

IronKey Locker+ 50 G2

Find the language and latest documentation here.

-  For instructions in English
-  Para instrucciones en Español
-  Für Anleitungen in Deutsch
-  Pour des instructions en Français
-  Per le istruzioni in Italiano
-  Por as instruções em Português
-  Instrukcje w języku Polskim
-  日本語マニュアル用

Simplified Chinese 简体中文说明书

Traditional Chinese 繁體中文說明



**IRONKEY™ Locker+ 50 G2
(LP50G2) SECURE USB 3.2 Gen 1
FLASH DRIVE**

User Guide



Contents

Introduction.....	3
Locker+ 50 G2 Features	4
About this Manual	4
System Requirements	4
Recommendations	5
Using the Correct File System.....	5
Usage Reminders	5
Best Practices for Password Setup	6
Setting Up My Device	7
Device Access (Windows Environment).....	7
Device Access (macOS Environment)	7
Device Initialization (Windows & macOS Environment).....	8
Password Selection	9
Virtual Keyboard	11
Password Visibility Toggle.....	12
Admin & User Passwords.....	13
Contact Information.....	15
Device Usage (Windows & macOS Environment)	16
Login for Admin & User (Admin Enabled).....	16
Login for User-Only mode (Admin not enabled)	16
Brute-Force Attack Protection	17
Accessing my secure Files.....	17
Device Options.	18
LP50G2 Settings	20
Admin Settings	20
User Settings: Admin Enabled.....	21
User Settings: Admin Not Enabled	22
Changing and Saving LP50G2 Settings.....	23
Admin Features	24
User Password Reset	24
Help And Troubleshooting	25
LP50G2 Lockout.....	25
LP50G2 Device Reset	27
Drive letter conflict: (Windows)	28



Figure 1: IronKey LP50G2

Introduction

Kingston IronKey™ Locker+ 50 G2 USB Flash drives provides enterprise-grade security with FIPS 197 certified AES 256-bit hardware-encryption in XTS mode, including safeguards against BadUSB and brute force password attacks. LP50G2 is also TAA compliant.

LP50G2 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+50G2 is designed for convenience with a small metal casing and built-in key loop to take data anywhere.

LP50G2 is backed by a limited 5-year warranty with free Kingston technical support.

IronKey Locker+ 50 G2 Features

- FIPS 197 Certified
- 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 (02122026)

This user manual covers the IronKey Locker+ 50 G2 (LP50G2).

System Requirements

PC Platform • Intel & AMD • 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 28.	PC Operating System Support • Windows 11
Mac Platform • Intel & Apple SOC • 15MB free disk space • USB 2.0 - 3.2 Port	Mac Operating System Support • macOS 13.x – 26.x

Recommendations

To ensure there is ample power provided to the LP50G2 device, insert it directly into a USB port on your notebook or desktop, as seen in *Figure 1.1*. Avoid connecting the LP50G2 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 LP50G2 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 LP50G2 on a target system
- When using the drive on a public, or unfamiliar system, you may wish to set the Read-Only mode on the device to help protect the drive from Malware
- 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 issues.

Best Practices for Password Setup

Your LP50G2 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, LP50G2 will automatically wipe out the encrypted data – formatting itself back to a factory state.

Multi-Password

LP50G2 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 LP50G2 can support two different passwords you may use to recover data – Admin and User Password roles

LP50G2 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 all 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 LP50G2 can be Reset and reused, but the prior data will be erased forever.

Password Modes

The LP50G2 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

LP50G2 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 LP50G2 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 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 to the right, the drive letter is (E:).

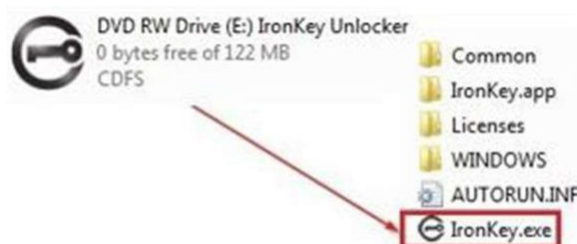


Figure 3.2 – File Explorer Window/IronKey.exe

Device Access (macOS Environment)

Insert the LP50G2 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.

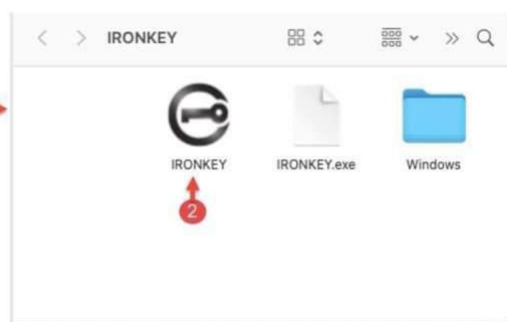


Figure 3.3 – IRONKEY Volume

Device Initialization (Windows & macOS Environment)

Language and EULA

Select your language preference from the drop-down menu and click **Next**. (See *Figure 4.1*)

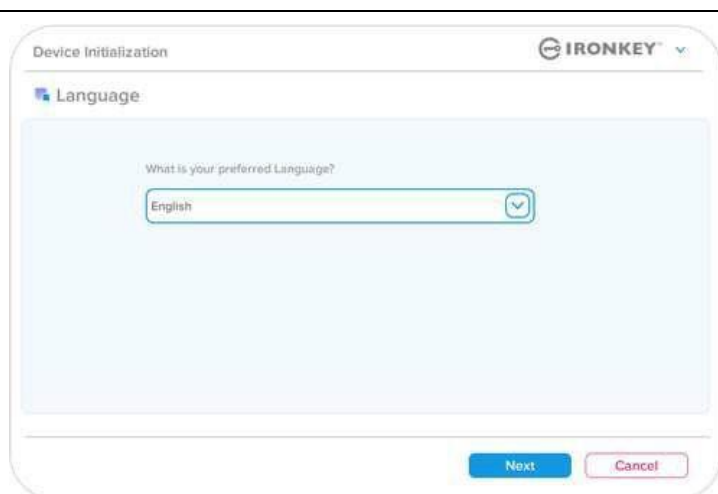


Figure 4.1 – Language Selection

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*)

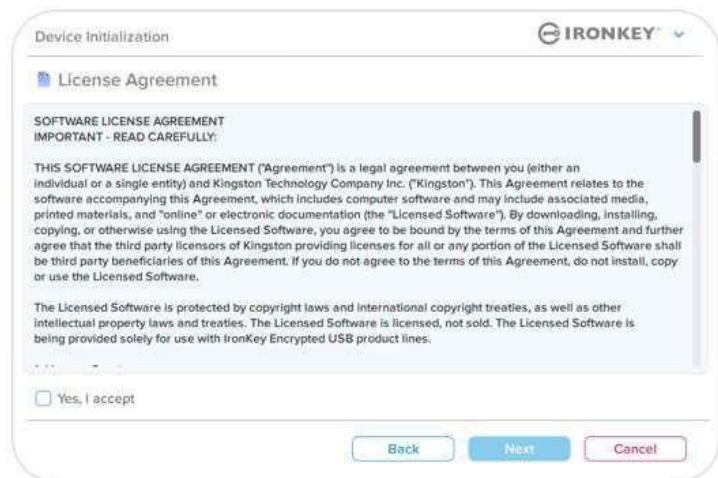


Figure 4.2 – License Agreement

Device Initialization

Password Selection

On the Password prompt screen, you will be able to create a password to protect your data on the LP50G2 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..)

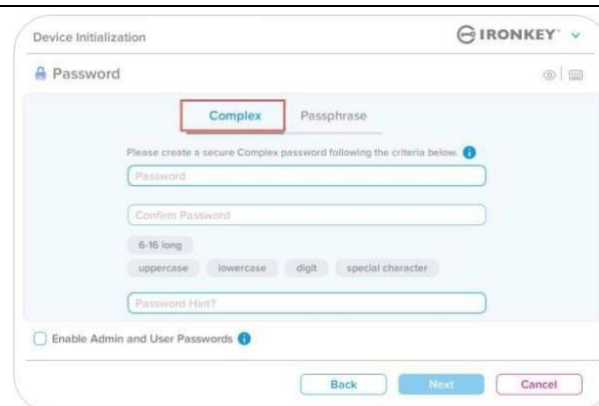


Figure 4.3 – Complex Password

Passphrase Password

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

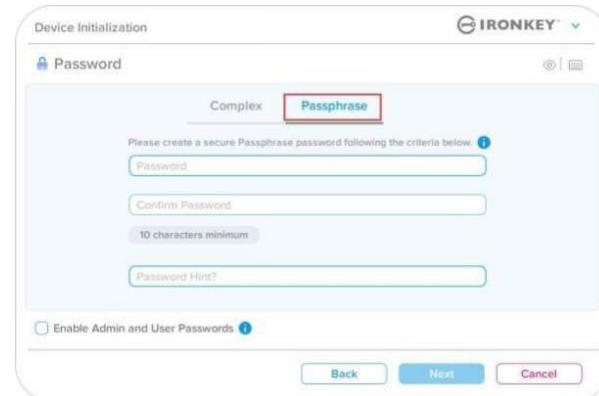


Figure 4.4 – Passphrase Password

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.

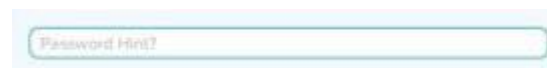
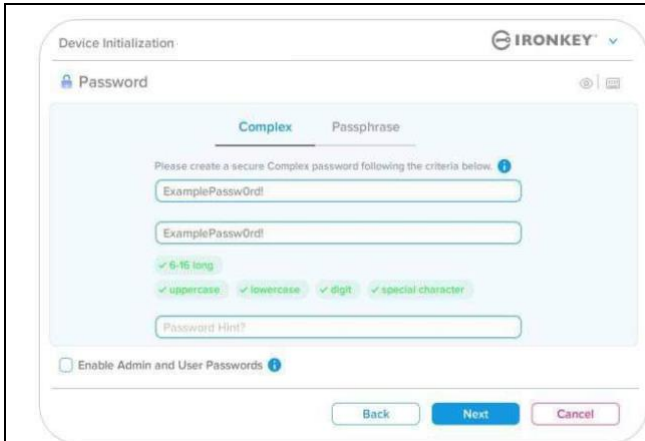


Figure 4.5 – Password Hint Field

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*)



Device Initialization

IRONKEY

Password

Complex Passphrase

Please create a secure Complex password following the criteria below.

ExamplePassw0rd!

ExamplePassw0rd!

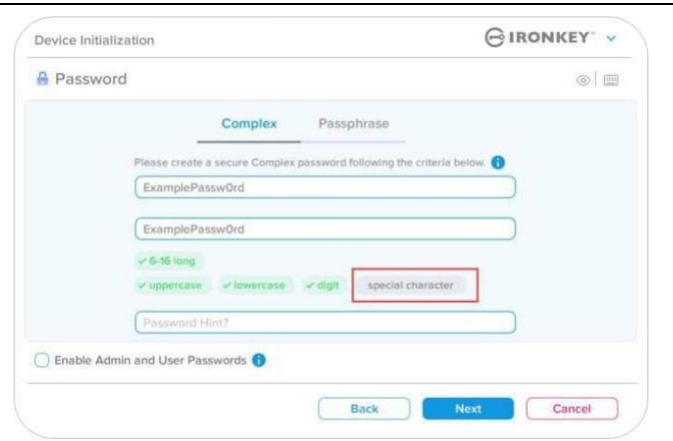
✓ 6-16 long ✓ uppercase ✓ lowercase ✓ digit ✓ special character

Password Hint?

☐ Enable Admin and User Passwords

Back Next Cancel

Figure 4.6a – Complex Password Condition Met



Device Initialization

IRONKEY

Password

Complex Passphrase

Please create a secure Complex password following the criteria below.

ExamplePassw0rd

ExamplePassw0rd

✓ 6-16 long ✓ uppercase ✓ lowercase ✓ digit special character

Password Hint?

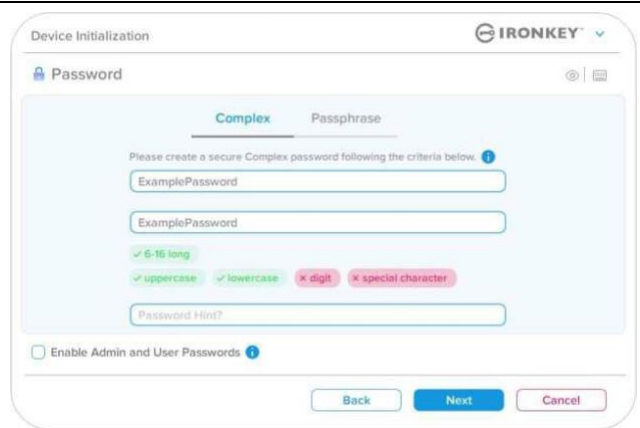
☐ Enable Admin and User Passwords

Back Next Cancel

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.



Device Initialization

IRONKEY

Password

Complex Passphrase

Please create a secure Complex password following the criteria below.

ExamplePassword

ExamplePassword

✓ 6-16 long ✓ uppercase ✓ lowercase ✗ digit ✗ special character

Password Hint?

☐ Enable Admin and User Passwords

Back Next Cancel

Figure 4.7 – Password Conditions Not Met

Device Initialization

Virtual Keyboard

The LP50G2 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.

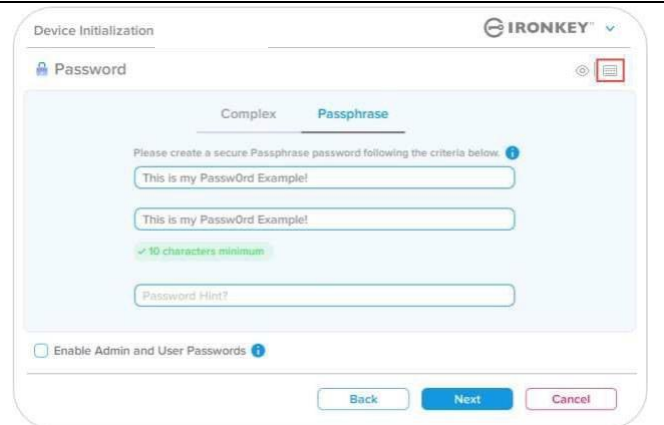


Figure 4.8 – Activating the Virtual Keyboard

- 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** (randomize) in the lower-right of the keyboard. Randomize will arrange the keyboard in a random order.



Figure 4.9 – Screenlogger Protection / Randomize

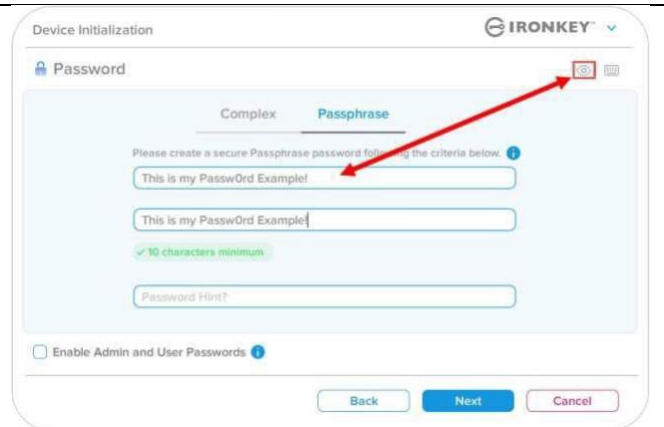
Device Initialization

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-right hand side of the Device Initialization window.

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

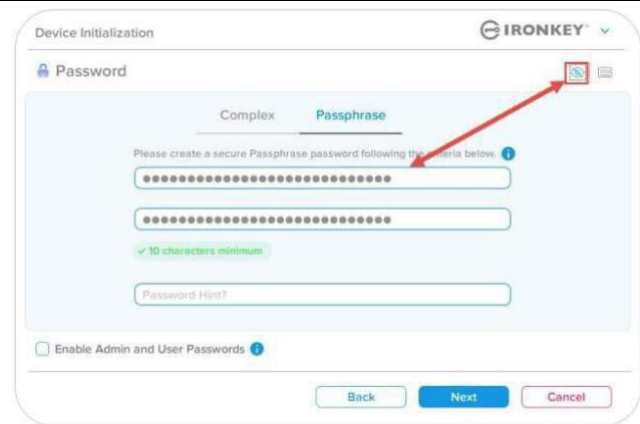
To **hide** the password string, click the gray icon.

The screenshot shows the 'Device Initialization' window with the 'Password' section. The 'Passphrase' tab is selected. The password field contains 'This is my Password Example!'. A red arrow points to the gray eye icon in the top right corner of the password field.

Figure 4.10 – Toggle 'hide' Password

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

The screenshot shows the 'Device Initialization' window with the 'Password' section. The 'Passphrase' tab is selected. The password field is filled with dots. A red arrow points to the blue eye icon in the top right corner of the password field.

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 24 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.

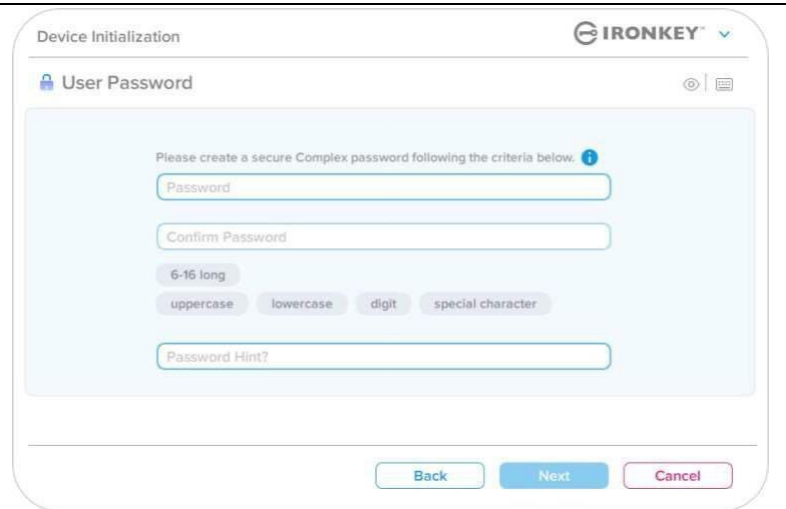
If the drive is set up with this feature NOT enabled (box unchecked), then the drive will be configured as a **Single User, Single Password** drive **without any Admin features**. This configuration will be referred to **User-Only mode** throughout this manual.

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 Moving forward. **Note:** 'Admin and User Passwords' will be referred to as 'Admin Role' throughout this manual for the remainder of this document.



Device Initialization

IRONKEY

User Password

Please create a secure Complex password following the criteria below. ⓘ

Password

Confirm Password

6-16 long

uppercase lowercase digit special character

Password Hint?

Back Next Cancel

Figure 4.13 - User Password (Admin and User Enabled)

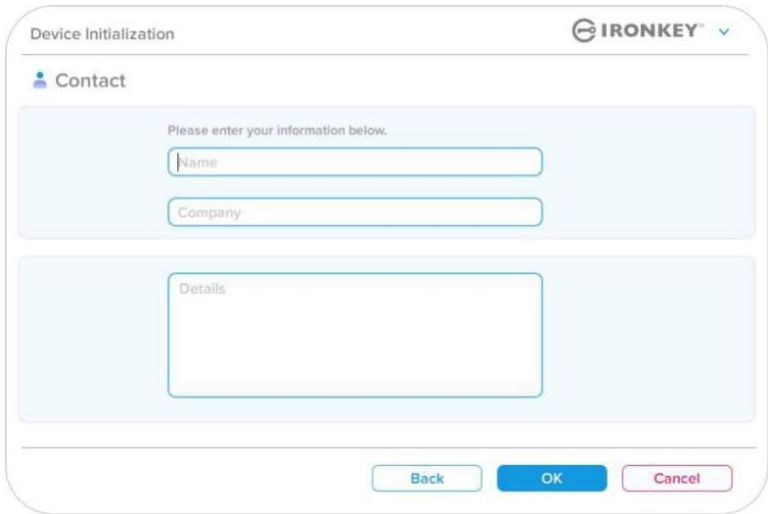
Note: The chosen Password Option (Complex or Passphrase) criteria will carry over to the User Password, and to any password resets that are needed after the drive is set up. The chosen password option may only be changed after a full device reset.

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 upto 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.

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 LP50G2 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*).

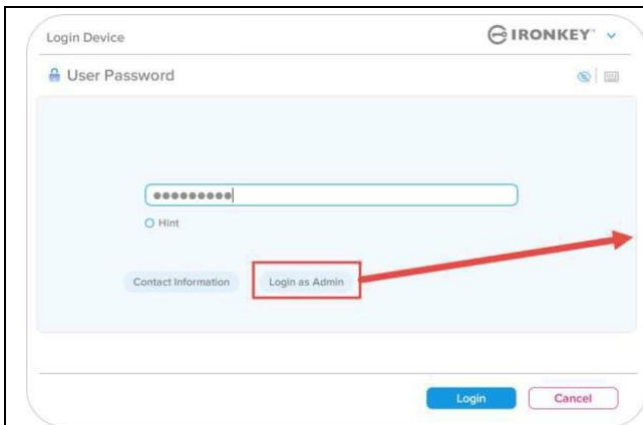


Figure 6.1 - User Password Login (Admin enabled)

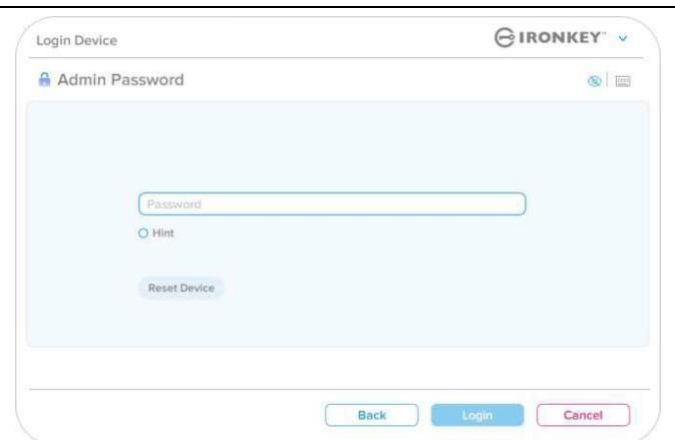


Figure 6.2 - Admin Password Login

Login for User-Only Mode (Admin not Enabled)

As 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 6.3*)

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.**

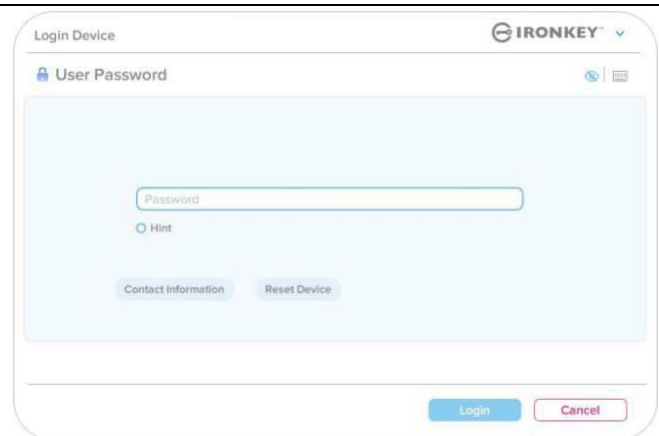


Figure 6.3 - User Password Login (Admin not enabled)

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 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 <u>NOT</u> 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

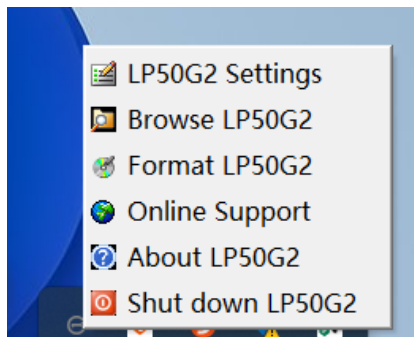
After unlocking the drive, you can access your secure files. Files are automatically encrypted and decrypted when you save or open them on the drive. This technology gives you the convenience of working as you normally would with a regular drive, while providing strong, “always-on” security.

Hint: You can also access your files by right clicking the **IronKey Icon** in the Windows taskbar and clicking **Browse LP50G2** (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 of the window. Right-clicking on the IronKey Icon will open the selection menu for available drive Options (*Figure 6.2*).

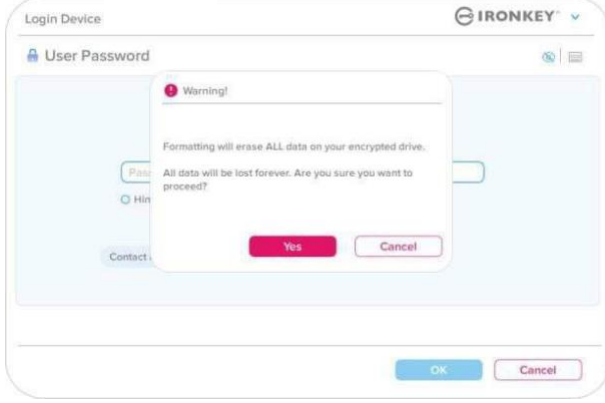
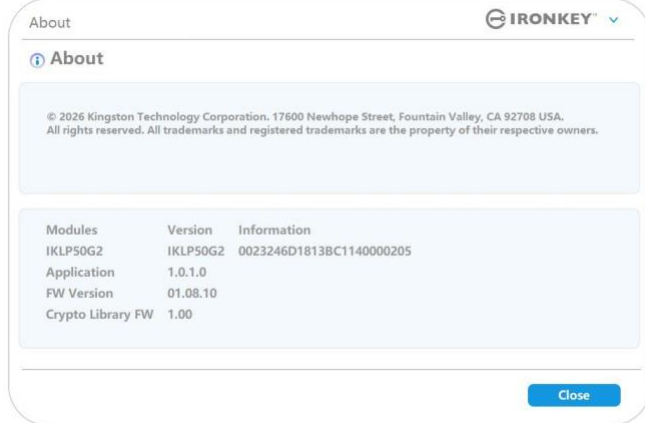
Details about these device options can be found on Pages 19-23 of this manual

While you are logged into the device, there will be an IronKey Icon located in the right-hand corner the Window. (<i>Figure 7.1</i>)	 Figure 7.1 IronKey Icon in Taskbar
Right clicking on the IronKey Icon will open the selection menu for available drive Options. (<i>Figure 7.2</i>) 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 LP50G2 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

LP50G2 Settings:	Change login Password, Contact Information, and other settings. (More details about device settings can be found in the 'LP50G2 Settings' section of this manual).
Browse LP50G2:	Allows you to view your secure files.
Format LP50G2: Allows you to format the secure data partition. (Warning: All data will be erased.) (Figure 6.1) Note: Password authentication will be required for format.	 Figure 7.4- Format LP50G2
Online Support:	Opens your internet browser and navigates to http://www.kingston.com/support where you can access additional support information.
About LP50G2: Provides specific details about the LP50G2, including Application, Firmware and Serial number Information (Figure 6.2) Note: The unique serial number of the drive will be under the 'Information Column'	 Figure 7.5- About LP50G2
Shut down LP50G2:	Properly shuts down the LP50G2, allowing you to safely remove it from your system.

LP50G2 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

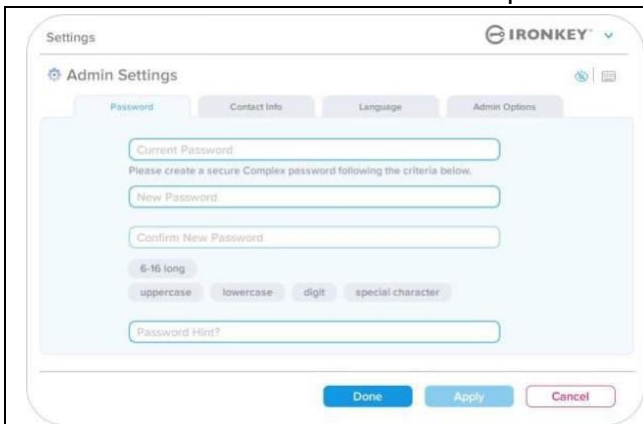


Figure 8.1 – Admin Password Options

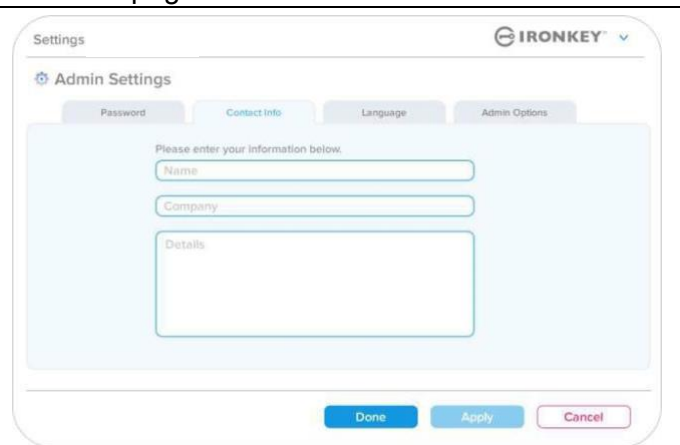


Figure 8.2- Contact Info

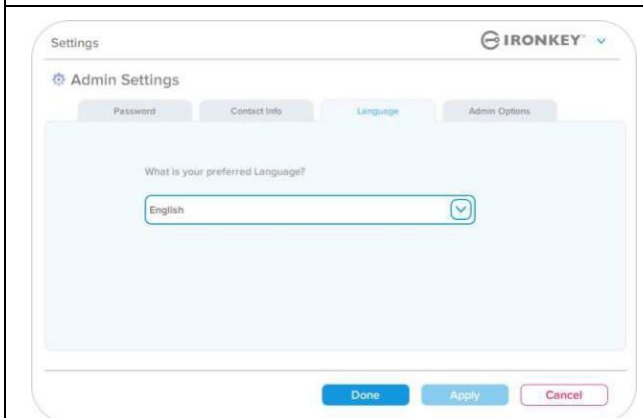


Figure 8.3 - Language Options

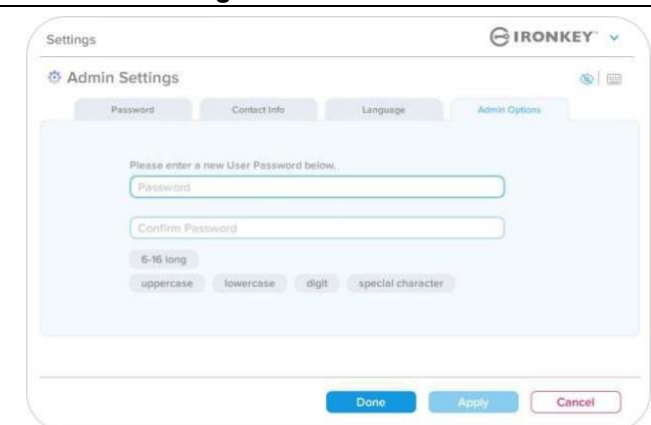


Figure 8.4- Admin Options

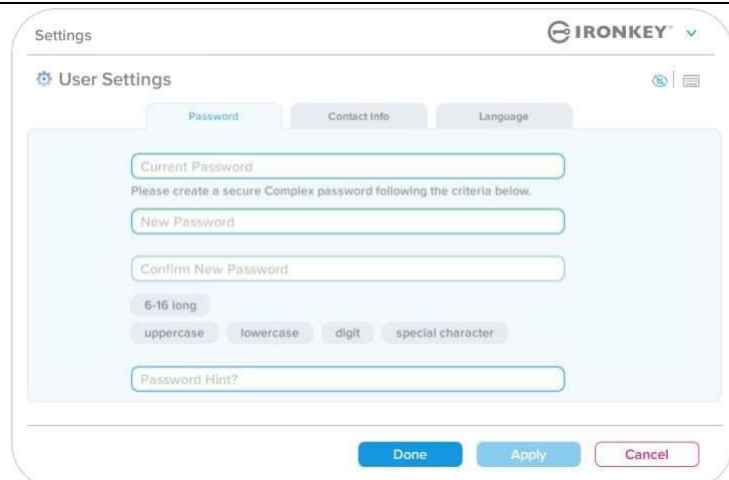
LP50G2 Settings

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 8.5)

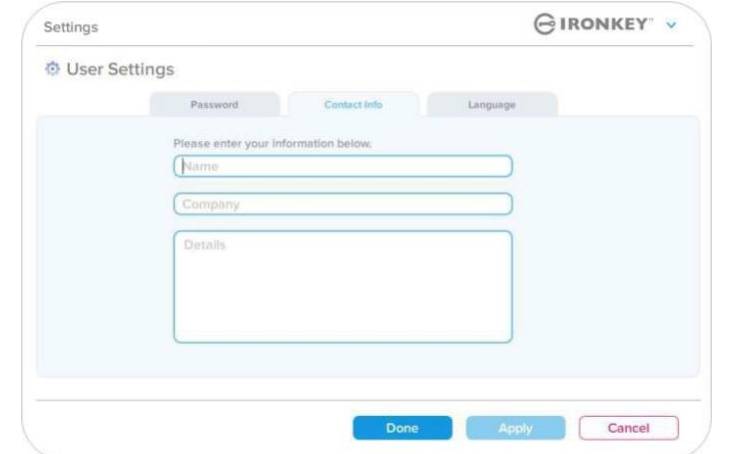


The screenshot shows the 'User Settings' interface with the 'Password' tab selected. It includes input fields for 'Current Password', 'New Password', and 'Confirm New Password'. Below these fields, there are criteria for a secure password: '6-16 long', 'uppercase', 'lowercase', 'digit', and 'special character'. A 'Password Hint?' field is also present. At the bottom, there are 'Done', 'Apply', and 'Cancel' buttons.

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

Contact Info:

Allows you to add/view/change your contact information. (Figure 8.6)

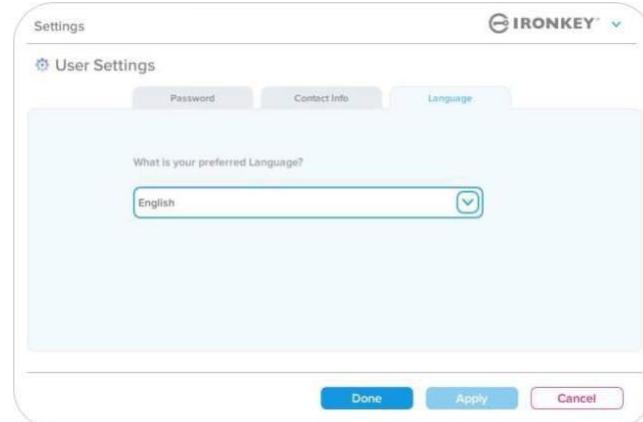


The screenshot shows the 'User Settings' interface with the 'Contact Info' tab selected. It includes input fields for 'Name' and 'Company', and a larger 'Details' text area. At the bottom, there are 'Done', 'Apply', and 'Cancel' buttons.

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

Language:

Allows you to change your current language selection. (Figure 8.7)



The screenshot shows the 'User Settings' interface with the 'Language' tab selected. It includes a dropdown menu labeled 'What is your preferred Language?' with 'English' selected. At the bottom, there are 'Done', 'Apply', and 'Cancel' buttons.

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

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

LP50G2 Settings

User Settings: Admin Not Enabled

As mentioned previously on Page 12, initializing the LP50G2 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 LP50G2 settings.

Password

Allows you to change your own User password and/or hint. (Figure 8.8)

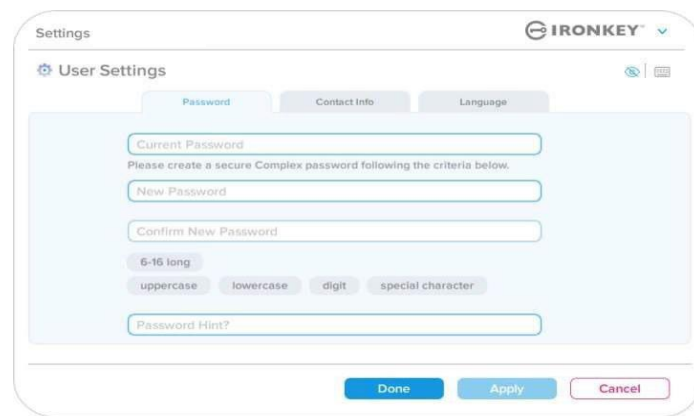


Figure 8.8- Password Options (User-Only Mode)

Contact Info:

Allows you to add/view/change your contact information. (Figure 8.9)

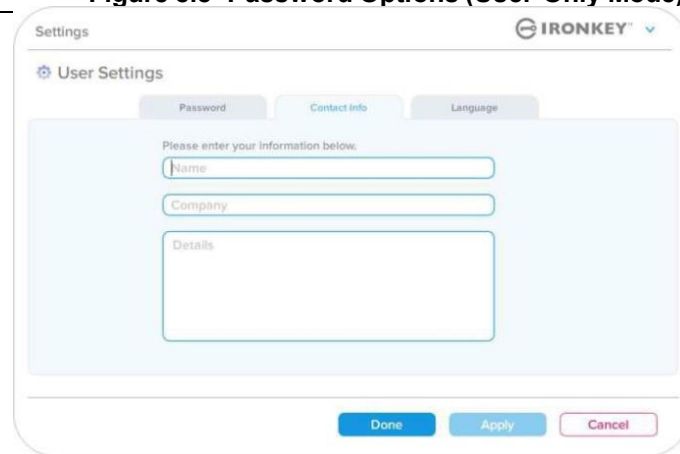


Figure 8.9- Contact Information (User-Only Mode)

Language:

Allows you to change your current language selection. (Figure 8.10)

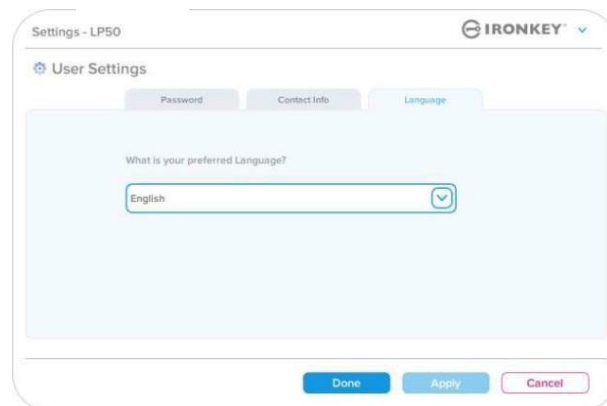


Figure 8.10- Language Settings (User-Only Mode)

LP50G2 Settings

Changing and Saving settings

- Whenever settings are changed in the LP50G2 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*)

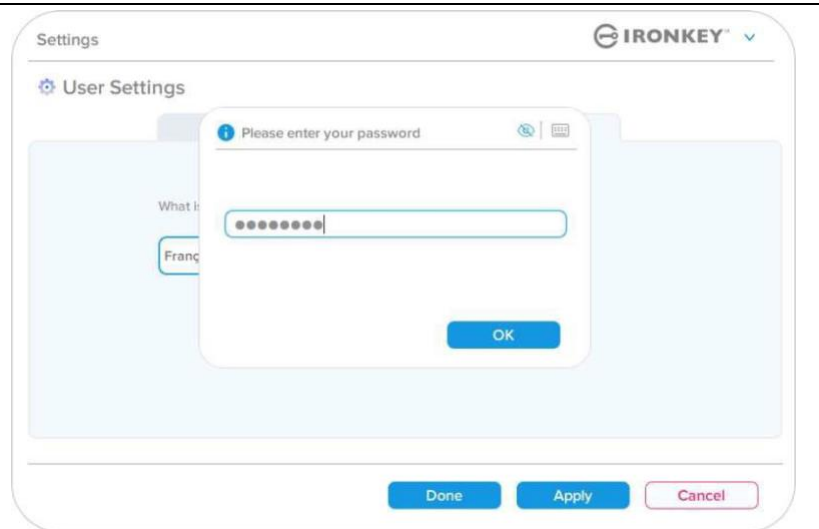


Figure 8.11- Password Prompt screen to save LP50G2 setting changes

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 LP50G2 settings menu.

Admin Features

Option Available to Reset the User Password

One of the useful features of Admin configuration allows 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).

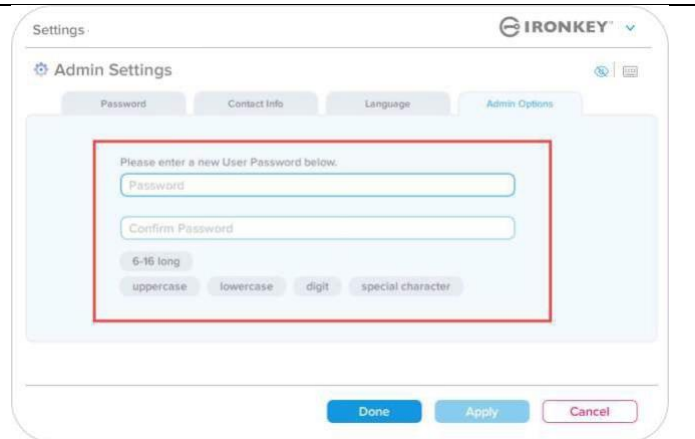


Figure 9.1- Admin Options/User Password Reset

Help and Troubleshooting

Device Lockout

The LP50G2 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*)

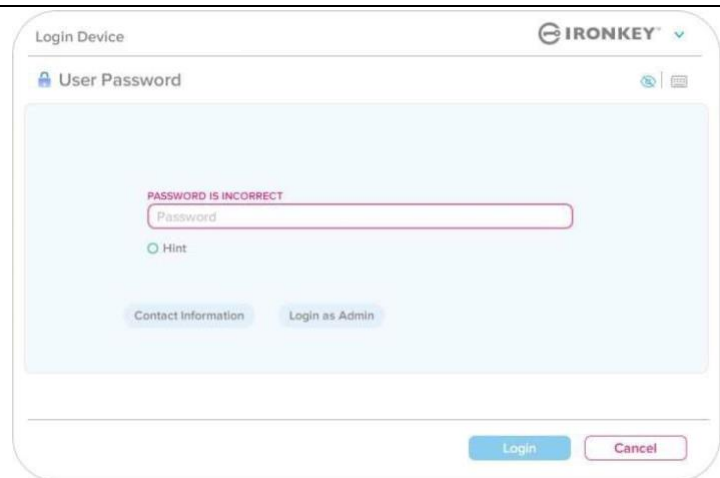


Figure 10.1- Incorrect Password message

- 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*)

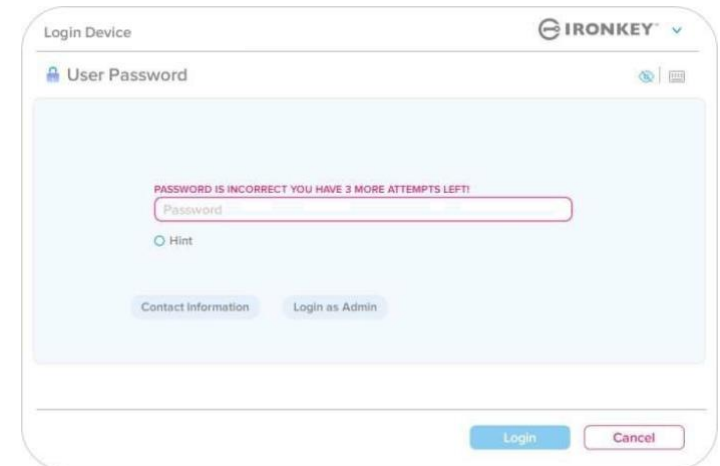


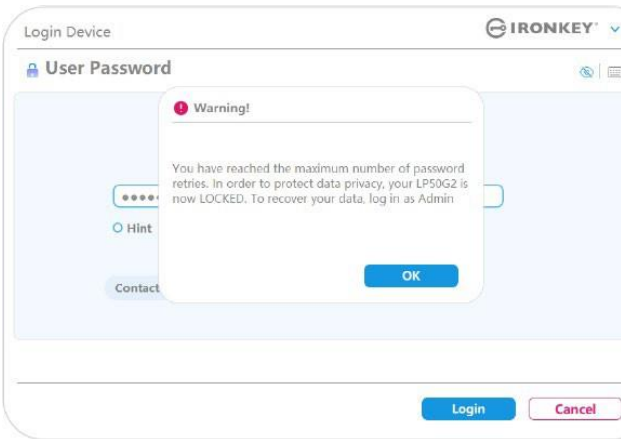
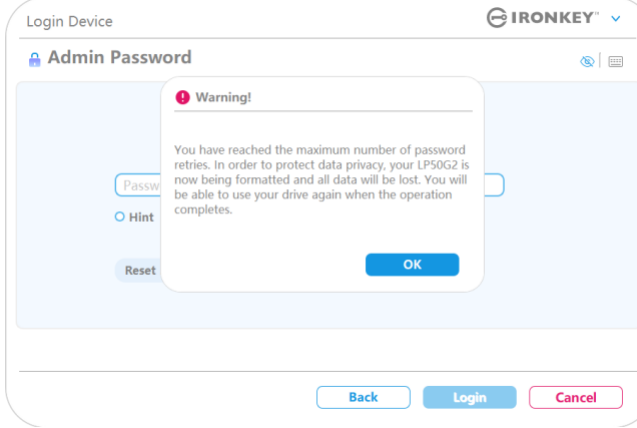
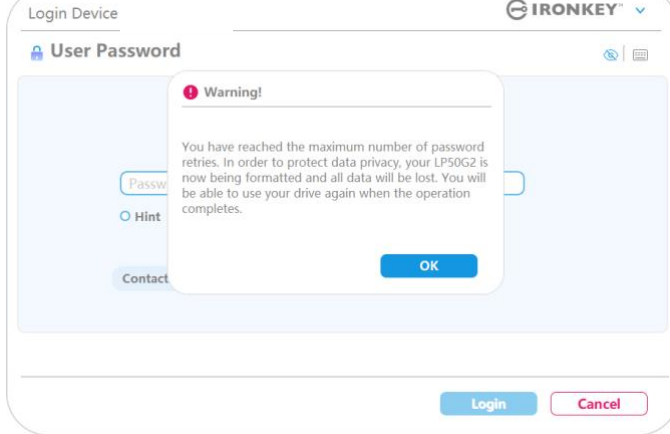
Figure 10.2- 7th incorrect Password attempt

Help and Troubleshooting

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 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 17 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 LP50G2 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 27.	User Password (Admin NOT Enabled)  DEVICE FORMAT* Figure 10.5

***Note:** A device format will erase ALL of the information stored on the LP50G2'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 LP50G2 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 LP50G2 will be formatted. This means that all of your data will be erased in the process.*

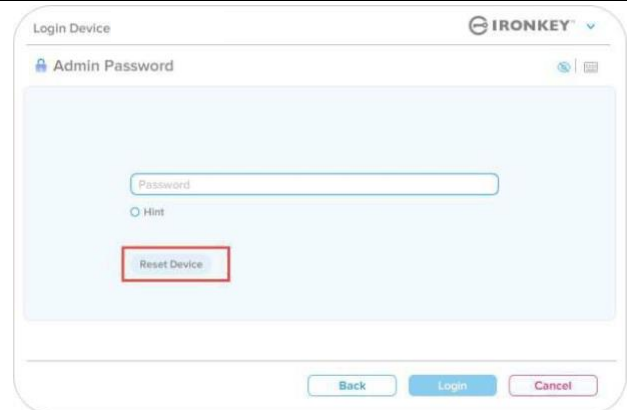


Figure 10.6- Admin Password: Reset Device Button

- 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 10.8)

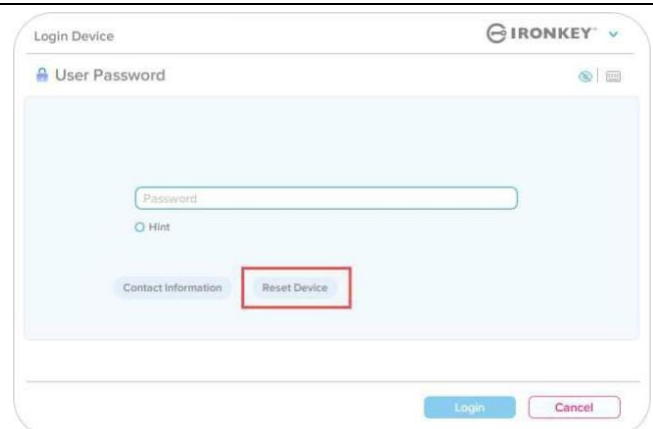


Figure 10.7- User Password (Admin/user not enabled) Reset Device

- 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.

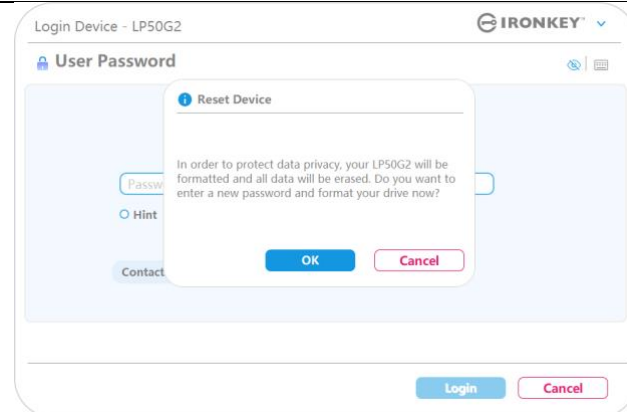


Figure 10.8- Reset device confirmation

Drive Letter Conflict: Windows Operating Systems

- As mentioned in the 'System Requirements' section of this manual (on page 4), the LP50G2 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.
- What this means is, Windows may assign the LP50G2 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.)

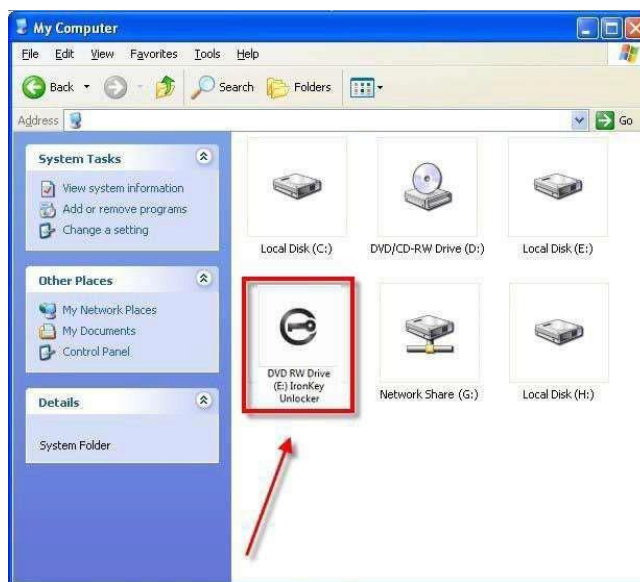


Figure 10.9- Drive Letter example

In this example (*Figure 10.9*), the LP50G2 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 LP50G2 may attempt to use it as its second drive letter, causing a conflict.

If there are no network shares on your system and the LP50G2 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 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](https://www.kingston.com/support) for further assistance.



UNIDAD FLASH IRONKEY™
Locker+ 50 G2 (LP50G2) SEGURA
USB 3.2 Gen 1

Guía de usuario



Contenidos

Introducción	3
Características de Locker+ 50 G2	4
Acerca de este Manual	4
Requisitos del sistema	4
Recomendaciones	5
Uso correcto del sistema de archivos	5
Recordatorios de uso	5
Mejores prácticas para la configuración de contraseñas	6
Configurar mi dispositivo	7
Acceso al dispositivo (Entorno Windows)	7
Acceso al dispositivo (Entorno macOS)	7
Inicialización del dispositivo (Entorno Windows y macOS)	8
Selección de contraseña	9
Teclado virtual	11
Activar visibilidad de contraseña	12
Contraseñas de Administrador y Usuario	13
Información de Contacto	15
Uso del dispositivo (Entorno Windows y macOS)	16
Inicio de sesión para Administrador/Usuario (Administrador habilitado)	16
Inicio de sesión para el modo de Solo usuario (Administrador no habilitado)	16
Protección contra Ataques de fuerza bruta	17
Acceso a mis archivos seguros	17
Opciones del dispositivo	18
Configuración del LP50G2	20
Configuración de administrador	20
Configuraciones de usuario: Administrador habilitado	21
Configuraciones de usuario: Administrador no habilitado	22
Cambiar y guardar la configuración del LP50G2	23
Funciones de administrador	24
Restablecer contraseña de Usuario	24
Ayuda y resolución de problemas	25
Bloqueo del LP50G2	25
LP50G2 Reinicio del dispositivo	27
Conflicto de letras de unidad: (Windows)	28



Figura 1: IronKey LP50G2

Introducción

Las unidades flash USB Kingston IronKey™ Locker+ 50 G2 proporcionan seguridad de nivel empresarial con certificación FIPS 197 y encriptado por hardware AES de 256 bits en modo XTS, incluyendo protecciones contra BadUSB y ataques de fuerza bruta contra contraseñas. LP50G2 también cumple con TAA.

LP50G2 ahora admite la opción de contraseñas múltiples (administrador y usuario) con los modos Complejo o Frase de contraseña. El modo Complejo permite contraseñas de 6 a 16 caracteres utilizando 3 de cada 4 conjuntos de caracteres. El modo de Frase de contraseña permite un PIN numérico, una frase, un listado de palabras o incluso letras de canciones de 10 a 64 caracteres. El Administrador puede habilitar la contraseña de Usuario o restablecer la contraseña de Usuario para restaurar el acceso a los datos. A modo de ayuda al introducir la contraseña, se puede habilitar el símbolo de “ojo” para revelar la contraseña escrita, lo que reduce los errores tipográficos que llevan a intentos fallidos de inicio de sesión. La protección contra ataques de fuerza bruta bloquea al Usuario cuando se introducen 10 contraseñas no válidas consecutivas, y borra con encriptado la unidad si la contraseña de administrador se introduce incorrectamente 10 veces consecutivas. Además, el teclado virtual incorporado protege las contraseñas de los registradores de teclas (keyloggers) o registradores de pantalla (screenloggers).

El Locker+ 50 G2 está diseñado para su comodidad con una pequeña carcasa de metal y un llavero integrado para llevar datos a cualquier lugar.

LP50G2 está respaldado por una garantía limitada de 5 años con soporte técnico gratuito de Kingston.

Características de Locker+ 50 G2

- Certificación FIPS 197
- Encriptado por hardware XTS-AES (el encriptado nunca se puede desactivar)
- Protección contra ataques de fuerza bruta y BadUSB
- Opciones de Múltiples contraseñas
- Modos de contraseña Complejo o de Frase de contraseña
- Símbolo de “ojo” para mostrar las contraseñas introducidas y reducir los intentos fallidos de inicio de sesión
- Teclado virtual para proteger contra keyloggers y screenloggers
- Compatible con Windows o macOS (consulte la hoja de datos para más detalles)

Acerca de este Manual (02122026)

Este manual de usuario cubre el IronKey Locker+ 50 G2 (LP50G2).

Requisitos del sistema

Plataforma de PC • Intel y AMD • Espacio libre en disco de 15 MB • Puerto USB 2.0 - 3.2 disponible • Dos letras de unidad consecutivas después de la última unidad física * *Nota: Consulte "Conflicto de letras de unidad" en la página 28.	Compatibilidad con el sistema operativo de PC • Windows 11
Plataforma Mac • Intel y Apple SOC • Espacio libre en disco de 15 MB • Puerto USB 2.0 - 3.2	Compatibilidad con el sistema operativo Mac • macOS 13.x – 26.x

Recomendaciones

Para asegurarse de que el dispositivo LP50G2 recibe suficiente energía, insértelo directamente en un puerto USB de su computadora portátil o de escritorio, como se ve en la *Figura 1.1*. Evite conectar el LP50G2 a cualquier dispositivo periférico que pueda tener un puerto USB, como un teclado o un concentrador alimentado por USB, como se ve en la *Figura 1.2*.



Figura 1.1 – Uso recomendado



Figura 1.2 – No se recomienda

Uso correcto del sistema de archivos

El IronKey LP50G2 viene preformateado con el sistema de archivos FAT32. Funcionará en sistemas Windows y macOS. Sin embargo, podría haber algunas otras opciones que podrían usarse para formatear el dispositivo manualmente, como NTFS para Windows y exFAT. Puede reformatear la partición de datos si es necesario, pero los datos se pierden cuando se reformatea la unidad.

Recordatorios de uso

Para mantener sus datos seguros, Kingston recomienda:

- Realizar un análisis de virus en su computadora antes de configurar y usar el LP50G2 en un sistema de destino
- Cuando utilice el dispositivo en un sistema público o desconocido, es posible que desee configurar el Modo de solo lectura en el dispositivo para ayudar a proteger el dispositivo del malware
- Bloquear el dispositivo cuando no esté en uso
- Expulsar la unidad antes de desenchufarla
- Nunca desenchufar el dispositivo cuando el LED esté encendido. Esto puede dañar el dispositivo y requerir un nuevo formato, que borrará sus datos
- Nunca compartir la contraseña de su dispositivo con nadie

Encuentre las últimas actualizaciones e información

Visite kingston.com/support para obtener las últimas actualizaciones de la unidad, preguntas frecuentes, documentación e información adicional.

NOTA: Solo deben aplicarse a la unidad las últimas actualizaciones disponibles (cuando estén disponibles). No se admite la degradación de la unidad a una versión anterior del software, ya que podría provocar la pérdida de los datos almacenados o afectar al funcionamiento de la unidad. Si tiene preguntas o problemas, póngase en contacto con el soporte técnico de Kingston.

Mejores prácticas para la configuración de contraseñas

Su LP50G2 viene con fuertes contramedidas de seguridad. Esto incluye protección contra ataques de fuerza bruta que impedirán que un atacante adivine contraseñas al limitar cada tentativa de contraseña a 10 reintentos. Cuando se alcanza el límite de la unidad, el LP50G2 borrará automáticamente los datos encriptados, formateándose al estado de fábrica.

Múltiples contraseñas

El LP50G2 admite Múltiples contraseñas como una característica principal para ayudar a proteger contra la pérdida de datos si se olvidan una o más contraseñas. Cuando todas las opciones de contraseña están habilitadas, el LP50G2 puede admitir dos contraseñas diferentes que puede usar para recuperar datos, funciones de contraseña de administrador y usuario.

El LP50G2 le permite seleccionar dos contraseñas principales: una contraseña de Administrador (denominada contraseña de Admin) y una contraseña de Usuario. El Administrador puede acceder a la unidad en cualquier momento y configurar opciones para el Usuario: el Admin es como un súper usuario.

El Usuario también puede acceder a la unidad, pero en comparación con el Administrador tiene privilegios limitados. Si se olvida una de las dos contraseñas, la otra contraseña se puede utilizar para acceder y recuperar los datos. La unidad se puede configurar de nuevo para que tenga dos contraseñas. Es importante configurar AMBAS contraseñas y guardar la contraseña de Administrador en un lugar seguro mientras se utiliza la contraseña de Usuario.

Si todas las contraseñas se olvidan o se pierden, no hay otra forma de acceder a los datos. Kingston no podrá recuperar los datos, ya que la seguridad no tiene otro respaldo. Kingston recomienda que los datos también se guarden en otros medios. El LP50G2 se puede restablecer y reutilizar, pero los datos anteriores se borrarán para siempre.

Modos de contraseña

El LP50G2 también admite dos modos de contraseña diferentes:

Complejo

Una contraseña compleja requiere cumplir con un mínimo de 6-16 caracteres utilizando al menos 3 de los siguientes caracteres:

- Caracteres alfabéticos en mayúsculas
- Caracteres alfabéticos en minúsculas
- Números
- Caracteres especiales

Frase de contraseña

El LP50G2 admite frases de contraseña de 10 a 64 caracteres. Una frase de contraseña no sigue ninguna regla adicional, pero si se utiliza correctamente, puede proporcionar niveles muy altos de protección de contraseña.

Una frase de contraseña es básicamente cualquier combinación de caracteres, incluidos caracteres de otros idiomas. Al igual que la unidad LP50G2, el idioma de la contraseña puede coincidir con el idioma seleccionado para el dispositivo. Esto le permite seleccionar varias palabras, una frase, letra de una canción, una línea de poesía, etc. Las buenas frases de contraseña se encuentran entre los tipos de contraseña más difíciles de adivinar para un atacante, pero pueden ser más fáciles de recordar para los usuarios.

Configurar mi dispositivo

Para asegurarse de que el dispositivo USB encriptado IronKey recibe suficiente energía, insértelo directamente en un puerto USB 2.0/3.0 de una computadora portátil o de escritorio. Evite conectarlo a cualquier dispositivo periférico que pueda tener un puerto USB, como un teclado o un concentrador alimentado por USB. La configuración inicial del dispositivo debe realizarse en un sistema operativo Windows o macOS compatible.

Acceso al dispositivo (Entorno Windows)

Conecte la unidad USB encriptada IronKey a un puerto USB disponible en el portátil o computadora y espere a que Windows la detecte.

- Los usuarios de Windows recibirán una notificación del controlador del dispositivo. (Figura 3.1)



Figura 3.1 – Notificación del controlador del dispositivo

- Una vez que la detección del nuevo hardware se haya terminado, seleccione la opción **IronKey.exe** dentro de la partición Unlocker que se puede encontrar en el Explorador de archivos. (Figura 3.2)
- Tenga en cuenta que la letra de la partición variará en función de la próxima letra de unidad libre. La letra de la unidad puede cambiar dependiendo de cuales dispositivos estén conectados. En la imagen a continuación, la letra de la unidad es (E:).

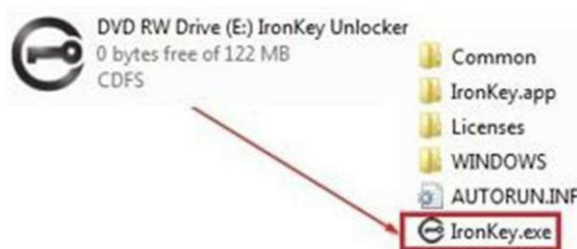


Figura 3.2 – Ventana Explorador de archivos/IronKey.exe

Acceso al dispositivo (Entorno macOS)

Inserte el LP50G2 en un puerto USB disponible en su portátil o computadora y espere a que el sistema operativo Mac lo detecte. Cuando lo haga, verá aparecer el volumen 'IRONKEY' en el escritorio. (Figura 3.3)

- Haga doble clic en el icono de CD-ROM IronKey.
- Luego, haga doble clic en el icono de la aplicación IronKey.app que se encuentra en la ventana que se muestra en la Figura 3.3. Esto comenzará el proceso de inicialización.

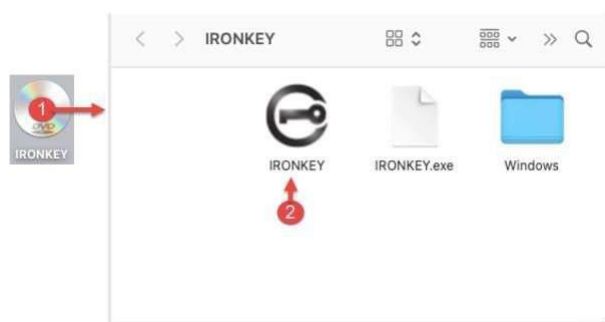


Figura 3.3 – Volumen IRONKEY

Inicialización del dispositivo (Entorno Windows y macOS)

Idioma y EULA o CLUF

Seleccione su idioma de preferencia en el menú desplegable y haga clic en **Siguiente**. (Ver la Figura 4.1)

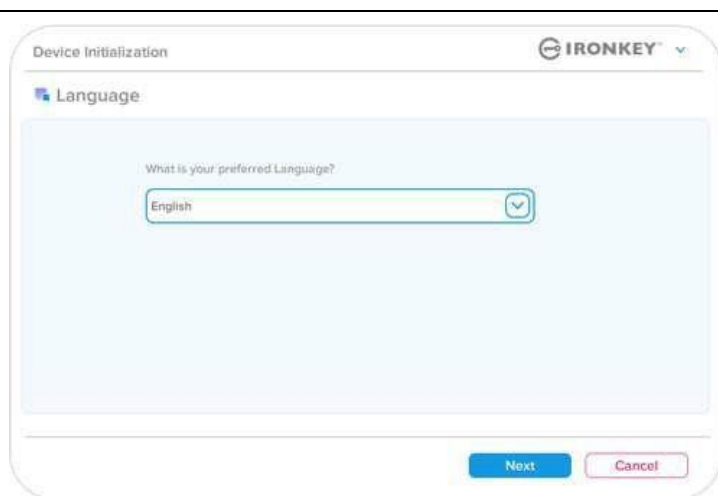


Figura 4.1 – Selección de idioma

Revise el acuerdo de licencia y haga clic en **Siguiente**.

Nota: Debe aceptar el acuerdo de licencia antes de continuar; de lo contrario, el botón **Siguiente** permanecerá deshabilitado. (Figura 4.2)

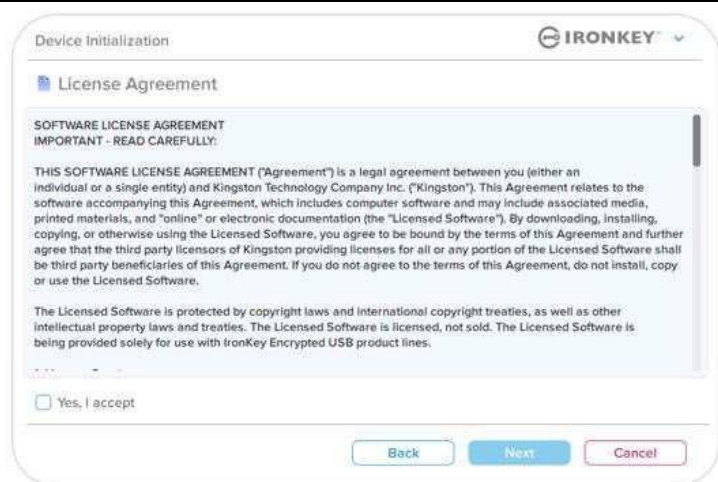


Figura 4.2 – Contrato de licencia

Inicialización del dispositivo

Selección de contraseña

En la pantalla de solicitud de contraseña, podrá crear una contraseña para proteger sus datos en el LP50G2 utilizando los modos de contraseña Complejo o Frase de contraseña (*Figuras 4.3- 4.4*). Además, las opciones de Administrador/Usuario con Contraseña múltiple también se pueden habilitar en esta pantalla. Antes de continuar con la selección de contraseña, consulte la sección de Habilitar contraseñas de Admin/Usuario a continuación para comprender mejor estas funciones.

Nota: Una vez que se elige el modo Complejo o Frase de acceso, el modo no se puede cambiar a menos que se restablezca el dispositivo. Para comenzar con la selección de contraseña, cree su contraseña en el campo "Contraseña" y, a continuación, vuelva a introducirla en los campos "Confirmar contraseña". La contraseña que cree debe cumplir con los siguientes criterios antes de que el proceso de inicialización le permita continuar:

Contraseña compleja

- Debe contener 6 caracteres o más (hasta 16 caracteres).
- Debe contener tres (3) de los siguientes criterios:
 - Mayúsculas
 - Minúsculas
 - Dígito numérico
 - Caracteres especiales (!, \$, &, etc.)

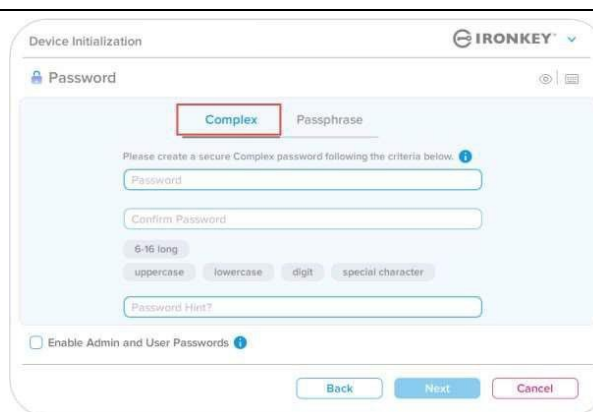


Figura 4.3 – Contraseña compleja

Contraseña de frase de acceso

- Debe contener:
 - 10 caracteres mínimo
 - 64 caracteres como máximo

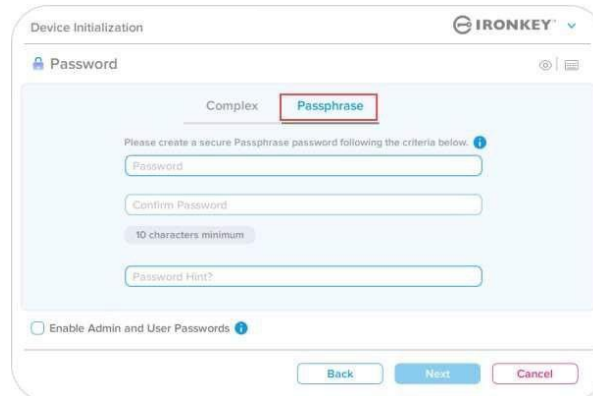


Figura 4.4 – Frase de contraseña

Sugerencia de contraseña (opcional)

Una pista de contraseña puede ser útil para proporcionar una pista sobre la contraseña en caso de que se olvide.

Nota: La pista NO PUEDE coincidir exactamente con la contraseña.

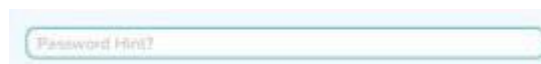


Figura 4.5 – Campo de pista de contraseña

Inicialización del dispositivo

Contraseñas válidas y no válidas

Para las contraseñas **válidas**, las Casillas de criterios de contraseña se resaltarán en **Verde** cuando se cumplan los criterios. (Ver Figuras 4.6a-b) Nota: Una vez que se cumpla el mínimo de tres criterios de contraseña, el cuarto cuadro de criterios se volverá gris, lo que indica que este criterio es opcional (Figura 4.6b)

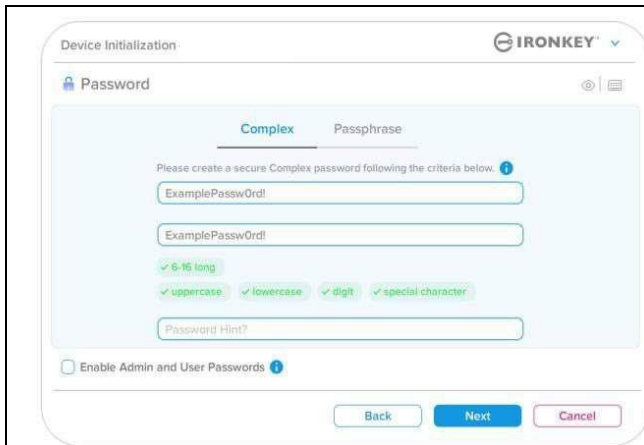


Figura 4.6a – Condición de contraseña compleja cumplida

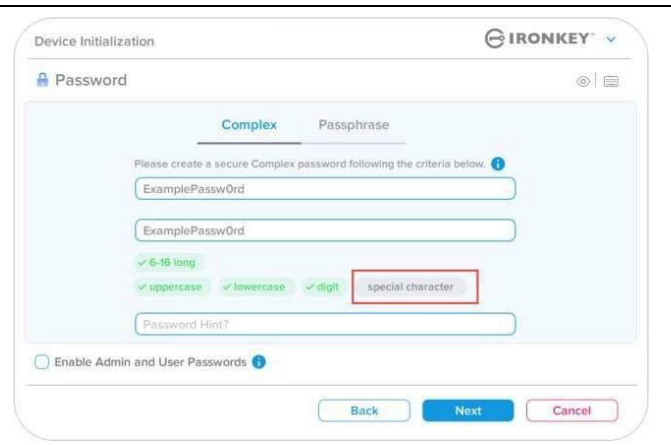


Figura 4.6b – Condición de contraseña compleja opcional

Para contraseñas **no válidas**, los cuadros de criterios de contraseña se resaltarán en **rojo** y el botón **Siguiente** se desactivará hasta que se cumplan los requisitos mínimos.

Esto también se aplica a las contraseñas Complejas y de Frase de contraseña.

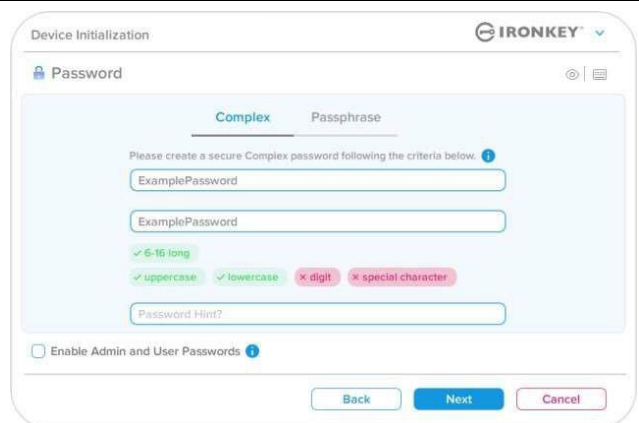


Figura 4.7 – Condiciones de la contraseña no cumplidas

Inicialización del dispositivo

Teclado virtual

El LP50G2 cuenta con un teclado virtual que se puede utilizar para la protección contra Keylogger.

- Para utilizar el **teclado virtual**, ubique el botón del teclado en el lado superior derecho de la pantalla de **inicialización del dispositivo** y selecciónelo.

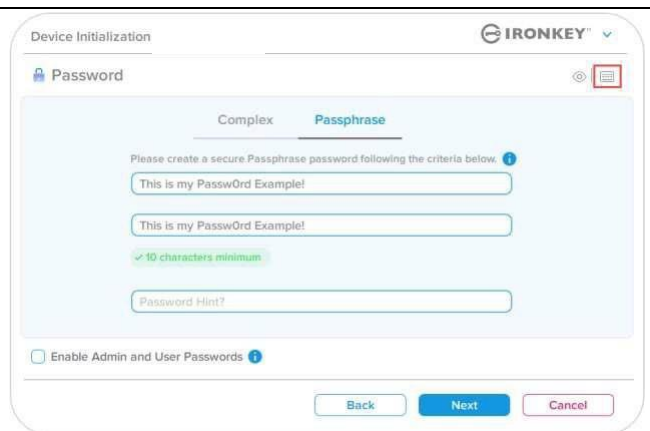


Figura 4.8 – Activación del teclado virtual

- Una vez que aparezca el teclado virtual, también puede habilitar la **Protección contra Screenlogger**. Al usar esta función, todas las teclas se quedarán en blanco brevemente. Este es el comportamiento esperado, ya que evita que los screenloggers capturen a lo que ha hecho clic.
- Para hacer que esta función sea más sólida, también puede optar por aleatorizar el teclado virtual seleccionando **aleatorizar** (randomizar) en la parte inferior derecha del teclado. Aleatorizar organizará el teclado en un orden aleatorio.

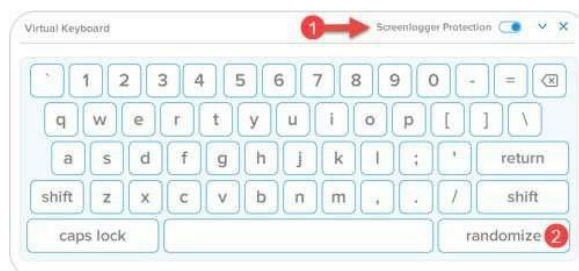


Figura 4.9 – Protección contra Screenlogger / Aleatorizar

Inicialización del dispositivo

Activar visibilidad de contraseña

De forma predeterminada, cuando crea una contraseña, la cadena de contraseña se mostrará en el campo a medida que la escribe. Si desea "ocultar" la cadena de contraseña mientras escribe, puede hacerlo activando el "ojo" de la contraseña ubicado en la parte superior derecha de la ventana de inicialización del dispositivo.

Nota: Después de que el dispositivo se haya inicializado, el campo de contraseña se volverá "oculto" por defecto.

Para **ocultar** la cadena de contraseña, haga clic en el icono gris.

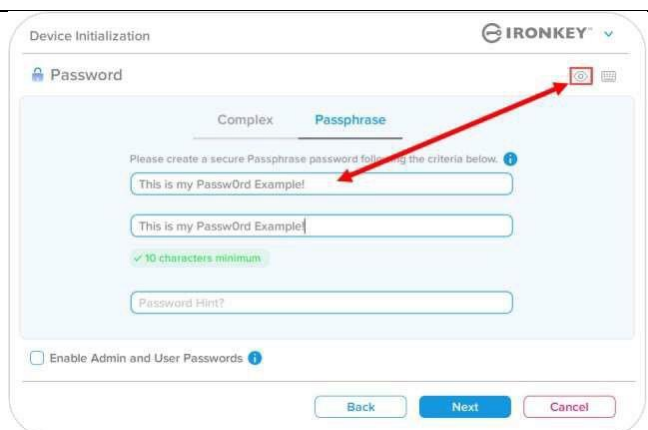


Figura 4.10 – Activar 'ocultar' contraseña

Para **mostrar** la contraseña oculta, haga clic en el icono azul.

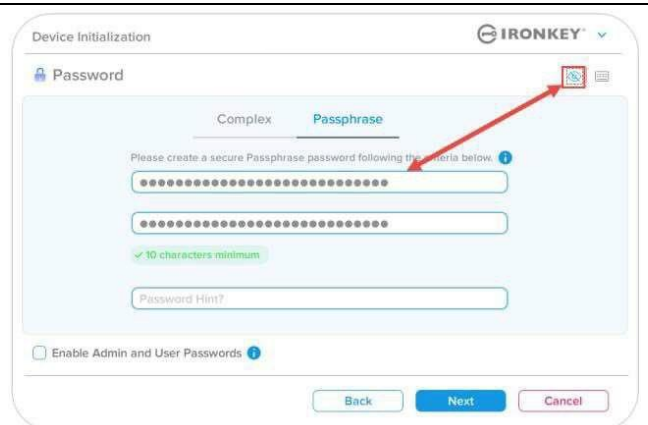


Figura 4.11 – Activar 'mostrar' contraseña

Inicialización del dispositivo

Contraseñas de administrador y usuario

Al habilitar las contraseñas de Administrador y Usuario, puede aprovechar la funcionalidad de contraseñas múltiples, en la que el rol de administrador puede manejar ambas cuentas. Seleccionar **"Habilitar contraseñas de Admin y Usuario"** permite un método alternativo de acceso a la unidad en caso de que se olvide una de las contraseñas.

Con **las contraseñas de Admin y Usuario habilitadas**, también puede acceder a:

- Restablecer contraseña de Usuario

Para obtener más información sobre la función de restablecimiento de contraseña de Usuario, vaya a la página 24 de esta guía del usuario.

- Para habilitar **las contraseñas de Admin y Usuario**, haga clic en la casilla junto a **"Habilitar contraseñas de Admin y usuario"** y seleccione **Siguiente** una vez que haya elegido una contraseña válida. (Figura 4.12)
- Si esta función está **habilitada**, la contraseña elegida en esta pantalla será la **contraseña de Administrador**. Haga clic en **Siguiente** para ir a la pantalla **Contraseña de Usuario** donde se elige una contraseña para el Usuario.

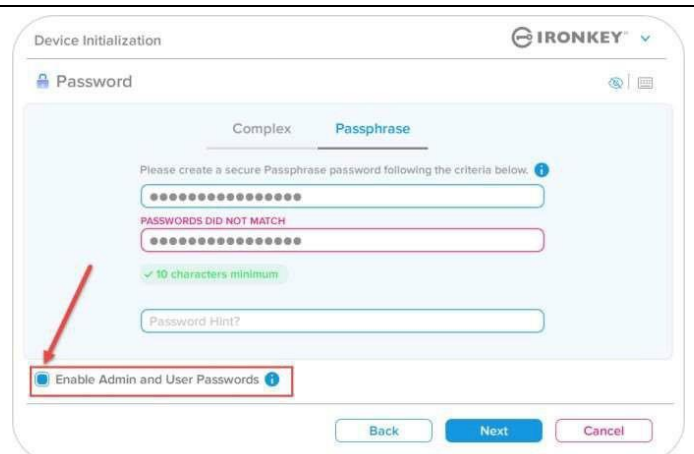


Figura 4.12 – Habilitación de contraseñas de Admin y Usuario

Nota: Habilitar las contraseñas de Admin y Usuario es opcional.

Si la unidad está configurada con esta función NO habilitada (casilla desmarcada), entonces la unidad se configurará como una unidad de **Usuario único** y **Contraseña única sin ninguna función de administrador**. Esta configuración se referirá al **modo de Solo usuario** a lo largo de este manual.

Para continuar con una configuración de Usuario único y Contraseña única, mantenga **Habilitar contraseñas de Administrador y Usuario** sin marcar y haga clic en **Siguiente** después de crear una contraseña válida.

Inicialización del dispositivo

Contraseñas de Administrador y Usuario

Si el rol de administrador se **habilitó** en la pantalla anterior, la siguiente pantalla solicitará la **contraseña de Usuario** (Figura 4.13). La contraseña de Usuario tendrá capacidades limitadas en comparación con el Administrador y se analizará con más detalle en el futuro.

Nota: ‘Las contraseñas de administrador y Usuario’ se denominarán como ‘Rol de Admin’ a lo largo de este manual por el resto de este documento.

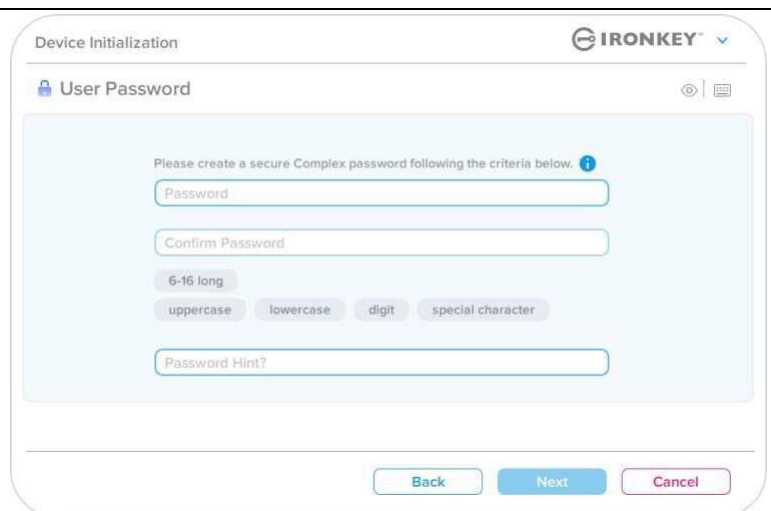


Figura 4.13 – Contraseña de Usuario (administrador y usuario habilitado)

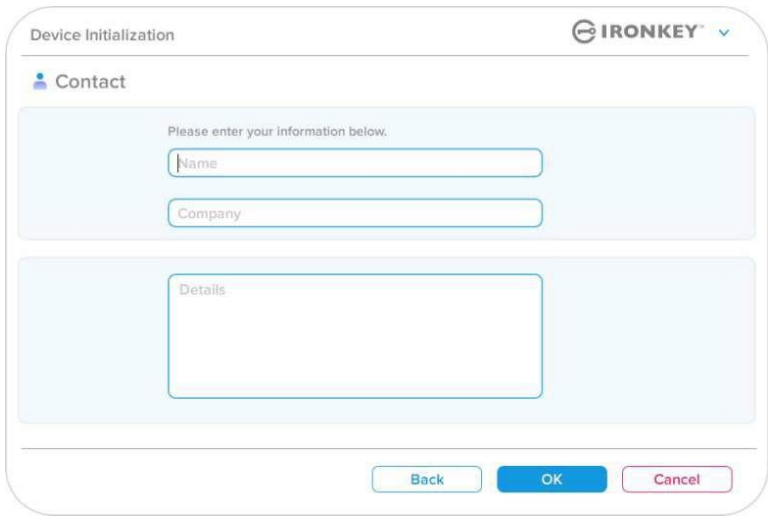
Nota: Los criterios de Opción de contraseña (Complejo o Frase de contraseña) elegidos se transferirán a la contraseña de Usuario y a cualquier restablecimiento de contraseña que sea necesario después de configurar la unidad. La opción de contraseña elegida solo se puede cambiar después de un restablecimiento completo del dispositivo.

Inicialización del dispositivo

Información de Contacto

Ingrese su información de contacto en los cuadros de texto proporcionados. (Ver la Figura 4.14)

Nota: La información que introduzca en estos campos NO puede contener la cadena de contraseña que ha creado en el paso 3. Sin embargo, estos campos son opcionales y se pueden dejar en blanco, si así se desea.

El campo 'Nombre' puede contener hasta 32 caracteres, pero no puede contener la contraseña exacta. El campo 'Compañía' puede contener hasta 32 caracteres, pero no puede contener la contraseña exacta. El campo 'Detalles' puede contener hasta 156 caracteres, pero no puede contener la contraseña exacta.	 Figura 4.14 – Información de contacto
--	---

Nota: Al hacer clic en 'Aceptar', se completará el proceso de inicialización y se procederá a desbloquear, luego montará la partición segura donde sus datos se pueden almacenar de forma segura. Proceda a desenchufar la unidad y vuelva a conectarla al sistema para ver los cambios reflejados.

Uso del dispositivo (Entorno Windows y macOS)

Inicio de sesión para Administrador/Usuario (Administrador habilitado)

Si el dispositivo se inicializa con las contraseñas de Administrador y Usuario habilitadas (rol de Admin), se iniciará la aplicación IronKey LP50G2, solicitando primero la pantalla de inicio de sesión de la contraseña de Usuario. Desde aquí puede iniciar sesión con la contraseña de Usuario, ver cualquier información de contacto ingresada o iniciar sesión como Administrador (*Figura 6.1*). Al hacer clic en el botón "Iniciar sesión como Administrador" (que se muestra a continuación), la aplicación procederá al menú de inicio de sesión de Admin, donde puede iniciar sesión como Administrador para acceder a la configuración y las funciones del Administrador (*Figura 6.2*).

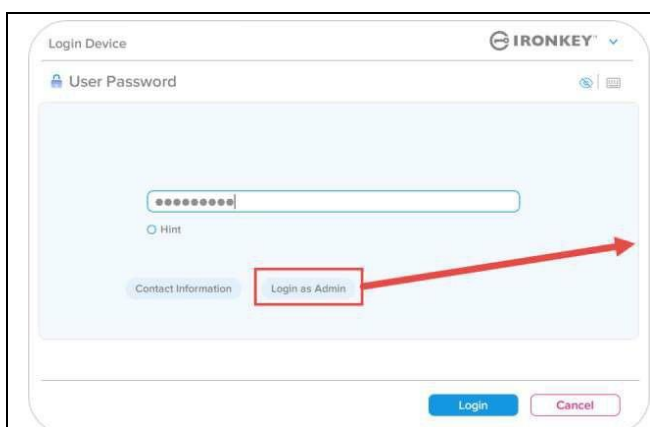


Figura 6.1 – Inicio de sesión con contraseña de Usuario (Administrador habilitado)

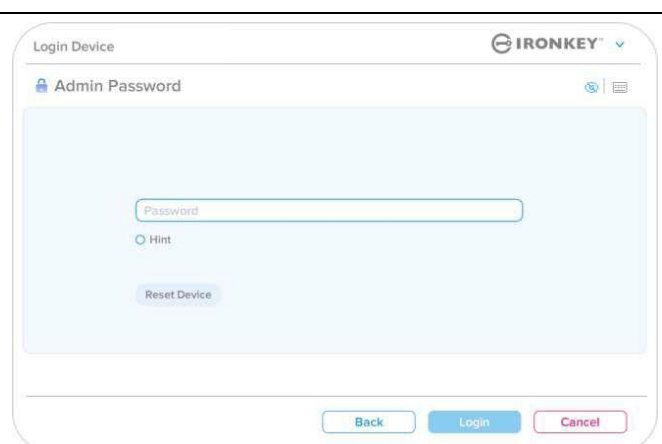


Figura 6.2 – Inicio de sesión con contraseña de Administrador

Inicio de sesión para el Modo de solo usuario (Administrador no habilitado)

Como se mencionó anteriormente en la **página 13**, aunque se recomienda utilizar la funcionalidad de rol de Admin para obtener el máximo beneficio de su dispositivo, la unidad IronKey también se puede inicializar en una configuración de Solo usuario (Contraseña única, Usuario único). Esta es una opción para aquellos que desean un enfoque de contraseña simple y única para proteger los datos en su unidad. (*Figura 6.3*)

Nota: Para habilitar las contraseñas de Administrador y Usuario, utilice el botón **Restablecer dispositivo** para volver a poner la unidad en el estado de inicialización donde puede habilitar las contraseñas de Administrador y Usuario. **TODOS los datos de la unidad se formatearán y se perderán para siempre cuando se produzca un reinicio del dispositivo.**

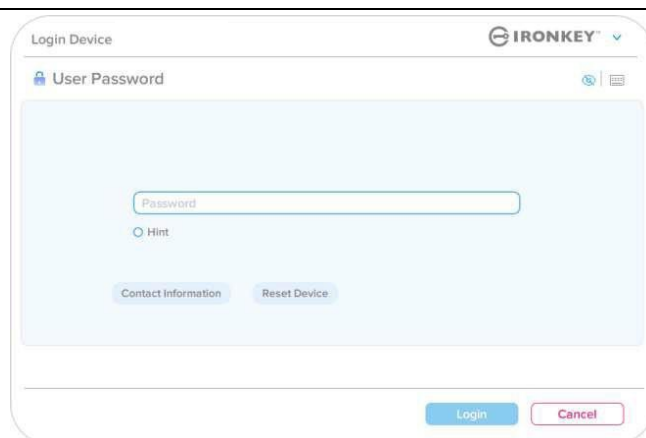


Figura 6.3 – Inicio de sesión con contraseña de Usuario (Administrador no habilitado)

Uso del dispositivo

Protección contra ataques de fuerza bruta

Importante: Durante el inicio de sesión, si se ingresa una contraseña incorrecta, tendrá otra oportunidad de ingresar la contraseña correcta; sin embargo, existe una característica de seguridad integrada (también conocida como protección contra ataques de fuerza bruta) que rastrea la cantidad de intentos fallidos de inicio de sesión. *

Si este número alcanza el valor preconfigurado de 10 intentos fallidos de contraseña, el comportamiento será el siguiente:

Administrador/Usuario habilitado	Comportamiento del dispositivo con protección contra fuerza bruta (10 intentos de contraseña incorrectos)	¿Borrado de datos y reinicio del dispositivo?
Contraseña de usuario:	Bloqueo de la contraseña. Iniciar sesión como Administrador para restablecer la contraseña de Usuario	NO
Contraseña de Administrador	Controlador de borrado criptográfico, Contraseñas, configuraciones y datos borrados para siempre	SÍ
Solo usuario Usuario único, contraseña única (Administrador/Usuario <u>NO</u> habilitado)	Comportamiento del dispositivo con protección contra fuerza bruta (10 intentos de contraseña incorrectos)	¿Borrado de datos y reinicio del dispositivo?
Contraseña de Usuario	Controlador de borrado criptográfico, Contraseñas, configuraciones y datos borrados para siempre	SÍ

* Una vez que se autentique en el dispositivo con éxito, el contador de inicio de sesión fallido se restablecerá en relación con el método de inicio de sesión utilizado. El borrado criptográfico eliminará todas las contraseñas, claves de encriptado y datos; **sus datos se perderán para siempre.**

Acceso a mis archivos seguros

Después de desbloquear el dispositivo puede acceder a sus archivos seguros. Los archivos se cifran y descifran automáticamente cuando los guarda o los abre en el dispositivo. Esta tecnología le brinda la comodidad de trabajar como lo haría normalmente con un dispositivo regular, al tiempo que proporciona una seguridad sólida y "siempre activa".

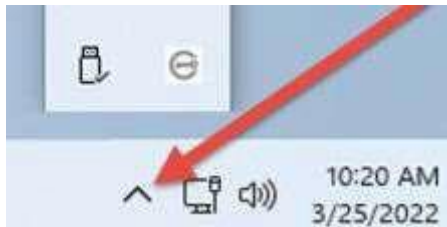
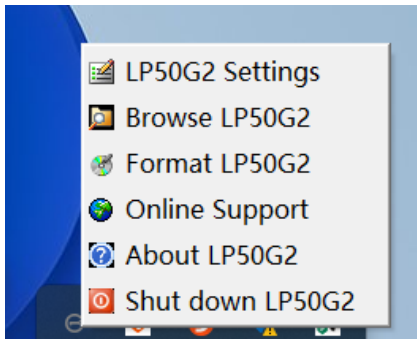
Pista: También puede acceder a sus archivos haciendo clic con el botón derecho en el **icono IronKey** de la barra de tareas de Windows y haciendo clic en

Explorar LP50G2 (Figura 7.2)

Opciones del dispositivo (Entorno Windows)

Mientras esté conectado al dispositivo, habrá un icono de IronKey ubicado en la esquina derecha de la ventana. Al hacer clic con el botón derecho en el icono de IronKey se abrirá el menú de selección de Opciones de dispositivo disponibles (*Figura 6.2*).

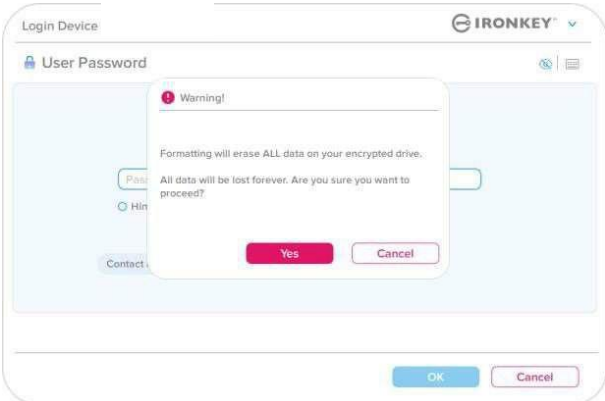
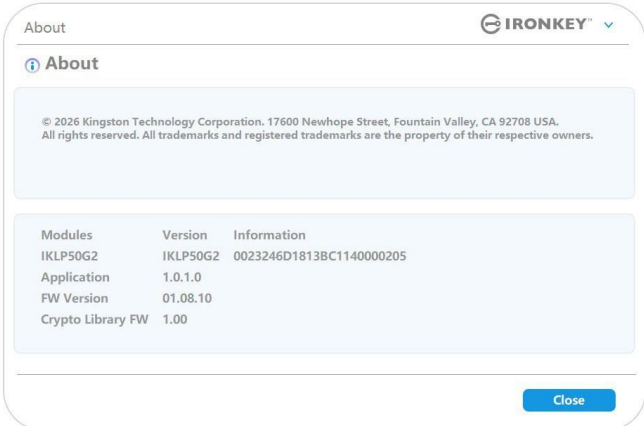
Los detalles sobre estas opciones de dispositivo se pueden encontrar en las páginas 19-23 de este manual

Mientras esté conectado al dispositivo, habrá un icono de IronKey ubicado en la esquina derecha de la ventana. (<i>Figura 7.1</i>)	 Figura 7.1 – Icono de IronKey en la barra de tareas
Al hacer clic con el botón derecho en el icono de IronKey se abrirá el menú de selección de Opciones de dispositivo disponibles. (<i>Figura 7.2</i>) Los detalles sobre estas opciones de dispositivo se pueden encontrar en las páginas 19-23 de este manual.	 Figura 7.2 – Clic con el botón derecho en el icono IronKey para acceder a las opciones del dispositivo.

Opciones del dispositivo (Entorno macOS)

Mientras esté conectado al dispositivo, habrá un ícono de 'IronKey LP50G2' ubicado en el menú de macOS que se ve en la Figura 7.3 que abrirá las opciones disponibles del dispositivo. Los detalles sobre estas opciones de dispositivo se pueden encontrar en las páginas 19-23 de este manual.	 Figura 7.3 – Icono de la barra de menú de macOS/Menú de opciones del dispositivo
--	---

Opciones del dispositivo

Configuración del LP50G2:	• Cambiar la contraseña de inicio de sesión, la información de contacto y otras configuraciones. (Se pueden encontrar más detalles sobre la configuración del dispositivo en la sección ‘Configuración del LP50G2’ de este manual).
Explorar el LP50G2:	• Le permite ver sus archivos seguros.
Formatear el LP50G2: Le permite formatear la partición de datos segura. (Advertencia: Todos los datos serán borrados). (Figura 6.1) Nota: Se requerirá autenticación por contraseña para el proceso de reformato.	 Figura 7.4 – Formato del LP50G2
Soporte en línea:	• Abre su navegador de internet y lo lleva a http://www.kingston.com/support , donde puede tener acceso a información de soporte adicional
Acerca de LP50G2: Proporciona detalles específicos sobre el LP50G2, incluida información sobre la aplicación, el firmware y el número de serie (Figura 6.2) Nota: El número de serie único de la unidad estará en la ‘Columna de Información’	 Figura 7.5 – Acerca del LP50G2
Apagar el LP50G2:	• Apaga correctamente el LP50G2, lo que le permite retirarlo de forma segura de su sistema.

Configuración del LP50G2

Configuración de Administrador

El inicio de sesión de administrador permite acceder a la siguiente configuración del dispositivo:

- **Contraseña:** Le permite cambiar su contraseña de Administrador y/o pista (*Figura 8.1*)
- **Información de contacto:** Le permite agregar/visualizar/cambiar su información de contacto (*Figura 8.2*)
- **Idioma:** Le permite cambiar su selección de idioma actual (*Figura 8.3*)
- **Opciones de Administrador** Le permite acceder a funciones adicionales como:
 - Cambiar la contraseña de Usuario (*Figura 8.4*)

NOTA: Se pueden encontrar detalles adicionales de las opciones de Administrador en la página 25

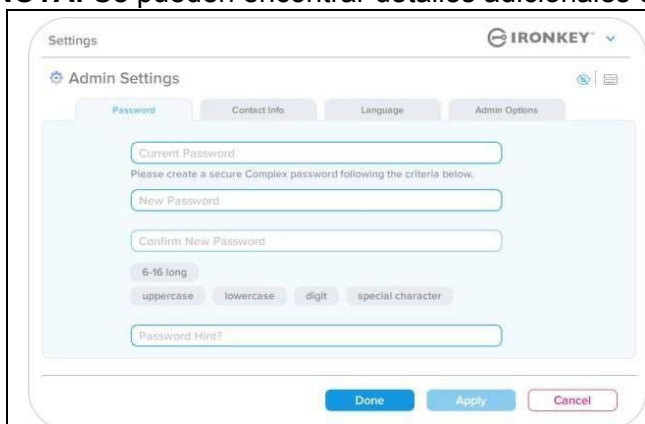


Figura 8.1 – Opciones de contraseña de administrador

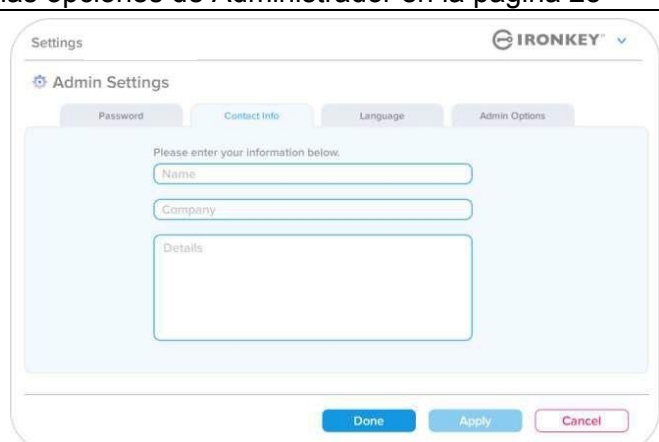


Figura 8.2 – Información de contacto

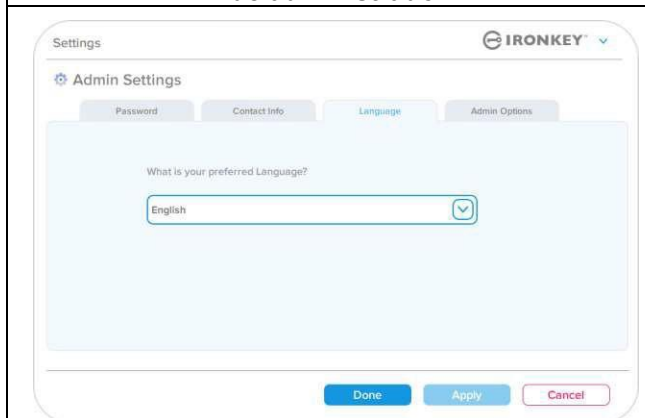


Figura 8.3 – Opciones de idioma

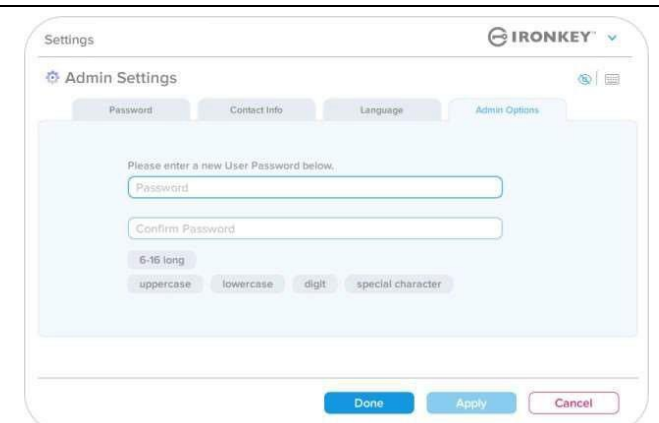


Figura 8.4 – Opciones de Admin

Configuración del LP50G2

Configuraciones de usuario: Administrador habilitado

El inicio de sesión del Usuario limita el acceso a las siguientes configuraciones:

Contraseña:

Le permite cambiar su contraseña de usuario y/o pista. (Figura 8.5)

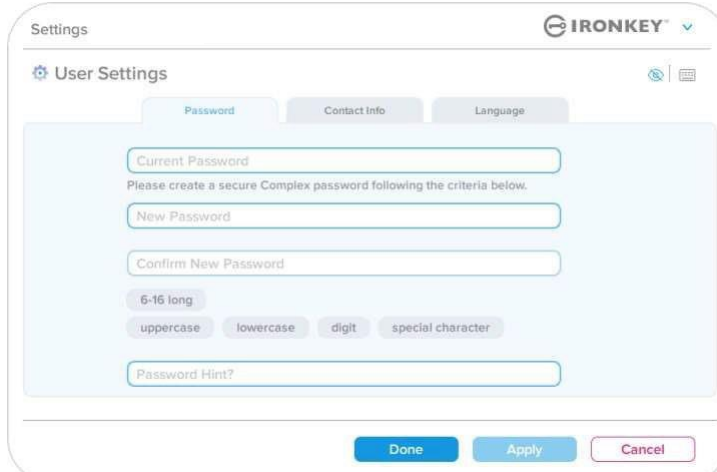


Figura 8.5 – Opciones de contraseña (Administrador habilitado: Inicio de sesión de Usuario)

Información de contacto:

Le permite agregar/visualizar/ cambiar su información de contacto. (Figura 8.6)

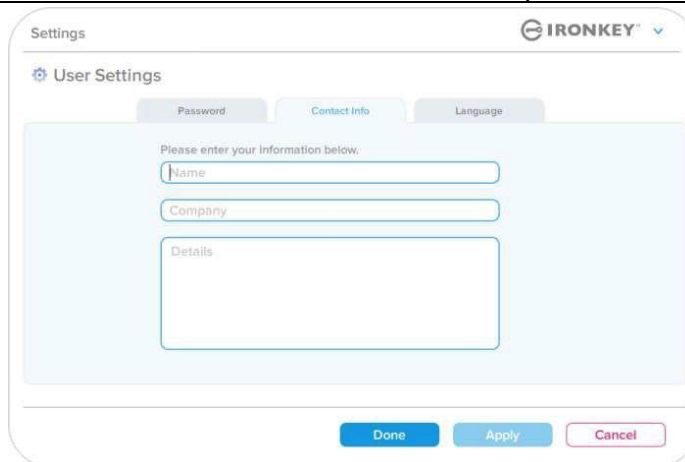


Figura 8.6– Información de contacto (Admin habilitado: Inicio de sesión de Usuario)

Idioma:

Le permite cambiar su selección de idioma actual. (Figura 8.7)

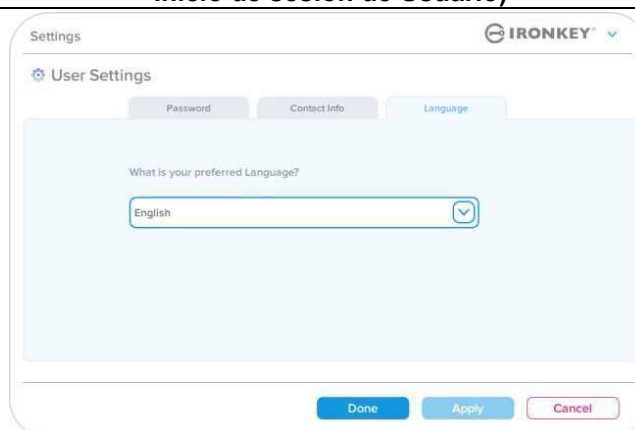


Figura 8.7 – Opciones Idioma (Administrador habilitado: Inicio de sesión de Usuario)

Nota: No se puede acceder a las opciones de administración cuando se inicia sesión con la contraseña de Usuario.

Configuración del LP50G2

Configuraciones de usuario: Administrador no habilitado

Como se mencionó anteriormente en la página 12, inicializar el LP50G2 sin habilitar las contraseñas de 'Administrador y Usuario' ajustará la unidad en una **configuración de Contraseña Única, Usuario Único**. Esta configuración no tiene acceso a ninguna opción o función de Administrador. Esta configuración tendrá acceso a los siguientes ajustes LP50G2.

Contraseña

Le permite cambiar su contraseña de usuario y/o pista. (Figura 8.8)

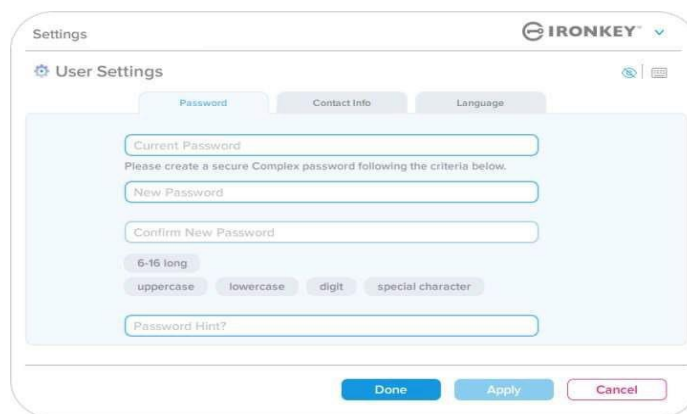


Figura 8.8– Opciones de contraseña (modo de Solo usuario)

Información de contacto:

Le permite agregar/visualizar/ cambiar su información de contacto. (Figura 8.9)

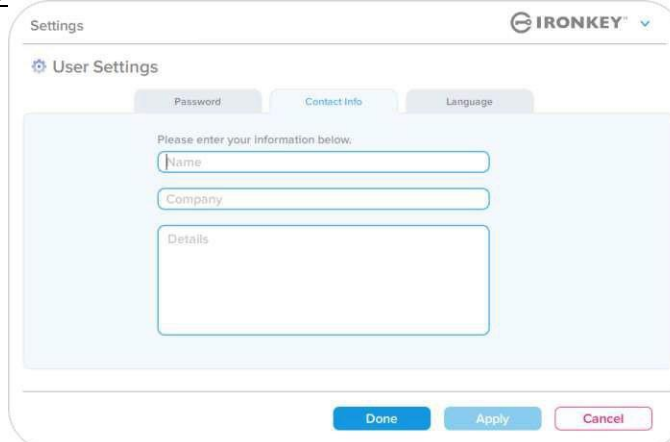


Figura 8.9 – Información de Contacto (modo de Solo usuario)

Idioma:

Le permite cambiar su selección de idioma actual. (Figura 8.10)

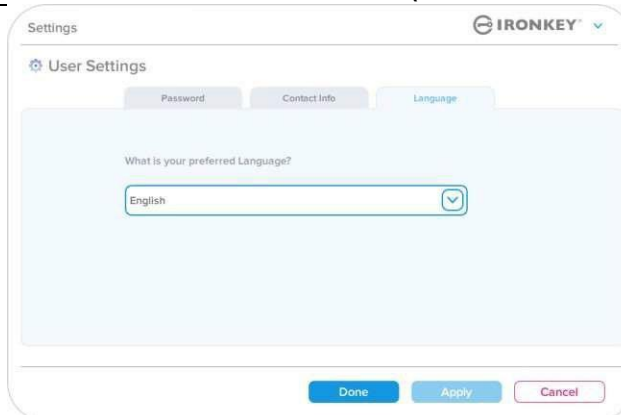


Figura 8.10– Configuración del idioma (modo de Solo usuario)

Configuración del LP50G2

Cambiar y guardar configuraciones

- Siempre que se cambie la configuración en la configuración de LP50G2 (por ejemplo, información de contacto, idioma, cambios de contraseña, opciones de administrador, etc.), la unidad le pedirá que ingrese su contraseña para aceptar y aplicar los cambios. (Ver la Figura 8.11)

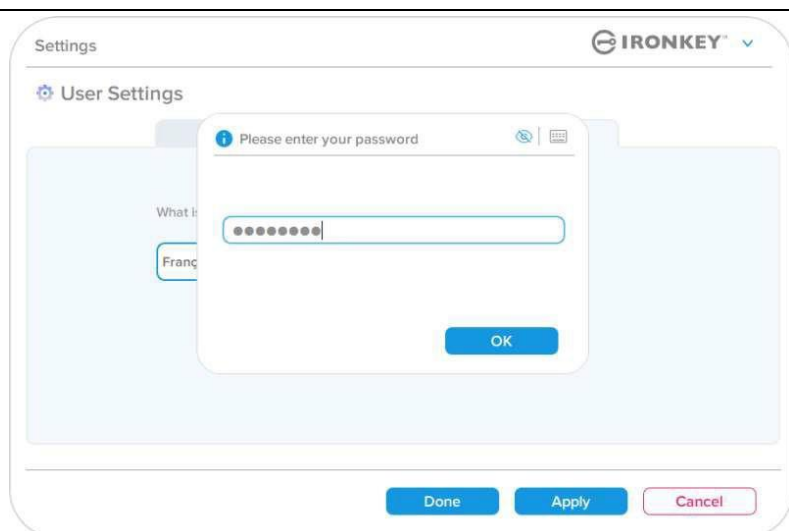


Figura 8.11 – Pantalla de solicitud de contraseña para guardar cambios de configuración del LP50G2

Nota: Si se encuentra en la pantalla de solicitud de contraseña anterior y desea cancelar o modificar sus cambios, puede hacerlo simplemente asegurándose de que el campo de contraseña esté en blanco y haga clic en "Aceptar". Esto cerrará el cuadro "Introduzca su contraseña" y volverá al menú de configuración del LP50G2.

Funciones de administrador

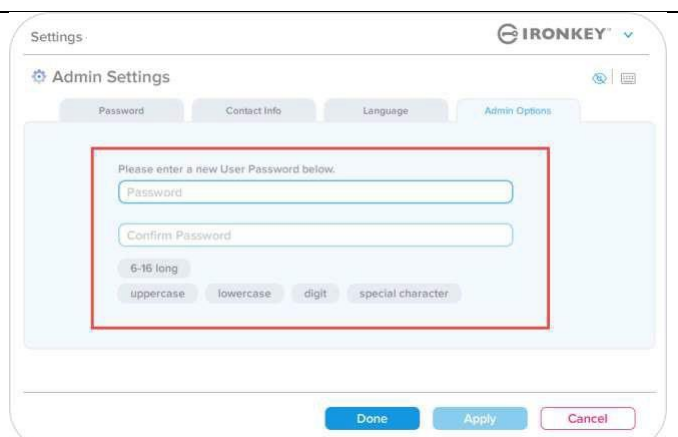
Opción disponible para restablecer la contraseña de Usuario

Una de las características útiles de la configuración de Admin le permite restablecer de forma segura la contraseña de Usuario, en caso de que alguna vez se olvide. A continuación, se muestra la función de restablecimiento de contraseña de Usuario que puede ser útil para restablecer la contraseña de Usuario:

Restablecer contraseña de Usuario:

Cambie manualmente la Contraseña de usuario en el menú 'opciones de Administrador', el cual es un cambio instantáneo y entrará en vigor en el próximo Inicio de sesión. (Figura 9.1)

Nota: Los criterios de requisito de contraseña serán los criterios originales que se establecieron durante el proceso de inicialización (opciones Compleja o Frase de contraseña).



The screenshot shows the 'Settings' screen of the IronKey Admin interface. The 'Admin Settings' section is active, with tabs for 'Password', 'Contact Info', 'Language', and 'Admin Options'. The 'Admin Options' tab is selected, and a red box highlights the 'Please enter a new User Password below:' section. This section contains two input fields: 'Password' and 'Confirm Password'. Below these fields are four criteria buttons: '6-16 long', 'uppercase', 'lowercase', 'digit', and 'special character'. At the bottom of the form are three buttons: 'Done', 'Apply', and 'Cancel'.

Figura 9.1 – Opciones de Admin/Restablecimiento de contraseña de Usuario

Ayuda y resolución de problemas

Bloqueo del dispositivo

El LP50G2 incluye una función de seguridad que evita el acceso no autorizado a la partición de datos una vez que se ha realizado un número máximo de intentos de inicio de sesión fallidos **consecutivos** (*MaxNoA* para abreviar). La configuración predeterminada "lista para usar" tiene un valor preconfigurado de 10 (número de intentos) por cada método de inicio de sesión (Administrador/Usuario).

El contador de 'bloqueo' rastrea cada inicio de sesión fallido y **se restablece de dos** maneras:

1. Un inicio de sesión exitoso antes de llegar a MaxNoA
2. Llegar a MaxNoA y realizar un bloqueo de dispositivo o un formato de dispositivo dependiendo de cómo esté configurada la unidad.

- Si se introduce una contraseña incorrecta, aparecerá un mensaje de error en rojo justo encima del campo Entrada de contraseña, que indica un error de inicio de sesión. (Figura 10.1)

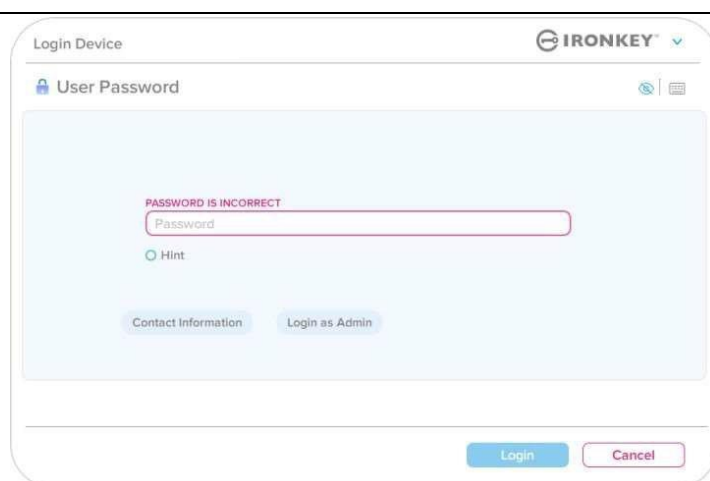


Figura 10.1 – Mensaje de contraseña incorrecta

- Cuando se realiza un 7º intento fallido, verá un mensaje de error adicional que indica que le quedan 3 intentos antes de llegar a MaxNoA (que está establecido en 10 de forma predeterminada). (Figura 10.2)

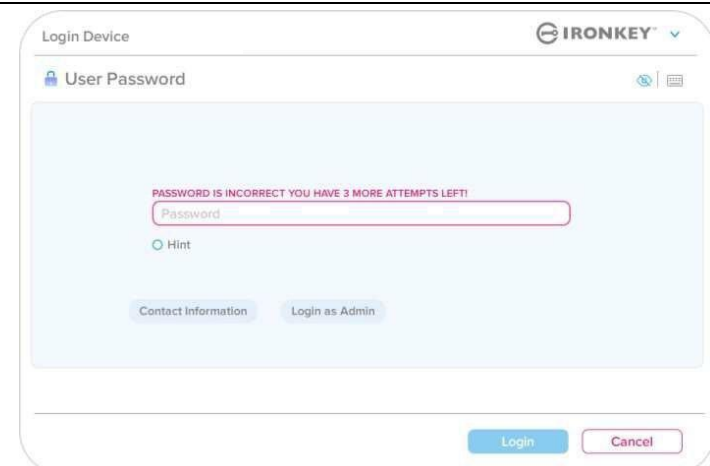


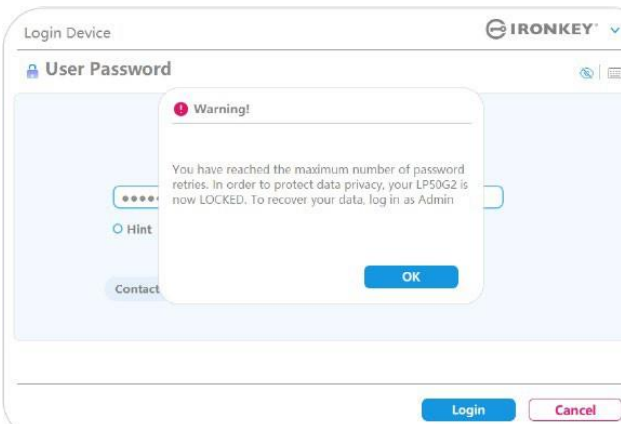
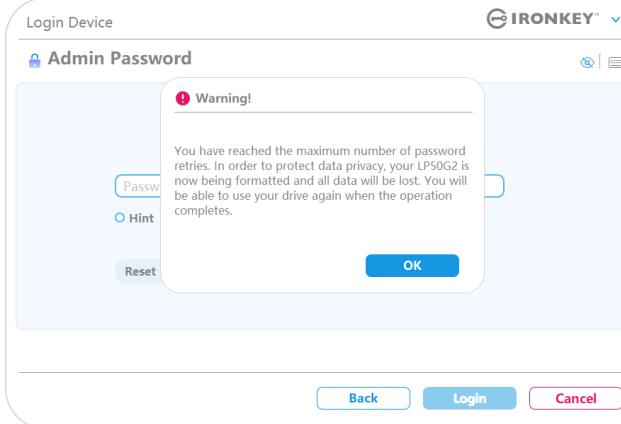
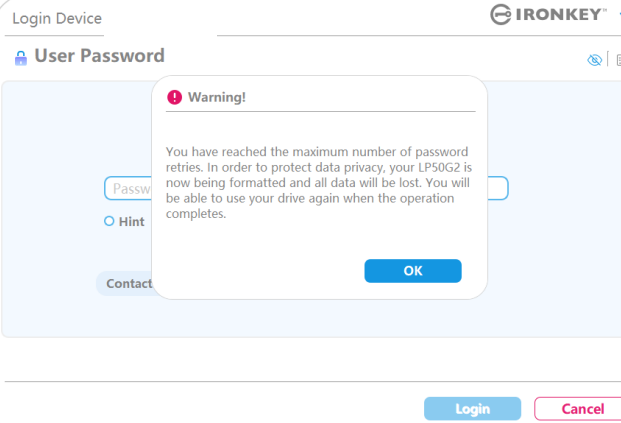
Figura 10.2 – 7º intento de contraseña incorrecto

Ayuda y resolución de problemas

Bloqueo del dispositivo

Importante: Después de un 10º y último intento de inicio de sesión fallido, dependiendo de cómo se configuró el dispositivo y el método de inicio de sesión utilizado (Admin/ Usuario), el dispositivo se bloqueará, lo que requerirá que inicie sesión con un método alternativo (si corresponde), o un restablecimiento del dispositivo que **formateará los datos y todos los datos de la unidad se perderán para siempre**. Los comportamientos también se mencionan en la página 17 de esta Guía de usuario.

Las Figuras 10.3- 10.6 a continuación demuestran el comportamiento visual para el 10º y último inicio de sesión fallido por cada método de contraseña de inicio de sesión:

Contraseña de usuario: (Administrador/usuario habilitado)  BLOQUEO DEL DISPOSITIVO Figura 10.3	Contraseña de administrador (Administrador/ Usuario habilitado)  FORMATEO DEL DISPOSITIVO Figura 10.4
Estas medidas de seguridad limitan a alguien (que no tiene su contraseña) a intentar innumerables intentos de inicio de sesión y obtener acceso a sus datos confidenciales (también conocido como ataque de fuerza bruta). Si usted es el propietario del LP50G2 y ha olvidado su contraseña, se aplicarán las mismas medidas de seguridad, incluido un formato de dispositivo. * Para obtener más información sobre esta función, consulte 'Restablecer dispositivo' en la página 27.	Contraseña de Usuario (Administrador NO habilitado)  FORMATEO DEL DISPOSITIVO Figura 10.5

***Nota:** Un formato de dispositivo borrará TODA la información almacenada en la partición de datos segura del LP50G2.

Ayuda y resolución de problemas

Restablecer dispositivo

Si olvida su contraseña o necesita restablecer su dispositivo, puede hacer clic en el botón '*Restablecer dispositivo*' que aparece en uno de dos lugares, dependiendo de cómo esté configurada la unidad (ya sea en el menú Contraseña de inicio de sesión del administrador si está habilitado el modo Administrador/Usuario, o en el menú 'Contraseña de Usuario' si no está habilitado el modo Administrador/Usuario) cuando se ejecuta el iniciador LP50G2. (ver Figura 10.7 y 10.8)

- Esta opción le permitirá crear una nueva contraseña, pero para proteger la privacidad de sus datos, se formateará el LP50G2. Esto significa que todos sus datos se borrarán en el proceso.*

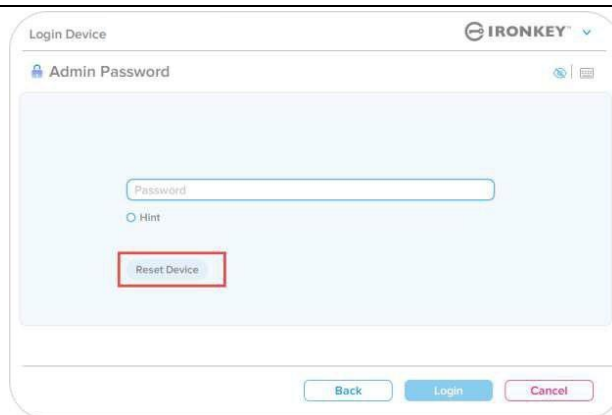


Figura 10.6 – Contraseña de Administrador Botón de Restablecer dispositivo

- Nota:** Cuando haga clic en '*Restablecer dispositivo*', aparecerá un cuadro de mensaje y preguntará si desea introducir una nueva contraseña antes de ejecutar el formateo. En este punto, puede hacer 1) clic en '*Aceptar*' para confirmar o 2) hacer clic en '*Cancelar*' para volver a la ventana de inicio de sesión. (Ver la Figura 10.8)

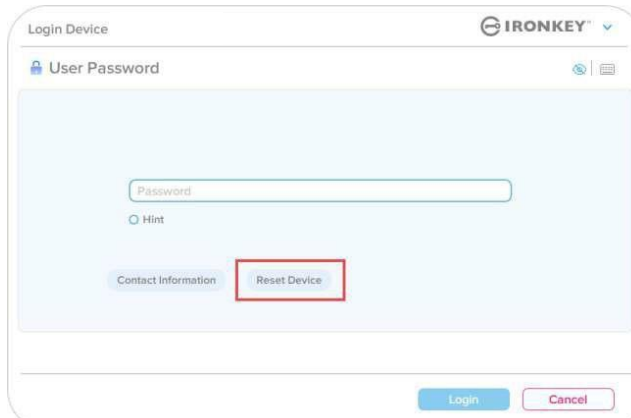


Figura 10.7 – Contraseña de Usuario (Administrador/ Usuario no habilitado) Restablecer dispositivo

- Si opta por continuar, se le pedirá que acceda a la pantalla Inicializar, donde puede habilitar los modos de 'Administrador y Usuario' e ingresar su nueva contraseña en función de la Opción de contraseña que elija (Compleja o Frase de contraseña). La pista no es un campo obligatorio, pero puede ser útil para proporcionar una pista sobre la contraseña en caso de que se olvide.

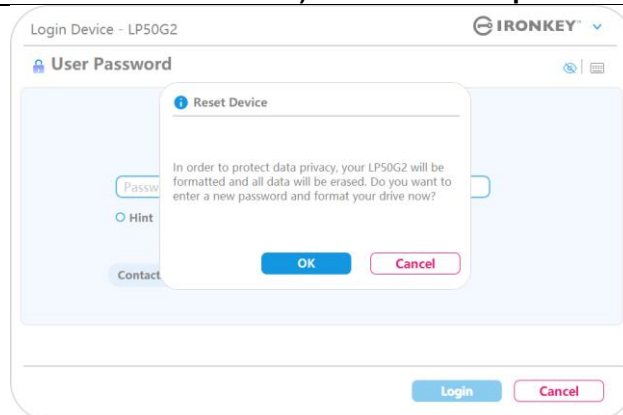


Figura 10.8 – Confirmación de reinicio del dispositivo

Conflicto de letras de unidad: Sistemas operativos Window

- Como se menciona en la sección "*Requisitos del sistema*" de este manual (en la página 4), el LP50G2 requiere dos letras de unidad consecutivas DESPUÉS del último disco físico que aparece antes de la "brecha" en las asignaciones de letras de unidad (consulte la Figura 10.9). Esto NO se refiere a los recursos compartidos de red porque son específicos de los perfiles de usuario y no del perfil de hardware del sistema en sí, por lo que parecen estar disponibles para el sistema operativo.
- Lo que esto significa es que Windows puede asignar al LP50G2 una letra de unidad que ya está en uso por un recurso compartido de red o una ruta de la Convención de nomenclatura universal o Universal Naming Convention (UNC), lo que causa un conflicto de letras de unidad. Si eso ocurre, pida asistencia al administrador de su sistema o al departamento de soporte técnico respecto al cambio de las asignaciones de letras del dispositivo en la utilidad "Administración de discos" de Windows (se requieren privilegios administrativos)

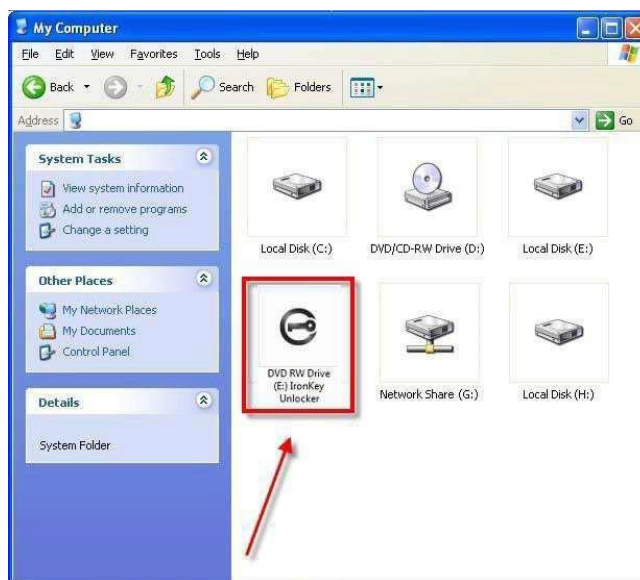


Figura 10.9 – Ejemplo de letra de unidad

En este ejemplo (Figura 10.9), el LP50G2 utiliza la unidad F:, que es la primera letra de unidad disponible después de la unidad E: (el último disco físico antes del espacio entre letras de unidad). Debido a que la letra G: es un recurso compartido de red y no forma parte del perfil de hardware, el LP50G2 puede intentar usarla como su segunda letra de unidad, causando un conflicto.

Si no hay recursos compartidos de red en su sistema y el LP50G2 sigue sin cargarse, es posible que un lector de tarjetas, un disco extraíble u otro dispositivo instalado previamente se esté aferrando a una asignación de letra de unidad y siga causando un conflicto.

Tenga en cuenta que la administración de letras de unidad o Drive Letter Management (DLM), ha mejorado significativamente en Windows 11, por lo que es posible que no se encuentre con este problema, pero si no puede resolver el conflicto, póngase en contacto con el Departamento de soporte técnico de Kingston o visite [Kingston.com/support](https://www.kingston.com/support) para obtener más ayuda.

IRONKEY™ Locker+ 50 G2 (LP50G2)
SICHERER USB-STICK 3.2 Gen 1

Anleitung



Inhalt

Einführung	3
Locker+ 50 G2 Merkmale	4
Über dieses Benutzerhandbuch	4
Systemvoraussetzungen	4
Empfehlungen	5
Verwenden des korrekten Dateisystems	5
Hinweise zur Verwendung	5
Bewährte Praktiken für die Passwort-Einrichtung	6
Einrichten des Geräts	7
Gerätezugriff (Windows-Umgebung)	7
Gerätezugriff (macOS-Umgebung)	7
Geräteinitialisierung (Windows- und macOS-Umgebung)	8
Passwort-Auswahl	9
Virtuelle Tastatur	11
Umschalten der Passwortsichtbarkeit	12
Admin- und Benutzer-Passwörter	13
Kontaktinformationen	15
Gerätenutzung (Windows- und macOS-Umgebung)	16
Anmeldung für Admin und Benutzer (Admin aktiviert)	16
Anmeldung für Nur-Benutzer-Modus (Admin nicht aktiviert)	16
Schutz vor Brute-Force-Angriffen	17
Zugriff auf die sicheren Dateien	17
Geräteoptionen	18
LP50G2 Einstellungen	20
Admin-Einstellungen	20
Benutzer-Einstellungen: Admin aktiviert	21
Benutzer-Einstellungen: Admin nicht aktiviert	22
Ändern und Speichern von LP50G2 Einstellungen	23
Admin-Funktionen	24
Zurücksetzen des Benutzer-Passworts	24
Hilfe und Fehlerbehebung	25
LP50G2 Sperrung	25
LP50G2 Gerät zurücksetzen	27
Laufwerksbuchstaben-Konflikt: (Windows)	28



Abb. 1: IronKey LP50G2

Einführung

Die Kingston IronKey™ Locker+ 50 G2 USB-Sticks bieten mit der FIPS-197-zertifizierten AES-256-Bit-Hardwareverschlüsselung im XTS-Modus Sicherheit auf Unternehmensniveau, einschließlich Schutzmaßnahmen gegen BadUSB- und Brute-Force-Passwort-Angriffe. Der LP50G2 ist auch TAA-konform.

Der LP50G2 unterstützt jetzt die Option für mehrere Passwörter (Admin und Benutzer) mit den Modi Komplex oder Passphrase. Im Komplex-Modus sind Passwörter mit 6–16 Zeichen möglich, wobei 3 von 4 Zeichensätzen verwendet werden. Der neue Passphrase-Modus unterstützt numerische PINs, Sätze, Wortlisten oder sogar Liedtexte mit 10 bis 64 Zeichen. Der Administrator kann ein Benutzerpasswort aktivieren oder das Benutzerpasswort zurücksetzen, um den Zugriff auf die Daten wiederherzustellen. Zur Erleichterung der Passwordeingabe kann das Symbol „Auge“ markiert werden, damit das eingegebene Passwort angezeigt und Tippfehler vermieden werden, die zu fehlgeschlagenen Anmeldeversuchen führen. Der Schutz vor Brute-Force-Angriffen sperrt Benutzer, wenn 10 ungültige Passwörter hintereinander eingegeben werden, und löscht den USB-Stick unwiederbringlich, wenn das Admin-Passwort 10 Mal hintereinander falsch eingegeben wird. Darüber hinaus schützt eine integrierte virtuelle Tastatur Passwörter vor Keyloggern oder Screenloggern.

Der Locker+ 50 G2 ist mit einem kleinen Metallgehäuse und einer integrierten Schlüsselschleife ausgestattet, damit Sie Ihre Daten überallhin mitnehmen können.

Der LP50G2 wird durch eine 5-Jahres-Garantie mit kostenlosem technischen Kingston Support unterstützt.

IronKey Locker+ 50 G2 Merkmale

- FIPS 197-zertifiziert
- XTS-AES-Hardwareverschlüsselung (die Verschlüsselung kann niemals deaktiviert werden)
- Schutz vor Brute-Force- und BadUSB-Angriffen
- Mehrfach-Passwort-Optionen
- Modi „Komplexes Passwort“ oder „Passphrase“
- Schaltfläche „Auge“ für die Anzeige eingegebener Passwörter, um fehlgeschlagene Anmeldeversuche zu reduzieren
- Virtuelle Tastatur zum Schutz vor Key- und Screenloggern
- Windows- oder macOS-kompatibel (Details siehe Datenblatt)

Über dieses Benutzerhandbuch (02122026)

Dieses Benutzerhandbuch bezieht sich auf den IronKey Locker+ 50 G2 (LP50G2).

Systemanforderungen

PC-Plattform • Intel und AMD. • 15MB freier Speicherplatz • Freier USB 2.0 – 3.2-Anschluss • Zwei freie, aufeinanderfolgende Laufwerksbuchstaben nach dem letzten physischen Speicher* *Hinweis: Siehe „Laufwerksbuchstabenkonflikt“ auf Seite 28.	Unterstützte PC-Betriebssysteme • Windows 11
Mac-Plattform • Intel und Apple SOC • 15MB freier Festplattenspeicher • USB 2.0 – 3.2 Anschluss	Unterstützte Mac-Betriebssysteme • macOS 13.x – 26.x

Empfehlungen

Um eine ausreichende Stromversorgung des LP50G2 sicherzustellen, schließen Sie ihn direkt in einen USB-Anschluss Ihres Notebooks oder PCs an, siehe *Abb. 1.1*. Schließen Sie den LP50G2 nach Möglichkeit nicht an Peripheriegeräte mit einem USB-Anschluss an, wie beispielsweise eine Tastatur oder einen USB-Hub, siehe *Abb. 1.2*.



Abb. 1.1 – Empfohlener Anschluss



Abb. 1.2 – Nicht empfehlenswert

Verwenden des korrekten Dateisystems

Der IronKey LP50G2 ist mit dem FAT32-Dateisystem vorformatiert. Es funktioniert mit Windows- und macOS-Systemen. Es gibt jedoch einige andere Optionen, die zum manuellen Formatieren des Sticks verwendet werden können, z. B. NTFS für Windows und exFAT. Die Datenpartition lässt sich bei Bedarf neu formatieren, aber die Daten gehen bei der Neuformatierung des Laufwerks unwiederbringlich verloren.

Hinweise zur Verwendung

Für den Schutz Ihrer Daten empfiehlt Kingston Folgendes:

- Viren-Scan auf Ihrem Computer durchführen, bevor der LP50G2 auf einem Zielsystem eingerichtet und verwendet wird.
- Wenn der USB-Stick in einem öffentlichen oder unbekannten System verwendet wird, sollte der Schreibschutz-Modus auf dem Gerät aktiviert sein, damit der Stick vor Malware geschützt ist.
- Den Stick sperren, wenn er nicht benutzt wird.
- Den USB-Stick trennen, bevor er herausgezogen wird.
- Den Stick niemals herausziehen, wenn die LED leuchtet. Denn dadurch kann der USB-Stick beschädigt und eine Neuformatierung erforderlich werden, wodurch Ihre Daten unwiederbringlich gelöscht werden.
- Das Passwort des USB-Sticks niemals an Dritte weitergeben.

Nach den neuesten Updates und Informationen suchen.

Unter kingston.com/support finden Sie die neuesten Laufwerks-Updates, FAQs, Dokumentationen und weitere Informationen.

HINWEIS: Es sollten nur die neuesten Stick-Updates (sofern vorhanden) auf dem USB-Stick angewendet werden. Ein Downgrade des Sticks auf eine ältere Software-Version wird nicht unterstützt und kann möglicherweise zum Verlust gespeicherter Daten führen oder andere Laufwerksfunktionen beeinträchtigen. Bei Fragen oder Problemen wenden Sie sich bitte an den technischen Support von Kingston.

Bewährte Praktiken für die Passwort-Einrichtung

Der LP50G2 bietet starke Sicherheitsvorkehrungen. Dazu gehört ein Schutz gegen Brute-Force-Angriffe, der Angreifer am Erraten von Passwörtern hindert, indem er alle Passwort-Eingabeversuche auf 10 Wiederholungen begrenzt. Wenn das Limit des USB-Sticks erreicht ist, löscht der LP50G2 automatisch die verschlüsselten Daten unwiederbringlich und formatiert sich selbst zurück auf den Werkszustand.

Mehrfach-Passwort

Der LP50G2 unterstützt Mehrfach-Passwörter als eine wichtige Funktion zum Schutz vor Datenverlust, wenn ein oder mehrere Passwörter vergessen wurden. Wenn alle Passwortoptionen aktiviert sind, kann der LP50G2 zwei verschiedene Passwörter unterstützen, die Sie zur Wiederherstellung von Daten verwenden können – Admin- und Benutzer-Passwortrollen

Der LP50G2 bietet Ihnen die Auswahl von zwei Hauptpasswörtern – ein Administrator-Passwort (als Admin-Passwort bezeichnet) und ein Benutzer-Passwort. Der Administrator kann jederzeit auf das Laufwerk zugreifen und Optionen für den Benutzer einrichten – der Administrator ist damit so etwas wie ein Superuser.

Der Benutzer kann ebenfalls auf den USB-Stick zugreifen, hat aber im Vergleich zum Administrator nur eingeschränkte Rechte. Wird eines der beiden Passwörter vergessen, kann das andere Passwort verwendet werden, um auf die Daten zuzugreifen und sie abzurufen. Der Stick kann dann wieder so eingerichtet werden, dass er über zwei Passwörter verfügt. Es ist wichtig, BEIDE Passwörter einzurichten und das Admin-Passwort an einem sicheren Ort aufzubewahren, während Sie das Benutzer-Passwort verwenden.

Wenn alle Passwörter vergessen werden oder verloren gehen, gibt es keine weitere Möglichkeit, auf die Daten zuzugreifen. Kingston ist dann auch nicht in der Lage, die Daten abzurufen, da das Sicherheitssystem keine Hintertüren hat. Kingston empfiehlt, die Daten auch auf anderen Medien zu speichern. Der LP50G2 kann zurückgesetzt und wieder verwendet werden, aber die vorherigen Daten werden für immer gelöscht.

Passwort-Modi

Der LP50G2 unterstützt außerdem zwei verschiedene Passwort-Modi:

Komplex

Ein komplexes Passwort muss mindestens 6–16 Zeichen lang sein und mindestens 3 der folgenden Zeichen enthalten:

- Großbuchstaben
- Kleinbuchstaben
- Zahlen
- Sonderzeichen

Passphrase

Der LP50G2 unterstützt Passphrasen mit 10 bis 64 Zeichen. Eine Passphrase folgt keinen zusätzlichen Regeln, kann aber bei richtiger Verwendung ein sehr hohes Maß an Passwortschutz bieten.

Eine Passphrase ist im Grunde eine beliebige Kombination von Zeichen, einschließlich Zeichen aus anderen Sprachen. Wie beim LP50G2-Stick kann die Sprache des Passworts mit der für den USB-Stick gewählten Sprache übereinstimmen. So können mehrere Wörter, eine Phrase, einen Liedtext, eine Gedichtzeile usw. ausgewählt werden. Gute Passphrasen gehören zu den am schwersten zu erratenden Passworttypen für einen Angreifer, sind aber für die Benutzer leichter zu merken.

Einrichten des Geräts

Um sicherzustellen, dass die Stromversorgung des verschlüsselten IronKey USB-Sticks ausreichend ist, schließen Sie ihn direkt an einem USB 2.0/3.0-Anschluss an einem Notebook oder PC an. Vermeiden Sie den Anschluss des USB-Sticks an Peripheriegeräte mit einem USB-Anschluss, wie z. B. eine Tastatur oder einen USB-Hub. Die Ersteinrichtung des Geräts muss unter einem unterstützten Windows- oder macOS-basierten Betriebssystem erfolgen.

Gerätezugriff (Windows-Umgebung)

Stecken Sie den verschlüsselten IronKey USB-Stick in einen freien USB-Anschluss am Notebook oder Desktop und warten Sie, bis Windows ihn erkennt.

- Unter Windows wird eine Nachricht über die Gerätetreiberinstallation angezeigt. (Abb. 3.1)



Abb. 3.1 – Gerätetreiber-Meldung

- Sobald die Erkennung der neuen Hardware abgeschlossen ist, wählen Sie die Option **IronKey.exe** innerhalb der Unlocker-Partition, die über den Datei-Explorer zu finden ist. (Abb. 3.2)
- Bitte beachten Sie, dass der Partitionsbuchstabe je nach dem nächsten freien Laufwerksbuchstaben variiert. Der Laufwerksbuchstabe kann sich ändern, je nachdem, welche Geräte angeschlossen sind. In der Abbildung auf der rechten Seite ist der Laufwerksbuchstabe „(E:)“.



Abb. 3.2 – Fenster Datei-Explorer/IronKey.exe

Gerätezugriff (macOS-Umgebung)

Schließen Sie den LP50G2 an einem freien USB-Anschluss Ihres Notebooks oder Desktops an und warten Sie, bis das Mac-Betriebssystem ihn erkennt. Wenn dies der Fall ist, wird das Laufwerk „IRONKEY“ auf dem Desktop angezeigt. (Abb. 3.3)

- Doppelklicken Sie auf das CD-ROM-Symbol des IronKey.
- Dann auf das Symbol der IronKey.app doppelklicken, das in dem in der Abb. 3.3 dargestellten Fenster angezeigt wird. Dadurch wird der Installationsprozess gestartet.

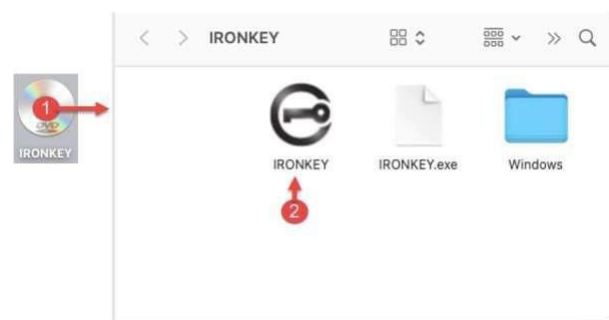


Abb. 3.3 – IRONKEY Laufwerk

Geräteinitialisierung (Windows- und macOS-Umgebung)

Sprache und EULA

Wählen Sie die von Ihnen gewünschte Sprache aus dem Dropdown-Menü aus und klicken Sie auf **Weiter (Next)**.
(Siehe Abb. 4.1)

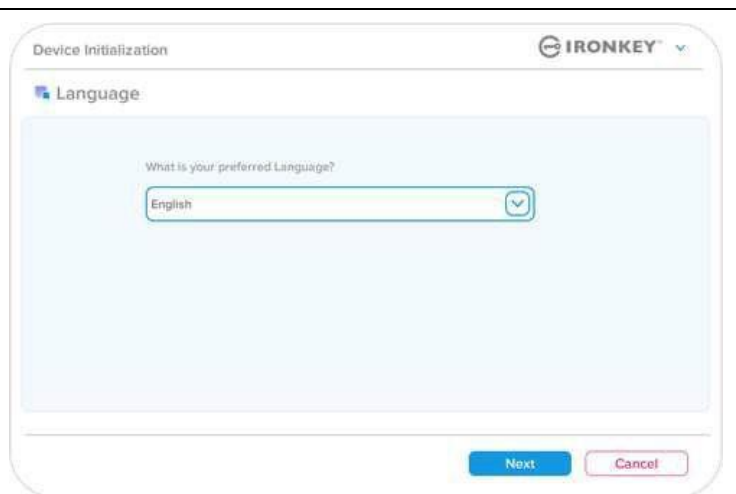


Abb. 4.1 – Sprachauswahl

Lesen Sie die Lizenzvereinbarung und klicken Sie auf **Weiter (Next)**.

Hinweis: Die Schaltfläche **Weiter (Next)** wird erst aktiviert, nachdem Sie die Lizenzvereinbarung akzeptiert haben.
(Abb. 4.2)

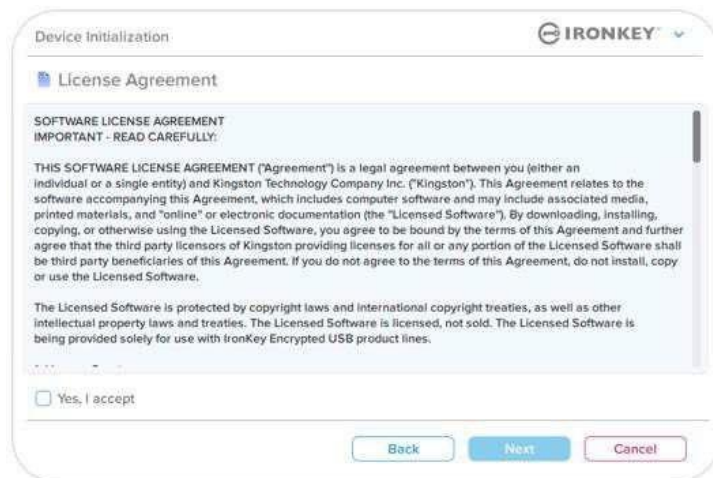


Abb. 4.2 – Lizenzvereinbarung

Geräteinitialisierung

Passwort-Auswahl

Auf dem Bildschirm der Passwortabfrage können Sie ein Passwort erstellen, um die Daten auf dem LP50G2 zu schützen, indem Sie entweder den Passwortmodus „Komplex (Complex)“ oder „Passphrase“ verwenden (Abb. 4.3 – 4.4). Darüber hinaus können Sie auf diesem Bildschirm auch die Mehrfach-Passwort-Admin/Benutzer-Optionen aktivieren. Bevor Sie mit der Auswahl des Passworts fortfahren, lesen Sie bitte den Abschnitt „Aktivieren von Admin-/Benutzer-Passwörtern“ unten, um diese Funktionen besser zu verstehen.

Hinweis: Sobald der Modus „Komplex“ oder „Passphrase“ ausgewählt wurde, kann der Modus nicht mehr geändert werden, es sei denn, der Stick wird zurückgesetzt. Erstellen Sie zu Beginn der Passwortauswahl Ihr Passwort im Feld „Passwort“ und geben Sie es dann erneut in das Feld „Passwort bestätigen“ ein. Sie können mit der Installationseinrichtung erst fortfahren, nachdem Sie ein Passwort nach folgenden Kriterien eingegeben haben:

Komplexes Passwort

- Muss mindestens 6 Zeichen lang sein (bis zu 16 Zeichen).
- Muss 3 (drei) der folgenden Kriterien enthalten:
 - Großbuchstabe
 - Kleinbuchstabe
 - Zahl
 - Sonderzeichen (!,\$,& usw.)

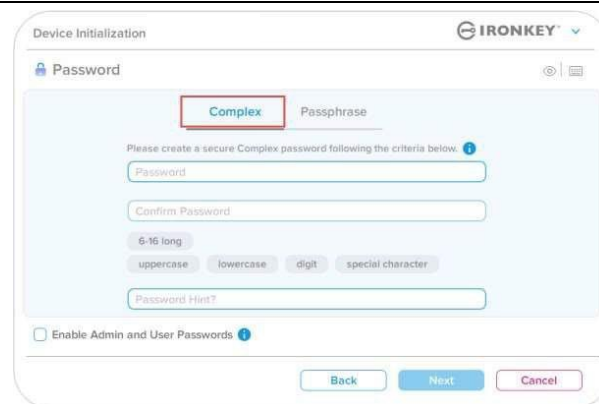


Abb. 4.3 – Komplexes Passwort

Passwort als Passphrase

- Muss enthalten:
 - Minimal 10 Zeichen
 - Maximal 64 Zeichen

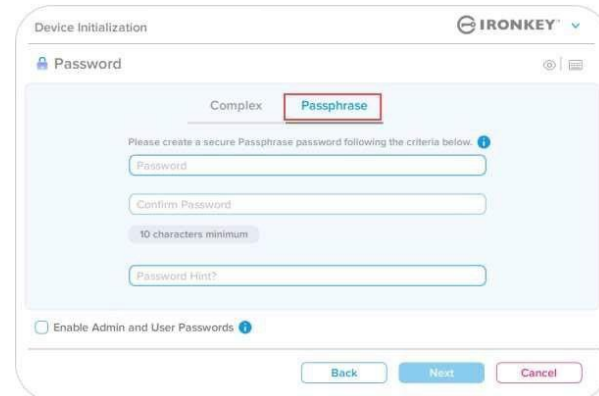


Abb. 4.4 – Passphrasen-Passwort

Passwort-Hinweis (optional)

Ein Passwort-Hinweis kann nützlich sein, um einen Hinweis auf das Passwort zu geben, falls das Passwort einmal vergessen werden sollte.

Hinweis: Der Hinweis und das Passwort dürfen NICHT identisch sein.

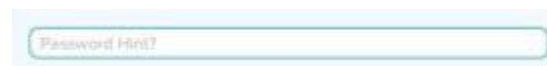


Abb. 4.5 – Passwort-Hinweisfeld

Geräteinitialisierung

Gültige und ungültige Passwörter

Bei **gültigen** Passwörtern werden die Felder für die Passwortkriterien **grün** markiert, wenn die Kriterien erfüllt sind. (Siehe Abb. 4.6a-b) Hinweis: Sobald mindestens drei Passwortkriterien erfüllt sind, wird das vierte Kriterium grau, um anzuzeigen, dass dieses Kriterium jetzt optional ist (Abb. 4.6b).

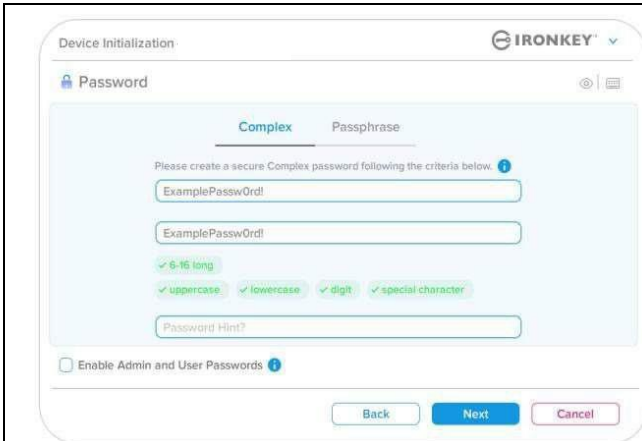


Abb. 4.6a – Bedingung für komplexes Passwort erfüllt

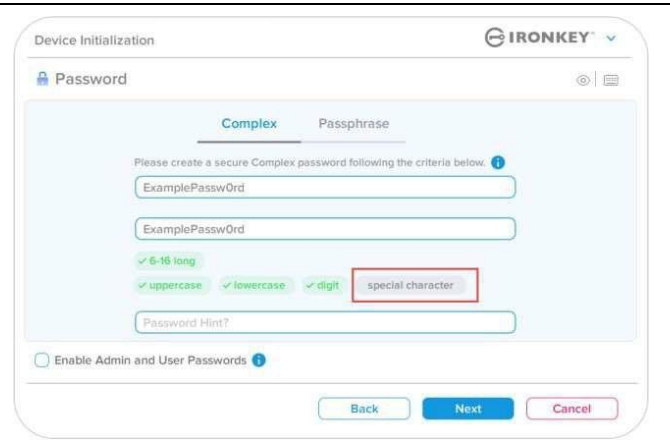


Abb. 4.6b – Bedingung für komplexes Passwort ist optional

Bei **ungültigen** Passwörtern werden die Felder für die Passwortkriterien **rot** markiert und die Schaltfläche **Weiter (Next)** ist deaktiviert, bis die Mindestanforderungen erfüllt sind.

Dies gilt sowohl für komplexe als auch für Passphrasen-Passwörter.

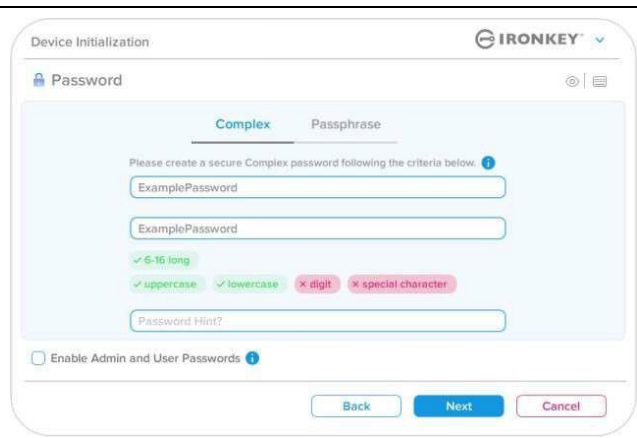


Abb. 4.7 – Passwort-Bedingungen nicht erfüllt

Geräteinitialisierung

Virtuelle Tastatur

Der LP50G2 verfügt über eine virtuelle Tastatur, die zum Schutz vor Keyloggern verwendet werden kann.

- Zur Verwendung der **virtuellen Tastatur** suchen Sie die Tastaturschaltfläche oben rechts auf dem Bildschirm **Geräteinitialisierung (Device Initialization)** und wählen Sie sie aus.

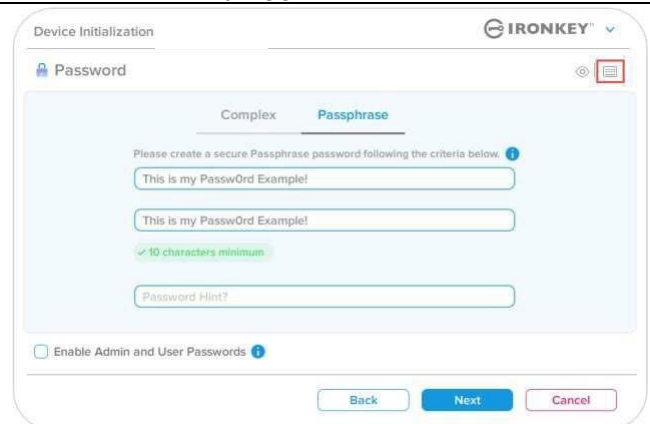


Abb. 4.8 – Aktivieren der virtuellen Tastatur

- Sobald die virtuelle Tastatur angezeigt wird, können Sie auch **Screenlogger-Schutz (Screenlogger Protection)** aktivieren. Wenn Sie diese Funktion verwenden, werden alle Tasten kurzzeitig leer angezeigt. Dies ist ein erwartetes Verhalten, da es verhindert, dass Screenlogger aufzeichnen, welche Schaltfläche Sie geklickt haben.
- Damit diese Funktion noch sicherer wird, können Sie die virtuelle Tastatur auch zufällig auswählen, indem Sie unten rechts auf der Tastatur **zufällig (randomize)** wählen. Durch Zufallseingabe wird die Tastatur in einer zufälligen Reihenfolge angeordnet.



Abb. 4.9 – Screenlogger-Schutz/Zufällig anordnen

Geräteinitialisierung

Umschalten der Passwortsichtbarkeit

Wenn Sie ein Passwort erstellen, wird die Passwortzeichenfolge standardmäßig während der Eingabe in das Feld eingeblendet. Wenn Sie die Passwort-Zeichenfolge während der Eingabe ausblenden möchten, können Sie dies tun, indem Sie die Markierung des Passwort-„Auges“ auf der oberen rechten Seite des Fensters für die Geräteinitialisierung entfernen.

Hinweis: Nach der Geräteinitialisierung ist das Passwortfeld standardmäßig auf „verbergen (hidden)“ eingestellt.

Klicken Sie auf das graue Symbol, um die Passwortzeichenfolge zu **verbergen**.

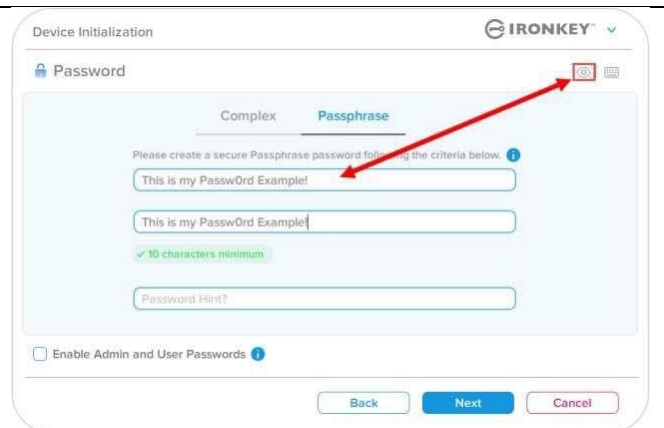



Abb. 4.10 – Auf Passwort „verbergen (hide)“ umschalten

Auf das blaue Symbol klicken, um das verborgene Passwort **anzuzeigen**.

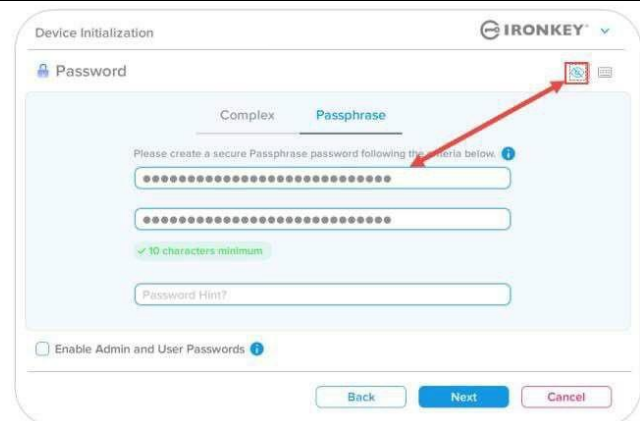



Abb. 4.11 – Auf Passwort „anzeigen (show)“ umschalten

Geräteinitialisierung

Admin- und Benutzer-Passwörter

Durch die Aktivierung von Admin- und Benutzer-Passwörtern steht die Mehrfach-Passwort-Funktion zur Verfügung, bei der der Admin beide Konten verwalten kann. Wenn Sie **„Admin- und Benutzer-Passwörter aktivieren (Enable Admin and User passwords)“** wählen, können Sie eine alternative Methode für den Laufwerkszugriff wählen, falls eines der Passwörter vergessen wurde.

Mit aktivierten Admin- und Benutzer-Passwörtern besteht ebenfalls Zugriff auf:

- Zurücksetzen des Benutzer-Passworts

Weitere Informationen zur Funktion „Benutzerpasswort zurücksetzen (User Password reset)“ finden Sie auf Seite 24 in diesem Benutzerhandbuch.

- Damit Sie **Admin- und Benutzer-Passwörter aktivieren (Enable Admin and User passwords)** können, klicken Sie auf das Kontrollkästchen neben **„Admin- und Benutzer-Passwörter aktivieren“** und wählen Sie dann **Weiter (Next)**, sobald Sie ein gültiges Passwort ausgewählt haben. (Abb. 4.12)
- Wenn diese Funktion **aktiviert (enabled)** ist, dann ist das gewählte Passwort auf diesem Bildschirm das **Admin-Passwort**. Klicken Sie auf **Weiter (Next)**, um zum Bildschirm **Benutzer-Passwort (User Password)** zu wechseln, wo ein Passwort für den Benutzer ausgewählt wird.

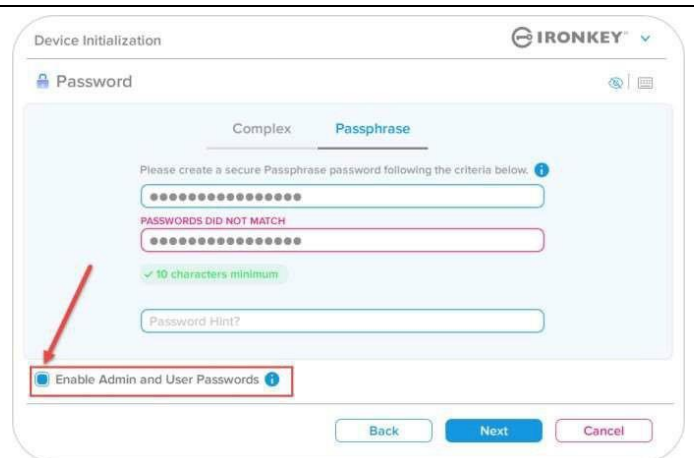


Abb. 4.12 – Aktivieren von Admin- und Benutzer-Passwörtern

Hinweis: Die Aktivierung von Admin- und Benutzer-Passwörtern ist optional.

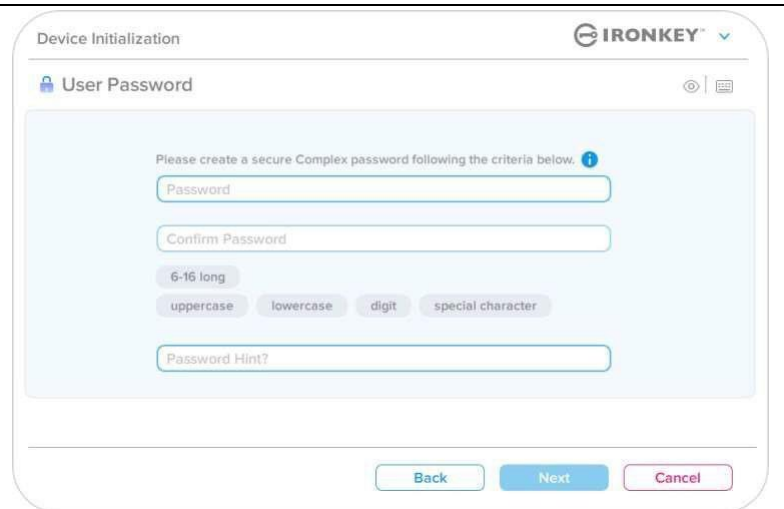
Wenn der USB-Stick so eingerichtet wird, dass diese Funktion NICHT aktiviert ist (Kontrollkästchen nicht markiert), wird der USB-Stick als **Einzel-Benutzer (Single User)**, **Einzel-Passwort (Single Password)**-Laufwerk **ohne jegliche Admin-Funktionen** konfiguriert. Diese Konfiguration wird in diesem Benutzerhandbuch als **Nur Benutzer-Modus (User-Only mode)** bezeichnet.

Lassen Sie, um mit der Einrichtung eines Einzelanwenders und eines einzigen Passworts fortzufahren, **Admin- und Benutzer-Passwörter aktivieren (Enable Admin and User Passwords)** unmarkiert und klicken Sie auf **Weiter (Next)**, nachdem Sie ein gültiges Passwort erstellt haben.

Geräteinitialisierung

Admin- und Benutzer-Passwörter

Wenn im vorherigen Bildschirm die Admin-Rolle **aktiviert** wurde, wird im folgenden Bildschirm das **Benutzer-Passwort** abgefragt (Abb. 4.13). Das Benutzer-Passwort hat im Vergleich zum Admin-Passwort nur eingeschränkte Möglichkeiten und wird nachfolgend näher erläutert. **Hinweis:** „Admin- und Benutzer-Passwörter (Admin and User Passwords)“ werden im Folgenden als „Admin-Rolle“ bezeichnet.



The screenshot shows the 'Device Initialization' screen with the 'User Password' section active. It prompts the user to 'Please create a secure Complex password following the criteria below.' The criteria listed are: 6-16 long, uppercase, lowercase, digit, and special character. There are input fields for 'Password', 'Confirm Password', and 'Password Hint?'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

**Abb. 4.13 – Benutzer-Passwort
(Admin und Benutzer aktiviert)**

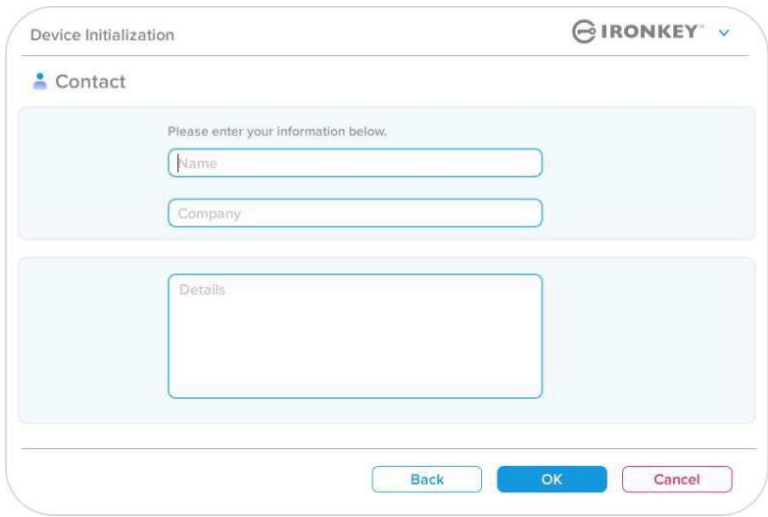
Hinweis: Die gewählte Passwortooption (Komplex oder Passphrase) wird für das Benutzer-Passwort und alle Passwort-Rücksetzungen übernommen, die nach der Einrichtung des Sticks erforderlich sind. Die gewählte Passwortooption kann nur nach einem vollständigen Geräte-Reset geändert werden.

Geräteinitialisierung

Kontaktinformationen

Geben Sie Ihre Kontaktinformationen in die vorgesehenen Textfelder ein. (Siehe Abb. 4.14)

Hinweis: Die Informationen, die Sie in diese Felder eingeben, dürfen NICHT die Passwortzeichenfolge enthalten, die Sie in Schritt 3 erstellt haben. Diese Felder sind jedoch optional und können auf Wunsch leer gelassen werden.

Im Feld „Name“ können bis zu 32 Zeichen eingegeben werden, das genaue Passwort darf jedoch nicht darin enthalten sein. Im Feld „Firma (Company)“ können bis zu 32 Zeichen eingegeben werden, das genaue Passwort darf jedoch nicht darin enthalten sein. Im Feld „Details“ können bis zu 156 Zeichen eingegeben werden, das genaue Passwort darf jedoch nicht darin enthalten sein.	 Abb. 4.14 – Kontaktinformationen
--	--

Hinweis: Wenn Sie auf „OK“ klicken, wird der Initialisierungsprozess abgeschlossen und die sichere Partition, auf der Ihre Daten sicher gespeichert werden können, wird entsperrt und eingebunden. Ziehen Sie den USB-Stick heraus und schließen Sie ihn wieder an, um die Änderungen anzuzeigen.

Gerätenutzung (Windows- und macOS-Umgebung)

Anmeldung für Admin und Benutzer (Admin aktiviert)

Wenn der Stick mit aktivierten Admin- und Benutzer-Passwörtern (Admin-Rolle) initialisiert wird, startet die Anwendung IronKey LP50G2 und fordert Sie zunächst zur Eingabe des Benutzer-Passworts auf. Hier können Sie sich mit dem Benutzer-Passwort anmelden, alle eingegebenen Kontaktinformationen einsehen oder sich als Administrator anmelden (Abb. 6.1). Wenn Sie auf die Schaltfläche „Als Administrator anmelden (Login as Admin)“ (siehe unten) klicken, wechselt die Anwendung zum Menü „Admin-Anmeldung (Login as Admin)“, wo Sie sich als Admin anmelden können, um auf die Admin-Einstellungen und -Funktionen zuzugreifen (Abb. 6.2).

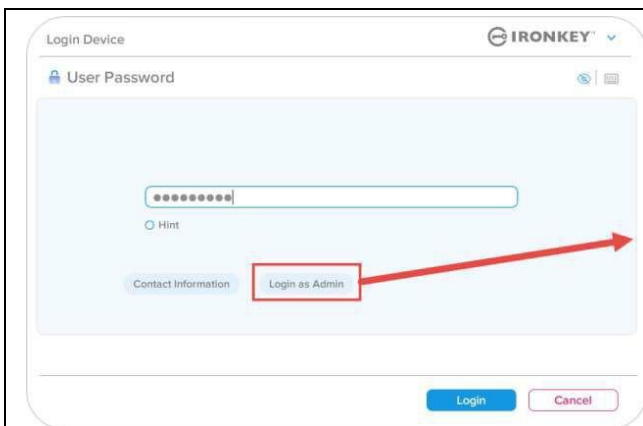


Abb. 6.1 – Anmeldung mit Benutzer-Passwort (Admin aktiviert)

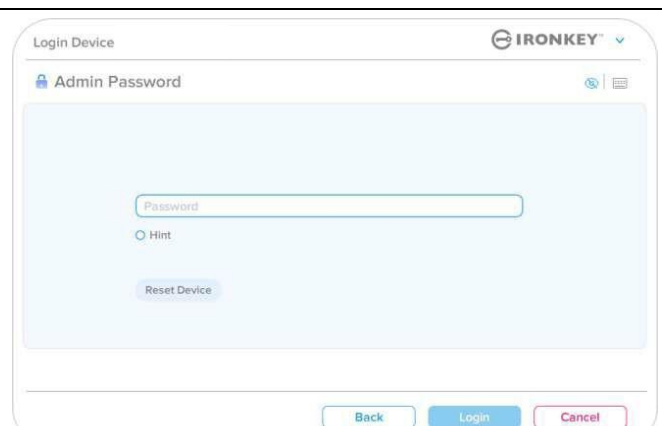


Abb. 6.2 – Anmeldung mit Admin-Passwort

Anmeldung für Nur-Benutzer-Modus (Admin nicht aktiviert)

Wie bereits auf **Seite 13** erwähnt, ist es zwar empfehlenswert, die Admin-Rollenfunktion zu nutzen, um den vollen Nutzen aus dem Gerät zu ziehen, aber der IronKey-Stick kann auch in einer Nur-Benutzer-Konfiguration (Einzelpasswort, Einzelbenutzer) initialisiert werden. Dies ist eine Option für diejenigen, die die Daten auf ihrem Stick mit einem einzigen Passwort sichern möchten. (Abb. 6.3)

Hinweis: Verwenden Sie zum Aktivieren von Admin- und Benutzer-Passwörtern die Schaltfläche **Gerät zurücksetzen (Reset Device)**, um den USB-Stick wieder in den Initialisierungszustand zu versetzen, in dem Admin- und Benutzer-Passwörter aktiviert werden können. **ALLE Daten auf dem Stick werden formatiert und gehen für immer verloren, wenn „Gerät zurücksetzen (Reset Device)“ durchgeführt wird.**

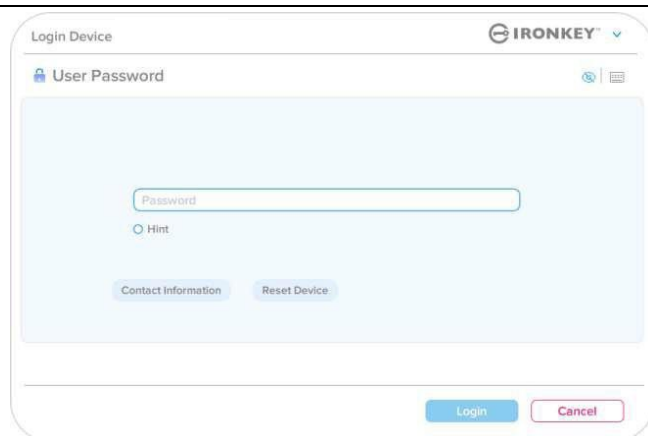


Abb. 6.3 – Anmeldung mit Benutzer-Passwort (Admin nicht aktiviert)

Gerät verwenden

Schutz vor Brute-Force-Angriffen

Wichtig: Wenn Sie während der Anmeldung ein falsches Passwort eingeben, erhalten Sie eine weitere Gelegenheit, das korrekte Passwort einzugeben. Das integrierte Sicherheitsmodul (auch bekannt als Schutz vor Brute-Force-Angriffen) registriert die Anzahl der fehlgeschlagenen Anmeldeversuche.*

Wenn die voreingestellte Anzahl von 10 fehlgeschlagenen Passwordeingabeversuche erreicht wurde, verhält sich das System wie folgt:

Admin/Benutzer aktiviert	Brute-Force-Schutz Geräteverhalten (10 falsche Passwordeingabeversuche)	Datenlöschung und Geräte-Reset?
Benutzer-Passwort:	Passwort-Sperre. Als Administrator anmelden, um das Benutzer-Passwort zurückzusetzen	NEIN
Admin-Passwort	Krypto-Löschen des Laufwerks, Passwörter, Einstellungen und Daten werden für immer gelöscht.	JA
Nur-Benutzer Einzelner Benutzer, einzelnes Passwort (Admin/Benutzer <u>NICHT</u> aktiviert)	Brute-Force-Schutz Geräteverhalten (10 falsche Passwordeingabeversuche)	Datenlöschung und Geräte-Reset?
Benutzerpasswort	Krypto-Löschung des Laufwerks, Passwörter, Einstellungen und Daten werden endgültig gelöscht	JA

*Sobald Sie sich erfolgreich am Gerät authentifiziert haben, wird der Zähler für fehlgeschlagene Anmeldungen zurückgesetzt, je nachdem, welche Anmeldemethode verwendet wurde. Das Krypto-Löschen löscht alle Passwörter, Verschlüsselungsschlüssel und Daten – **Ihre Daten gehen für immer verloren.**

Zugriff auf die sicheren Dateien

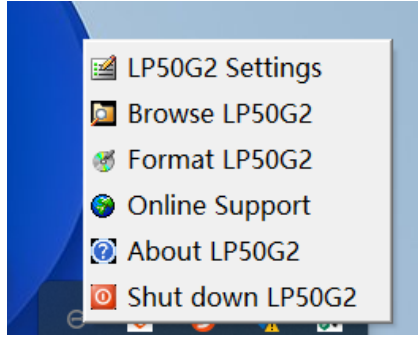
Nachdem Sie den USB-Stick entsperrt haben, können Sie auf Ihre sicheren Dateien zugreifen. Dateien werden automatisch ver- und entschlüsselt, wenn diese auf dem Stick gespeichert oder geöffnet werden. Diese Technologie bietet Ihnen den Komfort des Arbeitens wie mit einem normalen Stick, während sie gleichzeitig eine starke „Immer-aktive“-Sicherheit bietet.

Hinweis: Der Zugriff auf Ihre Dateien ist auch möglich, indem Sie mit der rechten Maustaste auf das **IronKey-Symbol** in der Windows-Taskleiste klicken und dann auf Secure Files (Sichere Dateien) klicken. **LP50G2 durchsuchen** (Abb. 7.2)

Geräteoptionen – (Windows-Umgebung)

Solange Sie auf dem Gerät angemeldet sind, wird in der rechten Ecke des Fensters das IronKey-Symbol angezeigt. Wenn Sie mit der rechten Maustaste auf das IronKey-Symbol klicken, öffnet sich das Auswahlmenü für die verfügbaren Laufwerksoptionen (Abb. 6.2).

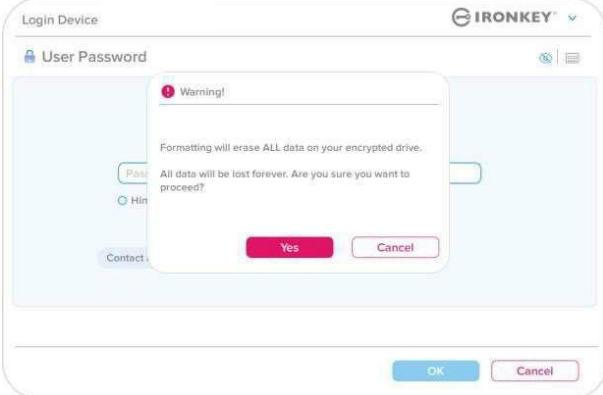
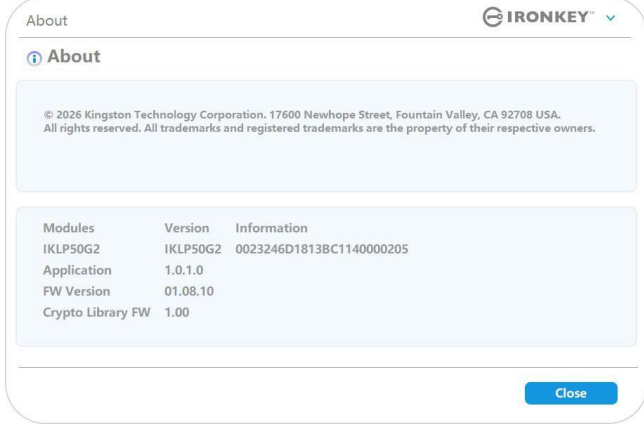
Einzelheiten zu diesen Geräteoptionen siehe die Seiten 19–23 dieses Benutzerhandbuchs.

Solange Sie auf dem Gerät angemeldet sind, wird in der rechten Ecke des Fensters das IronKey-Symbol angezeigt. (Abb. 7.1)	 Abb. 7.1 – IronKey-Symbol in Taskleiste
Wenn Sie mit der rechten Maustaste auf das IronKey-Symbol klicken, öffnet sich das Auswahlmenü für die verfügbaren Laufwerksoptionen. (Abb. 7.2) Einzelheiten zu diesen Geräteoptionen siehe die Seiten 19–23 dieses Benutzerhandbuchs.	 Abb. 7.2 – Rechtsklick auf das IronKey-Symbol für Geräteoptionen

Geräteoptionen – (macOS-Umgebung)

Wenn Sie auf dem Gerät angemeldet sind, finden Sie im macOS-Menü ein IronKey LP50G2-Symbol (siehe Abb. 7.3), mit dem die verfügbaren Geräteoptionen geöffnet werden. Einzelheiten zu diesen Geräteoptionen siehe die Seiten 19–23 dieses Benutzerhandbuchs.	 Abb. 7.3 – Symbol in Menüleiste für macOS/Menü Geräteoptionen
--	--

Geräteoptionen

LP50G2-Einstellungen:	• Ändern des Anmelde-Passworts, der Kontaktinformationen und anderer Einstellungen. (Weitere Einzelheiten zu den Geräteeinstellungen finden Sie im Abschnitt „LP50G2 Einstellungen“ in diesem Benutzerhandbuch.)
LP50G2 durchsuchen:	• Damit können Ihre gesicherten Dateien angezeigt werden.
LP50G2 formatieren: Mit dieser Funktion können Sie die sichere Datenpartition formatieren. (Warnhinweis: Hierbei werden alle Daten gelöscht.) (Abb. 6.1) Hinweis: Zum Formatieren ist eine Passwort-Authentifizierung erforderlich.	 Abb. 7.4 – LP50G2 formatieren
Online-Support:	• Öffnet Ihren Internetbrowser und navigiert zu http://www.kingston.com/support, wo Sie Zugang zu weiteren Support-Informationen erhalten.
Über LP50G2: Hier finden Sie spezifische Informationen über den LP50G2, einschließlich Informationen zu Anwendung, Firmware und Seriennummer (Abb. 6.2). Hinweis: Die individuelle Seriennummer des Laufwerks finden Sie in der Spalte „Information (Informationen)“.	 Abb. 7.5 – Über den LP50G2
LP50G2 trennen:	• Führt den LP50G2 ordnungsgemäß herunter, damit Sie ihn sicher aus Ihrem System entfernen können.

LP50G2 Einstellungen

Admin-Einstellungen

Mit der Admin-Anmeldung haben Sie Zugriff auf die folgenden Geräteeinstellungen:

- **Passwort:** Hiermit können Sie das Admin-Passwort bzw. den Hinweis ändern (Abb. 8.1).
- **Kontaktinformationen (Contact Info):** Hier können Kontaktinformationen hinzugefügt, angezeigt oder geändert werden (Abb. 8.2).
- **Language:** Hier lässt sich die gewählte Sprache ändern (Abb. 8.3).
- **Admin-Optionen (Admin Options):** Damit erhalten Sie Zugriff auf zusätzliche Funktionen, wie z. B.:
 - Ändern des Benutzerpassworts (Abb. 8.4)

HINWEIS: Weitere Einzelheiten zu den Admin-Optionen finden Sie auf Seite 25.

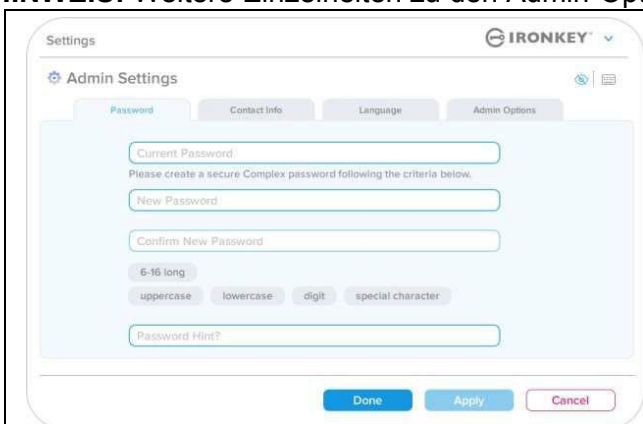


Abb. 8.1 – Optionen mit Admin-Passwort

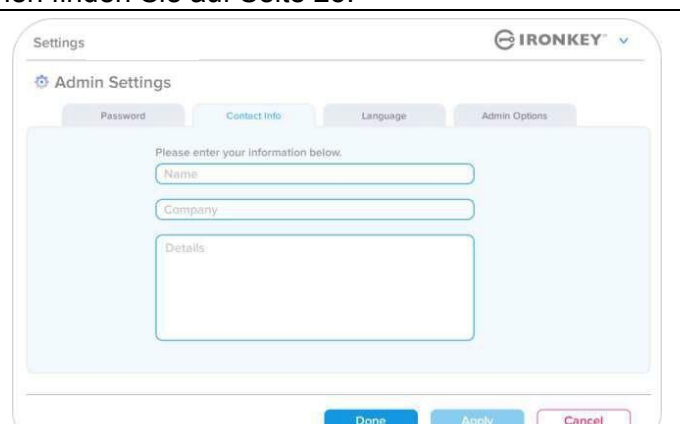


Abb. 8.2 – Kontaktinformationen

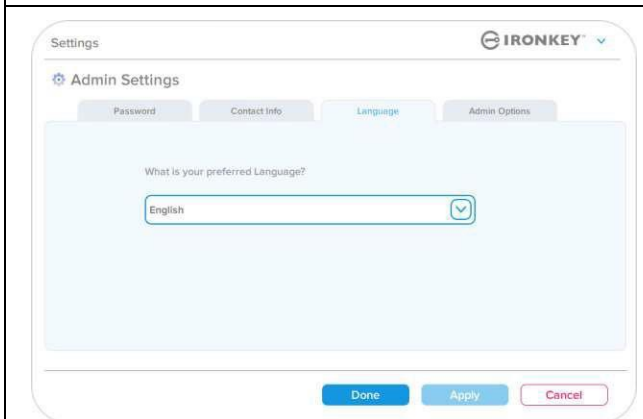


Abb. 8.3 – Sprachauswahl

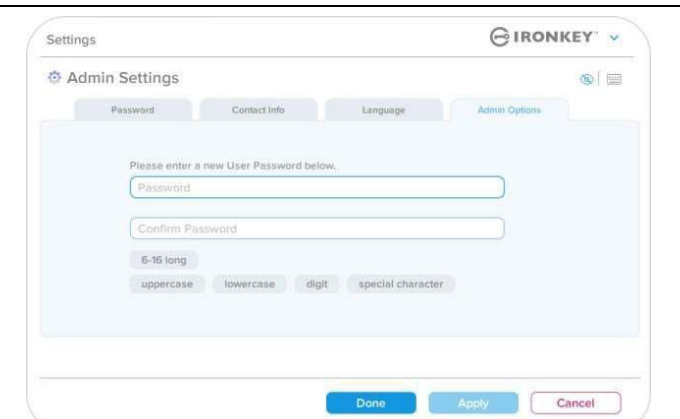


Abb. 8.4 – Admin-Optionen

LP50G2 Einstellungen

Benutzer-Einstellungen: Admin aktiviert

Die Benutzeranmeldung beschränkt den Zugriff auf die folgenden Einstellungen:

Passwort:

Ermöglicht Ihnen, Ihr eigenes Benutzer-Passwort bzw. Ihren Hinweis zu ändern. (Abb. 8.5)

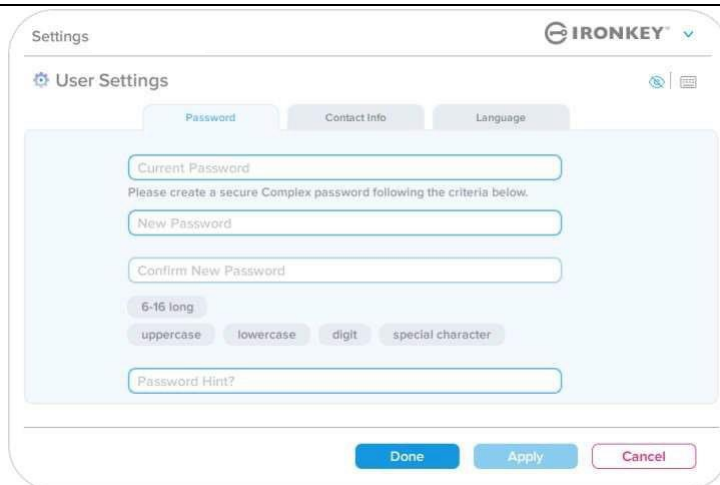


Abb. 8.5 – Passwort-Optionen (Admin aktiviert: Benutzeranmeldung)

Kontaktinformationen (Contact Info):

Hiermit können Sie Ihre Kontaktinformationen hinzufügen/anzeigen/ändern. (Abb. 8.6)

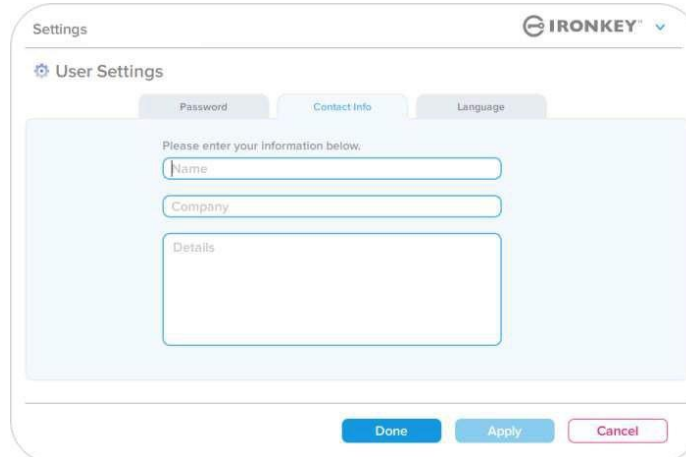


Abb. 8.6 – Kontaktinformationen (Admin aktiviert: Benutzeranmeldung)

Language:

Hiermit können Sie Ihre aktuelle Sprachauswahl ändern. (Abb. 8.7)

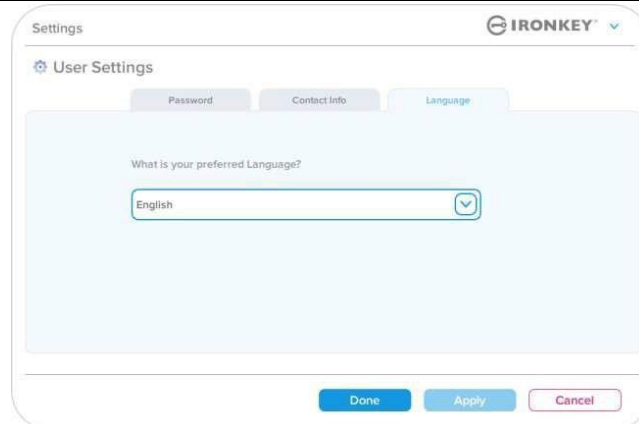


Abb. 8.7 – Spracheinstellungen (Admin aktiviert: Benutzeranmeldung)

Hinweis: Die Admin-Optionen sind nicht zugänglich, wenn Sie sich mit dem Benutzer-Passwort angemeldet haben.

LP50G2 Einstellungen

Benutzer-Einstellungen: Admin nicht aktiviert

Wie bereits auf Seite 12 erwähnt, führt die Initialisierung des LP50G2 ohne Aktivierung von „Admin- und Benutzer-Passwörtern“ zu einer Konfiguration des Sticks mit der Konfiguration **„Einzelnes Passwort“ und „Einzelner Benutzer“**. Diese Konfiguration bietet keinen Zugriff auf Admin-Optionen oder -Funktionen. Mit dieser Konfiguration haben Sie Zugriff auf die folgenden LP50G2-Einstellungen:

Passwort

Ermöglicht Ihnen, Ihr eigenes Benutzer-Passwort bzw. Ihren Hinweis zu ändern. (Abb. 8.8)

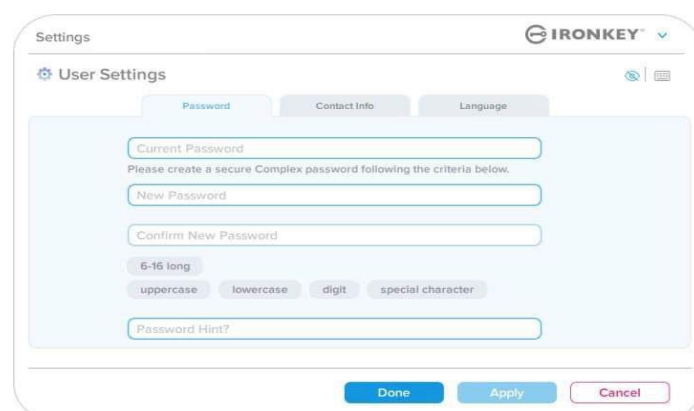


Abb. 8.8 – Passwortoptionen (Nur-Benutzer-Modus)

Kontaktinformationen (Contact Info):

Hiermit können Sie Ihre Kontaktinformationen hinzufügen/anzeigen/ändern. (Abb. 8.9)

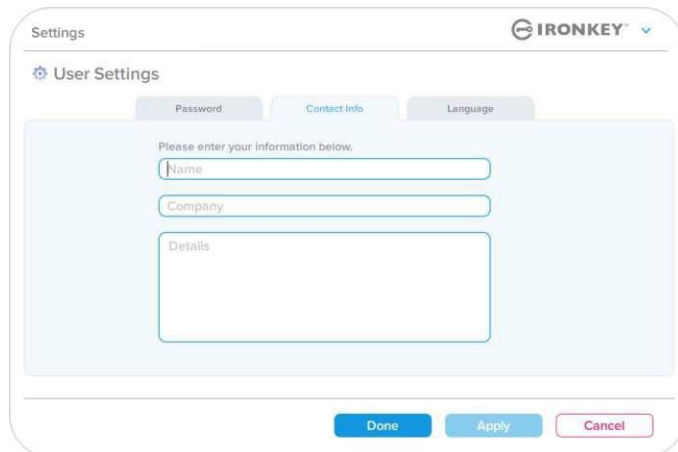


Abb. 8.9 – Kontaktinformationen (Nur-Benutzer-Modus)

Language:

Hiermit können Sie Ihre aktuelle Sprachauswahl ändern. (Abb. 8.10)

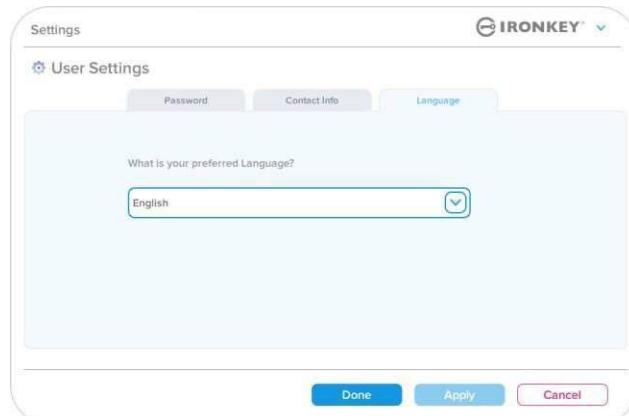


Abb. 8.10 – Spracheinstellungen (Nur-Benutzer-Modus)

LP50G2 Einstellungen

Ändern und Speichern von Einstellungen

- Wenn Einstellungen in den LP50G2-Einstellungen geändert werden (z. B. Kontaktinformationen, Sprache, Passwortänderungen, Admin-Optionen usw.), fordert der USB-Stick Sie auf, Ihr Passwort einzugeben, um die Änderungen zu akzeptieren und zu übernehmen. (Siehe Abb. 8.11)

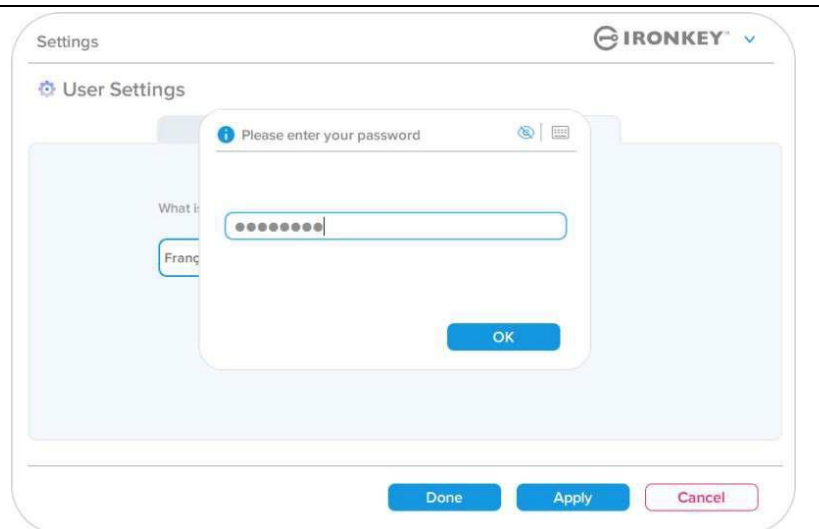


Abb. 8.11 – Bildschirm mit Passwortabfrage zum Speichern von LP50G2-Einstellungsänderungen

Hinweis: Wenn Sie sich auf dem obigen Bildschirm mit der Passwortabfrage befinden und Ihre Änderungen rückgängig machen oder ändern möchten, ist dies möglich, wenn das Passwortfeld leer ist und Sie auf „OK“ klicken. Dadurch wird das Feld „Bitte Passwort eingeben (Please enter your Password)“ geschlossen und das Menü „LP50G2 Einstellungen (Settings)“ wird wieder angezeigt.

Admin-Funktionen

Verfügbare Optionen zum Zurücksetzen des Benutzer-Passworts

Eine der nützlichen Funktionen der Admin-Konfiguration ermöglicht es Ihnen, das Passwort des Benutzers sicher zurückzusetzen, falls es einmal vergessen werden sollte. Im Folgenden ist die Funktion „Benutzer-Passwort zurücksetzen (User Password Reset)“ aufgeführt, die beim Zurücksetzen des Benutzer-Passworts hilfreich sein kann:

Benutzer-Passwort zurücksetzen:

Ändern Sie das Benutzer-Passwort manuell im Menü „Admin-Optionen (Admin Options)“. Die Änderung ist sofort wirksam und wird bei der nächsten Anmeldung des Benutzers übernommen. (Abb. 9.1)

Hinweis: Die Kriterien für die Passwortanforderungen werden auf die ursprünglichen Kriterien zurückgesetzt, die während des Initialisierungsprozesses festgelegt wurden (Optionen für „Komplex (Complex)“ oder „Passphrase“).

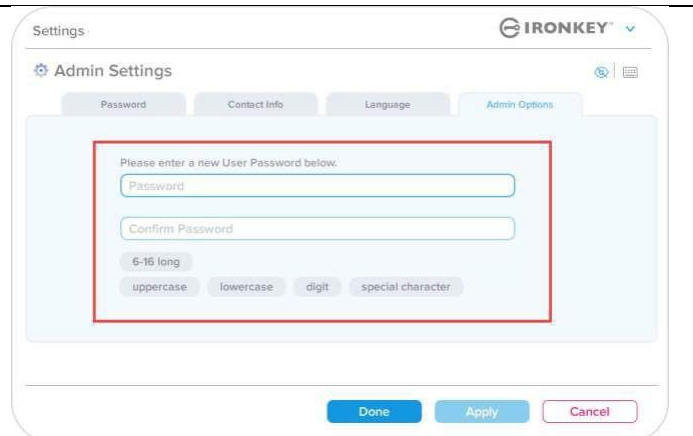


Abb. 9.1 – Admin-Optionen/Benutzer-Passwort zurücksetzen

Hilfe und Fehlerbehebung

Gerätesperrung

Der LP50G2 verfügt über eine Sicherheitsfunktion, die den unbefugten Zugriff auf die Datenpartition verhindert, sobald eine maximale Anzahl von **aufeinanderfolgenden** fehlgeschlagenen Anmeldeversuchen (kurz: *MaxNoA*) erfolgt ist. Die Standardkonfiguration „Fabrikneu (Out-of-Box)“ verfügt über einen vorkonfigurierten Wert von 10 (Anzahl der Versuche) für jede Anmeldemethode (Admin/Benutzer).

Der „Sperr“-Zähler registriert alle fehlgeschlagenen Anmeldeversuche und kann auf **eine von zwei** Arten zurückgesetzt werden:

1. Eine erfolgreiche Anmeldung vor dem Erreichen von MaxNoA
2. Erreichen von MaxNoA und Ausführen einer Gerätesperrung oder einer Geräteformatierung, je nachdem, wie der USB-Stick konfiguriert ist.

- Wenn Sie ein falsches Passwort eingeben, erscheint eine rote Fehlermeldung über dem Feld für die Passworteingabe, die auf einen Anmeldefehler hinweist. (Abb. 10.1)

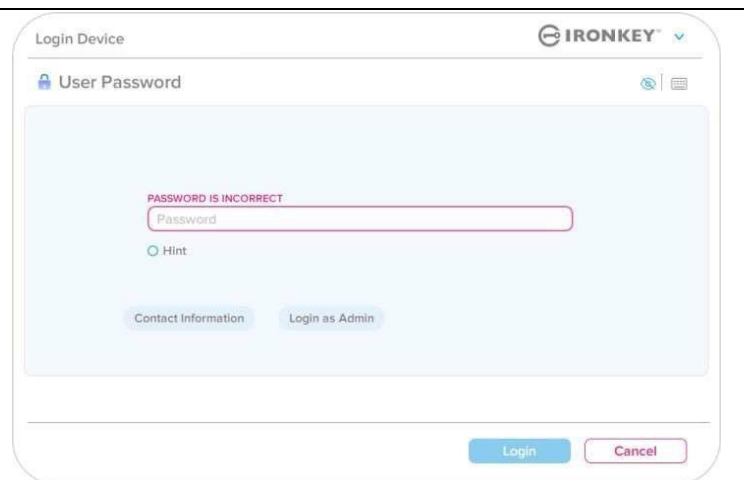


Abb. 10.1 – Meldung „Falsches Passwort“

- Wenn der Anmeldeversuch das 7. Mal fehlgeschlagen ist, wird eine weitere Fehlermeldung mit der Mitteilung angezeigt, dass Ihnen noch 3 Versuche bis zum Erreichen von MaxNoA bleiben (der standardmäßig auf 10 eingestellt ist). (Abb. 10.2)

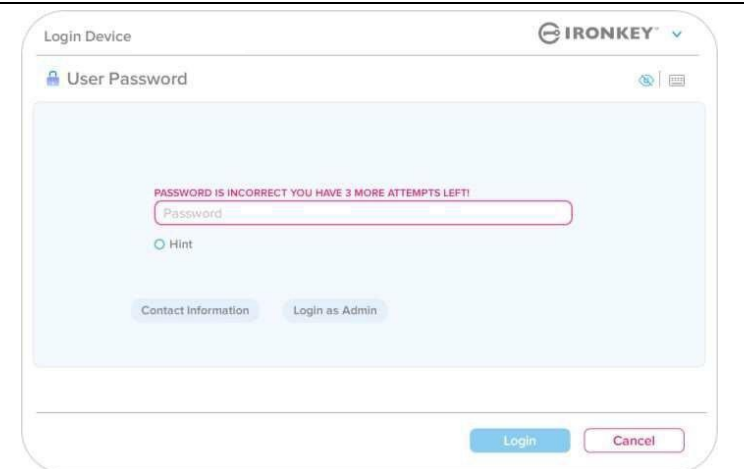


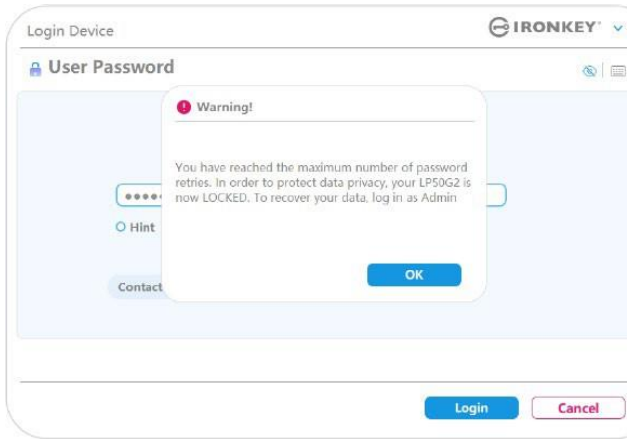
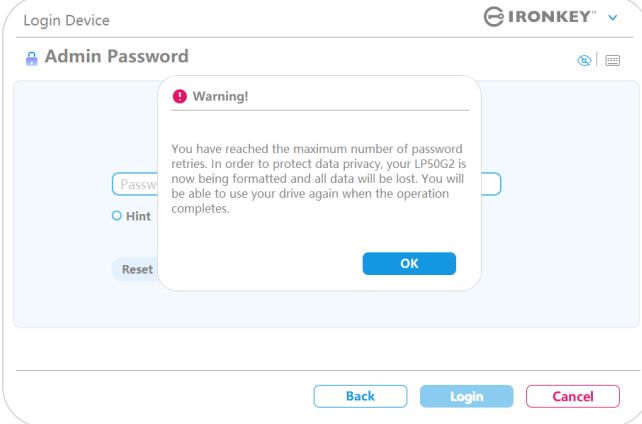
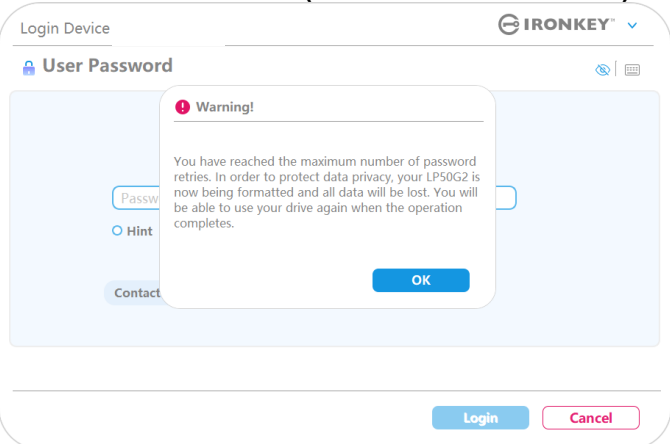
Abb. 10.2 – 7. falscher Passworteingabeversuch

Hilfe und Fehlerbehebung

Gerätesperrung

Wichtig: Nach dem 10. und letzten fehlgeschlagenen Anmeldeversuch wird das Gerät je nach Konfiguration und Anmeldemethode (Admin, Benutzer) entweder gesperrt, wodurch Sie sich mit einer anderen Methode anmelden müssen (falls zutreffend), oder das Gerät wird zurückgesetzt, wodurch **die Daten formatiert werden und alle Daten auf dem Stick unwiederbringlich verloren gehen**. Verhaltensmöglichkeiten, die auch auf Seite 17 in diesem Benutzerhandbuch erwähnt werden.

Die folgenden Abb. 10.3 – 10.6 zeigen das visuelle Verhalten für die 10. und letzte fehlgeschlagenen Anmeldung bei jeder Anmeldepasswortmethode:

Benutzer-Passwort: (Admin/Benutzer aktiviert)  GERÄTESPERRUNG Abb. 10.3	Admin-Passwort (Admin/Benutzer aktiviert)  GERÄT FORMATIEREN* Abb. 10.4
• Diese Sicherheitsmaßnahmen verhindern, dass jemand (der Ihr Passwort nicht kennt) unzählige Anmeldeversuche unternimmt und sich Zugang zu Ihren sensiblen Daten verschafft (auch bekannt als Brute-Force-Angriff). Auch wenn Sie der Besitzer des LP50G2 sind und Ihr Passwort vergessen haben, werden dieselben Sicherheitsmaßnahmen ausgeführt, einschließlich der Geräteformatierung. Weitere Einzelheiten zu dieser Funktion siehe „Gerät zurücksetzen (Reset Device)“ auf Seite 27.	Benutzer-Passwort (Admin NICHT aktiviert)  GERÄT FORMATIEREN* Abb. 10.5

***Hinweis:** Bei einer Geräteformatierung werden ALLE auf der sicheren Datenpartition des LP50G2 gespeicherten Informationen gelöscht.

Hilfe und Fehlerbehebung

Gerät zurücksetzen

Wenn Sie Ihr Passwort vergessen haben oder Ihr Gerät zurücksetzen müssen, können Sie auf die Schaltfläche „Gerät zurücksetzen (Reset Device)“ klicken, die an einer von zwei Stellen erscheint, je nachdem, wie der USB-Stick eingerichtet ist (entweder im Menü „Admin-Anmeldepasswort (Admin Login Password)“, wenn Admin/ Benutzer aktiviert ist, oder im Anmeldemenü „Benutzer-Passwort (User Password)“, wenn der Admin/ Benutzer-Modus nicht aktiviert ist), wenn der LP50G2-Launcher ausgeführt wird. (Siehe Abb. 10.7 und 10.8)

- Mit dieser Option können Sie ein neues Passwort erstellen, jedoch wird der LP50G2 zum Schutz Ihrer Daten neu formatiert. Das bedeutet, dass alle Ihre Daten in diesem Prozess unwiederbringlich gelöscht werden.*

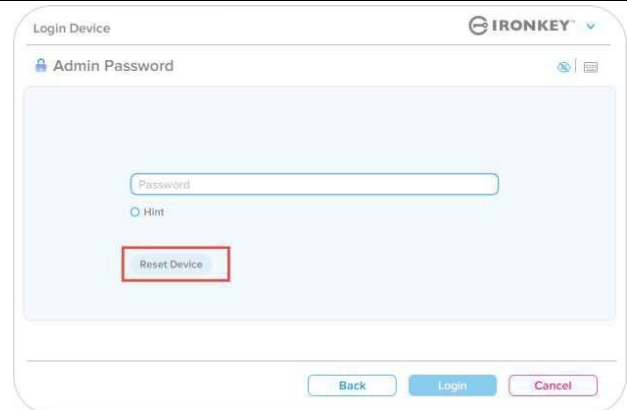


Abb. 10.6 – Admin-Passwort: Schaltfläche „Gerät zurücksetzen (Reset Device)“

- Hinweis:** Wenn Sie auf „Gerät zurücksetzen (Reset Device)“ klicken, erscheint eine Meldung, die fragt, ob Sie ein neues Passwort eingeben möchten, bevor die Formatierung durchgeführt wird. Sie haben jetzt die Wahl 1) dies durch Klicken auf „OK“ zu bestätigen oder 2) durch Klicken auf „Abbrechen (Cancel)“ abzubrechen und zum Anmeldefenster zurückzukehren. (Siehe Abb. 10.8)

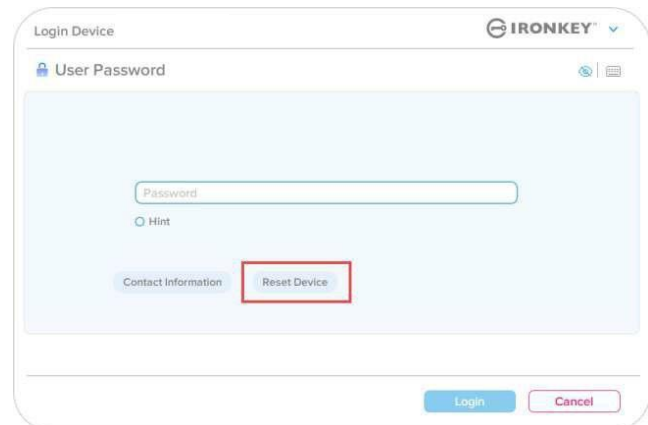


Abb. 10.7 – Benutzer-Passwort (Admin/Benutzer nicht aktiviert) Gerät zurücksetzen

- Wenn Sie sich entscheiden, fortzufahren, werden Sie zum Bildschirm „Initialisieren (Initialize)“ weitergeleitet, wo Sie „Admin- und Benutzer-Modus (Admin and User modes)“ aktivieren und Ihr neues Passwort eingeben können, je nachdem, welche Passwortooption Sie gewählt haben (Komplex oder Passphrase). Der Hinweis ist kein Pflichtfeld, kann jedoch eine nützliche Hilfestellung zur Erinnerung an das Passwort sein, falls Sie es vergessen haben sollten.

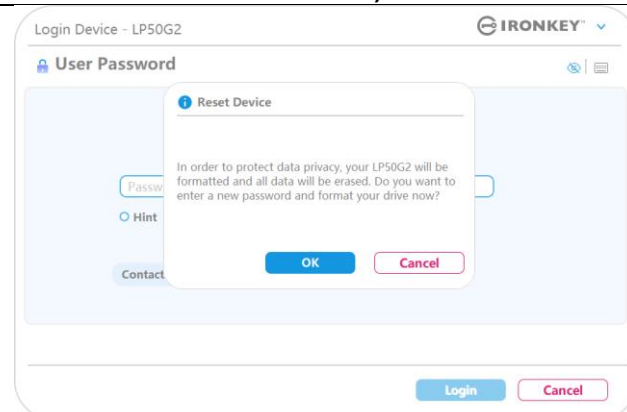


Abb. 10.8 – Bestätigung „Gerät zurücksetzen (Reset Device)“

Laufwerksbuchstaben-Konflikt: Windows-Betriebssysteme

- Wie bereits im Abschnitt „Systemanforderungen“, Seite 4 in dieser Anleitung erwähnt, benötigt der LP50G2 zwei freie aufeinanderfolgende Laufwerksbuchstaben NACH dem letzten physischen Speicher, der vor der Lücke“ in den Laufwerksbuchstabenzuweisungen angezeigt wird (siehe Abb. 10.9.) Dies bezieht sich NICHT auf Netzwerkfreigaben, da diese speziell für Benutzerprofile sind und sich nicht auf das System-Hardwareprofil selbst beziehen, und daher im Betriebssystem als verfügbar erscheinen.
- Das bedeutet, dass Windows dem LP50G2 möglicherweise einen Laufwerksbuchstaben zuweist, der bereits von einer Netzwerkfreigabe oder einem UNC-Pfad (Universal Naming Convention) verwendet wird, wodurch ein Konflikt bei Laufwerksbuchstaben entsteht. Wenn dies geschieht, wenden Sie sich bitte an Ihren Administrator oder die Helpdesk-Abteilung hinsichtlich der Änderung von Laufwerksbuchstabenzuweisungen in der Windows Datenträgerverwaltung (Administratorrechte erforderlich).

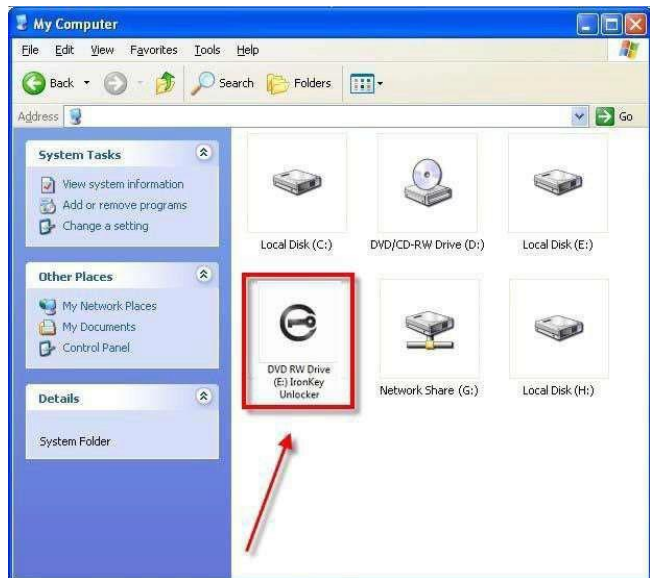


Abb. 10.9 – Beispiel für Laufwerksbuchstaben

In diesem Beispiel (Abb. 10.9) verwendet der LP50G2 der Stick „F:“, das erste verfügbare Laufwerk nach Laufwerk „E:“ (dem letzten physischen Laufwerk vor der Laufwerksbuchstabenlücke). Da der Buchstabe „G:“ eine Netzwerkfreigabe und nicht Teil des Hardware-Profiles ist, kann der LP50G2 versuchen, ihn als zweiten Laufwerksbuchstaben zu verwenden und dadurch einen Konflikt verursachen.

Wenn es in Ihrem System keine Netzwerkfreigaben gibt und der LP50G2 nicht lädt, ist es möglich, dass ein Kartenleser, ein Wechselmedium oder ein vorher installiertes Gerät noch eine Laufwerksbuchstabenzuordnung beibehält und noch immer einen Konflikt verursacht.

Beachten Sie bitte, dass die „Drive Letter Management“ oder (DLM) unter Windows 11 erheblich verbessert wurde, und dieses Problem evtl. gar nicht auftritt. Sollten Sie den Konflikt jedoch nicht lösen können, wenden Sie sich für technischen Support bitte an Kingston.com/support.



**CLÉ USB 3.2 Gen 1 SÉCURISÉE
IRONKEY™ Locker+ 50 G2
(LP50G2)**

Guide de l'utilisateur



Sommaire

Introduction	3
Fonctionnalités de la Locker+ 50 G2	4
À propos de ce manuel	4
Configuration système	4
Recommandations	5
Utiliser le bon système de fichiers	5
Rappels concernant l'utilisation	5
Meilleures pratiques pour la configuration des mots de passe	6
Configurer ma clé USB	7
Accès à la clé USB (environnement Windows).....	7
Accès à la clé USB (environnement macOS)	7
Initialisation de la clé USB (environnements Windows et macOS).....	8
Sélection du mot de passe	9
Clavier virtuel	11
Icône de visibilité du mot de passe	12
Mots de passe Admin et Utilisateur	13
Informations de contact.....	15
Utilisation de la clé USB (environnements Windows et macOS)	16
Connexion pour l'Administrateur et l'Utilisateur (Admin activé).....	16
Connexion pour le mode Utilisateur uniquement (Admin non activé).....	16
Protection contre les attaques par force brute.....	17
Accès à mes fichiers sécurisés	17
Options de la clé USB	18
Paramètres de la LP50G2	20
Paramètres Admin	20
Paramètres Utilisateur : Admin activé	21
Paramètres utilisateur : Admin non activé	22
Modifier et sauvegarder les paramètres de la LP50G2	23
Fonctionnalités Admin.....	24
Réinitialisation du mot de passe Utilisateur	24
Aide et dépannage	25
Verrouillage de la LP50G2	25
Réinitialisation de la LP50G2	27
Conflit de lettres de lecteur : (Windows).....	28



Figure 1 : IronKey LP50G2

Introduction

La clé USB Kingston IronKey™ Locker+ 50 G2 offre une sécurité de classe entreprise reposant sur le chiffrement matériel AES 256 bits en mode XTS certifié FIPS 197, comprenant des protections contre les attaques BadUSB et par force brute. La LP50G2 est également conforme à la TAA.

La LP50G2 prend désormais en charge l'option de mots de passe multiples (Admin et Utilisateur) avec les modes Complexe ou Phrase de passe. Le mode Complexe permet des mots de passe de 6 à 16 caractères en utilisant 3 des 4 jeux de caractères. Le nouveau mode Phrase de passe permet d'utiliser un code numérique, une phrase, une liste de mots ou même des paroles de 10 à 64 caractères. L'Administrateur peut activer un mot de passe Utilisateur ou réinitialiser le mot de passe Utilisateur pour restaurer l'accès aux données. Pour faciliter la saisie du mot de passe, le symbole « œil » peut être activé pour révéler le mot de passe saisi, ce qui réduit les fautes de frappe pouvant générer des échecs de tentative de connexion. La protection contre les attaques par force brute verrouille l'Utilisateur si le mot de passe Utilisateur est saisi incorrectement 10 fois de suite. Et efface les données et chiffre la clé si le mot de passe Admin est saisi incorrectement 10 fois de suite. En outre, un clavier virtuel intégré protège les mots de passe contre les enregistreurs de frappe ou d'écran.

La Locker+ 50 G2 est conçue pour être pratique, avec un petit boîtier métallique et un porte-clés intégré, pour emporter vos données partout avec vous.

La LP50G2 bénéficie d'une garantie limitée de 5 ans et du support technique gratuit de Kingston.

Fonctionnalités de l'IronKey Locker+ 50 G2

- Certification FIPS 197
- Chiffrement matériel XTS-AES (le chiffrement ne peut jamais être désactivé)
- Protection contre les attaques par force brute et BadUSB
- Mots de passe multiples
- Modes de mot de passe Complexe ou Phrase de passe
- Bouton en forme d'œil pour afficher les mots de passe saisis afin de réduire les tentatives de connexion ratées
- Clavier virtuel pour se protéger des enregistreurs de frappe et des enregistreurs d'écran
- Compatible avec Windows ou macOS (consulter la fiche technique pour plus de détails)

À propos de ce manuel (02122026)

Ce manuel d'utilisation concerne la clé USB IronKey Locker+ 50 G2 (LP50G2).

Configuration système requise

Plateforme PC • Intel et AMD • 15 Mo d'espace disque libre • Port USB 2.0 – 3.2 disponible • Deux lettres de lecteur consécutives après le dernier disque physique* *Remarque : voir la section « Conflit de lettres de lecteur » à la page 28.	Systèmes d'exploitation PC pris en charge • Windows 11
Plateforme Mac • Intel et Apple SOC • 15 Mo d'espace disque libre • Port USB 2.0 – 3.2	Système d'exploitation Mac pris en charge • macOS 13.x – 26.x

Recommandations

Pour que la LP50G2 bénéficie d'une alimentation suffisante, elle doit être insérée directement dans le port USB d'un ordinateur portable ou de bureau, comme illustré à la *Figure 1.1*. Évitez de connecter la LP50G2 à un périphérique équipé d'un port USB, par exemple un clavier ou un concentrateur/hub alimenté par USB, comme illustré à la *Figure 1.2*.



Figure 1.1 – Utilisation recommandée



Figure 1.2 – Utilisation non recommandée

Utiliser le bon système de fichiers

L'IronKey LP50G2 est livrée préformatée avec le système de fichiers FAT32. Ce système de fichiers fonctionne sur les systèmes Windows et macOS. Cependant, il pourrait y avoir d'autres options pouvant être utilisées pour la formater manuellement, comme NTFS pour Windows et exFAT. Vous pouvez reformater la partition de données si nécessaire, mais cela entraînera la perte des données qui s'y trouvent.

Rappels concernant l'utilisation

Pour assurer la sécurité de vos données, Kingston vous recommande ce qui suit :

- Procédez à une analyse antivirus sur votre ordinateur avant de configurer et d'utiliser la LP50G2 sur un système cible.
- Lorsque vous utilisez la clé USB sur un système public ou inconnu, vous pouvez utiliser le mode lecture seule afin de la protéger contre les logiciels malveillants.
- Verrouillez la clé USB lorsque vous ne l'utilisez pas.
- Éjectez la clé USB avant de la débrancher.
- Ne débranchez jamais la clé USB lorsque son voyant est allumé. Cela peut l'endommager et nécessiter un reformatage, ce qui effacera vos données.
- Ne communiquez jamais le mot de passe de votre clé USB à quiconque.

Obtenir les dernières mises à jour et informations

Rendez-vous sur kingston.com/support pour obtenir les dernières mises à jour de la clé USB, les réponses aux questions fréquentes, la documentation et des informations supplémentaires.

REMARQUE : seules les dernières mises à jour de la clé USB (le cas échéant) doivent lui être appliquées. La rétrogradation de la clé USB à une version antérieure du logiciel n'est pas prise en charge et peut potentiellement entraîner une perte des données stockées ou altérer d'autres fonctionnalités. Si vous avez des questions ou des problèmes, veuillez contacter le support technique de Kingston.

Meilleures pratiques pour la configuration des mots de passe

Votre LP50G2 est livrée avec de solides contre-mesures de sécurité. Notamment une protection contre les attaques par force brute qui empêchera un pirate de deviner des mots de passe en limitant les échecs de tentative de saisie mot de passe à 10. Lorsque cette limite est atteinte, la LP50G2 efface automatiquement les données chiffrées et s'auto-formate aux paramètres d'usine.

Mots de passe multiples

La LP50G2 présente une fonctionnalité majeure, à savoir les mots de passe multiples afin d'éviter les pertes de données en cas d'oubli d'un ou plusieurs mots de passe. Lorsque toutes les options de mot de passe sont activées, la LP50G2 peut prendre en charge deux mots de passe différents que vous pouvez utiliser pour récupérer des données : Admin et Utilisateur.

La LP50G2 vous permet de sélectionner deux mots de passe principaux : un mot de passe Administrateur (appelé mot de passe Admin) et un mot de passe Utilisateur. L'Administrateur peut accéder à la clé USB à tout moment et configurer des options pour l'Utilisateur : l'Administrateur est une sorte de « super utilisateur ».

L'Utilisateur peut également accéder à la clé USB, mais ses privilèges sont limités par rapport à ceux de l'Administrateur. Si l'un des deux mots de passe est oublié, l'autre mot de passe peut être utilisé pour accéder aux données et les récupérer. La clé USB peut alors être configurée de nouveau pour avoir deux mots de passe. Il est important de configurer les DEUX mots de passe et de sauvegarder le mot de passe Admin dans un endroit sûr tout en utilisant le mot de passe Utilisateur.

Si les deux mots de passe sont oubliés ou perdus, il n'y a aucun autre moyen d'accéder aux données. Kingston ne pourra pas récupérer les données, car le système de sécurité ne présente aucune porte dérobée. Kingston vous recommande d' également sauvegarder les données sur d'autres supports. La LP50G2 peut être réinitialisée et réutilisée, mais les données antérieures seront définitivement supprimées.

Modes de mot de passe

La LP50G2 prend en charge deux modes de mot de passe :

Complexe

Un mot de passe complexe doit comporter 6 à 16 caractères et utiliser au moins 3 de ces types de caractères :

- Caractères alphabétiques majuscules
- Caractères alphabétiques minuscules
- Chiffres
- Caractères spéciaux

Phrase de passe

La LP50G2 prend en charge les phrases de passe de 10 à 64 caractères. Une phrase de passe ne suit aucune règle supplémentaire, mais si elle est utilisée correctement, elle peut fournir des niveaux de protection très élevés.

Une phrase de passe est en fait n'importe quelle combinaison de caractères, notamment des caractères d'autres langues. Comme pour la LP50G2, la langue du mot de passe peut correspondre à la langue sélectionnée pour la clé USB. Cela vous permet de sélectionner plusieurs mots, une phrase entière, les paroles d'une chanson, un vers extrait d'un poème, etc. Les bonnes phrases de passe font partie des types de mots de passe les plus difficiles à deviner pour les attaquants, tout en étant plus faciles à retenir pour les utilisateurs.

Configurer ma clé USB

Pour que la clé USB chiffrée IronKey ait une alimentation suffisante, insérez-la directement dans un port USB 2.0/3.0 d'un ordinateur portable ou de bureau. Évitez de la brancher sur un périphérique doté d'un port USB, tel qu'un clavier ou un concentrateur/hub alimenté par USB. La configuration initiale de la clé USB doit être effectuée sur un système d'exploitation pris en charge basé sur Windows ou macOS.

Accès à la clé USB (environnement Windows)

Connectez la clé USB chiffrée IronKey à un port USB disponible de votre ordinateur de bureau ou portable et attendez que Windows la détecte.

- Les utilisateurs de Windows recevront une notification relative au pilote du périphérique.
(Figure 3.1)



Figure 3.1 – Notification relative au pilote du périphérique.

- Une fois la détection du nouveau matériel terminée, sélectionnez l'option **IronKey.exe** à l'intérieur de la partition Unlocker qui se trouve dans l'Explorateur de fichiers.
(Figure 3.2)
- Veuillez noter que la lettre de partition varie en fonction de la lettre du prochain lecteur libre. La lettre du lecteur peut changer en fonction des périphériques connectés. Dans l'image à droite ci-dessous, la lettre de la clé est (E:).

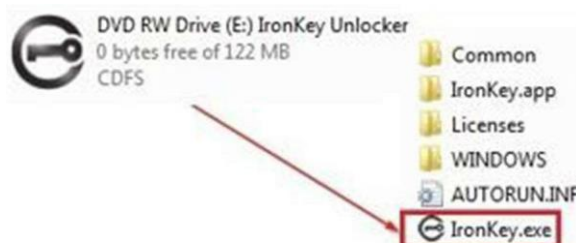


Figure 3.2 – Fenêtre de l'Explorateur de fichiers/IronKey.exe

Accès à la clé USB (Environnement macOS)

Insérez la LP50G2 dans un port USB disponible sur votre ordinateur de bureau ou portable et attendez que le système d'exploitation Mac la détecte. Lorsque la clé USB est détectée, un volume « IRONKEY » s'affiche sur le bureau. (Figure 3.3)

- Double-cliquez sur l'icône CD-ROM IronKey.
- Double-cliquez ensuite sur l'icône de l'application IronKey.app affichée dans la fenêtre illustrée à la Figure 3.3. Le processus d'initialisation va alors démarrer.

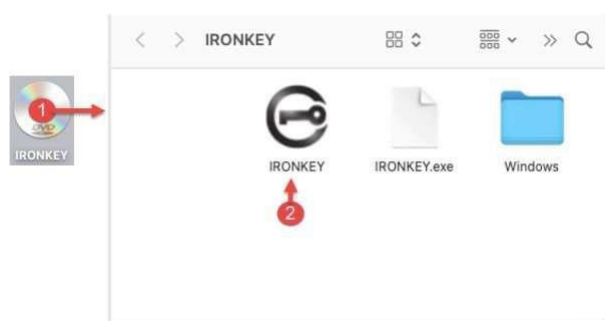


Figure 3.3 – Volume IRONKEY

Initialisation de la clé USB (environnements Windows et macOS)

Langue et Contrat de licence utilisateur final

Sélectionnez la langue de votre choix dans le menu déroulant, puis cliquez sur **Next** (Suivant).
(Figure 4.1)

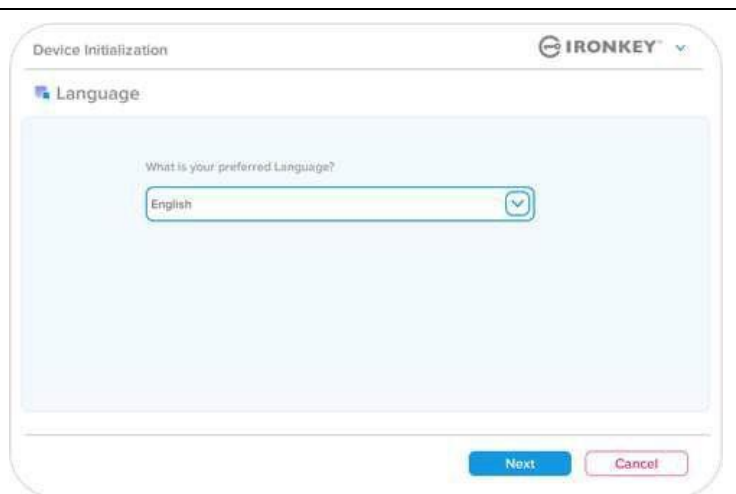


Figure 4.1 – Sélection de la langue

Lisez le contrat de licence et cliquez sur **Suivant**.

Remarque : vous devez accepter le contrat de licence pour continuer. Autrement, le bouton **Next** (Suivant) restera désactivé.
(Figure 4.2)

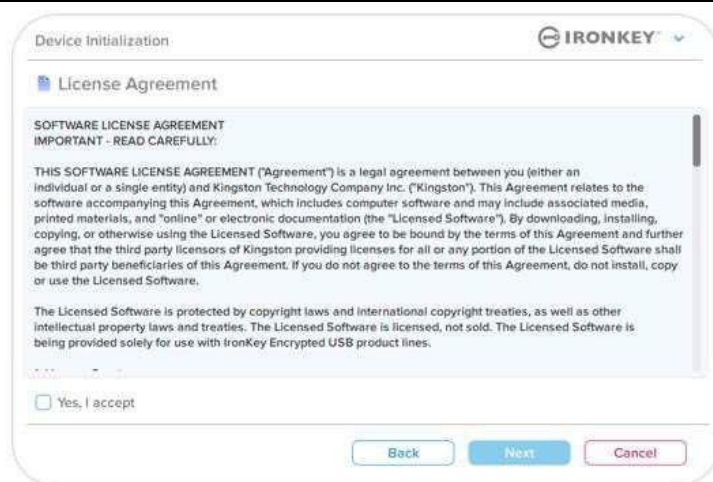


Figure 4.2 – Contrat de licence

Initialisation de la clé USB

Sélection du mot de passe

Sur l'écran d'invite Mot de passe, vous pourrez créer un mot de passe pour protéger vos données sur la LP50G2 en utilisant les modes Complexe ou Phrase de passe (*Figures 4.3 et 4.4*). En outre, les options Mots de passe multiples Admin/Utilisateur peuvent également être activées sur cet écran. Avant de procéder à la sélection du mot de passe, veuillez consulter la rubrique Activation des mots de passe Admin/Utilisateur ci-dessous pour mieux comprendre ces fonctionnalités.

Remarque : une fois que le mode Complexe ou Phrase de passe est choisi, il ne peut pas être modifié, sauf si la clé USB est réinitialisée. Pour commencer, créez votre mot de passe dans le champ « Password » (Mot de passe), puis saisissez-le à nouveau dans le champ « Confirm Password » (Confirmer le mot de passe). Le mot de passe doit respecter les critères suivants pour que le processus d'initialisation vous autorise à continuer :

Mot de passe complexe

- Doit contenir entre 6 et 16 caractères.
- Doit contenir trois (3) des types de caractères suivants :
 - Majuscule
 - Minuscule
 - Chiffre
 - Caractères spéciaux (!,\$,&, etc..)

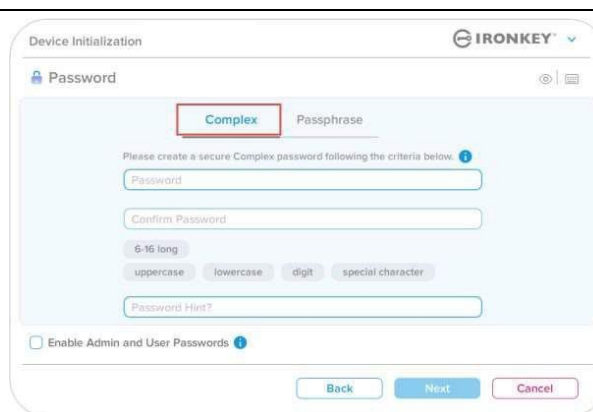


Figure 4.3 – Mot de passe complexe

Phrase de passe

- Doit contenir :
 - 10 caractères minimum
 - 64 caractères maximum

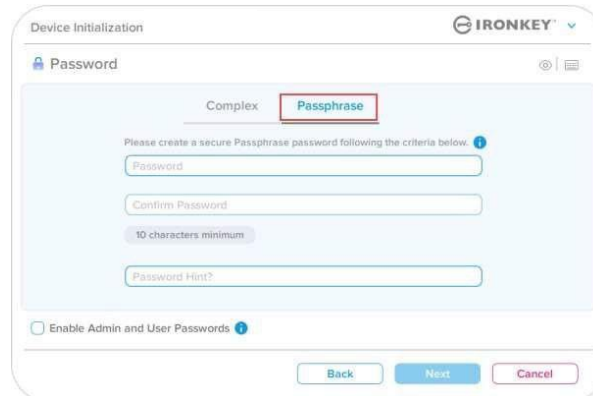


Figure 4.4 – Phrase de passe

Indice de mot de passe (facultatif)

Un indice de mot de passe peut être utile pour fournir une indication de ce qu'est le mot de passe, si jamais vous l'oubliez.

Remarque : l'indice NE DOIT PAS être le mot de passe lui-même.

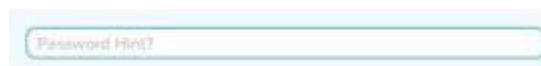


Figure 4.5 – Champ Password Hint (Indice de mot de passe)

Initialisation de la clé USB

Mots de passe valides et non valides

Pour les mots de passe **valides**, les cases de critères de mot de passe s'affichent en **vert** lorsque les critères sont remplis. (Voir les Figures 4.6a-b) Remarque : une fois que le minimum de trois critères de mot de passe est respecté, la case du quatrième critère devient grise, indiquant que ce critère est facultatif (Figure 4.6b).

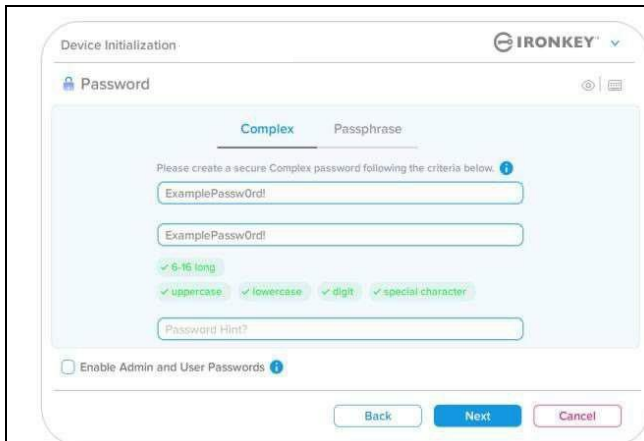


Figure 4.6a – Condition de mot de passe complexe remplie

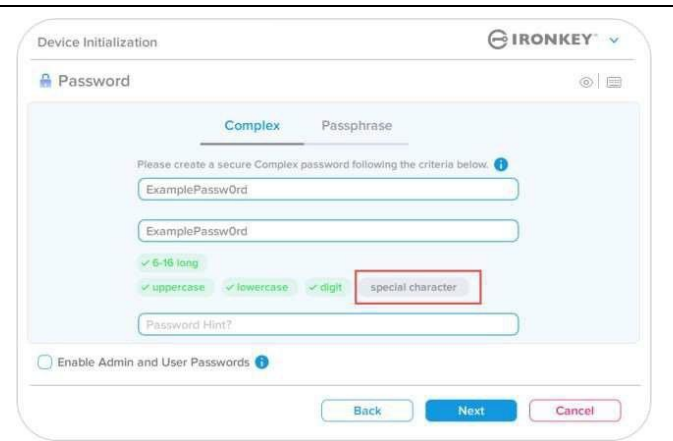


Figure 4.6b – Condition de mot de passe complexe facultative

Pour les mots de passe **non valides**, les cases de critères de mot de passe s'affichent en **rouge** et le bouton **Next (Suivant)** est désactivé jusqu'à ce que les conditions minimales soient remplies.

Cela s'applique à la fois aux mots de passe complexes et aux phrases de passe.

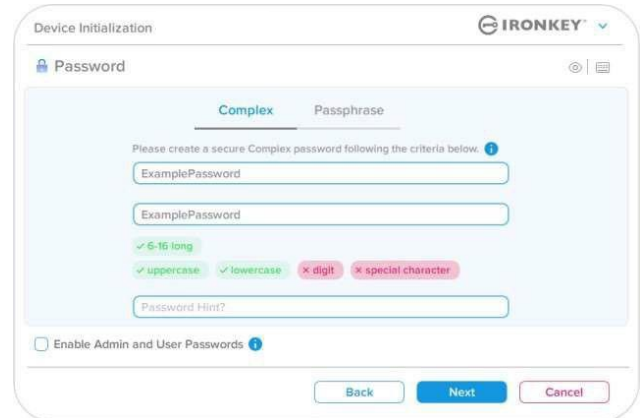


Figure 4.7 – Conditions de mot de passe non remplies

Initialisation de la clé USB

Clavier virtuel

La LP50G2 est dotée d'un clavier virtuel qui peut être utilisé pour se protéger contre les enregistreurs de frappe.

- Pour utiliser le **clavier virtuel**, localisez le bouton du clavier dans la partie supérieure droite de l'écran **Device Initialization** (Initialisation de la clé USB) et sélectionnez-le.

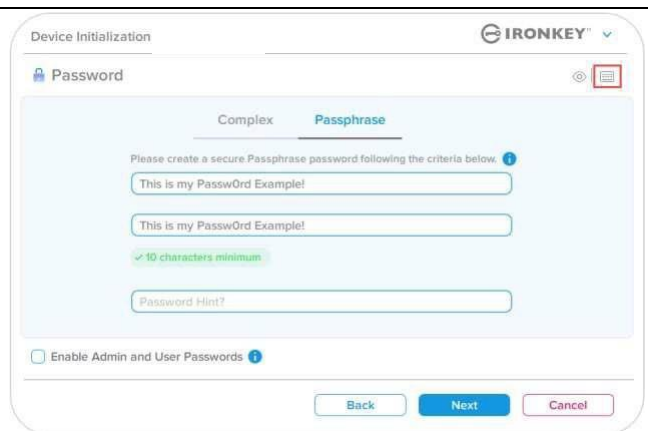


Figure 4.8 – Activation du clavier virtuel

- Une fois que le clavier virtuel apparaît, vous pouvez également activer la fonction **Screenlogger Protection** (Protection contre les enregistreurs d'écran). Lors de l'utilisation de cette fonctionnalité, toutes les touches apparaîtront brièvement comme vides. Ce comportement est normal, car il empêche les enregistreurs d'écran de capturer ce sur quoi vous avez cliqué.
- Pour rendre cette fonctionnalité plus robuste, vous pouvez également choisir de randomiser le clavier virtuel en sélectionnant **Randomize** (Disposition aléatoire) dans le coin inférieur droit du clavier. Le clavier sera alors organisé dans un ordre aléatoire.

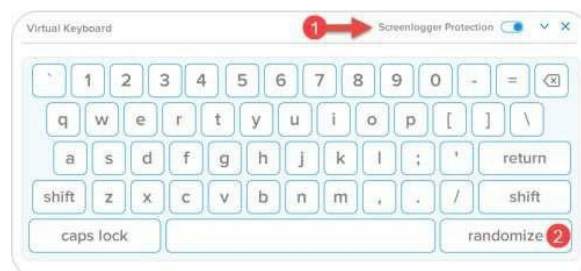


Figure 4.9 – Protection contre les enregistreurs d'écran/Disposition aléatoire

Initialisation de la clé USB

Icône de visibilité du mot de passe

Par défaut, lorsque vous créez un mot de passe, la chaîne du mot de passe s'affiche dans le champ au fur et à mesure que vous la saisissez. Si vous souhaitez masquer les caractères au fur et à mesure que vous tapez, vous pouvez activer l'icône en forme d'œil située dans la partie supérieure droite de la fenêtre d'initialisation de la clé USB.

Remarque : une fois la clé USB initialisée, le champ du mot de passe sera masqué par défaut.

Pour **masquer** le mot de passe, cliquez sur l'icône grise.

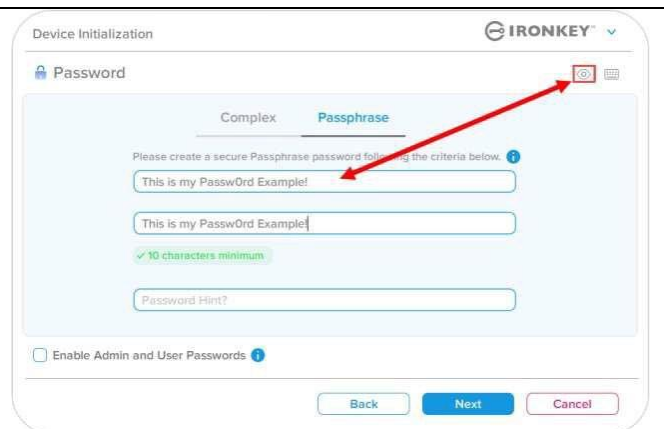


Figure 4.10 – Icône pour masquer le mot de passe

Pour **afficher** le mot de passe masqué, cliquez sur l'icône bleue.

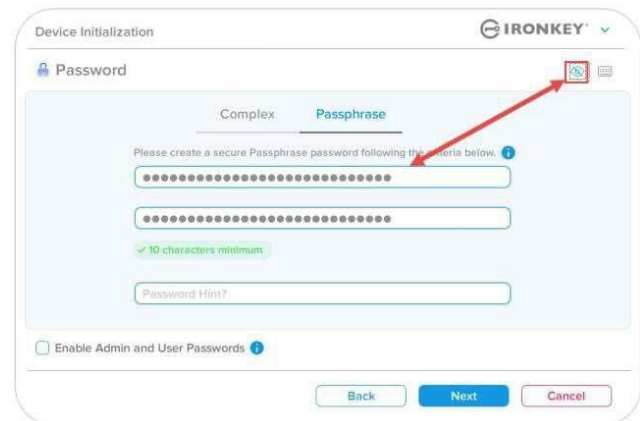


Figure 4.11 – Icône pour afficher le mot de passe

Initialisation de la clé USB

Mots de passe Admin et Utilisateur

En activant les mots de passe Admin et Utilisateur, vous pouvez tirer parti de la fonctionnalité de mots de passe multiples, via laquelle le rôle Administrateur peut gérer les deux comptes. En sélectionnant « **Enable Admin and User Passwords** » (Activer les mots de passe Admin et Utilisateur), vous disposez d'une méthode alternative d'accès à la clé USB en cas d'oubli de l'un des mots de passe.

Lorsque la fonctionnalité **Admin and User Passwords** (Mots de passe Admin et Utilisateur) est activée, vous pouvez également accéder aux options suivantes :

- Réinitialisation du mot de passe Utilisateur

Pour en savoir plus sur la fonctionnalité de réinitialisation du mot de passe Utilisateur, allez à la page 24 du présent Guide de l'utilisateur.

- Pour activer **les mots de passe Admin et Utilisateur**, cliquez sur la case située à côté de « **Enable Admin and User Passwords** » (Activer les mots de passe Admin et Utilisateur) et sélectionnez **Next** (Suivant) une fois qu'un mot de passe valide a été choisi. (Figure 4.12)

- Si cette fonctionnalité est **activée**, le mot de passe choisi sur cet écran sera le **mot de passe Admin**. Cliquez sur **Next** (Suivant) pour passer à l'écran **User Password** (Mot de passe Utilisateur), où vous pouvez choisir un mot de passe pour l'Utilisateur.

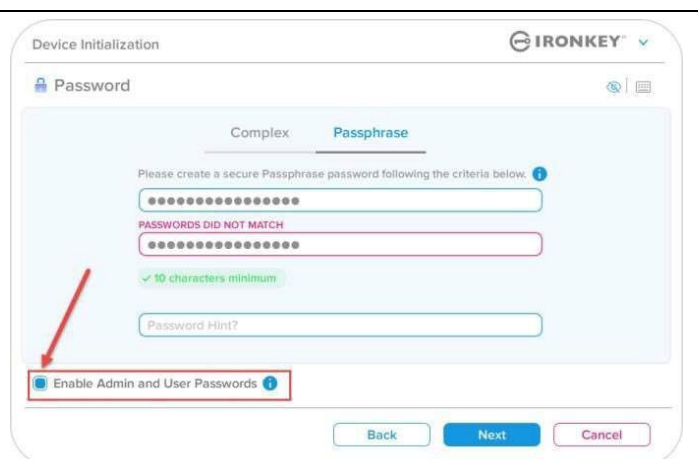


Figure 4.12 – Activation des mots de passe Admin et Utilisateur

Remarque : l'activation des mots de passe Admin et Utilisateur est facultative.

Si la clé USB est configurée avec cette fonctionnalité NON activée (case non cochée), elle sera configurée en tant que clé USB à **utilisateur unique** et à **mot de passe unique**, sans aucune fonctionnalité Administrateur. Cette configuration sera appelée **mode Utilisateur uniquement** tout au long de ce manuel.

Pour procéder à la configuration à un seul utilisateur et à un seul mot de passe, ne cochez pas la case **Enable Admin and User Passwords** (Activer les mots de passe Admin et Utilisateur) et cliquez sur **Next** (Suivant) après avoir créé un mot de passe valide.

Initialisation de la clé USB

Mots de passe Admin et Utilisateur

Si le rôle Admin a été **activé** à l'écran précédent, l'écran suivant demandera le **mot de passe Utilisateur** (Figure 4.13). Le mot de passe Utilisateur aura des capacités limitées par rapport au mot de passe Admin ; il fera l'objet d'une section plus détaillée ultérieurement. **Remarque :** « **Mots de passe Admin et Utilisateur** » sera désigné par « **rôle Admin** » dans la suite du présent document.

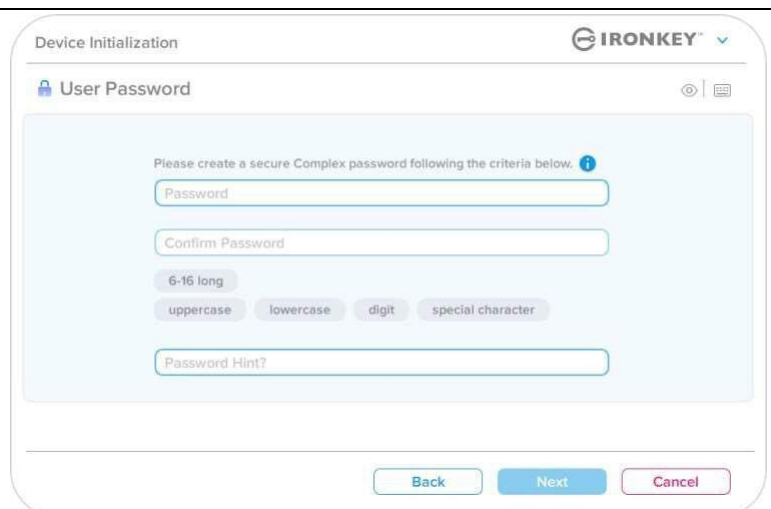


**Figure 4.13 – Mot de passe Utilisateur
(Admin et Utilisateur activés)**

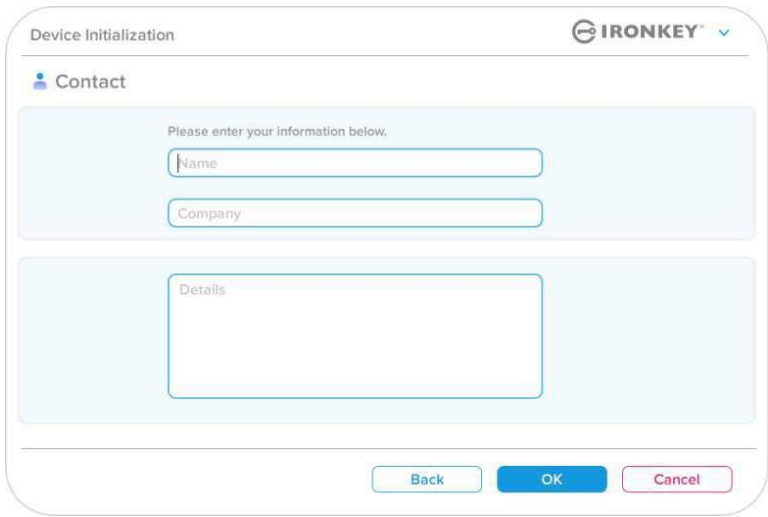
Remarque : l'option de mot de passe choisie (Complexe ou Phrase de passe) sera appliquée au mot de passe Utilisateur et à toute réinitialisation du mot de passe nécessaire après la configuration de la clé USB. L'option de mot de passe choisie ne peut être modifiée qu'après une réinitialisation complète de la clé USB.

Initialisation de la clé USB

Informations de contact

Entrez vos informations de contact dans les zones de texte prévues à cet effet (*Figure 4.14*).

Remarque : les informations que vous saisissez dans ces champs NE DOIVENT PAS contenir le mot de passe que vous avez créée à l'étape 3. Toutefois, ces champs sont facultatifs et peuvent être laissés vides, si vous le souhaitez.

Le champ « Name » (Nom) peut contenir jusqu'à 32 caractères, mais ne doit pas contenir le mot de passe exact. Le champ « Company » (Société) peut contenir jusqu'à 32 caractères, mais ne doit pas contenir le mot de passe exact. Le champ « Details » (Détails) peut contenir jusqu'à 156 caractères, mais ne doit pas contenir le mot de passe exact.	 Figure 4.14 – Informations de contact
---	---

Remarque : cliquez sur « OK » pour terminer le processus d'initialisation et procéder au déverrouillage puis au montage de la partition sécurisée, où vos données pourront être stockées en toute sécurité. Déconnectez la clé USB et reconnectez-la au système pour voir les changements effectifs.

Utilisation de la clé USB (environnements Windows et macOS)

Connexion pour l'Administrateur et l'Utilisateur (Admin activé)

Si la clé USB est initialisée avec les mots de passe Admin et Utilisateur (rôle Admin) activés, l'application de l'IronKey LP50G2 se lancera, en affichant d'abord l'écran de connexion User Password (Mot de passe Utilisateur). À partir de là, vous pouvez vous connecter avec le mot de passe Utilisateur, afficher les informations de contact saisies ou vous connecter en tant qu'Admin (*Figure 6.1*). Si vous cliquez sur le bouton « Login as Admin » (Se connecter en tant qu'Admin) (illustré ci-dessous), l'application passe au menu de connexion Admin, où vous pouvez vous connecter en tant qu'Admin pour accéder aux paramètres et fonctionnalités associées à ce rôle (*Figure 6.2*).

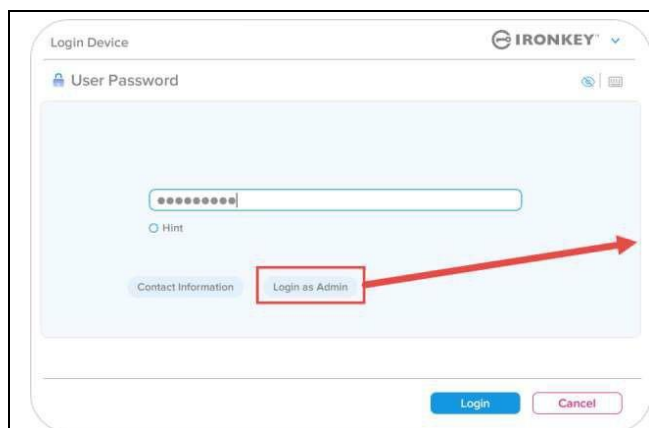


Figure 6.1 – Connexion à l'aide du Mot de passe Utilisateur (Admin activé)

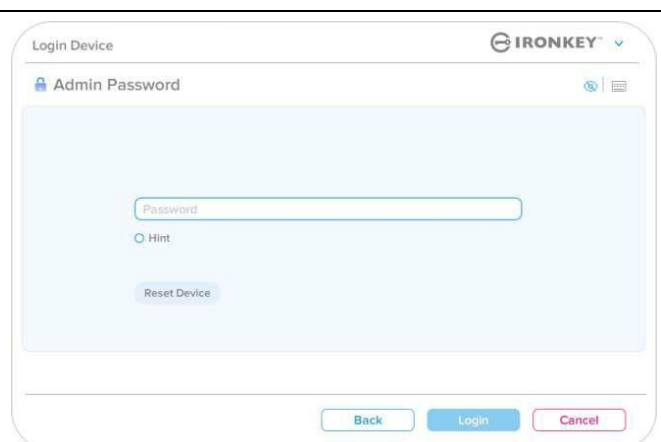


Figure 6.2 – Connexion à l'aide du Mot de passe Admin

Connexion en Mode Utilisateur uniquement (Admin non activé)

Comme indiqué à la **page 13**, bien qu'il soit recommandé d'utiliser la fonctionnalité du rôle Admin pour en tirer pleinement parti, la clé USB IronKey peut également être initialisée en mode Utilisateur uniquement (mot de passe unique, utilisateur unique). Cette option est destinée aux personnes qui souhaitent une approche simple, avec un seul mot de passe, pour sécuriser leurs données sur leur clé USB. (*Figure 6.3*)

Remarque : pour activer les mots de passe Admin et Utilisateur, utilisez le bouton **Reset Device** (Réinitialiser la clé USB) pour remettre la clé USB à l'état d'initialisation, où vous pouvez activer les mots de passe Admin et Utilisateur. **La réinitialisation de la clé USB entraîne son formatage et la perte définitive de TOUTES les données qu'elle contient.**

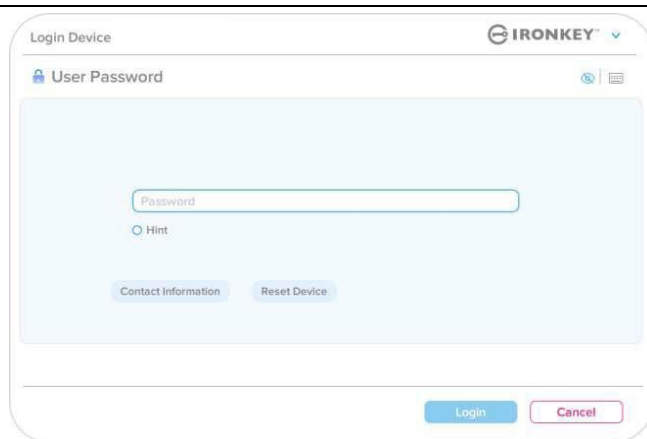


Figure 6.3 – Connexion à l'aide du mot de passe Utilisateur (Admin non activé)

Utilisation de la clé USB

Protection contre les attaques par force brute

Important : lors de la connexion, si un mot de passe incorrect est saisi, vous aurez une autre occasion d'entrer le mot de passe correct. Cependant, il existe une fonctionnalité de sécurité intégrée (également connue sous le nom de protection contre les attaques par force brute) qui comptabilise le nombre de tentatives de connexion ratées.*

Si ce nombre atteint la valeur préconfigurée de 10 saisies de mot de passe erroné, le comportement sera le suivant :

Admin/Utilisateur activé	Protection contre les attaques par force brute - Comportement de la clé USB (10 tentatives de saisie de mot de passe infructueuses)	Suppression des données et réinitialisation de la clé USB ?
Mot de passe Utilisateur	Verrouillage du mot de passe. Se connecter en tant qu'Admin pour réinitialiser le mot de passe Utilisateur	NON
Mot de passe Admin	Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimés définitivement	OUI
Utilisateur uniquement Un seul utilisateur, un seul mot de passe (Admin/Utilisateur <u>NON</u> activé)	Protection contre les attaques par force brute - Comportement de la clé USB (10 tentatives de saisie de mot de passe infructueuses)	Suppression des données et réinitialisation de la clé USB ?
Mot de passe Utilisateur	Effacement chiffré du mot de passe ; mots de passe, paramètres et données supprimés définitivement	OUI

* Une fois que vous vous êtes authentifié avec succès sur la clé USB, le compteur d'échecs de connexion sera réinitialisé en fonction de la méthode de connexion utilisée. L'effacement chiffré effacera tous les mots de passe, les clés de chiffrement et les données ; **vos données seront perdues définitivement.**

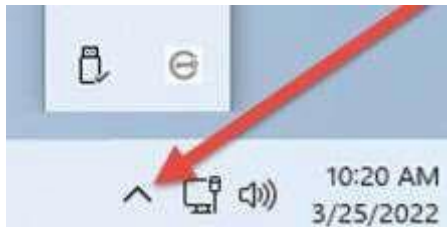
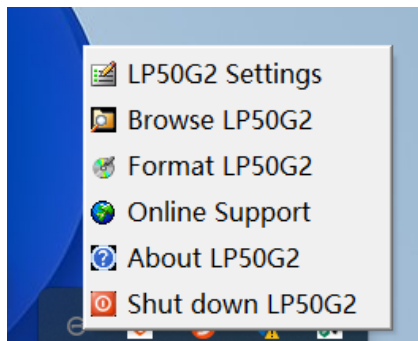
Accès à mes fichiers sécurisés

Après avoir déverrouillé la clé USB, vous pouvez accéder à vos fichiers sécurisés. Les fichiers sont automatiquement chiffrés et déchiffrés lorsque vous les enregistrez ou les ouvrez sur la clé USB. Cette technologie vous permet de travailler comme vous le feriez avec un lecteur ordinaire, tout en offrant une sécurité élevée et permanente.

Conseil : vous pouvez également accéder à vos fichiers en cliquant avec le bouton droit sur l'**icône IronKey** dans la barre des tâches de Windows, puis en cliquant sur **Parcourir LP50G2** (Figure 7.2)

Options de la clé USB (environnement Windows)

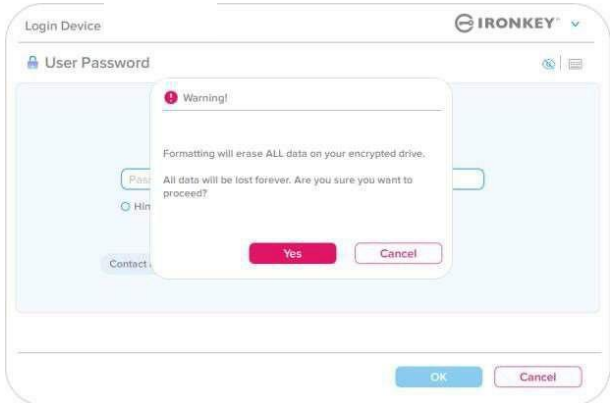
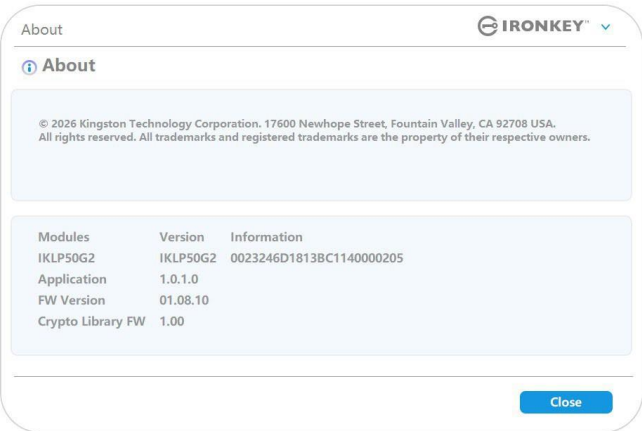
Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles (*Figure 6.2*). Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.

Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. (<i>Figure 7.1</i>)	 Figure 7.1 – Icône IronKey dans la barre des tâches
Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles. (<i>Figure 7.2</i>) Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.	 Figure 7.2 – Clic droit sur l'icône IronKey pour accéder aux options de la clé USB

Options de la clé USB (environnement macOS)

Lorsque vous êtes connecté à la clé USB, une icône « IronKey LP50G2 » se trouve dans le menu macOS illustré dans la Figure 7.3 ; elle permet d'afficher ses options disponibles. Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.	 Figure 7.3 – Icône de la barre de menu macOS/menu des options de la clé USB
---	--

Options de la clé USB

LP50G2 Settings (Paramètres de la LP50G2) :	Permet de modifier le mot de passe de connexion, les informations de contact et d'autres paramètres. (Vous trouverez plus de détails sur les paramètres de la clé USB dans la section « Paramètres de la LP50G2 » du présent manuel).
Browse LP50G2 (Parcourir la LP50G2) :	Permet de visualiser vos fichiers sécurisés.
Format LP50G2 (Formater la LP50G2) : permet de formater la partition de données sécurisée. (Avertissement : toutes les données seront détruites). (Figure 6.1) Remarque : l'authentification par mot de passe sera requise pour le formatage.	 Figure 7.4 – Formater la LP50G2
Online Support (Support en ligne) :	Cette fonction ouvre votre navigateur Internet et affiche la page http://www.kingston.com/support pour vous permettre de consulter les informations supplémentaires du support.
About LP50G2 (À propos de la LP50G2) : affiche des données détaillées sur la LP50G2, notamment des informations sur l'application, le firmware et le numéro de série (Figure 6.2). Remarque : le numéro de série unique de la clé USB se trouve sous la colonne « Informations ».	 Figure 7.5 – À propos de la LP50G2
Shut down LP50G2 (Arrêter la LP50G2) :	Permet de fermer correctement et en toute sécurité la LP50G2 avant de la déconnecter physiquement du système.

Paramètres de la LP50G2

Paramètres Admin

La connexion Admin permet d'accéder aux paramètres suivants de la clé USB :

- **Password** (Mot de passe) : permet de modifier le mot de passe Admin et/ou l'indice (*Figure 8.1*)
- **Contact Info** (Informations de contact) : permet d'ajouter/d'afficher/de modifier vos informations de contact (*Figure 8.2*)
- **Language** (Langue) : permet de modifier la langue actuelle (*Figure 8.3*)
- **Admin Options** (Options Admin) : permet d'accéder à des fonctionnalités supplémentaires telles que :
 - Changing the User Password (Modification du mot de passe Utilisateur) (*Figure 8.4*)

REMARQUE : des détails supplémentaires sur les options Admin sont indiqués à la page 25.

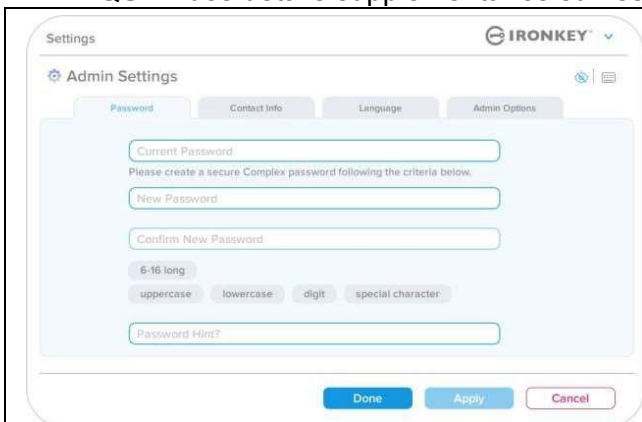


Figure 8.1 – Options du mot de passe Admin

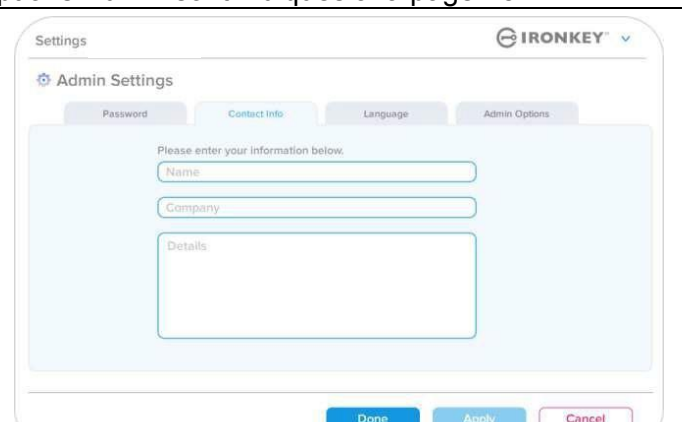


Figure 8.2 – Informations de contact

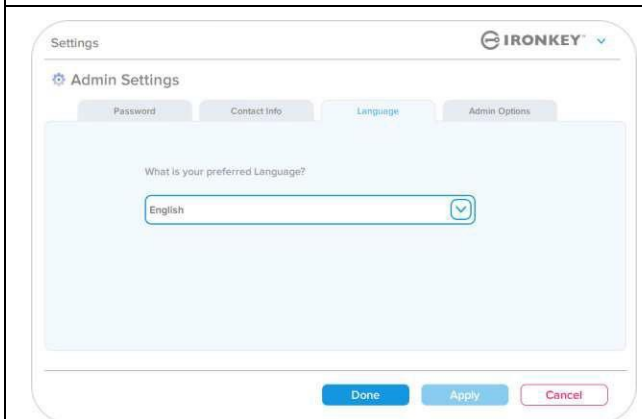


Figure 8.3 – Options de langue

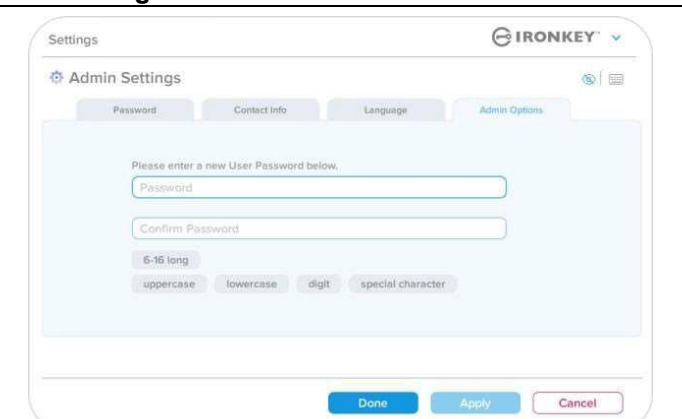


Figure 8.4 – Options Admin

Paramètres de la LP50G2

Paramètres utilisateur : Admin activé

La connexion Utilisateur limite l'accès aux paramètres suivants :

Password (Mot de passe) :

permet de modifier le mot de passe Utilisateur et/ou l'indice.

(Figure 8.5)

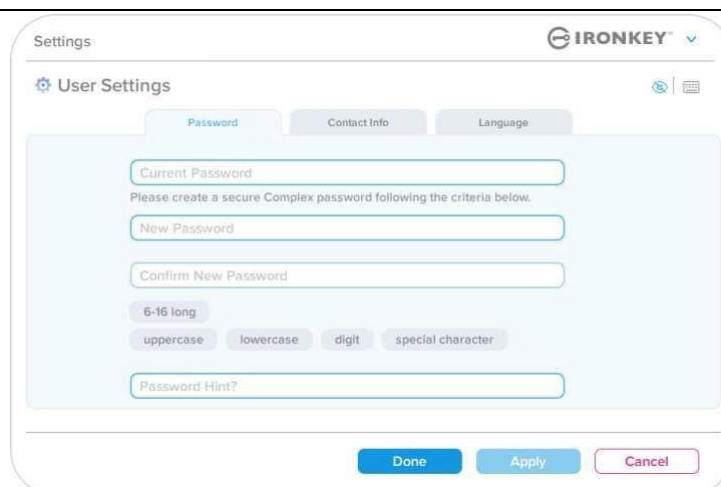


Figure 8.5 – Options de mot de passe (Admin activé : connexion Utilisateur)

Contact Info (Informations de contact) :

permet d'ajouter/d'afficher/de modifier les informations de contact.

(Figure 8.6)

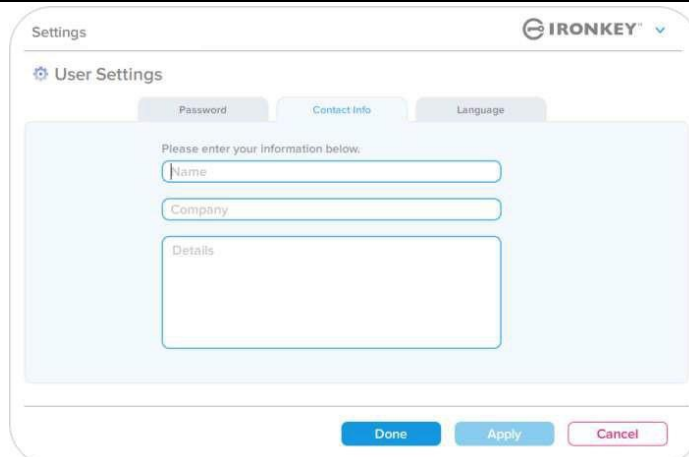


Figure 8.6 – Informations de contact (Admin activé : connexion Utilisateur)

Language (Langue) :

permet de modifier votre sélection de langue actuelle.

(Figure 8.7)

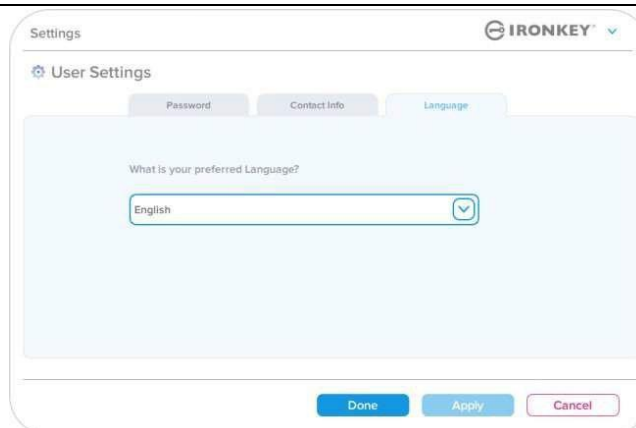


Figure 8.7 – Paramètres de langue (Admin activé : connexion Utilisateur)

Remarque : les options Admin ne sont pas accessibles lorsque la connexion est établie à l'aide du mot de passe Utilisateur.

Paramètres de la LP50G2

Paramètres utilisateur : Admin non activé

Comme mentionné précédemment à la page 12, l'initialisation de la LP50G2 sans activer les mots de passe « Admin et Utilisateur » configurera la clé USB dans une **configuration Mot de passe unique, Utilisateur unique**. Cette configuration n'a pas accès aux options ou fonctionnalités Admin. Cette configuration aura accès aux paramètres suivants de la LP50G2 :

Password (Mot de passe) :
permet de modifier le mot de passe Utilisateur et/ou l'indice.
(Figure 8.8)

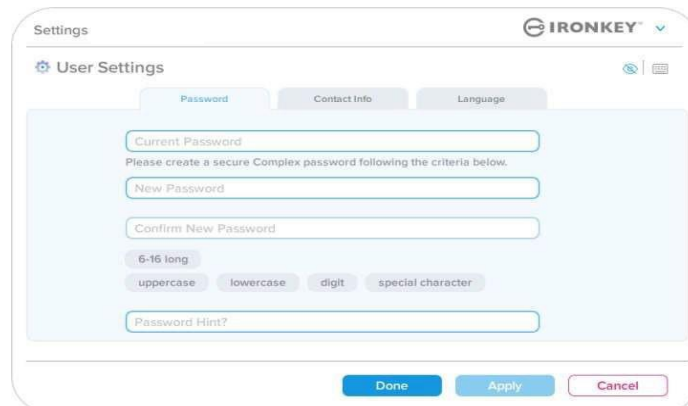


Figure 8.8 – Options de mot de passe (mode Utilisateur uniquement)

Contact Info (Informations de contact) :
permet d'ajouter/d'afficher/de modifier les informations de contact.
(Figure 8.9)

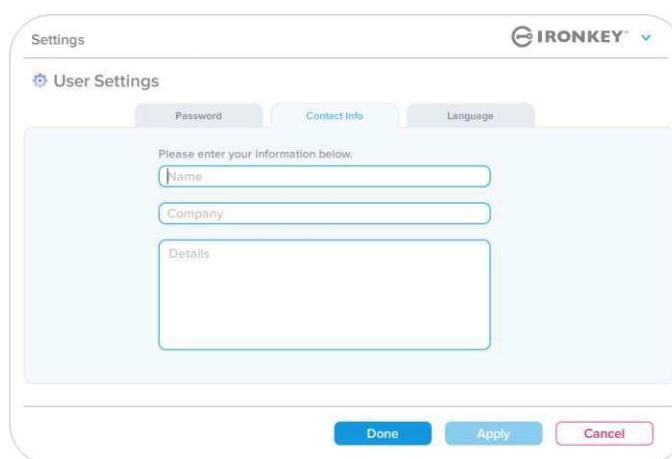


Figure 8.9 – Informations de contact (mode Utilisateur uniquement)

Language (Langue) :
permet de modifier votre sélection de langue actuelle.
(Figure 8.10)

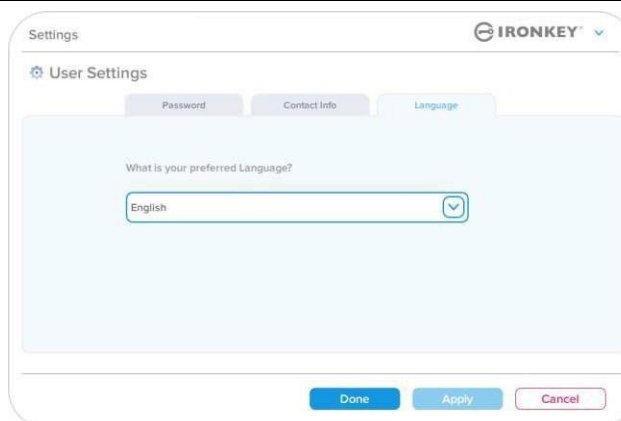


Figure 8.10 – Paramètres de langue (mode Utilisateur uniquement)

Paramètres de la LP50G2

Modifier et sauvegarder les paramètres

- Chaque fois que vous modifiez les paramètres de la LP50G2 (par exemple : coordonnées, langue, modification du mot de passe, options Admin, etc.), elle vous invitera à saisir votre mot de passe afin d'accepter et d'appliquer ces modifications.
(Figure 8.11)

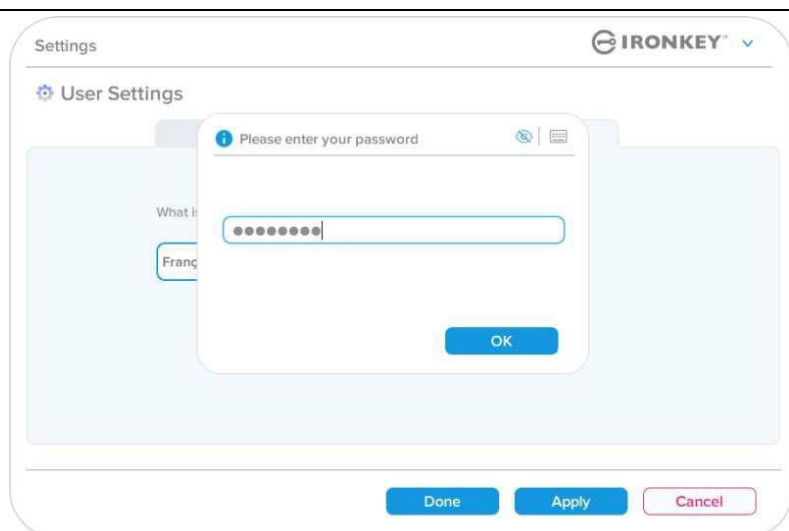


Figure 8.11 – Écran d'invite du mot de passe pour sauvegarder les modifications des paramètres de la LP50G2

Remarque : si vous êtes sur l'écran d'invite du mot de passe ci-dessus et que vous souhaitez annuler ou modifier vos modifications, vous pouvez le faire en vous assurant simplement que le champ du mot de passe est vide et en cliquant sur « OK ». Cela fermera la boîte de dialogue « Please enter your password » (Veuillez saisir votre mot de passe) et vous ramènera au menu des paramètres de la LP50G2.

Fonctionnalités Admin

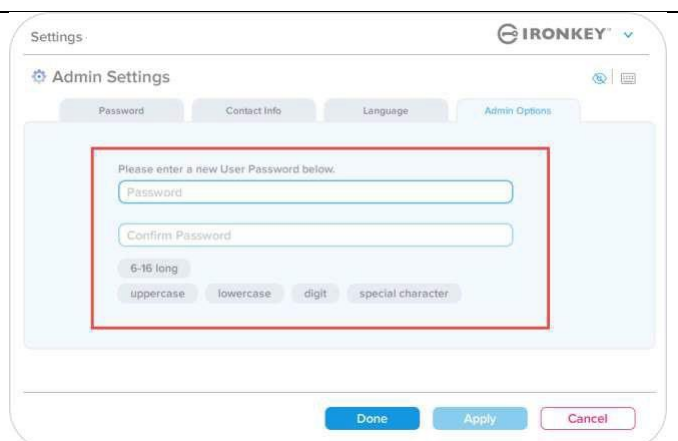
Option disponible pour réinitialiser le mot de passe Utilisateur

L'une des fonctionnalités utiles de la configuration Admin vous permet de réinitialiser en toute sécurité le mot de passe Utilisateur, en cas d'oubli. Vous trouverez ci-dessous la fonctionnalité de réinitialisation du mot de passe Utilisateur :

User Password Reset (Réinitialisation du mot de passe Utilisateur) :

permet de modifier manuellement le mot de passe Utilisateur dans le menu « Admin Options » (Options Admin). Cette modification est instantanée ; elle prendra effet à la prochaine connexion de l'Utilisateur. (Figure 9.1)

Remarque : les critères de mot de passe seront par défaut les critères originaux qui ont été définis pendant le processus d'initialisation (options Complexe ou Phrase de passe).



The screenshot shows the 'Settings' screen of the IronKey management interface. Under the 'Admin Settings' section, the 'Admin Options' tab is selected. Within this tab, the 'Password' sub-tab is active. A red rectangular box highlights the 'Please enter a new User Password below:' section, which contains two input fields: 'Password' and 'Confirm Password'. Below these fields are four criteria buttons: '6-16 long', 'uppercase', 'lowercase', 'digit', and 'special character'. At the bottom of the screen, there are three buttons: 'Done', 'Apply', and 'Cancel'.

Figure 9.1 – Options Admin/réinitialisation du mot de passe Utilisateur

Aide et dépannage

Verrouillage de la clé USB

La LP50G2 comprend une fonctionnalité de sécurité qui empêche tout accès non autorisé à la partition de données après un certain nombre maximum de tentatives de connexion infructueuses **consécutives** (« MAX » pour faire court). Par défaut, ce nombre de tentatives infructueuses est de 10 pour chaque méthode de connexion (Admin/Utilisateur).

Le compteur de tentatives enregistre chaque échec de connexion. Il est remis à zéro **de deux** façons :

1. Une connexion réussie avant d'atteindre le MAX.
2. Atteindre le MAX et effectuer un verrouillage ou un formatage de la clé USB, selon sa configuration.

- Si un mot de passe incorrect est saisi, un message d'erreur s'affiche en rouge juste au-dessus du champ de saisie du mot de passe, indiquant un échec de connexion.
(Figure 10.1)

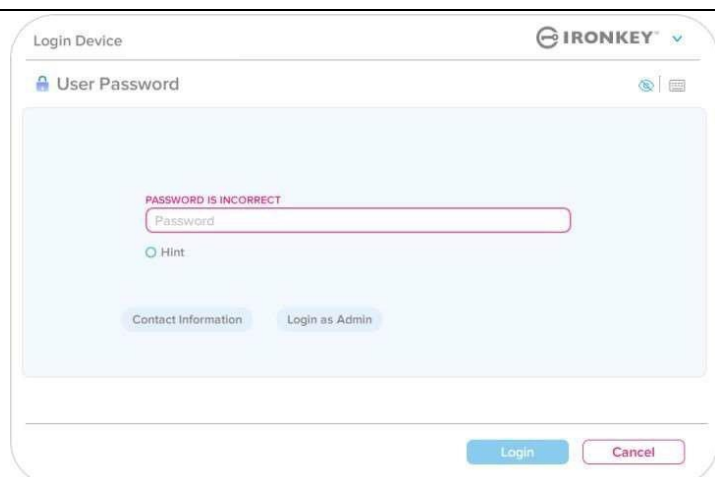


Figure 10.1 – Message Mot de passe incorrect

- Après la 7^{ème} tentative erronée consécutive, un message d'erreur supplémentaire avertit l'utilisateur qu'il lui reste trois tentatives avant d'atteindre la limite MAX (par défaut, 10 tentatives).
(Figure 10.2)

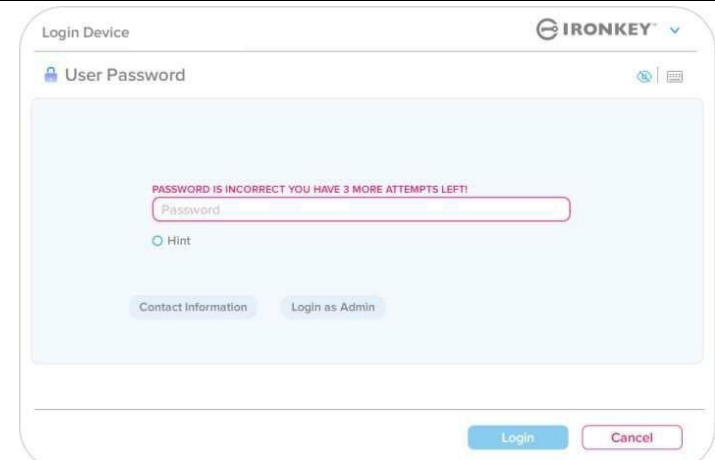


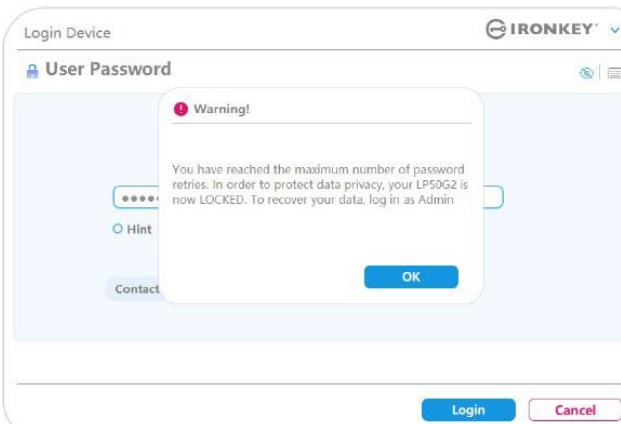
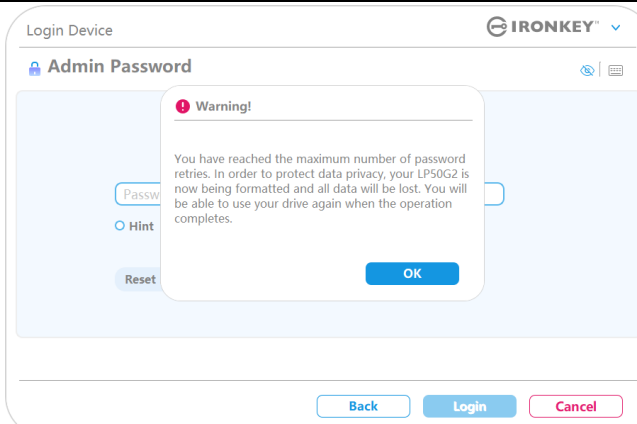
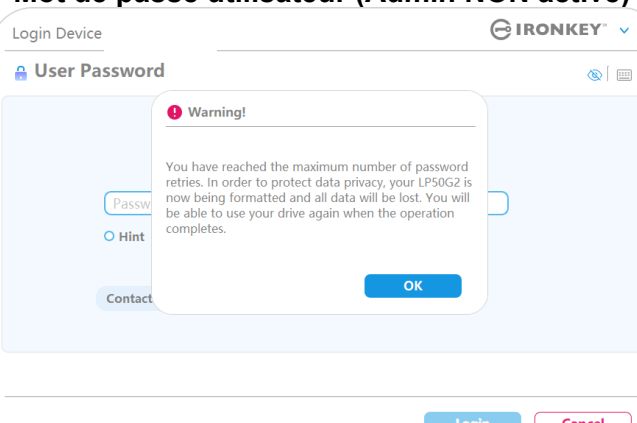
Figure 10.2 – 7^{ème} tentative de connexion infructueuse

Aide et dépannage

Verrouillage de la clé USB

Important : après la 10^{ème} et dernière tentative de connexion infructueuse, selon la configuration de la clé USB et la méthode de connexion utilisée (Admin/Utilisateur), la clé se verrouillera, ce qui vous obligera à vous connecter avec une autre méthode (le cas échéant), ou à effectuer une réinitialisation de la clé, ce qui **formatera les données, lesquelles seront définitivement perdues**. Comportements également mentionnés à la page 17 de ce Guide de l'utilisateur.

Les figures 10.3 à 10.6 ci-dessous illustrent le comportement visuel pour la 10^{ème} et dernière tentative de connexion infructueuse pour chaque méthode de mot de passe de connexion :

<u>Mot de passe Utilisateur : (Admin/Utilisateur activé)</u>  VERROUILLAGE DE LA CLÉ USB Figure 10.3	<u>Mot de passe Admin (Admin/Utilisateur activé)</u>  FORMATAGE DE LA CLÉ USB* Figure 10.4
Ces mesures de sécurité empêchent qu'une autre personne (qui n'a pas votre mot de passe) puisse effectuer d'innombrables tentatives de connexion et d'accéder à vos données sensibles (également connu sous le nom d'attaque par force brute). Si vous êtes le propriétaire de la LP50G2 et que vous avez oublié votre mot de passe, cette mesure de sécurité sera également appliquée et aboutira au formatage de la clé USB.* Pour en savoir plus sur cette fonctionnalité, voir la section « Réinitialiser la clé USB » à la page 27.	<u>Mot de passe utilisateur (Admin NON activé)</u>  FORMATAGE DE LA CLÉ USB* Figure 10.5

***Remarque :** le formatage supprimera TOUTES les informations stockées sur la partition de données sécurisée de la LP50G2.

Aide et dépannage

Réinitialiser la clé USB

Si vous oubliez votre mot de passe ou si vous devez réinitialiser votre clé USB, vous pouvez cliquer sur le bouton « *Reset Device* » (Réinitialiser la clé USB). Ce bouton peut apparaître à deux endroits selon la configuration de la clé USB au lancement du programme Launcher : dans le menu Admin Login Password (Mot de passe de connexion Admin) si le mode Admin/Utilisateur est activé, ou dans le menu de connexion « User Password » (Mot de passe Utilisateur) si le mode Admin/Utilisateur n'est pas activé (Figure 10.7 et Figure 10.8).

- Cette option vous permet de créer un nouveau mot de passe, mais pour protéger la confidentialité de vos données, la LP50G2 sera formatée. Par conséquent, ce processus effacera définitivement toutes vos données.*

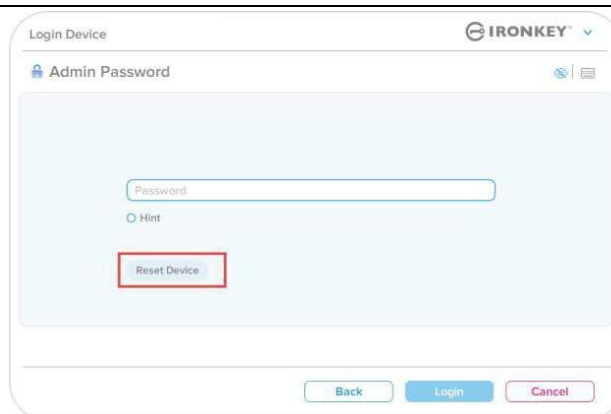


Figure 10.6 – Mot de passe Admin : bouton Reset Device (Réinitialiser la clé USB)

- **Remarque :** lorsque vous cliquez sur « *Reset Device* » (Réinitialiser la clé USB), un message vous demande si vous souhaitez saisir un nouveau mot de passe avant le lancement du formatage. Vous pouvez alors 1) cliquer sur « *OK* » pour confirmer, ou 2) cliquer sur « *Cancel* » (Annuler) pour revenir à la fenêtre de connexion. (Figure 10.8)

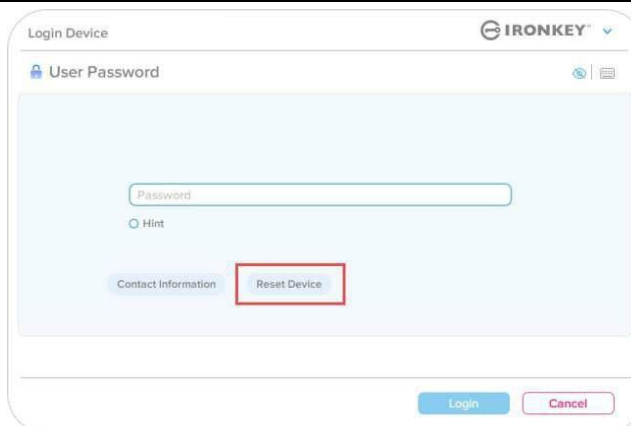


Figure 10.7 – Mot de passe Utilisateur (Admin/Utilisateur non activé) – Réinitialiser la clé USB

- Si vous choisissez de continuer, vous serez renvoyé à l'écran d'initialisation, où vous pouvez activer les modes Admin et Utilisateur et saisir votre nouveau mot de passe en fonction de l'option de mot de passe choisie (Complexe ou Phrase de passe). L'indice n'est pas obligatoire, mais il peut vous aider à vous souvenir du mot de passe si vous l'oubliez.

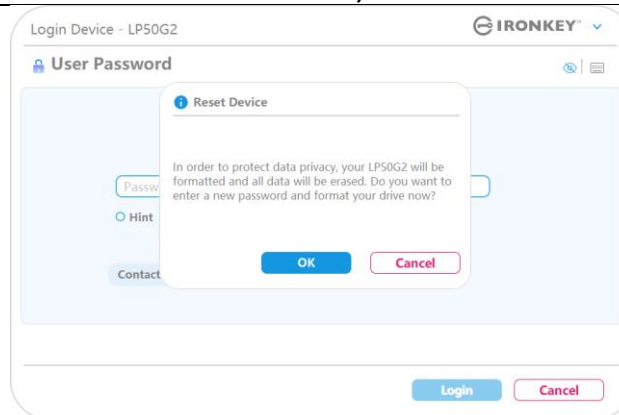


Figure 10.8 – Confirmation de réinitialisation de la clé USB

Conflit de lettres de lecteur : systèmes d'exploitation Windows

- Comme indiqué dans la section « *Configuration système requise* » du présent manuel (page 4), la LP50G2 a besoin de deux lettres de lecteur consécutives APRÈS le dernier disque physique qui apparaît avant l'« écart » dans les affectations de lettres de lecteur (*Figure 10.9*). Cette attribution NE DÉPEND PAS des partages de réseau parce que ces partages sont spécifiques aux profils d'utilisateur et pas au profil matériel du système. Une lettre attribuée à un volume du réseau peut donc apparaître comme disponible pour le système d'exploitation.
- Autrement dit, Windows peut attribuer à la LP50G2 une lettre de lecteur qui est déjà utilisée par un élément du réseau ou un chemin UNC (Universal Naming Convention), ce qui provoque un conflit de lettres de lecteur. Dans ce cas, veuillez consulter votre administrateur ou le service d'assistance pour modifier l'attribution des lettres de lecteur dans le gestionnaire des disques Windows Disk Management (les droits d'administrateur sont nécessaires).

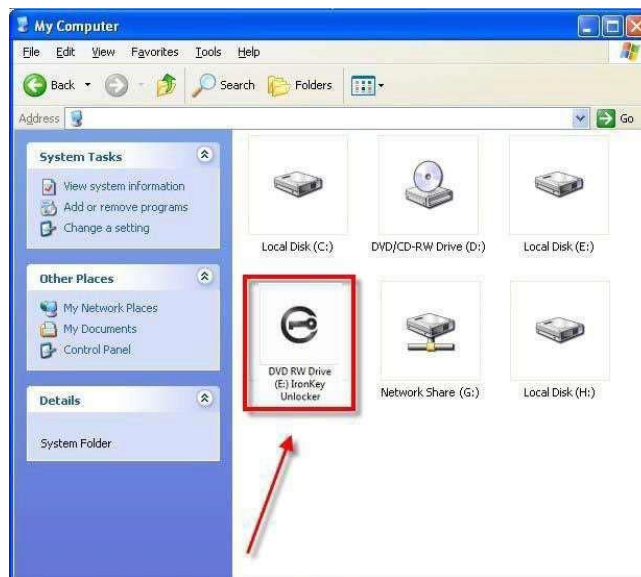


Figure 10.9 – Exemple de lettre de lecteur

Dans cet exemple (*Figure 10.9*), la LP50G2 utilise le lecteur F:, qui est la première lettre de lecteur disponible après le lecteur E: (qui est le dernier disque physique affiché avant l'écart dans l'attribution des lettres de lecteurs). Comme la lettre G: est un partage réseau et qu'elle ne fait pas partie du profil matériel, la LP50G2 peut tenter de l'utiliser comme deuxième lettre de lecteur, ce qui provoque un conflit.

Si vous n'avez aucun volume de réseau sur votre système et que la LP50G2 ne se charge toujours pas, il est possible qu'un lecteur de cartes, un disque amovible ou un autre périphérique précédemment installé conserve une lettre de lecteur attribuée et génère un conflit.

Précisons que la gestion des lettres de lecteur a été considérablement améliorée dans Windows 11, ce qui peut vous éviter ce problème. Toutefois, si vous ne parvenez pas à résoudre un conflit de lettres de lecteur, veuillez contacter le Support technique de Kingston ou consultez le site Kingston.com/support pour obtenir de l'aide.

DRIVE FLASH USB 3.2 Gen 1
SICURO IRONKEY™
Locker+ 50 G2 (LP50G2)

Guida per l'utente



Contenuti

Introduzione	3
Caratteristiche Locker+ 50 G2.....	4
Informazioni sulla guida	4
Requisiti di sistema	4
 Raccomandazioni	 5
Utilizzo del file system corretto	5
Note di utilizzo	5
Best practice per l'impostazione delle password	6
 Configurazione del dispositivo.....	 7
Accesso al dispositivo (Ambienti Windows).....	7
Accesso al dispositivo (Ambienti macOS)	7
 Inizializzazione del dispositivo (ambienti Windows e macOS).....	 8
Selezione della password	9
Tastiera virtuale	11
Pulsante di commutazione visualizzazione password	12
Password amministratore e utente	13
Informazioni di contatto.....	15
 Utilizzo del dispositivo (ambienti Windows e macOS)	 16
Accesso per amministratore e utente (modalità amministratore abilitata).....	16
Modalità di accesso per solo utente (modalità amministratore non abilitata)	16
Protezione contro gli attacchi brute-force	17
Accesso ai file sicuri	17
 Opzioni dispositivo.	 18
 Impostazioni LP50G2	 20
Impostazioni amministratore.....	20
Impostazioni utente: modalità amministratore abilitata.....	21
Impostazioni utente: modalità amministratore non abilitata.....	22
Modifica e salvataggio delle impostazioni LP50G2	23
 Funzionalità amministratore.....	 24
Reset della password utente	24
 Guida alla risoluzione dei problemi	 25
Blocco LP50G2.....	25
Reset dispositivo LP50G2	27
Conflitti con le lettere di unità: (Windows)	28



Figura 1: IronKey LP50G2

Introduzione

I drive flash USB Kingston IronKey™ Locker+ 50 G2 offrono sicurezza di classe enterprise con certificazione FIPS 197 e crittografia hardware AES a 256-bit in modalità XTS, comprese le protezioni contro attacchi BadUSB e contro gli attacchi con password Brute Force. LP50G2 è anche conforme allo standard TAA.

Il drive LP50G2 supporta un'opzione multi-password (amministratore e utente) con modalità complessa o frase password. La modalità complessa per le password supporta da 6 a 16 caratteri tramite l'utilizzo di 3 set di caratteri su 4. La nuova modalità frase password supporta un PIN numerico, una frase, un elenco di parole o persino testi composti da 10 a 64 caratteri. L'amministratore può abilitare una password utente oppure reimpostare la password utente per ripristinare l'accesso ai dati. Per inserire la password più facilmente, è possibile abilitare il simbolo dell'occhio in modo da visualizzare la password digitata, riducendo gli errori di battitura che portano a tentativi di accesso non riusciti. La protezione dagli attacchi Brute Force blocca le password utente dopo l'immissione di 10 password non valide consecutive ed esegue la cancellazione criptata del drive quando la password dell'amministratore viene inserita in modo errato per 10 volte di seguito. In più, una tastiera virtuale integrata protegge le password da keylogger o screenlogger.

Locker+ 50 G2 è progettato per garantire la massima praticità, con un piccolo involucro di metallo e un'asola di aggancio integrata per portare i dati ovunque.

Il drive LP50G2 è supportato da una garanzia limitata di 5 anni, con servizio di Supporto Tecnico Kingston gratuito.

Caratteristiche di IronKey Locker+ 50 G2

- Certificazione FIPS 197
- Crittografia hardware XTS-AES (la crittografia non può mai essere disattivata)
- Protezione contro gli attacchi brute force e BadUSB
- Funzione multi-password opzionale
- Modalità complessa o frase password
- Pulsante con il simbolo dell'occhio per visualizzare la password digitata ed evitare tentativi di accesso non riusciti
- Tastiera virtuale per maggiore protezione da keylogger e screenlogger durante l'inserimento della password
- Compatibile con Windows o macOS (consultare la scheda tecnica per i dettagli)

Informazioni sulla guida (02122026)

La presente guida contiene informazioni su IronKey Locker+ 50 G2 (LP50G2).

Requisiti di sistema

Piattaforma PC • Intel o AMD • 15MB di spazio libero su disco • Porta USB 2.0 / 3.2 disponibile • Due lettere di unità libere consecutive dopo quella associata all'ultimo drive fisico presente sull'unità* *Nota: vedere sezione “Conflitti con le lettere di unità”, a pagina 28.	Supporto per sistemi operativi per PC • Windows 11
Piattaforma Mac • SOC Apple o Intel • 15MB di spazio libero su disco • Porta USB 2.0/3.2	Supporto per sistemi operativi Mac • macOS 13.x – 26.x

Raccomandazioni

Per garantire una potenza adeguata al funzionamento del drive LP50G2, collegarlo direttamente a una porta USB sul computer notebook o desktop, come illustrato in *Figura 1.1*. Evitare di collegare il drive LP50G2 a qualunque tipo di periferica dotata di porta USB, come tastiere o hub USB, come illustrato in *Figura 1.2*.



Figura 1.1 – Metodi di collegamento raccomandati



Figura 1.2 – Metodi di collegamento sconsigliati

Utilizzo del file system corretto

Il drive IronKey LP50G2 viene fornito preformattato con il file system FAT32. Il drive è compatibile con i sistemi Windows e macOS. Tuttavia, vi potrebbero essere alcune altre opzioni che possono essere utilizzate per formattare il drive manualmente, come lo standard NTFS per Windows oppure exFAT. È possibile riformattare la partizione dati, se necessario; tuttavia, in questo caso tutti i dati andranno persi durante la formattazione del drive.

Note di utilizzo

Per proteggere i dati, Kingston consiglia di:

- Eseguire una scansione antivirus sul computer prima di configurare e utilizzare LP50G2 su un sistema di destinazione.
- Quando si utilizza il drive su un sistema di tipo pubblico o non conosciuto, potrebbe essere necessario impostare la modalità di sola lettura sul dispositivo al fine di proteggere il drive contro eventuali attacchi malware.
- Bloccare il dispositivo quando non in uso.
- Espellere in modo sicuro il dispositivo prima di disconnetterlo.
- Non scollegare mai il dispositivo quando il LED è acceso. Tale operazione potrebbe danneggiare il drive e richiedere una riformattazione che cancellerà tutti i dati.
- Non condividere mai la password del dispositivo.

Ricerca di aggiornamenti e informazioni più recenti

Per ottenere gli ultimi aggiornamenti sulle unità e consultare le domande frequenti, la documentazione e ulteriori informazioni, visitare il sito kingston.com/support.

NOTA: al drive vanno applicati sempre e solo gli aggiornamenti più recenti (non appena divengono disponibili) Il downgrade del drive a una versione software precedente non è supportato. Tale operazione può causare potenziali perdite di dati o influenzare negativamente altre funzioni del drive. Per eventuali dubbi o problemi, contattare il supporto tecnico Kingston.

Best practice per l'impostazione delle password

Il drive LP50G2 è dotato di solide misure di sicurezza. Tra queste, vi è la protezione contro gli attacchi Brute Force che impediranno a un malintenzionato di indovinare le password limitando ogni fase di inserimento della password a 10 tentativi. Quando viene raggiunto questo limite, il drive LP50G2 cancellerà automaticamente i dati crittografati, formattandosi e riportandosi alle impostazioni di fabbrica.

Supporto per password multiple

Il drive LP50G2 supporta la funzione multi-password, una caratteristica chiave per la protezione contro la perdita di dati in caso di smarrimento di una o più password. Quando tutte le opzioni di inserimento password sono abilitate, l'unità LP50G2 è in grado di supportare due password utente differenti che possono essere utilizzate per recuperare i dati: password Amministratore (Admin) e password utente (User).

Il drive LP50G2 consente all'utente di selezionare due password principali: una password amministratore (che di seguito chiameremo "password Admin") e una password Utente. L'account Admin può accedere al drive in qualunque momento e impostare le opzioni per Utente e Admin come se fosse un Super User.

L'account Utente può accedere al drive come l'Admin, ma al contrario di quest'ultimo, l'account Utente ha meno privilegi di accesso. Se una delle password viene dimenticata, è possibile utilizzare l'altra password per accedere e recuperare i dati. Il drive può essere quindi reimpostato con due password. È estremamente importante impostare ENTRAMBE le password e salvare la password Admin in un luogo sicuro, quando si utilizza la password Utente.

Se si dimenticano o si perdono entrambe le password, non sarà possibile accedere ai dati in alcun modo. Kingston non sarà in grado di recuperare i dati in quanto le funzioni di sicurezza non consentono alcun accesso secondario. Pertanto, Kingston raccomanda di salvare i dati anche su altri supporti. Il drive LP50G2 può essere reimpostato e riutilizzato, ma in tal caso tutti i dati in esso contenuti saranno eliminati definitivamente.

Modalità password

Il drive LP50G2 supporta due diverse modalità password.

Password complessa

Una password complessa deve contenere almeno 6-16 caratteri e utilizzare almeno 3 dei seguenti caratteri:

- Caratteri alfabetici maiuscoli
- Caratteri alfabetici minuscoli
- Numeri
- Caratteri speciali

Frase-password

Il drive LP50G2 supporta frasi password composte da 10 fino a 64 caratteri. Una frase password non segue regole aggiuntive, ma se utilizzata correttamente può fornire livelli molto elevati di protezione della password.

Si tratta sostanzialmente di una combinazione qualsiasi di caratteri, compresi quelli di altre lingue. La lingua utilizzata per la password può essere anche corrispondente alla lingua selezionata per il drive LP50G2. È possibile scegliere di impostare parole multiple, una frase, il testo di una canzone, la strofa di una poesia, ecc. Una buona frase password è difficile da indovinare per gli hacker e facile da ricordare per gli utenti.

Configurazione del dispositivo

Al fine di garantire un'adeguata potenza di alimentazione per il drive USB crittografato IronKey, inserirlo direttamente in una porta USB 2.0/3.0 su un computer notebook o desktop. Evitare di collegare l'unità a periferiche dotate di porte USB, come tastiere o hub USB. La configurazione iniziale del dispositivo deve essere effettuata su un sistema operativo Windows o macOS di tipo supportato.

Accesso al dispositivo (Ambienti Windows)

Collegare il drive USB crittografato IronKey in una delle porte USB disponibili sul notebook o sul PC desktop e attendere che Windows rilevi il dispositivo.

- Gli utenti di Windows riceveranno una notifica relativa all'installazione del driver. (Figura 3.1)

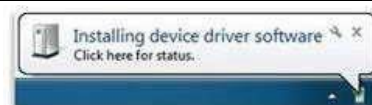


Figura 3.1 – Notifica di installazione del driver del dispositivo

- Una volta completato il rilevamento del nuovo hardware, selezionare l'opzione **IronKey.exe** dalla partizione dell'IronKey Unlocker, visualizzabile in Esplora risorse. (Figura 3.2)
- Si noti che la lettera di partizione varia, assumendo la denominazione della prima lettera di unità libera. La lettera di unità può variare in base al tipo di dispositivo connesso. Nell'immagine a destra, la lettera dell'unità è (E:).



Figura 3.2: Finestra Esplora file/IronKey.exe

Accesso al dispositivo (Ambienti macOS)

Inserire il drive LP50G2 in una delle porte USB disponibili sul computer notebook o desktop in uso e attendere il rilevamento da parte del sistema operativo Mac. Una volta che il drive viene rilevato, sul desktop del computer Mac in uso verrà visualizzata l'icona del volume IRONKEY. (Figura 3.3)

- Fare doppio clic sull'icona del CD-ROM dell'unità IronKey.
- Quindi, fare doppio clic sull'icona IronKey.app, visualizzata nella finestra raffigurata in Figura 3.3. Verrà avviata la procedura di inizializzazione.

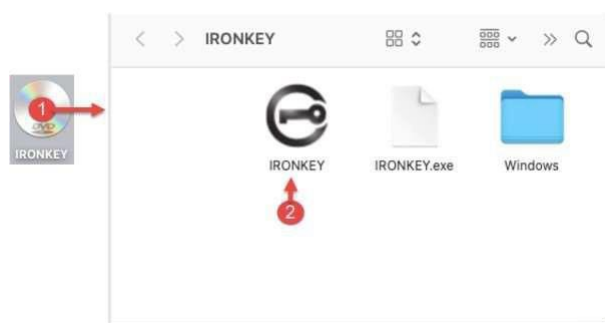


Figura 3.3 – Volume IRONKEY

Inizializzazione del dispositivo (ambienti Windows e macOS)

Lingua e EULA

Selezionare la lingua preferita dal menu a discesa e fare clic sulla voce **Successivo**. (Vedere Figura 4.1)

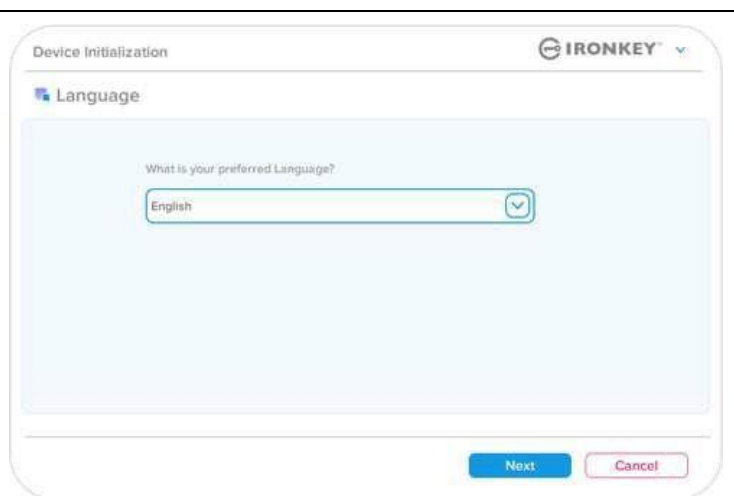


Figura 4.1 – Selezione della lingua

Leggere l'accordo di licenza e quindi fare clic su **Successivo**.

Nota: è necessario accettare l'accordo di licenza prima di proseguire; in caso contrario il pulsante **Successivo** resterà disabilitato. (Figura 4.2)

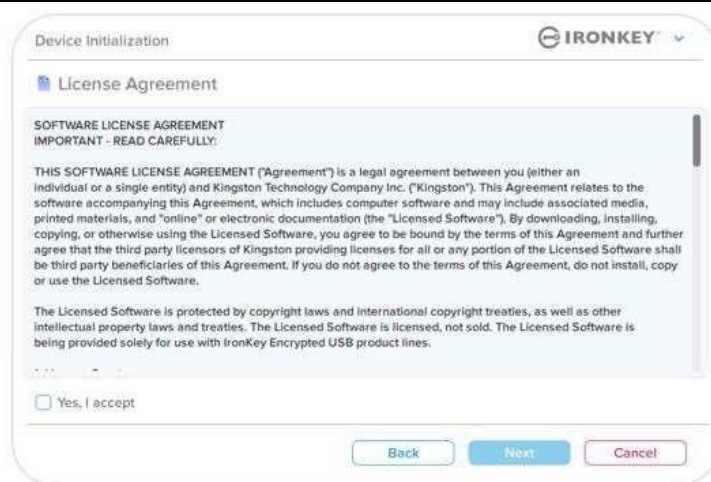


Figura 4.2 – Accordo di licenza

Inizializzazione del dispositivo

Selezione della password

Nella schermata di richiesta della password, è possibile creare una password per proteggere i dati contenuti questa schermata è possibile abilitare anche le opzioni Multi-password Admin/User (Amministrazione/Utente con password multiple). Prima di procedere con la selezione della password, consultare la sezione Abilitazione delle password amministratore/utente riportata di seguito per comprendere meglio queste funzionalità.

Nota: una volta selezionata la modalità password complessa o frase password, tale modalità non può essere modificata a meno che il dispositivo non venga resettato. Il primo passo consiste nel digitare la password nel campo "Password" per poi reinserirla nel campo "Conferma password". Affinché sia possibile proseguire la procedura di inizializzazione, è necessario creare una password avente i seguenti requisiti:

Password complessa

- Deve essere composta da un minimo di 6 fino a un massimo di 16 caratteri.
- Deve contenere tre (3) dei seguenti requisiti:
 - Lettere maiuscole
 - Lettere minuscole
 - Numeri
 - Caratteri speciali (!,\$,&, ecc..)

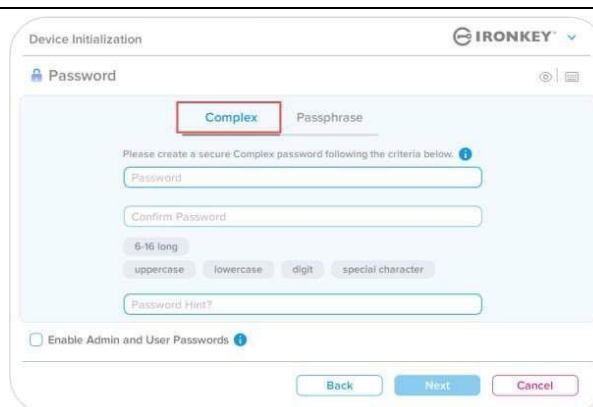


Figura 4.3 – Password complesse

Frase password

- Devono contenere:
 - Minimo 10 caratteri
 - Massimo 64 caratteri

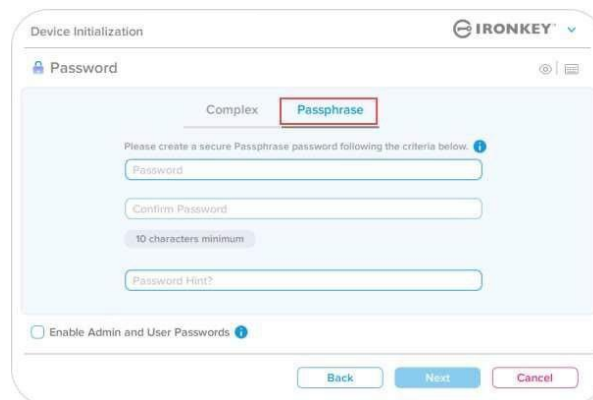


Figura 4.4 – Frasi password

Suggerimento password (opzionale)

Un suggerimento può rivelarsi utile per aiutare l'utente a ricordare la password, qualora questa vada persa o dimenticata

Nota: il suggerimento NON DEVE corrispondere alla stessa password utilizzata per l'accesso.

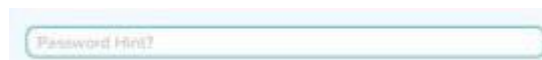
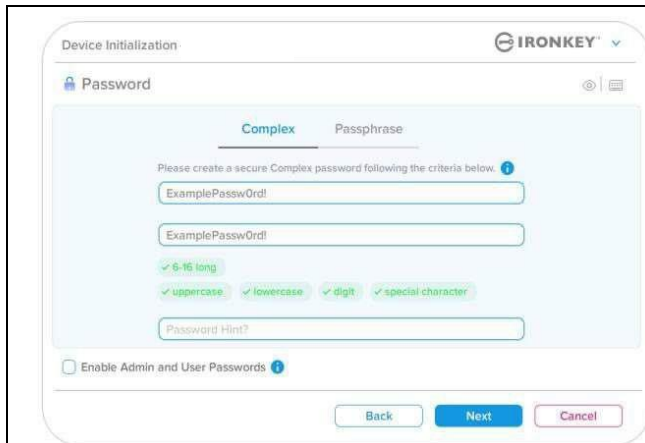


Figura 4.5 – Campo suggerimento password

Inizializzazione del dispositivo

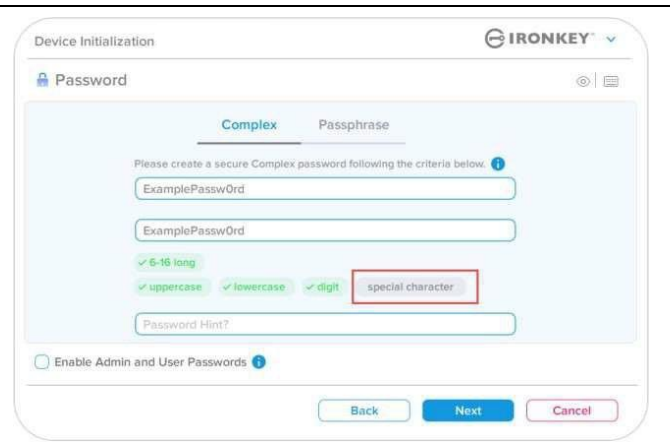
Password valide e non valide

Nel caso delle password **valide**, il campo dei criteri password si illumina di colore **verde** quando vengono rispettati i criteri di inserimento corretti. (Vedere *Figure 4.6a-b*) nota: Una volta soddisfatti i tre criteri minimi relativi alla password, la casella del quarto criterio diventerà grigia, indicando che tale criterio è facoltativo (*Figura 4.6b*)



The screenshot shows the 'Device Initialization' window with the 'Password' tab selected. Under the 'Complex' sub-tab, there are two password input fields, both containing 'ExamplePasswOrd!'. Below the fields, four criteria are listed with green checkmarks: '6-16 long', 'uppercase', 'lowercase', and 'digit'. The 'special character' criterion is also listed but is currently greyed out. At the bottom, there is a 'Password Hint?' field and an unchecked checkbox for 'Enable Admin and User Passwords'.

Figura 4.6a – Requisiti di inserimento della password complessa rispettati

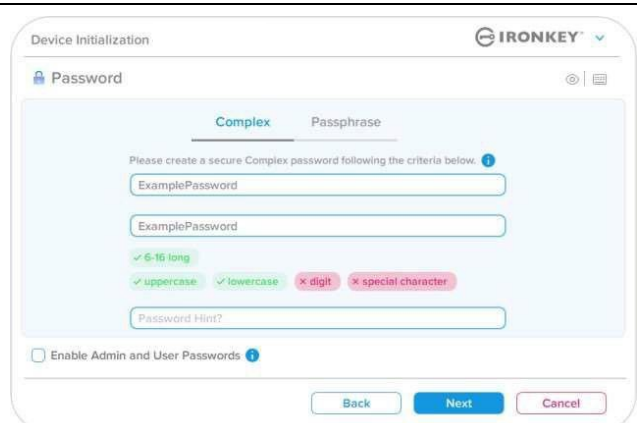


This screenshot is similar to Figure 4.6a, but the 'special character' criterion is now highlighted with a red box, indicating it is an optional requirement that can be satisfied to proceed.

Figura 4.6b – Condizione password complessa facoltativa

Nel caso di password **invalida**, il campo dei criteri password si illumina di colore **rosso** e il pulsante **Successivo** rimarrà disabilitato fino al raggiungimento dei requisiti minimi.

Questo vale sia per le password complesse che per quelle con frase password.



The screenshot shows the 'Device Initialization' window with the 'Password' tab selected. Under the 'Complex' sub-tab, the two password input fields now contain 'ExamplePassword'. The criteria below show '6-16 long' and 'uppercase' with green checkmarks, while 'lowercase', 'digit', and 'special character' are marked with red 'x' icons, indicating they are not met.

Figura 4.7 – Requisiti password non rispettati

Inizializzazione del dispositivo

Tastiera virtuale

Il drive LP50G2 è dotato di una tastiera virtuale che può essere utilizzata per la protezione da keylogger.

- Per utilizzare la **Tastiera virtuale**, individuare il pulsante della tastiera nella parte superiore destra della schermata **Inizializzazione dispositivo** e selezionarlo.

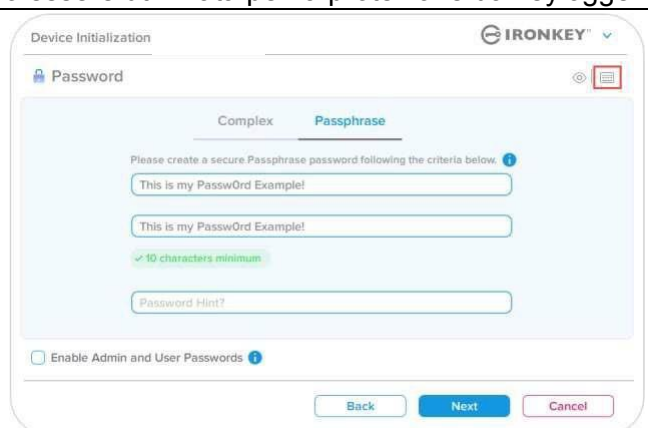


Figura 4.8 – Attivazione della tastiera virtuale

- Una volta visualizzata la tastiera virtuale, è anche possibile abilitare la **protezione Screenlogger**. Quando si utilizza questa funzione, tutti i tasti rimarranno vuoti per un breve periodo. Questo è un comportamento previsto, poiché impedisce agli screenlogger di vedere ciò che viene cliccato.
- Per rendere questa funzione più robusta, è anche possibile scegliere di randomizzare la tastiera virtuale selezionando **randomize** (rendere casuale) nella parte inferiore destra della tastiera. La funzione Randomize (Layout casuale) dispone i tasti in ordine casuale.

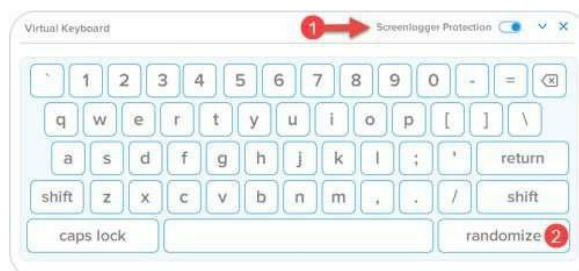


Figura 4.9 – Protezione Screenlogger / Randomizza

Inizializzazione del dispositivo

Pulsante di commutazione visualizzazione password

Per impostazione predefinita, quando si crea una password, i caratteri che compongono la password sono visibili nel relativo campo mentre vengono digitati. Se si desidera "nascondere" la stringa della password durante la digitazione, è possibile farlo usando l'icona "occhio" situata nella parte superiore destra della finestra di inizializzazione del dispositivo.

Nota: dopo l'inizializzazione del dispositivo, il campo della password sarà impostato di default su "nascosto".

Per **nascondere** la stringa della password, fare clic sull'icona grigia.

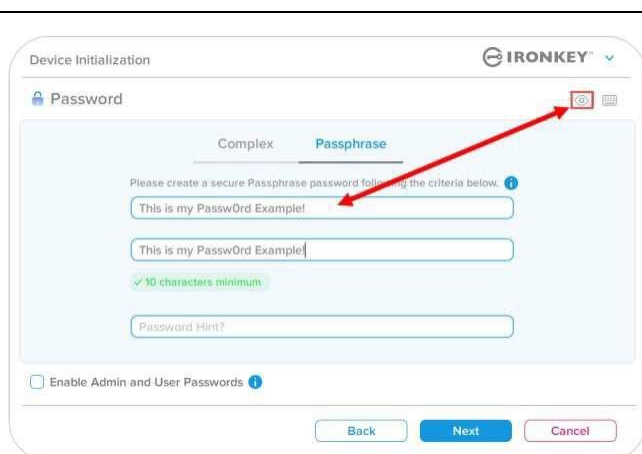


Figura 4.10 – Pulsante per "nascondere" la password

Per **visualizzare** la password nascosta, fare clic sull'icona blu.

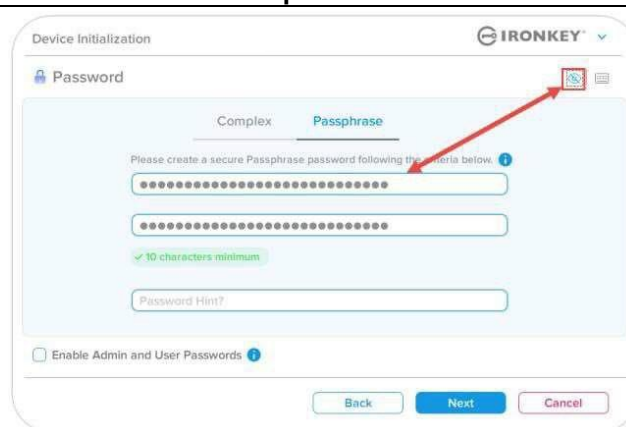


Figura 4.11 – Pulsante per "visualizzare" la password

Inizializzazione del dispositivo

Password amministratore e utente

Abilitando le password amministratore e utente, è possibile sfruttare la funzionalità multi-password, che permette al ruolo amministratore di gestire entrambi gli account. Selezionando **"Abilita password amministratore e utente"** è possibile accedere all'unità in modo alternativo nel caso in cui si dimentichi una delle password.

Dopo aver abilitato le **Password amministratore e utente**, è inoltre possibile accedere alla funzione:

- Reset della password utente

Per ulteriori informazioni sulla funzione di reimpostazione della password utente, consultare la pagina 24 della presente guida utente.

- Per abilitare le **password amministratore e utente** fare clic sulla casella accanto a **"Abilita password amministratore e utente"** e selezionare **Successivo** dopo aver scelto una password valida. (Figura 4.12)
- Se questa funzione è **abilitata**, la password scelta in questa schermata sarà la **password amministratore**. Fare clic su **Successivo** per passare alla schermata **Password utente** in cui sarà possibile scegliere una password per l'utente.

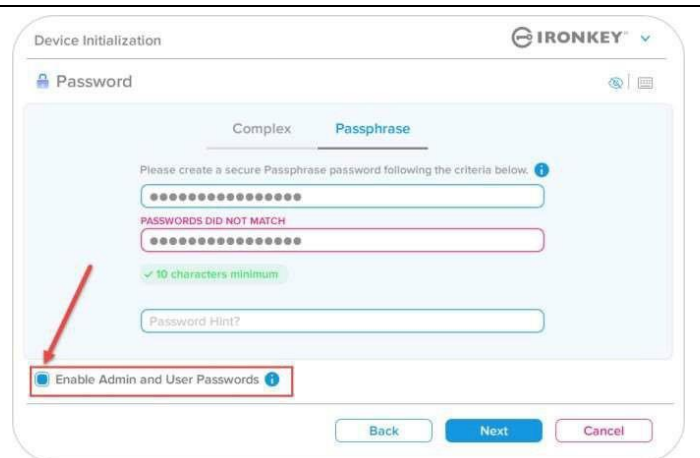


Figura 4.12 – Attivazione delle password amministratore e utente

Nota: l'attivazione di password amministratore e utente è facoltativa.

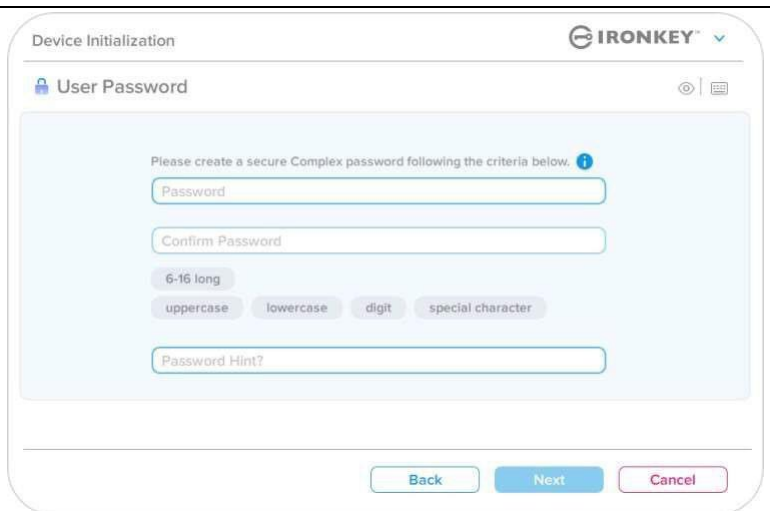
Se l'unità è configurata con questa funzione NON abilitata (casella deselezionata), l'unità sarà configurata come unità **Utente singolo**, **Password singola senza alcuna funzione di amministrazione**. Nella presente guida, a questa configurazione viene fatto riferimento con la denominazione **Modalità solo utente**.

Per procedere con la configurazione di un utente singolo e una password singola, lasciare deselezionata l'opzione **Abilita password amministratore e utente** e fare clic su **Successivo** dopo aver creato una password valida.

Inizializzazione del dispositivo

Password amministratore e utente

Se nella schermata precedente è stato **abilitato** il ruolo di amministratore, la schermata seguente richiederà di immettere la **password utente** (Figura 4.13). La password utente avrà funzionalità limitate rispetto a quella amministratore e verrà dettagliatamente spiegata nel prosieguo di questa guida. **Nota:** nella restante sezione di questo manuale, la funzione **Password amministratore e utente** sarà denominata "**Ruolo amministratore**".



The screenshot shows the 'Device Initialization' screen with the 'User Password' section active. It prompts the user to 'Please create a secure Complex password following the criteria below.' The criteria listed are: 6-16 long, uppercase, lowercase, digit, and special character. There are input fields for 'Password', 'Confirm Password', and 'Password Hint?'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Figura 4.13 – Password utente (con amministratore e utente attivi)

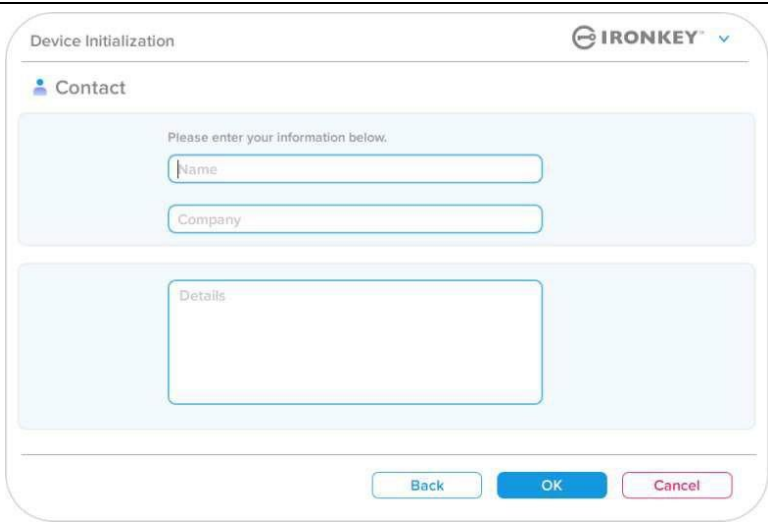
Nota: i criteri scelti per l'opzione Password (Complessa o Passphrase) verranno applicati alla password utente e a qualsiasi reimpostazione della password necessaria dopo la configurazione dell'unità. L'opzione password selezionata può essere modificata solamente dopo aver effettuato un reset completo del dispositivo.

Inizializzazione del dispositivo

Schermata informazioni di contatto

Inserire le informazioni di contatto nei relativi campi di testo. (Vedere Figura 4.14)

Nota: le informazioni immesse in questi campi NON possono contenere la stringa password creata al Punto 3 di questa procedura. Tuttavia, questi campi sono facoltativi e pertanto possono anche essere lasciati vuoti, se lo si desidera.

Il campo “Nome” può contenere fino a 32 caratteri, ma non può contenere la password esatta. Il campo “Azienda” può contenere fino a 32 caratteri, ma non può contenere la password esatta. Il campo “Dettagli” può contenere fino a 156 caratteri, ma non può contenere la password esatta.	 Figura 4.14 – Schermata dei dati di contatto
--	--

Nota: facendo clic su “OK” si completerà la procedura di inizializzazione e sarà possibile procedere allo sblocco dell'unità, per poi effettuare il montaggio della partizione sicura in cui effettuare l'archiviazione sicura dei dati. Scollegare l'unità dal sistema per poi ricollegarla così da visualizzare le modifiche apportate.

Utilizzo del dispositivo (ambienti Windows e macOS)

Accesso per amministratore e utente (modalità amministratore abilitata)

Se il dispositivo viene inizializzato con le password amministratore e utente (ruolo amministratore) abilitate, verrà avviata l'applicazione IronKey LP50G2, che richiederà prima di tutto l'immissione della password utente nella schermata di accesso. In questa schermata è possibile effettuare il login con la password utente, visualizzare tutte le informazioni di contatto inserite o effettuare il login come amministratore (Figura 6.1). Facendo clic sul pulsante "Accedi come amministratore" (mostrato sotto), l'applicazione passerà al menu di accesso amministratore dove sarà possibile eseguire il login da amministratore ed accedere così alle impostazioni e alle funzioni amministrative (Figura 6.2).

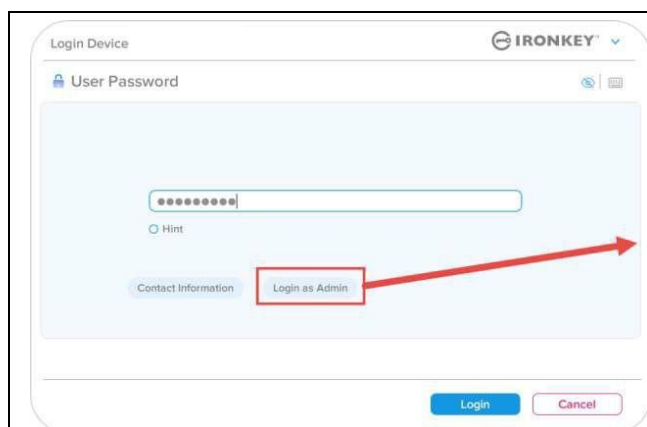


Figura 6.1 – Login con password utente (con amministratore abilitato)

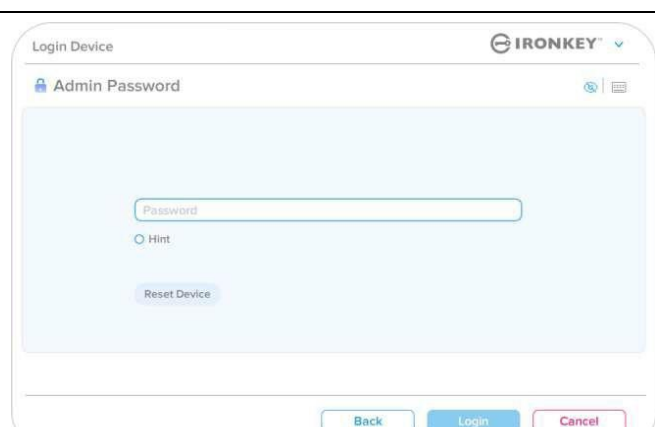


Figura 6.2 – Login con password amministratore

Modalità di accesso per solo utente (modalità amministratore non abilitata)

Come detto a **pagina 13**, sebbene sia consigliabile utilizzare la funzionalità Ruolo amministratore per sfruttare appieno le potenzialità del dispositivo, l'unità IronKey può essere inizializzata anche con una configurazione solo utente (password singola, utente singolo). In genere questa soluzione è preferibile per chi desidera un approccio semplice, con una sola password, per proteggere i dati presenti sul proprio disco. (Figura 6.3)

Nota: per abilitare le password amministratore e utente, è necessario usare il pulsante **Reset dispositivo**, per riportare l'unità allo stato di inizializzazione in cui è possibile abilitare le password amministratore e utente. **TUTTI i dati contenuti nel drive verranno formattati e persi definitivamente quando si esegue un reset del dispositivo.**

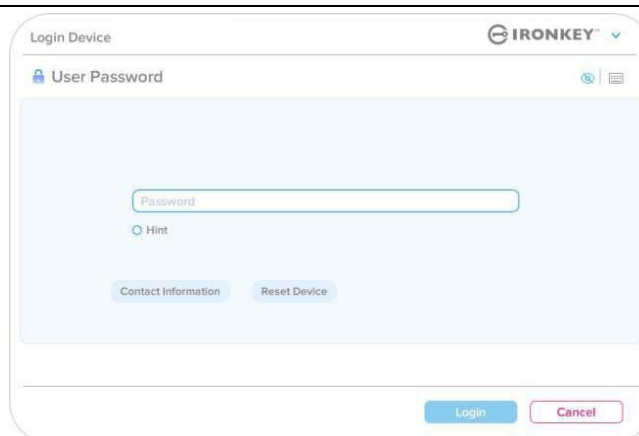


Figura 6.3 – Login con password utente (con amministratore non abilitato)

Utilizzo del dispositivo

Protezione contro gli attacchi brute-force

Importante: se durante l'accesso viene inserita una password non corretta, l'utente avrà a disposizione un'altra possibilità per inserire la password corretta; tuttavia, il drive dispone di una funzione di sicurezza integrata (nota col nome di protezione contro attacchi brute force), che conta il numero di tentativi di accesso falliti. *

Se questo numero supera il valore preimpostato di 10 di tentativi falliti, si verificheranno le seguenti conseguenze:

Funzione Amministratore/ Utente abilitata	Comportamento di protezione da attacchi Brute Force (dopo 10 tentativi di immissione password falliti)	Cancellazione dati e reset dispositivo?
Password utente:	Blocco password. Accedere come amministratore per reimpostare la password	NO
Password amministratore	Eliminazione della partizione crittografica del drive, delle password, delle impostazioni e eliminazione definitiva di tutti i dati	Sì
Modalità solo utente Un utente e una password (Amministratore/Utente NON abilitato)	Comportamento di protezione da attacchi Brute Force (dopo 10 tentativi di immissione password falliti)	Cancellazione dati e reset dispositivo?
Password utente	Eliminazione della partizione crittografica del drive, delle password, delle impostazioni ed eliminazione definitiva di tutti i dati	Sì

* Una volta effettuata con successo l'autenticazione sul dispositivo, verrà azzerato il contatore dei tentativi di login falliti relativo al metodo di login utilizzato. L'eliminazione crittografica cancellerà tutte le password, le chiavi di crittografia e i dati: **i dati saranno quindi persi per sempre.**

Accesso ai file sicuri

Una volta sbloccato il drive, è possibile accedere ai file sicuri. I file vengono crittografati e decrittati automaticamente quando vengono salvati o aperti sul drive. Questa tecnologia offre il vantaggio della massima trasparenza, consentendo di utilizzare i dati come se questi fossero memorizzati su un drive normale, offrendo al contempo solide funzionalità di sicurezza "always-on".

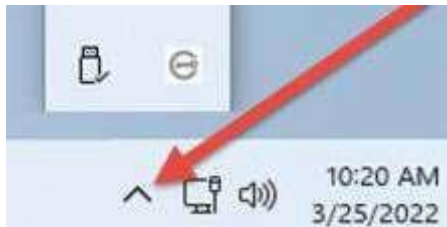
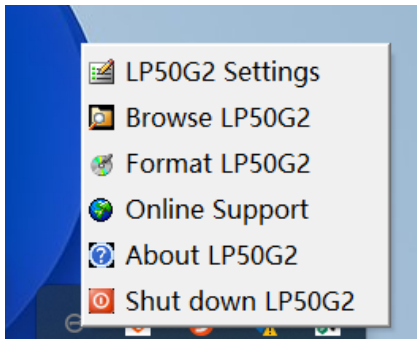
Suggerimento: è anche possibile accedere ai file facendo clic col tasto destro del mouse **sull'icona IronKey**, sulla barra applicazioni di Windows, per poi selezionare

Esplora LP50G2 (Figura 7.2)

Opzioni del dispositivo (ambienti Windows)

Dopo aver eseguito l'accesso al dispositivo, nell'angolo destro della finestra è presente l'icona del drive IronKey. Facendo clic con il tasto destro del mouse sull'icona IronKey, sarà possibile aprire il menu di selezione che include le opzioni del drive (*Figura 6.2*).

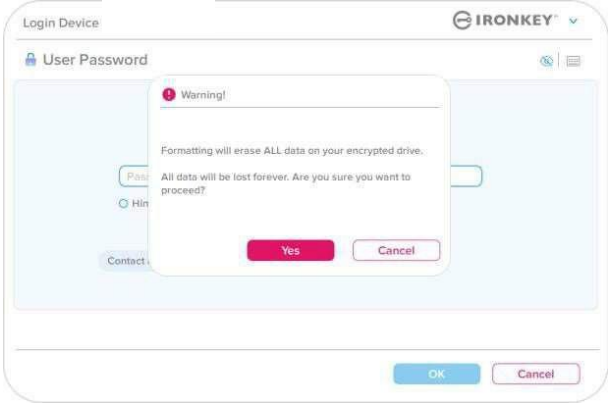
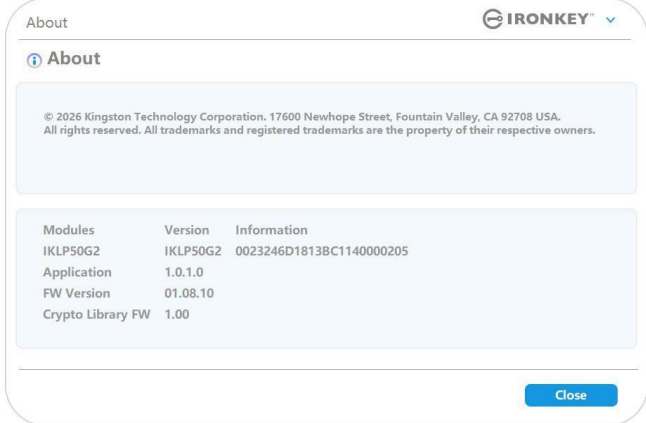
Alle pagine 19-23 della presente guida sono esposti ulteriori dettagli su queste opzioni del dispositivo.

Dopo aver eseguito l'accesso al dispositivo, nell'angolo destro della finestra è presente l'icona del drive IronKey. (<i>Figura 7.1</i>)	 Figura 7.1 – Icona IronKey nella barra delle applicazioni
Facendo clic con il tasto destro del mouse sull'icona IronKey, sarà possibile aprire il menu di selezione che include le opzioni del drive. (<i>Figura 7.2</i>) Alle pagine 19-23 della presente guida sono esposti ulteriori dettagli su queste opzioni del dispositivo.	 Figura 7.2 – Clic con il tasto destro del mouse sull'icona IronKey per accedere alle opzioni del dispositivo

Opzioni dispositivo - (Ambiente macOS)

Quando si è connessi al dispositivo, nel menu macOS visibile nella Figura 7.3 è presente l'icona "IronKey LP50G2" che consente di accedere alle opzioni disponibili per il dispositivo. Alle pagine 19-23 della presente guida sono esposti ulteriori dettagli su queste opzioni del dispositivo.	 Figura 7.3 – Barra dei menu di macOS Icona/ Menu delle opzioni del dispositivo
---	---

Opzioni dispositivo

Impostazioni LP50G2:	Modifica password di accesso, informazioni di contatto e altre impostazioni (maggiori dettagli sulle impostazioni del dispositivo sono disponibili nella sezione "Impostazioni LP50G2" della presente guida).
Esplora LP50G2:	Consente di visualizzare i file sicuri.
Formatta LP50G2: Consente di formattare la partizione dati sicura. (Attenzione: tutti i dati contenuti nell'unità verranno eliminati). (Figura 6.1) Nota: la formattazione richiede l'autenticazione mediante password.	 Figura 7.4 – Formatta LP50G2
Supporto online:	Apri automaticamente il browser Internet puntando al linkhttp://www.kingston.com/support dal quale è possibile accedere a una serie di informazioni di supporto aggiuntive.
Informazioni su LP50G2: Fornisce informazioni relative al drive LP50G2, inclusi il numero di serie, la versione firmware e l'applicativo (Figura 6.2) Nota: il numero di serie unico dell'unità si trova riportato nella colonna "Informazioni".	 Figura 7.5 – Informazioni su LP50G2
Chiudi LP50G2:	Permette di arrestare correttamente l'unità LP50G2, consentendo all'utente di scollegare il drive dal computer in tutta sicurezza

Impostazioni LP50G2

Impostazioni amministratore

Il login amministratore consente di accedere alle seguenti impostazioni del dispositivo:

- **Password:** permette di modificare la propria password Amministratore e/o il suggerimento (*Figura 8.1*)
- **Dati di contatto:** consente di aggiungere/visualizzare/modificare le informazioni di contatto dell'utente (*Figura 8.2*)
- **Lingua:** consente di modificare la lingua impostata (*Figura 8.3*)
- **Opzioni amministratore:** consente di accedere a funzionalità aggiuntive quali:
 - Modifica della password utente (*Figura 8.4*)

NOTA: ulteriori dettagli sulle opzioni di amministrazione sono disponibili a pagina 25.

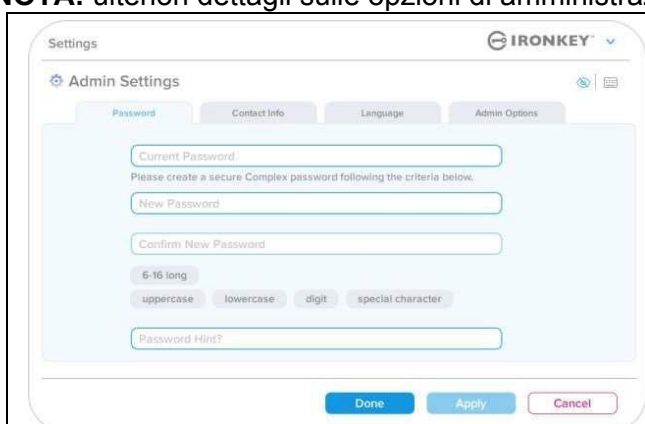


Figura 8.1 – Opzioni password amministratore

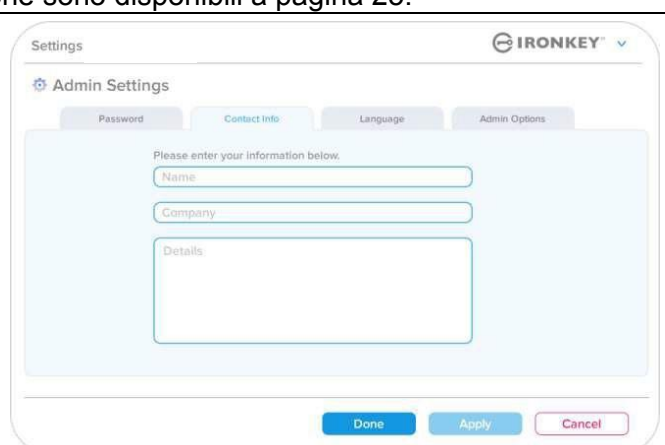


Figura 8.2 – Dati di contatto

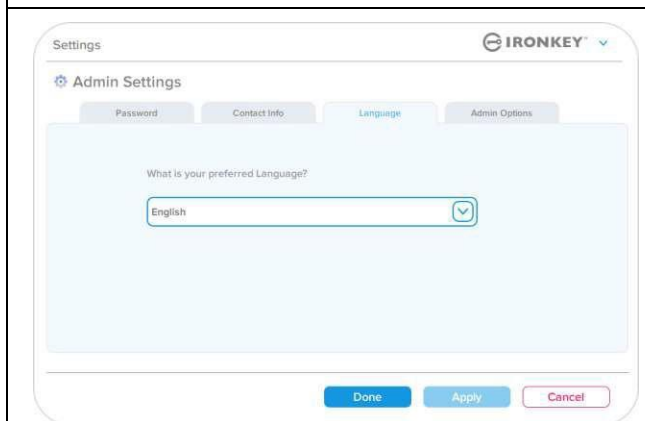


Figura 8.3 – Opzioni lingua

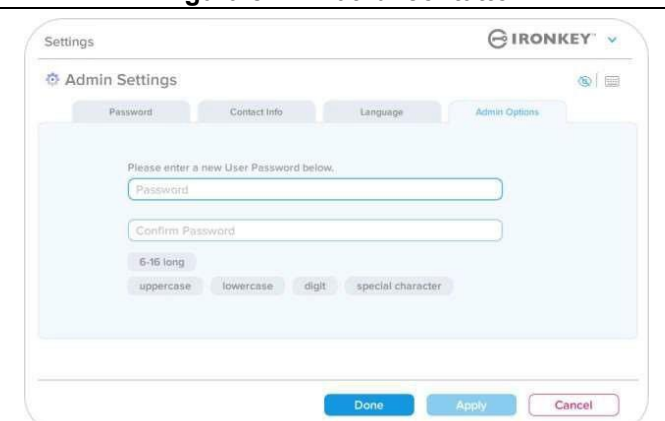


Figura 8.4 – Opzioni amministratore

Impostazioni LP50G2

Impostazioni utente: funzione amministratore abilitata

Il login utente limita l'accesso alle seguenti impostazioni:

Password:

Consente di modificare la password Utente e/o il suggerimento. (Figura 8.5)

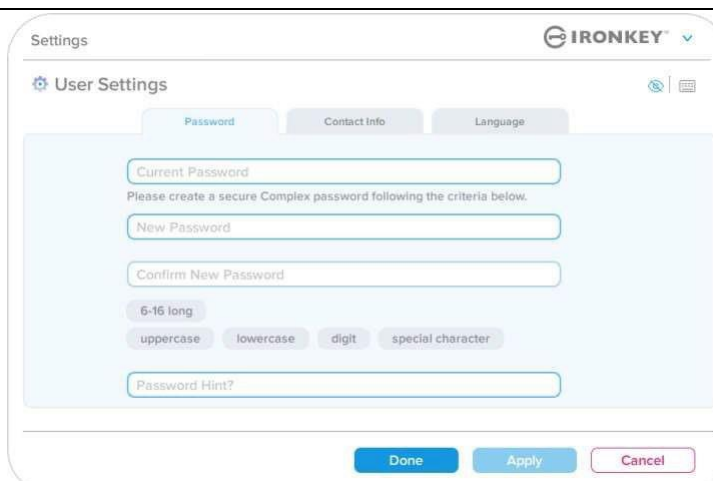


Figura 8.5 – Opzioni password (funzione amministratore abilitata: accesso Utente)

Dati di contatto:

Consente di aggiungere/visualizzare/modificare i dati di contatto. (Figura 8.6)

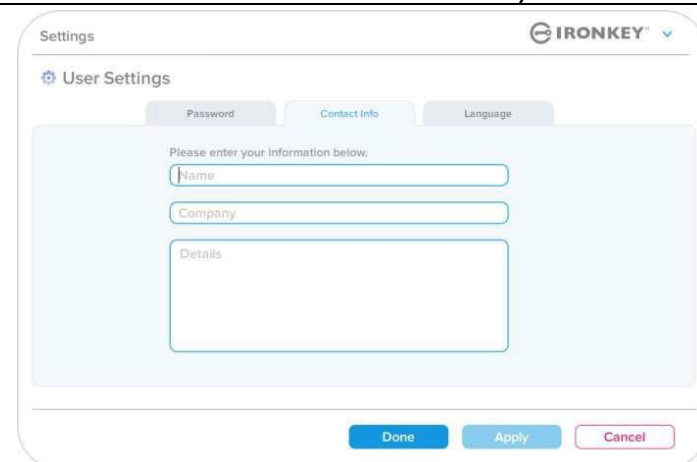


Figura 8.6 - Informazioni di contatto (modalità amministratore abilitata: accesso Utente)

Lingua:

Consente di modificare le impostazioni della lingua corrente. (Figura 8.7)

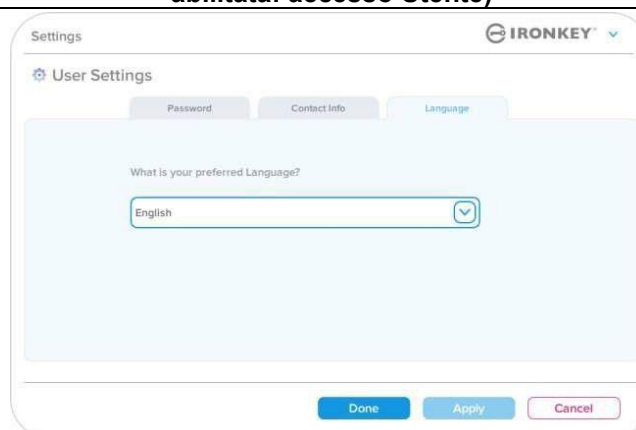


Figura 8.7 – Impostazioni lingua (modalità amministratore abilitata: accesso Utente)

Nota: le opzioni di amministrazione non sono accessibili quando si fa il login con la password utente.

Impostazioni LP50G2

Impostazioni utente: modalità amministratore non abilitata

Come indicato in precedenza a pagina 12, l'inizializzazione dell'unità LP50G2 senza abilitare le password "Amministratore e Utente" configurerà l'unità con un'impostazione **Password singola, Utente singolo**. Questa configurazione non permette di accedere ad alcuna opzione o funzione di amministrazione. Sarà invece possibile accedere alle seguenti impostazioni dell'unità LP50G2.

Password

Consente di modificare la password Utente e/o il suggerimento. (Figura 8.8)

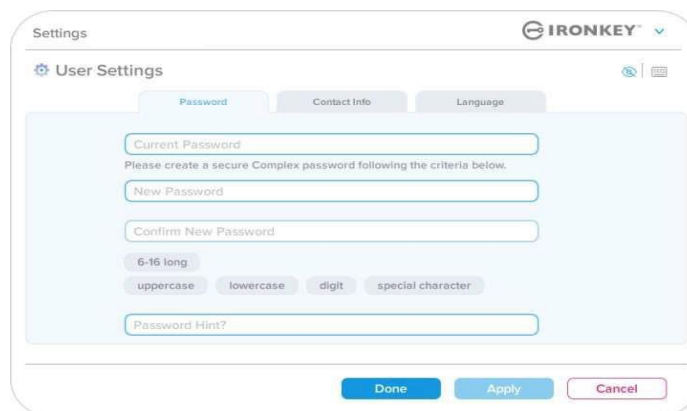


Figura 8.8 – Opzioni password (Modalità solo utente)

Dati di contatto:

Consente di aggiungere/visualizzare/modificare i dati di contatto. (Figura 8.9)

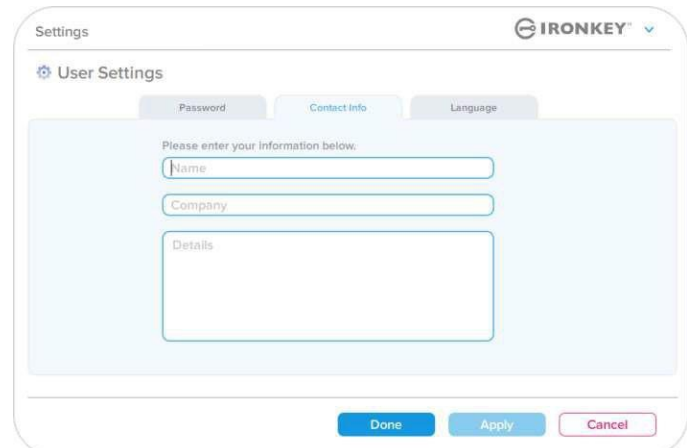


Figura 8.9 – Dati di contatto (Modalità solo utente)

Lingua:

Consente di modificare le impostazioni della lingua corrente. (Figura 8.10)

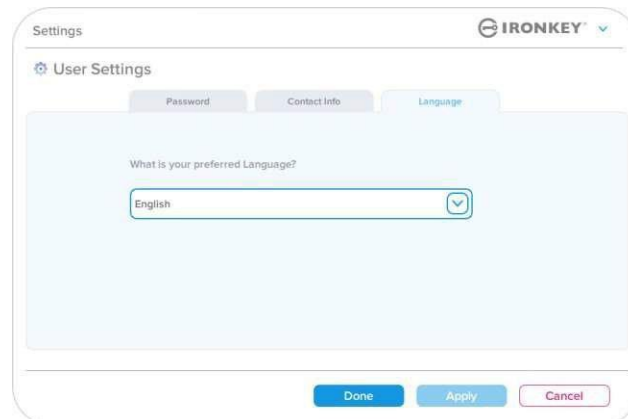


Figura 8.10 - Impostazioni lingua (Modalità solo utente)

Impostazioni LP50G2

Modifica e salvataggio delle impostazioni

- Ogni volta che vengono modificate le impostazioni nella scheda "Impostazioni LP50G2" (ad es. dati di contatto, lingua, password, opzioni amministratore ecc.), l'unità richiederà di inserire la password per accettare e applicare le modifiche. (Vedere Figura 8.11)

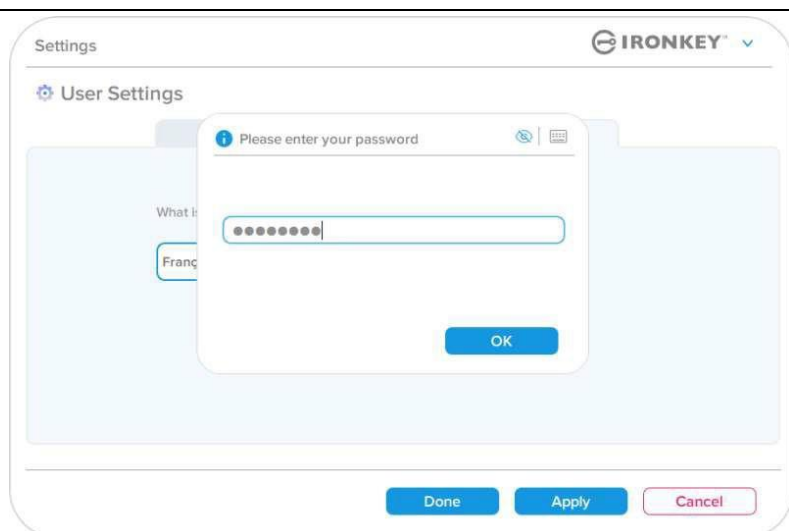


Figura 8.11 – Schermata di richiesta della password per salvare le impostazioni LP50G2

Nota: se si desidera annullare o modificare le modifiche apportate, basta lasciare il campo della password vuoto in questa schermata e fare clic su "OK". In questo modo la finestra "Inserisci la password" verrà chiusa e si tornerà al menu delle impostazioni LP50G2.

Funzionalità amministratore

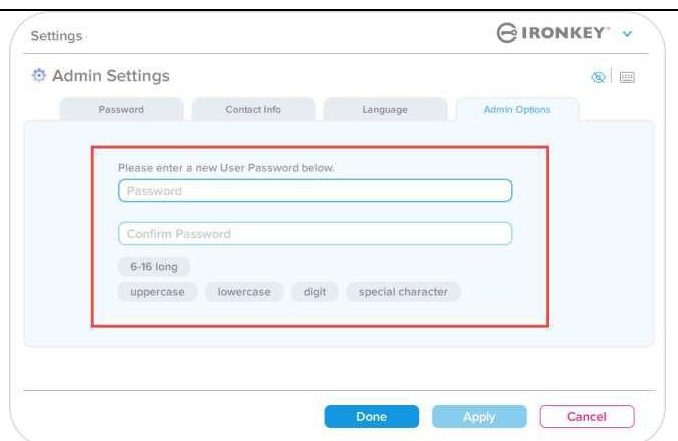
Opzione disponibile per reimpostare la password utente

Una dei motivi per cui è utile attivare il ruolo dell'amministratore consiste nella possibilità di reimpostare in modo sicuro la password degli utenti, qualora dovesse essere dimenticata. Di seguito viene spiegato come utilizzare questa funzione che permette di reimpostare la password utente:

Reset della password utente:

Dal menu “Opzioni amministratore”, modificare manualmente la password utente. La modifica effettuata avrà effetto istantaneo, in occasione del prossimo accesso dell'utente. (Figura 9.1)

Nota: i criteri relativi alla password verranno riportati per impostazione predefinita ai valori originali definiti durante il processo di inizializzazione (password Complessa o Frase password).



The screenshot shows the 'Settings' window for IronKey. The 'Admin Settings' section is active, with the 'Admin Options' tab selected. A red box highlights the 'Please enter a new User Password below:' section, which includes a 'Password' field, a 'Confirm Password' field, and a list of password requirements: '6-16 long', 'uppercase', 'lowercase', 'digit', and 'special character'. At the bottom of the window are 'Done', 'Apply', and 'Cancel' buttons.

Figura 9.1 – Opzioni amministratore/Reset password utente

Guida alla risoluzione dei problemi

Blocco del dispositivo

Il drive LP50G2 è dotato di una funzionalità di sicurezza che impedisce di accedere alla partizione dati quando si supera un determinato numero di tentativi di accesso falliti **consecutivi** (definiti come *MaxNoA* , in forma abbreviata). Il numero di tentativi preimpostato in fabbrica come valore di default è pari a 10 (n. max di tentativi consecutivi) per ciascun metodo di login (Amministratore/utente).

Il contatore che attiva il blocco tiene traccia di ogni tentativo di accesso fallito e può essere resettato in **uno dei due** seguenti modi:

1. Inserendo la password di accesso corretta prima di raggiungere il valore “MaxNoA”
2. Superando il numero di tentativi previsti dall'impostazione MaxNoA ed eseguendo un blocco del dispositivo o la sua formattazione, a seconda delle configurazioni attive nel drive.

- Se viene inserita una password errata, proprio sopra il campo di immissione della password verrà visualizzato un messaggio di errore in rosso indicante il tentativo di accesso fallito. (Figura 10.1)

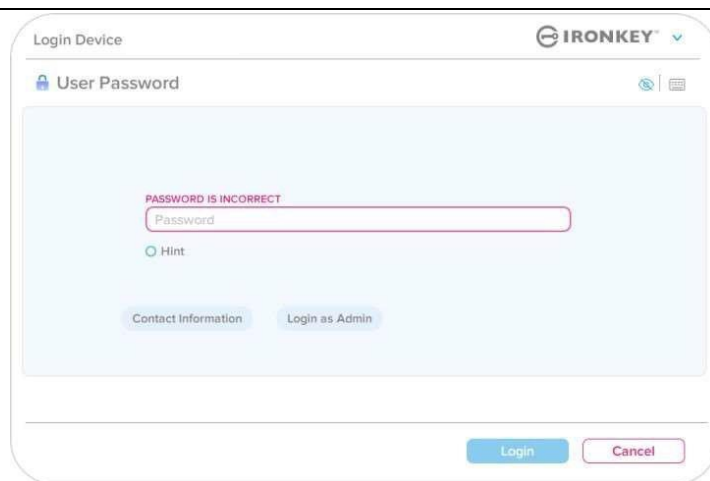


Figura 10.1 – Avviso che è stata inserita una password non corretta

- Raggiunto il 7° tentativo fallito, verrà visualizzato un ulteriore messaggio di errore che informa l'utente che ha a disposizione solo altri 3 tentativi prima di raggiungere il numero di tentativi specificati dal valore MaxNoA (impostato su 10 per default). (Figura 10.2)

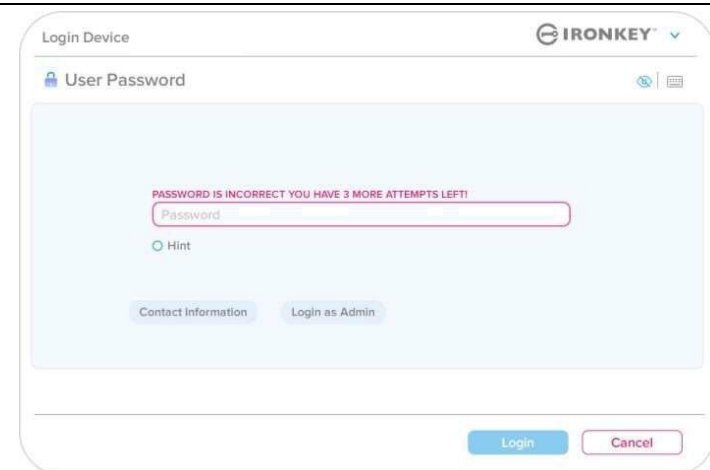


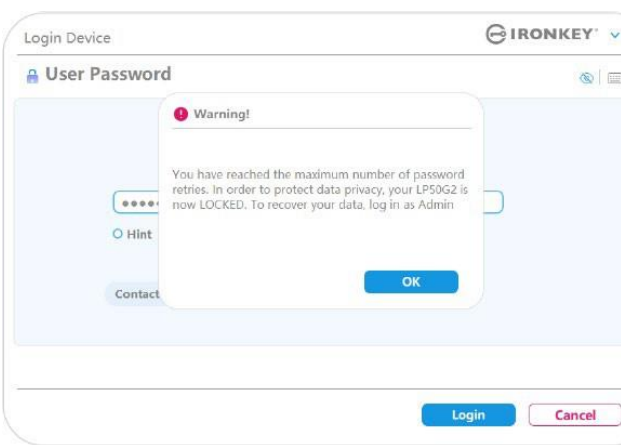
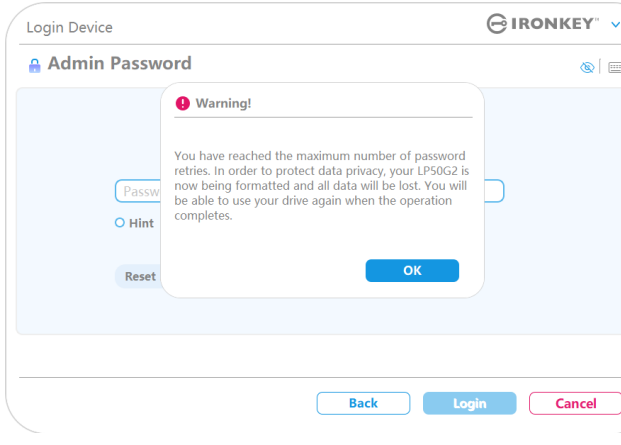
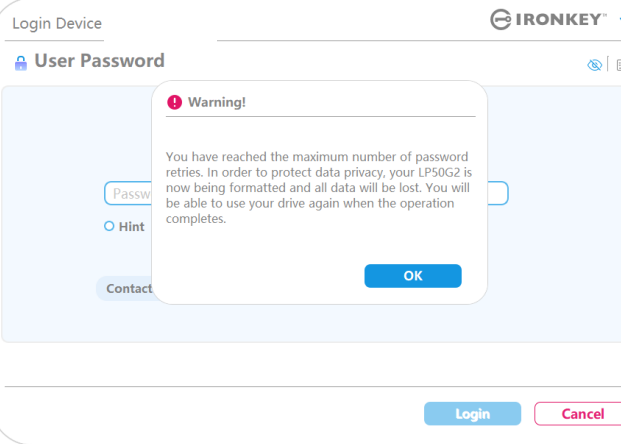
Figura 10.2 – 7° tentativo di immissione password non corretta

Guida alla risoluzione dei problemi

Blocco del dispositivo

Importante: dopo il 10° e ultimo tentativo di accesso non riuscito, a seconda della configurazione del dispositivo e del metodo di accesso utilizzato (amministratore/utente), il dispositivo si bloccherà, richiedendo l'accesso con un metodo alternativo (se previsto), oppure verrà eseguito un ripristino del dispositivo che **formatterà l'unità e tutti i dati contenuti nell'unità andranno persi per sempre**. Comportamenti menzionati anche a pagina 17 della presente Guida per l'utente.

Le figure 10.3-10.6 riportate di seguito mostrano visivamente cosa accade in occasione del 10° e ultimo accesso non riuscito, per ciascun metodo di password di accesso:

<u>Password utente: (Funzione Amministratore/Utente abilitata)</u>  BLOCCO DEL DISPOSITIVO Figura 10.3	<u>Password Amministratore (funzione Amministratore/Utente abilitata)</u>  FORMATTAZIONE DISPOSITIVO* Figura 10.4
Queste misure di sicurezza hanno lo scopo di limitare l'accesso a coloro che non dispongono della password, impedendo loro di effettuare tentativi di accesso ripetuti all'infinito allo scopo di accedere ai vostri dati sensibili (tentativi a cui viene comunemente dato il nome di attacco "Brute-Force"). Per i possessori di drive LP50G2 che hanno dimenticato la password di accesso, verranno applicate le medesime misure di sicurezza, compresa la formattazione del dispositivo. * Per ulteriori dettagli su questa funzione, consultare la sezione "Reset dispositivo" a pagina 27.	<u>Password utente (Modalità amministratore NON abilitata)</u>  FORMATTAZIONE DISPOSITIVO* Figura 10.5

***Nota:** la formattazione del dispositivo causerà l'eliminazione di **TUTTI** i dati contenuti nella partizione dati sicura dell'unità LP50G2.

Guida alla risoluzione dei problemi

Reset dispositivo

Se si dimentica la password o è necessario reimpostare il dispositivo, è possibile fare clic sul pulsante “Reset dispositivo” visualizzato all'esecuzione del launcher dell'unità LP50G2 in uno dei due seguenti punti a seconda di come è stata configurata l'unità: nel menu Password di accesso amministratore se la modalità Amministratore/Utente è abilitata; oppure nel menu di accesso “Password utente” se la modalità Amministratore/Utente non è abilitata. (vedere *Figure 10.7 e 10.8*)

- Questa opzione consente di creare una nuova password. Tuttavia, al fine di garantire la privacy dei dati contenuti nel drive LP50G2, l'unità verrà formattata. Ciò significa che durante tale procedura tutti i dati precedentemente archiviati andranno persi.*

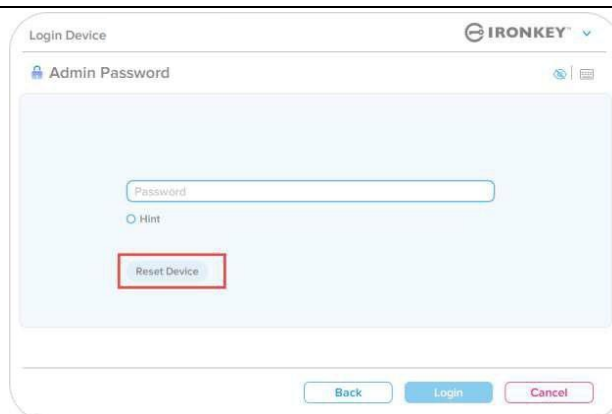


Figura 10.6 – Password amministratore: pulsante di Reset dispositivo

- Nota:** facendo clic sul pulsante “Reset dispositivo”, verrà visualizzata una finestra di notifica in cui si chiede all'utente se desidera inserire una nuova password prima della formattazione. A questo punto, è possibile 1) fare clic su “OK” per confermare, oppure 2) fare clic su “Annulla”, per tornare alla schermata di accesso. (Vedere *figura 10.8*)

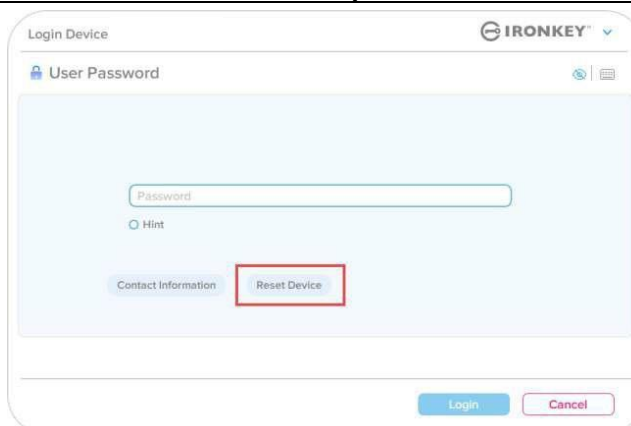


Figura 10.7 – Password utente (con amministratore non abilitato): Reset dispositivo

- Se si decide di continuare, sarà visualizzata la schermata di inizializzazione dalla quale è possibile abilitare la modalità Amministratore e Utente e inserire una nuova password in base all'opzione di configurazione password selezionata (Password complessa o frase password). Il campo suggerimento (Hint) non è obbligatorio, ma può rivelarsi utile per aiutare l'utente a ricordare la password, qualora questa vada persa o dimenticata.

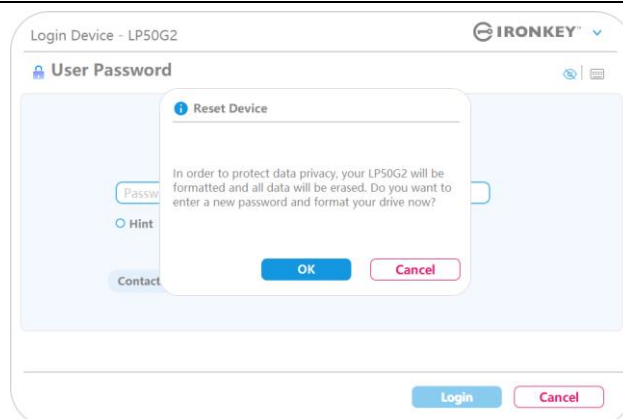


Figura 10.8 – Conferma reset dispositivo

Conflitti con le lettere di unità (Sistemi operativi Windows)

- Come anticipato nella sezione “*Requisiti di sistema*” di questa guida (a pagina 4), il drive LP50G2 richiede due lettere di unità consecutive libere DOPO quella assegnata all'ultimo disco fisico che appare prima delle lettere di unità assegnate ai profili non hardware. (vedere *Figura 10.9*). L'assegnazione delle lettere di unità in ordine cronologico NON interessa le unità di rete condivise, in quanto queste sono unità associate a profili utente specifici e non al profilo hardware di sistema e pertanto appaiono disponibili per il sistema operativo.
- Ciò significa che Windows potrebbe assegnare al drive LP50G2 una lettera di unità che è già utilizzata da una unità di rete condivisa o è assegnata a un percorso UNC (Universal Naming Convention), causando un conflitto tra le lettere assegnate ai vari drive. In tal caso, sarà necessario contattare l'amministratore di rete o il reparto assistenza, chiedendo di modificare le lettere di unità assegnate da Gestione Disco di Windows (l'operazione richiede l'accesso con diritti di amministratore).

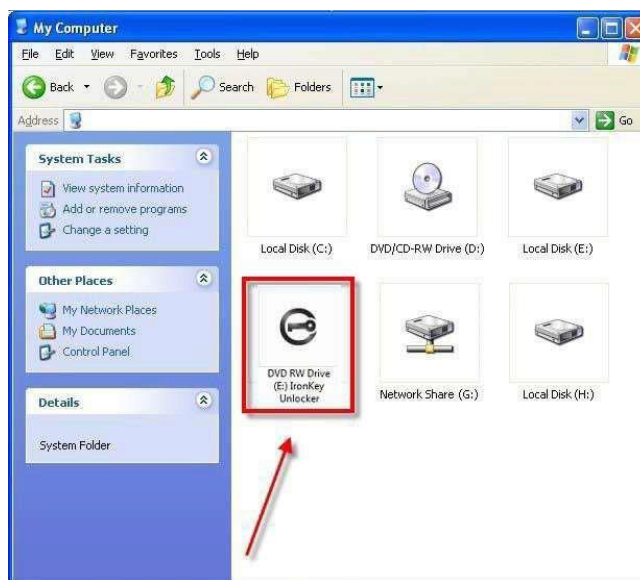


Figura 10.9 – Esempio di lettera di unità

In questo esempio (*Figura 10.9*), all'unità LP50G2 è assegnata la lettera F: che è la prima lettera disponibile dopo l'unità E: (l'ultima lettera di unità assegnata a un disco fisico prima dell'elenco di lettere di unità assegnate a unità non fisiche). Dato che alla lettera G: è assegnata una condivisione di rete, che non appartiene al profilo hardware del computer in uso, l'unità LP50G2 tenterà di utilizzare tale lettera come seconda unità, generando un conflitto.

Se sul computer in uso non sono presenti condivisioni di rete, ma l'unità LP50G2 continua a non avviarsi, è possibile che altri dispositivi esterni, come lettori di schede, dischi rimovibili, o altri dispositivi installati in precedenza stiano utilizzando la lettera di unità richiesta per il funzionamento dell'unità IronKey, causando ulteriori conflitti.

Si noti che le funzionalità di Gestione delle Lettere di Unità (DLM) sono migliorate significativamente su Windows 11; pertanto, tale problema non dovrebbe manifestarsi. Tuttavia, se l'utente non dovesse essere in grado di risolvere il conflitto, si raccomanda di contattare la divisione Supporto Tecnico di Kingston o di visitare la pagina Web Kingston.com/support per richiedere ulteriore assistenza.



FLASH DRIVE USB 3.2 SEGURO
Gen 1 IRONKEY™ Locker+ 50 G2
(LP50G2)

Manual do Usuário



Índice

Introdução	3
Recursos Locker+ 50 G2.....	4
Sobre este Manual.....	4
Requisitos do sistema.....	4
 Recomendações	 5
Utilizando o sistema de arquivo correto.....	5
Lembretes de utilização.....	5
Melhores práticas para configuração de senha	6
 Configurar meu dispositivo	 7
Acesso ao dispositivo (Ambiente Windows)	7
Acesso ao dispositivo (Ambiente macOS).....	7
 Inicialização do dispositivo (Ambiente Windows e macOS)	 8
Escolha de senha	9
Teclado virtual	11
Botão de visibilidade de senha	12
Senhas de Admin e de Usuário	13
Informações de contato	15
 Uso do dispositivo (Ambiente Windows e macOS)	 16
Login para Admin e Usuário (Admin habilitado).....	16
Login para modo Apenas Usuário (Admin não habilitado)	16
Proteção de ataque de força bruta	17
Acessando meus arquivos seguros.....	17
 Opções do dispositivo.....	 18
 Configurações do LP50G2	 20
Configurações do Admin	20
Configurações do Usuário: Admin habilitado	21
Configurações do Usuário: Admin não habilitado	22
Alterar e Salvar configurações do LP50G2	23
 Recursos do Admin.....	 24
Redefinição da senha de usuário	24
 Ajuda e Resolução de Problemas	 25
Bloqueio do LP50G2	25
Restauração do dispositivo LP50G2	27
Conflito de letra do drive: (Windows)	28



Figura 1: IronKey LP50G2

Introdução

Os pendrives USB Kingston IronKey™ Locker+ 50 G2 proporcionam uma segurança de nível empresarial com certificação FIPS 197 e criptografia por hardware AES de 256 bit no modo XTS, incluindo proteções contra BadUSB e ataques à senha por força bruta. O LP50G2 também está em conformidade com TAA.

O LP50G2 agora suporta a opção de múltiplas senhas (Admin e Usuário) com modos Complexos ou de Frase-passe. O modo Complexo permite senhas de 6 a 16 caracteres usando 3 de 4 conjunto de caracteres. O novo modo de Frase-passe permite um PIN numérico, frase, lista de palavras ou até letras de música de 10 a 64 caracteres. O Admin pode habilitar uma senha de Usuário ou redefinir a senha de Usuário para restaurar o acesso aos dados. Para ajudar na entrada da senha, o símbolo de “olho” pode ser habilitado para revelar a senha digitada, reduzindo erros de digitação que levam a tentativas de login malsucedidas. A proteção contra ataques de força bruta bloqueia o Usuário após 10 senhas inválidas inseridas seguidamente, e apaga o drive criptograficamente se a senha do Admin for inserida incorretamente 10 vezes seguidas. Além disso, um teclado virtual integrado protege as senhas de registros do teclado e da tela.

O Locker+ 50 G2 foi projetado com a conveniência de uma pequena capa de metal e aro de metal embutido para levar os dados aonde quiser.

O LP50G2 conta com uma garantia limitada de 5 anos e suporte técnico Kingston gratuito.

Recursos do IronKey Locker+ 50 G2

- Certificado FIPS 197
- Criptografia de hardware XTS-AES (a criptografia nunca pode ser desligada)
- Proteção contra ataque de BadUSB e por força bruta
- Opção de multissenhas
- Modos de senha Complexas ou de Frase-passe
- Botão de olho para exibir senhas digitadas e reduzir tentativas de login malsucedidas
- Teclado virtual para ajudar na proteção contra registros do toque do teclado ou da tela
- Compatível com Windows ou macOS (consultar a ficha técnica para mais detalhes)

Sobre este Manual (02122026)

Este manual do usuário trata do IronKey Locker+ 50 G2 (LP50G2).

Requisitos do sistema

Plataforma de PC • Intel e AMD • 15 MB de espaço livre no disco • Porta USB 2.0 - 3.2 disponível • Duas letras consecutivas de drive após o último drive físico* *Observação: Consulte “Conflito de Letra de Drive” na página 28.	Suporte do Sistema Operacional do PC • Windows 11
Plataforma Mac • Intel e Apple SOC • 15 MB de espaço livre no disco • Porta USB 2.0 - 3.2	Suporte do Sistema Operacional Mac • macOS 13.x – 26.x

Recomendações

Para garantir que haja uma ampla energia fornecida ao dispositivo LP50G2, insira-o diretamente em uma porta USB em seu notebook ou desktop, como visto na *Figura 1.1*. Evite conectar o LP50G2 a qualquer dispositivo periférico que possa ter uma porta USB, como um teclado ou um hub USB, como visto na *Figura 1.2*.



Figura 1.1 – Uso recomendado



Figura 1.2 – Não Recomendado

Utilizar o sistema de arquivo correto

O IronKey LP50G2 vem pré-formatado com o sistema de arquivos FAT32. Ele funcionará nos sistemas Windows e macOS. Entretanto, pode haver algumas outras opções que podem ser usadas para formatar o drive manualmente, como NTFS para Windows e exFAT. Você pode reformatar a partição de dados se necessário mas os dados são perdidos quando o drive é reformatado.

Utilização

Para manter a segurança de seus dados, a Kingston recomenda que você:

- Realize um escaneamento para vírus em seu computador antes de instalar e usar o LP50G2 em um sistema
- Ao usar o drive em um sistema público e que não esteja familiarizado, você deve definir o modo Somente Leitura no dispositivo para ajudar a proteger o drive de malwares
- Bloqueie o dispositivo quando não estiver usando
- Ejeite o drive antes de desconectá-la
- Nunca desconecte o dispositivo quando o LED estiver aceso. Isso pode danificar o drive e exigir uma reformatação, o que apagará seus dados
- Nunca compartilhe a senha do seu dispositivo com ninguém

Busque as últimas Informações e Atualizações

Visite kingston.com/support para ver as últimas atualizações do drive, Perguntas Frequentes, Documentos e informações adicionais.

OBSERVAÇÃO: Somente as últimas atualizações do drive (quando disponíveis) devem ser aplicadas ao drive. Não é suportado rebaixar o drive para uma versão de software mais antiga e isso pode potencialmente causar a perda dos dados armazenados ou impedir outra funcionalidade do drive. Entre em contato com o Suporte Técnico Kingston se tiver problemas ou dúvidas.

Melhores práticas para configuração de senha

Seu LP50G2 conta com fortes contramedidas de segurança. Isso inclui proteção contra ataques de força bruta que impedirão que um invasor adivinhe as senhas limitando a 10 tentativas de senha. Quando o limite do drive é alcançado, o LP50G2 automaticamente limpará os dados criptografados - formatando-se de volta para as configurações de fábrica.

Multissenhas

O LP50G2 suporta multissenhas como um recurso superior para ajudar a proteger contra perda de dados se uma ou mais senhas forem esquecidas. Quando todas as opções de senha estiverem habilitadas, o LP50G2 pode suportar duas senhas diferentes utilizadas para recuperar os dados - funções de senha de Admin e Usuário

O LP50G2 permite que você selecione duas senhas principais - uma senha de Administrador (chamada de senha de Admin) e uma senha de Usuário. O Admin pode acessar o drive a qualquer momento e definir opções para o Usuário - o Admin é como um Superusuário.

O usuário também pode acessar o drive mas possui privilégios limitados em comparação com o Admin. Se uma das duas senhas for esquecida, a outra senha pode ser utilizada para acessar e recuperar os dados. O drive pode então ser configurado de volta para ter duas senhas. É importante configurar AMBAS as senhas e salvar a senha de Admin em um local seguro enquanto utiliza a senha de Usuário.

Se ambas as senhas forem esquecidas ou perdidas, não há outra forma de acessar os dados. A Kingston não poderá recuperar os dados, pois a segurança não possui brechas. A Kingston recomenda que você também tenha os dados salvos em outra mídia. Os LP50G2 pode ser restaurado e reutilizado, mas os dados anteriores serão excluídos para sempre.

Modos de senha

O LP50G2 também suporta dois modos de senha diferentes:

Complexa

Uma senha complexa exige o mínimo de 6 a 16 caracteres utilizando pelo menos 3 dos seguintes caracteres:

- Caracteres alfabéticos maiúsculos
- Caracteres alfabéticos minúsculos
- Números
- Caracteres especiais

Frase-passe

O LP50G2 suporta frases-passe de 10 a 64 caracteres. Uma frase-passe não segue nenhuma regra adicional, mas se utilizada de maneira apropriada, pode fornecer níveis muito altos de proteção da senha.

Uma frase-passe é basicamente qualquer combinação de caracteres, incluindo caracteres de outro idioma. Como o drive LP50G2, o idioma da senha pode combinar o idioma selecionado para o drive. Isso permite que você selecione múltiplas palavras, uma frase, letra de uma música, uma linha de uma poesia etc. Boas frases-passes estão entre os tipos de senha mais difíceis de um invasor adivinhar e ao mesmo tempo podem ser mais fáceis para os usuários recordarem.

Configurar o meu dispositivo

Para garantir que haja uma ampla energia fornecida para o drive USB criptografado IronKey, insira-o diretamente em uma porta USB 2.0 / 3.0 de um notebook ou computador. Evite conectá-lo a qualquer dispositivo periférico que possa conter uma porta USB, como um teclado ou um hub USB. A instalação inicial do dispositivo deve ser feita em um sistema operacional Windows ou macOS que seja compatível.

Acesso ao dispositivo (Ambiente Windows)

Conecte o drive USB criptografado IronKey à uma porta USB disponível em um notebook ou computador e espere o Windows detectá-lo.

- Os usuários do Windows receberão uma notificação do driver do dispositivo. (Figura 3.1)



Figura 3.1 – Notificação do Driver do Dispositivo

- Quando a detecção de hardware estiver concluída, selecione a opção **IronKey.exe** dentro da partição Unlocker que pode ser encontrada no Gerenciador de Arquivos. (Figura 3.2)
- Observe que a letra da partição vai variar com base na próxima letra do drive livre. A letra do drive pode mudar dependendo de quais dispositivos estão conectados. Na imagem à direita, a letra do drive é (E:).

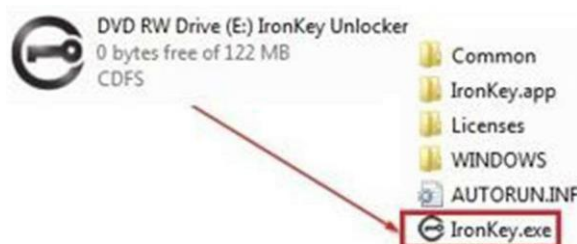


Figura 3.2 - File Explorer Window/IronKey.exe

Acesso ao dispositivo (Ambiente macOS)

Insira o LP50G2 em uma porta USB disponível no seu notebook ou computador e aguarde o sistema operacional do Mac detectá-lo. Quando isso acontecer, você verá aparecer o volume 'IRONKEY' no computador. (Figura 3.3)

- Clique duas vezes no ícone do IronKey CD-ROM.
- Depois, clique duas vezes no ícone do aplicativo IronKey.app encontrado na janela exibida na Figura 3.3. Isso fará começar o processo de inicialização.

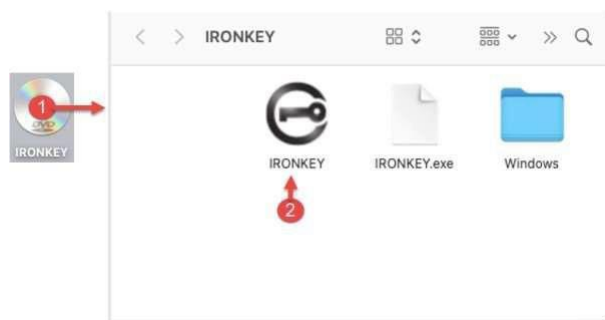


Figura 3.3 – Volume IRONKEY

Inicialização do dispositivo (Ambiente Windows e macOS)

Idioma e EULA

Selecione o seu idioma de preferência no menu suspenso e clique em **Avançar**. (Ver Figura 4.1)

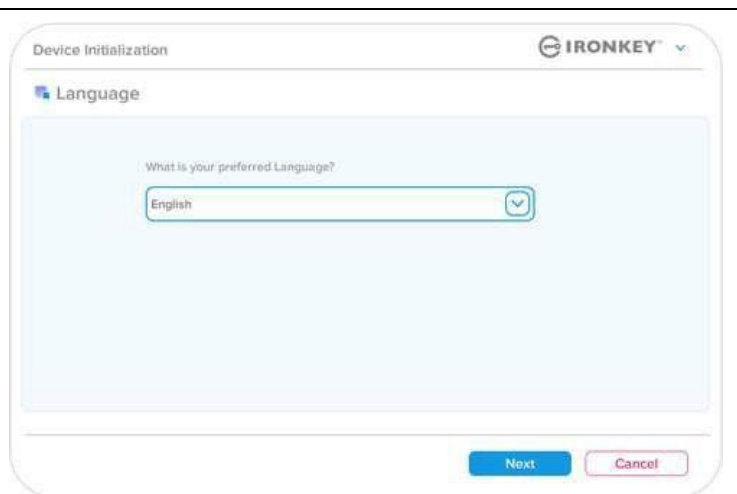


Figura 4.1 – Seleção de idioma

Analise o acordo de licença e clique em **Avançar**.

Observação: Você deve aceitar o acordo de licença antes de continuar; de outra forma, o botão **Avançar** continuará inativo. (Figura 4.2)

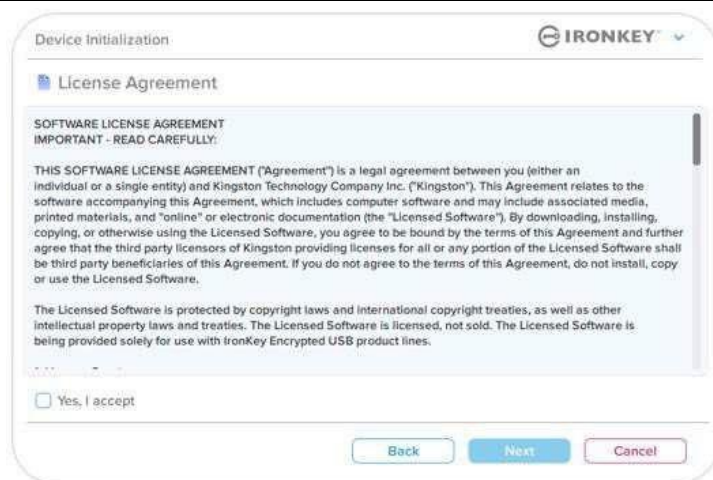


Figura 4.2 – Contrato de Licença

Inicialização do dispositivo

Escolha de senha

Na tela de mensagem de Senha, você poderá criar uma senha para proteger seus dados no LP50G2 usando os modos de senha Complexas ou de Frase-passe (*Figuras 4.3 - 4.4*). Além disso, as opções de Usuário/Admin multissenhas também podem ser habilitadas nesta tela. Antes de continuar com a escolha da senha, veja Habilitando as Senhas de Usuário / Admin abaixo para entender melhor esses recursos.

Observação: Seja o modo Complexo ou frase-passe o escolhido, o modo não pode ser alterado a menos que o dispositivo seja Redefinido. Para começar com a escolha da senha, crie sua senha no Campo de Senha, depois redigite-a nos campos de Confirmar Senha. A senha que você criar deve seguir os seguintes critérios antes do processo de inicialização permitir que você continue:

Senha complexa

- Deve conter 6 caracteres ou mais (até 16 caracteres).
- Deve conter três (3) dos seguintes critérios:
 - Letra maiúscula
 - Letra minúscula
 - Dígito numérico
 - Caracteres especiais (!, \$, &, etc.)

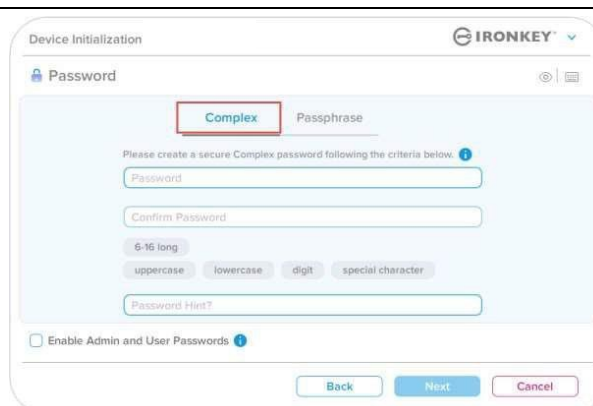


Figura 4.3 – Senha complexa

Senha de frase-passe

- Deve conter:
 - Mínimo de 10 caracteres
 - Máximo de 64 caracteres

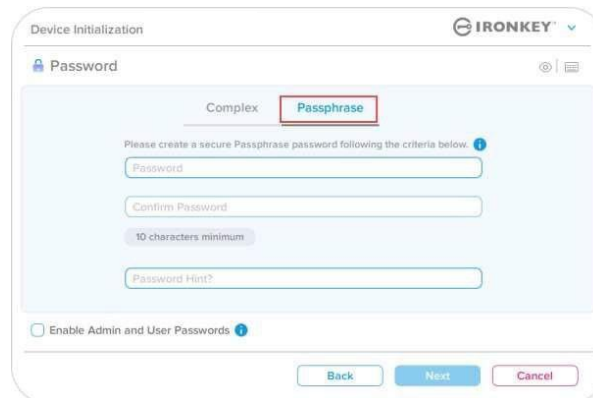


Figura 4.4 - Senha de frase-passe

Dica de senha (Opcional)

Uma Dica de senha pode ser útil para fornecer uma pista sobre a senha, se algum dia ela for esquecida.

Observação: A dica NÃO pode ser exatamente a mesma que a senha.

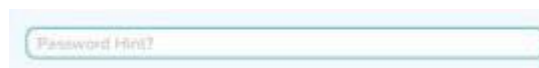


Figura 4.5 – Campo da dica de senha

Inicialização do dispositivo

Senhas válidas e inválidas

Para senhas **válidas**, as Caixas de critério de senha ficarão **verdes** quando o critério for seguido. (Ver Figuras 4.6a-b) Observação: Quando o mínimo de três critérios de senha forem seguidos, a quarta caixa de critérios ficará cinza, indicando que este critério é opcional (Figura 4.6b)

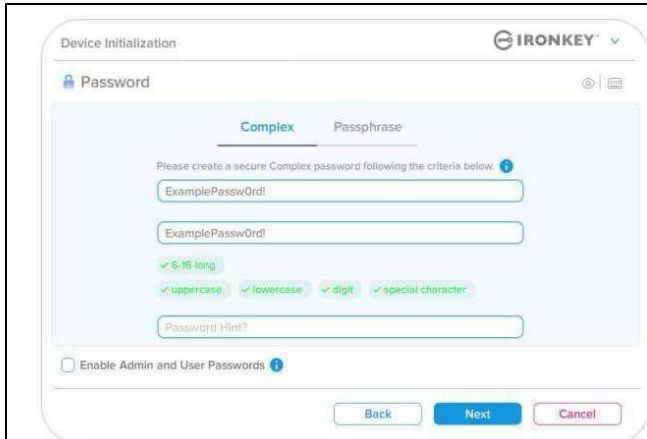


Figura 4.6a – Condição de senha complexa atendida

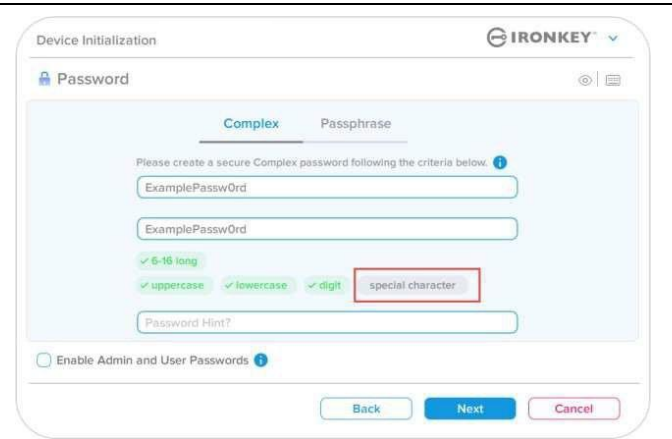


Figura 4.6b – Condição de senha complexa opcional

Para senhas **inválidas**, as Caixas de critério de senha ficarão **vermelhas** e o botão **Avançar** será desabilitado até que os requisitos mínimos sejam atendidos.

Isso se aplica às senhas complexas e de frase-passe.

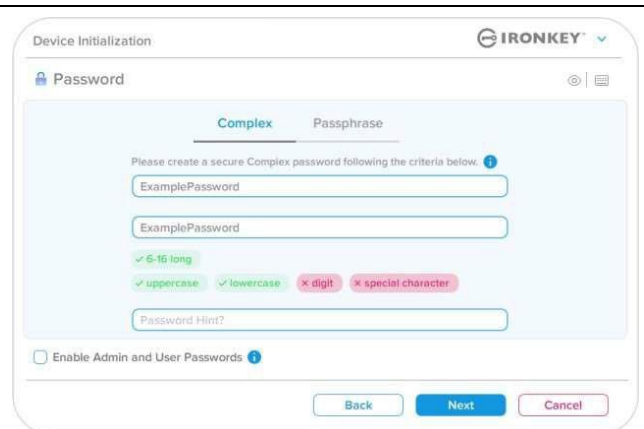


Figura 4.7 – Condições de senha não atendidas

Inicialização do dispositivo

Teclado virtual

O LP50G2 oferece um Teclado virtual que pode ser utilizado para proteção contra registros de toque do teclado (keylogger).

- Para usar o **Teclado virtual**, localize o botão de teclado do lado superior direito da tela de **Inicialização do dispositivo** e clique nele.

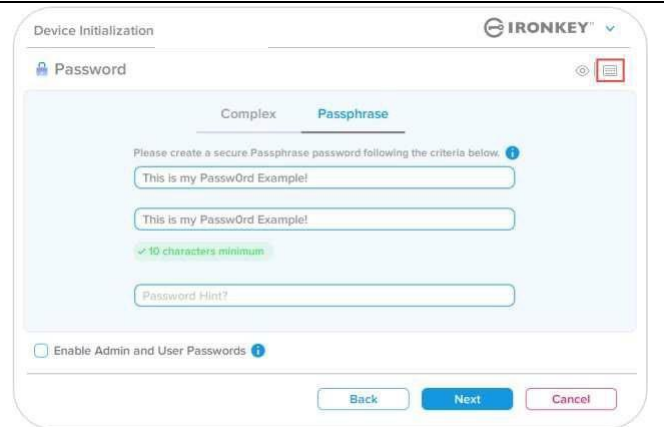


Figura 4.8 – Ativando o Teclado virtual

- Quando o teclado virtual aparecer, você também pode habilitar a **Proteção contra registros da tela**. Ao usar esse recurso, todas as teclas ficarão brevemente em branco. Isso é um comportamento esperado, já que previne que invasores registrem a tela quando você clicar nas teclas.
- Para fazer com que este recurso seja mais sólido, você também pode escolher randomizar o teclado virtual selecionando **randomize** (randomizar) na parte inferior direita do teclado. A Randomização vai ordenar as teclas em uma ordem aleatória.



Figura 4.9 – Proteção contra registro de tela / Randomização

Inicialização do dispositivo

Botão de visibilidade de senha

Por padrão, quando você cria uma senha, a sequência da senha será mostrada no campo conforme você digitou. Se você quiser “ocultar” a sequência de senha como você digitou, você pode fazer isso acionando o botão de “olho” da senha localizado no lado superior direito da janela de Inicialização do dispositivo.

Observação: Após o dispositivo ser inicializado, o campo de senha ficará no padrão “oculto”.

Para **ocultar** a sequência de senha, clique no ícone cinza.

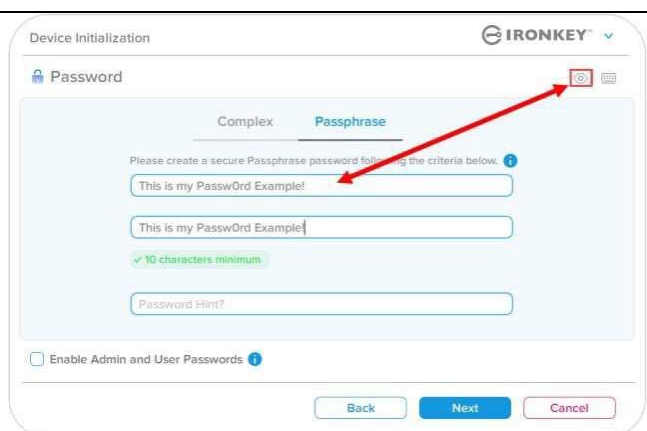


Figura 4.10 – Botão para “ocultar” a Senha

Para **exibir** a senha oculta, clique no ícone azul.

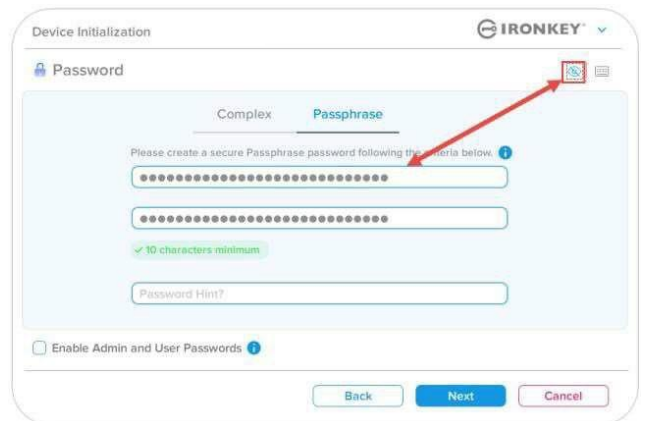


Figura 4.11 – Botão para “exibir” a Senha

Inicialização do dispositivo

Senhas de Admin e de Usuário

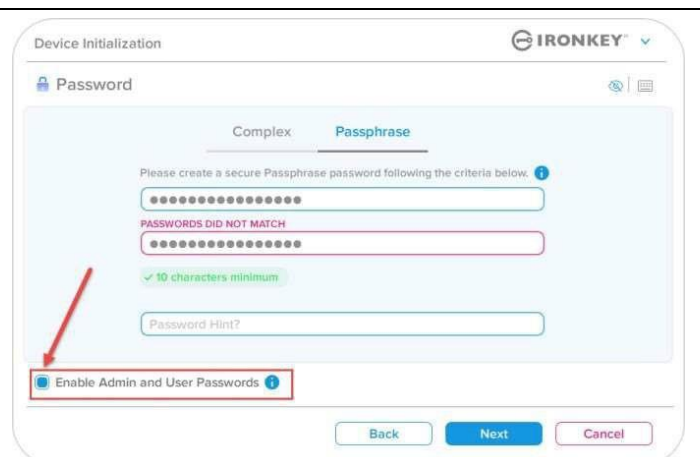
Ao habilitar as senhas de Admin e de Usuário, você pode utilizar a funcionalidade multissenhas, na qual a função de Admin pode administrar ambas as contas. Selecionar “**Habilitar senhas de Admin e de Usuário**” permite um método alternativo de acesso ao drive em caso de uma das senhas ser esquecida.

Com as **senhas de Admin e de Usuário** habilitadas, você também pode acessar:

- Redefinição da senha de Usuário

Para saber mais sobre o recurso da senha de Usuário, vá até a página 24 dentro deste guia do usuário.

- Para habilitar as **senhas de Admin e de Usuário** clique na caixa próxima a “**Habilitar as senhas de Admin e de Usuário**” e selecione **Avançar** assim que uma senha válida for escolhida. (Figura 4.12)
- Se este recurso estiver **habilitado**, então a senha escolhida neste tela será a **senha de Admin**. Clique em **Avançar** para continuar para a tela da **senha de Usuário** onde uma senha é escolhida para o Usuário.



4.12 – Habilitando as senhas de Admin e de Usuário

Observação: Habilitar as senhas de Admin e de Usuário é opcional.

Se o drive estiver configurado com este recurso NÃO habilitado (caixa desmarcada), então o drive será configurado como um **Usuário único**, drive de **Senha única sem qualquer recurso de Admin**. Esta configuração será chamada de **Modo Somente Usuário** ao longo deste manual.

Para continuar com um Usuário único, configuração de senha única, mantenha **Habilitar senhas de Admin e de Usuário** desmarcado, e clique em **Avançar** depois de criar uma senha válida.

Inicialização do dispositivo

Senhas de Admin e de Usuário

Se a função de Admin foi **habilitada** na tela anterior, a tela seguinte pedirá a senha de Usuário **Senha de Usuário** (Figure 4.13) A Senha de Usuário terá capacidades limitadas em comparação com a do Admin e será discutida com mais detalhes posteriormente. **Observação:** As “**Senhas de Admin e de Usuário**” serão mencionadas como “**Função de Admin**” durante todo este manual para o restante deste documento.

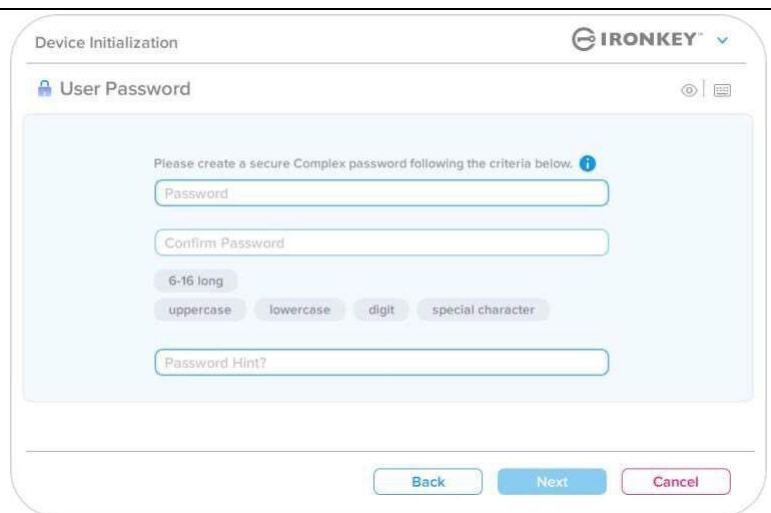


Figura 4.13 – Senha de Usuário (Admin e Usuário habilitados)

Observação: O critério da Opção de Senha escolhida (complexa ou frase-passe) vai se estender à Senha de Usuário, e a qualquer redefinição de senhas necessárias depois que o drive for instalado. A opção de senha escolhida pode ser alterada apenas depois de uma completa restauração do dispositivo.

Inicialização do dispositivo

Informações de contato

Insira suas informações de contato nas caixas de texto fornecidas. (Ver Figura 4.14)

Observação: As informações que você digitar nesses campos NÃO podem conter a sequência de senha que você criou no Passo 3. Entretanto, esses campos são opcionais e podem ser deixados em branco se desejar.

O campo do “**Nome**” pode conter até 32 caracteres, mas não pode conter a senha **exata**.

O campo da “**Empresa**” pode conter até 32 caracteres, mas não pode conter a senha **exata**.

O campo “**Detalhes**” pode conter até 156 caracteres, mas não pode conter a senha **exata**.

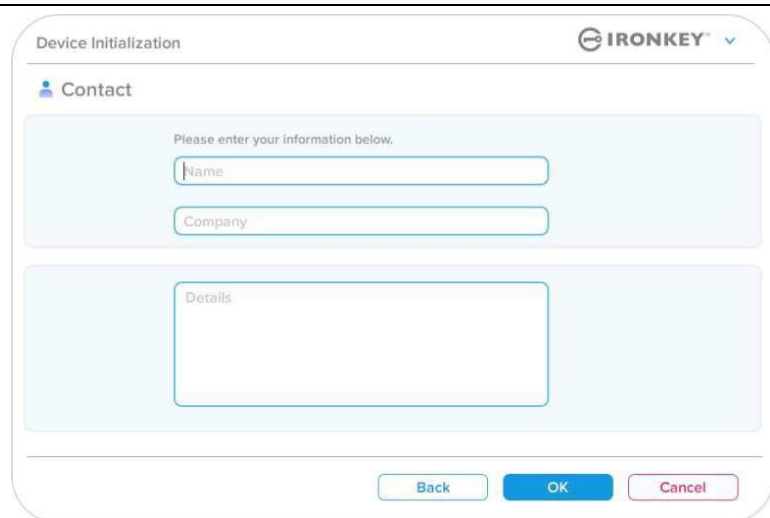
The screenshot shows a 'Device Initialization' window with the IronKey logo in the top right. Below the title bar, there is a 'Contact' section with a person icon. A prompt says 'Please enter your information below.' There are three input fields: 'Name', 'Company', and 'Details'. The 'Name' and 'Company' fields are short text boxes, while 'Details' is a larger text area. At the bottom of the window, there are three buttons: 'Back', 'OK', and 'Cancel'.

Figura 4.14 – Informações de contato

Observação: Clicar em “OK” vai concluir o processo de inicialização e prosseguir para desbloquear, depois prepare a partição segura onde seus dados possam ser armazenados com segurança. Prosseguir para desconectar o drive e conectá-lo de volta ao sistema para ver as mudanças refletidas.

Uso do dispositivo (Ambiente Windows e macOS)

Login para Admin e Usuário (Admin habilitado)

Se o dispositivo for inicializado com as senhas de Admin e de Usuário (função de Admin) habilitadas, o aplicativo IronKey LP50G2 vai iniciar, iniciando a tela de login da Senha de Usuário primeiro. A partir daqui você pode fazer login com a Senha de Usuário, visualizar qualquer informação de contato inserida ou fazer login como Admin (*Figura 6.1*). Clicando no botão de “Login como Admin” (mostrado abaixo) o aplicativo prosseguirá para o menu de login do Admin onde você pode fazer login como Admin para acessar os recursos e configurações do Admin (*Figura 6.2*).

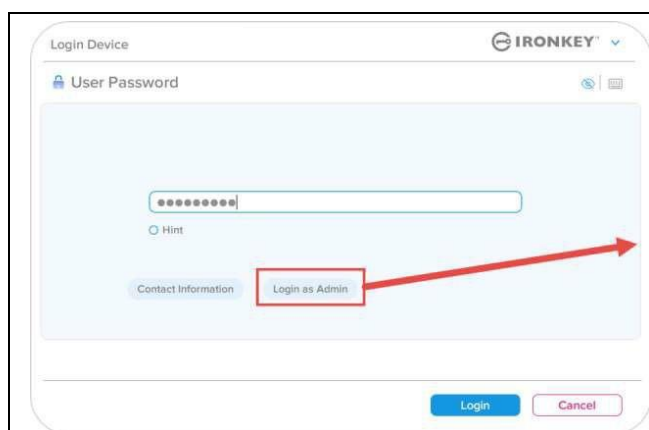


Figura 6.1 – Login de Senha de Usuário (Admin habilitado)

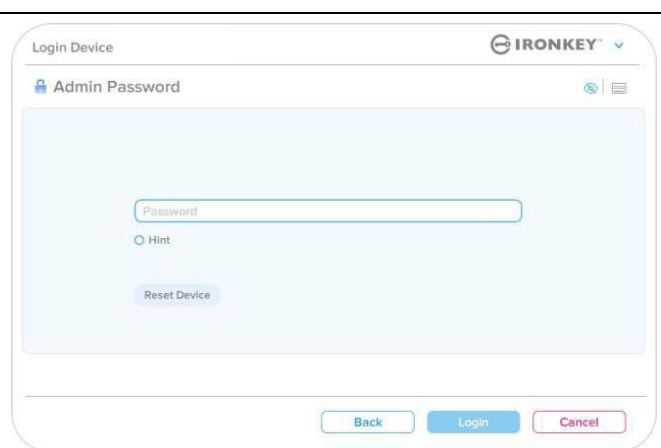


Figura 6.2 – Login de senha do Admin

Login para modo Somente Usuário (Admin não habilitado)

Como mencionado anteriormente na **Página 13**, embora seja recomendado usar a funcionalidade da Função de Admin para obter todos os benefícios de seu dispositivo, o drive IronKey também pode ser iniciado em uma configuração Somente Usuário (Senha única, Usuário único). Essa é uma opção para aqueles que gostariam simplesmente de uma abordagem de senha única para proteger os dados em seu drive. (*Figura 6.3*)

Observação: Para habilitar as Senhas de Admin e de Usuário, use o botão **Restaurar dispositivo** para colocar o drive de volta ao estado de inicialização onde você pode habilitar as Senhas de Admin e de Usuário. **TODOS os dados o drive serão formatados e perdidos para sempre quando ocorre a Restauração do dispositivo.**

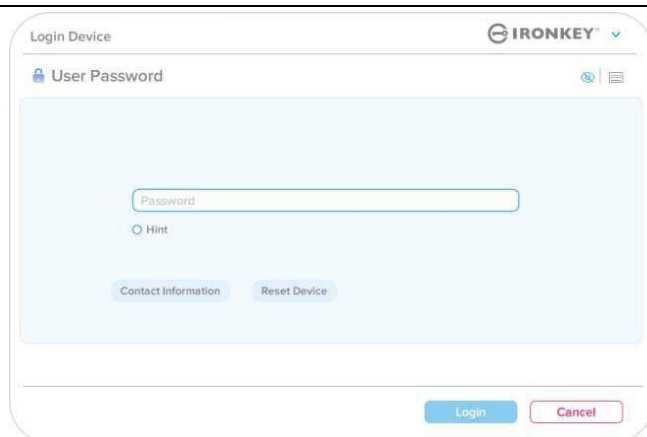


Figura 6.3 – Login de Senha de Usuário (Admin não habilitado)

Uso do dispositivo

Proteção de ataque de força bruta

Importante: Durante o login, se for digitada uma senha incorreta, você terá outra oportunidade para digitar a senha correta; entretanto há um recurso de segurança integrado (também conhecido como proteção de ataque de força bruta) que monitora o número de tentativas erradas de login. *

Se esse número alcançar o valor pré-configurado de 10 tentativas erradas de senha, o comportamento será o seguinte:

Admin/Usuário habilitado	Comportamento do dispositivo para proteção contra força bruta (10 tentativas de senha incorretas)	Apagamento de Dados e Restauração de Dispositivo?
Senha de Usuário:	Bloqueio de senha. Fazer login como Admin para redefinir a Senha de Usuário	NÃO
Senha de Admin	Apagar drive criptograficamente, Senhas, configurações e dados apagados para sempre	SIM
Somente usuário Usuário Único, Senha Única (Admin/Usuário <u>NÃO</u> habilitados)	Comportamento do dispositivo para proteção contra força bruta (10 tentativas de senha incorretas)	Apagamento de Dados e Restauração de Dispositivo?
Senha de Usuário	Exclusão criptográfica de drive, senhas, configurações e dados excluídos para sempre	SIM

* Depois que você fizer a autenticação no dispositivo corretamente, o contador de erros de login será reiniciado em relação ao método de Login foi utilizado. Excluir criptograficamente excluirá todas as senhas, dados e chaves de criptografia – **seus dados serão perdidos para sempre.**

Acessar meus arquivos seguros

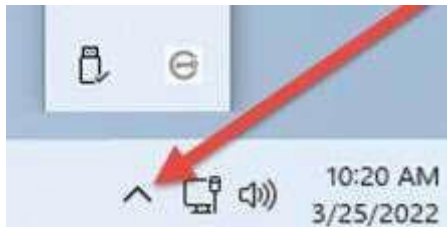
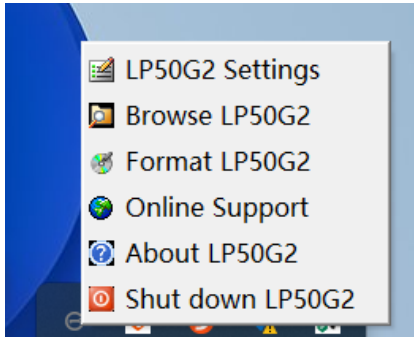
Depois de desbloquear o dispositivo, você pode acessar seus arquivos seguros. Os arquivos são automaticamente criptografados e descriptografados quando você salva ou abre os arquivos no drive. Esta tecnologia facilita que você trabalhe normalmente como em um drive comum, enquanto tem segurança forte e ininterrupta garantida.

Dica: Você também pode acessar seus arquivos clicando com o botão direito no ícone do IronKey na barra de tarefas do Windows e clicando em **Browse (Navegar) LP50G2** (Figura 7.2)

Opções do dispositivo - (Ambiente Windows)

Enquanto você estiver logado no dispositivo, haverá um ícone IronKey localizado no canto direito da janela. Clicar com o botão direito no Ícone IronKey abrirá o menu de seleção para Opções do drive disponíveis (*Figura 6.2*).

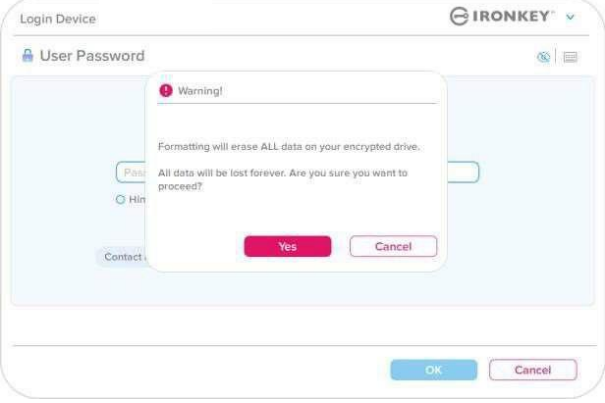
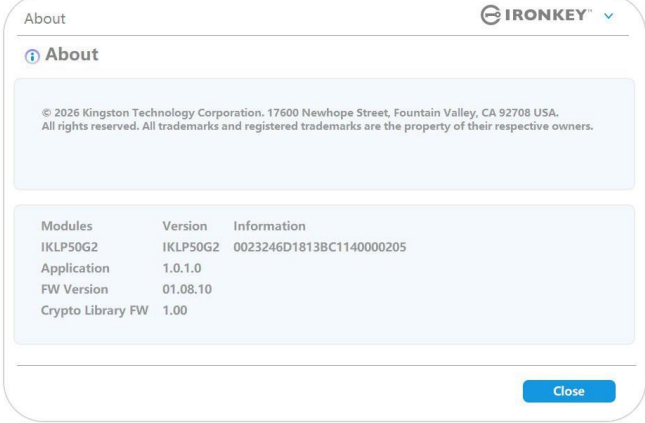
Detalhes sobre essas opções do dispositivo podem ser encontradas nas Páginas 19-23 deste manual.

• Enquanto você estiver logado no dispositivo, haverá um ícone IronKey localizado no canto direito da janela. (<i>Figura 7.1</i>)	 Figura 7.1 – Ícone IronKey na barra de tarefas
• Clicar com o botão direito no Ícone IronKey abrirá o menu de seleção para opções do drive disponíveis. (<i>Figura 7.2</i>) Detalhes sobre essas opções do dispositivo podem ser encontradas nas páginas 19-23 deste manual.	 Figura 7.2 – Clique com o botão direito no ícone IronKey para opções do dispositivo

Opções do dispositivo - (Ambiente macOS)

• Enquanto você estiver logado no dispositivo, haverá um ícone IronKey LP50G2 localizado no menu do macOS visto na Figura 7.3 que abrirá as opções de dispositivo disponíveis. Detalhes sobre essas opções do dispositivo podem ser encontradas nas Páginas 19-23 deste manual.	 Figura 7.3 – Menu de opções do dispositivo/Ícone da barra de menu do macOS
--	---

Opções do dispositivo

Configurações do LP50G2:	Alterar senha de login, Informações de contato e outras configurações. (Mais detalhes sobre configurações do dispositivo podem ser encontrados na seção “Configurações do LP50G2” deste manual).
Browse (Navegar) LP50G2:	Permite que você visualize seus arquivos de segurança.
Formatar o LP50G2: Permite que você formate a partição de dados segura. (Aviso: Todos os dados serão apagados.) (Figura 6.1) Observação: A autenticação da senha será exigida para formatar.	 Figura 7.4 – Formatar o LP50G2
Suporte on-line:	Abre seu navegador de internet e vai para http://www.kingston.com/support onde você pode acessar as informações de suporte adicionais.
Sobre o LP50G2: Fornece detalhes específicos sobre o LP50G2, incluindo Aplicação, Firmware e Informações de número de série (Figura 6.2) Observação: O número de série único do drive estará na “Coluna de informações”	 Figura 7.5 – Sobre o LP50G2
Desligar o LP50G2:	Encerra de modo apropriado o LP50G2, permitindo que seja removido com segurança do seu sistema.

Configurações do LP50G2

Configurações do Admin

O login do Admin permite acesso às seguintes configurações do dispositivo:

- **Senha:** Permite que você altere sua própria senha de Admin e/ou dica (*Figura 8.1*)
- **Informações de contato:** Permite que você adicione/visualize/altere suas informações de contato (*Figura 8.2*)
- **Idioma:** Permite que você altere sua seleção de idioma atual (*Figura 8.3*)
- **Opções do Admin:** Permite que você acesse recursos adicionais como:
 - Alterar Senha de Usuário (*Figura 8.4*)

OBSERVAÇÃO: Detalhes adicionais das Opções do Admin podem ser encontradas na página 25.

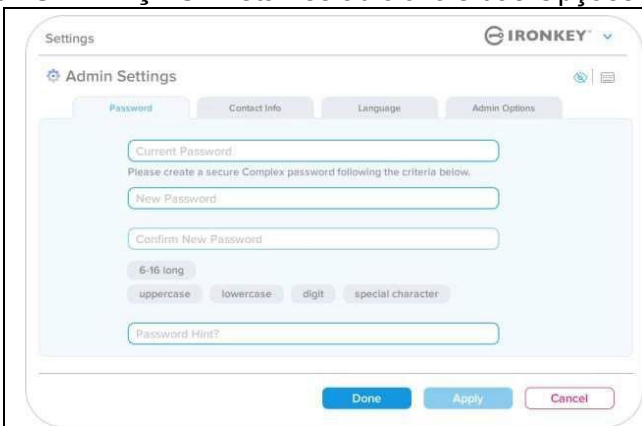


Figura 8.1 – Opções de senha do Admin

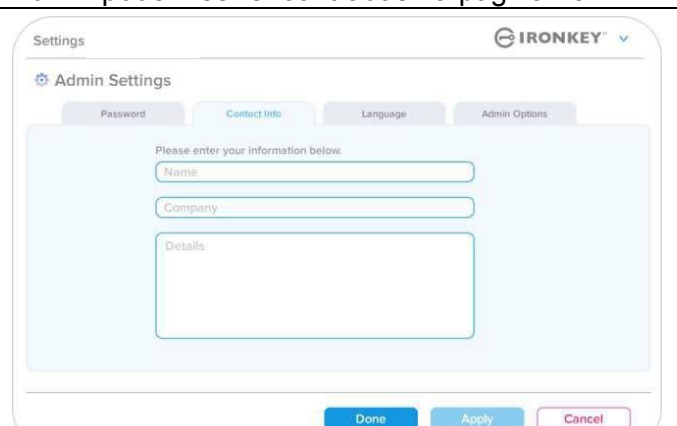


Figura 8.2 – Informações de contato

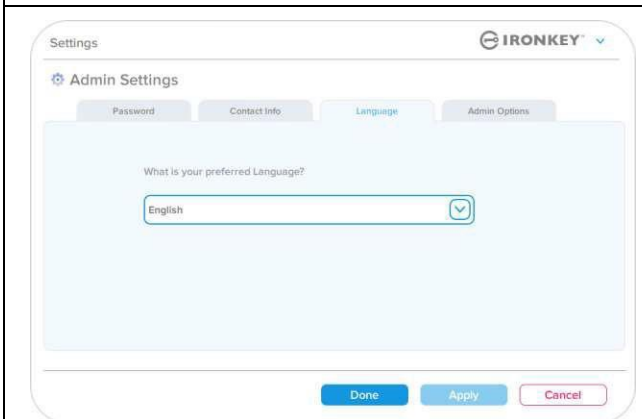


Figura 8.3 – Opções de idioma

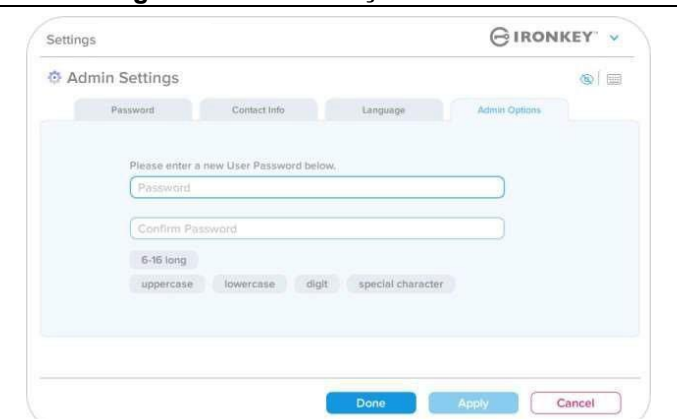


Figura 8.4 – Opções do Admin

Configurações do LP50G2

Configurações do Usuário: Admin habilitado

O login do Usuário limita o acesso às seguintes configurações:

Senha:

Permite que você altere sua própria senha de Usuário e/ou dica.
(Figura 8.5)

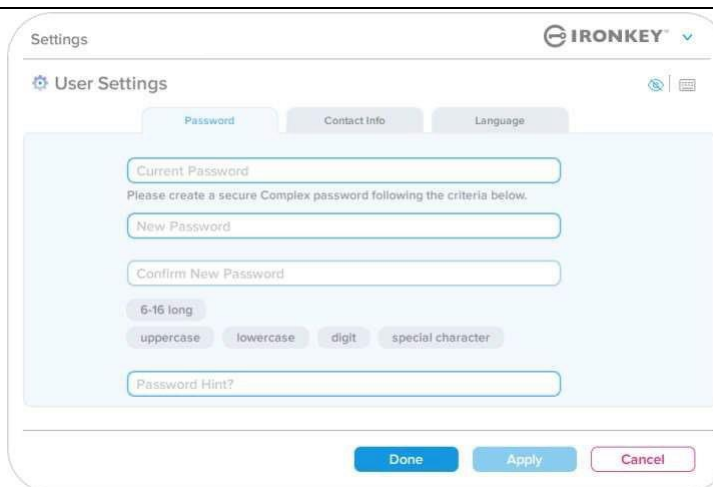


Figura 8.5 – Opções de senha (Admin habilitado: Login do Usuário)

Informações de contato:

Permite que você adicione/visualize/altere suas informações de contato. (Figura 8.6)

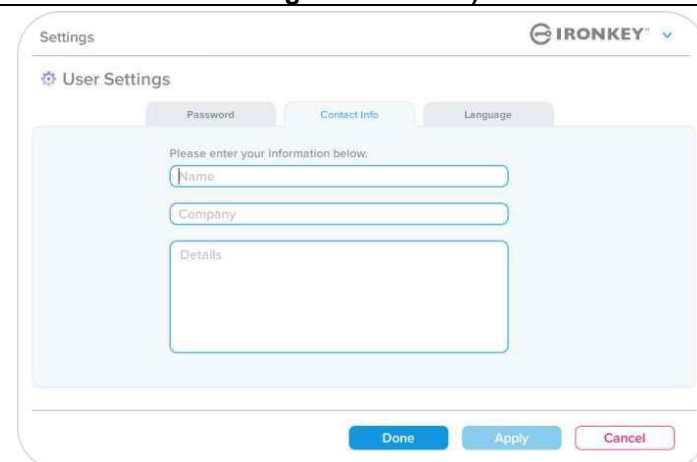


Figura 8.6 – Informações de contato (Admin habilitado: Login do Usuário)

Idioma:

Permite que você altere sua seleção de idioma atual.
(Figura 8.7)

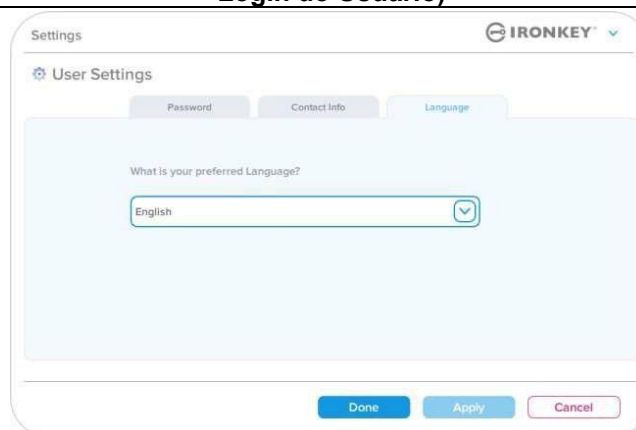


Figura 8.7 – Configurações de Idioma (Admin habilitado: Login do Usuário)

Observação: As opções do Admin não estão acessíveis quando logado com a senha de Usuário.

Configurações do LP50G2

Configurações do Usuário: Admin não habilitado

Como mencionado anteriormente na Página 12, iniciar o LP50G2 sem habilitar as senhas de “Admin e Usuário” vai configurar o drive em uma **configuração de Senha única, Usuário único**. Esta configuração não possui acesso a qualquer recurso ou opção do Admin. Esta configuração terá acesso às seguintes configurações do LP50G2.

Senha

Permite que você altere sua própria senha de Usuário e/ou dica. (Figura 8.8)

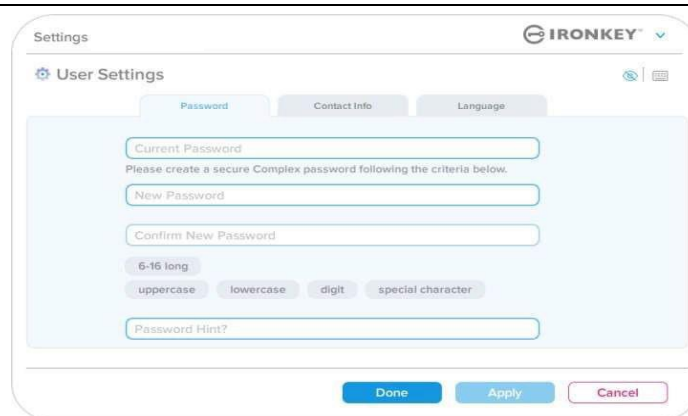


Figura 8.8 – Opções de Senha (Modo Somente Usuário)

Informações de contato:

Permite que você adicione/visualize/altere suas informações de contato. (Figura 8.9)

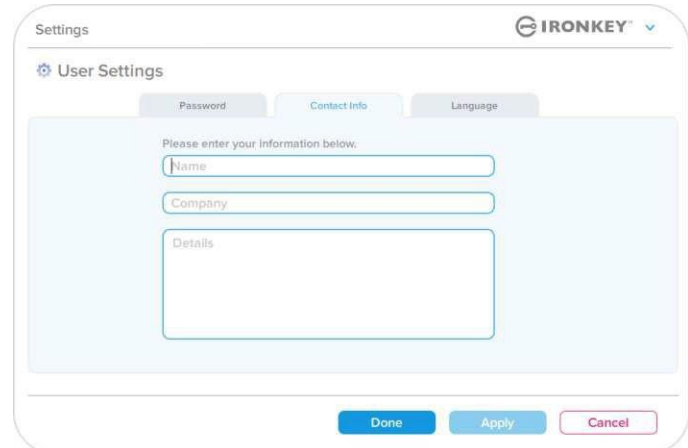


Figura 8.9 – Informações de contato (Modo Somente Usuário)

Idioma:

Permite que você altere sua seleção de idioma atual. (Figura 8.10)

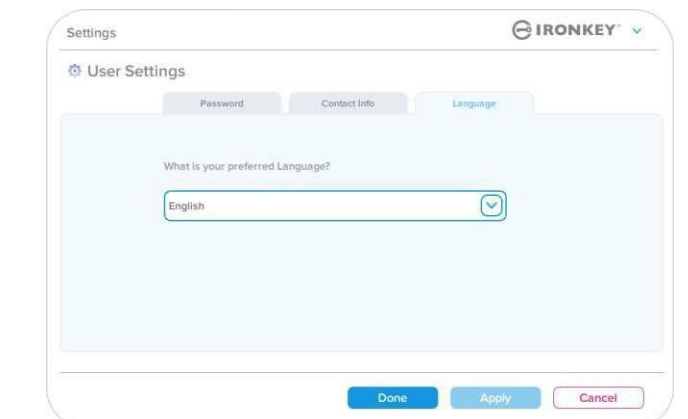


Figura 8.10 – Definições de Idioma (Modo Somente Usuário)

Configurações do LP50G2

Alterar e Salvar configurações

- Sempre que as configurações forem alteradas nas Configurações do LP50G2 (por ex., Informações de contato, idioma, alteração de senha, opções do Admin etc.), o drive pedirá para que você insira sua senha para aceitar e aplicar as alterações. (Ver Figura 8.11)

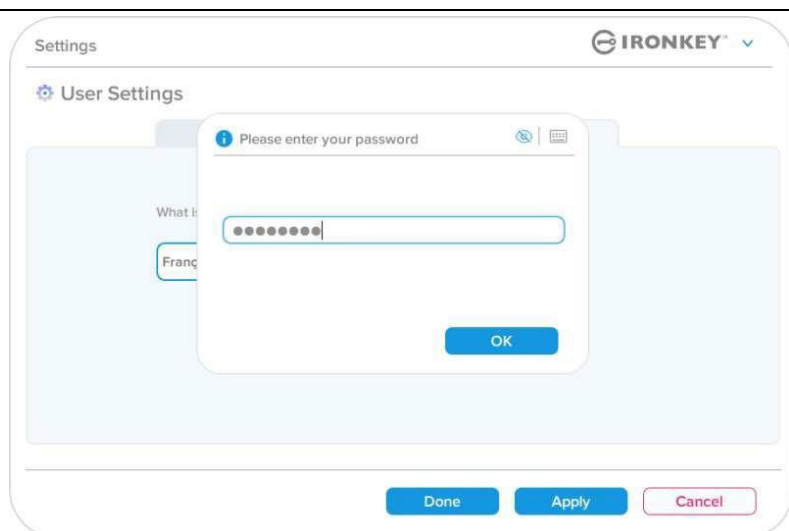


Figura 8.11 – Tela de alerta de Senha para salvar as alterações de configurações do LP50G2

Observação: Se você estiver na tela de alerta de Senha acima e gostaria de cancelar ou modificar suas alterações, você pode fazer isso simplesmente deixando o campo de senha em branco e clicando em “OK”. Isso vai fechar a caixa “Insira sua senha” e voltar para o menu de configurações do LP50G2.

Recursos do Admin

Opção disponível para redefinir a senha de Usuário

Um dos recursos úteis da configuração de Admin permite que você redefina a Senha de Usuários com segurança, caso ela tenha sido esquecida. Abaixo está o recurso de Redefinição da senha de Usuário que pode ser útil para redefinir a senha de Usuário:

Redefinição da senha de Usuário:

Altere manualmente a Senha de Usuário no menu de “Opções do Admin”, que é uma mudança instantânea e fará efeito no próximo login de Usuário. (Figura 9.1)

Observação: Os critérios de exigência de senha não cumprirão os critérios originais que foram definidos durante o processo de inicialização (opções de frase-passe ou complexa).

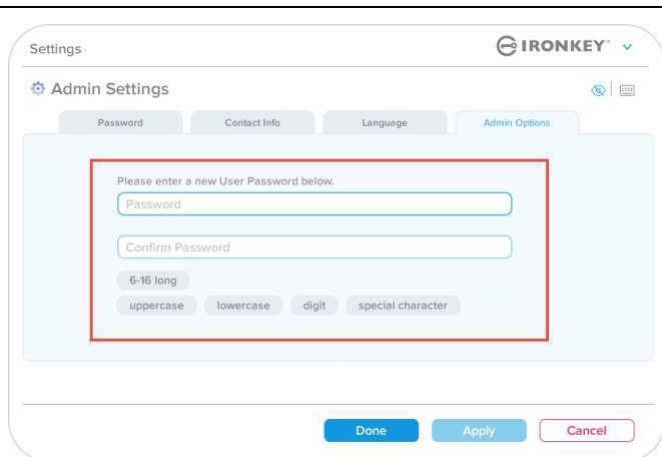


Figura 9.1 – Redefinição de Senha de Usuário/ Opções do Admin

Ajuda e Resolução de Problemas

Bloqueio do dispositivo

O LP50G2 inclui um recurso de segurança que previne acesso não autorizado à partição de dados quando um número máximo de tentativas erradas de login **consecutivas** (abreviado como **MaxNoA**) foi feito. A configuração padrão de fábrica tem um valor pré-configurado de 10 (nº de tentativas) para cada método de Login (Usuário/Admin).

O contador de “bloqueio” monitora cada login malsucedido e redefine **de uma das duas** maneiras:

1. Um login bem-sucedido antes de atingir o MaxNoA
2. Atingindo o MaxNoA e realizando um bloqueio de dispositivo ou formatação de dispositivo dependendo de como o drive for configurado.

- Se uma senha incorreta for inserida, uma mensagem de erro vai aparecer em vermelho logo acima do campo de entrada de senha, indicando uma falha no login. (Figura 10.1)

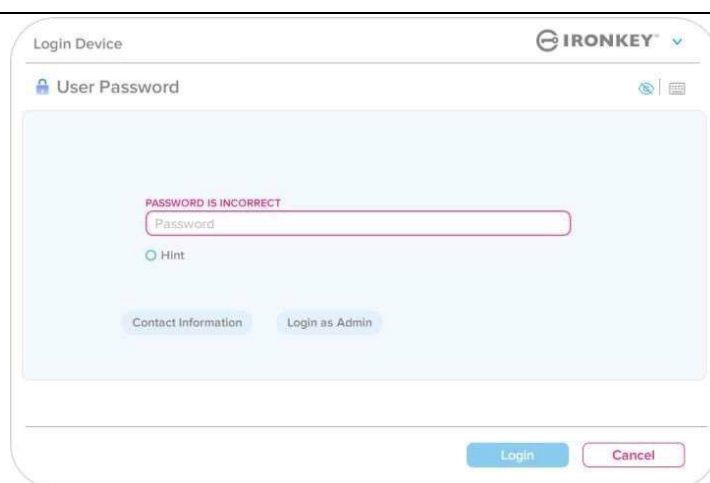


Figura 10.1 – Mensagem de senha incorreta

- Quando a 7ª tentativa errada for feita, você verá uma mensagem de erro adicional indicando que você tem mais 3 tentativas antes de chegar ao MaxNoA (que é 10 por padrão). (Figura 10.2)

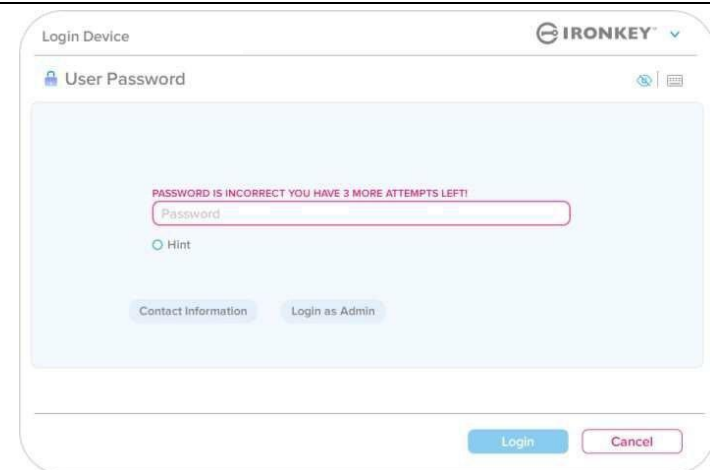


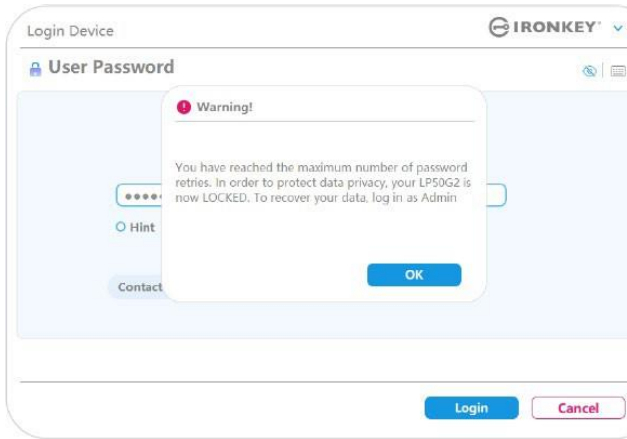
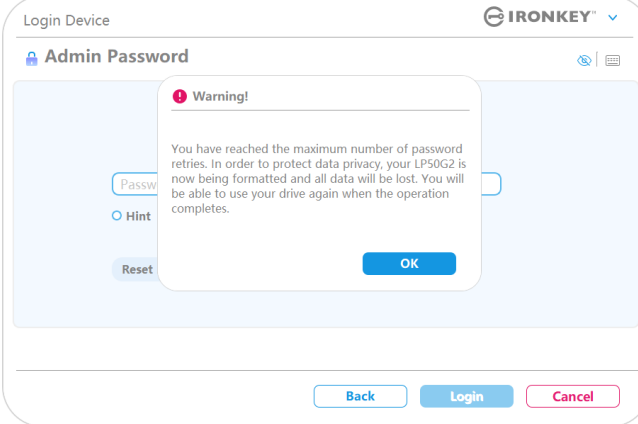
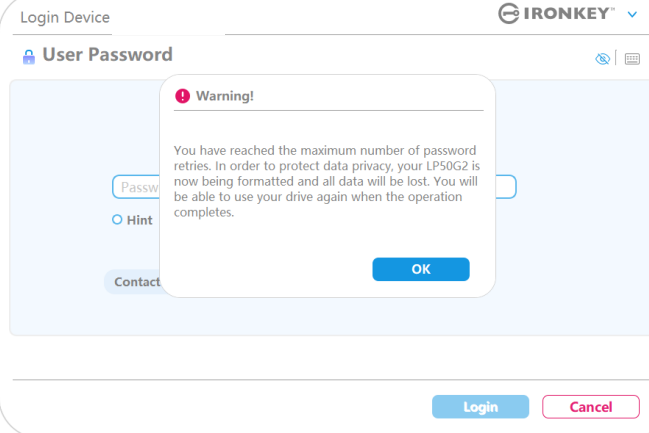
Figura 10.2 – 7ª tentativa de senha incorreta

Ajuda e Resolução de Problemas

Bloqueio do dispositivo

Importante: Depois da 10ª e última tentativa de login errada, dependendo de como o dispositivo foi configurado e método de login utilizado (Usuário/Admin), o dispositivo vai fechar, exigindo que você faça login por um método alternativo (se aplicável) ou uma Restauração de Dispositivo que **formatará os dados e todos os dados no drive serão perdidos para sempre.** Comportamentos também mencionados na página 17 desde Guia do Usuário.

As Figuras 10.3 a 10.6 abaixo demonstram o comportamento visual do 10º e último login errado de cada método de senha de login:

Senha de Usuário: (Admin/Usuário habilitado)  BLOQUEIO DO DISPOSITIVO Figura 10.3	Senha do Admin (Admin/Usuário habilitado)  FORMATAÇÃO DO DISPOSITIVO* Figura 10.4
Essas medidas de segurança impedem que alguém (que não tenha a sua senha) faça incontáveis tentativas de login e consiga acesso aos seus dados confidenciais (também conhecido como ataque de força bruta). Se você for o proprietário do LP50G2 e esquecer sua senha, as mesmas medidas de segurança serão aplicadas, incluindo a formatação do dispositivo. * Para mais sobre este recurso, veja “Restaurar Dispositivo” na página 27.	Senha de Usuário (Admin NÃO habilitado)  FORMATAÇÃO DO DISPOSITIVO* Figura 10.5

***Observação:** Uma formatação de dispositivo apagará **TODAS** as informações armazenadas na partição de dados segura do LP50G2.

Ajuda e Resolução de Problemas

Restaurar dispositivo

Se você esqueceu a sua senha ou precisa restaurar seu dispositivo, você pode clicar no botão “*Restaurar Dispositivo*” que aparece em um dos dois lugares dependendo de como o drive está configurado (no menu de Senha de Login do Admin se o Admin/Usuário estiver habilitado, ou no menu de Login de “Senha de Usuário” se o modo Admin/Usuário não estiver habilitado) quando o iniciador do theLP50G2 for executado. (Ver Figura 10.7 e 10.8)

- Esta opção vai permitir que você crie uma nova senha, mas para proteger a privacidade de seus dados, o LP50G2 será formatado. Isso significa que todos os seus dados serão apagados no processo.*

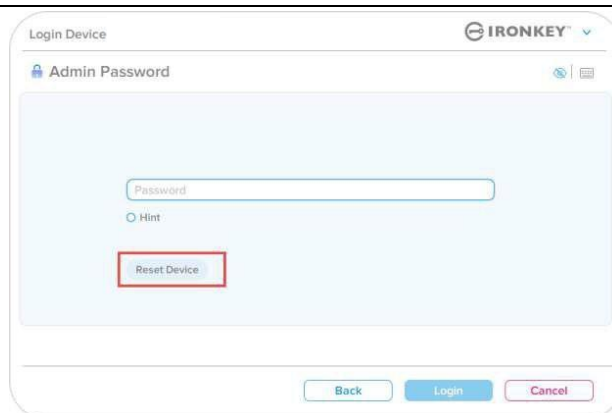


Figura 10.6 – Senha do Admin: Botão para Restaurar Dispositivo

- Observação:** Quando você clicar em “*Restaurar Dispositivo*”, uma caixa de mensagem vai aparecer e perguntar se você deseja inserir uma nova senha antes de executar a formatação. Nesse ponto, você pode 1) clicar em “OK” para confirmar ou 2) clicar em “Cancelar” para voltar para a janela de login. (Ver Figura 10.8)

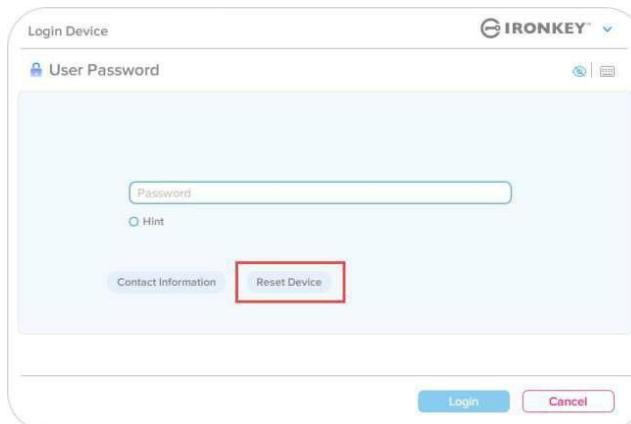


Figura 10.7 – Senha de Usuário (Admin/Usuário não habilitado) Restaurar Dispositivo

- Se você optar por continuar, você será levado para a tela de inicialização onde você pode habilitar os “modos de Admin e Usuário” e inserir sua nova senha com base na opção de Senha que escolher (Complexa ou Frase-passe). A dica não é um campo obrigatório, mas pode ser útil para fornecer uma pista sobre a senha, se algum dia ela for esquecida.

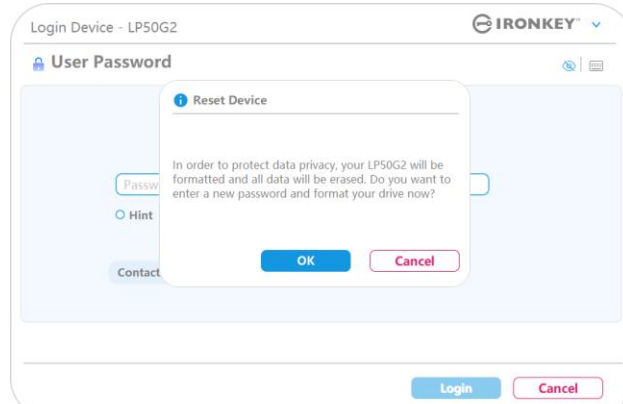


Figura 10.8 – Confirmação para Restaurar Dispositivo

Conflito de letra do drive: Sistema operacional Windows

- Como mencionado na seção de “*Requisitos do Sistema*” deste manual (na página 4), o LP50G2 precisa de duas letras de drive consecutivas DEPOIS do último disco físico que aparece antes do “intervalo” nas atribuições de letra do drive (ver *Figura 10.9*.) Isto NÃO está relacionado com compartilhamentos de rede porque eles são específicos aos perfis de usuário e não ao próprio perfil de hardware de sistema, aparecendo assim disponível no Sistema Operacional.
- Isso significa que, o Windows pode atribuir ao LP50G2 uma letra de drive que já está em uso por um compartilhamento de rede ou caminho de Convenção de Nomenclatura Universal (UNC), causando um conflito de letra de drive. Se isto ocorrer, consulte o seu administrador ou departamento de assistência técnica para alterar a atribuição das letras de drive no Gerenciamento do Disco do Windows (necessários privilégios de administrador).

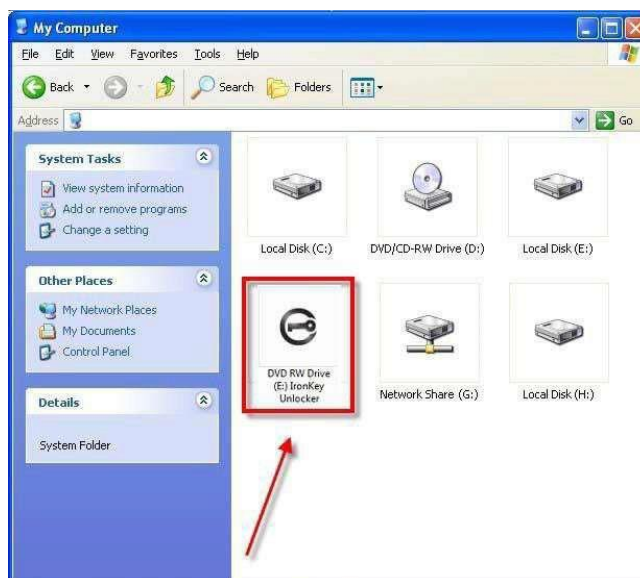


Figura 10.9 – Exemplo de letra de drive

Neste exemplo, (*Figura 10.9*), o LP50G2 utiliza o drive F:, que é a primeira letra de drive disponível após o drive E: (o último disco físico antes do intervalo de letra de drive.) Como a letra G: é um compartilhamento de rede e não faz parte do perfil de hardware, o LP50G2 pode tentar utilizá-lo como sua segunda letra de drive, causando um conflito.

Se não existirem compartilhamentos de rede no seu sistema e o LP50G2 continuar não iniciando, é possível que um leitor de cartões, um disco removível ou outro dispositivo previamente instalado esteja mantendo a letra de unidade atribuída e causando o conflito.

Observe que o Gerenciamento de Letra de Drive, ou DLM, melhorou significativamente no Windows 11 então pode ser que você não encontre este problema, mas se não conseguir resolver o conflito, entre em contato com o Departamento de Suporte Técnico da Kingston ou visite o site Kingston.com/support para mais assistência.



BEZPIECZNA PAMIĘĆ USB 3.2
Gen 1 IRONKEY™ Locker+ 50 G2
(LP50G2)

Instrukcja obsługi



Spis treści

Wprowadzenie	3
Charakterystyka pamięci Locker+ 50 G2	4
Informacje o tej instrukcji	4
Wymagania systemowe	4
Zalecenia	5
Używanie prawidłowego systemu plików	5
Zalecenia dotyczące użytkowania	5
Najlepsze metody konfiguracji hasła	6
Konfiguracja urządzenia	7
Dostęp do urządzenia (środowisko Windows)	7
Dostęp do urządzenia (środowisko macOS)	7
Inicjalizacja urządzenia (środowiska Windows i macOS)	8
Wybór hasła	9
Wirtualna klawiatura	11
Przełącznik widoczności hasła	12
Hasła administratora i użytkownika	13
Informacje kontaktowe	15
Korzystanie z urządzenia (środowiska Windows i macOS)	16
Logowanie administratora i użytkownika (włączony tryb administratora)	16
Logowanie w trybie Tylko użytkownik (wyłączony tryb administratora)	16
Ochrona przed atakami Brute Force	17
Dostęp do zabezpieczonych plików	17
Opcje urządzenia	18
Ustawienia urządzenia LP50G2	20
Ustawienia administratora	20
Ustawienia użytkownika: włączony tryb administratora	21
Ustawienia użytkownika: wyłączony tryb administratora	22
Zmiana i zapisywanie ustawień urządzenia LP50G2	23
Funkcje administracyjne	24
Resetowanie hasła użytkownika	24
Pomoc i rozwiązywanie problemów	25
Blokada urządzenia LP50G2	25
Resetowanie urządzenia LP50G2	27
Konflikt liter dysku (Windows)	28



Ilustracja 1 – Urządzenie IronKey LP50G2

Wprowadzenie

Pamięć USB Kingston IronKey™ Locker+ 50 G2 oferuje zabezpieczenia klasy korporacyjnej z 256-bitowym szyfrowaniem sprzętowym AES w trybie XTS z certyfikatem FIPS 197, w tym ochronę przed atakami BadUSB i Brute Force z wykorzystaniem hasła. Pamięć LP50G2 jest również zgodna z przepisami TAA.

Pamięć LP50G2 obsługuje obecnie opcję wielu haseł (administratora i użytkownika) w trybie haseł złożonych lub wyrażeń hasłowych. Tryb haseł złożonych umożliwia wprowadzanie haseł składających się z 6–16 znaków należących do 3 z 4 zestawów znaków. Nowy tryb wyrażeń hasłowych umożliwia wprowadzenie numeru PIN, zdania, listy słów, a nawet tekstu piosenki o długości od 10 do 64 znaków. Administrator może włączyć hasło użytkownika lub je zresetować w celu przywrócenia dostępu do danych. Aby ułatwić wpisywanie hasła, można włączyć symbol oka, dzięki czemu hasło staje się widoczne, co zmniejsza ryzyko popełnienia literówek skutkujących nieudanymi próbami logowania. Funkcja ochrony przed atakami siłowymi (Brute Force) blokuje użytkownika po 10 kolejnych próbach wprowadzenia nieprawidłowego hasła, a po 10 kolejnych próbach wprowadzenia błędnego hasła administratora kryptograficznie wymazuje pamięć. Ponadto wbudowana wirtualna klawiatura chroni hasła przed oprogramowaniem rejestrującym naciśnięcia klawiszy (keyloggerami) lub zawartość ekranu (screenloggerami).

Z myślą o wygodzie użytkowania i swobodnym przenoszeniu danych pamięć Locker+ 50 G2 została umieszczona w małej metalowej obudowie z zaczepem na kółko do kluczy.

Pamięć LP50G2 jest objęta ograniczoną 5-letnią gwarancją i bezpłatną pomocą techniczną firmy Kingston.

Charakterystyka pamięci IronKey Locker+ 50 G2

- Certyfikat FIPS 197
- Szyfrowanie sprzętowe XTS-AES (nie można go wyłączyć)
- Ochrona przed atakami Brute Force i BadUSB
- Opcje obsługi wielu haseł
- Tryby haseł złożonych i wyrażań hasłowych
- Przycisk z symbolem „oka” do wyświetlania wprowadzanych haseł w celu ograniczenia liczby nieudanych prób logowania
- Wirtualna klawiatura pomagająca chronić przed keyloggerami i screenloggerami
- Zgodność z systemem Windows lub macOS (szczegóły w arkuszu danych)

Informacje o tej instrukcji (02122026)

Niniejsza instrukcja obsługi dotyczy pamięci IronKey Locker+ 50 G2 (LP50G2).

Wymagania systemowe

Platforma PC • Intel oraz AMD • 15MB wolnego miejsca na dysku • Dostępny port USB 2.0–3.2 • Dwie kolejne litery dysku po ostatnim dysku fizycznym* * Uwaga: patrz rozdział „Konflikt liter dysków” na str. 28.	Obsługiwane systemy operacyjne komputerów PC • Windows 11
Platforma Mac • Intel oraz Apple SOC • 15MB wolnego miejsca na dysku • Port USB 2.0–3.2	Obsługiwane systemy operacyjne komputerów Mac • macOS 13.x – 26.x

Zalecenia

Aby zagwarantować odpowiednie zasilanie urządzenia LP50G2, należy podłączać je bezpośrednio do portu USB w notebooku lub komputerze stacjonarnym, jak pokazano na *ilustracji 1.1*. Nie zaleca się podłączania urządzenia LP50G2 do urządzeń peryferyjnych z portem USB, takich jak klawiatura czy koncentrator zasilany z portu USB, jak pokazano na *ilustracji 1.2*.



Ilustracja 1.1 – Zalecany sposób użycia



Ilustracja 1.2 – Niezalecany sposób użycia

Używanie prawidłowego systemu plików

Pamięć IronKey LP50G2 jest fabrycznie sformatowana w systemie plików FAT32. Pozwala to na działanie w systemach Windows i macOS. Niezależnie od tego możliwe jest wykorzystanie innych opcji ręcznego sformatowania pamięci, takich jak system NTFS dla Windows czy exFAT. W razie potrzeby można ponownie sformatować partycję danych, jednak podczas ponownego formatowania pamięci zostaną utracone zapisane w niej dane.

Zalecenia dotyczące użytkowania

W celu zapewnienia bezpieczeństwa danych Kingston zaleca:

- Przeprowadzenie skanowania antywirusowego w komputerze przed skonfigurowaniem i użyciem pamięci LP50G2 w docelowym systemie.
- W przypadku korzystania z pamięci w dostępnym publicznie lub nieznanym systemie można włączyć w urządzeniu tryb tylko do odczytu, aby chronić pamięć przed złośliwym oprogramowaniem.
- Blokowanie urządzenia, gdy nie jest używane.
- Wysuwanie urządzenia z systemu przed jego odłączeniem.
- Nieodłączanie urządzenia, gdy świeci się jego dioda LED. Może to spowodować uszkodzenie pamięci wymagające ponownego sformatowania, co będzie skutkowało usunięciem danych
- Nieudostępnianie hasła innym osobom.

Najnowsze aktualizacje i informacje

Najnowsze aktualizacje oprogramowania pamięci, odpowiedzi na najczęściej zadawane pytania, dokumentację i dodatkowe informacje można znaleźć na stronie kingston.com/support.

UWAGA: należy instalować wyłącznie najnowsze aktualizacje oprogramowania pamięci.

Zmiany na starsze wersje oprogramowania nie są obsługiwane i mogą potencjalnie spowodować utratę przechowywanych danych lub zakłócić działanie innych funkcji pamięci. Wszelkie pytania należy kierować do działu pomocy technicznej firmy Kingston.

Najlepsze metody konfiguracji hasła

Pamięć LP50G2 ma silne zabezpieczenia. Obejmuje to ochronę przed atakami Brute Force, która uniemożliwia hakerom odgadywanie haseł dzięki ograniczeniu liczby prób wprowadzenia hasła do dziesięciu. Po osiągnięciu tego limitu pamięć LP50G2 automatycznie wymazuje zaszyfrowane dane, formatując się do stanu fabrycznego.

Obsługa wielu haseł

Jedną z głównych funkcji pamięci LP50G2 jest obsługa wielu haseł, która pomaga chronić dane w przypadku zapomnienia jednego z nich. Gdy wszystkie opcje haseł są włączone, pamięć LP50G2 umożliwia korzystanie z dwóch różnych haseł służących do odzyskiwania danych – hasła administratora oraz hasła użytkownika.

Pamięć LP50G2 pozwala wybrać dwa główne hasła: hasło administratora oraz hasło użytkownika. Administrator może w dowolnej chwili uzyskać dostęp do pamięci i skonfigurować opcje dla użytkownika.

Użytkownik może również uzyskać dostęp do pamięci, ale w porównaniu z administratorem ma ograniczone uprawnienia. W przypadku zapomnienia jednego z dwóch haseł można użyć drugiego z nich w celu uzyskania dostępu do danych i ich odzyskania. Następnie można ponownie skonfigurować pamięć, tak aby miała dwa hasła. Ważne jest, aby skonfigurować OBA hasła i zapisać hasło administratora w bezpiecznym miejscu, a na co dzień używać hasła użytkownika.

W przypadku zapomnienia lub utraty wszystkich haseł nie będzie możliwe uzyskanie dostępu do danych. Kingston nie będzie w stanie odzyskać danych, ponieważ zastosowanego mechanizmu zabezpieczeń nie można obejść. Kingston zaleca zapisywanie danych również na innych nośnikach. Pamięć LP50G2 można bezpiecznie wymazać w celu ponownego wykorzystania, jednak znajdujące się w niej dane zostaną bezpowrotnie usunięte.

Tryby hasła

Pamięć LP50G2 obsługuje również dwa różne tryby hasła:

Hasło złożone

Hasło złożone musi składać się z co najmniej 6–16 znaków oraz zawierać co najmniej trzy z następujących rodzajów znaków:

- Wielkie litery alfabetu
- Małe litery alfabetu
- Cyfry
- Znaki specjalne

Wyrażenie hasłowe

Pamięć LP50G2 obsługuje wyrażenia hasłowe o długości od 10 do 64 znaków. Wyrażenie hasłowe nie podlega żadnym dodatkowym regułom, ale jeśli jest używane prawidłowo, może zapewnić bardzo wysoki poziom ochrony.

Wyrażenie hasłowe to w zasadzie dowolna kombinacja znaków, w tym znaków z innych języków. Język hasła może odpowiadać językowi wybranemu dla pamięci LP50G2. Pozwala to na wybór kilku słów, frazy, tekstu piosenki, wersu z wiersza itp. Dobre wyrażenia hasłowe należą do najtrudniejszych do odgadnięcia przez nieuprawnioną osobę, a jednocześnie mogą być łatwiejsze do zapamiętania przez użytkownika.

Konfiguracja urządzenia

Aby zapewnić odpowiednie zasilanie szyfrowanej pamięci USB IronKey, podłącz ją bezpośrednio do portu USB 2.0/3.0 w notebooku lub komputerze stacjonarnym. Unikaj podłączania pamięci do urządzeń peryferyjnych, które mogą być wyposażone w port USB, takich jak klawiatura czy koncentrator zasilany przez USB. Początkową konfigurację urządzenia należy przeprowadzić w obsługiwanym systemie operacyjnym Windows lub macOS.

Dostęp do urządzenia (środowisko Windows)

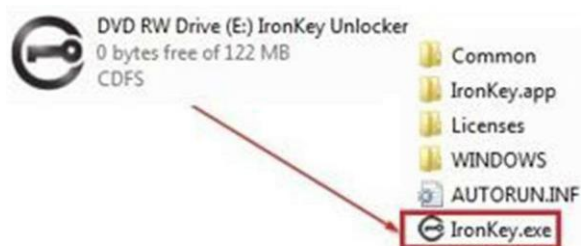
Podłącz szyfrowaną pamięć USB IronKey do wolnego portu USB w notebooku lub komputerze stacjonarnym i zaczekaj, aż zostanie wykryta przez system Windows.

- Wyświetli się powiadomienie dotyczące instalacji sterownika urządzenia (*ilustracja 3.1*).



Ilustracja 3.1 – Powiadomienie o instalacji sterownika urządzenia

- Po zakończeniu wykrywania nowego sprzętu wybierz opcję **IronKey.exe** w partycji Unlocker, którą można znaleźć w Eksploratorze plików (*ilustracja 3.2*).
- Pamiętaj, że litera partycji będzie różnić się w zależności od kolejnej wolnej litery dysku. Litera dysku może się zmienić w zależności od tego, jakie urządzenia są podłączone. Na ilustracji po prawej stronie litera dysku to (E:).

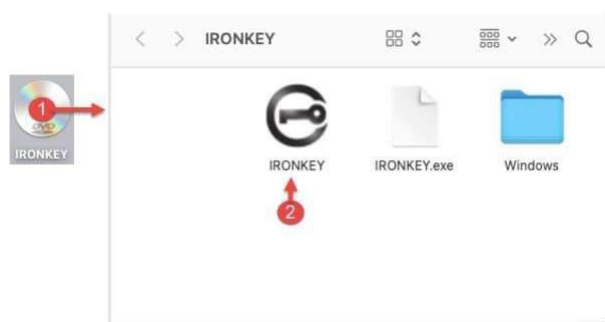


Ilustracja 3.2 – Okno Eksploratora plików/IronKey.exe

Dostęp do urządzenia (środowisko macOS)

Podłącz pamięć LP50G2 do wolnego portu w notebooku lub komputerze stacjonarnym i zaczekaj, aż zostanie wykryta przez system operacyjny macOS. Po wykryciu pamięci na pulpicie wyświetli się wolumin „IRONKEY” (*ilustracja 3.3*).

- Kliknij dwukrotnie ikonę CD-ROM IronKey.
- Następnie kliknij dwukrotnie ikonę aplikacji IronKey.app, widoczną w oknie pokazanym na *ilustracji 3.3*. Spowoduje to rozpoczęcie procesu inicjalizacji.

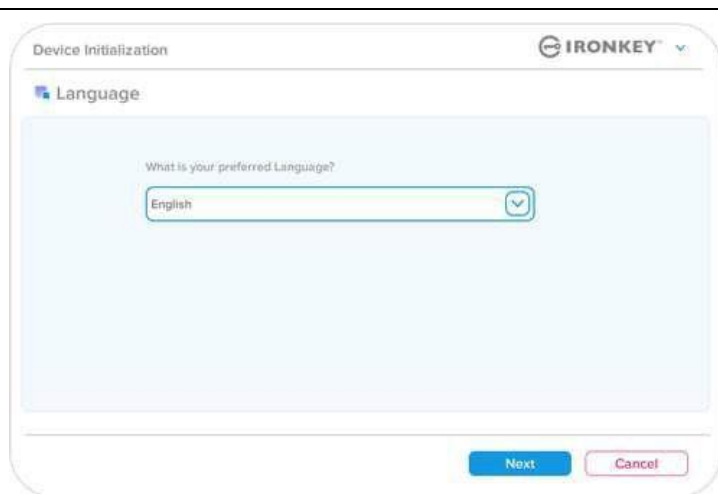


Ilustracja 3.3 – Wolumin IRONKEY

Inicjalizacja urządzenia (środowiska Windows i macOS)

Język i umowa licencyjna użytkownika końcowego

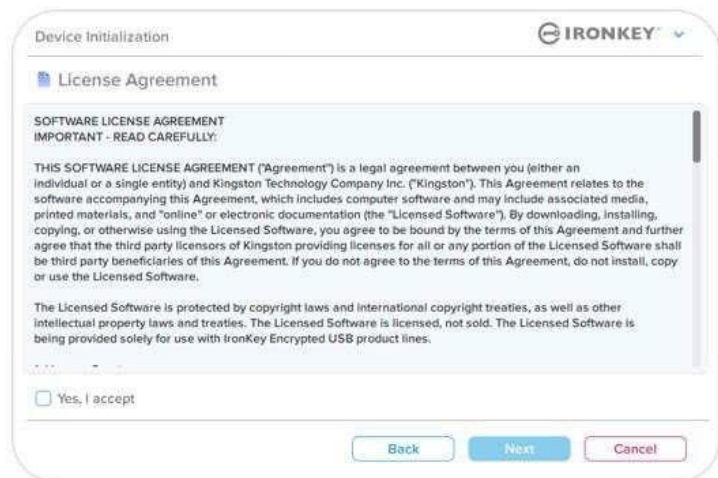
Wybierz preferowany język z menu rozwijanego i kliknij przycisk **Next (Dalej)** (patrz ilustracja 4.1).



Ilustracja 4.1 – Wybór języka

Zapoznaj się z umową licencyjną i kliknij przycisk **Next (Dalej)**.

Uwaga: aby kontynuować, zaakceptuj umowę licencyjną; w przeciwnym razie przycisk **Next (Dalej)** pozostanie nieaktywny (ilustracja 4.2).



Ilustracja 4.2 – Umowa licencyjna

Inicjalizacja urządzenia

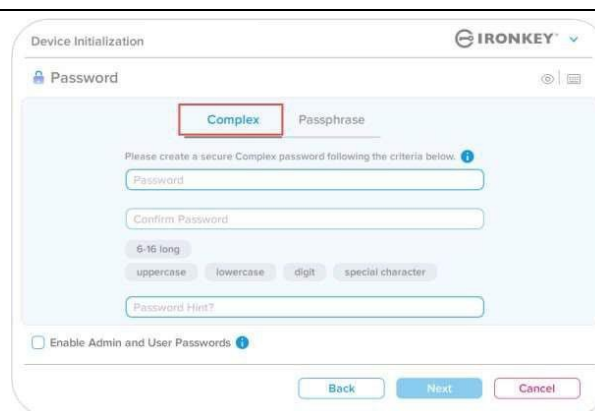
Wybór hasła

Na ekranie monitu o podanie hasła można utworzyć hasło do ochrony danych zapisanych w pamięci LP50G2, korzystając z trybu hasła złożonego lub wyrażenia hasłowego (*ilustracje 4.3-4.4*). Ponadto na tym ekranie można również włączyć opcje wielu haseł administratora/użytkownika. Zanim przejdziesz do wyboru hasła, zapoznaj się z informacjami dotyczącymi włączania haseł administratora/użytkownika poniżej, aby lepiej zrozumieć działanie tych funkcji.

Uwaga: po wybraniu trybu hasła złożonego lub wyrażenia hasłowego nie można go zmienić, o ile urządzenie nie zostanie zresetowane. Aby rozpocząć wybór hasła, utwórz hasło w polu „Password” (Hasło), a następnie wprowadź je ponownie w polach „Confirm Password” (Potwierdź hasło). Utworzone hasło musi spełniać poniższe kryteria, aby można było kontynuować proces inicjalizacji:

Hasło złożone

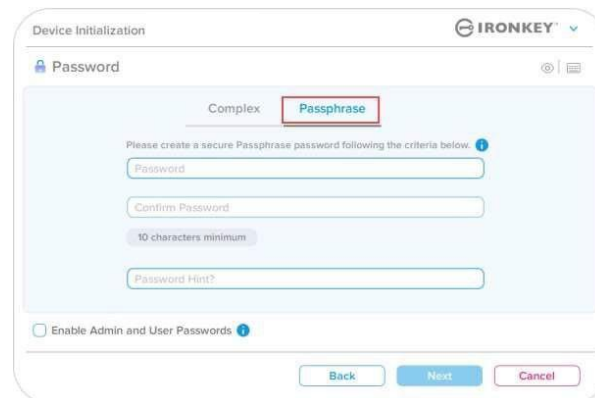
- Musi zawierać co najmniej 6 znaków (maks. 16 znaków).
- Musi zawierać trzy (3) z następujących rodzajów znaków:
 - Wielkie litery
 - Małe litery
 - Cyfry
 - Znaki specjalne (!,\$,&, itp.)



Ilustracja 4.3 – Hasło złożone

Wyrażenie hasłowe

- Musi zawierać:
 - Co najmniej 10 znaków
 - Maksymalnie 64 znaki

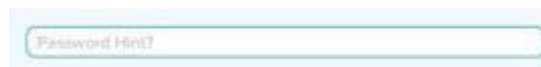


Ilustracja 4.4 – Wyrażenie hasłowe

Podpowiedź hasła (opcjonalnie)

Podpowiedź hasła może pomóc w przypomnieniu sobie zapomnianego hasła.

Uwaga: podpowiedź NIE MOŻE być taka sama jak hasło.

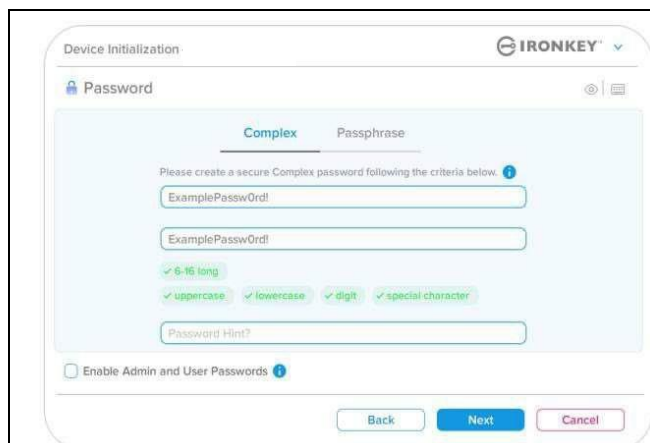


Ilustracja 4.5 – Pole podpowiedzi hasła

Inicjalizacja urządzenia

Prawidłowe i nieprawidłowe hasła

Po zdefiniowaniu **prawidłowych** haseł, które spełniają wymagane kryteria, pola kryteriów hasła podświetlą się na **zielono** (patrz ilustracje 4.6a-b). Uwaga: po spełnieniu co najmniej trzech kryteriów czwarte pole kryteriów hasła stanie się szare, co oznacza, że to kryterium jest opcjonalne (ilustracja 4.6b).



Device Initialization

IRONKEY

Password

Complex Passphrase

Please create a secure Complex password following the criteria below.

ExamplePasswOrd!

ExamplePasswOrd!

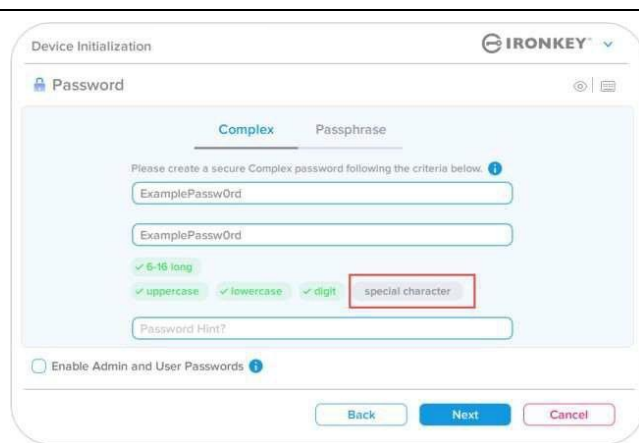
✓ 6-16 long ✓ uppercase ✓ lowercase ✓ digit ✓ special character

Password Hint?

☐ Enable Admin and User Passwords

Back Next Cancel

Ilustracja 4.6a – Spełnione warunki dla hasła złożonego



Device Initialization

IRONKEY

Password

Complex Passphrase

Please create a secure Complex password following the criteria below.

ExamplePasswOrd

ExamplePasswOrd

✓ 6-16 long ✓ uppercase ✓ lowercase ✓ digit special character

Password Hint?

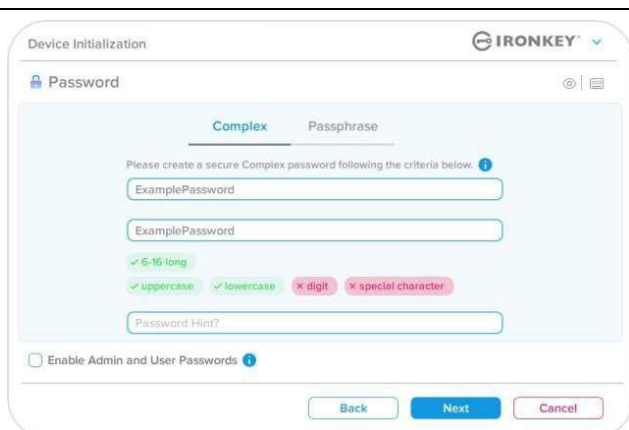
☐ Enable Admin and User Passwords

Back Next Cancel

Ilustracja 4.6b – Opcjonalny warunek dla hasła złożonego

W przypadku zdefiniowania **nieprawidłowego** hasła pola kryteriów hasła podświetlą się na **czerwono**, a przycisk **Next (Dalej)** stanie się nieaktywny do czasu spełnienia minimalnych wymagań.

Dotyczy to zarówno haseł złożonych, jak i wyrażen hasłowych.



Device Initialization

IRONKEY

Password

Complex Passphrase

Please create a secure Complex password following the criteria below.

ExamplePassword

ExamplePassword

✓ 6-16 long ✓ uppercase ✓ lowercase ✗ digit ✗ special character

Password Hint?

☐ Enable Admin and User Passwords

Back Next Cancel

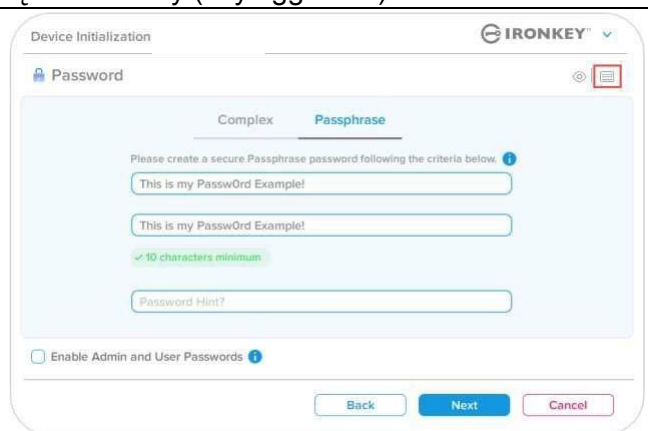
Ilustracja 4.7 – Niespełnione warunki dla hasła

Inicjalizacja urządzenia

Wirtualna klawiatura

Pamięć LP50G2 jest wyposażona w funkcję wirtualnej klawiatury, która może służyć do ochrony przed oprogramowaniem rejestrującym naciśnięcia klawiszy (keyloggerami).

- Aby skorzystać z funkcji **wirtualnej klawiatury**, znajdź symbol klawiatury w prawym górnym rogu ekranu **Device Initialization (Inicjalizacja urządzenia)** i zaznacz go.



Ilustracja 4.8 – Aktywacja wirtualnej klawiatury

- Gdy pojawi się wirtualna klawiatura, możesz również włączyć funkcję **Screenlogger Protection (Ochrona przed screenloggerami)**. Podczas korzystania z tej funkcji wszystkie klawisze przez chwilę staną się niewidoczne. Jest to celowe działanie, które zapobiega przechwytywaniu kliknięć przez screenloggery.
- Aby ta funkcja była jeszcze bardziej skuteczna, możesz wybrać losowy układ wirtualnej klawiatury, klikając klawisz **randomize (randomizacja)** w prawym dolnym rogu klawiatury. Wybór tej opcji spowoduje rozmieszczenie klawiszy w losowy sposób.



Ilustracja 4.9 – Ochrona przed screenloggerami/ randomizacja

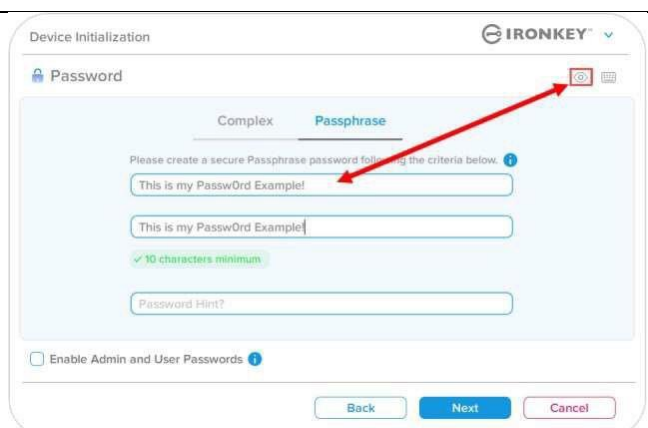
Inicjalizacja urządzenia

Przełącznik widoczności hasła

Domyślnie podczas tworzenia hasła (jego wpisywania) ciąg znaków jest wyświetlany w polu hasła. Aby ukryć hasło podczas wpisywania, kliknij symbol oka w prawym górnym rogu okna inicjalizacji urządzenia.

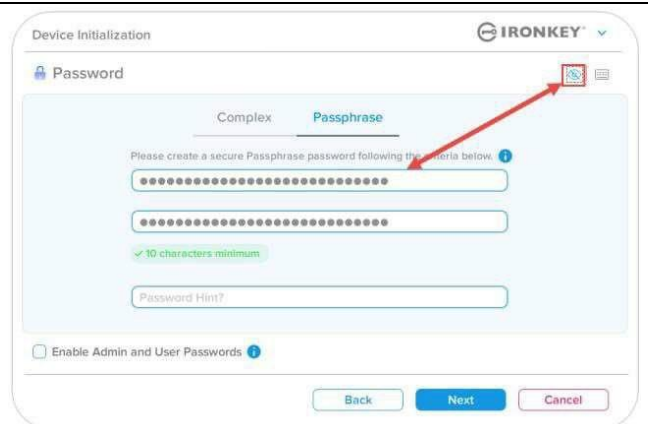
Uwaga: po zakończeniu inicjalizacji urządzenia pole hasła będzie domyślnie „ukryte”.

Aby **ukryć** ciąg znaków hasła, kliknij szarą ikonę.



Ilustracja 4.10 – Wybór opcji „ukryj” hasło

Aby **wyświetlić** ukryte hasło, kliknij niebieską ikonę.



Ilustracja 4.11– Wybór opcji „pokaż” hasło

Inicjalizacja urządzenia

Hasła administratora i użytkownika

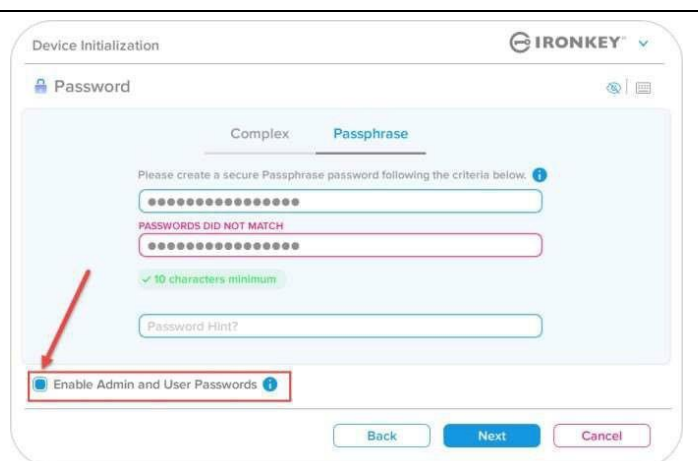
Włączenie haseł administratora i użytkownika umożliwia korzystanie z funkcji wielu haseł oraz zarządzanie obydwooma kontami z poziomu administratora. Zaznaczenie opcji **Enable Admin and User passwords (Włącz hasła administratora i użytkownika)** umożliwia skorzystanie z alternatywnej metody dostępu do pamięci w przypadku zapomnienia jednego z haseł.

Gdy **hasła administratora i użytkownika** są włączone, można również uzyskać dostęp do następujących funkcji:

- Resetowanie hasła użytkownika

Aby dowiedzieć się więcej o funkcji resetowania hasła użytkownika, przejdź na str. 24 niniejszej instrukcji.

- Aby włączyć **hasła administratora i użytkownika**, kliknij pole obok opcji **Enable Admin and User passwords (Włącz hasła administratora i użytkownika)** i po wybraniu prawidłowego hasła kliknij przycisk **Next (Dalej)** (ilustracja 4.12).
- Jeśli ta funkcja jest **włączona**, hasło wybrane na tym ekranie będzie **hasłem administratora**. Kliknij przycisk **Next (Dalej)**, aby przejść do ekranu **hasła użytkownika** i zdefiniować hasło dla użytkownika.



Ilustracja 4.12 – Włączanie haseł administratora i użytkownika

Uwaga: włączenie hasła administratora i użytkownika jest opcjonalne.

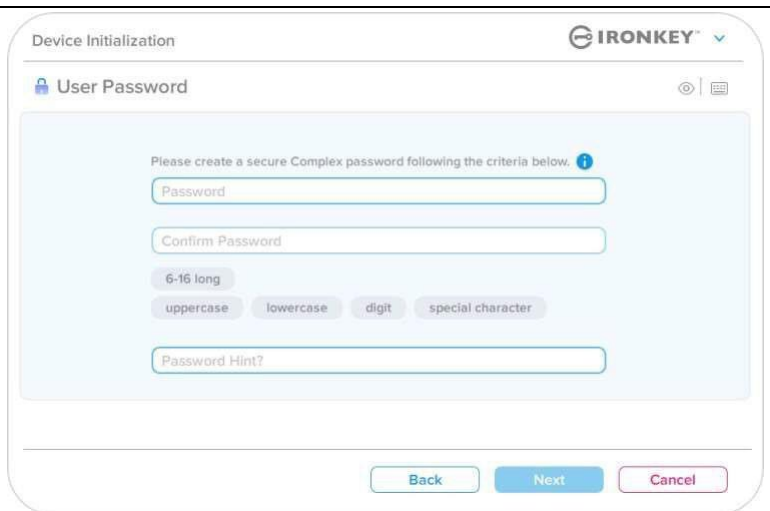
Jeśli w konfiguracji pamięci ta funkcja **NIE** jest włączona (pole niezaznaczone), pamięć zostanie skonfigurowana z **jednym hasłem dla pojedynczego użytkownika – bez funkcji administracyjnych**. W niniejszej instrukcji taka konfiguracja będzie określana jako **tryb Tylko użytkownik**.

Aby kontynuować konfigurację dla pojedynczego użytkownika z jednym hasłem, pozostaw niezaznaczoną opcję **Enable Admin and User Passwords (Włącz hasła administratora i użytkownika)** i po utworzeniu prawidłowego hasła kliknij przycisk **Next (Dalej)**.

Inicjalizacja urządzenia

Hasła administratora i użytkownika

Jeśli na poprzednim ekranie została **włączona** rola administratora, na następnym ekranie pojawi się monit o podanie **hasła użytkownika** (ilustracja 4.13). Hasło użytkownika zapewnia ograniczone uprawnienia w porównaniu z hasłem administratora, co zostanie szczegółowo omówione w dalszej części instrukcji. **Uwaga:** w dalszej części tego dokumentu **tryb z włączonymi hasłami administratora i użytkownika** będzie określany jako „Rola administratora”.



The screenshot shows the 'Device Initialization' screen with the 'User Password' section. It instructs the user to 'Please create a secure Complex password following the criteria below.' The criteria are: 6-16 long, uppercase, lowercase, digit, and special character. There are input fields for 'Password', 'Confirm Password', and 'Password Hint?'. At the bottom, there are 'Back', 'Next', and 'Cancel' buttons.

Ilustracja 4.13 – Hasło użytkownika (włączone hasła administratora i użytkownika)

Uwaga: wybrane kryteria opcji hasła (złożonego lub wyrażenia hasłowego) zostaną przeniesione na hasło użytkownika i ewentualne czynności resetowania hasła, niezbędne po skonfigurowaniu pamięci. Wybraną opcję hasła można zmienić dopiero po całkowitym zresetowaniu urządzenia.

Inicjalizacja urządzenia

Informacje kontaktowe

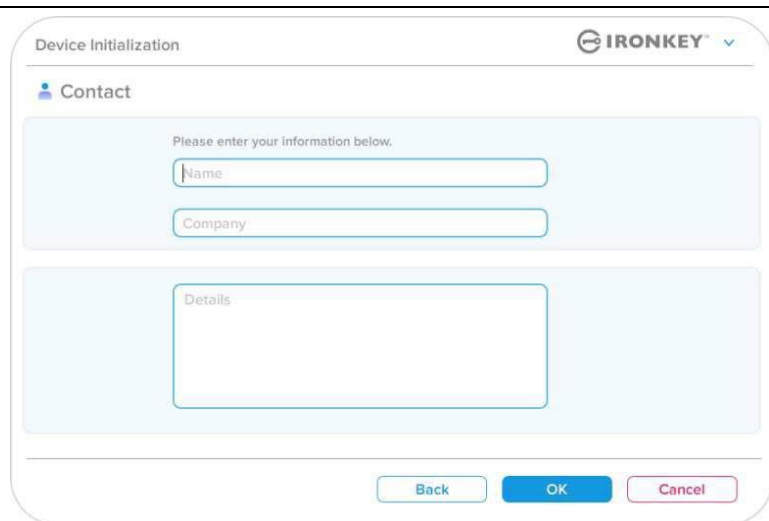
W wyświetlonych polach tekstowych wprowadź informacje kontaktowe (*patrz ilustracja 4.14*).

Uwaga: informacje wprowadzone w tych polach NIE MOGĄ zawierać hasła utworzonego w kroku 3 (pola te są opcjonalne i można pozostawić je puste).

Pole **Name (Nazwa)** może zawierać do 32 znaków, ale nie może zawierać **samego** hasła.

Pole **Company (Firma)** może zawierać do 32 znaków, ale nie może zawierać **samego** hasła.

Pole **Details (Szczegóły)** może zawierać do 156 znaków, ale nie może zawierać **samego** hasła.

The screenshot shows a mobile application interface titled "Device Initialization" with the IRONKEY logo in the top right corner. Below the title is a "Contact" section with a person icon. It contains the instruction "Please enter your information below." followed by three input fields: "Name", "Company", and "Details". The "Name" and "Company" fields are short text boxes, while "Details" is a larger text area. At the bottom of the form are three buttons: "Back", "OK", and "Cancel".

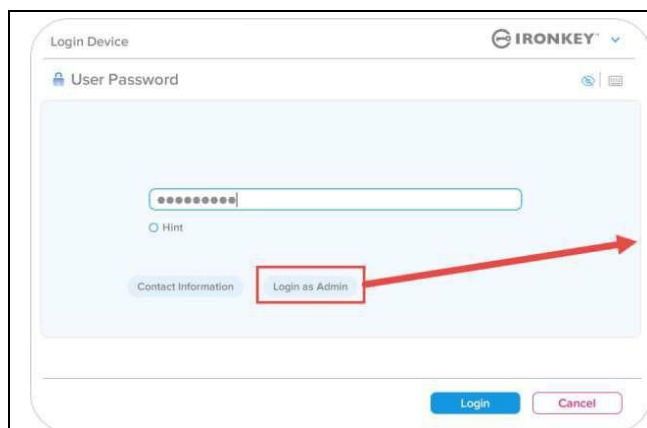
Ilustracja 4.14 – Informacje kontaktowe

Uwaga: Kliknięcie przycisku „OK” spowoduje zakończenie procesu inicjalizacji i przejście do odblokowania, a następnie zamontowania bezpiecznej partycji, gdzie będą bezpiecznie przechowywane dane. Odłącz pamięć i podłącz ją ponownie do komputera, aby zobaczyć wprowadzone zmiany.

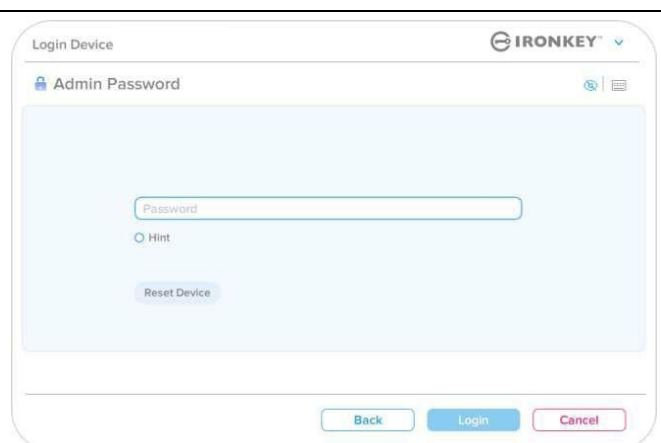
Korzystanie z urządzenia (środowiska Windows i macOS)

Logowanie administratora i użytkownika (włączony tryb administratora)

Jeśli urządzenie zostało zainicjalizowane z włączoną funkcją haseł administratora i użytkownika (rolą administratora), aplikacja IronKey LP50G2 uruchomi się, wyświetlając najpierw ekran logowania hasłem użytkownika. Z tego poziomu można zalogować się przy użyciu hasła użytkownika, wyświetlić wprowadzone informacje kontaktowe lub zalogować się jako administrator (*ilustracja 6.1*). Po kliknięciu przycisku Login as Admin (Zaloguj się jako administrator) (patrz poniżej) aplikacja przejdzie do menu logowania administratora, w którym można zalogować się jako administrator, aby uzyskać dostęp do ustawień i funkcji administratora (*ilustracja 6.2*).



Ilustracja 6.1 – Logowanie za pomocą hasła użytkownika (włączony tryb administratora)

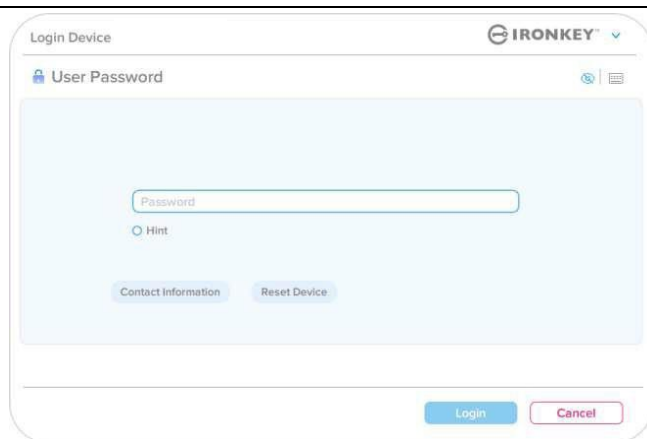


Ilustracja 6.2 – Logowanie za pomocą hasła administratora

Logowanie w trybie Tylko użytkownik (wyłączony tryb administratora)

Jak wspomniano na **stronie 13**, chociaż zaleca się korzystanie z funkcji administratora, aby w pełni wykorzystać możliwości urządzenia, pamięć IronKey można również zainicjalizować w konfiguracji Tylko użytkownik (jedno hasło, jeden użytkownik). Jest to opcja dla tych użytkowników, którzy preferują prostotę obsługi i ochronę danych za pomocą pojedynczego hasła (*ilustracja 6.3*).

Uwaga: w celu włączenia haseł administratora i użytkownika użyj przycisku **Reset Device (Resetuj urządzenie)**, aby przywrócić pamięć do stanu inicjalizacji, w którym można aktywować hasła administratora i użytkownika. **Zresetowanie urządzenia spowoduje sformatowanie WSZYSTKICH zapisanych danych i ich bezpowrotną utratę.**



Ilustracja 6.3 – Logowanie za pomocą hasła użytkownika (wyłączony tryb administratora)

Korzystanie z urządzenia

Ochrona przed atakami Brute Force

Ważne: jeżeli podczas logowania zostanie wprowadzone nieprawidłowe hasło, będzie można ponownie wprowadzić prawidłowe hasło, przy czym wbudowana funkcja zabezpieczeń (funkcja ochrony przed atakami Brute Force) zlicza nieudane próby logowania. *

Jeśli liczba ta osiągnie wstępnie skonfigurowaną wartość 10 nieudanych prób wprowadzenia hasła, zachowanie urządzenia będzie następujące:

Włączony tryb administratora/użytkownika	Zachowanie urządzenia (10 nieudanych prób wprowadzenia hasła)	Usunięcie danych i zresetowanie urządzenia
Hasło użytkownika	Blokada hasła; zaloguj się jako administrator, aby zresetować hasło użytkownika	NIE
Hasło administratora	Bezpowrotne wymazanie metodą kryptograficzną pamięci, haseł, ustawień i danych	TAK
Tylko użytkownik Jeden użytkownik, jedno hasło (tryb administratora/użytkownika <u>WYŁĄCZONY</u>)	Zachowanie urządzenia (10 nieudanych prób wprowadzenia hasła)	Usunięcie danych i zresetowanie urządzenia
Hasło użytkownika	Bezpowrotne wymazanie metodą kryptograficzną pamięci, haseł, ustawień i danych	TAK

* Po pomyślnym uwierzytelnieniu użytkownika licznik nieudanych logowań jest resetowany odpowiednio dla użytej metody logowania. Funkcja Crypto-Erase usunie wszystkie hasła, klucze szyfrowania i dane – **zostaną one bezpowrotnie utracone**.

Dostęp do zabezpieczonych plików

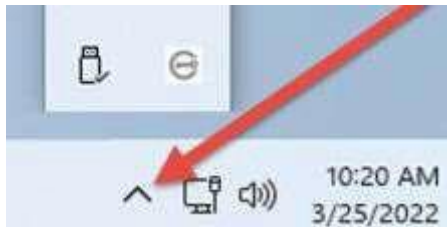
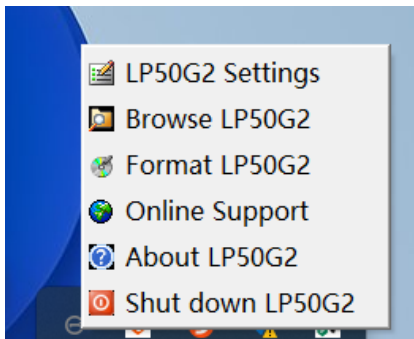
Po odblokowaniu urządzenia możliwy jest dostęp do zabezpieczonych plików. Pliki są automatycznie szyfrowane i odszyfrowywane podczas ich zapisywania lub otwierania w pamięci. Technologia ta pozwala na wygodną pracę podobnie jak w przypadku zwykłej pamięci, a jednocześnie zapewnia silną, „zawsze włączoną” ochronę plików.

Wskazówka: można również uzyskać dostęp do plików, klikając prawym przyciskiem myszy **ikonę IronKey** na pasku zadań systemu Windows, a następnie klikając opcję

Browse LP50G2 (Przeglądanie zawartości pamięci LP50G2) (ilustracja 7.2).

Opcje urządzenia (środowisko Windows)

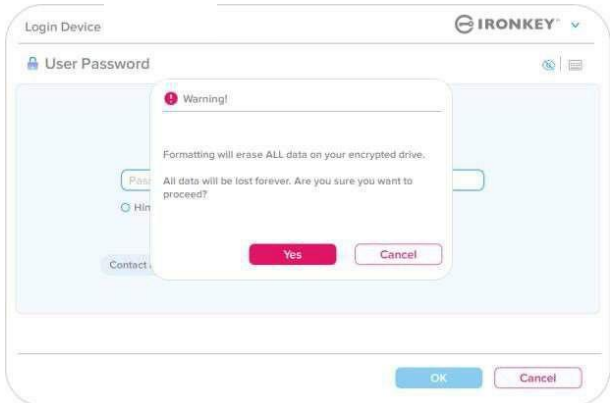
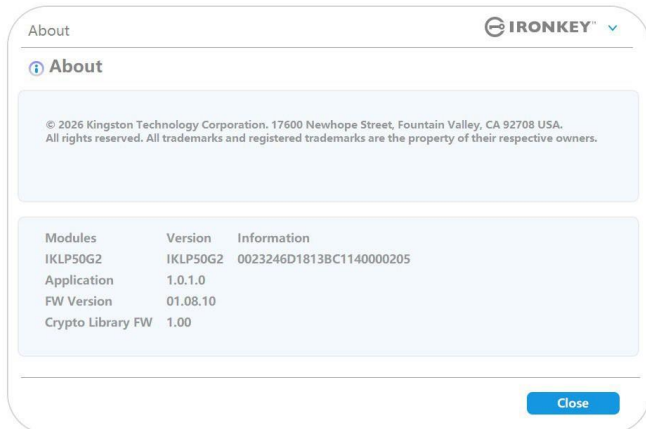
Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey. Kliknięcie prawym przyciskiem myszy ikony IronKey spowoduje otwarcie menu wyboru dostępnych opcji pamięci (*ilustracja 6.2*). Szczegółowe informacje na temat tych opcji znajdują na str. 19–23 niniejszej instrukcji.

Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey (<i>ilustracja 7.1</i>).	 Ilustracja 7.1 – Ikona IronKey na pasku zadań
Kliknięcie prawym przyciskiem myszy ikony IronKey spowoduje otwarcie menu wyboru dostępnych opcji pamięci (<i>ilustracja 7.2</i>). Szczegółowe informacje na temat tych opcji znajdują na str. 19–23 niniejszej instrukcji.	 Ilustracja 7.2 – Kliknij prawym przyciskiem myszy ikonę IronKey, aby wyświetlić opcje urządzenia

Opcje urządzenia (środowisko macOS)

Gdy użytkownik jest zalogowany do urządzenia, w menu systemu macOS widoczna jest ikona pamięci IronKey LP50G2 (patrz <i>ilustracja 7.3</i>), której kliknięcie powoduje wyświetlenie dostępnych opcji urządzenia. Szczegółowe informacje na temat tych opcji znajdują na str. 19–23 niniejszej instrukcji.	 Ilustracja 7.3 – Ikona opcji urządzenia na pasku menu systemu macOS
--	--

Opcje urządzenia

Ustawienia pamięci LP50G2:	Zmiana hasła logowania, informacji kontaktowych i innych ustawień. (Więcej informacji na temat ustawień urządzenia znajduje się w części „Ustawienia pamięci LP50G2” niniejszej instrukcji).
Browse LP50G2 (Przeglądanie zawartości pamięci LP50G2):	Umożliwia przeglądanie zabezpieczonych plików.
Format LP50G2 (Formatowanie pamięci LP50G2): Umożliwia sformatowanie bezpiecznej partycji danych. (Ostrzeżenie: wszystkie dane zostaną wymazane) (ilustracja 6.1). Uwaga: formatowanie wymaga uwierzytelnienia hasłem.	 Ilustracja 7.4 – Formatowanie pamięci LP50G2
Online Support (Pomoc techniczna online):	Otwarcie przeglądarki internetowej i przejście na stronę http://www.kingston.com/support, gdzie dostępne są dodatkowe informacje.
About LP50G2 (Informacje o pamięci LP50G2): Dostęp do szczegółowych informacji na temat pamięci LP50G2, w tym informacji o aplikacji, oprogramowaniu sprzętowym i numerze seryjnym (ilustracja 6.2). Uwaga: Unikalny numer seryjny znajduje się w kolumnie „Informacje”.	 Ilustracja 7.5 – Informacje o pamięci LP50G2
Shut down LP50G2 (Wyłączenie pamięci LP50G2):	Prawidłowe wyłączenie pamięci LP50G2, umożliwiające jej bezpieczne odłączenie od komputera.

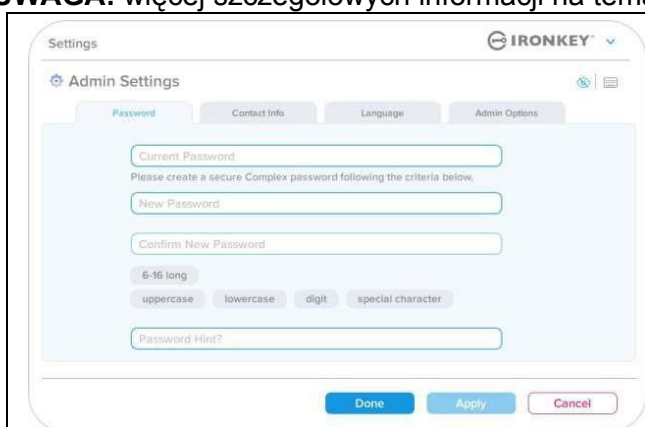
Ustawienia urządzenia LP50G2

Ustawienia administratora

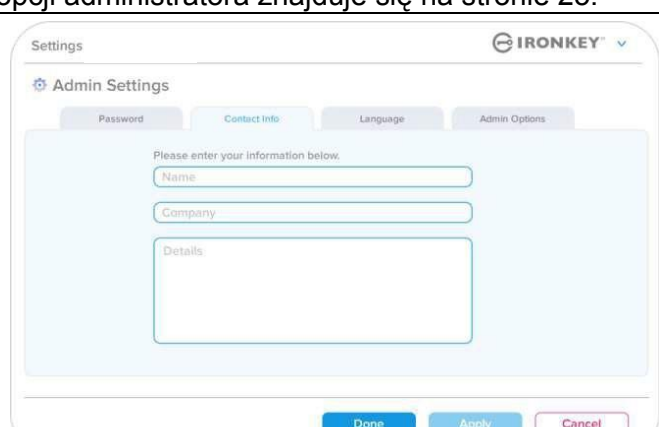
Zalogowanie się jako administrator umożliwia dostęp do następujących ustawień urządzenia:

- **Password (Hasło):** umożliwia zmianę hasła lub podpowiedzi hasła administratora (*ilustracja 8.1*).
- **Contact Info (Informacje kontaktowe):** umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 8.2*).
- **Language (Język):** umożliwia zmianę aktualnie wybranego języka (*ilustracja 8.3*).
- **Admin Options (Opcje administratora):** umożliwia włączenie dodatkowych funkcji, takich jak:
 - Zmiana hasła użytkownika (*ilustracja 8.4*)

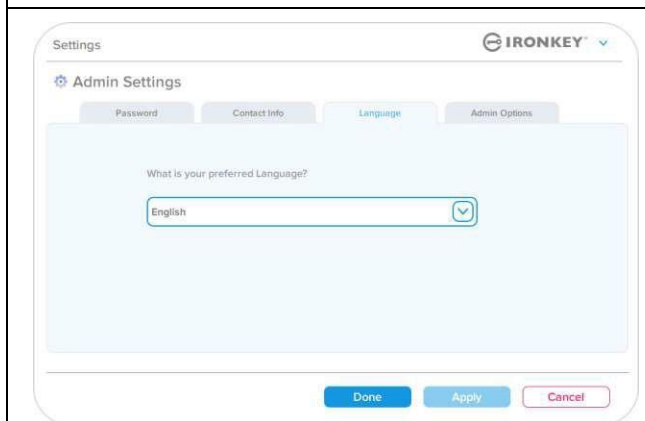
UWAGA: więcej szczegółowych informacji na temat opcji administratora znajduje się na stronie 25.



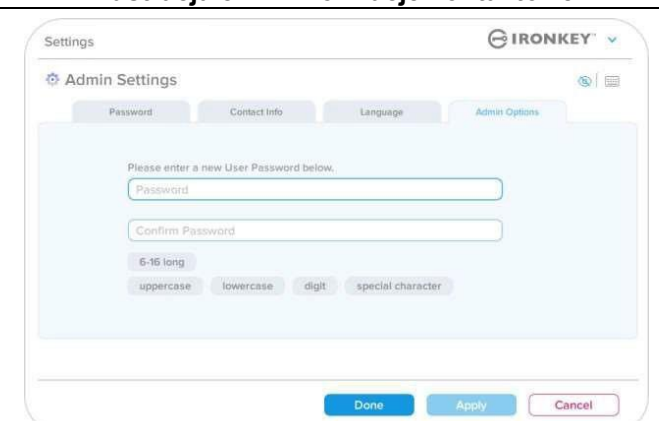
Ilustracja 8.1 – Opcje hasła administratora



Ilustracja 8.2 – Informacje kontaktowe



Ilustracja 8.3 – Opcje języka



Ilustracja 8.4 – Opcje administratora

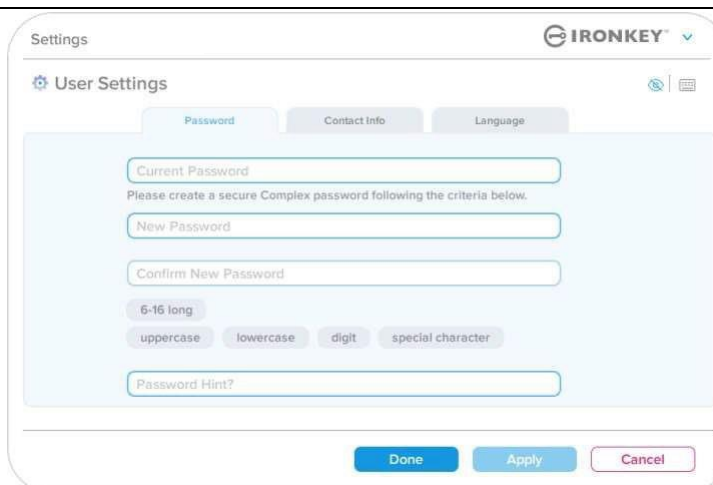
Ustawienia urządzenia LP50G2

Ustawienia użytkownika: włączony tryb administratora

Zalogowanie się jako użytkownik ogranicza dostęp do następujących ustawień:

Password (Hasło):

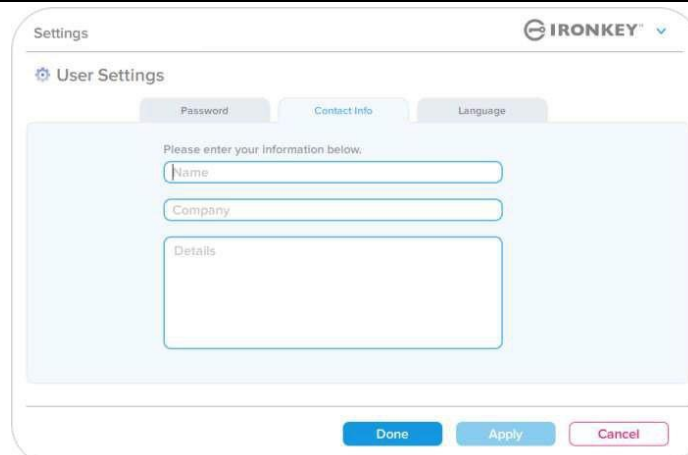
Umożliwia zmianę hasła i/lub odpowiedzi do hasła użytkownika (*ilustracja 8.5*).



Ilustracja 8.5 – Opcje hasła (włączony tryb administratora: logowanie użytkownika)

Contact Info (Informacje kontaktowe):

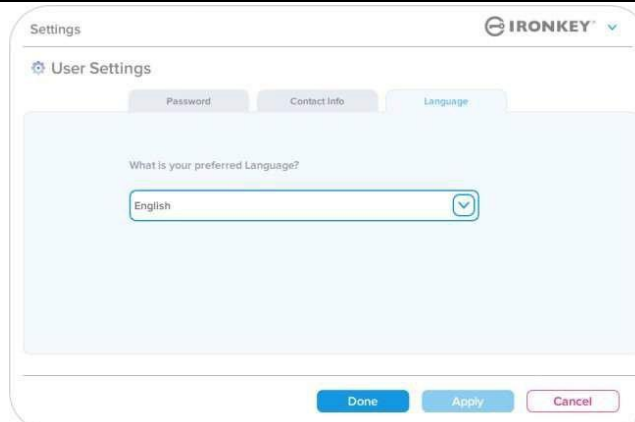
Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 8.6*).



Ilustracja 8.6 – Informacje kontaktowe (włączony tryb administratora: logowanie użytkownika)

Language (Język):

Umożliwia zmianę aktualnie wybranego języka (*ilustracja 8.7*).



Ilustracja 8.7 – Ustawienia języka (włączony tryb administratora: logowanie użytkownika)

Uwaga: opcje administratora nie są dostępne po zalogowaniu się przy użyciu hasła użytkownika.

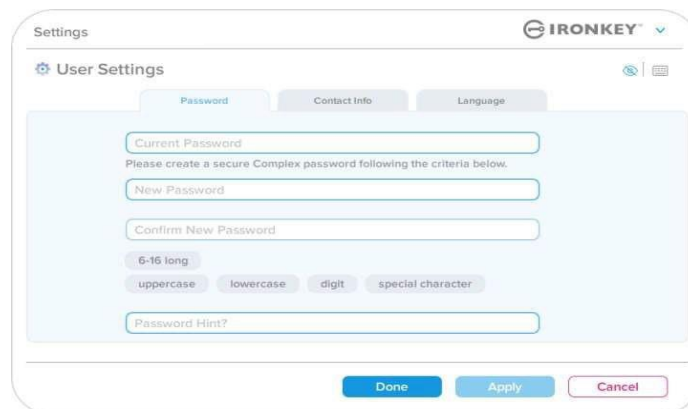
Ustawienia urządzenia LP50G2

Ustawienia użytkownika: wyłączony tryb administratora

Jak wspomniano wcześniej na stronie 12, inicjalizacja pamięci LP50G2 bez włączania haseł administratora i użytkownika spowoduje skonfigurowanie pamięci z **jednym hasłem dla pojedynczego użytkownika**. Konfiguracja ta nie zapewnia dostępu do żadnych opcji ani funkcji administracyjnych. Konfiguracja ta umożliwia dostęp do następujących ustawień pamięci LP50G2:

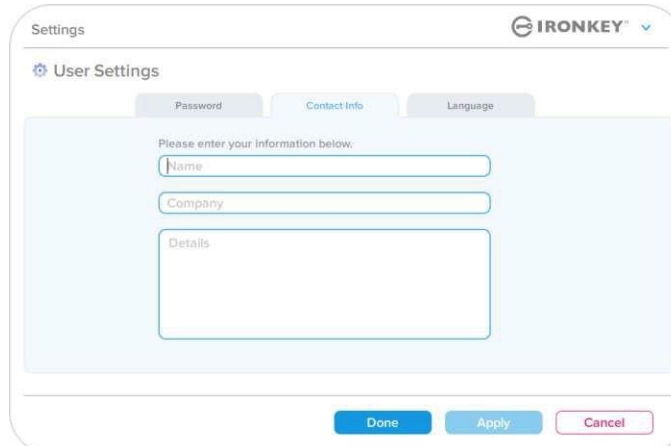
Password (Hasło):

Umożliwia zmianę hasła i/lub podpowiedzi do hasła użytkownika (*ilustracja 8.8*).



Ilustracja 8.8 – Opcje hasła (tryb Tylko użytkownik)

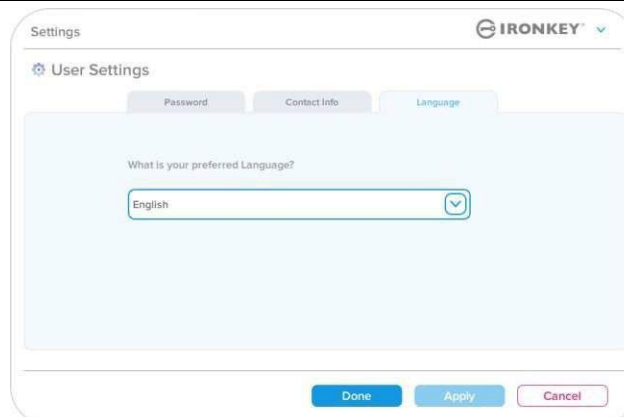
Contact Info (Informacje kontaktowe): Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 8.9*).



Ilustracja 8.9 – Informacje kontaktowe (tryb Tylko użytkownik)

Language (Język):

Umożliwia zmianę aktualnie wybranego języka (*ilustracja 8.10*).

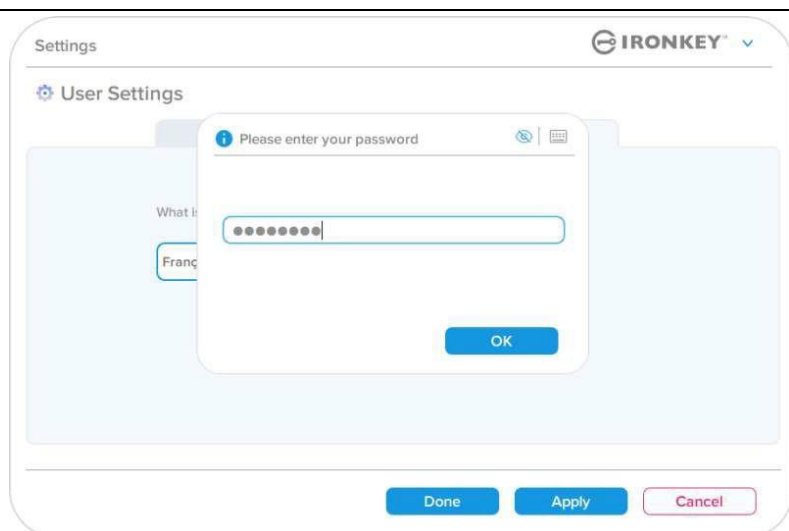


Ilustracja 8.10 – Ustawienia języka (tryb Tylko użytkownik)

Ustawienia urządzenia LP50G2

Zmiana i zapisywanie ustawień

- Po każdej zmianie ustawień pamięci LP50G2 (np. informacji kontaktowych, języka, hasła, opcji administratora itp.) pamięć wyświetli monit o wprowadzenie hasła w celu zaakceptowania i zastosowania zmian (patrz ilustracja 8.11).



Ilustracja 8.11 – Ekran monitu o wprowadzenie hasła w celu zapisania zmiany ustawień pamięci LP50G2

Uwaga: jeśli wyświetlany jest powyższy ekran monitu o hasło i konieczne jest anulowanie lub zmodyfikowanie wprowadzonych zmian, należy pozostawić pole hasła puste i kliknąć przycisk „OK”. Spowoduje to zamknięcie okna „Please enter your password” (Wprowadź hasło) i powrót do menu ustawień pamięci LP50G2.

Funkcje administracyjne

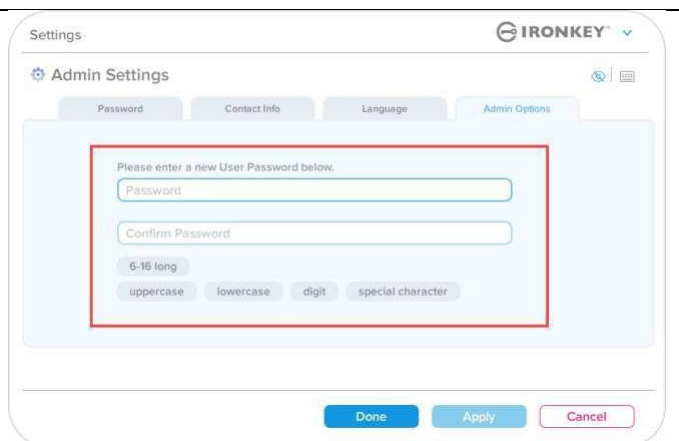
Dostępne opcje resetowania hasła użytkownika

Jedną z przydatnych funkcji konfiguracji, które są dostępne dla administratora, jest możliwość bezpiecznego zresetowania hasła użytkownika, jeśli dojdzie do jego zapomnienia. Poniżej omówiono funkcję resetowania hasła użytkownika, która może być pomocna w zresetowaniu hasła użytkownika.

Resetowanie hasła użytkownika:

Zmień ręcznie hasło użytkownika w menu „Admin Options” (Opcje administratora) – zmiana będzie natychmiastowa i zacznie obowiązywać przy następnym logowaniu użytkownika (*ilustracja 9.1*).

Uwaga: Kryteria wymagań dla hasła zostaną domyślnie ustawione na pierwotne kryteria, które zostały ustawione podczas procesu inicjalizacji (opcje hasła złożonego lub wyrażenia hasłowego).



Ilustracja 9.1 – Opcje administratora / Resetowanie hasła użytkownika

Pomoc i rozwiązywanie problemów

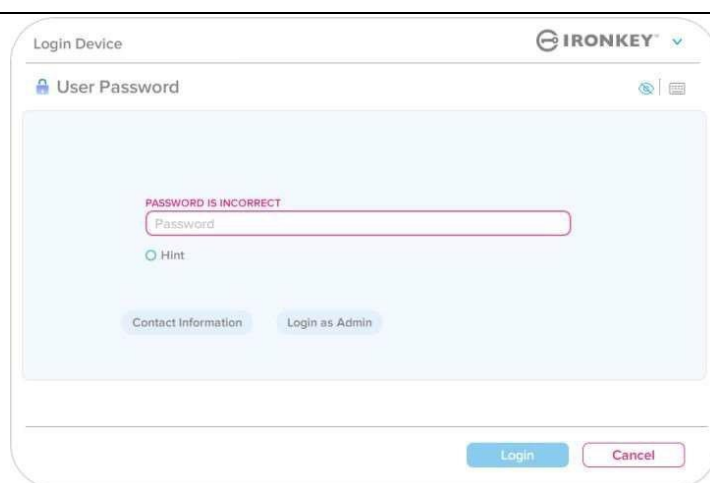
Blokada urządzenia

Pamięć LP50G2 jest wyposażona w funkcję bezpieczeństwa, która uniemożliwia nieuprawniony dostęp do partycji danych w przypadku osiągnięcia maksymalnej liczby **kolejnych** nieudanych prób zalogowania (w skrócie *MaxNoA*). W domyślnej fabrycznej konfiguracji ustawiona jest wartość 10 (liczba prób) dla każdej z metod logowania (administrator/użytkownik).

Licznik blokady zlicza nieudane logowania i można go zresetować na jeden z **dwóch sposobów**:

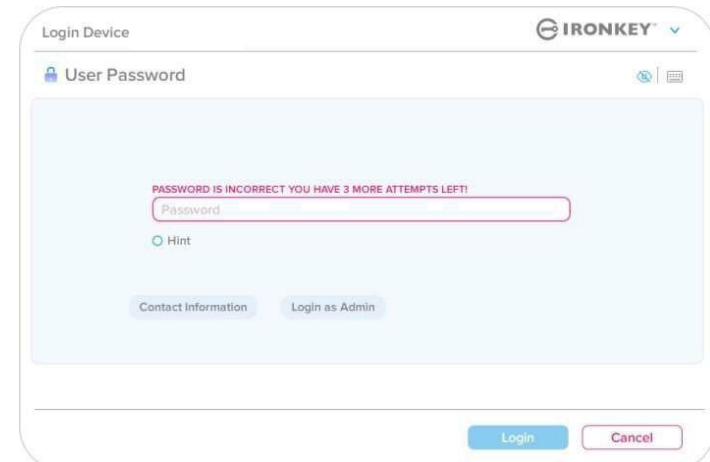
1. Pomyślne logowanie przed osiągnięciem limitu MaxNoA.
2. Osiągnięcie limitu MaxNoA i zablokowanie lub sformatowanie urządzenia, zależnie od konfiguracji pamięci.

- Jeśli zostanie wprowadzone nieprawidłowe hasło, tuż nad polem wprowadzania hasła pojawi się komunikat o błędzie w kolorze czerwonym, informujący o niepowodzeniu logowania (*ilustracja 10.1*).



Ilustracja 10.1 – Komunikat o wprowadzeniu nieprawidłowego hasła

- Po **siódmej** nieudanej próbie zostanie wyświetlony dodatkowy komunikat o błędzie, informujący o tym, że pozostały trzy próby przed osiągnięciem limitu MaxNoA (ustawionego domyślnie na wartość 10) (*ilustracja 10.2*).



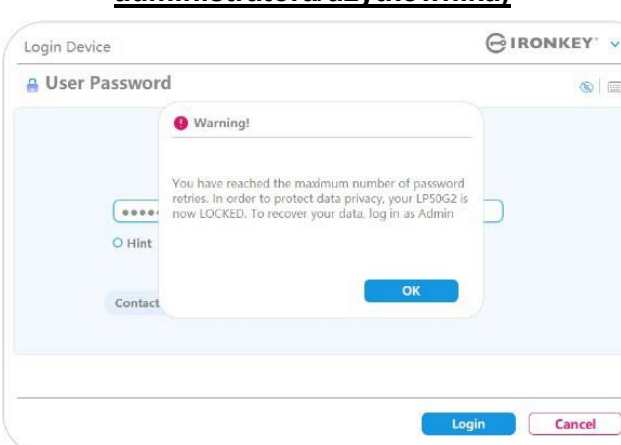
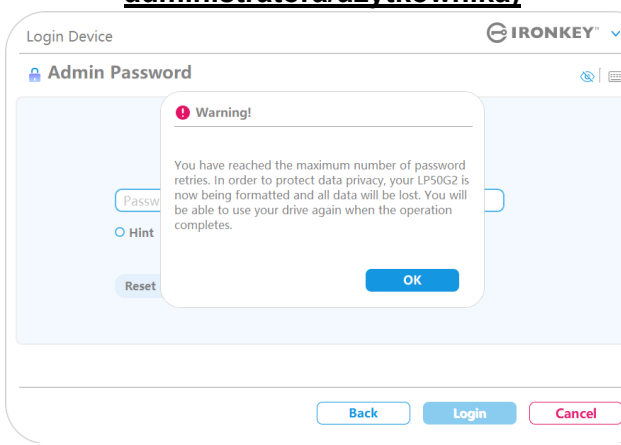
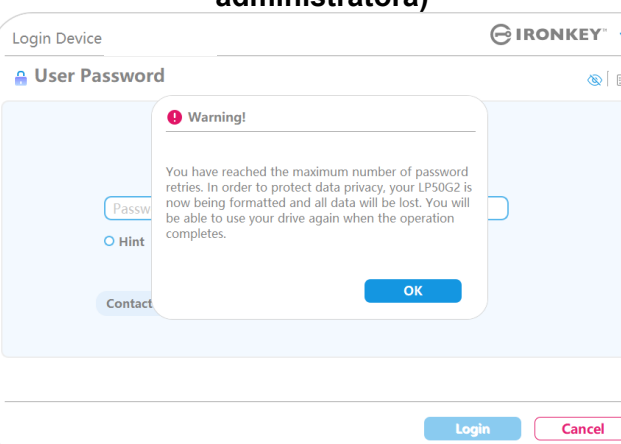
Ilustracja 10.2 – Siódma nieudana próba wprowadzenia hasła

Pomoc i rozwiązywanie problemów

Blokada urządzenia

Ważne: Po **dziesiątej** i ostatniej nieudanej próbie zalogowania, w zależności od tego, jak zostało skonfigurowane urządzenie i jakiej użyto metody logowania (administrator/użytkownik), urządzenie zostanie zablokowane, co będzie wymagało zalogowania się inną metodą (jeśli dotyczy) lub zresetowania urządzenia, co spowoduje **sformatowanie danych i ich bezpowrotną utratę**. O takim zachowaniu urządzenia wspomniano również na str. 17 niniejszej instrukcji.

Ilustracje 10.3–10.6 poniżej przedstawiają zachowanie urządzenia po dziesiątej i ostatniej nieudanej próbie zalogowania dla każdej z metod logowania:

Hasło użytkownika: (włączony tryb administratora/użytkownika)  BLOKADA URZĄDZENIA Ilustracja 10.3	Hasło administratora (włączony tryb administratora/użytkownika)  SFORMATOWANIE URZĄDZENIA* Ilustracja 10.4
Zabezpieczenia te mają na celu ograniczenie możliwości podjęcia nieograniczonej liczby prób zalogowania i uzyskania dostępu do poufnych danych przez osoby, które nie znają hasła (tzw. atak Brute Force). Jeżeli właściciel pamięci LP50G2 zapomni hasło, zostaną zastosowane takie same mechanizmy bezpieczeństwa, w tym sformatowanie urządzenia. * Więcej informacji na temat tej funkcji znajduje się w rozdziale „Resetowanie urządzenia” na stronie 27.	Hasło użytkownika (WYŁĄCZONY tryb administratora)  SFORMATOWANIE URZĄDZENIA* Ilustracja 10.5

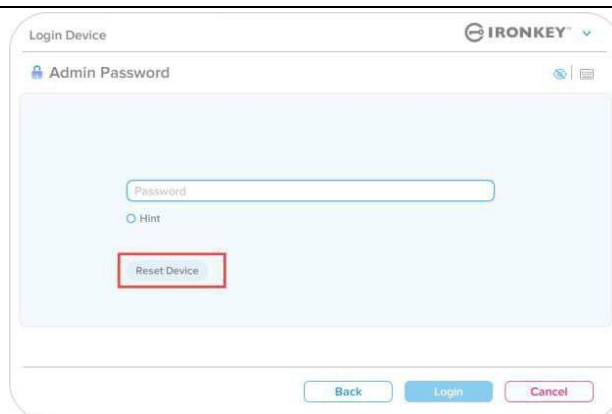
*** Uwaga:** sformatowanie urządzenia spowoduje wymazanie **WSZYSTKICH** informacji przechowywanych na bezpiecznej partycji danych pamięci LP50G2.

Pomoc i rozwiązywanie problemów

Resetowanie urządzenia

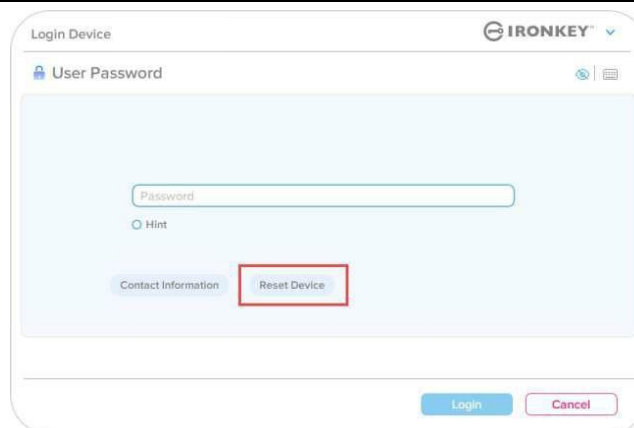
W przypadku zapomnienia hasła lub konieczności zresetowania urządzenia można kliknąć przycisk *Reset Device* (*Resetuj urządzenie*), który pojawia się w jednym z dwóch miejsc, zależnie od konfiguracji urządzenia (w menu logowania administratora, jeśli włączony jest tryb administratora/użytkownika, lub w menu logowania użytkownika, jeśli tryb administratora/użytkownika jest wyłączony) podczas uruchamiania oprogramowania pamięci LP50G2 (patrz ilustracje 10.7 i 10.8).

- Ta opcja umożliwia utworzenie nowego hasła, jednak w celu ochrony poufności danych pamięć LP50G2 zostanie sformatowana. Oznacza to, że wszystkie dane zostaną usunięte.*



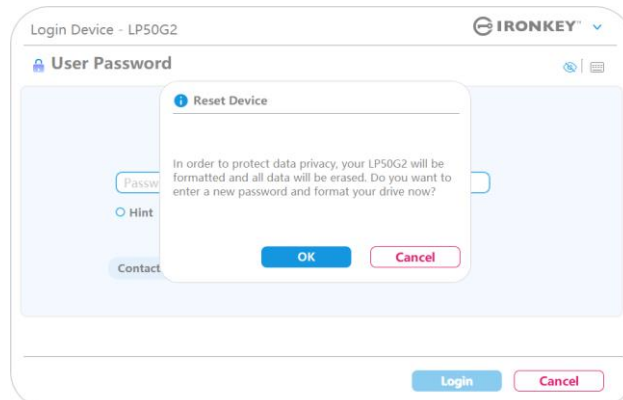
Ilustracja 10.6 – Hasło administratora:
przycisk resetowania urządzenia

- Uwaga:** Po kliknięciu przycisku *Reset Device* (*Resetuj urządzenie*) wyświetli się komunikat z pytaniem, czy użytkownik chce wprowadzić nowe hasło przed rozpoczęciem formatowania. Na tym etapie można 1) kliknąć przycisk OK, aby potwierdzić, lub 2) kliknąć przycisk Cancel (Anuluj), aby powrócić do okna logowania (patrz ilustracja 10.8).



Ilustracja 10.7 – Hasło użytkownika
(tryb administratora/użytkownika włączony):
przycisk resetowania urządzenia

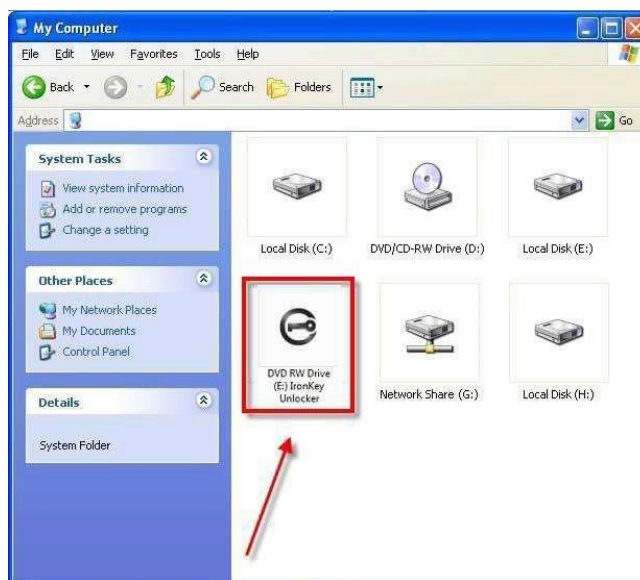
- Po wybraniu opcji kontynuacji zostanie wyświetlony ekran inicjalizacji, na którym można włączyć tryb administratora i użytkownika oraz wprowadzić nowe hasło zgodnie z wybraną opcją (hasło złożone lub wyrażenie hasłowe). Wypełnienie pola wskazówki nie jest konieczne, może jednak pomóc w przypomnieniu sobie zapomnianego hasła.



Ilustracja 10.8 – Potwierdzenie resetowania urządzenia

Konflikt liter dysku: system operacyjny Windows

- Jak wspomniano w części *Wymagania systemowe* niniejszej instrukcji (str. 4), pamięć LP50G2 wymaga dwóch kolejnych liter dysku PO ostatnim dysku fizycznym, który pojawia się przed „luką” w przypisaniu liter dysku (patrz *ilustracja 10.9*). NIE ma to zastosowania do zasobów sieciowych, ponieważ są one specyficzne dla profili użytkownika, a nie samego profilu sprzętu, przez co wydają się one dostępne dla systemu operacyjnego.
- Oznacza to, że system Windows może przypisać pamięci LP50G2 literę dysku, która jest już używana przez zasób sieciowy lub ścieżkę Universal Naming Convention (UNC), powodując konflikt liter dysku. W takim przypadku należy skontaktować się z administratorem lub działem pomocy technicznej w celu zmiany przypisania liter dysku w obszarze Zarządzanie dyskami systemu Windows (wymagane są uprawnienia administratora).



Ilustracja 10.9 – Przykład litery dysku

W tym przykładzie (*ilustracja 10.9*) pamięć LP50G2 korzysta z litery dysku F:, która jest pierwszą dostępną literą po literze E: (przypisanej do ostatniego dysku fizycznego przed luką). Ponieważ litera G: jest zasobem sieciowym nieobjętym profilem sprzętu, pamięć LP50G2 może podjąć próbę użycia jej jako drugiej litery, co spowoduje konflikt.

Jeśli w systemie nie ma udziałów sieciowych, ale pamięci LP50G2 nadal nie można uruchomić, możliwe, że konflikt powoduje inne, wcześniej zainstalowane urządzenie, do którego przypisano literę dysku (np. czytnik kart lub dysk wymienny).

W systemie Windows 11 funkcja zarządzania literami dysków została znacznie ulepszona, więc powyższy problem może nie wystąpić. Jeśli jednak nie można rozwiązać konfliktu, należy skontaktować się z działem pomocy technicznej firmy Kingston lub przejść na stronę Kingston.com/support w celu uzyskania pomocy.

IRONKEY™ Locker+ 50 G2
(LP50G2) セキュア USB 3.2 Gen 1
フラッシュドライブ

ユーザー ガイド



目次

はじめに	3
Locker+ 50 G2 の機能	4
本書について	4
システム要件	4
推奨事項	5
適切なファイルシステムの使用	5
使用上の注意	5
パスワード設定のベストプラクティス	6
マイデバイスの設定	7
デバイスへのアクセス（Windows 環境）	7
デバイスへのアクセス（macOS 環境）	7
デバイスの初期化（Windows および macOS 環境）	8
パスワードの選択	9
仮想キーボード	11
パスワード表示の切り替え	12
管理者およびユーザーのパスワード	13
連絡先情報	15
デバイスの使用（Windows および macOS 環境）	16
管理者およびユーザーのログイン（管理者が有効な場合）	16
ユーザー専用モードでのログイン（管理者が無効）	16
ブルートフォース攻撃の防止	17
セキュリティ保護されたファイルへのアクセス	17
デバイスオプション。	18
LP50G2 の設定	20
管理者設定	20
ユーザー設定: 管理者有効	21
ユーザー設定: 管理者無効	22
LP50G2 設定の変更と保存	23
Adm管理者の機能	24
ユーザーパスワードのリセット	24
ヘルプとトラブルシューティング	25
LP50G2 の設定	25
LP50G2 デバイスのリセット	27
ドライブ文字の競合:（Windows）	28



図 1: IronKey LP50G2

はじめに

Kingston IronKey™ Locker+ 50 G2 USB フラッシュドライブは、XTS モードで FIPS 197 認証の AES 256 ビットハードウェア暗号化を使用してインタープライズグレードのセキュリティ機能を提供し、BadUSB やブルートフォース攻撃などの脅威を防御します。LP50G2 は TAA にも準拠しています。

LP50G2 は、マルチパスワード（管理者およびユーザー）オプションをサポートするようになったため、複雑モードまたはパズルモードを使用できるようになりました。複雑モードでは、6～16文字のパスワードを4種類の文字セットのうち3種類以上を使用して設定できます。新しいパズルモードでは、10～64文字で数値の PIN、文章、単語リスト、または歌詞を使用して設定できます。管理者は、ユーザーパスワードを有効にしたり、データへのアクセスを復元するためにユーザーパスワードをリセットしたりできます。パスワードの入力を間違えないようにするために、「目」のマークを有効にしてパスワードの入力内容が確認できるため、ログイン試行の失敗につながる入力ミスを低減できます。ブルートフォース攻撃保護では、10 回連続で誤ったパスワードを入力したユーザーがロックされ、10 回連続で管理者パスワードが入力されるとドライブが暗号化消去されます。また、内蔵の仮想キーボードにより、キーロガーやスクリーンロガーからパスワードが保護されます。

Locker+ 50 G2 は、小型の金属製ケースに収納されており、キーループが付属しているため、持ち運びしやすい設計になっています。

LP50G2 は、5 年間の限定保証付きで無料の Kingston テクニカルサポートを無料で受けることができます。

IronKey Locker+ 50 G2 の機能

- FIPS 197 認証済み
- XTS-AES ハードウェア暗号化（暗号化機能はオフにすることはできません）
- ブルートフォース攻撃と BadUSB 攻撃の保護
- マルチパスワードオプション
- 複雑またはパスフレーズパスワードモード
- 目のボタンを使用して入力したパスワードを表示することで、ログイン試
行の失敗を低減
- 仮想キーボードによるキーロガーやスクリーンロガーからの保護
- Windows または macOS 対応（詳細はデータシートを参照）

本書について（02122026）

本書は IronKey Locker+ 50 G2（LP50G2）を対象にしています。

システム要件

PC プラットフォーム • Intel および AMD • 15MB の空き容量 • USB 2.0～3.2 ポートに対応 • 最後の物理ドライブの後に、2 つの連続した ドライブ文字を使用する* *注：「ドライブ文字の競合」（28ページ）を参照して ください。	PC オペレーティングシステムのサポート • Windows 11
Mac プラットフォーム • Intel および Apple SOC • 15MB のディスク空き容量 • USB 2.0～3.2 ポート	Mac オペレーティングシステムのサポート • macOS 13.x～26.x

推奨事項

LP50G2 デバイスに十分な電力が供給されるようにするために、ノートパソコンやデスクトップの USB ポートに直接挿入してください（図 1.1 を参照）。LP50G2 は キーボードや USB 電源ハブなどの USB ポート搭載の周辺機器に接続しないでください（図 1.2 を参照）。



図 1.1 – 推奨される使用方法



図 1.2 - 推奨されない使用方法

適切なファイルシステムの使用

IronKey LP50G2 は、事前に FAT32 ファイルシステムでフォーマットされています。Windows と macOS システムで動作します。ドライブを手動でフォーマットすれば、Windows での NTFS や exFAT など他のオプションも使用できます。必要に応じてデータパーティションを再フォーマットできますが、ドライブが再フォーマットされるとデータが失われます。

使用上の注意

データを保護する場合、Kingston では次のことを推奨しています。

- コンピュータでウイルススキャンを実行してから、対象のシステムで LP50G2 を設定して使用してください。
- 共有システムまたは馴染みのないシステムのドライブを使用する場合、マルウェアからドライブを保護するために、読み取り専用モードに設定してください。
- 使用されていないデバイスをロックしてください。
- ドライブを取り外す前にイジェクト操作を実行してください。
- LED が点灯しているときは、絶対に電源をオフにしないでください。オフにすると、ドライブが損傷して再フォーマットが必要になるおそれがあります。その場合、データが消去されます。
- デバイスのパスワードを他人と共有しないでください。

ドライブの最新の更新プログラムと情報を確認する

ドライブの最新の更新プログラム、よくある質問、参考資料、その他の情報については、kingston.com/support を参照してください。

注記：ドライブの最新の更新プログラム 保存データの喪失やその他のドライブ機能が影響を受ける可能性があるため、古いソフトウェアバージョンにドライブをダウングレードすることはサポートされていません。質問や問題がある場合は、Kingston テクニカルサポートまでお問い合わせください。

パスワード設定のベストプラクティス

LP50G2 には、強力なセキュリティ対策が施されています。これらの対策には、ブルートフォース攻撃に対する保護機能が含まれており、パスワードの再入力を 10 回までに制限することで、攻撃者がパスワードを推測できないようにします。ドライブの制限に達すると、LP50G2 は暗号化したデータを自動的に削除し、工場出荷時設定にフォーマットします。

マルチパスワード

ひとつ以上のパスワードを忘れた場合のデータ損失を防ぐ主な機能として、LP50G2 ではマルチパスワードをサポートしています。すべてのパスワードオプションを有効にすると、LP50G2 ではデータ回復用に、管理者とユーザーの役割に合わせて、2 つの異なるパスワードを使用することができます。

LP50G2 では、管理者パスワード（Admin パスワードとも言う）とユーザーパスワードの 2 種類のパスワードを選択できます。管理者は、いつでもドライブにアクセスして、管理者はスーパーユーザーのようにユーザー用のオプションを設定できます。

ユーザーもドライブにアクセスできますが、管理者と比較すると権限が制限されています。2 つのうち一方のパスワードを忘れた場合、もう一方のパスワードを使用して、ドライブにアクセスしてデータを取得できます。その後、ドライブに 2 つのパスワードを設定しなおすことができます。2 種類のパスワードを設定し、管理者パスワードは安全な場所に保存し、ユーザーパスワードを使用することを推奨します。

すべてのパスワードを忘れたり、紛失したりした場合、データにアクセスできなくなります。このセキュリティ機能には、バックドアがないため、Kingston はデータを取得できません。Kingston では、データを別のメディアにも保存しておくことを推奨しています。LP50G2 は、リセットや再使用できますが、以前のデータは完全に消去されます。

パスワードモード

LP50G2 は、次の 2 つの異なるパスワードモードもサポートしています。

複雑なパスワード

複雑なパスワードは、次のうち 3 種類以上の文字を使用して、6～16 文字以上で作成する必要があります。

- 英大文字
- 英小文字
- 数字
- 特殊文字

パスフレーズ

LP50G2 では、10～64 文字のパスフレーズをサポートしています。パスフレーズには、追加ルールはありませんが、適切に使用すれば、非常に高いレベルのパスワード保護が提供されます。

基本的にパスフレーズは、別の言語の文字を含む任意の文字列を組み合わせで設定できます。LP50G2 のように、パスワードの言語を、ドライブ用に選択した言語と一致させることができます。これにより、複数の単語、フレーズ、歌詞、詩の一節など使用できます。攻撃者にとって推測することが最も困難なパスワードの 1 つですが、ユーザーにとっては覚えやすいパスワードになります。

マイデバイスの設定

IronKey 暗号化 USB ドライブに十分な電力を供給するように、ノートパソコンまたはデスクトップパソコンの USB 2.0/3.0 ポートに直接に差し込んでください。キーボードや USB 電源ハブなどの USB ポート搭載の周辺機器に接続しないでください。デバイスの初期設定は、サポート対象の Windows または macOS ベースのオペレーティングシステムで実行する必要があります。

デバイスへのアクセス（Windows 環境）

IronKey 暗号化 USB ドライブをノートパソコンまたはデスクトップの空いている USB ポートに接続して、Windows により認識されるのを待ちます。

- Windows ユーザーは、デバイスドライバーの通知を受信します。
(図 3.1)



図 3.1 – デバイスドライバーの通知

- 新しいハードウェアが検出されたら、File Explorer で Unlocker パーティション内の **IronKey.exe** オプションを選択します。
(図 3.2)
- パーティション文字は、次の空ドライブ文字に応じて変化することに注意してください。ドライブ文字は、接続されたデバイスに応じて変更されます。右の画像では、ドライブ文字を (E:) にしています。



図 3.2 – File Explorer Window/IronKey.exe

デバイスへのアクセス（macOS 環境）

LP50G2 をノートパソコンやデスクトップの空いている USB ポートに挿入し、Mac オペレーティングシステムにより検出されるのを待ちます。検出されたら、デスクトップに「IRONKEY」ボリュームが表示されます (図 3.3)。

- IronKey CD-ROM アイコンをダブルクリックします。
- その後、図 3.3 のウィンドウに表示された IronKey.app アプリケーションのアイコンをダブルクリックします。これで初期化プロセスが開始されます。

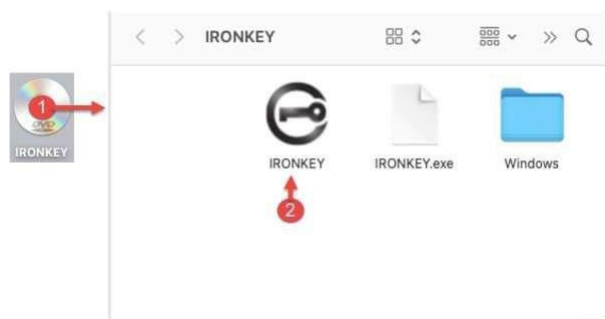


図 3.3 – IRONKEY ボリューム

デバイスの初期化（Windows および macOS 環境）

言語と EULA

ドロップダウンから優先減を選択して 次へ をクリックします。（図 4.1 を参照）

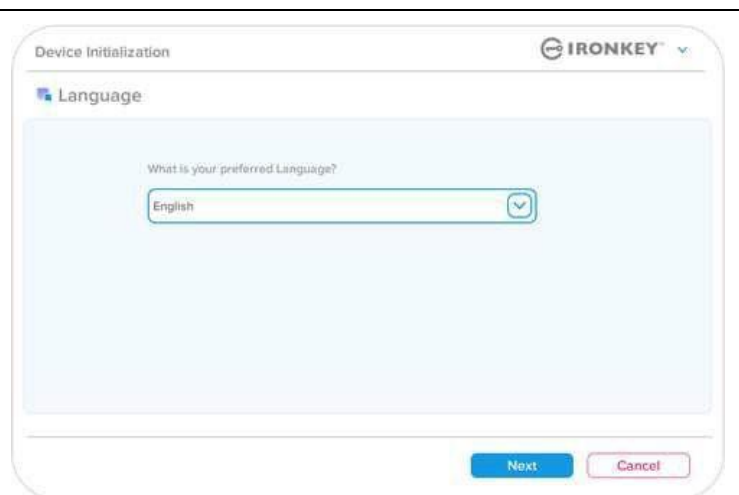


図 4.1 – 言語の選択

ライセンス契約を確認して、次へ をクリックします。

注：続行するにはライセンス契約に同意します。
同意しない場合は、次へ ボタンが有効になりません。（図 4.2）

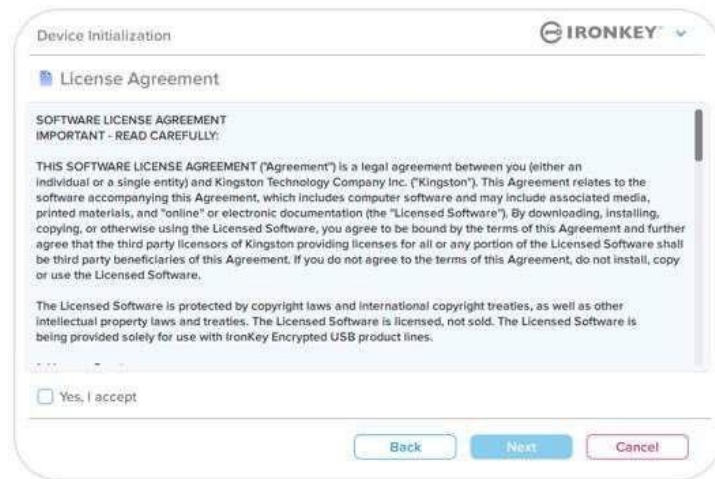


図 4.2 – ライセンス契約

デバイスの初期化

パスワードの選択

パスワード入力画面で、複雑パスワードモードまたはパスフレーズパスワードモードのいずれかを使用して、LP50G2 のデータを保護するためのパスワードを設定できます（図 4.3～4.4）。また、この画面では、マルチパスワード管理者/ユーザーオプションも有効にできます。パスワードの選択に進む前に、以下の 管理者/パスワードの有効化 を確認して、これらの機能を理解してください。

注: 一旦複雑なパスワードとパスフレーズモードのどちらかを選択した後は、デバイスをリセットするまでモードを変更できません。パスワードの選択を開始するには、パスワード フィールドでパスワードを設定してから、パスワードの確認 フィールドにパスワードを再入力してください。作成したパスワードは次の条件を満たさないと、初期化プロセスに進むことができません。

複雑なパスワード

- 6 文字以上（最大 16 文字）で構成
- 次の 3 つの条件を満たすこと
 - 英大文字
 - 英小文字
 - 数字
 - 特殊文字（!、\$、& など）

図 4.3 – 複雑なパスワード

パスフレーズパスワード

- 文字数の制限：
 - 最短 10 文字
 - 最長 64 文字

図 4.4 – パスフレーズパスワード

パスワードのヒント（任意）

パスワードのヒントは、パスワードを忘れた場合に、手がかりを提供します。

注: パスワードのヒントは、パスワードと完全に一致させることはできません。

図 4.5 – パスワードのヒント フィールド

デバイスの初期化

有効なパスワードと無効なパスワード

有効なパスワードの場合、基準に合致していると、パスワードの基準ボックスが**緑**で表示されます。（図 4.6a～b を参照）

注: パスワードの条件が 3 つ以上満たされると、4 つめの条件のボックスが自動的にグレー表示になり、その条件が任意になったことが示されます（図 4.6b）。

The screenshot shows the 'Device Initialization' window with the 'Password' tab selected. Under the 'Complex' sub-tab, there is a prompt to create a secure password. Two input fields contain 'ExamplePasswOrd!'. Below the fields, four criteria are listed with green checkmarks: '6-16 long', 'uppercase', 'lowercase', and 'digit'. The 'special character' criterion is also present but is grayed out. A 'Password Hint?' field is at the bottom. At the very bottom, there is a checkbox for 'Enable Admin and User Passwords' and three buttons: 'Back', 'Next', and 'Cancel'.

図 4.6a – 複雑なパスワードの条件を満たしている場合

This screenshot is similar to the previous one, but the 'special character' criterion is highlighted with a red box and has a red 'x' icon, indicating it is an optional requirement. The other criteria ('6-16 long', 'uppercase', 'lowercase', 'digit') are still marked with green checkmarks.

図 4.6b – 複雑なパスワードの条件（任意）

無効なパスワードの場合、パスワードの条件ボックスが、**赤**で強調表示され、最低限の要件が満たされない限り **次へ** ボタンが無効になります。

この動作は、複雑なパスワードとパスフレーズパスワードの両方に適用されます。

The screenshot shows the password creation screen where the criteria 'digit' and 'special character' are marked with red 'x' icons, indicating they are not met. The '6-16 long' and 'uppercase' criteria are still marked with green checkmarks. The 'Next' button is disabled.

図 4.7 – パスワードの条件が満たされていない

デバイスの初期化

仮想キーボード

LP50G2 は、キーロガーを防御できる仮想キーボードを搭載しています。

- 仮想キーボードを使用するには、デバイスの初期化画面の右上にあるキーボードボタンを選択します。

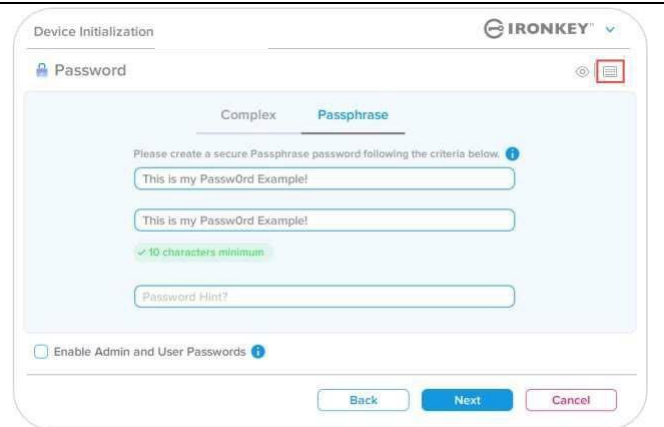


図 4.8 – 仮想キーボードの有効化

- 仮想キーボードが表示されると、スクリーンロガー保護も有効になります。この機能を使用すると、すべてのキーが一時的にブランクになります。これは仕様どおりの動作です。これにより、スクリーンロガーによるクリック動作の取得を防ぎます。
- この機能をより堅牢するために、キーボードの右下にある **ランダム化** を選択して、仮想キーボードをランダム化できます。ランダム化すると、キー配列がランダムになります。



図 4.9 – スクリーンロガー保護/ランダム化

デバイスの初期化

パスワード表示の切り替え

デフォルトでは、パスワードを設定すると、パスワードの入力に応じて、その文字列がフィールドに表示されます。パスワードの文字列の入力を非表示にしたい場合は、デバイスの初期化 ウィンドウの右上にある「目」で表示/非常時を切り替えることができます。

注: デバイスが初期化されると、パスワードフィールドはデフォルトで「非表示」になります。

パスワードの文字列を**非表示**にするには、グレーのアイコンをクリックします。

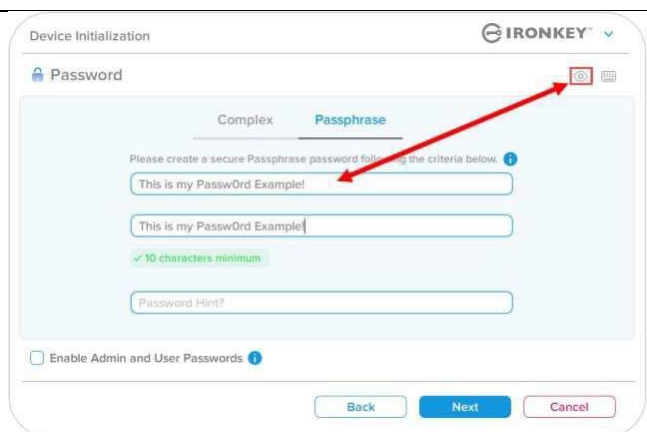


図 4.10 – パスワードを非表示にする

非表示のパスワードを**表示**するには、青のアイコンをクリックします。

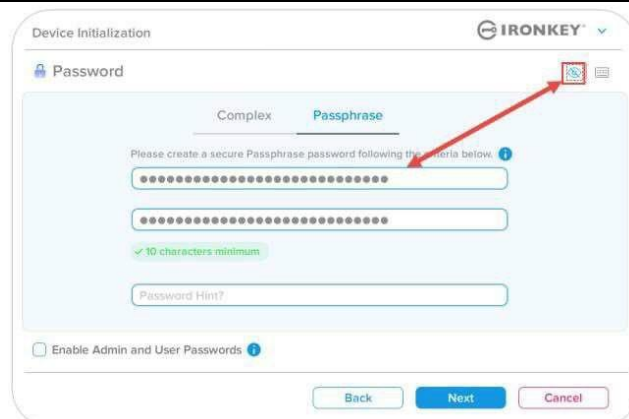


図 4.11 – パスワードを表示する

デバイスの初期化

管理者およびユーザーのパスワード

管理者およびユーザーパスワードを有効にするには、マルチパスワード機能を利用します。これにより、管理者ロールは両方のアカウントを管理できます。**管理者/ユーザーパスワードを有効にする** を選択すると、どちらかのパスワードを忘れた場合に別の方法でドライブにアクセスできるようになります。

管理者/ユーザーパスワードを有効にすると、次の機能にアクセスできます。

- ユーザーパスワードのリセット

ユーザーパスワードのリセット機能の詳細については、本書の 24 ページを参照してください。

- **管理者/ユーザーパスワードを有効にするには、管理者/ユーザーパスワードを有効にする** の横にあるボックスをクリックして、有効なパスワードが選択されたら **次へ** を選択します。(図 4.12)
- この機能が**有効**な場合、この画面で選択したパスワードが**管理者パスワード**になります。**次へ** を選択すると、**ユーザーパスワード** 画面に移動し、ユーザー用に選択されたパスワードを確認できます。

図 4.12 – 管理者/ユーザーパスワードの有効化

注: 管理者/ユーザーパスワードの有効化はオプションです。

この機能を有効にせずにドライブを設定すると（ボックスを選択しない）、ドライブは、**管理者機能のないシングルユーザー/シングルパスワード**を使用したドライブとして設定されます。本書では、この設定のことをユーザー専用モードと言います。

シングルユーザー/シングルパスワード設定で操作を続けるには、**管理者/ユーザーパスワードを有効にする** を選択せずに、有効なパスワードを作成してから **次へ** をクリックします。

デバイスの初期化

管理者およびユーザーのパスワード

前の画面で管理者ロールが**有効**になっている場合、次の画面で**ユーザーパスワード**の入力を求められます（図 4.13）。ユーザーパスワードは管理者パスワードと比較すると機能が限定されています。詳細は以降で説明します。**注：**以降、本書では「**管理者およびユーザーのパスワード**」を「**管理者ロール**」と呼びます。

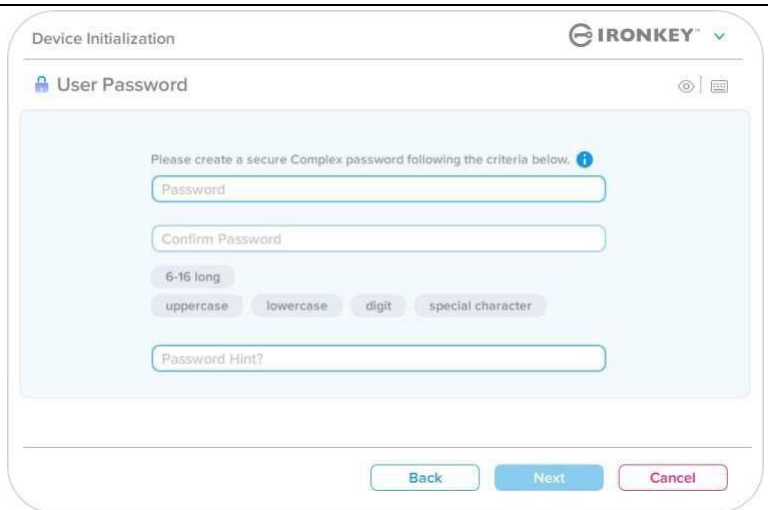


図 4.13 – ユーザーパスワード（管理者およびユーザー有効）

注： 選択したパスワードオプション（複雑またはパズフレーズ）条件はユーザーパスワードと、ドライブの設定後に必要なパスワードリセットに引き継がれます。選択したパスワードオプションは、デバイス全体のリセット後にのみ変更できます。

デバイスの初期化

連絡先情報

表示されたテキストボックスに連絡先情報を入力してください。（図 4.14 を参照）

注: これらのフィールドに入力された情報には、手順 3 で設定したパスワードを入力しないでください。ただし、これらのフィールドは任意のため、必要に応じて空白にすることもできます。

名前 フィールドには、最大 32 文字を入力できますが、パスワードとまったく同じ文字列を入れることはできません。

会社 フィールドには、最大 32 文字を入力できますが、パスワードとまったく同じ文字列を入れることはできません。

詳細 フィールドには、最大 156 文字を入力できますが、パスワードとまったく同じ文字列を入れることはできません。

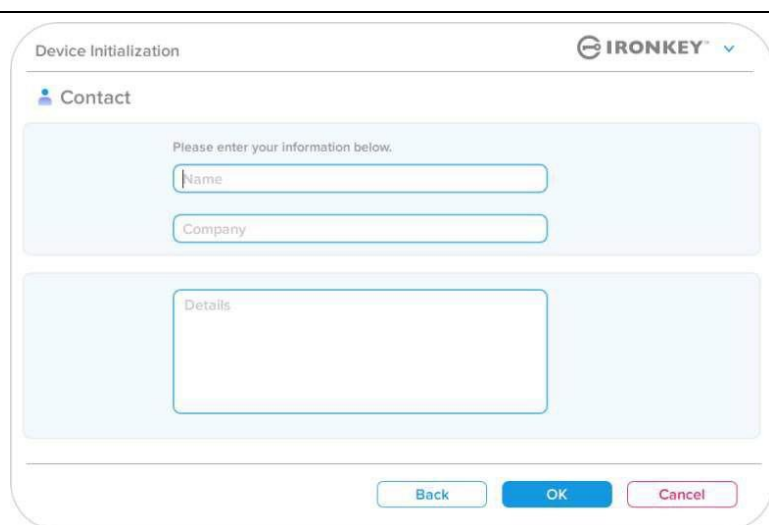
The screenshot shows a 'Device Initialization' window with the 'IRONKEY' logo in the top right. Below the title bar is a 'Contact' section with a person icon. A light blue box contains the text 'Please enter your information below.' followed by three input fields: 'Name', 'Company', and 'Details'. The 'Name' and 'Company' fields are short text boxes, while 'Details' is a larger text area. At the bottom of the window are three buttons: 'Back', 'OK', and 'Cancel'.

図 4.14 – 連絡先情報

注: OK をクリックすると、初期化プロセスが完了し、アンロックに進んで、データを安全に保存できる安全なパーティションを取り付けます。変更が適用されているかどうかを確認するには、ドライブを抜き差ししてください。

デバイスの使用（Windows および macOS 環境）

管理者およびユーザーのログイン（管理者が有効）

デバイスが管理者/ユーザーパスワード（管理者ロール）を有効にして初期化されている場合、IronKey LP50G2 アプリケーションが起動し、最初にユーザーパスワードのログイン画面が表示されます。この画面から、ユーザーパスワードでログインして、入力した連絡先情報を表示したり、管理者としてログインしたりできます（図 6.1）。管理者としてログインする（以下を参照）をクリックすると、アプリケーションが管理者ログインメニューに移動し、管理者としてログインして、管理者設定と機能にアクセスできます（図 6.2）。

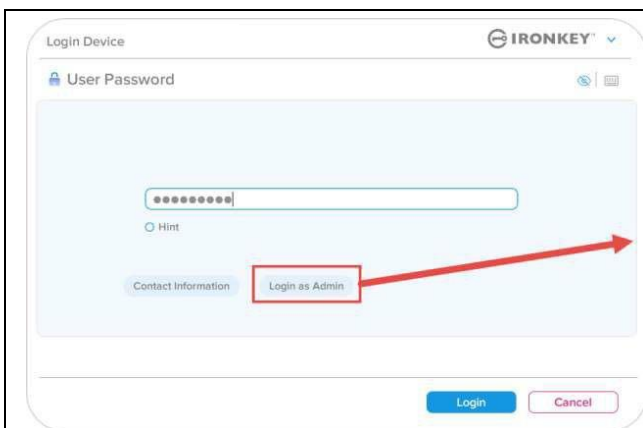


図 6.1 – ユーザーパスワードによるログイン（管理者が有効）

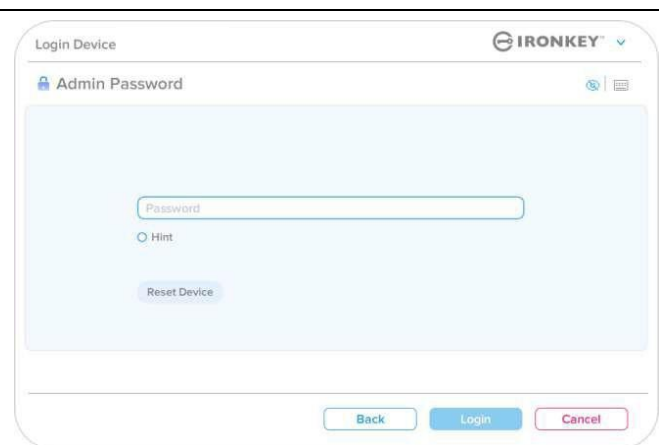


図 6.2 – 管理者パスワードによるログイン

ユーザー専用モードでのログイン（管理者が無効な場合）

13 ページで説明したように、デバイスの機能を最大限利用するには管理者ロールを使用することが推奨されますが、IronKey ドライブはユーザー専用（シングルパスワード、シングルユーザー）設定で初期化することもできます。これは、シンプルなシングルパスワードアプローチでドライブのデータを保護したいユーザーに適したオプションです。（図 6.3）

注： 管理者/ユーザーパスワードを有効にするには、**デバイスのリセット** ボタンを使用してドライブを初期化状態に戻し、管理者/ユーザーパスワードを有効にできます。
デバイスのリセットを実行すると、ドライブ上のすべてのデータは、フォーマットされ完全に消去されます。

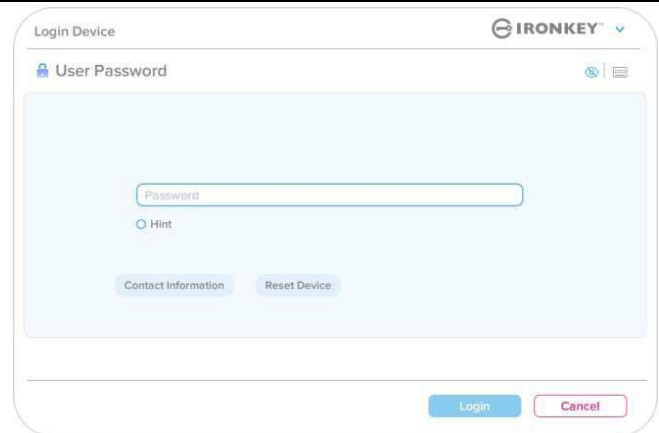


図 6.3 – ユーザーパスワードのログイン（管理者が無効）

デバイスの使用

ブルートフォース攻撃の防止

重要: ログイン中に間違ったパスワードを入力した場合、正しいパスワードを入力し直せます。ただし、不正アクセス回数を記録するセキュリティ機能（ブルートフォース攻撃防止機能ともいいます）がありますのでご注意ください。*

この回数が事前設定された 10 回のパスワード試行の失敗 に達すると、次のような動作が発生します:

管理者/ユーザー有効	ブルートフォース攻撃保護デバイスの動作 (10 回の間違ったパスワード試行)	データ消去および デバイスをリセットします か？
ユーザーパスワード	パスワードがロックされます。管理者としてログインしユーザーパスワードをリセットする	いいえ
管理者パスワード	ドライブを暗号化消去します。パスワード、設定、およびデータが永久に消去されます	はい
ユーザーのみ シングルユーザー/シングルパスワード (管理者/ユーザーが無効)	ブルートフォース攻撃保護デバイスの動作 (10 回の間違ったパスワード試行)	データ消去および デバイスをリセットします か？
ユーザーパスワード	暗号化消去ドライブ、パスワード、設定、および完全なデータ消去	はい

*デバイスが正常に認証されると、使用しているログイン方法に応じて失敗したログインの回数がリセットされます。暗号化消去では、すべてのパスワード、暗号化キー、およびデータが削除されます。**この場合、データは完全に消去されます。**

セキュリティ保護されたファイルへのアクセス

ドライブのロック解除後、保護下のファイルにアクセスできます。ファイルは、ドライブで保存したり開いたりすると、自動的に暗号化/復号化されます。この技術により、通常のドライブと同じように作業できる利便性と、強力な「常時オン」のセキュリティが実現します。

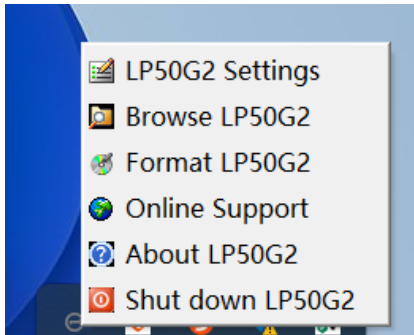
ヒント: Windows タスクバーで **IronKey アイコン** を右クリックするとファイルにアクセスすることもできます。

LP50G2 の参照 (図 7.2)

デバイスのオプション（Windows 環境）

デバイスにログインすると、ウィンドウの右上隅に IronKey アイコンが表示されます。IronKey アイコンを右クリックすると、利用可能なドライブオプションの選択メニューが開きます（図 6.2）。

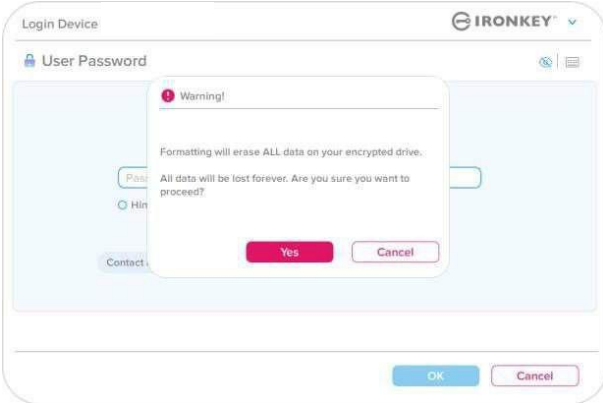
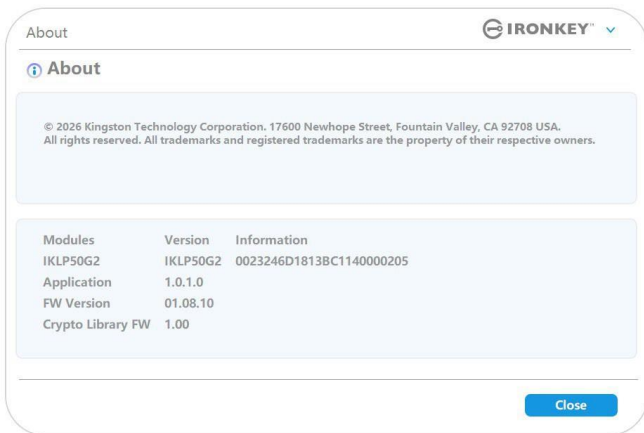
これらのデバイスオプションについて詳しくは、本書の 19～23 ページに記載されています。

• デバイスにログインすると、ウィンドウの右上隅に IronKey アイコンが表示されます。（図 7.1）	 図 7.1 – タスクバーの IronKey アイコン
• IronKey アイコンを右クリックすると、利用可能なドライブオプションの選択メニューが開きます。（図 7.2） これらのデバイスオプションについて詳しくは、本書の 19～23 ページに記載されています。	 図 7.2 – デバイスの IronKey アイコンの右クリック

デバイスのオプション（macOS 環境）

• デバイスにログインすると、図 7.3 のように macOS メニューに IronKey LP50G2 アイコンが表示され、使用可能なデバイスオプションを使用できます。 これらのデバイスオプションについて詳しくは、本書の 19～23 ページに記載されています。	 図 7.3 – macOS メニューバーアイコン/デバイスのオプションメニュー
--	---

デバイスオプション

LP50G2 設定:	ログインパスワード、連絡先情報、およびその他の設定を変更します。（デバイスの設定の詳細は、本書の「LP50G2 設定」セクションで確認できます）。
LP50G2 の参照:	セキュリティ保護されたファイルを表示できます。
LP50G2 のフォーマット: 保護下のデータパーティションをフォーマット できます。（警告：すべてのデータが消去 されます。）（図 6.1） 注: フォーマットにはパスワード認証が必要です。	 図 7.4 – LP50G2 のフォーマット
オンラインサポート:	インターネット・ブラウザを開いて - http://www.kingston.com/support に移動すると、詳しいサポート情報にアクセスできます。
LP50G2 について LP50G2 固有の詳細（アプリケーション、ファームウェア、シリアル番号の情報など）が表示されます（図 6.2） 注: ドライブの固有のシリアル番号が情報列の下に表示されます。	 図 7.5 – LP50G2 について
LP50G2 のシャットダウン	LP50G2 を適切にシャットダウンすると、システムから安全に取り外すことができます。

LP50G2 の設定

管理者設定

管理者ログインにより、次のデバイス設定にアクセスできます。

- **パスワード:** 管理者パスワードやヒントを変更できます（図 8.1）。
- **連絡先情報:** 連絡先の情報を追加/表示/変更できます（図 8.2）。
- **言語:** 現在の言語を変更できます（図 8.3）
- **管理者オプション:** 次の追加機能にアクセスできます。
 - ユーザーパスワードの変更（図 8.4）

注記：管理者オプションの詳細については、25 ページで確認できます。

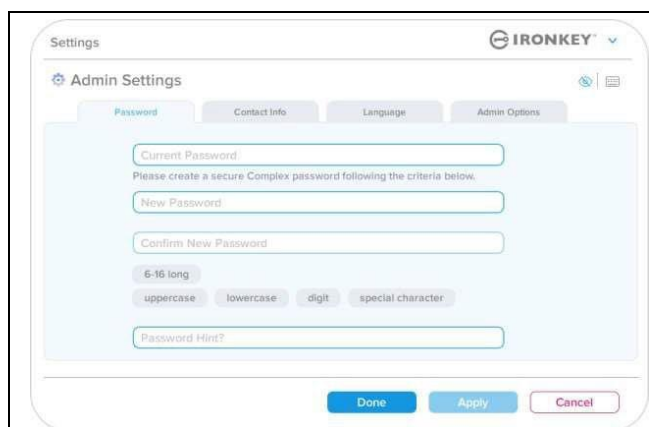


図 8.1 – 管理者パスワードオプション

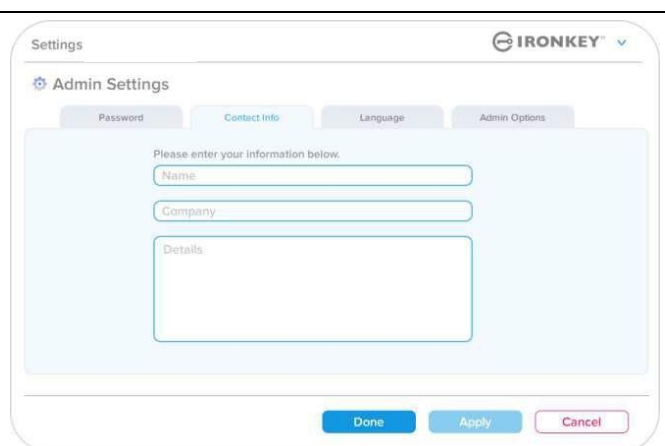


図 8.2 – 連絡先情報

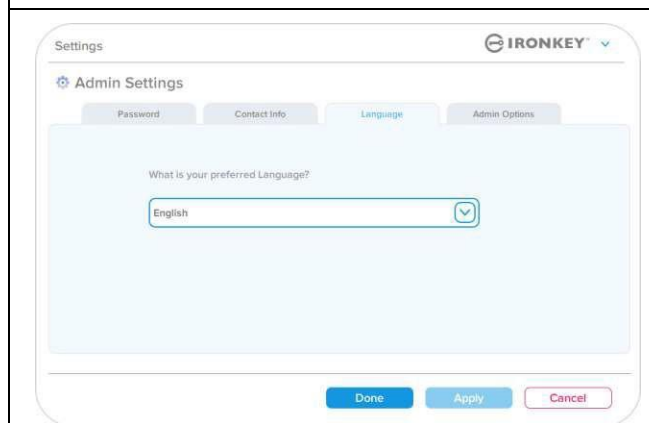


図 8.3 – 言語オプション

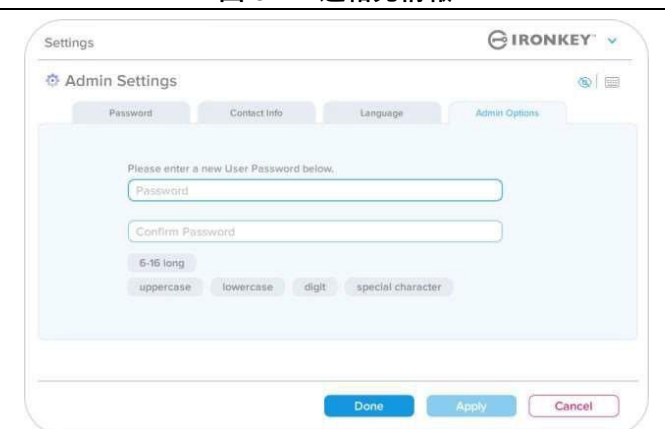


図 8.4 – 管理者オプション

LP50G2 の設定

ユーザー設定:管理者有効

ユーザーログインでは、次の設定へのアクセスが制限されています。

パスワード:

自分のユーザーパスワードやヒントを変更できます。(図 8.5)

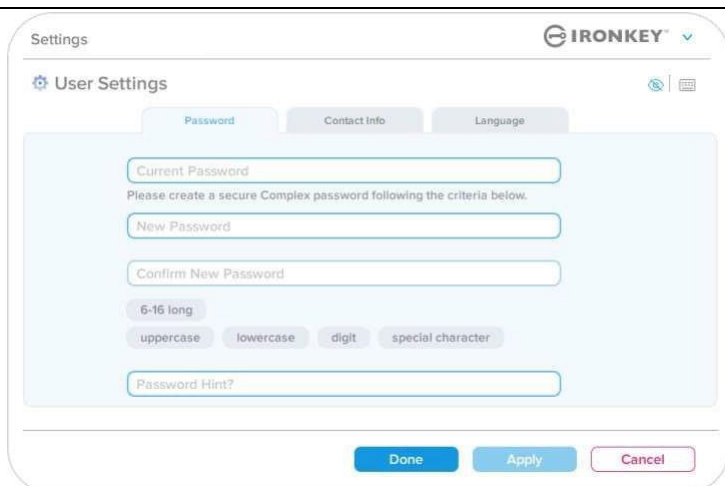


図 8.5 – パスワードオプション (管理者が有効: ユーザーログイン)

連絡先情報:

連絡先情報を追加/表示/変更できます。(図 8.6)

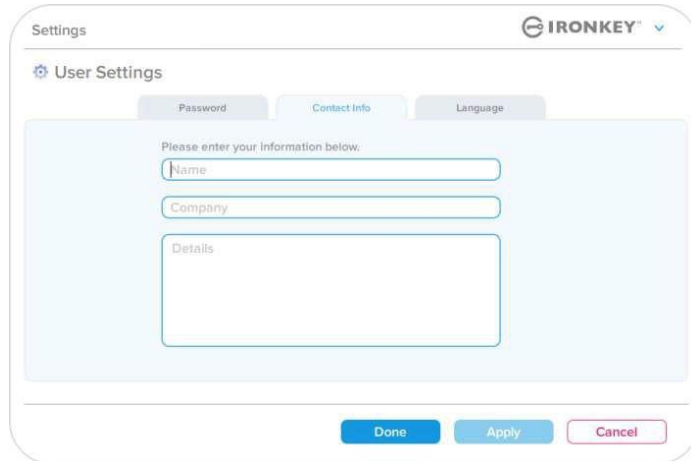


図 8.6 – 連絡先情報 (管理者が有効: ユーザーログイン)

言語:

現在の言語を変更できます。(図 8.7)

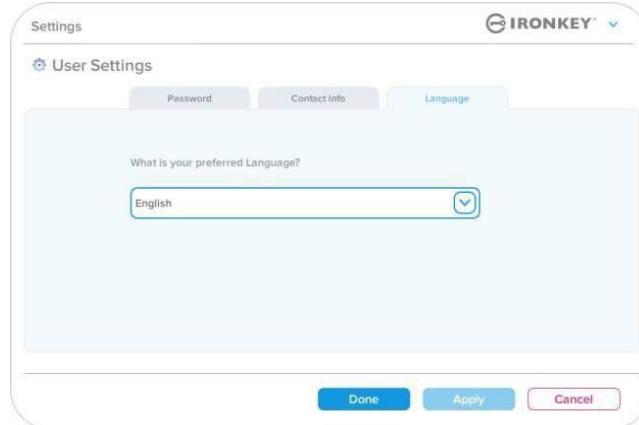


図 8.7 – 言語設定 (管理者が有効: ユーザーログイン)

注: ユーザーパスワードでログインした場合、管理者オプションにはアクセスできません。

LP50G2 の設定

ユーザー設定: 管理者無効

12 ページで説明したように、「管理者およびユーザー」パスワードを有効にせずに LP50G2 を初期化すると、ドライブがシングルユーザー/シングルパスワードで設定されます。この設定では、管理者オプションや機能にアクセスできません。この設定は、次の LP50G2 設定にアクセスできるようになります。

パスワード

自分のユーザーパスワードやヒントを変更できます。(図 8.8)

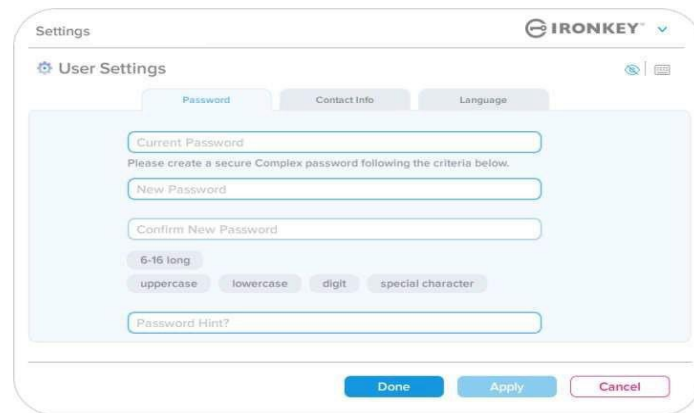


図 8.8 – パスワードオプション (ユーザー専用モード)

連絡先情報:

連絡先情報を追加/表示/変更できます。(図 8.9)

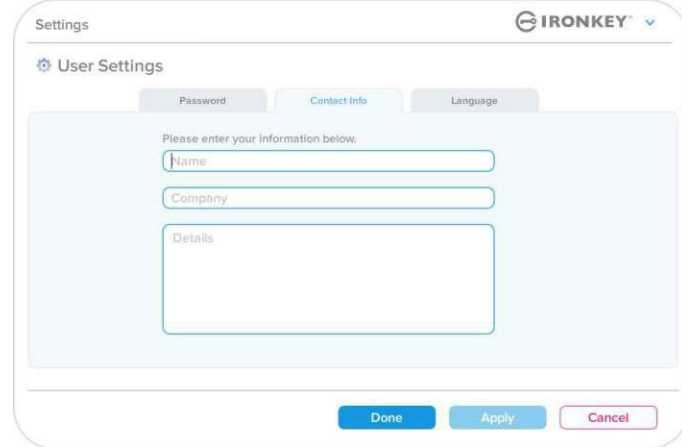


図 8.9 – 連絡先情報 (ユーザー専用モード)

言語:

現在の言語を変更できます。(図 8.10)

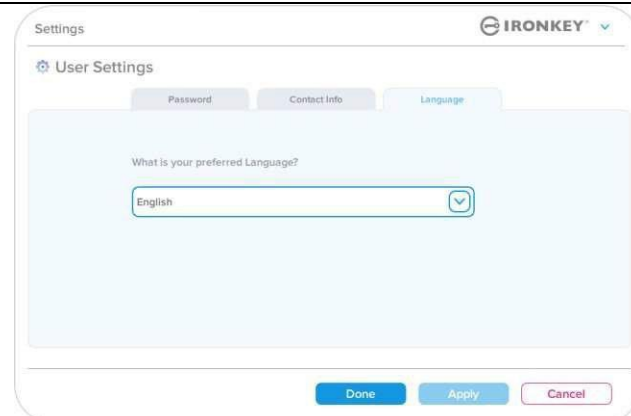


図 8.10 – 言語の設定 (ユーザー専用モード)

LP50G2 の設定

設定の変更と保存

- LP50G2 設定（連絡先情報、言語、パスワードの変更、管理者オプションなど）で設定が変更されると、ドライブにより変更内容に同意して適用するために、パスワードの入力を求められます。（図 8.11 を参照）

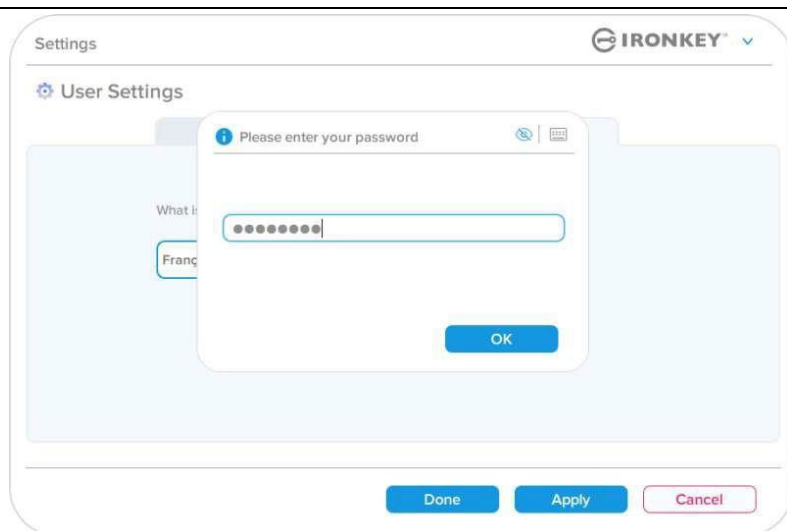


図 8.11 – LP50G2 の設定変更を保存する パスワード入力 画面

注: 上記の手順で、パスワードの入力 画面で捜査している場合、変更内容をキャンセル、または修正には、パスワードフィールドを空白のままにして、OK をクリックします。これにより、パスワードを入力してください ボックスが閉じ、LP50G2 設定メニューに戻ります。

管理者の機能

ユーザーパスワードをリセットするオプション

管理者設定の便利な機能の 1 つは、ユーザーパスワードを忘れた場合に安全にリセットできることです。以下は、ユーザーパスワードのリセット機能です。この機能により、ユーザーパスワードをリセットできます。

ユーザーパスワードのリセット:

管理者オプション メニューでユーザーパスワードを手動で簡単に変更できます。変更内容は、次のユーザーログインで有効になります。(図 9.1)

注: パスワード要件は、初期化プロセス時に設定されたデフォルトの条件に設定されます (複雑またはパスフレーズオプション)。

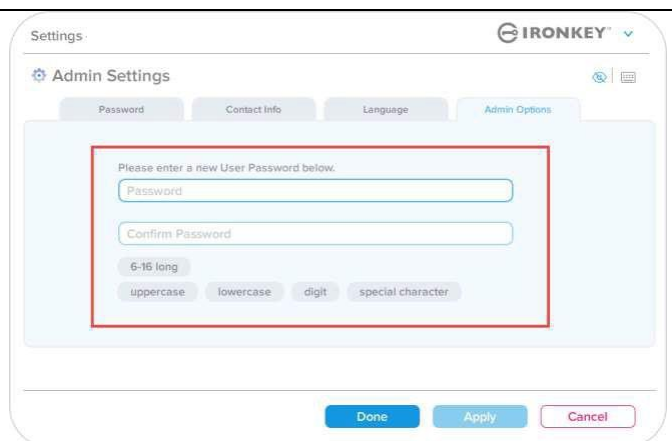
The screenshot shows the 'Settings' window of an IronKey device. The 'Admin Settings' tab is selected, and the 'Password' sub-tab is active. A red rectangular box highlights the password reset section, which includes the text 'Please enter a new User Password below:', two input fields labeled 'Password' and 'Confirm Password', and a list of requirements: '6-16 long', 'uppercase', 'lowercase', 'digit', and 'special character'. At the bottom of the settings window are three buttons: 'Done', 'Apply', and 'Cancel'.

図 9.1 – 管理者オプション/ユーザーパスワードのリセット

ヘルプとトラブルシューティング

デバイスのロックアウト

LP50G2 には、失敗したログイン試行が**連続して**最大回数に達した場合（MaxNoA）に、データパーティションへの不正アクセスを防ぐセキュリティ機能が搭載されています。デフォルトの設定では、各ログイン方法（管理者/ユーザー）に対して 10 回の試行回数が事前設定されています。

「ロックアウト」カウンターがログインの失敗を数え、次の **2 つのいずれかの方法** でリセットします。

1. MaxNoA に達する前に成功したログイン

2. MaxNoA に達し、ドライブの設定方法に応じてデバイスのロックアウトまたはデバイスのフォーマットのいずれかを実行します。

- 不正なパスワードが入力されると、エラーメッセージがパスワード入力フィールドの真上に赤色で表示され、ログインの失敗を通知します。
(図 10.1)

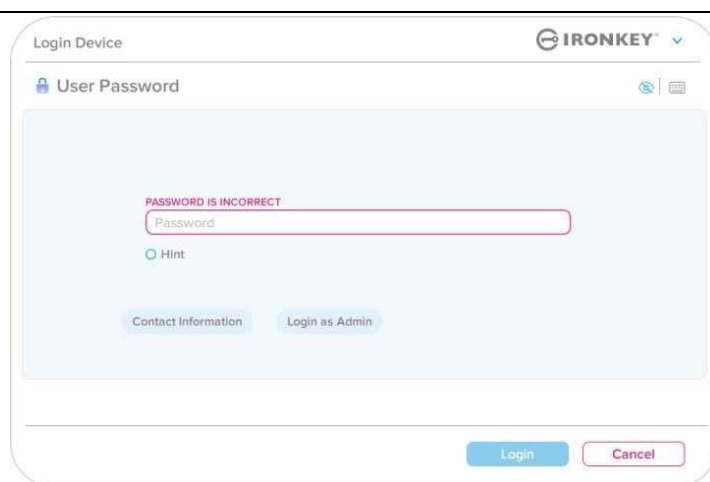


図 10.1 – 誤ったパスワードを通知するメッセージ

- 7 回目**の試行が失敗すると、追加のエラーメッセージが表示され、あと 3 回で MaxNoA（デフォルトで 10 回に設定）に達することが通知されます。(図 10.2)

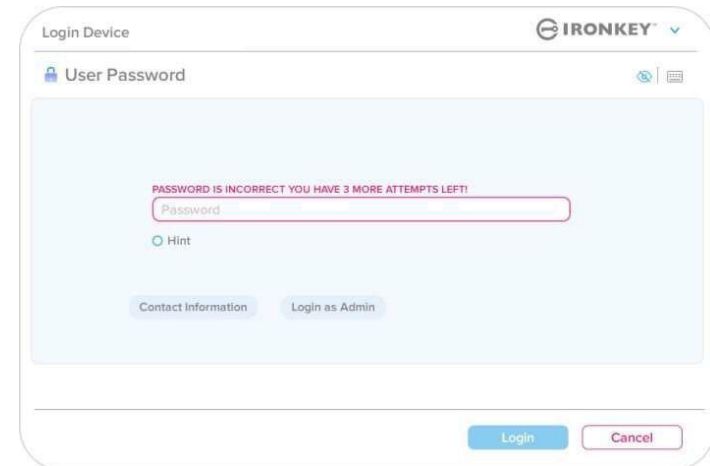


図 10.2 – 7 回の誤ったパスワード試行

ヘルプとトラブルシューティング

デバイスのロックアウト

重要: 10 回目の（最後の）ログイン試行が失敗すると、デバイスの設定方法と使用されているログイン方法（管理者/ユーザー）に応じて、デバイスがロックされ別の方法でログインするか（ある場合）、デバイスリセットを実行する必要があります。デバイスリセットの場合は、データがフォーマットされドライブに保存されているすべてのデータが完全に消去されます。動作は、本書の 17 ページでも説明されています。

以下の図 10.3～10.6 は、各ログインパスワード方法の 10 回目の（最後の）ログイン失敗時の視覚的動作を示しています。

ユーザーパスワード（管理者/ユーザーが有効な場合）

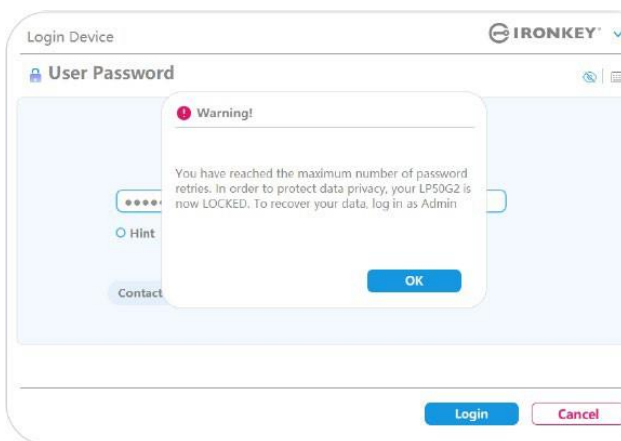


図 10.3: デバイスのロックアウト

管理者パスワード（管理者/ユーザー有効）

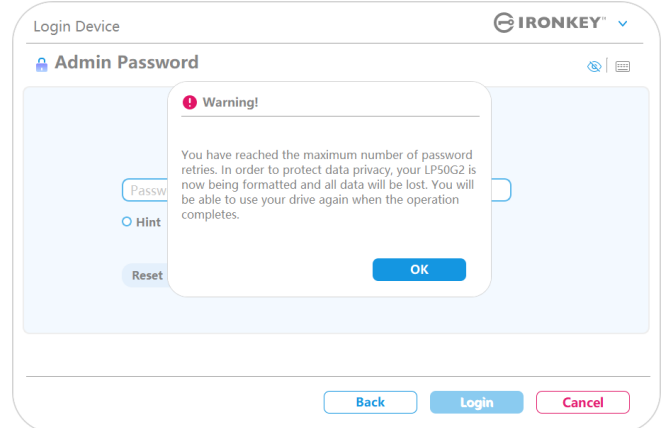


図 10.4: デバイスのフォーマット*

- これらのセキュリティ対策により、パスワードを設定していないユーザーが何回もログインを試行し、機密データにアクセスしようとする（ブルートフォース攻撃ともいう）を防ぐことができます。LP50G2 を持っており、パスワードを忘れた場合、デバイスのフォーマットなど同じセキュリティ対策が適用されます。*この機能の詳細については、「デバイスのリセット」（27 ページ）を参照してください。

ユーザーパスワード（管理者が無効）

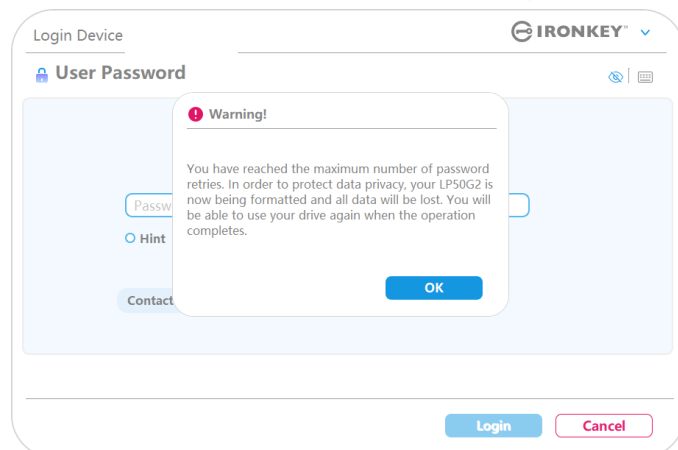


図 10.5: デバイスのフォーマット*

*注：デバイスのフォーマットでは、LP50G2 のセキュアデータパーティションに保存されたすべての情報が消去されます。

ヘルプとトラブルシューティング

デバイスのリセット

パスワードを忘れた場合、またはデバイスのリセットが必要な場合、LP50G2 ランチャーが実行されると、ドライブの設定方法に応じて 2 つの場所のいずれかに表示される デバイスのリセット ボタンをクリックできます（管理者/ユーザーが有効な場合は、管理者ログインパスワード メニュー、または管理者/ユーザーモードが有効ではない場合は、ユーザーパスワード ログインメニューのいずれかに表示されます）。（図 10.7 および 10.8 を参照）

- このオプションを使用すると、新しいパスワードを作成できますが、データのプライバシーを保護するために、LP50G2 がフォーマットされます。これにより、すべてのデータがプロセスから消去されます。*

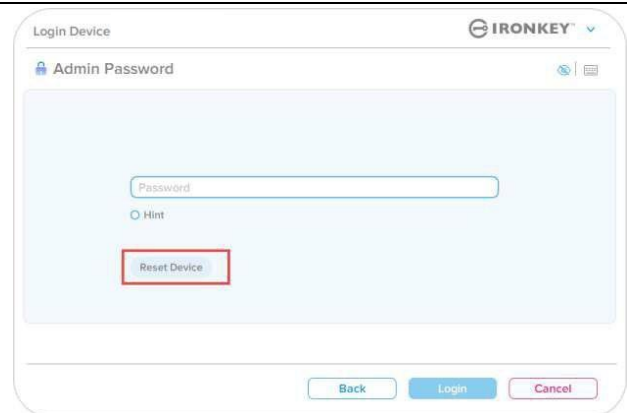


図 10.6 – 管理者パスワード: デバイスのリセットボタン

- 注:** デバイスのリセット をクリックすると、メッセージボックスが表示され、初期化を行う前に新しいパスワードの入力を求めるかどうか尋ねられます。この時点で、1) OK をクリックして確認するか、2) キャンセル をクリックしてログインウィンドウに戻ることができます。（図 10.8 を参照）

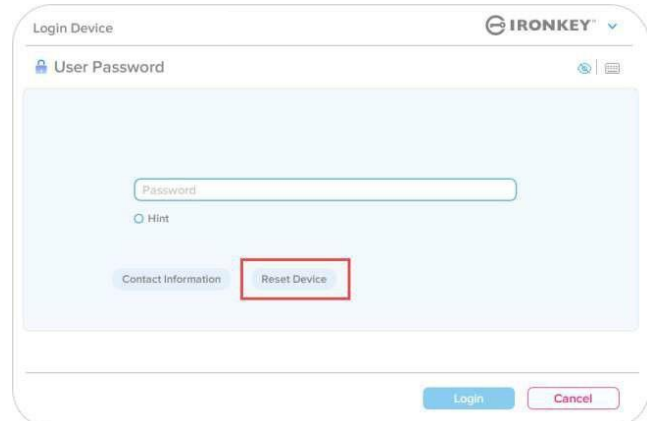


図 10.7 – ユーザーパスワード（管理者/ユーザーが無効）によるデバイスのリセット

- 続行したい場合は、初期化画面が表示され、☑「管理者およびユーザーモード」を有効にして、選択したパスワードオプション（複雑なパスワードまたはパズルフレーズパスワード）に応じて新しいパスワードを入力できます。ヒントの項目は必須ではありませんが、パスワードを忘れた場合に、手がかりを提供します。

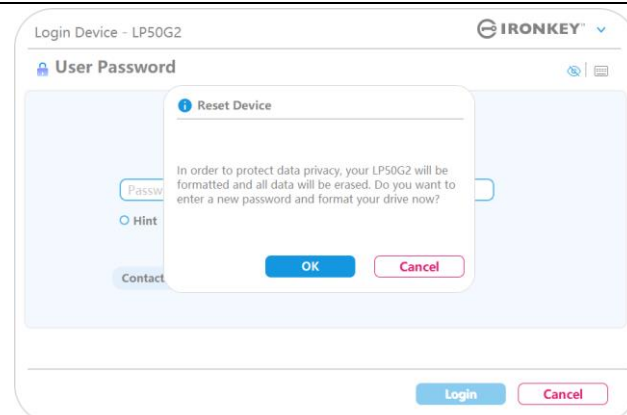
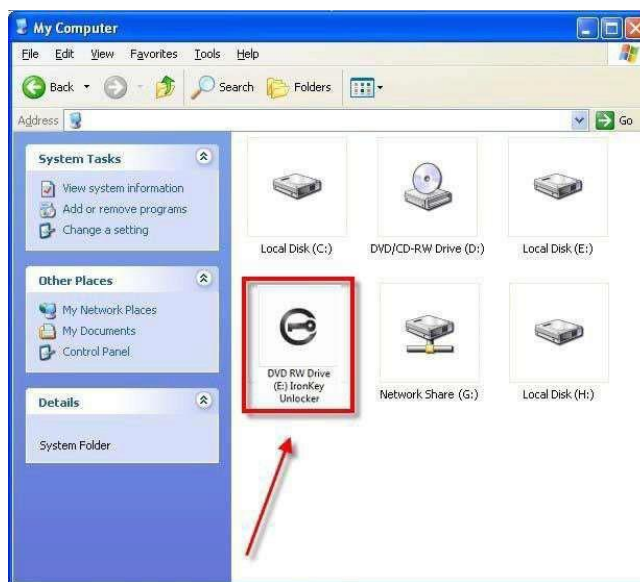


図 10.8 – デバイス認証のリセット

ドライブ文字の競合: Windows オペレーティングシステム

- 本書の「システム要件」セクション（4 ページ）で説明したように、LP50G2 は、ドライブ文字の割り当てに「空き」がある場合、その前に表示されている最後の物理ディスクの後に 2 つの連続したドライブ文字が必要です。（図 10.9 を参照）。これは、ネットワーク共有とは関連していません。ネットワーク共有はユーザープロファイル固有であり、システムハードウェアプロファイル自体ではないため、OS に表示されます。
- この場合、Windows は LP50G2 にネットワーク共有または汎用命名規則（UNC）パスで 사용되는ドライブ文字を割り当てる可能性があり、ドライブ文字の競合が発生します。このような場合は、Windows のディスク管理（管理者権限が必要）でドライブレターの割り当てを変更する方法について、管理者またはヘルプデスク部門にご相談ください。

**図 10.9 – ドライブ文字の例**

この例（図 10.9）では、LP50G2 はドライブ E の後に使用可能な最初のドライブ文字 ドライブ F を使用しています。

（ドライブ文字の空きの前にある最後の物理ディスク）文字 G はネットワーク共有で、ハードウェアプロファイルの一部ではないため、LP50G2 は G を 2 番目のドライブ文字として使用しようとする場合があります、競合が発生します。

システム上でネットワーク共有がなく、LP50G2 が読み込まれない場合、カードリーダー、リムーバブルディスク、または他のインストール済みデバイスがドライブ文字の割り当てを維持していると、競合が発生します。

ドライブ文字管理（DLM）は、Windows 11 で大幅に改善されており、この問題が発生する可能性はありません。ただし、競合を解決できない場合は、Kingston のテクニカルサポートにお問い合わせするか、[Kingston.com/support](https://www.kingston.com/support) からサポートを依頼してください。



IRONKEY™ Locker+ 50 G2
(LP50G2) 安全 USB 3.2 第 1 代
闪存盘

用户指南



目录

简介	3
Locker+ 50 G2 功能	4
关于本手册	4
系统要求	4
建议	5
使用正确的文件系统	5
使用提醒	5
密码设置最佳实践	6
设置设备	7
设备访问 (Windows 环境)	7
设备访问 (macOS 环境)	7
设备初始化 (Windows 和 macOS 环境)	8
密码选择	9
虚拟键盘	11
密码可见性切换	12
管理员密码和用户密码	13
联系信息	15
设备使用 (Windows 和 macOS 环境)	16
管理员和用户登录 (管理员已启用)	16
仅用户模式登录 (管理员未启用)	16
暴力攻击防护	17
访问我的安全文件	17
设备选项	18
LP50G2 设置	20
管理员设置	20
用户设置: 管理员已启用	21
用户设置: 管理员未启用	22
更改和保存 LP50G2 设置	23
管理员功能	24
用户密码重置	24
帮助和故障排除	25
LP50G2 锁定	25
LP50G2 设备重置	27
驱动器盘符冲突: (Windows)	28



图 1： IronKey LP50G2

简介

Kingston IronKey™ Locker+ 50 G2 USB 闪存盘采用经 FIPS 197 认证的 AES 256 位硬件加密技术（XTS 模式），提供企业级安全防护，可防范 BadUSB 攻击及暴力破解密码攻击。LP50G2 还符合 TAA 标准。

LP50G2 现支持多密码（管理员和用户）选项，提供复杂密码模式和密码短语模式两种选择。复杂密码模式允许使用 6 至 16 位密码，密码需包含 4 种字符集中的 3 种。全新密码短语模式支持使用 10 至 64 位数字 PIN 码、句子、单词列表甚至歌词作为密码。管理员可启用或重置用户密码，以恢复数据访问权限。为方便密码输入，可启用“眼睛”图标显示已输入的密码，减少因输入错误导致的登录失败。暴力破解防护功能会在用户连续 10 次输入错误密码后锁定设备，若管理员密码连续 10 次输入错误，则会自动加密擦除闪存盘数据。此外，内置虚拟键盘可防止密码被键盘记录器或屏幕记录器窃取。

Locker+ 50 G2 设计精巧，采用小型金属外壳并配备内置钥匙环，便于随身携带数据。

LP50G2 提供 5 年有限质保，并享受 Kingston 免费技术支持服务。

IronKey Locker+ 50 G2 功能

- FIPS 197 认证
- XTS-AES 硬件加密（加密永远不能关闭）
- 暴力破解和 BadUSB 攻击保护
- 多密码选项
- 复杂密码模式或密码短语模式
- “眼睛”按钮可显示已输入的密码，减少登录失败次数
- 虚拟键盘有助于防范键盘记录器和屏幕记录器的攻击
- 兼容 Windows 或 macOS 系统（详情请查阅产品数据表）

关于本手册 (02122026)

本用户手册涵盖 IronKey Locker+ 50 G2 (LP50G2)。

系统要求

PC 平台 • Intel 和 AMD • 15MB 可用磁盘空间 • 可用的 USB 2.0 - 3.2 端口 • 在最后一个物理驱动器之后连续分配的两个驱动器盘符* *注意：请参阅第 28 页的“驱动器盘符冲突”。	PC 操作系统支持 • Windows 11
Mac 平台 • Intel 和 Apple SOC • 15MB 可用磁盘空间 • USB 2.0 - 3.2 端口	Mac 操作系统支持 • macOS 13.x – 26.x

建议

为确保为 LP50G2 设备提供充足电力，请按照图 1.1 所示，直接将其插入笔记本电脑或台式机的 USB 端口。请避免将 LP50G2 连接到任何可能带有 USB 端口的外设（如键盘或 USB 供电集线器），如图 1.2 所示。



图 1.1——推荐用法



图 1.2——不推荐用法

使用正确的文件系统

IronKey LP50G2 预格式化为 FAT32 文件系统。这种格式支持 Windows 和 macOS 两种系统。不过，可以使用其他选项手动格式化闪存盘，例如适合 Windows 的 NTFS 和 exFAT。如有需要，您可以重新格式化数据分区，但重新格式化会导致数据丢失。

使用提醒

为确保数据安全，Kingston 建议您：

- 在目标系统上设置并使用 LP50G2 之前，先对计算机进行病毒扫描
- 在公共系统或不熟悉的系统上使用闪存盘时，您可能会希望将设备设为只读模式，帮助闪存盘防范恶意软件
- 不使用时锁定设备
- 拔出闪存盘前先将其弹出
- 从不在 LED 亮着时拔出设备。这可能会损坏闪存盘并需要重新格式化，而这会擦除您的数据
- 切勿与任何人共享您的设备密码

获取最新更新与信息

请访问 kingston.com/support，获取闪存盘的最新更新、常见问题解答、文档及其他相关信息。

注意：仅当有最新更新时，才应将其应用于闪存盘。不支持将闪存盘降级至旧版软件，此操作可能导致存储数据丢失或损害闪存盘的其他功能。如有疑问或遇到问题，请联系 Kingston 技术支持。

密码设置最佳实践

您的 LP50G2 配备了强大的安全防护措施。其中包括防暴力破解攻击功能，该功能通过限制每次密码尝试次数为 10 次，阻止攻击者猜测密码。当达到尝试次数上限时，LP50G2 将自动擦除加密数据，并将闪存盘恢复至出厂状态。

多密码功能

LP50G2 支持多密码功能，这是其一项重要特性，可防止因遗忘一个或多个密码而导致数据丢失。当启用所有密码选项时，LP50G2 支持两种不同的密码，您可使用这两种密码恢复数据——管理员密码和用户密码。

LP50G2 允许您设置两个主要密码——管理员密码（简称 Admin 密码）和用户密码。管理员可随时访问闪存盘，并为用户设置选项——管理员相当于超级用户。

用户也可访问闪存盘，但与管理员相比，权限有限。如果遗忘了两个密码中的一个，可使用另一个密码访问并检索数据。之后，可重新设置闪存盘，使其拥有两个密码。在使用用户密码时，务必设置两个密码，并将管理员密码保存在安全位置。

如果所有密码均被遗忘或丢失，则无法访问数据。Kingston 无法恢复数据，因为该安全机制没有后门。Kingston 建议您将数据也保存在其他存储介质上。LP50G2 可重置并重复使用，但之前的数据将被永久擦除。

密码模式

LP50G2 还支持两种不同的密码模式：

复杂

复杂密码要求长度至少为 6 至 16 个字符，且必须包含以下 4 类字符中的至少 3 类：

- 大写字母字符
- 小写字母字符
- 数字
- 特殊字符

密码短语

LP50G2 支持 10 至 64 个字符的密码短语。密码短语无需遵循额外规则，但若使用得当，可提供极高的密码保护级别。

密码短语基本上可以是任意字符组合，包括其他语言的字符。与 LP50G2 闪存盘的语言设置一样，密码短语的语言也可与闪存盘所选语言保持一致。这样，您就可以选择多个单词、一个短语、一首歌的歌词、一句诗等作为密码短语。对于攻击者而言，好的密码短语是最难猜测的密码类型之一，但用户可能更容易记住。

设置设备

为确保 IronKey 加密 USB 闪存盘获得充足供电，应将其直接插入笔记本电脑或台式机的 USB 2.0/3.0 接口。请避免将其连接到任何可能带有USB端口的外设，如键盘或 USB 供电集线器。设备初始设置必须在受支持的 Windows 或 macOS 操作系统上进行。

设备访问 (Windows 环境)

将 IronKey 加密 USB 闪存盘插入笔记本电脑或台式机的可用 USB 端口，并等待 Windows 检测到它。

- Windows 用户将收到设备驱动程序通知。(图 3.1)



图 3.1 – 设备驱动程序通知

- 新硬件检测完成后，在文件资源管理器中找到解锁分区，然后选择其中的 **IronKey.exe** 选项。(图 3.2)
- 请注意，分区盘符会根据下一个可用的驱动器盘符而有所不同。驱动器盘符可能会因所连接设备的情况而发生变化。在右侧图中，驱动器盘符是 (E:)。



图 3.2 – 文件资源管理器窗口/IronKey.exe

设备访问 (macOS 环境)

将 LP50G2 插入笔记本电脑或台式机上的可用 USB 接口，并等待 Mac 操作系统检测到它。检测到后，您会在桌面上看到“IRONKEY”卷盘图标出现。(图 3.3)

- 双击 IronKey CD-ROM 图标。
- 然后，双击图 3.3 显示的窗口中的 IronKey.app 应用图标。这会开始初始化过程。

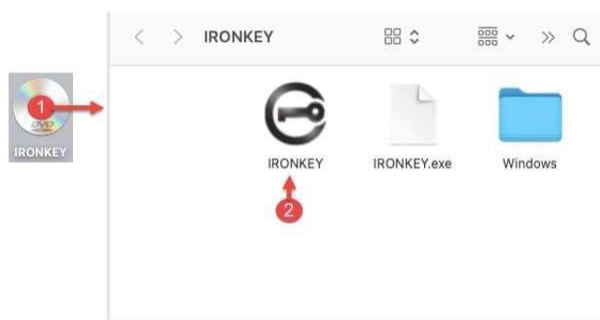


图 3.3 – IRONKEY 卷

设备初始化 (Windows 和 macOS 环境)

语言和最终用户许可协议 (EULA)

从下拉菜单中选择您的语言首选项，然后单击 **Next (下一步)**。（参见图 4.1）

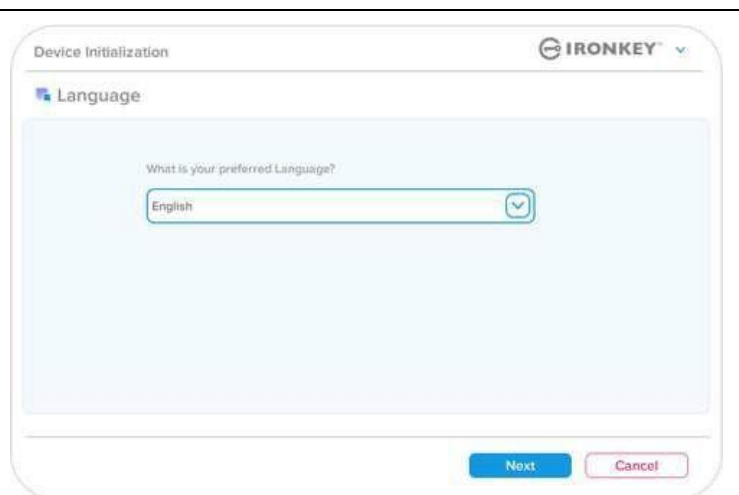


图 4.1 - 语言选择

查阅许可协议，然后单击 **Next (下一步)**。

注意：您必须先接受许可协议才能继续操作；否则，**Next (下一步)** 按钮将保持禁用状态。（图 4.2）

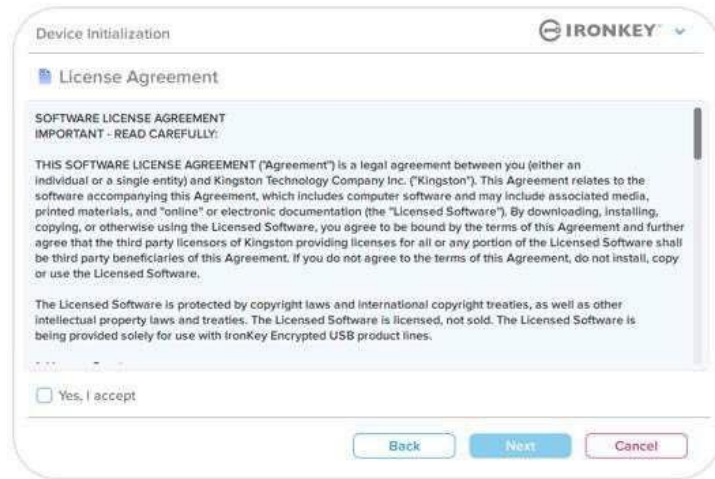


图 4.2 – 许可协议

设备初始化

密码选择

在密码提示界面，您可以使用“复杂密码”或“密码短语”模式（图 4.3-4.4）为 LP50G2 上的数据创建密码进行保护。此外，您还可以在此界面启用“多密码管理员/用户”选项。在继续选择密码前，请先阅读下方关于“启用管理员/用户密码”的说明，以便更好地了解这些功能。

注意：一旦选择复杂密码或密码短语模式，除非重置设备，否则无法更改模式。开始选择密码时，请在“密码”字段中创建您的密码，然后在“确认密码”字段中重新输入该密码。在初始化流程允许您继续操作之前，您创建的密码必须满足以下条件：

复杂密码

- 必须至少包含 6 个字符
(最多 16 个字符)。
- 必须满足以下三 (3) 项条件：
 - 大写
 - 小写
 - 数字
 - 特殊字符 (!、\$、& 等)

图 4.3 - 复杂密码

密码短语密码

- 必须包含：
 - 最少 10 个字符
 - 最多 64 个字符

图 4.4 - 密码短语

密码提示 (可选)

密码提示在忘记密码时有用，可以提供有关密码是什么的线索。

注意：提示不能与密码完全一致。

图 4.5 - 密码提示字段

设备初始化

有效密码和无效密码

对于 **有效** 密码，密码条件框会在条件满足时以 **绿色** 高亮显示。（参见图 4.6a-b）注意：一旦满足至少三项密码条件，第四项条件框将变为灰色，表示此条件为可选（图 4.6b）。



图 4.6a - 已满足复杂密码条件

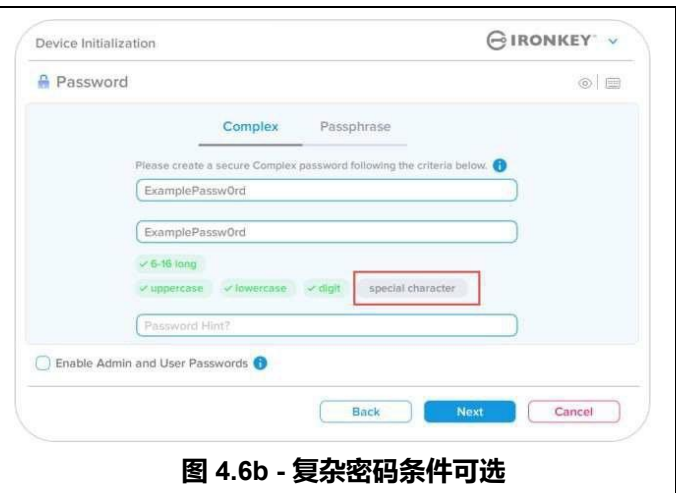


图 4.6b - 复杂密码条件可选

若输入的密码 **无效**，密码条件框会以 **红色** 高亮显示，且在满足最低要求之前，**Next（下一步）** 按钮将保持禁用状态。

此规则同时适用于复杂密码和密码短语。

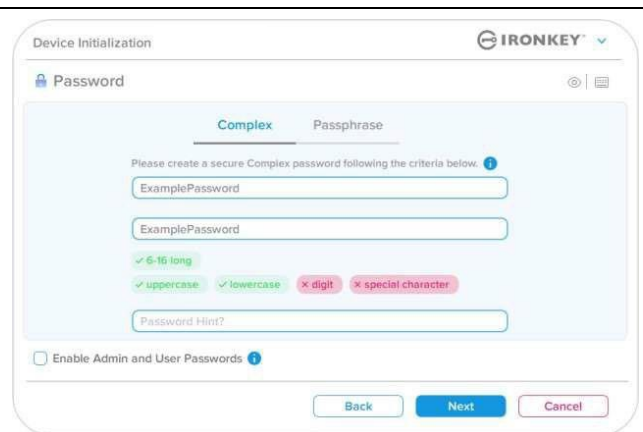


图 4.7 - 未满足密码条件

设备初始化

虚拟键盘

LP50G2 配备有虚拟键盘，可用于防范键盘记录器。

- 要使用 **虚拟键盘**，请在 **Device Initialization (设备初始化)** 界面的右上角找到键盘按钮并单击它。

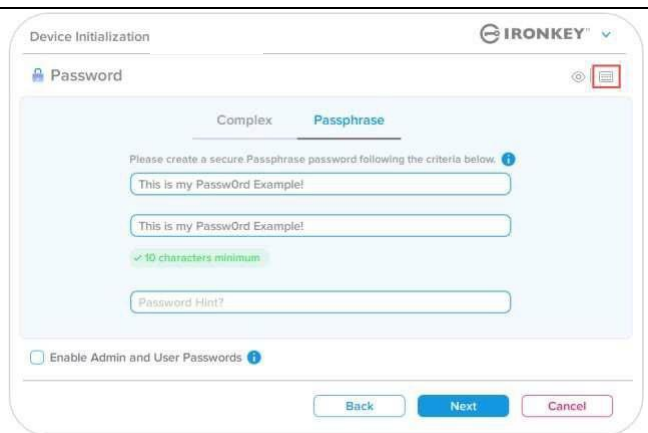


图 4.8 – 激活虚拟键盘

- 虚拟键盘出现后，您还可以启用**屏幕记录防护功能**。使用此功能时，所有按键会短暂显示为空白。这是正常现象，因为这样可以防止屏幕记录器捕获您的单击操作。
- 为使此功能更加强大，您还可以选择随机化虚拟键盘布局，只需单击键盘右下角的 **randomize (随机化)** 按钮即可。随机排列会以随机方式排列键盘布局。



图 4.9 – 屏幕记录防护/随机化

设备初始化

密码可见性切换

默认情况下，当您创建密码时，输入的密码字符会实时显示在输入框中。如果您希望在输入时“隐藏”密码字符，可以通过切换设备初始化窗口右上角的密码“显示/隐藏”图标（通常形似眼睛）来实现。

注意：设备初始化完成后，密码字段将默认处于“隐藏”状态。

要 **隐藏** 密码字符，请单击灰色图标。

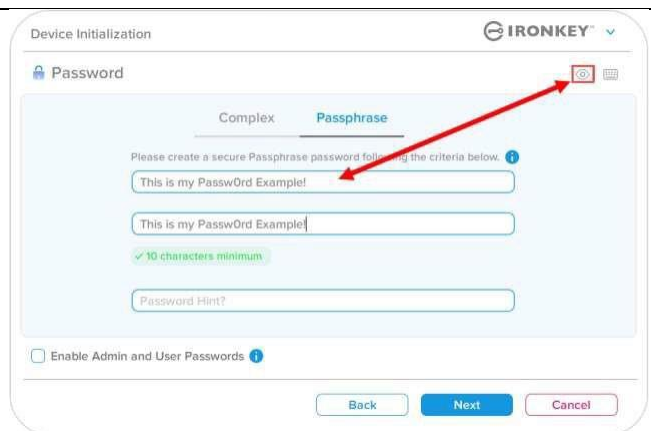


图 4.10 - 切换“隐藏”密码

要 **显示** 已隐藏的密码，请单击蓝色图标。

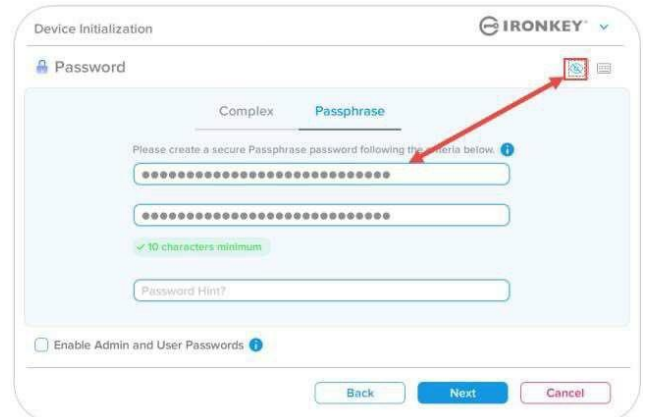


图 4.11 - 切换“显示”密码

设备初始化

管理员密码和用户密码

启用管理员密码和用户密码后，您可利用多密码功能，其中管理员角色可同时管理这两个账户。选择“**Enable Admin and User Passwords（启用管理员和用户密码）**”后，若遗忘其中一个密码，仍可通过另一种方式访问驱动器。

启用**管理员和用户密码**后，您还可以访问以下内容：

- 用户密码重置

如需了解有关用户密码重置功能的更多信息，请参阅本用户指南第 24 页。

- 要启用**管理员和用户密码**，请勾选 **Enable Admin and User Passwords（启用管理员和用户密码）** 旁边的方框，并在选择有效密码后单击 **Next（下一步）**。（图 4.12）
- 如果此功能 **已启用**，则在此界面选择的密码将成为 **管理员密码**。单击 **Next（下一步）** 进入 **User Password（用户密码）** 界面，为普通用户选择密码。

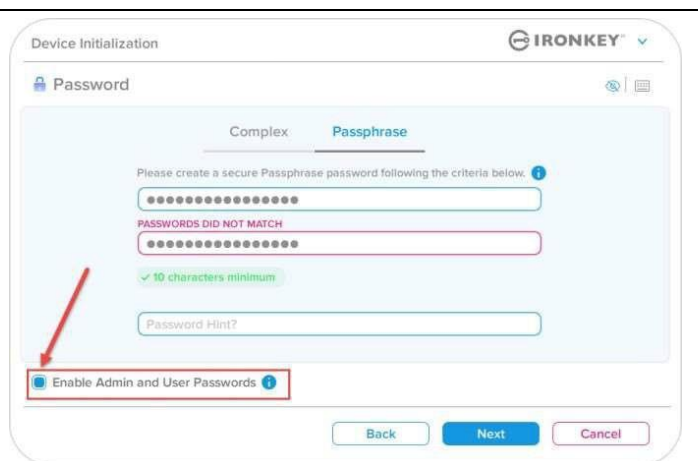


图 4.12 – 启用管理员密码和用户密码

注意：启用管理员和用户密码为可选操作。

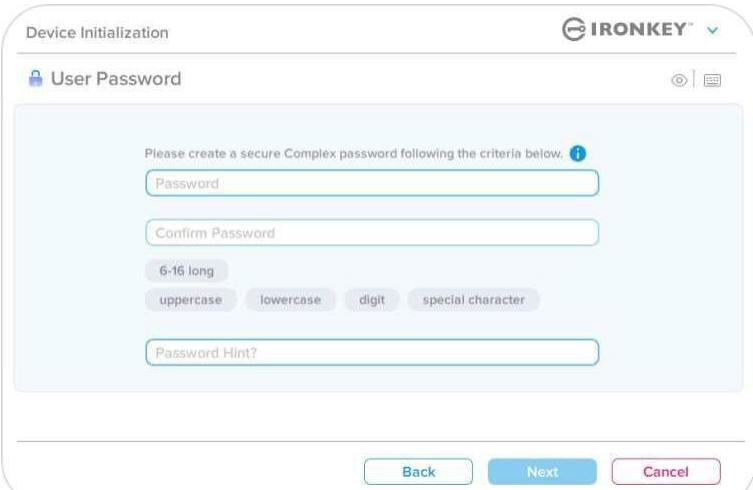
如果未启用此功能（未勾选方框）来设置驱动器，则驱动器将被配置为 **单用户、单密码** 驱动器，且**不包含任何管理员功能**。本手册将此配置称为 **仅用户模式**。

如需进行单用户、单密码设置，请保持 **Enable Admin and User Passwords（启用管理员和用户密码）** 未勾选状态，并在创建有效密码后单击 **Next（下一步）**。

设备初始化

管理员密码和用户密码

如果上一界面 **启用** 了管理员角色，则下一界面将提示设置 **用户密码**（图 4.13）。与管理员密码相比，用户密码的功能将受到限制，下文将对此进行详细说明。**注意：**“管理员密码和用户密码”在本手册下文中称作“管理员角色”。



The screenshot shows the 'Device Initialization' window with the 'User Password' section active. It prompts the user to create a secure complex password. The interface includes input fields for 'Password', 'Confirm Password', and 'Password Hint?'. Below these fields, there are five criteria buttons: '6-16 long', 'uppercase', 'lowercase', 'digit', and 'special character'. At the bottom of the window are three buttons: 'Back', 'Next', and 'Cancel'.

图 4.13 – 用户密码（管理员和用户已启用）

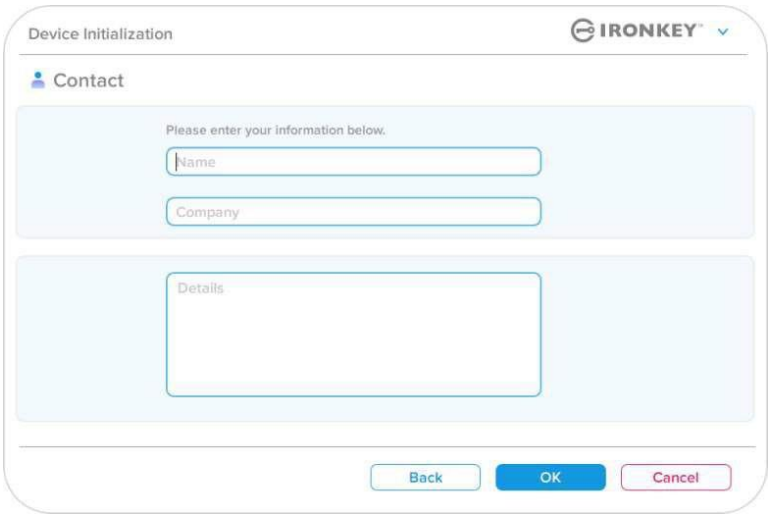
注意：所选的密码选项（复杂密码或密码短语）所设定的条件将同样适用于用户密码，并且在驱动器设置完成后，任何所需的密码重置操作也需遵循这些条件。所选密码选项只能在完整设备重置后进行更改。

设备初始化

联系信息

在下面提供的文本框中输入您的联系信息。（参见图 4.14）

注意：您在这些字段中输入的信息不得包含您在第 3 步中创建的密码字符串。不过，这些字段为可选填写项，如需留空也可。

“Name（姓名）”字段最多可包含 32 个字符，但不得与密码 完全一致。 “Company（公司）”字段最多可包含 32 个字符，但不得与密码 完全一致。 “Details（详细信息）”字段最多可包含 156 个字符，但不得与密码 完全一致。	 图 4.14——联系信息
--	---

注意：单击“OK（确定）”将完成初始化流程，并解锁安全分区，随后挂载该分区，以便您安全存储数据。请先拔出闪存盘，再重新插入系统，以查看更改后的效果。

设备使用 (Windows 和 macOS 环境)

管理员与用户登录 (管理员功能已启用)

若设备初始化时启用了管理员密码和用户密码 (管理员角色)，IronKey LP50G2 应用程序将启动，并首先显示用户密码登录界面。在此，您可使用用户密码登录，查看已输入的联系信息，或以管理员身份登录 (图 6.1)。单击下方的“以管理员身份登录”按钮，应用程序将进入管理员登录菜单，您可在此以管理员身份登录，访问管理员设置和功能 (图 6.2)。

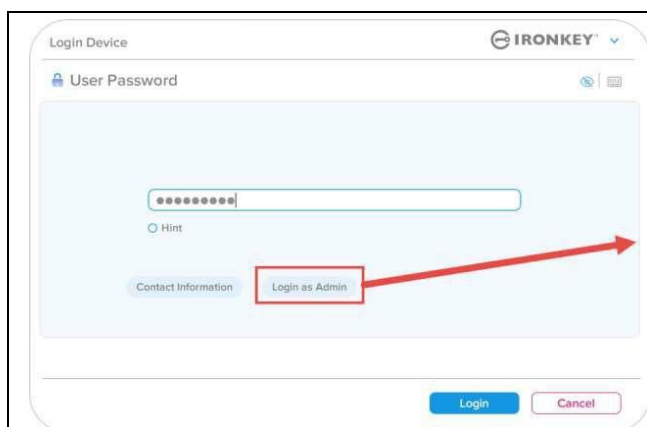


图 6.1 – 用户密码登录 (管理员已启用)

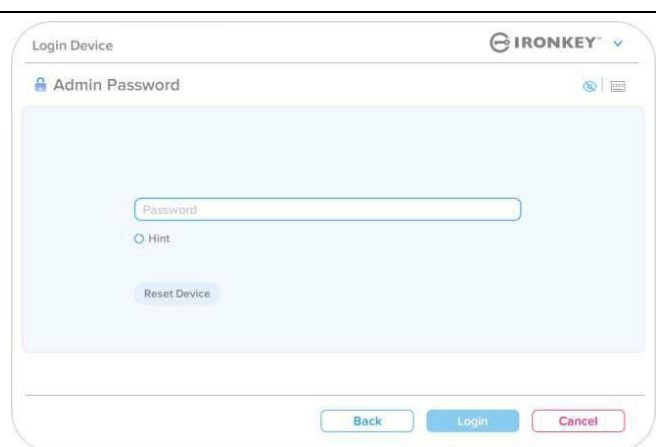


图 6.2 - 管理员密码登录

仅用户模式登录 (管理员未启用)

如前文第 13 页所述，尽管建议使用管理员角色功能以充分发挥设备的全部优势，但 IronKey 闪存盘也可初始化为仅用户模式 (单一密码、单一用户) 配置。这一选项适用于希望采用简单的单一密码方式来保护闪存盘上数据安全的用户。(图 6.3)

注意：要启用管理员密码和用户密码，请使用**重置设备**按钮将闪存盘恢复至初始化状态，此时您可启用管理员密码和用户密码。**执行“Reset Device (重置设备)”操作时，闪存盘上的所有数据将被格式化并永久丢失。**

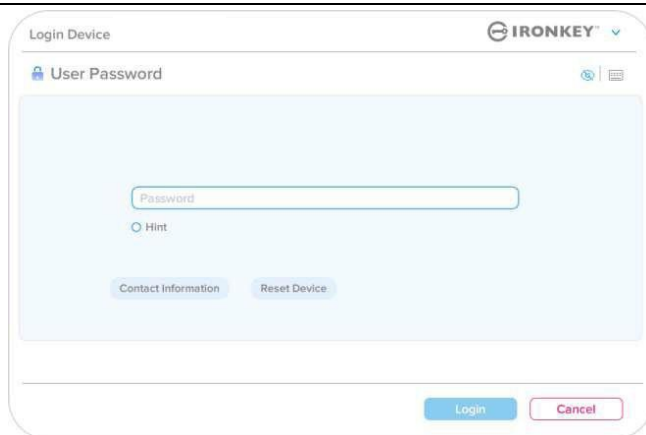


图 6.3 – 用户密码登录 (管理员未启用)

设备使用

暴力攻击防护

重要提示：在登录过程中，如果输入了错误的密码，您还有机会输入正确的密码；但是，内置安全功能（也称暴力攻击防护）会记录失败登录尝试的次数。*

如果错误密码尝试次数达到预设的 10 次上限，系统将采取以下措施：

管理员/用户已启用	暴力破解防护机制下设备行为表现 (10 次错误密码尝试后)	数据擦除及 设备重置?
用户密码:	密码锁定。 登录为管理员以重置用户密码	否
管理员密码	加密擦除闪存盘、密码、设置和数据	是
仅用户 单用户、单密码 (管理员/用户未启用)	暴力破解防护机制下设备行为表现 (10 次错误密码尝试后)	数据擦除及 设备重置?
用户密码	加密擦除驱动器，密码、设置及数据将 被永久删除	是

* 成功通过设备身份验证后，失败登录计数器将根据所使用的登录方式重置。加密擦除操作将删除所有密码、加密密钥及数据 – **您的数据将永久丢失。**

访问我的安全文件

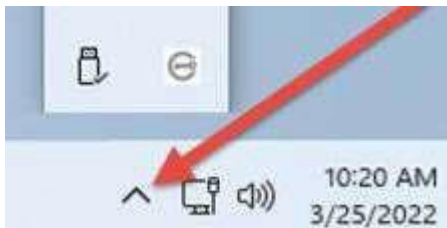
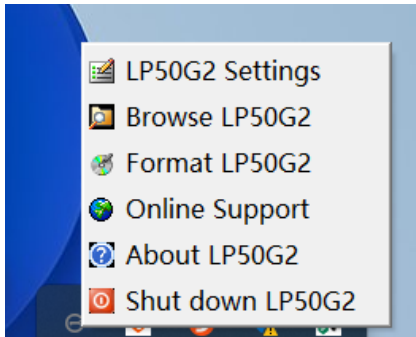
解锁闪存盘后，您可以访问自己的安全文件。在驱动器上保存或打开文件时，文件会自动进行加密和解密操作。这项技术不仅让您可以像通常操作普通闪存盘一样方便，还提供了“始终在线”的强大安全性。

提示：您还可以通过右键单击 Windows 任务栏中的 **IronKey 图标**，然后单击 **浏览 LP50G2** 来访问您的文件（图 7.2）

设备选项 - (Windows 环境)

当您登录该设备时，窗口的右上角会显示一个 IronKey 图标。右击 IronKey 图标，会打开可用闪存盘选项的选择菜单（图 6.2）。

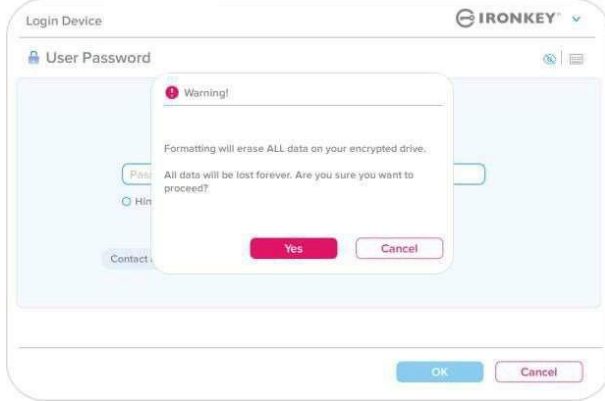
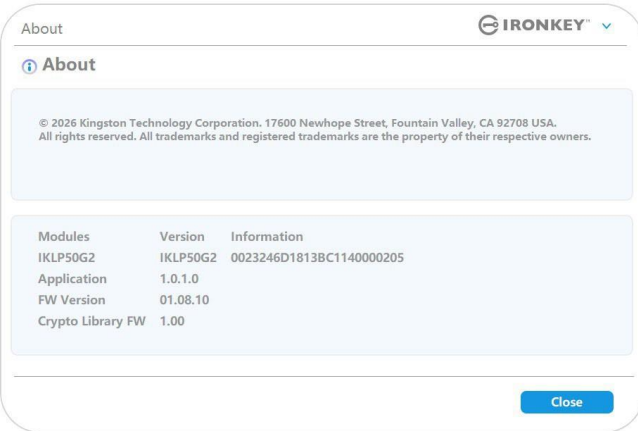
关于这些设备选项的详情，可在本手册第 19-23 页找到

当您登录该设备时，窗口的右上角会显示一个 IronKey 图标。（图 7.1）	 图 7.1 – 任务栏中的 IronKey 图标
右击 IronKey 图标，会打开可用闪存盘选项的选择菜单。（图 7.2） 关于这些设备选项的详情，可在本手册第 19-23 页找到。	 图 7.2 – 右击 IronKey 图标以打开设备选项

设备选项 - (macOS 环境)

当您登录该设备时，在如 图 7.3 所示的 macOS 菜单栏中会出现一个“IronKey LP50G2”图标，单击该图标可打开可用的设备选项。 关于这些设备选项的详情，可在本手册第 19-23 页找到。	 图 7.3 – macOS 菜单栏图标/设备选项菜单
---	--

设备选项

LP50G2 设置:	修改登录密码、联系方式及其他设置。（有关设备设置的更多详情，请参阅本手册中“LP50G2 设置”部分）。
浏览 LP50G2:	可让您查看您的安全文件。
格式化 LP50G2: 允许您格式化安全数据分区。 （警告：所有数据都将擦除。） (图 6.1) 注意： 格式化需要密码身份认证。	 图 7.4 - 格式化 LP50G2
在线支持:	打开互联网浏览器并导航至 http://www.kingston.com/support，您可以在这里获取更多的支持信息。
关于 LP50G2: 提供有关 LP50G2 的具体详情，包括应用信息、固件信息以及序列号信息 (图 6.2) 注意： 该驱动器的唯一序列号可在“信息栏”下查看。	 图 7.5 - 关于 LP50G2
关闭 LP50G2:	正确关闭 LP50G2，以便您能安全地从系统中移除该设备。

LP50G2 设置

管理员设置

管理员登录将限制访问以下设备设置：

- **Password (密码)**：允许您更改您自己的管理员密码和/或提示 (图 8.1)
- **Contact Info (联系信息)**：允许您添加/查看/更改联系信息 (图 8.2)
- **Language (语言)**：可让您更改当前语言选择(图 8.3)
- **Admin Settings (管理员选项)**：可让您访问如下其他功能：
 - 更改用户密码 (图 8.4)

注意：管理员选项的更多详细信息可查阅第 25 页

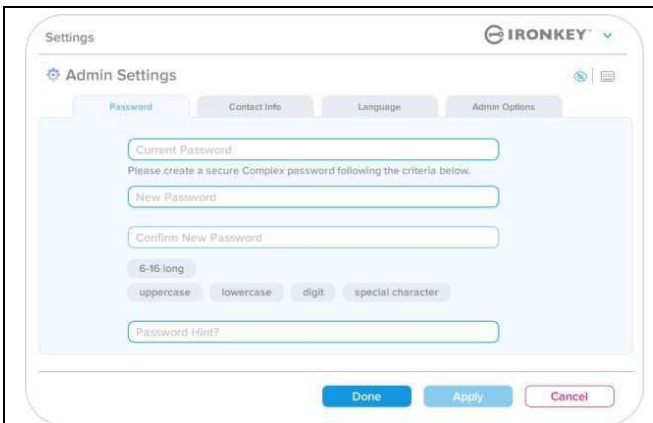


图 8.1 - 管理员密码选项

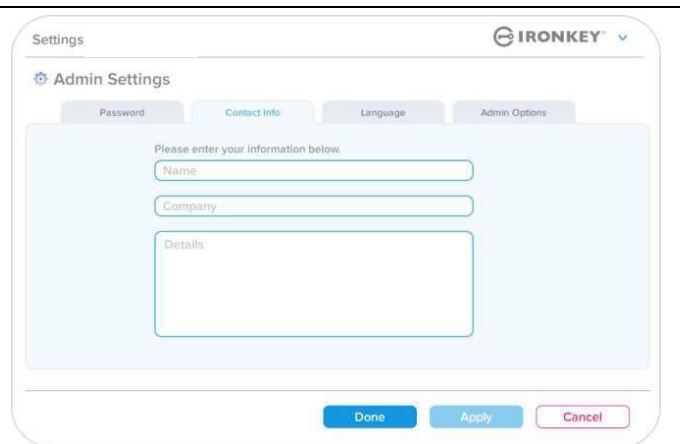


图 8.2 - 联系信息

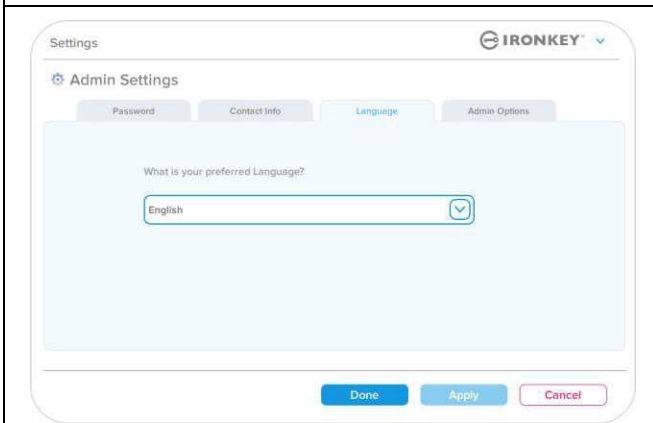


图 8.3 - 语言选项

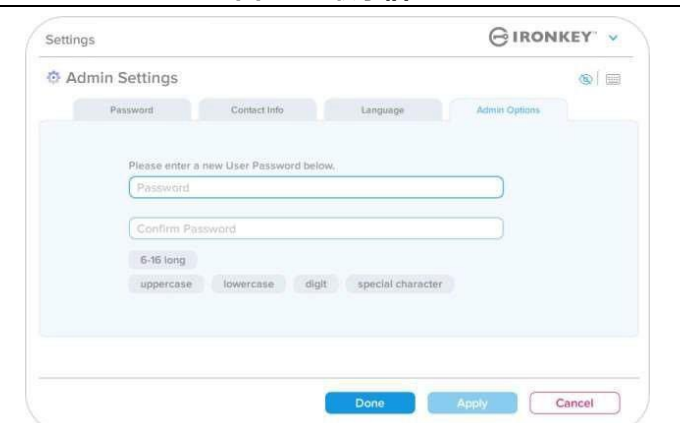


图 8.4 - 管理员选项

LP50G2 设置

用户设置：管理员已启用

用户登录将限制访问以下设置：

密码：

允许您更改您自己的用户密码和/或提示。
(图 8.5)

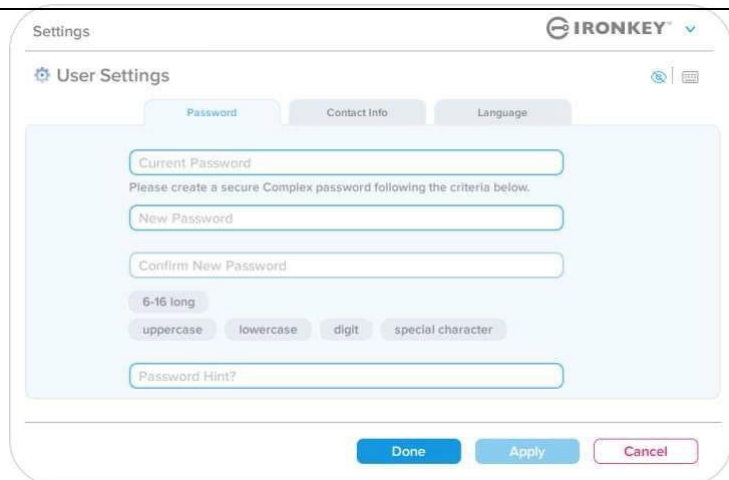


图 8.5 – 密码选项 (管理员已启用：用户登录)

联系信息：

允许您添加/查看/更改联系信息。
(图 8.6)

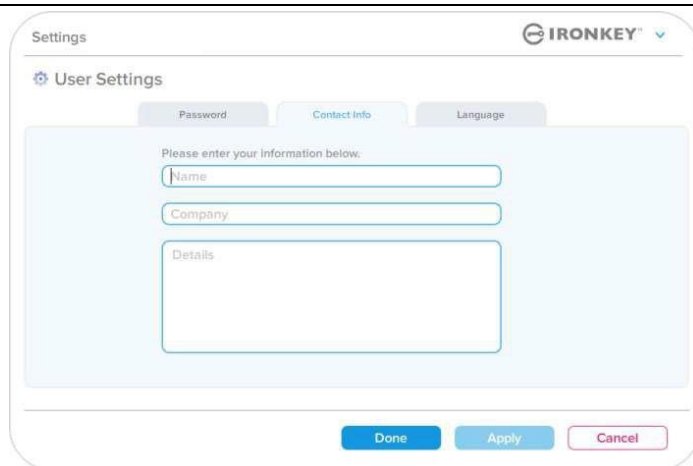


图 8.6 – 联系信息 (管理员已启用：用户登录)

语言：

让您可以更改当前语言选择。
(图 8.7)

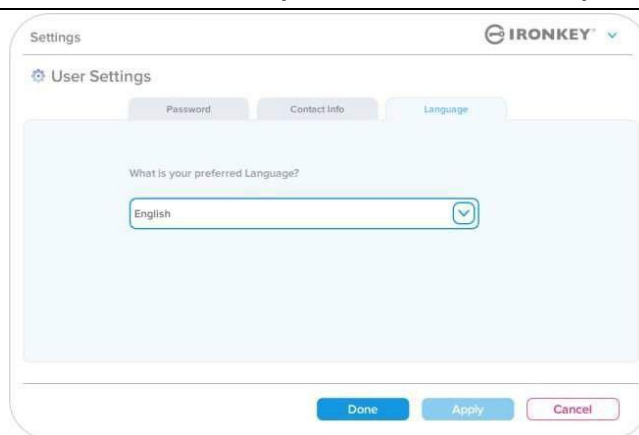


图 8.7 – 语言设置 (管理员已启用：用户登录)

注意： 使用用户密码登录时，无法访问管理员选项。

LP50G2 设置

用户设置：管理员未启用

如第12页所述，若在初始化 LP50G2 时未启用“管理员和用户”密码，则设备将配置为**单密码**、**单用户模式**。此配置下无法访问任何管理员选项或功能。此配置可访问以下 LP50G2 设置：

密码：

允许您更改您自己的用户密码和/或提示。(图 8.8)

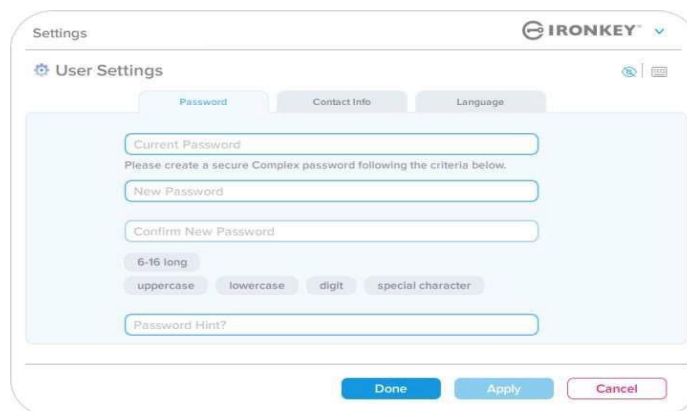


图 8.8– 密码选项（仅用户模式）

联系信息：

允许您添加/查看/更改联系信息。(图 8.9)

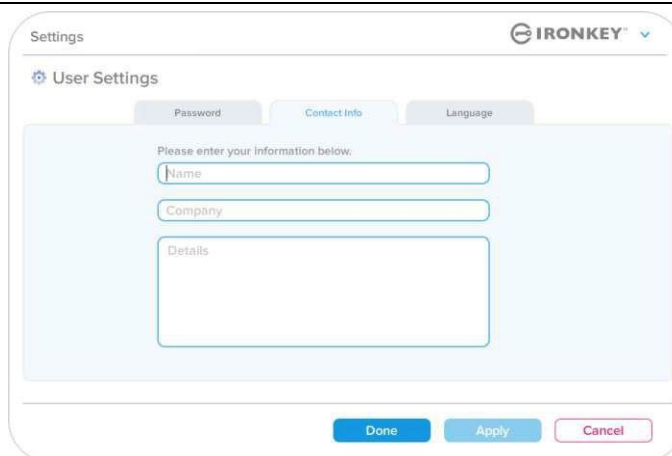


图 8.9– 联系信息（仅用户模式）

语言：

让您可以更改当前语言选择。(图 8.10)

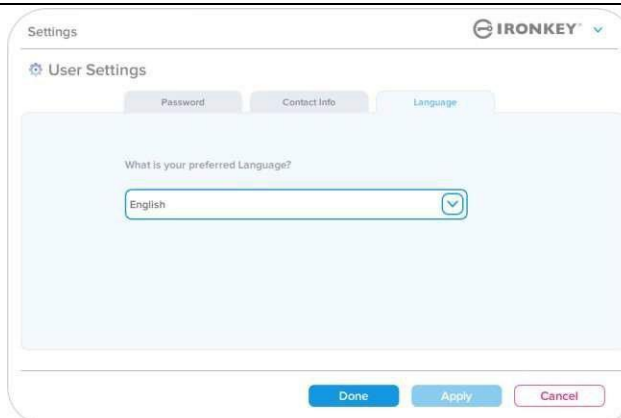


图 8.10– 语言设置（仅用户模式）

LP50G2 设置

更改和保存设置

- 每当在 LP50G2 设置中修改配置（例如联系方式、语言、密码更改、管理员选项等）时，设备将提示您输入密码，以确认并应用这些更改。（参见图 8.11）

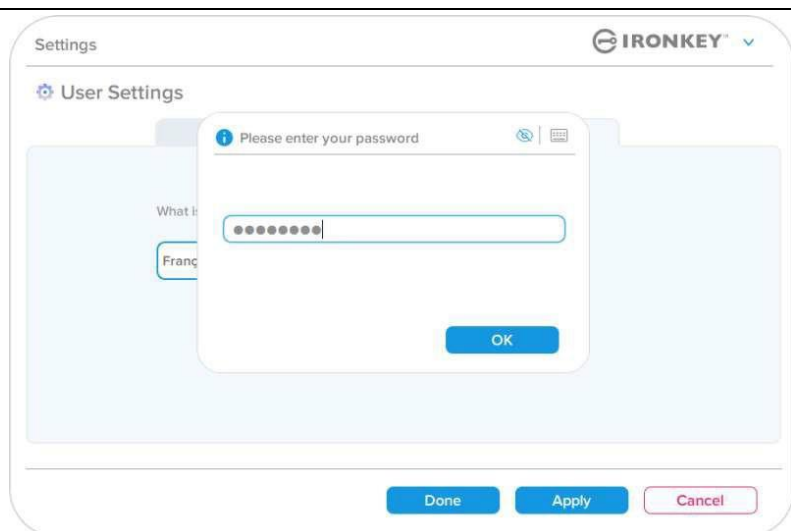


图 8.11 - 保存 LP50G2 设置更改时的密码提示界面

注意：若您处于上述密码输入提示界面，且希望取消或修改所做的更改，只需确保密码输入框为空，然后单击“OK（确定）”即可。此操作将关闭“Please enter your password（请输入您的密码）”对话框，并返回至 LP50G2 设置菜单。

管理员功能

重置用户密码的选项

管理员配置的一项实用功能是：若用户忘记密码，可安全重置用户密码。以下是可帮助您重置用户密码的用户密码重置功能说明：

用户密码重置：

在“Admin Options（管理员选项）”菜单中手动更改用户密码，这可以立即实现更改并在下次用户登录时生效。(图 9.1)

注意：密码要求标准将默认采用初始化过程中设定的原始标准（复杂密码或密码短语选项）。

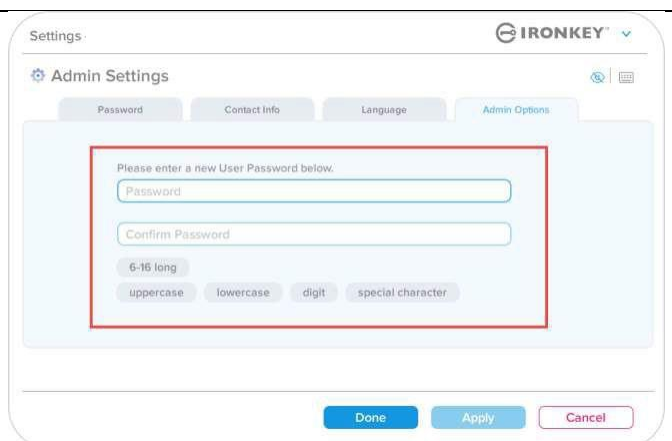


图 9.1 – 管理员选项/用户密码重置

帮助和故障排除

设备锁定

LP50G2 配备了一项安全功能：当**连续**登录失败次数达到预设的最大值（简称 *MaxNoA*）时，将阻止对数据分区的未授权访问。该设备“开箱即用”的默认配置中，每种登录方式（管理员/用户）的 *MaxNoA* 预设值均为 10 次（尝试次数）。

“锁定”计数器会记录每次登录失败情况，并通过以下**两种方式之一**重置：

1. 在达到 *MaxNoA* 前成功登录；
2. 达到 *MaxNoA* 后，根据驱动器配置执行设备锁定或设备格式化操作。

- 若输入错误密码，密码输入框上方将显示红色错误提示信息，表明登录失败。
(图 10.1)

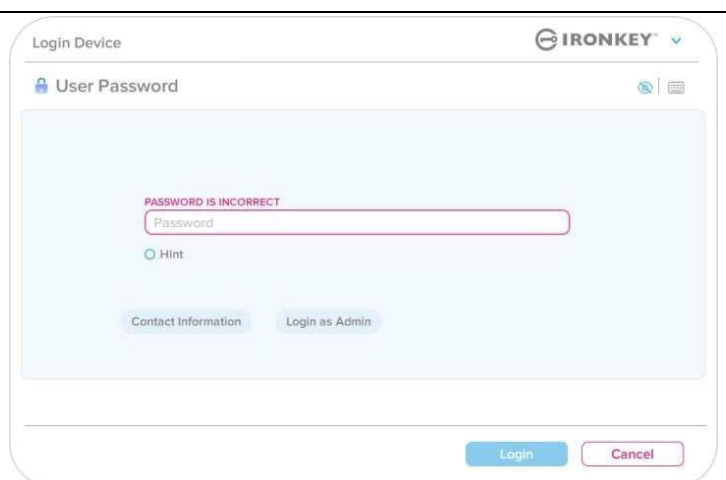


图 10.1 – 密码错误消息

- 当第 7 次登录尝试失败时，您将看到一条额外的错误提示信息，告知您在达到最大尝试次数（*MaxNoA*，默认设置为 10 次）之前，还剩余 3 次尝试机会。
(图 10.2)

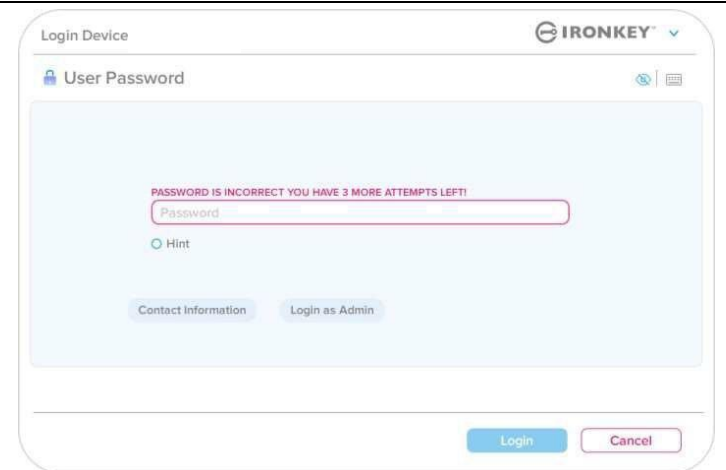


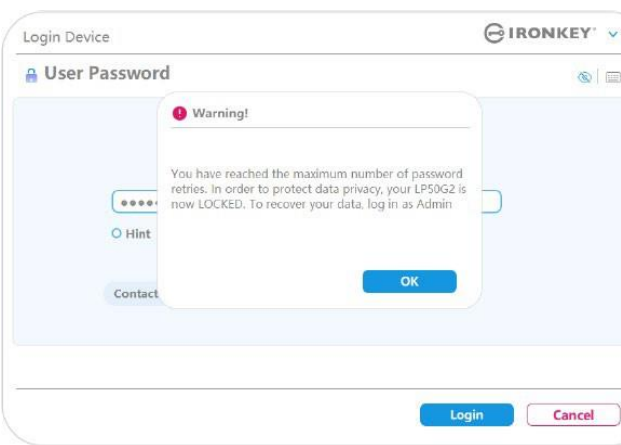
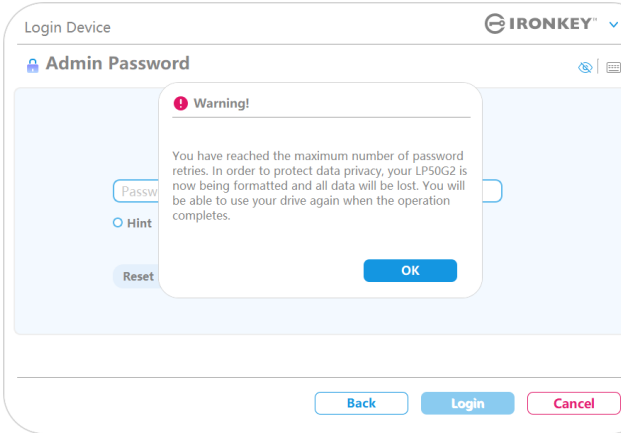
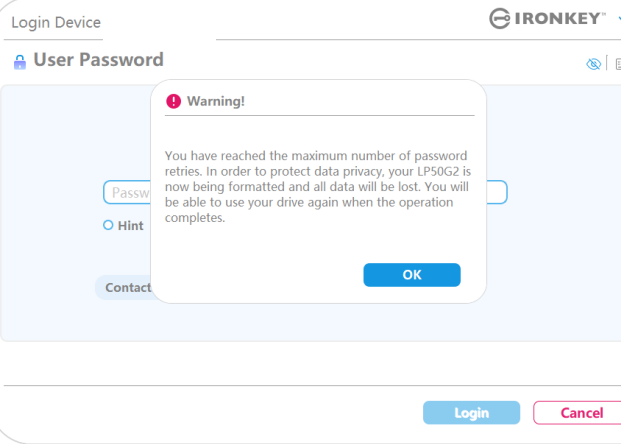
图 10.2 – 第 7 次密码输入错误

帮助和故障排除

设备锁定

重要提示：在第 10 次且为最后一次登录尝试失败后，根据设备的设置方式及所使用的登录方法（管理员/用户模式），设备将采取以下两种措施之一：要么锁定设备，要求您使用备用方法登录（若适用）；要么执行设备重置操作，此操作将格式化设备，导致驱动器上的所有数据永久丢失。相关行为说明也见本用户指南第 17 页。

以下图 10.3 至图 10.6 展示了每种登录密码方法在第十次且为最后一次登录失败时的界面表现：

用户密码（管理员/用户已启用）  设备锁定 图 10.3	管理员密码（管理员/用户已启用）  设备格式化* 图 10.4
这些安全措施可防止未掌握您密码的人员通过无限次尝试登录来窃取您的敏感数据（即防止暴力破解攻击）。若您是 LP50G2 设备的所有者且忘记了密码，系统仍会执行相同的安全措施，包括强制格式化设备。* 有关该功能的更多信息，请参见第 27 页的“重置设备”。	用户密码（管理员未启用）  设备格式化* 图 10.5

***注意：**对设备进行格式化将清除 LP50G2 安全数据分区上存储的所有信息。

帮助和故障排除

重置设备

如果您忘记了密码或需要重置设备，可在运行 LP50G2 启动器时，根据设备设置方式的不同，单击以下两个位置之一出现的“Reset Device (重置设备)”按钮：若已启用管理员/用户模式，则该按钮位于管理员登录密码菜单中；若未启用管理员/用户模式，则该按钮位于“User Password (用户密码)”登录菜单中。

(参见图 10.7 和 10.8)

- 该选项允许您创建新密码，但为保护您的数据隐私，LP50G2 将被格式化。这意味着您的所有数据将在操作过程中被彻底删除。*

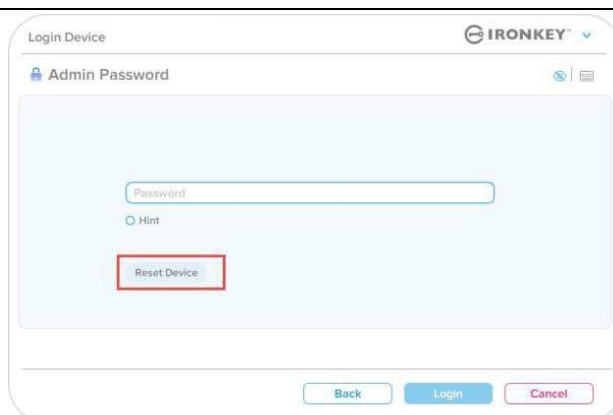


图 10.6 - 管理员密码：“重置设备”按钮

- 注意：**单击“Reset Device (重置设备)”后，会出现一个消息框，询问您是否要在执行格式化之前输入新密码。* 此时，您可以 1) 单击“OK (确定)”以确认，或 2) 单击“Cancel (取消)”返回登录窗口。(参见图 10.8)

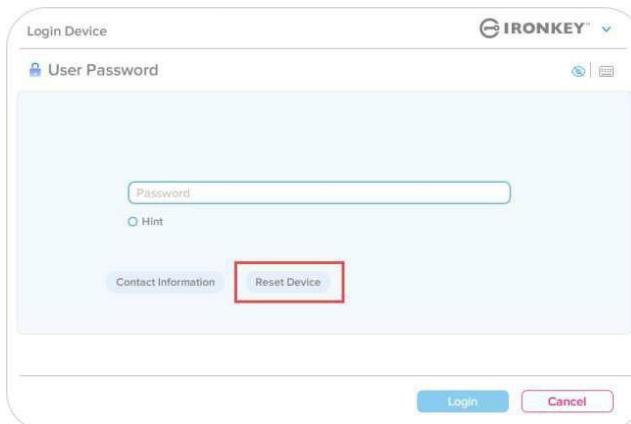


图 10.7 – 用户密码 (管理员/用户未启用) 重置设备

- 如果选择继续，会弹出“Initialization” (初始化) 屏幕，您在此可以启用“管理员和用户模式”，并根据所选密码选项 (复杂密码或密码短语) 输入新密码。提示不是必填字段，但是该字段在忘记密码时有用，可以提供有关密码是什么的线索。

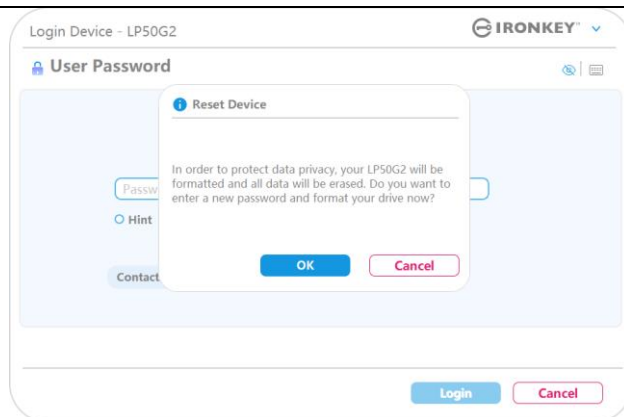
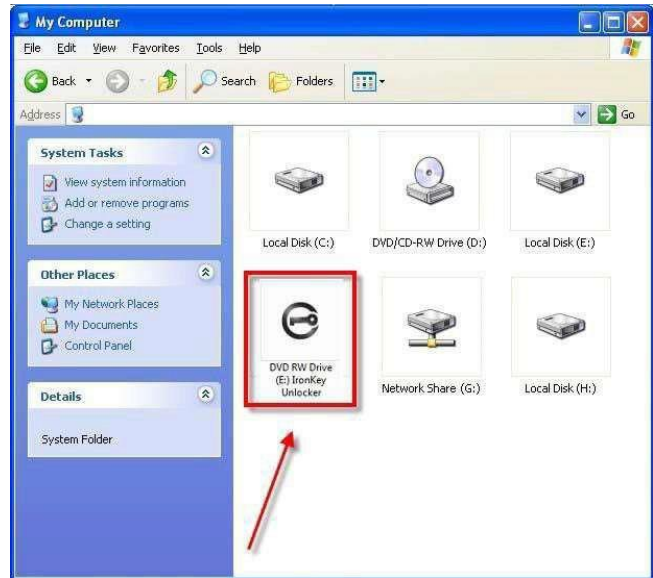


图 10.8 – 重置设备确认

驱动器盘符冲突：Windows 操作系统

- 如本手册“系统要求”部分（第 4 页）所述，LP50G2 需要在驱动器盘符分配出现“间隔”前最后一个物理磁盘之后的两个连续驱动器盘符（见图 10.9）。此要求不适用于网络共享，因为网络共享与用户配置文件相关，而非系统硬件配置文件本身，因此操作系统会将其识别为可用资源。
- 这意味着，Windows 可能会将 LP50G2 分配到一个已被网络共享或通用命名约定（UNC）路径占用的驱动器盘符，从而导致驱动器盘符冲突。如果发生这种情况，请联系您的管理员或帮助台部门，以便在 Windows 磁盘管理中更改驱动器盘符分配（需要管理员权限）。

**图 10.9——驱动器盘符示例**

在图 10.9 的示例中，LP50G2 使用驱动器 F:，这是驱动器 E:（驱动器盘符间隔前的最后一个物理磁盘）之后的第一个可用驱动器盘符。由于驱动器 G: 是网络共享，不属于硬件配置文件的一部分，因此 LP50G2 可能会尝试将其作为第二个驱动器盘符使用，从而导致冲突。

如果系统中没有网络共享，但 LP50G2 仍无法加载，则可能是读卡器、可移动磁盘或其他先前安装的设备占用了驱动器盘符分配，仍导致冲突。

请注意，Windows 11 的驱动器盘符管理（DLM）功能已显著改进，因此您可能不会遇到此问题。但如果无法解决冲突，请联系 Kingston 技术支持部门或访问 [Kingston.com/support](https://www.kingston.com/support) 获取进一步帮助。



IRONKEY™ Locker+ 50 G2
(LP50G2) 安全性 USB 3.2 Gen 1
快閃隨身碟

使用者指南



目錄	
簡介	3
Locker+ 50 G2 特色	4
關於本使用手冊	4
系統需求	4
建議	5
使用正確的檔案系統	5
使用提醒	5
密碼設定的最佳做法	6
設定我的裝置	7
裝置存取 (Windows 環境)	7
裝置存取 (macOS 環境)	7
裝置初始化 (Windows 與 macOS 環境)	8
密碼選擇	9
虛擬鍵盤	11
密碼顯示切換	12
管理員和使用者密碼	13
聯絡資訊	15
裝置使用 (Windows 與 macOS 環境)	16
管理員和使用者登入 (管理員已啟用)	16
僅供使用者登入模式 (管理員未啟用)	16
暴力破解保護	17
存取我的安全檔案	17
裝置選項	18
LP50G2 設定	20
管理員設定	20
使用者設定：管理員啟用	21
使用者設定：管理員未啟用	22
變更與儲存 LP50G2 設定	23
管理員功能	24
使用者密碼重設	24
說明與疑難排解	25
LP50G2 鎖定	25
LP50G2 裝置重設	27
磁碟代號衝突：(Windows)	28



圖 1：IronKey LP50G2

簡介

Kingston IronKey™ Locker+ 50 G2 USB 隨身碟提供企業級安全性，具備 FIPS 197 認證的 AES 256 位元 XTS 模式硬體加密，包含針對 BadUSB 與暴力密碼破解攻擊的防護機制。LP50G2 也符合 TAA 規範。

LP50G2 支援多密碼 (管理員和使用者) 選項，包含複雜模式和密碼短語模式。複雜模式允許使用 4 種字元集中的 3 種來輸入 6-16 個字元長度的密碼。新的短語模式允許輸入 10 到 64 個字元長度數字 PIN、句子、單詞列表，甚至是歌詞。管理員可以啟用使用者密碼，或重設使用者密碼以恢復對資料的存取權限。輸入密碼時，可以開啟「眼睛」符號顯示輸入的密碼，以減少因打字錯誤而導致登入失敗。暴力攻擊防護會在連續輸入 10 次無效密碼時鎖定使用者；如果連續 10 次輸入錯誤的管理員密碼時，則會加密刪除隨身碟的資料。此外，內建的虛擬鍵盤提升安全性，以防止鍵盤記錄程式或螢幕記錄程式盜取密碼。

Locker+ 50 G2 便利性十足，小巧金屬外殼和鑰匙圈設計，以便將資料帶到任何地方。

LP50G2 享有 5 年有限產品保固及免費技術支援服務。

IronKey Locker+ 50 G2 特色

- 獲得 FIPS 197 認證
- XTS-AES 硬體式加密 (永遠啟動的加密模式)
- 暴力密碼破解與 BadUSB 攻擊保護
- 多重密碼選項
- 複雜或密碼片語模式
- 眼睛按鈕可顯示輸入的密碼，藉此減少失敗的登入嘗試
- 虛擬鍵盤可協助防範密碼側錄器和螢幕側錄器
- Windows 或 macOS 相容 (詳情請查詢資料集)

關於本使用手冊 (02122026)

本使用手冊涵蓋 IronKey Locker+ 50 G2

(LP50G2)

系統需求

電腦平台 • Intel 和 AMD • 15MB 免費磁碟空間 • 可用的 USB 2.0 - 3.2 連接埠 • 最後一個實體磁碟之後的兩個連續磁碟機代號* *注意：請參閱第 28 頁「磁碟代號衝突」。	PC 作業系統支援 • Windows 11
Mac 平台 • Intel 與 Apple SOC • 15 MB 可用硬碟空間 • USB 2.0 - 3.2 連接埠	Mac 作業系統支援 • macOS 13.x – 26.x

建議

為確保充分電力提供給 LP50G2 裝置，請直接將其插入筆記型電腦或桌上型電腦的 USB 連接埠中，如圖 1.1 所示。避免將 LP50G2 連接至任何具有 USB 連接埠的週邊裝置 (如鍵盤或 USB 供電的集線器)，如圖 1.2 所示。



圖 1.1 - 建議的使用方式



圖 1.2 - 不建議的使用方式

使用正確的檔案系統

IronKey LP50G2 預設格式化為 FAT32 檔案系統。其適用於 Windows 和 macOS 系統。但是，還有一些手動格式化磁碟的選項，例如 Windows 的 NTFS 和 exFAT。如果需要，您可以重新格式化資料分區，但注意重新格式化後會失去儲存其中的資料。

使用小提醒

為確保您的資料安全，Kingston 建議您：

- 在目標系統上設定和使用 LP50G2 之前，在您的電腦上執行病毒掃描
- 在公共或不熟悉的系統上使用隨身碟時，您可能需要在裝置上設定唯讀模式，以協助保護隨身碟免受惡意軟體的侵害
- 不使用時鎖定裝置
- 在拔下隨身碟之前先將隨身碟退出
- 當 LED 燈亮起時，切勿切斷裝置電源。如此可能損壞隨身碟並需要重新格式化，此時將會刪除您的資料
- 切勿將您的裝置密碼告訴任何人

尋找最新更新和資訊

造訪 kingston.com/support 以獲得最新的隨身碟更新、常見問題解答、文件和其他資訊。

注意：如果您的隨身碟有任何更新，請務必升級至最新版本。我們不支援將您的磁碟降級為較舊的軟體版本，這可能會導致儲存資料丟失，或者損害磁碟的其他功能。如果您有任何問題或疑問，請聯絡 Kingston 技術支援。

密碼設定的最佳做法

您的 LP50G2 具備強大的安全對策。其中包括針對暴力密碼破解的保護，密碼輸入嘗試只能重試 10 次，藉此阻止攻擊者猜測密碼。達到隨身碟重試次數上限時，LP50G2 將自動清除加密資料，將自身格式化並恢復到出廠設定。

多重密碼

LP50G2 支援多重密碼這項主要功能，有助於避免忘記一個或多個密碼時導致資料遺失。啟用所有密碼選項後，LP50G2 可支援兩種不同密碼，包括管理員和使用者密碼角色，可用來還原資料。

LP50G2 允許您選擇管理員密碼和使用者密碼這兩種主要密碼。管理員是類似超級使用者的角色，能隨時存取硬碟，並且設定使用者選項。

使用者也能存取硬碟，但與管理員相比則權限有限。如果您忘記了這兩個密碼中的其中一者，則可以使用另一組密碼來存取並取回資料。並將磁碟設定為具備兩組密碼。儘管只使用使用者密碼，但請務必切記，設定好兩組密碼，並且將管理員密碼存放在安全位置。

如果所有密碼都遺失，那就沒有其他方式能夠存取資料。此安全性裝置沒有設定任何後門，故 Kingston 也無法取回資料。Kingston 建議您，同時將這些資料儲存到其他媒體裝置上。LP50G2 可以重設並重複使用，但先前儲存其中的資料將被永久清除。

密碼模式

LP50G2 同時還支援兩個不同的密碼模式：

複雜

複雜密碼至少需要符合 6-16 個字元的要求，並且至少使用 3 個下列字元：

- 大寫字母字元
- 小寫字母字元
- 數字
- 特殊字元

密碼短語

LP50G2 支援 10 到 64 個字元的密碼短語。密碼短語並不遵循任何額外的規則，但是如果正確使用，可以提供極高程度的密碼保護。

密碼短語基本上是字元的任意組合，包括其他語言的字元。與 LP50G2 隨身碟一樣，密碼短語可與隨身碟所選擇的語言相符。這能讓您使用多個單字、一個短語、歌曲中歌詞和一行詩歌等，強大的複雜密碼是攻擊者最難猜到的密碼類型之一，而且使用者相對好記。

設定我的裝置

為確保 IronKey 加密 USB 隨身碟具有足夠的電源供應，請將其直接插入筆記型電腦或桌上型電腦的 USB 2.0/3.0 連接埠。避免將其連接到具有 USB 連接埠的任何週邊設備，例如鍵盤或 USB 供電的集線器。裝置初始設定必須在支援 Windows 或 macOS 的作業系統上完成。

裝置存取 (Windows 環境)

將 IronKey 加密 USB 隨身碟插入筆記型電腦或桌上型電腦上的可用 USB 連接埠，然後等待 Windows 偵測到它。

- Windows 使用者會接收到裝置驅動程式通知。(圖 3.1)



圖 3.1 - 裝置驅動程式通知

- 一旦新的硬體偵測完成，請在檔案總管中找到 Unlocker 分割區，並在其中選取 **IronKey.exe** 選項。(圖 3.2)
- 請注意，分割區代號將依照下一個可用磁碟機代號而有所不同。磁碟機代號會依據所連接的裝置而變動。右圖中，磁碟機代號為 (E:)。



圖 3.2 - Window 檔案總管/IronKey.exe

裝置存取 (macOS 環境)

將 LP50G2 插入至筆記型電腦或桌上型電腦上的 USB 連接埠，或是由 Mac 作業系統自動偵測。完成後，您會在桌面看見「IRONKEY」磁碟區。(圖 3.3)

- 連按兩下 IronKey CD-ROM 圖示。
- 接著在圖 3.3 顯示視窗中連按兩下 IronKey.app 應用程式圖示。接著會啟動初始化流程。

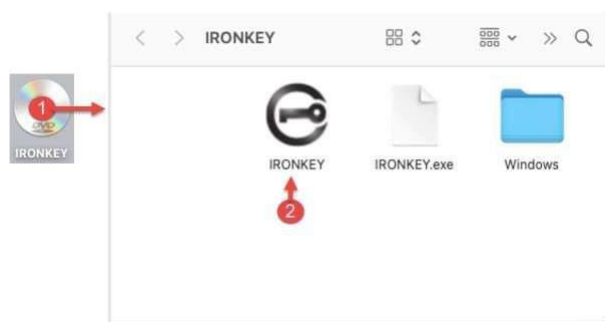


圖 3.3 - IRONKEY 磁碟區

裝置初始化 (Windows 和 macOS 環境)

語言和 EULA

從下拉式選單中選擇語言偏好，然後按一下「Next」(下一步)。(詳見圖 4.1)

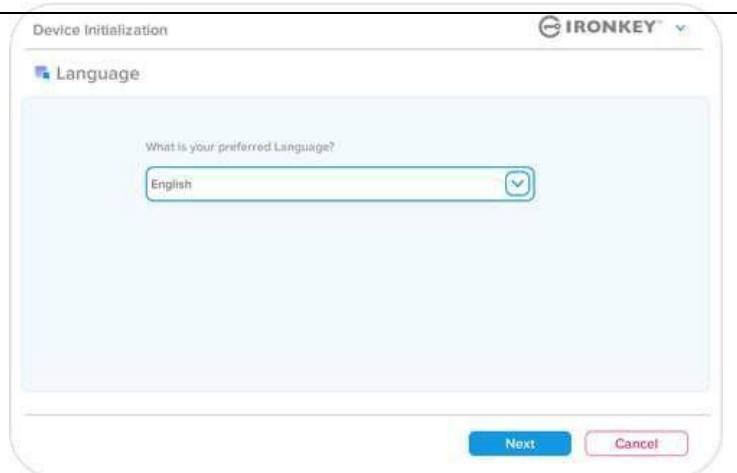


圖 4.1 - 語言選項

檢閱授權合約然後按一下「Next」(下一步)。

注意：您必須先接受授權合約才能繼續，否則「Next」(下一步) 按鈕將呈現在停用狀態。(圖 4.2)

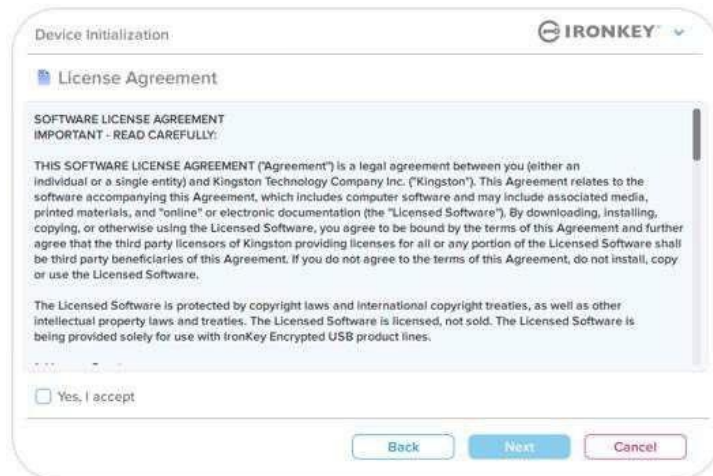


圖 4.2 - 授權合約

裝置初始化

密碼選擇

在密碼提示畫面上，可使用複雜密碼或密碼短語模式建立密碼，以保護 LP50G2 中的資料 (圖 4.3-4.4)。此外，還可以在此畫面上啟用多重密碼管理員/使用者選項。在繼續密碼選擇之前，請查看下面的「啟用管理員/使用者密碼」以便對於這些功能有更好的認識。

注意：一旦選擇了複雜或密碼短語模式，除非重設裝置，否則無法變更模式。要開始密碼選擇，請在「密碼」欄位中建立您的密碼，然後在「確認密碼」欄位重新輸入。您建立的密碼必須符合下列條件，系統才會讓您繼續初始化流程：

複雜密碼

- 必須包含 6 個以上的字元 (最多 16 個字元)。
- 必須包含下列的三 (3) 個條件：
 - 大寫
 - 小寫
 - 數字
 - 特殊字元 (!,\$,&, etc..)

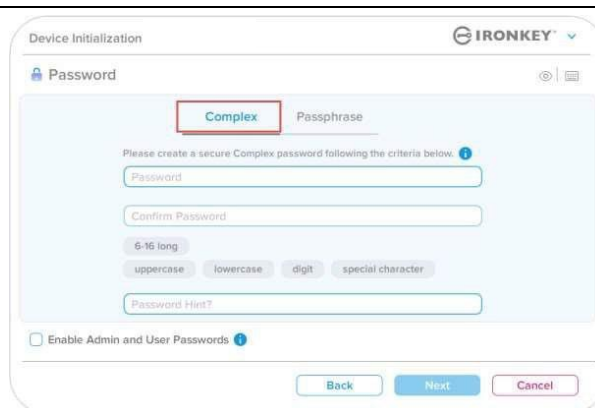


圖 4.3 - 複雜密碼

密碼短語

- 必須包含：
 - 最少 10 個字元
 - 最多 64 個字元

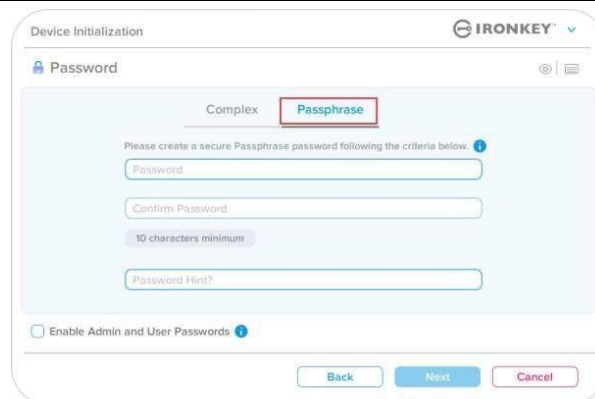


圖 4.4 - 密碼短語

密碼提示 (可選擇之選項)

如果您忘記密碼，密碼提示可提供有關密碼內容的線索。

注意：提示「不得」與密碼 完全相符。

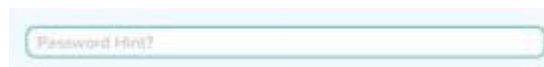
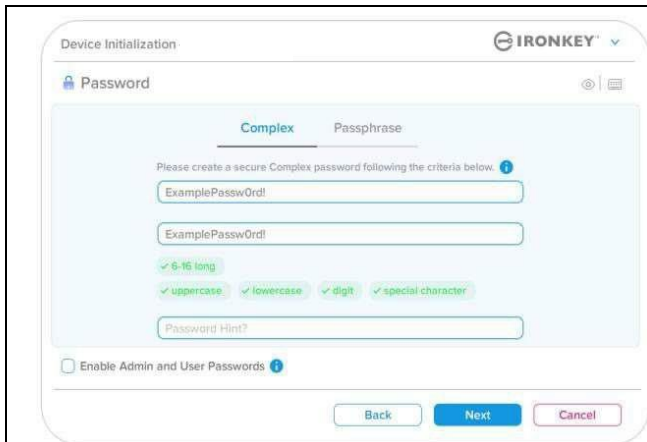


圖 4.5 - 密碼提示欄位

裝置初始化

有效與無效的密碼

如果是**有效**的密碼，在條件符合時，「密碼條件方塊」將會以**綠色**強調顯示。(詳見圖 4.6a-b) 注意：一旦符合三個密碼條件的最低限度，第四個條件方塊將變為灰色，表示此為選用條件。(圖 4.6b)



Device Initialization - IRONKEY™

Password

Complex Passphrase

Please create a secure Complex password following the criteria below. ⓘ

ExamplePassw0rd!

ExamplePassw0rd!

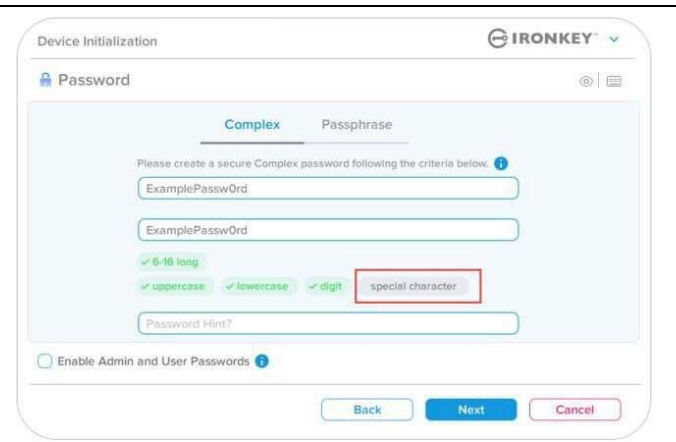
✓ 6-16 long
✓ uppercase ✓ lowercase ✓ digit ✓ special character

Password Hint?

☐ Enable Admin and User Passwords ⓘ

Back Next Cancel

圖 4.6a - 符合複雜密碼條件



Device Initialization - IRONKEY™

Password

Complex Passphrase

Please create a secure Complex password following the criteria below. ⓘ

ExamplePassw0rd

ExamplePassw0rd

✓ 6-16 long
✓ uppercase ✓ lowercase ✓ digit special character

Password Hint?

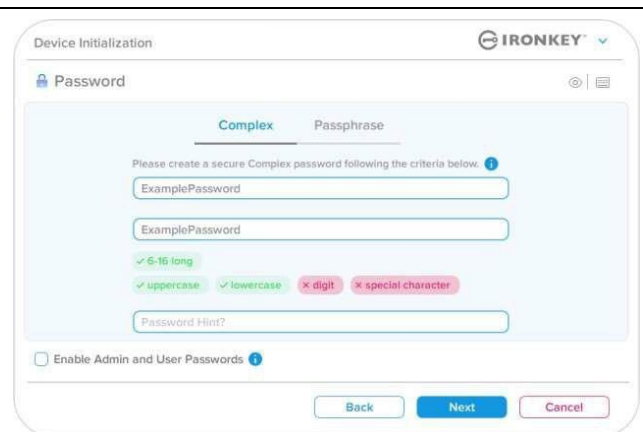
☐ Enable Admin and User Passwords ⓘ

Back Next Cancel

圖 4.6b - 選用複雜密碼條件

如果是**無效**的密碼，「密碼條件方塊」會以**紅色**強調顯示，同時會停用「Next」(下一步) 按鈕，直到符合最低條件需求為止。

此情況適用於複雜密碼與密碼短語。



Device Initialization - IRONKEY™

Password

Complex Passphrase

Please create a secure Complex password following the criteria below. ⓘ

ExamplePassword

ExamplePassword

✓ 6-16 long
✓ uppercase ✓ lowercase ✗ digit ✗ special character

Password Hint?

☐ Enable Admin and User Passwords ⓘ

Back Next Cancel

圖 4.7 - 密碼條件不符

裝置初始化

虛擬鍵盤

LP50G2 具有可用於鍵盤記錄程式保護的虛擬鍵盤。

- 若要利用**虛擬鍵盤**，請在**裝置初始化**畫面的右上角找到鍵盤按鈕然後加以選取。

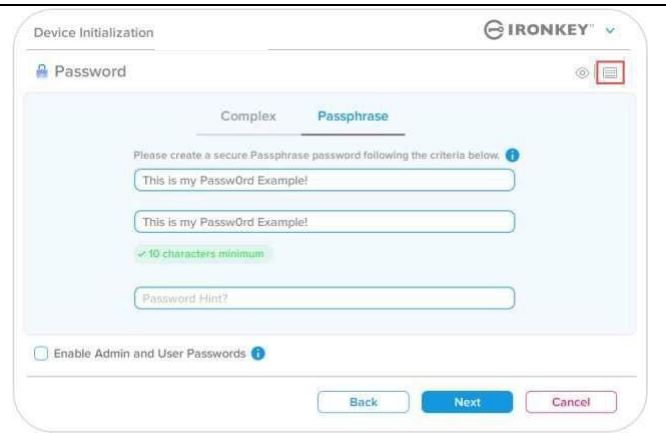


圖 4.8 - 啟用虛擬鍵盤

- 出現虛擬鍵盤後，您還可以啟用**螢幕記錄程式保護**。在使用此功能時，所有按鍵將短暫變為空白。這是預期中的效果，可避免螢幕側錄器擷取您所點選的內容。
- 為使得此功能更加強大，您還可以選擇鍵盤右下角的**隨機化 (randomize)**，以便隨機化虛擬鍵盤。隨機排列將隨機排列鍵盤位置。



圖 4.9 - 螢幕側錄器防護/隨機排列

裝置初始化

密碼顯示切換

預設情況，當您建立密碼時，密碼字串將在您輸入時顯示在欄位中。如果您想要在您輸入時隱藏密碼字串，可以切換位於裝置初始化視窗右上角的密碼眼睛，將密碼字串隱藏。

注意：在裝置初始化之後，密碼欄位將會預設為「隱藏」。

若要**隱藏**密碼字串，請按一下灰色圖示。

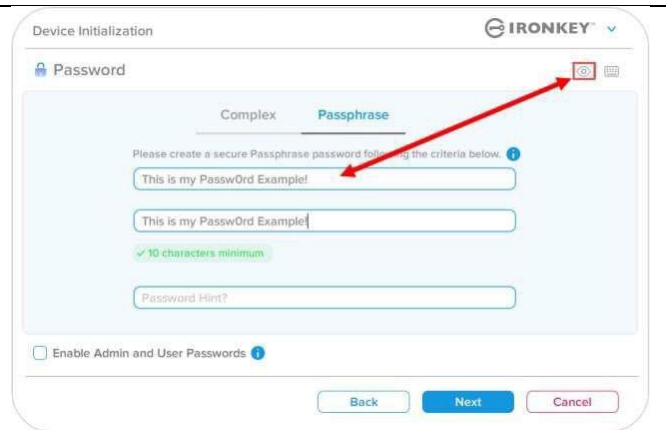


圖 4.10 - 切換隱藏的密碼

若要**顯示**隱藏的密碼，請按一下藍色圖示。

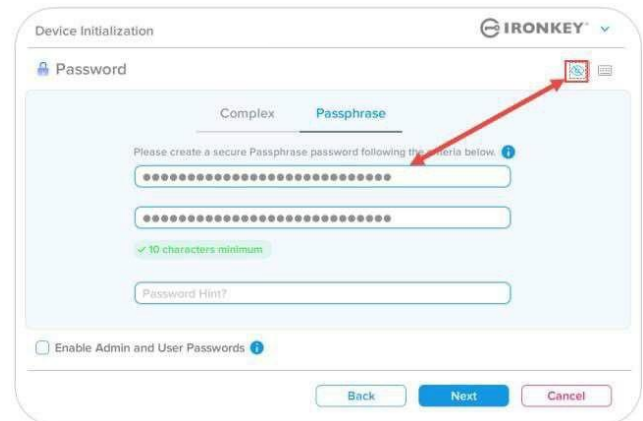


圖 4.11 - 切換顯示的密碼

裝置初始化

管理員和使用者密碼

藉由啟用「管理員和使用者密碼」，您可以利用多密碼功能，擁有管理員角色者可以利用此功能管理兩個帳戶。選取「**啟用管理員和使用者密碼**」允許在忘記其中一個密碼的情況下，使用另一種隨身碟存取的替代方法。

在**管理員和使用者密碼**啟用的情況下，您也可以存取：

- 使用者密碼重設

如要瞭解這些功能的更多相關資訊，請瀏覽本使用者指南中的第 24 頁。

- 若要啟用**管理員和使用者密碼**，請按一下「**啟用管理員和使用者密碼**」旁邊的方塊，然後在完成選擇有效的密碼之後選取「**Next**」(下一步)。(圖 4.12)
- 如果此功能已經**啟用**，則在此畫面中選擇的密碼將會是**管理員密碼**。按一下「**Next**」(下一步)以前進至**使用者密碼**畫面，可在此畫面中為使用者選擇密碼。

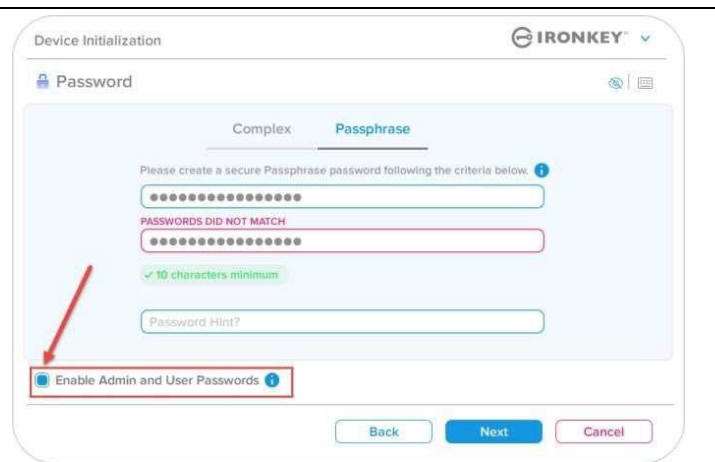


圖 4.12 - 啟用管理員和使用者密碼

注意：啟用管理員和使用者密碼為可選功能。

如果已經設定隨身碟但未啟用此功能 (方塊取消核取)，則會將隨身碟設定為「**單一使用者，單一密碼**」隨身碟，而且**不擁有任何管理員功能**。在本手冊當中，此組態也被稱為**僅使用者模式**。

若要繼續「**單一使用者，單一密碼**」設定，請將「**啟用管理員和使用者密碼**」維持取消核取，然後在建立有效的密碼之後，按一下「**Next**」(下一步)。

裝置初始化

管理員和使用者密碼

如果已在上一個畫面中啟用管理員角色，則後續畫面會提示輸入**使用者密碼** (圖 4.13)，與管理員密碼相比，使用者密碼在功能上會受到限制，本使用者指南會在稍後討論更多細節。**注意：**在本文件的其他部分，「**管理員和使用者密碼**」將被稱為「**管理員角色**」。

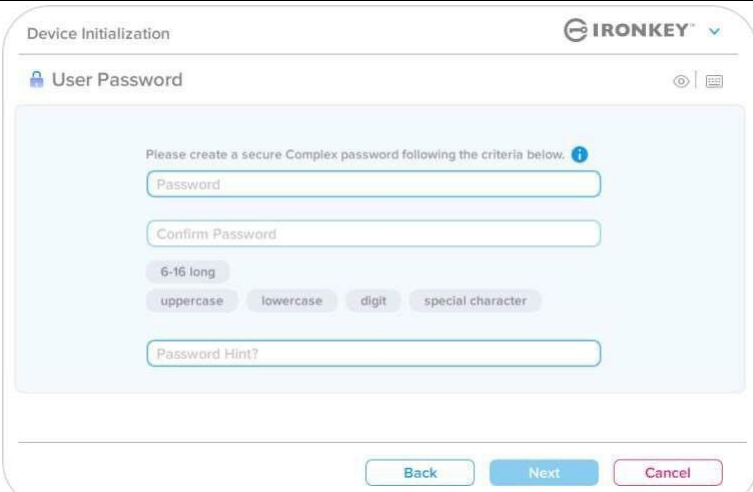


圖 4.13 - 使用者密碼 (管理員與使用者已啟用)

注意：選擇的「密碼選項」(複雜或密碼短語) 條件將會延續至使用者密碼，以及在設定隨身碟後需要進行的任何密碼重設。選擇的密碼選項僅可在完整裝置重設後方可變更。

裝置初始化

聯絡資訊

在提供的文字方塊中輸入您的聯絡資訊。(詳見圖 4.14)

注意：您在這些欄位中輸入的資訊可能並未包含您在步驟 3 中建立的密碼字串。但這些是可選填欄位，如果必要可以留空。

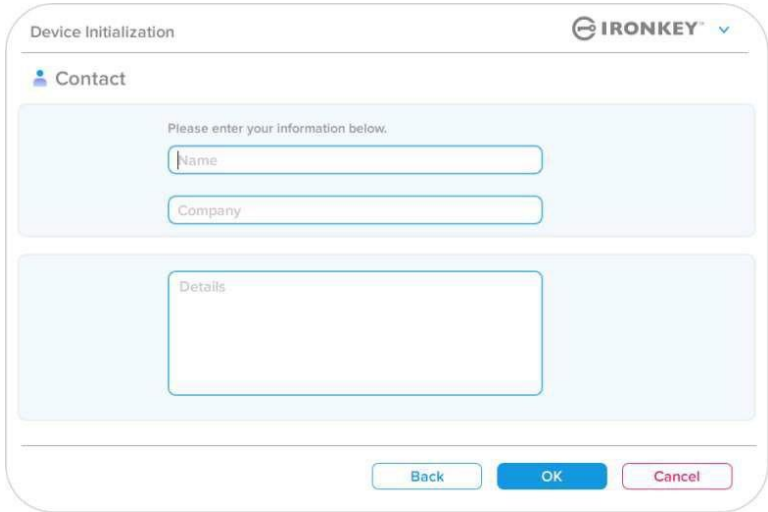
「Name」(名稱) 欄位可包含多達 32 個字元，但不得包含確切密碼。 「Company」(公司) 欄位可包含多達 32 個字元，但不得包含確切密碼。 「Details」(詳細資訊) 欄位可包含多達 156 個字元，但不得包含確切密碼。	 The screenshot shows a 'Device Initialization' window with the 'IRONKEY' logo. Under the 'Contact' section, there is a prompt 'Please enter your information below.' followed by three input fields: 'Name', 'Company', and 'Details'. At the bottom, there are three buttons: 'Back', 'OK', and 'Cancel'.
--	---

圖 4.14 - 聯絡資訊

注意：按一下 OK (確定) 將完成初始化過程並繼續解鎖，然後安裝可以在其中安全地儲存資料的安全分割區。拔下隨身碟並將其重新插回系統以查看反映的變更。

裝置使用 (Windows 和 macOS 環境)

管理員和使用者的登入 (管理員已啟用)

如果裝置在已經啟用管理員和使用者密碼 (管理員角色) 的情況下初始化，IronKey LP50G2 應用程式將啟動，並且先提示使用者密碼登入畫面。您可以利用「使用者密碼」在此處登入，查看輸入的任何聯絡資訊，或是以管理員身分登入 (圖 6.1)。按一下「以管理員身分登入」按鈕 (如下所示)，應用程式會繼續「管理員登入」選單，您可以在這裡以管理員身分登入，存取管理員設定與功能 (圖 6.2)。

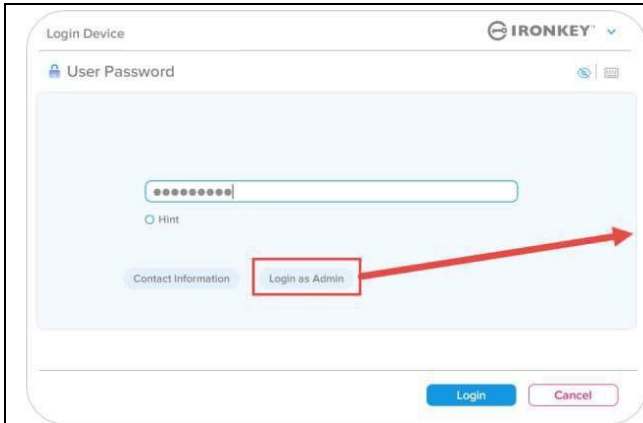


圖 6.1 - 使用者密碼登入 (管理員已啟用)

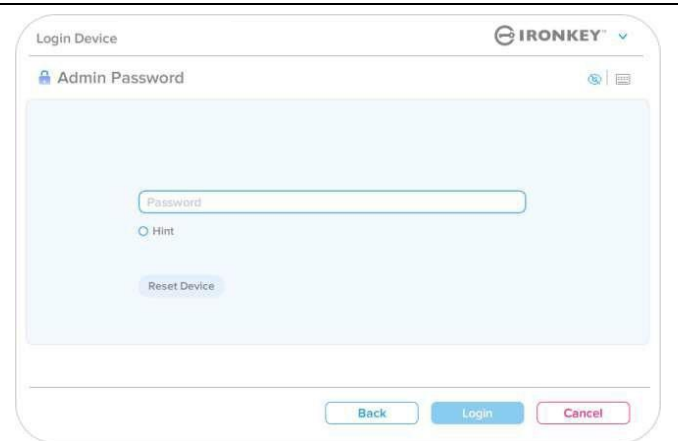


圖 6.2 - 管理員密碼登入

單一使用者登入模式 (管理員未啟用)

正如第 13 頁中所提到的，儘管建議使用「管理員角色」功能以使用裝置的完整功能，但還是在僅使用者 (單一密碼，單一使用者) 設定中初始化 IronKey 隨身碟。對於那些希望使用簡單的單一密碼方法來保護隨身碟資料的人來說，這可說是一個選項。(圖 6.3)

注意：若要啟用管理員與使用者密碼，請使用「重設裝置」按鈕將隨身碟回復至初始狀態，您可以在這裡啟用管理員與使用者密碼。**進行重設裝置時，隨身碟中的所有資料將進行格式化並且永久遺失。**

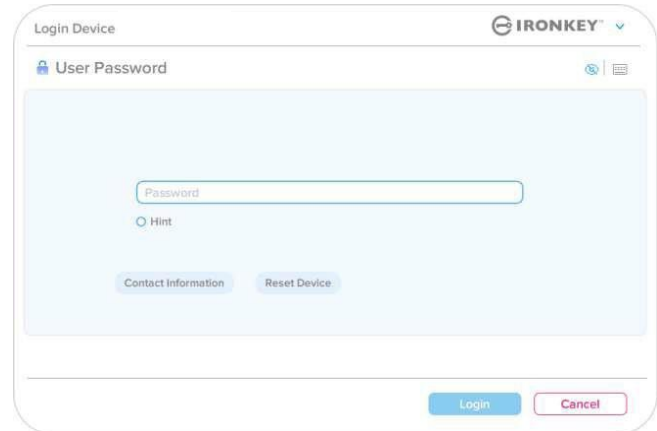


圖 6.3 - 使用者密碼登入 (管理員未啟用)

裝置使用

暴力破解保護

重要須知：在登入過程中，如果輸入錯誤密碼，您可嘗試第二次登入，但是系統內建的安全性功能(也稱為暴力破解保護)會自動記錄嘗試登入失敗的次數。*

如果此數字達到預先設定的 10 次失敗密碼嘗試 的數值，行為將會如下：

管理員/使用者啟用	暴力破解保護裝置動作 (10 次錯誤密碼嘗試)	資料清除與 裝置重設？
使用者密碼：	密碼鎖定。以管理員身分登入以重設使用者密碼	否
管理員密碼	加密清除隨身碟、密碼、設定以及資料 永久清除	是
僅使用者 單一使用者，單一密碼 (管理員/使用者未啟用)	暴力破解保護裝置動作 (10 次錯誤密碼嘗試)	資料清除與 裝置重設？
使用者密碼	加密清除隨身碟、密碼、設定以及資料 永久清除	是

* 成功驗證裝置後，將根據使用的登入方法重設失敗登入計數器。加密清除將會刪除所有密碼、加密金鑰與資料 – **您的資料將會永久遺失**。

安全存取我的檔案

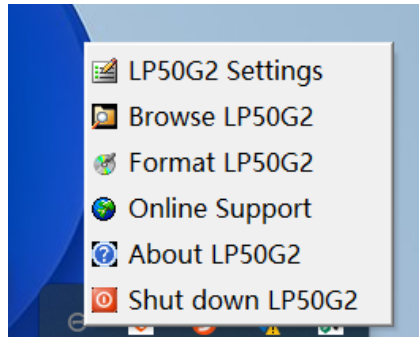
解鎖隨身碟後，您可以存取安全檔案。在隨身碟上儲存或開啟檔案時，檔案會自動加密和解密。這項技術提供您如一般隨身碟正常運作的便利性，同時提供了強大「永遠啟動」的安全性。

提示：您也可以 Windows 工作列中的 **IronKey** 圖示 上按一下右鍵，然後按一下 **瀏覽 LP50G2** 以存取您的檔案 (圖 7.2)。

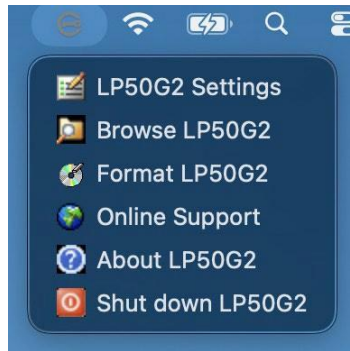
裝置選項 - (Windows 環境)

當您登入裝置時，視窗右上角會出現一個 IronKey 圖示。在 IronKey 圖示上按一下右鍵，會開啟選項選單，可選取可用的隨身碟選項 (圖 6.2)。

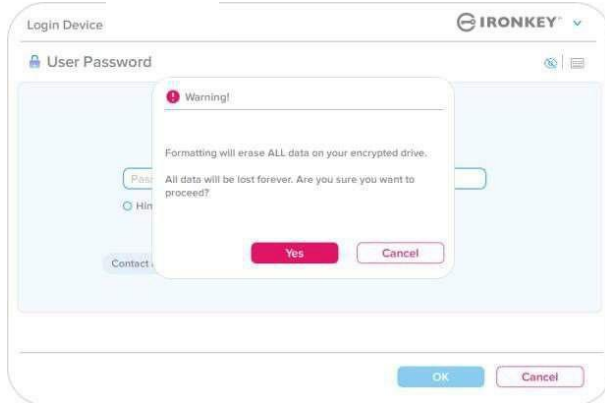
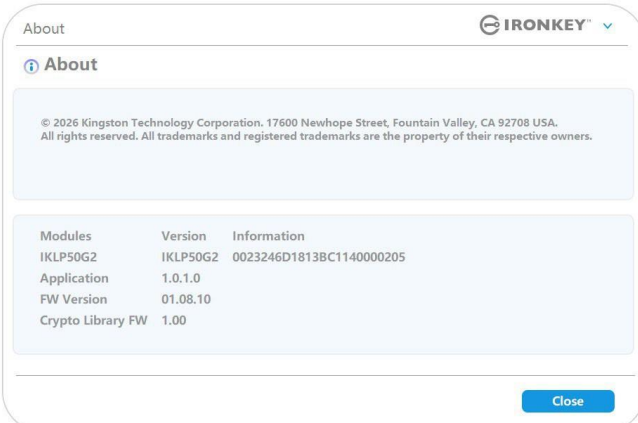
有關這些裝置選項的詳細資訊，請參閱本手冊的第 19-23 頁。

當您登入裝置時，視窗右上角會出現 IronKey 圖示。(圖 7.1)	 圖 7.1 - 工作列中的 IronKey 圖示
在 IronKey 圖示上按一下右鍵將會開啟選項選單以選取可用的隨身碟選項。(圖 7.2) 有關這些裝置選項的詳細資訊，請參閱本手冊的第 19-23 頁。	 圖 7.2 - 在 IronKey 圖示按一下右鍵以顯示裝置選項

裝置選項 - (macOS 環境)

在您登入裝置時，將會有如圖 7.3 所示的 IronKey LP50G2 圖示位於 macOS 選單中，在選單中可開啟可用的裝置選項。 有關這些裝置選項的詳細資訊，請參閱本手冊的第 19-23 頁。	 圖 7.3 - macOS 選單列圖示/裝置選項選單
--	--

裝置選項

LP50G2 設定：	變更登入密碼、聯絡資訊以及其他設定。(有關裝置設定的更多詳細資訊，請參閱本手冊的「LP50G2 設定」一節)。															
瀏覽 LP50G2：	可讓您檢視自己的安全檔案。															
格式化 LP50G2： 可讓您格式化安全資料磁碟分割區。 (警告：會清除所有資料。)(圖 6.1) 注意：格式化步驟需要密碼驗證。	 圖 7.4 - 格式化 LP50G2															
線上支援：	開啟網際網路瀏覽器並瀏覽至 http://www.kingston.com/support，您可以在該網站獲得其他支援資訊。															
關於 LP50G2： 提供 LP50G2 的特定詳細資訊，包括應用程式、韌體和序號資訊 (圖 6.2) 注意：隨身碟的唯一序號將會在「資訊欄」底下	 圖 7.5 - 關於 LP50G2 <table><tr><th>Modules</th><th>Version</th><th>Information</th></tr><tr><td>IKLP50G2</td><td>IKLP50G2</td><td>0023246D1813BC1140000205</td></tr><tr><td>Application</td><td>1.0.1.0</td><td></td></tr><tr><td>FW Version</td><td>01.08.10</td><td></td></tr><tr><td>Crypto Library FW</td><td>1.00</td><td></td></tr></table>	Modules	Version	Information	IKLP50G2	IKLP50G2	0023246D1813BC1140000205	Application	1.0.1.0		FW Version	01.08.10		Crypto Library FW	1.00	
Modules	Version	Information														
IKLP50G2	IKLP50G2	0023246D1813BC1140000205														
Application	1.0.1.0															
FW Version	01.08.10															
Crypto Library FW	1.00															
將 LP50G2 關機：	正確關閉 LP50G2，讓您從系統中安全地移除。															

LP50G2 設定

管理員設定

管理員登入允許下列裝置設定的存取：

- **密碼：**允許您變更您自己的管理員密碼和/或提示 (圖 8.1)
- **聯絡資訊：**允許您新增/查看/變更您的聯絡資訊 (圖 8.2)
- **語言：**可讓您變更目前語言選項 (圖 8.3)
- **管理員選項：**可允許您存取其他功能，例如：
 - 變更使用者密碼 (圖 8.4)

注意：有關管理員選項的其他詳細資訊，請參閱第 25 頁

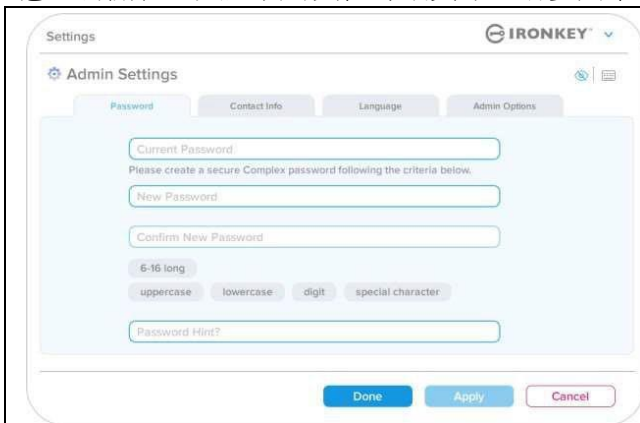


圖 8.1 - 管理員密碼選項

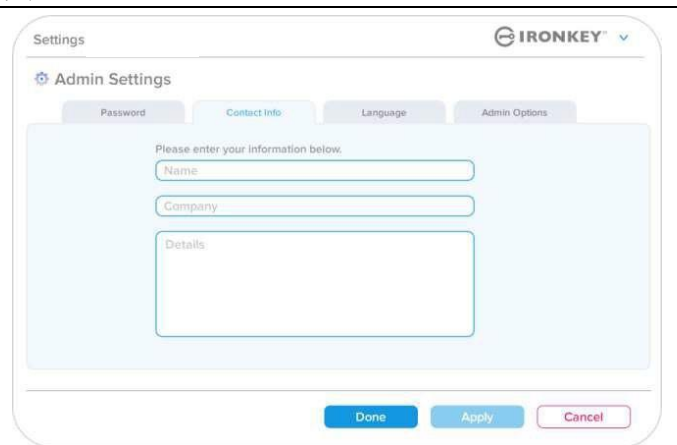


圖 8.2 - 聯絡資訊

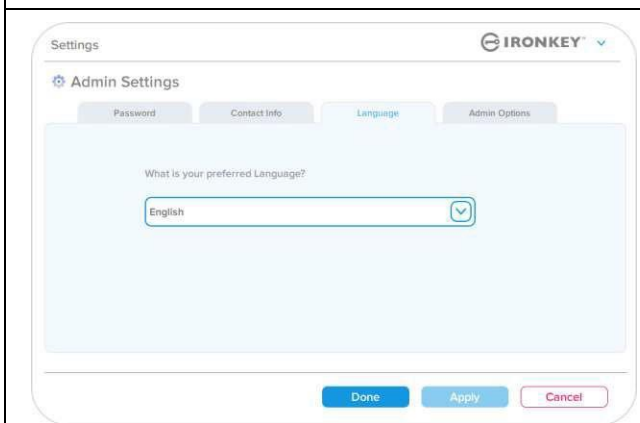


圖 8.3 - 語言選項

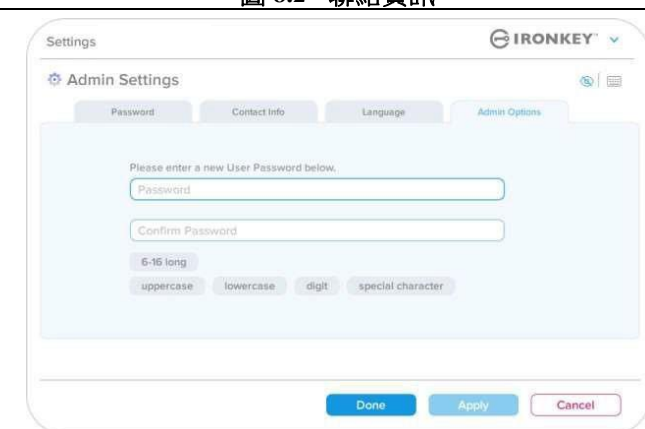


圖 8.4 - 管理員選項

LP50G2 設定

使用者設定：管理員啟用

使用者登入限制下列設定的存取：

密碼：

允許您變更自己的使用者密碼和/或提示。(圖 8.5)

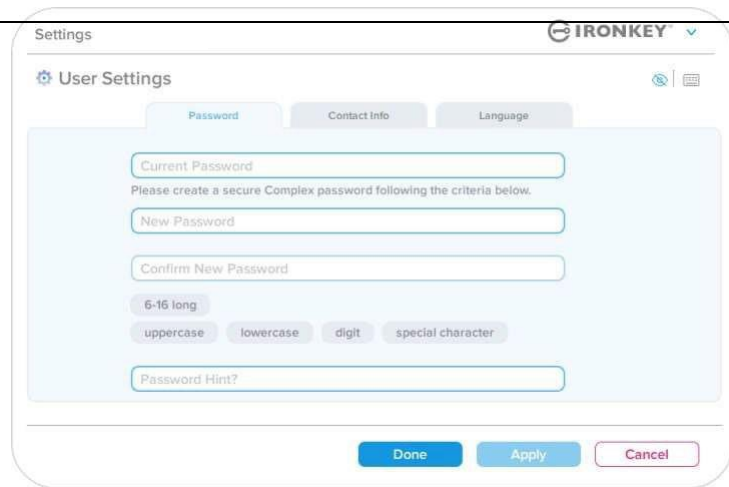


圖 8.5 - 密碼選項 (管理員啟用：使用者登入)

聯絡資訊：

允許 您新增/查看/變更您的聯絡資訊。(圖 8.6)

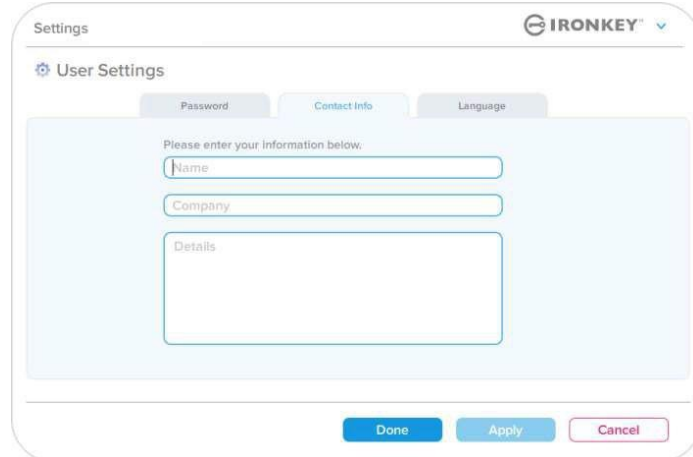


圖 8.6 - 聯絡資訊 (管理員啟用：使用者登入)

語言：

可讓您變更目前語言選項。(圖 8.7)

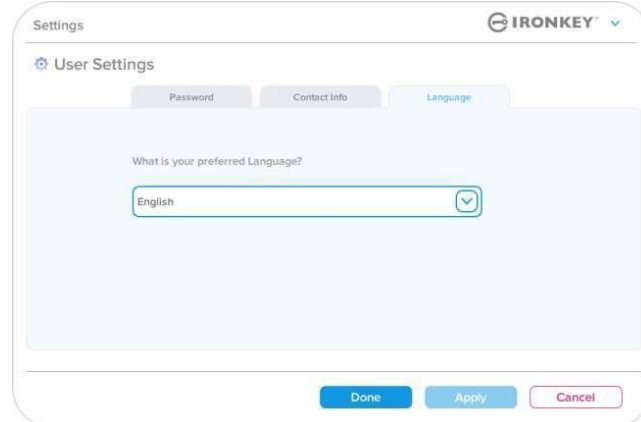


圖 8.7 - 語言設定 (管理員啟用：使用者登入)

注意：以使用者密碼登入時，無法存取管理員選項。

LP50G2 設定

使用者設定：管理員未啟用

管理員未啟用如同先前在第 12 頁中所提到的，如果初始化 LP50G2 而不啟用管理員和使用者密碼，將會以單一密碼，單一使用者設定配置隨身碟。此設定無權存取任何管理員選項或功能。此設定將有權存取以下 LP50G2 設定：

密碼

允許您變更自己的使用者密碼和/或提示。(圖 8.8)

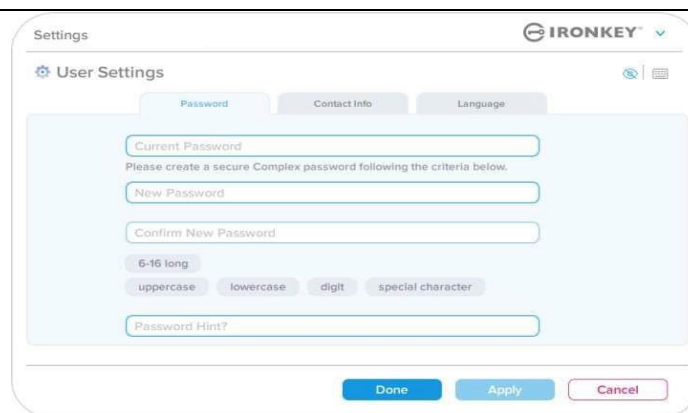


圖 8.8 - 密碼選項 (僅供使用者模式)

聯絡資訊：

允許您新增/查看/變更您的聯絡資訊。(圖 8.9)

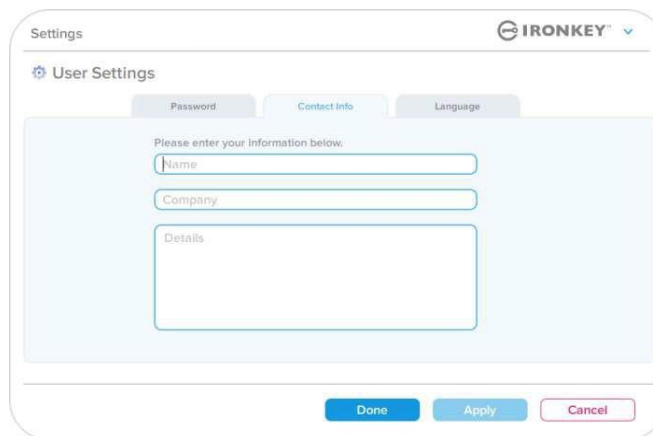


圖 8.9 - 聯絡資訊 (僅供使用者模式)

語言：

可讓您變更目前語言選項。(圖 8.10)

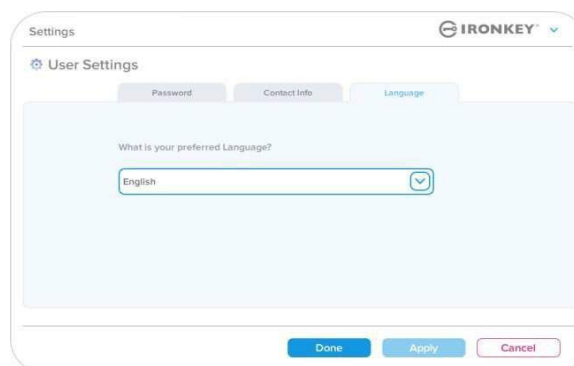


圖 8.10 - 語言設定 (僅供使用者模式)

LP50G2 設定

變更與儲存設定

- 每當 LP50G2 設定中的設定發生變更 (例如聯絡資訊、語言、密碼變更、管理員選項等) 時，隨身碟將提示您輸入密碼以便接受並套用變更。(詳見圖 8.11)

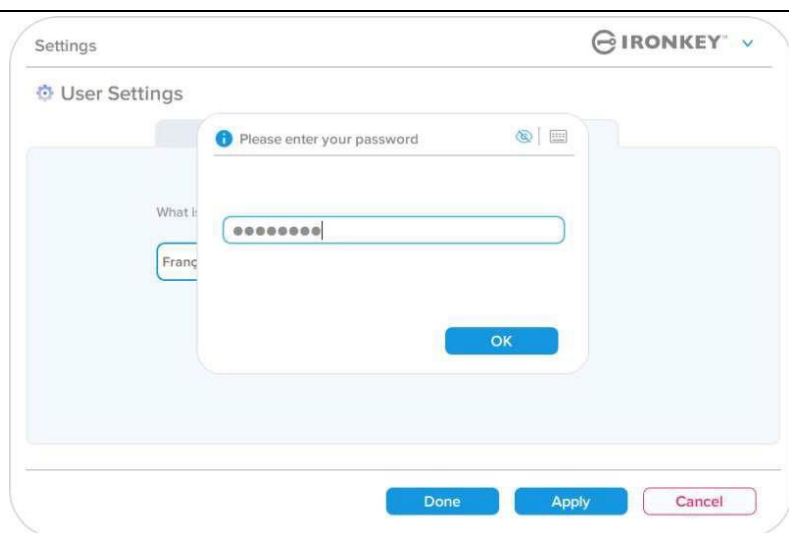


圖 8.11 - 儲存 LP50G2 設定變更的密碼提示畫面

注意：如果您在上面的密碼提示畫面中，並想取消或修改您的變更，只需確保密碼欄位為空白，然後按一下「確定」即可。這樣將會關閉「請輸入您的密碼」方塊並返回 LP50G2 設定選單。

管理員功能

可用於重設使用者密碼的選項

管理員設定中有一項實用功能，可允許您在忘記使用者密碼時安全地重設使用者密碼。以下是能協助您重設使用者密碼的功能：

使用者密碼重設：

在「管理員選項」選單中手動變更「使用者密碼」，此為立即變更，並且會在下次使用者登入時生效。(圖 9.1)

注意：預設的密碼需求標準為在初始化過程期間設定的原始標準 (複雜或密碼短語選項)。

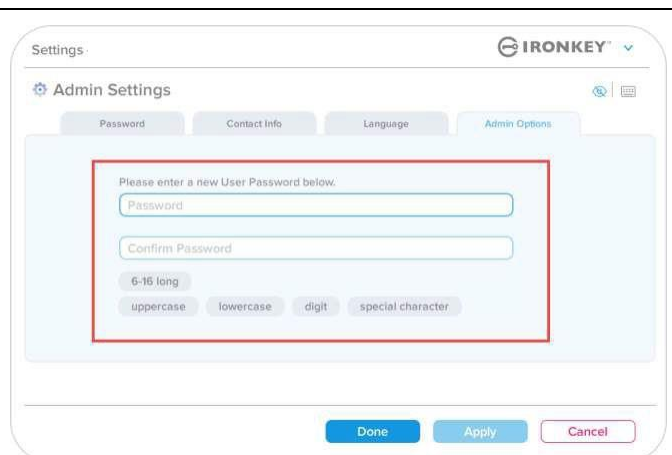


圖 9.1 - 管理員選項/使用者密碼重設

說明與疑難排解

裝置解鎖

LP50G2 包括可避免未經授權存取資料分割區的安全功能，一旦達到最大**連續**失敗登入嘗試 (簡稱 *MaxNoA*) 次數之後，即無法繼續登入。預設的「開箱即用」設定已經在每種登入方法 (管理員/使用者) 中預先設定嘗試次數為 10。

「鎖定」計數器會追蹤每次登入失敗次數，並以下列**兩種方式之一**進行重設：

1. 在達到密碼輸入失敗上限前的成功登入。
2. 達到 *MaxNoA* 並且執行裝置鎖定或是裝置格式化需視裝置的設定方式而定。

- 如果輸入不正確的密碼，「Password Entry」(密碼輸入) 欄位上方便會以紅色顯示錯誤訊息，表示發生登入錯誤。(圖 10.1)

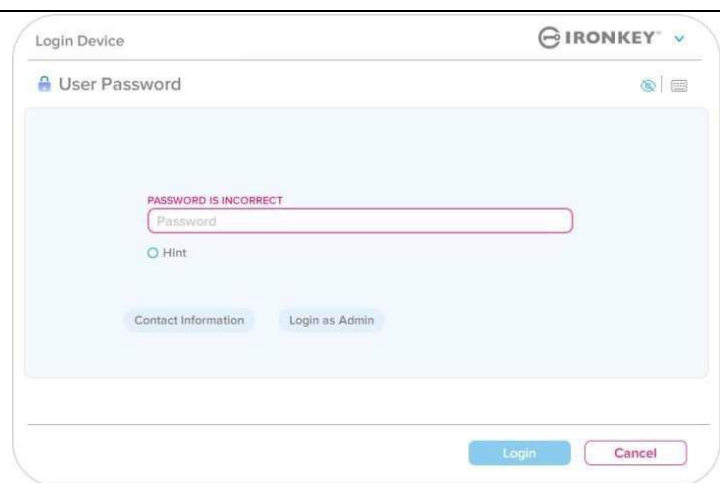


圖 10.1 - 密碼不正確訊息

- 如果嘗試失敗的次數達到第 7 次，您就會看到其他錯誤訊息，表示您再進行 3 次嘗試登入就會達到 *MaxNoA* (預設值為 10)。(圖 10.2)

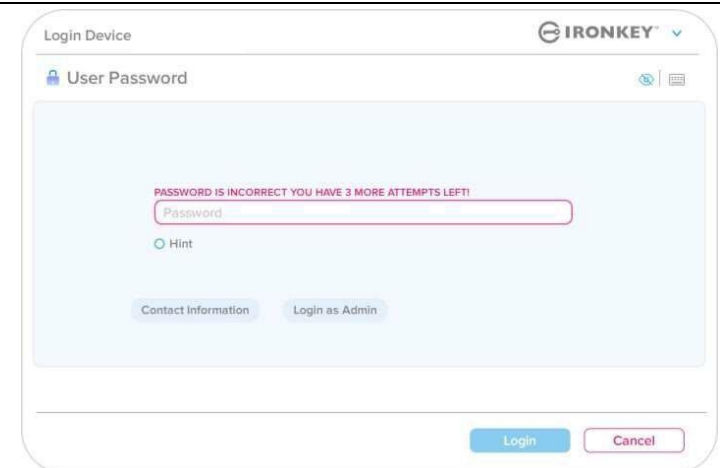


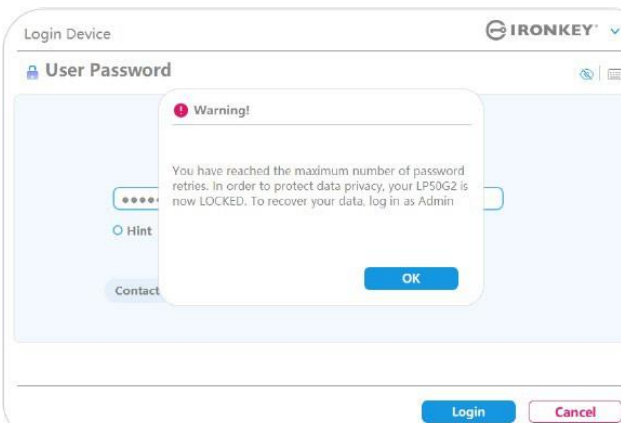
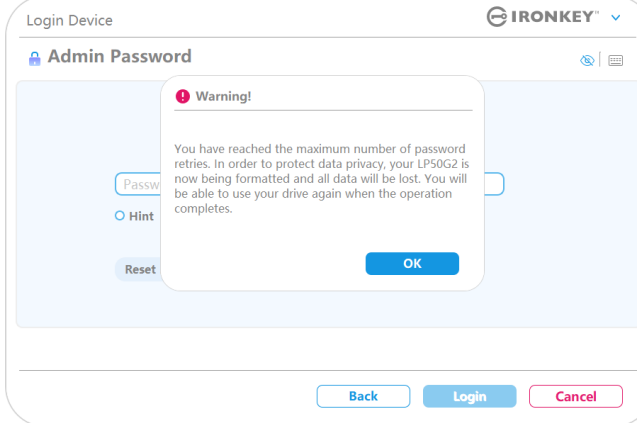
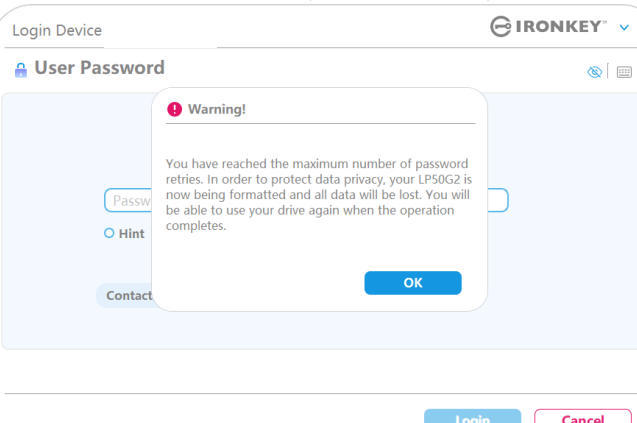
圖 10.2 - 第 7 次錯誤密碼嘗試

說明與疑難排解

裝置解鎖

重要須知：在輸入 **10** 次最終仍為失敗登入嘗試時，根據裝置的設定情況以及使用的登入方法 (管理員/使用者)，裝置將會遭到鎖定並且需要您使用替代方式登入 (如果適用)，或者需要裝置重設，此時將會**格式化資料**，**同時隨身碟上的所有資料將會永久遺失**。本使用者手冊中的第 17 頁也提及了相關行為。

下面的圖 10.3- 10.6 展示每個登入密碼方法第 10 次以及最後一次失敗登入的視覺行為。

使用者密碼：(管理員/使用者啟用)  裝置解鎖 圖 10.3	管理員密碼 (管理員/使用者啟用)  裝置格式化* 圖 10.4
- 這些安全措施會限制某人 (不知道您密碼的人)，使得他們無法無限次數嘗試登入並且取得您的敏感資訊 (也稱為暴力破解)。如果您是 LP50G2 的擁有者且忘記密碼，系統也會強制執行相同的安全性措施，包含裝置格式化。 * 如需此功能的更多資料，請參閱第 27 頁的「重設裝置」一節。	使用者密碼 (管理員未啟用)  裝置格式化* 圖 10.5

***注意：**裝置格式化將清除 LP50G2 安全資料分割區中儲存的所有資訊。

說明與疑難排解

重設裝置

如果您忘記密碼或是需要重設裝置，您可以按一下「Reset Device」(重設裝置) 按鈕，而該按鈕出現的位置則取決於 LP50G2 Launcher 執行時隨身碟的設定方式 (如果啟用管理員/使用者，則出現在管理員登入密碼選單，如果未啟用管理員/使用者，則出現在「使用者密碼」登入選單)。(詳見圖 10.7 和 10.8)

- 此選項可讓您建立新密碼，但如果是為了保護您資料的隱私權，則會格式化 LP50G2。這代表您的所有資料皆會在過程中被移除。*

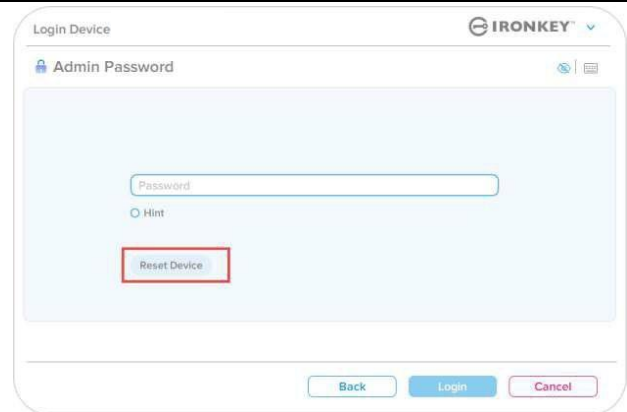


圖 10.6 - 管理員密碼：重設裝置按鈕

- 注意：**當您按一下「Reset Device」(重設裝置) 時，便會顯示一個訊息方塊且會詢問您是否希望先輸入新密碼，然後再執行格式化。此時，您可以：1) 按一下「OK」(確定) 確認；或是：2) 按一下「Cancel」(取消) 以返回登入視窗。(詳見圖 10.8)

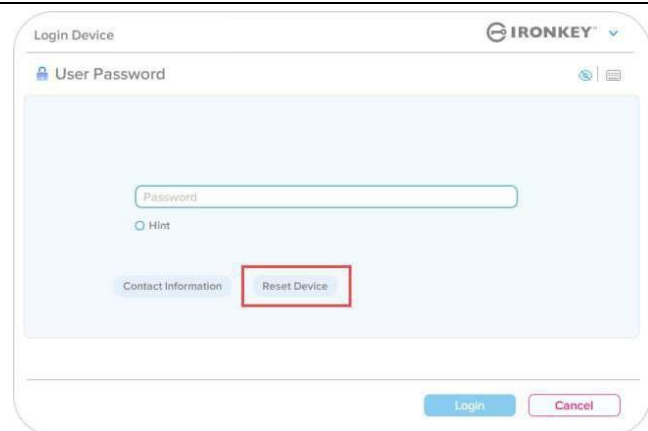


圖 10.7 - 使用者密碼 (管理員/使用者未啟用) 重設裝置

- 如果您選擇繼續，系統將提示您進入初始化螢幕，您可以在其中啟用「管理員和使用者模式」，並根據您選擇的密碼選項 (複雜或密碼片語) 輸入新密碼。提示不是必填欄位，但如果您忘記密碼，提示欄位可提供有關密碼內容的線索。

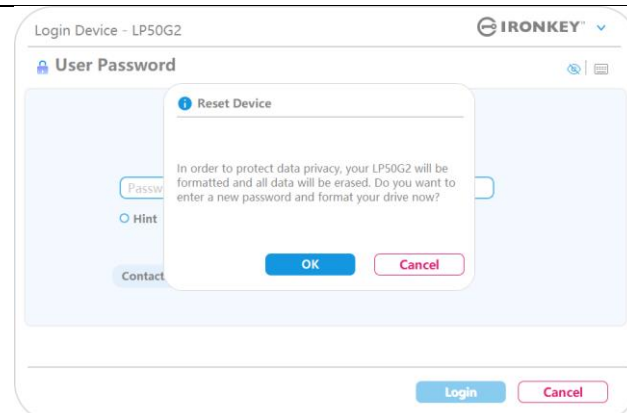


圖 10.8 - 重設裝置確認

磁碟代號衝突：Windows 作業系統

- 如同本使用者手冊第 4 頁的「系統要求」一節所述，LP50G2 需要兩個連續磁碟機代號位於最後實體磁碟之後，而最後實體磁碟則是出現在磁碟機代號指派「間隙」之前 (詳見圖 10.9。)此實體磁碟「不」屬於網路共用磁碟機，因為它專屬於使用者設定檔，而不是系統硬體設定檔本身，因此其狀態顯示為可供作業系統使用。
- 如此表示，Windows 可能指定 LP50G2 一個磁碟機代號，但是該代號已經被網路共用或是通用命名慣例 (UNC) 路徑所使用，導致磁碟代號衝突。如果遇上這種情況，請洽詢系統管理員或服務台支援部門，以瞭解在「Windows 磁碟管理」變更磁碟機代號指定的事宜 (需要用到管理員權限)。

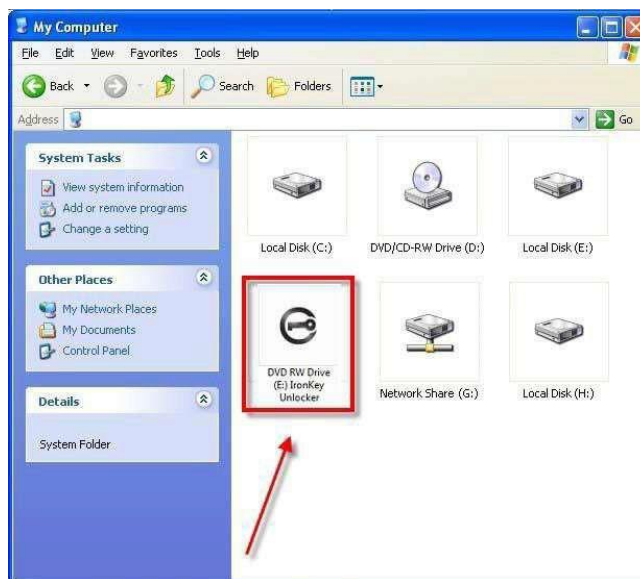


圖 10.9 - 磁碟機範例

在本例 (圖 10.9) 中，LP50G2 使用磁碟機 F:，這是磁碟機 E: (即磁碟機代號中斷前的最後一個實體磁碟機) 之後第一個可用的磁碟機代號。由於代號 G: 為網路共用磁碟機，而不是硬體設定檔的一部分，所以 LP50G2 可能會將它當作自己的第二個磁碟機代號，因此造成衝突。

如果您的系統上沒有網路共用，卻仍然無法載入 LP50G2，可能是因為讀卡機、卸除式磁碟或其他先前安裝的裝置佔用了指定的磁碟機代號，因此造成衝突。

請注意，Windows 11 已大幅改善了「磁碟機代號管理」(或 DLM) 的功能，因此您可能遇上這類問題，不過，如果您無法解決衝突的問題，請聯絡 Kingston 的技術支援部門或造訪 [Kingston.com/support](https://www.kingston.com/support)，以獲得進一步的協助。