

datashur™



Руководство пользователя

© IStorage Limited, 2011

Авторское право © IStorage Limited, 2011 год. Все права защищены.

Windows является зарегистрированным товарным знаком Microsoft Corporation.

Все другие торговые марки и авторские права являются собственностью их соответствующих владельцев.

Распространение существенно видоизмененных версий данного руководства запрещено без точного разрешения владельца авторских прав. Распространение или переработка материалов в любом стандартном (бумажном) виде книги в коммерческих целях запрещено без письменного разрешения владельца авторских прав.

ДОКУМЕНТАЦИЯ ПРЕДОСТАВЛЯЕТСЯ КАК ЕСТЬ И НИКАКИХ ПРЯМЫХ ИЛИ КОСВЕННЫХ УСЛОВИЙ, ПРЕДОСТАВЛЕНИЙ И ГАРАНТИЙ, ВКЛЮЧАЯ ГАРАНТИИ ПРИГОДНОСТИ ДЛЯ КОНКРЕТНЫХ ТОВАРОВ ИЛИ ОТСУТСТВИЯ НАРУШЕНИЯ ПРАВ, ЗА ИСКЛЮЧЕНИЕМ СЛУЧАЕВ, КОГДА ТАКИЕ ЗАЯВЛЕНИЯ ДОЛЖНЫ БЫТЬ ЛЕГАЛИЗИРОВАНЫ.



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

OS and Host Independent



Содержание

Вступление 4 ст.
LED Индикаторы 5 ст.
Как изменить PIN-код пользователя 6 ст.
Как создать новый PIN-код пользователя 7 ст.
Как разблокировать устройство с помощью PIN-кода пользователя 8 ст.
Как заблокировать iStorage datashur 8 ст.
Как создать PIN-код администратора 9-11 ст.
Как разблокировать устройство с помощью PIN-кода администратора 11-12 ст.
Как изменить PIN-код администратора 12-13 ст.
Как выполнить «сброс» устройства 14 ст.
Часто задаваемые вопросы 15 ст.

Вступление



Благодарим Вас за покупку iStorage datashur, аппаратный шифрованный USB флэш-диск с PIN-кодом.

iStorage datashur - это безопасный, простой в использовании и доступный USB накопитель с доступом по PIN-коду и AES 256-битным аппаратным шифрованием военного класса. Datashur включает в себя аккумулятор позволяющий пользователю ввести 7-15- значный PIN-код на встроенной клавиатуре до подключения диска к порту USB. Все данные передаются в зашифрованном виде в режиме реального времени со встроенным аппаратным шифрованием системы и защищены от несанкционированного доступа или если ваш iStorage datashur потерян или украден. Datashur автоматически блокируется при отключении от компьютера или выключении USB порта.

В Datashur могут создаваться как пользовательские, так и администраторские PIN-коды, что делает его удобным для использования в различных корпоративных целях.

Так как iStorage datashur разблокируется с клавиатуры на корпусе устройства, а не с компьютерной клавиатуры, это делает невозможным атаки основанные на программных или аппаратных key-loggers или атаки перебором.

ПРЕДУПРЕЖДЕНИЕ

Datashur поставляется с PIN по умолчанию  1-1-2-2-3-3-4-4  и хотя PIN-код по умолчанию может быть использован сразу же, по соображениям безопасности, мы настоятельно рекомендуем, изменить PIN-код пользователя, следуя инструкциям в разделе №2 «Как изменить PIN-код пользователя»

1. LED индикаторы

LED (лампочка)	Активность	Какие действия выполняются
Все лампочки	Выключены	Устройство заблокировано – вся информация зашифрована
Зеленый	Мигает	Устройство разблокировано и готово к использованию
Зеленый	Непрерывно	Устройство подключено к USB порту
Синий	Непрерывно	Устройство подключено к компьютеру и находится в режиме ожидания
Синий	Мигает	Обмен данными с компьютером
Красный	Мигает	Устройство заблокировано – вся информация зашифрована
Красный	Непрерывно	Нет созданных PIN-кодов пользователя
Красный и зеленый	Мигают вместе	Подтверждение ввода PIN-кода пользователя
Красный и зеленый	Мигают дважды	Подтверждение ввода PIN-кода администратора
Красный и зеленый	Непрерывно	Устройство приняло новый PIN-код
Красный и зеленый	Мигают по очереди	Ошибка

Примечание:

Если не указано иное, все действия данной ИНСТРУКЦИИ выполняются при не подключенном к компьютеру устройстве.






2. Как изменить PIN-код пользователя

ПРЕДУПРЕЖДЕНИЕ

Если вы забыли свой PIN-код пользователя, а PIN-код администратора не существует, или вы забыли оба PIN-кода, все данные будут недоступны.

Требования к PIN-коду:

- Должен быть 7-15 цифр
- Не должен содержать повторяющихся цифр или букв, например, (3-3-3-3-3-3-3)
- Не должен содержать последовательных цифр или букв, например, (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1).

Действие	Индикация лампочек
1. Нажмите  кнопку	Красный и зеленый мигают вместе
2. Введите PIN-пользователя для разблокировки устройства и затем нажмите 	Зеленый мигает
3. Нажмите  кнопку и удержите 3 секунды	Красный и зеленый постоянно
4. Введите новый PIN-код пользователя	Красный и зеленый загорятся
5. Нажмите  кнопку	Красный и зеленый мигают вместе
6. Повторно введите новый PIN-код пользователя	Красный и зеленый мигают вместе
7. Нажмите  кнопку	Зеленый мигает, если первая и вторая пара введена. Красный и зеленый мигает попеременно, если ошибка ввода PIN-кода. Если красный и зеленый мигает поочередно, начните снова с шага №3

Примечание:

Если ошибка была допущена при определении нового PIN-кода или процедура не была завершена, устройство сохранит старый PIN-код.

3. Как создать новый PIN-код пользователя




Новый ключ шифрования создается автоматически при следующих обстоятельствах:

- После обнаружения попытки взлома, было 10 последовательных неудачных попыток, чтобы разблокировать устройство.
- Устройство было «сброшено» вручную (см. раздел 9).

В таком случае необходимо установить новый PIN-код пользователя, следуя инструкциям ниже.

Требования к PIN-коду пользователя:



- Должен быть 7-15 цифр
- Не должен содержать повторяющихся цифр или букв, например, (3-3-3-3-3-3-3)
- Не должен содержать последовательных цифр или букв, например, (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1).

Действие	Индикация лампочек
1. Нажмите  кнопку и удержите 3 секунды	Красный и зеленый загорятся
2. Введите новый PIN-код пользователя	Красный и зеленый горят
3. Нажмите  кнопку	Красный и зеленый мигают вместе
4. Повторно введите новый PIN-код пользователя	Красный и зеленый мигают вместе
5. Нажмите  кнопку	Зеленый мигает, если первая и вторая пара введена. Красный и Зеленый мигает попеременно, если ошибка ввода PIN-кода. Если Красный и Зеленый светодиоды мигают поочередно, начните снова с шага 1

Примечание: PIN-код пользователя может быть определен только тогда, когда Красный светодиод горит в постоянном состоянии или изменяется, когда Зеленый светодиод мигает (разблокированный). Ни Пользователя, ни Администратора PIN-коды не могут быть созданы в то время, когда диск подключен к компьютеру.

4. Как разблокировать устройство с помощью PIN-кода пользователя

Как только пользователь создал PIN-код, все данные, хранящиеся на iStorage datashur становятся сразу же зашифрованными на аппаратном уровне **AES 256-бит CBC спецификации**. Чтобы получить доступ к данным, хранящимся на диске, необходимо сначала разблокировать привод с помощью вашего пользовательского PIN-кода.

Действие	Индикация лампочек
1. Нажмите  кнопку	Красный и зеленый мигают вместе
2. Введите PIN-код пользователя	Красный и зеленый продолжают мигать вместе
3. Нажмите  кнопку	Зеленый мигает, если пользователь ввел правильный PIN-код. Красный мигает, если пользователь ввел неправильный PIN-код. Если Красный и Зеленый светодиоды мигают поочередно, начните снова с шага №1.
4. Вставьте iStorage datashur в USB порт	Зеленый будет гореть постоянно, синий загорится и мигнет

Примечание:

После разблокирования Зеленый светодиод будет мигать в течение 30 секунд, в течение которых устройство должно быть подключено к порту USB. Если соединение не обнаружено в течение 30 секунд, устройство заблокируется и вам придется начать процесс разблокировки снова.

5. Как заблокировать iStorage datashur

iStorage datashur автоматически блокируется с момента изъятия устройства из USB порта. Информация на устройстве заблокирована и зашифрована.

6. Как создать PIN-код администратора

PIN-код администратора является полезной функцией для корпоративного использования, например:

- Восстановление данных с устройства и настройки нового PIN-кода пользователя в случае работник забыл свой PIN-код
- Получение данных с диска, если сотрудник уходит из компании

ПРЕДУПРЕЖДЕНИЕ

Ввод PIN-кода Администратора для доступа к заблокированному диску приведет к удалению пользовательского PIN-кода. Если пользователь забыл свой PIN-код, доступ к его диску восстанавливается посредством определения нового Пользовательского PIN-кода. Из соображений безопасности, мы настоятельно рекомендуем, чтобы новый пользовательский PIN-кода был создан сразу, как только диск был разблокирован при помощи PIN-кода Администратора.

Требования к PIN-коду администратора:

- Должен быть 7-15 цифр
- Не должен содержать повторяющихся цифр или букв, например, (3-3-3-3-3-3-3)
- Не должен содержать последовательных цифр или букв, например, (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1).

При запуске если диск был восстановленным или был обнаружен взлом (т.е. не существует Пользователя PIN-кода или Администратора PIN-кода), приведенным ниже инструкциям можно следовать. Если PIN-код Пользователя уже существует, datashur должен быть сначала разблокирован при помощи Пользовательского PIN-кода, следуя инструкциям в разделе 4, перед тем, как будет создан PIN-код Администратора, следуя инструкциям ниже.




Действие	Индикация лампочек
1. Нажмите  кнопку дважды и удерживайте ее 3 секунды на втором нажатии	Красный и зеленый мигают один раз, затем остаются гореть
2. Введите новый PIN-код Администратора	Красный и зеленый светятся
3. Нажмите  кнопку	Красный и зеленый двойное мигание
4. Повторно введите новый PIN-код Администратора	Красный и зеленый продолжают двойное мигание
5. Нажмите  кнопку	Зеленый два раза мигает, если первая и вторая запись правильная. Красный и Зеленый мигают попеременно, то это ошибка ввода PIN-кода. Если Красный и Зеленый светодиоды мигают поочередно, начните снова с шага №1.

Рисунок 1 показывает характеристики зеленого мигающего огонька, когда диск был открыт в режиме пользователя по сравнению с режимом администратора.

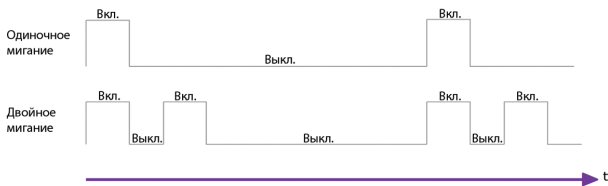


Рисунок 1: Пользовательский Режим индикации лампочки (LED) по сравнению с Администраторским Режимом удваивает мигание


Рисунок 2 показывает разницу между нажатием клавиши  кнопки, чтобы задать PIN-код пользователя в отличие от настроек администратора.





Рисунок 2: Ключевой вход для выбора режима Пользователь/Администратор

7. Как разблокировать с помощью PIN-кода Администратора

ПРЕДУПРЕЖДЕНИЕ

Ввод PIN-кода администратора для разблокирования диска приведет к сбросу пользователя PIN-кода. Новый PIN-код Пользователя ДОЛЖЕН БЫТЬ создан сразу же, как только диск был разблокирован с использованием PIN-кода администратора.

Действие	Индикация лампочек
1. Нажмите  кнопку два раза подряд (похоже на двойной щелчок мыши)	Красный и зеленый мигают удвоенно вместе (рис. 1, на стр. 10)
2. Введите PIN-код Администратора	Красный и зеленый продолжают мигать вместе

3. Нажмите  кнопку	Зеленый два раза мигает, если администратор ввел правильный PIN-код. Красный будет мигать, если неверный PIN-код был введен. Если Красный и Зеленый светодиоды мигают поочередно, начните снова с шага №1.
4. Вставьте IStorage datashur в USB-порт в течение 30 секунд	Зеленый будет гореть постоянно, синий загорится и мигнет

Примечание:

После разблокирования Зеленый светодиод будет мигать в течение 30 секунд, в течение которых устройство должно быть подключено к порту USB. Если соединение не обнаружено в течение 30 секунд, устройство заблокируется и вам придется начать процесс разблокировки снова.

8. Как изменить PIN-код администратора

ПРЕДУПРЕЖДЕНИЕ

Изменение PIN-кода администратора приведет к сбросу PIN-кода пользователя. Новый PIN-код пользователя ДОЛЖЕН БЫТЬ создан сразу же, как только PIN-код администратора был изменен.

Требования к PIN-коду

- Должен быть в пределах от 7-15 цифр
- Не должен содержать повторяющихся цифр или букв, например (3-3-3-3-3-3-3)
- Не должен содержать последовательные цифры или буквы, например (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4-5-6), (7-6-5-4-3-2-1)

После того, как PIN-код администратора был создан, datashur должна быть разблокирована администратором, чтобы изменить PIN-код администратора. PIN-код администратора не может быть изменен из пользовательского режима.

Действие	Индикация лампочек
1. Нажмите  кнопку два раза подряд (похоже на двойной щелчок мыши)	Красный и зеленый вместе мигают два раза (<i>рис. 2, на стр. 11</i>)
2. Введите PIN-код администратора	Красный и зеленый светятся
3. Нажмите  кнопку	Зеленый вдвойне замигает, если администратор ввел правильный PIN-код. Красный будет мигать, если введен неверный PIN-код.
4. Нажмите  кнопку дважды удерживая 3 секунды на втором нажатии	Красный и зеленый будут гореть
5. Отпустите  кнопку	Красный и зеленый замигают два раза, а затем будут гореть
6. Введите желательный PIN-код администратора	Красный и зеленый светятся
7. Нажмите  кнопку	Красный и зеленый двойное мигание
8. Повторно введите новый PIN-код администратора	Красный и зеленый продолжают двойное мигание
9. Нажмите  кнопку	Зеленый два раза мигает, если первый и второй PIN-код введен правильно. Красный и зеленый мигают попеременно, если была ошибка ввода PIN-кода. Если красные и зеленые светодиоды мигают поочередно, начните снова с шага №4.





9. Как выполнить «сброс» устройства

В случае, если оба PIN-кода администратора и пользователя были забыты или, если вы хотите удалить все данные, хранящиеся на диске, и создать новые PIN-коды пользователя и администратора, следуйте инструкциям ниже.

Процесс сброса очистит все PIN-коды и ключи шифрования. Это означает, что новый PIN-код пользователя должен быть определен для того, чтобы снова включить диск. Кроме того, поскольку это вызовет создание нового ключа шифрования, диск придется переформатировать.

ПРЕДУПРЕЖДЕНИЕ

Сброс Datashur сделает все данные на диске недоступными навсегда.

Действие	Индикация лампочек
1. Нажмите  кнопку дважды с паузой в 2 секунды между ними, чтобы запустить диск	Красный мигает
2. Нажмите и удерживайте  и «2» кнопки вместе на 3 секунды	Красный и зеленый светятся вместе
3. Отпустите кнопки	Красный и зеленый мигают одновременно
4. Введите «9-9-9»	Красный и зеленый мигают одновременно
5. Нажмите  кнопку	Оба светодиода погаснут
6. Нажмите  кнопку еще раз	Красный горит постоянно (Указывает, что PIN-код пользователя должен быть установлен до использования, см. раздел №3. «Как создать новый PIN-код пользователя»)

Часто задаваемые вопросы

1. Как открыть устройство, если батарея села

Ваш iStorage datashur поставляется со встроенной аккумуляторной батареей. Если аккумулятор полностью разряжен, вы все равно можете продолжать использовать продукт, следуя инструкциям ниже:

1. Подключите iStorage datashur к порту USB на любом компьютере
2. Пока datashur подключен к компьютеру, введите PIN-код Пользователя или Администратора для разблокирования устройства
3. В то время, когда устройство подключено к USB-порту, встроенный аккумулятор будет автоматически заряжаться. Мы рекомендуем держать устройство, подключенным в течение 1 часа для полной зарядки батареи.

2. Вы забыли свой PIN-КОД

Если вы забыли PIN-коды Пользователя и Администратора, нет абсолютно никакой возможности получить доступ к данным, хранящимся на диске, потому что секретный код отсутствует. Вы можете продолжать повторное использование iStorage datashur, сбросив PIN-код, однако, делая это, все данные, хранящиеся на диске, будут недоступны. Чтобы сбросить PIN-код, следуйте инструкциям в разделе 9. Как только это будет сделано, происходит следующее:

- Новый ключ шифрования будет создан
- PIN-коды Пользователя и Администратора будут удалены
- Все существующие данные будут недоступны
- Новый PIN-код Пользователя должен быть установлен
- Устройство должно быть переформатированно

3. Brute Force Hack защитный механизм

После 10 последовательных неудачных попыток ввода PIN-кода, происходит следующее:

- Новый ключ шифрования будет создан
- PIN-коды Пользователя и Администратора будут удалены
- Все существующие данные будут недоступны
- Новый PIN-код Пользователя должен быть установлен
- Устройство должно быть переформатированно

iStorage datashur, в отличие от других подобных устройств, имеет предварительное неограниченное количество случайно сгенерированных ключей шифрования. Каждый раз, когда взлом будет обнаружен (т.е. неправильный PIN-код вводится в общей сложности 10 раз подряд), текущий ключ шифрования удаляется по причине случайного формирования нового ключа шифрования. Новый 256-битный ключ шифрования создается один раз, если PIN-код Пользователя успешно установлен. Из-за этого iStorage datashur должен быть отформатированным каждый раз после того, как защитный механизм срабатывает.

Copyright © iStorage Limited, 2011. 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 datashur is developed and manufactured by iStorage Ltd. and is based on DataLock® technology licensed from CieVX, LLC

OS and Host Independent



Table of Contents

Introduction	4 p.
LED Indicators	5 p.
How to change User PIN	6 p.
How to create a new User Pin	7 p.
How to unlock drive with User PIN	8 p.
How to lock the iStorage datashur	8 p.
How to create an Admin PIN	9-11 p.
How to unlock with Admin PIN	11-12 p.
How to change Admin PIN	12-13 p.
How to reset drive	14 p.
Frequently asked questions	15 p.

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	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	Blink	Drive is locked and secure - all data is encrypted
Red	Constantly on	No User PIN created
Red and Green	Blink together	Accepting User PIN input
Red and Green	Double blink	Accepting Admin PIN input
Red and Green	Constantly lit	Drive is accepting new PIN
Red and Green	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 1 st and 2 nd 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 1 st and 2 nd 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  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)
- 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 for 3 seconds on the 2 nd 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 1 st and 2 nd 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.

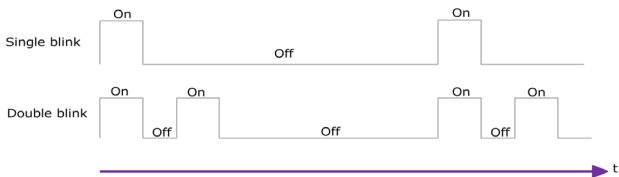


Figure 1: User Mode single blink LED output compared to Admin Mode double blink

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

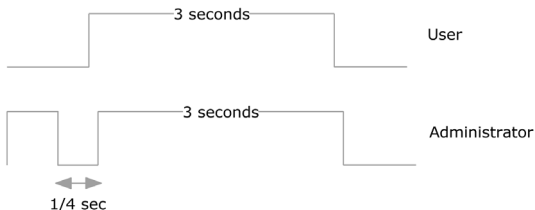




Figure 2: Key entry for User/Admin mode selection

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 (<i>figure 1, on page 24</i>)
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)
- 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 (<i>figure 2, on page 25</i>)
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 2 nd 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 1 st and 2 nd 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, <i>see 3. «How to create a new User PIN»</i>)

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:

1. Connect the iStorage datashur to a USB port on any computer
2. While the datashur is connected to the computer, enter the User or Admin PIN to unlock the drive
3. 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
