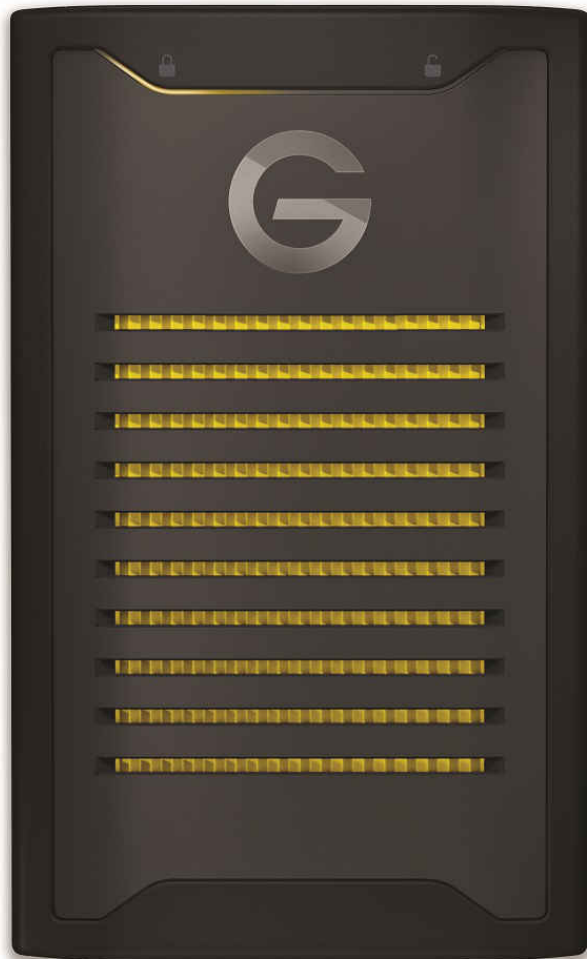




# ArmorLock™

NVMe™ SSD mit Verschlüsselung und Mobile- sowie Desktop-Apps

Bedienungsanleitung



## Zugriff auf den Onlinesupport

Auf unserer [Produktsupport-Website](#) können Sie unter folgenden Themen wählen:

- **Downloads:** Laden Sie Software und Updates für Ihr ArmorLock-Produkt herunter.
- **Garantie und Rückgabe:** Überprüfen Sie Ihre Garantie, fordern Sie ein Ersatzprodukt an (RMA).
- **Frage stellen:** Senden Sie eine Anfrage zu einem Produkt oder eröffnen Sie einen Supportfall.
- **AarmorLock Community:** Tauschen Sie sich in unserer [Community](#) mit anderen ArmorLock-Nutzern aus.

Wenn Sie eine G-Technology® ArmorLock™ NVMe SSD, Modellnummer OG10484-1, erworben haben, verwenden Sie bitte den folgenden Link für Ihre Bedienungsanleitung mit Garantieinformationen:  
[https://support-en.g-technology.com/app/answers/detail/a\\_id/29803](https://support-en.g-technology.com/app/answers/detail/a_id/29803).

# Inhalt

Zugriff auf den Onlinesupport.....	i
------------------------------------	---

## Kapitel 1: Willkommen bei ArmorLock..... 1

Hauptmerkmale.....	1
ArmorLock-App.....	2
Ihr Schlüssel zu maximaler Sicherheit, Geschwindigkeit und Benutzerfreundlichkeit.....	2
Lieferumfang.....	2
Technische Hinweise.....	2
Laufwerkskompatibilität.....	2
App-Kompatibilität.....	2
Kompatibilität zwischen USB und Betriebssystem.....	3
Bluetooth Kompatibilität.....	3
Ein Blick auf das ArmorLock-Laufwerk.....	3

## Kapitel 2: Erste Schritte..... 5

Beschaffung der Mobile-App.....	5
Herunterladen und Einrichten der App.....	5
Übersicht zur ArmorLock Mobile-App.....	6
Hinzufügen eines neuen Laufwerks in der Mobile-App.....	7
Einrichten und Verwenden des Laufwerks.....	7
Beschaffung der Desktop-App.....	9
Herunterladen und Einrichten der App.....	9
Übersicht zur ArmorLock Desktop-App.....	10
Hinzufügen eines neuen Laufwerks in der Desktop-App.....	11
Einrichten und Verwenden des Laufwerks.....	11

## Kapitel 3: Wichtigste Funktionen..... 13

Entsperren und Sperren des Laufwerks.....	13
Automatisch entsperren.....	13
Mobile-App.....	13
Desktop-App.....	14
Entfernen einer Festplatte.....	14
Mobile-App.....	14
Desktop-App.....	14
Autorisieren von lokalen Anwendern.....	14
Anwender sendet Anfrage auf Laufwerkszugriff.....	15
Manager autorisiert Zugriff.....	15
Autorisieren von entfernten Anwendern vor Verschicken des Laufwerks.....	15

Anwender sendet Anfrage auf Laufwerkszugriff.....	16
Manager autorisiert Zugriff.....	16
Anwender erhält Laufwerk und fügt es hinzu.....	16
Autorisieren von Remote-Anwendern nach Verschicken des Laufwerks.....	17
Anwender sendet Anfrage auf Laufwerkszugriff.....	17
Manager autorisiert Zugriff.....	18
Anwender erhält Autorisierung und Zugriff auf das Laufwerk.....	19

-----

**Kapitel 4: Weitere Informationen zu ArmorLock-Apps und  
-Laufwerken.....20**

Festplattenanzeigen.....	20
Anwendungsversion.....	20
Anwender-Authentifizierung.....	20
Standortverfolgung.....	21
Festplatteninfos.....	21
Verwendung des Wiederherstellungsschlüssels.....	21
Wiederherstellung der Kopplung bei neuen Geräten.....	22

-----

**Kapitel 5: Manager-Einstellungen..... 23**

Hinzufügen und Entfernen von Anwendern bei einem Laufwerk.....	23
Hinzufügen eines Anwenders.....	23
Entfernen eines Anwenders.....	23
Anwendername.....	24
Neuer Wiederherstellungsschlüssel.....	24
Schreibgeschützter Modus.....	24
Aktualisierungen einschränken.....	25
Zurück auf Werkseinstellungen.....	25

-----

**Kapitel 6: Aktualisieren des ArmorLock-Laufwerks.....26**

Firmwareaktualisierungen: Mobile-App unter iOS.....	26
Firmwareaktualisierungen: Desktop-App unter macOS.....	26

-----

**Kapitel 7: Konformitäts- und Garantieinformationen.....27**

Einhaltung gesetzlicher Bestimmungen.....	27
Konformität mit Sicherheitsanforderungen.....	27
Informationen zu FCC Klasse B.....	27
Industry Canada Statement.....	28
ICES-3(B)/NMB-3(B) Konformitätserklärung.....	28
CE-Konformität für Europa.....	28
KC-Hinweis (Nur Republik Korea).....	28

VCCI-Erklärung.....	29
NCC-Erklärung (Taiwan).....	29
RoHS (Taiwan).....	29
Garantieinformationen.....	29
Garantie für SanDisk Einzelhandelsprodukte (alle Regionen außer Australien).....	29
Garantie für SanDisk Einzelhandelsprodukte (Australien).....	30
Nur für Verbraucher in Australien:.....	30
Handhabung eines ArmorLock-Laufwerks.....	31

-----  
**Kapitel 8: Glossar..... 32**

Autorisierter Anwender.....	32
Dateisystem.....	32
Manager.....	32
QR-Code.....	32
USB.....	32
Anwender.....	32
Anwender-ID.....	33
Anwenderschlüssel.....	33
Anwendername.....	33

**Index..... 34**

# Willkommen bei ArmorLock

Die G-DRIVE ArmorLock SSD und die dazugehörigen Apps wurden entwickelt, um eine innovative und benutzerfreundliche Lösung zur Datensicherung zu schaffen. Absolut sicher, erstaunlich einfach. Die Verschlüsselung ist nur der Anfang.

## Hauptmerkmale

### PASSWÖRTER WAREN GESTERN

Wenn Sie Passwörter suchen, Codes eingeben und Software herunterladen müssen, verlangsamt das den Zugriff auf wichtige Inhalte. Wir haben solche Hindernisse beseitigt, ohne Kompromisse bei der Sicherheit einzugehen. Bei der ArmorLock™ - Technologie ist Ihr Smartphone der Schlüssel – mithilfe der biometrischen Authentifizierung sind die Inhalte schnell und einfach abrufbereit.

### BLITZSCHNELLE DATENÜBERTRAGUNG

Übertragungszeit bedeutet Stillstand. Der wärmeabführende Aluminiumkern der G-DRIVE™ ArmorLock™ SSD sorgt für dauerhafte Übertragungsgeschwindigkeiten auf Profi-Niveau von bis zu 1.000 MB/s\*\* beim Lesen und Schreiben.

### AUTOMATISCHES ENTSPERREN

Autorisieren Sie Ihr Telefon oder Ihren Computer für schnellen Zugriff auf die vertraulichen Daten Ihrer G-DRIVE™ ArmorLock™ SSD. Mit dem neuen Feature zum automatischen Entsperren können Sie Ihre Festplatte bequem automatisch entsperren lassen, wenn sie mit einem autorisierten Smartphone oder Computer verbunden wird.

### INNOVATIVE AUTORISIERUNG

Zusammenarbeit spielt eine entscheidende Rolle. Doch mit der Zunahme der Anwender und Speichergeräte steigen auch Sicherheitsrisiken. Deshalb bietet die ArmorLock™ -App sichere Funktionen für die Autorisierung und Verwaltung vieler Anwender. So behalten Sie jederzeit Überblick und Kontrolle – auch wenn viele Laufwerke verwaltet werden müssen.

### ZUVERLÄSSIGE LAUFWERKSVERWALTUNG

Bevor Sie wichtigen Content an Partner versenden, können Sie diese Partner über Ihren bevorzugten E-Mail- oder Messaging-Dienst zum Zugriff auf die Daten der G-DRIVE™ ArmorLock™ SSD autorisieren. Mit der App können Sie Ihr Laufwerk in eines der kompatiblen Dateisysteme formatieren. Wenn Sie die Inhalte nicht mehr benötigen, können Sie die Inhalte einfach und sicher mit Secure Erase löschen. Sie wissen nicht, wo Ihr Laufwerk zuletzt verwendet wurde? Die App zeigt es Ihnen auf einer Karte.

### MAXIMALE DATENSICHERHEIT

Die immer aktive hochsichere 256-Bit-AES-XTS-Hardwareverschlüsselung sorgt für zuverlässigen Datenschutz ohne Kompromisse bei der Geschwindigkeit. Die G-DRIVE™ ArmorLock™ SSD wird herstellerseitig gesperrt geliefert und ist somit vor dem Eintreffen bei Ihnen für niemanden zugänglich. Sobald das Laufwerk entsperrt ist, haben Sie schnellen Zugriff auf die gespeicherten Inhalte. Durch das Auswerfen wird das Laufwerk automatisch gesperrt – und auf die Inhalte kann nicht mehr unberechtigt zugegriffen werden.

### ROBUSTES DESIGN

Produktionstrucks, DIT-Wägen, Pelican Cases und Rucksäcke. Die G-DRIVE™ ArmorLock™ SSD bietet professionelle und verlässliche Robustheit. Dafür sorgen ein stabiles und leicht zu tragendes Gehäuse, Fallsicherheit bis 3 m\*\*\*, Stoßfestigkeit bis 500 kg und Staub- und Wasserdichtheit gemäß IP67.

## ArmorLock-App

### Ihr Schlüssel zu maximaler Sicherheit, Geschwindigkeit und Benutzerfreundlichkeit

Die ArmorLock Mobile- und Desktop-Apps wurden so entwickelt, dass Sie Ihr ArmorLock-Laufwerk besonders einfach entsperren und verwalten können. Statt Passwörtern und Fingerabdrücken wird das Smartphone oder der Computer zum Schlüssel für das Entsperren des Laufwerks. Die App bietet wichtige Funktionen wie das Management mehrerer Laufwerke und Anwender, Secure Erase, sichere Selbstformatierung und Nachverfolgung des letzten bekannten Standorts des Laufwerks. Die Technik funktioniert wirklich einfach – wenn Sie mit Ihrem Smartphone zurechtkommen, dann auch mit ArmorLock.

## Lieferumfang

- G-DRIVE ArmorLock SSD
- Kabel für USB-C™ zu USB-C (unterstützt SuperSpeed USB 10 Gbps)
- Kabel für USB-C™ zu USB-A (unterstützt SuperSpeed USB 10 Gbps)
- Kurzanleitung
- Informationen zu Technischem Support und Garantie

## Technische Hinweise

---

**Hinweis:** Die G-DRIVE ArmorLock SSD ist ein Direct-Attached-Storage-Gerät, bei dem der Speicherzugriff direkt über den USB-Anschluss erfolgt. Das Produkt ist kein drahtloser internetbasierter Speicher.

---

## Laufwerkskompatibilität

Das Laufwerk kann über USB-C und USB-A 3.0 mit anderen Geräten verbunden werden und ist mit den folgenden Betriebssystemen kompatibel.

*Tabelle 1.1*

Windows®	macOS
Windows 10+	macOS 10.15+

## App-Kompatibilität

Die ArmorLock-App ist mit den nachfolgenden Betriebssystemen kompatibel. Die App ist erforderlich, um das Laufwerk zu entsperren und zu verwalten.

Tabelle 1.2

macOS	iOS
macOS 10.15+	iOS 13.2.+

**Wenn Sie über einen PC mit der Desktop-App auf ein ArmorLock-Laufwerk zugreifen möchten, müssen Sie ein 64-Bit-Betriebssystem verwenden.** Die Kompatibilität hängt von der jeweiligen Hardwarekonfiguration und dem Betriebssystem ab. Installieren Sie immer die aktuellsten App-Aktualisierungen für die neuesten Funktionen und Kompatibilitätsoptionen.

## Kompatibilität zwischen USB und Betriebssystem

Die folgende Tabelle enthält die Kombinationen aus USB-Verbindung und Betriebssystem, die derzeit mit dem ArmorLock-Laufwerk funktionieren.

Tabelle 1.3

Per USB angeschlossen unter ...	macOS	Windows
Die macOS-App ermöglicht ...	Koppeln und entsperren	–
Die iPhone-App ermöglicht ...	Koppeln und entsperren	Koppeln und entsperren
Die Android-App ermöglicht ...	Koppeln und entsperren	Koppeln und entsperren

## Bluetooth Kompatibilität

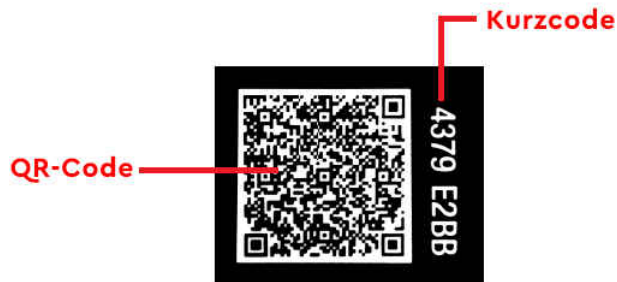
Ihr Smartphone und die G-DRIVE ArmorLock SSD kommunizieren per Bluetooth. Die G-DRIVE ArmorLock SSD ist mit der WPAN-Technologie (Wireless Personal Area Network) BLE (Bluetooth Low Energy) kompatibel, die Teil von Bluetooth 4.2 und neueren Spezifikationen dieser drahtlosen Technologie ist. Alle Betriebssysteme der vorhergehenden Liste sind mit Bluetooth Low Energy kompatibel.

## Ein Blick auf das ArmorLock-Laufwerk

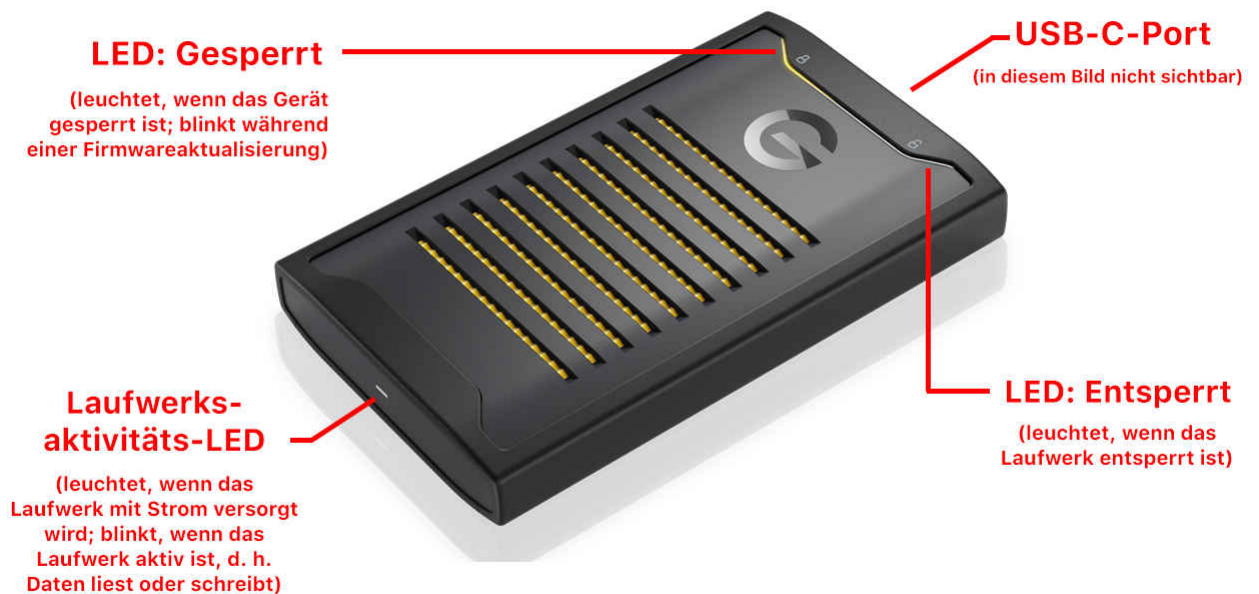
Die G-DRIVE ArmorLock SSD hat einige wichtige Features:

- Ein USB-C-Anschluss
- Drei (3) LEDs: gesperrt, entsperrt und Stromversorgung/Aktivität
- QR-Code und Kurzcode, eindeutig für jedes individuelle Laufwerk (auf der Rückseite des Laufwerks). Der QR-Code wird mit einer Smartphone-Kamera gescannt und der Kurzcode wird bei Computern eingegeben, um die App mit dem Laufwerk zu koppeln.





Auf dem nachfolgenden Bild sehen Sie die Positionen, Farben und Status der LEDs sowie die Position vom USB-C-Anschluss.



## 2

## Erste Schritte

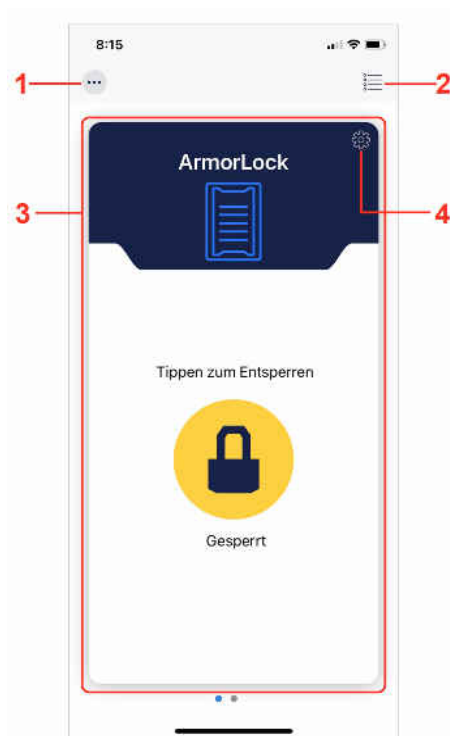
In diesem Kapitel erfahren Sie, wie Sie die ArmorLock-App herunterladen, die G-DRIVE ArmorLock SSD verbinden und einrichten.

### Beschaffung der Mobile-App

#### Herunterladen und Einrichten der App

1. Sie können die ArmorLock-App auf eine der folgenden Weisen herunterladen:
  - a. Verwenden Sie die Kamera Ihres Smartphones, um den QR-Code zu scannen, der sich auf der Rückseite des Laufwerks befindet
  - b. Besuchen Sie [GetArmorLock.com/Apps](http://GetArmorLock.com/Apps)
  - c. Suchen Sie im App Store nach „ArmorLock“
2. Starten Sie die ArmorLock-App.
3. Wählen Sie **Weiter** aus.  
**Hinweis:** Indem Sie **Weiter** auswählen, stimmen Sie dem Endbenutzer-Lizenzvertrag und der Datenschutzerklärung zu.
4. Das Fenster **Absturzberichte teilen** wird geöffnet. Wählen Sie **Zustimmen** aus, wenn Sie Absturzberichtsdaten teilen möchten. Andernfalls wählen Sie **Ablehnen** aus.
5. Wischen Sie durch die ArmorLock-Einführungsseiten (oder wählen Sie **Weiter** aus). Anschließend wählen Sie **Fertig** aus.
6. Geben Sie Ihren **Anwendernamen** für das Smartphone ein und wählen Sie **Speichern** aus.
7. Wenn die App die Berechtigung zum Senden von Benachrichtigungen erbittet, wählen Sie **Erlauben** aus. Wählen Sie erneut **Erlauben** aus, um fortzufahren.
  - a. **Hinweis:** Benachrichtigungen sind wichtig und helfen Ihnen, wenn neue Aktionen erforderlich sind, z. B. beim Autorisieren neuer Anfragen für den Zugriff auf das Laufwerk.
8. Wenn die globalen Standortdienste für das Mobilgerät deaktiviert sind, werden Sie aufgefordert, sie zu aktivieren.
  - a. Öffnen Sie die Einstellungen Ihres Smartphones und aktivieren Sie die globalen Standortdienste.
9. Wenn die Standortdienste für die App deaktiviert sind, werden Sie aufgefordert, sie zu aktivieren.
  - a. Öffnen Sie die Einstellungen Ihres Smartphones und aktivieren Sie die globalen Standortdienste.
10. Einige Tooltips werden angezeigt. Tippen Sie auf **Weiter** oder **OK**, um fortzufahren.
11. ArmorLock kann jetzt ein neues Laufwerk hinzufügen.

## Übersicht zur ArmorLock Mobile-App



1. **Hauptmenü:** Das Drei-Punkte-Hauptmenü bietet folgende Möglichkeiten:
  - a. **Anwender-ID teilen:** Ein neuer Anwender, der Zugriff auf ein Laufwerk anfordert, kann 1) die Anwender-ID seines Smartphones an einen Manager senden, wenn sich das Laufwerk an einem anderen Standort befindet, oder 2) sich den QR-Code seiner Anwender-ID am Smartphone anzeigen lassen, damit er von einem Manager am gleichen Standort gescannt werden kann.
  - b. **Anwender-ID scannen:** Der Manager eines Laufwerks kann die Anwender-ID eines Smartphones scannen, um den Anwender zur Anwenderliste hinzuzufügen. Das ist eine nützliche Methode, um Anwender-IDs von Ihrem Team zu sammeln, damit sie auf ein Laufwerk zugreifen können.
  - c. **App gemeinsam nutzen:** Sie können die ArmorLock-App mit anderen Anwendern teilen. Das ist besonders wichtig, wenn Sie entfernte Anwender autorisieren, bevor Sie ihnen ein Laufwerk zuschicken.
  - d. **Festplatte hinzufügen** oder **Festplatte entfernen.**
  - e. **Anwendungseinstellungen:** Ermöglicht Folgendes:
    - Teilen von Absturzberichten mit Western Digital über die Option **Datenschutz**
    - Bearbeiten des ArmorLock-**Benutzernamens** des Smartphones, wie mit dem ArmorLock-Gerät identifiziert
    - Aktivieren der Funktion **Automatische Entsperrung**
    - Aktivieren von **Tooltips**
  - f. **Hilfe** der Online-Bedienungsanleitung aufrufen. Sie können auch die Einführungsbildschirme und Anleitungsvideos anzeigen oder die Support-Webseite besuchen.
  - g. Bildschirm **Über** öffnen.
2. **Umschalt-Symbol:** Mit dem Umschaltersymbol können Sie zwischen den Modi „Kartenansicht“ und „Listenansicht“ wechseln.

3. **Laufwerkskarte:** Sobald Sie ein Laufwerk hinzugefügt haben, wird die „Laufwerkskarte“ für dieses Laufwerk angezeigt. Wischen Sie nach links, um ein neues Laufwerk hinzuzufügen. Wenn Sie mehrere Laufwerke hinzugefügt haben, können Sie nach links oder rechts wischen, um zwischen den Laufwerken umzuschalten.
4. **Zahnrad-Symbol der Laufwerkskarte:** Das Zahnrad-Symbol ist spezifisch für jedes einzelne Laufwerk und ermöglicht es Ihnen, die Laufwerkeinstellungen zu aktualisieren und zu verwalten.

## Hinzufügen eines neuen Laufwerks in der Mobile-App

In diesem Abschnitt erfahren Sie, wie Sie zum ersten Mal ein neues Laufwerk hinzufügen. Sie können diese Schritte auch verwenden, um zusätzliche Laufwerke für die Verwaltung mit der ArmorLock-App hinzuzufügen.

### Einrichten und Verwenden des Laufwerks

1. Schalten Sie Ihren Computer ein und melden Sie sich an.
2. Schließen Sie das Laufwerk an Ihren Computer an.
  - a. **Hinweis:** Es wird nicht empfohlen, das ArmorLock-Laufwerk an einen USB-Hub anzuschließen. Wenn es erforderlich ist, wird die Verwendung eines USB-Hubs mit Stromversorgung empfohlen, damit das Laufwerk ordnungsgemäß mit Energie versorgt wird.
3. Das ArmorLock-Laufwerk wird aktiviert und die LED unter dem Sperr-Symbol leuchtet auf.
4. Öffnen Sie die ArmorLock-App und fügen Sie ein neues Laufwerk hinzu.
  - a. **Kartenansicht** (Standardansicht): Wählen Sie das Symbol für **Festplatte hinzufügen** aus.
  - b. **Listenansicht:** Wählen Sie die Schaltfläche **+ Festplatte hinzufügen** aus.
  - c. **Hauptmenü:** Klicken Sie auf das **Drei-Punkte-Symbol** und wählen Sie **Festplatte hinzufügen** aus.
5. Die Meldung „Bluetooth erforderlich“ wird angezeigt, wählen Sie **Erlauben** aus. Wählen Sie **OK** aus, um fortzufahren.
  - a. **Hinweis:** ArmorLock verwendet Bluetooth, um eine Verbindung zu einem Laufwerk herzustellen, deshalb muss Bluetooth aktiviert sein.
6. Wenn Bluetooth deaktiviert ist, fordert Sie ein Popup dazu auf, Bluetooth einzuschalten.
  - a. Öffnen Sie die Einstellungen Ihres Smartphones und aktivieren Sie Bluetooth.
  - b. Öffnen Sie ArmorLock wieder und wählen Sie **Festplatte hinzufügen** aus.
7. Die Meldung „Kamerazugriff erforderlich“ wird angezeigt, wählen Sie **Erlauben** aus. Wählen Sie **OK** aus, um fortzufahren.
  - a. **Hinweis:** Der Kamerazugriff muss erlaubt werden, damit Sie QR-Codes mit dem Smartphone scannen können.
  - b. Bei Dunkelheit müssen Sie möglicherweise die **Taschenlampe** einschalten, um den QR-Code zu scannen.
8. Suchen Sie den QR-Code auf der Rückseite des Laufwerks und scannen Sie ihn mit Ihrem Smartphone. Drei Optionen werden angezeigt:
  - a. **Als Neu einrichten:** Startet die Ersteinrichtung für ein neues Laufwerk (Laufwerksname, Farbe, Format usw.).
  - b. **Schlüssel verwenden:** Ermöglicht es Ihnen, den gespeicherten Wiederherstellungsschlüssel einzugeben, um wieder Zugriff auf Ihr Laufwerk zu

- erhalten, wenn alle anderen Methoden ausscheiden. Hinweis: Dadurch werden auch alle anderen Anwender/Manager vom Laufwerk entfernt.
- c. **Zugriffsanfrage:** Ermöglicht es Ihnen, Zugriff auf eine Festplatte anzufordern, die bereits von einem anderen Gerät verwaltet wird.
9. Wählen Sie im Menü **Als Neu einrichten** aus. Konfigurieren Sie die Optionen zur **Einrichtung** des Laufwerks.
    - a. Geben Sie den **Namen** des Laufwerks ein (erforderlich). Nur Anwender mit Manager-Rolle können einen Festplattennamen eingeben.
    - b. Wählen Sie eine **Farbkennzeichnung** aus. Nur Anwender mit Manager-Rolle können eine Farbkennung auswählen.
    - c. Wählen Sie ein **Laufwerksformat** aus.
      - macOS (HFS+): Kompatibel mit Time Machine
      - Windows (NTFS): Windows-Format
      - Windows und macOS (exFAT): Zur flexiblen Verwendung mit beiden Betriebssystemen
    - d. Wählen Sie **Standortverfolgung** aus (optional).
      - Standortverfolgung ist standardmäßig deaktiviert. Aktivieren Sie den Erhalt von Hintergrundmeldungen und die ArmorLock-Funktionen.
      - Wenn die Option aktiviert wird, wird ein Popup zur Berechtigung für den Standortzugriff angezeigt. Wählen Sie **Erlauben** aus. Eine weitere Standorteinstellung muss ausgewählt werden: Sie haben die Wahl zwischen „Beim Verwenden der App erlauben“, „Einmal erlauben“ und „Nicht erlauben“.
    - e. **Erweiterte Einstellungen.**
      - **Anwender-Authentifizierung:** Standardmäßig deaktiviert. Aktiviert die Anwenderauthentifizierung (per Passcode, Fingerabdruck oder Face ID) für zusätzliche Sicherheit, um sicherzustellen, dass es sich beim Nutzer der App um den echten autorisierten Anwender handelt.
      - **Auto-Firmware-Aktualisierungen:** Standardmäßig aktiviert. Es wird empfohlen, diese Einstellung aktiviert zu lassen, damit zukünftige Aktualisierungen installiert werden.
    - f. Wählen Sie **Festpl. formatieren** aus.
      - Eine letzte Warnung meldet, dass alle vorhandenen Inhalte des Laufwerks dauerhaft gelöscht werden.
    - g. Wählen Sie **Löschen** aus.
      - Der Secure Erase-Vorgang für die Festplatte wird gestartet. Nicht die Verbindung des Laufwerks trennen oder die App verlassen.
  10. Speichern Sie den **Wiederherstellungsschlüssel**. Mit dem Wiederherstellungsschlüssel lässt sich der Zugriff auf das Laufwerk bei Bedarf wiederherstellen, wenn alle anderen Methoden nicht funktionieren. Es gibt mehrere Optionen zur Aufbewahrung.
    - a. **Fotos:** Dazu muss ArmorLock Zugriff auf die Fotos-App erhalten.
    - b. **Dateien:** Speichert ihn auf Ihrem Smartphone als PDF.
    - c. **Drucken:** Es wird dringend empfohlen, ihn zu drucken und an einem sicheren Ort aufzubewahren.
      - **Western Digital kann Ihren Zugriff nicht wiederherstellen, wenn Sie Ihren Wiederherstellungsschlüssel verlieren.**

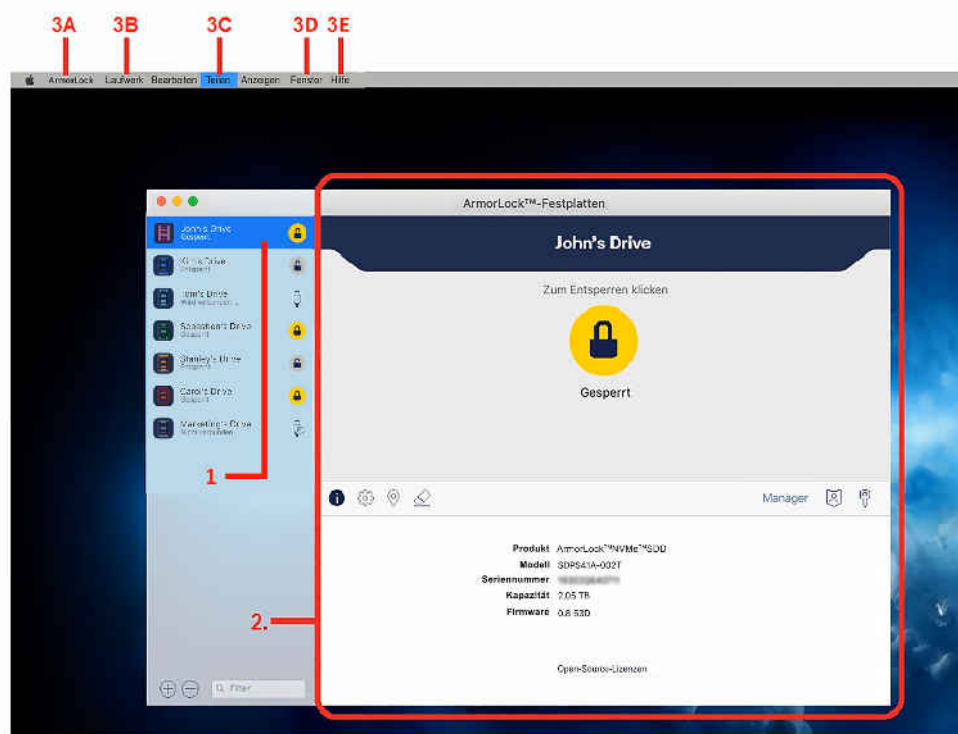
## Beschaffung der Desktop-App

Die ArmorLock Desktop-App ermöglicht es Ihnen, das Laufwerk mit dem Computer zu entsperren und zu verwalten. Einer der Hauptunterschiede bei der Verwendung der ArmorLock-App an einem Computer ist das Eingeben von eindeutigen alphanumerischen Kurzcodes, anstelle des Scannens von QR-Codes am Smartphone. Wenn ein Laufwerk hinzugefügt wird, muss der eindeutige **Kurzcode** eingegeben werden, der sich neben dem QR-Code befindet.

### Herunterladen und Einrichten der App

1. Sie können die ArmorLock-App auf eine der folgenden Weisen herunterladen:
  - a. Besuchen Sie [GetArmorLock.com/Apps](https://getarmorlock.com/apps)
  - b. Suchen Sie im App Store nach „ArmorLock“
2. Starten Sie die ArmorLock-App. Wählen Sie **Weiter** aus.
3. Das Fenster **Absturzberichte teilen** wird geöffnet. Wählen Sie **Zustimmen** aus, wenn Sie Absturzberichtsdaten teilen möchten. Andernfalls wählen Sie **Ablehnen** aus.
4. Klicken Sie sich durch die ArmorLock-Einführungsseiten und wählen Sie **Fertig** aus.
5. Geben Sie Ihren **Anwendernamen** für den Computer ein und klicken Sie auf **Speichern**.
6. Wenn die App die Berechtigung zum Senden von Benachrichtigungen erbittet, klicken Sie auf **Erlauben**. Klicken Sie erneut auf **Erlauben**, um fortzufahren.
  - a. **Hinweis:** Benachrichtigungen sind wichtig und helfen Ihnen, wenn neue Aktionen erforderlich sind, z. B. beim Autorisieren neuer Anfragen für den Zugriff auf das Laufwerk.
7. ArmorLock kann jetzt ein neues Laufwerk hinzufügen.

## Übersicht zur ArmorLock Desktop-App



1. **Listenansicht:** Wenn ArmorLock geöffnet ist, ist die Listenansicht der Ort, wo Sie die hinzugefügten Laufwerke finden.
  - a. In der unteren linken Ecke können Sie mit den Schaltflächen + und – Laufwerke **hinzufügen** bzw. **entfernen**.
  - b. Eine Liste der hinzugefügten Laufwerke wird auch in diesem Bereich angezeigt.
2. **Laufwerkskartenansicht:** Wenn Sie auf ein Laufwerk **kllicken**, werden ein Sperr-Symbol und Laufwerksinformationen in der Laufwerkskartenansicht angezeigt.
  - a. **Sperr-Symbol:** Klicken Sie darauf, um das Laufwerk zu entsperren.
  - b. **Entsperr-Symbol:** Klicken Sie darauf, um das Laufwerk zu sperren und auszuwerfen.
  - c. **i-Symbol:** Klicken Sie darauf (Standardansicht), damit der Laufwerksname, das Modell, die Seriennummer, die Kapazität, die Firmware und die Open-Source-Lizenzen angezeigt werden.
  - d. **Zahnrad-Symbol:** Klicken Sie darauf, um die **Einstellungen** des Laufwerks zu bearbeiten.
  - e. **Kartenstecknadel:** Klicken Sie darauf, damit der **letzte aufgezeichnete Standort** des Laufwerks angezeigt wird.
  - f. **Lösch-Symbol:** Damit können Sie das Laufwerk **sicher löschen** und **neu formatieren**.
  - g. **(Nur Manager-Rolle) ID-Symbol:** Klicken Sie darauf, um die Liste der **autorisierten Anwender** anzuzeigen und die jeweilige **Rolle** zu bearbeiten.
  - h. **(Nur Manager-Rolle) Schlüssel-Symbol:** Klicken Sie darauf, um einen **neuen Wiederherstellungsschlüssel** zu generieren und den bestehenden zu ersetzen.
3. **Hauptmenü:** Das Hauptmenü kann oben im App-Fenster aufgerufen werden. Es folgen die zentralen Untermenüs und ihre wichtigsten Optionen (nicht erschöpfend).

- a. **ArmorLock**
  - **Über ArmorLock:** ArmorLock-Version und Lizenzvertrag ansehen.
  - **Einstellungen:** ArmorLock-Anwendername festlegen und automatischen Start von ArmorLock bei der Anmeldung konfigurieren.
  - **Datenschutz:** Teilen von Absturzberichten mit Western Digital aktivieren oder deaktivieren
- b. **Laufwerk**
  - **Festplatte hinzufügen:** ArmorLock-Laufwerk zur App hinzufügen.
  - **Festplatte entfernen:** ArmorLock-Laufwerk von der App entfernen.
- c. **Teilen**
  - **Anwender-ID teilen:** Anwender-ID an einen Laufwerksmanager senden, um Zugriff auf ein anderes ArmorLock-Laufwerk anzufordern.
  - **App gemeinsam nutzen** – Sie können die ArmorLock-App mit anderen Anwendern teilen.
- d. **Fenster**
  - **Laufwerke:** Zeigt eine Liste der bekannten Laufwerke an.
  - **Benutzerliste:** Zeigt eine Liste der bekannten Benutzernamen an.
- e. **Hilfe**
  - **Bedienungsanleitung:** Zeigt die Online-Bedienungsanleitung an.
  - **Einführung anzeigen:** Zeigt eine Einführung zu der App an.
  - **Anleitung:** Zeigt Anleitungsvideos an.
  - **Support:** Öffnet die Support-Webseite.

## Hinzufügen eines neuen Laufwerks in der Desktop-App

In diesem Abschnitt erfahren Sie, wie Sie zum ersten Mal ein neues Laufwerk hinzufügen. Sie können diese Schritte auch verwenden, um zusätzliche Laufwerke für die Verwaltung mit der ArmorLock-App hinzuzufügen.

### Einrichten und Verwenden des Laufwerks

1. Schalten Sie Ihren Computer ein und melden Sie sich an.
2. Schließen Sie das Laufwerk an Ihren Computer an.
  - a. **Hinweis:** Es wird nicht empfohlen, das ArmorLock-Laufwerk an einen USB-Hub anzuschließen. Wenn es erforderlich ist, wird die Verwendung eines USB-Hubs mit Stromversorgung empfohlen, damit das Laufwerk ordnungsgemäß mit Energie versorgt wird.
3. Das ArmorLock-Laufwerk wird aktiviert und die LED unter dem Sperr-Symbol leuchtet auf.
4. Es gibt in der App drei Methoden, um ein neues Laufwerk hinzuzufügen.
  - a. **Listenansicht:** Klicken Sie auf die Schaltfläche **+ Festplatte hinzufügen**. Diese Option wird nur angezeigt, wenn im Fenster **Listenansicht** keine Laufwerke vorhanden sind.
  - b. **Untere linke Ecke:** Klicken Sie auf **+** oder **-**, um Laufwerke hinzuzufügen oder zu entfernen.
  - c. **Laufwerksmenü:** Klicken Sie auf **Festplatte** und wählen Sie **Festplatte hinzufügen** aus.



5. Klicken Sie auf **Festplatte hinzufügen**.
6. Das Fenster **Kurzcode** wird angezeigt. Geben Sie den Kurzcode des Laufwerks ein.
  - a. Der 8-stellige Kurzcode befindet sich auf der Rückseite des Laufwerks neben dem QR-Code.
  - b. Nach Eingabe der letzten Ziffer findet die App das Laufwerk automatisch.
7. Drei Optionen werden angezeigt.
  - a. **Als Neu einrichten**: die Ersteinrichtung (Name, Farbe, Format usw.) für ein neues Laufwerk.
  - b. **Schlüssel verwenden**: Stellt den Zugriff auf des Laufwerk wieder her, wenn alle anderen Methoden ausscheiden. Dadurch werden auch alle anderen Anwender/Manager vom Laufwerk **entfernt**.
  - c. **Zugriffsautorisierung**: Ihre Anwender-ID kann vom Manager der Festplatte gescannt werden, um Zugriff zu erhalten.
8. Klicken Sie auf **Als Neu einrichten**. Konfigurieren Sie die Optionen zur **Einrichtung** des Laufwerks.
  - a. Geben Sie den **Namen** des Laufwerks ein. Nur Anwender mit Manager-Rolle können einen Festplattennamen eingeben.
  - b. Wählen Sie ein **Laufwerksformat** aus.
    - macOS (HFS+): Kompatibel mit Time Machine
    - Windows (NTFS): Windows-Format
    - Windows und macOS (exFAT): Zur flexiblen Verwendung mit beiden Betriebssystemen
  - c. Wählen Sie eine **Farbkennzeichnung** aus. Nur Anwender mit Manager-Rolle können eine Farbkennung auswählen.
  - d. Wählen Sie **optionale** Einstellungen aus.
    - **Standortverfolgung**: Standardmäßig deaktiviert. Aktivieren Sie diese Option, damit der letzte bekannte Standort angezeigt wird, an dem das Laufwerk verwendet wurde, und ein Kartenstandort zu jedem Eintrag hinzugefügt wird.
    - **Anwender-Authentifizierung**: Standardmäßig deaktiviert. Ermöglicht die Anwenderauthentifizierung (Passwort, TouchID), dient als zusätzliche Authentifizierungsebene.
    - **Auto-Firmware-Aktualisierungen**: Standardmäßig aktiviert. Es wird empfohlen, diese Einstellung aktiviert zu lassen, damit zukünftige Aktualisierungen installiert werden.
  - e. Klicken Sie auf **Festpl. formatieren**.
    - Die Formatierung des Laufwerks beginnt. Nicht die Verbindung des Laufwerks trennen oder die App schließen.
9. Speichern Sie den **Wiederherstellungsschlüssel**. Mit dem **Wiederherstellungsschlüssel** lässt sich der Zugriff auf die Festplatte wiederherstellen, wenn alle anderen Methoden nicht funktionieren. Dadurch werden alle autorisierten Benutzer von der Festplatte entfernt. Es gibt mehrere Optionen zur Aufbewahrung.
  - a. **Drucken**: Es wird dringend empfohlen, ihn zu drucken und an einem sicheren Ort aufzubewahren. Western Digital kann Ihren Zugriff nicht wiederherstellen, wenn Sie Ihren Wiederherstellungsschlüssel verlieren.
  - b. **Als PDF speichern**: Speichert die Datei als PDF auf dem Computer.
10. Nach dem Speichern klicken Sie auf **Fertig**. Wenn Sie aufgefordert werden, zu bestätigen, dass Sie den Wiederherstellungsschlüssel gespeichert haben, klicken Sie auf **Bestätigen**.
11. Ihr Computer ist jetzt der **Manager** des Laufwerks und einsatzbereit.

## Wichtigste Funktionen

### Entsperren und Sperren des Laufwerks

Um das ArmorLock-Laufwerk zu sperren, müssen Sie es von Ihrem Computer auswerfen lassen. Ausgeworfene ArmorLock-Laufwerke sind gesperrt und können nur mit einer ArmorLock-App auf autorisierten Smartphones oder Computern entsperrt werden. In den folgenden Schritten wird beschrieben, wie das Laufwerk entsperrt und gesperrt werden kann.

1. Schließen Sie das ArmorLock-Laufwerk an einen Computer an.
  - a. Dadurch wird das Laufwerk mit Strom versorgt, damit es über eine ArmorLock-App sicher mit einem Smartphone oder Computer verbunden werden kann.
2. Öffnen Sie die ArmorLock-App auf Ihrem Smartphone oder Computer.
  - a. Die Mobile-App findet alle ArmorLock-Laufwerke innerhalb einer Entfernung von **10 Metern**.
3. Die App erkennt den aktuellen Zustand des ArmorLock-Laufwerks als **Gesperrt** oder **Entsperrt** und zeigt ein entsprechendes Statussymbol an.
4. Um das Laufwerk zu **Entsperren**, wählen Sie das Sperr-Statussymbol aus. Sobald es entsperrt ist, wird der Status durch ein Symbol mit offenem Schloss angezeigt.
  - a. Wenn die **Anwenderauthentifizierung** aktiviert ist, kann die Festplatte mit den Funktionen zur Anwenderauthentifizierung Ihres Smartphones entsperrt werden.
5. Um das Laufwerk zu **Sperren**, wählen Sie das Entsperr-Statussymbol aus.
  - a. **Mobile-App:** Die folgende Meldung wird angezeigt: „Verwenden Sie den Computer, um die Festplatte auszuwerfen und zu sperren.“ Es wird empfohlen, das Laufwerk vom Computer auswerfen zu lassen, um das Risiko von verlorenen oder beschädigten Daten zu minimieren.
  - b. **Desktop-App:** Verwenden Sie die ArmorLock-App, um das Laufwerk zu sperren.
6. Sobald das Laufwerk erfolgreich ausgeworfen wurde, zeigt die App das Symbol für den **Gesperrten** Status an.

### Automatisch entsperren

Mit dem neuen Feature zum automatischen Entsperren können Sie Ihr Laufwerk bequem automatisch entsperren lassen, wenn es mit einem autorisierten Smartphone oder Computer verbunden wird. Laufwerke mit aktivierter Anwender-Authentifizierung werden nicht automatisch entsperrt. Die Erlaubnis zur Geräteortung **Beim Verwenden der App erlauben** ist für dieses Feature erforderlich.

#### Mobile-App

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie das **3-Punkte-Symbol** für das Hauptmenü aus.
3. Wählen Sie **Anwendungseinstellungen** aus.
4. Verwenden Sie den Umschalter **Automatisch entsperren** zum Aktivieren.

## Desktop-App

1. Öffnen Sie die ArmorLock-App.
2. Öffnen Sie das **ArmorLock-Hauptmenü** oben im Fenster.
3. Wählen Sie **Voreinstellungen** und dann **Einstellungen** aus.
4. Aktivieren Sie das Kontrollkästchen **Bekannte Laufwerke beim Verbinden automatisch entsperren**.

**Hinweis:** Laufwerke mit aktivierter Anwender-Authentifizierung werden nicht automatisch entsperrt.

## Entfernen einer Festplatte

Führen Sie die folgenden Schritte durch, um ein ArmorLock-Laufwerk zu deauthorisieren oder von der App zu trennen.

### Mobile-App

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie das 3-Punkte-Symbol für das Hauptmenü aus.
3. Wählen Sie **Festplatte entfernen** aus.
  - a. Das Menü „Laufwerk entfernen“ wird geöffnet und alle verbundenen ArmorLock-Laufwerke werden aufgelistet.
4. Wählen Sie die Laufwerke aus, die Sie entfernen möchten, und tippen Sie auf **Entfernen**.
5. Ein Popup wird angezeigt, auf dem Sie bestätigen müssen, dass die ausgewählten Laufwerke entfernt werden sollen.
6. Wählen Sie **Entfernen** aus, um fortzufahren, oder tippen Sie auf **Abbrechen**.
7. Sie werden ggf. vom Mobilgerät aufgefordert, sich (per Fingerabdruck, Face ID oder Passcode) zu authentifizieren.
8. Dann werden die ArmorLock-Laufwerke deauthorisiert und aus der Liste entfernt.

### Desktop-App

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie in der **Listenansicht** das Laufwerk aus, das Sie entfernen möchten.
3. Klicken Sie am **Ende** der Listenansicht auf das – **Symbol**, um ein Laufwerk zu entfernen.
4. Ein Popup wird angezeigt, auf dem Sie bestätigen müssen, dass das ausgewählte Laufwerk entfernt werden soll.
5. Klicken Sie auf **Entfernen**, um fortzufahren, oder wählen Sie **Abbrechen** aus.
6. Sie werden ggf. dazu aufgefordert, sich bei Ihrem Computer (per Passwort) zu authentifizieren.
7. Dann wird das ArmorLock-Laufwerk deauthorisiert und aus der Liste entfernt.

## Autorisieren von lokalen Anwendern

Zusätzliche Anwender können nur über Smartphones oder Computer autorisiert werden, die als Manager festgelegt wurden. In diesem Abschnitt wird beschrieben, wie ein Manager den Zugriff anderer Anwender auf das Laufwerk autorisieren

kann. Anwender eines ArmorLock-Laufwerks müssen die ArmorLock-App entweder auf ihrem Smartphone oder Desktop-Computer installiert haben. Um einen neuen Anwender lokal zu autorisieren, müssen sowohl der Manager als auch der neue Anwender sich in der physischen Nähe des ArmorLock-Laufwerks befinden. Die Autorisierung gilt so lange, bis ein Manager diese vom Anwender/Manager aufhebt oder die Festplatte auf die Werkseinstellungen zurücksetzt, die Festplatte sicher entfernt, oder der Wiederherstellungsschlüssel verwendet wird, um wieder auf die Festplatte zugreifen zu können.

## Anwender sendet Anfrage auf Laufwerkszugriff

1. Laden Sie die ArmorLock-App herunter und öffnen Sie sie.
2. Fügen Sie das Laufwerk hinzu.
  - a. **Mobil:** Wählen Sie **Festplatte hinzufügen** aus und scannen Sie den **QR-Code** auf der Rückseite des Laufwerks.
  - b. **Desktop:** Klicken Sie in der **Listenansicht** auf die Schaltfläche **Festplatte hinzufügen**. Geben Sie den 8-stelligen **Kurzcode** ein, der sich auf der Rückseite des Laufwerks neben dem QR-Code befindet.
3. Senden Sie eine Zugriffsanfrage.
  - a. **Mobil:** Wählen Sie **Zugriffsanfrage** aus. Der Schritt **QR-Code scannen** wird angezeigt und der Anforderer muss warten, bis der Manager den QR-Code scannt.
  - b. **Desktop:** Klicken Sie auf **Zugriffsanfrage** und dann auf **Anfrage senden**. Die Meldung „Warte auf Manager-Genehmigung“ wird angezeigt.

## Manager autorisiert Zugriff

1. Der **Manager** des Laufwerks überprüft die Anfrage und kann sie ablehnen oder genehmigen.
  - a. **Mobil:** Wählen Sie **Lokale Zugriffsanfrage überprüfen** aus. Dann können Sie den **Anwendernamen** bearbeiten und den Anwender bei Bedarf als einen **Manager** festlegen. Wählen Sie **Anwender-ID scannen** aus und scannen Sie den QR-Code, der auf dem Gerät des neuen Anwenders angezeigt wird. Dem neuen Anwender wird der Zugriff gewährt.
  - b. **Desktop:** In der **Listenansicht** zeigt das Gerät **Zugriffsanfrage ausstehend** an. Klicken Sie auf das Laufwerk und dann auf **Autorisieren**, um die Anfrage zu genehmigen. Geben Sie dann den **Kurzcode** des Smartphones ein, von dem die Zugriffsanfrage ausgeht. Ihnen wird die Meldung **Kurzcode überprüft** angezeigt und Sie können auf **Autorisieren** klicken.
    - **Hinweis:** Nach dem Senden der Anfrage werden ein QR-Code und ein Kurzcode auf dem anfragenden Gerät angezeigt.
2. Das Laufwerk wird automatisch authentifiziert und zur Liste der Laufwerke hinzugefügt.

## Autorisieren von entfernten Anwendern vor Verschicken des Laufwerks

Zusätzliche Anwender können nur über Smartphones oder Computer autorisiert werden, die als Manager festgelegt wurden. In diesem Abschnitt wird beschrieben, wie ein Manager mit einem ArmorLock-Laufwerk Remote-Anwender per ArmorLock-App

autorisieren kann, damit sie das Laufwerk entsperren und verwenden oder verwalten können.

Dieses Verfahren ermöglicht es dem Manager, andere Anwender zum Zugriff auf das Laufwerk zu autorisieren, bevor das Laufwerk verschickt wird. Die Autorisierung gilt solange, bis ein Manager des Laufwerks diese vom Anwender/Manager aufhebt oder das Laufwerk auf die Werkseinstellungen zurücksetzt oder der Wiederherstellungsschlüssel verwendet wird, um wieder auf das Laufwerk zugreifen zu können.

## Anwender sendet Anfrage auf Laufwerkszugriff

1. Laden Sie die ArmorLock-App herunter und öffnen Sie sie.
2. Öffnen Sie das **Hauptmenü**.
  - a. **Mobil:** Wählen Sie das Drei-Punkte-Symbol in der oberen linken Ecke und dann **Anwender-ID teilen** aus.
  - b. **Desktop:** Klicken Sie im Hauptmenü auf **Teilen** und dann auf **Anwender-ID teilen**.
3. Wählen Sie **Anwender-ID senden** und dann Ihre bevorzugte Methode zum Senden aus, d. h. **E-Mail** oder eine **Messaging App**.
  - a. Geben Sie die Daten des Empfängers ein und senden Sie die Nachricht.
  - b. Schließen Sie das Fenster.

## Manager autorisiert Zugriff

1. Öffnen Sie die E-Mail oder Textnachricht des Anwenders und rufen Sie den Link auf, um den Anwender zu **autorisieren**.
  - a. **Mobil:** Die App wird geöffnet und die Bestätigungsmeldung „Anwender-ID hinzugefügt“ wird angezeigt. Wählen Sie **Autorisieren** aus, um fortzufahren.
  - b. **Desktop:** Die App wird geöffnet und ein Pop-up fordert Sie auf, die Anwender-ID hinzuzufügen. Sie können auch den Namen des Anwenders bearbeiten. Klicken Sie auf **Hinzufügen**, damit der Anwender zur Liste der autorisierten Anwender hinzugefügt wird. Klicken Sie auf **OK**, um fortzufahren.
2. Wählen Sie ein Laufwerk aus, um den Anwender **hinzuzufügen**.
  - a. **Mobil:** Die Festplattenliste wird angezeigt. Manager können den Anwender mehreren Laufwerken hinzufügen, indem sie die Laufwerke von der Liste und dann **Autorisieren** auswählen.  
**Hinweis:** Wenn Sie mehrere Laufwerke ausgewählt haben, wird ein weitere Popup mit der Anzahl der ausgewählten Laufwerke angezeigt. Wählen Sie **Autorisieren** aus, damit der Anwender für den Zugriff auf diese Laufwerke autorisiert wird.
  - b. **Desktop:** Klicken Sie auf ein Laufwerk und dann auf das **Manager-ID-Symbol**. Klicken Sie am Ende der **Kartenansicht** auf das **+** Symbol, damit die Liste der autorisierten Anwender angezeigt wird. Klicken Sie auf den Anwender, wählen Sie seine **Rolle** aus und klicken Sie auf **Hinzufügen**. Der Anwender sollte jetzt zum Fenster **Manager-Einstellungen** vom Laufwerk hinzugefügt worden sein.
3. Der **Manager** kann das Laufwerk jetzt zum entfernten **Anwender** schicken.

## Anwender erhält Laufwerk und fügt es hinzu

1. Der **Anwender** verbindet das Laufwerk mit dem Computer und öffnet die ArmorLock-App.

- a. **Mobil:** Wählen Sie **Festplatte hinzufügen** aus. Suchen Sie den **QR-Code** auf der Rückseite des Laufwerks und scannen Sie ihn mit Ihrem Smartphone.
  - b. **Desktop:** Klicken Sie in der **Listenansicht** auf die Schaltfläche **Festplatte hinzufügen**. Geben Sie den eindeutigen 8-stelligen **Kurzcode** ein, der sich auf der Rückseite des Laufwerks unter dem QR-Code befindet.
2. Das Laufwerk wird automatisch authentifiziert und zu Ihrer Liste der Laufwerke hinzugefügt.

## Autorisieren von Remote-Anwendern nach Verschicken des Laufwerks

Die Funktion zur Remote-Autorisierung ermöglicht es einem Manager, den Zugriff eines Anwenders auf das ArmorLock-Laufwerk ortsunabhängig zu autorisieren. Der Manager muss über einen Internetzugang verfügen, um diese Funktion nutzen zu können. Mit diesem Verfahren wird der Zugriff autorisiert, nachdem das Laufwerk verschickt wurde.

Diese Funktion beinhaltet die Verwendung der Remote-Anfrage-Autorisierungsdatei und lässt sich in drei Schritte unterteilen:

- **Anwender fordert Zugriff auf Laufwerk an** – Der Anwender fordert Zugriff auf das Laufwerk an, indem er die Remote-Anfrage-Datei erstellt und sendet.
- **Manager autorisiert Zugriff auf Laufwerk** – Der Manager erhält die Remote-Anfrage-Datei, autorisiert den Zugriff remote und sendet die Remote-Anfrage-Datei zurück.
- **Anwender erhält Autorisierung und greift auf Laufwerk zu** – Der Anwender erhält die Remote-Anfrage-Datei vom Manager zurück und erhält Zugriff auf das Laufwerk.

Diese Schritte werden in den folgenden Abschnitten ausführlicher beschrieben.

### Anwender sendet Anfrage auf Laufwerkszugriff

Wenn ein Anwender ein ArmorLock-Laufwerk ohne Zugriff erhält, muss der Anwender eine Anfrage für den Zugriff an einen Manager des Laufwerks mit einer Remote-Anfrage-Datei senden. In diesem Abschnitt wird beschrieben, wie Sie Zugriff auf ein ArmorLock-Laufwerk anfordern, indem Sie eine Remote-Anfrage-Autorisierungsdatei erstellen und senden.

#### Mobile-App

1. Laden Sie die ArmorLock-App herunter und öffnen Sie sie.
2. Fügen Sie das Laufwerk hinzu und scannen Sie den QR-Code.
3. Wählen Sie **Zugriffsanfrage** aus.
4. Wählen Sie **Remote-Anfrage** aus.
5. Optional können Sie einen Kommentar eingeben und Ihren Standort teilen. Wählen Sie **Senden** aus.
6. Wählen Sie aus, wie Sie die Remote-Anfrage-Datei senden möchten.
  - a. Um sie per Textnachricht zu senden, wählen Sie **Nachricht** aus.
  - b. Um sie per E-Mail zu senden, wählen Sie **Mail** aus.
7. Wenn Sie sie per Textnachricht senden, geben Sie die Telefonnummer des Managers ein oder wählen Sie den Manager in der Kontaktliste Ihres Smartphones aus. Wählen Sie **Senden** aus.
8. Wenn Sie sie per E-Mail senden, geben Sie die E-Mail-Adresse des Managers ein. Wählen Sie **Senden** aus.
9. Die Nachricht **Anfrage auf Zugriff ausstehend** wird für das Laufwerk angezeigt.

## Desktop-App

1. Laden Sie die ArmorLock-App herunter und öffnen Sie sie.
2. Fügen Sie in der ArmorLock-App das ArmorLock-Laufwerk hinzu und geben Sie den Kurzcode ein.
3. Klicken Sie auf **Zugriffsanfrage**.
4. Klicken Sie auf **Remote-Anfrage senden**.
5. Optional können Sie einen Kommentar eingeben und Ihren aktuellen Standort angeben.
6. Klicken Sie auf **In Dateien speichern...**, um die Remote-Anfrage-Datei zu erstellen und wählen Sie einen Dateispeicherort aus.
7. Öffnen Sie eine E-Mail-Anwendung und erstellen Sie eine neue E-Mail.
8. Geben Sie die E-Mail-Adresse des Managers, eine Betreffzeile und eine kurze Nachricht ein.
9. Fügen Sie die Remote-Anfrage-Datei bei, die Sie erstellt haben, und senden Sie die E-Mail.
10. Die Nachricht **Anfrage auf Zugriff ausstehend** wird für das Laufwerk angezeigt.

## Manager autorisiert Zugriff

In diesem Abschnitt wird beschrieben, wie ein Manager reagieren und eine Autorisierung für ein ArmorLock-Laufwerk remote gewähren kann.

### Mobile-App

1. Öffnen Sie die E-Mail vom Anwender und wählen Sie die beigefügte Remote-Anfrage-Datei aus. Die ArmorLock-App wird automatisch gestartet.
2. Wählen Sie die gewünschte Zugriffsstufe aus:
  - **Als Anwender genehmigen** – Autorisieren Sie den Anwender mit der Zugriffsstufe „Anwender“.
  - **Als Manager genehmigen** – Autorisieren Sie den Anwender mit der Zugriffsstufe „Manager“.
  - **Löschen und als Neu einrichten** – Löschen Sie das ArmorLock-Laufwerk mit Secure Erase und gewähren Sie den Zugriff als „Neuer Anwender“.
  - **Ablehnen** – Lehnen Sie den Zugriff des Anwenders auf das Laufwerk ab.
3. Wählen Sie aus, wie Sie die Remote-Anfrage-Antwortdatei senden möchten.
  - a. Um sie per Textnachricht zu senden, wählen Sie **Nachricht** aus.
  - b. Um sie per E-Mail zu senden, wählen Sie **Mail** aus.
4. Wenn Sie sie per Textnachricht senden, geben Sie die Telefonnummer des Anwenders ein oder wählen Sie den Anwender in der Kontaktliste Ihres Smartphones aus. Wählen Sie **Senden** aus.
5. Wenn Sie sie per E-Mail senden, geben Sie die E-Mail-Adresse des Anwenders ein. Wählen Sie **Senden** aus.
6. Sie werden zur Hauptseite des Laufwerks weitergeleitet.

### Desktop-App

1. Öffnen Sie die E-Mail vom Anwender und dann die beigefügte Remote-Anfrage-Datei. Die ArmorLock-App wird automatisch gestartet.
2. Wählen Sie die gewünschte Zugriffsstufe aus:
  - **Als Anwender genehmigen** – Autorisieren Sie den Anwender mit der Zugriffsstufe „Anwender“.

- **Als Manager genehmigen** – Autorisieren Sie den Anwender mit der Zugriffsstufe „Manager“.
  - **Löschen und als Neu einrichten** – Löschen Sie das ArmorLock-Laufwerk mit Secure Erase und gewähren Sie den Zugriff als „Neuer Anwender“.
  - **Ablehnen** – Lehnen Sie den Zugriff des Anwenders auf das Laufwerk ab.
3. Klicken Sie auf **In Dateien speichern...** und wählen Sie einen Dateispeicherort aus.
  4. Klicken Sie auf **Speichern**.
  5. Öffnen Sie eine E-Mail-Anwendung und erstellen Sie eine neue E-Mail.
  6. Geben Sie die E-Mail-Adresse des Anwenders, eine Betreffzeile und eine kurze Nachricht ein.
  7. Fügen Sie Remote-Anfrage-Antwortdatei bei, die Sie gespeichert haben, und senden Sie die E-Mail.

## Anwender erhält Autorisierung und Zugriff auf das Laufwerk

In diesem Abschnitt wird beschrieben, wie Sie die Remote-Anfrage-Autorisierungsdatei von einem Manager und Zugriff auf das Laufwerk erhalten.

**Anmerkung:** Sie müssen die beigefügte Remote-Anfrage-Datei auf dem Gerät öffnen, auf dem auch die ursprüngliche Remote-Anfrage-Datei erstellt wurde.

### Mobile-App

1. Schließen Sie das ArmorLock-Laufwerk an Ihren Computer an.
2. Öffnen Sie die Antwort-E-Mail oder -Textnachricht vom Manager.
3. Öffnen Sie die beigefügte Remote-Anfrage-Antwortdatei. Dadurch wird die ArmorLock-App gestartet.
4. Die ArmorLock-App erkennt das Laufwerk.
5. Eine Erfolgsmeldung für den Zugriff auf das Laufwerk wird angezeigt.

### Desktop-App

1. Schließen Sie das ArmorLock-Laufwerk an Ihren Computer an.
2. Öffnen Sie die Antwort-E-Mail vom Manager.
3. Öffnen Sie die beigefügte Remote-Anfrage-Antwortdatei. Dadurch wird die ArmorLock-App gestartet.
4. Die ArmorLock-App erkennt das Laufwerk.
5. Eine Erfolgsmeldung für den Zugriff auf das Laufwerk wird angezeigt.



## 4

## Weitere Informationen zu ArmorLock-Apps und -Laufwerken

Mit den ArmorLock Mobile- und Desktop-Apps können Sie ArmorLock-Festplatten entsperren und sperren, mehrere Anwender und Festplatten verwalten und den letzten bekannten Standort einer Festplatte nachverfolgen. Es folgen weitere Funktionen der ArmorLock-Apps und -Laufwerke.

### Festplattenanzeigen

Die LEDs am ArmorLock-Laufwerk zeigen an, ob das Laufwerk gesperrt oder entsperrt ist. Um die LEDs zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor.

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie das **Zahnrad-Symbol** des gewünschten Laufwerks am Hauptbildschirm aus.
3. Wählen Sie im Abschnitt **Einstellungen** die Schaltfläche für die Laufwerks-LEDs aus, um die LEDs zu aktivieren oder zu deaktivieren. Die LEDs sind standardmäßig aktiviert.

### Anwendungsversion

Führen Sie die nachfolgenden Schritte aus, um sich die Version der ArmorLock-App anzeigen zu lassen. Dieses Verfahren könnte erforderlich sein, wenn Sie den Support kontaktieren.

1. Öffnen Sie die ArmorLock-App.
2. Rufen Sie das **Hauptmenü** auf.
  - a. **Mobil:** Wählen Sie das **3-Punkte-Symbol** aus.
  - b. **Desktop:** Klicken Sie auf das **ArmorLock**-Menü oben im Fenster.
3. Wählen Sie **Über** aus.
4. Die **App-Version** wird in der Notation des folgenden Beispiels angezeigt: Version 1.0.0 (303).

### Anwender-Authentifizierung

Wenn diese Option aktiviert ist, verwendet die ArmorLock-Authentifizierung die Funktionen zur Anwenderauthentifizierung Ihres Smartphones oder Computers, um Ihre Berechtigung für die App zu bestätigen. Wenn der Manager eines Laufwerks die „Authentifizierung“ aktiviert hat, wird sie für alle Anwender des Laufwerks aktiviert. Wenn ein Anwender die Anwenderauthentifizierung bei seinem Smartphone oder Computer deaktiviert, kann er die Festplatte nicht über die App entsperren. Um diese Funktion zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor.

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie das **Zahnrad-Symbol** des gewünschten Laufwerks am Hauptbildschirm aus.
3. Verwenden Sie im Abschnitt **Manager-Einstellungen** den Schieberegler für die **Authentifizierung**, um die Anwenderauthentifizierung zu aktivieren oder zu deaktivieren.

## Standortverfolgung

Diese optionale Funktion zeigt den letzten bekannten Standort an, an dem das Laufwerk verwendet wurde, und fügt einen Kartenstandort hinzu. Um diese Funktion zu aktivieren oder zu deaktivieren, gehen Sie wie folgt vor.

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie ein Laufwerk aus und öffnen Sie die **Manager-Einstellungen**.
  - a. **Mobil:** Wählen Sie das **Zahnrad-Symbol** und dann **Standortverfolgung** aus.
  - b. **Desktop:** Klicken Sie auf ein Laufwerk und dann auf das **Zahnrad-Symbol**. Klicken Sie auf **Standortverfolgung**.
3. Um den Standort des Laufwerks anzuzeigen, wählen Sie das Laufwerk aus.
  - a. **Mobil:** Wählen Sie die Schaltfläche **Letzter bekannter Ort** aus.
  - b. **Desktop:** Klicken Sie auf das **Kartenstecknadel-Symbol**.

## Festplatteninfos

Mit dieser Funktion werden Seriennummer, Firmwareversion und weitere Informationen angezeigt, die erforderlich sein können, wenn Sie den Technischen Support kontaktieren.

1. Öffnen Sie die ArmorLock-App.
  - a. **Mobil:** Wählen Sie das **Zahnrad-Symbol** und dann **Festplatteninfos** in den Einstellungen aus.
  - b. **Desktop:** Klicken Sie auf ein Laufwerk und dann auf das **i-Symbol**.
2. Die Festplatteninfos und verfügbaren Open-Source-Lizenzen werden angezeigt.

## Verwendung des Wiederherstellungsschlüssels

Die folgenden Schritte beschreiben den Wiederherstellungsvorgang, um ein zuvor autorisiertes Laufwerk zur ArmorLock-App hinzuzufügen. Es stehen zwei Methoden (Mobil oder Desktop) zur Wahl. Durch diesen Prozess bleiben die bestehenden Daten auf dem Laufwerk erhalten, aber der Zugriff aller anderen Anwender, einschließlich autorisierter Anwender, wird entfernt. Die gewünschten Anwender müssen neu autorisiert werden.

1. **Mobil:** Sie können Ihr Mobilgerät verwenden, um ein Laufwerk wiederherzustellen.
  - a. Schließen Sie das ArmorLock-Laufwerk an Ihren Computer an.
  - b. Scannen Sie den **QR-Wiederherstellungscodes**, der bei der Ersteinrichtung gespeichert wurde.
  - c. Wenn der Wiederherstellungsprozess abgeschlossen ist, wird das Fenster „Setup erfolgreich“ angezeigt. Wählen Sie **Schließen** aus.
2. **Desktop:** Sie können ein Laufwerk auch über einen macOS-Computer wiederherstellen.
  - a. Schließen Sie das ArmorLock-Laufwerk an Ihren Computer an.
  - b. Klicken Sie auf **Festplatte hinzufügen**.
  - c. Geben Sie den 8-stelligen **Kurzcode** ein, der sich auf der Rückseite der Festplatte befindet.
  - d. Klicken Sie auf **Schlüssel verwenden**.
  - e. Geben Sie den 64-stelligen **Wiederherstellungscodes** ein.
  - f. Wenn der Wiederherstellungsprozess abgeschlossen ist, wird das Fenster „Setup erfolgreich“ angezeigt. Klicken Sie auf **Schließen**.

## Wiederherstellung der Kopplung bei neuen Geräten

Wenn autorisierte Anwender ein neues Smartphone oder einen neuen Laptop haben, müssen sie den ArmorLock-Zugriff auf das Laufwerk wiederherstellen. Folgende Schritte beschreiben, wie Sie mit dem Wiederherstellungsschlüssel die Kopplung mit einem neuen Mobilgerät oder Desktopsystem wiederherstellen.

### Kopplung wiederherstellen (Mobil)

1. Schließen Sie das ArmorLock-Laufwerk an Ihren Computer an.
2. Wählen Sie **Kopplung wiederherstellen** aus.
3. Wählen Sie **Schlüssel verwenden** aus.
4. Scannen oder geben Sie den 64-stelligen QR-Wiederherstellungscode ein.
5. Wenn der Wiederherstellungsprozess abgeschlossen ist, wird das Fenster „Setup erfolgreich“ angezeigt.
6. Wählen Sie **Schließen** aus.

### Kopplung wiederherstellen (Desktop)

1. Schließen Sie das ArmorLock-Laufwerk an Ihren Computer an.
2. Klicken Sie auf **Kopplung wiederherstellen**.
3. Klicken Sie auf **Schlüssel verwenden**.
4. Geben Sie den 64-stelligen Wiederherstellungscode ein.
5. Nachdem die Wiederherstellung abgeschlossen ist, werden die Rollen von Anwendern und Managern wiederhergestellt.

## Manager-Einstellungen

Der Manager eines Laufwerks hat Zugriff auf einige managerspezifische Einstellungen. Wählen Sie das **Zahnrad-Symbol** in der Kartenansicht aus, damit die vollständige Liste der Manager-Einstellungen angezeigt wird, die auf ein ArmorLock-Laufwerk in der Nähe Ihres Geräts angewendet werden können.

### Hinzufügen und Entfernen von Anwendern bei einem Laufwerk

Mit der ArmorLock-App kann gesteuert werden, welche Anwender über autorisierten Zugriff auf ein bestimmtes ArmorLock-Laufwerk verfügen.

#### Hinzufügen eines Anwenders

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie ein Laufwerk aus, öffnen Sie die **Manager-Einstellungen** und Sie können den Anwender **hinzufügen**.
  - a. **Mobil:** Wählen Sie das **Zahnrad-Symbol** und dann **Manager-Einstellungen** aus. Wählen Sie **Autorisierte Anwender** und dann das **+** Symbol aus, um einen Anwender zu autorisieren. Wählen Sie den Anwender aus und klicken Sie auf **Autorisieren**. Der Anwender sollte jetzt zur Liste der autorisierten Anwender hinzugefügt worden sein.
  - b. **Desktop:** Klicken Sie auf ein Laufwerk und dann auf das **Manager-ID-Symbol**. Klicken Sie am Ende der **Kartenansicht** auf das **+** Symbol, damit die Liste der autorisierten Anwender angezeigt wird. Klicken Sie auf den Anwender, wählen Sie seine/ihre **Rolle** aus, und klicken Sie auf **Hinzufügen**. Der Anwender sollte jetzt zum Fenster **Manager-Einstellungen** vom Laufwerk hinzugefügt worden sein.
3. Sie können jetzt die **Rolle** bearbeiten und auch jederzeit einen autorisierten Anwender entfernen.

#### Entfernen eines Anwenders

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie ein Laufwerk aus und öffnen Sie die **Manager-Einstellungen**.
  - a. **Mobil:** Wählen Sie das **Zahnrad-Symbol** und dann **Manager-Einstellungen** aus. Wählen Sie **Autorisierte Anwender** und dann den **Anwendernamen** aus, den Sie entfernen möchten. Wählen Sie die Schaltfläche **Anwender entfernen** aus.
  - b. **Desktop:** Klicken Sie auf eine Festplatte und dann auf das **Manager-ID-Symbol**. Wählen Sie den Namen des Anwenders aus, der entfernt werden soll. Klicken Sie am Ende der Kartenansicht auf das **- Symbol**, um den Anwender zu entfernen.

## Anwendername

Über den Anwendernamen kann der Name geändert werden, der in Verbindung mit dem ArmorLock-Laufwerk für das Smartphone angezeigt wird. Dadurch ändert sich nicht der Name des Smartphones.

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie eine Festplatte aus.
  - a. **Mobil:** Zum Bearbeiten wählen Sie das **Dreipunkte**-Symbol und dann **App-Einstellungen** aus. Wählen Sie den **Anwendernamen** aus, der geändert werden soll, und tippen Sie auf **Änderungen speichern**.
  - b. **Desktop:** Klicken Sie auf das **ArmorLock**-Menü und dann auf „Einstellungen“. Klicken Sie auf den Anwendernamen, der geändert werden soll, und dann auf **OK**, um die Änderungen zu speichern.
3. Der **ArmorLock**-Anwendername wurde jetzt geändert.

## Neuer Wiederherstellungsschlüssel

Die Option „Neuer Schlüssel“ ermöglicht es Managern des Laufwerks, einen neuen Wiederherstellungsschlüssel zu generieren, wenn sie den Verdacht haben, dass der bestehende Schlüssel nicht mehr geheim ist. Wenn diese Funktion verwendet wird, wird der vorherige Wiederherstellungsschlüssel ungültig. Führen Sie die folgenden Schritte aus, um einen neuen Wiederherstellungsschlüssel zu erstellen.

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie ein Laufwerk aus und öffnen Sie die **Manager-Einstellungen**.
  - a. **Mobil:** Wählen Sie das **Zahnrad-Symbol** und dann **Manager-Einstellungen** aus. Wählen Sie **Neuer Schlüssel** aus. Wählen Sie **Generieren** aus, um fortzufahren.
  - b. **Desktop:** Klicken Sie auf eine Festplatte und dann auf das **Schlüssel**-Symbol. Klicken Sie auf **Neu generieren**.
3. Denken Sie daran, den neuen Wiederherstellungsschlüssel zu **sichern**.
  - a. **Hinweis:** Der alte Wiederherstellungsschlüssel wird dadurch ungültig.

## Schreibgeschützter Modus

Das ArmorLock-Laufwerk kann in den schreibgeschützten Modus versetzt werden. Dadurch können Anwender keine Dateien bearbeiten oder löschen. Bitte beachten Sie, dass diese Funktion verzögert aktiviert wird; sie wird nach dem nächsten Entsperren angewandt.

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie ein Laufwerk aus und öffnen Sie die **Manager-Einstellungen**.
  - a. **Mobil:** Wählen Sie das **Zahnrad-Symbol** und dann **Manager-Einstellungen** aus. Anschließend wählen Sie **Schreibgeschützt** aus.
  - b. **Desktop:** Klicken Sie auf das Zahnrad-Symbol des **Laufwerks** und dann in den **Manager-Einstellungen** auf **Schreibgeschützt**.
3. Änderungen an der Einstellung **Schreibgeschützt** werden beim nächsten Entsperren des Laufwerks angewandt.

## Aktualisierungen einschränken

Diese Einstellung ist standardmäßig auf **Aus** eingestellt. Es wird empfohlen, diese Einstellung für zukünftige Aktualisierungen deaktiviert zu lassen.

## Zurück auf Werkseinstellungen

Das ArmorLock-Laufwerk kann auf die Werkseinstellungen zurückgesetzt werden. Dadurch werden alle Daten, Einstellungen, Autorisierungen, Anwender-IDs und Wiederherstellungsschlüssel gelöscht.

1. Öffnen Sie die ArmorLock-App.
2. Wählen Sie ein Laufwerk aus und öffnen Sie die **Manager-Einstellungen**.
  - a. **Mobil:** Wählen Sie das **Zahnrad-Symbol** und dann **Manager-Einstellungen** aus. Anschließend wählen Sie **Zurück auf Werkseinstellungen** aus. Wählen Sie **Zurücksetzen** aus, um fortzufahren.
  - b. **Desktop:** Klicken Sie auf das Zahnrad-Symbol des **Laufwerks** und dann in den **Manager-Einstellungen** auf **Zurück auf Werkseinstellungen**. Klicken Sie auf **Zurück auf Werkseinstellungen**, um fortzufahren.
3. Alle Daten, Einstellungen, Autorisierungen, Anwender-IDs und der Wiederherstellungsschlüssel werden dauerhaft gelöscht.

## Aktualisieren des ArmorLock-Laufwerks

### Firmwareaktualisierungen: Mobile-App unter iOS

Anwendern wird empfohlen, die aktuellste Version der ArmorLock-Firmware zu verwenden. Nach dem Verbinden des Laufwerks wird eine Benachrichtigung angezeigt, wenn eine Aktualisierung verfügbar ist.

1. Die Benachrichtigung „Aktualisierung verfügbar“ wird angezeigt.
  - a. **Hinweis:** Wenn Sie eine veraltete App-Version verwenden, wird die Meldung „Firmwareaktualisierung erforderlich“ angezeigt.
2. Wählen Sie die Benachrichtigung aus, um die ArmorLock-App zu öffnen.
3. Wählen Sie die Schaltfläche **Tippen, um Aktualisierung durchzuführen** aus.
4. Lassen Sie das Laufwerk vom Computer auswerfen.
5. Die Benachrichtigung „Aktualisierung abgeschlossen“ wird angezeigt.

### Firmwareaktualisierungen: Desktop-App unter macOS

Es kann konfiguriert werden, dass die ArmorLock-Firmware automatisch aktualisiert werden soll. Wenn die automatischen Aktualisierungen nicht aktiviert sind, führen Sie die folgenden Schritte aus, um die aktuellste Version zu installieren.

1. Schließen Sie das ArmorLock-Laufwerk an den Computer an.
2. Öffnen Sie die ArmorLock-App.
3. Wenn eine Aktualisierung verfügbar ist, wird die Meldung „Firmware-Update verfügbar“ unter dem Sperren-/Entsperren-Symbol angezeigt.
  - a. **Hinweis:** Wenn Sie eine veraltete App-Version verwenden, wird die Meldung „Firmwareaktualisierung erforderlich“ angezeigt.
4. Klicken Sie auf **Firmware jetzt aktualisieren**.
5. Lassen Sie das Laufwerk auswerfen und führen Sie einen Neustart durch.
6. Die Meldung „Firmwareaktualisierung abgeschlossen“ wird angezeigt.

## Konformitäts- und Garantieinformationen

### Einhaltung gesetzlicher Bestimmungen

#### Konformität mit Sicherheitsanforderungen

Zugelassen für die USA und Kanada. 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.

#### Informationen zu FCC Klasse B

HINWEIS: Dieses Gerät wurde mit dem Ergebnis getestet, dass die Grenzwerte für digitale Geräte der Klasse B nach Abschnitt 15 der FCC-Vorschriften eingehalten werden. Diese Grenzwerte sind so bemessen, dass sie in einem Wohngebiet angemessenen Schutz vor schädlichen Störungen bieten. Dieses Gerät erzeugt, nutzt und emittiert unter Umständen hochfrequente Energie und kann bei nicht anleitungsgemäßer Installation und Verwendung schädliche Störungen der Radiokommunikation verursachen. Es gibt jedoch keine Garantie, dass in einer gegebenen Installation keine Störungen auftreten. Ob das Gerät eine Störung des Radio- oder Fernsehempfangs verursacht, kann durch Aus- und Einschalten des Geräts bestimmt werden. Um diese Störung zu beheben, wird dem Anwender empfohlen, einen oder mehrere der folgenden Schritte durchzuführen:

- Richten Sie die Empfangsantenne neu aus oder platzieren Sie sie an einen anderen Ort.
- Erhöhen Sie den Abstand zwischen Gerät und Empfänger.
- Schließen Sie das Gerät an eine Steckdose an, die einen anderen Stromkreis verwendet als die des Empfängers.
- Bitten Sie den Händler oder einen qualifizierten Rundfunk-/Fernsehtechniker um Hilfe.

Änderungen, die nicht ausdrücklich vom Hersteller genehmigt wurden, können zum Verlust der Betriebszulassung für das Gerät führen.

Die Strahlungsquelle darf nicht mit einer anderen Antenne oder einem anderen Sender zusammen aufgestellt oder in Verbindung damit betrieben werden.

#### Erklärung zur Strahlenbelastung:

Dieses Gerät erfüllt die FCC-Grenzwerte für die Strahlenbelastung in einer nicht kontrollierten Umgebung. Dieses Gerät sollte so installiert und betrieben werden, dass ein Mindestabstand von 20 cm zwischen dem Gerät und Ihrem Körper gewährleistet ist.



## 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) Konformitätserklärung

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

Dieses Gerät erfüllt die Bestimmungen der kanadischen ICES-003 Klasse B.

## CE-Konformität für Europa

Die CE-Kennzeichnung zeigt an, dass dieses System die anwendbaren Richtlinien der Europäischen Union erfüllt, einschließlich der Niederspannungsrichtlinie 2014/35/EU, der Funkanlagenrichtlinie (2014/53/EU) und der RoHS-Richtlinie (2011/65/EU) in der abgeänderten Fassung gemäß 2015/863/EU. Betriebsmerkmale der Funkverwendung: (a) Frequenzband: 2.412-2.472 MHz (b) Maximale Leistung der Funkfrequenz, die auf den Bändern übertragen wird, beträgt 8 dBm. Eine Konformitätserklärung gemäß den anwendbaren Richtlinien wurde abgegeben und kann bei Western Digital Europe eingesehen werden.

## KC-Hinweis (Nur Republik Korea)

기종별	사용자 안내문
B 급기기 (가정용방송통신기자재)	이기기는가정용(B 급) 전자파적합기기로서주로 가정에서사용하는것을목적으로하며, 모든지역에서사용할수있습니다

Gerät der Klasse B. Bitte beachten Sie, dass dieses Gerät für nicht geschäftliche Zwecke zugelassen wurde und in jeder Umgebung, einschließlich Wohngebieten, verwendet werden kann.

Koreanische KCC-Zertifizierungsnr: R-R-WDT-J1C

## VCCI-Erklärung

Das VCCI-Logo auf dem Produkt bedeutet, dass das Produkt den EMI-Regeln in Japan entspricht.

## NCC-Erklärung (Taiwan)

取得審驗證明之低功率射頻器材，非經核准，公司、商號或使用者均不得擅自變更頻率、加大功率或變更原設計之特性及功能。

低功率射頻器材之使用不得影響飛航安全及干擾合法通信；經發現有干擾現象時，應立即停用，並改善至無干擾時方得繼續使用。前述合法通信，指依電信管理法規定作業之無線電通信。低功率射頻器材須忍受合法通信或工業、科學及醫療用電波輻射性電機設備之干擾。

## RoHS (Taiwan)

設備名稱：硬式磁碟機 型號 ( 型式 )：SanDisk Professional series

單元	限用物質及其化學符號					
	鉛 (Pb)	汞 (Hg)	鎘 (Cd)	六價鉻 (Cr (VI))	多溴聯苯 (PBB)	多溴二苯醚 (PBDE)
機箱外皮殼與鏡片	○	○	○	○	○	○
塑料其它部件	○	○	○	○	○	○
橡皮腳墊, 4 片	○	○	○	○	○	○
片金屬部件	-	○	○	○	○	○
固態硬碟/硬碟/電路板組合	-	○	○	○	○	○
組合電纜線/電源	-	○	○	○	○	○

備考1. "超出0.1 wt %" 及 "超出0.01 wt %" 係指限用物質之百分比含量超出百分比含量基準  
備考2. "○" 係指該項限用物質之百分比含量未超出百分比含量基準值  
備考3. "-" 係指該項限用物質為排除項目。

## Garantiefinformationen

Wenn Sie eine G-Technology® ArmorLock™ NVMe SSD, Modellnummer OG10484-1, erworben haben, verwenden Sie bitte den folgenden Link für Ihre Bedienungsanleitung mit Garantiefinformationen: [https://support-en.g-technology.com/app/answers/detail/a\\_id/29803](https://support-en.g-technology.com/app/answers/detail/a_id/29803).

## Garantie für SanDisk Einzelhandelsprodukte (alle Regionen außer Australien)

Für dieses SanDisk Professional Produkt gilt eine 5-jährige Garantie ab dem Kaufdatum. Sie unterliegt den geltenden Geschäftsbedingungen der Garantie, die unter <http://www.sandisk.com/wug> definiert sind.

## Einen Garantieanspruch geltend machen

Öffnen Sie die Seite [www.sandisk.com](http://www.sandisk.com) und wählen Sie „Support“, um weitere Informationen zur Geltendmachung eines Garantieanspruchs zu erhalten (SanDisk Support-Seite).

Wenn festgestellt wird, dass Ihr Produkt defekt sein könnte, erhalten Sie eine RMA-Nummer (Berechtigung zur Warenrücksendung) sowie Anweisungen zur Rücksendung des Produkts. Für Ausgaben in Verbindung mit einer Forderung aus einer SanDisk Garantie sind Sie verantwortlich.

Sie müssen Ihr Produkt in einem sicheren, vorab bezahlten Paket an die Adresse versenden, die Sie zusammen mit der RMA-Nummer erhalten. Für alle Garantieforderungen ist ein Kaufbeleg erforderlich.

## Garantie für SanDisk Einzelhandelsprodukte (Australien)

SanDisk garantiert dem Endanwender, dass dieses Produkt, mit Ausnahme von Software oder Inhalten, die mit oder auf dem Produkt bereitgestellt werden, frei von Material- und Verarbeitungsfehlern ist, den veröffentlichten Produktspezifikationen von SanDisk entspricht und ab Kaufdatum 5 Jahre lang normal genutzt werden kann, sofern das Produkt legal verkauft wurde.

Wenn diese Garantie geltend gemacht wird, kann SanDisk entscheiden, ob das Produkt repariert wird oder Sie ein entsprechendes Produkt erhalten. Sollte das Produkt nicht repariert oder ersetzt werden können, erhalten Sie den Kaufpreis zurück. Die vollständigen Bedingungen der Garantie und Garantiedauer von SanDisk finden Sie hier: [www.sandisk.com/wug](http://www.sandisk.com/wug).

Kontaktdaten des Garantiegebers:

Hamilton House, Regent Park, Kingston Road Leatherhead, Surrey, KT22 7PL, UK Tel: 0808-234-9816 (gebührenfrei für Ortsgespräche aus UK) oder (44) 203-3183-965 (UK)

So machen Sie einen Garantieanspruch geltend:

Bevor Sie das Produkt zurückgeben, brauchen Sie eine RMA-Nummer (Return Material Authorization). Sie haben folgende Möglichkeiten:

1. Kontaktieren Sie SanDisk unter 1 800 262 504 (Mo.–Fr. | 9:00 Uhr – 18:00 Uhr New South Wales Time) oder senden Sie eine E-Mail an SanDisk ([support@SanDisk.com](mailto:support@SanDisk.com)) mit einem Kaufbeleg (inkl. Kaufdatum, Einkaufsort und Verkäufername) sowie Produktname, -typ und -nummer; oder
2. Kontaktieren Sie den Verkäufer, von dem Sie das Produkt ursprünglich erworben haben.

Besuchen Sie [www.sandisk.com/support](http://www.sandisk.com/support), um weitere Informationen zur Geltendmachung eines Garantieanspruchs zu erhalten (SanDisk Support-Seite). Wenn festgestellt wird, dass Ihr Produkt defekt sein könnte, erhalten Sie eine RMA-Nummer sowie Anweisungen zur Rückgabe des Produkts. Für Ausgaben in Verbindung mit einer Forderung aus einer SanDisk Garantie sind Sie verantwortlich. Sie müssen Ihr Produkt in einem sicheren, vorab bezahlten Paket an die Adresse versenden, die Sie zusammen mit der RMA-Nummer erhalten. Für alle Garantieforderungen ist ein Kaufbeleg erforderlich.

## Nur für Verbraucher in Australien:

Trotz der Bedingungen dieser Garantie gelten für SanDisk Produkte Garantien, die gemäß Australian Consumer Law nicht ausgeschlossen werden können. Bei einem

wesentlichen Mangel haben Sie einen Anspruch auf Ersatz oder Erstattung. Bei jedem anderen realistisch vorhersehbaren Verlust oder Schaden haben Sie Anspruch auf Entschädigung. Zudem haben Sie einen Anspruch auf Reparatur oder Ersatz der Produkte, wenn die Produkte keine akzeptable Qualität aufweisen und es sich beim Mangel um keinen wesentlichen Mangel handelt.

## **Handhabung eines ArmorLock-Laufwerks**

SanDisk Professional Produkte sind Präzisionsgeräte, die mit Vorsicht ausgepackt und installiert werden müssen. Festplatten können durch grobe Handhabung, Stöße oder Vibrationen beschädigt werden. Befolgen Sie beim Auspacken und Installieren Ihres externen Speicherprodukts immer die folgenden Vorsichtsmaßnahmen:

- Das robuste ArmorLock-Laufwerk ist so konzipiert, dass es einem Fall aus einer Höhe von bis zu drei Metern (3 m, auf Betonboden mit Teppich) und einem Druck von bis zu 450 kg standhält. Setzen Sie das Laufwerk keinen Fallhöhen und keinen Drücken aus, bei denen diese Werte überschritten werden.
- Es wird empfohlen, mit dem Laufwerk immer so vorsichtig wie möglich umzugehen.

## Glossar

Viele der Begriffe, die in dieser Bedienungsanleitung verwendet werden, sind in diesem Abschnitt definiert.

### **Autorisierter Anwender**

Ein Anwender, der ein ArmorLock-Laufwerk entsperren oder darauf zugreifen kann.

### **Dateisystem**

Entscheidet darüber, wie Daten gespeichert und abgerufen werden. Gängige Typen:

- macOS (HFS+): Kompatibel mit Time Machine
- Windows (NTFS): Standardmäßiges Windows-Dateisystem
- Windows und macOS (exFAT): Flexibel für beide Betriebssysteme

### **Manager**

Eine der beiden Rollen zur Verwendung des ArmorLock-Laufwerks. Der Manager kann das Laufwerk entsperren, das Laufwerk löschen/formatieren, zusätzliche Geräte autorisieren/deautorisieren und bestimmte Parameter konfigurieren (schreibgeschützt usw.). Es muss mindestens einen Manager pro Laufwerk geben, aber es können auch weitere Manager hinzugefügt werden.

### **QR-Code**

Ein „Quick-Response“-Matrix-Barcode für unmittelbaren Zugriff auf die Informationen im Code. Der ArmorLock-QR-Code befindet sich auf der Rückseite des Laufwerks und wird mit der App verwendet.

### **USB**

Universal Serial Bus (USB) ist ein Industriestandard zum Verbinden von Computern und Peripheriegeräten. Das ArmorLock-Laufwerk besitzt einen USB-C-Anschluss. Ein USB-A- und ein USB-C-Kabel sind im Lieferumfang enthalten, um das Laufwerk an einen Computer anschließen zu können.

### **Anwender**

Ein Smartphone oder Computer mit Autorisierung und der Fähigkeit, das Laufwerk zu entsperren. Diese Rolle kann auch das Laufwerk löschen oder formatieren (außer der Manager hat diese Option deaktiviert). Die Anwenderrolle ist nicht erforderlich, um das Gerät zu verwenden.

## **Anwender-ID**

Informationen, die den Anwender identifizieren, z. B. Anwenderschlüssel und Anwendername.

## **Anwenderschlüssel**

Ein (öffentlicher) Schlüssel, der von der App generiert und einem Anwender zugewiesen wird. Wenn die App gelöscht und neu installiert wird, wird ein neuer Schlüssel erstellt und das Gerät muss neu gekoppelt werden.

## **Anwendername**

Der „einfache“ Name des Anwenders. Diese Informationen werden auf dem Laufwerk gespeichert, können aber vom Manager geändert werden.

# Index

## A

Aktualisierung, Firmware [25](#)  
Aktualisierungen einschränken [25](#)  
Anwender [32](#)  
Anwender-ID [33](#)  
Anwendername [24](#), [33](#)  
Anwenderschlüssel [33](#)  
Anwendungsversion [20](#)  
App-Kompatibilität [2](#)  
Australien/Neuseeland [30](#)  
Automatisch entsperren [13](#)  
Automatische Firmwareaktualisierung [25](#)  
Automatisches Entsperren Desktop-App [14](#)  
Automatisches Entsperren Mobile-App [13](#)  
Autorisieren von Anwendern [23](#)  
Autorisierter Anwender [32](#)

## B

Beschreibung der Komponenten [3](#)  
Bluetooth Kompatibilität [3](#)

## D

Dienst [29](#)

## E

Einhaltung gesetzlicher Bestimmungen [27](#)  
Entsperren [13](#)

## F

Firmware, automatische Aktualisierung [25](#)

## G

Garantieinformationen [29](#)  
Gerät entfernen [14](#)  
Glossar [32](#)

## H

Hardware [2](#)

## I

IC Statement [28](#)  
ICES-3(B)/NMB-3(B) Konformität [28](#)  
Informationen zu FCC Klasse B [27](#)

## K

KC-Hinweis [28](#)  
Konformität mit Sicherheitsanforderungen [27](#)

Konformität, Zulassungen [27](#)

## L

Laufwerk  
Verwendungshinweise [31](#)  
LEDs – aktivieren oder deaktivieren [20](#)  
Lieferumfang [2](#)

## N

NCC-Erklärung [29](#)  
Neuer Wiederherstellungsschlüssel [24](#)

## P

Packungsinhalt [2](#)

## R

Remote-Autorisierung  
Anwender erhält Autorisierung [19](#)  
Anwender fordert Zugriff an [17](#)  
Manager autorisiert Zugriff [18](#)  
RoHS-Erklärung (Taiwan) [29](#)

## S

Sperren [13](#)  
Standortverfolgung [21](#)

## T

Technische Hinweise [2](#)

## V

VCCI-Erklärung [29](#)  
Vorsichtsmaßnahmen beim Umgang mit dem Gerät [31](#)

## W

WD  
Service, Inanspruchnahme [29](#)

## Z

Zugriff remote anfordern [17](#)  
Zurück auf Werkseinstellungen [25](#)

Diese Informationen wurden von Western Digital gewissenhaft und unter Annahme ihrer Richtigkeit erstellt. Western Digital übernimmt jedoch keine Haftung für deren Verwendung oder für die Verletzung von Patenten oder Rechten Dritter, die aus der Verwendung entstehen können. Es wird keine implizite oder anderweitige Lizenz für Patente oder Patentrechte von Western Digital erteilt. Western Digital, das Logo von Western Digital, SanDisk, SanDisk Professional, ArmorLock und G-DRIVE sind eingetragene Marken oder Marken der Western Digital Corporation oder ihrer Tochterunternehmen in den USA und/oder anderen Ländern. Android ist eine Marke oder eingetragene Marke von Google LLC in den USA und/oder anderen Ländern. macOS ist eine Marke von Apple Inc., eingetragen in den USA und anderen Ländern. Windows ist eine eingetragene Marke oder Marke der Microsoft Corporation in den USA und/oder anderen Ländern. iOS ist eine Marke oder eingetragene Marke von Cisco in den USA und anderen Ländern und wird von Apple Inc. unter Lizenz verwendet. USB-C ist eine Marke des USB Implementers Forum. Die Bluetooth Wortmarke und die Logos sind eingetragene Marken von Bluetooth SIG, Inc. und jegliche Verwendung solcher Marken durch Western Digital erfolgt unter Lizenz. Alle anderen Marken sind Eigentum ihrer jeweiligen Inhaber. Die gezeigten Bilder können vom tatsächlichen Produkt abweichen. Änderungen der technischen Produktdaten ohne Vorankündigung vorbehalten. \*Bei der Angabe der Speicherkapazität gilt: 1 GB = 1 Milliarde Bytes und 1 TB = 1 Billion Bytes. Abhängig von der Betriebsumgebung kann die tatsächlich nutzbare Kapazität abweichen. \*\*Bei der Angabe von Übertragungsraten gilt: 1 Megabyte pro Sekunde (MB/s) = 1 Million Bytes pro Sekunde. Basierend auf internen Tests; die Leistung kann je nach Hostgerät, Nutzungsbedingungen, Laufwerkskapazität und anderen Faktoren variieren. \*\*\*Auf einem Betonboden mit Teppich.

© 2022 Western Digital Corporation und Tochterunternehmen. Alle Rechte vorbehalten.

Western Digital  
5601 Great Oaks Parkway  
San Jose, Kalifornien 95119 USA

D015-000043-AE03