
CLOUDASHUR®
A
1
2 ABC
3 DEF
4 GHI
5 JKL
6 MNO
7 PQRS
8 TUV
9 WXYZ
0

Manual

Please make sure you remember your PIN (password), without it there is no way to access your encrypted data.

If you are having difficulty using your cloudAshur please contact our technical department by email - support@istorage-uk.com or by phone on +44 (0) 20 8991 6260.

RoHS Compliant

REACH COMPLIANCE

Trade Agreements Act (TAA) Compliant

CITRIX vmware

Table of Contents

Introduction

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

Thank you for purchasing the iStorage cloudAshur Hardware Security Module, your unique physical key to your data, making it the perfect solution for anyone wanting to store, share (including email and file transfer services) and manage data in the cloud in the most secure way imaginable, by eliminating the security vulnerabilities that exist with cloud platforms, such as lack of control, ownership, privacy and unauthorised access.

The cloudAshur hardware security module provides five factor authentication:

- **Something you have** -

1. Your cloudAshur hardware security module, your physical key to your data.

- **Something you know** -

2. Your cloudAshur hardware security module 7-15 digit PIN.
3. Your username and password for the cloudAshur client app.
4. Where your data is stored (cloud storage).
5. Username and password for your cloud account.

In addition, your cloudAshur hardware security modules can also be managed and monitored using the iStorage cloudAshur Remote Management Console giving you full control of all cloudAshur hardware security modules deployed within your organisation and offering the administrator a wide range of features such as real-time geo-fencing, time fencing, user logs, remote disable, remote kill and a lot more to manage and monitor all users with the utmost of ease.

Box Contents

- iStorage cloudAshur Hardware Security Module
- Extruded Aluminium Sleeve
- QSG - Quick Start Guide

Registering and Installing your cloudAshur Client App

This manual is divided into two parts, **Part A** (sections 1-40) and **Part B** (sections 41 and 42).

You will first need to configure your cloudAshur Hardware Security Module with the relevant configurations as described in **Part A** of this manual, for instance changing the Admin PIN, configuring a User PIN, Self-Destruct PIN and so on.

Once your cloudAshur Hardware Security Module has been configured with your preferred settings (**Part A**), you can now refer to **Part B** to register and install your Windows or macOS cloudAshur Client App.

PART A

1. LED indicators and their actions

LED	LED State	Description	LED	LED State	Description
▲	RED Solid	Locked cloudAshur (in either Standby or Reset states)	▲	BLUE Solid	cloudAshur in Admin mode
▲	RED - Fade Out	cloudAshur Turning off	▲▼▲	RED, GREEN and BLUE Blinking	Waiting for User PIN entry
▼	GREEN Blinking	Unlocked cloudAshur as Admin (not connected to USB port)	▼▲	GREEN and BLUE Blinking together	Waiting for Admin PIN entry
▼	GREEN Solid	Unlocked cloudAshur as User (not connected to USB port) or cloudAshur in User mode	▼▲	GREEN and BLUE Blinking alternately	Authentication in progress
▼	GREEN Solid	cloudAshur unlocked and connected to host	▲		Blue LED blinks every 5 seconds when charging is in progress

2. Battery and LED States

Note: The normal function of the cloudAshur 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 cloudAshur incorporates voltage detection circuitry that monitors the battery output when the cloudAshur 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 cloudAshur to a powered USB port and charge for 20-30 minutes. Once recharged, the cloudAshur will resume normal function.

To wake from Idle State

Idle state is defined as when cloudAshur is not being used and all LEDs are off.

To wake cloudAshur from the idle state do the following.

Press and hold down the **SHIFT** (⬆) button for one second or connect the cloudAshur to a powered USB port	▲ ▼ ▲ ▲	RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the cloudAshur is in Standby State

To enter Idle State

To force cloudAshur to enter Idle State (all LEDs off), execute either of the following operations:

- If the cloudAshur is connected to a USB port, disconnect it.
- If the cloudAshur 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).

Power-on States

After the cloudAshur wakes from Idle State, it will enter one of the three possible 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 15-30 minutes

Note: When your cloudAshur is unlocked and not connected to a USB port and no operations are performed within 30 seconds, the cloudAshur will enter Idle State automatically. The LED turns to solid RED and then fades out.

When connected to a powered USB port, a locked cloudAshur will start charging after 30 seconds, indicated by a blinking BLUE LED.

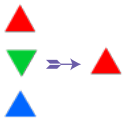
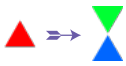
When the cloudAshur is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

3. First Time Use

Your cloudAshur Hardware Security Module ships with the following factory default Admin PIN: **11223344**.

Important: In its default state, the cloudAshur Hardware Security Module cannot be registered. You **MUST change the default Admin PIN immediately** as described under section 7 '**How to change Admin Pin**' in order to register your cloudAshur Hardware Security Module via the cloudAshur client application.

Please follow the simple steps below to unlock your cloudAshur for the first time with the factory default Admin PIN.

Instructions - first time use	LED	LED State
1. Press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the cloudAshur is in Standby State
2. In Standby State (solid RED LED) press the **KEY (⚷)** button once		GREEN and BLUE LEDs blink together
3. With both GREEN and BLUE LEDs blinking together, enter the **Admin PIN** (factory pre-set **11223344**) and press the **KEY (⚷)** button once		GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED changing to a blinking GREEN indicating the cloudAshur is unlocked as Admin

Note: Once your cloudAshur has been successfully unlocked, the GREEN LED will remain blinking for 30 seconds only, during which time the cloudAshur needs to be connected to a powered USB port. It can be locked down immediately by pressing and holding down the **SHIFT** (⬆) button for a second.

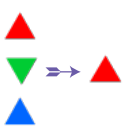
When the cloudAshur is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

Locking cloudAshur

To lock the cloudAshur, simply unplug from the USB port or right click on the cloudAshur app in the system tray and click exit.

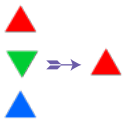
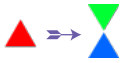
4. Unlocking your cloudAshur with the Admin PIN

Please follow the simple steps in the table below to unlock the cloudAshur with your 7-15 digit Admin PIN.

1. Press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the cloudAshur is in Standby State
2. In Standby State (solid RED LED) press the **KEY (⚷)** button once		GREEN and BLUE LEDs blink together
3. With both GREEN and BLUE LEDs blinking together, enter your **Admin PIN** and press the **KEY (⚷)** button once		GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED changing to a blinking GREEN indicating the cloudAshur is unlocked as Admin

5. To Enter Admin Mode

To Enter Admin Mode, do the following.

1. Press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the cloudAshur is in Standby State
2. In Standby State (solid RED LED) press the **KEY (⚷)** button once		GREEN and BLUE LEDs blink together
3. With the GREEN and BLUE LEDs blinking together, enter the **Admin PIN** (factory pre-set **11223344**) and press the **KEY (⚷)** button once		GREEN and BLUE LEDs will alternately blink several times and then to a solid BLUE LED changing to a blinking GREEN indicating the cloudAshur is unlocked
4. Press the **KEY (⚷)** button **Three** times within 2 seconds (**KEY (⚷)** x **3**)		Blinking GREEN LED will change to a solid BLUE LED indicating the cloudAshur is in Admin mode

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

6. To Exit Admin Mode

When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 - the solid BLUE LED switches to a solid RED which then fades out to the Idle state.

7. Changing the Admin PIN

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- 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)

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 (**p**qrs) **2** (**a**bc) **7** (pqr**s**) **7** (pqr**s**) **9** (**w**xyz) **6** (mn**o**) **7** (pq**r**s) **3** (**d**ef)
- For "**iStorage**" press the following buttons:
  4 (gh**i**) **7** (pqr**s**) **8** (**t**uv) **6** (mn**o**) **7** (pq**r**s) **2** (**a**bc) **4** (**g**hi) **3** (d**e**f)

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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both the '**KEY (🔑) + 2**' buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New Admin PIN** and press **KEY (🔑)** 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 **New Admin PIN** and press **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking BLUE LED and finally to a solid BLUE LED indicating the Admin PIN has been successfully changed

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur 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 7 to 15 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 7-15 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 cloudAshur 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 7-15 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 7-15 digits, with no special character required.

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

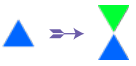
1. In Admin mode, press and hold down both **KEY (🔑) + 7** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter your **3 digits**, remember the first two digits denote minimum PIN length and last digit (0 or 1) whether or not a special character has been used.		Blinking GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) 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 cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur 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 your cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **KEY (🔑) + 7** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **070** and press **SHIFT** (⬆) 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 deleted

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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down **SHIFT** (⬆) + **7**"		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY (🔑)** button and the following happens; a. All LEDs (RED, GREEN & BLUE) become solid for 1 second. b. A RED LED blink equates to ten (10) units of a PIN. c. Every GREEN LED blink equates to a single (1) unit of a PIN d. A BLUE blink indicates that a 'Special Character' was used. e. All LEDs (RED, GREEN & BLUE) become solid for 1 second. f. LEDs return to solid BLUE		

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 used	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 used	090	0	9 Blinks	0

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur 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

PIN requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both '**KEY (🔑) + 3**' buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New User PIN** and press **KEY (🔑)** 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 **New User PIN** and press **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking GREEN LED and finally to a solid BLUE LED indicating a New User PIN has been successfully configured

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur 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

To change an existing **User PIN**, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both '**KEY (🔑) + 3**' buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New User PIN** and press **KEY (🔑)** 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 **New User PIN** and press **KEY (🔑)** button		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking GREEN LED and finally to a solid BLUE LED indicating the User PIN has been successfully changed

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

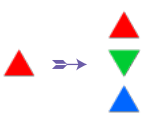
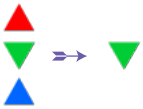
1. In Admin mode, press and hold down both '**SHIFT** (⬆) **+ 3**' buttons		Solid BLUE LED will change to a blinking RED LED
2. Press and hold down both '**SHIFT** (⬆) **+ 3**' buttons again		Blinking RED LED will change to a solid RED LED and then to a solid BLUE LED indicating the User PIN has been successfully deleted

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

14. How to Unlock your cloudAshur with User PIN

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

1. In a standby state (solid RED LED) Press and hold down both the **SHIFT** (⬆) + **KEY (🔑)** buttons		RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter **User PIN** and press the **KEY (🔑)** button		RED, GREEN and BLUE blinking LEDs will change to alternating GREEN and BLUE LEDs then to a solid GREEN LED indicating the cloudAshur successfully unlocked in User Mode

15. Changing the User PIN in User Mode

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

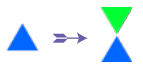
1. In User mode press and hold down both **KEY (⚷) + 4**		Solid GREEN LED will change to a blinking GREEN LED and a solid BLUE LED
2. Enter **New User PIN** and press the **KEY (⚷)** button		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
3. Re-enter **New User PIN** and press the **KEY (⚷)** button		Blinking GREEN and solid BLUE LEDs will switch to a rapidly blinking GREEN LED and then to a solid GREEN LED indicating a successful User PIN change

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 been used. The administrator can refer to section 10 to check the user PIN restrictions.

16. Configuring a One-Time User Recovery PIN

The One-Time User Recovery PIN is extremely useful in situations where a user has forgotten their PIN to unlock the cloudAshur. 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 encryption key and Admin PIN, however the user is forced to configure a new 7-15 digit User PIN.

To configure a One-Time 7-15 digit User Recovery PIN, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **'KEY (⚷) + 4'** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **a One-Time Recovery PIN** and press **KEY (⚷)** 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 **a One-Time Recovery PIN** and press **KEY (⚷)** button again		Blinking GREEN and solid BLUE LEDs change to a rapidly blinking GREEN LED and finally to a solid BLUE LED indicating the One-Time Recovery PIN has been successfully configured

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both '**SHIFT** (⬆) **+ 4**' buttons		Solid BLUE LED will change to blinking RED LED
2. Press and hold down both '**SHIFT** (⬆) **+ 4**' buttons again		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

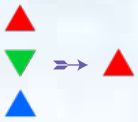
Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the cloudAshur will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

18. Activating Recovery Mode and configuring New User PIN

The One-Time User Recovery PIN is extremely useful in situations where a user has forgotten their PIN to unlock the cloudAshur. 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 encryption key and Admin PIN, however the user is forced to configure a new 7-15 digit User PIN.

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

1. With the cloudAshur in **Idle State,** press and hold down the **SHIFT** (⬆) button for one second		RED, GREEN and BLUE LEDs blink once in sequence then the GREEN LED blinks twice and finally switches to a solid RED LED indicating the cloudAshur is in Standby State
2. In **Standby State,** press and hold down both '**KEY (🔑) + 4**' buttons		Solid RED LED will change to blinking RED and GREEN LEDs
3. Enter the One-Time **Recovery PIN** and press the **KEY (🔑)** 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 **New User PIN** and press the **KEY (🔑)** 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 **New User PIN** and press the **KEY (🔑)** button again		GREEN LED blinks rapidly then becomes solid GREEN 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. How to set your cloudAshur to enable KeyWriter Cloning

Note: The cloudAshur is set as default to enable cloning by the KeyWriter.

The cloudAshur can be used in conjunction with the iStorage KeyWriter to enable cloning of up to 9 devices at a time. To enable the cloudAshur to be cloned by the KeyWriter, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur 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 BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter '**11**' and press the '**SHIFT** (⬆)' button once.		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating the cloudAshur is set to enable KeyWriter cloning

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

20. How to disable KeyWriter Cloning

To disable KeyWriter cloning, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur 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 BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter '**44**' and press the '**SHIFT** (⬆)' button once.		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid BLUE LED indicating KeyWriter cloning is disabled

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

21. How to check KeyWriter Cloning Configuration

To check whether the cloudAshur KeyWriter cloning is enabled or disabled, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **'SHIFT** (⬆) + **8'** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs

2. Press the **KEY (⚷)** button and the following happens;

- **If your cloudAshur is set to enable KeyWriter cloning, the following happens;**

a. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks once.
c. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

- **If KeyWriter cloning is disabled, the following happens;**

a. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
b. All LEDs are off
c. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

22. How to disable the cloudAshur Client Application Registration

The cloudAshur is configured so that it cannot be registered by the client application when it is shipped from factory or completely reset. The client application feature is automatically enabled when the initial Admin PIN is changed or when a User PIN is configured or changed.

To disable client application registration, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both '**3 + 7**' buttons.		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY (🔑)** button once.		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

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

23. How to check whether Client Application Registration is enabled

To check whether the cloudAshur client application registration is enabled, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **'2 + 7'** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs

2. Press the **KEY (⚷)** button and the following happens;

- **If your cloudAshur client application registration is enabled, the following happens;**

a. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks once.
c. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

- **If your cloudAshur client application registration is disabled, the following happens;**

a. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
b. All LEDs are off
c. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

24. How to Configure the cloudAshur Encryption Mode

WARNING: Changing the encryption mode from AES-XTS (default state) to AES-ECB or vice versa will delete the encryption key and cause the cloudAshur to reset and render all data encrypted by your cloudAshur as inaccessible and lost forever! Only perform this operation before any data is uploaded to the cloud or local folders, or you have one or more cloudAshur hardware security modules containing the same encryption key from which to copy, or if a complete and non-encrypted backup of your data is available.

Perform the following steps to configure the cloudAshur encryption mode to either **AES-ECB**, indicated by the number **'01'**, or **AES-XTS**, indicated by the number **'02'**. This feature is set as AES-XTS (02) by default. When a specific encryption mode is configured, the data will be encrypted by the cloudAshur using the corresponding algorithm.

To configure the cloudAshur encryption mode, first enter the "Admin Mode" as described in section 5. Once the cloudAshur 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 **01** to set as **AES-ECB** Enter **02** to set as **AES-XTS (default state)**		Blinking GREEN and BLUE LEDs will continue to blink
3. Press the **SHIFT** (⬆) button once.		GREEN and BLUE LEDs will change to a solid GREEN LED and then to a solid RED LED (**Reset State**) indicating successful cloudAshur encryption mode switch.

Important: After configuring the cloudAshur encryption mode, the cloudAshur completely resets and a new Admin PIN must be configured, refer to Section 29 on page 23 on 'How to Configure an Admin PIN after a Brute Force attack or Reset'.

25. How to check the encryption mode

To check the cloudAshur encryption mode, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur 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

2. Press the **KEY (🔑)** button and the following happens;

- **If the encryption mode is configured as AES-ECB, the following happens;**

a. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
b. GREEN LED blinks once.
c. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

- **If the encryption mode is configured as AES-XTS, the following happens;**

a. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
b. All LEDs are off
c. All LEDs (RED, GREEN & BLUE) become solid for 1 second.
d. LEDs return to solid BLUE

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

26. How to configure a Self-Destruct PIN

You can configure a self-destruct PIN which, when entered deletes all configured PINs and performs a Crypto-Erase on the cloudAshur (encryption key is deleted). Running this feature will cause the self-destruct PIN to become the new User PIN.

To set the Self-Destruct PIN, first enter the "**Admin Mode**" as described in section 5. Once the cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both '**KEY (🔑) + 6**' buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
2. Configure a 7-15 digit **Self-Destruct PIN** and press the **KEY (🔑)** 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 **Self-Destruct PIN** and press the **KEY (🔑)** button		GREEN LED will rapidly blink for several seconds and then changes to a solid BLUE LED to indicate the Self-Destruct PIN has been successfully configured

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

27. 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both '**SHIFT** (⬆) **+ 6**' buttons		Solid BLUE LED will change to a blinking RED LED
2. Press and hold down '**SHIFT** (⬆) **+ 6**' buttons again		Blinking RED LED will become solid and then change to a solid BLUE LED indicating the Self-Destruct PIN was successfully deleted

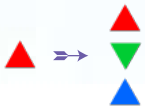
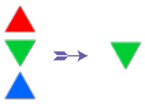
Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the cloudAshur will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

28. How to Unlock with the Self-Destruct PIN

When used, the self-destruct PIN will **delete the encryption key, Admin/User PINs** and then unlock the cloudAshur. Activating this feature will cause the **Self-Destruct PIN to become the New User PIN.**

To activate the Self-Destruct mechanism, the cloudAshur needs to be in the standby state (solid RED LED) and then proceed with the following steps.

1. In standby state (solid RED LED), press and hold down both the **SHIFT** (⬆) + **KEY (🔑)** buttons		RED LED switches to all LEDs, RED, GREEN & BLUE blinking on and off
2. Enter the **Self-Destruct PIN** and press the **KEY (🔑)** button		RED, GREEN and BLUE blinking LEDs will change to GREEN and BLUE LEDs alternating on and off for a few seconds and will finally shift to a solid GREEN LED indicating the cloudAshur has successfully self-destructed

WARNING: When the Self-Destruct mechanism is activated, the encryption key and the Admin/User PINs are deleted. **The Self-Destruct PIN becomes the User PIN.** No Admin PIN exists after the Self-Destruct mechanism is activated. The **cloudAshur will need to be reset** (see 'How to perform a complete reset' Section 36, on page 29) first in order to configure an Admin PIN with full Admin privileges including the ability to configure a User PIN.

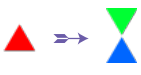
29. How to Configure an Admin PIN after a Brute Force attack or Reset

It will be necessary after a Brute Force attack or when the cloudAshur has been reset to configure an Admin PIN before the cloudAshur can be used.

PIN Requirements:

- Must be between 7-15 digits in length
- Must not contain only repetitive numbers, e.g. (3-3-3-3-3-3-3)
- 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)

If the cloudAshur has been brute forced or reset, the cloudAshur 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 **SHIFT** (⬆) **+ 1** buttons		Solid RED LED will change to blinking GREEN and solid BLUE LEDs
2. Enter **New Admin PIN** and press **KEY (🔑)** 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 **New Admin PIN** and press **KEY (🔑)** button		Blinking GREEN LED and solid BLUE LED change to BLUE LED rapidly blinking for a few seconds and then to a solid BLUE LED indicating the Admin PIN was successfully configured.

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

30. Setting the Unattended Auto-Lock Clock

To protect against unauthorised access if the cloudAshur is unlocked and unattended, the cloudAshur can be set to automatically lock after a pre-set amount of time. In its default state, the cloudAshur 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **KEY (🔑) + 5** buttons		Solid BLUE LED will change to blinking GREEN and BLUE 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: **05 for 5 minutes** **20 for 20 minutes** **99 for 99 minutes**		
3. Press the **SHIFT** (⬆) button		Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto-Lock time out is successfully configured

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

31. 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **KEY (⚷) + 5** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Enter **00** and press the **SHIFT** (⬆) button		Blinking GREEN and BLUE LEDs will change to a solid GREEN for a second and then finally to a solid BLUE LED indicating the Auto-Lock time out has been successfully disabled

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

32. 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down **SHIFT** (⬆) + **5**		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY (⚷)** button and the following happens; a. All LEDs (RED, GREEN & BLUE) become solid for 1 second. b. Each RED LED blink equates to ten (10) minutes. c. Every GREEN LED blink equates to one (1) minute. d. All LEDs (RED, GREEN & BLUE) become solid for 1 second. e. LEDs return to solid BLUE		

The table below describes the LED behaviour whilst checking the unattended auto-lock, for instance if you have set the cloudAshur 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 cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

33. Brute Force Hack Defence Mechanism

The cloudAshur incorporates a defence mechanism to protect the cloudAshur against Brute Force attacks. By default, the initial shipment state values of the brute force limitation (consecutive incorrect PIN entries) for both the Admin PIN and User PIN is **10** and **5** for the Recovery PIN. Three independent brute force counters are used to record the incorrect attempts for each PIN authorisation (Admin, User and Recovery) as set out below.

- 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.
- If an **incorrect Admin PIN** is entered 10 consecutive times, the cloudAshur will reset. All PINs and data are deleted and lost forever.

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

PIN used to unlock cloudAshur	Consecutive incorrect PIN enteries	Description of what happens
User PIN	10	• The User PIN is deleted. • The Recovery PIN, the Admin PIN and all data remain intact and accessible.
Recovery PIN	5	• The Recovery PIN is deleted. • The Admin PIN and all data remain intact and accessible.
Admin PIN	10	• The cloudAshur will reset. All PINs and data are deleted and lost forever.

Note: The brute force limitation is defaulted to initial shipment state values when the cloudAshur is completely reset, or self-destruct feature is activated, or brute forced. If Admin changes the User PIN, or a new User PIN is set when activating the recovery feature, the User PIN brute force counter is zeroed (0) but the brute force limitation is not affected. If Admin changes the Recovery PIN, the Recovery PIN brute force counter is zeroed.

Successful authorisation of a certain PIN will zero 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.

34. 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 cloudAshur is either completely reset, brute forced or the self-destruct PIN is activated.

The brute force limitation for the cloudAshur 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode, press and hold down both **7 + 0** buttons		Solid BLUE LED will change to GREEN and BLUE LEDs blinking together
2. Enter the number of attempts for the brute force limitation (between 01-10), for example enter: • **01** for 1 attempt • **10** for 10 attempts		
3. Press the **SHIFT** (⬆) button once		Blinking GREEN and BLUE LEDs will switch to a solid GREEN LED for a second and then to a solid BLUE LED indicating the brute force limitation was successfully configured

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

35. 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both **2** + **0** buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY (⚷)** button and the following happens; a. All LEDs (RED, GREEN & BLUE) become solid for 1 second. b. Each RED LED blink equates to ten (10) units of a brute force limitation number. c. Every GREEN LED blink equates to one (1) single unit of a brute force limitation number. d. All LEDs (RED, GREEN & BLUE) become solid for 1 second. e. LEDs return to solid BLUE		

The table below describes the LED behaviour whilst checking the brute force limitation setting, for instance if you have set the cloudAshur 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

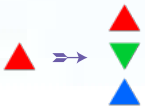
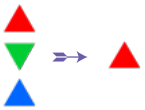
Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the cloudAshur will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

36. How to perform a complete reset

To perform a complete reset, the cloudAshur must be in standby state (solid RED LED). Once the cloudAshur is reset then all Admin/User PINs and the encryption key will be deleted, leaving all associated data encrypted and inaccessible.

To reset the cloudAshur 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 become solid for a second and then to a solid RED LED indicating the cloudAshur has been reset

Important: After a complete reset a new Admin PIN must be configured, refer to Section 29 on page 23 on 'How to Configure an Admin PIN after a Brute Force attack or Reset'.

37. 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 cloudAshur is in **Admin Mode** (solid BLUE LED) proceed with the following steps.

1. In Admin mode press and hold down both "**3** + **8**" buttons		Solid BLUE LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY (⚷)** button once and the following happens; a. All LEDs (RED, GREEN & BLUE) become solid for 1 second. b. RED LED blinks indicating the integral part of the firmware revision number. c. GREEN LED blinks indicating the fractional part. d BLUE LED blinks indicating the last digit of the firmware revision number e. All LEDs (RED, GREEN & BLUE) become solid for 1 second. f. RED, GREEN & BLUE LEDs switch to a solid BLUE LED		

For example, if the firmware revision number is '**4.2**', the RED LED will blink four (**4**) times and the GREEN LED will blink twice (**2**). Once the sequence has ended the RED, GREEN & BLUE LEDs will blink together once and then return to Admin mode, a solid BLUE LED.

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

38. 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 cloudAshur is in **User Mode** (solid GREEN LED) proceed with the following steps.

1. In User mode press and hold down both "**3** + **8**" buttons until GREEN and BLUE LEDs blink together		Solid GREEN LED will change to blinking GREEN and BLUE LEDs
2. Press the **KEY (🔑)** button and the following happens; a. All LEDs (RED, GREEN & BLUE) become solid for 1 second. b. RED LED blinks indicating the integral part of the firmware revision number. c. GREEN LED blinks indicating the fractional part. d BLUE LED blinks indicating the last digit of the firmware revision number e. All LEDs (RED, GREEN & BLUE) become solid for 1 second. f. RED, GREEN & BLUE LEDs switch to a solid BLUE LED		

For example, if the firmware revision number is '**4.2**', the RED LED will blink four (**4**) times and the GREEN LED will blink twice (**2**). Once the sequence has ended the RED, GREEN & BLUE LEDs will blink together once and then return to the User mode, a solid GREEN LED.

Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur 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 cloudAshur 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 unlock and access your data, your cloudAshur must first be in the idle state (all LEDs off) before an Admin/User PIN can be entered.

39. Technical Support

iStorage provides the following helpful resources for you:

Website:
https://www.istorage-uk.com

E-mail Support:
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.

40. 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, NONINFRINGEMENT. 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

PART B

41. Register and Install Windows cloudAshur Client App

cloudAshur Registration

Please download the Windows cloudAshur client App from the following link:
https://istorage-uk.com/software-and-updates/

Important Please Read: To register your cloudAshur hardware security module please choose one of the following registration methods that apply to you:

- **Personal** - cloudAshur **NOT** to be used with **Remote Management** (central management software).
- **Enterprise** - cloudAshur used in conjunction with **Remote Management** (central management software).

Personal Registration

As your cloudAshur hardware security module will not be used in conjunction with the 'Remote Management, you will **NOT** require a 'PIN Number' or 'License Key' during the registration process. Simply complete (**step 3**) field numbers 1-6, leave the checkbox in field number 7 unchecked, skip field numbers 8 and 9 and then click 'Register' and start using your cloudAshur.

Enterprise Registration

The cloudAshur hardware security module is to be used by organisations that will centrally manage and monitor all employees who use the cloudAshur modules issued by the organisation through the use of the cloudAshur **Remote Management Console** (central management software).

If you are an employee and have been issued with a cloudAshur module by your organisation's Administrator, a '**You Have Been Invited**' email will be sent to you by your Administrator containing the following important registration information:

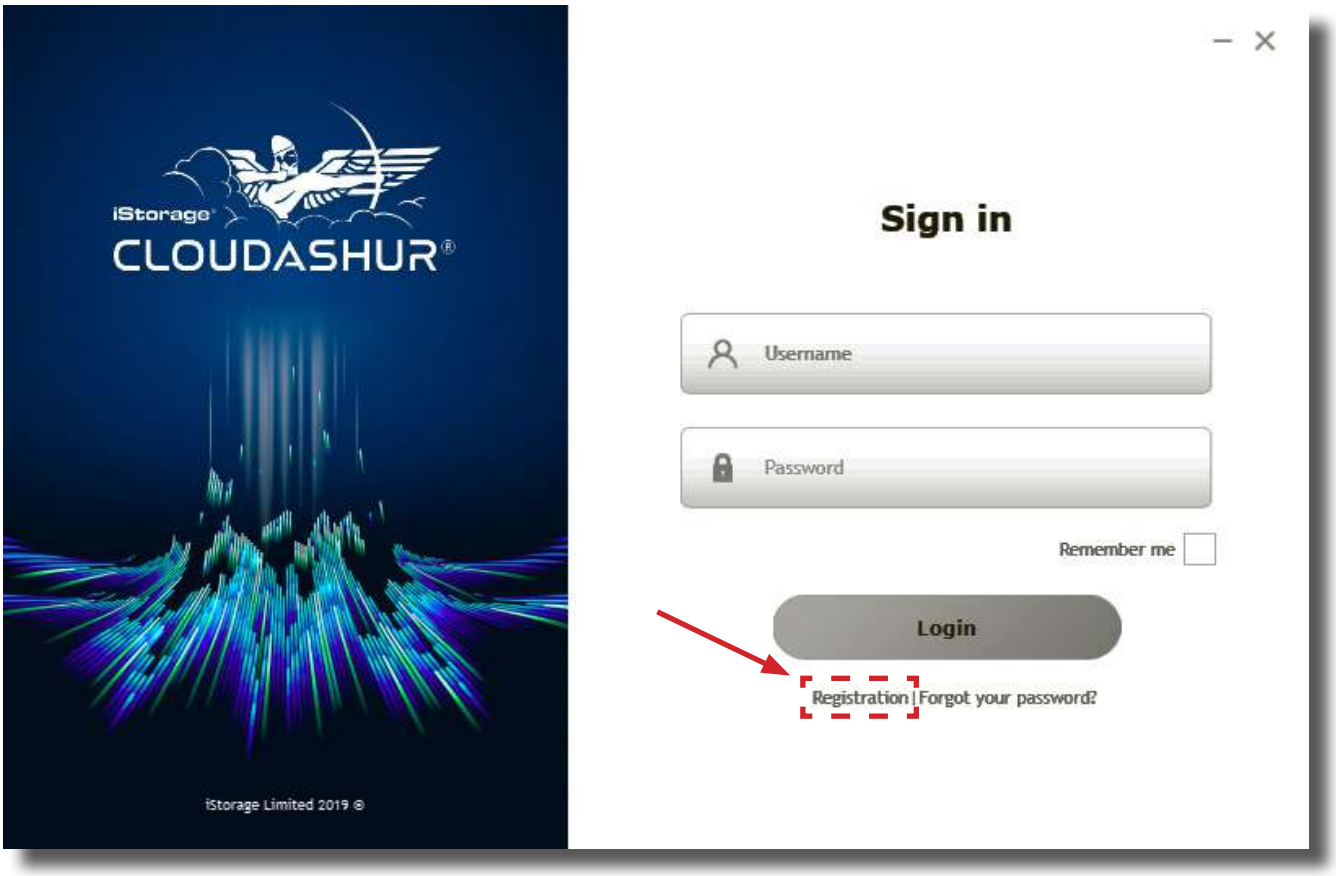
1. A Link to download your Windows cloudAshur client App.
2. A **PIN Number** - this will be required to be entered in field No. 8 during the registration process (**step 3**).
3. A **License Key** - this will also be required to be entered in field No. 9 during the registration process (**step 3**).

Step 01

Once you have finished installing the Windows client App, unlock your cloudAshur hardware security module with either your Admin PIN or User PIN as described in **Part A** of this manual. With your cloudAshur Hardware Security Module unlocked (GREEN LED), connect to your computer's USB port.

Step 02

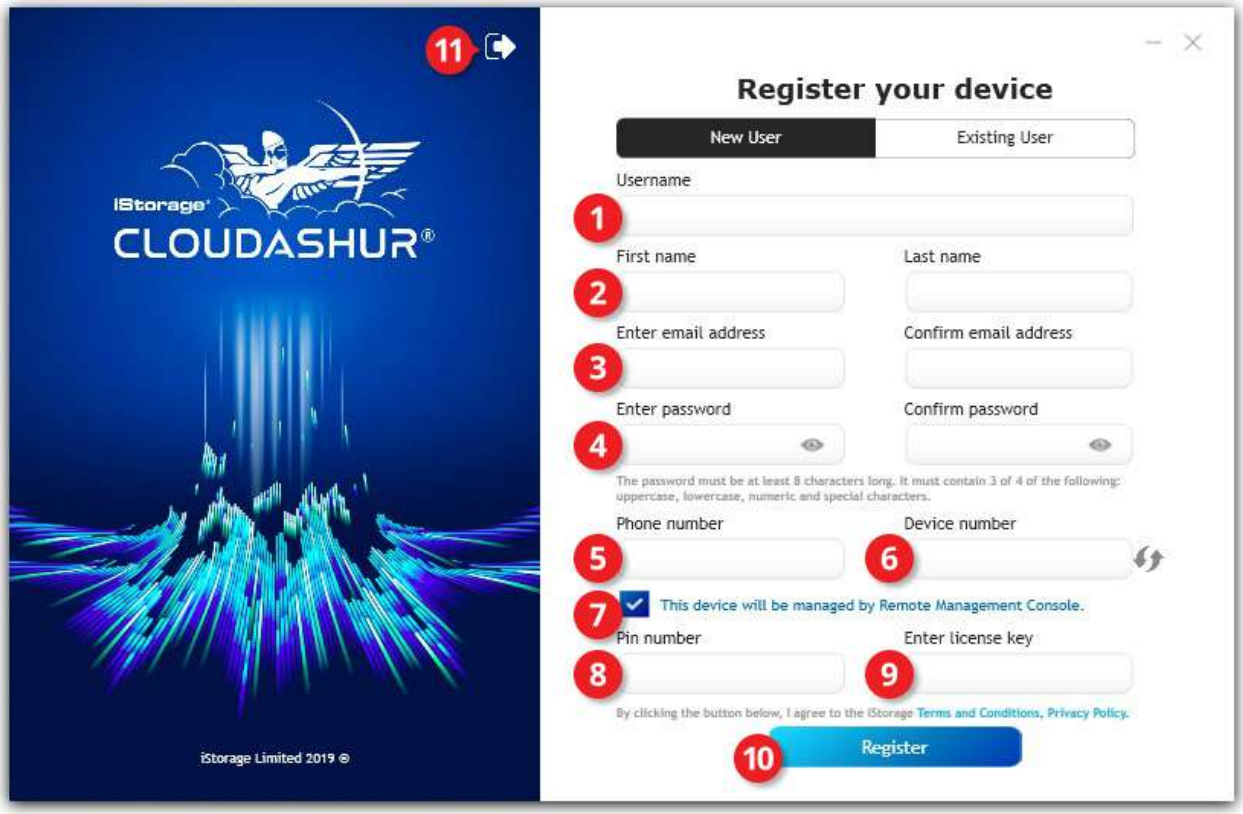
Open your Windows client App (image 1) and click '**Registration**' to register your cloudAshur hardware security module.



(image 1)

Step 03

To 'Register your cloudAshur' (image 2) complete all the fields under '**New User**'.

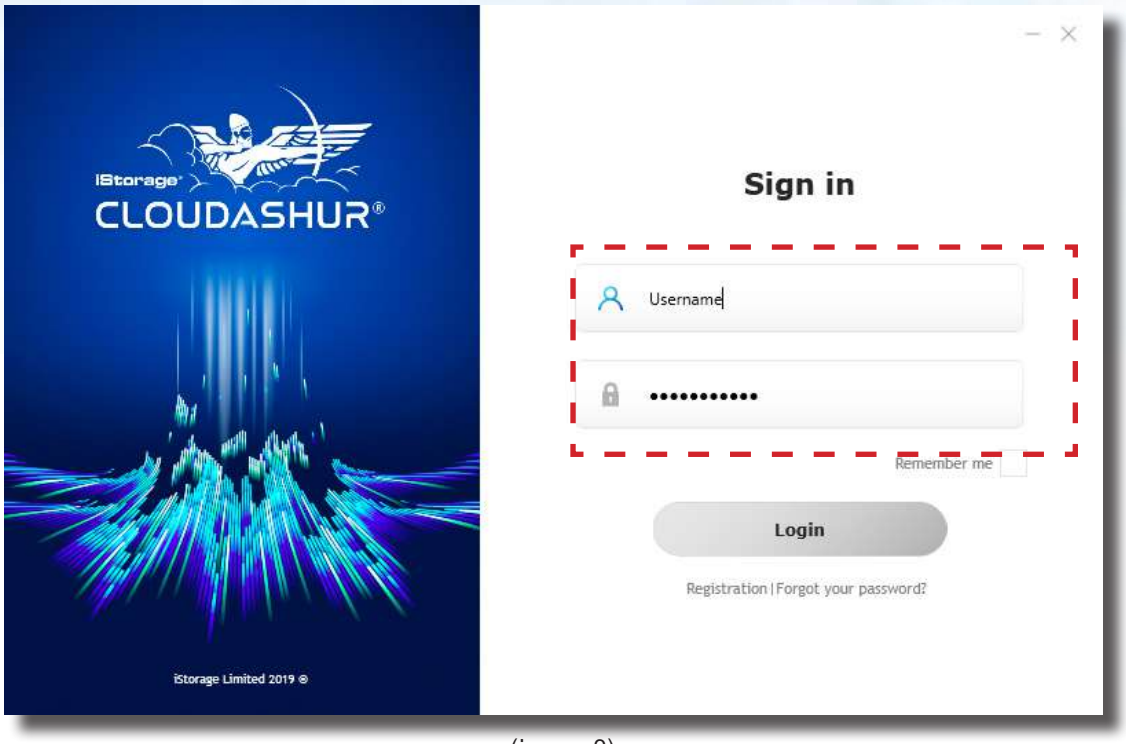


(image 2)

1. Enter a '**Username**'.
2. Enter your '**First**' and '**Last**' name.
3. Enter and confirm your '**Email Address**'.
4. Enter and confirm your '**Password**' - your password must be at least 8 characters long and must contain 3 out of 4 of the following: uppercase, lowercase, numeric and special characters.
5. Enter your '**Phone number**'.
6. The '**Device number**' will be automatically detected if your cloudAshur module is unlocked and connected to your computer (GREEN LED). If the device number has not been detected, click on the refresh button to detect.
7. If your cloudAshur module is to be **Enterprise Registered**, issued to you by your organisation's Administrator, make sure to check the checkbox as in above image 2. If your cloudAshur is to be **Personal Registered** leave the checkbox unchecked, skip steps 8 and 9 and proceed to step 10.
8. Enter the '**PIN**' emailed to you by your Administrator (**Enterprise Registration Only**).
9. Enter the '**License Key**' emailed to you by your Administrator (**Enterprise Registration Only**)
10. Click the '**Register**' button to complete the registration process.
11. Click on the forward button to login (**step 4**).

Step 04

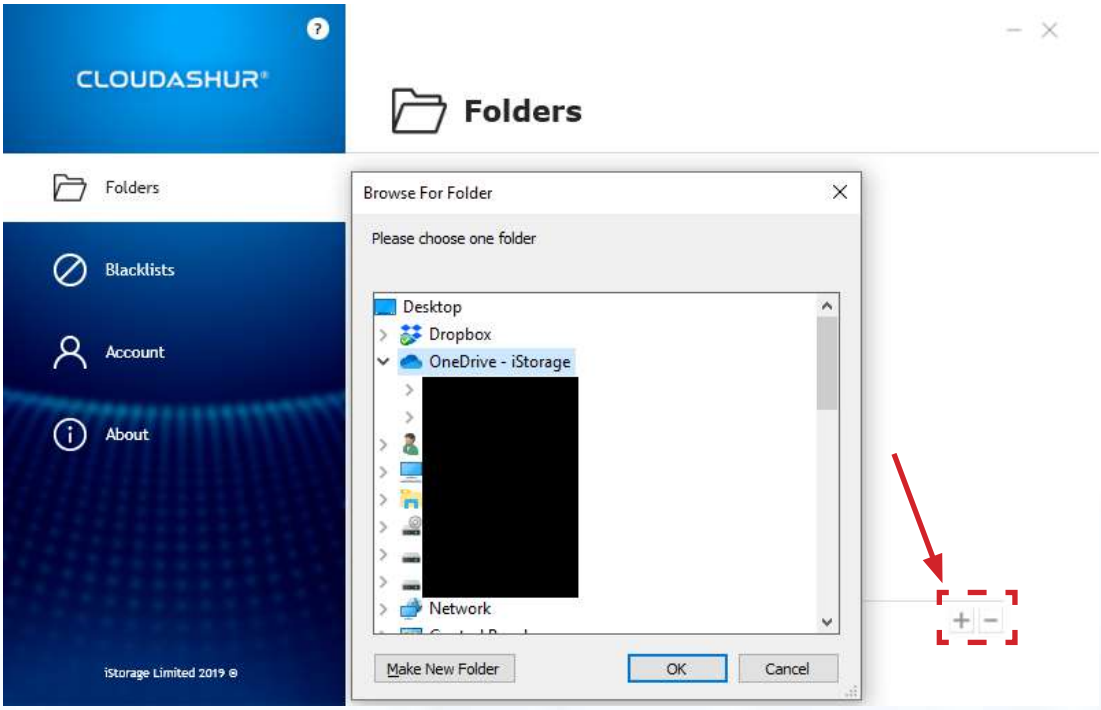
Enter your '**Username**' and '**Password**' created during step 3 and then click the '**Login**' button as in image 3 below.



(image 3)

Step 05

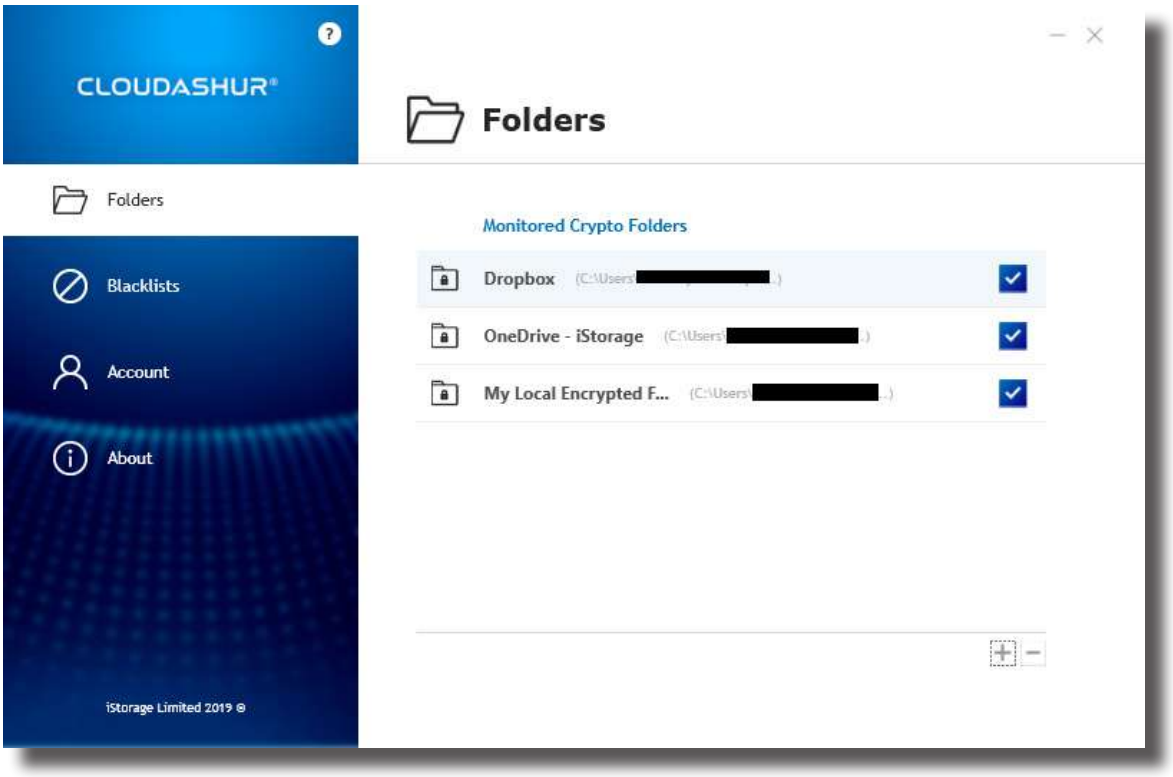
After 'Sign in' your cloudAshur virtual drive will open. To add your cloud folder/s and local folders to your cloudAshur virtual drive, click the cloudAshur icon in your system tray (bottom right hand corner of your screen) once to open the preferences menu and then click on the '**+**' symbol to browse and select your cloud folder/s and any local folder/s as in image 4 below.



(image 4)

Step 06

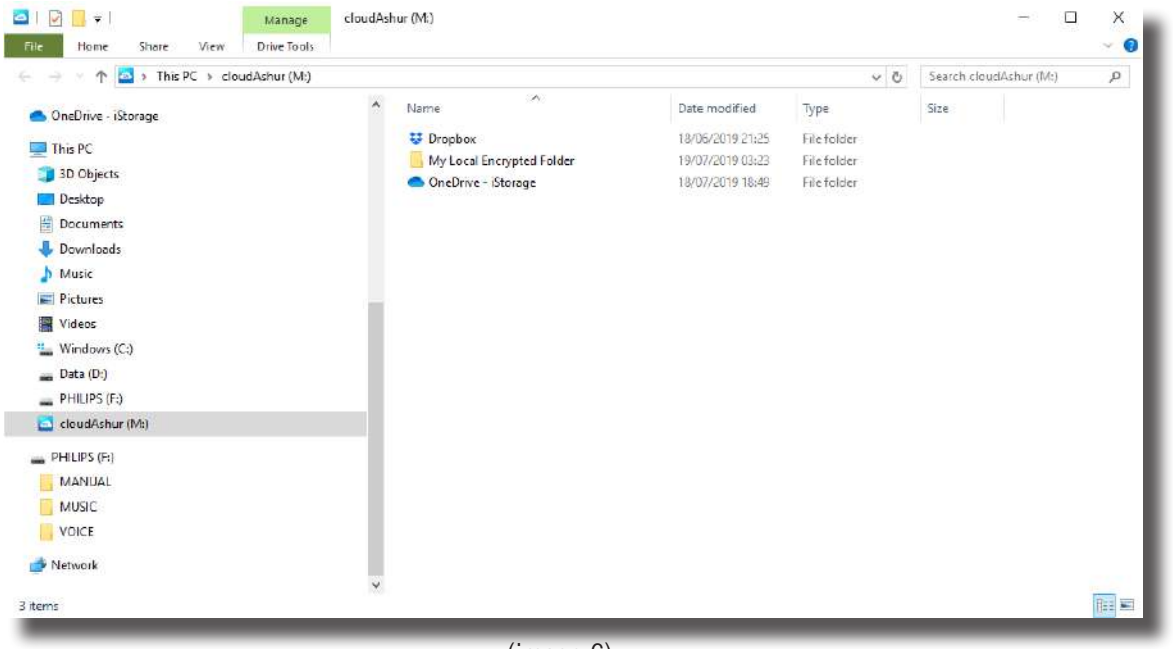
After adding your cloud accounts and any local folder (as seen in image 5), double click the cloudAshur icon in your system tray (bottom right hand corner of your screen) to open your cloudAshur virtual drive (image 6).



(image 5)

Step 07

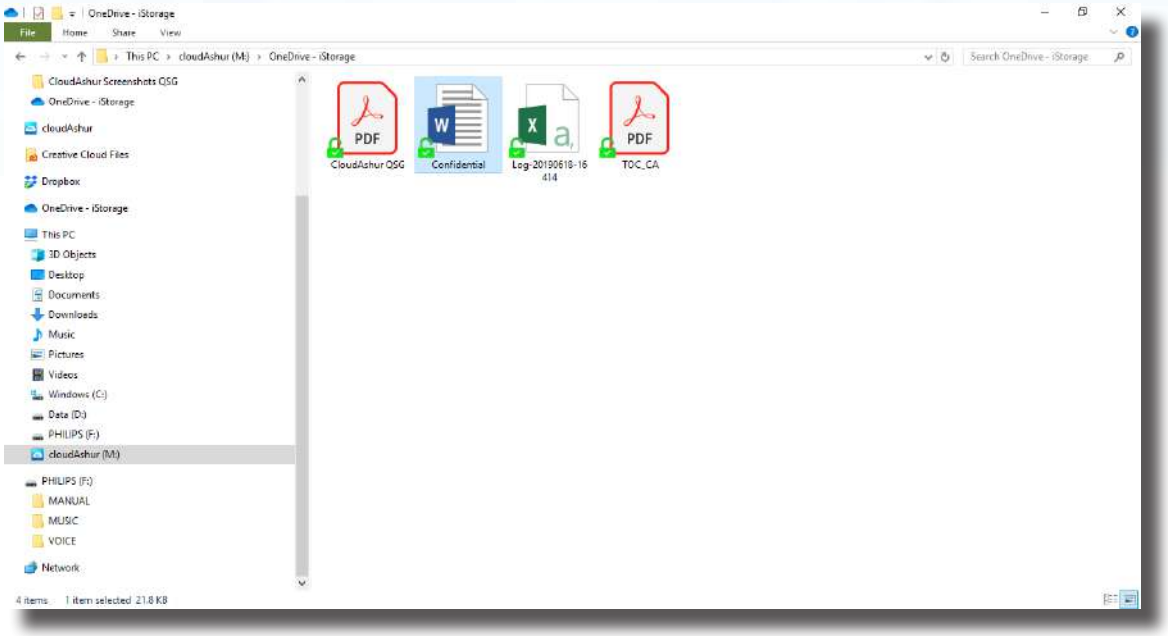
Within your cloudAshur virtual drive, click on your cloud/local folder to open, in this case, '**OneDrive - iStorage**' as seen in image 6.



(image 6)

Step 08

Drag and drop or copy and paste your files to your cloudAshur virtual drive and a green unlocked padlock symbol will appear on the bottom left hand corner of each file as seen in image 7 indicating the files have been encrypted but can be accessed through your virtual drive. Meanwhile the same files are encrypted when accessed directly from your cloud account.



(image 7)

42. Sign Up and Install macOS cloudAshur Client App

cloudAshur Registration

Please download the macOS cloudAshur client App from the following link:
https://istorage-uk.com/software-and-updates/

Important Please Read: To register your cloudAshur hardware security module please choose one of the following two registration methods that apply to you:

- **Personal** - cloudAshur **NOT** to be used with **Remote Management** (central management software).
- **Enterprise** - cloudAshur used in conjunction with **Remote Management** (central management software).

Personal Registration

As your cloudAshur hardware security module will not be used in conjunction with the 'Remote Management, you will **NOT** require a 'PIN Number' or 'License Key' during the registration process. Simply complete (**step 3**) field numbers 1-6, leave the checkbox in field number 7 unchecked, skip field numbers 8 and 9 and then click 'Register' and start using your cloudAshur.

Enterprise Registration

The cloudAshur hardware security module is to be used by organisations that will centrally manage and monitor all employees who use the cloudAshur modules issued by the organisation through the use of the cloudAshur **Remote Management Console** (central management software).

If you are an employee and have been issued with a cloudAshur module by your organisation's Administrator, a '**You Have Been Invited**' email will be sent to you by your Administrator containing the following important registration information:

1. A Link to download your macOS cloudAshur client App.
2. A **PIN Number** - this will be required to be entered in field No. 8 during the registration process (**step 3**).
3. A **License Key** - this will also be required to be entered in field No. 9 during the registration process (**step 3**).

Step 01

Once you have finished installing the macOS client App, unlock your cloudAshur hardware security module with either your Admin PIN or User PIN as described in **Part A** of this manual. With your cloudAshur Hardware Security Module unlocked (GREEN LED), connect to your computer's USB port.

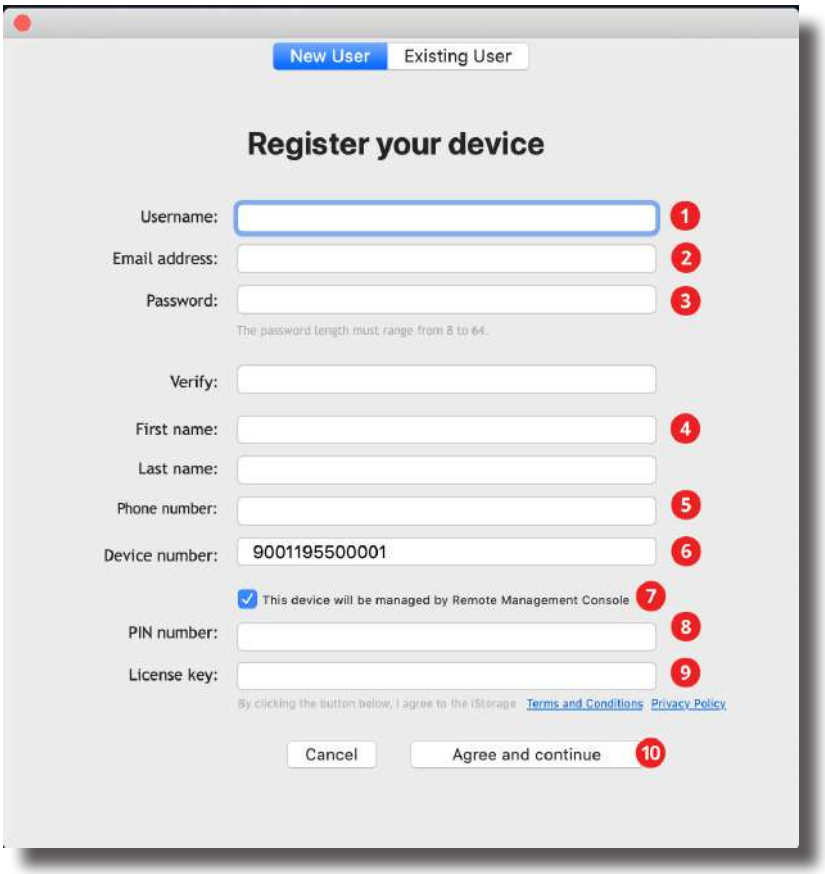
Step 02

Open your macOS client App (image 1) and click '**Sign Up**' to register your cloudAshur hardware security module.

(image 1)

Step 03

To 'Register your cloudAshur' (image 2) complete all the fields under '**New User**'.



(image 2)

1. Enter a '**Username**'.
2. Enter your '**Email Address**'.
3. Enter and verify your '**Password**' - your password must be at least 8 characters long and must contain 3 of 4 of the following: uppercase, lowercase, numeric and special characters.
4. Enter your '**First name**' and '**Last name**'.
5. Enter your '**Phone number**'.
6. The '**Device number**' will be automatically detected if your cloudAshur module is unlocked and connected to your computer (GREEN LED).
7. If your cloudAshur module is to be **Enterprise Registered**, issued to you by your organisation's Administrator, make sure to check the checkbox as in above image 2. If your cloudAshur is to be **Personal Registered** leave the checkbox unchecked, skip steps 8 and 9 and proceed to step 10.
8. Enter the '**PIN**' emailed to you by your Administrator (**Enterprise Registration Only**).
9. Enter the '**License Key**' emailed to you by your Administrator (**Enterprise Registration Only**)
10. Click the '**Register**' button to complete the registration process.

Step 04

Enter your '**Username**' and '**Password**' created during step 3 and then click the '**Login**' button as in image 3 below.

(image 3)

Step 05

After 'Sign in' your cloudAshur virtual drive will open. To add your cloud folder/s and local folders to your cloudAshur virtual drive, click the cloudAshur icon CA in your **menu bar** (top of your screen), and click on preferences and then click on the '**+**' symbol to browse and select your cloud folder/s and any local folder/s as in image 4 below.

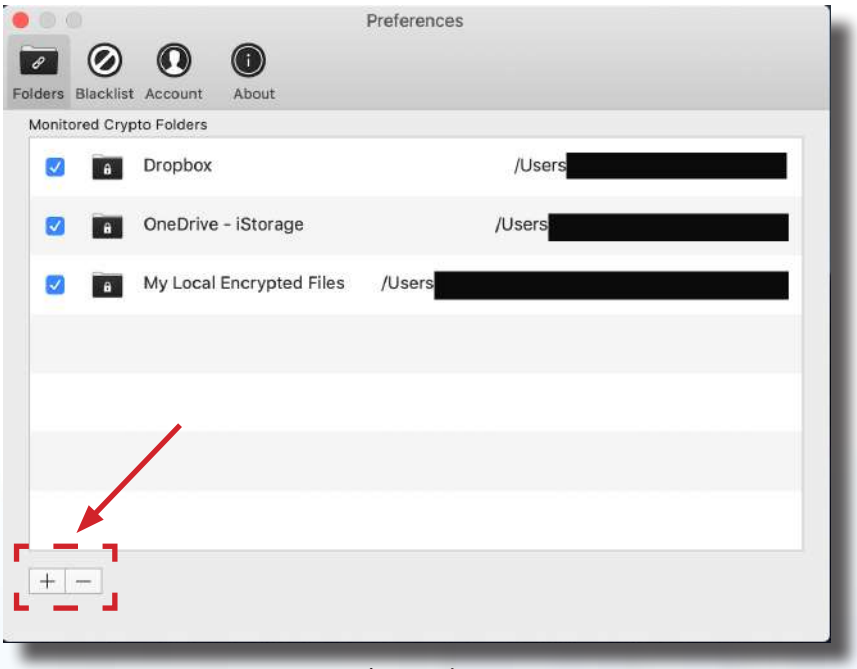
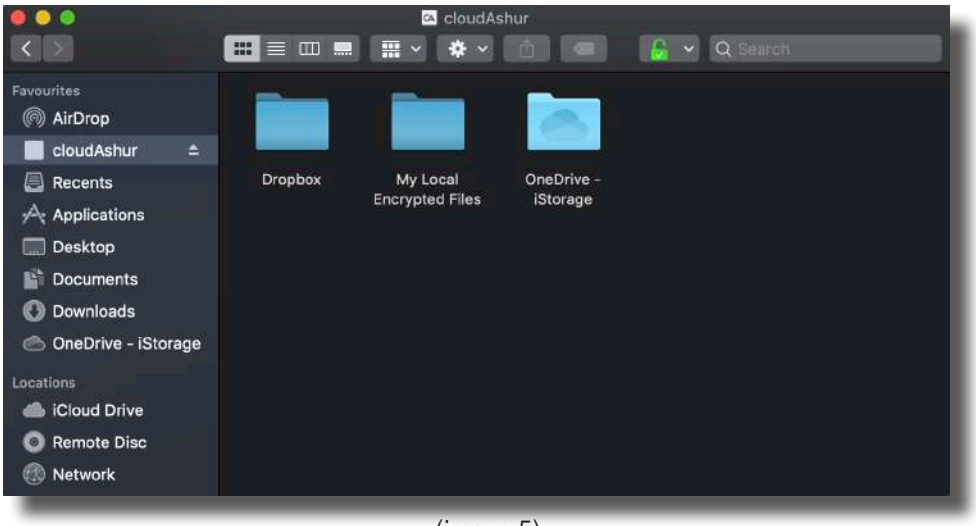


image 4

Step 06

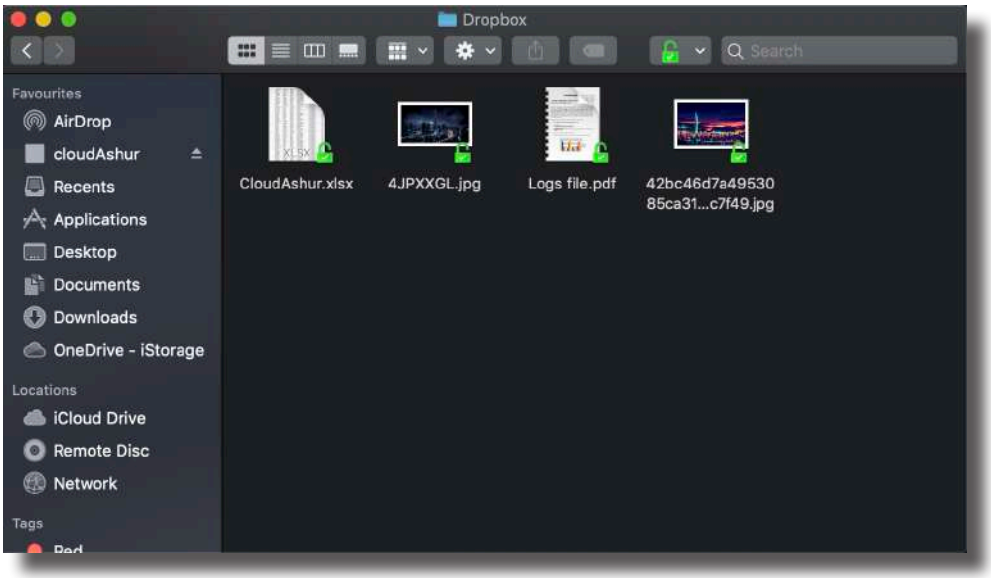
After adding your cloud accounts and any local folder, click the cloudAshur icon CA in your **menu bar** (top of your screen), and then click to open your cloudAshur virtual drive (image 5). Click on your cloud/local folder to open, in this case, '**Dropbox**' as seen below.



(image 5)

Step 07

Drag and drop or copy and paste your files to your cloudAshur virtual drive and a green unlocked padlock symbol will appear on the bottom right hand corner of each file as seen in image 6 indicating the files have been encrypted but can be accessed through your virtual drive. Meanwhile the same files are encrypted when accessed directly from your cloud account.



(image 6)

iStorage®

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 | web: www.istorage-uk.com