User Manual

IronKey Locker Plus 50

Find the language and latest documentation here.

IKLP50 User Manual

 .....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 jezyku 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 (LP50)
SECURE USB 3.2 Gen 1 FLASH DRIVE

User Guide

Contents

Figure 1: IronKey LP50

Introduction

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

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

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

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

IronKey Locker+ 50 Features

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

About This Manual (09242024)

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

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 32.	**PC Operating System Support** • Windows 11 • Windows 10
Mac Platform • Intel & Apple SOC • 15MB free disk space • USB 2.0 - 3.2 Port	**Mac Operating System Support** • macOS 12.x – 15.x

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

Recommendations

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

Figure 1.1- Recommended Usage

Figure 1.2- Not recommended

Using the Correct File System

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

Usage Reminders

To keep your data safe, Kingston recommends that you:

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

Find the Latest Updates and Information

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

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

Best Practices for Password Setup

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

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

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

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

If 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 LP50 can be Reset and reused, but the prior data will be erased forever.

Password Modes
The LP50 also supports two different password modes:

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

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

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

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

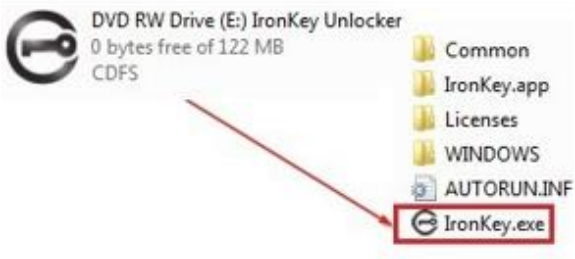
Setting Up My Device

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

Device Access (Windows Environment)

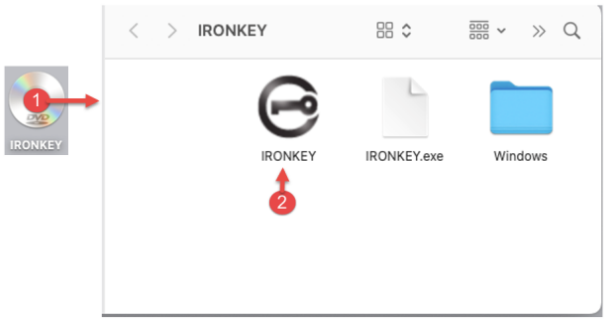
Plug the IronKey encrypted USB drive into an available USB port on the notebook or desktop and wait for Windows to detect it.

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

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

Device Access (macOS Environment)

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

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

Device Initialization (Windows & macOS Environment)

Language and EULA

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

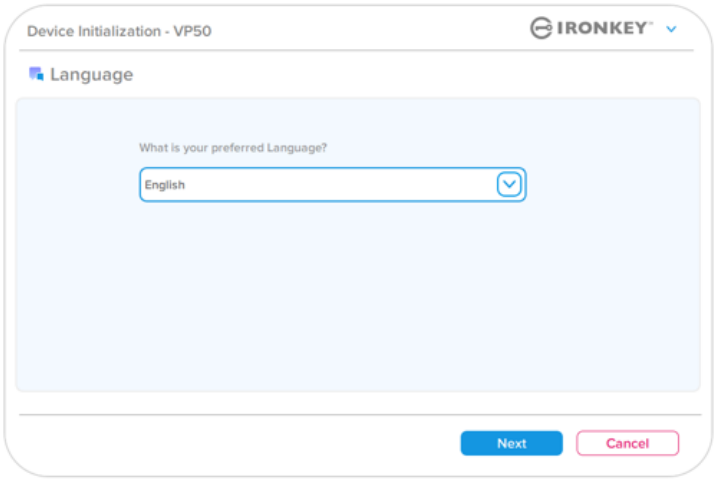


Figure 4.1 – Language Selection

- Review the license agreement and click **Next**.

  Note: You must accept the license agreement before continuing; otherwise, the **Next** button will remain disabled. (*Figure 4.2*)

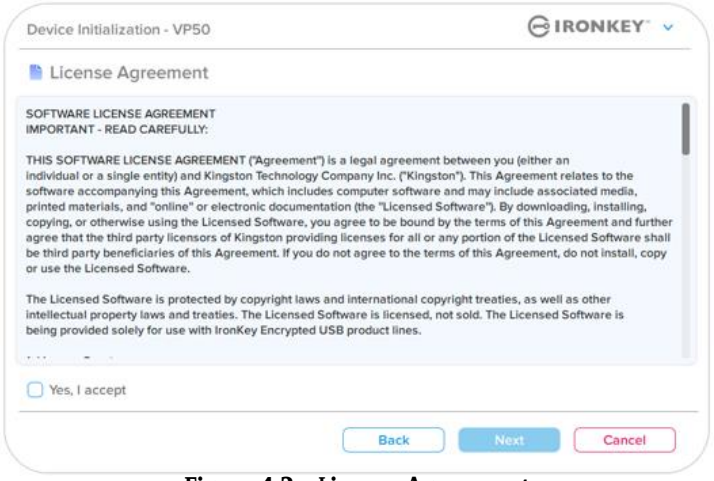


Figure 4.2 – License Agreement

Device Initialization

Password Selection

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

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

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

<table>
<tr>
<td>Complex Password
• Must contain 6 characters or more (up to 16 characters).

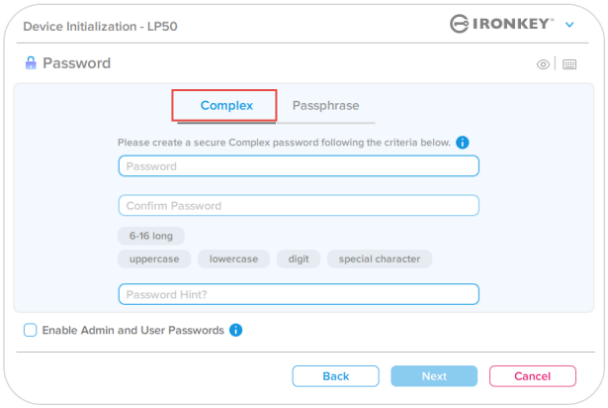
• Must contain three (3) of the following criteria:
o Upper Case
o Lower Case
o Numerical Digit
o Special characters (!,$,&, etc..)</td>
<td> 

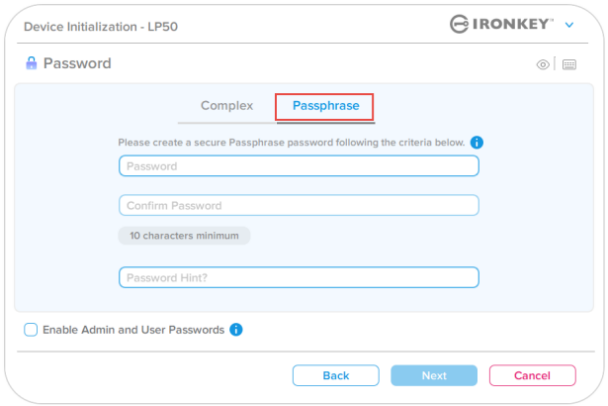
Figure 4.3 – Complex Password</td>
</tr>
<tr>
<td>Passphrase Password
• Must contain:
o 10 characters minimum
o 64 characters maximum</td>
<td> 

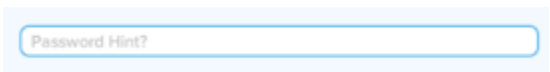
Figure 4.4 – Passphrase Password</td>
</tr>
<tr>
<td>Password Hint (Optional)
A password hint can be useful for providing a clue as to what the password is, should the password ever be forgotten.
Note: The hint CANNOT be an exact match to the password.</td>
<td> 

Figure 4.5 – Password Hint Field</td>
</tr>
</table>

Device Initialization

Valid and Invalid Passwords

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

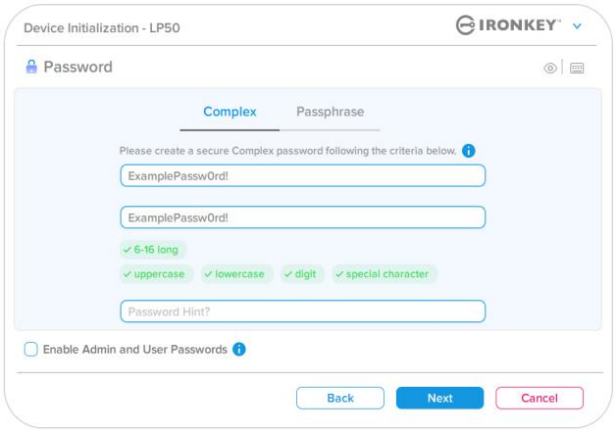


Figure 4.6a – Complex Password Condition Met

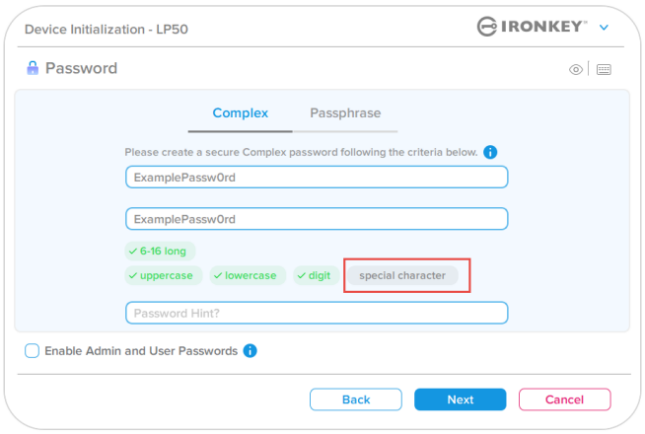


Figure 4.6b – Complex Password Condition Optional

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

This applies to both Complex and Passphrase Passwords.

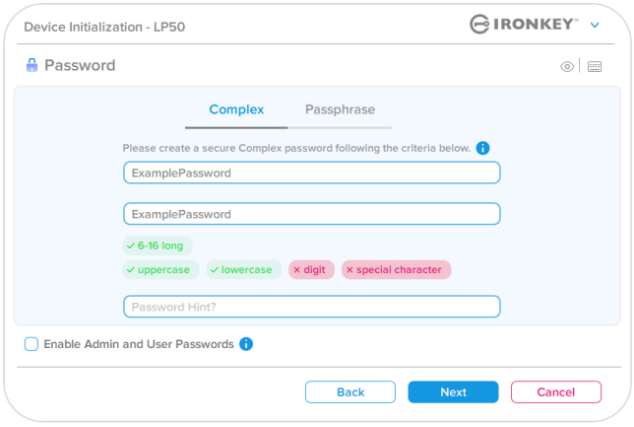


Figure 4.7 – Password Conditions Not Met

Device Initialization

Virtual Keyboard

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

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

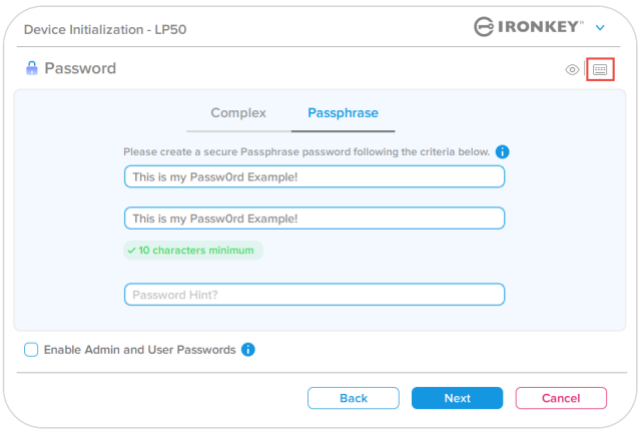


Figure 4.8 – Activating the Virtual Keyboard

- Once the virtual keyboard appears, you may also enable **Screenlogger Protection**. When using this feature, all the keys will briefly go blank. This is expected behavior, as it prevents screenloggers from capturing what you've clicked.
- To make this feature more robust, you may also choose to randomize the virtual keyboard by selecting **randomize** [(randomize)] in the lower-right of the keyboard. Randomize will arrange the keyboard in a random order.

Figure 4.9 – Screenlogger Protection / Randomize

Device Initialization

Password Visibility Toggle

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

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

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

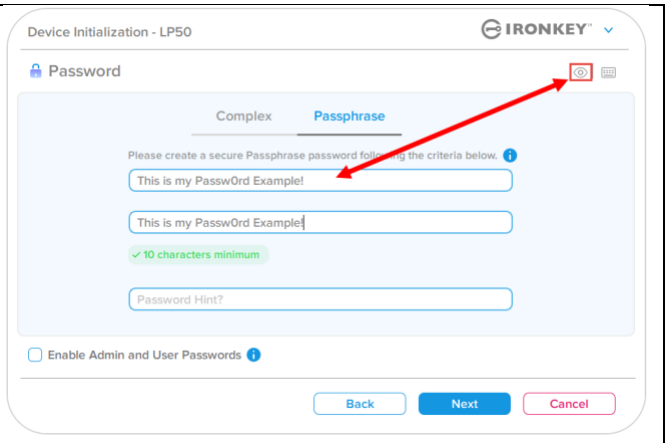


Figure 4.10 – Toggle 'hide' Password

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

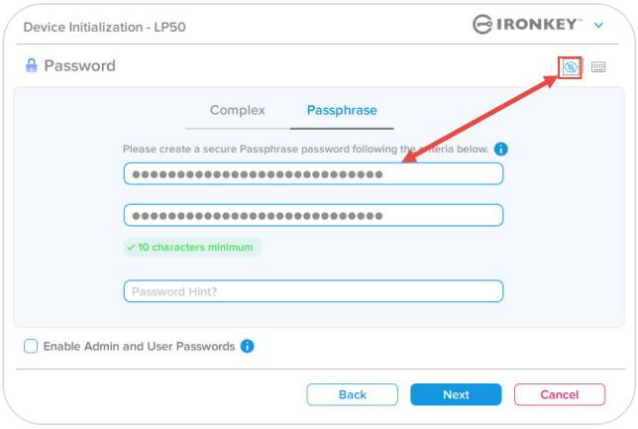


Figure 4.11 – Toggle 'show' Password

Device Initialization

Admin and User Passwords

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

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

- User Password reset

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

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

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

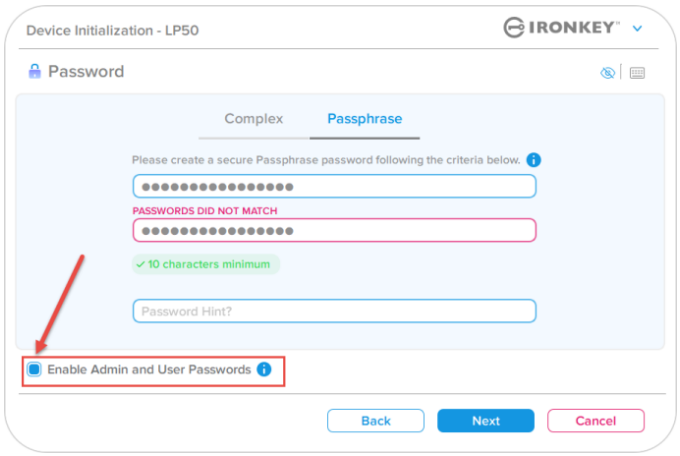


Figure 4.12 – Enabling Admin and User Passwords

Note: Enabling Admin and User passwords is optional.

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

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

Device Initialization

Admin and User Passwords

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

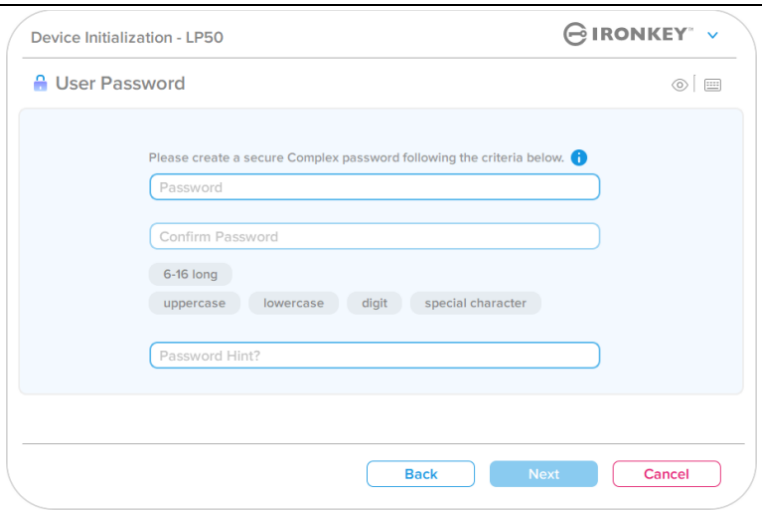


Figure 4.13 - User Password (Admin and User Enabled)

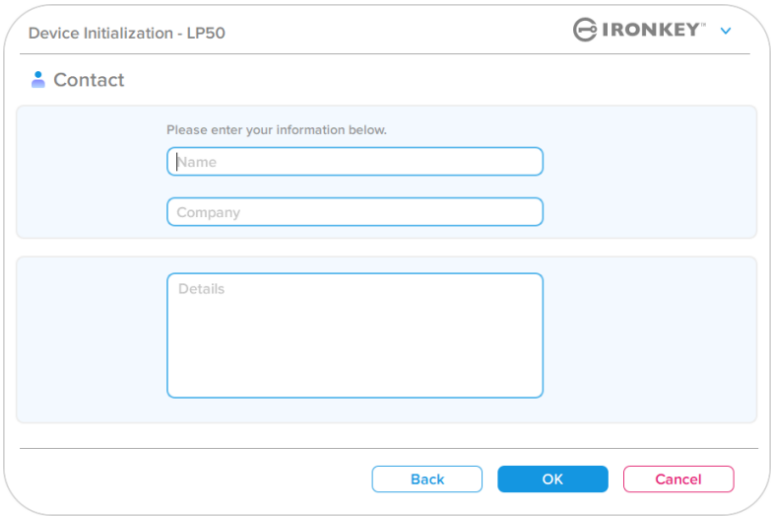
Note: The chosen Password Option (Complex or Passphrase) criteria will carry over to the User Password, and to any password resets that are needed after the drive is set up. The chosen password option may only be changed after a full device reset.

Device Initialization

Contact Information

Enter your contact information into the text boxes provided. (*See Figure 4.14*)

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

The '**Name'** field may contain up to 32 characters, but cannot contain the **exact** password. The '**Company'** field may contain up to 32 characters, but cannot contain the **exact** password. The '**Details'** field may contain up to 156 characters, but cannot contain the **exact** password.	 **Figure 4.14 - Contact information**

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

USB ß → Cloud Initialization (Windows Environment)

Once the device has been initialized in Windows, the USB-to-Cloud application will appear as seen in *Figure 5.1* on the right. Please make sure you have a working Internet connection before you continue.

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

Figure 5.1 – USBtoCloud Windows EULA

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

Figure 5.2 – Windows security alert

USB ß → Cloud Initialization (Windows Environment)

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

Figure 5.3 – Cloud Selection

USB ß → Cloud Usage (Windows Environment)

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

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

In the 'Settings' menu, you can:

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

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

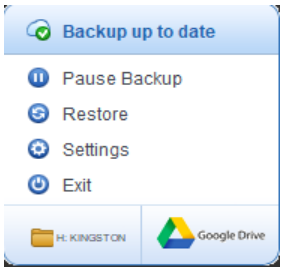


Figure 5.4- Services

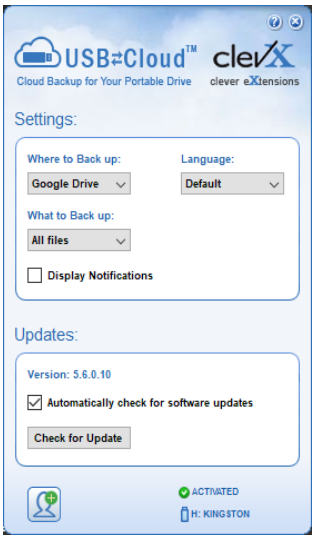


Figure 5.5- Settings

USB ß → Cloud Initialization (macOS Environment)

- Once the device has been initialized, the USB-to-Cloud application will appear as seen in *Figure 5.6* to the right. Please make sure you have a working Internet connection before you continue.
- To proceed with the installation, click the 'Accept' button in the bottom right-hand corner of the clevX window.

  (Note: On macOS 12.x + will be prompted to allow access to files on a removable volume. Select OK.) (*See Figure 5.7*)
- To decline the installation, click the 'Decline' button in the bottom left-hand corner of the clevX window.

Figure 5.6 – USBtoCloud macOS EULA

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

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

Figure 5.7- macOS access

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

  (Note: If you currently do not have an account set up with any of the cloud options listed, you may create one at this time, using your favorite Internet browser, and then completing this option afterwards.)
- Once you've chosen a cloud option and authenticated to the corresponding service, the USB-to-Cloud program will perform an initial comparison of the data partition against what is stored in the Cloud. As long as the USB-to-Cloud service is running in Task Manager, content written to the data partition will automatically back up (sync) to theCloud.

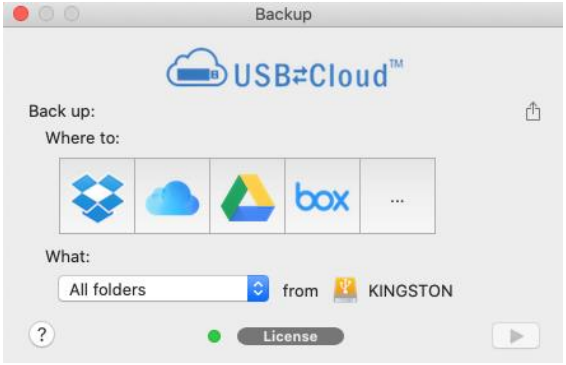


Figure 5.8- Cloud Selection

USB ß →Cloud Usage (macOS Environment)

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

- **Pause Backup** (Pauses a databackup)
- **Restore** (Restores data from the cloud to the device)
- **Backup** (Opens Cloud Options) *See Figure 5.9*
- **Exit** (Exits the USB-to-Cloudservice)

Figure 5.9- Services

In the 'Preferences' menu, you can:

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

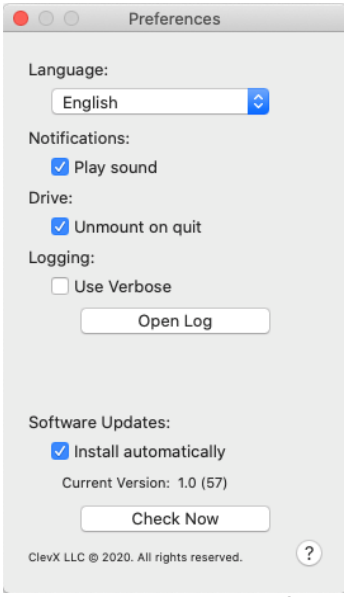


Figure 5.10- USBtoCloud Preferences

Device Usage (Windows & macOS Environment)

Login For Admin & User (Admin Enabled)

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

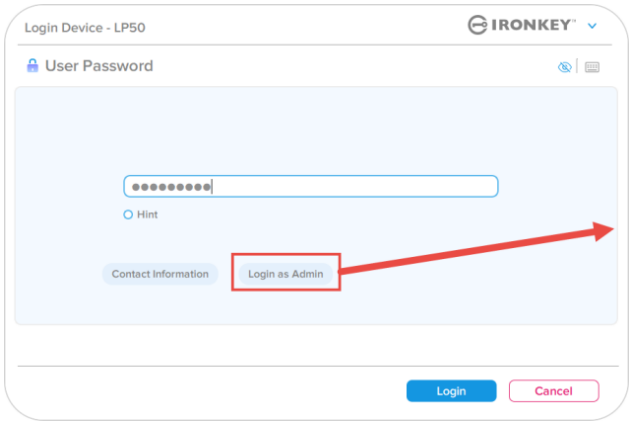


Figure 6.1 - User Password Login (Admin enabled)

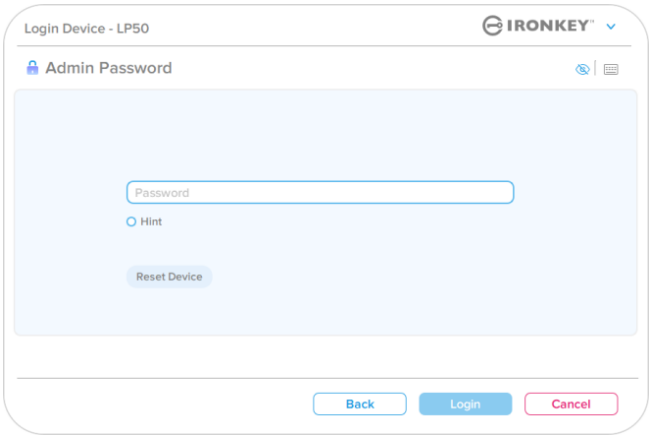


Figure 6.2 - Admin Password Login

Login for User-Only Mode (Admin not Enabled)

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

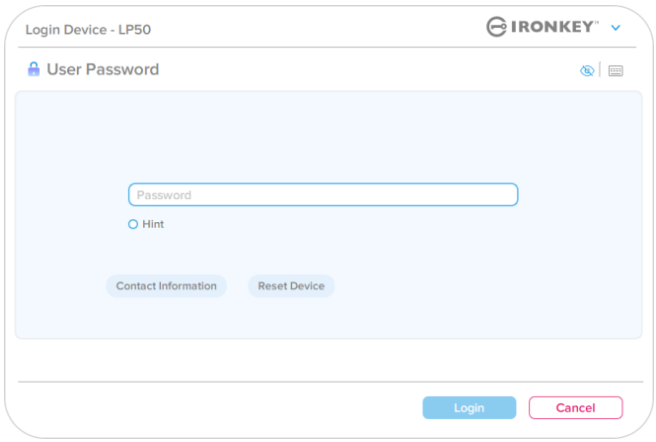


Figure 6.3 - User Password Login (Admin not enabled)

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 NOT Enabled)	**Brute Force protection Device Behavior (10 Incorrect Password attempts)**	**Data Erase and Device Reset?**
User Password	Crypto-Erase drive, Passwords, settings, and data erased forever	**YES**

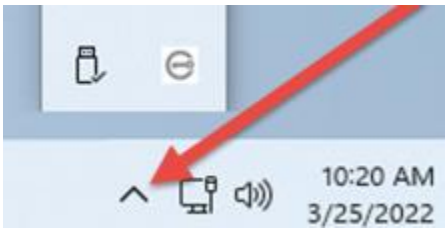
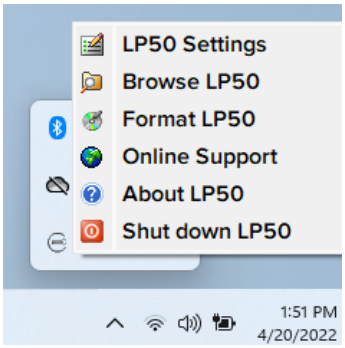
* Once you authenticate to the device successfully, the failed login counter will be reset in relation to which Login method was used. Crypto-Erase will delete all passwords, encryption keys and data – **your data will be lost forever.**

Accessing My Secure Files

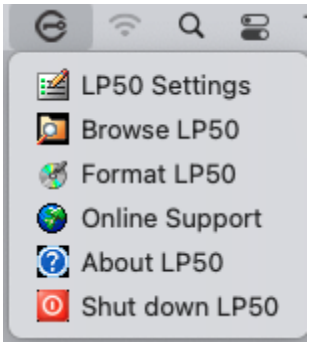
After unlocking the drive, you can access your secure files. Files are automatically encrypted and decrypted when you save or open them on the drive. This technology gives you the convenience of working as you normally would with a regular drive, while providing strong, "always-on" security.
Hint: You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

Device Options - (Windows Environment)

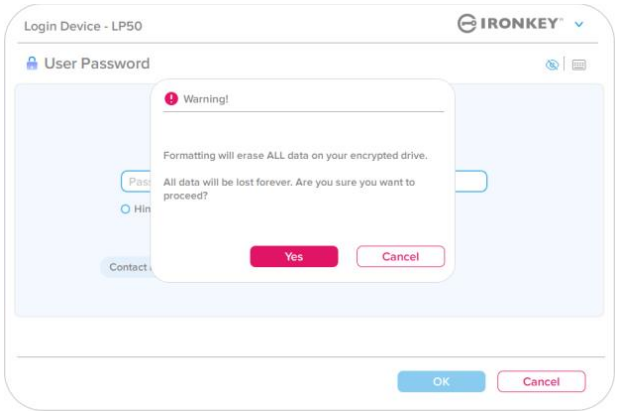
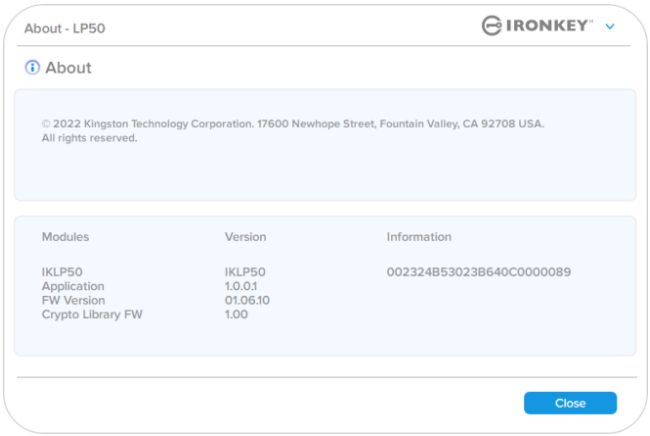
While you are logged into the device, there will be an IronKey Icon located in the right-hand corner the window. Right-clicking on the IronKey Icon will open the selection menu for available drive Options (*Figure 6.2*). Details about these device options can be found on Pages 19-23 of this manual

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

Device Options- (macOS Environment)

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

Device Options

LP50 Settings:	• Change login Password, Contact Information, and other settings. (More details about device settings can be found in the 'LP50 Settings' section of this manual).
Browse LP50:	• Allows you to view your secure files.
Format LP50: Allows you to format the secure data partition. (Warning: All data will be erased.) (*Figure 6.1*) **Note:** Password authentication will be required for format.	 **Figure 7.4- Format LP50**
Online Support:	• Opens your internet browser and navigates to http://www.kingston.com/support where you can access additional support information.
About LP50: Provides specific details about the LP50, including Application, Firmware and Serial number Information (*Figure 6.2*) **Note:** The unique serial number of the drive will be under the 'Information Column'	 **Figure 7.5- About LP50**
Shut down LP50:	• Properly shuts down the LP50, allowing you to safely remove it from your system.

LP50 Settings

Admin Settings

The Admin Login allows access to the following device settings:

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

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

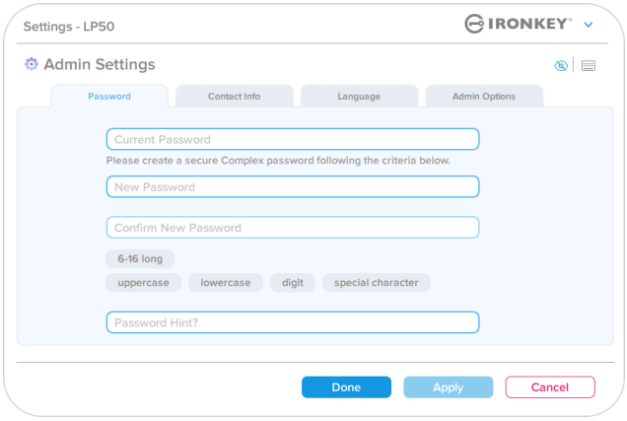


Figure 8.1 – Admin Password Options

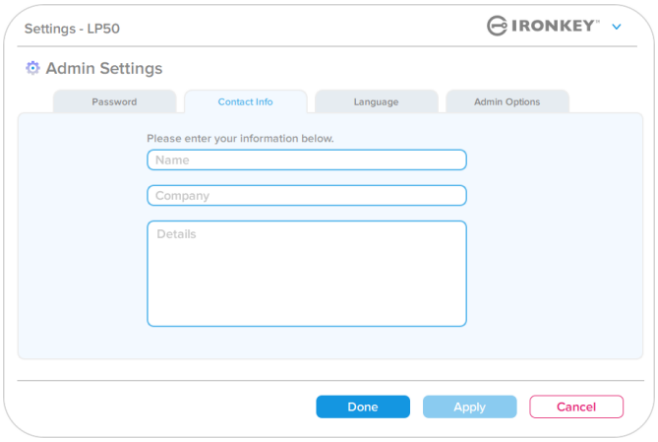


Figure 8.2- Contact Info

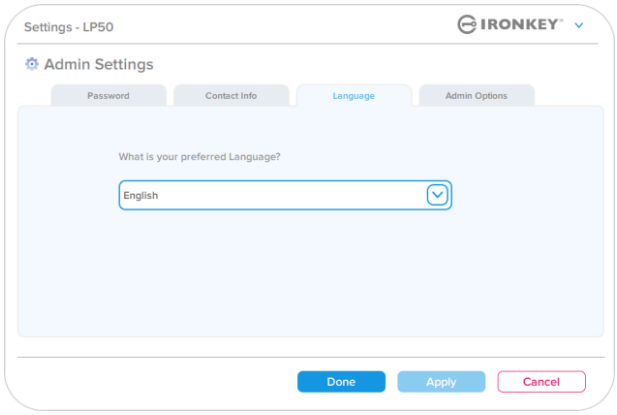


Figure 8.3 - Language Options

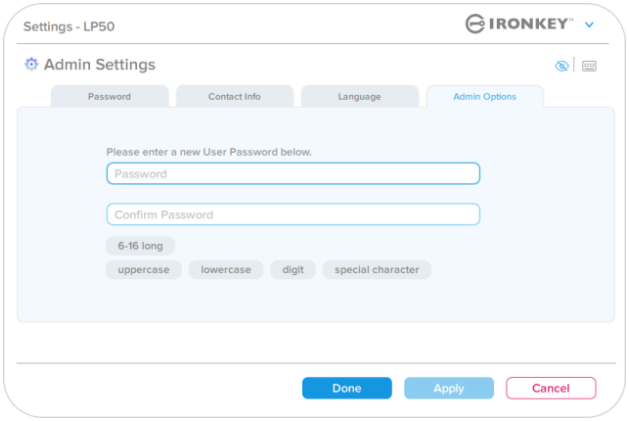
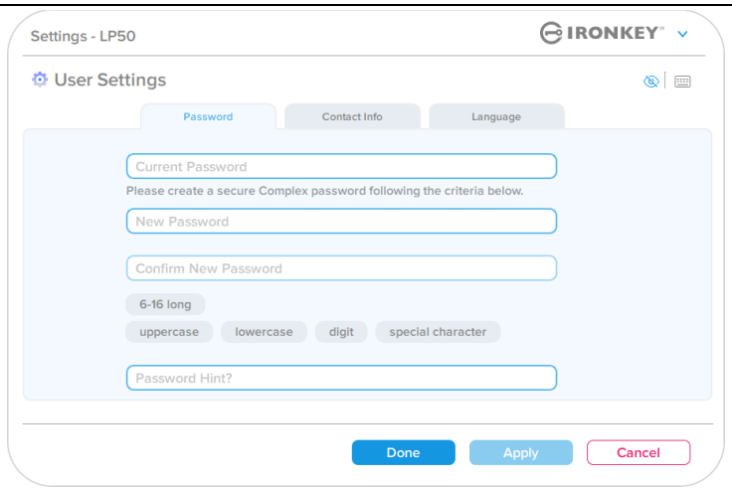
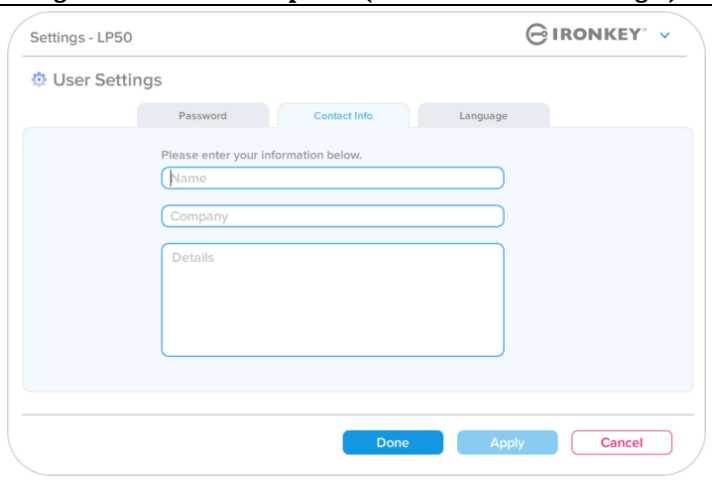
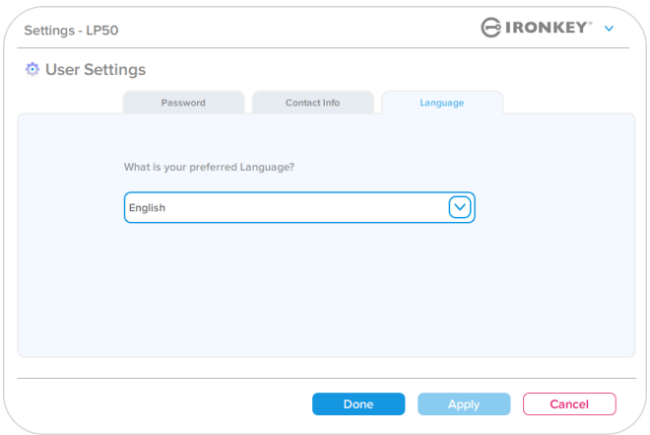


Figure 8.4- Admin Options

LP50 Settings

User Settings: Admin Enabled

The User Login limits access to the following settings:

Password: Allows you to change your own User password and/or hint. (*Figure 8.5*)	 **Figure 8.5- Password Options (Admin Enabled: User Login)**
Contact Info: Allows you to add/view/change your contact information. (*Figure 8.6*)	 **Figure 8.6- Contact Information (Admin Enabled: User Login)**
Language: Allows you to change your current language selection. (*Figure 8.7*)	 **Figure 8.7- Language Settings (Admin Enabled: User Login)**

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

LP50 Settings

User Settings: Admin Not Enabled

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

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

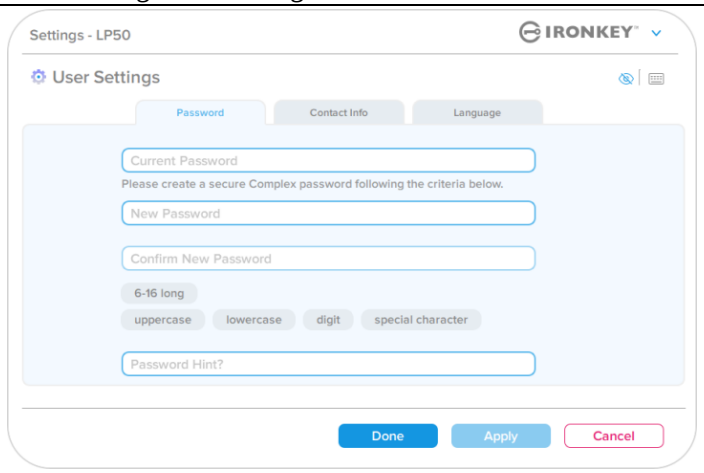


Figure 8.8- Password Options (User-Only Mode)

Contact Info:
Allows you to add/view/change your contact information. (*Figure 8.9*)

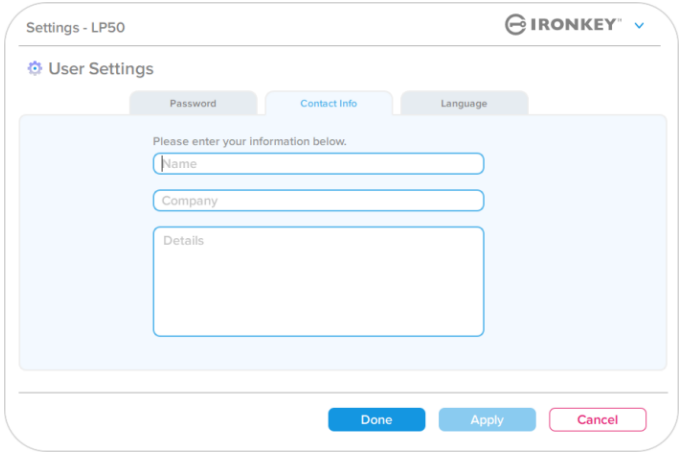


Figure 8.9- Contact Information (User-Only Mode)

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

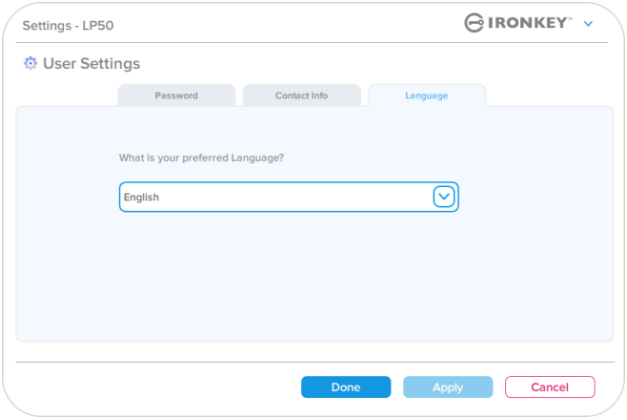


Figure 8.10- Language Settings (User-Only Mode)

LP50 Settings

Changing and Saving settings

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

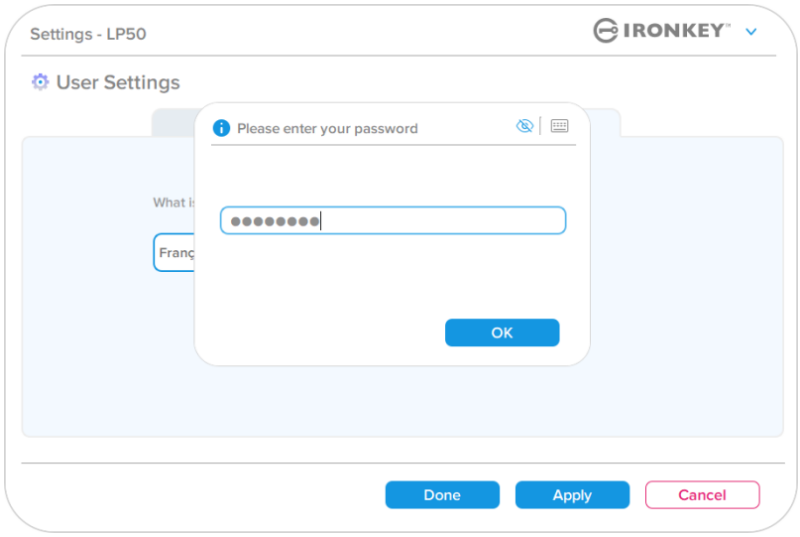


Figure 8.11- Password Prompt screen to save LP50 setting changes

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

Admin Features

Option Available to Reset the User Password

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

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

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

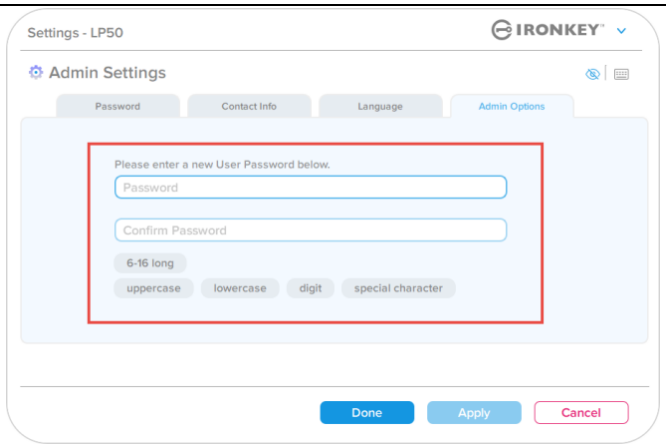


Figure 9.1- Admin Options/User Password Reset

Help and Troubleshooting

Device Lockout

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

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

1. A successful login prior to reaching MaxNoA

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

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

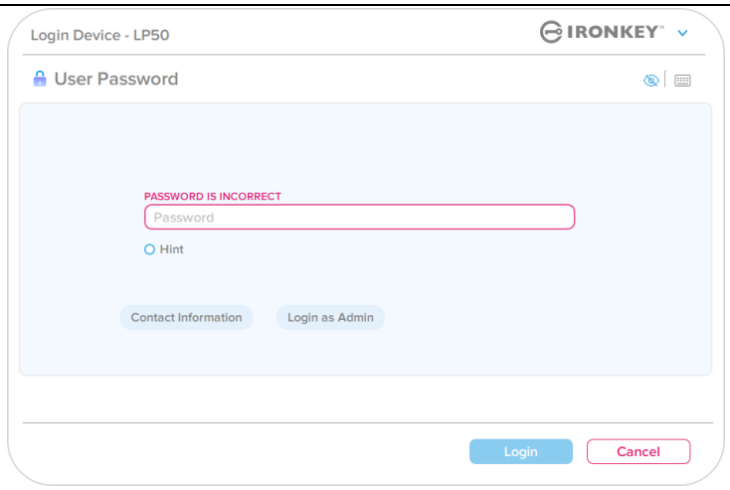


Figure 10.1- Incorrect Password message

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

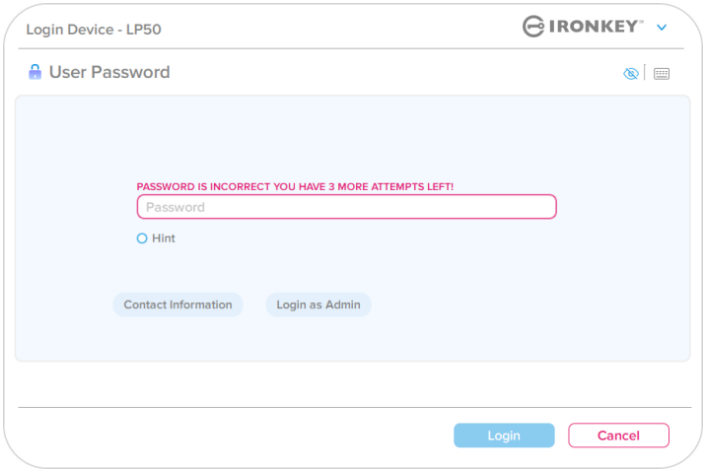


Figure 10.2- 7th incorrect Password attempt

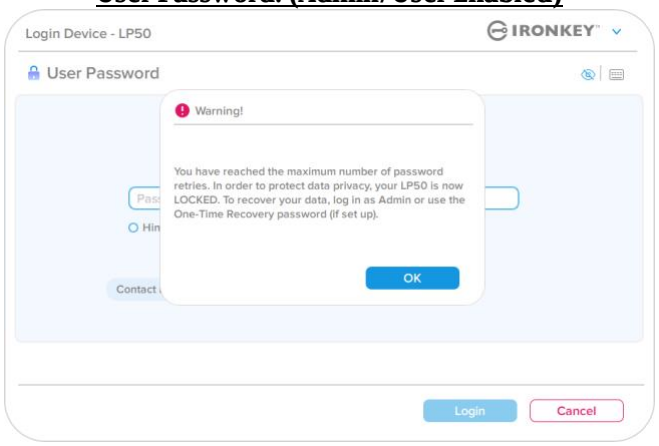
Help and Troubleshooting

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 18 of this User Guide.

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

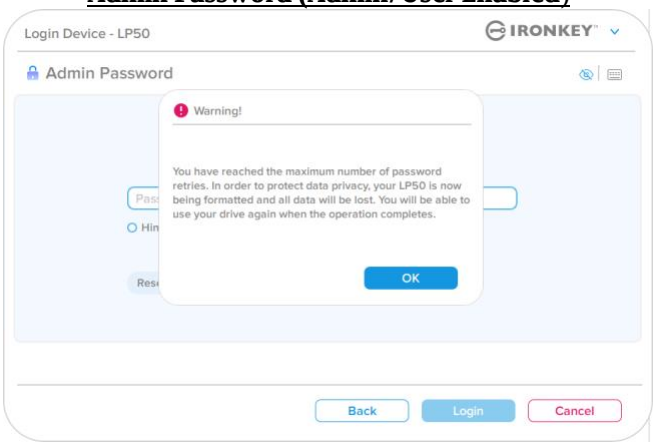
User Password: (Admin/User Enabled)



DEVICE LOCKOUT

Figure 10.3

Admin Password (Admin/User Enabled)

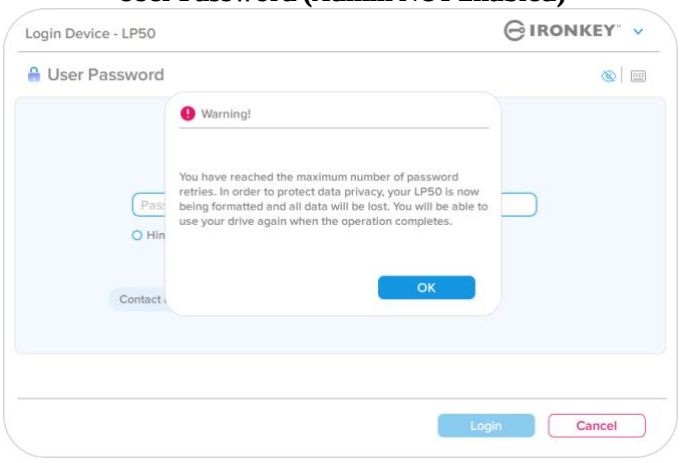


DEVICE FORMAT*

Figure 10.4

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

User Password (Admin NOT Enabled)



DEVICE FORMAT*

Figure 10.5

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

Help and Troubleshooting

Reset Device

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

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

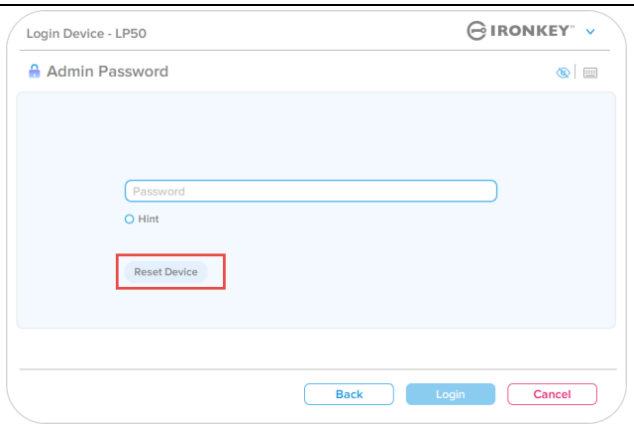


Figure 10.6- Admin Password: Reset Device Button

- **Note:** When you do click on '*Reset Device*', a message box will appear and ask if you want to enter a new password prior to executing the format. At this point, you can either 1) click '*OK*' to confirm or 2) click 'Cancel' to return to the login window. (*See figure 10.8*)

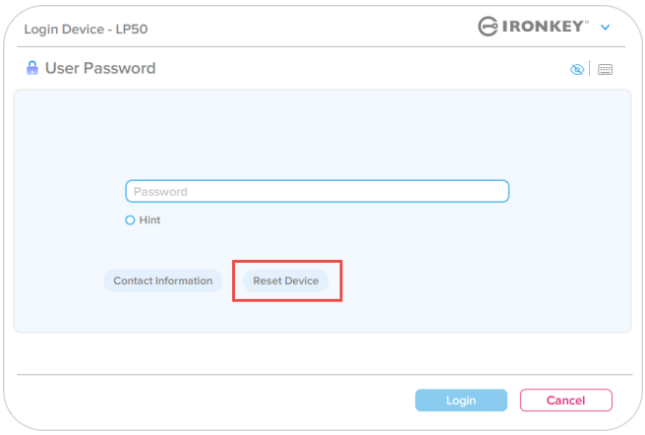


Figure 10.7- User Password (Admin/user not enabled) Reset Device

- 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.

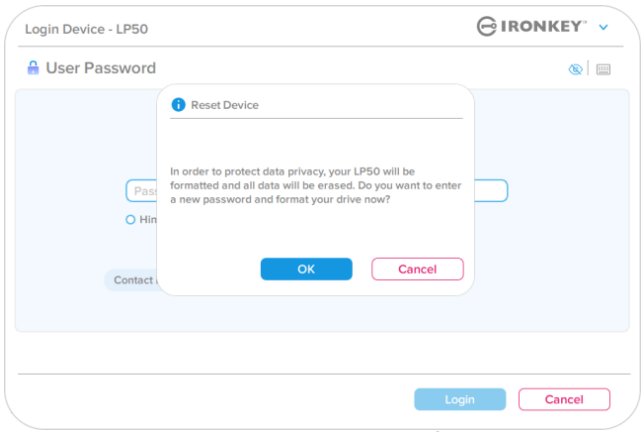


Figure 10.8- Reset device confirmation

Help and Troubleshooting

Drive Letter Conflict: Windows Operating Systems

- As mentioned in the '*System Requirements*' section of this manual (on page 3), the LP50 requires two consecutive drive letters AFTER the last physical disk that appears before the 'gap' in drive letter assignments (*see Figure 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 LP50 a drive letter that's already in use by a network share or Universal Naming Convention (UNC) path, causing a drive letter conflict. If this happens, please consult your administrator or helpdesk department on changing drive letter assignments in Windows Disk Management (administrator privileges required.)

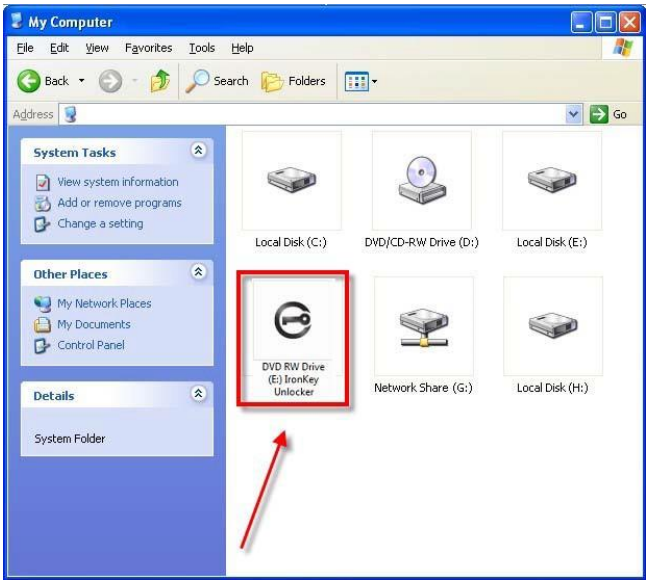


Figure 10.9- Drive Letter example

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

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

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

IRONKEY™ Locker+ 50 (LP50)
DISPOSITIVO SEGURO FLASH USB 3.2 GEN 1

Guía del usuario

Contenidos

Figura 1: IronKey LP50

Introducción

Las unidades flash USB IronKey Locker+ 50 de Kingston brindan seguridad de nivel de consumidor con cifrado basado en hardware AES en modo XTS, que incluye protecciones contra BadUSB con firmware firmado digitalmente y ataques de contraseña de fuerza bruta. El LP50 también cumple con TAA.

El LP50 ahora admite la opción de varias contraseñas (Administrador y Usuario) con los modos complejo o de frase de contraseña. El modo complejo tradicional permite contraseñas de 6 a 16 caracteres, con 3 de 4 conjuntos de caracteres. El nuevo 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 una 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 cifrado la unidad si la contraseña de administrador se introduce incorrectamente 10 veces consecutivas. Además, un teclado virtual incorporado protege las contraseñas contra el registro de teclas (keylogger) y el registro de pantalla (screenlogger).

El LP50 está diseñado para su comodidad con una pequeña carcasa de metal y un llavero integrado para llevar los datos a cualquier parte El LP50 también posee respaldo opcional de USBtoCloud (de ClevX®) para tener acceso a los datos del dispositivo desde su almacenamiento personal en la nube a través de Google Drive™, OneDrive (Microsoft®), Amazon Cloud Drive, Dropbox™ o Box. El LP50 es fácil de configurar y usar, ya que no es necesario instalar ninguna aplicación; todo el software y la seguridad que necesita ya están en la unidad. Funciona tanto en Windows® como en macOS®, por lo que los usuarios pueden acceder a archivos desde varios sistemas.

El LP50 está respaldado por una garantía limitada de 5 años con soporte técnico gratuito de Kingston.

Características del IronKey Locker+ 50

- Encriptado por hardware XTS-AES (El encriptado no se puede desactivar.)
- Protección contra ataques de Fuerza bruta y BadUSB
- Opciones de Múltiples contraseñas
- Modos de contraseña Complejo o de Frase de contraseña
- Botón de ojo para mostrar las contraseñas introducidas, y así reducir los intentos de inicio de sesión fallidos
- Teclado virtual para ayudar a proteger contra keyloggers y screenloggers
- Compatible con Windows o macOS (consulte la hoja de datos para obtener más detalles)

Acerca de este Manual (09242024)
Este manual del usuario se refiere al IronKey Locker+ 50 (LP50).

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:** Ver ‘‘Conflicto de letras de unidad’ en la página 32.	**Soporte del sistema operativo de la PC** • Windows 11 • Windows 10
Plataforma Mac • Intel y Apple SOC • Espacio libre en disco de 15 MB • Port USB 2.0 - 3.2	**Compatible con el sistema operativo Mac** • macOS 12.x – 15.x

Nota: Se incluye una suscripción gratuita de 5 años a USB-to-Cloud con cada unidad al momento de la activación. Opciones de activación continua disponibles para la compra por parte de ClevX más allá del plazo incluido.

Recomendaciones

Para asegurarse que disponga de la conexión de energía adecuada para el dispositivo LP50, insértelo directamente en un puerto USB de su portátil o computadora de escritorio, como se ve en la *Figura 1.1*. Evite conectar el LP50 a dispositivo(s) periférico(s) que pueda contar con un puerto USB, tal como un teclado o un concentrador alimentado vía USB, como se ve en la *Figura 1.2*.

Figura 1.1 - Uso recomendado

Figura 1.2 - No recomendado

Uso del sistema de archivos correcto
El IronKey LP50 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 volver a formatear la partición de datos si es necesario, pero los datos se pierden cuando se vuelve a formatear el dispositivo.

Recordatorios de uso
Para mantener sus datos seguros, Kingston recomienda que:

- Realice un análisis de virus en su computadora antes de configurar y usar el LP50 en un sistema de destino
- Bloquee el dispositivo cuando no esté en uso
- Expulse el dispositivo antes de desenchufarlo
- Nunca desenchufe el dispositivo cuando el LED esté encendido. Esto puede dañar el dispositivo y requerir que vuelva a formatear, lo que borrará sus datos
- Nunca comparta la contraseña de su dispositivo con nadie

Encuentre las últimas actualizaciones e información

Vaya a kingston.com/support para obtener las últimas actualizaciones del dispositivo, preguntas frecuentes, documentación e información adicional.

NOTA: Solo se deben aplicar sobre dispositivo las últimas actualizaciones del dispositivo (cuando estén disponibles). No se admite la reducción del dispositivo a una versión de software anterior, ya que esto puede causar una pérdida de datos almacenados o afectar a otras funciones del dispositivo Comuníquese con el Soporte técnico de Kingston si tiene preguntas o problemas.

Mejores prácticas para la configuración de contraseñas
Su LP50 viene con fuertes contramedidas de seguridad. Esto incluye la protección contra ataques de fuerza bruta que impedirán que un atacante adivine contraseñas al limitar cada intento de contraseña a 10 reintentos. Cuando se alcanza el límite del dispositivo, el LP50 eliminará automáticamente los datos encriptados, volviendo a formatearse a sí mismo al estado de fábrica.

Múltiples contraseñas
El LP50 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 LP50 puede admitir dos contraseñas diferentes que puede usar para recuperar datos, funciones de contraseña de administrador y usuario.

El LP50 le permite seleccionar dos contraseñas principales, una Contraseña de administrador (conocida como Contraseña de Admin) y una Contraseña de usuario. El administrador puede acceder al dispositivo en cualquier momento y configurar las opciones para Usuario – Administrador es como un Súper Usuario.

El Usuario también puede acceder al dispositivo, pero en comparación con el Administrador tiene privilegios limitados. Si una de las dos contraseñas se olvida, la otra contraseña se puede utilizar para acceder y recuperar los datos. El dispositivo se puede configurar de nuevo para tener dos contraseñas. Es importante configurar AMBAS contraseñas y guardar la Contraseña de administrador en un lugar seguro mientras usa la Contraseña de usuario.

Si todas las contraseñas se olvidan o se pierden, no hay otra manera de acceder a los datos. Kingston no podrá recuperar los datos ya que la seguridad no tiene puertas traseras. Kingston recomienda que los datos también se guarden en otros medios. El LP50 se puede restablecer y reutilizar, pero los datos previos se borrarán para siempre.

Modos de contraseña
El LP50 también admite dos modos de contraseña diferentes:

Complejo
Una contraseña compleja requiere cumplir 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 LP50 admite frases de contraseña de 10 a 64 caracteres. Una Frase de contraseña no sigue ninguna regla, pero si se usa correctamente, puede proporcionar niveles muy altos de protección con contraseña.

Una Frase de contraseña es básicamente cualquier combinación de caracteres, incluidos los caracteres de otros idiomas. Al igual que la unidad LP50, el idioma de la contraseña puede coincidir con el idioma seleccionado para el dispositivo. Esto le permite seleccionar varias palabras, una frase, letras 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 las más fáciles de recordar para los usuarios.

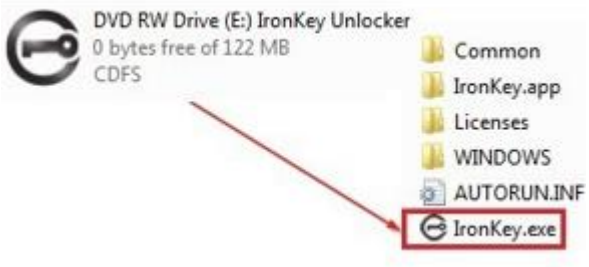
Configurar mi dispositivo

Para asegurarse de que haya suficiente energía disponible para el dispositivo USB encriptado IronKey, insértela directamente en un puerto USB 2.0/3.0 en 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 a dispositivos (Entorno Windows)

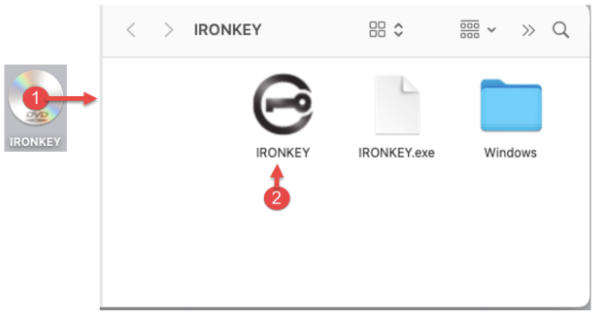
Conecte la unidad USB encriptada IronKey a un puerto USB disponible en el portátil o computadora y espere a que Windows la detecte.

• Windows 8.1/10/11 los usuarios recibirán una notificación del controlador del dispositivo. (*Figura 3.1*)	 **Figura 3.1 – Notificación del controlador del dispositivo**

• Una vez que se complete la nueva detección de hardware, 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 libre de la unidad. La letra de la unidad puede cambiar dependiendo de qué dispositivos estén conectados. En la imagen a continuación, la letra de la unidad es (E:).	 **Figura 3.2 – File Explorer Window/IronKey.exe**

Acceso a dispositivos (Entorno macOS)

Inserte el LP50 en un puerto USB disponible en su portátil o computadora de escritorio, y espere a que el sistema operativo Mac lo detecte. Cuando lo haga, verá que aparece el volumen 'IRONKEY en el escritorio. (*Figura 3.3*)

• Haga doble clic en el ícono del CD-ROM de 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 IKLP**

Inicialización del dispositivo (entorno Windows y macOS)

Idioma y CLUF

- Seleccione su idioma en el menú desplegable y haga clic en **Siguiente** (Next)(*Figura 4.1*).

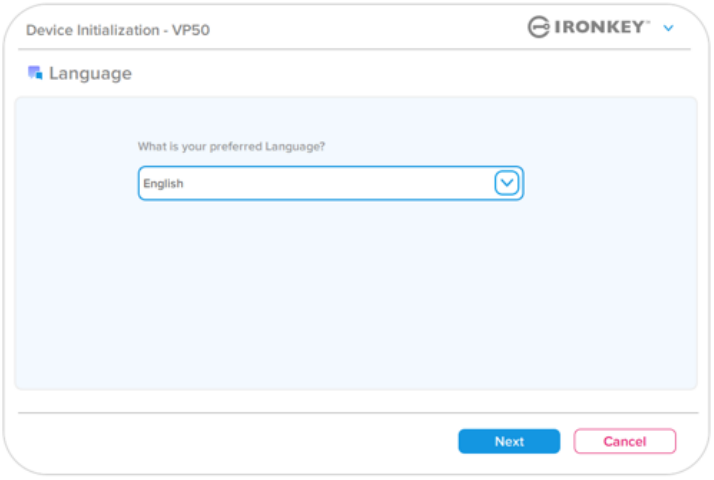


Figura 4.1 – Selección de idioma

- Revise el acuerdo de licencia y haga clic en **Siguiente** (Next).

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

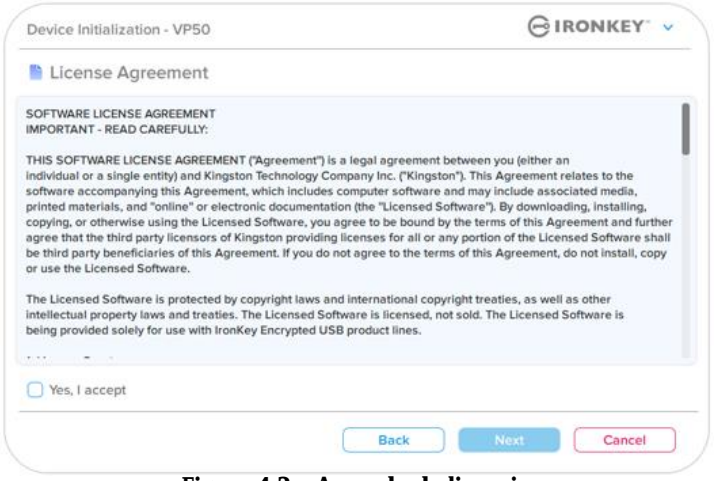


Figura 4.2 – Acuerdo de licencia

Inicialización del dispositivo

Selección de contraseña

En la pantalla de solicitud de contraseña, podrá crear una contraseña para proteger sus datos en el LP50 utilizando los modos de contraseña Complejo o Frase de contraseña (*Figuras 4.3- 4.4*). Además, las opciones de Usuario/Administrador de Múltiples contraseñas también se pueden habilitar en esta pantalla. Antes de proceder con la selección de contraseñas, revise la habilitación de Contraseñas de administrador/usuario a continuación para comprender mejor estas características.

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 vuelva a introducirla en los campos ‘‘Confirmar contraseña’. La contraseña que usted cree debe cumplir con los siguientes criterios antes que el proceso de inicialización le permita continuar:

Uso obligatorio del modo Complejo (Complex)

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

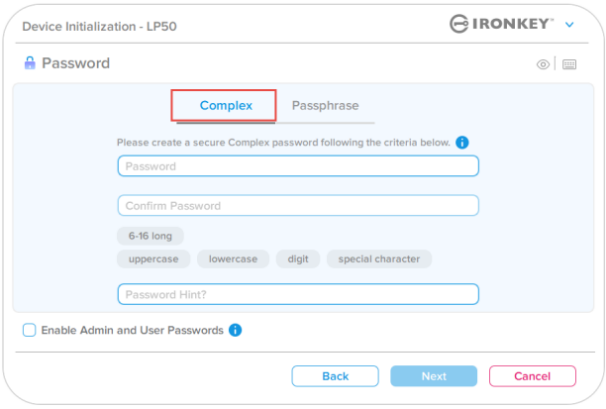


Figura 4.3 – Contraseña compleja

Frase de contraseña (Passphrase)

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

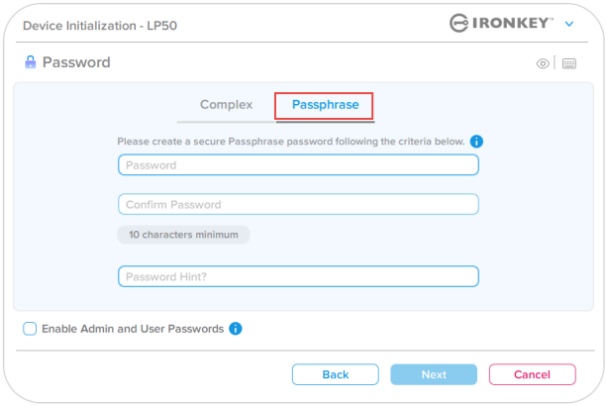


Figura 4.4 – Frase de contraseña

Pista para recordar la contraseña (Password Hint) (Opcional)

Una pista de contraseña puede ser útil para proporcionar una sugerencia sobre cuál es la contraseña, en caso de que la contraseña se olvide.
Nota: La pista NO PUEDE coincidir exactamente con la contraseña.

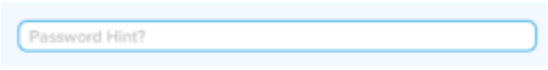


Figura 4.5 - Campo de pista para recordar contraseña

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, indicando que este criterio ahora es opcional (*Figura 4.6b*)

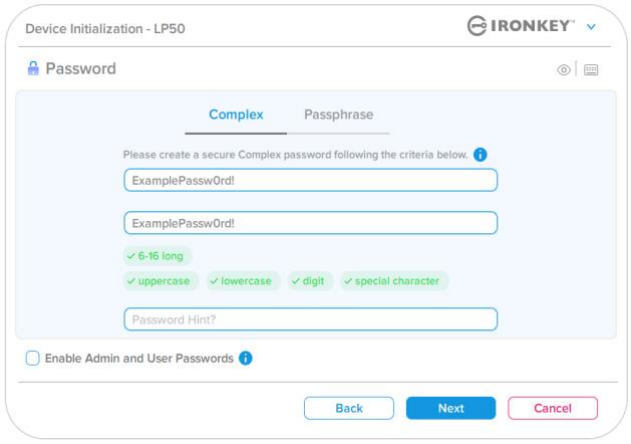


Figura 4.6a – Condición de contraseña compleja cumplida

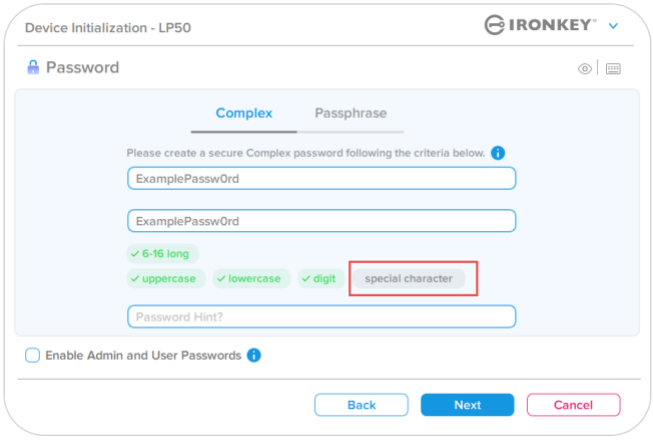


Figura 4.6b – Condición de contraseña compleja opcional

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

Esto aplica tanto para las Contraseñas complejas como para las Contraseñas de frase de acceso.

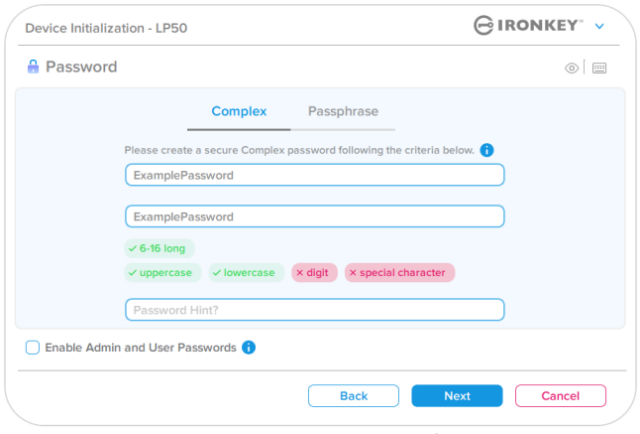


Figura 4.7 – Condiciones de contraseña no cumplidas

Inicialización del dispositivo

Teclado virtual
El LP50 cuenta con un Teclado virtual que puede ser utilizado para la protección contra Keylogger.

- Para utilizar el **Teclado virtual**, ubique el botón del teclado en la parte superior derecha de la pantalla de **Inicialización del dispositivo** (Device Initialization) y selecciónelo.

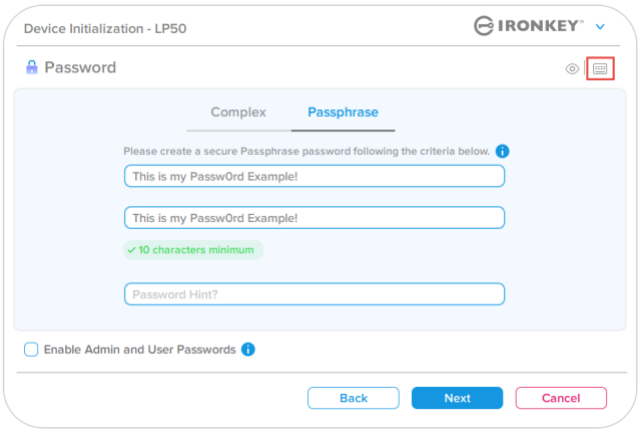


Figura 4.8 – Activación del Teclado virtual

- Una vez que aparezca el teclado virtual, también puede habilitar la **Protección contra screenlogger** (Screenlogger Protection). Cuando se utiliza esta función, todas las teclas quedarán brevemente en blanco. Este es un comportamiento esperado, ya que evita que los screenloggers capturen las teclas en las que ha hecho clic.

- Para que esta función sea más robusta, también puede optar por aleatorizar el teclado virtual seleccionando **aleatorizar** (randomize) en la parte inferior derecha del teclado. Aleatorizar organizará el teclado en un orden aleatorio.

Figura 4.9 – Protección/aleatorización contra Screenlogger

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 a medida que 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 pasará a ‘oculto’ de forma predeterminada.

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

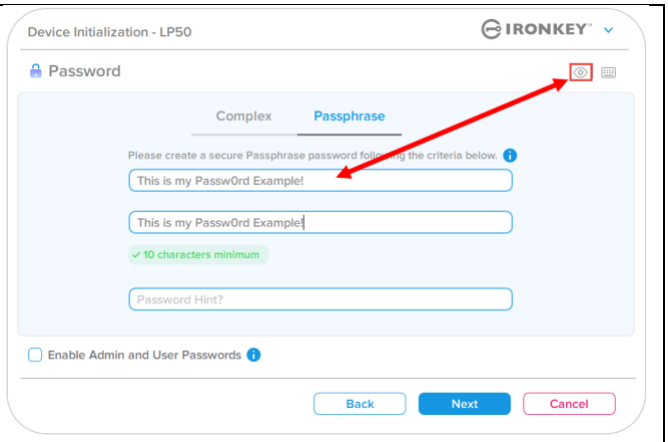


Figura 4.10 – Active ‘ocultar’ Contraseña

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

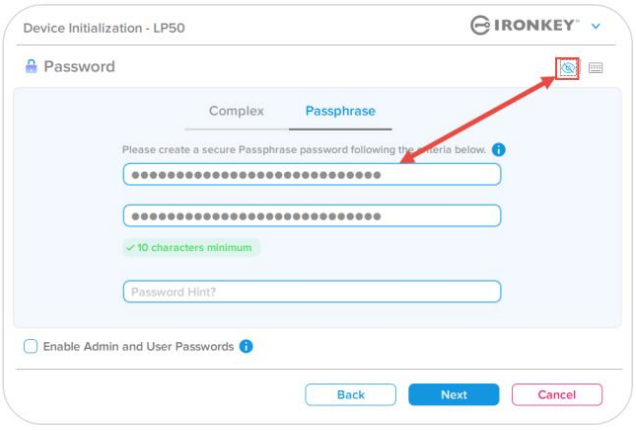


Figura 4.11 – Active ‘mostrar’ Contraseña

Inicialización del dispositivo

Contraseñas de administrador y usuario

Al habilitar las Contraseñas de administrador y usuario, puede aprovechar la funcionalidad de múltiples contraseñas, en la que el Rol de administrador puede administrar ambas cuentas. La selección de **'Habilitar contraseñas de administrador y usuario'** permite un método alternativo de acceso al dispositivo en caso de que se olvide una de las contraseñas.

Con las **Contraseñas de administrador y usuario** habilitadas, también puede acceder a:

- Restablecer la contraseña de usuario

Para obtener más información sobre la función de restablecimiento de la contraseña de usuario, vaya a la página 28 de esta guía del usuario.

- Para habilitar **las contraseñas de administrador y usuario**, haga clic en la casilla junto a '**Habilitar contraseñas de administrador y usuario**' (Enable Admin and User Passwords) y seleccione **Siguiente** (Next) 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** (Next) para pasar a la pantalla **Contraseña de usuario**, donde se elige una contraseña para el usuario.

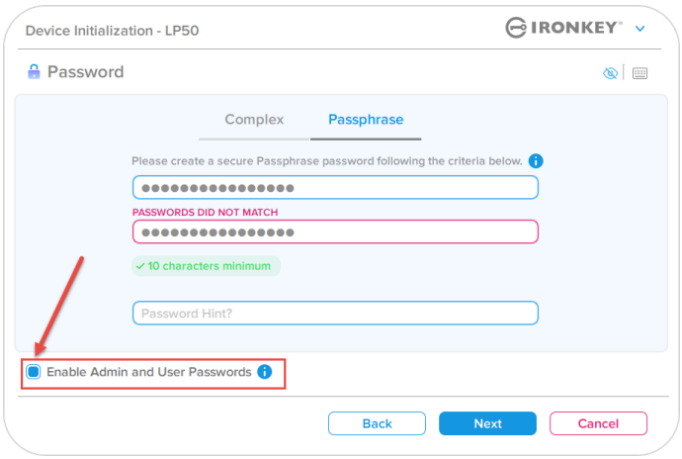


Figura 4.12 – Habilitación de Contraseñas de administrador y usuario

Nota: Habilitar las Contraseñas de administrador y usuario es opcional.

Si el dispositivo está configurado con esta función NO habilitada (casilla desmarcada), entonces el dispositivo se configurará como un dispositivo de **Usuario único, Contraseña única, sin ninguna función de Administrador.** Esta configuración se referirá como **Modo de solo usuario** a lo largo de este manual.

Para continuar con la configuración de Usuario único, Contraseña única, mantenga **Habilitar contraseñas de administrador y usuario** desmarcada 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, en la siguiente pantalla se le pedirá **la Contraseña de usuario** (User Password)(*Figura 4.13*). La Contraseña de usuario tendrá capacidades limitadas en comparación con la de Administrador esto se analizará con más detalle más adelante en esta Guía del usuario. **Nota: 'Las Contraseñas de administrador y usuario**' se denominarán como **'Rol de administrador'** a lo largo de este manual por el resto de este documento.

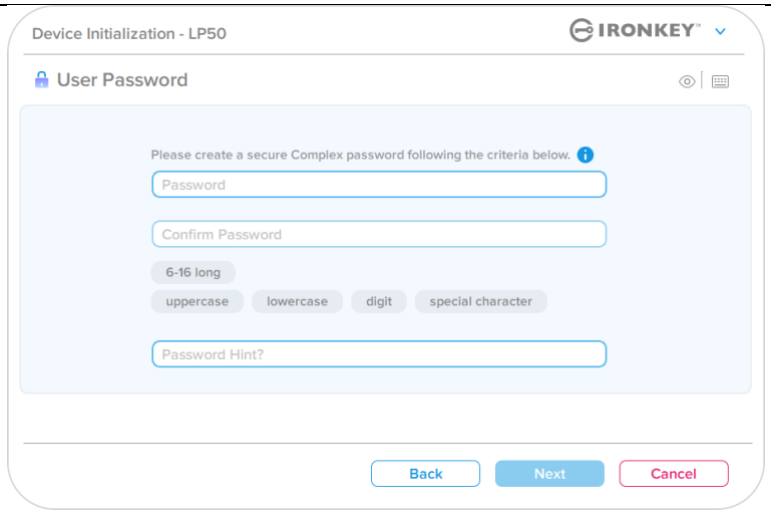


Figura 4.13 - Contraseña de usuario (administrador y usuario habilitado)

Nota: Los criterios de Opción de contraseña elegidos (Complejo o Frase de acceso) se transferirán a la Contraseña de usuario, y a cualquier restablecimiento de contraseña que se necesite después de configurar el dispositivo. 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 previstos (*ver la Figura 4.14*)

Nota: La información que usted ingrese en estos campos NO puede contener la cadena de la contraseña que creó en el Paso 3. Sin embargo, estos campos son opcionales y pueden dejarse en blanco, si así se desea.

El campo **'Nombre'** (Name) puede contener hasta 32 caracteres, pero no puede contener la contraseña **exacta**.

El campo **'Compañía'** (Company) puede contener hasta 32 caracteres, pero no puede contener la contraseña **exacta**.

El campo **'Detalles'** (Details) puede contener hasta 156 caracteres, pero no puede contener la contraseña **exacta**.

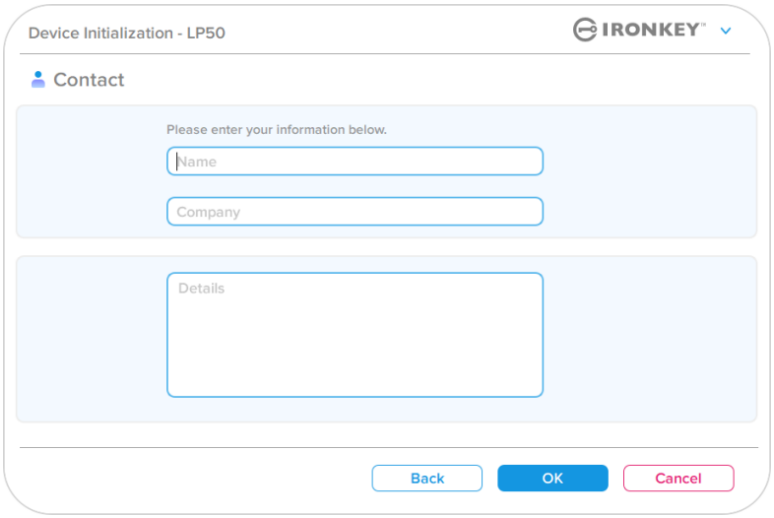


Figura 4.14 - Información de contacto

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 el dispositivo y vuelva a enchufarlo al sistema para ver los cambios reflejados.

USB ß → Inicialización en la nube (entorno Windows)

Una vez que se haya inicializado el dispositivo en Windows, aparecerá la aplicación USB-to-Cloud como se ve en la *Figura 5.1* a la derecha. Por favor asegúrese que dispone de una conexión a Internet establecida antes de continuar.

- Para proceder con la instalación, haga clic en el botón verde 'Aceptar' (Accept) en la esquina inferior derecha de la ventana de ClevX
- Para rechazar la instalación, haga clic en el botón rojo 'Rechazar' (Decline) en la esquina inferior izquierda de la ventana de ClevX.
- (Nota: Si hace clic en el botón rojo 'Rechazar', cancelará la instalación de USB-to-Cloud. Al hacer esto, se crea un archivo de texto especial llamado 'USBtoCloudInstallDeclined.txt' en la partición de datos. La presencia de este archivo evitará que la aplicación le solicite la instalación en el futuro).

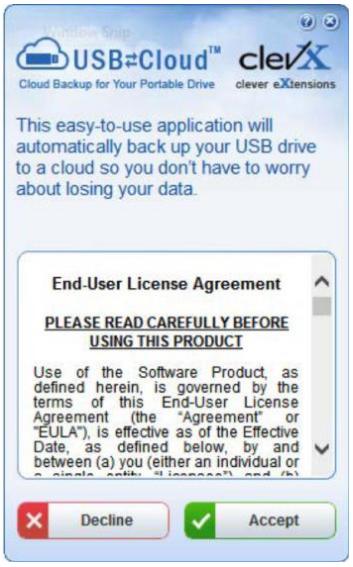


Figura 5.1 – CLUF USBtoCloud Windows

- Si la siguiente ventana de Alerta de seguridad de Windows aparece durante el proceso de inicialización, por favor haga clic en "Permitir acceso" para continuar (o cree una excepción de Firewall de Windows) así la aplicación USB-to-Cloud puede continuar.

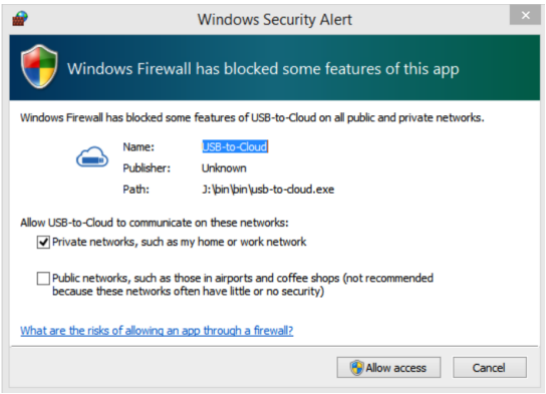


Figura 5.2 – Alerta de seguridad de Windows

USB ß → Inicialización en la nube (entorno Windows)

- Una vez completada la instalación, aparecerá un cuadro de aplicación con una lista de opciones a elegir (para sincronizar sus datos del LP50).
- Seleccione la opción de nube que desea usar como su aplicación de copia de seguridad, y proporcione las credenciales necesarias para la autenticación.
- (Nota: Si actualmente no tiene una cuenta configurada con cualquiera de las opciones que figuran en la Nube, puede crear una en este momento a través de su navegador de Internet favorito, y completar esta opción posteriormente).
- Una vez que haya elegido una opción de Nube y se haya autentificado para el servicio correspondiente, el programa USB-to-Cloud llevará a cabo una comparación inicial de la partición de datos contra lo que está almacenado en la Nube. Mientras que el servicio USB-to-Cloud se esté ejecutando en el Administrador de tareas, el contenido escrito en la partición de datos se respaldará (sincronizará) automáticamente en la nube.

Figura 5.3 – Selección de Nube

USB ß → Uso de la nube (entorno Windows)

La aplicación USB-a-Cloud proporciona los siguientes servicios adicionales:

- Pausar copia de seguridad (Pausa la copia de seguridad de datos).
- Restaurar (Restaura datos desde la nube al dispositivo).
- Ajustes (Opciones adicionales para su copia de seguridad).
- Salir (Sale del servicio USB-to-Cloud).

En el menú 'Ajustes, usted puede:

- Cambiar la aplicación de servicio en la nube que está utilizando actualmente para las copias de seguridad.
- Cambiar el idioma que está utilizando actualmente.
- Seleccionar qué archivos y/o carpetas está respaldando en la nube.
- Buscar actualizaciones de software.

(**Nota**: Si inicializa (o formatea) la unidad LP50, se perderán todos los datos en el dispositivo. Sin embargo, todos los datos que se almacenen en la Nube siguen estando seguros e intactos.)

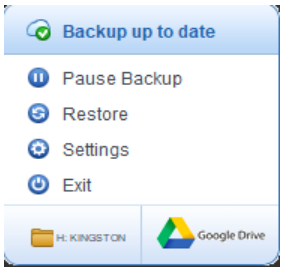


Figura 5.4 - Servicios

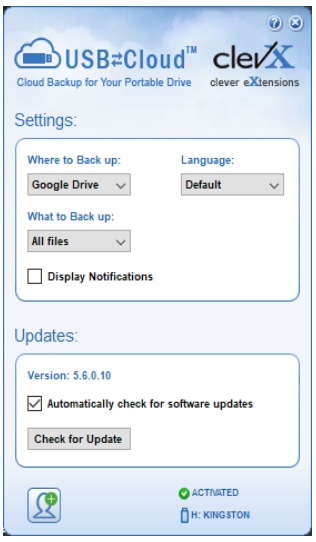


Figura 5.5 -Ajustes

USB ß → Inicialización en la nube (entorno macOS)

- Una vez que se haya inicializado el dispositivo aparecerá la aplicación USB-to-Cloud como se ve en la *Figura 5.6* a la derecha. Por favor asegúrese que dispone de una conexión a Internet establecida antes de continuar.
- Para proceder con la instalación, haga clic en el botón 'Aceptar' (Accept) en la esquina inferior derecha de la ventana de ClevX.

  (Nota: En macOS 12.x + se le solicitará que permita el acceso a los archivos en un volumen extraíble. Seleccione Aceptar.) (*Ver figura 5.7*)
- Para rechazar la instalación, haga clic en el botón 'Rechazar' (Decline) en la esquina inferior izquierda de la ventana de ClevX.

Figura 5.6 – CLUF USBtoCloud macOS

(Nota: Si hace clic en el botón 'Rechazar', cancelará la instalación de USB-to-Cloud. Al hacer esto, se crea un archivo de especial llamado 'DontInstallUSBtoCloud' en la partición de datos. La presencia de este archivo evitará que la aplicación le solicite la instalación en el future.)

- Una vez completada la instalación, aparecerá un cuadro de aplicación con una lista de opciones a elegir (para sincronizar sus datos del LP50). (*Figura 5.8*)

Figura 5.7- Acceso macOS

- Seleccione la opción de nube que desea usar como su aplicación de copia de seguridad, y proporcione las credenciales necesarias para la autenticación.

  (Nota: Si actualmente no tiene una cuenta configurada con cualquiera de las opciones que figuran en la Nube, puede crear una en este momento a través de su navegador de Internet favorito, y completar esta opción posteriormente).
- Una vez que haya elegido una opción de Nube y se haya autentificado para el servicio correspondiente, el programa USB-to-Cloud llevará a cabo una comparación inicial de la partición de datos contra lo que está almacenado en la Nube. Mientras que el servicio USB-to-Cloud se esté ejecutando en el Administrador de tareas, el contenido escrito en la partición de datos se respaldará (sincronizará) automáticamente en la nube.

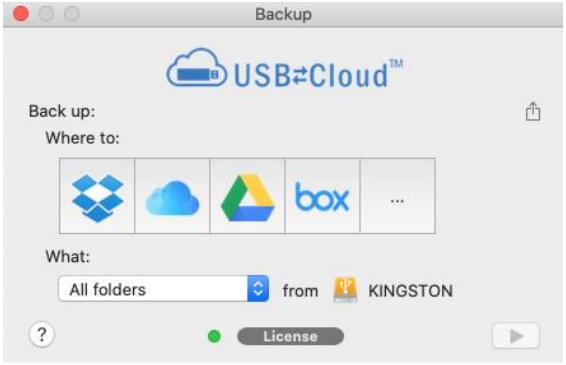


Figura 5.8 - Selección de Nube

USB ß →Uso de la nube (entorno macOS)

La aplicación USB-to-Cloud proporciona los siguientes servicios adicionales (*Figura 5.9*):

- **Pausar copia de seguridad** (Pausa la copia de seguridad de datos)
- **Restaurar** (Restaura datos desde la nube al dispositivo)
- **Copia de seguridad (**abre las opciones de la nube) *Vea figura 5.9*
- **Salir** (sale del servicio USB-to-Cloud)

Figura 5.9 - Servicios

En el menú 'Preferencias, usted puede:

- Cambiar el idioma que está utilizando actualmente
- Activar/desactivar notificaciones de sonido
- Activar/desactivar desmontar la unidad si se cierra la aplicación
- Activar/desactivar el registro para la solución de problemas
- Activar/desactivar las actualizaciones automáticas de software y la búsqueda de actualizaciones

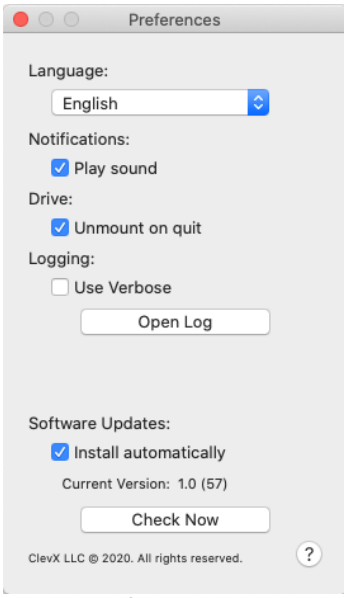


Figura 5.10- Preferencias de USBtoCloud

Uso del dispositivo (entorno Windows y macOS)

Inicio de sesión para Administrador y Usuario (Administrador Habilitado)

Si el dispositivo se inicializa con las Contraseñas de administrador y usuario (Rol de administrador) habilitadas, se iniciará la aplicación IronKey LP50, mostrando primero la pantalla de inicio de sesión de 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 botón ‘‘Iniciar sesión como Administrador (Login as Admin) (que se muestra a continuación), la aplicación procederá al menú Inicio de sesión de administrador, donde puede iniciar sesión como Administrador para acceder a la configuración y las funciones de Administrador (*Figura 6.2*).

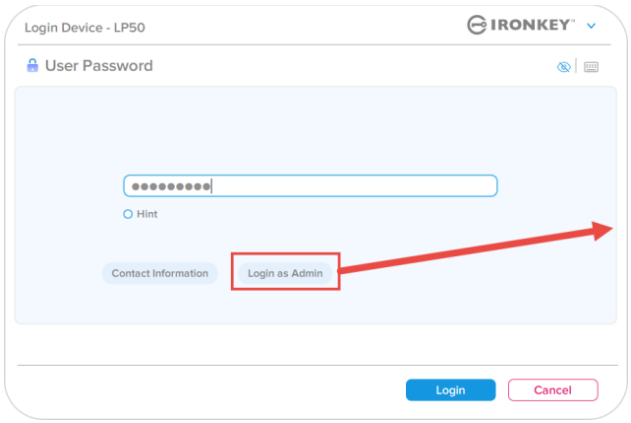


Figura 6.1 - Inicio de sesión con Contraseña de usuario (Administrador habilitado)

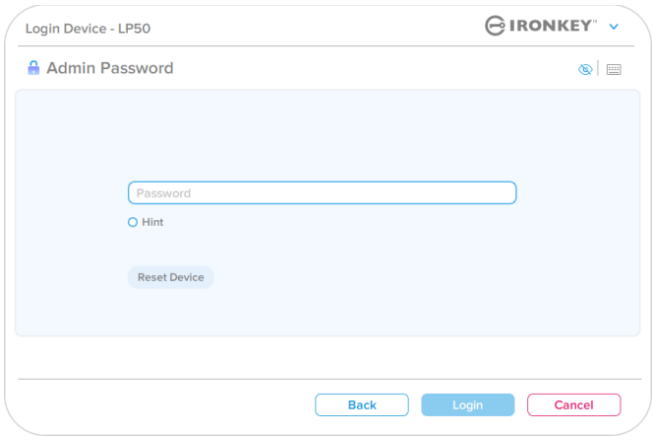


Figura 6.2 - Inicio de sesión con Contraseña de administrador

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

Como se mencionó anteriormente en la **página 13**, aunque se recomienda usar la funcionalidad de Rol de administrador 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 simple y de contraseña única para proteger los datos en su dispositivo. (*Figura 6.3*)

Nota: Para habilitar las Contraseñas de administrador y usuario, utilice el botón **Restablecer el dispositivo** (Reset Device) para volver a poner el dispositivo al estado de inicialización, donde puede habilitar las Contraseñas de administrador y usuario. **TODOS los datos del dispositivo se formatearán y perderán para siempre cuando se produzca un Restablecer el dispositivo.**

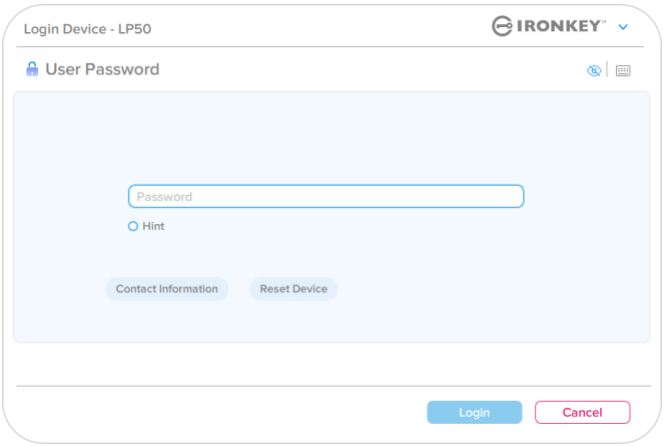


Figura 6.3 - Inicio de sesión con contraseña de usuario (el Administrador no está habilitado)

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 de contraseña fallidos, el comportamiento será el siguiente:

Administrador/usuario habilitado	**Protección contra ataques de fuerza bruta Comportamiento del dispositivo (10 intentos fallidos de ingreso de la contraseña)**	**¿Borrado de datos y reinicio del dispositivo?**
Contraseña de usuario:	Bloqueo de la contraseña. Inicie sesión como Administrador para restablecer la contraseña de usuario	NO
Contraseña de administrador	Dispositivo de borrado criptográfico, Contraseñas, configuraciones y datos borrados para siempre	**SÍ**
Solo usuario Usuario único, Contraseña única (Administrador/usuario NO habilitado)	**Protección contra ataques de fuerza bruta Comportamiento del dispositivo (10 intentos fallidos de ingreso de la contraseña)**	**¿Borrado de datos y reinicio del dispositivo?**
Contraseña de usuario	Dispositivo de borrado criptográfico, Contraseñas, configuraciones y datos borrados para siempre	**SÍ**

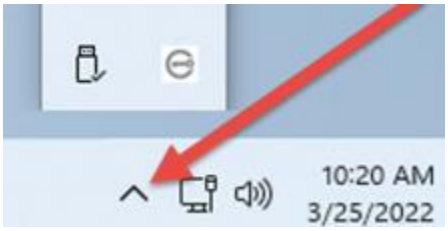
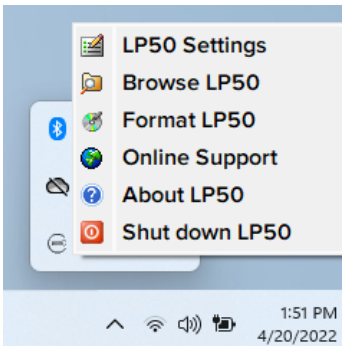
* Una vez que se autentique correctamente en el dispositivo, el contador de inicio de sesión fallido se restablecerá en relación con el método de inicio de sesión que se utilizó. Crypto-Erase eliminará todas las contraseñas, claves de encriptado y datos – **sus datos se perderán para siempre.**

Accesando a mis archivos seguros

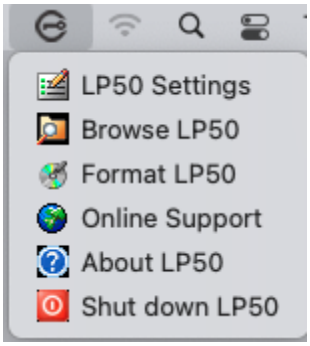
Después de desbloquear el dispositivo puede acceder a sus archivos seguros. Los archivos se cifran y descifran automáticamente cuando los guarda o los abre en el dispositivo. Esta tecnología le brinda la comodidad de trabajar como lo haría normalmente con un dispositivo regular, al tiempo que proporciona una seguridad sólida y "siempre activa".
Pista: También puede acceder a sus archivos haciendo clic con el botón derecho en el **icono de IronKey** en la barra de tareas de Windows y haciendo clic en **Examinar el LP50** (*Figure 7.2*)

Opciones del dispositivo - (Entorno Windows)

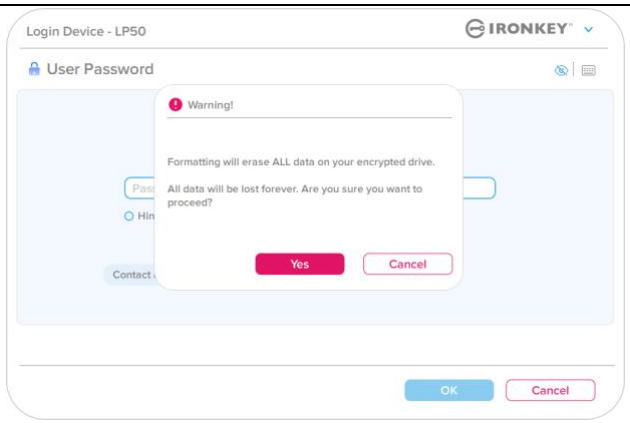
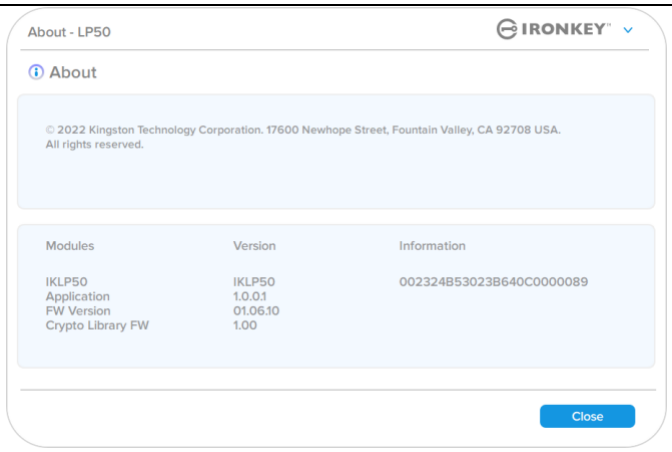
Mientras esté conectado al dispositivo, habrá un icono de IronKeyubicado en la esquina derecha de la ventana. Al hacer clic con el botón derecho en el icono de IronKey se abrirá el menú de selección para las Opciones disponibles del dispositivo (*Figura 6.2*).
Los detalles sobre estas opciones del dispositivo se pueden encontrar en las páginas 19-23 de este manual.

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

Opciones del dispositivo - (Entorno macOS)

• Mientras esté conectado al dispositivo, encontrará un icono 'IronKey LP50 ubicado en el menú macOS como 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 - Menú de opciones de Icono/Dispositivo de la barra de menú macOS**

Opciones de dispositivo

Configuración del LP50:	• Cambiar Contraseña de inicio de sesión, Información de contacto y otros ajustes. (Se pueden encontrar más detalles sobre la configuración del dispositivo en la sección 'Configuración del LP50 ' de este manual).
Explorar el LP50:	• Le permite ver sus archivos seguros.
Formatear el LP50: Le permite formatear la partición de datos segura. (Advertencia: Se borrarán todos los datos). (*Figura 6.1*) **Nota:** Se requerirá autentificación por contraseña para el proceso de reformateo.	 **Figura 7.4 - Reformateo del LP50**
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 LP50: Proporciona detalles específicos sobre el LP50, incluida la información de la aplicación, el firmware y el número de serie (*Figura 6.2*) **Nota:** El número de serie único del dispositivo estará debajo de la columna de 'información'	 **Figura 7.5 - Acerca del LP50**
Apagar el LP50:	• Apaga correctamente el LP50 lo cual le permite retirarlo de forma segura de su sistema.

Configuración del LP50

Configuración de administrador

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

- **Contraseña (Password):** Le permite cambiar su contraseña de administrador y/o pista (*Figura 8.1*)
- **Información de contacto (Contact Info):** Le permite agregar/visualizar/cambiar su información de contacto (*Figura 8.2*)
- **Idioma (Language):** Le permite cambiar su preferencia actual de idioma (*Figura 8.3*)
- **Opciones de administrador (Admin Options):** Le permite habilitar funciones adicionales como:
    - Cambiar la contraseña de usuario (*Figura 8.4*)

NOTA: Los detalles adicionales de las Opciones de administrador se pueden encontrar en la página 25.

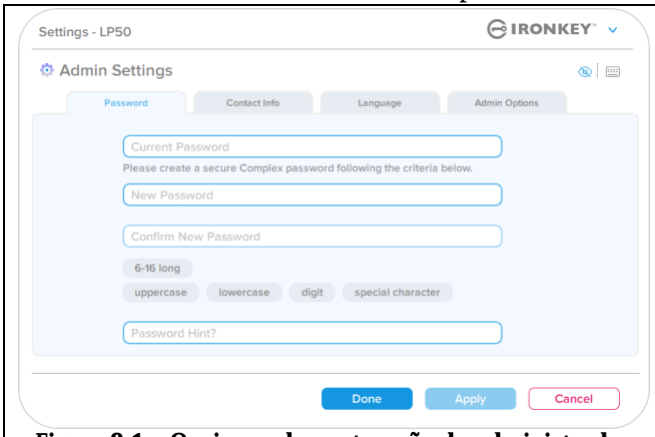


Figura 8.1 – Opciones de contraseña de administrador

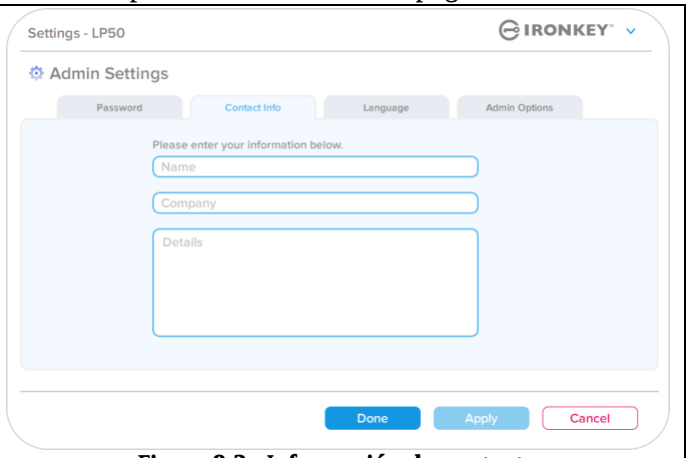


Figura 8.2 - Información de contacto

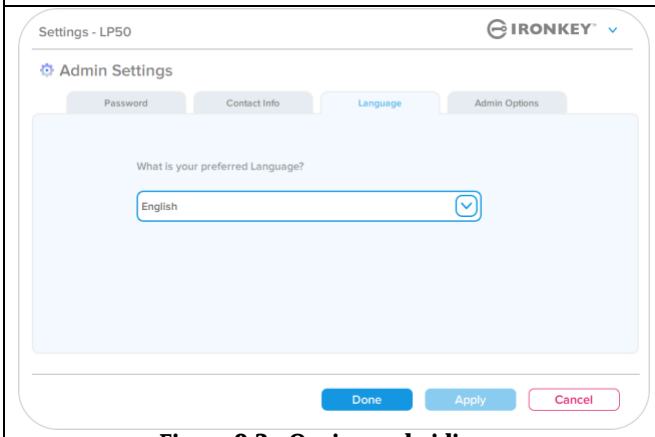


Figura 8.3 - Opciones de idioma

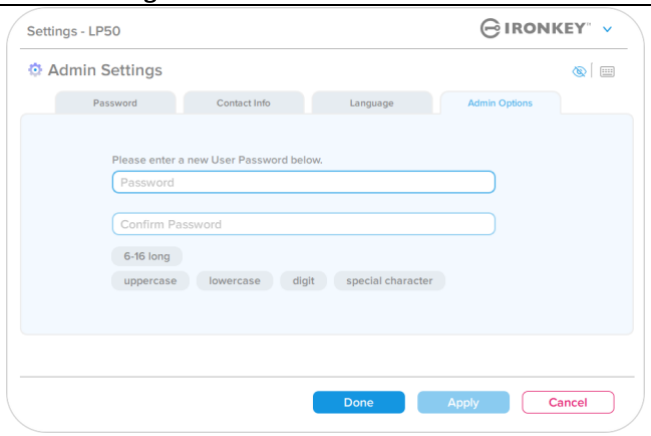
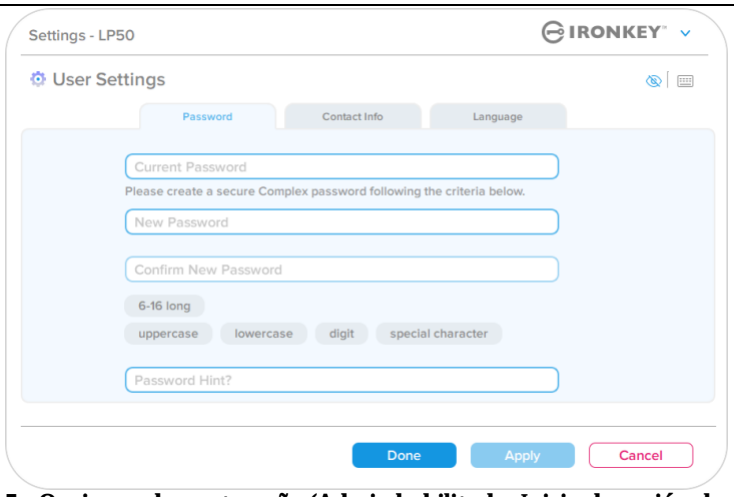
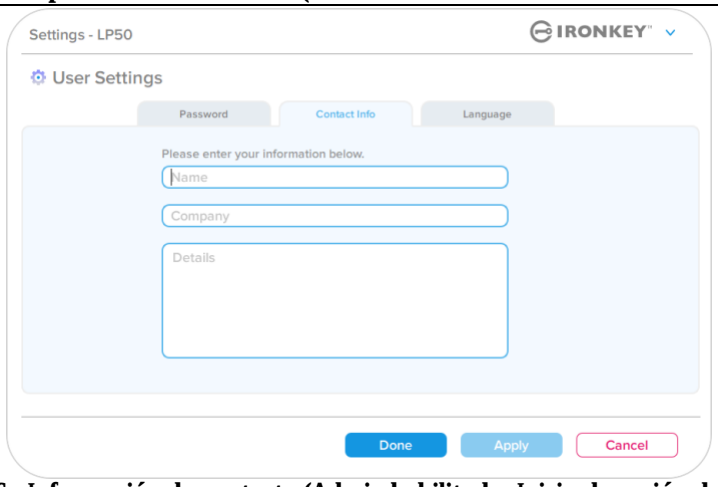
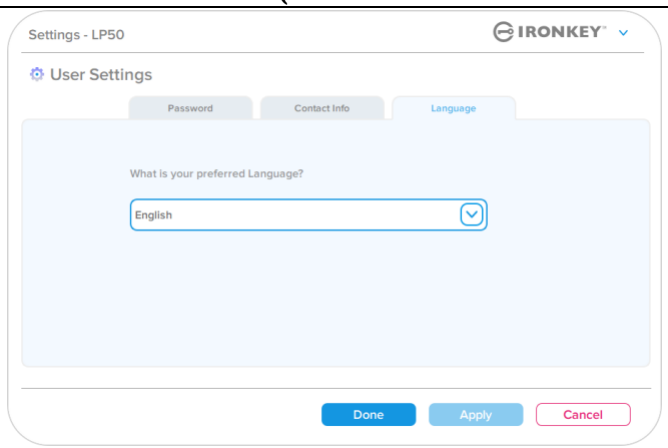


Figura 8.4 - Opciones de Administrador

Configuración del LP50

Configuración de usuario: Administrador habilitado

El Inicio de sesión de usuario limita el acceso a la siguiente configuración:

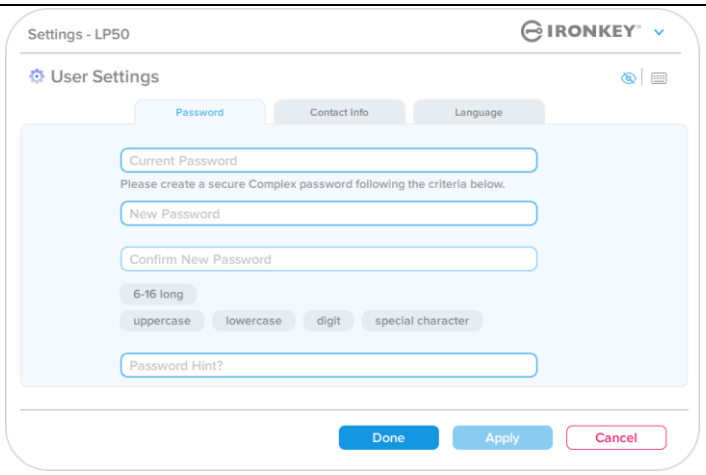
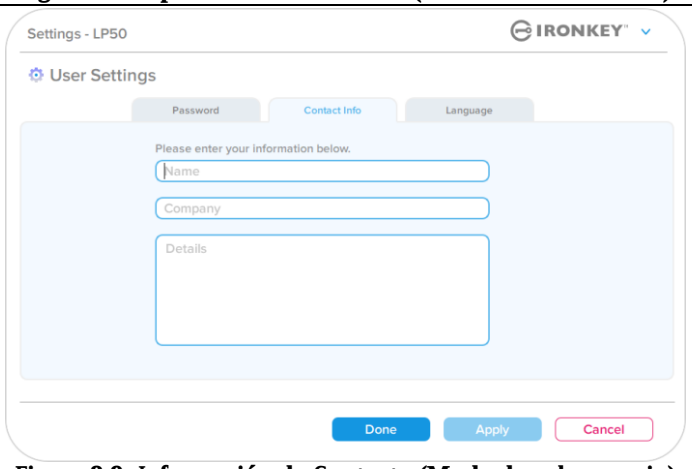
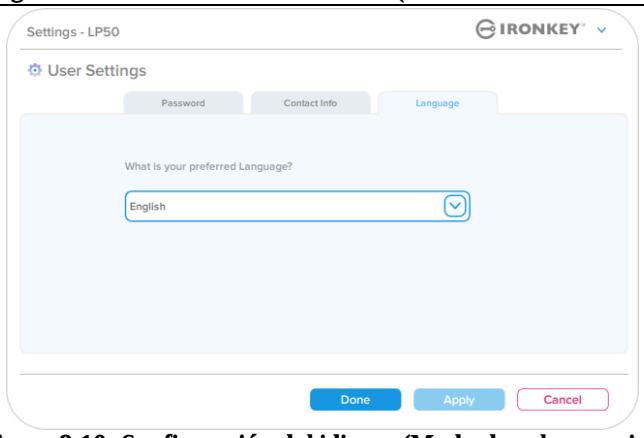
Contraseña (Password): Le permite cambiar su contraseña de usuario y/o pista. (*Figura 8.5*)	 **Figura 8.5 - Opciones de contraseña (Admin habilitado: Inicio de sesión de usuario)**
Información de contacto (Contact Info): Le permite agregar/visualizar/cambiar su información de contacto. (*Figura 8.6*)	 **Figura 8.6 - Información de contacto (Admin habilitado: Inicio de sesión de usuario)**
Idioma (Language): Le permite cambiar su selección de idioma actual. (*Figura 8.7*)	 **Figura 8.7 - Configuración del idioma (Admin habilitado: Inicio de sesión de usuario)**

Nota: Las Opciones de administrador no son accesibles cuando se inicia sesión con la Contraseña de usuario.

Configuración del LP50

Configuración de usuario: Administrador no habilitado

Como se mencionó anteriormente en la página 12, la inicialización del LP50 sin habilitar las 'Contraseñas de administrador y usuario ajustará el dispositivo en una configuración de **Contraseña única, Usuario único**. Esta configuración no tiene acceso a ninguna de las opciones o funciones de Admin. Esta configuración tendrá acceso a los siguientes ajustes del LP50:

Contraseña (Password): 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 (Contact Info): Le permite agregar/visualizar/cambiar su información de contacto. (*Figura 8.9*)	 **Figura 8.9- Información de Contacto (Modo de solo usuario)**
Idioma (Language): Le permite cambiar su selección de idioma actual. (*Figura 8.10*)	 **Figura 8.10- Configuración del idioma (Modo de solo usuario)**

Configuración del LP50

Cambiar y guardar la configuración

- Siempre que se cambien los ajustes en la configuración del LP50 (por ejemplo, Información de contacto, idioma, Cambios de contraseña, Opciones de administrador, etc.), el dispositivo le pedirá que ingrese su contraseña para aceptar y aplicar los cambios. (*Ver figura 8,11*)

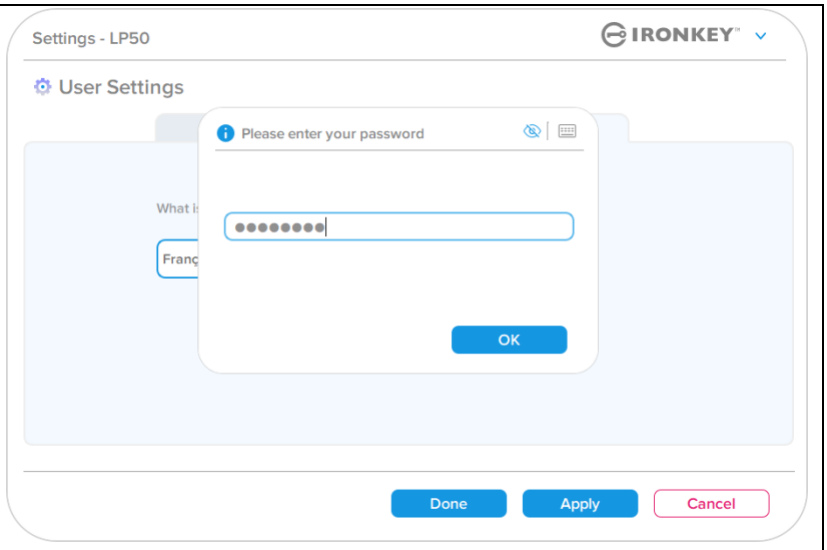


Figura 8.11 - Pantalla de solicitud de contraseña para guardar los cambios de configuración del LP50

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 (OK). Esto cerrará el cuadro 'de 'Por favor, introduzca su contraseña' y volverá al menú de configuración del LP50.

Funciones de administrador

Opciones disponibles para Restablecer la Contraseña de usuario

Una de las características útiles de la configuración de administrador le permite restablecer de forma segura la contraseña de los usuarios, en caso de que la 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 requisitos de la contraseña se ajustarán por defecto a los criterios originales que se establecieron durante el proceso de inicialización (opciones Complejo o Frase de acceso).

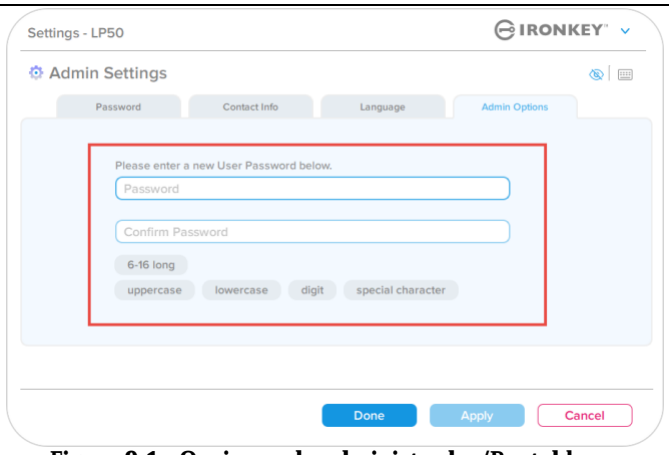


Figura 9.1 - Opciones de administrador/Restablecer contraseña de usuario

Ayuda y resolución de problemas

Bloqueo del dispositivo

El LP50 incluye una característica de seguridad que impide el acceso no autorizado a la partición de datos, una vez que se ha hecho 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 (n.º de intentos) para cada método de Inicio de sesión (Admin/Usuario).

El 'contador de 'bloqueo hace el seguimiento de cada inicio de sesión fallido y es reinicializado de **una de estas dos** maneras:

1. Un inicio de sesión exitoso antes de llegar a MaxNoA

2. Alcanzar MaxNoA y realizar un bloqueo de dispositivo o formateo de dispositivo dependiendo de cómo se configuró el dispositivo.

- 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*)

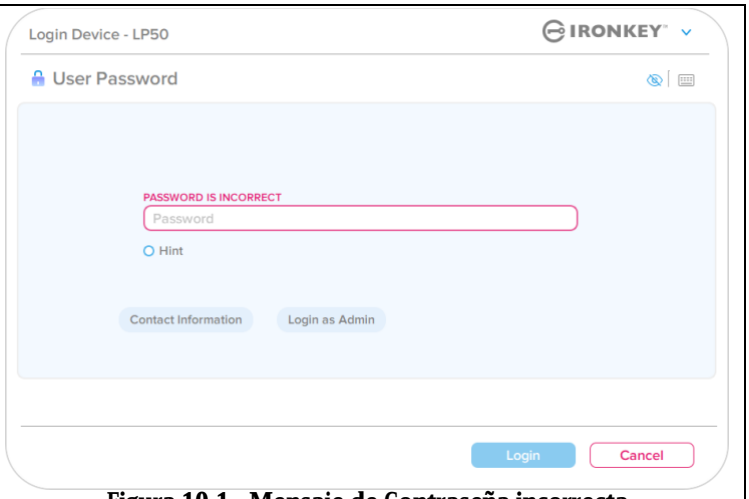


Figura 10.1 - Mensaje de Contraseña incorrecta

- Cuando se realiza un **séptimo** intento fallido, verá un mensaje de error adicional que indica que le quedan 3 intentos antes de alcanzar MaxNoA (establecido en 10 por defecto). (*Figura 10.2*)

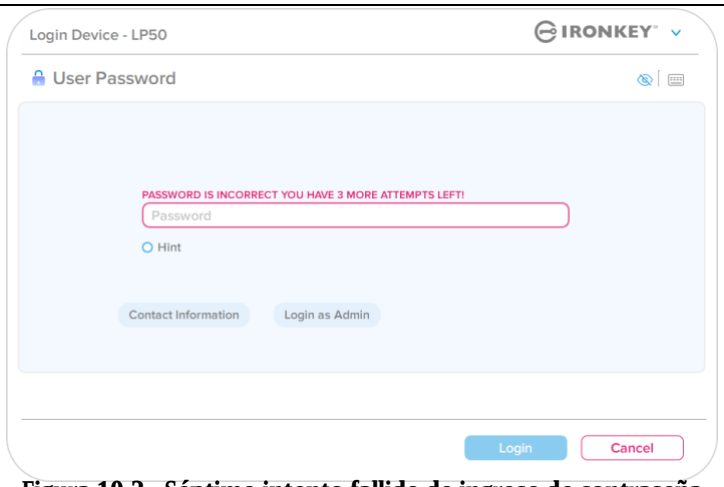


Figura 10.2 - Séptimo intento fallido de ingreso de contraseña

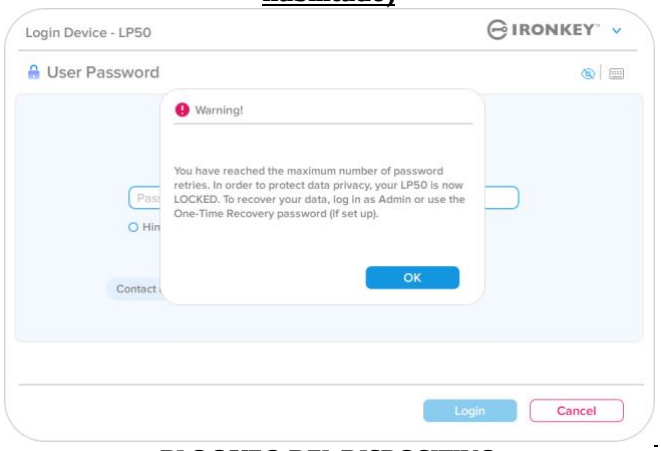
Ayuda y resolución de problemas

Bloqueo del dispositivo

Importante: Después de un **décimo** y último intento fallido de inicio de sesión, dependiendo de cómo se configuró el dispositivo y del método de inicio de sesión utilizado (Administrador / Usuario), el dispositivo se bloqueará y deberá iniciar sesión con un método alternativo (si aplica), o un restablecimiento del dispositivo que **formateará los datos y todos los datos en el dispositivo se perderán para siempre**. Los comportamientos también se mencionan en la página 18 de esta Guía del usuario.

Las Figuras 10.3- 9.6 a continuación demuestran el comportamiento visual para el décimo y último intento fallido de inicio de sesión de cada método de contraseña de inicio de sesión:

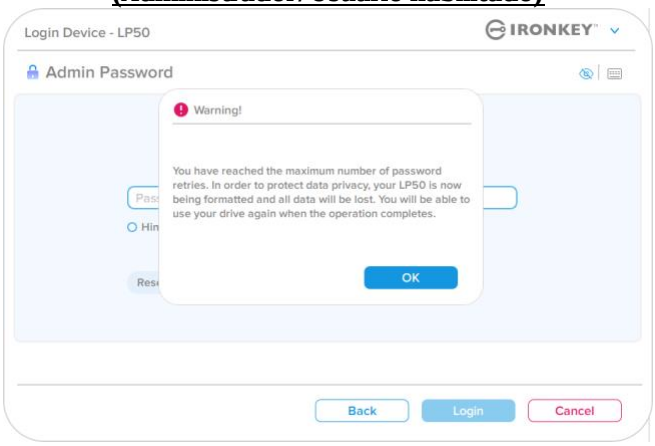
Contraseña de usuario: (Administrador/usuario habilitado)



BLOQUEO DEL DISPOSITIVO

Figura 10.3

Contraseña de administrador (Administrador/Usuario habilitado)

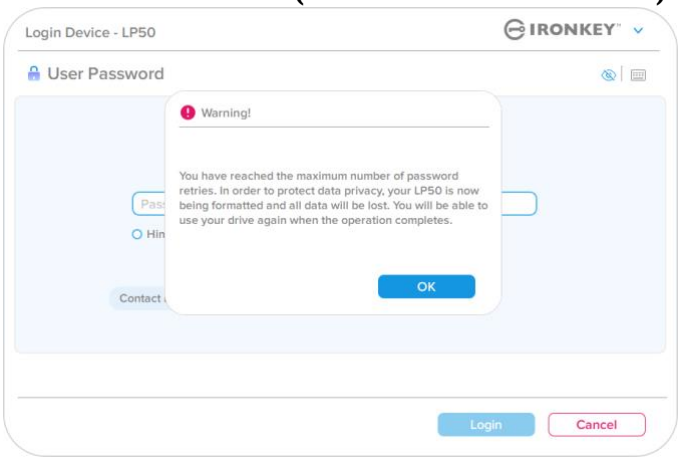


REFORMATEO DEL DISPOSITIVO*

Figura 10.4

- Estas medidas de seguridad limitan que alguien (que no tenga su contraseña) intente innumerables intentos de inicio de sesión y obtenga acceso a sus datos confidenciales (también conocido como ataque de fuerza bruta). Si usted es el propietario del LP50 y ha olvidado su contraseña, aplican las mismas medidas de seguridad, incluyendo el formateo del dispositivo. *Para obtener más información sobre esta función, consulte *'Restablecer dispositivo'* en la página 25.

Contraseña de usuario (Administrador NO habilitado)



REFORMATEO DEL DISPOSITIVO*

Figura 10.5

** Nota: El formatear un dispositivo borrará TODA la información almacenada en la partición de datos segura del LP50.*

Ayuda y resolución de problemas

Reiniciar 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 configurado el dispositivo (ya sea en el menú de inicio de sesión de la Contraseña de administrador si Administrador/Usuario está habilitado , o en el menú de inicio de sesión de la 'contraseña de usuario si el modo Administrador/Usuario no está habilitado) cuando se ejecuta el iniciador del LP50. (*ver Figura 10.7 y 10.8*)

- Esta opción le permitirá crear una nueva contraseña, pero el LP50 será formateado con el fin de proteger la privacidad de sus datos. Esto significa que todos sus datos se borrarán en el proceso.*

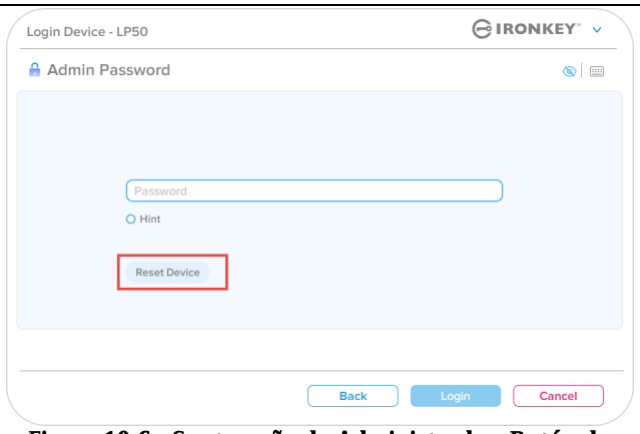


Figura 10.6 - Contraseña de Administrador: Botón de Restablecer dispositivo

- **Nota:** Cuando haga clic en '*Restablecer dispositivo*' (Reset Device), aparecerá un cuadro de mensaje y se le 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 Figura 10.8*)

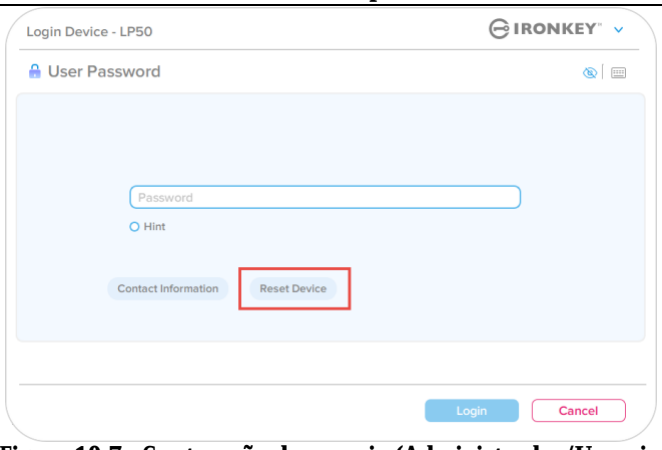


Figura 10.7 - Contraseña de usuario (Administrador/Usuario no habilitado) Restablecer dispositivo

- 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.

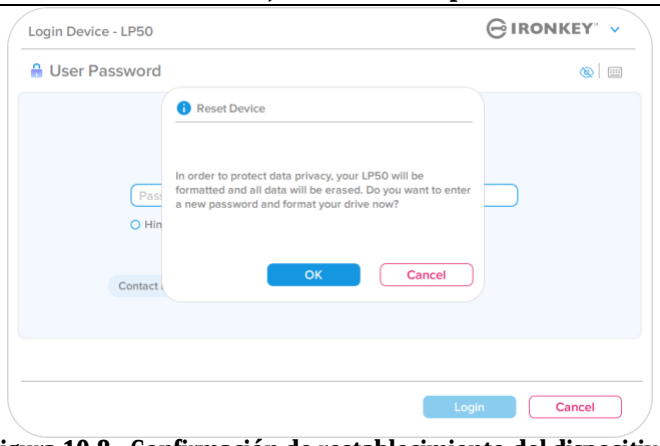


Figura 10.8 - Confirmación de restablecimiento del dispositivo

Ayuda y resolución de problemas

Conflicto con letras de unidad: Sistemas operativos Windows

- Como se ha mencionado en la sección *'Requerimientos del sistema'* de este manual (en la página 3), el LP50 requiere dos letras consecutivas de dispositivo DESPUÉS del último disco físico que aparece antes de la 'brecha en las asignaciones de letras del dispositivo (*ver Figura 10.9*). Lo anterior NO se refiere a los recursos compartidos de red, dado que son específicos de los perfiles del usuario y no del perfil del hardware del sistema mismo, por lo cual ante el sistema operativo se muestran como disponibles.

- Lo anterior significa que Windows podría asignar al LP50 una letra de dispositivo que ya esté en uso por parte de un recurso compartido de red o en una ruta UNC (Convención de Nomenclatura Universal), lo que causa un conflicto en las letras del dispositivo. Si eso ocurre, pida asistencia al administrador de su sistema o al departamento de soporte técnico, respecto al cambio de las asignaciones de letras de unidad en la utilidad Administración de discos de Windows (se requieren privilegios de administrador)

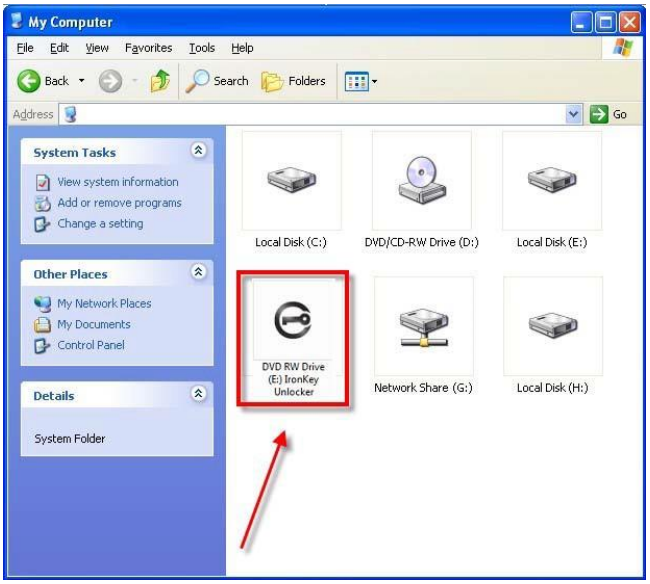


Figura 10.9 - Ejemplo de letra de unidad

En este ejemplo (*Figura 10.9*), el LP50 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 la unidad). Dado que la letra G: está asignada a un recurso compartido de red y no forma parte del perfil del hardware, el LP50 podría intentar usar dicha letra como su segunda letra de unidad, lo cual causaría un conflicto.

Si no hay recursos compartidos de red en su sistema y el LP50 aún no se carga, es posible que un lector de tarjetas, disco extraíble u otro dispositivo instalado previamente se aferre a una asignación de letras de unidad y siga causando un conflicto.

Tenga en cuenta que Drive Letter Management, o DLM, ha mejorado significativamente en Windows 8.1,10 y 11, por lo que es posible que no encuentre 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 para obtener más ayuda.

IRONKEY™ Locker+ 50 (LP50)
SICHERER USB 3.2 Gen 1-STICK

Anleitung

Inhalt

Abb. 1: IronKey LP50

Einführung

Kingston IronKey Locker+ 50 USB-Sticks bieten mit der AES-Hardwareverschlüsselung im XTS-Modus Sicherheit auf Verbraucherniveau, einschließlich Schutzmaßnahmen gegen BadUSB mit digital signierter Firmware und Brute-Force-Passwortangriffe. Der LP50 ist auch TAA-konform.

Der LP50 unterstützt jetzt die Option für mehrere Passwörter (Admin und Benutzer) mit den Modi Komplex oder Passphrase. Im Modus Komplex 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 Passworteingabe 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. Außerdem schützt eine integrierte virtuelle Tastatur die Passwörter vor Key- und Screenloggern.

Der Locker+ 50 ist mit einem kleinen Metallgehäuse und einer integrierten Schlüsselschlaufe ausgestattet, damit Sie Ihre Daten überallhin mitnehmen können. Der LP50 bietet außerdem eine optionale USBtoCloud-Sicherung (von ClevX®), mit der Sie von Ihrem persönlichen Cloud-Speicher über Google Drive™, OneDrive (Microsoft®), Amazon Cloud Drive, Dropbox™ oder Box auf die Daten auf dem Laufwerk zugreifen können. Der LP50 lässt sich leicht einrichten und verwenden, da keine Anwendungsinstallation erforderlich ist. Die gesamte benötigte Software und Sicherheitsfunktionen befinden sich bereits auf dem Stick. Funktioniert sowohl unter Windows® als auch unter macOS®, sodass Benutzer von mehreren Systemen aus auf Dateien zugreifen können.

Der LP50 wird durch eine 5-Jahres-Garantie mit kostenlosem technischen Kingston Support unterstützt.

IronKey Locker+ 50 Merkmale

- 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
- Mit Windows- oder macOS kompatibel (Details siehe Datenblatt)

Über dieses Handbuch (09242024)
Dieses Benutzerhandbuch bezieht sich auf den IronKey Locker+ 50 (LP50).

Systemvoraussetzungen

PC-Plattform • Intel und AMD • 15MB freier Festplattenspeicher • Freier USB 2.0 – 3.2-Anschluss • Zwei freie, aufeinander folgende Laufwerksbuchstaben nach dem letzten physischen Laufwerk * * **Hinweis:** Siehe „Laufwerksbuchstabenkonflikt“ auf Seite 32.	**Unterstützte PC-Betriebssysteme** • Windows 11 • Windows 10
Mac Plattform • Intel und Apple SOC • 15MB freier Festplattenspeicher • USB 2.0 – 3.2 Anschluss	**Unterstützte Mac-Betriebssysteme** • macOS 12.x – 15.x

Hinweis: Ein kostenloses 5-Jahres-Abonnement für USB-to-Cloud ist bei jedem Stick bei der Aktivierung enthalten. Fortgesetzte Aktivierungsoptionen, die von ClevX über den angegebenen Zeitrahmen hinaus erworben werden können.

Empfehlungen

Für eine ausreichende Stromversorgung des LP50 schließen Sie ihn direkt in einen USB-Anschluss Ihres Notebooks oder PCs an, siehe Abb. 1.1. Schließen Sie den LP50 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

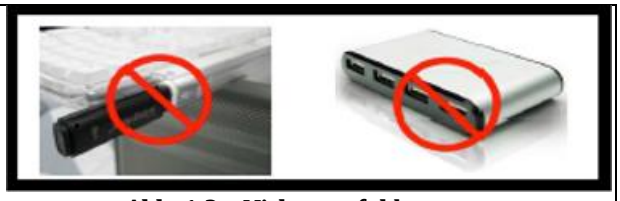


Abb. 1.2 – Nicht empfehlenswert

Verwenden des korrekten Dateisystems
Der IronKey LP50 ist mit dem FAT32-Dateisystem vorformatiert. Dies 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 LP50 auf einem Zielsystem eingerichtet und verwendet wird
- 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 LP50 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 LP50 automatisch die verschlüsselten Daten unwiederbringlich und formatiert sich selbst zurück auf den Werkszustand.

Mehrfach-Passwort
Der LP50 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 LP50 zwei verschiedene Passwörter unterstützen, die Sie zur Wiederherstellung von Daten verwenden können – Admin- und Benutzer-Passwortrollen.

Der LP50 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 LP50 kann zurückgesetzt und wieder verwendet werden, aber die vorherigen Daten werden für immer gelöscht.

Passwort-Modi
Der LP50 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 LP50 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 LP50-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-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 8,1, 10 und 11 wird eine Meldung 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:)“.

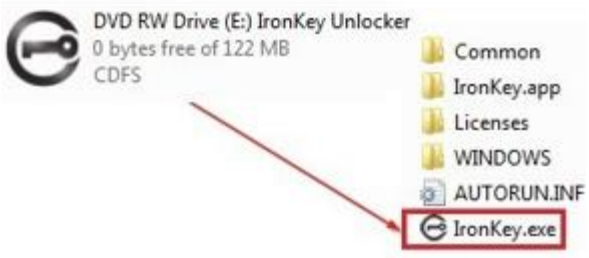


Abb. 3.2 – Fenster Datei-Explorer/IronKey.exe

Gerätezugriff (macOS-Umgebung)

Schließen Sie den LP50 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.
- Doppelklicken Sie dann auf das Symbol der IronKey.app, das in dem in der Abb. 3.3 dargestellten Fenster angezeigt wird. Dadurch wird der Installationsprozess gestartet.

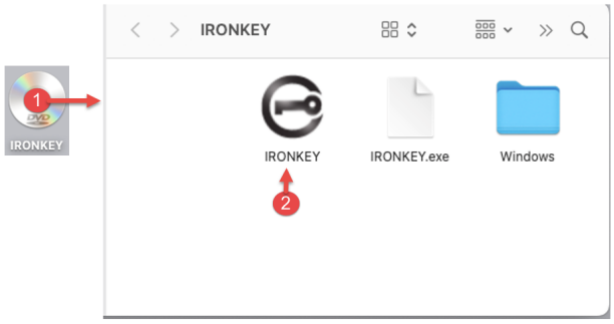


Abb. 3.3 – IKLP Laufwerk

Geräteinitialisierung (Windows- und macOS-Umgebung)

Sprache und EULA

- Wählen Sie die von Ihnen gewünschte Sprache aus dem Drop-Down-Menü und klicken Sie auf „**Weiter** (Next)“ (beachten Sie die Abb. 4.1)

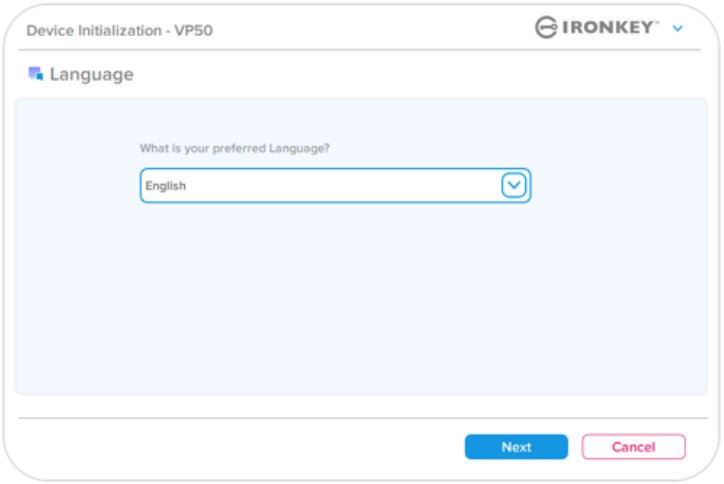


Abb. 4.1 – Sprachauswahl

- 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)

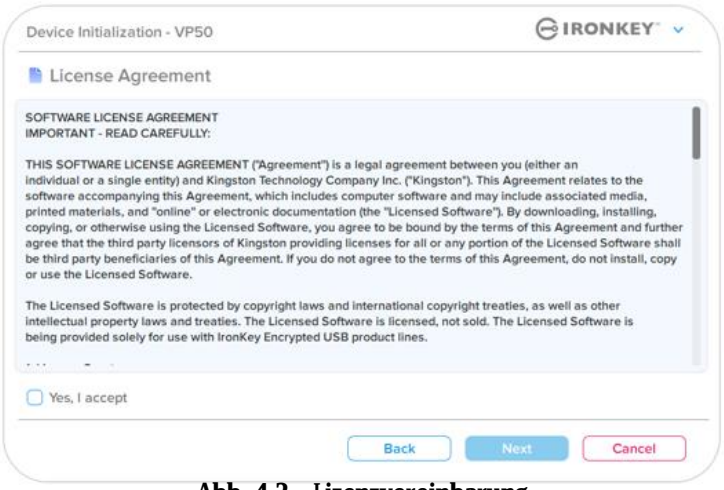


Abb. 4.2 – Lizenzvereinbarung

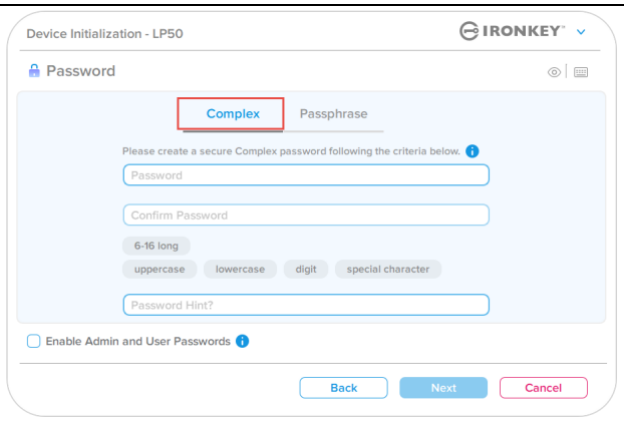
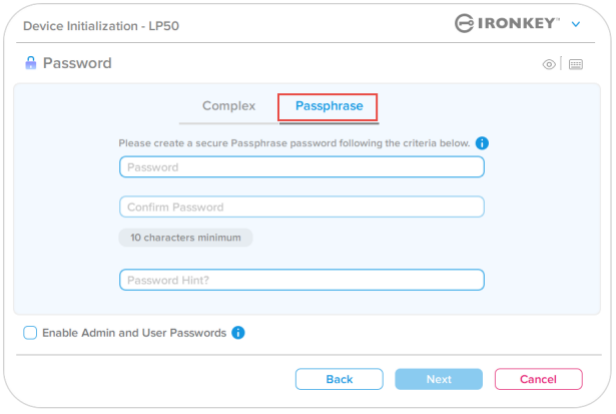
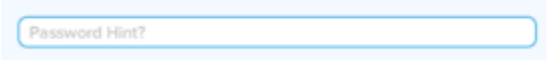
Geräteinitialisierung

Passwort-Auswahl

Auf dem Bildschirm der Passwortabfrage können Sie ein Passwort erstellen, um die Daten auf dem LP50 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 (Password)“ und geben Sie es dann erneut in das Feld „Passwort bestätigen (Confirm Password)“ ein. Bevor Sie mit der Installationseinrichtung fortfahren können, müssen Sie ein Passwort nach folgenden Kriterien eingeben:

Komplexes (Complex) Passwort • Muss mindestens 6 Zeichen lang sein (bis zu 16 Zeichen). • Muss 3 (drei) der folgenden Kriterien erfüllen: o Großbuchstabe o Kleinbuchstaben o Zahl o Sonderzeichen (!,$,& usw.)	 **Abb. 4.3 – Komplexes Passwort**
Passphrasen (Passphrase) Passwort • Muss enthalten: o Minimal 10 Zeichen o Maximal 64 Zeichen	 **Abb. 4.4 – Passphrasen-Passwort**
Passwort-Hinweis (Password Hint) (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).

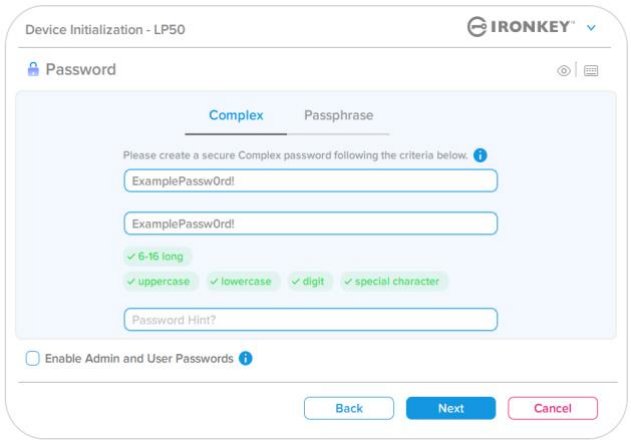


Abb. 4.6a – Bedingung für komplexes Passwort erfüllt

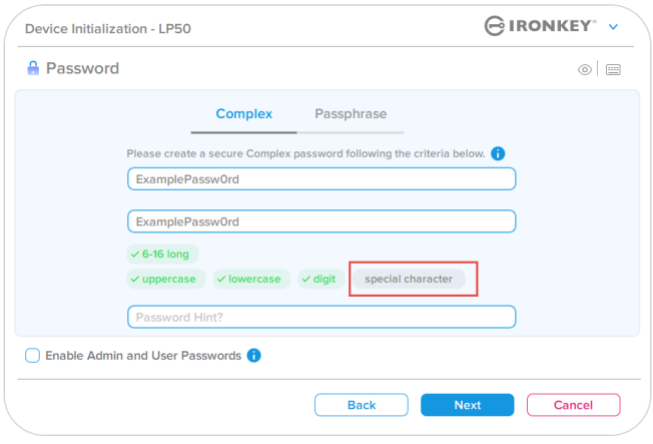


Abb. 4.6b – Bedingung für komplexes Passwort ist optional

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.

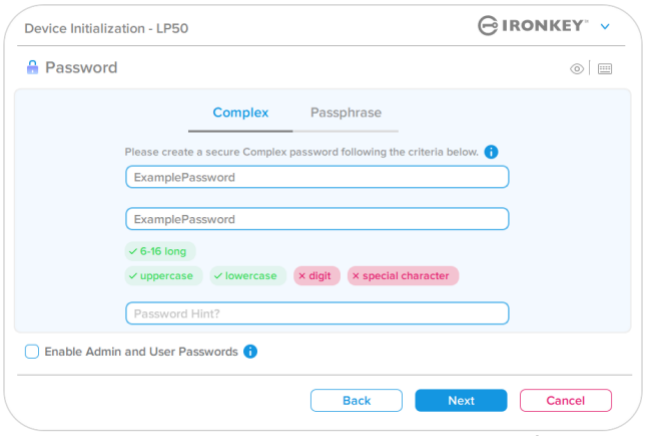


Abb. 4.7 – Passwort-Bedingungen nicht erfüllt

Geräteinitialisierung

Virtuelle Tastatur
Der LP50 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 drücken Sie darauf.

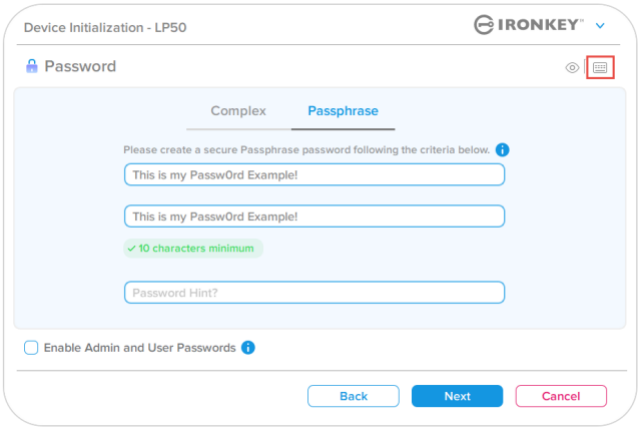


Abb. 4.8 – Aktivieren der virtuellen Tastatur

- 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 anordnen** (Randomize)“ wählen. Durch Zufallseingabe wird die Tastatur in einer zufälligen Reihenfolge angeordnet

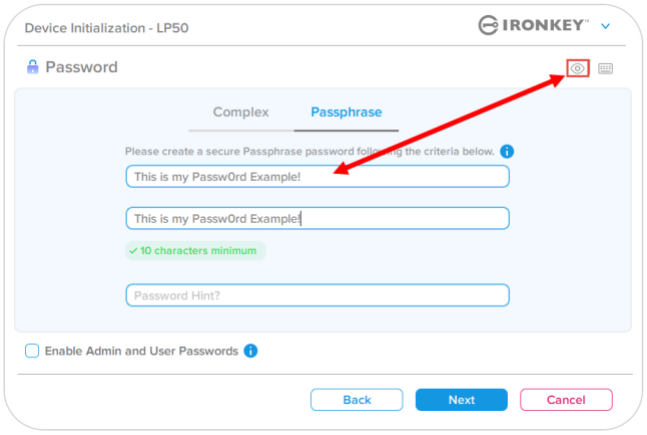
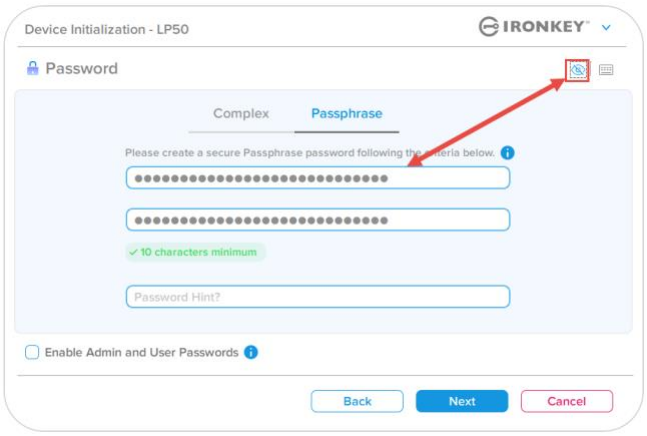
Abb. 4.9 – Screenlogger-Schutz/Zufällig anordnen

Geräteinitialisierung

Umschalten der Passwortsichtbarkeit

Wenn Sie ein Passwort erstellen, wird die Passwortzeichenfolge standardmäßig während der Eingabe in das Feld eingeblendet. Wenn die Passwort-Zeichenfolge während der Eingabe ausgeblendet werden soll, entfernen Sie die Markierung des Passwort-„Auges“ auf der oberen rechten Seite im Fenster „Geräteinitialisierung (Device Initialization)“.

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 Passort „Verbergen (Hide)“ umschalten**
Auf das blaue Symbol klicken, um das verborgene Passwort **anzuzeigen**. 	 **Abb. 4.11 – Auf Passort „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 Folgendes:

- Zurücksetzen des Benutzer-Passworts

Weitere Informationen zur Funktion „Benutzerpasswort zurücksetzen (User Password reset) finden Sie auf Seite 28 in dieser Bedienungsanleitung.

- Damit Sie **Admin- und Benutzer-Passwörter** aktivieren können, klicken Sie auf das Kontrollkästchen neben „**Admin- und Benutzer-Passwörter aktivieren** (Enable Admin and User passwords)“ und wählen Sie dann „**Weiter** (Next)“, sobald Sie ein gültiges Passwort ausgewählt haben. (Abb. 4.12)

- Wenn diese Funktion **aktiviert** ist, dann ist das auf diesem Bildschirm gewählte Passwort 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.

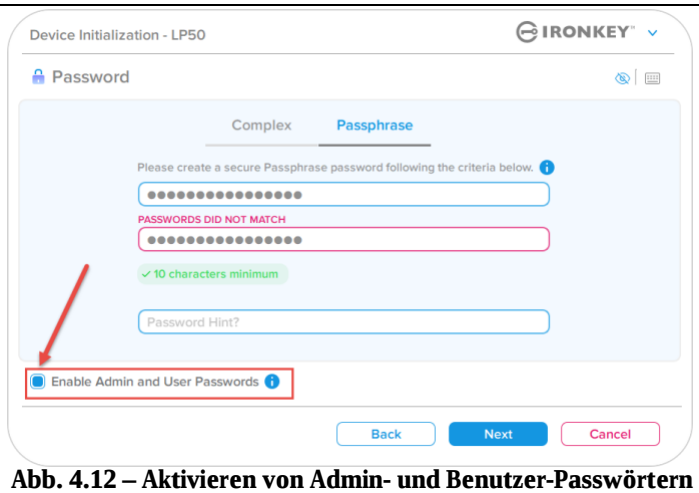


Abb. 4.12 – Aktivieren von Admin- und Benutzer-Passwörtern

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 dieser Bedienungsanleitung 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** (User Password) 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.

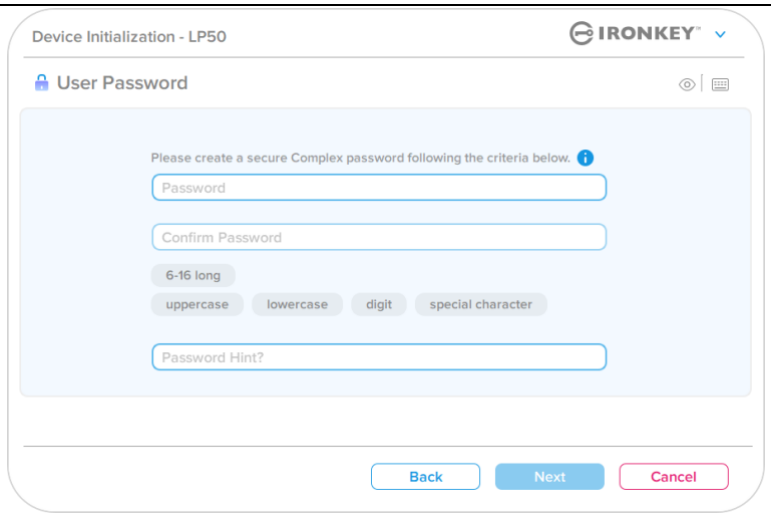


Abb. 4.13 – Benutzer-Passwort (Admin und Benutzer aktiviert)

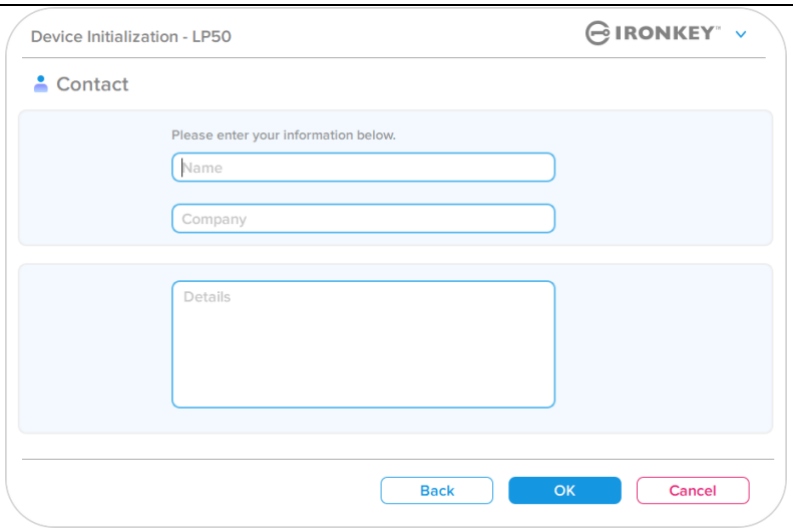
Hinweis: Die gewählte Passwortoption (Komplex oder Passphrase) wird für das Benutzer-Passwort, die einmalige Wiederherstellung von Passwörtern und alle Passwort-Rücksetzungen übernommen, die nach der Einrichtung des Sticks erforderlich sind. Die gewählte Passwortoption kann nur nach einem vollständigen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

Geräteinitialisierung

Kontaktangaben

Geben Sie Ihre Kontaktdaten in den angezeigten Textfeldern 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** (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** (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.

USB ß → Cloud Initialisierung (Windows-Umgebung)

Nach der Einrichtung des Geräts wird die USB-to-Cloud-Anwendung angezeigt, siehe *Abb. 5.1* rechts. Vergewissern Sie sich, bevor Sie fortfahren, dass eine Internetverbindung besteht.

- Klicken Sie zum Fortfahren mit der Installation im Fenster „clevX“ auf die grüne Schaltfläche „Akzeptieren (Accept)“ in der rechten unteren Ecke.
- Zum Ablehnen der Installation klicken Sie im Fenster „clevX“ auf die rote Schaltfläche „Ablehnen (Decline)“ in der linken unteren Ecke.
- (Hinweis: Wenn Sie auf die rote Schaltfläche „Ablehnen (Decline)“ klicken, wird die USB-to-Cloud-Installation abgebrochen. Bei diesem Vorgang wird in der Datenpartition eine spezielle Textdatei mit der Bezeichnung „USBtoCloudInstallDeclined.txt“ erstellt. Diese Datei verhindert, dass die Anwendung Sie weiterhin zur Installation auffordert.)

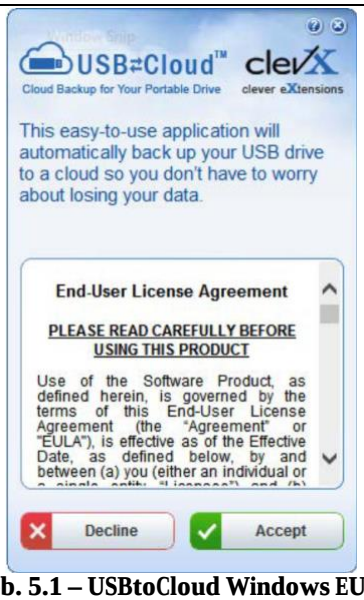


Abb. 5.1 – USBtoCloud Windows EULA

- Wenn während des Einrichtungsprozesses das folgende Windows Fenster „Sicherheitswarnung“ angezeigt wird, klicken Sie bitte auf „Zugriff erlauben”, damit die USB-to-Cloud-Anwendung weiterhin ausgeführt werden kann (andernfalls erstellen Sie eine Ausnahme für die Windows-Firewall).

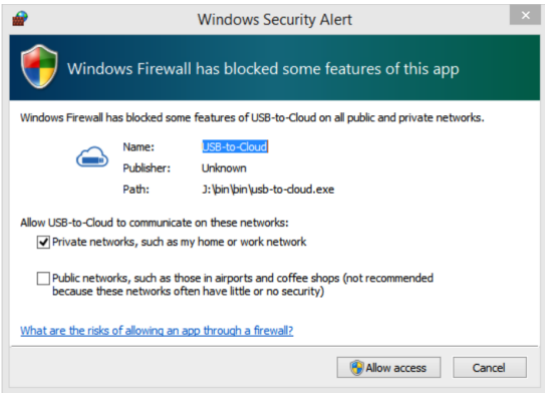


Abb. 5.2 – Windows Sicherheitswarnung

USB ß → Cloud Initialisierung (Windows-Umgebung)

- Nach Abschluss der Installation wird ein Anwendungsfeld mit einer Auswahlliste angezeigt (zum Synchronisieren IhrerLP50-Daten).
- Wählen Sie die Cloud-Option, die Sie für Ihre Datensicherung verwenden möchten, und geben Sie die zur Anmeldung erforderlichen Kenndaten ein.
- (Hinweis: Wenn Sie aktuell noch kein Konto bei einer der aufgelisteten Cloud-Optionen haben, können Sie es jetzt bei dem von Ihnen gewünschten Internetbrowser erstellen und diese Option nachfolgend ausfüllen.)
- Nachdem Sie eine-Option ausgewählt und sich bei dem entsprechenden Dienst angemeldet haben, wird das USB-to Cloud-Programm als erstes die Datenpartition mit den Daten abgleichen, die in der Cloud gespeichert sind. Solange der Dienst USB-to-Cloud im Task-Manager läuft, wird Inhalt, der auf die Datenpartition geschrieben wird, automatisch auch in der Cloud gesichert (synchronisiert).

Abb. 5.3 – Cloud-Auswahl

USB ß → Cloud Nutzung (Windows-Umgebung)

Die USB-to-Cloud-Anwendung enthält folgende zusätzliche Dienste:

- Backup anhalten (Pause Backup) (die Datensicherung wird angehalten).
- Wiederherstellen (Restore) (stellt Daten aus der Cloud auf dem Gerät wieder her).
- Einstellungen (Settings) (weitere Optionen für Ihre Datensicherung).
- Beenden (Exit) (beendet den Dienst USB-to-Cloud).

Im Menü „Einstellungen“ ist Folgendes möglich:

- Ändern der Cloud-Service-App, die Sie derzeit für Backups verwenden.
- Ändern der Sprache, die derzeit verwendet wird.
- Auswahl der Dateien bzw. Ordner, die in der Cloud gesichert werden sollen.
- Suche nach Software-Updates.

(**Hinweis**: Wenn Sie den LP50 zurücksetzen oder formatieren, werden alle Daten auf dem Gerät gelöscht. Die in der Cloud gespeicherten Daten sind davon jedoch nicht betroffen und bleiben sicher gespeichert.)

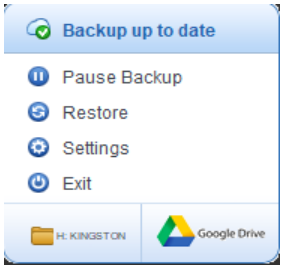


Abb. 5.4 – Dienste

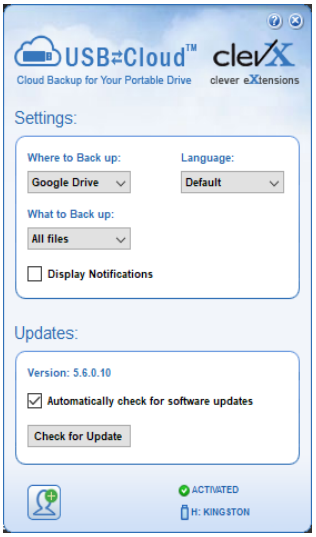


Abb. 5.5 – Einstellungen

USB ß → Cloud Initialisierung (macOS Umgebung)

- Nach der Einrichtung des Geräts wird die USB-to-Cloud-Anwendung angezeigt, siehe *Abb. 5.6* rechts. Vergewissern Sie sich, bevor Sie fortfahren, dass eine Internetverbindung besteht.
- Klicken Sie zum Fortfahren mit der Installation im Fenster „clevX“ auf die grüne Schaltfläche „Akzeptieren (Accept)“ in der rechten unteren Ecke.

  (Hinweis: Unter macOS 12.x und höher werden Sie aufgefordert, „IRONKEY“ den Zugriff auf Dateien auf einem Wechseldatenträger zu erlauben. Wählen Sie OK.) *(Siehe Abb. 5,7)*

- Zum Ablehnen der Installation klicken Sie im Fenster „clevX“ auf die rote Schaltfläche „Ablehnen (Decline)“ in der linken unteren Ecke.

Abb. 5.6 - USBtoCloud macOS EULA

(Hinweis: Wenn Sie auf die rote Schaltfläche „Ablehnen (Decline)“ klicken, wird die USB-to-Cloud-Installation abgebrochen. Bei diesem Vorgang wird in der Datenpartition eine spezielle Datei mit dem Namen „‘DontInstallUSBtoCloud“ erstellt. Diese Datei verhindert, dass die Anwendung Sie weiterhin zur Installation auffordert.)

- Nach Abschluss der Installation wird ein Anwendungsfeld mit einer Auswahlliste angezeigt (zum Synchronisieren IhrerLP50-Daten). *(Abb. 5.8)*

Abb. 5.7 – macOS-Zugang

- Wählen Sie die Cloud-Option, die Sie für Ihre Datensicherung verwenden möchten, und geben Sie die zur Anmeldung erforderlichen Kenndaten ein.

  (Hinweis: Wenn Sie aktuell noch kein Konto bei einer der aufgelisteten Cloud-Optionen haben, können Sie es jetzt bei dem von Ihnen gewünschten Internetbrowser erstellen und diese Option nachfolgend ausfüllen.)

- Nachdem Sie eine-Option ausgewählt und sich bei dem entsprechenden Dienst angemeldet haben, wird das USB-to Cloud-Programm als erstes die Datenpartition mit den Daten abgleichen, die in der Cloud gespeichert sind. Solange der Dienst USB-to-Cloud im Task-Manager läuft, wird Inhalt, der auf die Datenpartition geschrieben wird, automatisch auch in der Cloud gesichert (synchronisiert).

Abb. 5.8 Cloud-Auswahl

USB ß →Cloud Nutzung (macOS-Umgebung)

Die USB-to-Cloud-Anwendung bietet folgende zusätzliche Dienste *(Abb. 5.9)*:

- **Backup anhalten (Pause Backup)** (die Datensicherung wird angehalten)
- **Wiederherstellen (Restore)** (stellt Daten aus der Cloud auf dem Gerät wieder her)
- **Backup ausführen (Backup)** (öffnet die Cloud-Optionen) *Siehe Abb. 5.9*
- **Beenden (exit)** (beendet den Dienst USB-to-Cloud)

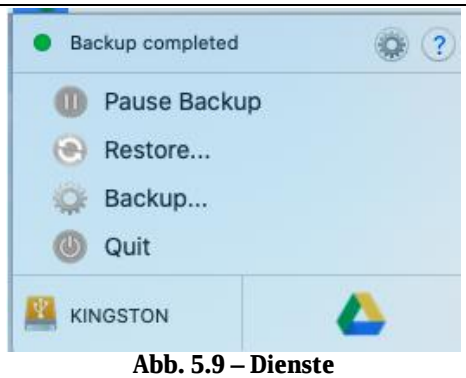


Abb. 5.9 – Dienste

Im Menü „Voreinstellungen (Preferences)“ sind folgende Einstellungen möglich:

- Ändern der gerade verwendeten Sprache
- Aktivieren/Deaktivieren von akustischen Benachrichtigungen
- Aktivieren/Deaktivieren des Trennens von Laufwerken beim Beenden der Anwendung
- Aktivieren/Deaktivieren der Protokollierung zur Fehlerbehebung
- Automatische Software-Updates aktivieren/ deaktivieren und jetzt nach Updates suchen

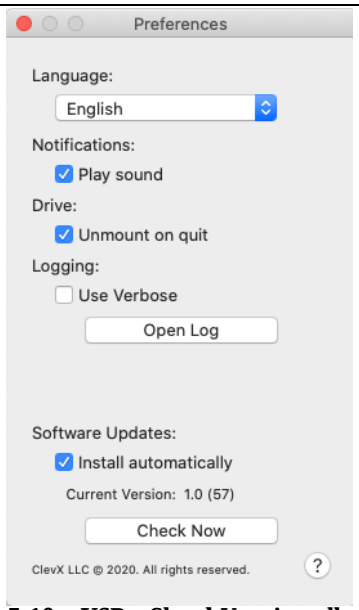


Abb. 5.10 – USBtoCloud-Voreinstellungen

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 LP50 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)*.

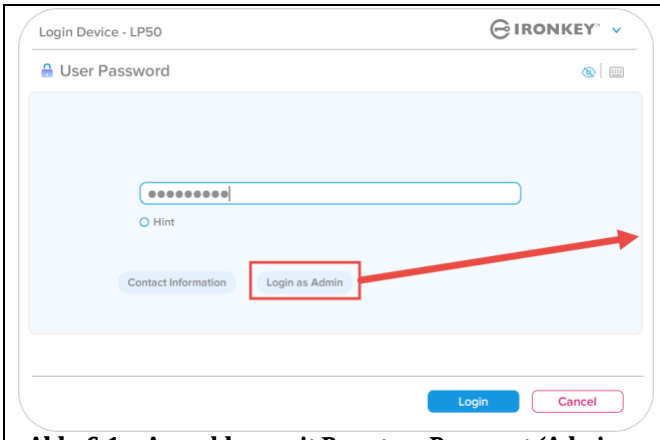


Abb. 6.1 – Anmeldung mit Benutzer-Passwort (Admin aktiviert)

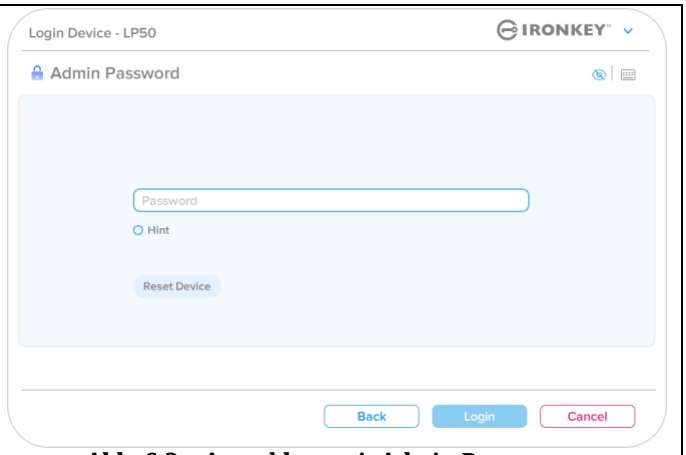


Abb. 6.2 – Anmeldung mit Admin-Passwort

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.**

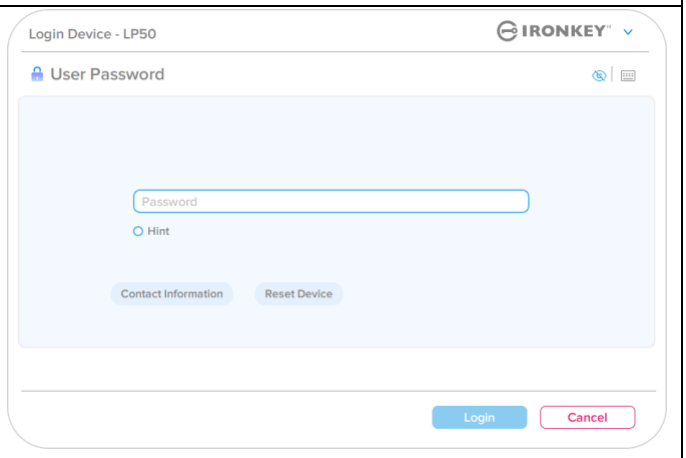


Abb. 6.3 – Anmeldung mit Benutzer-Passwort (Admin nicht aktiviert)

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 Passworteingabeversuche erreicht wurde, verhält sich das System wie folgt:

Admin/Benutzer aktiviert	**Schutz vor Brute-Force-Angriffen Geräteverhalten (10 falsche Passworteingabeversuche)**	**Datenlöschung und Geräte-Reset?**
Benutzer-Passwort:	Passwort-Sperre. Melden Sie sich als Admin um das Benutzer-Passwort zurückzusetzen	NEIN (NO)
Admin-Passwort	Crypto-Löschen des Laufwerks, Passwörter, Einstellungen und Daten werden für immer gelöscht	**YES (JA)**
Nur-Benutzer Einzelner Benutzer, einzelnes Passwort (Admin/Benutzer NICHT aktiviert)	**Schutz vor Brute-Force-Angriffen Geräteverhalten (10 falsche Passworteingabeversuche)**	**Datenlöschung und Geräte-Reset?**
Benutzerpasswort	Crypto-Löschen des Laufwerks, Passwörter, Einstellungen und Daten werden für immer gelöscht	**YES (JA)**

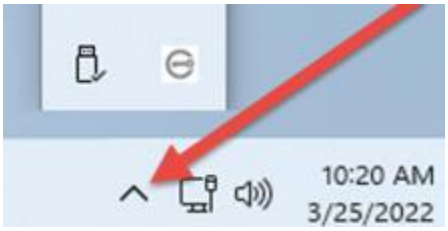
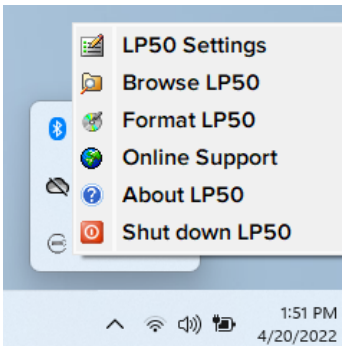
* Sobald Sie sich erfolgreich am Gerät authentifiziert haben, wird der Zähler für fehlgeschlagene Anmeldungen zurückgesetzt, je nachdem, welche Anmeldemethode verwendet wurde. Das Crypto-Löschen löscht alle Passwörter, Verschlüsselungsschlüssel und Daten – **die Daten gehen für immer verloren.**

Zugriff auf die sicheren Dateien

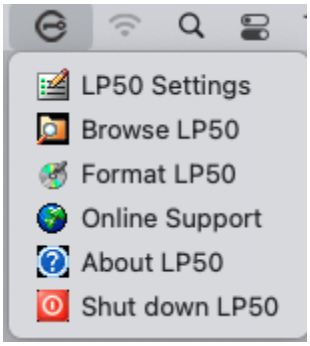
Nachdem Sie den USB-Stick entsperrt haben, können Sie auf Ihre sicheren Dateien zugreifen. Dateien werden automatisch ver- und entschlüsselt, wenn diese auf dem Stick gespeichert oder geöffnet werden. Diese Technologie bietet Ihnen den Komfort des Arbeitens wie mit einem normalen Stick, während sie gleichzeitig 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 „**LP50 durchsuchen** (Browse LP50)“ klicken *(Abb. 7.2)*.

Geräteoptionen – (Windows-Umgebung)

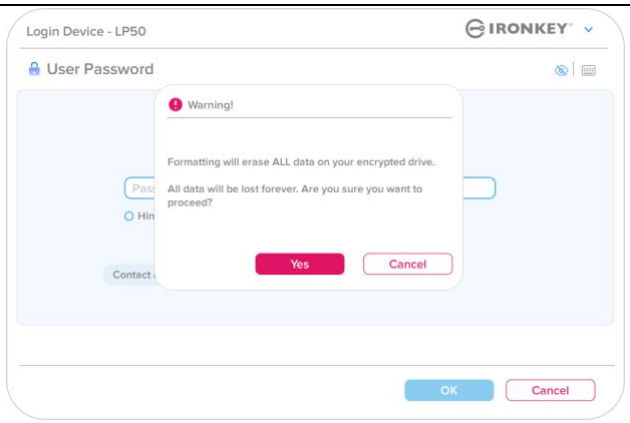
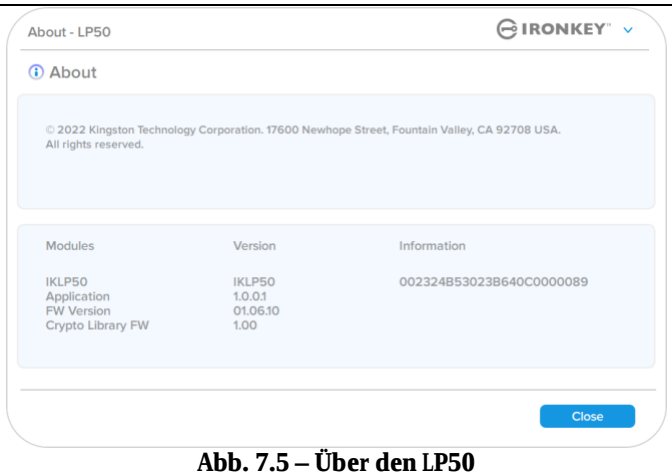
Solange Sie auf dem Gerät angemeldet sind, wird in der rechten Ecke des Fensters das IronKey-Symbol angezeigt. Wenn Sie mit der rechten Maustaste auf das IronKey-Symbol klicken, öffnet sich das Auswahlmenü für die verfügbaren Laufwerksoptionen *(Abb. 6.2)*.
Einzelheiten zu diesen Geräteoptionen finden Sie auf den Seiten 19–23 dieser Bedienungsanleitung

• 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 finden Sie auf den Seiten 19–23 dieser Bedienungsanleitung.	 **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 LP50-Symbol ***(siehe Abb. 7.3)***, mit dem die verfügbaren Geräteoptionen geöffnet werden. Einzelheiten zu diesen Geräteoptionen finden Sie auf den Seiten 19–23 dieser Bedienungsanleitung.	 **Abb. 7.3 – Symbol in Menüleiste für macOS/Geräteoptionsmenü**

Geräteoptionen

LP50-Einstellungen:	• Ändern des Anmelde-Passworts, der Kontaktinformationen und anderer Einstellungen. (Weitere Einzelheiten zu den Geräteeinstellungen finden Sie im Abschnitt „LP50 Einstellungen“ in dieser Bedienungsanleitung.)
LP50 durchsuchen:	• Damit können Ihre gesicherten Dateien angezeigt werden.
LP50 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 – LP50 formatieren**
Online-Support:	• Öffnet Ihren Internetbrowser und navigiert zu http://www.kingston.com/support/, wo Sie Zugang zu weiteren Support-Informationen erhalten.
Über LP50: Hier finden Sie spezifische Informationen über den LP50, einschließlich Informationen zu Anwendung, Firmware und Seriennummer *(Abb. 6.2)*. **Hinweis:** Die individuelle Seriennummer des Laufwerks finden Sie in der Spalte „Informationen (Information)“.	 **Abb. 7.5 – Über den LP50**
LP50 trennen:	• Fährt den LP50 ordnungsgemäß herunter, damit Sie ihn sicher aus Ihrem System entfernen können.

LP50 Einstellungen

Admin-Einstellungen

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

- **Passwort (Password):** Hiermit können Sie das Admin-Passwort bzw. den Hinweis ändern *(Abb. 8.1)*
- **Kontaktinformationen (Contact Info):** Sie können hier Ihre Kontaktangaben hinzufügen, ansehen oder ändern *(Abb. 8.2)*
- **Sprache (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

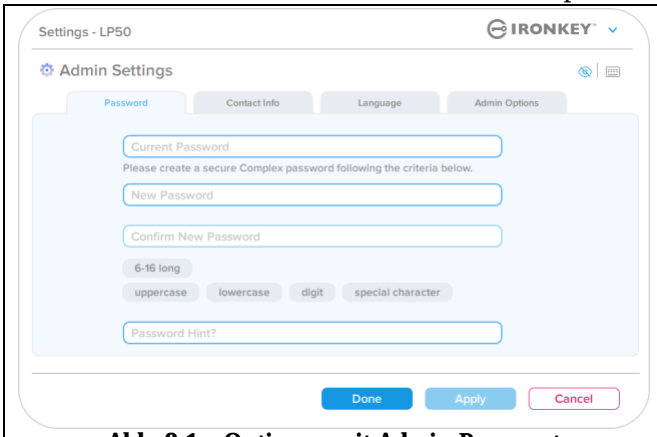


Abb. 8.1 – Optionen mit Admin-Passwort

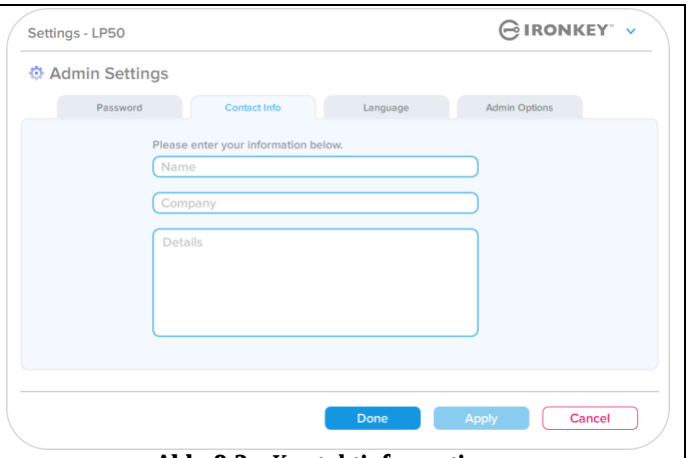


Abb. 8.2 – Kontaktinformationen

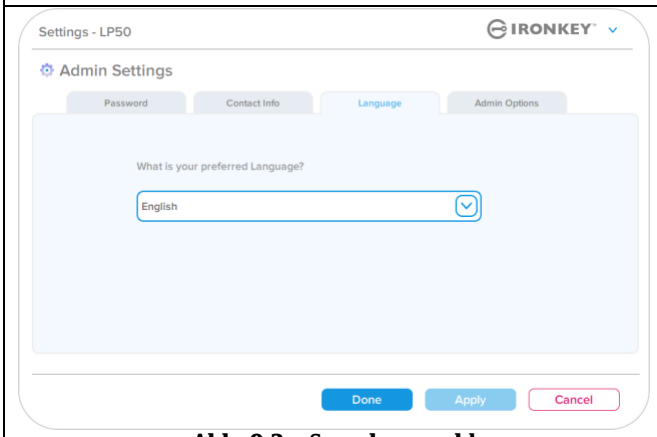


Abb. 8.3 – Sprachauswahl

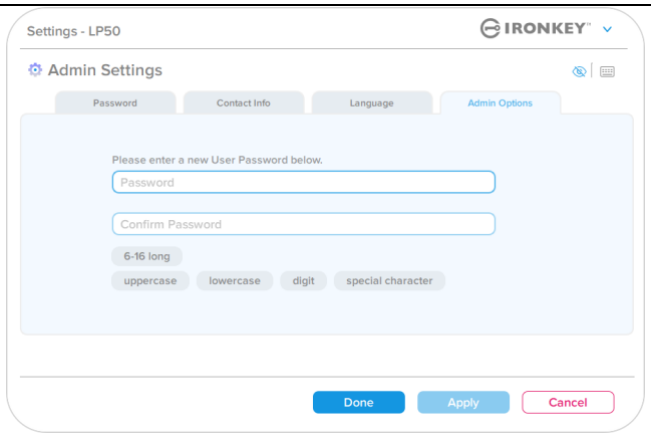
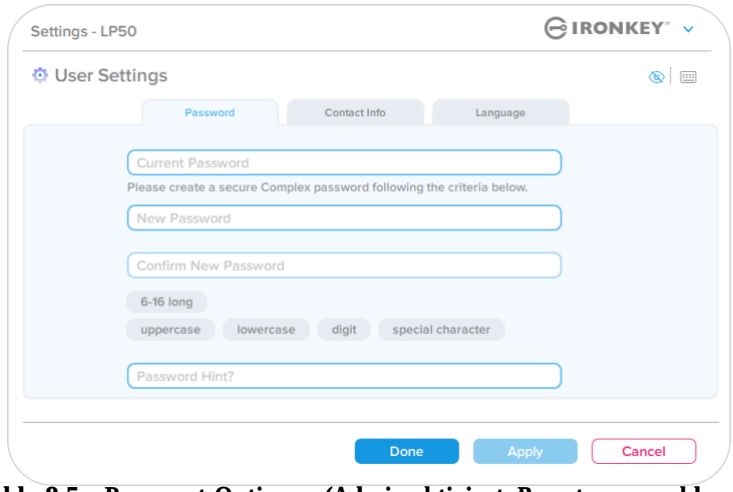
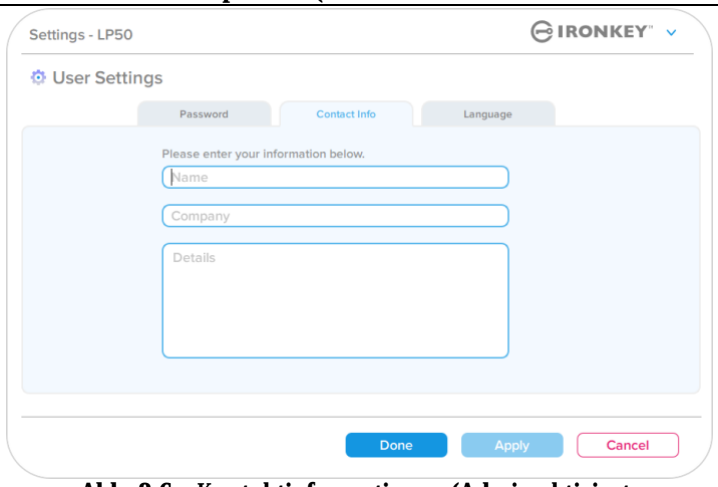
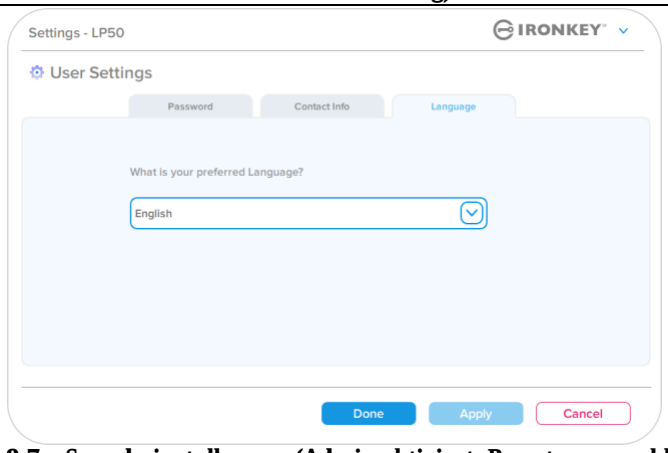


Abb. 8.4 – Admin-Optionen

LP50 Einstellungen

Benutzer-Einstellungen: Admin aktiviert

Die Benutzeranmeldung beschränkt den Zugriff auf die folgenden Einstellungen:

Passwort (Password): 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)**
Sprache (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.

LP50 Einstellungen

Benutzer-Einstellungen: Admin nicht aktiviert

Wie bereits auf Seite 12 erwähnt, führt die Initialisierung des LP50 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 LP50-Einstellungen:

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

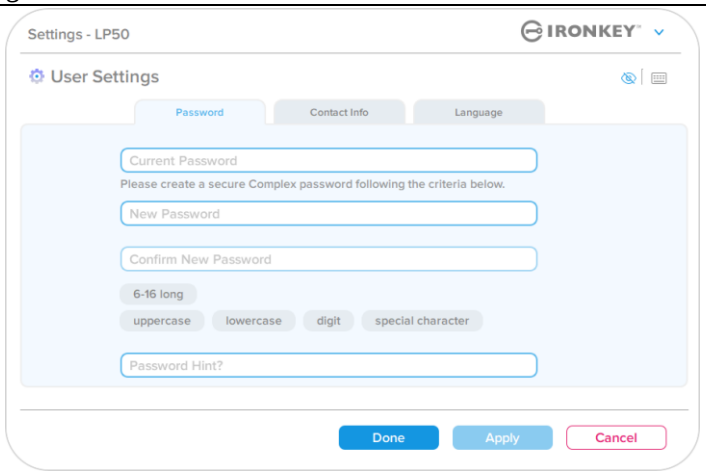


Abb. 8.8 – Passwortoptionen (Nur-Benutzer-Modus)

Kontaktinformationen (Contact Info):
Hiermit können Sie Ihre Kontaktinformationen hinzufügen/anzeigen/ändern. *(Abb. 8.9)*

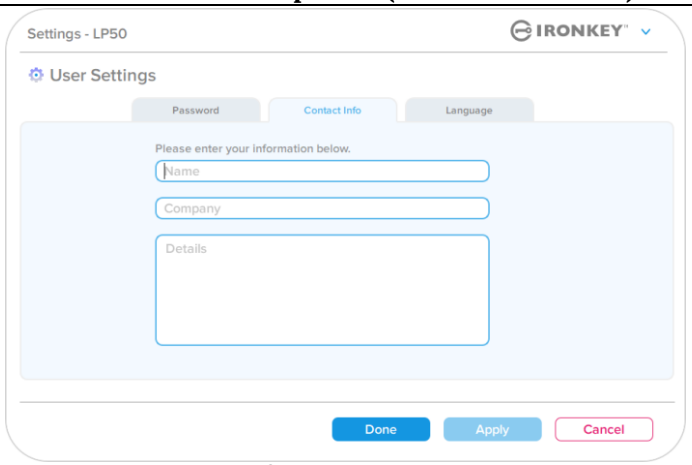


Abb. 8.9 – Kontaktinformationen (Nur-Benutzer-Modus)

Sprache (Language):
Hiermit können Sie Ihre aktuelle Sprachauswahl ändern. *(Abb. 8.10)*

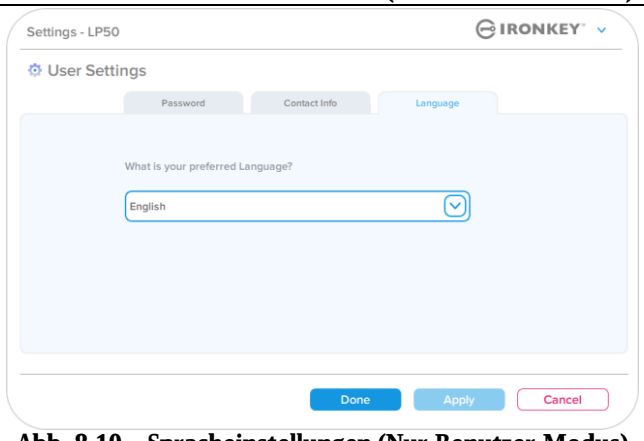


Abb. 8.10 – Spracheinstellungen (Nur-Benutzer-Modus)

LP50 Einstellungen

Ändern und Speichern von Einstellungen

- Wenn Einstellungen in den LP50-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)*

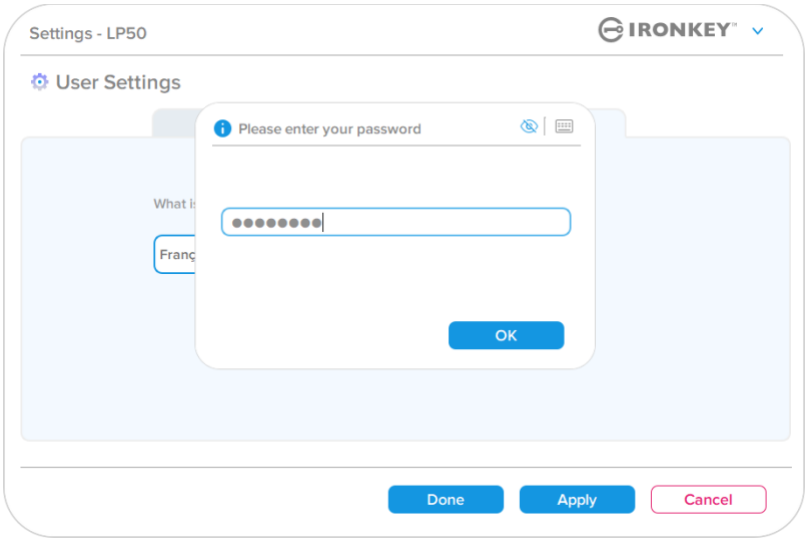


Abb. 8.11 – Bildschirm mit Passwortabfrage zum Speichern von LP50-Einstellungsänderungen

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 „LP50 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“).

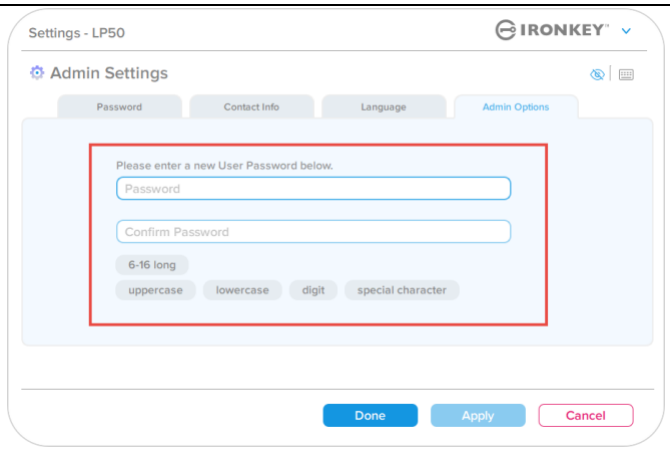


Abb. 9.1 – Admin-Optionen/Benutzer-Passwort zurücksetzen

Hilfe und Fehlerbehebung

Gerätesperrung

Der LP50 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 „Sperrzähler“ registriert jeden fehlgeschlagenen Anmeldeversuch und **kann auf zwei** Wegen 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)*

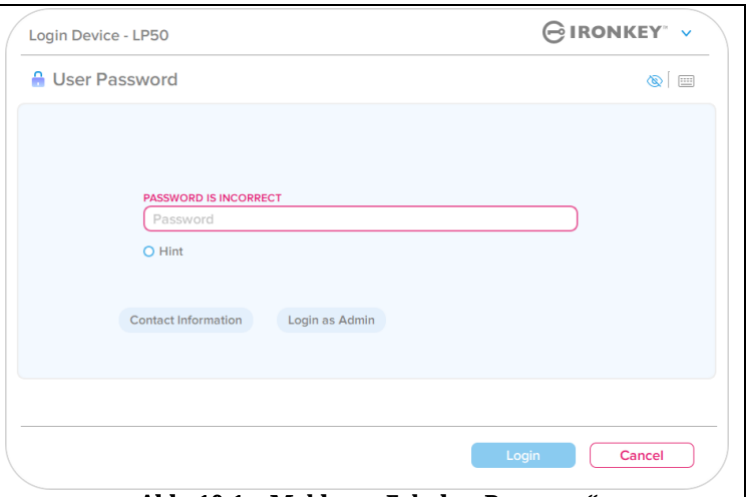


Abb. 10.1 – Meldung „Falsches Passwort“

- 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 verbleiben (der standardmäßig auf 10 eingestellt ist). *(Abb. 10.2)*

Abb. 10.2 – 7. falscher Passworteingabeversuch

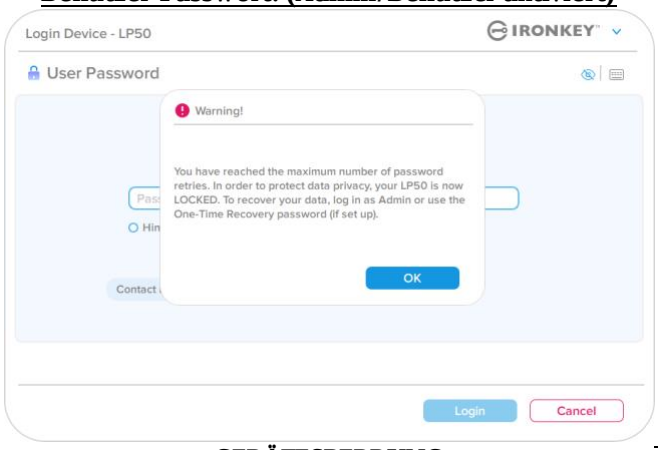
Hilfe und Fehlerbehebung

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 18 dieser Bedienungsanleitung erwähnt werden.

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

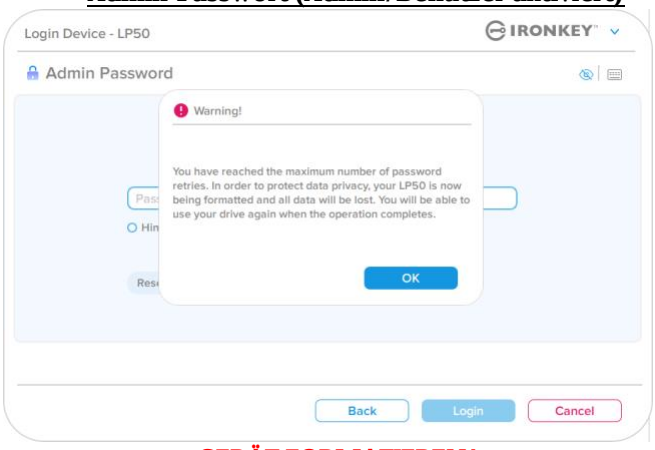
Benutzer-Passwort: (Admin/Benutzer aktiviert)



GERÄTESPERRUNG

Abb. 10.3

Admin-Passwort (Admin/Benutzer aktiviert)

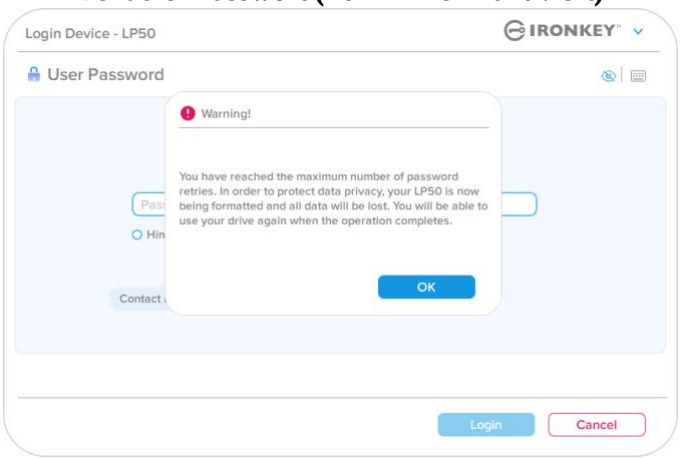


GERÄT FORMATIEREN*

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 LP50 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 25.

Benutzer-Passwort (Admin NICHT aktiviert)



GERÄT FORMATIEREN*

Abb. 10.5

**Hinweis*: *Bei einer Geräteformatierung werden ALLE auf der sicheren Datenpartition des LP50 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 LP50 Launcher ausgeführt wird. (*Siehe Abb. 10.7 und 10.8*)

- Mit dieser Option können Sie ein neues Passwort erstellen, jedoch wird der LP50 zum Schutz Ihrer Daten neu formatiert. Das bedeutet, dass alle Ihre Daten in diesem Prozess unwiederbringlich gelöscht werden.*

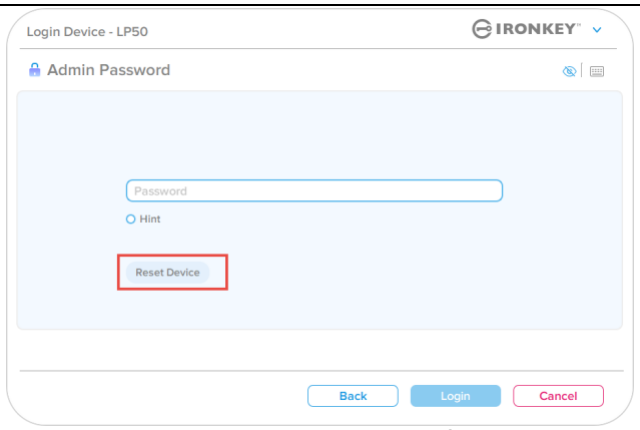


Abb. 10.6 – Admin-Passwort: Schaltfläche „Gerät zurücksetzen (Reset Device)“

- **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 können dies jetzt wahlweise durch 1) Klicken auf „*OK*“ bestätigen, oder 2) durch Klicken auf „Abbrechen (Cancel)“ abbrechen und zum Anmeldefenster zurückkehren. (*Siehe Abb. 10.8*)

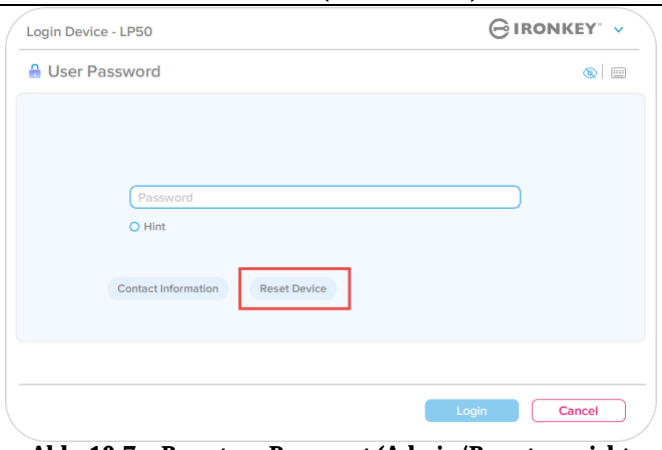


Abb. 10.7 – Benutzer-Passwort (Admin/Benutzer nicht aktiviert) Gerät zurücksetzen

- 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 Passwortoption Sie gewählt haben (Komplex (Complex) oder Passphrase). Der Hinweis ist kein Pflichtfeld, kann jedoch eine nützliche Hilfestellung zur Erinnerung an das Passwort sein, falls Sie es vergessen haben sollten.

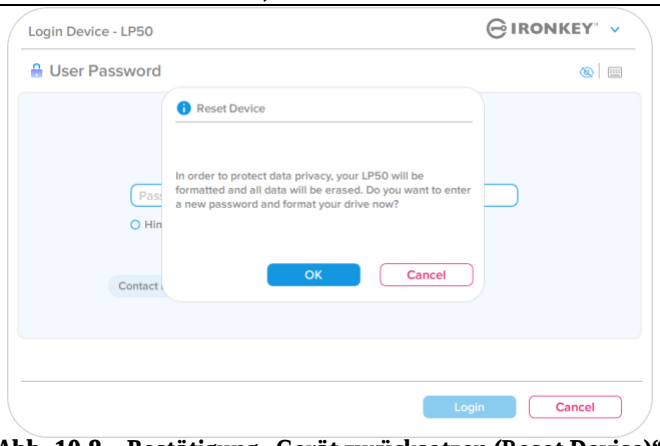


Abb. 10.8 – Bestätigung „Gerät zurücksetzen (Reset Device)“

Hilfe und Fehlerbehebung

Laufwerksbuchstaben-Konflikt: Windows-Betriebssysteme

- Wie bereits im Abschnitt *Systemanforderungen*“, Seite 3 in dieser Anleitung erwähnt, benötigt der LP50 zwei freie, aufeinander folgende 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 LP50 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 Laufwerkbuchstabenzuweisungen in Windows Datenträgerverwaltung (Administratorrechte erforderlich).

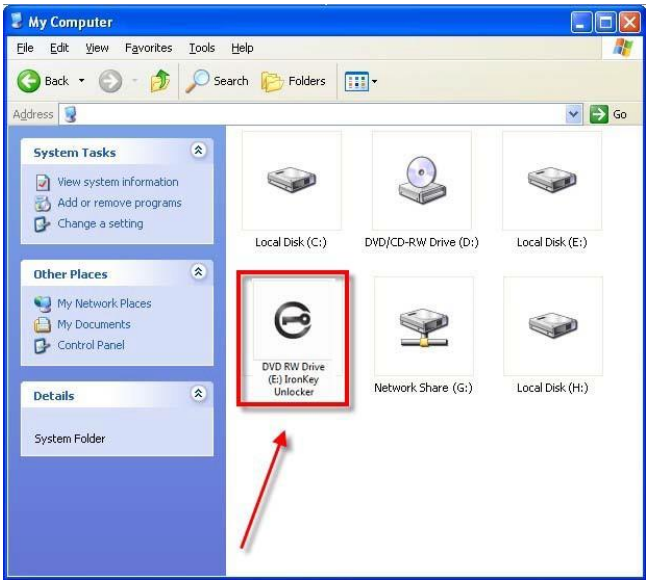


Abb. 10.9 – Beispiel für Laufwerksbuchstaben

In diesem Beispiel (*Abb 9.10*) verwendet der LP50 das Laufwerk „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-Profils ist, kann der LP50 versuchen, ihn als zweiten Laufwerksbuchstaben zu verwenden und dadurch einen Konflikt verursachen.

Wenn es in Ihrem System keine Netzwerkfreigaben gibt und der LP50 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 das „Drive Letter Management (DLM)“ unter Windows 8.1, 10 und 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.

IRONKEY™ Locker+ 50 (LP50)
CLÉ USB SÉCURISÉE 3.2 GEN 1

Guide de l'utilisateur

Sommaire

Figure 1 : IronKey LP50

Introduction

Les clés USB Kingston IronKey Locker+ 50 offrent une sécurité de niveau grand public grâce au chiffrement matériel AES en mode XTS, notamment contre les attaques par Force Brute et BadUSB avec firmware signé numériquement. La LP50 est également conforme à la norme TAA.

La LP50 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 bloque l'Utilisateur après 10 tentatives consécutives de mot de passe invalide et vérouille la clé USB si le mot de passe Admin est entré 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 est conçue pour être pratique. Elle présente un petit boîtier métallique et un porte-clés intégré pour emporter les données partout. La LP50 offre également une fonctionnalité de sauvegarde USBtoCloud (par ClevX®) en option pour accéder à ses données à partir de votre stockage Cloud personnel via Google Drive™, OneDrive (Microsoft®), Amazon Cloud Drive, Dropbox™ ou Box. La LP50 est facile à configurer et à utiliser pour tous, sans aucune installation d'application ; elle intègre déjà tous les logiciels et la sécurité nécessaires. Fonctionne à la fois sur Windows® et macOS® afin que les utilisateurs puissent accéder aux fichiers depuis plusieurs systèmes.

La LP50 bénéficie d'une garantie limitée de 5 ans avec le support technique gratuit de Kingston.

Fonctionnalités de la IronKey Locker+ 50

- Chiffrement matériel XTS-AES (le chiffrement ne peut jamais être désactivé)
- Protection contre les attaques par force brute et BadUSB
- Options de 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 (09242024)
Ce manuel d'utilisation concerne la clé USB IronKey Locker+ 50 (LP50).

Système requis

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 32.	**Systèmes d'exploitation acceptés** • Windows 11 • Windows 10
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 12.x – 15.x

Remarque : Un abonnement gratuit de 5 ans à USB-to-Cloud est inclus avec chaque clé lors de l'activation. Options d'activation continue disponibles à l'achat par ClevX au-delà du délai inclus.

Recommandations

Pour que la LP50 bénéficie d'une alimentation suffisante, elle doit être insérée directement sur un port USB d'un ordinateur portable ou de bureau, comme illustré dans la *Figure 1.1*. Évitez de brancher la LP50 sur un périphérique équipé d'un port USB, par exemple un clavier ou un concentrateur/hub alimenté par USB, comme illustré dans la *Figure 1.2*.

Figure 1.1 – Utilisation conseillée

Figure 1.2- Déconseillé

Utiliser le bon système de fichiers

La IronKey LP50 est livrée préformatée avec le système de fichiers FAT32. Elle 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 les données sont perdues lorsque la clé USB est reformatée.

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 LP50 sur un système cible.
- 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 endommager la clé 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. Veuillez contacter le support technique de Kingston si vous avez des questions ou des problèmes.

Meilleures pratiques pour la configuration des mots de passe
Votre LP50 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 LP50 efface automatiquement les données chiffrées et s'auto-formate aux paramètres d'usine.

Mots de passe multiples
La LP50 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 LP50 peut prendre en charge deux mots de passe différents que vous pouvez utiliser pour récupérer des données : Admin et Utilisateur.

La LP50 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 n'a pas de porte dérobée. Kingston vous recommande de sauvegarder également les données sur d'autres supports. La LP50 peut être réinitialisée et réutilisée, mais les données antérieures seront définitivement supprimées.

Modes de mot de passe
La LP50 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 LP50 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 LP50, 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, les paroles d'une chanson, un vers de poésie, etc. Les bonnes phrases de passe font partie des types de mots de passe les plus difficiles à deviner pour un attaquant, tout en étant plus faciles à retenir pour les utilisateurs.

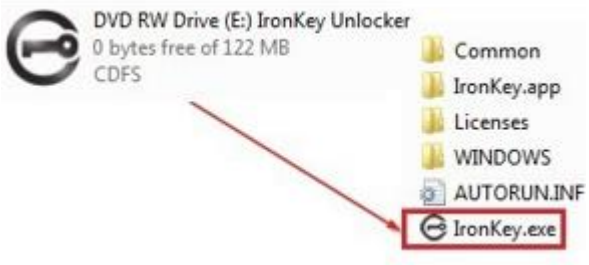
Configurer ma clé USB

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)

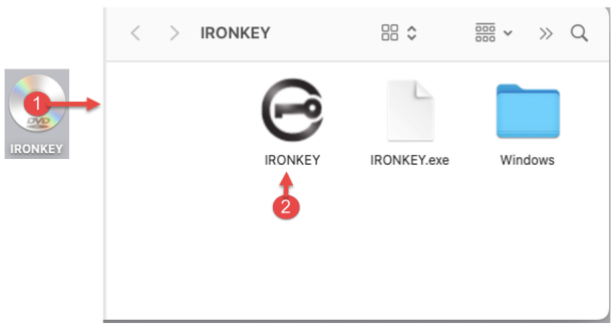
Connectez la clé USB chiffrée IronKey à un port USB disponible de votre ordinateur de bureau ou portable et attendez que Windows la détecte.

• Les utilisateurs de Windows 8.1/10/11 recevront une notification de pilote de la clé USB. (*Figure 3.1*)	 **Figure 3.1 – Notification du pilote de l'appareil**

• 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 – File Explorer Window/IronKey.exe**

Accès à la clé USB (environnement macOS)

Insérez la LP50 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 de 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 démarrera aussi.	 **Figure 3.3 – Volume IKLP**

Initialisation de la clé USB (environnements Windows & macOS)

Langue et Contrat de licence utilisateur final

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

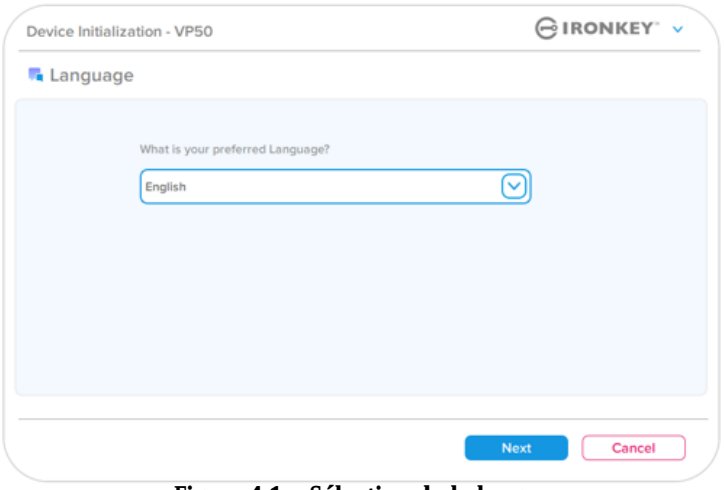


Figure 4.1 – Sélection de la langue

- Lisez le contrat de licence et cliquez sur **Suivant** (Next).

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

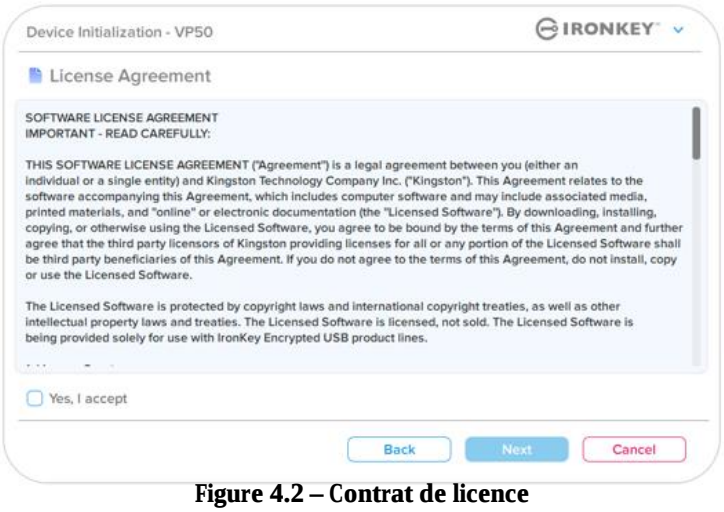


Figure 4.2 – Contrat de licence

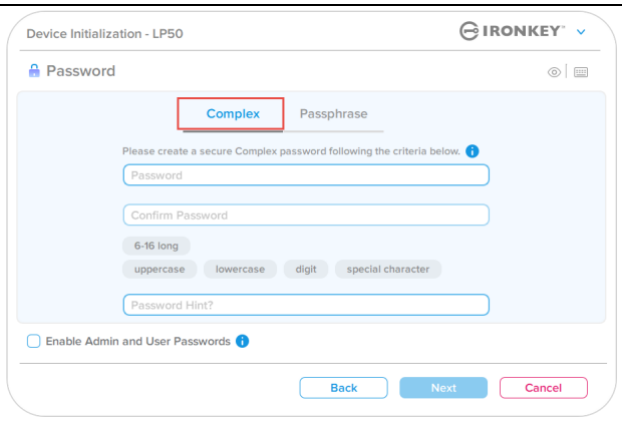
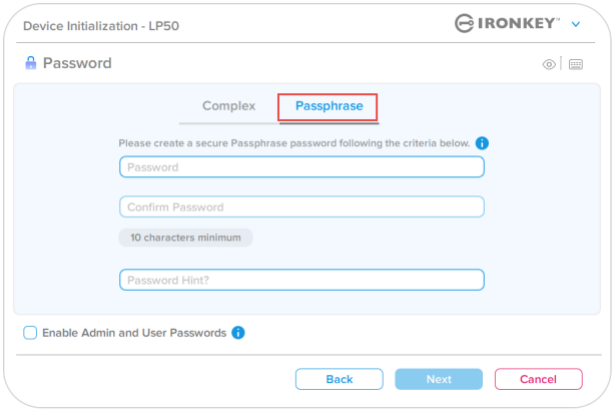
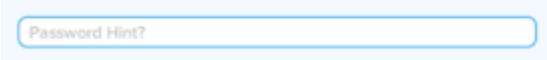
Initialisation de la clé USB

Sélection du mot de passe

Sur l'écran de saisie du Mot de passe, vous pourrez créer un mot de passe pour protéger vos données sur la LP50 en utilisant les modes Complexe ou Phrase de passe (*Figures 4.3- 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' « Mot de passe », puis saisissez-le à nouveau dans le champ '« Confirmer le mot de passe ». Le mot de passe que vous créez doit respecter les critères suivants pour que le processus d'initialisation vous autorise à continuer :

Mot de passe Complex (Complex) • Doit contenir entre 6 et 16 caractères. • Doit contenir trois (3) des types de caractères suivants : o Majuscule o Minuscule o Chiffre o Caractères spéciaux (!,$,&, etc..)	 **Figure 4.3 – Mot de passe Complexe**
Phrase de passe (Passphrase) • Doit contenir : o 10 caractères minimum o 64 caractères maximum	 **Figure 4.4 – Phrase de passe**
Indice de mot de passe (Password Hint) (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 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*)

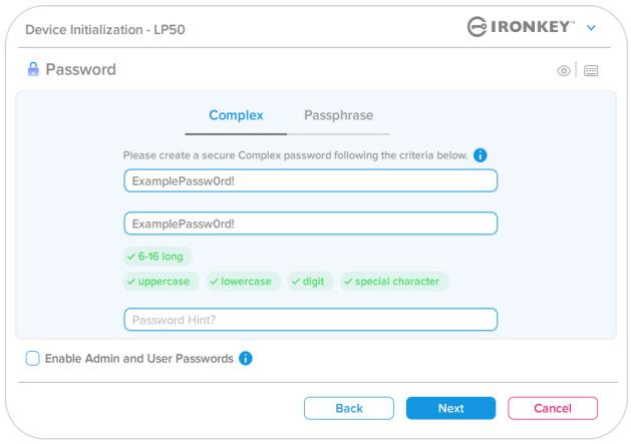


Figure 4.6a – Condition de mot de passe complexe remplie

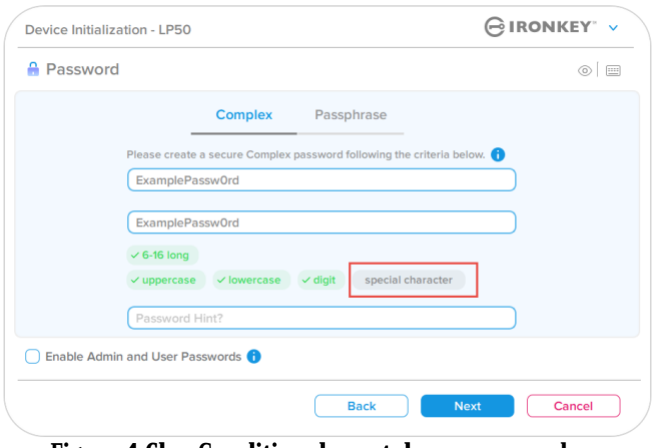


Figure 4.6b – Condition de mot de passe complexe facultative

Pour les mots de passe **non valides**, les cases de critères de mot de passe s'affichent en **rouge** et le bouton **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.

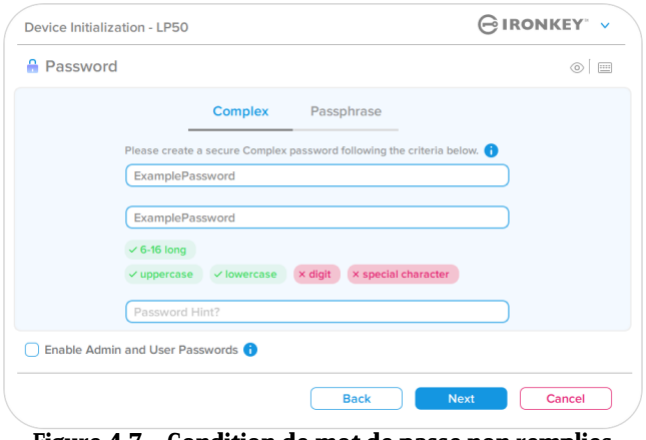


Figure 4.7 – Condition de mot de passe non remplies

Initialisation de la clé USB

Clavier virtuel
La LP50 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 **Initialisation de la clé USB** (Device Initialization) et sélectionnez-le.

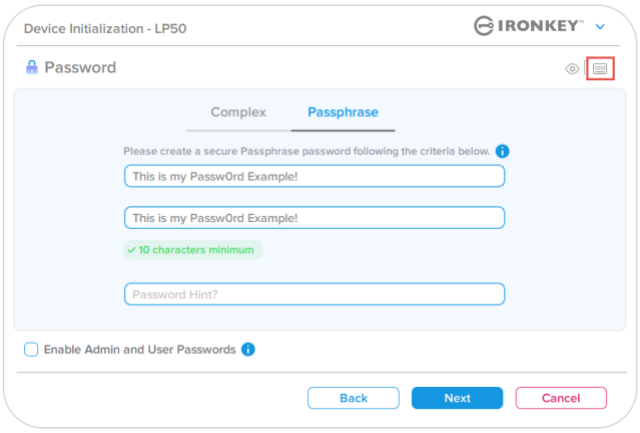


Figure 4.8 – Activation du clavier virtuel

- Une fois que le clavier virtuel apparaît, vous pouvez également activer la fonction **Protection contre les enregistreurs d'écran** (Screenlogger Protection). 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 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, celui-ci 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 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.

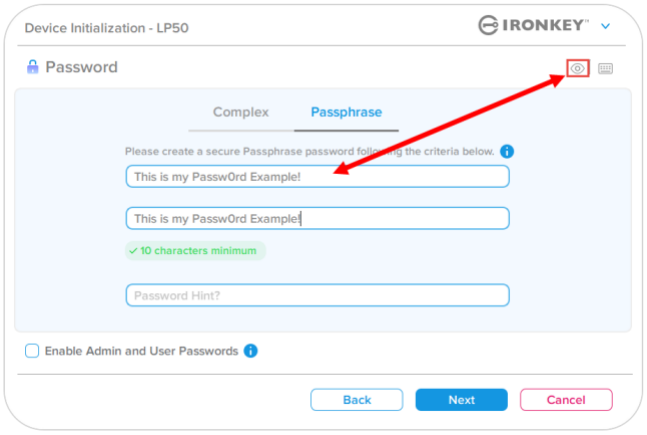


Figure 4.10 - Icône pour '« masquer » le mot de passe

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

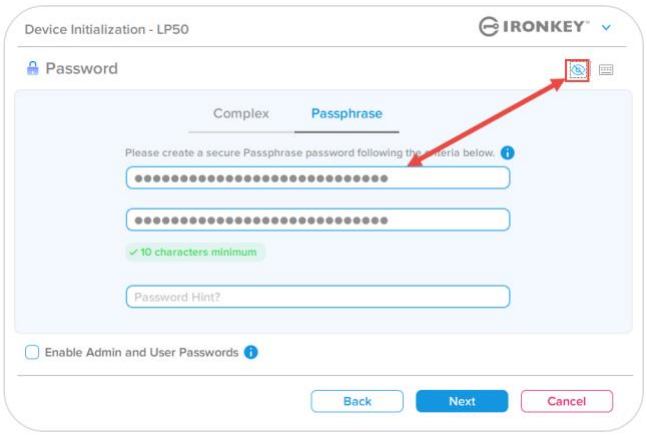


Figure 4.11 - Icône pour '« afficher » le mot de passe

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 '« **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 **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 28 du présent Guide de l'utilisateur.

- Pour activer les **mots de passe Admin et Utilisateur**, cliquez sur la case située à côté de '« **Activer les mots de passe Admin et Utilisateur** » (Enable Admin and User Passwords) et sélectionnez **Suivant** (Next) 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 **Suivant** (Next) pour passer à l'écran **Mot de passe Utilisateur**, où un mot de passe est choisi pour l'Utilisateur.

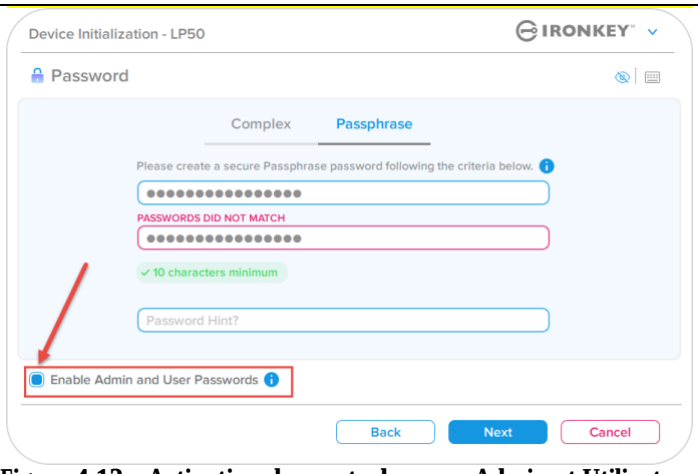


Figure 4.12 – Activation des mots de passe Admin et Utilisateur

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 **Activer les mots de passe Admin et Utilisateur** et cliquez sur **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** (User Password) (*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.

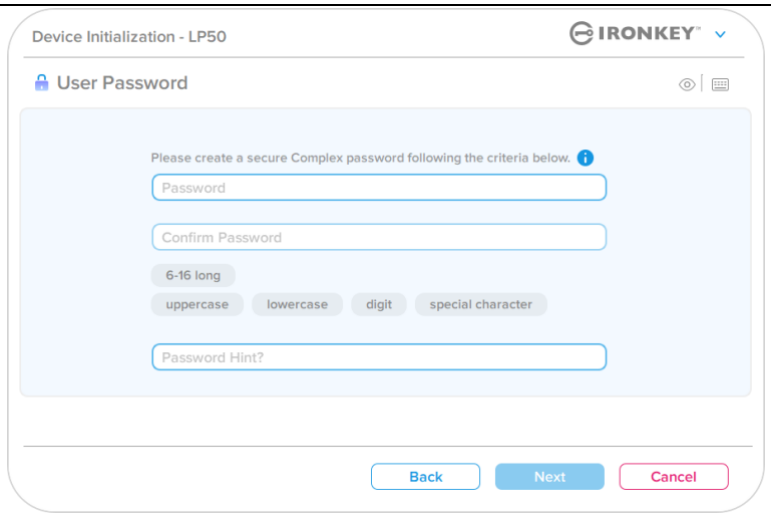


Figure 4.13 – Mot de passe Utilisateur (Admin et Utilisateur activés)

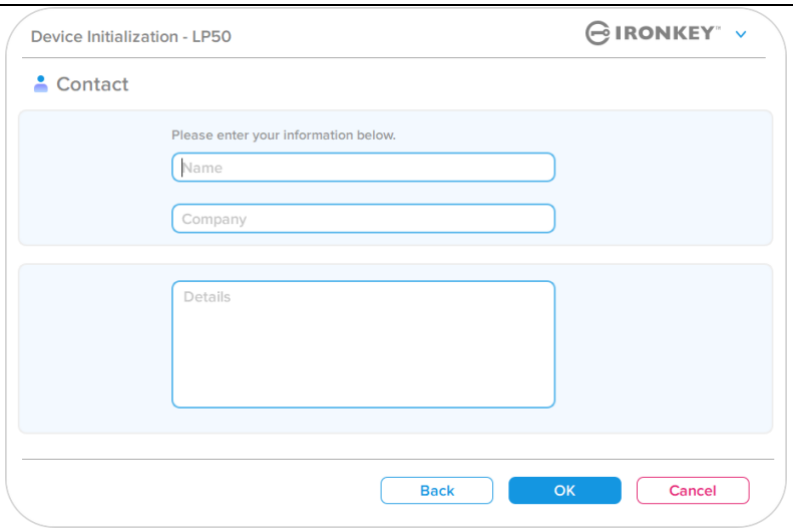
Remarque : Le critère Option de mot de passe choisi (Complexe ou Phrase de passe) sera appliqué au mot de passe Utilisateur, et à toute réinitialisation du mot de passe nécessaire après la configuration de la clé USB. L'option de mot de passe choisie ne peut être modifiée qu'après une réinitialisation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

Initialisation de la clé USB

Informations de contact

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

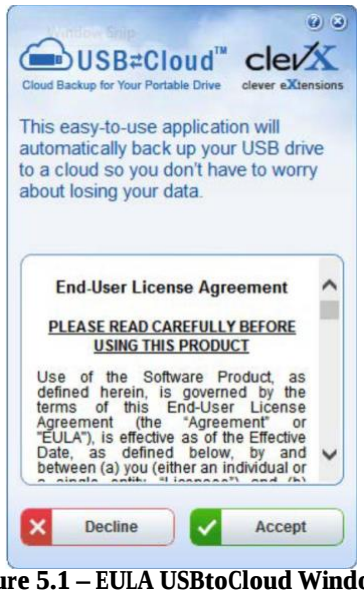
Remarque : Les informations que vous saisissez dans ces champs NE DOIVENT PAS contenir la chaîne de mots de passe que vous avez créée à l'étape 3. Ces champs sont facultatifs et peuvent être laissés vides, si vous le souhaitez.

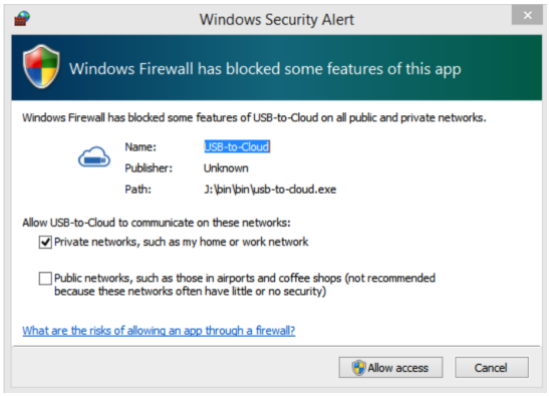
Le champ '« **Nom** » (Name) peut contenir jusqu'à 32 caractères, mais ne doit pas contenir le mot de passe **exact**. Le champ '« **Société** » (Company) peut contenir jusqu'à 32 caractères, mais ne doit pas contenir le mot de passe **exact**. Le champ' « **Détails** » (Details) peut contenir jusqu'à 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.

USB ß → Initialisation du Cloud (environnement Windows)

Une fois la clé initialisée dans Windows, l'application USB-to-Cloud apparaît, comme le montre la *Figure 5.1* à droite. Votre connexion internet doit être active pour continuer.

• Pour lancer l'installation, cliquez sur le bouton vert '« Accepter » (Accept) dans le coin inférieur droit de la fenêtre clevX. • Pour annuler l'installation, cliquez sur le bouton rouge '« Refuser » (Decline) dans le coin inférieur gauche de la fenêtre clevX. • (Remarque : Si vous cliquez sur le bouton rouge' « Refuser », l'installation d'USB-to-Cloud sera annulée. Dans ce cas, un fichier texte spécial intitulé 'USBtoCloudInstallDeclined.txt' sera créé sur la partition de données. Ce fichier évite que l'application vous demande à nouveau de lancer l'installation.)	 **Figure 5.1 – EULA USBtoCloud Windows**

• Si la fenêtre d'alerte de sécurité Windows suivante s'affiche pendant le processus d'initialisation, cliquez sur « Autoriser accès » (ou créez une exception dans le pare-feu Windows) pour que l'application USB-to-Cloud puisse continuer.	 **Figure 5.2 – Alerte de sécurité Windows**

USB ß → Initialisation du Cloud (environnement Windows)

- Lorsque l'installation est terminée, un cadre de l'application affiche une liste d'options à sélectionner (pour synchroniser les données de votre LP50.)
- Sélectionnez l'option Cloud que vous souhaitez utiliser comme application de sauvegarde et saisissez les références d'authentification requises.
- (Remarque : Si vous n'avez pas actuellement un compte configuré avec une des options Cloud listées, vous pouvez en créer un immédiatement, avec votre navigateur internet habituel. Vous pourrez ensuite sélectionner cette option.)
- Après la sélection de l'option Cloud et votre authentification sur le service correspondant, l'application USB-to-Cloud effectuera une comparaison initiale entre la partition de données et les données stockées dans le Cloud. Tant que le service USB-to-Cloud est ouvert dans le Gestionnaire des tâches (Task Manager), les contenus écrits dans la partition de données seront automatiquement sauvegardés (sync) dans le Cloud.

Figure 5.3 – Sélection du Cloud

USB ß → Utilisation de la clé USB (Environnement Windows)

L'application USB-to-Cloud offre les services supplémentaires suivants :

- Mettre la sauvegarde en pause (met momentanément en pause la sauvegarde des données en cours).
- Restaurer (restaure les données depuis le Cloud sur la clé USB).
- Paramètres (Options supplémentaires de votre sauvegarde des données).
- Quitter (ferme le service USB-to-Cloud).

Dans le menu' « Paramètres », vous pouvez :

- Changer l'application de service cloud que vous utilisez actuellement pour les sauvegardes.
- Modifier la langue que vous utilisez actuellement
- Sélectionner les fichiers et/ou dossiers à sauvegarder dans le cloud.
- Vérifier l'existence de mises à jour du logiciel.

(**Remarque :** Si vous réinitialisez (ou formatez) la clé USB LP50, toutes les données qu'elle contient seront perdues. Par contre, toutes les données stockées dans le Cloud restent disponibles et inchangées.)

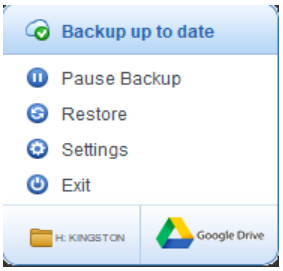


Figure 5.4- Services

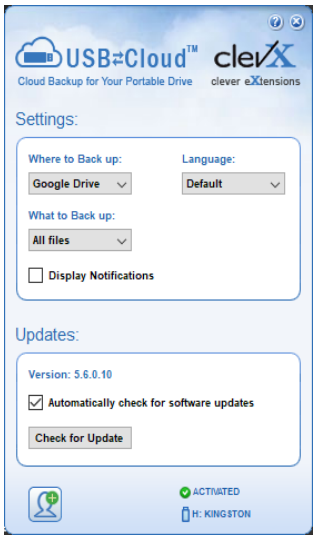


Figure 5.5 - Paramètres

USB ß → Initialisation du Cloud (environnement macOS)

- Une fois la clé initialisée, l'application USB-to-Cloud apparaît, comme le montre la *Figure 5.6* à droite. Votre connexion internet doit être active pour continuer.

- Pour lancer l'installation, cliquez sur le bouton '« Accepter » (Accept) dans le coin inférieur droit de la fenêtre clevX. (Remarque : Sous macOS 12.x +, vous serez invité à autoriser l'accès aux fichiers d'un volume amovible. Sélectionner OK.) (*Voir la Figure 5.7*)

- Pour annuler l'installation, cliquez sur le bouton '« Refuser » (Decline) dans le coin inférieur gauche de la fenêtre clevX.

Figure 5.6 – EULA USBtoCloud macOS

(Remarque : Si vous cliquez sur le bouton '« Refuser », l'installation d'USB-to-Cloud sera annulée. Dans ce cas, un fichier texte spécial nommé 'DontInstallUSBtoCloud' sera créé sur la partition de données. Ce fichier évite que l'application vous demande à nouveau de lancer l'installation.)

- Lorsque l'installation est terminée, vous verrez une fenêtre de l'application affichant une liste d'options à sélectionner (pour synchroniser les données de votre LP50.) (*Figure 5.8*)

Figure 5.7- Accès macOS

- Sélectionnez l'option Cloud que vous souhaitez utiliser comme application de sauvegarde et saisissez les références d'authentification requises

  (Remarque : Si vous n'avez pas actuellement un compte configuré avec une des options Cloud listées, vous pouvez en créer un immédiatement, avec votre navigateur internet habituel. Vous pourrez ensuite sélectionner cette option.)

- Après la sélection de l'option Cloud et votre authentification sur le service correspondant, l'application USB-to-Cloud effectuera une comparaison initiale entre la partition de données et les données stockées dans le Cloud. Tant que le service USB-to-Cloud est ouvert dans le Gestionnaire des tâches (Task Manager), les contenus écrits dans la partition de données seront automatiquement sauvegardés (sync) dans le Cloud.

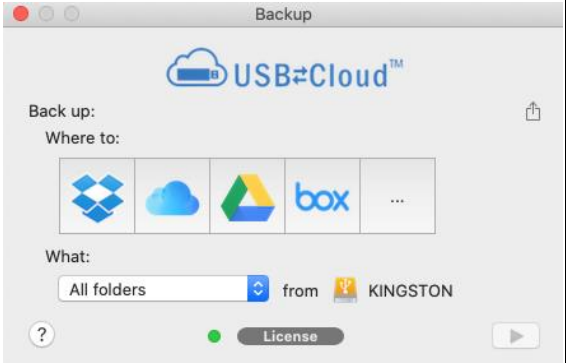


Figure 5.8 – Sélection du Cloud

USB ß →Utilisation du Cloud (environnement macOS)

L'application USB-to-Cloud offre les services supplémentaires suivants (*Figure 5.9*) :

- **Mettre la sauvegarde en pause** (met momentanément en pause la sauvegarde des données en cours)
- **Restaurer** (restaure les données depuis le Cloud sur la clé USB)
- **Sauvegarder** (ouvre les options Cloud) *Voir la Figure 5.9*
- **Quitter** (ferme le service USB-to-Cloud)

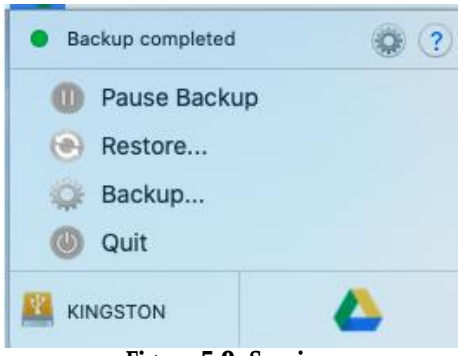


Figure 5.9- Services

Dans le menu '« Préférences », vous pouvez :

- Modifier la langue que vous utilisez actuellement
- Activer/désactiver les notifications sonores
- Activer/désactiver le démontage de la clé USB si l'application est quittée
- Activer/désactiver la journalisation pour le dépannage
- Activer/désactiver les mises à jour logicielles automatiques et vérifier les mises à jour maintenant

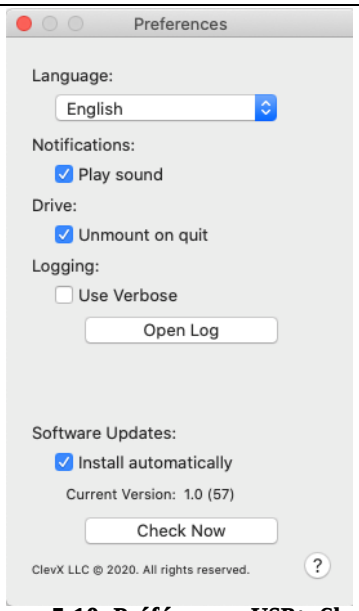


Figure 5.10- Préférences USBtoCloud

Utilisation de la clé USB (environnements Windows & 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 IronKey LP50 se lancera, en affichant d'abord l'écran de connexion 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 '« Se connecter en tant qu'Admin » (Login as Admin) (illustré ci-dessous), l'application passe au menu de connexion Admin, où vous pouvez vous connecter en tant qu'administrateur pour accéder aux paramètres et fonctionnalités Admin (*Figure 6.2*).

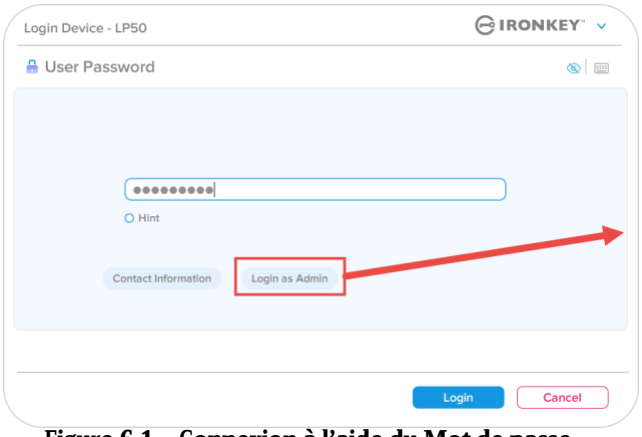


Figure 6.1 – Connexion à l'aide du Mot de passe Utilisateur (Admin activé)

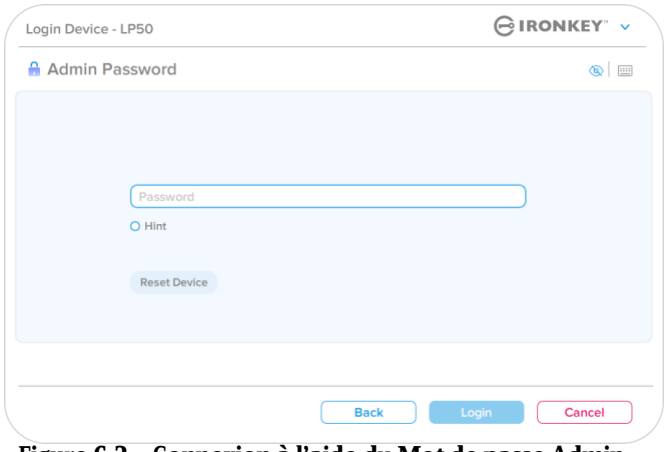


Figure 6.2 – Connexion à l'aide du Mot de passe Admin

Connexion pour le mode Utilisateur uniquement (Admin non activé)

Comme indiqué précédemment à la **page 13**, bien qu'il soit recommandé d'utiliser la fonctionnalité du rôle Admin pour tirer pleinement parti de votre clé, 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 **Réinitialiser la clé USB** (Reset Device) 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.**

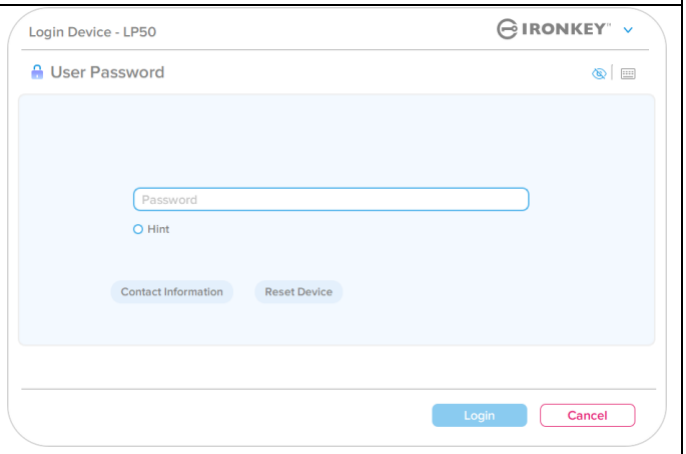


Figure 6.3 – Connexion à l'aide du mot de passe Utilisateur (Admin non activé)

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 (10 tentatives de saisie de mot de passe ratées)**	**Suppression des données et réinitialisation de la clé USB ?**
Mot de passe Utilisateur :	Verrouillage du mot de passe. Connectez-vous en tant qu'Administrateur pour réinitialiser le mot depasse Utilisateur	NON
Mot de passe Admin	Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimées définitivement	**OUI**
Utilisateur uniquement Un seul utilisateur, un seul mot de passe (Admin/Utilisateur NON activé)	**Protection contre les attaques par force brute Comportement de la clé (10 tentatives de saisie de mot de passe ratées)**	**Suppression des données et réinitialisation de la clé USB ?**
Mot de passe Utilisateur	Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimées définitivement	**OUI**

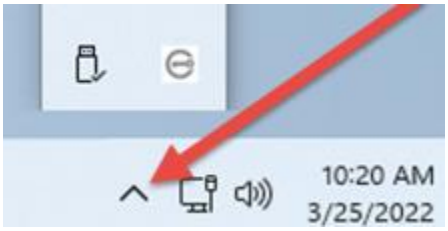
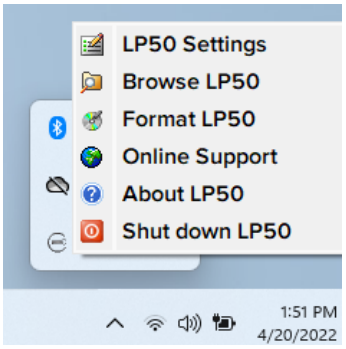
* Une fois que vous vous êtes authentifié avec succès sur la clé USB, le compteur d'échecs de connexion sera réinitialisé en fonction de la méthode de connexion utilisée. L'effacement chiffré effacera tous les mots de passe, les clés de chiffrement et les données ; **vos données seront perdues définitivement.**

Accès à mes fichiers sécurisés

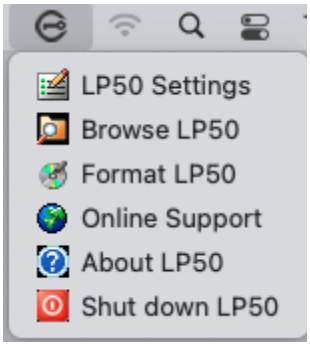
Après avoir déverrouillé la clé USB, vous pouvez accéder à vos fichiers sécurisés. Les fichiers sont automatiquement chiffrés et déchiffrés lorsque vous les enregistrez ou les ouvrez sur la clé USB. Cette technologie vous permet de travailler comme vous le feriez avec une clé USB ordinaire, tout en offrant une sécurité forte 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 et en cliquant sur **Parcourir la LP50** (*Figure 7.2*).

Options de la clé USB (environnement Windows)

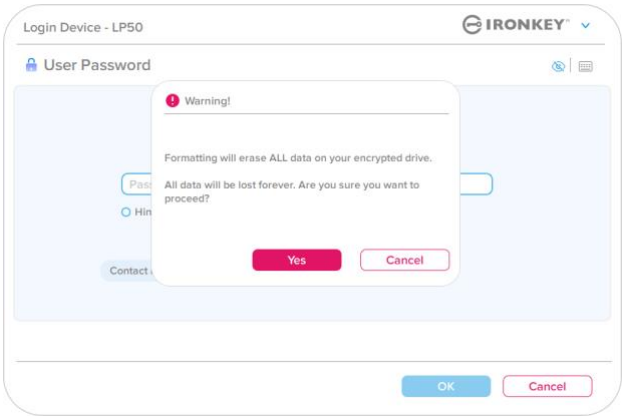
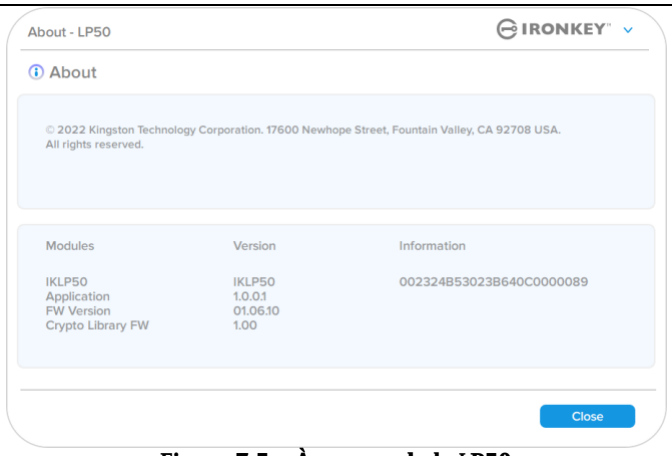
Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles (*Figure 6.2*).
Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.

• Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. (*Figure 7.1*)	 **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. (*Figure 7.2*) 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 LP50 » se trouve dans le menu macOS illustré dans la ***Figure 7.3*** ; elle permet d'afficher les options disponibles de la clé USB. Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.	 **Figure 7.3 – Barre de menu macOS, icône/menu des options de la clé USB**

Options de la clé USB

Paramètres de la LP50 :	• Changer 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 LP50 » du présent manuel).
Parcourir la LP50 :	• Permet de visualiser vos fichiers sécurisés.
Formater la LP50 : Permet de formater la partition de données sécurisée. (Avertissement : Toutes les données seront supprimées) (*Figure 6.1*) **Remarque :** L'authentification par mot de passe sera requise pour le formatage.	 **Figure 7.4 – Formater la LP50**
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.
À propos de la LP50 : Affiche des données détaillées sur la LP50, 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 LP50**
Arrêter la LP50 :	• Permet de fermer correctement la LP50 avant de la déconnecter physiquement du système, en toute sécurité.

Paramètres de la LP50

Paramètres administrateur

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

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

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

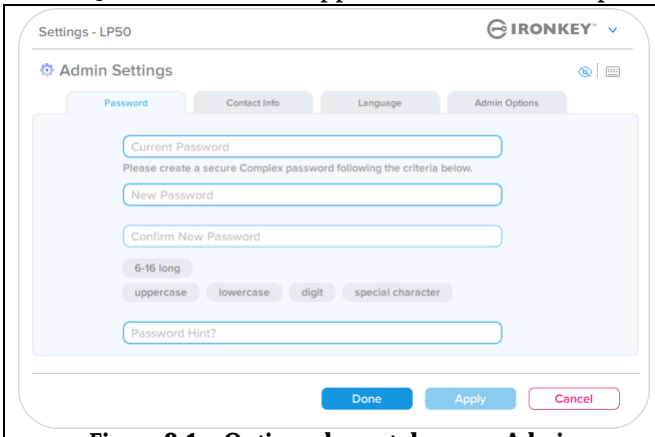


Figure 8.1 – Options du mot de passe Admin

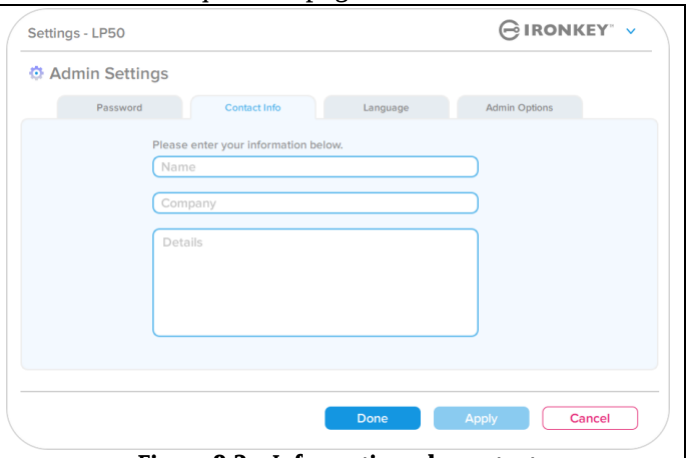


Figure 8.2 – Informations de contact

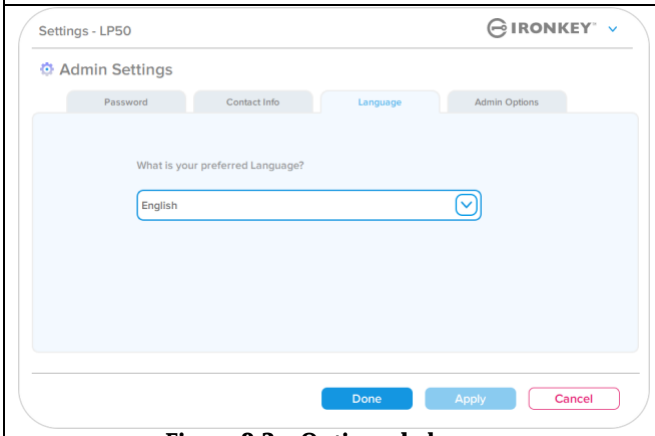


Figure 8.3 – Options de langue

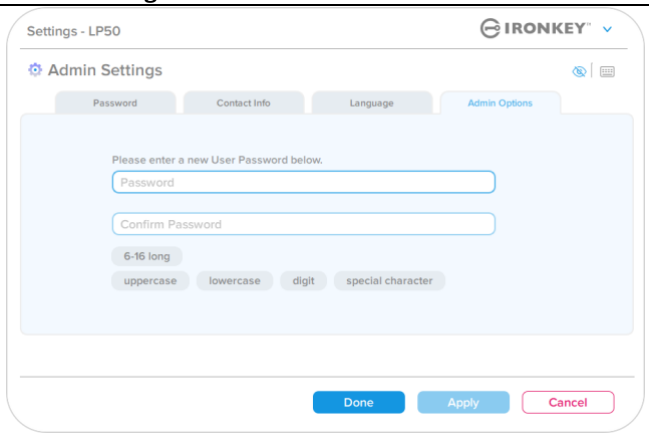


Figure 8.4 – Options Admin

Paramètres de la LP50

Paramètres utilisateur : Admin activé

La connexion Utilisateur limite l'accès aux paramètres suivants :

Mot de passe (Password) :
Permet de modifier le mot de passe Utilisateur et/ou l'indice. (*Figure 8.5*)

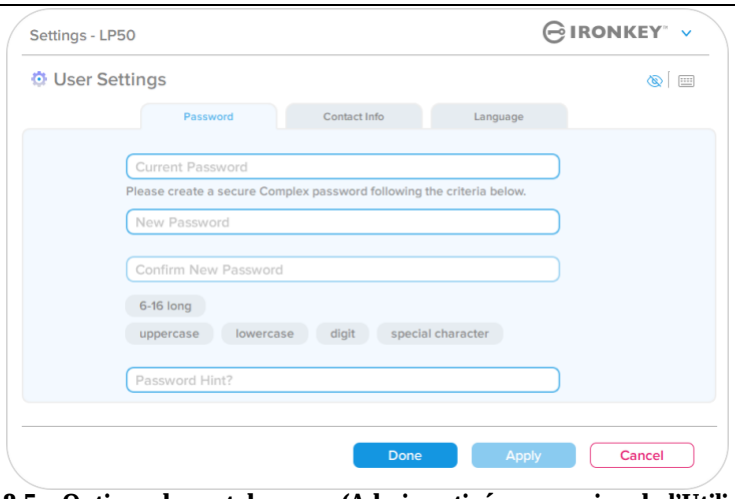


Figure 8.5 – Options de mot de passe (Admin activé : connexion de l'Utilisateur)

Informations de contact (Contact Info) :
Permet d'ajouter/d'afficher/de modifier les informations de contact. (*Figure 8.6*)

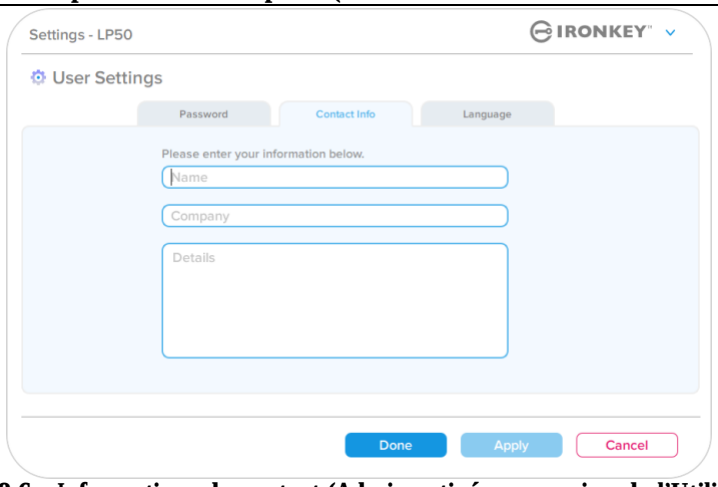


Figure 8.6 – Informations de contact (Admin activé : connexion de l'Utilisateur)

Langue (Language) :
Permet de modifier votre sélection de langue actuelle. (*Figure 8.7*)

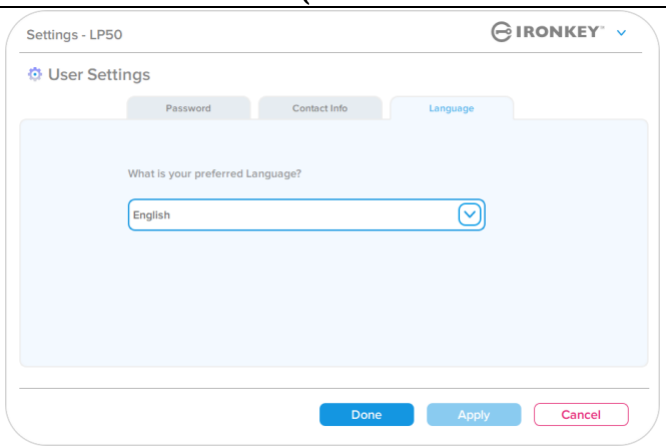


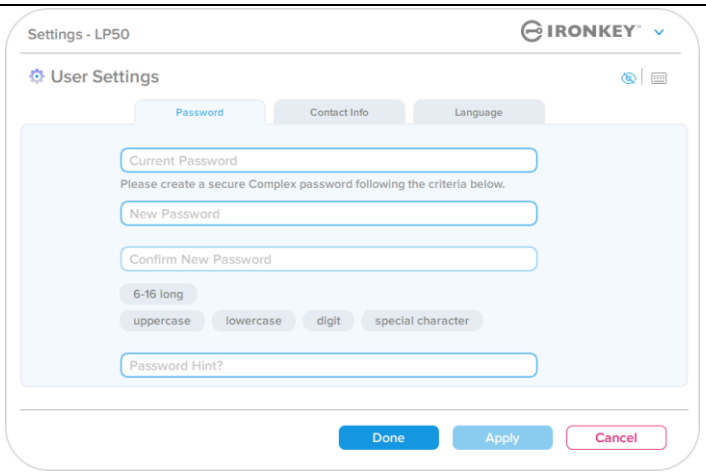
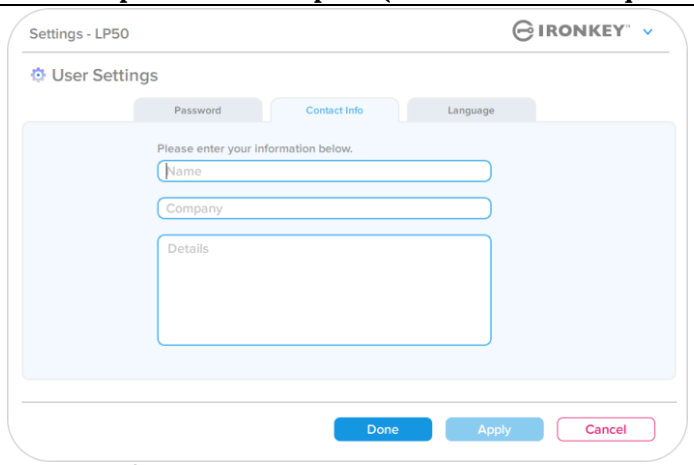
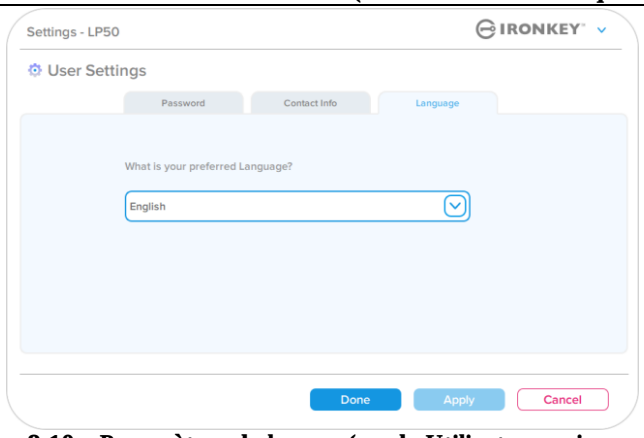
Figure 8.7 – Paramètres de langue (Admin activé : connexion de l'Utilisateur)

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

Paramètres de la LP50

Paramètres utilisateur : Admin non activé

Comme mentionné précédemment à la page 12, l'initialisation de la LP50 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 LP50 :

Mot de passe (Password) : 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)**
Informations de contact (Contact Info) : Permet d'ajouter/d'afficher/de modifier les informations de contact. (Figure 8.9)	 **Figure 8.9 – Informations de contact (mode Utilisateur uniquement)**
Langue (Language) : Permet de modifier votre sélection de langue actuelle. (*Figure 8.10*)	 **Figure 8.10 – Paramètres de langue (mode Utilisateur uniquement)**

Paramètres de la LP50

Modifier et sauvegarder les paramètres

- Chaque fois que les paramètres sont modifiés dans les Paramètres de la LP50 (par exemple : Informations de contact, langue, modification du mot de passe, options Admin, etc.), la clé USB vous invitera à saisir votre mot de passe afin d'accepter et d'appliquer ces modifications. (*Voir la Figure 8.11*)

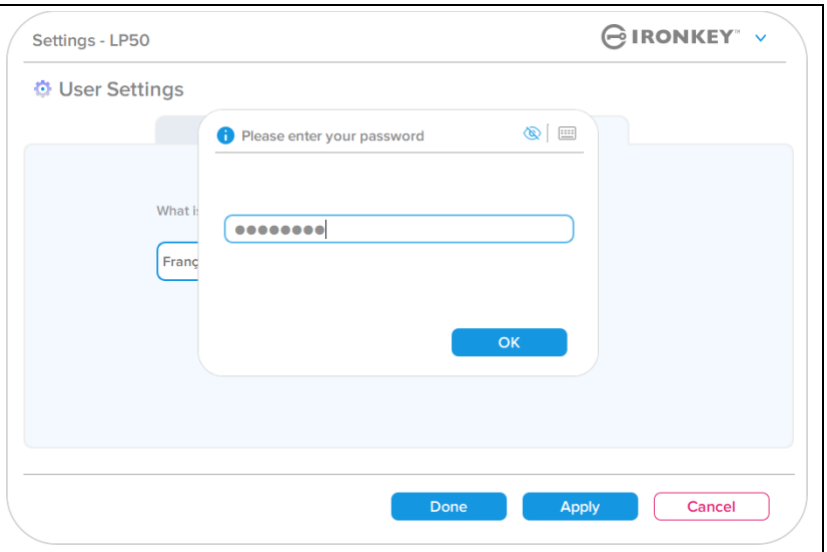


Figure 8.11 – Écran de saisie du mot de passe pour sauvegarder les modifications des paramètres de la LP50

Remarque : Si vous êtes sur l'écran de saisie 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 » (OK). Cela fermera la boîte de dialogue '« Veuillez saisir votre mot de passe » et vous ramènera au menu des paramètres de la LP50.

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, si jamais il est oublié. Vous trouverez ci-dessous la fonctionnalité Réinitialisation du mot de passe Utilisateur, laquelle peut être utile pour réinitialiser le mot de passe Utilisateur :

Réinitialisation du mot de passe Utilisateur :
Changer manuellement le mot de passe Utilisateur dans le menu '« Options Admin ». Ce changement est instantané ; il prendra effet à la prochaine connexion de l'Utilisateur. (*Figure 9.1*)

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

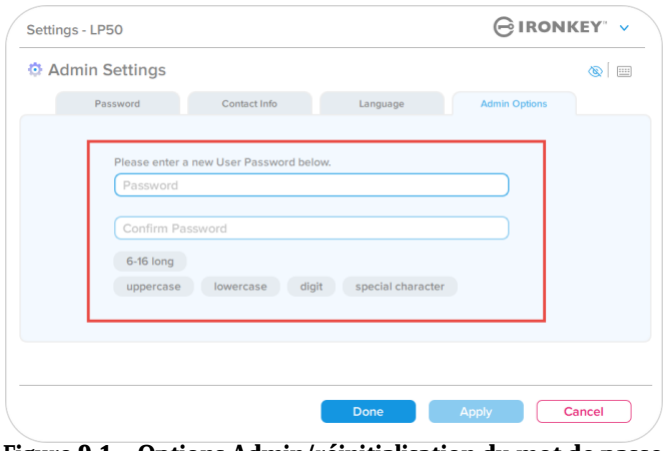


Figure 9.1 – Options Admin/réinitialisation du mot de passe Utilisateur

Aide et dépannage

Verrouillage de la clé USB

La LP50 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 **consécutives** ratées (« MAX » pour faire court). Par défaut, ce nombre de tentatives ratées 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 **7ème** 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*)

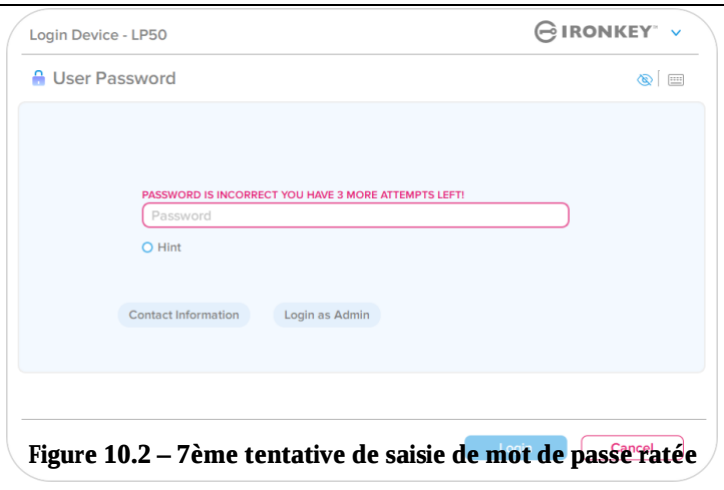


Figure 10.2 – 7ème tentative de saisie de mot de passe ratée

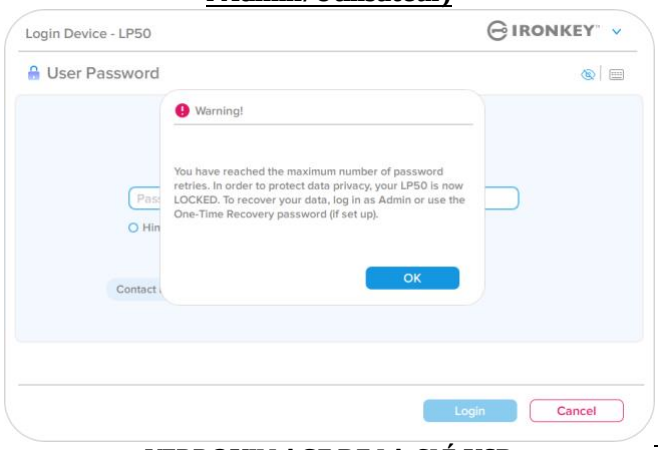
Aide et dépannage

Verrouillage de la clé USB

Important : Après la **10ème** et dernière tentative de connexion ratée, 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 18 de ce Guide de l'utilisateur.

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

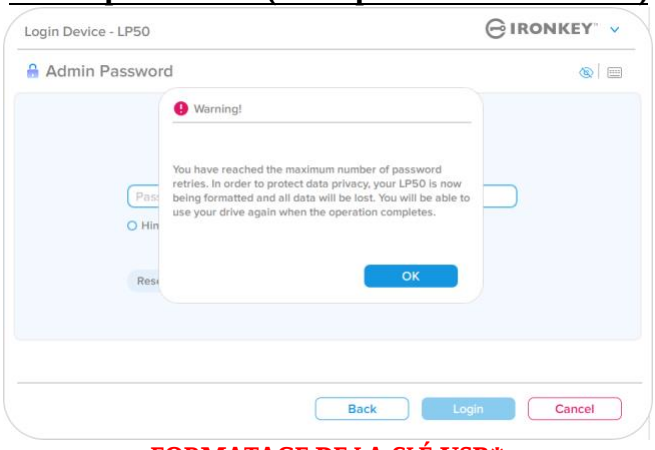
Mot de passe Utilisateur : (activé par l'Admin/Utilisateur)



VERROUILLAGE DE LA CLÉ USB

Figure 10.3

Mot de passe Admin (activé par l'Admin/Utilisateur)

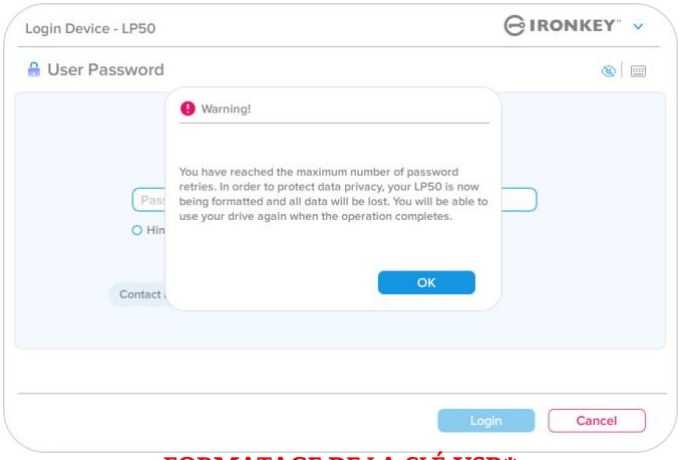


FORMATAGE DE LA CLÉ USB*

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 la force brute). Si vous êtes le propriétaire de la LP50 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* », page 25.

Mot de passe utilisateur (Admin NON activé)



FORMATAGE DE LA CLÉ USB*

Figure 10.5

** Remarque : Un formatage de la LP50 supprimera TOUTES les informations stockées sur sa partition de données sécurisée.*

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 '« Réinitialiser la clé USB » qui peut apparaître à deux endroits selon la configuration de la clé (soit dans le menu Mot de passe de connexion Admin si le mode Admin/Utilisateur est activé, soit dans le menu' « Mot de passe de connexion Utilisateur » si le mode Admin/Utilisateur n'est pas activé) lorsque le programme LP50 Launcher est exécuté. (*voir la Figure 10.7 et la Figure 10.8*)

- Cette option vous permet de créer un nouveau mot de passe, mais pour protéger la confidentialité de vos données, la LP50 sera formatée. Par conséquent, ce processus effacera définitivement toutes vos données.*

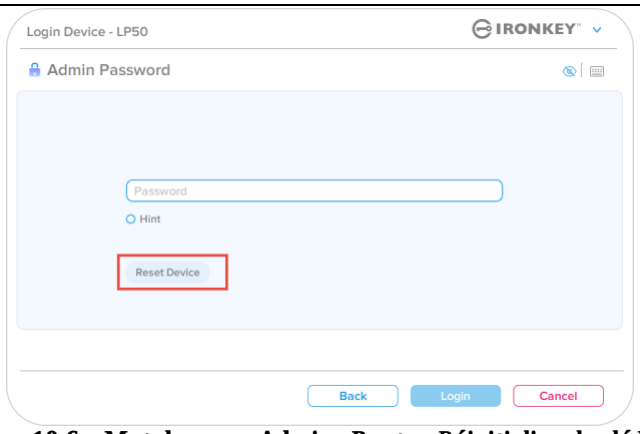


Figure 10.6 – Mot de passe Admin : Bouton Réinitialiser la clé USB

- **Remarque :** Lorsque vous cliquez sur le bouton' « *Réinitialiser la clé USB* » (Reset Device), 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 '« Annuler » pour revenir à la fenêtre de connexion. (*Voir la Figure 10.8*)

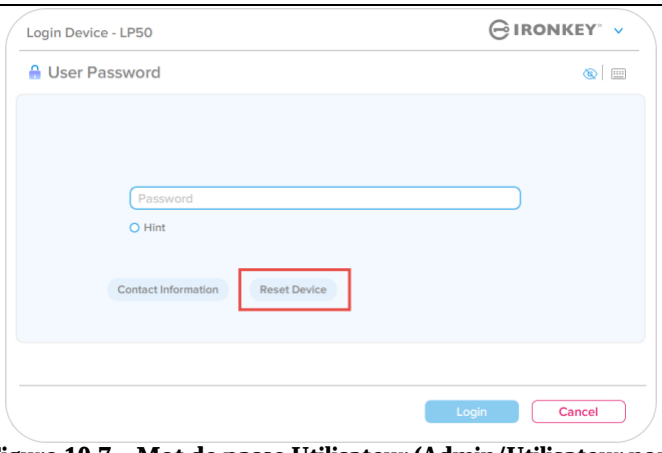


Figure 10.7 – Mot de passe Utilisateur (Admin/Utilisateur non activé) – Réinitialiser la clé USB

- 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.

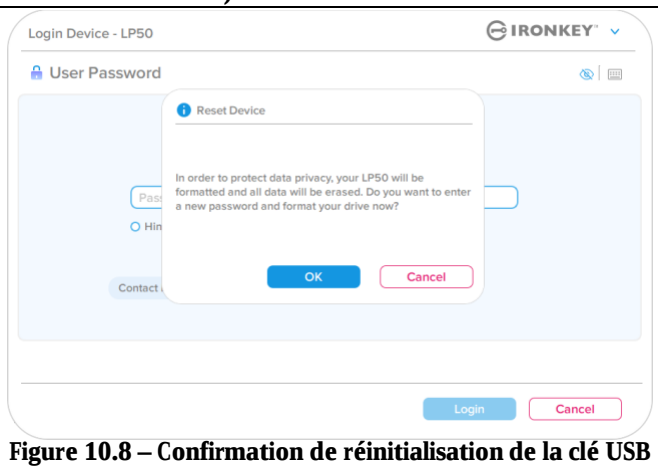


Figure 10.8 – Confirmation de réinitialisation de la clé USB

Aide et dépannage

Conflit de lettres de lecteur : environnements Windows

- Comme indiqué dans la section « *'Configuration système* » du présent manuel (page 3), la LP50 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 (*voir la Figure 10.9*). Cela ne concerne PAS les partages réseau car ils sont spécifiques aux profils d'utilisateur et non au profil matériel du système lui-même, et apparaissent donc disponibles pour le système d'exploitation.

- Autrement dit, Windows peut attribuer à la LP50 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).

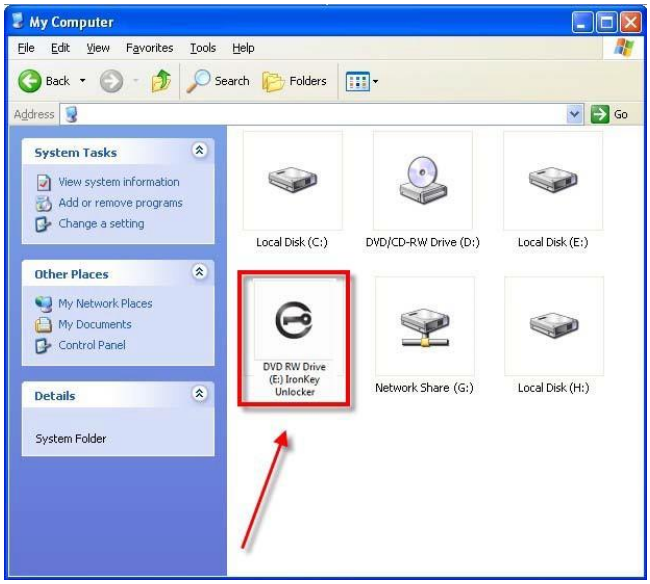


Figure 10.9 – Exemple de lettre de lecteur

Dans cet exemple (*Figure 10.9*), la LP50 utilise le lecteur F:, qui est la première lettre de lecteur disponible après le lecteur E: (le dernier disque physique avant l'écart entre les lettres de lecteur). Comme la lettre G: est un partage réseau et qu'elle ne fait pas partie du profil matériel, la LP50 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 LP50 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 8.1, 10 et 11 et 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.

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

Guida per l'utente

Contenuti

Figura 1: IronKey LP50

Introduzione

I drive flash USB Kingston IronKey Locker+ 50 offrono sicurezza di classe consumer con crittografia hardware AES in modalità XTS, comprese le protezioni contro attacchi BadUSB con firmware con firma digitale e funzionalità di prevenzione contro gli attacchi con password Brute Force. Il drive LP50 è anche conforme allo standard TAA.

Il drive LP50 ora supporta l'opzione multipassword (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. Inoltre, una tastiera virtuale integrata protegge le password da keylogger o screenlogger.

Locker+ 50 è progettato per garantire la massima praticità, con un piccolo involucro di metallo e un'asola di aggancio integrata per portare i dati ovunque. LP50 dispone anche del backup USBtoCloud® opzionale (di ClevX®) per accedere ai dati sul drive dal tuo archivio cloud personale tramite Google Drive™, OneDrive (Microsoft®), Amazon Cloud Drive, Dropbox™ o Box. LP50 è facile da configurare e utilizzare, senza che sia richiesta l'installazione di applicazioni; tutto il software e la sicurezza necessari sono già sul drive. Compatibile con Windows® e macOS®, in modo che gli utenti possano accedere ai file da più sistemi.

Il drive LP50 è supportato da una garanzia limitata di 5 anni, con servizio di supporto tecnico Kingston gratuito.

Funzionalità di IronKey Locker+ 50

- Crittografia hardware XTS-AES (funzione crittografica non disattivabile)
- Protezione contro gli attacchi brute force e BadUSB
- Funzione multi password opzionale
- Modalità con password complessa o frase password
- Pulsante di attivazione icona “occhio”, per visualizzare le password inserite e minimizzare il rischio di inserimento di password errate
- Tastiera virtuale , che offre protezione contro keylogger e screenlogger
- Compatibile con sistemi operativi Windows e macOS (consultare la scheda tecnica per ulteriori dettagli)

Informazioni sulla guida (09242024)
Questa guida utente descrive il dispositivo IronKey Locker+ 50 (LP50).

Requisiti di sistema

Piattaforma PC • Intel & AMD • 15 MB 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 32.	**Supporto per sistemi operativi per PC** • Windows 11 • Windows 10
Piattaforma Mac • Intel & Apple SOC • 15 MB di spazio libero su disco • Porta USB 2.0 - 3.2	**Supporto per sistemi operativi per Mac** • macOS 12.x – 15.x

Nota: Sottoscrizione gratuita per 5 anni a USB-to-Cloud inclusa con ogni drive, all'atto dell'attivazione. Possibilità opzionale di proseguire l’attivazione con l’acquisto di ClevX oltre il periodo di sottoscrizione standard.

Raccomandazioni

Per garantire una potenza adeguata al funzionamento del drive LP50, collegarlo direttamente a una porta USB sul computer notebook o desktop, come illustrato in *Figura 1.1*. Evitare di collegare il drive LP50 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 utilizzo raccomandati

Figura 1.2 - Metodi di utilizzo sconsigliati

Utilizzo del file system corretto
Il drive IronKey LP50 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 tenere i dati al sicuro, Kingston raccomanda quanto segue:

- Eseguire una scansione antivirus sul computer prima di impostare utilizzare il drive LP50 su un sistema target
- Bloccare il dispositivo quando non utilizzato
- Espellere il drive prima di scollegarlo
- 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 con nessuno la password del dispositivo

Esplorate informazioni e aggiornamenti più recenti

Accedere al sito web kingston.com/support per consultare i più recenti aggiornamenti, FAQ, documentazione, e informazioni aggiuntive sui drive.

NOTA: Il drive deve essere aggiornato esclusivamente con gli aggiornamenti più recenti (se 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.

Prassi raccomandate per l'impostazione della password
Il drive LP50 è dotato di solide contromisure di sicurezza. Ciò include la protezione contro gli attacchi brute force, che impediscono agli aggressori di scoprire le password limitando i tentativi di inserimento password a10 tentativi. Una volta raggiunto il limite di tentativi di inserimento password sul drive, LP50 effettuerà la cancellazione automatica di tutti i dati crittografati per poi effettuare la formattazione alle impostazioni di fabbrica.

Supporto per password multiple
LP50 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 LP50 è in grado di supportare due password utente differenti che possono essere utilizzate per recuperare i dati: password Amministratore (Admin) e password utente (User).

L'unità LP50 consente l'impostazione di due password principali; una password Amministratore (chiamata "Password Admin"), e una password Utente. L'account amministratore (Admin) può accedere al drive in qualunque momento e impostare le opzioni per gli account utente e amministratore, come se fosse un Super User.

L'account Utente può accedere al drive come quello Amministratore, 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 amministratore 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 LP50 può essere sottoposto a un reset; ma in tal caso, tutti i dati in esso contenuti saranno eliminati definitivamente.

Modalità password
Il drive LP50 supporta inoltre due modalità password differenti:

Password complessa
Una password complessa comprende da 6 a 16 caratteri e deve utilizzare almeno 3 dei seguenti caratteri:

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

Frase-password
Il drive LP50 le frasi password composte da 10 fino a 64 caratteri. Una frase password non segue alcuna regola aggiuntiva, ma se utilizzata correttamente livelli di protezione password estremamente elevati.

Una frase password è fondamentalmente composta da qualunque combinazione di caratteri inclusi caratteri provenienti da altre lingue. Come nel caso del drive LP50, la lingua utilizzata per la password può essere anche corrispondente alla lingua selezionata per il drive. Ciò consente di selezionare 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.

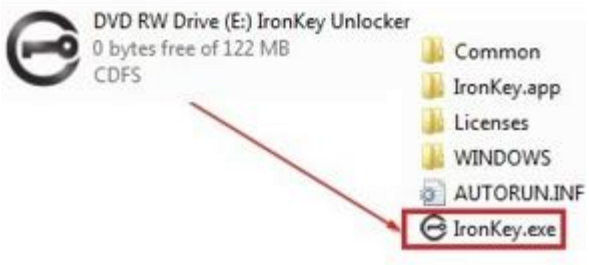
Configurazione del dispositivo

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)

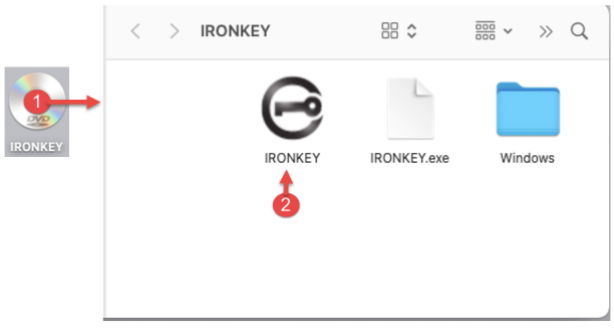
Collegare il drive USB crittografato IronKey in una delle porte USB disponibili sul notebook o sul PC desktop e attendere che Windows rilevi il dispositivo.

• Gli utenti di Windows 8,1/10/11 riceveranno una notifica che richiede l'installazione del driver del dispositivo. *(Figura 3.1)*	 **Figura 3.1– Notifica di rilevamento del driver del dispositivo**

• Una volta completato il rilevamento del nuovo hardware, selezionare l'opzione **IronKey.exe**, all'interno della partizione Unlocker presente su 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 – File Explorer Window/IronKey.exe**

Accesso al dispositivo (ambienti macOS)

Inserire il drive LP50 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 verrà visualizzata l'icona del volume “IRONKEY”. (*Figura 3.3*)

• Fare doppio clic sull'icona 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 dell'unità IKLP**

Inizializzazione del dispositivo (ambienti Windows e macOS)

Lingua e EULA

- Selezionare la lingua preferita dal menu a discesa e fare clic sulla voce **"Successivo" (Next)** (*vedere Figura 4.1*)

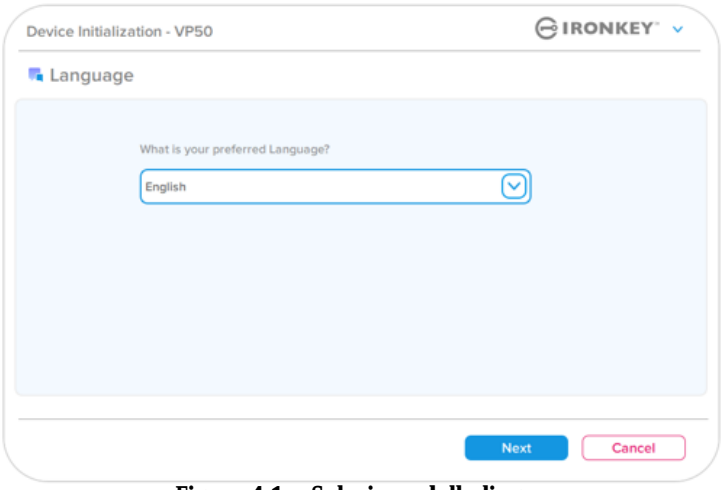


Figura 4.1 – Selezione della lingua

- Leggere l'accordo di licenza e quindi fare clic su **"Successivo" (Next)**.

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

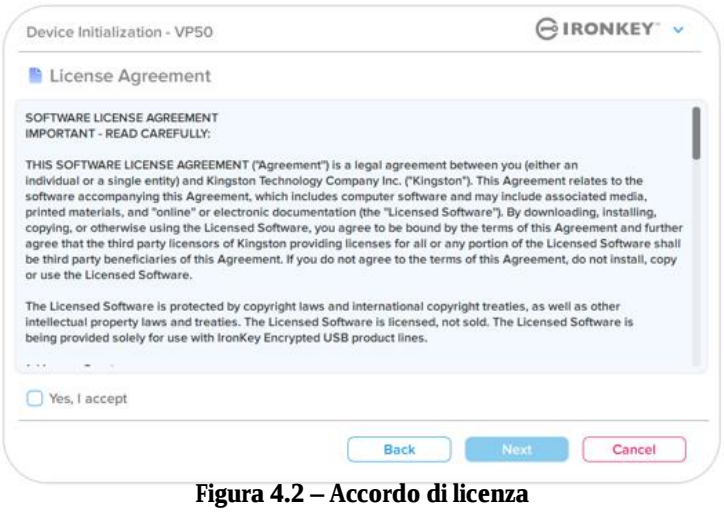


Figura 4.2 – Accordo di licenza

Inizializzazione del dispositivo

Selezione della password

Sulla schermata di selezione password, è possibile creare una password a protezione dei dati dell'unità LP50. La password utilizzata può essere tipo complesso oppure una frase password (*Figure 4.3 - 4.4*). Inoltre, da questa schermata è anche possibile utilizzare le opzioni multi password Amministratore/Utente. Prima di procedere con la selezione della password, consultare nuovamente la sezione abilitazione Password Amministratore/Utente sotto, per familiarizzare con 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.

Per iniziare a selezionare una password, creare una password nel campo "Password" quindi reinserire la stessa password nel campo "Conferma password". Affinché sia possibile proseguire la procedura di inizializzazione, è necessario creare una password avente i seguenti requisiti:

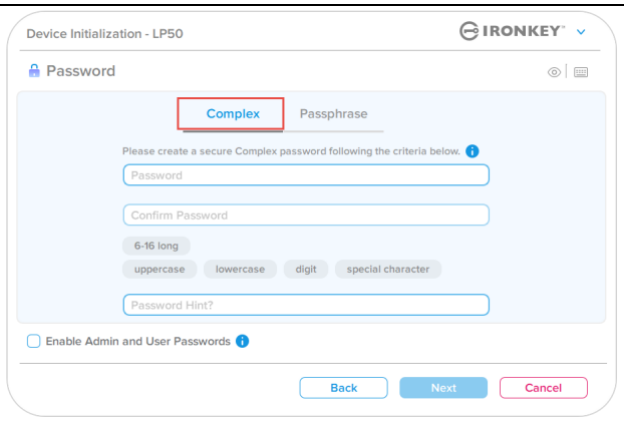
<table>
<tr>
<td>Utilizzo di password complesse (Complex)
Le password devono essere composte da un minimo di 6 fino a un massimo di 16 caratteri.
Le password devono includere tre (3) dei seguenti criteri:
Lettere maiuscole
Lettere minuscole
Numeri
Generati Caratteri speciali (!,$,&, ecc..)</td>
<td> 

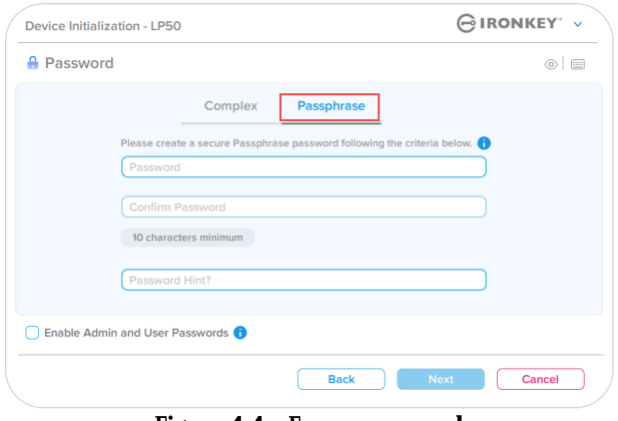
Figura 4.3 – Password complesse</td>
</tr>
<tr>
<td>Password con frase password (Passphrase)
Deve contenere:
Minimo 10 caratteri
Massimo 64 caratteri</td>
<td> 

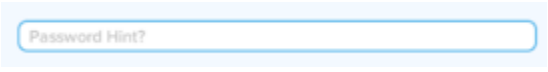
Figura 4.4 – Frase-password</td>
</tr>
<tr>
<td>Suggerimento password (Password Hint) (opzionale)
Un suggerimento password può rivelarsi utile per aiutare l'utente a ricordare la password, qualora questa vada persa o dimenticata.
Nota: il suggerimento NON DEVE corrispondere alla stessa password utilizzata per l'accesso.</td>
<td> 

Figura 4.5 – Campo suggerimento password</td>
</tr>
</table>

Inizializzazione del dispositivo

Password valide e password 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: Quando vengono soddisfatti almeno tre criteri minimi per la password, la casella associata al quarto criterio diventa di colore grigio, a indicare che tale criterio è opzione (*Figura 4.6b*)

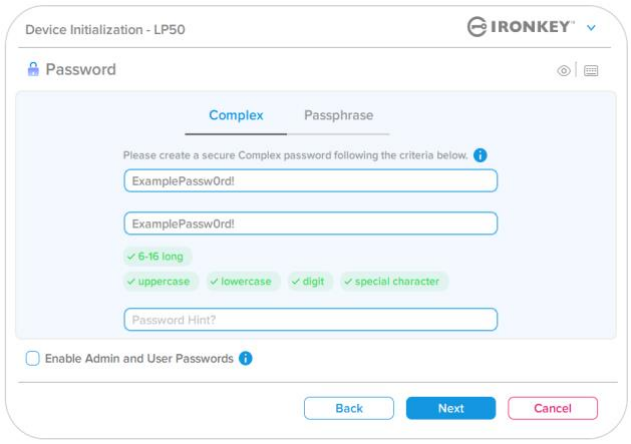


Figura 4.6a – Requisiti di inserimento della password complessa rispettati

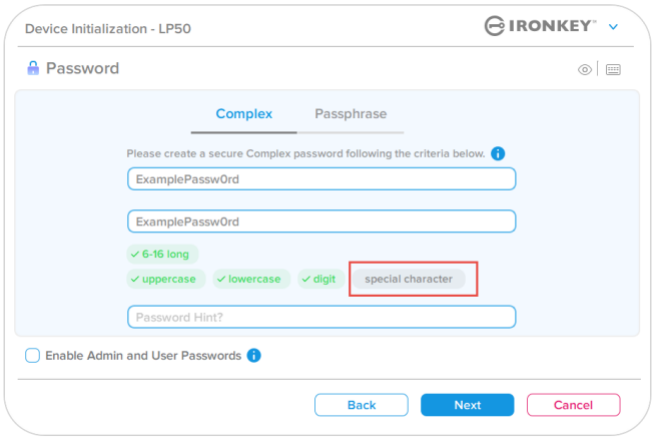


Figura 4.6b – Requisiti condizionali opzionali della password complessa

Nel caso di inserimento di password **Non valide**, i campi associati ai criteri delle password, si illumineranno di colore **rosso**, e il pulsante "**Successivo**" (Next) Resterà disabilitato fino a quando non vengono rispettati i requisiti di inserimento corretti.

Tale condizione è applicabile sia alle password complesse che alle frasi password.

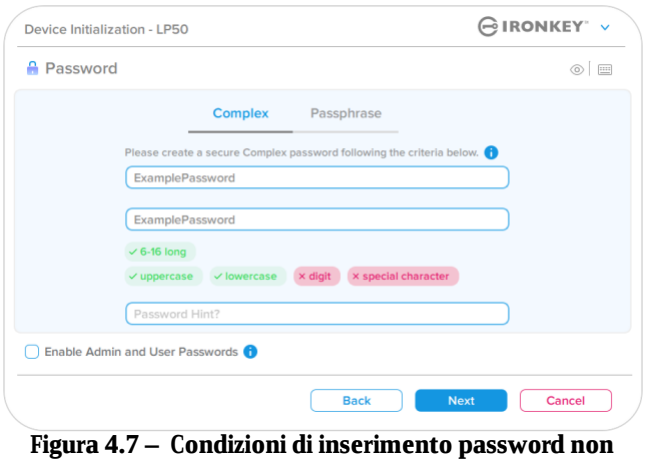


Figura 4.7 – Condizioni di inserimento password non rispettate

Inizializzazione del dispositivo

Tastiera virtuale
Il drive LP50 integra una tastiera virtuale che può essere utilizzata per la protezione contro attacchi keylogger.

- Per utilizzare la **tastiera virtuale**, identificare il pulsante raffigurante la tastiera sul lato superiore destro della schermata "**Inizializzazione dispositivo**" (Device Initialization), e quindi selezionare tale opzione.

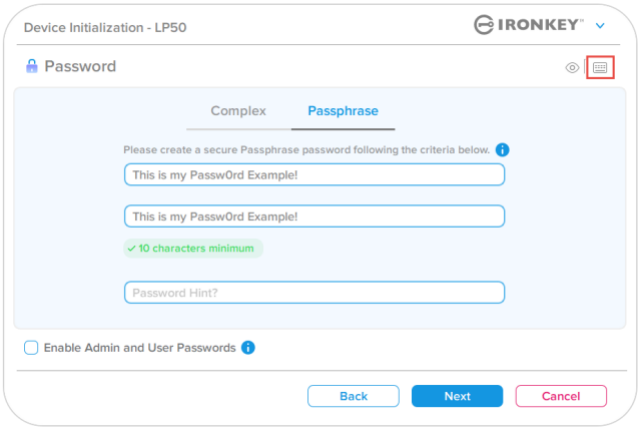


Figura 4.8 – Attivazione della tastiera virtuale

- Una volta che viene visualizzata la tastiera virtuale, è anche possibile attivare la protezione contro gli "**Protezione contro gli screenlogger**" (Screenlogger Protection). Quando si utilizza tale funzionalità, tutti i tasti vengono temporaneamente disattivati. Questo è un tipo di comportamento prevedibile in quanto impedisce agli screenlogger di catturare i contenuti di ciò che l'utente sta cliccando sulla tastiera.

- A fine di garantire una maggiore protezione di questa funzionalità, è anche possibile selezionare la funzione di layout casuale dei tasti della tastiera virtuale, selezionando l'opzione "**Randomize**" (Layout casuale) sul lato inferiore destro della tastiera. La funzione Randomize (Layout casuale) dispone i tasti in ordine casuale.

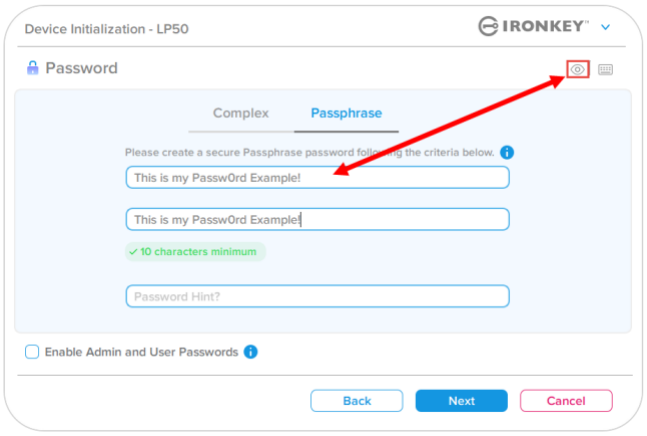
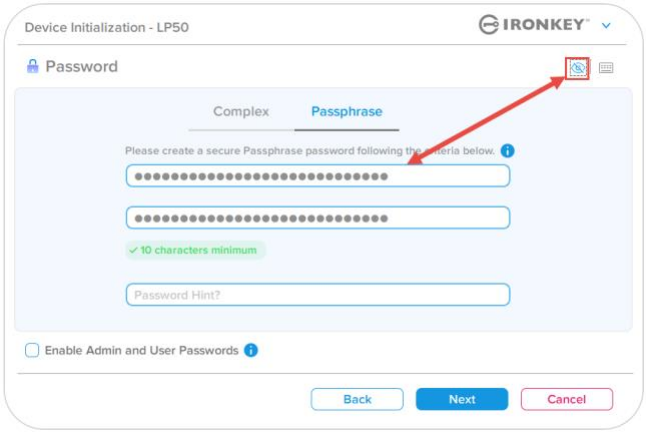
Figura 4.9 – Protezione contro screenlogger / funzione di layout casuale tastiera

Inizializzazione del dispositivo

Pulsante di commutazione visualizzazione password

Per impostazione predefinita, quando si crea una password, la password inserita sarà visualizzata nel campo di inserimento mentre mentre viene digitata. Se si desidera nascondere la password mentre viene digitata, è possibile fare ciò commutando la funzione di visualizzazione password mediante l'icona raffigurante un “occhio” posizionata sul lato superiore destro della schermata di inizializzazione dispositivo.

Nota: Una volta che il dispositivo è stato inizializzato, il campo password sarà impostato automaticamente in modalità “nascosta”.

Per **nascondere** la stringa contenente la password, fare clic sull’icona grigia. 	 **Figura 4.10 – Commutare la modalità “Nascondi password”**
Per **mostrare** la password nascosta, fare clic sull’icona blu. 	 **Figura 4.11 – Commutare la modalità “Mostra password”**

Inizializzazione del dispositivo

Password amministratore e utente

Abilitando le password Amministratore e Utente, è possibile sfruttare le funzionalità multi password, in cui la funzione di amministratore può gestire entrambi gli account. Selezionare l'opzione "**Abilita le password amministratore e utente**". Tale funzione offre un metodo alternativo per accedere al drive in caso di smarrimento di una delle password.

Quando la modalità "**Password amministratore e utente**" è abilitata , è anche possibile accedere alle seguenti funzionalità:

- Reset della password utente

Per ulteriori informazioni sulla funzionalità "Reset della password utente", andare a pagina 28 della guida utente.

- Per abilitare la funzione "**Password amministratore e utente",** fare clic sulla casella posta accanto all'opzione "**Abilita password amministratore e utente**" (Enable Admin and User Passwords) e selezionare il pulsante"**Successivo** (Next), dopo aver selezionato una password valida. (*Figura 4.12*)

- Quando questa funzionalità è **abilitata**, la password selezionata per questa schermata è quella **amministratore**. Fare clic su "**Successivo**" (Next), per procedere verso la schermata "**Password utente**", dalla quale è possibile selezionare una password utente.

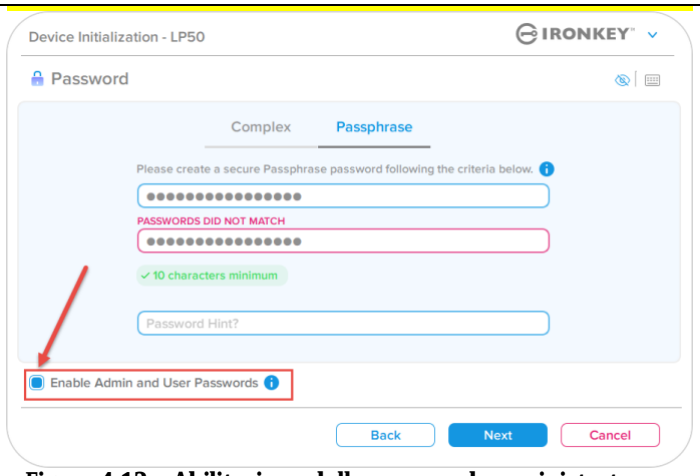


Figura 4.12 – Abilitazione delle password amministratore e utente

Nota: L'abilitazione della password amministratore e della password utente è opzionale.

Se il drive è impostato con questa funzione NON abilitata (casella non selezionata), esso sarà configurato come unità **Utente singolo, Password singola**, senza **alcuna funzionalità Amministratore attiva**. All'interno di questo manuale, questa configurazione prende il nome di "**Modalità solo utente**".

Per procedere con la modalità "Utente singolo" e "Password singola" tenere la funzione "**Abilita le password amministratore e utente**" deselezionata e fare clic su "**Successivo**" , dopo aver creato una password valida.

Inizializzazione del dispositivo

Password amministratore e utente

Se la regola amministratore è stata **abilitata** nella schermata precedente, sarà visualizzata la schermata successiva associata alla "**Password utente**" (User Password) (*Figura 4.13*). La password Utente sarà dotata di funzionalità limitate rispetto a quella Amministratore. Tali funzionalità saranno discusse in dettaglio nelle sezioni successive. **Nota:** 'nella restante sezione di questo manuale, la funzione "**Password amministratore e utente**" sarà denominata "**Regola amministratore**".

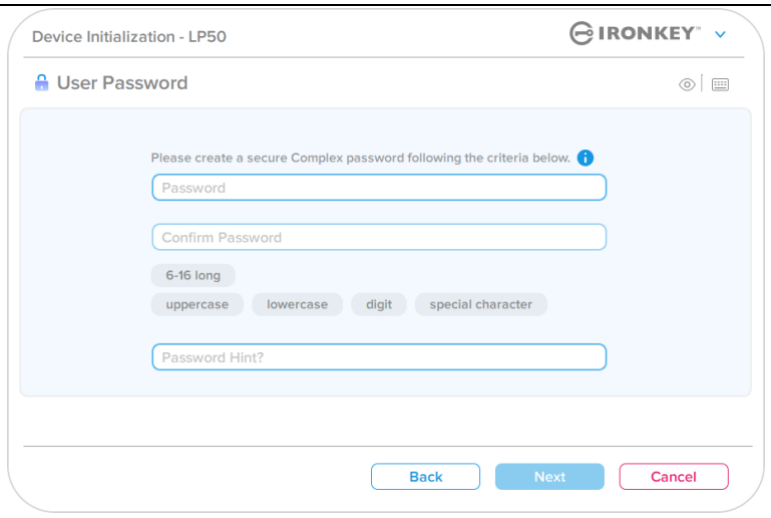


Figura 4.13 - Password Utente (Funzioni "Amministratore" e "Utente abilitate)

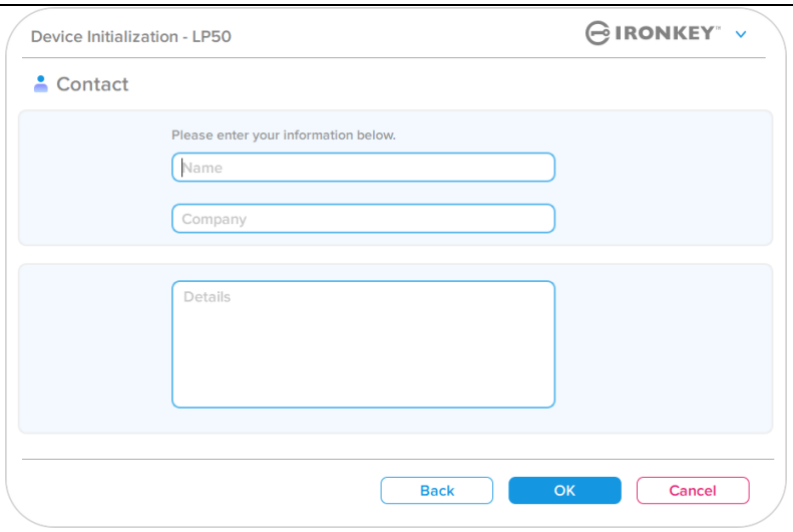
Nota: L'opzione password selezionata (complessa o frase password), sarà trasferita anche alla password utente, a qualunque attività di reset password richiesta per la configurazione del drive. L'opzione password selezionata può essere modificata solamente dopo aver effettuato un reset completo del dispositivo.

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**" (Name) può contenere fino a 32 caratteri, ma non può contenere la password **esatta**. Il campo "**Azienda**" (Company) può contenere fino a 32 caratteri, ma non può contenere la password **esatta**. Il "**Dettagli**" (Details) 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. Procedere a scollegare il drive per poi ricollegarlo al sistema, al fine di poter visualizzare le modifiche apportate.

USB ß → Inizializzazione cloud (ambienti Windows)

Al termine dell'inizializzazione del dispositivo su Windows, verrà visualizzata l'applicazione USB-to-Cloud, come mostrato nella *Figura 5.1* qui a destra. Prima di proseguire, assicurarsi di disporre di una connessione Internet attiva.

- Per procedere con l'installazione, fare clic sul pulsante verde "Accetto" (Accept) nell'angolo inferiore destro della finestra clevX
- Per rinunciare all'installazione, fare clic sul pulsante rosso declinare "Rifiuto"(Decline) che si trova nell'angolo inferiore sinistro della finestra clevX.
- (Nota: Facendo clic sul pulsante rosso "Rifiuto", l'installazione della funzionalità USB-to-Cloud sarà annullata. In tal caso, nella partizione dei dati verrà creato uno speciale file di testo denominato 'USBtoCloudInstallDeclined.txt'. La presenza di tale file eviterà che la richiesta relativa all'installazione dell'applicazione sia visualizzata in futuro).

Figura 5.1 – EULA per la funzione USBtoCloud Windows

- Nel caso in cui venisse visualizzata la seguente finestra sulla sicurezza di Windows durante l'installazione, fare clic su "Consenti accesso" per proseguire con l'installazione. In alternativa, creare un'eccezione nel Firewall di Windows al fine di consentire l'utilizzo dell'applicazione USB-to-Cloud.

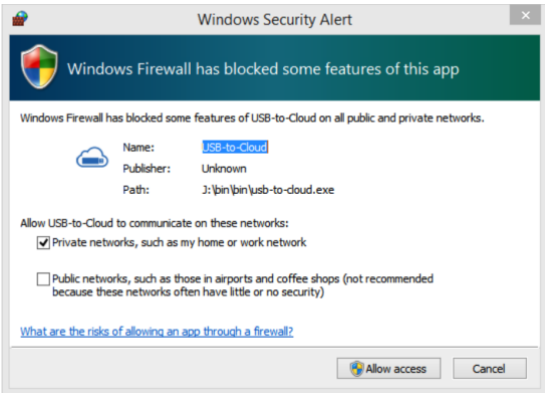


Figura 5.2 – Avviso sulla sicurezza di Windows

USB ß → Inizializzazione cloud (ambienti Windows)

- Terminata l'installazione, l'applicazione visualizzerà un riquadro contenente un elenco di opzioni tra cui scegliere (per la sincronizzazione dati con il drive LP50).
- Selezionare il cloud che si desidera utilizzare come applicazione di backup ed inserire le credenziali di autenticazione richieste.
- (Nota: Se non si dispone ancora di un account presso uno dei servizi di cloud elencati, procedere alla creazione di un account utilizzando il proprio browser Internet preferito e quindi tornare a questo punto della procedura).
- Una volta selezionata l'opzione Cloud ed eseguito l'accesso al servizio corrispondente, l'applicazione USB-to-Cloud eseguirà un confronto iniziale fra i dati presenti nella partizione e quelli presenti nel Cloud. Fin quando il servizio USB-to-Cloud sarà attivo in Gestione attività, i contenuti scritti nella partizione dei dati saranno automaticamente archiviati (sincronizzandosi) nel Cloud.

Figura 5.3 – selezione Cloud

USB ß → Inizializzazione cloud (ambienti Windows)

L'applicazione USB-to-Cloud offre i seguenti servizi aggiuntivi:

- Sospensione backup (sospende l'esecuzione del backup dei dati).
- Ripristino (ripristina nel dispositivo i dati presenti nel cloud).
- Impostazioni (opzioni aggiuntive per il backup dei dati).
- Uscita (termina l'esecuzione del servizio USB-to-Cloud).

Nel menu "Impostazioni" è possibile:

- Modificare l'applicazione del servizio cloud attualmente utilizzata per i backup.
- Modificare la lingua attualmente in uso,
- Selezionare i file e/o le cartelle di cui si desidera eseguire il backup nel Cloud.
- Controllare la disponibilità di aggiornamenti software.

(**Nota:** eseguendo il reset (o la formattazione) del driveLP50 tutti i dati contenuti nel dispositivo andranno persi. Tuttavia, i dati in quel momento archiviati nel cloud resteranno salvi ed intatti.)

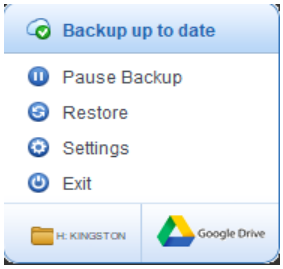


Figura 5.4 - Servizi

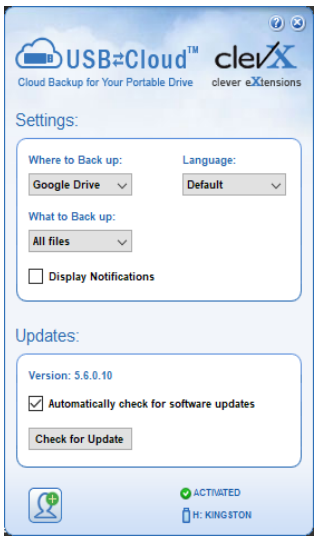


Figura 5.5 - Impostazioni

USB ß → Inizializzazione cloud (ambienti MacOS)

- Al termine dell'inizializzazione del dispositivo, verrà visualizzata l'applicazione USB-to-Cloud come mostrato nella *Figura 5.6* qui a destra. Prima di proseguire, assicurarsi di disporre di una connessione Internet attiva.

- Per procedere con l'installazione, fare clic sul pulsante "Accetto" (Accept), nell'angolo inferiore destro della finestra clevX.
  (Nota: Sui sistemi macOS 12.x, selezionare "OK" per consentire l'accesso ai file su un volume rimovibile. Selezionare "OK").
  (*Vedere Figura 5,7*)

- Per rinunciare all'installazione, fare clic sul pulsante "Rifiuto"(Decline) che si trova nell'angolo inferiore sinistro della finestra clevX.

Figura 5.6 – EULA per la funzione USBtoCloud macOS

(Nota: Facendo clic sul pulsante "Rifiuto", l'installazione della funzionalità USB-to-Cloud sarà annullata. In tal caso, nella partizione dei dati verrà creato uno speciale file denominato "DontInstallUSBtoCloud". La presenza di tale file eviterà che la richiesta relativa all'installazione dell'applicazione sia visualizzata in futuro).

- Terminata l'installazione, l'applicazione visualizzerà un riquadro contenente un elenco di opzioni tra cui scegliere (per la sincronizzazione dati con il drive LP50). (*Figura 5.8*)

Figura 5.7- accesso su sistemi macOS

- Selezionare il cloud che si desidera utilizzare come applicazione di backup ed inserire le credenziali di autenticazione richieste.

  (Nota: Se non si dispone ancora di un account presso uno dei servizi di cloud elencati, procedere alla creazione di un account utilizzando il proprio browser Internet preferito e quindi tornare a questo punto della procedura.)

- Una volta selezionata l'opzione Cloud ed eseguito l'accesso al servizio corrispondente, l'applicazione USB-to-Cloud eseguirà un confronto iniziale fra i dati presenti nella partizione e quelli presenti nel Cloud. Fin quando il servizio USB-to-Cloud sarà attivo in Gestione attività, i contenuti scritti nella partizione dei dati saranno automaticamente archiviati (sincronizzandosi) nel Cloud.

Figura 5.8 - selezione Cloud

USB ß →Utilizzo cloud (ambienti MacOS)

L'applicazione USB-to-Cloud offre i seguenti servizi aggiuntivi (*Figura 5.9*):

- **Sospensione backup** (sospende l'esecuzione del backup dei dati)
- **Ripristino** (ripristina nel dispositivo i dati presenti nel cloud)
- **Backup** (apre la schermata opzioni cloud) *Vedere Figura 5.9*
- **Uscita** (termina l'esecuzione del servizio USB-to-Cloud)

Figura 5.9 - Servizi

Nel menu “Preferenze” è possibile:

- Modificare la lingua attualmente in uso
- Abilitare/disabilitare le notifiche audio
- Abilitare/disabilitare la disconnessione del drive all’uscita dell'applicazione
- Abilitare/disabilitare la connessione per l’identificazione e risoluzione dei problemi
- Abilitare/disabilitare gli aggiornamenti automatici del software e verificare ora la disponibilità di aggiornamenti

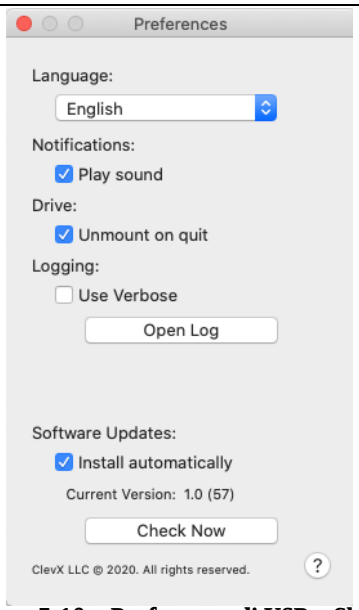


Figura 5.10 – Preferenze di USBtoCloud

Utilizzo del dispositivo (ambienti Windows e macOS)

Accesso per amministratore e utente (amministratore abilitato)

Se il dispositivo viene inizializzato con la configurazione che consente di utilizzare le password Amministratore e Utente (Regola amministratore), sarà eseguita l'applicazione integrata nel drive IronKey LP50, che richiederà l'inserimento della Password Utente durante l'accesso. Da qui sarà possibile effettuare l'accesso con la Password Utente, visualizzare qualunque informazione di contatto inserita oppure effettuare l'accesso come Amministratore (*Figura 6.1*). Facendo clic sul pulsante "Accedi come amministratore" (Login as Admin) (illustrato sotto), l'applicazione mostrerà il menu di accesso amministratore, dal quale è possibile effettuare l'accesso come amministratore e accedere alle relative funzionalità e impostazioni amministratore (*Figura 6.2*).

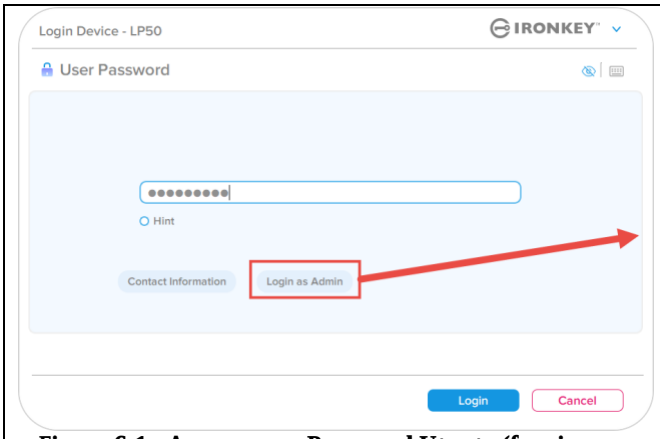


Figura 6.1 - Accesso con Password Utente (funzione amministratore abilitata)

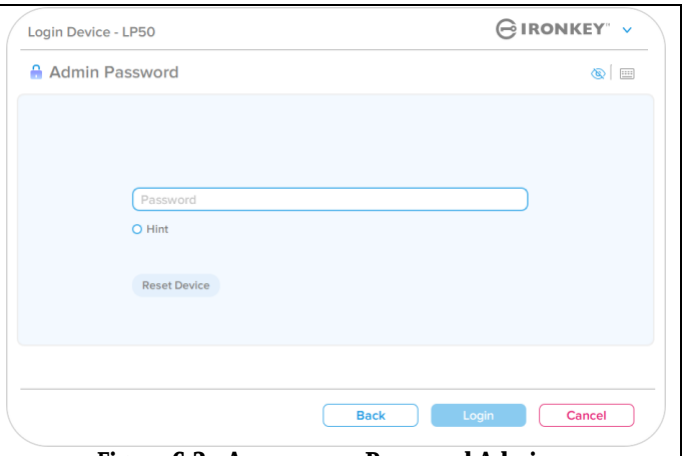


Figura 6.2 - Accesso con Password Admin

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

Come indicato in precedenza, a **Pagina 13**, sebbene sia consigliabile utilizzare la Regola amministratore per sfruttare appieno i vantaggi del dispositivo, il drive IronKey può essere inizializzato anche in modalità "Solo utente" (Password singola, utente singolo). Questa è un'opzione utilizzabile da colore che desiderano un approccio più semplice verso le password singole come strumento per mettere in sicurezza i dati del drive. (*Figura 6.3*)

Nota: Per abilitare le password Amministratore e Utente, utilizzare il pulsante "**Reset dispositivo**" (Reset Device), per riportare il drive in modalità di inizializzazione, dalla quale sarà possibile abilitare nuovamente le funzioni le password Amministratore e Utente. **Quando viene effettuato un reset del dispositivo, tutti i dati contenuti sul drive saranno formattati e andranno persi per sempre.**

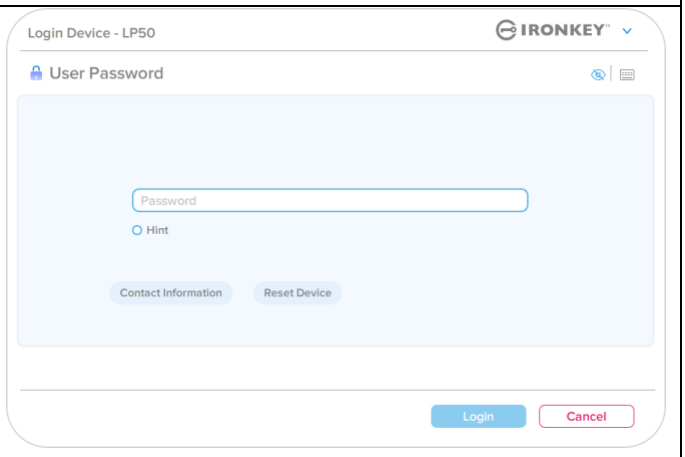


Figura 6.3 - Accesso con Password Utente (funzione amministratore non abilitata)

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 il numero di tentativi falliti supera il valore preimpostato di default, pari a 10 tentativi, il drive effettuerà le seguenti operazioni:

Funzione Amministratore/Utente abilitata	**Protezione contro gli attacchi Brute Force Comportamento del dispositivo (10 tentativi di accesso falliti)**	**Eliminazione dati e reset dispositivo?**
Password utente:	Blocco password. Accesso come Amministratore per effettuare il reset della Password Utente	NO
Password amministratore	Eliminazione della partizione crittografica del drive, delle password, delle impostazioni e eliminazione definitiva di tutti i dati	**SÌ**
Versione solo utente Utente singolo, password singola (Modalità Amministratore/Utente NON abilitata)	**Protezione contro gli attacchi Brute Force Comportamento del dispositivo (10 tentativi di accesso falliti)**	**Eliminazione dati e reset dispositivo?**
Password utente	Eliminazione della partizione crittografica del drive, delle password, delle impostazioni e eliminazione definitiva di tutti i dati	**SÌ**

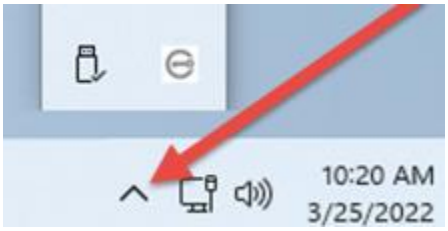
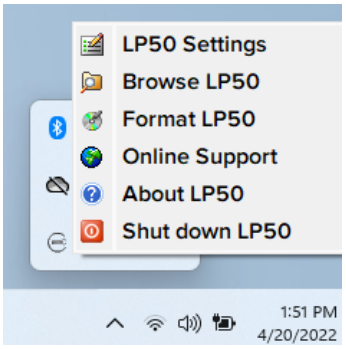
* Una volta effettuata con successo l'autenticazione sul dispositivo, il contatore dei tentativi di login falliti per il tipo di metodo utilizzato verrà azzerato. La cancellazione crittografica elimina tutte le password le chiavi crittografiche e i dati – **i dati contenuti nell'unita andranno persi per sempre.**

Accesso ai file sicuri

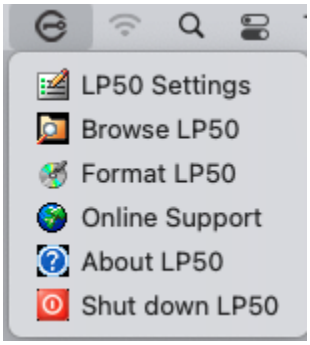
Una volta sbloccato il drive, è possibile accedere ai file sicuri. I file vengono crittografati e decrittati automaticamente quando vengono salvati o aperti sul drive. Questa tecnologia offre il vantaggio della massima trasparenza, consentendo di utilizzare i dati come se questi fossero memorizzati su 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**, nella barra applicazioni di Windows, per poi selezionare "**Esplora LP50**" (Browse LP50) (*Figura 7.2*)

Opzioni del dispositivo (ambienti Windows)

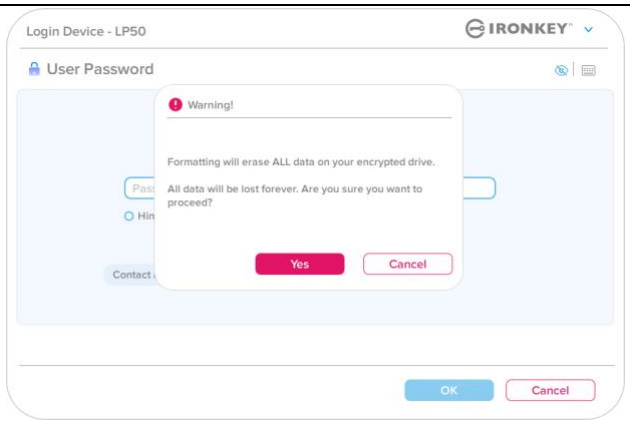
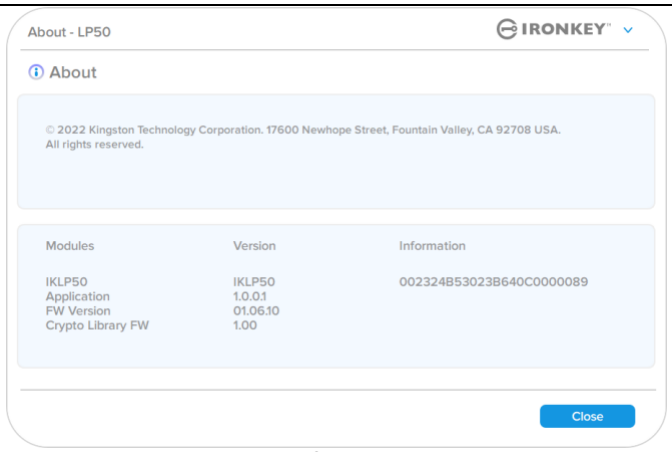
Durante l'accesso al dispositivo, sull'angolo destro della barra applicazioni di Windows verrà visualizzata l'icona del drive IronKey. Facendo clic con il tasto destro del mouse sull'icona IronKey, sarà possibile aprire il menù di selezione che include le opzioni del drive (*Figura 6.2*).
Ulteriori dettagli su questi dispositivi possono essere reperiti alle pagine 19-23 di questa guida

• Durante l'accesso al dispositivo, sull'angolo destro della barra applicazioni di Windows verrà visualizzata l'icona del drive IronKey. (*Figura 7.1*)	 **Figura 7.1 - Icona del drive IronKey sulla barra applicazioni**
• Facendo clic con il tasto destro del mouse sull'icona IronKey, sarà possibile aprire il menù di selezione che include le opzioni del drive. (*Figura 7.2*) Ulteriori dettagli su questi dispositivi possono essere reperiti alle pagine 19-23 di questo manuale.	 **Figura 7.2 - Fare clic con il pulsante destro del mouse sull'icona IronKey per visualizzare le opzioni del dispositivo**

Opzioni del dispositivo - (ambienti macOS)

• Quando si è connessi al dispositivo viene visualizzata un'icona IronKey LP50 posizionata sul menu macOS mostrato in ***Figura 7.3***. Tale menu consente di accedere alle opzioni del dispositivo. Ulteriori dettagli su questi dispositivi possono essere reperiti alle pagine 19-23 di questo manuale.	 **Figura 7.3 - icona barra dei menu/opzioni dispositivo macOS**

Opzioni dispositivo

Impostazioni del drive LP50:	• Modifica password di accesso, informazioni di contatto, altre impostazioni. (Ulteriori dettagli sulle impostazioni del dispositivo possono essere reperiti nella sezione “Impostazioni LP50” di questo manuale).
Esplora LP50:	• Consente di visualizzare i file sicuri.
Formatta LP50: 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 – Formattazione LP50**
Supporto online:	• Questa opzione consente di accedere al link http://www.kingston.com/support, dal quale è possibile accedere a una serie di informazioni di supporto aggiuntive.
Informazioni su LP50: La sezione contiene dettagli specifici sull'unità LP50 incluse le applicazioni, il firmware e informazioni sul numero di serie (*Figura 6.2*) **Nota:** il numero di serie univoco del drive può essere visualizzato nella colonna “Informazioni”	 **Figura 7.5 – Informazioni su LP50**
Arresta LP50:	• Questa funzione permette di arrestare correttamente l'unità LP50 consentendo all'utente di scollegare il drive dal computer in tutta sicurezza.

Impostazioni del drive LP50

Impostazioni amministratore

La schermata di accesso Amministratore consente di accedere alle impostazioni seguenti:

- **Password (Password):** Consente di modificare la password Amministratore e/o il suggerimento (*Figura 8.1*)
- **Dati di contatto (Contact Info):** Consente di aggiungere/visualizzare/modificare le informazioni di contatto dell'utente (*Figura 8.2*)
- **Lingua (Language):** Consente di modificare le impostazioni della lingua corrente (*Figura 8.3*)
- **Opzioni amministratore (Admin Options):** Consente di accedere alle funzionalità aggiuntive come:
    - Modifica della password Utente corrente (*Figura 8.4*)

NOTA: Per ulteriori dettagli sulle opzioni amministratore consultare le informazioni a pagina 25

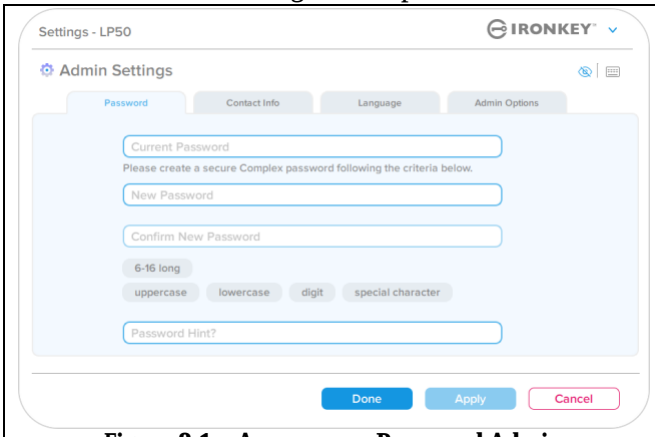


Figura 8.1 – Accesso con Password Admin

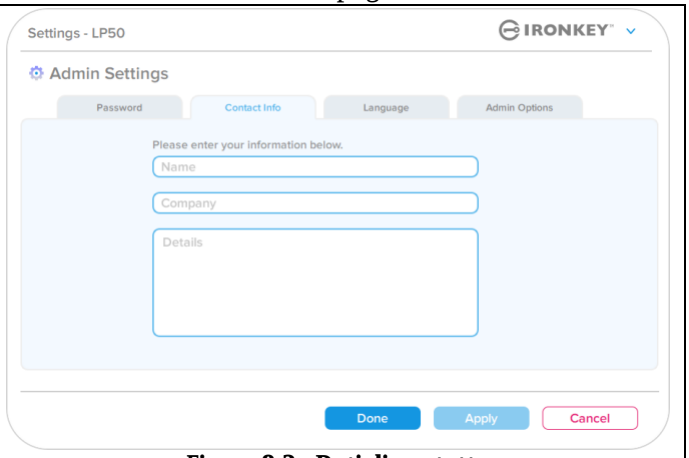


Figure 8.2 - Dati di contatto

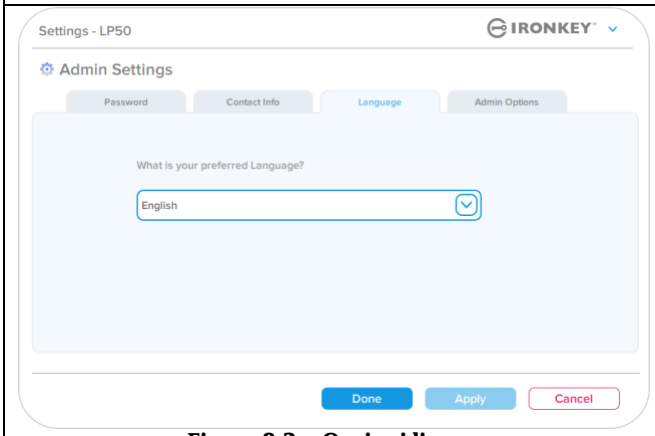


Figura 8.3 – Opzioni lingua

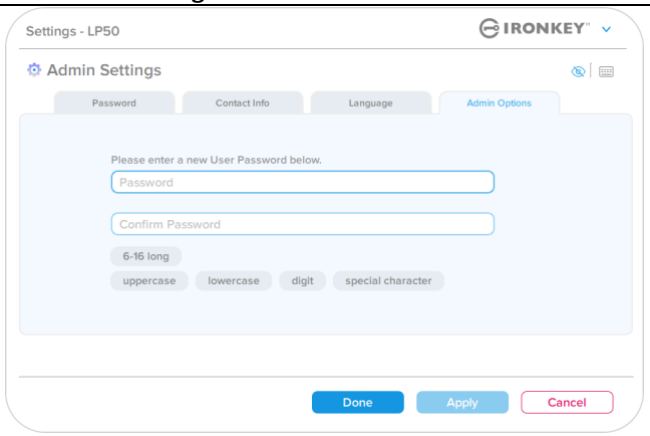


Figura 8.4 – Opzioni amministratore

Impostazioni del drive LP50

Impostazioni utente: Funzione amministratore abilitata

L'accesso Utente limita la disponibilità delle impostazioni seguenti:

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

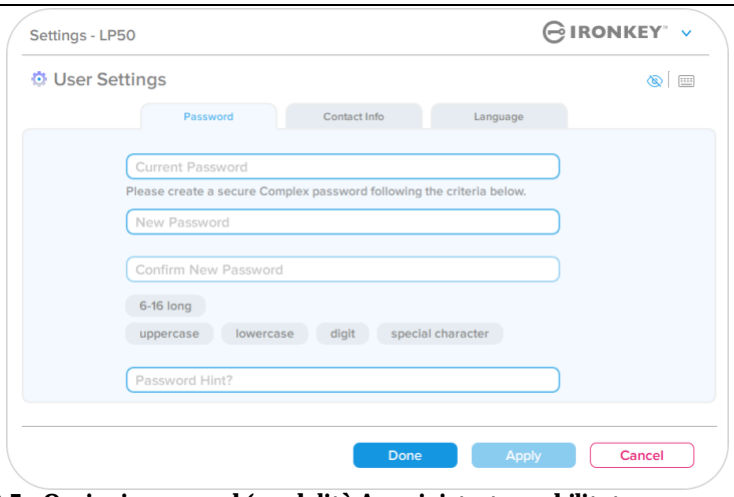


Figura 8.5 - Opzioni password (modalità Amministratore abilitata: accesso Utente)

Dati di contatto (Contact Info):
Consente di aggiungere/visualizzare/modificare i dati di contatto. (Figura 8.6)

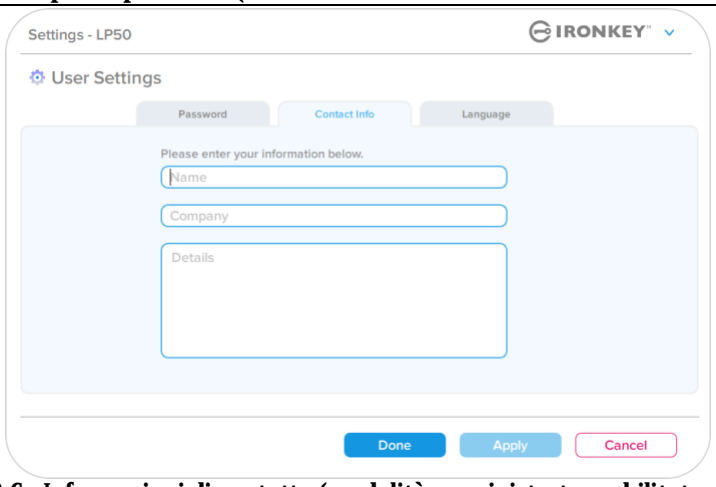


Figura 8.6 - Informazioni di contatto (modalità amministratore abilitata: accesso Utente)

Lingua (Language):
Consente di modificare le impostazioni della lingua corrente. (*Figura 8.7*)

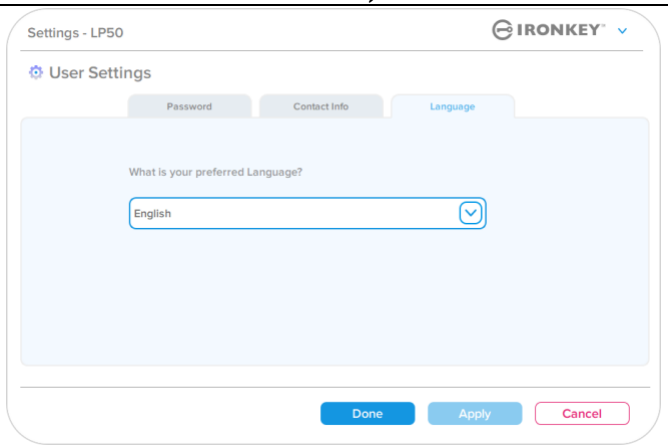


Figura 8.7 - Impostazioni lingua (modalità Amministratore abilitata: accesso Utente)

Nota: Le opzioni amministratore non sono disponibili quando si effettua l'accesso con la password Utente.

Impostazioni del drive LP50

Impostazioni utente: Modalità amministratore non abilitata

Come precedentemente specificato a pagina 12, l'avvio del drive LP50 senza avere prima abilitato le password Amministratore e Utente, farà sì che l'unità sia configurata in modalità **Password singola, utente singolo.** Questa modalità di configurazione non garantisce l'accesso ad alcuna opzione o funzionalità di amministrazione. Questa configurazione garantisce l'accesso alle seguenti impostazioni del drive LP50:

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

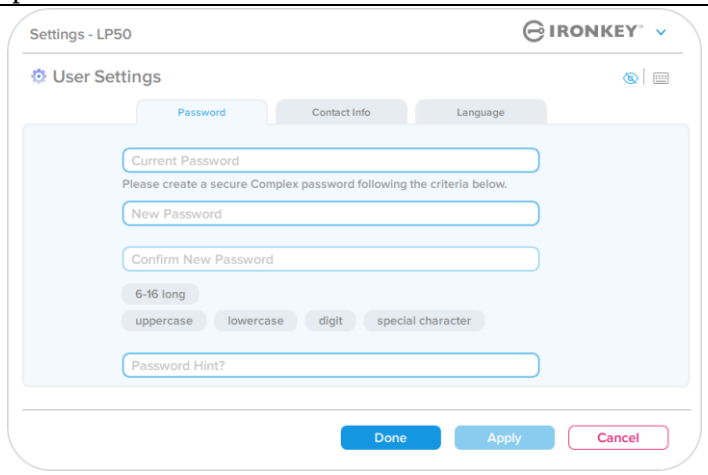


Figura 8.8- Opzioni password (Modalità solo utente)

Dati di contatto (Contact Info):
Consente di aggiungere/visualizzare/modificare i dati di contatto. (*Figura 8.9*)

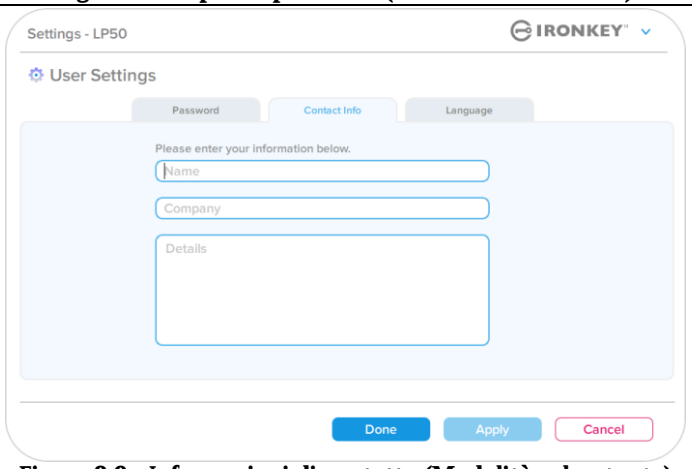


Figura 8.9 - Informazioni di contatto (Modalità solo utente)

Lingua (Language):
Consente di modificare le impostazioni della lingua corrente. (*Figura 8.10*)

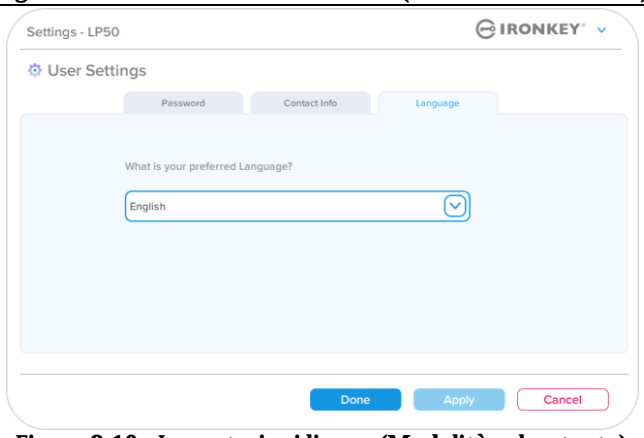


Figura 8.10 - Impostazioni lingua (Modalità solo utente)

Impostazioni del drive LP50

Modifica e salvataggio delle impostazioni

- Ogni qualvolta si effettuano dei cambiamenti alle impostazioni dell'unità LP50 (per esempio, modifica dei dati di contatto, modifica della lingua, cambiamenti della password e delle opzioni amministratore ecc.), il drive chiederà all'utente di inserire la password, al fine di accettare e applicare le modifiche effettuate. (*Vedere Figura 8,11*)

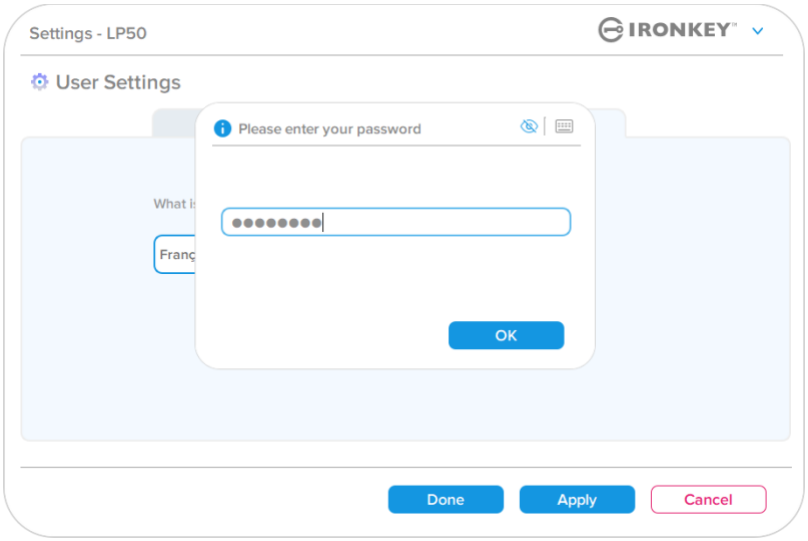


Figura 8.11 - Schermata password che richiede il salvataggio delle impostazioni per l'unità LP50

Nota: Se è visualizzata la schermata di inserimento password, come quella raffigurata sopra, e si desidera annullare o apportare cambiamenti alle modifiche, è possibile farlo semplicemente lasciando il campo password vuoto e facendo click su “OK” (OK). L'operazione consente di chiudere la finestra di inserimento password e tornare al menu impostazioni del drive LP50.

Funzionalità amministratore

Opzioni disponibili per effettuare un reset della password Utente

Una delle funzionalità più utili tra le opzioni di configurazione dell'account Amministratore, è quella che consente di eseguire un reset sicuro della password Utente in caso questa venga dimenticata. La sezione sotto illustra la funzionalità di Reset della password utente, che può essere d'aiuto durante la procedura di reset della 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 che regolano la creazione di una password sono basati sui requisiti originali che sono stati impostati durante la fase di inizializzazione (modalità di password complessa o frase password).

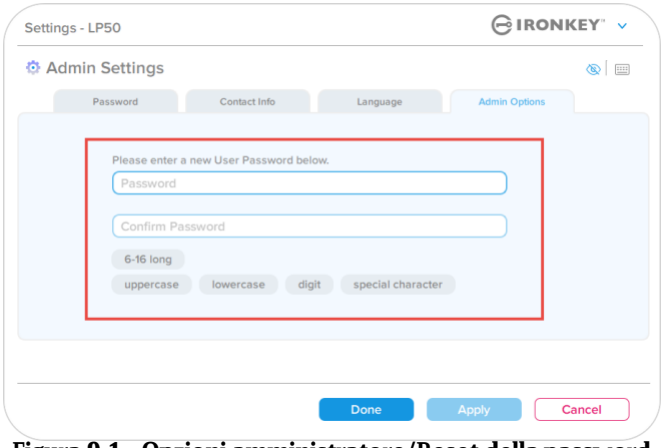


Figura 9.1 - Opzioni amministratore/Reset della password utente

Guida alla risoluzione dei problemi

Blocco del dispositivo

Il drive LP50 integra una funzione di sicurezza che impedisce gli accessi non autorizzati alla partizione dati quando si supera un determinato numero **consecutivo** di tentativi di accesso falliti (indicato dal parametro MaxNoA, in breve). La configurazione "di fabbrica" predefinita include un valore pari a 10 (numero di tentativi per ciascun metodo di accesso (Amministratore/Utente).

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

1. Un tentativo di accesso completato con successo prima di raggiungere il numero di accessi MaxNoA prestabilito

2. Raggiungere il numero di accessi MaxNoA prestabilito per poi eseguire un blocco del dispositivo o una formattazione dispositivo in base alla configurazione del drive.

- Se viene inserita una password errata, sopra il campo "Inserimento password" "Password Entry", verrà visualizzato un messaggio di errore di colore rosso indicante il tentativo di accesso fallito. (*Figura 10.1*)

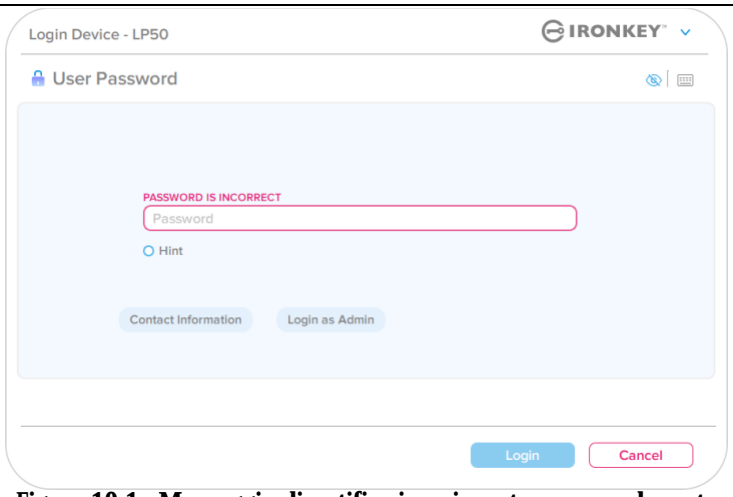


Figura 10.1 - Messaggio di notifica inserimento password errata

- Una volta raggiunto il settimo 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*)

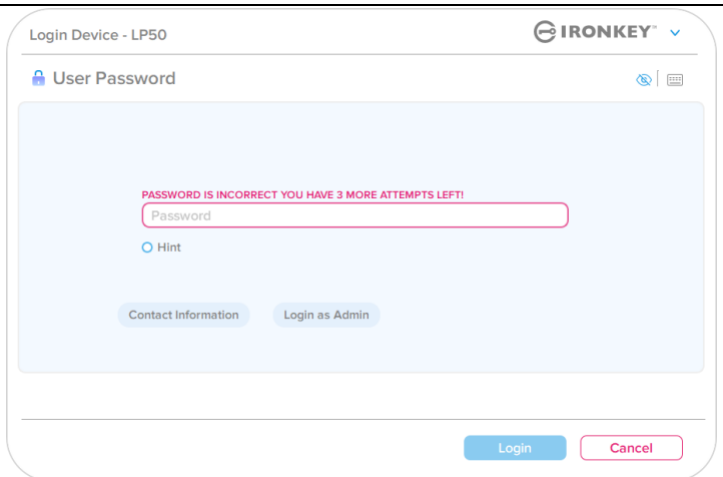


Figura 10.2 - Notifica del 7° tentativo di inserimento password errato

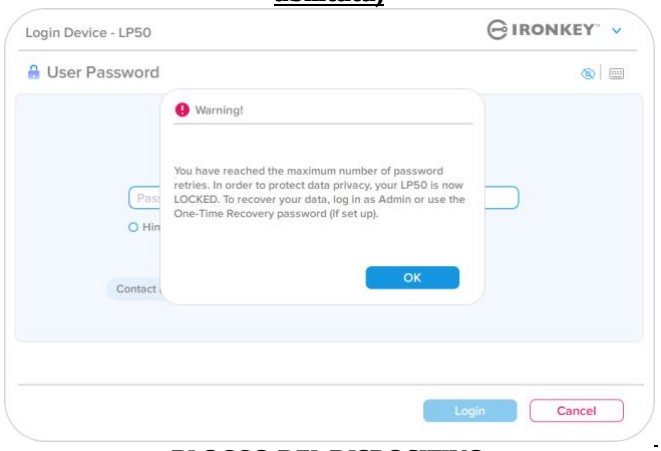
Guida alla risoluzione dei problemi

Blocco del dispositivo

Importante: Una volta raggiunto il **10**° e ultimo tentativo di accesso fallito, in base alla modalità di configurazione della modalità utilizzata (Amministratore/Utente), il dispositivo potrebbe bloccarsi automaticamente, richiedere all'utente di accedere con un metodo alternativo (se disponibile), oppure potrebbe essere necessario effettuare un reset del dispositivo, con conseguente formattazione ed **eliminazione permanente di tutti i dati presenti sul drive.** Tipi di comportamenti già citati a pagina 18 del manuale utente.

Le Figure 10.3 - 10.6 sotto, illustrano visivamente le schermate visualizzate dopo il 10° tentativo di accesso fallito con ciascun metodo di accesso:

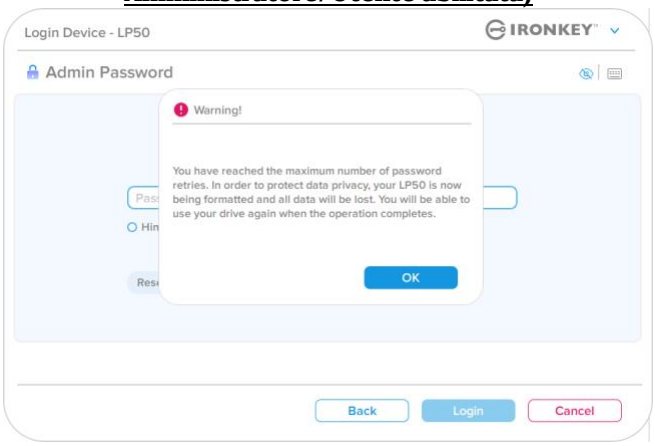
Password utente: (Funzione Amministratore/Utente abilitata)



BLOCCO DEL DISPOSITIVO

Figura 10.3

Password Amministratore (funzione Amministratore/Utente abilitata)

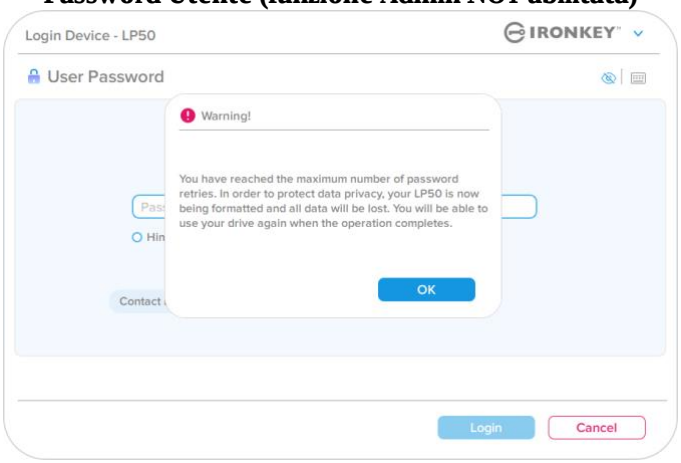


FORMATTAZIONE DISPOSITIVO*

Figura 10.4

- Questa misura di sicurezza ha lo scopo di limitare l'accesso a coloro che non dispongono della password, impedendo di effettuare tentativi di accesso ripetuti all'infinito allo scopo di accedere ai dati sensibili dell'utente (noti anche come attacchi brute force). Per i possessori di drive LP50 che hanno scordato la password di accesso verranno applicate le medesime misure di sicurezza, compresa la formattazione del dispositivo. * Per ulteriori informazioni su questa funzionalità, consultare la sezione "*Reset del dispositivo*" a pagina 25.

Password Utente (funzione Admin NOT abilitata)



FORMATTAZIONE DISPOSITIVO*

Figura 10.5

* *Nota: La formattazione del dispositivo eliminerà tutti i dati archiviati sulla partizione dati sicura del drive LP50.*

Guida alla risoluzione dei problemi

Reset dispositivo

Se si è dimenticata la password, oppure se è necessario effettuare un reset del drive è possibile fare clic sul pulsante "Reset dispositivo". Tale pulsante può essere posizionato in due punti, in base alla configurazione utilizzata (sul menu di "Accesso password amministratore" con funzione Amministratore/Utente abilitata; oppure sul menu di "Accesso password utente" quando tale funzione non è abilitata), quando viene eseguito il programma di avvio del drive LP50. (*vedere Figure 10.7 e 10.8*)

- Questa opzione consente di creare una nuova password; ma per proteggere la privacy, il drive LP50 sarà formattato. Ciò significa che durante tale procedura tutti i dati precedentemente archiviati andranno persi.*

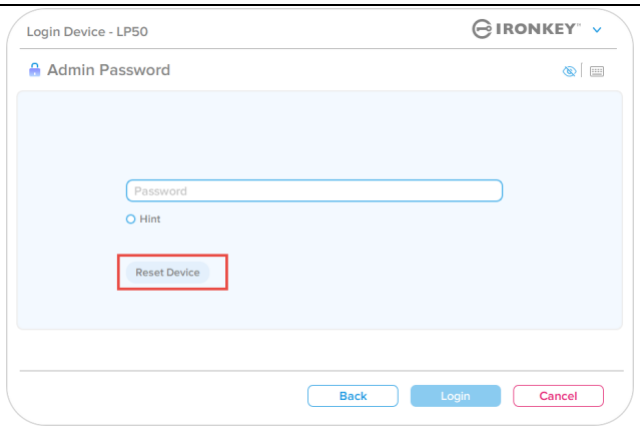


Figura 10.6 - Password Amministratore: Pulsante di reset dispositivo

- **Nota:** Cliccando sul pulsante "*Reset dispositivo*" (Reset Device), 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) cliccare su "*OK*" per confermare, oppure 2) cliccare su "Annulla", per tornare alla schermata di accesso. (*Vedere Figura 10.8*)

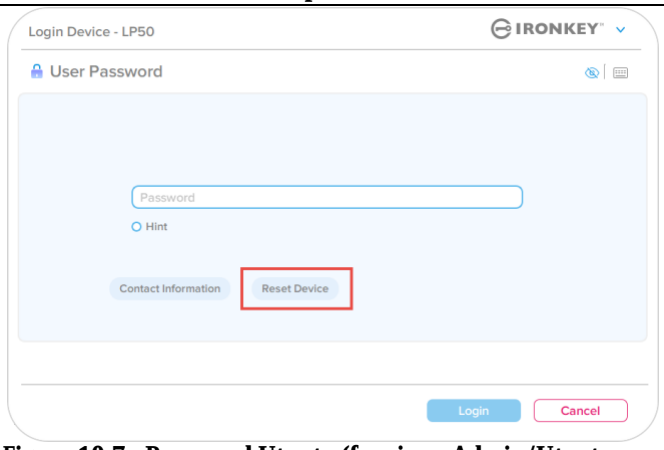


Figura 10.7 - Password Utente (funzione Admin/Utente non abilitata) Reset dispositivo

- 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.

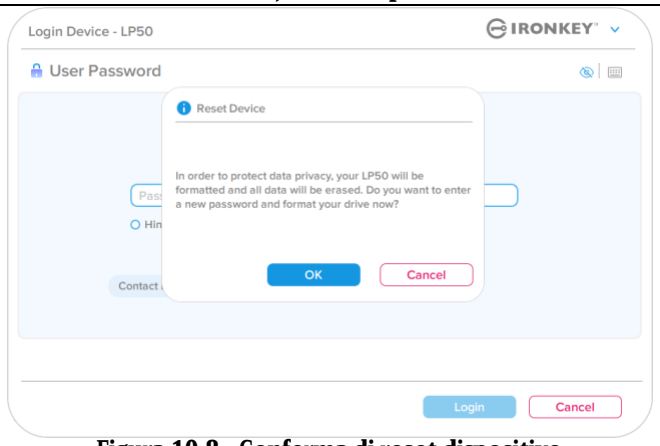


Figura 10.8 - Conferma di reset dispositivo

Guida alla risoluzione dei problemi

Conflitti tra le lettere di unità: Sistemi operativi Windows

- Come citato nella sezione "*Requisiti di sistema*" di questo manuale (a pagina 3), il drive LP50 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 consecutivo NON interessa le unità di rete condivise in quanto queste sono unità associate a profili utente specifici e non sono assegnate al profilo hardware di sistema e pertanto appaiono disponibili per il sistema operativo.

- Ciò significa che Windows potrebbe assegnare al drive LP50 una lettera di unità che è già utilizzata da una unità di rete condivisa, o 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).

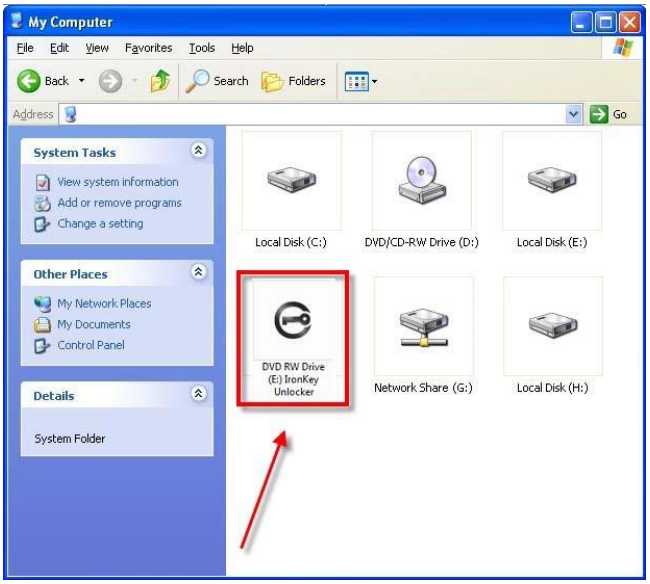


Figura 10.9 - Esempio di lettera di unità

In questo esempio (*Figura 10.9*), all'unità LP50 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 LP50 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 LP50 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 DataTraveler, causando ulteriori conflitti.

Si noti che le funzionalità di Gestione delle lettere di unità (DLM) sono migliorate significativamente su Windows XP SP3, 8.1, 10 e 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 visitare Kingston.com/support per richiedere ulteriore assistenza.

IRONKEY™ Locker+ 50 (LP50)
PENDRIVE SEGURO USB 3.2 Gen 1

Manual do Usuário

Índice

Figura 1: IronKey LP50

Introdução

Os pendrives USB IronKey Locker+ 50 da Kingston proporcionam uma segurança para o consumidor com criptografia de hardware AES no modo XTS, incluindo proteções contra BadUSB com firmware assinado digitalmente e ataques à senha por força bruta. O LP50 também está em conformidade com TAA.

O LP50 agora suporta a opção de múltiplas senhas (Admin e Usuário) com modos Complexos ou de Passe-frase. O modo Complexo permite senhas de 6 a 16 caracteres usando 3 de 4 conjunto de caracteres. O novo modo de Passe-frase 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 foi projetado com a conveniência de uma pequena capa de metal e aro de metal embutido para levar os dados aonde quiser. O LP50 também conta com um backup USBtoCloud (by ClevX®) adicional para acessar dados no drive de um armazenamento de nuvem pessoal através do Google Drive™, OneDrive (Microsoft®), Amazon Cloud Drive, Dropbox™ ou Box. O LP50 é fácil de qualquer pessoa instalar e usar, sem necessidade de instalação de aplicativo; todo o software e segurança necessária já está no drive. Funciona tanto no Windows® quanto no macOS ® para que os usuários possam acessar arquivos de vários sistemas.

O LP50 conta com uma garantia limitada de 5 anos e suporte técnico Kingston gratuito.

Recursos IronKey Locker+ 50

- 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 Passe-frase
- 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 (09242024)
Este manual do usuário trata do IronKey Locker+ 50 (LP50).

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 32.	**Suporte do Sistema Operacional do PC** • Windows 11 • Windows 10
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 12.x – 15.x

Observação: Uma inscrição gratuita de 5 anos para a USB-to-Cloud está incluída em cada drive após a ativação. Opções de ativação continuadas disponíveis para compra pela ClevX além do tempo incluído.

Recomendações

Para garantir que haja uma ampla energia fornecida ao dispositivo LP50, insira-o diretamente em uma porta USB em seu notebook ou desktop, como visto na *Figura 1.1*. Evite conectar o LP50 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 LP50 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 dos seus dados, a Kingston recomenda que você:

- Realize um escaneamento para vírus em seu computador antes de instalar e usar o LP50 em um sistema
- Bloqueie o dispositivo quando não estiver usando
- Ejete 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 LP50 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 LP50 automaticamente limpará os dados criptografados - formatando-se de volta para as configurações de fábrica.

Multissenhas
O LP50 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 LP50 pode suportar duas senhas diferentes utilizadas para recuperar os dados - funções de senha de Admin e Usuário.

O LP50 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 já que a segurança não tem porta dos fundos. A Kingston recomenda que você também tenha os dados salvos em outra mídia. O LP50 pode ser redefinido e reutilizado, mas os dados anteriores serão excluídos para sempre.

Modos de senha
O LP50 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 LP50 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.

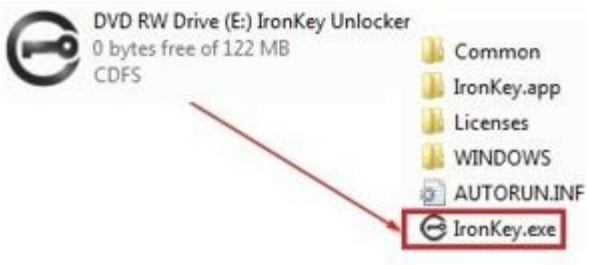
Uma frase-passe é basicamente qualquer combinação de caracteres, incluindo caracteres de outro idioma. Como o drive LP50, o idioma da senha pode combinar o idioma selecionado para o drive. Isso permite que você selecione múltiplas palavras, uma frase, letra de uma música, uma linha de uma poesia etc. 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.

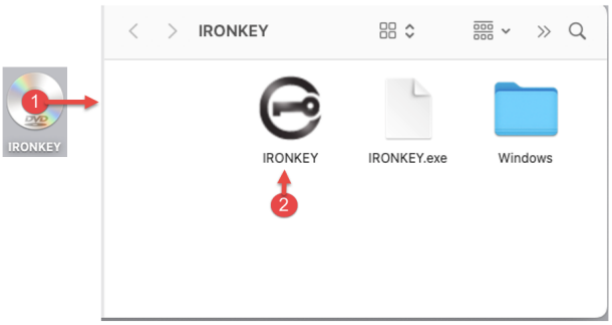
Acesso ao dispositivo (Ambiente Windows)

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

• Usuários do Windows 8.1/10/11 receberão uma notificação do driver de 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 LP50 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 CD-ROM do IronKey. • 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 IKLP**

Inicialização do dispositivo (Ambiente Windows e macOS)

Idioma e EULA

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

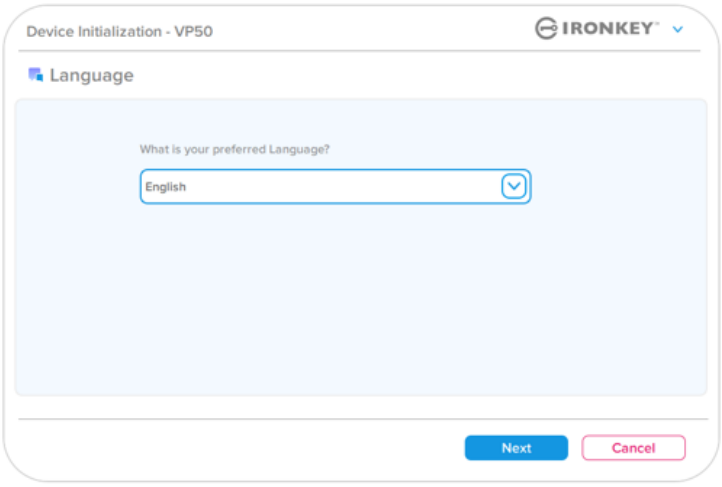


Figura 4.1 – Seleção de idioma

- Analise o acordo de licença e clique em **Avançar** (Next).

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

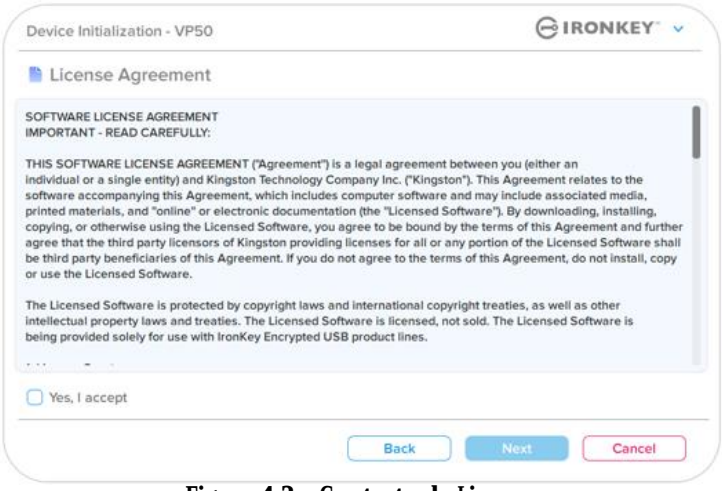


Figura 4.2 – Contrato de Licença

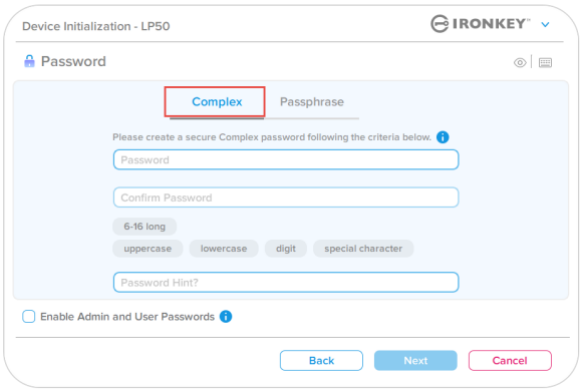
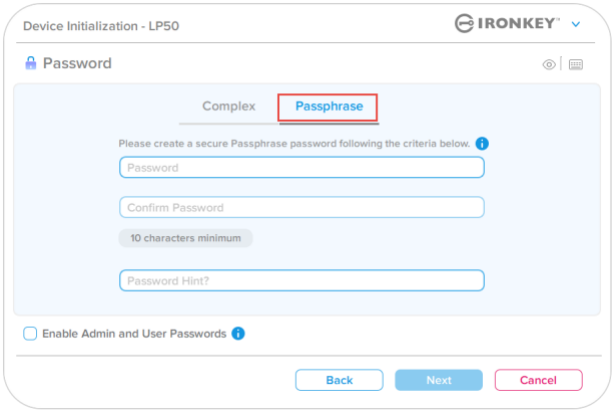
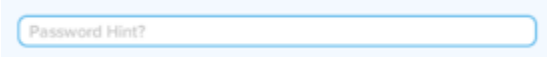
Inicialização do dispositivo

Escolha de senha

Na tela de mensagem de Senha, você poderá criar uma senha para proteger seus dados no LP50 usando os modos de senha Complexas ou de Passe-frase (*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 passe-frase 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 (Complex) • Deve conter 6 caracteres ou mais (até 16 caracteres). • Deve conter três (3) dos seguintes critérios: o Letra maiúscula o Letra minúscula o Dígito numérico o Caracteres especiais (!,$,&, etc.)	 **Figura 4.3 – Senha complexa**
Senha de frase-passe (Passphrase) • Deve conter: o Mínimo de 10 caracteres o Máximo de 64 caracteres	 **Figura 4.4 - Senha de frase-passe**
Dica de senha (Password Hint) (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 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*)

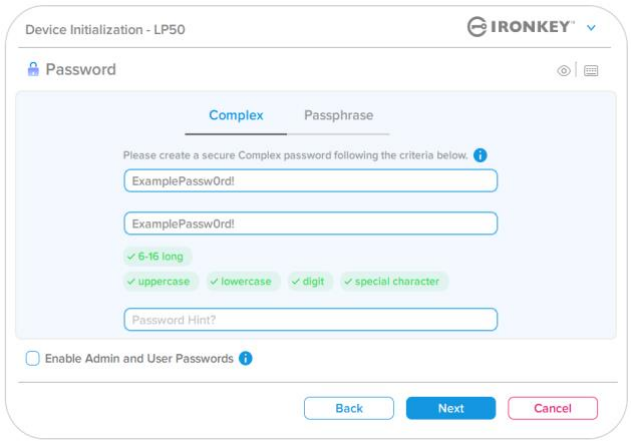


Figura 4.6a – Condição de senha complexa atendida

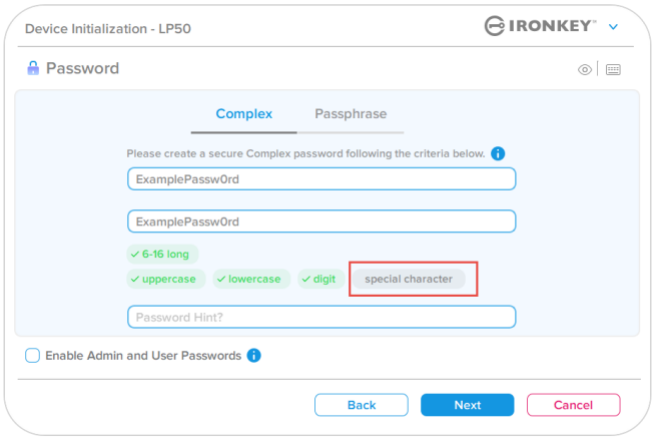


Figura 4.6b – Condição de senha complexa opcional

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.

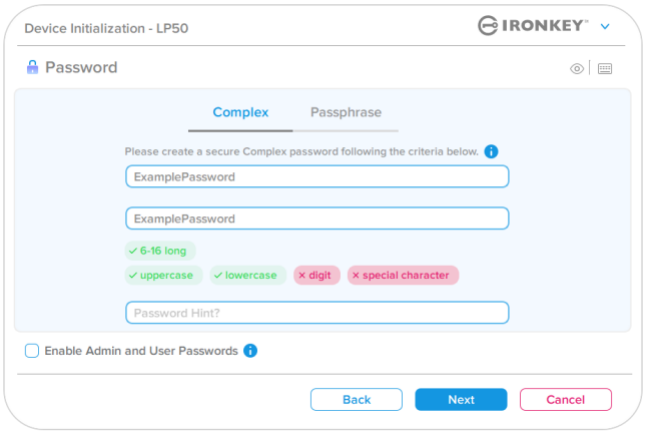


Figura 4.7 – Condições de senha não atendidas

Inicialização do dispositivo

Teclado virtual
O LP50 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** (Device Initialization) e clique nele.

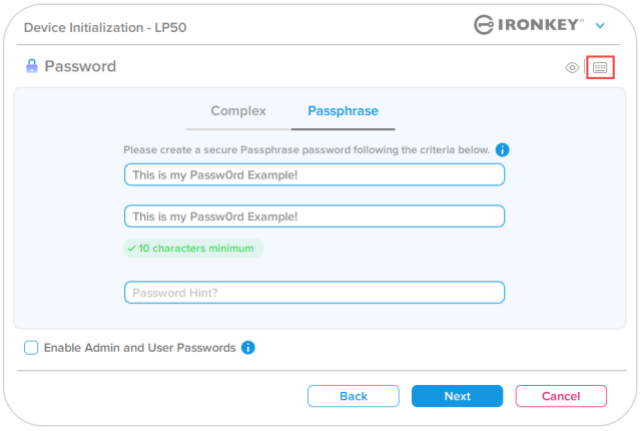


Figura 4.8 – Ativando o Teclado virtual

- Quando o teclado virtual aparecer, você também pode habilitar a **Proteção contra registros da tela** (Screenlogger Protection). 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 randomizar na parte inferior direita do teclado. A **Randomização** vai ordenar as teclas em uma ordem aleatória.

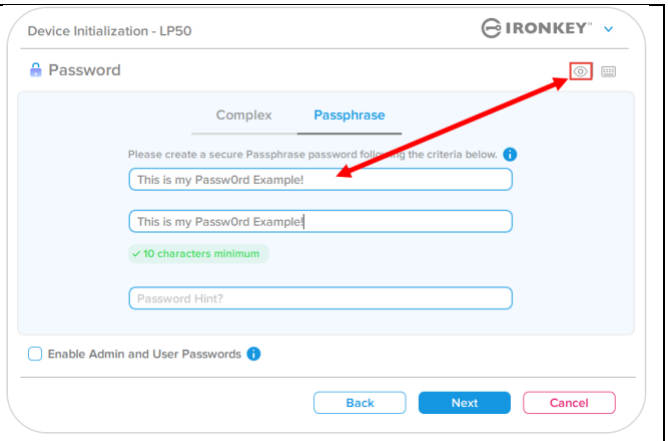
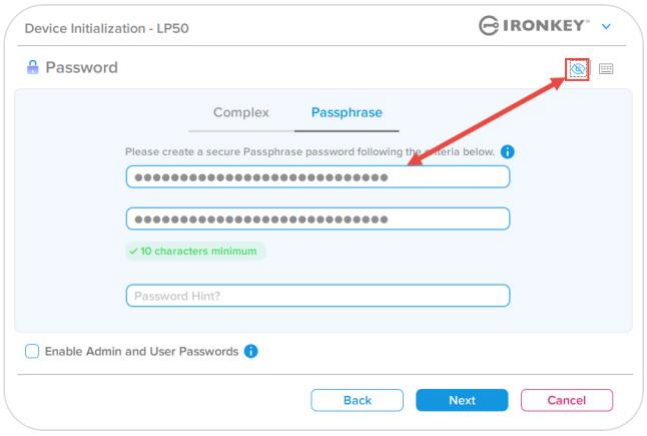
Figura 4.9 – Proteção contra registro de tela / Randomização

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.

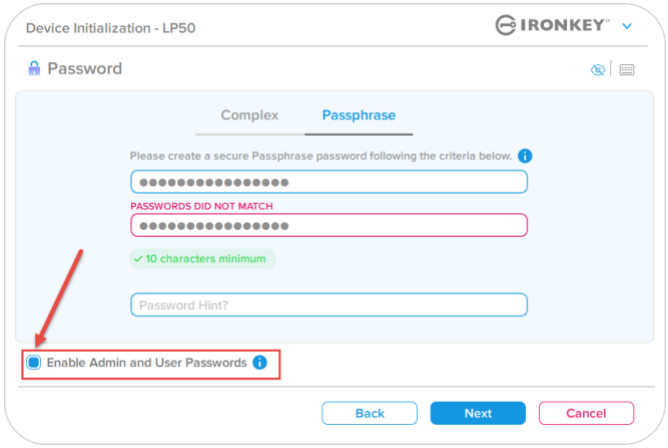
Com as **senhas de Admin e de Usuário** habilitadas, você também pode acessar:

- Redefinição da senha de Usuário

Para saber mais sobre o recurso da senha de Usuário, vá até a página 28 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** (Enable Admin and User Passwords) e selecione **Avançar** (Next) assim que uma senha válida for escolhida. (*Figura 4.12*)

- Se este recurso estiver **habilitado**, então a senha escolhida nesta tela será a **senha de Admin**. Clique em **Avançar** (Next) 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** (User Password) (*Figura 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..

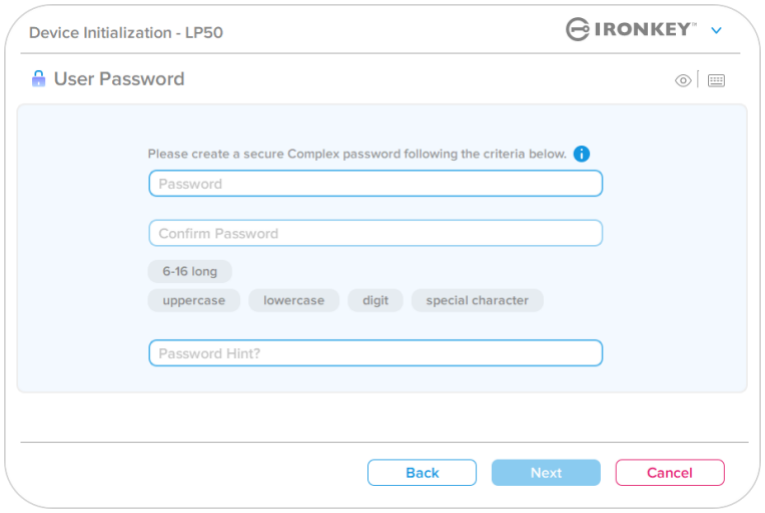


Figura 4.13 - Senha de Usuário (Admin e Usuário habilitados)

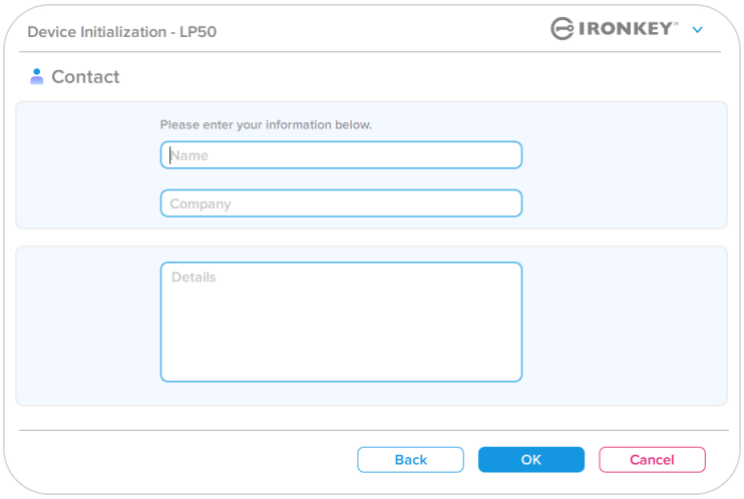
Observação: O critério da Opção de senha escolhida (complexa ou passe-frase) vai se estender à Senha de Usuário, redefinição de senhas necessárias depois que o drive for instalado. A opção de senha escolhida pode ser alterada apenas depois de uma completa restauração do dispositivo.

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 '**Nome** (Name) pode conter até 32 caracteres, mas não pode conter a senha **exata**. O campo '**Empresa** (Company) pode conter até 32 caracteres, mas não pode conter a senha **exata**. O campo '**Detalhes** (Details) pode conter até 156 caracteres, mas não pode conter a senha **exata**.	 **Figura 4.14 - Informações de contato**

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

USB ß → Inicialização de Nuvem (Ambiente Windows)

Uma vez que o dispositivo foi iniciado no Windows, o aplicativo USB-to-Cloud aparecerá como visto na *Figura 5.1* à direita. Certifique-se de que a conexão à Internet está funcionando antes de continuar.

- Para prosseguir com a instalação, clique no botão 'Aceitar (Accept) verde no canto inferior direito da janela clevX.
- Para recusar a instalação, clique no botão 'Recusar (Decline) vermelho no canto inferior esquerdo da janela clevX.
- (Observação: Se você clicar no botão vermelho 'Recusar, a instalação USB-to-Cloud será cancelada. Ao fazer isso, um arquivo de texto especial chamado 'USBtoCloudInstallDeclined.txt é criado na partição de dados. A presença deste arquivo irá impedir que o aplicativo pergunte sobre a instalação no futuro.)

Figura 5.1 – USBtoCloud Windows EULA

- Se a seguinte janela de Alerta de Segurança do Windows aparecer durante o processo de inicialização, clique em "Permitir acesso" para continuar (ou crie uma Exceção de Firewall no Windows) para que o aplicativo USB-to-Cloud continue.

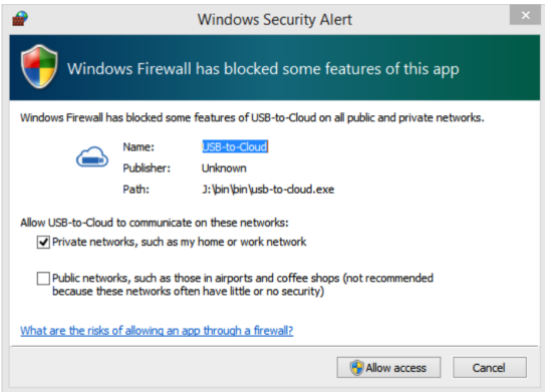


Figura 5.2 – Alerta de segurança do Windows

USB ß → Inicialização de Nuvem (Ambiente Windows)

- Quando a instalação estiver concluída, você verá o aplicativo com uma lista de opções para selecionar (para sincronizar os dados do seu LP50.)
- Selecione a opção de nuvem que deseja usar como seu aplicativo de backup e forneça as credenciais necessárias exigidas para a autenticação.
- (Observação: Se você não tem atualmente uma conta configurada com alguma das opções de nuvem relacionadas, você pode criar uma neste momento, usando seu navegador de Internet, e depois completar com esta opção.)
- Assim que tiver selecionado uma opção de nuvem e autenticado o serviço correspondente, o programa USB-to-Cloud irá realizar uma comparação inicial da partição de dados com o que está armazenado na Nuvem. Desde que o serviço USB-to-Cloud esteja funcionando no Task Manager, será feito o backup automático do conteúdo gravado na partição dados (sincronizado) na Nuvem.

Figura 5.3 – Seleção de nuvem

USB ß → Uso de Nuvem (Ambiente Windows)

O aplicativo USB-to-Cloud oferece os seguintes serviços adicionais:

- Pausar backup (Pausa um backup de dados)
- Restaurar (Restaura dados da nuvem para o dispositivo)
- Configurações (Opções adicionais para seu backup de dados)
- Sair (Sai do serviço USB-to-Cloud)

No menu 'Configurações, você pode:

- Alterar qual aplicativo de serviço de nuvem você está usando atualmente para fazer backups.
- Alterar o idioma que você está usando no momento.
- Selecionar quais arquivos e/ou pastas você está fazendo backup para a nuvem.
- Verificar se há atualizações..

(**Observação:** Se você redefinir (ou formatar) o LP50, todos os dados contidos no dispositivo serão perdidos. Entretanto, qualquer dado armazenado na nuvem continua seguro e intacto.)

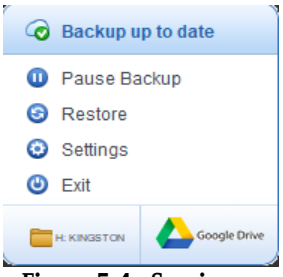


Figura 5.4 - Serviços

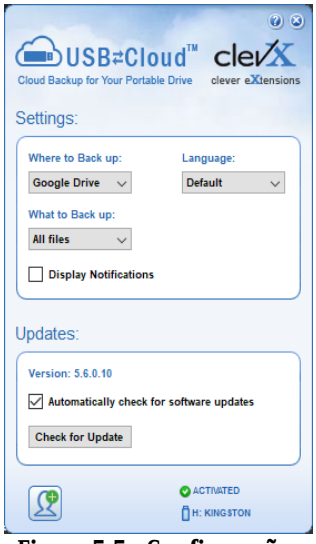


Figura 5.5 - Configurações

USB ß → Inicialização de Nuvem (Ambiente macOS)

- Quando o dispositivo for inicializado, o aplicativo USB-to-Cloud aparecerá como visto na *Figura 5.6* à direita. Certifique-se de que a conexão à Internet está funcionando antes de continuar.

- Para prosseguir com a instalação, clique no botão 'Aceitar (Accept) no canto inferior direito da janela clevX..

  (Observação: No macOS 12.x + será solicitada a permissão do acesso a arquivos em um volume removível. Selecione OK.) (*Ver Figura 5.7*)

- Para recusar a instalação, clique no botão 'Recusar (Decline) no canto inferior esquerdo da janela clevX.

Figura 5.6 – USBtoCloud macOS EULA

(Observação: Se você clicar no botão 'Recusar, a instalação do USB-to-Cloud será cancelada. Ao fazer isso, um arquivo de texto especial chamado 'DontInstallUSBtoCloud' é criado na partição de dados. A presença deste arquivo irá impedir que o aplicativo pergunte sobre a instalação no futuro.)

- Quando a instalação estiver concluída, você verá o aplicativo com uma lista de opções para selecionar (para sincronizar os dados do seu LP50.) (*Figura 5.8*)

Figura 5.7 - acesso macOS

- Selecione a opção de nuvem que deseja usar como seu aplicativo de backup e forneça as credenciais necessárias exigidas para a autenticação.

  (Observação: Se você não tem atualmente uma conta configurada com alguma das opções de nuvem relacionadas, você pode criar uma neste momento, usando seu navegador de Internet, e depois completar com esta opção.)

- Assim que tiver selecionado uma opção de nuvem e autenticado o serviço correspondente, o programa USB-to-Cloud irá realizar uma comparação inicial da partição de dados com o que está armazenado na Nuvem. Desde que o serviço USB-to-Cloud esteja funcionando no Task Manager, será feito o backup automático do conteúdo gravado na partição dados (sincronizado) na Nuvem.

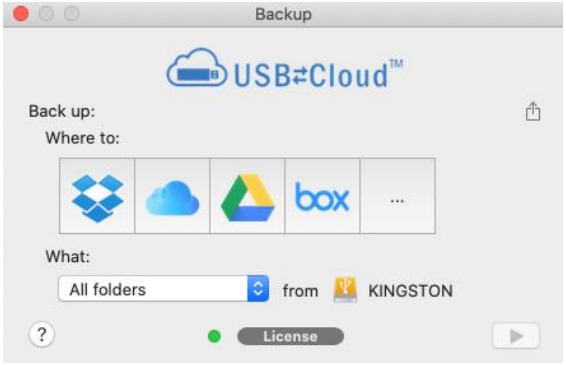


Figura 5.8 – Seleção de nuvem

USB ß →Uso de Nuvem (Ambiente macOS)

O aplicativo USB-to-Cloud oferece os seguintes serviços adicionais (*Figura 5.9*):

- **Pausar backup** (Pausa um backup de dados)
- **Restaurar** (Restaura dados da nuvem para o dispositivo)
- **Backup** (Abre opções de nuvem) *Ver Figura 5.9*
- **Sair** (Sai do serviço USB-to-Cloud)

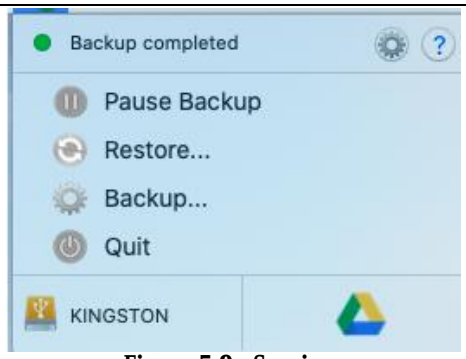


Figura 5.9 - Serviços

No menu 'Preferências, você pode:

- Alterar o idioma que você está usando no momento.
- Habilitar/desabilitar notificações sonoras
- Habilitar/desabilitar drive não montado se o app sair
- Habilitar/desabilitar logging para resolução de problemas
- Habilitar/desabilitar atualizações automáticas de software e para verificar atualizações agora

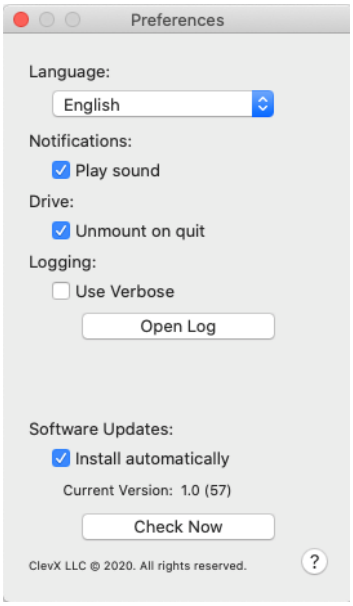


Figura 5.10 – Preferência USBtoCloud

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 LP50 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 (Login as 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*).

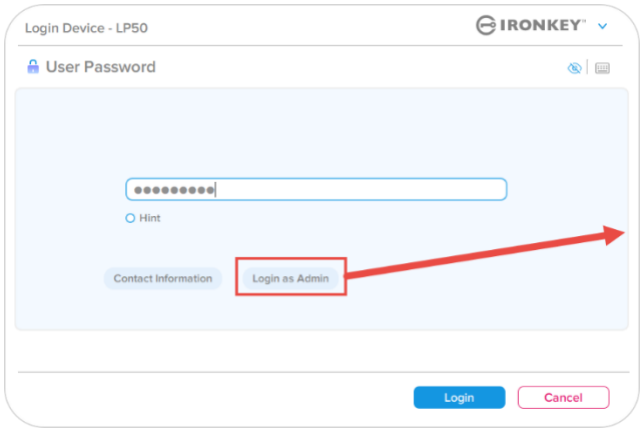


Figura 6.1 - Login de Senha de Usuário (Admin habilitado)

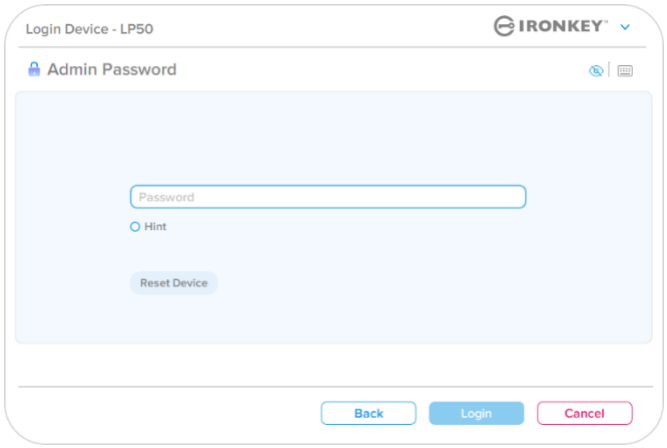


Figura 6.2 - Login de senha do Admin

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 do 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 no seu drive. (*Figura 6.3*)

Observação: Para habilitar as senhas de Admin e de Usuário, use o botão **Restaurar dispositivo** (Reset Device) 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.**

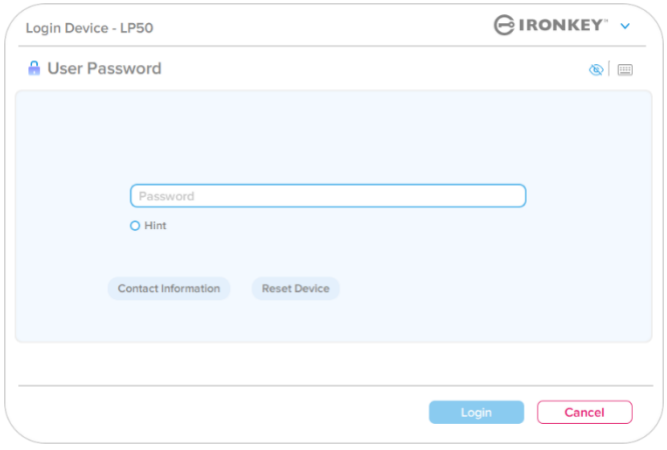


Figura 6.3 - Login de Senha de Usuário (Admin não habilitado)

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	**Proteção de Força Bruta Comportamento do dispositivo (10 tentativas de senha incorretas)**	**Apagar dados e Restaurar 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 NÃO habilitado)	**Proteção de Força Bruta Comportamento do dispositivo (10 tentativas de senha incorretas)**	**Apagar dados e Restaurar dispositivo?**
Senha de Usuário	Apagar drive criptograficamente, Senhas, configurações e dados apagados para sempre	**SIM**

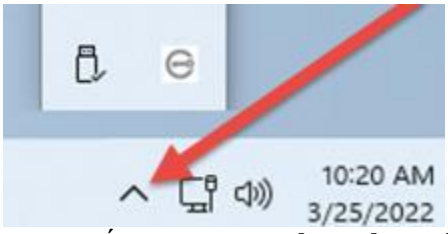
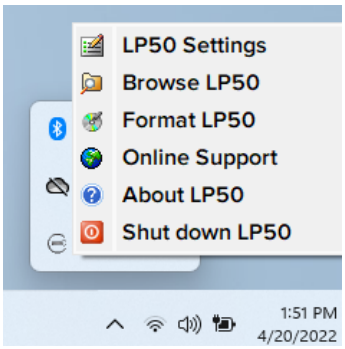
* Depois que você fizer a autenticação no dispositivo corretamente, o contador de erros de login será reiniciado em relação ao método de Login foi utilizado. Apagar criptograficamente apagará todas as senhas, dados e chaves de criptografia – **seus dados serão perdidos para sempre.**

Acessar meus arquivos seguros

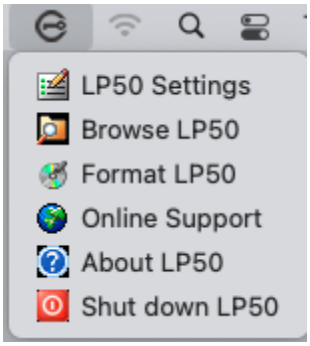
Depois de desbloquear o dispositivo, você pode acessar seus arquivos seguros. Os arquivos são automaticamente criptografados e descriptografados quando você salva ou abre os arquivos no drive. Esta tecnologia gera a conveniência de trabalhar como você faria normalmente com um drive regular, enquanto fornece uma segurança forte e ininterrupta.
Dica: Você também pode acessar seus arquivos clicando com o botão direito no **Ícone IronKey** na barra de tarefas do Windows e clicando em **Browse LP50** (*Figura 7.2*)

Opções do dispositivo - (Ambiente Windows)

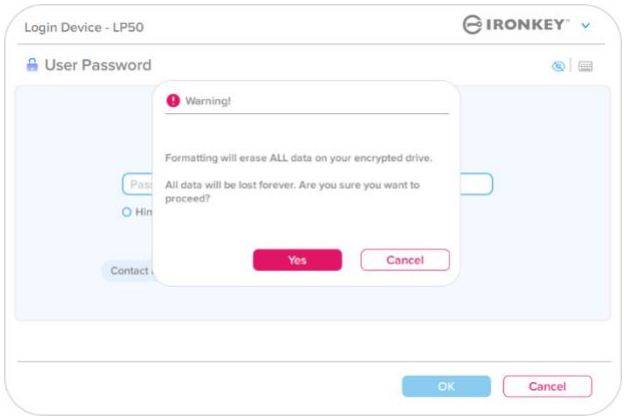
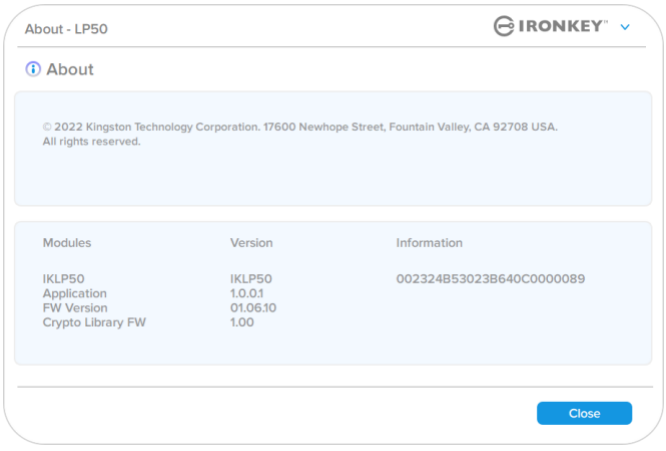
Enquanto você estiver logado no dispositivo, haverá um Ícone IronKey localizado no canto direito da janela. Clicar com o botão direito no Ícone IronKey abrirá o menu de seleção para opções do drive disponíveis (*Figura 6.2*). Detalhes sobre essas opções do dispositivo podem ser encontradas nas Páginas 19-23 deste manual.

• Enquanto você estiver logado no dispositivo, haverá um ícone IronKey localizado no canto direito da janela. (*Figura 7.1*)	 **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. (*Figura 7.2*) 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 LP50 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 LP50:	• Alterar senha de login, Informações de contato e outras configurações. (Mais detalhes sobre configurações do dispositivo podem ser encontrados na seção 'Configurações do LP50 deste manual).
Browse LP50:	• Permite que você visualize seus arquivos seguros.
Formatar o LP50: 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 LP50**
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 LP50: Fornece detalhes específicos sobre o LP50, 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 LP50**
Desligar o LP50:	• Encerra de modo apropriado o LP50, permitindo que seja removido com segurança do seu sistema.

Configurações do LP50

Configurações do Admin

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

- **Senha (Password):** Permite que você altere sua própria senha de Admin e/ou dica (*Figura 8.1*)
- **Informações de contato (Contact Info):** Permite que você adicione/visualize/altere suas informações de contato (*Figure 8.2*)
- **Idioma (Language):** Permite que você altere sua seleção de idioma atual (*Figura 8.3*)
- **Opções do Admin (Admin Options):** 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.

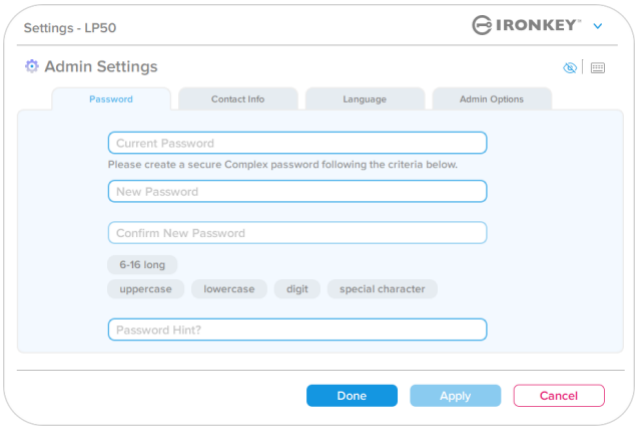


Figura 8.1- Opções de senha do Admin

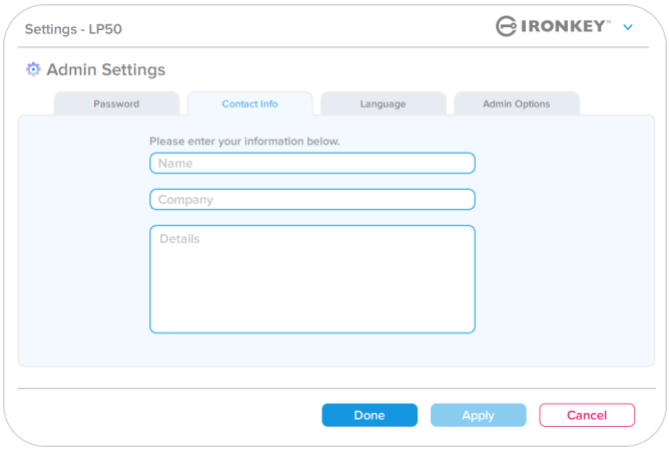


Figura 8.2 - Informações de contato

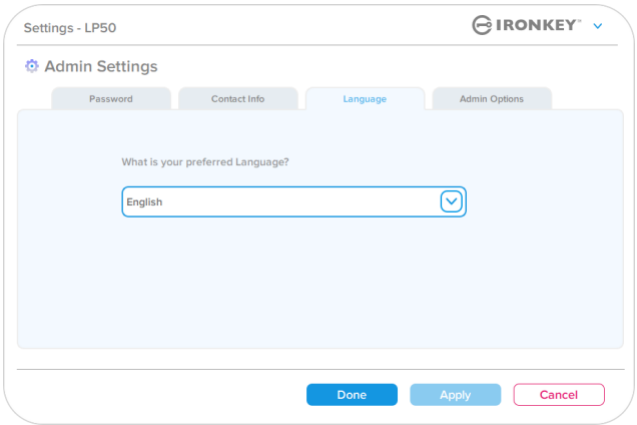


Figura 8.3 - Opções de idioma

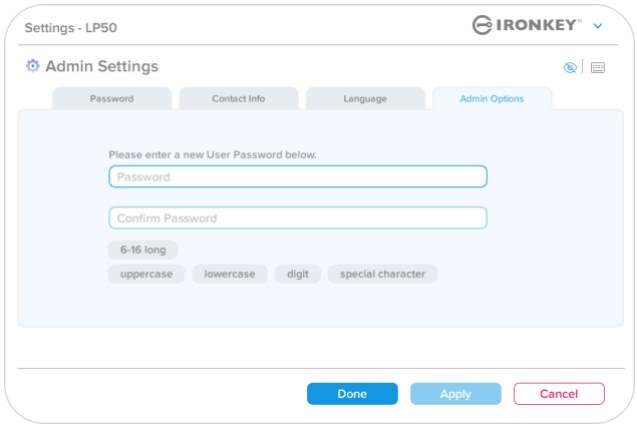
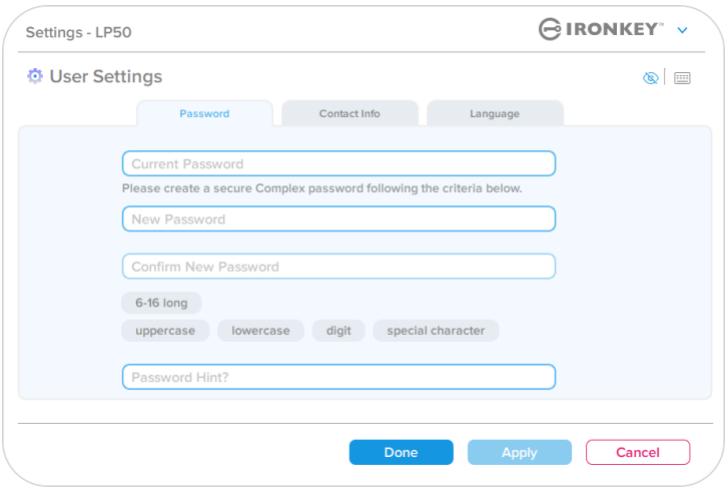
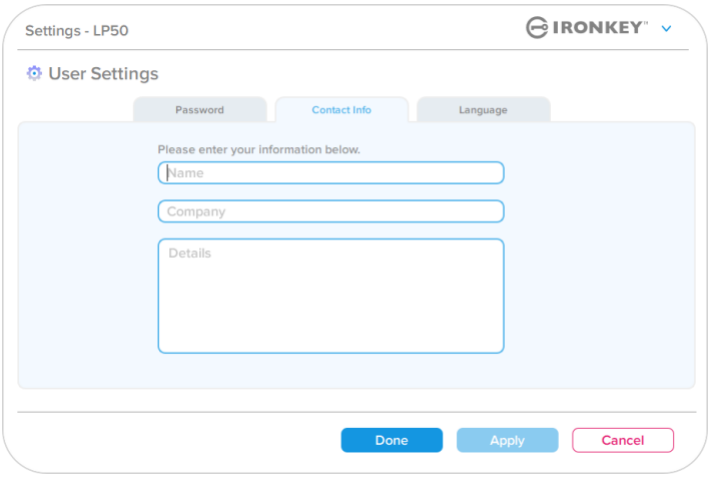
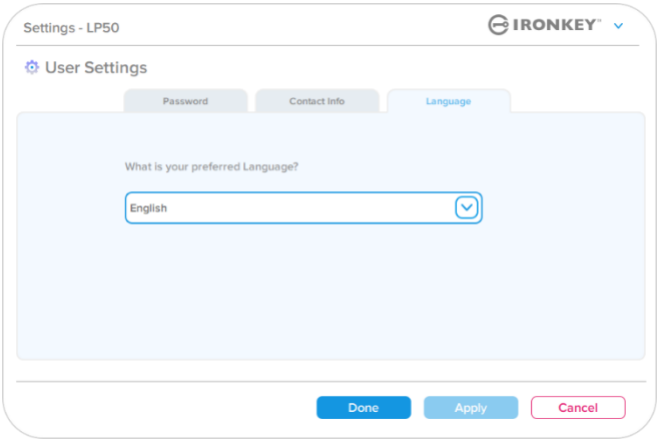


Figura 8.4 - Opções do Admin

Configurações do LP50

Configurações do Usuário: Admin habilitado

O login do Usuário limita o acesso às seguintes configurações:

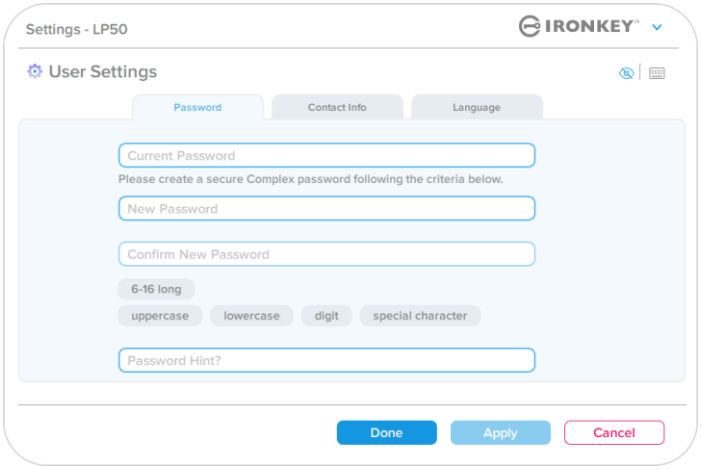
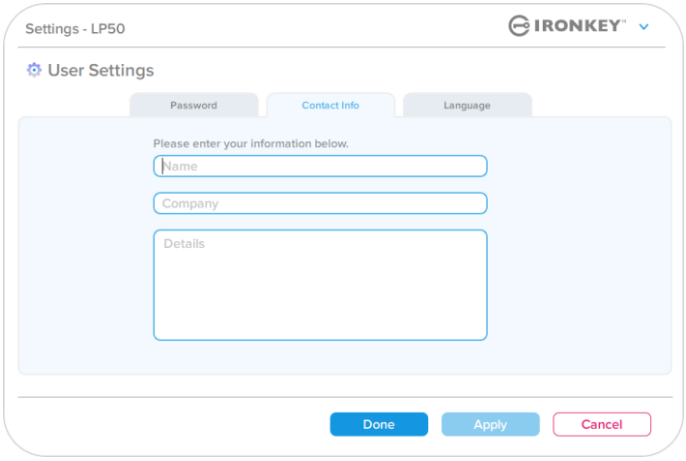
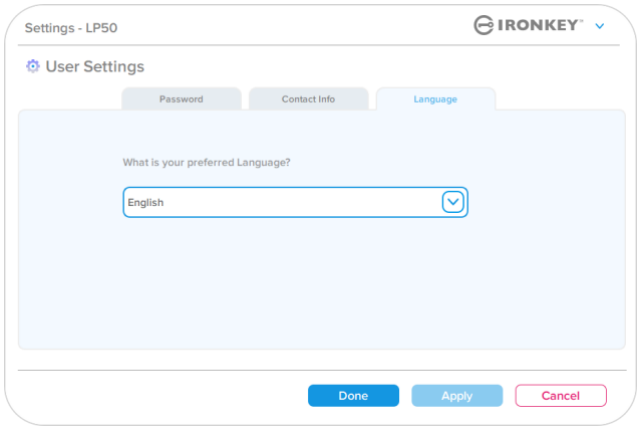
Senha (Password): Permite que você altere sua própria senha de Usuário e/ou dica. (*Figura 8.5*)	 **Figura 8.5 - Opções de senha (Admin habilitado: Login do Usuário)**
Informações de contato (Contact Info): Permite que você adicione/visualize/altere suas informações de contato. (*Figura 8.6*)	 **Figura 8.6 - Informações de contato (Admin habilitado: Login do Usuário)**
Idioma (Language): 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 LP50

Configurações do Usuário: Admin não habilitado

Como mencionado anteriormente na Página 12, iniciar o LP50 sem habilitar as senhas de 'Admin e de 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 LP50:

Senha (Password): 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 (Contact Info): Permite que você adicione/visualize/altere suas informações de contato. (*Figura 8.9*)	 **Figura 8.9 - Informações de contato (Modo Somente Usuário)**
Idioma (Language): Permite que você altere sua seleção de idioma atual. (*Figura 8.10*)	 **Figura 8.10 - Definições de Idioma (Modo Somente Usuário)**

Configurações do LP50

Alterar e Salvar configurações

- Sempre que as configurações forem alteradas nas Configurações do LP50 (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*)

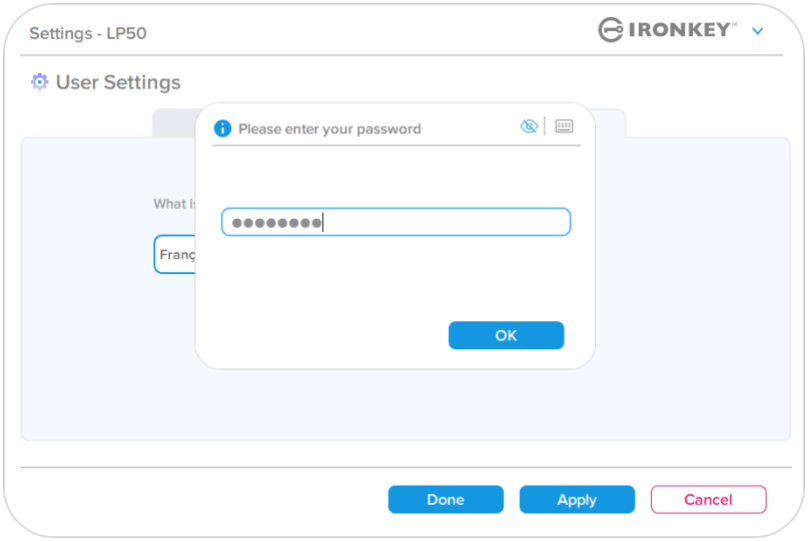


Figura 8.11 - Tela de alerta de Senha para salvar as alterações de configurações do LP50

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 (OK). Isso fechará a caixa 'Insira sua Senha e voltará para o menu de configurações do LP50.

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 do 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 passe-frase ou complexa).

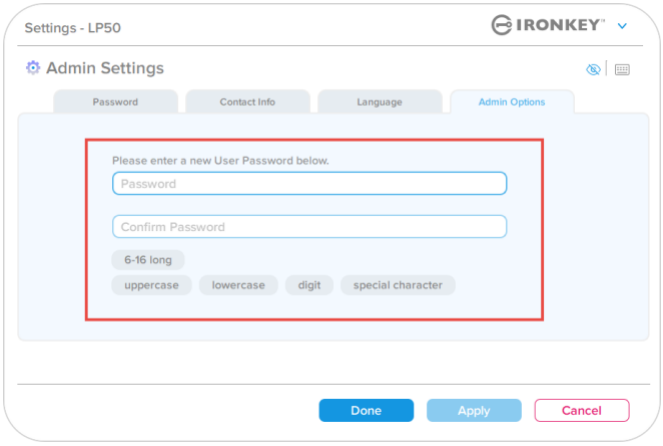


Figura 9.1 - Redefinição de Senha de Usuário/Opções do Admin

Ajuda e Resolução de Problemas

Bloqueio do dispositivo

O LP50 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*)

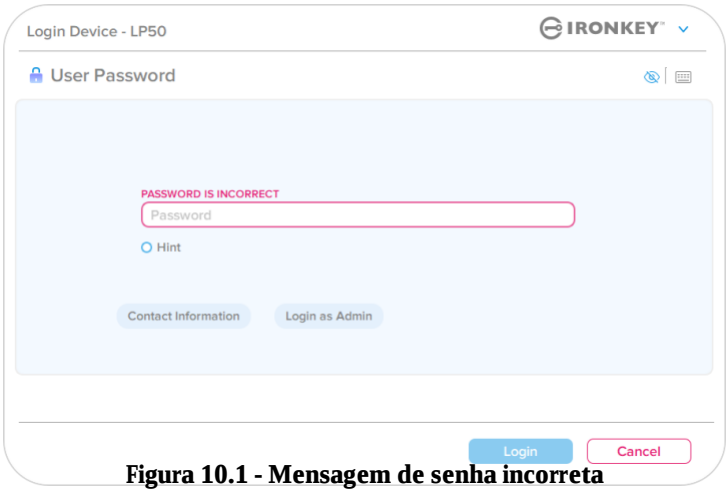


Figura 10.1 - Mensagem de senha incorreta

- 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*)

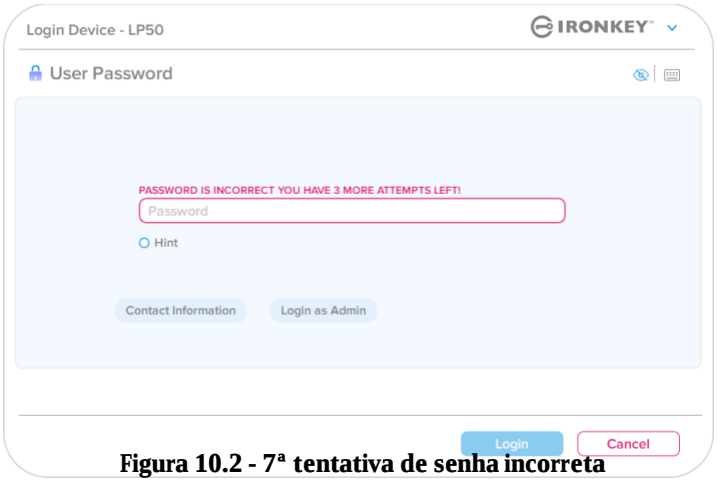


Figura 10.2 - 7ª tentativa de senha incorreta

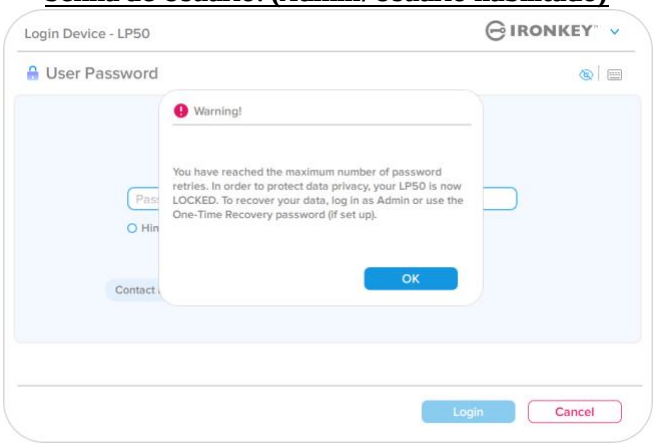
Ajuda e Resolução de Problemas

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 ou 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 18 desde Guia do Usuário.

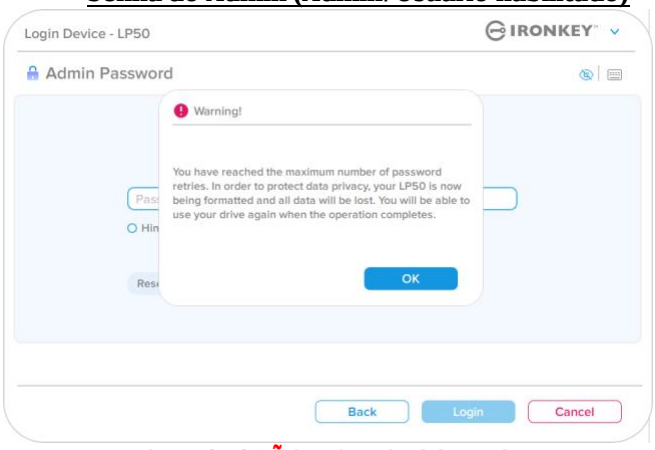
As Figuras 10.3 - 10.6 abaixo demonstram o comportamento visual do 10º e último login errado de cada método de senha de login:

Senha de Usuário: (Admin/Usuário habilitado)



BLOQUEIO DO DISPOSITIVO
Figura 10.3

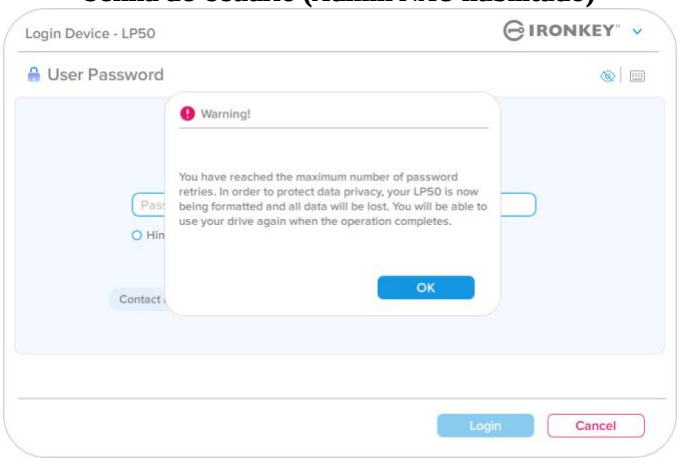
Senha do Admin (Admin/Usuário habilitado)



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 LP50 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 25.

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 LP50.*

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 da 'Senha de Usuário se o modo Admin/Usuário não estiver habilitado) quando o iniciador do LP50 for executado. (*Ver Figura 10.7 e 10.8*)

- Esta opção vai permitir que você crie uma nova senha, mas para proteger a privacidade dos seus dados, o LP50 será formatado. Isso significa que todos os seus dados serão apagados no processo.*

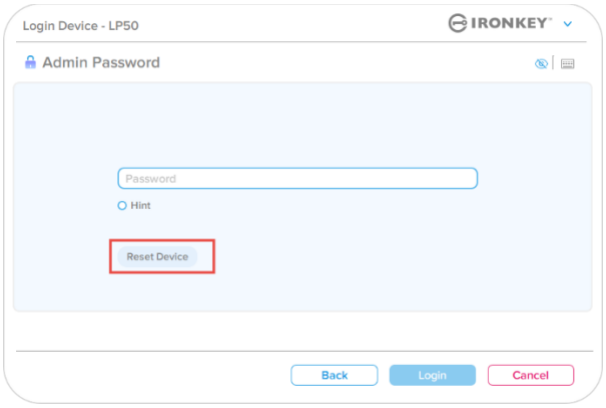


Figura 10.6 - Senha do Admin: Botão para Restaurar Dispositivo

- **Observação**: Quando você clicar em '*Restaurar dispositivo* (Reset Device), 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*)

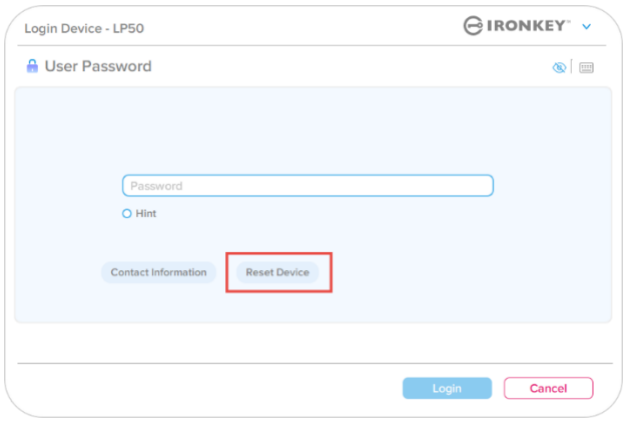


Figura 10.7 - Senha de Usuário (Admin/Usuário não habilitado) Restaurar Dispositivo

- 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.

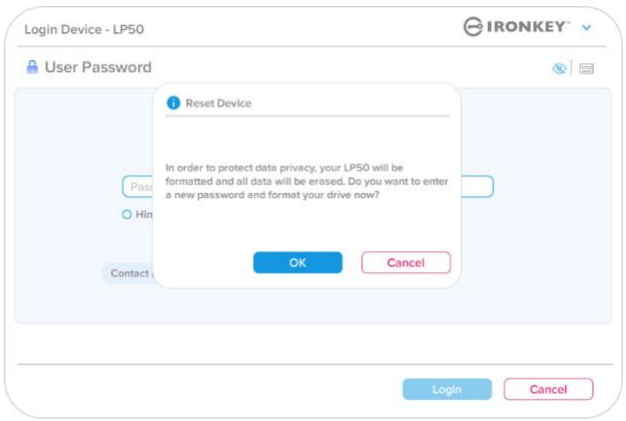


Figura 10.8 - confirmação para Restaurar Dispositivo

Ajuda e Resolução de Problemas

Conflito de letra do drive: Sistemas operacionais Windows

- Como mencionado na seção de '*Requisitos do Sistema* deste manual (na página 3), o LP50 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 LP50 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.)

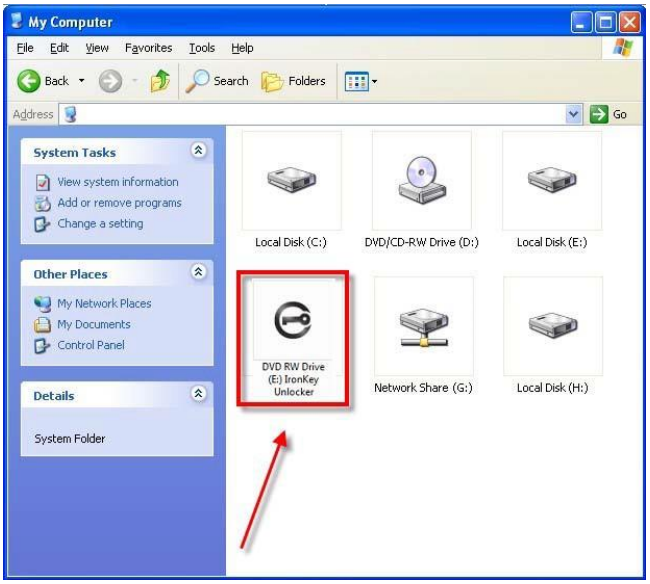


Figura 10.9 - Exemplo de letra de drive

Neste exemplo, (*Figura 10.9*), o LP50 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 LP50 pode tentar utilizá-lo como sua segunda letra de drive, causando um conflito.

Se não existirem compartilhamentos de rede no seu sistema e o LP50 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 8.1, 10 e 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 for para mais assistência.

IRONKEY™ Locker+ 50 (LP50)
SZYFROWANA PAMIĘĆ FLASH USB 3.2 Gen 1

Instrukcja obsługi

Spis treści

Ilustracja 1 – Urządzenie IronKey LP50

Wprowadzenie

Pamięci flash USB Kingston IronKey Locker+ 50 oferują zabezpieczenia klasy konsumenckiej z szyfrowaniem sprzętowym AES w trybie XTS, w tym ochronę przed atakami metodą BadUSB dzięki cyfrowo podpisanemu oprogramowaniu sprzętowemu oraz przed atakami siłowymi (Brute Force) na hasła. Pamięć LP50 jest również zgodna z aktem prawnym TAA (Trade Agreements Act).

Pamięć LP50 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 wprowadzonych z rzędu nieprawidłowych hasłach, a jeżeli hasło administratora zostanie wprowadzone niepoprawnie 10 razy z rzędu, wymazuje kryptograficznie pamięć. Co więcej, wbudowana klawiatura wirtualna chroni hasła przed oprogramowaniem rejestrującym naciśnięcia klawiszy (keylogger) lub zawartość ekranu (screenlogger).

Pamięć Locker+ 50 została zaprojektowana z myślą o wygodzie użytkowania, więc umieszczono ją w małej metalowej obudowie z zaczepem na kółko do kluczy, dzięki czemu pozwala swobodnie przenosić zapisane dane. Pamięć LP50 jest także wyposażona w opcjonalną funkcję tworzenia kopii zapasowych USBtoCloud (firmy ClevX®), umożliwiającą dostęp do danych zapisanych w pamięci z wykorzystaniem usługi pamięci w chmurze: Google Drive™, OneDrive (Microsoft®), Amazon Cloud Drive, Dropbox™ lub Box. Każdy użytkownik może z łatwością skonfigurować pamięć LP50, ponieważ nie wymaga to instalacji żadnej aplikacji, a całe potrzebne oprogramowanie i zabezpieczenia znajdują się już w pamięci. Urządzenie działa w systemach Windows® i macOS®, co umożliwia użytkownikom dostęp do plików z wielu systemów.

Pamięć LP50 jest objęta ograniczoną 5-letnią gwarancją i bezpłatną pomocą techniczną firmy Kingston.

Charakterystyka pamięci IronKey Locker+ 50

- Szyfrowanie sprzętowe XTS-AES (nie można go nigdy wyłączyć)
- Ochrona przed atakami metodą Brute Force i BadUSB
- Opcje wielu haseł (Multi-Password)
- Tryby hasła złożonego i wyrażenia hasłowego
- 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 (09242024)
Niniejsza instrukcja obsługi dotyczy pamięci IronKey Locker+ 50 (LP50).

Wymagania systemowe

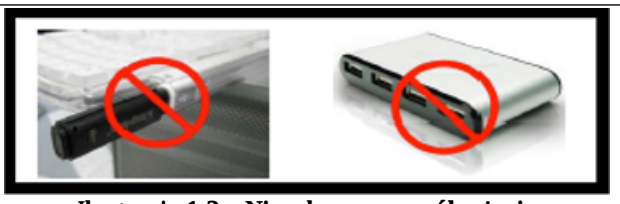
Platforma PC • Intel i AMD • 15MB wolnego miejsca na dysku • Dostępny port USB 2.0/3.2 • Dwie kolejne litery dysku po ostatnim dysku fizycznym* *** Uwaga:** Patrz rozdział „Konflikt liter dysków” na str. 32.	**Obsługiwane systemy operacyjne komputerów PC** • Windows 11 • Windows 10
Platforma Mac • Intel i Apple SOC • 15MB wolnego miejsca na dysku • Port USB 2.0/3.2	**Obsługiwane systemy operacyjne komputerów Mac** • macOS 12.x – 15.x

Uwaga: Po aktywacji każde urządzenie pamięci jest objęte bezpłatną 5-letnią subskrypcją usługi USBtoCloud. Po zakończeniu tego okresu możliwe jest dalsze odpłatne korzystanie z usługi firmy ClevX.

Zalecenia

Aby zagwarantować odpowiednie zasilanie urządzenia LP50, należy podłączać je bezpośrednio do portu USB w notebooku lub komputerze stacjonarnym, jak pokazano na *ilustracji 1.1*. Należy unikać podłączania urządzenia LP50 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 LP50 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 firma Kingston zaleca:

- Przeprowadzenie skanowania antywirusowego na komputerze przed skonfigurowaniem i użyciem pamięci LP50 w systemie docelowym
- Zablokuj urządzenie, gdy nie jest używane
- Wysuń urządzenie z systemu przed jego odłączeniem
- Nie odłączaj urządzenia, gdy świeci się jego dioda LED. Może to spowodować uszkodzenie pamięci wymagające ponownego sformatowania, co będzie skutkować usunięciem danych
- Nie udostępniaj hasła innym osobom

Najnowsze aktualizacje i informacje

Odwiedź stronę kingston.com/support, aby uzyskać najnowsze wersje oprogramowania pamięci, często zadawane pytania, dokumentację i dodatkowe informacje.

UWAGA: Należy instalować wyłącznie najnowsze wersje 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 LP50 ma silne zabezpieczenia. Obejmuje to ochronę przed atakami metodą Brute Force, która uniemożliwia hakerom odgadywanie haseł dzięki ograniczeniu liczby prób wprowadzenia hasła do 10. Po osiągnięciu tego limitu pamięć LP50 automatycznie wymaże zaszyfrowane dane, formatując się z powrotem do stanu fabrycznego.

Wiele haseł (funkcja Multi-Password)
Jedną z głównych funkcji funkcji pamięci LP50 jest obsługa wielu haseł, która pomaga chronić przed utratą danych w przypadku zapomnienia jednego lub więcej haseł. Gdy wszystkie opcje haseł są włączone, pamięć LP50 może obsługiwać dwa różne hasła, które można wykorzystać do odzyskania danych – hasło administratora oraz hasło użytkownika.

Pamięć LP50 pozwala wybrać dwa główne hasła: hasło administratora oraz hasło użytkownika. Administrator może w dowolnej chwili uzyskać dostęp do pamięci i skonfigurować opcje dla użytkownika – jest kimś w rodzaju „superużytkownika".

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. Firma Kingston nie będzie w stanie odzyskać danych, ponieważ zastosowanego mechanizmu zabezpieczenia nie można obejść. Firma Kingston zaleca zapisywanie danych również na innych nośnikach. Pamięć LP50 można bezpiecznie wymazać w celu ponownego wykorzystania, ale znajdujące się w niej dane zostaną bezpowrotnie usunięte.

Tryby hasła
Pamięć LP50 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 znaków:

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

Wyrażenie hasłowe
Pamięć LP50 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 LP50. Pozwala to na wybranie wielu słów, frazy, tekstu piosenki, wersu z wiersza itp. Dobre wyrażenia hasłowe są jednymi z najtrudniejszych rodzajów haseł do odgadnięcia przez atakującego, a jednocześnie mogą być łatwiejsze do zapamiętania przez użytkownika.

Konfiguracja urządzenia

Aby zapewnić wystarczające zasilanie szyfrowanej pamięci USB IronKey, należy podłączyć ją bezpośrednio do portu USB 2.0/3.0 w notebooku lub komputerze stacjonarnym. Unikaj podłączania pamięci do jakichkolwiek urządzeń peryferyjnych, które mogą być wyposażone w port USB, takich jak klawiatura lub koncentrator zasilany przez USB. Początkową konfigurację urządzenia należy przeprowadzić na 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 system Windows ją wykryje.

- W systemie Windows 8.1/10/11 wyświetli się powiadomienie dotyczące instalacji sterownika urządzenia (*ilustracja 3.1*).

Ilustracja 3.1 – Powiadomienie o instalacji sterownika urządzenia

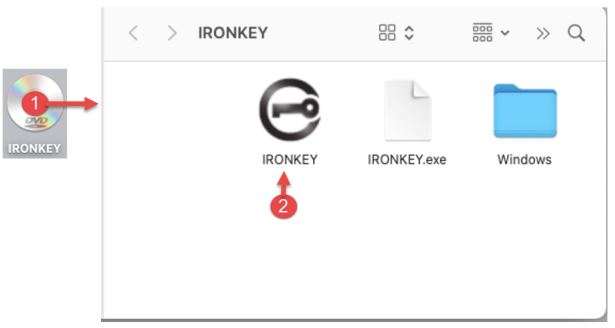
- Po zakończeniu wykrywania nowego sprzętu wybierz opcję **IronKey.exe** w partycji Unlocker, którą można znaleźć w Eksploratorze plików (*ilustracja 3.2*).
- Pamiętaj, że litera partycji będzie się różnić w zależności od kolejnej wolnej litery dysku. Litera dysku może się zmienić w zależności od tego,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

Ilustracja 3.2 – Okno Eksploratora plików/IronKey.exe

Dostęp do urządzenia (środowisko macOS)

Włóż pamięć LP50 do dostępnego portu w notebooku lub komputerze stacjonarnym i zaczekaj, aż zostanie wykryta przez system operacyjny komputera Mac. Po wykryciu pamięci na pulpicie zostanie wyświetlony 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 inicjowania.

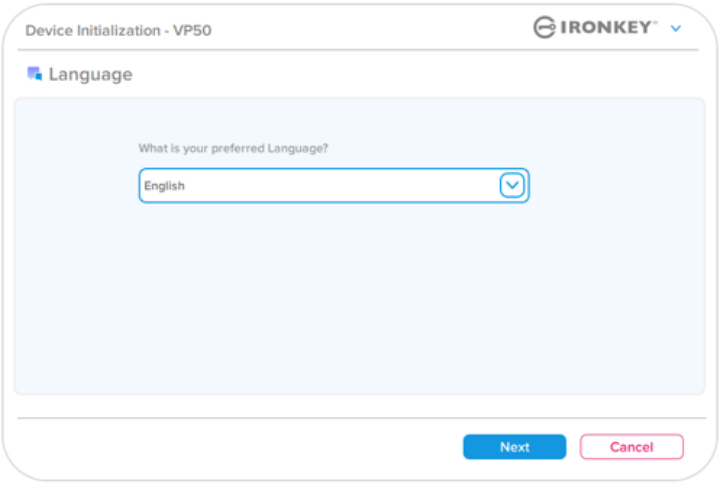


Ilustracja 3.3 – wolumin IKLP

Inicjowanie urządzenia (środowisko Windows i macOS)

Język i umowa licencyjna użytkownika końcowego

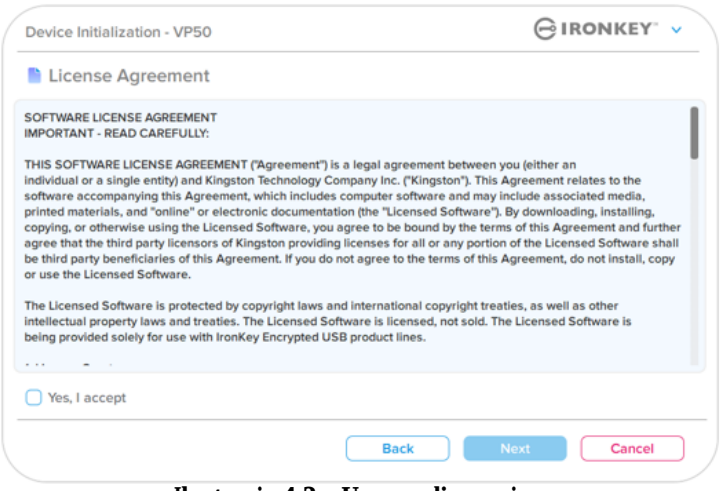
- Wybierz preferowany język z menu rozwijanego i kliknij przycisk **Next** (Dalej) (*patrz ilustracja 4.1*).



Ilustracja 4.1 – Wybór języka

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

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



Ilustracja 4.2 – Umowa licencyjna

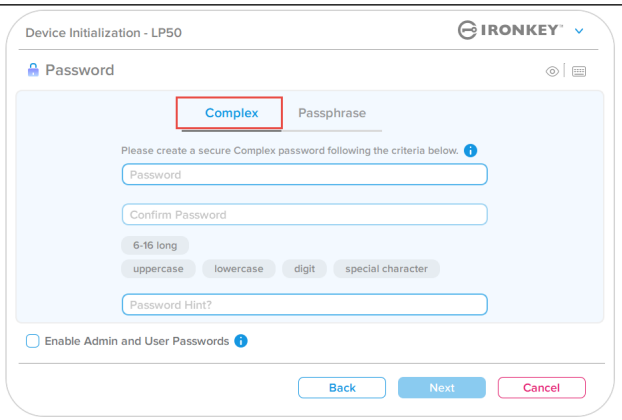
Inicjowanie urządzenia

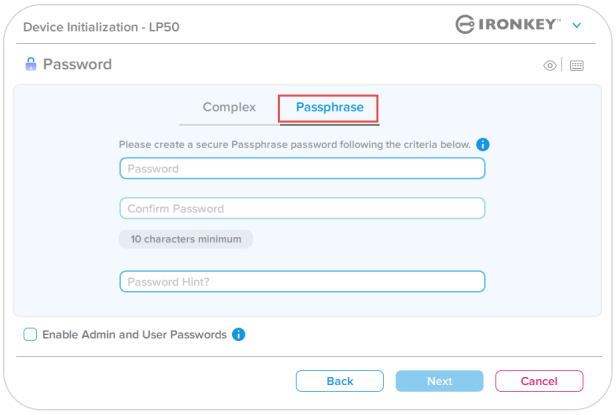
Wybór hasła

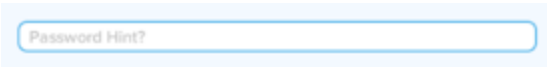
Na ekranie monitu o podanie hasła można utworzyć hasło do ochrony danych zapisanych w pamięci LP50, korzystając z trybu hasła złożonego lub wyrażenia hasłowego (*ilustracje 4.3-4.4*). Ponadto na tym ekranie można również włączyć opcje wielu haseł administratora/użytkownika. Zanim przejdziesz do wyboru hasła, zapoznaj się z informacjami dotyczącymi włączania haseł administratora/użytkownika poniżej, aby lepiej zrozumieć te funkcje.

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 inicjowania:

<table>
<tr>
<td>Hasło złożone (Complex Password)
Musi zawierać co najmniej 6 znaków (maks. 16 znaków).
Musi zawierać znaki należące do trzech (3) z następujących kategorii:
wielkie litery
małe litery
cyfry
znaki specjalne (!, $, & itp.)</td>
<td> 

Ilustracja 4.3 – Hasło złożone</td>
</tr>
<tr>
<td>Wyrażenie hasłowe (Passphrase)
Musi zawierać:
co najmniej 10 znaków
maksymalnie 64 znaki</td>
<td> 

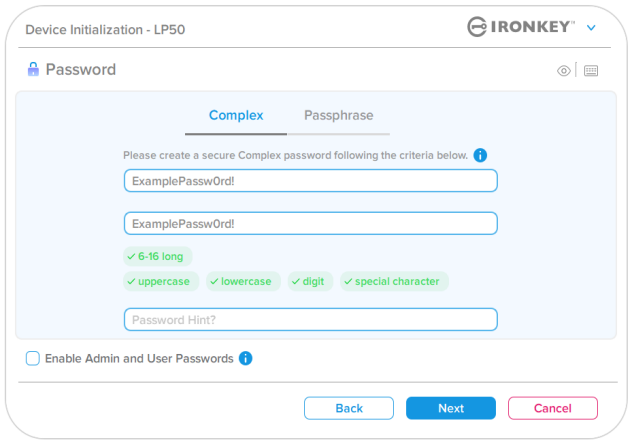
Ilustracja 4.4 – Wyrażenie hasłowe</td>
</tr>
<tr>
<td>Podpowiedź hasła (Password Hint) (opcjonalnie)
Podpowiedź hasła może być pomocna w przypomnieniu sobie zapomnianego hasła.
Uwaga: Podpowiedź NIE MOŻE być taka sama jak hasło.</td>
<td> 

Ilustracja 4.5 – Pole podpowiedzi hasła</td>
</tr>
</table>

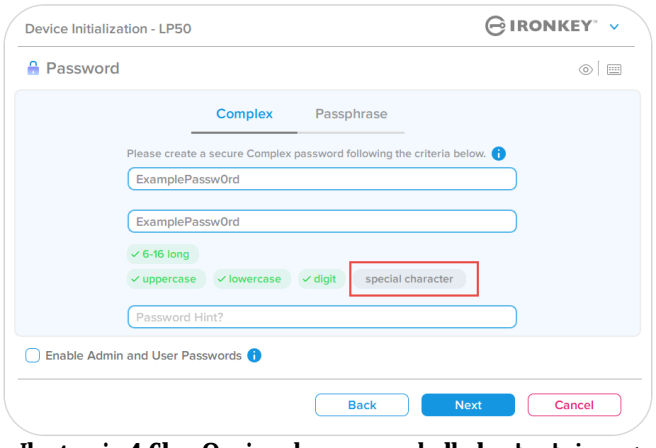
Inicjowanie urządzenia

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 hasła czwarte pole kryteriów stanie się szare, co oznacza, że to kryterium jest opcjonalne (*ilustracja 4.6b*).



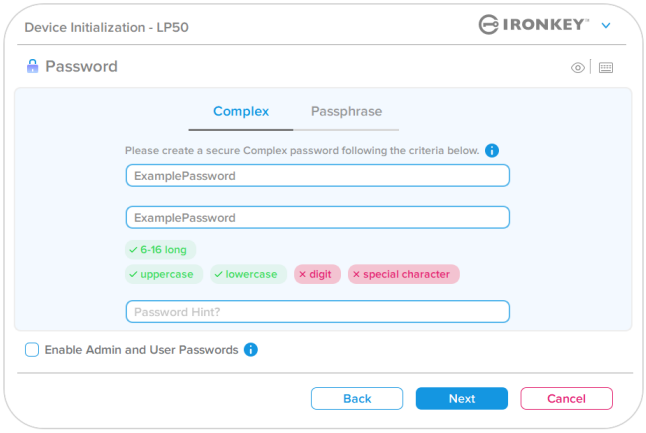
Ilustracja 4.6a – Spełnione warunki dla hasła złożonego



Ilustracja 4.6b – Opcjonalny warunek dla hasła złożoneg

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 wyrażeń hasłowych.

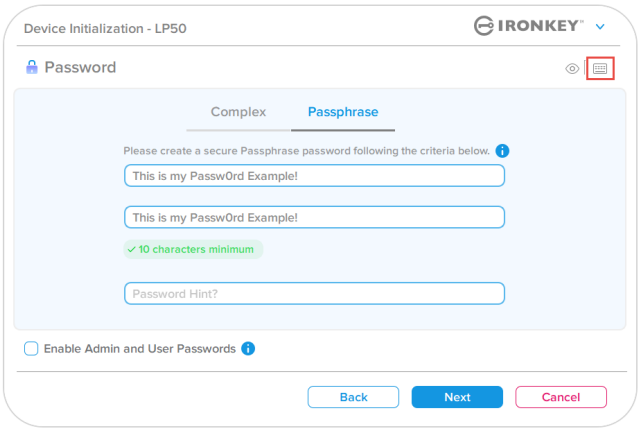


Ilustracja 4.7 – Niespełnione warunki dla hasła

Inicjowanie urządzenia

Wirtualna klawiatura
Pamięć LP50 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 **inicjalizacji urządzenia** (Device Initialization) i zaznacz go.



Ilustracja 4.8 – Aktywacja wirtualnej klawiatury

- Gdy pojawi się wirtualna klawiatura, możesz również włączyć funkcję ochrony przed **screenloggerami** (Screenlogger Protection). Podczas korzystania z tej funkcji wszystkie klawisze przez chwilę staną się niewidoczne. Jest to celowe działanie, ponieważ zapobiega przechwytywaniu kliknięć przez screenloggery..

- Aby ta funkcja była jeszcze bardziej skuteczna, możesz wybrać losowy układ wirtualnej klawiatury, klikając klawisz **randomizacji** (randomize) w prawym dolnym rogu klawiatury. Wybór tej opcji spowoduje rozmieszczenie klawiszy w losowy sposób.

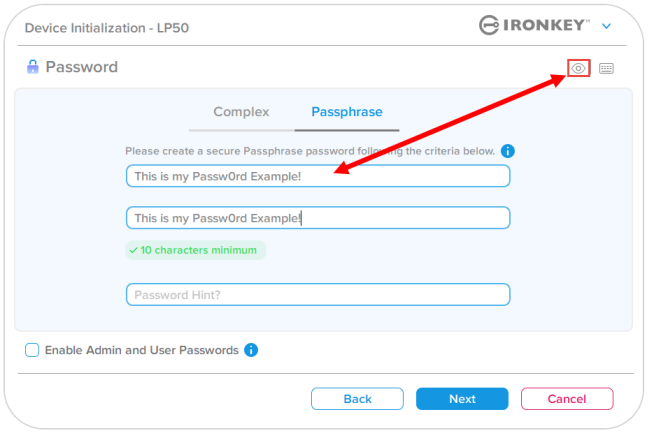
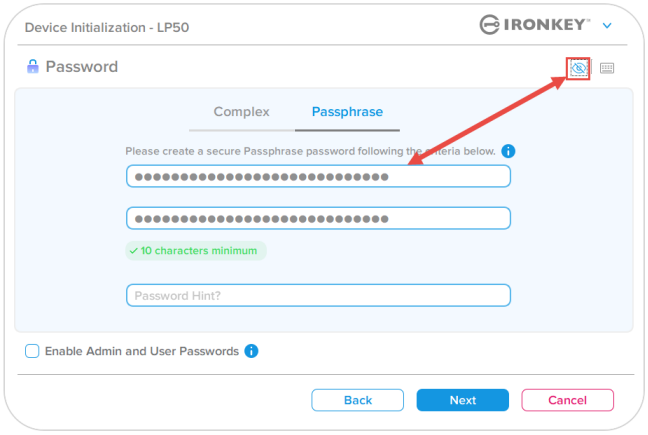
Ilustracja 4.9 – Ochrona przed screenloggerami/randomizacja

Inicjowanie urządzenia

Przełącznik widoczności hasła

Domyślnie podczas tworzenia hasła (jego wpisywania) ciąg znaków hasła jest wyświetlany w polu hasła. Aby ukryć ciąg znaków hasła 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**

Inicjowanie urządzenia

Hasła administratora i użytkownika

Włączenie haseł administratora i użytkownika umożliwia korzystanie z funkcji wielu haseł i zarządzanie obydwoma kontami w roli 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.

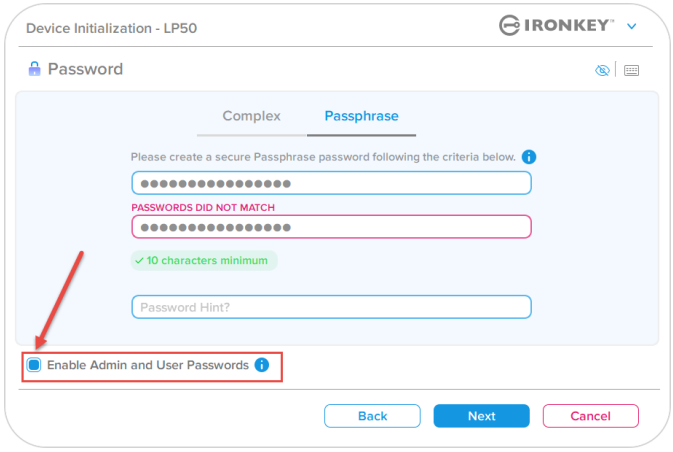
Gdy włączone są **hasła administratora i użytkownika**, można również uzyskać dostęp do następujących funkcji:

- Resetowanie hasła użytkownika

Aby dowiedzieć się więcej o funkcji resetowania hasła użytkownika, przejdź na str. 28 niniejszej instrukcji.

- Aby włączyć **hasła administratora i użytkownika**, kliknij pole obok opcji „**Enable Admin and User Passwords**” (Włącz hasła administratora i użytkownika) i kliknij przycisk **Next** (Dalej) po wybraniu prawidłowego hasła (*ilustracja 4.12*).

- Jeśli 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.

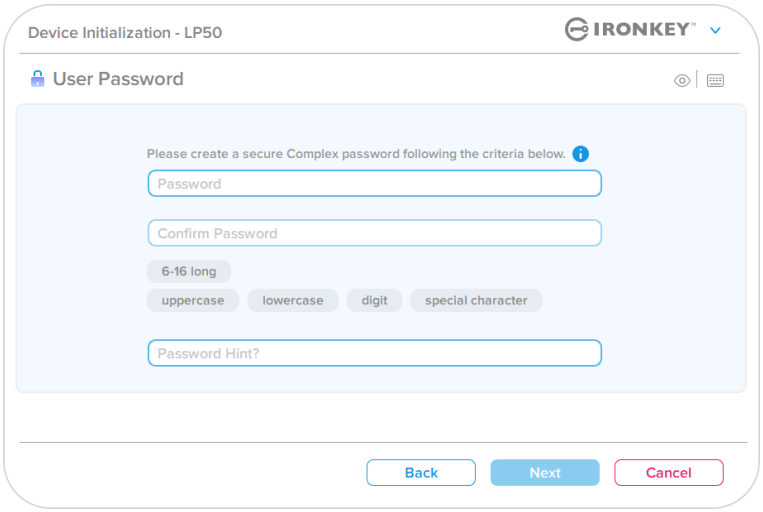
Jeśli w konfiguracji pamięci ta funkcja NIE jest włączona (pole niezaznaczone), pamięć zostanie skonfigurowana z jednym **hasłem dla pojedynczego użytkownika – bez żadnych funkcji administracyjnych**. W niniejszej instrukcji taka konfiguracja będzie określana jako **tryb Tylko użytkownik.**

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).

Inicjowanie urządzenia

Hasła administratora i użytkownika

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



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

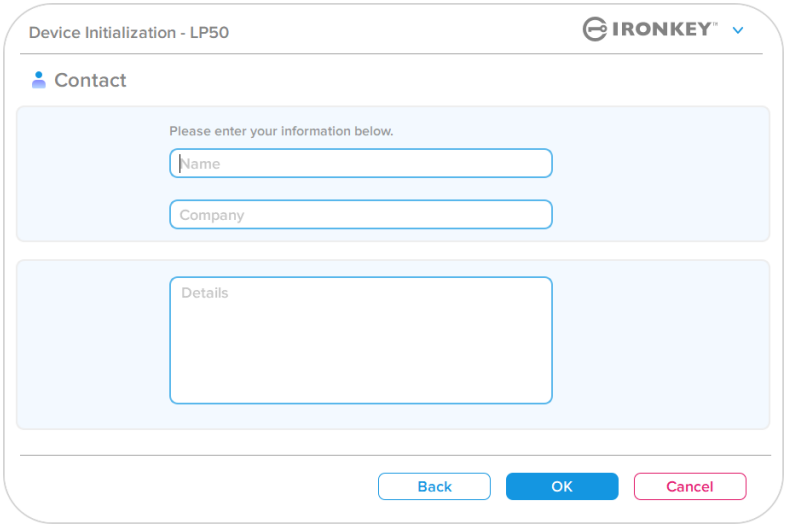
Uwaga: Wybrane kryteria opcji hasła (złożonego lub wyrażenia hasłowego) zostaną przeniesione na hasło użytkownika, niezbędne po skonfigurowaniu pamięci. Wybraną opcję hasła można zmienić dopiero po całkowitym zresetowaniu urządzenia.

Inicjowanie 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).

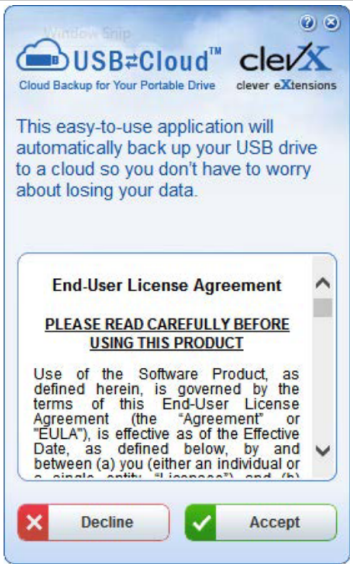
Pole „**Name**” (Nazwa) może zawierać do 32 znaków, ale nie może zawierać samego hasła. Pole „**Company**” (Firma) może zawierać do 32 znaków, ale nie może zawierać samego hasła. Pole „**Details**” (Szczegóły) może zawierać do 156 znaków, ale nie może zawierać samego hasła.	 **Ilustracja 4.14 – Informacje kontaktowe**

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

Inicjowanie funkcji USBtoCloud (środowisko Windows)

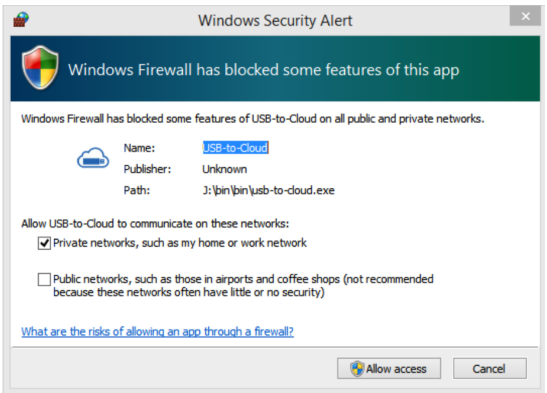
Po zainicjowaniu urządzenia w systemie Windows na ekranie pojawi się aplikacja USBtoCloud, jak pokazano na *ilustracji 5.1* po prawej stronie. Przed wykonaniem dalszych czynności należy upewnić się, że dostępne jest połączenie z Internetem.

- Aby kontynuować instalację, kliknij zielony przycisk „Accept” (Zaakceptuj) w prawym dolnym rogu okna aplikacji firmy clevX.
- Aby zrezygnować z instalacji, kliknij czerwony przycisk „Decline” (Odrzuć) w lewym dolnym rogu okna aplikacji firmy clevX.
- (Uwaga: Kliknięcie czerwonego przycisku „Decline” (Odrzuć) spowoduje anulowanie instalacji aplikacji USBtoCloud. W efekcie na partycji danych zostanie utworzony specjalny plik tekstowy o nazwie „USBtoCloudInstallDeclined.txt”. Zadaniem tego pliku jest zapobieganie wyświetlaniu zapytania o instalację aplikacji.)



Ilustracja 5.1 – Umowa licencyjna użytkownika końcowego aplikacji USBtoCloud w systemie Windows

- Jeśli podczas procesu inicjowania system Windows wyświetli okno alertu zabezpieczeń, kliknij przycisk „Allow access” (Zezwalaj na dostęp), aby kontynuować (lub utworzyć wyjątek zapory systemu Windows) w celu umożliwienia działania aplikacji USBtoCloud.



Ilustracja 5.2 – Okno alertu zabezpieczeń systemu Windows

Inicjowanie funkcji USBtoCloud (środowisko Windows)

- Po zakończeniu instalacji wyświetlone zostaje okno aplikacji z listą opcji do wyboru (umożliwiających synchronizowanie danych w pamięci LP50).
- Wybierz opcję obsługi chmury, w której ma być zapisywana kopia zapasowa i podaj niezbędne dane użytkownika wymagane do uwierzytelnienia.
- (Uwaga: Użytkownik nieposiadający jeszcze konta w żadnej z podanych usług chmury może je w tej chwili utworzyć w preferowanej przeglądarce internetowej, a następnie powrócić do listy opcji w aplikacji.)
- Po wybraniu opcji usługi chmury i uwierzytelnieniu jej użytkownika aplikacja USBtoCloud wykona procedurę wstępnego porównania zawartości partycji danych z danymi w chmurze. Jeśli tylko usługa USBtoCloud jest uruchomiona w Menedżerze zadań, dane dodawane do partycji danych będą automatycznie kopiowane do chmury (synchronizowana z chmurą).

Ilustracja 5.3 – Wybór języka

Inicjowanie funkcji USBtoCloud (środowisko Windows)

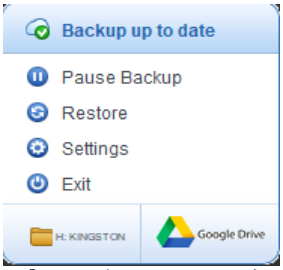
Aplikacja USBtoCloud oferuje następujące dodatkowe opcje:

- Pause Backup (Wstrzymaj tworzenie kopii zapasowej) – wstrzymuje tworzenie kopii zapasowej danych.
- Restore (Przywróć) – przywraca dane z chmury na urządzenie.
- Settings (Ustawienia) – dodatkowe opcje kopii zapasowej.
- Exit (Wyjście) – wyjście z usługi USBtoCloud

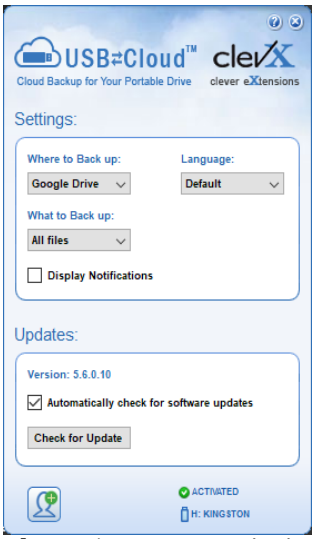
W menu „Settings" (Ustawienia) można:

- Zmienić usługę chmury wykorzystywaną aktualnie do tworzenia kopii zapasowej.
- Zmienić aktualnie używany język aplikacji.
- Wybrać pliki lub foldery uwzględniane w tworzonej w chmurze kopii zapasowej.
- Sprawdzić dostępność aktualizacji oprogramowania

(**Uwaga**: Przywrócenie domyślnych ustawień pamięci LP50 (lub jej sformatowanie) spowoduje utratę wszystkich zapisanych danych. Nie dotyczy to jednak danych przechowywanych w chmurze, które są bezpieczne i nie są w żaden sposób modyfikowane.)



Ilustracja 5.4 – Usługi



Ilustracja 5.5 – Ustawienia

Inicjowanie funkcji USBtoCloud (środowisko macOS)

- Po zainicjowaniu urządzenia wyświetli się aplikacja USBtoCloud, jak pokazano na *ilustracji 5.6* po prawej stronie. Przed wykonaniem dalszych czynności należy upewnić się, że dostępne jest połączenie z Internetem.

- Aby kontynuować instalację, kliknij przycisk „Accept” (Zaakceptuj) w prawym dolnym rogu okna aplikacji firmy clevX.
  (Uwaga: W systemie macOS 12.x i nowszych zostanie wyświetlony monit o zezwolenie na dostęp do plików w woluminie wymiennym. Wybierz opcję OK.) (*patrz ilustracja 5.7*).

- Aby zrezygnować z instalacji, kliknij przycisk „Decline” (Odrzuć) w lewym dolnym rogu okna aplikacji firmy clevX.

Ilustracja 5.6 – Umowa licencyjna użytkownika końcowego aplikacji USBtoCloud w systemie macOS

(Uwaga: Kliknięcie przycisku „Decline” (Odrzuć) spowoduje anulowanie instalacji aplikacji USBtoCloud. W efekcie na partycji danych zostanie utworzony specjalny plik o nazwie „DontInstallUSBtoCloud”. Zadaniem tego pliku jest zapobieganie wyświetlaniu zapytania o instalację aplikacji.)

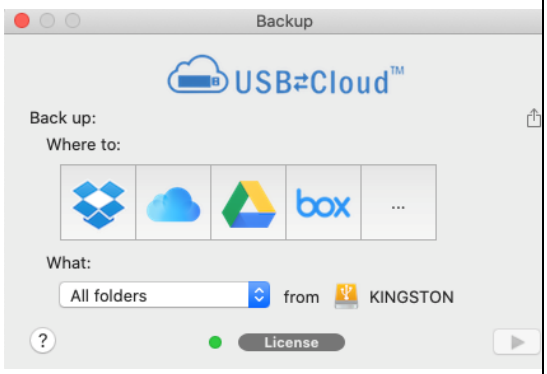
- Po zakończeniu instalacji wyświetlone zostaje okno aplikacji z listą opcji do wyboru (umożliwiających synchronizowanie danych w pamięci LP50). (*ilustracja 5.8*)

Ilustracja 5.7 – Dostęp w systemie macOS

- Wybierz opcję obsługi chmury, w której ma być zapisywana kopia zapasowa i podaj niezbędne dane użytkownika wymagane do uwierzytelnienia.

  (Uwaga: Użytkownik nieposiadający jeszcze konta w żadnej z podanych usług chmury może je w tej chwili utworzyć w preferowanej przeglądarce internetowej, a następnie powrócić do listy opcji w aplikacji.)

- Po wybraniu opcji usługi chmury i uwierzytelnieniu jej użytkownika aplikacja USBtoCloud wykona procedurę wstępnego porównania zawartości partycji danych z danymi w chmurze. Jeśli tylko usługa USBtoCloud jest uruchomiona w Menedżerze zadań, dane dodawane do partycji danych będą automatycznie kopiowane do chmury (synchronizowana z chmurą).

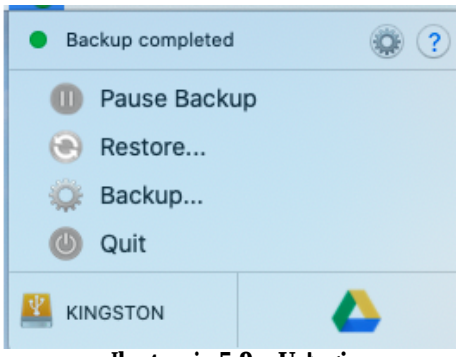


Ilustracja 5.8 – Wybór usługi w chmurze

Korzystanie z funkcji USBtoCloud (środowisko macOS)

Aplikacja USBtoCloud oferuje następujące dodatkowe opcje (*ilustracja 5.9*):

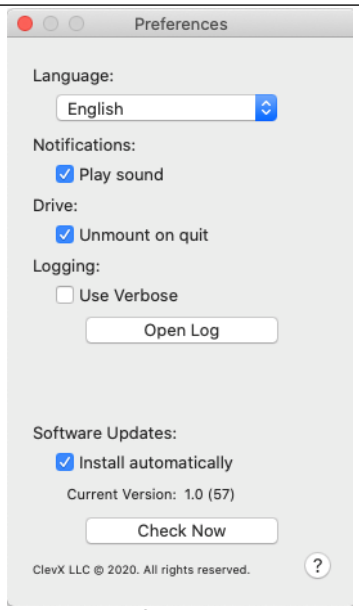
- **Pause Backup (Wstrzymaj tworzenie kopii zapasowej) –** wstrzymuje tworzenie kopii zapasowej danych
- **Restore (Przywróć)** (przywraca dane z chmury na urządzenie)
- **Backup (Kopia zapasowa)** (otwiera opcje chmury) – *patrz ilustracja 5.9*
- **Exit (Wyjście)** (zamyka usługę USBtoCloud)



Ilustracja 5.9 – Usługi

W menu „Preferences” (Preferencje) można:

- Zmienić aktualnie używany język aplikacji
- Włączyć/wyłączyć powiadomienia dźwiękowe
- Włączyć/wyłączyć wysuwanie nośnika, jeśli aplikacja jest zamknięta
- Włączy/wyłączyć rejestrowanie w celu rozwiązywania problemów
- Włączyć/wyłączyć automatyczne aktualizacje oprogramowania i sprawdzić dostępność aktualizacji

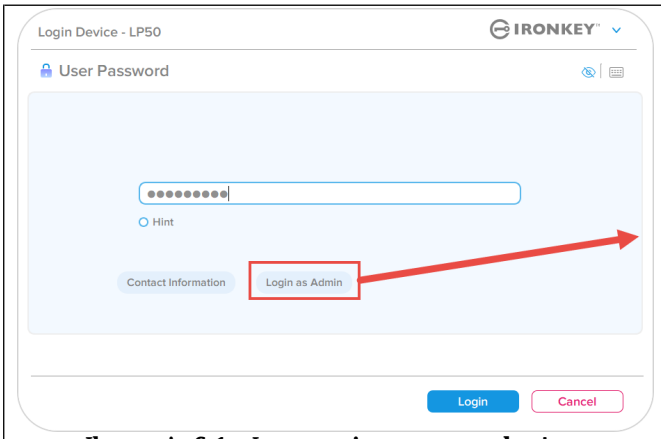


Ilustracja 5.10 – Preferencje usługi USBtoCloud

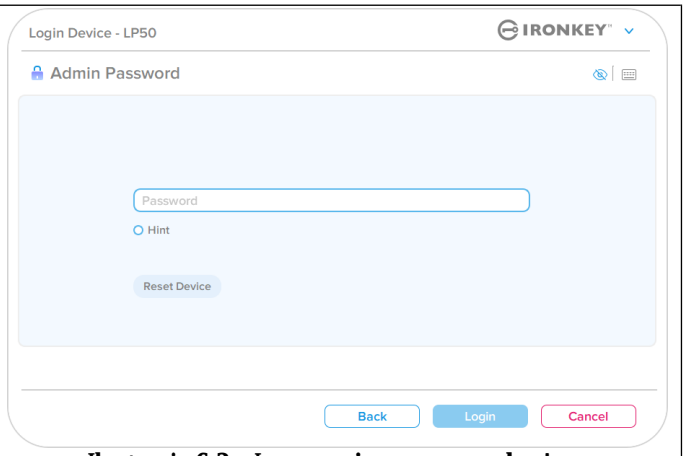
Korzystanie z urządzenia (środowisko Windows i macOS)

Logowanie administratora i użytkownika (włączony tryb administratora)

Jeśli urządzenie zostało zainicjowane z włączonymi hasłami administratora i użytkownika (rola administratora), nastąpi uruchomienie aplikacji IronKey LP50 i wyświetlenie w pierwszej kolejności ekranu z monitem o podanie hasła użytkownika. Z tego miejsca można zalogować się za pomocą 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)

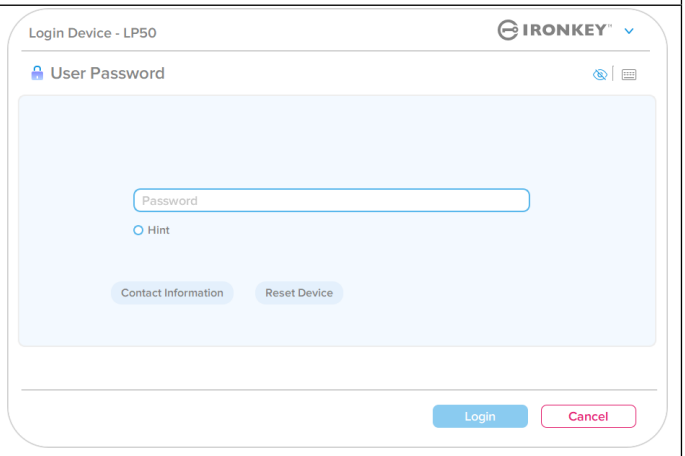


Ilustracja 6.2 – Logowanie za pomocą hasła administratora

Logowanie w trybie Tylko użytkownik (wyłączony tryb administratora)

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

Uwaga: Aby aktywować hasła 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 bezpowrotna utratę.**



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

Korzystanie z urządzenia

Ochrona hasła przed atakami metodą 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 metodą 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	**Ochrona przed atakami metodą Brute Force Zachowanie urządzenia (10 nieudanych prób wprowadzenia hasła)**	**Wymazanie 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 (WYŁĄCZONY tryb administratora/użytkownika)	**Ochrona przed atakami metodą Brute Force Zachowanie urządzenia (10 nieudanych prób wprowadzenia hasła)**	**Wymazanie danych i zresetowanie urządzenia?**
Hasło użytkownika	Bezpowrotne wymazanie metodą kryptograficzną pamięci, haseł, ustawień i danych	**TAK**

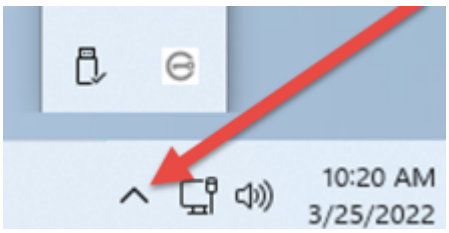
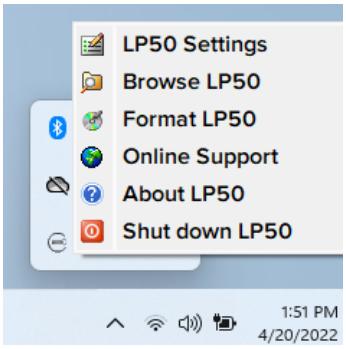
* Po pomyślnym uwierzytelnieniu użytkownika licznik nieudanych logowań jest resetowany odpowiednio dla użytej metody logowania. Funkcja Crypto-Erase usunie wszystkie hasła, klucze szyfrowania i dane – **zostaną one bezpowrotnie utracone.**

Uzyskiwanie dostępu do bezpiecznych plików

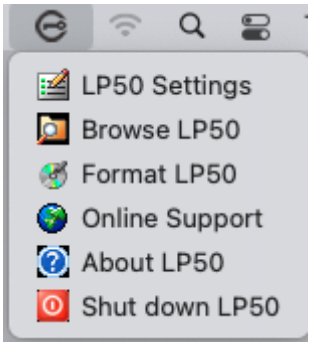
Po odblokowaniu urządzenia uzyskasz dostęp do zabezpieczonych plików. Pliki są automatycznie szyfrowane i odszyfrowywane, gdy zapisujesz lub otwierasz je w pamięci. Technologia ta pozwala na wygodną pracę, tak jak w przypadku zwykłej pamięci, zapewniając jednocześnie silne, „zawsze włączone” zabezpieczenia.
Wskazówka: Możesz również uzyskać dostęp do plików, klikając prawym przyciskiem myszy **ikonę IronKey** na pasku zadań systemu Windows, a następnie klikając opcję **Browse LP50** (Przeglądanie zawartości pamięci LP50) (*ilustracja 7.2*).

Opcje urządzenia – środowisko Windows

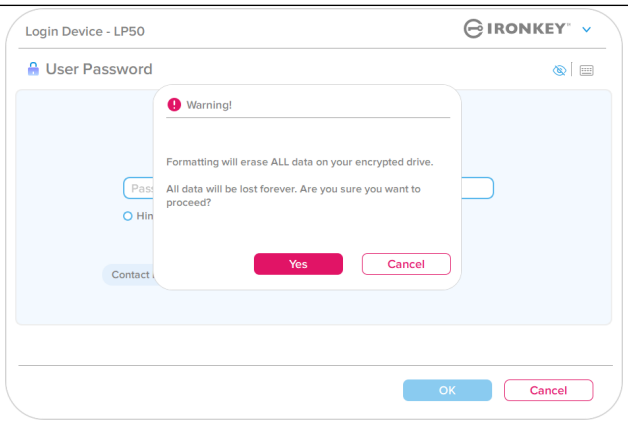
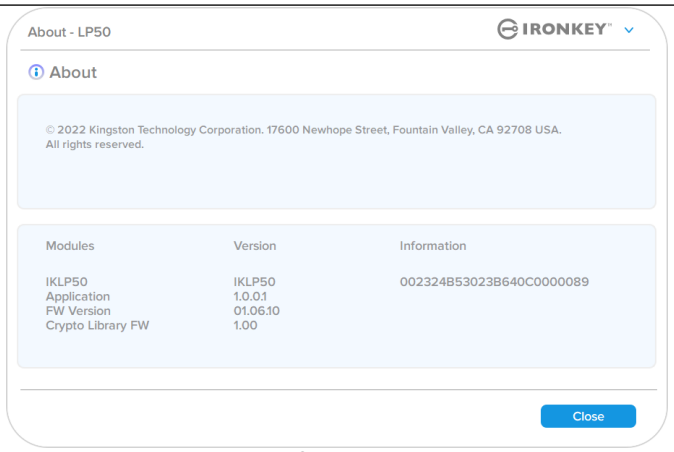
Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey. Kliknięcie prawym przyciskiem myszy ikony IronKey spowoduje otwarcie menu wyboru dostępnych opcji pamięci (*ilustracja 6.2*). Szczegółowe informacje na temat tych opcji urządzenia można znaleźć na str. 19-23 niniejszej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

• Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey (*ilustracja 7.1*).	 **Ilustracja 7.1 – Ikona IronKey na pasku zadań**
• Kliknięcie prawym przyciskiem myszy ikony IronKey spowoduje otwarcie menu wyboru dostępnych opcji pamięci (*ilustracja 7.2*). Szczegółowe informacje na temat tych opcji urządzenia można znaleźć 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 IronKey LP50 (*patrz ilustracja 7.3*), której kliknięcie powoduje wyświetlenie dostępnych opcji urządzenia. Szczegółowe informacje na temat tych opcji urządzenia można znaleźć na str. 19-23 niniejszej instrukcji.	 **Ilustracja 7.3 – Ikona na pasku menu systemu macOS / menu opcji urządzenia**

Opcje urządzenia

Ustawienia pamięci LP50:	• Zmiana hasła logowania, informacji kontaktowych i innych ustawień. (Więcej informacji na temat ustawień urządzenia można znaleźć w części „Ustawienia pamięci LP50” niniejszej instrukcji).
Browse LP50 (Przeglądanie zawartości pamięci LP50:	• Umożliwia przeglądanie bezpiecznych plików.
Format LP50 (Formatowanie pamięci LP50): Umożliwia sformatowanie zabezpieczonej partycji danych. (Ostrzeżenie: Wszystkie dane zostaną wymazane) (*ilustracja 6.1*) **Uwaga:** Do formatowania wymagane jest uwierzytelnienie hasłem.	 **Ilustracja 7.4 – Formatowanie pamięci LP50**
Online Support (Pomoc techniczna online):	• Umożliwia otwarcie przeglądarki internetowej i przejście na stronę http://www.kingston.com/support, gdzie dostępne są dodatkowe informacje.
About LP50 (Informacje o pamięci LP50): Dostęp do szczegółowych informacji na temat pamięci LP50, w tym informacji o aplikacji, oprogramowaniu sprzętowym i numerze seryjnym (*ilustracja 6.2*) **Uwaga:** Unikalny numer seryjny znajduje się w kolumnie „Information” (Informacje).	 **Ilustracja 7.5 – Informacje o pamięci LP50**
Shut down LP50 (Wyłączenie pamięci LP50):	• Umożliwia prawidłowe wyłączenie pamięci LP50, co pozwala na jej bezpieczne odłączenie od komputera.

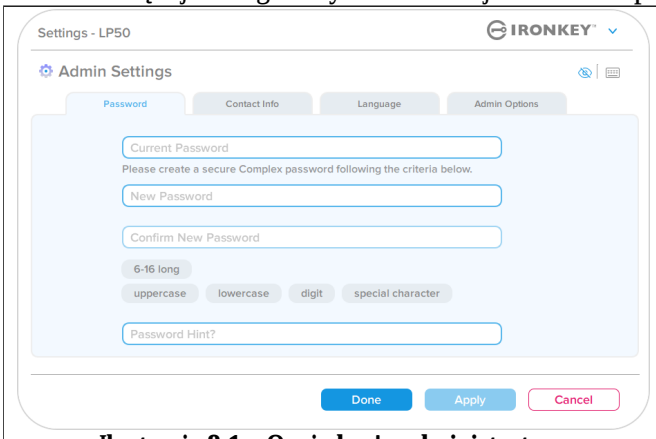
Ustawienia pamięci LP50

Ustawienia administratora

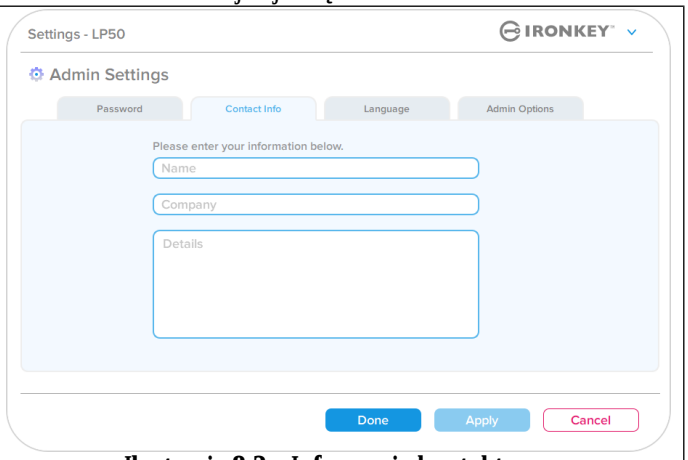
Zalogowanie się jako administrator umożliwia dostęp do następujących ustawień urządzenia:

- **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*)

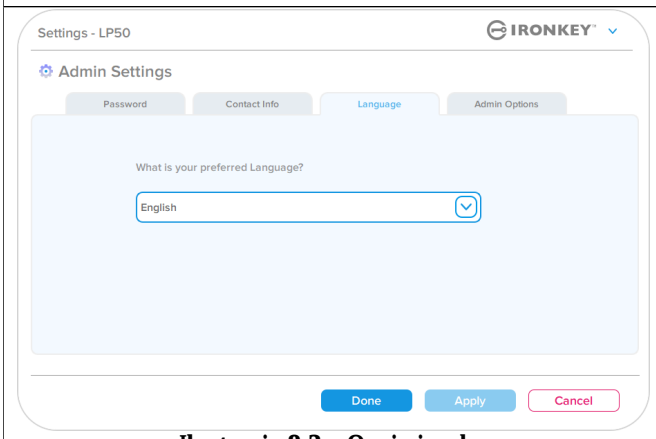
UWAGA: Więcej szczegółowych informacji na temat opcji administratora znajduje się na stronie 25



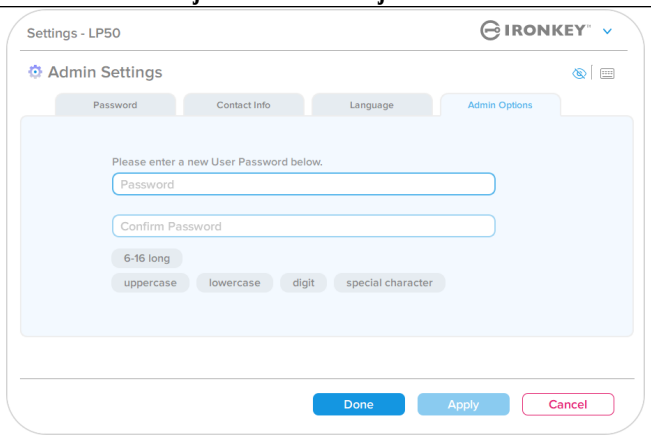
Ilustracja 8.1 – Opcje hasła administratora



Ilustracja 8.2 – Informacje kontaktowe



Ilustracja 8.3 – Opcje języka

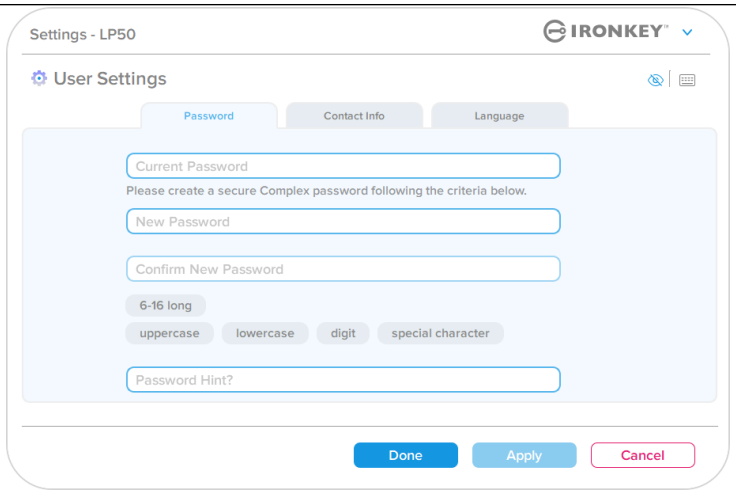
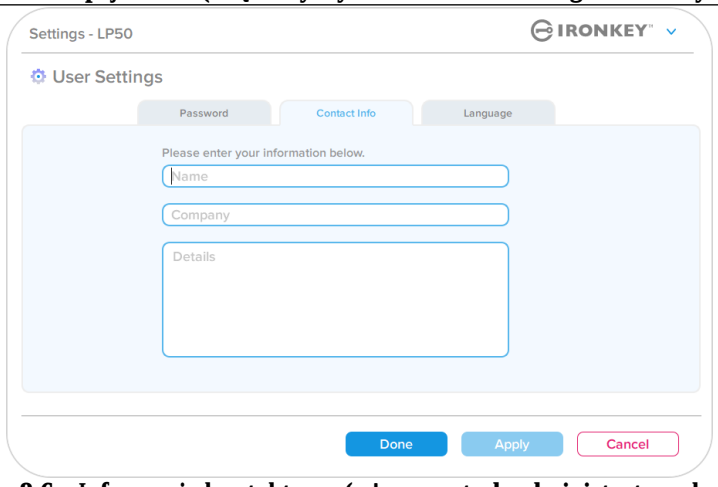
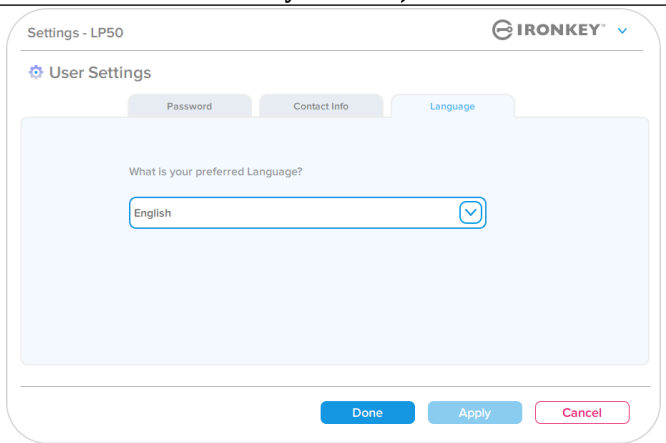


Ilustracja 8.4 – Opcje administratora

Ustawienia pamięci LP50

Ustawienia użytkownika: włączony tryb administratora

Zalogowanie się jako użytkownik powoduje ograniczenie dostępu do następujących ustawień:

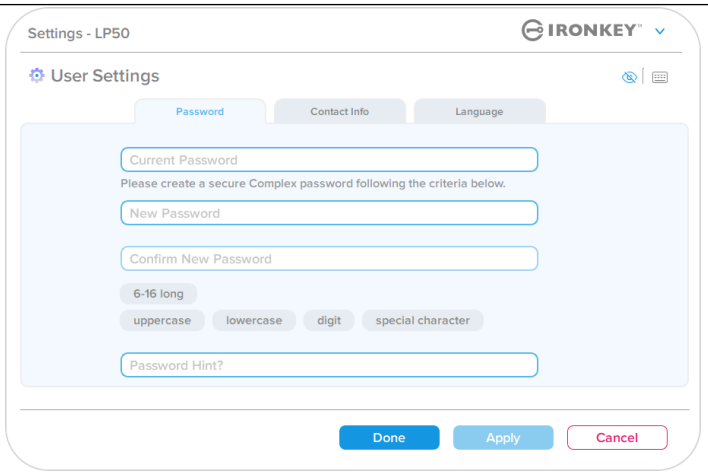
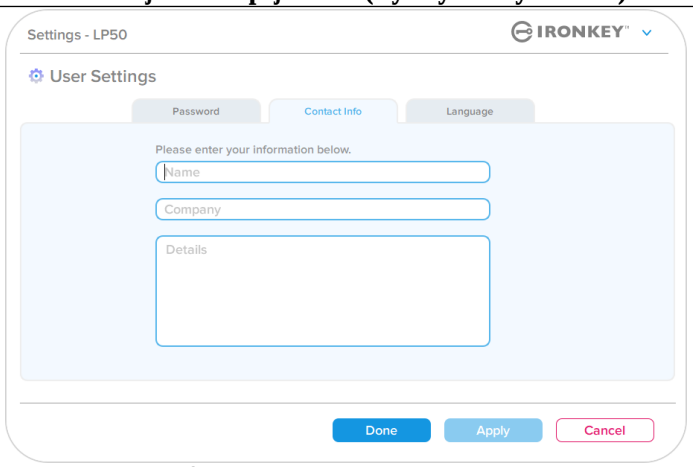
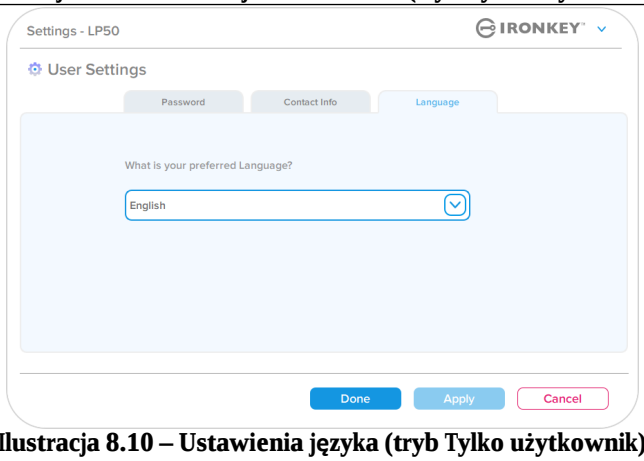
Password (Hasło): Umożliwia zmianę hasła i/lub podpowiedzi do hasła użytkownika (*ilustracja 8.5*).	 **Ilustracja 8.5 – Opcje hasła (włączony tryb administratora: logowanie użytkownika)**
Contact Info (Informacje kontaktowe): Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 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 przy użyciu hasła użytkownika.

Ustawienia pamięci LP50

Ustawienia użytkownika: wyłączony tryb administratora

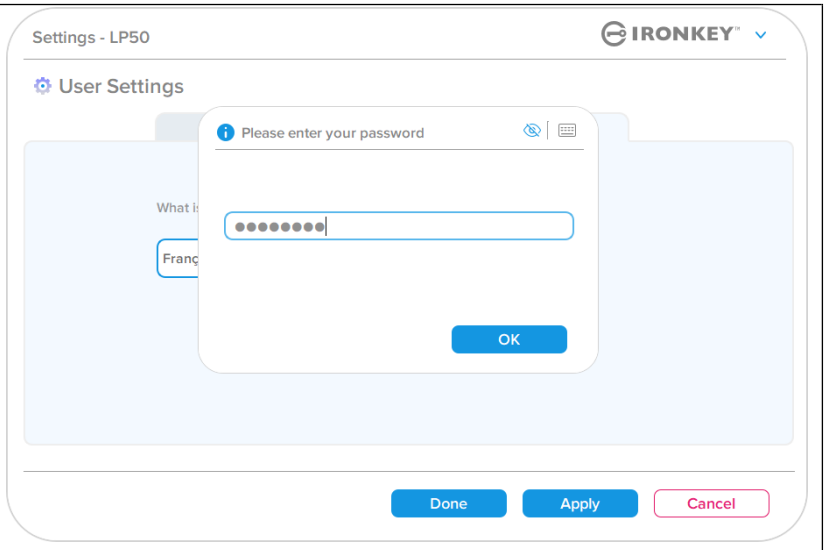
Jak wspomniano wcześniej na stronie 12, zainicjowanie pamięci LP50 bez włączania haseł administratora i użytkownika spowoduje skonfigurowanie pamięci z **jednym hasłem dla pojedynczego użytkownika**. Konfiguracja ta nie zapewnia dostępu do żadnych opcji ani funkcji administracyjnych. Konfiguracja ta umożliwia dostęp do następujących ustawień pamięci LP50:

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 pamięci LP50

Zmiana i zapisywanie ustawień

- Po każdej zmianie ustawień pamięci LP50 (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 podanie hasła w celu zapisania zmiany ustawień pamięci LP50

Uwaga: Jeśli znajdujesz się na ekranie z monitem o hasło powyżej i chcesz anulować lub zmodyfikować swoje zmiany, możesz to zrobić, upewniając się, że pole hasła jest puste i klikając przycisk „OK”. Spowoduje to zamknięcie okna „Please enter your password” (Wprowadź hasło) i powrót do menu ustawień pamięci LP50.

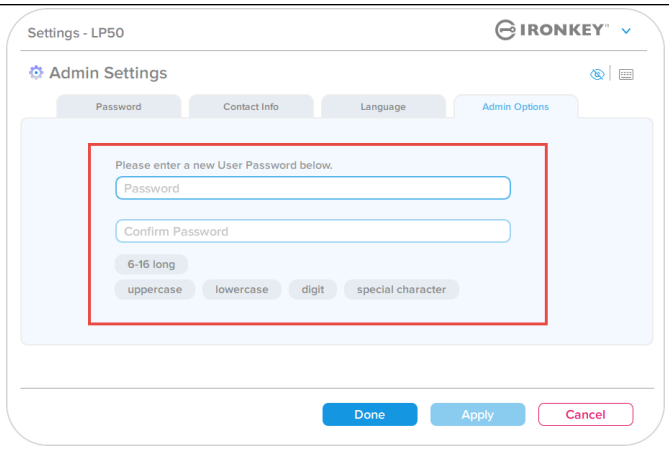
Funkcje administracyjne

Dostępne opcje resetowania hasła użytkownika

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

Resetowanie hasła użytkownika:
Ręcznie zmień 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

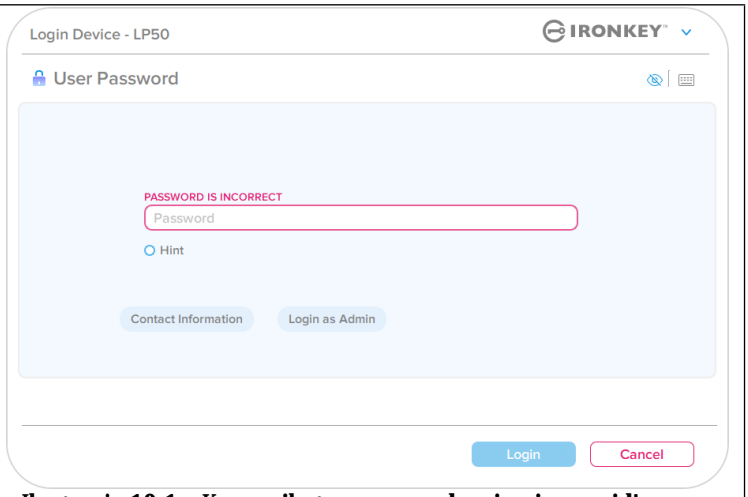
Pamięć LP50 jest wyposażona w funkcję bezpieczeństwa, która uniemożliwia nieuprawniony dostęp do partycji danych w przypadku osiągnięcia maksymalnej liczby kolejnych nieudanych prób zalogowania (w skrócie MaxNoA). W domyślnej fabrycznej konfiguracji ustawiona jest wartość 10 (liczba prób) dla każdej 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

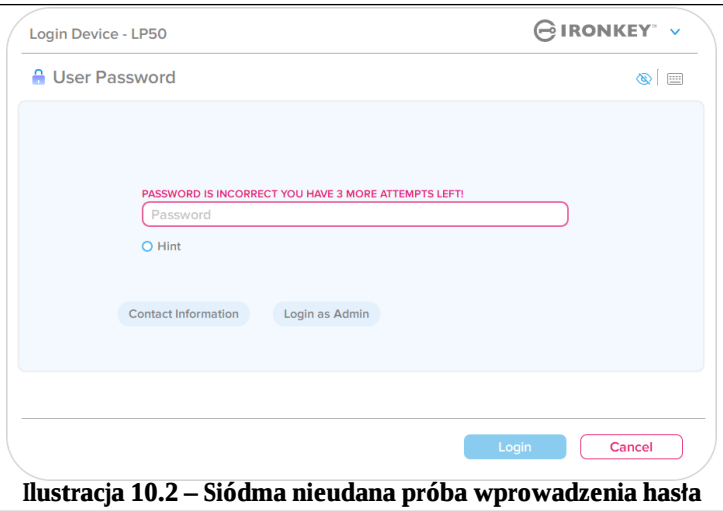
2. Osiągnięcie limitu MaxNoA i zablokowanie lub sformatowanie urządzenia, zależnie od konfiguracji pamięci.

- 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

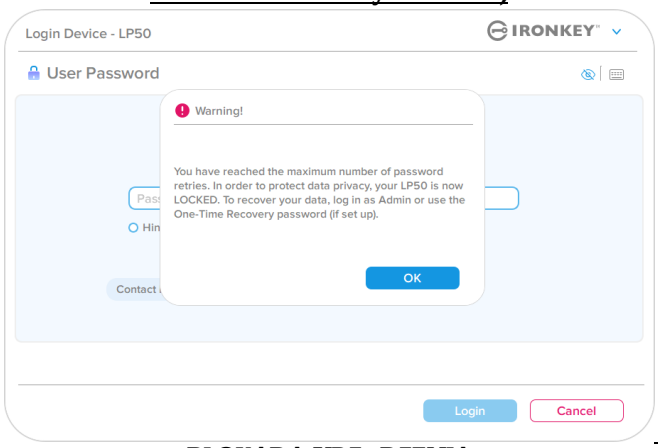
Pomoc i rozwiązywanie problemów

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 pamięci i bezpowrotną utratę danych**. O takim zachowaniu działania urządzenia wspomniano również na str. 18 niniejszej instrukcji.

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

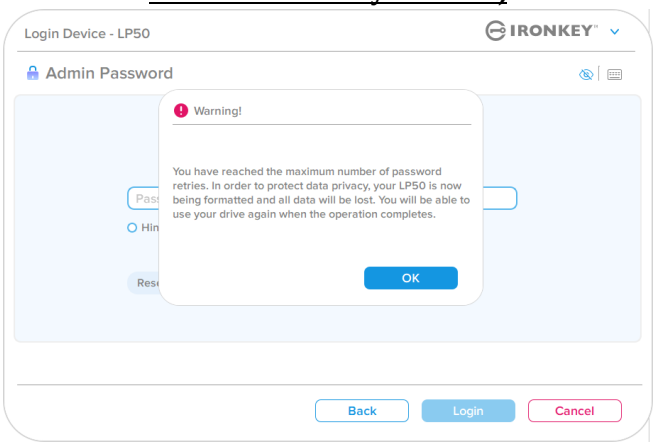
Hasło użytkownika: (włączony tryb administratora/użytkownika)



BLOKADA URZĄDZENIA

ilustracja 10.3

Hasło administratora (włączony tryb administratora/użytkownika)

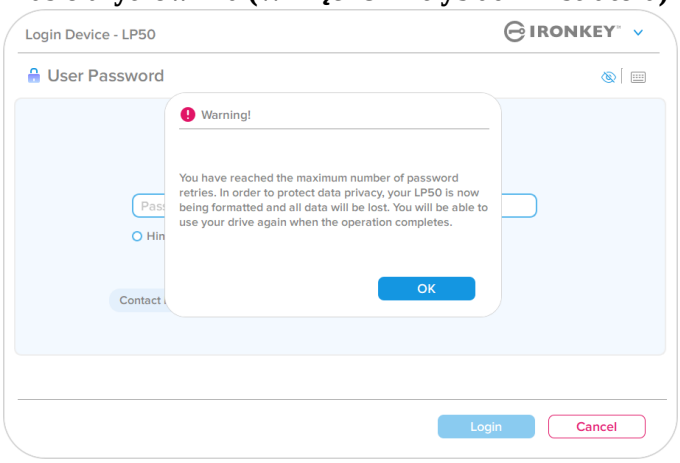


FORMATOWANIE URZĄDZENIA*

ilustracja 10.4

- Te zabezpieczenia mają na celu ograniczenie możliwości podjęcia nieograniczonej liczby prób zalogowania i uzyskania dostępu do poufnych danych (tzw. atak metodą Brute Force) osobom, które nie znają hasła, . Jeżeli właściciel pamięci LP50 zapomni hasło, zostaną zastosowane takie same środki bezpieczeństwa, w tym również formatowanie urządzenia. * Aby uzyskać więcej informacji dotyczących tej funkcji, zapoznaj się z rozdziałem „*Resetowanie urządzenia*” na str. 25.

Hasło użytkownika (WYŁĄCZONY tryb administratora)



FORMATOWANIE URZĄDZENIA*

ilustracja 10.5

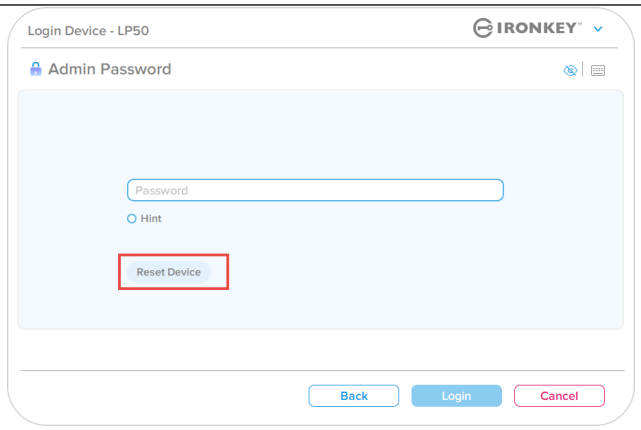
** Uwaga: Sformatowanie urządzenia spowoduje wymazanie WSZYSTKICH informacji przechowywanych na bezpiecznej partycji danych pamięci LP50.*

cPomoc i rozwiązywanie problemów

Resetowanie urządzenia

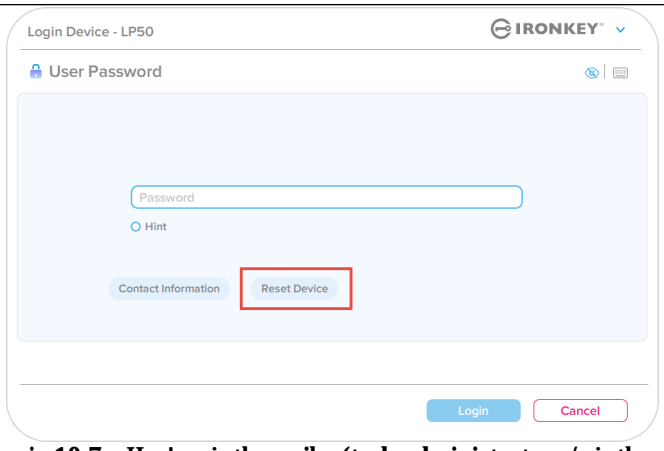
Jeśli zapomnisz hasło lub zechcesz zresetować urządzenie, możesz kliknąć przycisk „*Reset Device*” (Resetuj urządzenie), który pojawia się w jednym z dwóch miejsc, zależnie od konfiguracji urządzenia (w menu hasła logowania administratora, jeśli włączony jest tryb administratora/użytkownika, lub w menu hasła logowania użytkownika, jeśli tryb administratora/użytkownika jest wyłączony), podczas uruchamiania oprogramowania pamięci LP50 (*patrz ilustracje 10.7 i 10.8*).

- Ta opcja umożliwia utworzenie nowego hasła, jednak w celu ochrony poufności danych pamięć LP50 zostanie sformatowana. Oznacza to, że wszystkie dane zostaną usunięte.*



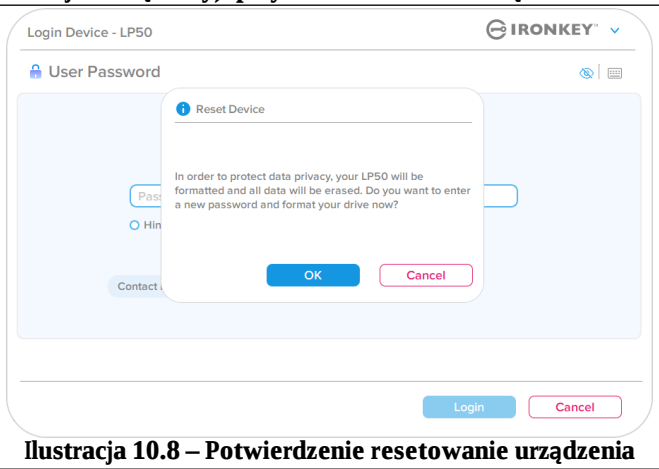
Ilustracja 10.6 – Hasło administratora: przycisk resetowania urządzenia

- **Uwaga:** Po kliknięciu przycisku „*Reset Device*” (Resetuj urządzenie) zostanie wyświetlony komunikat z pytaniem, czy chcesz 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 jest włączony): przycisk resetowania urządzenia

- Jeśli zdecydujesz się kontynuować, wyświetli się ekran inicjalizacji, gdzie można włączyć tryby administratora i użytkownika oraz wprowadzić nowe hasło zależnie od wybranej opcji (hasło złożone lub wyrażenie hasłowe). Nie musisz wypełniać pola podpowiedzi, może to jednak pomóc w przypomnieniu sobie zapomnianego hasła.



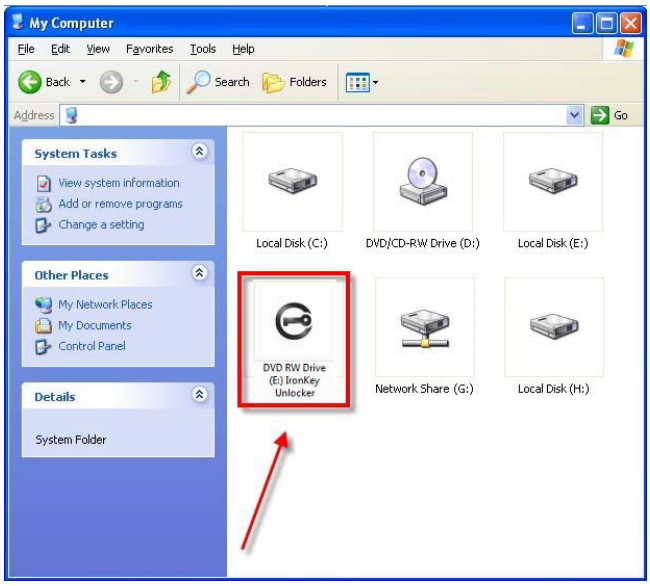
Ilustracja 10.8 – Potwierdzenie resetowanie urządzenia

Pomoc i rozwiązywanie problemów

Konflikt liter dysku: system operacyjny Windows

- Jak wspomniano w części „*Wymagania systemowe*” niniejszej instrukcji (na str. 3), pamięć LP50 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 LP50 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 LP50 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 LP50 może podjąć próbę użycia jej jako drugiej litery, co spowoduje konflikt.

Jeśli w systemie nie ma udziałów sieciowych, lecz urządzenia LP50 nadal nie można uruchomić, możliwe, że konflikt powoduje inne, wcześniej zainstalowane urządzenie, do którego przypisano literę dysku (np. czytnik kart lub dysk wymienny).

Funkcja zarządzania literami dysków została znacznie ulepszona w systemach Windows 8.1, 10 i 11, 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 dalszej pomocy.

IRONKEY™ Locker+ 50 (LP50)
高セキュリティの USB 3.2 Gen 1 フラッシュドライブ

ユーザーガイド

目次

図 1：IronKey LP50

はじめに

Kingston IronKey Locker+ 50 USB フラッシュドライブは、XTS モードでの AES ハードウェア暗号化による**コンシューマーグレードのセキュリティを提供します。デジタル署名されたファームウェアによる** BadUSB **や総当りパスワード攻撃に対して保護されます。また、**LP50 **は** TAA **に準拠しています。**

LP50 **は、複合/パスフレーズモードによるマルチパスワード（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りました。複合モードでは、**4 **種類の文字セットから** 3 **種類を使用して** 6～16 **文字のパスワードを設定できます。新しいパスフレーズモードでは、**10～64 **文字の範囲で、数字のパスワード、文章、単語の並び、さらには歌詞すら、使用できます。管理者はユーザーパスワードを有効にしたり、ユーザーパスワードをリセットしてデータアクセスを回復できます。パスワードを入力しやすくするために、「目」のマークを有効にして入力したパスワードを表示し、タイプミスでログインできない事態を減らすことができます。総当たり攻撃から保護するために、無効なパスワードが連続して** 10 **回入力された場合、ユーザーをロックアウトします。管理者パスワードが連続して** 10 **回間違って入力された場合、ドライブを暗号化消去します。さらに、組み込みの仮想キーボードにより、キーロガーまたはスクリーンロガーからパスワードが保護されます。**

Locker+ 50 **は、小型の金属製ケースにキーループが付いており、どこにでも便利にデータを持ち運べられるよう設計されています。また、**LP50 **はオプションで** USBtoCloud®（ClevX® **提供）バックアップも搭載しており、**GoogleDrive™、OneDrive（Microsoft®）、Amazon Cloud Drive、Dropbox™ **または** Box **を介してパーソナルクラウドストレージからドライブ上のデータにアクセスできます。**LP50 **は、アプリケーションのインストールは不要で、誰でも簡単にセットアップして使用できます。必要なソフトウェアやセキュリティはすべてドライブ上に組み込まれています。**Windows®、macOS ® **のどちらにも対応しており、ユーザーは複数のシステムからファイルにアクセスできます。**

LP50 **は、**5 **年限定保証と** Kingston **無料技術サポートが付属しています。**

IronKey Locker+ 50 の機能

- XTS-AES ハードウェア暗号化（暗号化をオフにできません）
- 総当たりおよび BadUSB 攻撃の防止
- マルチパスワードのオプション
- 複雑なパスワードまたはパスフレーズパスワードのモード
- 入力したパスワードを表示する目のボタンを通じて、ログインの失敗回数が減少
- キーロガーおよびスクリーンロガーから守る仮想キーボード
- Windows または macOS 互換 (詳細はデータシートを参照)

本書について (09242024)
このユーザーマニュアルは、IronKey Locker+ 50（LP50）**について説明しています。**

システム要件

PC プラットフォーム • Intel および AMD • 15MB のディスク空き容量 • USB 2.0 - 3.2 ポート搭載 • 最後の物理ドライブの後の、2 つの連続したドライブ文字 *注：「ドライブ文字の競合」(32 ページ) を参照してください。	**対応 PC オペレーティングシステム (OS)** • Windows 11 • Windows 10
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	**対応 Mac オペレーティングシステム (OS)** • macOS 12.x – 15.x

注：すべてのドライブには、アクティベーションから 5 年間の USB-to-Cloud の無料サブスクリプションが含まれています。無料期間終了後は、ClevX から継続アクティベーションのオプションを購入できます。

推奨事項

LP50 に十分な電力を供給するために、以下の*図 1.1* に示すように、ノートパソコンまたはデスクトップパソコン本体の USB ポートに直接、差し込んでください。*図 1.2* に示すようなキーボードや USB から給電するハブなどのように、USB ポートを持つ周辺機器には、LP50 を接続しないでください。

図 1.1 - 正しい使い方

図 1.2 - 間違った使い方

正しいファイルシステムの使用
IronKey LP50 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。ドライブを手作業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は消えます。

使用上の注意
データの安全性を保つため、Kingston では次のことを推奨します。

- ターゲットシステムで LP50 を設定し使用する前に、コンピュータ上でウイルスのスキャンを実行してください。。
- 使用しない時にはデバイスをロックしてください。
- ドライブを抜く前にイジェクトしてください。
- LED の点灯中にデバイスを抜かないでください。抜くと、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は誰にも教えないでください。

最新のアップデートと情報の入手

kingston.com/support にドライブに関する最新のアップデート、FAQ、資料、追加情報があります。

注：ドライブのアップデートを利用できる場合は、最新バージョンのみを使用してください。ドライブを旧バージョンのソフトウェアにダウングレードした場合、サポート対象外になり、保管中のデータの損失や、他のドライブ機能の不具合の原因となるおそれがあります。ご不明な点や問題がある場合は、Kingston 技術サポート宛に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

LP50 は強力なセキュリティ対策が搭載されています。これには、総当たり攻撃の防止が含まれ、各パスワードの試行回数を 10 回に制限し、攻撃者がパスワードを推測できないようにします。試行回数がドライブの制限に達した場合、LP50 は自動的に暗号化データを消去し、フォーマットして出荷時の状態に戻します。

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、LP50 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、LP50 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持つことができます。

LP50 では、管理者パスワード（Admin パスワードとも言います）とユーザーパスワードの２つのメイン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、ユーザーのオプションを設定できます。管理者はスーパーユーザーのようなものです。

ユーザーもドライブにアクセスできますが、管理者に比べて権限が制約されます。ふたつのパスワードのうちひとつを忘れた場合、他のパスワードでデータアクセスして取得できます。その後、ドライブをふたつのパスワードがある状態に戻せます。ユーザーパスワードを使用している間は、両方のパスワードを設定し、管理者パスワードを安全な場所に保管しておくことが重要です。。

すべてのパスワードを忘れたか紛失した場合、他にデータにアクセスする方法はありません。セキュリティ重視のため秘密のアクセス手段などは設けていませんので、Kingston がデータを取り出すことはできません。Kingston では、データを他のメディアにも保管しておくことをおすすめします。LP50 をリセットして再使用できますが、以前のデータは永久に消去されます。

パスワードモード

また LP50 では、2つの異なるパスワードモードをサポートします。

複雑なパスワード

複雑なパスワードは、次の文字のうち最低３種類を使用して、6～16 文字に収める必要があります。

- 英大文字
- 英小文字
- 数字
- 特殊文字

パスフレーズ

LP50 では、10～64 文字のパスフレーズをサポートしています。パスフレーズが従うべき他のルールはありませんが、適切に使用すれば、非常に高レベルのパスワード保護を提供できます。

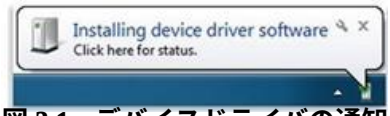
パスフレーズは基本的にどんな文字も組み合わせられ、他の言語の文字の使用も可能です。LP50 のように、パスワードの言語を、ドライブ用に選択した言語と一致させることができます。このため、複数の単語、フレーズ、歌詞、詩句などを選択できます。優れたパスフレーズは、攻撃者にとっては最も推測しにくいタイプのパスワードで、しかしユーザーにとっては覚えやすくなります。

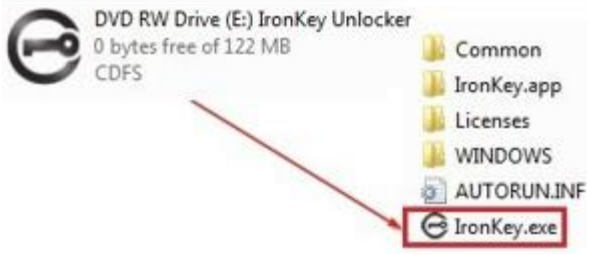
デバイスのセットアップ

IronKey 暗号化 USB ドライブに十分な電力を供給するために、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、差し込んでください。キーボードや USB から給電するハブなどの USB ポートを持つ周辺機器には接続しないでください。デバイス初期設定は、対応の Windows または macOS ベースのオペレーティングシステムで実行しなければなりません。

デバイスへのアクセス （Windows 環境）

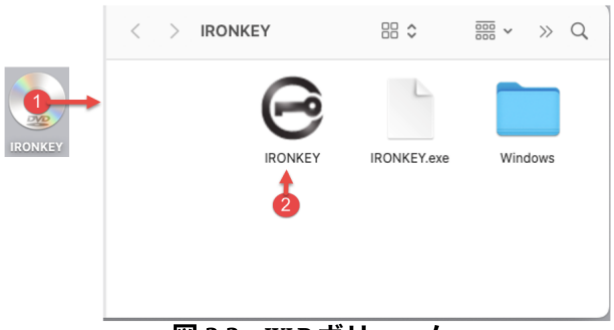
IronKey 暗号化 USB ドライブを、ノートパソコンまたはデスクトップパソコンの空いている USB ポートに差し込み、Windows がこのドライブを検出するまで待ちます。

• Windows 8.1/10/11 ユーザーは、デバイスドライバの通知を受け取ります。*(図 3.1)*	 図 3.1 – デバイスドライバの通知

• 新しいハードウェアの検出が完了したら、ファイルエクスプローラにある Unlocker パーティションの中のオプション IronKey.exe を選択してください。*(図 3.2)* • パーティションの文字は、空き状況に応じて自動的に選択されることに注意してください。ドライブ文字は、接続されているデバイスによって変化します。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）

LP50 をノートパソコンまたはデスクトップパソコンの空いている USB ポートに差し込み、Mac がこのドライブを検出するまで待ちます。検出したら、デスクトップに「IRONKEY」というボリュームが表示されます。*(図 3.3)*

• IronKey CD-ROM の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 – IKLP ボリューム

デバイスの初期化 (Windows および macOS 環境)

言語と EULA

- ドロップダウンメニューから使用したい言語を選択し、次へ (Next) をクリックします *(図 4.1 を参照してください)*。

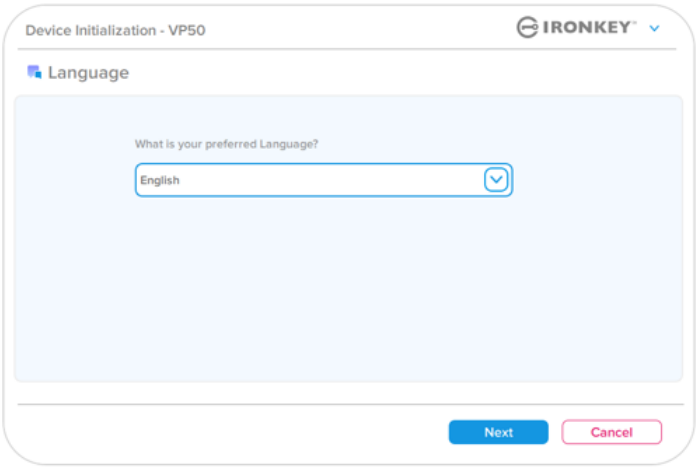


図 4.1 – 言語の選択

- 使用許諾契約をよく読んで、次へ (Next) をクリックします。

  注：次のステップに進む前に、使用許諾契約に同意する必要があります。同意しないと、「次へ」のボタンは有効になりません。*(図 4.2)*

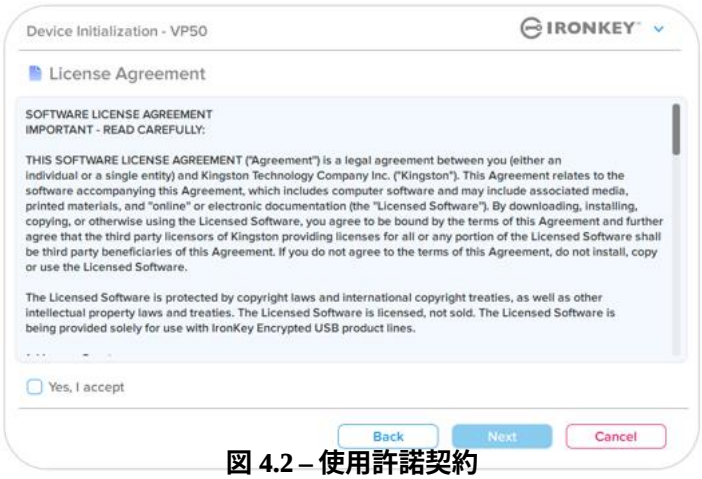


図 4.2 – 使用許諾契約

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、複雑なパスワードかパスフレーズのどちらかを使用して、LP50 のデータを保護するためのパスワードを作成できます（*図 4.3～4.4*）。さらに、この画面で管理者/ユーザーのマルチパスワードオプションを有効にできます。パスワードの選択に進む前に、下の Admin/ユーザーパスワードの有効化方法をよく読んで、これらの機能をよく理解してください。

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」フィールドに作成するパスワードを入力し、「パスワードの確認」フィールドに再入力します。作成するパスワードが以下の基準を満たしていない限り、初期化を継続することはできません。

~~複雑な (Complex) パスワード~~

- **6 文字以上の長さ (最大 16 文字) でなければなりません。**
- **以下の文字の種類のうち、3 つが含まれていなければなりません。**
  - **英大文字**
  - **英小文字**
  - **数字**
  - **特殊文字 (！、$、& など)**

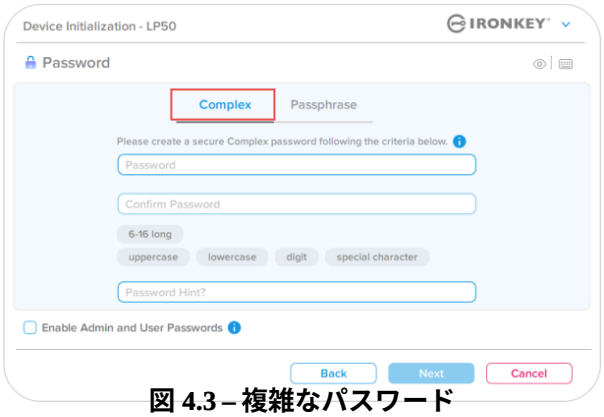


図 4.3 – 複雑なパスワード

~~パスフレーズ (Passphrase) パスワード~~

- **文字数の制限：**
  - **最短 10 文字**
  - **最長 64 文字**

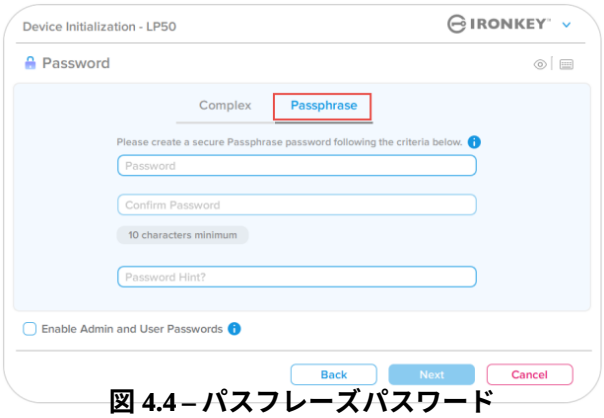


図 4.4 – パスフレーズパスワード

~~パスワードのヒント (Password Hint)~~（オプション）
パスワードのヒントは、パスワードを忘れた場合に、パスワードの手がかりを示してくれます。
注：パスワードと同じ文字列をヒントフィールドに入力することはできません。

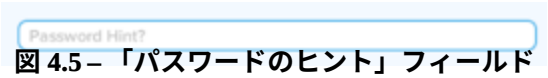


図 4.5 – 「パスワードのヒント」フィールド

デバイスの初期化

有効または無効なパスワード

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：最低３つのパスワード基準を満たすと、４つ目の基準ボックスがグレーになり、この基準の選択は任意であることを示します *（図 4.6b）*

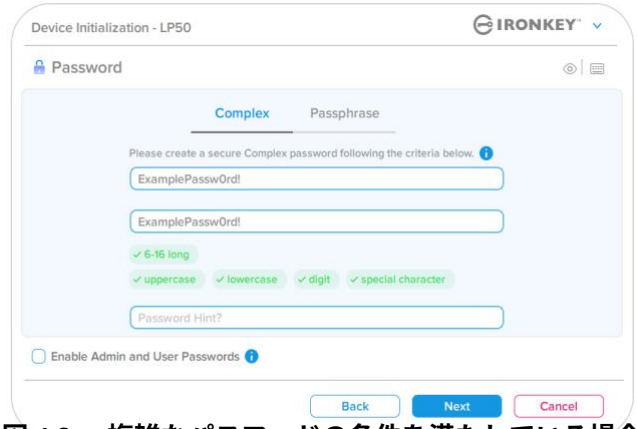


図 4.6a – 複雑なパスワードの条件を満たしている場合

図 4.6b – 任意の複雑なパスワードの条件

無効なパスワードの場合、パスワードの基準ボックスが赤で表示され、最低限の要件を満たすまで、「次へ」ボタンを使用できません。

これ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。

図 4.7 – パスワード条件を満たしていない場合

デバイスの初期化

仮想キーボード
LP50 は、キーロガーから守るために使用できる仮想キーボードが搭載されています。

- 仮想キーボードを使用するには、デバイス初期化 (デバイスの初期化) 画面の右上の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た後で、スクリーンロガー保護 (Screenlogger Protection) を有効にすることができます。この機能を使用するとき、すべてのキーが一時的にブランクになります。これは、スクリーンロガーがクリックした内容を取得することを防ぐための、想定内の動きです。
- 仮想キーボードの右下のランダム化を選択して、この機能をさらに堅牢にすることもできます。ランダム化すると、キー配列がランダムになります。

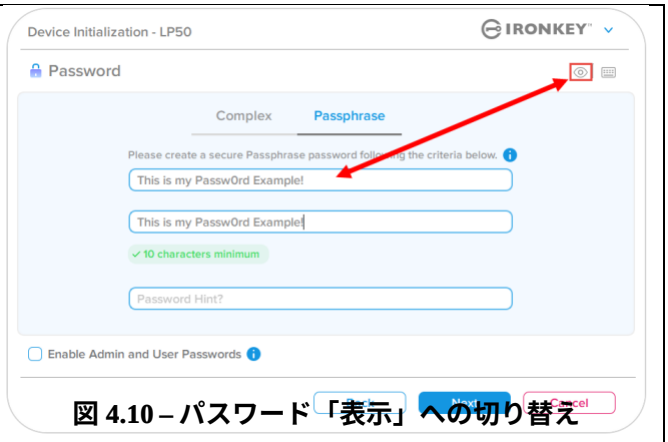
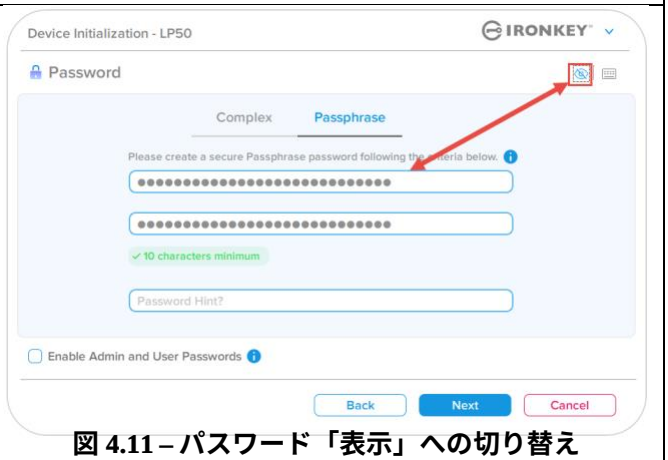
図 4.9 – スクリーンロガー保護/ランダム化

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、パスワードを作成する際に、入力したパスワードの文字列がフィールドに表示されます。入力時にパスワードの文字列を「非表示」にしたい場合は、デバイス初期化ウィンドウの右上にある「目」ボタンをクリックするたびに、表示と非表示が切り替わります。

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の「非表示」になります。

パスワードの文字列を非表示にしたい場合は、グレーのアイコンをクリックします。 	 図 4.10 – パスワード「表示」への切り替え
非表示のパスワードを表示するには、ブルーのアイコンをクリックします。 	 図 4.11 – パスワード「表示」への切り替え

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のパスワードを有効にするには、マルチパスワードの機能を利用できます。管理者ロールで両方のアカウントを管理できます。「管理者およびユーザーのパスワードを有効にする」を選択すると、パスワードを忘れた場合でも別の手段でドライブへアクセスできるようになります。

管理者およびユーザーのパスワードが有効になると、次の機能を利用できます。

- **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について詳しくは、このユーザーガイドの 28 ページをご覧ください。

- **管理者およびユーザーのパスワードを有効にするには、「管理者およびユーザーのパスワードを有効にする」(Enable Admin and User Passwords) の隣のボックスをクリックし、有効なパスワードを設定してから次へ (Next) を選択します。** *(図 4.12)*
- **この機能が有効な場合、この画面で選択されているパスワードは管理者パスワードになります。次 (Next) を選択し、ユーザーパスワード画面に進んで、ユーザー用のパスワードを選択します。**

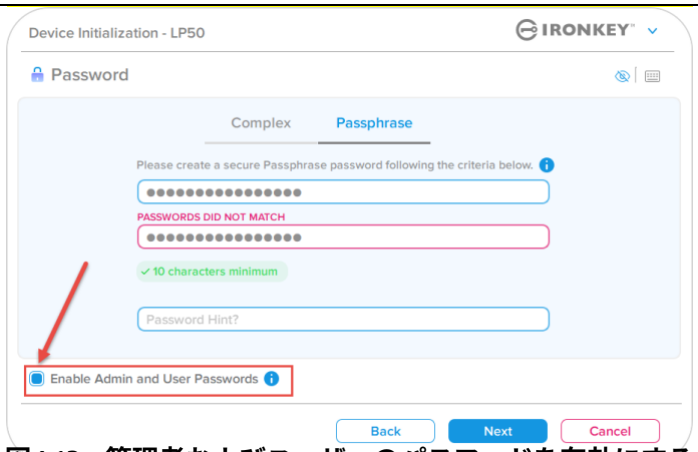


図4.12 – 管理者およびユーザーのパスワードを有効にする

注：管理者およびユーザーのパスワードの有効化は任意です。

ドライブでこの機能が「無効」に設定されている場合（ボックスがチェックされていない場合）、ドライブは、管理者機能のない単一ユーザー、単一パスワードドライブとして構成されています。本書では、この構成をユーザー専用モードと呼びます。

単一ユーザー、単一パスワード設定で進めるには、「管理者およびユーザーのパスワードを有効にする」にチェックしないまま、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を有効にした場合、次の画面でユーザーパスワード (User Password) の~~入力が求められます（図 4.13）~~。ユーザーパスワードの機能は管理者よりも制限されていますが、後ほど詳しく説明します。注：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（管理者とユーザーが有効な場合）

注：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スフレーズパスワード）の基準は、ユーザーパスワードに引き継がれ、ドライブの設定後に任意のパスワードリセットが必要になります。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4.14参照*）

注：これらのフィールドに入力する情報には、ステップ３で作成したパスワード文字列を入れることはできません。ただし、これらのフィールドは任意で、ブランクのまま残してもかまいません。）

「名前」(Name) 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力することはできません。

「会社名」(Company) のフィールドには、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力することはできません。

「詳細」(Details) 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含めることはできません。

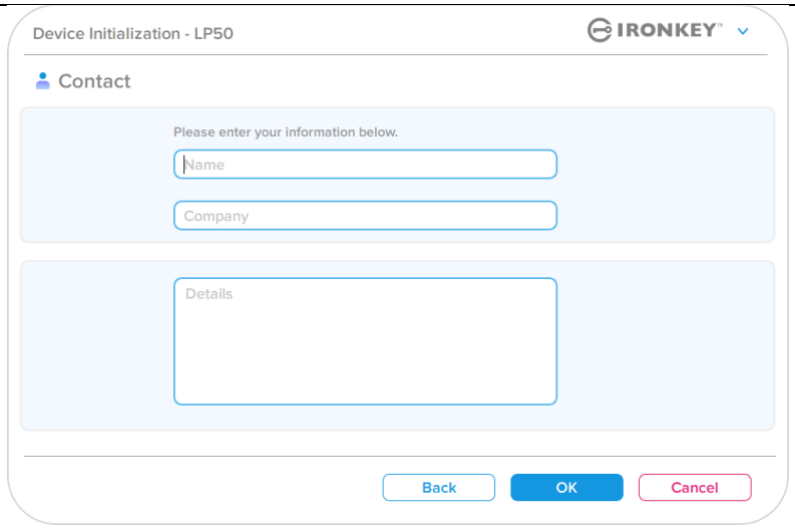
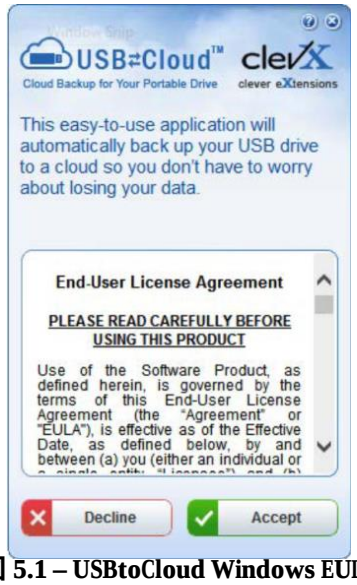


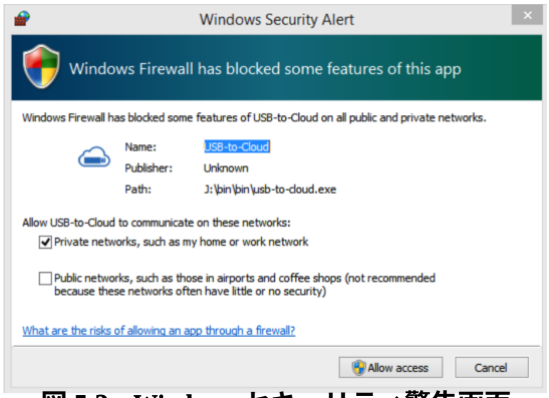
図 4.14 - 連絡先情報

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。ドライブの取り外しに進んでから、システムに差し込み直して、変更が反映されているかを確認します。

USB ß → クラウドの初期化 (Windows 環境)

Windows でデバイスの初期化が終わると、右側の 図 5.1 に示すように、USB-to-Cloud アプリケーションが表示されます。以下の手順に進む前に、インターネット接続がつながっているか確認してください。

• インストールを続けるには、clevX ウィンドウの右下の緑色の承諾 (Accept) ボタンをクリックしてください • インストールを中止する場合は、clevX ウィンドウの左下の赤色の拒否 (Decline) ボタンをクリックしてください。 • (注：赤色の「拒否」ボタンをクリックした場合、USB-to-Cloud のインストールは取り消されます。その場合は、データパーティションに USBtoCloudInstallDeclined.txt' という名前の特別なテキストファイルが作成されます。このファイルが存在する場合、将来のインストール時にアプリケーションのプロンプトが出力されません。)	 図 5.1 – USBtoCloud Windows EULA

• 初期化プロセス中に以下の Windows セキュリティ警告ウィンドウがポップアップ表示された場合は、「アクセスを許可する」（Allow access）をクリックして継続し、(または Windows ファイアウォール例外を作成し) USB-to-Cloud アプリケーションを継続します。	 図 5.2 – Windows セキュリティ警告画面

USB ß → クラウドの初期化 (Windows 環境)

- インストールが完了すると、(ユーザーの LP50 データと同期を取るための) オプションを一覧から選択するアプリケーションボックスが表示されます。
- バックアップアプリケーションとして使いたいクラウドオプションを選択し、認証に必要な証明を行ってください。
- (注：一覧で示されたクラウドオプションのいずれかでアカウントの設定を行っていない場合は、この時点でお気に入りのインターネットブラウザを使ってアカウントを作成し、このオプションの設定を行うことができます。)
- ユーザーがクラウドオプションを選択し、対応するサービスに対して認証を行うと、USB-to-Cloud プログラムは、データパーティションとクラウドの保存内容との最初の比較を行います。USB-to-Cloud サービスをタスクマネージャで実行している限り、データパーティションに書き込まれた内容はクラウドに自動的にバックアップ(同期)されます。

図 5.3 – クラウドの選択

USB ß → クラウドの使用 (Windows 環境)

USB-to-Cloud アプリケーションアプリケーションは、以下の拡張サービスを提供します。

- バックアップの一時停止 (データのバックアップを一時停止します)。
- 復元 (クラウドからデバイスへデータを復元します)。
- 設定 (データバックアップの追加オプションです)。
- 終了 (USB-to-Cloud サービスを終了します)。

「設定」メニューでは次のことができます。

- 現在バックアップに使用しているクラウドサービスアプリの変更。
- 現在使用している言語の変更。
- クラウドへバックアップするファイルやフォルダの選択。
- ソフトウェアのアップデート確認。

(注意:LP50 デバイスをリセット(またはフォーマット)すると、デバイスに保存されているデータがすべて失われます。しかしクラウドに保存されているデータデータは、安全に保持されます。)

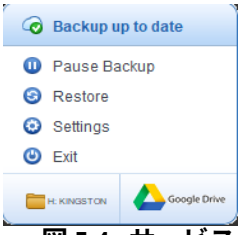


図 5.4 - サービス

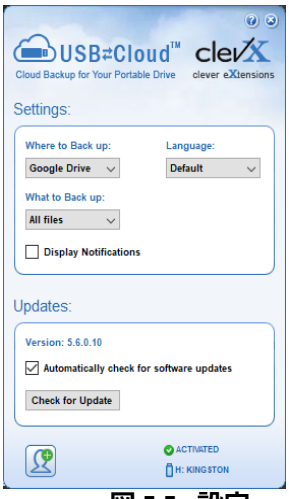


図 5.5 - 設定

USB ß → クラウドの初期化 (macOS 環境)

- デバイスの初期化が終わると、右側の*図 5.6* に示すように、USB-to-Cloud アプリケーションが表示されます。以下の手順に進む前に、インターネット接続がつながっているか確認してください。
- インストールを続けるには、clevX ウィンドウの右下の緑色の「承諾」 (Accept) ボタンをクリックしてください。 (注意:macOS 12.x 以上では、取外し可能なボリュームのファイルへのアクセスを許可するかどうかを選択する画面が表示されます。OK を選択します。)（図 5.7 参照）
- インストールを中止する場合は、clevX ウィンドウの左下の拒否 (Decline) ボタンをクリックしてください。

図 5.6 – USBtoCloud macOS EULA

(注意:「拒否」ボタンをクリックした場合、USB-to-Cloud のインストールは取り消されます。その場合は、データパーティションに DontInstallUSBtoCloud' という名前の特別なファイルが作成されます。このファイルが存在する場合、将来のインストール時にアプリケーションのプロンプトが出力されません。）

- インストールが完了すると、(ユーザーの LP50 データと同期を取るための) オプションを一覧から選択するアプリケーションボックスが表示されます。*(図 5.8)*

図 5.7- macOS アクセス

- バックアップアプリケーションとして使いたいクラウドオプションを選択し、認証に必要な証明を行ってください。

  (注意:一覧で示されたクラウドオプションのいずれかでアカウントの設定を行っていない場合は、この時点でお気に入りのインターネットブラウザを使ってアカウントを作成し、このオプションの設定を行うことができます。）
- ユーザーがクラウドオプションを選択し、対応するサービスに対して認証を行うと、USB-to-Cloud プログラムは、データパーティションとクラウドの保存内容との最初の比較を行います。USB-to-Cloud サービスをタスクマネージャで実行している限り、データパーティションに書き込まれた内容はクラウドに自動的にバックアップ(同期)されます。

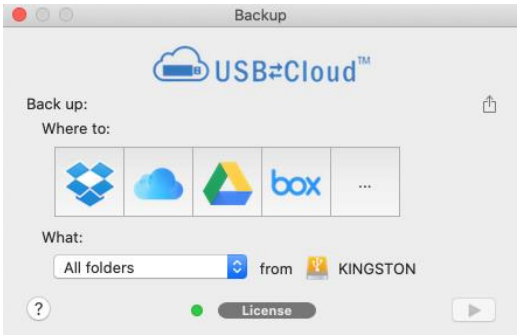
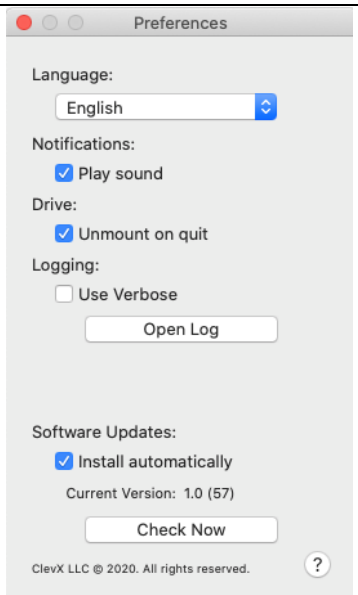


図 5.8 - クラウドの選択

USB ß →クラウドの使用 (macOS 環境)

USB-to-Cloud アプリケーションは、以下の拡張サービスを提供します（*図 5.9*）。 • バックアップの一時停止 (データのバックアップを一時停止します) • 復元 (クラウドからデバイスへデータを復元します) • バックアップ (クラウドオプションを開きます) *図 5.9 参照* • 終了 (USB-to-Cloud サービスを終了します)	 **図 5.9 - サービス**
「プリファレンス」メニューでは次のことができます。 • 現在使用している言語を変更 • サウンド通知を有効化/無効化 • アプリが終了した場合のドライブの取り外しを有効化/無効化 • トラブルシューティングの記録を有効化/無効化 • 今すぐアップデートを確認する自動ソフトウェア更新を有効化/無効	 **図 5.10 - USBtoCloud プレファレンス**

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（管理者が有効な場合）

デバイスが 管理者およびユーザーのパスワード（管理者ロール）を有効にして初期化されている場合、IronKey LP50 アプリケーションが起動し、ユーザーパスワードのログイン画面が最初に表示されます。ここでユーザーパスワードでログインし、入力した連絡先情報を表示するか、管理者としてログイン *（図 6.1）*できます。「管理者としてログイン」 (Login as Admin)ボタン（下図参照）をクリックすると、アプリケーションは管理者ログインメニューに進み、そこで管理者としてログインして管理者の設定と機能にアクセスすることができます*(図 6.2)*。

図 6.1 – ユーザーパスワードでのログイン（管理者が有効な場合）

図 6.2 – 管理者パスワードでのログイン

~~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 ページで前述したように、デバイスの利点を完全に活用するには、管理者ロール機能の使用が推奨されますが、ユーザー専用モード（単一パスワード、単一ユーザー）設定でも IronKey ドライブを初期化できます。これは、シンプルな単一パスワード手法を好む人が、ドライブでデータの安全を保つためのオプションです。*(図 6.3)*

注：管理者およびユーザーのパスワードを有効にするには、デバイスのリセット (Reset Device) ボタンを使用して初期化状態にドライブを戻します。そこで、管理者およびユーザーのパスワードを有効にできます。デバイスがリセットされると、ドライブ上のすべてのデータがフォーマットされ、永久に失われます。

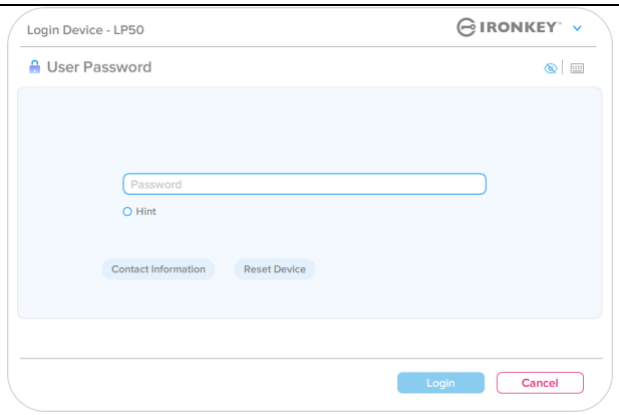


図 6.3 – ユーザーパスワードでのログイン（管理者が無効な場合）

デバイスの使用

総当たり攻撃の防止

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（総当たり攻撃防止機能ともいいます）が存在する点にご注意ください。*

パスワードの失敗回数が事前設定された 10 回に達すると、次のような処理が行われます。

管理者/ユーザー有効	総当たり攻撃防止 デバイスの動作 （間違ったパスワードを 10 回）	データの消去 およびデバイスの リセット？
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してください。	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 単一のユーザー、単一のパスワード (管理者/ユーザーが無効な場合)	総当たり攻撃防止 デバイスの動作 （間違ったパスワードを 10 回）	データの消去 およびデバイスの リセット？
ユーザーパスワード	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

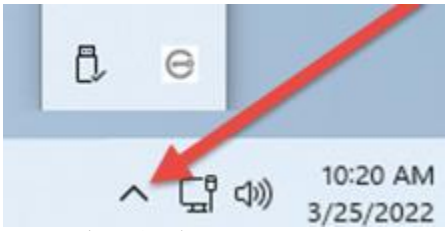
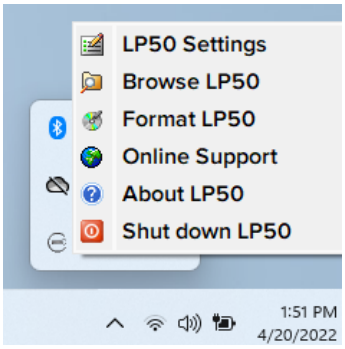
* デバイスの認証に一回成功すると、使用したログイン方式に関するログイン失敗回数がゼロにリセットされます。暗号化消去は、すべてのパスワード、暗号化キーおよびデータを削除します。**データは恒久的に失われます。**

保護下のファイルへのアクセス

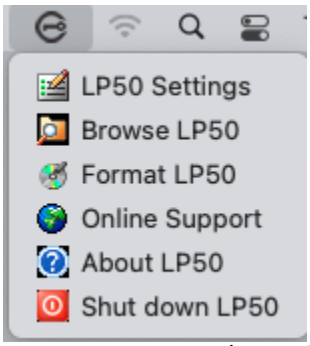
ドライブのロック解除後、保護下のファイルにアクセスできます。ドライブでそれらファイルを保存したり開くと、自動的に暗号化され復号化されます。このテクノロジーによって、強力な「常時オン」のセキュリティを利用しながら、いつものドライブでいつもの通り、便利に作業できます。
ヒント：ファイルにアクセスするには、Windows **タスクバーの IronKey アイコンを右クリックしてから、「LP50 の表示」をクリックします** *(**図** 7.2)*

デバイスの各種オプション - (Windows 環境の場合)

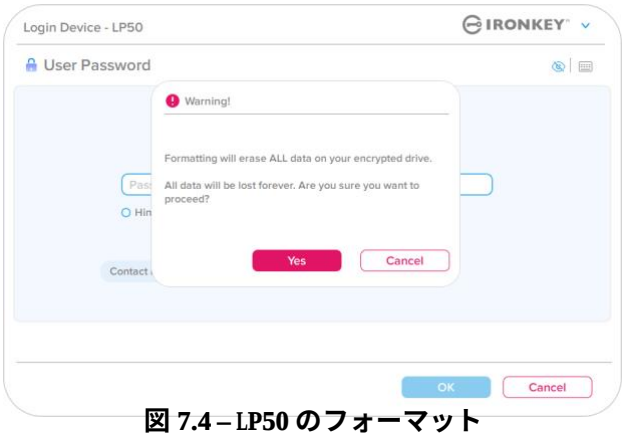
デバイスへログインしている状態では、ウィンドウの右隅に IronKey アイコンが表示されます。IronKey アイコンを右クリックすると、利用可能なドライブオプションの選択メニューが開きます*(図 6.2)*。これらのデバイスオプションについて詳しくは、本書の 19〜23 ページにあります。

• デバイスへログインしている状態では、ウィンドウの右隅に 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 ページにあります。	 図 7.2 IronKey アイコンを右クリックしてデバイスオプションを表示

デバイスの各種オプション - (macOS 環境の場合)

• デバイスへのログイン中には、*図 7.3* のように macOS メニューの中に IronKey LP50 アイコンがあり、利用可能なデバイスオプションを開くことができます。 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 ページにあります。	 図 7.3 - macOS メニューバーアイコン/デバイスオプションメニュー

デバイスオプション

LP50 の設定:	• **ログインパスワード、連絡先情報、その他の設定を変更します。（デバイス設定について詳しくは、本書の「LP50 の設定」セクションにあります。）**
LP50 の表示：	• **保護下のファイルを表示できます。**
LP50 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：データはすべて消去されます。）*(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 – LP50 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。**
LP50 について： アプリケーション、ファームウェア、シリアル番号情報など LP50 について詳しく説明します *(図 6.2)*。 注：ドライブ特有のシリアル番号は「情報欄」の下にあります。	 **図 7.5 – LP50 について**
LP50 のシャットダウン：	• **LP50 を適切にシャットダウンすると、システムから安全に切り離すことができます。**

LP50 の設定

管理者設定

管理者ログインによって、次のデバイス設定にアクセスできます。

- パスワード (Password)：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 (Contact Info)：連絡先の情報の追加/表示/変更が可能になります *(図 8.2)*。
- 言語 (Language)：現在の言語を変更できます *(図 8.3)*。
- 管理者オプション (Admin Options)：次のような追加機能を有効にできます。
    - o ユーザーパスワードの変更 *(図 8.4)*

注：管理者オプションについて詳しくは 25 ページにあります。

図 8.1 – 管理者パスワードのオプション

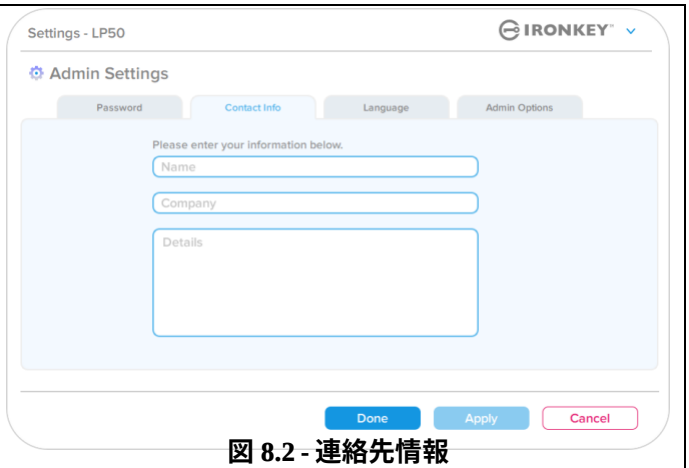


図 8.2 - 連絡先情報

図 8.3 - 言語オプション

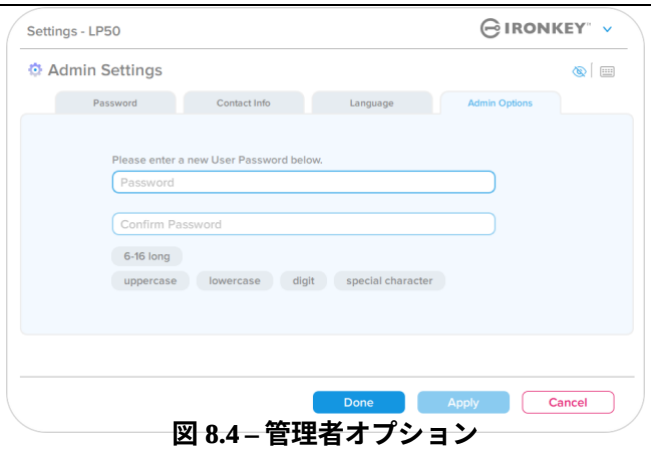
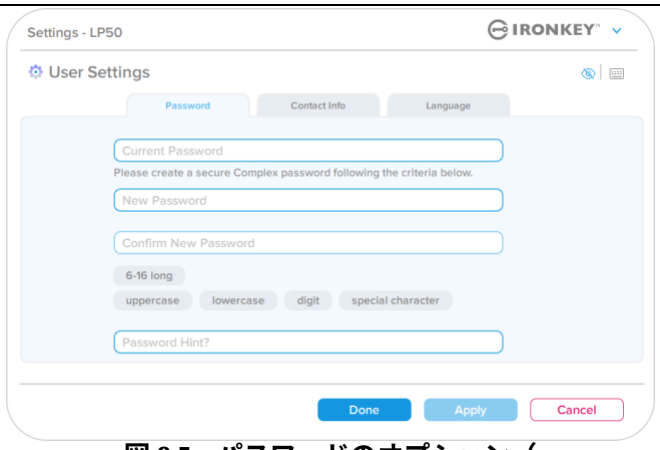
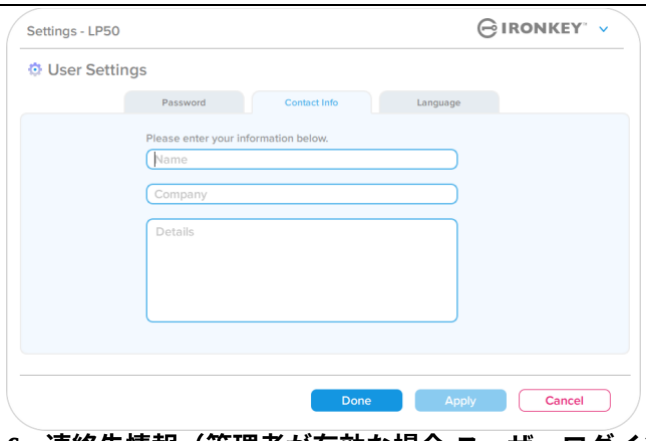
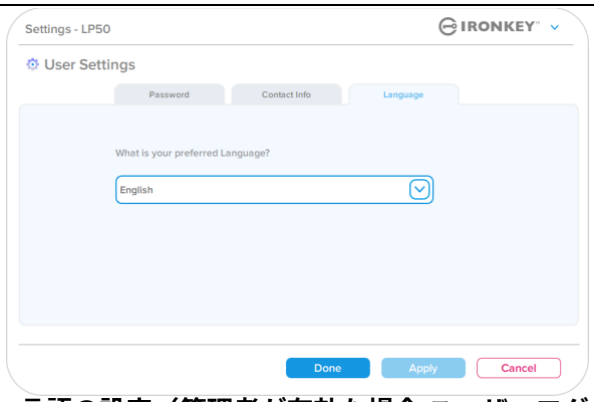


図 8.4 – 管理者オプション

LP50 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のみに制限されています。

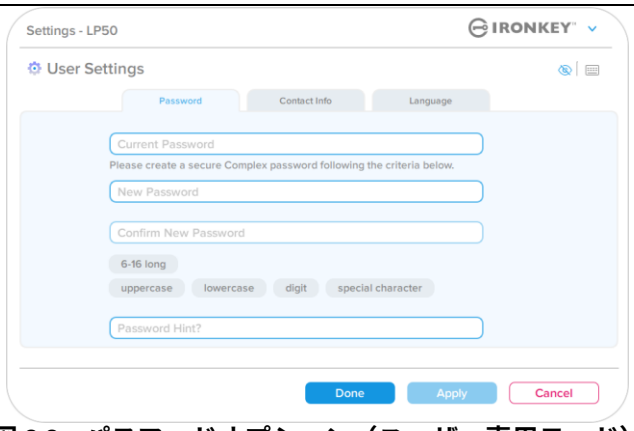
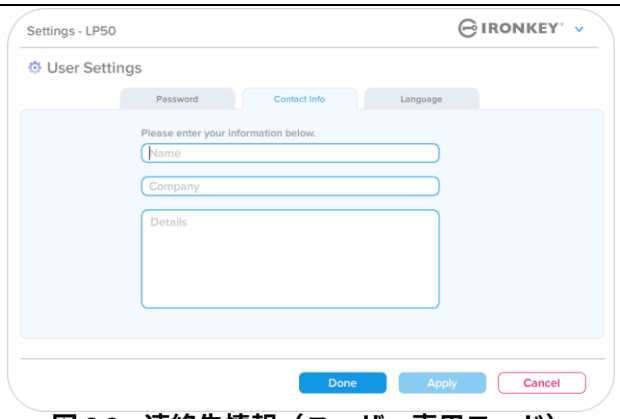
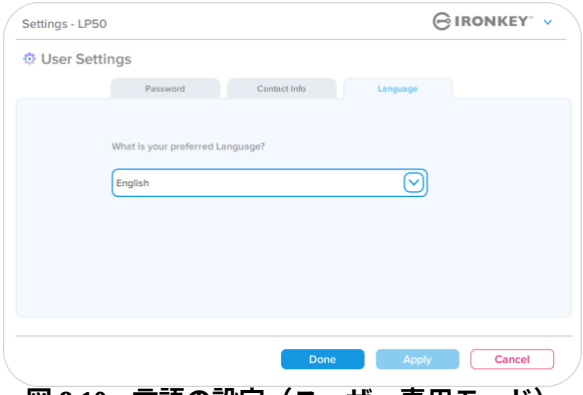
パスワード (Password)： **自分のユーザーパスワードやヒントを変更できます。*(図 8.5)***	 **図 8.5 – パスワードのオプション（管理者が有効な場合:ユーザーログイン）**
連絡先情報 (Contact Info)： **連絡先情報を追加/表示/変更できます。*(図 8.6)***	 **図 8.6 – 連絡先情報（管理者が有効な場合:ユーザーログイン）**
言語 (Language)： **現在の言語を変更できます。*(図 8.7)***	 **図 8.7 – 言語の設定（管理者が有効な場合:ユーザーログイン）**

注管理者オプションは、ユーザーパスワードでログインした場合にはアクセスできません。

LP50 の設定

ユーザー設定：管理者無効

12 ページで前述したように、「管理者およびユーザーのパスワード」を有効にせずに LP50 を初期化すると、ドライブは単一パスワード、単一ユーザー設定で構成されます。この構成では、管理者オプションまたは機能にアクセスできません。この構成では次の LP50 設定にアクセスできません。

パスワード (Password)： **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 (Contact Info)： **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 (Language)： **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）**

LP50 の設定

設定の変更および保存

- LP50 の設定（たとえば連絡先情報、言語、パスワード変更、管理者オプションなど）が変更された場合は常に、承認して適用するために、ドライブにパスワードの入力画面が表示されます。 *（図 8.11 参照）*

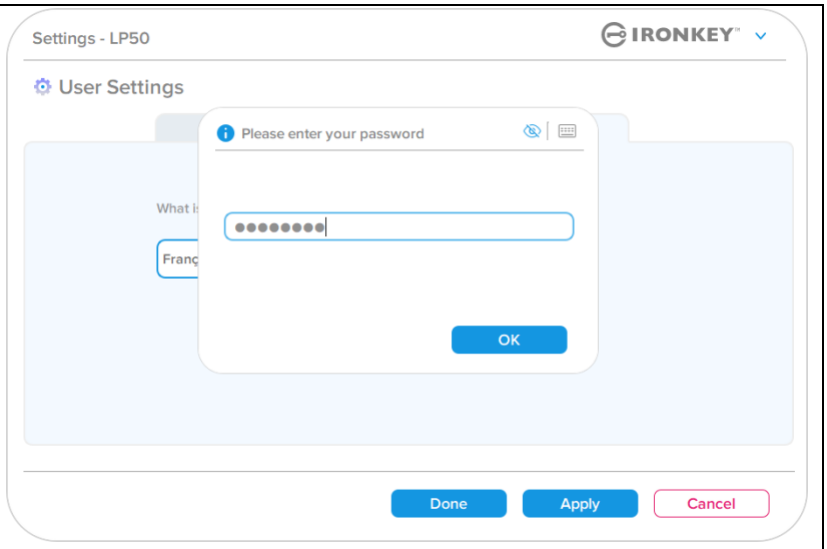


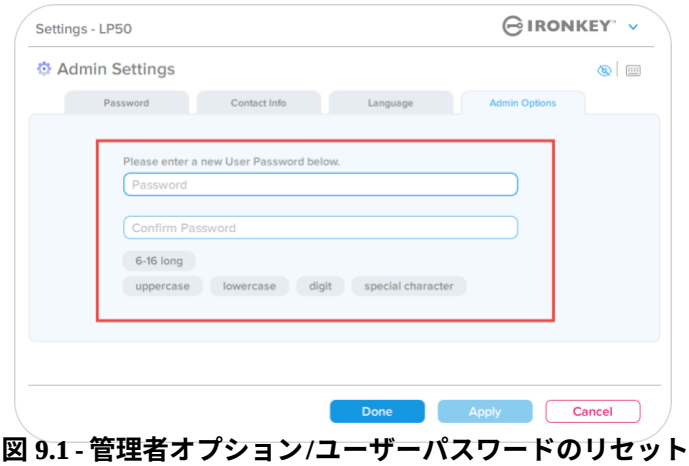
図 8.11 - LP50 の設定の変更を保存するためのパスワード入力画面

注：上図のパスワード入力画面が表示され、変更を取り消したいか修正したい場合は、パスワードフィールドをブランクにしたまま、OK (OK) をクリックします。すると、「パスワードを入力してください」ボックスが閉じ、LP50 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できるオプション

管理者構成の便利な機能として、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ます。下記は、ユーザーパスワードのリセットに役立つ「ユーザーパスワードのリセット」機能です。

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操作で変更します。すぐに変更でき、次のユーザーログインで有効になります。*(図 9.1)*** **注：パスワード要件の基準は、初期化プロセスで設定された基準に戻されます（複雑なパスワードまたはパスフレーズパスワード）。**	 **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

LP50 には、ログインの失敗回数が連続で最大回数に達すると（略語は *MaxNoA*）、データパーティションへの不正なアクセスを防ぐセキュリティ機能があります。「購入時」のデフォルト構成の事前設定値は、各ログイン方式（管理者/ユーザー）それぞれに対して 10 回（試行回数）です。

「ロック」カウンタは、不正アクセス回数を記録しており、この値は以下の 2 つの方法のいずれかでリセットされます。

1. MaxNoA の回数に達する前に、正常にログインした場合。

2. MaxNoA に達し、ドライブの構成に応じてデバイスのロックまたはデバイスのフォーマットのいずれかを実行した場合。

• 間違ったパスワードが入力された場合は、エラーメッセージがパスワード入力フィールドの上に赤で表示され、ログインが失敗したことを示します。*(図 10.1)*	 図 10.1 – パスワードが間違っている場合のメッセージ
• ログインが続けて 7 回失敗した場合、あと 3 回で MaxNoA の回数 (デフォルトの設定は 10 回) に達することを示す追加のエラーメッセージが表示されます。*(図 10.2)*	 図 10.2 - 7 回パスワードを間違えた場合のメッセージ

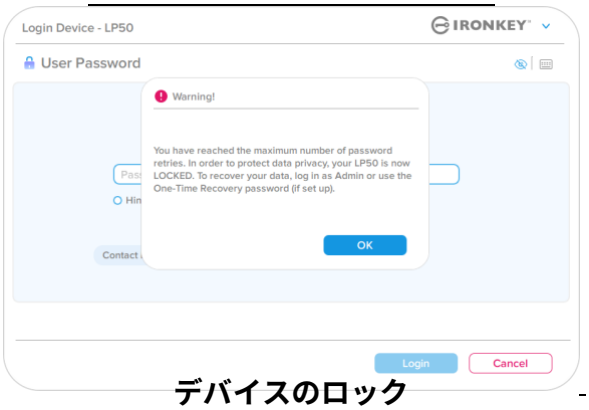
ヘルプとトラブルシューティング

デバイスのロック

重要：最後の 10 回目のログインに失敗した後、デバイスの設定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、デバイスはロックされるか、代替方法（利用できる場合）でのログインが必要になるか、デバイスリセット（データがフォーマットされ、ドライブ上のすべてのデータが永久に失われます）されます。この動きは、本書の 18 ページでも説明されています。

下の図 10.3～10.6 では、各パスワード方式で 10 回失敗し、試行できる最後のログイン回数に達した時に、どのような表示になるかを示しています。

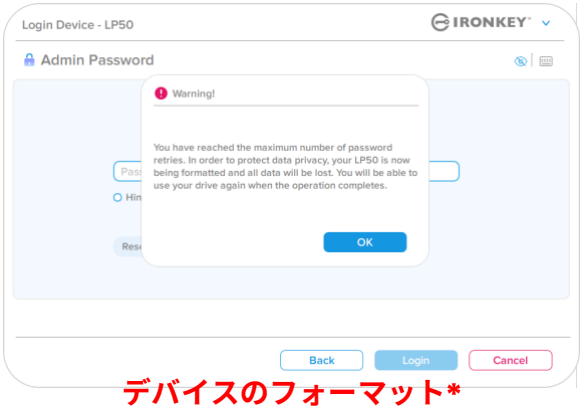
ユーザーパスワード：
(Admin/ユーザーが有効な場合)



デバイスのロック

(図 10.3)

管理者パスワード
(管理者/ユーザーが有効な場合)

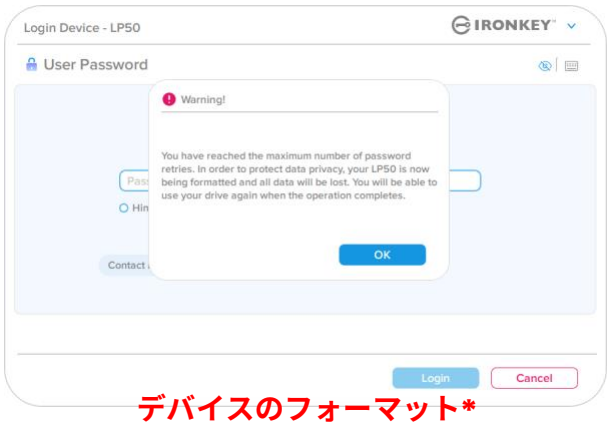


デバイスのフォーマット*

(図 10.4)

- **これらのセキュリティ対策は、（パスワードを知らない）誰かが何度もログインを試して、機密データへアクセスする（総当たり攻撃やブルートフォース攻撃と呼ばれます）ことのないよう、制限をかけます。LP50 の正規ユーザーの方がパスワードを忘れた場合でも、デバイスのフォーマットを含む同じセキュリティ対策が行われます。この機能の詳細は、*「デバイスのリセット」(25 ページ) をご覧ください。***

ユーザーパスワード（管理者が無効な場合）



デバイスのフォーマット*

(図 10.5)

注：デバイスをフォーマットすると、LP50 の保護下の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、LP50 の起動時に、ドライブの設定に応じて、2 か所のどちらかに表示（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。管理者/ユーザーが無効な場合は、ユーザーパスワードのログインメニュー）される「デバイスのリセット」ボタンをクリックできます。 ***（図 10.7 および 10.8 を参照してください）***

- **このオプションを選択して新しいパスワードを作成できますが、ユーザーデータのプライバシーを保護するために、LP50 は初期化されます。これは、上記のプロセス時にユーザーデータがすべて消去されることを意味します。***

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」** (Reset Device) **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を入力したいかどうか、質問されます。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 参照）***

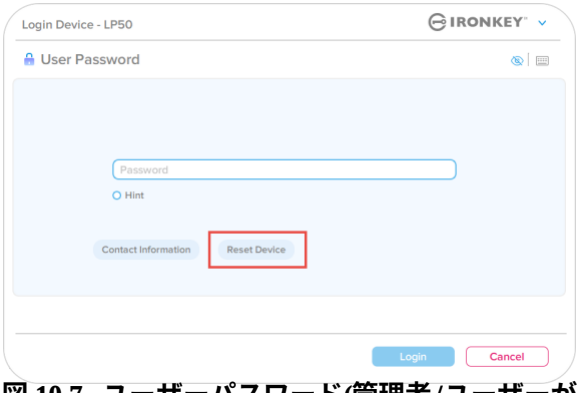


図 10.7 - ユーザーパスワード(管理者/ユーザーが無効な場合)デバイスのリセット

- **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ス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。ヒントは必須フィールドではありませんが、パスワードを忘れた場合、パスワードの手がかりを教えてくれるため、便利です。**

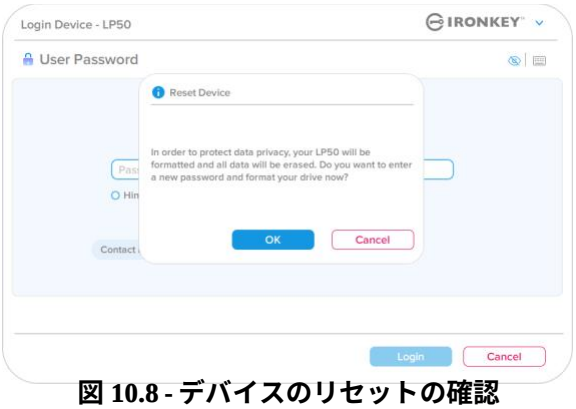


図 10.8 - デバイスのリセットの確認

ヘルプとトラブルシューティング

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（ページ 3）で前述したとおり、LP50 には、連続した２つのドライブ文字が必要です。この文字は、ドライブ文字の割当てが途切れる前の、最後の物理ディスクの直後になります（図 10.9 参照）これは、ネットワーク共有と連動しません。ネットワーク共有はユーザープロファイルに指定されており、ハードウェアプロファイル自体には指定がないので、OS からは利用可能に見えるためです。

- つまり Windows は、ネットワーク共有や UNC（汎用名前付け規則）がすでに使用しているパスに LP50 の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。競合が発生した場合、管理者またはヘルプデスク部門にお問い合わせいただき、Windows の「ディスクの管理」でドライブ文字の変更方法をお尋ねください (変更には管理者権限が必要です)。

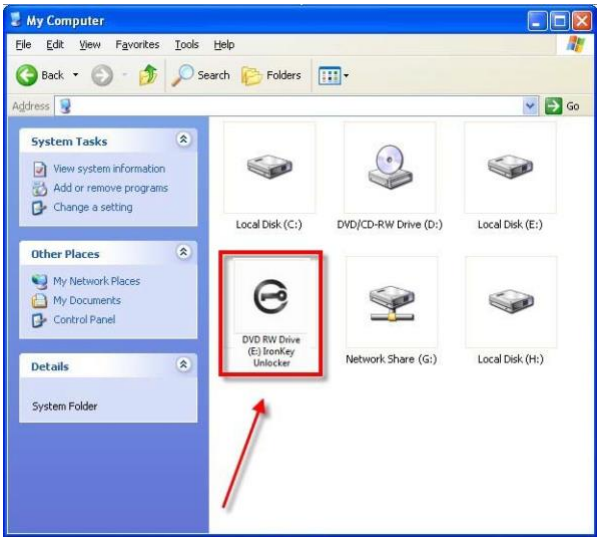


図 10.9 - ドライブレターの例

この例で言えば *(図 10.9)*、VP50 はドライブ E：の後の最初の利用可能なドライブ文字である F：を使用しています(E：がドライブ文字のギャップ前の最後の物理ディスクです)。ドライブ文字 G：はネットワーク共有であり、ハードウェアプロファイルの一部ではないため、LP50 は 2 番目のドライブ文字として G：を使用する可能性があり、競合が発生します。

システムにネットワーク共有がないのに LP50 が読み込まれない場合、カードリーダーやリムーバブルディスクなど、以前に取り付けられたデバイスにドライブ文字が割り当てられたままの状態になっているために、競合が発生する可能性があります。

ドライブ文字管理 (DLM) は、Windows 8.1 10 および 11 では大幅に改善されているため、この問題が発生しない場合もあります。しかし競合を解消できない場合、詳細を Kingston の技術サポート部門までお問い合わせいただくか、Kingston.com/support を参照してください。

IRONKEY™ Locker+ 50 (LP50)
USB 3.2 Gen 1 加密闪存盘

用户指南

目录

图 1：IronKey LP50

简介

金士顿 IronKey Locker+ 50 USB 闪存盘通过 XTS 模式下的 AES 硬件加密提供消费级安全性，包括通过数字签名固件防范 BadUSB 和防范暴力破解密码攻击。LP50 也符合 TAA 规范。

LP50 现在支持复杂或口令模式，可使用多密码（管理员和用户）选项。复杂模式允许使用 4 个字符集中的 3 个来输入包含 6-16 个字符的密码。新的口令模式允许输入数字 PIN、句子、单词列表，甚至可以输入包含 10 到 64 个字符的歌词。管理员可以启用用户密码，也可以重置用户密码，以恢复数据访问权限。为了便于输入密码，可以启用“眼睛”符号来显示输入的密码字符，从而减少导致登录尝试失败的拼写错误。暴力破解攻击保护会在连续输入 10 个无效密码时锁定用户，如果连续 10 次错误输入管理员密码，则会加密擦除闪存盘。此外，内置的虚拟键盘可以保护密码不被键盘记录器或屏幕记录器获取。

Locker+ 50 专为方便而设计，配有小型金属外壳和内置钥匙环，可将数据带到任何地方。LP50 还提供可选的 USBtoCloud（由 ClevX® 支持）备份，以便您通过 Google Drive™、OneDrive (Microsoft®)、Amazon Cloud Drive、Dropbox™ 或 Box 从个人云存储中访问闪存盘上的数据。LP50 易于任何人设置和使用，无需安装应用程序；所需的所有软件和安全性都已在闪存盘上。适用于 Windows® 和 macOS ®，因此用户可以从多个系统访问文件。

LP50 享有 5 年有限保固和免费金士顿技术支持服务。

IronKey Locker+ 50 功能

- XTS-AES 硬件加密（加密永远无法关闭）
- 暴力攻击和 BadUSB 攻击防护
- 多密码选项
- 复杂或口令密码模式
- “眼睛”按钮可显示输入的密码，减少失败的登录尝试
- 虚拟键盘有助于防范按键记录程序和屏幕记录器
- Windows 或 macOS 兼容（参见数据表了解详情）

关于本手册 (09242024)
本手册介绍了 IronKey Locker+ 50 (LP50)。

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 接口 • 在最后一个物理驱动器之后有两个连续的驱动器号* *注意：参见第 32 页的“ 驱动器号冲突 ”。	**PC操作系统支持** • Windows 11 • Windows 10
Mac 平台 • Intel 和 Apple SOC • 15MB 可用磁盘空间 • USB 2.0 - 3.2 接口	**Mac操作系统支持** • macOS 12.x – 15.x

注意：每个闪存盘在激活后享有免费的 5 年 USB-to-Cloud 订阅。满 5 年后可通过 ClevX 提供的继续激活选项进行购买。

建议

为了确保 LP50 设备供电充足，请将其直接插在笔记本电脑或台式机所带的 USB 接口中，如图 1.1 所示。避免将 LP50 连接到任何带 USB 接口的外围设备中，如键盘或 USB 供电集线器，如*图 1.2* 所示。

图 1.1 - 建议使用

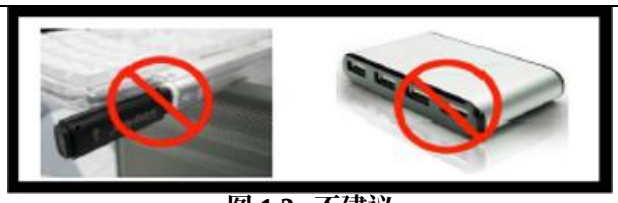


图 1.2 - 不建议

使用正确的文件系统
IronKey LP50 使用 FAT32 文件系统进行了预格式化。这种格式支持 Windows 和 macOS 两种系统。不过，可以使用一些其他选项手动格式化闪存盘，例如适合 Windows 的 NTFS 和 exFAT。您可以根据需求重新格式化数据分区，但闪存盘重新格式化后数据会丢失。

使用提醒
为了确保数据安全，金士顿建议您：

- 在目标系统上设置和使用 LP50 之前，对计算机执行病毒扫描
- 不使用时锁定闪存盘
- 在拔出前从系统中弹出闪存盘
- 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
- 从不向任何人透露您的设备密码

查找最新更新与信息

访问 kingston.com/support，获取最新闪存盘驱动程序、常见问题解答、文档和其他信息。

注意：仅为闪存盘应用最新的闪存盘可用更新。不支持将闪存盘降级为更早的软件版本，否则可能导致存储的数据丢失或损坏闪存盘功能。如有疑问或问题，请联系金士顿技术支持部门。

密码设置最佳实践

LP50 配备强大的安全应对举措。这包括暴力攻击防范，通过将密码尝试次数限制为 10 次，阻止攻击者猜出密码。达到闪存盘上限后，LP50 会自动清除加密数据 – 即执行格式化并恢复出厂设置。

多密码
多密码是 LP50 的一大功能，用于在忘记一个或多个密码时避免数据丢失。启用所有密码选项后，LP50 支持利用两个不同的密码来恢复数据 – 管理员密码和用户密码。

LP50 让您可以选择两个主要密码 – 管理员密码和用户密码。管理员可以随时访问闪存盘并为用户设置选项，管理员就像是超级用户。

用户也可以访问闪存盘，但相比管理员权限有限。如果忘记两个密码中的一个，可以使用另一个密码访问和找回数据。然后闪存盘可以重新设置最多两个密码。务必设置两个密码，并在使用用户密码的同时将管理员密码保存到安全的地方。

如果忘记了所有密码，则无法以任何方式访问数据。由于安全设置不存在后门，金士顿也无法找回数据。金士顿建议您也将数据保存到其他介质。LP50 可被重置并重新投入使用，但之前的数据会永久删除。

密码模式
LP50 还支持两个不同的密码模式：

复杂
复杂密码需要至少包含 6-16 个字符，并使用至少 3 个以下字符：

- 大写字母字符
- 小写字母字符
- 数字
- 特殊字符

口令
LP50 支持 10 至 64 个字符的口令。口令没有额外规则，但若使用得当，可以提供极高水平的密码保护。

口令基本上是任何组合的字符，包括来自其他语言的字符。就像 LP50 闪存盘，密码语言可以匹配为此闪存盘选择的语言。这让您可以选择多个单词、一个短语、歌词、一行诗等。优秀的密码短语是攻击者最难猜到的密码类型之一，且可能更易于用户记住。

设置我的设备

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。避免将其连接到包含 USB 接口的任何外围设备，例如键盘或 USB 供电的集线器。该设备的初始设置必须在受支持的 Windows 或 macOS 操作系统中完成。

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 接口，等待 Windows 检测到该闪存盘。

- Windows 8.1/10/11 用户会收到设备驱动程序通知。 *（图 3.1）*

图 3.1 – 设备驱动程序通知

- 一旦新硬件检测完成，可利用文件资源管理器在 Unlocker 分区中找到**IronKey.exe**。 *（图 3.2）*
- 请注意，分区号可能有所不同，具体取决于下一个空闲驱动器号。驱动器号可能因连接的设备不同而异。在右侧图中，驱动器号是 (E:)。

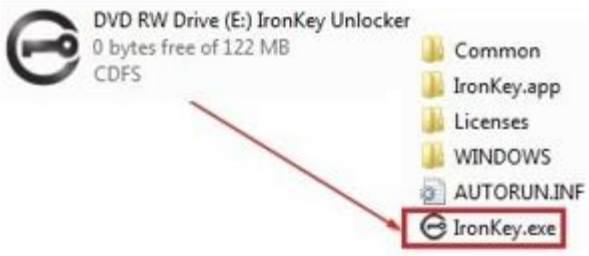


图 3.2 – File Explorer Window/IronKey.exe

设备访问（macOS 环境）

将 LP50 插入笔记本电脑或台式机的可用 USB 接口，等待 Mac 操作系统检测到该闪存盘。检测到后，您会在桌面上看到“ IRONKEY ”盘标。 *（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。

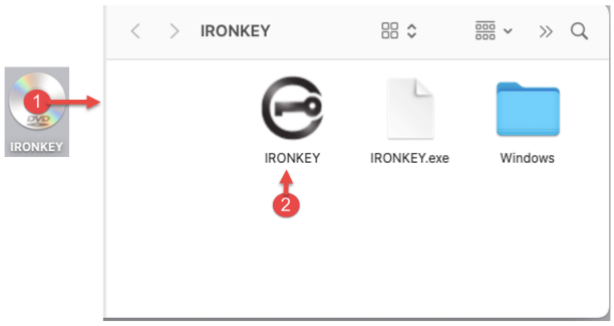


图 3.3 - IKLP 盘标

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偏好，并单击“下一步”**(Next)**（*参见图 4.1*）。

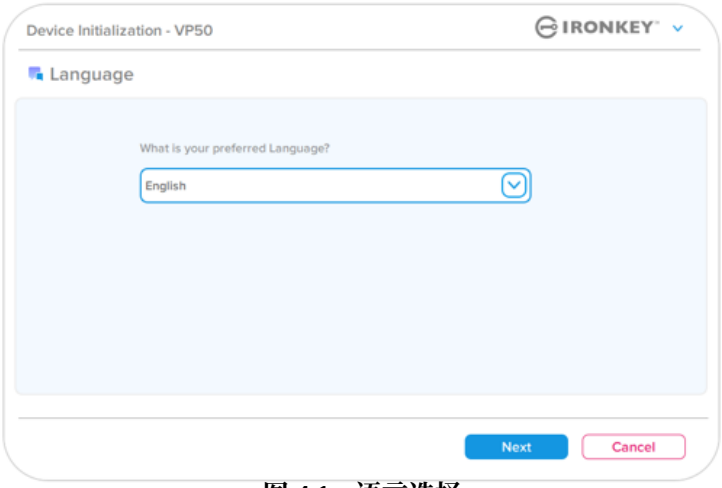


图 4.1 – 语言选择

- 查看许可协议并单击“下一步”**(Next)**。

  注意：您必须接受许可证协议才能继续操作；否则“下一步”(Next) 按钮将一直处于禁用状态。（*图 4.2*）

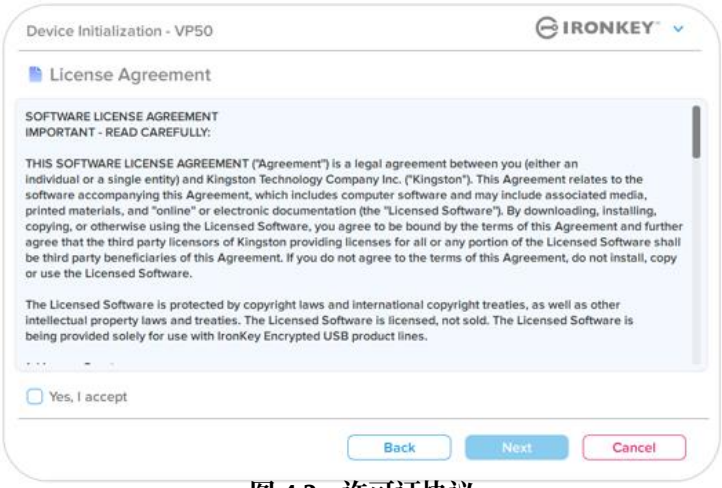


图 4.2 – 许可证协议

设备初始化

密码选择

在“密码”(Password)提示窗口中，您能够使用复杂或口令密码模式创建密码，来保护您在 LP50 中的数据（*图 4.3- 4.4*）。此外，还可以在该屏幕中启用多密码管理员/用户选项。在继续选择密码前，请查看下文的“启用管理员/用户密码”，更好地理解这些功能。

注意：一旦选择复杂或口令模式，除非重置设备，否则无法更改模式。

要开始密码选择流程，请在“密码”(Password) 字段中创建密码，然后在“确认密码”(Confirm Password) 字段中重新输入密码。创建的密码必须符合以下条件，然后才能继续进行初始化过程：

<table>
<tr>
<td>

“复杂”(Complex) 密码

- 密码必须包含 6 个或更多字符（最多 16 个字符）。
- 必须满足以下三 (3) 个条件：
  - 大写
  - 小写
  - 数字
  - 特殊字符（!、$、& 等）

</td>
<td>

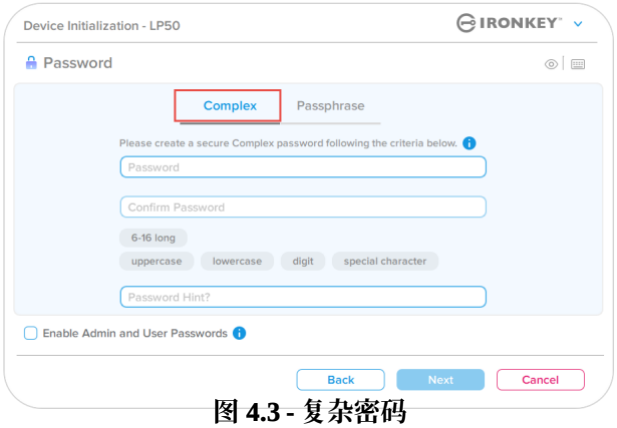


图 4.3 - 复杂密码

</td>
</tr>
<tr>
<td>

“口令”(Passphrase) 密码

- 必须包含：
  - 最少 10 个字符
  - 最多 64 个字符

</td>
<td>

图 4.4 - 口令密码

</td>
</tr>
<tr>
<td>

“密码提示”(Password Hint)（可选）

密码提示在忘记密码时很有用，它可以提供有关密码的线索。
注意：提示内容不得与密码完全相同。

</td>
<td>

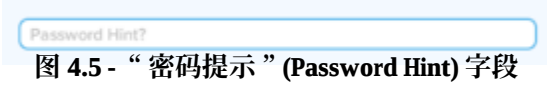


图 4.5 - “密码提示”(Password Hint) 字段

</td>
</tr>
</table>

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：一旦满足至少三个密码条件，第四个条件框会变成灰色，表示此条件可选项*（图 4.6b）*。

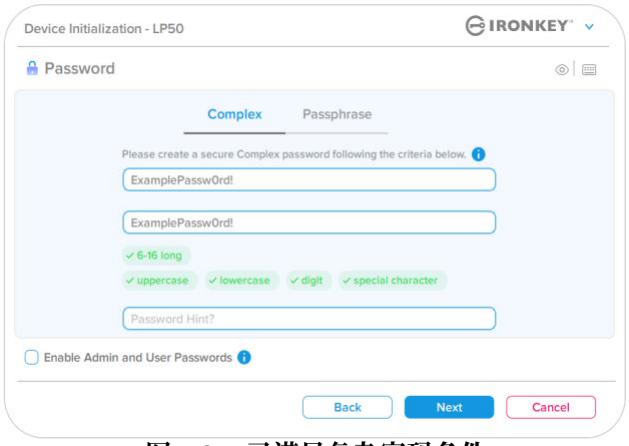


图 4.6a - 已满足复杂密码条件

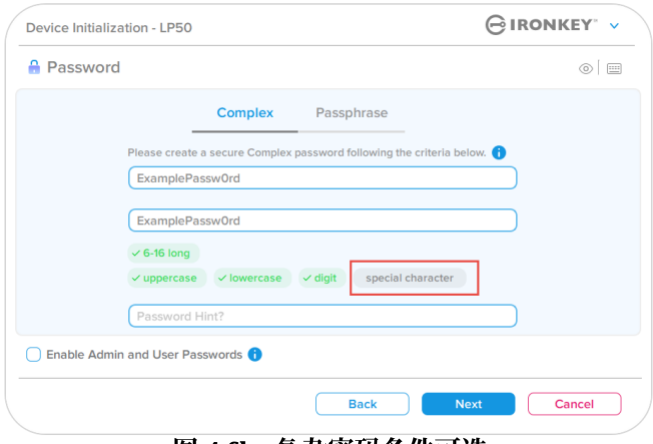


图 4.6b - 复杂密码条件可选

对于无效密码，密码条件框会以红色高亮显示，“下一步”(Next) 按钮会在满足最低要求前被停用。

这适用于复杂密码和口令密码。

图 4.7 - 未满足复杂密码条件

设备初始化

虚拟键盘
LP50 配备虚拟键盘，可防范按键记录程序。

- 要利用虚拟键盘，在“ 设备初始化 ”(设备初始化) 屏幕的右上角找到键盘按钮，并选择该按钮。

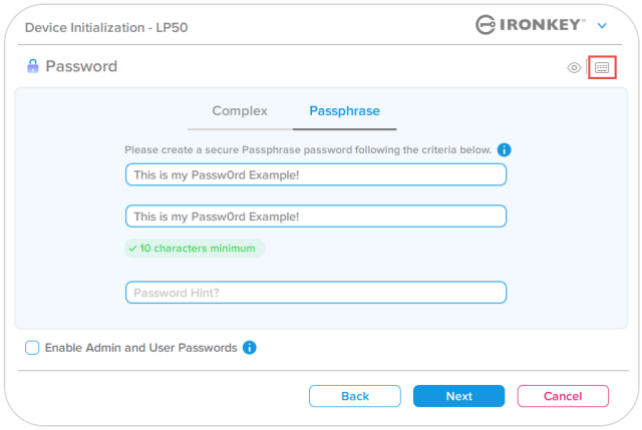


图 4.8 - 激活虚拟键盘

- 一旦虚拟键盘出现，您还可以启用“ 屏幕记录器防护 ”(Screenlogger Protection)。使用该功能后，所有按键都会短暂变成空白。这是预期的行为，可以阻止屏幕记录器捕获您点击的内容。
- 为了让这项功能更加强大，您还可以选择键盘右下角的“ 随机排列 ”(randomize)，让虚拟键盘随机排列。随机排列会以随机方式排列键盘布局。

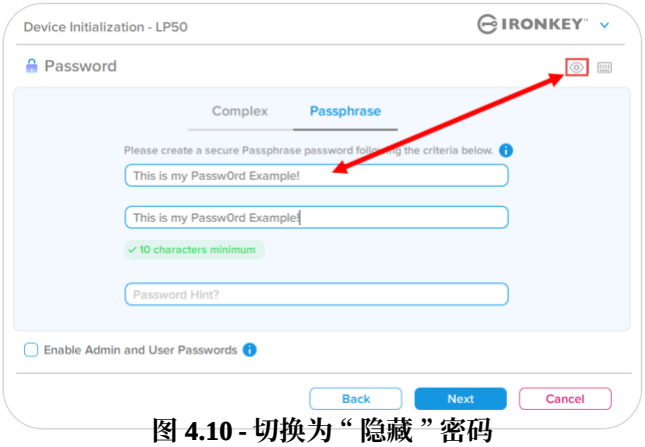
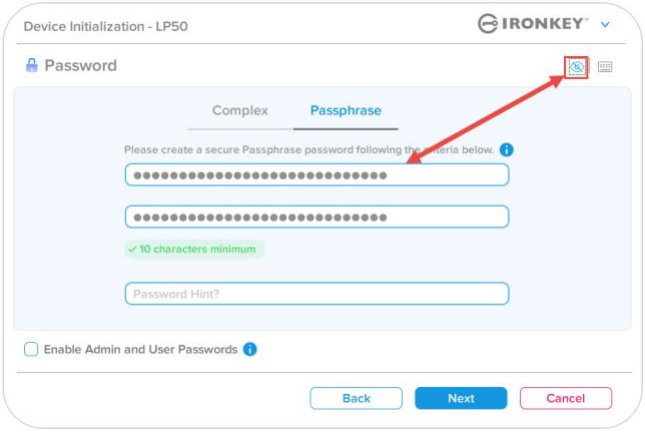
图 4.9 - 屏幕记录器保护 / 随机排列

设备初始化

密码可见性切换

默认情况下，当您创建密码时，密码字符串会在输入过程中显示在字段中。如果希望在输入过程中隐藏密码，可以切换“ 设备初始化 ”(设备初始化) 窗口右上角的密码“ 眼睛 ”。

注意：在设备完成初始化后，密码字段默认为“ 隐藏 ”。

要隐藏密码字符串，请单击灰色图标。 	 **图 4.10 - 切换为“ 隐藏 ”密码**
要显示隐藏的密码，请单击蓝色图标。 	 **图 4.11 - 切换为“ 显示 ”密码**

设备初始化

管理员密码和用户密码

通过启用管理员密码和用户密码，您可以利用多密码功能，其中管理员角色可以管理这两种帐号。通过选择“启用管理员密码和用户密码”(Enable Admin and User passwords)，可在忘记密码时实现替代的闪存盘访问方法。

启用管理员密码和用户密码后，您还可以访问：

- **用户密码重置**

要详细了解用户密码重置功能，请转到本用户指南第 28 页。

- **要启用管理员密码和用户密码，请单击“启用管理员密码和用户密码”(Enable Admin and User Passwords) 旁的框，然后在选中有效密码后选择“下一步”(Next)。** *（图 4.12）*
- **如果该功能已启用，那么本屏幕中的所选密码是管理员密码。单击“下一步”(Next)，会转到“用户密码”(User Password) 屏幕，在此可为用户选择密码。**

图 4.12 - 启用管理员密码和用户密码

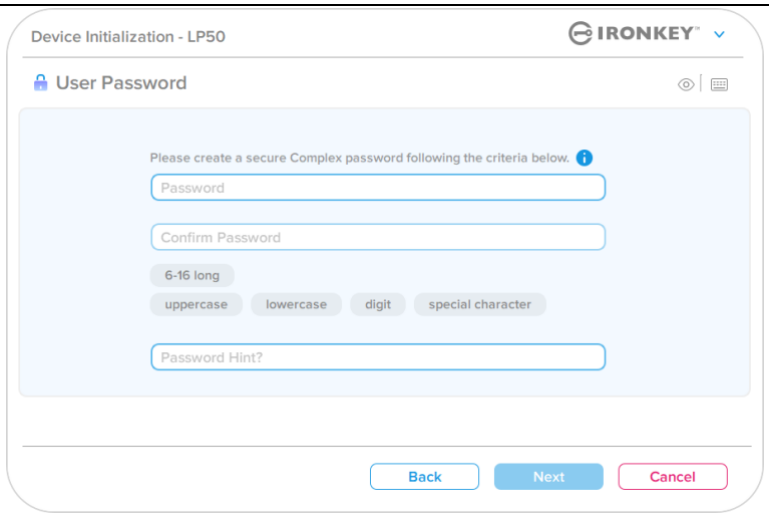
注意：启用管理员密码和用户密码是可选项。

如果设置闪存盘时未启用该功能（未勾选框），那么闪存盘会配置为单用户、单密码闪存盘，且无任何管理员功能。该配置在本手册中称为仅用户模式。

要继续进行单用户、单密码设置，请确保“启用管理员密码和用户密码”(Enable Admin and User Passwords) 未勾选，然后在创建有效密码后单击“下一步”(Next)。

设备初始化

管理员密码和用户密码

如果管理员角色在前一屏幕中已启用，下一屏幕会提示创建“用户密码”(User Password)（*图 4.13*）。用户密码的权限比管理员密码少，在本指南后续部分将作详细介绍。注意：“管理员密码和用户密码”(Admin and User Passwords) 在本手册下文中称作“管理员角色”(Admin Role)。	 **图 4.13 - 用户密码（管理员和用户已启用）**

注意：所选密码选项（复杂或口令）条件会应用于用户密码，以及闪存盘设置后所需的任何密码重置。所选密码选项只能在完整设备重置后可以更改。

设备初始化

联系信息

在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在第 3 步创建的密码字符串。（不过，这些字段是可选项，可以根据需要留空。）

“姓名”(Name) 字段最多可包含 32 个字符，但是不得包含确切密码。

“公司”(Company) 字段最多可包含 32 个字符，但是不得包含确切密码。

“详情”(Details) 字段最多可包含 156 个字符，但是不得包含确切密码。

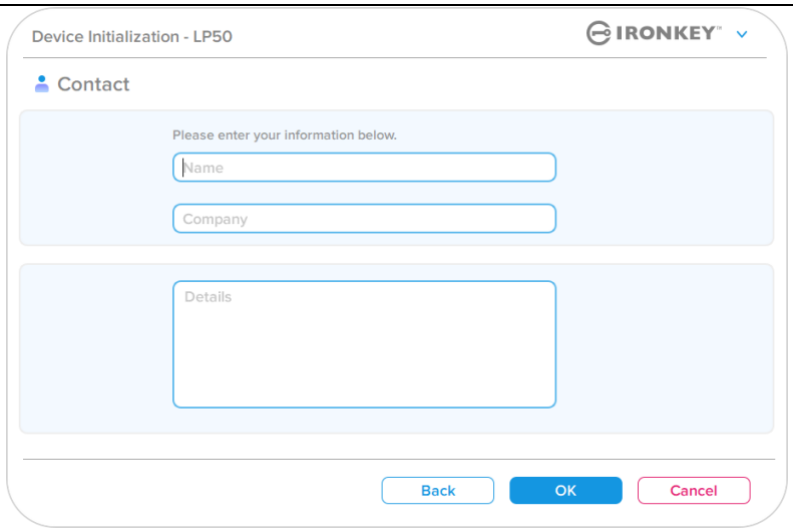


图 4.14 - 联系信息

注意：单击“确定”(OK) 将完成初始化流程并进入解锁环节，然后装载安全分区，您可以在此分区中安全地存储数据。继续从系统拔出闪存盘并重新插入，即可看到所作更改。

USB ß → Cloud 初始化和使用（Windows 环境）

一旦在 Windows 中设备完成初始化，USB-to-Cloud 应用程序将会出现，如右侧*图 5.1* 所示。请在继续前确保您拥有有效的互联网连接。

- 要继续安装，单击 clevX 窗口右下角的绿色“ 接受 ”(Accept) 按钮。
- 要拒绝安装，单击 clevX 窗口底部左侧的红色“ 拒绝 ”(Decline) 按钮。
- (注意：如果您单击红色的“ 拒绝 ”(Decline) 按钮，USB-to-Cloud 安装将会取消。这样做，将在数据分区创建一个名为 'USBtoCloudInstallDeclined.txt' 的特殊文本文件。此文件的存在将阻止应用程序今后提醒您进行安装。）

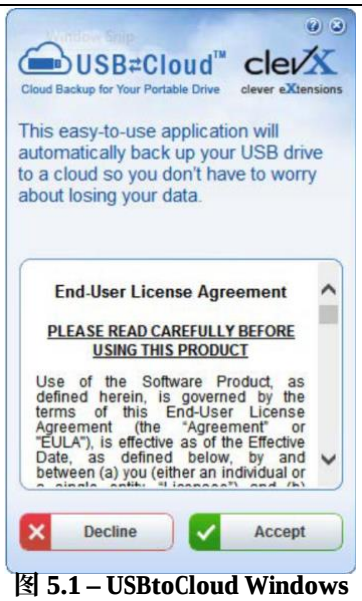


图 5.1 – USBtoCloud Windows 最终用户许可协议 (EULA)

- 如果初始化过程中弹出以下“ Windows 安全警报 ”窗口，请单击“ 允许访问 ”继续（或创建 Windows 防火墙例外），以继续安装 USB-to-Cloud 应用程序。

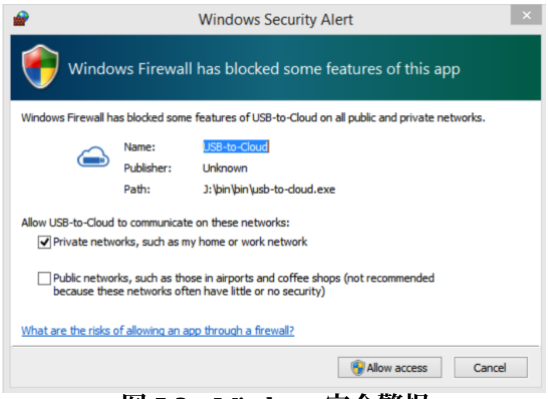


图 5.2 – Windows 安全警报

USB ß → Cloud 使用（Windows 环境）

- 一旦安装完成，您将看到一个包含一系列选项的应用程序窗口（用于同步您的 LP50 数据）。
- 选择您期望使用的云选项作为备份应用程序，并提供验证所需的凭证。
- （注意：如果您当前尚未创建所列云选项的帐户，您现在可以使用您喜欢的互联网浏览器创建一个，并随后完成此选项。）
- 一旦您选定云选项并完成对应服务的验证，USB-to-Cloud 程序将对数据分区和云中存储的内容执行初次比较。只要 USB-to-Cloud 服务运行在任务管理器中，写入数据分区的内容将自动备份（同步）到云中。

图 5.3 – 云选择

USB ß → Cloud 使用（Windows 环境）

USB-to-Cloud 应用程序提供以下额外服务：

- 暂停备份（暂停数据备份）。
- 恢复（将数据从云恢复到设备）。
- 设置（数据备份的额外选项）。
- 退出（退出 USB-to-Cloud 服务）。

在“ 设置 ” (Settings) 菜单中，您可以：

- 更改当前用于备份的云服务应用。
- 更改当前使用的语言。
- 选择要备份到云中的文件和/或文件夹。
- 检查软件更新。

（注意：如果您重置（或格式化）LP50 设备，设备上的所有数据将会丢失。不过，云中存储的所有数据都是安全、完整的。）

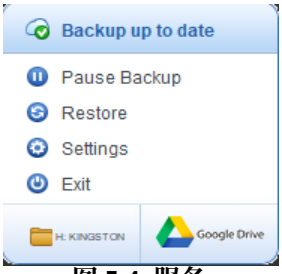


图 5.4- 服务

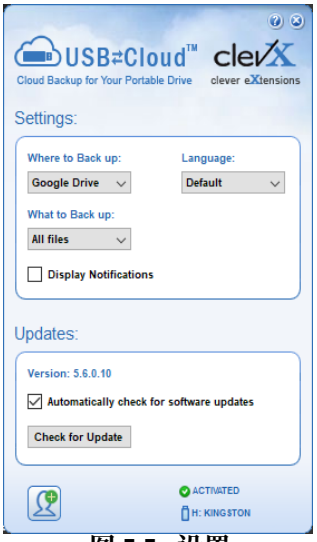


图 5.5 - 设置

USB ß → Cloud 初始化和使用（macOS 环境）

- 一旦设备完成初始化，USB-to-Cloud 应用程序将会出现，如右侧*图 5.6* 所示。请在继续前确保您拥有有效的互联网连接。
- 要继续安装，单击 clevX 窗口右下角的“ 接受 ”(Accept) 按钮。

  （注意：在 macOS 12.x + 上，系统会提示您允许访问可移动盘上的文件。选择“ 好 ”。） *（参见图 5.7）*
- 要拒绝安装，单击 clevX 窗口底部左下角的“ 拒绝 ”(Decline) 按钮。

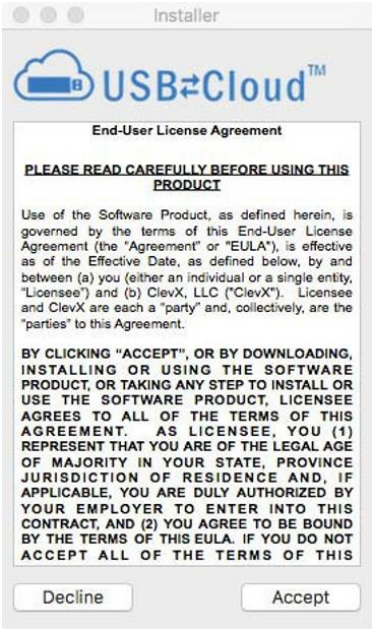


图 5.6 – USBtoCloud macOS 最终用户许可协议 (EULA)

（注意：如果您单击“ 拒绝 ”(Decline) 按钮，USB-to-Cloud 安装将会取消。如此一来，在数据分区中会创建一个名为 'DontInstallUSBtoCloud' 的特殊文件。此文件的存在将阻止应用程序今后提醒您进行安装。）

- 一旦安装完成，您将看到一个包含一系列选项的应用程序窗口（用于同步您的 LP50 数据）。 *（图 5.8）*

图 5.7- macOS 访问

- 选择您期望使用的云选项作为备份应用程序，并提供验证所需的凭证。

  （注意：如果您当前尚未创建所列云选项的帐户，您现在可以使用您喜欢的互联网浏览器创建一个，并随后完成此选项。）
- 一旦您选定云选项并完成对应服务的验证，USB-to-Cloud 程序将对数据分区和云中存储的内容执行初次比较。只要 USB-to-Cloud 服务运行在任务管理器中，写入数据分区的内容将自动备份（同步）到云中。

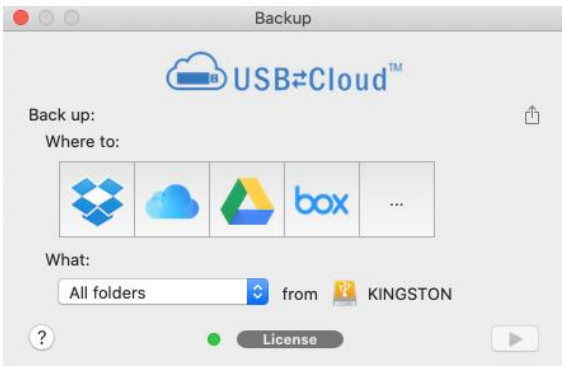
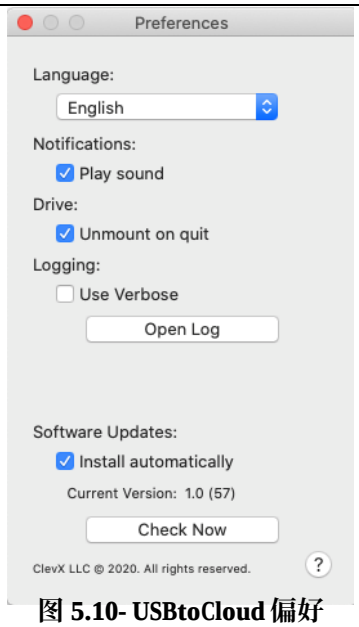


图 5.8 – 云选择

USB ß →Cloud 使用（macOS 环境）

USB-to-Cloud 应用程序提供以下额外服务（*图 5.9*）： • 暂停备份（暂停数据备份） • 恢复（将数据从云恢复到设备） • 备份（打开云选项） *参见图 5.9* • 退出（退出 USB-to-Cloud 服务）	 图 5.9- 服务
在“偏好”(Preferences) 菜单中，您可以： • 更改当前使用的语言 • 启用/停用声音通知 • 启用/停用在应用退出时取消挂载闪存盘 • 启用/停用故障排除日志记录 • 启用/停用自动软件更新和立即检查更新	 图 5.10- USBtoCloud 偏好

设备使用（Windows 和 macOS 环境）

管理员和用户的登录（管理员已启用）

如果设备已初始化并启用了管理员密码和用户密码（管理员角色），IronKey LP50 应用会启动，首先会弹出“用户密码”(User Password) 登录屏幕。在此，您可以使用用户密码进行登录、查看任何输入的联系信息，或作为管理员登录（*图 6.1*）。单击“作为管理员登录”(Login as Admin) 按钮（如下所示），该应用会转到管理员登录菜单，您在此可以作为管理员登录，以访问管理员设置和功能（*图 6.2*）。

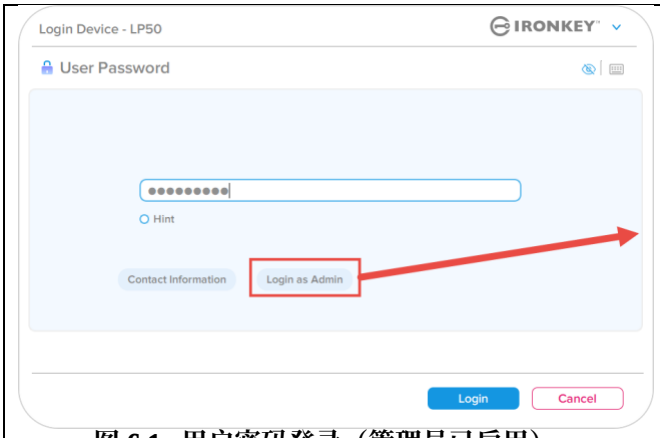


图 6.1 - 用户密码登录（管理员已启用）

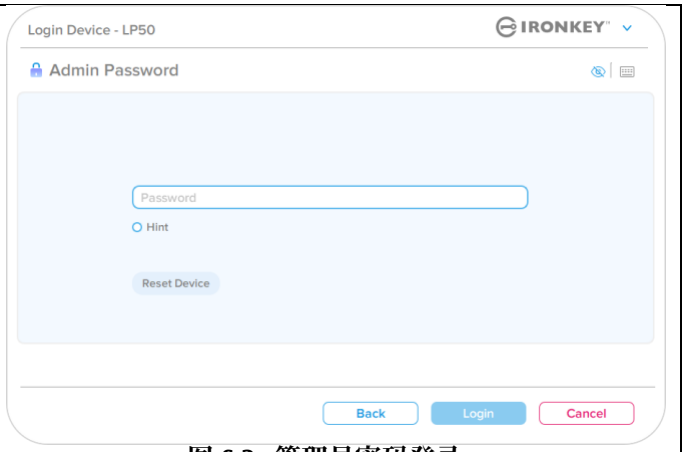


图 6.2 - 管理员密码登录

仅用户模式登录（管理员未启用）

如第 13 页所述，尽管建议使用管理员角色功能来发挥设备的全部优势，但 IronKey 设备也可以初始化为仅用户（单密码、单用户）配置。这个选项适合希望用简单的单密码方法保护闪存盘数据的用户。（*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”(Reset Device) 按钮，让闪存盘进入初始化状态，从而可以启用管理员密码和用户密码。重置闪存盘后，闪存盘会被格式化，其中所有数据会丢失。

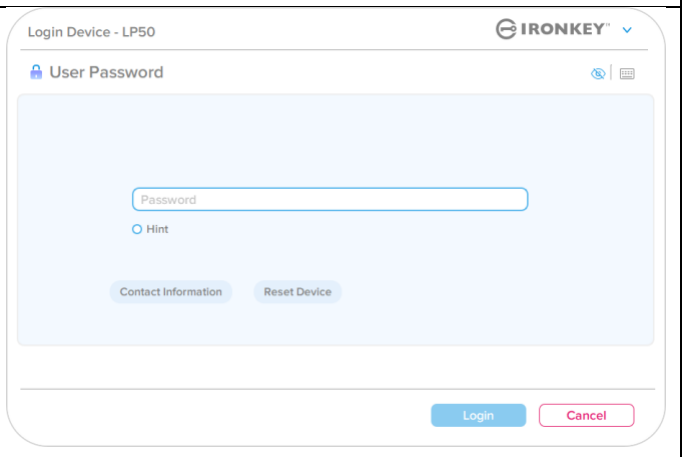


图 6.3 - 用户密码登录（管理员未启用）

设备使用

暴力攻击防护

重要事项：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。*

如果此值达到预先配置的 10 次密码尝试失败次数，闪存盘会出现以下行为：

管理员/用户已启用	暴力攻击防护 设备行为 （10 次不正确的密码尝试）	数据擦除和 设备重置？
用户密码：	密码锁定。作为管理员登录重置用户密码。	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） — 用户密码	暴力攻击防护 设备行为 （10 次不正确的密码尝试） 加密擦除闪存盘、密码、设置和数据	数据擦除和 设备重置？ 是

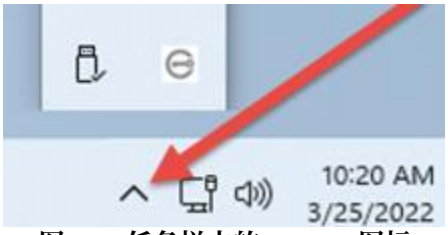
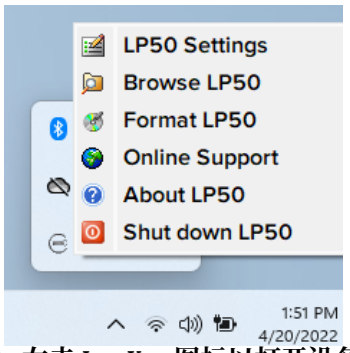
* 一旦您成功完成设备的身份验证，则会针对所用的登录方法重置失败登录计数器。加密擦除会删除所有密码、加密密钥和数据 – 您的数据会永久丢失。

访问我的安全文件

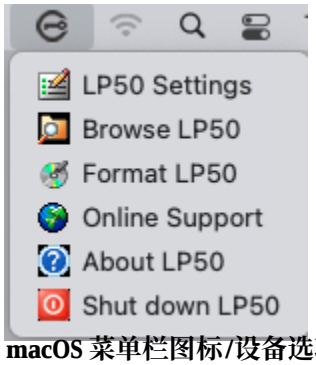
解锁闪存盘后，您可以访问自己的安全文件。当您在闪存盘上保存或打开文件时，会自动加密和解密文件。这项技术不仅让您可以像通常操作普通闪存盘一样方便，还提供了“始终在线”的强大安全性。
提示：通过直接单击 Windows 任务栏中的 **IronKey** 图标并单击“ 浏览 LP50 ”**(Browse LP50)**，您也可以访问自己的文件 *（图 7.2）*。

设备选项 - （Windows 环境）

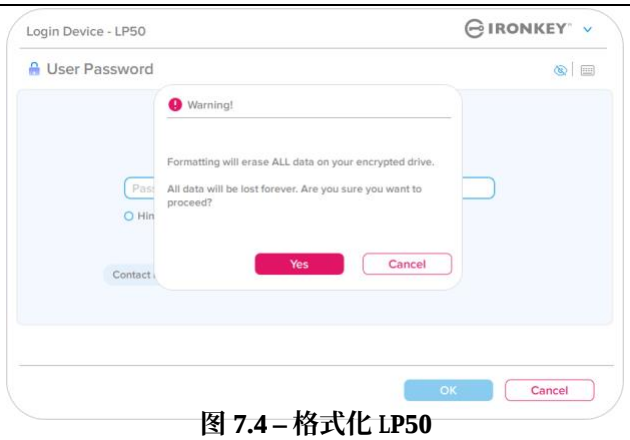
登录设备后，IronKey 图标会出现在 Window 右下角。右击 IronKey 图标，会打开可用闪存盘选项的选择菜单（*图 6.2*）。关于这些设备选项的详情，可在本手册第 19-23 页找到。

• 登录设备后，IronKey 图标会出现在 Window 右下角。 *（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）

• 登录设备后，IronKey LP50 图标会出现在 macOS 菜单中（如*图 7.3* 所示），打开后显示可用的设备选项。 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

LP50 设置：	• 更改登录密码、联系信息和其他设置。（有关设备设置的更多详情，请参见本手册“LP50 设置”部分。）
浏览 LP50 (Browse LP50)：	• 让您可以查看安全文件。
格式化 LP50 (Format LP50)： **允许您格式化安全数据分区。** **（警告：所有数据都将被抹除。）** ***（图 6.1）*** **注意：格式化需要密码身份认证。**	 **图 7.4 – 格式化 LP50**
在线支持 (Online Support)：	• 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 LP50 (About LP50)： **提供关于 LP50 的具体详情，包括应用程序、固件和序列号信息（图 6.2）** **注意：闪存盘的唯一序列号位于“Information”（信息）列下**	 **图 7.5 – 关于 LP50（About LP50）**
关闭 LP50 (Shut down LP50)：	• 正确关闭 LP50，允许您将其从系统上安全删除。

LP50 设置

管理员设置

管理员登录支持访问以下设备设置：

- 密码 (Password)：允许您更改您自己的管理员密码和/或提示（图 8.1）
- 联系信息 (Contact Info)：允许您添加/查看/更改联系信息（图 8.2）
- 语言 (Language)：让您可以更改当前语言选择（图 8.3）
- 管理员选项 (Admin Options)：让您可以访问额外的功能，例如：
    - 更改用户密码（*图 8.4*）

注意：有关管理员选项的更多详情，请参见第 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

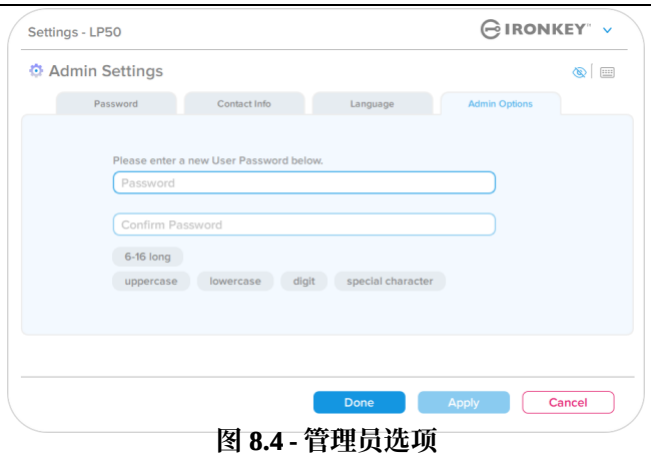


图 8.4 - 管理员选项

LP50 设置

用户设置：管理员已启用

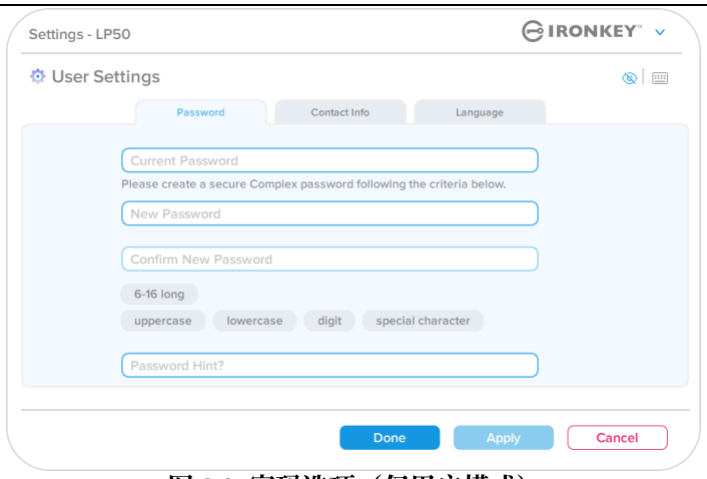
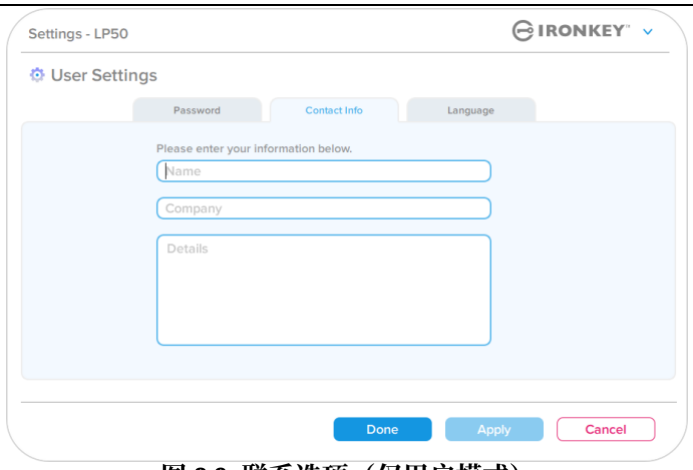
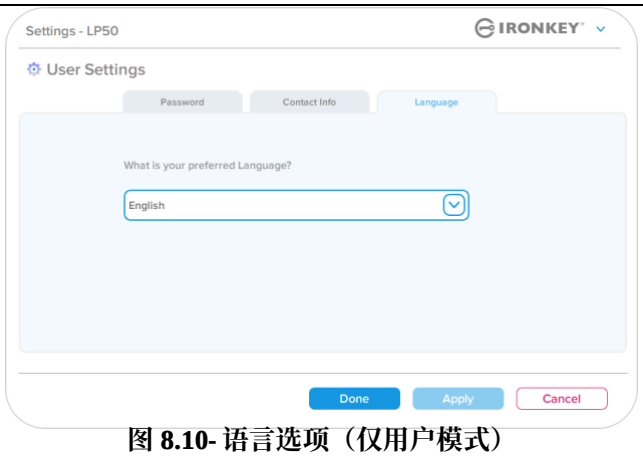
用户登录仅能访问以下设置：

密码 (Password)： **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 (Contact Info)： **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 (Language)： **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。

LP50 设置

如第 12 页所述，如果在初始化 LP50 时不启用“管理员密码和用户密码”，会将闪存盘配置为“单密码、单用户”设置。该配置无法访问任何管理员选项或功能。该配置可以访问以下 LP50 设置：

密码 (Password)： 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 (Contact Info)： 允许您添加/查看/更改联系信息。 *（图 8.9）*	 **图 8.9- 联系选项（仅用户模式）**
语言 (Language)： 让您可以更改当前语言选择。 *（图 8.10）*	 **图 8.10- 语言选项（仅用户模式）**

LP50 设置

更改和保存设置

- **每当 LP50 设置中的设置（例如联系信息、语言、密码更改、管理员选项）更改时，闪存盘都会提示输入您的密码以接受并应用更改。*（参见图 8.11）***

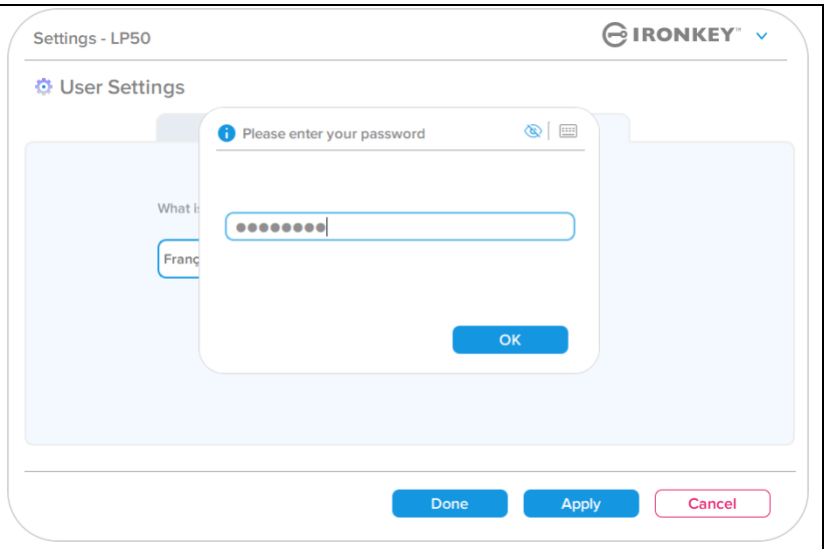


图 8.11 - 用来保存 LP50 更改的“密码提示”屏幕

注意：如果您处于上面的“密码提示”屏幕并希望取消或修改所作更改，只需确保密码字段为空并单击“确定”(OK)。这将关闭“请输入您的密码”(Please enter your password) 框，并返回到 LP50 设置菜单。

管理员功能

用于重置用户密码的选项

管理员配置包含一项有用功能，支持您在忘记用户密码时进行安全重置。以下是用户密码重置功能，有助于重置用户密码：

用户密码重置： **在“管理员选”(Admin Options) 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：密码要求条件默认为在初始化流程中设定的原始条件（复杂或口令选项）。**	 **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

LP50 包含一项安全功能，当达到最大连续登录失败尝试次数（简称 *MaxNoA*）时，会阻止未经授权的人员访问数据分区。默认的“出厂”配置为每种登录方式（管理员/用户）预先配置的值为 10（尝试次数）。

“锁定”计数器记录每次的失败登录，并且在满足下列两种条件之一时重置：

1. 在达到 MaxNoA 前成功登录

2. 达到 MaxNoA 并执行设备锁定或设备格式化，具体取决于闪存盘是如何配置的。

• 如果输入了错误的密码，将在密码输入字段下方出现一条错误消息，说明登录失败。*（图 10.1）*	 **图 10.1 - 密码错误消息**
• 如果出现第 7 次失败尝试，您将看到另外一条错误消息，提醒您在达到 MaxNoA（默认被设置为 10）之前还可以尝试 3 次。*（图 10.2）*	 **图 10.2- 第 7 次不正确的密码输入**

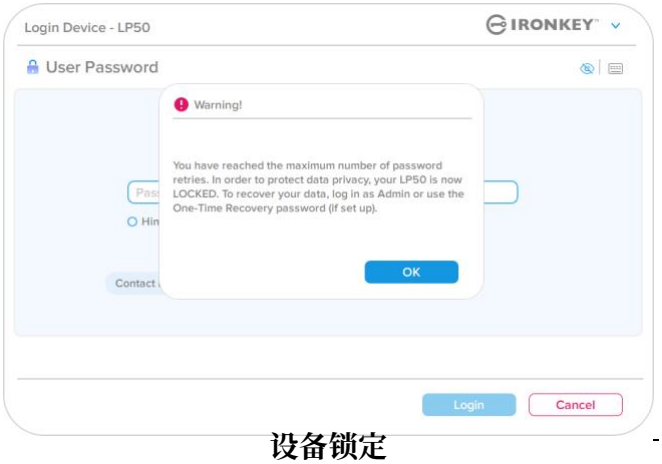
帮助和故障排除

设备锁定

重要事项：第 10 次即最后一次失败的登录尝试后，根据设备的设置和使用的登录方法（管理员、用户），设备要么会锁定并要求您使用其他方法（若适用）进行登录，要么进行设备重置，这会格式化数据，闪存盘中的所有数据会永久丢失。本用户指南第 18 页也介绍了各种行为。

下面的图 10.3- 10.6 展示了各种登录密码方式在第 10 次即最后一次登录失败后的行为：

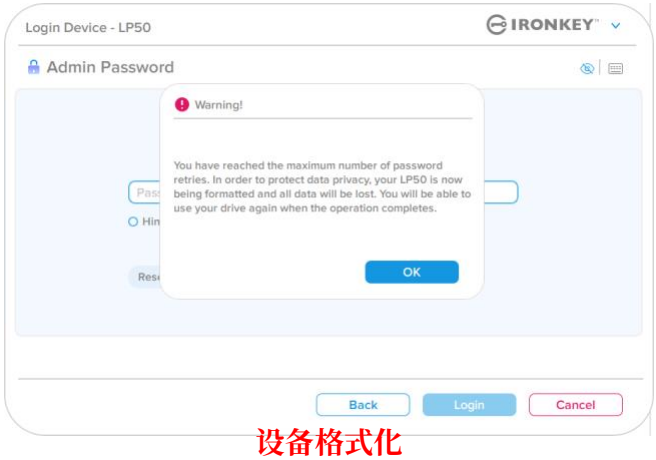
用户密码：（管理员/用户已启用）



设备锁定

（图 10.3）

管理员密码（管理员/用户已启用）

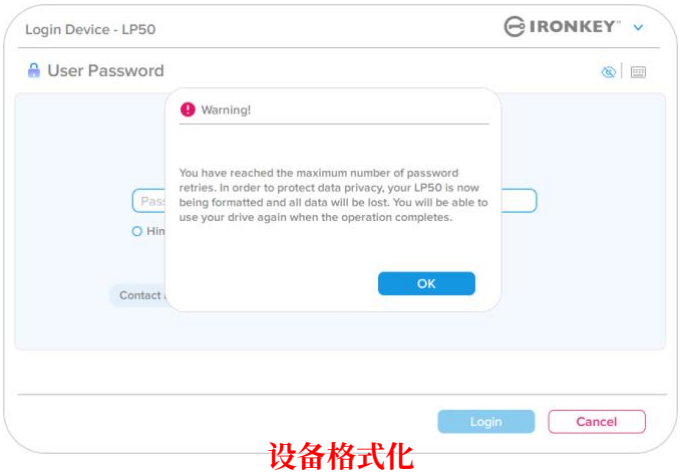


设备格式化

（图 10.4）

- **这些安全举措可以限制他人（不知道您的密码）不限次数地尝试登录来访问您的敏感数据（又称暴力攻击）。如果您是 LP50 的所有者，但忘记了密码，那么相同的安全措施将同样会生效，包括设备格式化。有关该功能的更多信息，请参见第 25 页 *“重置密码”*。**

用户密码（管理员未启用）



设备格式化

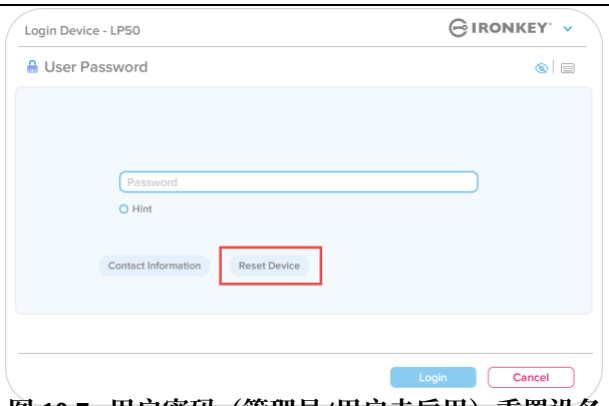
（图 10.5）

注意：*设备格式化将擦除 LP50 安全数据分区中保存的所有信息。

帮助和故障排除

重置设备

如果忘记密码或需要重置设备，可以单击“重置设备”(Reset Device) 按钮。根据 LP50 启动程序执行时对闪存盘的设置方式，该按钮可能出现在两个地方中的一个（在启用管理员/用户时位于“管理员登录密码”(Admin Login Password) 菜单中，在未启用管理员/用户模式时则位于“用户密码”(User Password) 登录菜单中。）*（参见图 10.7 和 10.8）*

• 您可以通过这一选项新建密码，但是为了保护您数据的隐私，LP50 将被格式化。这意味着在这个过程中所有数据会被擦除。*	 图 10.6 - 管理员密码：“重置设备”按钮
• 注意：注意：单击“重置设备”*(Reset Device)* 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“确定”*(OK)* 以确认，也可以 2) 单击“取消”(Cancel) 以返回登录窗口。*（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“初始化”(Initialize) 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（复杂或口令）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

帮助和故障排除

驱动器号冲突：Windows 操作系统

- **正如本手册“*系统要求*”部分（第 3 页）所述，LP50 需要使用 2 个连续的驱动器号（在驱动器号分配“空缺”之前出现的最后一个物理磁盘之后）*（参见图 10.9）*。这不适用于网络共享，因为它们特定于用户配置文件而不是系统硬件配置文件本身，因此对操作系统而言看起来是可用的。**

- **这意味着，Windows 可能会给 LP50 分配已经被网络共享或者被通用命名约定 (UNC) 路径使用的驱动器号，从而导致驱动器号冲突。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号分配（需要管理员权限）。**

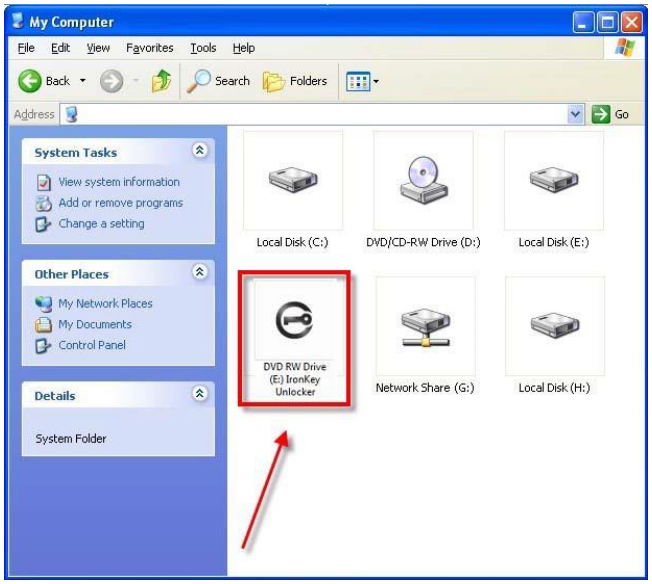


图 10.9 - 驱动器号示例

在本例中*（图 10.9）*，LP50 使用驱动器 F:，这是驱动器 E：之后第一个可供使用的驱动器号（E：是驱动器号空缺之前的最后一个物理磁盘。）由于驱动器号 G:是一个网络共享而不是硬件配置文件的一部分，所以 LP50 可能会尝试将它用作其第二个驱动器号，从而导致冲突。

如果您的系统中没有网络共享，但 LP50 仍然不能加载，那可能是读卡器、可移动磁盘或者其他以前安装的设备正在占用驱动器号分配，并仍然导致冲突。

请注意，驱动器号管理（或 DLM）在 Windows 8.1、10 和 11 中已大大改善，因此您可能不会遇到此问题，但是如果您无法解决冲突，请联系金士顿技术支持部门或访问 Kingston.com/support，获取进一步的协助。

IRONKEY™ Locker+ 50 (LP50)
加密 USB 3.2 Gen 1 隨身碟

使用者指南

目錄

圖 1：IronKey LP50

簡介

Kingston IronKey Locker+ 50 USB 隨身碟採用 XTS 區塊加密模式的 AES 硬體式加密，提供標準的安全性，並採用數位簽章韌體和暴力密碼攻擊法來防止 BadUSB 的攻擊。LP50 亦符合 TAA 規範。

LP50 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數字 PIN、句子、單詞列表，甚至是 10 到 64 個字元長度的歌詞。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，可以點擊「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 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。LP50 亦可選擇 ClevX® 的 USBtoCloud 進行備份，並透過 Google Drive™、OneDrive (Microsoft®)、Amazon Cloud Drive、Dropbox ™ 或 Box 等個人雲端儲存服務存取裝置 上的資料。任何人都能輕易設定和使用 LP50，無需額外安裝任何應用程式。所有需要的軟體和安全保護皆已內建其中。適用於 Windows® 和 macOS®，方便使用者從多個系統中存取檔案。

LP50 享有 5 年有限產品保固及免費技術支援服務。

IronKey Locker+ 50 特色

- 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
- 多密碼選項
- 複雜或密碼短語模式
- 按下眼睛按鈕即可顯示輸入的密碼，藉此減少失敗的登入嘗試
- 虛擬鍵盤可協助防範鍵盤記錄程式和螢幕記錄程式
- Windows 或 macOS 相容 (詳情請查詢產品資料表)

關於本使用手冊 (09242024) IronKey Locker+ 50 (LP50) 使用手冊。

系統要求

電腦平台 • Intel 和 AMD • 15 MB 可用硬碟空間 • 可用的 USB 2.0 - 3.2 連接埠 • 最後一個實體磁碟後的兩個連續磁碟機代號* ***注意：**請參閱'第 32 頁「磁碟機代號衝突」。	**PC 作業系統支援** • Windows 11 • Windows 10
Mac 平台 • Intel 和 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 12.x – 15.x

注意：啟用後，每個裝置都含 5 年免費 USB-to-Cloud 訂閱。可在訂閱有效期間內向 ClevX 續購。

建議

為確保提供充分電力給 LP50 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 LP50 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 LP50 預設格式化為 FAT32 檔案系統。適用於 Windows 和 macOS 系統。但是，可能還有一些其他選項可用於手動格式化硬碟，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 LP50 之前，在您的電腦上執行病毒掃描
- 不使用時將裝置鎖定
- 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將其格式化，資料會被刪除
- 切勿將您的裝置密碼告訴任何人 Never share your device password with anyone

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：您的隨身碟如果有任何更新，請務必升級至最新版本。我們不支援將您的硬碟降級為較舊的軟體版本，這可能會導致儲存資料丟失，或者損害硬碟的其他功能。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 LP50 具備強大的安全對策。其中包括針對暴力密碼破解的保護，該項防護將限制每個密碼僅能嘗試輸入 10 次，藉此阻止攻擊者猜測密碼。當達到嘗試上限時，LP50 將自動清除加密資料 – 格式化並恢復到出廠設定。

多密碼

LP50 主要功能為支援多密碼，以免忘記一個或多個密碼時資料遺失。啟用所有密碼選項後，LP50 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。

LP50 允許您選取兩個主要密碼 – 管理員密碼 (Admin password) 和使用者密碼。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，但管理員的存取權限比使用者更多。如果您忘記這兩個密碼中的其中之一，則可以使用另一個密碼來存取並取回資料。並將硬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。LP50 可以重設並重複使用，但先前儲存的資料將被永久清除。

密碼模式

LP50 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

LP50 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 LP50 隨身碟一樣，密碼短語可以與隨身碟選擇的語言相符。這能讓您使用多個單字、一個短語、歌曲中歌詞或一句詩歌等，強大的複雜密碼是攻擊者最難破解的密碼類型之一，而且使用者較於好記。

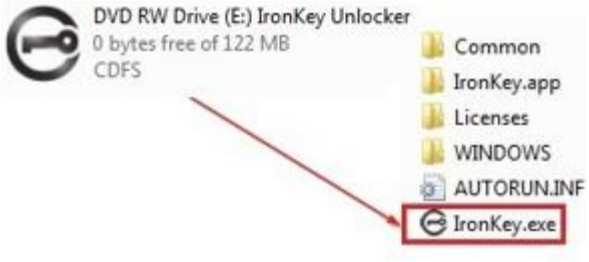
設定我的裝置

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。避免將隨身碟連接到具有 USB 連接埠的任何周邊裝置，例如鍵盤或 USB 供電的集線器。裝備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)

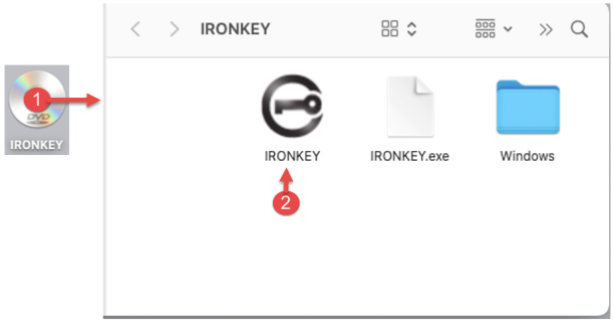
將 IronKey 加密 USB 隨身碟插入筆記型電腦或桌上型電腦上的可用 USB 連接埠，然後等待 Windows 偵測。

• Windows 8.1/10/11 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備而變動。右圖中，磁碟機代號為 (E:)。	 **圖 3.2 – File Explorer Window/IronKey.exe**

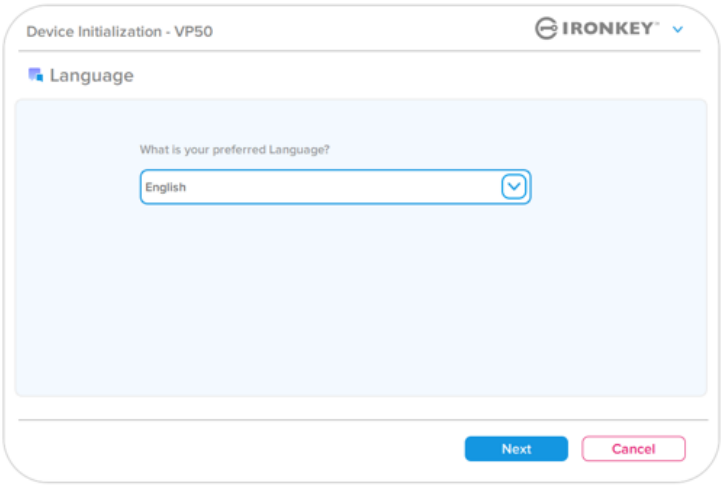
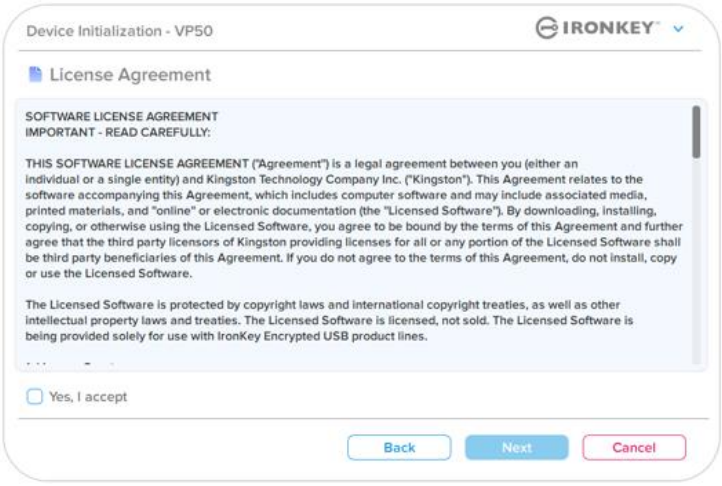
裝置存取 (macOS 環境)

將 LP50 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 盤標」。*(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。接著初始化流程就會啟動。	 **圖 3.3 - IKLP 盤標**

裝置初始化 (Windows 和 macOS 環境)

語言和 EULA

圖 4.1 - 從下拉式選單中選擇語言偏好，然後按一下「下一步」**(Next)**。	 **圖 4.1 – 語言選項**
檢閱授權協議然後按一下「下一步」**(Next)**。 注意：您必須先接受授權合約才能繼續，否則「下一步」**(Next)** 按鈕將呈現在停用狀態。(圖 4.2)	 **圖 4.2 – 授權合約**

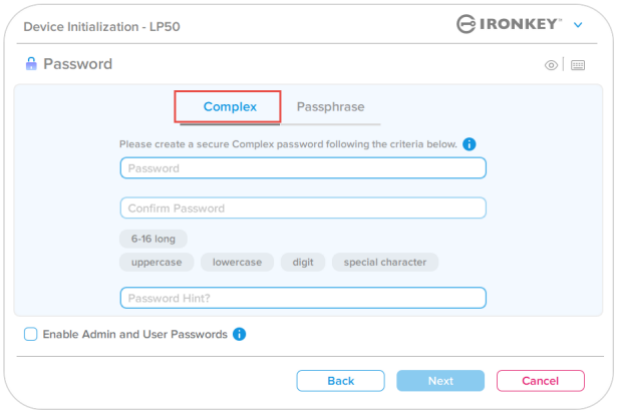
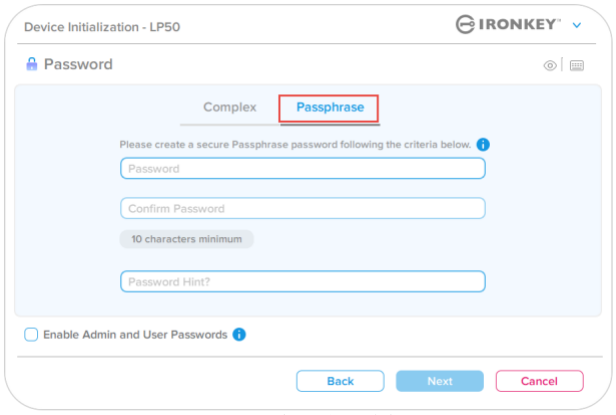
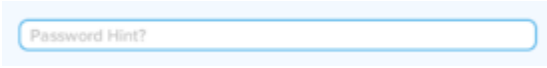
裝置初始化

密碼選擇

在密碼提示畫面上，可使用複雜密碼或密碼短語密碼模式建立密碼，以保護 LP50 中的資料 *(圖 4.3-4.4)*。此外，還可以在此螢幕上啟用多密碼管理員/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程序：

複雜 (Complex) 密碼 • 必須包含 6 個以上的字元 (最多 16 個字元)。 • 必須包含下列三 (3) 種字元： ○ 大寫 ○ 小寫 ○ 數字 ○ 特殊字元 (!、$、& 等) Upper Case	 **圖 4.3 - 複雜密碼**
短語 (Passphrase) 密碼 • 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**
密碼提示 (Password Hint) (選用) 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」將會顯示綠色。*(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)*

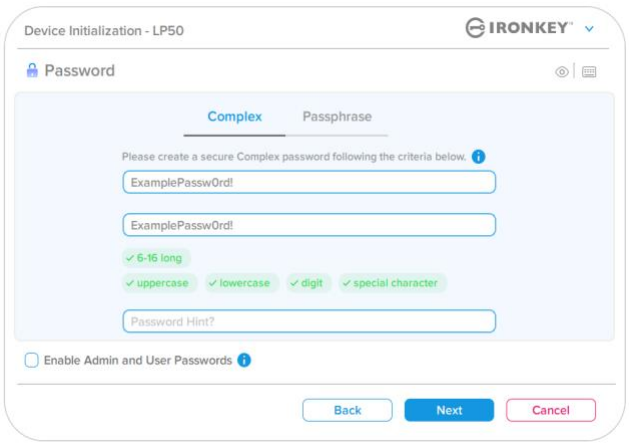


圖 4.6a - 複雜密碼條件符合

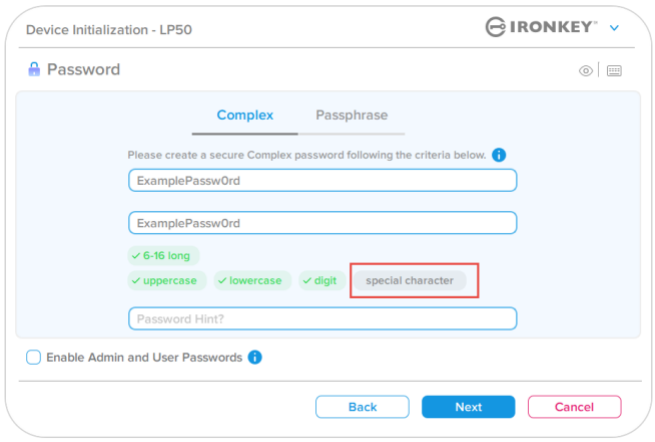


圖 4.6b - 複雜密碼條件選擇性

如果是**無效的**密碼，「密碼條件方塊」將會顯示紅色，同時將會停用「**Next**」(下一步) 按鈕，直到符合最低限度要求為止。

此情況適用於複雜密碼與密碼短語密碼。

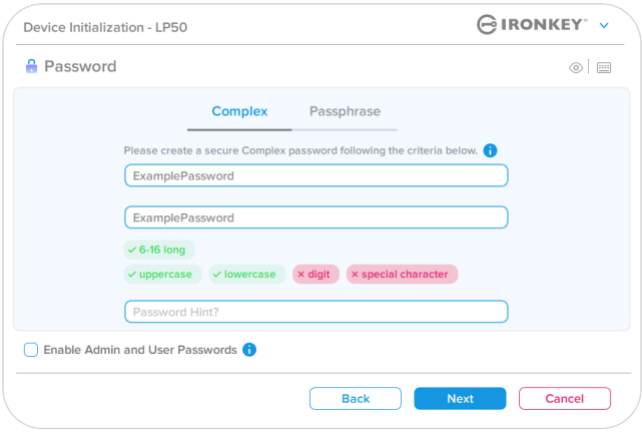


圖 4.7 - 密碼條件不符

裝置初始化

虛擬鍵盤

LP50 具有可用於鍵盤記錄程式保護的虛擬鍵盤。

- 若要使用**虛擬鍵盤**，請在**裝置初始化 (Device Initialization)** 畫面的右上角找到鍵盤按鈕並點選。

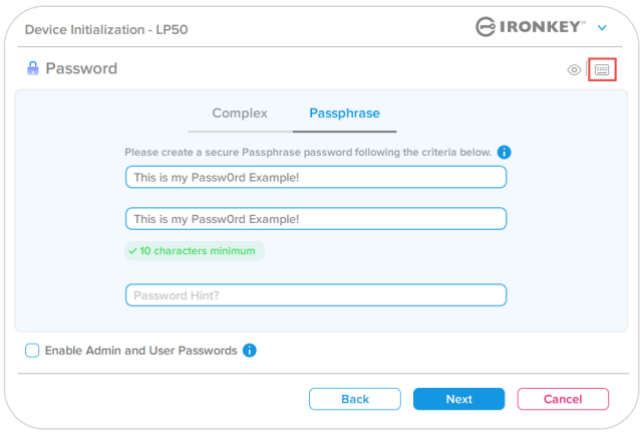


圖 4.8 - 啟用虛擬鍵盤

- 出現虛擬鍵盤後，您還可以啟用**螢幕記錄程式保護 (Screenlogger Protection)**。在使用此功能時，所有按鍵將短暫變為空白。這是可預期的行為，因為它可避免螢幕記錄程式擷取您所點按的內容。
- 若要加強此功能，您還可以選擇鍵盤右下角的**隨機化**，讓虛擬鍵盤隨機化。隨機排列可依隨機順序排列鍵盤位置。

圖 4.9 - 螢幕記錄程式保護/隨機

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。

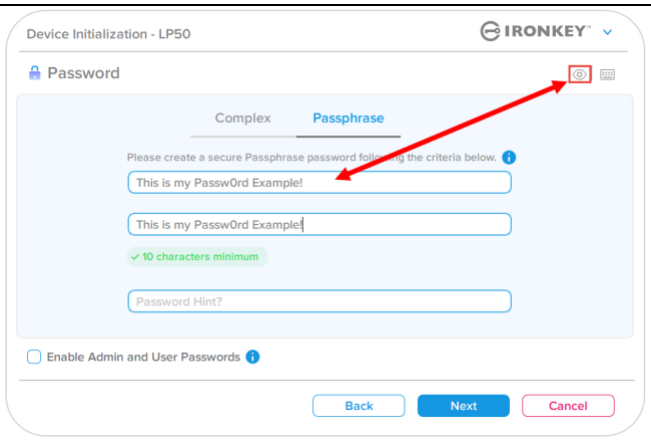


圖 4.10 - 切換「隱藏」的密碼

若要**顯示**隱藏的密碼，請按一下藍色圖示。

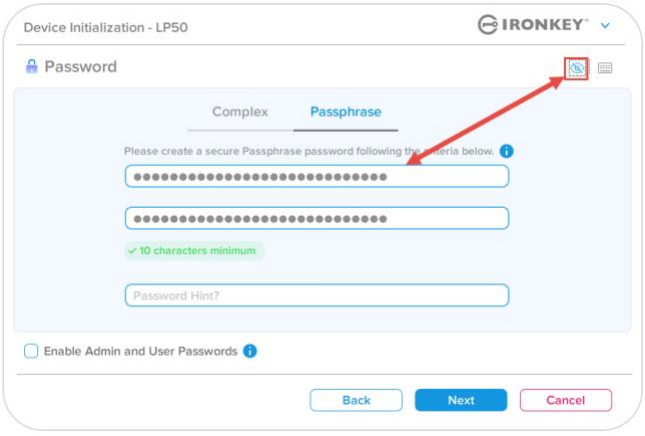


圖 4.11 - 切換「顯示」的密碼

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，讓管理員角色管理兩個帳戶。選擇**「啟用管理員和使用者密碼」**，即允許在忘記其中一個密碼的情況下，使用另一個密碼存取隨身碟。

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 28 頁。

- 如要啟用**管理員和使用者密碼**，請按一下**「啟用管理員和使用者密碼」(Enable Admin and User Passwords)**旁邊的方塊，然後選擇有效的密碼，再選取**「下一步」(Next)**。*(圖 4.12)*

- 若**已啟用**本功能，則在此畫面中選擇的密碼就會是**管理員密碼**。按一下**「下一步」(Next)** 即可前往至**「使用者密碼」**畫面，可在此畫面中選擇使用者的密碼。

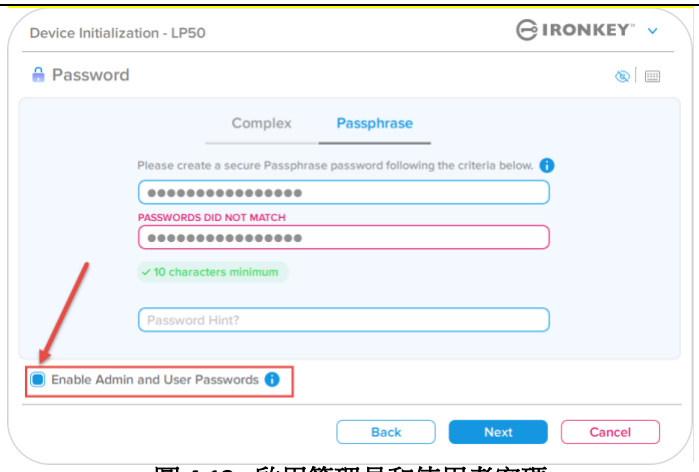


圖 4.12 - 啟用管理員和使用者密碼

注意：啟用管理員和使用者密碼為選擇性質。

如果已經設定隨身碟但是未啟用此功能 (方塊取消核取)，則會將隨身碟設定為**「Single User, Single Password」(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，此設定也被稱為**使用者模式**。

若要繼續**「Single User, Single password」(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 (User Password)** *(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**意指為**「管理員角色」**。

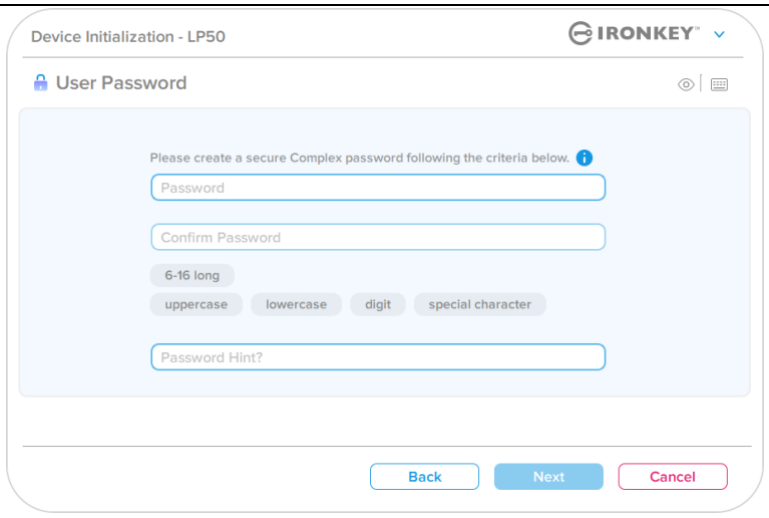


圖 4.13 - 使用者密碼 (管理員與使用者已啟用)

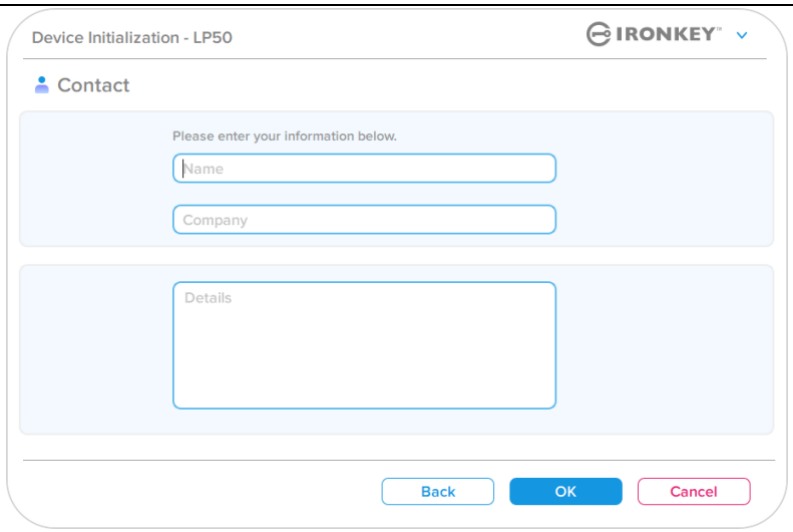
注意：選擇的「密碼選項」(複雜或密碼短語) 條件將會延續至使用者密碼，以及在設定隨身碟後需要進行的任何密碼重設。選擇的密碼選項僅可在完整裝置重設後方可變更。

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 *(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。但是這些欄位是選填性質的，如果需要可以留空。

「名稱」(Name) 欄位最多可包含 32 個字元，但不得包含實際密碼。 **「公司」(Company)** 欄位最多可包含 32 個字元，但不得包含實際密碼。 **「詳細資訊」(Details)** 欄位最多可包含 156 個字元，但不得包含**實際**密碼。	 **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變更。

USB ← → 雲端初始化 (Windows 環境)

在 Windows 中初始化裝置之後，USB-to-Cloud 應用程式將顯示在右側，如*圖 5.1* 所示。請先確定您的網際網路連線運作正常，然後再繼續。

- 若要繼續安裝，請按一下 clevX 視窗右下方的綠色「接受」(Accept) 按鈕。
- 若要拒絕安裝，請按一下 clevX 視窗左下方的紅色「拒絕」(Decline) 按鈕。
- (注意：如果您按下紅色的「Decline」(拒絕) 按鈕，USB-to-Cloud 功能將會取消安裝。同時會在資料分割區上建立名為「USBtoCloudInstallDeclined.txt」的文字檔案。此檔案的存在會導致以後應用程式無法提示您進行安裝。)

圖 5.1 - *USBtoCloud Windows EULA*

- 在初始化程序期間，如果跳出下列的 Windows 安全性警示視窗，請按一下「Allow access」(允許存取) 以繼續 (或是建立 Windows 防火牆封鎖例外)，以便讓 USB-to-Cloud 功能繼續安裝。

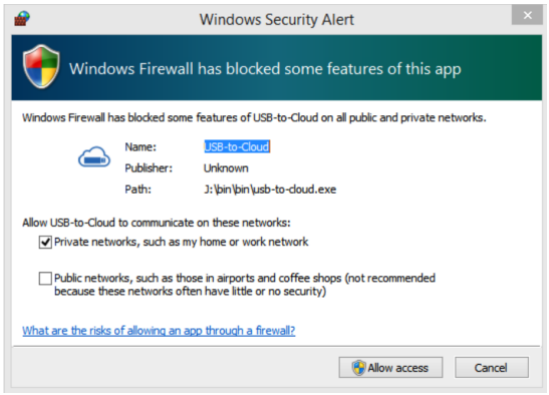


圖 5.2 – Windows 安全性警示

USB ← → 雲端初始化 (Windows 環境)

- 安裝完成後，您會看到應用程式方塊且有許多選項可供選擇 (用於同步 LP50 上的資料)。
- 選取您要作為備份應用程式的雲端選項並提供驗證所需的必要憑證。
- (注意：如果您目前沒有使用任何雲端選項所列出之帳戶，您需要先在您最愛的網際網路瀏覽器上建立一個帳戶，之後再完成此選項。)
- 選擇雲端選項並驗證到對應服務之後，USB-to-Cloud 程式會針對儲存在雲端的內容，來執行資料磁碟分區的初始對照。只要 USB-to-Cloud 服務是在「工作管理員」身份下執行，寫入到該磁碟分區的內容便會自動備份 (同步) 到雲端。

圖 5.3 - 雲端選項

USB ← → 雲端使用 (Windows 環境)

USB-to-Cloud 功能提供下列其他服務：

- 暫停備份 (暫停資料備份)。
- 還原 (將資料從雲端還原到裝置)。
- 設定 (資料備份的附加選項)。
- 退出 (退出 USB-to-Cloud 服務)。

在「設定」選單中，您可以：

- 變更目前備份使用的雲端服務應用程式。
- 變更目前使用的語言，
- 選擇要備份到雲端的檔案及/或資料夾。
- 檢查軟體更新。

(注意：如果您重設 (或格式化) LP50，裝置上的所有資料都會遺失。不過，儲存在雲端的資料仍會存在。)

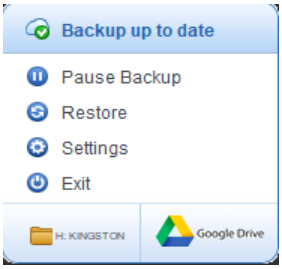


圖 5.4 - 服務

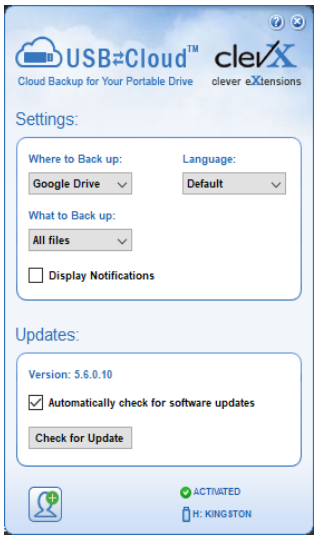


圖 5.5 - 設定

USB ← → 雲端初始化 (macOS 環境)

- 初始化裝置之後，USB-to-Cloud 功能將會顯示在右側，如**圖 5.6** 所示。請先確定您的網際網路連線運作正常，然後再繼續。
- 如要繼續安裝，請按一下 clevX 視窗右下方的綠色「接受」(Accept) 按鈕。

  (注意：macOS 12.x 會提示可存取可卸除式盤標上的檔案。選擇「OK」。) **(詳見圖 5.7)**
- 若要拒絕安裝，請按一下 clevX 視窗左下方的「拒絕」(Decline) 按鈕。

圖 5.6 - USBtoCloud macOS EULA

(注意：如按下「拒絕」(Decline) 按鈕，將會取消 USB-to-Cloud 安裝。同時會在資料分割區上建立名為「DontInstallUSBtoCloud」的文字檔案。此檔案的存在會導致以後應用程式無法提示您進行安裝。)

- 安裝完成後，您會看到應用程式方塊且有許多選項可供選擇 (用於同步 LP50 上的資料)。*(圖 5.8)*

圖 5.7 - macOS 存取

- 選取您要作為備份應用程式的雲端選項並提供驗證所需的必要憑證。

  (注意：如果您目前沒有使用任何雲端選項所列出之帳戶，您需要先在您最愛的網際網路瀏覽器上建立一個帳戶，之後再完成此選項。)
- 選擇雲端選項並驗證到對應服務之後，USB-to-Cloud 程式會針對儲存在雲端的內容，來執行資料磁碟分區的初始對照。只要 USB-to-Cloud 服務是在「工作管理員」身份下執行，寫入到該磁碟分區的內容便會自動備份 (同步) 到雲端。

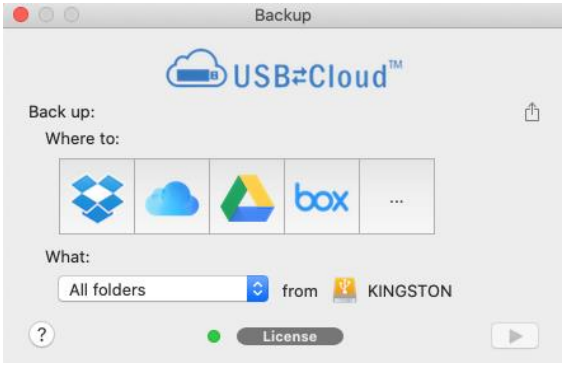
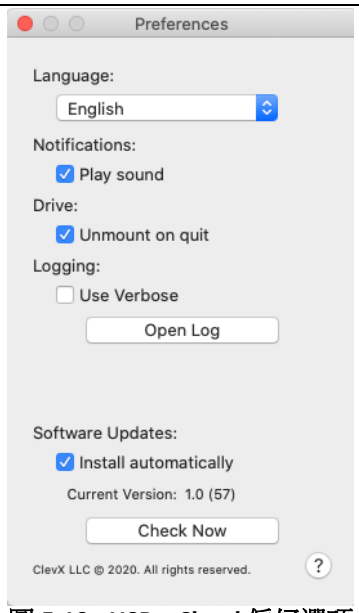


圖 5.8 - 雲端選項

USB ← → 雲端使用 (macOS 環境)

USB-to-Cloud 應用程式提供下列其他服務 *(圖 5.9)*： • 暫停備份 (暫停資料備份) • 還原 (將資料從雲端還原到裝置) • 備份 (開啟雲端選項) *參照圖 5.9* • 退出 (退出 USB-to-Cloud 服務)	 **圖 5.9 - 服務**
在「偏好選項」選單中，您可以： • 變更目前使用的語言 • 啟用/停用音效通知 • 退出應用程式時啟用/停用移除裝置 • 啟用/停用日誌記錄以進行故障排除 • 啟用/停用自動軟體更新，和立即檢查更新	 **圖 5.10 - USBtoCloud 偏好選項**

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 LP50 應用程式將啟動，並且先提示使用者密碼登入螢幕。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)*。藉由按一下「以管理員身分登入」(Login as Admin) 按鈕 (如下所示)，應用程式將繼續「管理員登入」選單，您可以在此處以管理員身分登入，存取管理員設定與功能 *(圖 6.2)*。

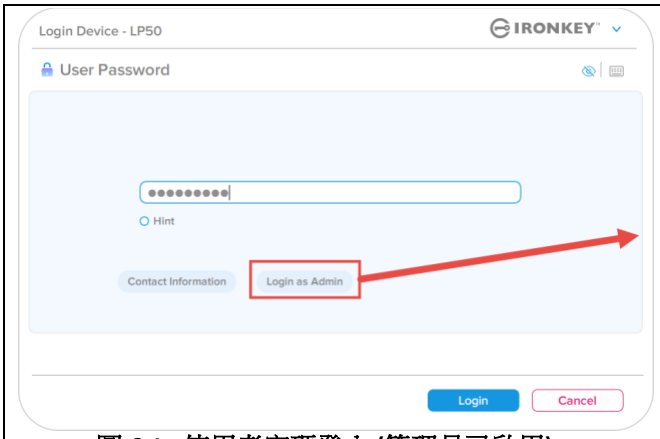


圖 6.1 - 使用者密碼登入 (管理員已啟用)

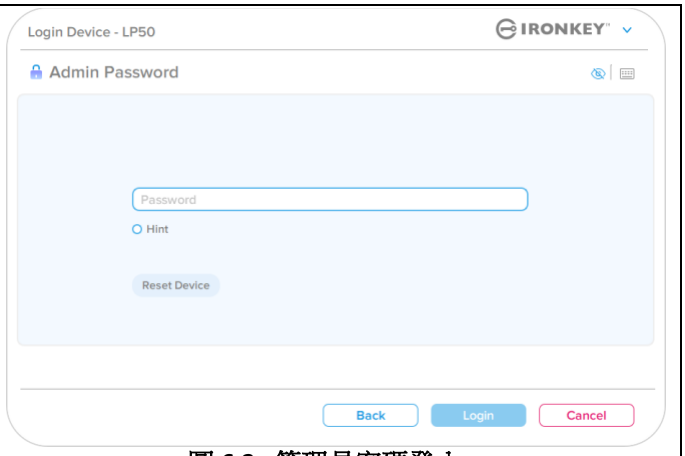


圖 6.2 - 管理員密碼登入

供僅使用者模式登入 (管理員未啟用)

正如先前**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，但還是可以在僅使用者 (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」(Reset Device)** 按鈕將隨身碟還原至初始化狀態，您可以在此狀態中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。**

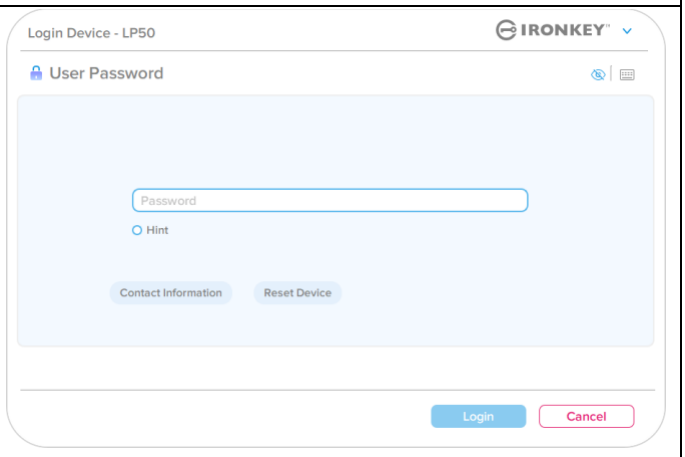


圖 6.3 - 使用者密碼登入 (管理員未啟用)

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，硬碟將會：

管理員/使用者啟用	**暴力破解保護 裝置行為 (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	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 裝置行為 (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「隨時在線」的安全性。
提示：您也可以在 Windows 工作列中的 **IronKey 圖示**上按一下右鍵，然後按一下**瀏覽** LP50 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 IronKey 圖示。在 IronKey 圖示上按一下右鍵，將會開啟選項選單，可選取可用的隨身碟選項 *(圖 6.2)*。

- 當您登入裝置時，視窗右上角會出現 IronKey 圖示。*(圖 7.1)*

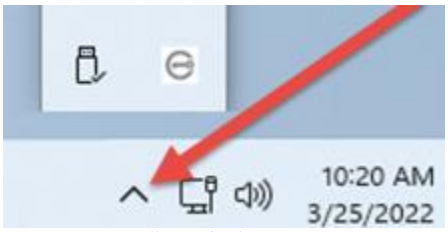


圖 7.1 工作列中的 IronKey 圖示

- 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。

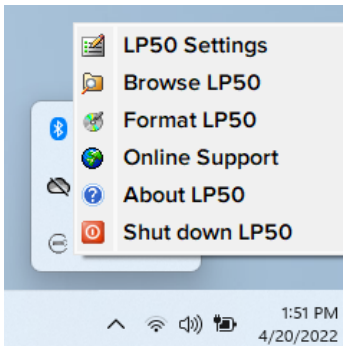


圖 7.2 在 IronKey 圖示按一下右鍵以顯示裝置選項

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 LP50」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。

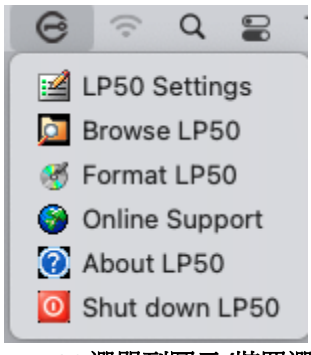
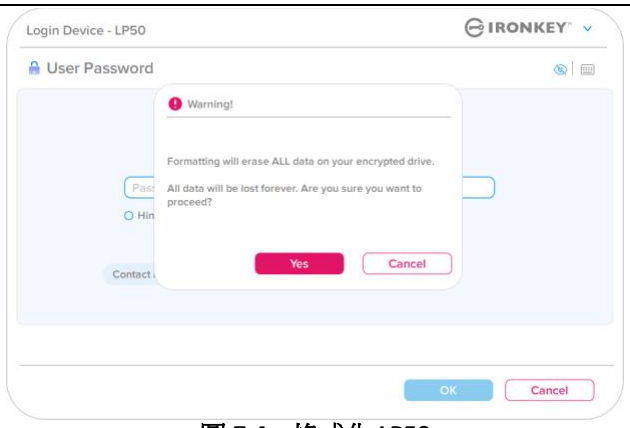
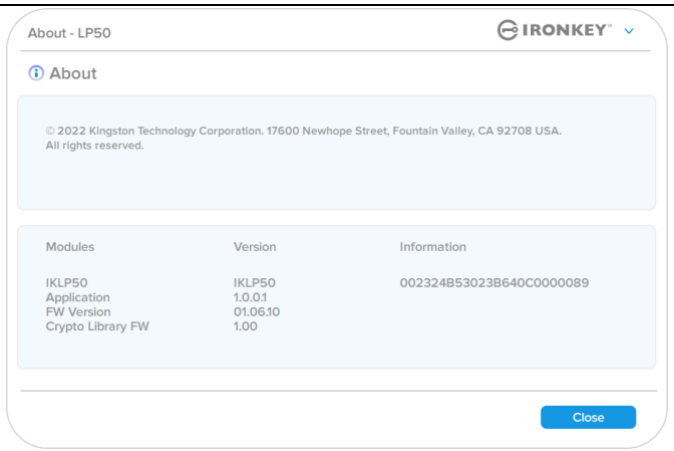


圖 7.3 - macOS 選單列圖示/裝置選項選單

裝置選項

LP50 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「LP50 設定」一節)。
瀏覽 LP50：	• 可讓您安全地檢視自己的檔案。
格式化 LP50： 可讓您格式化安全資料磁碟分割區。(警告：將會清除所有資料。) *(圖 6.1)* **注意：**密碼認證需要進行格式化。	 **圖 7.4 – 格式化 LP50**
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 LP50： 提供 LP50 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：**「資訊欄」下方可找到隨身碟的唯一序號	 **圖 7.5 - 關於 LP50**
將 LP50 關機：	• 正確關閉 LP50，如此可讓您從系統安全地將其移除。

LP50 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 (Password)**：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 (Contact Info)**：允許您您新增/查看/變更您的聯絡資訊 *(圖 8.2)*
- **語言 (Language)**：可讓您變更目前語言選項 *(圖 8.3)*
- **管理員選項 (Admin Options)**：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

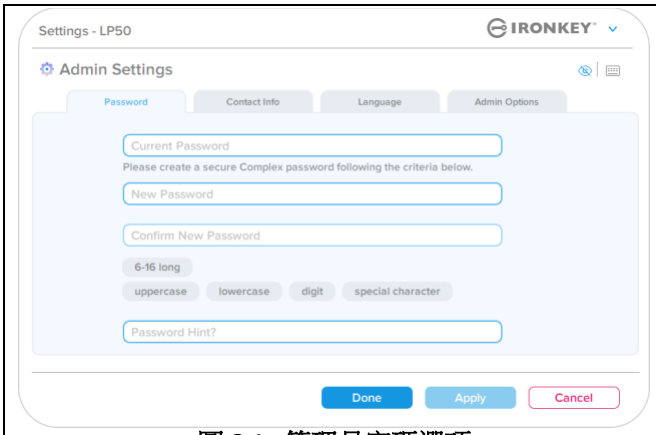


圖 8.1 - 管理員密碼選項

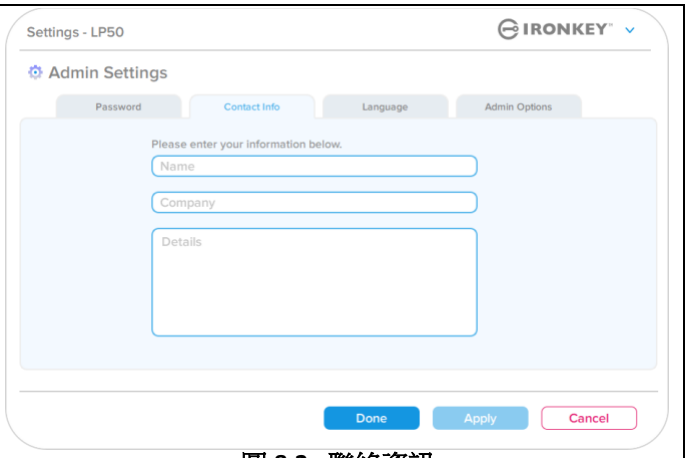


圖 8.2 - 聯絡資訊

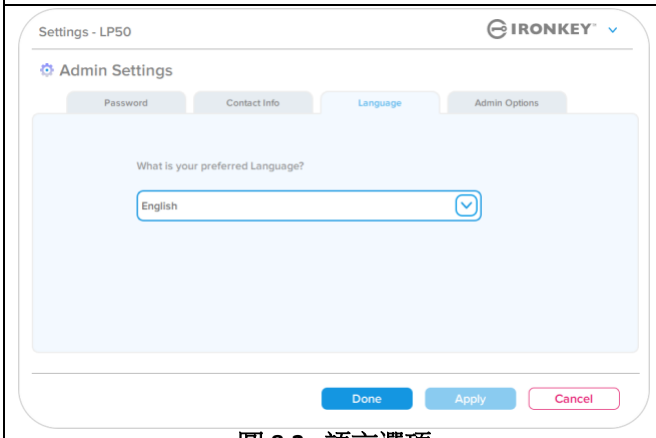


圖 8.3 - 語言選項

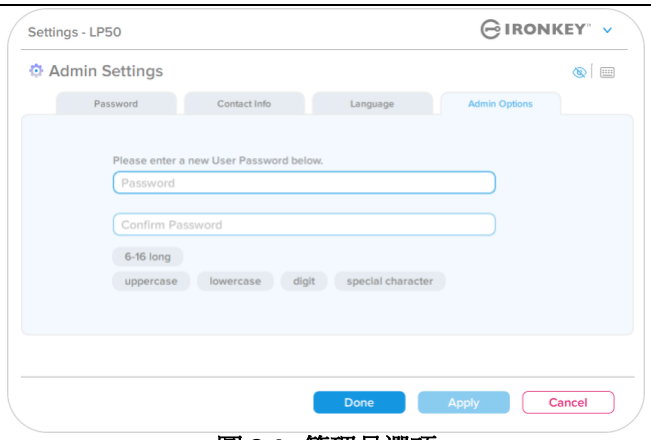


圖 8.4 - 管理員選項

LP50 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 (Password)：
允許您變更自己的使用者密碼和/或提示。*(圖 8.5)*

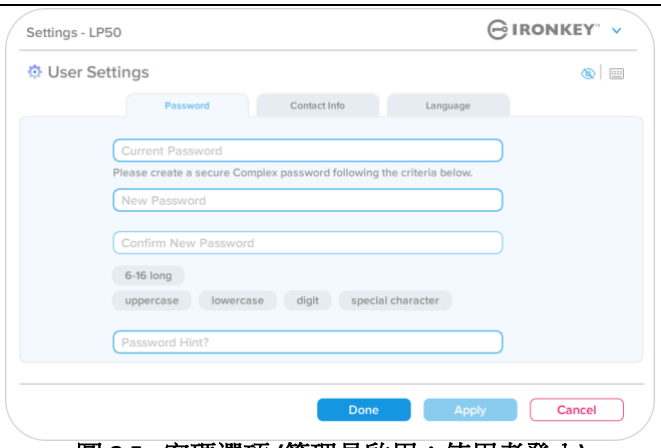


圖 8.5 - 密碼選項 (管理員啟用：使用者登入)

聯絡資訊 (Contact Info)：
允許 您新增/查看/變更您的聯絡資訊。*(圖 8.6)*

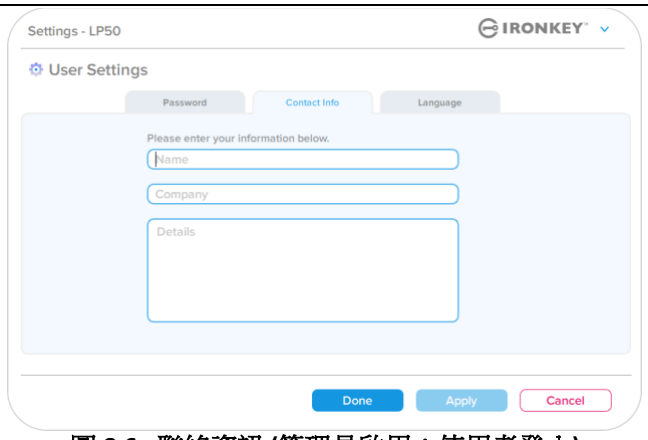


圖 8.6 - 聯絡資訊 (管理員啟用：使用者登入)

語言 (Language)：
可讓您變更目前語言選項。*(圖 8.7)*

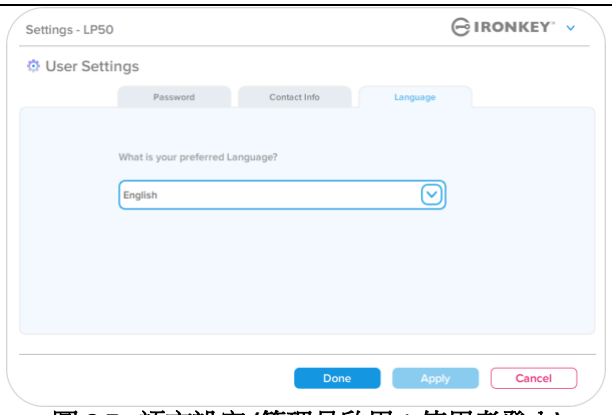


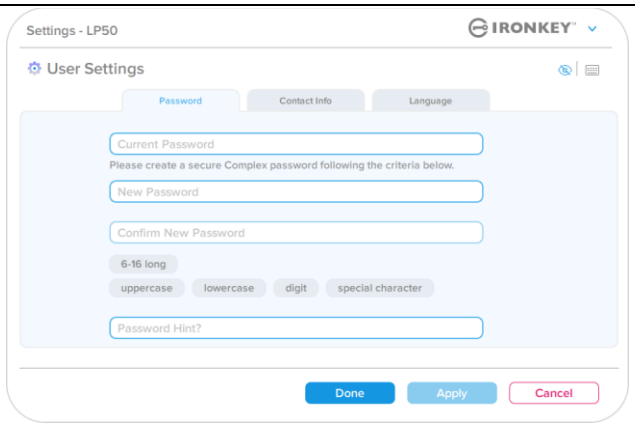
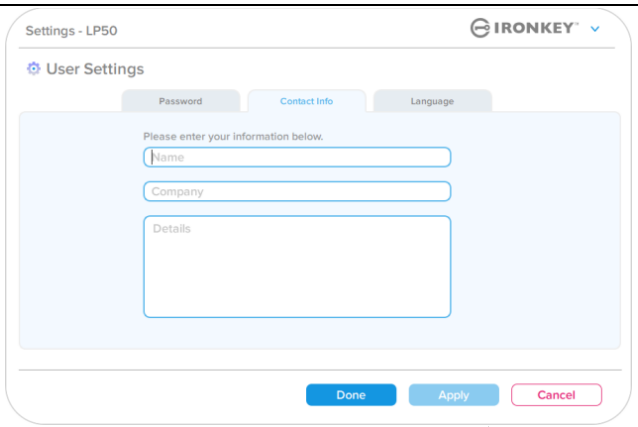
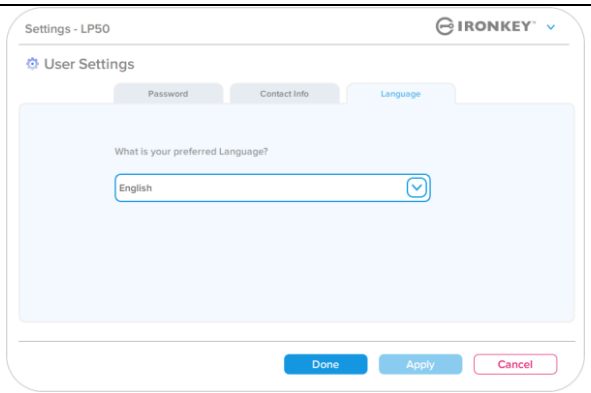
圖 8.7 - 語言設定 (管理員啟用：使用者登入)

注意：以使用者密碼登入時，無法存取管理員選項。

LP50 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 LP50 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 LP50 設定：

密碼 (Password)： 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 (僅使用者模式)**
聯絡資訊 (Contact Info)： 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 (僅使用者模式)**
語言 (Language)： 可讓您變更目前語言選項。*(圖 8.10)*	 **圖 8.10 - 語言設定 (僅使用者模式)**

LP50 設定

變更與儲存設定

- 每當 LP50 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)*

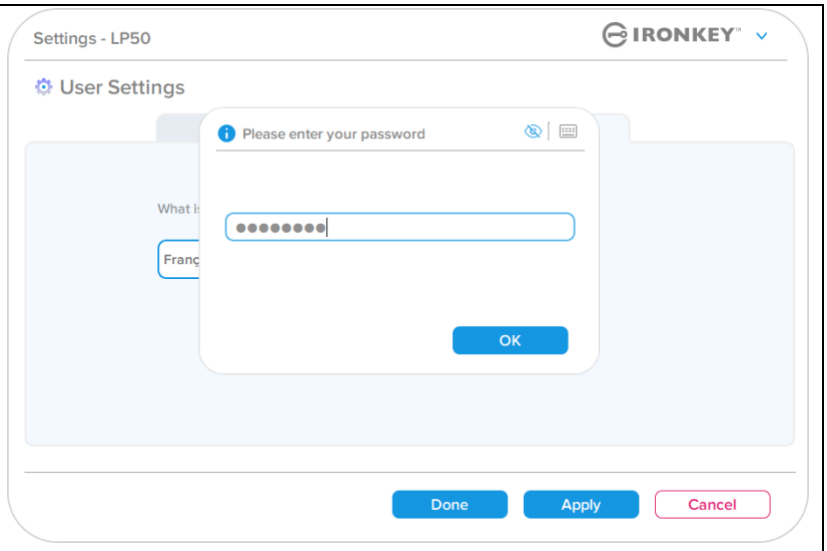


圖 8.11 - 儲存 LP50 設定變更的密碼提示畫面

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」(OK) 即可。這樣將會關閉「請輸入您的密碼」方塊並返回 LP50 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)。

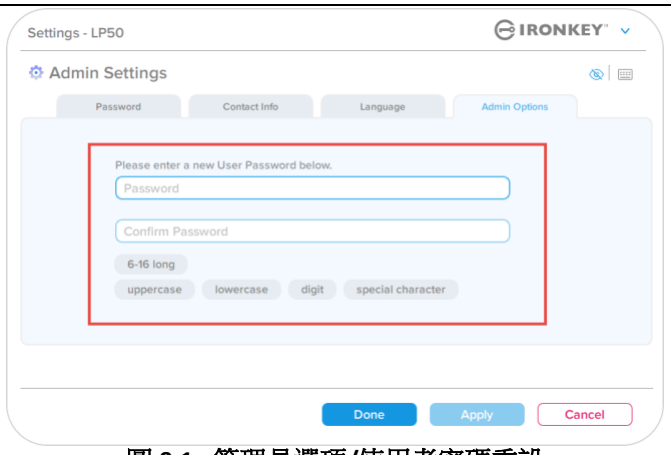


圖 9.1 - 管理員選項/使用者密碼重設

說明與疑難排解

裝置解鎖

LP50 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。預設的出廠設定已經在每個登入方法 (管理員/使用者) 中預先設定 數值 10 (嘗試次數)。

「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)*

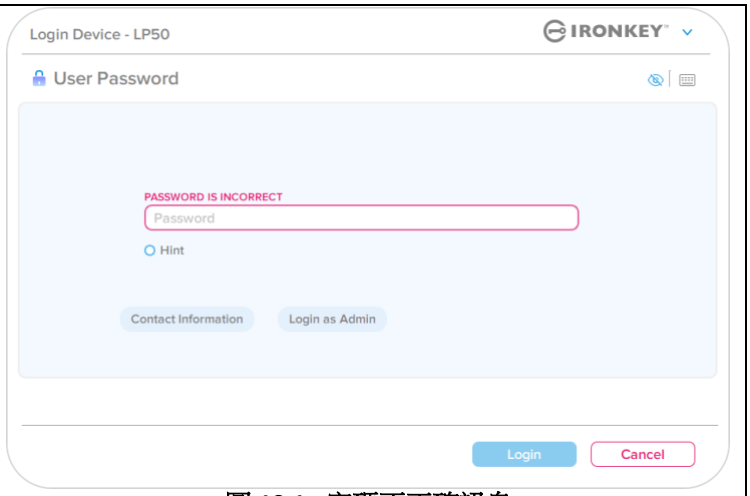


圖 10.1 - 密碼不正確訊息

- 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密碼輸入失敗上限 (預設值為 10)。*(圖 10.2)*

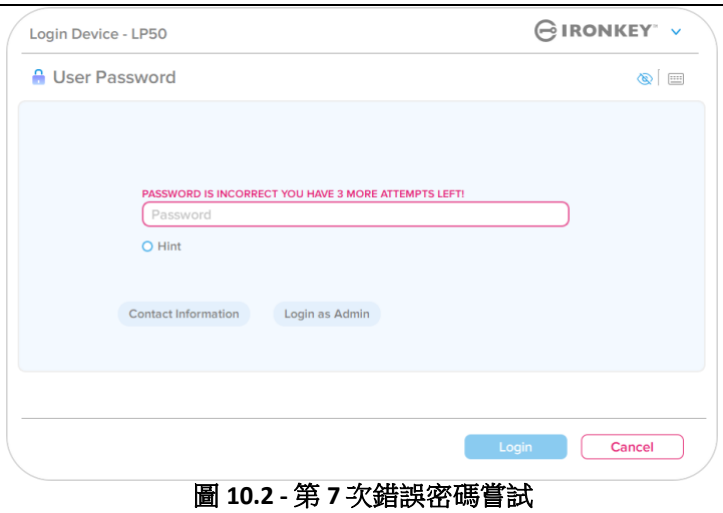


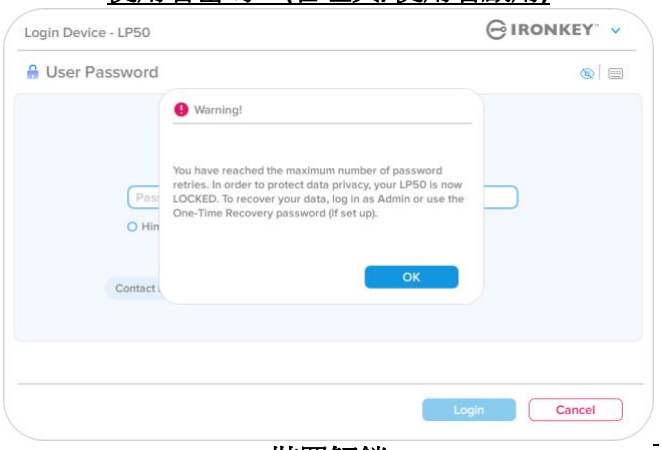
圖 10.2 - 第 7 次錯誤密碼嘗試

說明與疑難排解

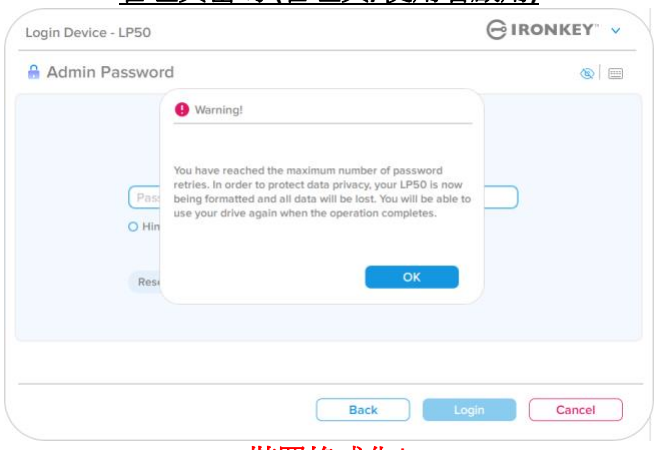
裝置解鎖

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 18 頁也提及了相關行為。

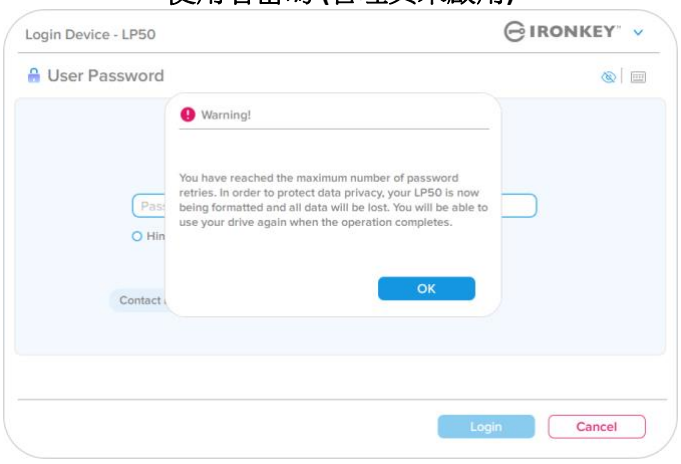
下面的圖 10.3- 10.6 展示每個登入密碼方法第 10 次以及最後一次失敗登入的畫面。

<table>
<tr>
<td><u>使用者密碼：(管理員/使用者啟用)</u>
 

<u>裝置解鎖</u>

(圖 10.3)</td>
<td><u>管理員密碼 (管理員/使用者啟用)</u>
 

裝置格式化*

(圖 10.4)</td>
</tr>
<tr>
<td>• 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 LP50 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 25 頁的「重設裝置」一節。</td>
<td>使用者密碼 (管理員未啟用)
 

裝置格式化

(圖 10.5)</td>
</tr>
</table>

**注意：裝置格式化將清除 LP50 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 LP50 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<u>未</u>啟用管理員/使用者，則出現在「使用者密碼」登入選單)。*(請參閱圖 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 LP50。這代表您的所有資料皆會在程序中被移除。*

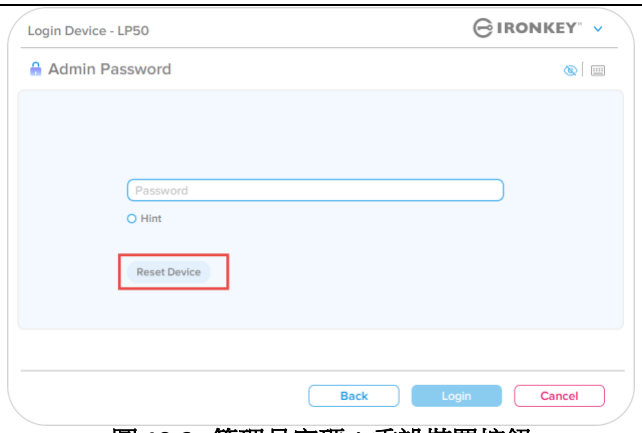


圖 10.6 - 管理員密碼：重設裝置按鈕

- **注意：**當您按一下「重設裝置」(Reset Device) 時，便會顯示一個訊息方塊，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)*

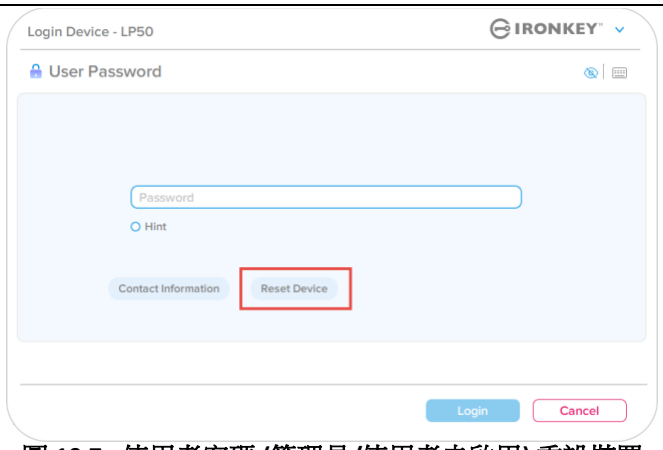


圖 10.7 - 使用者密碼 (管理員/使用者未啟用) 重設裝置

- 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 (複雜或密碼短語) 輸入新密碼。提示不是必填欄位，但如果您忘記密碼，提示欄位可幫助您提供有關密碼內容的線索。

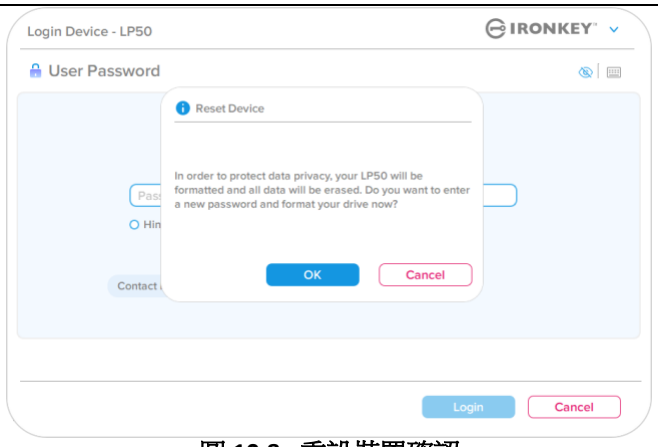


圖 10.8 - 重設裝置確認

說明與疑難排解

磁碟字母衝突：Windows 作業系統

- 如同本使用者手冊第 3 頁的「系統要求」一節所述，LP50 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 *(請參閱圖 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 LP50 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，導致磁碟機代號發生衝突。如果發生了這種情況，請向系統管理員或服務台支援部門洽詢，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)。

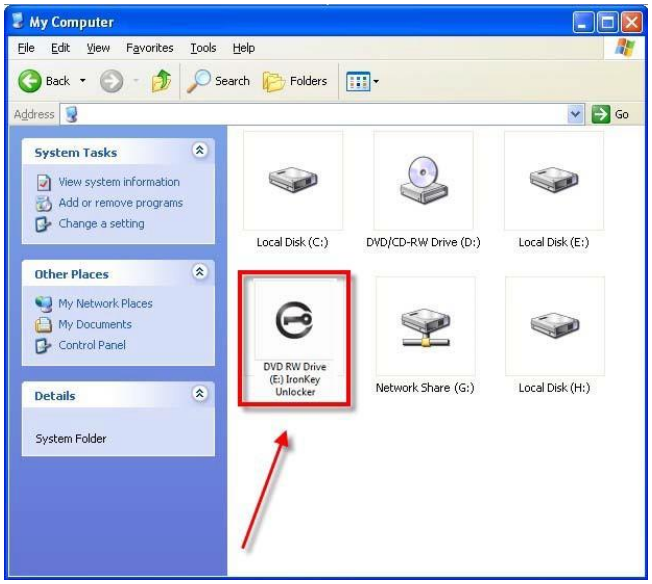


圖 10.9 - 磁碟機範例

在本例 (圖 10.9)中，LP50 使用磁碟機 F:，這是磁碟機 E:(即磁碟機代號字母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。由於字母 G：為網路共用磁碟機，而不是硬體設定檔的一部分，所以 LP50 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 LP50，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 8.1,10 及 11 已大幅改善了「磁碟機代號管理」(或 DLM) 的功能，因此您可能不會有這方面的問題，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，以獲得進一步的協助。