User Guide DL4 FE (FIPS Edition)

FIPS 140-3 Level 3 pending* certified and
FIPS 140-2 Level 3 certified

Encrypted External Hard Drive



* The DL4 FE has been designed for FIPS 140-3 Level 3 and is being tested by an accredited NIST lab. The product is in process for certification and is officially listed by NIST, MIP and/or IUT list dependent on the current stage.

Table of Contents

Table of Contents **2**
At A Glance **4**
Introduction 4
About the DL4 4
General operation of the encryption 4
Updating Your Device 4
Product Specifications 4
Getting Started **6**
Tap with precision to input data 6
Tap instead of softly touching - different than a smartphone 6
Randomized key placements 6
Best Practices 6
Initializing and Connecting Your DL4 7
Disconnecting Your DL4 8
Additional Windows Configuration Changes **9**
Disabling Windows 10 Power Save 10
Disabling Windows 10 Selective Suspend 10
Formatting Your DL4 **11**
Selecting the Correct File System 11
Formatting Your DL4 on Windows 11
Formatting Your DL4 on macOS 13
Linux Compatibility and Configuration **14**
Features **16**
Administrator Menu 16
User Menu 17
Accessing the Onboard Administrator or User Menu 17
Using the Administrator Menu **18**
Change Password 18
Set User 18
Step-by-step Process to Set User 19
Step by step process for USER configuration 20
Access User data as an Admin 20
Assist a user that forgot their password 20
SafeConsole 21
Zeroize Drive 21
Self Destruct 23
Password Complexity 24
Password Length 24
Auto-Lock Time 25
Touch Sounds 25
Brightness 25

©2024 DataLocker Inc. All rights reserved.

Read-Only Mode 25
Language 26
Touch Calibration 26
DL4 is not correctly taking input 26
Using the User Menu 27
Change password 27
Auto-Lock Time 27
Touch Sounds 27
Brightness 28
Language 28
SilentKill Code 28
Generating a SilentKill Code 28
Registering Your DL4 to SafeConsole 29
Using a SafeConsole Managed Device 30
Unlocking in SafeConsole Mode 30
Locking Your Managed DL4 31
Manually Locking your DL4 31
Setting your DL4 to Automatically Lock 31
Standalone Logins 32
Requesting Standalone Logins 32
Using Standalone Logins 33
Password Reset 33
Unlocking In Read-Only Mode 34
Changing the Unlock Message 34
Minimize Control Panel on unlock 34
Restricted Files Notifications 35
Scanning your Device for Malware 35
Restoring or Deleting a Quarantined File 35
Using ZoneBuilder 36
Reformat Using DataLocker Control Panel 36
Sanitize 36
Device Information 37
Before Unlocking 37
After Unlocking 37
Getting Help 39
Document Version 39
Notices 39
Disclaimer 39
Patents 39
FCC Information 39

©2024 DataLocker Inc. All rights reserved.

At A Glance

Introduction

Congratulations on your purchase of the DataLocker DL4 FE (FIPS Edition) hardware encrypted external hard drive.

Although the DL4 FE is designed with user friendliness at its core, it is recommended that you review this guide to ensure that you become fully acquainted with your DL4 and make the most of all of its features.

About the DL4

The DL4 FE is a FIPS 140-2 Level 3 certified device built around a powerful AES 256-bit cryptographic hardware architecture that then adds layer after layer of security with automated policies that intelligently change its security posture based on its location, how it's being used, and the type of data being stored on it. Available as a SSD or a more economical HDD, the DL4 FE meets the strictest security requirements while offering large-capacity storage (up to 15.3 TB) and an easy-to-use touchscreen for setup and use. A powerful addition to the DataLocker line of securely managed solutions, the DL4 FE continues our proud tradition of providing Simply Secure™ solutions, plus it's backed by a limited 3-year warranty. The DL4 is fully cross-platform compatible and OS agnostic. With no software or special drivers required, works with Windows, Linux, and macOS.

General operation of the encryption

Your DL4 utilizes a hardware encryption engine to encrypt and decrypt data that you store on the device. When your device is plugged in and powered on, you will authenticate with the onboard system using your password to enable the encryption and use your data. When you lock, power off or disconnect your device, the data is stored in an encrypted state.

Updating Your Device

Updated software and documentation are freely available for download at our website:

- Latest device updates - **http://datalocker.com/device-updates**
- Documentation and support - **https://support.datalocker.com**

Important: Only the latest device updates should be applied to the device. Downgrading the device to an older software or firmware version is not supported and can potentially cause a loss of stored data or impair other device functionality. The latest device updates will always be available at the link above.

Product Specifications

Specification	Details
Capacity*	500GB, 1TB, 2TB, 1TB SSD, 2TB SSD, 4TB SSD, 7.6TB SSD, 15.3TB SSD
Speed**	USB C: - 150MB/s Read, 100MB/s Write USB 3.2: - 150MB/S Read, 100MB/s Write USB 2.0: - 40MB/s read, 20MB/s write

©2024 DataLocker Inc. All rights reserved.

Dimensions	120mm(L) x 75mm(W) x 23mm(D)
Weight	Approximately 0.85 - 1.1 lbs / 385 - 500 Gram
Water Resistant***	IP64
Operating System Compatibility	Windows, macOS, Linux Note: SafeConsole managed DL4 requires Windows 7+. Managed DL4 will require a Standalone logins for use on macOS and Linux.
Operating Temperature	0°C - 45°C
Storage Temperature	-20°C - 60°C
Long Term Storage Temperature (More than 1 week)	-20°C - 40°C
Warranty	3 years Limited
Interface	USB-C on the device, compatible with USB 3.2, USB 2.0 (8 TB drives and under) (USB-C to USB-A and USB-C to USB-C cables included)

* Advertised capacity is approximate. Some space is required for onboard software.
** Speed varies with host hardware, software, and usage. Tests were performed on 1TB HDD model.
*** Device should be completely dry before use.

©2024 DataLocker Inc. All rights reserved.

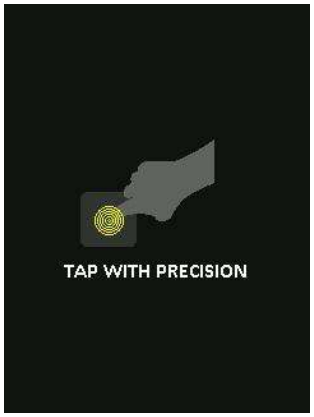
Getting Started

Tap with precision to input data

The DL4 allows you to navigate its durable screen very accurately using a pointy, non-puncturing object of any material as a stylus. You can use the tip of your finger, a retracted ballpoint pen, or even the edge of a plastic card, making input available and stable in any situation. The screen uses a resistive technology that takes input from precise mechanical presses/taps. In the password entry, a touch indicator marks where the device has detected the tap. For the input to be successful, most of the indicator needs to appear over the expected target character.

Tap instead of softly touching - different than a smartphone

Note that entry on a DL4 is different from your smartphone touch screen that uses the presence of conductivity such as the moisture of your finger or a capacitive stylus to take input.



As an instruction, an animation is displayed during startup. You can skip the animation by tapping anywhere on the screen.

Randomized key placements

The input keys of the password entry screen are randomized for each use. The randomization will leave the row of letters in order, but the different rows will shift positions. The randomization is to guard against smudge attacks, where an attacker analyses the fingerprint patterns on the device. It also helps against sneak peek attacks if someone gets a glance at the password entry.

Best Practices

- The DL4 is IP64-rated but must be completely dry before connecting to a computer.
- Only connect the DL4 to certified USB ports. The DL4 has a minimum power requirement of 5 Volts and 1A current drawn from the USB port.
- Safely eject the DL4 from the operating system before removing it. For more information, see **Disconnecting your DL4**.
- Use a strong password and be sure to remember it. Remote password resets can be enabled if the device is managed by SafeConsole.
- Use the correct file system based on your operating system and file needs. See **Formatting your DL4** for more information. The DL4 comes preformatted with the exFAT file system.

©2024 DataLocker Inc. All rights reserved.

Initializing and Connecting Your DL4

1. Connect the DL4 to your computer with the included USB cable.
2. The device will display “PERFORMING SELF TEST” and then will display a DataLocker loading screen.
3. You will then be prompted to create a password. Tap OK to continue.



4. Your DL4 will show an “Enter New Password” prompt. Enter a desired password and then tap the -button. Tap 123 to swap the keyboard to numbers and special characters. Tap ABC to swap back to letters.

Note: Linear and repetitive passwords are not supported and passwords must contain a MINIMUM of 8 characters. It is recommended that you use a combination of letters, numbers and special characters for your password.
Some examples of invalid passwords are:
‘78901234’, ‘43210987’, ’12345678’, ‘1111111’



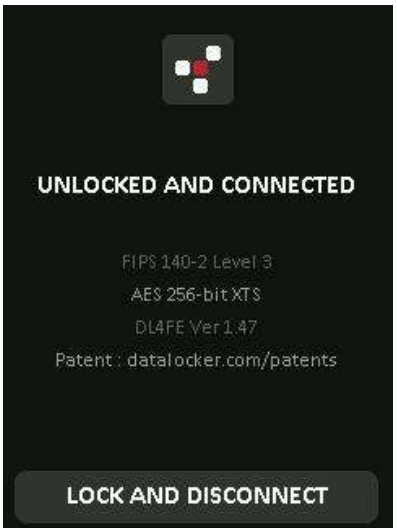
5. Confirm your password from Step 4 and tap the -button.
   If the confirmed password does not match the password entered in Step 4, the device will ask you to enter a new password and to confirm the password again. This process will repeat itself until the passwords match each other.

©2024 DataLocker Inc. All rights reserved.

6. After the device password is input, the connect screen is shown. Tap Connect to connect the DL4 instantly. Otherwise, the device will automatically connect to the computer after 10 seconds. Selecting Read-Only Mode will connect the device with read-only access - allowing data to be read from the device, but not modified or deleted. Tapping the -icon on the screen will take you to the administrator menu. See **Using the Administrator Menu** for more information. Tap the globe to change display language, you confirm the language selection when you tap Connect.



7. After the device successfully connects, the DL4 will show the Unlocked and Connected-screen with a Lock and Disconnect option available. A volume labeled “DataLocker” will be mounted to the computer and be available for use. You can now work with the device as if it was a standard storage device in your computer. All data is transparently encrypted by the hardware when you store it on the DL4.



Note: Tapping Lock and Disconnect will disconnect the DL4 drive from the computer. To prevent data loss or damage to the disk, it is recommended that the DL4 drive be properly ejected from the operating system. For more details, see **Disconnecting Your DL4**.

Disconnecting Your DL4

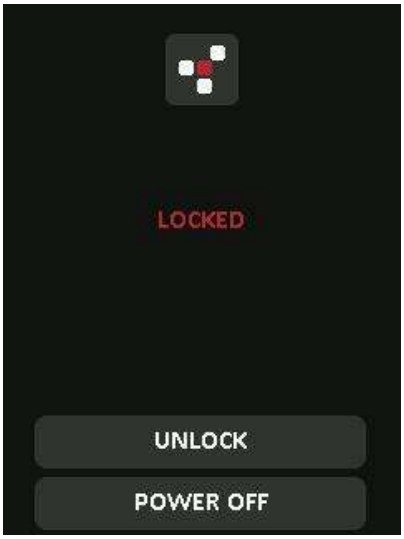
To prevent loss or corrupted data, it is recommended that you properly eject the DL4 drive when you’re finished using it. The best practice is to use your operating system’s Safely Remove Hardware or Eject function before you

©2024 DataLocker Inc. All rights reserved.

power down or detach the DataLocker DL4 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 DL4 from Windows. Your DL4 will automatically lock when ejected.
3. Tap Power Off on your DL4 and unplug from the computer. Tap Unlock to start a new session.



macOS Users

1. a. Click the Eject button that corresponds with the DataLocker DL4

OR

1. b. Drag the drive to the trashcan in the macOS dock. Note: The trash can will transition to an eject button while dragging the drive.
2. Once the drive has been ejected from macOS, press Lock and Disconnect on the DL4 drive.
3. Tap Power Off on your DL4 and unplug from the computer. Tap Unlock to start a new session.

Additional Windows Configuration Changes

By default, Windows 10 attempts to shut off USB devices after a set period of inactivity. If the DL4 is put into this low power state, the drive will automatically lock the drive and require re-authentication.
It is recommended that you perform the steps below to ensure the best DL4 user experience on Windows.

Disabling Windows 10 Power Save

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

1. Log in as a local administrator on your computer.

©2024 DataLocker Inc. All rights reserved.

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.

2. Unlock your DL4 device. If your device is being managed by SafeConsole, launch the client on your computer. See **Initializing and connecting your DL4** for more information.
3. Right click the Start button, and select "Device Manager".
4. Click on the arrow next to "Universal Serial Bus controllers".
5. Right click on "USB Mass Storage Device".
6. Click "Properties".
7. Click the "Power Management" tab.
8. Uncheck "Allow the computer to turn off this device to save power".
9. Click OK and close the "Device Manager" window.

Disabling Windows 10 Selective Suspend

1. In the search box on the taskbar, type control panel.
2. Click and Open Control Panel.
3. Click on Hardware and Sound.
4. Click on Power Options.
5. Click the Change plan settings link for the plan you're currently using.
6. Click the Change advanced power settings link.
7. Click (+) next to "USB settings".
8. Click (+) next to "USB selective suspend setting".
9. Select "Disabled" from the drop-down menu.

NOTE: If you are using a device with a battery (ie. Laptop or Tablet), you will need to set this for On Battery and Plugged in.

10. Click OK.

Formatting Your DL4

Selecting the Correct File System

Your device is formatted as exFAT from the factory.
The DL4 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:

©2024 DataLocker Inc. All rights reserved.

exFAT
- Pros: No file size limitations.
- Cons: Not supported by legacy operating systems.

NTFS
- Pros: No file size limitations.
- Cons: Limited cross-platform compatibility - Windows, macOS (read-only), and Linux (read-only).

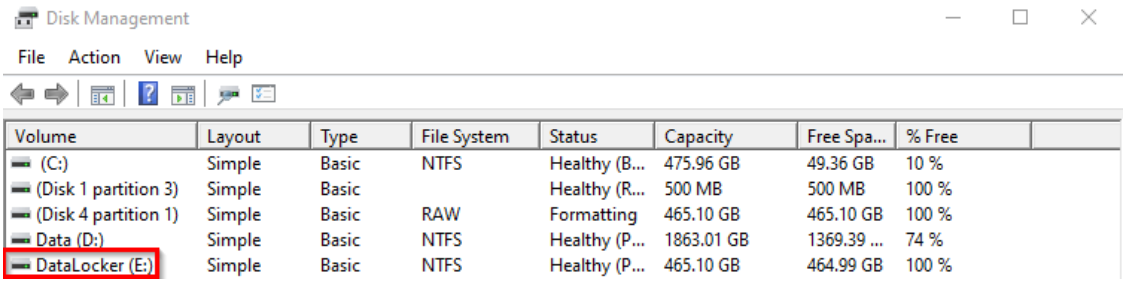
Note: Reformatting your DL4 drive will erase all your files but will not erase your device password and settings. As such, formatting should not be used as a method of securely erasing files. To securely erase your files, perform a Zeroize function. For more information, see the **Zeroize Drive** section.
Important: Before you reformat the device, back up your drive to a separate location, for example, to cloud storage or your computer.

Formatting Your DL4 on Windows

1. Connect the DL4 to the computer and log in. See **Initializing and Connecting your DL4** for more information.
2. In the search box on the taskbar, type control panel.
3. Click and Open Control Panel.
4. Click on System and Security.
5. Click on Create and format hard disk partitions.

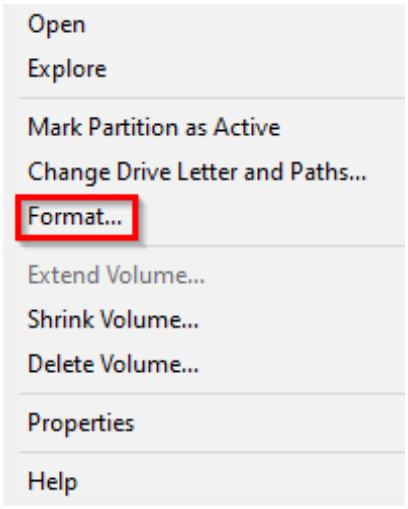


6. Right click on the drive letter that corresponds to your DL4. This example shows (E:).

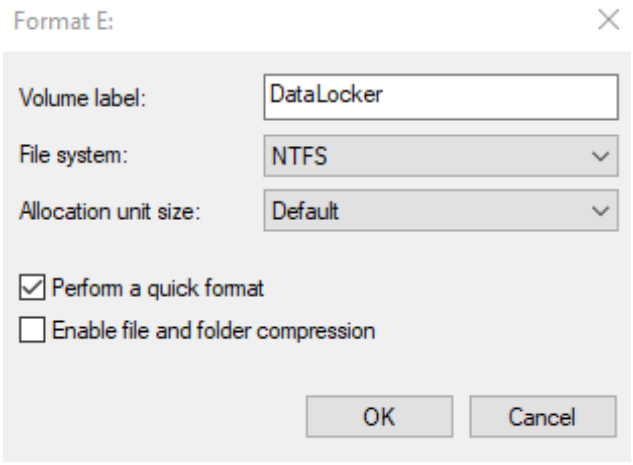


7. Select Format.

©2024 DataLocker Inc. All rights reserved.

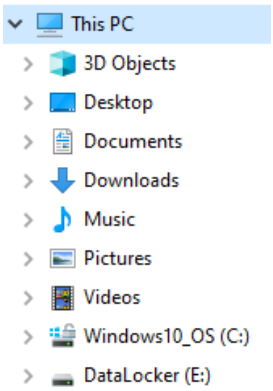


8. Choose an appropriate 'Volume Label' and 'File system'. Click OK.



9. You will be warned that all data will be erased and asked if you would like to continue. Click OK.

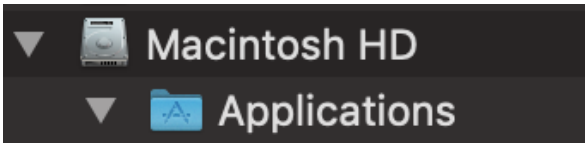
When finished, your DL4 will available under This PC.



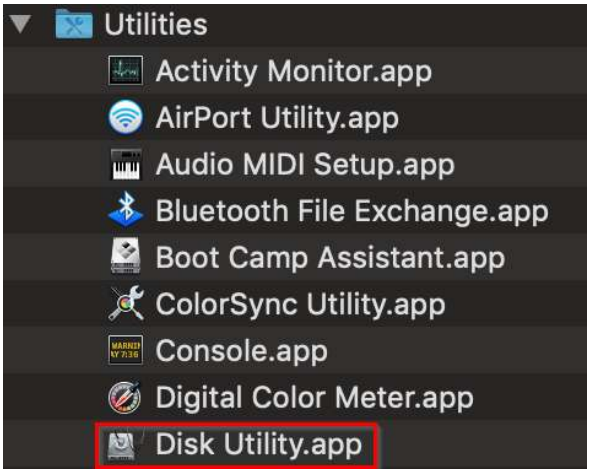
©2024 DataLocker Inc. All rights reserved.

Formatting Your DL4 on macOS

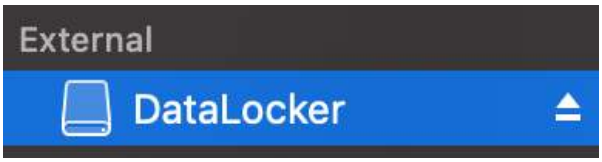
1. Go to Applications under your Finder.



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



3. Select the unformatted DL4 disk.



4. Click the Erase tab at the top of the screen.

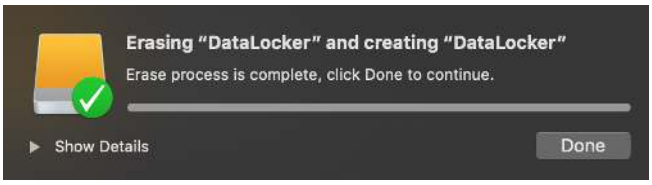


5. Rename the disk label to “DataLocker” and choose a file system.

©2024 DataLocker Inc. All rights reserved.



6. Click Erase. The drive will begin formatting.



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



8. Click Done. Your formatted DL4 should now appear under Devices.

Linux Compatibility and Configuration

The DL4 is platform-independent, 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
```

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'
```

©2024 DataLocker Inc. All rights reserved.

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, 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:

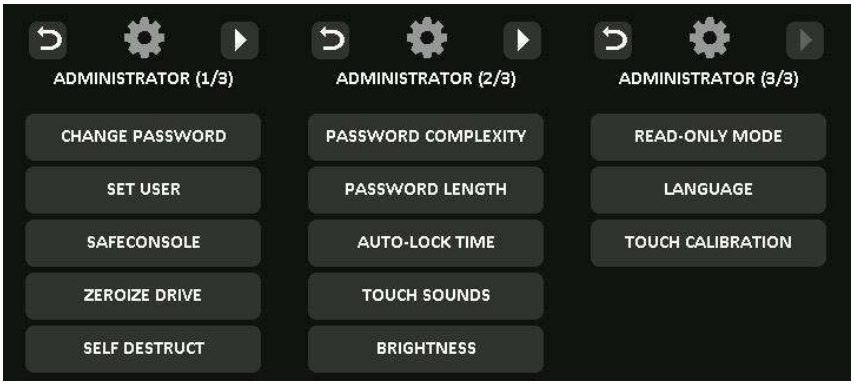
```
# e2label /dev/sdb1 /DataLocker
```

©2024 DataLocker Inc. All rights reserved.

Features

Administrator Menu

- Tap the -icon when you have unlocked the DL4 to access the Administrator Menu.
- Your configurations are saved when you connect the DL4.



Menu Option	**Details**
Previous Menu/Back Button	Tap to go back to the previous menu screen and save the current settings.
Next Menu/Forward Button	Tap to go forward to the next menu screen.
Change Password	Change current administrator password.
Set User	Configure a user profile for use on your DL4. Only available to administrator.
SafeConsole	Used to Enable SafeConsole functionality for your DL4. Only available to administrator.
Zeroize Drive	Zeroize the device. Only available to administrator.
Self Destruct	Used to configure self-destruct counters and methods. Only available to administrator or for the device user when managed by SafeConsole.
Password Complexity	Enable various options for increasing password strength. Only available to administrator.
Password Length	Set the acceptable minimum password length. Only available to administrator.
Auto-lock Time	Modify the length of time before your device automatically locks.
Touch sounds	Enable or disable touch sounds.

©2024 DataLocker Inc. All rights reserved.

Brightness	Change the level of brightness for your device's touch screen.
Read-Only Mode	Enable or disable forced read-only mode. Only available to administrators.
Language	Set preferred Language for the profile.
Touch Calibration	Calibrate the touch screen interface.

User Menu

NOTE: This menu is only accessible after creating a user in the administrator menu. The User profile is not available if SafeConsole is enabled for the device.

Menu Option	**Details**
Previous Menu/ Back Button	Tap to go back to the previous menu screen and save the current settings.
Change Password	Change current user password.
Auto-lock Time	Modify the length of time before your device automatically locks.
Touch sounds	Enable or disable touch sounds.
Brightness	Change the level of brightness for your device's touch screen.
Language	Set preferred Language for the profile.

Accessing the Onboard Administrator or User Menu

For detailed menu information, see **Using the Administrator Menu** OR **Using the User Menu**.

NOTE: If your drive was connected to your computer, disconnect your DL4 (See **Disconnecting Your DL4**), unplug and reinsert the USB cable to your computer.

1. Connect the DL4 to your computer with the included USB Cable.
   OPTIONAL: If the USER profile is enabled, you must tap ADMIN OR USER when your DL4 loads.
2. Enter your password on the "ENTER PASSWORD" screen and tap the -button.
3. Tap the -icon to enter the Onboard Menu.

NOTE: After entering the password, the connect screen is briefly shown for 10 seconds. To enter the onboard administrator menu, you must tap the -icon quickly.

©2024 DataLocker Inc. All rights reserved.



Using the Administrator Menu

The administrator menu has various options and features spread over three screens. The administrator menu helps administrators configure various functions that DL4 offers. The available administrator menu features and settings are explained in their own sections below.
Once inside the administrator menu, the forward(2) and back(1) button can be used to navigate through the administrator menu. The Back button can also be used to save and exit out of the administrator menu to get back to the connect screen.

NOTE: Highlighted (white) text on a selection button denotes the current selection. Upon changing the values on the various functions, the DL4 automatically saves the changed value when the Back button is pressed. Your configurations are finally confirmed when you connect the DL4 during the same usage session.



Change Password

This option allows the administrator to change the current administrator password. When setting up a device, the administrator creates a password and if they desire to change it later this is where they will update the password. Follow these steps to change the DL4 administrator password.

1. From the administrator menu, tap Change Password.
2. Enter the New Password and tap the -button.
3. Re-enter the password to confirm and tap the -button. You must confirm using the same password you entered in Step 2.
4. Upon successful completion, the device defaults to page 1 of the administrator menu.

Set User

This allows the administrator to either Enable or Disable a user role. When a user password is created your DL4 will show a login selection screen upon the next DL4 connection. If User is selected upon login, your DL4 will force the user to create a user unlock password. The user will use this password to unlock the device. The DL4 user has

©2024 DataLocker Inc. All rights reserved.

a limited feature set compared to the administrator. For detailed information, see **Using the User Menu**. To create a User profile for your DL4, follow the below steps.

NOTE: The User profile is not available if SafeConsole is enabled for your DL4.

Step-by-step Process to Set User

1. From the administrator menu, Tap Set User.
2. Tap Enable. (Option is set to Disable as default).



3. Tap Back from upper left to select Enable and exit.
4. Your DL4 will show a “User has been set” prompt upon successful creation of the user. Tap OK.



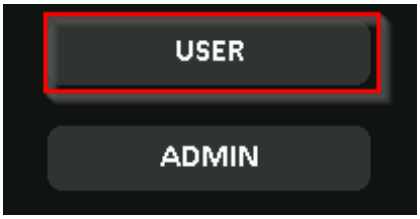
5. Your DL4 will go back to the administrator menu. Proceed to connect the DL4 to confirm your setting and then lock, and power off. On the next power on the role selection will be available.

©2024 DataLocker Inc. All rights reserved.

Note: The password for this user profile will be set when the device is next plugged into a workstation and the User option is selected for log in. Detailed steps for the user profile configuration are below. The User login will have its own User menu. For detailed information, see **Using the User Menu**.

Step by step process for USER configuration

1. Plug your device into the computer.
2. Tap User when prompted to select login mode.



3. Tap OK on the “Please create your password” screen.
4. Enter desired password on the “Enter New Password” screen. Tap the -button.
5. Confirm the new password and tap the -button. You must confirm using the same password you entered in Step 4.
6. Tap Connect to connect the DL4 instantly or wait for 10 seconds for DL4 to automatically connect to your computer.

Note: The User Menu can be accessed by tapping the -icon instead of tapping Connect. For detailed information, see **Using the User Menu**.

Access User data as an Admin

1. Power on.
2. Select Admin role, unlock with admin password.
3. Connect. User data is accessible on the private partition.

Assist a user that forgot their password

The scalable method for remote password resets with an audit trail is available when managing DL4 with SafeConsole. If the DL4 is not centrally managed and a User role is activated, the following procedure can be used.

1. User forgets the password.
2. Power off/on. Select Admin role, unlock with admin password. Tap COG-icon -
3. Tap Set User and tap Disable. Connect, power off/on.
4. Select Admin role, unlock again with Admin password.
5. Set User to Enable. Connect, power off/on
6. Select User role, enter and confirm the new User password. Connect to confirm and access your data.

©2024 DataLocker Inc. All rights reserved.

SafeConsole

This option enables SafeConsole management for your DL4. SafeConsole is a central management console used to optionally manage DL4 devices. Managed DL4s 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** / (913)310-9088
SafeConsole offers several key features including audit logging, anti-malware services (license sold separately), remote password reset, and more!

Enabling SafeConsole

1. From the administrator menu, Tap SafeConsole.
2. Tap Enable.
3. Tap Back from the upper left menu to save and exit to the administrator menu.
4. See **Registering your DL4 to SafeConsole** to complete registration.

Zeroize Drive

This feature allows the administrator to zeroize the drive. Performing this action deletes all the data, removes the user and administrator passwords, and deletes the SilentKill Code. The Data Encryption Key (DEK) will also be wiped and regenerated.
NOTE: Zeroize will retain the configuration set by the administrator.

There are two options available when you zeroize the drive:

A. Zeroize - Tap Zeroize Drive from the administrator menu and follow the on screen steps.
B. Factory Initialize - Tap & hold Zeroize Drive in the administrator menu for 5 seconds. Your device will show a “Factory Initialize” prompt.

Although both of the Zeroize processes reset the DL4 there’s a slight difference. See the chart below for the difference:

	A.Zeroize	**B.Factory Initialize**
Feature	**Tap & release Zeroize**	**Tap & hold Zeroize for five seconds**
Administrator Password	Deleted	Deleted
User Password	Deleted and Disabled	Deleted and Disabled
SilentKill Code	Deleted	Deleted
Configuration by administrator (menus)	Kept	Reset
Drive Data	Deleted	Deleted

For assistance with either process, please see the steps outlined below:

How to Zeroize your DL4

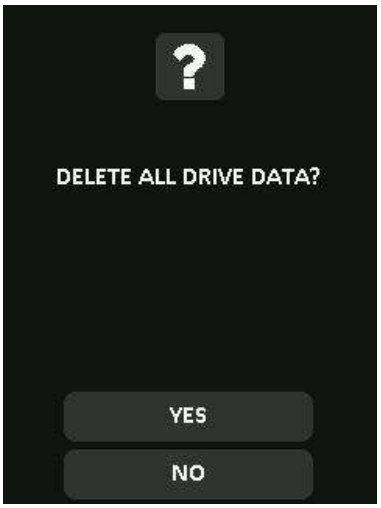
1. Use the table above to assist with the decision if you want to A.Zeroize or B.Factory Initialize,

©2024 DataLocker Inc. All rights reserved.

2. When your device asks for “Zeroize Drive” (A) or “Factory Initialize” (B), tap Yes. Selecting No will cancel the Zeroize process.

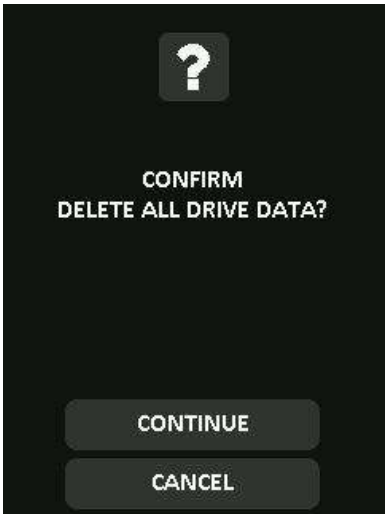


3. When your device asks for “Delete ALL drive data?”, tap Yes. Selecting No will cancel the Zeroize process.



4. When your DL4 shows the “Confirm Delete all drive data?” prompt, tap Continue. Selecting Cancel will cancel the Zeroize process.

©2024 DataLocker Inc. All rights reserved.



5. Upon successfully completing the Zeroize process, you will see “Please initialize and reformat the drive”. Tap OK to continue.



NOTE: You must now follow the initialization process as shown in the **Initializing and Connecting Your DL4** section of this manual.

Self Destruct

The self destruct action helps prevent brute force attacks by triggering when an individual inputs an incorrect password too many times.
This feature allows the administrator to set a threshold of incorrect password attempts for the DL4 before the Self Destruct occurs. The administrator can also configure the self-destruct to destroy the data, encryption keys, and settings OR destroy the device (and data) when the defined number of allowed password attempts is reached. The default number of allowed password attempts is 10 and can be increased up to 50 but not lower than 10. When enabling the feature, there are two types of self destruct options to select. Please refer to the below table for more details.

©2024 DataLocker Inc. All rights reserved.

NOTE: Incorrect password attempts from both users and administrators are calculated cumulatively towards the incorrect password attempts self destruct counter. The counter will reset upon correct password attempt.



A. Destroy Device - Your device is killed completely and all device data, encryption keys, passwords are destroyed and cannot be recovered. The device CANNOT be initialized again, the destruction is permanent.

B. Destroy Data (default selection) - Your device is wiped completely and all device data, encryption keys, passwords are destroyed and cannot be recovered. The device needs to go through the initialization process again.

Deleted asset	**B.Destroy Data (default)**	**A.Destroy Device**
Administrator Password	Deleted	Deleted and DL4 cannot be used anymore
User Password	Deleted and Disabled	Deleted and DL4 cannot be used anymore
SilentKill Code	Deleted	Deleted and DL4 cannot be used anymore
Configuration by administrator (menus)	Kept	Deleted and DL4 cannot be used anymore

Password Complexity

This feature allows the device administrator to configure the password requirement, increasing password strength. There are 3 options that can be used in any combination.
- Numeric - Will require numeric characters be included in password when enabled.
- Alphabet - Will require alphabet characters be included in password when enabled.
- Special - Will require special characters be included in the password when enabled.

Password Length

The device administrator can use this feature to set the minimum required password length. It can be set between the minimum of 8 to a maximum of 64. Tapping Default will reset the counter to “8”.
To modify minimum password length, follow these steps:

1. Tap the Required Password Length option from the administrator menu.
2. Tap (+) to increase the length and (-) to decrease the length.
3. Tap Back from the upper left to save and exit the administrator menu.

©2024 DataLocker Inc. All rights reserved.

Auto-Lock Time

This feature is disabled by default but can be enabled by the administrator and the user. Auto-lock will disconnect the drive once it is idle (i.e. zero activity) for the configured amount of time. The amount of idle time required to time out the device is configurable from 10 to 720 minutes.
To enable auto-lock, follow these steps:

1. Tap Auto-Lock Time from the administrator menu.
2. Configure the desired number of minutes the device can remain unlocked and idle.

NOTE: You can increase or decrease this limit in increments of 5 or 60 minutes

3. Tap Enable.
4. Tap Back from the upper left to save and exit to the administrator menu.

Touch Sounds

The DL4 touch sounds are enabled by default.
To disable these sounds, follow these steps:

1. Tap the Touch Sounds feature from the administrator menu.
2. Tap the Disable button.
3. Tap Back from the upper left to save and exit to the administrator menu.

Brightness

Your DL4 screen brightness can be adjusted via this feature. The default value is 10.
To change the value, follow these steps:

1. Tap the Brightness option from the administrator menu
2. Tap (+) to increase the brightness and (-) to decrease the brightness.

NOTE: The minimum brightness value can be 1 and maximum is 30.

3. Tap Back from the upper left to save and exit to the administrator menu.

Read-Only Mode

Administrators can select the Read-Only Mode to globally enforce the DL4 to always unlock in read-only mode. Enabling this option will also enforce read-only access for the User profile (if the user profile is enabled). Once the Read-Only Mode is enabled, data can only be read from the DL4 and no data can be written or modified.
To enable Read-Only Mode, follow these steps:

1. Tap the Read-Only Mode feature from the administrator menu.
2. Tap Enable.
3. Tap Back from the upper left to save and exit to the administrator menu.

NOTE: The administrator and the user can each set Read-Only Mode for a single login by tapping Read-Only Mode after entering the password. The Read-Only Mode will enforce this functionality for every login.

©2024 DataLocker Inc. All rights reserved.

Language

A total of 4 languages can be selected. The selected language will be used for all on board menu prompts. The available languages are:
- English
- French
- German
- Spanish

To set a preferred language, follow these steps:

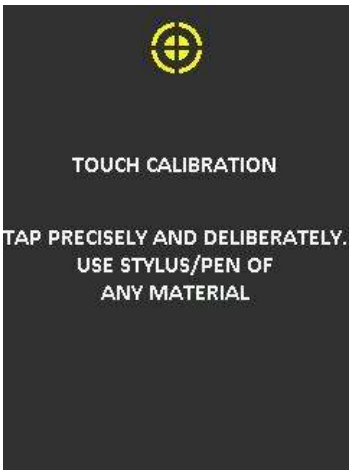
1. Tap the Language option from the administrator menu.
2. Tap your desired language.
3. Tap Back from the upper left to save and exit to the administrator menu.

NOTE: The administrator and User both can select their own preferred language from their respective menus.

Touch Calibration

Your DL4's touchscreen interface can be manually calibrated when needed. To calibrate the interface follow the below steps. Proceed with care and have a stylus/pen of any material avaible. The precision of the calibration highly influences how accurately the device receives input.

1. Tap the Touch Calibration option from the administrator menu.
2. You will now be prompted to touch your DL4 screen in 3 various spots one after the other. Tap the on screen Target icon each time you are prompted using your stylus.



3. Once complete, your DL4 will return to the administrator menu.

DL4 is not correctly taking input

If your DL4 is not correctly detecting your taps on the screen, it can be due to a failed Touch Calibration. It is possible to enter the Touch Calibration without entering a password. Tap & hold the screen for exactly 5 seconds (use a timer if needed) when the DataLocker logo with a progress bar under it is displayed during startup. Follow the **Touch Calibration** steps.

©2024 DataLocker Inc. All rights reserved.

Using the User Menu

Once inside the User menu, the back button can be used to navigate back to the connect screen. The back button can also be used to save and exit out of any of the option menus to get back to the User menu.

NOTE: Highlighted (white) text on a selection button denotes the current selection. Upon changing the values on the various functions, the DL4 automatically saves the changed value when the Back button is pressed. Your configurations are finally confirmed when you connect the DL4 during the same usage session.



Change password

This option allows the user to change the current user password. When setting up a user profile, the user password is created. If the user desires to change it at a later time, this is where they will update the password.

1. Tap the Change Password option from the User menu.
2. Enter the New Password and tap the -button.
3. Re-enter the password to confirm and tap the -button again.
4. Upon successful completion, the device defaults to the User menu.

Auto-Lock Time

This feature is disabled by default but can be enabled by the DL4 administrator or user. Auto-lock will disconnect the drive once it is idle (i.e. zero activity) for the configured amount of time. The amount of idle time required to time out the device is configurable from 10 to 720 minutes.
To enable auto-lock, follow these steps:

1. Tap Auto-Lock Time from the user menu.
2. Configure the desired number of minutes the device can remain unlocked and idle.

NOTE: You can increase or decrease this limit in increments of 5 or 60 minutes.

3. Tap Enable.
4. Tap Back from the upper left to save and exit to the user menu.

Touch Sounds

The DL4 touch sounds are enabled by default.
To disable these sounds, follow these steps:

1. Tap the Touch Sounds feature from the user menu.
2. Tap the Disable button.
3. Tap Back from the upper left to save and exit to the user menu.

©2024 DataLocker Inc. All rights reserved.

Brightness

Your DL4 screen brightness can be adjusted via this feature. The default value is 10.
To change the value, follow these steps:

1. Tap the Brightness option from the user menu.
2. Tap (+) to increase the brightness and (-) to decrease the brightness.

NOTE: The minimum brightness value can be 1 and maximum is 30.

3. Tap Back from the upper left to save and exit to the user menu.

Language

A total of 4 languages can be selected. The selected language will be used for all on board menu prompts. The available languages are:
- English
- French
- German
- Spanish

To set a preferred language, follow these steps:

1. Tap the Language option from the user menu.
2. Tap your desired language.
3. Tap Back from the upper left to save and exit to the user menu.

NOTE: The administrator and user both can select their own preferred language from their respective menus.

SilentKill Code

A SilentKill code can be set up by the DL4 administrator, and also when managed. This code can be entered during the login process instead of the password. When this code is entered, the device will follow the configured Self Destruct process. A brief description of each Self Destruct process can be found below. Please review the **Self Destruct** portion of this guide for more information.

If Destroy Data is configured, the encryption keys, password(s), and any data on the device is deleted. The SilentKill code then becomes the DL4 administrator password. NOTE: The device must be reformatted after this process is completed.

If Destroy Device is configured, your DL4 will be rendered inoperable after the SilentKill code is used during login. When the device is managed by SafeConsole a configured Destroy Device will result in a Destroy Data process as the management overrides the command.

Generating a SilentKill Code

1. Enter the administrator password and navigate to the administrator menu. See **Accessing the Onboard Administrator or User Menu**.
2. Tap and hold the Change Password option for 5 seconds and then release.

©2024 DataLocker Inc. All rights reserved.

NOTE: Upon release, the device will display a message. “Silent Kill Code -This code is used to immediately initiate the self destruct process”.

3. Tap OK.
4. Set a Silent Kill Code by entering a desired password.
5. Confirm the code by re-entering the password.
6. The device returns to the administrator menu upon completion.

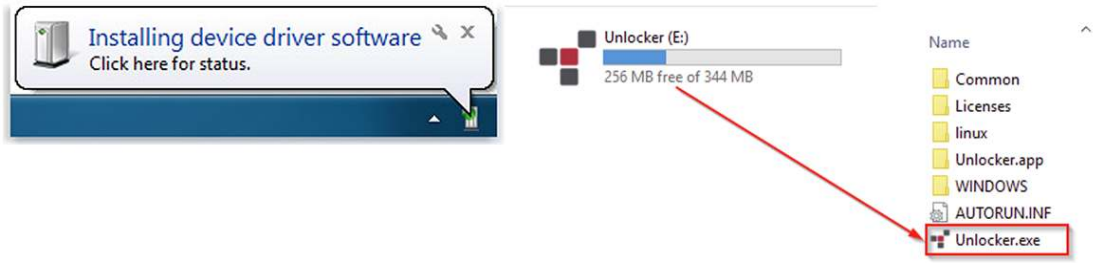
Registering Your DL4 to SafeConsole

Before registering your drive to SafeConsole, make sure SafeConsole is enabled on your DL4. For more information, see **Enabling SafeConsole**. The registration process will begin by allowing the device to communicate with the SafeConsole server. The steps needed to register a DL4 to SafeConsole will depend on the policies that your SafeConsole administrator is enforcing. Not all options will be shown.
A SafeConsole Connection Token will be needed. The SafeConsole Connection Token is obtained by the SafeConsole administrator through the Quick Connect Guide and is usually sent via email.
Users without access to a Management Server, please contact sales: **sales@datalocker.com** / +1(913)310-9088

1. Plug in and log into your DL4. Tap the Connect button. Your DL4 will show a “Waiting…” prompt.

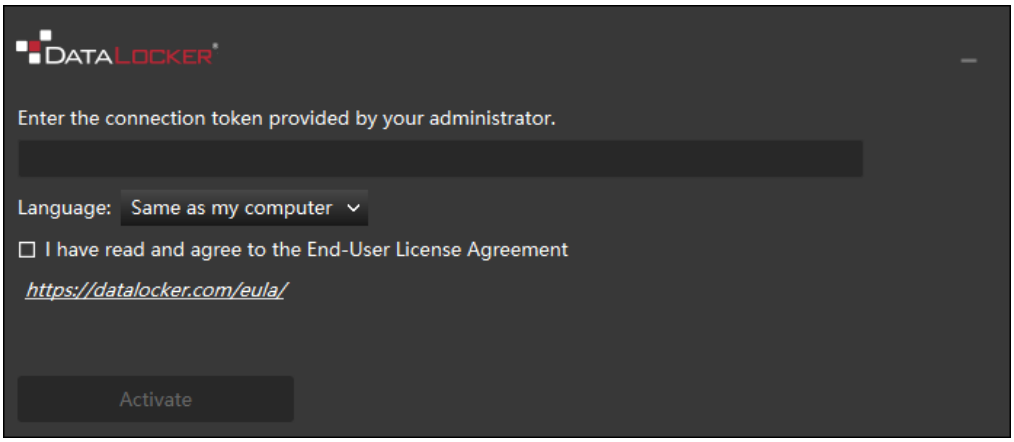


2. On your computer, double-click the “Unlocker” CD drive under “Devices and Drives”.



©2024 DataLocker Inc. All rights reserved.

3. Upon launch, the “Device Setup” page should appear.



4. Enter the SafeConsole Connection Token provided by your SafeConsole administrator and confirm the EULA. Click Activate.
5. Your device will connect to the SafeConsole server.
6. Optionally Enabled Policies - These policies may or may not be enabled by your SafeConsole 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 SafeConsole administrator usually via email.
    - Administrator Registration Approval: The SafeConsole administrator may require their approval to proceed with device registration.
7. Select your desired file system from the “Format” prompt. Click Continue. See **Selecting the Correct File System**.
8. After formatting, your device will show the “Control Panel”. See **Using a SafeConsole Managed Device** for more information.

NOTE: The “Unlocker” client will generate a Password Recovery Code after your next device unlock. It is recommended that your device be disconnected and reconnected to ensure your DL4 Password Recovery Code is saved to the SafeConsole.

Using a SafeConsole Managed Device

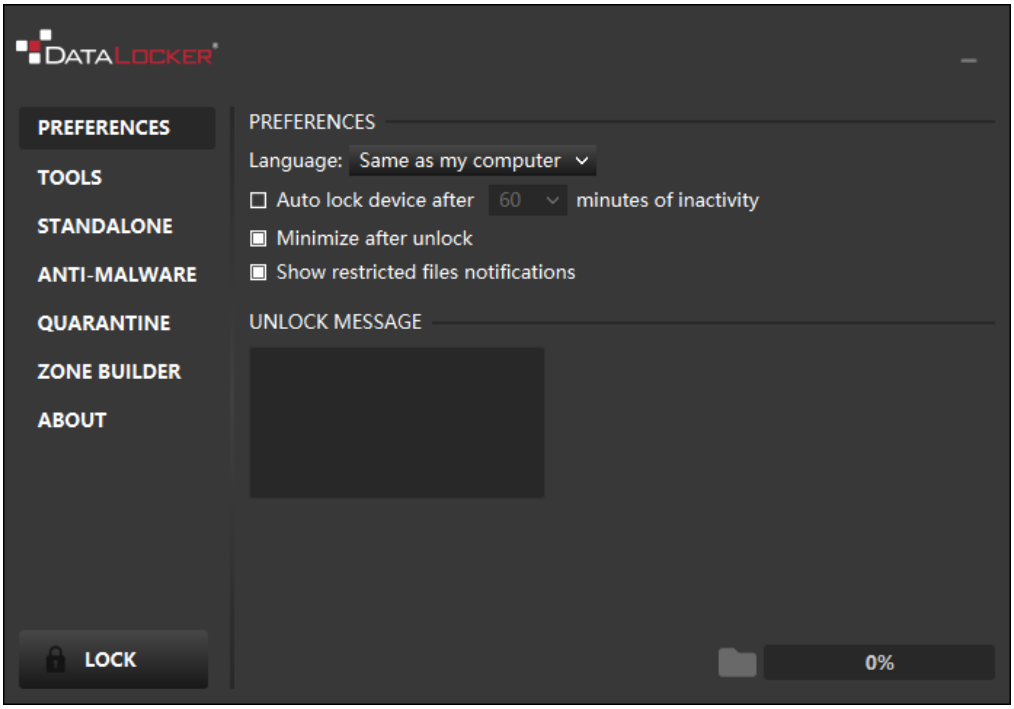
Unlocking in SafeConsole Mode

Once the DL4 is registered to SafeConsole, the Secure Volume can be accessed by following the steps below:

1. Log into your DL4 and tap the Connect button. Your DL4 will show a “Waiting…” prompt.

©2024 DataLocker Inc. All rights reserved.

2. Select the option Unlocker.exe inside of the Unlocker partition that can be found in File Explorer.
3. Click the Unlock button shown on the DataLocker Control Panel.
4. The Secure Volume will be mounted to a separate drive letter on your workstation. The Secure Volume can also be accessed by clicking the Folder Icon in the lower right corner.



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

Locking Your Managed DL4

Lock your device when you are not using it to prevent unwanted access to your secure files on the drive. You can manually lock the device or you can set the device to automatically lock after a specified period of inactivity.

NOTE: If a file or application is open when the device tries to auto-lock, it will not force the application or file to close.

Manually Locking your DL4

1. Click Lock in the bottom left-hand corner of the DataLocker Control Panel to safely lock your device. You can also use the keyboard shortcut: CTRL + L (Windows only), or right click the DataLocker Icon in the system tray and click Lock Device.
2. Tap Power Off on your DL4.

NOTE: Managed devices will automatically lock during use if an administrator remotely disables the device. You will not be able to unlock the device until the SafeConsole administrator re-enables the device.

©2024 DataLocker Inc. All rights reserved.

Setting your DL4 to Automatically Lock

You can configure the device to automatically lock using the DL4 onboard menu (See **Auto-Lock Time**) or by using the Control Panel. If enforced by your SafeConsole administrator, you may be unable to modify this feature. Follow the below steps to configure this automatic lock using the Control Panel.

NOTE: Changing this setting in the Control Panel will be reflected on the DL4 onboard menu and vice versa.

1. Unlock your device and click Preferences in the left sidebar.
2. Click the Checkbox for auto-locking the device and set the time-out to one of the following time intervals: 5, 15, 30, 60, 120, or 180 minutes.

Standalone Logins

Requesting Standalone Logins

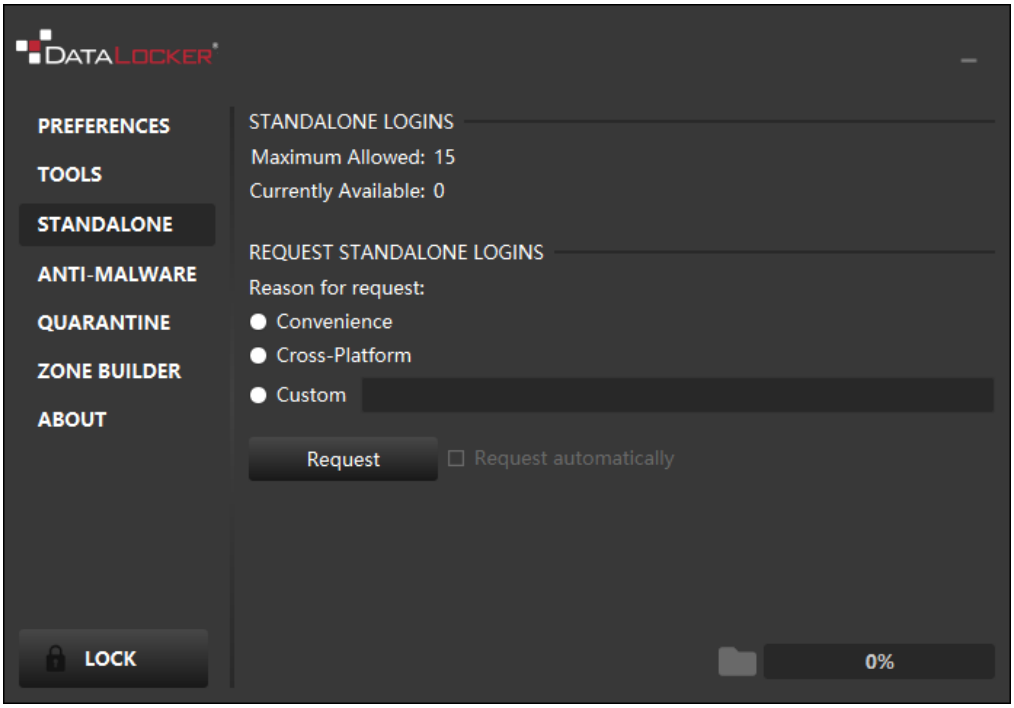
Standalone mode allows the Secure Volume of the DL4 to be accessed by any computer that has support for removable storage without running the Windows Unlocker application. Standalone mode is controlled by a policy that is set by your SafeConsole administrator. If this mode is not available, please contact them to enable this feature. SafeConsole administrators will define the maximum allowed times your DL4 can be unlocked in Standalone mode before the device needs to be returned to a Windows computer to check-in.

To request Standalone logins, perform the following steps on a workstation that has a valid connection to the SafeConsole server:

1. Log into your DL4 and tap the Connect button. Your DL4 will show a “Waiting…” prompt.
2. Select the option Unlocker.exe inside of the Unlocker partition that can be found in File Explorer.
3. Click the Unlock button shown on the DataLocker Control Panel.
4. On the DL4 Control Panel, select the Standalone tab in the left sidebar.
5. Select the reason for the request or enter a custom reason. This information will be sent to the SafeConsole administrator.
6. Click the Request button. You will receive the maximum number allowed.

Note: The Request automatically checkbox can optionally be enabled by your SafeConsole administrator. When checked, the Control Panel will automatically request the maximum allowed Standalone logins after unlocking on a Windows workstation with a valid connection to SafeConsole.

©2024 DataLocker Inc. All rights reserved.



Using Standalone Logins

On the next unlock of your DL4, you can select Standalone after you input your password to unlock in Standalone mode. When in Standalone mode, the Unlocker partition will not be mounted to the host computer and the DataLocker Control Panel will not need to be executed.

1. Connect your DL4 and log in.
2. Tap Standalone at the “Login Mode” prompt.
3. Tap OK when you are prompted with the number of remaining Standalone logins.
4. Tap Connect or wait 10 seconds to utilize the secure partition.

NOTE: This will decrease the Currently Available count of Standalone logins by one.

To continue to use your DL4 in the normal SafeConsole mode, tap SafeConsole in step 2.

Note: The Currently Available number of Standalone logins will be reset to zero if a SafeConsole administrator remotely disables or factory resets your DL4. Currently available will also be set back to zero after a password reset or when the device is blocked by GeoFence.

Password Reset

If your DL4 cannot be unlocked due to a forgotten password, a recovery password can be sent by your SafeConsole administrator.

1. Plug in your DL4 and input the recovery password.
2. Once the password is entered, the DL4 will prompt to change the password.

©2024 DataLocker Inc. All rights reserved.

3. The password should be changed to something secure. For more information see **Initializing and Connecting Your DL4**

NOTE: Each password recovery code can only be used once. Your DL4 must be unlocked in **SafeConsole Mode** with a valid connection to SafeConsole before a new password recovery code can be generated. Failure to do so could cause loss of access to the device and the data on it if the password is forgotten again.

Unlocking In Read-Only Mode

You can unlock your device in a read-only state so that files cannot be altered on your secure drive. For example, when using an untrusted or unknown computer, unlocking your device in Read-Only Mode will prevent any malware on that computer from infecting your device or modifying your files. Managed devices can be forced to unlock in a read-only state by an administrator.

When working in this mode, the DataLocker Control Panel will display the text Read-Only Mode. In this mode, you cannot perform any operations that involve modifying files on the device. For example, you cannot reformat the device, restore applications or edit the Applications List, or edit files on the drive.

To unlock your device in Read-Only Mode through the Control Panel:

1. Plug in and log into your DL4. Tap Connect. Run the Unlocker.exe.
2. Check the Read-Only Checkbox below the Unlock button.
3. Click Unlock. The DataLocker Control Panel will appear with the text Read-Only Mode at the bottom.

To unlock the device in Read-Only Mode from the device:

1. Plug in and log into your DL4.
2. In the connection menu tap READ-ONLY MODE.

NOTE: Unlocking in “Read-Only Mode” from the connection menu also works in **Standalone mode**.

Changing the Unlock Message

The Unlock Message is custom text that displays in the Control Panel when you unlock the device. This feature allows you to customize the message that displays. For example, adding classification labels can help identify which documents can be saved to the device due to company policy. Your SafeConsole administrator can set a pre-defined message or prevent the DL4 user from changing this message.

To change the Unlock Message:

1. In the DataLocker Control Panel, click Preferences in the left sidebar.
2. Type the message text in the Unlock Message field. The text must fit in the space provided (approximately 6 lines and 200 characters).

Minimize Control Panel on unlock

When your device is unlocked, the Control Panel is minimized to the taskbar automatically. If desired, the Control Panel can remain displayed after the user unlocks the device.

To disable Minimize after unlock:

1. In the DataLocker Control Panel, click **Preferences** in the left sidebar.

©2024 DataLocker Inc. All rights reserved.

2. Click the Checkbox for Minimize after unlock.

Restricted Files Notifications

If enabled by your SafeConsole administrator, your device may restrict certain files from being saved to the secure storage. When an affected file is restricted, you will receive a notification containing the file's name. If desired, you can disable these notifications.
NOTE: Affected files will still be restricted when notifications are disabled.

To disable restricted files notifications:

1. Unlock your device.
2. Click Preferences in the left sidebar.
3. Click the Checkbox for Show restricted files notifications.

Scanning your Device for Malware

If enabled by your SafeConsole administrator, the Malware Scanner is a self-cleaning technology that detects and quarantines malware on your device. Powered by the McAfee® anti-virus and anti-malware signature database, and constantly updated to combat the latest malware threats, the scanner first checks for the latest updates, scans your device, then reports and cleans any malware that is found.

Your system administrator may require the anti-malware definition to be updated before the device can be unlocked. In this event, the full anti-malware definition will need to be downloaded to a temporary folder on the local computer before the password can be entered. This can increase the time it takes to unlock the device based on the host computer's networking connection and the size of malware updates needed.

Some things to know about scanning your device:

- The scanner runs automatically when you unlock your device.
- It scans all onboard files (compressed and uncompressed).
- It will report and delete any detected malware.
- (Optional) If your SafeConsole has enabled quarantine, it may quarantine any malware it finds. See **Restoring or Deleting a Quarantined File** for more information.
- The scanner will automatically update itself before each scan to protect you from the latest malware threats.
- An update requires an internet connection. Ensure a minimum of 135 MB of free space on the device to accommodate the downloaded malware signature files.
- Your first update may take a long time to download, depending on your internet connection.
- The date of the last update is displayed in the Control Panel.
- If the scanner becomes too far out of date, it will need to download a large file to bring it back up-to-date.

Restoring or Deleting a Quarantined File

If your SafeConsole administrator has enabled quarantine, you will have the option of restoring or deleting detected malware. This process helps when McAfee® detects a valid document as malware.

©2024 DataLocker Inc. All rights reserved.

NOTE: Depending on the size of infected files, quarantine may not be available. If the file cannot be quarantined it will be deleted and will not be able to be restored using the following process.

If a file is detected as infected a warning dialog will be shown with the option to lock the drive at that time. Quarantined files remain on the device in an encrypted state to prevent further execution.

To view quarantined files:

1. Unlock your device and click Quarantine in the left sidebar.

Selecting a file from the list will display additional details including, Threat Name, Threat Type, anti-malware definition version, and the date of quarantine. After the file is selected files can either be Restored or Deleted.

Restored files will be exempt from automatic scanning while the device is currently unlocked. The file will be scanned during the next unlock or if a manual scan is selected from the Anti-Malware tab. If the anti-malware definitions still determine that the file is infected it will quarantine the file once again.

Deleted files will be permanently deleted.

Using ZoneBuilder

If enabled by your SafeConsole administrator, ZoneBuilder is a SafeConsole feature used to create a Trusted Zone of computers. It can be used to restrict device access to computers within the Trusted Zone.

If your administrator chooses to enable this policy, you may be required to trust your account within the Control Panel.

Trusting your account:

1. Unlock your device and click Zone Builder in the left sidebar.
2. Click Trust This Account.
3. Enter the password for the device and click OK. Your account will now show up in the Trusted Accounts box.

Your account is now in the Trusted Zone of computers. Depending on the policy set by your SafeConsole administrator, you may have restricted device access outside of the Trusted Zone or when offline.
To remove a trusted account, simply highlight the account you wish to remove and click Remove.

Reformat Using DataLocker Control Panel

Important: Before you reformat the device, back up your files to a separate location.

To reformat a device:

1. Unlock your device and click Tools in the left sidebar.
2. Under Device Health, select the file system then click the Reformat Secure Volume button.

Warning: Reformatting your DL4 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, contact your SafeConsole administrator or use **Sanitize**.

Sanitize

Sanitize allows for the contents of the encrypted drive to be securely erased. This is accomplished by erasing the encryption key that the drive uses to access files on the Secure Volume while still retaining the connection to

©2024 DataLocker Inc. All rights reserved.

SafeConsole. This action prevents the need of registering the device back to SafeConsole like after a full device reset.

Warning: Performing this action will completely erase all data on the Secure Volume. This action is permanent.

The ability to sanitize a drive depends on the settings configured by your SafeConsole administrator. If allowed your drive can be sanitized by the following steps:

1. Unlock your DL4 and open the device Control Panel by launching Unlocker.exe.
2. Right click the system tray icon for the Control Panel and select Sanitize Device.
3. Enter the numbers prompted in the dialog box to confirm that all data can be wiped from the drive.
4. The device will reset. Unplug and plug your DL4 back into your workstation.
5. You will need to initialize you DL4, see **Initializing and connecting your DL4** for more information.
6. Log into your DL4 and launch Unlocker.exe. You will be prompted to format the Secure Volume, see **Reformat Using DataLocker Control Panel** for more information.

Device Information

Before Unlocking

To see information about the device without logging into it, plug your DL4 into your PC. Before entering the password, tap the -button.

Device information shown:

- QR Code Serial Number
- Alpha-numeric Serial Number
- Firmware Version
- Capacity
- Certification Logos
- Patent Information

After Unlocking

More information can be obtained after logging into the device and launching the unlocker.exe application.

Use the Capacity Meter, located at the bottom right of the DataLocker Control Panel, to see how much storage space is still available on your device. The green bar graph represents how full the device is. For example, the meter will be completely green when the device is full. The white text on the Capacity Meter displays how much free space remains.

For general information about your device, see the “Device Info” page.

To view device information:

1. Unlock your device and click Device Info in the left sidebar.

The About This Device section includes the following details about your device:

©2024 DataLocker Inc. All rights reserved.

- Model Number
- Hardware ID
- Serial Number
- Software Version
- Firmware Version
- Release Date
- Secure Files Drive Letter
- Unlocker Drive Letter
- Operating System and System administrative Privileges
- Management Console

NOTE: You can click one of the information buttons on the Device Info page to visit the DataLocker website or access more information about legal notices or certifications for DataLocker products.
Hint: Click Copy to copy the device information to the clipboard so that you can paste it in an email or support request.

©2024 DataLocker Inc. All rights reserved.

Getting Help

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

support.datalocker.com: Information, knowledgebase articles, and video tutorials
support@datalocker.com: Feedback and feature requests
datalocker.com: General information
datalocker.com/warranty: Warranty information

Document Version

The latest version of this document resides at
https://media.datalocker.com/manuals/dl4/DataLocker_DL4FE_User_Guide.pdf

This document was compiled on Feb 21, 2024

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

©2024 DataLocker Inc. All rights reserved.

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.

©2024 DataLocker Inc. All rights reserved.