CLOUDASHUR® KEY WRITER

iStorage®

CLOUDASHUR®

KEY WRITER

User Manual

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

www.istorage-uk.com

Version 1.2

Introduction

cloudAshur KeyWriter (*patent pending*) makes sharing of data in the cloud, 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.

Key features

cloudAshur KeyWriter clones all critical security parameters including the randomly generated encryption key, all PINs and administrator defined configurations between the Master cloudAshur hardware security module and as many secondary cloudAshur hardware security modules as required using any off the shelf USB hub (we recommend using a 10 port 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 hardware security module and are stored in the Common Criteria EAL4+ ready secure microprocessor.

The process of cloning the encrypted encryption key and all critical credentials between the Master cloudAshur hardware security module and the Secondary cloudAshur hardware security 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 hardware security modules can be used during the key exchange process.

The cloudAshur hardware security 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 hardware security 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 hardware security module.

cloudAshur links

The following complete and detailed user manuals can be found by clicking the link below:

- cloudAshur Hardware Security Module complete and detailed user manual
- cloudAshur Remote Management user manual

https://istorage-uk.com/product-documentation/

Table of Contents

1. Activating and Installing cloudAshur KeyWriter

Please note: If you purchased your cloudAshur Remote Management software directly from iStorage, follow the instructions contained in the email from iStorage, then skip '*section 1*' and proceed to '*section 2: Registration and Login*'.

1. After purchasing your cloudAshur KeyWriter software, you will receive an email containing your **License number** and **PIN number**, complete the fields (*Image 1: License Activation*) and then click the '**Activate**' button.

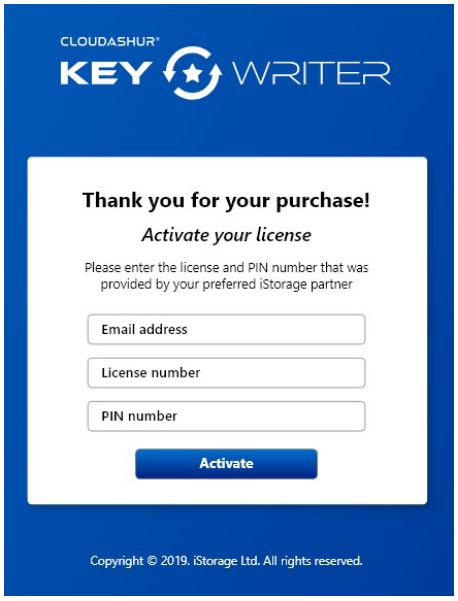

Image 1: - License Activation

2. You will receive a notice of a verification email sent from iStorage (*Image 2: Verification email*). Please click on the link provided in the email, and follow the instructions to complete the activation process.

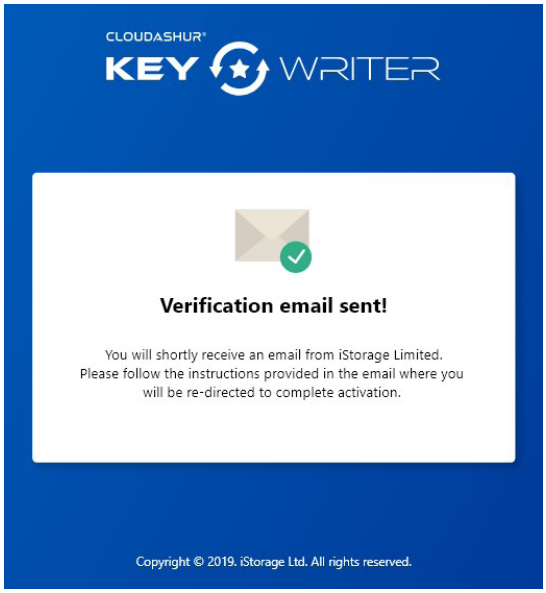

Image 2: - Verification email

3. Complete all the fields (*Image 3: - Complete your activation*) and then click '**Confirm**'.

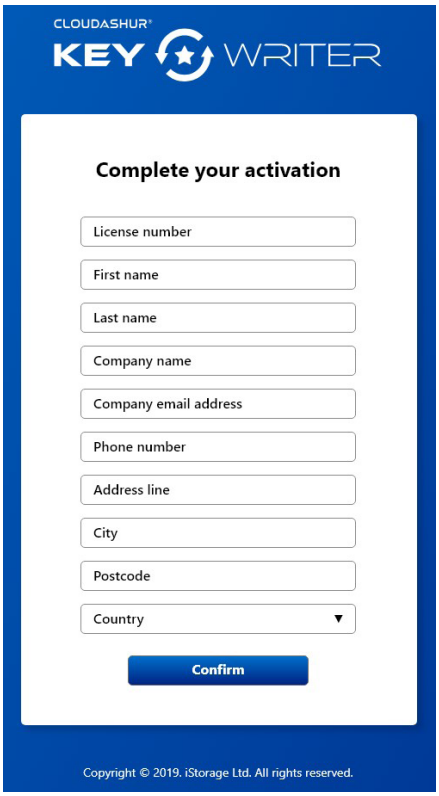

Image 3: - Complete your activation

4. Follow the steps (*Image 4: Activation successful*) and click on the '**Download**' button to install the KeyWriter app. Next, authenticate (*7-15 digit PIN*) your cloudAshur hardware security module and connect to your computer. Finally, register and login to your cloudAshur KeyWriter app using the information received as in '*Image 4*' to get started.

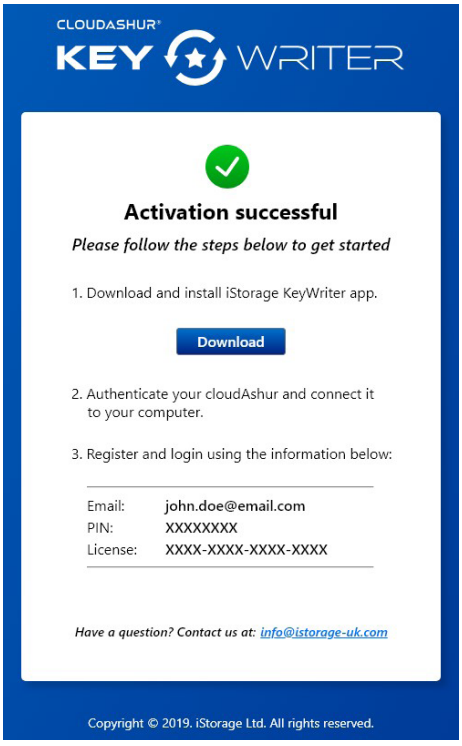

Image 4: - Activation successful

2. Registration

1. Open your cloudAshur KeyWriter app (*Image 5: Registration*) and click on the '**Register**' tab. If you don't have a license, click on the '**Don't have a license?**' link and follow the instructions to purchase your KeyWriter license.

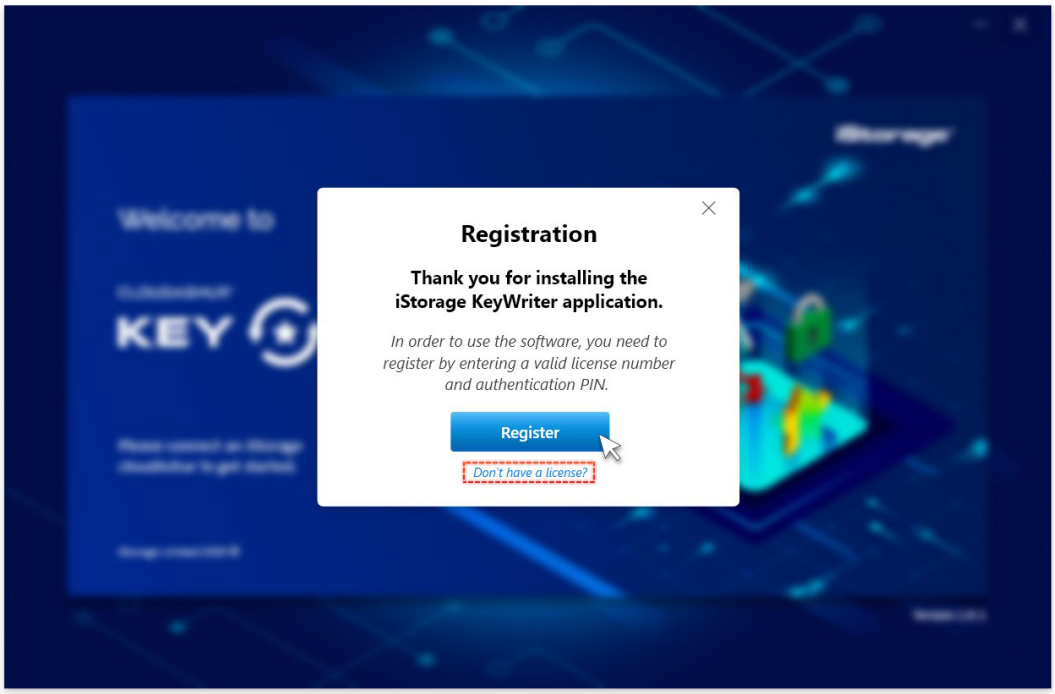

Image 5: - Register

2. Enter your **License number** and **PIN number** precisely as received (*Image 4: Activation successful*) and then click '**Next**' to continue (*Image 6: Registration*).

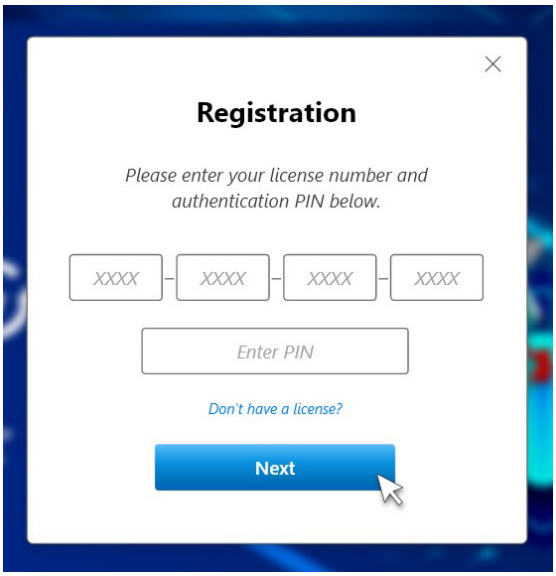

Image 6: - Registration

3. Click **Continue** (*Image 7: Registration successful*) and the KeyWriter app will launch and is ready for use.

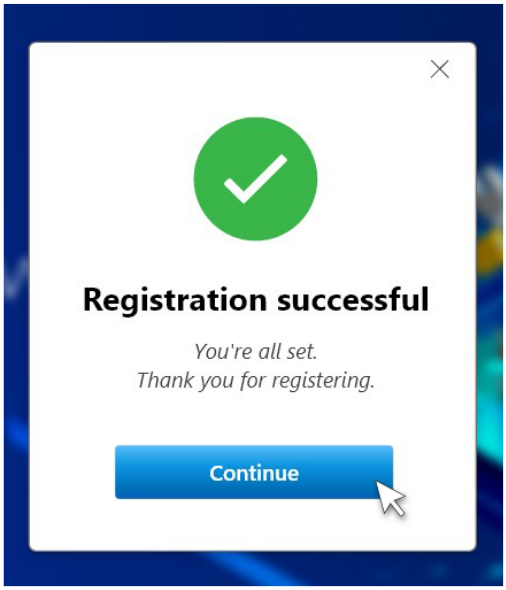

Image 7: - Registration successful

3. Setting your cloudAshur Master Device

Important!

Before cloning: As you will be cloning all security parameters from one cloudAshur hardware security module (*Master device*) to any number of secondary cloudAshur hardware security modules, it is important to ensure the 'Master device' has been pre-configured by the administrator to include as many of the following:

1. **Setting a User PIN Policy**
2. **Adding a User PIN**
3. **Setting your cloudAshur hardware security module to enable KeyWriter cloning**
4. **Configuring the cloudAshur hardware security module Encryption Mode - AES-XTS (*default*) or AES-ECB**
5. **Configuring a Self-Destruct PIN**
6. **Setting the unattended Auto-Lock**

If your cloudAshur hardware security module has been disabled from cloning, refer to section 19 of the cloudAshur Hardware Security Module user manual for complete and detailed instructions of all configurations.

Setting the Master Device

Please note: You will be required to enter your KeyWriter app **PIN** each time you launch the cloudAshur KeyWriter app. This is the **PIN** that was sent in an email to you together with the license number. The KeyWriter app **PIN** can be changed see section 5: '**Change your KeyWriter PIN**'. In addition, ensure your 'Master device' is unlocked and connected to your computer before setting the master device.

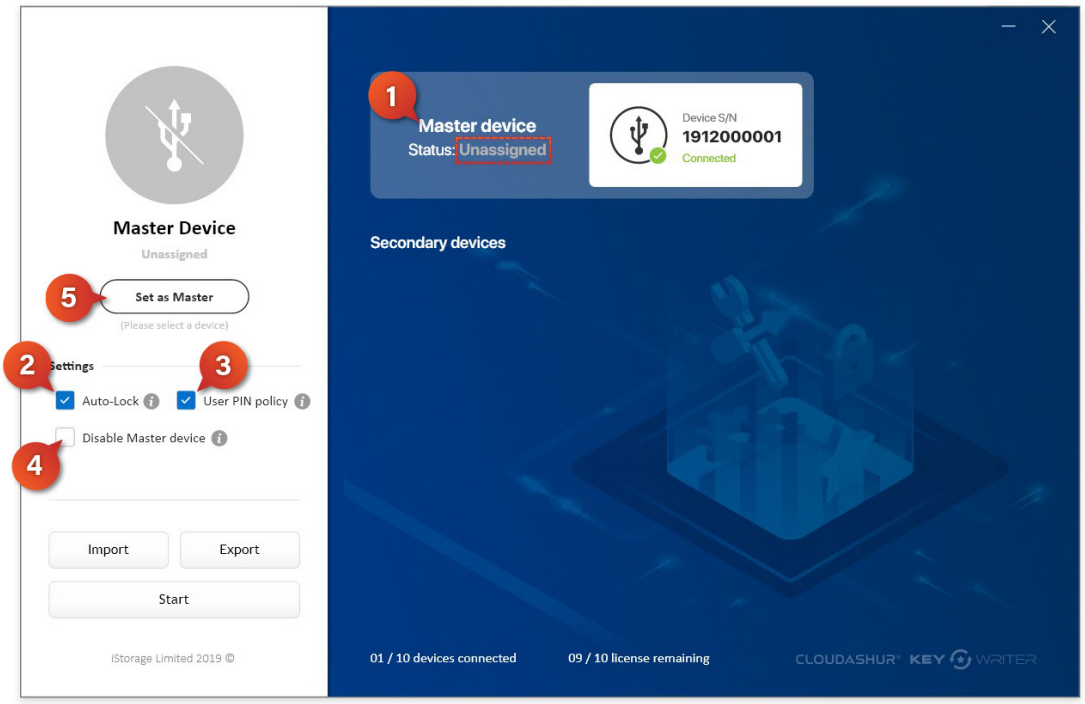

Image 8: - Setting the Master Device

1. **Master Device -** (*Image 8: Setting the Master Device*) when you connect your Master cloudAshur hardware security module to the KeyWriter for the first time, the cloudAshur hardware security module will show as 'Master device - Status '**Unassigned**' together with the device serial number.

2. **Auto-Lock -** checking this box will copy the '*Auto-Lock*' setting, if one has been configured, from the master cloudAshur device to the secondary cloudAshur device. Please refer to the user manual for further information about the '*Auto-Lock*' feature.User Name.

3. **User PIN Policy -** checking this box will copy the '*User PIN Policy*' setting, if one has been configured, from the master cloudAshur device to the secondary cloudAshur device. Please refer to the user manual for further information about the '*User PIN Policy*' feature.

4. **Disable Master Device -** checking this box will disable the cloning feature of the Master cloudAshur device once a cycle of the cloning process has successfully completed. If you intend to continue to clone from the Master device to additional secondary devices, leave the checkbox unchecked.

5. Once you are happy with your settings (*steps 2-4 above*), click the '**Set as Master**' button. Your Master cloudAshur status will now show up as '**Active**' as seen below in '*Image 9: Master Device Active*'.

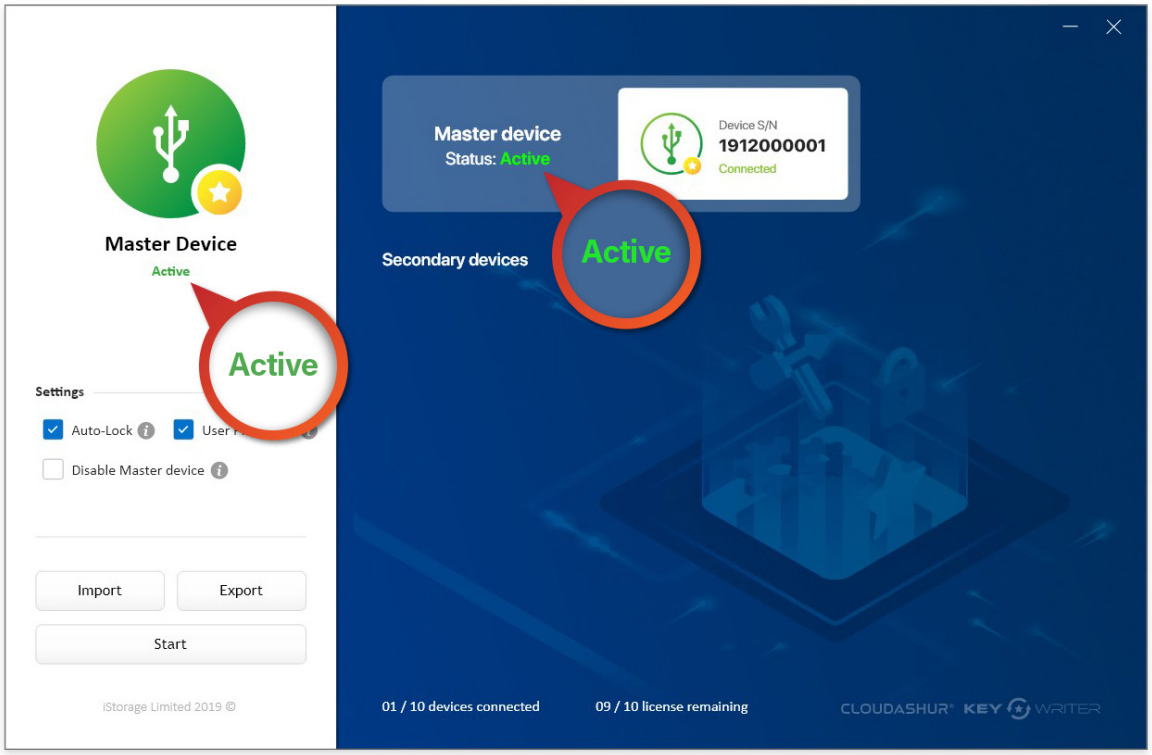

Image 9: - Master Device Active

4. Cloning from Master Device to Secondary Devices

Start Cloning

With your cloudAshur Master device active, insert up to 9 cloudAshur '**Secondary devices**' (*on a 10 port USB hub*) and proceed as follows, see below '*Image 10: Cloning Secondary devices*'.

1. Click the '**Start**' button. Every secondary device will be cloned one at a time until cloning of all devices is complete. The cloudAshur hardware security modules are now ready for use see '*Image 11: Device cloned*'.
2. To save your settings (*Auto-Lock and User PIN Policy*) locally on your computer, click '**Export**' and save.
3. The next time you need to clone more secondary devices and wish to import your '*saved*' settings, click on the '**Import**' button and navigate to where you saved your settings - see step 2.

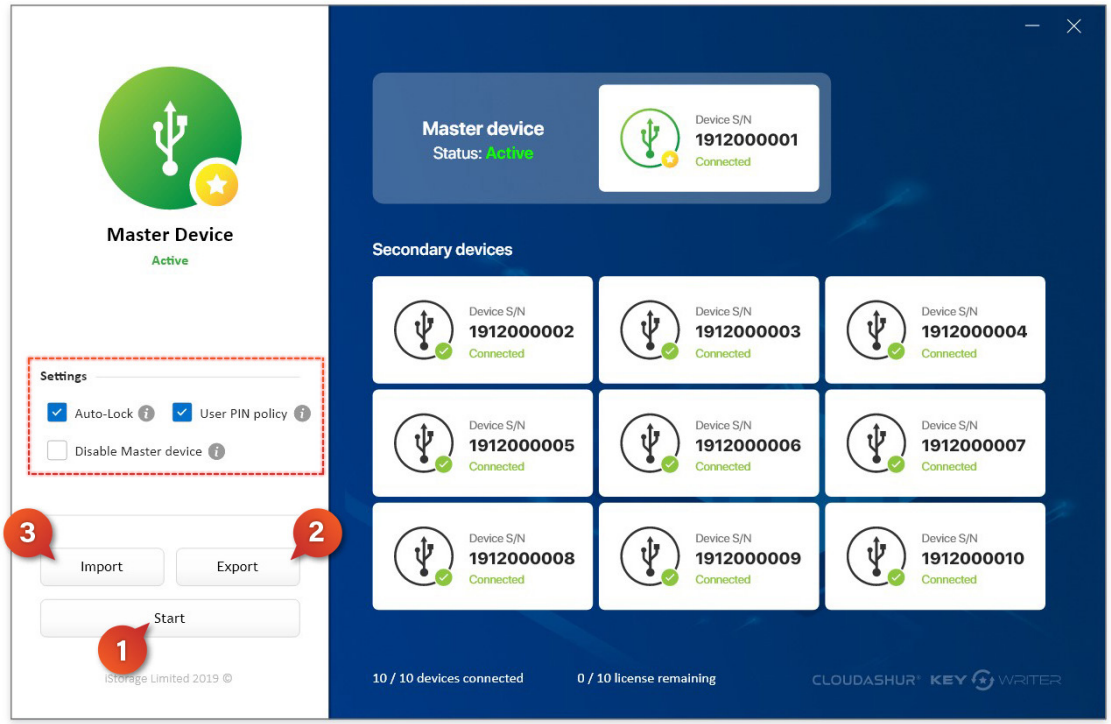

Image 10: - Cloning Secondary devices

Cloning Complete

Once cloning is complete, all cloudAshur secondary devices that have been successfully cloned will appear with a checkmark as 'Device cloned '*see Image 11: Cloning complete*'.

Please note: The Administrator can use any of the cloned (*secondary*) cloudAshur hardware security modules and set as a '**Master Device**', please refer to the cloudAshur hardware security module user manual to first ensure that your secondary device is enabled to allow cloning.

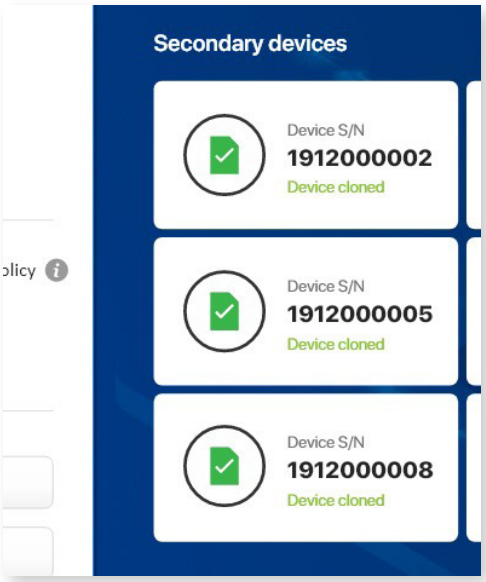

Image 11: - Cloning complete

5. Change your KeyWriter PIN

To change your KeyWriter PIN, click on '**Change PIN**' as seen on '*Image 12: Change PIN*'.

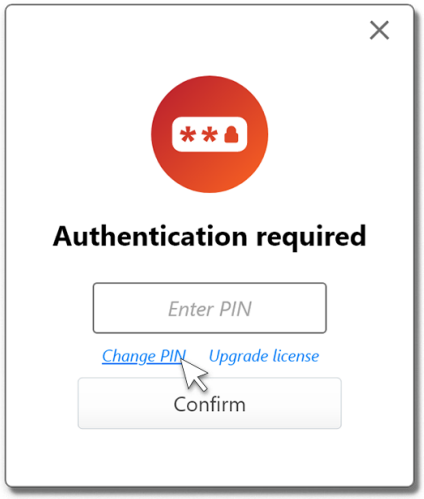

Image 12: - Change PIN

To change your PIN, enter your *current PIN*, next enter your *new PIN*, then *confirm new PIN* and finally click the '**Change PIN**' button and your new KeyWriter PIN will change and become active the next time you open your cloudAshur KeyWriter app.

Please note: The 'Change KeyWriter PIN' screen (*Image 13: PIN Changed*) will automatically detect your License number and the text input fields can be set to show or hide the PIN characters.

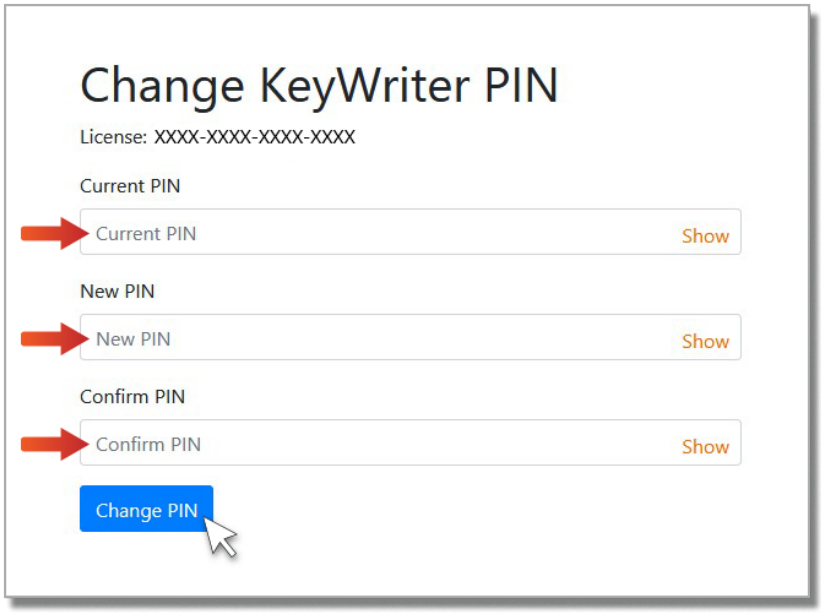

Image 13: - PIN changed

iStorage®

CLOUDASHUR®

KEY WRITER

User Manual - Version 1.2

www.istorage-uk.com | info@istorage-uk.com | +44 (0) 20 8991 6260

iStorage®

CLOUDASHUR®

KEY WRITER

Benutzerhandbuch

Wenn Sie Probleme mit der cloudAshur Remote Management Console haben, wenden Sie sich bitte per E-Mail oder telefonisch an unsere Technische Support-Abteilung: support@istorage-uk.com oder +44 (0) 20 8991 6260.

www.istorage-uk.com

Version 1.2

Einführung

cloudAshur KeyWriter (*Patent ausstehend*) macht die gemeinsame Nutzung von Daten in der Cloud per E-Mail und über Datenübertragungsdienste (*z. B. WeTransfer*) zwischen autorisierten Benutzern einfach möglich und sorgt für ultimative Sicherheit und Gelassenheit. Benutzer können so Daten unabhängig von ihrem Standort sicher und in Echtzeit gemeinsam nutzen.

Hauptfunktionen

iStorage KeyWriter klont unter Verwendung eines handelsüblichen USB-Hubs (wir empfehlen die Verwendung eines 10-Port-USB-Hubs) alle kritischen Sicherheitsparameter einschließlich des zufällig erzeugten Verschlüsselungsschlüssels, alle PINS und vom Administrator definierten Konfigurationen zwischen dem Master-cloud-Ashur-Hardwaremodul und so vielen sekundären cloudAshur-Modulen wie benötigt. Autorisierte Benutzer können damit Daten in Echtzeit und unabhängig von ihrem Standort gemeinsam nutzen.

Die kritischen Sicherheitsparameter verlassen zu keiner Zeit das cloudAshur-Hardwaresicherheitsmodul und werden im sicheren, Common-Criteria-EAL4+-fähigen Mikroprozessor gespeichert.

Das Klonen des verschlüsselten Verschlüsselungsschlüssels und aller kritischen Anmeldedaten vom cloudAshur-Hardwaresicherheitsmodul auf die sekundären cloudAshur-Hardwaresicherheitsmodule ist durch ein sicheres Protokoll geschützt, das in den sicheren iStorage-cloudAshur-Microcontroller integriert ist. Das Protokoll ist mithilfe FIPS-zertifizierter kryptografischer Algorithmen integriert. Jedes cloudAshur verfügt über ein eindeutiges Zertifikat, das von einem Vertrauensanker ausgestellt wurde und sicherstellt, dass während des Schlüsselaustauschprozesses ausschließlich iStorage-cloudAshur-Hardwaresicherheitsmodule verwendet werden können.

Der erstellte Sitzungsschlüssel wird von den cloudAshur-Hardwaresicherheitsmodulen beim Ausführen des sicheren Protokolls niemals ausgegeben. Die kopierten sensiblen Daten werden ausschließlich im validierten cloudAshur-Hardwaresicherheitsmodul entschlüsselt. Die auf dem PC ausgeführte iStorage-KeyWriter-Software koordiniert die aufgrund des sicheren Protokolls erforderlichen Abläufe. Jedoch sind weder der Sitzungsschlüssel noch die entschlüsselten Daten in der Software sichtbar, wodurch es für Hacker unmöglich ist, auf im cloudAshur-Hardwaresicherheitsmodul gespeicherte Sicherheitsparameter zuzugreifen oder diese abzurufen.

cloudAshur-Links

Die folgenden vollständigen und detaillierten Bedienungsanleitungen finden Sie, indem Sie auf den folgenden Link klicken:

- Vollständiges und detailliertes Benutzerhandbuch für das cloudAshur-Hardware-Sicherheitsmodul
- cloudAshur Remote Management Benutzerhandbuch

https://istorage-uk.com/product-documentation/

Inhaltsverzeichnis

1. CloudAshur KeyWriter aktivieren und installieren

Zu beachten: Wenn Sie Ihre cloudAshur-Remote-Management-Software direkt bei iStorage gekauft haben, befolgen Sie die Anweisungen in der E-Mail von iStorage und überspringen Sie*Abschnitt 1*. Gehen Sie weiter zu "*Abschnitt 2: Registrierung und Login*".

1. Nach dem Kauf Ihrer cloudAshur-KeyWriter-Software erhalten Sie eine E-Mail mit Ihrer **Lizenznummer** und der **PIN Nummer**, füllen Sie die Felder aus (*Bild 1: Lizenzaktivierung*) und klicken Sie dann auf die Schaltfläche "**Aktivieren**".

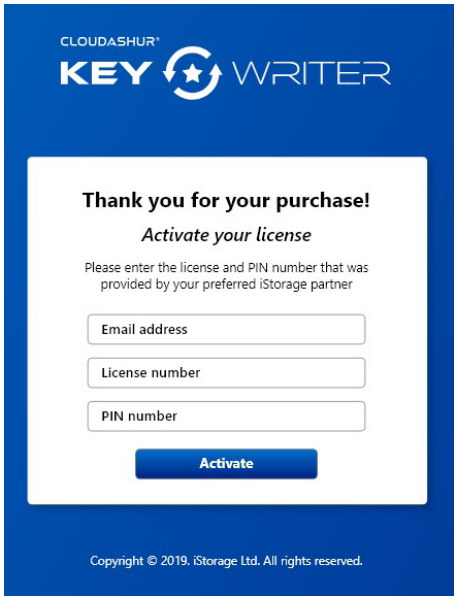

Bild 1: Lizenzaktivierung

2. Sie erhalten eine Benachrichtigung über eine Bestätigungs-E-Mail von iStorage (*Bild 2: Bestätigungs-E-Mail*). Klicken Sie auf den Link in der E-Mail und befolgen Sie die Anweisungen, um den Aktivierungsvorgang abzuschließen.

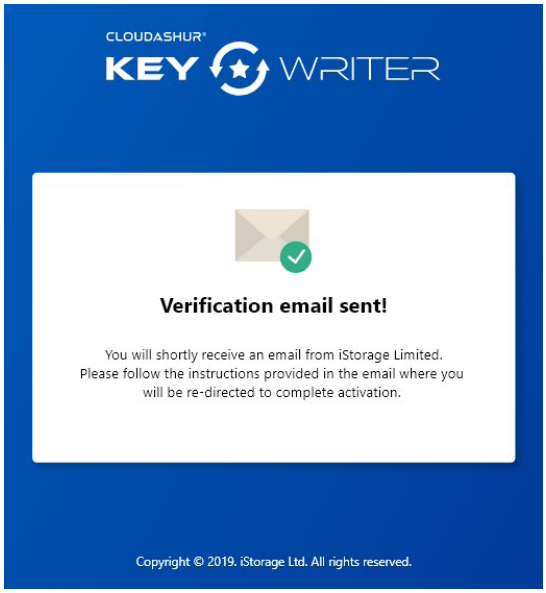

Bild 2: Bestätigungs-E-Mail

3. Füllen Sie alle Felder aus (*Bild 3: – Schließen Sie Ihre Aktivierung ab*) und klicken Sie dann auf "**Bestätigen**".

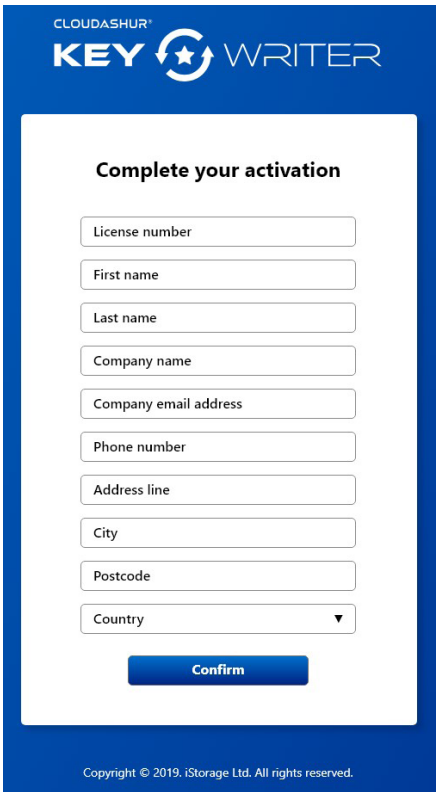

Bild 3: Schließen Sie Ihre Aktivierung ab

4. Befolgen Sie die Schritte (*Bild 4: Aktivierung erfolgreich*) und klicken Sie auf "**Herunterladen**", um die KeyWriter-App zu installieren. Als nächstes authentifizieren Sie (*7–15 stellige PIN*) Ihr cloudAshur-Hardwaresicherheitsmodul und stellen Sie eine Verbindung zu Ihrem Computer her. Registrieren Sie sich und melden Sie sich bei der cloudAshur-KeyWriter-App mit den in "*Bild 4*"erhaltenen Anweisungen an, um zu beginnen.

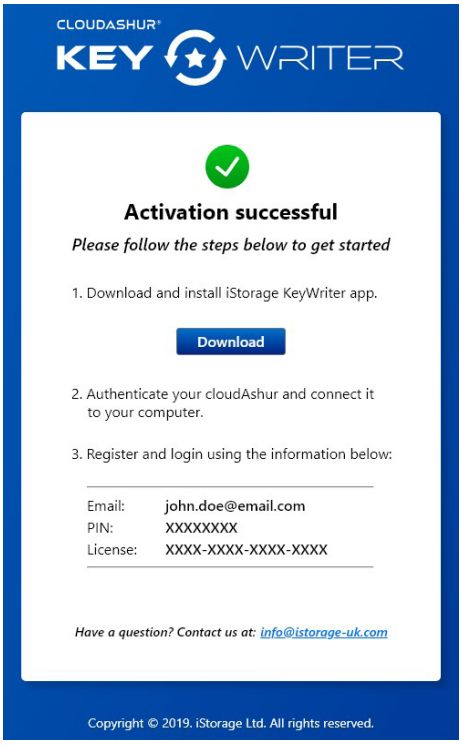

Bild 4: Aktivierung erfolgreich

2. Registrierung

1. Öffnen Sie die cloudAshur KeyWriter-App (*Bild 5: Registrierung*) und klicken Sie auf die Schaltfläche"**Registrieren**". Wenn Sie keine Lizenz haben, klicken Sie auf "**Sie haben noch keine Lizenz?**" Folgen Sie den Anweisungen, um Ihre KeyWriter-Lizenz zu erwerben.

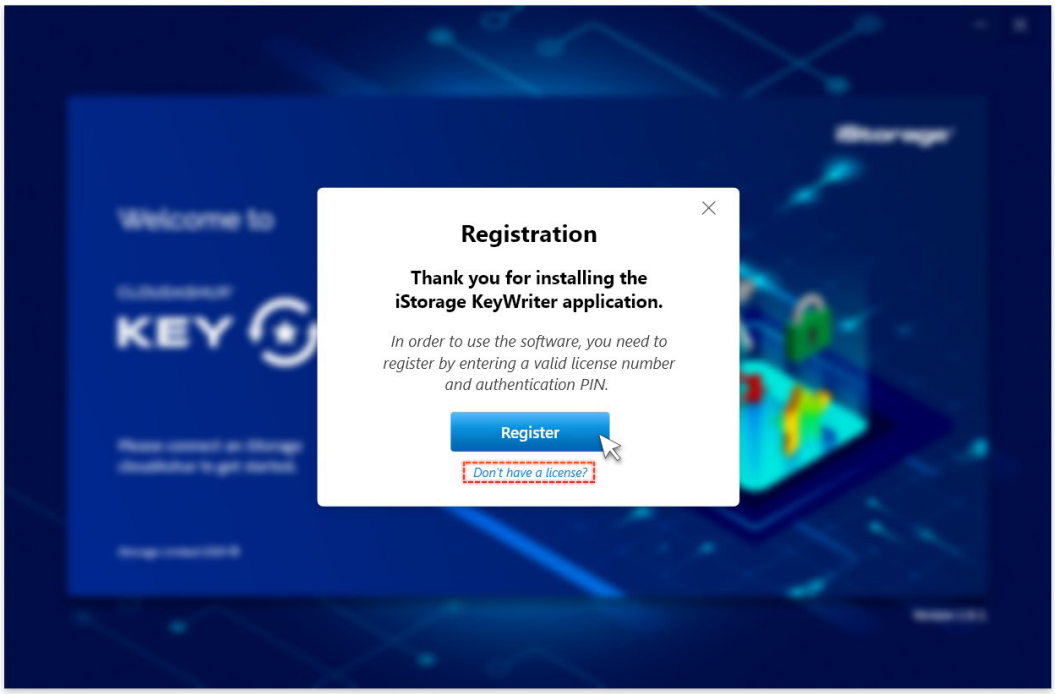

Bild 5: Registrieren

2. Geben Sie Ihre **Lizenznummer** und die **PIN Nummer** genau wie erhalten ein (*Bild 4: Aktivierung erfolgreich*) und klicken Sie anschließend auf "**Weiter**", um fortzufahren (*Bild 6: Registrierung*).

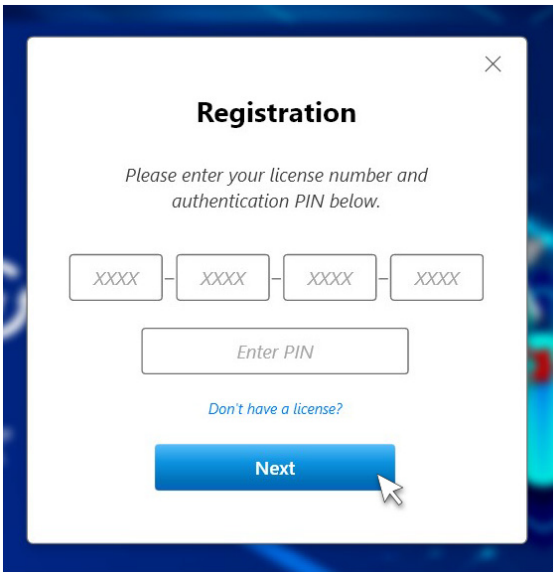

Bild 6: Registrierung

3. Klicken **Fortfahren** (*Bild 7: Registrierung erfolgreich*) und die KeyWriter-App wird gestartet und ist einsatzbereit.

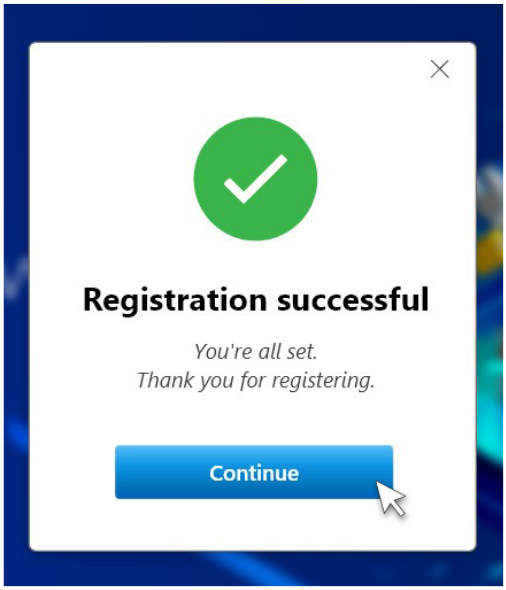

Bild 7: Registrierung erfolgreich

3. Einrichten Ihres cloudAshur Master-Geräts

Wichtig!

Vor dem Klonen: Wenn Sie alle Sicherheitsparameter von einem cloudAshur-Hardwaresicherheitsmodul (*Master-Gerät*) auf eine beliebige Anzahl sekundärer cloudAshur-Hardwaresicherheitsmodule klonen, muss sichergestellt werden, dass das „Master-Gerät“ vom Administrator so vorkonfiguriert wurde, dass es möglichst viele der folgenden Komponenten enthält:

1. **Festlegen einer Benutzer-PIN-Richtlinie**
2. **Hinzufügen einer Benutzer-PIN**
3. **Festlegen des cloudAshur-Hardwaresicherheitsmoduls zum Aktivieren des KeyWriter-Klonens**
4. **Konfigurieren des CloudAshur-Hardwaresicherheitsmodul-Verschlüsselungsmodus – AES-XTS (*Standard*) oder AES-ECB**
5. **Selbstzerstörungs-PIN konfigurieren**
6. **Einstellen der unbeaufsichtigten automatischen Sperre**

Wenn das Klonen Ihres cloudAshur-Hardwaresicherheitsmoduls deaktiviert wurde, lesen Sie Abschnitt 19 des Benutzerhandbuchs zum cloudAshur-Hardware-Sicherheitsmodul für eine vollständige und detaillierte Anleitung aller Konfigurationen.

Einstellen des Master-Geräts

Bitte beachten: Sie werden aufgefordert, Ihre KeyWriter-App- **PIN einzugeben.** Das geschieht jedes Mal, wenn Sie die cloudAshur-KeyWriter-App starten. Dies ist die **PIN,** die Sie gemeinsam mit der Lizenznummer per E-Mail erhalten haben. Die KeyWriter-App- **PIN** kann geändert werden, siehe Abschnitt 5: "**Ändern Sie Ihre KeyWriter-PIN**". Stellen Sie außerdem sicher, dass Ihr „Master-Gerät" entsperrt und mit Ihrem Computer verbunden ist, bevor Sie das Master-Gerät einrichten.

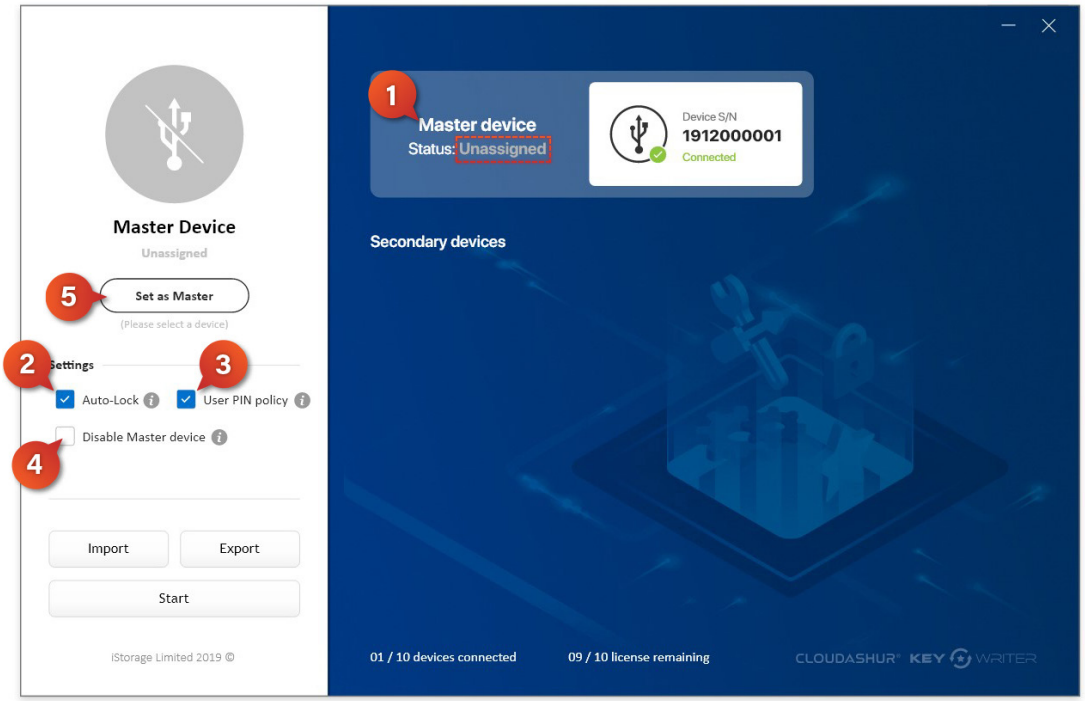

Bild 8: Einstellen des Master-Geräts

1. **Master-Gerät -** (*Bild 8: Einstellen des Master-Geräts*) Wenn Sie Ihr Master-CloudAshur-Hardwaresicherheitsmodul zum ersten Mal mit dem KeyWriter verbinden, wird das CloudAshur-Hardwaresicherheitsmodul als "Master-Gerät – Status" **nicht zugewiesen** angezeigt, zusammen mit der Seriennummer des Geräts.

2. **Automatische Sperre -** Wenn Sie dieses Kästchen markieren, wird die Einstellung "*Automatische Sperre*" – falls konfiguriert – vom Master-CloudAshur-Gerät auf das sekundäre CloudAshur-Gerät kopiert. Weitere Informationen zur Funktion "*Automatische Sperre*" finden Sie in der Bedienungsanleitung. Benutzerame.

3. **Benutzer-PIN-Richtlinie –** Wenn Sie dieses Kästchen markieren, wird die Einstellung "*Benutzer-PIN-Richtlinie*" – falls konfiguriert – vom Master-CloudAshur-Gerät auf das sekundäre CloudAshur-Gerät kopiert. Weitere Informationen zur Funktion "*Benutzer-PIN-Richtlinie*" finden Sie in der Bedienungsanleitung.

4. **Master-Gerät deaktivieren –** Durch Markieren dieses Kontrollkästchens wird die Klonfunktion des Master CloudAshur-Geräts deaktiviert, sobald ein Zyklus des Klonvorgangs erfolgreich abgeschlossen wurde. Wenn Sie weiterhin vom Master-Gerät auf zusätzliche sekundäre Geräte klonen möchten, lassen Sie das Kontrollkästchen deaktiviert.

5. Sobald Sie mit Ihren Einstellungen zufrieden sind (*Schritte 2–4 oben*), klicken sie auf die Schaltfläche "**Als Master festlegen**". Ihr Master-cloudAshur-Status wird nun angezeigt als "**Aktiv**", wie unten in "*Bild 9: Master-Gerät Aktiv*" dargestellt.

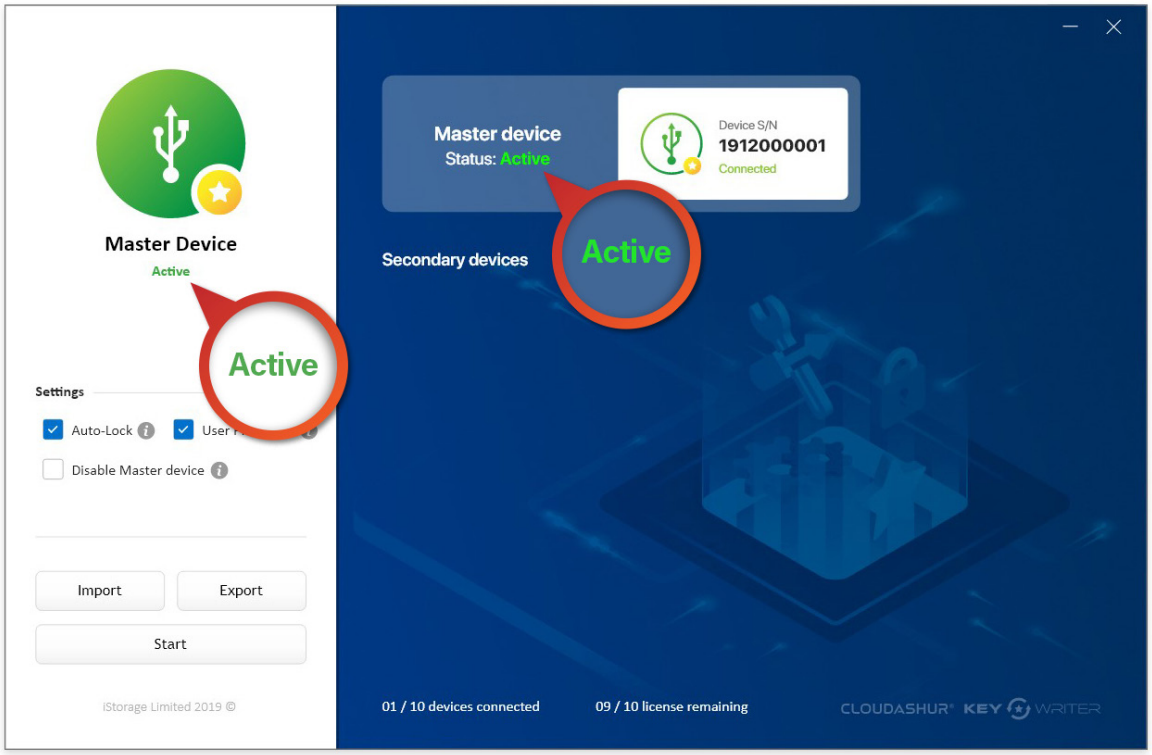

Bild 9: Master-Gerät aktiv

4. Klonen vom Master-Gerät auf sekundäre Geräte

Klonen starten

Stecken Sie bei aktiviertem cloudAshur Master-Gerät bis zu 9 cloudAshur "**Sekundäre Geräte**" (*auf einem 10-Port-USB-Hub ein*) und gehen Sie wie folgt vor: "*Bild 10: Klonen von Sekundärgeräten*".

1. Klicken sie auf die Schaltfläche "**Start**". Jedes sekundäre Gerät wird einzeln geklont, bis das Klonen aller Geräte abgeschlossen ist. Die cloudAshur-Hardware-Sicherheitsmodule sind jetzt einsatzbereit, siehe "*Bild 11: Gerät geklont*".
2. Klicken Sie zum lokalen Speichern Ihrer Einstellungen (*Automatische Sperre und Benutzer-PIN-Richtlinie*) auf Ihrem Computer auf "**Exportieren**" und speichern Sie.
3. Wenn Sie das nächste Mal weitere sekundäre Geräte klonen möchten und Ihre*gespeicherten*"Einstellungen speichern wollen, klicken Sie auf die Schaltfläche "**Importieren**" und navigieren Sie zu dem Ort, an dem Sie Ihre Einstellungen gespeichert haben – siehe Schritt 2.

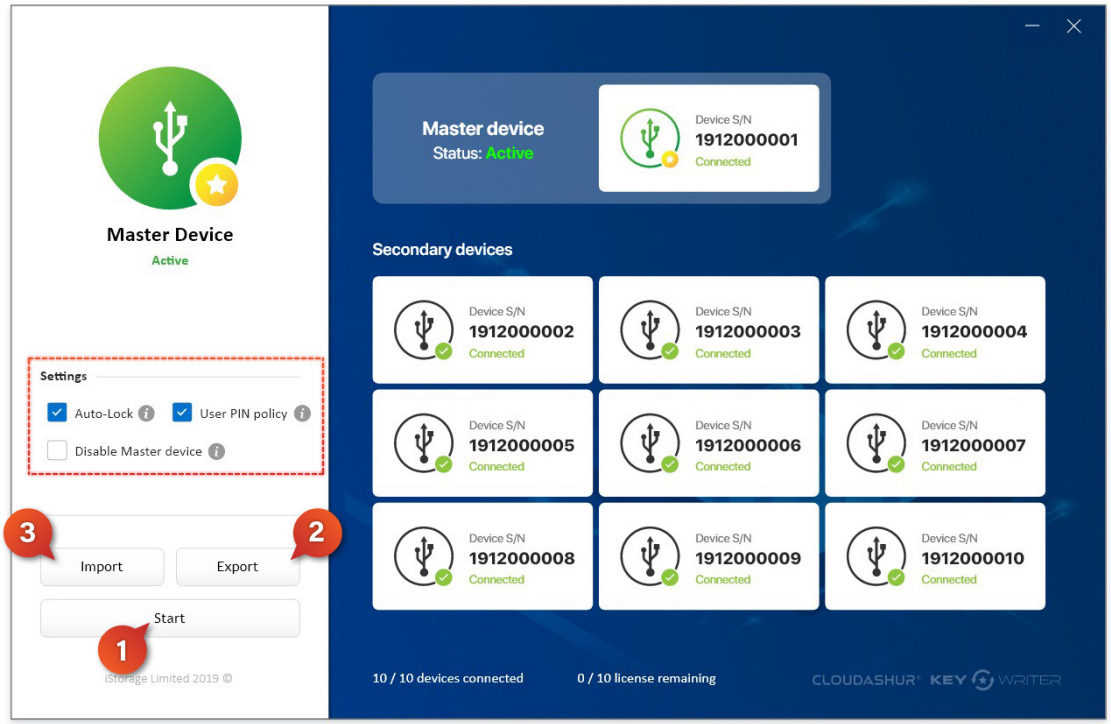

Bild 10: Klonen von Sekundärgeräten

Klonen abgeschlossen

Sobald das Klonen abgeschlossen ist, werden alle cloudAshur-Sekundärgeräte, die erfolgreich geklont wurden, mit einem Häkchen als "Gerät geklont" angezeigt, *siehe "Bild 11: Klonen abgeschlossen*".

Bitte beachten: Der Administrator kann jedes der geklonten (*Sekundär*-) CloudAshur Hardware-Sicherheitsmodule verwenden und als "**Master-Gerät eingerichtet werden**", lesen Sie bitte das Benutzerhandbuch des CloudAshur-Hardwaresicherheitsmoduls, um zunächst sicherzustellen, dass Ihr sekundäres Gerät aktiviert ist, um das Klonen zu ermöglichen.

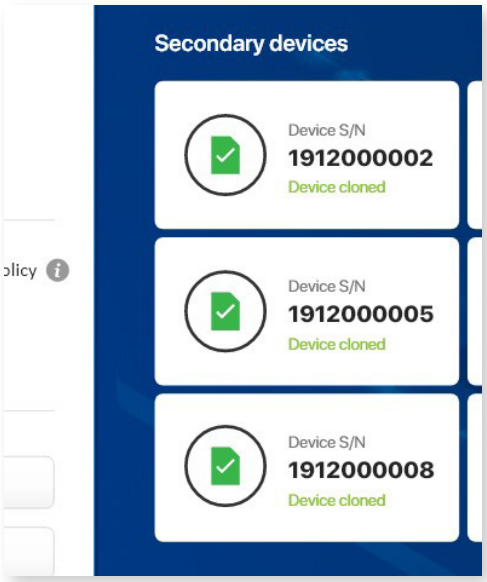

Bild 11: Klonen abgeschlossen

5. Ändern Sie Ihre KeyWriter-PIN

Um Ihre KeyWriter-PIN zu ändern, klicken Sie auf "**PIN ändern**" wie in "*Bild 12 angezeigt: PIN ändern*".

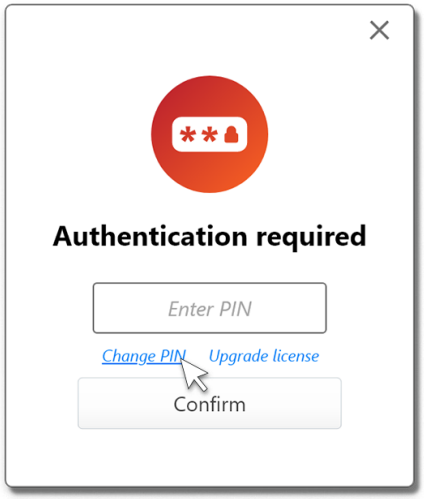

Bild 12: PIN ändern

Um Ihre PIN zu ändern, geben Sie Ihre *aktuelle PIN ein*, anschließend Ihre *neue Pin*. Bestätigen Sie *die neue PIN* und klicken Sie abschließend auf die Schaltfläche "**PIN ändern**". Ihre neue KeyWriter-PIN ändert sich und wird beim nächsten Öffnen Ihrer cloudAshur KeyWriter-App aktiv.

Bitte beachten: Der Bildschirm "KeyWriter-PIN ändern" (*Bild 13: PIN geändert*) erkennt automatisch Ihre Lizenznummer, und die Texteingabefelder können so eingestellt werden, dass die PIN-Zeichen ein- oder ausgeblendet werden.

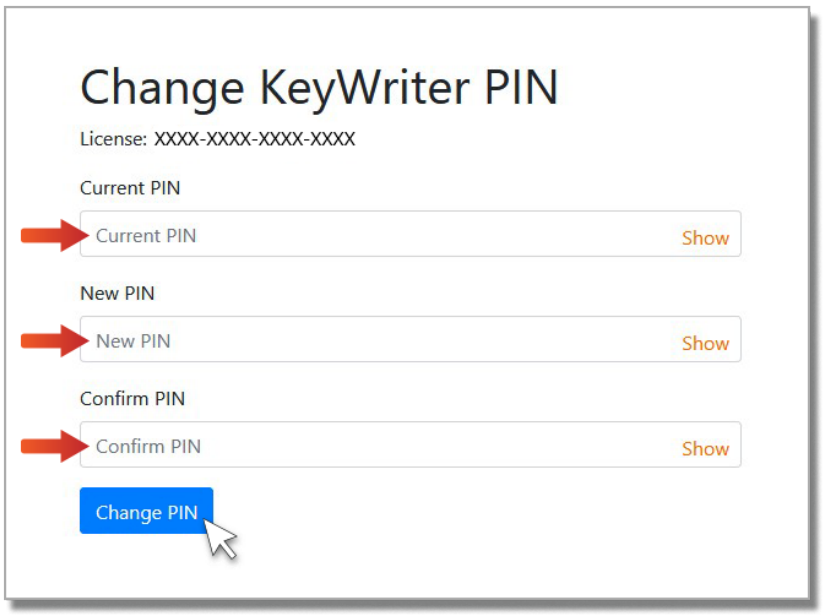

Bild 13: PIN geändert

iStorage®

CLOUDASHUR®

KEY WRITER

Benutzerhandbuch – Version 1.2

www.istorage-uk.com | info@istorage-uk.com | +44 (0) 20 8991 6260

iStorage®

CLOUDASHUR®

KEY WRITER

Manuel d'utilisation

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

www.istorage-uk.com

Version 1.2

Introduction

KeyWriter cloudAshur (*brevet en instance*) facilite considérablement le partage de données dans le cloud, par e-mail et via des services de transfert de fichiers (*par exemple WeTransfer*) entre des utilisateurs autorisés, en garantissant une sécurité optimale et la tranquillité d'esprit : les données s'échangent en toute sécurité, en temps réel, quel que soit leur emplacement.

Fonctionnalités clés

KeyWriter cloudAshur clone tous les paramètres de sécurité critiques, y compris la clé de chiffrement générée de manière aléatoire, l'ensemble des codes PIN et les configurations définies par l'administrateur, entre le module de sécurité matériel cloudAshur maître et autant de modules de sécurité matériels cloudAshur secondaires que nécessaire, en utilisant n'importe quel hub USB du commerce (nous recommandons toutefois un hub USB à 10 ports). Cela permet aux utilisateurs autorisés de partager des données en toute sécurité, en temps réel, quel que soit leur emplacement.

Les paramètres de sécurité critiques ne quittent jamais le module de sécurité matériel cloudAshur et sont stockés dans le microprocesseur sécurisé conforme aux Critères communs EAL4+.

Le processus de clonage de la clé de chiffrement chiffrée et de tous les identifiants entre le module de sécurité matériel cloudAshur maître et les modules de sécurité matériels cloudAshur secondaires est protégé par un protocole sécurisé incorporé dans le microcontrôleur sécurisé iStorage cloudAshur. Ce protocole est mis en œuvre à l'aide d'algorithmes cryptographiques, qui sont tous certifiés FIPS. Chaque cloudAshur possède un certificat unique émis par une racine de confiance, qui garantit que seuls des modules de sécurité matériels iStorage cloudAshur peuvent être utilisés pendant le processus d'échange de clés.

Les modules de sécurité matériels cloudAshur ne fournissent jamais la clé de session établie au cours du protocole sécurisé, et les données sensibles qui sont copiées ne sont déchiffrées que dans le module de sécurité matériel cloudAshur de destination qui aura été vérifié. Le logiciel iStorage KeyWriter, qui s'exécute sur un PC, coordonne les opérations requises par le protocole sécurisé. Toutefois, le logiciel n'a aucune visibilité sur la clé de session ni sur les données déchiffrées, ce qui empêche totalement un pirate d'accéder aux paramètres de sécurité critiques stockés dans le module de sécurité matériel cloudAshur ou d'en extraire les données.

Liens cloudAshur

Les manuels d'utilisation suivants, complets et détaillés, peuvent être consultés en suivant le lien ci-dessous :

- Manuel d'utilisation complet et détaillé du module de sécurité matériel cloudAshur
- Manuel d'utilisation de la console Remote Management cloudAshur

https://istorage-uk.com/product-documentation/

Table des matières

1. Activation et installation de cloudAshur KeyWriter

Remarque : Si vous avez acheté votre logiciel Remote Management cloudAshur directement auprès d'iStorage, suivez les instructions contenues dans l'e-mail envoyé par iStorage. Ignorez la « *section 1* » et passez directement à la « *section 2 : Enregistrement et connexion* ».

1. Après avoir acheté votre logiciel KeyWriter cloudAshur, vous recevrez un e-mail contenant votre **numéro de licence** et votre **code PIN**. Renseignez les champs ci-contre (*Image 1 : Activation de la licence*), puis cliquez sur le bouton « **Activer** ».

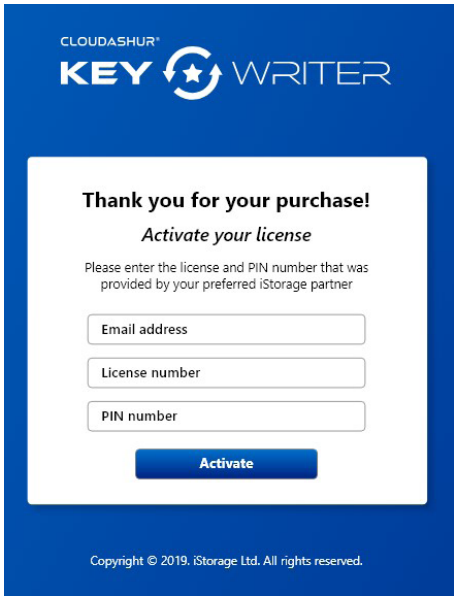

Image 1 : Activation de la licence

2. Un message s'affichera pour vous avertir qu'un e-mail de vérification vous a été envoyé (*Image 2 : E-mail de vérification*). Cliquez sur le lien inclus dans l'e-mail, puis suivez les instructions afin d'achever le processus d'activation.

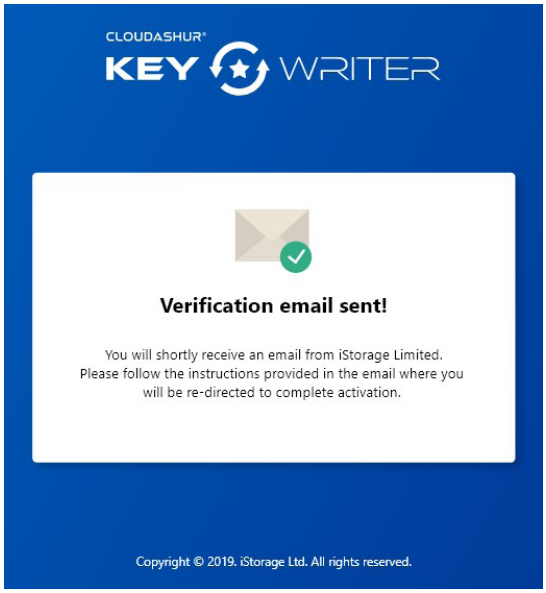

Image 2 : E-mail de vérification

3. Renseignez tous les champs (*Image 3 : Terminez l'activation*), puis cliquez sur « **Confirmer** ».

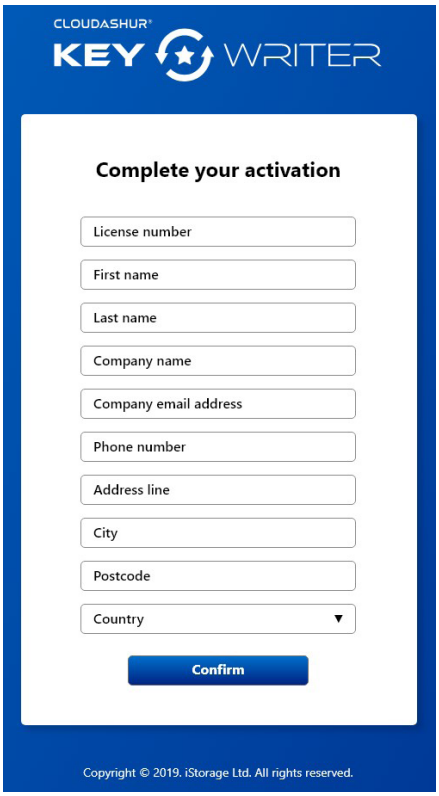

Image 3 : Terminez l'activation

4. Suivez les étapes (*Image 4 : Activation réussie*), puis cliquez sur le bouton « **Télécharger** » pour installer l'appli KeyWriter. Ensuite, authentifiez (*Code PIN de 7 à 15 caractères*) votre module de sécurité matériel cloudAshur et connectez-le à votre ordinateur. Enfin, enregistrez-vous et connectez-vous à l'appli KeyWriter cloudAshur à l'aide des informations qui vous ont été fournies (voir l'*Image 4* ci-contre) pour commencer à utiliser votre produit.

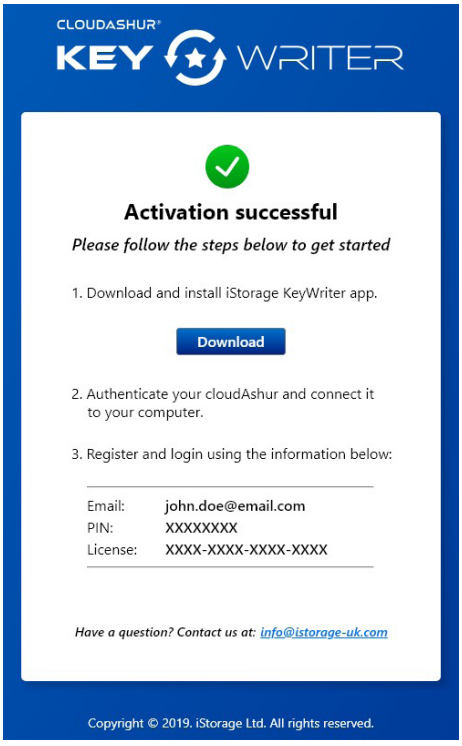

Image 4 : Activation réussie

2. Enregistrement

1. Ouvrez votre appli KeyWriter cloudAshur (*Image 5 : S'enregistrer*), puis cliquez sur le bouton « **S'enregistrer** ». Si vous n'avez pas de licence, cliquez sur « **Vous n'avez pas de licence ?** », puis suivez les instructions afin d'acheter votre licence KeyWriter.

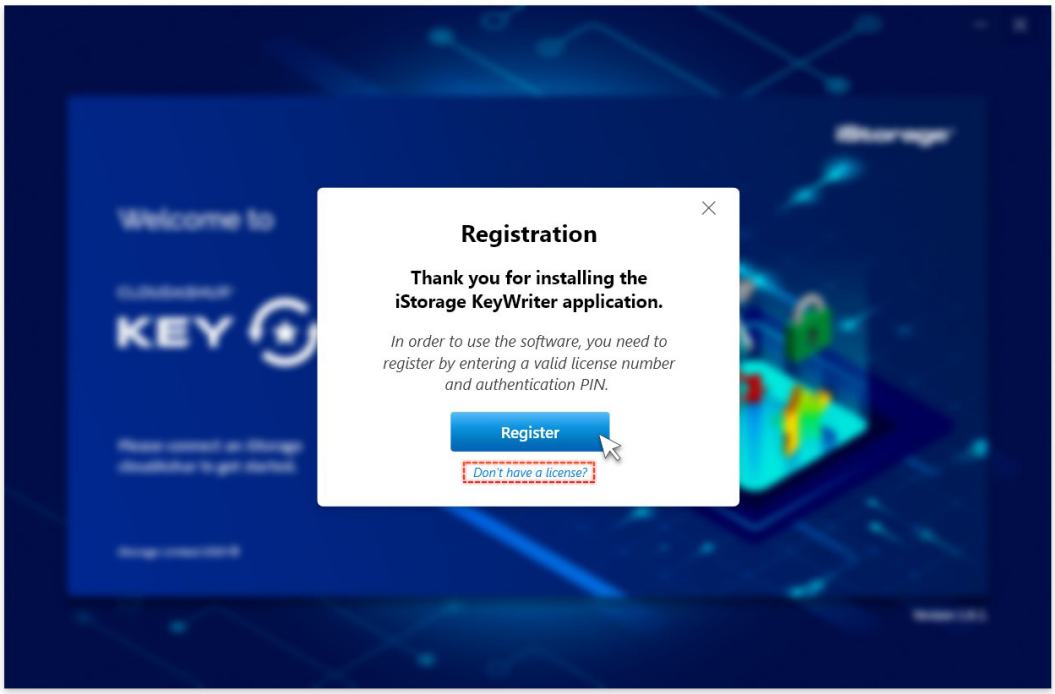

Image 5 : S'enregistrer

2. Saisissez votre **Numéro de licence** et votre **Code PIN** exacts, tel qu'ils vous ont été communiqués (*Image 4 : Activation réussie*), puis cliquez sur « **Suivant** » pour continuer (*Image 6 : Enregistrement*).

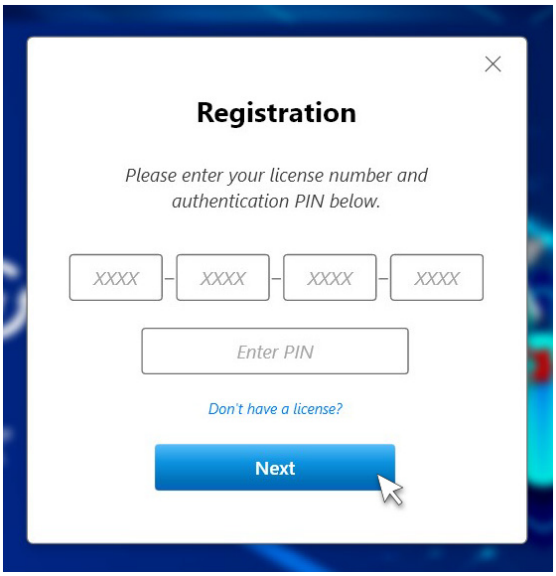

Image 6 : Enregistrement

3. Cliquez sur **Continuer** (*Image 7 : Enregistrement réussi*). L'appli KeyWriter s'ouvre et est prête à être utilisée.

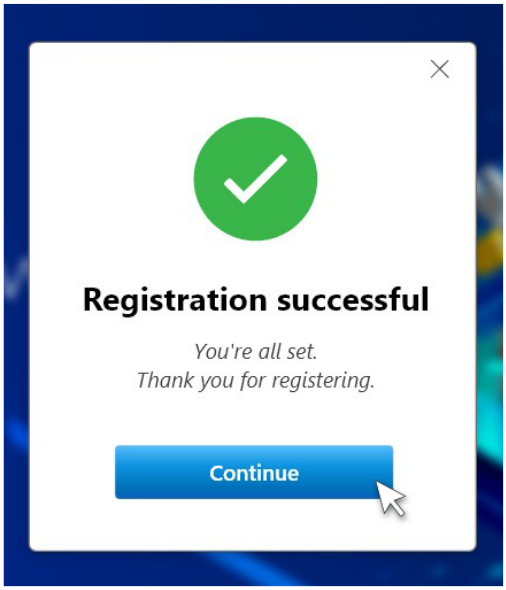

Image 7 : Enregistrement réussi

3. Paramétrage de votre appareil cloudAshur maître

Important !

Avant le clonage : Vous allez procéder au clonage de l'ensemble des paramètres de sécurité d'un module de sécurité matériel cloudAshur (*appareil maître*) vers un ou plusieurs modules de sécurité matériels cloudAshur secondaires. Veillez à ce que l'administrateur préconfigure autant d'éléments que possible sur l'« appareil maître » parmi la liste ci-dessous :

1. **Paramétrage d'une Règle de code PIN utilisateur**
2. **Ajout d'un code PIN utilisateur**
3. **Paramétrage de votre module de sécurité matériel cloudAshur afin d'activer la fonction de clonage KeyWriter**
4. **Configuration du mode de chiffrement du module de sécurité matériel cloudAshur - AES-XTS (*par défaut*) ou AES-ECB**
5. **Configuration d'un code PIN à destruction automatique**
6. **Paramétrage du verrouillage automatique des appareils laissés sans surveillance**

Si la fonction de clonage est désactivée sur votre module de sécurité matériel cloudAshur, référez-vous à la section 19 du manuel d'utilisation du module de sécurité matériel cloudAshur pour obtenir les instructions complètes et détaillées propres à chaque configuration.

Paramétrage de l'appareil maître

Remarque : Vous devrez saisir le **code PIN** de votre appli KeyWriter à chaque fois que vous lancez l'appli KeyWriter cloudAshur. Il s'agit du **code PIN** qui vous a été envoyé par e-mail avec votre numéro de licence. Le **code PIN** de l'appli KeyWriter peut être modifié. Pour cela, consultez la section 5 : « **Modifier votre code PIN KeyWriter** ». Par ailleurs, vous devez veiller à ce que votre « appareil maître » soit déverrouillé et connecté à votre ordinateur avant de le paramétrer.

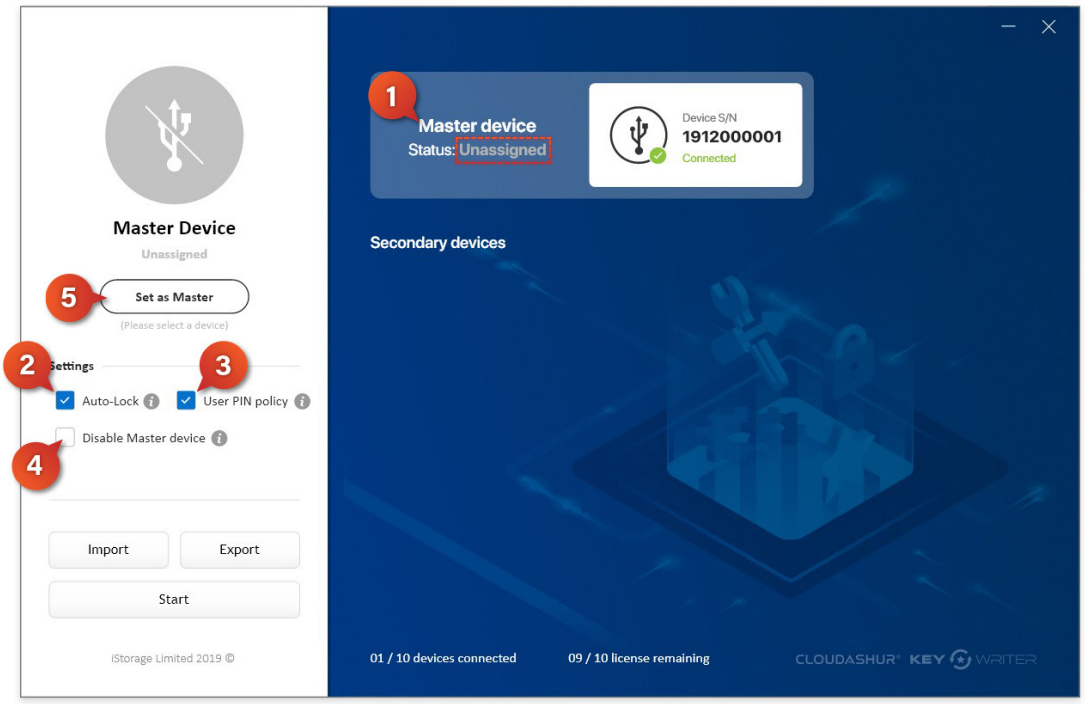

Image 8 : Paramétrer l'appareil maître

1. **Appareil maître :** (*Image 8 : Paramétrer l'appareil maître*) lorsque vous connectez votre module de sécurité matériel cloudAshur maître à KeyWriter pour la première fois, il apparaît sous « Appareil maître - État : **non assigné** », avec son numéro de série affiché à côté.

2. **Verrouillage automatique :** cochez cette case pour copier le paramètre « *Verrouillage automatique* » (s'il a été configuré), de l'appareil cloudAshur maître vers l'appareil cloudAshur secondaire. Veuillez vous référer au manuel d'utilisation pour tout complément d'information concernant le « *Verrouillage automatique* ». Nom d'utilisateur.

3. **Règle de code PIN utilisateur :** cochez cette case pour copier le paramètre « *Règle de code PIN utilisateur* » (s'il a été configuré), de l'appareil cloudAshur maître à l'appareil cloudAshur secondaire. Veuillez vous référer au manuel d'utilisation pour tout complément d'information concernant la fonctionnalité « *Règle de code PIN utilisateur* ».

4. **Désactiver l'appareil maître :** cochez cette case pour désactiver la fonctionnalité de clonage sur l'appareil cloudAshur maître dès lors que le cycle du processus de clonage s'est achevé avec succès. Si vous envisagez de continuer à cloner l'appareil maître vers d'autres appareils secondaires, ne cochez pas cette case.

5. Lorsque vous êtes satisfait des paramétrages effectués (*étapes 2 à 4 ci-dessus*), cliquez sur le bouton « **Définir comme appareil maître** ». L'état de votre appareil cloudAshur maître apparaît alors comme « **Actif** », comme indiqué ci-dessous dans l'*Image 9 : Appareil maître actif*.

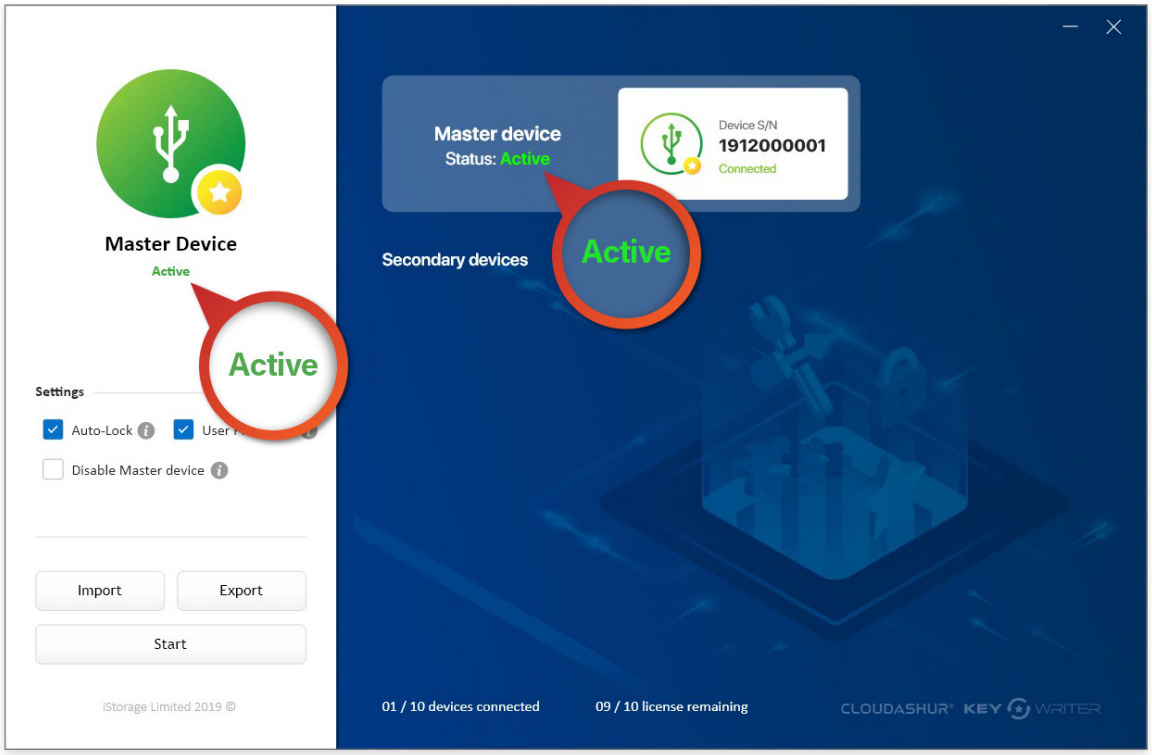

Image 9 : Appareil maître actif

4. Clonage d'un appareil maître vers des appareils secondaires

Début du clonage

Pendant que votre appareil maître est actif, insérez jusqu'à 9 « **appareils secondaires** » cloudAshur (*sur un hub USB à 10 ports*), et procédez comme suit - voir « *Image 10 : Clonage d'appareils secondaires* ».

1. Cliquez sur le bouton « **Démarrer** ». Tous les appareils secondaires seront clonés chacun leur tour. Les modules de sécurité matériels cloudAshur sont maintenant prêts à être utilisés. Voir « *Image 11 : Appareil cloné* ».
2. Pour sauvegarder vos paramètres (*Verrouillage automatique et Règle de code PIN utilisateur*) en local sur votre ordinateur, cliquez sur « **Exporter** » et enregistrez les informations.
3. La prochaine fois que vous devrez cloner des appareils secondaires et que vous voudrez importer vos paramètres « *sauvegardés* », cliquez sur le bouton « **Importer** » et accédez à l'emplacement où vous avez sauvegardé vos paramètres (voir l'étape 2).

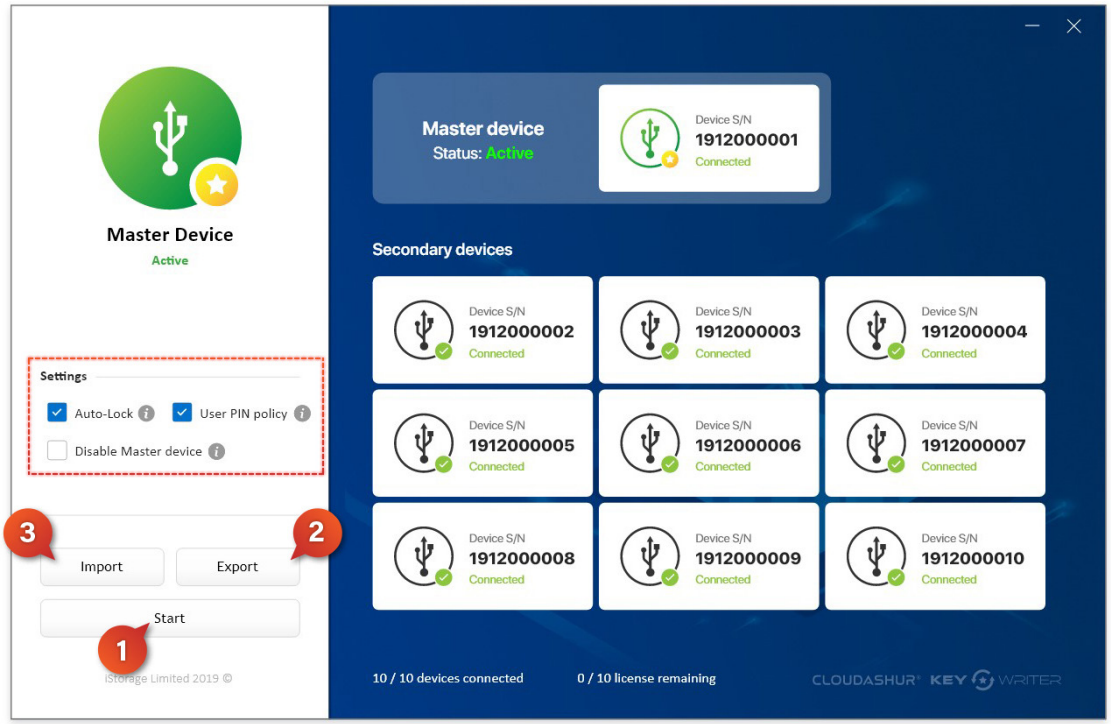

Image 10 : Clonage d'appareils secondaires

Clonage terminé

Lorsque le processus de clonage est terminé, tous les appareils secondaires cloudAshur ayant été clonés avec succès sont marqués d'une coche verte et le texte « Appareil cloné » s'affiche pour chacun d'eux - *voir Image 11 : Clonage terminé*.

Remarque : L'administrateur peut définir n'importe quel module de sécurité matériel (*secondaire*) cloudAshur cloné comme « **appareil maître** ». Référez-vous au manuel d'utilisation du module de sécurité matériel cloudAshur pour vous assurer dans un premier temps que la fonction de clonage est activée sur votre appareil secondaire.

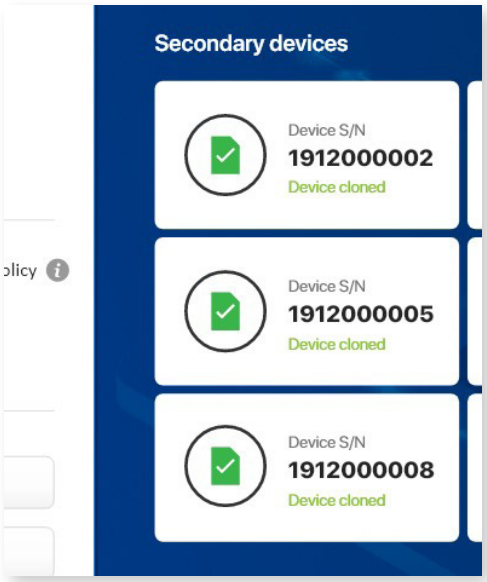

Image 11 : Clonage terminé

5. Modifier votre code PIN KeyWriter

Pour modifier votre code PIN KeyWriter, cliquez sur « **Modifier le code PIN** », comme indiqué dans l'*Image 12 : Modifier le code PIN*.

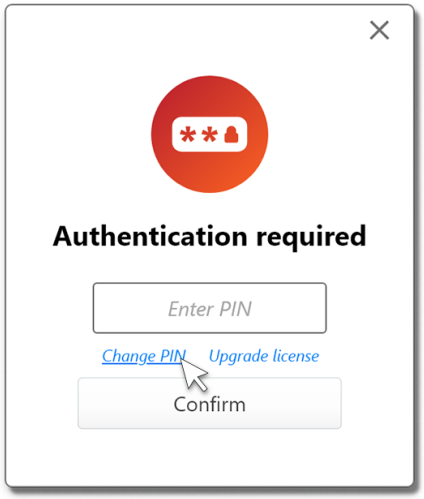

Image 12 : Modifier le code PIN

Pour modifier votre code PIN, saisissez votre *code PIN actuel*, suivi de votre *nouveau code PIN*, puis *confirmez le nouveau code PIN*. Enfin, cliquez sur le bouton « **Modifier le code PIN**. Votre code PIN KeyWriter sera alors modifié et deviendra actif à la prochaine ouverture de l'appli KeyWriter cloudAshur.

Remarque : L'écran « Modifier le code PIN KeyWriter » (*Image 13 : PIN modifié*) détecte automatiquement votre numéro de licence. Les champs de saisie de texte peuvent être configurés pour afficher ou masquer les caractères du code PIN.

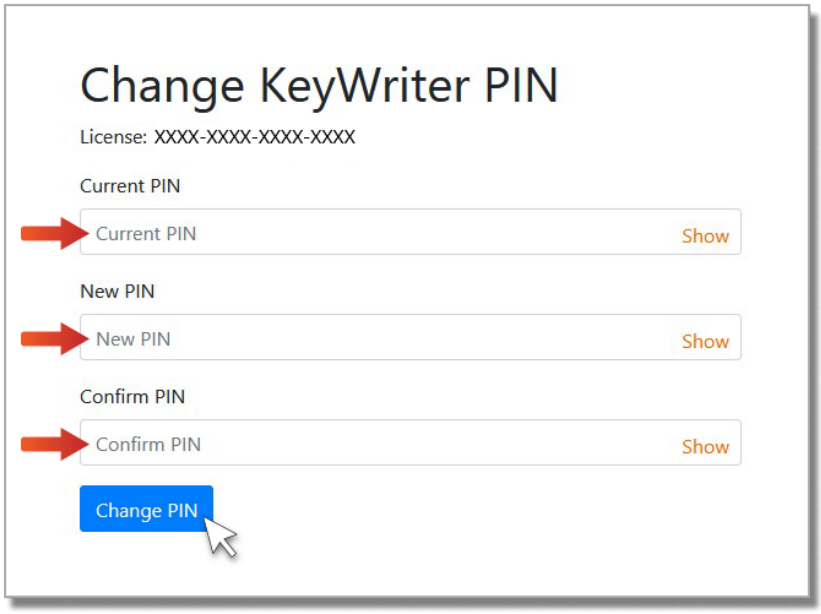

Image 13 : PIN modifié

iStorage®

CLOUDASHUR®

KEY WRITER

Manuel d'utilisation - Version 1.2

www.istorage-uk.com | info@istorage-uk.com | +44 (0) 20 8991 6260