CLOUDASHUR®

The key to your data™

ENCRYPT

to ensure the ultimate protection of your data stored in the cloud or on your local network drive, PC/MAC or any data storage device

SHARE

your encrypted data with authorised users in the cloud as well as on your local network drive, via email and file transfer services, in real-time

MANAGE

and monitor your cloudAshur devices centrally

To achieve data privacy, encryption of data is important, protection of the encryption key is vital. To be a truly secure solution, it is imperative that the encryption key is stored away from the data.

That is why we developed the cloudAshur Hardware Security Module (patent pending), a PIN authenticated hardware encrypted security module, that encrypts all data in transit and data at rest with a FIPS certified randomly generated AES 256-bit encrypted encryption key which is stored within an on-board Common Criteria EAL5+ (Hardware Certified) secure microprocessor.

Overview

cloudAshur is the perfect solution for anyone wanting to securely store, share, manage and monitor data in the cloud. cloudAshur eliminates the security vulnerabilities that exist with cloud platforms, such as lack of control and unauthorised access. Hackers are devising many sophisticated methods to target innocent and vulnerable users. Human error is also prevalent amongst data leakage incidents.

The consequences of a cloud account being hacked can bring about theft and leakage of confidential data, leading to potential job losses, adverse publicity, hefty fines and the downfall of a business.

iStorage software suite

cloudAshur Client app *(Windows & macOS)*

cloudAshur is compatible with both PCs and MACs and works with numerous cloud providers including Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud and many more.

cloudAshur KeyWriter app *(Windows)*

The iStorage Patented KeyWriter software makes sharing of encrypted data in the cloud as well as on your local network drive, via email and file transfer services (e.g. WeTransfer) between authorised users a breeze with ultimate security and peace of mind, allowing users to securely share data with one another, in real-time, regardless of their location.

cloudAshur Remote Management app *(Windows)*

iStorage cloudAshur Remote Management console gives you full control of all cloudAshur hardware security modules deployed within your organisation offering a wide range of features to manage and monitor all users.

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

iStorage®

CLOUDASHUR ENCRYPTION MODULE KEY FEATURES

PIN authenticated, hardware encrypted, cloud encryption module (patents pending)

Ultra-secure 7-15-digit PIN to authenticate the cloudAshur module

On-device Crypto-chip

Offering 100% real-time military grade AES-XTS or AES-ECB 256-bit Hardware Encryption with FIPS PUB 197 certified USB 3.0 encryption controller.

Brute force hack defence mechanism

If the User PIN is entered incorrectly 10 consecutive times, the User PIN will be deleted and the drive can only be accessed by entering the Admin PIN in order to reset the User PIN. (Admin can change this from the default 10 incorrect PIN entries, to 1-9, for the User only)

If the Admin PIN is entered incorrectly 10 consecutive times, all PINs and the encrypted encryption key will be lost forever.

Five factor authentication

Something you have:

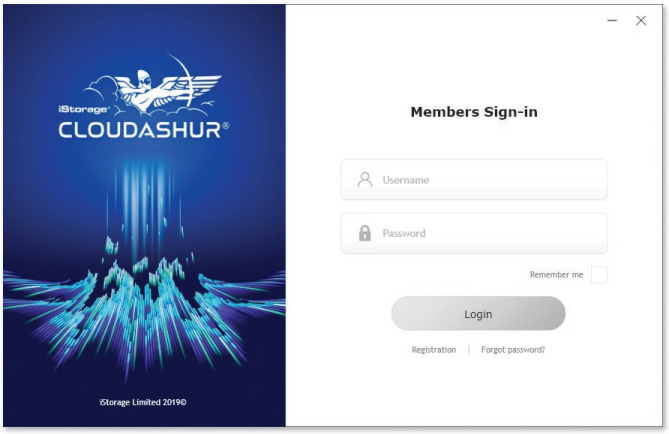
1. *The cloudAshur hardware security module.*

Something you know:

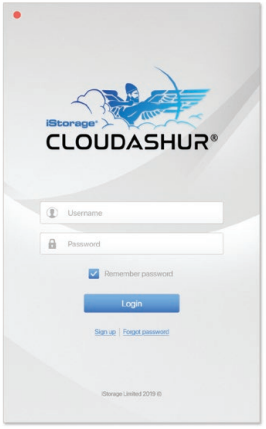
2. *7-15 digit Admin/User configurable PIN*
3. *Username and password for the iStorage cloudAshur Windows or macOS client app*
4. *Where the data is stored, which cloud provider*
5. *Username and password for the cloud account*

Compatible with Windows and macOS

cloudAshur client applications are Windows (7/8/10) and macOS (Sierra/High Sierra/Catalina) compatible.



(*Windows Client App*)



(*macOS Client App*)

Two encryption modes

The cloudAshur can be configured in two encryption modes AES-ECB 256-bit (FIPS Compliant) and AES-XTS 256-bit.

FIPS 140-2 Level 3 compliant tamper proof & evident design

All critical components within the cloudAshur enclosure are covered by a layer of super tough epoxy resin, which is virtually impossible to remove without causing permanent damage to the critical components.

If breached, the cloudAshur modules tamper evident design will provide visible evidence that tampering has occurred.

Incorporates a Common Criteria EAL5+ (Hardware Certified) secure microprocessor

Which offers ultimate security against hackers, detecting and responding to tampering with features such as:

- *Dedicated hardware for protection against SPA/DPA/ SEMA, DEMA attacks*
- *Advanced protection against physical attacks, including Active Shield, Enhance Protection Object, CStack checker, Slope Detector and Parity Errors*
- *Environmental Protection Systems protecting against voltage monitor, frequency monitor, temperature monitor and light protection*
- *Secure Memory Management/Access Protection*

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

iStorage®

CLOUDASHUR ENCRYPTION MODULE KEY FEATURES *(continued)*

Polymer coated, wear resistant on-board alphanumeric keypad

The cloudAshur is authenticated (unlocked) and all functions are performed using the onboard keypad with zero host involvement. cloudAshur is not vulnerable to key-loggers and brute force attacks.

The cloudAshur keypad is coated with a layer of wear resistant polymer for added protection.

Whitelisting on networks

Configured with a unique VID/PID and internal/external serial number with barcode, allowing easy integration into standard end-point management software (white-listing), to meet internal corporate requirements.

User PIN enrolment

The Admin can set a restriction policy for the user PIN. This includes setting the minimum length of the PIN, as well as requiring the input of one or more 'Special Character' if needed.

The 'Special Character' functions as 'SHIFT (⇧) + digit'

Inactivity Auto-lock

Configurable to lock after a predetermined period of inactivity. cloudAshur automatically locks when unplugged from the host computer or when there is no longer any power to the USB port.

Immune to Bad USB

Both the USB Cryptochip and Secure Microprocessor incorporate digitally-signed flash lock mechanisms making the cloudAshur immune to Bad USB.

Customisation services available

Offering an in-house PIN configuration and laser-etching service whereby the cloudAshur sleeve or side of the module can be customised with your name, company name and/or logo, web/email address, phone number.

IP68 certified

Dust and water resistant. Includes hard anodized and ruggedised extruded aluminium protective sleeve.

Separate Admin and User modes

Supports independent Admin and User PINs.

Self-destruct feature

Pre-program the cloudAshur with a self-destruct PIN, which once entered, the encrypted encryption key and all PINs are deleted.

One-time User recovery PIN

The Admin can program the cloudAshur with a one-time recovery PIN. This is extremely useful in situations where a User has forgotten the PIN to authenticate the cloudAshur.

This feature allows the User to enter the Recovery PIN and configure a new User PIN.

LED lights

RED - standby state / locked
GREEN - user mode / unlocked
BLUE - admin mode

Polymer coated, wear resistant, alphanumeric keypad

Hard anodized and ruggedised extruded aluminium housing

SHIFT key / ON-OFF button

Rubber gasket

Making the module waterproof when sleeve is fitted

Incorporates Common Criteria EAL4+ ready secure microprocessor

Offers ultimate security against hackers, detecting and responding to tampering

Epoxy coated

All critical components inside the cloudAshur are covered by a layer of super tough epoxy resin

Key button

Zinc alloy

(can be attached to keyring)

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

ISTORAGE PATENTED KEYWRITER SOFTWARE

Makes sharing of data in the cloud, on your local network drive, via email and file transfer services between authorised users a breeze with ultimate security and peace of mind!

KEYWRITER FEATURES

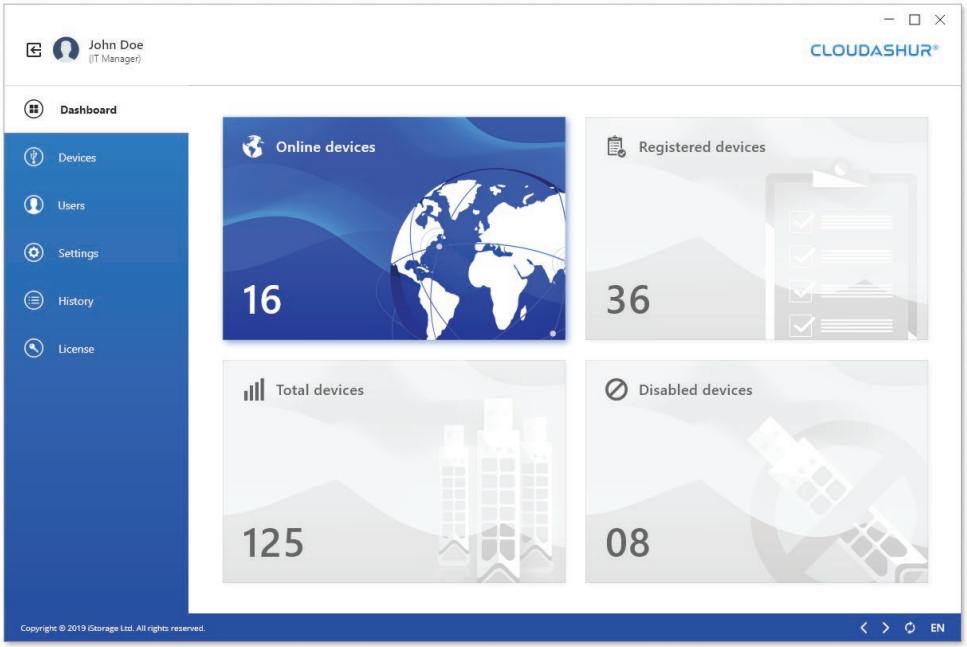
- *iStorage KeyWriter copies all critical security parameters including the randomly generated encryption key and all PINs between the Master cloudAshur module and as many secondary cloudAshur modules as required using any off the shelf USB hub, allowing authorised users to securely share data with one another, in real-time, regardless of their location.*
- *The critical security parameters never leave the cloudAshur module and are stored in the Common Criteria EAL4+ ready secure microprocessor.*
- *The process of copying the encrypted encryption key and all critical credentials between the Master cloudAshur module and the secondary cloudAshur modules is protected by a secure protocol incorporated within the iStorage cloudAshur secure microcontroller. The protocol is implemented using cryptographic algorithms, all of which are FIPS certified. Every cloudAshur has a unique certificate issued by a root of trust, which ensures that only iStorage cloudAshur modules can be used during the key exchange process.*
- *The cloudAshur modules never output the established session key when running the secure protocol and the sensitive data being copied is only decrypted in the validated recipient cloudAshur module. The iStorage KeyWriter software running on the PC coordinates the operations required by the secure protocol, however the software has zero visibility of both the session key and decrypted data, making it impossible for a hacker to access or retrieve any critical security parameters stored within the cloudAshur module.*

iStorage KeyWriter is compatible with Windows (*Vista/7/8/10*).

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

CLOUDASHUR REMOTE MANAGEMENT CONSOLE

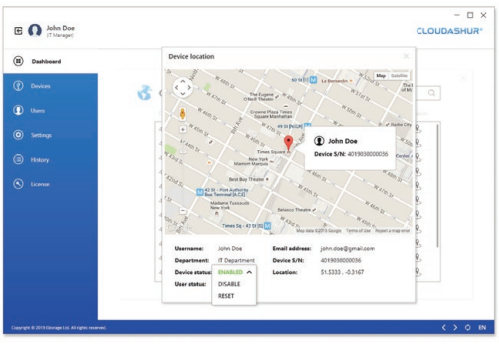
Gives you full control of all cloudAshur hardware security modules deployed within your organisation offering a wide range of features to manage all users.



CONSOLE FEATURES

iStorage Remote Management Console provides the Administrator full visibility and control over the following:

- *Temporarily disable or reset (remote kill) Users cloudAshur modules - in the event of suspicious activity or an employee leaving the organisation without returning their cloudAshur encryption module.*
- *Restrict file types – control what file types are being uploaded and shared in the cloud (EXE, PNG, PDF, etc...)*
- *View User's log files – full visibility over what each User is doing in the cloud, such as, what files they are uploading, downloading, modifying, etc...*
- *Display User's location – You can view the location of User's cloudAshur modules via an on-screen map.*
- *Geofencing and Time fencing - restrict the time and location of where and when the cloudAshur encryption module can be used by each individual User.*



iStorage Remote Management Console is compatible with Windows (*Vista/7/8/10*).

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

WHY USE CLOUDASHUR?

- *You hold the encryption key to your data in the securest way possible - you no longer need to worry about whether your data in the cloud is being viewed, stolen and shared.*
- *Five Factor Authentication - making it virtually impossible to hack your data.*
- *GDPR Compliance – The terms and conditions of major cloud providers includes a "Limitations of Liability" clause which puts data security responsibility on the cloud user/customer, even though the data is stored on their servers. For example, AWS states in their T&Cs that they accept no liability whatsoever if there is "Any unauthorized access to, alteration of, or the deletion, destruction, damage, loss or failure to store any of your content or other data." cloudAshur gives you ultimate protection, if a hacker gains access to your cloud account, they won't be able to decrypt your data.*
- *If a hacker manages to get hold of your cloud login credentials using "phishing" or other advanced hacking methods, they won't be able to decrypt your data.*
- *Human error no longer becomes an issue.*
- *Protection against Administrative personnel working for cloud providers who have the capability to access your data as they control the encryption keys.*
- *Protection against data privacy concerns. Tens of thousands of requests for user data are sent to Google, Microsoft, and other businesses each year by government agencies. A large percentage of the time, these companies hand over at least some kind of data, even if it's not the content in full...*

Technical specifications

Hardware	Hardware Security Module (patent pending)
Interface	FIPS PUB 197 certified USB 3.0 encryption controller
Battery	3.7V Li-Polymer rechargeable battery
Dimension - H/W/D	87.40mm / 19.40 mm / 13.40mm
Weight	Without sleeve: approx. 28 grams With sleeve: approx. 37 grams
Compatibility	cloudAshur is compatible with both Windows (7/8/10) and macOS (Sierra/High Sierra/Mojave/ Catalina) and works with numerous cloud providers including Amazon Drive, Google Drive, OneDrive, Dropbox, iCloud and many more.
Hardware data encryption	Can be configured in two encryption modes AES-ECB 256-bit (FIPS Compliant) and AES-XTS 256-bit.
Certifications	FIPS 140-2 Level 3, NLNCSA BSPA & NATO Restricted Level (Pending Q4)
Approvals	
Ordering information	IS-EM-CA-256
Warranty	3 year warranty with free lifetime technical support

GDPR Compliant

Designed and Developed in the UK
Assembled in China

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