DATASHUR® BT
ADMIN MANUAL

ADMIN MANUAL / MANUEL DE L'ADMINISTRATEUR / ADMINISTRATORENHANDBUCH

English User Manual - Table of Contents 4

Français Manuel d'utilisation - Table des matières 32

Deutsch Benutzerhandbuch - Inhaltsverzeichnis 60

ADMIN MANUAL

EMI Cautions

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Cautions

Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate this device. The normal function of the product may be disturbed by strong Electro-Magnetic Interference. If so, simply reset the product to resume normal operation by following the instruction manual. In case the function could not resume, please use the product in other location."

This device complies with part 15 of the FCC Rules and with Industry Canada License-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) This device must accept any interference received, including interference that may cause undesired operation.

RF Exposure Statement

The device has been evaluated to meet general RF exposure requirement.

Table of Contents

Introduction 5
Box contents 5
Useful Links 5
datAshur BT Layout 6
Drive LED Indicators and their actions 6
1. **Registration** 7
2. **How to enroll as an Administrator (Admin)** 8
3. **How to Provision datAshur BT Managed Drives** 9
4. **How to Create Users via the Remote Management Console** 12
5. **How to Assign Drives to Users** 13
6. **Managing Users Dashboard** 14
   - User Dashboard at a glance 14
   - How to Enable or Disable User Access 14
   - How to Delete a User from Remote Management 14
   - How to Reset User's datAshur BT Managed App Password 14
   - Search Bar 15
   - Opening the Geo & Time-Fencing Panel 15
7. **Managing Drives Dashboard** 15
   - Drives Dashboard at a glance 15
   - How to Delete a Drive from Remote Management 16
   - Search by Drive Serial Number 16
   - Managing Access Control 16
   - How to Wipe a Drive via Remote Management 17
   - How to Change a Drive Password via Remote Management 17
   - How to Unlock a Drive via Remote Management 17
   - Viewing Assigned to & Access Log 18
8. **How to Apply Geo & Time-Fencing Restrictions** 18
   - Geo & Time-Fencing at a glance 18
   - Allowed Drives 19
   - How to set Time-Fencing Restrictions 19
   - How to set Geo-Fencing Restrictions 19
9. **How to Change the Admin Password** 20
10. **Account Summary** 20
11. **How to Provision a Non-Managed Drive** 21
12. **Formatting the datAshur BT for Windows** 24
13. **Formatting the datAshur BT for mac OS** 25
14. **Technical Support** 28
15. **Warranty and RMA information** 28

Introduction

Thank you for purchasing the Managed Drive subscription for the datAshur BT, a hardware encrypted USB 3.2 Gen 1 flash drive that utilises mobile phone technology via Bluetooth and turns your (iOS/Android) Smartphone into a wireless user-authentication device that enables secure access to data stored on your datAshur BT Managed flash drive.

The datAshur BT Managed Drive uses military grade AES-XTS 256-bit hardware encryption (full disk encryption), which encrypts all data stored on the drive in real-time.

The datAshur BT Managed Drive is designed for remote management via the web-based iStorage Remote Management Console that allows the Administrator to control where and when the Drive can be accessed with Geo and Time-Fencing. Additional features include, remote wipe, remote unlock, change passwords, disable access and more.

Box Contents

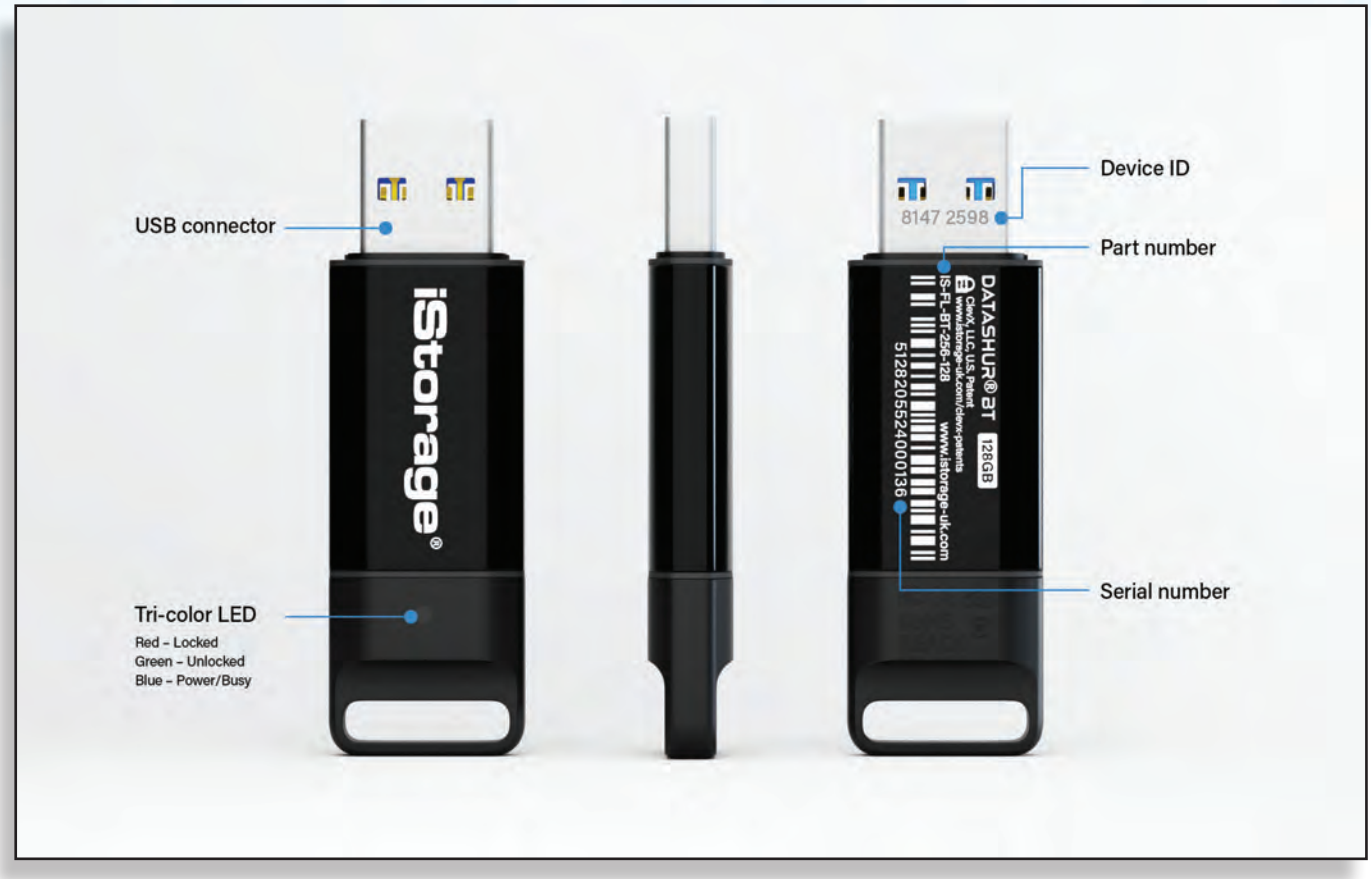
- iStorage datAshur BT
- QSG - Quick Start Guide for '**Non-Managed**' datAshur BT Personal

Note: The datAshur BT packaging contains a QSG insert applicable only to the 'Non-Managed' datAshur BT Personal. Please ignore the QSG insert and refer to the instructions contained in this manual.

Useful Links

1. datAshur BT Admin Registration Link: https://rm.bt.istorage-uk.com/Account/Register
2. Remote Management Login Link: https://rm.bt.istorage-uk.com/Account/Login
3. datAshur BT Managed User Manual: https://istorage-uk.com/product-documentation/
4. datAshur BT Managed User QSG: https://istorage-uk.com/product-documentation/
5. datAshur BT Personal User Manual: https://istorage-uk.com/product-documentation/

datAshur BT Layout



Drive LED indicators and their actions

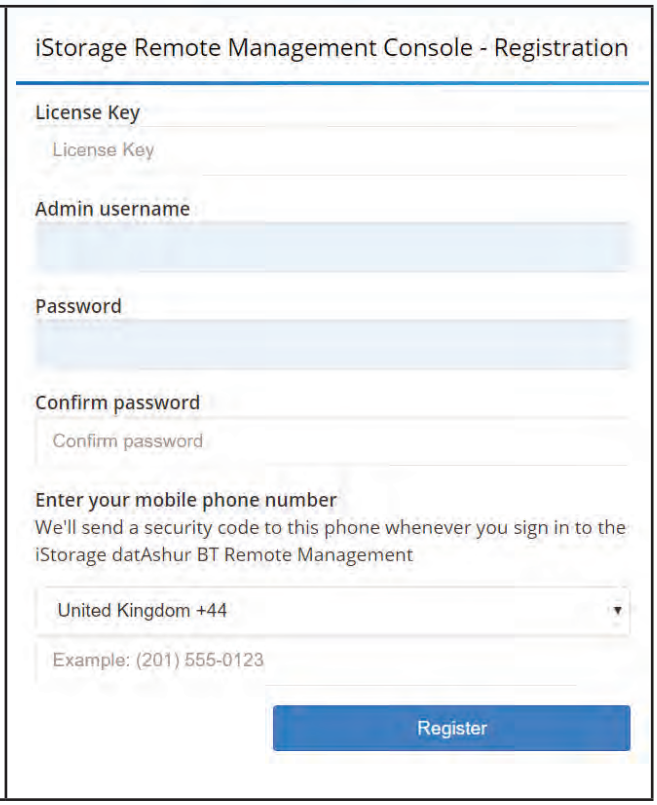
LEDs	LED State	Description
	All LEDs blink once	datAshur BT conducts a self test when plugged to a computer
	Solid Red	Locked - datAshur BT App not open
	Blinking Red	Locked - datAshur BT App open
	Solid Blue	datAshur BT is unlocked
	Blinking Blue	datAshur BT is unlocked and communication in progress

1. Registration

Upon purchase of the iStorage Remote Management Console license, you will receive an email containing a '**Registration link**' and '**License Key**' to begin the registration process as described below.

Open the following link to take you to the registration page and complete the registration fields as set out below.
https://rm.bt.istorage-uk.com/Account/Register

1. **License Key:** Refer to the registration email from iStorage that contains your License Key.
2. **Admin Username:** This must be an **email address** which will be used for **Admin sign-in**.
3. **Password:** Create a secure password.
4. **Confirm Password:** Re-enter your password to confirm.
5. Select your **Country** from the drop down menu and then **Enter your mobile phone number:** This is required for '**Two Factor Authentication**'.
6. Click '**Register**'.
7. On the '**Enable two-step verification**' page, enter the **6-digit code** received by text message and click **Next**.
8. Click '**Done**'.



2. How to enroll as an Administrator (Admin)

The Administrator is able to provision, set security policies and have full control and visibility of all datAshur BT Managed Drives deployed throughout an organisation by using the iStorage web based Remote Management Console.

To setup as Admin, you will need your **Username** and **Password** you created during the registration process as described in '**section 1 - Registration'** and then proceed with the following steps.

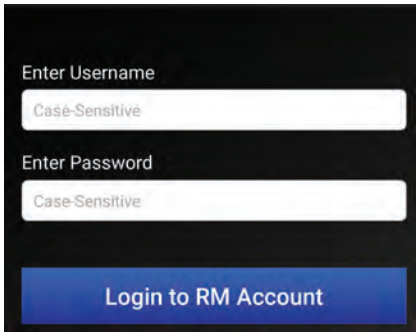
1. Download and install the **datAshur BT Admin App** from the **Apple App Store** or **Google Play**, or **scan the QR code** directly from your smartphone to download.

datAshur BT Admin App

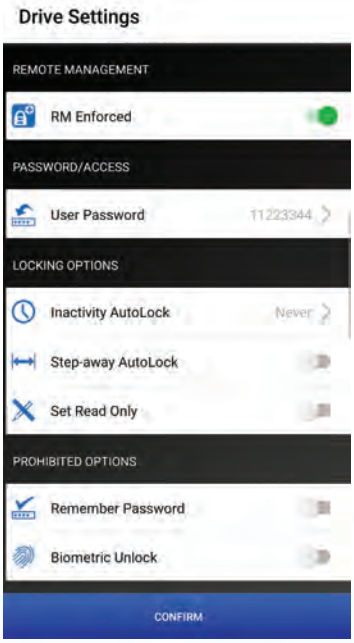
2. In the pop message, tap **Allow**.

3. Enter your **Username** and **Password** and then tap on **Login to RM (**Remote Management**) Account.**

Note: Your Username and Password for both the datAshur BT Admin App and the iStorage web based Remote Management Console are the same.



After successfully logging in, the **Drive Settings** menu will open ready for setting security policies and provisioning all datAshur BT Managed Drives as described in the following section.

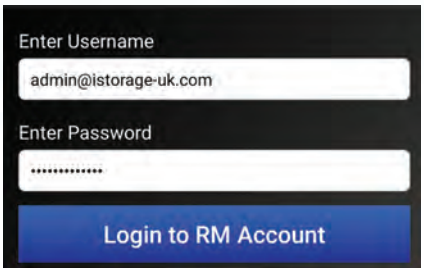


3. How to Provision datAshur BT Managed Drives

After setting up as Admin (section 2), you will first need to provision all datAshur BT Managed Drives you intend to manage via the Remote Management Console one Drive at a time.

To start provisioning, proceed with the following steps.

1. Open your **datAshur BT Admin App** and enter your **Username** and **Password** and then tap on **Login to RM (**Remote Management**) Account.**



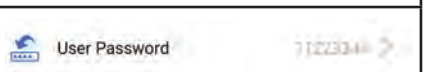
2. After successfully logging in, the **Drive Settings** menu will open ready for you to review and apply your security settings as described below:

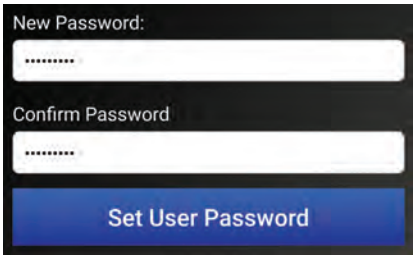
- **RM Enforced:** This is switched on by default (**GREEN** light on) and MUST remain **ON** to enable Remote Management provisioning. When switched off, a Drive can be provisioned to work with the non-managed App (datAshur BT App - refer to a separate user manual).

- **User Password:** The datAshur BT ships with a **default password** (**11223344**). To change the default password, tap on '**User Password**' and then **enter** and **confirm** your New **7-15** character Password and finally tap on '**Set User Password**'.

  Password Requirement: Password must be 7-15 characters in length and cannot contain only consecutive or repetitive numbers or letters.

  Note: For security reasons, we strongly recommend that each user change the default or Admin set password to their own unique 7-15 character password once the Drive has been issued to them.

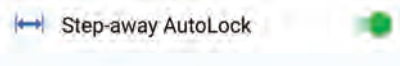
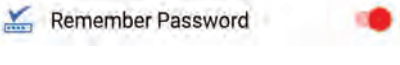
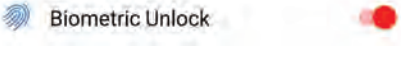
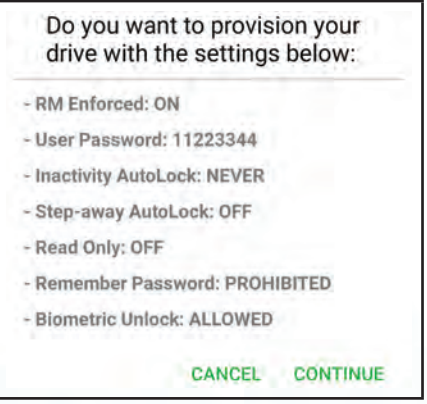




- **Inactivity AutoLock:** To protect against unauthorised access if the Drive is unlocked and unattended, the datAshur BT can be set to automatically lock after a pre-set amount of time. In its default state, the datAshur BT Unattended Inactivity AutoLock feature is turned off (Never) but can be set to autolock between **1 - 60** minutes.

  To set a time limit, tap on Inactivity AutoLock and then tap to choose your desired length of time.

  Note: When Admin sets the Inactivity AutoLock, the User is prohibited from disabling this feature.

• **Step-away AutoLock:** The Step-away AutoLock is switched off by default, if enabled (**GREEN** light on), this will set all the deployed datAshur BT Managed Drives to lock when a user's Smartphone (Android/iOS) is moved approximately 5 meters away from the datAshur BT Drive for more than 5 seconds. **Note:** When Admin enables Step-away AutoLock, the User is prohibited from disabling this feature.	
• **Set Read Only:** The Read Only feature is switched off by default, when enabled (**GREEN** light on), all deployed datAshur BT Managed Drives will be set as Read Only/Write Protect. **Note:** When Admin enables Read Only, the User is prohibited from disabling this feature.	
• **Remember Password:** The Remember Password feature is operational (ON) by default, enabling Users to set their Drives to unlock without entering their password. To disable this feature (**recommended**) and prohibit Users from setting their Drives to unlock without entering a password, tap on the greyed out switch to prohibit (**RED** light on). **Note:** When Admin **prohibits** Remember Password (**RED** light on), the User cannot enable this feature and will need to enter their password each time they need to unlock their Drive.	
• **Biometric Unlock:** The Biometric Unlock feature is operational (ON) by default, enabling Users to set a Biometric Unlock to access their Drives. To disable this feature and prohibit Users from setting a Biometric Unlock to access their Drives, tap on the greyed out switch to prohibit (**RED** light on). **Note:** When Admin **prohibits** Biometric Unlock (**RED** light on), the User cannot enable this feature.	
3. Tap to Confirm your Drive Settings.	
4. Tap **Continue** to provision all datAshur BT Managed Drives with your preferred settings.	

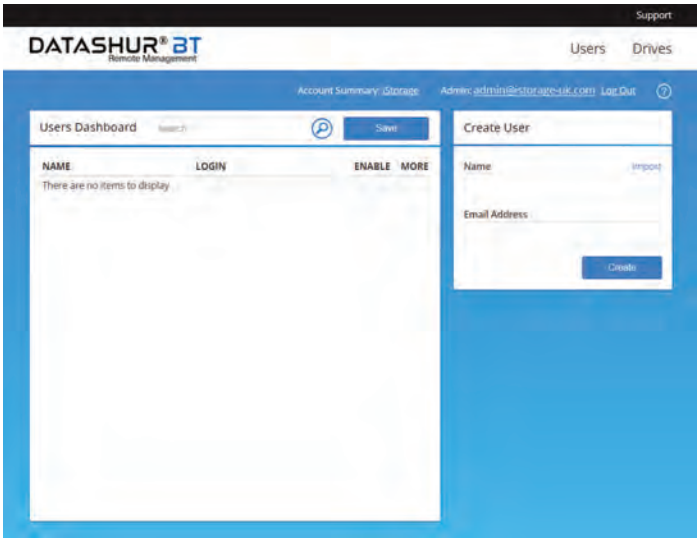
5. Make a note of the **Device ID** number printed on the USB connector and **connect** the datAshur BT Managed Drive to a powered USB port.	
6. Tap on the **RED** padlock. **Note:** The Drive LED will be blinking **RED**.	
7. Enter the **Device ID** number and then tap **OK**.	
8. Tap on the **GREY** (Blank) padlock to finish provisioning.	
9. Once provisioning is complete, the App will display a **GREEN checkmark** and the Drive LED will be solid Blue, indicating that the datAshur BT Managed Drive has been provisioned and will be automatically detected by your Remote Management Console and ready to be assigned to a user. **Note:** If provisioning multiple Drives that are connected to a multi-port USB hub, repeat steps 6-9 for each and every Drive, one Drive at a time.	
10. You will now be prompted by your computer to format all provisioned datAshur BT Managed Drives. Refer to section 12 'Formatting the datAshur BT for Windows' or section 13 'Formatting the datAshur BT for mac OS'. **Note:** Once formatted, Admin is able to access the Drive and add data if necessary.	

4. How to Create Users via the Remote Management Console

1. Click on the following link to open the Remote Management Console, https://rm.bt.istorage-uk.com/Account/Login

2. Sign in using your Admin **Username** and **Password**.

3. After successfully signing in, the datAshur BT Remote Management Dashboard will open.

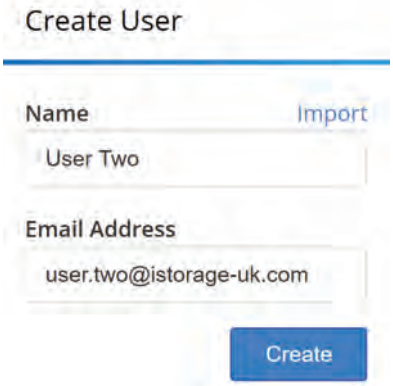


4. To add users, under '**Create User**', type in the **Name** and **Email Address** of the intended user and click on **Create** to send an email to the recipient containing their username and temporary password and a download link for the **datAshur BT Managed** App. All users that are created will appear on the Users Dashboard.

   To create and **import** a list of users, do the following:

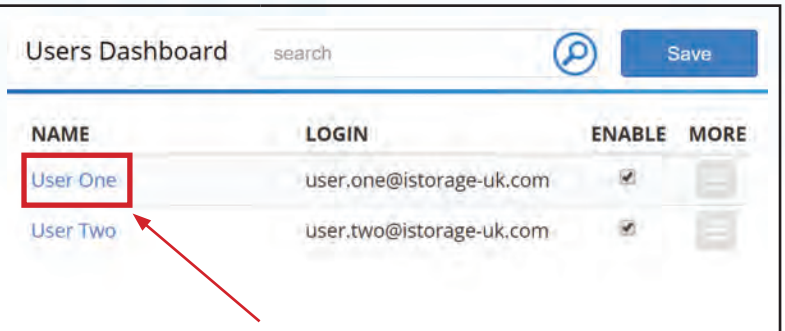
- In an excel spreadsheet, enter the name of each user followed by a semi-colon (**;**) before the email address. For example:
  '**User One;user.one@istorage-uk.com**'
  '**User Two;user.two@istorage-uk.com**'
- Save your spreadsheet as a '**.CSV**' file.
- Click on '**Import**'.
- In the '**Import Users**' dialog, click on '**Choose a file**', navigate to your file and then click '**Import**'.
- All the imported users will appear listed on the Users Dashboard.

Note: For detailed instructions on how to use the datAshur BT Managed App, please refer to the **datAshur BT Managed User Manual**.



5. How to Assign Drives to Users

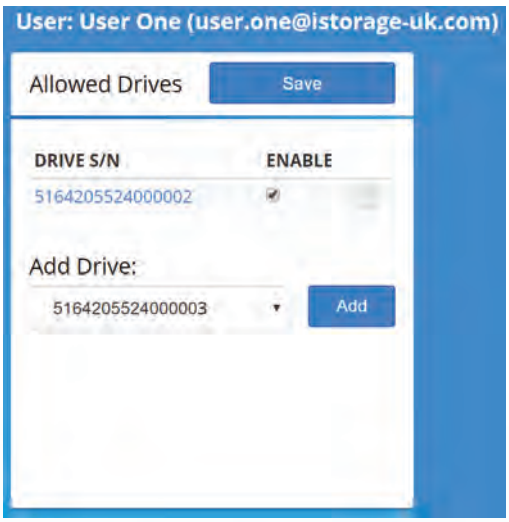
1. Sign in to the Remote Management Console.
2. In the '**Users**' tab under '**Users Dashboard**' click on the **User Name**. For example 'User One'.



3. Select a Drive from the dropdown menu under '**Add Drive**' to assign to the User then click on '**Add**' and finally click '**Save**'.

   The Drive, identified by the serial number will be assigned to the User and enabled. The example provided in the image bottom right shows that the '**Drive S/N**' ending in **02** has been assigned to **User One**.

Note: To assign additional Drives to users, repeat steps 2 and 3. You can also assign multiple Drives to one User.

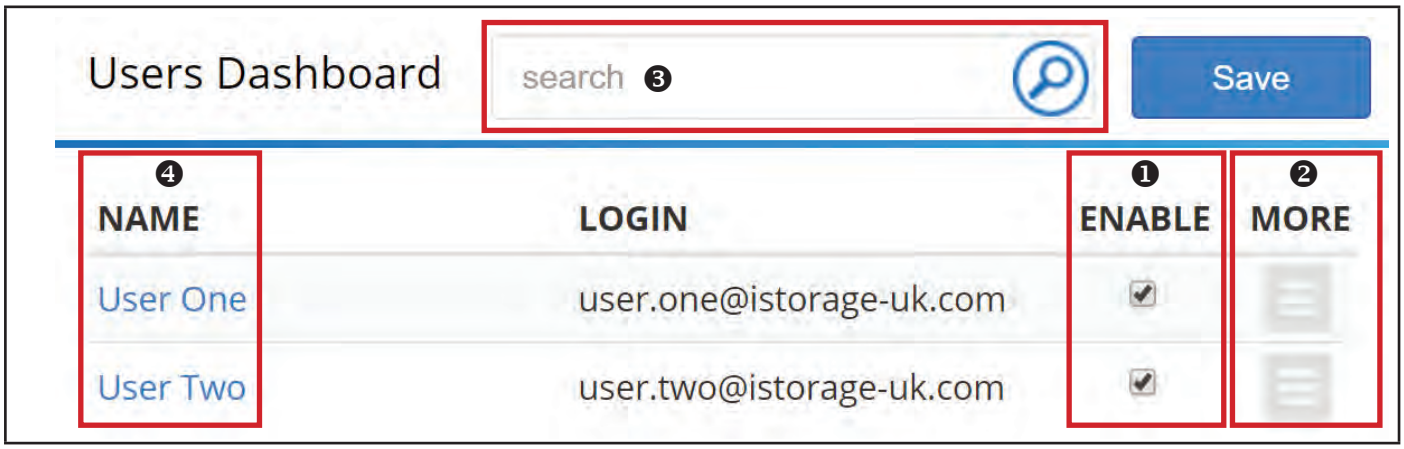


6. Managing Users Dashboard

Users Dashboard at a glance

Once all the datAshur BT Managed Drives have been assigned to users, Admin will now be able to perform the following actions from the **Users Dashboard**.

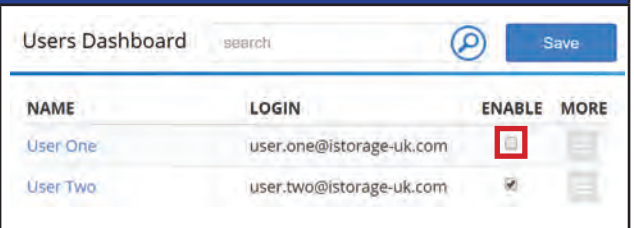
❶ **Enable or Disable User Access.**
❷ **Delete User from system & Reset the Users App password.**
❸ **Search for Users.**
❹ Click on a user name to open **Geo & Time-Fencing and Allowed Drives** panel.



How to Enable or Disable User Access

1. To Disable (prohibit) a User access to the datAshur BT Managed Drive, **uncheck** the **Check box** under '**Enable**' to clear the check mark and click **Save** to disable access for the user.

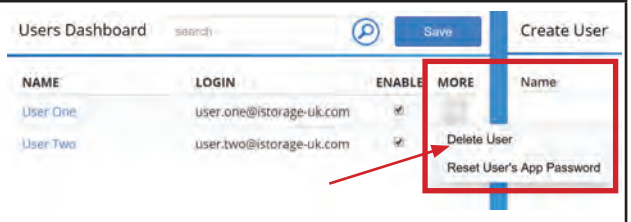
Note: To enable user access, click the **Check box** to restore the checkmark and click **Save**.



How to Delete a User from Remote Management

2. To delete a User from Remote Management, click on the **menu field** under **More**, then click **Delete User** and in the '**Delete Confirmation**' dialog, click **Delete**.

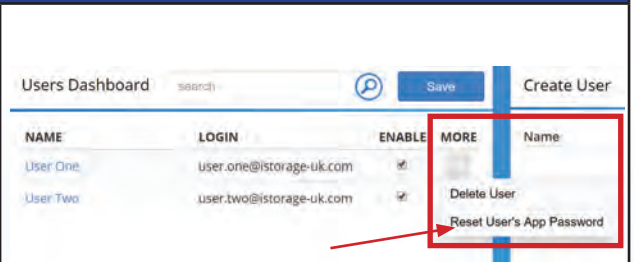
Note: To add the User back to Remote Management, refer to **section 4 - How to Create Users via the Remote Management Console**.



How to Reset User's datAshur BT Managed App Password

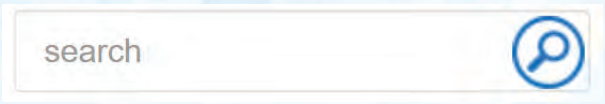
3. To reset a User's datAshur BT Managed App Password, click on the **menu field** under **More**, then click **Reset User's App Password** and then in the '**Reset Confirmation**' dialog, click **Reset**.

Note: Resetting the App password will not affect, nor change the Drive Password (default: 11223344).
When the App password has been reset, the user will receive an automated email containing a temporary password.



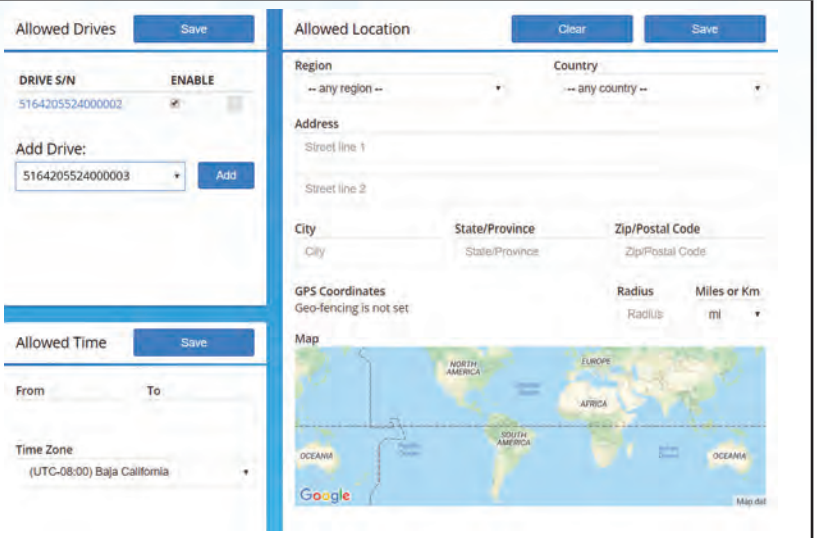
Search Bar

4. To search for a User, enter either the User's name or email address in the search bar and click on the magnifying glass.



Opening the Geo & Time-Fencing Panel

5. By clicking on a User name, you will open and be able to manage Geo-Fencing and Time-Fencing restrictions. Refer to **section 8 'How to Apply Geo & Time-Fencing Restrictions'**.

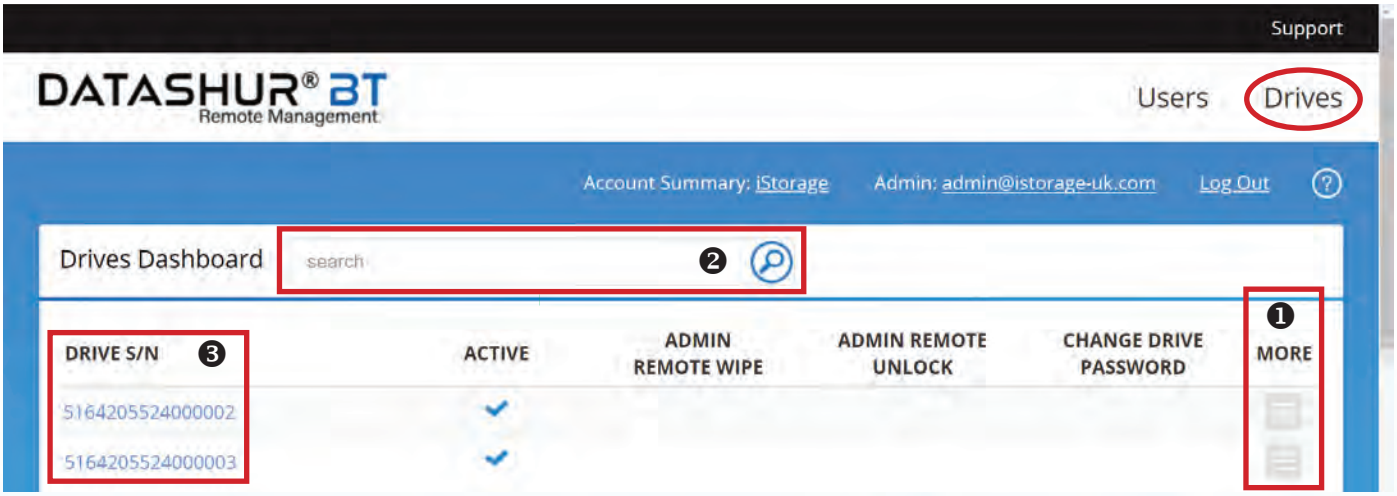


7. Managing Drives Dashboard

Click on '**Drives**' top right corner of screen to open the '**Drives Dashboard**' where Admin will be able to perform the following actions.

Drives Dashboard at first glance

❶ **How to Delete a Drive from Remote Management.**
❷ **Search by Drive Serial Number.**
❸ Click on a **Drive Serial Number** to open and **Manage Access Control.**

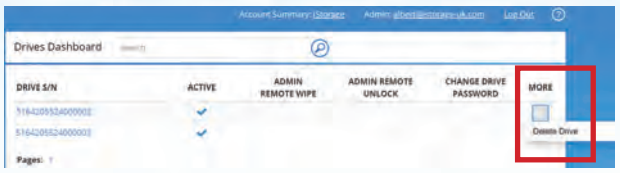


Note: The **checkmark** under '**ACTIVE**' indicates that the Drive is active and managed by Remote Management.

How to Delete a Drive from Remote Management

1. To delete a Drive from Remote Management, click on the **menu field** under **More**, then click **Delete Drive** and in the '**Delete Confirmation**' dialog referencing the Drive Serial Number to be deleted, click **Delete**.

Note: To add the Drive back to Remote Management, refer to **section 3 - How to Provision datAshur BT Managed Drives**.



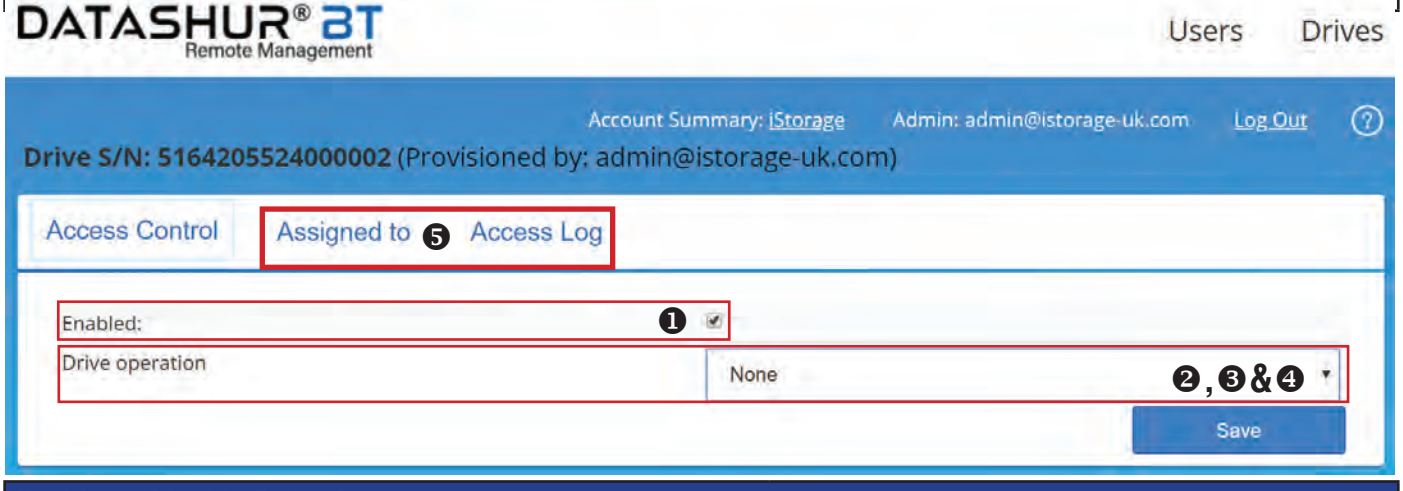
Search by Drive Serial Number

2. To search for a Drive, enter the Drive Serial Number in the search bar and click on the magnifying glass.

Managing Access Control

3. By clicking on a **Drive Serial Number (S/N)**, you will be able to access the Drive and manage the following actions remotely:

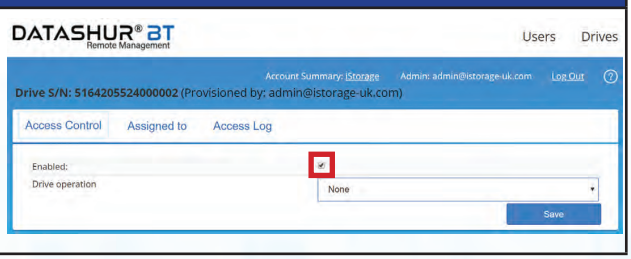
❶ **Enable** or **Disable** Drive Access.
❷ How to **Wipe a Drive** via Remote Management.
❸ How to **Change a Drive Password** via Remote Management.
❹ How to **Unlock a Drive** via Remote Management.
❺ Viewing **Assigned to** & **Access Log**.



Enable or Disable Drive Access

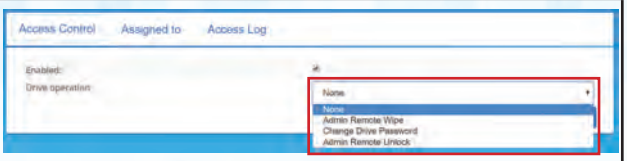
4. To **Disable** (prohibit) a User access to the datAshur BT Managed Drive, **uncheck** the **Check box** under '**Enable**' to clear the check mark and disable Drive access for the user.

Note: To enable user access, click the **Check box** to restore the checkmark.

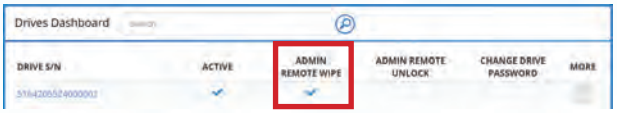


How to Wipe a Drive via Remote Management

6. Click on the drop down menu under **Drive operation** and then select '**Admin Remote Wipe**' (Reset) and click '**Save**'. A '*Drive changes have been saved*' confirmation message will be displayed.



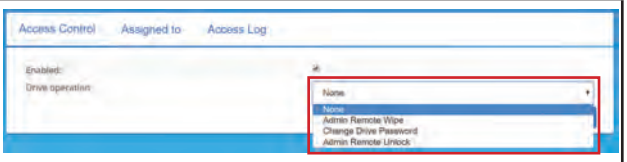
Note: Once 'Admin Remote Wipe' has been activated, a **check mark** will be displayed under '**ADMIN REMOTE WIPE**' in '**Drives Dashboard**', indicating that '**Remote Wipe**' is pending and will be activated the next time the datAshur BT Managed Drive is connected to the datAshur Managed App.



The check mark will clear (unchecked) as soon as the Drive is connected to a computer, indicating the Drive has been remotely wiped (reset).

How to Change a Drive Password via Remote Management

7. Click on the drop down menu under **Drive operation** then select '**Change Drive Password**' and then enter the **New Password** in the **Drive's User Password** field and click '**Save**'. A '*Drive changes have been saved*' confirmation message will be displayed.

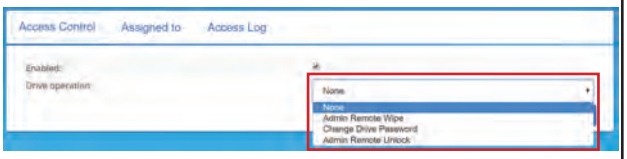


Note: Once 'Change Drive Password' has been activated, a **check mark** will be displayed under '**CHANGE DRIVE PASSWORD**' in '**Drives Dashboard**', indicating that action is pending and that the next time the datAshur BT Managed Drive is connected to the datAshur Managed App, the New Password will be required to unlock the Drive.

The check mark will clear (unchecked) as soon as the Drive is connected to a computer and unlocked using the New Password.

How to Unlock a Drive via Remote Management

8. Click on the drop down menu under **Drive operation** and then select '**Admin Remote Unlock**' and click '**Save**'. A '*Drive changes have been saved*' confirmation message will be displayed.



Note: Once 'Admin Remote Unlock' has been activated, a **check mark** will be displayed under '**ADMIN REMOTE UNLOCK**' in '**Drives Dashboard**', indicating that action is pending and that the next time the datAshur BT Managed Drive is connected to a computer the Drive will be unlocked without entering the Drive User Password. This is a '**One-Time**' action only.

The check mark will clear (unchecked) as soon as the Drive is connected to a computer and remotely unlocked.

Viewing Assigned to & Access Log

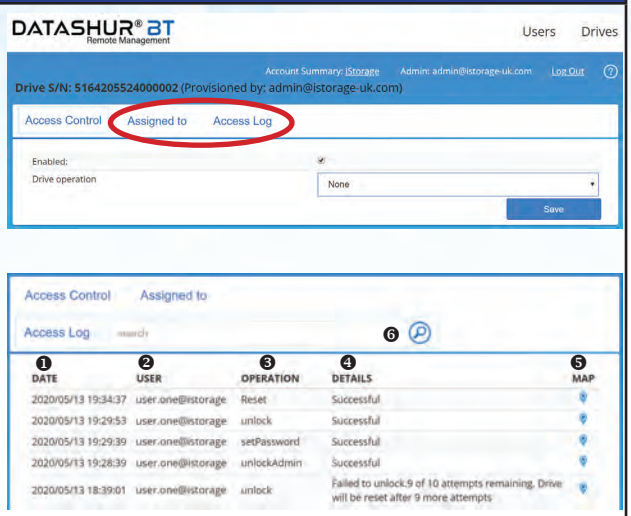
Assigned to

9. The '**Assigned to**' tab contains the name of the User the Drive has been assigned to, or names of Users if the Drive is assigned to more than one user.

Access Log

The 'Access Log' contains the following information:

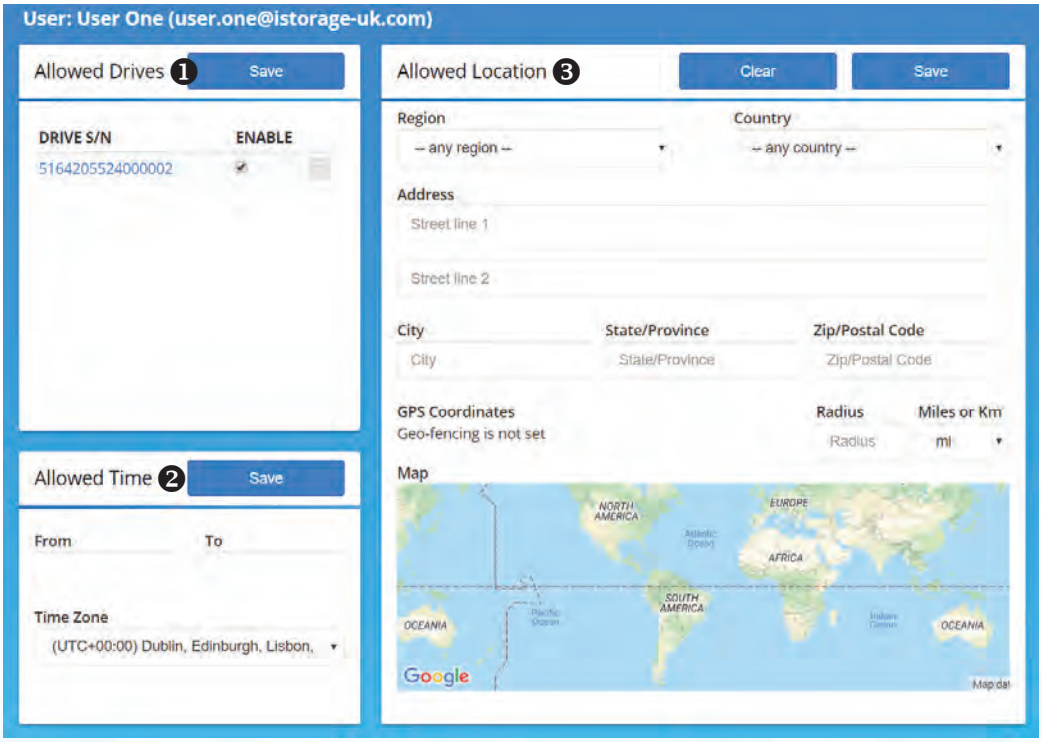
❶ Date and Time of when the User accessed the Drive.
❷ User's email address.
❸ Type of operation performed, i.e, 'Unlock' / 'Reset' etc.
❹ Details of Drive access
❺ Click on the '**Map**' icon to view the location of where the Drive was last accessed.
❻ Search by 'Type of operation performed' to filter.



8. How to Apply Geo & Time-Fencing Restrictions

Geo & Time-Fencing at first glance

❶ **Allowed Drives -** Enable/Disable or Delete Drive
❷ **Allowed Time -** Time-Fencing
❸ **Allowed Location -** Geo-Fencing



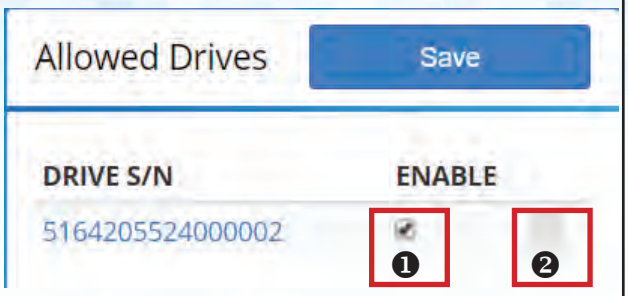
Allowed Drives

1. To Disable (prohibit) a User access to the datAshur BT Managed Drive, click the **Check box** (**1**) under '**Enable**' to clear the check mark and click **Save** to disable access for the User.

Note: To enable User access, click the **Check box** to restore the check mark and click **Save**.

2. To delete a Drive from Remote Management, click on the **menu field** (**2**), then click **Delete Drive** and in the '**Delete Confirmation**' dialog referencing the Drive Serial Number to be deleted, click **Delete**.

Note: To add the Drive back to Remote Management, refer to **section 3 - How to Provision datAshur BT Managed Drives**.

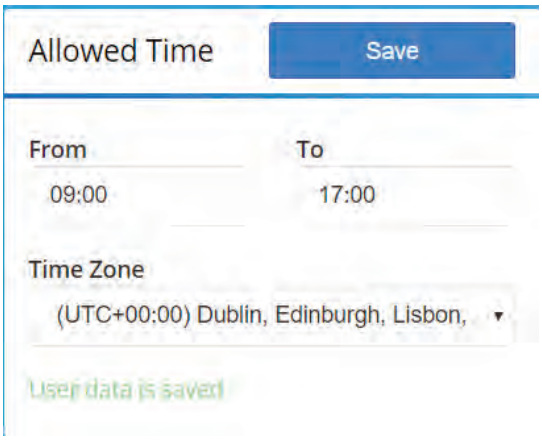


How to set Time-Fencing Restrictions

Time-Fencing can be applied to any individual User restricting the use of a Drive to within a specific time frame, for instance between, '**From 09:00**' - '**To 17:00**' only.

1. To Set Time-Fencing, click in the '**From**' field and either select the time, or type in manually and do the same with the '**To**' field. Then select your '**Time Zone**' from the drop down menu and click **Save**. A '**User data is saved**' message will be displayed as confirmation.

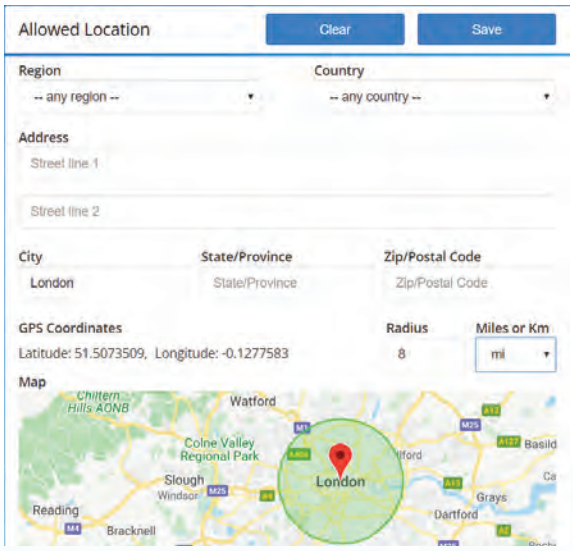
Note: To clear your time selection, click on the '**From**' and '**To**' fields and delete the entries, then click **Save**.



How to set Geo-Fencing Restrictions

A User's access can be restricted by setting the '**Allowed Location**' as follows:

1. **Region:** User access can be set by '**Region**', for instance 'Europe'.
2. **Country:** First select the '**Region**' and then select the '**Country**' from the drop down menu.
3. **Address:** Complete the '**Address**' field including Zip/Postal Code to restrict User access to that Address only.
4. **City:** Enter a name of a '**City**', for instance London.
5. **State/Province:** Restrict User access to a specific State or Province.
6. **Zip/Postal Code:** Restrict User Access to a specific Zip/Postal Code.
7. **Radius:** To expand the 'Allowed Location' radius, enter a value under **Radius** and then choose either '**Miles or Km**'.
8. Click '**Save**' to apply your restrictions or click '**Clear**' to remove all values.

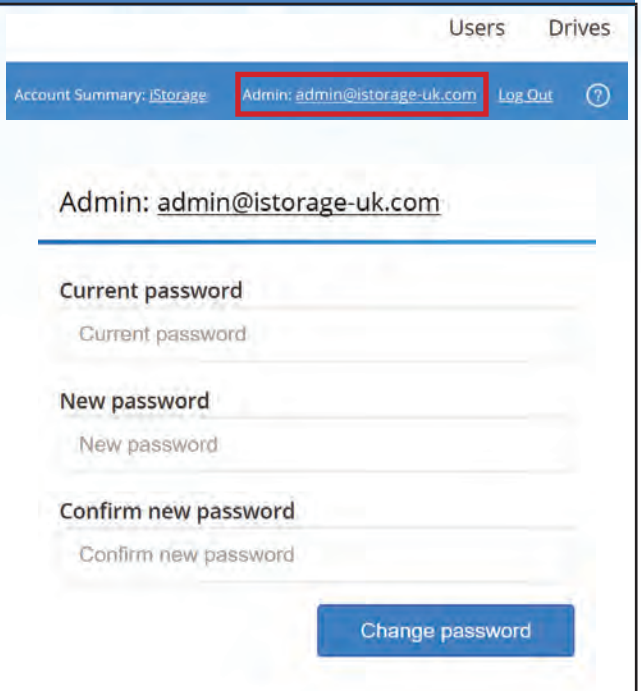


9. How to Change the Admin Password

To change the Admin Password, do the following:

1. Click on the '**Admin's email address**'.
2. Enter your '**Current Password**' followed by your '**New Password**' then '**Confirm New Password**' and finally click '**Change Password**'.

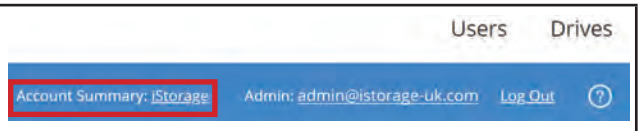
Note: Changing the Admin Password for the **Remote Management Console** will automatically update and change the Password for the **datAshur BT Admin App** to be the same. Remember the Admin Password is the same for both, the **Remote Management Console** and the **datAshur BT Admin App**.



10. Account Summary

To access and view your Account information, do the following:

1. Click on the name of the account next to '**Account Summary**' and then navigate through the following tabs:
   - **Summary**: View information relating to your valid License including the number of Admin's, User's and Drives.
   - **Admin Contacts:** View details of all enrolled Admin's, including email addresses, mobile numbers and date and time of Admin's last login.
   - **User Contacts:** View the User names, email addresses and date and time of User's last login.
   - **Drives Activity:** View list of all Serial Numbers, when they were provisioned and by whom, last login attempt and User's email addresses.



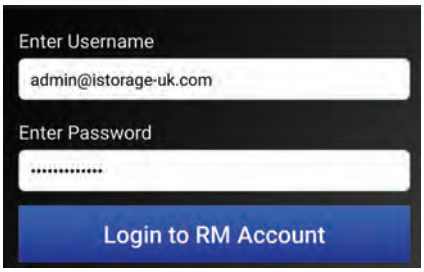
11. How to Provision a Non-Managed Drive

You are able to provision a previously used '**Managed**' Drive into a stand-alone '**Non-Managed**' Drive that will only work with the **datAshur BT Personal App** available to download on the Apple App Store and Google Play.

To start provisioning and set the security parameters as a non-managed Drive, proceed with the following steps.

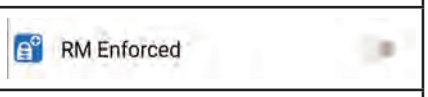
1. Open your **datAshur BT Admin App** and enter your **Username** and **Password** and then tap on **Login to RM (**Remote Management**) Account.**

Note: Your Username and Password for both the datAshur BT Admin App and the iStorage web based Remote Management Console are the same.



2. After successfully logging in, the **Drive Settings** menu will open ready for you to review and apply your security settings as described below:

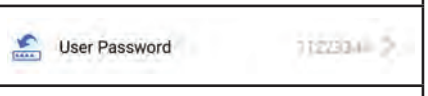
- **RM Enforced:** Switch the **GREEN** light **OFF.** Remote Management disabled.

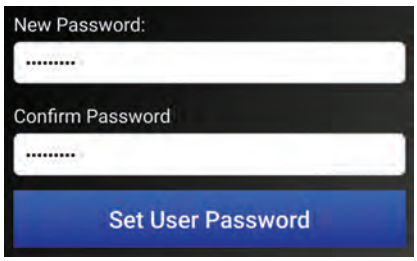


- **User Password:** The datAshur BT ships with a **default password** (**11223344**). To change the default password, tap on '**User Password**' and then **enter** and **confirm** your New **7-15** character Password and finally tap on '**Set User Password**'.

  Password Requirement: Password must be 7-15 characters in length and cannot contain only consecutive or repetitive numbers or letters.

  Note: For security reasons, we strongly recommend that each user change the default or Admin set password to their own unique 7-15 character password once the Drive has been issued to them.

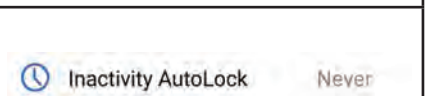


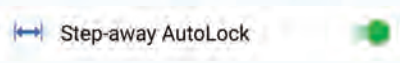
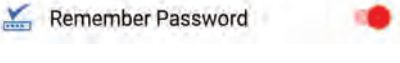
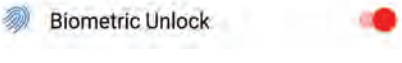
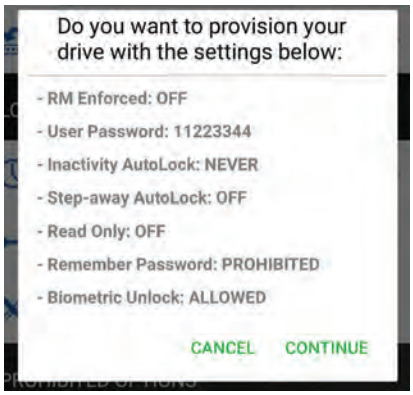


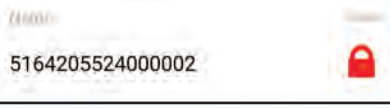
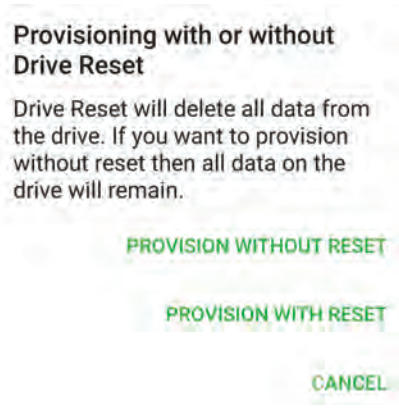
- **Inactivity AutoLock:** To protect against unauthorised access if the Drive is unlocked and unattended, the datAshur BT can be set to automatically lock after a pre-set amount of time. In its default state, the datAshur BT Unattended Inactivity AutoLock feature is turned off (Never) but can be set to autolock between **1 - 60** minutes.

  To set a time limit, tap on Inactivity AutoLock and then tap to choose your desired length of time.

  Note: When Admin sets the Inactivity AutoLock, the User is prohibited from disabling this feature.



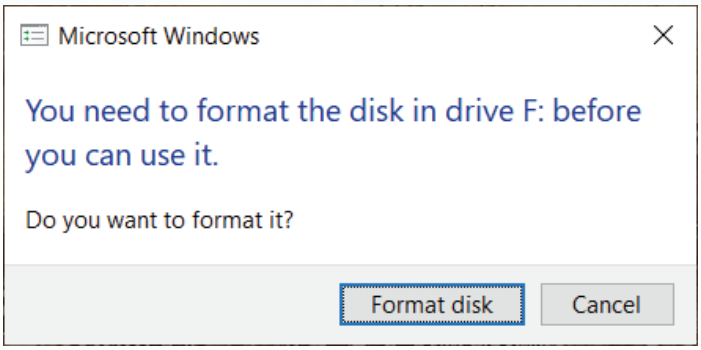
• **Step-away AutoLock:** The Step-away AutoLock is switched off by default, if enabled (**GREEN** light on), this will set the Drive to lock when a User's Smartphone (Android/iOS) is moved approximately 5 meters away from the datAshur BT Drive. **Note:** When Admin enables Step-away AutoLock, the User is prohibited from disabling this feature.	
• **Set Read Only:** The Read Only feature is switched off by default, when enabled (**GREEN** light on), the Drive will be set as Read Only/Write Protect. **Note:** When Admin enables Read Only, the User is prohibited from disabling this feature.	
• **Remember Password:** The Remember Password feature is operational (ON) by default, enabling Users to set their Drives to unlock without entering their password. To disable this feature and prohibit Users from setting their Drives to unlock without entering a password, tap on the greyed out switch to prohibit (**RED** light on). **Note:** When Admin **prohibits** Remember Password (**RED** light on), the User cannot enable this feature.	
• **Biometric Unlock:** The Biometric Unlock feature is operational (ON) by default, enabling Users to set a Biometric Unlock to access their Drives. To disable this feature and prohibit Users from setting a Biometric Unlock to access their Drives, tap on the greyed out switch to prohibit (**RED** light on) **Note:** When Admin **prohibits** Biometric Unlock (**RED** light on), the User cannot enable this feature.	
3. Tap to Confirm your Drive Settings.	
4. Tap **Continue** to provision the datAshur BT Drive with your preferred settings.	

5. Make a note of the **Device ID** number printed on the USB connector and **connect** the datAshur BT Managed Drive to a powered USB port.	
6. Tap on the **RED** padlock. **Note:** The Drive LED will be blinking **RED**.	
7. Enter the **Device ID** number and then tap **OK**.	
8. If provisioning a previously used Drive that has not been Reset proceed as follows, otherwise skip this step (if Drive has been reset) and proceed to step 9. • **Provision With Reset:** Tap on '**Provision With Reset**' and proceed to step 9. • **Provision Without Reset:** Tap on '**Provision Without Reset**' and proceed to step 10. **Note:** Provisioning Without Reset will NOT delete any data previously stored on the Drive being provisioned.	
9. Tap on the **GREY** (Blank) padlock to finish provisioning.	
10. Once provisioning is complete, the App will display a **GREEN checkmark** and the Drive LED will be solid **Blue**, indicating that the datAshur BT Drive has been provisioned.	
11. If the Drive was Provisioned With Reset (step 8), you will be prompted by your computer to format the Drive. Refer to section 12 'Formatting the datAshur BT for Windows' or section 13 'Formatting the datAshur BT for mac OS'. **Note:** Once formatted, Admin is able to access the Drive and add data if necessary.	

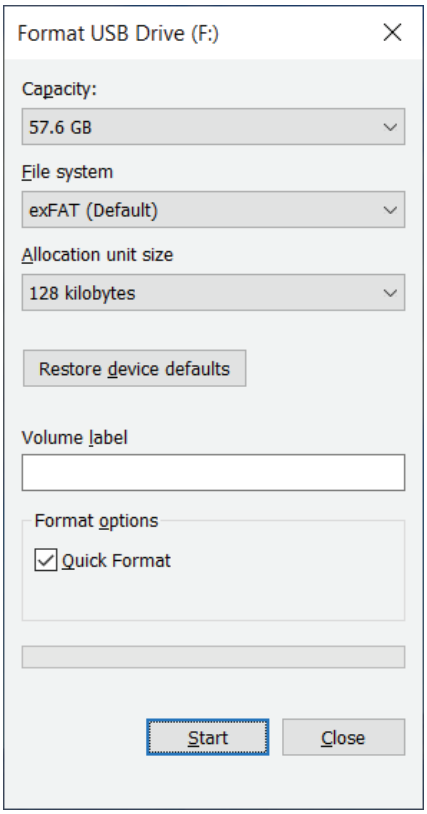
12. Formatting the datAshur BT for Windows

To format your datAshur BT on Windows, please do the following:

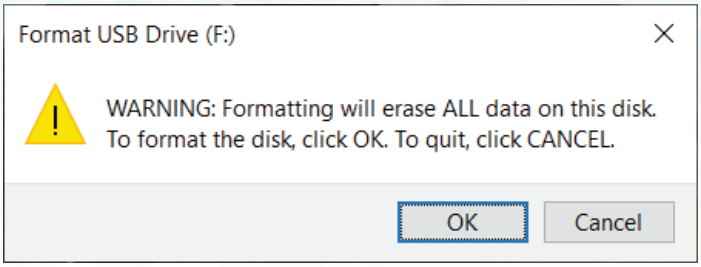
1. The system will prompt you with the **Format** window.



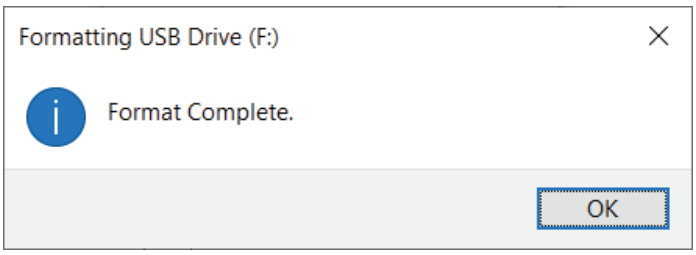
2. Press Format disk and Format USB Drive window will open.



3. Enter a name for the drive on the Volume label. The name of the drive will eventually appear on the Desktop. The File System dropdown menu lists the available drive formats that the windows supports. Select FAT32 or exFAT as per your requirement.
4. Click **Start**.
5. Click **OK** to continue with formatting the drive.



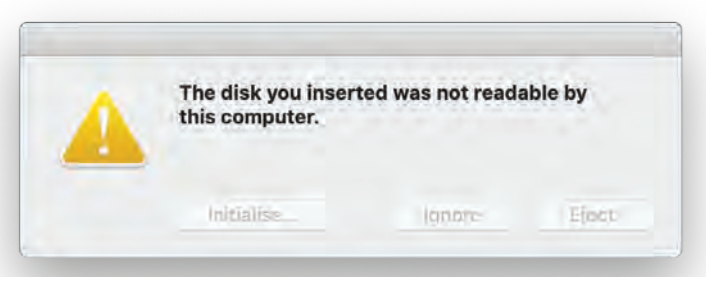
6. The procedure will finish formatting the drive and confirm that formatting has been completed.



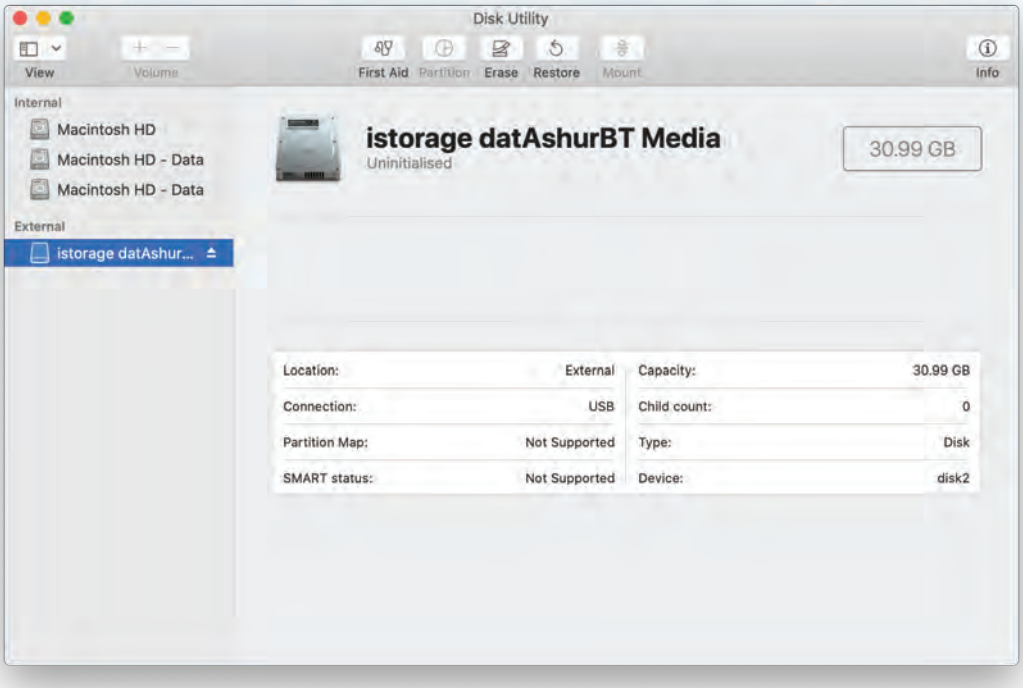
13. Formatting the datAshur BT for mac OS

To format your datAshur BT on mac OS, please do the following:

1. The system will prompt you with the **INITIALISE** window.

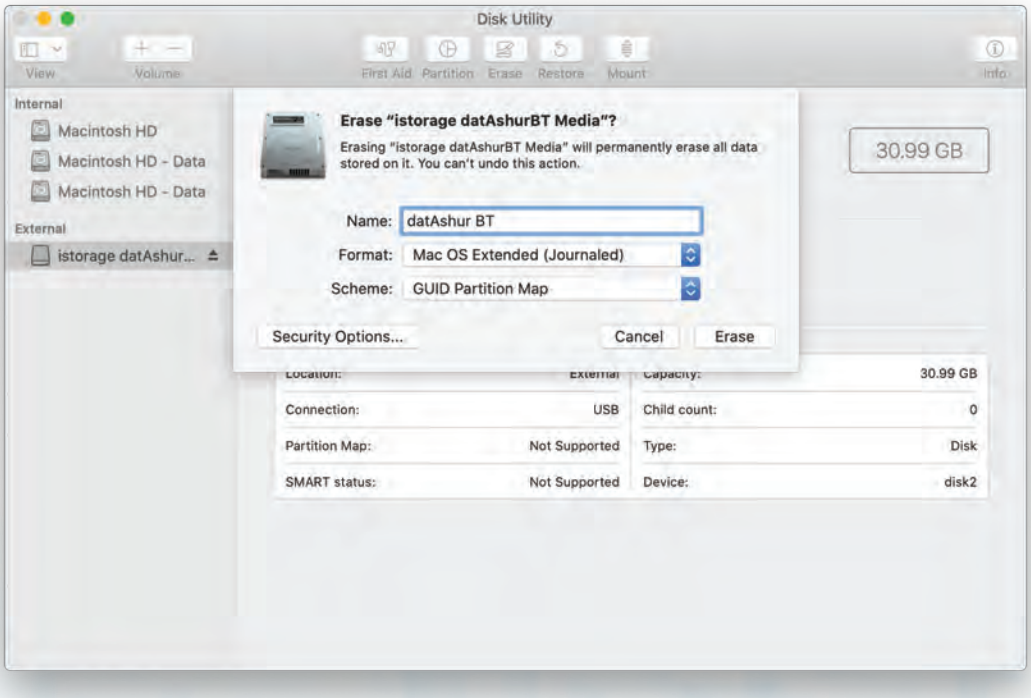


2. Press **INITIALISE**, open Disk Utility select the iStorage datAshur BT in the Disk Utility window.

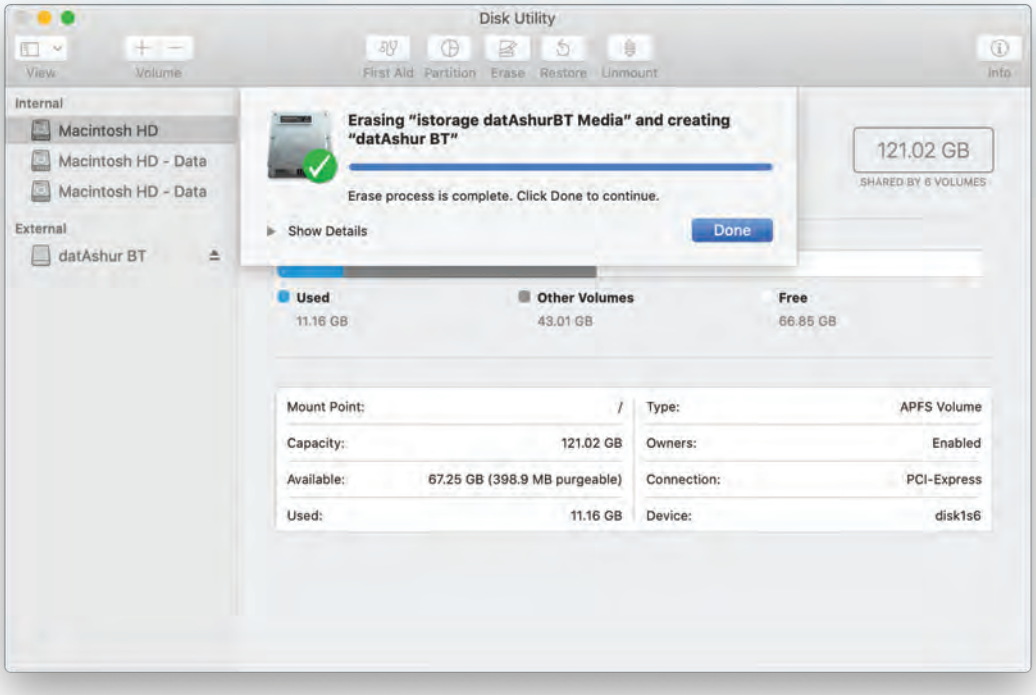


3. Choose **Erase** from the contextual menu.

4. Enter a name for the drive, the default name is Untitled. The name of the drive will eventually appear on the Desktop. Select a scheme and volume format to use. The Volume Format dropdown menu lists the available drive formats that the Mac supports. The recommended format type is Mac OS Extended (Journaled) for macOS and MS-DOS for cross platform. The scheme format dropdown menu lists the available schemes to use.



5. Click **Erase**.
6. The formatted datAshur BT will appear in the **Disk Utility** window and will mount onto the desktop



14. Technical Support

iStorage provides the following helpful resources for you:

iStorage's Website
https://www.istorage-uk.com

E-mail correspondence
support@istorage-uk.com

Telephone support with our Technical Support Department on **+44 (0) 20 8991 6260**.
iStorage's Technical Support Specialists are available from 9:00 a.m. to 5:30 p.m.
GMT - Monday through Friday.

15. 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

DATASHUR® BT
ADMIN MANUAL

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 DE L'ADMINISTRATEUR

Précautions liées aux interférence électromagnétiques

Cet équipement a été testé et déclaré conforme aux limites des appareils numériques de Classe B, en accord avec le chapitre 15 du règlement de la FCC. Ces limites sont fixées de façon à garantir une protection raisonnable contre les interférences nuisibles dans une installation résidentielle. Cet équipement génère, utilise et peut émettre de l'énergie radiofréquence. En cas de non-respect des consignes d'installation et d'utilisation, il est susceptible de provoquer des interférences nuisibles avec les communications radio. Il n'existe toutefois aucune garantie concernant l'absence d'interférences dans une installation spécifique. Si cet équipement provoque des interférences nuisibles avec la réception radio ou TV (ce qui peut être déterminé en allumant et en éteignant l'appareil), l'utilisateur est invité à essayer de résoudre ce problème en adoptant une ou plusieurs des solutions suivantes :

- Réorienter ou déplacer l'antenne de réception.
- Éloigner l'équipement du récepteur.
- Brancher l'équipement sur une prise appartenant à un circuit différent de celui auquel le récepteur est connecté.
- Demander de l'aide au revendeur ou à un technicien radio/TV expérimenté.

Précautions

Tout changement ou toute modification apporté(e) sans l'approbation expresse du tiers responsable de la conformité peut avoir pour conséquence d'annuler le droit de l'utilisateur à utiliser cet appareil. Les interférences électromagnétiques de haute intensité peuvent gêner le fonctionnement normal du produit. Dans ce cas, réinitialisez simplement le produit pour rétablir son fonctionnement normal en suivant le manuel d'instructions. S'il vous est impossible de rétablir le fonctionnement normal du produit, veuillez l'utiliser à un autre endroit. »

Cet appareil est conforme aux dispositions de la partie 15 des règles de la FCC, ainsi qu'aux normes RSS exemptes de licence d'Industrie Canada. Son utilisation est soumise aux deux conditions suivantes : (1) cet appareil ne doit pas provoquer d'interférences nuisibles, et (2) cet appareil doit accepter toutes les interférences reçues, y compris celles qui pourraient provoquer un fonctionnement non souhaité.

Exposition aux radiofréquences

L'appareil a été évalué de façon à assurer une conformité aux exigences générales en matière d'exposition aux radiofréquences.

La clé datAshur BT d'iStorage est fabriquée par iStorage Ltd., elle utilise la technologie DataLock® sous licence de ClevX, LLC. Brevet américain. www.istorage-uk.com/clevx-patents

Sommaire

Introduction ... 33
Contenu de l'emballage ... 33
Liens utiles ... 33
Agencement de la clé USB datAshur BT ... 34
Les différents voyants LED du lecteur et leur signification ... 34
1. **Enregistrement** ... 35
2. **Comment s'enregistrer en tant qu'administrateur (Admin)** ... 36
3. **Comment provisionner des clés datAshur BT gérées** ... 37
4. **Créer des utilisateurs en utilisant la Console de gestion à distance** ... 40
5. **Attribuer des clés aux utilisateurs** ... 41
6. **Gérer le tableau de bord des utilisateurs** ... 42
Le tableau de bord des utilisateurs en un coup d'œil ... 42
Activer et désactiver l'accès des utilisateurs ... 42
Retirer des utilisateurs de la gestion à distance ... 42
Réinitialiser le mot de passe de l'application datAshur BT gérée de l'utilisateur ... 42
Barre de recherche ... 43
Ouverture du panneau Géo-blocage et Restriction temporelle ... 43
7. **Gérer le tableau de bord des clés** ... 43
Le tableau de bord des clés en un coup d'œil ... 43
Retirer des clés de la gestion à distance ... 44
Rechercher une clé par Numéro de série ... 44
Gérer les contrôles d'accès ... 44
Activer ou Désactiver l'accès à la clé ... 44
Effacer une clé via la Gestion à distance ... 45
Modifier le mot de passe d'une clé via la Gestion à distance ... 45
Déverrouiller une clé via la Gestion à distance ... 45
Affichage des journaux attribués et Accès aux journaux ... 46
8. **Appliquer des restrictions géographiques et temporelles** ... 46
Les restrictions géographiques et temporelles en un coup d'œil ... 46
Clés autorisées ... 47
Définir des restrictions géographiques et temporelles ... 47
Définir des restrictions géographiques ... 47
9. **Modifier le mot de passe administrateur** ... 48
10. **Récapitulatif du compte** ... 48
11. **Provisionner une clé non gérée** ... 49
12. **Formater la clé datAshur BT pour le système d'exploitation Windows** ... 52
13. **Formater la clé datAshur BT pour le système d'exploitation Mac OS** ... 53
14. **Assistance technique** ... 56
15. **Informations sur la garantie et la demande de retour de produits** ... 56

Introduction

Merci pour votre acquisition d'une licence de gestion destiné à la datAshur BT, une clé USB 3.2 (gén. 1) à chiffrement matériel qui utilise la connexion Bluetooth de votre smartphone (iOS et Android) afin de le transformer en un dispositif d'authentification sans filde l'utilisateur permettant un accès sécurisé aux données stockées sur la clé USB datAshur BT gérée.

La clé datAshur BT gérée utilise un chiffrement matériel AES-XTS 256 bits de grade militaire (chiffrement intégral du disque), celui-ci chiffre toutes les données stockées sur la clé en temps réel.

La clé datAshur BT gérée est conçue pour être gérée à distance via la Console Web de gestion à distance d'iStorage. Cette console permet à l'administrateur de contrôler où et quand la clé est accessible au moyen du Géo-blocage et de la Restriction temporelle. D'autres fonctionnalités incluent l'effacement à distance, le déverrouillage à distance, la modification des mots de passe, la désactivation des accès et bien plus encore.

Contenu de l'emballage

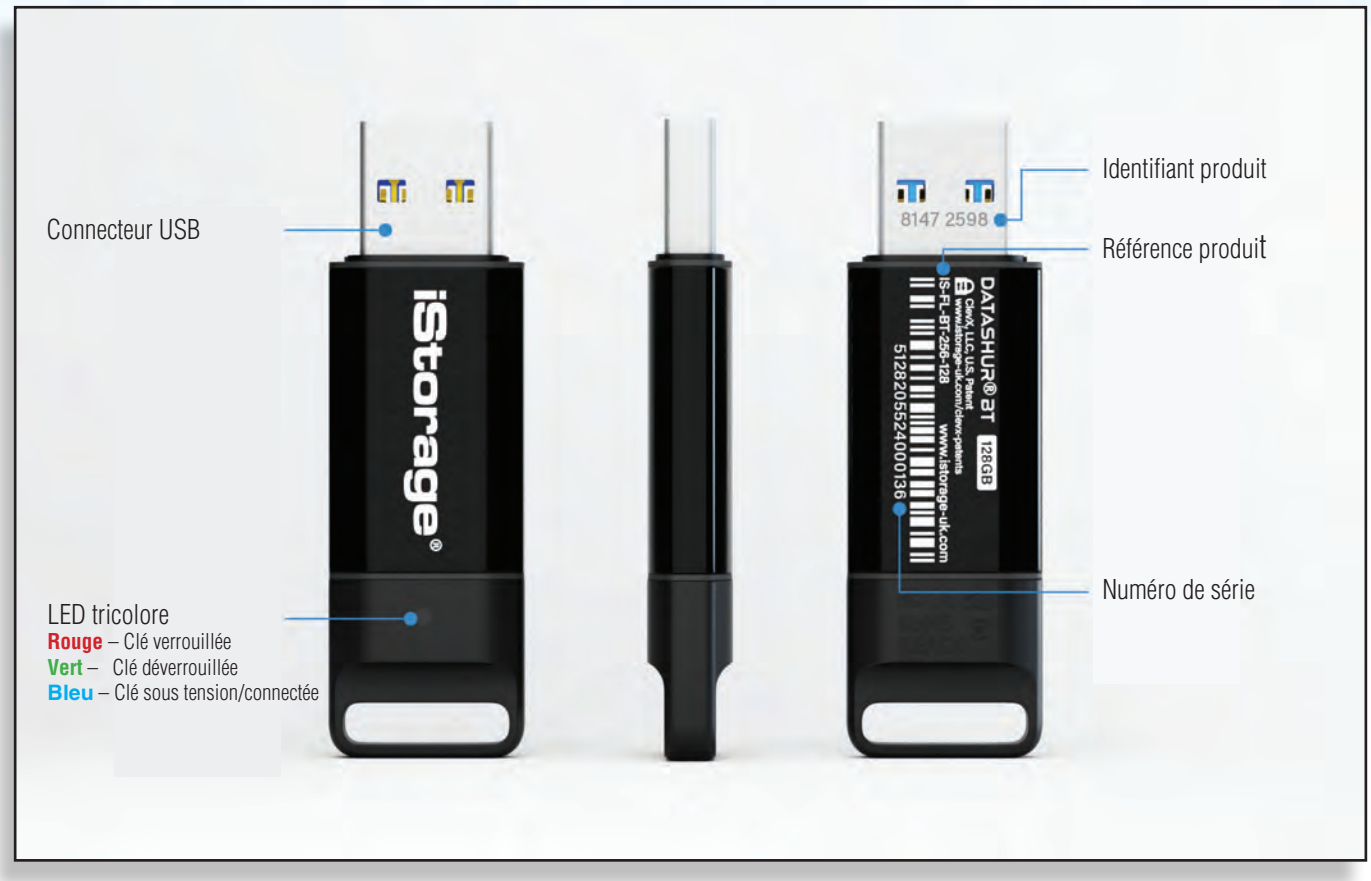
- Clé datAshur BT d'iStorage
- GDR - Guide de démarrage rapide pour la clé datAshur BT personnelle non gérée

Remarque : L'emballage de la clé USB datAshur BT contient un Guide de démarrage rapide qui s'applique uniquement à la clé datAshur BT personnelle « non gérée ». Veuillez ignorer le contenu du Guide de démarrage rapide, consultez plutôt les instructions contenues dans ce manuel.

Liens utiles

1. Lien d'enregistrement du compte administrateur de la datAshur BT :
   https://rm.bt.istorage-uk.com/Account/Register
2. Lien pour accéder a la console de gestion à distance :
   https://rm.bt.istorage-uk.com/Account/Login
3. Manuel d'utilisation de la clé USB datAshur BT gérée :
   https://istorage-uk.com/product-documentation/
4. Guide de démarrage rapide de la clé USB datAshur BT gérée :
   https://istorage-uk.com/product-documentation/
5. Manuel d'utilisation de la clé USB datAshur BT Personnelle :
   https://istorage-uk.com/product-documentation/

Agencement de la clé USB datAshur BT



Les différents voyants LED du lecteur et leur signification

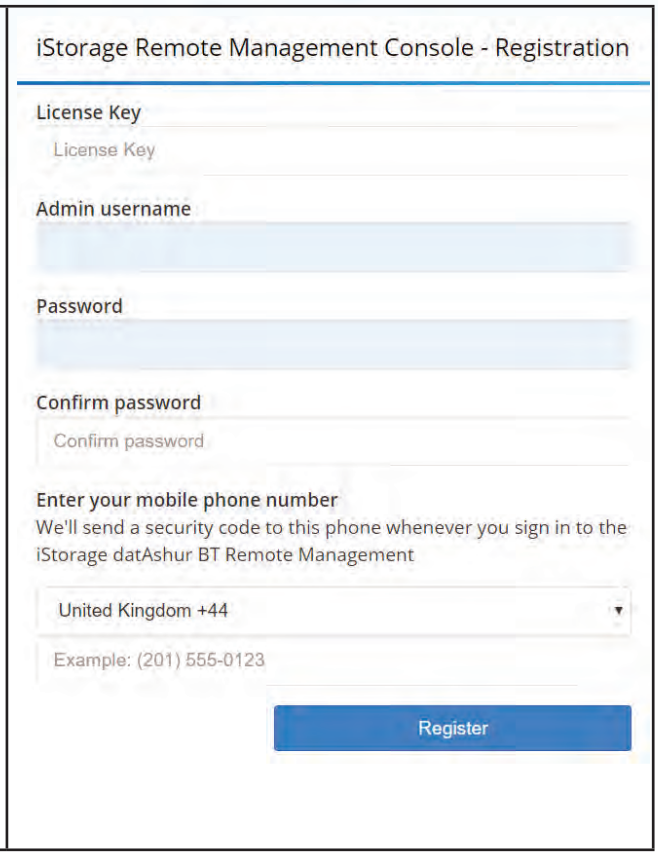
Voyants LED	État du voyant LED	Description
	Tous les voyants LED clignotent une fois.	La clé datAshur BT effectue un auto-test lorsqu'elle est branchée au port USB d'un ordinateur.
	Rouge fixe	Verrouillée : l'application datAshur BT est fermée.
	Clignote en rouge	Verrouillée : l'application datAshur BT est ouverte.
	Bleu fixe	La clé USB datAshur BT est déverrouillée.
	Bleu fixe	La clé USB datAshur BT est déverrouillée et un transfert de données est en cours.

1. Enregistrement

Lorsque vous achetez une licence pour la Console de gestion à distance d'iStorage, vous recevez un e-mail contenant un « **Lien pour l'enregistrement** » accompagné d'une « **Clé de licence** », ces éléments vous permettent de démarrer le processus d'enregistrement de la façon décrite ci-dessous.

Ouvrez le lien suivant pour accéder à la page d'enregistrement, remplissez ensuite les différents champs comme indiqué ci-dessous.
https://rm.bt.istorage-uk.com/Account/Register

1. **Clé de licence :** reportez-vous à l'e-mail d'enregistrement d'iStorage, celui-ci contient votre clé de licence.
2. **Nom d'utilisateur de l'administrateur :** vous devez saisir ici une **adresse e-mail**, qui sera utilisée lors du processus de **Connexion de l'administrateur**.
3. **Mot de passe :** saisissez ici un mot de passe sécurisé.
4. **Confirmer le mot de passe :** saisissez à nouveau votre mot de passe pour le confirmer.
5. Sélectionnez votre **Pays** dans le menu déroulant, puis **Entrez votre numéro de téléphone portable** : Cela est requis pour « **L'authentification à deux facteurs** ».
6. Cliquez sur « **S'enregistrer** ».
7. Sur la page « **Activer la vérification en deux étapes** », saisissez le **Code à 6 chiffres** que vous avez reçu par SMS, puis cliquez sur **Suivant**.
8. Cliquez sur « **Terminé** ».



2. Comment s'enregistrer en tant qu'administrateur (Admin)

Avec la Console Web de gestion à distance d'iStorage, l'administrateur peut provisionner, définir des politiques de sécurité et disposer d'un contrôle et d'une visibilité complets sur l'ensemble des clés datAshur BT déployées dans l'organisation.

Pour configurer un compte d'administrateur, vous aurez besoin du **Nom d'utilisateur** et du **Mot de passe** que vous avez créés durant le processus d'enregistrement, selon les instructions de la « **Section 1 - Enregistrement** ». Poursuivez en observant les étapes suivantes.

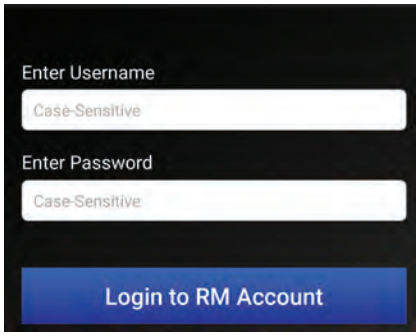
1. Téléchargez et installez **l'application datAshur BT Administrateur** à partir de **l'App Store d'Apple** ou de **Google Play**, vous pouvez également **scanner directement le code QR** en utilisant votre smartphone pour la télécharger.

datAshur BT Admin App

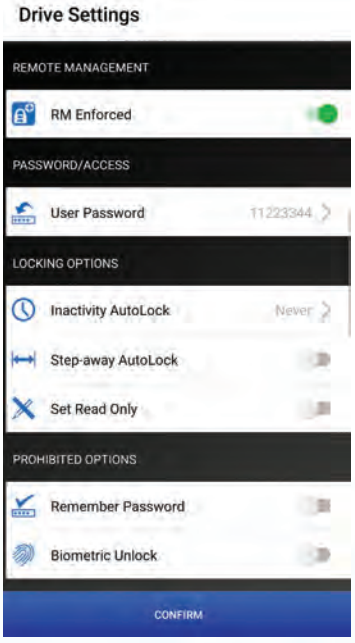
2. Dans le message contextuel, appuyez sur **Autoriser**.

3. Entrez votre **Nom d'utilisateur** et votre **Mot de passe**, appuyez ensuite sur **Se connecter au compte de la CGD** (Console de gestion à distance).

Remarque : Votre nom d'utilisateur et votre mot de passe liés à l'application datAshur BT Administrateur sont identiques à ceux de la Console Web de gestion à distance.



Une fois la connexion établie, le menu **Paramètres de la clé** s'ouvre, vous pouvez alors l'utiliser pour définir les politiques de sécurité et provisionner toutes les clés datAshur BT gérées de la façon décrite dans la section suivante.

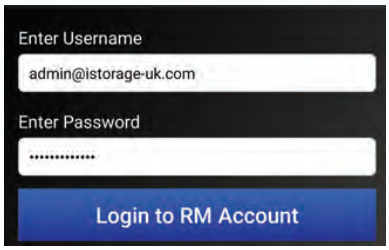


3. Comment provisionner des clés datAshur BT gérées

Après avoir effectué la configuration en tant qu'administrateur (section 2), vous devrez d'abord provisionner l'ensemble des clés datAshur BT gérées que vous prévoyez de gérer via la Console de gestion à distance, à raison d'une clé à la fois.

Pour démarrer le provisionnement, procédez comme suit.

1. Ouvrez votre **application datAshur BT Administrateur,** entrez votre **Nom d'utilisateur** et votre **Mot de passe**, appuyez ensuite sur **Se connecter au compte de la CGD** (Console de gestion à distance).



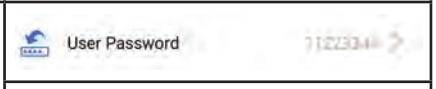
2. Une fois la connexion établie, le menu **Paramètres de la clé** s'ouvre, vous pouvez alors vérifier et appliquer vos paramètres de sécurité de la façon décrite ci-dessous :

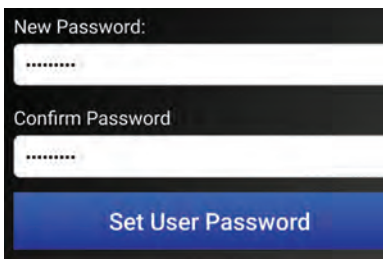
- **Appliqué par la gestion à distance :** Cette option est activée par défaut (voyant **VERT** allumé) et DOIT rester **ACTIVÉE** pour permettre le provisionnement de la gestion à distance. Lorsque cette option est désactivée, une clé peut être configurée de façon à fonctionner avec l'application non gérée (application datAshur BT : reportez-vous au manuel d'utilisation distinct).

- **Mot de passe de l'utilisateur :** La clé datAshur BT est livrée avec un **Mot de passe par défaut (11223344)** déjà défini. Pour changer le mot de passe par défaut, appuyez sur « **Mot de passe de l'utilisateur** », **entrez** et **confirmez** votre nouveau mot de passe composé de **7 à 15** caractères, puis appuyez sur « **Définir le mot de passe utilisateur** ».

  Exigences liées au mot de passe : le mot de passe doit comporter entre 7 et 15 caractères, il ne peut contenir que des chiffres ou des lettres consécutifs ou répétitifs.

  Remarque : pour des raisons de sécurité, nous recommandons vivement à chaque utilisateur de remplacer le mot de passe par défaut ou le mot de passe Administrateur par son propre mot de passe unique de 7 à 15 caractères une fois sa clé attribuée.

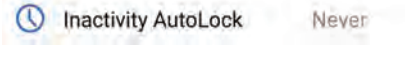




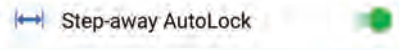
- **Verrouillage automatique d'inactivité :** pour se protéger des accès non autorisés pouvant survenir lorsque la clé est déverrouillée et non surveillée, la clé datAshur BT peut être configurée pour se verrouiller automatiquement au bout d'une période prédéfinie. Par défaut, la fonction Verrouillage automatique d'inactivité de datAshur BT est désactivée (Jamais), elle peut cependant être configurée pour se verrouiller automatiquement entre 1 et 60 minutes.

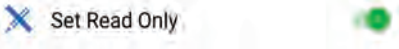
  Pour définir un délai, appuyez sur Verrouillage automatique d'inactivité, puis sélectionnez la durée souhaitée.

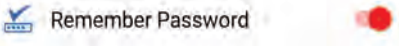
  Remarque : lorsque l'Administrateur active la fonction Verrouillage automatique d'inactivité, il devient impossible pour l'utilisateur ne la désactiver.

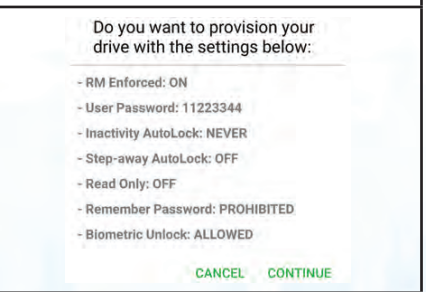


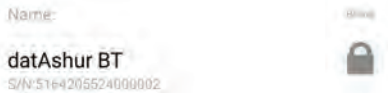
•	**Verrouillage automatique en cas d'éloignement :** la fonction Verrouillage automatique en cas d'éloignement est désactivée par défaut. Lorsqu'elle est activée (voyant **VERT** allumé), toutes les clés datAshur BT gérées étant déployées se verrouilleront lorsque le smartphone d'un utilisateur (fonctionnant sous Android/iOS) s'éloignera d'environ 5 mètres de la clé datAshur BT pendant plus de 5 secondes. **Remarque :** lorsque l'Administrateur active la fonction Verrouillage automatique en cas d'éloignement, il devient impossible pour l'utilisateur de la désactiver.
•	**Définir en Lecture seule uniquement :** la fonction Lecture seule est désactivée par défaut, lorsqu'elle est activée (voyant **VERT** allumé), toutes les clés datAshur BT gérées qui sont déployés seront définies en tant que clé en Lecture seule / Protégé en écriture. **Remarque :** Lorsque l'Administrateur active la fonction Lecture seule, il devient impossible pour l'utilisateur de la désactiver.
•	**Mémorisation du mot de passe :** La fonction Mémorisation du mot de passe est disponible (ACTIVÉE) par défaut, elle permet aux utilisateurs de configurer leurs clés de façon à ce que celles-ci mémorisent le mot de passe et ne le demandent pas lors du déverrouillage. Pour désactiver cette fonction (**recommandé**) et interdire aux utilisateurs de configurer leurs clés afin que celles-ci ne demandent pas de mot de passe au déverrouillage, appuyez sur le bouton bascule grisé (voyant **ROUGE** allumé). **Remarque :** lorsque l'administrateur **interdit** l'utilisation de la fonction Mémorisation du mot de passe (voyant **ROUGE** allumé), l'utilisateur ne peut pas activer cette fonction et devra saisir son mot de passe à chaque déverrouillage de sa clé.
•	**Déverrouillage biométrique :** la fonction Déverrouillage biométrique est disponible (ACTIVÉE) par défaut, elle permet aux utilisateurs de définir un déverrouillage biométrique pour l'accès à leurs clés. Pour désactiver cette fonction et interdire aux utilisateurs de configurer le Déverrouillage biométrique sur leurs clés, appuyez sur le bouton bascule grisé (voyant **ROUGE** allumé). **Remarque :** lorsque l'administrateur **interdit** l'utilisation du Déverrouillage biométrique (voyant **ROUGE** allumé), l'utilisateur ne peut pas activer cette fonction.
3.	Appuyez pour confirmer les nouveaux paramètres de la clé.
4.	Appuyez sur **Continuer** pour provisionner vos paramètres favoris sur toutes les clés datAshur BT gérées.









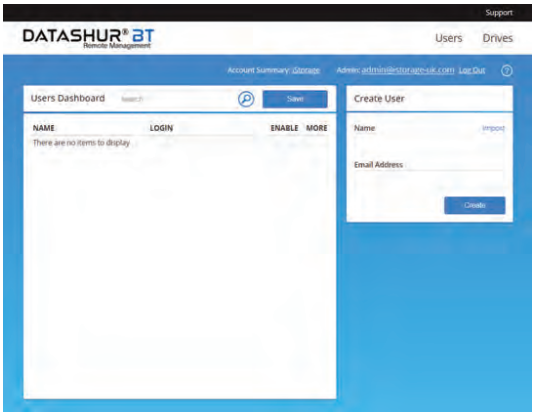
5. Notez le **Numéro d'identification de la clé** figurant sur le connecteur USB et **Connectez** la clé datAshur BT gérée à un port USB sous tension.	
6. Appuyez sur le cadenas **ROUGE**. **Remarque :** Le voyant de la clé clignote en ROUGE.	
7. Saisissez le **Numéro d'identification de la clé**, puis appuyez sur **OK**.	
8. Appuyez sur le cadenas **GRIS** (vide) pour terminer le provisionnement.	
9. Une fois le provisionnement terminé, l'application affiche une **coche VERTE**. Le voyant de la clé s'allume en bleu de manière fixe, indiquant que la clé datAshur BT gérée a été provisionnée et sera automatiquement détectée par votre console de gestion à distance, elle est par ailleurs prête à être attribuée à un utilisateur. **Remarque :** si vous provisionnez plusieurs clés connectées à un hub USB multiports, répétez les étapes 6 à 9 pour chaque clé, à raison d'une clé à la fois.	
10. Votre ordinateur vous demande désormais de formater l'ensemble des clés datAshur BT gérées qui sont provisionnées. Reportez-vous à la section 12 « Formater la clé datAshur BT pour le système d'exploitation Windows » ou à la section 13 « Formater la clé datAshur BT pour le système d'exploitation Mac OS ». **Remarque :** Une fois la clé formatée, l'administrateur peut accéder à celle-ci et y ajouter des fichiers si nécessaire.	

4. Créer des utilisateurs en utilisant la Console de gestion à distance

1. Cliquez sur le lien suivant pour ouvrir la Console de gestion à distance : https://rm.bt.istorage-uk.com/Account/Login

2. Connectez-vous en utilisant votre **Nom d'utilisateur** et votre **Mot de passe** d'administrateur.

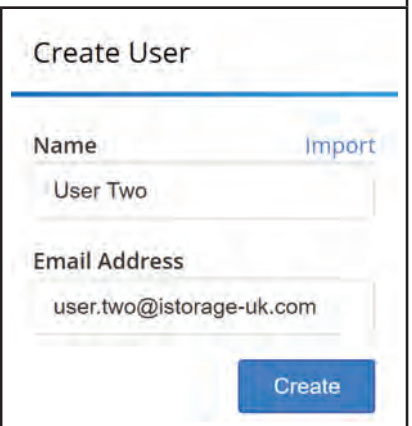
3. Une fois la connexion établie, le Tableau de bord de gestion à distance datAshur BT s'ouvre.



4. Pour ajouter des utilisateurs, sous « **Créer un utilisateur** », saisissez le **Nom** et l'**Adresse e-mai**l de l'utilisateur, puis cliquez sur **Créer** pour envoyer un e-mail au destinataire, l'e-mail contient son nom d'utilisateur et son mot de passe temporaire, ainsi qu'un lien de téléchargement pour l'application **datAshur BT gérée**. Tous les utilisateurs créés s'affichent sur le Tableau de bord des utilisateurs.

   Pour créer et **importer** une liste d'utilisateurs, procédez comme suit :

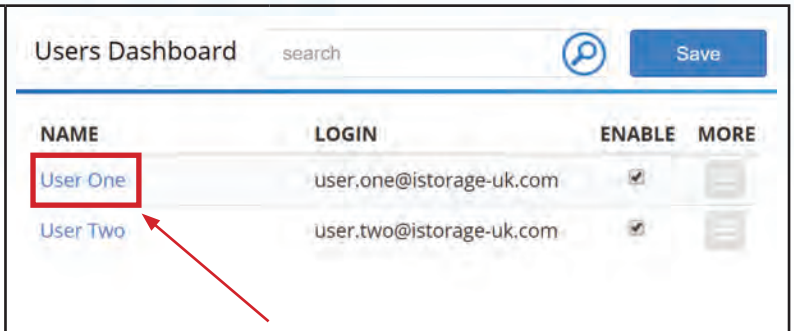
- Dans une feuille de calcul Excel, entrez le nom de chaque utilisateur suivi d'un point-virgule (;) avant l'adresse e-mail. Exemple : « **Utilisateur Un;utilisateur.un@istorage-uk.com** » « Utilisateur **Utilisateur;utilisateur.deux@storage-uk.com** »
- Enregistrez votre feuille de calcul en tant que fichier « .**CSV** ».
- Cliquez sur « **Importer** ».
- Dans la boîte de dialogue « **Importer des utilisateurs** », cliquez sur « **Choisir un fichier** », accédez à votre fichier et cliquez sur « **Importer** ».
- Tous les utilisateurs importés s'affichent sur le Tableau de bord des utilisateurs.



Remarque : pour des instructions détaillées sur l'utilisation de l'application datAshur BT gérée, veuillez vous reporter au **Manuel d'utilisation de la clé USB datAshur BT gérée**.

5. Attribuer des clés aux utilisateurs

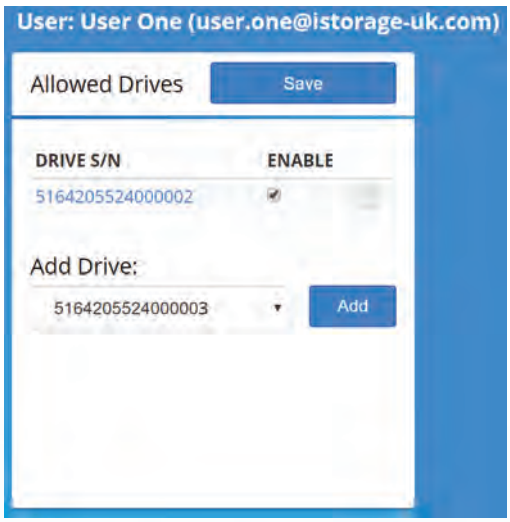
1. Connectez-vous à la Console de gestion à distance.
2. Dans l'onglet « **Utilisateurs** » situé sous « **Tableau de bord des utilisateurs** », cliquez sur le **Nom d'utilisateur**. Par exemple « Utilisateur 1 ».



3. Sélectionnez une clé dans le menu déroulant sous « **Ajouter une clé** » pour l'attribuer à l'utilisateur, puis cliquez sur « **Ajouter** ». Cliquez enfin sur « **Enregistrer** ».

   La clé, identifiée par son numéro de série, sera attribuée à l'utilisateur et désormais active. L'exemple fourni dans l'image en bas à droite indique que le « **N° de série de la clé** » se terminant par **02** a été attribué à l'**Utilisateur 1**.

Remarque : pour attribuer d'autres clés aux utilisateurs, répétez les étapes 2 et 3. Vous pouvez également attribuer plusieurs clés à un utilisateur.



6. Gérer le tableau de bord des utilisateurs

Le tableau de bord des utilisateurs en un coup d'œil

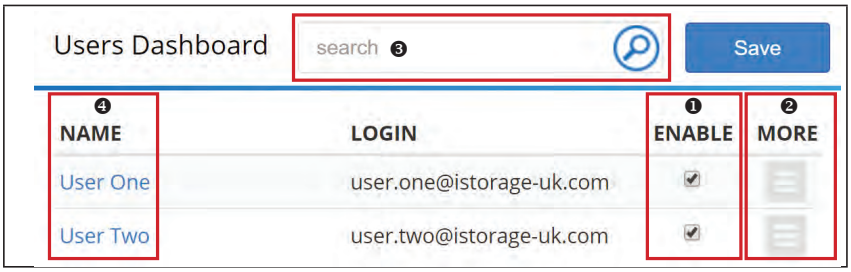
Une fois l'ensemble des clés datAshur BT gérées attribués aux utilisateurs, l'administrateur pourra désormais effectuer les actions suivantes à partir du **Tableau de bord des utilisateurs**.

❶ **Activer et désactiver l'accès des utilisateurs.**

❷ **Supprimer un utilisateur du système et réinitialiser le mot de passe de l'application Utilisateur.**

❸ **Rechercher des utilisateurs.**

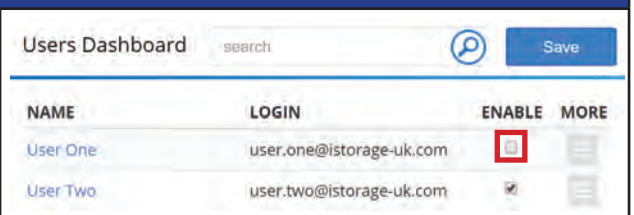
❹ Cliquez sur un nom d'utilisateur pour ouvrir le panneau **Restrictions géographiques et temporelles et Clés autorisées**.



Activer et désactiver l'accès des utilisateurs

1. Pour Désactiver (interdire) l'accès d'un utilisateur à la clé datAshur BT gérée, **décochez** la **Case** sous « **Activer** » afin de retirer la coche, puis cliquez sur **Enregistrer** pour désactiver l'accès de l'utilisateur.

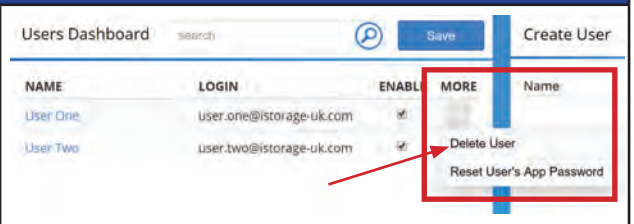
Remarque : pour activer l'accès de l'utilisateur, cliquez sur la **Case à cocher** pour restaurer la coche et cliquez sur **Enregistrer**.



Retirer des utilisateurs de la gestion à distance

2. Pour retirer un utilisateur de la Gestion à distance, cliquez sur le **champ Menu** situé sous **Plus**, puis cliquez sur **Supprimer l'utilisateur**, puis dans la boîte de dialogue « **Confirmation de suppression** », cliquez sur **Supprimer**.

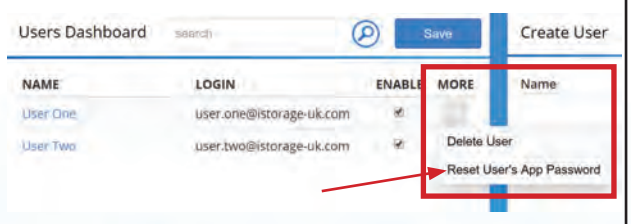
Remarque : pour ajouter l'utilisateur à la Gestion à distance, reportez-vous à la **section 4 - Créer des utilisateurs en utilisant la Console de gestion à distance**.



Réinitialiser le mot de passe de l'application datAshur BT gérée de l'utilisateur

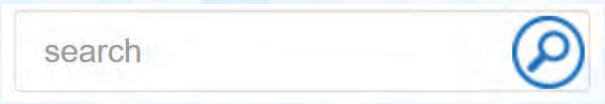
3. Pour réinitialiser le mot de passe de l'application datAshur BT gérée de l'utilisateur, cliquez sur le **champ Menu** situé sous Plus, puis sur **Réinitialiser le mot de passe de l'application de l'utilisateur**. Dans la boîte de dialogue « **Confirmation de la réinitialisation** », cliquez sur **Réinitialiser**.

Remarque : la réinitialisation du mot de passe de l'application n'affectera ni ne modifiera le mot de passe de la clé (par défaut : 11223344). Une fois le mot de passe de l'application réinitialisé, l'utilisateur recevra un e-mail automatisé contenant un mot de passe temporaire.



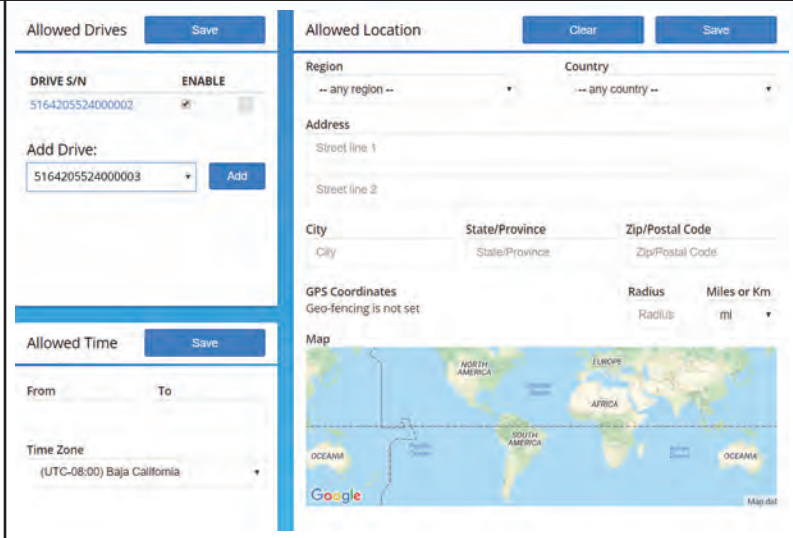
Barre de recherche

4. Pour rechercher un utilisateur, saisissez le nom d'utilisateur ou son adresse e-mail dans la barre de recherche, puis cliquez sur la loupe.



Ouverture du panneau Géo-blocage et Restriction temporelle

5. En cliquant sur un nom d'utilisateur, vous ouvrez et pouvez gérer les restrictions géographiques et temporelles. Reportez-vous à la **section 8 « Appliquer des restrictions géographiques et temporelles »**.

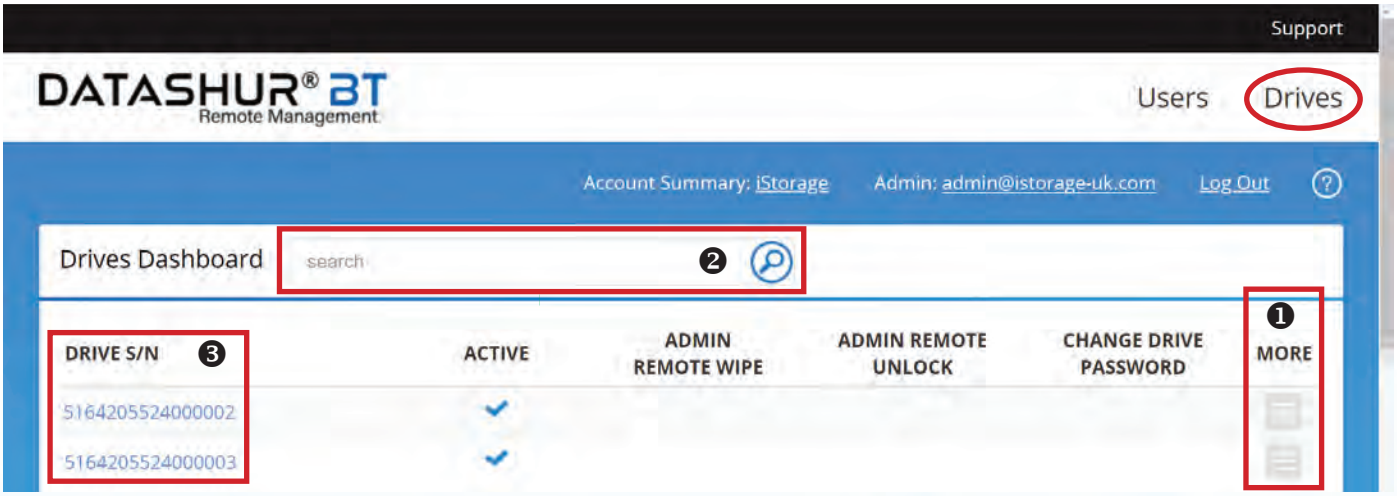


7. Gérer le tableau de bord des clés

Cliquez sur l'option « **Clés** » située dans le coin supérieur droit de de l'écran pour ouvrir le « **Tableau de bord des clés** », dans lequel l'administrateur pourra effectuer les actions suivantes.

Le tableau de bord des clés en un coup d'œil

❶ **Retirer des clés de la gestion à distance.**
❷ **Rechercher une clé par Numéro de série.**
❸ Cliquez sur un **Numéro de série de clé** pour ouvrir et **Gérer le contrôle d'accès**.

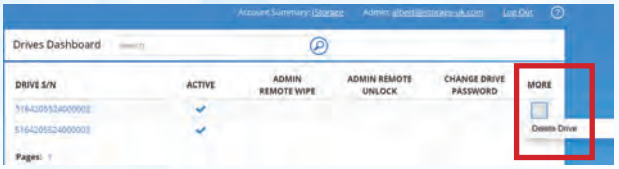


Remarque : la **coche** située sous « **ACTIVÉ** » indique que la clé est active et gérée au moyen de la gestion à distance.

Retirer des clés de la gestion à distance

1. Pour retirer une clé de la Gestion à distance, cliquez sur le **champ Menu** situé sous **Plus**, puis cliquez sur **Retirer la clé**. Dans la boîte de dialogue « **Confirmation de la suppression** » faisant référence au numéro de série de la clé à supprimer, cliquez sur **Supprimer**.

Remarque : pour ajouter une clé à la gérée à distance, reportez-vous à la **section 3 - Provisionner des clés datAshur BT gérées.**



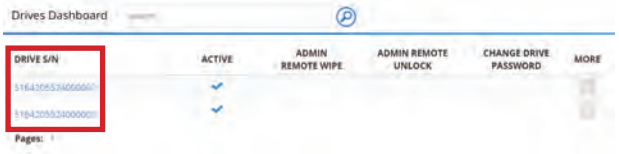
Rechercher une clé par Numéro de série

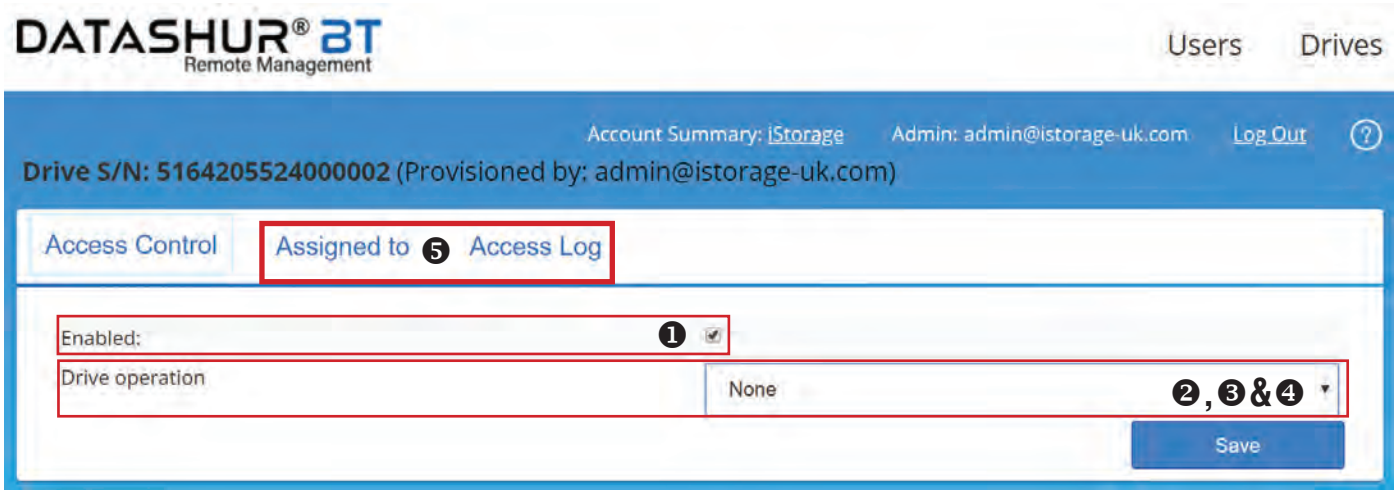
2. Pour rechercher une clé, saisissez le numéro de série de la clé dans la barre de recherche, puis cliquez sur la loupe.

Gérer les contrôles d'accès

3. En cliquant sur un **Numéro de série de clé**, il est possible d'accéder à la clé et de gérer les actions suivantes à distance :

❶ **Activer** ou **Désactiver** l'accès à la clé.
❷ **Effacer une clé** via la Gestion à distance.
❸ **Modifier le mot de passe d'une clé** via la Gestion à distance.
❹ **Déverrouiller une clé** via la Gestion à distance.
❺ **Affichage des journaux attribués** et **Accès aux journaux**.

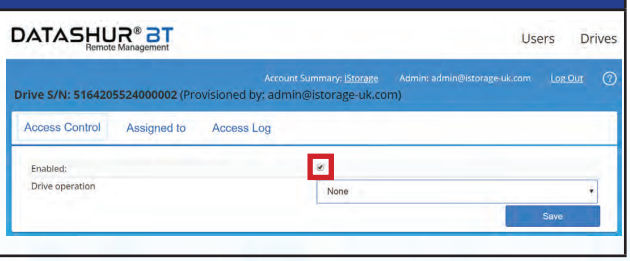




Activer ou Désactiver l'accès à la clé

4. Pour **Désactiver** (interdire) l'accès d'un utilisateur à la clé datAshur BT gérée, **décochez** la **Case à cocher** située sous « **Activer** » pour effacer la coche et désactiver l'accès à la clé de l'utilisateur.

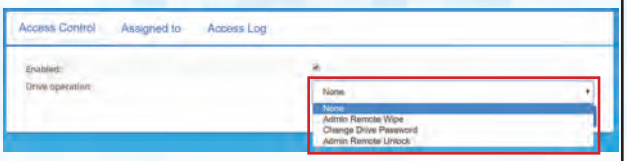
Remarque : pour activer l'accès de l'utilisateur, cliquez sur la Case à cocher pour restaurer la coche.

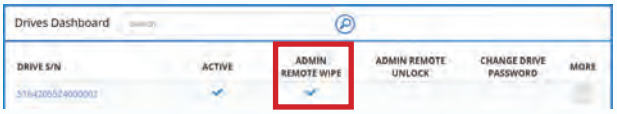


Effacer une clé via la Gestion à distance

6. Cliquez sur le menu déroulant situé sous **Fonctionnement de la clé**, sélectionnez « **Effacement à distance par l'administrateur** » (Réinitialiser), puis cliquez sur « **Enregistrer** ». Un message de confirmation « Les modifications apportées à la clé ont été enregistrées. » s'affiche.

Remarque : une fois l'« Effacement à distance par l'administrateur » activé, une **coche** s'affiche sous « **EFFACEMENT À DISTANCE PAR L'ADMINISTRATEUR** » dans « **Tableau de bord des clés** », indiquant que l'opération **Effacement à distance** » est en attente. Elle sera activée la prochaine fois que la clé datAshur BT gérée sera connectée à l'application datAshur gérée.
La coche disparaîtra (elle sera décochée) une fois la clé connectée à un ordinateur, ce qui indique que la clé a été effacée à distance (réinitialisée).

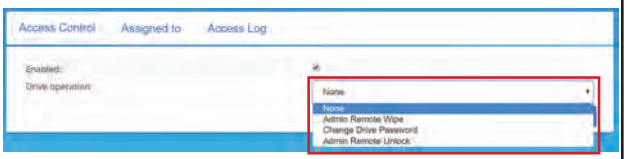




Modifier le mot de passe d'une clé via la Gestion à distance

7. Cliquez sur le menu déroulant sous **Fonctionnement de la clé**, sélectionnez « **Modifier le mot de passe de la clé** », puis entrez le **Nouveau mot de passe** dans le champ **Mot de passe utilisateur de la clé** et cliquez sur « **Enregistrer** ». Un message de confirmation « Les modifications apportées à la clé ont été enregistrées. » s'affiche.

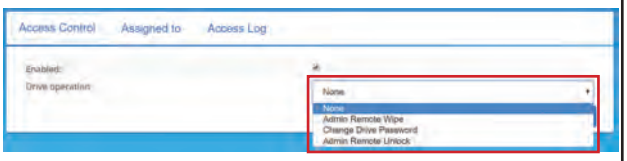
Remarque : Une fois la fonction « Modification du mot de passe de la clé » activée, une coche s'affiche sous « **MODIFIER LE MOT DE PASSE DE LA CLÉ** » dans « T**ableau de bord des clés** ». Cela indique que l'opération est en attente et que le nouveau mot de passe sera nécessaire pour déverrouiller la clé à la prochaine connexion de celle-ci à l'application datAshur BT gérée.
La coche disparaîtra (elle sera décochée) une fois la clé connectée à un ordinateur et déverrouillée à l'aide du Nouveau mot de passe.



Déverrouiller une clé via la Gestion à distance

8. Cliquez sur le menu déroulant situé sous **Fonctionnement de la clé**, sélectionnez « **Déverrouillage à distance par l'administrateur** », puis cliquez sur « **Enregistrer** ». Un message de confirmation « Les modifications apportées à la clé ont été enregistrées. » s'affiche.

Remarque : une fois la fonction « Déverrouillage à distance par l'administrateur » activée, une coche s'affiche sous « **DÉVERROUILLAGE À DISTANCE PAR L'ADMINISTRATEUR** » dans « **Tableau de bord des clés** ». Cela indique que l'opération est en attente et que la prochaine fois que l'utilisateur connecte la clé datAshur BT gérée à un ordinateur, la clé sera déverrouillée sans qu'il ne soit nécessaire de saisir le mot de passe de l'utilisateur de la clé. Cette opération en doit être effectuée « **qu'une fois** ».
La coche disparaîtra (elle sera décochée) une fois la clé connectée à un ordinateur et déverrouillée à distance.



Affichage des journaux attribués et Accès aux journaux

Attribué à

9. L'onglet « **Attribué à** » contient le nom de l'utilisateur auquel la clé a été attribuée (ou les noms des utilisateurs, lorsque la clé a été attribuée à plusieurs utilisateurs).

Accéder au journal

L'option « Accéder au journal » comporte les informations suivantes :

❶ La date et l'heure auxquelles l'utilisateur a accédé à la clé.

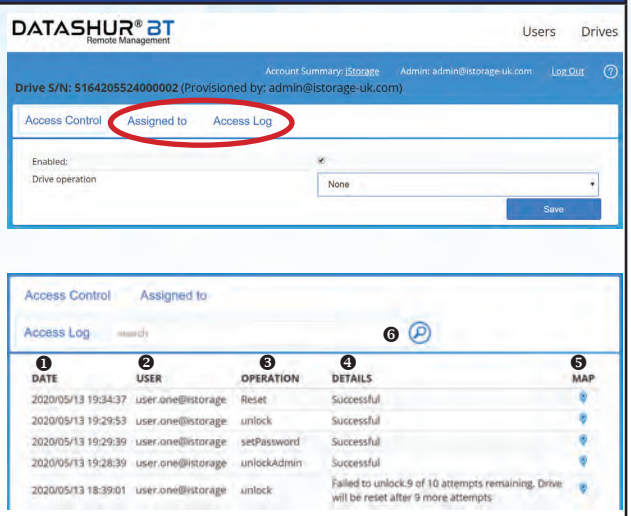
❷ L'adresse e-mail de l'utilisateur.

❸ Le type d'opération effectuée, par ex. « Déverrouiller » / « Réinitialiser », etc.

❹ Les détails des accès à la clé.

❺ Cliquez sur l'icône « **Carte** » pour afficher l'emplacement du dernier accès à la clé.

❻ Vous pouvez effectuer une recherche par « Type d'opération effectuée » pour filtrer les résultats.



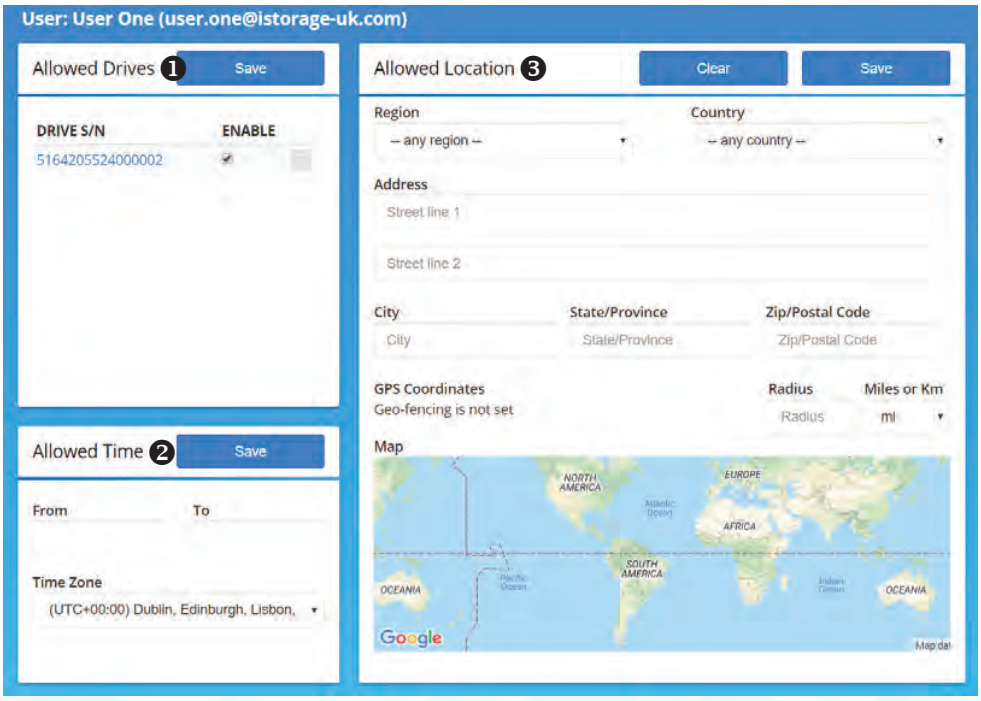
8. Appliquer des restrictions géographiques et temporelles

Les restrictions géographiques et temporelles en un coup d'œil

❶ **Clés autorisées** - Pour activer/désactiver ou supprimer une clé.

❷ **Temps admis -** Pour définir une restriction temporelle.

❸ **Zone géographique admise** - Pour définir un blocage géographique.



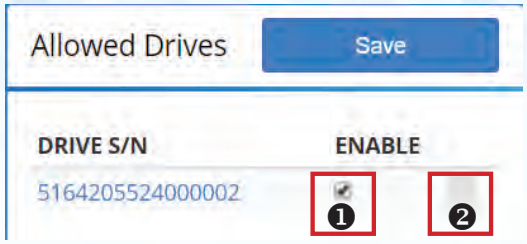
Clés autorisées

1. Pour Désactiver (interdire) l'accès d'un utilisateur à la clé datAshur BT gérée, cliquez sur la **Case à cocher** (**1**) située sous « **Activer** » pour retirer la coche, puis cliquez sur **Enregistrer** pour désactiver l'accès de l'utilisateur.

Remarque : pour activer l'accès de l'utilisateur, cliquez sur la Case à cocher pour restaurer la coche et cliquez sur Enregistrer.

2. Pour supprimer des clés de la Gestion à distance, cliquez sur le **champ Menu** (**2**). Cliquez sur **Supprimer la clé** et dans la boîte de dialogue « **Confirmation de la suppression** » faisant référence au numéro de série de la clé à supprimer, cliquez sur **Supprimer**.

Remarque : pour ajouter une clé à la gérée à distance, reportez-vous à la **section 3 - Provisionner des clés datAshur BT gérées**.

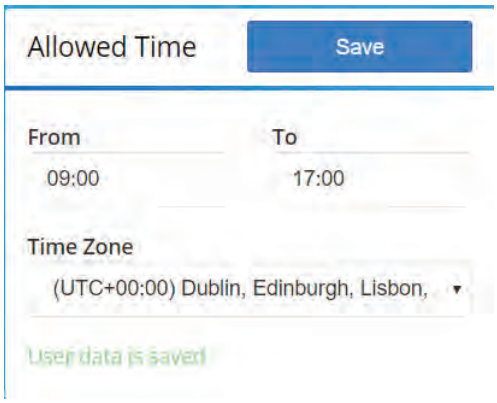


Définir des restrictions géographiques et temporelles

La fonction de restriction temporelle peut être appliquée à tout utilisateur afin de limiter l'utilisation d'une clé à une période spécifique, par exemple entre « **De 09h00** » à « **À 17h00** » uniquement.

1. Pour définir la restriction temporelle, cliquez dans le champ « **De** » et sélectionnez l'heure, ou saisissez-la manuellement, puis procédez de même pour le champ « **À** ». Sélectionnez ensuite votre « **Fuseau horaire** » dans le menu déroulant, puis cliquez sur **Enregistrer**. Un message « **Les données de l'utilisateur ont été enregistrées**. » s'affiche à titre de confirmation.

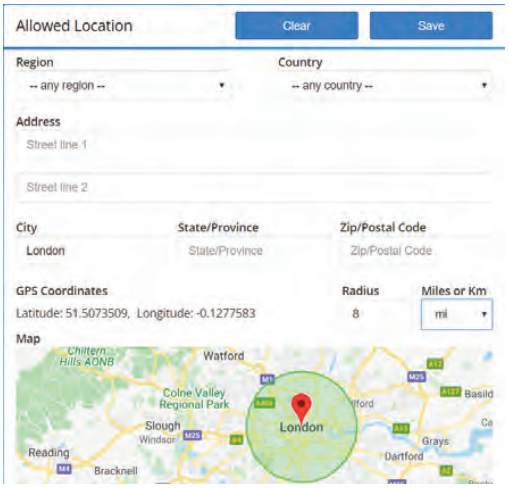
Remarque : pour effacer la période choisie, cliquez sur les champs « **De** » et « **À** », supprimez les entrées, puis cliquez sur **Enregistrer**.



Définir des restrictions géographiques

L'accès d'un utilisateur peut être restreint en définissant la « **Zone géographique autorisée** » comme suit :

1. **Région** : L'accès de l'utilisateur peut être défini par l'option « **Région** », par exemple « Europe ».
2. **Pays** : sélectionnez d'abord la « **Région** », puis sélectionnez le « **Pays** » dans le menu déroulant.
3. **Adresse** : remplissez le champ « **Adresse** », cela inclut le code postal, pour restreindre l'accès de l'utilisateur à cette adresse uniquement.
4. **Ville** : saisissez le nom d'une « **Ville** », par exemple Londres.
5. **Département** : pour restreindre l'accès de l'utilisateur à un état ou une province spécifique.
6. **Code postal :** pour restreindre l'accès de l'utilisateur à un code postal spécifique.
7. **Rayon** : pour étendre le rayon géographique « Emplacement autorisé », saisissez une valeur sous **Rayon**, puis choisissez **« Miles ou Km ».**
8. Cliquez sur « **Enregistrer** » pour appliquer vos restrictions, ou sur « **Effacer** » pour supprimer toutes les valeurs.

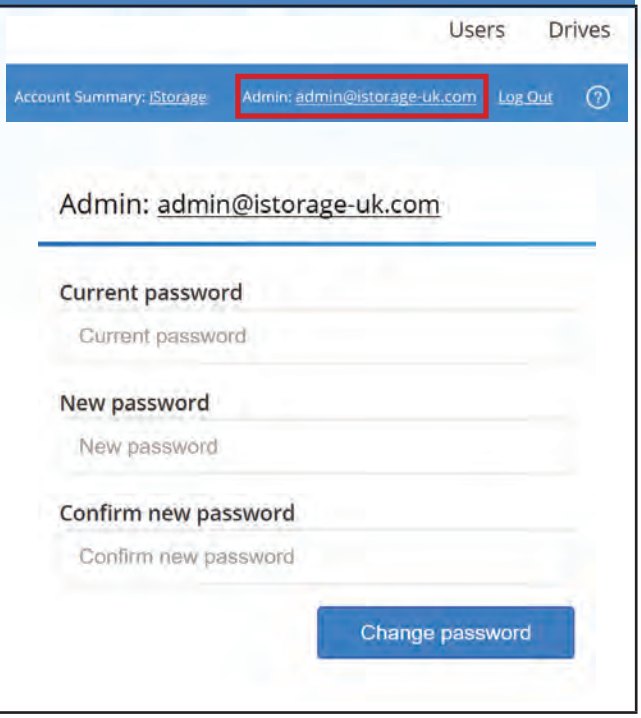


9. Modifier le mot de passe administrateur

Pour modifier le mot de passe administrateur, procédez comme suit :

1. Cliquez sur « **Adresse e-mail de l'administrateur** ».
2. Saisissez votre « **Mot de passe actuel** », votre « **Nouveau mot de passe** », puis saisissez à nouveau le mot de passe dans le champ « **Confirmer le nouveau mot de passe** ». Cliquez enfin sur « **Modifier le mot de passe** ».

Remarque : la modification du mot de passe administrateur de la Console de gestion à distance mettra automatiquement à jour et modifiera celui de l'application datAshur BT Administrateur. N'oubliez pas que le mot de passe administrateur est le même pour les deux environnements : la **Console de gestion à distance** et l'**application datAshur BT Administrateur**.

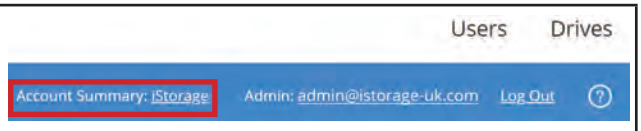


10. Récapitulatif du compte

Pour accéder aux informations de votre compte et les afficher, procédez comme suit :

1. Cliquez sur le nom du compte près de « **Récapitulati du compte** », puis parcourez les onglets suivants :

- **Récapitulatif** : pour afficher les informations relatives à votre licence valide, cela inclut le nombre d'administrateurs, d'utilisateurs et de clés.
- **Informations sur les administrateurs** : pour afficher les informations de tous les administrateurs inscrits, cela inclut les adresses e-mail, les numéros de téléphone portable, la date et l'heure de la dernière connexion de l'administrateur.
- **Informations sur les utilisateurs** : pour afficher les noms des utilisateurs, leur adresse e-mail, la date et l'heure de leur dernière connexion de chaque utilisateur.
- **Activité des clés** : pour afficher la liste de tous les numéros de série, la date à laquelle ils ont été fournis et par qui, la dernière tentative de connexion et les adresses e-mail des utilisateurs.



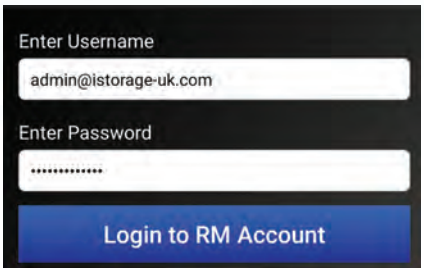
11. Provisionner une clé non gérée

Vous pouvez provisionner une clé « **gérée**» précédemment utilisée en tant que clé autonome « **non gérée** », qui ne fonctionnera qu'avec l'**application datAshur BT personnelle** disponible au téléchargement sur l'App Store d'Apple et Google Play.

Pour démarrer le provisionnement et définir les paramètres de sécurité en tant que clé non gérée, procédez comme suit.

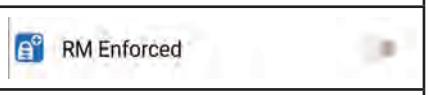
1. Ouvrez votre **application datAshur BT Administrateur**, entrez votre **Nom d'utilisateur** et votre **Mot de passe**, appuyez ensuite sur **Se connecter au compte de la CGD** (Console de gestion à distance).

Remarque : Votre nom d'utilisateur et votre mot de passe liés à l'application datAshur BT Administrateur sont identiques à ceux de la Console Web de gestion à distance.



2. Une fois la connexion établie, le menu **Paramètres de la clé** s'ouvre, vous pouvez alors vérifier et appliquer vos paramètres de sécurité de la façon décrite ci-dessous :

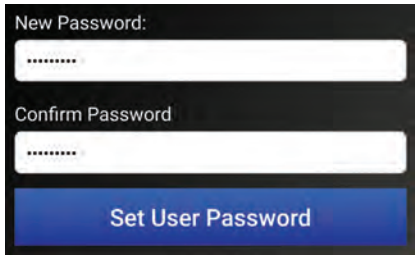
- **Appliqué par la gestion à distance :** Éteignez le voyant **VERT**. La gestion à distance est désactivée.



- **Mot de passe de l'utilisateur :** La clé datAshur BT est livrée avec un **Mot de passe par défaut (11223344)** déjà défini. Pour changer le mot de passe par défaut, appuyez sur « **Mot de passe de l'utilisateur** », **entrez** et **confirmez** votre nouveau mot de passe composé de **7 à 15** caractères, puis appuyez sur « **Définir le mot de passe utilisateur** ».

  Exigences liées au mot de passe : le mot de passe doit comporter entre 7 et 15 caractères, il ne peut contenir que des chiffres ou des lettres consécutifs ou répétitifs.

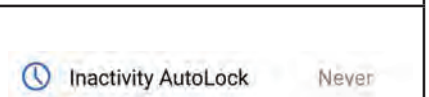
  Remarque : pour des raisons de sécurité, nous recommandons vivement à chaque utilisateur de remplacer le mot de passe par défaut ou le mot de passe Administrateur par son propre mot de passe unique de 7 à 15 caractères une fois sa clé attribuée.

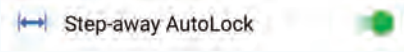
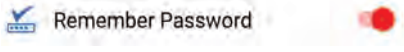
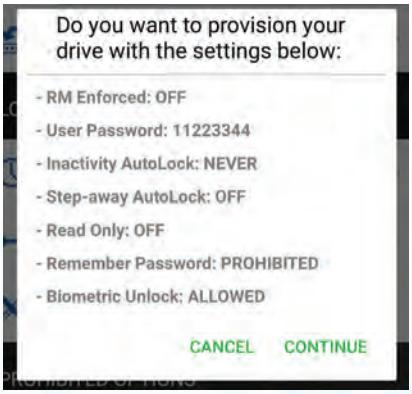


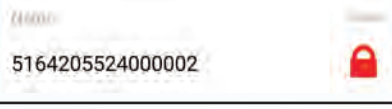
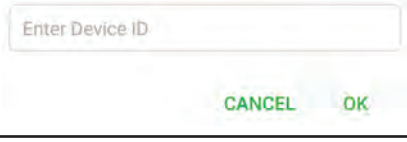
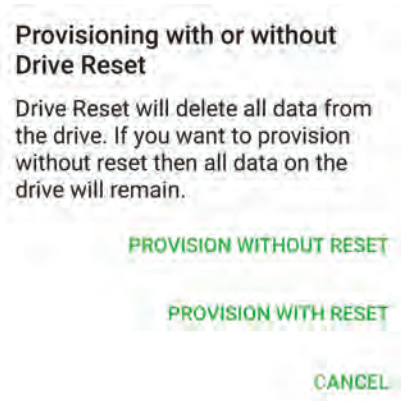
- **Verrouillage automatique d'inactivité :** pour se protéger des accès non autorisés pouvant survenir lorsque la clé est déverrouillée et non surveillée, la clé datAshur BT peut être configurée pour se verrouiller automatiquement au bout d'une période prédéfinie. Par défaut, la fonction Verrouillage automatique d'inactivité de la datAshur BT est destinée aux périodes où la clé n'est pas surveillée est désactivée (Jamais), elle peut cependant être configurée pour se verrouiller automatiquement entre **1 et 60** minutes.

  Pour définir un délai, appuyez sur Verrouillage automatique d'inactivité, puis appuyez sur pour choisir la durée souhaitée.

  Remarque : lorsque l'Administrateur active la fonction Verrouillage automatique d'inactivité, il devient impossible pour l'utilisateur ne la désactiver.



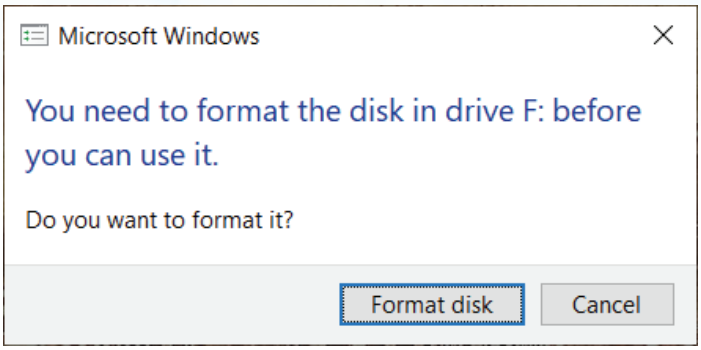
• **Verrouillage automatique en cas d'éloignement :** la fonction Verrouillage automatique en cas d'éloignement est désactivée par défaut. Lorsqu'elle est activée (voyant **VERT** allumé), la clé se verrouillera lorsque le smartphone d'un utilisateur (fonctionnant sous Android/iOS) s'éloignera d'environ 5 mètres de la clé datAshur BT. **Remarque :** lorsque l'Administrateur active la fonction Verrouillage automatique en cas d'éloignement, il devient impossible pour l'utilisateur ne la désactiver.	
• **Définir en Lecture seule uniquement :** la fonction Lecture seule est désactivée par défaut. Lorsqu'elle est activée (voyant **VERT** allumé), la clé sera définie en tant que clé en Lecture seule / Protégé en écriture. **Remarque :** lorsque l'Administrateur active la fonction Lecture seule, il devient impossible pour l'utilisateur ne la désactiver.	
• **Mémorisation du mot de passe :** La fonction Mémorisation du mot de passe est disponible (ACTIVÉE) par défaut, elle permet aux utilisateurs de configurer leurs clés de façon à ce que celles-ci mémorisent le mot de passe et ne le demandent pas lors du déverrouillage. Pour désactiver cette fonction et interdire aux utilisateurs de configurer leurs clés afin que celles-ci demandent le mot de passe au déverrouillage, appuyez sur le bouton bascule grisé (voyant **ROUGE** allumé). **Remarque :** lorsque l'administrateur **interdit** l'utilisation de la fonction Mémorisation du mot de passe (voyant **ROUGE** allumé), l'utilisateur ne peut pas activer cette fonction.	
• **Déverrouillage biométrique :** la fonction Déverrouillage biométrique est disponible (ACTIVÉE) par défaut, elle permet aux utilisateurs de définir un déverrouillage biométrique pour l'accès à leurs clés. Pour désactiver cette fonction et interdire aux utilisateurs de configurer le Déverrouillage biométrique sur leurs clés, appuyez sur le bouton bascule grisé (voyant **ROUGE** allumé). **Remarque :** lorsque l'administrateur **interdit** l'utilisation du Déverrouillage biométrique (voyant **ROUGE** allumé), l'utilisateur ne peut pas activer cette fonction.	
3. Appuyez pour confirmer les nouveaux paramètres de la clé.	
4. Appuyez sur **Continuer** pour provisionner vos paramètres favoris sur la clé datAshur BT.	

5. Notez le **Numéro d'identification de la clé** figurant sur le connecteur USB et **Connectez** la clé datAshur BT gérée à un port USB sous tension.	
6. Appuyez sur le cadenas **ROUGE**. **Remarque :** Le voyant de la clé clignote en ROUGE.	
7. Saisissez le **Numéro d'identification de la clé**, puis appuyez sur **OK**.	 
8. Si vous provisionnez une clé précédemment utilisée et n'ayant pas été réinitialisée, procédez comme suit. Sinon ignorez cette étape (si la clé a été réinitialisée), puis passez à l'étape 9. • **Provisionnement avec réinitialisation :** Appuyez sur **« Provisionnement avec réinitialisation»** et passez à l'étape 9**.** • **Provisionnement sans réinitialisation :** Appuyez sur **« Provisionnement sans réinitialisation»** et passez à l'étape 10**.** **Remarque :** le provisionnement sans réinitialisation ne supprimera PAS les données précédemment stockées sur la clé en cours de provisionnement.	
9. Appuyez sur le cadenas **GRIS** (vide) pour terminer le provisionnement.	
10. Une fois le provisionnement terminé, l'application affiche une **coche VERTE**, le voyant de la clé s'allume en **BLEU** de manière fixe, indiquant que la clé datAshur BT a été provisionnée.	
11. Si la clé a été provisionnée avec réinitialisation (étape 8), votre ordinateur vous demandera de procéder au formatage de la clé. Reportez-vous à la section 12 « Formater la clé datAshur BT pour le système d'exploitation Windows » ou à la section 13 « Formater la clé datAshur BT pour le système d'exploitation Mac OS ». **Remarque :** Une fois la clé formatée, l'administrateur peut accéder à celle-ci et y ajouter des fichiers si nécessaire.	

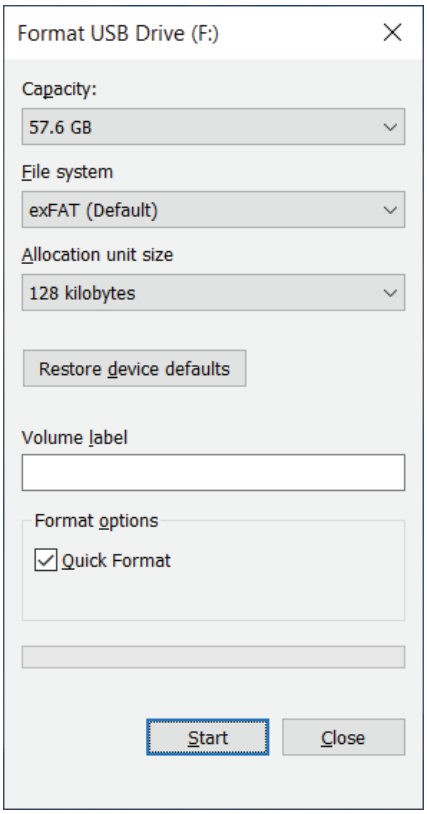
12. Formater la clé datAshur BT pour le système d'exploitation Windows

Pour formater votre clé datAshur BT sous Windows, procédez comme suit :

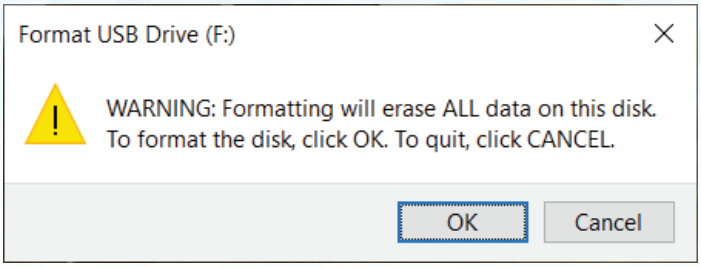
1. Le système affiche la fenêtre **Formatage**.



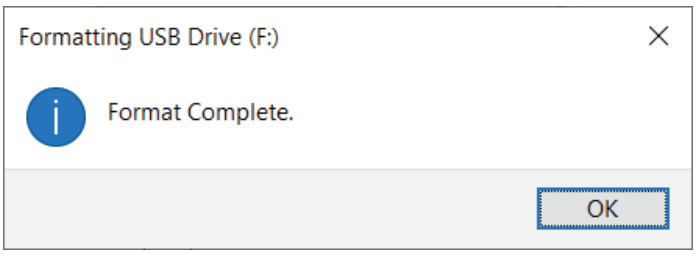
2. Cliquez sur Formater le disque, la fenêtre Formater la clé USB s'ouvre.



3. Entrez un nom pour le volume dans le champ Nom de volume. Le nom de la clé s'affiche éventuellement sur le bureau. Le menu déroulant Système de fichiers répertorie les formats de disque disponibles et pris en charge par Windows. Sélectionnez FAT32 ou exFAT selon vos besoins.
4. Cliquez sur **Démarrer**.
5. Cliquez sur **OK** pour poursuivre le formatage de la clé.



6. L'ordinateur termine le formatage et affiche une confirmation de fin du formatage.

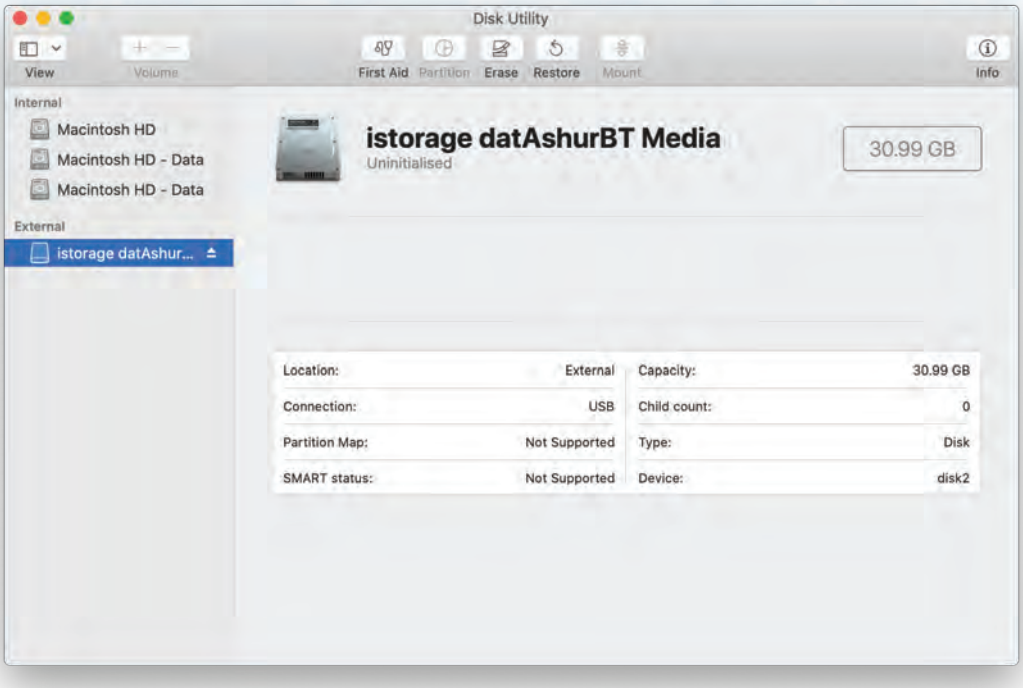


13. Formater la clé datAshur BT pour le système d'exploitation Mac OS

Pour formater votre clé datAshur BT sur Mac OS, procédez comme suit :

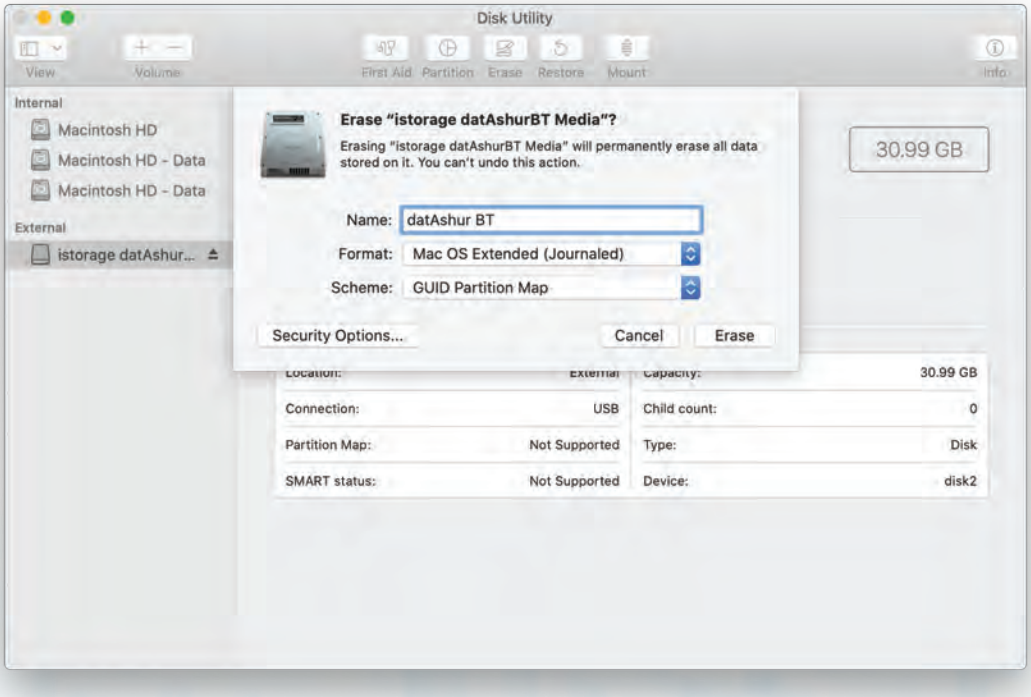
1. Le système affiche la fenêtre **INITIALISATION**.

2. Appuyez sur **INITIALISER**, ouvrez l'utilitaire de disque, sélectionnez iStorage datAshur BT dans la fenêtre de l'utilitaire de disque.

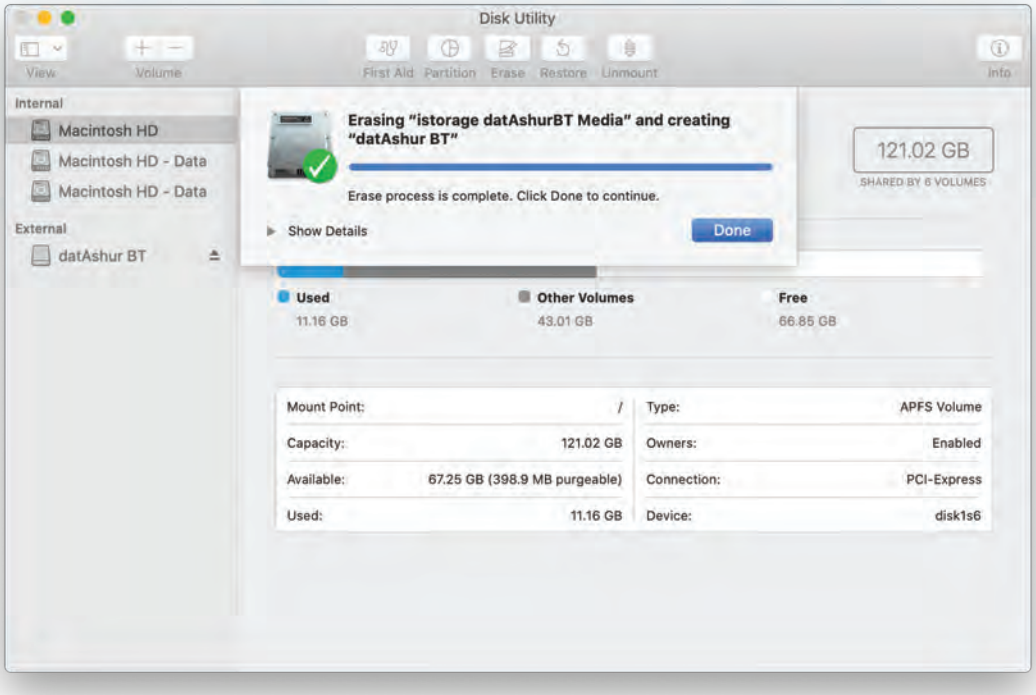


3. Cliquez sur l'option **Effacer** du menu contextuel.

4. Entrez un nom de clé, le nom par défaut est Sans titre. Le nom de la clé s'affiche éventuellement sur le bureau. Sélectionnez le système de fichiers et le format de volume à utiliser. Le menu déroulant Format du volume répertorie les formats de lecteur disponibles et pris en charge par le système Mac. Le type de format recommandé est Mac OS étendu (journalisé) pour une utilisation multi-plateforme entre mac OS et MS-DOS. Le menu déroulant des formats système répertorie les systèmes disponibles.



5. Cliquez sur **Effacement**.
6. La clé datAshur BT formatée s'affiche dans la fenêtre **Utilitaire de disque** et sera présente sur le bureau



14. Assistance technique

iStorage fournit ces ressources utiles pour vous :

Site Web d'iStorage
https://www.istorage-uk.com

Contact par e-mail
support@istorage-uk.com

Assistance téléphonique avec notre service d'assistance technique joignable au **+44 (0) 20 8991 6260**. Les spécialistes de l'assistance technique d'iStorage sont disponibles de 9h00 à 17h30 GMT du lundi au vendredi.

15. Informations sur la garantie et la demande de retour de produits

AVIS DE NON-RESPONSABILITÉ ET GARANTIE DU PRODUIT ISTORAGE

iStorage garantit que ses Produits seront exempts de défauts matériels à la livraison et pendant une période de 36 mois à compter de la livraison. Cette garantie ne s'applique cependant pas dans les situations décrites ci-dessous. iStorage garantit que les Produits sont conformes aux normes énumérées dans les fiches techniques correspondantes sur son site Web au moment du passage de la commande.

Ces garanties ne s'appliquent à aucun défaut des Produits découlant des éléments suivants :

- usure normale ;
- dommages intentionnels, conditions de stockage ou de fonctionnement anormales, accident, négligence de votre part ou de toute tierce partie ;
- lorsque vous ou une tierce partie ne parvenez pas à faire fonctionner ou à utiliser les Produits conformément aux instructions d'utilisation ;
- toute modification ou réparation effectuée par vous ou une tierce partie n'étant pas l'un de nos réparateurs agréés ; ou
- toute spécification fournie par vous.

En vertu de ces garanties, nous allons, à notre discrétion, procéder à la réparation, au remplacement ou au remboursement pour tout produit présentant des défauts matériels, à condition qu'à la livraison :

- vous inspectiez les Produits afin de vérifier s'ils présentent des défauts matériels ; et
- vous testiez le mécanisme de chiffrement des produits.

Nous ne serons en aucun cas tenus responsables des défauts matériels ou des défauts du mécanisme de chiffrement des Produits pouvant être vérifiés durant une inspection lors de la livraison, sauf si vous nous notifiez ces défauts dans les 30 jours suivant la livraison. Nous ne serons en aucun cas tenus responsables des défauts matériels ou des défauts du mécanisme de chiffrement des Produits qui ne sont pas vérifiables lors de l'inspection à la livraison, sauf si vous nous notifiez ces défauts dans les 7 jours suivant le moment où vous découvrez (ou auriez dû découvrir) les défauts. Nous ne serons pas tenus responsables au titre de ces garanties lorsque vous, ou une autre tierce partie, continuez d'utiliser des produits après avoir découvert un défaut sur ceux-ci. Vous devez nous retourner le produit défectueux juste après nous avoir notifié d'un défaut sur celui-ci. Si vous êtes une entreprise, vous aurez à votre charge les frais de transport que vous avez engagés pour nous renvoyer des produits/pièces de produits sous garantie, nous prendrons alors à notre charge l'ensemble des frais de transport que nous engagerons pour vous renvoyer les produits réparés (ou les produits de remplacement). Si vous êtes un consommateur, veuillez consulter nos Conditions générales.

Les produits retournés doivent être placés dans leur emballage d'origine et être propres. Dans le cas contraire et à la discrétion de notre Société, les produits retournés seront soit refusés, soit majorés de frais supplémentaires que nous vous facturerons afin de couvrir les coûts supplémentaires occasionnés. Les produits retournés pour réparation sous garantie doivent être accompagnés d'une copie de la facture originale, vous devez autrement indiquer le numéro de facture original ainsi que la date d'achat.

Si vous êtes un consommateur, cette garantie s'ajoute à vos droits légaux liés aux produits défectueux ou non conformes à la description. Des conseils sur vos droits légaux sont disponibles auprès de votre bureau local de conseil aux citoyens ou de votre bureau des pratiques commerciales.

Les garanties mentionnées dans cette clause s'appliquent uniquement à l'acheteur d'origine d'un produit d'iStorage, ayant réalisé l'achat auprès d'un revendeur ou distributeur iStorage agréé. Ces garanties ne sont pas transférables

À L'EXCEPTION DE LA GARANTIE LIMITÉE PRÉVUE DANS LES PRÉSENTES ET DANS LA MESURE AUTORISÉE PAR LA LOI, ISTORAGE DÉCLINE TOUTE GARANTIE, QU'ELLE SOIT EXPRESSE OU IMPLICITE, CELA INCLUANT TOUTES LES GARANTIES DE QUALITÉ MARCHANDE, D'ADAPTATION À UN USAGE PARTICULIER ET DE NON-CONTREFAÇON. ISTORAGE NE GARANTIT PAS UN FONCTIONNEMENT EXEMPT D'ERREUR DU PRODUIT. DANS LA MESURE OU TOUTES LES GARANTIES IMPLICITES PEUVENT EXISTER DE PLEIN DROIT, CES GARANTIES SE LIMITENT À LA DURÉE DE CETTE GARANTIE. LA RÉPARATION OU LE REMPLACEMENT DE CE PRODUIT, CONFORMÉMENT AU DISPOSITIONS DES PRÉSENTES, CONSTITUE VOTRE SEUL ET UNIQUE RECOURS.

EN AUCUN CAS, ISTORAGE NE SERA TENUE RESPONSABLE DE TOUTE PERTE OU BÉNÉFICE ESCOMPTÉS, OU DE TOUT DOMMAGE ACCESSOIRE, PUNITIF, EXEMPLAIRE, SPÉCIAL, DE CONFIANCE OU INDIRECT, Y COMPRIS, MAIS SANS S'Y LIMITER, LA PERTE DE REVENUS, LA PERTE DE PROFITS, LA PERTE D'UTILISATION DU LOGICIEL, LA PERTE DE DONNÉES, LES AUTRES PERTES OU LA RÉCUPÉRATION DE DONNÉES, LES DOMMAGES À LA PROPRIÉTÉ ET LES RÉCLAMATIONS DE TIERS, PROVENANT DE TOUT PRINCIPE DE RECOUVREMENT, Y COMPRIS CEUX LIÉS À LA GARANTIE, CONTRACTUELS, STATUTAIRES OU PROVENANT D'UN ACTE DOMMAGEABLE, QU'ELLE AIT ÉTÉ AVISÉE OU NON DE LA POSSIBILITÉ DE TELS DOMMAGES. NONOBSTANT À LA DURÉE DE TOUTE GARANTIE LIMITÉE OU DE TOUTE GARANTIE IMPLICITE AUX TERMES DE LA LOI, OU DANS L'ÉVENTUEL NON RESPECT DE L'OBJET PRINCIPAL DE LA GARANTIE LIMITÉE, EN AUCUN CAS LA RESPONSABILITÉ D'ISTORAGE EXCÉDERA LE PRIX D'ACHAT DE CE PRODUIT. | 4823-2548-5683.3
ENTIRE LIABILITY EXCEED THE PURCHASE PRICE OF THIS PRODUCT. | 4823-2548-5683.3

DATASHUR® BT
ADMIN MANUAL

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 | Site Web : www.istorage-uk.com

ADMINISTRATORENHANDBUCH

DIE DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR ZUR VERFÜGUNG GESTELLT, UND ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN BEDINGUNGEN, ZUSICHERUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH JEDER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER DER NICHT-VERLETZUNG VON RECHTEN, SIND AUSGESCHLOSSEN, ES SEI DENN, SOLCHE AUSSCHLÜSSE WERDEN FÜR RECHTLICH UNGÜLTIG ERKLÄRT

iStorage haftet weder aufgrund dieser Garantie noch anderweitig für zufällige, besondere oder Folgeschäden, einschließlich Datenverluste, die sich aus der Verwendung oder dem Betrieb des Produkts ergeben, unabhängig davon, ob iStorage von der Möglichkeit solcher Schäden in Kenntnis gesetzt wurde oder nicht

EMI-Warnhinweise

Dieses Gerät wurde getestet und entspricht den Grenzwerten für ein digitales Gerät der Klasse B gemäß Abschnitt 15 der FCC-Vorschriften. Diese Grenzwerte sind so ausgelegt, dass sie einen angemessenen Schutz gegen schädliche Störungen bei der Verwendung in Wohnräumen bieten. Dieses Gerät erzeugt, verwendet und kann Hochfrequenzenergie ausstrahlen und kann, falls es nicht in Übereinstimmung mit den Anweisungen installiert und verwendet wird, schädliche Störungen des Funkverkehrs verursachen. Es gibt jedoch keine Garantie, dass in einer bestimmten Installation keine Störungen auftreten. Wenn dieses Gerät schädliche Störungen des Radio- oder Fernsehempfangs verursacht, was durch Ein- und Ausschalten des Geräts festgestellt werden kann, sollte der Benutzer versuchen, die Störung durch eine oder mehrere der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne neu aus oder bewegen Sie sie an einen anderen Ort.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.
- Schließen Sie das Gerät an eine Steckdose an, die zu einem anderen Stromkreis gehört als der Stromkreis des Empfängers.
- Wenden Sie sich an den Händler oder einen erfahrenen Radio-/Fernsehtechniker, um Hilfe zu erhalten.

Warnungen

Änderungen oder Anpassungen, die nicht ausdrücklich von der für die Einhaltung der Vorschriften verantwortlichen Partei genehmigt wurden, können dazu führen, dass die Berechtigung des Benutzers zum Betrieb dieses Geräts erlischt. Die normale Funktion des Produkts kann durch starke elektromagnetische Interferenz gestört werden. Setzen Sie in diesem Fall das Produkt einfach zurück, um den normalen Betrieb wieder aufzunehmen, indem Sie der Bedienungsanleitung folgen. Falls der Betrieb nicht fortgesetzt werden konnte, verwenden Sie das Produkt bitte an einem anderen Ort“

Dieses Gerät entspricht Abschnitt 15 der FCC-Vorschriften und den von der Industry Canada License befreiten RSSs. Der Betrieb unterliegt den folgenden zwei Bedingungen: (1) Dieses Gerät darf keine schädlichen Interferenzen verursachen, und (2) Dieses Gerät muss alle eingehenden Interferenzen akzeptieren, einschließlich Interferenzen, die einen unerwünschten Betrieb verursachen können.

RF-Expositionserklärung

Das Gerät wurde evaluiert, um die allgemeinen Anforderungen für RF-Exposition zu erfüllen.

iStorage datAshur BT wird von iStorage Ltd. hergestellt und verwendet die DataLock®-Technologie, die von ClevX, LLC lizenziert wurde. U.S.-Patent. www.istorage-uk.com/clevx-patents

Inhaltsverzeichnis

Einführung 61
Verpackungsinhalt 61
Nützliche Links 61
datAshur BT Außenansicht 62
Stick-LEDs und ihre Zustände 62
1. **Registrierung** 63
2. **Anmeldung als Administrator** 64
3. **Bereitstellen von verwalteten datAshur BT-Sticks** 65
4. **Erstellen von Benutzern über die Fernverwaltungskonsole** 68
5. **Zuweisen von Sticks zu Benutzern** 69
6. **Dashboard für die Verwaltung von Benutzern** 70
   - Benutzer-Dashboard auf einen Blick 70
   - Aktivieren oder Deaktivieren des Benutzerzugriffs 70
   - Löschen eines Benutzers aus der Fernverwaltung 70
   - Zurücksetzen des Passworts der datAshur BT verwalteten App für einen Benutzer 70
   - Suchleiste 71
   - Öffnen des Panels für Geo- und Timefencing 71
7. **Dashboard für die Verwaltung von Sticks** 71
   - Sticks-Dashboard auf einen Blick 71
   - Löschen eines Sticks aus der Fernverwaltung 72
   - Suche nach Stick-Seriennummer 72
   - Zugriffskontrolle verwalten 72
   - Aktivieren oder Deaktivieren des Zugriffs auf den Stick 72
   - Löschen eines Sticks per Fernverwaltung 73
   - Ändern eines Stick-Passworts per Fernverwaltung 73
   - Entsperren eines Sticks per Fernverwaltung 73
   - Anzeigen der Zuordnung und des Zugriffsprotokolls 74
8. **Anwendung von Geo- und Timefencing-Einschränkungen** 74
   - Geo- und Timefencing auf einen Blick 74
   - Zugelassene Sticks 75
   - Festlegen von Timefencing-Einschränkungen 75
   - Festlegen von Geofencing-Einschränkungen 75
9. **Ändern des Admin-Passworts** 76
10. **Kontoübersicht** 76
11. **Bereitstellen von nicht verwalteten Sticks** 77
12. **Formatierung des datAshur BT für Windows** 80
13. **Formatierung des datAshur BT für Mac OS** 81
14. **Technische Unterstützung** 84
15. **Garantie- und RMA-Informationen** 84

Einführung

Vielen Dank, dass Sie das Managed-Drive-Abonnement für den datAshur BT erworben haben, ein hardwareverschlüsselter Stick mit USB 3.2 1. Gen., das über Bluetooth Ihr Smartphone (iOS/Android) als drahtloses Gerät zur Benutzer-Authentifizierung nutzt. So wird der sichere Zugriff auf Daten ermöglicht, die auf Ihrem verwalteten datAshur BT USB-Stick gespeichert sind.

Der verwaltete datAshur BT USB-Stick verwendet eine militärische AES-XTS 256-Bit-Hardwareverschlüsselung (Vollverschlüsselung des Laufwerks), die alle auf dem Stick gespeicherten Daten in Echtzeit verschlüsselt.

Der verwaltete datAshur BT Stick wurde für die Fernverwaltung über die webbasierte iStorage Fernverwaltungskonsole entwickelt, die es dem Administrator ermöglicht, mithilfe von Geo- und Timefencing zu steuern, wo und wann auf den Stick zugegriffen werden kann. Zu den zusätzlichen Funktionen gehören die Löschung, Freischaltung, Änderung von Passwörtern, Deaktivieren des Zugriffs und mehr per Fernsteuerung.

Verpackungsinhalt

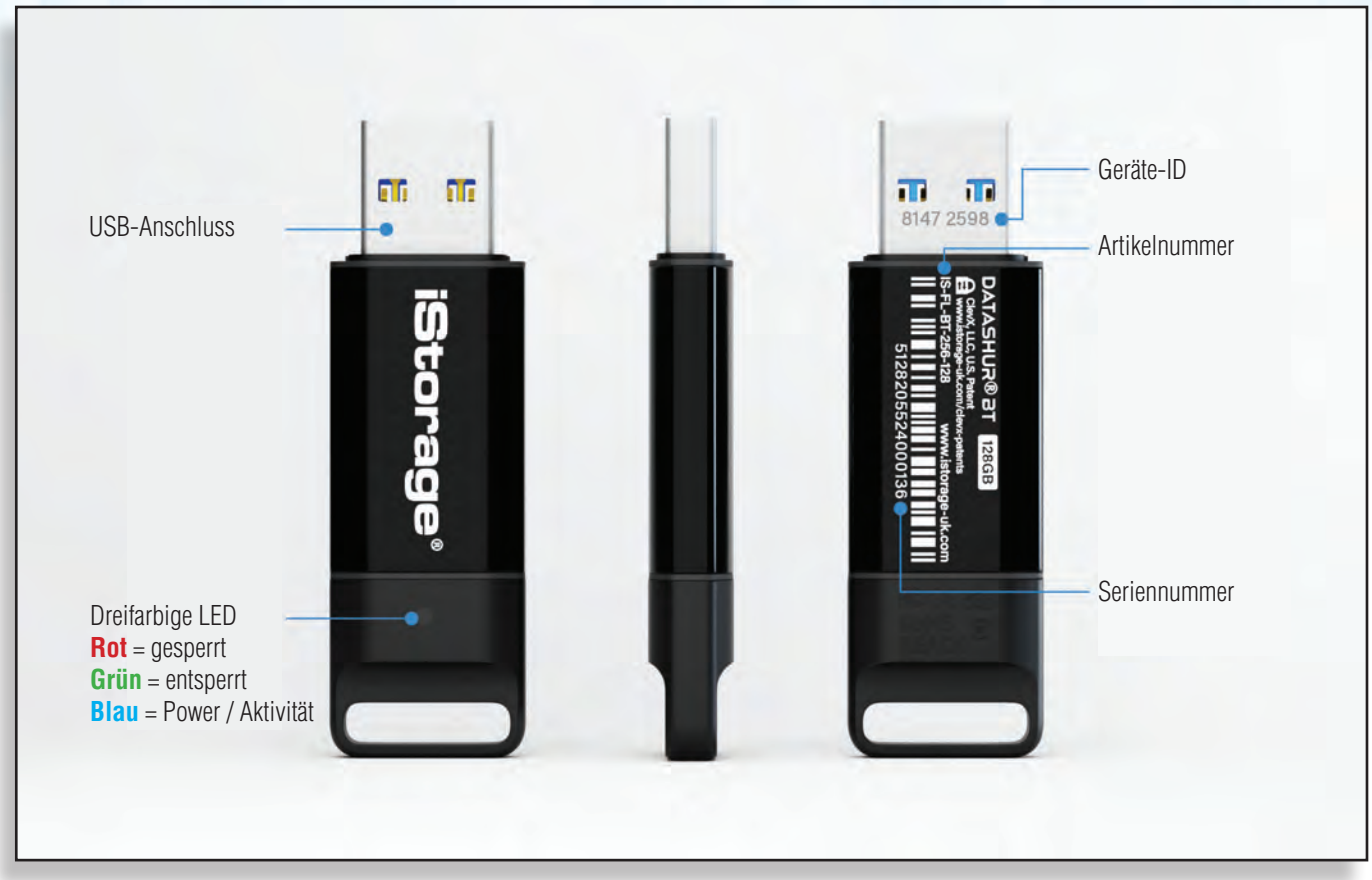
- iStorage datAshur BT
- SSA - Schnellstartanleitung für den „**nicht verwalteten**“ datAshur BT Personal

Anmerkung: Die datAshur BT-Verpackung enthält eine Schnellstartanleitung, die nur für den „nicht verwalteten“ datAshur BT Personal vorgesehen ist. Bitte ignorieren Sie die SSA-Beilage und befolgen Sie die in diesem Handbuch enthaltenen Anweisungen.

Nützliche Links

1. datAshur BT Registrierungslink für Administratoren: https://rm.bt.istorage-uk.com/Account/Register
2. Fernverwaltungs-Anmeldelink: https://rm.bt.istorage-uk.com/Account/Login
3. Verwalteter datAshur BT Benutzerhandbuch: https://istorage-uk.com/product-documentation/
4. Verwalteter datAshur BT Schnellstartanleitung: https://istorage-uk.com/product-documentation/
5. Persönlicher datAshur BT Benutzerhandbuch: https://istorage-uk.com/product-documentation/

datAshur BT Außenansicht



Stick-LEDs und ihre Zustände

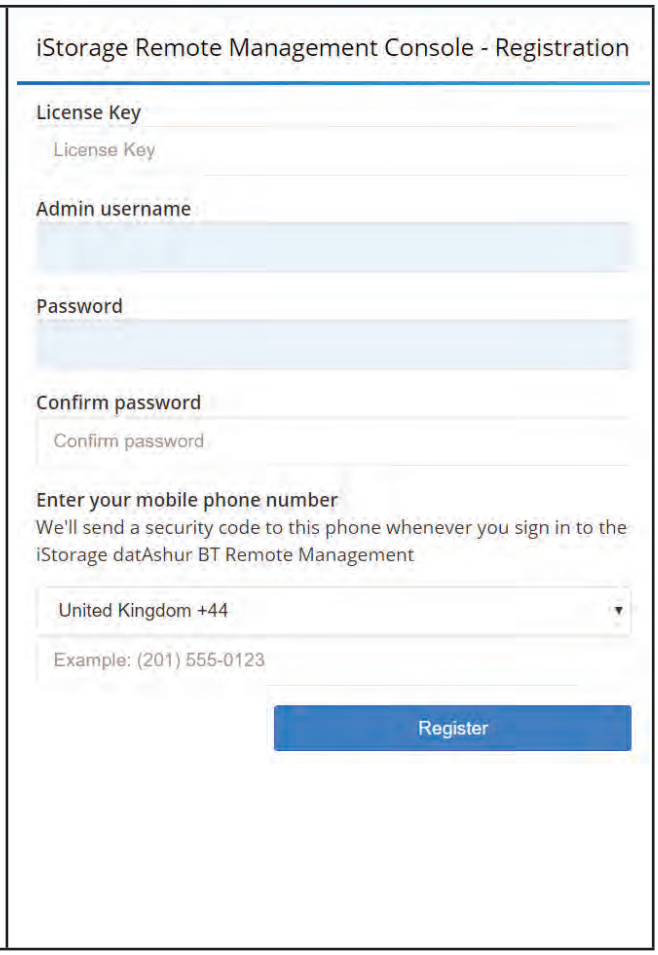
LEDs	LED-Zustand	Beschreibung
	Alle LEDs blinken einmal	Der datAshur BT führt einen Selbsttest durch, wenn er an einen Computer angeschlossen wird
	Durchgehend Rot	Gesperrt - datAshur BT App nicht geöffnet
	Rot blinkend	Gesperrt - datAshur BT App geöffnet
	Durchgehend Blau	datAshur BT ist freigeschaltet
	Blau blinkend	datAshur BT ist freigeschaltet und die Kommunikation funktioniert

1. Registrierung

Nach dem Kauf der Lizenz für die iStorage-Fernverwaltungskonsole erhalten Sie eine E-Mail mit einem „**Registrierungslink**“ und einem „**Lizenzschlüssel**“, um den Registrierungsprozess wie unten beschrieben zu beginnen.

Öffnen Sie den folgenden Link, um zur Registrierungsseite zu gelangen, und füllen Sie die Registrierungsfelder wie unten beschrieben aus.
https://rm.bt.istorage-uk.com/Account/Register

1. **Lizenzschlüssel:** Diesen finden Sie in der Registrierungs-E-Mail von iStorage, die Ihren Lizenzschlüssel enthält.
2. **Administrator-Benutzername:** Dies muss eine **E-Mail-Adresse** sein, die für die **Administrator-Anmeldung** verwendet wird.
3. **Passwort:** Erstellen Sie ein sicheres Passwort.
4. **Passwort bestätigen:** Geben Sie Ihr Passwort zur Bestätigung erneut ein.
5. Wählen Sie Ihr **Land** aus dem Dropdown-Menü aus und **geben Sie** dann **Ihre Mobiltelefonnummer** ein: Dies ist für die „Zwei-Faktor-Authentifizierung“ erforderlich.
6. Klicken Sie auf „**Registrieren**“.
7. Geben Sie auf der Seite „**Zweistufige Überprüfung aktivieren**“ den **6-stelligen Code**, den Sie per Textnachricht erhalten haben, ein und klicken Sie auf Weiter.
8. Klicken Sie auf „**Erledigt**“.



2. Anmeldung als Administrator

Mit der webbasierten Fernverwaltungskonsole von iStorage ist der Administrator in der Lage, alle verwalteten datAshur BT-Sticks, die im gesamten Unternehmen eingesetzt werden, bereitzustellen, Sicherheitsrichtlinien festzulegen und volle Kontrolle und Transparenz zu haben.

Um sich als Admin einzurichten, benötigen Sie Ihren **Benutzernamen** und Ihr **Passwort**, die Sie während des Registrierungsprozesses erstellt haben, wie in „**Abschnitt 1 – Registrierung**“ beschrieben. Fahren Sie anschließend mit den folgenden Schritten fort.

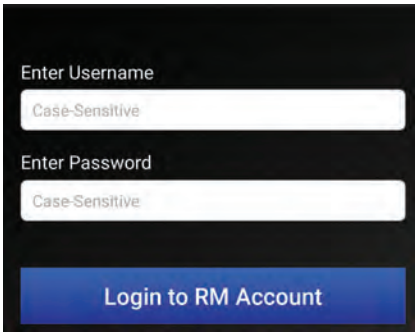
1. Laden Sie die **datAshur BT Admin-App** aus dem **Apple App Store** oder von **Google Play** herunter und installieren Sie sie, oder **scannen Sie den QR-Code** direkt von Ihrem Smartphone, um zum Download zu gelangen.

datAshur BT Admin App

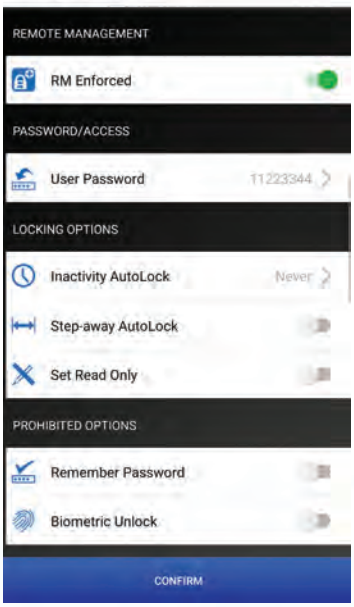
2. Tippen Sie in der Popup-Meldung auf **Zulassen**.

3. Geben Sie Ihren **Benutzernamen** und Ihr **Passwort** ein und tippen Sie dann auf **Zum FV-Konto anmelden** (Fernverwaltung).

Anmerkung: Ihr Benutzername und Ihr Passwort für die datAshur BT Administrator-App und die webbasierte iStorage-Fernverwaltungskonsole sind identisch.



Nach erfolgreicher Anmeldung öffnet sich das Menü **Laufwerkseinstellungen**, in dem Sicherheitsrichtlinien festgelegt und alle verwalteten datAshur BT-Sticks wie im folgenden Abschnitt beschrieben bereitgestellt werden können.

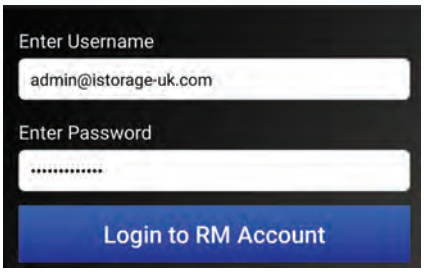


3. Bereitstellen von verwalteten datAshur BT-Sticks

Nach der Einrichtung als Administrator (Abschnitt 2) müssen Sie zunächst alle verwalteten datAshur BT-Sticks, die Sie über die Fernverwaltungskonsole verwalten möchten, einzeln bereitstellen.

Um mit der Bereitstellung zu beginnen, fahren Sie mit den folgenden Schritten fort.

1. Öffnen Sie Ihre **datAshur BT Administrator-App** und geben Sie Ihren **Benutzernamen** und Ihr **Passwort** ein. Tippen Sie dann auf **Beim FV-Konto anmelden** (Fernverwaltung).



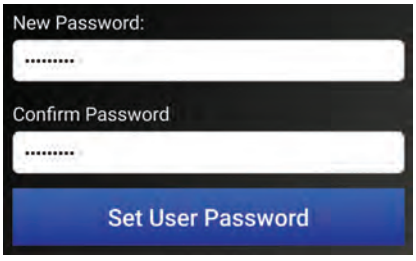
2. Nach erfolgreicher Anmeldung öffnet sich das Menü **Laufwerkseinstellungen**, in dem Sie Ihre Sicherheitseinstellungen wie unten beschrieben überprüfen und anwenden können:

- **FV erzwungen:** FV erzwungen (**GRÜNES** Licht an) und MUSS **AKTIVIERT** bleiben, um die Bereitstellung per Fernverwaltung zu ermöglichen. Im ausgeschalteten Zustand kann ein Laufwerk für die Arbeit mit der nicht verwalteten App bereitgestellt werden (datAshur BT App - siehe separates Benutzerhandbuch).

- **Benutzer-Passwort:** Der datAshur BT wird mit einem **Standardpasswort (11223344)** ausgeliefert. Um das Standardpasswort zu ändern, tippen Sie auf „**Benutzerpasswort**“, **geben Sie** dann Ihr neues **7-15-stelliges** Passwort **ein** und **bestätigen** Sie es. Tippen Sie schließlich auf „**Benutzerpasswort festlegen**“.

  Passwort-Anforderungen: Das Passwort muss 7-15 Zeichen lang sein und darf nicht nur aufeinanderfolgende oder sich wiederholende Zahlen oder Buchstaben enthalten.

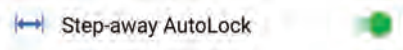
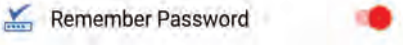
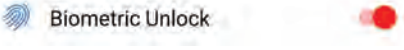
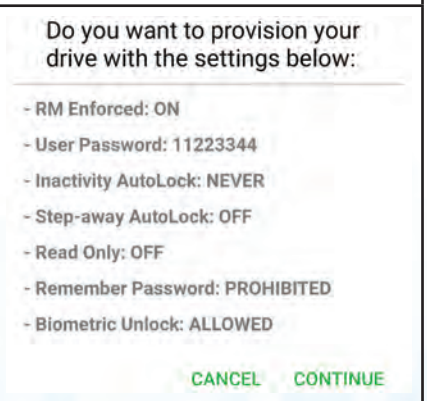
  Anmerkung: Aus Sicherheitsgründen empfehlen wir dringend, dass jeder Benutzer das Standard- oder vom Administrator festgelegte Passwort ändert, zu seinem/ihrem eigenen, eindeutigen 7-15 Zeichen langen Passwort, sobald der Stick an sie ausgegeben wurde.



- **Automatische Sperrung wegen Inaktivität:** Zum Schutz vor unbefugtem Zugriff kann der datAshur BT so eingestellt werden, dass er nach einer voreingestellten Zeitspanne automatisch gesperrt wird, wenn der Stick freigeschaltet und unbeaufsichtigt ist. In der Standardeinstellung ist die Funktion datAshur BT automatische Sperrung wegen unbeaufsichtigter Inaktivität deaktiviert („Nie“), kann aber auf einen Wert zwischen **1 und 60** Minuten eingestellt werden.

  Um ein Zeitlimit festzulegen, tippen Sie auf automatische Sperrung wegen Inaktivität und dann auf , um die gewünschte Zeitdauer festzulegen.

  Anmerkung: Wenn der Administrator die automatische Sperrung wegen Inaktivität einstellt, kann der Benutzer diese Funktion nicht deaktivieren.

• **Automatische Entfernungssperrung:** Die automatische Entfernungssperrung ist standardmäßig deaktiviert. Wenn sie aktiviert ist (**GRÜNES** Licht leuchtet), werden dadurch alle bereitgestellten verwalteten datAshur BT-Sticks gesperrt, wenn das Smartphone (Android/iOS) eines Benutzers für mehr als 5 Sekunden etwa 5 Meter vom datAshur BT-Stick entfernt ist. **Anmerkung:** Wenn der Administrator die automatische Entfernungssperrung wegen Inaktivität aktiviert, kann der Benutzer diese Funktion nicht deaktivieren.	
• **Schreibschutz einstellen:** Die Schreibschutzfunktion ist standardmäßig deaktiviert. Wenn sie aktiviert ist (**GRÜNES** Licht leuchtet), sind alle eingesetzten verwalteten datAshur BT-Sticks schreibgeschützt. **Anmerkung:** Wenn der Administrator den Schreibschutz aktiviert, kann der Benutzer diese Funktion nicht deaktivieren.	
• **Passwort merken:** Die Funktion Passwort merken ist standardmäßig aktiviert (AN), so dass Benutzer ihre Sticks ohne Eingabe des Passworts entsperren können. Um diese Funktion zu deaktivieren (**empfohlen**) und Benutzern zu untersagen, ihre Sticks ohne Eingabe eines Kennworts freizuschalten, tippen Sie auf den grau unterlegten Schalter zum Deaktivieren (**ROTES** Licht leuchtet). **Anmerkung:** Wenn der Admin die Funktion „Passwort merken“ **deaktiviert** (**ROTES** Licht leuchtet), kann der Benutzer diese Funktion nicht aktivieren und muss sein Passwort jedes Mal eingeben, wenn er seinen Stick freischalten muss.	
• **Biometrisches Entsperren:** Die biometrische Entsperrung ist standardmäßig aktiviert (AN), so dass Benutzer eine biometrische Freischaltung einstellen können, um auf ihren Stick zuzugreifen. Um diese Funktion zu deaktivieren und Benutzern zu untersagen, eine biometrische Freischaltung für den Zugriff auf ihre Sticks einzustellen, tippen Sie auf den grauen Schalter zum Deaktivieren (**ROTES** lLicht leuchtet). **Anmerkung:** Wenn der Admin die biometrische Entsperrung **deaktiviert** (**ROTES** Licht leuchtet), kann der Benutzer diese Funktion nicht aktivieren.	
3. Tippen Sie hier, um Ihre Laufwerkseinstellungen zu bestätigen.	
4. Tippen Sie auf **Weiter**, um alle verwalteten datAshur BT-Sticks mit Ihren bevorzugten Einstellungen bereitzustellen.	

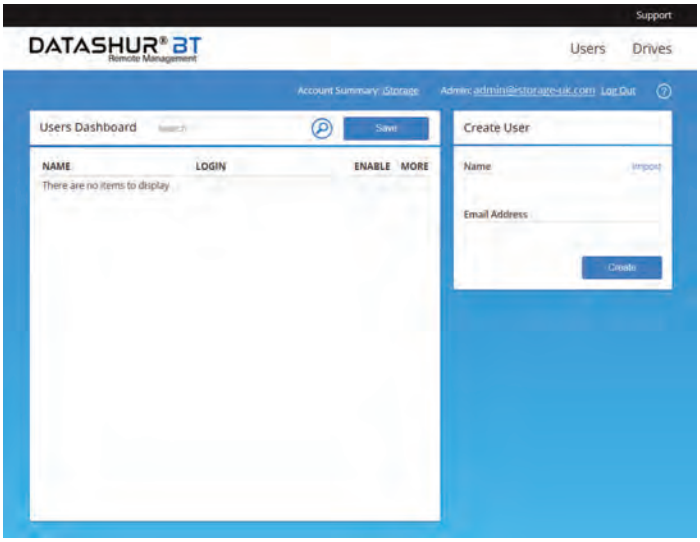
5. Notieren Sie sich die auf dem USB-Anschluss aufgedruckte **Geräte-ID** und **schließen Sie** den verwalteten datAshur BT-Stick an einen USB-Anschluss mit Stromversorgung an.	
6. Tippen Sie auf das **ROTE** Schlosssymbol. **Anmerkung:** Die Stick-LED blinkt (●) **ROT**.	
7. Geben Sie die **Geräte-ID-Nummer** ein und tippen Sie dann auf **OK**.	
8. Tippen Sie auf das **GRAUE** (leere) Schlosssymbol, um die Bereitstellung abzuschließen.	
9. Sobald die Bereitstellung abgeschlossen ist, zeigt die App ein **GRÜNES Häkchen an** und die LED des Sticks leuchtet durchgehend Blau. Dadurch wird angezeigt, dass der verwaltete datAshur BT-Stick bereitgestellt wurde, automatisch von Ihrer Fernverwaltungskonsole erkannt wird und bereit ist, einem Benutzer zugewiesen zu werden. **Anmerkung:** Wenn Sie mehrere Sticks bereitstellen, die an einen USB-Hub mit mehreren Anschlüssen angeschlossen sind, wiederholen Sie die Schritte 6-9 für jeden einzelnen Stick, ein Stick nach dem anderen.	
10. Sie werden nun von Ihrem Computer aufgefordert, alle bereitgestellten verwalteten datAshur BT-Sticks zu formatieren. Siehe Abschnitt 12 „Formatierung des datAshur BT für Windows“ bzw. Abschnitt 13 „Formatierung des datAshur BT für Mac OS“. **Anmerkung:** Nach der Formatierung kann der Administrator auf den Stick zugreifen und bei Bedarf Daten hinzufügen.	

4. Erstellen von Benutzern über die Fernverwaltungskonsole

1. Klicken Sie auf den folgenden Link, um die Fernverwaltungskonsole zu öffnen: https://rm.bt.istorage-uk.com/Account/Login

2. Melden Sie sich mit Ihrem **Administrator-Benutzernamen** und -**Passwort** an.

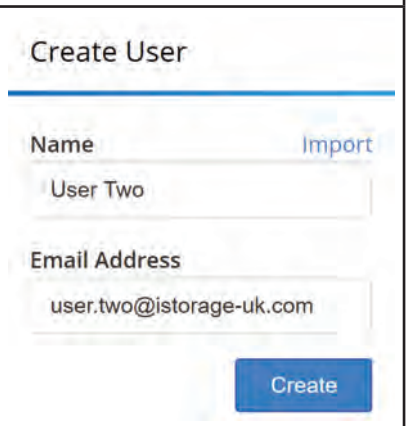
3. Nach erfolgreicher Anmeldung wird das datAshur BT Fernverwaltungsdashboard geöffnet.



4. Um Benutzer hinzuzufügen, geben Sie unter „**Benutzer erstellen**“ den Namen und die **E-Mail-Adresse** des vorgesehenen Benutzers ein und klicken Sie auf „**Erstellen**“, um eine E-Mail an den Empfänger zu senden, die den Benutzernamen und das temporäre Passwort sowie einen Download-Link für die **datAshur BT verwaltete App** enthält. Alle Benutzer, die erstellt werden, erscheinen auf dem Benutzer-Dashboard.

   Gehen Sie wie folgt vor, um eine Liste von Benutzern zu erstellen und zu **importieren**:

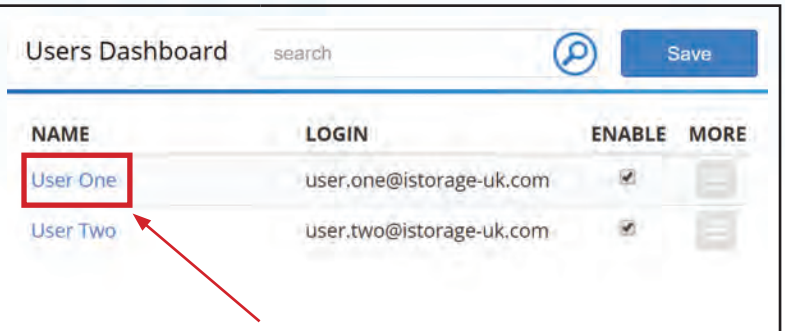
- Geben Sie in einer Excel-Tabelle den Namen jedes Benutzers ein, gefolgt von einem Semikolon (;) vor der E-Mail-Adresse. Zum Beispiel: **‘Benutzer Eins;benutzer.eins@istorage-uk.com’ ‘Benutzer Zwei;benutzer.zwei@istorage-uk.com’**
- Speichern Sie Ihre Tabelle als .**CSV**-Datei.
- Klicken Sie auf „**Importieren**“.
- Klicken Sie im Dialogfeld „**Benutzer importieren**“ auf „**Datei auswählen**“, navigieren Sie zu Ihrer Datei und klicken Sie dann auf „Importieren“.
- Alle importierten Benutzer werden auf dem Benutzer-Dashboard aufgelistet.



Anmerkung: Detaillierte Anweisungen zur Verwendung der datAshur BT verwalteten App finden Sie im **verwalteten datAshur BT Benutzerhandbuch.**

5. Zuweisen von Sticks zu Benutzern

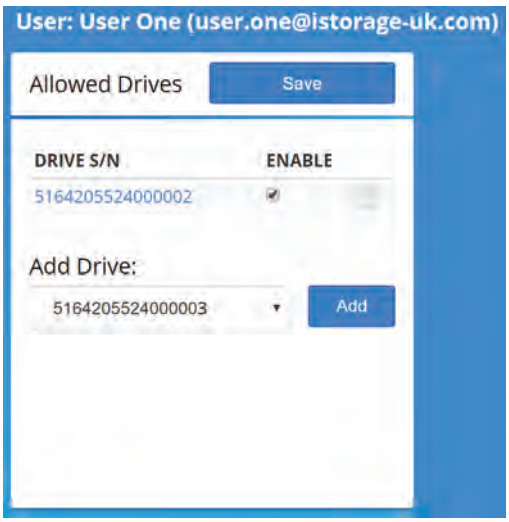
1. Melden Sie sich bei der Fernverwaltungskonsole an.
2. Klicken Sie in der Registerkarte „**Benutzer**“ unter „**Benutzer-Dashboard**“ auf den **Benutzernamen**. Zum Beispiel „Benutzer Eins“.



3. Wählen Sie einen Stick aus dem Dropdown-Menü unter „**Stick hinzufügen**“, den Sie dem Benutzer zuweisen möchten. Klicken Sie anschließend auf „**Hinzufügen**“ und schließlich auf „**Speichern**“.

   Der durch die Seriennummer identifizierte Stick wird dem Benutzer zugewiesen und aktiviert. Das Beispiel in der Abbildung unten rechts zeigt, dass die „**Stick-Seriennummer**“, die auf **02** endet, dem **Benutzer Eins** zugewiesen wurde.

Anmerkung: Um den Benutzern weitere Sticks zuzuweisen, wiederholen Sie die Schritte 2 und 3.
Sie können einem Benutzer auch mehrere Sticks zuweisen.

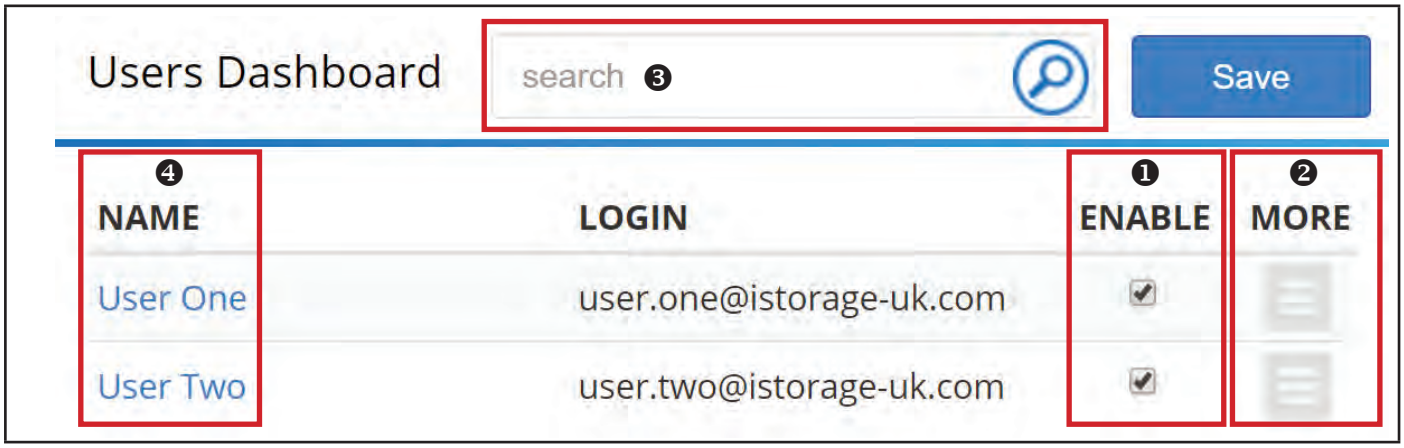


6. Dashboard für die Verwaltung von Benutzern

Benutzer-Dashboard auf einen Blick

Nachdem alle verwalteten datAshur BT-Sticks den Benutzern zugewiesen wurden, kann der Administrator nun die folgenden Aktionen über das **Benutzer-Dashboard** ausführen

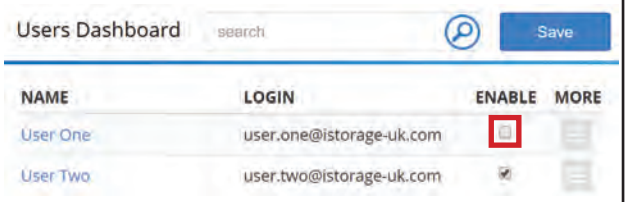
❶ **Aktivieren oder Deaktivieren des Benutzerzugriffs.**
❷ **Löschen eines Benutzers aus dem System und Zurücksetzen des App-Passworts von Benutzern.**
❸ **Suche nach Benutzern.**
❹ Klicken Sie auf einen Benutzernamen, um das Panel **Geo- und Timefencing und aktivierte Sticks** zu öffnen.



Aktivieren oder Deaktivieren des Benutzerzugriffs

1. Um den Zugriff eines Benutzers auf den verwalteten datAshur BT-Stick zu deaktivieren (zu untersagen), **deaktivieren** Sie das **Kontrollkästchen** unter „**Aktivieren**“, um das Häkchen zu entfernen, und klicken Sie auf „**Speichern**“, um den Zugriff für den Benutzer zu deaktivieren.

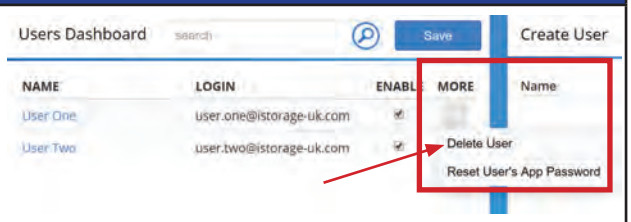
Anmerkung: Um den Benutzerzugriff zu aktivieren, klicken Sie auf das **Kontrollkästchen**, um das Häkchen erneut zu setzen, und klicken Sie dann auf **Speichern**.



Löschen eines Benutzers aus der Fernverwaltung

2. Um einen Benutzer aus der Fernverwaltung zu löschen, klicken Sie auf das **Menüfeld** unter „**Mehr**“, dann auf „**Benutzer löschen**“ und im Dialogfeld „**Bestätigung zum Löschen**“ auf „**Löschen**“.

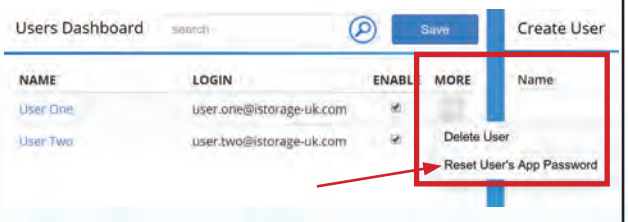
Anmerkung: Um den Benutzer wieder zur Fernverwaltung hinzuzufügen, gehen Sie zu **Abschnitt 4 - Erstellen von Benutzern über die Fernverwaltungskonsole.**



Zurücksetzen des Passworts der datAshur BT verwalteten App für einen Benutzer

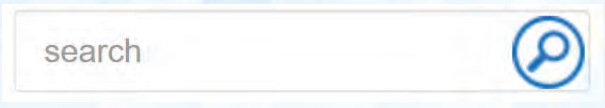
3. Um das Passwort für die datAshur BT verwaltete App eines Benutzers zurückzusetzen, klicken Sie auf das **Menüfeld** unter **Mehr** und dann auf **App-Passwort des Benutzers zurücksetzen**. Klicken Sie dann im Dialogfeld „**Zurücksetzen bestätigen**“ auf **Zurücksetzen**.

Anmerkung: Das Zurücksetzen des App-Passworts hat keinen Einfluss auf das Stick-Passwort und ändert dieses auch nicht (Standardeinstellung: 11223344). Wenn das App-Passwort zurückgesetzt wurde, erhält der Benutzer eine automatische E-Mail mit einem temporären Passwort.



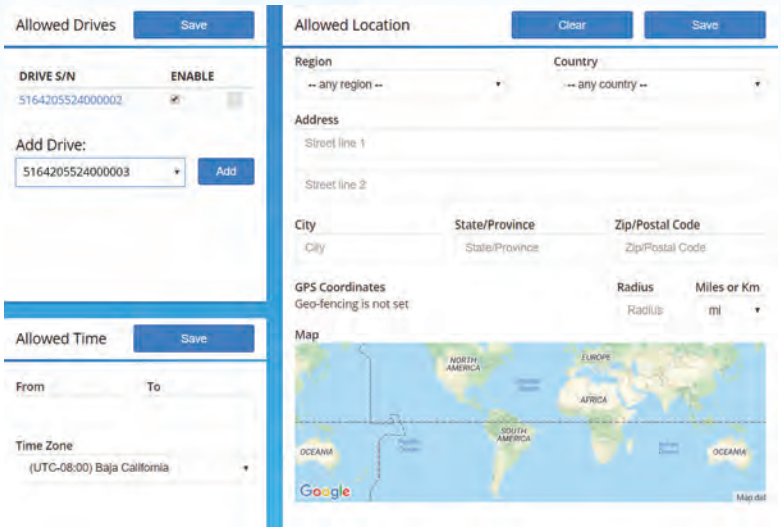
Suchleiste

4. Um nach einem Benutzer zu suchen, geben Sie entweder den Namen oder die E-Mail-Adresse des Benutzers in die Suchleiste ein und klicken Sie auf die Lupe.



Öffnen des Panels für Geo- und Timefencing

5. Wenn Sie auf einen Benutzernamen klicken, können Sie dort die Beschränkungen des Geo- und Timefencings verwalten. Siehe **Abschnitt 8 „Anwendung von Geo- und Timefencing-Einschränkungen“.**

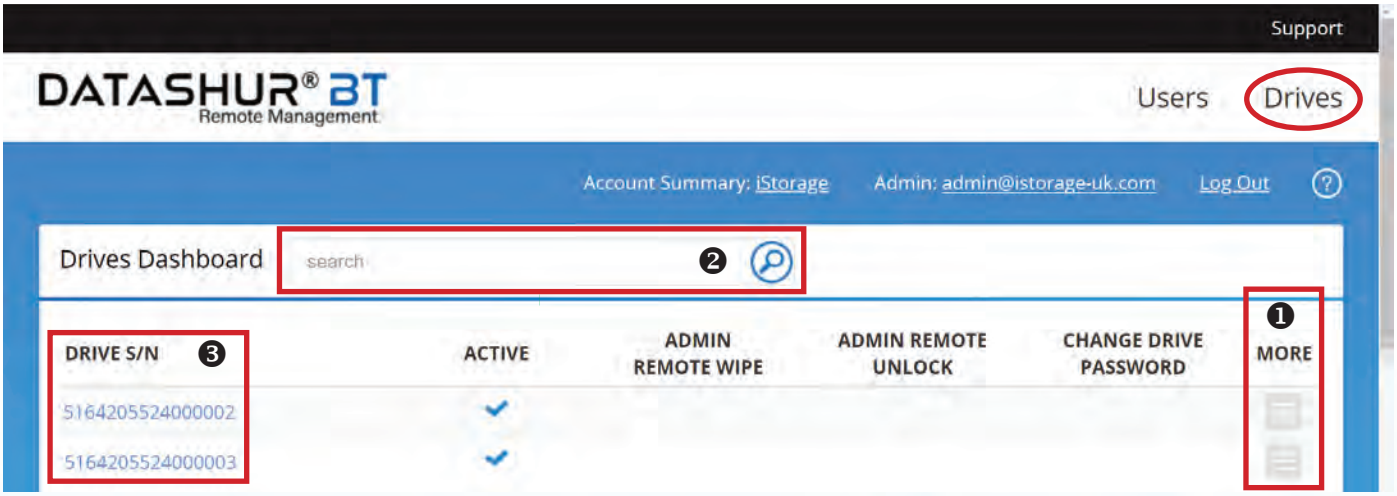


7. Dashboard für die Verwaltung von Sticks

Klicken Sie auf „**Sticks**“ in der oberen rechten Ecke des Bildschirms, um das „**Sticks-Dashboard**“ zu öffnen, wo der Administrator die folgenden Aktionen ausführen kann.

Sticks-Dashboard auf einen Blick

❶ **Löschen eines Benutzers aus der Fernverwaltung.**
❷ **Suche nach Stick-Seriennummer.**
❸ Klicken Sie auf eine **Stick-Seriennummer**, um die **Zugriffskontrolle** zu öffnen und zu verwalten.

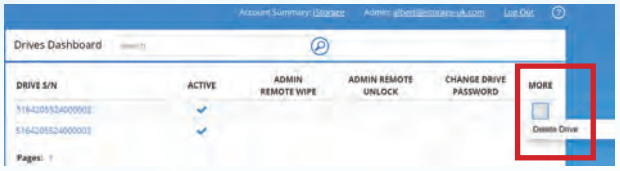


Anmerkung: Das **Häkchen** unter „**AKTIV**“ zeigt an, dass der Stick aktiv ist und von der Fernverwaltung verwaltet wird.

Löschen eines Sticks aus der Fernverwaltung.

1. Um einen Stick aus der Fernverwaltung zu löschen, klicken Sie auf das **Menüfeld** unter **Mehr**, dann auf Stick löschen und im Dialogfeld „**Löschen bestätigen**“, das auf die zu löschende Stick-Seriennummer verweist, auf „**Löschen**“.

Anmerkung: Um den Stick wieder zur Fernverwaltung hinzuzufügen, gehen Sie zu **Abschnitt 3 - Bereitstellung von verwalteten datAshur BT-Sticks.**



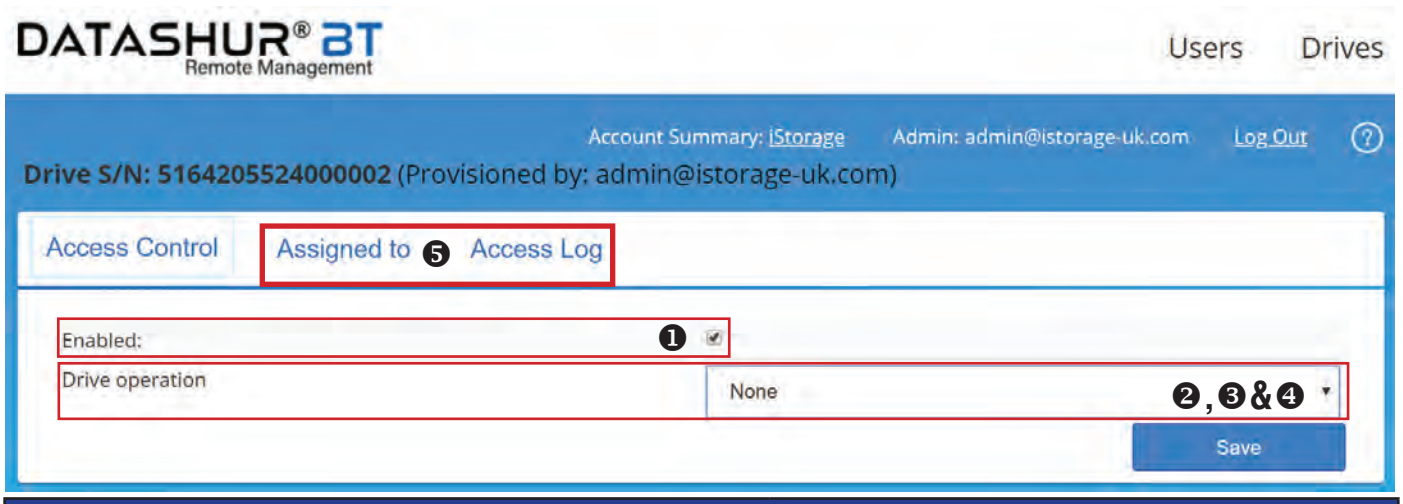
Suche nach Stick-Seriennummer.

2. Um nach einem Stick zu suchen, geben Sie die Seriennummer des Sticks in die Suchleiste ein und klicken Sie auf die Lupe.

Zugriffskontrolle verwalten

3. Wenn Sie auf eine **Stick-Seriennummer (S/N)** klicken, können Sie auf den Stick zugreifen und die folgenden Aktionen ferngesteuert verwalten:

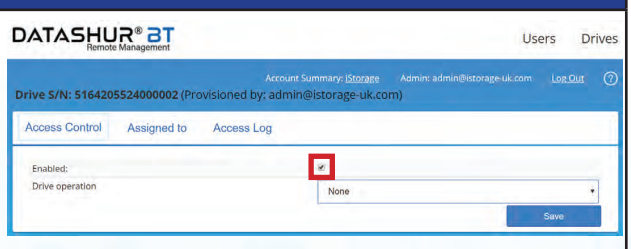
❶ **Aktivieren** oder **Deaktivieren** des Benutzerzugriffs.
❷ Löschen eines Sticks per Fernverwaltung.
❸ **Ändern eines Stick-Passworts** per Fernverwaltung.
❹ Entsperren eines Sticks per Fernverwaltung.
❺ Anzeigen der **Zuordnung** und des **Zugriffsprotokolls**



Aktivieren oder Deaktivieren des Zugriffs auf den Stick

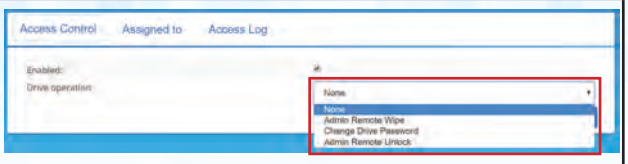
4. Um den Zugriff eines Benutzers auf den verwalteten datAshur BT-Stick zu **deaktivieren** (zu untersagen), **deaktivieren** Sie das **Kontrollkästchen** unter „**Aktivieren**“, um den Zugriff auf den Stick für den Benutzer zu deaktivieren.

Anmerkung: Um den Benutzerzugriff zu aktivieren, klicken Sie auf das **Kontrollkästchen**, um das Häkchen erneut zu setzen.



Löschen eines Sticks per Fernverwaltung.

6. Klicken Sie auf das Dropdown-Menü unter **Einsatz des Sticks** und anschließend auf „**Ferngesteuertes Löschen durch Administrator**“ (Zurücksetzen) und klicken Sie auf „**Speichern**“. Es wird die Bestätigungsmeldung „Stick-Änderungen wurden gespeichert“ angezeigt.

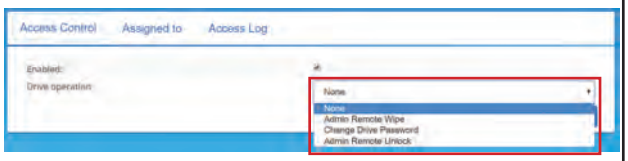


Anmerkung: Sobald „Ferngesteuertes Löschen durch den Administrator“ aktiviert wurde, wird ein **Häkchen** unter „**FERNGESTEUERTES LÖSCHEN DURCH DEN ADMINISTRATOR**“ im „Stick-Dashboard“ gesetzt. Dieses zeigt an, dass die „**ferngesteuerte Löschung**“ aussteht und aktiviert wird, sobald der verwaltete datAshur BT-Stick das nächste Mal mit der verwalteten datAshur App verbunden wird.

Das Häkchen wird entfernt (nicht markiert), sobald der Stick an einen Computer angeschlossen wird. So wird angezeigt, dass der Stick aus der Ferne gelöscht (zurückgesetzt) wurde.

Ändern eines Stick-Passworts per Fernverwaltung

7. Klicken Sie auf das Dropdown-Menü unter **Stick-Betrieb** und dann auf „**Stick-Passwort ändern**“. Geben Sie anschließend das **neue Passwort** in das Feld **Benutzerpasswort des Sticks** ein und klicken Sie auf „**Speichern**“. Es wird die Bestätigungsmeldung „*Stick-Änderungen wurden gespeichert*“ angezeigt.

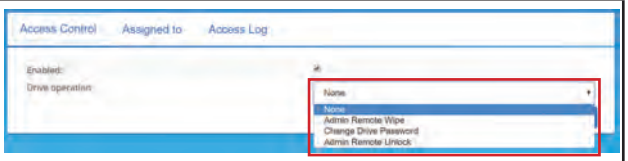


Anmerkung: Nach der Aktivierung von „Stick-Passwort ändern“ wird unter „STICK-PASSWORT ÄNDERN“ im „Sticks-Dashboard“ ein Häkchen angezeigt. Dieses gibt an, dass die Aktion aussteht und dass das neue Passwort zum Entsperren erforderlich ist, sobald der verwaltete datAshur BT-Stick das nächste Mal mit der verwalteten datAshur App verbunden wird.

Das Häkchen wird entfernt (nicht markiert), sobald der Stick an einen Computer angeschlossen und mit dem neuen Passwort entsperrt wird.

Entsperren eines Sticks per Fernverwaltung

8. Klicken Sie auf das Dropdown-Menü unter **Stick-Betrieb** und anschließend auf „**Ferngesteuertes Entsperren durch Administrator**“ und klicken Sie auf „**Speichern**“. Es wird die Bestätigungsmeldung „Stick-Änderungen wurden gespeichert“ angezeigt.



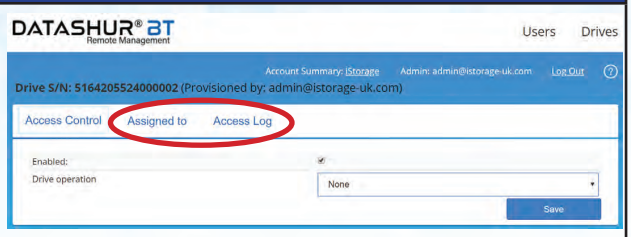
Anmerkung: Sobald „Ferngesteuertes Entsperren durch Administrator“ aktiviert wurde, wird unter „FERNGESTEUERTES ENTSPERREN DURCH ADMINISTRATOR“ im „Sticks-Dashboard“ ein Häkchen angezeigt. Dieses gibt an, dass die Aktion aussteht und dass beim nächsten Anschluss des verwalteten datAshur BT-Sticks an einen Computer der Stick ohne Eingabe des Stick-Benutzerkennworts entsperrt wird. Dies ist eine einmalige Aktion.

Das Häkchen wird entfernt (nicht markiert), sobald der Stick an einen Computer angeschlossen und per Fernsteuerung entsperrt wird.

Anzeigen der Zuordnung und des Zugriffsprotokolls

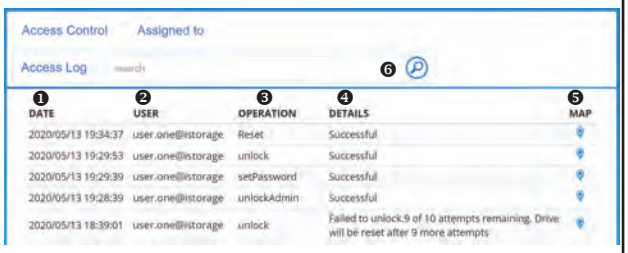
Zugeordnet zu

9. Die Registerkarte „**Zugeordnet zu**“ enthält den Namen des Benutzers, zu dem der Stick zugeordnet wurde, oder die Namen der Benutzer, wenn der Stick zu mehr als einem Benutzer zugeordnet wurde.



Zugriffsprotokoll

Das „Zugriffsprotokoll“ enthält die folgenden Informationen:



❶ Datum und Uhrzeit des Zugriffs des Benutzers auf den Stick.

❷ Die E-Mail-Adresse des Benutzers.

❸ Die Art der durchgeführten Operation, d. h. „Entsperren“ / „Zurücksetzen“ usw.

❹ Einzelheiten zu Stick-Zugriff

❺ Klicken Sie auf das Symbol „**Karte**“, um den Ort des letzten Zugriffs auf den Stick anzuzeigen.

❻ Suche nach „Art der durchgeführten Operation“ zum Filtern.

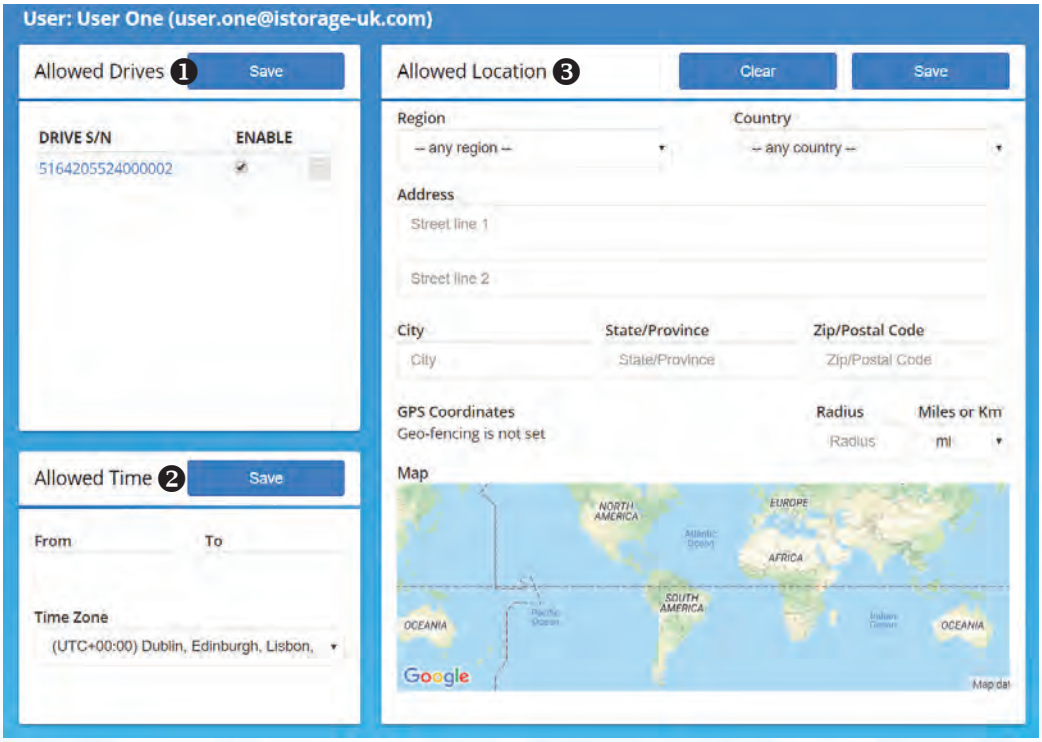
8. Anwendung von Geo- und Timefencing-Einschränkungen

Geo- und Timefencing auf einen Blick

❶ **Zugelassene Sticks -** Stick aktivieren/deaktivieren oder löschen

❷ **Zugelassene Zeit -** Timefencing

❸ **Zugelassener Ort -** Geofencing



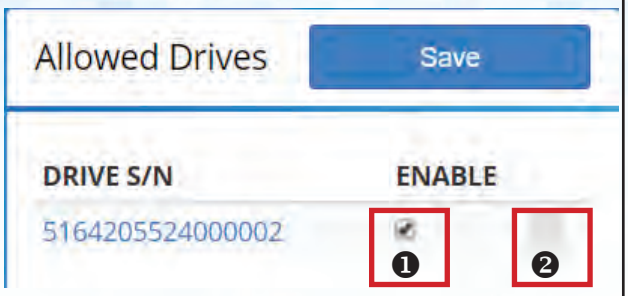
Zugelassene Sticks

1. Um den Zugriff eines Benutzers auf den verwalteten datAshur BT-Stick zu deaktivieren (zu untersagen), klicken Sie auf das **Kontrollkästchen (1)** unter „**Aktivieren**“, um das Häkchen zu entfernen, und klicken Sie auf „**Speichern**“, um den Zugriff für den Benutzer zu deaktivieren.

Anmerkung: Um den Benutzerzugriff zu aktivieren, klicken Sie auf das **Kontrollkästchen**, um das Häkchen erneut zu setzen, und klicken Sie dann auf **Speichern**.

2. Um einen Stick aus der Fernverwaltung zu löschen, klicken Sie auf das **Menüfeld (2)**, dann auf **Stick löschen** und im Dialogfeld „**Löschen bestätigen**“, das sich auf die Seriennummer des zu löschenden Sticks bezieht, auf **Löschen**.

Anmerkung: Um den Stick wieder zur Fernverwaltung hinzuzufügen, gehen Sie zu **Abschnitt 3 - Bereitstellung von verwalteten datAshur BT-Sticks**.

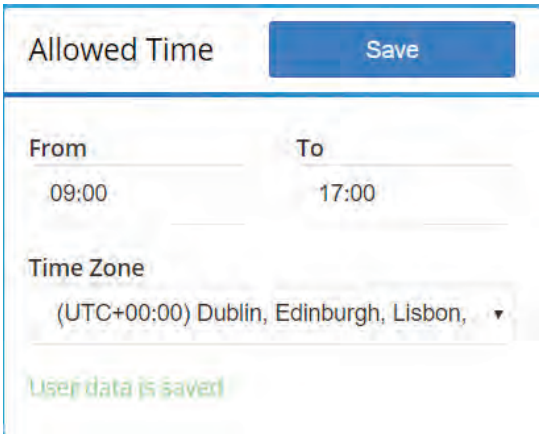


Festlegen von Timefencing-Einschränkungen

Timefencing kann auf jeden einzelnen Benutzer angewendet werden, wodurch die Nutzung eines Sticks auf einen bestimmten Zeitrahmen beschränkt wird, z. B. nur „**Von 09:00“ - „bis 17:00**“.

1. Um das Timefencing einzustellen, klicken Sie in das Feld „**Von**“ und wählen Sie entweder eine Zeit aus oder geben Sie sie manuell ein, und tun Sie dasselbe mit dem Feld „**Bis**“. Wählen Sie dann Ihre „**Zeitzone**“ aus dem Dropdown-Menü und klicken Sie auf **Speichern**. Als Bestätigung wird die Meldung „**Benutzerdaten gespeichert**“ angezeigt.

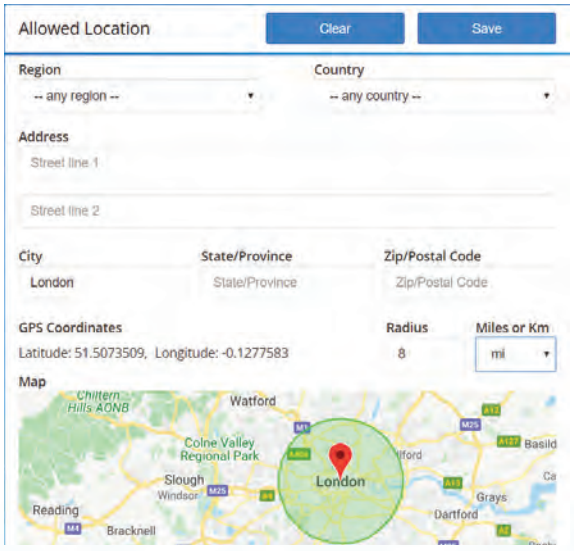
Anmerkung: Um Ihre Zeitauswahl zu löschen, klicken Sie auf die Felder „**Von**“ und „**Bis**“, löschen Sie die Einträge und klicken Sie dann auf **Speichern**.



Festlegen von Geofencing-Einschränkungen

Der Zugriff eines Benutzers kann eingeschränkt werden, indem der „**Erlaubte Standort**“ wie folgt eingestellt wird:

1. **Region:** Der Benutzerzugriff kann nach „**Region**“ eingestellt werden, zum Beispiel „Europa“.
2. **Land:** Wählen Sie zuerst die „**Region**“ und dann das „Land“ aus dem Dropdown-Menü.
3. **Adresse:** Füllen Sie das Feld „**Adresse**“ einschließlich Postleitzahl aus, um den Benutzerzugriff nur auf diese Adresse zu beschränken.
4. **Stadt:** Geben Sie den Namen einer „**Stadt**“ ein, z. B. London.
5. **Bundesland/Provinz:** Beschränken Sie den Benutzerzugriff auf ein bestimmtes Bundesland oder eine bestimmte Provinz.
6. **Postleitzahl:** Beschränken Sie den Benutzerzugriff auf eine bestimmte Postleitzahl.
7. **Radius:** Um den Radius um den „erlaubten Standort“ zu erweitern, geben Sie unter **Radius** einen Wert ein und wählen Sie dann entweder „**Meilen oder Km**“.
8. Klicken Sie auf „**Speichern**“, um Ihre Einschränkungen anzuwenden, oder klicken Sie auf „**Löschen**“, um alle Werte zu entfernen.

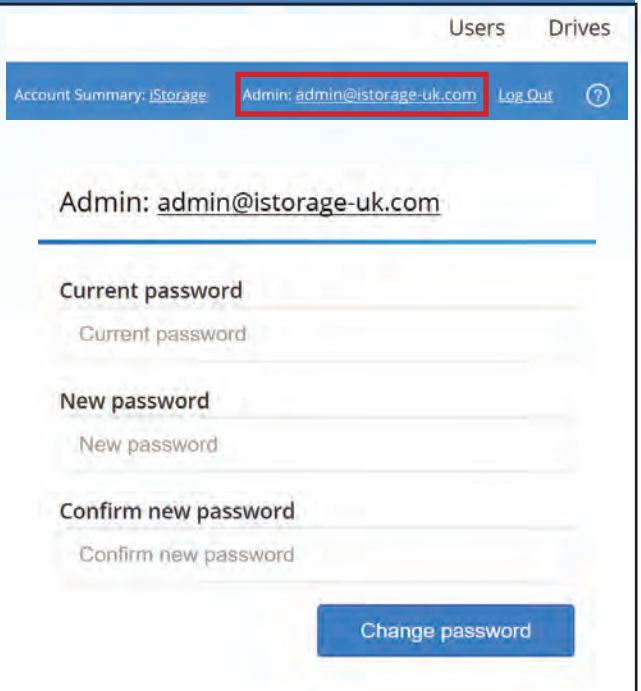


9. Ändern des Admin-Passworts

Um das Administrator-Passwort zu ändern, gehen Sie wie folgt vor:

1. Klicken Sie auf die „**E-Mail-Adresse des Administrators**“.
2. Geben Sie Ihr „**Aktuelles Passwort**“ ein, gefolgt von Ihrem „**Neuen Passwort**“, dann „**Neues Passwort bestätigen**“ und klicken Sie schließlich auf „**Passwort ändern**“.

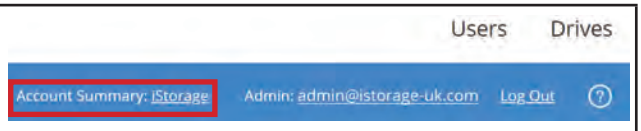
Anmerkung: Wenn Sie das Administrator-Passwort für die **Fernverwaltungskonsole** ändern, wird das Passwort für die **datAshur BT Administrator-App** automatisch aktualisiert und auf das gleiche Passwort gesetzt.
Denken Sie daran, dass das Administrator-Passwort sowohl für die **Fernverwaltungskonsole** als auch für die **datAshur BT Administrator-App** dasselbe ist.



10. Kontoübersicht

Um auf Ihre Kontoinformationen zuzugreifen und diese einzusehen, gehen Sie wie folgt vor:

1. Klicken Sie auf den Namen des Kontos neben „**Kontoübersicht**“ und navigieren Sie dann durch die folgenden Registerkarten:
   - **Übersicht**: Zeigen Sie Informationen bezüglich Ihrer gültigen Lizenz an, einschließlich der Anzahl der Administratoren, Benutzer und Sticks.
   - **Administratorenkontakte:** Zeigen Sie Details aller angemeldeten Administratoren an, einschließlich E-Mail-Adressen, Handynummern sowie Datum und Uhrzeit der letzten Anmeldung.
   - **Benutzerkontakte:** Zeigen Sie die Benutzernamen, E-Mail-Adressen sowie Datum und Uhrzeit der letzten Anmeldung an.
   - **Stick-Aktivität:** Zeigen Sie eine Liste aller Seriennummern, wann und von wem sie bereitgestellt wurden, den letzten Anmeldeversuch und die E-Mail-Adressen der Benutzer an.



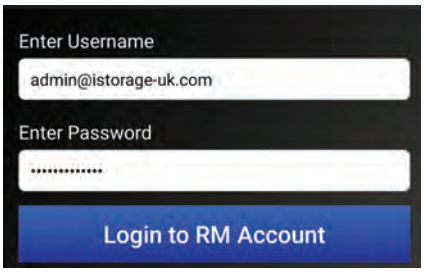
11. Bereitstellen von nicht verwalteten Sticks

Sie können einen zuvor verwendeten „**verwalteten**“ Stick in einen eigenständigen „**nicht verwalteten**“ Stick umwandeln, der nur mit der **datAshur BT persönlichen App** funktioniert, die im Apple App Store und in Google Play zum Download zur Verfügung steht.

Um mit der Bereitstellung zu beginnen und die Sicherheitsparameter für einen nicht verwalteten Stick einzustellen, fahren Sie mit den folgenden Schritten fort.

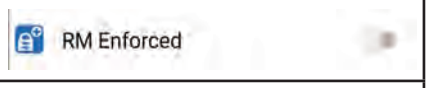
1. Öffnen Sie Ihre **datAshur BT Administrator-App** und geben Sie Ihren **Benutzernamen** und Ihr **Passwort** ein. Tippen Sie dann auf **Beim FV-Konto anmelden** (Fernverwaltung).

Anmerkung: Ihr Benutzername und Ihr Passwort für die datAshur BT Administrator-App und die webbasierte iStorage-Fernverwaltungskonsole sind identisch.



2. Nach erfolgreicher Anmeldung öffnet sich das Menü Laufwerkseinstellungen, in dem Sie Ihre Sicherheitseinstellungen wie unten beschrieben überprüfen und anwenden können:

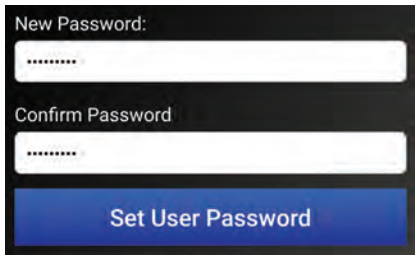
- **FV erzwungen:** Schalten Sie das **GRÜNE** Licht **AUS**. Fernverwaltungsfunktion deaktiviert



- **Benutzer-Passwort:** Der datAshur BT wird mit einem **Standardpasswort (11223344)** ausgeliefert. Um das Standardpasswort zu ändern, tippen Sie auf „**Benutzerpasswort**“, **geben** Sie dann Ihr neues **7-15**-stelliges Passwort ein und **bestätigen** Sie es. Tippen Sie schließlich auf „**Benutzerpasswort festlegen**“.

  Passwort-Anforderungen: Das Passwort muss 7-15 Zeichen lang sein und darf nicht nur aufeinanderfolgende oder sich wiederholende Zahlen oder Buchstaben enthalten.

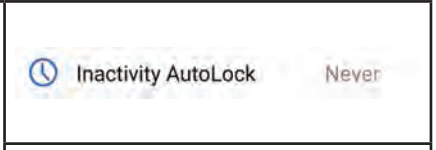
  Anmerkung: Aus Sicherheitsgründen empfehlen wir dringend, dass jeder Benutzer das Standard- oder vom Administrator festgelegte Passwort ändert, zu seinem/ihrem eigenen, eindeutigen 7-15 Zeichen langen Passwort, sobald der Stick an sie ausgegeben wurde.

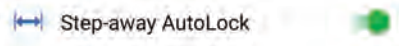
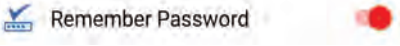
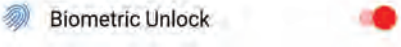
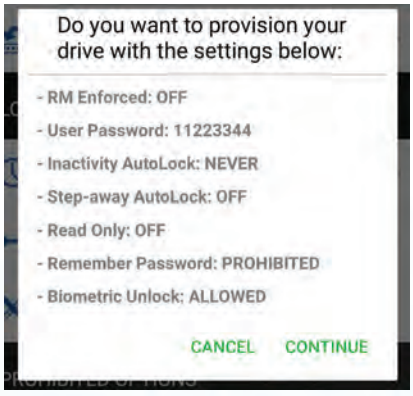


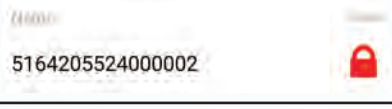
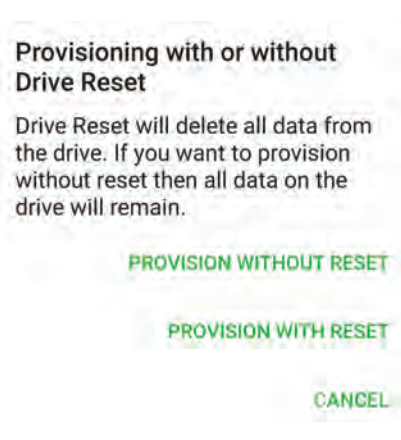
- **Automatische Sperrung wegen Inaktivität:** TZum Schutz vor unbefugtem Zugriff kann der datAshur BT so eingestellt werden, dass er nach einer voreingestellten Zeitspanne automatisch gesperrt wird, wenn der Stick entsperrt und unbeaufsichtigt ist. In der Standardeinstellung ist die Funktion datAshur BT automatische Sperrung wegen unbeaufsichtigter Inaktivität deaktiviert („Nie“), kann aber auf einen Wert zwischen **1 und 60** Minuten eingestellt werden.

  Um ein Zeitlimit festzulegen, tippen Sie auf automatische Sperrung wegen Inaktivität und dann auf , um die gewünschte Zeitdauer festzulegen.

  Anmerkung: Wenn der Administrator die automatische Sperrung wegen Inaktivität einstellt, kann der Benutzer diese Funktion nicht deaktivieren.



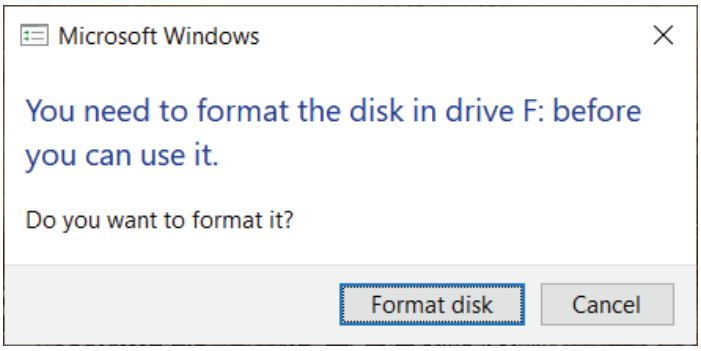
• **Automatische Entfernungssperrung:** Die automatische Entfernungssperrung ist standardmäßig deaktiviert. Wenn sie aktiviert ist (**GRÜNES** Licht leuchtet), wird dadurch der Stick gesperrt, wenn das Smartphone (Android/iOS) eines Benutzers für mehr als 5 Sekunden etwa 5 Meter vom datAshur BT-Stick entfernt ist. **Anmerkung:** Wenn der Administrator die automatische Entfernungssperrung wegen Inaktivität aktiviert, kann der Benutzer diese Funktion nicht deaktivieren.	
• **Schreibschutz einstellen:** Die Schreibschutzfunktion ist standardmäßig deaktiviert. Wenn sie aktiviert ist (**GRÜNES** Licht leuchtet), sind alle eingesetzten verwalteten datAshur BT-Sticks schreibgeschützt. **Anmerkung:** Wenn der Administrator den Schreibschutz aktiviert, kann der Benutzer diese Funktion nicht deaktivieren.	
• **Passwort merken:** Die Funktion Passwort merken ist standardmäßig aktiviert (AN), so dass Benutzer ihre Sticks ohne Eingabe des Passworts entsperren können. Um diese Funktion zu deaktivieren und Benutzern zu untersagen, ihre Sticks ohne Eingabe eines Kennworts freizuschalten, tippen Sie auf den grau unterlegten Schalter zum Deaktivieren (**ROTES** Licht leuchtet). **Anmerkung:** Wenn der Admin das Merken des Passworts **deaktiviert** (**ROTES** Licht leuchtet), kann der Benutzer diese Funktion nicht aktivieren.	
• **Biometrisches Entsperren:** Die biometrische Entsperrung ist standardmäßig aktiviert (AN), so dass Benutzer eine biometrische Entsperrung einstellen können, um auf ihren Stick zuzugreifen. Um diese Funktion zu deaktivieren und Benutzern zu untersagen, eine biometrische Entsperrung für den Zugriff auf ihre Sticks einzustellen, tippen Sie auf den grauen Schalter zum Deaktivieren (**ROTES** Licht leuchtet) **Anmerkung:** Wenn der Admin die biometrische Freischaltung **deaktiviert** (**ROTES** Licht leuchtet), kann der Benutzer diese Funktion nicht aktivieren.	
3. Tippen Sie hier, um Ihre Laufwerkseinstellungen zu bestätigen.	
4. Tippen Sie auf **Weiter**, um alle verwalteten datAshur BT-Sticks mit Ihren bevorzugten Einstellungen bereitzustellen.	

5. Notieren Sie sich die auf dem USB-Anschluss aufgedruckte **Geräte-ID** und **schließen Sie** den verwalteten datAshur BT-Stick an einen USB-Anschluss mit Stromversorgung an.	
6. Tippen Sie auf das **ROTE** Schlosssymbol. **Anmerkung:** Die Stick-LED blinkt **ROT**.	
7. Geben Sie die **Geräte-ID-Nummer** ein und tippen Sie dann auf **OK**.	
8. Wenn Sie einen zuvor verwendeten Stick bereitstellen, der nicht zurückgesetzt wurde, gehen Sie wie folgt vor. Andernfalls überspringen Sie diesen Schritt (wenn der Stick zurückgesetzt wurde) und fahren Sie mit Schritt 9 fort. • **Bereitstellung mit Rücksetzung:** Tippen Sie auf „**Bereitstellung mit Rücksetzung**“ und fahren Sie mit Schritt 9 fort. • **Bereitstellung ohne Rücksetzung:** Tippen Sie auf „**Bereitstellung ohne Rücksetzung**“ und fahren Sie mit Schritt 10 fort. **Anmerkung:** Die Bereitstellung ohne Rücksetzung löscht NICHT die zuvor auf dem bereitzustellenden Stick gespeicherten Daten.	
9. Tippen Sie auf das **GRAUE** (leere) Schlosssymbol, um die Bereitstellung abzuschließen.	
10. Sobald die Bereitstellung abgeschlossen ist, zeigt die App ein **GRÜNES** Häkchen an und die Stick-LED leuchtet durchgehend blau. Dadurch wird angezeigt, dass der datAshur BT-Stick bereitgestellt wurde.	
11. Wenn der Stick mit Rücksetzung bereitgestellt wurde (Schritt 8), werden Sie von Ihrem Computer aufgefordert, den Stick zu formatieren. Siehe Abschnitt 12 „Formatierung des datAshur BT für Windows“ bzw. Abschnitt 13 „Formatierung des datAshur BT für Mac OS“. **Anmerkung:** Nach der Formatierung kann der Administrator auf den Stick zugreifen und bei Bedarf Daten hinzufügen.	

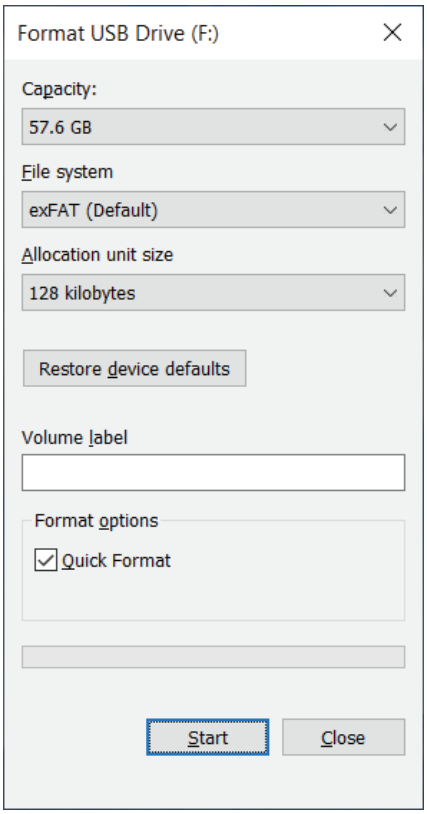
12. Formatierung des datAshur BT für Windows

Um Ihren datAshur BT für Windows zu formatieren, gehen Sie bitte wie folgt vor:

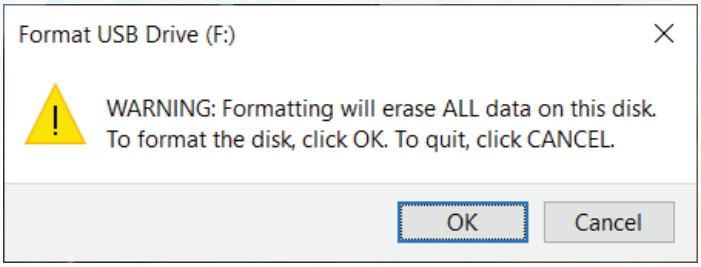
1. Das System zeigt das Fenster **Formatierung** an.



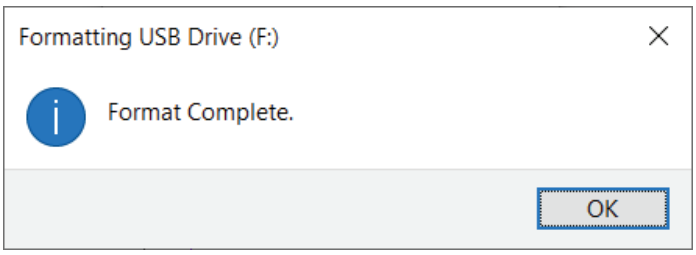
2. Klicken Sie auf „Laufwerk formatieren“ und das Fenster „USB-Laufwerk formatieren“ wird geöffnet.



3. Geben Sie im Feld „Volume“ einen Namen für das Laufwerk ein. Der Name des Laufwerks erscheint schließlich auf dem Desktop. Das Dropdown-Menü Dateisystem listet die verfügbaren Laufwerksformate auf, die Windows unterstützt. Wählen Sie entweder FAT32 oder exFAT, je nach Anforderung.
4. Klicken Sie auf **Start**.
5. Klicken Sie auf **OK**, um mit der Formatierung des Laufwerks fortzufahren.



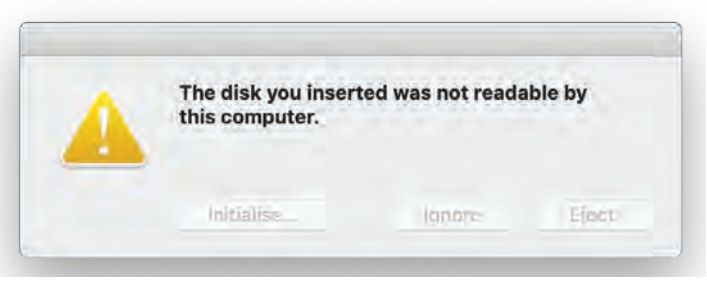
8. Der Vorgang beendet die Formatierung des Laufwerks und bestätigt, dass die Formatierung abgeschlossen ist.



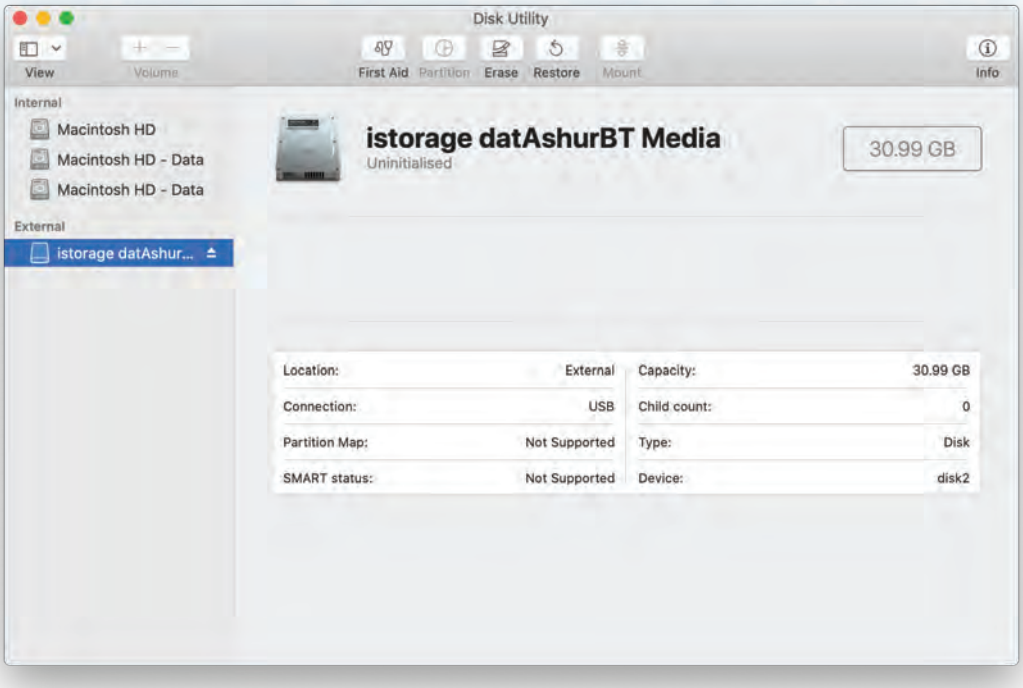
13. Formatierung des datAshur BT für Mac OS

Um Ihren datAshur BT für Mac OS zu formatieren, gehen Sie bitte wie folgt vor:

1. Das System zeigt das Fenster **INITIALISIERUNG** an.

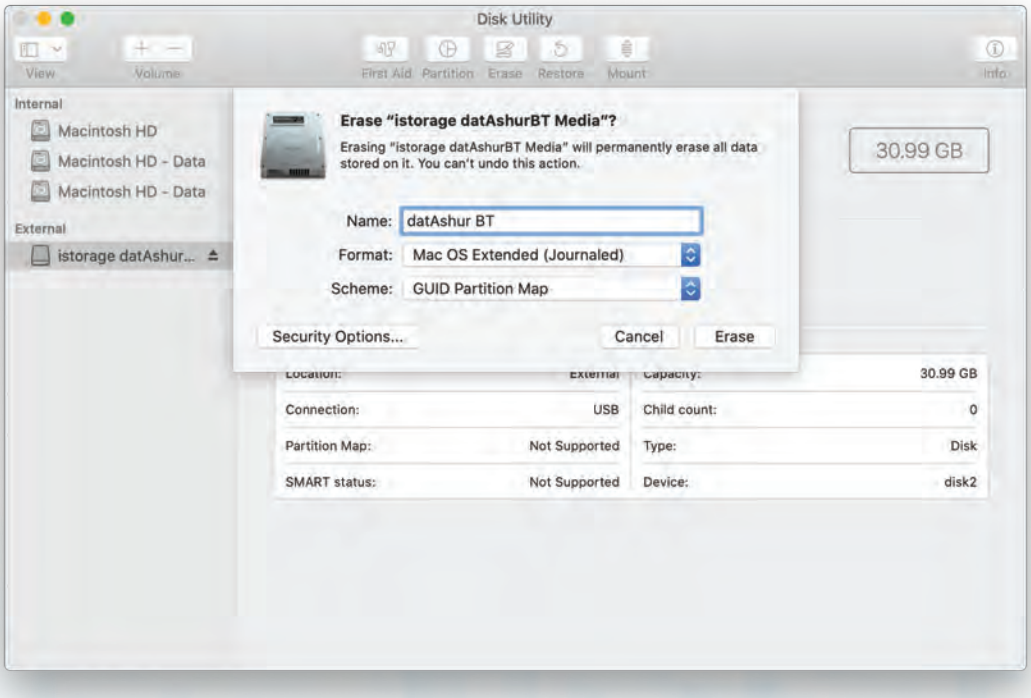


4. Klicken Sie auf **INITIALISIERUNG**, öffnen Sie das Festplatten-Dienstprogramm und wählen Sie den iStorage datAshur BT im Fenster des Festplatten-Dienstprogramms.

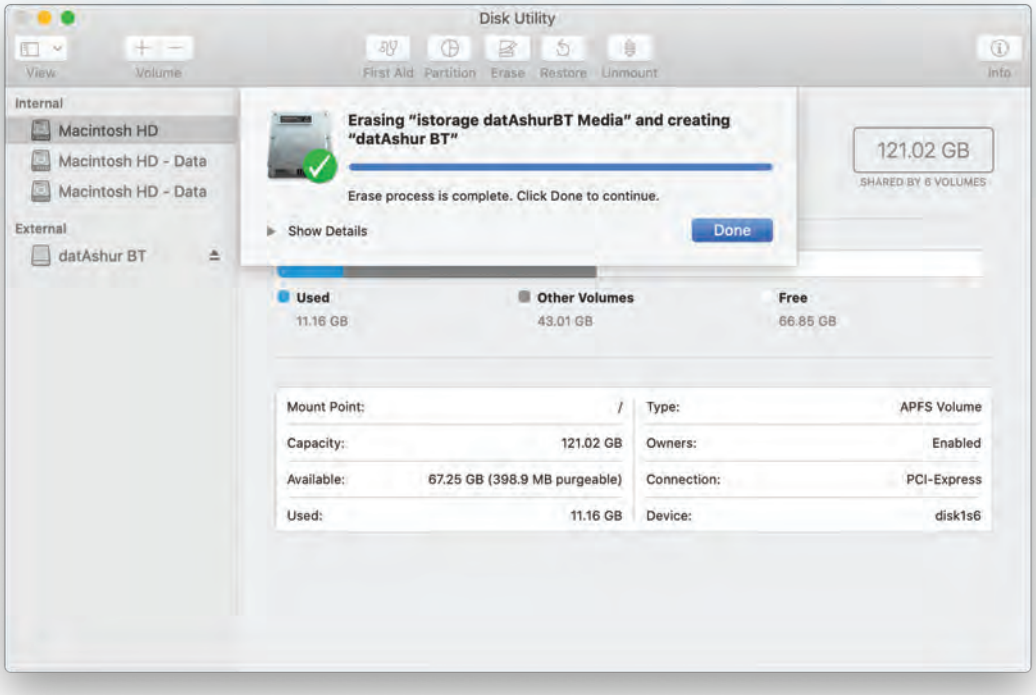


5. Wählen Sie **Löschen** aus dem Kontextmenü.

6. Geben Sie einen Namen für das Laufwerk ein. der Standardname lautet „Unbenannt“. Der Name des Laufwerks erscheint schließlich auf dem Desktop. Wählen Sie ein Schema und das zu verwendende Laufwerksformat aus. Das Dropdown-Menü „Laufwerksformat“ listet die verfügbaren Laufwerksformate auf, die der Mac unterstützt. Der empfohlene Formattyp ist Mac OS Extended (Journaled) für MacOS und MS-DOS für plattformübergreifende Nutzung. Das Dropdown-Menü „Schemaformat“ listet die verfügbaren Schemata auf, die verwendet werden können.



7. Klicken Sie auf **Löschen**.
8. Der formatierte datAshur BT erscheint im Fenster des **Festplatten-Dienstprogramms** und wird auf dem Desktop angezeigt



14. Technische Unterstützung

iStorage stellt die folgenden nützlichen Ressourcen für Sie bereit:

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

E-Mail-Kontakt
support@istorage-uk.com

Telefonischer Support über unsere Abteilung für technischen Support unter **+44 (0) 20 8991 6260**.
Die Spezialisten des technischen Supports von iStorage sind von 9:00 bis 17:30 Uhr
GMT von Montag bis Freitag erreichbar.

15. Garantie- und RMA-Informationen

ISTORAGE-PRODUKTHAFTUNG UND -GARANTIE

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

Diese Garantien gelten nicht für Mängel an den Produkten, die sich aus Folgendem ergeben:
- angemessene Abnutzung;
- mutwillige Beschädigung, anormale Lagerungs- oder Arbeitsbedingungen, Unfall, Fahrlässigkeit Ihrerseits oder durch Dritte;
- wenn Sie oder eine Drittpartei die Produkte nicht in Übereinstimmung mit der Bedienungsanleitung betreiben oder verwenden;
- jede Änderung oder Reparatur durch Sie oder durch einen Dritten, der nicht zu unseren autorisierten Reparaturdienstleistern gehört; oder
- jede von Ihnen zur Verfügung gestellte Spezifikation.

Im Rahmen dieser Garantien reparieren, ersetzen oder erstatten wir Ihnen nach unserem Ermessen alle Produkte, bei denen Materialfehler festgestellt wurden, vorausgesetzt, dass diese bei Lieferung vorhanden sind:
- sie inspizieren die Produkte, um zu prüfen, ob sie Materialfehler aufweisen; und
- Sie testen den Verschlüsselungsmechanismus in den Produkten.

Wir haften nicht für Sachmängel oder Mängel im Verschlüsselungsmechanismus der Produkte, die bei der Prüfung bei Lieferung feststellbar sind, sofern Sie uns diese Mängel nicht innerhalb von 30 Tagen nach Lieferung mitteilen. Wir haften nicht für Sachmängel oder Mängel im Verschlüsselungsmechanismus der Produkte, die nicht bei der Prüfung bei Lieferung feststellbar sind, sofern Sie uns diese Mängel nicht innerhalb von 7 Tagen mitteilen, nachdem Sie diese Mängel feststellen oder feststellen sollten. Wir sind im Rahmen dieser Garantien nicht haftbar, wenn Sie oder eine andere Person die Produkte weiterhin verwendet, nachdem ein Mangel festgestellt wurde. Nach der Mitteilung eines Defekts sollten Sie das defekte Produkt an uns zurücksenden. Wenn Sie ein Unternehmen sind, sind Sie für die Transportkosten verantwortlich, die Ihnen entstehen, wenn Sie Produkte oder Teile der Produkte im Rahmen der Garantie an uns senden, und wir sind für alle Transportkosten verantwortlich, die uns entstehen, wenn wir Ihnen ein repariertes oder Ersatzprodukt schicken. Wenn Sie eine Privatperson sind, lesen Sie bitte unsere Allgemeinen Geschäftsbedingungen.

Produkte, die zurückgegeben werden, müssen in der Originalverpackung und in sauberem Zustand sein. Zurückgegebene Produkte, die diesen Anforderungen nicht entsprechen, werden nach Ermessen des Unternehmens entweder abgelehnt oder es wird eine weitere zusätzliche Gebühr zur Deckung der zusätzlichen Kosten erhoben. Produkten, die zur Reparatur im Rahmen der Garantie zurückgesandt werden, muss eine Kopie der Originalrechnung beiliegen, oder es müssen die Originalrechnungsnummer und das Kaufdatum angegeben werden.

Wenn Sie eine Privatperson sind, gilt diese Garantie zusätzlich zu Ihren gesetzlichen Rechten in Bezug auf Produkte, die fehlerhaft sind oder der Beschreibung nicht entsprechen. Beratung über Ihre gesetzlichen Rechte erhalten Sie bei Ihrem örtlichen Bürgerberatungsbüro oder bei Ihrem Gewerbeaufsichtsamt

Die in diesem Abschnitt dargelegten Garantien gelten nur für den ursprünglichen Käufer eines Produkts von iStorage oder einem von iStorage autorisierten Wiederverkäufer oder Vertreiber. Diese Garantien sind nicht übertragbar.

MIT AUSNAHME DER HIERIN ENTHALTENEN BESCHRÄNKTEN GEWÄHRLEISTUNG UND SOWEIT GESETZLICH ZULÄSSIG, LEHNT ISTORAGE ALLE AUSDRÜCKLICHEN ODER STILLSCHWEIGENDEN GEWÄHRLEISTUNGEN AB, EINSCHLIESSLICH ALLER GEWÄHRLEISTUNGEN DER HANDELSÜBLICHEN QUALITÄT, DER EIGNUNG FÜR EINEN BESTIMMTEN ZWECK UND DER NICHTVERLETZUNG VON RECHTEN DRITTER. ISTORAGE GARANTIERT NICHT, DASS DAS PRODUKT FEHLERFREI FUNKTIONIERT. SOWEIT VON RECHTS WEGEN DENNOCH STILLSCHWEIGENDE GEWÄHRLEISTUNGEN BESTEHEN, SIND DIESE GEWÄHRLEISTUNGEN AUF DIE DAUER DIESER GARANTIE BESCHRÄNKT. DIE REPARATUR ODER DER ERSATZ DIESES PRODUKTS, WIE HIERIN VORGESEHEN, IST IHR AUSSCHLIESSLICHES RECHTSMITTEL.

IN KEINEM FALL IST ISTORAGE HAFTBAR FÜR VERLUSTE ODER ERWARTETE GEWINNE ODER FÜR MITTELBARE, STRAF-, BEISPIELHAFTE, BESONDERE, VERTRAUENS- ODER FOLGESCHÄDEN, EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF ENTGANGENE EINNAHMEN, ENTGANGENE GEWINNE, NUTZUNGSAUSFALL VON SOFTWARE, DATENVERLUST, ANDERWEITIGEN DATENVERLUST ODER -WIEDERHERSTELLUNG, SACHSCHÄDEN UND ANSPRÜCHE DRITTER, DIE SICH AUS EINER BELIEBIGEN WIEDERHERSTELLUNGSTHEORIE ERGEBEN, EINSCHLIESSLICH GARANTIE, VERTRAG, GESETZ ODER UNERLAUBTER HANDLUNG, UNABHÄNGIG DAVON, OB AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WURDE. UNGEACHTET DER LAUFZEIT EINER BESCHRÄNKTEN GARANTIE ODER EINER GESETZLICH IMPLIZIERTEN GARANTIE ODER FÜR DEN FALL, DASS EINE BESCHRÄNKTE GARANTIE IHREN WESENTLICHEN ZWECK VERFEHLT, ÜBERSTEIGT DIE GESAMTE HAFTUNG VON ISTORAGE IN KEINEM FALL DEN KAUFPREIS DIESES PRODUKTS. | 4823-2548-5683.3

DATASHUR® BT
ADMIN MANUAL

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