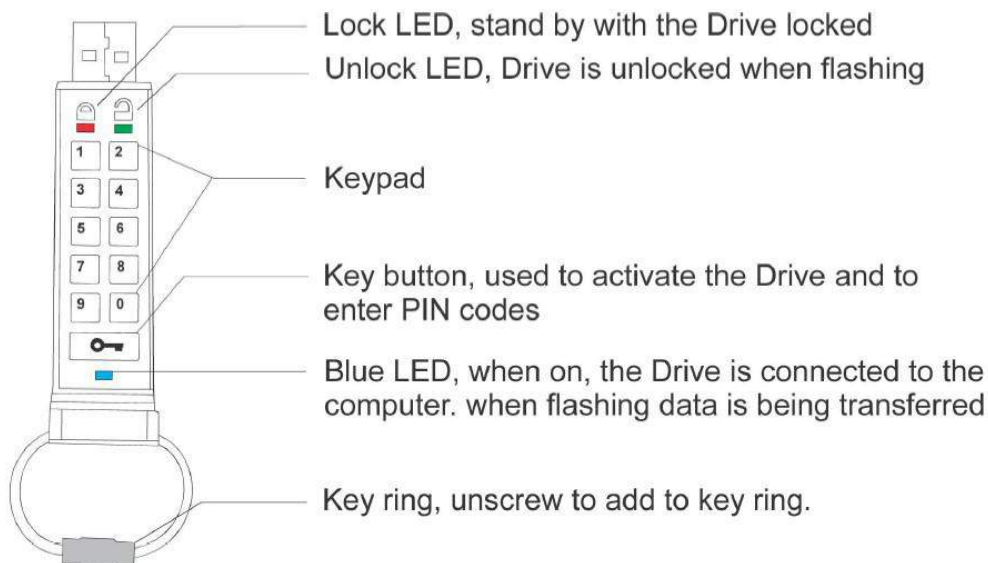
Introduction

Thank you for purchasing the iStorage datAshur, a PIN activated, hardware encrypted USB flash drive.

The iStorage datAshur uses military grade AES 256-bit hardware encryption, which encrypts all data stored on the drive in real-time. The datAshur requires no software and is OS and host independent. The datAshur incorporates a rechargeable battery allowing the user to enter a 7-15 digit PIN (Personal Identification Number) onto the on-board keypad before connecting the drive to the USB port. Should the drive be lost or stolen, the user can rest assured that all data held on the datAshur is safe and cannot be accessed by any unauthorised person.

The datAshur can be created with both User and Admin PINs, making it perfect for corporate and government deployment.

As the iStorage datAshur is unlocked with the on-board keypad and not with the keyboard, it is not vulnerable to software/hardware based key-loggers or brute force attacks.



1. LED indicators

	Blinking	Key is unlocked, plug into USB port		On solid	Key connected to USB port
	Blinking	Key is locked		On solid	Key does not have a User PIN
	Blinking	Data is being transferred		On solid	Key connected with host computer
	Blink alternately	Error		On solid	Key accepting new PIN code
	Blink together	Accepting User PIN		Double blink	Accepting Admin PIN
	Intensify	Security self testing			



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



Note: Unless otherwise noted, all INSTRUCTION steps are performed when datAshur is not connected to a computer.

CAUTION

The datAshur is shipped with a default User PIN of 1-1-2-2-3-3-4-4 and although it can be used straight out of the box with the default PIN, for security reasons, we highly recommend that a new User PIN be created immediately by following instructions under heading 2 "How to change User PIN".

2. How to change User PIN

CAUTION

If you forget your User PIN and no Admin PIN exists, or you forget both PINs, all data will be inaccessible.

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain repeating numbers/letters, e.g., (3-3-3-3-3-3)
- Must not contain sequential numbers/letters, e.g., (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Instructions	LED Activity
1. Press the Key button	will blink together (Factory default PIN: 1-1-2-2-3-3-4-4)
2. Enter your User PIN and press the Key button	will illuminate together for approximately 4 seconds, and then:- will blink indicating correct PIN entry
3. Press and hold the Key button for 3 seconds	will be on
4. Enter a new PIN number (The number must be 7 - 15 digits)	
5. Press the Key button to store the new PIN 6. Re-enter the new PIN number	will blink together
7. Press the Key button to confirm the new PIN	will illuminate together for approximately 4 seconds, and then:- will blink if both PIN entries match. Drive is now ready to use will blink alternately if PIN entry error. restart from step 3

Note: If a mistake was made while defining a new PIN or the procedure was not completed, the drive will retain the old PIN.

3. How to create a new User PIN
















A new encryption key is automatically created under the following circumstances:

- After hacking detection has been triggered by 10 successive failed attempts to unlock.
- Drive has been manually reset (see heading 10).

When either of the above two scenarios occur, it will be necessary to set a new User PIN by following the instructions below.

User PIN requirements:

- Must be between 7-15 digits in length
- Must not contain repeating numbers/letters, e.g., (3-3-3-3-3-3)
- Must not contain sequential numbers/letters, e.g., (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

Instructions	LED Activity
1. Press the Key button for 3 seconds 	  will be on
2. Enter a new User PIN	  will be on
3. Press the Key button to save 	  will blink together if accepted
4. Re-enter the new PIN number & press the Key button 	  will illuminate together for approximately 4 seconds, and then:-   will blink indicating correct PIN entry   will blink alternately if PIN entry error, restart from step 3

Note: A user PIN can only be defined when the red LED is lit in a constant state or changed when the green LED is blinking (unlocked). Neither User nor Admin PINs can be created while drive is connected to a host computer.

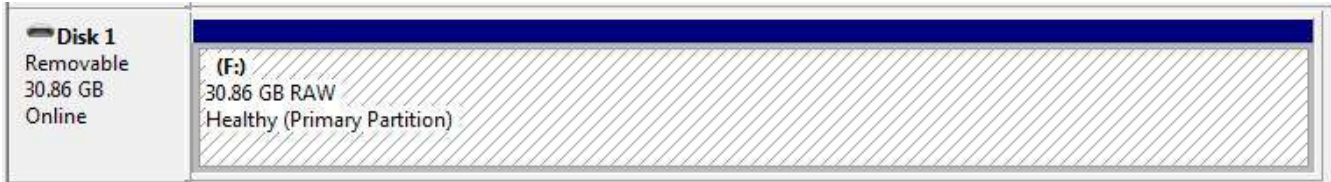
4. How to configure the datAshur with Windows after a complete reset

In the event that hacking detection has been triggered by entering the incorrect PIN 10 times in succession or the drive has been reset, all data on the drive will be lost forever. Once a new User PIN has been created, the datAshur drive will need to be initialised and formatted.

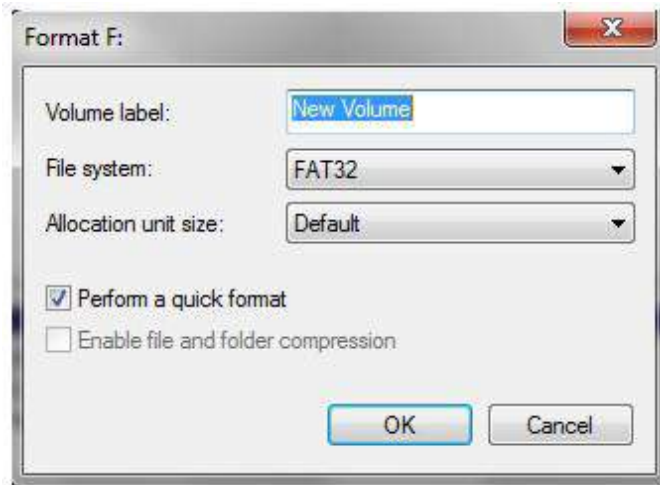
To initialise your datAshur drive, do the following:

1. Create a new User PIN (see point 3 above)

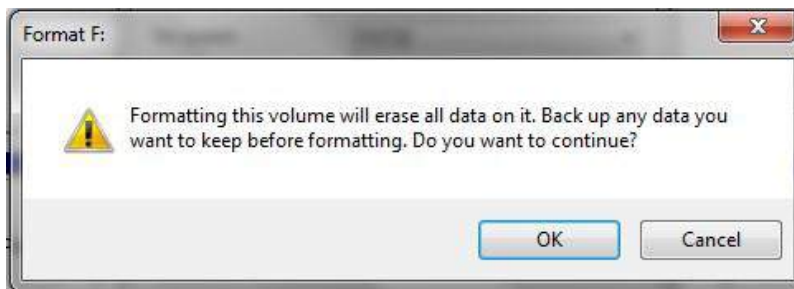
2. Unlock the datAshur drive by entering the new User PIN and connect to a computer
3. Right-click MY Computer and then click Manage.
4. In the Computer Management window, click "Disk Management". In the "Disk Management" window, the datAshur drive is recognised as a removable device in raw format.
5. Do the following to make the drive recognised as a basic drive.
 - Right-click Removable Raw drive, in the blank area under the unallocated section and the select "Format"



6. The Format window opens.













7. Select FAT32 or NTFS depending on your needs and click OK



8. Click OK on the Format warning window
9. While the datAshur drive is formatting the Blue LED will be flashing
10. When finished, the Blue LED will be on solid and your datAshur drive is ready for use.

5. How to unlock drive with User PIN

Once the User PIN is created, all data stored on the iStorage datAshur is encrypted, in hardware, to the AES 256-bit CBC specification. In order to access the data stored on the drive, you must first unlock the drive with your User PIN.

Instructions	LED Activity
1. Press the Key button 	  will blink together
2. Enter your User PIN (Factory default PIN: 1-1-2-2-3-3-4-4)	  will illuminate together for approximately 4 seconds, then:-  will blink indicating correct PIN entry
3. Press the Key button 	 will blink if incorrect PIN was entered
4. Insert your iStorage datAshur into USB Port	 will be on  will be on or blink for activity

Note: Once unlocked, the Green LED will blink for 30 seconds, within which time the drive needs to be connected to the USB port. If no connection is detected within 30 seconds, the drive will lock and you will need to start the process of unlocking again.

6. How to lock the iStorage datAshur

The iStorage datAshur automatically locks when unplugged from the host computer or power to the USB port is turned off. Data is kept locked using AES 256-bit CBC encryption.

7. How to create an Admin PIN

An Admin PIN is a useful feature for corporate deployment, for example:

- Recovering data from a drive and configuring a new User PIN in the event an employee has forgotten their PIN
- Retrieving data from a drive if an employee leaves the company

CAUTION

Entering the Admin PIN to access a locked drive will clear the User PIN. If a user forgets their PIN, access to their drive is regained by defining a new user PIN. For security reasons, we highly recommend that a new User PIN be created immediately once the drive has been unlocked using the Admin PIN.

Admin PIN requirements:

- Must be between 7-15 digits in length
- Must not contain repeating numbers/letters, e.g., (3-3-3-3-3-3)
- Must not contain sequential numbers/letters, e.g., (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

If the drive has been reset or hacking detection has been triggered (i.e., no User or Admin PIN exist), the instructions below can be followed. If a User PIN already exists, the datAshur must be unlocked first with the user PIN by following instructions under heading 5, before an Admin PIN can be created by following instructions below.















Instructions	LED Activity
1. Press the key button twice  holding the key for 3 seconds on 2 nd Press	  will blink once then remain lit
2. Enter a new Admin PIN	  will be on
3. Press key button 	  will double blink
4. Re-enter new Admin PIN	
5. Press key button 	  will illuminate together for approximately 4 seconds, and then:-  will blink indicating correct PIN entry   will blink alternately if PIN entry error restart from step 1

Figure 1 below shows the green blinking characteristics when the drive is opened in User mode versus Admin mode.

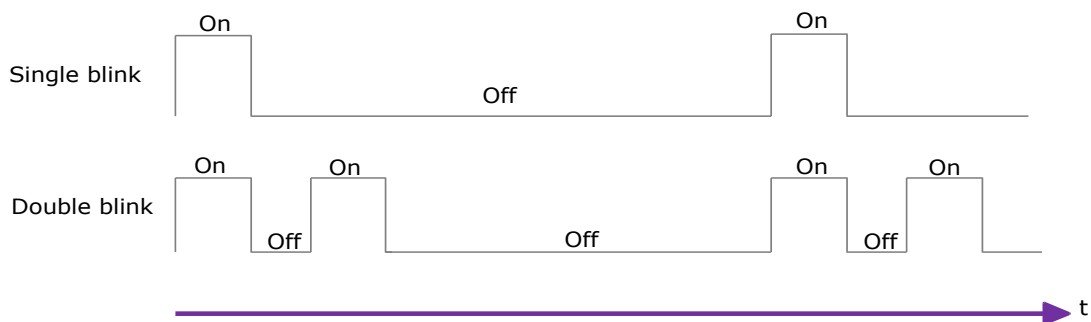


Figure 1: User Mode single blink LED output compared to Admin Mode double blink

Figure 2 below shows the difference between pressing KEY button to set the User PIN vs setting the Admin PIN.

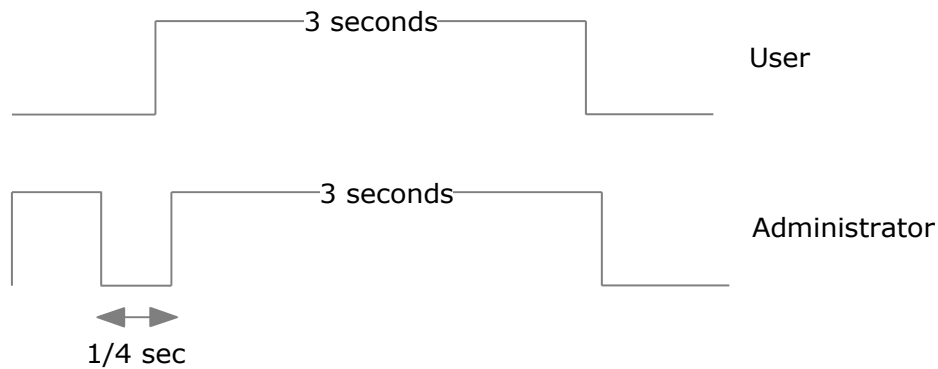














Figure 2: Key entry for User/Admin mode selection

8. How to unlock with ADMIN PIN

⚠ CAUTION

Entering the Admin PIN to unlock the drive will reset the User PIN. For security reasons, we recommend that a new User PIN be created immediately once the drive has been unlocked using the Admin PIN.

Instructions	LED Activity
1. Press the key button twice in succession (double click)  	  will double blink together
2. Enter the Admin PIN	
3. Press key button 	  will illuminate and then   will double blink indicating correct PIN entry  will blink if incorrect PIN entry
4. Insert your iStorage datAshur into USB port within 30 seconds	 will be on  will be on or blink for activity

Note: Green LED will blink for 30 seconds, within which time the drive needs to be connected to the USB port, if no connection is detected within 30 seconds, the drive will lock and you will need to start the process of unlocking again.

9. How to change ADMIN PIN






















⚠ CAUTION

Changing the Admin PIN will reset the User PIN. For security reasons, we recommend that a new User PIN be created immediately once the drive has been unlocked using the Admin PIN.

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain repeating numbers/letters, e.g., (3-3-3-3-3-3)
- Must not contain sequential numbers/letters, e.g., (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

















Once an Admin PIN has been created, the datAshur needs to be unlocked by the administrator in order to change the Admin PIN. The Admin PIN cannot be changed from user mode.

Instructions	LED Activity
1. Press the key button twice in succession (double click)  	 will double blink together
2. Enter the Admin PIN	 will illuminate together
3. Press key button 	 will illuminate together, then:-  double blinks  will blink if incorrect PIN was entered
4. Press the key button twice holding the key for 3 seconds on 2 nd Press  	 will remain lit
5. Release the key button 	 will blink twice and then will remain lit
6. Enter desired Admin PIN	 will illuminate together
7. Press key button 	 will double blink
8. Re-enter New Admin PIN	 will double blink
9. Press key button 	 will illuminate together, then:-  double blinks  will blink alternately if PIN entry error. restart from step 4

10. How to Reset the Drive

In case both Admin and User PINs have been forgotten or if you would like to delete all data stored on the drive and create new User and Admin PINs, follow the instructions below. The reset process will clear all PINs and encryption keys. This means a new User PIN will have to be defined in order to re-enable the drive. Also, since this will force the creation of a new encryption key, the drive will have to be reformatted (see heading 4).

⚠ CAUTION
Resetting the datAshur will make all data on the drive inaccessible forever.

Instructions	LED Activity
1. Press the Key button 	  will blink together
2. Press the Key button 	 will blink
3. Press and hold the Key button and the number 2 button for 3 seconds  	  will blink together
4. Enter 9 - 9 - 9 and press the Key Button    	LEDs will turn off
5. Press the Key button 	 will be on solid
Note: When the  is on and solid, a new user PIN will need to be set prior to use.	

11. FREQUENTLY ASKED QUESTIONS

a. How to unlock drive if battery is dead

Your iStorage datAshur is supplied with a built-in rechargeable battery. If the battery is fully discharged, you may still continue to use the product by following the instructions below:

- a) Connect the iStorage datAshur to a USB port on any computer
- b) While the datAshur is connected to the computer, enter the User or Admin PIN to unlock the drive
- c) Whilst connected to the USB port, the internal battery will automatically charge. We recommend you keep the drive connected for 1 hour to fully charge the battery.

b. Forgotten your PIN

If you forget the User and Admin PINs, there is absolutely no way of gaining access to the data stored on the drive, there are no backdoors into the drive. You may continue to re-use the iStorage datAshur by resetting it, however by doing so all data previously stored on the drive will be lost forever.

To reset the iStorage flash drive, follow instructions under heading 10. Once that is done, the following occurs:

- The existing encryption key is deleted
- The User and Admin PINs are deleted
- All data previously stored on the drive will be lost forever

c. Brute Force Hack Defence Mechanism

After 10 consecutive incorrect PIN attempts, the following occurs:

- The existing encryption key is deleted
- The User and Admin PINs are deleted
- All data previously stored on the drive will be lost forever

The iStorage datAshur, unlike other similar drives, is preloaded with an unlimited number of randomly generated encryption keys. Each time hacking is detected (i.e. the wrong PIN is entered a total of 10 consecutive times), the current encryption key is deleted and once a new User PIN is created the drive randomly generates a new encryption key. Because of this, the iStorage datAshur will have to be formatted after each time the defence mechanism is triggered.

d. Will unlocking the drive with the Admin PIN delete the User PIN?

Entering the Admin PIN to access a locked drive will clear the User PIN. If a user forgets their PIN, access to their drive is regained by defining a new user PIN. For security reasons, we highly recommend that a new User PIN be created immediately once the drive has been unlocked using the Admin PIN.

Therefore, the User PIN is deleted when:

The Admin PIN is used to unlock the drive. A new User PIN will need to be created.
When the Admin PIN is changed. A new User PIN will need to be created.

iStorage Limited
iStorage House
13 Alperton Lane
Perivale, Middlesex
UB6 8DH
www.istorage-uk.com
info@istorage-uk.com
Tel: +44 (0) 20 8991-2620
Fax: +44 (0) 20 8991-6277