ioSafe Solo G3 Waterproof External HDD Secure Storage User Guide

ioSafe®

ioSafe Solo G3 Secure
Quick Start Guide

Contents

Solo G3 Waterproof External HDD Secure Storage

A8-7140-00 Rev 1.0

Product Warranty: CDSG warrants this product to be free of significant defects in material and workmanship for a period of two (2) years from the original date of purchase. CDSG's warranty is nontransferable and is limited to the original purchaser.

Limitation of Liability: The warranties set forth in this agreement replace all other warranties. CDSG expressly disclaims all other warranties, including but not limited to, the implied warranties of merchantability and fitness for a particular purpose and non-infringement of third-party rights with respect to the documentation and hardware. No CDSG dealer, agent, or employee is authorized to make any modification, extension, or addition to this warranty. In no event will CDSG or its suppliers be liable for any costs of procurement of substitute products or services, lost profits, loss of information or data, computer malfunction, or any other special, indirect, consequential, or incidental damages arising in any way out of the sale of, use of, or inability to use any CDSG product or service, even if CDSG has been advised of the possibility of such damages. In no case shall CDSG's liability exceed the actual money paid for the products at issue. CDSG reserves the right to make modifications and additions to this product without notice or taking on additional liability.

FCC Compliance Statement: 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 operation.

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 instruction manual, may cause harmful interference to radio communications.
In the event that you experience Radio Frequency Interference, you should take the following steps to resolve the problem:

1. Ensure that the case of your attached drive is grounded.
2. Use a data cable with RFI reducing ferries on each end.

3. Use a power supply with an RFI reducing ferrite approximately 5 inches from the DC plug.
4. Reorient or relocate the receiving antenna.

INTRODUCTION

This User Manual shows you how to set up and maintain the ioSafe Solo G3 Secure, an app-controlled, hardware encrypted, fireproof and waterproof external storage device, powered by SecureData.
The SecureData User app on your Apple or Android device unlocks the G3 Secure using Bluetooth wireless user authentication, which makes it available for reading and writing until you disconnect the drive or lock it again using the app.
That means that if your G3 Secure is stolen, the data on it is protected by military grade AES-XTS 256-bit hardware encryption and can’t be accessed without entering the password into the SecureData User app.
The G3 Secure also protects your data while fully submersed underwater for up to 72 hours and in temperatures up to 1550° F for 30 minutes, ensuring that your data stays protected through floods and fires.

GENERAL INFORMATION

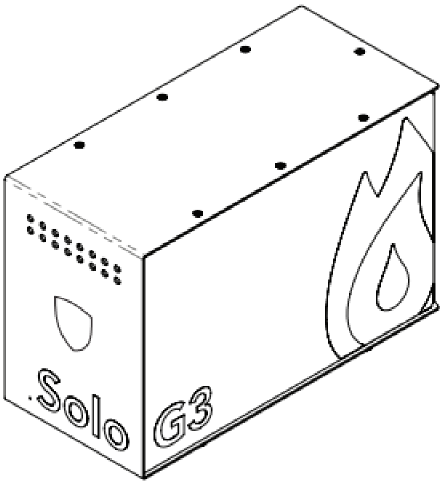
2.1. SAFETY INFORMATION

Please read the following before handling this product.

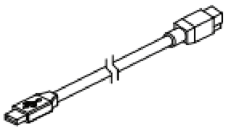
1. Do not drop the product, submit it to impact, or pierce it.
2. Avoid placing this product close to magnetic devices, high voltage devices, or in an area exposed to heat, flame, direct sunlight, dampness, moisture, rain, vibration, shock, dust, or sand.
3. To avoid overheating, this product should be operated in a well-ventilated area.
4. A damaged cable or device may malfunction and/or overheat and become a fire hazard.
5. Use only with high quality, undamaged cables and prevent cables from being pinched or damaged. The cable supplied with your system has been optimized for performance. Longer cables may not work or only work intermittently.

2.2. PACKAGE CONTENTS

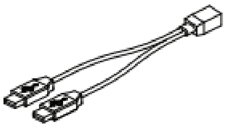
Check the package contents to verify that you have received the items below. Please contact ioSafe if any items are missing or damaged (see Contact ioSafe Support).



G3 Secure	Qty. 1



USB 3 Type A to Type B Cable	Qty. 1



USB 3 Y Cable (for boosting bus power)	Qty. 1

2.3. APP ICON INTERPRETATIONS

App Icon	Meaning
🔒	G3 Secure is locked
🔓	G3 Secure is unlocked
🔒	G3 Secure is blank (for example, it may not be formatted)
⚭	G3 Secure is connected to the app via Bluetooth and authenticated. If you don’t see this icon, the drive is connected but not authenticated, which means that if the drive is unlocked you can access your files but cannot access the Settings Menu or swipe right to lock.
2FA ••••	Two-factor authentication
↶ ••••	Change the password
	Touch ID
☺	Face ID
✓ ••••	App will remember the password
🕒	Inactivity auto-lock
|↔|	Step-away auto-lock
✗	Read-only mode
⌚	Enable Apple Watch
↺	Erase all data and settings
•••• ↻	Password recovery
	Remote wipe

INSTALLING THE SECUREDATA LOCK APP

The “SecureData Lock User” app must be installed on your iOS or Android device to connect to your new ioSafe Solo G3 Secure and control all of its functions.
Only one copy of the app is required to control multiple G3 Secures.
Download the 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 other app. Just scan the appropriate QR code below with your camera.

Download on the App Store	GET IT ON Google Play
https://apps.apple.com/us/app/securedata-lock/id1468147834	https://play.google.com/store/apps/details?id=com.securedatalock_bt&hl=en_US

PASSWORDS AND PROCEDURES

The ioSafe Solo G3 Secure is shipped with password 11223344. We strongly suggest changing the password for security.

⚠ **CAUTION**

Risk of loss of data. If you forget your password all data will be inaccessible and reformatting will be required. There is no backdoor.

4.1. PASSWORD REQUIREMENTS

Your password must:

- be 7-15 characters in length, letters or numbers. Special characters are okay.
- not contain only repetitive numbers or letters, e.g. (3333333) or (ccccccc)
- not contain only consecutive numbers or letters, e.g. (1234567), (7654321), (abcdefg)

4.2. PROCEDURAL CONVENTIONS

All actions require the ioSafe Solo G3 Secure to be connected to a computer with the USB cable. The procedures in this manual show what the app displays at some point during the procedure.

4.2.1. ADDING THE IOSAFE SOLO G3 SECURE TO THE APP (PAIRING)

The eight digit Device ID, which is located on the back of the G3 Secure, is required.

To add the drive, follow these steps:

Adding the G3 Secure	App Icon
1. Connect the G3 Secure to a computer with the USB cable.	–
2. Start the SecureData SD User App on your device. **Note:** Ensure your device is Bluetooth-enabled.	–
3. Tap ⊕ if you don’t see the G3 Secure in the list.	🔒
4. Tap the drive name that appears and follow the app instructions.	–
5. Tap Continue and follow the app instructions.	–

4.2.2. UNLOCKING THE IOSAFE SOLO G3 SECURE

⚠ **CAUTION**

After ten failed attempts to unlock the G3 Secure, the password and all data will be deleted. Refer to Section 6.2: Brute Force Hacking Detection, page 23. Until the G3 Secure is unlocked it will not appear on your computer.
To add the drive, follow the steps that apply to your situation below:

Unlock the Drive – When NOT Connected	App Icon
1. Connect the G3 Secure to a computer with the USB cable.	–
2. Start the SecureData SD User App on your device. Note: Ensure your device is Bluetooth-enabled.	–
3. Tap the drive name.	🔒
4. Type in the password and tap Unlock.	🔓

NOTE

The password on a new G3 Secure is 11223344. We strongly suggest changing the password after unlocking. If the G3 Secure still doesn't appear in your computer's file manager, see Section 8: Troubleshooting, page 30.

4.2.3. DISCONNECT THE IOSAFE SOLO G3 SECURE FROM THE COMPUTER

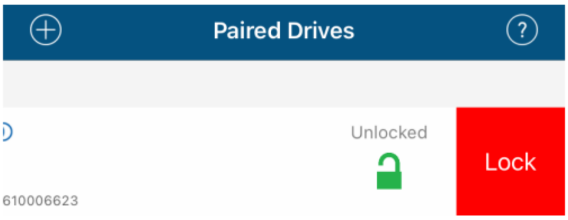
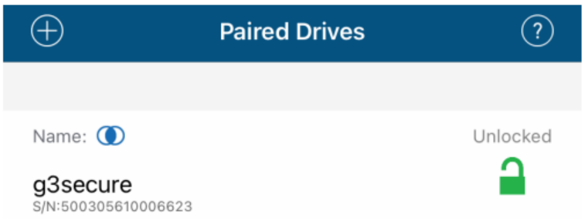
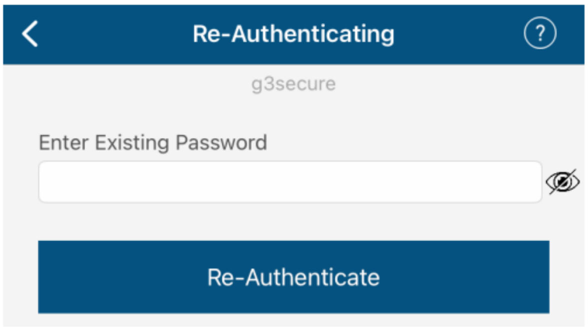
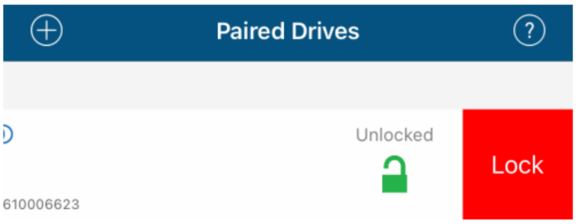
Generally, you can just unplug the USB cable.

NOTE

Some computer systems may require clicking the Safely Remove Hardware/Eject icon on your system prior to unplugging the cable from the computer. Wait for the red LED to come on indicating it is locked and ready to disconnect from the computer

4.2.4. LOCK WITHOUT UNPLUGGING FROM THE COMPUTER

The two methods shown below (A & B) allow for the two states the app could be in: Authenticated (logged in) or not.

A. Lock without Unplugging – App is connected to the ioSafe Solo G3 Secure and unlocked	**App**
1. In the app, swipe the desired drive name to the left. Note: If it does not swipe left, it needs to be authenticated. See B below.	
2. Tap Lock. The G3 Secure locks.	🔒
B. Lock without Unplugging – App is connected to G3 Secure but not authenticated. does not appear.	**App**
1. In the app, tap the desired Drive name. Note: If “Remember Password” is on, skip the next step.	 Paired Drives Name: Unlocked g3secure S/N:500305610006623
2. Type in the password and tap Re-Authenticate.	 Re-Authenticating g3secure Enter Existing Password Re-Authenticate
3. In the app, swipe the desired drive name to the left.	
4. Tap Lock. The G3 Secure locks.	🔒

ENTERING SETTINGS MODE

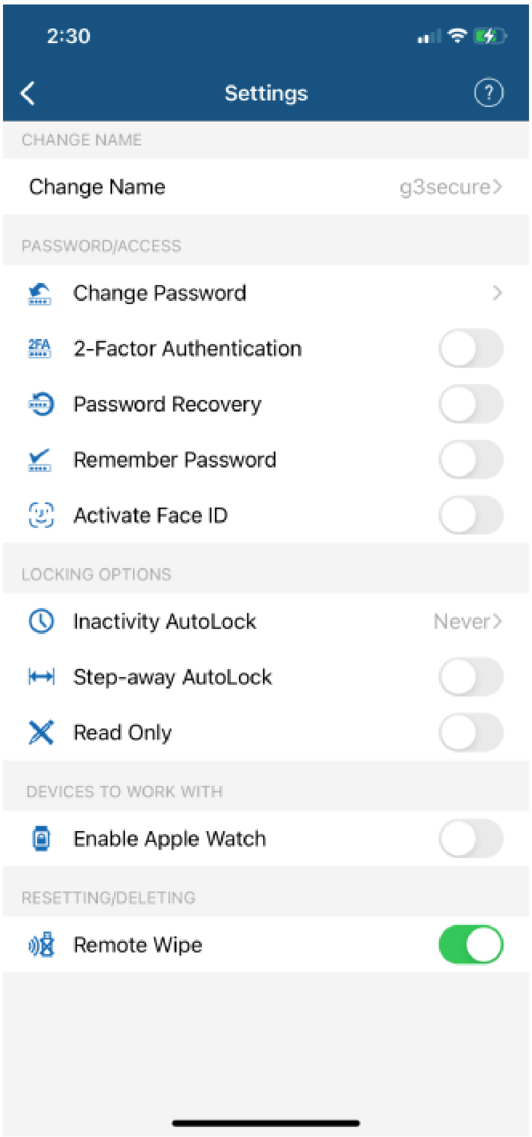
The Settings Mode allows functions such as enabling and disabling different settings available like the Read Only feature and an automatic Step-away AutoLock.
Access the Settings Mode by tapping the desired drive name anytime it’s unlocked and authenticated.

The image is an example of settings that may appear. Depending on the type of biometric settings available on the phone, these settings may vary.
The below sub-sections describe how to utilize these settings. If you have any questions, contact Technical Support.

NOTE

All actions require the ioSafe Solo G3 Secure to be connected to a computer with the USB cable.

Unless otherwise noted, procedures listed below assume the G3 Secure has already been unlocked and authenticated .



2:30

Settings

CHANGE NAME

Change Name g3secure

PASSWORD/ACCESS

Change Password

2-Factor Authentication ○

Password Recovery ○

Remember Password ○

Activate Face ID ○

LOCKING OPTIONS

Inactivity AutoLock Never

Step-away AutoLock ○

Read Only ○

DEVICES TO WORK WITH

Enable Apple Watch ○

RESETTING/DELETING

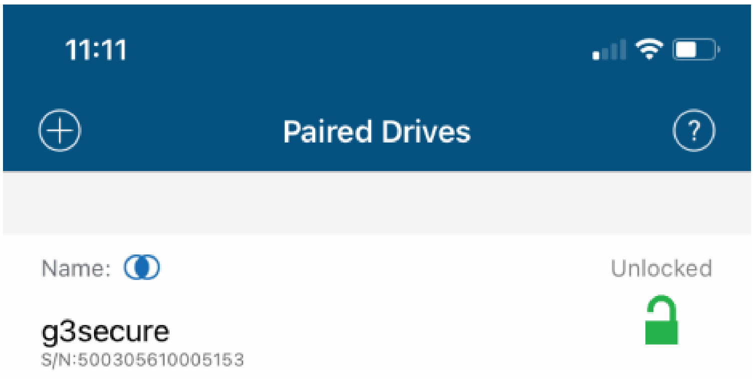
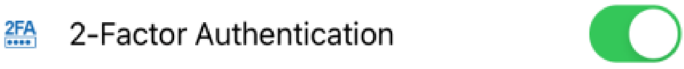
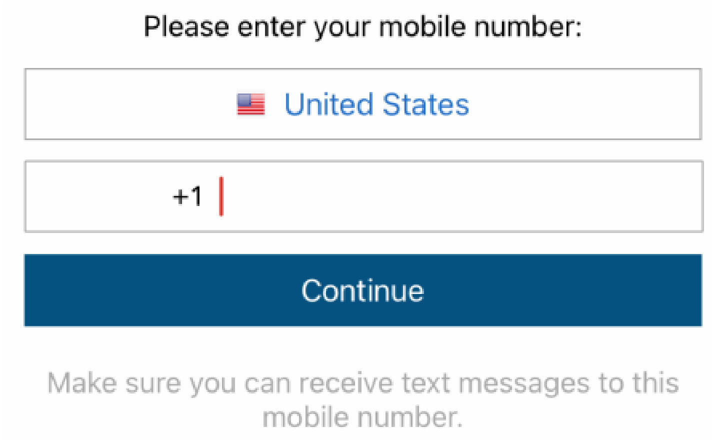
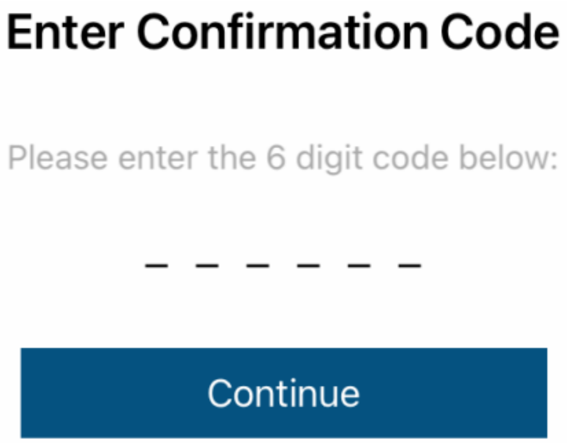
Remote Wipe ●

This is an example of settings that may appear. Depending on the type of biometric settings available on the phone, these settings may vary.

5.1. PASSWORD OPTIONS

5.1.1. ENABLING 2-FACTOR AUTHENTICATION

The 2-Factor Authentication feature will send a confirmation code to your registered mobile number as a text message and then prompt you for the password before granting access to the ioSafe Solo G3 Secure.

Enabling 2-Factor Authentication	App
1. Make sure the ioSafe Solo G3 Secure is unlocked and authorized (logged in) via the SecureData SD User app.	 11:11 Paired Drives Name: Unlocked g3secure S/N:500305610005153
2. Tap the drive name to access Settings.	–
3. Tap the 2-Factor Authentication button (green is ON).	 2FA 2-Factor Authentication
4. Read the “2-Factor Authentication” message and tap Continue.	–
5. Enter your mobile phone number.	 Please enter your mobile number: United States +1 Continue Make sure you can receive text messages to this mobile number.
6. Tap Continue.	–
7. Confirm your mobile phone number.	–
8. Wait for a text message and enter the confirmation code received. (The image to the right is an example only.) Click Continue.	 Enter Confirmation Code Please enter the 6 digit code below: _ _ _ _ _ _ Continue

You should get a confirmation message that 2-Factor Authentication is activated.

5.1.2. CHANGING THE PASSWORD

With your ioSafe Solo G3 Secure connected to a computer, follow these steps to change an existing password.

Change the Password	App
1. With the G3 Secure unlocked, tap the desired drive name.	–
2. Tap Change Password and enter your current password.	Refer to Settings image above.
3. Enter your old password, then new password and retype it into the Confirm field.	–
4. Tap Change Password.	🔓

NOTE

If a mistake was made while defining a new password or the procedure was not completed, the G3 Secure will retain the old password.

5.1.3. ENABLING REMEMBER PASSWORD

To avoid entering your password every time, you can have the password field auto-fill.

⚠ **CAUTION**

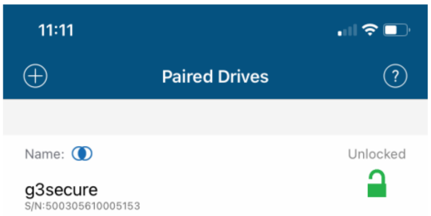
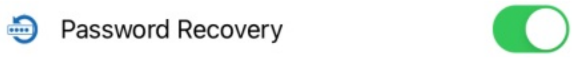
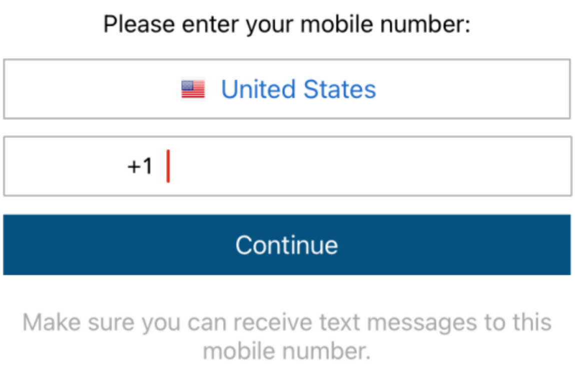
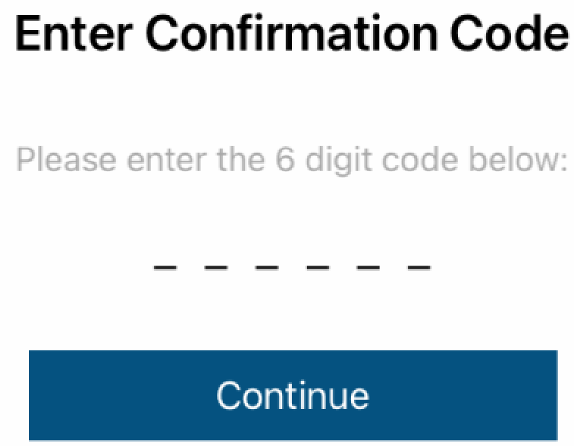
Security risk. The application will not require a password to unlock your ioSafe Solo G3 Secure. With this setting we strongly suggest that you enable a passcode on your iOS/Android device. Also, if the Step-away AutoLock feature is on, the G3 Secure will authenticate and unlock automatically as soon as the app is opened and within Bluetooth range.

Remember Password	App
1. With the G3 Secure unlocked and authenticated (logged in), tap t he desired drive name.	🔓
2. Tap the Remember Password button to the ON position (green).	Remember Password
3. Tap Yes to confirm.	🔓

5.1.4. ENABLING THE PASSWORD RECOVERY FEATURE

The Password Recovery feature will send a recovery code to your registered mobile number as a text message. There are two places where you can enable the Password Recovery:

- After creating password
- From the Settings menu

Enabling Password Recovery	App
1. Make sure the ioSafe Solo G3 Secure is unlocked and authorized (logged in) via the SecureData SD User app.	 11:11 Paired Drives Name: g3secure S/N:500305610005153 Unlocked
2. Tap the drive name to access Settings.	–
3. Tap the Password Recovery button (green is ON).	 Password Recovery
4. Read the Password Recovery message and tap Continue.	–
5. Enter your mobile phone number.	 Please enter your mobile number: United States +1 Continue Make sure you can receive text messages to this mobile number.
6. Tap Continue.	–
7. Confirm your mobile phone number.	–
8. Wait for a text message and enter the confirmation code received. (The image to the right is an example only.) Click Continue.	 Enter Confirmation Code Please enter the 6 digit code below: _ _ _ _ _ _ Continue

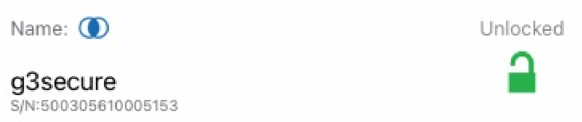
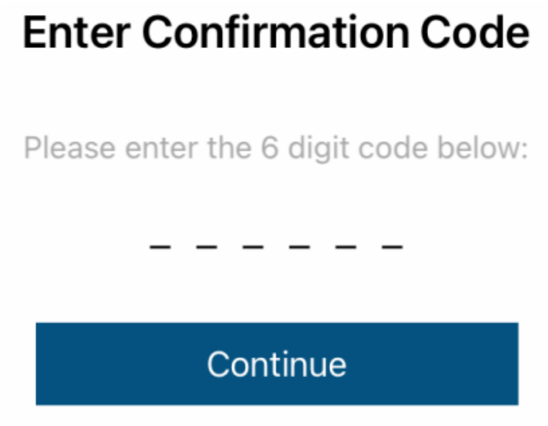
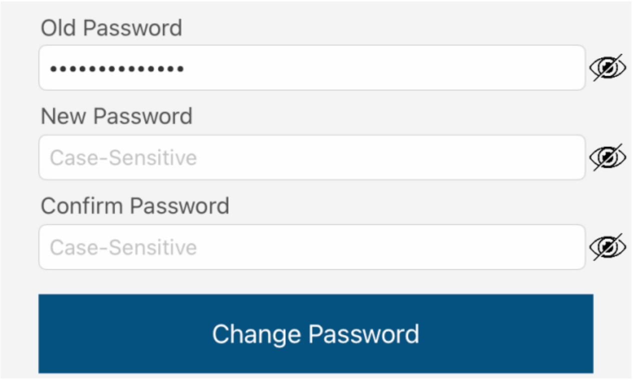
You should get a confirmation that Password Recovery is activated. To recover your password, see the next section.

5.1.5. RECOVERING A FORGOTTEN PASSWORD

Part A: If you have previously enabled the Password Recovery feature, follow these steps, otherwise skip down to part B.

NOTE

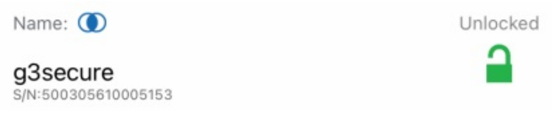
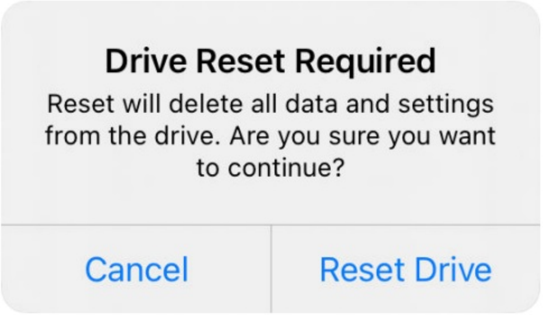
To receive password recovery code by text message you must be able to receive text messages to the phone number from where Password Recovery was enabled.

Part A: Recovering Forgotten Password	App
1. Tap the drive name.	 Name: g3secure S/N:500305610005153 Unlocked
2. Tap Forgot Password.	–
3. Tap Yes on the “Forgot Your Password” dialog.	–
4. Wait for the text message and then enter received confirmation code. (Example code used in image.	 Enter Confirmation Code Please enter the 6 digit code below: _ _ _ _ _ _
5. If entered correctly, you will see a “Change Password” dialog. Create a new password. Once complete, your ioSafe Solo G3 Secure should be unlocked.	 Old Password •••••••••••••• New Password Case-Sensitive Confirm Password Case-Sensitive

Part B: If you previously did not enable Password Recovery and forgot your password, resetting the G3 Secure is the only way to make it usable again. Although your data will be erased, this ensures that it is not breached or compromised. The G3 Secure Device ID is printed on the rear of the chassis to allow the unit to be reset. You will also need the Serial Number of the G3 Secure, which is displayed in the app below the drive’s name.

CAUTION

Data will be deleted. After performing a DRIVE RESET, it reverts to the default state:
unformatted AND ALL USER DATA AND SETTINGS WILL BE DELETED. Also, all settings (such as drive name, password, step-away, inactivity timer) will be set to default values.
Make sure the G3 Secure is authorized (logged-in) via the app.

Part B: Resetting the G3 Secure	App
1. Tap the drive name to open the “Drive Unlock” screen.	 Name: g3secure S/N:500305610005153 Unlocked 🔓
2. Tap Reset Drive.	–
3. Read the warning and tap Reset.	 Drive Reset Required Reset will delete all data and settings from the drive. Are you sure you want to continue? Cancel Reset Drive

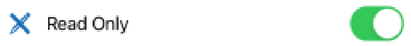
The G3 Secure reverts back to the default state. The default state is blank (has no password) and locked.

5.2. ACCESS OPTIONS AND LOCKING OPTIONS

Below are the three features for locking or restricting usage (and undoing them).

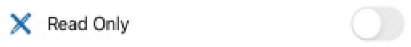
5.2.1. ENABLING READ-ONLY

With your ioSafe Solo G3 Secure connected to a computer, follow these steps to change an existing password.

Enable Read-Only	App
1. With the ioSafe Solo G3 Secure unlocked and authenticated, tap the desired drive name.	🔓
2. Tap the “Read Only” button to the ON position (green).	 Read Only
3. A “Read Only” dialog box will appear. Tap Lock. The G3 Secure will b e in Read-Only Mode when unlocked.	🔒

5.2.2. ENABLING READ/WRITE

Read-Only can be turned off restoring read and write access.

Enable Read/Write	App
1. With the ioSafe Solo G3 Secure unlocked and authenticated, t ap the desired drive name.	🔓
2. Tap the “Read Only” button to the OFF position (not green).	 Read Only
3. Tap Lock Now to confirm disabling Read-Only. The ioSafe Solo G3 Secure will be in Read/Write mode when unlocked.	🔒

5.2.3. SETTING THE INACTIVITY LOCK

To protect against unauthorized access when the ioSafe Solo G3 Secure is connected to a host computer and unattended, the G3 Secure can be set to automatically lock after a pre-set amount of time.

The default state of the Inactivity Lock is OFF. This feature can be set to activate (lock) at predefined times between 1 and 60 minutes.

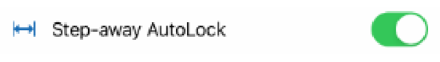
Enable Inactivity Lock	App
1. With the ioSafe Solo G3 Secure unlocked and authenticated, tap the desired drive name.	🔓
2. Tap Inactivity Lock.	–
3. Tap the desired inactivity interval after which time the G3 Secure will automatically lock.	A checkmark displays

5.2.4. DISABLING THE INACTIVITY LOCK

Disable the Inactivity Lock	App
1. With the ioSafe Solo G3 Secure unlocked and authenticated, tap the desired drive name.	🔓
2. Tap Inactivity Lock.	–
3. Tap Never. The Inactivity Lock is now disabled.	A checkmark displays

5.2.5. SETTING THE STEP-AWAY AUTOLOCK ON AND OFF

The Step-away AutoLock will lock the ioSafe Solo G3 Secure (disappear from the File Explorer/Finder) when the iOS/Android device is moved about 3m away from the Drive for longer than 5 seconds. When returned to the vicinity of the G3 Secure, the G3 Secure will automatically unlock when the Remember Password option is ON.

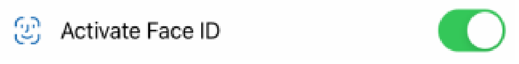
Enable Inactivity Lock	App
1. With the ioSafe Solo G3 Secure unlocked and authenticated, tap the desired drive name.	🔓
	 Step-away AutoLock ●
3. Tap Yes to confirm. The Step-away AutoLock is now on.	–

NOTE

To disable the Step-away AutoLock, tap the Step-away AutoLock button OFF (grey).

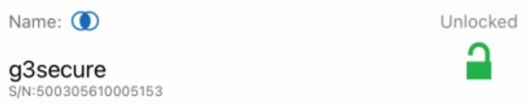
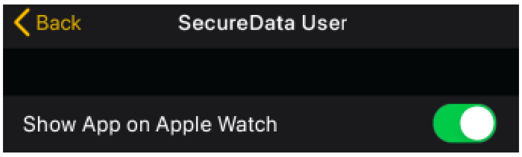
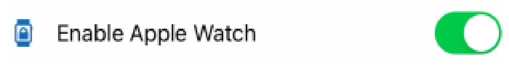
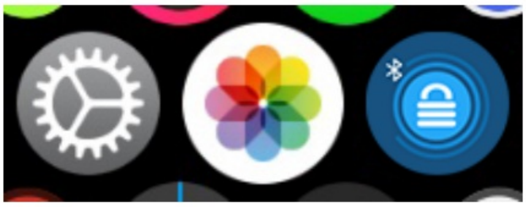
5.2.6. ENABLING BIOMETRIC AUTHENTICATION (TOUCH ID, FACE ID, FACIAL RECOGNITION)

Requirement: Android/iOS. Depending on the available biometric authentication on the device, options for the biometric features may vary. The following are generalized steps for how to enable the feature used by your phone:

Enable Biometric Authentication	App
1. Make sure the ioSafe Solo G3 Secure is unlocked and authorized (logged in) via the app.	 Name: g3secure S/N:500305610005153 Unlocked 🔓
2. Tap the drive name to access Settings.	–
3. Tap the button for your preferred biometric setting (green is ON). Example: Tap Activate Face ID.	 Activate Face ID ●

5.2.7. UNLOCKING THE DRIVE WITH AN APPLE WATCH

You can unlock your ioSafe Solo G3 Secure with an Apple Watch® if used with iPhone 5S or newer.

Unlock the G3 Secure with an Apple Watch	App
1. Make sure the ioSafe Solo G3 Secure is unlocked and authorized (logged in) via the app.	 Name: g3secure S/N:500305610005153 Unlocked
2. Tap the drive name to access Settings.	–
3. Make sure the SecureData SD User app is installed on your Apple Watch.	 Back SecureData User Show App on Apple Watch
4. Turn ON Enable Apple Watch.	 Enable Apple Watch
5. Start SecureData SD User app on your Apple Watch.	

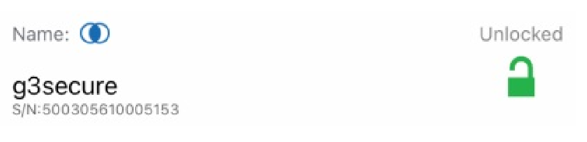
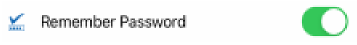
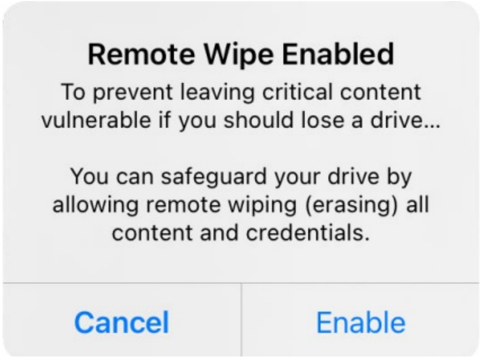
NOTE

Your G3 Secure’s password must contain numbers only to unlock with Apple Watch. If your current password contains letters then you will be redirected to the “Change Password” dialog.

You should be able to lock and unlock your Drive from your Apple Watch.

5.2.8. ENABLING REMOTE WIPE

To enhance protection for your ioSafe Solo G3 Secure in case it becomes stolen or lost, you can enable the Remote Wipe feature that will allow you to Remote Wipe (Reset) the unit.

Enable Remote Wipe	App
1. Make sure the ioSafe Solo G3 Secure is unlocked and authorized (logged in) via the app.	 Name: g3secure S/N:500305610005153 Unlocked
2. Tap the drive name to access Settings.	–
3. Tap the Remote Wipe button to ON (green).	 Remember Password
4. Tap Enable on the Remote Wipe dialog. You should see a confirmation that Remote Wipe is enabled.	 **Remote Wipe Enabled** To prevent leaving critical content vulnerable if you should lose a drive... You can safeguard your drive by allowing remote wiping (erasing) all content and credentials. Cancel Enable

NOTE

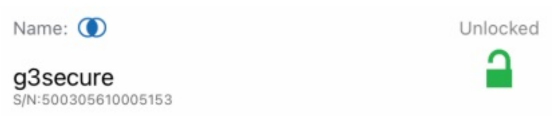
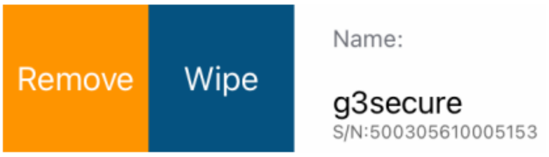
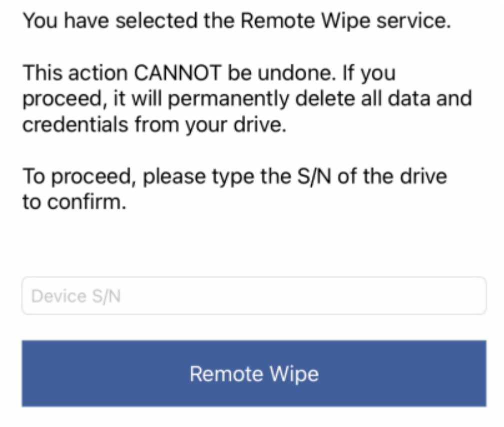
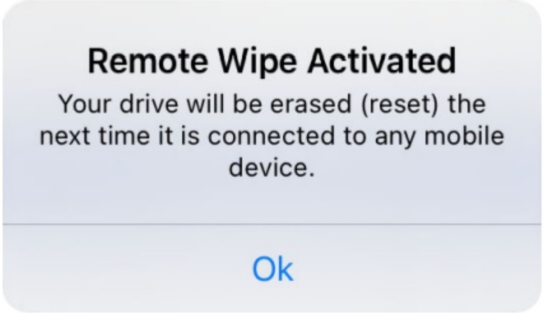
The Remote Wipe feature is only enabled, it is not activated. To activate it and remotely wipe your drive, see the next section.

5.2.9. ACTIVATING REMOTE WIPE IF YOU LOST YOUR DRIVE

The Remote Wipe option must have been enabled prior to losing the ioSafe Solo G3 Secure (see Section 5.2.8: Enabling Remote Wipe, page 20) If it has not been enabled, rest assured that your data on the G3 Secure cannot be accessed by whomever finds it. Follow this procedure to remotely wipe your G3 Secure:

⚠ **CAUTION**

Possible inadvertent loss of data. Once activated, there is no way to disable it. The next time the G3 Secure is discovered by the SecureData SD User app, it will be immediately wiped (reset) even if it is you who finds and attempts to use it. Please be sure you are ready to commit.

Activate Remote Wipe	App
1. In the app, copy the G3 Secure’s Serial Number which is displayed below the drive name.	 Name: Unlocked g3secure S/N:500305610005153
2. Swipe the drive name to the right and tap Wipe.	 Remove Wipe Name: g3secure S/N:500305610005153
3. As a validation, you must enter your G3 Secure’s Serial Number and tap Remote Wipe.	 You have selected the Remote Wipe service. This action CANNOT be undone. If you proceed, it will permanently delete all data and credentials from your drive. To proceed, please type the S/N of the drive to confirm. Device S/N Remote Wipe
4. You should see a confirmation that Remote Wipe is activated. Tap OK.	 **Remote Wipe Activated** Your drive will be erased (reset) the next time it is connected to any mobile device. Ok

The next time the G3 Secure is discovered by any mobile device with the SecureData SD User app installed, it will be immediately wiped (reset).

MANAGING THE IOSAFE SOLO G3 SECURE

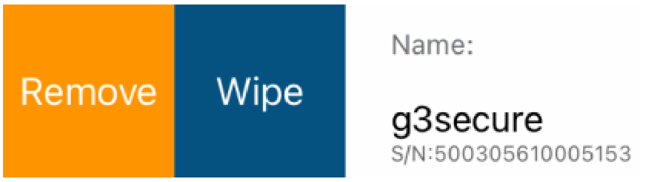
The following subsections discuss important, though less common, actions for managing your ioSafe Solo G3 Secure.

6.1. REMOVING A DRIVE

If you don’t want to use a previously paired ioSafe Solo G3 Secure with your smartphone app, you can remove it from the app. You can always add it back again by tapping the Home window. To add a Drive, see Section 4.2.1: Adding the ioSafe Solo G3 Secure to the App (Pairing), page 9.

⚠ **CAUTION**

Risk of unprotected data. Removing the G3 Secure from your device when it’s unlocked will leave the G3 Secure unlocked. Anyone will be able to access your data without a password until it is unplugged from the computer which will lock it.

Remove a Drive	App
1. With the G3 Secure locked or unlocked, touch the desired drive name and swipe right. (If unlocked, see the caution message above.	🔒 or 🔓
2. Tap Remove. If the G3 Secure does not have content on it, the 'Wipe' option will not be available.	 Name: g3secure S/N:500305610005153
3. Tap Remove to confirm.	🔒 or 🔓

6.2. BRUTE FORCE HACKING DETECTION

Entering an incorrect password ten consecutive times, the brute force hacking detection triggers and the password, all data, and format will be deleted. To re-use the ioSafe Solo G3 Secure , see Section 6.4: Creating a Password after a Reset (Blank Drive), page 24. The data is not recoverable.

6.3. RESETTING (DELETING) THE DRIVE

⚠ **CAUTION**

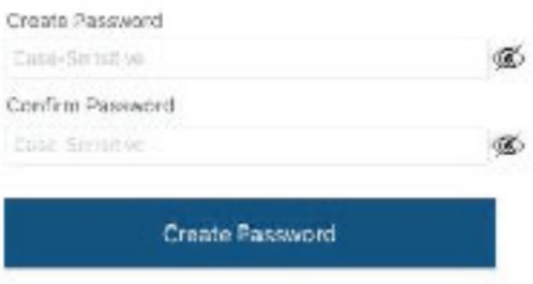
Resetting the ioSafe Solo G3 Secure will delete all data stored on it including password and formatting. After resetting it, the G3 Secure must be formatted. See Section 6.4:
Creating a Password after a Reset (Blank Drive), page 24.

If your password has been forgotten, or you want to delete all data stored on the G3 Secure including the password, you can perform the following Reset function. It also removes the encryption, requiring the G3 Secure to be reformatted to generate new encryption. To reformat the G3 Secure after resetting it, see
Section 7: Usage with Windows and Mac Operating Systems, page 26.

Reset the Drive	App
1. With the G3 Secure unlocked and authenticated (logged in) , tap the desired drive name.	🔓
2. Tap Reset Drive.	
3. Tap Reset to confirm.	–
4. Type in the Device ID (find it next to the USB port) and tap OK. All data is now removed from the G3 Secure.	🔒

6.4. CREATING A PASSWORD AFTER A RESET (BLANK DRIVE)

Perform this procedure after the ioSafe Solo G3 Secure has been reset. This password procedure is required to format the G3 Secure and must be performed after the app has been installed on your phone (or other device).

Create a Password	App
1. Connect the G3 Secure to a computer with a USB cable.	–
2. Open the app.	–
3. If the drive name doesn’t appear, tap (upper left) and then tap the drive name. Note: If the Drive is not blank you’ll see instead. If this happens, see Section 6.1: Removing a Drive, page 23.	🔒
4. Tap the drive name.	–
5. Type in password and confirm it.	 Create Password Case-Sensitive Confirm Password Case-Sensitive Create Password
6. Tap Create Password. To continue, your G3 Secure now requires formatting. See Section 7: Usage with Windows and Mac Operating Systems, page 26.	🔓

⚠ **CAUTION**

If a mistake was made while defining a new password or the procedure was not completed, you’ll find you won’t be able to use the G3 Secure until you create a password.

USAGE WITH WINDOWS AND MAC OPERATING SYSTEMS

7.1. USAGE WITH WINDOWS OPERATING SYSTEMS

7.1.1. ACCESS THE IOSAFE SOLO G3 SECURE

When the G3 Secure is properly connected and turned on, a window may open on your computer to allow you access it.

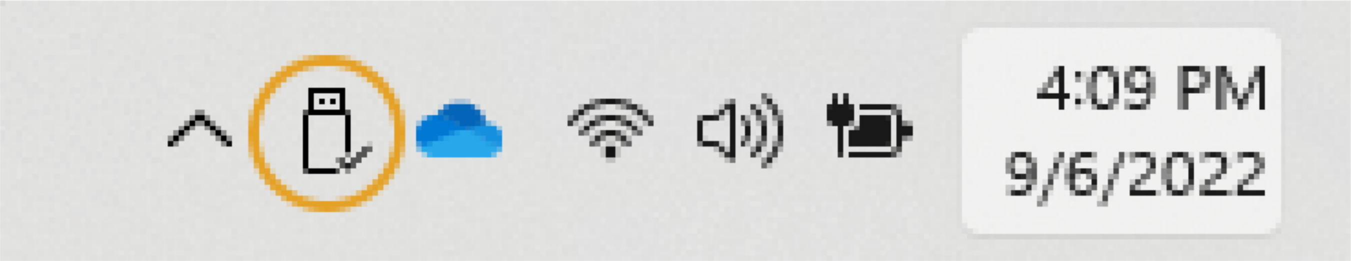
If no window appears, press Windows Key + E on your keyboard to open a File Explorer window. Then click on This PC in the File Explorer window’s navigation pane. Double-click on the icon representing the G3 Secure.

NOTE

If you can’t find the G3 Secure, then you may still need to format it. You will also need to format it if you wish to use the G3 Secure with both macOS and Windows computers. See Section 7.1.3: Format the ioSafe Solo G3 Secure, page 26 for directions.

7.1.2. DISCONNECT THE IOSAFE SOLO G3 SECURE

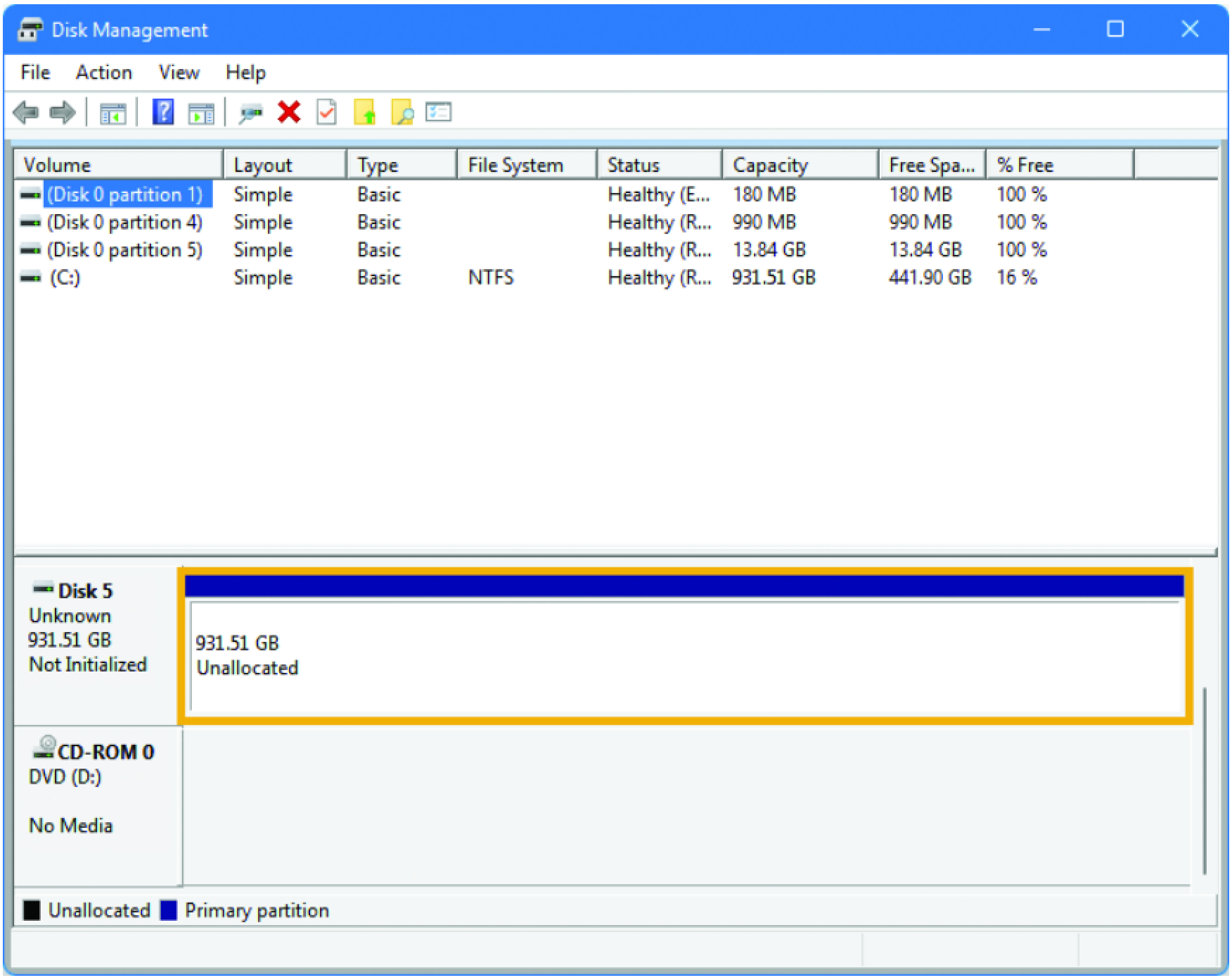
Left click the USB plug icon with the checkmark on the Desktop task bar (see the image below) and select the G3 Secure from the menu that pops up. You may have to click on the Show Hidden Icons arrow on the task bar to find the correct icon. Windows will indicate when it is safe to disconnect the G3 Secure and power it off.



7.1.3. FORMAT THE IOSAFE SOLO G3 SECURE

Follow the steps below for Windows 10 and 11 to format your G3 Secure.

1. Press WINKEY + X and then select Disk Management.
2. The drive should appear in the list of Disks in the lower pane. You may need to scroll down to see it. If the drive is already formatted, you can identify it easily by its volume name. If the drive is not initialized or is brand new, a window will pop up asking you to select a partition type. Select GPT and press OK.
3. To format the volume, right-click the Drive Properties Box of the drive (highlighted yellow in the figure below) and select New Simple Volume…



Volume	Layout	Type	File System	Status	Capacity	Free Spa...	% Free
(Disk 0 partition 1)	Simple	Basic		Healthy (E...	180 MB	180 MB	100 %
(Disk 0 partition 4)	Simple	Basic		Healthy (R...	990 MB	990 MB	100 %
(Disk 0 partition 5)	Simple	Basic		Healthy (R...	13.84 GB	13.84 GB	100 %
(C:)	Simple	Basic	NTFS	Healthy (R...	931.51 GB	441.90 GB	16 %

Disk 5
Unknown
931.51 GB
Not Initialized

931.51 GB
Unallocated

CD-ROM 0
DVD (D:)

No Media

■ Unallocated ■ Primary partition

The Disk Management pane with the Drive Properties Box highlighted in yellow.

4. Unless you wish to customize the settings in these dialog prompts, click Next on the Select Partition, Specify Volume/Partition Size, and Assign Drive Letter or Path dialog prompts, leaving the default settings.
5. Choose your preferred file system from the file system selection window that appears and enter a name for the new volume. Then check the box labeled Quick Format, which ensures that the formatting process will take less than a minute.

NOTE

If you want to use your G3 Secure with both macOS and Windows, choose the ExFAT file system.

6. Click Next and then Finish to start the format process. When the format is complete, the Drive Properties Box will update to show the new volume name.

   Once the G3 Secure is reformatted, a window may open on your computer to allow you access it.

   If no window appears, press Windows Key + E on your keyboard to open a File Explorer window. Then click on This PC in the File Explorer window's navigation pane.

7.2. USAGE WITH MACOS

7.2.1. ACCESS THE IOSAFE SOLO G3 SECURE

If the G3 Secure is already formatted, an icon representing it will appear on the desktop. Double-click on the icon to access it.

If it's unformatted, a message will appear on the desktop saying that the disk is unreadable. Use Disk Utility to easily format the drive (see Section 7.2.3: Format the ioSafe Solo G3 Secure, page 28).

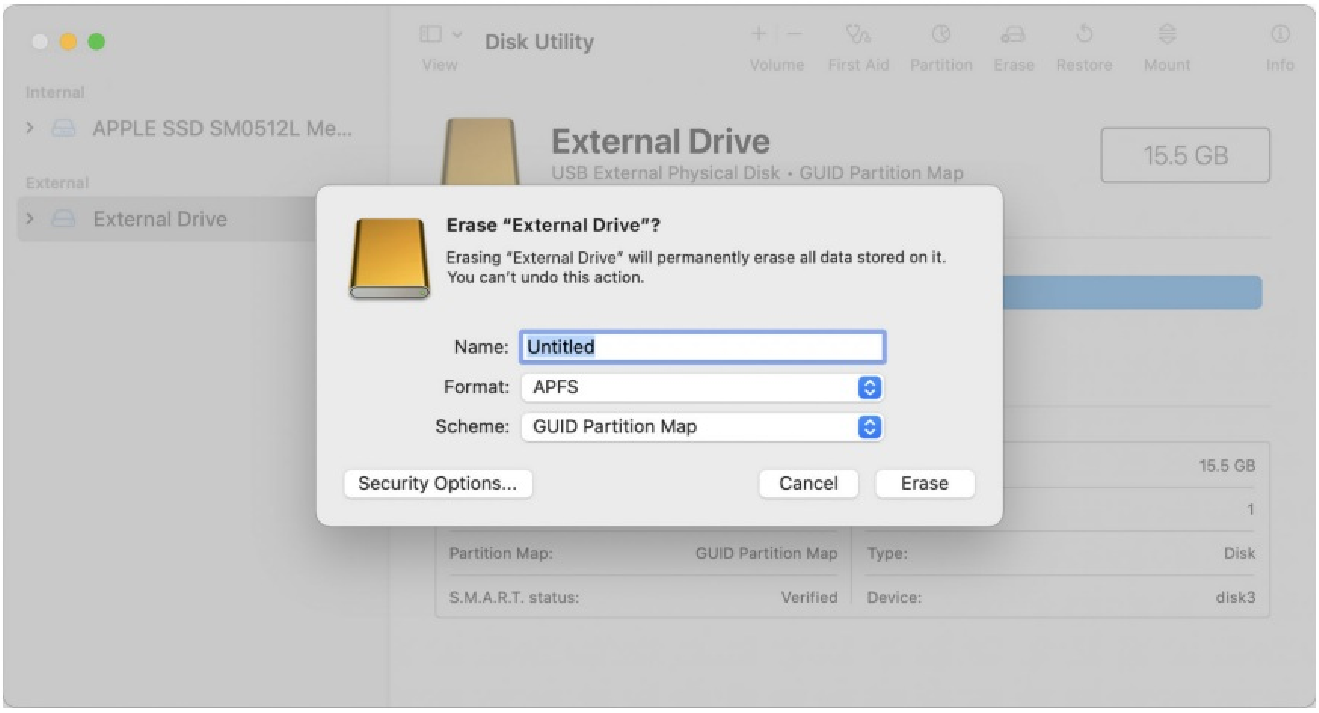
7.2.2. DISCONNECT THE IOSAFE SOLO G3 SECURE

1. Eject the G3 Secure before powering down the unit by dragging the G3 Secure's icon to the Trash, or by selecting the G3 Secure's icon and then pressing Command + E on your keyboard.
2. Power off the G3 Secure.

7.2.3. FORMAT THE IOSAFE SOLO G3 SECURE

Use Disk Utility to format the G3 Secure, which can be found in Applications → Utilities, or by selecting Spotlight Search (Command + Space) and typing in "Disk Utility" and then hitting Return on your keyboard.

1. Choose View → Show All Devices from the menu at the top of the Disk Utility window.
2. Click on the drive in the sidebar to the left.
3. Click on the Erase button at the top.
4. Enter a name for the new volume.



External Drive
USB External Physical Disk • GUID Partition Map
15.5 GB

Erase "External Drive"?
Erasing "External Drive" will permanently erase all data stored on it. You can't undo this action.

Name: Untitled
Format: APFS
Scheme: GUID Partition Map

15.5 GB
1
Partition Map: GUID Partition Map
Type: Disk
S.M.A.R.T. status: Verified
Device: disk3

macOS Disk Utility, showing the "Erase" submenu

5. Select the format type. Select APFS if you are using SSDs. If you are using hard drives, choose OS X

Extended (Journaled). If you need to use your G3 Secure with both macOS and Windows computers, choose ExFAT instead.

6. For the scheme, select GUID Partition Map.
7. (Optional) If available, click Security Options. Use the slider to choose how many times to write over the erased data, then click OK.

   Secure erase options are available only for some types of storage devices. If the Security Options button is not available, Disk Utility cannot perform a secure erase on the storage device.
8. Click Erase to start the process.
9. Once the format is complete, click Done.
10. Once the G3 Secure is formatted, double-click on the icon representing the G3 Secure on the desktop to access it.

NOTE

With a solid-state drives (SSDs), secure erase options are not available in Disk Utility. For more security, consider turning on FileVault encryption when you start using your SSD drive.

TROUBLESHOOTING

8.1. I CAN'T ACCESS THE DRIVE DATA OR FIND THE DRIVE AFTER I UNLOCK IT.

The ioSafe Solo G3 Secure is not initialized and needs to be formatted—no data exists. It may have been reset. To format, see Section 7: Usage with Windows and Mac Operating Systems, page 26.

8.2. I CAN'T SWIPE RIGHT TO LOCK THE DRIVE IN THE SECUREDATA SD USER APP EVEN THOUGH THE DRIVE NAME AND UNLOCK ICON DISPLAY.

The G3 Secure is not authenticated (does not display). Simply tap the drive name, enter the password and tap Re-Authenticate.

8.3. TAPPING THE DRIVE NAME IN THE APP DOESN'T DO ANYTHING.

If you've used a different drive prior to the current one, that old one may still display in the app. With the G3 Secure plugged in, and with Bluetooth on your iOS/Android device turned on, tap the plus sign ( ) to add your current drive. You'll need the Device ID number, which is located on the back of the G3 Secure.

8.4. I TRIED TO REPROVISION MY G3 SECURE, BUT IT DOESN'T SEEM TO BE WORKING.

You may not have the latest version of the app or a new-enough version of your phone's operating system.

PRODUCT SUPPORT AND DATA RECOVERY SERVICE

Register your product to activate your Data Recovery Service protection plan by visiting **iosafe.com/activate**.
If the ioSafe Solo G3 Secure breaks during the warranty period, we will repair or replace it. If you face possible data loss, immediately call ioSafe Data Recovery Services. ioSafe can determine the best actions to take to protect your valuable information.

Free Customer and Technical Support

- Phone: 1-530-820-3090 Option 2
- Email: **customersupport@iosafe.com**

Data Recovery Services

- Phone: 1-530-820-3090 Option 3
- Email: **disastersupport@iosafe.com**

Documents / Resources

	ioSafe Solo G3 Waterproof External HDD Secure Storage [pdf] User Guide Solo G3, Solo G3 Waterproof External HDD Secure Storage, Waterproof External HDD Secure Storage, External HDD Secure Storage, HDD Secure Storage, Secure Storage

Manuals+,