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.

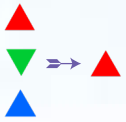
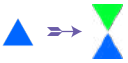
When the cloudAshur is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

3. First Time Use

Your cloudAshur hardware security module ships with the following factory default Admin PIN: **11223344**.

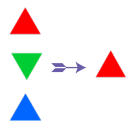
Important! Please Read: In its default state, the cloudAshur hardware security module cannot be registered. You **MUST change the default Admin PIN immediately** as described in the table below (Instructions - first time use).

Please follow the simple steps below to change the default Admin PIN to your own unique 7-15 digit 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
4. With the GREEN LED blinking on and off, press the **KEY (⚷)** button **3** times (**KEY (⚷)** x **3**) within 2 seconds		Blinking GREEN LED will change to a solid BLUE LED indicating the cloudAshur is in Admin Mode
5. With the cloudAshur in **Admin Mode** (solid BLUE LED) press and hold down together both **KEY (⚷)** + **2** buttons		Solid BLUE LED will change to blinking GREEN and solid BLUE LEDs
6. Enter your **NEW** 7-15 digit **Admin PIN** and press the **KEY (⚷)** button once		Blinking GREEN and solid BLUE LEDs will switch to a single GREEN LED blink and then back to blinking GREEN and solid BLUE LEDs
7. Re-enter your **NEW Admin PIN** and press the **KEY (⚷)** button once		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
8. To exit Admin Mode (solid BLUE LED) press and hold the **SHIFT** (⬆) button for one second.		Solid Blue LED will change to a Solid RED LED which then fades out to the idle state

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

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.

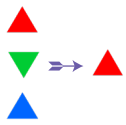
When the cloudAshur is unlocked and connected to a USB port, it will not accept further instructions via the keypad.

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.

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 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- For "**iStorage**" press the following buttons:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

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.

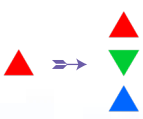
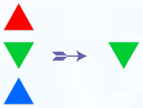
1. In Admin mode, press and hold down both '**SHIFT** (⬆) **+ 3**' buttons		Solid BLUE LED will change to a blinking RED LED
2. Press and hold down both '**SHIFT** (⬆) **+ 3**' buttons again		Blinking RED LED will change to a solid RED LED and then to a solid BLUE LED indicating the User PIN has been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

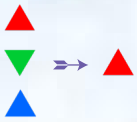
Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the cloudAshur will 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 24 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

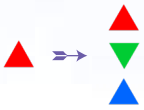
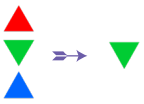
Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the cloudAshur will 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 30) first in order to configure an Admin PIN with full Admin privileges including the ability to configure a User PIN.

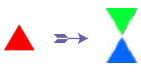
29. How to Configure an Admin PIN after a Brute Force attack or Reset

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

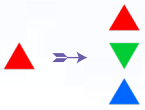
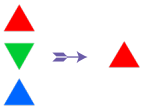
Note: When the cloudAshur is in Admin Mode, the BLUE LED will remain on and solid for 30 seconds only, during which time the cloudAshur can accept instructions via the keypad allowing it to be configured with a host of security features. If no key event happens within 30 seconds, the cloudAshur will 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 24 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 and install 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:

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

Unmanaged Registration

As your cloudAshur hardware security module will not be used in conjunction with '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.

Managed 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 or 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 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: Windows Client App - Sign-in) and click '**Registration**' to register your cloudAshur hardware security module.

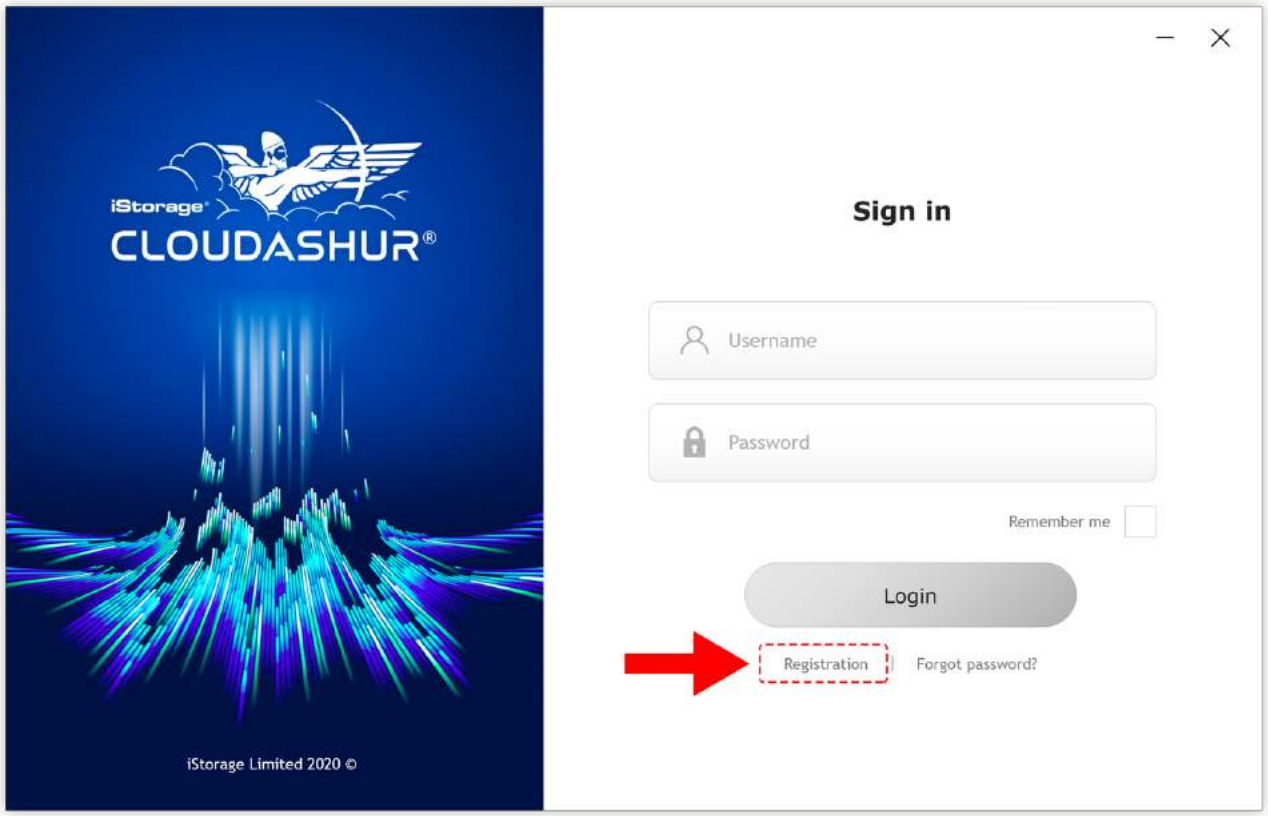


Image 1: Windows Client App - Sign-in

Step 03

To 'Register your cloudAshur' (Image 2: Windows Client App - Registration as a New User) complete all the fields under '**Create New User Account**'.

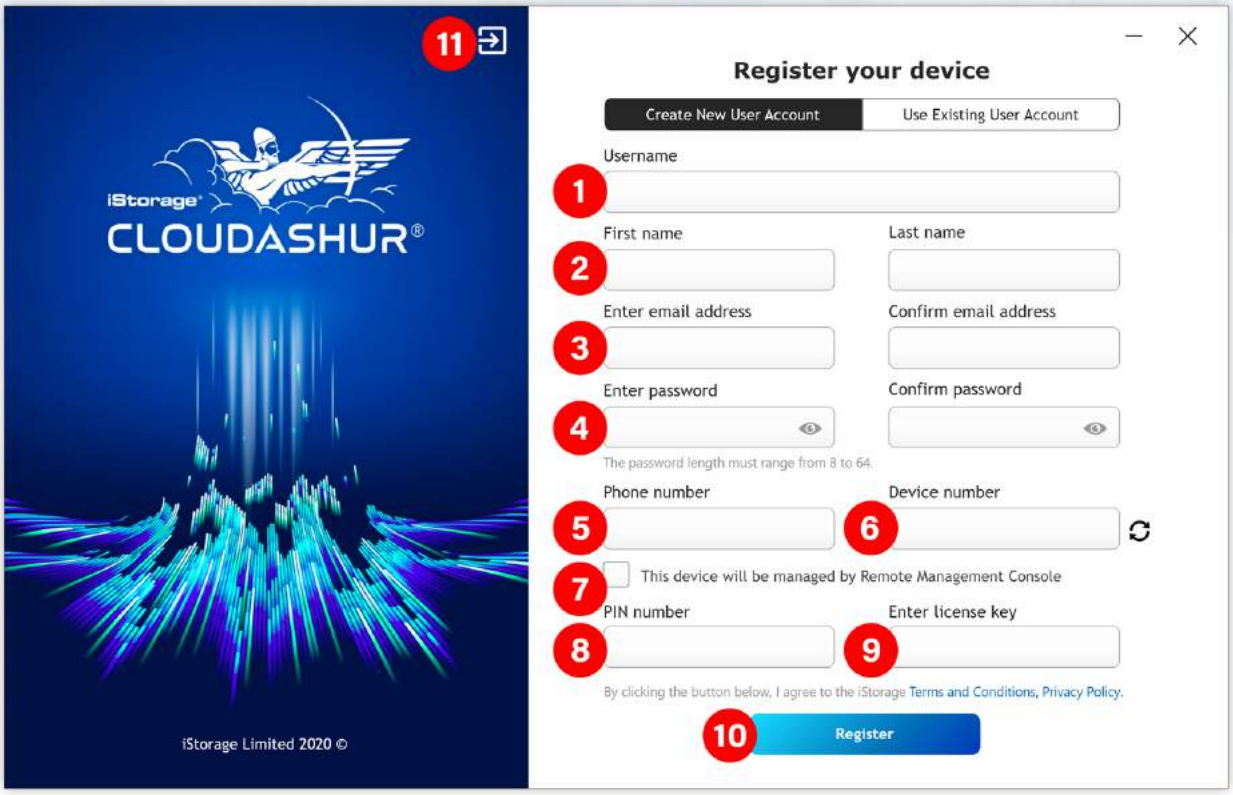


Image 2: Windows Client App - Registration as a New User

1. Enter a '**Username**'.
2. Enter your '**First name**' and '**Last name**.
3. Enter and confirm your '**Email Address**'.
4. Enter and confirm your '**Password**' - your password must be at least 8 to 64 characters in length.
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 managed by the **cloudAshur Remote Management Console (RMC)** and you have received your **Licence Key** and **PIN Number**, make sure to check the checkbox and proceed to the next step, otherwise please leave the checkbox unchecked and proceed to step 10.
8. Enter your **RMC** registration '**PIN**' which should have been emailed to you by your Administrator.
9. Enter your **RMC** registration '**License Key**' which should have been emailed to you by your Administrator.

10. Click the '**Register**' button to complete the registration process, a confirmation message will appear if registration is successful, click '**Okay**' to continue.

Note: If you are registering your cloudAshur as an **Unmanaged Module**, please confirm your email address by following the instructions shown in the verification dialog box as seen in 'Image 3: Windows Client App - Email Verification'.

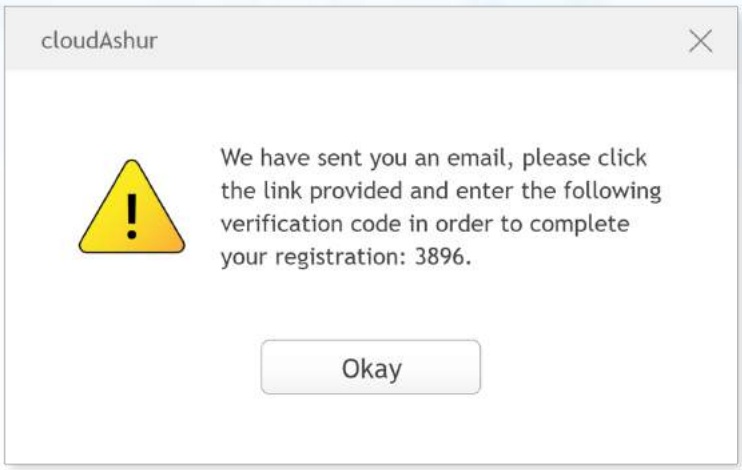


Image 3: Windows Client App - Email Verification

11. Click on the forward button  to go to the login page (step 4).

Step 04

To log into your Client App, enter your '**Username**' and '**Password**' created during step 3 and then click the '**Login**' button (Image 4: Windows Client App - Login). Ensure your cloudAshur hardware security module is unlocked (**GREEN** LED) and connected to your computer.

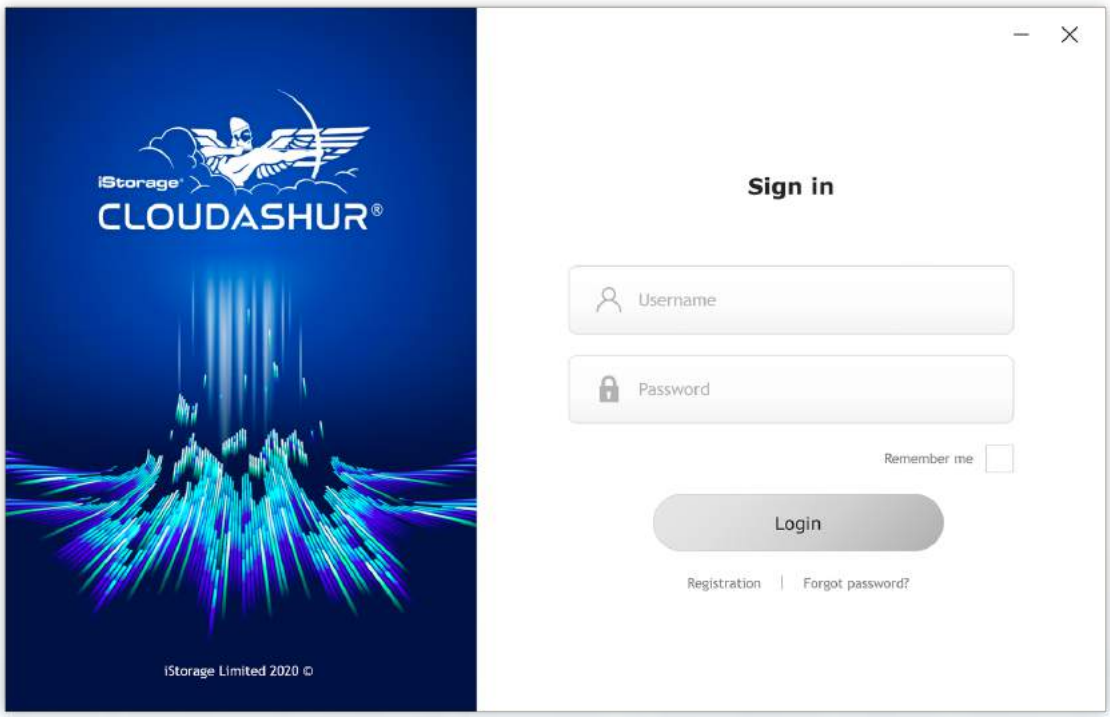


Image 4: Windows Client App - Login

Step 05

Note: In order to connect the iStorage virtual drive to your preferred Cloud account, you will need to download the relevant Cloud desktop app (i.e. Dropbox app, OneDrive app, etc) and install it to your local computer. Should you require assistance in locating the relevant Cloud desktop app, please visit https://istorage-uk.com/desktop-apps

After 'Sign-in' your cloudAshur virtual drive will open. To add your cloud or local folders to your cloudAshur virtual drive, click (once) the cloudAshur icon in your Windows System Tray (bottom right corner of your screen) to open the preferences and then click on the '**+**' symbol to browse and select any preferred Cloud or local folders that you intend to use to store encrypted data (Image 5: Windows Client App - Browse for folder).

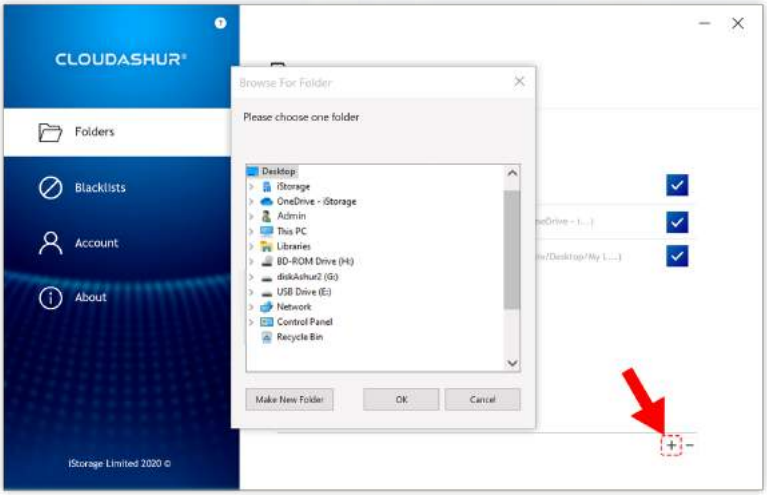


Image 5: Windows Client App - Browse for folder

Step 06

After adding your cloud or local folders (as seen in 'Image 6: Windows Client App - Folders'), **double click** the cloudAshur icon in your system tray (bottom right hand corner of your screen) to open your cloudAshur virtual drive (Image 7: Windows Client App - cloudAshur virtual drive).

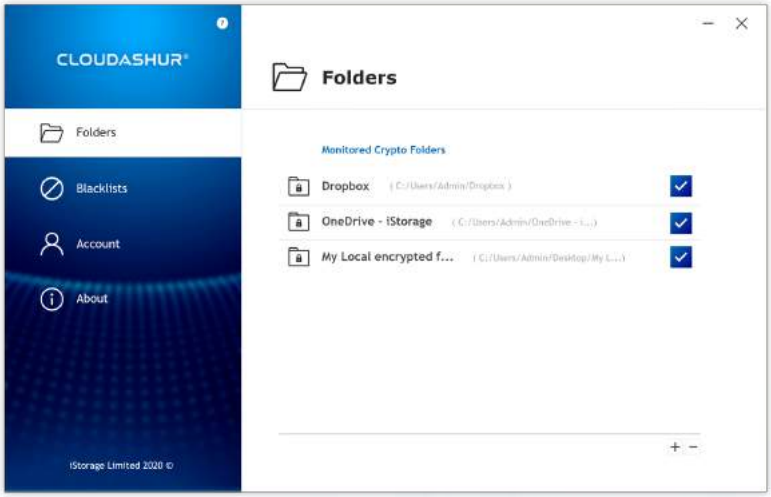


Image 6: Windows Client App - Folders

Step 07

Within your cloudAshur virtual drive, double click on your cloud/local folder to open, in this case, 'OneDrive - iStorage' as seen in 'Image 7: Windows Client App - cloudAshur virtual drive'.

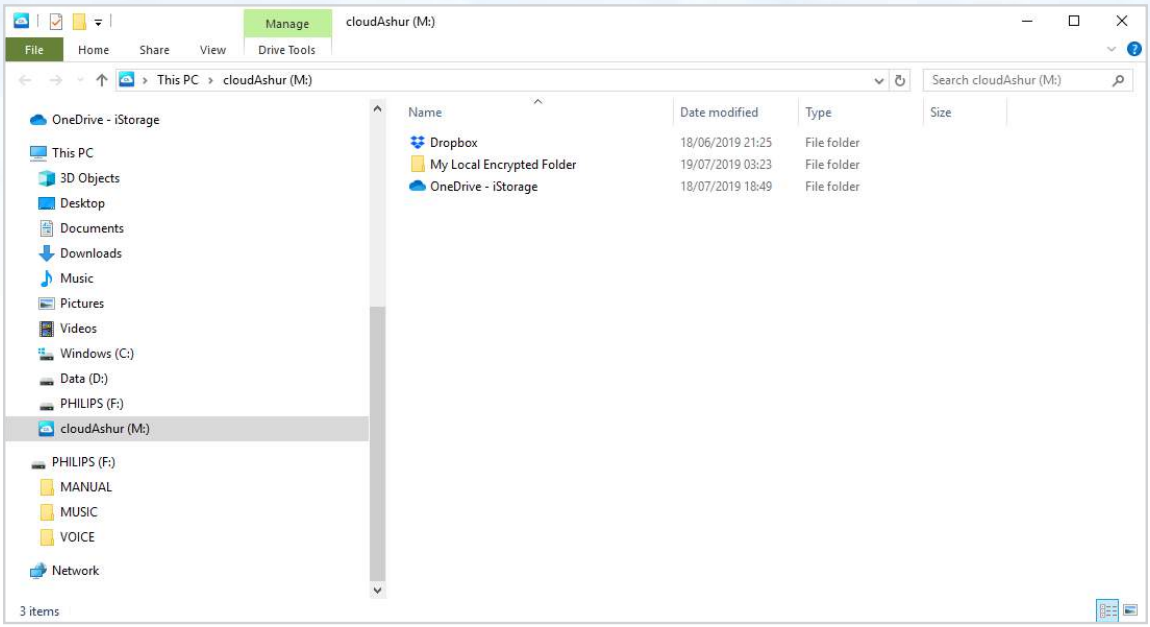


Image 7: Windows Client App - cloudAshur virtual drive

Step 08

Drag and drop or copy and paste your files to a folder within your cloudAshur virtual drive, in this case 'OneDrive - iStorage', and a **GREEN** unlocked padlock symbol will appear on the bottom corner of each file (Image 8: Windows Client App - iStorage OneDrive folder on cloudAshur virtual drive with encrypted files) indicating the file has been encrypted and can be accessed through your virtual drive. Meanwhile the same files are encrypted and cannot be opened when accessed directly from your Cloud account or local folder.

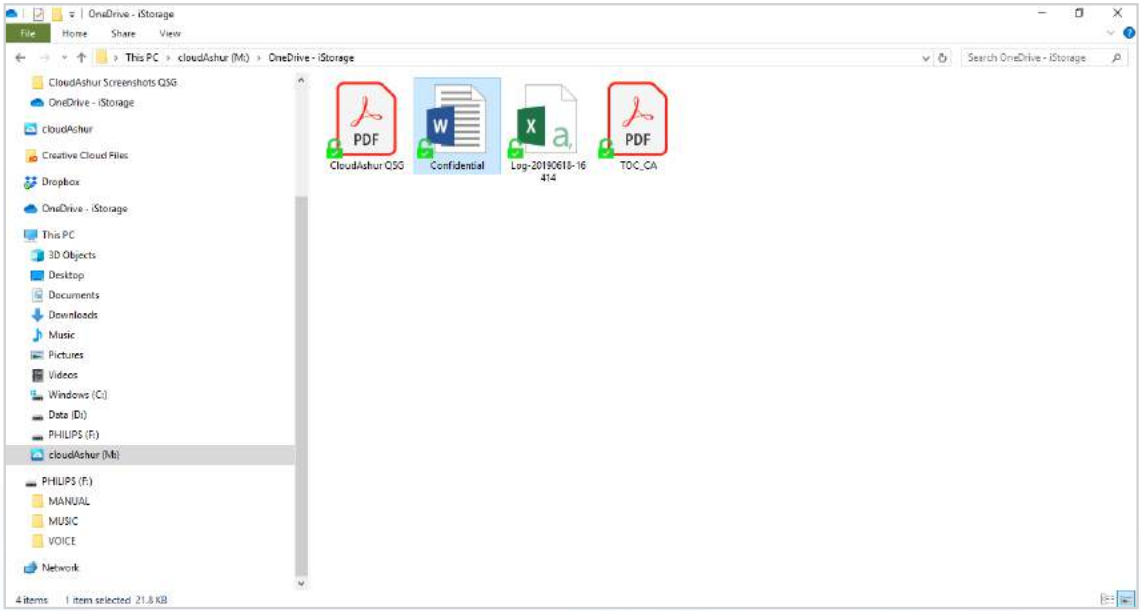


Image 8: Windows Client App - iStorage OneDrive folder on cloudAshur virtual drive with encrypted files

Note: Your cloudAshur will not encrypt any of your files previously stored in your cloud/local folders and will only encrypt those files which are being copied or changed when your cloudAshur module and Client App are authenticated.

42. Registering additional cloudAshur modules using existing User Account (Windows)

If you have previously registered a cloudAshur hardware security module, you will be able to register additional cloudAshur modules using your existing user account (username and password).

To Register additional cloudAshur modules complete all the fields under '**Use Existing User Account**' (Image 9: Windows Client App - Registration using Existing User Account).

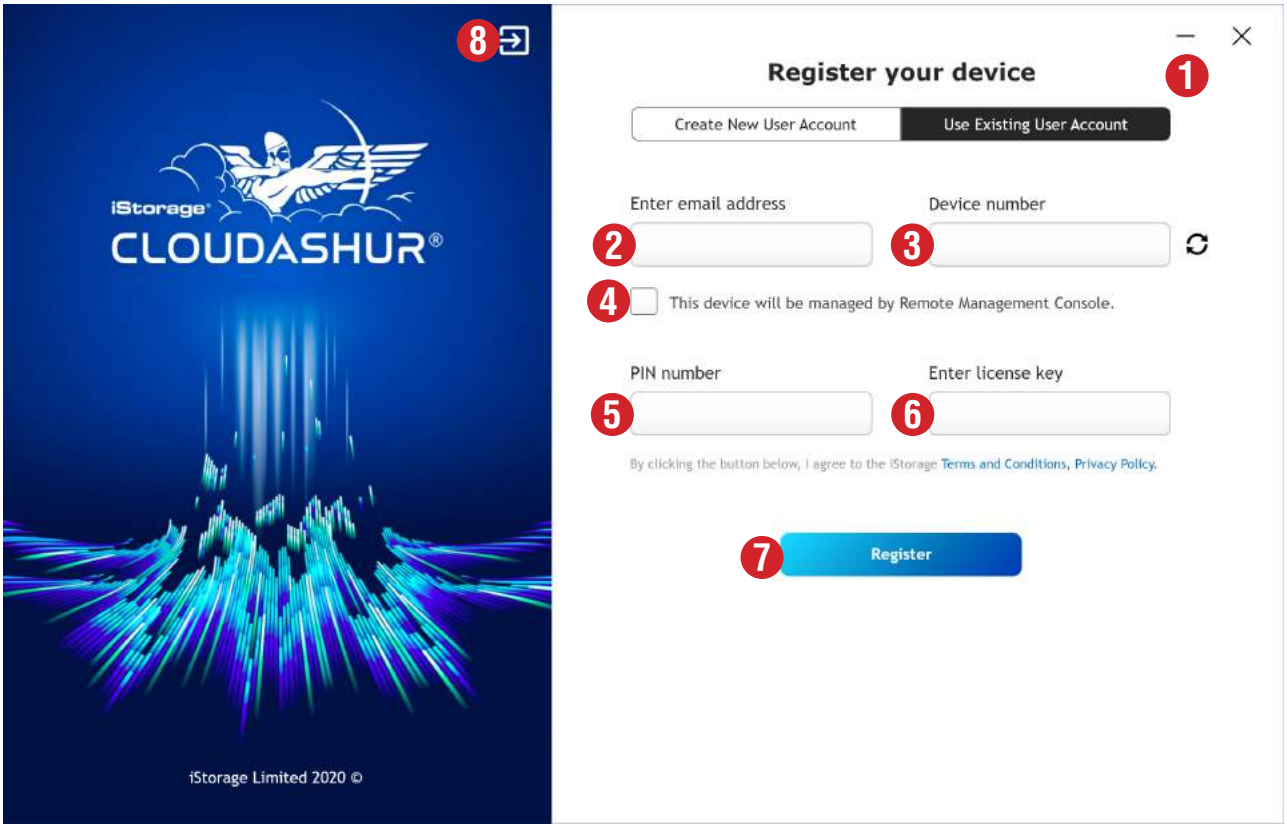


Image 9: Windows Client App - Registration using Existing User Account

1. Click the '**Use Existing User Account**' tab.
2. Enter your '**Email Address**', this must be the same email address previously used to register your cloudAshur Module.
3. The '**Device number**' will be automatically detected if your cloudAshur is unlocked and connected to your computer (solid **GREEN** LED). If the Device number is not displayed, click on the refresh ( ) button to detect.
4. If your cloudAshur module is to be managed by the **cloudAshur Remote Management Console (RMC)** and you have received your **Licence Key** and **PIN Number**, make sure to check the checkbox and proceed to the next step, otherwise please leave the checkbox unchecked and proceed to step 10.
5. Enter the '**PIN number**' emailed to you by your Administrator (**Remote Management Only**).
6. Enter the '**License Key**' emailed to you by your Administrator (**Remote Management Only**).
7. Click the '**Register**' button to complete the registration process, a confirmation message will pop up if registration is successful, click "**Okay**" to continue.

Note: If you are registering your cloudAshur as an **Unmanaged Module**, please confirm your email address by following the instructions shown in the verification dialog box as seen in 'Image 10: Windows Client App - Email Verification'.

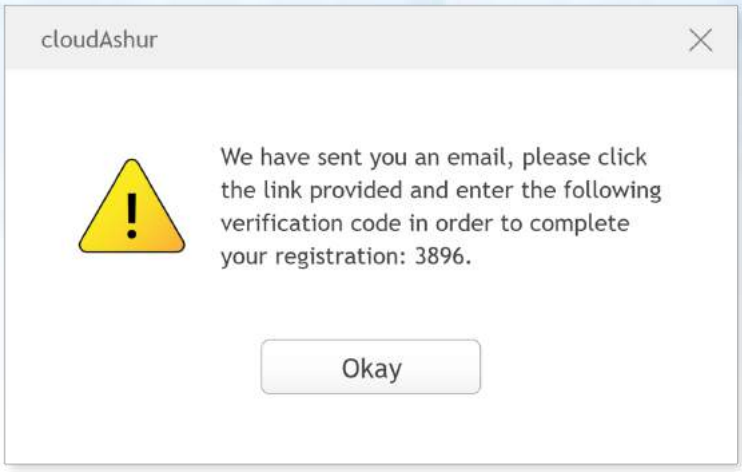


Image 10: Windows Client App - Email Verification

8. Click on the forward button to go to the login page.

43. Sign Up and Install macOS cloudAshur Client App

cloudAshur Registration

Please download and install 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 registration methods that apply to you:

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

Unmanaged Registration

As your cloudAshur hardware security module will not be used in conjunction with '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.

Managed 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 or 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: macOS Client App - Sign-in) and click '**Sign Up**' to register your cloudAshur hardware security module.

Image 1: macOS Client App - Sign-in

Step 03

To 'Register your cloudAshur' (Image 2: macOS Client App - Registration as a New User) complete all the fields under '**Create New User Account**'.

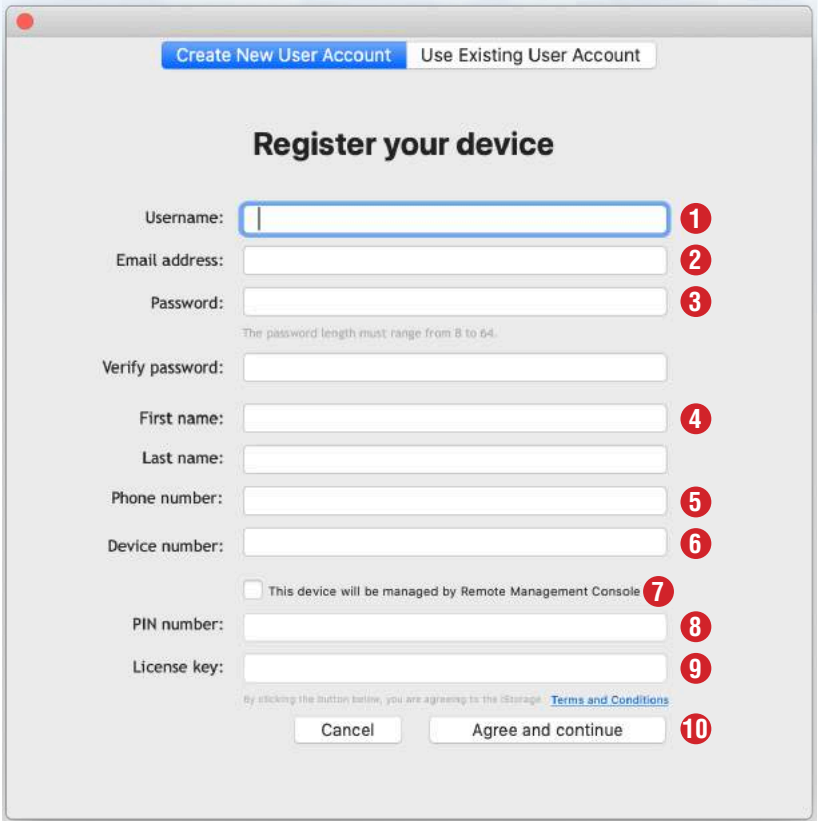


Image 2: macOS Client App - Registration as a New User

1. Enter a '**Username**'.
2. Enter your '**Email Address**'.
3. Enter and Verify your '**Password**' - your password must be at least 8 to 64 characters in length.
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 managed by the **cloudAshur Remote Management Console (RMC)** and you have received your **Licence Key** and **PIN Number**, make sure to check the checkbox and proceed to the next step, otherwise please leave the checkbox unchecked and proceed to step 10.
8. Enter your **RMC** registration '**PIN number**' which should have been emailed to you by your Administrator.
9. Enter your **RMC** registration '**License Key**' which should have been emailed to you by your Administrator.
10. Click the '**Agree and continue**' button to complete the registration process, a confirmation message will appear if registration is successful, click '**Okay**' to continue.

Note: If you are registering your cloudAshur as an **Unmanaged Module**, please confirm your email address by following the instructions shown in the verification dialog box as seen in 'Image 3: macOS Client App - Email Verification'.

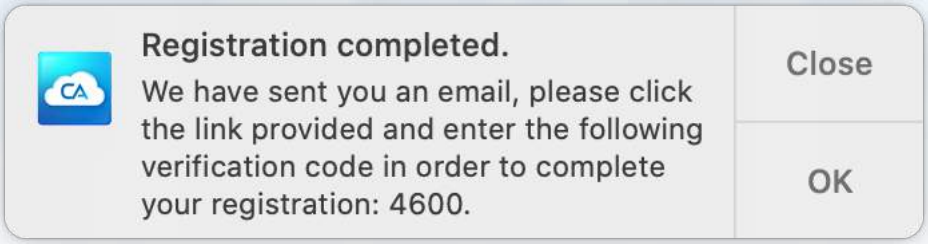


Image 3: macOS Client App - Email Verification

Step 04

To log into your Client App, enter your '**Username**' and '**Password**' created during step 3 and then click the '**Login**' button (Image 4: macOS Client App - Login). Ensure your cloudAshur hardware security module is unlocked (**GREEN** LED) and connected to your computer.

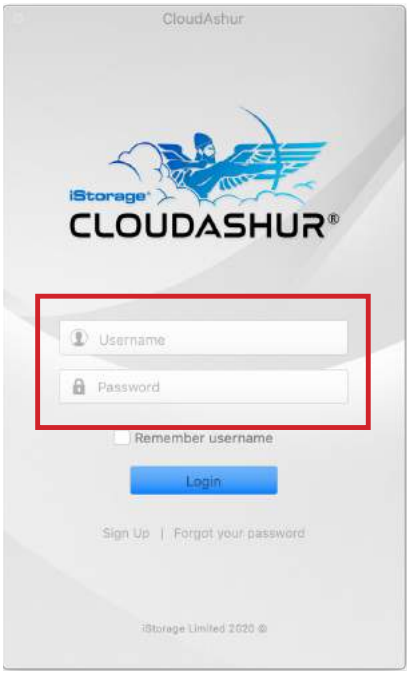


Image 4: macOS Client App - Login

Step 05

Note: In order to connect the iStorage virtual drive to your preferred Cloud account, you will need to download the relevant Cloud desktop app (i.e. Dropbox app, OneDrive app, etc) and install it to your local computer. Should you require assistance in locating the relevant Cloud desktop app, please visit https://istorage-uk.com/desktop-apps

After 'Sign-in' your cloudAshur virtual drive will open. To add your cloud or local folders to your cloudAshur virtual drive, click the cloudAshur icon in your **menu bar** (top of your screen) to open the preferences screen and then click on the '**+**' symbol to browse and select any preferred Cloud or local folders that you intend to use to store encrypted data (Image 5: macOS Client App - Browse for folder).

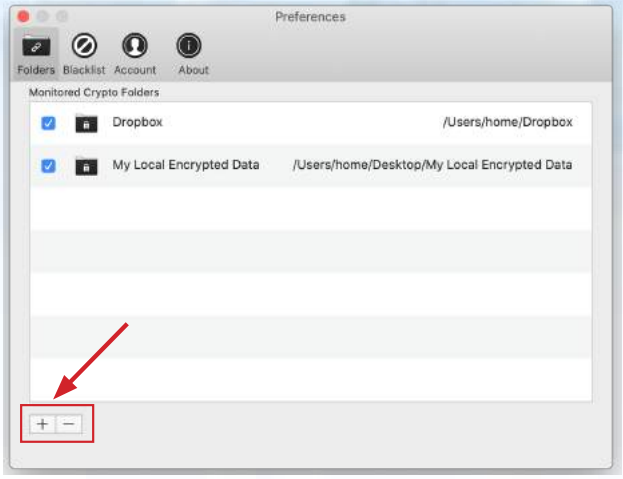


Image 5: macOS Client App - Browse for folder

Step 06

After adding your cloud or local folders, double click the cloudAshur icon CA in your **menu bar** (top of your screen), and then click to open your cloudAshur virtual drive (Image 6: macOS Client App - cloudAshur virtual folder). Click on your cloud/local folder to open, in this case, '**Dropbox**' as seen below.

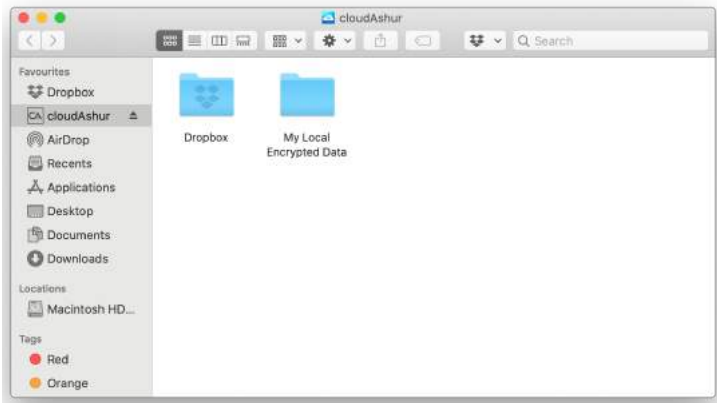


Image 6: macOS Client App - cloudAshur virtual folder

Step 07

Drag and drop or copy and paste your files to a folder within your cloudAshur virtual drive, in this case 'OneDrive - iStorage', and a **GREEN** unlocked padlock symbol will appear on the bottom corner of each file (Image 7: macOS Client App -iStorage OneDrive folder on cloudAshur virtual drive with encrypted files) indicating the file has been encrypted and can be accessed through your virtual drive. Meanwhile the same files are encrypted and cannot be opened when accessed directly from your Cloud account or local folder.

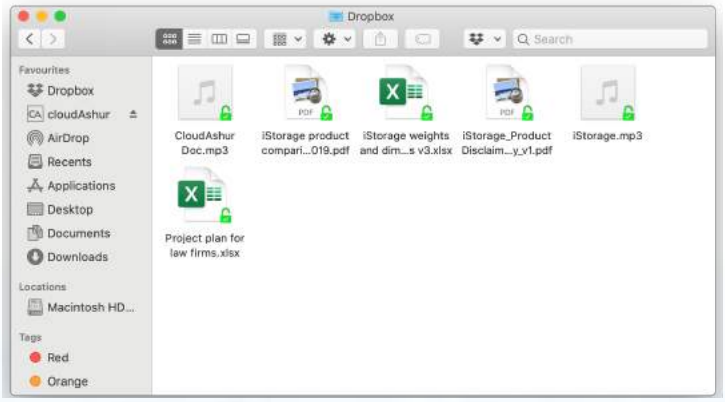


Image 7: macOS Client App -iStorage OneDrive folder on cloudAshur virtual drive with encrypted files

Note: Your cloudAshur will not encrypt any of your files previously stored in your cloud/local folders and will only encrypt those files which are being copied or changed when your cloudAshur module and Client App are authenticated.

44. Registering additional cloudAshur modules using existing User Account (macOS)

If you have previously registered a cloudAshur hardware security module, you will be able to register additional cloudAshur modules using your existing user account (username and password).

To Register additional cloudAshur modules (Image 8: macOS Client App - Registration using Existing User Account) complete all the fields under '**Use Existing User Account**'.

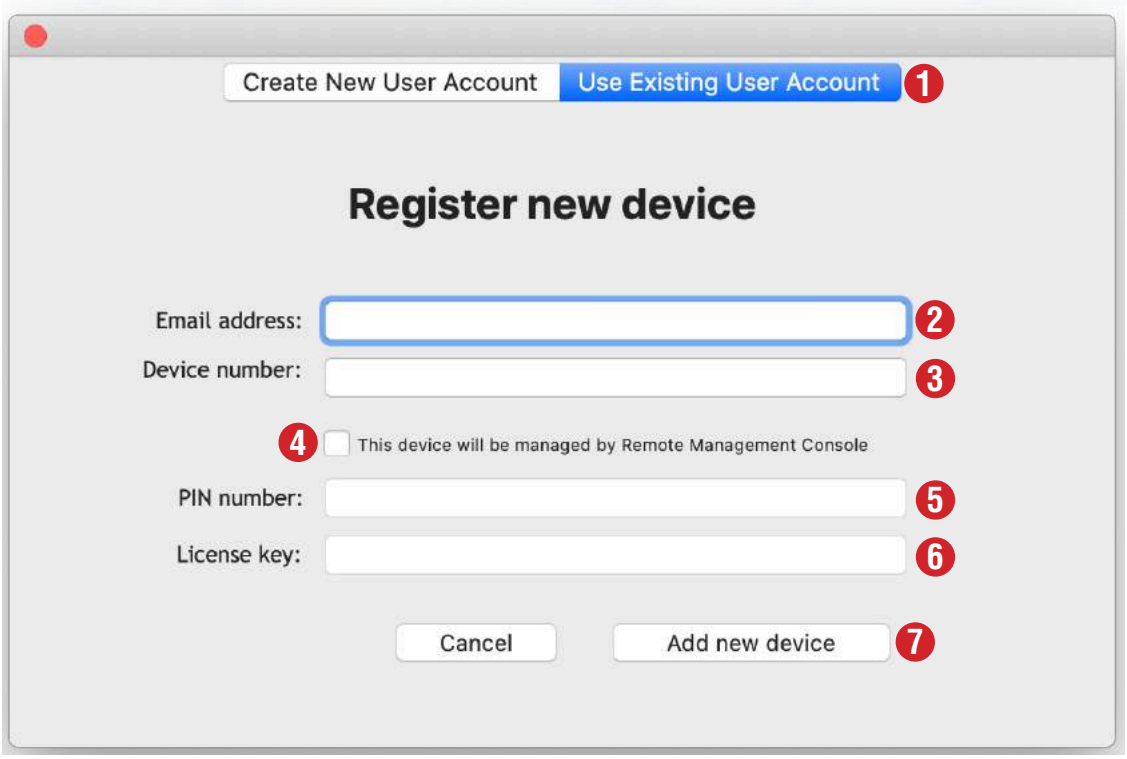


Image 8: macOS Client App - Registration using Existing User Account

1. Click the '**Use Existing User Account**' tab.
2. Enter your '**Email Address**', this must be the same email address previously used to register your cloudAshur Module.
3. The '**Device number**' will be automatically detected if your cloudAshur is unlocked and connected to your computer (solid **GREEN** LED).
4. If your cloudAshur module is to be managed by the **cloudAshur Remote Management Console (RMC)** and you have received your **Licence Key** and **PIN Number**, make sure to check the checkbox and proceed to the next step, otherwise please leave the checkbox unchecked and proceed to step 10.
5. Enter the '**PIN number**' emailed to you by your Administrator (**Remote Management Only**).
6. Enter the '**License Key**' emailed to you by your Administrator (**Remote Management Only**).
7. Click the '**Add new device**' button to complete the registration process, a confirmation message will pop up if registration is successful, click "**Okay**" to continue.

Note: If you are registering your cloudAshur as an **Unmanaged Module**, please confirm your email address by following the instructions shown in the verification dialog box as seen in 'Image 9: macOS Client App - Email Verification'.

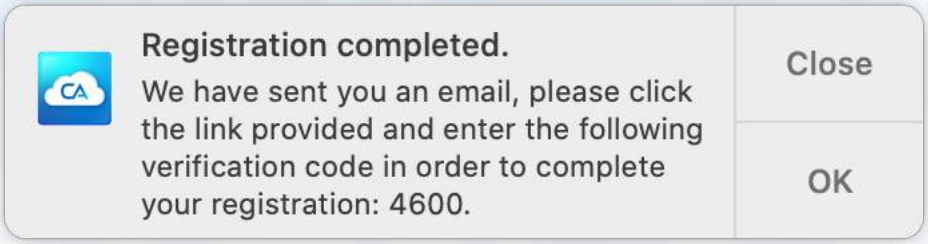
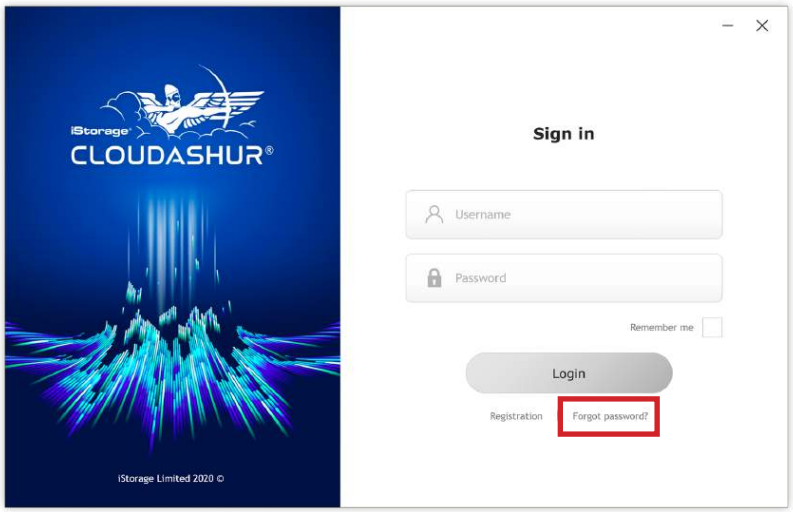


Image 9: macOS Client App - Email Verification

45. How to Reset a Forgotten Password

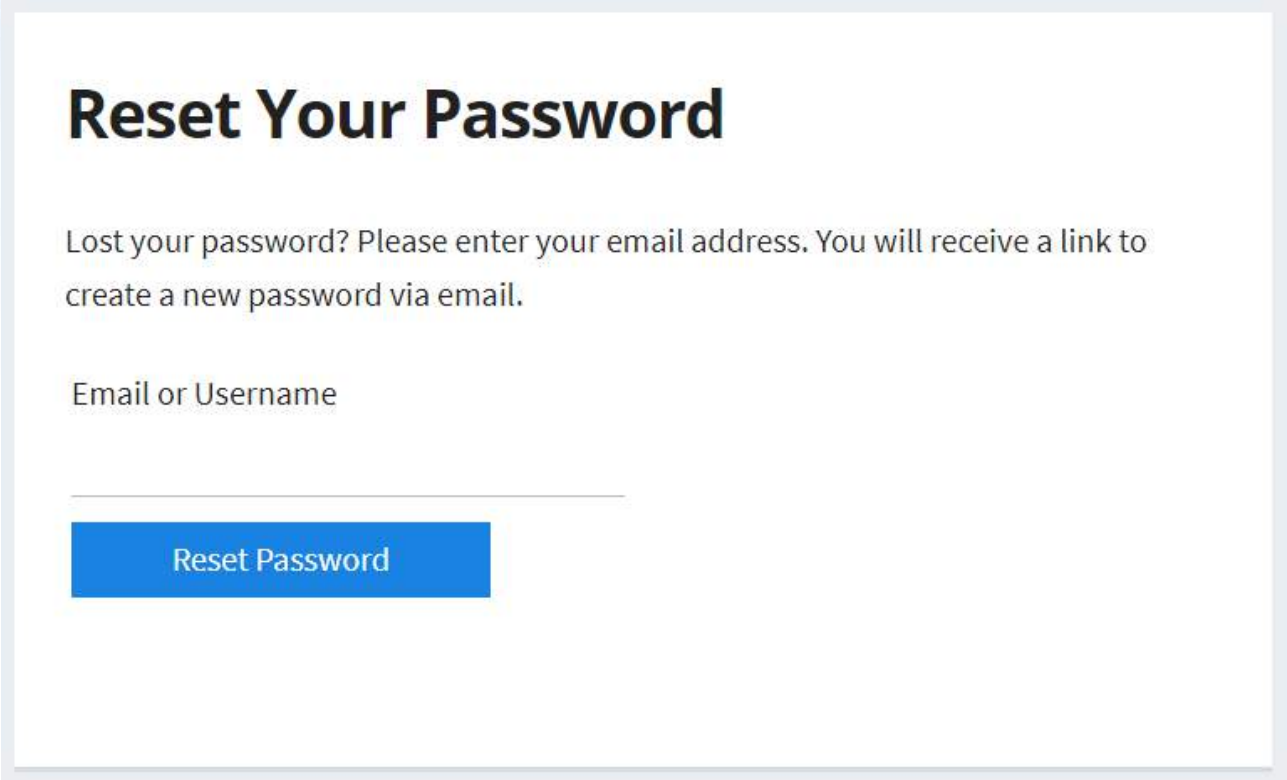
1. To reset a forgotten password using **Windows**, open your cloudAshur Client App (Sign in) and click '**Forgot password**'. For **macOS**, open your cloudAshur Client App and click '**Forgot your password**'.



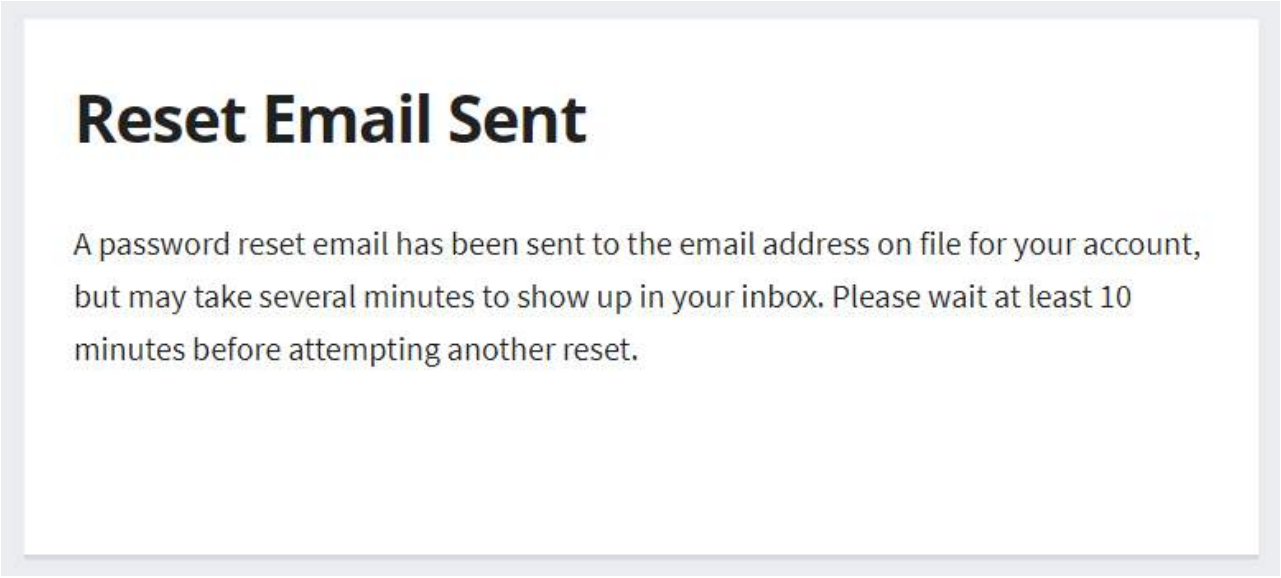
Windows Client App - Sign-in

macOS Client App - Sign-in

2. Enter your '**Email address**' or '**Username**' and then click '**Reset Password**'.



3. A 'Reset Email' will be sent to your registered email address. Follow the instructions contained in the email to reset your forgotten password.



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

Handbuch

Vergessen Sie Ihre PIN (Ihr Passwort) nicht, da Sie ohne PIN/Passwort nicht auf Ihre verschlüsselten Daten zugreifen können.

Wenn Sie Probleme bei der Nutzung von cloudAshur haben, wenden Sie sich per E-Mail oder telefonisch an unsere Technical Support-Abteilung: support@istorage-uk.com oder +44 (0) 20 8991 6260.

RoHS Compliant

REACH COMPLIANCE

Konform mit Trade Agreements Act (TAA)

Inhaltsverzeichnis

Einführung

Hinweis: Der Akku der cloudAshur ist nicht vollständig geladen. Wir empfehlen, den Akku vor der ersten Verwendung vollständig aufzuladen. Schließen Sie die cloudAshur bitte 20–30 Minuten lang an einen USB-Anschluss mit Stromversorgung an, um den Akku vollständig aufzuladen.

Vielen Dank, dass Sie sich für das iStorage cloudAshur-Hardwaresicherheitsmodul entschieden haben – einen einzigartigen physischen Schlüssel für Ihre Daten. Es ist die perfekte Lösung für alle, die Daten so sicher wie nur irgend möglich in der Cloud speichern, teilen (einschließlich E-Mail- und Datenübertragungsdienste) und verwalten möchten, da es die Sicherheitsanfälligkeiten von Cloudplattformen wie mangelnde Kontrolle, Eigentumsrecht- und Datenschutzprobleme sowie unbefugte Zugriffe beseitigt.

Das cloudAshur-Hardwaresicherheitsmodul bietet eine Fünffaktorauthentifizierung:

- **Was Sie haben**:

1. Ihr cloudAshur-Hardwaresicherheitsmodul, der physische Schlüssel zu Ihren Daten.

- **Was Sie wissen**:

2. Ihre 7- bis 15-stellige PIN für das cloudAshur-Hardwaresicherheitsmodul.
3. Ihr Benutzername und Ihr Passwort für die cloudAshur-Client-App.
4. Wo Ihre Daten gespeichert werden (Cloudspeicher).
5. Benutzername und Passwort für Ihr Cloudkonto.

Außerdem können Ihre cloudAshur-Hardwaresicherheitsmodule auch mit der cloudAshur Remote Management Console von iStorage verwaltet und überwacht werden. Dadurch haben Sie die vollständige Kontrolle über alle cloudAshur-Hardwaresicherheitsmodule, die in Ihrem Unternehmen eingesetzt werden. Dem Administrator steht damit eine breite Palette an Funktionen für eine mühelose Verwaltung und Überwachung aller Benutzer zur Verfügung, wie z. B. Echtzeit-Geofencing, Timefencing, Benutzerprotokolle, Ferndeaktivierung, Remote-Kill und vieles mehr.

Paketinhalt

- Das cloudAshur-Hardwaresicherheitsmodul von iStorage
- Hülle aus stranggepresstem Aluminium
- Schnellanleitung

Registrieren und Installieren Ihrer cloudAshur-Client-App

Dieses Handbuch besteht aus zwei Teilen – **Teil A** (Abschnitt 1–40) und **Teil B** (Abschnitt 41 und 42).

Sie müssen Ihr cloudAshur-Hardwaresicherheitsmodul zuerst gemäß der Beschreibung in **Teil A** in diesem Handbuch mit den entsprechenden Einstellungen konfigurieren. Dazu zählt z. B. das Ändern der Admin-PIN, das Konfigurieren einer Benutzer-PIN sowie einer Selbstzerstörungs-PIN usw.

Nach der Konfiguration des cloudAshur-Hardwaresicherheitsmoduls mit Ihren bevorzugten Einstellungen (**Teil A**) können Sie gemäß **Teil B** Ihre cloudAshur-Client-App für Windows oder macOS registrieren und installieren.

TEIL A

1. LED-Anzeigen und ihre Aktionen

LED	LED-Zustand	Beschreibung	LED	LED-Status	Beschreibung
▲	ROT leuchtet durchgehend	Gesperrtes cloudAshur (entweder im Standby- oder Zurücksetz-Status)	▲	BLAU leuchtet durchgehend	cloudAshur im Admin-Modus
▲	ROT – erlischt langsam	cloudAshur Wird abgeschaltet	▲▼▲	ROT, GRÜN und BLAU blinkt	Wartet auf die Eingabe der Benutzer-PIN
▼	GRÜN blinkt	Entsperrtes cloudAshur als Admin (nicht am USB-Anschluss angeschlossen)	▼▲	GRÜN und BLAU blinken gemeinsam	Wartet auf die Eingabe der Admin-PIN
▼	GRÜN leuchtet durchgehend	Entsperrtes cloudAshur als Benutzer (nicht am USB-Anschluss angeschlossen) oder cloudAshur im Benutzermodus	▼▲	GRÜN und BLAU blinken abwechselnd	Authentifizierung läuft
▼	GRÜN leuchtet durchgehend	cloudAshur entsperrt und mit dem Host verbunden	▲		Die blaue LED blinkt während des Ladevorgangs alle 5 Sekunden

2. Akku- und LED-Status

Hinweis: Die normale Funktion der cloudAshur kann durch starke elektromagnetische Störungen beeinträchtigt werden. Wenn das der Fall ist, schalten Sie das Produkt einfach aus und anschließend wieder ein, um den normalen Betrieb wieder aufzunehmen. Wenn der normale Betrieb nicht wieder aufgenommen wird, verwenden Sie das Produkt bitte an einem anderen Ort.

Sensor für niedrigen Akkustand

Die cloudAshur enthält einen Spannungserfassungskreis, der die Akkuausgangsleistung überwacht, wenn die cloudAshur eingeschaltet ist. Wenn die Akkuausgangsleistung auf oder unter 3,3 V abfällt, blinkt die ROTE LED dreimal auf und erlischt langsam. An diesem Punkt sollte der Benutzer die cloudAshur an einen USB-Anschluss mit Stromversorgung anschließen und 20–30 Minuten lang aufladen. Sobald sie aufgeladen ist, nimmt die cloudAshur ihre normale Funktion wieder auf.

Aus dem Leerlauf aktivieren

Der Leerlauf ist als der Zustand definiert, in dem die cloudAshur nicht verwendet wird und alle LEDs aus sind.
Zum Aktivieren der cloudAshur aus dem Leerlauf führen Sie Folgendes aus:

Halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt oder schließen Sie die cloudAshur an einen USB-Anschluss mit Stromversorgung an.	▲ ▼ → ▲ ▲	Die ROTE, die GRÜNE und die BLAUE LED blinken nacheinander jeweils einmal. Danach blinkt die GRÜNE LED zweimal und schließlich zeigt die ROTE LED Dauerlicht. Das bedeutet, dass sich die cloudAshur im Standby-Modus befindet.

In den Leerlauf wechseln

Um den Wechsel der cloudAshur in den Leerlauf (alle LEDs sind aus) zu erzwingen, führen Sie eines der folgenden Verfahren durch:

- Wenn die cloudAshur an einem USB-Anschluss angeschlossen ist, trennen Sie sie.
- Wenn die cloudAshur nicht an einem USB-Anschluss angeschlossen ist, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt, bis die ROTE LED Dauerlicht zeigt und dann beim Wechsel in den Leerlauf (Aus) langsam erlischt.

Eingeschalteter Status

Nach dem Aktivieren aus dem Leerlauf wechselt die cloudAshur in einen der drei möglichen, in der nachstehenden Tabelle gezeigten Zustände.

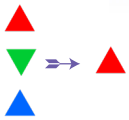
Eingeschalteter Zustand	LED-Anzeige	Verschlüs-selungsschlüs-sel	Admin-PIN	Beschreibung
Standby	ROT leuchtet durchgehend	✓	✓	Wartet auf die Eingabe der Admin- oder Be-nutzer-PIN
Rücksetzung	ROT leuchtet durchgehend	×	×	Wartet auf die Konfiguration einer Admin-PIN
Niedriger Akkustand	ROT blinkt dreimal	✓	✓	Aufladen an einem USB-Anschluss mit Strom-versorgung für 15–30 Minuten

Hinweis: Wenn die cloudAshur entsperrt und nicht an einem USB-Anschluss angeschlossen ist und wenn innerhalb von 30 Sekunden keine Aktionen ausgeführt werden, wechselt die cloudAshur automatisch in den Leerlauf. Die ROTE LED zeigt Dauerlicht und erlischt danach langsam.
Wenn eine gesperrte cloudAshur an einem USB-Anschluss mit Stromversorgung angeschlossen ist, beginnt der Ladevorgang nach 30 Sekunden.
Das wird durch eine blinkende BLAUE LED angezeigt.
Wenn die cloudAshur entsperrt und an einem USB-Anschluss mit Stromversorgung angeschlossen ist, akzep-tiert sie keine weiteren Anweisungen über die Tastatur.

3. Erstmalige Verwendung

Ihr cloudAshur-Hardwaresicherheitsmodul wird mit der folgenden werkseitig eingestellten Admin-PIN ausgeliefert: **11223344**.
Wichtig: Das cloudAshur-Hardwaresicherheitsmodul kann im Auslieferungszustand nicht registriert werden. Sie **MÜSSEN die Standard-Admin-PIN sofort** wie in Abschnitt 7 „**Ändern der Admin-PIN**" beschrieben ändern, damit Sie Ihr cloudAshur-Hardwaresicherheitsmodul über die cloudAshur-Clientanwendung registrieren können.

Um die cloudAshur zum ersten Mal mit der werkseitig eingestellten Admin-PIN zu entsperren, befolgen Sie einfach die nachstehenden Schritte.

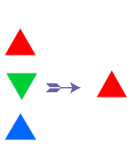
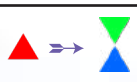
Anweisungen – erstmalige Verwendung	LED	LED-Status
1. Halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt.		Die ROTE, die GRÜNE und die BLAUE LED blinken nacheinander jeweils einmal. Danach blinkt die GRÜNE LED zweimal und schließlich zeigt die ROTE LED Dauerlicht. Das bedeutet, dass sich die cloudAshur im Standby-Modus befindet.
2. Drücken Sie im Standby-Modus (ROTE LED leuchtet durchgehend) einmal auf die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und die BLAUE LED blinken gemeinsam.
3. Wenn die GRÜNE und die BLAUE LED gemeinsam blinken, geben Sie die **Admin-PIN** (werkseitige Voreinstellung: **11223344**) ein und drücken Sie einmal auf die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und die BLAUE LED blinken mehrere Male abwechselnd. Danach wechselt die Anzeige von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN LED. Das bedeutet, dass die cloudAshur als Admin entsperrt ist.

Hinweis: Sobald die cloudAshur erfolgreich entsperrt wurde, blinkt die GRÜNE LED nur noch 30 Sekunden lang. In dieser Zeit muss die cloudAshur an einem USB-Anschluss mit Stromversorgung angeschlossen werden. Sie kann umgehend gesperrt werden, in dem Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt halten.
Wenn die cloudAshur entsperrt und an einem USB-Anschluss angeschlossen ist, akzeptiert sie keine weiteren Anweisungen über die Tastatur.

Sperren der cloudAshur
Um die cloudAshur zu sperren, trennen Sie sie einfach vom USB-Anschluss oder rechtsklicken Sie in der cloudAshur-App auf die Taskleiste und klicken dann auf „Beenden".

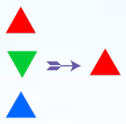
4. Entsperren der cloudAshur mit der Admin-PIN

Befolgen Sie bitte die einfachen Schritte in der nachstehenden Tabelle, um die cloudAshur mit Ihrer 7- bis 15-stelligen Admin-PIN zu entsperren.

1. Halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt.		Die ROTE, die GRÜNE und die BLAUE LED blinken nacheinander jeweils einmal. Danach blinkt die GRÜNE LED zweimal und schließlich zeigt die ROTE LED Dauerlicht. Das bedeutet, dass sich die cloudAshur im Standby-Modus befindet.
2. Drücken Sie im Standby-Modus (ROTE LED leuchtet durchgehend) einmal auf die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und die BLAUE LED blinken gemeinsam.
3. Wenn die GRÜNE und die BLAUE LED gemeinsam blinken, geben Sie Ihre **Admin-PIN** ein und drücken Sie einmal auf die **SCHLÜSSEL**-Taste (🔑).		Die GRÜNE und die BLAUE LED blinken mehrere Male abwechselnd. Danach wechselt die Anzeige von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN LED. Das bedeutet, dass die cloudAshur als Admin entsperrt ist.

5. In den Admin-Modus wechseln

Um in den Admin-Modus zu wechseln, gehen Sie wie folgt vor:

1. Halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt.		Die ROTE, die GRÜNE und die BLAUE LED blinken einmal in Folge. Danach blinkt die GRÜNE LED zweimal und wird schließlich zu einer durchgehend leuchtenden ROTEN LED. Das bedeutet, dass sich die cloudAshur im Standby-Modus befindet.
2. Drücken Sie im Standby-Modus (ROTE LED leuchtet durchgehend) einmal auf die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und die BLAUE LED blinken gemeinsam.
3. Wenn die GRÜNE und die BLAUE LED gemeinsam blinken, geben Sie die **Admin-PIN** ein (werkseitige Voreinstellung: **11223344**) und drücken Sie einmal auf die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE und die BLAUE LED blinken mehrere Male abwechselnd. Danach wechselt die Anzeige von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN LED. Das bedeutet, dass die cloudAshur als Admin entsperrt ist.
4. Drücken Sie die **SCHLÜSSEL-Taste (🔑)** innerhalb von 2 Sekunden **dreimal** (**SCHLÜSSEL-Taste (🔑)** x **3**).		Die Anzeige wechselt von einer blinkenden GRÜNEN LED zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass sich die cloudAshur im Admin-Modus befindet.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

6. Admin-Modus beenden

Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Wechsel in den Leerlauf langsam erlischt.

7. Ändern der Admin-PIN

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern aufweisen
- Darf nicht nur gleiche Ziffern enthalten, wie z. B. (3-3-3-3-3-3-3)
- Darf nicht nur sequenzielle Ziffern enthalten, wie z. B. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Passwort-Tipp: Sie können einen einprägsamen Begriff, Namen, Ausdruck oder eine andere alphanumerische PIN-Kombination erstellen, indem Sie einfach die Tasten mit den entsprechenden Buchstaben drücken.

Beispiele für alphanumerische PINs sind:

- Für „**Passwort**“ drücken Sie die folgenden Tasten:
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Für „**iStorage**“ drücken Sie die folgenden Tasten:
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Mit dieser Methode können lange und einfach zu merkende PINs konfiguriert werden.

Um die Admin-PIN zu ändern, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 2** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und dann zu einer durchgehend leuchtenden BLAUEN LED.
2. Geben Sie die **neue Admin-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie die **neue Admin-PIN** erneut ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED zu einer schnell blinkenden BLAUEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Admin-PIN erfolgreich geändert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

8. Einstellen einer Benutzer-PIN-Richtlinie

Der Administrator kann eine Beschränkungsrichtlinie für die Benutzer-PIN festlegen. Diese Richtlinie umfasst das Einstellen der PIN-Mindestlänge (7 bis 15 Zeichen) sowie die Angabe, ob ein oder mehrere „**Sonderzeichen**“ erforderlich sind oder nicht. Die „Sonderzeichen“ werden verfügbar, wenn die Tasten „**UMSCHALTTASTE** (⬆) + **Ziffer**“ gleichzeitig gedrückt werden.

Um eine Benutzer-PIN-Richtlinie (Beschränkungen) festzulegen, müssen Sie 3 Ziffern eingeben wie etwa „**091**“. Die ersten beiden Ziffern (**09**) geben die Mindest-PIN-Länge an (in diesem Fall **9**). Die letzte Ziffer (**1**) weist darauf hin, dass ein oder mehrere „Sonderzeichen“ verwendet werden müssen, d. h. „**UMSCHALTTASTE** (⬆) + **Ziffer**“. Auf die gleiche Weise kann eine Benutzer-PIN-Richtlinie ohne die Notwendigkeit eines „Sonderzeichens“ eingestellt werden. Bei „**120**“ zum Beispiel geben die ersten beiden Ziffern (**12**) die Mindestlänge der PIN an (in diesem Fall **12**). Die letzte Ziffer (**0**) bedeutet, dass kein Sonderzeichen erforderlich ist.

Sobald der Administrator die Benutzer-PIN-Richtlinie festgelegt hat, wie zum Beispiel „091“, muss eine neue Benutzer-PIN konfiguriert werden – siehe Abschnitt 11, „Neue Benutzer-PIN im Admin-Modus hinzufügen“. Wenn der Administrator die Benutzer-PIN als „**247688314**“ mit Verwendung eines „**Sonderzeichens**“ (**UMSCHALTTASTE** (⬆) **+ Ziffer** gleichzeitig drücken) konfiguriert, kann dieses Sonderzeichen wie in den folgenden Beispielen gezeigt bei der Erstellung der Benutzer-PIN an einer beliebigen Stelle in der 7- bis 15-stelligen PIN platziert werden.

A. „**UMSCHALTTASTE** (⬆) **+ 2**“, „4“, „7“, „6“, „8“, „8“, „3“, „1“, „4“,

B. „2“, „4“, „**UMSCHALTTASTE** (⬆) **+ 7**“, „6“, „8“, „8“, „3“, „1“, „4“,

C. „2“, „4“, „7“, „6“, „8“, „8“, „3“, „1“, „**UMSCHALTTASTE** (⬆) **+ 4**“,

Hinweis:

- Wenn bei der Konfiguration der Benutzer-PIN ein „Sonderzeichen“ verwendet wurde, zum Beispiel „**B**“ oben, kann die cloudAshur nur entsperrt werden, wenn die PIN mit dem „Sonderzeichen“ in genau der konfigurierten Reihenfolge eingegeben wird, wie zum Beispiel „**B**“ oben – („2“, „4“, „**UMSCHALTTASTE** (⬆) **+ 7**“, „6“, „8“, „8“, „3“, „1“, „4“).
- Es kann mehr als ein „Sonderzeichen“ verwendet und in der 7- bis 15-stelligen PIN platziert werden.
- Benutzer können ihre PIN ändern, werden jedoch gegebenenfalls gezwungen, die festgelegte „Benutzer-PIN-Richtlinie“ (Beschränkungen) einzuhalten.
- Durch das Festlegen einer neuen Benutzer-PIN-Richtlinie wird eine vorhandene Benutzer-PIN automatisch gelöscht.
- Diese Richtlinie gilt nicht für die „Selbstzerstörungs-PIN“. Die Komplexität für die Selbstzerstörungs-PIN und Admin-PIN ist immer auf 7–15 Ziffern ohne erforderliches Sonderzeichen eingestellt.

Um eine **Benutzer-PIN-Richtlinie** festzulegen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 7** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie Ihre **3 Ziffern** ein. Die ersten zwei Ziffern geben die Mindest-PIN-Länge an, und die letzte Ziffer (0 oder 1) gibt an, ob ein Sonderzeichen verwendet wurde oder nicht.		Die GRÜNE und die BLAUE LED blinken weiter.
3. Drücken Sie einmal die **UMSCHALTTASTE** (⬆).		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Benutzer-PIN-Richtlinie erfolgreich festgelegt wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

9. So löschen Sie die Benutzer-PIN-Richtlinie

Um eine **Benutzer-PIN-Richtlinie** zu löschen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 7** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **070** ein und drücken Sie einmal die **UMSCHALTTASTE** (⬆).		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Benutzer-PIN-Richtlinie erfolgreich gelöscht wurde.

10. So prüfen Sie die Benutzer-PIN-Richtlinie

Der Administrator kann die Benutzer-PIN-Richtlinie überprüfen und dabei die Mindest-PIN-Länge ermitteln sowie feststellen, ob ein Sonderzeichen verwendet werden muss, indem er wie nachstehend beschrieben die LED-Sequenz notiert.

Um eine Benutzer-PIN-Richtlinie zu prüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALT-TASTE** (⬆) + **7** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie auf die **SCHLÜSSEL-Taste (🔑)** – es geschieht Folgendes: a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht. b. Das Blinken einer ROTEN LED entspricht zehn (10) Einheiten einer PIN. c. Das Blinken einer GRÜNEN LED entspricht einer (1) Einheit einer PIN d. Das Blinken einer BLAUEN LED zeigt an, dass ein „Sonderzeichen“ verwendet wurde. e. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht. f. Die LEDs leuchten wieder durchgehend BLAU.		

In der nachfolgenden Tabelle wird das LED-Verhalten beim Prüfen der Benutzer-PIN-Richtlinie beschrieben. Wenn Sie etwa eine 12-stellige Benutzer-PIN mit Sonderzeichen (**121**) eingestellt haben, blinkt die ROTE LED einmal (**1**) und die GRÜNE LED blinkt zweimal (**2**) gefolgt von einer einmal (**1**) blinkenden BLAUEN LED. Das bedeutet, dass ein **Sonderzeichen** verwendet werden muss.

PIN-Beschreibung	**3-Ziffern-Einstellung**	**ROT**	**GRÜN**	**BLAU**
12-stellige PIN mit Sonderzeichen	121	1x Blinken	2x Blinken	1x Blinken
12-stellige PIN OHNE Sonderzeichen	120	1x Blinken	2x Blinken	0
9-stellige PIN mit Sonderzeichen	091	0	9x Blinken	1x Blinken
9-stellige PIN OHNE Sonderzeichen	090	0	9x Blinken	0

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

11. Hinzufügen einer neuen Benutzer-PIN im Admin-Modus

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern aufweisen
- Darf nicht nur gleiche Ziffern enthalten, wie z. B. (3-3-3-3-3-3-3)
- Darf nicht nur sequenzielle Ziffern enthalten, wie z. B. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- Die **UMSCHALTTASTE** (⬆) kann für zusätzliche PIN-Kombinationen verwendet werden, wie z. B. **UMSCHALTTASTE** (⬆) **+ 1** ist ein anderer Wert als nur „1“. Siehe Abschnitt 8 „Einstellen einer Benutzer-PIN-Richtlinie“.

Um eine **neue Benutzer-PIN** hinzuzufügen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den **Admin-Modus**. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 3** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und dann zu einer durchgehend leuchtenden BLAUEN LED.
2. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer schnell blinkenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die neue Benutzer-PIN erfolgreich konfiguriert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

12. Ändern der Benutzer-PIN im Admin-Modus

Um eine vorhandene **Benutzer-PIN** zu ändern, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 3** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und dann zu einer durchgehend leuchtenden BLAUEN LED.
2. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer schnell blinkenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Benutzer-PIN erfolgreich geändert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

13. Löschen der Benutzer-PIN im Admin-Modus

Um eine bestehende **Benutzer-PIN** zu löschen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE** (⬆) **+ 3** gedrückt.	▲ ➳ ▲	Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden ROTEN LED.
2. Halten Sie wieder die Tasten **SCHLÜSSEL** (⬆) **+ 3** gedrückt.	▲ ➳ ▲	Die Anzeige wechselt von einer blinkenden ROTEN LED zu einer durchgehend leuchtenden ROTEN LED und dann zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Benutzer-PIN erfolgreich gelöscht wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

14. So entsperren Sie cloudAshur mit einer Benutzer-PIN

Um die cloudAshur mit der **Benutzer-PIN zu entsperren,** müssen Sie die cloudAshur zuerst in den Standby-Modus versetzen (ROTE LED leuchtet durchgehend), in dem Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt halten.

1. Halten Sie im Standby-Modus (ROTE LED leuchtet durchgehend) die Tasten **UMSCHALTTASTE** (⬆) + **SCHLÜSSEL (🔑)** gedrückt.	▲ ➳ ▲ ▼ ▲	Statt der ROTEN LED mit Dauerlicht blinken nun alle LEDs (ROT, GRÜN und BLAU).
2. Geben Sie die **Benutzer-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.	▲ ▼ ▲ ➳ ▼	Die Anzeige wechselt von einer blinkenden ROTEN, einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu abwechselnd blinkenden GRÜNEN und BLAUEN LEDs und schließlich zu einer durchgehend leuchtenden GRÜNEN LED. Das bedeutet, dass die cloudAshur im Benutzermodus erfolgreich entsperrt wurde.

15. Ändern der Benutzer-PIN im Benutzermodus

Um die **Benutzer-PIN** zu ändern, entsperren Sie zuerst wie vorstehend in Abschnitt 14 beschrieben die cloudAshur mit einer Benutzer-PIN. Sobald sich die cloudAshur im **Benutzermodus** befindet (GRÜNE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Benutzermodus die Tasten **SCHLÜSSEL (⚷) + 4 gedrückt.**		Die Anzeige wechselt von einer durchgehend leuchtenden GRÜNEN LED zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
2. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUE LED zu einer schnell blinkenden GRÜNEN LED und dann zu einer durchgehend leuchtenden GRÜNEN LED. Das bedeutet, dass die Benutzer-PIN erfolgreich geändert wurde.

Wichtig: Die Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ geändert werden, wenn eine wie in Abschnitt 8 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie schreibt eine Mindest-PIN-Länge vor und ob ein „Sonderzeichen“ verwendet wurde. Der Administrator kann Abschnitt 10 heranziehen, um die Benutzer-PIN-Beschränkungen zu prüfen.

16. Konfigurieren einer einmaligen Benutzerwiederherstellungs-PIN

Die einmalige Wiederherstellungs-PIN ist sehr nützlich in Situationen, in denen ein Benutzer seine PIN vergessen hat, um die cloudAshur zu entsperren. Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zunächst die richtige einmalige Wiederherstellungs-PIN eingeben, wenn eine konfiguriert wurde. Der Wiederherstellungsprozess für die Benutzer-PIN wirkt sich nicht auf den Verschlüsselungsschlüssel und die Admin-PIN aus. Der Benutzer wird jedoch gezwungen, eine neue 7- bis 15-stellige Benutzer-PIN zu konfigurieren.

Um eine 7- bis 15-stellige einmalige Benutzerwiederherstellungs-PIN zu konfigurieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (⚷) + 4** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und dann zu einer durchgehend leuchtenden BLAUEN LED.
2. Geben Sie **eine einmalige Wiederherstellungs-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie **die einmalige Wiederherstellungs-PIN** erneut ein und drücken Sie wieder auf die **SCHLÜSSEL-Taste (⚷)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED zu einer schnell blinkenden GRÜNEN LED und schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die einmalige Wiederherstellungs-PIN erfolgreich konfiguriert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

17. Löschen der einmaligen Benutzerwiederherstellungs-PIN

Um die einmalige Benutzerwiederherstellungs-PIN zu löschen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE** (⬆) **+ 4** gedrückt.	▲ ➳ ▲	Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden ROTEN LED.
2. Halten Sie wieder die Tasten **UMSCHALTTASTE** (⬆) **+ 4** gedrückt.	▲ ➳ ▲	Die Anzeige wechselt von einer blinkenden ROTEN LED zu einer durchgehend leuchtenden ROTEN LED und danach zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die einmalige Benutzerwiederherstellungs-PIN erfolgreich gelöscht wurde.

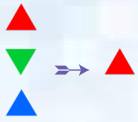
Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

18. Aktivieren des Wiederherstellungsmodus und Konfigurieren einer neuen Benutzer-PIN

Die einmalige Wiederherstellungs-PIN ist sehr nützlich in Situationen, in denen ein Benutzer seine PIN vergessen hat, um die cloudAshur zu entsperren. Um den Wiederherstellungsmodus zu aktivieren, muss der Benutzer zunächst die richtige einmalige Wiederherstellungs-PIN eingeben, wenn eine konfiguriert wurde. Der Wiederherstellungsprozess für die Benutzer-PIN wirkt sich nicht auf den Verschlüsselungsschlüssel und die Admin-PIN aus. Der Benutzer wird jedoch gezwungen, eine neue 7- bis 15-stellige Benutzer-PIN zu konfigurieren.

Zum Aktivieren des Wiederherstellungsprozesses und zum Konfigurieren einer neuen Benutzer-PIN führen Sie die folgenden Schritte durch:

1. Wenn sich die cloudAshur im **Leerlauf** befindet, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt.		Die ROTE, die GRÜNE und die BLAUE LED blinken nacheinander jeweils einmal. Danach blinkt die GRÜNE LED zweimal und schließlich zeigt die ROTE LED Dauerlicht. Das bedeutet, dass sich die cloudAshur im Standby-Modus befindet.
2. Halten Sie im **Standby-Modus** die Tasten **SCHLÜSSEL (⚷)** + **4** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden ROTEN LED zu einer blinkenden ROTEN und einer blinkenden GRÜNEN LED.
3. Geben Sie die einmalige **Wiederherstellungs-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**.		Zuerst schalten sich eine GRÜNE und eine BLAUE LED abwechselnd ein und aus. Dann wechselt die Anzeige zu einer durchgehend leuchtenden GRÜNEN LED sowie schließlich zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
4. Geben Sie die **neue Benutzer-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED zu einer einzelnen blinkenden GRÜNEN LED. Dann wechselt die Anzeige wieder zurück zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
5. Geben Sie die **neue Benutzer-PIN** erneut ein und drücken Sie wieder auf die **SCHLÜSSEL-Taste (⚷)**.		Die GRÜNE LED blinkt schnell und leuchtet danach durchgehend GRÜN. Das bedeutet, dass der Wiederherstellungsprozess erfolgreich durchgeführt und eine neue Benutzer-PIN konfiguriert wurde.

Wichtig: Eine neue Benutzer-PIN muss unter Einhaltung der „Benutzer-PIN-Richtlinie“ erstellt werden, wenn eine wie in Abschnitt 8 beschrieben konfiguriert wurde. Die Benutzer-PIN-Richtlinie schreibt eine Mindest-PIN-Länge vor und ob ein Sonderzeichen verwendet wurde. Siehe Abschnitt 10 für die Überprüfung der Benutzer-PIN-Beschränkungen.

19. So konfigurieren Sie Ihre cloudAshur zur Aktivierung der KeyWriter-Klonfunktion

Hinweis: Die KeyWriter-Klonfunktion ist für die cloudAshur standardmäßig aktiviert.

Die cloudAshur kann zusammen mit dem iStorage KeyWriter verwendet werden, um das Klonen von bis zu 9 Geräten gleichzeitig zu ermöglichen. Damit die cloudAshur vom KeyWriter geklont werden kann, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (⚷) + 8** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **11** ein und drücken Sie einmal die **UMSCHALTTASTE** (⬆).		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und dann zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die KeyWriter-Klonfunktion für die cloudAshur aktiviert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

20. So deaktivieren Sie die KeyWriter-Klonfunktion

Um die KeyWriter-Klonfunktion zu deaktivieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 8** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **44** ein und drücken Sie einmal die **UMSCHALTTASTE** (⬆).		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN und dann zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die KeyWriter-Klonfunktion deaktiviert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

21. So überprüfen Sie die Konfiguration der KeyWriter-Klonfunktion

Um zu überprüfen, ob die KeyWriter-Klonfunktion für cloudAshur aktiviert oder deaktiviert ist, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE** (⬆) + **8** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie auf die **SCHLÜSSEL-Taste (🔑)** und Folgendes geschieht:

- **Wenn für Ihre cloudAshur die KeyWriter-Klonfunktion aktiviert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
d. Die LEDs leuchten wieder durchgehend BLAU.

- **Wenn die KeyWriter-Klonfunktion deaktiviert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Alle LEDs sind aus
c. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
d. Die LEDs leuchten wieder durchgehend BLAU.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

22. So deaktivieren Sie die Registrierung der cloudAshur-Clientanwendung

Die cloudAshur ist so konfiguriert, dass sie im Auslieferungs- oder vollständig zurückgesetzten Zustand nicht über die Clientanwendung registriert werden kann. Die Clientanwendungsfunktion wird automatisch aktiviert, wenn die ursprüngliche Admin-PIN geändert oder eine Benutzer-PIN konfiguriert bzw. geändert wird.

Um die Registrierung der Clientanwendung zu deaktivieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **3 + 7** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie einmal auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und dann zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Registrierung der Clientanwendung deaktiviert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

23. So überprüfen Sie, ob die Registrierung der cloudAshur-Clientanwendung aktiviert ist

Um zu überprüfen, ob die Registrierung der cloudAshur-Clientanwendung aktiviert ist, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **2 + 7** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie auf die **SCHLÜSSEL-Taste (🔑)** und Folgendes geschieht:

- **Wenn die Registrierung der cloudAshur-Clientanwendung aktiviert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
d. Die LEDs leuchten wieder durchgehend BLAU.

- **Wenn die Registrierung der cloudAshur-Clientanwendung deaktiviert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Alle LEDs sind aus
c. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
d. Die LEDs leuchten wieder durchgehend BLAU.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

24. So konfigurieren Sie den cloudAshur-Verschlüsselungsmodus

WARNUNG: Wenn die Einstellung des Verschlüsselungsmodus von „AES-XTS“ (Standardeinstellung) in „AES-ECB“ oder umgekehrt geändert wird, wird der Verschlüsselungsschlüssel gelöscht und die cloudAshur zurückgesetzt. Alle Daten, die von der cloudAshur verschlüsselt wurden, sind dann nicht mehr zugänglich und für immer verloren! Führen Sie diesen Vorgang nur unter den folgende Umständen aus: Sie haben noch keine Daten in die Cloud hochgeladen oder in lokalen Ordnern gespeichert, Sie haben mindestens ein weiteres cloudAshur-Hardwaresicherheitsmodul mit dem gleichen Verschlüsselungsschlüssel, von dem Sie die Daten kopieren können, oder Ihnen steht eine vollständige und nicht verschlüsselte Sicherheitskopie Ihrer Daten zur Verfügung.

Führen Sie die folgenden Schritte durch, um für den cloudAshur-Verschlüsselungsmodus die Einstellung **AES-ECB** (angegeben durch die Nummer **„01“**) oder **AES-XTS** (angegeben durch die Nummer **„02“**) zu konfigurieren. Die Standardeinstellung dieser Funktion ist „AES-XTS“ (02). Wenn ein bestimmter Verschlüsselungsmodus konfiguriert ist, werden die Daten von der cloudAshur unter Verwendung des entsprechenden Algorithmus verschlüsselt.

Um den cloudAshur-Verschlüsselungsmodus zu konfigurieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „Admin-Modus“. Sobald sich die cloudAshur im Admin-Modus befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 1** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **01** für die Einstellung **AES-ECB** ein. Geben Sie **02** für die Einstellung **AES-XTS (Standardeinstellung) ein.**		Die GRÜNE und die BLAUE LED blinken weiter.
3. Drücken Sie einmal die **UMSCHALTTASTE** (⬆).		Die Anzeige wechselt von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED und dann zu einer durchgehend leuchtenden ROTEN LED (**Reset-Zustand**). Das bedeutet, dass die Änderung des cloudAshur-Verschlüsselungsmodus erfolgreich durchgeführt wurde.

Wichtig: Nach der Konfiguration des cloudAshur-Verschlüsselungsmodus wird die cloudAshur vollständig zurückgesetzt, und es muss eine neue Admin-PIN konfiguriert werden. Siehe hierzu Abschnitt 29 „So konfigurieren Sie eine Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung“ auf Seite 71.

25. So überprüfen Sie den Verschlüsselungsmodus

Um den cloudAshur-Verschlüsselungsmodus zu überprüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE** (⬆) + **1** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie auf die **SCHLÜSSEL-Taste (🔑)** und Folgendes geschieht:

- **Wenn „AES-ECB“ für den Verschlüsselungsmodus konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Die GRÜNE LED blinkt einmal.
c. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
d. Die LEDs leuchten wieder durchgehend BLAU.

- **Wenn „AES-XTS“ für den Verschlüsselungsmodus konfiguriert wurde, geschieht Folgendes:**

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Alle LEDs sind aus
c. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
d. Die LEDs leuchten wieder durchgehend BLAU.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

26. So konfigurieren Sie eine Selbstzerstörungs-PIN

Sie können eine Selbstzerstörungs-PIN konfigurieren, die bei ihrer Eingabe alle konfigurierten PINs löscht und ein Crypto-Erase auf der cloudAshur ausführt (der Verschlüsselungsschlüssel wird gelöscht). Wenn diese Funktion ausgeführt wird, wird die Selbstzerstörungs-PIN zur neuen Benutzer-PIN.
Um die Selbstzerstörungs-PIN festzulegen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**". Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 6** gedrückt.		Die Anzeige wechselt von der durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED.
2. Konfigurieren Sie eine 7- bis 15-stellige **Selbstzerstörungs-PIN** und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie die **Selbstzerstörungs-PIN** erneut ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die GRÜNE LED blinkt einige Sekunden lang schnell, dann wechselt die Anzeige zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Selbstzerstörungs-PIN erfolgreich konfiguriert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

27. So löschen Sie die Selbstzerstörungs-PIN

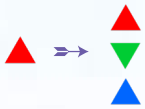
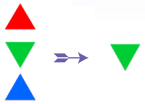
Um die Selbstzerstörungs-PIN zu löschen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**". Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE** (⬆) **+ 6** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden ROTEN LED.
2. Halten Sie wieder die Tasten **UMSCHALTTASTE** (⬆) **+ 6** gedrückt.		Die Anzeige wechselt von einer blinkenden ROTEN LED zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Selbstzerstörungs-PIN erfolgreich gelöscht wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

28. So entsperren Sie mit der Selbstzerstörungs-PIN

Die Selbstzerstörungs-PIN **löscht den Verschlüsselungsschlüssel sowie die Admin-/Benutzer-PINs** und entsperrt dann die cloudAshur. Bei Aktivierung dieser Funktion wird die **Selbstzerstörungs-PIN zur neuen Benutzer-PIN.**
Um den Selbstzerstörungsmechanismus zu aktivieren, muss sich die cloudAshur im Standby-Modus befinden (ROTE LED leuchtet durchgehend). Führen Sie anschließen die folgenden Schritte durch.

1. Halten Sie im Standby-Modus (ROTE LED leuchtet durchgehend), die Tasten **UMSCHALTTASTE** (⬆) + **SCHLÜSSEL (🔑)** gedrückt.		Statt der ROTEN LED mit Dauerlicht blinken nun alle LEDs (ROT, GRÜN und BLAU).
2. Geben Sie die **Selbstzerstörungs-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden ROTEN, GRÜNEN und BLAUEN LED zu einer GRÜNEN und einer BLAUEN LED, die sich einige Sekunden lang abwechselnd ein- und ausschalten. Schließlich wird eine durchgehend leuchtende GRÜNE LED angezeigt. Das bedeutet, dass die Selbstzerstörung der cloudAshur erfolgreich durchgeführt wurde.

WARNUNG: Wenn der Selbstzerstörungsmechanismus aktiviert ist, werden der Verschlüsselungsschlüssel und die Admin-/Benutzer-PINs gelöscht. **Die Selbstzerstörungs-PIN wird zur Benutzer-PIN.** Nach der Aktivierung des Selbstzerstörungsmechanismus ist keine Admin-PIN vorhanden. Die **cloudAshur muss zuerst zurückgesetzt werden** (siehe „So führen Sie eine komplette Rücksetzung durch“ in Abschnitt 36 auf Seite 77), damit eine Admin-PIN mit vollen Admin-Privilegien, einschließlich der Konfiguration einer Benutzer-PIN, erstellt werden kann.

29. So konfigurieren Sie eine Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung

Nach einem Brute Force-Angriff oder einer Rücksetzung der cloudAshur muss eine Admin-PIN konfiguriert werden, bevor die cloudAshur verwendet werden kann.

PIN-Anforderungen:

- Muss zwischen 7 und 15 Ziffern aufweisen
- Darf nicht nur gleiche Ziffern enthalten, wie z. B. (3-3-3-3-3-3-3)
- Darf nicht nur sequenzielle Ziffern enthalten, wie z. B. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Nach einem Brute Force-Angriff oder einer Rücksetzung befindet sich die cloudAshur im Standby-Modus (ROTE LED leuchtet durchgehend). Um eine Admin-PIN zu konfigurieren, führen Sie die folgenden Schritte durch.

1. Halten Sie im Standby-Modus (ROTE LED leuchtet durchgehend), die Tasten **UMSCHALTTASTE** (⬆) **+1** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden ROTEN LED zu einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED.
2. Geben Sie die **neue Admin-PIN** ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer einzigen blinkenden GRÜNEN LED und danach wieder zu einer blinkenden GRÜNEN und einer durchgehend leuchtenden BLAUEN LED.
3. Geben Sie die **neue Admin-PIN** erneut ein und drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**.		Die Anzeige wechselt von einer blinkenden GRÜNEN LED und einer durchgehend leuchtenden BLAUEN LED zu einer BLAUEN LED, die einige Sekunden lang schnell blinkt. Schließlich wird eine durchgehend leuchtende BLAUE LED angezeigt. Das bedeutet, dass die Admin-PIN erfolgreich konfiguriert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

30. Einstellen der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“

Um die cloudAshur vor unbefugtem Zugriff zu schützen, wenn sie entsperrt und unbeaufsichtigt ist, kann festgelegt werden, dass die cloudAshur automatisch nach einem vorab ausgewählten Zeitraum gesperrt wird. In Standardzustand ist die Zeitüberschreitungsfunktion „Automatische Sperre, wenn unbeaufsichtigt“ der cloudAshur deaktiviert. Die Funktion „Automatische Sperre, wenn unbeaufsichtigt“ kann auf einen Zeitraum von 5 bis 99 Minuten eingestellt werden.
Um die Funktion „Automatische Sperre, wenn unbeaufsichtigt“ einzustellen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (🔑) + 5** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie für die Funktion „Automatische Sperre, wenn unbeaufsichtigt“ den gewünschten Zeitraum ein. Der Mindestwert beträgt 5 Minuten und der Höchstwert 99 Minuten (5 bis 99 Minuten). Geben Sie beispielsweise Folgendes ein: **05 für 5 Minuten** **20 für 20 Minuten** **99 für 99 Minuten**		
3. Drücken Sie die **UMSCHALTTASTE** (⬆).		Die Anzeige wechselt für eine Sekunde von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED. Danach wechselt die Anzeige schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass der Zeitüberschreitungswert für die automatische Sperre erfolgreich konfiguriert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

31. Deaktivieren der Uhr für „Automatische Sperre, wenn unbeaufsichtigt“

Um die Funktion „Automatische Sperre, wenn unbeaufsichtigt“ zu deaktivieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **SCHLÜSSEL (⚷) + 5** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie **00** ein und drücken Sie die **UMSCHALT-TASTE** (⬆).		Die Anzeige wechselt für eine Sekunde von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED. Danach wechselt die Anzeige schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass der Zeitüberschreitungswert für die automatische Sperre erfolgreich deakiviert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

32. So überprüfen Sie die Uhr für „Automatische Sperre, wenn unbeaufsichtigt“

Der Administrator kann den Zeitraum für die Uhr der Funktion „Automatische Sperre, wenn unbeaufsichtigt“ überprüfen und bestimmen, indem er einfach die LED-Sequenz wie in der Tabelle unten auf dieser Seite beschrieben notiert.

Um die Funktion „Automatische Sperre, wenn unbeaufsichtigt“ zu überprüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **UMSCHALTTASTE** (⬆) **+ 5 gedrückt.**		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie auf die **SCHLÜSSEL-Taste (⚷)**. Es geschieht Folgendes:

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Das Blinken einer ROTEN LED entspricht zehn (10) Minuten.
c. Das Blinken einer GRÜNEN LED entspricht einer (1) Minute.
d. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
e. Die LEDs leuchten wieder durchgehend BLAU.

In der nachstehenden Tabelle wird das LED-Verhalten bei der Überprüfung der Funktion „Automatische Sperre, wenn unbeaufsichtigt“ beschrieben. Wenn Sie die cloudAshur beispielsweise für eine automatische Sperrung nach **25** Minuten konfiguriert haben, blinkt die ROTE LED zweimal (**2**) und die GRÜNE LED fünfmal (**5**).

Automatische Sperre in Minuten	ROT	GRÜN
5 Minuten	0	5 Blinken
15 Minuten	1 Blinken	5 Blinken
25 Minuten	2 Blinken	5 Blinken
40 Minuten	4 Blinken	0

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

33. Abwehrmechanismus gegen Brute-Force-Hacker-Angriffe

Die cloudAshur verfügt über einen Abwehrmechanismus, um sich vor Brute-Force-Angriffen zu schützen. Im Auslieferungszustand lautet der Standardwert der Brute-Force-Beschränkung (aufeinanderfolgende falsche PIN-Eingaben) für die Admin- und Benutzer-PIN **10** bzw. **5** für die Wiederherstellungs-PIN. Es werden drei voneinander unabhängige Brute-Force-Zähler verwendet, um fehlerhafte Versuche für jede PIN-Autorisierung (Admin, Benutzer und Wiederherstellung) wie nachfolgend dargelegt aufzuzeichnen.

- Wenn ein Benutzer zehnmal hintereinander eine **falsche Benutzer-PIN** eingibt, wird die Benutzer-PIN gelöscht. Die Daten sowie die Admin-PIN und die Wiederherstellungs-PIN bleiben jedoch intakt und zugänglich.
- Wenn fünfmal hintereinander eine **falsche Wiederherstellungs-PIN** eingegeben wird, wird die Wiederherstellungs-PIN gelöscht. Die Daten und die Admin-PIN bleiben jedoch intakt und zugänglich.
- Wenn zehnmal hintereinander eine **falsche Admin-PIN** eingegeben wird, wird die cloudAshur zurückgesetzt. Alle PINs und Daten werden gelöscht und sind für immer verloren.

In der nachfolgenden Tabelle wird davon ausgegangen, dass alle drei PINs eingerichtet wurden. Es werden die Auswirkungen eines ausgelösten Brute-Force-Abwehrmechanismus für jede einzelne PIN hervorgehoben.

PIN zum Entsperren der cloudAshur	Aufeinanderfolgende falsche PIN-Eingaben	Beschreibung der Auswirkungen
Benutzer-PIN	10	• Die Benutzer-PIN wird gelöscht. • Die Wiederherstellungs-PIN, die Admin-PIN und alle Daten bleiben intakt und zugänglich.
Wiederherstellungs-PIN	5	• Die Wiederherstellungs-PIN wird gelöscht. • Die Admin-PIN und alle Daten bleiben intakt und zugänglich.
Admin-PIN	10	• Die cloudAshur wird zurückgesetzt. Alle PINs und Daten werden gelöscht und sind für immer verloren.

Hinweis: Die Brute-Force-Beschränkung wird standardmäßig wieder auf die Auslieferungszustandswerte eingestellt, wenn die cloudAshur vollständig zurückgesetzt oder die Selbstzerstörungsfunktion aktiviert wird bzw. wenn ein Brute-Force-Angriff erfolgt. Wenn der Administrator die Benutzer-PIN ändert oder wenn bei Aktivierung der Wiederherstellungsfunktion eine neue Benutzer-PIN eingestellt wird, wird der Brute-Force-Zähler der Benutzer-PIN auf null (0) gestellt. Das hat jedoch keine Auswirkung auf die Brute-Force-Beschränkung. Wenn der Administrator die Wiederherstellungs-PIN ändert, wird der Brute-Force-Zähler der Wiederherstellungs-PIN auf null gestellt.
Durch die erfolgreiche Autorisierung einer bestimmten PIN wird der Brute-Force-Zähler für die betreffende PIN auf null gestellt. Das hat jedoch keine Auswirkung auf den Brute-Force-Zähler der anderen PINs. Durch die fehlgeschlagene Autorisierung einer bestimmten PIN zählt der Brute-Force-Zähler für die betreffende PIN hoch, was sich jedoch nicht auf den Brute-Force-Zähler der anderen PINs auswirkt.

34. So stellen Sie die Brute-Force-Beschränkung für die Benutzer-PIN ein

Hinweis: Die Standardeinstellung der Brute-Force-Beschränkung für die Benutzer-PIN erlaubt 10 aufeinanderfolgende falsche PIN-Eingaben, wenn die cloudAshur vollständig zurückgesetzt wird, ein Brute-Force-Angriff erfolgt oder die Selbstzerstörungs-PIN aktiviert wird.

Die Brute-Force-Beschränkung für die Benutzer-PIN der cloudAshur kann vom Administrator neu programmiert und eingestellt werden. Diese Funktion kann so eingestellt werden, dass 1 bis 10 Versuche für die Eingabe einer falschen PIN zulässig sind.
Um eine Brute-Force-Beschränkung für die Benutzer-PIN zu konfigurieren, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**“. Wenn sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **7 + 0** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Geben Sie die Anzahl der Versuche für die Brute-Force-Beschränkung ein (zwischen 01 und 10). Beispiel: • **01** für 1 Versuch • **10** für 10 Versuche		
3. Drücken Sie einmal die **UMSCHALTTASTE** (⬆).		Die Anzeige wechselt für eine Sekunde von einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden GRÜNEN LED. Danach wechselt die Anzeige schließlich zu einer durchgehend leuchtenden BLAUEN LED. Das bedeutet, dass die Brute-Force-Beschränkung erfolgreich konfiguriert wurde.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).
Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

35. So prüfen Sie die Brute-Force-Beschränkung für die Benutzer-PIN

Der Administrator kann die Anzahl der zulässigen aufeinanderfolgenden Eingabe einer falschen Benutzer-PIN vor dem Auslösen des Brute-Force-Abwehrmechanismus beobachten und bestimmen, indem er die LED-Sequenz einfach wie nachfolgend beschrieben notiert.

Um die Einstellung der Brute-Force-Beschränkung zu prüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den „**Admin-Modus**". Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **2** + **0** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.
2. Drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**. Es geschieht Folgendes: a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht. b. Das Blinken einer ROTEN LED entspricht zehn (10) Einheiten einer Brute-Force-Beschränkungsanzahl. c. Das Blinken einer GRÜNEN LED entspricht einer (1) einzelnen Einheit einer Brute-Force-Beschränkungsanzahl. d. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht. e. Die LEDs leuchten wieder durchgehend BLAU.		

In der nachstehenden Tabelle wird das LED-Verhalten bei der Prüfung der Brute-Force-Beschränkungseinstellung beschrieben. Wenn Sie die cloudAshur beispielsweise so eingestellt haben, dass sie **5** aufeinanderfolgende falsche PIN-Eingaben als Brute-Force-Angriff wertet, blinkt die GRÜNE LED fünfmal (**5**).

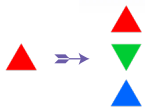
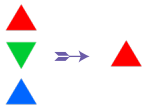
Brute-Force-Beschränkungseinstellung	**ROT**	**GRÜN**
2 Versuche	0	2x Blinken
5 Versuche	0	5x Blinken
10 Versuche	1x Blinken	0

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

36. So führen Sie eine komplette Rücksetzung durch

Für eine komplette Rücksetzung muss sich die cloudAshur im Standby-Modus befinden (ROTE LED leuchtet durchgehend). Nach der cloudAshur-Rücksetzung werden alle Admin-/Benutzer-PINs und der Verschlüsselungscode gelöscht. Alle entsprechenden Daten bleiben verschlüsselt und sind somit nicht mehr zugänglich.
Um die cloudAshur zurückzusetzen, führen Sie die folgenden Schritte durch.

1. Halten Sie im Standby-Modus (ROTE LED leuchtet durchgehend) die Taste **0** gedrückt.		Statt einer durchgehend leuchtenden ROTEN LED blinken alle LEDs – ROT, GRÜN und BLAU – abwechselnd.
2. Halten Sie die Tasten **2 + 7** gedrückt.		Die ROTE, die GRÜNE und die BLAUE LED blinken und zeigen dann für eine Sekunde Dauerlicht. Die Anzeige wechselt schließlich zu einer durchgehend leuchtenden ROTEN LED. Das bedeutet, dass die cloudAshur zurückgesetzt wurde.

Wichtig: Nach einer kompletten Rücksetzung muss eine neue Admin-PIN konfiguriert werden. Siehe hierfür Abschnitt 29 „So konfigurieren Sie eine Admin-PIN nach einem Brute-Force-Angriff oder einer Rücksetzung“ auf Seite 71.

37. So prüfen Sie Firmware im Admin-Modus

Um die Firmware-Revisionsnummer zu prüfen, wechseln Sie zuerst wie in Abschnitt 5 beschrieben in den den „**Admin-Modus**“. Sobald sich die cloudAshur im **Admin-Modus** befindet (BLAUE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Admin-Modus die Tasten **3** + **8** gedrückt.		Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie einmal auf die **SCHLÜSSEL-Taste (🔑)**. Es geschieht Folgendes:

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Die ROTE LED blinkt und gibt so den ganzzahligen Teil der Firmware-Versionsnummer an.
c. Die GRÜNE LED blinkt und gibt so den Nachkommateil der Firmware-Versionsnummer an.
d. Die BLAUE LED blinkt und gibt so die letzte Ziffer der Firmware-Versionsnummer an.
e. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
f. Die Anzeige wechselt von einer blinkenden ROTEN, einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden BLAUEN LED.

Wenn die Firmware-Versionsnummer beispielsweise „**4.2**“ ist, blinkt die ROTE LED viermal (**4**) und die GRÜNE LED zweimal (**2**). Nach dem Ende der Sequenz blinken die ROTE, die GRÜNE und die BLAUE LED gemeinsam einmal, und danach wechselt die Anzeige in den Admin-Modus zurück, d. h. zu einer durchgehend leuchtenden BLAUEN LED.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

38. So prüfen Sie Firmware im Benutzermodus

Um die Firmware-Versionsnummer zu prüfen, wechseln Sie zuerst wie in Abschnitt 14 beschrieben in den „**Benutzermodus**“. Sobald sich die cloudAshur im **Benutzermodus** befindet (GRÜNE LED leuchtet durchgehend), führen Sie die folgenden Schritte durch.

1. Halten Sie im Benutzermodus die Tasten **3** + **8** gedrückt, bis die GRÜNE und die BLAUE LED gemeinsam blinken.		Die Anzeige wechselt von einer durchgehend leuchtenden GRÜNEN LED zu einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED.

2. Drücken Sie auf die **SCHLÜSSEL-Taste (🔑)**. Es geschieht Folgendes:

a. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
b. Die ROTE LED blinkt und gibt so den ganzzahligen Teil der Firmware-Versionsnummer an.
c. Die GRÜNE LED blinkt und gibt so den Nachkommateil der Firmware-Versionsnummer an.
d. Die BLAUE LED blinkt und gibt so die letzte Ziffer der Firmware-Versionsnummer an.
e. Alle LEDs (ROT, GRÜN und BLAU) zeigen 1 Sekunde lang Dauerlicht.
f. Die Anzeige wechselt von einer blinkenden ROTEN, einer blinkenden GRÜNEN und einer blinkenden BLAUEN LED zu einer durchgehend leuchtenden BLAUEN LED.

Wenn die Firmware-Versionsnummer beispielsweise „**4.2**“ ist, blinkt die ROTE LED viermal (**4**) und die GRÜNE LED zweimal (**2**). Nach dem Ende der Sequenz blinken die ROTE, die GRÜNE und die BLAUE LED gemeinsam einmal, und danach wechselt die Anzeige in den Benutzermodus zurück, d. h. zu einer durchgehend leuchtenden GRÜNEN LED.

Hinweis: Wenn sich die cloudAshur im Admin-Modus befindet, zeigt die BLAUE LED nur noch 30 Sekunden lang Dauerlicht. In dieser Zeit kann die cloudAshur Anweisungen über die Tastatur annehmen und so mit einer Vielzahl von Sicherheitsfunktionen konfiguriert werden. Wenn innerhalb von 30 Sekunden kein Schlüsselereignis eintritt, verlässt die cloudAshur den Admin-Modus automatisch. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt (alle LEDs sind aus).

Um den Admin-Modus (BLAUE LED leuchtet durchgehend) sofort zu verlassen, halten Sie die **UMSCHALTTASTE** (⬆) eine Sekunde lang gedrückt. Die Anzeige wechselt von einer durchgehend leuchtenden BLAUEN LED zu einer durchgehend leuchtenden ROTEN LED, die danach beim Übergang in den Leerlauf langsam erlischt. Damit Sie die cloudAshur entsperren und auf Ihre Daten zugreifen können, muss sich die cloudAshur zunächst im Leerlauf befinden (alle LEDs sind aus), bevor eine Admin-/Benutzer-PIN eingegeben werden kann.

39. Technischer Support

iStorage stellt Ihnen die folgenden nützlichen Ressourcen bereit:

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

E-Mail-Support:
support@istorage-uk.com

Telefonsupport:
+44 (0) 20 8991-6260.

Die Spezialisten des technischen Supports von iStorage sind Montag bis Freitag von 9:00 bis 17:30 Uhr GMT erreichbar.

40. Garantie- und RMA-Informationen

PRODUKT-HAFTUNGSAUSSCHLUSS UND -GEWÄHRLEISTUNG VON ISTORAGE

iStorage garantiert, dass seine Produkte bei Lieferung und für einen Zeitraum von 36 Monaten frei von Materialfehlern sind. Diese Garantie gilt jedoch nicht unter den nachfolgend beschriebenen Bedingungen. iStorage garantiert, dass die Produkte zum Zeitpunkt Ihrer Bestellung den Standards entsprechen, die im zugehörigen Datenblatt auf unserer Website aufgeführt sind.

Diese Garantien gelten nicht für Mängel an Produkten, die zurückzuführen sind auf:
- normale Abnutzung und Verschleiß
- vorsätzliche Beschädigung, unsachgemäße Lager- oder Einsatzsbedingungen, Unfall, Fahrlässigkeit durch Sie oder Dritte
- unsachgemäße Bedienung oder Nutzung der Produkte durch Sie oder Dritte entgegen der Benutzerhinweise
- jegliche Änderung oder Reparatur durch Sie oder Dritte, die nicht zu unseren autorisierten Reparaturbetrieben gehören
- jegliche von Ihnen bereitgestellten Spezifikationen

Im Rahmen dieser Garantien reparieren, ersetzen oder erstatten wir nach eigenem Ermessen jedes Produkt, bei dem Materialfehler festgestellt wurden, sofern Sie bei Lieferung:
- die Produkte geprüft haben, um festzustellen, ob sie Materialfehler aufweisen, und
- den Verschlüsselungsmechanismus der Produkte getestet haben

Wir haften nur für Materialfehler oder Mängel am Verschlüsselungsmechanismus der Produkte, die durch Prüfung bei Lieferung festgestellt und uns innerhalb von 30 Tagen nach Lieferung mitgeteilt werden. Sofern Materialfehler oder Mängel am Verschlüsselungsmechanismus nicht durch Prüfung der Produkte bei Lieferung festgestellt wurden, haften wir nur für Mängel, die Sie uns innerhalb von 7 Tagen mitteilen, nachdem Sie sie entdeckt haben oder hätten erkennen müssen. Wir haften im Rahmen dieser Garantien nicht, wenn Sie oder andere Personen die Produkte nach der Feststellung eines Mangels weiter verwenden. Wenn Sie einen Mangel feststellen, senden Sie das defekte Produkt bitte an uns zurück. Wenn Sie ein Unternehmen sind, tragen Sie die Transportkosten für die Rücksendung von Produkten oder Produktteilen an uns im Rahmen der Garantie. Wir tragen alle Transportkosten für das Versenden von reparierten oder ersetzten Produkten an Sie. Wenn Sie privater Verbraucher sind, lesen Sie bitte unsere Allgemeinen Geschäftsbedingungen.

Zurückgesandte Produkte müssen sich in der Originalverpackung und in einem sauberen Zustand befinden. Anderenfalls werden zurückgesandte Produkte nach dem Ermessen des Unternehmens entweder abgelehnt oder es werden für entstehende Kosten zusätzliche Gebühren berechnet. Wenn Produkte im Rahmen der Garantie zur Reparatur eingeschickt werden, muss eine Kopie der Originalrechnung beigelegt oder die Originalrechnungsnummer mit Kaufdatum angegeben werden.

Wenn Sie privater Verbraucher sind, gilt diese Garantie zusätzlich zu Ihren gesetzlichen Rechten für Produkte, die fehlerhaft oder nicht wie beschrieben sind. Informationen zu diesen Rechten erhalten Sie von Ihrer örtlichen Beratungsstelle für Privatverbraucher.

Die in dieser Klausel aufgeführten Garantien gelten nur für Erstkäufer, für von iStorage autorisierte Wiederverkäufer oder für Händler von iStorage-Produkten. Diese Garantien sind nicht übertragbar.

MIT AUSNAHME DER HIER GEWÄHRTEN BESCHRÄNKTEN GARANTIE UND IM GESETZLICH ZULÄSSIGEN UMFANG LEHNT ISTORAGE ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GARANTIEN AB, EINSCHLIESSLICH IN BEZUG AUF MARKTGÄNGIGKEIT, EIGNUNG FÜR BESTIMMTE ZWECKE UND NICHTVERLETZUNG DER RECHTE DRITTER. ISTORAGE GARANTIERT NICHT, DASS DAS PRODUKT FEHLERFREI FUNKTIONIERT. SOWEIT IMPLIZITE GARANTIEN GESETZLICH ZULÄSSIG SIND, SIND DIESE AUF DIE GÜLTIGKEITSDAUER DIESER GARANTIE BESCHRÄNKT. IHR ANSPRUCH UMFASST AUSSCHLIESSLICH EINE REPARATUR ODER EINEN ERSATZ DES PRODUKTS WIE HIER ANGEGEBEN.

IN KEINEM FALL HAFTET ISTORAGE FÜR VERLUSTE, ERWARTETE GEWINNE ODER ZUFÄLLIGE, STRAFRECHTLICHE, BEISPIELHAFTE, SPEZIELLE, VERTRAUENS- ODER FOLGESCHÄDEN, EINSCHLIESSLICH ABER NICHT BESCHRÄNKT AUF ENTGANGENE UMSÄTZE, GEWINNE, NUTZUNGSVERLUSTE FÜR SOFTWARE, DATENVERLUSTE, SONSTIGE VERLUSTE ODER WIEDERHERSTELLUNG VON DATEN, SACHSCHÄDEN UND ANSPRÜCHE DRITTER, DIE SICH THEORETISCH AUS EINER WIEDERHERSTELLUNG ERGEBEN, EINSCHLIESSLICH GARANTIEN, VERTRÄGEN, UNGESETZLICHEN ODER UNERLAUBTEN HANDLUNGEN, UNABHÄNGIG DAVON, OB AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE. UNGEACHTET DER LAUFZEIT EINER BESCHRÄNKTEN GARANTIE ODER EINER GESETZLICH FESTGELEGTEN GARANTIE ODER WENN EINE BESCHRÄNKTE GARANTIE IHREN WESENTLICHEN ZWECK VERFEHLT, ÜBERSTEIGT DIE GESAMTE HAFTUNG VON ISTORAGE IN KEINEM FALL DEN KAUFPREIS DES PRODUKTS. | 4823-2548-5683.3

TEIL B

41. Registrieren und Installieren der cloudAshur-Client-App für Windows

cloudAshur-Registrierung

Laden Sie die cloudAshur-Client-App für Windows unter dem folgenden Link herunter:
https://istorage-uk.com/software-and-updates/

Wichtig – bitte lesen: Wählen Sie für die Registrierung Ihres cloudAshur-Hardwaresicherheitsmoduls eine für Sie passende Registrierungsmethode aus:

- **Personal** – cloudAshur **darf NICHT** zusammen mit **Remote Management** (zentrale Managementsoftware) verwendet werden.
- **Enterprise** – cloudAshur wird zusammen mit **Remote Management** (zentrale Managementsoftware) verwendet.

Personal-Registrierung

Da Ihr cloudAshur-Hardwaresicherheitsmodul nicht zusammen mit „Remote Management" verwendet wird, brauchen Sie zur Registrierung **KEINE** „PIN-Nummer" und auch keinen „Lizenzschlüssel". Füllen Sie einfach die Felder 1–6 aus (**3. Schritt**), vergewissern Sie sich, dass das Kontrollkästchen in Feld Nr. 7 nicht markiert ist, überspringen Sie die Felder 8 und 9 und klicken Sie auf „Registrieren". Dann können Sie mit der Verwendung Ihrer cloudAshur beginnen.

Enterprise-Registrierung

Das cloudAshur-Hardwaresicherheitsmodul wird von Unternehmen eingesetzt, die jeden ihrer Mitarbeiter, der die vom Unternehmen bereitgestellten cloudAshur-Module verwendet, über die cloudAshur **Remote Management Console** (zentrale Managementsoftware) zentral verwalten und überwachen.

Wenn Sie ein Mitarbeiter sind und vom Administrator Ihres Unternehmens ein cloudAshur-Modul erhalten haben, sendet Ihnen der Administrator eine E-Mail „**Sie wurden eingeladen**" mit den folgenden wichtigen Registrierungsinformationen:

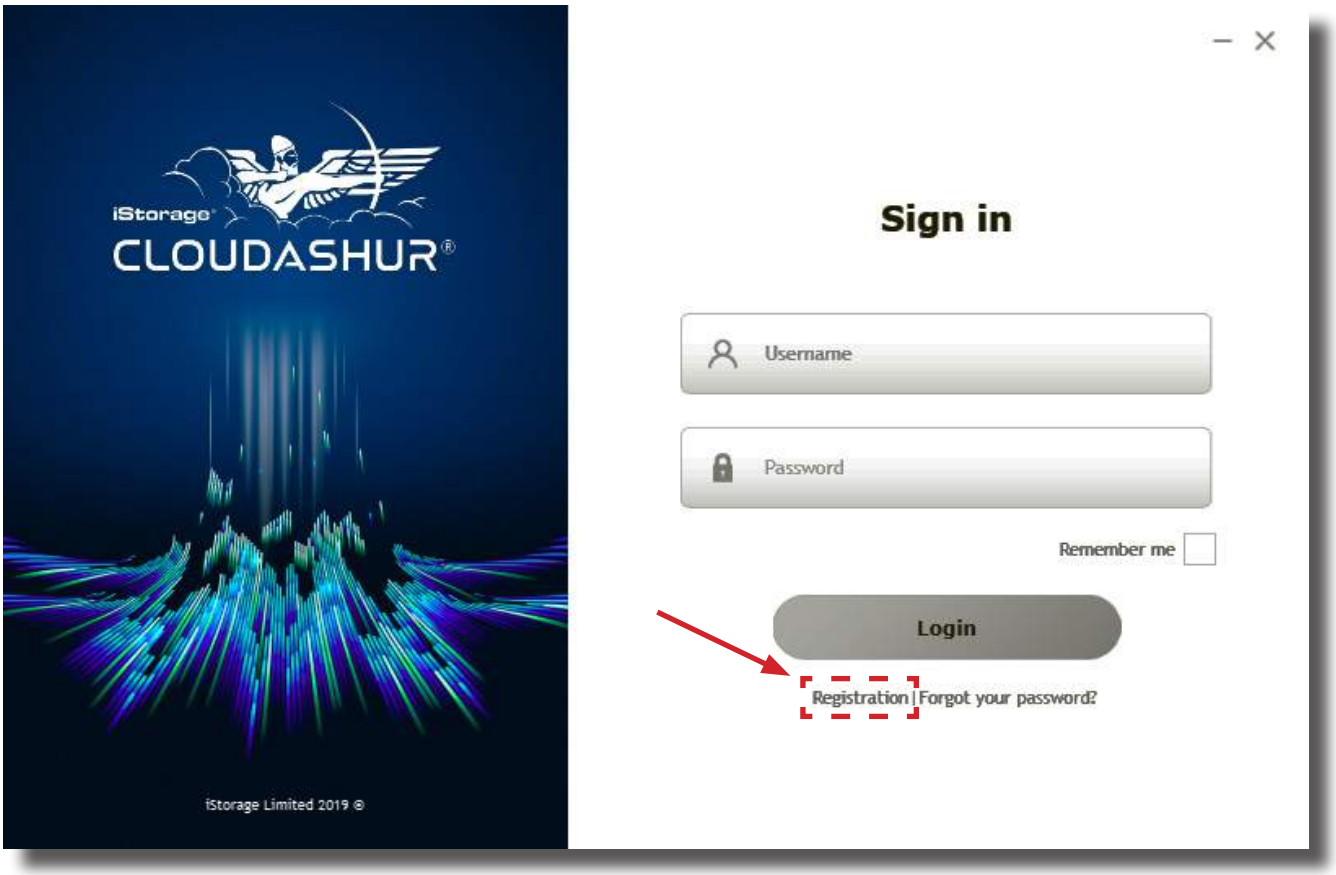
1. Einen Link zum Herunterladen der cloudAshur-Client-App für Windows.
2. Eine **PIN-Nummer** – diese Nummer muss im Registrierungsverfahren im Feld Nr. 8 eingegeben werden (**3. Schritt**).
3. Ein **Lizenzschlüssel** – dieser Schlüssel muss im Registrierungsverfahren im Feld Nr. 9 eingegeben werden (**3. Schritt**).

1. Schritt

Nach der Installation der Windows-Client-App entsperren Sie Ihr cloudAshur-Hardwaresicherheitsmodul mit der Admin- bzw. der Benutzer-PIN wie in **Teil A** in diesem Handbuch beschrieben. Schließen Sie das entsperrte cloudAshur-Hardwaresicherheitsmodul (GRÜNE LED) an einem USB-Anschluss Ihres Computers an.

2. Schritt

Öffnen Sie die Windows-Client-App (Abbildung 1) und klicken Sie auf „**Registrierung**“, um das cloudAshur-Hardwaresicherheitsmodul zu registrieren.



(Abbildung 1)

03. Schritt

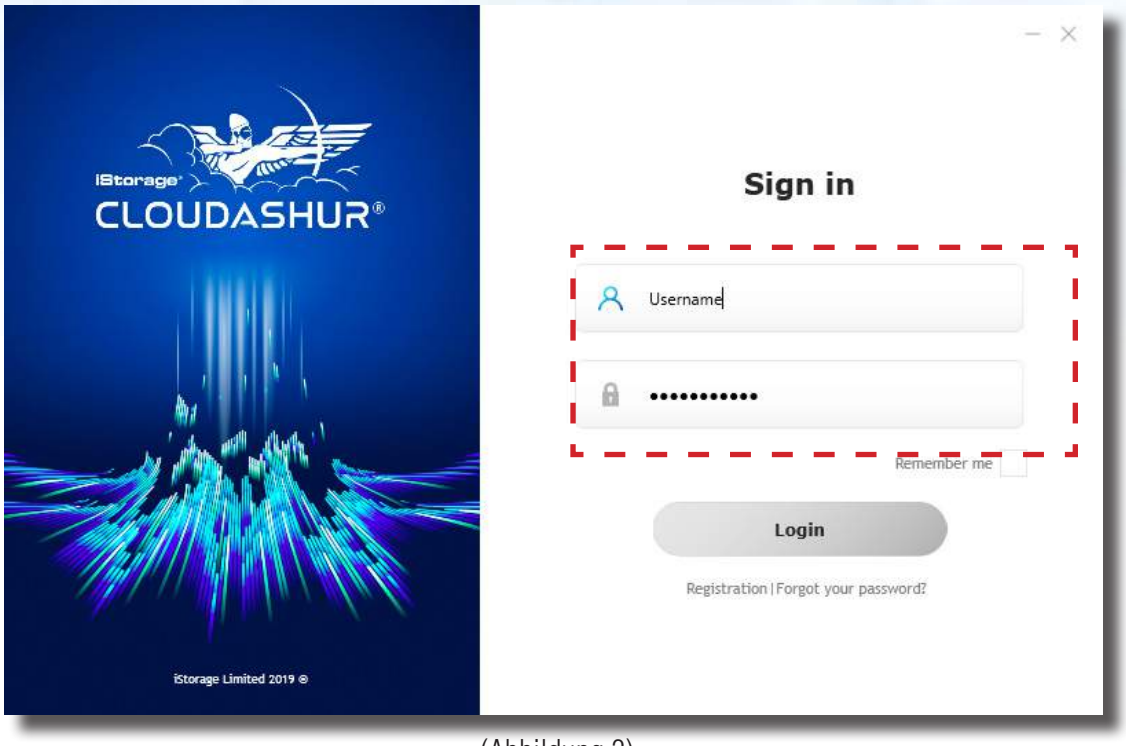
Füllen Sie für die „Registrierung Ihrer cloudAshur“ (Abbildung 2) alle Felder unter „**Neuer Benutzer**“ aus.

(Abbildung 2)

1. Geben Sie einen „**Benutzernamen**“ ein.
2. Geben Sie Ihren „**Vornamen**“ und Ihren „**Nachnamen**“ ein.
3. Geben Sie Ihre „**E-Mail-Adresse**“ ein und bestätigen Sie sie.
4. Geben Sie Ihr „**Passwort**“ ein und bestätigen Sie es. Ihr Passwort muss mindestens 8 Zeichen lang sein und 3 der folgenden 4 Optionen enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen.
5. Geben Sie Ihre „**Telefonnummer**“ ein.
6. Die „**Gerätenummer**“ wird automatisch erfasst, wenn das cloudAshur-Modul entsperrt und an Ihrem Computer angeschlossen wird (GRÜNE LED). Wenn die Gerätenummer nicht erfasst wird, klicken Sie zur Erfassung auf die Schaltfläche „Aktualisieren“.
7. Wenn für das cloudAshur-Modul, das Sie vom Administrator Ihres Unternehmens erhalten haben, eine **Enterprise-Registrierung** erfolgen soll, stellen Sie sicher, dass Sie das Kontrollkästchen wie in der vorstehenden Abbildung 2 gezeigt markieren. Wenn Sie für die cloudAshur eine **Personal-Registrierung** vornehmen wollen, dann markieren Sie das Kontrollkästchen nicht, überspringen Sie die Schritte 8 und 9 und fahren Sie mit Schritt 10 fort.
8. Geben Sie die „**PIN**“ ein, die Sie von Ihrem Administrator per E-Mail erhalten haben (**nur Enterprise-Registrierung**).
9. Geben Sie den „**Lizenzschlüssel**“ ein, den Sie von Ihrem Administrator per E-Mail erhalten haben (**nur Enterprise-Registrierung**).
10. Klicken Sie auf die Schaltfläche „**Registrieren**“ , um die Registrierung abzuschließen.
11. Klicken Sie auf die Schaltfläche „Vorwärts“, um sich anzumelden (**4. Schritt**).

04. Schritt

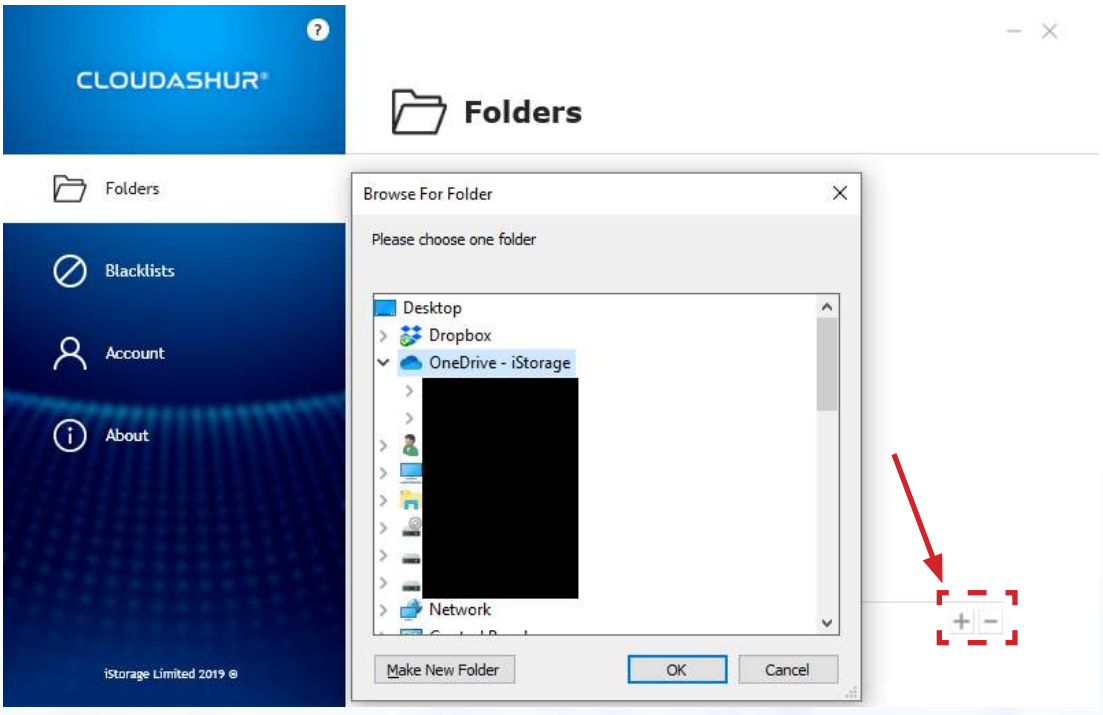
Geben Sie Ihren „**Benutzernamen**“ und Ihr „**Passwort**“ ein, den bzw. das Sie im 3. Schritt erstellt haben. Klicken Sie anschließend wie in der nachstehenden Abbildung 3 gezeigt auf die Schaltfläche „**Anmelden**“.



(Abbildung 3)

05. Schritt

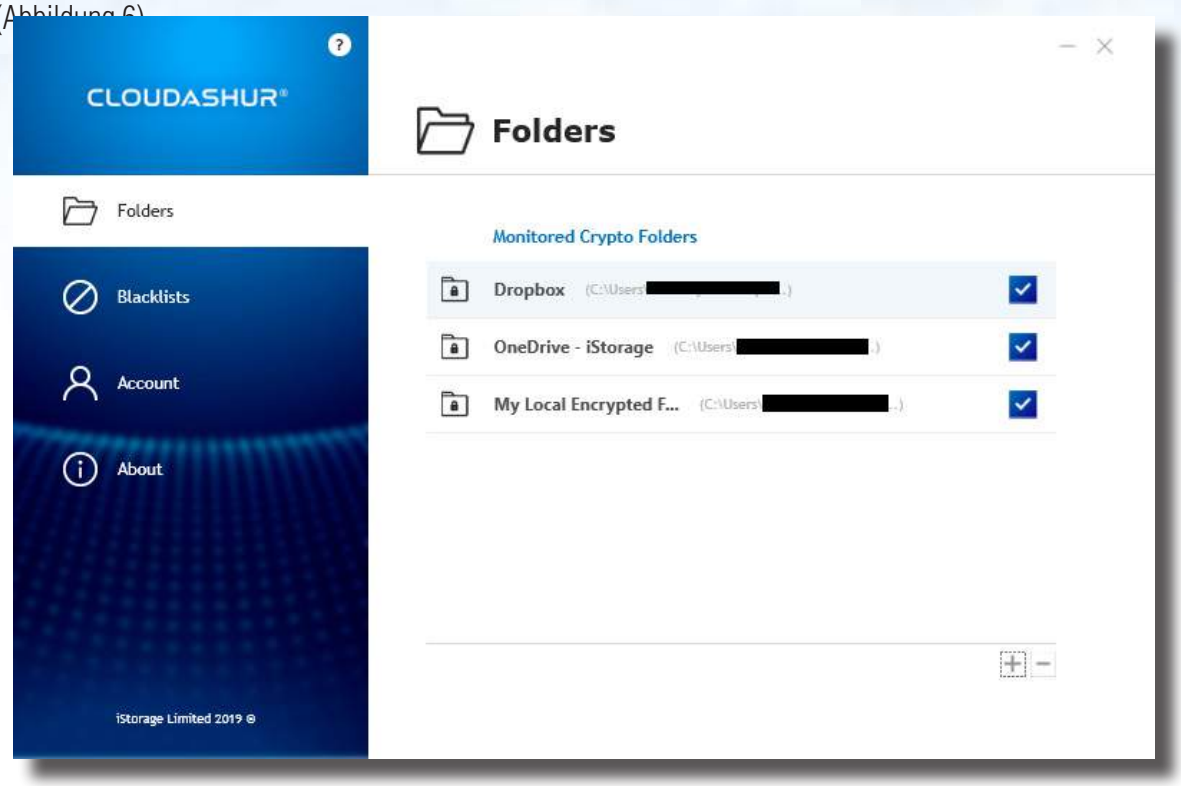
Nach der „Anmeldung“ öffnet sich das virtuelle Laufwerk der cloudAshur. Damit Sie Ihre Cloud- und lokalen Ordner zu Ihrem virtuellen cloudAshur-Laufwerk hinzuzufügen können, klicken Sie in der Taskleiste einmal auf das cloudAshur-Symbol (rechts unten auf Ihrem Bildschirm), um das Menü „Einstellungen“ zu öffnen. Klicken Sie anschließend auf das Symbol „**+**“, um Ihre Cloud- und lokalen Ordern wie in der nachstehenden Abbildung 4 gezeigt auszuwählen.



(Abbildung 4)

06. Schritt

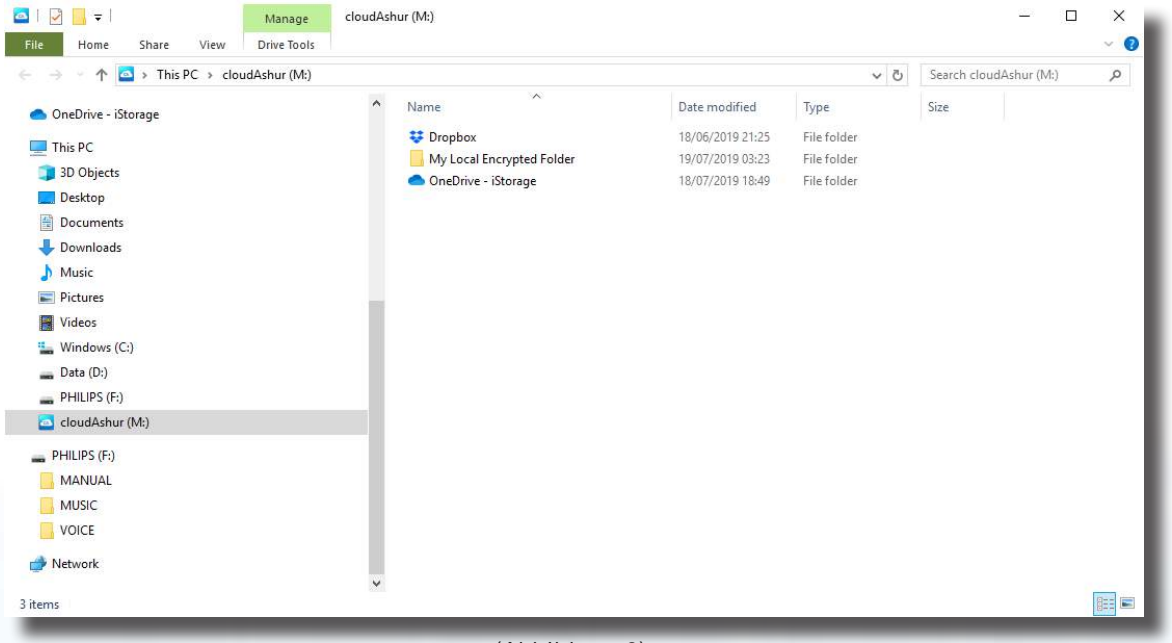
Nachdem Sie Ihre Cloudkonten und lokalen Ordner hinzugefügt haben (wie in Abbildung 5 dargestellt), doppelklicken Sie in der Taskleiste auf das cloudAshur-Symbol (rechts unten auf Ihrem Bildschirm), um das virtuelle cloudAshur-Laufwerk zu öffnen (Abbildung 6).



(Abbildung 5)

07. Schritt

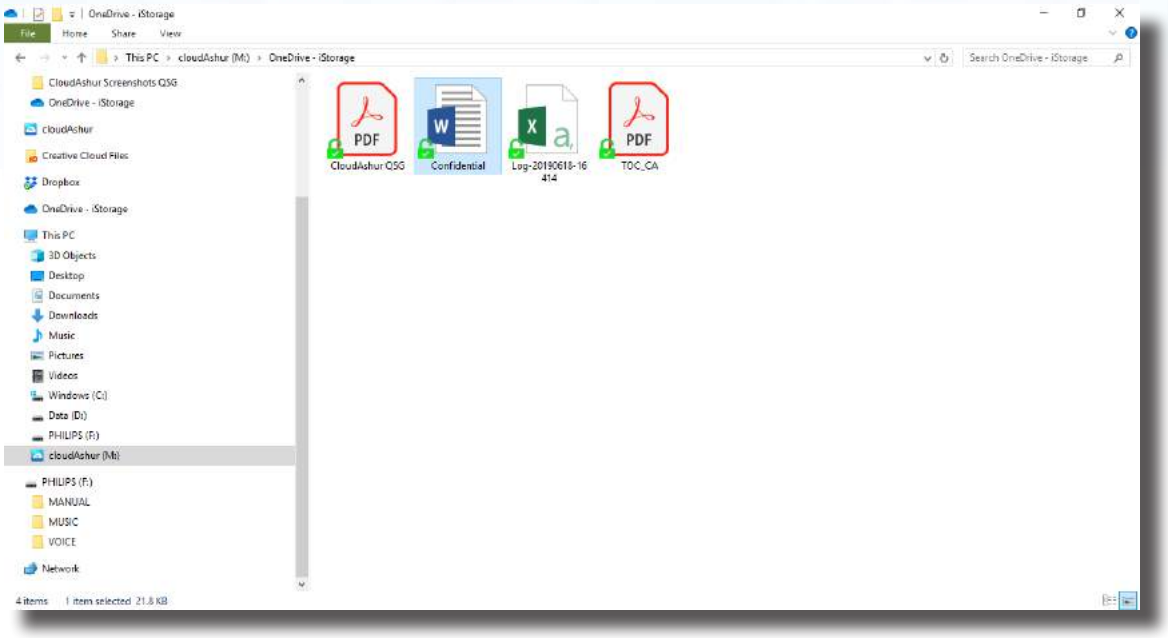
Klicken Sie im virtuellen cloudAshur-Laufwerk auf Ihren Cloud- bzw. lokalen Ordner, um diesen zu öffnen – in diesem Fall auf „**OneDrive – iStorage**“ (wie in Abbildung 6 dargestellt).



(Abbildung 6)

08. Schritt

Verschieben Sie Ihre Dateien per Drag & Drop oder per Kopieren und Einfügen zu Ihrem virtuellen cloudAshur-Laufwerk. Wie in Abbildung 7 gezeigt erscheint ein grünes geöffnetes Vorhängeschloss-Symbol links unten an jeder Datei. Das bedeutet, dass die Dateien verschlüsselt wurden, aber trotzdem über das virtuelle Laufwerk zugänglich sind. Werden dieselben Dateien direkt über Ihr Cloudkonto abgerufen, werden sie verschlüsselt angezeigt.



(Abbildung 7)

42. Registrieren und Installieren der cloudAshur-Client-App für macOS

cloudAshur-Registrierung

Laden Sie die cloudAshur-Client-App für macOS unter dem folgenden Link herunter:
https://istorage-uk.com/software-and-updates/

Wichtig – bitte lesen: Wählen Sie für die Registrierung Ihres cloudAshur-Hardwaresicherheitsmoduls eine für Sie passende Registrierungsmethode aus:

- **Personal** – cloudAshur **darf NICHT** zusammen mit **Remote Management** (zentrale Managementsoftware) verwendet werden.
- **Enterprise** – cloudAshur wird zusammen mit **Remote Management** (zentrale Managementsoftware) verwendet.

Personal-Registrierung

Da Ihr cloudAshur-Hardwaresicherheitsmodul nicht zusammen mit „Remote Management" verwendet wird, brauchen Sie zur Registrierung **KEINE** „PIN-Nummer" und auch keinen „Lizenzschlüssel". Füllen Sie einfach die Felder 1–6 aus (**3. Schritt**), vergewissern Sie sich, dass das Kontrollkästchen in Feld Nr. 7 nicht markiert ist, überspringen Sie die Felder 8 und 9 und klicken Sie auf „Registrieren". Dann können Sie mit der Verwendung Ihrer cloudAshur beginnen.

Enterprise-Registrierung

Das cloudAshur-Hardwaresicherheitsmodul wird von Unternehmen eingesetzt, die jeden ihrer Mitarbeiter, der die vom Unternehmen bereitgestellten cloudAshur-Module verwendet, über die cloudAshur **Remote Management Console** (zentrale Managementsoftware) zentral verwalten und überwachen.

Wenn Sie ein Mitarbeiter sind und vom Administrator Ihres Unternehmens ein cloudAshur-Modul erhalten haben, sendet Ihnen der Administrator eine E-Mail „**Sie wurden eingeladen**" mit den folgenden wichtigen Registrierungsinformationen:

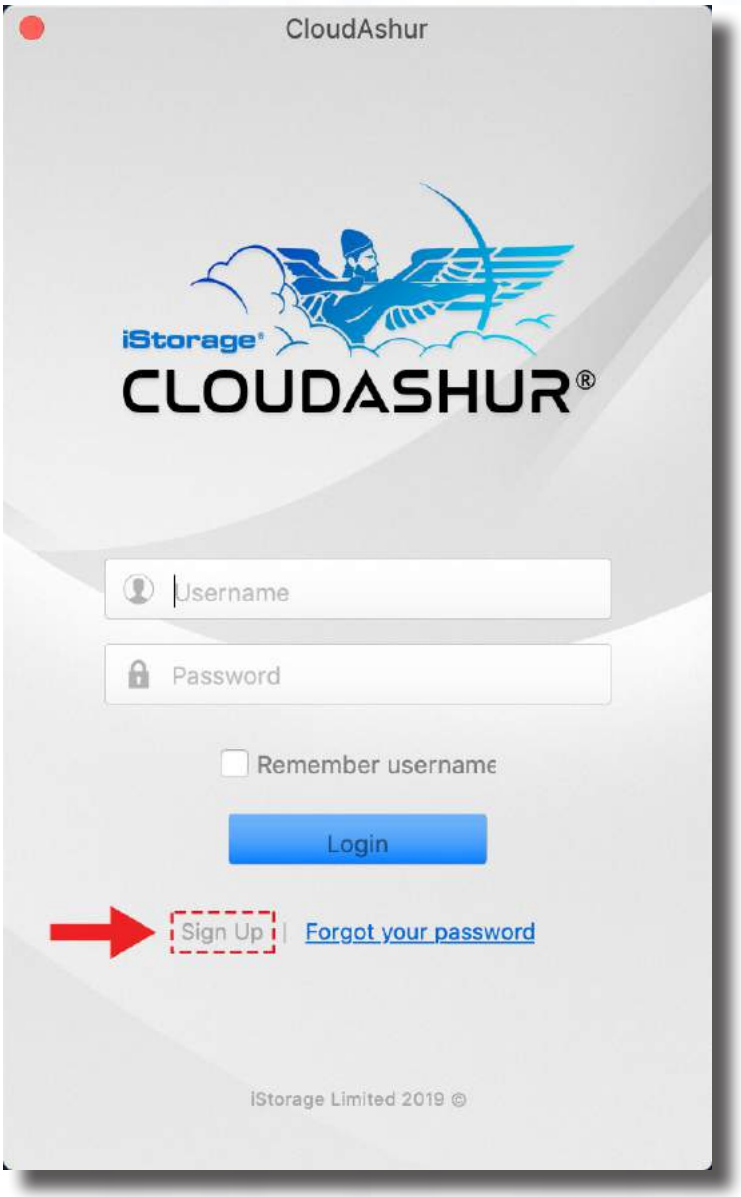
1. Einen Link zum Herunterladen der cloudAshur-Client-App für macOS.
2. Eine **PIN-Nummer** – diese Nummer muss im Registrierungsverfahren im Feld Nr. 8 eingegeben werden (**3. Schritt**).
3. Ein **Lizenzschlüssel** – dieser Schlüssel muss im Registrierungsverfahren im Feld Nr. 9 eingegeben werden (**3. Schritt**).

01. Schritt

Nach der Installation der macOS-Client-App, entsperren Sie Ihr cloudAshur-Hardwaresicherheitsmodul mit der Admin- bzw. der Benutzer-PIN wie in **Teil A** in diesem Handbuch beschrieben. Schließen Sie das entsperrte cloudAshur-Hardwaresicherheitsmodul (GRÜNE LED) an einem USB-Anschluss Ihres Computers an.

02. Schritt

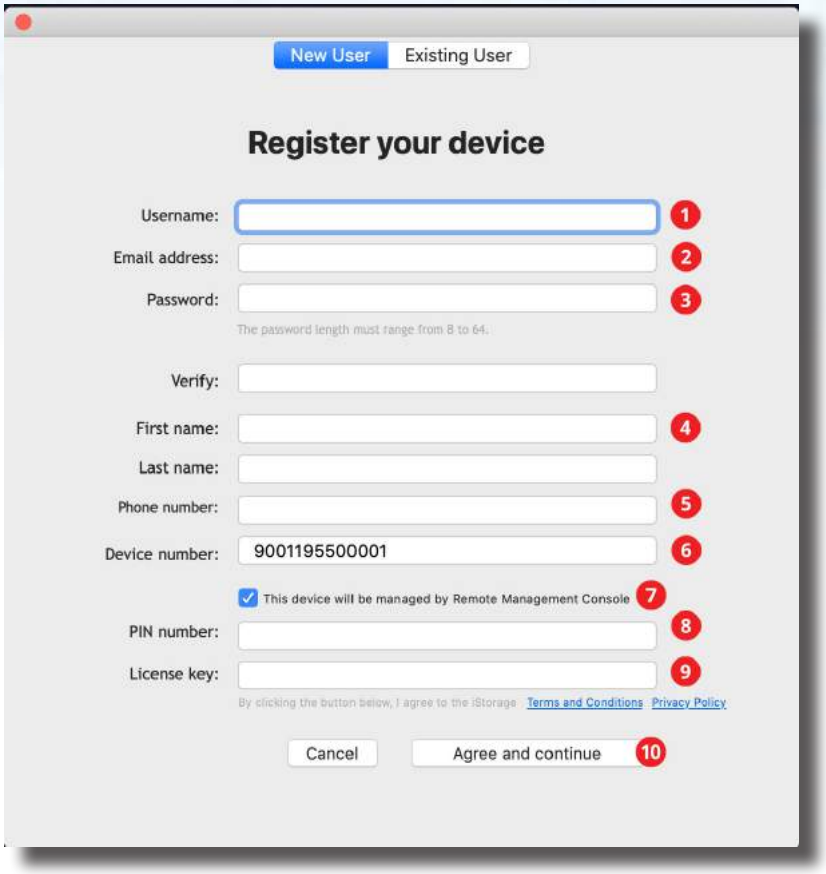
Öffnen Sie die macOS-Client-App (Abbildung 1) und klicken Sie auf „**Registrieren**“, um das cloudAshur-Hardwaresicherheitsmodul zu registrieren.



(Abbildung 1)

03. Schritt

Füllen Sie für die „Registrierung Ihrer cloudAshur“ (Abbildung 2) alle Felder unter „**Neuer Benutzer**“ aus.



(Abbildung 2)

1. Geben Sie einen „**Benutzernamen**“ ein.
2. Geben Sie Ihre „**E-Mail-Adresse**“ ein.
3. Geben Sie Ihr „**Passwort**“ ein und bestätigen Sie es. Ihr Passwort muss mindestens 8 Zeichen lang sein und 3 der folgenden 4 Optionen enthalten: Großbuchstaben, Kleinbuchstaben, Zahlen und Sonderzeichen.
4. Geben Sie Ihren „**Vornamen**“ und Ihren „**Nachnamen**“ ein.
5. Geben Sie Ihre „**Telefonnummer**“ ein.
6. Die „**Gerätenummer**“ wird automatisch erfasst, wenn das cloudAshur-Modul entsperrt und an Ihrem Computer angeschlossen wird (GRÜNE LED).
7. Wenn für das cloudAshur-Modul, das Sie vom Administrator Ihres Unternehmens erhalten haben, eine **Enterprise-Registrierung** erfolgen soll, stellen Sie sicher, dass Sie das Kontrollkästchen wie in der vorstehenden Abbildung 2 gezeigt markieren. Wenn Sie für die cloudAshur eine **Personal-Registrierung** vornehmen wollen, dann markieren Sie das Kontrollkästchen nicht, überspringen Sie die Schritte 8 und 9 und fahren Sie mit Schritt 10 fort.
8. Geben Sie die „**PIN**“ ein, die Sie von Ihrem Administrator per E-Mail erhalten haben (**nur Enterprise-Registrierung**).
9. Geben Sie den „**Lizenzschlüssel**“ ein, den Sie von Ihrem Administrator per E-Mail erhalten haben (**nur Enterprise-Registrierung**).
10. Klicken Sie auf die Schaltfläche „**Registrieren**“, um die Registrierung abzuschließen.

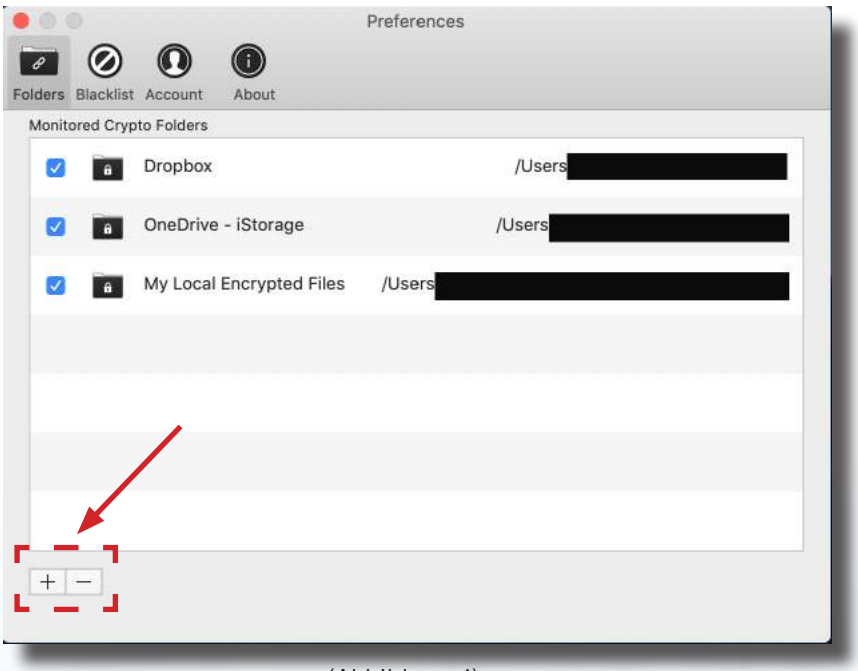
04. Schritt

Geben Sie Ihren „**Benutzernamen**“ und Ihr „**Passwort**“ ein, den bzw. das Sie im 3. Schritt erstellt haben. Klicken Sie anschließend wie in der nachstehenden Abbildung 3 gezeigt auf die Schaltfläche „**Anmelden**“.

(Abbildung 3)

05. Schritt

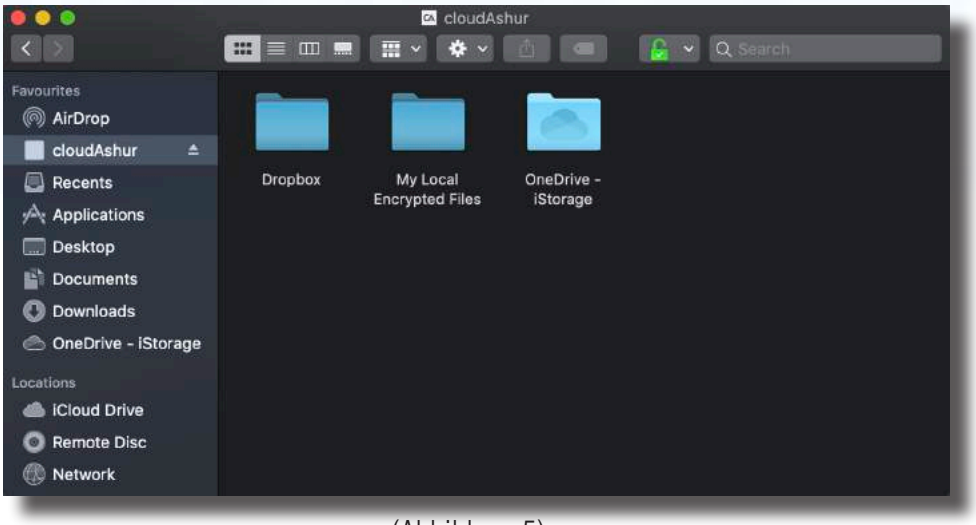
Nach der „Anmeldung“ öffnet sich das virtuelle Laufwerk der cloudAshur. Damit Sie Ihre Cloud- und lokalen Ordner zu Ihrem virtuellen cloudAshur-Laufwerk hinzuzufügen können, klicken Sie in der **Menüleiste** auf das cloudAshur-Symbol (oben auf Ihrem Bildschirm). Klicken Sie anschließend auf „Einstellungen“ und dann auf das Symbol „**+**“, um Ihre Cloud- und lokalen Ordern wie in der nachstehenden Abbildung 4 gezeigt auszuwählen.



(Abbildung 4)

06. Schritt

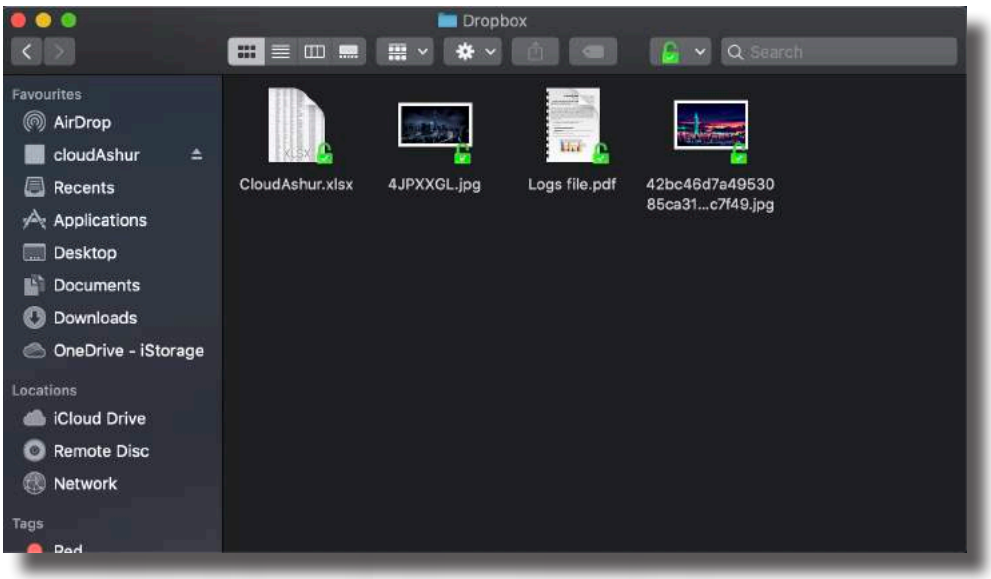
Nachdem Sie Ihre Cloudkonten und lokalen Ordner hinzugefügt haben, klicken Sie in der **Menüleiste** auf das cloudAshur-Symbol (oben auf Ihrem Bildschirm), um das virtuelle cloudAshur-Laufwerk zu öffnen (Abbildung 5). Klicken Sie wie nachstehend gezeigt auf Ihren Cloud- bzw. lokalen Ordner, um diesen zu öffnen – in diesem Fall auf „**Dropbox**“.



(Abbildung 5)

07. Schritt

Verschieben Sie Ihre Dateien per Drag & Drop oder per Kopieren und Einfügen zu Ihrem virtuellen cloudAshur-Laufwerk. Wie in Abbildung 6 gezeigt erscheint ein grünes geöffnetes Vorhängeschloss-Symbol links unten an jeder Datei. Das bedeutet, dass die Dateien verschlüsselt wurden, aber trotzdem über das virtuelle Laufwerk zugänglich sind. Werden dieselben Dateien direkt über Ihr Cloudkonto abgerufen, werden sie verschlüsselt angezeigt.



(Abbildung 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

Manuel

Attention ne pas oublier votre code PIN (mot de passe) car sans lui, vous ne disposez d'aucun moyen pour accéder à vos données cryptées.

Si vous rencontrez des difficultés à utiliser votre cloudAshur, merci de contacter notre service technique par courriel à l'adresse support@istorage-uk.com ou par téléphone au +44 (0) 20 8991 6260.

RoHS Compliant

REACH COMPLIANCE

Conforme au Trade Agreements Act (TAA)

CITRIX® vmware®

Table des matières

Introduction

Remarque : La batterie rechargeable du cloudAshur ne sera pas entièrement chargée. Nous recommandons de charger la batterie avant la première utilisation. Veuillez brancher le cloudAshur à un port USB alimenté pendant 20-30 minutes pour charger totalement la batterie.

Merci d'avoir acheté le module de sécurité informatique iStorage cloudAshur, la clé physique unique pour accéder à vos données, faisant d'elle la solution parfaite pour quiconque souhaitant stocker, partager (y compris des services d'email ou de transfert de fichiers), et gérer des données dans le cloud de la manière la plus sûre que vous pouvez imaginer, en éliminant les failles de sécurité existant chez les plateformes du cloud, comme le manque de contrôle, la propriété, la confidentialité et l'interdiction d'accès.

Le module de sécurité informatique cloudAshur offre cinq facteurs d'authentification :

- **Une chose que vous possédez** :

1. Votre module de sécurité informatique cloudAshur, votre clé physique pour accéder à vos données.

- **Une chose que vous savez** :

2. Votre code PIN de 7 à 15 chiffres associé au module de sécurité informatique cloudAshur.
3. Votre identifiant et votre mot de passe pour l'appli client cloudAshur.
4. L'endroit où vos données sont stockées (stockage sur le cloud).
5. L'identifiant et le mot de passe associés à votre compte cloud.

De plus, vos modules de sécurité informatique cloudAshur peuvent également être gérés et surveillés à l'aide de la Console de gestion à distance iStorage cloudAshur, vous offrant ainsi un contrôle total de tous les modules de sécurité informatique cloudAshur déployés au sein de votre organisme, et offrant ainsi à l'administrateur une vaste gamme de fonctionnalités comme la clôture géographique en temps réel, la clôture de temps, les identifiants de l'utilisateur, la désactivation à distance, l'arrêt à distance et bien plus encore pour gérer et surveiller tous les utilisateurs avec un maximum de simplicité.

Contenu de la boîte

- Le module de sécurité informatique iStorage cloudAshur
- Chemise en aluminium extrudé
- GDR - Guide de démarrage rapide

Enregistrer et installer votre appli client cloudAshur

Le présent manuel est divisé en deux parties, **Partie A** (sections 1-40) et **Partie B** (sections 41 et 42).

Vous devrez d'abord configurer vote module de sécurité informatique cloudAshur avec les configurations pertinentes décrites en **Partie A** de ce manuel, comme changer le code PIN administrateur, configurer un code PIN utilisateur, un code PIN d'autodestruction, etc.

Une fois votre module de sécurité informatique cloudAshur configuré avec les paramètres de votre choix (**Partie A**), vous pouvez consulter la **Partie B** pour enregistrer et installer votre appli client Windows ou macOS cloudAshur.

PARTIE A

1. Les indicateurs LED et leur signification

LED	Statut de la LED	Description	LED	Statut de la LED	Description
▲	ROUGE fixe	cloudAshur verrouillé (à l'état de Veille ou de Réinitialisation)	▲	BLEUE fixe	cloudAshur en mode Administrateur
▲	ROUGE - s'affaiblit graduellement	cloudAshur s'éteint	▲▼▲	ROUGE, VERTE et BLEUE clignotantes	En attente de saisie du code PIN utilisateur
▼	VERTE clignotante	cloudAshur déverrouillé en tant qu'administrateur (non connecté au port USB)	▼▲	VERTE et BLEUE clignotent simultanément	En attente de saisie du code PIN administrateur
▼	VERTE fixe	cloudAshur déverrouillé en tant qu'utilisateur (non connecté au port USB) ou cloudAshur en mode Utilisateur	▼▲	VERTE et BLEUE clignotent alternativement	Authentification en cours
▼	VERTE fixe	cloudAshur déverrouillé et connecté à l'hôte	▲		La LED bleue clignote toutes les 5 secondes lorsque le chargement est en cours

2. États de la batterie et des LED

Remarque : le fonctionnement normal du cloudAshur peut être perturbé par les interférences électromagnétiques intenses. Si tel est le cas, éteignez puis rallumez le produit afin de rétablir le fonctionnement normal. Si le fonctionnement normal n'est pas rétabli, veuillez utiliser le produit à un endroit différent.

Capteur de batterie faible

Le cloudAshur comprend un circuit de détection de la tension qui analyse la tension en sortie de batterie lorsque le cloudAshur est allumé. Lorsque la tension de la batterie chute pour atteindre 3,3 V ou moins, la LED ROUGE s'allume trois fois puis s'éteint. Dans ce cas, l'utilisateur doit connecter le cloudAshur à un port USB alimenté et le charger pendant 20-30 minutes. Une fois rechargé, le cloudAshur reprendra son fonctionnement normal.

Pour le réveiller de l'état Inactif

Le cloudAshur est à l'état inactif lorsqu'il n'est pas en cours d'utilisation et que toutes les LED sont éteintes.
Pour réveiller le cloudAshur de l'état Inactif, procédez comme suit.

Appuyez et maintenez enfoncée la touche **Maj** (⬆) pendant une seconde pour connecter le cloudAshur à un port USB alimenté	▲ ▼ → ▲ ▲	Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, puis est remplacée par la LED ROUGE fixe, ce qui indique que le cloudAshur est en mode Veille

Pour passer à l'état Inactif

Pour forcer le cloudAshur à passer à l'état Inactif, exécutez l'une des opérations suivantes :

- Si le cloudAshur est connecté à un port USB, déconnectez-le.
- Si le cloudAshur n'est pas connecté à un port USB, appuyez et maintenez enfoncée la touche **Maj** (⬆) pendant une seconde jusqu'à ce que la LED passe en ROUGE fixe et s'éteigne en passant en mode Inactif (éteint).

États sous tension

Lorsque le cloudAshur sort de l'état Inactif, il passe à l'un des trois états possibles présentés dans le tableau ci-dessous.

État sous tension	Indication de la LED	Clé de chiffrement	Code PIN Administrateur	Description
Veille	ROUGE fixe	✓	✓	En attente de saisie du code PIN administrateur ou utilisateur
Réinitialiser	ROUGE fixe	×	×	Attente de configuration d'un code PIN administrateur
Niveau de batterie faible	ROUGE clignote 3 fois	✓	✓	Charger sur un port USB alimenté pendant 15-30 minutes

Remarque : si votre cloudAshur est déverrouillé et n'est pas connecté à un port USB et qu'aucune opération n'est effectuée dans un délai de 30 secondes, le cloudAshur passe automatiquement à l'état Inactif. La LED passe au ROUGE fixe puis son intensité diminue.

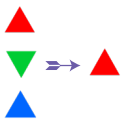
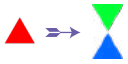
Lorsqu'il est connecté à un port USB connecté, un cloudAshur connecté commencera à charger au bout de 30 secondes, ce qui est indiqué par une LED BLEUE clignotante. Lorsque le cloudAshur est déverrouillé et connecté à un port USB, il n'acceptera plus aucune instruction du clavier.

3. Première utilisation

Votre module de sécurité informatique cloudAshur se lance avec le code PIN administrateur par défaut d'usine suivant : **11223344**.

Important : dans son état par défaut, le module de sécurité informatique cloudAshur ne peut être enregistré. Vous **DEVEZ modifier immédiatement le code PIN administrateur par défaut** tel qu'indiqué à la section 7 «**Comment changer le code PIN administrateur**» afin d'enregistrer votre module de sécurité informatique cloudAshur via l'application client cloudAshur.

Merci de suivre les étapes simples indiquées ci-dessous pour déverrouiller votre cloudAshur pour la première fois avec le code PIN administrateur par défaut d'usine.

Instructions (première utilisation)	LED	Statut de la LED
1. Appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde.		Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, puis est remplacée par la LED ROUGE fixe, ce qui indique que le cloudAshur est en mode Veille
2. En état de veille (LED ROUGE fixe), appuyez une fois sur le bouton **CLÉ (🔑)** .		Les LED de couleur VERTE et BLEUE se mettent à clignoter simultanément.
3. Avec les deux LED VERTE et BLEUE clignotent simultanément, saisissez le code **PIN administrateur** (préréglé d'usine **11223344**) puis appuyez sur la touche **CLÉ (🔑)** une fois		Les LED VERTE et BLEUE clignotent plusieurs fois en alternance, puis la LED BLEUE devient fixe avant d'être remplacée par la VERTE clignotante, ce qui indique que le cloudAshur est déverrouillé en tant qu'Administrateur

Remarque : Une fois que votre cloudAshur a bien été déverrouillé, la LED VERTE reste allumée pendant seulement 30 secondes , pendant lesquelles le cloudAshur doit être connecté à un port USB alimenté. Il peut être immédiatement verrouillé en appuyant et en maintenant enfoncée la touche **MAJ** (⬆) pendant une seconde.

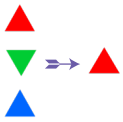
Une fois le cloudAshur déverrouillé et connecté à un port USB, il n'accepte plus d'instructions du clavier.

Verrouiller le cloudAshur

Pour verrouiller le cloudAshur, il vous suffit simplement de le débrancher du port USB ou de faire un clic droit sur l'appli cloudAshur dans le système, puis de cliquer sur Quitter.

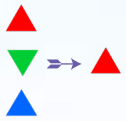
4. Déverrouillage du cloudAshur à l'aide du code PIN administrateur

Suivez les simples étapes du tableau ci-dessous pour déverrouiller le cloudAshur grâce à votre code PIN administrateur à 7-15 chiffres.

1. Appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde.		Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, puis est remplacée par la LED ROUGE fixe, ce qui indique que le cloudAshur est en mode Veille
2. En état de veille (LED ROUGE fixe), appuyez une fois sur le bouton **CLÉ (🔑)** .		Les LED de couleur VERTE et BLEUE se mettent à clignoter simultanément.
3. Alors que les LED de couleur VERTE et BLEUE clignotent simultanément , saisissez votre **code PIN administrateur** et appuyez à nouveau sur la touche **CLÉ (🔑)** une fois.		Les LED VERTE et BLEUE clignotent plusieurs fois en alternance, puis la LED BLEUE devient fixe avant d'être remplacée par la LED VERTE clignotante, ce qui indique que le cloudAshur est déverrouillé en tant qu'Administrateur

5. Pour accéder au mode Administrateur

Pour accéder au mode Administrateur, effectuez les étapes suivantes :

1. Appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde.		Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, et devient ROUGE fixe, ce qui indique que le cloudAshur est en mode Veille
2. En état de veille (LED ROUGE fixe), appuyez une fois sur la touche **CLÉ (⚷)** .		Les LED de couleur VERTE et BLEUE se mettent à clignoter simultanément.
3. Alors que les LED de couleur VERTE et BLEUE clignotent simultanément, saisissez le **code PIN** administrateur (réglage d'usine : **11223344**) et appuyez une fois sur la touche **CLÉ (⚷)** .		Les LED VERTE et BLEUE clignotent plusieurs fois en alternance, puis la LED BLEUE devient fixe avant de devenir VERTE clignotante, ce qui indique que le cloudAshur est déverrouillé.
4. Appuyez sur la touche **CLÉ (⚷) trois** fois en l'espace de 2 secondes (**CLÉ (⚷)** x **3**)		La LED VERTE clignotante sera remplacée par la BLEUE fixe, ce qui indique que le cloudAshur est en mode Administrateur

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

6. Pour quitter le mode Administrateur

Lorsque le cloudAshur est en mode administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode administrateur (LED BLEUE continue), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe devient ROUGE fixe puis s'éteint ensuite et passe en mode Inactif.

7. Modifier le code PIN administrateur

Exigences pour le code PIN :

- Doit comprendre de 7 à 15 chiffres
- Ne doit contenir aucune répétition de chiffres, par ex. (3-3-3-3-3-3-3)
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Conseil pour le mot de passe : pour votre code PIN, vous pouvez configurer une phrase, un nom ou un mot mémorables, ou toute autre combinaison de PIN alphanumérique en appuyant simplement sur les touches qui portent les lettres correspondantes.

Voici des exemples de ces types de codes PIN alphanumériques :

- Pour le terme «**password**», vous appuieriez sur les touches suivantes :
  7 (pqrs) **2** (abc) **7** (pqrs) **7** (pqrs) **9** (wxyz) **6** (mno) **7** (pqrs) **3** (def)
- Pour « **iStorage** » vous appuieriez sur :
  4 (ghi) **7** (pqrs) **8** (tuv) **6** (mno) **7** (pqrs) **2** (abc) **4** (ghi) **3** (def)

Cette méthode permet de configurer des codes PIN longs et faciles à mémoriser.

Pour modifier le code PIN administrateur, accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **CLÉ (🔑) + 2**et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe.
2. Saisissez votre **NOUVEAU code PIN administrateur** et appuyez une fois sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
3. Saisissez à nouveau le **nouveau code PIN administrateur** et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED BLEUE qui se met à clignoter rapidement avant de passer au BLEU fixe indiquant que le code PIN administrateur a été correctement modifié.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif.
Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

8. Définir une politique de code PIN utilisateur

L'administrateur peut définir une politique de restriction pour le code PIN utilisateur. Cette politique consiste à définir la longueur minimum du code PIN (de 7 à 15 chiffres), ainsi que la saisie ou non d'un ou plusieurs «**caractères spéciaux**». Le « caractère spécial » fonctionne comme une pression simultanée sur les deux touches «**Maj** (⬆) + **chiffre**».

Pour définir une politique (restrictions) en matière de code PIN utilisateur, vous devez saisir 3 chiffres, par exemple «**091**», les deux premiers chiffres (**09**) indiquent la longueur minimale du code PIN (dans ce cas, **9**) et le dernier chiffre (**1**) indique qu'un « caractère spécial » doit être utilisé, en d'autres termes « **Maj** (⬆) + **chiffre**. » De même, une politique de code PIN utilisateur peut être définie sans recourir à un « caractère spécial », par exemple «**120**», les deux premiers chiffres (**12**) indiquent la longueur minimale du PIN (dans ce cas,**12**) et le dernier chiffre (**0**), qui indique qu'aucun caractère spécial n'est requis.

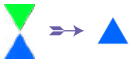
Une fois que l'administrateur a défini la politique de code PIN utilisateur, par exemple « 091 », un nouveau code PIN utilisateur doit être configuré - voir
section 11 « Ajouter un nouveau code PIN utilisateur en mode Administrateur ». Si l'administrateur configure le code PIN utilisateur «**247688314**» avec l'utilisation d'un «**caractère spécial**» (**Maj** (⬆) **+ chiffre** en même temps), celui-ci peut être placé n'importe où dans votre code PIN de 7 à 15 chiffres durant le processus de création du code PIN utilisateur, comme le montrent les exemples ci-dessous.

A. '**Maj** (⬆) **+ 2**', '4', '7', '6', '8', '8', '3', '1', '4',
B. '2', '4', '**Maj** (⬆) **+ 7**', '6', '8', '8', '3', '1', '4',
C. '2', '4', '7', '6', '8', '8', '3', '1', '**Maj** (⬆) **+ 4**',

Remarque :

- Si un « caractère spécial » a été utilisé durant la configuration du code PIN utilisateur, par exemple, l'exemple «**B**» ci-dessus, le cloudAshur ne peut être déverrouillé qu'en saisissant le code PIN avec le « caractère spécial » précisément dans l'ordre configuré soit, dans l'exemple «**B**» ci-dessus - (« 2 », « 4 », «**Maj** (⬆) **+ 7**» , « 6 », « 8 », « 8 », « 3 », « 1 », « 4 »).
- Plus d'un « caractère spécial » peut être utilisé à n'importe quel emplacement dans votre code PIN de 7 à 15 chiffres.
- Les utilisateurs peuvent changer leur code PIN mais sont contraints de respecter la « politique de code PIN utilisateur » définie (restrictions), si et quand elle est applicable.
- Le fait de définir une nouvelle politique en matière de code PIN utilisateur supprimera automatiquement le code PIN utilisateur s'il en existe un.
- Cette politique ne s'applique pas au « code PIN d'autodestruction ». Le paramètre de complexité pour le code PIN d'autodestruction et le code PIN administrateur comporte toujours de 7 à 15 chiffres, sans caractère spécial requis.

Pour définir une politique de **code PIN utilisateur**, accédez d'abord au «**mode administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **CLÉ (🔑) + 7** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez vos **3 chiffres**, n'oubliez pas que les deux premiers chiffres représentent la longueur minimale du code PIN et que le dernier chiffre (0 ou 1) indique si un caractère spécial a été utilisé ou non.		Les LED VERTE et BLEUE clignotantes continueront de clignoter
3. Appuyez une fois sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE continue, puis une LED BLEUE continue, indiquant que la politique en matière de code PIN utilisateur a été correctement définie.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

9. Comment supprimer la politique de code PIN utilisateur

Pour supprimer la **politique de code PIN utilisateur**, accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que votre cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **CLÉ (🔑) + 7** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez **070** et appuyez une fois sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE fixe, puis une LED BLEUE fixe, indiquant que la politique de code PIN utilisateur a été correctement supprimée.

10. Comment vérifier la politique de code PIN utilisateur

L'administrateur peut vérifier la politique de code PIN utilisateur et peut identifier la règle de longueur minimale du code PIN et si l'utilisation d'un caractère spécial a été définie ou non en notant la séquence de LED décrite ci-dessous.

Pour vérifier la politique de code PIN utilisateur, accédez d'abord au «**mode administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **Maj** (⬆) + **7**» et maintenez-les enfoncées.		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ (🔑)** et vous observerez ce qui suit : a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. b. Un clignotement de la LED ROUGE est égal à dix (10) unités d'un code PIN. c. Chaque clignotement de la LED VERTE est égal à une (1) unité d'un code PIN. d. Un clignotement BLEU indique l'utilisation d'un caractère spécial. e. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. f. Les LED reviennent au BLEU fixe.		

Le tableau ci-dessous décrit le comportement des LED lorsque vous vérifiez la politique de code PIN utilisateur, par exemple si vous avez défini un code PIN utilisateur de 12 chiffres avec utilisation d'un caractère spécial (**121**), la LED ROUGE clignotera une fois (**1**) et la LED VERTE clignotera deux fois (**2**), suivie d'un seul (**1**) clignotement de la LED BLEUE indiquant qu'un seul **caractère spécial** doit être utilisé.

Description du PIN	**Configuration à 3 chiffres**	**ROUGE**	**VERT**	**BLEU**
Code PIN de 12 chiffres avec utilisation d'un caractère spécial	121	1 clignotement	2 clignotements	1 clignotement
Code PIN de 12 chiffres SANS utilisation d'un caractère spécial	120	1 clignotement	2 clignotements	0
Code PIN de 9 chiffres avec utilisation d'un caractère spécial	091	0	9 clignotements	1 clignotement
Code PIN de 9 chiffres SANS utilisation d'un caractère spécial	090	0	9 clignotements	0

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

11. Ajouter un nouveau code PIN utilisateur en mode Administrateur

Exigences pour le code PIN :

- Doit comprendre de 7 à 15 chiffres
- Ne doit contenir aucune répétition de chiffres, par ex. (3-3-3-3-3-3-3)
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)
- La touche **Maj** (⬆) peut être utilisée pour d'autres combinaisons de PIN - par ex. **Maj** (⬆) **+ 1** produit une valeur différente de 1. Voir la section 8. « Définir une politique de code PIN utilisateur »

Pour ajouter un **nouveau Code PIN**utilisateur, accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**CLÉ (🔑) + 3**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe.
2. Saisissez le **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
3. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez à nouveau sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui se met à clignoter rapidement avant de passer au BLEU fixe, indiquant que le code PIN utilisateur a été correctement configuré.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

12. Modifier le code PIN utilisateur en mode administrateur

Pour modifier un **code PIN utilisateur**existant, accédez d'abord au «**mode administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**CLÉ (🔑) + 3**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe.
2. Saisissez le **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
3. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez à nouveau sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE continue sont remplacées par la LED VERTE qui se met à clignoter rapidement avant d'être continue et BLEUE , indiquant que le code PIN utilisateur a été correctement modifié.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif.
Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

13. Supprimer le code PIN utilisateur en mode Administrateur

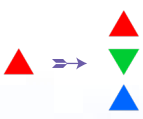
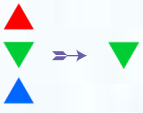
Pour supprimer un **code PIN utilisateur**existant, accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**Maj** (⬆) **+ 3**» et maintenez-les enfoncées.		La LED BLEUE continue est remplacée par la LED ROUGE clignotante.
2. Appuyez sur les touches «**Maj** (⬆) **+ 3**» et maintenez-les enfoncées.		La LED ROUGE clignotante est remplacée par la LED ROUGE continue, puis par la LED BLEUE continue, indiquant que le code PIN utilisateur a été correctement supprimé.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif.
Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

14. Comment déverrouiller votre cloudAshur avec le code PIN utilisateur

Pour déverrouiller à l'aide du **code PIN utilisateur,** le cloudAshur doit d'abord être en mode Veille (LED ROUGE fixe) en appuyant sur la touche **Maj** (⬆) pendant une seconde.

1. En état de veille (LED ROUGE continue), appuyez sur les touches **Maj** (⬆) + **CLÉ (🔑)** et maintenez-les enfoncées		La LED ROUGE est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter.
2. Saisissez le **code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)** .		Les LED ROUGE, VERTE et BLEUE clignotantes seront remplacées par des LED VERTE et BLEUE en alternance, puis par une LED VERTE continue qui indique un déverrouillage réussi du cloudAshur en mode Utilisateur.

15. Modifier le code PIN utilisateur en mode Utilisateur

Pour modifier le **code PIN utilisateur**, déverrouillez d'abord le cloudAshur avec un code PIN utilisateur tel que décrit dans la section 14. Une fois que le cloudAshur est en **mode Utilisateur** (LED VERTE continue), effectuez les étapes suivantes.

1. En mode Utilisateur, appuyez sur les touches **CLÉ (🔑) + 4 et maintenez-les enfoncées**		La LED VERTE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe.
2. Saisissez le **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
3. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui se met à clignoter rapidement avant de passer au VERT fixe, indiquant une modification réussie du code PIN utilisateur.

Important: la modification du code PIN utilisateur doit se conformer à la « Politique de code PIN utilisateur », si cette dernière a été configurée tel que décrit dans la section 8, et qui impose une longueur minimale du code PIN et spécifie si un caractère spécial doit être utilisé. L'administrateur peut se reporter à la section 10 pour vérifier les restrictions en matière de code PIN utilisateur.

16. Configurer un code PIN utilisateur de récupération à usage unique

Le code PIN de récupération utilisateur à usage unique est extrêmement utile dans les situations où un utilisateur a oublié son code PIN, afin de déverrouiller le cloudAshur. Pour activer le mode Récupération, l'utilisateur doit d'abord saisir le code PIN de récupération à usage unique, si ce dernier a été configuré. Le processus de récupération du code PIN n'affecte pas la clé de chiffrement et le code PIN administrateur. Cependant, l'utilisateur est contraint de configurer un nouveau code PIN utilisateur de 7 à 15 chiffres.
Pour configurer un code PIN utilisateur de récupération à usage unique de 7 à 15 chiffres, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**CLÉ (🔑) + 4**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe.
2. Saisissez un **code PIN de récupération à usage unique** et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
3. Saisissez à nouveau un **code PIN de récupération à usage unique** et appuyez à nouveau sur la touche **CLÉ (🔑)**		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui se met à clignoter rapidement avant de se fixer en BLEU indiquant que le code PIN de récupération à usage unique a été correctement configuré.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

17. Supprimer le code PIN utilisateur de récupération à usage unique

Pour supprimer la code PIN utilisateur de récupération à usage unique, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**Maj** (⬆) **+ 4**» et maintenez-les enfoncées.	▲ ➙ ▲	La LED BLEUE fixe est remplacée par la LED ROUGE clignotante.
2. Appuyez sur les touches «**Maj** (⬆) **+ 4**» et maintenez-les enfoncées.	▲ ➙ ▲	La LED ROUGE clignotante s'allumera en ROUGE fixe, puis sera remplacée par une LED BLEUE fixe, ce qui indique que le code PIN utilisateur de récupération à usage unique a été supprimé avec succès

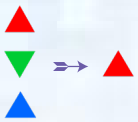
Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

18. Activer le mode Récupération et configurer un nouveau code PIN utilisateur

Le code PIN de récupération utilisateur à usage unique est extrêmement utile dans les situations où un utilisateur a oublié son code PIN, afin de déverrouiller le cloudAshur. Pour activer le mode Récupération, l'utilisateur doit d'abord saisir le code PIN de récupération à usage unique, si ce dernier a été configuré. Le processus du code PIN utilisateur de récupération n'affecte pas la clé de cryptage ni le code PIN administrateur. Toutefois, l'utilisateur est dans l'obligation de configurer un nouveau code PIN utilisateur à 7-15 chiffres.

Pour lancer le processus de récupération et configurer un nouveau code PIN utilisateur, voici les étapes que vous devez suivre.

1. Lorsque le cloudAshur est à **l'état Inactif,** appuyez sur la touche **Maj** (⬆) et maintenez-le enfoncée pendant une seconde		Les LED ROUGE, VERTE et BLEUE clignotent l'une après l'autre, puis la LED VERTE clignote deux fois, puis est remplacée par la LED ROUGE fixe, ce qui indique que le cloudAshur est en mode Veille
2. En **mode Veille,** appuyez sur les touches «**CLÉ (🔑) + 4**» et maintenez-les enfoncées		La LED ROUGE fixe est remplacée par les LED ROUGE et VERTE clignotantes
3. Saisissez le **code PIN de récupération** à usage unique et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE et BLEUE clignotent en alternance, puis sont remplacées par une LED VERTE fixe, puis par les LED VERTE clignotante et BLEUE fixe.
4. Saisissez le **Nouveau code PIN utilisateur** et appuyez sur la touche **CLÉ (🔑)**		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
5. Saisissez à nouveau le **nouveau code PIN utilisateur** et appuyez à nouveau sur la touche **CLÉ (🔑)**		La LED VERTE clignote rapidement, puis devient VERTE fixe, ce qui indique que le processus de récupération est réussi et qu'un nouveau code PIN utilisateur a été configuré

Important: La création d'un nouveau code PIN utilisateur doit se conformer à la « Politique de code PIN utilisateur », si une telle politique a été configurée, tel que décrit dans la section 8, qui impose une longueur minimale du code PIN et spécifie si un caractère spécial doit être utilisé. Reportez-vous à la section 10 pour vérifier les restrictions en matière de code PIN utilisateur.

19. Comment paramétrer votre cloudAshur pour autoriser le KeyWriter Cloning

Remarque: le cloudAshur est paramétré par défaut pour autoriser le clonage par le KeyWriter.

Le cloudAshur peut être utilisé en conjonction avec le iStorgae KeyWriter afin de permettre le clonage d'un maximum de 9 appareils en même temps. Pour permettre au cloudAshur d'être cloné par le KeyWriter, saisissez tout d'abord le «**Mode Administrateur**» tel qu'indiqué dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**CLÉ (🔑) + 8**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez «**11**» et appuyez sur la touche «**Maj** (⬆) » une fois.		Les LED VERTE et BLEUE sont remplacées par la LED VERTE fixe, puis la LED BLEUE fixe indiquant que le cloudAshur est paramétré pour autoriser le KeyWriter cloning

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

20. Comment désactiver le KeyWriter Cloning

Pour désactiver le KeyWriter Cloning, accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**CLÉ (🔑) + 8**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez «**44**» et appuyez sur la touche «**Maj** (⬆) ».		Les LED VERTE et BLEUE sont remplacées par la LED VERTE fixe, puis par la LED BLEUE fixe, indiquant que le KeyWriter Cloning est désactivé.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

21. Comment vérifier la configuration du KeyWriter Cloning

Pour vérifier si le KeyWriter Cloning de cloudAshur est activé ou non, saisissez d'abord le «**Mode Administrateur**» tel que décrit à la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur appuyez, sur les touches **Maj** (⬆) + **8»** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.

2. Appuyez sur la touche **CLÉ (🔑)** et vous observerez ce qui suit :

- **Si votre cloudAshur est paramétré pour permettre le KeyWriter Cloning, voici ce qui ce produit :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote une fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU fixe.

- **Si le KeyWriter Cloning est désactivé, voici ce qui se produit :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. Toutes les LED s'éteignent
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU fixe.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

22. Comment désactiver l'enregistrement de l'appli client cloudAshur

Le cloudAshur est configuré de manière à ne pas pouvoir être enregistré par l'application client lorsqu'il est expédié de l'usine, ou totalement réinitialisé. La fonctionnalité de l'application client est automatiquement activée lorsque le code PIN administrateur initial est modifié ou lorsqu'un code PIN utilisateur est configuré ou modifié.

Pour désactiver l'enregistrement de l'application client, saisissez d'abord le «**Mode Administrateur**» tel que décrit à la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**3 + 7**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez une fois sur la touche **CLÉ (ර)** .		Les LED VERTE et BLEUE seront remplacées par une LED VERTE fixe, puis une LED BLEUE fixe indiquant que l'enregistrement de l'application client est désactivé.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

23. Comment vérifier si l'enregistrement de l'application client est activé

Pour vérifier si l'enregistrement de l'application client cloudAshur est activé, commencez par saisir le «**Mode Administrateur**» tel que décrit à la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches « **2 + 7** » et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.

2. Appuyez sur la touche **CLÉ (⚷)** et vous observerez ce qui suit :

- **Si l'enregistrement de votre application client est activé :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote une fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU fixe.

- **Si l'enregistrement de votre application client cloudAshur est désactivé :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. Toutes les LED s'éteignent
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU fixe.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

24. Comment configurer le mode cryptage de cloudAshur

ATTENTION : Passer le mode cryptage de AES-XTS (par défaut) à AES-ECB ou vice versa, supprimera la clé de cryptage et cloudAshur se réinitialisera et encodera toutes vos données pour votre cloudAshur, et seront donc inaccessibles et définitivement perdues ! N'effectuez cette action uniquement avant que toute donnée soit téléchargée sur le cloud ou des fichiers locaux, ou si vous disposez d'un ou plusieurs modules de sécurité informatique cloudAshur contenant la même clé de cryptage depuis laquelle effectuer la copie, ou si une sauvegarde complète et non codée de vos données est disponible.

Suivez ces étapes pour configurer le mode cryptage de cloudAshur, en **AES-ECB**, indiqué par le numéro **01**, ou **AES-XTS**, indiqué par le numéro **02**. Cette fonctionnalité est paramétrée comme AES-XTS (02) par défaut. Lorsqu'un mode cryptage spécifique est configuré, les données sont cryptées par le cloudAshur à l'aide de l'algorithme indépendant.

Pour configurer le mode cryptage de cloudAshur, accédez d'abord au mode Administrateur tel que décrit dans la section 5. Une fois que le cloudAshur est en mode Administrateur (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**CLÉ (⚷) + 1**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez **01** pour choisir **AES-ECB** Saisissez **02** pour choisir **AES-XTS (par défaut)**		Les LED VERTE et BLEUE clignotantes continueront de clignoter
3. Appuyez une fois sur le bouton **Maj** (⬆)		Les LED VERTE et BLEUE seront remplacées par une LED VERTE fixe, puis une LED ROUGE fixe (**Le stade de Réinitialisation**) indique un passage réussi au mode de cryptage cloudAshur .

Important: Après avoir configuré le mode de cryptage cloudAshur , le cloudAshur se réinitialise totalement, et un nouveau code PIN Administrateur doit être configuré. Référez-vous à la Section 29 de la page 114 à «Comment configurer un code PIN Administrateur après une attaque brutale ou une réinitialisation».

25. Comment vérifier le mode de cryptage

Pour vérifier le mode de cryptage cloudAshur accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur appuyez sur les touches **«Maj** (⬆) + **1»** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.

2. Appuyez sur la touche **CLÉ (⚷)** et vous observerez ce qui suit :

- **Si le mode de cryptage est configuré AES-ECB :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED VERTE clignote une fois.
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU fixe.

- **Si le mode est configuré AES-XTS :**

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. Toutes les LED s'éteignent
c. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
d. Les LED reviennent au BLEU fixe.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

26. Comment configurer un code PIN d'autodestruction

Vous pouvez configurer un code PIN d'autodestruction qui, une fois saisi, supprime tous les codes PIN configurés et réalise une suppression d'encodage sur le cloudAshur (la clé de cryptage est supprimée). À l'activation de cette fonction, le code PIN d'autodestruction deviendra le nouveau code PIN utilisateur.

Pour paramétrer le code PIN d'autodestruction, commencez par saisir le «**Mode Administrateur**» tel que décrit à la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**CLÉ (🔑) + 6**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe
2. Configurez un **code PIN d'autodestruction** de 7 à 15 chiffres et appuyez sur la touche **CLÉ (🔑)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
3. Saisissez à nouveau le **code PIN d'autodestruction** et appuyez sur la touche **CLÉ (🔑)**		La LED VERTE clignote rapidement pendant plusieurs secondes, puis est remplacée par la LED BLEUE fixe, ce qui indique que le code PIN d'autodestruction a été correctement configuré.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

27. Comment supprimer le code PIN d'autodestruction

Pour supprimer le code PIN d'autodestruction, accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

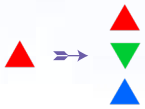
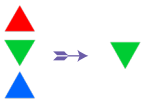
1. En mode Administrateur appuyez sur les touches **«Maj** (⬆) **+ 6»** et maintenez-les enfoncées		La LED BLEUE continue est remplacée par la LED ROUGE clignotante.
2. Appuyez à nouveau sur les touches «**Maj** (⬆) **+ 6»** et maintenez-les enfoncés.		La LED ROUGE clignotante devient continue, puis est remplacée par la LED BLEUE continue, indiquant que le code PIN d'autodestruction a été correctement supprimé.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

28. Comment déverrouiller avec le code PIN d'autodestruction

Lorsqu'il est utilisé, le code PIN d'autodestruction **supprime la clé de chiffrement, TOUTES les données, les codes PIN administrateur/utilisateur,** puis déverrouille le cloudAshur. À l'activation de cette fonction, le **code PIN d'autodestruction deviendra le nouveau code PIN utilisateur.**
Pour activer le mécanisme d'autodestruction, le cloudAshur doit être en état de Veille (LED ROUGE fixe) puis passer aux étapes suivantes.

1. En état de Veille (LED ROUGE fixe), appuyez sur les touches **Maj** (⬆) + **CLÉ (⚷)** et maintenez-les enfoncées		La LED ROUGE est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter.
2. Saisissez le **code PIN d'autodestruction** et appuyez sur la touche **CLÉ (⚷)** .		Les LED ROUGE, VERTE et BLEUE clignotantes sont remplacées par les LED VERTE et BLEUE qui s'allument en alternance pendant quelques secondes, avant de céder la place à la LED VERTE, ce qui indique que le cloudAshur s'est autodétruit avec succès.

Avertissement : quand le mécanisme d'autodestruction est activé, la clé de chiffrement et les codes PIN administrateur/utilisateur sont supprimés. **Le code PIN d'autodestruction devient le code PIN utilisateur.** Aucun code PIN administrateur n'existe après l'activation du mécanisme d'autodestruction. Le **cloudAshur doit d'abord être réinitialisé** (voir la section 36 « Comment effectuer une réinitialisation complète » à la page 120) afin de configurer un code PIN administrateur avec les pleins privilèges administrateur, notamment la possibilité de configurer un code PIN utilisateur.

29. Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation

Après une attaque par force brute ou quand le cloudAshur a été réinitialisé, vous devez configurer un code PIN administrateur avant de pouvoir utiliser le cloudAshur .

Exigences pour le code PIN :

- Doit comprendre de 7 à 15 chiffres
- Ne doit contenir aucune répétition de chiffres, par ex. (3-3-3-3-3-3-3)
- Ne doit pas se composer uniquement de chiffres consécutifs, par ex. (1-2-3-4-5-6-7), (7-8-9-0-1-2-3-4), (7-6-5-4-3-2-1)

Si le cloudAshur a subit une attaque par force brutale ou été réinitialisé, le cloudAshur sera en état de Veille (LED ROUGE fixe). Pour configurer un codde PIN Administrateur, voici les étapes à suivre.

1. En mode Veille (LED ROUGE fixe), appuyez sur les touches **Maj** (⬆) **+ 1** et maintenez-les enfoncés		La LED ROUGE fixe est remplacée par les LED VERTE clignotante et BLEUE fixe.
2. Saisissez le **nouveau code PIN administrateur** et appuyez une fois sur la touche **CLÉ (⚷)** .		Les LED VERTE clignotante et BLEUE fixe sont remplacées par la LED VERTE qui clignote une seule fois, puis par les LED VERTE clignotante et BLEUE fixe.
3. Saisissez à nouveau le **nouveau code PIN administrateur** et appuyez sur la touche **CLÉ (⚷)**		La LED VERTE clignotante et la LED BLEUE fixe sont remplacées par la LED BLEUE qui se met à clignoter rapidement avant de passer au BLEU fixe indiquant que le code PIN administrateur a été correctement configuré.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

30. Définir l'horloge du verrouillage automatique

Pour protéger le cloudAshur contre les accès non autorisés s'il est déverrouillé et laissé sans surveillance, il est possible de configurer le cloudAshur de façon à ce qu'il se verrouille automatiquement au bout d'un intervalle prédéfini. Dans son état par défaut, la fonctionnalité de verrouillage automatique pour non-utilisation du cloudAshur est désactivée. Le verrouillage automatique peut être défini de façon à se déclencher au bout de 5 à 99 minutes.

Pour définir le verrouillage automatique pour non-utilisation, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **CLÉ (🔑) + 5** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez la durée sur laquelle vous souhaitez définir le délai de verrouillage automatique, le délai minimal possible étant de 5 minutes et le maximal étant de 99 minutes (de 5 à 99 minutes). Par exemple, saisissez : **05 pour 5 minutes** **20 pour 20 minutes** **99 pour 99 minutes**		
3. Appuyez sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE fixe pendant une seconde, puis enfin par la LED BLEUE fixe, indiquant que le délai du verrouillage automatique a été correctement configuré.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

31. Désactiver la minuterie de verrouillage automatique en cas de non-utilisation

Pour désactiver le verrouillage automatique en cas de non-utilisation, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **CLÉ (🔑) + 5** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Saisissez « **00** » et appuyez sur la touche **Maj** (⬆).		Les LED VERTE et BLEUE clignotantes sont remplacées par la LED VERTE fixe pendant une seconde, puis enfin par la LED BLEUE fixe, indiquant que le délai du verrouillage automatique a été correctement désactivé.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

32. Comment vérifier la minuterie de verrouillage automatique en cas de non-utilisation

L'administrateur est en mesure de vérifier et de déterminer la durée définie pour la minuterie de verrouillage automatique en cas de non-utilisation en notant simplement la séquence des LED décrite dans le tableau en bas de cette page.

Pour vérifier le verrouillage automatique en cas de non-utilisation, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE continue), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **Maj** (⬆) + **5 et maintenez-les enfoncés.**		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ (🔑)** et vous observerez ce qui suit : a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. b. Chaque clignotement de la LED ROUGE est égal à dix (10) minutes. c. Chaque clignotement de la LED VERTE est égal à une (1) minute. d. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. e. Les LED reviennent au BLEU fixe.		

Le tableau ci-dessous décrit le comportement des LED lorsque vous vérifiez la minuterie de verrouillage automatique en cas de non-utilisation, par exemple si vous avez programmé le cloudAshur pour se verrouiller automatiquement au bout de **25** minutes, la LED ROUGE clignotera deux (**2**) fois et la LED VERTE clignotera cinq (**5**) fois.

Verrouillage automatique en minutes	ROUGE	VERT
5 minutes	0	5 clignotements
15 minutes	1 clignotement	5 clignotements
25 minutes	2 clignotements	5 clignotements
40 minutes	4 clignotements	0

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

33. Mécanisme de défense contre les tentatives de piratage par la force brute

Le cloudAshur intègre un mécanisme de défense visant à protéger le clloudAshur contre les attaque par force brute. Par défaut, les valeurs de l'état d'expédition initial pour la limite d'attaque par force brute (nombre de saisies incorrectes consécutives du code PIN) pour le code PIN administrateur et le code PIN utilisateur sont fixées à **10** et **5** pour le code PIN de récupération. Trois compteurs d'attaques par force brute indépendants sont utilisés pour enregistrer le nombre de de tentatives infructueuses pour chaque autorisation par code PIN (administrateur, utilisateur et récupération), tel que défini ci-dessous.

- Si un utilisateur saisit un **code PIN** utilisateur incorrect 10 fois consécutives, le code PIN utilisateur sera supprimé mais les données, le code PIN administrateur et le code PIN de récupération resteront intacts et accessibles.
- Si un **code PIN de récupération incorrect** est saisi 5 fois consécutives, le code PIN de récupération est supprimé mais les données et le code PIN admin restent intacts et accessibles.
- Si un code **PIN administrateur** incorrect est saisi 10 fois consécutives, le cloudAshur sera réinitialisé. Tous les codes PIN et les données sont supprimés et définitivement perdus.

Le tableau ci-dessous suppose que les trois codes PIN ont été configurés et souligne les effets produits par le déclenchement du mécanisme de défense contre les attaques de force brute de chaque type de code PIN.

Code PIN utilisé pour déverrouiller le cloudAshur	Saisies consécutives d'un code PIN erroné	Description des conséquences
Code PIN Utilisateur	10	• Le code PIN utilisateur est supprimé. • Le code PIN de récupération, le code PIN administrateur et toutes les données restent intacts et accessibles.
Code PIN de récupération	5	• Le code PIN de récupération est supprimé. • Le code PIN administrateur et toutes les données restent intacts et accessibles.
Code PIN Administrateur	10	• Le cloudAshur se réinitialisera. Tous les codes PIN et les données sont supprimés et définitivement perdus.

Remarque: La limite d'attaques par force brute est définie par défaut sur les valeurs de l'état d'expédition initial lorsque le cloudAshur est complètement réinitialisé, que la fonctionnalité d'autodestruction et activée, ou qu'il fait l'objet d'une attaque par force brute. Si l'administrateur modifie le code PIN utilisateur ou qu'un nouveau code PIN utilisateur est configuré lors de l'activation de la fonctionnalité de récupération, le compteur d'attaques par force brute du code PIN utilisateur est remis à zéro (0), mais la limite d'attaques par force brute n'est pas affectée. Si l'administrateur modifie le code PIN de récupération, le compteur d'attaques par force brute du code PIN de récupération est remis à zéro.

L'autorisation réussie d'un code PIN donné provoque une remise à zéro du compteur d'attaques par force brute pour ce code PIN, mais n'affecte pas le compteur de force brute des autres codes PIN. L'échec de l'autorisation d'un certain code PIN provoquera une incrémentation du compteur pour ce code PIN, mais n'affectera pas le compteur d'attaques par force brute des autres codes PIN.

34. Comment définir la limite d'attaque par force brute du code PIN utilisateur

Remarque: la limite d'attaque par force brute du code PIN utilisateur est définie par défaut sur 10 saisies de code PIN erroné, lorsque le cloudAshur est complètement réinitialisé, subit une attaque par force brute ou que le code PIN d'autodestruction est activé.

La limite d'attaque par force brute du code PIN utilisateur du cloudAshur peut être reprogrammée et définie par l'administrateur. Cette fonctionnalité peut être configurée de manière à permettre de 1 à 10 tentatives de saisie de code PIN erroné.
Pour configurer le nombre limite d'attaques par force brute, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **7 + 0** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE qui clignotent simultanément.
2. Saisissez le nombre de tentatives pour la limite d'attaque par force brute (entre 01 et 10). Par exemple, saisissez : • **01** pour 1 tentative • **10** pour 10 tentatives		
3. Appuyez une fois sur la touche **Maj** (⬆)		Les LED VERTE et BLEUE clignotantes seront remplacée par une LED VERTE fixe pendant une seconde, puis par une LED BLEUE qui indique que la limite d'attaque par force brute a été configurée avec succès

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).
Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif.
Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

35. Comment vérifier la limite d'attaques par force brute du code PIN utilisateur

L'administrateur peut observer et déterminer le nombre de saisies consécutives autorisées d'un code PIN utilisateur erroné avant de déclencher le mécanisme de défense contre l'attaque par force brute en notant simplement la séquence LED décrite ci-dessous.

Pour vérifier le paramètre de limite d'attaques par force brute, accédez d'abord au « **mode Administrateur** » tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches **2** + **0** et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ (🔑)** et vous observerez ce qui suit; a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. b. Chaque clignotement de la LED ROUGE est égal à dix (10) unités d'un chiffre de limite d'attaques par force brute. c. Chaque clignotement de la LED VERTE est égal à une (1) unité d'un chiffre de limite d'attaques par force brute. d. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. e Les LED reviennent au BLEU fixe.		

Le tableau ci-dessous décrit le comportement des LED lorsque vous vérifiez la limite d'attaques par force brute, par exemple si vous avez programmé le cloudAshur pour détecter une attaque par force brute au bout de **5** saisies consécutives d'un code PIN erroné, la LED VERTE clignotera cinq (**5**) fois.

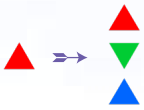
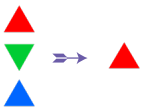
Paramètre de limite d'attaque par force brute	ROUGE	VERT
2 tentatives	0	2 clignotements
5 tentatives	0	5 clignotements
10 tentatives	1 clignotement	0

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

36. Comment effectuer une réinitialisation complète

Pour effectuer une réinitialisation complète, le cloudAshur doit être en état de veille (LED ROUGE continue). Une fois le cloudAshur réinitialisé, alors tous les codes PIN Administrateur/Utilisateur ainsi que le clé de chiffrement seront supprimés. Toutes les données associées seront alors codées et inaccessibles.
Pour réinitialiser le cloudAshur, effectuez les étapes suivantes.

1. En mode veille (LED ROUGE fixe), appuyez sur la touche "**0**" et maintenez-la enfoncée		La LED ROUGE fixe est remplacée par toutes les LED, ROUGE, VERTE et BLEUE qui se mettent à clignoter en alternance.
2. Appuyez sur les touches **2 + 7** et maintenez-les enfoncées.		Les LED ROUGE, VERTE et BLEUE qui clignotaient en alternance s'allument toutes en continu pendant une seconde, puis sont remplacées par une LED ROUGE fixe indiquant que le lecteur a été réinitialisé.

Important: après une réinitialisation complète, un nouveau code PIN doit être configuré. Référez-vous à la Section 29 de la page 114 sur 'Comment configurer un code PIN administrateur après une attaque par force brute ou une réinitialisation'.

37. Comment vérifier le microprogramme en mode Administrateur

Pour vérifier le numéro de révision du microprogramme, accédez d'abord au «**mode Administrateur**» tel que décrit dans la section 5. Une fois que le cloudAshur est en **mode Administrateur** (LED BLEUE fixe), effectuez les étapes suivantes.

1. En mode Administrateur, appuyez sur les touches «**3** + **8**» et maintenez-les enfoncées		La LED BLEUE fixe est remplacée par les LED VERTE et BLEUE clignotantes.

2. Appuyez une fois sur la touche **CLÉ (🔑)** et vous observerez ce qui suit :

a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
b. La LED ROUGE clignote, indiquant la partie intégrante du numéro de révision du microprogramme.
c. La LED VERTE clignote pour indiquer la partie fractionnaire.
d. La LED BLEUE clignote pour indiquer le dernier chiffre du numéro de révision du micrologiciel
e. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde.
f. Les LED ROUGE, VERTE et BLEUE sont remplacées par une LED BLEUE fixe

Par exemple, si le numéro de révision du microprogramme est «**4.2**», la LED ROUGE clignote quatre (**4**) fois et la LED VERTE clignote deux (**2**) fois. Une fois la séquence terminée, les LED ROUGE, VERTE et BLEUE clignotent une fois simultanément, puis sont remplacées par la LED BLEUE fixe.

Remarque : Lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

38. Comment vérifier le microprogramme en mode Utilisateur

Pour vérifier le numéro de révision du microprogramme, accédez d'abord au «**mode Utilisateur**» tel que décrit dans la section 14. Une fois que le cloudAshur est en **mode utilisateur** (LED VERTE fixe), effectuez les étapes suivantes.

1. En mode Utilisateur, appuyez sur les touches «**3** + **8**» et maintenez-les enfoncées jusqu'à ce que les LED VERTE et BLEUE clignotent simultanément.		La LED VERTE fixe est remplacée par les LED VERTE et BLEUE clignotantes.
2. Appuyez sur la touche **CLÉ (🔑)** et vous observerez ce qui suit : a. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. b. La LED ROUGE clignote, indiquant la partie intégrante du numéro de révision du microprogramme. c. La LED VERTE clignote pour indiquer la partie fractionnaire. d. La LED BLEUE clignote pour indiquer le dernier chiffre du numéro de révision du micrologiciel e. Toutes les LED (ROUGE, VERTE et BLEUE) s'allument en continu pendant 1 seconde. f. Les LED ROUGE, VERTE et BLEUE sont remplacées par une LED BLEUE fixe		

Par exemple, si le numéro de révision du microprogramme est «**4.2**», la LED ROUGE clignote quatre (**4**) fois et la LED VERTE clignote deux (**2**) fois. Une fois la séquence terminée, les LED ROUGE, VERTE et BLEUE clignotent une fois simultanément, puis sont remplacées par la LED BLEUE fixe.

Remarque : lorsque le cloudAshur est en mode Administrateur, la LED BLEUE reste allumée en continu pendant seulement 30 secondes, durant lesquelles le cloudAshur peut accepter des instructions du clavier, ce qui permet de configurer plusieurs fonctionnalités de sécurité. Si aucune saisie n'est effectuée pendant 30 secondes, le cloudAshur quitte automatiquement le mode Administrateur - la LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif (toutes les LED éteintes).

Pour quitter immédiatement le mode Administrateur (LED BLEUE fixe), appuyez sur la touche **Maj** (⬆) et maintenez-la enfoncée pendant une seconde - La LED BLEUE fixe est remplacée par la ROUGE fixe puis s'éteint ensuite et passe en mode Inactif. Pour déverrouiller et accéder à vos données, votre cloudAshur doit d'abord être en mode Inactif (toutes les LED éteintes) avant qu'un code PIN administrateur/utilisateur puisse être saisi.

39. Assistance technique

iStorage vous fournit les ressources utiles suivantes :

Site Internet :
https://www.istorage-uk.com

E-mail d'assistance technique :
support@istorage-uk.com

Téléphone d'assistance technique :
+44 (0) 20 8991-6260.

Les spécialistes de l'assistance technique d'iStorage sont disponibles de 9 h 00 à 17 h 30 (GMT), du lundi au vendredi.

40. Informations de garantie et de renvoi de matériel

LIMITE DE RESPONSABILITÉ ET GARANTIE DU PRODUIT ISTORAGE

iStorage garantit qu'à la livraison et pour la période de 36 mois qui la suit, ses produits ne présenteront aucun défaut matériel. Toutefois, cette garantie ne concerne pas les cas décrits ci-dessous. iStorage garantit que les produits sont conformes aux normes listées dans la fiche de données correspondante qui se trouvait sur notre site web au moment où vous avez passé votre commande.

Ces garanties ne couvrent aucun défaut des produits découlant de :

- une usure normale ;
- un dommage volontaire, stockage ou conditions de fonctionnement anormaux, accident, négligence de votre part ou de celle de toute tierce partie ;
- si un tiers ou vous manquez à faire fonctionner ou utiliser les produits conformément aux instructions de l'utilisateur ;
- toute modification ou réparation effectuée par vous ou un tiers n'étant pas l'un de nos réparateurs autorisés ; ou
- toute caractéristique fournie par vous.

Dans le cadre de ces garanties et à notre seule discrétion, nous réparerons, remplacerons ou vous rembourserons tout produit présentant un défaut matériel, à condition qu'à la livraison :

- vous ayez inspecté les produits afin de vérifier qu'ils ne comportaient aucun défaut matériel ; et
- vous ayez testé le mécanisme d'encodage des produits.

Nous ne serons tenus responsable d'aucun défaut matériel ou défaut du mécanisme d'encodage des produits qui aurait pu être vérifié à la livraison, sauf si vous déclarez ce défaut auprès de nous dans un délai de 30 jours après la livraison. Nous ne serons tenu responsables d'aucun défaut matériel ou défaut du mécanisme d'encodage des produits n'étant pas détectable lors d'une inspection réalisée à la livraison, sauf si vous nous signalez ce défaut dans un délai de 7 jours après l'avoir découvert ou après le jour où vous auriez dû le remarquer. Dans le cadre des présentes garanties, nous ne serons en aucun tenus responsable si vous ou qui que ce soit d'autre continuez à utiliser les produits après avoir découvert le défaut. Après le signalement d'un défaut, vous devez nous renvoyer le produit. Si vous êtes une entreprise, les frais de port liés au renvoi du produit ou des pièces du produit concernées à notre adresse dans le cadre de cette garantie, seront à votre charge, et nous prendrons en charge les frais de port liés au renvoi d'un produit réparé ou remplacé à votre adresse. Si vous êtes un particulier, merci de consulter nos conditions générales.

Les produits renvoyés doivent l'être dans leur emballage d'origine et dans un état propre. Les produits retournés autrement seront, à la seule discrétion de l'entreprise, refusés, ou des frais supplémentaires vous seront facturés pour couvrir les coûts additionnels. Les produits renvoyés à des fins de réparation dans le cadre de la garantie, doivent être accompagnés d'une copie de la facture originale, ou d'une feuille de papier libre contenant le numéro de facture originale ainsi que la date d'achat.

Si vous êtes un particulier, la présente garantie s'ajoute à vos droits légaux concernant les produits défectueux, ou ne correspondant pas à la description qui en est faite. Vous pouvez recueillir des conseils sur vos droits auprès de votre Bureau local de conseils aux citoyens, ou du Bureau des normes commerciales.

Les garanties présentées dans la présente clause s'appliquent uniquement à l'acheteur original d'un produit iStorage, ou au distributeur ou revendeur autorisé iStorage. Ces garanties sont non cessibles.

À L'EXCEPTION DE LA GARANTIE LIMITÉE EXPRIMÉE ICI, ET DANS LA MESURE MAXIMALE AUTORISÉE PAR LA LOI, ISTORAGE SE DÉGAGE DE TOUTES LES GARANTIES, EXPRESSES OU TACITES, Y COMPRIS TOUTES LES GARANTIES DE CONFORMITÉ ET D'USAGE NORMAL, NON INFRACTION. ISTORAGE NE GARANTIT PAS QUE LE PRODUIT FONCTIONNERA SANS ERREUR. DANS LA MESURE OU UNE GARANTIE POURRAIT TOUTEFOIS EXISTER PAR APPLICATION DE LA LOI, TOUTE GARANTIE DE CE TYPE EST LIMITÉE À LA DURÉE DE CETTE GARANTIE. LA RÉPARATION OU LE REMPLACEMENT DE CE PRODUIT, TEL QU'INDIQUÉ ICI, CONSTITUE VOTRE RECOURS EXCLUSIF.

EN AUCUN CAS ISTORAGE NE SERA TENU RESPONSABLE D'AUCUNE PERTE OU PROFIT ANTICIPÉ, NI AUCUN DOMMAGE FORTUIT, PUNITIF, EXEMPLAIRE, SPÉCIAL, DÉPENDANT OU AYANT LIEU EN CONSÉQUENCE, INCLUANT SANS POUR AUTANT S'Y LIMITER, LA PERTE DE REVENUS, LA PERTE DE PROFITS, LA PERTE DE L'UTILISATION DU LOGICIEL, LA PERTE DE DONNÉES, LES DOMMAGES AUX BIENS, ET LES RÉCLAMATIONS DE TIERS, DÉCOULANT DE TOUTE THÉORIE DE RÉCUPÉRATION, Y COMPRIS LA GARANTIE? CONTRACTUELLE, STATUTAIRE OU DÉLICTUELLE, QU'IL AIT ÉTÉ OU NON INFORMÉ DE LA POSSIBILITÉ QUE CES DOMMAGES SE PRODUISENT. NONOBSTANT LA DURÉE DE TOUTE GARANTIE LIMITÉE OU TOUTE GARANTIE IMPLIQUÉE PAR LA LOI, NI EN AUCUN CAS OU TOUTE GARANTIE LIMITÉE MANQUE À SATISFAIRE SON OBJECTIF ESSENTIEL, EN AUCUN CAS LA RESPONSABILITÉ TOTALE DE ISTORAGE N'EXCÈDERA LE PRIX D'ACHAT DE CE PRODUIT. | 4823-2548-5683.3

PARTIE B

41. Enregistrer et installer l'appli client cloudAshur

Enregistrement de cloudAshur

Téléchargez l'appli client cloudAshur Windows en cliquant sur le lien suivant :
https://istorage-uk.com/software-and-updates/

Important À lire : Pour enregistrer votre module de sécurité informatique cloudAshur, choisissez l'une des méthodes d'enregistrement suivantes qui vous concernent :

- **Personnel** - cloudAshur **NE DOIT PAS** être utilisé avec la **Remote Management** (logiciel de gestion centrale).
- **Enterprise** - cloudAshur utilisé conjointement à **Remote Management** (logiciel de gestion centrale).

Enregistrement personnel

Comme votre module de sécurité informatique cloudAshur ne sera pas utilisé avec Remote Management, vous n'aurez **PAS** besoin d'un code PIN, ni d'une Clé de licence pendant le processus d'enregistrement. Complétez simplement (**étape 3**) numéros de champs 1-6, laissez la case à cocher du numéro 7 non cochée, passez les champs numéros 8 et 9, puis cliquez sur 'Enregistrer' et commencez à utiliser cloudAshur.

Enregistrement de l'entreprise

Le module de sécurité informatique cloudAshur a été conçu pour être utilisé par des organismes qui gèreront et surveilleront de manière centrale tous les employés qui utilisent les modules cloudAshur émis par l'organisme, via l'utilisation de la **Console de gestion à distance** (logiciel de gestion centrale) cloudAshur.

Si vous êtes un employé et avez reçu un module cloudAshur de la part de l'Administrateur de votre organisme, un email '**Vous avez été invité**' vous sera envoyé de la part de votre administrateur. Il contiendra les données d'enregistrement importantes suivantes :

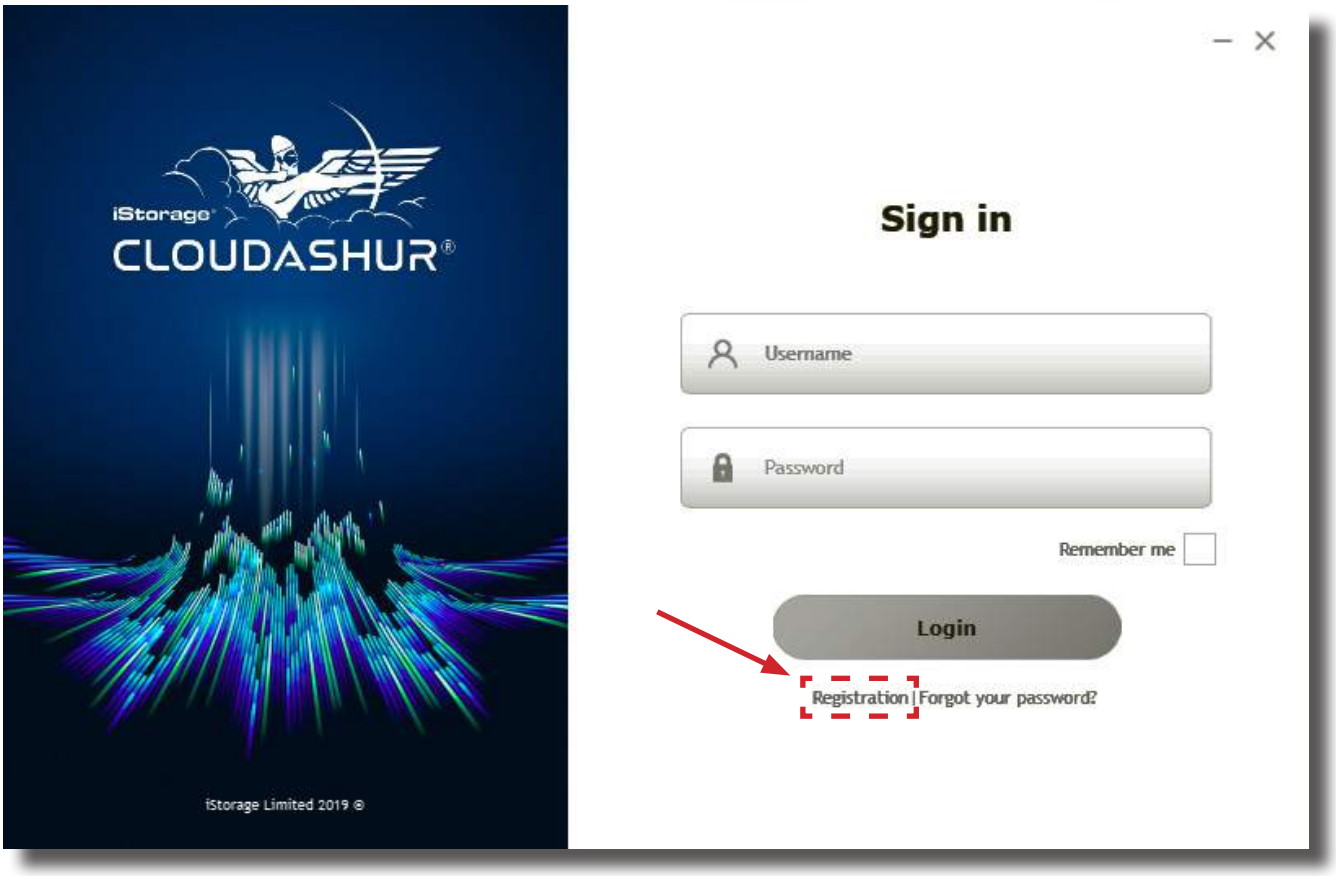
1. Un lien pour télécharger votre appli client cloudAshur Windows.
2. Un **code PIN** - il devra être saisi dans le champ n° 8 lors du processus d'enregistrement (**étape 3**).
3. Une **clé de licence** - qui devra également être saisie au champ n° 9 lors du processus d'enregistrement (**étape 3**).

Étape 01

Quand vous avez fini d'installer l'appli client Windows, téléchargez votre module de sécurité informatique cloudAshur avec votre code PIN administrateur ou votre code PIN utilisateur tel que décrit dans la **Partie A** de ce manuel. Une fois votre module de sécurité informatique cloudAshur déverrouillé (LED VERTE), connectez-le au port USB de votre ordinateur.

Étape 02

Ouvre votre appli client Windows (image 1) et cliquez sur '**Enregistrer**' pour enregistrer votre module de sécurité informatique cloudAshur.



(image 1)

Étape 03

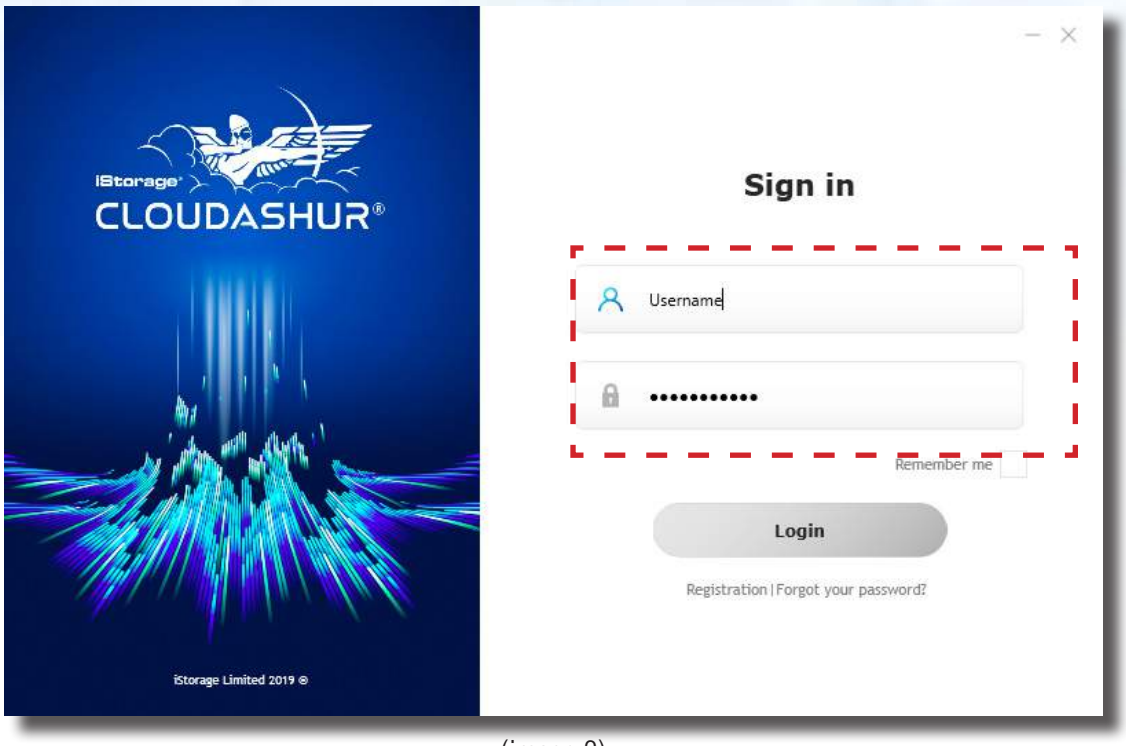
Pour « Enregistrer votre cloudAshur » (image 2) renseignez tous les champs de la partie '**Nouvel utilisateur**'.

(image 2)

1. Saisissez un '**Nom d'utilisateur**'.
2. Saisissez votre '**Prénom**' et votre '**Nom de famille**'.
3. Saisissez et confirmez votre '**Adresse email**'.
4. Saisissez et confirmez votre '**Mot de passe**' - votre mot de passe doit comporter au moins 8 caractères, et 3 de ces 4 éléments : lettre majuscule, lettre minuscule, numéro et caractère spécial.
5. Saisissez votre '**Numéro de téléphone**'.
6. Le '**Numéro du périphérique**' sera automatiquement détecté si votre module cloudAshur est déverrouillé et connecté à votre ordinateur (LED VERTE). Si le numéro du périphérique n'a pas été détecté, cliquez sur Rafraîchir pour le détecter.
7. Si votre module cloudAshur doit être **Enregistré en entreprise**, vous a été remis par l'Administrateur de votre organisme, veillez à bien cocher la case comme dans l'image 2 ci-dessus. Si votre cloudAshur doit être **Enregistré personnellement** ne cochez pas la case, sautez les étapes 8 et 9, et passez directement à l'étape 10.
8. Saisir le '**code PIN**' quevotre Administrateur vous a envoyé (**Enregistrement en entreprise uniquement**).
9. Saisissez la '**Clé de licence**' que votre Administrateur vous a envoyée (**Enregistrement en entreprise uniquement**)
10. Cliquez sur '**Enregistrer** ' pour achever le processus d'enregistrement.
11. Cliquez sur le bouton Suivant pour vous connecter (**étape 4**).

Étape 04

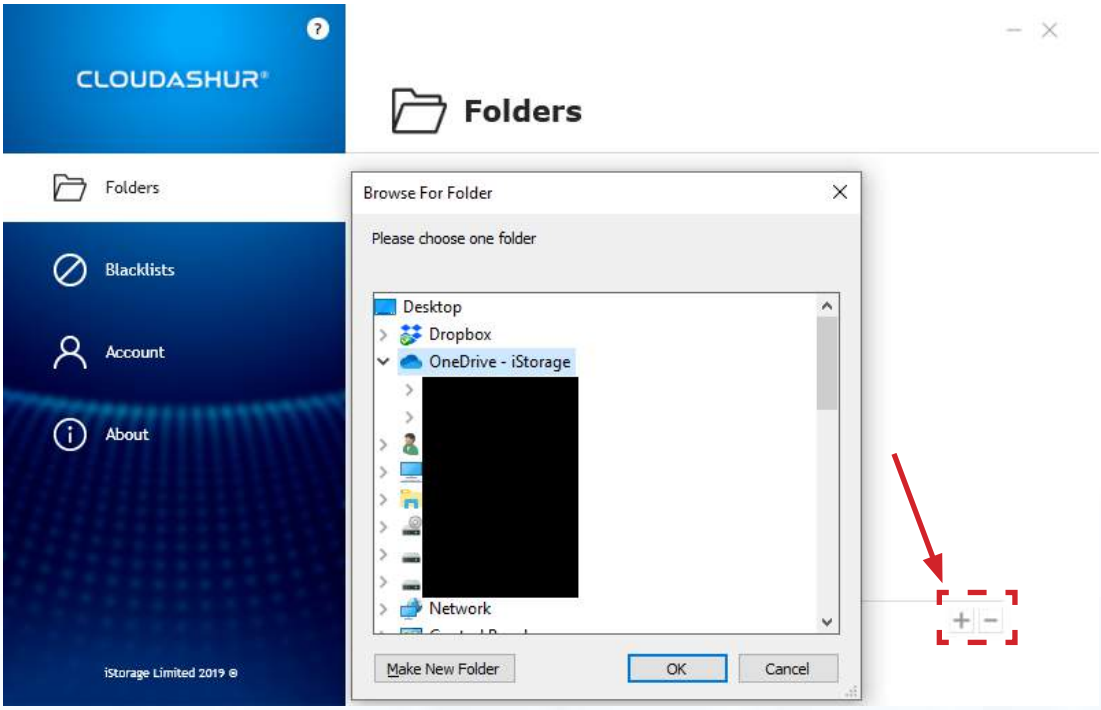
Saisissez votre '**Identifiant**' et '**Mot de passe**' créés à l'étape 3, puis cliquez sur '**Connexion**' comme à l'image 3 ci-dessous.



(image 3)

Étape 05

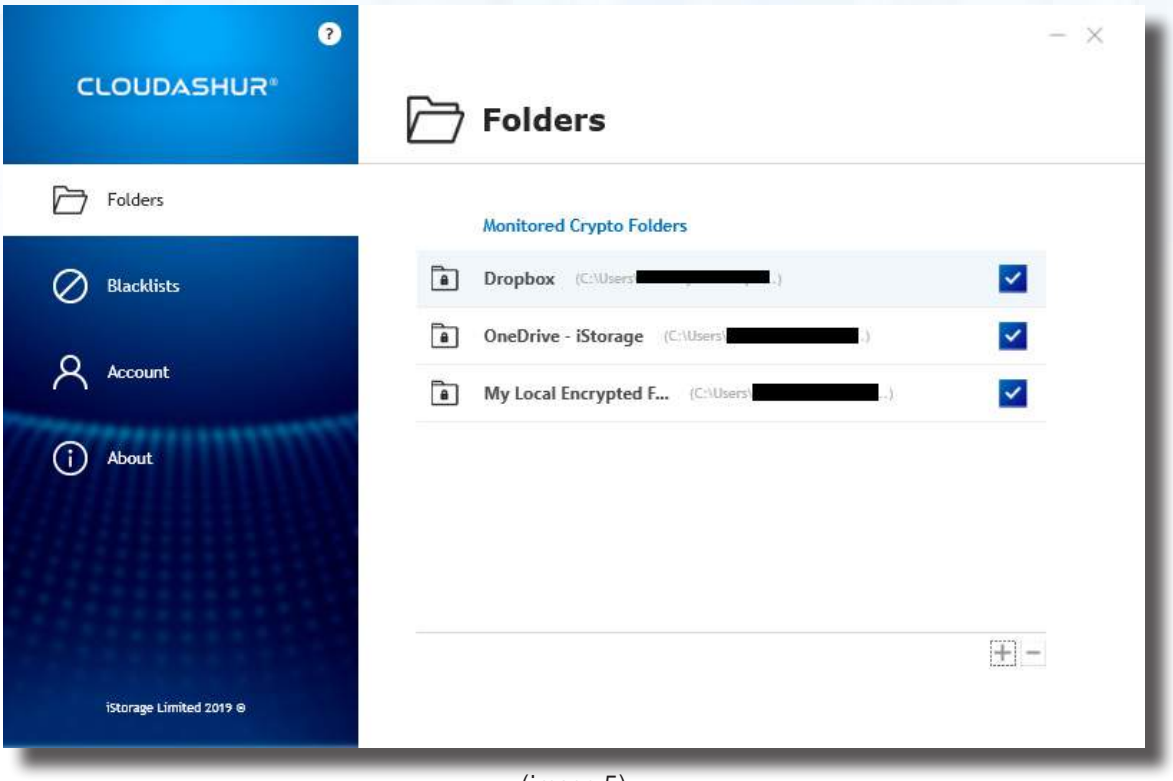
Une fois l'inscription terminée, votre clé virtuelle cloudAshur s'ouvre. Pour ajouter vos fichiers cloud et vos fichiers locaux à votre clé virtuelle cloudAshur, cliquez sur l'icone cloudAshur dans votre système (coin inférieur droit de votre écran) une fois pour ouvrir le menu Préférences, puis cliquez sur le '**+**' pour parcourir et sélectionner vos fichiers cloud et tout fichier local, comme illustré à l'image 4 ci-dessous.



(image 4)

Étape 06

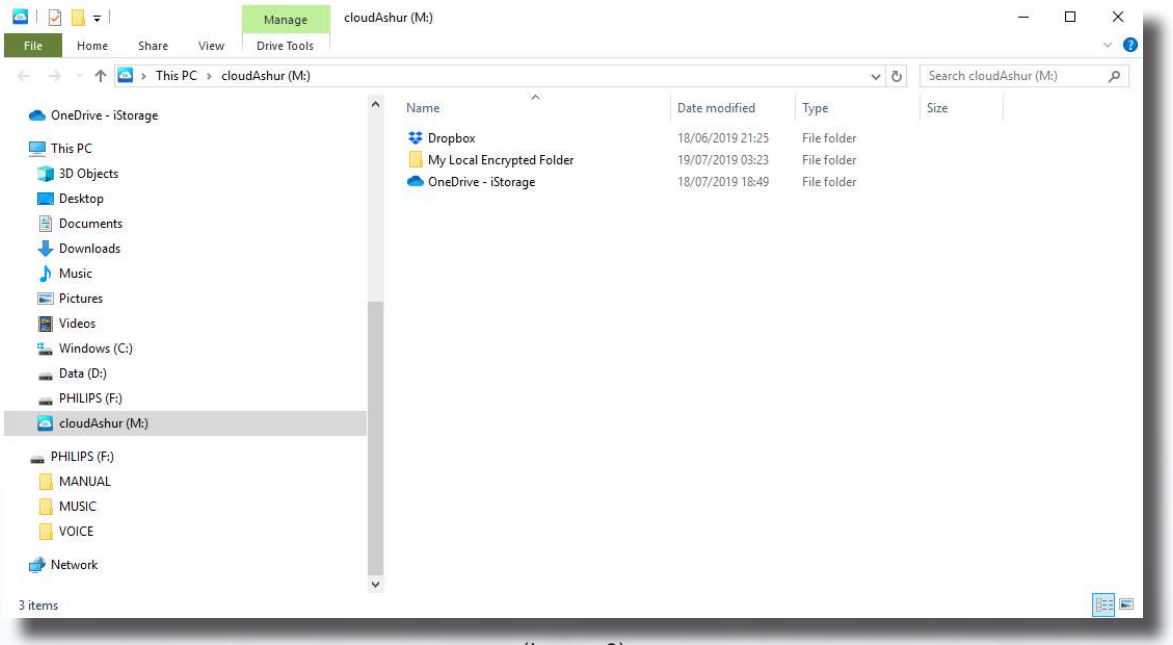
Après avoir ajouté vos comptes cloud et tout fichier local (tel qu'illustré à l'image 5), faites un double-clic sur l'icône cloudAshur sur votre système (coin inférieur droit de votre écran) pour ouvrir votre clé virtuelle cloudAshur (image 6).



(image 5)

Étape 07

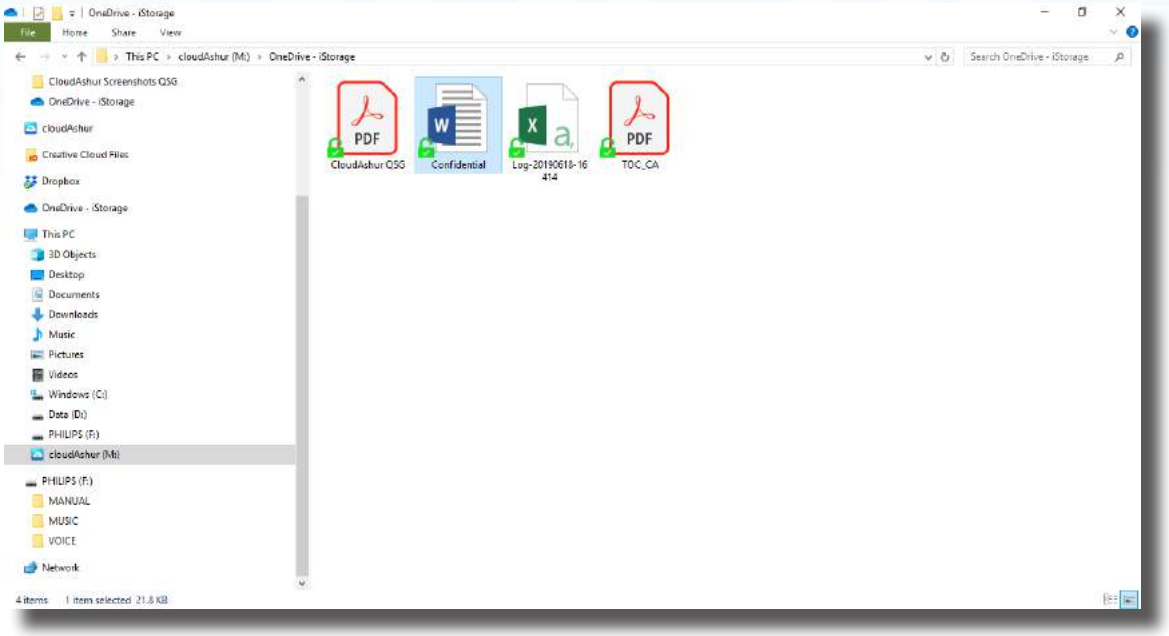
Dans votre clé virtuelle cloudAshur, cliquez sur votre fichier cloud/ local pour ouvrir, dans le cas présent, '**OneDrive - iStorage**' comme illustré à l'image 6.



(image 6)

Étape 08

Faites un glisser-déposer ou copier-coller vos fichiers sur votre clé virtuelle cloudAshur, et un cadenas ouvert vert apparaîtra sur le coin inférieur gauche de chaque fichier, tel qu'illustré à l'image 7. Ceci indique que les fichiers ont été codés mais que vous pouvez y accéder par le biais de votre clé virtuelle. Pendant ce temps, les mêmes fichiers sont codés lorsque vous y accédez directement depuis votre compte sur le cloud.



(image 7)

42. S'inscrire et installer l'appli client macOS cloudAshur

Enregistrement de cloudAshur

Veuillez télécharger l'appli client macOS cloudAshur en cliquant sur le lien suivant :
https://istorage-uk.com/software-and-updates/

Important À lire : Pour enregistrer votre module de sécurité informatique cloudAshur, merci de choisir l'une des deux méthodes d'enregistrement suivantes qui vous concerne :

- **Personnel** - cloudAshur **NE DOIT PAS** être utilisé avec la **Remote Management** (logiciel de gestion centrale).
- **Enterprise** - cloudAshur utilisé conjointement à **Remote Management** (logiciel de gestion centrale).

Enregistrement personnel

Comme votre module de sécurité informatique cloudAshur ne sera pas utilisé avec Remote Management, vous n'aurez **PAS** besoin d'un code PIN, ni d'une Clé de licence pendant le processus d'enregistrement. Complétez simplement (**étape 3**) numéros de champs 1-6, laissez la case à cocher du numéro 7 non cochée, passez les champs numéros 8 et 9, puis cliquez sur 'Enregistrer' et commencez à utiliser cloudAshur.

Enregistrement de l'enterprise

Le module de sécurité informatique cloudAshur a été conçu pour être utilisé par des organismes qui gèreront et surveilleront de manière centrale tous les employés qui utilisent les modules cloudAshur émis par l'organisme, via l'utilisation de la **Console de gestion à distance** (logiciel de gestion centrale) cloudAshur.

Si vous êtes un employé et avez reçu un module cloudAshur de la part de l'Administrateur de votre organisme, un email '**Vous avez été invité**' vous sera envoyé de la part de votre administrateur. Il contiendra les données d'enregistrement importantes suivantes :

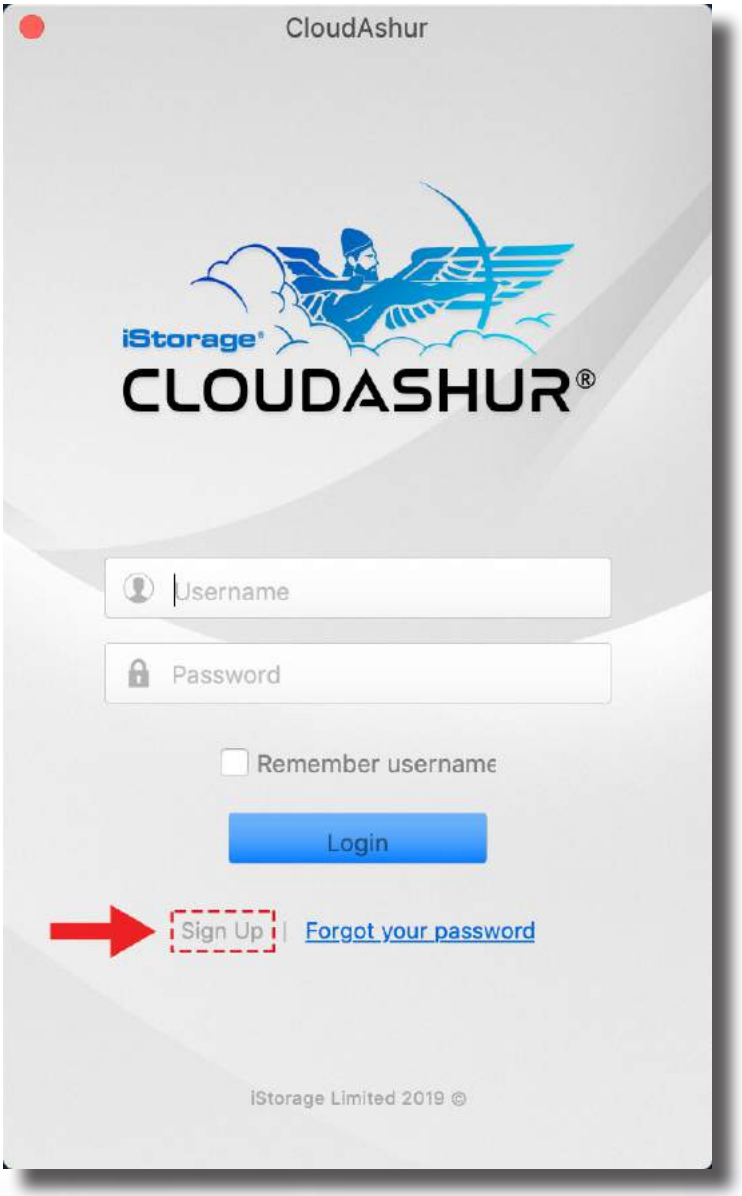
1. Un lien pour télécharger votre appli client macOS cloudAshur.
2. Un **code PIN** - il devra être saisi dans le champ n° 8 lors du processus d'enregistrement (**étape 3**).
3. Une **clé de licence** - qui devra également être saisie au champ n° 9 lors du processus d'enregistrement (**étape 3**).

Étape 01

Une fois l'installation de l'appli client macOS terminée, déverrouillez votre module de sécurité informatique cloudAshur avec votre code PIN administrateur ou votre code PIN utilisateur, tel qu'indiqué en **Partie A** de ce manuel. Avec votre module de sécurité informatique cloudAshur déverrouillé (LED VERTE), connectez-vous au port USB de votre ordinateur.

Étape 02

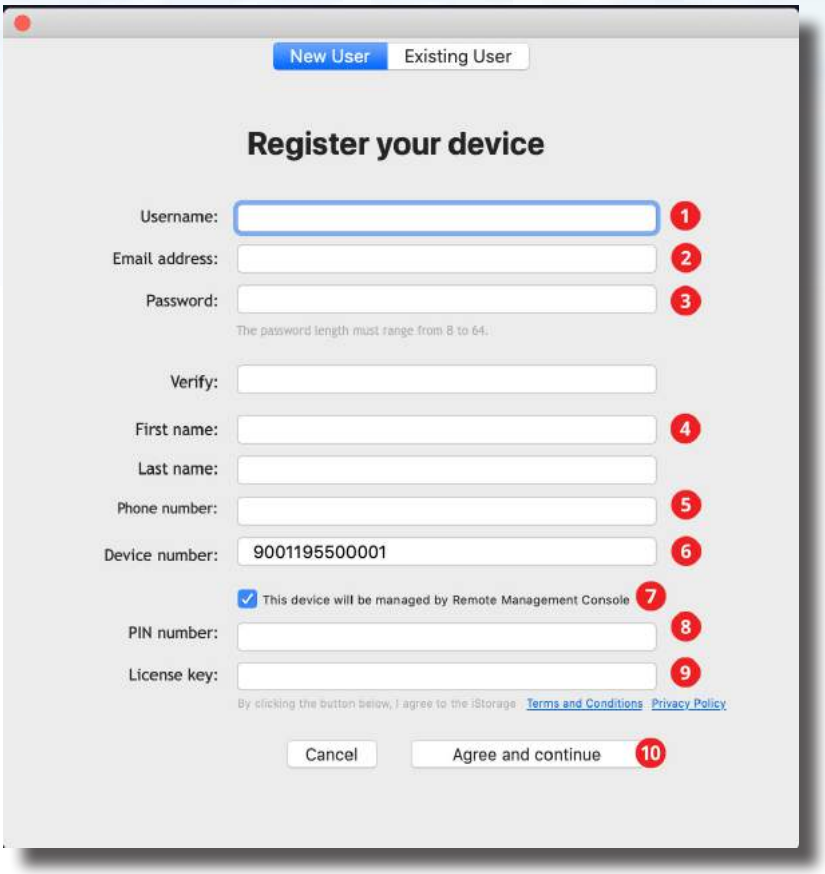
Ouvrez votre appli client macOS (image 1) et cliquez sur '**S'inscrire**' pour enregistrer votre module de sécurité informatique cloudAshur.



(image 1)

Étape 03

Pour « Enregistrer votre cloudAshur » (image 2) renseignez tous les champs de la partie '**Nouvel utilisateur**'.



(image 2)

1. Saisissez un '**Nom d'utilisateur**'.
2. Saisissez votre '**Adresse email**'.
3. Saisissez et vérifiez votre '**Mot de passe**' - votre mot de passe doit contenir au moins 8 caractères, dont 3 ou 4 des caractéristiques suivantes : lettre majuscule, lettre minuscule, chiffre et caractère spécial.
4. Saisissez votre '**Prénom**' et '**Nom de famille**'.
5. Saisissez votre '**Numéro de téléphone**'.
6. Le '**Numéro du périphérique**' sera automatiquement détecté si votre module cloudAshur est déverrouillé et connecté à votre ordinateur (LED VERTE).
7. Si votre module cloudAshur doit être **Enregistré en entreprise**, vous a été remis par l'Administrateur de votre organisme, veillez à bien cocher la case comme dans l'image 2 ci-dessus. Si votre cloudAshur doit être **Enregistré personnellement** ne cochez pas la case, sautez les étapes 8 et 9, et passez directement à l'étape 10.
8. Saisir le '**code PIN**' quevotre Administrateur vous a envoyé (**Enregistrement en entreprise uniquement**).
9. Saisissez la '**Clé de licence**' que votre Administrateur vous a envoyée (**Enregistrement en entreprise uniquement**)
10. Cliquez sur '**Enregistrer**' pour achever le processus d'enregistrement.

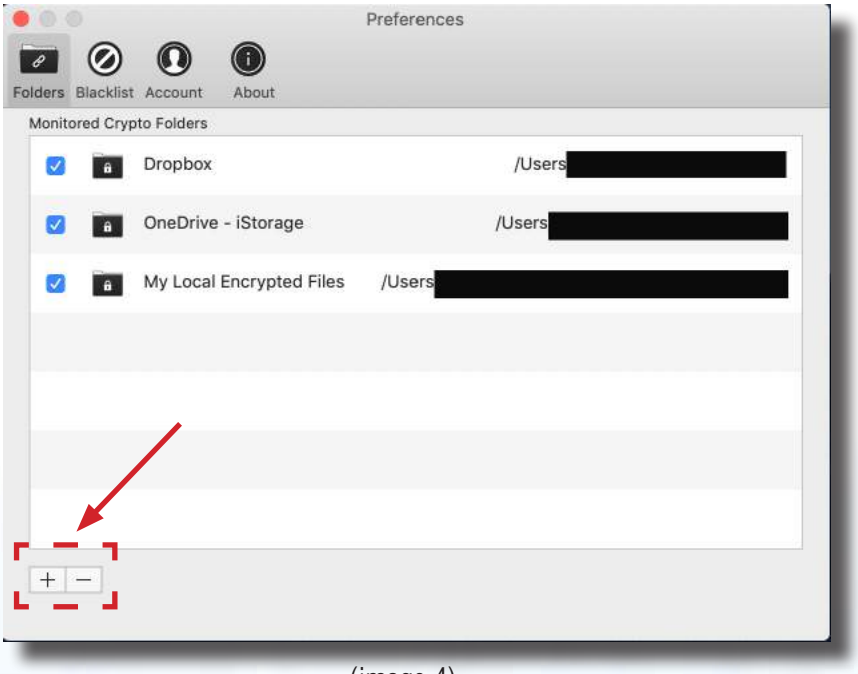
Étape 04

Saisissez votre '**Identifiant**' et '**Mot de passe**' créés à l'étape 3, puis cliquez sur '**Connexion**' comme à l'image 3 ci-dessous.

(image 3)

Étape 05

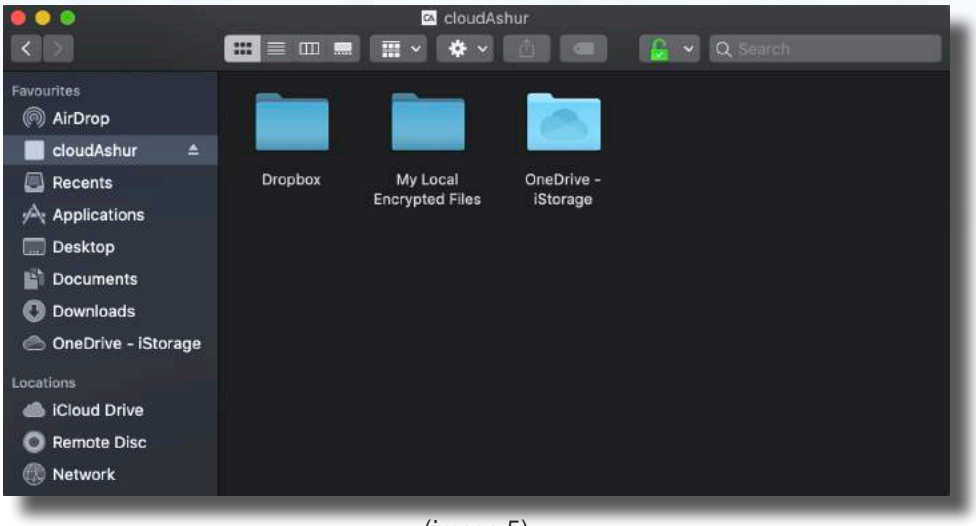
Une fois l'inscription terminée, votre clé virtuelle cloudAshur s'ouvre. Pour ajouter vos fichiers cloud et locaux à votre clé virtuelle cloudAshur, cliquez sur l'icône cloudAshur CA se trouvant dans votre **barre de menu** (en haut de votre écran), et cliquez sur les préférences, puis cliquez sur le '**+**' pour parcourir et sélectionner votre fichier cloud et tout fichier local, tel qu'illustré à l'image 4.



(image 4)

Étape 06

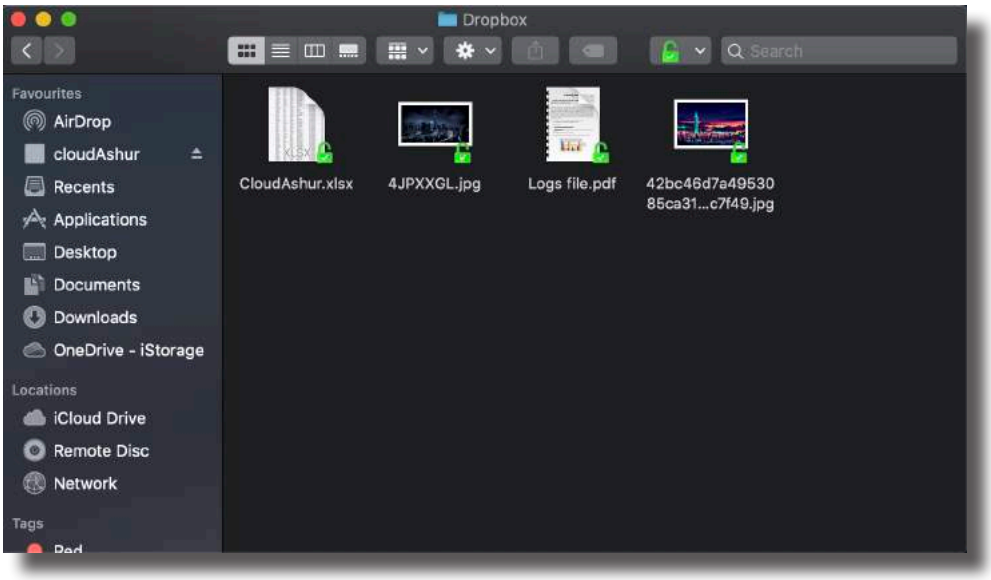
Après avoir ajouté vos comptes cloud et tout fichier cloud, cliquez sur l'icône CA cloudAshur depuis votre **barre de menu** (en haut de votre écran), puis cliquez sur votre clé virtuelle cloudAshur (image 5). Cliquez sur votre fichier cloud/local pour ouvrir, dans ce cas, la '**Dropbox**' tel qu'illustré ci-dessous.



(image 5)

Étape 07

Faites un glisser-déposer ou copier-coller pour vos fichiers jusque dans votre clé virtuelle cloudAshur, et un cadenas ouvert vert apparaîtra dans le coin inférieur droit de chaque fichier, tel qu'illustré à l'image 6. Ceci indique que les fichiers ont été codés mais que vous pouvez y accéder via votre clé virtuelle. Pendant ce temps, les mêmes fichiers sont codés lorsque vous y accédez directement depuis votre compte sur le cloud.



(image 6)

iStorage®

iStorage Limited, iStorage House, 13 Alperton Lane
Perivale, Middlesex. UB6 8DH, Angleterre
Tél. : +44 (0) 20 8991 6260 | Fax : +44 (0) 20 8991 6277
e-mail : info@istorage-uk.com | web : www.istorage-uk.com