IRONKEY™ Locker + 50 (LP50)
SECURE USB 3.2 Gen 1 FLASH DRIVE

User Guide

Contents

Figure 1: IronKey LP50

Introduction

Kingston IronKey Locker+ 50 USB Flash drives provide consumer-grade security with AES hardware-encryption in XTS mode, including safeguards against BadUSB with digitally-signed firmware and Brute Force password attacks. LP50 is also TAA compliant.

LP50 now supports multi-password (Admin and User) option with Complex or Passphrase modes. Complex mode allows for passwords from 6-16 characters using 3 out of 4 character sets. New passphrase mode allows for a numeric PIN, sentence, list of words, or even lyrics from 10 to 64 characters long. Admin can enable a User password, or reset the User password to restore access to data. To aid in password entry, the “eye” symbol can be enabled to reveal the typed in password, reducing typos leading to failed login attempts. Brute Force attack protection locks out User upon 10 invalid password entries in a row and crypto-erases the drive if the Admin password is entered incorrectly 10 times in a row. Additionally, a built-in virtual keyboard shields passwords from keyloggers or screenloggers.

Locker+ 50 is designed for convenience with a small metal casing and built-in key loop to take data anywhere. LP50 also features optional USBtoCloud (by ClevX®) backup to access data on the drive from your personal cloud storage through Google Drive™, OneDrive (Microsoft®), Amazon Cloud Drive, Dropbox™ or Box. LP50 is easy for anyone to setup and use, with no application installation required; all the software and security needed is already on the drive. Works on both Windows® and macOS® so users can access files from multiple systems.

LP50 is backed by a limited 5-year warranty with free Kingston technical support.

IronKey Locker+ 50 Features

- XTS-AES hardware encryption (encryption can never be turned off)
- Brute Force and BadUSB attack protection
- Multi-Password options
- Complex or Passphrase password modes
- Eye button to display entered passwords to reduce failed login attempts
- Virtual keyboard to help protect against keyloggers and screenloggers
- Windows or macOS compatible (consult datasheet for details)

About This Manual

This user manual covers the IronKey Locker+ 50 (LP50).

System Requirements

PC Platform • Intel, AMD & Apple M1 SOC • 15MB free disk space • Available USB 2.0 - 3.2 port • Two consecutive drive letters after the last physical drive* ***Note:** See 'Drive Letter Conflict' on page 32.	**PC Operating System Support** • Windows 11 • Windows 10 • Windows 8.1
Mac Platform • 15MB free disk space • USB 2.0 - 3.2 Port	**Mac Operating System Support** • macOS X (v. 10.13.x – 12.x.x)

Note: A free 5-year subscription to USB-to-Cloud is included with every drive upon activation. Continued activation options available for purchase by ClevX beyond included timeframe.

Recommendations

To ensure there is ample power provided to the LP50 device, insert it directly into a USB port on your notebook or desktop, as seen in ***Figure 1.1***. Avoid connecting the LP50 to any peripheral device(s) that may feature a USB port, such as a keyboard or USB-powered hub, as seen in ***Figure 1.2***.

Figure 1.1- Recommended Usage

Figure 1.2- Not recommended

Using the Correct File System

The IronKey LP50 comes preformatted with the FAT32 file system. It will work on Windows and macOS systems. However, there could be some other options that could be used to format the drive with manually, such as NTFS for Windows and exFAT. You can reformat the data partition if needed but data is lost when the drive is reformatted.

Usage Reminders

To keep your data safe, Kingston recommends that you:

- Perform a virus scan on your computer before setting up and using the LP50 on a target system
- Lock the device when not in use
- Eject the drive before unplugging it
- Never unplug the device when the LED is lit. This may damage the drive and require a reformat, which will erase your data
- Never share your device password with anyone

Find the Latest Updates and Information

Go to kingston.com/support for the latest drive updates, FAQs, Documentation, and additional information.

NOTE: Only the latest drive updates (when available) should be applied to the drive. Downgrading the drive to an older software version is not supported and can potentially cause a loss of stored data or impair other drive functionality. Please contact Kingston Technical Support if you have questions or issue

Best Practices for Password Setup

Your LP50 comes with strong security countermeasures. This includes protection against Brute Force attacks that will stop an attacker guessing passwords by limiting each password attempt to 10 retries. When the drive's limit is reached, LP50 will automatically wipe out the encrypted data – formatting itself back to a factory state.

Multi-Password
LP50 supports Multi-Passwords as a major feature to help protect against data loss if one or more passwords are forgotten. When all password options are enabled, the LP50 can support two different passwords you may use to recover data – Admin and User Password roles

LP50 allows you to select two main passwords – an Administrator password (referred to as Admin password) and a User password. Admin can access the drive at any time and set up options for User – Admin is like a Super User.

User can access the drive as well but compared to Admin has limited privileges. If one of the two passwords is forgotten, the other password can be used to access and retrieve the data. The drive can then be set back up to have two passwords. It is important to set up BOTH passwords and save the Admin password in a safe location while using the User password.

If both passwords are forgotten or lost, there is no other way to access the data. Kingston will not be able to retrieve the data as the security has no back doors. Kingston recommends that you have the data also saved on other media. The LP50 can be Reset and reused, but the prior data will be erased forever.

Password Modes
The LP50 also supports two different password modes:

Complex
A complex password requires to meet a minimum of 6-16 characters using at least 3 of the following characters:

- Upper case alphabet characters
- Lower case alphabet characters
- Numbers
- Special characters

Passphrase
LP50 supports Passphrases from 10 to 64 characters. A Passphrase follows no additional rules, but if used properly, can provide very high levels of password protection.

A Passphrase is basically any combination of characters, including characters from other languages. Like the LP50 drive, the password language can match the language selected for the drive. This allows you to select multiple words, a phrase, lyrics from a song, a line from poetry, etc. Good passphrases are among the most difficult password types to guess for an attacker yet may be easier to remember for users.

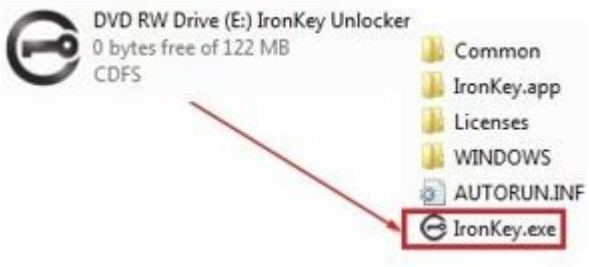
Setting Up My Device

To ensure there is ample power provided to the IronKey encrypted USB drive, insert it directly into a USB 2.0/3.0 port on a notebook or desktop. Avoid connecting it to any peripheral devices that may feature a USB port, such as a keyboard or USB-powered hub. Initial setup of the device must be done on a supported Windows or macOS based operating system.

Device Access (Windows Environment)

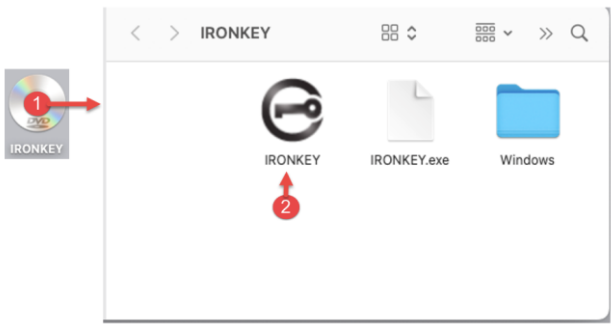
Plug the IronKey encrypted USB drive into an available USB port on the notebook or desktop and wait for Windows to detect it.

• Windows 8.1/10/11 users will receive a device driver notification. (Figure 3.1)	 **Figure 3.1 – Device Driver Notification**

• Once the new hardware detection is complete, select the option **IronKey.exe** inside of the Unlocker partition that can be found in File Explorer. (Figure 3.2) • Please note that the partition letter will vary based on the next free drive letter. The drive letter may change depending on what devices are connected. In the image below, the drive letter is (E:)	 **Figure 3.2 – File Explorer Window/IronKey.exe**

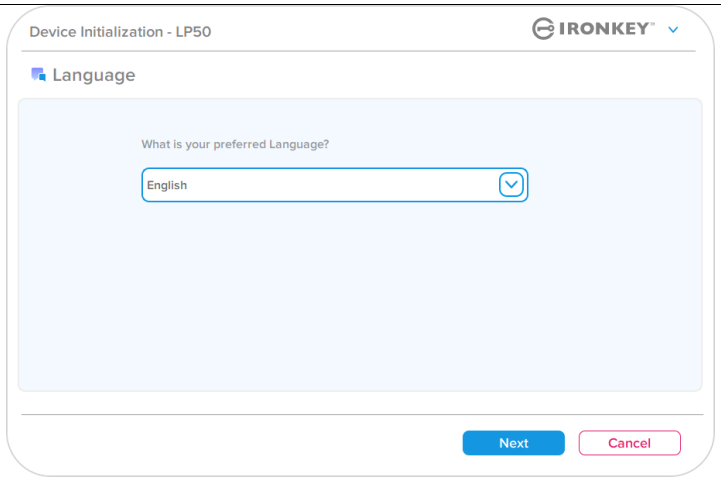
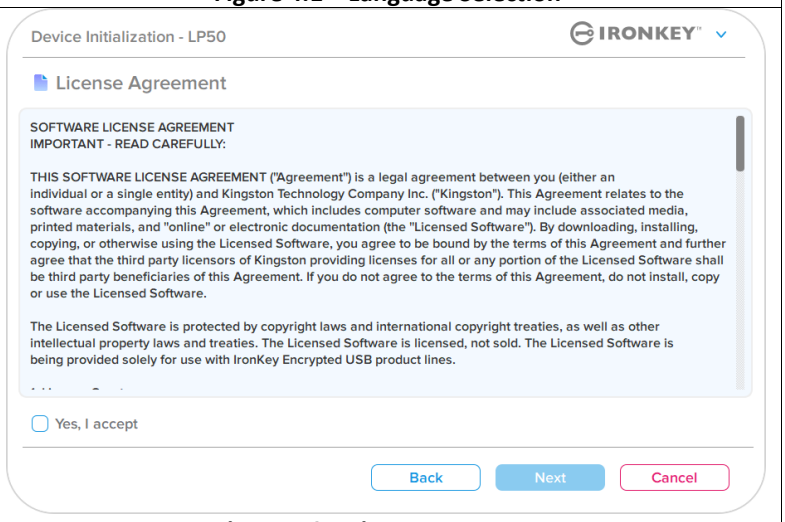
Device Access (macOS Environment)

Insert the LP50 into an available USB port on your notebook or desktop and wait for the Mac operating system to detect it. When it does, you will see the 'IRONKEY' volume appear on the desktop. (Figure 3.3)

• Double-click the IronKey CD-ROM icon • Then, double-click the IronKey.app application icon found in the window displayed in Figure 3.3. This will start the initialization process.	 **Figure 3.3 – IKLP Volume**

Device Initialization (Windows & macOS Environment)

Language and EULA

Select your language preference from the drop-down menu and click **Next** (See Figure 4.1)	 **Figure 4.1 – Language Selection**
Review the license agreement and click **Next**. Note: You must accept the license agreement before continuing; otherwise, the **Next** button will remain disabled. (Figure 4.2)	 **Figure 4.2 – License Agreement**

Device Initialization

Password Selection

On the Password prompt screen, you will be able to create a password to protect your data on the LP50 using either the Complex or Passphrase password modes (Figures 4.3- 4.4). Additionally, the Multi-password Admin/User options can also be enabled on this screen. Before proceeding with Password Selection, please review Enabling Admin / User Passwords below for a better understand of these features.

Note: Once either Complex or Passphrase mode is chosen, the mode cannot be changed unless a device is Reset.

To begin with password selection, create your password in the 'Password' field, then re-enter it in the 'Confirm Password' fields. The password you create must meet the following criteria before the initialization process will allow you to continue:

Complex Password

- Must contain 6 characters or more (up to 16 characters.)
- Must contain three (3) of the following criteria:
  - Upper Case
  - Lower Case
  - Numerical Digit
  - Special characters (!,$,&, etc..)

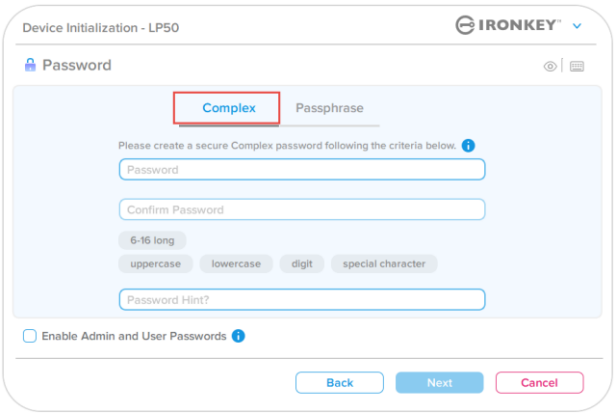


Figure 4.3 – Complex Password

Passphrase Password

- Must contain:
  - 10 characters minimum
  - 64 characters maximum

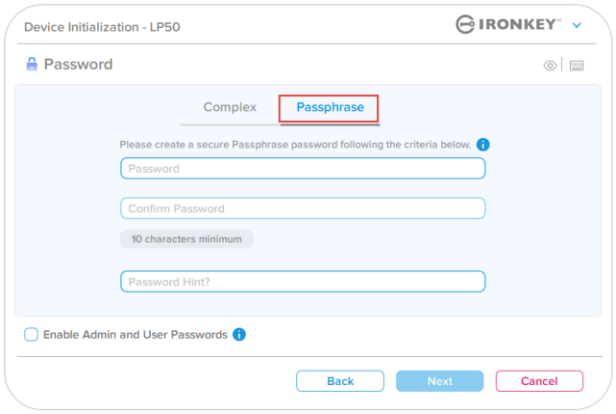


Figure 4.4 – Passphrase Password

Password Hint (Optional)

A password hint can be useful for providing a clue as to what the password is, should the password ever be forgotten.

Note: The hint CANNOT be an exact match to the password.

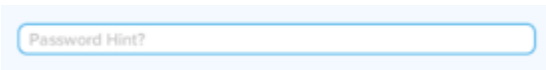


Figure 4.5 – Password Hint Field

Device Initialization

Valid and Invalid Passwords

For **valid** passwords, the Password Criteria Boxes will highlight **green** when the criteria are met. (See Figures 4.6a-b) Note: Once the minimum of three password criteria are met, the fourth criteria box will become gray, indicating that this criterion is optional (Figure 4.6b)

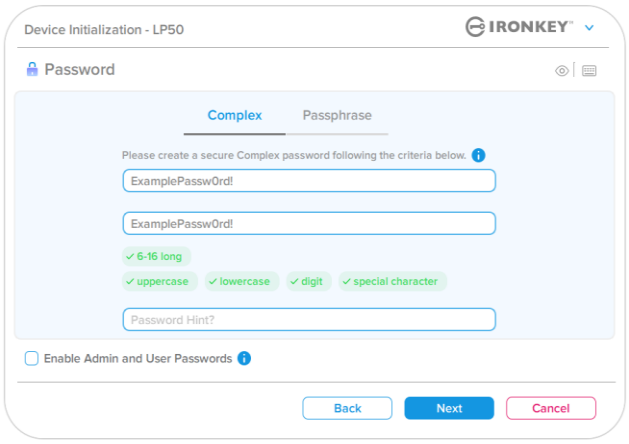


Figure 4.6a – Complex Password Condition Met

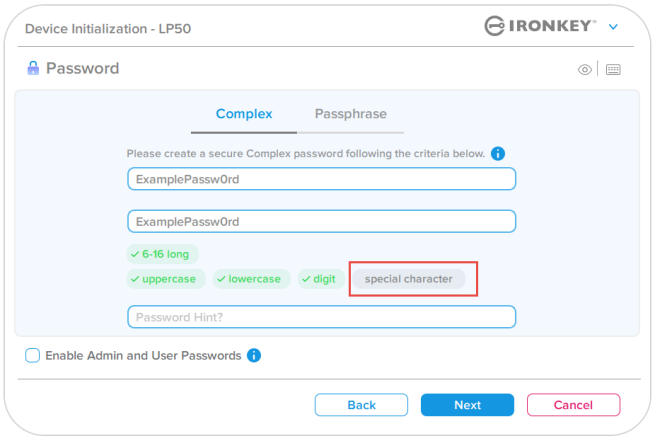


Figure 4.6b – Complex Password Condition Optional

For **invalid** passwords, the Password Criteria Boxes will highlight **red** and the **Next** button will be disabled until the minimum requirements are met.

This applies to both Complex and Passphrase Passwords.

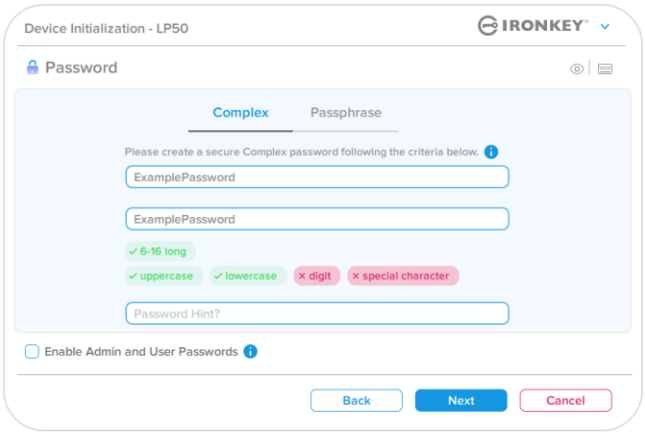


Figure 4.7 – Password Conditions Not Met

Device Initialization

Virtual Keyboard
The LP50 features a Virtual Keyboard that can be used for Keylogger protection.

- To utilize the **Virtual Keyboard**, locate the keyboard button on the upper-right side of the **Device Initialization** screen and select it.

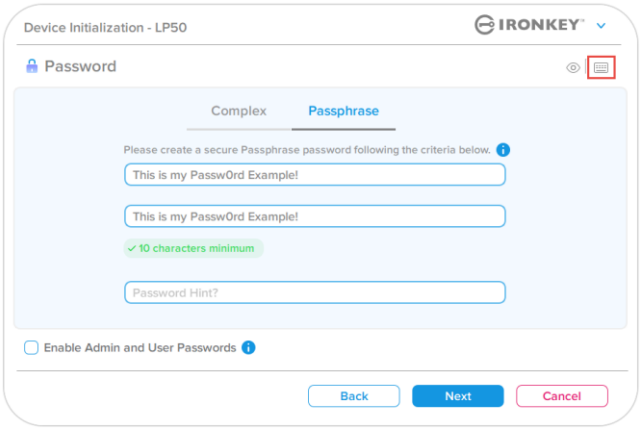


Figure 4.8 – Activating the Virtual Keyboard

- Once the virtual keyboard appears, you may also enable **Screenlogger Protection**. When using this feature, all the keys will briefly go blank. This is expected behavior, as it prevents screenloggers from capturing what you've clicked.

- To make this feature more robust, you may also choose to randomize the virtual keyboard by selecting **randomize** in the lower-right of the keyboard. Randomize will arrange the keyboard in a random order.

Figure 4.9 – Screenlogger Protection / Randomize

Device Initialization

Password Visibility Toggle

By default, when you create a password, the password string will be shown in the field as you type it in. If you wish to 'hide' the password string as you type, you can do so by toggling the password 'eye' located on the upper-righthand side of the Device Initialization window.

Note: After the device has been initialized, the password field will default to 'hidden'.

To **hide** the password string, click the gray icon.

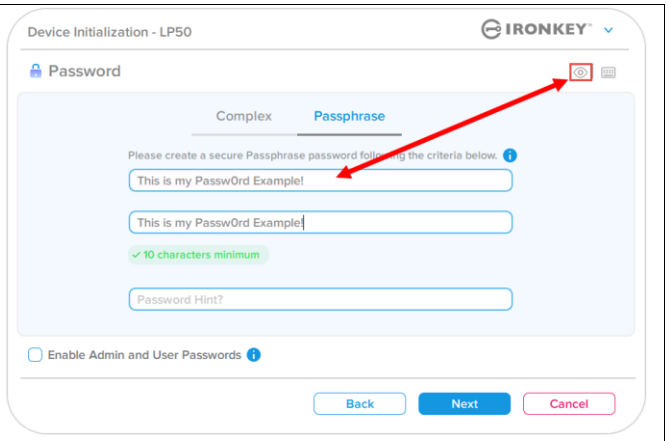


Figure 4.10 – Toggle 'hide' Password

To **show** the hidden password, click the blue icon.

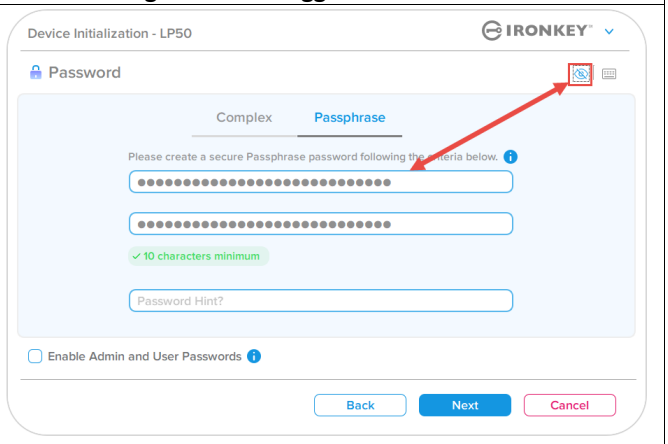


Figure 4.11 – Toggle 'show' Password

Device Initialization

Admin and User Passwords

By enabling Admin and User Passwords, you can leverage multi-password functionality, in which the Admin Role can manage both accounts. Selecting **'Enable Admin and User passwords**' allows for an alternative method of drive access in case one of the passwords is forgotten.

With **Admin and User passwords** enabled, you can also access:

- User Password reset

To learn more about the User Password reset feature, navigate to page 28 within this user guide.

- To Enable **Admin and User passwords** click on the box next to '**Enable Admin and User Passwords**' and select **Next** once a valid password has been chosen. (Figure 4.12)

- If this feature is **enabled**, then the chosen Password at this screen will be the **Admin Password**. Click **Next** to proceed to the **User Password** screen where a password is chosen for the User.

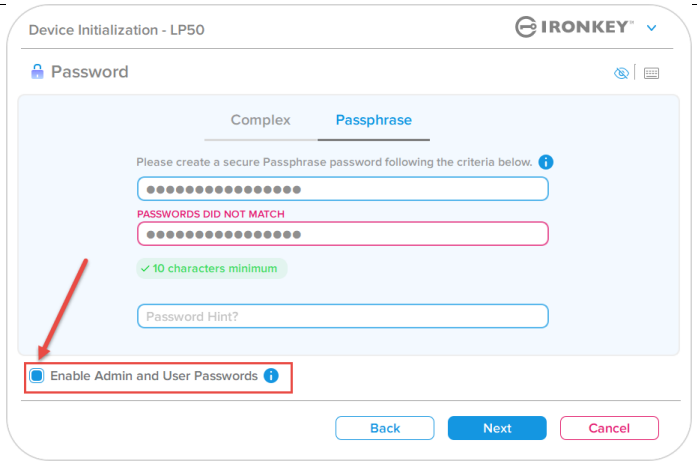


Figure 4.12 – Enabling Admin and User Passwords

Note: Enabling Admin and User passwords is optional.

If the drive is set up with this feature NOT enabled (box unchecked), then the drive will be configured as a **Single User**, **Single Password** drive **without any Admin features**. This configuration will be referred to **User-Only mode** throughout this manual.

To proceed with a Single User, Single password setup, keep **Enable Admin and User Passwords** unchecked, and click **Next** after creating a valid password.

Device Initialization

Admin and User Passwords

If Admin Role was **enabled** in the previous screen, the following screen will prompt for the **User Password** (Figure 4.13) The User Password will have limited capabilities compared to Admin and will be discussed in further detail l**Moving forward, theNote:** '**Admin and User Passwords'** will be referred to as '**Admin Role**' throughout this manual.for the remainder of this document.

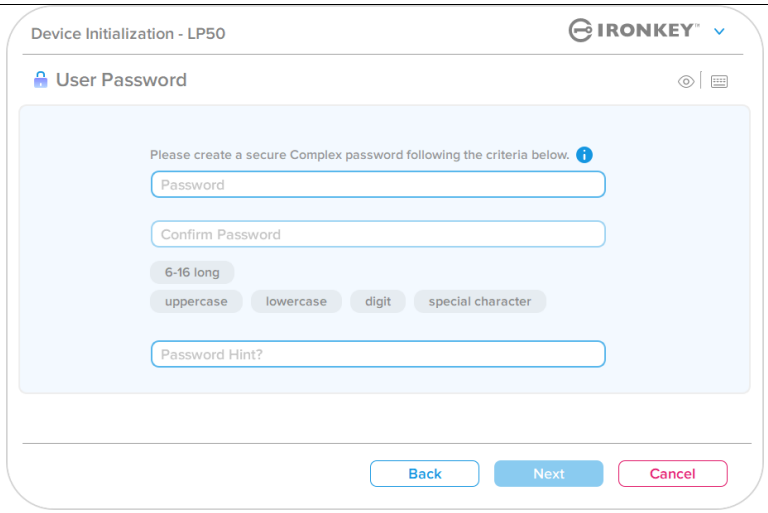


Figure 4.13 - User Password (Admin and User Enabled)

Note: The chosen Password Option (Complex or Passphrase) criteria will carry over to the User Password, and to any password resets that are needed after the drive is set up. The chosen password option may only be changed after a full device reset.

Device Initialization

Contact Information

Enter your contact information into the text boxes provided (see Figure 4.14)

Note: The information you enter in these fields may NOT contain the password string you created in Step 3. However, these fields are optional and can be left blank, if so desired.)

The '**Name'** field may contain up to 32 characters, but cannot contain the **exact** password.

The '**Company'** field may contain up to 32 characters, but cannot contain the **exact** password.

The '**Details'** field may contain up to 156 characters, but cannot contain the **exact** password.

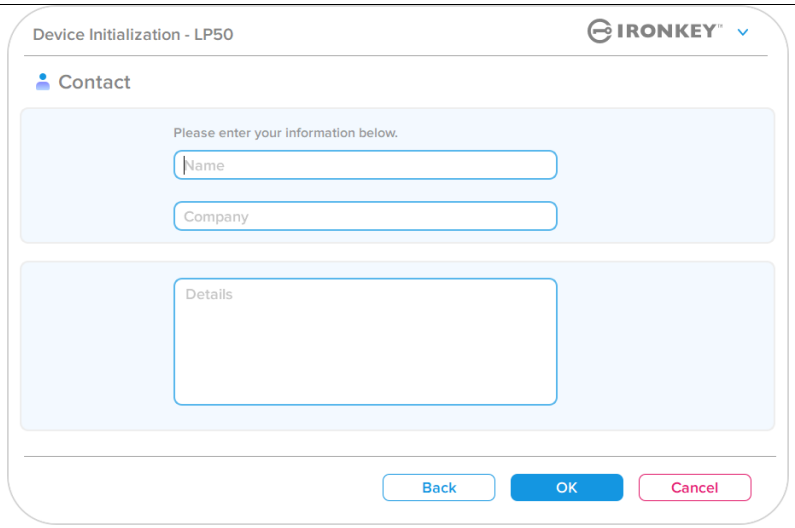


Figure 4.14 - Contact information

Note: Clicking 'OK' will complete the initialization process and proceed to unlock, then mount the secure partition where your data can be securely stored. Proceed to Unplug the drive and plug it back into the system to see the reflected changes.

USB ← → Cloud Initialization (Windows Environment)

Once the device has been initialized in Windows, the USB-to-Cloud application will appear as seen in Figure 3.7 on the right. Please make sure you have a working Internet connection before you continue.

- To proceed with the installation, click the green 'Accept' button in the bottom right-hand corner of the clevX window
- To decline the installation, click the red 'Decline' button in the bottom left-hand corner of the clevX window.
- (Note: If you click the red 'Decline' button, it will cancel the USB-to-Cloud installation. In doing so, a special text file named 'USBtoCloudInstallDeclined.txt' is created on the data partition. The presence of this file will prevent the application from prompting you for the installation in the future.)

Figure 5.1 – USBtoCloud Windows EULA

- If the following Windows Security Alert window pops up during the initialization process, please click "Allow access" to continue (or create a Windows Firewall Exception) in order for the USB-to-Cloud application to continue.

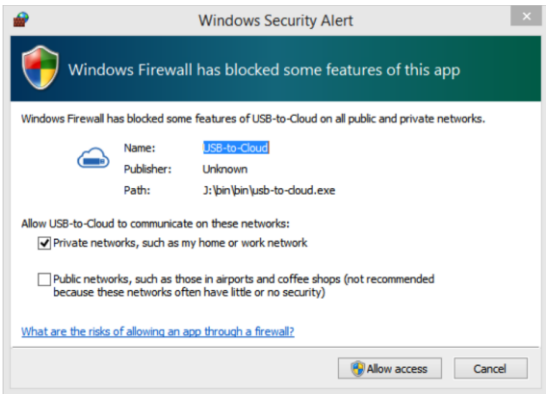


Figure 5.2 – Windows security alert

USB ← → Cloud Initialization (Windows Environment)

- Once the installation has completed, you will see an application box with a list of options to choose from (for syncing your LP50 data.)
- Select the cloud option you wish to use as your backup application and provide the necessary credentials required for authentication.
- (Note: If you currently do not have an account set up with any of the cloud options listed, you may create one at this time, using your favorite Internet browser, and then completing this option afterwards.
- Once you've chosen a cloud option and authenticated to the corresponding service, the USB-to-Cloud program will perform an initial comparison of the data partition against what is stored in the Cloud. As long as the USB-to-Cloud service is running in Task Manager, content written to the data partition will automatically back up (sync) to the Cloud.

Figure 5.3 – Cloud Selection

USB ← → Cloud Usage (Windows Environment)

The USB-to-Cloud application provides the following additional services:

- Pause Backup (Pauses a data backup)
- Restore (Restores data from the cloud to the device)
- Settings (Additional options for your data backup)
- Exit (Exits the USB-to-Cloud service

In the 'Settings' menu, you can:

- Change which cloud service app you are currently using for backups.
- Change the language you are currently using,
- Select which files and/or folders you are backing up to the cloud.
- Check for software updates

(**Note:** If you reset (or format) the LP50 device, all data on the device will be lost. However, whatever data is stored in the cloud remains safe and intact.)

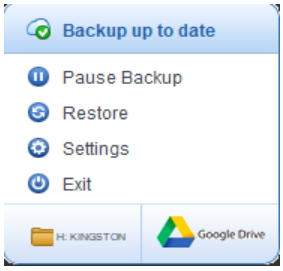


Figure 5.4- Services

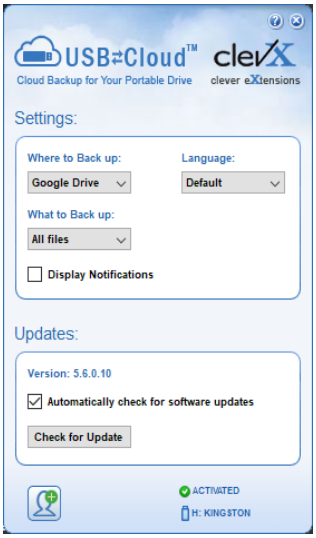


Figure 5.5- Settings

USB ← → Cloud Initialization (macOS Environment)

- Once the device has been initialized, the USB-to-Cloud application will appear as seen in **Figure 5.6** to the right. Please make sure you have a working Internet connection before you continue.

- To proceed with the installation, click the green 'Accept' button in the bottom right-hand corner of the clevX window.

  (Note: On macOS 10.15.x + will be prompted to allow access to files on a removable volume. Select OK. (see Figure 5.7)

- To decline the installation, click the red 'Decline' button in the bottom left-hand corner of the clevX window.

Figure 5.6 – USBtoCloud macOS EULA

(Note: If you click the red 'Decline' button, it will cancel the USB-to-Cloud installation. In doing so, a special file named 'DontInstallUSBtoCloud' is created on the data partition. The presence of this file will prevent the application from prompting you for the installation in the future.)

- Once the installation has completed, you will see an application box with a list of options to choose from (for syncing your LP50 data.) ***Figure 5.8***

Figure 5.7- macOS access

- Select the cloud option you wish to use as your backup application and provide the necessary credentials required for authentication

  (Note: If you currently do not have an account set up with any of the cloud options listed, you may create one at this time, using your favorite Internet browser, and then completing this option afterwards.)

- Once you've chosen a cloud option and authenticated to the corresponding service, the USB-to-Cloud program will perform an initial comparison of the data partition against what is stored in the Cloud. As long as the USB-to-Cloud service is running in Task Manager, content written to the data partition will automatically back up (sync) to theCloud

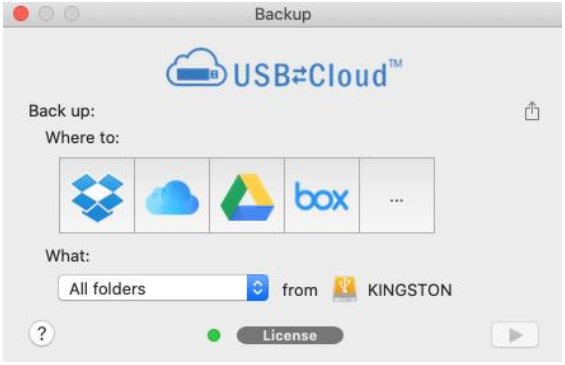


Figure 5.8- Cloud Selection

USB ← → Cloud Usage (macOS Environment)

The USB-to-Cloud application provides the following additional services (*Figure 5.9)*:

- **Pause Backup** (Pauses a data backup)
- **Restore** (Restores data from the cloud to the device)
- **Backup** (Opens Cloud Options)
- **Exit** (Exits the USB-to-Cloud service)

Figure 5.9- Services

In the 'Preferences' menu, you can:

- Change the language you are currently using
- Enable/disable sound notifications
- Enable/disable unmount drive if app is quit
- Enable/disable logging for troubleshooting
- Enable/disable automatic software updates and to check for updates now

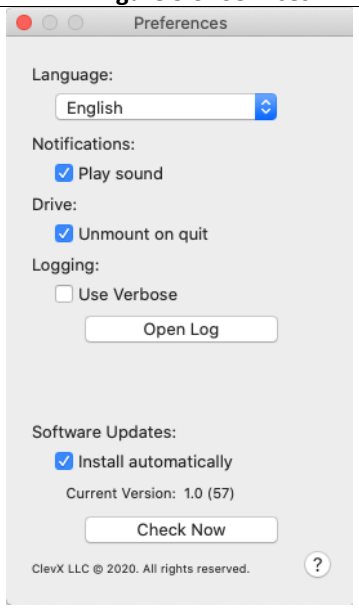


Figure 5.10- USBtoCloud Preferences

Device Usage (Windows & macOS Environment)

Login For Admin & User (Admin Enabled)

If the device is initialized with Admin and User Passwords (Admin Role) enabled, the IronKey LP50 application will launch, prompting for the User Password login screen first. From here you can login with the User Password, view any entered contact Information, or Login as Admin (Figure 6.1). By clicking on the 'Login as Admin' button (shown below) the application will proceed to the Admin Login menu where you can login As Admin to access the Admin settings and features (Figure 6.2) .

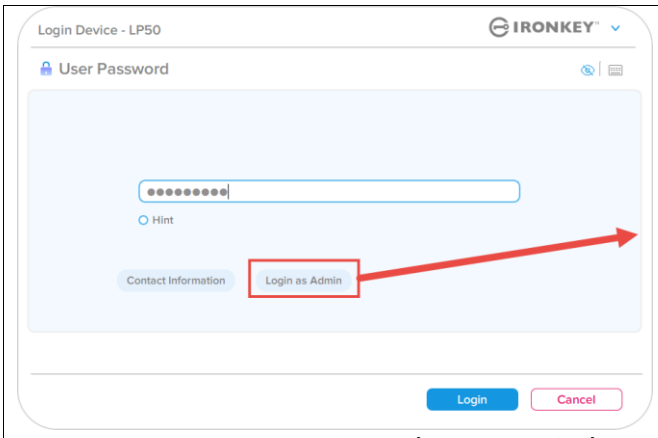


Figure 6.1 - User Password Login (Admin enabled)

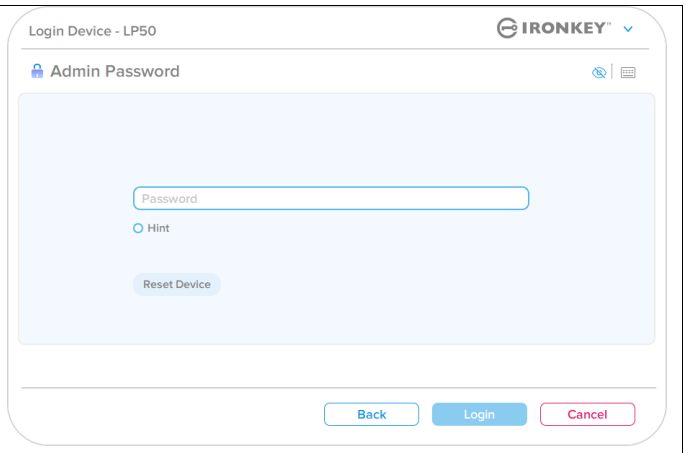


Figure 6.2 - Admin Password Login

Login for User-Only Mode (Admin not Enabled)

As previously mentioned previously on **Page 13,** although it is recommended to use the Admin Role functionality to get the full benefit of your device, The IronKey drive can also be initialized in a User-Only (Single Password, Single User) configuration. This is an option for those who would like a simple, single password approach to securing the data on your drive. (Figure 5.3)

Note: To enable Admin and user Passwords, use the **Reset Device** button to put the drive back into the initialization state where you can enable Admin and User Passwords. **ALL Data on the drive will be formatted and lost forever when a Reset Device occurs.**

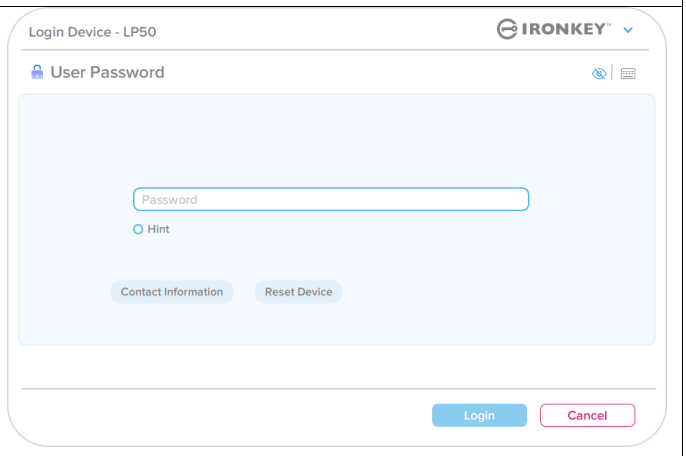


Figure 6.3 - User Password Login (Admin not enabled)

Device Usage

Brute-Force attack protection

Important: During login, if an incorrect password is entered, you will be given another opportunity to enter the correct password; however, there is a built-in security feature (also known as Brute Force attack protection) that tracks the number of failed login attempts. *

If this number reaches the pre-configured value of 10 failed password attempts, the behavior will be as follows:

Admin/User Enabled	**Brute Force protection Device Behavior (10 Incorrect Password attempts)**	**Data Erase and Device Reset?**
User Password:	Password Lockout. Login as Admin or to reset User Password	NO
Admin Password	Crypto-Erase drive, Passwords, settings, and data erased forever	**YES**
User-Only Single User, Single Password (Admin/User NOT Enabled)	**Brute Force protection Device Behavior (10 Incorrect Password attempts)**	**Data Erase and Device Reset?**
User Password	Crypto-Erase drive, Passwords, settings, and data erased forever	**YES**

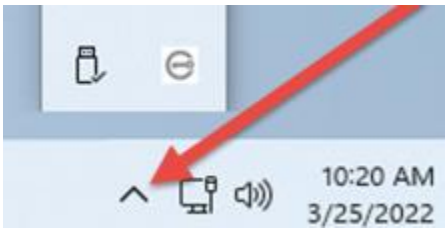
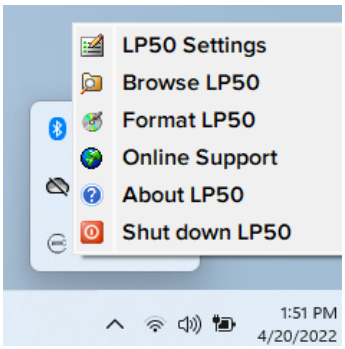
* Once you authenticate to the device successfully, the failed login counter will be reset in relation to which Login method was used. Crypto-Erase will delete all passwords, encryption keys and data – **your data will be lost forever.**

Accessing My Secure Files

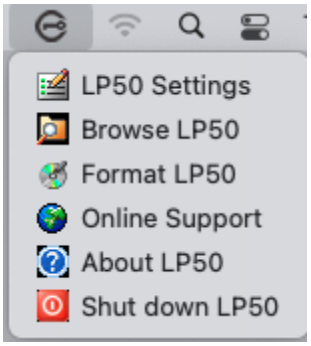
After unlocking the drive, you can access your secure files. Files are automatically encrypted and decrypted when you save or open them on the drive. This technology gives you the convenience of working as you normally would with a regular drive, while providing strong, “always-on” security.
Hint: You can also access your files by right clicking the **IronKey Icon** in the Windows taskbar and clicking **Browse LP50** (Figure 7.2)

Device Options - (Windows Environment)

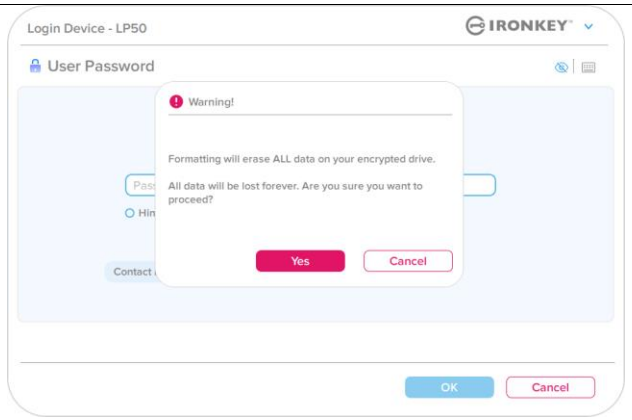
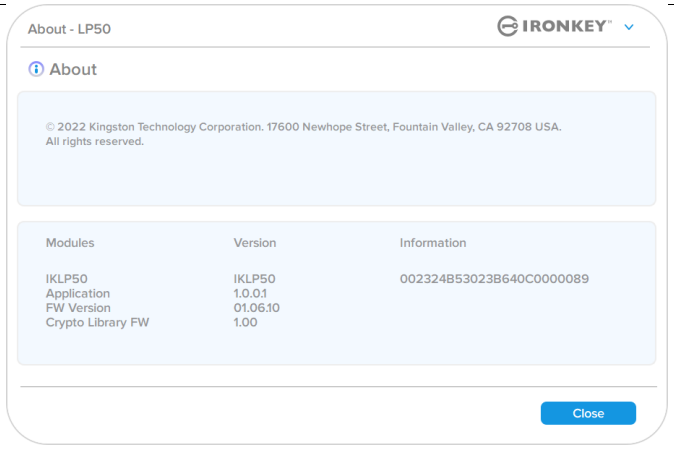
While you are logged into the device, there will be an IronKey icon located in the right-hand corner the window. Right-clicking on the IronKey Icon will open the selection menu for available drive Options (Figure 6.2). Details about these device options can be found on Pages 19-23 of this manual

• While you are logged into the device, there will be an IronKey icon located in the right-hand corner the Window (Figure 7.1)	 **Figure 7.1 IronKey Icon in Taskbar**
• Right clicking on the IronKey Icon will open the selection menu for available drive Options (Figure 7.2). Details about these device options can be found on pages 19-23 of this manual	 **Figure 7.2 Right-Click IronKey Icon for Device Options**

Device Options- (macOS Environment)

• While you are logged into the device, there will be a 'IronKey LP50 icon located in the macOS menu seen in (Figure 7.3) that will open the available device options. Details about these device options can be found on Pages 19-23 of this manual	 **Figure 7.3- macOS menu bar Icon/Device options menu**

Device Options

LP50 Settings:	• Change login Password, Contact Information, and other settings. (More details about device settings can be found in the 'LP50 Settings' section of this manual).
Browse LP50:	• Allows you to view your secure files.
Format LP50: Allows you to format the secure data partition. (Warning: All data will be erased.) (Figure 7.4) **Note:** Password authentication will be required for format.	 **Figure 7.4- Format LP50**
Online Support:	• Opens your internet browser and navigates to http://www.kingston.com/support where you can access additional support information
About LP50: Provides specific details about the LP50, including Application, Firmware and Serial number Information (Figure 7.5) **Note:** The unique serial number of the drive will be under the 'Information Column'	 **Figure 7.5- About LP50**
Shut down LP50:	• Properly shuts down the LP50, allowing you to safely remove it from your system.

LP50 Settings

Admin Settings

The Admin Login allows access to the following device settings:

- **Password:** Allows you to change your own Admin password and/or hint (*Figure 8.1*)
- **Contact Info:** Allows you to add/view/change your contact information (*Figure 8.2*)
- **Language:** Allows you to change your current language selection (*Figure 8.3*)
- **Admin Options:** Allows you to access additional features such as:
    - Changing the User Password (Figure 8.4)

NOTE: Additional details of the Admin Options can be found on page 25

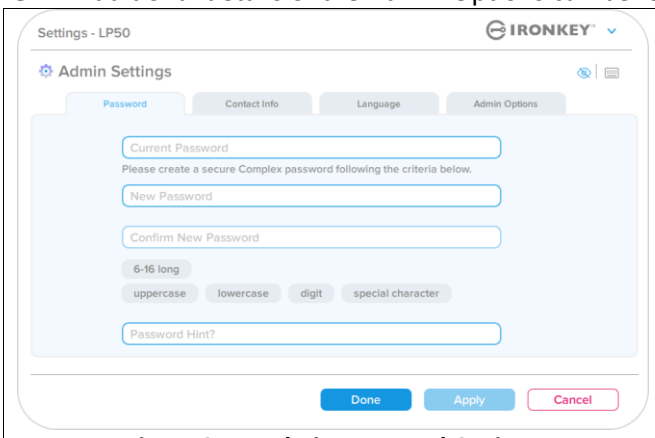


Figure 8.1 – Admin Password Options

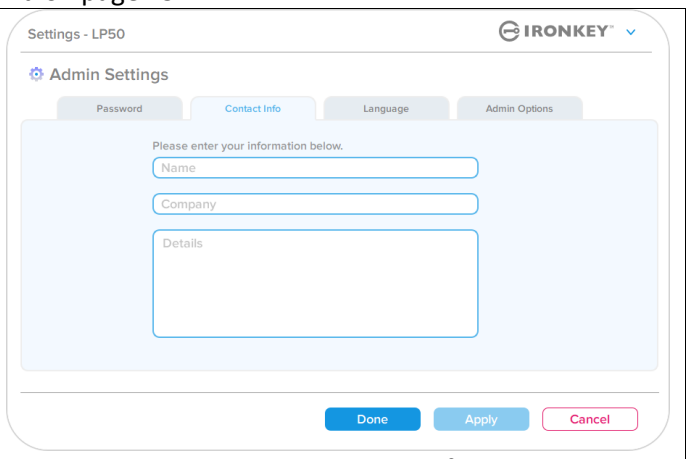


Figure 8.2- Contact Info

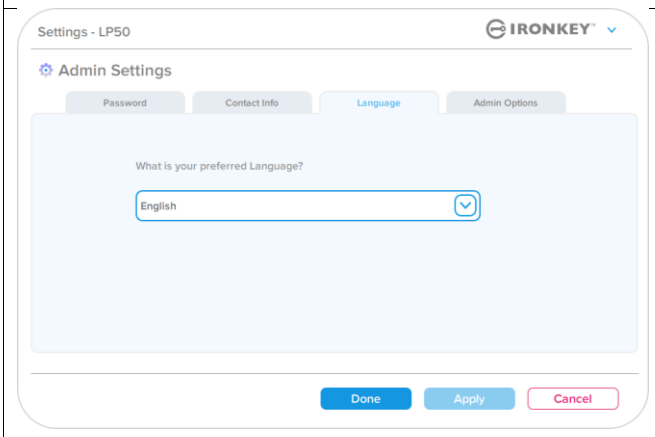


Figure 8.3 - Language Options

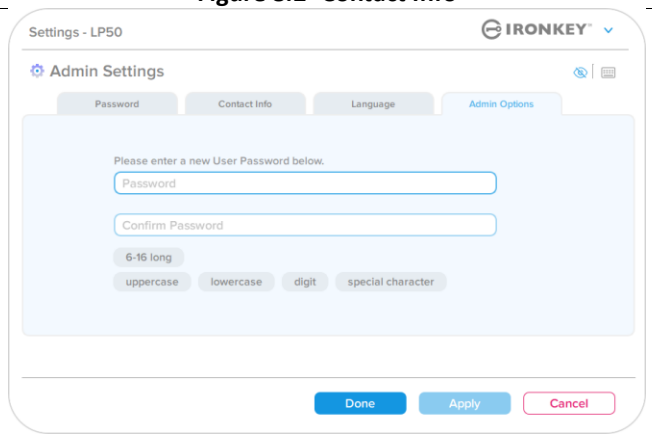


Figure 8.4- Admin Options

LP50 Settings

User Settings: Admin Enabled

The User Login limits access to the following settings:

Password:
Allows you to change your own User password and/or hint (*Figure 7.5*)

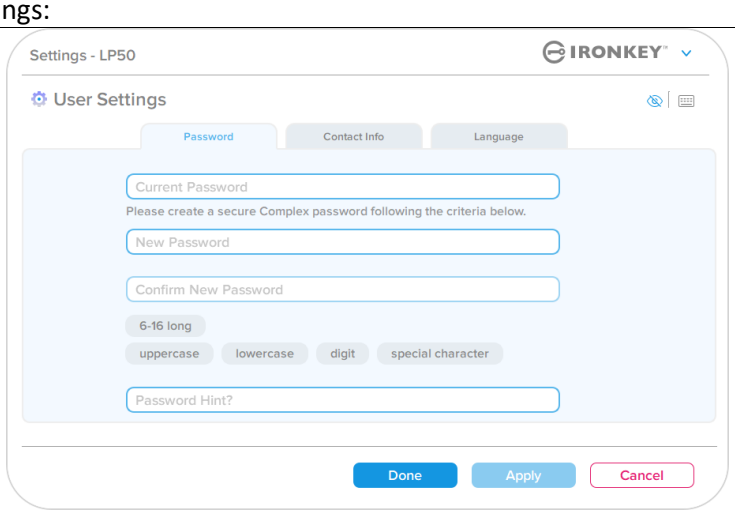


Figure 8.5- Password Options (Admin Enabled: User Login)

Contact Info:
Allows you to add/view/change your contact information (*Figure 7.6*)

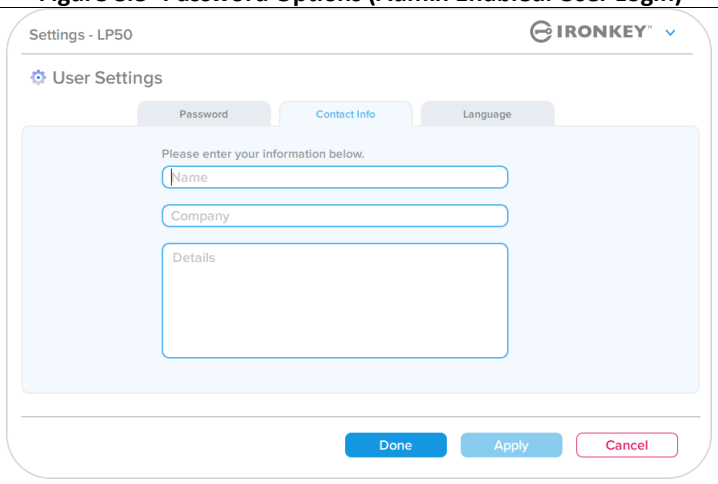


Figure 8.6- Contact Information (Admin Enabled: User Login)

Language:
Allows you to change your current language selection (*Figure 7.7*)

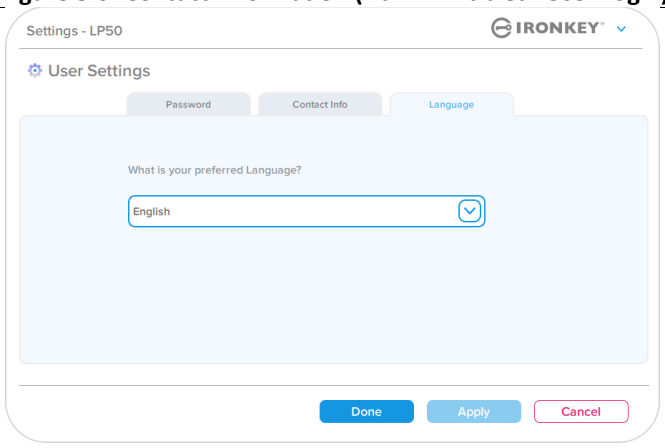


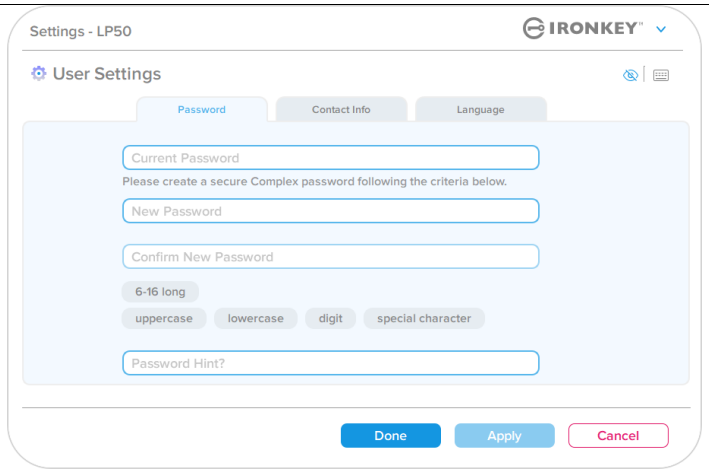
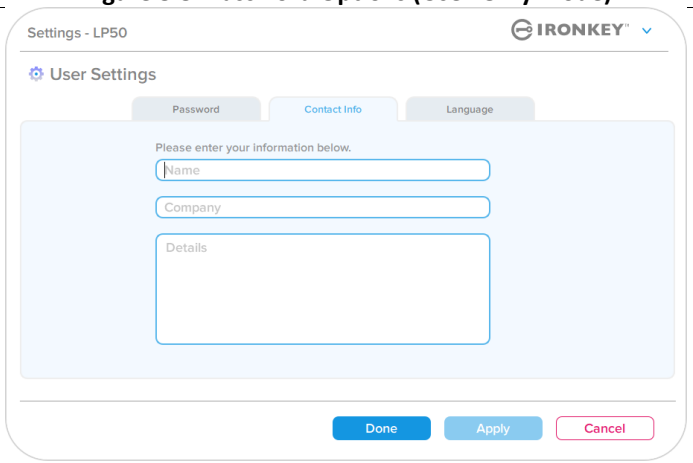
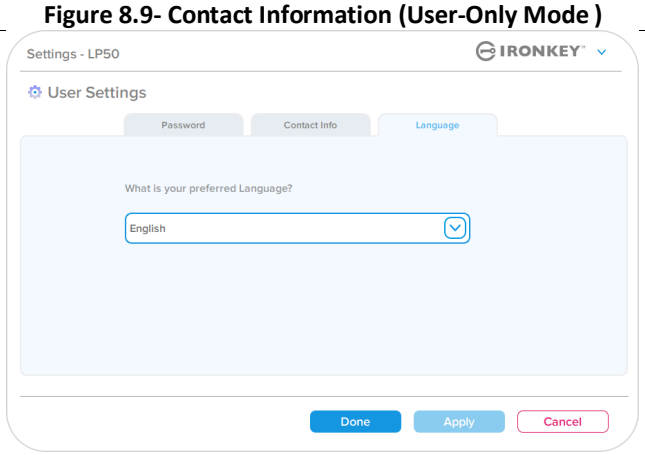
Figure 8.7- Language Settings (Admin Enabled: User Login)

Note: Admin Options are not accessible when the logged in with the User Password.

LP50 Settings

User Settings: Admin Not Enabled

As mentioned previously on Page 12, initializing the LP50 without enabling 'Admin and User' passwords will configure the drive up in a **Single Password, Single User setup**. This configuration does not have access to any Admin options or features. This configuration will have access to the following LP50 Settings:

Password: Allows you to change your own User password and/or hint (Figure 8.8)	 **Figure 8.8- Password Options (User-Only Mode)**
Contact Info: Allows you to add/view/change your contact information (Figure 8.9)	 **Figure 8.9- Contact Information (User-Only Mode)**
Language: Allows you to change your current language selection (*Figure 8.10*)	 **Figure 8.10- Language Settings (User-Only Mode)**

LP50 Settings

Changing and Saving settings

- Whenever settings are changed in the LP50 Settings (e.g.) Contact information, language, Password changes, Admin options etc..), the drive will prompt to enter your password in order to accept and apply the changes (see Figure 8.11)

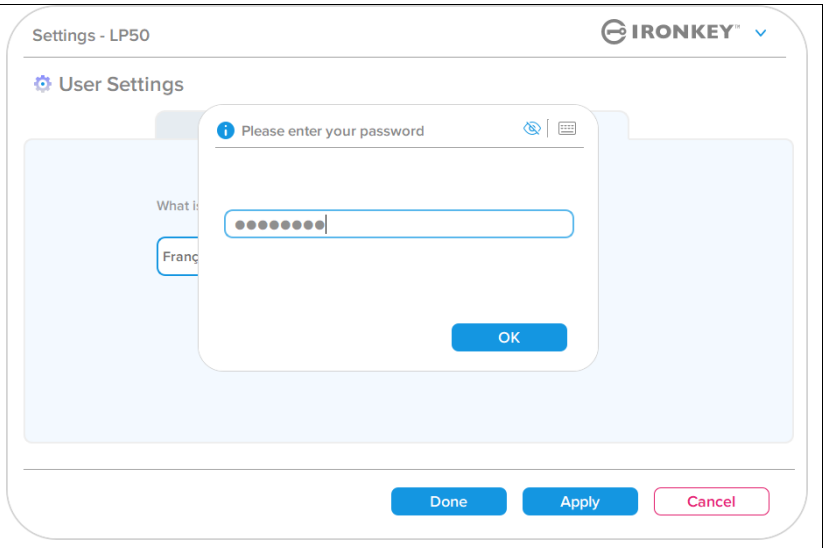


Figure 8.11- Password Prompt screen to save LP50 setting changes

Note: If you are at the Password prompt screen above and would like to cancel or modify your changes, you can do so by simply making sure the password field is blank and Click 'OK'. This will close the 'Please enter your password' box and revert back to the LP50 settings menu.

Admin Features

Option Available to Reset the User Password

One of the useful features of Admin configuration allow you to securely reset the Users Password, should it ever be forgotten. Below is the User Password Reset feature that can be helpful to Reset the User Password:

User Password Reset:
Manually change the User Password in the 'Admin Options' menu, which is an instant change and will take effect on next User login (Figure 9.1)

Note: The password requirement criteria will default to the original criteria that was set during the initialization process (Complex or Passphrase options).

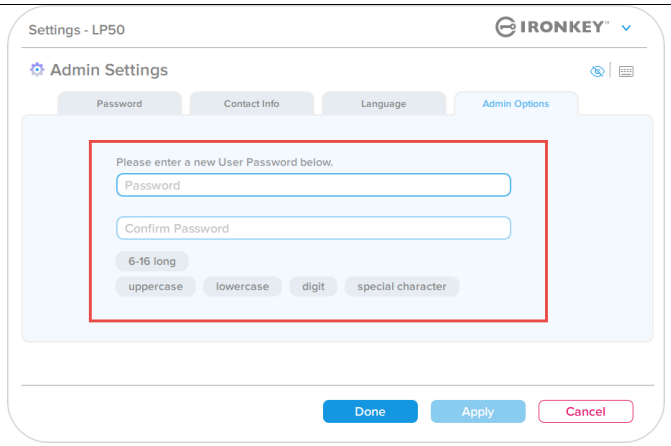


Figure 9.1- Admin Options/User Password Reset

Help and Troubleshooting

Device Lockout

The LP50 includes a security feature that prevents unauthorized access to the data partition once a maximum number of **consecutive** failed login attempts (*MaxNoA* for short) has been made. The default "out-of-box" configuration has a pre-configured value of 10 (no. of attempts.) for each Login method (Admin/User)

The 'lock-out' counter tracks each failed login and gets reset **one of two** ways:

1. A successful login prior to reaching MaxNoA

2. Reaching MaxNoA and performing either a device lockout or device format depending on how the drive is configured.

- If an incorrect password is entered, an error message will appear in red just above the Password Entry field, indicating a login failure. (Figure 10.1)

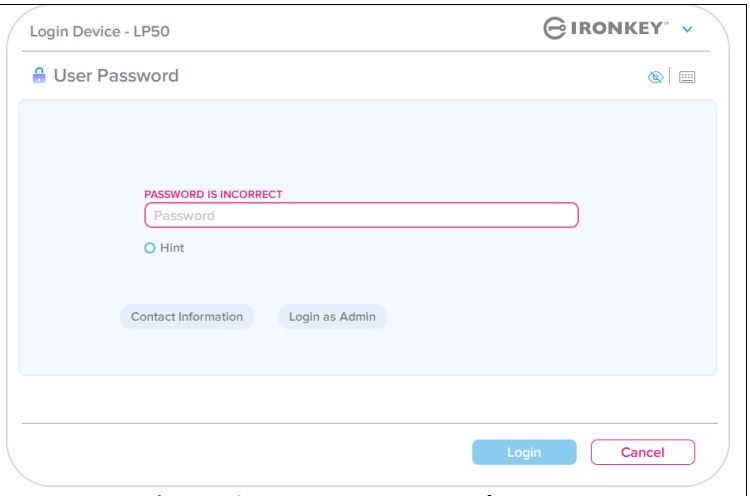


Figure 10.1- Incorrect Password message

- When a **7th** failed attempt is made, you will see an additional error message indicating you have 3 attempts left before reaching MaxNoA (which is set to 10 by default.)(Figure 10.2)

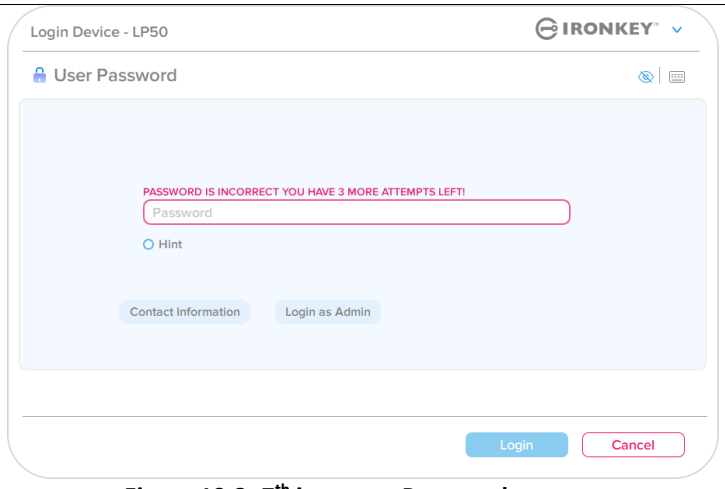


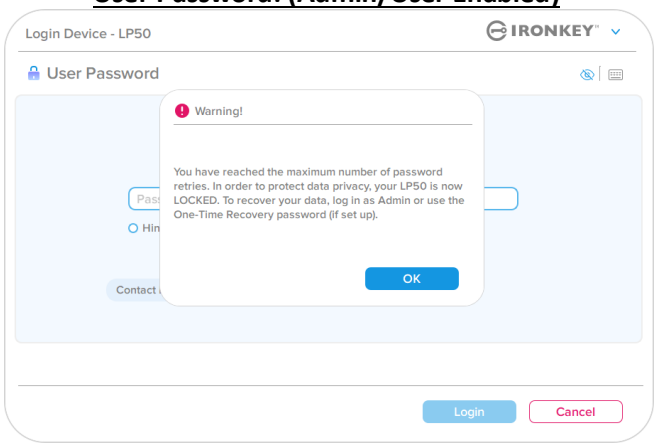
Figure 10.2- 7th incorrect Password attempt

Device Lockout

Important: After a **10th** and final failed login attempt, depending on how the device was set up and Login method used, (Admin, User or) The device will either Lock down, requiring you to login with an alternate method (If applicable), or a Device Reset which will **format the data and all data on the drive will be lost forever.** behaviors also mentioned on page 18 of this User Guide.

Figures 10.3- 10.6 below demonstrate the visual behavior for the 10th and final failed logins of each login password method:

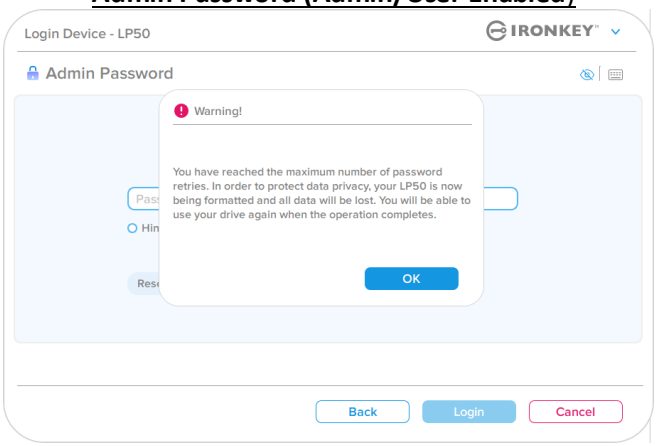
User Password: (Admin/User Enabled)



DEVICE LOCKOUT

(Figure 10.3)

Admin Password (Admin/User Enabled)

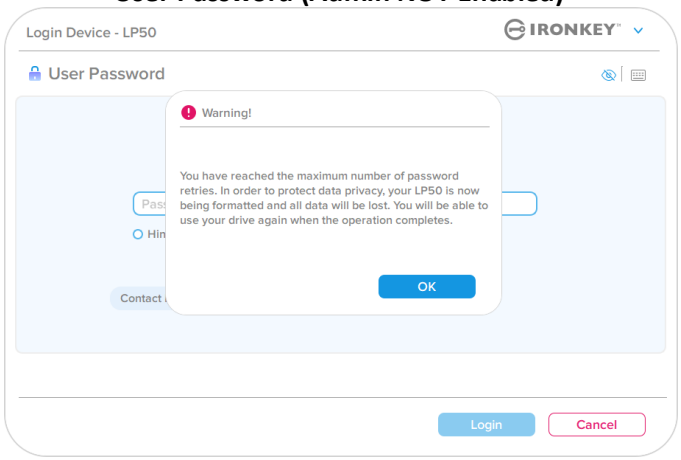


DEVICE FORMAT*

(Figure 10.4)

- These security measures limit someone (who does not have your password) from attempting countless login attempts and gaining access to your sensitive data (Also known as a Brute-Force attack). If you are the owner of the LP50 and have forgotten your password, the same security measures will be enforced, including a device format. * For more on this feature, see '*Reset Device*' on page 25.

User Password (Admin NOT Enabled)



DEVICE FORMAT*

(Figure 10.5)

**Note*: *A device format will erase ALL of the information stored on the LP50's secure data partition.*

Help and Troubleshooting

Reset Device

If you forget your password or need to reset your device, you can click on the '*Reset Device*' button that appears in one of two places depending on how the drive is set up(either on the Admin Login Password menu If Admin/User is enabled, or on the 'User Password' Login menu if Admin/User mode is not enabled) when the LP50 Launcher is executed (see *Figure 10.7* and 10.8)

- This option will allow you to create a new password, but to protect the privacy of your data, the LP50 will be formatted. This means that all of your data will be erased in the process.*

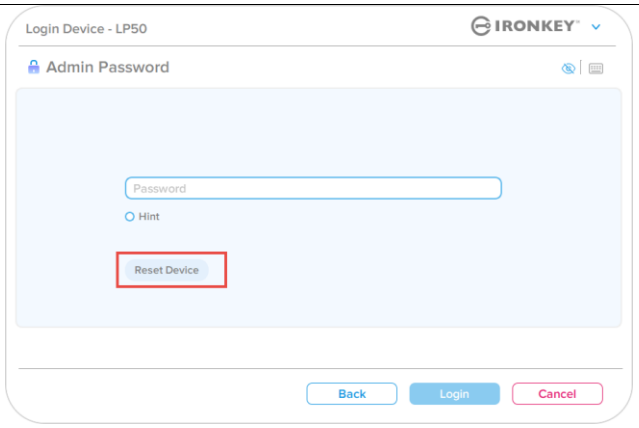


Figure 10.6- Admin Password: Reset Device Button

- **Note:** When you do click on '*Reset Device*', a message box will appear and ask if you want to enter a new password prior to executing the format. At this point, you can either 1) click '*OK*' to confirm or 2) click 'Cancel' to return to the login window. (See figure 9.8)

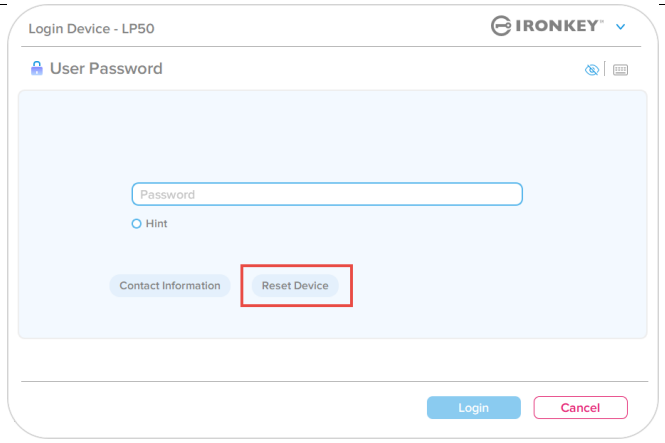


Figure 10.7- User Password (Admin/user not enabled) Reset Device

- If you opt to continue, you will be prompted to the Initialize screen where you can enable 'Admin and User modes' and enter your new password based on the Password option you choose (Complex or Passphrase). The hint is not a mandatory field, but it can be useful in providing a clue as to what the password is, should the password ever be forgotten

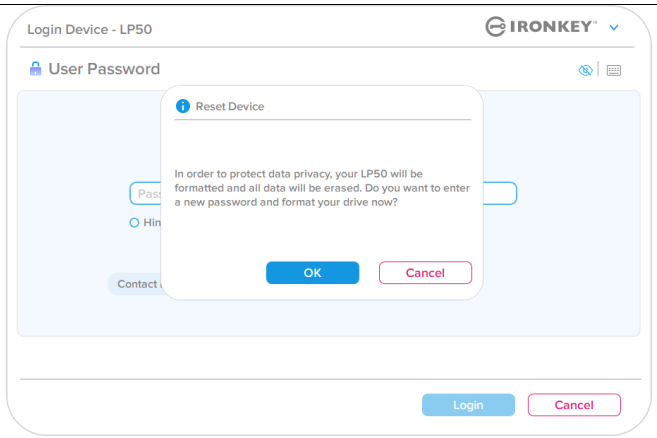


Figure 10.8- Reset device confirmation

Help and Troubleshooting

Drive Letter Conflict: Windows Operating Systems

- As mentioned in the '*System Requirements*' section of this manual (on page 3), the LP50 requires two consecutive drive letters AFTER the last physical disk that appears before the 'gap' in drive letter assignments (see *Figure 9.10*.) This does NOT pertain to network shares because they are specific to user- profiles and not the system hardware profile itself, thus appearing available to the OS.

- What this means is, Windows may assign the LP50 a drive letter that's already in use by a network share or Universal Naming Convention (UNC) path, causing a drive letter conflict. If this happens, please consult your administrator or helpdesk department on changing drive letter assignments in Windows Disk Management (administrator privileges required.) As mentioned in the '*System Requirements*' section of this manual (on page 3), the LP50 requires two consecutive drive letters AFTER the last physical disk that appears before the 'gap' in drive letter assignments (see *Figure 10.9*) This does NOT pertain to network shares because they are specific to user- profiles and not the system hardware profile itself, thus appearing available to the OS

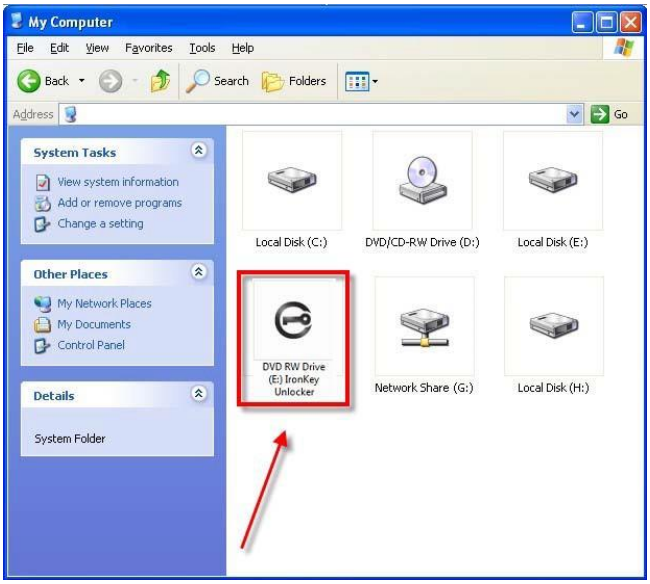


Figure 10.9- Drive Letter example

In this example (Figure 10.9), the LP50 uses drive F:, which is the first available drive letter after drive E: (the last physical disk before the drive letter gap.) Because letter G: is a network share and not part of the hardware profile, the LP50 may attempt to use it as its second drive letter, causing a conflict.

If there are no network shares on your system and the LP50 still won't load, it is possible that a card reader, removable disk, or other previously installed device is holding on to a drive-letter assignment and still causing a conflict.

Please note that Drive Letter Management, or DLM, has improved significantly in Windows 8.1,10 and 11 so you may not come across this issue, but if you are unable to resolve the conflict, please contact Kingston's Technical Support Department or visit Kingston.com/support for further assistance