Copyright © 2020 iStorage Limited. All rights reserved.
Windows is a registered trademark of Microsoft Corporation.
All other trademarks and copyrights referred to are the property of their respective owners.
Distribution of the work or derivative work in any standard (paper) book form for commercial purposes is prohibited unless prior permission is obtained from the copyright holder.

DOCUMENTATION IS PROVIDED AS IS AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE HELD TO BE LEGALLY INVALID

iStorage shall not be liable by virtue of this warranty, or otherwise, for any incidental, special or consequential damage including any loss of data resulting from use or operation of the product, whether or not iStorage was apprised of the possibility of such damages

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 ................................................................................................................................. 4  
Box contents ................................................................................................................................. 4  
Useful Links ................................................................................................................................. 4  

datAshur BT Layout .................................................................................................................... 5  
Drive LED Indicators and their actions ....................................................................................... 5  

1. Registration .......................................................................................................................... 6  
2. How to enroll as an Administrator (Admin) ........................................................................ 7  
3. How to Provision datAshur BT Managed Drives ................................................................. 8  
4. How to Create Users via the Remote Management Console ............................................... 11  
5. How to Assign Drives to Users ........................................................................................... 12  
6. Managing Users Dashboard ............................................................................................... 13  
   User Dashboard at a glance ................................................................................................. 13  
   How to Enable or Disable User Access ............................................................................... 13  
   How to Delete a User from Remote Management .................................................................. 13  
   How to Reset User's datAshur BT Managed App Password ................................................ 13  
   Search Bar ............................................................................................................................ 14  
   Opening the Geo & Time-Fencing Panel .............................................................................. 14  
7. Managing Drives Dashboard .............................................................................................. 14  
   Drives Dashboard at a glance ............................................................................................ 14  
   How to Delete a Drive from Remote Management .............................................................. 15  
   Search by Drive Serial Number .......................................................................................... 15  
   Managing Access Control ................................................................................................. 15  
   How to Wipe a Drive via Remote Management .................................................................. 16  
   How to Change a Drive Password via Remote Management ............................................. 16  
   How to Unlock a Drive via Remote Management ............................................................... 16  
   Viewing Assigned to & Access Log ..................................................................................... 17  
8. How to Apply Geo & Time-Fencing Restrictions .................................................................. 17  
   Geo & Time-Fencing at a glance ......................................................................................... 17  
   Allowed Drives ..................................................................................................................... 18  
   How to set Time-Fencing Restrictions ............................................................................... 18  
   How to set Geo-Fencing Restrictions ................................................................................ 18  
9. How to Change the Admin Password ................................................................................ 19  
10. Account Summary .............................................................................................................. 19  
11. How to Provision a Non-Managed Drive .......................................................................... 20  
12. Formatting the datAshur BT for Windows ........................................................................ 23  
13. Formatting the datAshur BT for macOS .......................................................................... 24  
14. Technical Support ............................................................................................................. 27  
15. Warranty and RMA information ....................................................................................... 27
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
datAshur BT Layout

Drive LED indicators and their actions

<table>
<thead>
<tr>
<th>LEDs</th>
<th>LED State</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>🟢 (🟢) (🔵)</td>
<td>All LEDs blink once</td>
<td>datAshur BT conducts a self test when plugged to a computer</td>
</tr>
<tr>
<td>🔴</td>
<td>Solid Red</td>
<td>Locked - datAshur BT App not open</td>
</tr>
<tr>
<td>🔴 (🔴)</td>
<td>Blinking Red</td>
<td>Locked - datAshur BT App open</td>
</tr>
<tr>
<td>🔵</td>
<td>Solid Blue</td>
<td>datAshur BT is unlocked</td>
</tr>
<tr>
<td>🔵 (🔵)</td>
<td>Blinking Blue</td>
<td>datAshur BT is unlocked and communication in progress</td>
</tr>
</tbody>
</table>
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.

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.

### 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.

1. Enable or Disable User Access.
2. Delete User from system & Reset the Users App password.
4. 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

1. How to Delete a Drive from Remote Management.
2. Search by Drive Serial Number.
3. 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:
   - Enable or Disable Drive Access.
   - How to Wipe a Drive via Remote Management.
   - How to Change a Drive Password via Remote Management.
   - How to Unlock a Drive via Remote Management.
   - 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:
1. Date and Time of when the User accessed the Drive.
2. User’s email address.
3. Type of operation performed, i.e, 'Unlock' / 'Reset' etc.
4. Details of Drive access
5. Click on the 'Map' icon to view the location of where the Drive was last accessed.
6. Search by 'Type of operation performed' to filter.

8. How to Apply Geo & Time-Fencing Restrictions

Geo & Time-Fencing at first glance
1. Allowed Drives - Enable/Disable or Delete Drive
2. Allowed Time - Time-Fencing
3. 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.  
   
   Name: 5164205524000002
   
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.
8. 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.

![Disk Utility Window](image1)

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

6. 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.

![Erase Window](image2)
7. Click **Erase**.

8. 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) 20 891 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 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 NONETHLESS 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