User Guide

DL GO Encrypted USB Flash Drive

Contents

DataLocker® DL GO User Guide

1. Intro

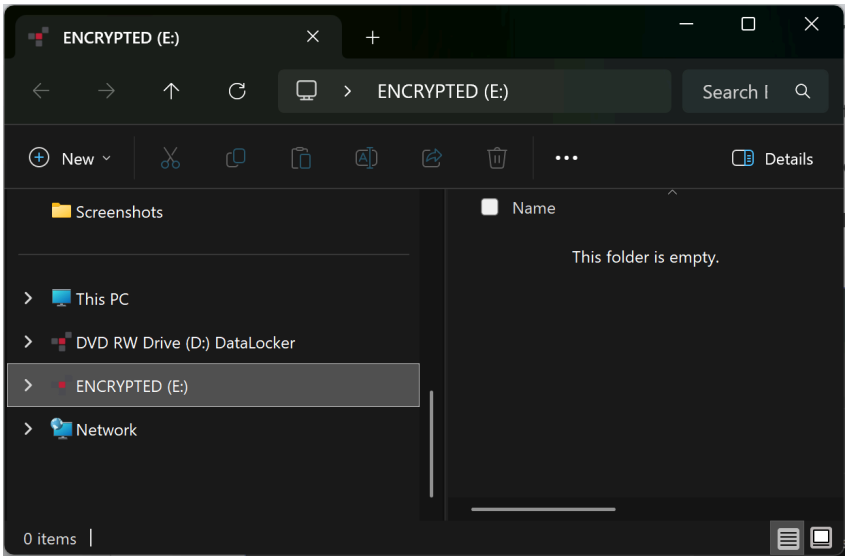
Welcome to the DataLocker DL GO, the simple way to protect your data.

What DL GO does

The drive provides hardware-based, always-on encryption of stored files. Files written to the **ENCRYPTED** storage drive are protected automatically—no extra steps are required.

When you connect your DL GO, two volumes appear in turn:

1. **DataLocker** — First, a read-only launcher that shows as a DVD RW drive (virtual read-only). It contains the DataLocker app you run to unlock your device.
2. **ENCRYPTED** — After you unlock the device the ENCRYPTED secure storage drive becomes available. This is where you store your data.



Volume letters may differ.

How DL GO locks

The DL GO locks when you unplug it, click the Lock button in the Control Panel (shortcut Ctrl+L), or fully power off the host. **Note** that it remains unlocked during computer sleep or after a user logs out. We also recommend you turn on auto-lock in Settings after setup.

Password protection and recommended recovery

There are **10 password attempts**. After 10 failures, the device performs a **cryptographic reset** that permanently erases data, referred to as **brute-force protection**. To avoid data loss, set up **biometric unlock** on your computer and/or the recommended **Password Recovery** with MySafeConsole/SafeConsole.

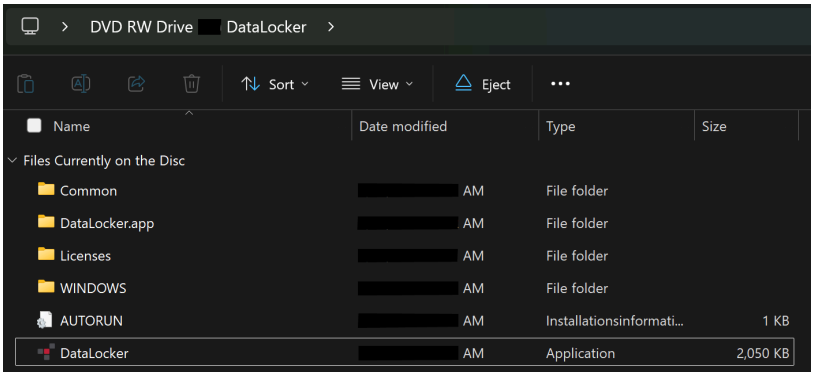
Register with MySafeConsole/SafeConsole to add Password Recovery, but also Remote Lock/Reset, basic usage tracking, and automatic security updates. You can connect during setup or later from the Manage tab.

Rugged by design
DL GO is IP68 dustproof and waterproof. The heavy-duty metal shell and epoxy-sealed internals add extra protection. Always ensure the USB connector is clean and completely dry before plugging it in.

2. Setup: Connect, Launch, Configure

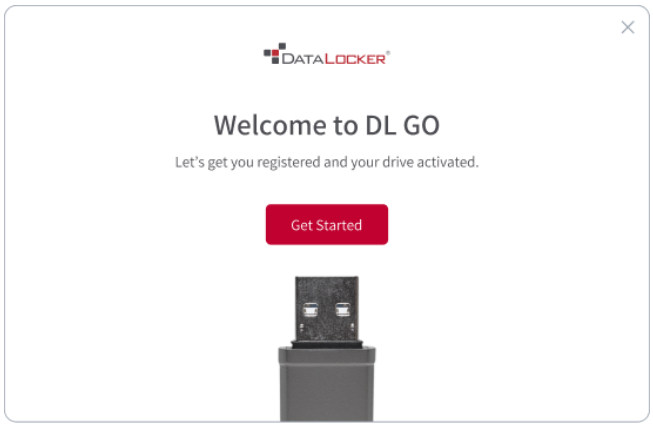
Follow these steps to set up your DL GO for the first time.

1. **Setup: Connect Your Device**
   Plug the DL GO into a USB port on your computer.
2. **Setup: Launch the Application**
   A drive named DataLocker (DVD RW drive virtual read-only) will appear. Open it and run the DataLocker application to begin.
   - **Windows:** Open **File Explorer** and click **DataLocker** under This PC > Devices and Drives. Double-click DataLocker.exe.
   - **macOS:** Open **Finder** and click **DataLocker** under Locations. Double-click the DataLocker application.



The DataLocker application is used to set up and unlock your device.

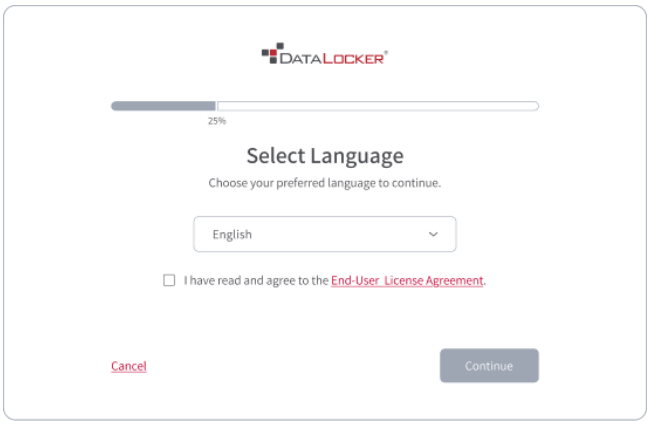
3. **Setup: Get Started**
    - A **Welcome to DL GO** screen will appear. Click **Get Started**.



Screenshot of DataLocker.exe running,
also referred to as the DataLocker Control Panel

4. **Setup: Language and License Agreement**

- Choose your preferred language. The application is available in: English, French, Spanish, German, Japanese, Korean, Traditional Chinese, and Simplified Chinese.
- You must check the box to agree to the End-User License Agreement before you can click **Continue**.

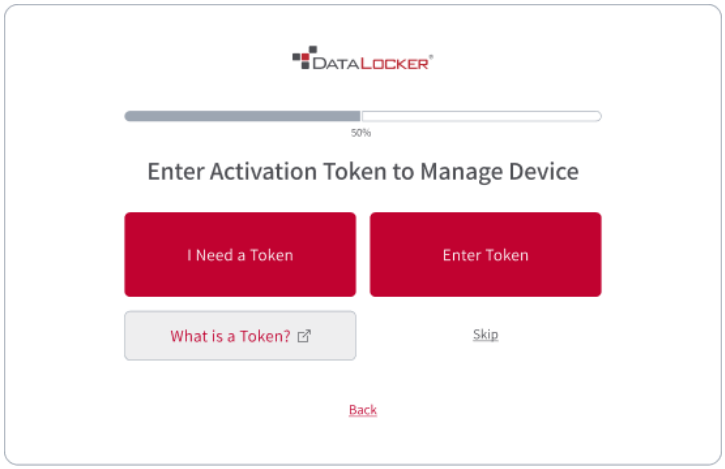


You must agree to the EULA to proceed.

5. **Setup: Choose Your Management Option (Optional)**
   Note that after 10 incorrect password attempts, the device will erase all data.
   Device management with MySafeConsole or SafeConsole offers password recovery and is strongly recommended to avoid data loss in case of a forgotten password.

   - For enterprise users, this step may be required and pre-configured by an IT department.
   - You will see the **Enter Activation Token to Manage Device** screen. Your path forward depends on your situation.

     Follow either path A, B, or C.
     - **For Enterprise Users - Path A**
     - **Personal/Small Business Users - Path B**
     - **Skip management - Path C**



Setup: 5 Path A For Enterprise Users (SafeConsole)

- If you received this device from your IT department, they may have pre-configured it, provided you with an activation token/URL, or pushed a policy to your computer.
- If your screen is pre-filled, simply follow the prompts.
- If you were given a token or URL, click **Enter Token**.
- On the **Activate Your Device** screen, enter the code or URL and click **Activate Device**.

Setup: 5 Path B For Personal / Small Business Users (MySafeConsole)

- If this is your personal device and you want to use the cloud features, follow these steps to get and use a token:
- From the **Enter Activation Token...** screen, click

I Need a Token button.

- On the next screen **Connect Your DL GO to MySafeConsole.com**, click **Sign Up and Get My Token** button. This will open the MySafeConsole web portal in your browser.
- In the web portal, **create a new account or log in**. Follow the steps to generate your unique DL GO Activation Token.
- **Return to the device setup application**. You may need to navigate back to the first management screen. Now click **Enter Token**.
- On the **Activate Your Device** screen, enter the token you just generated in the web portal and click **Activate Device**.

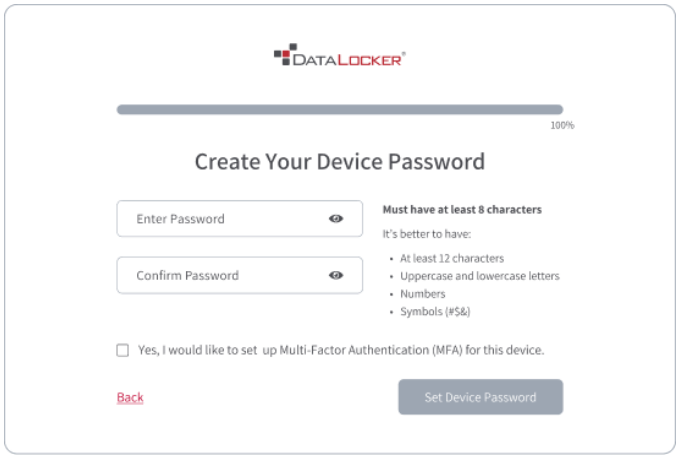
Setup: 5 Path C To Use as a Standalone Device

If you do not wish to use management features, you can use the device standalone.

- Click **Skip** on the **Enter Activation Token…** screen.
- A final screen will appear titled **Not Registering Your Device?** explaining the features you will miss.
- To proceed without management, click **Do Not Register My Device**.

Changed your mind? You can register your device at any time after setup. Simply unlock your device to open the Control Panel and click on the **Manage** tab to begin the registration process.

6. **Setup: Create Your Password**
    - Create a secure password for your device. You can also choose to enable biometrics (Windows Hello/Touch ID) for password-free unlocks on the current host computer on this screen.

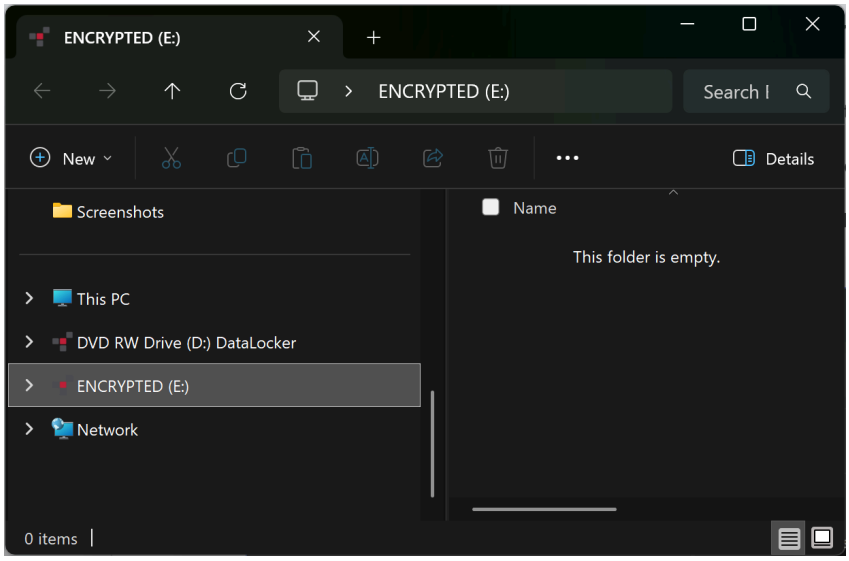


7. **Setup Finalization**
    - The application will finalize the setup. If you enabled biometrics, your computer will prompt you to authenticate. A **Setup Complete!** message will appear when your drive is ready.

3. Daily Use: Unlock, Work, Lock

This is the core function of your DL GO.

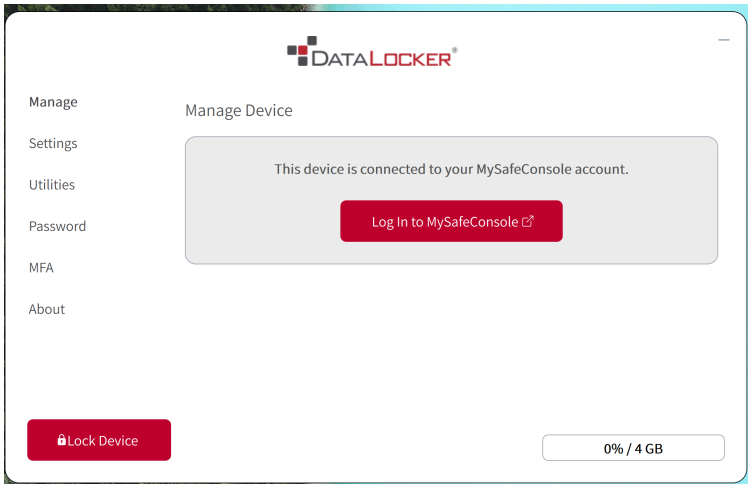
1. **Unlock Your Device:** Run the **DataLocker** application on the DVD RW drive (virtual read-only) and enter your password or use biometrics. Check Read-Only Mode to unlock the storage as write-protected.
2. **Access Your Files:** Once unlocked, the **ENCRYPTED** storage drive will appear on your computer.
3. **Save Your Data:** Simply drag and drop files into the **ENCRYPTED** drive. All data saved here is automatically encrypted and secured.
4. **Lock:** The **DL GO** locks when you **unplug it**, **click the lock button** in the control panel (shortcut Ctrl+L), or **fully power off the host**, but it remains unlocked during computer sleep or after a user logs out. Always ensure the device is locked before leaving it unattended.



Your secure ENCRYPTED storage drive appears after you unlock the device.

4. Control Panel Overview

After unlocking your drive, the Control Panel in the DataLocker application provides access to local device settings. It can also be accessed by right-clicking the **DataLocker icon** in your computer's system tray (taskbar).



The main Control Panel dashboard.

- **Manage:** If unregistered, this tab prompts you to connect to MySafeConsole. If connected, it confirms the link and provides a button to log into the web portal.
- **Settings:** Customize language, set an auto-lock timer (enabling auto lock after inactivity is recommended), and add a custom “If found:” message that is displayed on the Unlock screen.
- **Utilities:** Check for software updates and reformat the ENCRYPTED storage drive.
    - When reformatting, you can choose between:
        - **FAT32:** Compatible with most operating systems (Windows, macOS, Linux), but cannot store individual files larger than 4GB.
        - **exFAT:** Allows for file sizes larger than 4GB.
- **Password/MFA:** Change your password or manage multi-factor authentication settings. On enrolled computers, DL GO uses your fingerprint or face **and** a secure hardware key to unlock—no password needed. For recovery or setting up a new computer, use your long password.
- **About:** View technical details like your device's serial number and software version.

5. Reset & Sanitize

Use these options to securely wipe the drive when repurposing it or transferring ownership. Both methods use cryptographic erasure (destroying the encryption keys) so data is permanently unrecoverable. (Admin note: aligns with NIST SP 800-88 guidance.)

Reset Device (Factory Reset)

Restores the device to first-use state and removes any management link (MySafeConsole/SafeConsole). Use this before selling, gifting, or moving the device to a new owner.

Sanitize Device (Keep Managed)

Erases all data but keeps the device registered to your MySafeConsole/SafeConsole account. Ideal for clean-media reuse without re-registration.

How to wipe

1. Unlock the device.
2. Right-click the DataLocker icon in the system tray/menu bar → choose Sanitize Device or Reset Device (Factory Reset).
3. Confirm by typing the on-screen digits, then proceed.

Important

- Wipes are irreversible. Back up any needed files first.
- Keep the drive plugged in and do not close the app until the wipe completes.
- If managed by an admin, policies may restrict which wipe options are available.

6. Troubleshooting

- **I forgot my password!**

  Option 1 — Use biometrics on an enrolled computer

  If you previously set up Windows Hello or Touch ID on this computer, unlock with your biometric, back up your files. Now Reset and set up again.

  Option 2 — Use MySafeConsole recovery

  - In the DataLocker app, click Forgot Password? to show your Request Code (e.g., 3RVX-DUP6).
  - Go to MySafeConsole.com (or contact your administrator), sign in, select the device, and choose Password Reset in the More (···) menu.
  - Paste the Request Code. The portal returns a Recovery Code (24 characters) to copy.
  - Paste the Recovery Code back into the DataLocker app to unlock and set a new password.

  The recovery process never reveals your current password. Codes are verified on the device. Incorrect codes are rejected and repeated failures may trigger anti-brute-force protection.

  Option 3 — No biometrics, not registered

  If you're not enrolled with biometrics and haven't linked to MySafeConsole/SafeConsole, you have 10 password attempts. After 10 failures, the device activates brute-force protection and performs a cryptographic reset that permanently erases the data. If you're unsure, pause and try later—many users recall the password after a break.

- **I only see a drive called DataLocker.**

  You haven't unlocked yet. Open DataLocker, run the DataLocker app, and authenticate to mount ENCRYPTED (which is where you will store your files).

- **I want read-only but I'm using biometrics.**

  Cancel the biometric prompt → check Read-Only Mode → exit the app from the tray/menu bar → relaunch from DataLocker → unlock with Windows Hello/Touch ID. The ENCRYPTED volume mounts read-only.

- **ENCRYPTED didn't appear after unlock or even the DataLocker volume did not show up at first.**

  Use a direct USB port (avoid unpowered hubs), check any cables, and ensure security software allows new volumes.

- **I unplugged without locking.**

The device locks when powered down so that is OK. As long as nothing was being actively saved to the drive at the unplugging all your data is safe.

7. Getting Help

The following resources provide more information about DataLocker products. Please contact your Help Desk or System administrator if you have further questions.

The full DL GO specification is available in the datasheet.

support.datalocker.com: Support tickets, information, knowledgebase articles, and video tutorials
datalocker.com: General information
datalocker.com/warranty: Warranty information

Document Version

The latest version of this document resides at
https://media.datalocker.com/manuals/DataLocker_DL_GO_User_Guide.pdf

This document was compiled on Sep 3, 2025

Notices

DataLocker is continuously updating its products, the images and text in this manual may vary slightly from the images and text displayed by your device. These changes are minor and should not adversely affect the ease of setup.

Disclaimer

DataLocker is not liable for technical or editorial errors and/or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing or use of this material. The information provided herein is subject to change without notice. The information contained in this document represents the current view of DataLocker on the issue discussed as of the date of publication. DataLocker cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. DataLocker makes no warranties, expressed or implied, in this document. DataLocker, DataLocker Sentry, and the DataLocker logo are registered trademarks of DataLocker Inc. and its subsidiaries. All other trademarks are the property of their respective owners. All rights reserved.

Patents

Patent: **datalocker.com/patents**

FCC Information

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user 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 equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.