datashur™

User Guide

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

Table of Contents

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 customer 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.

⚠ 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".

1. LED indicators

LED (LAMP) ACTIVITY	ACTION BEING PERFORMED
All LEDs are off	drive is locked and secure – all data is encrypted
Green blink	drive is unlocked and ready for use
Green solid	drive connected to powered USB port
Blue solid	drive connected to host computer and is idle
Blue blink	data exchange with host computer
Red LED blink	drive is locked and secure – all data is encrypted
Red constantly on	No User PIN created
Red and Green LEDs blink together	accepting User PIN input
Red and Green LEDs double blink	accepting Admin PIN input
Red and Green LEDs constantly lit	drive is accepting new PIN
Red and Green LEDs blink alternately	Error

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

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., (3-3-3-3-3-3-3)
- 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)

INSTRUCTION	LED ACTIVITY
1. Press button	Red and Green LEDs blink together
2. Enter user PIN to unlock drive and press	Green blink
3. Press and hold button for 3 seconds	Red and Green will illuminate together
4. Enter new User PIN	Red and Green illuminated
5. Press button	Red and Green blink in unison
6. Re-enter new User PIN	Red and Green blink in unison
7. Press button	Green blink if 1st and 2nd entries match Red and Green blink alternately if PIN entry error If Red and Green LEDs blink alternately, 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 9).

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., (3-3-3-3-3-3-3)
- 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)

INSTRUCTION	LED ACTIVITY
1. Press and hold button for 3 seconds	Red and Green will illuminate
2. Enter a new User PIN	Red and Green illuminated
3. Press button	Red and Green blink in unison
4. Re-enter new User PIN	Red and Green blink in unison
5. Press button	Green blink if 1st and 2nd entries match Red and Green blink alternately if PIN entry error If Red and Green LEDs blink alternately, restart from step 1

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 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.

INSTRUCTION	LED ACTIVITY
1. Press the button	Red and Green will blink together
2. Enter the User PIN	Red and Green will continue to blink together
3. Press button	Green will blink if user entered correct PIN Red will blink if incorrect PIN was entered If Red and Green LEDs blink alternately, restart from Step 1
4. Insert iStorage datashur into USB port	Green LED will illuminate in constant state Blue will illuminate and flicker

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.

5. 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.

6. 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., (3-3-3-3-3-3-3)
- 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 4, before an Admin PIN can be created by following instructions below.

INSTRUCTION	LED ACTIVITY
1. Press the button twice holding button for 3 seconds on the 2nd press	Red and Green will blink once then remain lit
2. Enter a new Admin PIN	Red and Green illuminated
3. Press button	Red and Green double blink
4. Re-enter new Admin PIN	Red and Green continue to double blink
5. Press button	Green double blink if 1st and 2nd entries match Red and Green blink alternately if PIN entry error If Red and Green LEDs blink alternately, restart from step 1

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

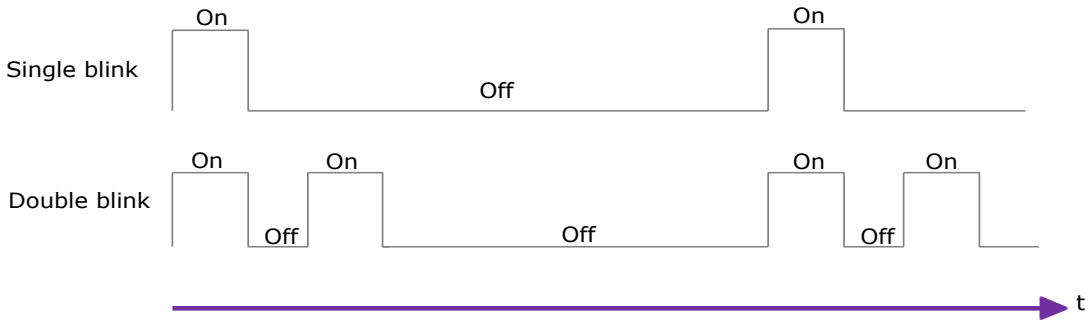

Figure 1: User Mode single blink LED output compared to Admin Mode double blink

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

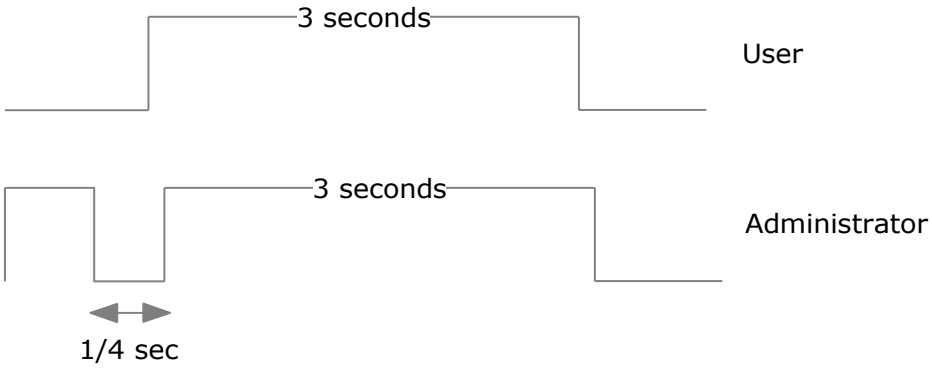

Figure 2: Key entry for User/Admin mode selection

7. How to unlock with ADMIN PIN

⚠ CAUTION

Entering the Admin PIN to unlock the drive will reset the User PIN. A new User PIN MUST be created immediately once the drive has been unlocked using the Admin PIN.

INSTRUCTION	LED ACTIVITY
1. Press the button twice in succession (similar to double-clicking a mouse)	Red and Green will double blink together (figure 1, on page 7)
2. Enter the Admin PIN	Red and Green will continue to blink together
3. Press button	Green will double blink if admin entered correct PIN Red will blink if incorrect PIN was entered If Red and Green LEDs blink alternately, restart from step 1
4. Insert iStorage datashur into USB port within 30 seconds	Green LED will illuminate in constant state Blue will illuminate and flicker

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.

8. How to change ADMIN PIN

⚠ CAUTION

Changing the Admin PIN will reset the User PIN. A new User PIN MUST be created immediately once the Admin PIN has been changed.

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain repeating numbers/letters, e.g., (3-3-3-3-3-3-3)
- 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.

INSTRUCTION	LED ACTIVITY
1. Press the button twice in succession (similar to double-clicking a mouse)	Red and Green will double blink together (figure 2, on page 8)
2. Enter Admin PIN	Red and Green illuminated
3. Press button	Green will double blink if admin entered correct PIN Red will blink if incorrect PIN was entered
4. Press the button twice holding for 3 seconds on the 2nd press	Red and Green will remain lit
5. Release button	Red and Green will blink twice then remain lit
6. Enter desired Admin PIN	Red and Green illuminated
7. Press button	Red and Green double blink
8. Re-enter new Admin PIN	Red and Green continue to double blink
9. Press button	Green double blink if 1st and 2nd entries match Red and Green blink alternately if PIN entry error If Red and Green LEDs blink alternately, restart from Step 4

9. 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.

⚠ CAUTION

Resetting the datashur will make all data on the drive inaccessible forever.

INSTRUCTION	LED ACTIVITY
1. Press the button twice with a two seconds pause in between to wake the drive	Red blink
2. Press and hold & '2' buttons together for three seconds	Red and Green will illuminate together
3. Release buttons	Red and Green blink in unison
4. Enter 9-9-9	Red and Green blink in unison
5. Press button	Both LEDs will turn off
6. Press button again	Red lit in constant state (Indicates User PIN must be set prior to use, see 3. How to create a new User PIN)

FREQUENTLY ASKED QUESTIONS

1. 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.

2. 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 stored on the drive will be inaccessible.

To reset the iStorage flash drive, follow instructions under heading 9. Once that is done, the following occurs:

- A new encryption key is created
- The User and Admin PINs are deleted
- All existing data is no longer accessible
- A new User PIN must be set
- Drive must be reformatted

3. Brute Force Hack Defence Mechanism

After 10 consecutive incorrect PIN attempts, the following occurs:

- A new encryption key is created
- The User and Admin PINs are deleted
- All existing data is no longer accessible
- A new User PIN must be set
- Drive must be reformatted

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 causing the unit to randomly generate a new encryption key. The new 256-bit encryption key is created

once a User PIN is successfully set. Because of this, the iStorage datashur will have to be formatted after each time the defence mechanism is triggered.

iStorage Limited
Research House
Fraser Road
Greenford, Middlesex
UB6 7AQ
www.istorage-uk.com
info@istorage-uk.com
Tel: +44 (0) 20 8537-3435
Fax: +44 (0) 20 8537-3438