

# DataLocker DL3 User Guide

version 3.35

*DataLocker Inc.*

*August, 2018*



**DL3/DL3 FE**

## Contents

|   |           |
|---|-----------|
| <b>At a Glance</b>                              | <b>3</b>  |
| Introduction . . . . .                          | 3         |
| About the DL3 . . . . .                         | 3         |
| Citrix Compatibilities . . . . .                | 4         |
| <b>Getting Started</b>                          | <b>4</b>  |
| Accessing The Setup Menu . . . . .              | 4         |
| Administrator Password . . . . .                | 5         |
| Connecting The Device . . . . .                 | 6         |
| Main Screen . . . . .                           | 7         |
| Disconnecting Your DL3 . . . . .                | 7         |
| <b>Features</b>                                 | <b>9</b>  |
| Administrative Controls . . . . .               | 9         |
| System Menu . . . . .                           | 9         |
| User Options . . . . .                          | 10        |
| User Password . . . . .                         | 10        |
| Self-Destruct Mode . . . . .                    | 11        |
| Zeroize . . . . .                               | 12        |
| RFID Authentication . . . . .                   | 12        |
| Read-Only Mode . . . . .                        | 14        |
| Auto-Lock . . . . .                             | 15        |
| <b>SafeConsole</b>                              | <b>17</b> |
| Enabling SafeConsole . . . . .                  | 17        |
| Registering The DL3 To SafeConsole . . . . .    | 17        |
| Using A SafeConsole Managed Device . . . . .    | 20        |
| Disabling SafeConsole . . . . .                 | 23        |
| <b>Initializing And Formatting Your DL3</b>     | <b>24</b> |
| How To Initialize Your Drive . . . . .          | 24        |
| Selecting The Correct File System . . . . .     | 24        |
| Formatting Your DL3 On Windows . . . . .        | 24        |
| Formatting Your DL3 on macOS . . . . .          | 26        |
| Linux Compatibility And Configuration . . . . . | 28        |
| Frequently Asked Questions . . . . .            | 29        |
| Contact The Support Team . . . . .              | 29        |

## At a Glance

### Introduction

Congratulations on your purchase of the DataLocker DL3™ Encrypted Hard Drive. This user manual is intended to help you configure your device. Because DataLocker is constantly updating its products, the images and text in this manual may vary slightly from the images and text displayed by your DataLocker DL3. These changes are minor and should not effect the ease of setup adversely.

Updated software and documentation are freely available for download at our website. Visit our [Device Firmware Updates](#) page for all available updates.

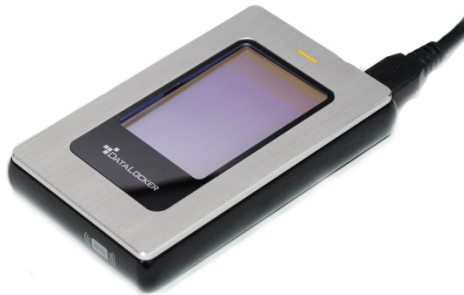
The DataLocker DL3 stands alone as the only external hard drive equipped with a patented, on board, LCD touch screen. This feature allows the user to conveniently perform all processes directly through the LCD Interface, making it truly 100% platform independent.

Although the DataLocker DL3 is extremely user friendly, it is recommended that you review this guide to ensure that you become fully acquainted with the DataLocker DL3 and all of its features.

### About the DL3

The DataLocker DL3 has a minimum power requirement of 5 Volts and 1A of current that is drawn from the USB port. The DataLocker DL3 utilizes 256-bit AES encryption operating in XTS mode to fully encrypt your drive's contents.

The DataLocker DL3 FE (FIPS Edition) has FIPS validated components and two independent crypto processors. Data undergoes two passes of 256-bit AES encryption - the first pass being in XTS mode, the second pass in FIPS 140-2 validated CBC mode - before it is stored on the hard drive.



The DataLocker DL3 comes preformatted with the Windows NTFS file system. All major file systems are supported (HFS, NTFS, EXT, FAT).

If you require a different file system, please consult your operating system for initialization and formatting instructions.

For more information on initializing and formatting your DL3, see [Initializing And Formatting Your DL3](#).

The DataLocker DL3 is completely cross-platform compatible and OS agnostic. With no software or special drivers required, the DL3 works with Windows, Linux, MacOS, Android phones and tablets, Chromebooks, and embedded systems - any system that can utilize USB Mass Storage.

**Note:** Managed DL3s require Windows 7+.

## Citrix Compatibilities

The DataLocker DL3 and DL3 FE are compatible with:

- XenApp 7.14
- XenApp 7.15 LTSR
- XenApp 7.16
- XenApp 7.17
- XenDesktop 7.14
- XenDesktop 7.15 LTSR
- XenDesktop 7.16
- XenDesktop 7.17

Additionally, the DL3 is compatible with:

- Citrix Virtual Apps and Desktops service on Azure

## Getting Started

### Accessing The Setup Menu

The Setup menu is where all options and controls are displayed, including changing your password.

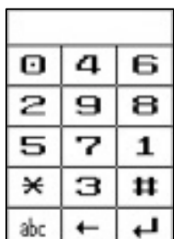
To access the Setup menu:

1. Connect the DL3 to your computer with the included USB cable.
2. At the startup screen press **Start**.

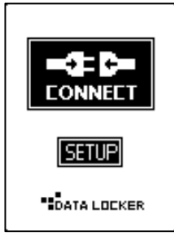


3. Enter the administrator password. If this is your first time logging in, the default password is *0000000*.

Then press the **Enter** symbol.



4. Press the **Setup** button on the touch screen. If it is not selected within 3 seconds, the DataLocker DL3 will connect to the computer automatically.



5. You can navigate the Setup menu using the function buttons listed, or go back to the Connect menu by pressing the **Return** button in the top left corner of Setup menu.

From the Setup menu, you can:

- Change your password
- Enable/disable the user password
- Access the System menu
- Access the SafeConsole setting

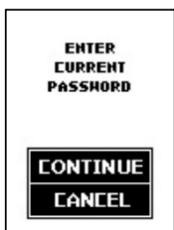
## Administrator Password

It is highly recommended that you set a new administrator password using alpha-numeric characters upon the first use.

1. From the Setup menu, press the **Change Password** button.



2. Press the **Continue** button and enter the current password. Follow the onscreen instructions to set your new password. It is recommended that you use a combination of both alpha and numeric characters for your password.

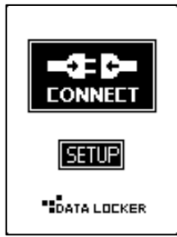


3. After the new password has been set, you may set other options, or save and go back to the Connect menu by pressing the **Return** button located at the top left hand corner next to Setup.

**Warning:** A lost or forgotten password cannot be reset or recovered without losing all the stored data. To reset a device with an unknown password, incorrect passwords can be entered until the device self-destructs. This will delete all stored data on the drive. The device will need to be initialized again before reuse. For more information on initializing your device, see [Initializing And Formatting Your DL3](#).

## Connecting The Device

After entering the password, press the **Connect** button to start using the DL3 drive.



The drive will begin connecting to the computer. By default, Windows will show an AutoPlay dialog once the drive has successfully connected.

### CD Drive (D:) Login DataLo...

Choose what to do with this disc.

#### Install or run program from your media



Run DataLockerDL3.exe  
Published by DataLocker Inc.

#### Other choices



Open folder to view files  
File Explorer

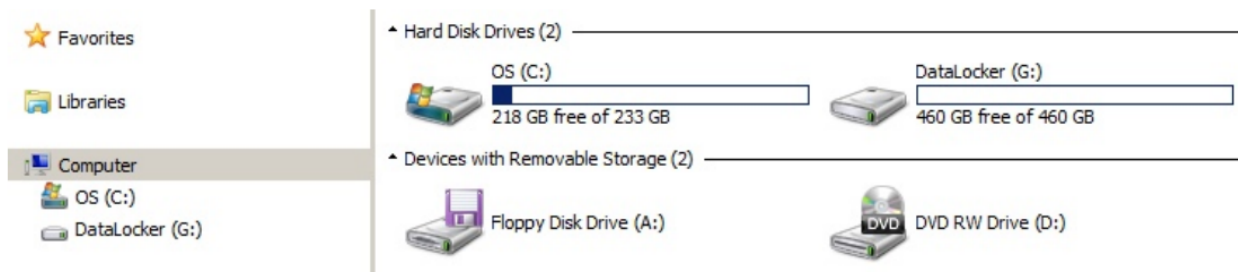


Import photos and videos  
Dropbox



Take no action

In Windows Explorer you will now see a drive called "DataLocker" listed in the Hard Disk Drives section. A new drive letter will be automatically assigned to this drive. You may now start using your DL3 drive!

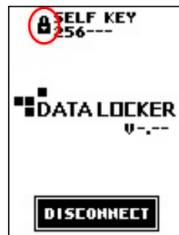


## Main Screen

The connected status screen on your DL3 drive displays useful information.



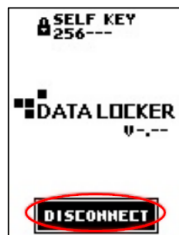
Indicates that the DL3 drive has a **User Password** enabled.



Indicates that the DL3 drive's **User Password** is disabled.



Displays the current firmware installed on the DL3 drive.



Disconnects the DL3 drive from the computer. **Note:** To prevent data loss or damage to disk, ensure the DL3 drive has been properly ejected from the operating system before pressing this button.

## Disconnecting Your DL3

To prevent loss or corrupted data, properly eject the DL3 drive when you're finished using it. The best practice is to use your operating system's **Safely Remove Hardware** or **Eject** function before you power down or detach the DataLocker DL3 from the host system.

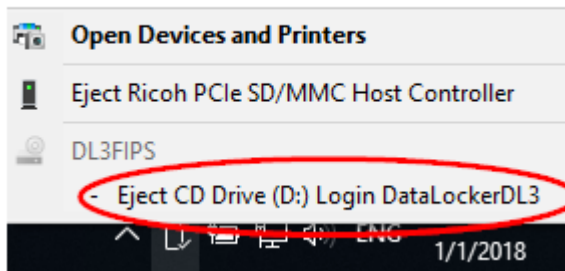
This will also help prevent damage to the disk.

## Windows Users

1. Right click the **Safely Remove Hardware** icon located on the lower right hand corner of the Windows taskbar.



2. Once the popup menu has appeared, click the correct drive to safely eject the DL3 from Windows.



## macOS Users

1. Click the **Eject** button that corresponds with the DataLocker DL3 on macOS.



2. Once the drive has been ejected from macOS, press **Disconnect** on the DL3 drive.



## Features

### Administrative Controls

| Menu Option                            | Details   |
|--|---|
| Previous Menu/<br>Save Settings Button | Used to go back to the previous menu and save the current settings.   |
| Change Password                        | Used to set the administrator password.   |
| User Password                          | Used to create a user password.   |
| System                                 | Enter the System Menu. For more information see the <a href="#">System Menu</a> section.  |
| SafeConsole                            | If enabled, allows the device to be managed by the company's SafeConsole central management system. For more information about this feature, please read the <a href="#">SafeConsole</a> section. |

### System Menu

| Menu Option                            | Details   |
|--|---|
| Previous Menu/<br>Save Settings Button | Used to go back to the previous menu and save the current settings.   |
| Next Menu Button                       | Used to go to the next screen.  |
| Language                               | Set the menu language. Supported languages are: <ul style="list-style-type: none"> <li>- English</li> <li>- French</li> <li>- German</li> <li>- Spanish</li> <li>- Japanese</li> <li>- Korean</li> </ul>  |
| Strong Password                        | The DL3 allows the administrator to enforce strong password rules for authentication. With the Strong Password feature enabled, all passwords must meet the following requirements: <ul style="list-style-type: none"> <li>- Password must be 8 characters long or greater. The minimum password length is adjustable from 8 to 32 characters.</li> <li>- Sequential passwords such as "12345678", "98765432", "ABCDEFGH", are prohibited.</li> <li>- Repeating passwords such as "11111111", "AAAAAAA", are prohibited.</li> <li>- The password must contain both numeric and alpha characters.</li> </ul> |

| Menu Option          | Details   |
|----------------------|---|
| LCD Contrast         | Adjust the LCD screen's contrast.   |
| Previous Menu Button | Used to go back to previous menu and save the current settings.   |
| Key Tone             | Turn the keypad tone on or off.   |
| Zeroize Drive        | <b>Note:</b> This does not turn off all other device sounds. Initiates the destruction of all encryption keys and user passwords, making the data on the drive irretrievable. The DL3 will be reset to the original factory state. The device will need to be reinitialized and formatted in order for it to be redeployed. |
| RFID                 | Enters the optional RFID Authentication module setup menu.  |

## User Options

User options can be found by logging into the device with the user password and entering the Setup menu. For more information, see the [User Password](#) section.

| Menu Option                            | Details  |
|--|--|
| Previous Menu/<br>Save Settings Button | Used to go back to previous menu and save the current settings.  |
| Change Password                        | Used to set the user password. For more information, see the <a href="#">User Password</a> section.  |
| Language                               | Set the menu language. Supported languages are: <ul style="list-style-type: none"> <li>- English</li> <li>- French</li> <li>- German</li> <li>- Spanish</li> <li>- Japanese</li> <li>- Korean</li> </ul> |
| LCD Contrast                           | Adjust the LCD screen's contrast.  |
| Key Tone                               | Turn the keypad tone on or off.  |

## User Password

The DL3 supports the creation of a user password. The user will have access to all data on the drive, however, the user will not be able to access certain administrative options and controls.

**Note:** You must change the default administrator password before creating a user password.

1. Navigate to the Setup Menu. For more information, see [Accessing The Setup Menu](#).

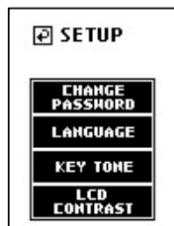
- At the setup menu press the **User Password** button.



- Press the **Create** button. A user with the default password of *0000000* is now created.



- The user should then re-login with the default user password of *0000000* and change the default password to a personal password. The user password change process is identical to changing the administrator's password. The user's setup menu is limited to Change Password, Language, Key Tone, and LCD Contrast settings. See [User Options](#) for more information.



## Self-Destruct Mode

The self-destruct feature is designed to defend against brute force password hacks. The DL3 performs this by zeroizing all of the device's encryption keys once the appointed number of failed login attempts is reached.

Once the encryption key is deleted, your data is no longer recoverable. Powering off the unit does NOT reset the unsuccessful password attempts counter. The password attempts counter will only reset after a successful password attempt. Use this feature with **caution**.

- The self-destruct function deters brute force password attacks. The number of password attempts is 10 tries.

Once the defined number of failed password attempts is reached, all data on the DL3 drive will be irrecoverably destroyed.

- The DL3 drive is designed to automatically power off after the first five tries. You will have to unplug and reconnect the DL3 drive to reattempt the connection process.

- If you are within the final three tries you will be alerted with a "Hack Detected" warning.



- After 9 unsuccessful attempts you will see the "Self-destruct Will Begin" warning. If the next attempt fails, the self-destruct function will destroy all encryption keys on the DL3 drive. This process is instantaneous and all data will be inaccessible.



- The DL3 drive will emit a steady alert tone and will not stop until you unplug the USB cable from the computer. The drive will have to be reinitialized and formatted to work with your operating system again.

## Zeroize

Zeroizing the device will wipe all data on the drive and return the device to factory settings.

**Note:** The SafeConsole feature must be disabled to use the Zeroize function.

To zeroize the DL3:

- Navigate to the Setup menu. For more information see, [Accessing The Setup Menu](#).
- Find and press the **System** button to access the System menu.
- Press the **Zeroize** button.

**Note:** The option is on the second page of the System menu.

- Follow the onscreen prompts to complete the process.
- The DL3 will power off and back on automatically when it has finished zeroizing. To use your DL3 once again, you will need to reinitialize it. See [How To Initialize Your Drive](#) for more information.

## RFID Authentication

The DL3 FE features an optional RFID module for a second layer of authentication. A maximum of five RFID tags can be registered on each DL3 drive. RFID models of the DL3 FE come with two RFID tags. If you would like to pair your own tag, the DL3 RFID module supports ISO 14443A and ISO 15693 with a frequency of 13.56 MHz.

1. Navigate to the Setup Menu. For more information, see [Accessing The Setup Menu](#).
2. At the Setup menu, press the **System** button.



3. Press the button to display the **System 2/2** screen.



4. At the next menu screen, press the **RFID** button.



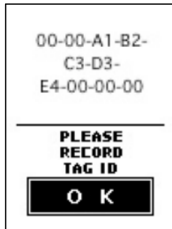
5. At the setup RFID screen, press the **Add RFID Tag** button.



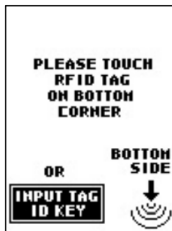
6. Place the supplied RFID tag near the bottom right hand corner of the DL3 until you hear a "beep" tone.



7. After registering, the RFID tag value will be displayed. Please make note of the RFID tag ID in case the tag is lost or damaged.



You have now successfully registered a RFID tag and the RFID function is enabled.



The next time you reconnect the DL3 drive, you are required to use the RFID tag to authenticate before entering the password.



## Read-Only Mode

The DL3 drive comes with two Read-Only Mode options. The administrator can force Read-Only Mode for all users or users and administrators can set the feature individually. Both options are disabled by default.

### Forced Read-Only Mode

The administrator can force Read-Only Mode for users. Once the feature is enabled, only the administrator will be able to change it. Users of a DL3 drive that has Read-Only Mode enabled can still view the files and copy them, but they will not be able to save any changes to the files on the drive nor delete them.

**Note:** With this setting enabled, administrators will not be forced into Read-Only Mode.

To enable forced Read-Only Mode, follow these steps:

1. Navigate to the **Setup** menu. For more information, see [Accessing The Setup Menu](#).
2. At the Setup menu, press the **System** button.
3. Select **Read-Only Mode**.

**Note:** This option is located on the second page of the System menu.

4. Change to **Enable**.



### Individual Read-Only Mode

The administrator and the user can each set Read-Only Mode individually, by checking the box on the Connection screen after entering the password. Checking the box will enable Read-Only Mode for a single login. Upon disconnecting and logging in again, the setting can be toggled.

**Note:** After checking the Read-Only Mode box and disconnecting, the option will remain checked until the user unchecks it.

### Auto-Lock

Auto-lock is a security feature available on the DL3. This feature is disabled by default but can be enabled by the administrator and the user. The amount of idle time required to time out the device is configurable from 10 to 180 minutes in increments of 10 minutes.

Auto-lock will disconnect the drive once it is idle (i.e. zero activity) for the configured amount of time. The device will beep and display a 30 second countdown on the touchscreen before the timeout limit is reached. Modifying the contents on the drive or even viewing the files will reset the timeout counter.

To enable auto-lock, follow these steps:

1. Navigate to the **Setup** menu. For more information, see [Accessing The Setup Menu](#).
2. At the setup menu, press the **System** button.
3. Press the **Next Page** button two times to arrive at the **System 3/3** screen.
4. Select **Auto-Lock**.
5. Adjust the minutes of idle time required.

- Change to **Enable**.



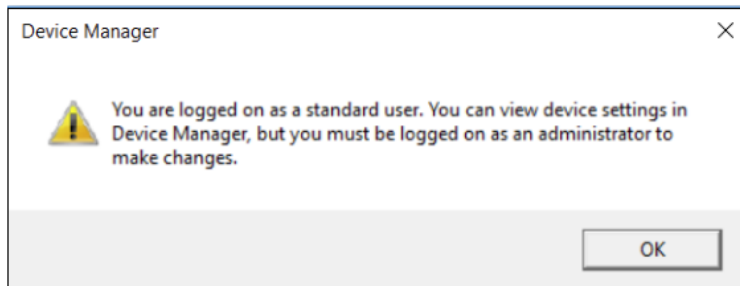
### Disabling Windows 10 Power Save

By default, Windows 10 attempts to shut off USB devices after a set period of inactivity. If the DL3 is put into this low power state, the drive will automatically lock the drive and require reauthentication. To disable this feature of Windows, follow the steps below.

**Note:** You will need to complete the following steps once for each drive plugged into your computer.

- Log in as a local administrator on your computer.

**Note:** If you are not an administrator you will receive a warning indicating you won't be able to make changes when you open Device Manager. Please contact your administrator for further assistance.



- Unlock your DL3 device. If your device is being managed by SafeConsole, launch the client on your computer.
- Open **Device Manager** (Click the windows button and type "device manager").
- Click on the arrow next to Universal Serial Bus controllers.
- Right click on **USB Mass Storage Device**.
- Click **Properties**.
- Go to the **Power Management** tab.
- Uncheck "Allow the computer to turn off this device to save power".
- Click **OK**.



## SafeConsole

SafeConsole™ is a central management console used to optionally manage DL3 devices. Managed DL3s require a Connection Token upon initialization. The SafeConsole Connection Token is obtained by the System Administrator through the Quick Connect Guide, located inside of the SafeConsole user interface. SafeConsole requires a device license for activation. *License sold separately.*

Users without access to a Management Server, please contact sales: [sales@datalocker.com](mailto:sales@datalocker.com) / (913)310-9088

SafeConsole offers several key features including audit logging, anti-malware services (license sold separately), remote password reset, and more!

### Enabling SafeConsole

Toggleing the SafeConsole feature requires administrative access to your DL3. If you are a user, please contact your administrator for assistance. Enabling SafeConsole will limit drive usage to Windows machines with a valid connection to the SafeConsole Server.

To Enable SafeConsole:

1. Navigate to the Setup menu. For more information, see [Accessing The Setup Menu](#).
2. Select the **SafeConsole** option.
3. Choose **Enable**.
4. Return to the Connection menu and select **Connect**.
5. Upon launching the client on your computer, it will ask for your SafeConsole Connection Token. This can be found in the Quick Connect Guide within the SafeConsole user interface.

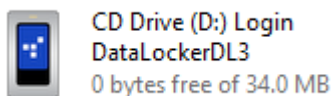
**Note:** If the SafeConsole client is not shown, the latest firmware may need to be installed on your device. Find the latest firmware update [here](#).

### Registering The DL3 To SafeConsole

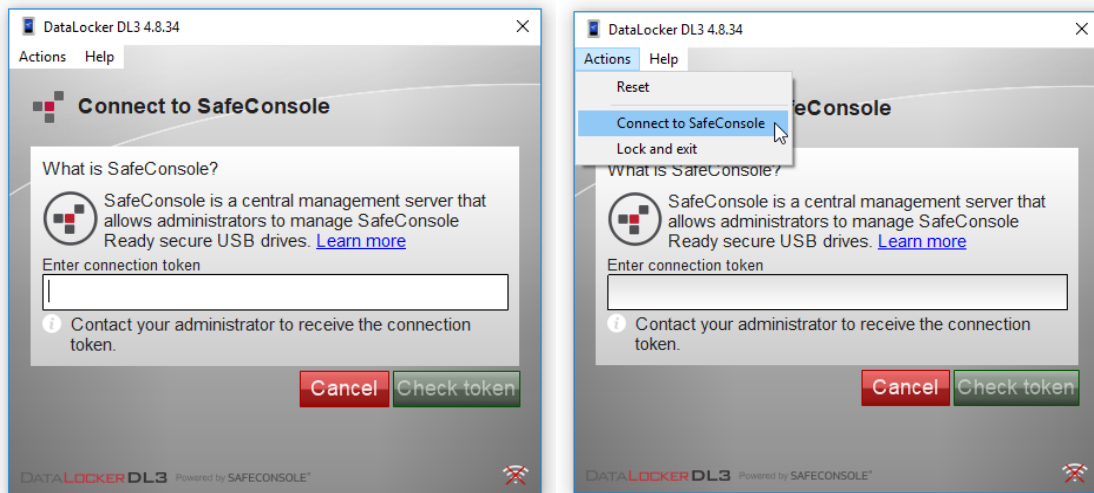
Before registering your drive to SafeConsole, make sure SafeConsole is enabled on your DL3. For more information, see [Enabling And Disabling SafeConsole](#).

You will need a Connection Token, provided by your system administrator, to complete the registration.

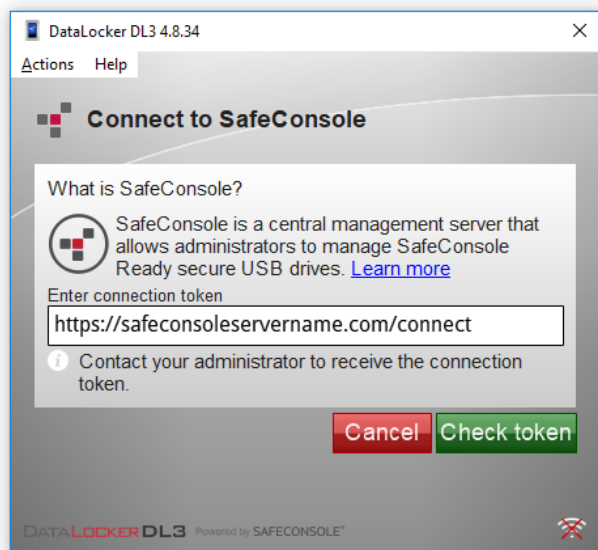
1. Log into the DL3 and press the **Connect** button.
2. On your computer, double click the **DataLocker DL3** drive under Devices and Drives to launch the client.



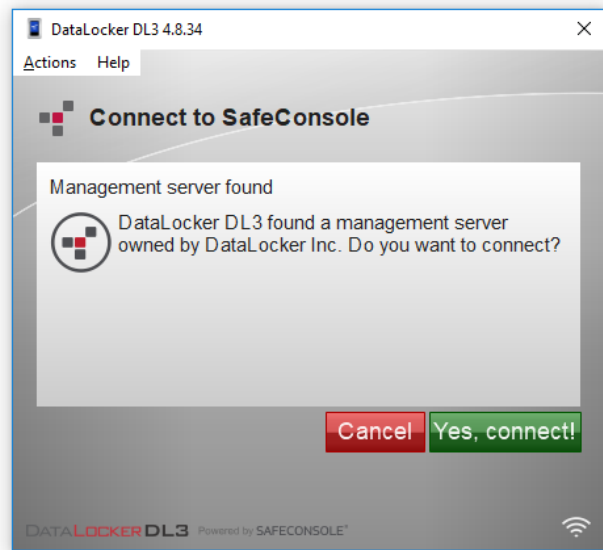
3. Upon launch, the SafeConsole Connection page should appear. If it doesn't, click on **Actions**, then **Connect to SafeConsole**.



4. Enter the **SafeConsole Connection Token** provided by your SafeConsole Administrator and click **Check Token**.



- The client will search for the correct SafeConsole server and will ask you to confirm the connection when it finds one. Click **Yes, Connect**.



- Your device will connect to the server. You can determine if your device is reaching the server by the connection symbol in the bottom right corner.



**Optionally Enabled Policies** - These policies may or may not be enabled by your System Administrator. They will appear during device registration if they have been enabled.

- **Confirm Ownership of the device:** Enter the Windows username and password that is associated with the login credentials of the computer the device is plugged into.
- **Custom Device Information:** Required information about you or your device. The required fields will vary.
- **Unique User Token:** This token is directly associated with the end user's account and will be provided by the System Administrator.
- **Administrator Registration Approval:** The System Administrator may require their approval to proceed with device registration.

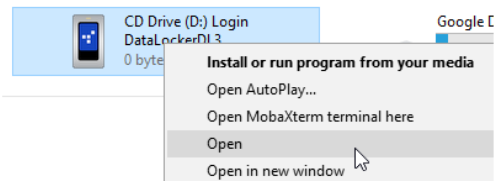
- Upon the second login on the device after registering to SafeConsole, the client will save the backup password. You will be notified with a popup.



## Registration Troubleshooting

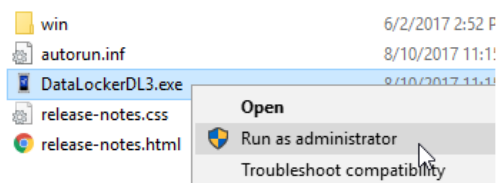
If you have trouble registering your DL3 or your device consistently loses the connection between the client and the SafeConsole server, follow the steps below.

- Log into the DL3 and press **Connect**.
- On your computer, right click the **DataLocker DL3** icon and click **Open**.



- Right click **DataLockerDL3.exe** and click **Run as administrator**.

This is a one time action that should solve the connection problem. Next time you connect, you should be able to run the DL3 client as usual.



## Using A SafeConsole Managed Device

### Logging In And Accessing Files

To log into to your SafeConsole registered device:

- Enter the correct password on the DL3 screen.
- Press **Connect**.

3. On your computer, find the **DataLocker DL3** icon under This PC and double click.
4. The device client will launch and you will have access to your files by clicking **Files**.

## Locking The Device

To lock your SafeConsole registered device:

1. With the client open on your computer, click the **Actions** button in the top left corner.
2. Click **Lock and Exit**.

Your files have now been secured and the drive will be ejected from the computer. Your DL3 screen will either show the **Connect** button to reconnect your device or will show a message stating it is safe to remove your device from the computer.

## Password Reset

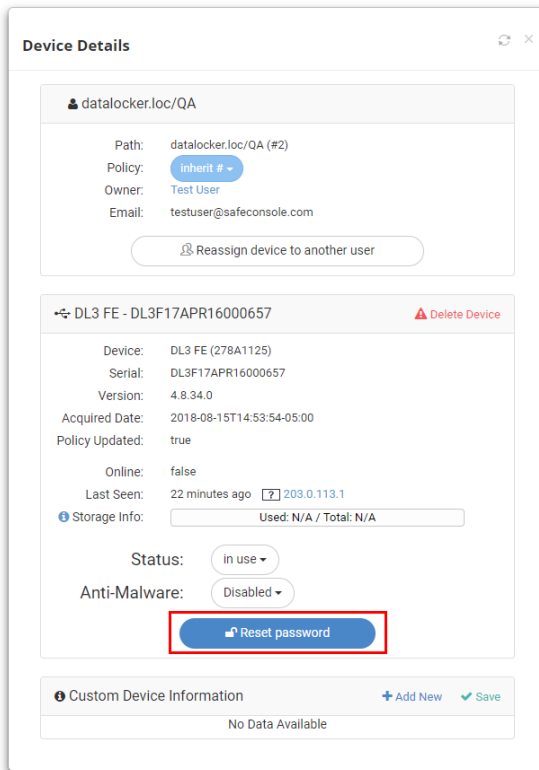
The password reset function of SafeConsole is a useful tool to provide users a way to reset a lost or forgotten password without losing the data on the drive.

**Note:** Remote Password Reset must be turned on within SafeConsole for this option to be available on the DL3.

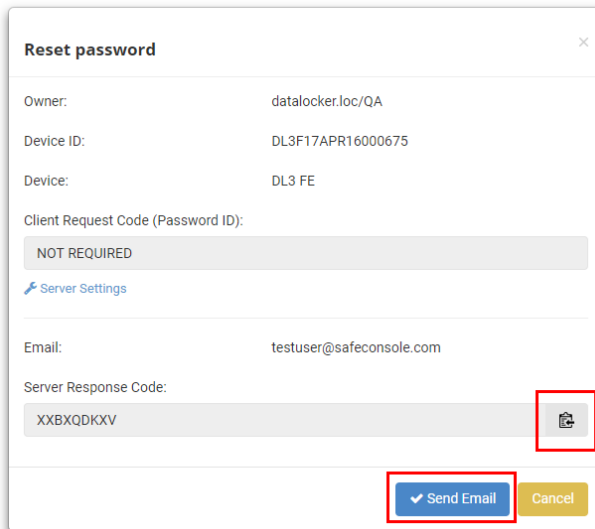
1. Log into the SafeConsole user interface and navigate to the correct device on the Devices page. You may need to ask the user for the serial number of the drive to ensure you select the correct device in SafeConsole.
  - To find the correct serial number, the user should go to **Help** in the upper left corner and then **About**.
2. Click the serial number of the correct device.

|                          | Owner                | Device               | Serial               | Version              | Status               | Anti-Malware         | Last Seen                     | Action |
|--------------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|-------------------------------|--------|
|                          | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | From <input type="text"/>     |        |
| <input type="checkbox"/> | Test User            | DL3 FE               | DL3F17APR16000657    | 4.8.34.0             | in use               | Disabled             | 9 minutes ago [7] 203.0.113.1 | Action |

3. In the Device Details popup, click the blue **Reset Password** button.



4. You will be given a Server Response Code to give to the user. Options include copying the code to send to the user or clicking **Send Email** to send an email to the user from SafeConsole with the code inside.



5. The user should enter the Server Response Code into their DL3 on the password screen.
6. The device will reset the password to *0000000*. The user will be prompted to change the password upon the next use.

## Disabling SafeConsole

### To Disable SafeConsole Before Device Registration

Follow these steps to disable SafeConsole only if you have *not* registered your device with SafeConsole previously.

1. Navigate to the Setup menu as an administrator. For more information, see [Accessing The Setup Menu](#).
2. Select the **SafeConsole** option.
3. Choose **Disable**.
4. Return to the Connection menu and select **Connect**.
5. Your device will appear as **DataLocker** in the Hard Drives and Devices section, under This PC.

### To Disable SafeConsole After Device Registration

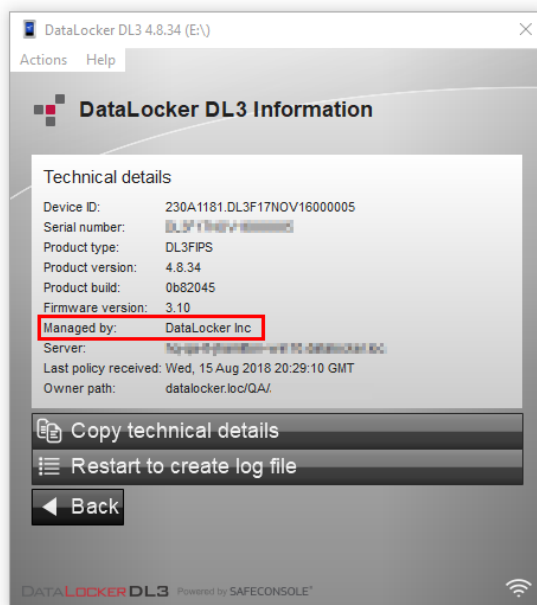
Follow these steps to disable SafeConsole if you have previously registered or are currently registered to a SafeConsole server. Disabling SafeConsole on a DL3 that has already been registered with SafeConsole will require contact with DataLocker technical support because the device is now tied to the SafeConsole server.

**Note:** Technical support agents are only able to assist system administrators. If you are not the system administrator of your device, please contact your system administrator for assistance.

You can reach support by calling (913) 310-9088 or emailing [support@datalocker.com](mailto:support@datalocker.com).

You will need the company name when contacting support. To find this:

1. Log in and launch client.
2. Click **Help** in the upper left corner and then click **About**.
3. The company name will be in the **Managed by** section.



## Initializing And Formatting Your DL3

On occasion - for example, after self-destructing your DL3 - you will need to initialize and reformat the drive to make it usable again.

### How To Initialize Your Drive

1. Touch start screen.
2. Follow the onscreen prompts, hitting **Yes** and **Continue**.
3. Touch screen 16 times to generate a new AES key.

The default password is *000000*.

You will now have to format your drive. The instructions to format your drive will vary depending on your operating system.

### Selecting The Correct File System

Your device is formatted as **NTFS** from the factory.

The DL3 can be reformatted to any file system of your choosing to accommodate a different operating system or to remove file size restrictions.

Recommended file systems:

- FAT32
  - Pros: Cross-platform compatible (Windows, macOS, and Linux)
  - Cons: Limited individual file size of 4GB
- NTFS
  - Pros: No file size limitations
  - Cons: Limited cross-platform compatibility - Windows, macOS (read-only), and Linux (read-only)
- exFAT
  - Pros: No file size limitations
  - Cons: Not supported by legacy operating systems

**Note:** Reformatting your DL3 drive will erase all your files but will not erase your device password and settings. This should not be used as a method of securely erasing files. To securely erase your files, perform a Zeroize function. For more information, see the [Zeroize](#) section.

**Important:** Before you reformat the device, back up your drive to a separate location, for example, to cloud storage or your computer.

### Formatting Your DL3 On Windows

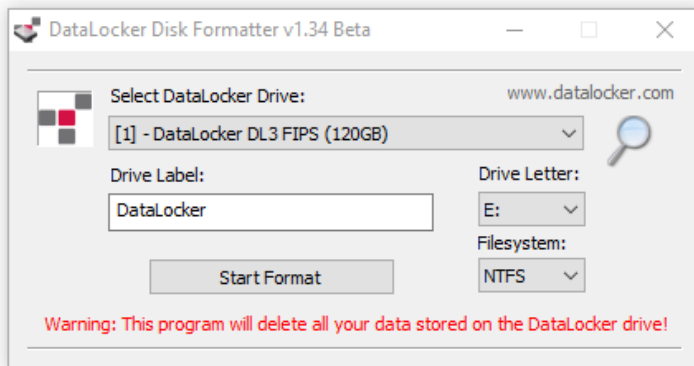
1. Connect the DL3 to the computer and log in.
2. Download the **DataLocker Disk Formatter Tool**, which can be found [here](#).



3. Run the **DataLocker\_Disk\_Formatter.exe**. The formatting tool will automatically find the DL3 device.

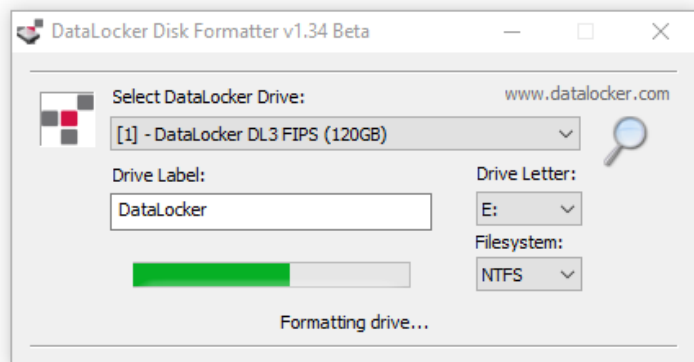


4. Select the **Drive Letter** and **Format Type**, and rename your **Drive Label**.

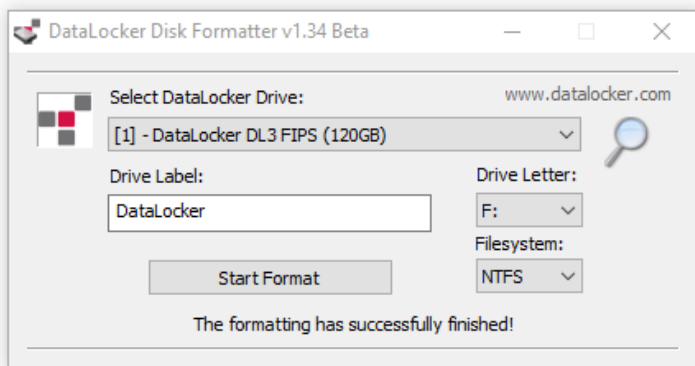


5. Click **Start Format**.
6. The formatting tool will show **Formatting drive...**

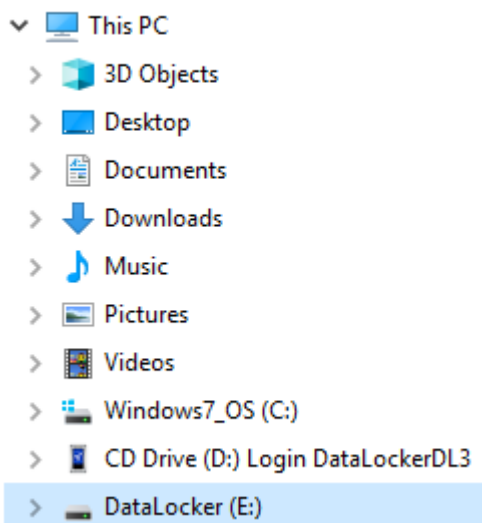
**Note:** Windows may recognize that the drive needs to be formatted after the formatting tool has already started. Feel free to close any popups from Windows that say the drive needs to be formatted.



- When finished, the formatting tool should display the message “**The formatting has successfully finished!**”

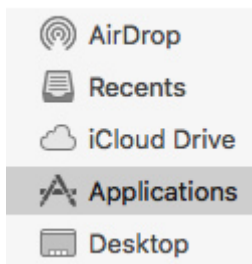


Your DL3 will now appear under **This PC**.

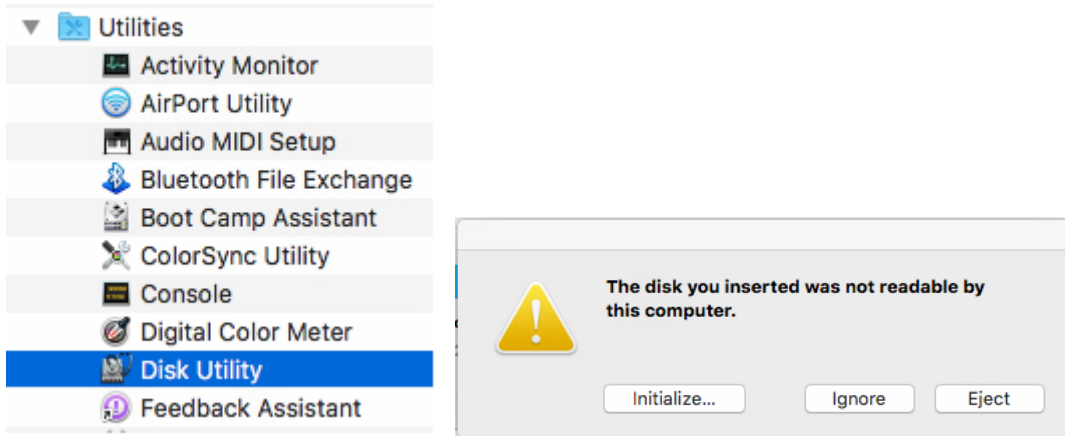


## Formatting Your DL3 on macOS

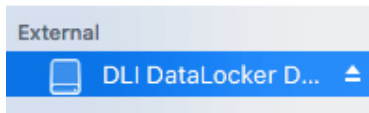
- Go to **Applications** under your **Finder**.



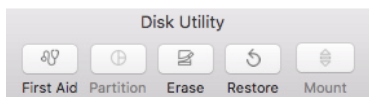
- Click **Utilities** and open **Disk Utility**. You will receive a warning message that the drive is not readable. Click **Ignore**.



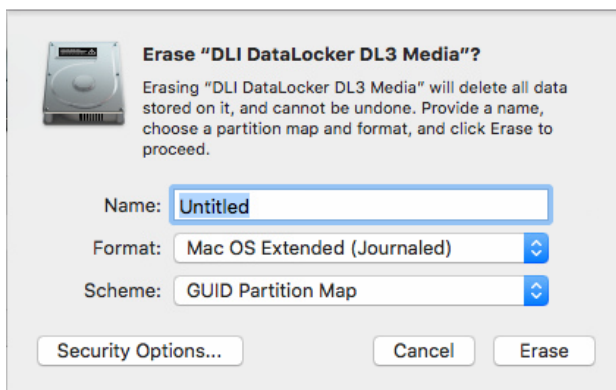
- Select the unformatted DL3 disk.



- Click the **Erase** tab at the top of the screen.



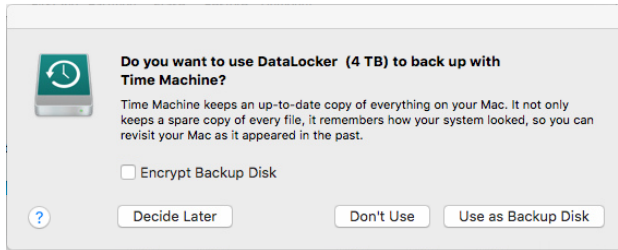
- Rename the disk label and choose a file system.



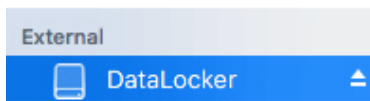
- Click **Erase**. The drive will begin formatting.



- When it is finished formatting, you may get a popup message asking if you would like to backup your drive with Time Machine. Choose your preferred option.



- Click **Done**.
- Your formatted DL3 should now appear under Devices.



Click on the links below for a video walkthrough on formatting your DL3.

[Format your DL3 - Windows](#)

[Format your DL3 - macOS](#)

## Linux Compatibility And Configuration

The DL3 is platform independent when used apart from SafeConsole and capable of being run with 100% compatibility on most systems. For optimal Linux or Unix based system compatibility, we recommend using at least the Linux 2.6.31 Kernel (released 9 September 2009), which implemented the xHCI specification for USB 3.0. Although older versions should work, they might run in USB 2.0 mode, which can be significantly slower.

You can check your kernel version by typing the following command in the terminal:

```
# uname -r
```

Because there are so many distribution versions of Linux, we cannot guarantee that every version of every operating system has been tested. The following distributions have been tested and found working with ext4 file system formatting:

- Red Hat Enterprise Linux 6.5
- CentOS 6.5
- Debian 7.4
- Ubuntu 13.10
- Ubuntu 14.04

In most newer distributions the drive should automatically mount. To format the drive, first enter terminal, then list detected hard disks using

```
# fdisk -l | grep '^Disk'
```

Your configuration may vary. For this example, we'll assume the disk is at /dev/sdb

You will then type

```
# fdisk /dev/sdb
```

Follow the instructions in fdisk to create a new partition. Finally you'll use the mkfs command to format the disk for Linux. Here, we use ext4.

```
# mkfs.ext4 /dev/sdb1
```

If you want to rename the drive, use the e2label command.

```
# e2label /dev/sdb1 /DataLocker
```

## Frequently Asked Questions

If you still have questions after reviewing the user guide, please consult our FAQ page at [datalocker.com](http://datalocker.com).

You can find warranty information at [datalocker.com/warranty](http://datalocker.com/warranty).

## Contact The Support Team

If you have any unresolved issues with your DL3, you can give us a call at (913) 310-9088.

If you would like to contact us outside of our business hours (Monday through Friday from 9:00AM - 5:00PM CST), visit our [Support](#) page to post your question and we will get back to you as soon as possible.

**Note:** 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 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.

Patent: [datalocker.com/patents](http://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.