SecureData Lock

MANAGED APP

SecureData Lock
Managed App
User Guide

SECURE
DATA

TABLE OF CONTENTS

SECUREDATA LOCK MANAGED

The SecureData Lock Managed application allows users to lock and unlock the SecureData BT and DUO drives (hereafter "drives") that are managed through Remote Management (RM). Additionally, users can adjust available drive settings and change their user password.

This app is used in conjunction with RM. Only Admins can set up user accounts and provision drives to be assigned to specific users.

Once the drives are assigned, the user can then use the functionality described in this manual.

For more information about RM and Admin capabilities, contact your Admin or SecureData.

Glossary

RM	Remote Management
Admin	IT Manager, administrator, or corporate manager
SecureData RM	Web software service to remotely control managed BT and DUO drive
SecureDrive BT	Secure Bluetooth-capable external portable drives from SecureData
SecureUSB BT	Secure Bluetooth-capable flash drives from SecureData
SecureDrive DUO	Secure keypad- and Bluetooth-capable external portable drives from SecureData
SecureUSB DUO	Secure keypad- and Bluetooth-capable flash drives from SecureData
SecureData Lock Admin	Mobile Admin app (iOS/Android) that controls BT and DUO drives
SecureData Lock Managed	Mobile app to be used with managed BT and DUO drives and RM

NOTE: The DUO drives have an onboard keypad, which cannot be used to unlock or input commands when a drive is managed.

SECTION 1: INSTALLATION AND CONFIGURATION

This section describes how to download and install the SecureData Lock Managed app.

Installing the SecureData Lock Managed App

The SecureData Lock Managed app must be installed on an iOS or Android device to manage the SecureDrive BT, SecureUSB BT, SecureDrive DUO and/or SecureUSB DUO.

To download the app, follow these steps:

1. Follow one of these links to download the app.

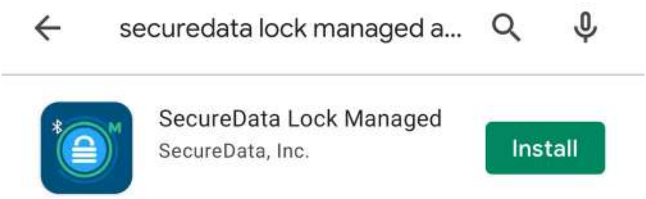
   Download on the App Store

   GET IT ON Google Play

   or

   On your device, go to the **Apple App Store** (iOS) or **Google Play Store** (Android).

2. In the search field, enter **SecureData Lock Managed**, and click the search button.



Select the application and download it onto the device.

> **NOTE:** Opening the application for the first time may be different for devices. Be sure to allow the app to access your location while using it. Contact SecureData Customer Support if you experience issues downloading or opening the app.

Configuration

Admin must set up your user credentials first. Use these credentials to log into the app. The only drives you may access are those assigned to your user credentials by Admin.

You cannot provision additional drives for use with this app. Contact your Admin to add additional drives or adjust settings.

SECTION 2: OPERATING INSTRUCTIONS

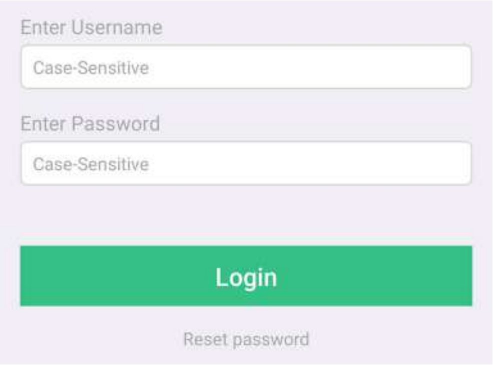
This section describes how to log in/out of the application, how to lock/unlock the drive, and how to adjust drive settings.

User Authentication

To log into the app, follow these steps:

1. Open the **SD Managed** app on your device.
2. On the **User Account Login** page, enter the email address and password for your user account.

NOTE: This is the email Admin used to set up the user account in Remote Management.

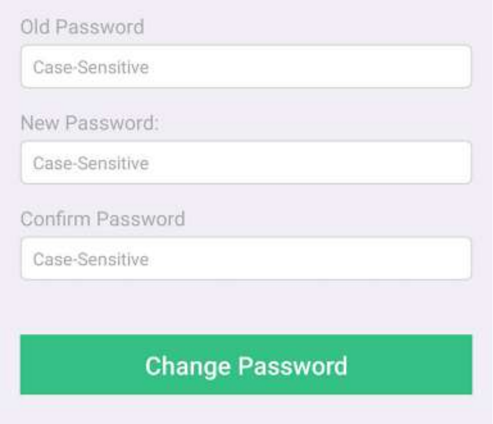


Click **Login**.

NOTE: This is a temporary password sent via email. You must change it once logged in.

To reset a password, follow these steps:

1. On the **User Account Login** page, click the **Reset Password** option.
2. Enter your user email address and click **Submit**.
3. Use the temporary password sent to your email to sign into the app.
4. On the **Set User Password** page, enter the temporary password in the **Old Password** field.
5. Enter your new password in the **New Password** and **Confirm Password** fields.
6. Click **Change Password**.



NOTE: After the new password is created, you will be taken to the **Managed Drives** page.

To change your password, follow these steps:

1. When logged into the app, click ? (iOS) or ⋯ (Android) in the upper right.
2. On the **Help Center** (iOS) or **Options** (Android) popup click the **Change Password** option.
3. On the **Change Password** page, enter the current password in the **Old Password** field.
4. Enter the new password into both the **New Password** and **Confirm Password** fields.
5. Click **Change Password**.

To log out of the app, follow these steps:

1. When logged into the app, click ? and then **Log Out** (iOS) or ⇦ in the upper right corner (Android)
2. After the **Notification** popup appears, click **Yes**.

> **NOTE:** To begin using the drive, you must create a password through the mobile app.

Password Requirements

Your password must:

- be 7–64 digits in length for DUO drives; or 7–15 characters in lenght for BT drives
- not contain only repetitive digits, e.g. (33333333) or characters
- not contain only consecutive digits, e.g. (12345678), (87654321), etc.

Creating a Password

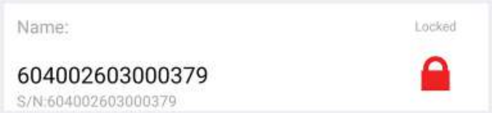
To create a user password, follow these steps:

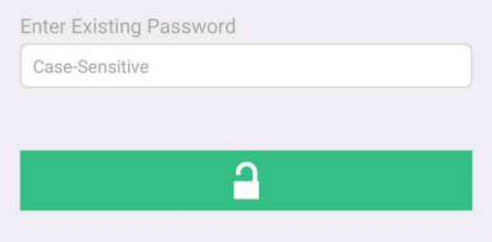
1. Connect the drive to a computer.
2. Start the **SD Managed** app on your device.
3. After it initializes, tap the drive name.
4. When prompted, enter the new password twice.

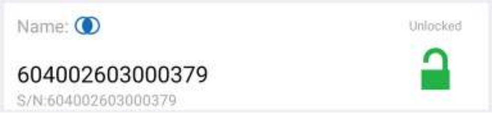
Unlocking the Drive

To unlock the drive, follow these steps:

1. On the **Managed Drives** page, click the drive you want to unlock.
2. On the **Drive Unlock** page, enter the password in the available field.
3. Click the **Unlock** button.


Name:
Locked
604002603000379
S/N:604002603000379


Enter Existing Password
Case-Sensitive


Name:
Unlocked
604002603000379
S/N:604002603000379

> **NOTE:** After unlocking the drive, you will be returned to the Managed Drives page. You will see the drive name with a green "unlocked" icon on the right along with the word "Unlocked."

> **NOTE:** After 10 consecutive, unsuccessful password attempts the user account will be deleted from the provisioned drive. All data is safe until Admin resets the drive.

Locking the Drive

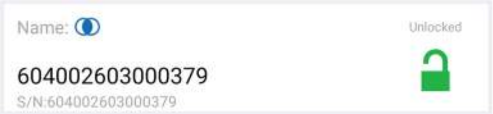
To lock the drive, follow these steps:

1. On the Managed Drives page, click the drive you want to lock and swipe left to reveal the red Lock button.
2. Click the Lock button.

> **NOTE:** You will be returned to the Managed Drives page and the drive will display the red “locked” icon.

To unlock the drive, follow the steps above.

> **NOTE:** You cannot unlock a managed DUO-drive with the onboard keypad, however you may press and hold the 🔑 button to lock it.

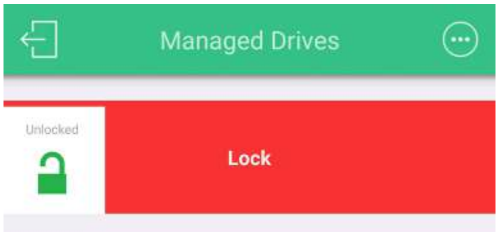


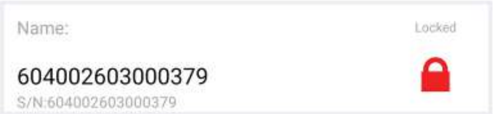
Name:

Unlocked

604002603000379

S/N:604002603000379





Name:

Locked

604002603000379

S/N:604002603000379

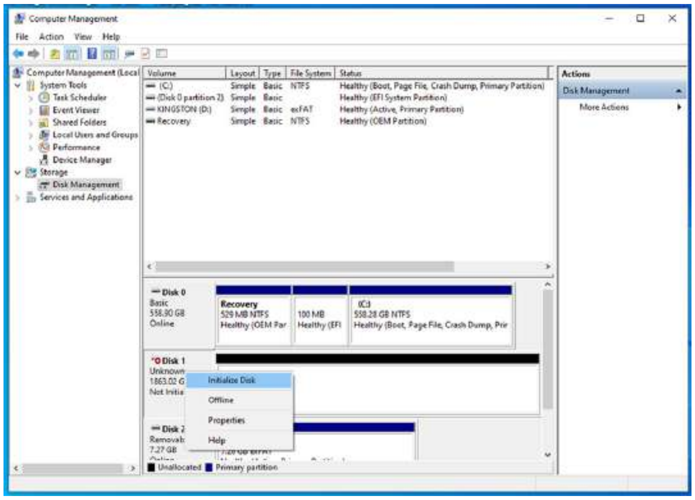
Initializing the Drive on Windows OS

When using the drive for the first time you most likely need to initialize it. To initialize your drive, do the following:

Admin permission for the PC is required for this procedure.

If you use **SecureDrive DUO** or **SecureDrive BT** do the following:

1. Connect the drive to your computer.
2. Create user password if you have not already done so.
3. Open **File Explorer**.
4. Right-click **This PC** > Left-click **Manage**.
5. In the Computer Management dialog’s left column, click **Storage** > **Disk Management** and wait for it to populate.
6. If the Initialize Disk dialog doesn’t pop up, right-click the “Unknown” disk (usually Disk 1) and click **Initialize Disk**.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)
(Disk 0 partition 2)	Simple	Basic		Healthy (EFI System Partition)
KINGSTON (D:)	Simple	Basic	exFAT	Healthy (Active, Primary Partition)
Recovery	Simple	Basic	NTFS	Healthy (OEM Partition)

Disk 0
Basic
558.90 GB
Online

Recovery
529 MB NTFS
Healthy (OEM Par

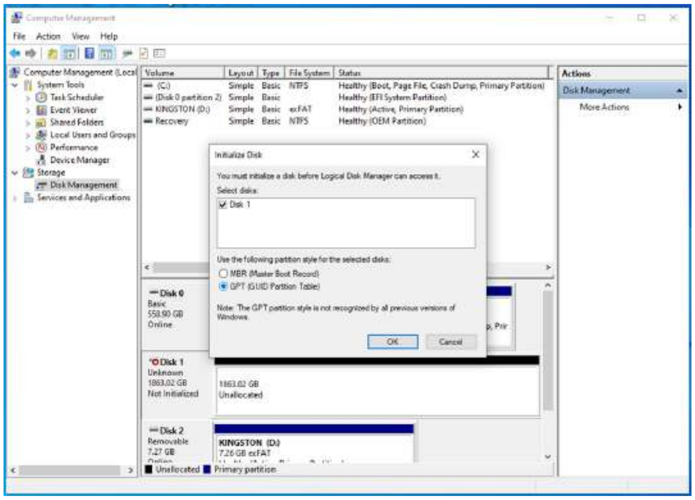
100 MB
Healthy (EFI

(C:)
558.28 GB NTFS
Healthy (Boot, Page File, Crash Dump, Pri

Disk 1
Unknown
1863.02 G
Not Initia

Disk 2
Removab
7.27 GB

7. Make sure **GPT** is selected, then click **OK**.



Volume	Layout	Type	File System	Status
(C:)	Simple	Basic	NTFS	Healthy (Boot, Page File, Crash Dump, Primary Partition)
(Disk 0 partition 2)	Simple	Basic		Healthy (EFI System Partition)
KINGSTON (D:)	Simple	Basic	exFAT	Healthy (Active, Primary Partition)
Recovery	Simple	Basic	NTFS	Healthy (OEM Partition)

Initialize Disk

You must initialize a disk before Logical Disk Manager can access it.

Select disks:

☑ Disk 1

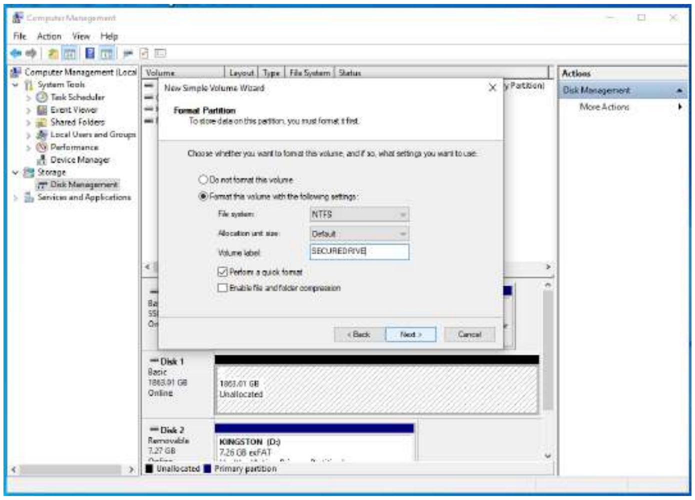
Use the following partition style for the selected disks:

○ MBR (Master Boot Record)

● GPT (GUID Partition Table)

Note: The GPT partition style is not recognized by all previous versions of Windows.

8. After Unknown changes to Online, right-click near **Unallocated** > **New Simple Volume**.



New Simple Volume Wizard

Format Partition

To store data on this partition, you must format it first.

Choose whether you want to format this volume, and if so, what settings you want to use.

○ Do not format this volume

● Format this volume with the following settings:

File system: NTFS

Allocation unit size: Default

Volume label: SECUREDRIVE

☑ Perform a quick format

☐ Enable file and folder compression

9. Follow the Wizard prompts. Select a drive letter (it generally defaults to the next available letter), then follow the prompts in the Wizard.
10. At the Format Removable Disk dialog, select a **Volume Label** and select **NTFS**.
11. Continue to follow the prompts. While the drive is formatting, the blue LED blinks (▬▬).
12. Click **Finish** to end and close the Wizard.
13. Close the Computer Management dialog if it's still open.

When finished, the new volume reads healthy and a second Explorer window opens to display the drive contents, and the blue LED on the drive lights up (▬).

Reformatting on Windows OS

If you use **SecureUSB DUO** or **SecureUSB BT**, you must next reformat the drive. To reformat, do the following:

To reformat on a Windows-powered computer, follow these steps:

1. Insert into a computer.
2. Unlock the drive with the user password.
3. In the popup message, click **Format Disk**.
4. Select **FAT32**, **NTFS** or **exFAT**, depending on your needs.
5. Click **Start**.
6. At the popup message, click **OK** to continue.
7. Click **OK**.

In the event that the Formatting Wizard doesn't display:

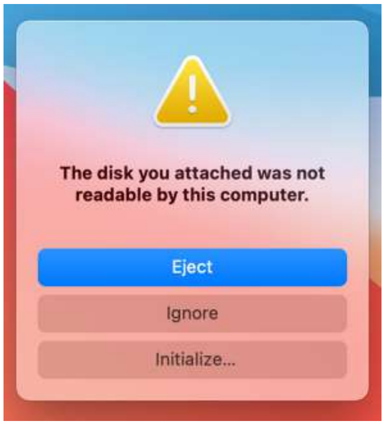
1. Open **File Explorer**.
2. Right-click the **Drive**. Click **Format**.
3. In the Format window, enter a volume label (optional) and then select **FAT32**, **NTFS**, or **exFAT**.
4. Click **OK**. This erases all data on the drive.
5. Click **OK** on the popup warning message.

NOTE: If you want your drive to be recognized by both PC and Mac, please format as **exFAT**.

Initializing the Drive on Mac OS

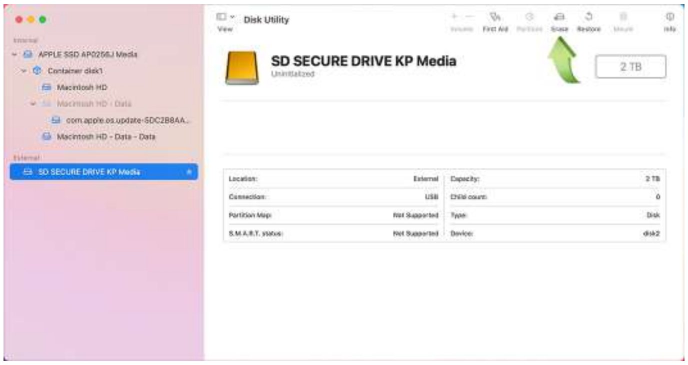
When using the drive for the first time you most likely need to initialize it. To initialize your drive, do the following:

1. Connect the drive to your computer.
2. Create user password if you have not already done so.
3. Click Initialize in the popup message. You may need to open Disk Utilities to begin formatting.



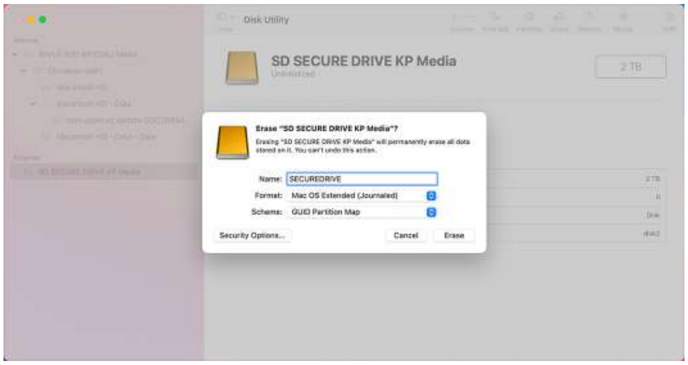
The disk you attached was not readable by this computer.

4. Ensure that your drive is highlighted in the list of external drives and click Erase. On the **Erase** popup choose the name and format, then click Erase.



SD SECURE DRIVE KP Media
Uninitialized

Location:	External	Capacity:	2 TB
Connection:	USB	Child count:	0
Partition Map:	Not Supported	Type:	Disk
S.M.A.R.T. status:	Not Supported	Device:	disk2

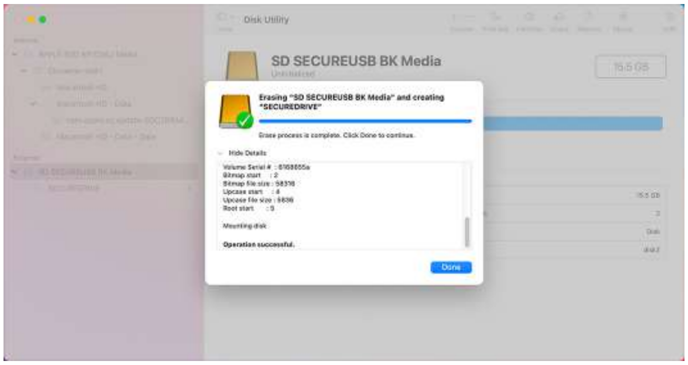


Erase "SD SECURE DRIVE KP Media"?
Erasing "SD SECURE DRIVE KP Media" will permanently erase all data stored on it. You can't undo this action.

Name: SECUREDRIVE
Format: Mac OS Extended (Journaled)
Scheme: GUID Partition Map

Security Options... Cancel Erase

5. Click Done in the message dialog when available.



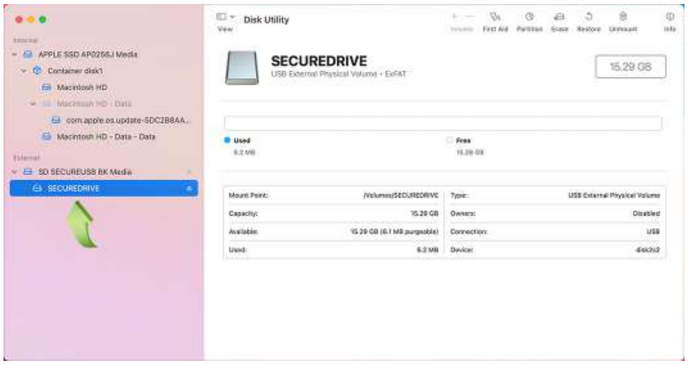
Erasing "SD SECUREUSB BK Media" and creating "SECUREDRIVE"

Erase process is complete. Click Done to continue.

```
Volume Serial # : 6168855a
Bitmap start     : 2
Bitmap file size : 58316
Upcase start     : 4
Upcase file size : 5836
Root start       : 5

Mounting disk

Operation successful.
```



SECUREDRIVE
USB External Physical Volume • ExFAT

Mount Point:	/Volumes/SECUREDRIVE	Type:	USB External Physical Volume
Capacity:	15.29 GB	Owners:	Disabled
Available:	15.29 GB (6.1 MB purgeable)	Connection:	USB
Used:	6.2 MB	Device:	disk2s2

NOTE: Your drive is now displayed under External in the left column.

6. Close the Disk Utility.

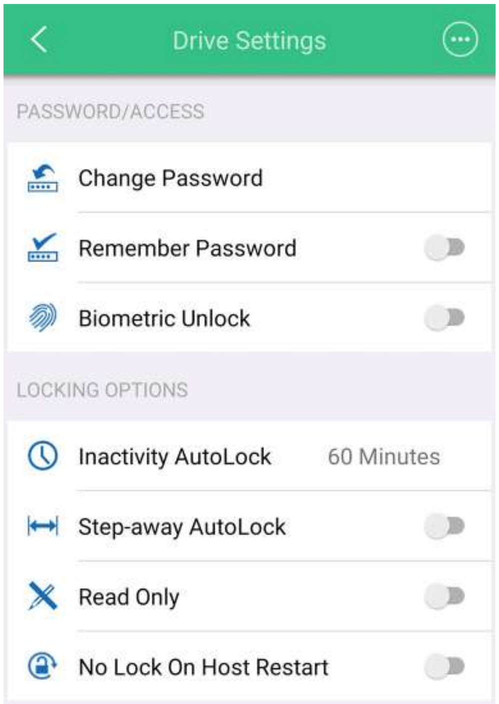
Modifying Settings

To access and modify the drive's settings, follow these steps:

1. Click on the drive name in the **Managed Drives** page to access settings.
2. On the **Settings** page, to enable/disable a feature press the button or text to the right when applicable:

NOTE: Modifiable settings are only available if they were initially enabled by the Admin at the time the drive was provisioned. If a setting was disabled by the Admin, it will display as grayed-out text and is not able to be modified or utilized.

- **Change Password** — This allows you to change the password to unlock the drive in the Managed Drives screen.



Drive Settings

PASSWORD/ACCESS

Change Password
Remember Password
Biometric Unlock

LOCKING OPTIONS

Inactivity AutoLock 60 Minutes
Step-away AutoLock
Read Only
No Lock On Host Restart

- **Remember Password** — This allows the drive to remember the password and bypass authentication.
- **Activate Biometric Unlock** — This allows you to skip the password and unlock via Touch ID or Face ID. Note that you must have these features enabled on your phone to use them on the app.
- **Inactivity AutoLock** — This feature allows you to set a time within which the drive locks after a period of inactivity. Select “Never” if you do not wish to have this feature active.
- **Step-Away AutoLock** — This feature locks the drive when the mobile device with the SD Managed app running on it is moved more than 10 feet from the drive or the SD Managed app is closed.
- **Read Only** — To put the drive in read only, select this option. You must lock and unlock the drive again for this feature to go into effect.
- **No Lock on Host Restart** — If you would like to boot from the drive and need it to remain unlocked while restarting the host (e.g. computer), select this option to allow the drive to remain unlocked.

NOTE: No Lock on Host Restart is not available on BT drives.

3. Click the back arrow to return to the **Managed Drives** screen.

DUO-Only Features

DUO drives include unique security features not available in BT drives. Admin must enable these features during provisioning, and users must contact Admin for details on these operations.

Self-Destruct PIN

In case of an emergency, should all data stored on the drive need to be quickly and irretrievably deleted, a user can enter the Self-Destruct PIN which Admin must provide. The Self-Destruct PIN is randomly generated during provisioning and has a one-time use.

NOTE: To get a new PIN, the drive must be reprovisioned.

NOTE: The Self-Destruct PIN is entered via the app.

Recovery PIN

In the event you need access to the drive and cannot remember the password and there is no internet connection, contact your Admin for the Recovery PIN. It is randomly generated and has a one-time use. Follow the steps below using the **onboard keypad:**

1. The user needs to press 3 + 🔑 together on the keypad.
2. The LED display on the drive shows a steady green light, and the red and blue lights blinking simultaneously.
3. Enter the Recovery PIN and press 🔑. The drive will unlock.

NOTE: To get a new PIN, the drive must be reprovisioned.

NOTE: If the one-time Recovery PIN has already been used, the drive indicates an unsuccessful password attempt (see **SecureDrive DUO** or **SecureUSB DUO** Manuals).

Offline Mode

Although the DUO has keypad and Bluetooth capabilities, managed drives are restricted to the app. An Admin may provision a drive to be in offline mode for a number of keypad unlocks at their discretion via an offline counter.

1. After Admin sets an offline counter, the user must open the **SD Managed** app at least once first to store the offline counter in the drive logic.
2. After the drive connects to the app, you may close the app and unlock the drive with the keypad by pressing 🔑, then entering the drive PIN.
3. Press 🔑 and the blue and red LEDs blink simultaneously.
4. Enter PIN and press 🔑.
5. The counter decreases by 1 after each successful unlock.

NOTE: When a user reaches the limit and the counter hits 0, when pressing 🔑 the red LED blinks rapidly.

NOTE: Keypad use is meant to allow use of the drive in situations where phone use is not allowed. Offline mode is limited to locking/unlocking only.

CONTACT AND COPYRIGHT INFORMATION

Contact Information

SecureData, Inc.
3255 Cahuenga Blvd. West #301
Los Angeles, CA 90068-1178

www.securedrive.com
US: 1-800-875-3230
International: 1-323-944-0822

Copyright Information

SecureDrive and SecureUSB products are developed and manufactured by SecureData and are based on DataLock technology licensed from ClevX, LLC. U.S. Patent. www.clevx.com/patents

All other trademarks and copyrights referred to are the property of their respective owners.

Registered Trademark	Owner
Android	Google, Inc.
Bluetooth	Bluetooth SIG, Inc.
DataLock, ClevX	ClevX, LLC
Mac, iOS	Apple, Inc.
SecureUSB, SecureDrive, SecureData	SecureData, Inc.
Windows	Microsoft

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.

RoHS