ARMORLOCK™

ArmorLock™

Encrypted NVMe™ SSD with Mobile and Desktop Apps

User Manual

Accessing Online Support

For those that have previously purchased a G-Technology® ArmorLock™ NVMe SSD, model number 0G10484-1, please see the following link for your user manual with warranty information at https://support-en.g-technology.com/app/answers/detail/a_id/29803.

Visit our product support website and choose from these topics:

- **Downloads —** Download software and updates for your ArmorLock product
- **Warranty & Returns —** Check warranty, get product replacement (RMA)
- **Ask a Question —** Submit a query about a product or open a support case
- **ArmorLock Community —** Share your thoughts and connect with other ArmorLock users at our community

Table of Contents

1 Welcome to ArmorLock

We built the ArmorLock™ Encrypted NVMe™ SSD and app to deliver revolutionary data protection that's amazingly simple to use. It's next-generation security, with new-generation simplicity. Encryption is just the beginning.

Key Features

PASSWORDS ARE A THING OF THE PAST

Remembering passwords, entering codes and downloading software slows down access to critical content. We've removed access barriers without sacrificing content security. With ArmorLock™ technology, your phone is your key, leveraging your phone's user authentication to simply and quickly access your content with the tap of a button.

THE NEW AUTHORITY ON AUTHORIZATION

Collaboration is critical to your workflow. Multiple users and drives create security risks. The ArmorLock™ app provides easy, multi-user authorization and management features. Before you ship your precious content to your partner, authorize them to unlock the ArmorLock™ drive using your favorite email or messaging service.

ROBUST DRIVE MANAGEMENT

With the app, you can format your drive to one of the compatible file systems and when your content is no longer needed, use the secure erase feature to confidently erase the drive with the tap of a button. Can't remember where you last used your drive? The app will show you on a map.

HIGH-GRADE DATA SECURITY

Built with always on, high-grade 256-bit AES-XTS hardware encryption for powerful data protection without compromising on speed. The ArmorLock encrypted NVMe™ SSD comes completely locked out of the box, shutting out access from the start. When a drive is unlocked you have fast access to stored content. Ejecting the drive automatically locks it - rendering all content inaccessible.

ADRENALINE FOR YOUR CONTENT

Transfer time is down time. With the ArmorLock encrypted NVMe™ SSD's heat-dispersing cool aluminum core, you get sustained pro-grade transfer speeds up to 1000MB/s read and 1000MB/s write.**

BUILT FOR RIGOR

Production trucks, DIT carts, Pelican cases, and backpacks. The ArmorLock encrypted NVMe™ SSD gives you pro-grade durability you can rely on. Hand it off and trust it's safe with our durable, easy-to-hold enclosure, up to 3-meter drop protection***, 1,000-pound crush resistance, and IP67 dust and water resistance.

ArmorLock App

Your key to revolutionary security, speed and convenience

We designed the ArmorLock mobile and desktop apps to make unlocking and managing your ArmorLock drive really simple. Instead of remembering passwords or using fingerprints, your phone or computer becomes the key to unlock your drive. The app is packed with features such as multi-drive and multi-user management, secure erase and self-formatting, and tracking your drive's last known location. We've made this technology so easy to use that if you can use your phone, you can use ArmorLock.

What's in the Box

- ArmorLock encrypted NVMe SSD
- USB-C™ to USB-C cable (supports SuperSpeed USB 10Gbps)
- USB-C to USB-A cable (supports SuperSpeed USB 10Gbps)
- Quick Start Guide
- Technical Support and Limited Warranty Guide

Tech Notes

Note: The ArmorLock Encrypted NVMe SSD drive is a direct attached storage unit that uses USB for storage access. This product is not a wireless Internet-enabled drive.

Drive Compatibility

The drive works with USB-C and USB-A 3.0 hosts, and is compatible with the following operating systems.

Table 1.1

Windows®	macOS
Windows 10+	macOS 10.14+

App Compatibility

The ArmorLock app is compatible with the following operating systems. The app is required to unlock and manage the drive.

Table 1.2

macOS	iOS
macOS 10.14+	iOS 13.2.+

When ArmorLock drives are accessed from a personal computer system via the desktop app, a 64-bit operating system is required. Compatibility can vary, depending on hardware configuration and operating system. For the newest features and compatibility options, always install the latest app updates.

USB Host and OS Compatibility

The following table lists the USB host and operating system combinations that can be used with ArmorLock.

Table 1.3

When plugged into USB host...	macOS	Windows
You can use the macOS app to...	Pair & Unlock	—
You can use the iPhone app to...	Pair & Unlock	Pair & Unlock

Bluetooth™ Compatibility

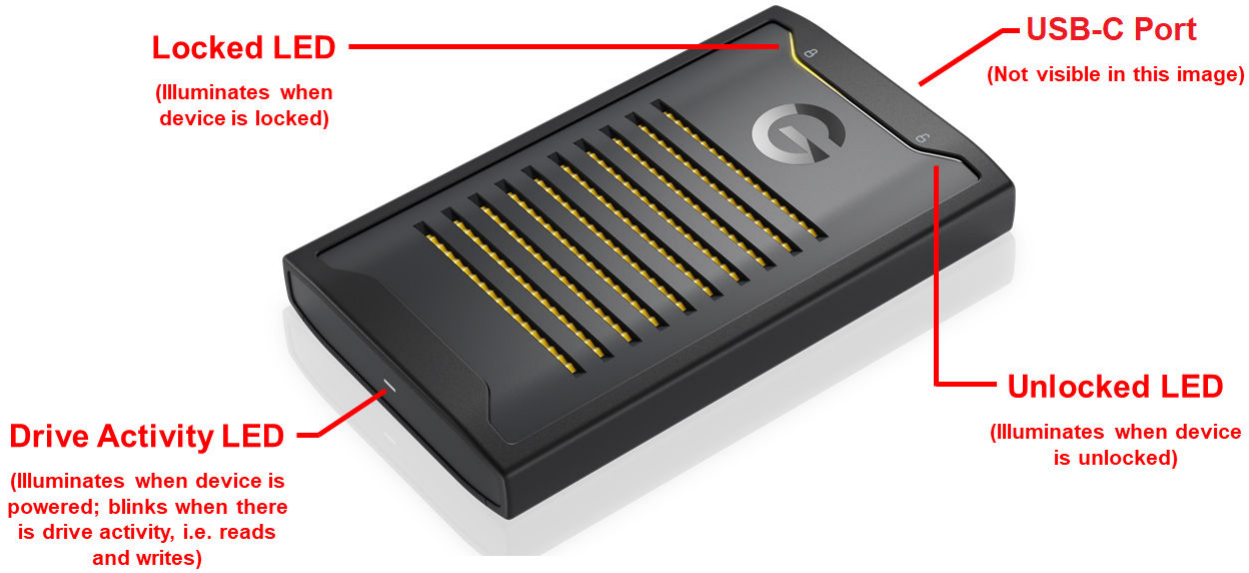
Your smartphone and ArmorLock SSD communicate via Bluetooth. The ArmorLock SSD is compatible with the Bluetooth Low Energy (BLE) wireless personal area network technology that is part of the Bluetooth 4.2 and later wireless technology standards. All of the operating systems included in the preceding list are compatible with Bluetooth Low Energy.

A Look at the ArmorLock Drive

The ArmorLock encrypted NVMe SSD contains a number of prominent features:

- A USB-C interface port
- Three (3) LEDs: locked, unlocked, and power/activity
- QR code and Short Code unique to each individual drive (located on the back of the drive). QR Code is to be used with a phone camera and the Short Code is to be used with computers for app-to-drive pairing.

The image below illustrates the location, color, and status of the LEDs, and the location of the USB-C port.



2 Getting Started

This chapter provides instructions for downloading the ArmorLock app, connecting to and setting up the ArmorLock encrypted NVMe SSD.

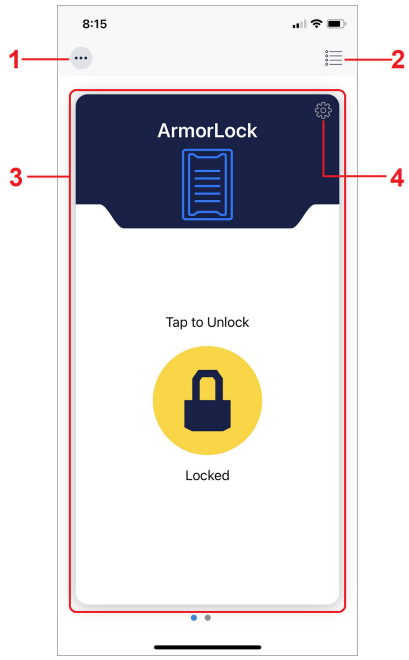
Get the Mobile App

Download and Setup the App

1. Download the ArmorLock app in one of the following ways:
   a. Use your phone's camera to scan the QR code located on the back of your drive
   b. Go to GetArmorLock.com/Apps
   c. Search for ArmorLock on the App Store
2. Launch the ArmorLock app.
3. Select **Continue**.

   Note: By selecting **Continue**, you are agreeing to the End User License Agreement and Privacy Statement.
4. The **Share Crash Reports**window will open. Select **Agree** if you want to share your crash report data. Otherwise, select **Decline**.
5. Swipe (or select **Next**) through the ArmorLock intro pages, then select **Done**.
6. Enter your **User Name** for the phone, then select **Save**.
7. The app will then request permission to send notifications, select **Allow**. Select **Allow** again to proceed.
   a. **Note:** Notifications are important and will help guide you when new actions are required, such as authorizing new requests to access your drive.
8. If Global Location Services are off, a popup will tell you to turn it on.
   a. Go to your phone's settings and turn on Global Location Services.
9. If Location Services are off, a popup will tell you to turn it on.
   a. Go to your phone's settings and turn on Global Location Services.
10. A series of tooltips will appear. Select **Next** or **OK** to proceed.
11. ArmorLock is now ready to add a drive.
12. The Share Crash Reports will open. Select **Agree** if you want to share your crash report data. Otherwise, select **Decline**.

ArmorLock Mobile App Overview



1. **Main Menu:** The “three-dot” main menu allows you to:
   a. **Share User ID:** A new User requesting access to a drive can 1) send their phone’s User ID to a Manager with the drive in a different location, or 2) display their phone’s User ID QR Code to be scanned by a Manager in the same location.
   b. **Scan User ID:** A drive Manager can scan another phone’s User ID to add them into their User List. This is a good way to gather User IDs from your team to give them access to a drive.
   c. **Share App:** Share the ArmorLock app with other Users. This is especially important when you are authorizing remote users before you ship them a drive.
   d. Select **Add Drive** or **Remove Drives**.
   e. **App Settings**: Enable tooltips and the Auto Unlock feature.
   f. Get **Help** through the online user manual. You can also view the introduction screens and How-To videos, or go to the support web page.
   g. Open **About** screen.
2. **Toggle icon:** The toggle icon lets you switch between Card view and List view modes.
3. **Drive Card:** Once you’ve added a drive your screen shows the “Drive Card” for that drive. Swipe left to add a new drive, and when you have multiple drives added, you can swipe left or right to toggle between drives.
4. **Drive Card Gear Icon:** The gear icon is specific to each drive and allows you update and manage drive settings.

Add a New Drive with the Mobile App

This section takes you through the steps to add a new drive for the first time. You can also use these steps to add additional drives to manage with your ArmorLock app.

Setup and Use the Drive

1. Turn on your computer and log-in.
2. Connect the drive to your computer.
   a. **Note:** Connecting the ArmorLock drive to a USB hub is not recommended. If such a connection is used, a powered USB hub is recommended in order to supply the appropriate power to the drive.
3. The ArmorLock drive will power on and the LED light under the Lock Symbol will turn on.
4. Open the ArmorLock app and add a new drive.
   a. **Card View** (default view) – select the **Add Drive** icon.
   b. **List View** – select the **+ Add Drive** button.
   c. **Main Menu** - select the **3-dot** icon then select **Add Drive**.
5. A "Bluetooth Required" permission will popup, select **Allow**. Select **OK** to proceed.
   a. **Note**: ArmorLock uses Bluetooth to connect to drives and must be enabled.
6. If Bluetooth is off, a popup will tell you to turn Bluetooth on.
   a. Go to your phone's settings and turn on Bluetooth.
   b. Reopen ArmorLock and select **Add Drive**.
7. A "Camera Access Required" permission will popup, select **Allow**. Select **OK** to proceed.
   a. **Note:** Camera access must be allowed to scan QR codes with your phone.
   b. You may need to turn on the **flashlight** in low-light conditions in order to scan the QR code.
8. Locate the QR code on the back of the drive and scan it with your phone. Three options will appear:
   a. **Setup as New –** Takes you through the initial setup for a new drive (drive name, color, format, etc.).
   b. **Use Recovery Key –** Lets you enter your saved Recovery Key to restore access to your drive when all other methods are unavailable. Note: This will also remove all other users/managers from the drive.
   c. **Request Authorization–** Allows you to request access to a drive already managed by another device.
9. From the menu, select **Setup as New**. Then complete the **Setup** options for the drive.
   a. Enter the **name** for the drive (required). Only users designated as Manager can enter a drive name.
   b. Choose a **color identifier**. Only users designated as Manager can choose a color identifier.
   c. Select the **drive format**.
      - macOS (HFS+): Time Machine compatible
      - Windows (NTFS): Windows format
      - Windows and macOS (exFAT): For flexibility between both operating systems
   d. Select **drive's last known location** (optional).
      - Location tracking is off by default. Turn on to view the last known location where the drive was used and add a map location to each entry.
      - When turned on, a location permission popup will appear, select **Allow**. Additional location setting must be selected: Allow while using the app, allow once, or don't allow.
   e. **Advanced Settings**.

- **User Authentication**: Off by default. Enables user authentication (Passcode, Touch, or Face ID) for an additional layer of security to verify that the person using the app is the correct, authorized user.

- **Auto Firmware Updates**: On by default. We recommend leaving this on for future updates.

f. Select **Format Drive**.

- A final warning says that any existing drive content will be permanently erased.

g. Select **Erase**.

- The drive will begin secure erase. Do not disconnect the drive or leave the app.

10. Save the **Recovery Key**. The Recovery Key restores access to the drive when all other methods are unavailable, and all Authorized Users will be removed. Several options are available for saving.
    a. **Photos** – Requires giving ArmorLock access to the photos app.
    b. **Files** – Saves in your phone's file system as a PDF.
    c. **Print** – We strongly recommend printing and storing in a safe location.

    - Western Digital cannot restore your access if you lose your Recovery Key.

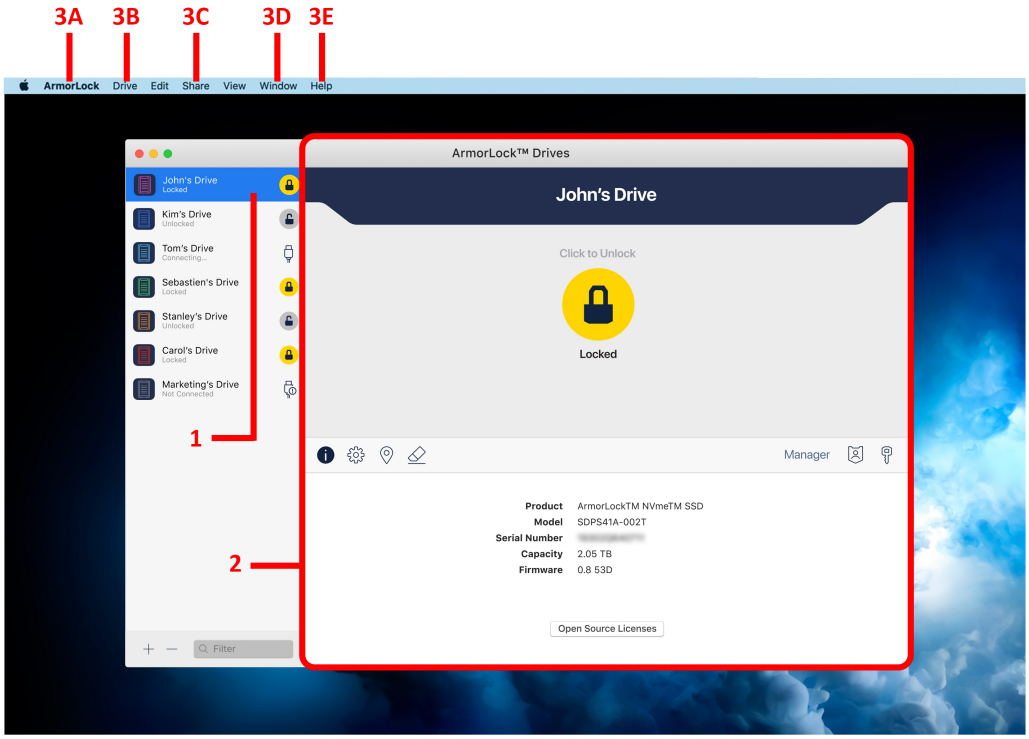
Get the Desktop App

The ArmorLock desktop app allows you to unlock and manage your drive using your computer. One main difference with using the ArmorLock app on a computer is the use of unique alphanumeric Short Codes instead of scanning QR codes like you do with your phone. Adding a drive requires entering its unique **Short Code** located next to the QR code.

Download and Setup the App

1. Download the ArmorLock app in one of the following ways:
    a. Go to GetArmorLock.com/Apps
    b. Search for ArmorLock on the App Store
2. Launch the ArmorLock app. Select **Continue**.
3. The **Share Crash Reports**window will open. Select **Agree** if you want to share your crash report data. Otherwise, select **Decline**.
4. Click through the ArmorLock intro pages, then click **Done**.
5. Enter your **User Name** for the computer, then click **Save**.
6. The app will then request permission to send notifications, click **Allow**. Click **Allow** again to proceed.
    a. **Note:** Notifications are important and will help guide you when new actions are required, such as authorizing new requests to access your drive.
7. ArmorLock is now ready to add a drive.
8. The **Share Crash Reports**window will open. Select **Agree** if you want to share your crash report data. Otherwise, select **Decline**.

ArmorLock Desktop App Overview



1. **List View:** When ArmorLock is open, the List View is where added drives are located.
   a. At the bottom left corner, the **+** and **– buttons** are for **adding** or **removing** drives.
   b. Multiple drives will also appear as a list in this pane.
2. **Drive Card view:** When you **click** on a drive, a lock icon and drive information will appear in the Drive Card view.
   a. **Lock icon** – click to unlock the drive.
   b. **Unlock icon** – click to lock and eject the drive.
   c. **i icon** – click to display (default view) the drive name, model, serial number, capacity, firmware, and open source licenses.
   d. **Gear icon** – click to edit the drive **settings**.
   e. **Map pin** – click to show the **last recorded location** of the drive.
   f. **Erase icon** – click to **securely erase** and **reformat** the drive.
   g. **(Manager role only) ID icon** – click to view the list of **authorized devices** and edit each **role**.
   h. **(Manager role only) Key icon** – click to generate a **new recovery key** and replace the existing one.
3. **Main Menu:** The main menu can be accessed at the top of the app window. The following are the main submenus and their primary selections (not exhaustive).
   a. **ArmorLock**

      - **About ArmorLock** – View the ArmorLock version and license agreement.

      - **Preferences** – Set the ArmorLock Username and select to automatically start ArmorLock at Login.

      - **Services** – Services Preferences for your operating system.

   b. **Drive**

- **Add Drive** – Add an ArmorLock drive to the app.
- **Remove Drive** – Remove an ArmorLock drive from the app.

c. **Share**

- **Share User ID** – Send your User ID to a Drive Manager to request access to an ArmorLock drive.
- **Share App** – Share the ArmorLock app with other Users.

d. **Window**

- **Devices** - Displays a list of authorized devices.
- **Authorized Users** - Displays a list of authorized users.

e. **Help**

- **User Manual** - View the online user manual.
- **View Introduction** - View the introductory app screens.
- **How To** - View How To videos.
- **Support** - Go to the Support web page.

Add a New Drive with the Desktop App

This section takes you through the steps to add a new drive for the first time. You can also use these steps to add additional drives to manage with your ArmorLock app.

Setup and Use the Drive

1. Turn on your computer and log-in.
2. Connect the drive to your computer.
   a. **Note:** Connecting the ArmorLock drive to a USB hub is not recommended. If such a connection is used, a powered USB hub is recommended in order to supply the appropriate power to the drive.
3. The ArmorLock drive will power on and the LED light under the Lock Symbol will turn on.
4. Inside the app, there are three ways to add a new drive.
   a. **List View** – click the **+ Add Drive** button. This option only displays if there are no drives present in the **List View** window.
   b. **Bottom** left corner – click **+** or **–** to add or remove drives.
   c. **Drive Menu** – click **Drive** and select **Add Drive**.
5. Click **Add Drive**.
6. A **Short Code** window will popup. Enter the drive's Short Code.
   a. The Short Code is an 8-digit code on the back of the drive, next to the QR code.
   b. After the last digit is entered, the app will automatically locate the drive.
7. Three options will popup.
   a. **Setup as New** – The initial setup (name, color, format, etc.) for a new drive.
   b. **Use Recovery Key** – Restores access to the drive when all other methods are unavailable. This will also **remove** all other users/managers from the drive.
   c. **Request Authorization** – Your User ID can be scanned by the drive Manager for access.
8. Click **Setup as New**. Then select the **Setup** options for the drive.
   a. Enter the **name** for the drive. Only users designated as Manager can enter a drive name.

b. Select the **drive format**.

- macOS (HFS+): Time Machine compatible
- Windows (NTFS): Windows format
- Windows and macOS (exFAT): For flexibility between both operating systems

c. Choose a **color identifier**. Only users designated as Manager can choose a color identifier.

d. Select **optional** settings.

- **Location tracking**: Off by default. Turn on to find the last known location where the drive was used and add a map location to each entry.
- **User Authentication**: Off by default. Enables user authentication (Password, TouchID) for an additional layer of authentication.
- **Auto Firmware Updates**: On by default. We recommend leaving this on for future updates.

e. Click **Format Drive**.

- The drive will begin formatting. Do not disconnect the drive or close the app.

9. Save the **Recovery Key**. The **Recovery Key** restores access to the drive when all other methods are unavailable. This will remove all authorized users from the drive. Several options are available for saving.

a. **Print** – We strongly recommend printing and storing in a safe location. Western Digital cannot restore your access if you lose your Recovery Key.

b. **Save as PDF** – Saves in your computer's file system as a PDF.

10. After saving, click **Done**. Then you will be asked to confirm that the Recovery Key is saved, click **Confirm**.

11. Your computer is now the drive **Manager** and ready to use.

3 Main Activities

Unlock and Lock the Drive

To lock the ArmorLock drive, you must eject it from your computer. Any ejected ArmorLock drive is securely locked and can only be unlocked with the ArmorLock app using an Authorized phone or computer. The following steps describe how to unlock and lock the drive.

1. Connect the ArmorLock drive to a host computer.
   a. This will provide the drive with power so that it can be securely connected to a phone or computer using the ArmorLock app.
2. Open the ArmorLock app on your phone or computer.
   a. The mobile app will locate all ArmorLock drives within **10 meters**.
3. The app will show the current condition of the ArmorLock drive as either **Locked** or **Unlocked** and display a status icon matching this condition.
4. To **Unlock** the drive, select the Lock status icon. Once unlocked, the status will change to an open lock icon.
   a. If **user authentication** is enabled, the drive can be unlocked using the user authentication features of your smartphone.
5. To **Lock** the drive, select the Unlock status icon.
   a. **Mobile app**: The following message will be displayed: "Use the computer to eject and lock the drive." We recommend using the computer to eject the drive to minimize risk of data loss or corruption.
   b. **Desktop app**: Use the ArmorLock app to lock the drive.
6. Once the drive is ejected successfully, the app will display the **Locked** status icon.

Auto Unlock

The Auto Unlock feature allows you to conveniently unlock your drive automatically when connected to an authorized phone or computer.

Known drives are automatically unlocked when they are connected. Drives with User Authentication enabled will not be automatically unlocked. The **Allow While Using App** location permission is required to use this feature.

Mobile App

1. Open the ArmorLock app.
2. Select the **3-dot** icon for the Main Menu.
3. Select **App Settings**.
4. Switch the **Auto Unlock** toggle to turn it on.

Desktop App

1. Open the ArmorLock app.
2. Access the **ArmorLock** main menu at the top of the window.
3. Select **Preferences**.
4. Select the **Automatically unlock known drives when they are connected** box.

Note: Drives with User Authentication enabled will not be automatically unlocked.

Remove a Drive

Use the following steps to disconnect or unpair an ArmorLock drive from the app.

Mobile App

1. Open the ArmorLock app.
2. Select the 3-dot icon for the Main Menu.
3. Select **Remove Drive**.
   a. This will open the Remove Device menu and list all connected ArmorLock drives.
4. Select the drive that you want to remove, then select **Remove**.
5. A popup screen will confirm the drive selected to be removed.
6. Select **Remove** to continue or select **cancel**.
7. You may be asked to enter the authentication (fingerprint, face ID, or passcode) for your mobile device.
8. The ArmorLock drive will then disconnect and be removed from the list.

Desktop App

1. Open the ArmorLock app.
2. In the **List View**, select the drive you want to remove.
3. At the **bottom** of the List View, click the **– icon** to remove a drive.
4. A popup screen will confirm the drive selected to be removed.
5. Click **Remove** to continue or click **cancel**.
6. You may be asked to enter the authentication (password) for your computer.
7. The ArmorLock drive will then disconnect and removed from the list.

Authorize Local Users

Authorizing additional users can only be done from a phone or computer that is a designated Manager. This section describes how a Manager can authorize another phone or computer to unlock and use or manage an ArmorLock drive when they are all in the same physical location (both within distance to the ArmorLock drive). Authorization will remain in place until a Manager deauthorizes that user/manager, resets the drive to factory settings, performs a "remove drive" operation, or the Recovery Key is used to regain access to the drive.

User Requesting Access to a Drive

1. Download and open the ArmorLock app.
2. Add the drive.
   a. **Mobile** – Select **Add Drive** and scan the **QR code** on the back of the drive.
   b. **Desktop** – In the **List View**, click the **Add Drive** button. Enter the 8-digit **Short Code** found on the back of the drive, next to the QR code.
3. Request access.

a. **Mobile** – Select **Request Access**. A **Scan QR Code** step will appear, and the requester must wait for the Manager to scan the QR code.
b. **Desktop** – Click **Request Access**, then click **Send Request**. The message "Waiting for Manager Approval" will appear.

Manager Authorizing Access

1. Drive **manager** reviews and rejects or approves the request.
   a. **Mobile** – Select **review local access request**. You can then edit the **User Name** and make the user a **Manager** if needed. Select **Scan User ID** and scan the QR Code displayed on the new user's device. Access is granted to the new user.
   b. **Desktop** – In **List View**, the drive will show **access request pending**. Click the drive and click **Authorize** to approve the request. Then enter the **Short Code** from the phone that is requesting access. You should see **Short Code Verified**, then click **Authorize**.

      - **Note:** On the requesting device, a QR code and Short Code will be displayed after the request is sent.
2. The drive will be automatically authenticated and added to the list of drives.

Authorize Remote Users Before You Ship the Drive

Authorizing additional users can only be done from a phone or computer that is a designated Manager. This section describes how a Manager with an ArmorLock drive in their possession can authorize a remote phone or computer to unlock and use or manage the drive. This procedure is used to authorize access to someone else before you ship them the drive. Authorization will remain in place until a Manager deauthorizes that user/manager, resets the drive to factory settings, or the Recovery Key is used to regain access to the drive.

User Requesting Access to a Drive

1. Download and open the ArmorLock app.
2. Go to the **Main Menu**.
   a. **Mobile** – Select the three-dot icon in the top-left corner then select **Share User ID**.
   b. **Desktop** – From the Main Menu, click **Share** then click **Share User ID**.
3. Select **Send User ID** and select your preferred method of sending, **email** or a **messaging** app.
   a. Input the recipient's credentials and send.
   b. Close the window.

Manager Authorizing Access

1. Open the email or text message from the user and open the link to **authorize** the User.
   a. **Mobile** – The app will open and a "User ID Added" confirmation will popup. Select **Authorize** to continue.
   b. **Desktop** – The app will open, and a popup window will ask you to add the user ID. You can also edit the name of the User. Click **Add**, and the user will be added to your authorized users list. Click **OK** to continue.

2. Select a drive to **add** the User.
   a. **Mobile** – The Drive List view will appear. Managers can add the User to multiple drives by selecting the drives from the list, then selecting **Authorize**.

      Note: If you selected multiple drives, an additional popup that displays the number of selected drives will appear. Select **Authorize** to authorize the User for access to those drives.
   b. **Desktop** – Click on a drive and then click on **Manager ID icon**. At the bottom of the **card view**, click the **+ icon** to see the list of authorized users. Click the user and select his or her **Role** and click **Add**. You should now see the User added to the drive **Manager Settings** window.
3. The **Manager** can then ship the drive to the remote **User**.

User Receives and Adds the Drive

1. The **User** connects the drive to the computer and opens the ArmorLock app.
   a. **Mobile** – Select **Add Drive**. Locate the **QR code** on the back of the drive and scan it with your phone.
   b. **Desktop** – In the **List View**, click the **Add Drive** button. Enter the unique 8-digit **Short Code** found on the back of the drive, underneath the QR code.
2. The drive will be automatically authenticated and added to your list of drives.

4 More About Your ArmorLock App and Drive

The ArmorLock mobile and desktop apps can be used to unlock and lock ArmorLock drives, manage multiple users and drives and track the last known location of a drive. The following are additional features of your ArmorLock app and drive.

Drive Indicators

The LED lights on the ArmorLock drive indicate whether the drive is locked or unlocked. To enable or disable the LED, follow these steps.

1. Open the ArmorLock app.
2. Select the **gear** icon of the desired drive located on the main screen.
3. Under the **Settings** section, select the drive indicator button to enable or disable the LED. By default, the LED is enabled.

App Version

To view the version of the ArmorLock app, follow the steps below. This process may be required when contacting support.

1. Open the ArmorLock app.
2. Access the **Main Menu**.
   a. **Mobile** – Select the **3-dot** icon.
   b. **Desktop** – Click the **ArmorLock** menu at the top of the window.
3. Select **About**.
4. The **app version** will be displayed with the same syntax as the following example: Version 1.0.0 (303).

User Authentication

When enabled, user authentication uses the user authentication features of your smartphone or computer to validate your authorization to use the app. If the Manager of a drive has enabled "User Authentication" then that will be enforced for all drive Users. If a user turns off their user authentication feature on their phone or computer, they will not be able to use the app to unlock the drive. To enable or disable this feature, follow these steps.

1. Open the ArmorLock app.
2. Select the **gear** icon of the desired drive located on the main screen.
3. Under the **Manager Settings** section, use the slider-button for **User Authentication** option to enable or disable user authentication access.

Location Tracking

This optional feature displays the last known location where the drive was used and adds a map location to each entry. To enable or disable this feature, follow these steps.

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings**.

   a. **Mobile** – Select the **gear** icon, then select **Location Tracking**.
   b. **Desktop** – Click on a drive and then click on the **gear** icon. Click **Location Tracking**.
3. To view the drive's location, select the drive.
   a. **Mobile** - Select the **Last Known Location** button.
   b. **Desktop** - Click the **map pin** icon.

Drive Information

This feature displays the serial number, firmware version, and other information which may be useful when contacting Technical Support.

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings**.
   a. **Mobile** – Select the **gear** icon, then select **Drive Information** under Settings.
   b. **Desktop** – Click on a drive and then click on the **'i'** icon.
3. The drive information will be displayed and open source licenses available to view.

How to Use Recovery Key

The following steps illustrate how to use the Recovery process to add a previously-authorized drive to the ArmorLock app. Either method (mobile or desktop) can be used. This operation will preserve existing data on the drive, but will remove access for all other users.

1. **Mobile:** Your mobile device can be used to recover a drive.
   a. Connect the ArmorLock drive to your computer.
   b. Scan the **Recovery Key QR code** saved during initial setup.
   c. After the recovery process is complete, a Successful Setup window will open. Select **Close**.
2. **Desktop:** You can also recover a drive using a macOS system.
   a. Connect the ArmorLock drive to your computer.
   b. Click **Add Drive**.
   c. Enter the 8-digit **Short Code** located on the back of the drive.
   d. Click **Use Recovery Key**.
   e. Type in the 64-character **Recovery Code**.
   f. After the recovery process is complete, a Successful Setup window will open. Click **Close**.

Damaged Pairing Recovery for New Devices

On occasion, authorized users may acquire a new phone or laptop and need to recover ArmorLock pairing or remove a drive card. The following steps illustrate how to use the recovery key to recover pairing with a new mobile device or desktop system.

Recover Pairing

1. Connect the ArmorLock drive to your computer.
2. Select **Recover Pairing**.
3. Select **Use Recovery Key**.
4. Scan or type in the 64-character Recovery QR Code.
5. After the recovery process is complete, a Successful Setup window will open.

6. Select **Close**.

Recover Pairing (Desktop)

1. Connect the ArmorLock drive to your computer.
2. Click **Recover Pairing**.
3. Click **Use Recovery Key**.
4. Type in the 64-character Recovery Code.
5. After the recovery process is complete, User and Manager roles will be recovered.

5 Manager Settings

The Manager of a drive has access to a number of manager-specific settings. In Card view, select the **gear** icon to view the full list of manager settings that can be applied to an ArmorLock drive within distance of your device.

Adding and Removing Users

The ArmorLock app can be used to manage which users have authorized access to each ArmorLock drive.

Adding a User

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings** to **add** the User.
   a. **Mobile** – Select the **gear** icon, then select **Manager Settings**. Select **Authorized Users**, then select the **+** icon to authorize a user. Select the user, then click **Authorize**. You should now see that user added to the list of authorized users.
   b. **Desktop** – Click on a drive and then click on the **Manager ID** icon. At the bottom of the **card view**, click the **+** icon to see the list of authorized users. Click the user and select his or her **Role** and click **Add**. You should now see the user added to the drive **Manager Settings** window.
3. You can now edit the **role** and also remove an authorized user at any time.

Removing a User

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings**.
   a. **Mobile** – Select the **gear** icon, then select **Manager Settings**. Select **Authorized Users**, then select the **User Name** to be removed. Select the **Remove User** button.
   b. **Desktop** – Click on a drive and then click the **Manager ID** icon. Select on the name of the user to be removed. At the bottom of the card view, click the **-** icon to remove the user.

User Name

The User Name feature allows the smartphone to be renamed as it is identified in connection with the ArmorLock drive. This does not change the smartphone name.

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings**.
   a. **Mobile** – Select the **gear** icon, then select **Manager Settings** to edit. Select **User Name** to edit, then select **Save Changes**.
   b. **Desktop** – Click on the **ArmorLock** menu, then preferences. Click the user name to edit and click **OK** to save.
3. The **ArmorLock** User Name is now changed.

New Recovery Key

The New Recovery Key option allows Drive Managers to generate a new Recovery Key if they suspect the existing key has been compromised. Using this feature will make the previous Recovery Key invalid. Use the following steps to create a new Recovery Key.

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings**.
   a. **Mobile** – Select the **gear** icon, then select **Manager Settings**. Select **New Recovery Key**. Select **Generate** to continue.
   b. **Desktop** – Click on a drive and then click on the **key** icon. Click **Generate New**.
3. Make sure to **save** the new Recovery Key.
   a. **Note:** The old Recovery Key will be invalid.

Read-Only Mode

The ArmorLock drive can be set to read-only mode. This prevents users from modifying or deleting files. Note that this feature has a delayed effect; it takes effect after the next unlock.

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings**.
   a. **Mobile** – Select the **gear** icon, then select **Manager Settings**. Next, select **Read-Only**.
   b. **Desktop** – Click on the **drive gear** tab and then, under **Manager Settings**, click **Read-Only**.
3. Changes to **read-only** will be applied next time the drive is unlocked.

Reset to Factory Settings

The ArmorLock drive can be reset to the factory settings. This action erases all data, settings, authorizations, user IDs, and recovery keys.

1. Open the ArmorLock app.
2. Select a drive and go to **Manager Settings**.
   a. **Mobile** – Select the **gear** icon, then select **Manager Settings**. Next, select **Reset to Factory Settings**. Select **Reset** to continue.
   b. **Desktop** – Click on the **drive gear** tab and, under **Manager Settings**, click **Reset to Factory Settings**. Click **Reset to Factory Settings** to continue.
3. All data, settings, authorizations, user IDs, and the recovery key will be permanently erased.

6 Keeping ArmorLock Up to Date

Firmware Updates: Using iOS Mobile App

Users are encouraged to use the latest version of the ArmorLock firmware. A notification will appear if an update is available after connecting the drive.

1. An "Update Available" notification will appear.
   a. **Note:** If your app is out-of-date, the message will be "Firmware Update Required".
2. Select the notification to open the ArmorLock app.
3. Select the **Tap to update** button.
4. Using the computer, eject the drive.
5. An "Update Complete" notification will appear.

If you are not ready to update the firmware for your iOS device, select **Update Later**.

Firmware Updates: Using macOS Desktop App

The ArmorLock firmware can be set to update automatically. If automatic updates are not enabled, use the following steps to install the latest version.

1. Connect the ArmorLock drive to the computer.
2. Open the ArmorLock app.
3. If an update is available, a "Firmware Update Available" message will appear beneath the lock/unlock icon.
   a. **Note:** If your app is out-of-date, the message will be "Firmware Update Required".
4. Click **Update Firmware Now.**
5. Eject the drive and reboot.
6. A "Firmware Update Complete" message will appear.

If you are not ready to update the firmware for your macOS system, select **Update Later**.

7 Compliance and Warranty Information

Regulatory Compliance

Safety Compliance

Approved for US and Canada. CAN/CSA C22.2 No. 62368-1-14: Audio/Video, Information and Communication Technology Equipment Part 1: Safety requirements)

Approuvé pour les Etats-Unis et le Canada. CAN/CSA C22.2 No. 62368-1-14: Sûreté d'équipement de technologie de l'information.

FCC Class B Information

NOTE: This device 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 device 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 device does cause harmful interference to radio or television reception, which can be determined by turning the device off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

Any changes or modifications not expressly approved by the manufacturer could void the user's authority to operate the device.

This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Radiation Exposure Statement:

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Industry Canada Statement

This device complies with ISED's license-exempt RSSs. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Le présent appareil est conforme aux CNR d' ISED applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes : (1) le dispositif ne doit pas produire de brouillage préjudiciable, et (2) ce dispositif doit accepter tout brouillage reçu, y compris un brouillage susceptible de provoquer un fonctionnement indésirable.

Radiation Exposure Statement:

This equipment complies with ISED radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator and your body.

Déclaration d'exposition aux radiations:

Cet équipement est conforme aux limites d'exposition aux rayonnements ISED établies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé avec un minimum de 20 cm de distance entre la source de rayonnement et votre corps.

ICES-3(B)/NMB-3(B) Compliance Statement

Cet appareil numérique de la classe B est conforme à la norme NMB-003(B) du Canada.

This device complies with Canadian ICES-003 Class B.

CE Compliance For Europe

Marking by the CE symbol indicates compliance of this system to the applicable Council Directives of the European Union, including Low-Voltage Directive (LVD) 2014/35/EU, the Radio Equipment Directive (RED) (2014/53/EU), and RoHS Directive (2011/65/EU) as amended by 2015/863/EU. Operating characteristics of the wireless radio (a) Frequency band: 2412-2472Mhz (b) Maximum radio-frequency power transmitted in the bands is 8dBm. A "Declaration of Conformity" in accordance with the applicable directives has been made and is on file at Western Digital Europe.

Warranty Information

For those that have previously purchased a G-Technology® ArmorLock™ NVMe SSD, model number 0G10484-1, please see the following link for your user manual with warranty information at https://support-en.g-technology.com/app/answers/detail/a_id/29803.

SanDisk® Manufacturer's Retail Products Limited Warranty (All Regions Except Australia)

This SanDisk Professional device is covered by a 3-year limited warranty (or 3-year warranty in regions not recognizing "limited") from the date of purchase, subject to the applicable warranty terms and conditions, as defined in http://www.sandisk.com/wug.

How To Make A Warranty Claim

Please go to www.sandisk.com and select "support" for more information on making a warranty claim (SanDisk Support Page).

If it is determined that your product may be defective, you will receive an RMA and product return instructions. You are responsible for any expenses associated with a claim under SanDisk's Limited Warranty.

You must send your product in a secure, prepaid package, to the address provided with your RMA number. Proof of purchase is required for all warranty claims.

SanDisk Manufacturer's Retail Products Limited Warranty (Australia)

SanDisk warrants to the end user, that this product, excluding content and or software supplied with or on the product, will be free from material defects in manufacture, will conform to SanDisk's published product specifications and be fit for normal use for a period of 3 years from the date of purchase, provided that the product is legally placed on the market.

When making a claim under this Limited Warranty, SanDisk may at its option repair this product or provide you with an equivalent product; and if unable to repair or replace the product, will refund the purchase price. The full terms of SanDisk's warranty and warranty period are available at: www.sandisk.com/wug.

Warrantor details:

Hamilton House, Regent Park, Kingston Road Leatherhead, Surrey, KT22 7PL, UK Tel: 0808-234-9816 (UK local toll free) or (44) 203-3183-965 (UK)

How to make a warranty claim:

Before you return the product you must first obtain a Return Material Authorization (RMA) number. Please either:

1. contact SanDisk at 1 800 262 504 (M-F | 9 am – 6 pm New South Wales Time) or email SanDisk (support@SanDisk.com) and provide proof of purchase (showing date and place of purchase and name of the reseller) and product name, type and number; or
2. contact the dealer from whom you originally purchased the product.

Please go to www.sandisk.com/support for more information on making a warranty claim (SanDisk Support Page). If it is determined that your product may be defective, you will receive an RMA number and product return instructions. You are responsible for any expenses associated with a claim under SanDisk's Limited Warranty. You must send your product in a secure, prepaid package, to the address provided with your RMA number. Proof of purchase is required for all warranty claims.

Australian consumers only:

Notwithstanding the terms of this Limited Warranty, SanDisk's products come with guarantees that cannot be excluded under the Australian Consumer Law. You are entitled to a replacement or refund for a major failure and for compensation for any other reasonably foreseeable loss or damage. You are also entitled to have the products repaired or replaced if the products fail to be of acceptable quality and the failure does not amount to a major failure.

How to Handle an ArmorLock Drive

SanDisk Professional products are precision instruments and must be handled with care during unpacking and installation. Rough handling, shock, or vibration can damage drives. Always observe the following precautions when unpacking and installing your external storage product:

- The rugged ArmorLock drive is built to withstand up to a three meter (3m) drop (on carpeted concrete floor) and 1,000 lb. crush resistance. Do not subject the drive to drop or crush events with higher limits.
- It is always recommended to handle the drive with as much care as possible.

8 Glossary

Many of the terms used in this User Manual are defined in this section.

Authorized User

A user that can unlock or access an ArmorLock device.

File System

Controls how data is stored and retrieved. Common types include:

- macOS (HFS+) – Time Machine compatible
- Windows (NTFS) – Standard Windows file format
- Windows and macOS (exFAT) – For flexibility between both operating systems

Manager

One of two roles to manage the ArmorLock drive. The manager can unlock the drive, erase/format the drive, authorize/deauthorize additional devices, view/edit logs, and set certain parameters (read-only, etc.). There must be at least one manager per drive, but additional managers can be added.

QR Code

A "Quick Response" matrix barcode which allows instant access to the information hidden within the code. The ArmorLock QR code is located on the back of the drive, and is used with the app.

USB

Universal Serial Bus (USB) is an industry standard for connecting computers and peripherals. The ArmorLock drive features a USB-C connector, and includes USB-A and USB-C cables for connecting the drive to a computer.

User

An authorized phone or computer that can unlock the drive. This role also has the ability to erase or format the drive (unless the manager has prevented this option). A user role is not required to use the drive.

User ID

Information that identifies the user, such as user key and user name.

User Key

A (public) key generated by the app, and assigned to a user. Note that if the app is deleted and reinstalled, a new key is created and the device will need to be paired again.

User Name

The "friendly" name of the user. This information is stored on the drive, but can be changed by the manager.

Index

Western Digital
5601 Great Oaks Parkway
San Jose, California 95119 U.S.A

D015-000043-AA00