

SecureDrive DUO

User Guide

TABLE OF CONTENTS

SECTION 1: SECUREDRIVE DUO OVERVIEW.....	4
Requirements.....	4
Safety Information.....	5
EMI Cautions.....	5
Cautions.....	5
RF Exposure Statement.....	5
SECTION 2: GETTING STARTED.....	6
SecureDrive DUO Features.....	6
How It Works.....	6
LED Interpretations.....	7
Installing SecureData Lock App.....	9
Password Requirements.....	9
Procedural Conventions.....	9
Creating a Password.....	10
Adding the Drive to the App (Pairing).....	10
Creating a Password.....	10
Changing a Password.....	11
Unlocking the Drive.....	11
Locking the Drive.....	11
SECTION 3: SECUREDRIVE DUO SECURITY FEATURES.....	12
Brute-Force Protection.....	12
Reformatting.....	12
SECTION 4: BASIC COMMANDS.....	14
Bluetooth Feature and Status.....	14
Cancelling a Procedure.....	14
Inactivity AutoLock.....	15

Step-Away AutoLock.....	16
No Lock On Host Restart Mode.....	16
Read-Only and Read/Write Modes.....	17
App-Only Features.....	19
Change Name.....	19
2-Factor Authentication.....	19
Password Recovery.....	19
Remember Password.....	19
Activate Biometric Unlock.....	20
Enable Apple Watch.....	20
Remote Wipe.....	20
Minor Features.....	21

SECTION 5: COMMAND QUICK REFERENCE CHARTS.....22

SECTION 1: SECUREDRIVE DUO OVERVIEW

Thank you for purchasing the SecureDrive DUO External Portable Drive ('Drive' hereafter). This drive combines both user-authentication features of our SecureDrive KP and BT models. It's an easy-to-use, hardware-encrypted USB 3.0/3.1gen 1/3.2 gen1 external drive that is unlocked via the onboard alphanumeric keypad or wirelessly by a smartphone app.

The Drive uses military grade XTS-AES 256-bit hardware encryption, which encrypts all data stored on it in real-time. It works on all computer and embedded systems that support standard USB protocol. If your Drive is lost or stolen, rest assured that all data on it is protected and cannot be accessed without entering the password via the onboard keypad or the mobile app.

The Drive must be configured with a password prior to use, making it perfect for personal and business use and ideal for such regulated industries as healthcare, legal, corporate, and government.

Your Drive has Cloud Backup (one-month free trial subscription) with built-in DriveSecurity® anti-virus features installed. DriveSecurity is a one-year free license beginning on the date the drive is first used. For more information, please contact Technical Support at support@securedrive.com.

Requirements

The Drive must be connected to a computer for access. It works on Windows, Mac, Android, Linux, and Chrome operating systems, or any embedded system supporting USB 2.0, minimum.

Safety Information

This icon  indicates important information regarding safety of the product. Please be mindful of these messages. Contact Technical Support if you have questions.

-  Do not expose the Drive to water or moisture.
-  Resetting the Drive deletes all stored data as well as all passwords and settings.
-  Forgetting your password renders the Drive inaccessible. There is no ‘backdoor.’
-  Any changes or modifications not expressly approved by the party responsible for compliance could void the user’s authority to operate the device.

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 should 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 to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio or TV technician for help.

Cautions

Changes or modifications not expressly approved by the party responsible could void the user’s authority to operate this device. The normal function of the product may be disturbed by strong electromagnetic interference. If so, simply reset the product to resume normal operation by following the instruction manual. If you are unable to resume functions, please use the product in another location.

This device complies with part 15 of the FCC Rules. 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 operations.

RF Exposure Statement

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment.

SECTION 2: GETTING STARTED

SecureDrive DUO Features



How It Works

The SecureDrive DUO External Portable Drive combines the security features of our KP and BT models. It features an onboard, alphanumeric keypad and Bluetooth that can be paired with a mobile device through the SecureData Lock app.

Most commands can be entered through both the keypad and app features, though the user has access to all features using either. For specific information, please read further in this section and Section 4: Basic Commands below to see app- and keypad-specific commands.

NOTE: When using the keypad, you have 10 seconds to complete each step before the Drivetimes out.

NOTE: When using the app, the keypad is mostly disabled, except for the  button, as detailed below.

LED Interpretations

LED displays on the Drive are interpreted here by colored icons.

On the Drive

LED	Meaning
 (green and blue alternating blinks)	User password does not exist
 (momentarily, in that order)	Plugged into computer; momentary LED test
	Locked
	Locked, ready for the user password or Bluetooth is active. Keypad disabled (fast blinking)
 (half lit)	Unlocked; or Drive is in No Lock On Host Restart mode
	Settings mode; ready for keypad input
	Plugged into a computer and unlocked
	Ready for new User password through keypad input
	Ready for new password confirmation through keypad input
 (slowly blinking)	Drive is in Read Only mode
 (slowly blinking)	Charging and locked
 x5 (slowly blinking)	Keypad command failed
 x5 (slowly blinking)	Keypad command succeeded

On the App

App Icon	App Description	Meaning
	Change Password	Allows the user to change the password
	2-Factor Authentication	Enables user to add extra security by requiring authentication via password and a six-digit code sent via text message
	Password Recovery	Enables user to receive a text notification in the event of a forgotten password
	Remember Password	Allows user to unlock the Drive without entering a password
	Activate Biometric Unlock	Allows user to unlock via Touch ID and Face ID (iOS and Android)
	Inactivity AutoLock	Locks the Drive after a user-set period of inactivity
	Step-Away AutoLock	Requires the mobile device with the app to be within 10 feet of the Drive in order to operate
	Read Only	Sets the Drive to read-only mode
	No Lock On Host Restart	Prevents the Drive from locking during the host restart
	Enable Apple Watch	Allows syncing with an Apple Watch
	Reset Drive	Completely resets the drive and wipes all data
	Remote Wipe	Wipes data remotely

Installing SecureData Lock App

The SecureData Lock User is the app used to unlock your Drive via Bluetooth and must be installed on an iOS or Android mobile device to control the Drive's functions. Only one app is necessary to control multiple Drives.

Download the free app for an iOS device from the Apple App Store or for an Android device from Google Play. It can be installed just like any app by clicking Download, then Install.



To learn how to add or pair the app to the Drive, please read *Section 3: Adding the App to the Drive (Pairing)* below.

Password Requirements

NOTE: For customers who purchase the Drive through retail, you must create a new password prior to usage. For data recovery customers who receive their files returned on a Drive, a sales technician will supply you with the password.

Your password must:

- be 7–64 digits in length when using the onboard keypad or mobile app
- not contain only repetitive digits, e.g. (3333333)
- not contain only consecutive digits, e.g. (1234567), (7654321), etc.

⚠ CAUTION: Risk of loss of data. If you forget your password, all data will become inaccessible and reformatting will be required. There is no 'backdoor.' We recommend you enable the Password Recovery feature (see below) to prevent this.

NOTE: When setting a password for the onboard keypad, creating words by using corresponding number keys can be easier to remember than strings of numbers.

Procedural Conventions

You may unlock the Drive and perform other functions via the onboard keypad or the SecureData Lock App (or 'app') after inserting it into a host. The LED status shown is what you should see after performing each step.

Creating a Password

To begin using the Drive, you must create a password either through the onboard keypad or through the mobile app.

To create a password using the onboard keypad, follow these steps:

1. Press . The LED displays on the Drive will show solid red  and alternating blinking blue and blinking green lights , .
2. Press  . The LED will show a blinking blue light . Then enter a 7–64 digit password.
3. Press  . You will see a blinking green light  then re-enter the password.
4. Press  .
5. If successful, you will see ,  five times; if the command failed, you will see ,  five times.

To create a password using the app, follow these steps:

Adding the Drive to the App (Pairing)

You will need the eight-digit Device ID to pair the app. It is located on top of the Drive where the USB cable is inserted. To add the Drive, follow these steps:

1. Plug the Drive into a host.
2. Start the SecureData Lock App on your device.
NOTE: Ensure your device is Bluetooth-enabled.
3. If you have no paired drives, the new drive will automatically appear. If you have existing paired drives, tap the plus sign in the upper left corner.
4. Tap the Drive Name.
NOTE: If a password has not been created, the Drive will appear in the Paired Drives menu without asking for the device ID.
5. Enter the Device ID.

Creating a Password Creating a Password

To create a user password, follow these steps:

1. Connect the Drive to a computer.
2. Start the SecureData Lock App on your device.
3. After it initializes, tap the Drive name.
4. When prompted, enter the new password twice.
5. Enter a phone number for password recovery. You will also have the option to configure password recovery later.
6. If you proceeded with Step 5, enter the confirmation code sent to you via text.
NOTE: Use a mobile device when entering a number in the app to allow text messages.
NOTE: Per Step 5, for more information see *Section 4: Basic Commands below*.

Changing a Password

To change your password, you may do so through either the keypad or app features. Alongside the keypad commands are the LED indicators displayed on the Drive that show the code was entered properly.

To change the password by keypad, follow these steps:

1. Press  . 
2. Enter existing User Password.
3. Press   . 
4. Enter new User Password.
5. Press   . 
6. Re-enter new User Password.
7. Press  .
8. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

To change the password through the app, follow these steps:

1. Connect the Drive to a computer.
2. Open the SecureData Lock app on your mobile device.
3. Select the device by tapping its name and enter the existing password.
4. Wait until the Drive unlocks and tap on it. This takes you to SETTINGS.
5. Under PASSWORD/ACCESS, select Change Password.
6. Enter the old password.
7. Enter the new password in the New and Confirm Password fields.

Unlocking the Drive

You can unlock the Drive only after inserting it into the computer. To unlock the Drive by keypad, press  , enter the user password, then press .

To unlock the Drive by mobile app/Bluetooth, insert it into the computer. Open the app on the mobile device and enter the password.

Locking the Drive

The Drive can be locked multiple ways. We recommend safely ejecting it through the operating system. You may also press and hold  to lock the Drive.

From the app, you may select the Drive name. Swipe to the left and tap on Lock.

If the Drive is being used, the Drive will wait to lock until the activity has been completed. The red lock LED  indicates that the Drive is waiting to lock before it completes the action.

SECTION 3: SECUREDRIVE DUO SECURITY FEATURES

The SecureDrive DUO External Portable Drive is a password-protected drive designed with real-time military grade XTS-AES 256-bit hardware encryption. It is designed to protect data from breaches, or from unauthorized users who access a lost or stolen drive.

Brute-Force Protection

If a user enters an incorrect password ten consecutive times, regardless of the time intervals between attempts, the Drive's brute-force detection will trigger and the password, data, and all settings will be deleted. The encryption key and all data will become inaccessible and lost forever. The Drive will need to be formatted before it can be reused.

Reformatting

If the Drive needs to be reformatted due to hacking detection or following a reset, all data on it will be lost forever.

⚠ CAUTION: Loss of data. All data and settings will be deleted from the SecureDrive DUO when formatted, whether or not the brute-force hacking detection was triggered.

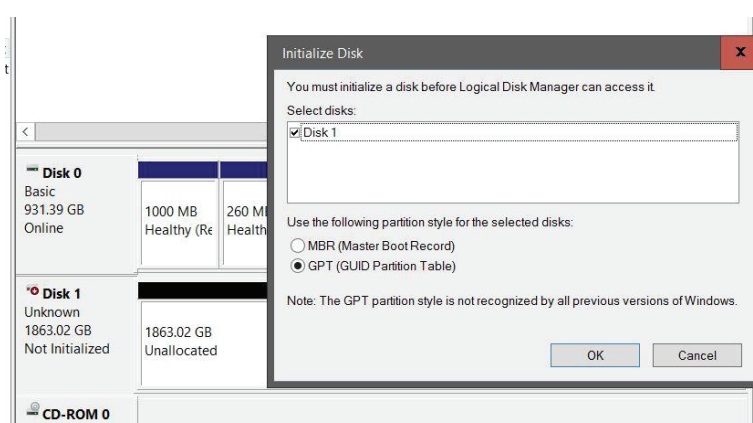
To initialize (reformat) your Drive, do the following:

Windows OS

Admin permission on the PC is required for this procedure. To reformat on a Windows-powered computer, follow these steps:

1. Connect the Drive to your computer with the USB cable.
2. Unlock the Drive with the User Password (for more information on creating one, see Section 3: Creating a Password below).
3. Open Explorer.
4. Right-click This PC then left-click Manage.
5. In the Computer Management window 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 'Unknown' (or 'Not Initialized') and click Initialize Disk.
7. Choose the desired partition type between MBR or GPT, then click OK.

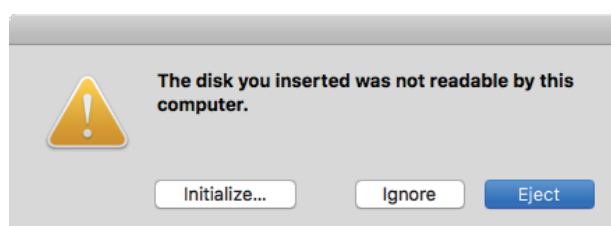
NOTE: GPT is needed for drives larger than 2 TB. For drives under 2 TB, use the MBR option.



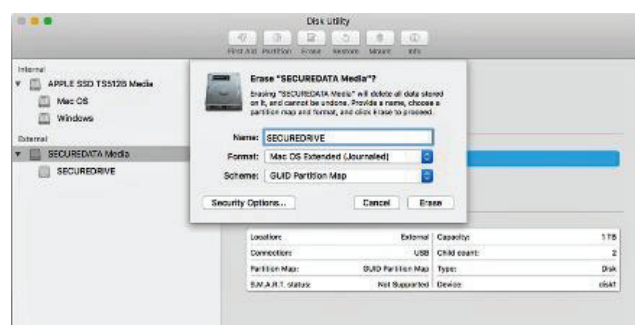
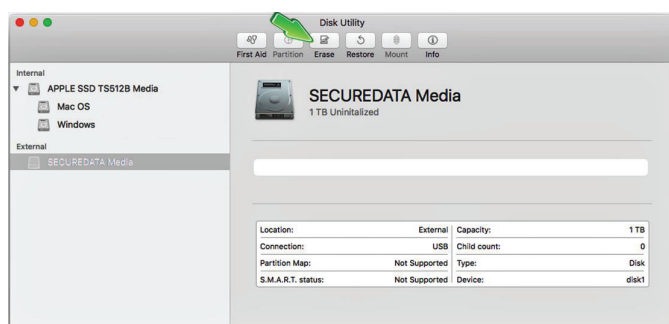
8. After Unknown changes to Online, right-click near Unallocated > New Simple Volume.
9. Follow the Wizard prompts. Select a Drive letter (it generally defaults to the next available letter) and then follow the prompts in the Wizard.
10. At the Format Removable Disk dialog, select a Volume label, and select the appropriate file system.
11. Continue to follow the prompts.
NOTE: 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.

For Mac OS

1. Connect to a Mac computer's USB port.
2. Unlock the Drive with the User Password (for more information on creating one, see Section 3: Creating a Password below).
3. Click Initialize in the popup message.



4. Ensure that your SecureDrive DUO is highlighted in the list of external drives and click Erase. The system begins erasing the external Drive.



5. Click Done in the message dialog when available.
NOTE: SecureDrive DUO is now displayed under External in the left column.
6. Close the Disk Utility.

SECTION 4: BASIC COMMANDS

Below are keypad codes and app functions that detail how to perform basic commands on the Drive. Alongside the keypad commands are the LED indicators displayed on the Drive that show the code was entered properly. Often, when proceeding to the next step after pressing  the LED display remains the same as the previous step.

Bluetooth Feature and Status

The Drive includes Bluetooth, which it uses to communicate with the mobile app. In some situations, you may not be able to use Bluetooth or wish to disable it. Even after disabling Bluetooth you may enable it again through the keypad.

By default, Bluetooth is already active. To disable this feature, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 280.
5. Press  .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

Once disabled, you may reactivate the Bluetooth feature. To enable it again, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 281.
5. Press  .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

If you are uncertain if Bluetooth has been enabled or disabled, using the keypad you may enter a command to check. To see its status on the Drive, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 728.
5. Press  .
6. If Bluetooth is currently enabled, you will see  ,  five times. If it is disabled, you will see  ,  five times.

Cancelling a Procedure

To cancel most procedures prior to finishing the input on the keypad, press and hold  for six seconds. You may also let the Drive time-out after 10 seconds.

Inactivity AutoLock

With the Inactivity AutoLock feature, you may set the Drive to automatically lock after a specified time between 1 and 60 minutes due to inactivity. Alternatively, you may deactivate this feature at any time.

Enabling

To set AutoLock via keypad, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 85 (or T, L for Time-Lock).
5. Press  . 
6. Enter the number of minutes before the Drive should go idle, 01–60. (means 1 through 60 minutes).
7. Press  .
8. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

To set AutoLock via the app, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under LOCKING OPTIONS, select Inactivity AutoLock.
4. Select the number of minutes before the Drive should go idle.

Disabling

To disable the AutoLock feature via keypad, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 85 (or T, L for Time-Lock).
5. Press  . 
6. Enter 00.
7. Press  .
8. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

To disable AutoLock via the app, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under LOCKING OPTIONS, select Inactivity AutoLock.
4. Select Never.

Step-Away AutoLock

When connected to the app, the Drive can be set to lock when the mobile device is more than 10 feet away from the Drive. This feature cannot be activated by keypad.

To set up the Step-Away AutoLock feature, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under LOCKING OPTIONS, select Step-away AutoLock.
4. The button will shift to the right and will appear green when activated.

To turn off the Step-Away AutoLock feature, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under LOCKING OPTIONS, select Step-away AutoLock.
4. The button will shift to the left and will no longer appear green when deactivated.

No Lock On Host Restart Mode

If you want to allow the Drive to remain unlocked when restarting a host, you may activate the No Lock On Host Restart feature.

⚠ CAUTION: This feature could compromise the security of the Drive. We suggest disabling this feature when it is not needed.

NOTE: The Inactivity AutoLock and Step-Away AutoLock features will override the No Lock On Host Restart feature. If you have either of these active, the Inactivity AutoLock will lock the Drive after the time limit you set and Step-Away AutoLock will lock the Drive if the mobile device is more than 10 feet from it.

Enabling

To turn on the No Lock On Host Restart mode via keypad, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 561.
5. Press  .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

To turn on the No Lock On Host Restart mode via the app, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Select the No Lock On Host Restart option.

4. Read the warnings and tap Continue.

5. The button will shift to the right and will appear green when activated.

Disabling

To turn off the No Lock On Host Restart mode via keypad, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 560.
5. Press  .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

To turn on the No Lock On Host Restart mode via the app, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Select the No Lock On Host Restart option.
4. The button will shift to the left and will no longer be green when deactivated.

Read-Only and Read/Write Modes

You may set the Drive to be read-only and prevent any alteration of documents or saving to the drive, permitting only reading from it. You may also disable this feature and allow writing to the Drive.

NOTE: When Read-Only mode is activated, the Drive will lock in order to set this mode. After enabling Read-Only mode, simply unlock the device with your User password and it will be in Read-Only mode.

Read Only

To put the Drive in Read-Only mode via keypad, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 76 (or R, O for read only).
5. Press  .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

To put the Drive in Read-Only mode via the app, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under LOCKING OPTIONS, select Read Only.
4. When the prompt appears, press Lock.
5. The button will shift to the right and will appear green when activated.

Read/Write

To allow a user to write to the Drive via keypad, follow these steps:

1. Press  . .
2. Enter User Password.
3. Press    .  , .
4. Enter 79 (for R, W or read/write).
5. Press .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

To allow a user to write to the Drive via the app, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under LOCKING OPTIONS, select Read Only.
4. When the prompt appears, press Lock.
5. The button will shift to the left and will no longer appear green when deactivated.

Resetting the Drive

If you need to completely reset the Drive, you may do so using the keypad or app.

⚠ CAUTION: Resetting the Drive will wipe it clean and you will lose all data stored on it.

To reset the Drive via keypad, follow these steps:

1. Press and hold 7 and  .  ,  (alternating)
2. Press 999.
3. Press and hold 7 and  . .

To reset the Drive via the app, follow these steps:

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under RESETTING/DELETING, select Reset Drive.
4. At the prompt, press Reset Drive.
5. Enter the serial number OR use the mobile device's camera to scan the barcode.

If you forgot your password and want to reset the drive, you may do so through the app. To reset without entering a password, follow these steps:

1. Open the app and select the Drive.
2. Tap the Drive name to open the Drive Unlock screen.
3. At the bottom of the screen, tap Reset Drive.
4. When the prompt appears, to proceed press Reset Drive.

App-Only Features

While most of the functions can be entered via keypad or app, there are some that are available only using the app. Open the app and you may select any of the following to enable them.

Change Name

You may customize the name of your drive showing in the app by selecting Change Name. Simply rename the device to any you like, then press Change Name.

NOTE: Changing the name will not change the Drive's volume label.

2-Factor Authentication

You may use this feature for additional security.

1. In the SETTINGS menu, under PASSWORD/ACCESS, select 2-Factor Authentication.
2. When the prompt appears, press Continue.
3. On the next screen, enter your mobile number and continue.
4. You will receive a confirmation code via text.
5. At the Enter Confirmation Code screen, enter the six-digit code you received via text and press Continue.
6. In all future attempts to unlock the Drive, you will need to unlock via your password and a six-digit code sent via text.

Password Recovery

If you forget your password, all data will become inaccessible and reformatting will be required. There is no 'backdoor.' We recommend that you enable the Password Recovery feature to prevent this.

1. In the SETTINGS menu, under PASSWORD/ACCESS, select Password Recovery.
2. When the prompt appears, press Continue.
3. On the next screen, enter your mobile phone number.
4. You will receive a confirmation code via text.
5. At the Enter Confirmation Code screen, enter the six-digit code you received via text and press Continue.

Remember Password

If you would like to opt out of the added security, you may set the app to remember the password. Once you open the app and select the Drive, it will automatically unlock without requiring any authentication.

⚠ CAUTION: Security is degraded when the password is stored.

Activate Biometric Unlock

For Apple/iOS and Android users, you may unlock the Drive using Touch ID or Face ID.

1. In the SETTINGS menu, under PASSWORD/ACCESS, select Biometric Unlock.
2. When the prompt appears, press Yes.

NOTE: Ensure that Touch ID or Face ID are enabled on your mobile device.

Enable Apple Watch

If you have an Apple Watch, you may use it to unlock the Drive.

Remote Wipe

To wipe the Drive of its data remotely, you may do so through Remote Wipe.

NOTE: This is a two-part process: enabling/disabling and activating. We suggest enabling Remote Wipe if you are worried that you may lose your drive and would like to initiate this feature if the Drive is lost.

The first part is the enabling/disabling step.

1. Open the app, select the Drive, and unlock it.
2. Tap the Drive name to go to SETTINGS.
3. Under RESETTING/DELETING, select Remote Wipe.
4. The button will shift to the right and will appear green when activated.
5. When the prompt appears, press Enable.

⚠ CAUTION: The next part of the process is irreversible. Be certain that the drive is lost or stolen before proceeding.

This will erase all data from the drive. The second part is the activating step. To perform a remote wipe of data, follow these steps:

1. Open the app.
2. Write down the serial number (shown underneath the drive name)
3. Press on the Drive name and swipe right.
4. Press Wipe.
5. Type the serial number of the drive and tap Remote wipe button

At the next attempt to unlock the Drive, it will automatically be reset.

⚠ CAUTION: If you lost the Drive and activated Remote Wipe, but locate the Drive later, do **NOT** try to open it. Please contact SecureData Tech Support, as it will otherwise be irreversibly wiped.

Minor Features

The keypad has codes for minor features that you may find beneficial when using the Drive, and their operations are expressed through the LEDs.

You may see the system version and an indicator of when a button is pushed on the keypad. These are additions to help with your experience, but are not security features.

To see the version, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 86 (or V, N for version number).
5. Press  .  ,  ,  once, then  , .
6. The green and red LEDs will display which version is in use: the red lock () blinks if it's a major version; the green lock () blinks if it's a minor version.

To get a visual confirmation that a button on the keypad is pressed, you may activate the key press indication. To do this, follow these steps:

1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 571.
5. Press .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

Once this has been activated, the red, blue, and green LEDs will flicker each time a button is pushed,

To turn off the key press indication, follow these steps:

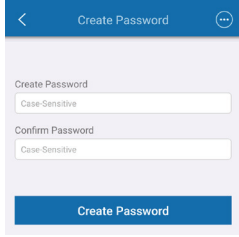
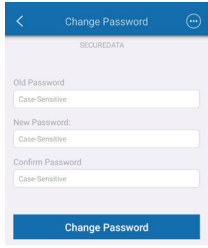
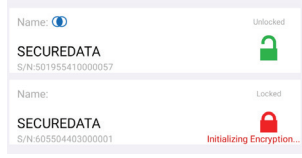
1. Press  . 
2. Enter User Password.
3. Press    .  , 
4. Enter 570.
5. Press .
6. If successful, you will see  ,  five times; if the command failed, you will see  ,  five times.

SECTION 5: COMMAND QUICK REFERENCE CHARTS

Please see the following tables for basic commands using the keypad and mobile app features. For keypad features, enter the values in its cell in order from top to bottom. In the adjacent cell to the right are corresponding LED displays on the drive.

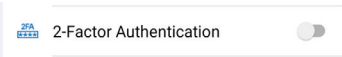
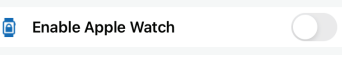
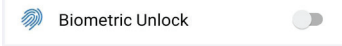
To access the part of the manual detailing the function, please click the hyperlink in the function cell.

Getting Started

Function	Keypad		User App
Create User Password	  enter new password then  re-enter password then 	   	
Change User Password	 Existing Password  New Password  Re-enter new Password 	   	
Unlock	 Enter Password 	 	

Basic Commands

NOTE: Unlock Drive with your password, then enter the command to enable or disable the feature. The Drive must be disconnected from your computer to enter password and commands.

Function	Keypad		User App
2-Factor Authentication	N/A	N/A	 
Apple Watch	N/A	N/A	 
Biometric Unlock	N/A	N/A	 

Function	Keypad		User App	
Bluetooth, Enable	 User password    281 	  ,   ,  5x	N/A	N/A
Bluetooth, Disable	 User Password    280 	  ,   ,  5x	N/A	N/A
Bluetooth Status	 User Password    728 	  ,   ,  5x	N/A	N/A
Cancel a Procedure	Press and hold 	None; returns to original status	N/A	N/A
Change Drive Name	N/A	N/A	Change Name SECUREDATA	
Inactivity AutoLock, Enable	 User Password    85 (for T, L)  Enter time (01–60) 	  ,    , 		 Inactivity AutoLock 5 Minutes
Inactivity AutoLock, Disable	 User Password    85 (for T, L)  00 	  ,    , 		 Inactivity AutoLock Never
Key Press Indication ON	 User Password    571 	  ,   ,  5x	N/A	N/A

Function	Keypad		User App	
Key Press Indication OFF	 User Password  570 	  ,   ,  5x	N/A	N/A
No Lock on Host Restart ON	 User Password  561 	  ,   ,  5x		 No Lock On Host Restart ☒
No Lock on Host Restart OFF	 User Password  560 	  ,   ,  5x		 No Lock On Host Restart ☐
Password Recovery	N/A	N/A		 Password Recovery ☒
Read Only	 User Password  76 (for R,O) 	  ,   ,  5x		 Read Only ☒
Read/Write	 User Password  79 (for R, W) 	  ,   ,  5x		 Read Only ☐
Remember Password	N/A	N/A		 Remember Password ☒
Remote Wipe	N/A	N/A		 Remote Wipe ☒
Resetting/ Deleting the Drive	Press and hold 7 and  999 Press and hold 7 and 	 ,  alternating 		 Reset Drive
Step-Away	N/A	N/A		 Step-away AutoLock ☒

Function	Keypad		User App	
Version	 User Password  86 	 for major version  for minor version	N/A	Firmware version :2.12