# User Manual

## IronKey Vault Privacy 50

Find the language and latest documentation here.

**IronKey Vault Privacy 50 Installation Guide**

 ..... 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™ Vault Privacy 50 (VP50)
# ENCRYPTED USB 3.2 Gen 1 FLASH DRIVE

*User Guide*

## Contents


Figure 1: IronKey VP50

## Introduction

The Kingston IronKey Vault Privacy 50 (VP50) is a premium USB drive that provides business-grade security with FIPS 197 certified AES 256-bit hardware-encryption in XTS mode including safeguards against BadUSB with digitally signed firmware, and against Brute Force password attacks. VP50 is also TAA compliant and assembled in the U.S.A. Because it is encrypted storage under the user's physical control, VP50 series is superior to using the internet and Cloud services to safeguard data.

VP50 supports Multi-Password (Admin, User, and One-Time Recovery) options with Complex or Passphrase modes. The Multi-Password option enhances the ability to recover access to the data if one of the passwords is forgotten. In addition to supporting traditional Complex passwords, the 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 and a One-Time Recovery password or reset the User password to restore data access.

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 or One-Time Recovery passwords upon 10 invalid passwords entered in a row, and crypto-erases the drive if the Admin password is entered incorrectly 10 times in a row.

To protect against potential malware on untrusted systems, both Admin and User can set Read-Only mode to write-protect the drive; additionally, the built-in virtual keyboard shields passwords from keyloggers or screenloggers.

FIPS 197 certified and TAA compliant, organizations can customize and configure VP50 series drives with a Product ID (PID) for integration with standard Endpoint Management software to meet corporate IT and cybersecurity requirement through Kingston's Customization Program.

Small and Medium Businesses can use the Admin role to locally manage their drives, e.g. use Admin to configure or reset employee User or One-Time Recovery passwords, recover data access on locked drives, and comply with laws and regulations when forensics are required.

VP50 is backed by a limited 5-year warranty with free Kingston technical support.

**IronKey Vault Privacy 50 Features**

- FIPS 197 certified with XTS-AES 256-bit 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
- Dual Read-Only (write protect) settings to protect drive contents against changes or malware
- Small and Medium businesses can locally manage drives using the Admin role
- Windows or macOS compatible (consult datasheet for details)

## About This Manual

This user manual covers the IronKey Vault Privacy 50 (VP50) and is based on the factory image with no implemented customizations.

## System Requirements

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

## Recommendations

To ensure there is ample power provided to the VP50 device, insert it directly into a USB port on your notebook or desktop, as seen in ***Figure 1.1***. Avoid connecting the VP50 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 VP50 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 VP50 on a target system
- When using the drive on a public, or unfamiliar system, you may wish to set the Read-Only mode on the device to help protect the drive from Malware
- Lock the device when not in use
- Eject the drive before unplugging it
- Never unplug the device when the LED is lit. This may damage the drive and require a reformat, which will erase your data
- Never share your device password with anyone

### Find the Latest Updates and Information

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

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

## Best Practices for Password Setup

Your VP50 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, VP50 will automatically wipe out the encrypted data – formatting itself back to a factory state.

**Multi-Password**
VP50 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 VP50 can support three different passwords you may use to recover data – Admin, User, and a One-Time Recovery password.

VP50 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. In addition, Admin can set up the One-Time Recovery password for User to provide a way for User to log in and reset the User password.

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. User can use the One-Time Recovery password in order to reset the User password when needed.

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 VP50 can be Reset and reused, but the prior data will be erased forever.

**Password Modes**
The VP50 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**
VP50 supports Passphrases from 10 to 64 characters. A Passphrase follows no 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 VP50 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.

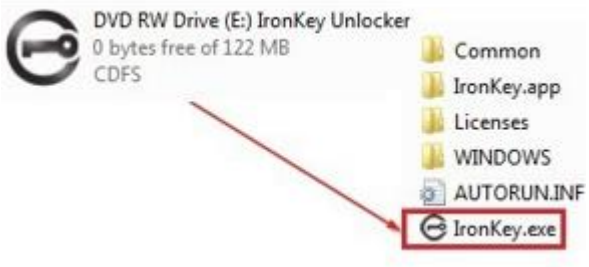
## Setting Up My Device

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)

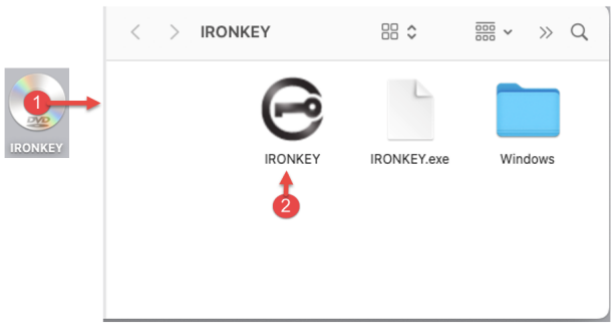
Plug the IronKey encrypted USB drive into an available USB port on the notebook or desktop and wait for Windows to detect it.

| | |
|---|---|
| • Windows 8.1/10/11 users will receive a device driver notification. (Figure 3.1) |  <br>**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)<br><br>• Please note that the partition letter will vary based on the next free drive letter. The drive letter may change depending on what devices are connected. In the image below, the drive letter is (E:). |  <br>**Figure 3.2 - File Explorer Window/IronKey.exe** |

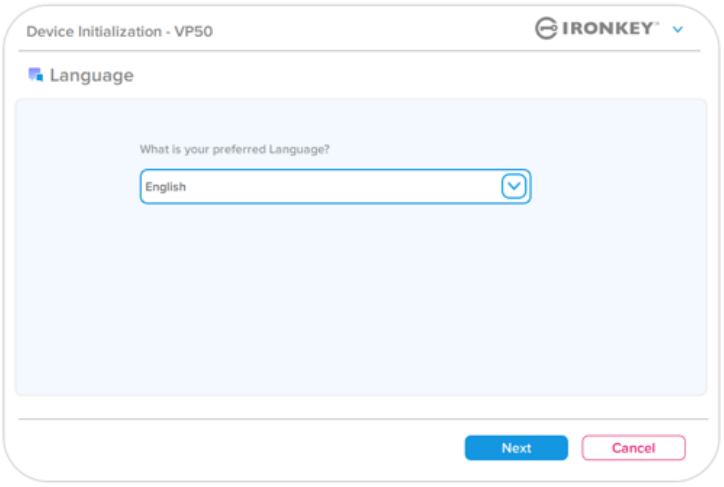
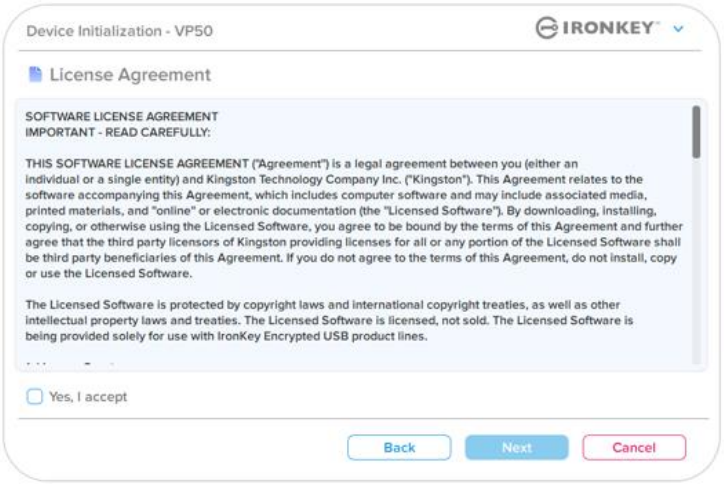
### Device Access (macOS Environment)

Insert the VP50 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 an IKVP50 (Or IRONKEY) volume appear on the desktop. (Figure 3.3)

| | |
|---|---|
| • Double-click the IronKey CD-ROM icon.<br><br>• Then, double-click the IKVP50 (Or IronKey.app) application icon found in the window displayed in Figure 3.3. This will start the initialization process. |  <br>**Figure 3.3 - IKVP 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) |  <br>**Figure 4.1 - Language Selection** |
| Review the license agreement and click **Next**.<br><br>Note: You must accept the license agreement before continuing; otherwise, the **Next** button will remain disabled. (Figure 4.2) |  <br>**Figure 4.2 - License Agreement** |

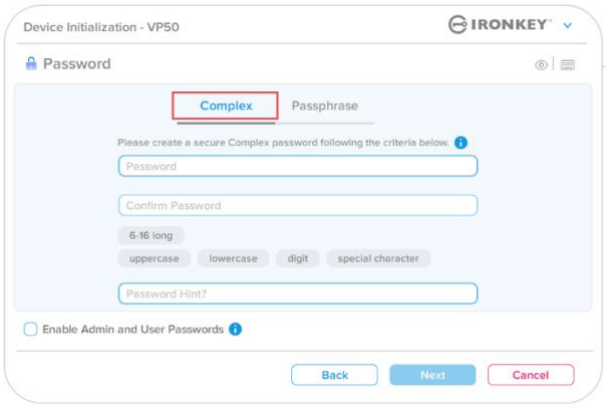
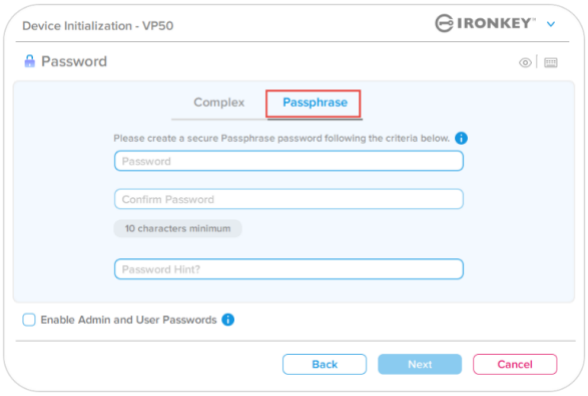
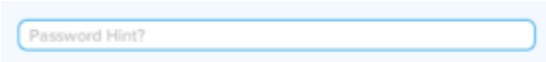
## Device Initialization

### Password Selection

On the Password prompt screen, you will be able to create a password to protect your data on the VP50 using either the Complex or Passphrase password modes (Figures 4.3- 4.4). Additionally, the Multi-password Admin/User options can also be enabled on this screen. Before proceeding with Password Selection, please review Enabling Admin / User Passwords below for a better understand of these features.

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

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

| | |
|---|---|
| **Complex Password**<br>• Must contain 6 characters or more (up to 16 characters).<br>• Must contain three (3) of the following criteria:<br>○ Upper Case<br>○ Lower Case<br>○ Numerical Digit<br>○ Special characters (!,$,&, etc..) |  <br>**Figure 4.3 - Complex Password** |
| **Passphrase Password**<br>• Must contain:<br>○ 10 characters minimum<br>○ 64 characters maximum |  <br>**Figure 4.4 - Passphrase Password** |
| **Password Hint (Optional)**<br>A password hint can be useful for providing a clue as to what the password is, should the password ever be forgotten.<br>**Note**: The hint CANNOT be an exact match to the password. |  <br>**Figure 4.5 - Password Hint Field** |

## Device Initialization

### Valid and Invalid Passwords

For **valid** passwords, the Password Criteria Boxes will highlight **green** when the criteria are met. (See Figures 4.6a-b) Note: Once the minimum of three password criteria are met, the fourth criteria box will become gray, indicating that this criterion is not optional. (Figure 4.6b)

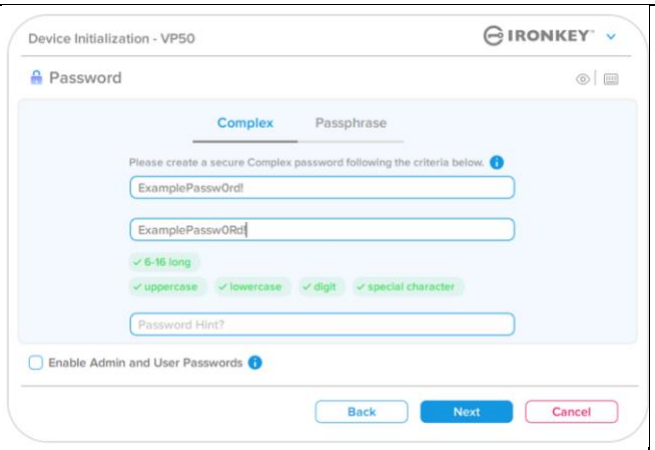



**Figure 4.6a - Complex Password Condition Met**

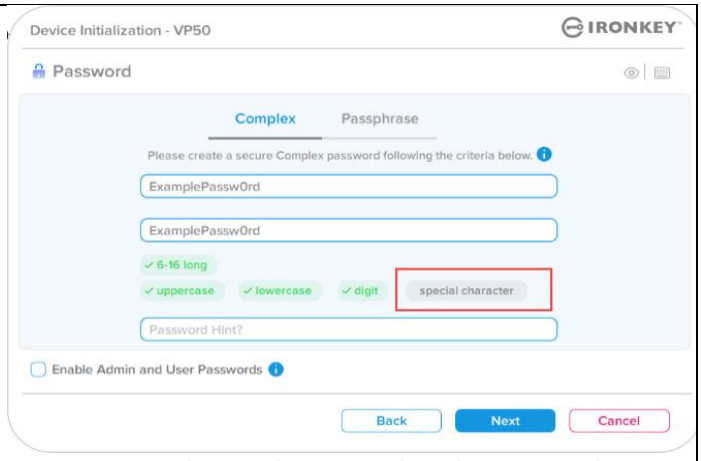



**Figure 4.6b - Complex Password Condition Optional**

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.

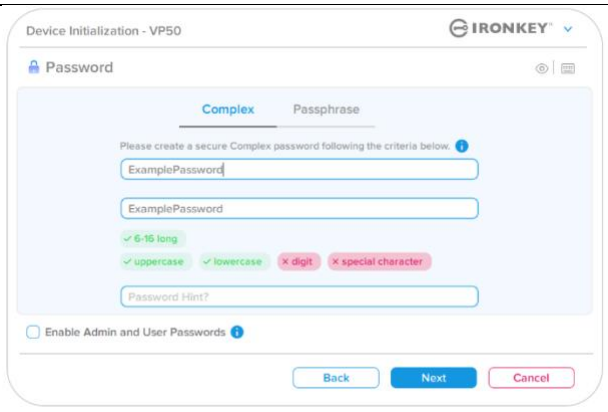



**Figure 4.7 - Password Conditions Not Met**

## Device Initialization

### Virtual Keyboard

The VP50 features a Virtual Keyboard that can be used for Keylogger protection.

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

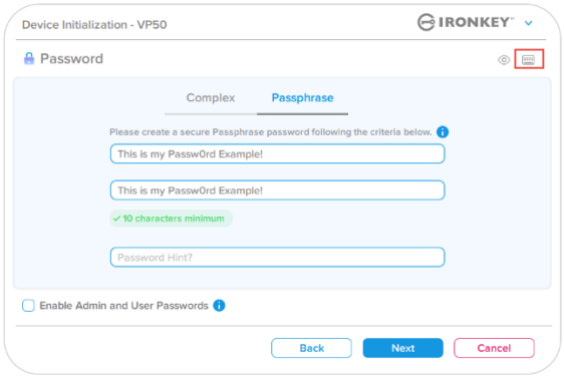



**Figure 4.8 - Activating the Virtual Keyboard**

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

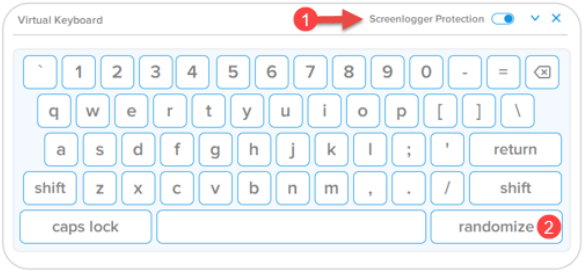



**Figure 4.9 - Screenlogger Protection / Randomize**

## Device Initialization

### Password Visibility Toggle

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

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

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

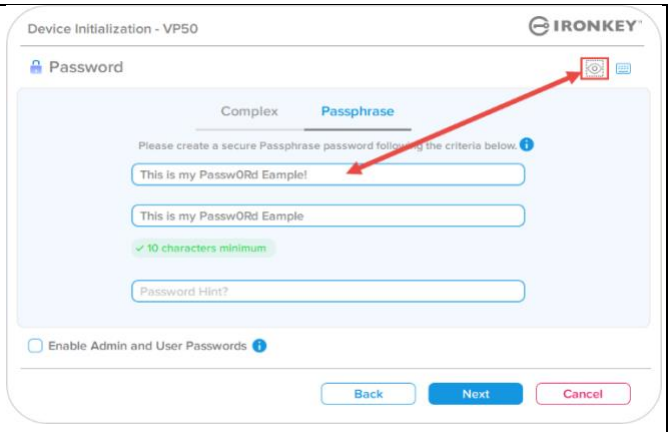



**Figure 4.10 - Toggle 'hide' Password**

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

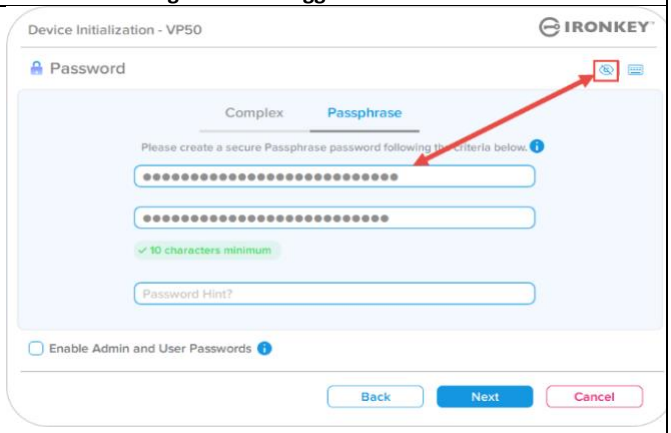



**Figure 4.11 - Toggle 'show' Password**

## Device Initialization

### Admin and User Passwords

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

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

- One-Time Recovery password
- Forced-Read only mode for User login
- User Password reset
- Force Reset Password for user login

To learn more about these features, navigate to page 25 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.

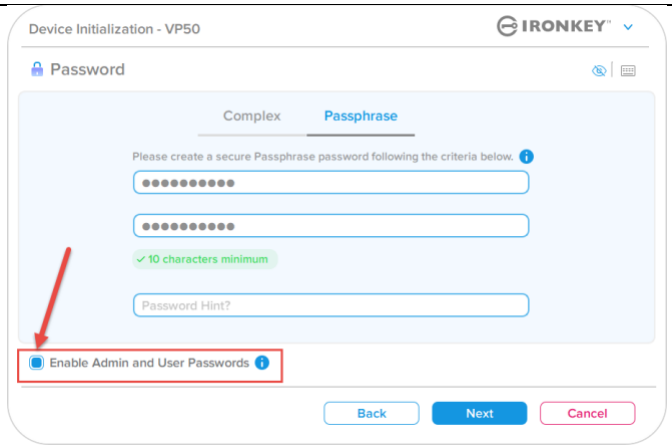



**Figure 4.12 - Enabling Admin and User Passwords**

**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.

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

## 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 later in this User Guide. (see Page 23)

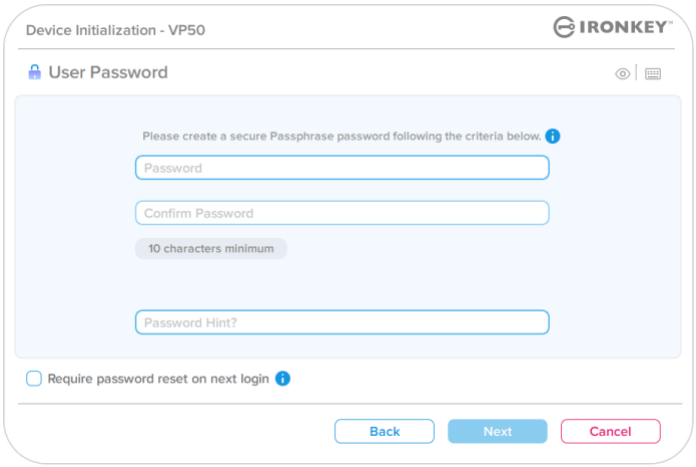



**Figure 4.13 - User Password (Admin and User Enabled)**

**Note:** The chosen Password Option (Complex or Passphrase) criteria will carry over to the User Password, One-Time Password Recovery 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.

- The '**Require password reset on next login'** feature on the bottom left corner of **Figure 4.13** is only for the User Password and can be enabled to force the User to login using the temporary password set by Admin during the initialization process, and then change it to a password of their choice after the drive is authenticated with the temporary password. This is useful when the drive is given to another person to use. (**Figure 4.14)**

  **Note:** For security, the new password cannot be the same as the temporary password.

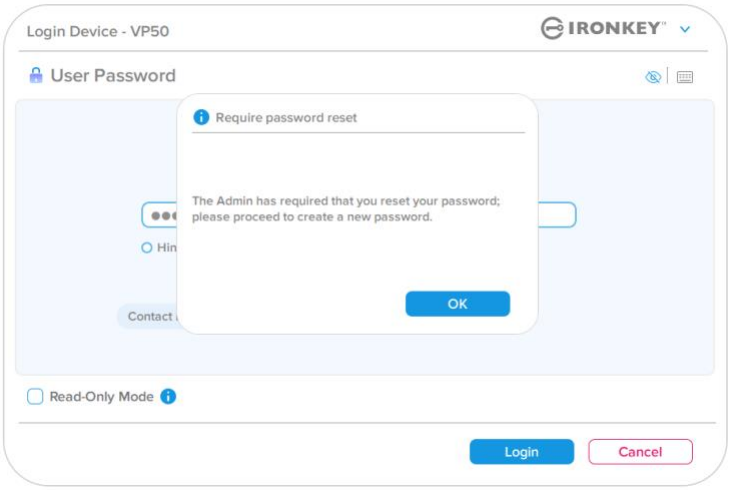


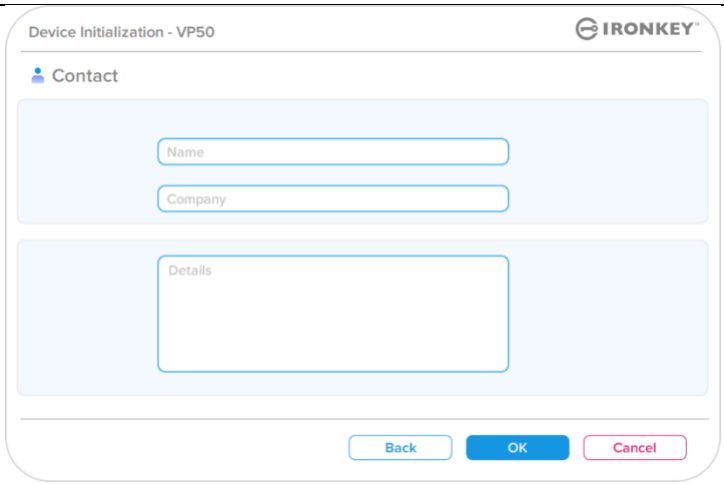

**Figure 4.14 - Require password reset on next login (For User Password)**

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

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

## Device Usage (Windows & macOS Environment)

### Login For Admin & User (Admin Enabled)

If the device is initialized with Admin and User Passwords (Admin Role) enabled, the IronKey VP50 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 5.1). 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 5.2)

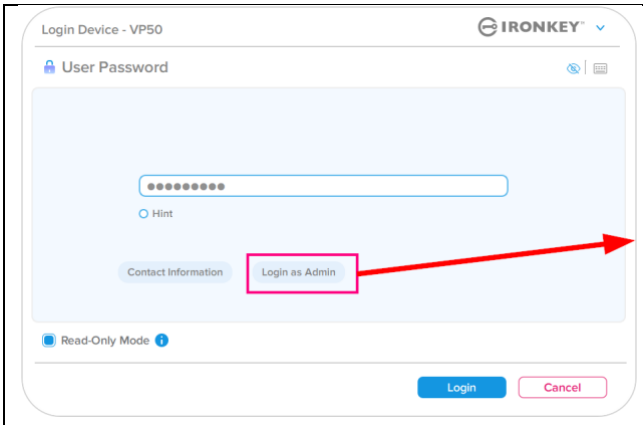



**Figure 5.1 - User Password Login (Admin enabled)**

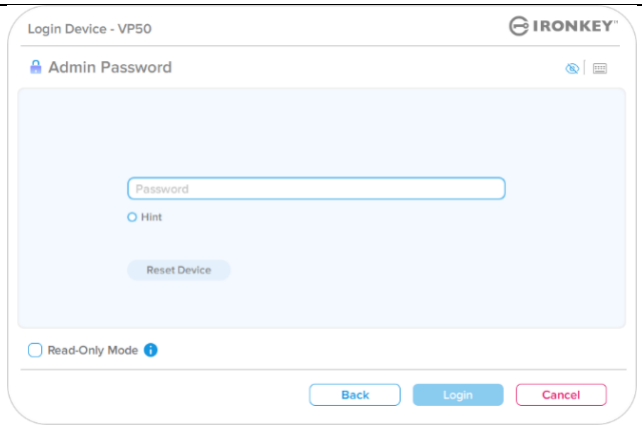



**Figure 5.2 - Admin Password Login**

### Login for User-Only Mode (Admin not Enabled)

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

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

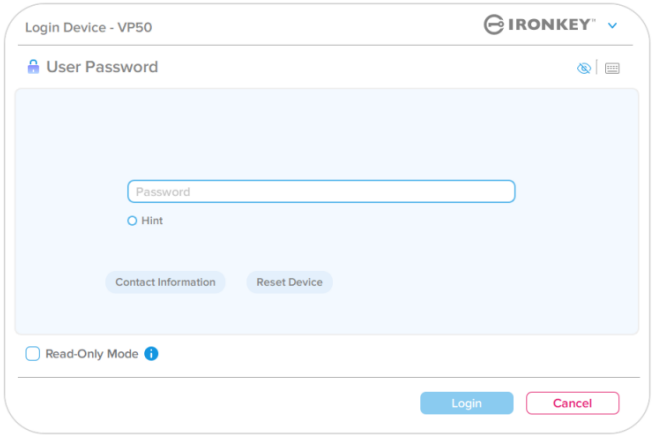



**Figure 5.3 - User Password Login (Admin not enabled)**

## Device Usage

### Unlocking in Read-Only Mode

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

When working in this mode, you cannot perform any operations that involve modifying files on the device. For example, you cannot reformat the device, restore, add, or edit files on the drive.

To unlock the device in Read-Only Mode:

1. Insert the device into the USB port of the host computer and run the **IronKey.exe**.
2. Check the **Read-Only Mode** below the password entry box. (**Figure 5.4)**
3. Type your device password and click **Login**. The IronKey will now be unlocked in Read-Only mode.

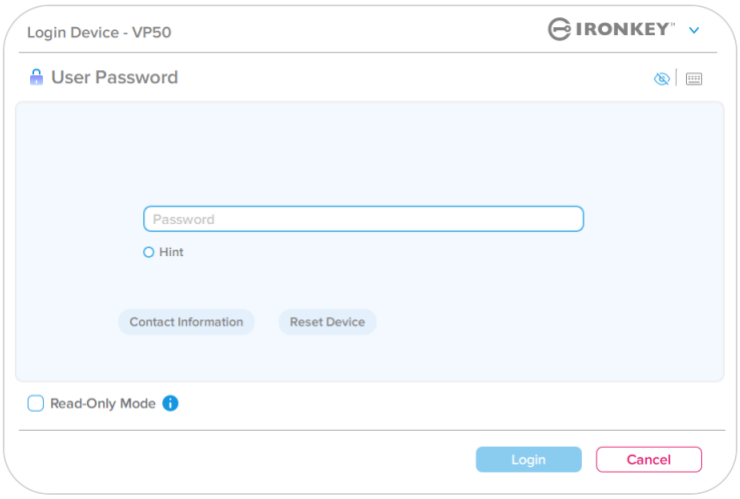



**Figure 5.4 - Read-Only Mode**

If you wish to unlock the device with full read/write access to the secure data partition, you must shutdown VP50 and log back in, leaving the 'Read-Only Mode' checkbox unchecked.

**Note:** The VP50 Admin options features a Forced Read-Only mode for the User data, meaning the User login can be forced to unlock in a read-only state by the Admin (See **page 28** For details).

## Device Usage

### Brute-Force attack protection

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

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

| **Admin/User Enabled** | **Brute Force protection Device Behavior (10 Incorrect Password attempts)** | **Data Erase and Device Reset?** |
|---|---|---|
| User Password | Password Lockout. Login as Admin or use One-Time Recovery password to reset User Password | NO |
| Admin Password | Crypto-Erase drive, Passwords, settings, and data erased forever | **YES** |
| One-Time Recovery Password | Password Lockout, Recovery Password button will gray out and become unusable. Login as Admin to Reset Password | NO |
| **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** |

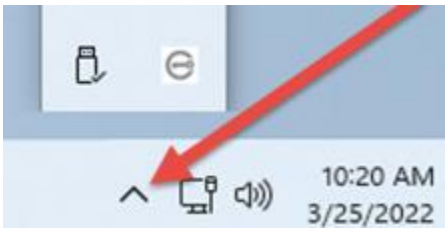
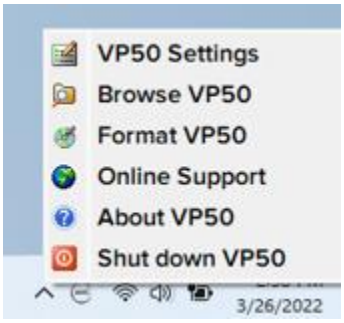
* Once you authenticate to the device successfully, the failed login counter will be reset in relation to which Login method was used. Crypto-Erase will delete all passwords, encryption keys and data – **your data will be lost forever.**

### Accessing My Secure Files

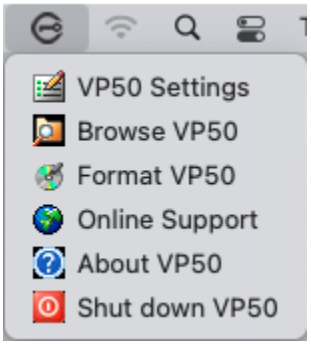
After unlocking the drive, you can access your secure files. Files are automatically encrypted and decrypted when you save or open them on the drive. This technology gives you the convenience of working as you normally would with a regular drive, while providing strong, “always-on” security.
**Hint**: You can also access your files by right clicking the **IronKey Icon** in the Windows taskbar and clicking **Browse VP50.** (Figure 6.2)

## Device Options - (Windows Environment)

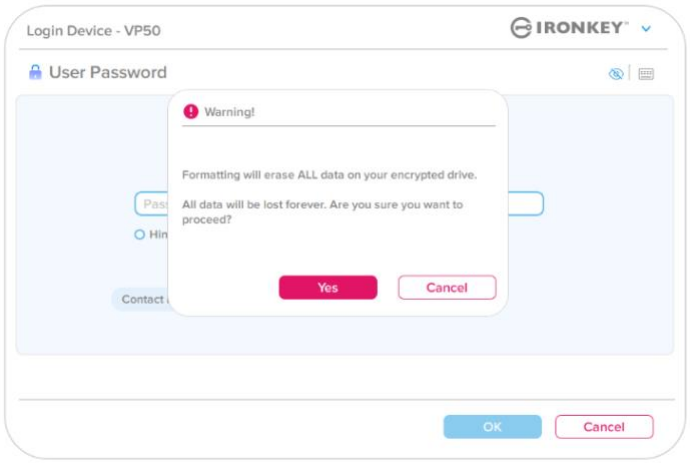
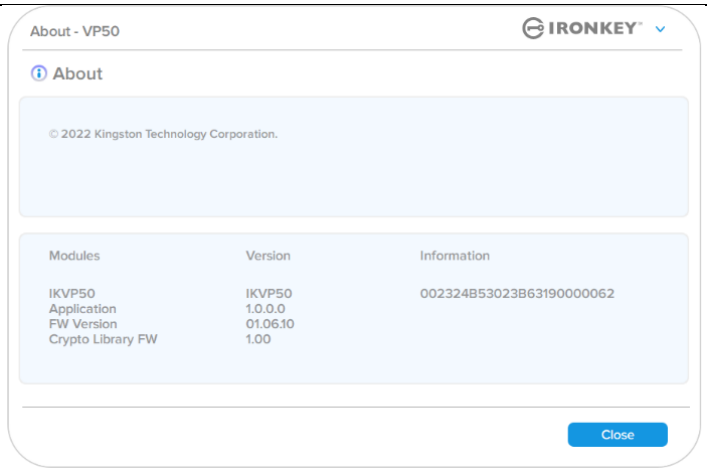
While you are logged into the device, there will be an IronKey icon located in the right-hand corner the window. Right-clicking on the IronKey Icon will open the selection menu for available drive Options. (Figure 6.2)
Details about these device options can be found on Pages 19-23 of this manual.

| | |
|---|---|
| • While you are logged into the device, there will be an IronKey icon located in the right-hand corner of the window. **(Figure 6.1)** |  <br>**Figure 6.1 - IronKey Icon in Taskbar** |
| • Right clicking on the IronKey Icon will open the selection menu for available drive Options. **(Figure 6.2)**<br><br>Details about these device options can be found on pages 19-23 of this manual. |  <br>**Figure 6.2 - Right-Click IronKey Icon for Device Options** |

## Device Options- (macOS Environment)

| | |
|---|---|
| • While you are logged into the device, there will be a 'IronKey VP50 icon located in the macOS menu seen in **Figure 6.3** that will open the available device options.<br><br>Details about these device options can be found on Pages 19-23 of this manual. |  <br>**Figure 6.3 - macOS menu bar Icon/Device options menu** |

## Device Options

| | |
|---|---|
| **VP50 Settings:** | • Change login Password, Contact Information, and other settings. (More details about device settings can be found in the 'VP50 Settings' section of this manual). |
| **Browse VP50:** | • Allows you to view your secure files. |
| **Format VP50:**<br>Allows you to format the secure data partition. (Warning: All data will be erased) (**Figure 6.1**)<br><br>**Note:** Password authentication will be required for format. |  <br>**Figure 6.1 - Format VP50** |
| **Online Support:** | • Opens your internet browser and navigates to http://www.kingston.com/support where you can access additional support information. |
| **About VP50:**<br>Provides specific details about the VP50, including Application, Firmware and Serial number Information. (**Figure 6.2**)<br><br>**Note:** The unique serial number of the drive will be under the 'Information Column'. |  <br>**Figure 6.2 - About VP50** |
| **Shut down VP50:** | • Properly shuts down the VP50, allowing you to safely remove it from your system. |

# VP50 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 7.1*)
- **Contact Info:** Allows you to add/view/change your contact information (*Figure 7.2*)
- **Language:** Allows you to change your current language selection (*Figure 7.3*)
- **Admin Options:** Allows you to enable additional features such as: (Figure 7.4)
    - Change the User Password
    - Login Password Reset (For User Password)
    - Enable a One-Time Recovery Password
    - Force Read-Only mode for User's data

**NOTE:** Additional details of the Admin Options can be found on page 24.

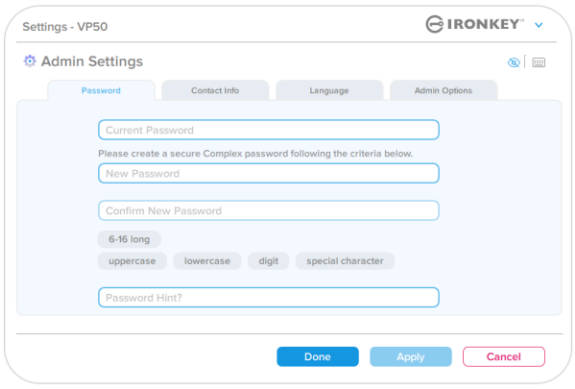



**Figure 7.1 - Password Options**

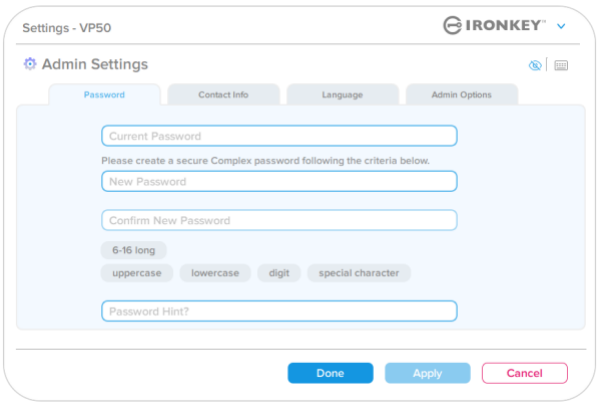



**Figure 7.2 - Contact Info**

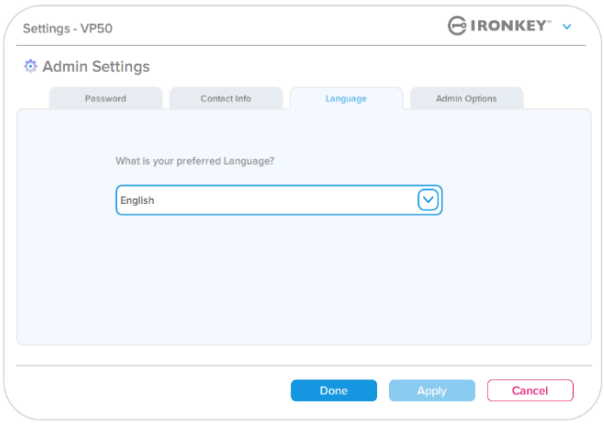



**Figure 7.3 - Language Options**

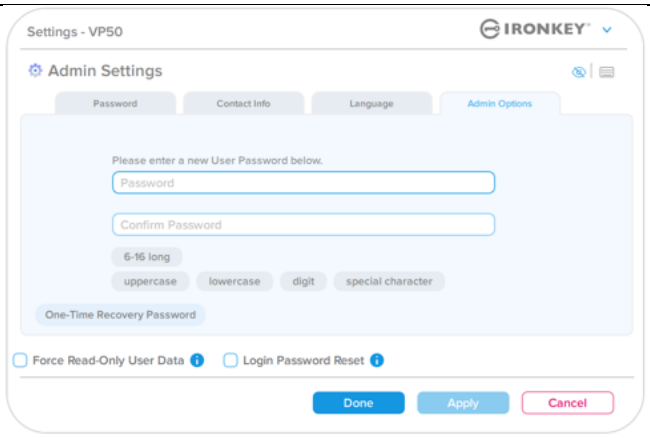



**Figure 7.4 - Admin Options**

## VP50 Settings

### User Settings: Admin Enabled

The User Login limits access to the following settings:

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

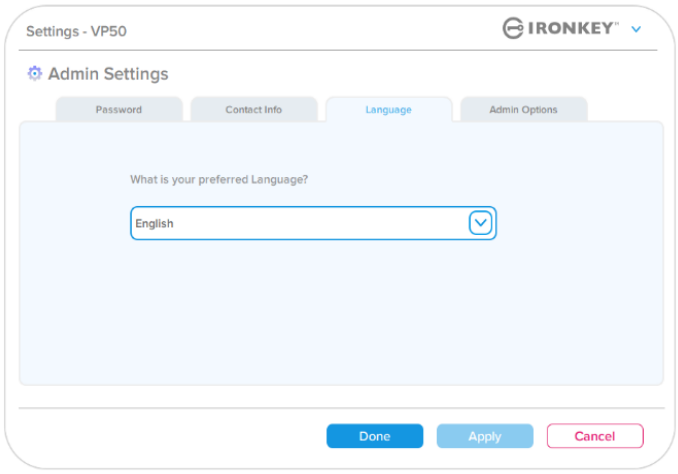



**Figure 7.5 - Password Options (Admin Enabled: User Login)**

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

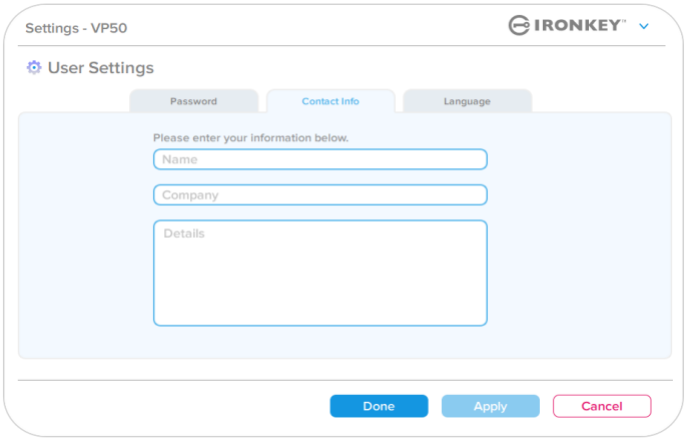



**Figure 7.6 - Contact Information (Admin Enabled: User Login)**

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

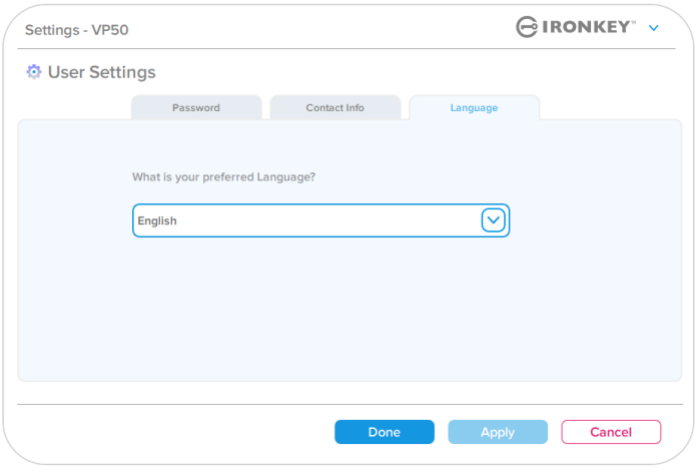



**Figure 7.7 - Language Settings (Admin Enabled: User Login)**

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

## VP50 Settings

### User Settings: Admin Not Enabled

As mentioned previously on Page 12, initializing the VP50 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 VP50 Settings:

### Changing and Saving settings

- Whenever settings are changed in the VP50 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 7.11)

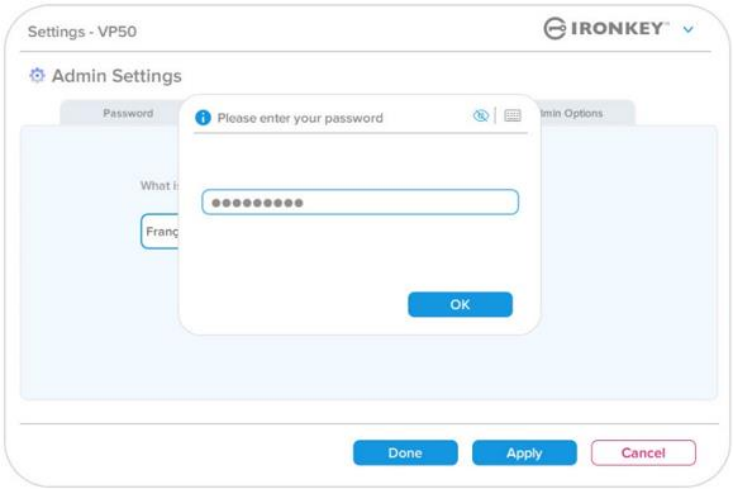



**Figure 7.11 - Password Prompt screen to save VP50 setting changes**

**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 VP50 settings menu.

## Admin Features

**Options Available to Reset the User Password**

The features of Admin configuration allow multiple ways to securely reset the Users Password, should it be forgotten, or if a temporary User password is created and you would like to enforce a password change upon next login for the User Login. Below are the features 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 8.1)**

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

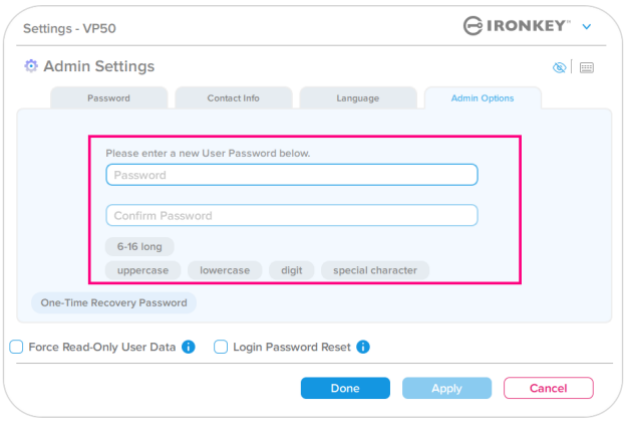



**Figure 8.1 - Admin Options/User Password Reset**

**Login Password Reset:**

Enabling Login Password Reset will **force the User to login using a temporary password set by the Admin**, and then change it to a password of their choice. This is useful when the drive is given to another person to use. (**See Figures 8.2A and 8.2B**)

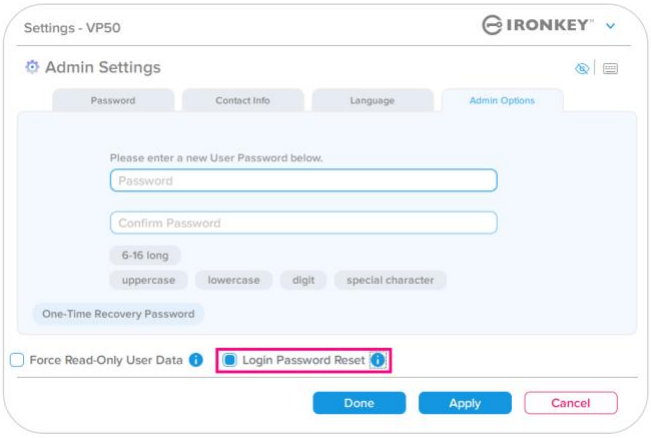



**Figure 8.2A - Login Passwords Reset button**

**Note:** Applying this reset will take place upon next successful User Login. Password requirement criteria will automatically be applied according to the original option set during the initialization process (Complex or Passphrase options).

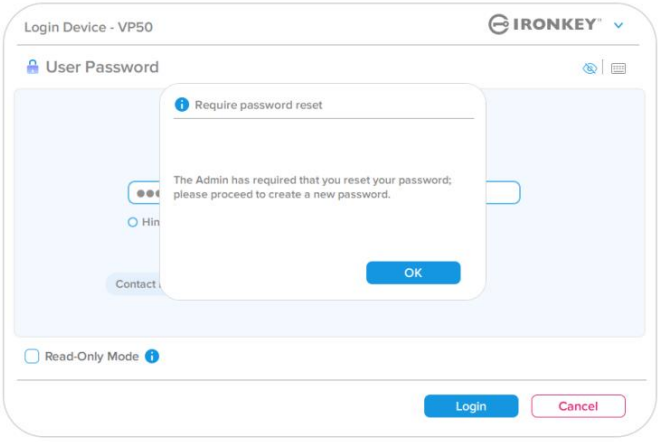



**Figure 8.2B - Reset Notification after User Password is entered**

## Admin Features

### One-Time Recovery Password

This section will discuss the process to enable and use the One-Time Recovery password feature.

**One-Time Recovery password**

**Step 1:** The One-Time Recovery password feature is a very useful, single-use password that can be enabled to help recover and reset the User password should the user password be forgotten. Click on the 'One-Time Recovery Password' button in the Admin options menu to start get started. **(Figures 8.4)**

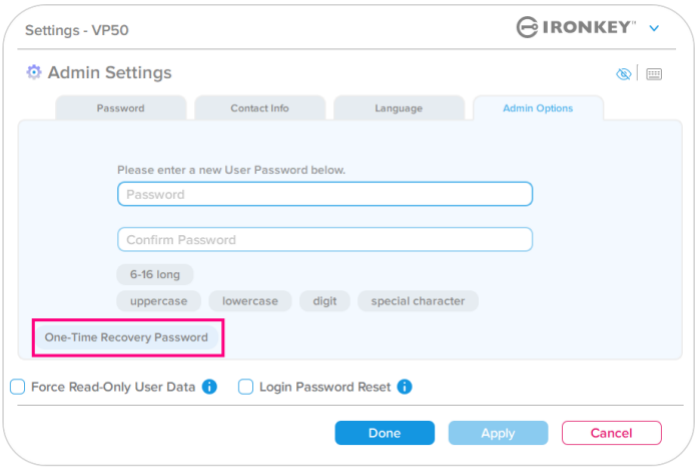



**Figure 8.4 - One-Time Recovery Password Button**

**Step 2:** Create a One-Time Recovery password using the same Password criteria the device was initially set with (Complex or Passphrase).

**Note:** Admin password will be required to apply changes.

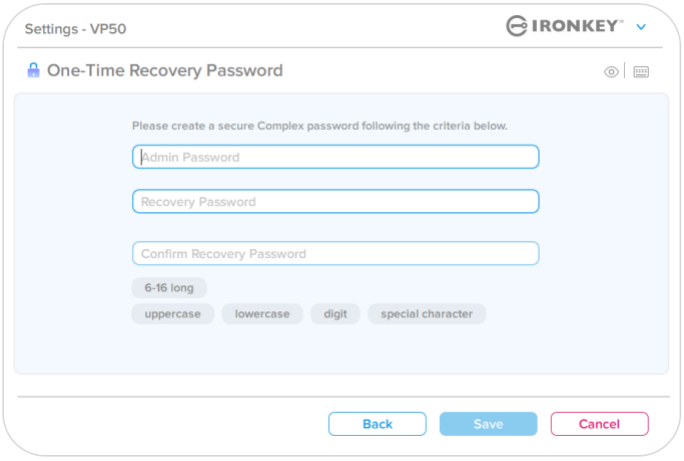
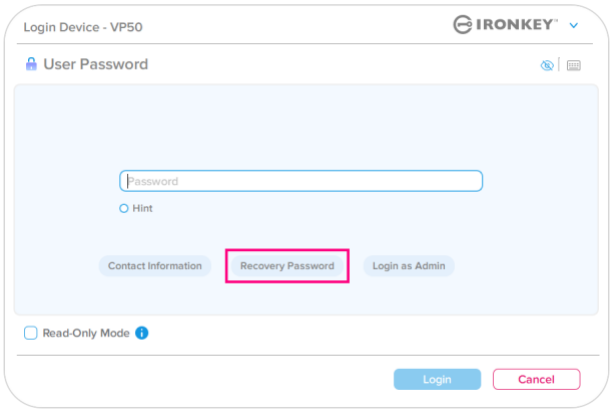
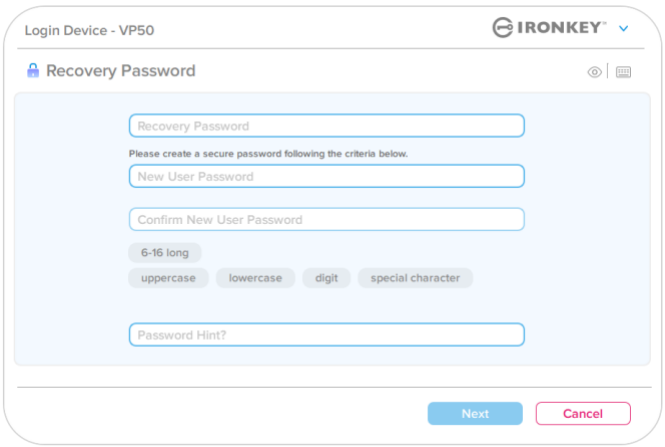
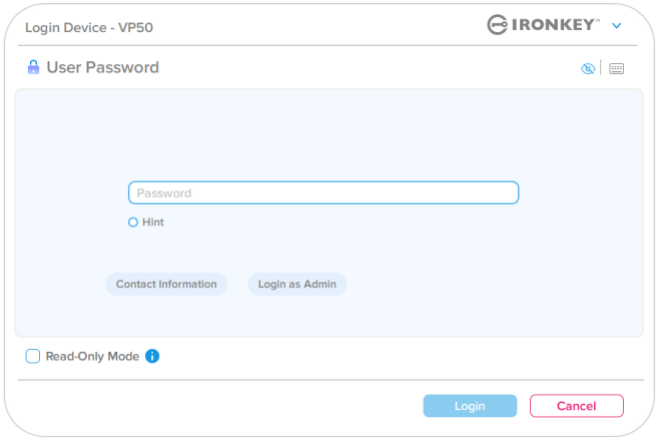



**Figure 8.5 - One-Time Recovery Password setup**

## Admin Features

Using One-Time Recovery Password

| | |
|---|---|
| **Step 1:** After the One-Time Recovery password has been created, a new button will appear on the **User Password** login screen upon next login. Click on the **Recovery Password** button to start the process. |  **Figure 8.6 - Recovery Password Button** |
| **Step 2:** The **Recovery Password** screen will appear where you can enter the Recovery Password and create a new a User Password. (Figure 8.7)<br><br>**Important:** The One-Time Recovery password also utilizes a built-in security feature that tracks the number of failed login attempts, **after 10 failed incorrect Login attempts with the One-Time Recovery password, the password will become disabled,** and will have to be re-enabled by logging to the drive as Admin. (see pages 18 and 30 for more details) |  **Figure 8.7 - Recovery Password menu** |
| **Step 3:** Upon success, you will be taken back to the **User Password** screen. The **Recovery Password** button is now gone, and the User password entered in **Step 2** will become the new User Password. (Figure 8.8) |  **Figure 8.8 - User Password Login screen showing the Recovery Password button disappears after successful use.** |

## Admin Features

### Force Read-Only User Data

The Forced Read-Only mode feature can be enabled to restrict write access to the drive for the User. This feature is useful if files on the drive are needed for read access-only.

- To enable Force Read-Only for the User data, click on the box and click 'Apply'. **(Figure 8.9)**

  **Note:** This Force Read-Only mode only applies to the User and does not affect the Admin login. Admin login will still have Read and Write access privileges, and still can enable Read-Only mode if needed.

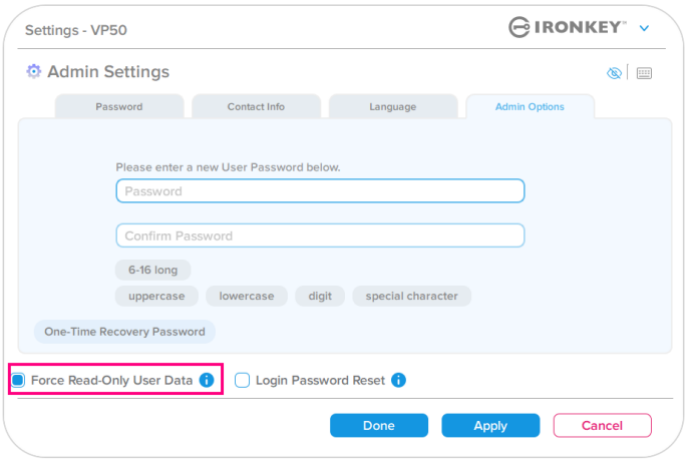



**Figure 8.9 - Enable 'Force Read-Only User data' (Admin Password will be required to apply changes)**

- Once enabled, the **'Read-Only Mode'** button box will be in a blue color, meaning that Forced Read-Only Mode is permanently enabled for the User Password, until it is disabled by the Admin. (Figure 8.10)

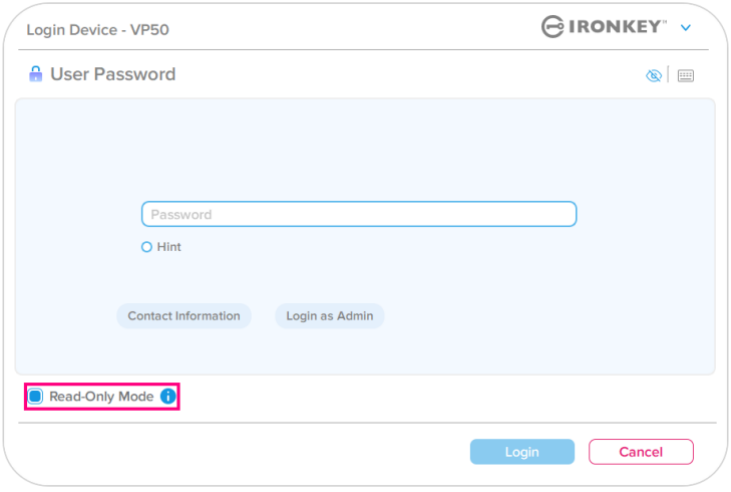



**Figure 8.10 - Read-Only Mode is forced enabled for the user and can only disabled by Admin**

## Help and Troubleshooting

### Device Lockout

The VP50 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/One-Time Recovery Password).

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 9.1)

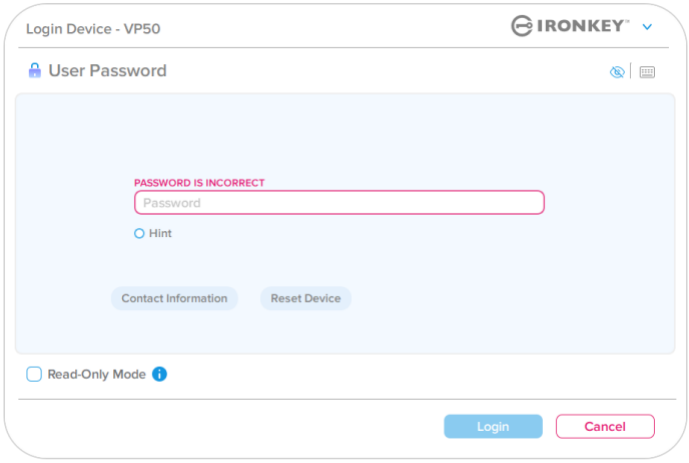



**Figure 9.1 - Incorrect Password message**

- 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 9.2)

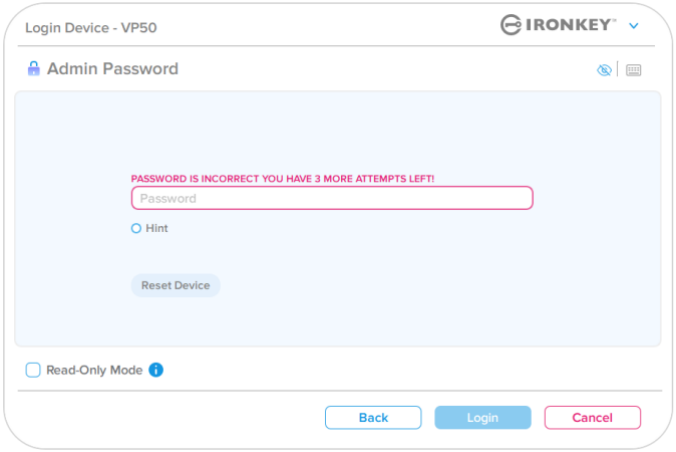



**Figure 9.2 - 7th incorrect Password attempt**

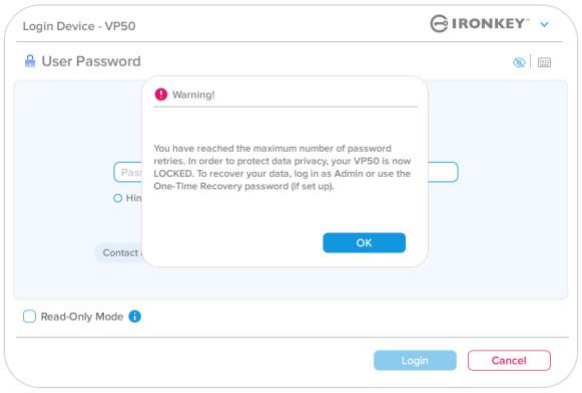
## Help and Troubleshooting

### 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 or One-Time Recovery Password) 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 9.3- 9.6 below demonstrate the visual behavior for the 10th and final failed logins of each login password method:

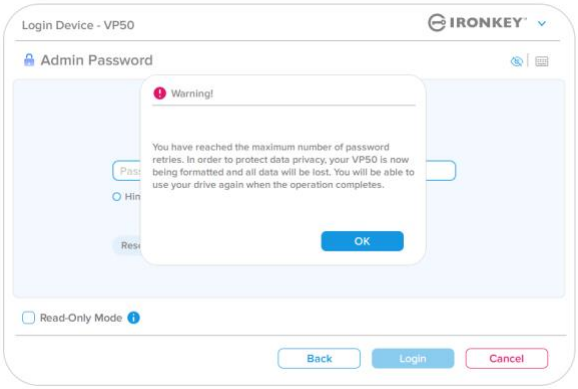
**User Password: (Admin/User Enabled)**




**DEVICE LOCKOUT**

**(Figure 9.3)**

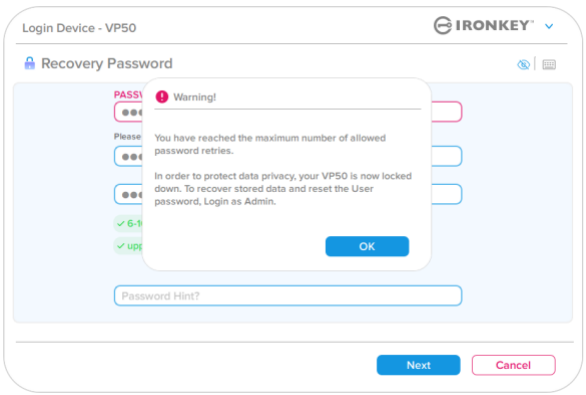
**Admin Password (Admin/User Enabled)**




**DEVICE FORMAT***

**(Figure 9.4)**

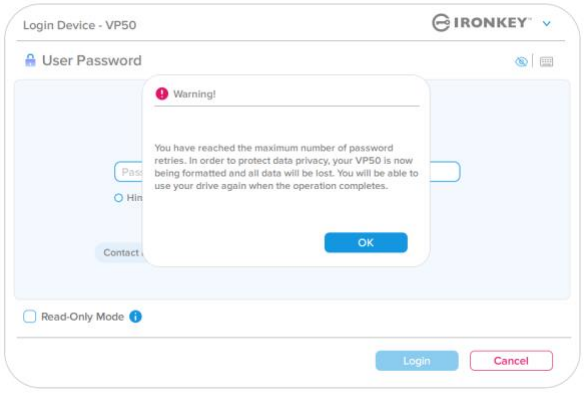
**One-Time Recovery: (Admin/User Enabled)**




**DEVICE LOCKOUT**

**(Figure 9.5)**

**User Password (Admin NOT Enabled)**




**DEVICE FORMAT***

**(Figure 9.6)**

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 VP50 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.

**Note: A device format will erase ALL of the information stored on the VP50'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 VP50 Launcher is executed. (see ***Figure 9.7*** and **9.8)**

- This option will allow you to create a new password, but to protect the privacy of your data, the VP50 will be formatted. This means that all of your data will be erased in the process.*

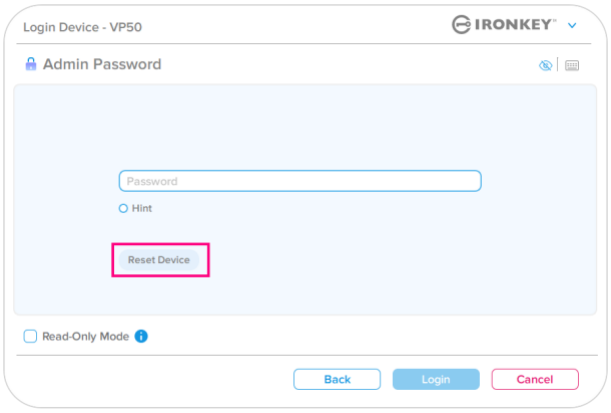



**Figure 9.7 - Admin Password: Reset Device Button**

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

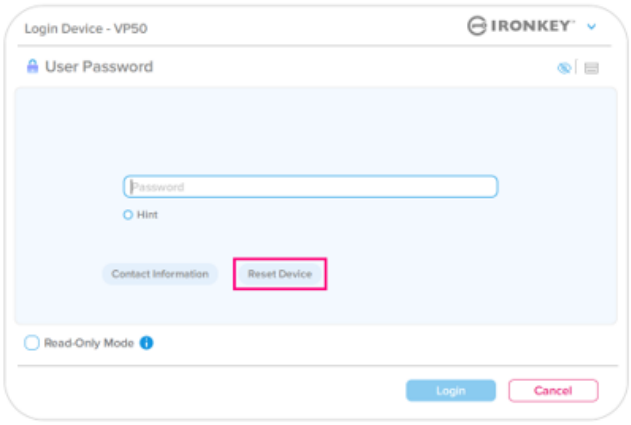



**Figure 9.8 - User Password (Admin/user not enabled) Reset Device**

- 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.

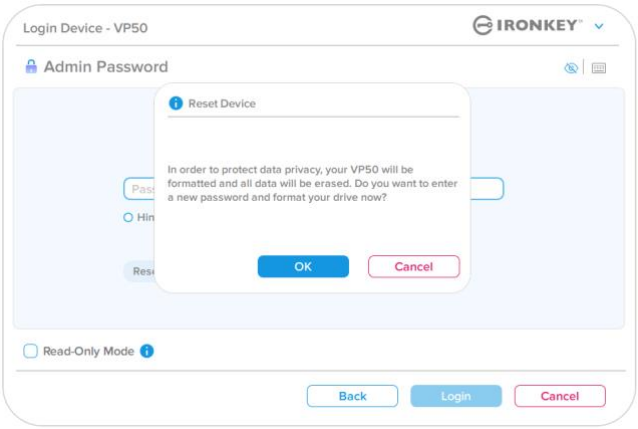



**Figure 9.9 - Reset device confirmation**

## Help and Troubleshooting

### Drive Letter Conflict: Windows Operating Systems

- As mentioned in the '*System Requirements*' section of this manual (on page 3), the VP50 requires two consecutive drive letters AFTER the last physical disk that appears before the 'gap' in drive letter assignments (see *Figure 9.10*.) This does NOT pertain to network shares because they are specific to user- profiles and not the system hardware profile itself, thus appearing available to the OS.

- What this means is, Windows may assign the VP50 a drive letter that's already in use by a network share or Universal Naming Convention (UNC) path, causing a drive letter conflict. If this happens, please consult your administrator or helpdesk department on changing drive letter assignments in Windows Disk Management (administrator privileges required.) As mentioned in the '*System Requirements*' section of this manual (on page 3), the VP50 requires two consecutive drive letters AFTER the last physical disk that appears before the 'gap' in drive letter assignments (see *Figure 9.10*.) This does NOT pertain to network shares because they are specific to user- profiles and not the system hardware profile itself, thus appearing available to the OS.

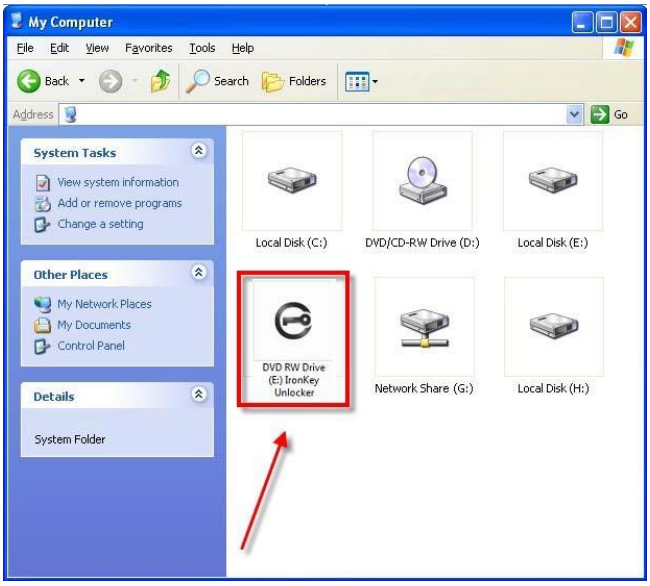



**Figure 9.10 - Drive Letter example**

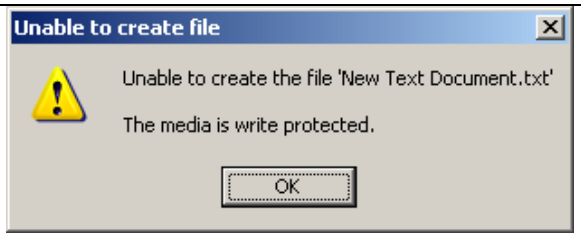
In this example (Figure 9.10), the VP50 uses drive F:, which is the first available drive letter after drive E: (the last physical disk before the drive letter gap.) Because letter G: is a network share and not part of the hardware profile, the VP50 may attempt to use it as its second drive letter, causing a conflict.

If there are no network shares on your system and the VP50 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.

## Help and Troubleshooting

### Error Messages

| | |
|---|---|
| **Unable to create file:**<br>This error message will appear when attempting to CREATE a file or folder ON the secure data partition while logged in under read-only mode. |  <br>**Figure 9.11 - Unable to Create File Error** |
| **Error copying file or folder:**<br>This error message will appear when attempting to COPY a file or folder TO the secure data partition while logged in under read-only mode. |  <br>**Figure 9.12 - Error Copying File or Folder Error** |
| **Error deleting file or Folder:**<br>This error message will appear when attempting to DELETE a file or folder FROM the secure data partition while logged in under read-only mode. |  <br>**Figure 9.13 - Error Deleting File or Folder Error** |

**Note:** If you are ever logged in under read-only mode and wish to unlock the device with full read/write access to the secure data partition, you must shutdown VP50 and log back in, leaving the 'Read-Only Mode' checkbox unchecked prior to login.

# IRONKEY™ Vault Privacy 50 (VP50)
# DISPOSITIVO FLASH USB 3.2 Gen 1 ENCRIPTADO

*Guía de usuario*

## Contenidos


Figura 1: IronKey VP50

## Introducción

El Kingston IronKey Vault Privacy 50 (VP50) es un dispositivo USB premium que proporciona seguridad de nivel empresarial con encriptado por hardware AES de 256 bits certificado FIPS 197 en modo XTS que incluye protección contra BadUSB con firmware firmado digitalmente, y contra ataques de contraseñas de fuerza bruta. VP50 también cumple con la TAA y se ensambla en los EE. UU. Debido a que es un almacenamiento encriptado bajo el control físico del usuario, la serie VP50 es superior al uso de Internet y los servicios en la nube para proteger los datos.

VP50 admite opciones de Múltiples contraseñas (Administrador, Usuario y Recuperación de una sola vez) con modos Complejos o de Frase de acceso. La opción Múltiples contraseñas mejora la capacidad de recuperar el acceso a los datos si se olvida una de las contraseñas. Además de admitir Contraseñas complejas tradicionales, el nuevo modo de Frase de acceso permite un PIN numérico, oración, lista de palabras o incluso letras de 10 a 64 caracteres. El administrador puede habilitar a un Usuario y una Contraseña de recuperación de una sola vez, o restablecer la Contraseña de usuario para restaurar el acceso a los datos.

Para ayudar en el ingreso de la contraseña, el símbolo de "ojo”  puede ser habilitado para revelar la contraseña escrita, reduciendo los errores tipográficos que conducen a intentos de inicio de sesión fallidos. La protección contra ataques de fuerza bruta bloquea las Contraseñas de usuario o de Recuperación de una sola vez cuando se ingresan 10 contraseñas no válidas seguidas y borra criptográficamente el dispositivo si la Contraseña de administrador se ingresa incorrectamente 10 veces seguidas.

Para protegerse contra el malware potencial en sistemas no confiables, tanto el Administrador como el Usuario pueden configurar el Modo de solo lectura para proteger el dispositivo de escritura; además, el teclado virtual integrado protege las contraseñas de keyloggers o screenloggers.

Las organizaciones certificadas FIPS 197 y compatibles con la TAA pueden personalizar y configurar dispositivos de la serie VP50 con un ID de producto (PID) para su integración con el software estándar Endpoint Management para cumplir con los requisitos corporativos de TI y ciberseguridad a través del Programa de personalización de Kingston.

Las pequeñas y medianas empresas pueden usar el Rol de administrador para administrar localmente sus dispositivos, por ejemplo, usar Administrador para configurar o restablecer las Contraseñas de usuario o de Recuperación de una sola vez de los empleados, recuperar el acceso a los datos en dispositivos bloqueados y cumplir con las leyes y regulaciones cuando se requieren análisis forenses.

El VP50 está respaldado por una garantía limitada de 5 años con soporte técnico gratuito de Kingston.

## IronKey Vault Privacy 50 Características

- Certificado FIPS 197 con encriptado de hardware XTS-AES de 256 bits (el encriptado nunca se puede desactivar)
- Fuerza bruta y protección contra ataques BadUSB
- Opciones de Múltiples contraseñas
- Modos de contraseña Compleja o de Frase de acceso
- Botón de ojo para mostrar las contraseñas introducidas, para así reducir los intentos de inicio de sesión fallidos
- Teclado virtual para ayudar a proteger contra keyloggers y screenloggers
- Configuración doble de Solo lectura (protección de escritura) para proteger el contenido del dispositivo contra cambios o malware
- Las pequeñas y medianas empresas pueden administrar localmente los dispositivos utilizando el Rol de administrador
- Compatible con Windows o macOS (consulte la hoja de datos para obtener más detalles)

## Acerca de este Manual

Este manual de usuario cubre la privacidad de IronKey Vault 50 (VP50) y se basa en la imagen de fábrica sin cambios personalizados implementados.

## Requisitos del sistema

| | |
|---|---|
| **Plataforma para PC**<br>• Intel, AMD y Apple M1 SOC<br>• Espacio libre en disco de 15 MB<br>• Puerto USB 2.0 - 3.2 disponible<br>• Dos letras de unidad consecutivas después de la última unidad física *<br><br>***Nota:** Vea Conflicto de letras de unidad' en la página 32. | **Soporte del sistema operativo de la PC**<br>• Windows 11<br>• Windows 10<br>• Windows 8,1 |
| **Plataforma Mac**<br>• Espacio libre en disco de 15 MB<br>• Puerto USB 2.0 - 3.2 | **Compatible con el sistema operativo Mac**<br>• macOS X (v. 10.13.x – 12.x.x) |

## Recomendaciones

Para asegurarse de que haya suficiente suministro de energía para el dispositivo VP50, insértelo directamente en un puerto USB en su portátil o escritorio, como se ve en la ***Figura 1.1.*** Evite conectar el VP50 a cualquier dispositivo(s) periférico(s) que pueda contar con un puerto USB, como un teclado o un concentrador alimentado por USB, como se ve en la ***Figura 1.2***.

**Figura 1.1 - Uso recomendado**

**Figura 1.2 - No recomendado**

### Uso del sistema de archivos correcto

El IronKey VP50 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 un VP50 en un sistema de destino
- Cuando utilice el dispositivo en un sistema público o desconocido, es posible que desee configurar el Modo de solo lectura en el dispositivo para ayudar a proteger el dispositivo del malware
- 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 un nuevo formato, 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 VP50 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 VP50 eliminará automáticamente los datos encriptados, volviendo a formatearse a sí misma a un estado de fábrica.

**Múltiples contraseñas**
El VP50 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 VP50 puede admitir tres contraseñas diferentes que puede usar para recuperar datos: Administrador, Usuario y una Contraseña de recuperación de una sola vez.

El VP50 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 Super Usuario. Además, el Administrador puede configurar la Contraseña de recuperación de una sola vez para el Usuario, con el fin de proporcionar una forma para que el Usuario inicie sesión y restablezca la Contraseña de 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. El usuario puede usar la Contraseña de Recuperación de una sola vez para restablecer la Contraseña de usuario cuando sea necesario.

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 VP50 se puede restablecer y reutilizar, pero los datos anteriores se borrarán para siempre.

**Modos de contraseña**
El VP50 también admite dos modos de contraseña diferentes:

**Compleja**
Una contraseña compleja requiere cumplir un mínimo de 6 a 16 caracteres utilizando al menos 3 de los siguientes caracteres:

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

**Frase de acceso**
El VP50 admite frases de acceso de 10 a 64 caracteres. Una Frase de acceso no sigue ninguna regla, pero si se usa correctamente, puede proporcionar niveles muy altos de protección con contraseña.

Una Frase de acceso es básicamente cualquier combinación de caracteres, incluidos los caracteres de otros idiomas. Al igual que el dispositivo VP50, 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 el dispositivo USB encriptado 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 al 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 de unidad libre. La letra de la unidad puede cambiar dependiendo de qué dispositivos estén conectados. En la imagen a continuación, la letra de unidad es (E:).

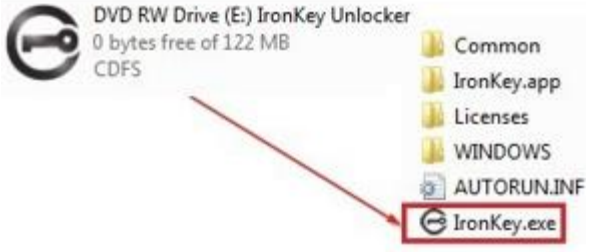



**Figura 3.2 - Ventana Explorador de archivos/IronKey.exe**

### Acceso a dispositivos (Entorno macOS)

Inserte el VP50 en un puerto USB disponible en su portátil o computadora y espere a que el sistema operativo Mac lo detecte. Cuando lo haga, verá que aparece un volumen IKVP50 (o IRONKEY) en el escritorio. (Figura 3.3)

- Haga doble clic en el icono de CD-ROM de IronKey.
- Luego, haga doble clic en el icono de la aplicación IKVP50 (O IronKey.app) que se encuentra en la ventana que se muestra en la Figura 3.3. Esto iniciará el proceso de inicialización.

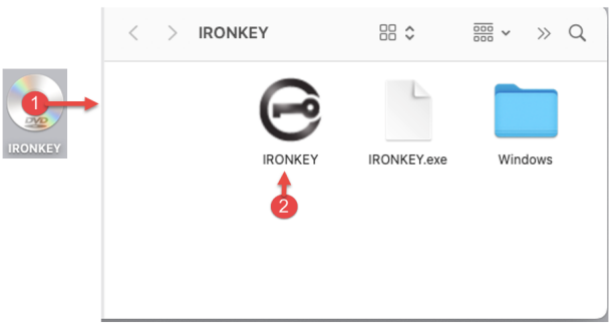



**Figura 3.3 - Volumen IKVP**

## Inicialización del dispositivo (entorno Windows y macOS)

### Idioma y EULA

Seleccione su preferencia de idioma en el menú desplegable y haga clic en **Siguiente (Next).** (Ver figura 4,1)

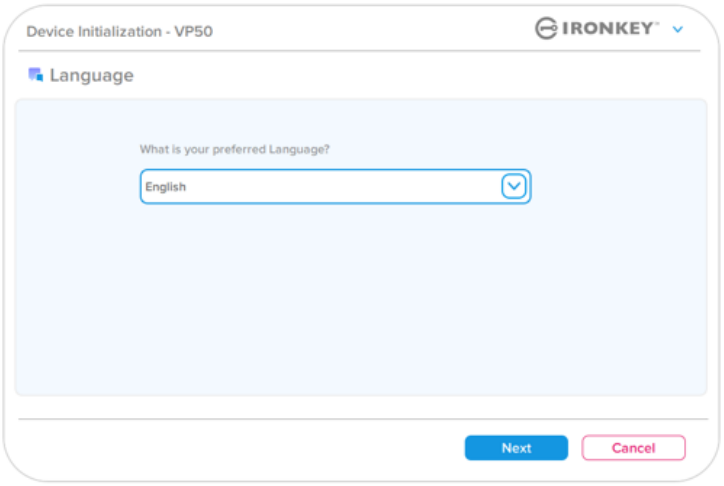



**Figura 4.1 - Selección de idioma**

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 (Next)** permanecerá deshabilitado. (Figura 4.2)

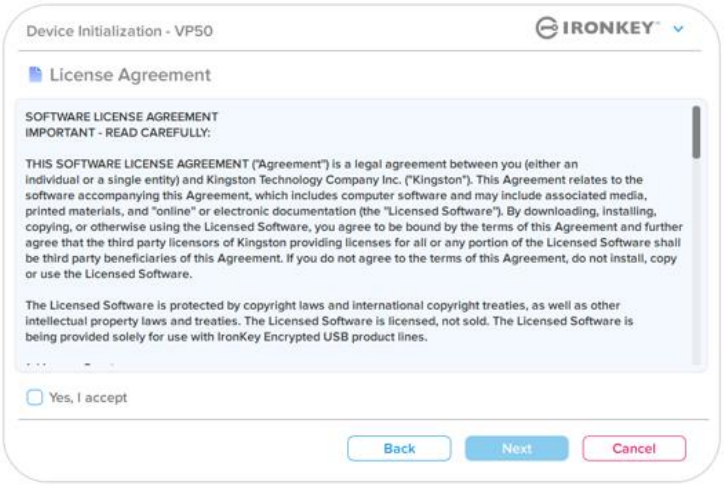



Figura 4.2 - Contrato de licencia

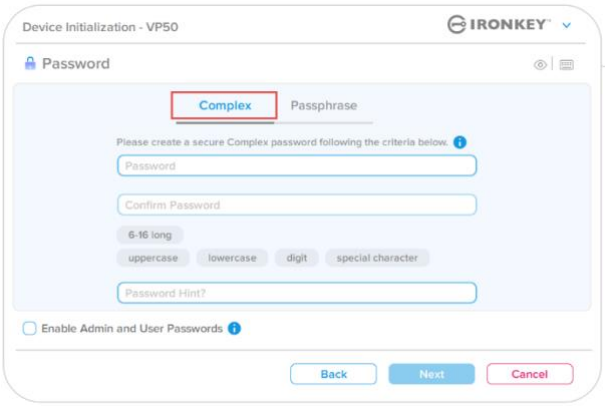
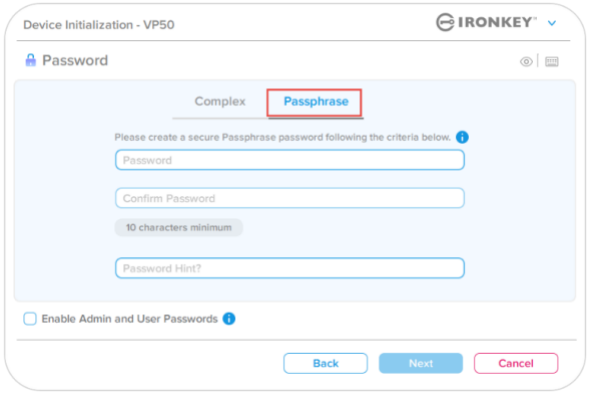
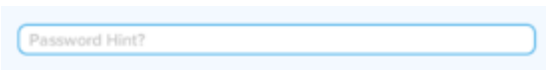
## Inicialización del dispositivo

### Selección de la contraseña

En la pantalla de solicitud de contraseña, podrá crear una contraseña para proteger sus datos en el VP50, utilizando los modos de contraseña Complejo o Frase de acceso (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' (Password) y vuelva a introducirla en los campos 'Confirmar contraseña' (Confirm Password). La contraseña que cree debe cumplir con los siguientes criterios antes de que el proceso de inicialización le permita continuar:

| | |
|---|---|
| **Contraseña compleja**<br>• Debe contener 6 caracteres o más (hasta 16 caracteres).<br>• Debe contener tres (3) de los siguientes criterios:<br>○ Mayúsculas<br>○ Minúsculas<br>○ Dígito numérico<br>○ Caracteres especiales (!,$,&, etc.) |  <br>**Figura 4.3 - Contraseña compleja** |
| **Contraseña de frase de acceso**<br>• Debe contener:<br>○ 10 caracteres mínimo<br>○ 64 caracteres como máximo |  <br>**Figura 4.4 - - Contraseña de la frase de acceso** |
| **Sugerencia de contraseña (opcional)**<br>Una pista de contraseña puede ser útil para proporcionar una pista sobre cuál es la contraseña, en caso de que la contraseña se olvide.<br>**Nota:** La pista NO PUEDE coincidir exactamente con la contraseña. |  <br>**Figura 4.5 - Campo de pista de contraseña** |

## Inicialización del dispositivo

### Contraseñas válidas y no válidas

Para las contraseñas **inválidas**, 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)

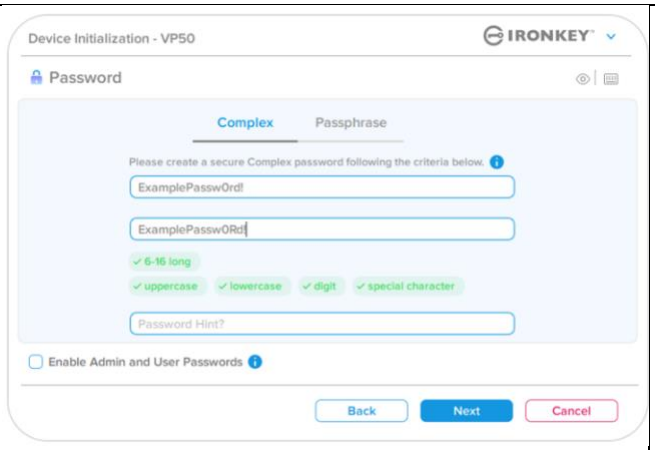



**Figura 4.6a - Condición de contraseña compleja cumplida**

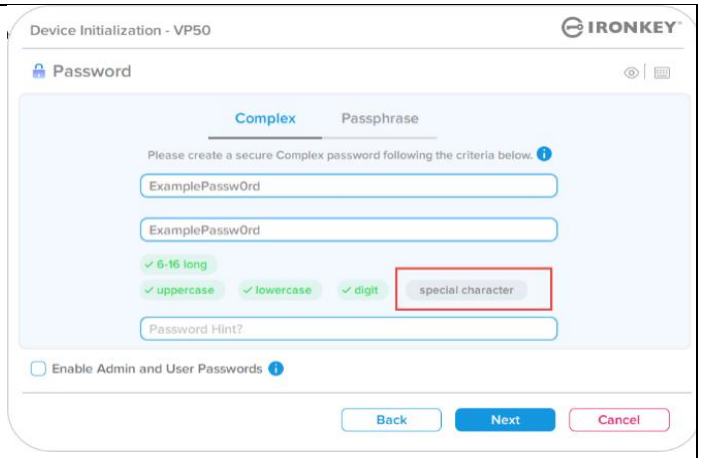



**Figura 4.6b - Condición de contraseña compleja opcional**

Para contraseñas **inválidas**, las Casillas de criterios de contraseña se resaltarán en **rojo** and y el botón **Siguiente (Next)** se deshabilitará hasta que se cumplan los requisitos mínimos.

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

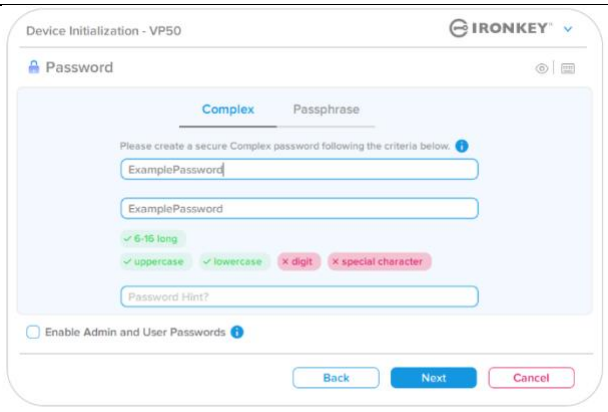



**Figura 4.7 - Condiciones de contraseña no cumplidas**

## Inicialización del dispositivo

### Teclado virtual

El VP50 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.

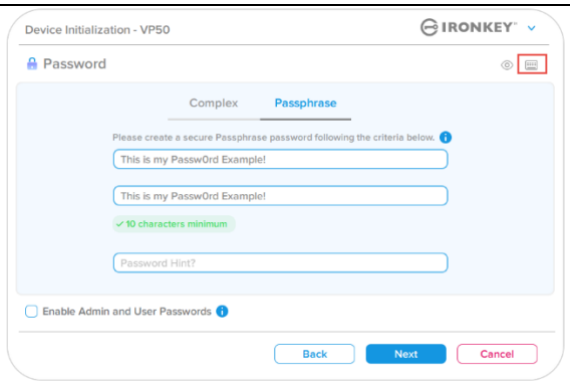



**Figura 4.8 - Activación del Teclado virtual**

- Una vez que aparezca el teclado virtual, también puede habilitar **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 elegir aleatorizar el teclado virtual seleccionando **aleatorizar (randomize)** en la parte inferior derecha del teclado. Aleatorizar organizará el teclado en un orden aleatorio.

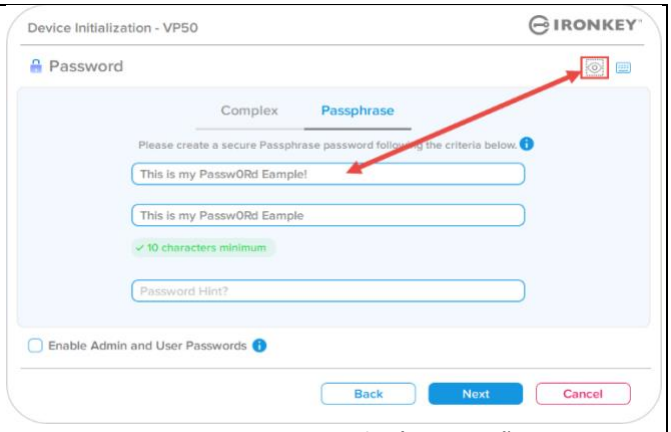
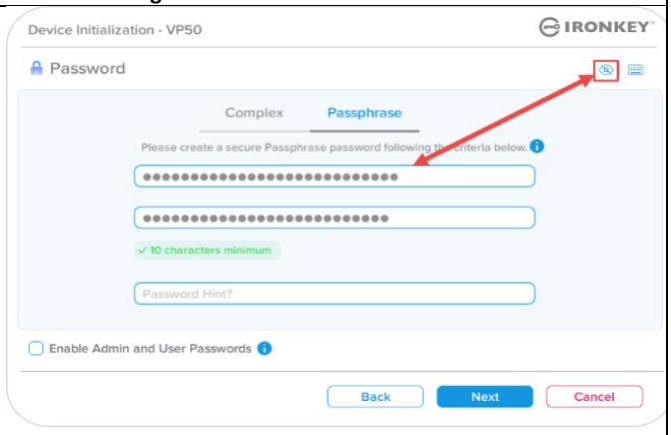

**Figura 4.9 - Protección/aleatorización contra Screenlogger**

## 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 alternando 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' (Enable Admin and User passwords)** 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:

- Contraseña de recuperación de una sola vez
- Modo de solo lectura forzada para el Inicio de sesión de usuario
- Restablecer contraseña de usuario
- Forzar el restablecimiento de la contraseña para el inicio de sesión de usuario

Para obtener más información sobre estas funciones, vaya a la página 25 de esta guía del usuario.

- Para habilitar las **Contraseñas de administrador y usuario**, haga clic en el cuadro junto a **Habilitar contraseñas de administrador y usuario' (Enable Admin and User Passwords)** y seleccione **Siguiente (Next)** una vez que se 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.

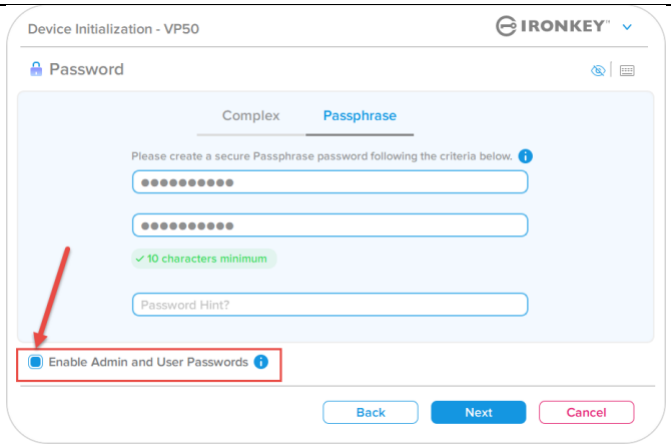



**Figura 4.12 - Habilitación de Contraseñas de administrador y usuario**

**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 característica del Administrador.** Esta configuración se referirá como **Modo de solo usuario** a lo largo de este manual.

Para continuar con la configuración de un Usuario único, Contraseña única, mantenga **Habilitar Contraseñas de administrador y usuario (Enable Admin and User passwords)** desmarcadas y haga clic en **Siguiente (Next)** después de crear una contraseña válida.

**Nota:** Las **Contraseñas de administrador y usuario'** se denominarán como **Rol de administrador'** para el resto de este documento.

## 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** (Figura 4.13). La Contraseña de usuario tendrá capacidades limitadas en comparación con la de Administrador y se analizará con más detalle más adelante en esta Guía del usuario. (ver página 23)

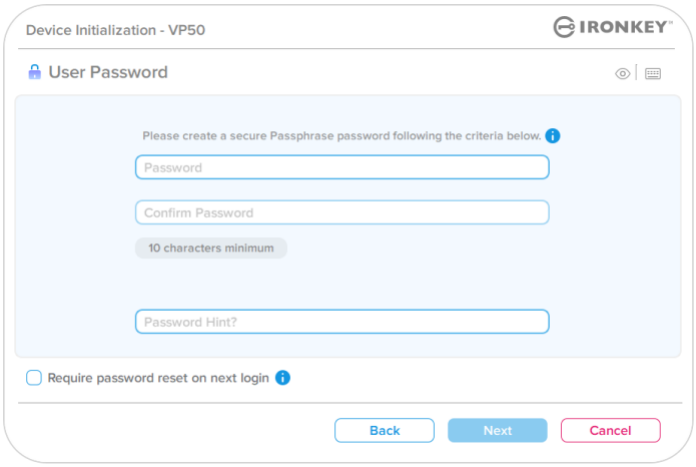



**Figura 4.13 - Contraseña de usuario (administrador y usuario habilitado)**

**Nota:** Los criterios de Opción de contraseña elegidos (Compleja o Frase de acceso) se transferirán a la Contraseña de usuario, Recuperación de contraseña de una sola vez 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.

- La función de **Requerir el restablecimiento de la contraseña en el próximo inicio de sesión' (Require password reset on next login)** en el botón en la esquina inferior izquierda de la **Figura 4.13** es solo para la Contraseña de usuario y se puede habilitar para forzar al Usuario a iniciar sesión con la contraseña temporal establecida por el Administrador durante el proceso de inicialización, para luego cambiarla por una contraseña de su elección después de que el dispositivo se autentifique con la contraseña temporal. Esto es útil cuando el dispositivo se entrega a otra persona para que la use. **(Figura 4.14)**

  **Nota:** Por seguridad, la nueva contraseña no puede ser la misma que la contraseña temporal.

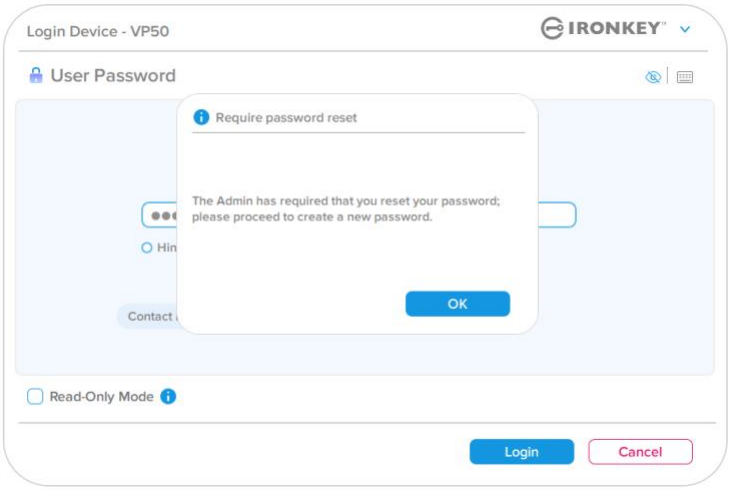


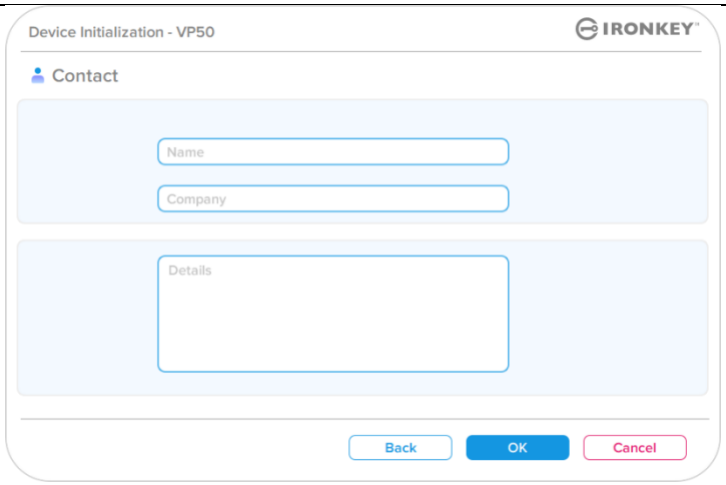

**Figura 4.14 - Requerir restablecimiento de contraseña en el próximo inicio de sesión**
**(Para contraseña de usuario)**

## Inicialización del dispositivo

### Información de contacto

Ingrese su información de contacto en los cuadros de texto proporcionados. (ver Figura 4,14)

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

| | |
|---|---|
| El campo de **'Nombre' (Name)** puede contener hasta 32 caracteres, pero no puede contener la contraseña **exacta**.<br><br>El campo de **'Compañía'** (**Company**) puede contener hasta 32 caracteres, pero no puede contener la contraseña **exacta**.<br><br>El campo de **'Detalles'(Details)** puede contener hasta 156 caracteres, pero no puede contener la contraseña **exacta**. |  <br>**Figura 4.14 - Información de contacto** |

**Nota:** Al hacer clic en 'Aceptar' (OK), 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.

## 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 VP50, 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 5.1). Al hacer clic en el 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 5.2)

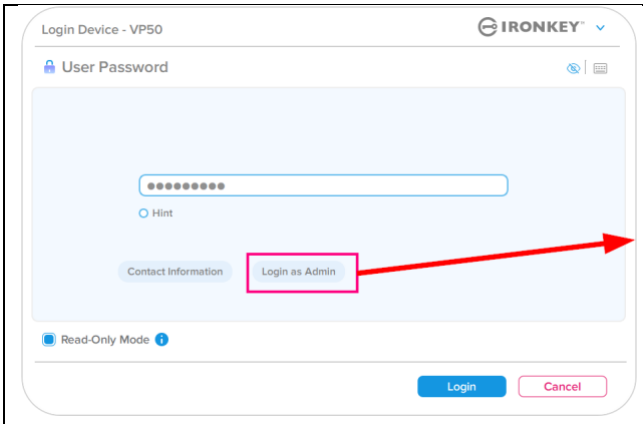



**Figura 5.1 - Inicio de sesión con Contraseña de usuario (Administrador habilitado)**

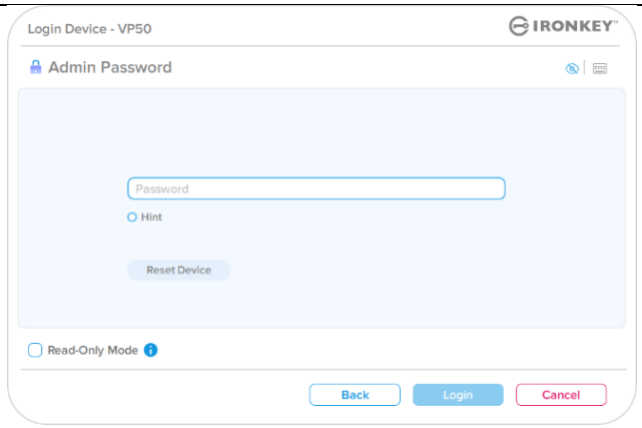



**Figura 5.2 - Inicio de sesión con Contraseña de administrador**

### 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, el dispositivo 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 5.3)

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

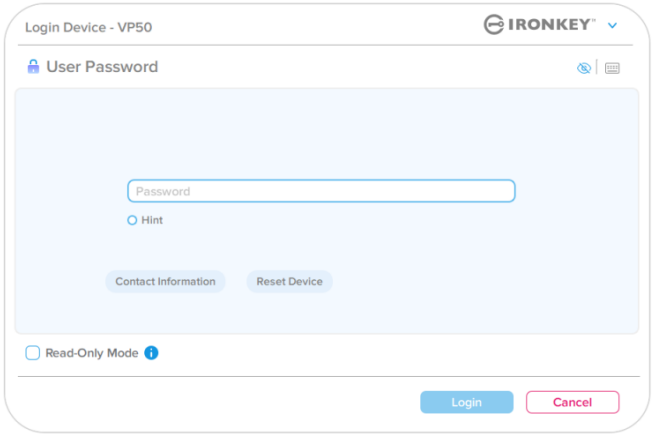



**Figura 5.3 - Inicio de sesión con contraseña de usuario (el Administrador no está habilitado)**

| | |
|---|---|
| **formatearán y perderán para siempre cuando se produzca un Restablecer el dispositivo.** | |

## Uso del dispositivo

### Desbloqueo en Modo de solo lectura

Puede desbloquear el dispositivo en un estado de solo lectura para que los archivos no se puedan alterar en el dispositivo IronKey. Por ejemplo, cuando se utiliza un equipo no confiable o desconocido, desbloquear el dispositivo en Modo de solo lectura evitará que cualquier malware en ese equipo infecte el dispositivo o modifique los archivos.

Al trabajar en este modo, no puede realizar ninguna operación que implique la modificación de archivos en el dispositivo.
Por ejemplo, no puede volver a formatear el dispositivo, restaurar, agregar o editar archivos en el dispositivo.

Para desbloquear el dispositivo en Modo de solo lectura:

1. Inserte el dispositivo en el puerto USB de la computadora huésped y ejecute el **IronKey.exe.**
2. Marque el **Modo de solo lectura (Read-Only Mode)** debajo del cuadro de ingreso de contraseña. **(Figura 5.4)**
3. Escriba la contraseña de su dispositivo y haga clic en **Iniciar sesión (Login).** La IronKey ahora se desbloqueará en el Modo de solo lectura.

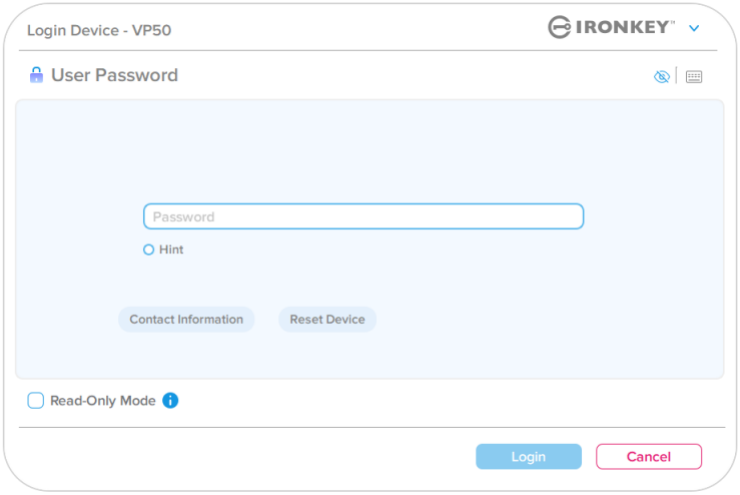



**Figura 5.4 - Modo de solo lectura**

Si desea desbloquear el dispositivo con acceso completo de lectura/escritura a una partición de datos segura, debe apagar el VP50 e iniciar sesión de nuevo, dejando la casilla de verificación 'Modo de solo lectura' (Read-Only Mode) sin marcar.

**Nota:** Las opciones de VP50 Admin cuentan con un Modo de solo lectura forzada para los Datos de usuario, lo que significa que el Administrador puede forzar al Inicio de sesión de usuario a desbloquearse en un estado de solo lectura (consulte la **página 28** para obtener más detalles).

## Uso del dispositivo

### Protección contra ataques de fuerza bruta

**Importante:** Durante el inicio de sesión, si se introduce una contraseña incorrecta, se le dará otra oportunidad para introducir la contraseña correcta; sin embargo, hay una función de seguridad integrada (también conocida como Protección contra ataques de fuerza bruta) que rastrea el número de intentos de inicio de sesión fallidos.*

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

| **Administrador/usuario habilitado** | **Protección contra fuerza bruta Comportamiento del dispositivo (10 Intentos de contraseña incorrecta)** | **¿Borrado de datos y restablecimiento del dispositivo?** |
|---|---|---|
| Contraseña de usuario | Bloqueo de la contraseña. Inicie sesión como Administrador o use la Contraseña de recuperación de una sola vez para restablecer la contraseña de usuario | NO |
| Contraseña de administrador | Dispositivo de borrado criptográfico, Contraseñas, configuraciones y datos borrados para siempre | **SÍ** |
| Contraseña de recuperación de una sola vez | Bloqueo de contraseña, el botón de Recuperar contraseña se pondrá gris y se volverá inutilizable. Inicie sesión como Administrador para Restablecer la contraseña | NO |
| **Solo usuario Usuario único, Contraseña única (Administrador/Usuario NO habilitado)** | **Protección contra fuerza bruta Comportamiento del dispositivo (10 Intentos de contraseña incorrecta)** | **¿Borrado de datos y restablecimiento del dispositivo?** |
| Contraseña de usuario | Dispositivo de borrado criptográfico, Contraseñas, configuraciones y datos borrados para siempre | **SÍ** |

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

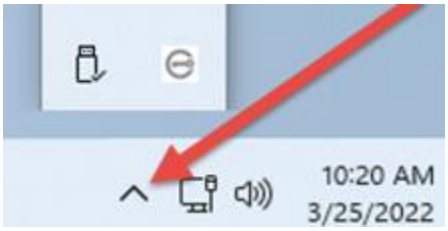
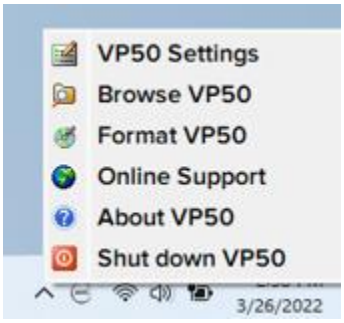
### Accesando a mis archivos seguros

Después de desbloquear el dispositivo puede acceder a sus archivos seguros. Los archivos se encriptan y desencriptan automáticamente cuando los guarda o abre en el dispositivo. Esta tecnología le brinda la comodidad

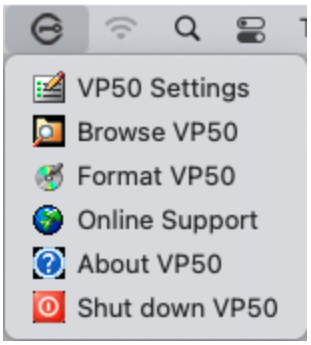
de trabajar como lo haría normalmente con un dispositivo regular, al tiempo que proporciona una seguridad sólida y "siempre activa".
**Pista:** También puede acceder a sus archivos haciendo clic con el botón derecho en el **icono de IronKey** en la barra de tareas de Windows y haciendo clic en **Examinar el VP50 (Browse VP50)**. (Figura 6.2)

## Opciones del dispositivo - (Entorno Windows)

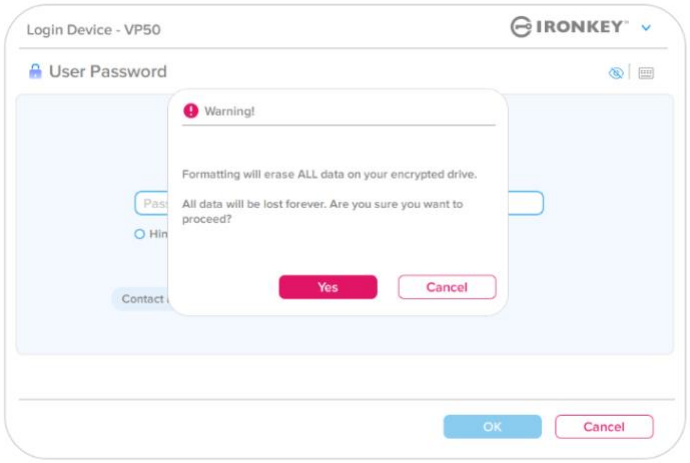
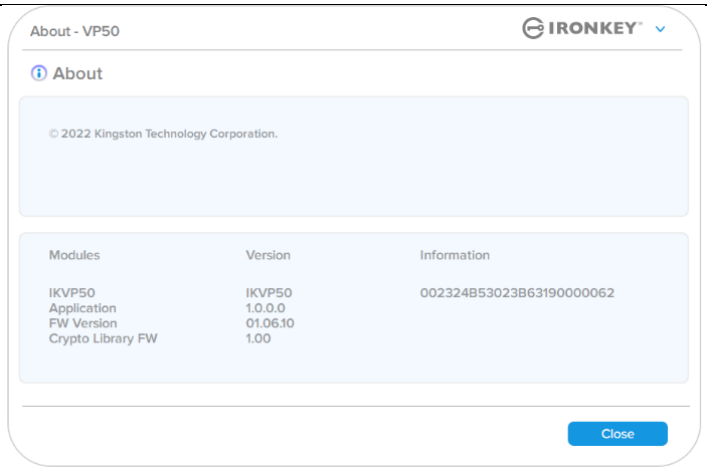
Mientras esté conectado al dispositivo, habrá un icono de IronKey ubicado en la esquina derecha de la ventana. Al hacer clic con el botón derecho en el icono de IronKey se abrirá el menú de selección de Opciones de dispositivo disponibles. (Figura 6.2)
Los detalles sobre estas opciones de dispositivo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

| | |
|---|---|
| • Mientras esté conectado al dispositivo, habrá un icono de IronKey ubicado en la esquina derecha de la ventana. **(Figura 6.1)** |  **Figura 6.1 - 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 de Opciones de dispositivo disponibles. **(Figura 6.2)**<br><br>Los detalles sobre estas opciones de dispositivo se pueden encontrar en las páginas 19-23 de este manual. |  **Figura 6.2 - Icono IronKey con el botón derecho para las opciones del dispositivo** |

## Opciones del dispositivo - (Entorno macOS)

| | |
|---|---|
| • Mientras esté conectado al dispositivo, encontrará un icono IronKey VP50 ubicado en el menú macOS que se ve en la **Figura 6.3** que abrirá las opciones disponibles del dispositivo.<br><br>Los detalles sobre estas opciones de dispositivo se pueden encontrar en las páginas 19-23 de este manual. |  **Figura 6.3 - Menú de opciones de Icono/Dispositivo de la barra de menú macOS** |

## Opciones de dispositivo

| | |
|---|---|
| **Configuración del VP50 (VP50 Settings):** | • 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 VP50' de este manual). |
| **Explorar el VP50 (Browse VP50):** | • Le permite ver sus archivos seguros. |
| **Formatear el VP50 (Format VP50):** Le permite formatear la partición de datos segura. (Advertencia: Se borrarán todos los datos) (**Figura 6.1**)<br><br>**Nota:** Se requerirá autentificación por contraseña para el proceso de reformateo. |  <br>**Figura 6.1 - Reformateo del VP50** |
| **Soporte en línea (Online Support):** | • Abra su navegador de Internet y navegue a http://www.kingston.com/support donde puede acceder a información de soporte adicional. |
| **Acerca del VP50 (About VP50):** Proporciona detalles específicos sobre el VP50, incluidos la información de la aplicación, el firmware y el número de serie. *(Figura 6.2)*<br><br>**Nota:** El número de serie único del dispositivo estará debajo de la **'**columna de información'. |  <br>**Figura 6.2 - Acerca del VP50** |
| **Apagar el VP50 (Shut down VP50):** | • Apaga correctamente el VP50, lo que le permite eliminarlo de forma segura de su sistema. |

# Configuración del VP50

## Configuración de administrador (Admin Settings)

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

- **Contraseña (Password):** Le permite cambiar su propia Contraseña de administrador y/o pista. (*Figure 7.1*)
- **Información de contacto (Contact Info):** Le permite agregar/ver/cambiar su información de contacto (*Figura 7.2*)
- **Idioma (Language):** Le permite cambiar su selección de idioma actual *(Figura 7.3)*
- **Opciones de Administrador (Admin Options):** Le permite habilitar funciones adicionales como: (Figura 7.4)
    - Cambiar la Contraseña de usuario
    - Restablecer contraseña de inicio de sesión (para Contraseña de usuario)
    - Habilitar la Contraseña de Recuperación de una sola vez
    - Forzar el Modo de solo lectura para los Datos de usuario

**NOTA:** Los detalles adicionales de las Opciones de administrador se pueden encontrar en la página 24.

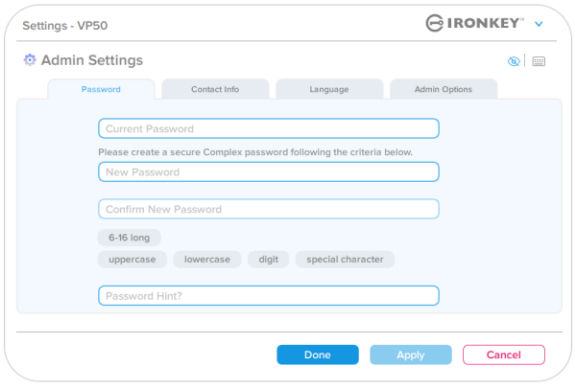



**Figura 7.1 - Opciones de contraseña**

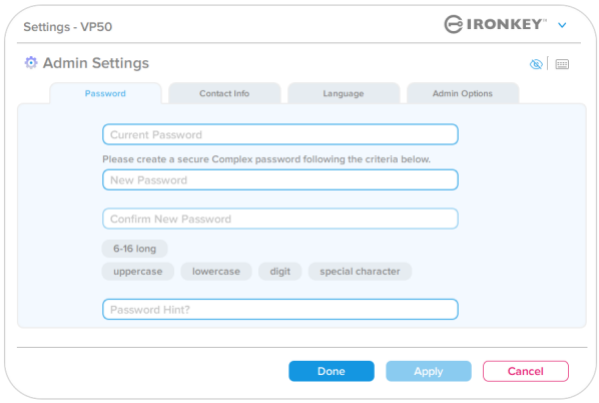



**Figura 7.2 - Información de contacto**

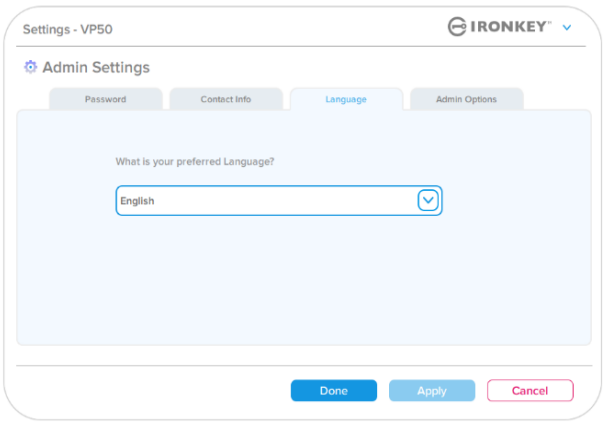



**Figura 7.3 - Opciones de idioma**

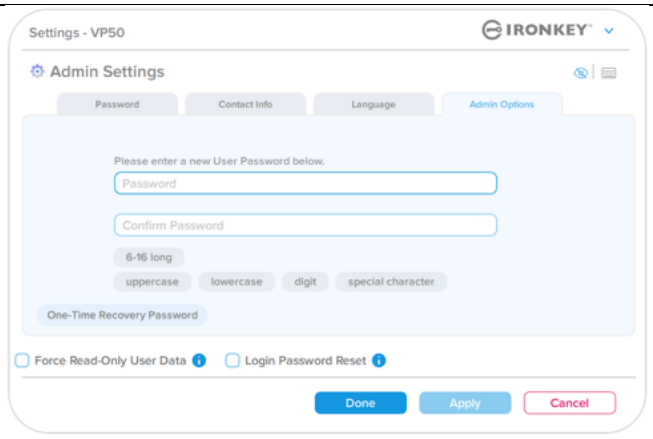
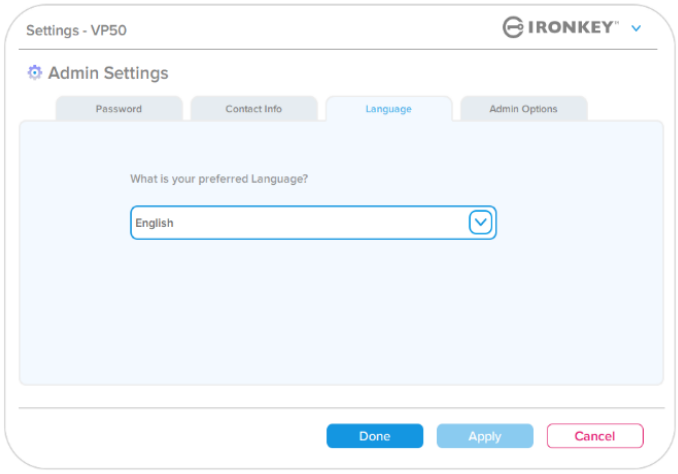
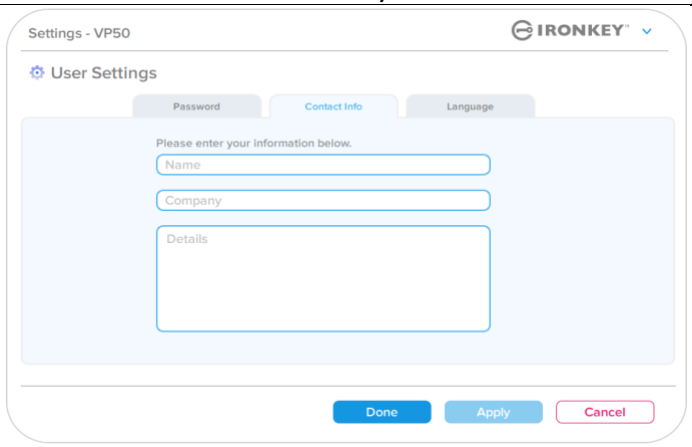
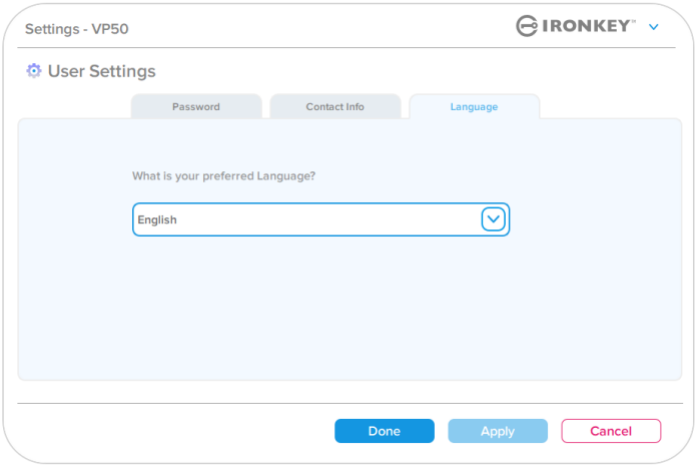



**Figura 7.4 - Opciones de Administrador**

## Configuración del VP50

### Configuración de usuario: Administrador habilitado

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

| | |
|---|---|
| **Contraseña (Password):**<br>Le permite cambiar su propia Contraseña de administrador y/o pista. *(Figura 7.5)* |  <br>**Figura 7.5 - Opciones de contraseña (Admin habilitado: Inicio de sesión de usuario)** |
| **Información de contacto (Contact Info):**<br>Le permite agregar/ver/cambiar su información de contacto. *(Figura 7.6)* |  <br>**Figura 7.6 - Información de contacto (Admin habilitado: Inicio de sesión de usuario)** |
| **Idioma (Language):**<br>Le permite cambiar su selección de idioma actual. *(Figura 7.7)* |  |

| | |
|---|---|
| | **Figura 7.7 - Configuración del idioma (Admin habilitado: Inicio de sesión de usuario)** |

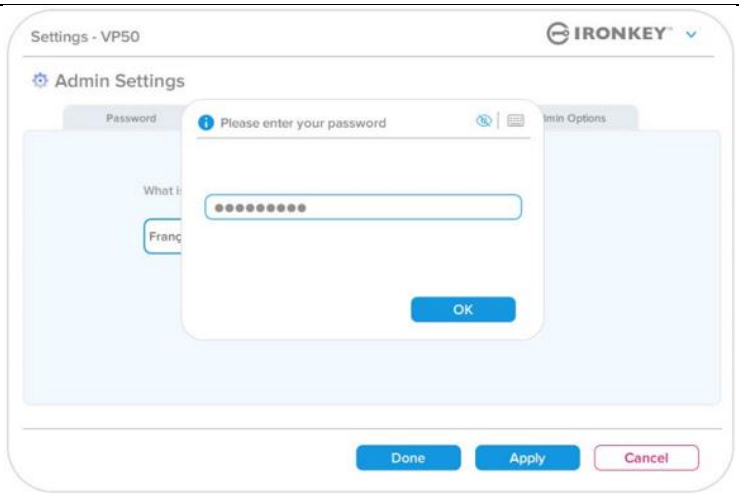
**Nota:** Las Opciones de administrador no son accesibles cuando se inicia sesión con la Contraseña de usuario.

## Configuración del VP50

### Configuración de usuario: Administrador no habilitado

Como se mencionó anteriormente en la página 12, la inicialización del VP50 sin habilitar las 'Contraseñas de administrador y usuario configurará 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 la siguiente configuración del VP50:

### Cambiar y guardar la configuración

| | |
|---|---|
| • Siempre que se cambien los ajustes en la Configuración del VP50 (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 7,11) |  <br>**Figura 7.11 - Pantalla de solicitud de contraseña para guardar los cambios de configuración de VP50** |

**Nota:** Si se encuentra en la pantalla de Solicitud de contraseña vista arriba 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 Ingrese su contraseña' y volverá al menú de configuración del VP50.

## Funciones de administrador

**Opciones disponibles para Restablecer la Contraseña de usuario**

Las funciones de la Configuración del administrador permiten múltiples formas de restablecer de forma segura la Contraseña de usuario, en caso de que se olvide, o si se crea una Contraseña de usuario temporal y desea forzar un cambio de contraseña en el próximo inicio de sesión para el Inicio de sesión de usuario. A continuación, se muestran las funciones que pueden ser útiles para Restablecer la contraseña de usuario:

**Restablecer contraseña de usuario:**

Cambie manualmente la Contraseña de usuario en el menú 'Opciones de administrador' (Admin Options), el cual es un cambio instantáneo y entrará en vigor en el próximo Inicio de sesión de usuario. **(Figura 8.1)**

**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).

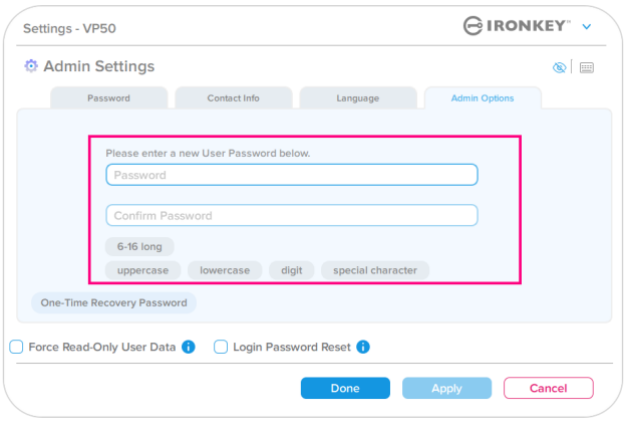



**Figura 8.1 - Opciones de administrador/Restablecer contraseña de usuario**

**Restablecimiento de contraseña de inicio de sesión:**

Habilitar el restablecimiento de contraseña de inicio de sesión **forzará al Usuario a iniciar sesión con una contraseña temporal establecida por el Administrador**, y luego cambiarla a una contraseña de su elección. Esto es útil cuando el dispositivo se entrega a otra persona para que la use. **(Ver Figuras 8.2A y 8.2B)**

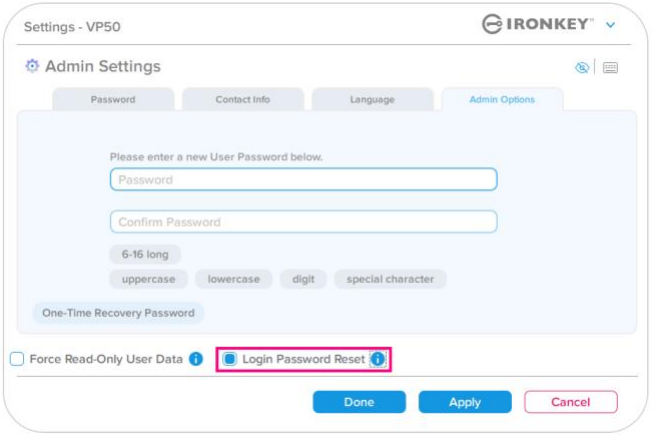



**Figura 8.2A - Botón de restablecer contraseñas de inicio de sesión**

**Nota:** La aplicación de este restablecimiento se llevará a cabo en el próximo Inicio de sesión de usuario exitoso. Los criterios de requisitos de la contraseña se aplicarán automáticamente de acuerdo con la opción original establecida durante el proceso de inicialización (opciones Complejo o Frase de acceso).

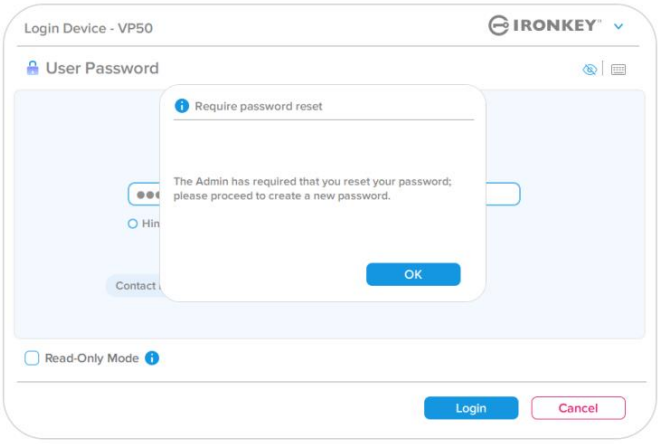



**Figura 8.2B - Restablecer notificación después de ingresar la Contraseña de usuario**

## Funciones de administrador

### Contraseña de recuperación de una sola vez

En esta sección se analizará el proceso para habilitar y utilizar la función de contraseña de recuperación de una sola vez.

**Contraseña de recuperación de una sola vez**

**Paso 1:** La función de Contraseña de recuperación de una sola vez, es la de una contraseña de un solo uso muy útil que se puede habilitar para ayudar a recuperar y restablecer la contraseña de usuario en caso de que se olvide la contraseña de usuario. Haga clic en el botón 'Contraseña de recuperación de una sola vez' (One-Time Recovery Password) en el Menú de opciones de administrador para comenzar a empezar. **(Figura 8.4)**

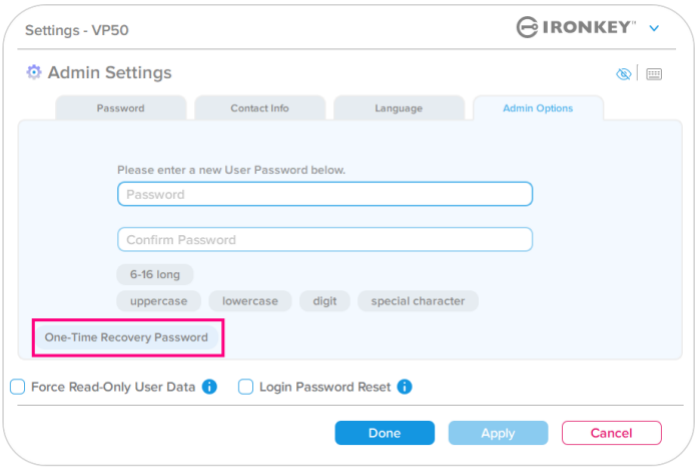



**Figura 8.4 - Botón de Contraseña de recuperación de una sola vez**

**Paso 2:** Cree una Contraseña de recuperación de una sola vez utilizando los mismos Criterios de contraseña con los que se configuró inicialmente el dispositivo (Complejo o Frase de acceso).

**Nota:** Se requerirá la Contraseña de administrador para aplicar los cambios.

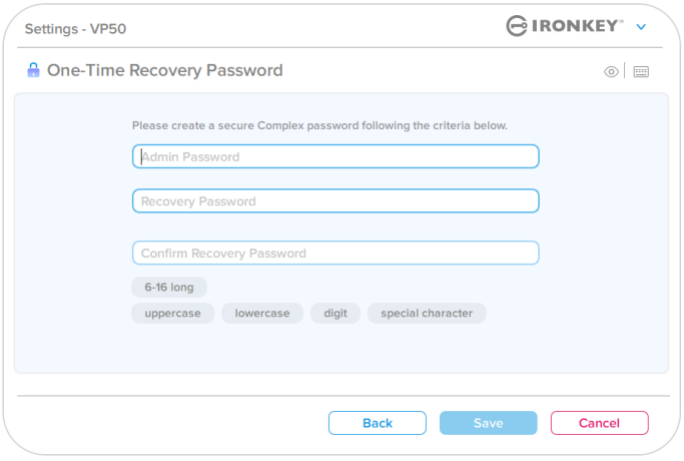
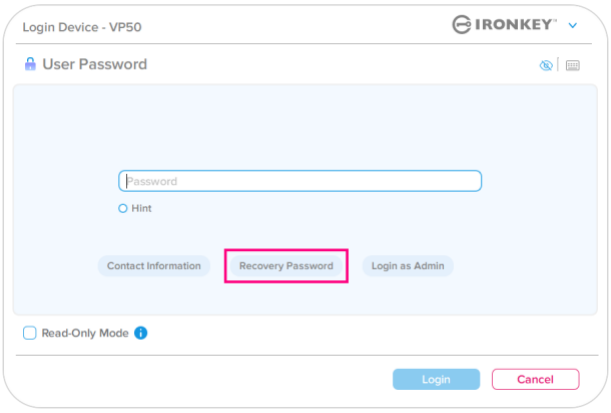
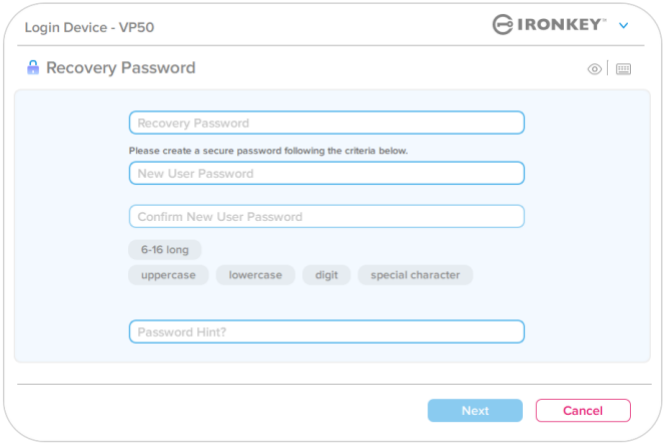
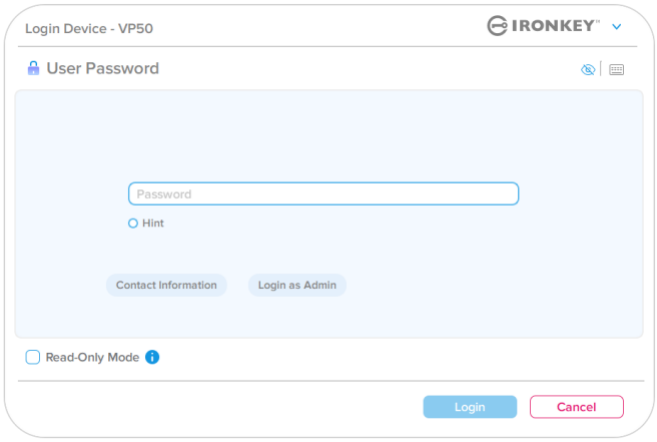



**Figura 8.5 - Configuración de la Contraseña de recuperación de una sola vez**

## Funciones de administrador

Usando la Contraseña de recuperación de una sola vez

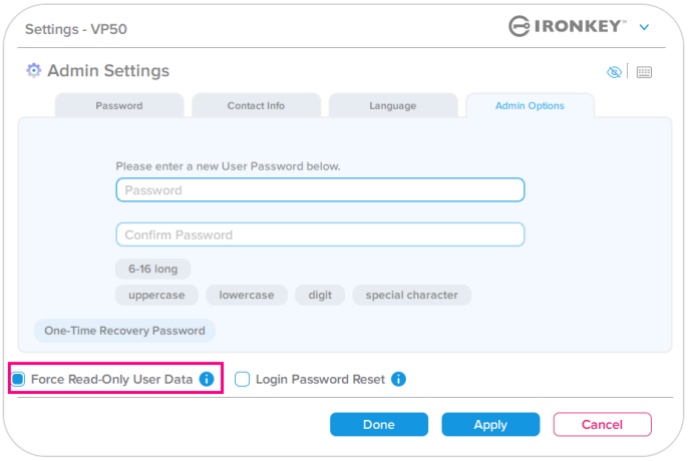
| | |
|---|---|
| **Paso 1:** Una vez que se haya creado la Contraseña de recuperación de una sola vez, aparecerá un nuevo botón en la pantalla de inicio de sesión de **Contraseña de usuario** en el próximo inicio de sesión. Haga clic en el botón **Recuperar contraseña (Recovery Password)** para iniciar el proceso. |  <br>**Figura 8.6 - Botón de recuperación de contraseña** |
| **Paso 2:** Aparecerá la pantalla Recuperar contraseña, donde puede ingresar la Contraseña de recuperación y crear una nueva contraseña de usuario. (Figura 8.7)<br><br>**Importante:** La Contraseña de recuperación de una sola vez también utiliza una función de seguridad integrada que rastrea el número de intentos de inicio de sesión fallidos, **después de 10 intentos de inicio de sesión incorrectos fallidos con la Contraseña de recuperación de una sola vez, la contraseña se desactivará** y tendrá que volver a habilitarse al iniciar sesión en el dispositivo como Administrador. (consulte las páginas 18 y 30 para obtener más detalles) |  <br>**Figura 8.7 - Menú de la Contraseña de recuperación** |

| | |
|---|---|
| **Paso 3:** Cuando tenga éxito, volverá a la pantalla **Contraseña de usuario**. El botón **Recuperar contraseña (Recovery Password)** ha desaparecido, y la Contraseña de usuario ingresada en el **Paso 2** se convertirá en la nueva Contraseña de usuario. (Figura 8.8) |  **Figura 8.8 - Pantalla de inicio de sesión de la Contraseña de usuario que muestra el botón Recuperar contraseña desaparecer después de un uso exitoso.** |

## Funciones de administrador

### Forzar datos de Usuario de solo lectura

La función de Modo de solo lectura forzada se puede habilitar para restringir el acceso de escritura al dispositivo del usuario. Esta función es útil si se necesitan archivos en el dispositivo para el acceso de solo lectura.

| | |
|---|---|
| • Para habilitar Forzar solo lectura para los Datos de usuario, haga clic en el cuadro y haga clic en 'Aplicar' (Apply). **(Figura 8.9)**<br><br>**Nota:** Este Modo de solo lectura forzado solo se aplica al Usuario y no afecta al Inicio de sesión de administrador. El Inicio de sesión de administrador seguirá teniendo privilegios de acceso de Lectura y Escritura, y aún puede habilitar el Modo de solo lectura si es necesario. |  **Figura 8.9 - Habilitar 'Forzar datos de Usuario de solo lectura' ('Force Read-Only User data)**<br>**(Se requerirá la Contraseña de administrador para aplicar los cambios)** |
| • Una vez habilitado, el cuadro de botón **'Modo de solo lectura' (Read-Only Mode)** estará en un color azul, lo que significa que el Modo de solo lectura forzada está habilitado permanentemente para la Contraseña | |

de usuario, hasta que el Administrador lo deshabilite. (Figura 8.10)

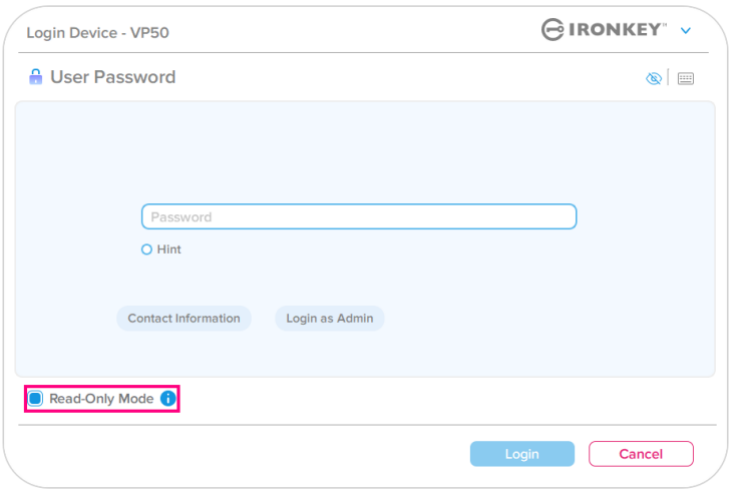



**Figura 8.10 - El Modo de solo lectura está habilitado por fuerza para el Usuario y solo puede ser deshabilitado por el Administrador**

## Ayuda y resolución de problemas

### Bloqueo del dispositivo

El VP50 incluye una función de seguridad que impide el acceso no autorizado a la partición de datos una vez que se ha realizado un número máximo de intentos fallidos **consecutivos** de inicio de sesión (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/Contraseña de recuperación de una sola vez).

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

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

**2.** 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 9.1)

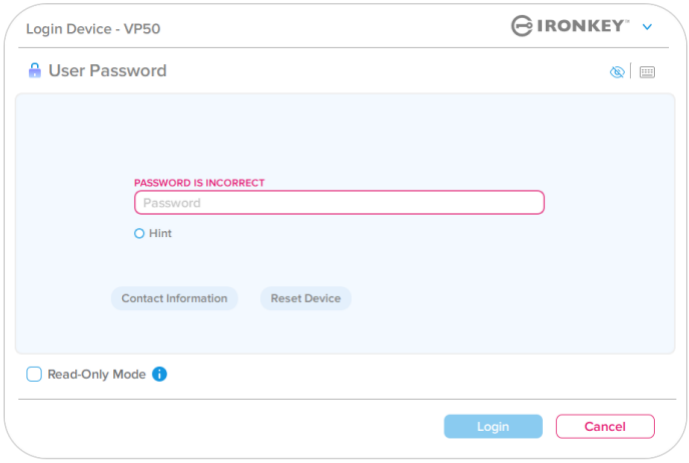



**Figura 9.1 - Mensaje de Contraseña incorrecta**

- Cuando se realiza un **séptimo** intento fallido, verá un mensaje de error adicional que indica que le quedan 3 intentos antes de alcanzar MaxNoA (que se establece en 10 por defecto). (Figura 9.2)

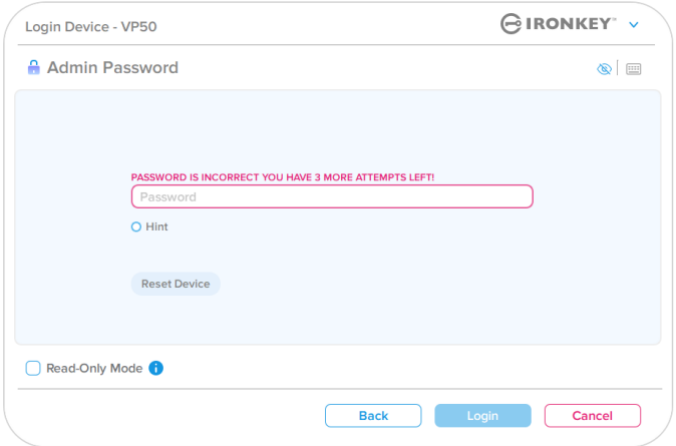



**Figura 9.2 - séptimo intento incorrecto de contraseña**

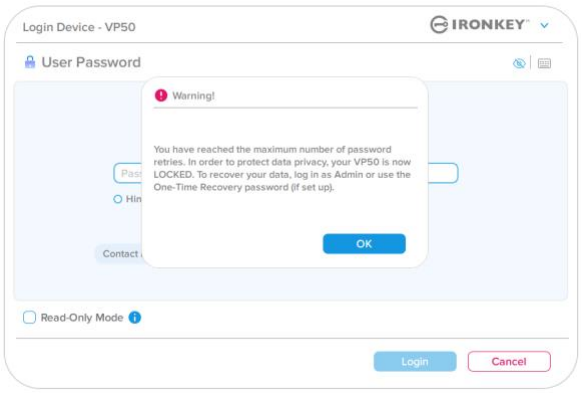
## Ayuda y resolución de problemas

### Bloqueo del dispositivo

**Importante:** Después de un décimo y último intento fallido de inicio de sesión, dependiendo de cómo se haya configurado el dispositivo y del método de inicio de sesión utilizado (administrador, usuario o contraseña de recuperación única), el dispositivo se bloqueará, requiriendo que se inicie sesión con un método alternativo (si es aplicable), o un restablecimiento del dispositivo que **formateará los datos y todos los datos del dispositivo se perderán para siempre.** Los comportamientos también se mencionan en la página 18 de esta Guía del usuario.

Las Figuras 9.3- 9.6 a continuación demuestran el comportamiento visual para el décimo y último inicio de sesión fallido de cada método de contraseña de inicio de sesión:

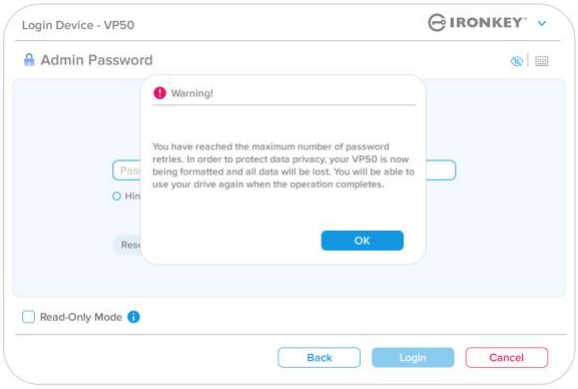
**Contraseña de usuario: (Administrador/usuario habilitado)**




**BLOQUEO DEL DISPOSITIVO**

**(Figura 9.3)**

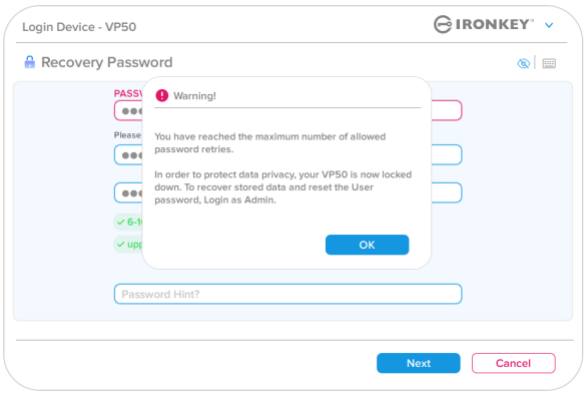
**Contraseña de administrador (Administrador/Usuario habilitado)**




**REFORMATEO DEL DISPOSITIVO ***

**(Figura 9.4)**

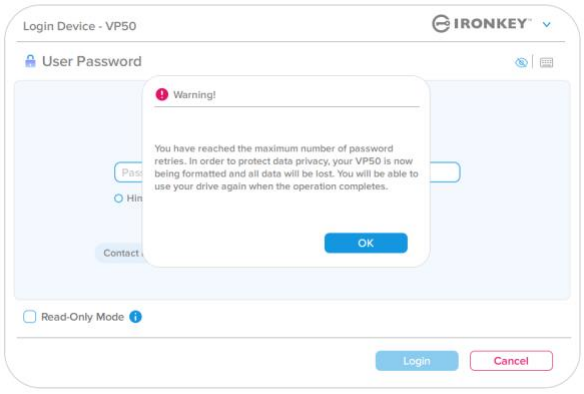
**Recuperación de una sola vez: (Administrador/usuario habilitado)**




**BLOQUEO DEL DISPOSITIVO**

**(Figura 9.5)**

**Contraseña de usuario (Administrador NO habilitado)**




**REFORMATEO DEL DISPOSITIVO ***

**(Figura 9.6)**

Estas medidas de seguridad limitan que alguien (que no tiene 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 VP50 y ha olvidado su contraseña, se aplicarán las mismas medidas de seguridad,

incluido un reformateo de dispositivo. * Para obtener más información sobre esta función, consulte *'Restablecer dispositivo'* en la página 25.

**Nota: Un reformateo del dispositivo borrará TODA la información almacenada en la partición de datos segura del VP50.*

## Ayuda y resolución de problemas

### Restablecer dispositivo

Si olvida su contraseña o necesita restablecer su dispositivo, puede hacer clic en el botón 'Restablecer dispositivo' (*Reset Device*) que aparece en uno de dos lugares dependiendo de cómo se configura el dispositivo (ya sea en el menú de Contraseña de Inicio de sesión de administrador si Administrador/usuario está habilitado, o en el en el Menú de inicio de sesión de la 'Contraseña de usuario' (User Password), si el modo Admin/Usuario no está habilitado) cuando se ejecuta el lanzador del VP50. (ver **Figura 9.7** y **9.8**)

- Esta opción le permitirá crear una nueva contraseña, pero para proteger la privacidad de sus datos, el VP50 se formateará. Esto significa que todos sus datos se borrarán en el proceso.*

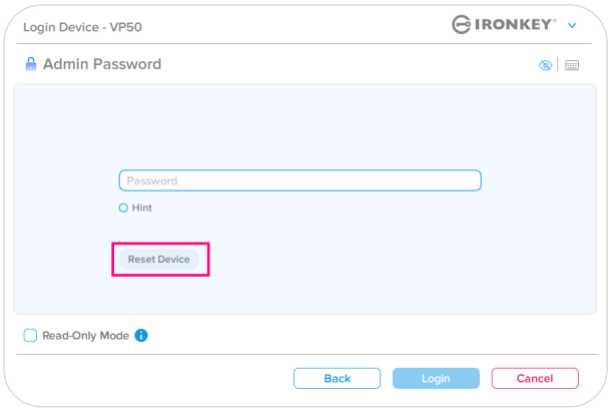



**Figura 9.7 - Contraseña de administrador: Botón de Restablecer dispositivo (Reset Device)**

- **Nota:** Cuando haga clic en 'Restablecer dispositivo' (Reset Device), aparecerá un cuadro de mensaje y preguntará si desea introducir una nueva contraseña antes de ejecutar el formateo. En este punto, puede hacer 1) clic en 'Aceptar' (OK) para confirmar o 2) hacer clic en 'Cancelar' (Cancel) para volver a la ventana de inicio de sesión. (Ver Figura 9,8)

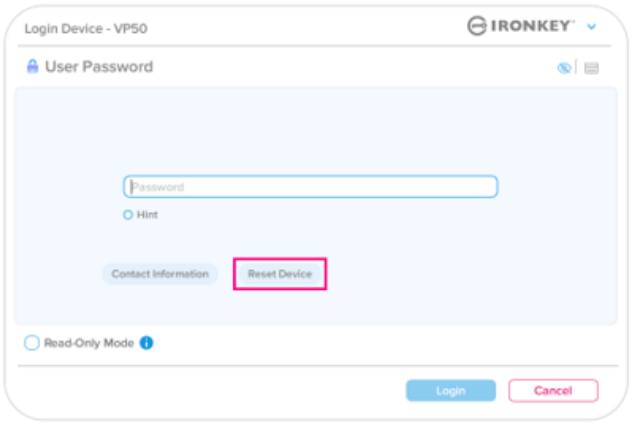



**Figura 9.8 - Contraseña de usuario (Administrador/Usuario no habilitado) Restablecer dispositivo**

- 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 (Complejo o Frase de acceso). La pista no es un campo obligatorio, pero puede ser útil para proporcionar una pista sobre la contraseña en caso de que se olvide.

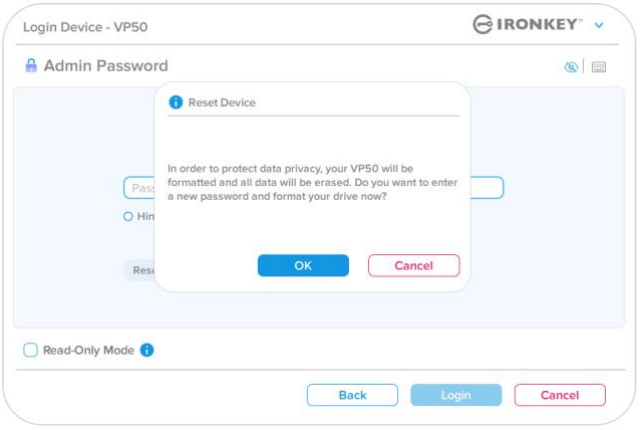



**Figura 9.9 - Confirmación de restablecimiento del dispositivo**

## Ayuda y resolución de problemas

### Conflicto con letras de unidad: Sistemas operativos Windows

- Como se menciona en la sección 'Requisitos del sistema' de este manual (en la página 3), el VP50 requiere dos letras de unidad consecutivas DESPUÉS del último disco físico que aparece antes del 'espacio' en la asignación de letras de unidad (véase la figura 9.10). Esto NO se refiere a los recursos compartidos de red, ya que estos son específicos de los perfiles de usuario y no del perfil de hardware del sistema en sí, por lo que aparecen disponibles para el sistema operativo.

- Lo que esto significa es que Windows puede asignar al VP50 una letra de unidad que ya está en uso por un recurso de red o una ruta de la Convención de Nombramiento Universal (UNC), lo que provoca un conflicto de letras de unidad. Si esto sucede, consulte a su administrador o al departamento del servicio de asistencia sobre cómo cambiar las asignaciones de letras de la unidad en la Administración de discos de Windows (se requieren privilegios de administrador). Como se menciona en la sección 'Requisitos del sistema' de este manual (en la página 3), el VP50 requiere dos letras de unidad consecutivas DESPUÉS del último disco físico que aparece antes del 'espacio' en la asignación de letras de unidad (véase la figura 9.10). Esto NO se refiere a los recursos compartidos de red, ya que estos son específicos de los perfiles de usuario y no del perfil de hardware del sistema en sí, por lo que aparecen disponibles para el sistema operativo.

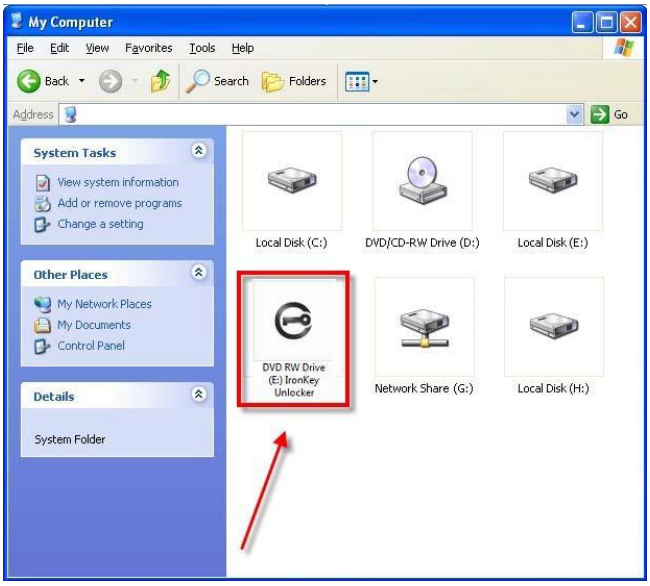



**Figura 9.10 - Ejemplo de letra de unidad**

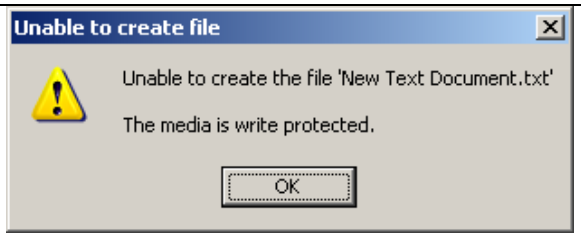
En este ejemplo (Figura 9.10), el VP50 utiliza la unidad F:, que es la primera letra de unidad disponible después de la unidad E: (el último disco físico antes del espacio entre letras de la unidad). Debido a que la letra G: es un recurso compartido de red y no forma parte del perfil de hardware, el VP50 puede intentar usarla como su segunda letra de unidad, lo que causa un conflicto.

Si no hay recursos compartidos de red en su sistema y el VP50 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 el 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.

## Ayuda y resolución de problemas

### Mensajes de error

| | |
|---|---|
| **No se puede crear archivo:**<br>Este mensaje de error aparecerá cuando intente crear un archivo o carpeta eb la partición de datos segura mientras está conectado en modo de solo lectura. |  <br>**Figura 9.11 - No se puede crear, Error de archivo** |
| **Error al copiar archivo o la carpeta:**<br>Este mensaje de error aparecerá cuando intente COPIAR un archivo o carpeta a la partición de datos segura mientras está conectado en modo de solo lectura. |  <br>**Figura 9.12 - Error al copiar el archivo o carpeta** |
| **Error al borrar archivo o la carpeta:**<br>Este mensaje de error aparecerá al intentar BORRAR un archivo o carpeta de la partición de datos segura mientras se inicia sesión en modo de solo lectura. |  <br>**Figura 9.13 - Error al borrar archivo o carpeta** |

**Nota:** Si siempre se accede en modo de sólo lectura y desea desbloquear el dispositivo con acceso completo de lectura/escritura a la partición de datos segura, debe apagar el VP50 e iniciar sesión de nuevo, dejando la casilla de verificación 'Modo de solo lectura' (Read-Only Mode) sin marcar.

# IRONKEY™ Vault Privacy 50 (VP50)
# VERSCHLÜSSELTER USB 3.2 Gen 1-STICK

*Anleitung*

## Inhalt


Abb. 1: IronKey VP50

## Einführung

Der Kingston IronKey Vault Privacy 50 (VP50) ist ein Premium-USB-Stick, der mit einer FIPS 197-zertifizierten AES-256-Bit-Hardwareverschlüsselung im XTS-Modus Sicherheit für Unternehmen bietet, einschließlich Schutzmaßnahmen gegen BadUSB mit digital signierter Firmware und gegen Brute-Force-Passwortangriffe. VP50 ist außerdem TAA-konform und wird in den USA montiert. Da es sich um eine verschlüsselte Speicherung unter der physischen Kontrolle des Benutzers handelt, ist die VP50 Serie bei der Datensicherung der Nutzung von Internet und Cloud-Diensten überlegen.

Der VP50 unterstützt Mehrfach-Passwort-Optionen (Admin, Benutzer und einmalige Wiederherstellung) mit den Modi Komplex oder Passphrase. Die Mehrfach-Passwort-Option verbessert die Möglichkeiten, den Zugriff auf die Daten wiederherzustellen, wenn eines der Passwörter vergessen wurde. Der neue Passphrase-Modus unterstützt nicht nur herkömmliche komplexe Passwörter, sondern auch numerische PINs, Sätze, Wortlisten oder sogar Liedtexte mit 10 bis 64 Zeichen. Der Administrator kann einen Benutzer und ein einmaliges Wiederherstellungs-Passwort aktivieren oder das Benutzer-Passwort zurücksetzen, um den Datenzugriff wiederherzustellen.

Zur Erleichterung der Passworteingabe kann das Symbol „Auge“  aktiviert werden, um das eingegebene Passwort anzuzeigen und Tippfehler zu vermeiden, die zu fehlgeschlagenen Anmeldeversuchen führen. Der Schutz vor Brute-Force-Angriffen sperrt Benutzer- oder einmalige Wiederherstellungs-Passwörter, wenn 10 ungültige Passwörter hintereinander eingegeben werden, und löscht den USB-Stick unwiederbringlich, wenn das Admin-Passwort 10 Mal hintereinander falsch eingegeben wird.

Zum Schutz vor potenzieller Malware auf nicht vertrauenswürdigen Systemen können sowohl der Administrator als auch der Benutzer den Schreibschutz für den USB-Stick aktivieren. Außerdem schützt die integrierte virtuelle Tastatur Passwörter vor Key- und Screenloggern.

Durch ihre FIPS 197-Zertifizierung und die TAA-Konformität können Unternehmen die USB-Sticks der VP50 Serie mit einer Produkt-ID (PID) für die Integration mit Standard-Endpoint-Management-Software anpassen und konfigurieren und somit die IT- und Cybersicherheits-Anforderungen des Unternehmens mithilfe Kingstons Personalisierungsprogramm erfüllen.

Kleine und mittlere Unternehmen können die Admin-Rolle zur lokalen Verwaltung ihrer USB-Sticks verwenden, z. B. zum Konfigurieren oder Zurücksetzen von Benutzer- oder einmaligen Wiederherstellungs-Passwörtern von Mitarbeitern, zur Wiederherstellung des Datenzugriffs auf gesperrten USB-Sticks und zur Einhaltung von Gesetzen und Vorschriften, wenn forensische Untersuchungen erforderlich sind.

Der VP50 wird durch eine 5-Jahres-Garantie mit kostenlosem technischen Kingston Support unterstützt.

**IronKey Vault Privacy 50 Funktionen**

- FIPS 197-zertifiziert, mit XTS-AES 256-Bit-Hardwareverschlüsselung (die Verschlüsselung kann niemals ausgeschaltet 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
- Zwei Schreibschutz-Einstellungen zum Schutz des USB-Sticks vor Änderungen oder Malware
- Kleine und mittlere Unternehmen können USB-Sticks mit der Admin-Rolle lokal verwalten
- Windows- oder macOS-kompatibel (Details siehe Datenblatt)

## Über diese Bedienungsanleitung

Dies ist die Bedienungsanleitung für den IronKey Vault Privacy 50 (VP50), sie basiert auf dem Produktbild, ohne Personalisierungen.

## Systemvoraussetzungen

| | |
|---|---|
| **PC-Plattform**<br>• Intel, AMD & Apple M1 SOC<br>• 15MB freier Festplattenspeicher<br>• Freier USB 2.0 – 3.2-Anschluss<br>• Zwei freie, aufeinanderfolgende Laufwerksbuchstaben nach dem letzten physischen Speicher*<br><br>***Hinweis:** Siehe „Laufwerksbuchstabenkonflikt“ auf Seite 32. | **Unterstützte PC-Betriebssysteme**<br>• Windows 11<br>• Windows 10<br>• Windows 8,1 |
| **Mac Plattform**<br>• 15MB freier Festplattenspeicher<br>• USB 2.0 – 3.2 Anschluss | **Unterstützte Mac-Betriebssysteme**<br>• macOS X (v. 10.13.x – 12.x.x) |

## Empfehlungen

Um eine ausreichende Stromversorgung des VP50 sicherzustellen, schließen Sie ihn direkt in einen USB-Anschluss Ihres Notebooks oder PCs an, siehe ***Abb. 1.1***. Schließen Sie den VP50 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 VP50 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 VP50 auf einem Zielsystem eingerichtet und verwendet wird.
- Wenn der USB-Stick in einem öffentlichen oder unbekannten System verwendet wird, sollte der Schreibschutz-Modus auf dem Gerät aktiviert sein, damit der Stick vor Malware geschützt ist.
- Den Stick sperren, wenn er nicht benutzt wird.
- Den USB-Stick trennen, bevor er herausgezogen wird.
- Den Stick niemals herausziehen, wenn die LED leuchtet. Denn dadurch kann der USB-Stick beschädigt und eine Neuformatierung erforderlich werden, wodurch Ihre Daten unwiederbringlich gelöscht werden.
- Das Passwort des USB-Sticks niemals an Dritte weitergeben.

### Nach den neuesten Updates und Informationen suchen.

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

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

## Bewährte Praktiken für die Passwort-Einrichtung

Der VP50 ist mit starken Sicherheitsvorkehrungen ausgestattet. 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 VP50 automatisch die verschlüsselten Daten unwiederbringlich und formatiert sich selbst zurück auf den Werkszustand.

**Mehrfach-Passwort**
Der VP50 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 VP50 drei verschiedene Passwörter unterstützen, die Sie zur Wiederherstellung von Daten verwenden können – Admin, Benutzer und das einmalige Wiederherstellungs-Passwort.

Der VP50 bietet Ihnen die Auswahl von zwei Hauptpasswörtern – ein Administrator-Passwort (als Admin-Passwort bezeichnet) und ein Benutzer-Passwort. Der Administrator kann jederzeit auf den USB-Stick zugreifen und Optionen für den Benutzer einrichten, der Administrator ist damit so etwas wie ein Superuser. Darüber hinaus kann der Administrator ein einmaliges Wiederherstellungs-Passwort für den Benutzer einrichten, um ihm die Möglichkeit zu geben, sich anzumelden und das Benutzer-Passwort zurückzusetzen.

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. Das Laufwerk kann dann wieder so eingerichtet werden, dass es 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. Der Benutzer kann das einmalige Wiederherstellungs-Passwort verwenden, um das Benutzer-Passwort bei Bedarf zurückzusetzen.

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 VP50 kann zurückgesetzt und wieder verwendet werden, aber die vorherigen Daten werden für immer gelöscht.

**Passwort-Modi**
Der VP50 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**
VP50 unterstützt Passphrasen mit 10 bis 64 Zeichen. Eine Passphrase folgt keinen 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 VP50-Laufwerk kann die Sprache des Passworts mit der für den USB-Stick gewählten Sprache übereinstimmen. So können mehrere Wörter, eine Phrase, ein 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.

- Benutzern von Windows 8.1/10/11 wird eine Meldung über die Gerätetreiber-Installation 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 nachfolgenden Abbildung ist der Laufwerksbuchstabe (E:).

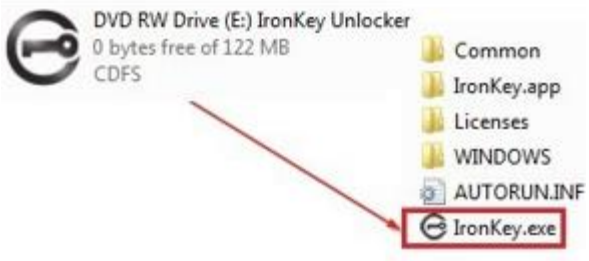



**Abb. 3.2 – Datei-Explorer Windows/IronKey.exe**

### Gerätezugriff (macOS-Umgebung)

Stecken Sie den VP50 in einen freien USB-Anschluss Ihres Notebooks oder Desktops ein und warten Sie, bis das Mac-Betriebssystem ihn erkannt hat. Wenn dies der Fall ist, erscheint IKVP50 (oder IRONKEY) auf dem Desktop. (Abb. 3.3)

- Doppelklicken Sie auf das CD-ROM-Symbol des IronKey.

- Doppelklicken Sie dann auf das Symbol der IKVP50-App (oder IronKey.app), das in dem in der Abb. 3.3 dargestellten Fenster angezeigt wird. Dadurch wird der Installationsprozess gestartet.

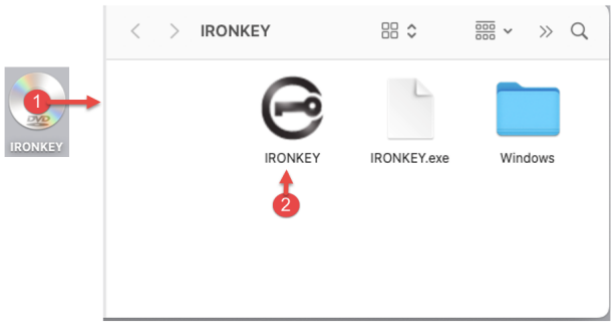
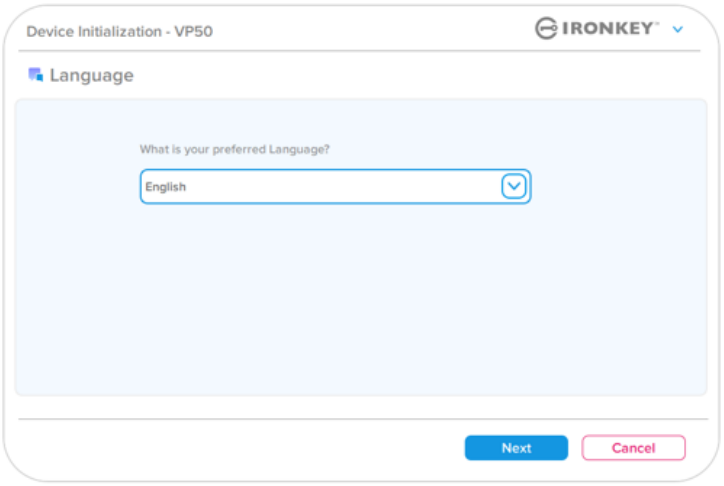
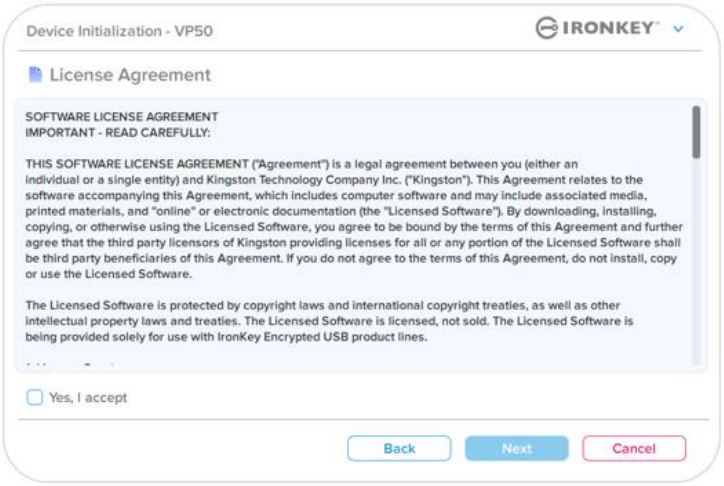



**Abb. 3.3 – IKVP-Laufwerk**

## Geräteinitialisierung (Windows- und macOS-Umgebung)

### Sprache und EULA

| | |
|---|---|
| Wählen Sie die von Ihnen gewünschte Sprache aus dem Dropdown-Menü aus und klicken Sie auf **Weiter (Next)**. (Siehe Abb. 4,1) |  <br>**Abb. 4.1 – Sprachauswahl** |
| Lesen Sie die Lizenzvereinbarung und klicken Sie auf **Weiter (Next)**.<br><br>Hinweis: Die Schaltfläche **Weiter (Next)** wird erst aktiviert, nachdem Sie die Lizenzvereinbarung akzeptiert haben. (Abb. 4.2) |  <br>**Abb. 4.2 – Lizenzvereinbarung** |

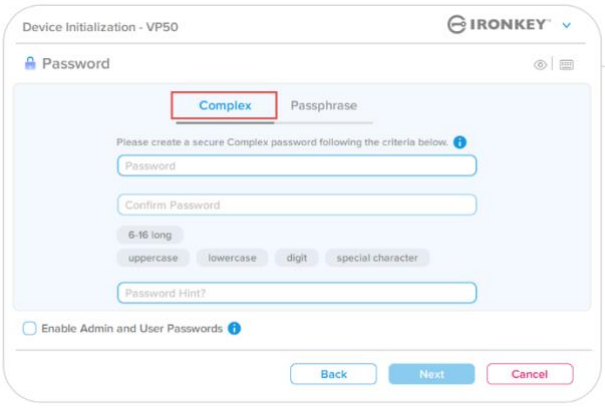
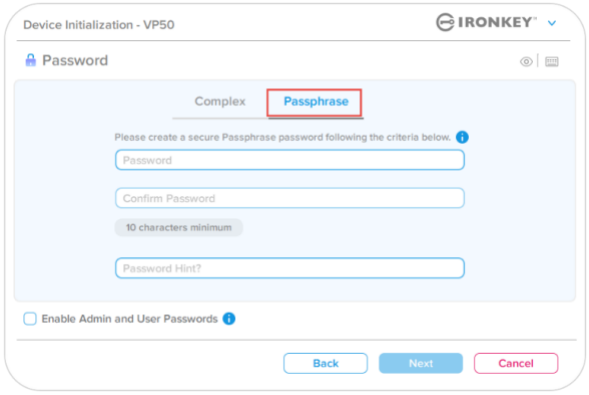
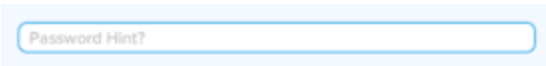
## Geräteinitialisierung

### Passwort-Auswahl

Auf dem Bildschirm der Passwortabfrage können Sie ein Passwort erstellen, um die Daten auf dem VP50 zu schützen, indem Sie entweder den Passwortmodus „Komplex (Complex)“ oder „Passphrase“ verwenden (Abbildungen 4.3 – 4.4). Darüber hinaus können Sie auf diesem Bildschirm auch die Mehrfach-Passwort-Admin/Benutzer-Optionen aktivieren. Bevor Sie mit der Auswahl des Passworts fortfahren, lesen Sie bitte den Abschnitt „Aktivieren von Admin-/Benutzer-Passwörtern“ unten, um diese Funktionen besser zu verstehen.

**Hinweis:** Sobald der Modus „Komplex“ oder „Passphrase“ ausgewählt wurde, kann der Modus nicht mehr geändert werden, es sei denn, der Stick wird zurückgesetzt.

Erstellen Sie zu Beginn der Passwortauswahl Ihr Passwort im Feld „Passwort“ und geben Sie es dann erneut in das Feld „Passwort bestätigen“ ein. Bevor Sie mit der Installationseinrichtung fortfahren können, müssen Sie ein Passwort nach folgenden Kriterien erstellen:

| | |
|---|---|
| **Komplexes Passwort**<br>• Muss mindestens 6 Zeichen lang sein (bis zu 16 Zeichen).<br>• Muss 3 (drei) der folgenden Kriterien enthalten:<br>○ Großbuchstabe<br>○ Kleinbuchstabe<br>○ Zahl<br>○ Sonderzeichen (!,$,& usw.) |  <br>**Abb. 4.3 – Komplexes Passwort** |
| **Passwort als Passphrase**<br>• Muss enthalten:<br>○ Minimal 10 Zeichen<br>○ Maximal 64 Zeichen |  <br>**Abb. 4.4 – Passphrasen-Passwort** |
| **Passwort-Hinweis (optional)**<br>Ein Passwort-Hinweis kann nützlich sein, um einen Hinweis auf das Passwort zu geben, falls das Passwort einmal vergessen werden sollte.<br>**Hinweis**: Der Hinweis und das Passwort dürfen NICHT identisch sein. |  <br>**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)

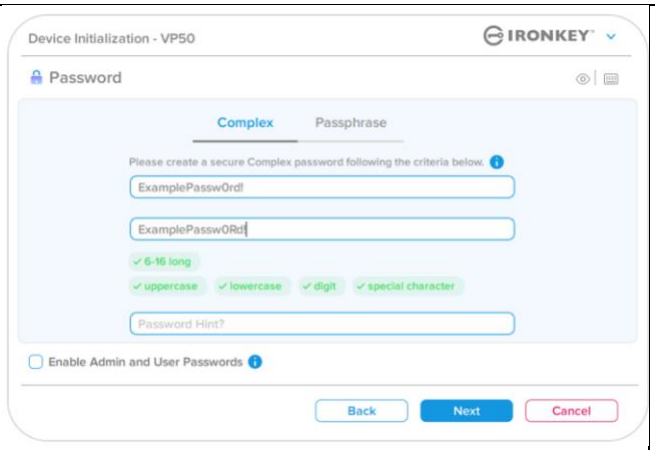



**Abb. 4.6a – Bedingung für komplexes Passwort erfüllt**

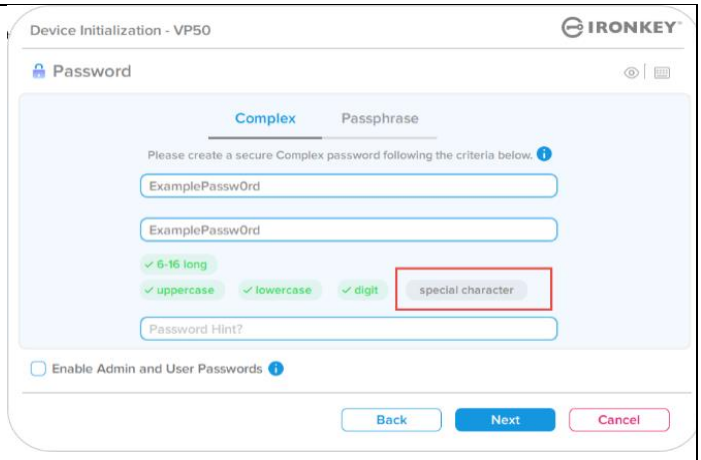



**Abb. 4.6b – Bedingung für komplexes Passwort ist optional**

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

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

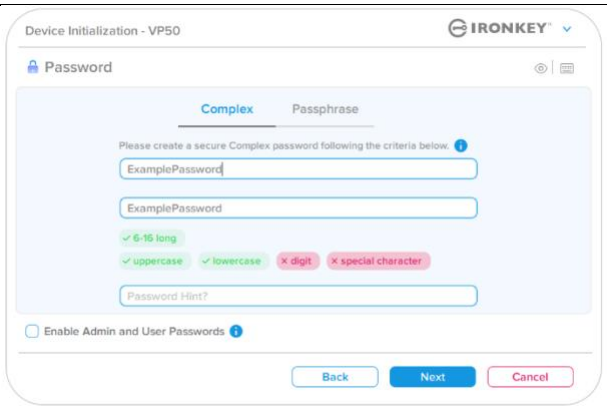



**Abb. 4.7 – Passwort-Bedingungen nicht erfüllt**

## Geräteinitialisierung

### Virtuelle Tastatur

Der VP50 verfügt über eine virtuelle Tastatur, die zum Schutz vor Keyloggern verwendet werden kann.

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

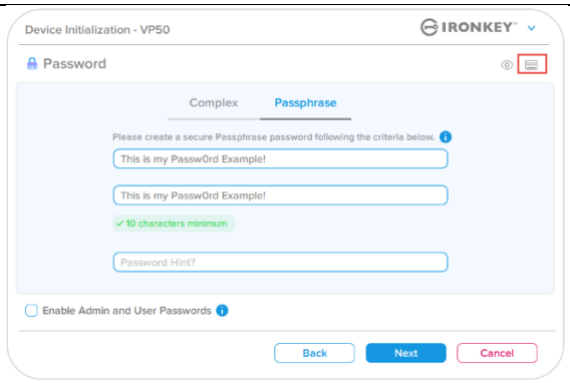



**Abb. 4.8 – Aktivieren der virtuellen Tastatur**

- Sobald die virtuelle Tastatur angezeigt wird, können Sie auch **Screenlogger-Schutz (Screenlogger Protection)** aktivieren. Wenn Sie diese Funktion verwenden, werden alle Tasten kurzzeitig leer angezeigt. Dies ist ein erwartetes Verhalten, da es verhindert, dass Screenlogger aufzeichnen, welche Schaltfläche Sie geklickt haben.

- Damit diese Funktion noch sicherer wird, können Sie die virtuelle Tastatur auch zufällig auswählen, indem Sie unten rechts auf der Tastatur **zufällig (randomize)** wählen. Durch Zufallseingabe wird die Tastatur in einer zufälligen Reihenfolge angeordnet.

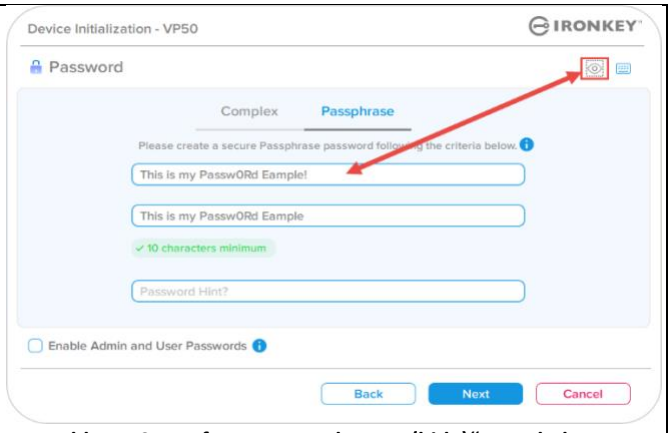
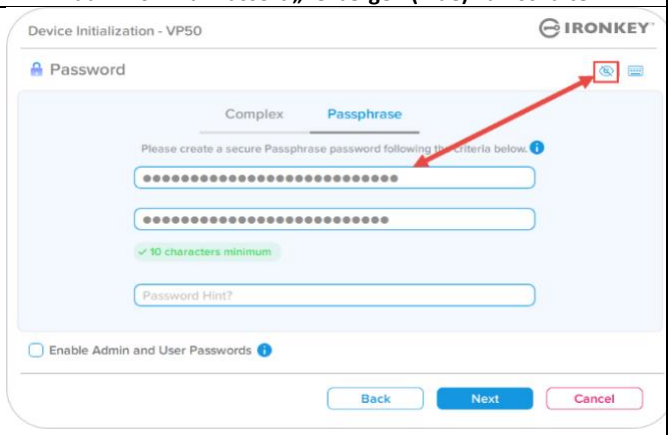

**Abb. 4.9 – Screenlogger-Schutz/Zufällig anordnen**

## Geräteinitialisierung

### Umschalten der Passwortsichtbarkeit

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

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

| | |
|---|---|
| Klicken Sie auf das graue Symbol, um die Passwortzeichenfolge zu **verbergen (hide)**.  |  **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:

- Einmaliges Wiederherstellungs-Passwort
- Erzwungener Schreibschutz-Modus für die Benutzeranmeldung
- Zurücksetzen des Benutzer-Passworts
- Erzwingen des Passwort-Reset für Benutzeranmeldung

Weitere Informationen zu diesen Funktionen finden Sie auf Seite 25 in dieser Bedienungsanleitung.

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

- Wenn diese Funktion **aktiviert (enabled)** ist, dann ist das gewählte Passwort auf diesem Bildschirm das **Admin-Passwort**. Klicken Sie auf **Weiter (Next)**, um zum Bildschirm **Benutzer-Passwort (User Password)** zu wechseln, wo ein Passwort für den Benutzer ausgewählt wird.

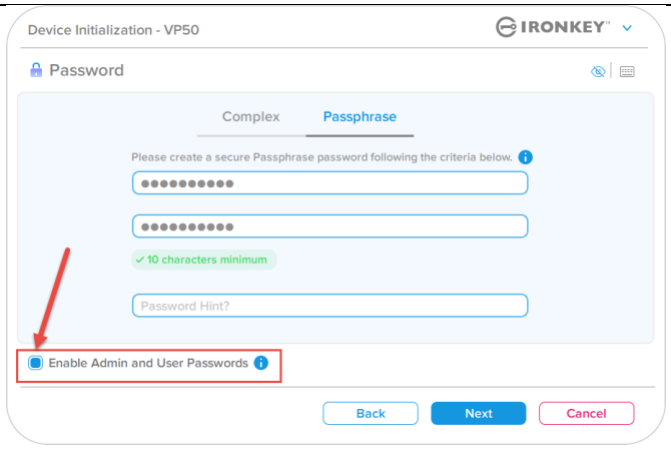



**Abb. 4.12 – Aktivieren von Admin- und Benutzer-Passwörtern**

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

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

**Hinweis:** „**Admin- und Benutzer-Passwörter (Admin and User Passwords)**“ werden im Folgenden als „**Admin-Rolle**“ bezeichnet.

## Geräteinitialisierung

### Admin- und Benutzer-Passwörter

- Wenn im vorherigen Bildschirm die Admin-Rolle **aktiviert (enabled)** 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 später in dieser Bedienungsanleitung näher erläutert. (Siehe Seite 23)

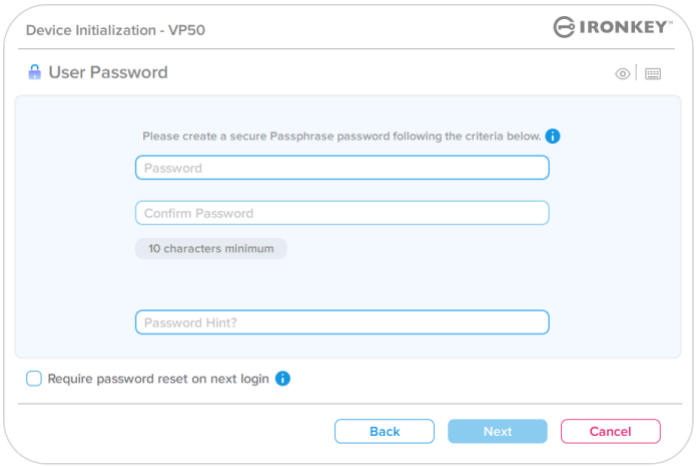



**Abb. 4.13 – Benutzer-Passwort (Admin und Benutzer aktiviert)**

**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.

- Die Funktion „**Passwort-Rücksetzen bei nächster Anmeldung anfordern (Require password reset on next login)**“ in der unteren linken Ecke von **Abb. 4.13** gilt nur für das Benutzer-Passwort und kann aktiviert werden, um den Benutzer zu zwingen, sich mit dem temporären Passwort anzumelden, das vom Administrator während des Initialisierungsprozesses festgelegt wurde. Er kann es dann in ein Passwort seiner Wahl ändern, nachdem der USB-Stick mit dem temporären Passwort authentifiziert wurde. Dies ist nützlich, wenn der USB-Stick einer anderen Person zur Nutzung überlassen wird. (**Abb. 4.14**)

  **Hinweis:** Aus Sicherheitsgründen darf das neue Passwort nicht mit dem temporären Passwort identisch sein.

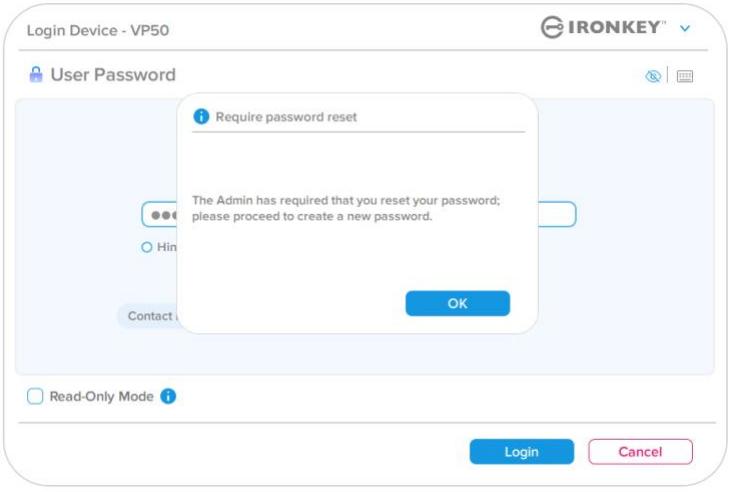


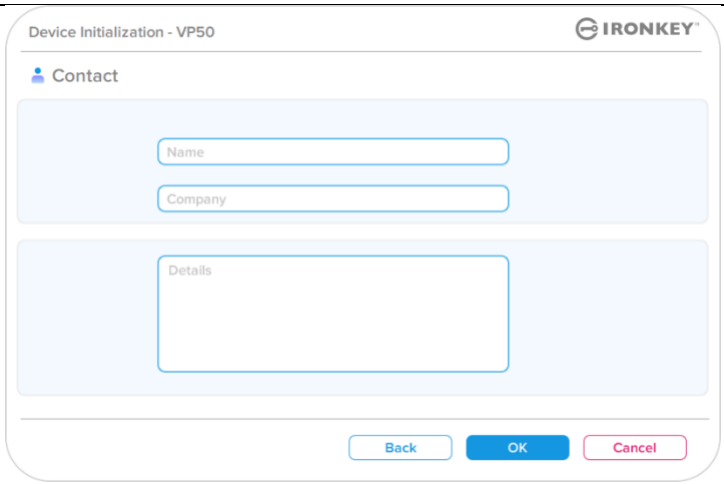

**Abb. 4.14 – Passwort-Rücksetzen bei nächster Anmeldung anfordern (Für Benutzer-Passwort)**

## Geräteinitialisierung

### Kontaktinformationen

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

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

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

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

## Gerätenutzung (Windows- und macOS-Umgebung)

### Anmeldung für Admin und Benutzer (Admin aktiviert)

Wenn der Stick mit aktivierten Admin- und Benutzer-Passwörtern (Admin-Rolle) initialisiert wird, startet die Anwendung IronKey VP50 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. 5.1). Wenn Sie auf die Schaltfläche „Login as Admin (Als Administrator anmelden)“ (siehe unten) klicken, wechselt die Anwendung zum Menü „Admin Login (Admin-Anmeldung)“, wo Sie sich als Admin anmelden können, um auf die Admin-Einstellungen und -Funktionen zuzugreifen. (Abb. 5.2)

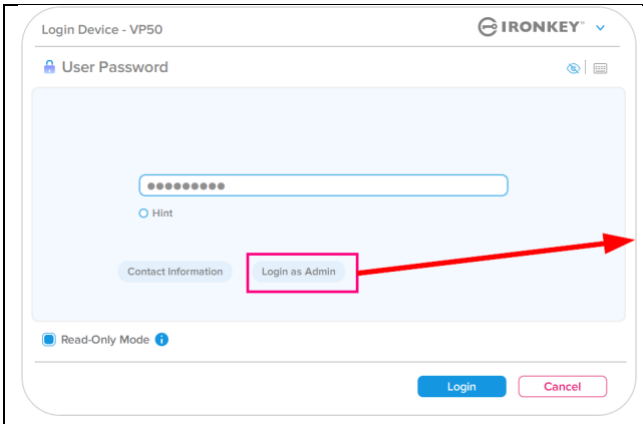



**Abb. 5.1 – Anmeldung mit Benutzer-Passwort (Admin aktiviert)**

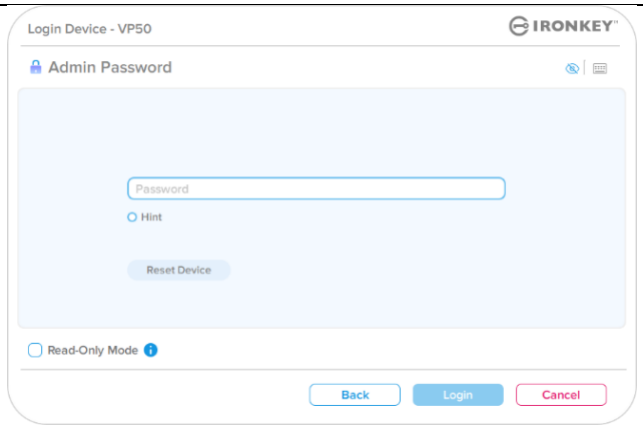



**Abb. 5.2 – Anmeldung mit Admin-Passwort**

### 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. 5.3)

**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**

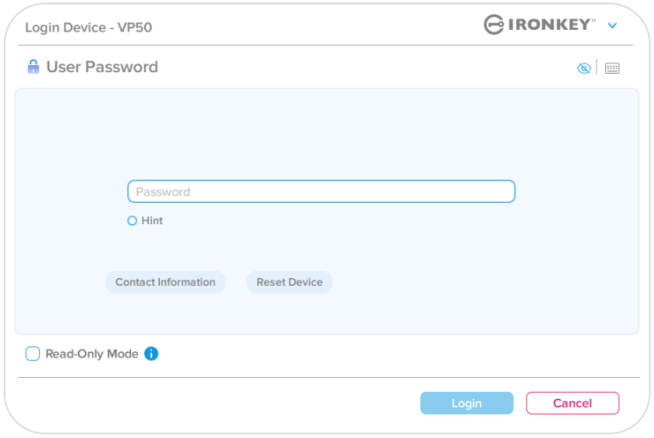



**Abb. 5.3 – Anmeldung mit Benutzer-Passwort (Admin nicht aktiviert)**

| | |
|---|---|
| **„Gerät zurücksetzen (Reset Device)“ durchgeführt wird.** | |

## Gerät verwenden

### Entsperren im Schreibschutz-Modus

Der Stick kann in einem schreibgeschützten Zustand entsperrt werden, damit die Dateien auf Ihrem IronKey-Laufwerk nicht verändert werden können. Wenn Sie z. B. einen nicht vertrauenswürdigen oder unbekannten Computer verwenden, verhindert das Entsperren Ihres Geräts im Schreibschutz-Modus, dass Malware auf diesem Computer Ihr Gerät infiziert oder Ihre Dateien verändert.

Wenn Sie in diesem Modus arbeiten, können Sie keine Vorgänge durchführen, bei denen Dateien auf dem Gerät verändert werden.
Der Stick kann z. B. nicht neu formatiert, Dateien auf dem Laufwerk wiederhergestellt, hinzugefügt oder bearbeitet werden.

So wird der Stick im Schreibschutz-Modus entsperrt:

1. Stecken Sie das Gerät in den USB-Anschluss des Host-Computers und führen Sie die Datei **IronKey.exe** aus.
2. Aktivieren Sie das Kontrollkästchen **Schreibgeschützt (Read-Only)** unter dem Passworteingabefeld. (**Abb. 5.4)**
3. Geben Sie Ihr Gerätepasswort ein und klicken Sie auf **Anmelden (Login)**. Der IronKey wird nun im Schreibschutz-Modus entsperrt.

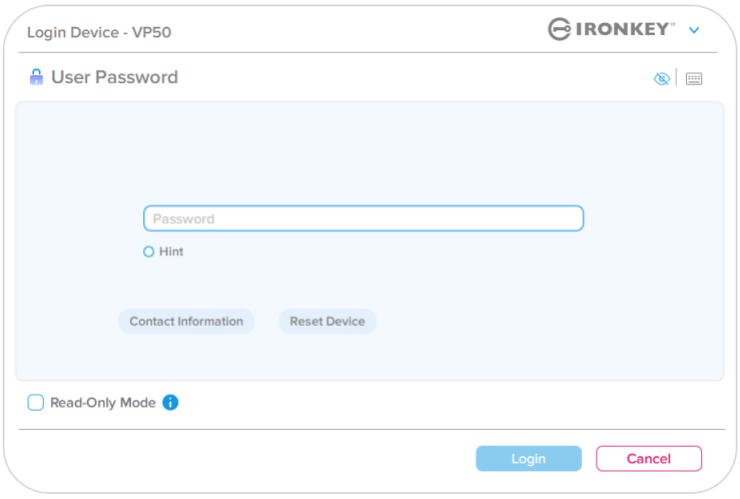



**Abb. 5.4 – Schreibschutz-Modus**

Wenn Sie den Stick mit vollem Lese-/Schreibzugriff auf die sichere Datenpartition entsperren möchten, müssen Sie den VP50 korrekt trennen und sich erneut anmelden, wobei das Kontrollkästchen „Schreibgeschützt (Read-Only)“ nicht markiert sein darf.

**Hinweis:** Die VP50 Admin-Optionen bieten einen erzwungenen Schreibschutz für die Benutzerdaten, d. h. die Benutzeranmeldung kann vom Administrator erzwungen werden, um sie im Schreibschutz-Status freizugeben (Details siehe **Seite 28**).

## 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 an oder verwenden Sie das einmalige Wiederherstellungs-Passwort, um das Benutzer-Passwort zurückzusetzen. | NEIN (NO) |
| Admin-Passwort | Crypto-Löschen des Laufwerks, Passwörter, Einstellungen und Daten werden für immer gelöscht. | **YES (JA)** |
| Einmaliges Wiederherstellungs-Passwort (One-Time Recovery Password) | Passwort-Sperre, die Schaltfläche „Wiederherstellungs-Passwort (Recovery Password)“ wird grau hinterlegt und ist nicht mehr verfügbar. Als Administrator anmelden, um das Passwort zurückzusetzen | NEIN (NO) |
| **Nur-Benutzer Einzelner Benutzer, einzelnes Passwort (Admin/Benutzer NICHT aktiviert)** | **Schutz vor Brute-Force-Angriffen Geräteverhalten (10 falsche Passworteingabeversuche)** | **Datenlöschung und Geräte-Reset?** |
| Benutzer-Passwort | Crypto-Löschen des Laufwerks, Passwörter, Einstellungen und Daten werden für immer gelöscht. | **YES (JA)** |

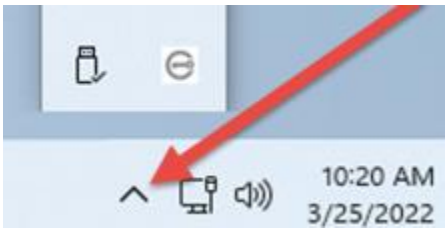
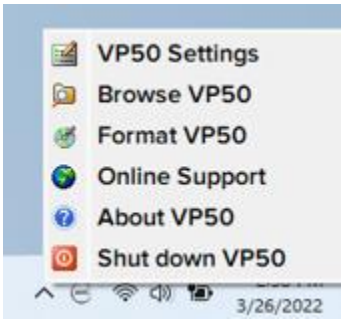
* Sobald Sie sich erfolgreich am Gerät authentifiziert haben, wird der Zähler für fehlgeschlagene Anmeldungen zurückgesetzt, je nachdem, welche Anmeldemethode verwendet wurde. Das Crypto-Löschen löscht alle Passwörter, Verschlüsselungsschlüssel und Daten – **die Daten gehen für immer verloren.**

**Zugriff auf die sicheren Dateien**

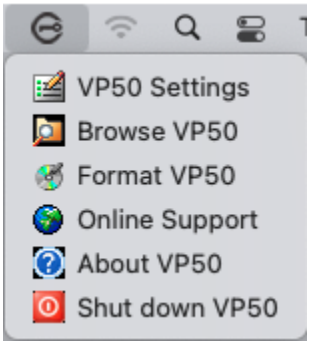
Nachdem Sie den USB-Stick entsperrt haben, können Sie auf Ihre sicheren Dateien zugreifen. Dateien werden automatisch ver- und entschlüsselt, wenn diese auf dem Stick gespeichert oder geöffnet werden. Diese Technologie bietet Ihnen den Komfort, wie mit einem normalen Stick zu arbeiten, während sie gleichzeitig 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 **VP50 durchsuchen (Browse VP50)** klicken. (Abb. 6.2)

## Geräteoptionen – (Windows-Umgebung)

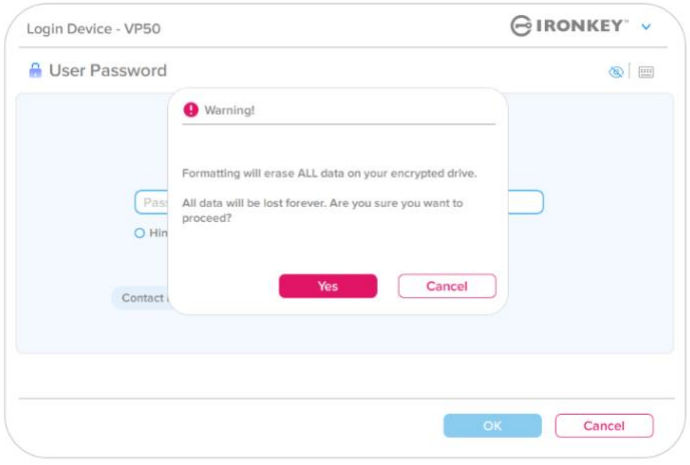
Solange Sie auf dem Gerät angemeldet sind, wird in der rechten Ecke des Fensters das IronKey-Symbol angezeigt. Wenn Sie mit der rechten Maustaste auf das IronKey-Symbol klicken, öffnet sich das Auswahlmenü für die verfügbaren Laufwerksoptionen. (Abb. 6.2)
Einzelheiten zu diesen Geräteoptionen finden 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. 6.1)** |  **Abb. 6.1 – IronKey-Symbol in Taskleiste** |
| • Wenn Sie mit der rechten Maustaste auf das IronKey-Symbol klicken, öffnet sich das Auswahlmenü für die verfügbaren Laufwerksoptionen. **(Abb. 6.2)**<br><br>Einzelheiten zu diesen Geräteoptionen finden Sie auf den Seiten 19–23 dieser Bedienungsanleitung. |  **Abbildung 6.2 – Rechtsklick auf das IronKey-Symbol für Geräteoptionen** |

## Geräteoptionen – (macOS-Umgebung)

| | |
|---|---|
| • Wenn Sie auf dem Gerät angemeldet sind, finden Sie im macOS-Menü ein IronKey VP50-Symbol (siehe **Abb. 6.3**), mit dem die verfügbaren Geräteoptionen geöffnet werden.<br><br>Einzelheiten zu diesen Geräteoptionen finden Sie auf den Seiten 19–23 dieser Bedienungsanleitung. |  <br>**Abb. 6.3 – Menüleiste für macOS Symbol/Geräteoptionsmenü** |

## Geräteoptionen

| | |
|---|---|
| **VP50 Einstellungen:** | • Ändern des Anmelde-Passworts, der Kontaktinformationen und anderer Einstellungen. (Weitere Einzelheiten zu den Geräteeinstellungen finden Sie im Abschnitt „VP50 Einstellungen“ in dieser Bedienungsanleitung.) |
| **VP50 durchsuchen:** | • Damit können Ihre gesicherten Dateien angezeigt werden. |
| **VP50 formatieren:**<br>Mit dieser Funktion können Sie die sichere Datenpartition formatieren. (Warnhinweis: Alle Daten werden unwiederbringlich gelöscht) (**Abb. 6.1**)<br><br>**Hinweis:** Zum Formatieren ist eine Passwort-Authentifizierung erforderlich. |  <br>**Abb. 6.1 – VP50 formatieren** |
| **Online-Support:** | • Öffnet Ihren Internet-Browser und navigiert Sie zu http://www.kingston.com/support/, wo Sie Zugang zu weiteren Support-Informationen haben. |

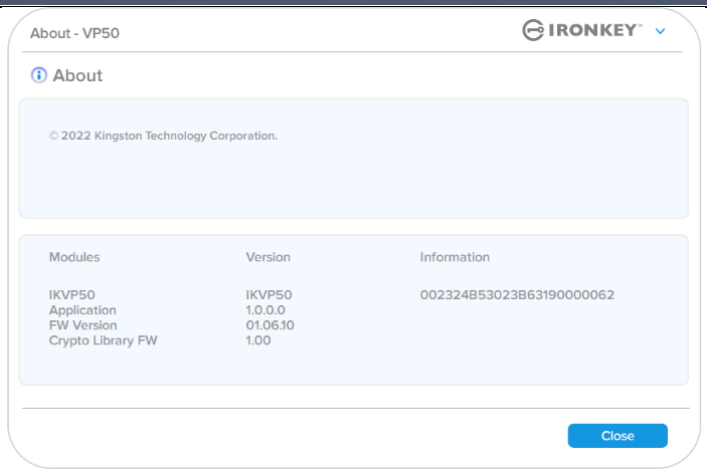
<table>
<tr>
<td>Über VP50:<br>Hier finden Sie spezifische Informationen über den VP50, einschließlich Informationen zu Anwendung, Firmware und Seriennummer. (Abb. 6.2)<br><br>Hinweis: Die individuelle Seriennummer des Laufwerks finden Sie in der Spalte „Information (Informationen)“.</td>
<td> 

Abb. 6.2 – Über VP50</td>
</tr>
<tr>
<td>VP50 trennen:</td>
<td>• Fährt den VP50 ordnungsgemäß herunter, damit Sie ihn sicher aus Ihrem System entfernen können.</td>
</tr>
</table>

## VP50-Einstellungen

### Admin-Einstellungen (Admin Settings)

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

- **Passwort (Password):** Hiermit können Sie das Admin-Passwort bzw. den Hinweis ändern (*Abb. 7.1*).
- **Kontaktinformationen (Contact Info):** Hier können Kontaktinformationen hinzugefügt, angezeigt oder geändert werden (*Abb. 7.2*).
- **Sprache (Language):** Hier lässt sich die gewählte Sprache ändern (*Abb. 7.3*).
- **Admin-Optionen (Admin Options):** Damit können Sie zusätzliche Funktionen aktivieren, wie z. B: (Abb. 7.4)
    - ○ Benutzer-Passwort ändern
    - ○ Anmelde-Passwort zurücksetzen (für Benutzer-Passwort)
    - ○ Einmaliges Wiederherstellungs-Passwort aktivieren
    - ○ Schreibschutz-Modus für Benutzerdaten erzwingen

**HINWEIS:** Weitere Einzelheiten zu den Admin-Optionen finden Sie auf Seite 24.

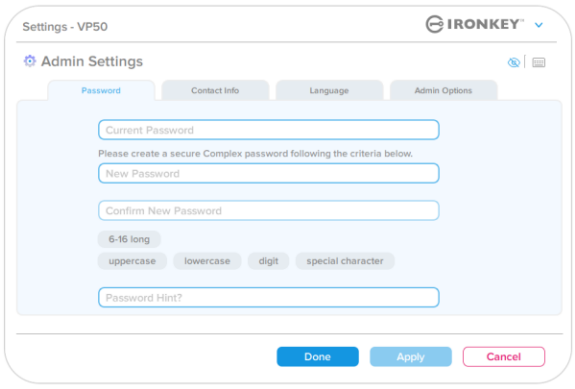



**Abb. 7.1 – Passwort-Optionen**

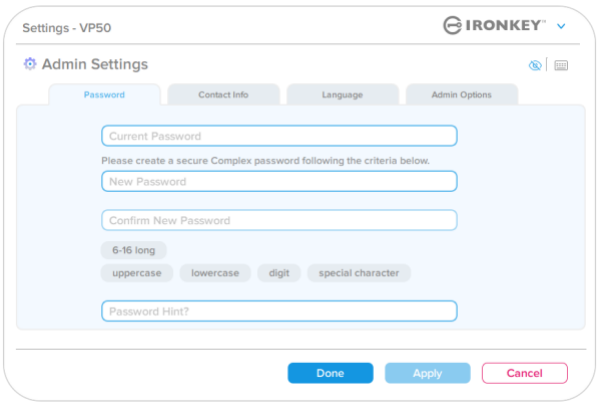



**Abb. 7.2 – Kontaktinformationen**

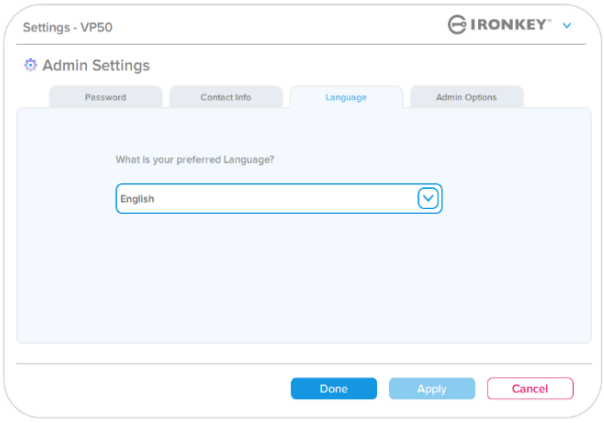



**Abb. 7.3 – Sprachauswahl**

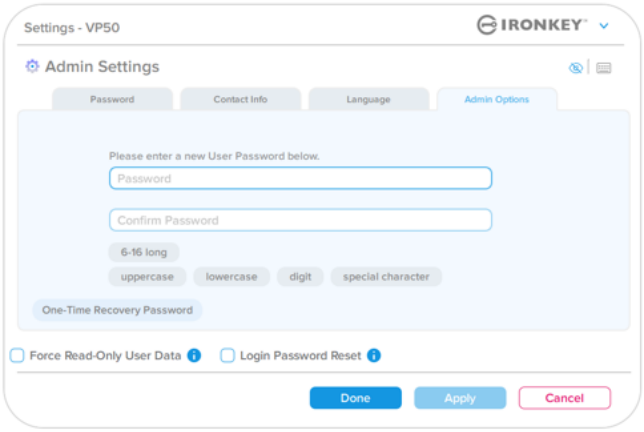
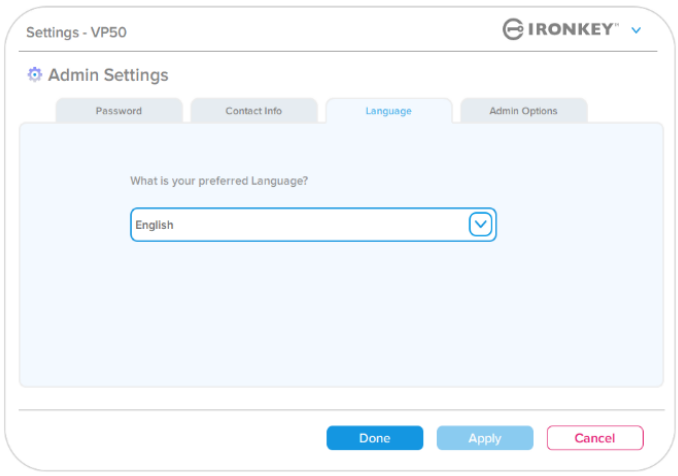
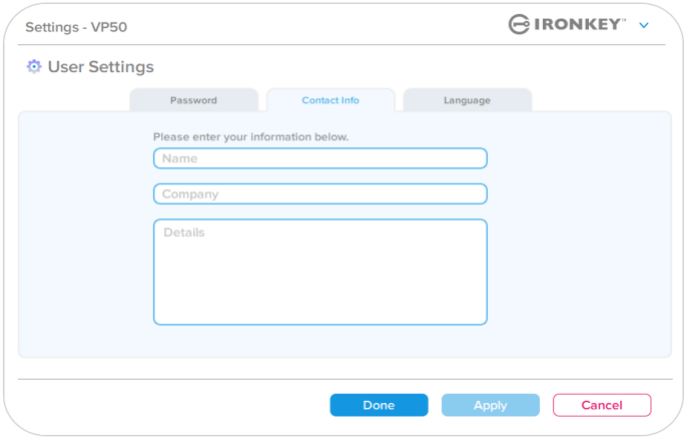
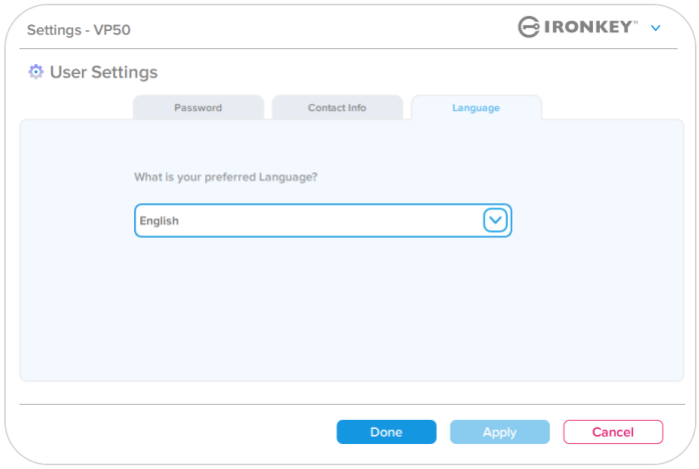



**Abb. 7.4 – Admin-Optionen**

## VP50-Einstellungen

### Benutzer-Einstellungen (User Settings): 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. 7.5*) |  **Abb. 7.5 – Passwort-Optionen (Admin aktiviert: Benutzeranmeldung)** |
| **Kontaktinformationen (Contact Info):** Hiermit können Sie Ihre Kontaktinformationen hinzufügen/anzeigen/ändern. (*Abb. 7.6*) |  **Abb. 7.6 – Kontaktinformationen (Admin aktiviert: Benutzeranmeldung)** |
| **Sprache (Language):** Hiermit können Sie Ihre aktuelle Sprachauswahl ändern. (*Abb. 7.7*) |  **Abb. 7.7 – Spracheinstellungen (Admin aktiviert: Benutzeranmeldung)** |

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

## VP50-Einstellungen

### Benutzer-Einstellungen (User Settings): Admin nicht aktiviert

Wie bereits auf Seite 12 erwähnt, führt die Initialisierung des VP50 ohne Aktivierung von Admin- und Benutzer-Passwörtern zu einer Konfiguration des Laufwerks 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 VP50-Einstellungen:

### Ändern und Speichern von Einstellungen

- Wenn Einstellungen in den VP50-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. 7.11)

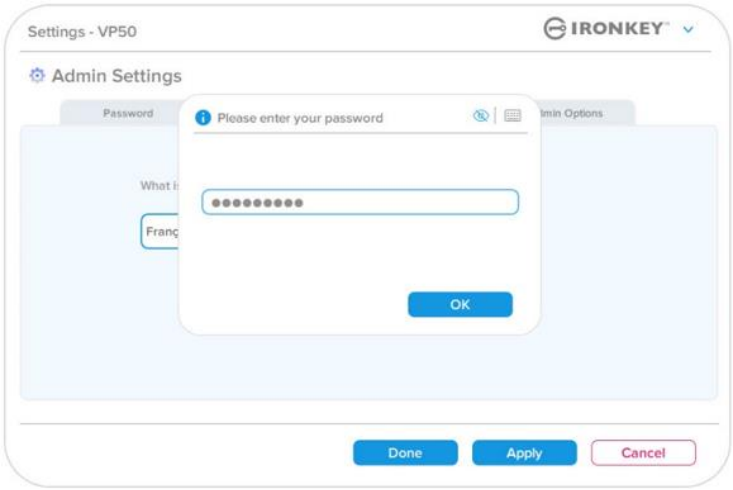



**Abb. 7.11 – Bildschirm mit Passwortabfrage zum Speichern von VP50-Einstellungsänderungen**

**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 „VP50 Einstellungen (Settings)“ wird wieder angezeigt.

## Admin-Funktionen

**Verfügbare Optionen zum Zurücksetzen des Benutzer-Passworts**
Die Funktionen der Administrationskonfiguration bieten mehrere Möglichkeiten, das Benutzer-Passwort sicher zurückzusetzen, wenn es vergessen wurde oder wenn ein temporäres Benutzer-Passwort erstellt wurde und Sie eine Passwortänderung bei der nächsten Anmeldung des Benutzers erzwingen möchten. Im Folgenden sind die Funktionen aufgeführt, die beim Zurücksetzen des Benutzer-Passworts hilfreich sein können:

**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. 8.1)**

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

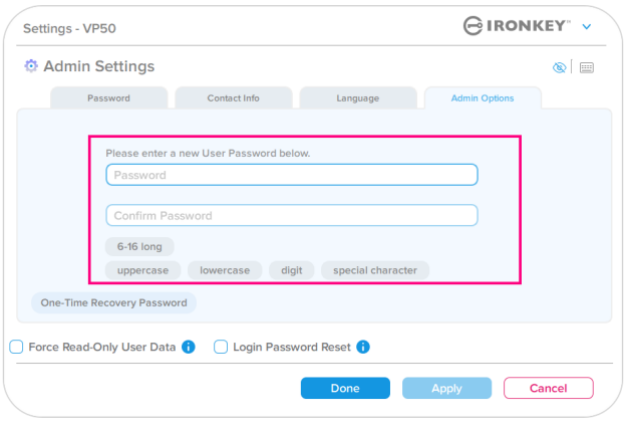



**Abb. 8.1 – Admin-Optionen/Benutzer-Passwort zurücksetzen**

**Anmelde-Passwort zurücksetzen (Login Password Reset):**
Wenn Sie die Funktion „Anmelde-Passwort zurücksetzen“ aktivieren, wird der Benutzer gezwungen, sich mit einem temporären Passwort anzumelden, das der Administrator festgelegt hat, und dann muss der Benutzer es in ein Passwort seiner Wahl ändern. Dies ist nützlich, wenn der USB-Stick einer anderen Person zur Nutzung überlassen wird. **(Siehe Abb. 8.2A und 8.2B**)

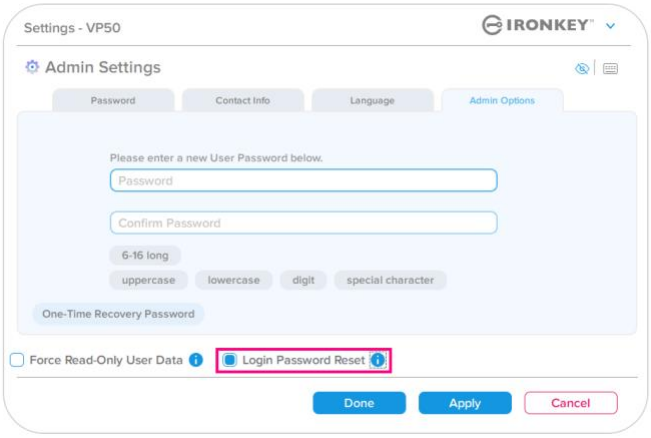



**Abb. 8.2A – Schaltfläche zum Zurücksetzen von Anmelde-Passwörtern**

**Hinweis:** Dieser Reset erfolgt beim nächsten erfolgreichen Benutzer-Login. Die Kriterien für die Passwortanforderungen werden automatisch entsprechend der ursprünglichen Option angewendet, die während des Initialisierungsprozesses festgelegt wurde (Optionen „Komplex (Complex)“ oder „Passphrase“).

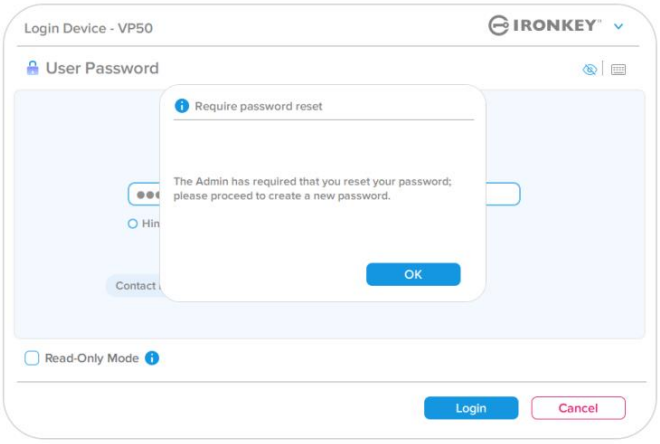



**Abb. 8.2B – Reset-Benachrichtigung nach Eingabe des Benutzer-Passworts**

## Admin-Funktionen

### Einmaliges Wiederherstellungs-Passwort (One-Time Recovery Password)

In diesem Abschnitt wird beschrieben, wie die Funktion zur einmaligen Wiederherstellung des Passworts aktivieren und verwendet werden kann.

#### Einmaliges Wiederherstellungs-Passwort

**1. Schritt:** Die Funktion zur einmaligen Wiederherstellung des Passworts ist sehr nützlich, da sie aktiviert werden kann, um das Benutzer-Passwort wiederherzustellen und zurückzusetzen, wenn der Benutzer sein Benutzer-Passwort vergessen hat. Klicken Sie auf die Schaltfläche „Einmaliges Wiederherstellungs-Passwort (One-Time Recovery Password)“ im Menü „Admin-Optionen (Admin Options)“, um mit der Wiederherstellung zu beginnen. **(Abb. 8.4)**

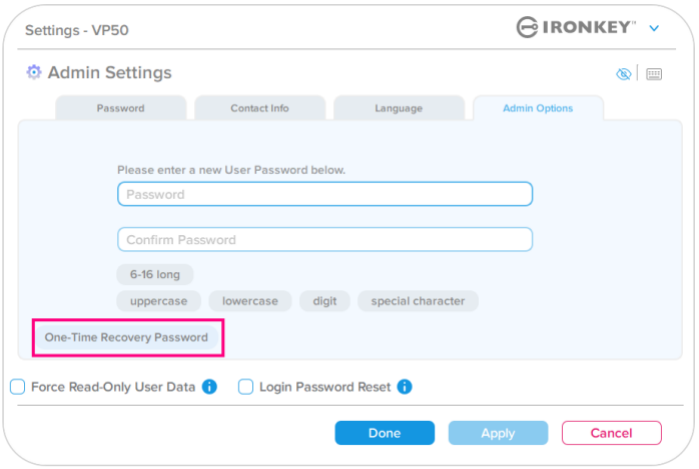



**Abb. 8.4 – Schaltfläche „Einmaliges Wiederherstellungs-Passwort“**

**2. Schritt:** Erstellen Sie ein einmaliges Wiederherstellungs-Passwort mit denselben Passwortkriterien, mit denen der Stick ursprünglich eingerichtet wurde (Komplex oder Passphrase).

**Hinweis:** Das Admin-Passwort ist erforderlich, um die Änderungen zu übernehmen.

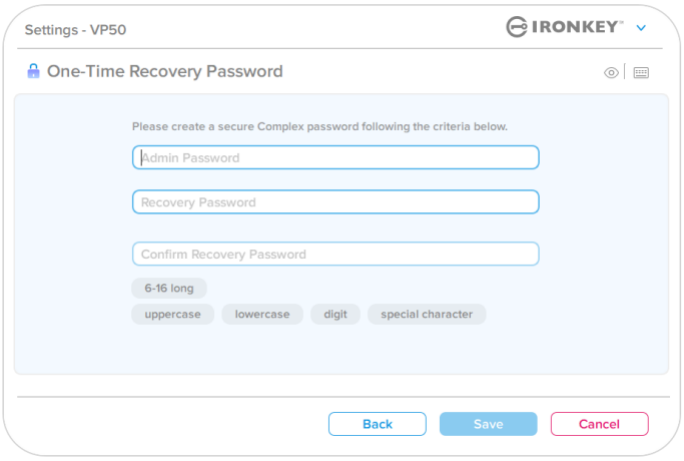
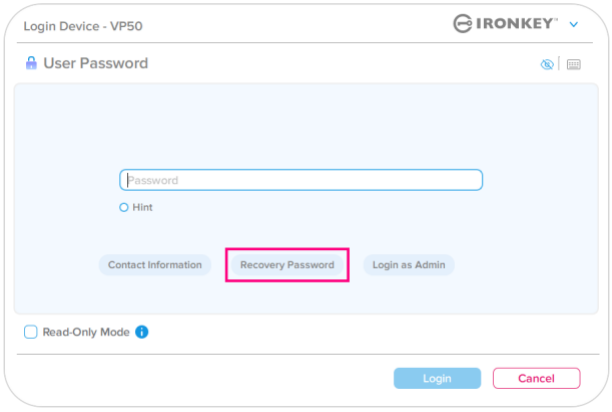
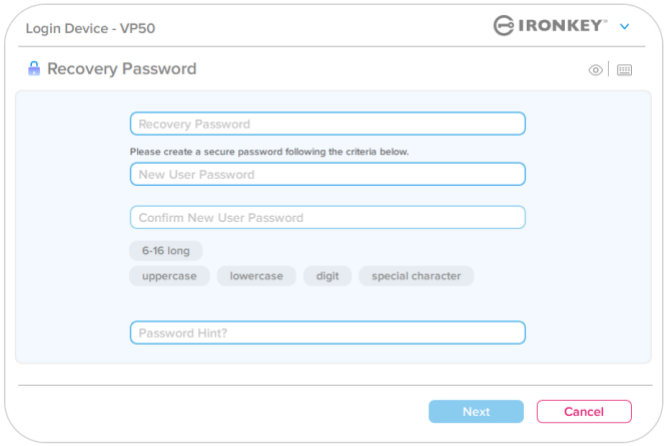



**Abb. 8.5 – Einrichten des einmaligen Wiederherstellungs-Passworts**

## Admin-Funktionen

Einmaliges Wiederherstellungs-Passwort verwenden

| | |
|---|---|
| **1. Schritt:** Nachdem das einmalige Wiederherstellungs-Passwort erstellt wurde, erscheint bei der nächsten Anmeldung eine neue Schaltfläche auf dem Anmeldebildschirm **Benutzer-Passwort (User Password)**. Klicken Sie auf die Schaltfläche **Wiederherstellungs-Passwort (Recovery Password)**, um den Vorgang zu starten. |  <br>**Abb. 8.6 – Schaltfläche „Wiederherstellungs-Passwort“** |
| **2. Schritt:** Der Bildschirm **Wiederherstellungs-Passwort (Recovery Password)** wird angezeigt, auf dem Sie das Wiederherstellungs-Passwort eingeben und ein neues Benutzer-Passwort erstellen können. (Abb. 8.7)<br><br>**Wichtig:** Das „Einmalige Wiederherstellungs-Passwort“ verwendet ebenfalls eine integrierte Sicherheitsfunktion, die die Anzahl der fehlgeschlagenen Anmeldeversuche verfolgt. **Nach 10 fehlgeschlagenen, falschen Anmeldeversuchen mit dem einmaligen Wiederherstellungs-Passwort wird das Passwort deaktiviert**, und muss erneut aktiviert werden, indem Sie sich im Stick als Administrator anmelden (siehe Seiten 18 und 30 für weitere Einzelheiten). |  <br>**Abb. 8.7 – Menü „Wiederherstellungs-Passwort“** |

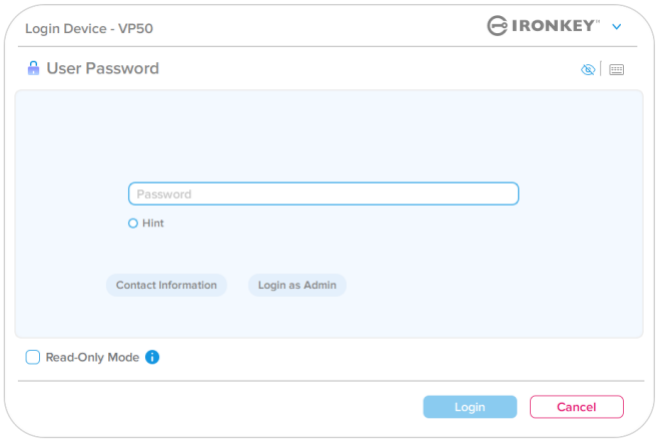
<table>
<tr>
<td>3. Schritt: Bei Erfolg werden Sie zum Bildschirm Benutzer-Passwort (User Password) zurückgeleitet. Die Schaltfläche Wiederherstellungs-Passwort (Recovery Password) ist nun nicht mehr vorhanden, und das in Schritt 2 eingegebene Benutzer-Passwort wird zum neuen Benutzer-Passwort. (Abb. 8.8)</td>
<td> 

Abb. 8.8 – Anmeldebildschirm für Benutzer-Passwort mit der Schaltfläche Wiederherstellungs-Passwort verschwindet nach erfolgreicher Verwendung.</td>
</tr>
</table>

## Admin-Funktionen

### Schreibgeschützte Benutzerdaten erzwingen

Die Funktion „Erzwungener Schreibschutz-Modus (Forced Read-Only mode)“ kann aktiviert werden, um den Schreibzugriff des Benutzers auf den USB-Stick zu beschränken. Diese Funktion ist nützlich, wenn auf Dateien auf dem USB-Stick nur lesend zugegriffen werden soll.

- Um den Schreibschutz für die Benutzerdaten zu erzwingen, klicken Sie auf das Kästchen und dann auf „Übernehmen (Apply)“. **(Abb. 8.9)**

  **Hinweis:** Dieser erzwungene Schreibschutz-Modus gilt nur für den Benutzer und hat keine Auswirkungen auf die Anmeldung als Administrator. Die Admin-Anmeldung hat weiterhin Lese- und Schreibrechte und kann bei Bedarf den Schreibschutz-Modus aktivieren.

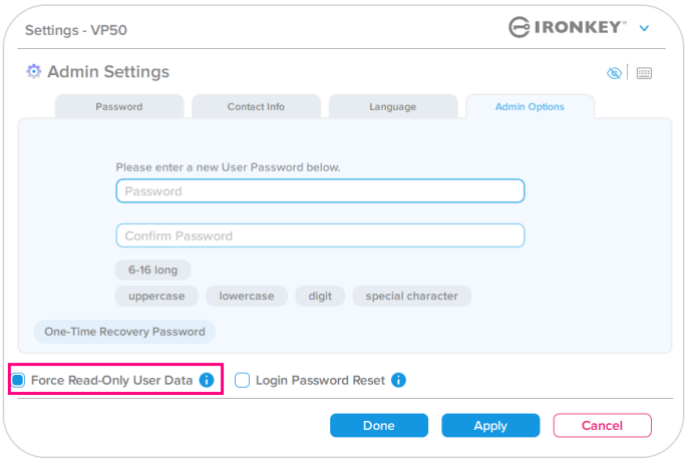



**Abb. 8.9 – Aktivieren von „Schreibgeschützte Benutzerdaten erzwingen“ (Admin-Passwort ist erforderlich, um die Änderungen zu übernehmen.)**

- Nach der Aktivierung wird die Schaltfläche „**Schreibschutz-Modus (Read-Only Mode)**“ in Blau angezeigt, was bedeutet, dass der erzwungene Schreibschutz-Modus für das Benutzer-Passwort dauerhaft aktiviert ist, bis er durch den Administrator deaktiviert wird. (Abb. 8.10)

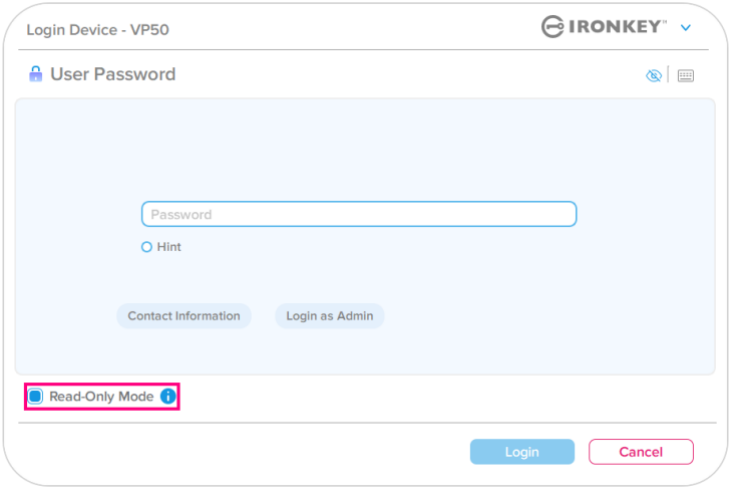



**Abb. 8.10 – Der Schreibschutz-Modus ist für den Benutzer zwangsweise aktiviert und kann nur vom Administrator deaktiviert werden**

## Hilfe und Fehlerbehebung

### Gerätesperrung

Der VP50 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/Einmaliges Wiederherstellungs-Passwort).

Der „Sperr“-Zähler registriert alle fehlgeschlagenen Anmeldeversuche 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. 9.1)

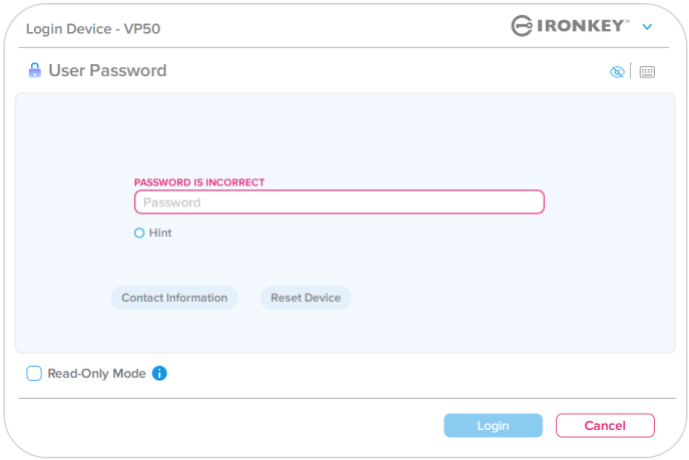



**Abb. 9.1 – Meldung „Falsches Passwort“**

- Wenn der Anmeldeversuch das **7.** Mal fehlgeschlagen ist, wird eine weitere Fehlernachricht mit der Mitteilung angezeigt, dass Ihnen noch 3 Versuche bis zum Erreichen von MaxNoA bleiben (der standardmäßig auf 10 eingestellt ist). (Abb. 9.2)

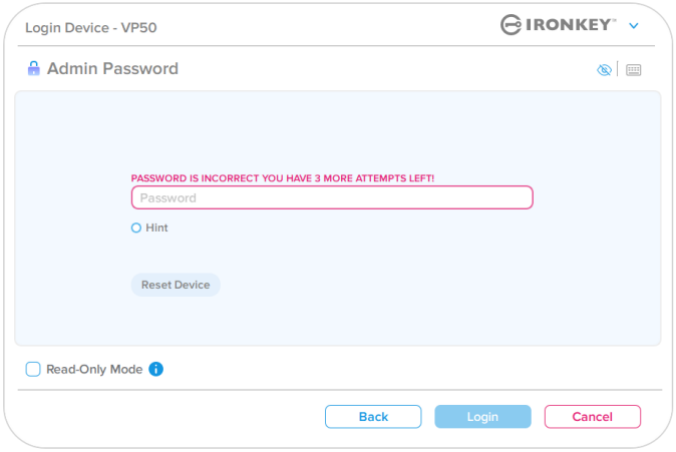



**Abb. 9.2 – 7. falscher Passworteingabeversuch**

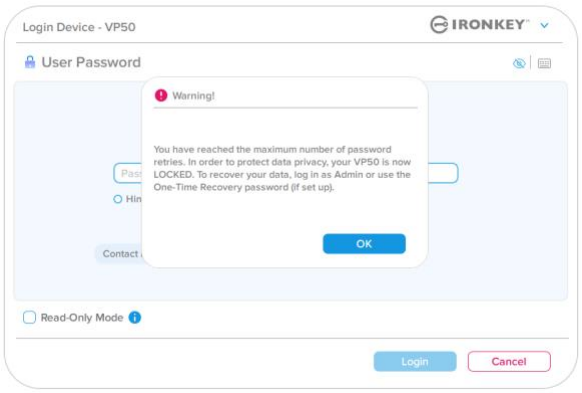
## Hilfe und Fehlerbehebung

### Gerätesperrung

**Wichtig:** Nach dem **10.** und letzten fehlgeschlagenen Anmeldeversuch wird das Gerät je nach Konfiguration und Anmeldemethode (Admin, Benutzer oder einmaliges Wiederherstellungs-Passwort) 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**. Handlungsweisen, die auch auf Seite 18 dieser Bedienungsanleitung erwähnt werden.

Die folgenden Abbildungen 9.3 – 9.6 zeigen das visuelle Verhalten für die 10. und letzte fehlgeschlagenen Anmeldung bei jeder Anmeldepasswortmethode:

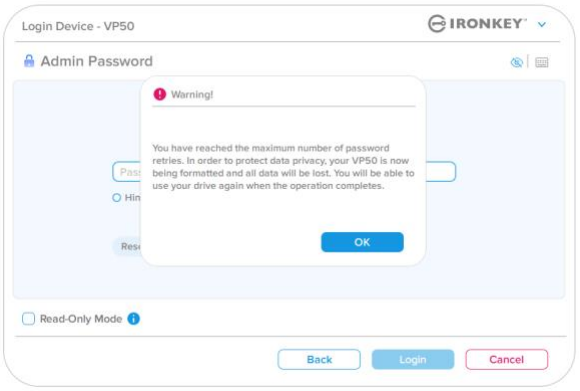
**Benutzer-Passwort: (Admin/Benutzer aktiviert)**




**GERÄTESPERRUNG**

**(Abb. 9.3)**

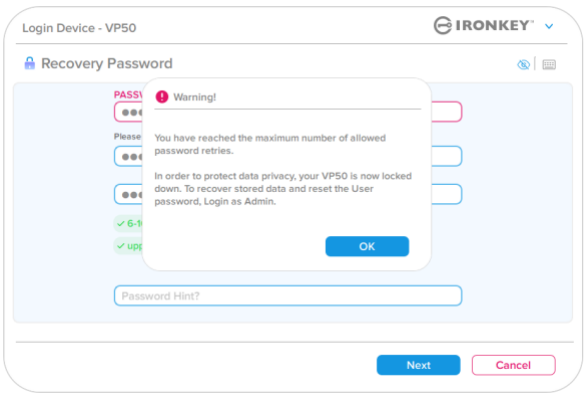
**Admin-Passwort (Admin/Benutzer aktiviert))**




**GERÄT FORMATIEREN***

**(Abb. 9.4)**

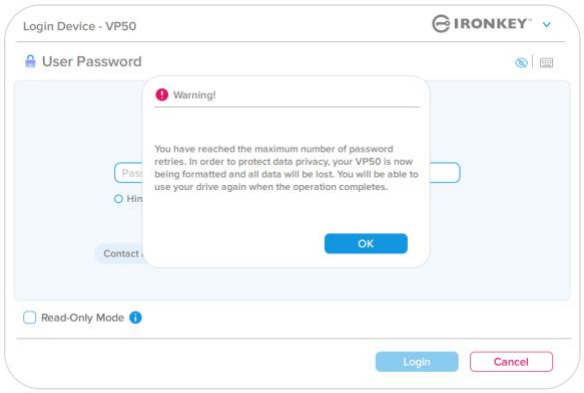
**Einmalige Wiederherstellung: (Admin/Benutzer aktiviert)**




**GERÄTESPERRUNG**

**(Abb. 9.5)**

**Benutzer-Passwort (Admin NICHT aktiviert)**




**GERÄT FORMATIEREN***

**(Abb. 9.6)**

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 VP50 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.

**Hinweis: Bei einer Geräteformatierung werden ALLE auf der sicheren Datenpartition des VP50 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 VP50 Launcher ausgeführt wird. (Siehe ***Abb. 9.7*** und **9.8**)

- Mit dieser Option können Sie ein neues Passwort erstellen, jedoch wird der VP50 zum Schutz Ihrer Daten neu formatiert. Das bedeutet, dass alle Ihre Daten in diesem Prozess unwiederbringlich gelöscht werden.*

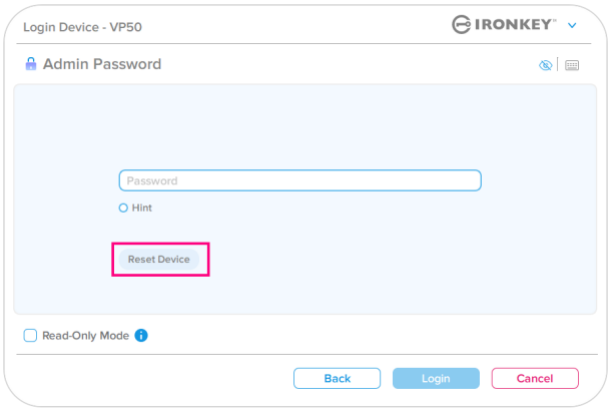



**Abb. 9.7 – Admin-Passwort: Schaltfläche „Gerät zurücksetzen (Reset Device)“**

- **Hinweis:** Wenn Sie auf *„Gerät zurücksetzen (Reset Device)“* klicken, erscheint eine Meldung, die fragt, ob Sie ein neues Passwort eingeben möchten, bevor die Formatierung durchgeführt wird. Sie haben jetzt die Wahl 1) dies durch Klicken auf *„OK“* zu bestätigen oder 2) durch Klicken auf „Abbrechen (Cancel)“ abzubrechen und zum Anmeldefenster zurückzukehren. (Siehe Abb. 9.8)

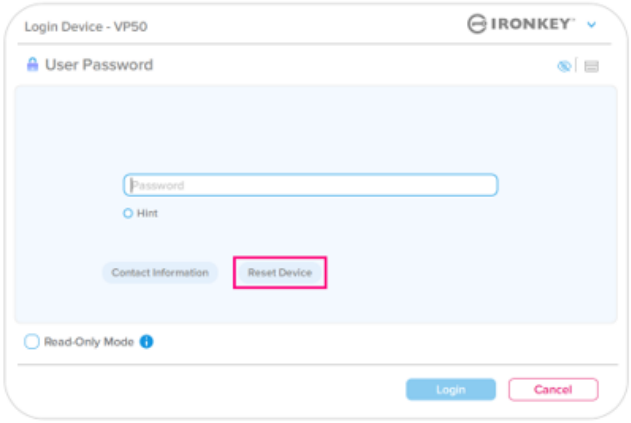



**Abb. 9.8 – Benutzer-Passwort (Admin/Benutzer nicht aktiviert) Gerät zurücksetzen**

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

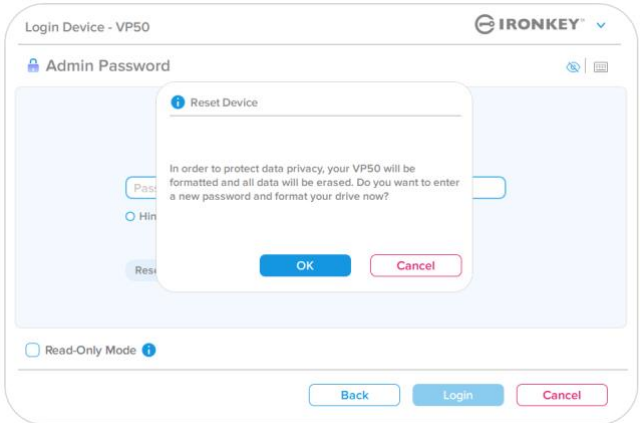



**Abb. 9.9 – Bestätigung „Gerät zurücksetzen (Reset Device)“**

## Hilfe und Fehlerbehebung

### Laufwerksbuchstaben-Konflikt: Windows-Betriebssysteme

- Wie bereits im Abschnitt *Systemanforderungen*“, Seite 3 in dieser Anleitung erwähnt, benötigt der VP50 zwei freie aufeinanderfolgende Laufwerksbuchstaben NACH dem letzten physischen Speicher, der vor der Lücke“ in den Laufwerksbuchstabenzuweisungen angezeigt wird (siehe *Abb. 9.10.*) 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 VP50 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 Disk Management (Administratorrechte erforderlich). Wie bereits im Abschnitt *Systemanforderungen*“, Seite 3 in dieser Anleitung erwähnt, benötigt der VP50 zwei freie aufeinanderfolgende Laufwerksbuchstaben NACH dem letzten physischen Speicher, der vor der Lücke“ in den Laufwerksbuchstabenzuweisungen angezeigt wird (siehe *Abb. 9.10.*) 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.

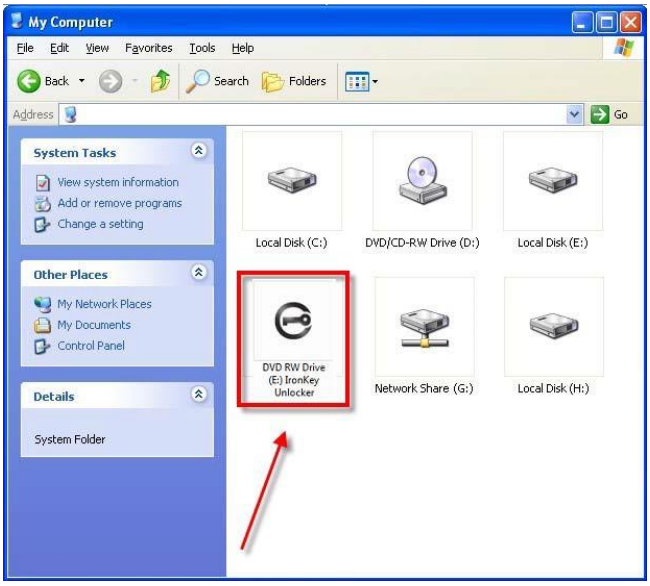



**Abb. 9.10 – Beispiel für Laufwerksbuchstaben**

In diesem Beispiel (Abb 9.10) verwendet der VP50 das Laufwerk „F:“, das erste verfügbare Laufwerk nach Laufwerk „E:“ (dem letzten physischen Laufwerk vor der Laufwerksbuchstabenlücke). Da der Buchstabe G: eine

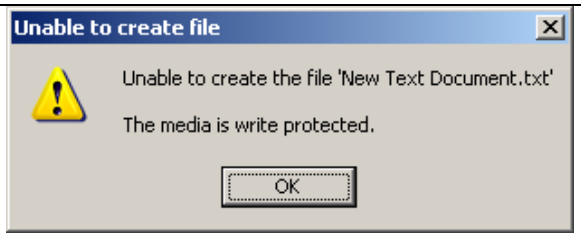
Netzwerkfreigabe und nicht Teil des Hardware-Profils ist, kann der VP50 versuchen, ihn als zweiten Laufwerksbuchstaben zu verwenden und dadurch einen Konflikt verursachen.

Wenn es in Ihrem System keine Netzwerkfreigaben gibt und der VP50 dennoch nicht lädt, ist es möglich, dass ein Kartenlesegerät, ein Wechselmedium oder ein vorher installiertes Gerät die Laufwerksbuchstabenzuordnung weiterhin belegt 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 jedoch den Konflikt nicht lösen können, wenden Sie sich für technischen Support bitte an Kingston.com/support.

## Hilfe und Fehlerbehebung

### Fehlermeldungen

| | |
|---|---|
| **Datei kann nicht erstellt werden (Unable to Create File):**<br>Diese Fehlermeldung wird angezeigt, wenn Sie im schreibgeschützten Modus angemeldet sind und versuchen, eine Datei oder einen Ordner IN einer sicheren Datenpartition zu ERSTELLEN. |  <br>**Abb. 9.11 – Fehlermeldung „Datei kann nicht erstellt werden“** |
| **Fehler beim Kopieren einer Datei oder eines Ordners (Error copying file or folder):**<br>Diese Fehlermeldung wird angezeigt, wenn Sie versuchen, eine Datei oder einen Ordner auf die sichere Datenpartition zu KOPIEREN, während Sie im Schreibschutz-Modus angemeldet sind. |  <br>**Abb. 9.12. – Fehlermeldung „Datei oder Ordner kopieren nicht möglich“** |
| **Fehler beim Löschen einer Datei oder eines Ordners (Error deleting file or Folder):**<br>Diese Fehlermeldung erscheint, wenn Sie versuchen, eine Datei oder einen Ordner VON der sicheren Datenpartition zu LÖSCHEN, während Sie im Schreibschutz-Modus angemeldet sind. |  <br>**Abb. 9.13 – Fehlermeldung „Datei löschen oder Ordner bearbeiten nicht möglich“** |

**Hinweis:** Falls bereits eine Anmeldung im Schreibschutz-Modus erfolgt ist und der Stick entsperrt werden soll, um vollen Lese-/Schreibzugriff auf die sichere Datenpartition zu erhalten, muss der VP50 korrekt getrennt und erneut angemeldet werden, wobei das Kontrollkästchen „Schreibschutz-Modus (Read-Only Mode)“ nicht markiert sein darf.

# IRONKEY™ Vault Privacy 50 (VP50)
# CLÉ USB CHIFFRÉE 3.2 Gen 1

*Guide de l'utilisateur*

## Sommaire


Figure 1 : IronKey VP50

## Introduction

La Kingston IronKey Vault Privacy 50 (VP50) est une clé USB haut de gamme qui offre une sécurité de niveau professionnel grâce à un chiffrement matériel AES 256 bits certifié FIPS 197 en mode XTS. Elle offre également des protections contre les BadUSB via un micrologiciel signé numériquement et contre les attaques par force brute visant les mots de passe. La VP50 est également conforme à la TAA et assemblée aux États-Unis. Comme il s'agit d'un stockage chiffré sous le contrôle physique de l'utilisateur, la série VP50 est supérieure à Internet et aux services cloud pour la sauvegarde des données.

La VP50 prend en charge les options de mots de passe multiples (Admin, Utilisateur et Mot de passe de récupération à usage unique) avec les modes Complexe ou Phrase de passe. L'option de mots de passe multiples permet de récupérer l'accès aux données si l'un des mots de passe est oublié. Outre la prise en charge des mots de passe complexes traditionnels, 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 et un Mot de passe de récupération à usage unique ou réinitialiser le mot de passe Utilisateur pour restaurer l'accès aux données.

Pour faciliter la saisie du mot de passe, le symbole « œil » peut être activé pour révéler le mot de passe saisi, ce qui réduit les fautes de frappe pouvant générer des échecs de tentative de connexion. La protection contre les attaques par force brute verrouille le mot de passe Utilisateur ou le Mot de passe de récupération à usage unique si 10 mots de passe non valides sont saisis de suite, et chiffre le lecteur si le mot de passe Admin est saisi incorrectement 10 fois de suite.

Pour se protéger contre les logiciels malveillants potentiels sur les systèmes non fiables, l'Administrateur et l'Utilisateur peuvent définir le Mode lecture seule pour protéger la clé USB en écriture. En outre, le clavier virtuel intégré protège les mots de passe contre les enregistreurs de frappe ou d'écran.

Certifiées FIPS 197 et conformes TAA, les clés USB de la série VP50 peuvent être personnalisées et configurées avec un identifiant produit (PID) via le programme de personnalisation de Kingston. pour les intégrer à un logiciel standard de gestion des terminaux afin de répondre aux exigences des entreprises en matière d'informatique et de cybersécurité.

Les petites et moyennes entreprises peuvent utiliser le rôle Administrateur pour gérer leurs clés USB en local, par exemple pour configurer ou réinitialiser le mot de passe Utilisateur ou le Mot de passe de récupération à usage unique des employés, récupérer l'accès aux données sur des clés USB verrouillées, et se conformer aux lois et règlements lorsque des enquêtes sont nécessaires.

La VP50 bénéficie d'une garantie limitée de 5 ans avec le support technique gratuit de Kingston.

## Fonctionnalités de l'IronKey Vault Privacy 50

- Certifiée FIPS 197 avec un chiffrement matériel XTS-AES 256 bits (le chiffrement ne peut jamais être désactivé).
- Protection contre les attaques par force brute et BadUSB
- Mots de passe multiples
- Modes de mot de passe Complexe ou Phrase de passe
- Bouton en forme d'œil pour afficher les mots de passe saisis afin de réduire les tentatives de connexion ratées
- Clavier virtuel pour se protéger des enregistreurs de frappe et des enregistreurs d'écran
- Double paramètre de protection en lecture seule (protection en écriture) pour protéger le contenu de la clé USB contre les modifications ou les logiciels malveillants
- Les petites et moyennes entreprises peuvent gérer leurs clés USB en local en utilisant le rôle Administrateur
- Compatible avec Windows ou macOS (consulter la fiche technique pour plus de détails)

## À propos de ce manuel

Ce manuel d'utilisation concerne la clé USB IronKey Vault Privacy 50 (VP50). Il est basé sur la version en sortie d'usine, sans personnalisation.

## Système requis

| | |
|---|---|
| **Plateforme PC**<br>• Intel, AMD & Apple M1 SOC<br>• 15 Mo d'espace disque libre<br>• Port USB 2.0 – 3.2 disponible<br>• Deux lettres de lecteur consécutives après le dernier disque physique*<br><br>***Remarque :** Voir la section « Conflit de lettres de lecteur » à la page 32. | **Systèmes d'exploitation acceptés**<br>• Windows 11<br>• Windows 10<br>• Windows 8,1 |
| **Plateforme Mac**<br>• 15 Mo d'espace disque libre<br>• Port USB 2.0 – 3.2 | **Systèmes d'exploitation Mac pris en charge**<br>• macOS X (v. 10.13.x – 12.x.x) |

## Recommandations

Pour que la VP50 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 VP50 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 VP50 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 le disque est reformaté.

### 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 VP50 sur un système cible.
- Lorsque vous utilisez la clé USB sur un système public ou inconnu, vous pouvez définir le Mode lecture seule afin de la protéger contre les logiciels malveillants.
- Verrouillez la clé USB lorsque vous ne l'utilisez pas.
- Éjectez la clé USB avant de la débrancher.
- Ne débranchez jamais la clé USB lorsque son voyant est allumé. Cela peut 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 VP50 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 VP50 efface automatiquement les données chiffrées et s'auto-formate aux paramètres d'usine.

**Mots de passe multiples**
La VP50 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 VP50 peut prendre en charge trois mots de passe différents que vous pouvez utiliser pour récupérer des données : Admin, Utilisateur et Mot de passe de récupération à usage unique.

La VP50 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 ». En outre, l'Administrateur peut configurer le Mot de passe de récupération à usage unique pour l'Utilisateur afin de lui fournir un moyen de se connecter et de réinitialiser son mot de passe.

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. L'Utilisateur peut utiliser le Mot de passe de récupération à usage unique afin de réinitialiser son mot de passe en cas de besoin.

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 VP50 peut être réinitialisée et réutilisée, mais les données antérieures seront définitivement supprimées.

**Modes de mot de passe**
La VP50 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 VP50 prend en charge les phrases de passe de 10 à 64 caractères. Une phrase de passe ne suit aucune règle, 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 VP50, la langue du mot de passe peut correspondre à la langue sélectionnée pour le lecteur. Cela vous permet de sélectionner plusieurs mots, une phrase entière, les paroles d'une chanson, un vers extrait d'un

poème, etc. Les bonnes phrases de passe font partie des types de mots de passe les plus difficiles à deviner pour les attaquants, tout en étant plus faciles à retenir pour les utilisateurs.

## Configurer ma clé USB

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

### Accès à la clé USB (environnement Windows)

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

- Les utilisateurs de Windows 8.1/10/11 recevront une notification de pilote de périphérique. (Figure 3.1)


**Figure 3.1 – Notification du pilote de périphérique**

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

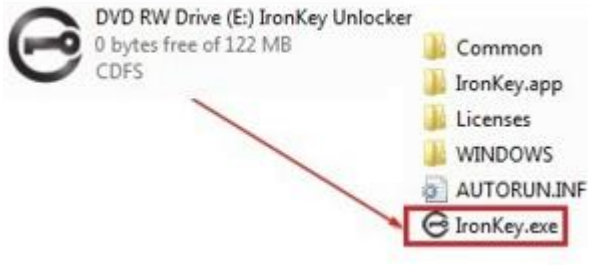



**Figure 3.2 – Fenêtre de l'Explorateur de fichiers/IronKey.exe**

### Accès à la clé USB (environnement macOS)

Insérez la VP50 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 IKVP50 (ou IRONKEY) s'affiche sur le bureau. (Figure 3.3)

- Double-cliquez sur l'icône CD-ROM IronKey.
- Double-cliquez ensuite sur l'icône de l'application IKVP50 (ou IronKey.app) affichée dans la fenêtre illustrée à la Figure 3.3. Cela lancera le processus d'initialisation.

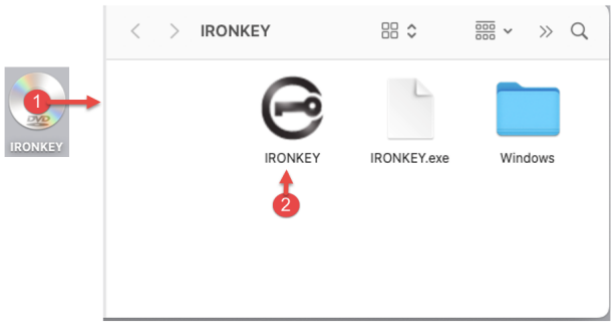
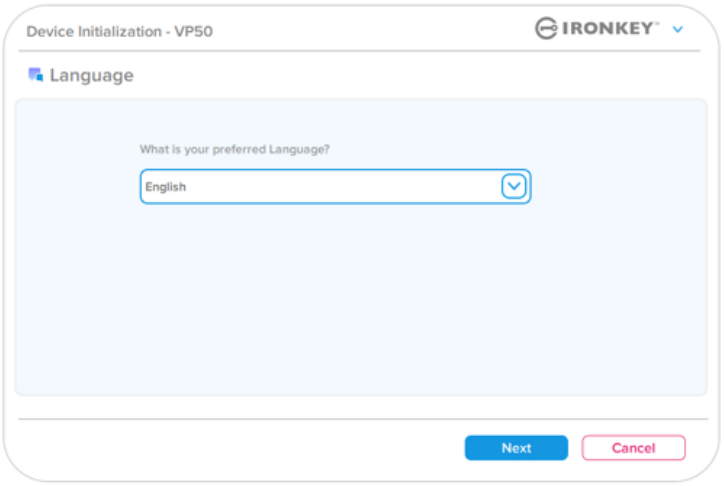
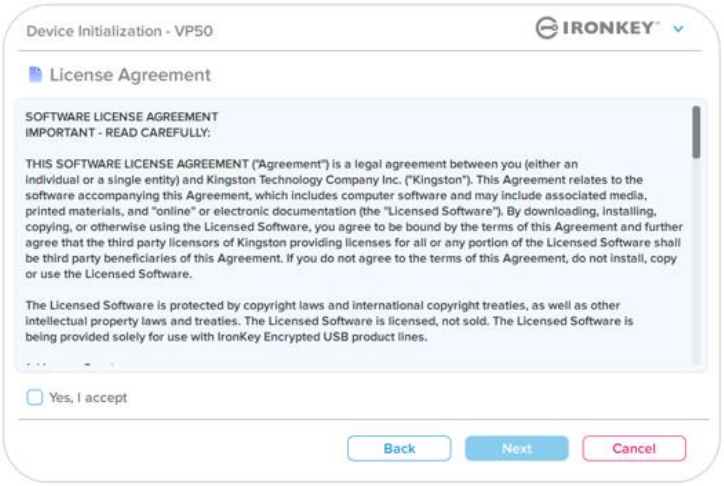



**Figure 3.3 – Volume IKVP**

| | |
|---|---|
| | |

## 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 l'illustration 4,1) |  <br>**Figure 4.1 – Sélection de la langue** |
| Lisez le contrat de licence et cliquez sur **Suivant (Next)**.<br><br>Remarque : Vous devez accepter le contrat de licence pour continuer. Autrement, le bouton **Suivant (Next)** restera désactivé. (Figure 4.2) |  <br>**Figure 4.2 – Contrat de licence** |

## Initialisation de la clé USB

### Sélection du mot de passe

Sur l'écran d'invite Mot de passe (Password), vous pourrez créer un mot de passe pour protéger vos données sur la VP50 en utilisant les modes Complexe (Complex) ou Phrase de passe (Passphrase) (Figures 4.3- 4.4). En outre, l'option de mots de passe multiples Activer les mots de passe Admin/Utilisateur (Enable Admin and User Passwords) peut également être activée 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 (Complex) ou Phrase de passe (Passphrase) 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 » (Password), puis saisissez-le à nouveau dans le champ « Confirmer le mot de passe » (Confirm Password). 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 Complexe**

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

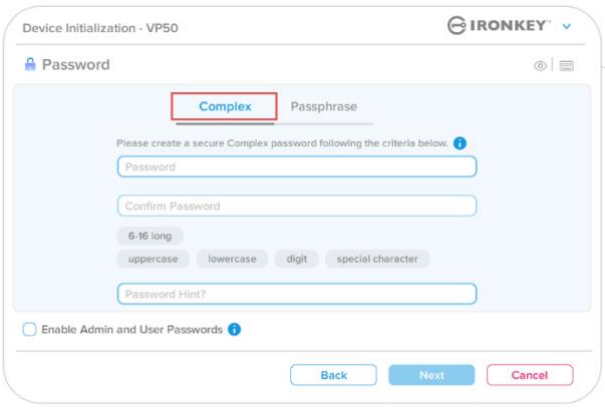



**Figure 4.3 – Mot de passe complexe**

**Phrase de passe**

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

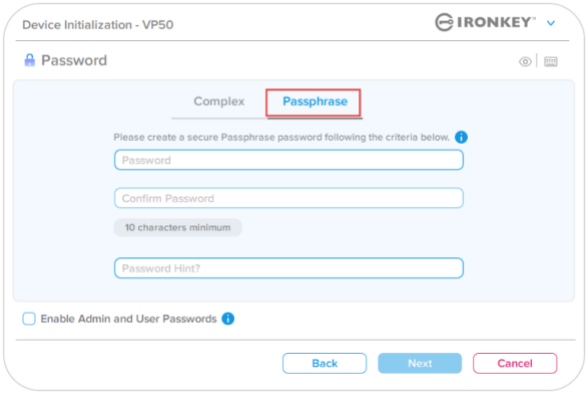



**Figure 4.4 – Phrase de passe**

**Indice de mot de passe (facultatif)**
Un indice de mot de passe (Password Hint) 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.

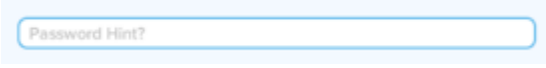



**Figure 4.5 – Champ Indice de mot de passe**

## 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)

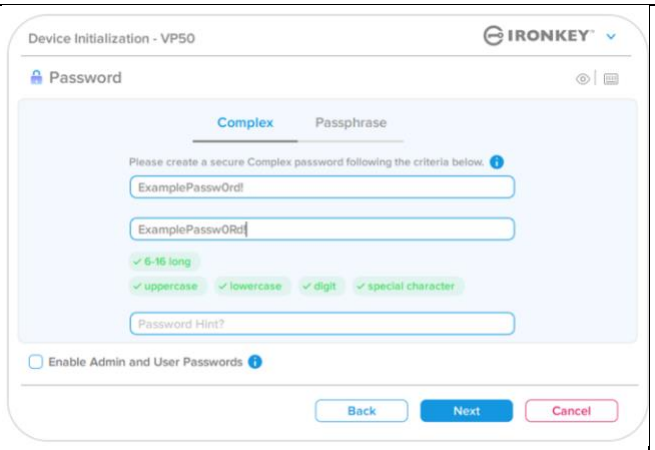



**Figure 4.6a – Condition de mot de passe complexe remplie**

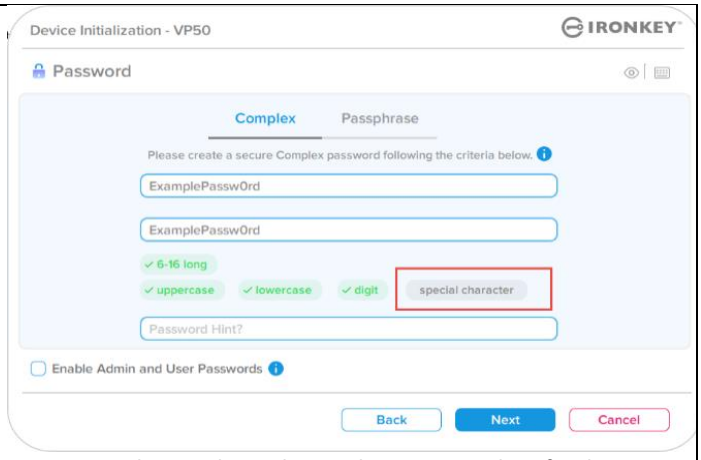



**Figure 4.6b – Condition de mot de passe complexe facultative**

Pour les mots de passe **non valides (Invalid)**, les cases de critères de mot de passe s'affichent en **rouge (red)** et le bouton **Suivant (Next)** 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.

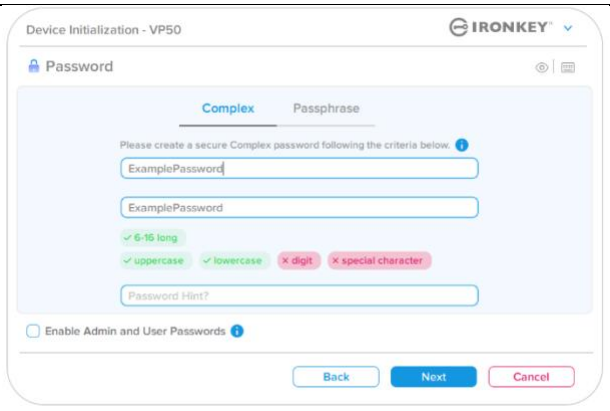



**Figure 4.7 – Condition de mot de passe non remplies**

## Initialisation de la clé USB

### Clavier virtuel

La VP50 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 – VP50) et sélectionnez-le.

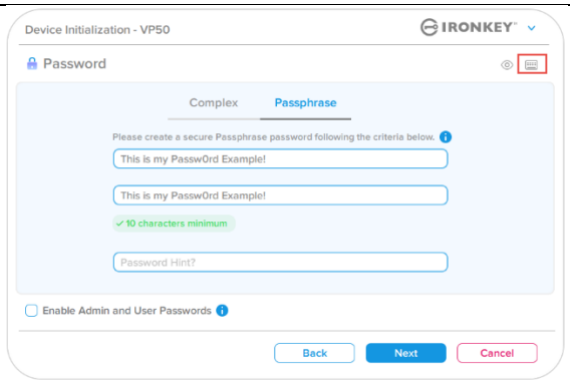



**Figure 4.8 – Activation du clavier virtuel**

- 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 (Randomize)** dans le coin inférieur droit du clavier. Le clavier sera alors organisé dans un ordre aléatoire.

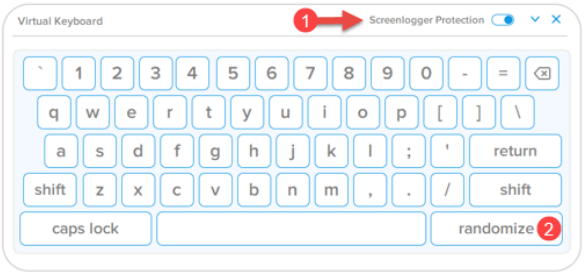



**Figure 4.9 – Protection contre les enregistreurs d'écran / Disposition aléatoire**

## Initialisation de la clé USB

### Icône de visibilité du mot de passe

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

**Remarque :** Une fois la clé USB initialisée, le champ du mot de passe sera « masqué » par défaut.

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

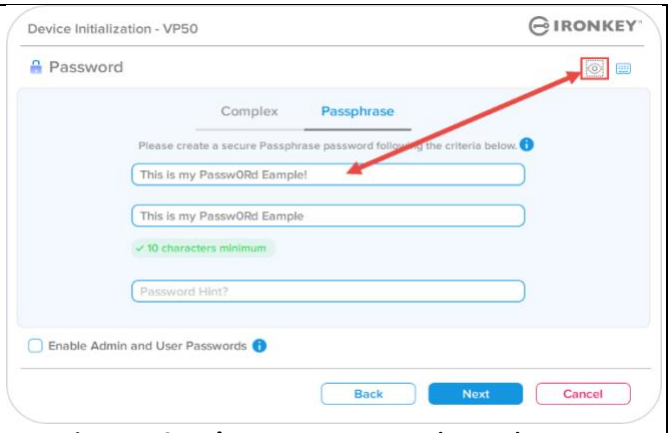



**Figure 4.10 – Icône pour « masquer » le mot de passe**

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

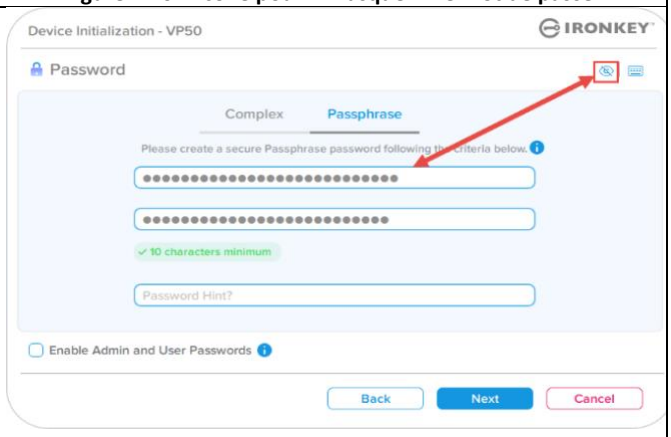



**Figure 4.11 – Icône pour « afficher » le mot de passe**

## Initialisation de la clé USB

### Mots de passe Admin et Utilisateur

En activant les mots de passe Admin et Utilisateur, vous pouvez tirer parti de la fonctionnalité de mots de passe multiples, via laquelle le rôle Administrateur peut gérer les deux comptes. En sélectionnant « **Activer les mots de passe Admin et Utilisateur** » **(Enable Admin and User Passwords)**, 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 :

- Mot de passe de récupération à usage unique
- Mode de lecture seule forcée pour la connexion Utilisateur
- Réinitialisation du mot de passe Utilisateur
- Forcer la réinitialisation du mot de passe pour la connexion Utilisateur

Pour en savoir plus sur ces options, allez à la page 25 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** » et sélectionnez **Suivant** une fois qu'un mot de passe valide a été choisi. (Figure 4.12)

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

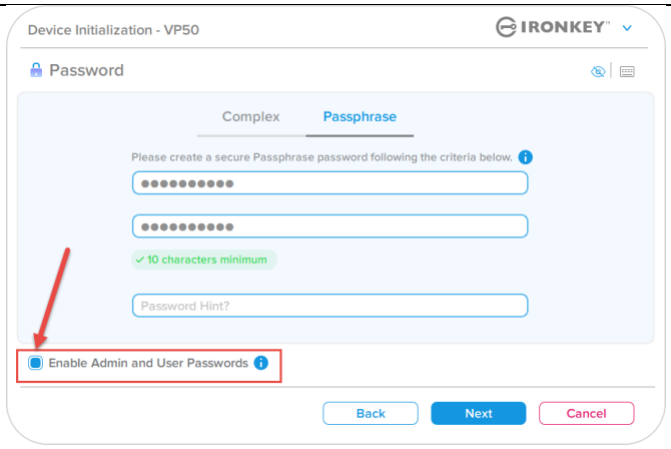



**Figure 4.12 – Activation des mots de passe Admin et Utilisateur**

**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.

**Remarque :** « **Mots de passe Admin et Utilisateur** » sera désigné par « **rôle Admin** » dans la suite du présent document.

## 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 dans le présent Guide de l'utilisateur. (voir la page 23)

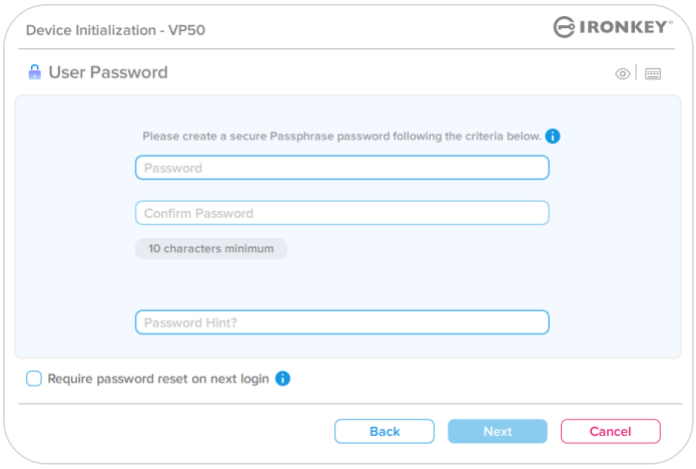



**Figure 4.13 – Mot de passe Utilisateur (Admin et Utilisateur activés)**

**Remarque :** Le critère Option de mot de passe choisi (Complexe ou Phrase de passe) sera appliqué au mot de passe Utilisateur, au Mot de passe de récupération à usage unique 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.

- La fonctionnalité « **Exiger la réinitialisation du mot de passe à la prochaine connexion** » **(Require password reset on next login)** située dans le coin inférieur gauche de la **Figure 4.13** ne concerne que le mot de passe Utilisateur. Elle peut être activée pour forcer l'Utilisateur à se connecter à l'aide du mot de passe temporaire défini par l'Administrateur au cours du processus d'initialisation, puis à le remplacer par un mot de passe de son choix une fois la clé USB authentifiée à l'aide de ce mot de passe temporaire. Cette fonctionnalité est utile lorsque la clé USB est confiée à une autre personne pour qu'elle l'utilise. (**Figure 4.14)**

  **Remarque :** Pour des raisons de sécurité, le nouveau mot de passe ne peut pas

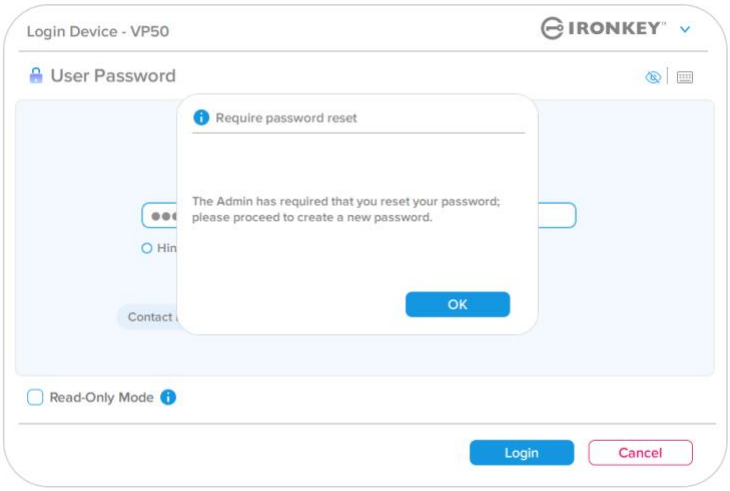



**Figure 4.14 – Exiger la réinitialisation du mot de passe à la prochaine connexion**
**(pour le mot de passe Utilisateur)**

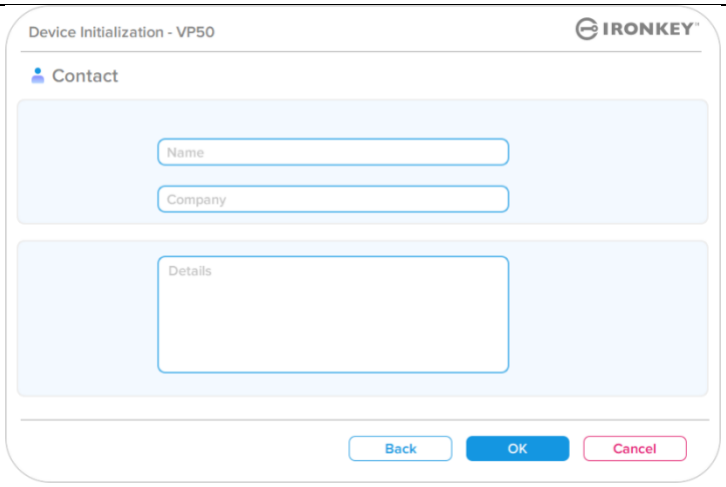
| | |
|---|---|
| être identique au mot de passe temporaire. | |

## Initialisation de la clé USB

### Informations de contact

Entrez vos informations de contact dans les zones de texte prévues à cet effet. (voir la 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**.<br><br>Le champ **« Société » (Company)** peut contenir jusqu'à 32 caractères, mais ne doit pas contenir le mot de passe **exact**.<br><br>Le champ « **Détails » (Details)** peut contenir jusqu'à 156 caractères, mais ne doit pas contenir le mot de passe **exact** . |  <br>**Figure 4.14 – Informations de contact** |

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

## Utilisation de la clé USB (environnements Windows & 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 VP50 se lancera, en affichant d'abord l'écran de connexion Mot de passe Utilisateur (User Password) . 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 5.1). 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 (Admin Password) , où vous pouvez vous connecter en tant qu'administrateur pour accéder aux paramètres et fonctionnalités Admin. (Figure 5.2)

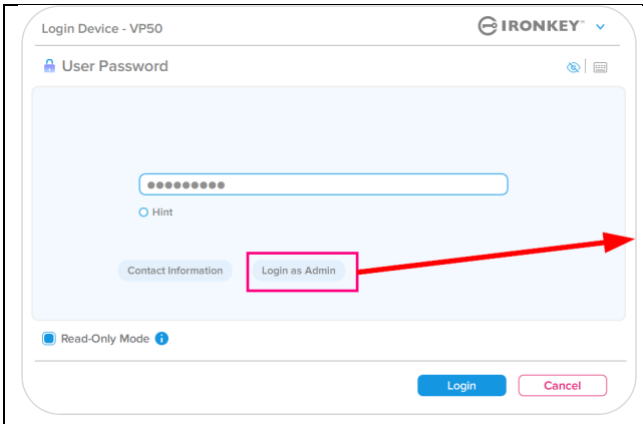



**Figure 5.1 – Connexion à l'aide du Mot de passe Utilisateur (Admin activé)**

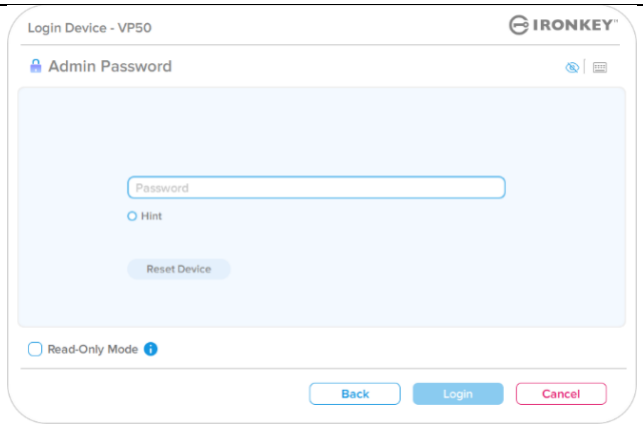



**Figure 5.2 – Connexion à l'aide du Mot de passe Admin**

### 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 dispositif, 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 5.3)

**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**

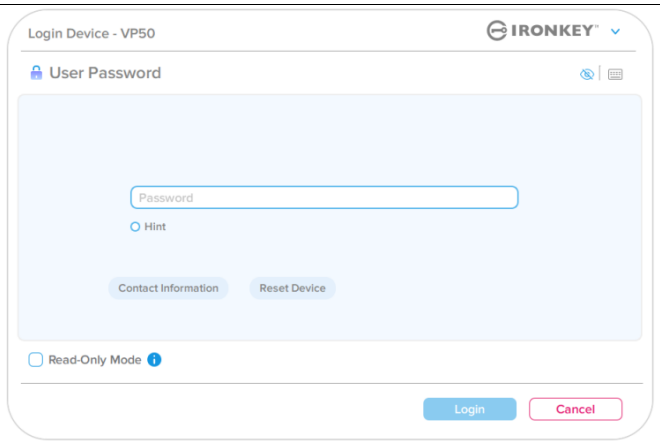



**Figure 5.3 – Connexion à l'aide du mot de passe Utilisateur (Admin non activé)**

| | |
|---|---|
| **clé USB entraîne un formatage de la clé et la perte définitive de TOUTES les données qu'elle contient.** | |

## Utilisation de la clé USB

### Déverrouillage en Mode lecture seule

Vous pouvez déverrouiller votre clé USB IronKey en mode lecture seule afin que ses fichiers ne puissent pas être modifiés. Par exemple, lorsque vous utilisez un ordinateur non fiable ou inconnu, le fait de déverrouiller votre clé USB en mode de lecture seule empêchera tout logiciel malveillant sur cet ordinateur d'infecter votre clé USB ou de modifier vos fichiers.

Lorsque vous travaillez dans ce mode, vous ne pouvez pas effectuer d'opérations qui impliquent la modification de fichiers sur la clé USB.
Par exemple, vous ne pouvez pas la reformater ou y restaurer, ajouter ou modifier des fichiers.

Pour déverrouiller la clé en mode Lecture seule :

1. Insérez la clé USB dans le port USB de l'ordinateur hôte et exécutez le fichier **IronKey.exe**.
2. Cochez la case **Mode lecture seule (Read-Only Mode)** sous la zone de saisie du mot de passe. (**Figure 5.4)**
3. Saisissez le mot de passe de votre clé USB et cliquez sur **Connexion (Login)**. La clé USB IronKey est désormais déverrouillée en Mode lecture seule.

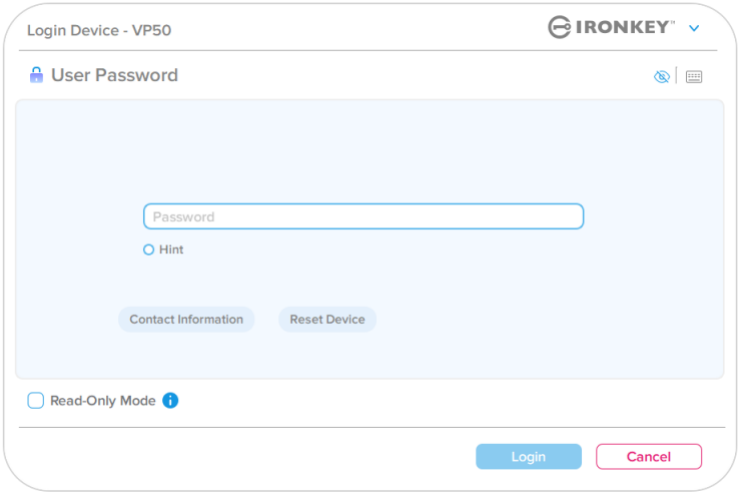



**Figure 5.4 – Mode lecture seule**

Si vous souhaitez déverrouiller la clé USB avec un accès complet en lecture/écriture à la partition de données sécurisée, vous devez arrêter la VP50 et vous reconnecter, en laissant la case « Mode lecture seule » (Read-Only Mode) décochée.

**Remarque :** Les options Admin de la VP50 ont une fonctionnalité Mode lecture seule forcée pour les données Utilisateur, ce qui signifie que l'Administrateur peut forcer le déverrouillage de la connexion de l'Utilisateur en lecture seule (voir **page 28** pour plus de détails).

## 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 ou utilisez le Mot de passe de récupération à usage unique pour réinitialiser le mot de passe Utilisateur | NON |
| Mot de passe Admin | Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimées définitivement | **OUI** |
| Mot de passe de récupération à usage unique | Verrouillage du mot de passe, le bouton de récupération du mot de passe s'estompe et devient inutilisable. Connectez-vous en tant qu'Administrateur pour réinitialiser le mot de passe | NON |
| **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** |

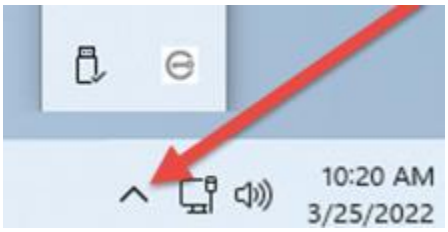
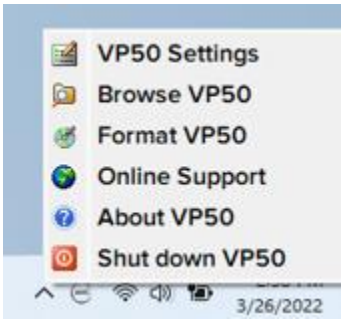
* Une fois que vous vous êtes authentifié avec succès sur la clé USB, le compteur d'échecs de connexion sera réinitialisé en fonction de la méthode de connexion utilisée. L'effacement chiffré effacera tous les mots de passe, les clés de chiffrement et les données ; **vos données seront perdues définitivement.**

### Accès à mes fichiers sécurisés

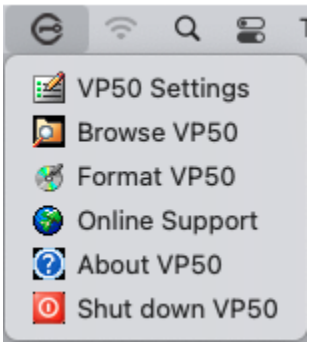
Après avoir déverrouillé la clé USB, vous pouvez accéder à vos fichiers sécurisés. Les fichiers sont automatiquement chiffrés et déchiffrés lorsque vous les enregistrez ou les ouvrez sur la clé USB. Cette technologie vous permet de travailler comme vous le feriez avec un disque ordinaire, tout en offrant 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 VP50.** (Figure 6.2)

## Options de la clé USB (environnement Windows)

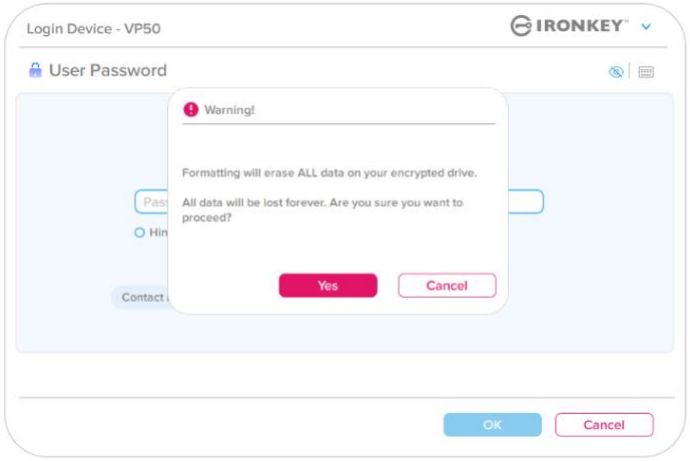
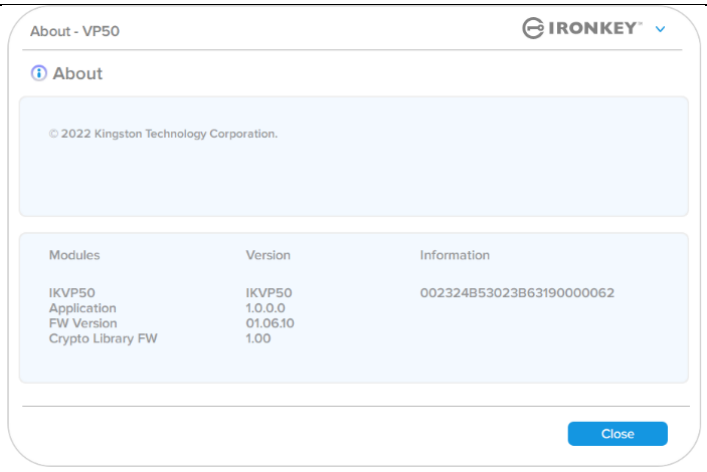
Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles. (Figure 6.2)
Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.

| | |
|---|---|
| • Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. **(Figure 6.1)** |  **Figure 6.1 – Icône IronKey dans la barre des tâches** |
| • Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles. **(Figure 6.2)**<br><br>Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel. |  **Figure 6.2 – 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 VP50 » se trouve dans le menu macOS illustré dans la **Figure 6.3** ; elle permet d'afficher les options disponibles de la clé USB.<br><br>Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel. |  **Figure 6.3 – Barre de menu macOS, icône/menu des options de la clé USB** |

## Options de la clé USB

| | |
|---|---|
| **Paramètres de la VP50 (VP50 Settings) :** | • 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 VP50 » du présent manuel). |
| **Parcourir la VP50 (Browse VP50) :** | • Permet de visualiser vos fichiers sécurisés. |
| **Formater la VP50 (Format VP50) :** Permet de formater la partition de données sécurisée. (Avertissement : Toutes les données seront supprimées) (**Figure 6.1**)<br><br>**Remarque :** L'authentification par mot de passe sera requise pour le formatage. |  <br>**Figure 6.1 – Formater la VP50** |
| **Support en ligne (Online Support) :** | • 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 VP50 (About VP50) :** Afficher des données détaillées sur la VP50, notamment des informations sur l'application, le firmware et le numéro de série. (**Figure 6.2**)<br><br>**Remarque :** Le numéro de série unique de la clé USB se trouve sous la colonne « Informations ». |  <br>**Figure 6.2 – À propos de la VP50** |
| **Arrêter la VP50 (Shut down VP50) :** | • Permet de fermer correctement la VP50 avant de la déconnecter physiquement du système, en toute sécurité. |

## Paramètres de la VP50

### 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 7.1*)
- **Informations de contact (Contact Info) :** Permet d'ajouter/d'afficher/de modifier les informations de contact (*Figure 7.2*)
- **Langue (Language) :** Permet de modifier la langue actuelle (*Figure 7.3*)
- **Options Admin (Admin Options) :** Permet d'activer des fonctionnalités supplémentaires telles que : (Figure 7.4)
    - Changer le mot de passe de l'utilisateur
    - Réinitialisation du mot de passe de connexion (pour le mot de passe Utilisateur)
    - Activer un mot de passe de récupération à usage unique
    - Forcer le mode lecture seule pour les données Utilisateur

**REMARQUE :** Des détails supplémentaires sur les options Admin sont indiqués à la page 24.

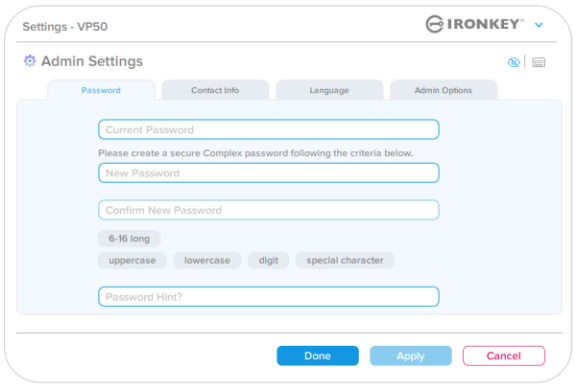



**Figure 7.1 – Options de mot de passe**

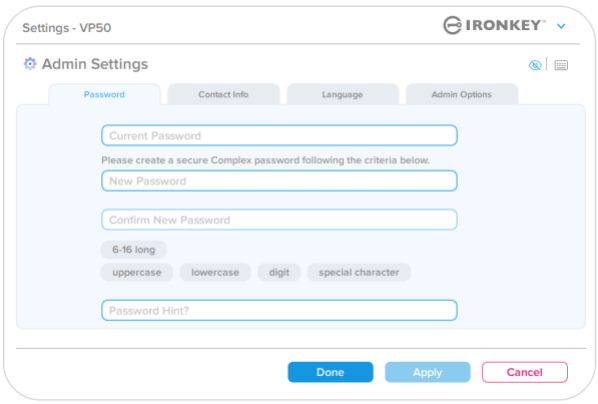



**Figure 7.2 – Informations de contact**

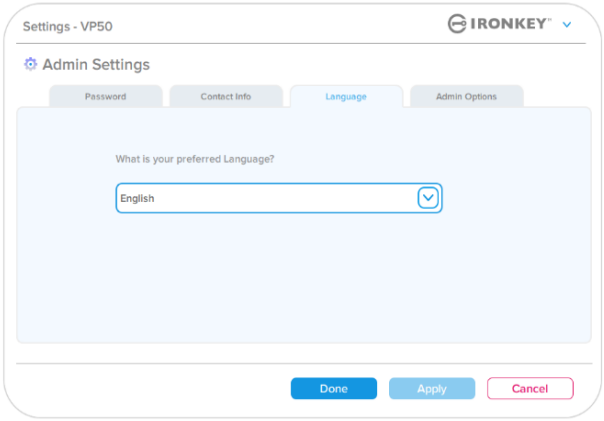



**Figure 7.3 – Options de langue**

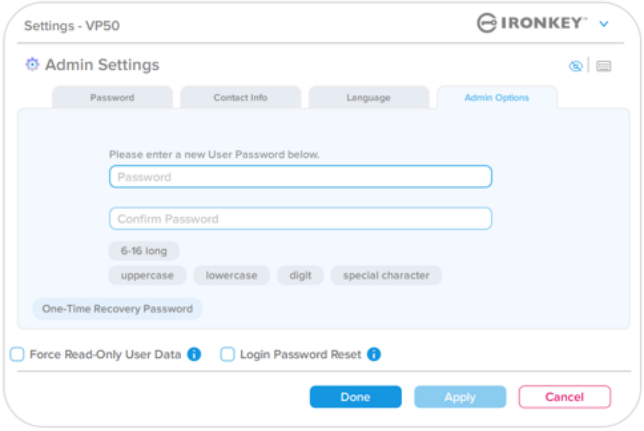



**Figure 7.4 – Options Admin**

## Paramètres de la VP50

### 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 7.5*)

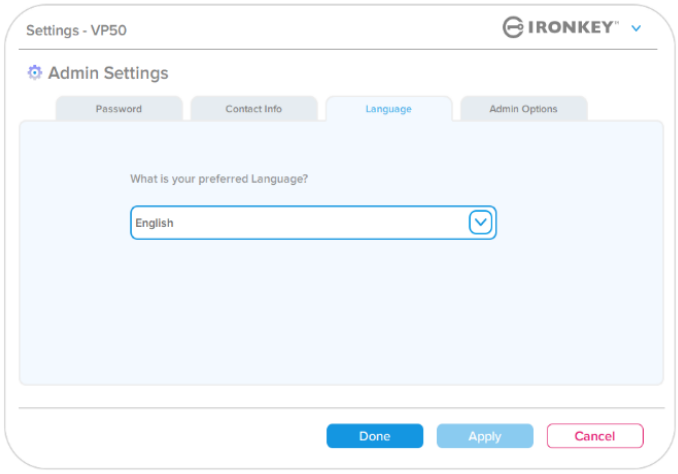



**Figure 7.5 – Options de mot de passe (Admin activé : connexion de l'Utilisateur)**

**Informations de contact (Contact Info) :**
Permet d'ajouter/d'afficher/de modifier les informations de contact. (*Figure 7.6*)

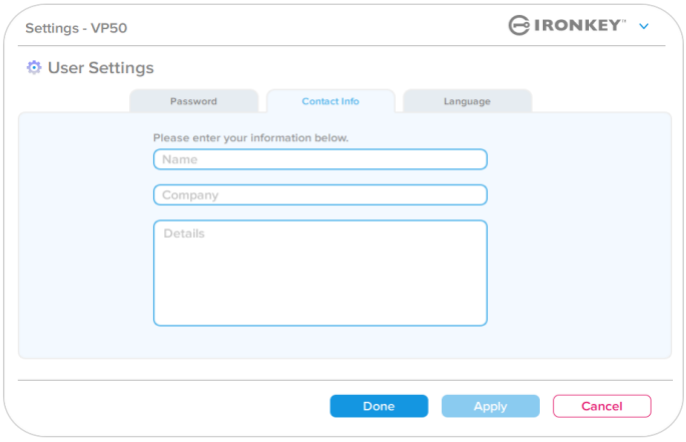
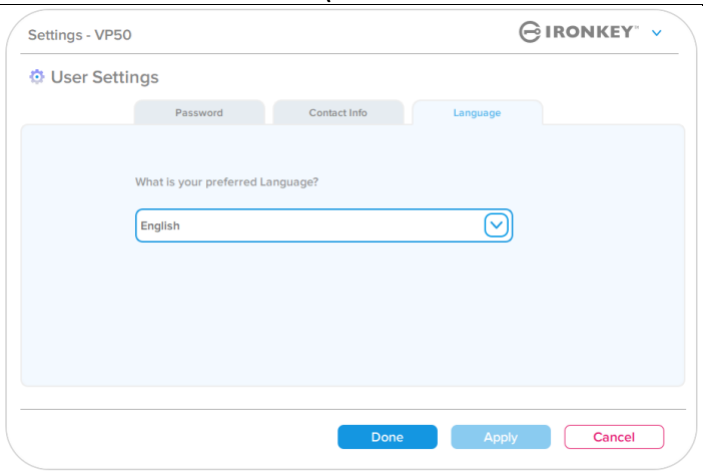



**Figure 7.6 – Informations de contact (Admin activé : connexion de l'Utilisateur)**

**Langue (Language) :**
Permet de modifier votre sélection de langue actuelle. (*Figure 7.7*)



| | |
|---|---|
| | **Figure 7.7 – Paramètres de langue (Admin activé : connexion de l'Utilisateur)** |

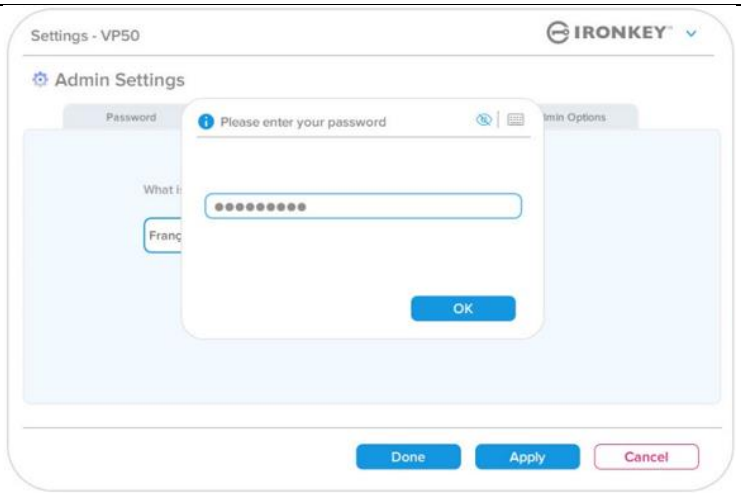
**Remarque** : Les options Admin ne sont pas accessibles lorsque la connexion est établie à l'aide du mot de passe Utilisateur.

## Paramètres de la VP50

### Paramètres utilisateur : Admin non activé

Comme mentionné précédemment à la page 12, l'initialisation de la VP50 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 VP50 :

### Modifier et sauvegarder les paramètres

| | |
|---|---|
| • Chaque fois que les paramètres sont modifiés dans les Paramètres de la VP50 (par exemple : coordonnées, 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 7.11) |  <br>**Figure 7.11 – Écran d'invite du mot de passe pour sauvegarder les modifications des paramètres de la VP50** |

**Remarque** : Si vous êtes sur l'écran d'invite du mot de passe ci-dessus et que vous souhaitez annuler ou modifier vos modifications, vous pouvez le faire en vous assurant simplement que le champ du mot de passe est vide et en cliquant sur « OK ». Cela fermera la boîte de dialogue « Veuillez saisir votre mot de passe » (Please enter your password) et vous ramènera au menu des paramètres de la VP50.

## Fonctionnalités Admin

**Options disponibles pour réinitialiser le mot de passe Utilisateur**

Les fonctionnalités de la configuration Admin offrent plusieurs façons de réinitialiser en toute sécurité le mot de passe Utilisateur en cas d'oubli, ou si un mot de passe temporaire est créé et que vous souhaitez imposer un changement de mot de passe lors de la prochaine connexion Utilisateur. Vous trouverez ci-dessous les fonctionnalités qui peuvent être utiles 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 » (Admin Options). Ce changement est instantané ; il prendra effet à la prochaine connexion de l'Utilisateur. **(Figure 8.1)**

**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).

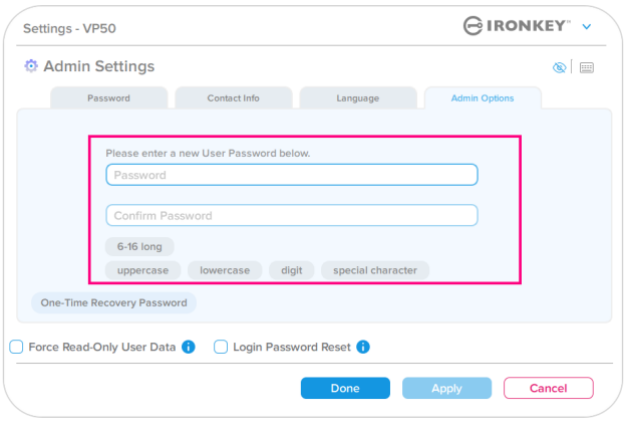



**Figure 8.1 – Options Admin/réinitialisation du mot de passe Utilisateur**

**Réinitialisation du mot de passe à la connexion (Login Password Reset) :**
L'activation de la réinitialisation du mot de passe **obligera l'Utilisateur à se connecter en utilisant le mot de passe temporaire défini par l'Administrateur**, puis à le changer pour un mot de passe de son choix. Cette fonctionnalité est utile lorsque la clé USB est confiée à une autre personne pour qu'elle l'utilise. (**Voir les Figures 8.2A et 8.2B**)

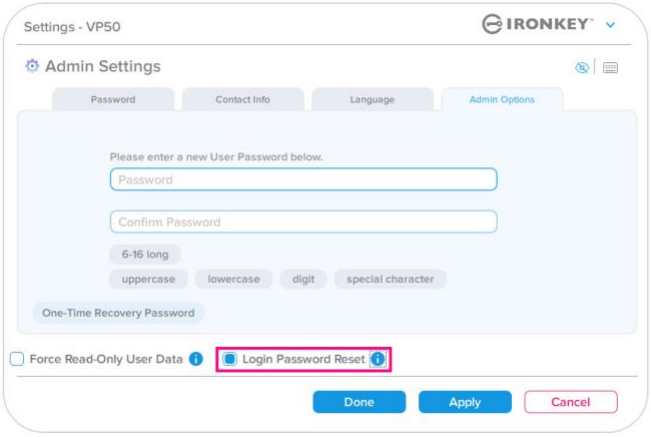



**Figure 8.2A – Bouton de réinitialisation des mots de passe de connexion**

**Remarque :** Cette réinitialisation prendra effet lors de la prochaine connexion réussie de l'Utilisateur. Les critères du mot de passe seront automatiquement appliqués en fonction de l'option initiale définie pendant le processus d'initialisation (Complexe ou Phrase de passe).

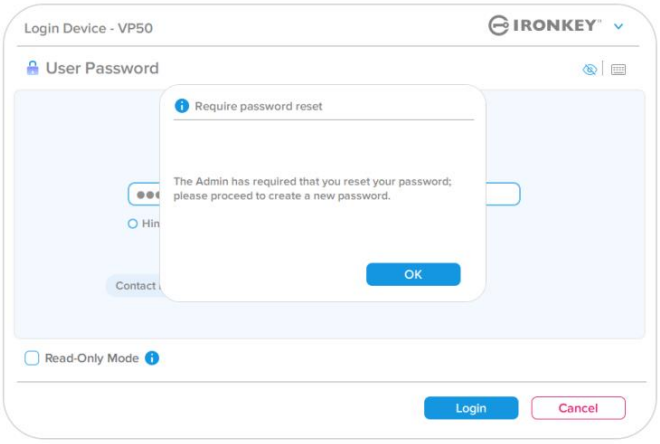



**Figure 8.2B – Notification de réinitialisation après saisie du mot de passe Utilisateur**

## Fonctionnalités Admin

### Mot de passe de récupération à usage unique

Cette section traite du processus d'activation et d'utilisation de la fonctionnalité Mot de passe de récupération à usage unique.

**Mot de passe de récupération à usage unique**

**Étape 1 :** La fonctionnalité Mot de passe de récupération à usage unique est un mot de passe à usage unique très utile qui peut être activé pour récupérer et réinitialiser le mot de passe Utilisateur en cas d'oubli de ce dernier. Cliquez sur le bouton « Mot de passe de récupération à usage unique » (One-Time Recovery Password) dans le menu des options Admin pour commencer. **(Figure 8.4)**

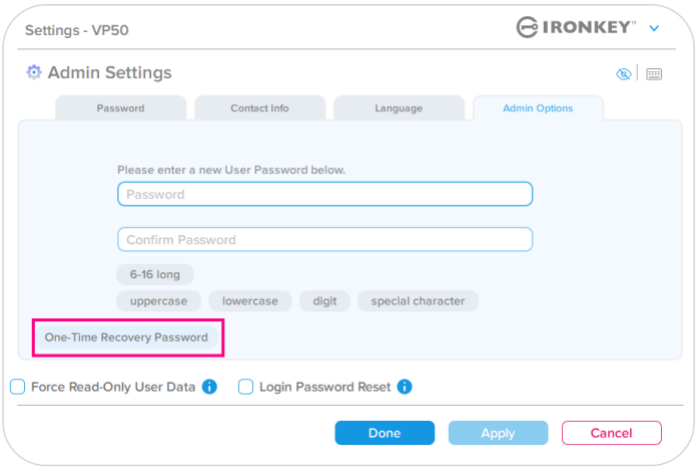



**Figure 8.4 – Bouton Mot de passe de récupération à usage unique**

**Étape 2 :** Créez un mot de passe de récupération à usage unique en utilisant le même critère que celui utilisé initialement pour la clé USB (Complexe ou Phrase de passe).

**Remarque :** Le mot de passe Admin sera nécessaire pour appliquer les modifications.

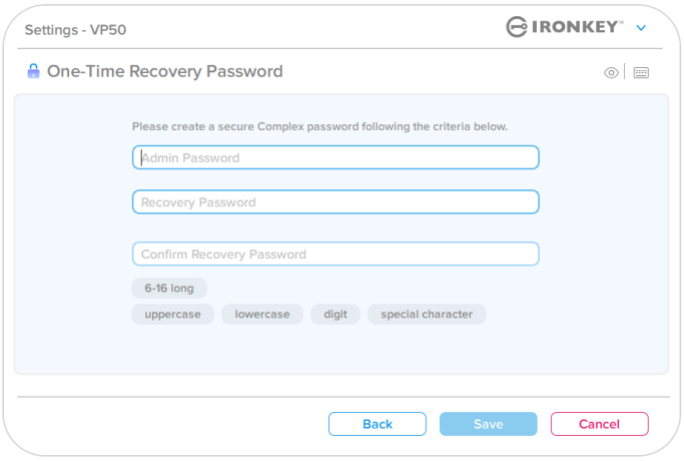
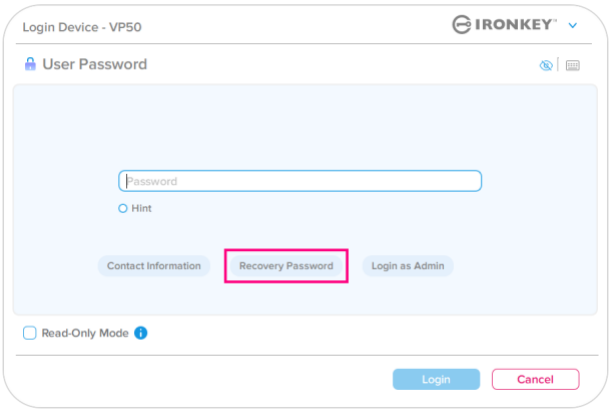
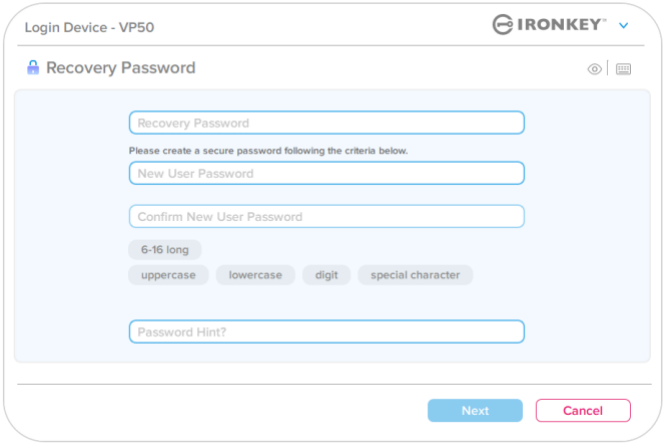
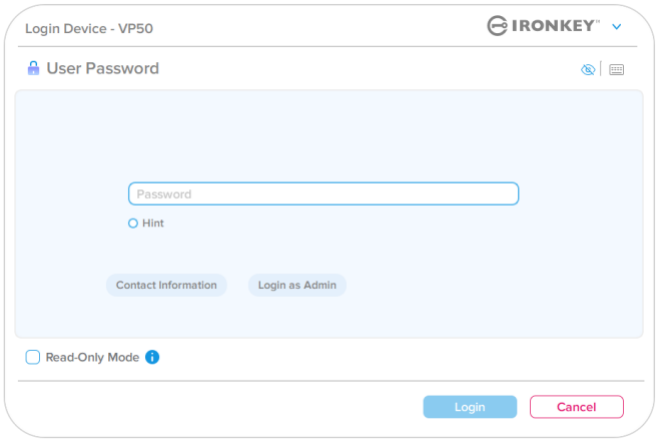



**Figure 8.5 – Configuration du mot de passe de récupération à usage unique**

## Fonctionnalités Admin

Utilisation du mot de passe de récupération à usage unique

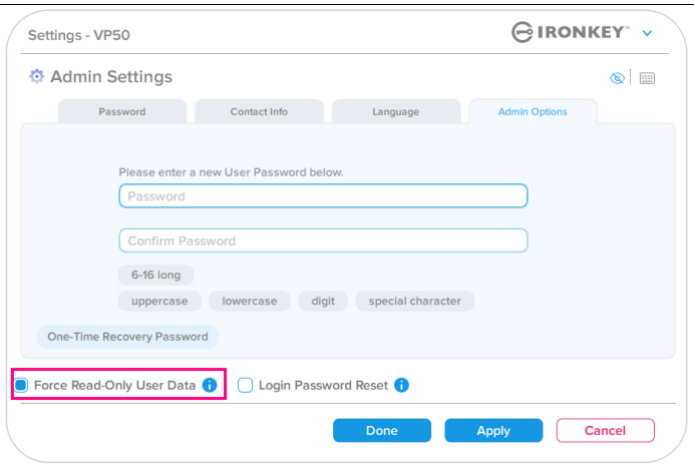
| | |
|---|---|
| **Étape 1 :** Après la création du mot de passe de récupération à usage unique, un nouveau bouton apparaîtra sur l'écran de connexion **Mot de passe Utilisateur (User Password)** lors de la prochaine connexion. Cliquez sur le bouton **Mot de passe de récupération (Recovery Password)** pour lancer le processus. |  <br>**Figure 8.6 – Bouton Mot de passe de récupération** |
| **Étape 2 :** L'écran **Mot de passe de récupération (Recovery Password)** s'affiche et vous permet d'entrer le mot de passe de récupération et de créer un nouveau mot de passe Utilisateur. (Figure 8.7)<br><br>**Important :** Le mot de passe de récupération à usage unique utilise également une fonctionnalité de sécurité intégrée qui comptabilise le nombre de tentatives de connexion ratées. **Après 10 saisies incorrectes du mot de passe de récupération à usage unique, ce dernier sera désactivé** et devra être réactivé en se connectant à la clé USB en tant qu'Admin. (voir les pages 18 et 30 pour plus de détails) |  <br>**Figure 8.7 – Menu Mot de passe de récupération** |

| | |
|---|---|
| **Étape 3 :** En cas de succès, vous serez ramené à l'écran **Mot de passe Utilisateur (User Password)**. Le bouton **Mot de passe de récupération (Recovery Password)** est maintenant absent, et le mot de passe Utilisateur saisi à l'**étape 2** deviendra le nouveau mot de passe Utilisateur. (Figure 8.8) |  **Figure 8.8 – Écran de connexion du mot de passe Utilisateur montrant que le bouton Mot de passe de récupération disparaît une fois utilisé correctement.** |

## Fonctionnalités Admin

### Forcer la lecture seule pour les données Utilisateur

La fonctionnalité Mode lecture seule forcée peut être activée pour restreindre l'accès en écriture à la clé USB pour l'Utilisateur. Cette fonctionnalité est utile si l'accès aux fichiers qu'elle contient doit être en lecture seule.

| | |
|---|---|
| • Pour activer l'option Forcer la lecture seule pour les données Utilisateur (Force Read-Only User Data), cochez la case correspondante et cliquez sur « Appliquer » (Apply). **(Figure 8.9)**<br><br>**Remarque :** Ce mode de lecture seule forcée ne s'applique qu'à l'Utilisateur et ne concerne pas la connexion Admin. La connexion Admin aura toujours les privilèges d'accès en lecture et en écriture, et pourra toujours activer le Mode lecture seule si nécessaire. |  **Figure 8.9 – Activer l'option « Forcer la lecture seule pour les données Utilisateur »**<br>**(Le mot de passe Admin sera nécessaire pour appliquer les modifications)** |
| • Une fois cette option activée, le bouton **« Mode lecture seule » (Read-Only Mode)** devient bleu, ce qui signifie que le mode de lecture seule forcée est activé en permanence pour le mot de | |

passe Utilisateur, jusqu'à ce qu'il soit désactivé par l'Admin. (Figure 8.10)

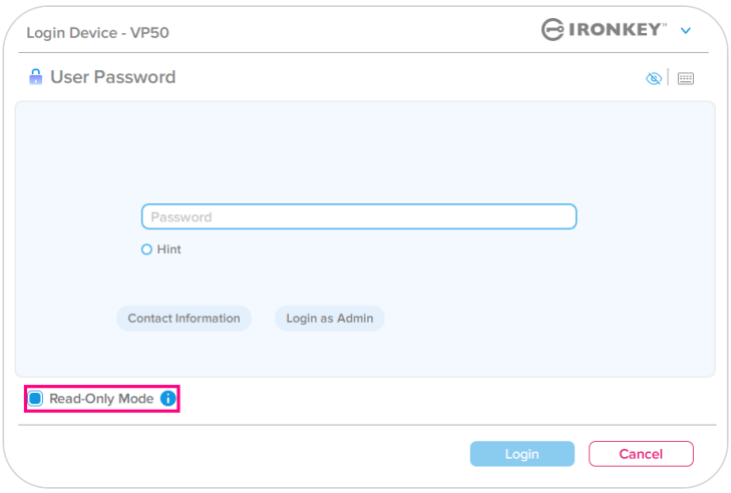



**Figure 8.10 – Le mode Lecture seule est activé de manière forcée pour l'utilisateur et ne peut être désactivé que par l'administrateur.**

## Aide et dépannage

### Verrouillage de la clé USB

LA VP50 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/Mot de passe de récupération à usage unique).

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 9.1)

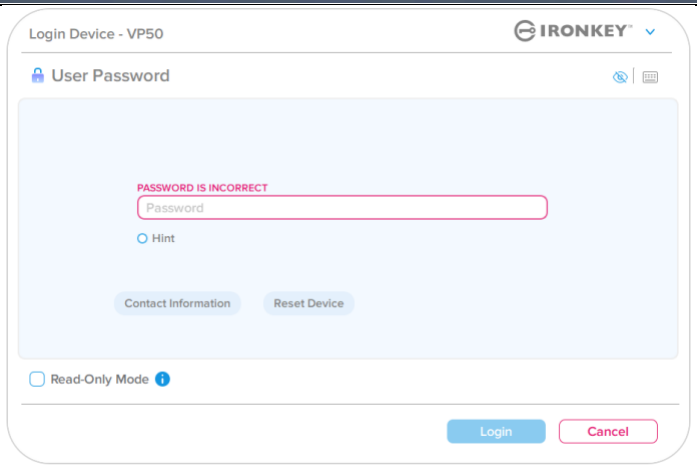



**Figure 9.1 – Message Mot de passe incorrect**

- 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 9.2)

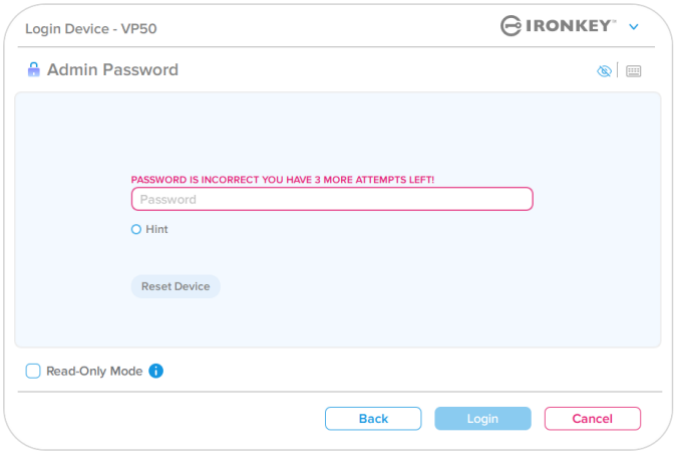



**Figure 9.2 – 7ème tentative de saisie de mot de passe ratée**

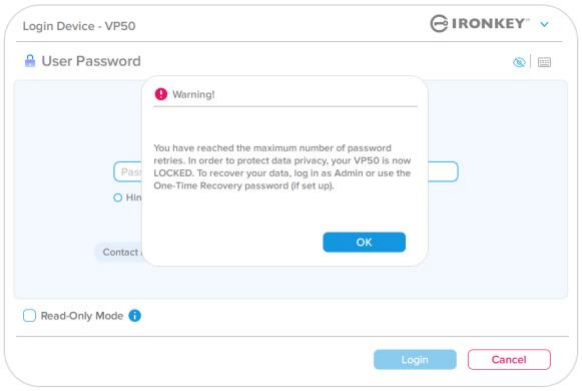
## Aide et dépannage

### 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 ou Mot de passe de récupération à usage unique), 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 9.3- 9.6 ci-dessous illustrent le comportement visuel pour la 10ème et dernière tentative de connexion ratée pour chaque méthode de mot de passe de connexion :

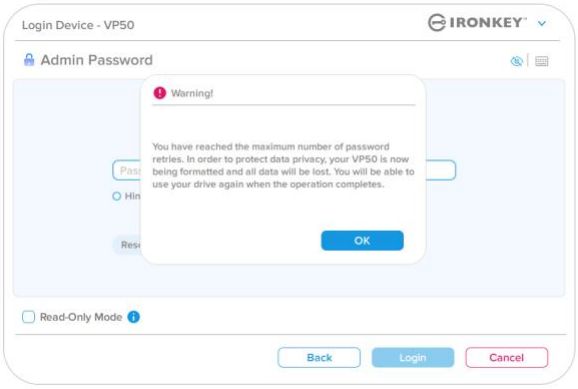
**Mot de passe Utilisateur : (activé par l'Admin/Utilisateur)**




**VERROUILLAGE DE LA CLÉ USB**

**(Figure 9.3)**

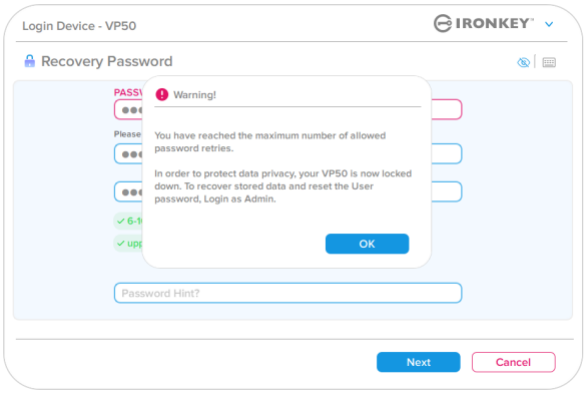
**Mot de passe Admin (activé par l'Admin/Utilisateur)**




**FORMATAGE DE LA CLÉ USB***

**(Figure 9.4)**

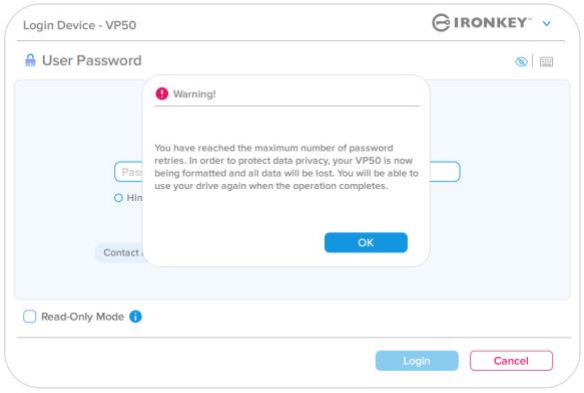
**Mot de passe de récupération à usage unique : (activé par l'Admin/Utilisateur)**




**VERROUILLAGE DE LA CLÉ USB**

**(Figure 9.5)**

**Mot de passe utilisateur (Admin NON activé)**




**FORMATAGE DE LA CLÉ USB***

**(Figure 9.6)**

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 VP50 et que vous avez oublié votre mot de passe, cette mesure de sécurité sera également appliquée et aboutira au formatage de la clé USB. * Pour en savoir plus sur cette fonctionnalité, voir la section *Réinitialiser la clé USB* à la page 25.

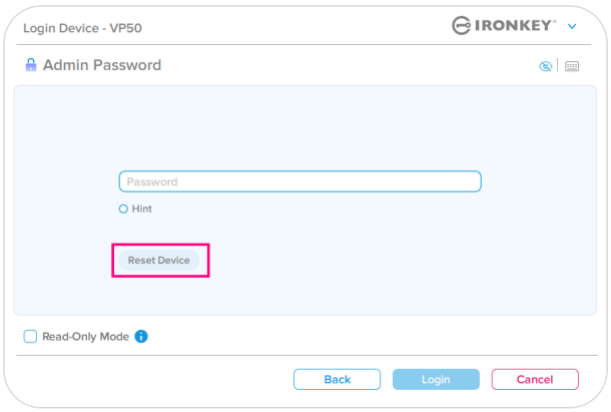
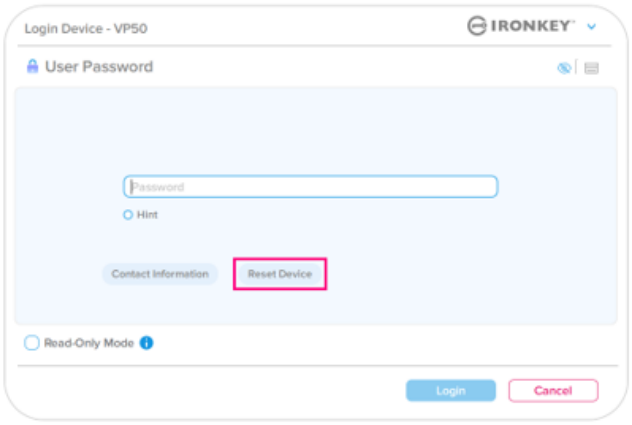
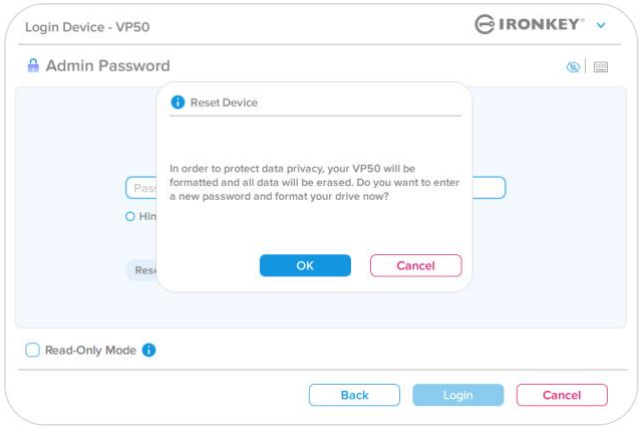
**Remarque : Un formatage de la VP50 supprimera TOUTES les informations stockées sur sa partition de données sécurisée.*

## 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 » (Reset Device)* qui peut apparaître à deux endroits selon la configuration de la clé (soit dans le menu Mot de passe de connexion Admin (Admin Password) si le mode Admin/Utilisateur est activé, soit

dans le menu « Mot de passe de connexion Utilisateur » (User Password) si le mode Admin/Utilisateur n'est pas activé) lorsque le programme VP50 Launcher est exécuté. (voir la ***Figure 9.7*** et la **Figure 9.8)**

| | |
|---|---|
| • Cette option vous permet de créer un nouveau mot de passe, mais pour protéger la confidentialité de vos données, la VP50 sera formatée. Par conséquent, ce processus effacera définitivement toutes vos données.* |  **Figure 9.7 – Mot de passe Admin : Bouton de réinitialisation de la clé** |
| • **Remarque :** Lorsque vous cliquez sur le bouton « *Réinitialiser le mot de passe* » *(Reset Password)*, 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 » (Cancel) pour revenir à la fenêtre de connexion. (Voir la Figure 9.8) |  **Figure 9.8 – Mot de passe Utilisateur (Admin/Utilisateur non activé) – Réinitialisation de 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 9.9 – Confirmation de réinitialisation de la clé USB** |

## Aide et dépannage

### Conflit de lettres de lecteur : Systèmes d'exploitation Windows

- Comme indiqué dans la section « *Configuration système* » du présent manuel (page 3), la VP50 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 9.10*). Cette attribution est indépendante des partages de réseau parce que ces partages sont spécifiques aux profils d'utilisateur et pas au profil matériel du système. Une lettre attribuée à un volume du réseau peut donc apparaître comme disponible pour le système d'exploitation.

- Autrement dit, Windows peut attribuer à la VP50 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). Comme indiqué dans la section « *Configuration système* » du présent manuel (page 3), la VP50 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 9.10*). Cette attribution est indépendante des partages de réseau parce que ces partages sont spécifiques aux profils d'utilisateur et pas au profil matériel du système. Une lettre attribuée à un volume du réseau peut donc apparaître comme disponible pour le système d'exploitation.

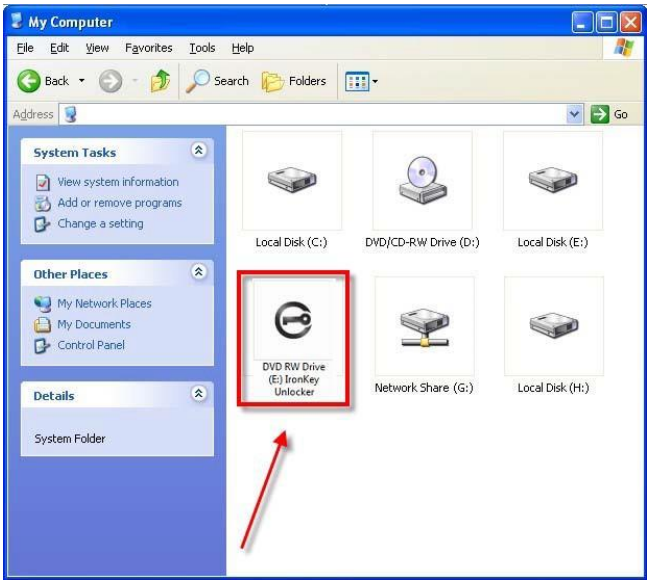



**Figure 9.10 – Exemple de lettre de lecteur**

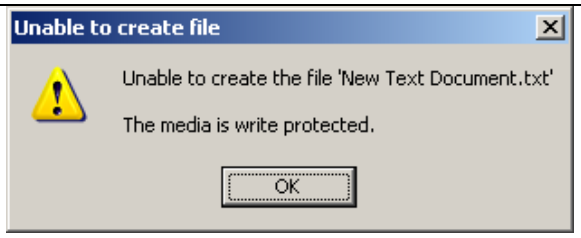
Dans cet exemple (Figure 9.10), la VP50 utilise le lecteur F:, qui est la première lettre de lecteur disponible après le lecteur E: (qui est le dernier disque physique affiché avant l'écart dans l'attribution des lettres de lecteurs). Comme la lettre G: est un partage réseau et qu'elle ne fait pas partie du profil matériel, la VP50 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 VP50 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.

## Aide et dépannage

### Messages d'erreur

| | |
|---|---|
| **Impossible de créer le fichier (Unable to create file) :** Ce message d'erreur s'affiche lorsque vous tentez de CRÉER un fichier ou un dossier SUR la partition de données sécurisée alors que vous êtes connecté en mode lecture seule. |  <br>**Figure 9.11 – Erreur « Impossible de créer le fichier »** |
| **Erreur lors de la copie du fichier ou du dossier (Error Copying File or Folder) :** Ce message d'erreur s'affiche lors d'une tentative de COPIE d'un fichier ou d'un dossier vers la partition de données sécurisée, alors que vous êtes connecté en mode lecture seule. |  <br>**Figure 9.12 – « Erreur lors de la copie du fichier ou du dossier »** |
| **Erreur lors de la suppression du fichier ou du dossier (Error Deleting File or Folder) :** Ce message d'erreur s'affiche lors d'une tentative de SUPPRESSION d'un fichier ou d'un dossier à partir de la partition de données sécurisée alors que vous êtes connecté en mode lecture seule. |  <br>**Figure 9.13 – « Erreur lors de la suppression du fichier ou du dossier »** |

**Remarque :** Lorsque vous êtes en train d'utiliser la clé USB en mode lecture seule et que vous souhaitez la déverrouiller pour bénéficier d'un accès complet en écriture et en lecture à la partition sécurisée, vous devez fermer la VP50, puis rétablir la connexion après avoir décoché la case « Mode lecture seule » (Read-Only mode).

# IRONKEY™ Vault Privacy 50 (VP50)
# DRIVE FLASH USB 3.2 Gen 1 CRITTOGRAFATO

*Guida per l'utente*

## Contenuti


Figura 1: IronKey VP50

## Introduzione

Il drive Kingston IronKey Vault Privacy 50 (VP50) è un drive USB di classe premium che garantisce funzionalità di sicurezza di classe aziendale con certificazione FIPS 197 e funzionalità di crittografia hardware AES 256-bit in modalità XTS. L'unità include numerose funzionalità contro BadUSB e firmware firmato digitalmente contro i tentativi di violazione password di tipo brute force. L'unità VP50 è anche conforme agli standard TAA ed è assemblata negli Stati Uniti. Dato che garantisce storage crittografato controllato fisicamente dall'utente, la gamma VP50 assicura funzionalità di salvaguardia dei dati superiori a quelle dei servizi Internet e cloud.

La gamma VP50 supporta  opzionimulti password (amministratore, utente, password di ripristino monouso) con frasi password complesse. L'opzione multi password massimizza la capacità di recupero dei dati in caso di smarrimento della password. Oltre al supporto delle tradizionali password complesse, la nuova modalità basata su frasi password consente di impostare un pin numerico, frasi, elenchi di parole o anche testi di brani di lunghezza compresa tra 10 e 64 caratteri. L'amministratore può abilitare un utente e una password di ripristino monouso, oppure resettare la password utente per ripristinare l'accesso ai dati.

Al fine di facilitare l'inserimento della password, l'icona raffigurante un "occhio"  consente di abilitare la modalità di visualizzazione password mentre viene inserita, così riducendo il rischio di digitare password incorrette e quindi prevenire errori di inserimento password durante l'accesso. La protezione contro attacchi brute-force impedisce l'accesso all'unità oppure consente l'uso di una password di ripristino monouso quando si superano i 10 tentativi consecutivi di inserimento password non validi. Inoltre, la funzione crittografica effettua la cancellazione completa dei dati presenti sul drive quando rileva 10 tentativi successivi non corretti di inserimento della password amministratore.

Al fine di prevenire attacchi causati da malware o sistemi non affidabili, sia l'amministratore che l'utente possono impostare la modalità di sola lettura per impedire operazioni di scrittura su drive; inoltre, la tastiera virtuale integrata protegge le password dai tentativi di utilizzare keylogger o screenlogger.

Grazie alla certificazione FIPS 197 e alla conformità TAA, le organizzazioni possono personalizzare e configurare i drive dalla famiglia VP50 con una ID prodotto (PID), che consente l'integrazione con software di gestione degli endpoint standard, al fine di soddisfare i requisiti di sicurezza informatica EIT aziendali attraverso il Programma di personalizzazione Kingston.

Le aziende di piccole e medie dimensioni possono utilizzare la funzione di amministratore per gestire su base locale i drive. Ad esempio, è possibile utilizzare il ruolo dell'Aamministratore per configurare o resettare le password utente o le password di ripristino monouso, recuperare l'accesso ai dati sui drive bloccati e garantire la conformità a normative e regolamenti quando richiesto per attività forensi.

Il drive VP50 è supportato da una garanzia limitata di 5 anni, con servizio di supporto tecnico Kingston gratuito.

## Funzionalità IronKey Vault Privacy 50

- Certificazione FIPS 197 con crittografia hardware XTS-AES a 256-bit (con funzione crittografica non disattivabile)
- Protezione contro gli attacchi brute force BadUSB
- Opzioni multi password
- Utilizzo 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 screen logger
- Doppia impostazione di sola lettura (protezione contro scrittura) per la protezione dei contenuti dei drive contro modifiche o malware
- Le aziende di dimensioni medie e piccole possono gestire i loro drive su base locale mediante il ruolo Amministratore
- Compatibile con sistemi operativi Windows e macOS (consultare la scheda tecnica per ulteriori dettagli)

## Informazioni sulla guida

Questo manuale d'uso contiene le istruzioni per l'uso di IronKey Vault Privacy 50 (VP50). Le istruzioni sono riferite all'unità in configurazione standard di fabbrica e pertanto priva di qualunque tipo di personalizzazione.

## Requisiti di sistema

| | |
|---|---|
| **Piattaforma PC**<br>• Intel, AMD & Apple M1 SOC<br>• 15MB di spazio libero su disco<br>• Porta USB 2.0 - 3.2 disponibile<br>• Due lettere di unità libere consecutive dopo quella associata all'ultimo drive fisico presente sull'unità*<br><br>***Nota:** Vedere sezione "Conflitti con le lettere di unità", a pagina 32. | **Supporto per sistemi operativi per PC**<br>• Windows 11<br>• Windows 10<br>• Windows 8.1 |
| **Piattaforma Mac**<br>• 15MB di spazio libero su disco<br>• Porta USB 2.0 - 3.2 | **Supporto per sistemi operativi per Mac**<br>• macOS X (v. 10.13.x – 12.x.x) |

## Raccomandazioni

Per garantire una'alimentazioneadeguata al funzionamento del drive VP50, collegarlo direttamente a una porta USB sul computer notebook o desktop, come illustrato in ***Figura 1.1***. Evitare di collegare il drive VP50 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 VP50 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 utilizzare il drive VP50 su un sistema target
- Quando si utilizza il drive su un sistema di tipo pubblico o non conosciuto, potrebbe essere necessario impostare la modalità di sola lettura sul dispositivo al fine di proteggere il drive contro eventuali attacchi malware
- Bloccare il dispositivo quando non 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 VP50 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 a 10 i tentativi di inserimento password. Una volta raggiunto il limite di tentativi di inserimento password sul drive, l'unità VP50 effettuerà la cancellazione automatica di tutti i dati crittografati per poi effettuare il ripristino dello stato in cui era quando è uscito dalla fabbrica.

**Supporto per password multiple**
Il drive VP50 supporta le opzioni 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 VP50 è in grado di supportare fino a tre password differenti che possono essere utilizzate per recuperare i dati: password Amministratore (Admin), password Utente (User) e password di ripristino monouso (One-Time Recovery).

L'unità VP50 consente l'impostazione di due password principali: una password Amministratore ( "Admin Password") e una password Utente ("User Password"). L'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. Inoltre, l'Amministratore può impostare una password di ripristino monouso (One-Time Recovery) per l'utente, al fine di garantire a quest'ultimo la possibilità di accedere ed reimpostare la propria password.

L'Utente (User) può accedere al drive al pari dell' Amministratore, ma, al contrario di quest'ultimo, 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. L'Utente può utilizzare la password di ripristino monouso al fine di resettare la password utente quando necessario.

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 VP50 può essere sottoposto a un reset; ma in tal caso, tutti i dati in esso contenuti saranno eliminati definitivamente.

**Modalità password**
Il drive VP50 supporta inoltre due modalità password differenti:

**Password complessa (Complex)**
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

**Password frase (Passphrase)**
Il drive VP50 supporta come password anche una frase composta da 10 fino a 64 caratteri. Questo tipo di password non segue alcuna regola, ma se utilizzata correttamente può fornire password caratterizzate da un elevato livello di protezione.

Si tratta password composte da qualunque combinazione di caratteri inclusi caratteri provenienti da altre lingue. Come nel caso del drive VP50, 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 (ambientiWindows)

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 sottostante, la lettera dell'unità è (E:).

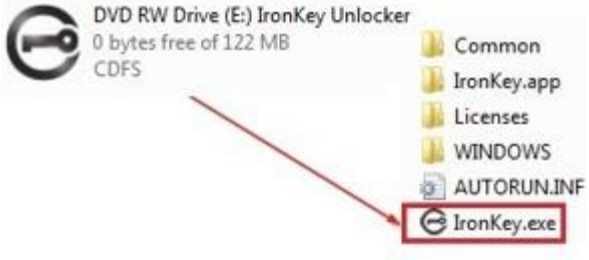



**Figura 3.2 - Esplora risorse Window/IronKey.exe**

### Accesso al dispositivo (ambienti macOS)

Inserire il drive VP50 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 IKVP50 (o IRONKEY). (Figura 3.3)

- Fare doppio clic sull'icona CD-ROM dell'unità IRONKEY.
- Quindi, fare doppio clic sull'icona IKVP50 (o IronKey.app), visualizzata nella finestra raffigurata in Figura 3.3. Verrà avviata la procedura di inizializzazione.

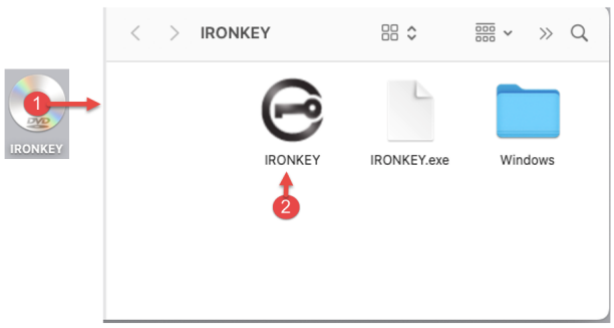
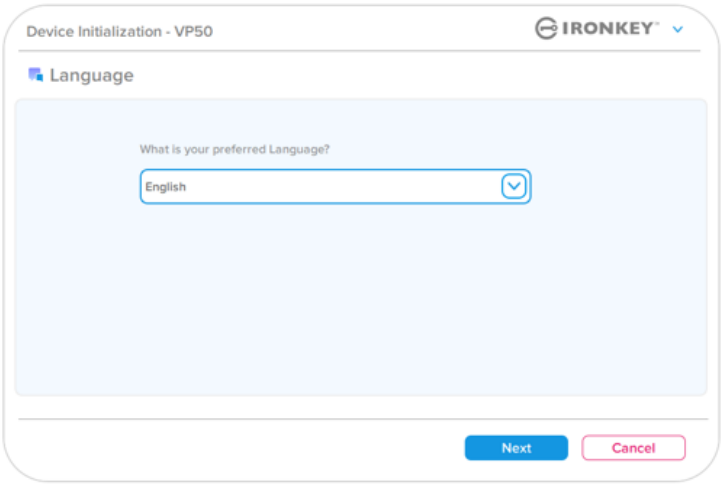
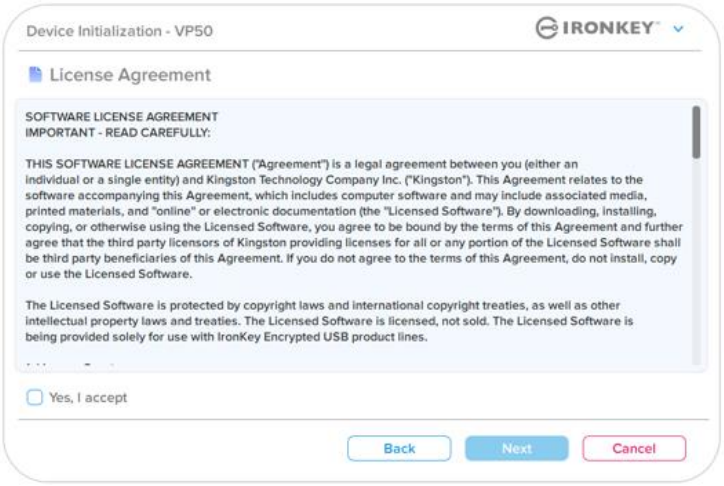



**Figure 3.3 - Icona di volume IKVP**

## Inizializzazione del dispositivo (ambienti Windows e macOS)

### Lingua e EULA

| | |
|---|---|
| Selezionare la lingua preferita dal menu a discesa e fare clic su "**Avanti**" (Next). (Vedere Figura 4.1) |  <br>**Figura 4.1- Selezione della lingua** |
| Leggere l'accordo di licenza e quindi fare clic su "**Avanti**" (Next).<br><br>Nota: è necessario accettare l'accordo di licenza prima di proseguire; in caso contrario il pulsante "**Avanti**" (Next) resterà disabilitato. (Figura 4.2) |  <br>**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 VP50. La password utilizzata può essere di tipo complesso oppure una password frase (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, 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” (Confirm Password). Affinché sia possibile proseguire la procedura di inizializzazione, è necessario creare una password avente i seguenti requisiti:

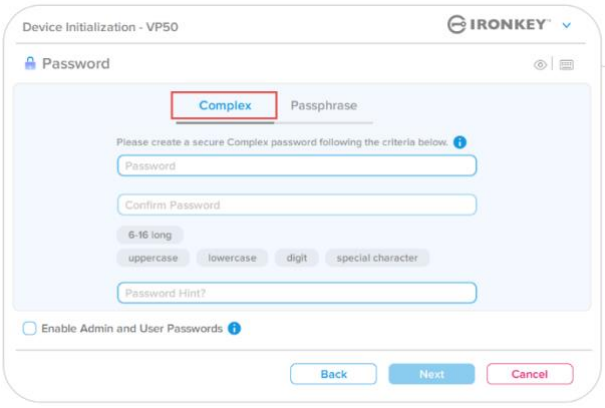
<table>
<tr>
<td>Password complessa<ul><li>Le password devono essere composte da un minimo di 6 fino a un massimo di 16 caratteri.</li><li>Le password devono includere tre (3) dei seguenti criteri:<ul><li>Lettere maiuscole</li><li>Lettere minuscole</li><li>Numeri</li><li>Caratteri speciali (!,$,&, ecc..)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

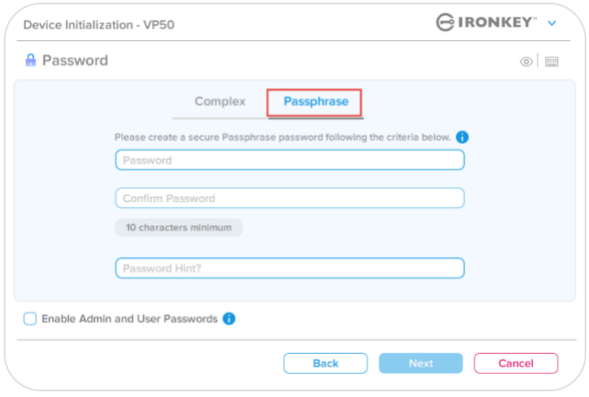
Figura 4.3 - Password complesse</td>
</tr>
<tr>
<td>Password frase<ul><li>Devono contenere:<ul><li>Minimo 10 caratteri</li><li>Massimo 64 caratteri</li></ul></li></ul></td>
<td> 

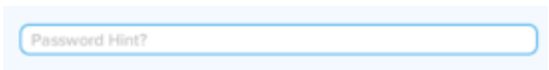
Figura 4.4 - Password frase</td>
</tr>
<tr>
<td>Suggerimento password (opzionale)<br>Un suggerimento password può rivelarsi utile per aiutare l'utente a ricordare la password, qualora questa vada persa o dimenticata.<br>Nota: il suggerimento NON DEVE corrispondere alla stessa password utilizzata per 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 non è più disponibile come opzione. (Figura 4.6b)

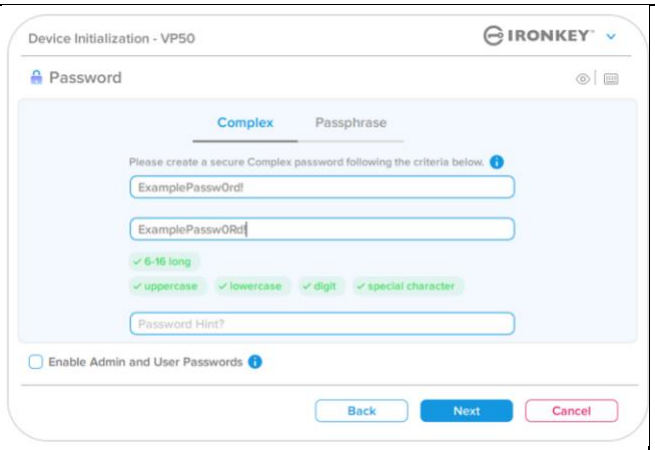



**Figura 4.6a - Requisiti di inserimento della password complessa rispettati**

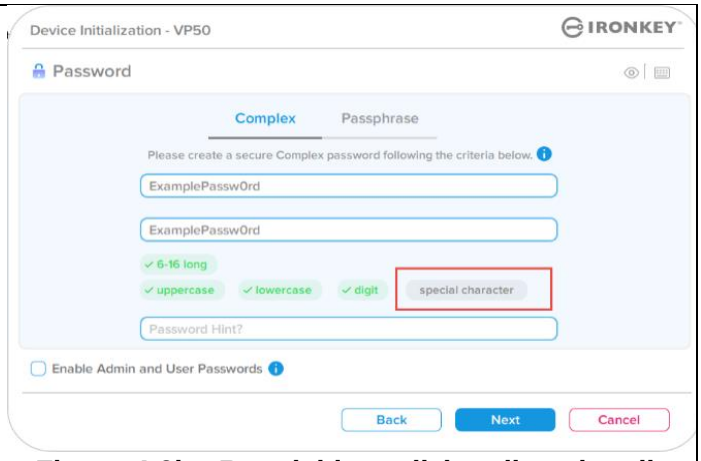



**Figura 4.6b - Requisiti condizionali opzionali della password complessa**

Nel caso di inserimento di password **Non valide**, i campi associati ai criteri delle password, si illumineranno di colore rosso e il pulsante "**Avanti**" (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.

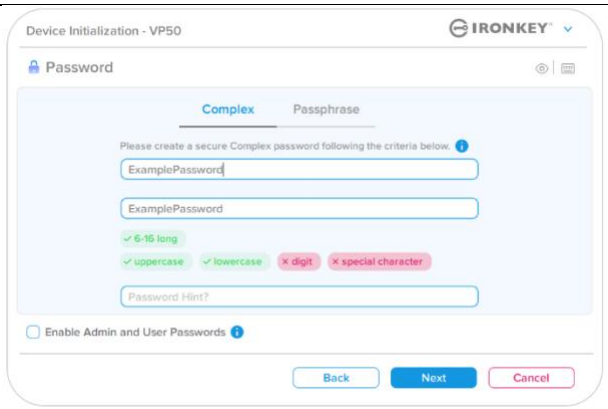



**Figura 4.7 - Condizioni di inserimento password non rispettate**

## Inizializzazione del dispositivo

### Tastiera virtuale

Il drive VP50 è dotato di 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.

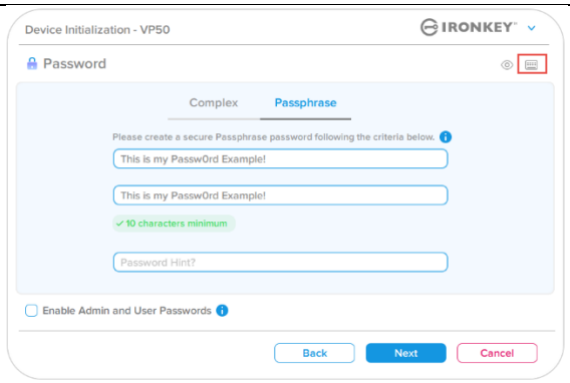



**Figura 4.8 - Attivazione della tastiera virtuale**

- Una volta che viene visualizzata la tastiera virtuale, è anche possibile attivare la funzione di **Protezione contro gli screenlogger**. 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.

- Al fine di massimizzare la sicurezza di questa funzionalità, è anche possibile selezionare la funzione di layout casuale dei tasti della tastiera virtuale, selezionando l'opzione "Layout casuale"(Randomize) sul lato inferiore destro della tastiera. Questa funzione dispone i tasti in ordine casuale.

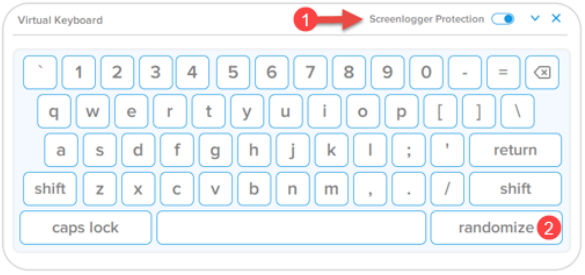


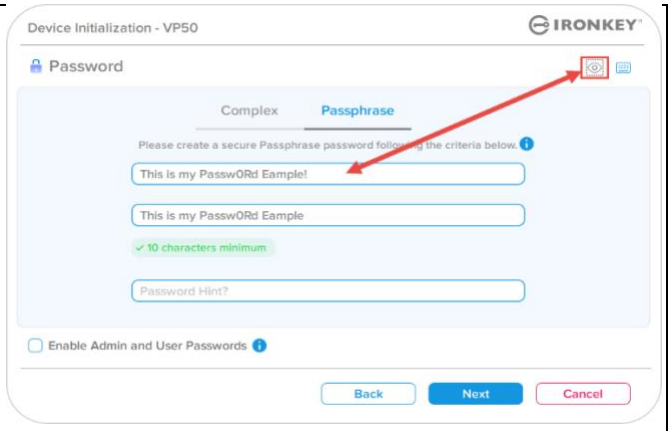
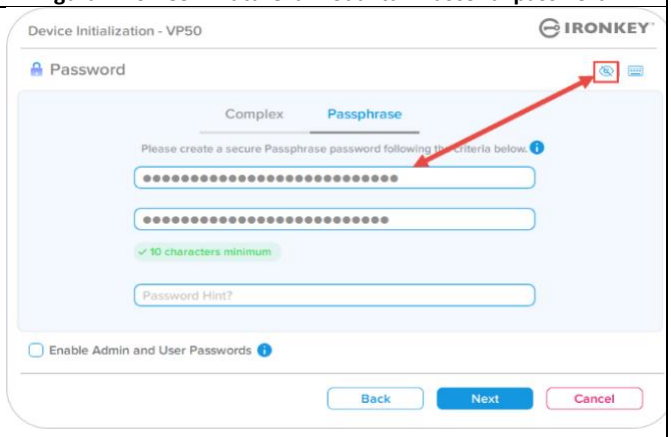

**Figura 4.9 - Protezione contro screenlogger / funzione di layout casuale tastiera**

## 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 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**" (Enable Admin and User passwords). 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**" (Admin and User passwords) è abilitata, è anche possibile accedere alle seguenti funzionalità:

- Password di ripristino monouso
- Funzione di sola lettura forzata per l'accesso Utente
- Reset della password utente
- Reset password forzato per l'accesso utente

Per ulteriori informazioni su queste funzionalità , consultare la pagina 25 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 "" (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.

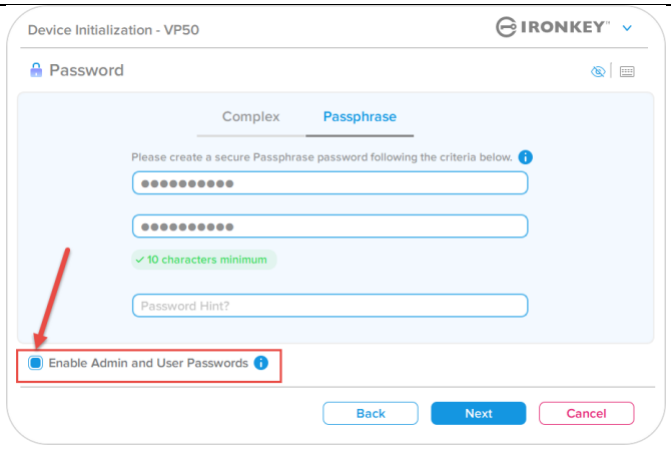



**Figura 4.12 - Abilitazione delle password amministratore e utente**

**Nota: l'abilitazione della funzionalità "Password amministratore e 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, password singola" tenere la funzione "**Abilita la password amministratore e la password utente**"( Enable Admin and User Passwords) deselezionata e fare clic su " **Successivo**" (Next ), dopo aver creato una password valida.

**Nota:** nella restante sezione di questo manuale, la funzione "**Password amministratore e password utente**" (Admin and User Passwords') sarà denominata "**Ruolo amministratore**".

## Inizializzazione del dispositivo

### Password amministratore e utente

- Se il ruolo amministratore è stato **abilitato** nella schermata precedente, la schermata successiva mostrerà la **Password utente** (Figura 4.13). La password Utente offre funzionalità limitate rispetto a quella Amministratore. Tali funzionalità saranno discusse in dettaglio nelle sezioni successive di questa guida utente. (vedere pagina 23)

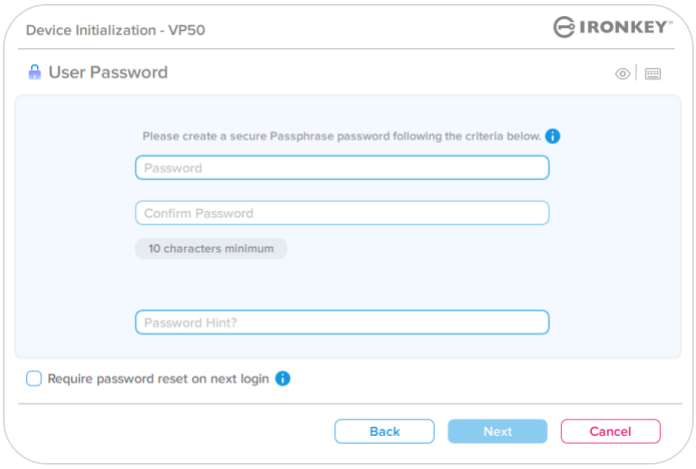



**Figura 4.13 - Password Utente (Funzione "Amministratore e utente" abilitata)**

**Nota:** Il tipo di password selezionato (complessa o frase) sarà trasferito anche alla password utente, alla password di ripristino monouso e a qualunque attività di reset password richiesta per la configurazione del drive. La scelta relativa al tipo di password può essere modificata solamente dopo aver effettuato un reset completo del dispositivo.

- La funzionalità "**Richiedi il reset password al prossimo accesso**", posta sul lato inferiore sinistro in **Figure 4.13**, è limitata alla sola password Utente e può essere abilitata al fine di forzare l'utente a effettuare l'accesso con una password temporanea impostata dall'amministratore durante la fase di inizializzazione. Tale password dovrà poi essere modificata con una password selezionata dall'utente, una volta che il drive è stato autenticato con la password temporanea. Tale procedura è utile quando il drive viene assegnato ad un altro utente. (**Figura 4.14**)

  **Nota:** per maggiore sicurezza, la nuova password non può essere identica alla password temporanea.

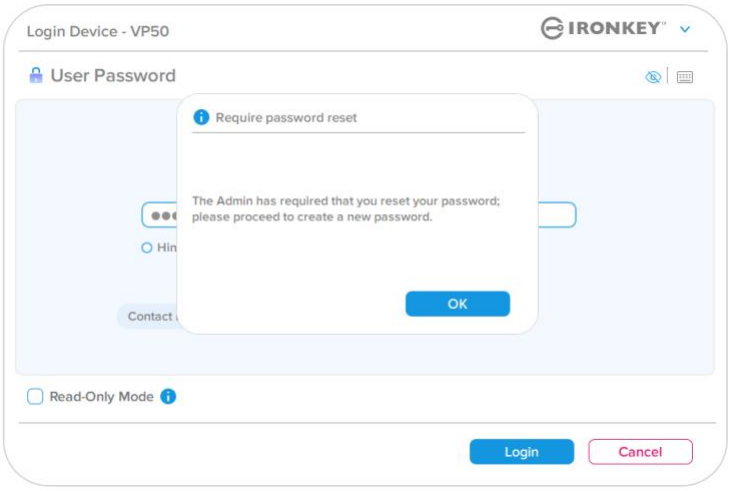


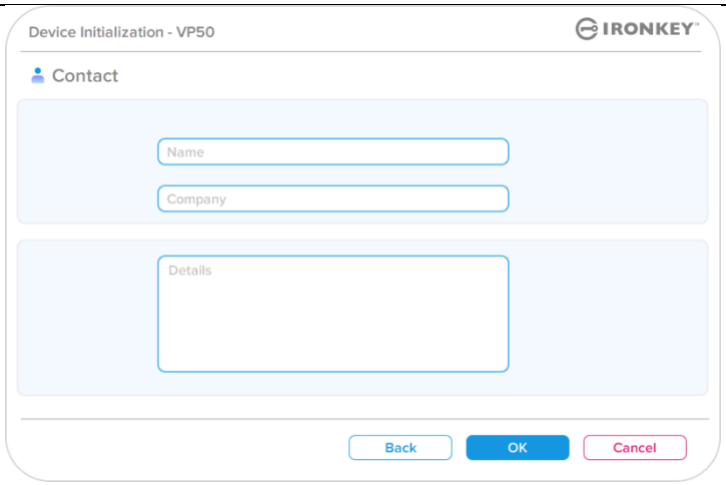

**Figura 4.14 - Richiedi il reset password al prossimo accesso (per password utente)**

## 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**.<br><br>Il campo " **Azienda**" (Company ) può contenere fino a 32 caratteri, ma non può contenere la password esatta.<br><br>Il campo " **Dettagli** " (Details) può contenere fino a 156 caratteri, ma non può contenere la password esatta. |  <br>**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 su 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.

## 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 (Ruolo amministratore), sarà eseguita l'applicazione integrata nel drive IronKey VP50, 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 5.1). Facendo clic sul pulsante "'Accedi come amministratore " (Login as Admin), qui di seguito illustrato, 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 5.2)

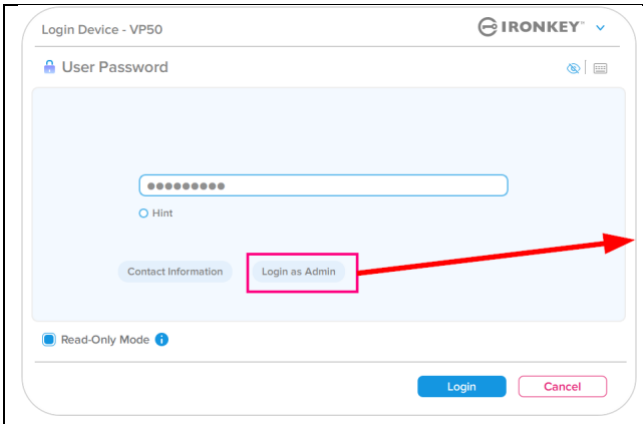



**Figura 5.1 - Accesso con Password Utente (Amministratore abilitato)**

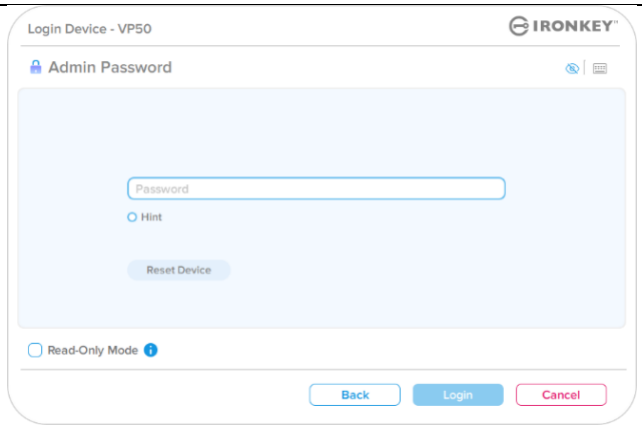



**Figura 5.2 - Accesso con Password Amministratore**

### Modalità di accesso per solo utente (Amministratore non abilitato)

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 coloro che desiderano un approccio più semplice verso le password singole come strumento per mettere in sicurezza i dati del drive. (Figura 5.3)

**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 password Amministratore e Utente. **Quando viene effettuato un reset del dispositivo,**

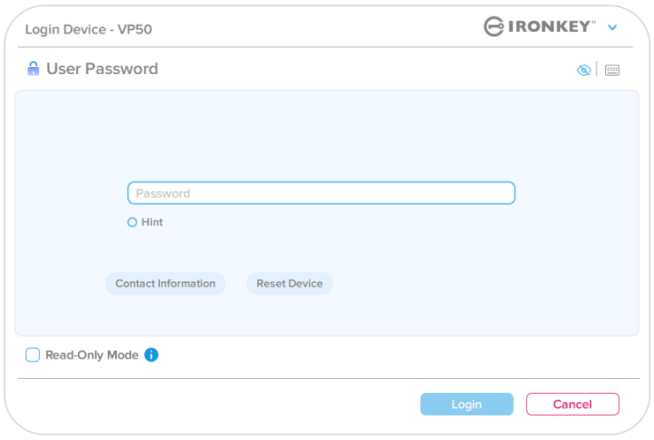



**Figura 5.3 - Accesso con Password Utente (Amministratore non abilitato)**

| | |
|---|---|
| **tutti i dati contenuti sul drive saranno formattati e andranno persi per sempre.** | |

## Utilizzo del dispositivo

### Sblocco in modalità di sola lettura

È possibile sbloccare il drive in modalità di sola lettura, in modo tale che i file che risiedono sul drive IronKey non vengano alterati. Ad esempio, quando si utilizza un computer ritenuto non sicuro o un computer non noto, sbloccare il dispositivo solo in modalità di sola lettura evita infezioni da parte di malware che possono passare dal computer al dispositivo, oppure potrebbero modificare i file in esso contenuti.

Quando si opera in tale modalità, non è possibile effettuare alcuna operazione che implichi la modifica dei file sul dispositivo.
Ad esempio, non è possibile riformattare il dispositivo, ripristinare, aggiungere o modificare i file presenti nel drive.

Per sbloccare il dispositivo in modalità di sola lettura:

1. Inserire il dispositivo nella porta USB del computer host ed eseguire l'applicazione **IronKey.exe**.
2. Selezionare la modalità "**Sola lettura**" (Read-Only) sotto il campo di inserimento della password. (**Figura 5.4**)
3. Immettere la password del dispositivo e fare clic su "" (Login) . Il drive IronKey è ora sbloccato e in modalità di sola lettura.

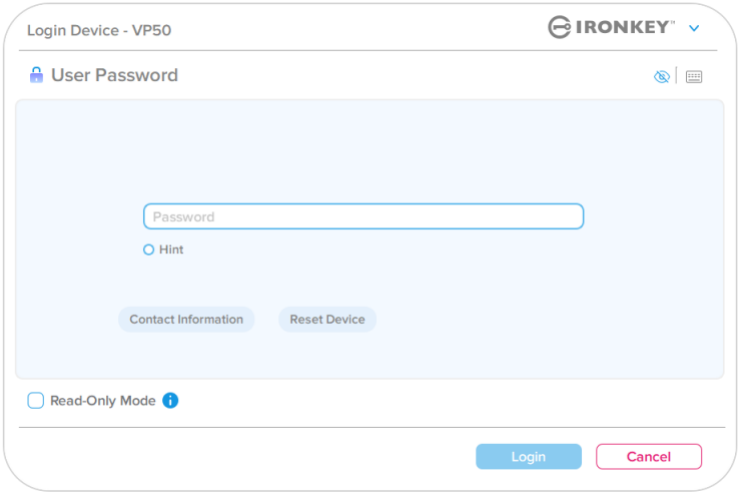



**Figura 5.4 - Modalità di sola lettura**

Se si desidera sbloccare l'unità ottenendo i diritti di accesso completi in lettura/scrittura alla partizione dati sicura, è necessario scollegare e disattivare il drive VP50, per poi effettuare nuovamente l'accesso, assicurandosi di deselezionare la casella dell'opzione "Modalità di sola lettura " (Read-Only Mode).

**Nota:** le opzioni di amministrazione del drive VP50 includono una modalità di sola lettura forzata per i dati dell'utente. Ciò significa che l'amministratore può forzare l'accesso dell'utente in modalità di sblocco in sola lettura (vedere **pagina 28** per ulteriori dettagli).

## 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 falliti, 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 o con password di ripristino monouso per effettuare il reset della Password Utente | NO |
| Password amministratore | Eliminazione della partizione crittografica del drive, delle password, delle impostazioni ed eliminazione definitiva di tutti i dati | **SÌ** |
| Password di ripristino monouso | Blocco password, pulsante di ripristino password disabilitato e di colore grigio. Accesso come amministratore per effettuare il reset password | NO |
| **Versione solo utente Utente singolo, password singola (Funzione 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 ed 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.**

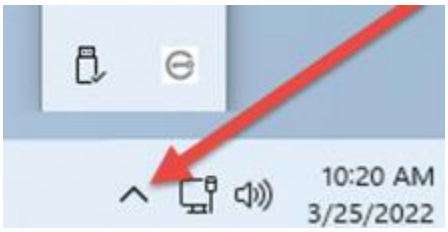
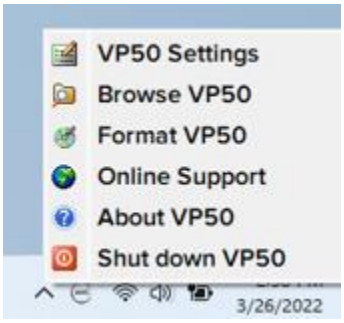
### Accesso ai file sicuri

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

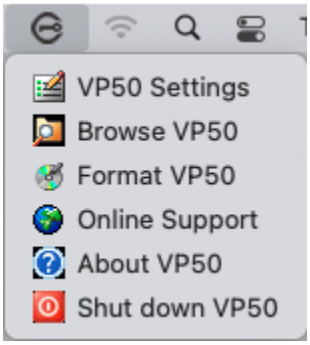
trasparenza, consentendo di utilizzare i dati come se questi fossero memorizzati su un drive normale, offrendo al contempo solide funzionalità di sicurezza "always-on".
**Suggerimento**: è anche possibile accedere ai file facendo clic col tasto destro del mouse sull'**icona IronKey**, sulla barra applicazioni di Windows, per poi selezionare"**Esplora VP50**" (Browse VP50). (Figura 6.2)

## Opzioni del dispositivo - (ambiente Windows)

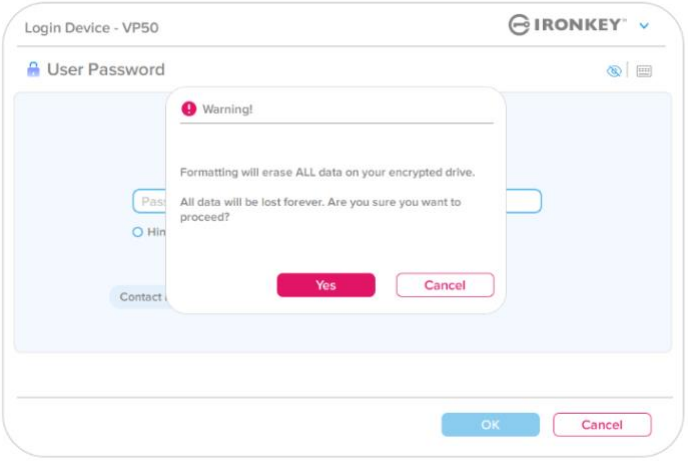
Durante l'accesso al dispositivo, sull'angolo destro della barra applicazioni di Windows verrà visualizzata l'icona del drive di IronKey. Facendo clic con il tasto destro del mouse sull'icona IronKey, sarà possibile aprire il menu di selezione che include le opzioni del drive. (Figura 6.2)
Ulteriori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

| | |
|---|---|
| • Durante l'accesso al dispositivo, sull'angolo destro della barra applicazioni di Windows sarà visualizzata l'icona del drive di IronKey. **(Figura 6.1)** |  **Figura 6.1 – Icona del drive IronKey sulla barra applicazioni** |
| • Facendo clic con il tasto destro del mouse sull'icona IronKey, sarà possibile aprire il menu di selezione che include le opzioni del drive. **(Figura 6.2)**<br><br>Ulteriori dettagli su questi dispositivi possono essere reperiti alle pagine 19-23 di questo manuale. |  **Figura 6.2 - Fare clic con il pulsante destro del mouse sull'icona IronKey per visualizzare le opzioni del dispositivo** |

## Opzioni del dispositivo - (ambiente MacOS)

| | |
|---|---|
| • Quando si è connessi al dispositivo viene visualizzata un'icona IronKey VP50 posizionata sul menu macOS mostrato in **Figura 6.3.** Tale menu consente di accedere alle opzioni del dispositivo.<br><br>Ulteriori dettagli su questi dispositivi possono essere reperiti alle pagine 19-23 di questo manuale. |  <br>**Figura 6.3 - Barra dei menu con icona/menu opzioni dispositivo macOS** |

## Opzioni dispositivo

| | |
|---|---|
| **Impostazioni VP50:** | • modifica password di accesso, informazioni di contatto, altre impostazioni. (Ulteriori dettagli sulle impostazioni del dispositivo possono essere reperiti nella sezione "Impostazioni 'VP50" di questo manuale). |
| **Esplora VP50 (Browse VP50):** | • consente di visualizzare i file sicuri. |
| **Formatta VP50 (Format VP50):** consente di formattare la partizione dati sicura. (Attenzione: tutti i dati saranno eliminati) (**Figura 6.1**)<br><br>**Nota:** la formattazione richiede l'autenticazione mediante password. |  <br>**Figura 6.1 – Formattazione del drive VP50** |
| **Supporto online (Online Support):** | • Questa opzione consente di accedere al link http://www.kingston.com/support, dal quale è |

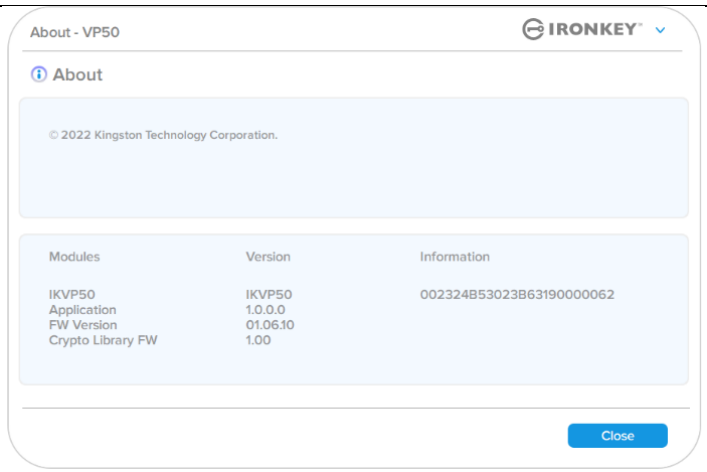
<table>
<tr><td></td><td>possibile accedere a una serie di informazioni di supporto aggiuntive.</td></tr>
<tr><td>Informazioni sul drive VP50 (About VP50): la sezione contiene dettagli specifici sull'unità VP50, incluse le applicazioni, il firmware e informazioni sul numero di serie. (Figura 6.2)<br><br>Nota: il numero di serie univoco del drive può essere visualizzato nella colonna “Informazioni”.</td><td> 

Figura 6.2 – Informazioni sul drive VP50</td></tr>
<tr><td>Arresta VP50 (Shut down VP50):</td><td>• questa funzione permette di arrestare correttamente l'unità VP50, consentendo all'utente di scollegare il drive dal computer in tutta sicurezza.</td></tr>
</table>

# Impostazioni del drive VP50

## Impostazioni amministratore

La schermata di accesso dell'amministratore consente di accedere alle impostazioni seguenti:

- **Password:** consente di modificare la password e/o il suggerimento dell'Amministratore (*Figura 7.1*)
- **Dati di contatto (Contact Info):** consente di aggiungere/visualizzare/modificare le informazioni di contatto dell'utente (*Figura 7.2*)
- **Lingua (Language):** Consente di modificare le impostazioni della lingua corrente (*Figura 7.3*)
- **Opzioni amministratore (Admin Options):** Consente di abilitare funzionalità aggiuntive come: (Figura 7.4)
    - Modifica della password Utente corrente (Change the User Password)
    - Reset della password di accesso (per Password Utente) (Login Password Reset (For User Password))
    - Abilita la funzione Password di ripristino monouso (Enable a One-Time Recovery Password)
    - Funzione di sola lettura forzata per i dati utente (Force Read-Only mode for User's data)

**NOTA:** per ulteriori dettagli sulle opzioni amministratore consultare le informazioni a pagina 24.

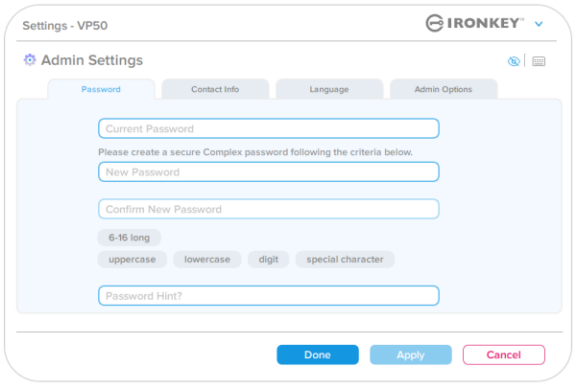



**Figura 7.1 – Opzioni password**

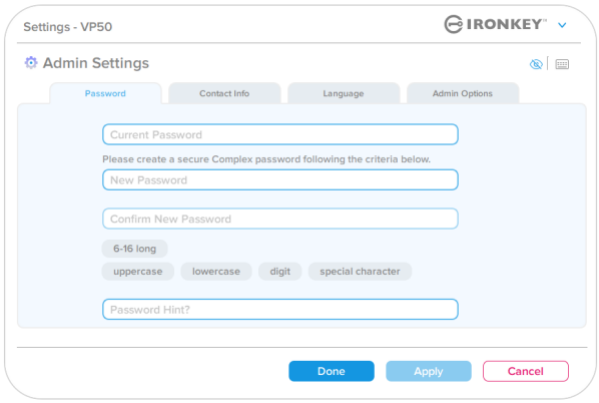



**Figura 7.2 - Dati di contatto**

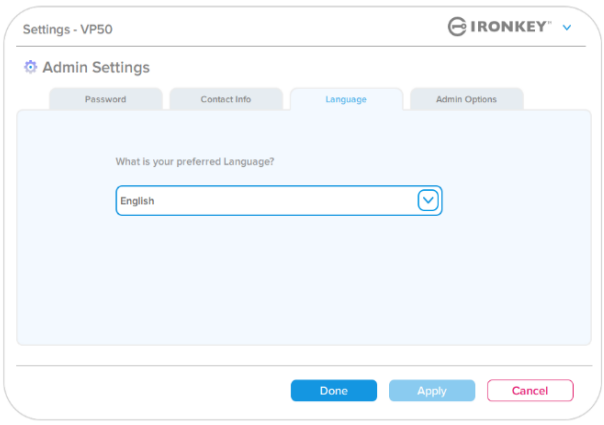



**Figura 7.3 – Opzioni lingua**

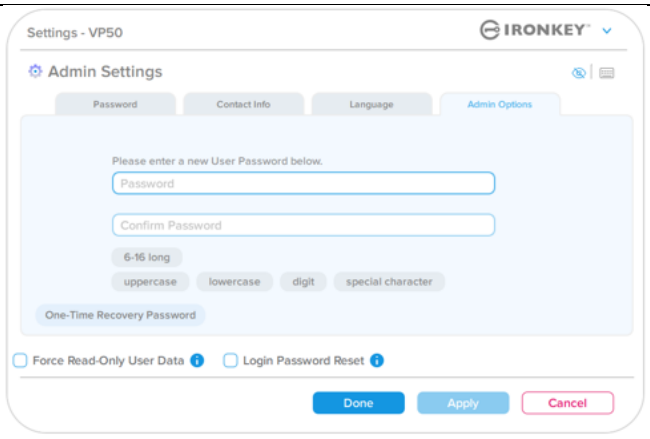
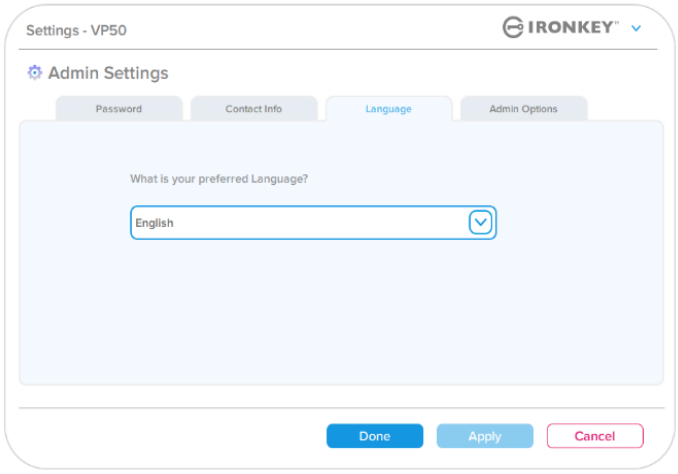
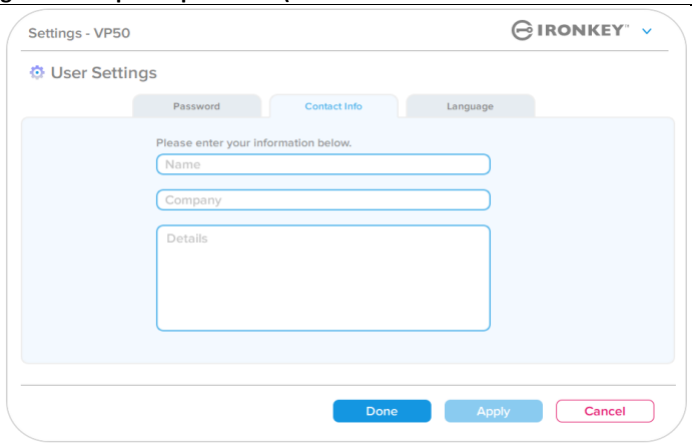
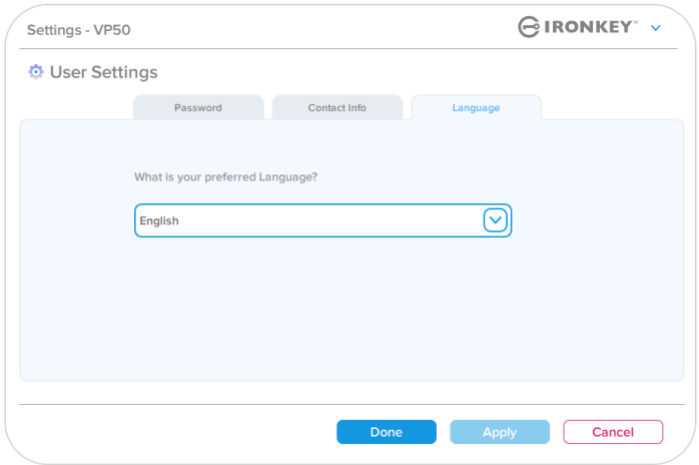



**Figura 7.4 – Opzioni amministratore**

## Impostazioni del drive VP50

### Impostazioni utente: Amministratore abilitato

L'Utente ha un accesso limitato alle sole impostazioni seguenti:

| | |
|---|---|
| **Password:**<br>consente di modificare la password Utente e/o il suggerimento. (**Figura 7.5**) |  <br>**Figura 7.5 - Opzioni password (Amministratore abilitato: Accesso utente)** |
| **Dati di contatto (Contact Info):**<br>consente di aggiungere/visualizzare/modificare i dati di contatto. (**Figura 7.6**) |  <br>**Figura 7.6 - Informazioni di contatto (Amministratore abilitato: Accesso utente)** |
| **Lingua (Language):**<br>consente di modificare le impostazioni della lingua corrente. (**Figura 7.7**) |  <br>**Figura 7.7 - Impostazioni lingua (Amministratore abilitato: Accesso utente)** |

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

## Impostazioni del drive VP50

### Impostazioni utente: Amministratore non abilitato

Come precedentemente specificato a pagina 12, l'avvio del drive VP50 senza avere abilitato le password Amministratore e Utente, farà sì che l'unità sia configurata in modalità **Password singola, Utente singolo**. Questa modalità di configurazione non permette di accedere ad alcuna opzione o funzionalità di amministrazione. Questa configurazione prevede l'accesso alle seguenti impostazioni del drive VP50:

### Modifica e salvataggio delle impostazioni

- Ogni qualvolta si effettuano dei cambiamenti alle impostazioni dell'unità VP50 (come, ad 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 7.11)

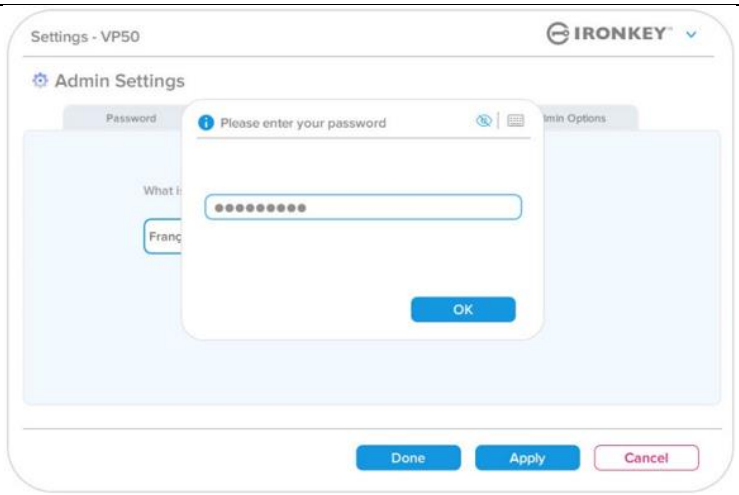



**Figura 7.11 - Schermata password che richiede il salvataggio delle impostazioni per l'unità VP50**

**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". L'operazione consente di chiudere la finestra di inserimento password e tornare al menu delle impostazioni dell'unità VP50.

## Funzionalità amministratore

**Opzioni disponibili per effettuare un reset della password Utente**
Le impostazioni di configurazione dell'account Amministratore offrono svariati metodi per eseguire un reset sicuro della password Utente, in caso questa venga dimenticata, oppure quando viene creata una password Utente temporanea e si desidera modificarla in occasione dell'accesso successivo dell'utente. La sezione seguente illustra tutte le funzionalità che possono essere utili durante la procedura di reset della password utente:

**Reset della password utente:**
Dal menu "Opzioni amministratore" (Admin Options), modificare manualmente la password utente. La modifica effettuata avrà effetto istantaneo, in occasione del prossimo accesso dell'utente. **(Figura 8.1)**

**Nota:** i criteri che regolano la creazione di una password sono basati sullescelte operate durante la fase di inizializzazione (password complessa o frase).

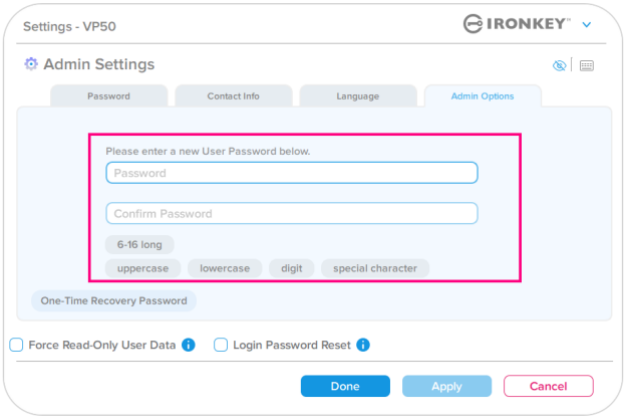



**Figura 8.1 - Opzioni amministratore/Reset della password utente**

**Reset password di accesso (Login Password Reset):**
l'abilitazione della funzione di reset della password di accesso **costringe l'utente a effettuare l'accesso mediante la password temporanea impostata dall'Amministratore,** per poi cambiarla con una password di propria scelta. Tale procedura è utile quando il drive viene assegnato ad un altro utente. (**Vedere Figure 8.2A e 8.2B**)

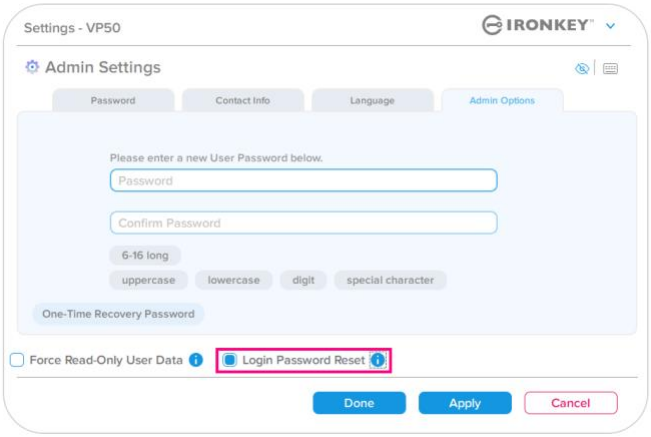



**Figura 8.2A - Pulsante Reset password di accesso (Login Password Reset):**

**Nota:** il reset effettivo della password sarà effettuato in occasione del successivo accesso dell'utente. I criteri di inserimento password saranno applicati automaticamente in base alle scelte operate durante il processo di inizializzazione (password complesse o frasi).

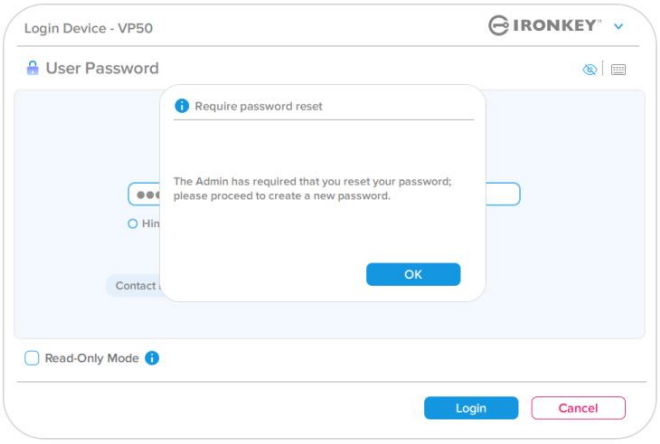



**Figura 8.2B - Notifica di reset dopo l'inserimento della password utente**

## Funzionalità amministratore

### Password di ripristino monouso (One-Time Recovery Password)

Questa sezione illustra la procedura necessaria per abilitare e utilizzare la funzionalità Password di ripristino monouso.

#### Password di ripristino monouso

**Fase 1:** La funzione di inserimento password di ripristino monouso consiste in una utile password monouso che può essere abilitata per aiutare gli utenti a recuperare e resettare la password utente quando questa viene persa o dimenticata. Fare clic sul pulsante “Password di ripristino monouso ” (One-Time Recovery Password), nel menu delle opzioni dell’ amministratore per avviare la procedura. **(Figura 8.4)**

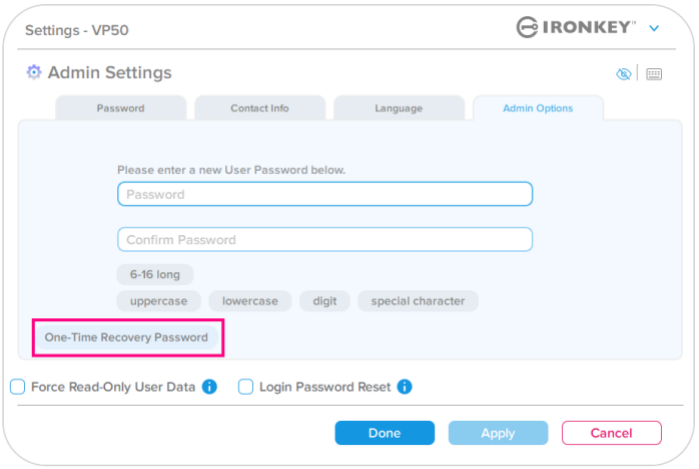



**Figura 8.4 - Pulsante “Password di ripristino monouso ” (One-Time Recovery Password),**

**Fase 2:** Creare una password di ripristino monouso utilizzando i medesimi criteri di impostazione password originariamente configurati per il dispositivo (password complesse o frasi).

**Nota:** lapplicazione delle modifiche apportate richiede l'inserimento della password Amministratore.

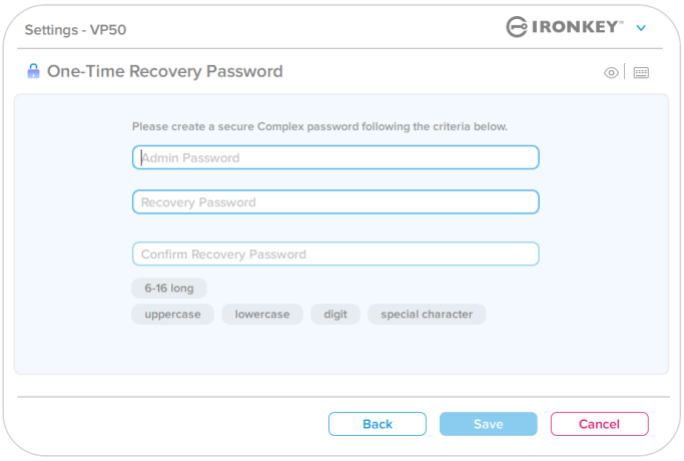
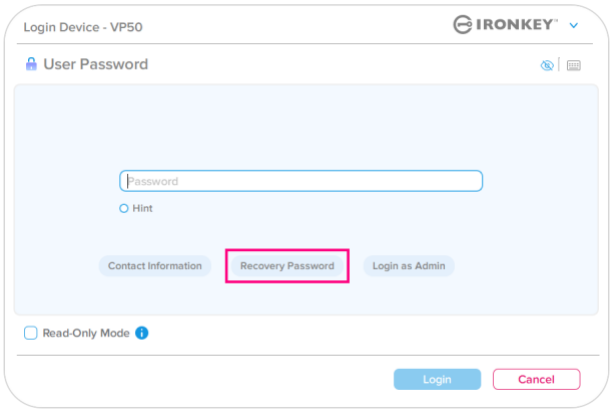
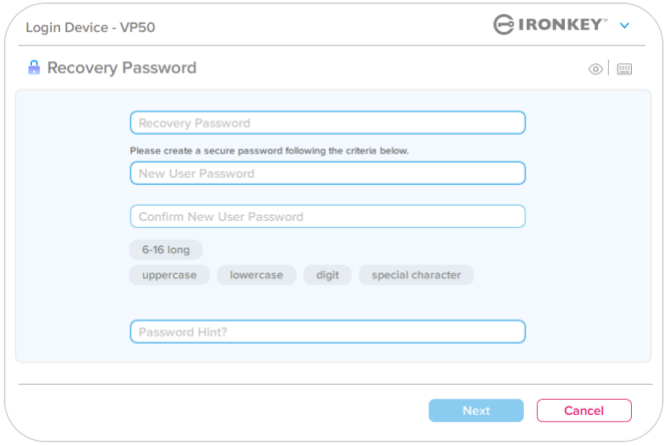
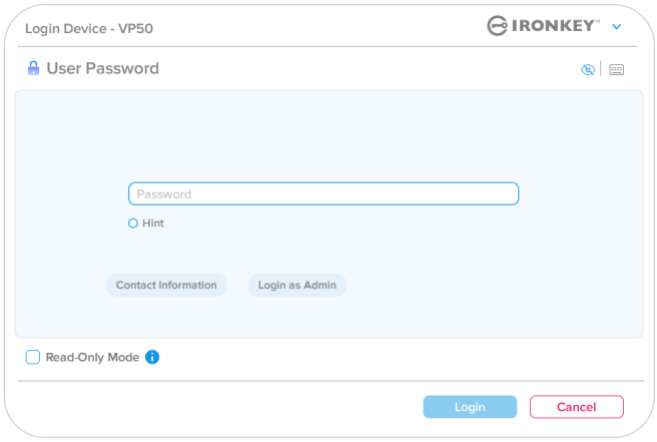



**Figura 8.5 - Configurazione della password di ripristino monouso**

## Funzionalità amministratore

Utilizzo della password di ripristino monouso

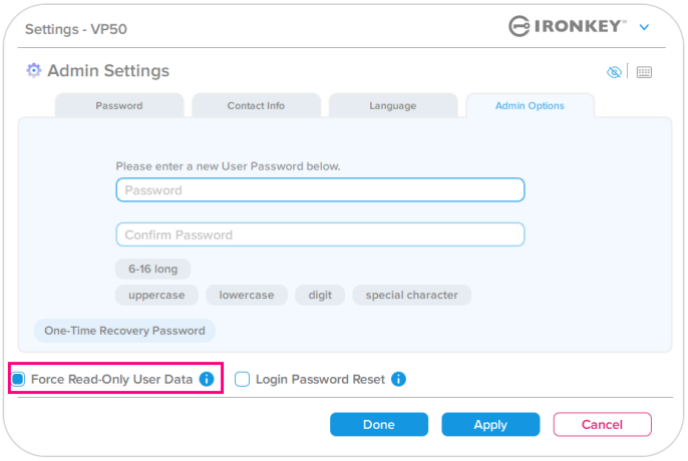
| | |
|---|---|
| **Fase 1:** Una volta creata la password di ripristino monouso, in occasione dell'accesso successivo, sarà visualizzato un nuovo pulsante nella schermata di accesso "**Password utente**" (User Password). Fare clic sul pulsante "**Recovery password**" (Password di ripristino)" per avviare la procedura. |  **Figura 8.6 - Pulsante Password di ripristino (Recovery password)** |
| **Fase 2:** Sarà visualizzata la schermata "**Password di ripristino**" (Recovery Password), nella quale è possibile inserire la password di ripristino e creare una nuova password utente. (Figura 8.7)<br><br>**Importante:** Anche la password ripristino monouso utilizza la funzionalità di sicurezza integrata che conteggia il numero di tentativi di accesso non riusciti. **Dopo 10 tentativi di accesso falliti, la funzione di inserimento password di ripristino monouso sarà disabilitata** e sarà necessario riabilitarla effettuando un nuovo accesso al drive come amministratore. (Vedere le pagine 18 e 30 per ulteriori dettagli) |  **Figura 8.7 - Menu per la password ripristino** |

| | |
|---|---|
| **Fase 3:** Una volta completata la procedura con successo sarà visualizzata nuovamente la schermata “**Password utente**” (User Password). Il pulsante “ **Password di ripristino** ” (Recovery password) scompare e la password utente inserita durante la **Fase 2** diventa la nuova password utente. (Figura 8.8) |  **Figura 8.8 - Schermata “Accesso password utente” (User Password Login), che mostra la scomparsa del pulsante password di ripristino dopo che tale funzionalità è stata utilizzata con successo.** |

## Funzionalità amministratore

### Forza sola lettura per i dati utente (Force Read-Only User Data)

La modalità “Forza sola lettura” (Forced Read-Only) può essere abilitata per impedire all’utente l’accesso in scrittura al drive. Questa funzionalità è particolarmente utile se i file presenti sul drive devono essere utilizzati in modalità di accesso in sola lettura.

| | |
|---|---|
| • Per abilitare la funzione “Forza sola lettura” (Forced Read-Only) per i dati dell'utente, fare clic sulla relativa casella e poi su su “‘Applica” (Apply). **(Figura 8.9)**<br><br>**Nota:** questa è applicabile esclusivamente all'account utente e non influenza in alcun modo l'account amministratore. L'account amministratore continuerà a mantenere privilegi di accesso in lettura e scrittura e potrà sempre abilitare la modalità di sola lettura quando necessario. |  **Figura 8.9 - Abilitazione della funzione Forza la modalità di sola lettura per i dati utente (l'applicazione delle modifiche apportate richiede l'inserimento della password Amministratore)** |
| • Una volta attivata la funzionalità, il pulsante “**Modalità sola lettura**” (Read-Only Mode) diventerà di colore blu, a indicare che la modalità è abilitata in | |

maniera permanente per la password utente, fino a quando tale funzione non verrà disabilitata dall'amministratore. (Figura 8.10)

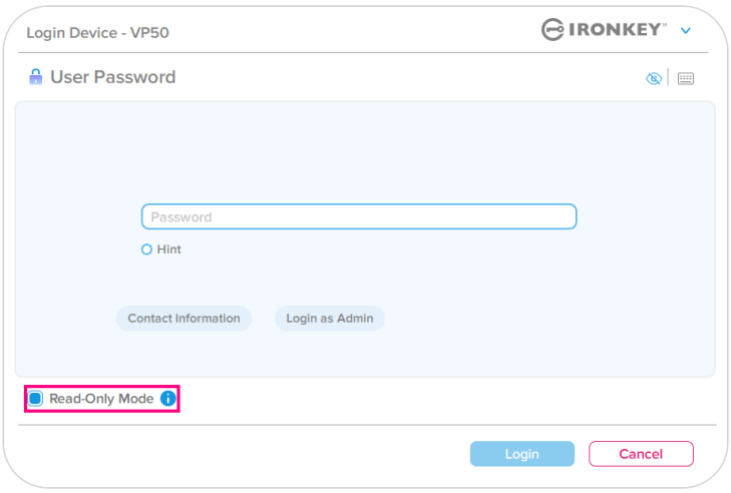



**Figura 8.10 - La modalità di sola lettura è abilitata forzatamente per l'account utente e può essere disabilitata esclusivamente dall'amministratore**

## Guida alla risoluzione dei problemi

### Blocco del dispositivo

Il drive VP50 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 sintetico *MaxNoA*). La configurazione "di fabbrica" predefinita include un valore pari a 10 (numero di tentativi) per ciascun metodo di accesso (Amministratore/Utente/Password di ripristino monouso).

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 9.1)

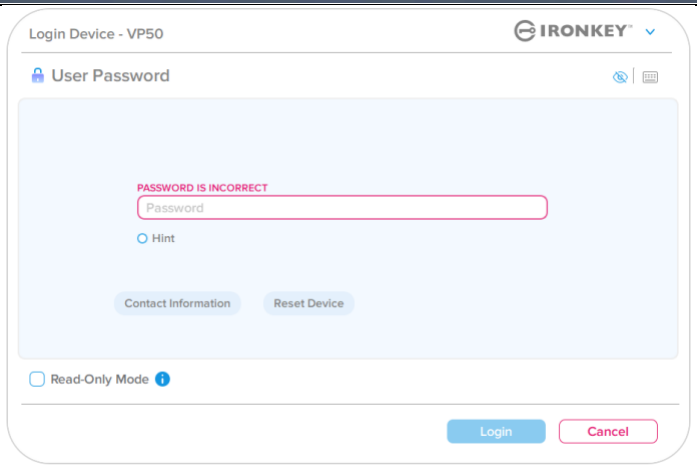



**Figura 9.1 - Messaggio di notifica inserimento password errata**

- Una volta raggiunto il **7°** tentativo fallito, verrà visualizzato un ulteriore messaggio di errore che informa l'utente che ha a disposizione solo altri 3 tentativi, prima di raggiungere il numero di tentativi specificati dal valore MaxNoA (impostato su 10 per default). (Figura 9.2)

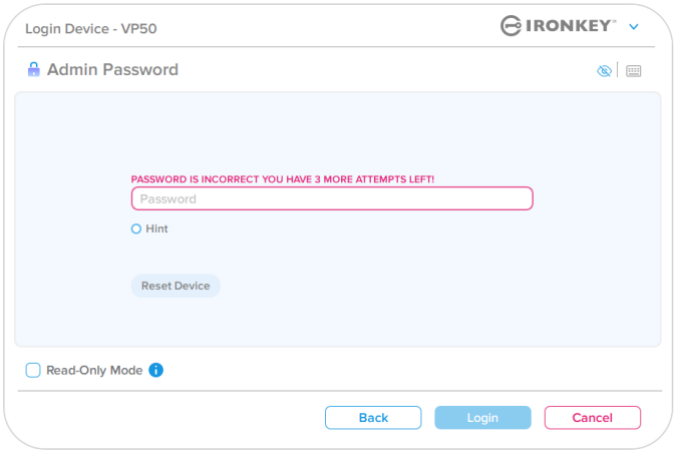


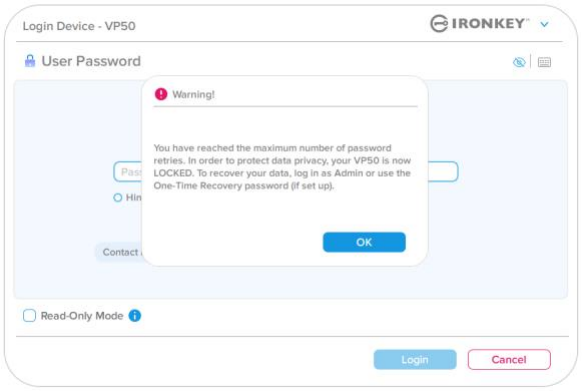
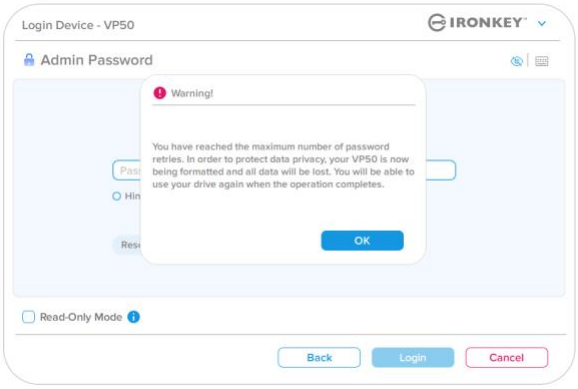
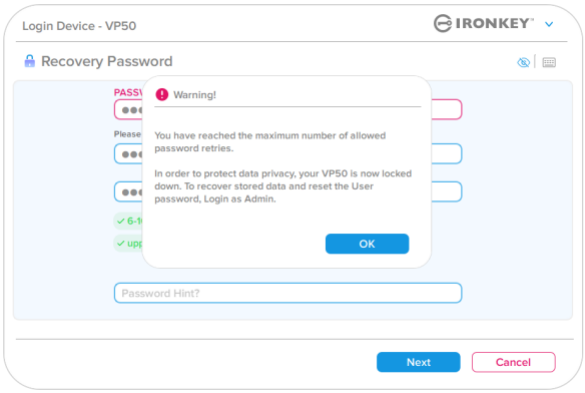
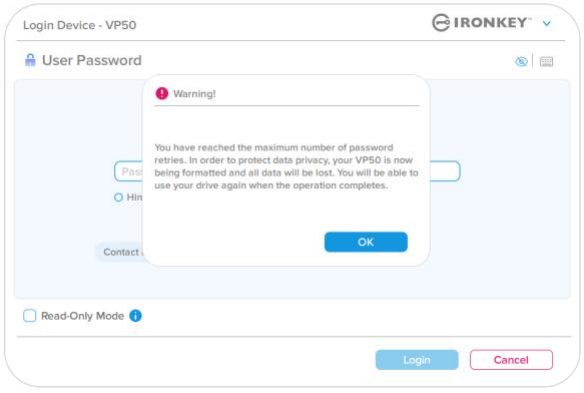

**Figura 9.2 - Notifica del 7° tentativo di inserimento password errato**

## 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 dei metodi utilizzati (Amministratore, Utente o Password di ripristino monouso), 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 9.3 - 9.6 sotto illustrano visivamente le schermate visualizzate dopo il 10° tentativo di accesso fallito con ciascun metodo di accesso:

<table>
<tr>
<td><u>Password utente: (Funzione Amministratore/Utente abilitata)</u><br> 
<br>BLOCCO DEL DISPOSITIVO<br><br>(Figura 9.3)</td>
<td>Password Amministratore (funzione Amministratore/Utente abilitata)<br> 
<br>FORMATTAZIONE DISPOSITIVO*<br><br>(Figura 9.4)</td>
</tr>
<tr>
<td><u>Password di ripristino monouso: (Funzione Amministratore/Utente abilitata)</u><br> 
<br>BLOCCO DEL DISPOSITIVO<br><br>(Figura 9.5)</td>
<td>Password Utente (funzione Admin NOT abilitata)<br> 
<br>FORMATTAZIONE DISPOSITIVO*<br><br>(Figura 9.6)</td>
</tr>
</table>

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 vostri dati sensibili (noti

anche come attacchi brute force). Per i possessori di drive VP50 che hanno dimenticato 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.

**Nota: la formattazione del dispositivo eliminerà tutti i dati archiviati sulla partizione dati sicura del drive VP50.*

## Guida alla risoluzione dei problemi

### Reset del dispositivo

Se si è dimenticata la password, oppure se è necessario effettuare un reset del drive è possibile fare clic sul pulsante "*Reset dispositivo*" (Reset Device). 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 Launcher dell'unità VP50. (Vedere ***Figure 9.7*** e ***9.8***)

- Questa opzione consente di creare una nuova password, ma per proteggere la privacy dell'unità VP50 il drive sarà formattato. Ciò significa che durante tale procedura tutti i dati andranno persi.*

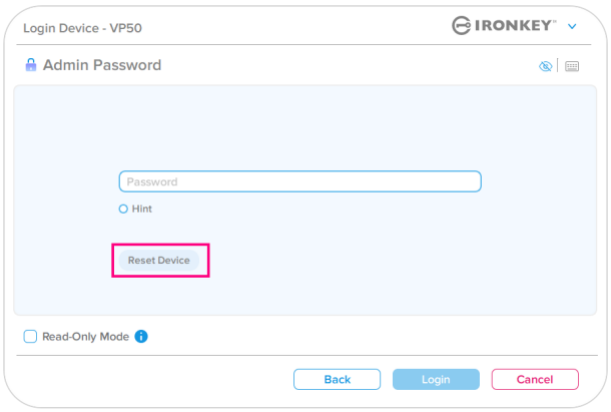



**Figura 9.7 - Accesso con password Amministratore: Pulsante di reset dispositivo**

- **Nota:** cliccando sul pulsante "*Reset* " (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) fare clic su "*OK*" per confermare, oppure 2) fare clic su "Annulla" (Cancel), per tornare alla schermata di accesso. (Vedere Figura 9.8)

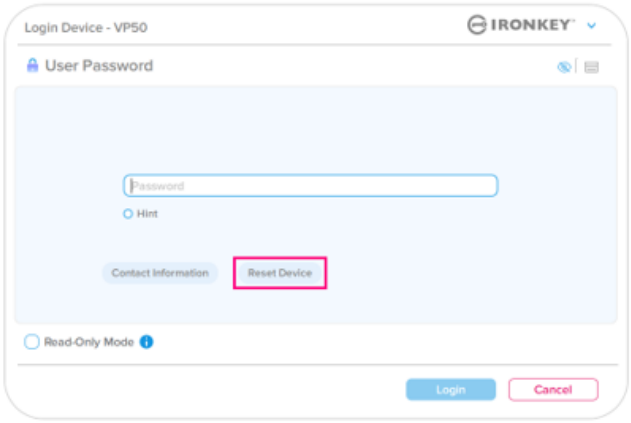



**Figura 9.8 - Password Utente (funzione Admin/Utente non abilitata) Reset dispositivo**

- 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). 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.

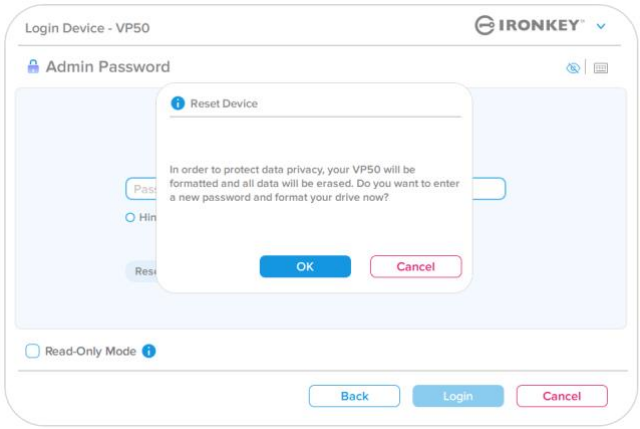



**Figura 9.9 - Conferma di reset dispositivo**

## 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 VP50 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 9.10*). 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 VP50 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). Come citato nella sezione "*Requisiti di sistema*" di questo manuale (a pagina 3), il drive VP50 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 9.10*). 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.

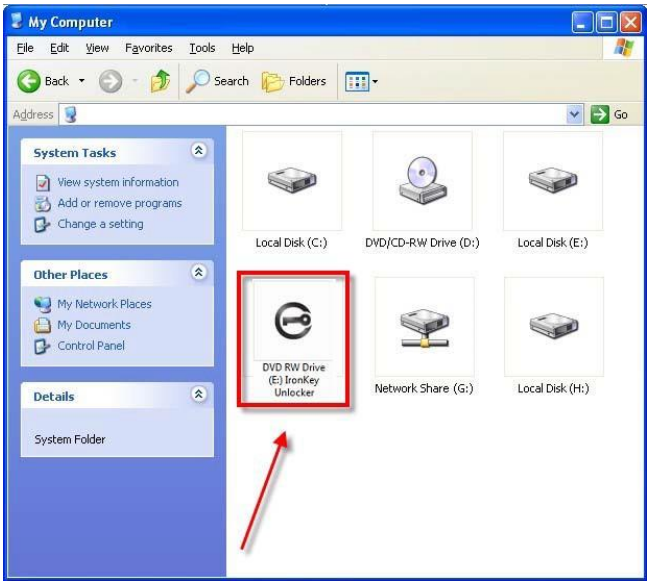



**Figura 9.10 - Esempio di lettera di unità**

In questo esempio (Figura 9.10), al drive VP50 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

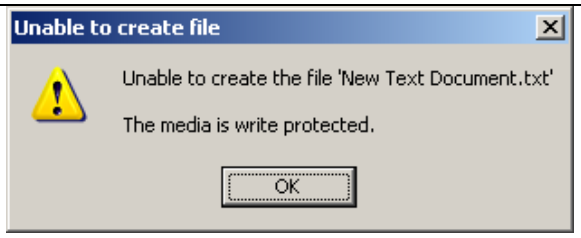
non fisiche). Dato che alla lettera “G:” è assegnata una condivisione di rete, che non appartiene al profilo hardware del computer in uso, l'unità VP50 tenterà di utilizzare tale lettera come seconda unità, generando un conflitto.

Se sul computer in uso non sono presenti condivisioni di rete, ma il drive VP50 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, causando ulteriori conflitti.

Si noti che le funzionalità di Gestione delle Lettere di Unità (DLM) sono migliorate significativamente su Windows 8.1, 10 e 11 e che, pertanto, tale problema non dovrebbe manifestarsi. Tuttavia, se l'utente non dovesse essere in grado di risolvere il conflitto, si raccomanda di contattare il Supporto Tecnico di Kingston o di visitare Kingston.com/support per richiedere ulteriore assistenza.

## Guida alla risoluzione dei problemi

### Messaggi di errore

| | |
|---|---|
| **Impossibile creare il file (Unable to create file):**<br>Questo messaggio di errore viene visualizzato quando si tenta di CREARE un file o una cartella NELLA partizione dati sicura, durante l'accesso in modalità di sola lettura. |  <br>**Figura 9.11- Finestra di notifica errore Impossibile creare il file (Unable to create file)** |
| **Impossibile copiare il file o la cartella (Error Copying File or Folder Error):**<br>Questo messaggio di errore viene visualizzato quando si tenta di COPIARE un file o una cartella NELLA partizione dati sicura, durante l'accesso in modalità di sola lettura. |  <br>**Figura 9.12- Finestra di notifica errore Impossibile copiare il file o la cartella (Error Copying File or Folder Error)** |
| **Impossibile eliminare il file o la cartella (Error Deleting File or Folder Error):**<br>Questo messaggio di errore viene visualizzato quando si tenta di ELIMINARE un file o una cartella NELLA partizione dati sicura, durante l'accesso in modalità di sola lettura. |  <br>**Figura 9.13 - Finestra di notifica errore "Impossibile eliminare il file o la cartella (Error Deleting File or Folder Error** |

**Nota:** se si sta effettuando l'accesso all'unità in modalità di sola lettura e si desidera sbloccare l'unità ottenendo i diritti di accesso completi in lettura/scrittura alla partizione dati sicura, è necessario scollegare e disattivare l'unità VP50 per poi effettuare nuovamente l'accesso, assicurandosi di deselezionare la casella dell'opzione " Modalità di sola lettura " (Read-Only Mode), prima di effettuare l'accesso.

# IRONKEY™ Vault Privacy 50 (VP50)
# PENDRIVE CRIPTOGRAFADO USB 3.2 Gen 1

*Manual do Usuário*

## Índice


Figura 1: IronKey VP50

## Introdução

O Kingston IronKey Vault Privacy 50 (VP50) é um drive USB superior que oferece uma segurança de grau empresarial com criptografia baseada em hardware AES de 256 bits com certificação FIPS 197 no modo XTS incluindo proteções contra BadUSB com firmware assinado digitalmente e contra ataques a senhas por força bruta. O VP50 também está com conformidade com a TAA e é montado nos EUA. Por ser um armazenamento criptografado sob o controle físico do usuário, a série VP50 é superior ao uso da internet e serviços de nuvem para guardar dados.

O VP50 suporta opções de múltiplas senhas (Admin, Usuário e Recuperação única) com modos Complexos ou de Passe-frase. A opção multissenhas aumenta a capacidade de recuperar o acesso aos dados se uma das senhas for esquecida. Além de ser compatível com as senhas Complexas tradicionais, 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 recuperação única e de Usuário ou redefinir a senha de Usuário para recuperar 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 a senha de recuperação única ou do Usuário após 10 senhas inválidas inseridas seguidamente, e apaga o drive criptograficamente se a senha do Admin for inserida incorretamente 10 vezes seguidas.

Para proteger contra potenciais malwares ou sistemas não confiáveis, o Admin e o Usuário podem aplicar o modo de Somente Leitura para proteger o drive de gravações; além disso, os teclados virtuais integrados protegem as senhas de registros do toque do teclado ou da tela.

Com certificação FIPS 197 e conformidade com a TAA, as organizações podem personalizar e configurar os drives de série VP50 com um Produto ID (PID) para integração com software padrão de Gestão de Endpoint para atender os requisitos corporativos de segurança cibernética e TI através do Programa de Customização da Kingston.

Pequenos e Médios Negócios podem usar a função de Admin para gerenciar seus drives localmente, por ex., utilizar o Admin para configurar ou redefinir as senhas de recuperação única ou do Usuário funcionário, recuperar o acesso aos dados em drives bloqueados e estar em conformidade com as leis e regulamentos quando perícias forem necessárias.

VP50 conta com uma garantia limitada de 5 anos e suporte técnico Kingston gratuito.

**Recursos IRONKEY Vault Privacy 50**

- Com certificação FIPS 197 e criptografia de hardware AES de 256 bits (a criptografia nunca poderá 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
- Configurações duplas de Somente Leitura (proteção de gravação) para proteger o conteúdo do drive contra alterações ou malwares
- Pequenos e médios negócios podem gerenciar os drives localmente usando a função de Admin
- Compatível com Windows ou macOS (consultar a ficha técnica para mais detalhes)

## Sobre este Manual

Este manual do usuário abrange o IronKey Vault Privacy 50 (VP50) e baseia-se na imagem de fábrica sem customizações implementadas.

## Requisitos do sistema

| | |
|---|---|
| **Plataforma de PC**<br>• Intel, AMD & Apple M1 SOC<br>• 15 MB de espaço livre no disco<br>• Porta USB 2.0 - 3.2 disponível<br>• Duas letras consecutivas de drive após o último drive físico*<br><br>***Observação:** Consulte "Conflito de Letra de Drive" na página 32. | **Suporte do Sistema Operacional do PC**<br>• Windows 11<br>• Windows 10<br>• Windows 8.1 |
| **Plataforma Mac**<br>• 15 MB de espaço livre no disco<br>• Porta USB 2.0 - 3.2 | **Suporte do Sistema Operacional Mac**<br>• macOS X (v. 10.13.x – 12.x.x) |

## Recomendações

Para garantir que haja uma ampla energia fornecida ao dispositivo VP50, insira-o diretamente em uma porta USB em seu notebook ou desktop, como visto na ***Figura 1.1***. Evite conectar o VP50 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 VP50 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.

### Lembretes de utilização

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

- Realize um escaneamento para vírus em seu computador antes de instalar e usar o VP50 em um sistema
- Ao usar o drive em um sistema público e que não esteja familiarizado, você deve definir o modo Somente Leitura no dispositivo para ajudar a proteger o drive de malwares
- Bloqueie o dispositivo quando não estiver usando
- 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 VP50 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 VP50 automaticamente limpará os dados criptografados - formatando-se de volta para as configurações de fábrica.

**Multissenhas**
O VP50 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 VP50 pode suportar três senhas diferentes utilizadas para recuperar os dados - Admin, Usuário e senha de Recuperação única**.**

O VP50 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. Além disso, o Admin pode configurar a senha de Recuperação única para o Usuário para fornecer uma forma do Usuário fazer o login e redefinir a senha de Usuário.

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. O Usuário pode utilizar a senha de Recuperação única para redefinir a senha de Usuário quando necessário.

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 VP50 pode ser redefinido e reutilizado, mas os dados anteriores serão excluídos para sempre.

**Modos de senha**
O VP50 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 VP50 suporta frases-passe de 10 a 64 caracteres. Uma frase-passe não segue regras, 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 VP50, 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.

## Configurando 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 a uma porta USB disponível em um notebook ou computador e espere o Windows detectá-lo.

- Usuários Windows 8.1/10/11 receberão uma notificação de 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 abaixo, a letra do drive é (E:).

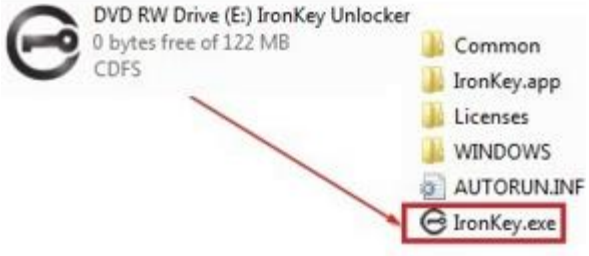



**Figura 3.2 - File Explorer Window/IronKey.exe**

### Acesso ao dispositivo (Ambiente macOS)

Insira o VP50 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 um volume IKVP50 (ou IRONKEY) no computador. (Figura 3.3)

- Clique duas vezes no ícone do IronKey CD-ROM.
- Depois, clique duas vezes no ícone do aplicativo IKVP50 (ou IronKey.app) encontrado na janela exibida na Figura 3.3. Isso fará começar o processo de inicialização.

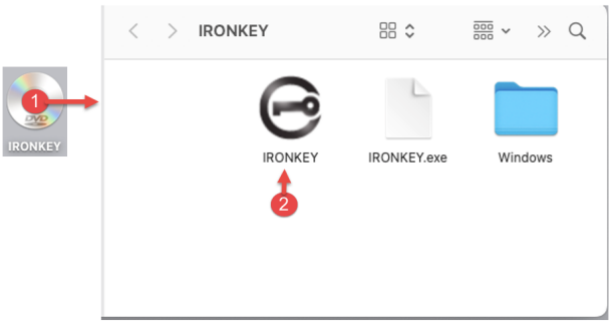
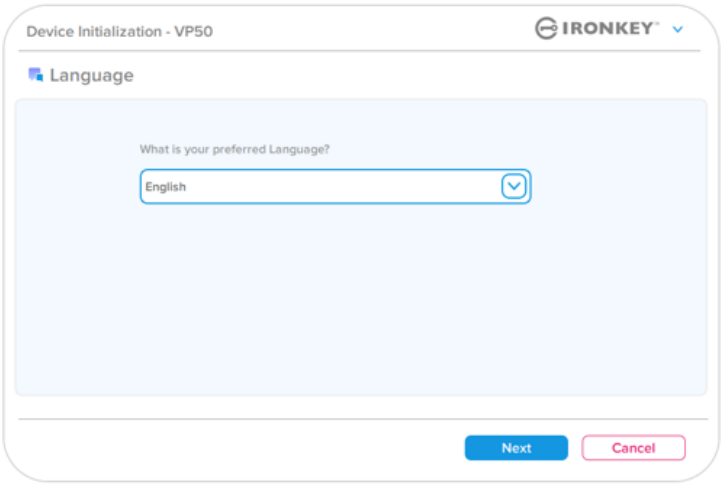
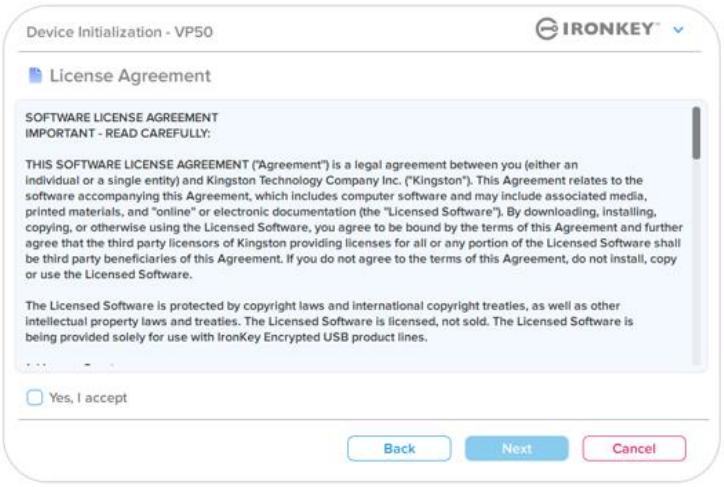



**Figura 3.3 - Volume IKVP**

## Inicialização do dispositivo (Ambiente Windows e macOS)

### Idioma e EULA

| | |
|---|---|
| Selecione o seu idioma de preferência no menu suspenso e clique em **Next** (Avançar). (Ver Figura 4.1) |  **Figura 4.1 - Seleção de idioma** |
| Analise o acordo de licença e clique em **Next** (Avançar).<br><br>Observação: Você deve aceitar o acordo de licença antes de continuar; de outra forma, o botão **Next** (Avançar) continuará inativo. (Figura 4.2) |  **Figura 4.2 - Contrato de Licença** |

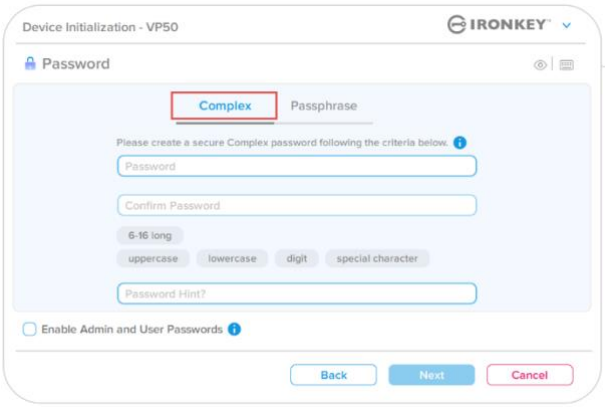
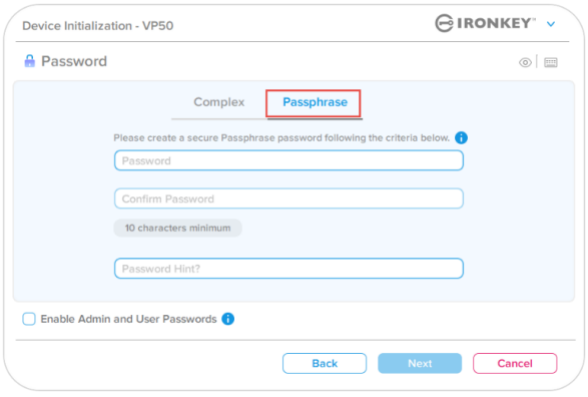
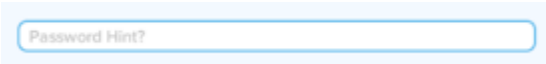
## Inicialização do dispositivo

### Escolha de senha

Na tela de mensagem de Senha, você poderá criar uma senha para proteger seus dados no VP50 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 “Password” (Senha), depois redigite-a nos campos “Confirm Password” (Confirmar Senha). A senha que você criar deve seguir os seguintes critérios antes do processo de inicialização permitir que você continue:

| | |
|---|---|
| **Senha complexa**<br>• Deve conter 6 caracteres ou mais (até 16 caracteres).<br>• Deve conter três (3) dos seguintes critérios:<br>○ Letra maiúscula<br>○ Letra minúscula<br>○ Dígito numérico<br>○ Caracteres especiais (!,$,&, etc.) |  <br>**Figura 4.3 - Senha complexa** |
| **Senha de frase-passe**<br>• Deve conter:<br>○ Mínimo de 10 caracteres<br>○ Máximo de 64 caracteres |  <br>**Figura 4.4 - Senha de frase-passe** |
| **Password Hint** (Dica de senha) **(Opcional)**<br>Uma Dica de senha pode ser útil para fornecer uma pista sobre a senha, se algum dia ela for esquecida.<br>**Observação:** A dica NÃO pode ser a mesma que a senha. |  <br>**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 agora é opcional. (Figura 4.6b)

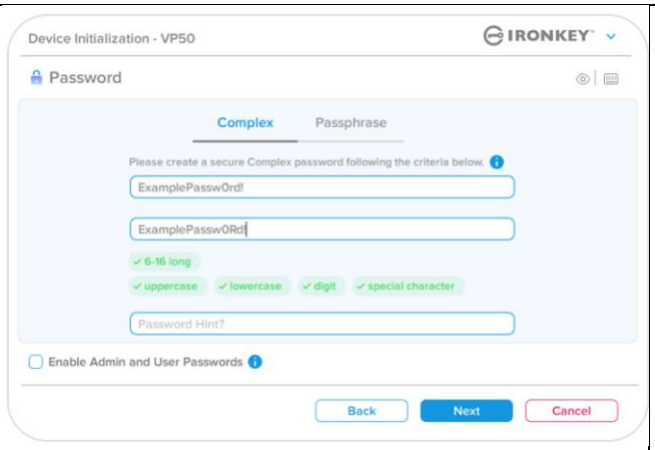



**Figura 4.6a - Condição de senha complexa atendida**

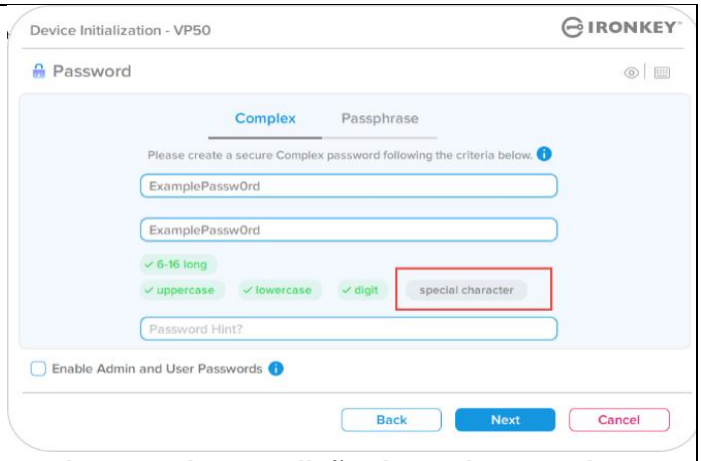



**Figura 4.6b - Condição de senha complexa opcional**

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

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

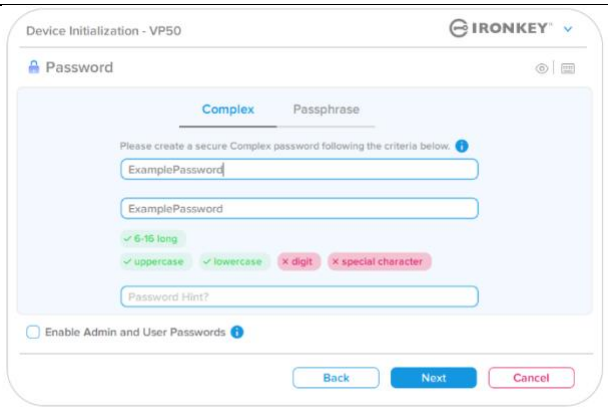



**Figura 4.7 - Condições de senha não atendidas**

## Inicialização do dispositivo

### Teclado virtual

O VP50 oferece um Teclado virtual que pode ser utilizado para proteção contra registros de toque do teclado (keylogger).

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

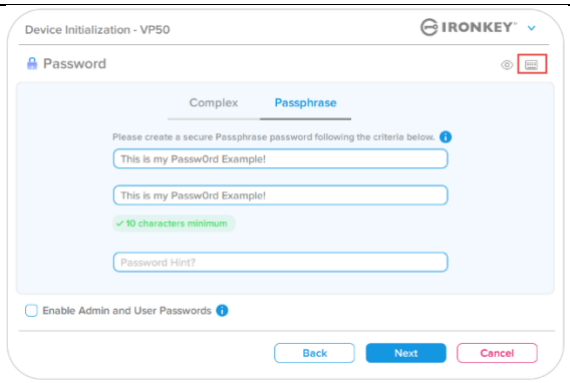



**Figura 4.8 - Ativando o Teclado virtual**

- Quando o teclado virtual aparecer, você também pode habilitar a **Screenlogger Protection** (Proteção contra registros da tela). Ao usar esse recurso, todas as teclas ficarão brevemente em branco. Isso é um comportamento esperado, já que previne que invasores registrem a tela quando você clicar nas teclas.

- Para fazer com que este recurso seja mais sólido, você também pode escolher randomizar o teclado virtual selecionando **randomize** (randomizar) na parte inferior direita do teclado. A Randomização vai ordenar as teclas em uma ordem aleatória.

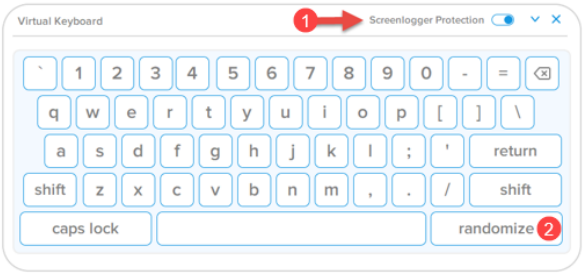


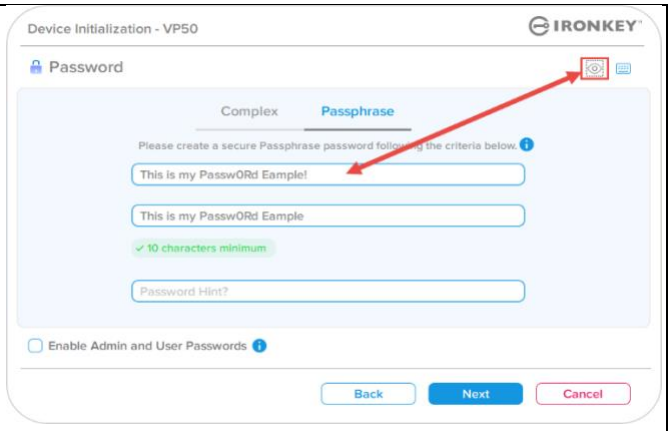
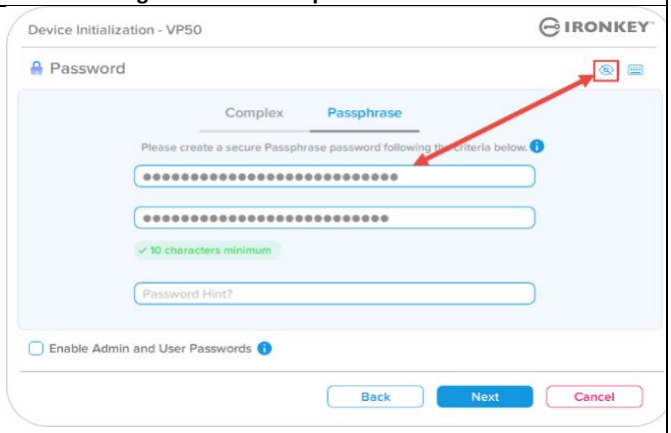

**Figura 4.9 - Proteção contra registro de tela / Randomização**

## Inicialização do dispositivo

### Botão de visibilidade de senha

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

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

| | |
|---|---|
| Para **ocultar** a sequência de senha, clique no ícone cinza.  |   **Figura 4.10 - Botão para “ocultar” a Senha** |
| Para **exibir** a senha oculta, clique no ícone azul.  |   **Figura 4.11 - Botão para “exibir” a Senha** |

## Inicialização do dispositivo

### Senhas de Admin e de Usuário

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

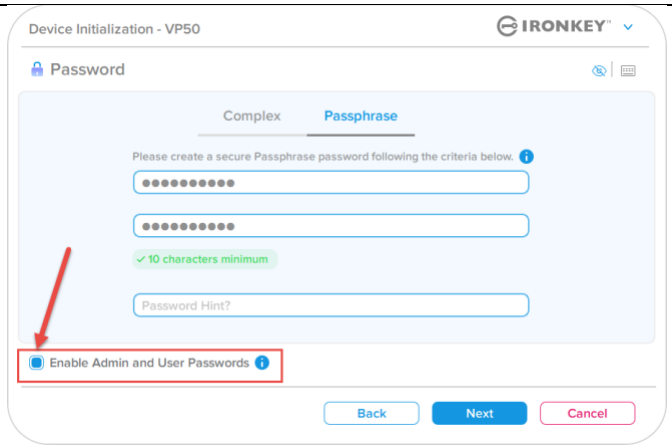
Com as **senhas de Admin e de Usuário** habilitadas, você também pode acessar:

- Senha de recuperação única
- Modo somente leitura forçada para login do Usuário
- Redefinição da senha de Usuário
- Redefinição de senha forçada para login do Usuário

Para saber mais sobre esses recursos, vá até a página 25 dentro deste guia do usuário.

- Para habilitar as **senhas de Admin e de Usuário** clique na caixa próxima a "**Enable Admin and User passwords**" (Habilitar as senhas de Admin e de Usuário) e selecione **Next** (Avançar) assim que uma senha válida for escolhida. (Figura 4.12)

- Se este recurso estiver **habilitado**, então a senha escolhida neste tela será a **senha de Admin**. Clique em **Next** (Avançar) para continuar para a tela da **senha de Usuário** onde uma senha é escolhida para o Usuário.




**4.12- Habilitando as senhas de Admin e de Usuário**

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

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

Para continuar com um Usuário único, configuração de senha única, mantenha **Enable Admin and User Passwords** (Habilitar senhas de Admin e de Usuário) desmarcado, e clique em **Next** (Avançar) depois de criar uma senha válida.

**Observação:** As "**senhas de Admin e de Usuário**" serão mencionadas como "**Função de Admin**" para o restante deste documento.

## 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 (Figura 4.13) A **Senha de Usuário** terá capacidades limitadas em comparação com a do Admin e será discutida com mais detalhes depois neste Guia do Usuário. (Consulte a página 23)

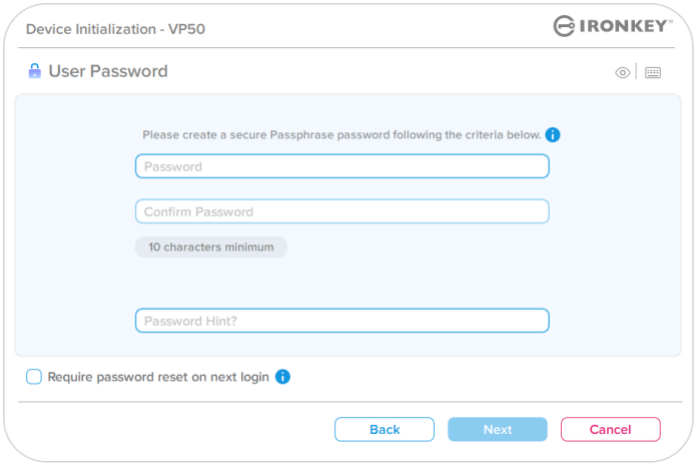



**Figura 4.13 - Senha de Usuário (Admin e Usuário habilitados)**

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

- O recurso de "**Require password reset on next login"** (Exigir redefinição de senha no próximo login) no canto inferior esquerdo da **Figura 4.13** é apenas para a Senha de Usuário e pode ser habilitada para forçar o Usuário a fazer login usando a senha temporária definida pelo Admin durante o processo de inicialização, e então alterá-la para uma senha de sua escolha depois que o drive for autenticado com a senha temporária. Isso é útil quando o drive é dado para outra pessoa usar. **(Figura 4.14)**

  **Observação:** Por segurança, a nova senha não pode ser a mesma da senha temporária.

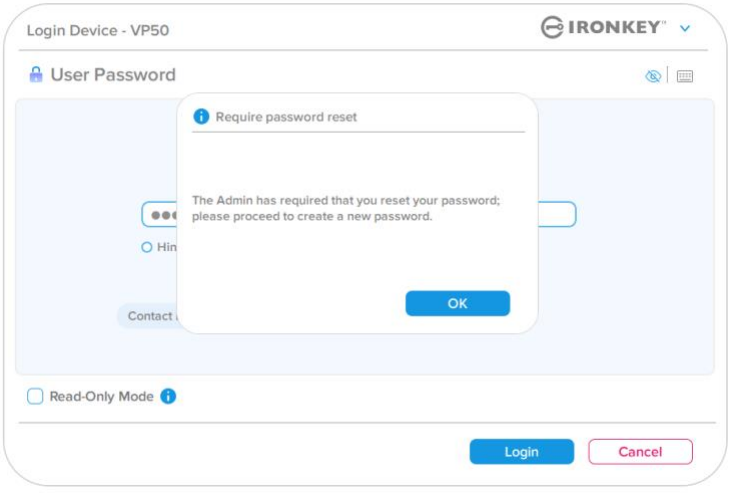


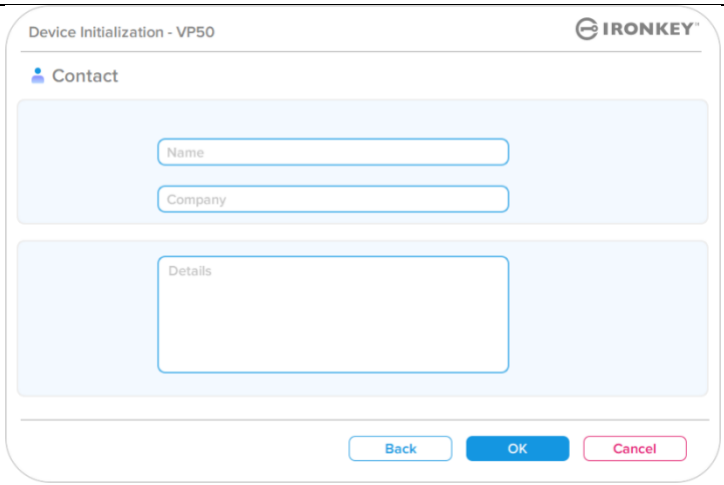

**Figura 4.14 - Exigir redefinição de senha no próximo login (para Senha de Usuário)**

## 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 "**Name**" (Nome) pode conter até 32 caracteres, mas não pode conter a senha **exata**.<br><br>O campo "**Company**" (Empresa) pode conter até 32 caracteres, mas não pode conter a senha **exata**.<br><br>O campo do "**Details**" (Detalhes) pode conter até 156 caracteres, mas não pode conter a senha **exata**. |  <br>**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.

## 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 VP50 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 5.1). Clicando no botão “Login as Admin” (Login como Admin) (mostrado abaixo) o aplicativo prosseguirá para o menu de login do Admin onde você pode fazer login como Admin para acessar os recursos e configurações do Admin. (Figura 5.2)

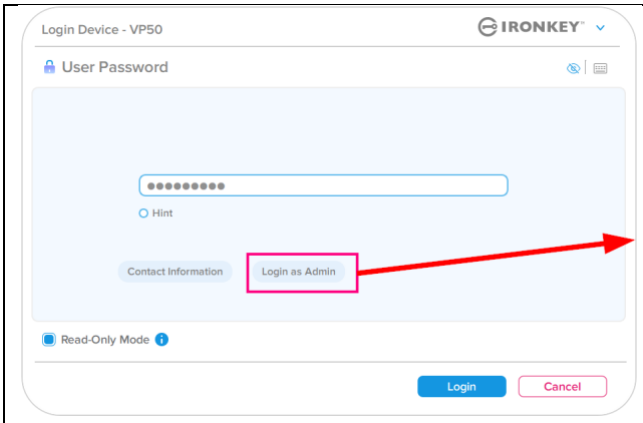



**Figura 5.1 - Login de Senha de Usuário (Admin habilitado)**

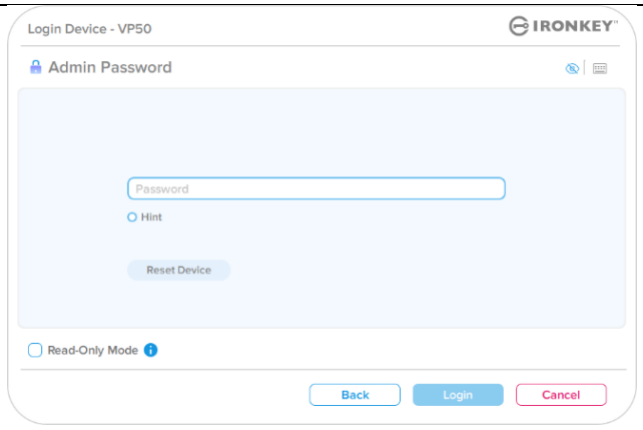



**Figura 5.2 - Login de senha do Admin**

### Login para modo Somente Usuário (Admin não habilitado)

Como mencionado anteriormente na **Página 13**, embora seja recomendado usar a funcionalidade da Função de Admin para obter todos os benefícios de seu dispositivo, o drive IronKey também pode ser iniciado em uma configuração Somente Usuário (Senha única, Usuário único). Essa é uma opção para aqueles que gostariam simplesmente de uma abordagem de senha única para proteger os dados em seu drive. (Figura 5.3)

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

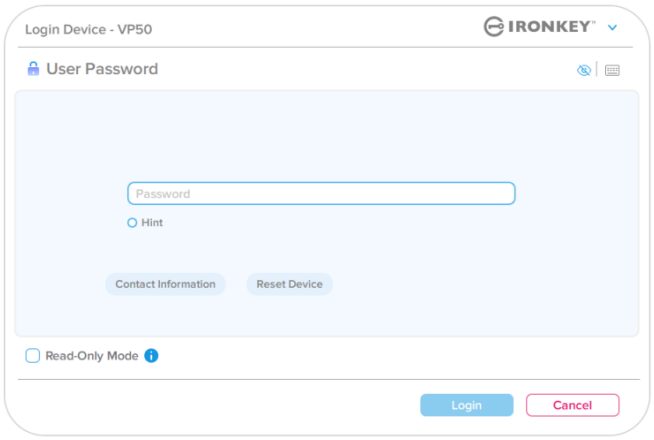



**Figura 5.3 - Login de Senha de Usuário (Admin não habilitado)**

## Uso do dispositivo

### Desbloqueando no módulo Somente Leitura

Você pode desbloquear seu dispositivo em um estado de Somente Leitura para que os arquivos não possam ser alterados em seu drive IronKey. Por exemplo, ao usar um computador desconhecido ou não confiável, desbloquear seu dispositivo no modo somente leitura evitará que qualquer malware neste computador infecte seu dispositivo ou modifique seus arquivos.

Ao funcionar nesse modo, você não pode executar nenhuma operação que envolva modificações dos arquivos no dispositivo.
Por exemplo, você não pode reformatar o dispositivo, restaurar, adicionar ou editar arquivos no drive.

Para desbloquear o dispositivo no Modo somente leitura:

1. Insira o dispositivo na porta USB do computador host e execute o **IronKey.exe**.
2. Marque o **Read-Only Mode** (modo Somente Leitura) abaixo da caixa de entrada da senha. **(Figura 5.4)**
3. Digite a senha do seu dispositivo e clique em **Login**. O IronKey será desbloqueado no modo Somente Leitura.

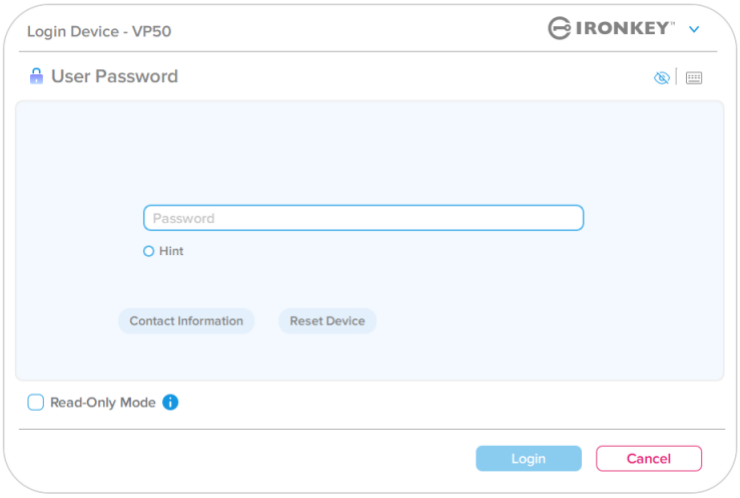



**Figura 5.4 - Modo Somente Leitura**

Se você deseja desbloquear o dispositivo com acesso total de leitura/gravação à partição de dados segura, você deve desligar o VP50 e entrar de novo, deixando a caixa de marcação “Read-Only Mode” (Modo Somente Leitura) desmarcada.

**Observação:** As opções do Admin do VP50 conta com um modo Somente Leitura forçado para os dados do Usuário, o que significa que o login do Usuário pode ser forçado a desbloquear em um estado de Somente Leitura pelo Admin (ver **página 28** para mais detalhes).

## 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 ou usar senha de Recuperação Única para redefinir a senha de Usuário | NÃO |
| Senha de Admin | Apagar drive criptograficamente, Senhas, configurações e dados apagados para sempre | **SIM** |
| Senha de recuperação única | Bloqueio de senha, o botão de senha de Recuperação ficará cinza e inutilizável. Fazer login como Admin para Redefinir a senha | NÃO |
| **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** |

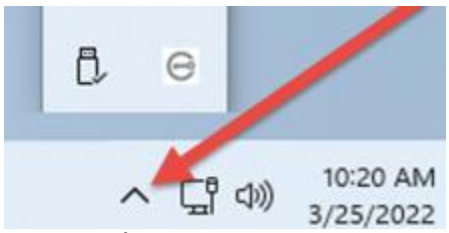
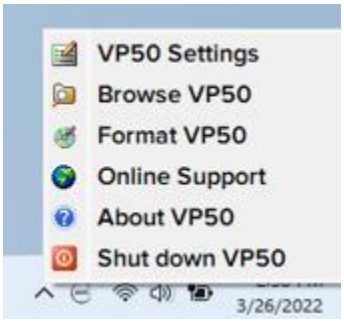
* Depois que você fizer a autenticação no dispositivo corretamente, o contador de erros de login será reiniciado em relação ao método de Login foi utilizado. Apagar criptograficamente excluirá todas as senhas, dados e chaves de criptografia – **seus dados serão perdidos para sempre.**

### Acessar meus arquivos seguros

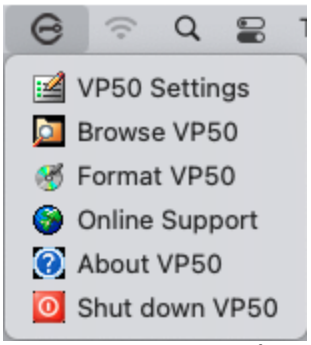
Depois de desbloquear o dispositivo, você pode acessar seus arquivos seguros. Os arquivos são automaticamente criptografados e descriptografados quando você salva ou abre os arquivos no drive. Esta tecnologia gera a conveniência de trabalhar como você faria normalmente com um drive regular, enquanto 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 VP50**. (Figura 6.2)

## Opções do dispositivo - (Ambiente Windows)

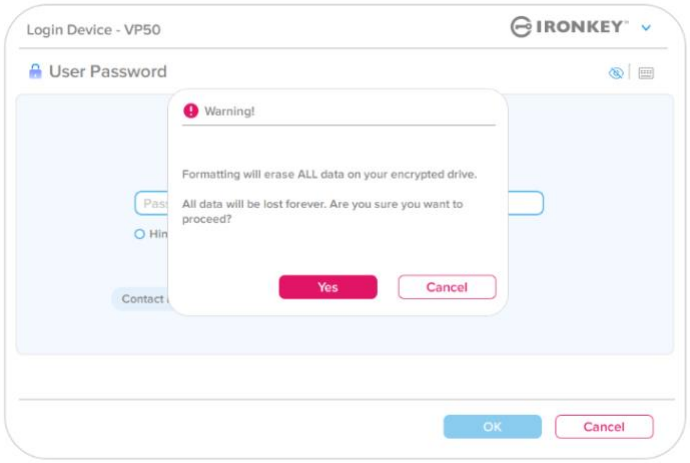
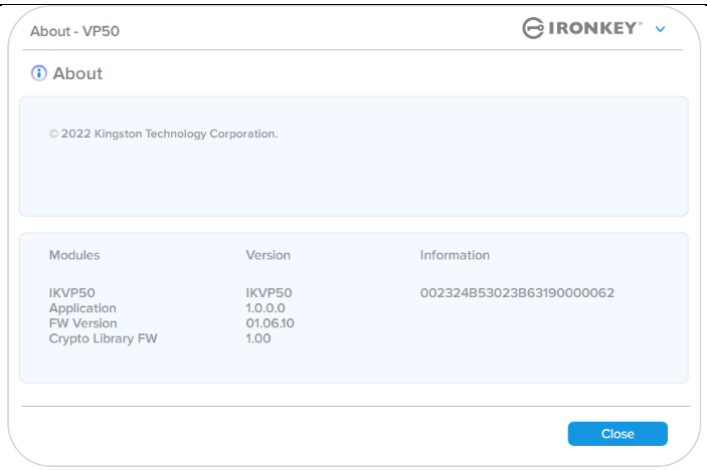
Enquanto você estiver logado no dispositivo, haverá um ícone IronKey localizado no canto direito da janela. Clicar com o botão direito no Ícone IronKey abrirá o menu de seleção para opções do drive disponíveis. (Figura 6.2) Detalhes sobre essas opções do dispositivo podem ser encontradas nas Páginas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

| | |
|---|---|
| • Enquanto você estiver logado no dispositivo, haverá um ícone IronKey localizado no canto direito da janela. **(Figura 6.1)** |  **Figura 6.1 – 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 6.2)**<br><br>Detalhes sobre essas opções do dispositivo podem ser encontradas nas páginas 19 a 23 deste manual. |  **Figura 6.2 - 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 VP50 localizado no menu do macOS visto na **Figura 6.3** que abrirá as opções de dispositivo disponíveis.<br><br>Detalhes sobre essas opções do dispositivo podem ser encontradas nas Páginas 19 a 23 deste manual. |  **Figura 6.3 - Menu de opções do dispositivo/Ícone da barra de menu do macOS** |

## Opções do dispositivo

| | |
|---|---|
| **Configurações do VP50:** | • Alterar senha de login, Informações de contato e outras configurações. (Mais detalhes sobre configurações do dispositivo podem ser encontrados na seção “Configurações do VP50” deste manual). |
| **Browse VP50:** | • Permite que você visualize seus arquivos de segurança. |
| **Format VP50:**<br>Permite que você formate a partição de dados segura. (Aviso: Todos os dados serão apagados) (**Figura 6.1**)<br><br>**Observação:** A autenticação da senha será exigida para formatar. |  <br>**Figura 6.1 – Formatar o VP50** |
| **Online Support** (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. |
| **About VP50** (Sobre o VP50):<br>Fornece detalhes específicos sobre o VP50, incluindo Aplicação, Firmware e Informações de número de série. (**Figura 6.2**)<br><br>**Observação:** O número de série único do drive estará na “Coluna de informações”. |  <br>**Figura 6.2 - Sobre o VP50** |
| **Shut down VP50** (Desligar o VP50): | • Encerra de modo apropriado o VP50, permitindo que seja removido com segurança do seu sistema. |

# Configurações do VP50

## Configurações do Admin

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

- **Senha:** Permite que você altere sua própria senha de Admin e/ou dica (*Figura 7.1*)
- **Informações de contato:** Permite que você adicione/visualize/altere suas informações de contato (*Figura 7.2*)
- **Idioma:** Permite que você altere sua seleção de idioma atual (*Figura 7.3*)
- **Opções do Admin:** Permite que você habilite recursos adicionais como: (Figura 7.4)
    - Alterar Senha de Usuário
    - Redefinição de senha de login (Para Senha de Usuário)
    - Habilitar senha de Recuperação única
    - Forçar modo Somente Leitura para dados do Usuário

**OBSERVAÇÃO:** Detalhes adicionais das Opções do Admin podem ser encontradas na página 24.

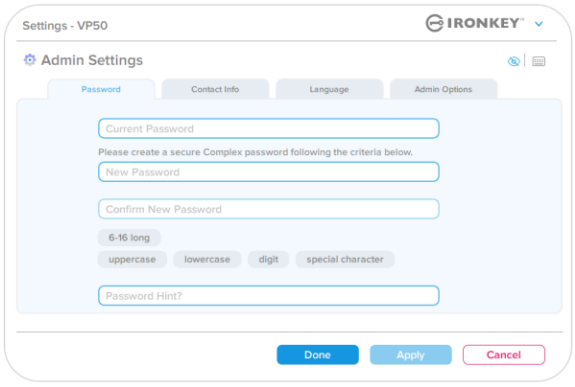



**Figura 7.1- Opções de Senha**

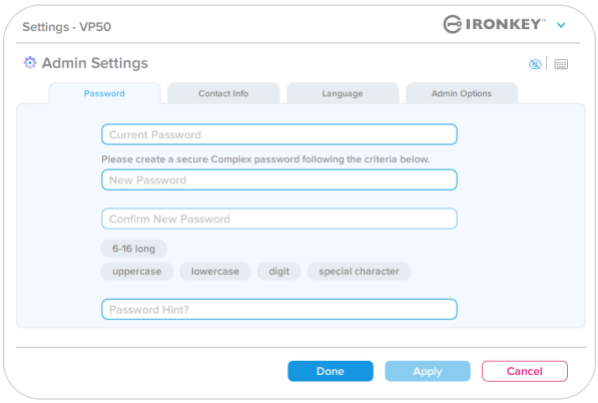



**Figura 7.2 - Informações de contato**

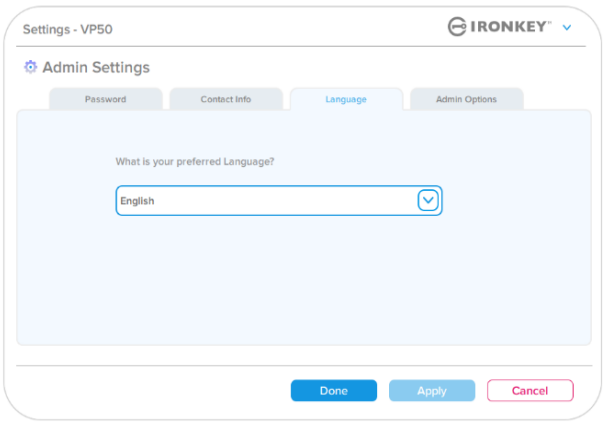



**Figura 7.3 - Opções de idioma**

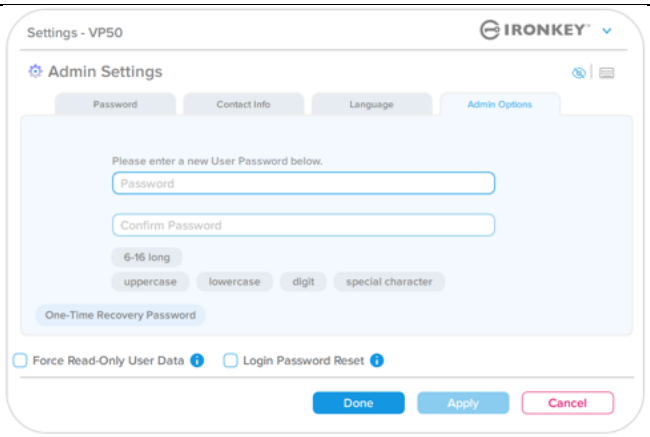
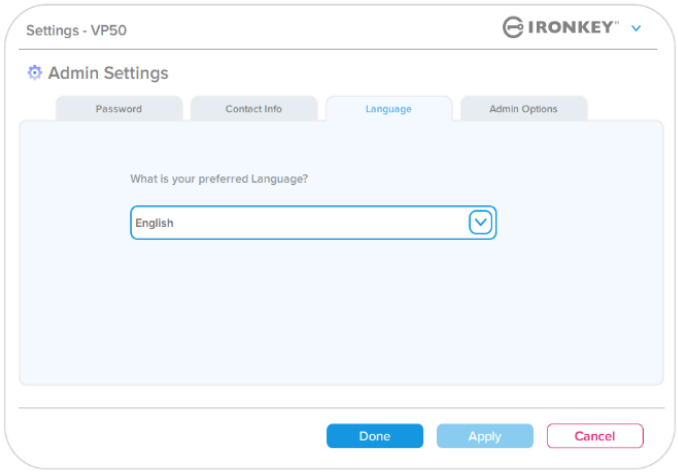
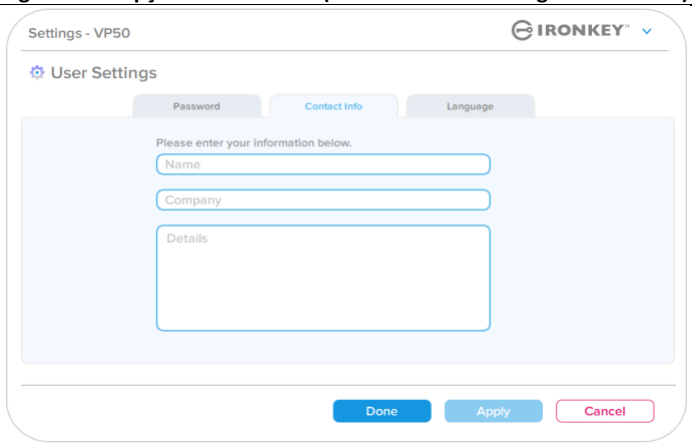
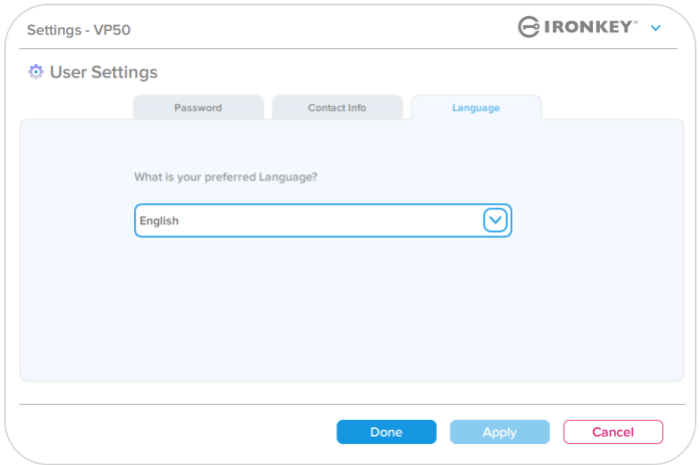



**Figura 7.4 - Opções do Admin**

## Configurações do VP50

### Configurações do Usuário: Admin habilitado

O login do Usuário limita o acesso às seguintes configurações:

| | |
|---|---|
| **Senha:**<br>Permite que você altere sua própria senha de Usuário e/ou dica. *(Figura 7.5)* |  <br>**Figura 7.5 - Opções de senha do (Admin habilitado: Login do Usuário)** |
| **Informações de contato:**<br>Permite que você adicione/visualize/altere suas informações de contato. *(Figura 7.6)* |  <br>**Figura 7.6 - Informações de contato (Admin habilitado: Login do Usuário)** |
| **Idioma:**<br>Permite que você altere sua seleção de idioma atual. *(Figura 7.7)* |  <br>**Figura 7.7 - 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 VP50

### Configurações do Usuário: Admin não habilitado

Como mencionado anteriormente na Página 12, iniciar o VP50 sem habilitar as senhas de “Admin e de Usuário” vai configurar o drive em uma **configuração de Usuário único, Senha única.** Esta configuração não possui acesso a qualquer recurso ou opção do Admin. Esta configuração terá acesso às seguintes configurações do VP50:

### Alterar e Salvar configurações

- Sempre que as configurações forem alteradas nas Configurações do VP50 (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 7.11)

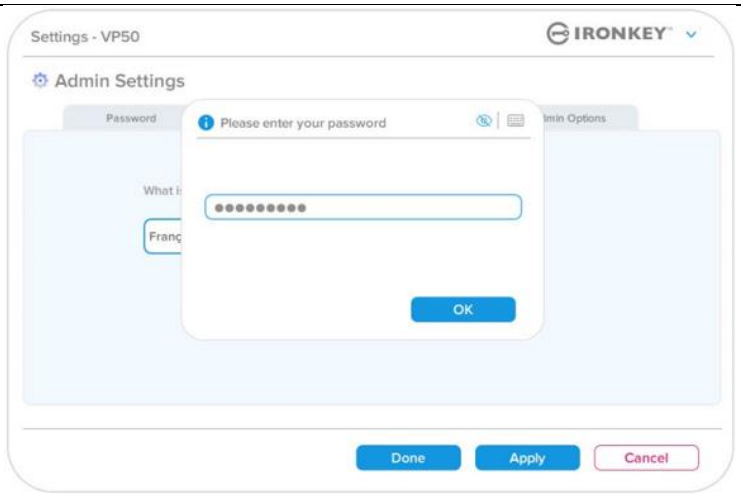



**Figura 7.11 - Tela de alerta de Senha para salvar as alterações de configurações do VP50**

**Observação:** Se você estiver na tela de alerta de Senha acima e gostaria de cancelar ou modificar suas alterações, você pode fazer isso simplesmente deixando o campo de senha em branco e clicando em “OK”. Isso vai fechar a caixa “Please enter your password” (Por favor insira sua senha) e voltar para o menu de configurações do VP50.

## Recursos do Admin

**Opções disponíveis para redefinir a senha de Usuário**
Os recursos de configuração do Admin permite várias formas de redefinir a Senha dos Usuários com segurança, seja por esquecimento ou caso uma senha de Usuário temporária seja criada e você desejar aplicar uma alteração de senha no próximo login para o Login do Usuário. Abaixo estão os recursos que podem ser úteis para redefinir a senha de Usuário:

**Redefinição da senha de Usuário:**
Altere manualmente a Senha de Usuário no menu de "Admin Options" (Opções do Admin), que é uma mudança instantânea e fará efeito no próximo login de Usuário. **(Figura 8.1)**

**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).

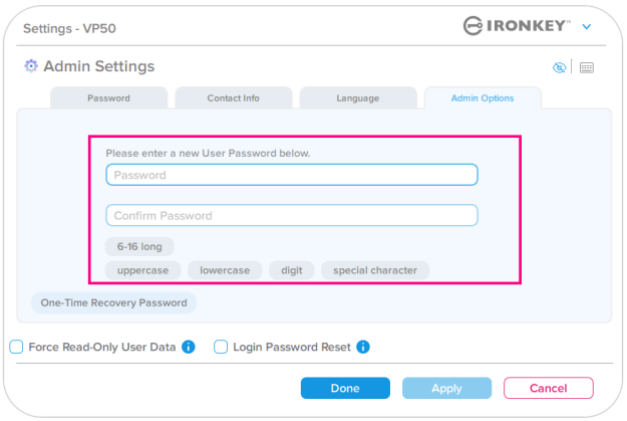



**Figura 8.1 - Redefinição de Senha de Usuário/Opções do Admin**

**Redefinição da senha de login:**
Habilitar a Redefinição de senha de login **forçará o Usuário a fazer login usando uma senha temporária definida pelo Admin** e depois mudar para uma senha de sua escolha. Isso é útil quando o drive é dado para outra pessoa usar. **(Ver Figuras 8.2A e 8.2B)**

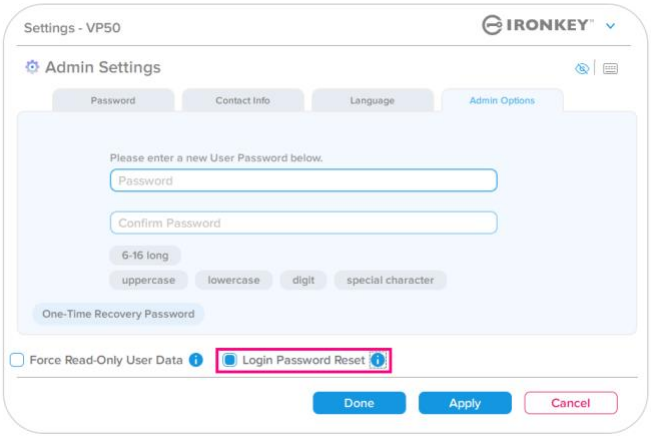
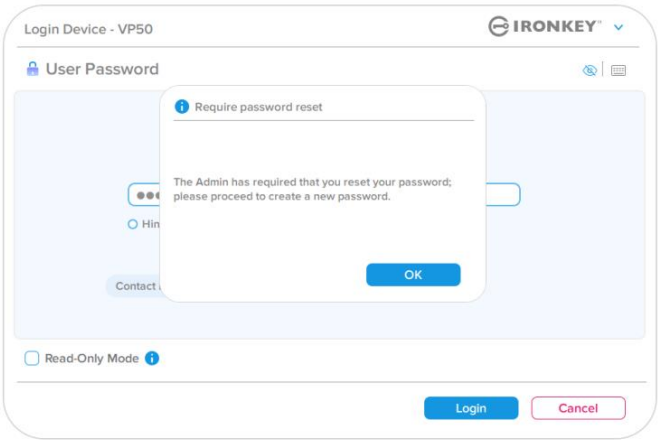



**Figura 8.2A - Botão de Redefinição de senha de login**

**Observação:** A aplicação dessa redefinição acontecerá no próximo login de Usuário bem-sucedido. Os critérios de exigência de senha serão aplicados automaticamente de acordo com a opção original definida durante o processo de inicialização (opções de frase-passe ou complexa).

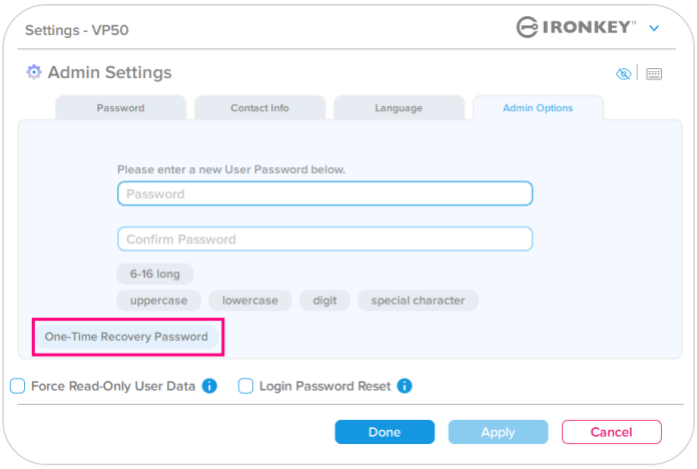


| | |
|---|---|
| | **Figura 8.2B - Notificação de redefinição depois que a senha de Usuário for inserida** |

## Recursos do Admin

### Senha de recuperação única

Esta seção discutirá o processo para habilitar e usar o recurso de Senha de recuperação única.

| | |
|---|---|
| **Senha de recuperação única**<br><br>**Passo 1:** O recurso de Senha de recuperação única é muito útil, a senha de uso único que pode ser habilitada para ajudar a recuperar e redefinir a senha de Usuário caso a senha de Usuário seja esquecida. Clique no botão “One-Time Recovery Password” (Senha de recuperação única) no menu de opções do Admin para iniciar. **(Figuras 8.4)** |  <br>**Figura 8.4 - Botão de Senha de recuperação única** |

**Passo 2:** Crie uma senha de recuperação única usando os mesmos critérios de senha que o dispositivo foi definido inicialmente com (Complexa ou Passe-frase).

**Observação:** A senha do Admin será exigida para aplicar as alterações.

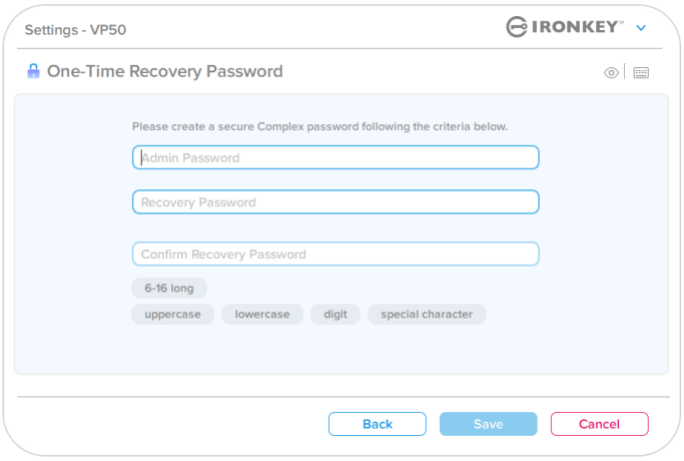



**Figura 8.5 - Configuração de Senha de recuperação única**

## Recursos do Admin

Usando a senha de recuperação única

**Passo 1:** Depois que a Senha de recuperação única foi criada, um novo botão vai aparecer na tela de login da **User Password** (Senha de Usuário) no próximo login. Clique no botão **Recovery Password** (Senha de recuperação) para iniciar o processo.

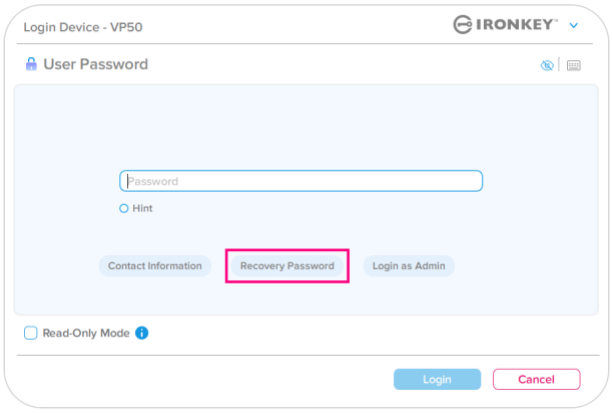



**Figura 8.6 - Botão de Senha de recuperação**

**Passo 2:** A tela da **Recovery Password** (Senha de recuperação) vai aparecer onde você pode inserir a Senha de recuperação e criar uma nova Senha de Usuário. (Figura 8.7)

**Importante:** A senha de recuperação única também utiliza um recurso de segurança integrado que monitora o número de tentativas erradas de login, **depois de 10 tentativas de Login incorretas com a senha de recuperação única, a senha será desabilitada**, e precisará ser reabilitada fazendo login no drive como Admin. (ver páginas 18 e 30 para mais detalhes)

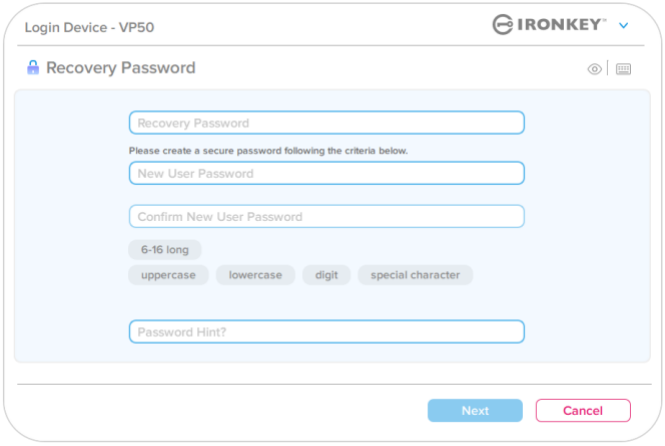



**Figura 8.7 - Menu de Senha de recuperação**

**Passo 3:** Se bem-sucedido, você será levado de volta à tela de **User Password** (Senha de Usuário). O botão **Recovery Password** (Senha de recuperação) não está mais lá e a senha de Usuário inserida no **Passo 2** se tornará a nova Senha de Usuário. (Figura 8.8)

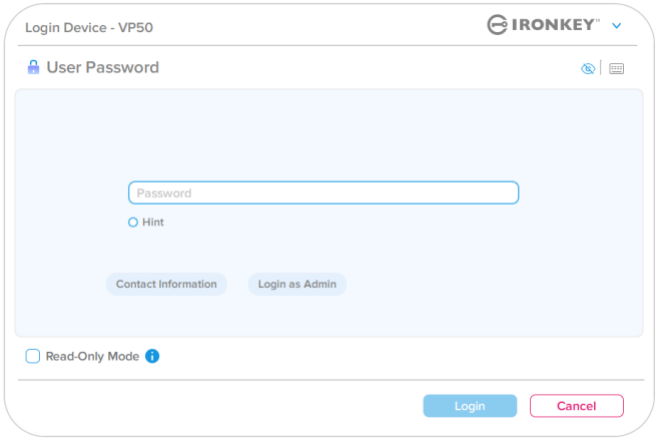



**Figura 8.8 - Tela de login da Senha de Usuário mostrando que o botão de Senha de recuperação desaparece depois do uso bem-sucedido.**

## Recursos do Admin

### Force os dados de usuário para somente leitura

O modo forçado de somente leitura pode ser habilitado para restringir o acesso à gravação no drive pelo Usuário. Este recurso é útil se arquivos no drive são necessários apenas para acesso de leitura.

- Para habilitar o Forçar Somente Leitura para os dados do Usuário, clique na caixa e clique em “Apply” (Aplicar). **(Figura 8.9)**

  **Observação:** Esse modo de Forçar Somente Leitura se aplica apenas ao Usuário e não afeta o login do Admin. O login do Admin ainda terá privilégios de acesso de Leitura e Gravação e ainda poderá habilitar o modo Somente Leitura se necessário.

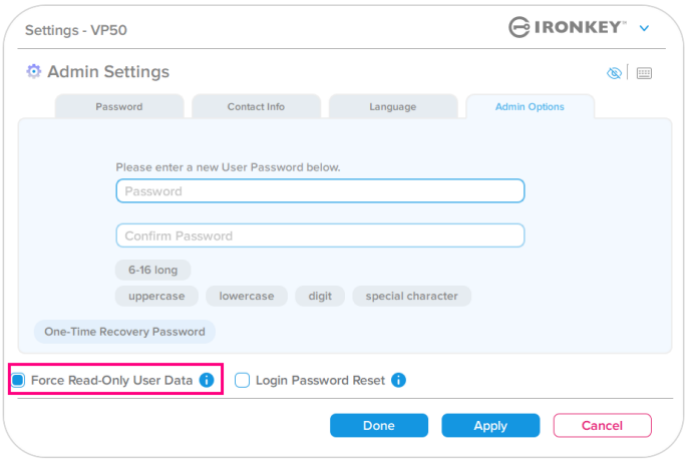



**Figura 8.9 - Habilitar “Forçar dados de usuário para Somente Leitura” (A Senha do Admin será exigida para aplicar as alterações)**

- Assim que for habilitada, a caixa de botão do **“Read-Only Mode”** (Modo Somente Leitura) ficará azul, o que significa que o modo de Somente Leitura Forçado está habilitado permanentemente para a senha de Usuário, até que seja desabilitado pelo Admin . (Figura 8.10)

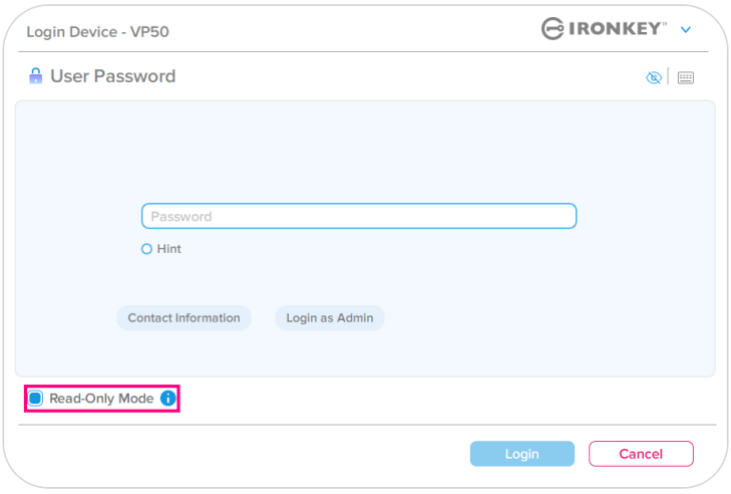



**Figura 8.10 - Modo Somente Leitura é forçado habilitado para o usuário e só pode ser desabilitado pelo Admin**

## Ajuda e Resolução de Problemas

### Bloqueio do dispositivo

O VP50 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 alcançado. A configuração padrão de fábrica tem um valor pré-configurado de 10 (nº de tentativas) para cada método de login (Senha de recuperação única/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 9.1)

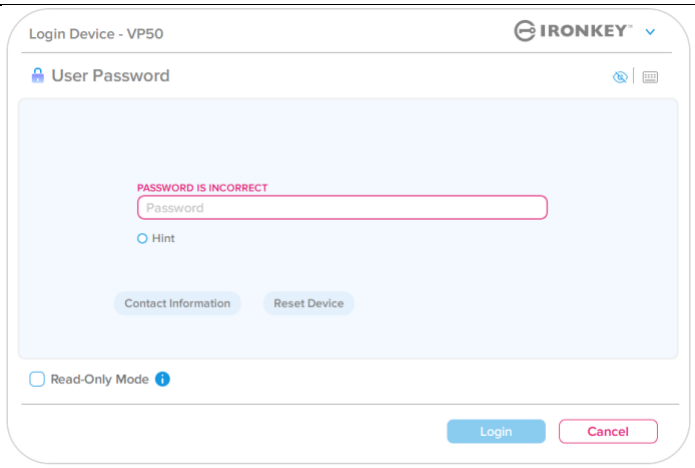



**Figura 9.1 - Mensagem de senha incorreta**

- 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 9.2)

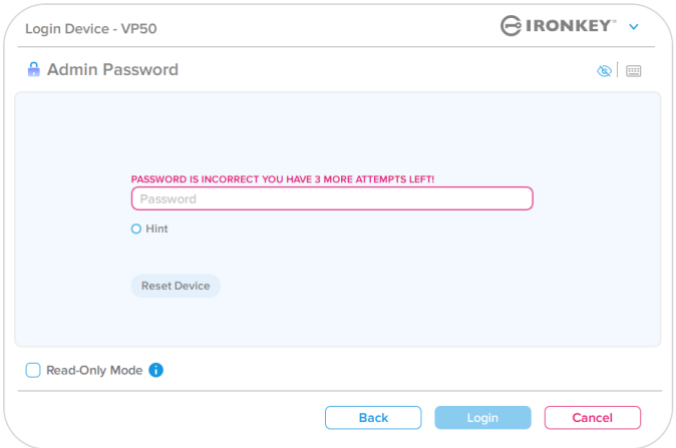



**Figura 9.2 - 7ª tentativa de senha incorreta**

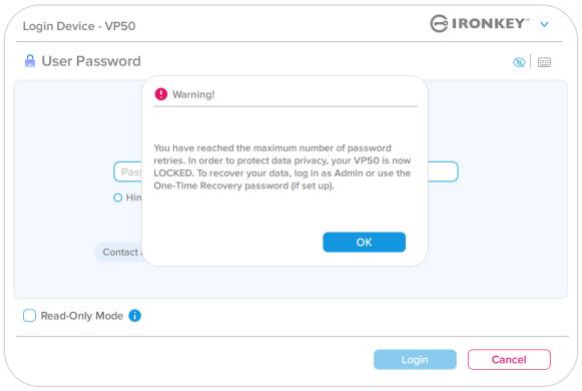
## Ajuda e Resolução de Problemas

### 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, (Senha de recuperação única, 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 9.3 - 9.6 abaixo demonstram o comportamento visual do 10º e último login errado de cada método de senha de login:

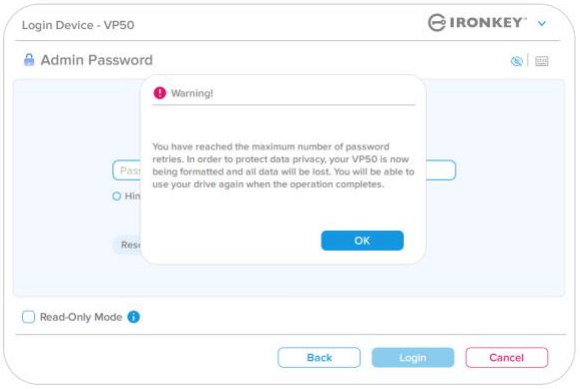
**Senha de Usuário: (Admin/Usuário habilitado)**




**BLOQUEIO DO DISPOSITIVO**

**(Figura 9.3)**

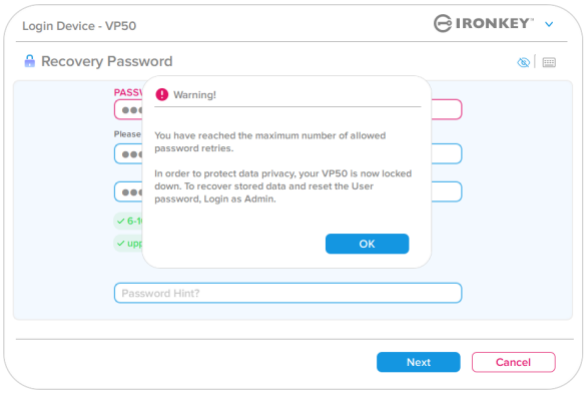
**Senha do Admin (Admin/Usuário habilitado)**




**FORMATAÇÃO DO DISPOSITIVO***

**(Figura 9.4)**

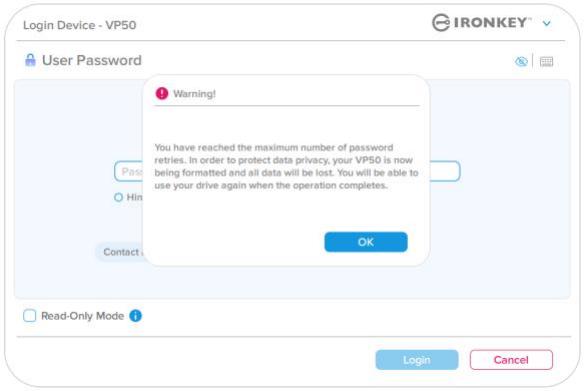
**Recuperação única: (Admin/Usuário habilitado)**




**BLOQUEIO DO DISPOSITIVO**

**(Figura 9.5)**

**Senha de Usuário (Admin NÃO habilitado)**




**FORMATAÇÃO DO DISPOSITIVO***

**(Figura 9.6)**

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 VP50 e esquecer sua senha, as mesmas medidas de segurança serão aplicadas, incluindo a formatação do dispositivo. * Para saber mais sobre este recurso, veja *"Restaurar Dispositivo"* na página 25.

**Observação: Uma formatação de dispositivo apagará TODAS as informações armazenadas na partição de dados segura do VP50.*

## Ajuda e Resolução de Problemas

### Restaurar dispositivo

Se você esqueceu a sua senha ou precisa restaurar seu dispositivo, você pode clicar no botão "*Reset Device*" (*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 "User Password' (Senha de Usuário) se o modo Admin/Usuário não estiver habilitado) quando o iniciador do VP50 for executado. (ver **Figura 9.7 e 9.8**)

- Esta opção vai permitir que você crie uma nova senha, mas para proteger a privacidade de seus dados, o VP50 será formatado. Isso significa que todos os seus dados serão apagados no processo.*

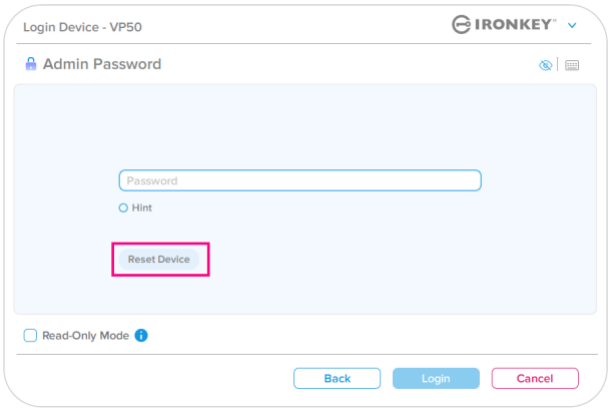



**Figura 9.7 - Senha do Admin: Botão para Restaurar Dispositivo**

- **Observação:** Quando você clicar em "*Reset Device" (Restaurar Dispositivo)*, uma caixa de mensagem vai aparecer e perguntar se você deseja inserir uma nova senha antes de executar a formatação. Nesse ponto, você pode 1) clicar em "OK" para confirmar ou 2) clicar em "Cancel" (Cancelar) para voltar para a janela de login. (Ver Figura 9.8)

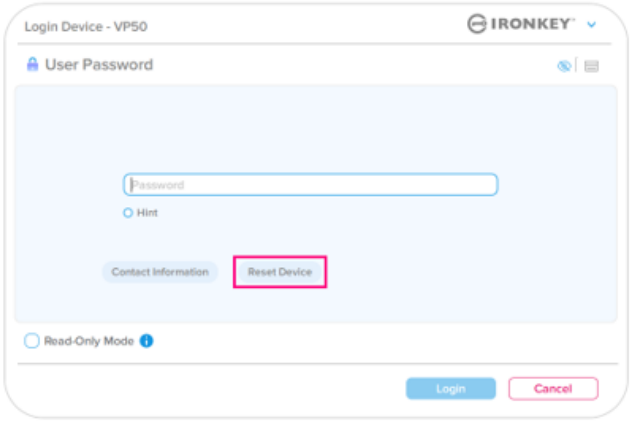
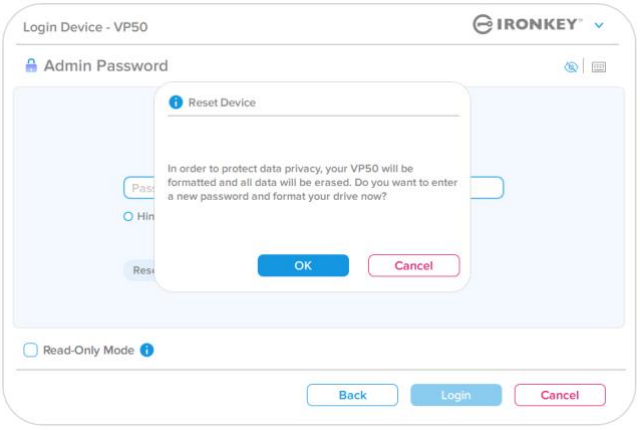



**Figura 9.8 - Senha de Usuário (Admin/Usuário não habilitado) Restaurar Dispositivo**

| | |
|---|---|
| • Ser você optar por continuar, você será levado para a tela de inicialização onde você pode habilitar os “Admin and User modes” (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. |  <br>**Figura 9.9 - 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 VP50 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 9.10*.) 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 VP50 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). Como mencionado na seção de *"Requisitos do Sistema"* deste manual (na página 3), o VP50 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 9.10*.) 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.

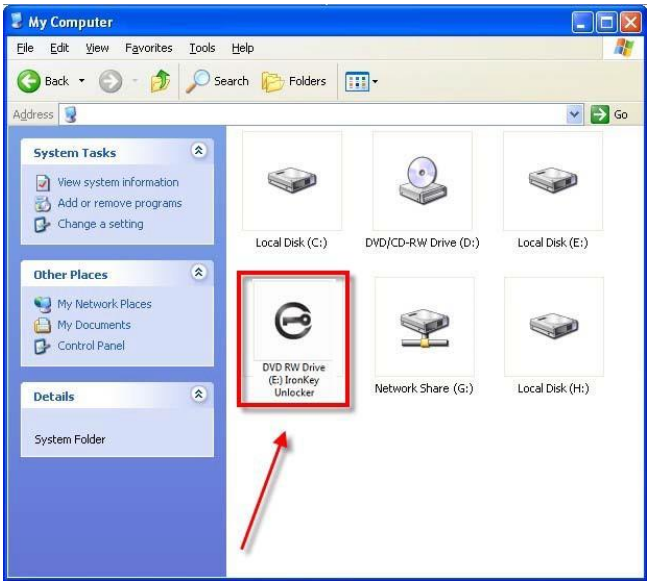



**Figura 9.10 - Exemplo de letra de drive**

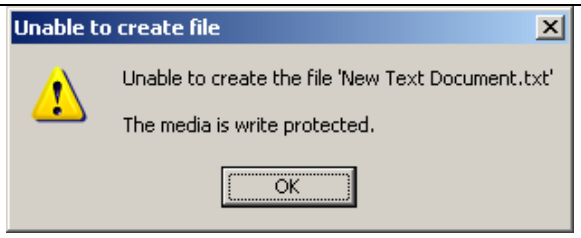
Neste exemplo, (Figura 9.10), o VP50 utiliza o drive F:, que é a primeira letra de drive disponível após o drive E: (o último disco físico antes do intervalo de letra de drive.) Como a letra G: é um compartilhamento de rede e não faz parte do perfil de hardware, o VP50 pode tentar utilizá-lo como sua segunda letra de drive, causando um conflito.

Se não existirem compartilhamentos de rede no seu sistema e o VP50 continuar não iniciando, é possível que um leitor de cartões, um disco removível ou outro dispositivo previamente instalado esteja mantendo atribuída a letra de drive e ainda causando 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.

## Ajuda e Resolução de Problemas

### Mensagens de Erro

| | |
|---|---|
| **Unable to create file** (Não é possível criar o arquivo):<br>Esta mensagem de erro vai aparecer quando tentar CRIAR um arquivo ou pasta NA partição de dados segura enquanto estiver logado no modo de Somente Leitura. |  <br>**Figura 9.11 - Erro Não é possível criar arquivo** |
| **Error copying file or folder** (Erro ao copiar arquivo ou pasta):<br>Esta mensagem de erro vai aparecer quando tentar COPIAR um arquivo ou pasta PARA a partição de dados segura enquanto estiver logado no modo de Somente Leitura. |  <br>**Figura 9.12 - Erro ao Copiar arquivo ou pasta** |
| **Error deleting file or Folder** (Erro ao apagar arquivo ou pasta):<br>Esta mensagem de erro vai aparecer quando tentar EXCLUIR um arquivo ou pasta DA partição de dados segura enquanto estiver logado no modo de Somente Leitura. |  <br>**Figura 9.13 - Erro ao excluir arquivo ou pasta** |

**Observação:** Se você já está logado no modo Somente Leitura e deseja desbloquear o dispositivo com acesso total de leitura/gravação à partição de dados segura, você deve desligar o VP50 e entrar de novo, deixando a caixa de marcação “Read-Only Mode” (Modo Somente Leitura) desmarcada antes de fazer login.

# IRONKEY™ Vault Privacy 50 (VP50)
# SZYFROWANA PAMIĘĆ FLASH USB 3.2 Gen 1

*Instrukcja obsługi*

## Spis treści


Ilustracja 1 – Urządzenie IronKey VP50

## Wprowadzenie

Kingston IronKey Vault Privacy 50 (VP50) to najwyższej jakości urządzenie pamięci USB, które zapewnia bezpieczeństwo klasy biznesowej dzięki 256-bitowemu szyfrowaniu sprzętowemu AES z certyfikatem FIPS 197 w trybie XTS, w tym ochronę przed atakami przez lukę BadUSB dzięki cyfrowo podpisanemu oprogramowaniu sprzętowemu oraz atakami Brute Force z wykorzystaniem hasła. Pamięć VP50 jest również zgodna z przepisami TAA i montowana w USA. Ponieważ pamięć VP50 jest szyfrowaną pamięcią masową znajdującą się pod fizyczną kontrolą użytkownika, korzystanie z niej jest lepszym rozwiązaniem niż korzystanie z Internetu i usług w chmurze w celu ochrony danych.

Pamięć VP50 obsługuje opcję wielu haseł (administratora, użytkownika i jednorazowe hasło odzyskiwania) w trybach haseł złożonych lub wyrażeń hasłowych. Opcja wielu haseł (Multi-Password) zwiększa możliwość odzyskania dostępu do danych w przypadku zapomnienia jednego z haseł. Oprócz obsługi tradycyjnych haseł złożonych, nowy tryb wyrażenia hasłowego umożliwia wprowadzenie numerycznego kodu PIN, zdania, listy słów, a nawet tekstu o długości od 10 do 64 znaków. Administrator może włączyć hasło użytkownika i funkcję jednorazowego hasła odzyskiwania lub zresetować hasło użytkownika, aby przywrócić dostęp do danych.

Aby ułatwić wprowadzanie hasła, można włączyć jego podgląd (symbol „oka”) , co pozwala ograniczyć liczbę literówek i nieudane próby zalogowania. Funkcja ochrony przed atakami typu Brute Force blokuje hasło użytkownika lub jednorazowe hasło odzyskiwania po 10 kolejnych próbach wprowadzenia nieprawidłowego hasła oraz kryptograficznie wymazuje zawartość pamięci po 10 kolejnych próbach wprowadzenia nieprawidłowego hasła administratora.

W celu ochrony przed potencjalnie złośliwym oprogramowaniem w niezaufanych systemach administrator i użytkownik mogą ustawić tryb tylko do odczytu, aby zabezpieczyć pamięć przed zapisem. Ponadto wbudowana klawiatura wirtualna chroni hasła przed keyloggerami i screenloggerami.

Posiadające certyfikat FIPS 197 i spełniające wymogi przepisów TAA urządzenia pamięci z serii VP50 umożliwiają organizacjom ich personalizację i konfigurację z wykorzystaniem identyfikatora produktu (PID) w celu integracji ze standardowym oprogramowaniem do zarządzania punktami końcowymi. Pozwala to spełnić wymagania korporacyjnych systemów informatycznych i bezpieczeństwa cybernetycznego w ramach Programu personalizacji produktów firmy Kingston.

Małe i średnie firmy mogą korzystać z funkcji administratora do lokalnego zarządzania urządzeniami pamięci, np. w celu konfigurowania lub resetowania haseł użytkownika lub jednorazowych haseł odzyskiwania dla pracowników, odzyskiwania dostępu do danych na zablokowanych nośnikach oraz w celu zachowania zgodności z przepisami i regulacjami, gdy niezbędne jest przeprowadzenie badań kryminalistycznych.

Pamięć VP50 jest objęta ograniczoną 5-letnią gwarancją i bezpłatną pomocą techniczną firmy Kingston.

## Cechy urządzenia IronKey Vault Privacy 50

- 256-bitowe szyfrowanie sprzętowe w trybie XTS-AES z certyfikatem FIPS 197 (funkcji szyfrowania nie można wyłączyć)
- Ochrona przed atakami typu 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
- Podwójne ustawienia trybu tylko do odczytu (ochrona przed zapisem) w celu ochrony zawartości pamięci przed zmianami lub złośliwym oprogramowaniem
- Małe i średnie firmy mogą lokalnie zarządzać urządzeniami pamięci, korzystając z funkcji administratora
- Zgodność z systemem Windows lub macOS (szczegóły w arkuszu danych)

## Informacje o tej instrukcji

Niniejsza instrukcja obsługi dotyczy pamięci IronKey Vault Privacy 50 (VP50) w wersji fabrycznej, tj. bez zmian dokonanych na życzenie klienta.

## Wymagania systemowe

| | |
|---|---|
| **Platforma PC**<br>• Intel, AMD i Apple M1 SOC<br>• 15MB wolnego miejsca na dysku<br>• Dostępny port USB 2.0/3.2<br>• Dwie kolejne litery dysku po ostatnim dysku fizycznym*<br><br>***Uwaga:** patrz rozdział „Konflikt liter dysków” na str. 32. | **Obsługiwane systemy operacyjne komputerów PC**<br>• Windows 11<br>• Windows 10<br>• Windows 8.1 |
| **Platforma Mac**<br>• 15MB wolnego miejsca na dysku<br>• Port USB 2.0/3.2 | **Obsługiwane systemy operacyjne komputerów Mac**<br>• macOS X (wer. 10.13.x – 12.x.x) |

## Zalecenia

Aby zagwarantować odpowiednie zasilanie urządzenia VP50, należy podłączać je bezpośrednio do portu USB w notebooku lub komputerze stacjonarnym, jak pokazano na ***ilustracji 1.1***. Należy unikać podłączania urządzenia VP50 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 VP50 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 VP50 w systemie docelowym
- W przypadku korzystania z pamięci w dostępnym publicznie lub nieznanym systemie można włączyć w urządzeniu tryb tylko do odczytu, aby chronić pamięć przed złośliwym oprogramowaniem
- Zablokowanie urządzenia, gdy nie jest używane
- Wysuwanie urządzenia z systemu przed jego odłączeniem
- Nieodłączanie urządzenia, gdy świeci się jego dioda LED. Może to spowodować uszkodzenie pamięci wymagające ponownego sformatowania, co będzie skutkować usunięciem danych
- Nieudostępnianie nikomu hasła

### 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 VP50 ma silne zabezpieczenia. Obejmuje to ochronę przed atakami typu Brute Force, która uniemożliwia napastnikom odgadywanie haseł dzięki ograniczeniu liczby prób wprowadzenia hasła do 10. Po osiągnięciu tego limitu pamięć VP50 automatycznie wymaże zaszyfrowane dane, formatując się z powrotem do stanu fabrycznego.

**Wiele haseł (funkcja Multi-Password)**
Jedną z głównych funkcji funkcji pamięci VP50 jest obsługa wielu haseł, która pomaga chronić przed utratą danych w przypadku zapomnienia jednego lub więcej haseł. Gdy wszystkie opcje haseł są włączone, pamięć VP50 może obsługiwać trzy różne hasła, które można wykorzystać do odzyskania danych – hasło administratora, użytkownika oraz jednorazowe hasło odzyskiwania.

Pamięć VP50 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". Ponadto Administrator może skonfigurować jednorazowe hasło odzyskiwania dla użytkownika, aby umożliwić użytkownikowi zalogowanie się i zresetowanie hasła użytkownika.

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

W przypadku zapomnienia lub utraty wszystkich haseł nie będzie możliwe uzyskanie dostępu do danych. Firma Kingston nie będzie w stanie odzyskać danych, ponieważ zastosowany mechanizm zabezpieczenia nie ma obejścia. Firma Kingston zaleca zapisywanie danych również na innych nośnikach. Pamięć VP50 można bezpiecznie wymazać w celu ponownego wykorzystania, ale znajdujące się w niej dane zostaną bezpowrotnie usunięte.

**Tryby hasła**
Pamięć VP50 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 VP50 obsługuje wyrażenia hasłowe o długości od 10 do 64 znaków. Wyrażenie hasłowe nie podlega żadnym 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 VP50. 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, podłącz ją bezpośrednio do portu USB 2.0/3.0 w notebooku lub komputerze stacjonarnym. Unikaj podłączania go 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.

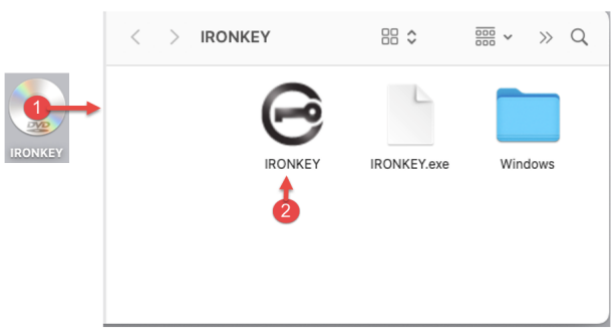
### Dostęp do urządzenia (środowisko Windows)

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). |  <br>**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).<br><br>• 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 poniższej ilustracji literą dysku jest litera (E:). |  <br>**Ilustracja 3.2 – Okno Eksploratora plików/IronKey.exe** |

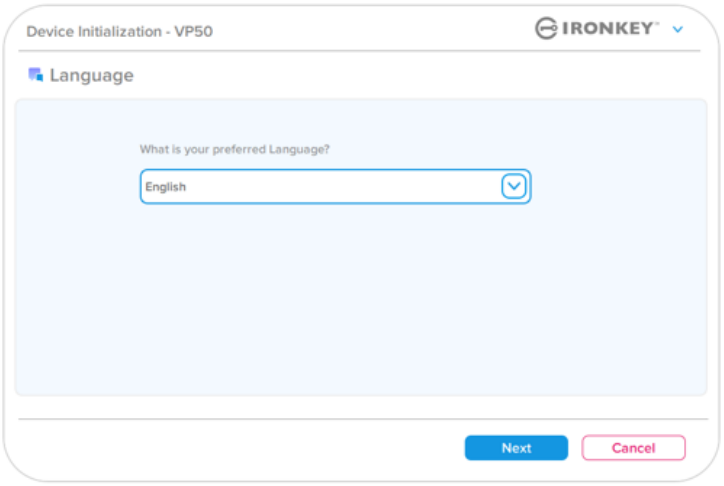
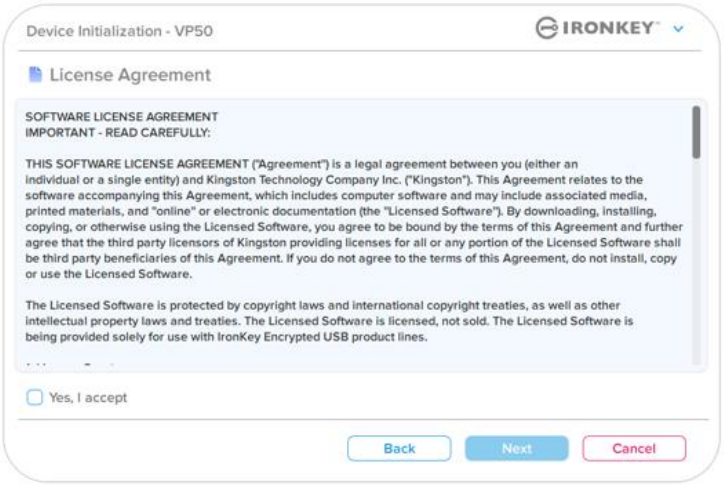
### Dostęp do urządzenia (środowisko macOS)

Włóż pamięć VP50 do dostępnego portu w notebooku lub komputerze stacjonarnym i zaczekaj, aż wykryje ją system operacyjny komputera Mac. Po wykryciu pamięci na pulpicie zostanie wyświetlony wolumin IKVP50 (lub IRONKEY) (ilustracja 3.3).

| | |
|---|---|
| • Kliknij dwukrotnie ikonę CD-ROM IronKey.<br><br>• Następnie kliknij dwukrotnie ikonę aplikacji IKVP50 (lub IronKey.app) widoczną w oknie pokazanym na ilustracji 3.3. Spowoduje to rozpoczęcie procesu inicjalizacji. |  <br>**Ilustracja 3.3 – wolumin IKVP** |

## Inicjalizacja 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). |  <br>**Ilustracja 4.1 – Wybór języka** |
| Zapoznaj się z umową licencyjną i kliknij przycisk **Next (Dalej)**.<br><br>Uwaga: Aby kontynuować należy zaakceptować umowę licencyjną; w przeciwnym razie przycisk **Next (Dalej)** pozostanie nieaktywny (ilustracja 4.2). |  <br>**Ilustracja 4.2 – Umowa licencyjna** |

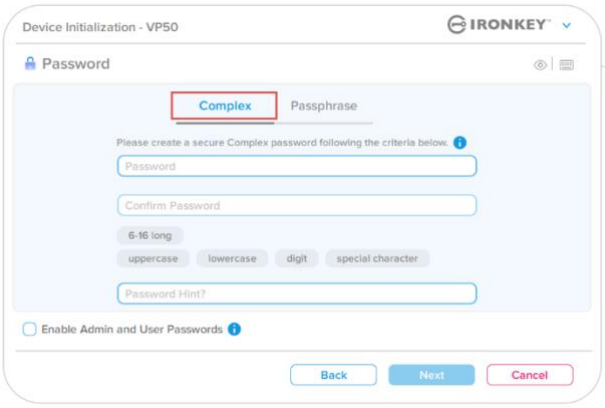
## Inicjalizacja urządzenia

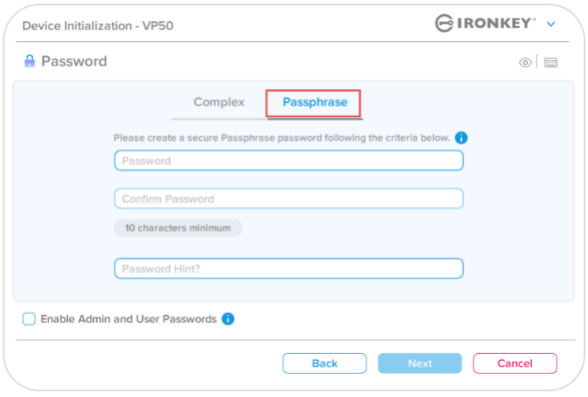
### Wybór hasła

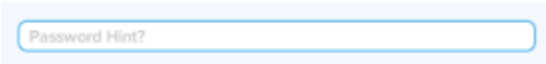
Na ekranie monitu o podanie hasła można utworzyć hasło do ochrony danych zapisanych w pamięci VP50, korzystając z trybu hasła złożonego lub wyrażenia hasłowego (ilustracje 4.3-4.4). Ponadto na tym ekranie można również włączyć opcje wielu haseł administratora/użytkownika. Zanim przejdziesz do wyboru 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 możliwa była kontynuacja procesu inicjalizacji:

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

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

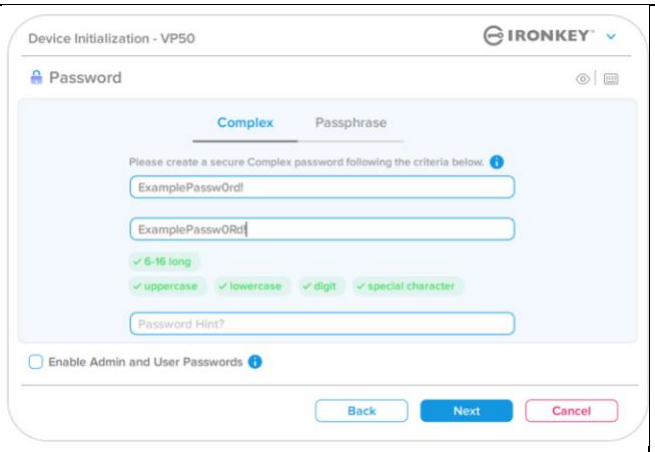
Ilustracja 4.4 – Wyrażenie hasłowe</td>
</tr>
<tr>
<td>Podpowiedź hasła (opcjonalnie)<br>Podpowiedź hasła może być pomocna w przypomnieniu sobie zapomnianego hasła.<br>Uwaga: Podpowiedź NIE MOŻE być taka sama jak hasło.</td>
<td> 

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

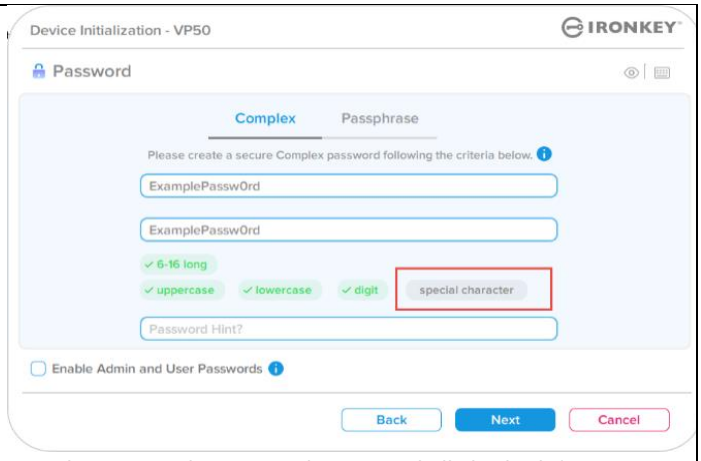
## Inicjalizacja urządzenia

### Prawidłowe i nieprawidłowe hasła

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



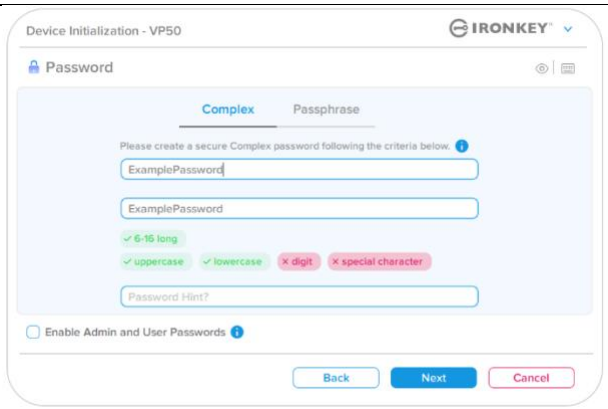

**Ilustracja 4.6a – Spełnione warunki dla hasła złożonego**




**Ilustracja 4.6b – Opcjonalny warunek dla hasła złożonego**

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

Dotyczy to zarówno haseł złożonych, jak i wyrażeń hasłowych.



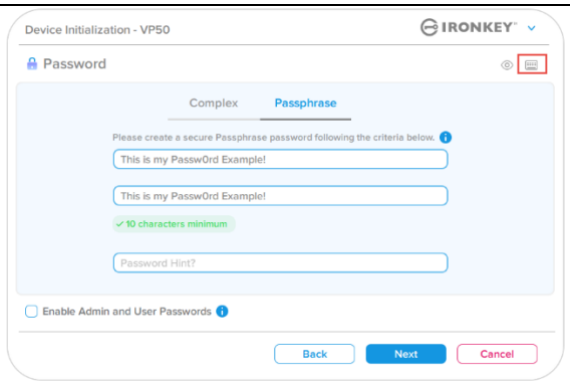

**Ilustracja 4.7 – Niespełnione warunki dla hasła**

## Inicjalizacja urządzenia

### Wirtualna klawiatura

Pamięć VP50 jest wyposażona w funkcję wirtualnej klawiatury, która może służyć do ochrony przed keyloggerami.

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




**Ilustracja 4.8 – Aktywacja wirtualnej klawiatury**

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

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

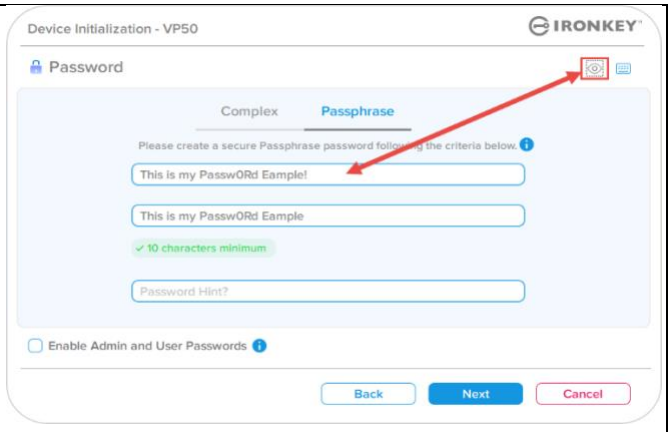
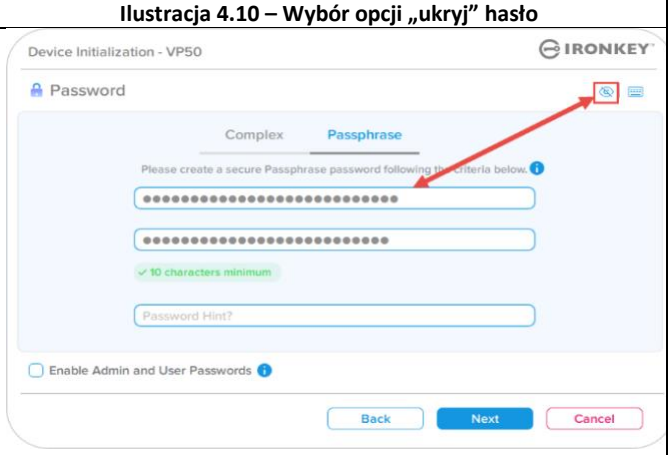

**Ilustracja 4.9 – Ochrona przed screenloggerami / randomizacja**

## Inicjalizacja urządzenia

### Przełącznik widoczności hasła

Domyślnie podczas tworzenia hasła (jego wpisywania) ciąg znaków 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** |

## Inicjalizacja 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.

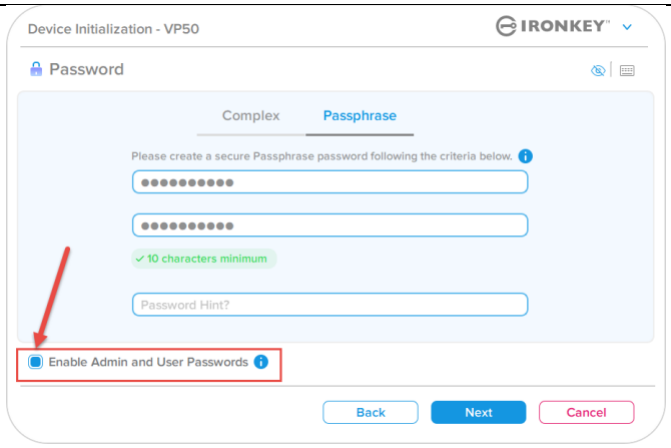
Gdy **hasła administratora i użytkownika** są włączone, można również uzyskać dostęp do następujących funkcji:

- Jednorazowe hasło odzyskiwania
- Wymuszony tryb tylko do odczytu dla logowania użytkownika
- Resetowanie hasła użytkownika
- Wymuszone resetowanie hasła dla logowania użytkownika

Aby dowiedzieć się więcej o tych funkcjach, przejdź na stronę 25 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 ta funkcja jest **włączona**, hasło wybrane na tym ekranie będzie **hasłem administratora**. Kliknij przycisk **Next (Dalej)**, aby przejść do ekranu **hasła użytkownika** i zdefiniować hasło dla użytkownika.




**Ilustracja 4.12 – Włączanie hasła 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**.

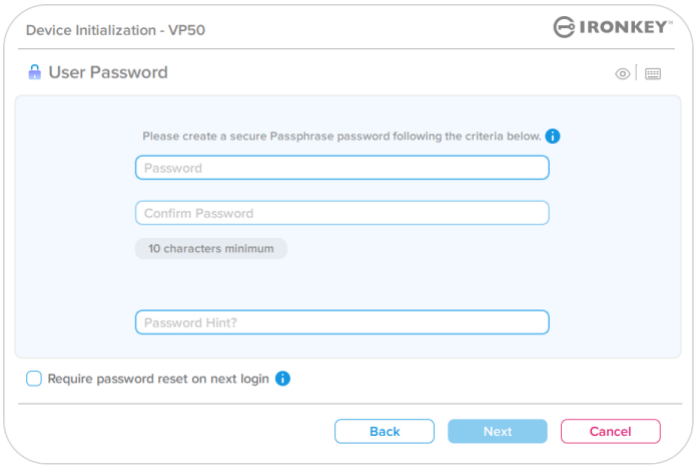
Aby kontynuować konfigurację dla pojedynczego użytkownika z jednym hasłem, pozostaw niezaznaczoną opcję **Enable Admin and User Passwords (Włącz hasła administratora i użytkownika)** i po utworzeniu prawidłowego hasła kliknij przycisk **Next (Dalej)**.

**Uwaga:** W dalszej części tego dokumentu tryb z włączonymi **hasłami administratora i użytkownika** będzie określany jako **rola administratora**.

## Inicjalizacja urządzenia

### Hasła administratora i użytkownika

- Jeśli rola administratora została **włączona** na poprzednim ekranie, na następnym ekranie pojawi się monit o podanie **hasła użytkownika** (ilustracja 4.13). Hasło użytkownika zapewnia ograniczone uprawnienia w porównaniu z hasłem administratora, co zostanie szczegółowo omówione w dalszej części niniejszej instrukcji obsługi (patrz strona 23).

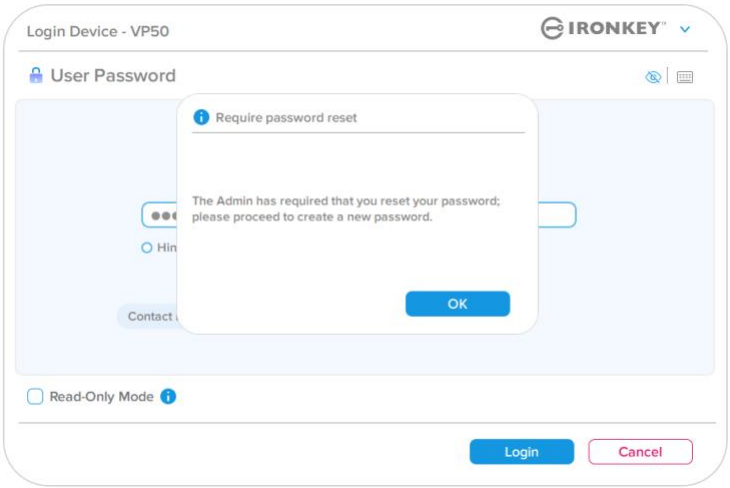



**Ilustracja 4.13 – Hasło użytkownika (włączone hasła administratora i użytkownika)**

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

- Funkcja **Require password reset on next login (Wymagaj zresetowania hasła przy następnym logowaniu)**, widoczna w lewym dolnym rogu **ilustracji 4.13**, dotyczy tylko hasła użytkownika i można ją włączyć, aby wymusić na użytkowniku zalogowanie się przy użyciu tymczasowego hasła ustawionego przez administratora podczas procesu inicjalizacji, a następnie do jego zmiany na wybrane przez siebie hasło po uwierzytelnieniu pamięci przy użyciu hasła tymczasowego. Jest to przydatne, gdy pamięć jest przekazywana do użytkowania innej osobie **(ilustracja 4.14)**.

  **Uwaga:** Ze względów bezpieczeństwa nowe hasło nie może być takie samo jak hasło tymczasowe.



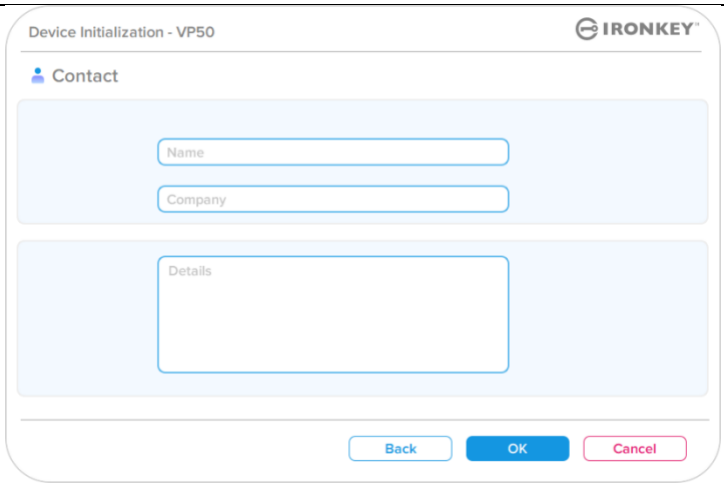

**4.14 – Wymaganie zresetowania hasła przy następnym logowaniu (dla hasła użytkownika)**

## Inicjalizacja urządzenia

### Informacje kontaktowe

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

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

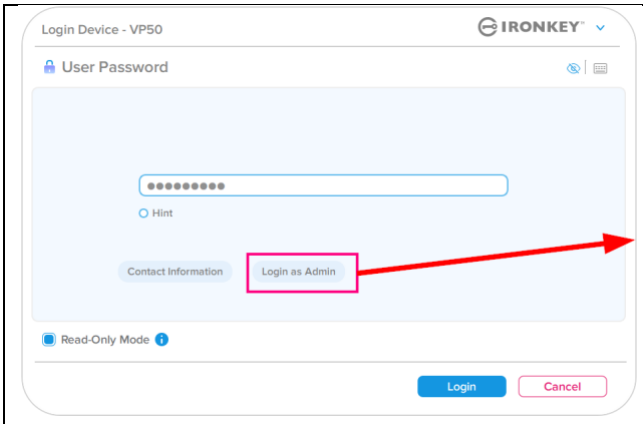
| | |
|---|---|
| Pole **Name (Nazwa)** może zawierać do 32 znaków, ale nie może zawierać **samego** hasła.<br><br>Pole **Company (Firma)** może zawierać do 32 znaków, ale nie może zawierać **samego** hasła.<br><br>Pole **Details (Szczegóły)** może zawierać do 156 znaków, ale nie może zawierać **samego** hasła. |  <br>**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.

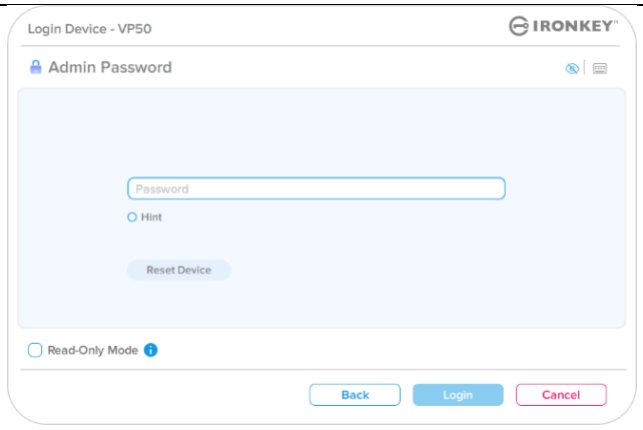
## Korzystanie z urządzenia (środowisko Windows i macOS)

### Logowanie administratora i użytkownika (włączony tryb administratora)

Jeśli urządzenie zostało zainicjowane z włączonymi hasłami administratora i użytkownika (rola administratora), nastąpi uruchomienie aplikacji IronKey VP50 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 5.1). 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 5.2).




**Ilustracja 5.1 – Logowanie za pomocą hasła użytkownika (włączony tryb administratora)**

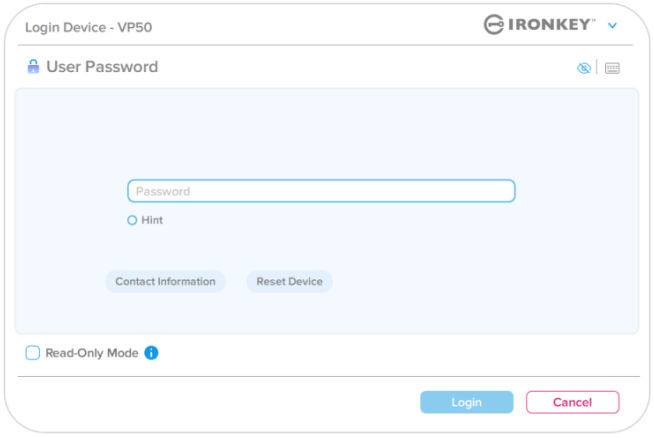



**Ilustracja 5.2 – Logowanie za pomocą hasła administratora**

### 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 zainicjalizować 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 5.3).

**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 5.3 – Logowanie za pomocą hasła użytkownika (wyłączony tryb administratora)**

| | |
|---|---|
| | |

## Korzystanie z urządzenia

### Odblokowywanie w trybie tylko do odczytu

Aby uniknąć omyłkowego wprowadzenia zmian w plikach zapisanych w pamięci IronKey, można odblokować urządzenie w trybie tylko do odczytu. Na przykład w przypadku korzystania z niezaufanego lub nieznanego komputera odblokowanie urządzenia w trybie tylko do odczytu uniemożliwi złośliwemu oprogramowaniu z tego komputera zainfekowanie urządzenia lub zmodyfikowanie plików.

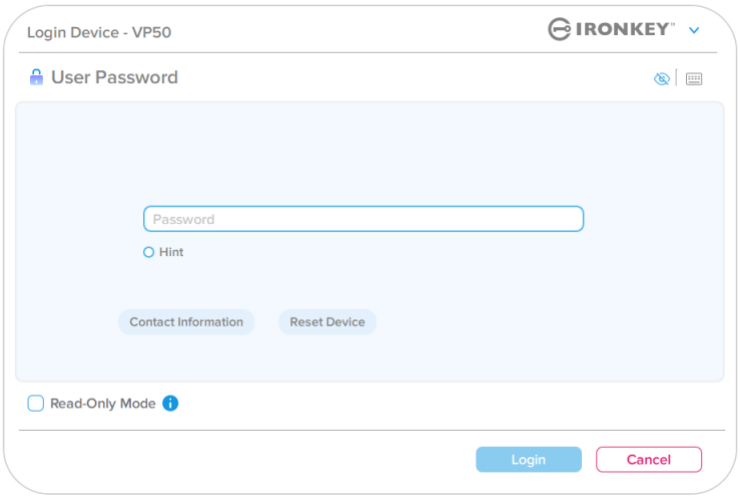
Podczas pracy w tym trybie nie można wykonywać żadnych operacji związanych z modyfikacją plików zapisanych w urządzeniu.
Nie można np. ponownie sformatować urządzenia ani przywracać, dodawać lub edytować plików zapisanych w pamięci.

Aby odblokować urządzenie w trybie tylko do odczytu:

1. Włóż urządzenie do portu USB komputera-hosta i uruchom program **IronKey.exe**.

2. Zaznacz pole wyboru opcji **Read-Only Mode (Tryb tylko do odczytu)** poniżej pola wprowadzania hasła **(ilustracja 5.4)**.

3. Wpisz swoje hasło do urządzenia i kliknij przycisk **Login (Zaloguj się)**. Pamięć IronKey zostanie odblokowana w trybie tylko do odczytu.




**Ilustracja 5.4 – Tryb tylko do odczytu**

Aby odblokować urządzenie z pełnymi uprawnieniami do odczytu/zapisu na bezpiecznej partycji danych należy odłączyć pamięć VP50 i zalogować się ponownie, usuwając zaznaczenie pola wyboru opcji Read-Only Mode (Tryb tylko do odczytu).

**Uwaga:** Opcje administratora pamięci VP50 obejmują wymuszony tryb tylko do odczytu dla danych użytkownika, co oznacza, że administrator może wymusić logowanie użytkownika w trybie tylko do odczytu (szczegółowe informacje – patrz **strona 28**).

## Korzystanie z urządzenia

### Ochrona hasła przed atakami typu 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 typu 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 typu Brute Force Zachowanie urządzenia (10 nieudanych prób wprowadzenia hasła)** | **Wymazanie danych i zresetowanie urządzenia** |
|---|---|---|
| Hasło użytkownika | Blokada hasła. Zaloguj się jako administrator lub użyj jednorazowego hasła odzyskiwania, aby zresetować hasło użytkownika | NIE (No) |
| Hasło administratora | Bezpowrotne wymazanie metodą kryptograficzną pamięci, haseł, ustawień i danych | **TAK (Yes)** |
| Jednorazowe hasło odzyskiwania | Blokada hasła, przycisk hasła odzyskiwania zostanie wyszarzony i stanie się nieaktywny. Zaloguj się jako administrator, aby zresetować hasło | NIE (No) |
| **Tylko użytkownik Jeden użytkownik, jedno hasło (WYŁĄCZONY tryb administratora/użytkownika)** | **Ochrona przed atakami typu 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 (Yes)** |

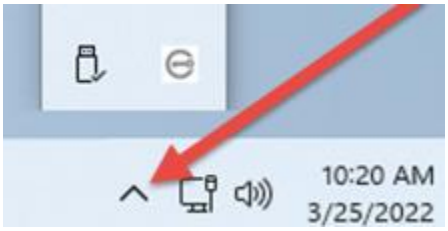
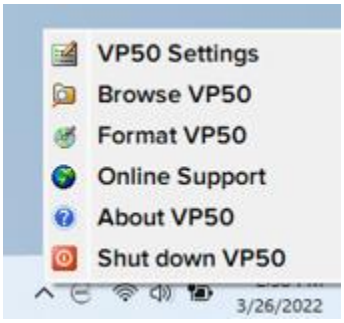
* Po pomyślnym uwierzytelnieniu użytkownika licznik nieudanych logowań jest resetowany odpowiednio dla użytej metody logowania. Funkcja Crypto-Erase usunie wszystkie hasła, klucze szyfrowania i dane – **zostaną one bezpowrotnie utracone**.

### Uzyskiwanie dostępu do zabezpieczonych plików

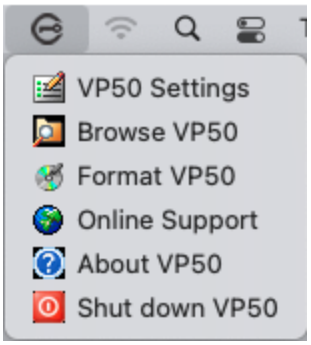
Po odblokowaniu urządzenia uzyskasz dostęp do zabezpieczonych plików. Pliki są automatycznie szyfrowane i odszyfrowywane, gdy zapisujesz lub otwierasz je w pamięci. Technologia ta pozwala na wygodną pracę, tak jak w przypadku zwykłej pamięci, zapewniając jednocześnie silne, „zawsze włączone” zabezpieczenia.
**Wskazówka:** możesz również uzyskać dostęp do plików, klikając prawym przyciskiem myszy **ikonę IronKey** na pasku zadań systemu Windows, a następnie klikając opcję **Browse VP50 (Przeglądanie zawartości pamięci VP50)** (ilustracja 6.2).

## Opcje urządzenia – środowisko Windows

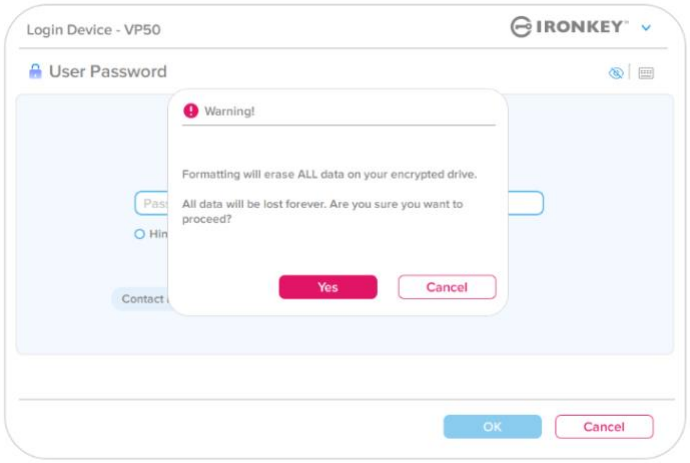
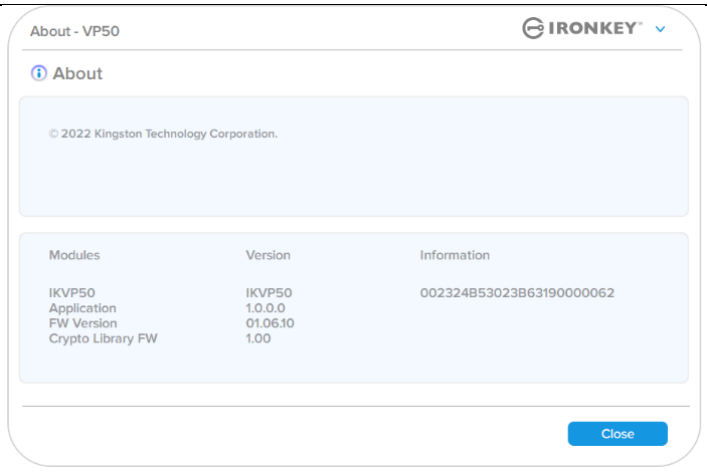
Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey. Kliknięcie prawym przyciskiem myszy ikony IronKey spowoduje otwarcie menu wyboru dostępnych opcji pamięci (ilustracja 6.2). Szczegółowe informacje na temat tych opcji urządzenia można znaleźć na str. 19-23 niniejszej instrukcji.

| | |
|---|---|
| • Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey **(ilustracja 6.1).** |  **Ilustracja 6.1 – Ikona IronKey na pasku zadań** |
| • Kliknięcie prawym przyciskiem myszy ikony IronKey spowoduje otwarcie menu wyboru dostępnych opcji pamięci **(ilustracja 6.2).**<br><br>Szczegółowe informacje na temat tych opcji urządzenia można znaleźć na str. 19-23 niniejszej instrukcji. |  **Ilustracja 6.2 – 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 VP50 (patrz **ilustracja 6.3**), której kliknięcie powoduje wyświetlenie dostępnych opcji urządzenia.<br><br>Szczegółowe informacje na temat tych opcji urządzenia można znaleźć na str. 19-23 niniejszej instrukcji. |  **Ilustracja 6.3 – Ikona na pasku menu systemu macOS / menu opcji urządzenia** |

## Opcje urządzenia

| | |
|---|---|
| **VP50 Settings (Ustawienia pamięci VP50):** | • Zmiana hasła logowania, informacji kontaktowych i innych ustawień. (Więcej informacji na temat ustawień urządzenia można znaleźć w części „Ustawienia pamięci VP50" niniejszej instrukcji). |
| **Browse VP50 (Przeglądanie zawartości pamięci VP50):** | • Umożliwia przeglądanie bezpiecznych plików. |
| **Format VP50 (Formatowanie pamięci VP50):**<br>Umożliwia sformatowanie zabezpieczonej partycji danych. (Ostrzeżenie: wszystkie dane zostaną usunięte) (**ilustracja 6.1**)<br><br>**Uwaga:** Do formatowania wymagane jest uwierzytelnienie hasłem. |  <br>**Ilustracja 6.1 – Formatowanie pamięci VP50** |
| **Online Support (Pomoc techniczna online):** | • Umożliwia otwarcie przeglądarki internetowej i przejście na stronę http://www.kingston.com/support, gdzie dostępne są dodatkowe informacje. |
| **About VP50 (Informacje o pamięci VP50):**<br>Dostęp do szczegółowych informacji na temat pamięci VP50, w tym informacji o aplikacji, oprogramowaniu sprzętowym i numerze seryjnym (**ilustracja 6.2**).<br><br>**Uwaga:** Unikalny numer seryjny znajduje się w kolumnie „Informacje". |  <br>**Ilustracja 6.2 – Informacje o pamięci VP50** |
| **Shut down VP50 (Wyłączenie pamięci VP50):** | • Umożliwia prawidłowe wyłączenie pamięci VP50, co pozwala na jej bezpieczne odłączenie od komputera. |

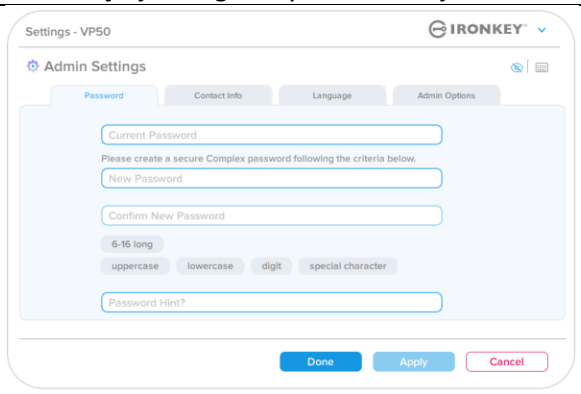
## Ustawienia pamięci VP50

### Ustawienia administratora

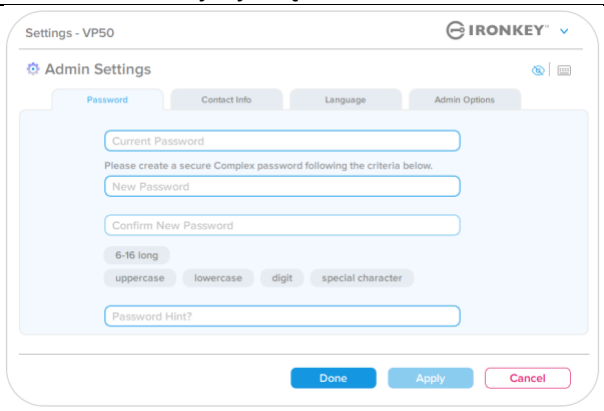
Zalogowanie się jako administrator umożliwia dostęp do następujących ustawień urządzenia:

- **Password (Hasło):** Umożliwia zmianę hasła i lub podpowiedzi do hasła administratora (*ilustracja 7.1*).
- **Contact Info (Informacje kontaktowe):** Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 7.2*).
- **Language (Język):** Umożliwia zmianę aktualnie wybranego języka (*ilustracja 7.3*).
- **Admin Options (Opcje administratora):** Umożliwia włączenie dodatkowych funkcji, takich jak (ilustracja 7.4):
    - Zmiana hasła użytkownika
    - Resetowanie hasła logowania (dla hasła użytkownika)
    - Jednorazowe hasło odzyskiwania
    - Wymuszony tryb tylko do odczytu dla danych użytkownika

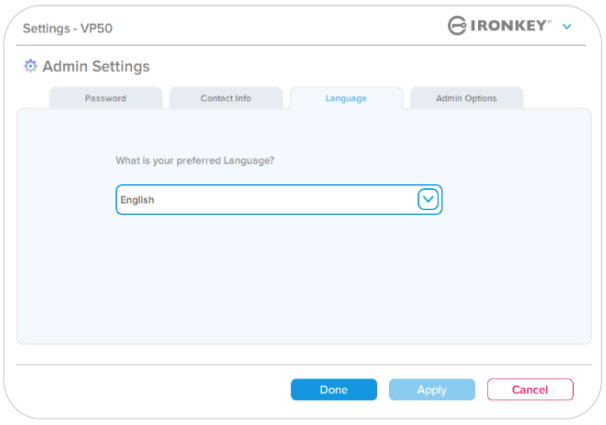
**UWAGA:** Więcej szczegółowych informacji na temat opcji administratora znajduje się na stronie 24.



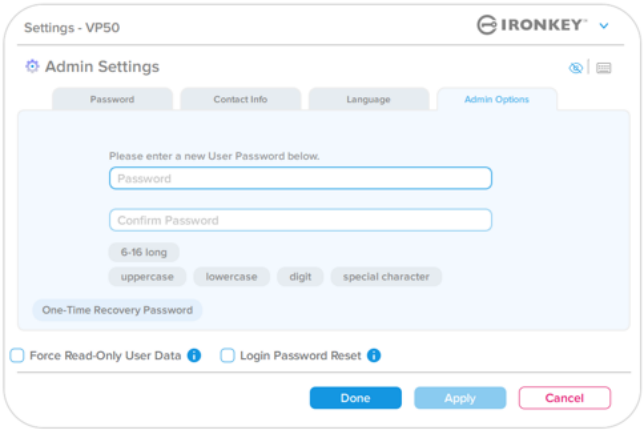

**Ilustracja 7.1 – Opcje hasła**




**Ilustracja 7.2 – Informacje kontaktowe**




**Ilustracja 7.3 – Opcje języka**



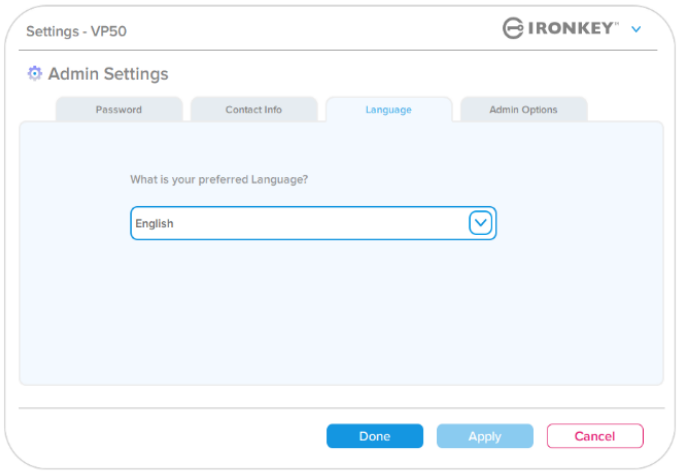

**Ilustracja 7.4 – Opcje administratora**

## Ustawienia pamięci VP50

### Ustawienia użytkownika: włączony tryb administratora

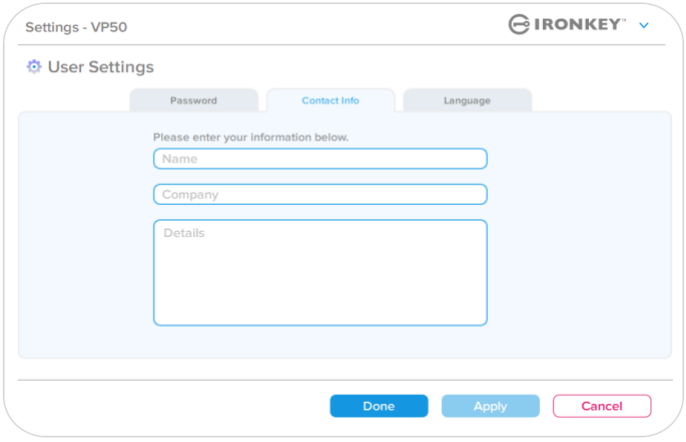
Zalogowanie się jako użytkownik powoduje ograniczenie dostępu do następujących ustawień:

**Password (Hasło):**
Umożliwia zmianę hasła i/lub podpowiedzi do hasła użytkownika (*ilustracja 7.5*).



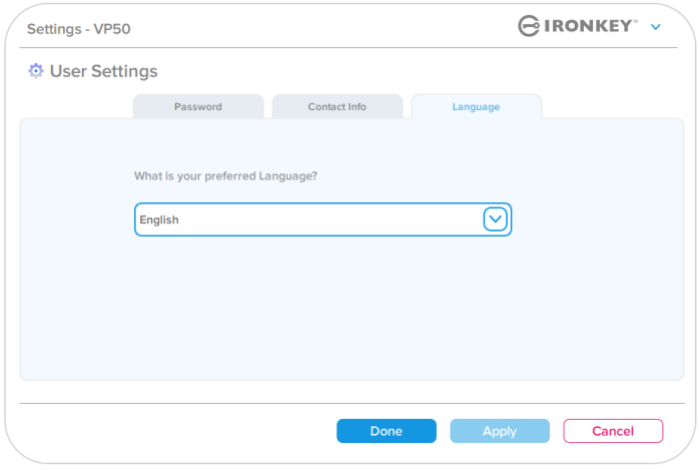

**Ilustracja 7.5 – Opcje hasła (włączony tryb administratora: logowanie użytkownika)**

**Contact Info (Informacje kontaktowe):**
Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 7.6*).




**Ilustracja 7.6 – Informacje kontaktowe (włączony tryb administratora: logowanie użytkownika)**

**Language (Język):**
Umożliwia zmianę aktualnie wybranego języka (*ilustracja 7.7*).




**Ilustracja 7.7 – Ustawienia języka (włączony tryb administratora: logowanie użytkownika)**

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

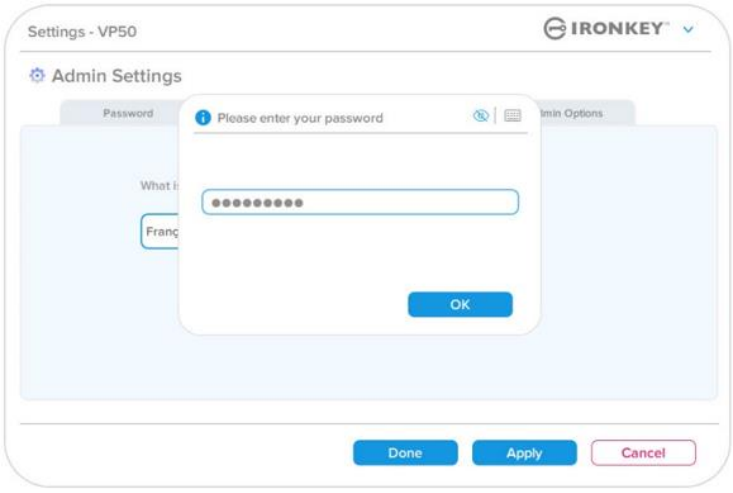
## Ustawienia pamięci VP50

### Ustawienia użytkownika: tryb administratora nie jest włączony

Jak wspomniano wcześniej na stronie 12, inicjalizacja pamięci VP50 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 VP50:

### Zmiana i zapisywanie ustawień

- Po każdej zmianie ustawień pamięci VP50 (np. informacji kontaktowych, języka, hasła, opcji administratora itp.) pamięć wyświetli monit o wprowadzenie hasła w celu zaakceptowania i zastosowania zmian (patrz ilustracja 7.11).

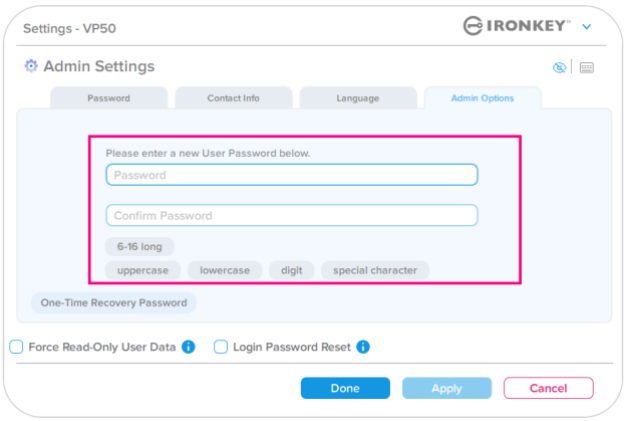
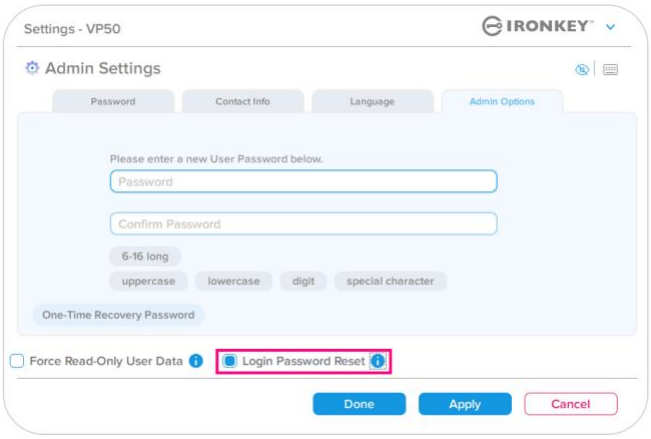


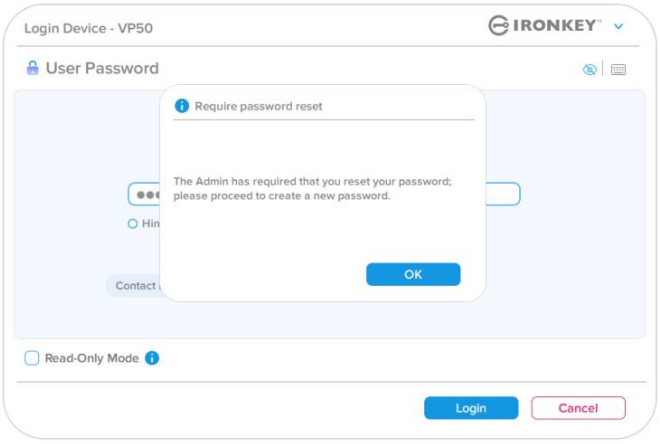

**Ilustracja 7.11 – Ekran monitu o podanie hasła w celu zapisania zmiany ustawień pamięci VP50**

**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 VP50.

## Funkcje administracyjne

**Dostępne opcje resetowania hasła użytkownika**
Funkcje konfiguracji administratora zapewniają wiele możliwości bezpiecznego zresetowania hasła użytkownika, jeśli zostanie ono zapomniane lub jeśli zostanie utworzone tymczasowe hasło użytkownika i administrator będzie chciał wymusić zmianę hasła przy następnym logowaniu użytkownika. Poniżej omówiono funkcje, które mogą być pomocne w zresetowaniu hasła użytkownika:

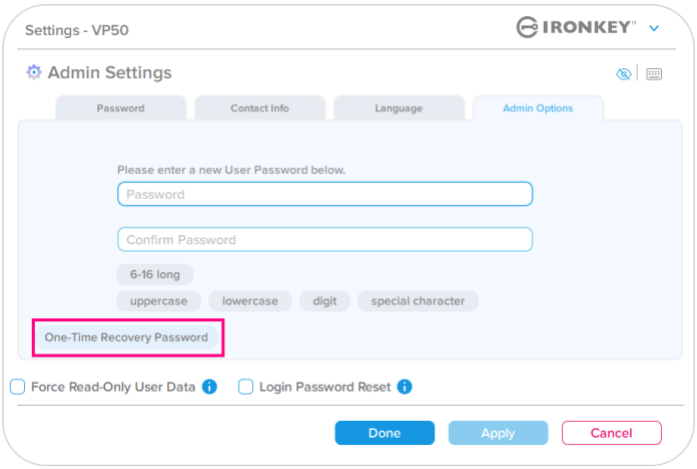
| | |
|---|---|
| **Resetowanie hasła użytkownika:**<br>Zmień ręcznie zmień hasło użytkownika w menu „Admin Options" (Opcje administratora) – zmiana będzie natychmiastowa i zacznie obowiązywać przy następnym logowaniu użytkownika **(ilustracja 8.1).**<br><br>**Uwaga:** Kryteria wymagań dla hasła zostaną domyślnie ustawione na pierwotne kryteria, które zostały ustawione podczas procesu inicjalizacji (opcje hasła złożonego lub wyrażenia hasłowego). |  <br>**Ilustracja 8.1 – Opcje administratora / resetowanie hasła użytkownika** |
| **Resetowanie hasła do logowania:**<br>Włączenie opcji resetowania hasła do logowania **wymusi na użytkowniku zalogowanie się przy użyciu hasła tymczasowego określonego przez administratora**, a następnie jego zmianę na hasło wybrane przez użytkownika. Jest to przydatne, gdy pamięć jest przekazywana do użytkowania innej osobie **(patrz ilustracje 8.2A i 8.2B)**. |  <br>**Ilustracja 8.2A – Przycisk resetowania haseł logowania** |

| | |
|---|---|
| **Uwaga:** Zresetowanie nastąpi po kolejnym udanym zalogowaniu się użytkownika. Kryteria wymagań dla hasła zostaną automatycznie zastosowane zgodnie z pierwotnym ustawieniem podczas procesu inicjalizacji (opcje hasła złożonego lub wyrażenia hasłowego). |  **Ilustracja 8.2B – Powiadomienie o zresetowaniu po wprowadzeniu hasła użytkownika** |

## Funkcje administracyjne

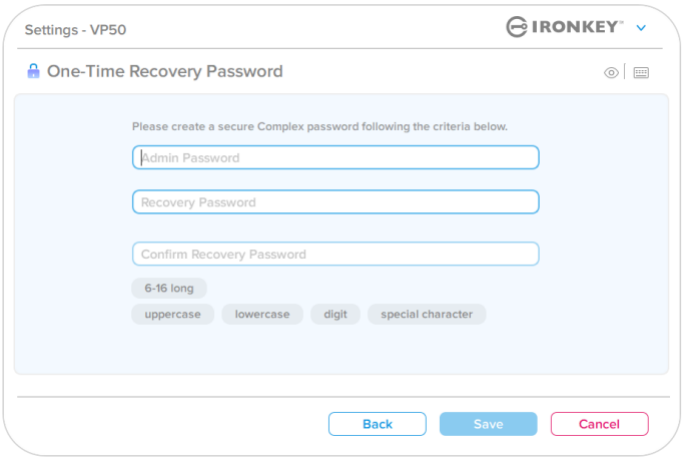
### Jednorazowe hasło odzyskiwania

W tej części omówiono proces włączania i używania funkcji jednorazowego hasła odzyskiwania.

| | |
|---|---|
| **Jednorazowe hasło odzyskiwania**<br><br>**Krok 1:** Funkcja jednorazowego hasła odzyskiwania to bardzo przydatna funkcja, którą można włączyć, aby pomóc odzyskać i zresetować hasło użytkownika w przypadku jego zapomnienia. Aby rozpocząć, kliknij przycisk „One-Time Recovery Password” (Jednorazowe hasło odzyskiwania) w menu opcji administratora **(ilustracja 8.4).** |  **Ilustracja 8.4 – Przycisk jednorazowego hasła odzyskiwania** |

**Krok 2:** Utwórz jednorazowe hasło odzyskiwania, korzystając z tych samych kryteriów hasła, które zostały początkowo ustawione na urządzeniu (hasło złożone lub wyrażenie hasłowe).

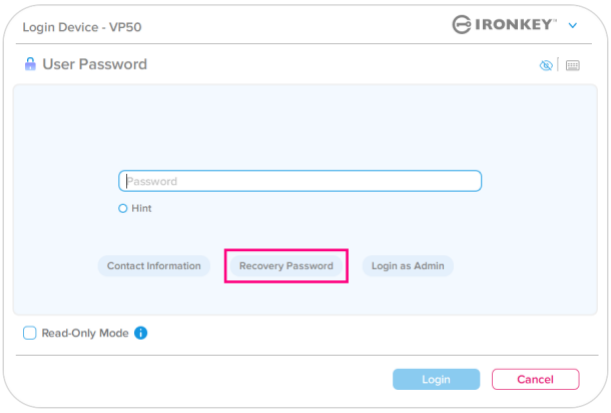
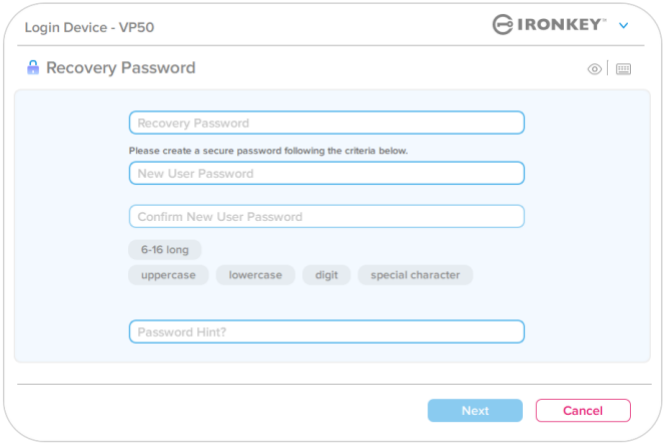
**Uwaga:** Do wprowadzenia zmian będzie wymagane hasło administratora.

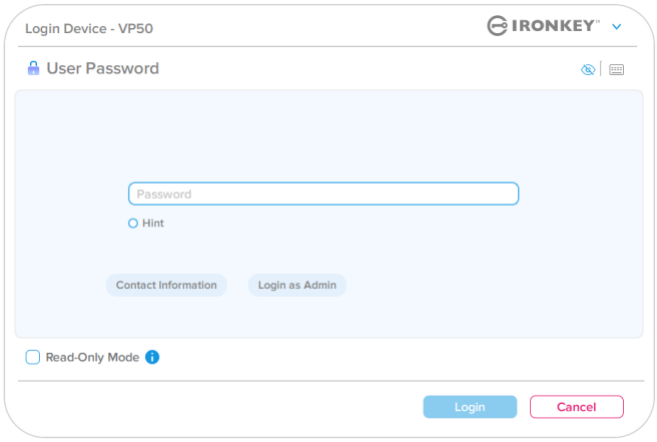



**Ilustracja 8.5 – Konfiguracja jednorazowego hasła odzyskiwania**

## Funkcje administracyjne

Korzystanie z jednorazowego hasła odzyskiwania

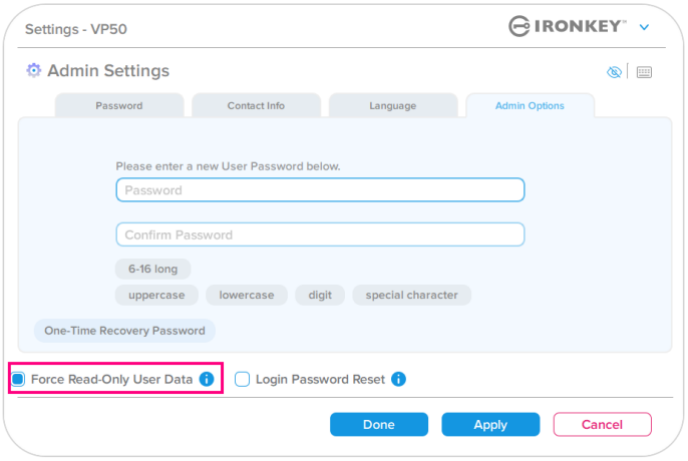
| | |
|---|---|
| **Krok 1:** Po utworzeniu jednorazowego hasła odzyskiwania, przy następnym logowaniu na ekranie logowania **User Password (Hasło użytkownika)** pojawi się nowy przycisk. Kliknij przycisk **Recovery Password (Hasło odzyskiwania)**, aby rozpocząć proces. |  <br>**Ilustracja 8.6 – Przycisk hasła odzyskiwania** |
| **Krok 2:** Wyświetli się ekran **Recovery Password (Hasło odzyskiwania)**, na którym można wprowadzić hasło odzyskiwania i utworzyć nowe hasło użytkownika (ilustracja 8.7).<br><br>**Ważne:** Jednorazowe hasło odzyskiwania wykorzystuje również wbudowaną funkcję bezpieczeństwa, która śledzi liczbę nieudanych prób logowania. **Po 10 nieudanych próbach zalogowania się za pomocą jednorazowego hasła odzyskiwania, hasło zostanie wyłączone** i konieczne będzie jego ponownie włączenie poprzez zalogowanie się do pamięci w roli administratora (więcej szczegółowych informacji podano na str. 18 i 30). |  <br>**Ilustracja 8.7 – Menu hasła odzyskiwania** |

| | |
|---|---|
| **Krok 3:** Po pomyślnej zmianie hasła zostanie ponownie wyświetlony ekran **User Password (Hasło użytkownika)**. Przycisk **Recovery Password (Hasło odzyskiwania)** zniknie, a hasło użytkownika wprowadzone w **kroku 2** stanie się nowym hasłem użytkownika (ilustracja 8.8). |  **Ilustracja 8.8 – Ekran logowania za pomocą hasła użytkownika bez widocznego przycisku odzyskiwania hasła po jego pomyślnym użyciu.** |

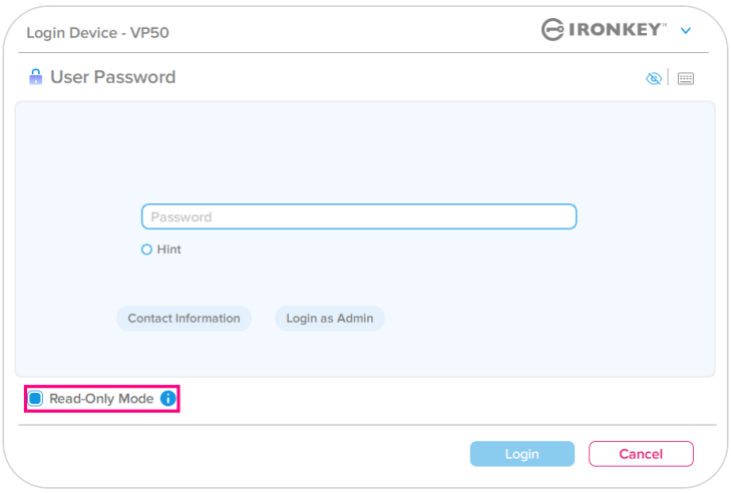
## Funkcje administracyjne

### Wymuszenie danych użytkownika tylko do odczytu

Aby uniemożliwić dostęp do pamięci w celu zapisu, można włączyć dla użytkownika wymuszony tryb tylko do odczytu. Funkcja ta jest przydatna, jeśli pliki w pamięci są potrzebne tylko do odczytu.

| | |
|---|---|
| • Aby włączyć wymuszony tryb tylko do odczytu dla danych użytkownika, kliknij odpowiednie pole, a następnie przycisk „Apply” (Zastosuj) **(ilustracja 8.9).**<br><br>**Uwaga:** Wymuszony tryb tylko do odczytu dotyczy wyłącznie użytkownika i nie ma wpływu na logowanie administratora. Administrator nadal będzie miał uprawnienia dostępu do odczytu i zapisu, a w razie potrzeby nadal będzie mógł włączyć tryb tylko do odczytu. |  **Ilustracja 8.9 – Włączenie opcji „Force Read-Only User Data” (Wymuś dane użytkownika tylko do odczytu) – do wprowadzenia zmian wymagane jest hasło administratora** |
| • Po włączeniu pole zaznaczenia **Read-Only Mode (Tryb tylko do odczytu)** będzie zaznaczone na niebiesko, co oznacza, że wymuszony tryb tylko do odczytu jest na stałe włączony dla hasła użytkownika, dopóki nie zostanie | |

wyłączony przez administratora (ilustracja 8.10).




**Ilustracja 8.10 – Tryb tylko do odczytu jest wymuszony dla użytkownika i może zostać wyłączony tylko przez administratora**

## Pomoc i rozwiązywanie problemów

### Blokada urządzenia

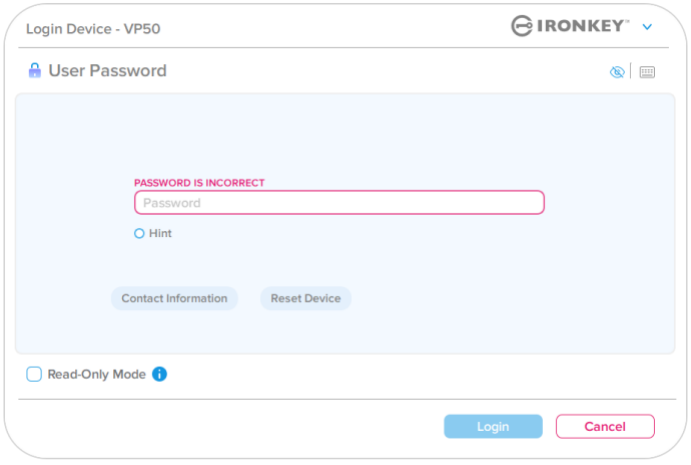
Pamięć VP50 jest wyposażona w funkcję bezpieczeństwa, która uniemożliwia nieuprawniony dostęp do partycji danych w przypadku osiągnięcia maksymalnej liczby **kolejnych** nieudanych prób zalogowania (w skrócie *MaxNoA*). W domyślnej fabrycznej konfiguracji ustawiona jest wartość 10 (liczba prób) dla każdej z metod logowania (administrator/użytkownik/jednorazowe hasło odzyskiwania).

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

**1.** Pomyślne logowanie przed osiągnięciem limitu MaxNoA.

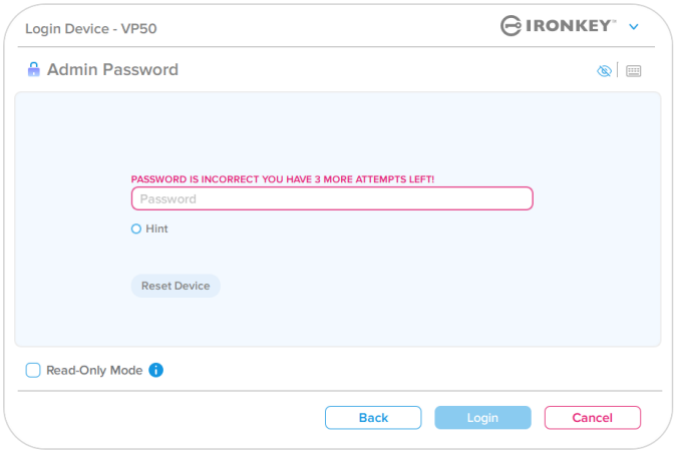
**2.** Osiągnięcie limitu MaxNoA i zablokowanie lub sformatowanie urządzenia, zależnie od konfiguracji pamięci.

- Jeśli zostanie wprowadzone nieprawidłowe hasło, tuż nad polem wprowadzania hasła pojawi się komunikat o błędzie w kolorze czerwonym, informujący o niepowodzeniu logowania (ilustracja 9.1).




**Ilustracja 9.1 – 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 9.2).




**Ilustracja 9.2 – Siódma nieudana próba wprowadzenia hasła**

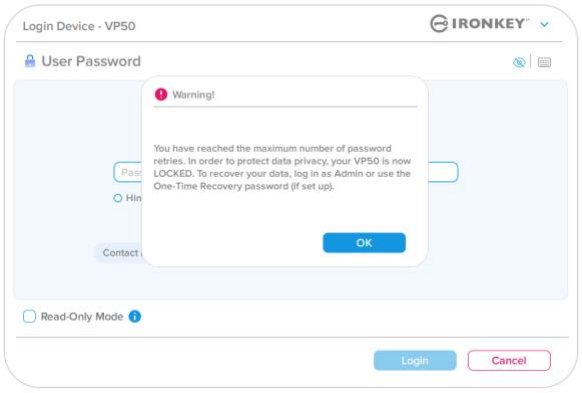
## Pomoc i rozwiązywanie problemów

### Blokada urządzenia

**Ważne:** Po **dziesiątej** i ostatniej nieudanej próbie logowania, w zależności od tego, jak zostało skonfigurowane urządzenie i jakiej użyto metody logowania (administrator, użytkownik lub jednorazowe hasło odzyskiwania), urządzenie zostanie zablokowane, co będzie wymagało zalogowania się inną metodą (jeśli dotyczy) lub zresetowania urządzenia, co spowoduje **sformatowanie danych i ich bezpowrotną utratę**. O tych zachowaniach urządzenia wspomniano również na stronie 18 niniejszej instrukcji obsługi.

Ilustracje 9.3-9.6 poniżej przedstawiają zachowanie urządzenia po dziesiątej i ostatniej nieudanej próbie logowania dla każdej z metod logowania:

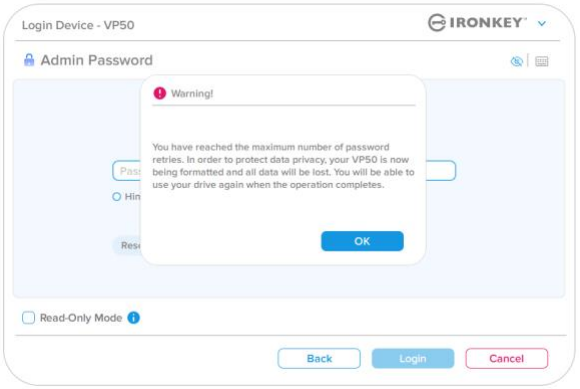
**Hasło użytkownika: (włączony tryb administratora/użytkownika)**




**BLOKADA URZĄDZENIA**

**(ilustracja 9.3)**

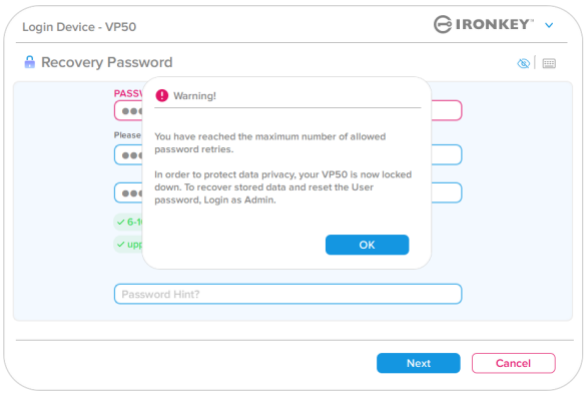
**Hasło administratora (włączony tryb administratora/użytkownika)**




**FORMATOWANIE URZĄDZENIA***

**(ilustracja 9.4)**

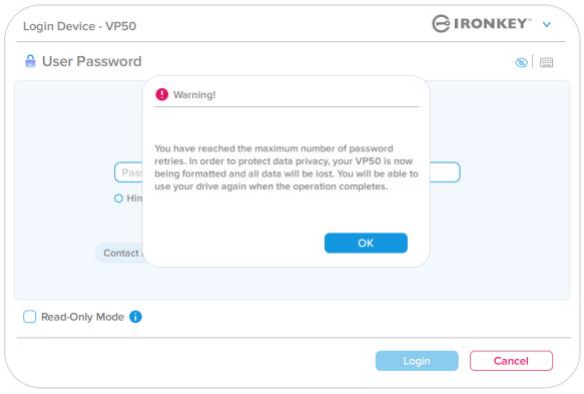
**Jednorazowe hasło odzyskiwania: (włączony tryb administratora/użytkownika)**




**BLOKADA URZĄDZENIA**

**(ilustracja 9.5)**

**Hasło użytkownika (WYŁĄCZONY tryb administratora)**




**FORMATOWANIE URZĄDZENIA***

**(ilustracja 9.6)**

Te zabezpieczenia mają na celu ograniczenie możliwości osobom, które nie znają hasła, podjęcia nieograniczonej liczby prób zalogowania i uzyskania dostępu do poufnych danych (tzw. atak metodą Brute-Force). Jeżeli właściciel pamięci VP50 zapomni hasła, zostaną zastosowane takie same środki bezpieczeństwa, w tym formatowanie

urządzenia. * Aby uzyskać więcej informacji dotyczących tej funkcji, przeczytaj rozdział *Resetowanie urządzenia* na stronie 25.

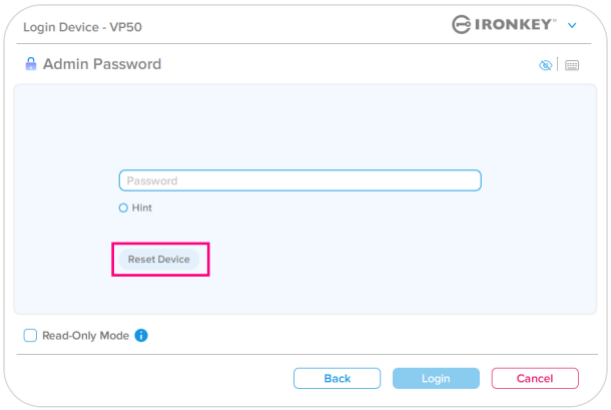
** Uwaga: Sformatowanie urządzenia spowoduje wymazanie WSZYSTKICH informacji przechowywanych na bezpiecznej partycji danych pamięci VP50.*

## Pomoc i rozwiązywanie problemów

### Resetowanie urządzenia

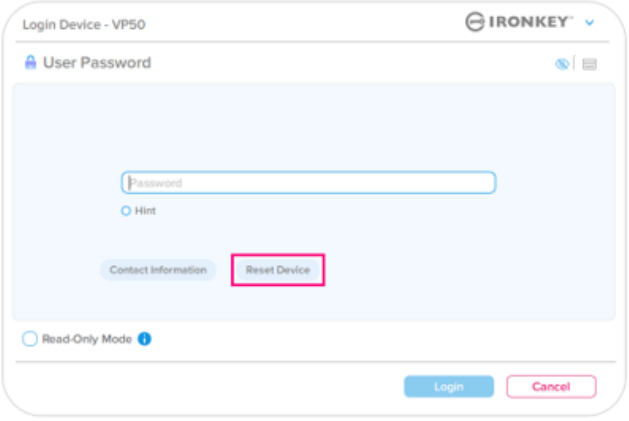
Jeśli zapomnisz hasło lub zechcesz zresetować urządzenie, możesz kliknąć przycisk *Reset Device* (Resetuj urządzenie), który pojawia się w jednym z dwóch miejsc, zależnie od konfiguracji urządzenia (w menu hasła logowania administratora, jeśli włączony jest tryb administratora/użytkownika, lub w menu hasła logowania użytkownika, jeśli tryb administratora/użytkownika jest wyłączony) podczas uruchamiania oprogramowania pamięci VP50 (patrz ***ilustracje 9.7*** i **9.8**).

- Ta opcja umożliwia utworzenie nowego hasła, ale w celu ochrony poufności danych pamięć VP50 zostanie sformatowana. Oznacza to, że wszystkie dane zostaną usunięte.*



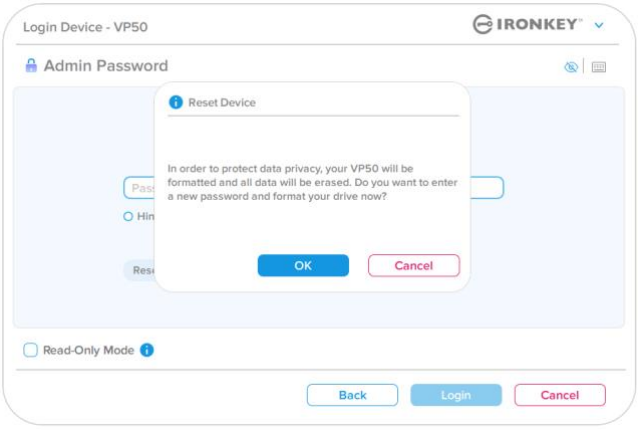

**Ilustracja 9.7 – Hasło administratora: przycisk resetowania urządzenia**

- **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 9.8).




**Ilustracja 9.8 – 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 jest konieczne wypełnianie pola podpowiedzi, może to jednak pomóc w przypomnieniu sobie zapomnianego hasła.



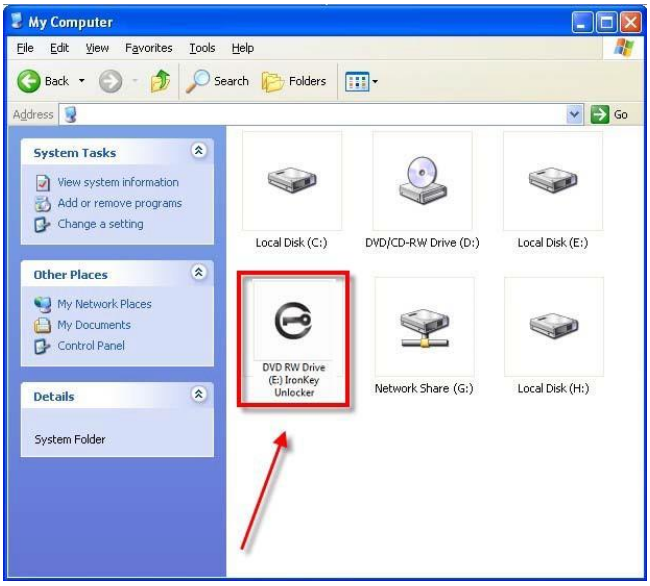

**Ilustracja 9.9 – Potwierdzenie resetowanie urządzenia**

## Pomoc i rozwiązywanie problemów

### Konflikt liter dysku: system operacyjny Windows

- Jak wspomniano w części *Wymagania systemowe* niniejszej instrukcji obsługi (na str. 3), pamięć VP50 wymaga dwóch kolejnych liter dysku PO ostatnim dysku fizycznym, który pojawia się przed „luką” w przypisaniu liter dysku (patrz *ilustracja 9.10*). 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 VP50 literę dysku, która jest już używana przez zasób sieciowy lub ścieżkę Universal Naming Convention (UNC), powodując konflikt liter dysku. W takim przypadku należy skonsultować się z administratorem lub działem pomocy technicznej w celu zmiany przypisania liter dysku w obszarze Zarządzanie dyskami systemu Windows (wymagane są uprawnienia administratora). Jak wspomniano w części *Wymagania systemowe* niniejszej instrukcji obsługi (na str. 3), pamięć VP50 wymaga dwóch kolejnych liter dysku PO ostatnim dysku fizycznym, który pojawia się przed „luką” w przypisaniu liter dysku (patrz *ilustracja 9.10*). 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.




**Ilustracja 9.10 – Przykład litery dysku**

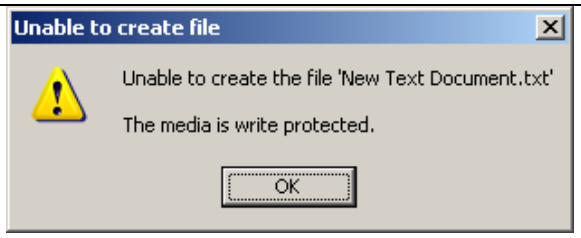
W tym przykładzie (ilustracja 9.10) pamięć VP50 korzysta z litery dysku F:, która jest pierwszą dostępną literą po literze E: (przypisanej do ostatniego dysku fizycznego przed luką). Ponieważ litera G: jest zasobem sieciowym nieobjętym profilem sprzętu, pamięć VP50 może podjąć próbę użycia jej jako drugiej litery, co spowoduje konflikt.

Jeśli w systemie nie ma zasobów sieciowych, ale nadal nie można uruchomić pamięci VP50, prawdopodobnie 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.

## Pomoc i rozwiązywanie problemów

### Komunikaty o błędach

| | |
|---|---|
| **Unable to create file (Nie można utworzyć pliku):** Ten komunikat o błędzie jest wyświetlany podczas próby UTWORZENIA pliku lub folderu NA bezpiecznej partycji danych po zalogowaniu się w trybie tylko do odczytu. |  **Ilustracja 9.11 – Błąd Unable to Create File (Nie można utworzyć pliku)** |
| **Error copying file or folder (Błąd kopiowania pliku lub folderu):** Ten komunikat o błędzie jest wyświetlany podczas próby SKOPIOWANIA pliku lub folderu DO bezpiecznej partycji danych po zalogowaniu się w trybie tylko do odczytu. |  **Ilustracja 9.12 – Błąd Error Copying File or Folder (Błąd kopiowania pliku lub folderu)** |
| **Error Deleting File or Folder (Błąd usuwania pliku lub folderu):** Ten komunikat o błędzie jest wyświetlany podczas próby USUNIĘCIA pliku lub folderu z bezpiecznej partycji danych po zalogowaniu się w trybie tylko do odczytu. |  **Ilustracja 9.13 – Błąd Error Deleting File or Folder (Błąd usuwania pliku lub folderu)** |

**Uwaga:** W przypadku zalogowania się w trybie tylko do odczytu i konieczności odblokowania pamięci z pełnymi uprawnieniami do odczytu/zapisu na bezpiecznej partycji danych należy wyłączyć pamięć VP50 i zalogować się ponownie, usuwając przed uwierzytelnieniem zaznaczenie pola wyboru ”Read-Only Mode” (Tryb tylko do odczytu).

# IRONKEY™ Vault Privacy 50 (VP50)
# 暗号化 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 VP50

## はじめに

Kingston IronKey Vault Privacy 50 (VP50) は、デジタル署名付きファームウェアによる BadUSB 対策や、総当たり (ブルートフォース) パスワード攻撃など、XTS モードで FIPS 197 認証取得済み AES 256 ビットハードウェア暗号化を行うことによって、ビジネスグレードのセキュリティを提供するプレミアム USB ドライブです。VP50 はまた、TAA 準拠で米国で組み立てられています。VP50 シリーズは、ユーザーが物理的に管理できる暗号化ストレージですので、インターネットやクラウドサービスを使用する場合よりもデータ保護に優れています。

VP50 は、複雑なパスワードまたはパスフレーズモードのマルチパスワード (管理者、ユーザー、および一回限りの回復) オプションをサポートします。パスワードのひとつを忘れた場合でも、マルチパスワードオプションを使用して、データへのアクセスを回復できます。従来の複雑なパスワードのサポートに加えて、新しいパスフレーズモードでは、数字の PIN、文章、単語リスト、歌詞などを 10～64 文字の長さで指定できます。管理者は、ユーザーおよび一回限りの回復パスワードを有効にするか、ユーザーパスワードをリセットして、データへのアクセスを回復できます。

パスワード入力を容易にするため、「目」 のシンボルで入力したパスワードを表示できますので、打ち間違いによるパスワード入力の失敗を減らすことができます。総当たり攻撃の防止のため、連続で 10 回間違ったパスワードを入力すると、ユーザーまたは一回限りの回復パスワードはロックされ、管理者パスワードの入力を連続で 10 回間違えると、ドライブが暗号化消去されます。

信頼できないシステム上の潜在的なマルウェアから保護するため、管理者およびユーザーの両方で、読み取り専用モードを設定してドライブを書き込み保護できます。さらに、内蔵された仮想キーボードが、キーロガーまたはスクリーンロガーからデバイスを守ります。

FIPS 197 認証取得済みで TAA 準拠ですので、会社などの組織で企業 IT およびサイバーセキュリティ要件に対応する標準的なエンドポイント管理ソフトウェアと統合するため、Kingston のカスタマイズプログラムにより、製品 ID (PID) を使って VP50 シリーズのドライブをカスタマイズして設定できます。

中小企業は管理者ロールをドライブのローカル管理に使用できます。たとえば、従業員のユーザーまたは一回限りの回復パスワードの設定またはリセットや、ロックされたドライブのデータアクセスの回復や、フォレンジクスが必要な場合の法規制への対応に管理者を使用します。

VP50 には、5 年限定保証と Kingston 無料技術保証が付属しています。

**IronKey Vault Privacy 50 の機能**

- XTS-AES 256 ビットハードウェア暗号化で FIPS 197 認証取得済み (暗号化をオフにすることはできません)
- 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モード
- 入力したパスワードをで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
- ドライブの内容を変更やマルウェアから保護する二重の読み取り専用 (書き込み保護) 設定
- 中小企業は管理者ロールを使用してドライブをローカル管理できます。
- 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

このユーザーガイドは、IronKey Vault Privacy 50 (VP50) について、カスタマイズ実施前の出荷時の状態を基に説明しています。

## システム要件

| | |
|---|---|
| **PC プラットフォーム**<br>• Intel、AMD および Apple M1 SOC<br>• 15MB のディスク空き容量<br>• USB 2.0〜3.2 ポート対応<br>• 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*<br><br>*** 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)**<br>• Windows 11<br>• Windows 10<br>• Windows 8.1 |
| **Mac プラットフォーム**<br>• 15MB のディスク空き容量<br>• USB 2.0〜3.2 ポート | **対応 Mac オペレーティングシステム (OS)**<br>• macOS X (v. 10.13.x〜12.x.x) |

## 推奨事項

VP50 デバイスに十分な電力を供給するために、以下の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、VP50 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 VP50 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 VP50 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。
- 共有システムまたは馴染みのないシステムのドライブを使用する場合、マルウェアからドライブを保護するために、読み取り専用モードを設定した方がよいでしょう。
- 使用しない時にはデバイスをロックします
- ドライブを抜く前にイジェクト操作をします
- 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 に最新のドライブアップデート、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

VP50 に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、VP50 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、VP50 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、VP50 ではデータ回復用に、管理者、ユーザー、一回限りの回復パスワードの、3つの異なるパスワードを持つことができます。

VP50 では、管理者パスワード（管理者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。さらに管理者は、ユーザーがユーザーパスワードにログインしてリセットできるように、ユーザーに一回限りの回復パスワードを設定できます。

ユーザーもドライブにアクセスできますが、管理者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でも、もう一方のパスワードでデータへアクセスできます。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。両方のパスワードを設定し、ユーザーパスワードを使用している間は、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。ユーザーは、必要に応じて一回限りの回復パスワードを使用し、ユーザーパスワードをリセットできます。

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、データを他の記憶媒体に保管しておくことをおすすめします。VP50 は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 VP50 では、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

複雑なパスワードには、次の文字種のうち最低３種を使用して、6～16 文字にする必要があります。

- 英大文字
- 英小文字
- 数字
- 特殊文字

### パスフレーズ

VP50 では、10～64 文字のパスフレーズをサポートしています。パスフレーズにはルールがありませんが、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文字の組み合わせで、他の言語の文字の使用も可能です。「VP50 drive」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。

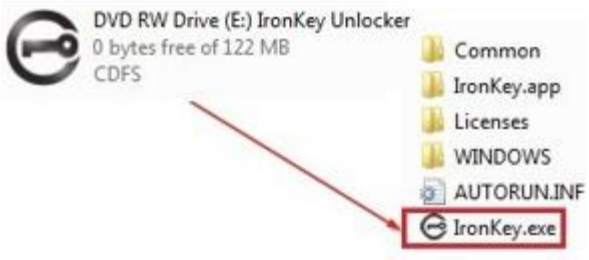
## マイデバイスの設定

IronKey 暗号化 USB ドライブに十分な電力を供給するために、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 パワードハブなどの 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) |  <br>**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アンロッカー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)<br><br>• 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。下の画像では、ドライブ文字を (E:) にしています。 |  <br>**図 3.2 - ファイルエクスプローラ Window/IronKey.exe** |

### デバイスアクセス（macOS 環境）

VP50 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 IKVP50（または 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 IKVP50（または IronKey.アプリ）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。

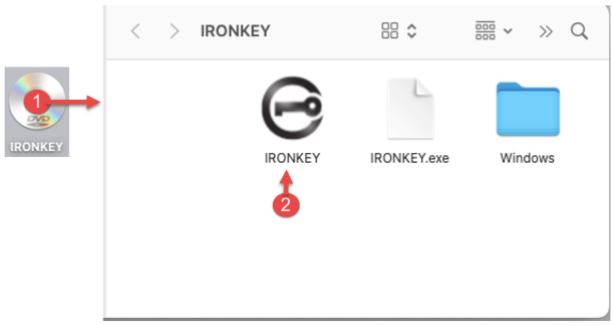
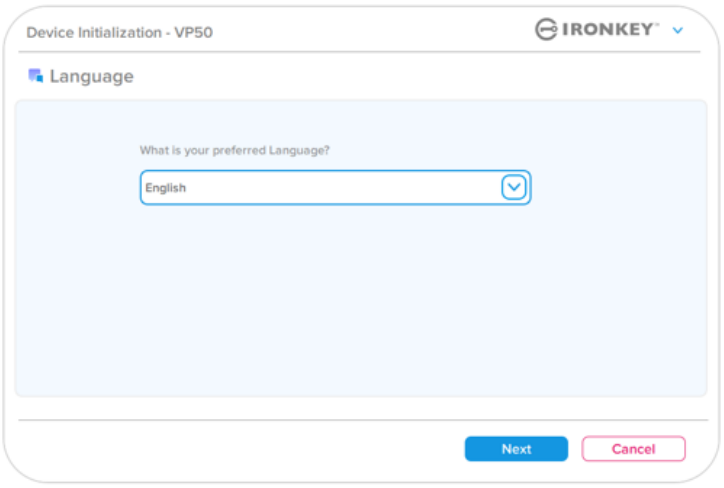
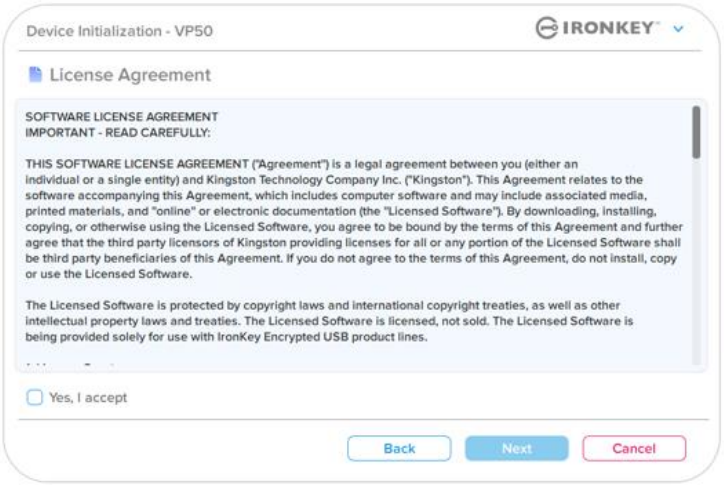



**図 3.3 - IKVP ボリューム**

# 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、**Next [次へ]** をクリックします。（図 4.1 参照） |  <br>**図 4.1 - Language [言語]の選択** |
| 使用許諾契約をよく読んで **Next [次へ]** をクリックします。<br><br>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、**Next [次へ]** のボタンは有効になりません。(図 4.2) |  <br>**図 4.2 – License Agreement [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、VP50 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、下の管理者/ユーザーパスワードを有効にする方法を読んで、これらの機能をよく理解してください。

**注：**複雑なパスワードまたはパスフレーズのどちらかを一旦選択すると、デバイスをリセットするまで選択をやり直せません。

パスワードの選択を開始するには、Password [パスワード] フィールドに作成するパスワードを入力し、Confirm Password [パスワードの確認] フィールドに再入力します。ユーザーが作成するパスワードが、以下の基準を満たしていないと、初期化プロセスを継続できません。

**Complex [複雑なパスワード]**

- 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)

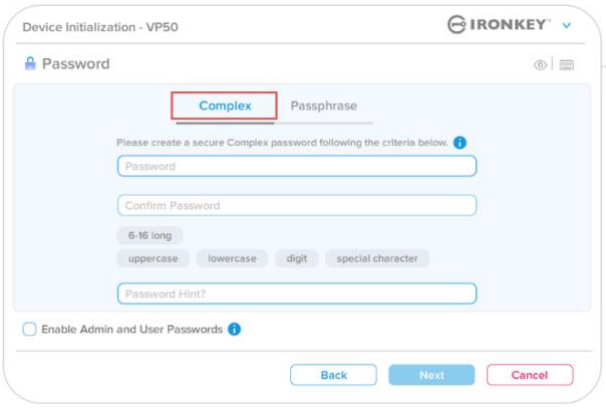



**図 4.3 - Complex [複雑なパスワード]**

**Passphrase [パスフレーズパスワード]**

- 文字数の制限：
  - 最短 10 文字
  - 最長 64 文字

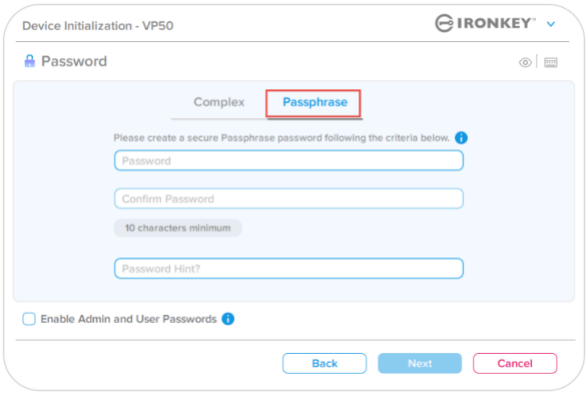



**図 4.4 - Passphrase [パスフレーズパスワード]**

**Password Hint [パスワードのヒント]（任意）**

パスワードのヒントは、パスワードを忘れた場合に、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。

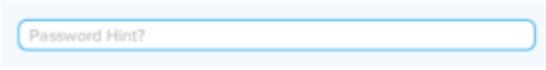



**図 4.5 – Password Hint [パスワードのヒント] フィールド**

## 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)

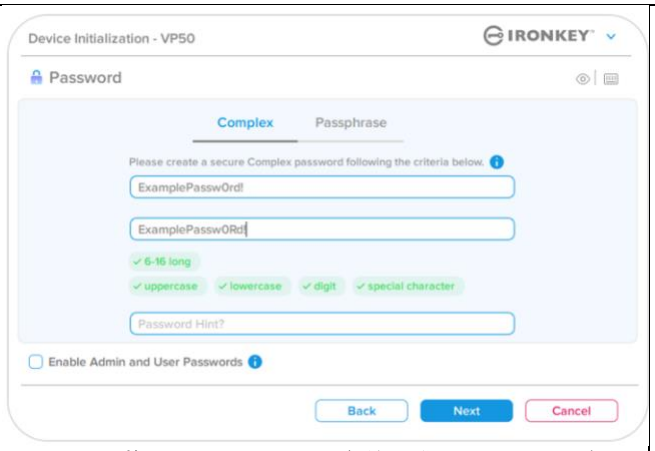



**図 4.6a - 複雑なパスワードの条件を満たしている場合**

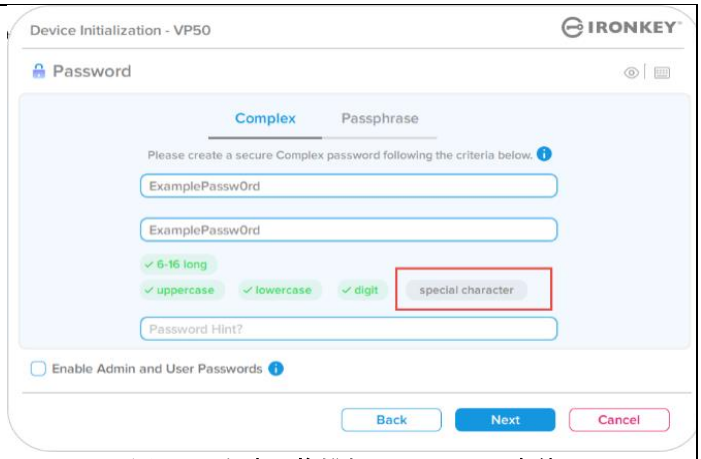



**図 4.6b - 任意の複雑なパスワードの条件**

**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、**Next [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。

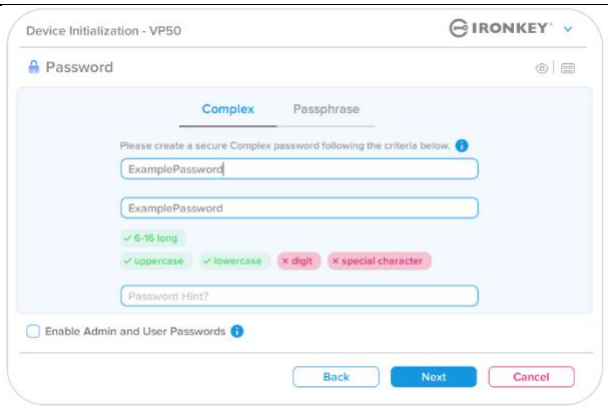



**図 4.7 - パスワード条件を満たしていない場合**

# デバイスの初期化

## 仮想キーボード

VP50 には、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、**Device Initialization [デバイスの初期化]** 画面の右上のキーボードボタンを探し、選択します。

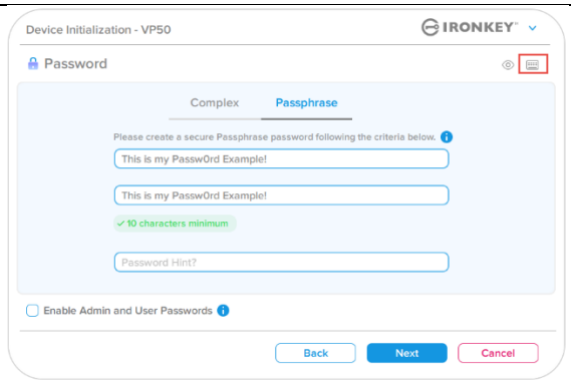



**図 4.8 - 仮想キーボードの有効化**

- 仮想キーボードが表示された後で、**Screenlogger Protection [スクリーンロガー保護]** 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あなたの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。

- この機能をさらに堅牢にするには、キーボードの右下の Randomize [ランダム化] を選択して、仮想キーボードの **Randomize [ランダム化]** を選択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。

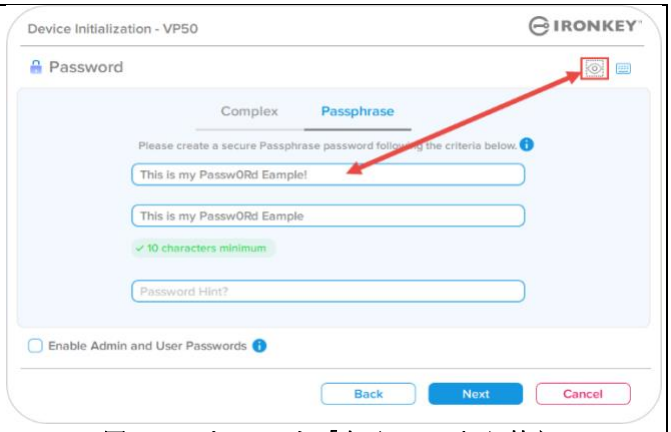
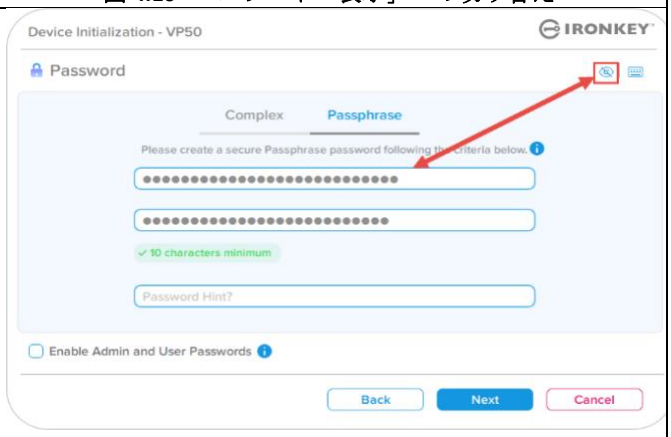

**図 4.9 – Screenlogger Protection [スクリーンロガー保護]/ Randomize [ランダム化]**

# 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。 |  <br>**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。<br>  |  <br>**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れば、管理者ロールで両方のアカウントを管理できるマルチパスワードの機能を利用できます。**Enable Admin and User Passwords [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。

- 一回限りの回復パスワード
- ユーザーログインの際に強制的に読み取り専用モードにする
- ユーザーパスワードのリセット
- ユーザーログインの際に強制的にパスワードをリセットする

これらの機能について詳しくは、このユーザーガイドの 25 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、**Enable Admin and User Passwords [管理者およびユーザーのパスワードを有効にする]** の隣のボックスをクリックし、有効なパスワードを選択してから Next [次へ] を選択します。(図 4.12)

- この機能が**有効**な場合、この画面で選択されているパスワードは**管理者パスワード**になります。Next [次へ] 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。

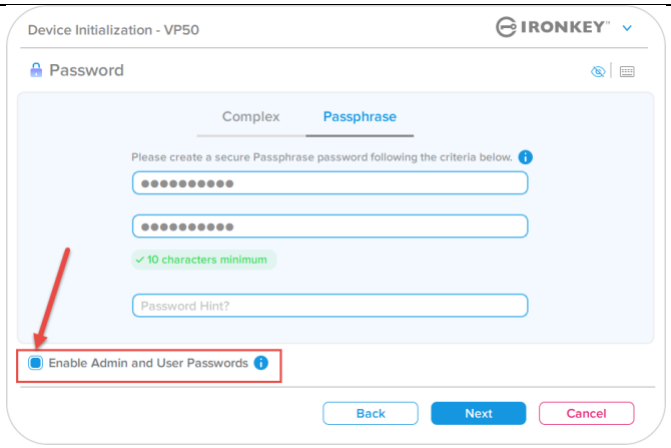



**図4.12 – Enable Admin and User Passwords [管理者およびユーザーのパスワードを有効にする]**

**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、Enable Admin and User Passwords **[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 Next [次へ] をクリックします。

**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。

# 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 User Password [ユーザーパスワード] 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、本書で後ほど詳しく説明します。(23 ページを参照してください)

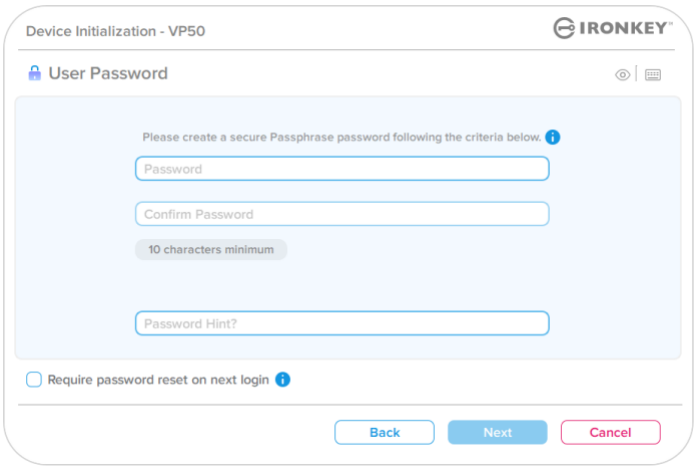



**図 4.13 – User Password [ユーザーパスワード]（管理者とユーザーが有効な場合）**

**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、一回限りのパスワードの回復、ドライブ設定後のパスワードへのリセットへ引き継がれます。選択したパスワードオプションは、デバイスを完全にリセットしない限り変更できません。

- **図 4.13** の左下の [**次のログイン時にパスワードのリセットが必要**] 機能は、ユーザーパスワードにのみ必要で、初期化プロセス中に管理者によって設定された一時パスワードを使用してユーザーがログインしてから、ドライブが一時パスワードで認証された後で、好きなパスワードに変更するように強制することができます。これは、ドライブを他の人用に譲る場合に便利です。**(図 4.14)**

  **注：**セキュリティのため、新しいパスワードを一時パスワードと同じにすることはできません。

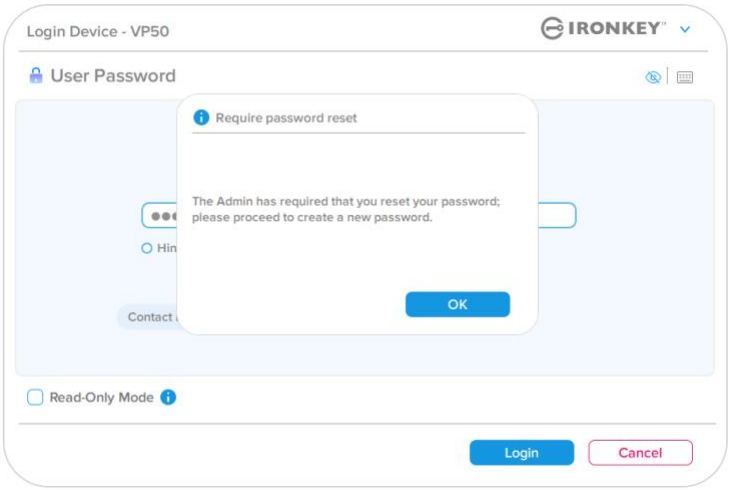



**図 4.14 - 次回ログイン時にパスワードのリセットが必要 (ユーザーパスワードの場合)**

# 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のため、空白にしておくこともできます。）

**Name [名前]** フィールドには、最大 32 文字を入力できますが、パスワードと**まったく同じ**文字列を入力することはできません。

**Company [会社]** フィールドには、最大 32 文字を入力できますが、パスワードと**まったく同じ**文字列を入力することはできません。

**Details [明細]** フィールドには、最大 156 文字を入力できますが、パスワードと**まったく同じ**文字列を入力することはできません。

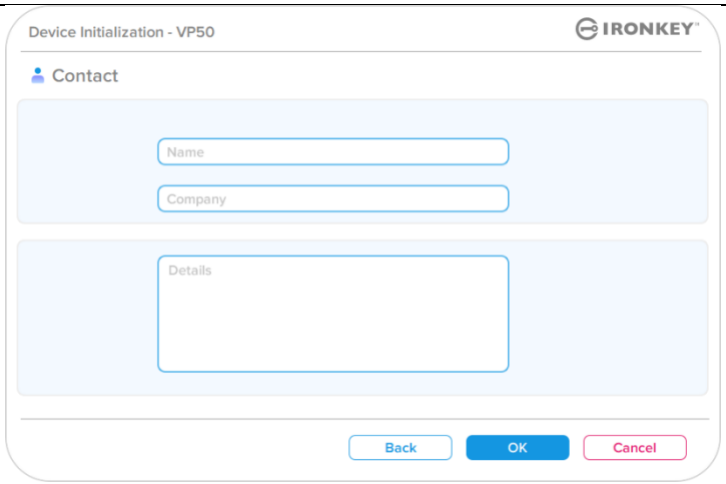



**図 4.14 – Contact [連絡先情報]**

**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マウントします。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。

# 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 VP50 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 5.1）できます。Login as Admin [管理者としてログイン] 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 5.2)

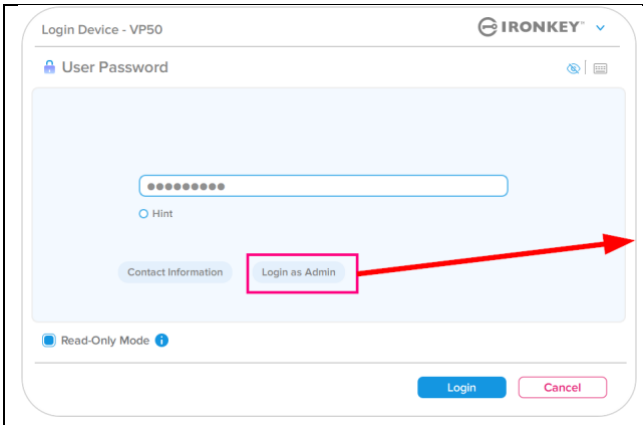



**図 5.1 - ユーザーパスワードでのログイン（管理者が有効な場合）**

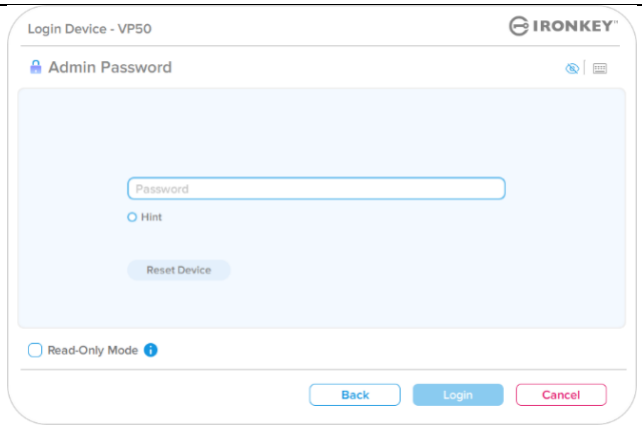



**図 5.2 - 管理者パスワードでのログイン**

## ユーザー専用モードでのログイン（管理者が無効な場合）

**ページ 13** 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 5.3)

**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、**Reset Device** [デバイスのリセット] 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。**

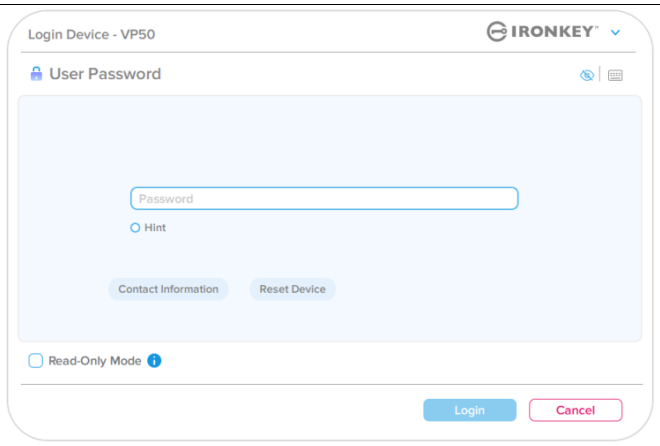



**図 5.3 - ユーザーパスワードでのログイン（管理者が無効な場合）**

# デバイスの使用

## 読み取り専用モードでのアンロック

IronKey ドライブ上のファイルが変更されないように、読み取り専用モードでドライブをアンロックできます。たとえば、信頼性が低いか、よく知らないコンピュータを使用する時に、読み取り専用モードでアンロックすれば、そのコンピュータにあるマルウェアがデバイスに感染することや、ファイルを変更することを防げます。

このモードで作業する時、デバイス上のファイルの変更などの操作は一切実行できません。
たとえば、デバイスの再フォーマットや、ドライブ上のファイルの回復、追加、編集はできません。

読み取り専用モードのデバイスのロックを解除するには：

1. ホストコンピュータの USB ポートにデバイスを差し込み、**IronKey.exe** を実行します。
2. パスワード入力ボックスの下の **Read-Only Mode [読み取り専用モード]** をチェックします。**(図 5.4)**
3. デバイスのパスワードを入力して **Login [ログイン]** をクリックします。これで、読み取り専用モードで IronKey がロック解除されました。

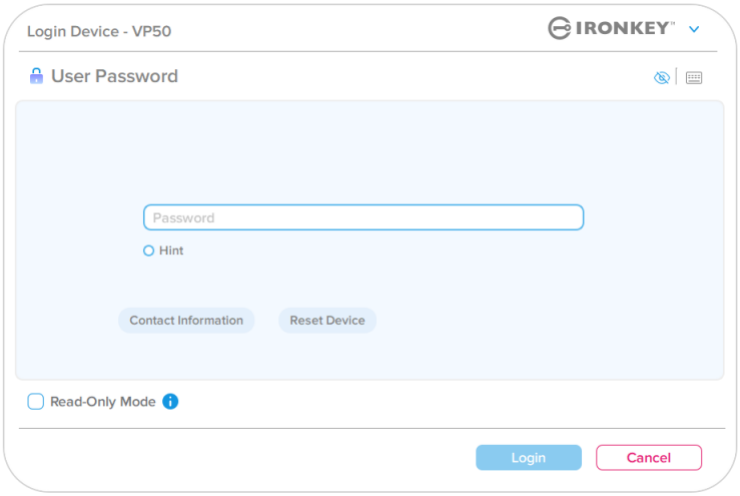



**図 5.4 – Read-Only Mode [読み取り専用モード]**

デバイスのロックを解除して、セキュリティで保護されたデータのパーティションに対して完全に読み書きのアクセスができるようにするには、VP50 を一度シャットダウンして、再度ログインし直し、Read-Only Mode [読取り専用モード] のチェックボックスのチェックを外してください。

**注：**VP50 の管理者オプションには、ユーザーデータの強制的な読み取り専用モードがあります。つまり、管理者によって強制的に、ユーザーのログイン時に読み取り専用モードのロックが解除されるようにできます（詳しくは **28 ページ**を参照してください）。

# 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なおせます。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値の 10 回に達すると、次のような動きをします。

| 管理者/ユーザー有効 | 総当たり攻撃防止<br>デバイスの動作<br>（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。管理者または一回限りの回復パスワードでログインし、ユーザーパスワードをリセットします。 | 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** |
| 一回限りの回復パスワード | パスワードがロックされます。Recovery Password [回復パスワード] のボタンはグレーに変わり、使用不可になります。管理者としてログインし、パスワードをリセットします。 | いいえ |
| **ユーザーのみ<br>単一のユーザー、単一のパスワード<br>(管理者/ユーザーが NOT な場合)** | **総当たり攻撃防止<br>デバイスの動作<br>（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。暗号化消去とは、すべてのパスワード、暗号化キーおよびデータを削除することです。**データはすべて失われます。**

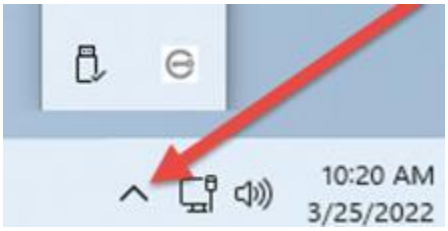
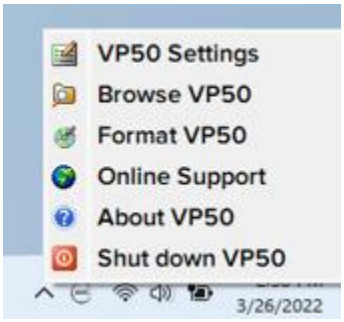
## 保護下のファイルへのアクセス

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、普通のドライブでいつもの通り、便利に作業できます。

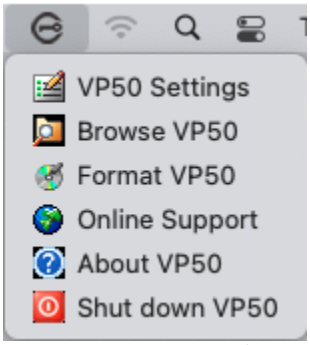
**ヒント**：ファイルにアクセスするには、Windows タスクバーの **IronKey アイコン**を右クリックしてから、[**VP50 の表示**] をクリックします。(図 6.2)

## デバイスの各種オプション – (Windows 環境の場合)

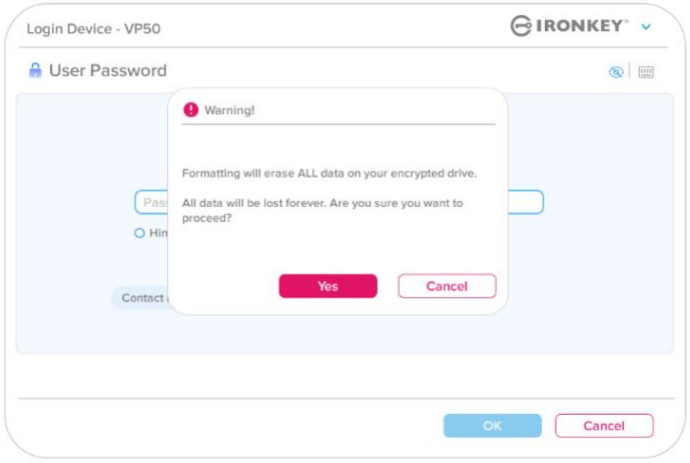
デバイスへログインしている状態では、ウィンドウの右隅に IronKey アイコンが表示されます。IronKey アイコンを右クリックすると、利用可能なドライブオプションの選択メニューが開きます。(図 6.2)
これらのデバイスオプションについて詳しくは、本書の 19～23 ページにあります。

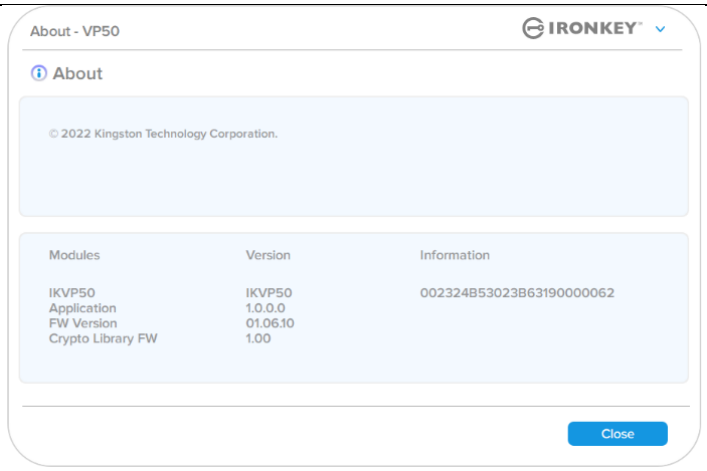
| | |
|---|---|
| • デバイスへログインしている状態では、ウィンドウの右隅に IronKey アイコンが表示されます。**(図 6.1)** |  <br>**図 6.1 – タスクバーの IronKey アイコン** |
| • IronKey アイコンを右クリックすると、利用可能なドライブオプションの選択メニューが開きます。**(図 6.2)**<br><br>これらのデバイスオプションについて詳しくは、本書の 19～23 ページにあります。 |  <br>**図 6.2 – IronKey アイコンをクリックしてデバイスオプションを表示** |

## 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 6.3** のように macOS メニューの中に IronKey VP50 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。<br><br>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。 |  <br>**図 6.3 - 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

| | |
|---|---|
| **VP50 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「VP50 の設定」セクションにあります。） |
| **VP50 の表示：** | • 保護下のファイルを表示できます。 |
| **VP50 のフォーマット：**<br>保護下のデータパーティションのフォーマットができます。（警告：すべてのデータが消去されます）（**図 6.1**）<br><br>**注：**フォーマットにはパスワード認証が必要です。 |  <br>**図 6.1 - VP50 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。 |
| **VP50 の詳細情報：**<br>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、VP50 について詳しく説明します。**(図 6.2)**<br><br>**注：**ドライブの個別シリアル番号は About [情報] 欄の下にあります。 |  <br>**図 6.2 - VP50 について** |
| **VP50 のシャットダウン：** | • VP50 を正常にシャットダウンすることにより、ユーザーシステムから安全に切り離すことができます。 |

## VP50 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:** 管理者パスワードやヒントを変更できます（*図 7.1*）
- **連絡先情報：**連絡先情報の追加／表示／変更ができます（*図 7.2*）
- **言語：**現在の言語選択の変更ができます (*図 7.3*)
- **管理者オプション**次のような追加機能を有効にできます。(図 7.4)
  - ユーザーパスワードの変更
  - ログインパスワードのリセット(ユーザーパスワードの場合)
  - 一回限りの回復パスワードの有効化
  - ユーザーデータを強制的に読み取り専用モードにする

**注：**管理者オプションについて詳しくは 24 ページにあります。

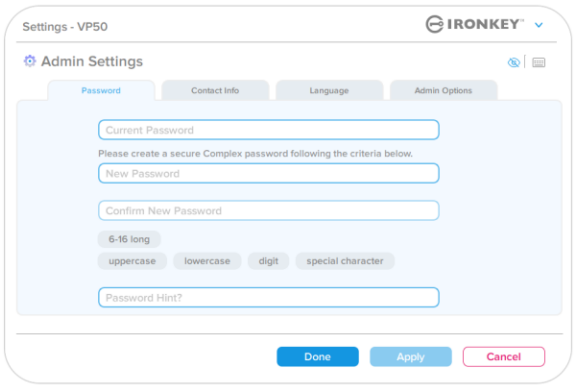



図 7.1 - Password [パスワードオプション]

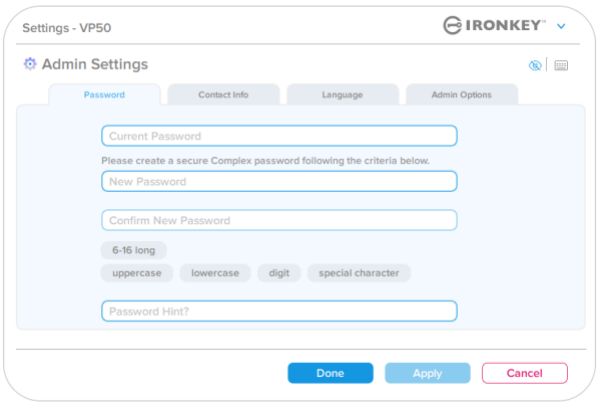



図 7.2 – Contact Info [連絡先情報]

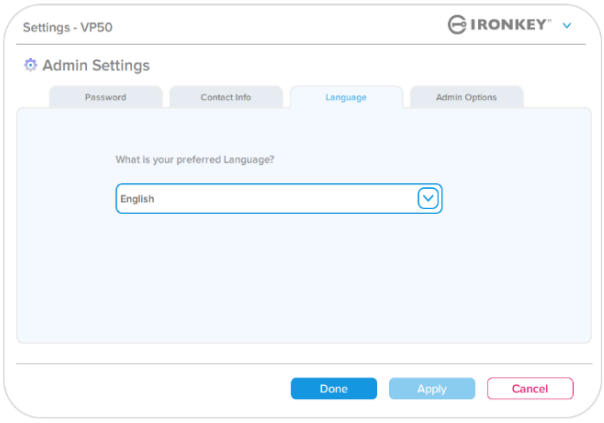



図 7.3 – Language [言語オプション]

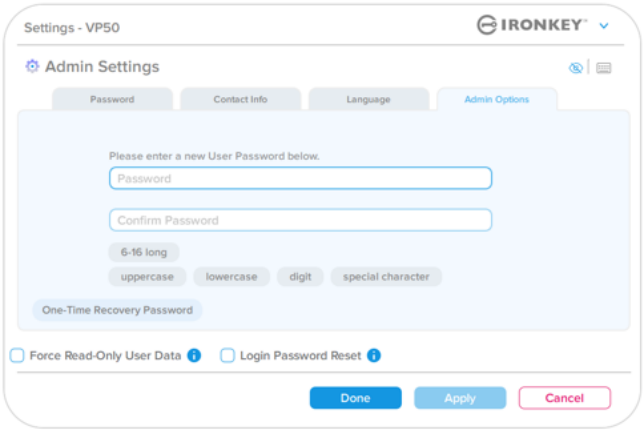



図 7.4 - Admin Options [管理者オプション]

## VP50 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:**
自分のユーザーパスワードやヒントを変更できます。(*図 7.5*)

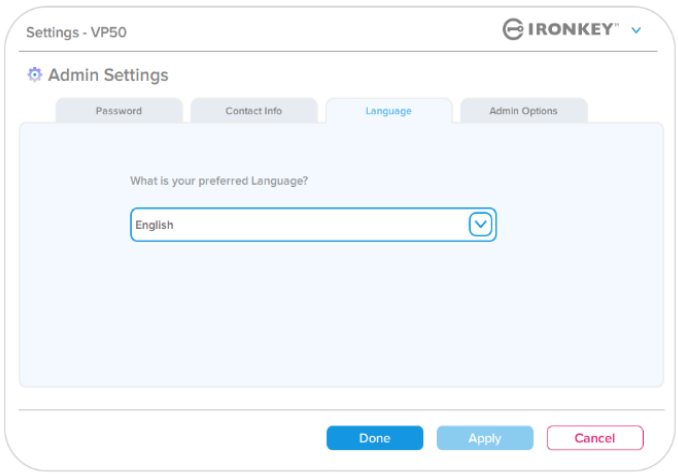



**図 7.5 - パスワードでのオプション（管理者が有効な場合: ユーザーログイン）**

**連絡先情報：**
連絡先情報を追加/表示/変更できます。(*図 7.6*)

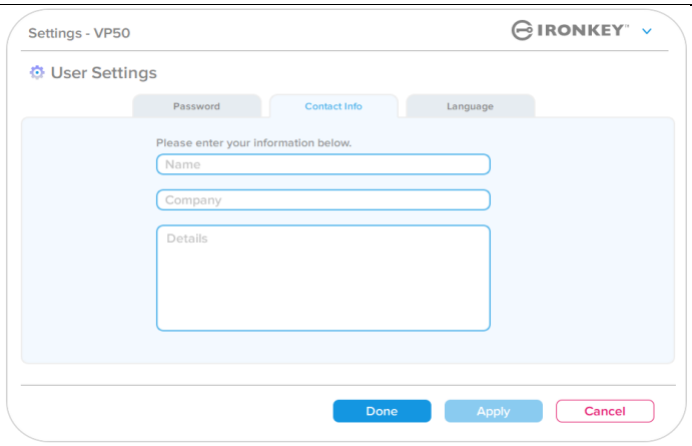



**図 7.6 - 連絡先情報（管理者が有効な場合: ユーザーログイン）**

**言語：**
現在の言語選択の変更ができます。(*図 7.7*)

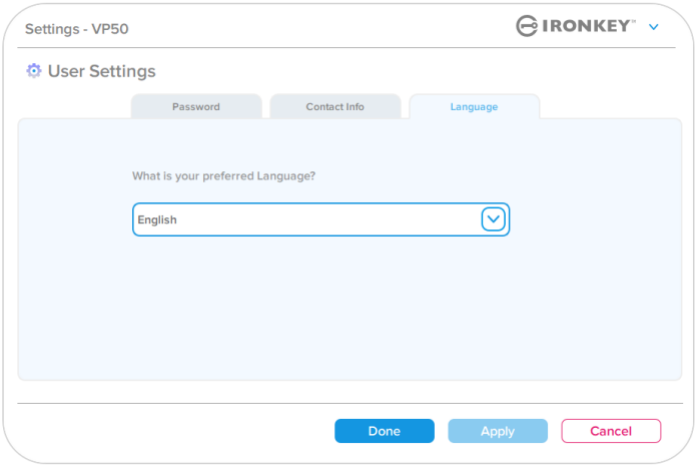



**図 7.7 - 言語の設定（管理者が有効な場合: ユーザーログイン）**

**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。

## VP50 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 VP50 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 VP50 設定にアクセスできません。

### 設定の変更および保存

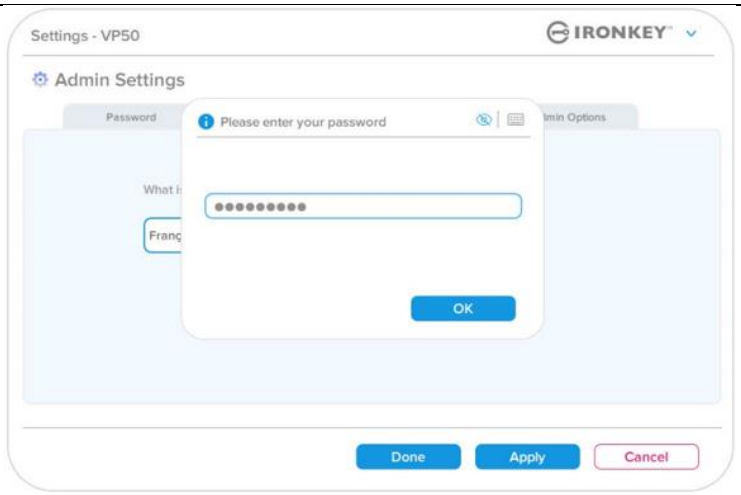
| | |
|---|---|
| • VP50 設定（たとえば連絡先情報、言語、パスワード変更、管理者オプションなど）が変更された場合は常に、承認して適用するために、ドライブにパスワードの入力画面が表示されます。（図 7.11 参照） |  |

**図 7.11 - VP50 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] をクリックします。すると、Please enter your password [パスワードを入力してください] ボックスが閉じ、VP50 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**
ユーザーパスワードを忘れた場合、または一時ユーザーパスワードが作成され次のログイン時にパスワードを変更させたい場合、管理者の機能設定により、複数の方法で安全にユーザーパスワードをリセットできます。ユーザーパスワードのリセットに役立つ次の機能があります。

**ユーザーパスワードのリセット：**
Admin Settings [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 8.1)**

**注**：パスワード要件基準は、初期化プロセスで設定された元々の基準に戻されます（複雑なパスワードまたはパスフレーズパスワード）。

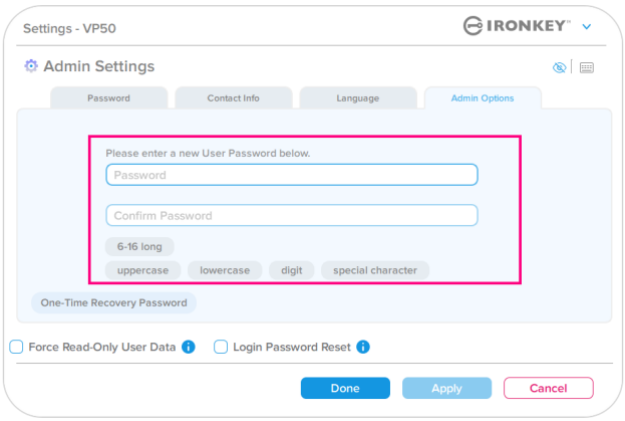



**図 8.1 – Admin Settings [管理者オプション]/ユーザーパスワードのリセット**

**ログインパスワードのリセット:**
ログインパスワードリセットを有効にすると、**ユーザーは強制的に、管理者の設定した一時パスワードでログイン**し、好きなパスワードに変更するように求められます。これは、ドライブを他の人用に譲る場合に便利です。（**図 8.2A および 8.2B を参照してください**）

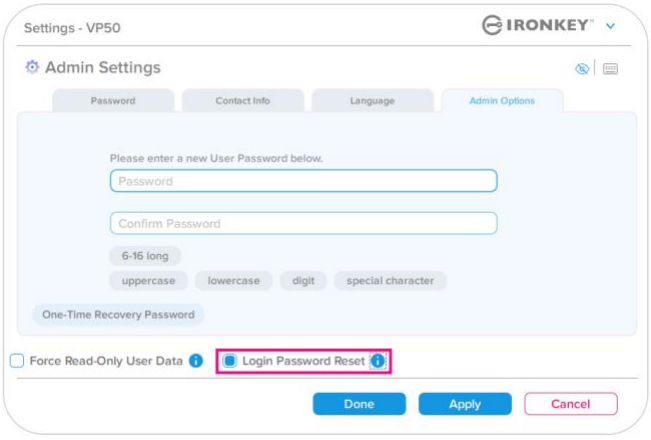



**図 8.2A – Login Password Reset [ログインパスワードのリセット] ボタン**

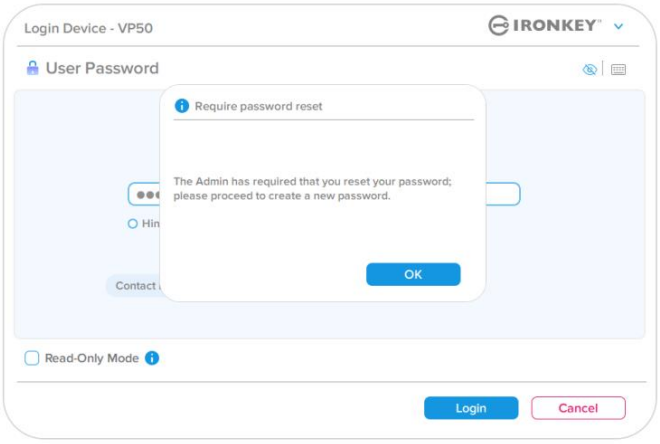
| | |
|---|---|
| **注：**このリセットを適用すると、次にユーザーログインに成功したときに有効になります。パスワード要件基準は、初期化プロセス中に設定された元々のオプションに従って自動的に適用されます（複雑なパスワードまたはパスフレーズパスワード）。 |  |

**図 8.2B – ユーザーパスワードの入力後の通知のリセット**

## 管理者の機能

### 一回限りの回復パスワード

一回限りの回復パスワード機能を有効にして使用する手順を説明します。

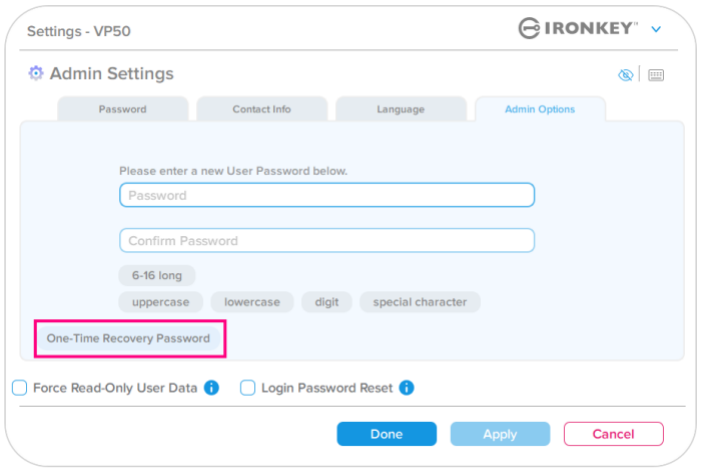
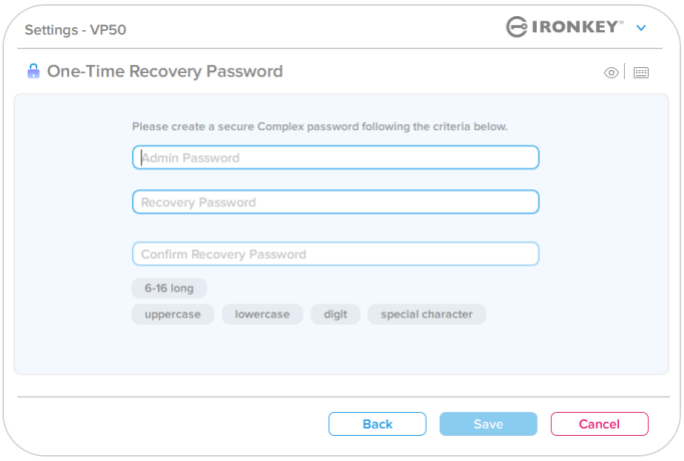
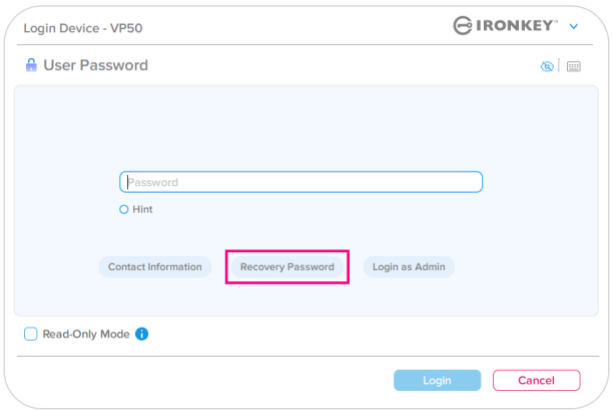
| | |
|---|---|
| 一回限りの回復パスワード<br><br>**ステップ 1：**一回限りの回復パスワード機能は非常に便利です。これは、ユーザーパスワードを忘れた場合に回復してリセットするために、一回だけ使用可能なパスワードです。まず最初に、管理者オプションメニューで One-Time Recovery Password [一回限りの回復パスワード] ボタンをクリックします。**(図 8.4)** |  |

**図 8.4 - One-Time Recovery Password[一回限りの回復パスワード]ボタン**

| | |
|---|---|
| **ステップ 2：**デバイスが初期設定された時と同じパスワード基準を使用して、One-Time Recovery Password [一回限りの回復パスワード] を作成します（複雑なパスワードまたはパスフレーズパスワード）。<br><br>**注：**変更の適用には、管理者パスワードが必要になります。 |  <br>**図 8.5 - One-Time Recovery Password [一回限りの回復パスワード] の設定** |

## 管理者の機能

一回限りの回復パスワードの使用

| | |
|---|---|
| **ステップ 1：**一回限りの回復パスワードの作成後、次のログイン時に**ユーザーパスワード**ログイン画面に新しいボタンが表示されます。**Recovery Password [回復パスワード]**ボタンをクリックすると、処理が開始されます。 |  <br>**図 8.6 Recovery Password [回復パスワード] ボタン** |

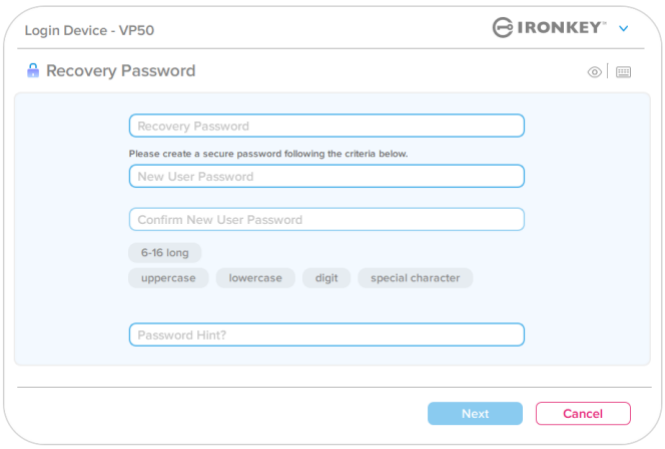
<table>
<tr>
<td>ステップ 2：回復パスワードの入力と新規ユーザーパスワードの作成が可能な時には、回復パスワード画面が表示されます。(図 8.7)<br><br>重要: 一回限りの回復パスワードでは、ログインの失敗回数を追跡する組み込みセキュリティ機能を活用できます。一回限りの回復パスワードを間違えてログインに 10 回失敗すると、パスワードは無効になり、ドライブに管理者としてログインして再度有効にする必要があります。（詳しくは 18 および 30 ページを参照してください)</td>
<td> 

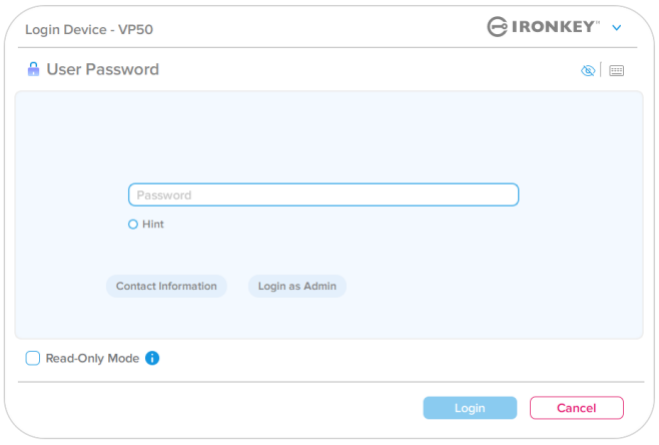
図 8.7 Recovery Password[回復パスワード] メニュー</td>
</tr>
<tr>
<td>ステップ 3：成功すると、ユーザーパスワード画面に戻ります。Recovery Password [回復パスワード] ボタンが消え、ステップ 2 で入力したユーザーパスワードが新しいユーザーパスワードになります。(図 8.8)</td>
<td> 

図 8.8 - 回復パスワードを正常に使用したあと、そのボタンが消えたユーザーパスワードログイン画面</td>
</tr>
</table>

## 強制的にユーザーデータを読み取り専用に設定

強制的な読み取り専用モード機能を有効にすると、ユーザーによるドライブへの書き込みを制限できます。この機能は、ドライブ上のファイルを読み取り専用アクセス専用にする必要がある場合に便利です。

- ユーザーデータに対して、強制的な読み取り専用を有効にする場合は、そのボックスをクリックして、Apply [適用] をクリックします。**(図 8.9)**

  **注：**この強制的な読み取り専用モードは、ユーザーにだけ適用され、管理者ログイン時は無効です。管理者ログインでは、まだ読み書きのアクセス権があります。しかし、必要であれば追加で読み取り専用モードを有効にできます。

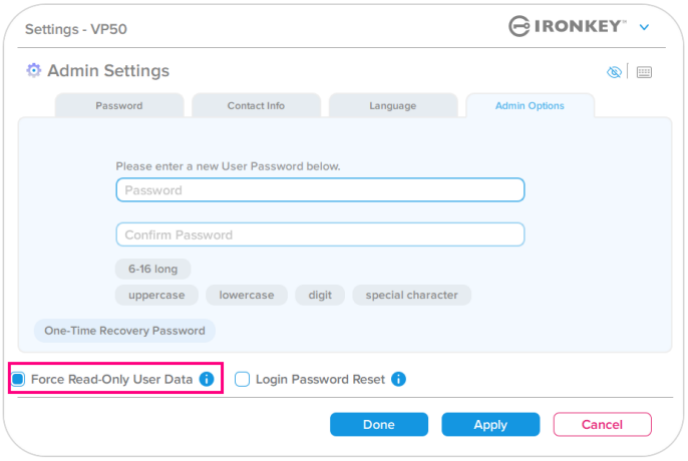



**図 8.9 – Force Read-Only User Data [ユーザーデータを強制的に読み取り専用にする] を有効にする**
**(変更の適用には、管理者パスワードが必要になります)**

- 一旦有効にすると、**Read-Only Mode [読み取り専用モード]** ボタンはブルーに変わります。これは、管理者によって無効化されるまで、強制的な読み取り専用モードがユーザーパスワードに対して永続的に有効になったことを意味します。(図 8.10)

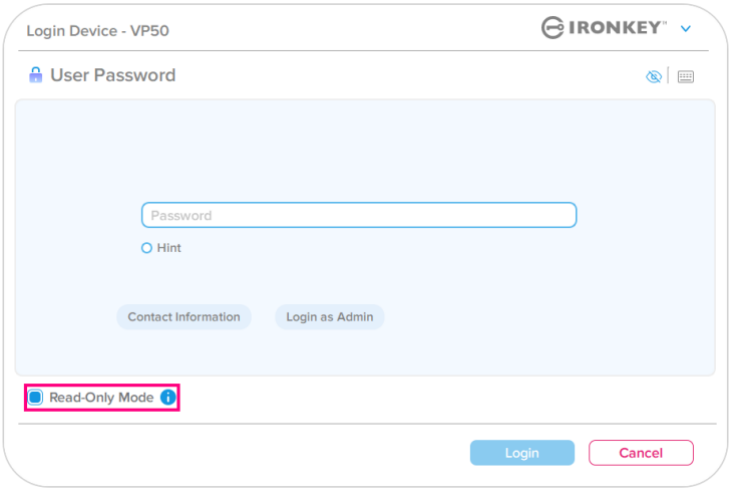



**図 8.10 - 読み取り専用モードがユーザーに対して強制的に有効になり管理者のみが無効化可能**

# ヘルプとトラブルシューティング

## デバイスのロック

VP50 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の設定値は、各ログイン方式（管理者/ユーザー/一回限りの回復パスワード）に対して 10 回（試行回数）です。

「ロックアウト」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 9.1)

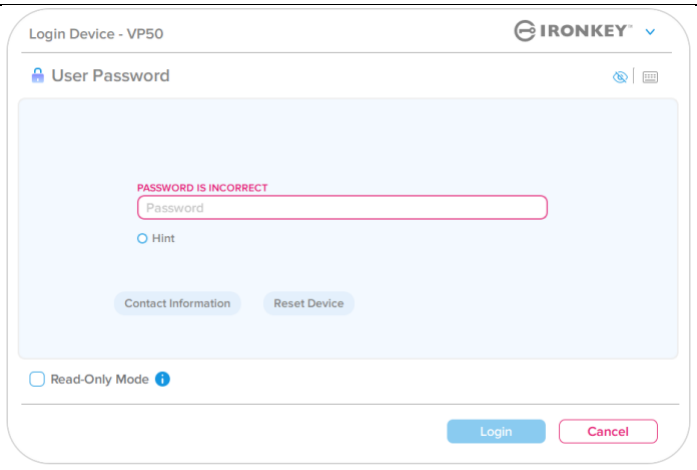



**図 9.1 - パスワードが間違っている場合のメッセージ**

- 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 9.2)

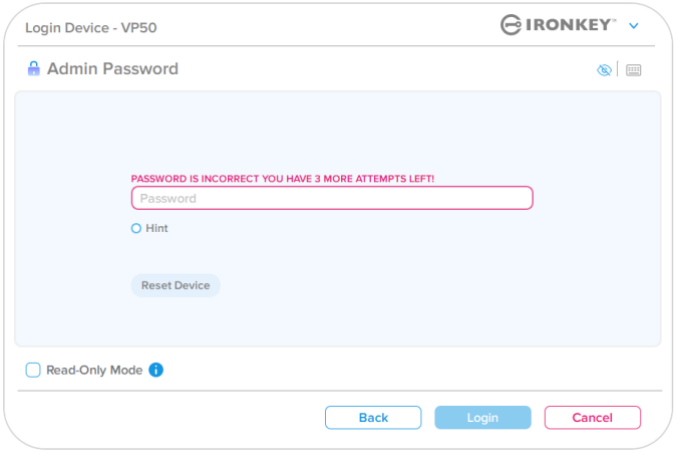



**図 9.2 - 7 回パスワードを間違えた場合のメッセージ**

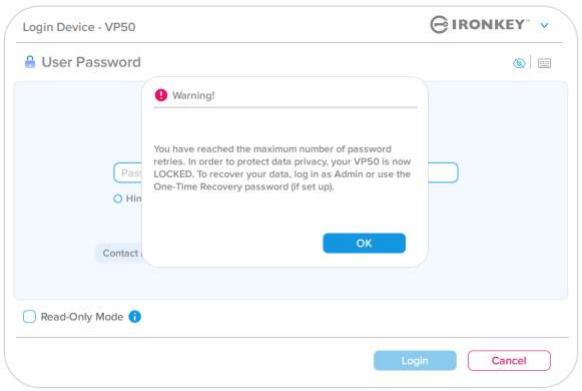
# ヘルプとトラブルシューティング

## 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によって（管理者、ユーザー、一回限りの回復パスワード）、デバイスはロックされ、代替方法（ある場合）でログインする必要があるか、**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 9.3～9.6 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。

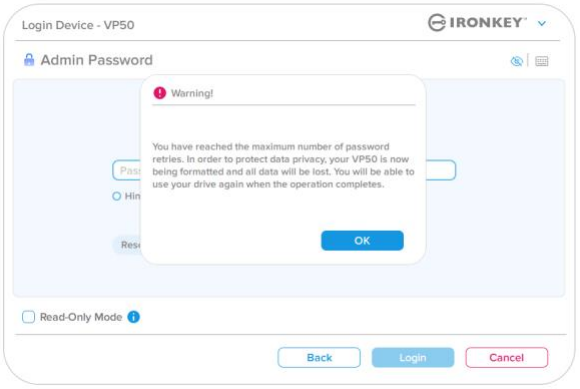
**ユーザーパスワード：(管理者/ユーザーが有効な場合)**




デバイスのロック

**(図 9.3)**

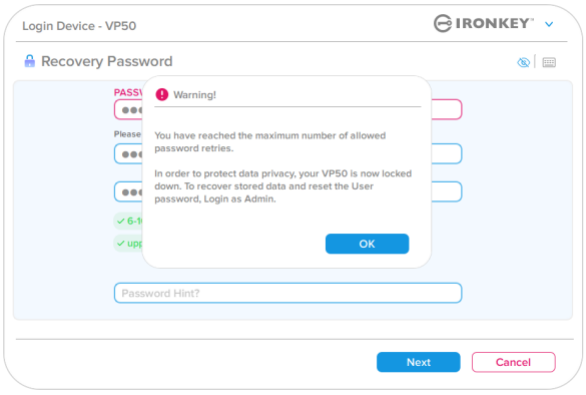
**管理者パスワード(管理者/ユーザーが有効な場合)**




デバイスのフォーマット*

**(図 9.4)**

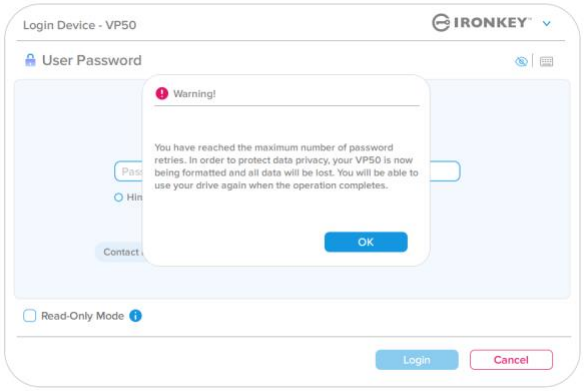
**一回限りの回復：(管理者/ユーザーが有効な場合)**




デバイスのロック

**(図 9.5)**

**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 9.6)**

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。

VP50 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。

** 注：デバイスをフォーマットすると、VP50 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、VP50 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 Reset Device [デバイスのリセット] ボタンをクリックします。（***図 9.7*** および **9.8** 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、VP50 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。*

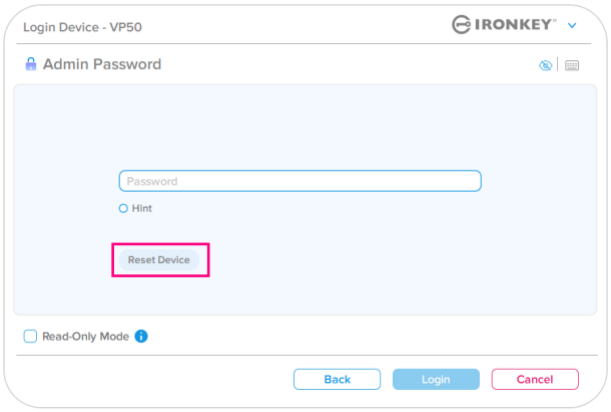



**図 9.7 - 管理者パスワード: Reset Device [デバイスのリセット] ボタン**

- **注：** Reset Device [*デバイスのリセット*] をクリックすると、メッセージボックスが表示され、初期化を行う前に新しいパスワードの入力を求めるかどうか質問してきます。この時点で、1) *OK* をクリックして確認するか、2) Cancel [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 9.8 参照）

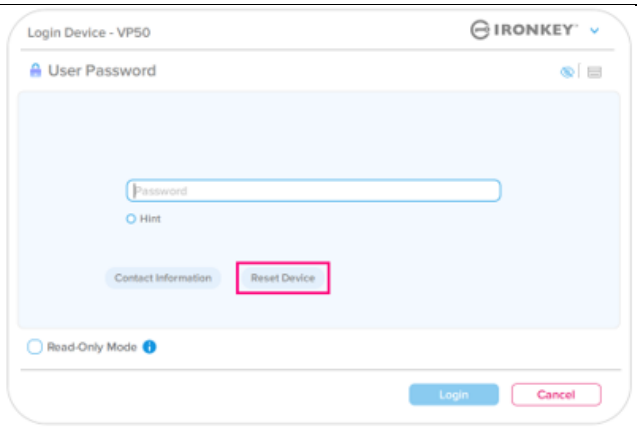



**図 9.8 - ユーザーパスワード(管理者/ユーザーが無効)デバイスのリセット**

- 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。

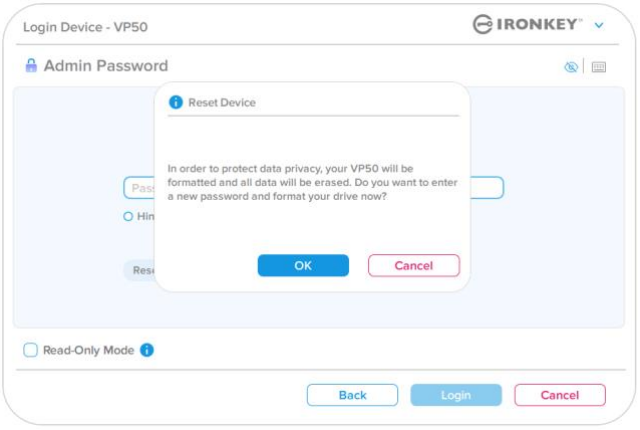



**図 9.9 - デバイスのリセットの確認**

## 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、VP50 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 9.10* 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、VP50 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)。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、VP50 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 9.10* 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。

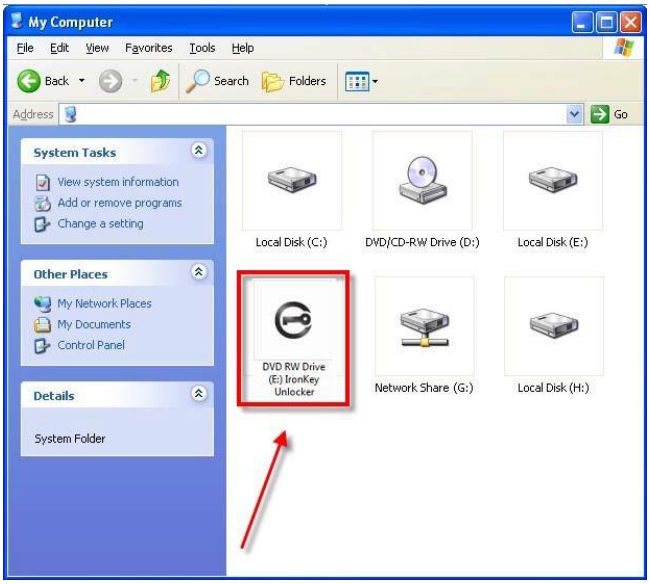


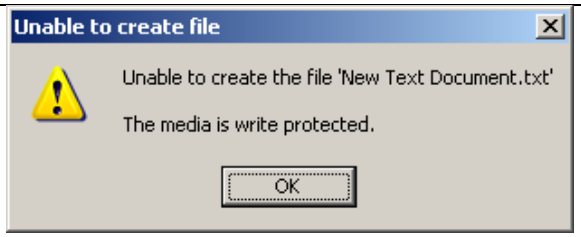

**図 9.10 - ドライブレターの例**

この例で言えば(図 9.10)、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、VP50 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 VP50 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。

## エラーメッセージ

| | |
|---|---|
| **ファイルを作成できません：**<br>このエラーメッセージは、読み取り専用モードでログイン中に、保護対象のデータパーティションでファイルまたはフォルダを作成しようとした時に表示されます。 |  <br>**図 9.11 - ファイル作成不可のエラー** |
| **ファイルまたはフォルダをコピーできません：**<br>このエラーメッセージは、読み取り専用モードでログイン中に、保護対象のデータパーティションにファイルまたはフォルダをコピーしようとした時に表示されます。 |  <br>**図 9.12 - ファイルまたはフォルダのコピー不可のエラー** |
| **ファイルまたはフォルダの削除でエラー：**<br>このエラーメッセージは、読み取り専用モードでログイン中に、保護対象のデータパーティションからファイルまたはフォルダを削除しようとした時に表示されます。 |  <br>**図 9.13 - ファイル/フォルダ削除の失敗のエラー** |

**注：**すでに読取り専用モードでログインし、デバイスのこのモードを解除して、セキュリティで保護されたデータのパーティションに対して完全に読み書きのアクセスができるようにするには、「読取り専用モード」のチェックボックスのチェックを外してから、VP50 を一度シャットダウンして、再度ログインしてください。

# IRONKEY™ Vault Privacy 50 (VP50)
# 加密 USB 3.2 Gen 1 闪存盘

*用户指南*

# 目录


图 1：IronKey VP50

## 简介

Kingston IronKey Vault Privacy 50 (VP50) 系列是一款高品质 USB 闪存盘，凭借通过 FIPS 197 认证的 XTS 模式 AES 256 位硬件加密，可提供企业级安全性，包括利用数字签名固件防范 BadUSB 以及防范暴力攻击密码破解。VP50 系列还符合 TAA 规范，并在美国组装。VP50 系列是由用户物理控制的加密存储设备，比使用互联网和云服务更能有效保护数据。

VP50 支持复杂或口令模式，可使用多密码（管理员、用户和一次性恢复）选项。多密码选项增强了恢复数据访问权限的能力，可有效应对忘记其中某个密码的情况。除了支持传统的复杂密码，新的口令模式允许输入数字 PIN、句子、单词表，甚至可以输入包含 10 到 64 个字符的歌词。为了恢复数据访问权限，管理员可以启用用户密码和一次性恢复密码，也可以重置用户密码。

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，减少导致登录尝试失败的拼写错误。暴力破解攻击防护会在连续输入 10 个无效密码时锁定用户或一次性恢复密码；如果连续 10 次输错管理员密码，则会加密擦除闪存盘。

为了防范不受信任的系统上存在的潜在恶意软件，管理员和用户都可以设置只读模式，为闪存盘启用写保护；此外，内置的虚拟键盘可以防止按键记录程序或屏幕记录器记录密码。

VP50 系列闪存盘通过 FIPS 197 认证且符合 TAA 规范。通过金士顿的定制计划，组织可以使用产品 ID (PID) 来自定义和配置 VP50，以便与标准端点管理软件进行集成，从而满足企业 IT 和网络安全的要求。

中小型企业可以利用管理员角色在本地管理闪存盘，比如说，利用管理员来配置或重置员工的用户密码或一次性恢复密码，恢复对锁定闪存盘中数据的访问权限，以及在要求取证时遵循法律法规等。

VP50 享有 5 年有限保固和免费金士顿技术支持服务。

**IronKey Vault Privacy 50 功能**

- 通过 FIPS 197 认证的 XTS-AES 256 位硬件加密（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”按钮可显示已输入的密码，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
- 双重只读（写保护）设置可保护闪存盘内容，避免被更改或遭受恶意软件攻击
- 中小型企业可以利用管理员角色在本地管理闪存盘
- Windows 或 macOS 兼容（参见数据表了解详情）

## 关于本手册

本用户手册介绍了 IronKey Vault Privacy 50 (VP50)，基于没有实施定制的出厂映像。

## 系统要求

| | |
|---|---|
| **PC 平台**<br>• Intel、AMD 和 Apple M1 SOC<br>• 15MB 可用磁盘空间<br>• 可用的 USB 2.0 - 3.2 接口<br>• 在最后一个物理驱动器之后有两个连续的驱动器号*<br><br>***注意：**参见第 32 页的“驱动器号冲突”。 | **PC 操作系统支持**<br>• Windows 11<br>• Windows 10<br>• Windows 8.1 |
| **Mac 平台**<br>• 15MB 可用磁盘空间<br>• USB 2.0 - 3.2 接口 | **Mac 操作系统支持**<br>• macOS X (v. 10.13.x – 12.x.x) |

## 建议

为了确保 VP50 设备供电充足，请将其直接插在笔记本电脑或台式机的 USB 接口中，如***图 1.1***.所示。避免将 VP50 连接到任何带 USB 接口的外围设备，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 VP50 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 VP50 之前，对计算机执行病毒扫描
- 在公共系统或不熟悉的系统上使用闪存盘时，您可能会希望将设备设为只读模式，帮助闪存盘防范恶意软件
- 不使用时锁定闪存盘
- 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

VP50 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，VP50 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 VP50 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，VP50 支持利用三个不同的密码来恢复数据 – 管理员密码、用户密码和一次性恢复密码。

VP50 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。此外，管理员可以为用户设置一次性恢复密码，让用户可以登录并重置用户密码。

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。应设置**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。如有需要，用户可以使用一次性恢复密码来重置用户密码。

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。VP50 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

VP50 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

VP50 支持 10 至 64 个字符的口令。口令没有规则，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 VP50 闪存盘，密码语言可与为闪存盘选择的语言一样。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。

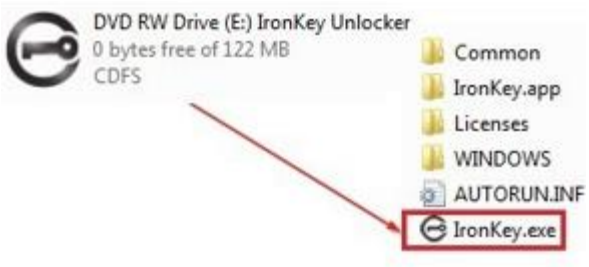
# 设置我的设备

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）

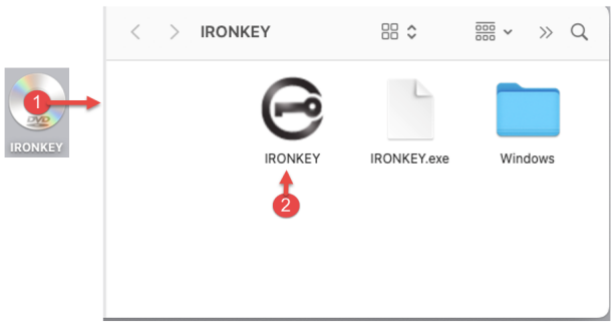
将 IronKey 加密 USB 闪存盘插入笔记本电脑或台式机的可用 USB 接口，等待 Windows 检测到该闪存盘。

| | |
|---|---|
| • Windows 8.1/10/11 用户会收到设备驱动程序通知。（图 3.1） |  <br>**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）<br>• 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。在下图中，驱动器号是 (E:)。 |  <br>**图 3.2 - “文件资源管理器”窗口/IronKey.exe** |

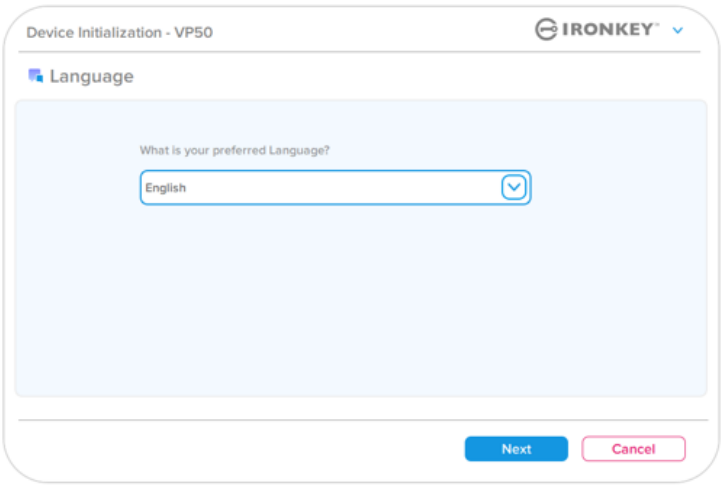
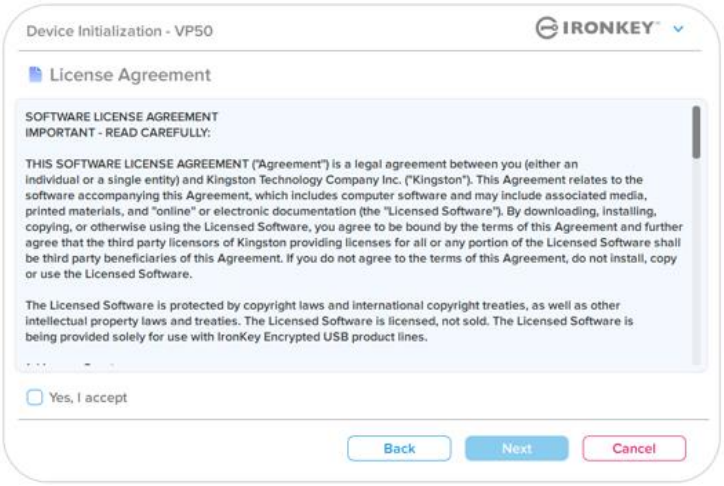
## 设备访问（macOS 环境）

将 VP50 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 IKVP50（或 IRONKEY）卷标。（图 3.3）

| | |
|---|---|
| • 双击 IronKey CD-ROM 图标。<br>• 然后，双击图 3.3 显示的窗口中的 IKVP50（或 IronKey.app）应用图标。这会开始初始化过程。 |  <br>**图 3.3 - IKVP 卷** |

# 设备初始化（Windows 和 macOS 环境）

## 语言和 EULA

| | |
|---|---|
| 从下拉菜单中选择偏好的语言，并单击**下一步 (Next)**。（参见图 4.1） |  <br>**图 4.1 - 语言选择** |
| 阅读许可协议并单击**下一步 (Next)**。<br><br>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） |  <br>**图 4.2 - 许可协议** |

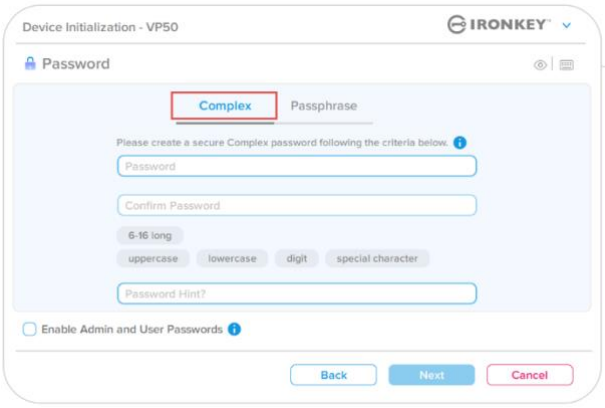
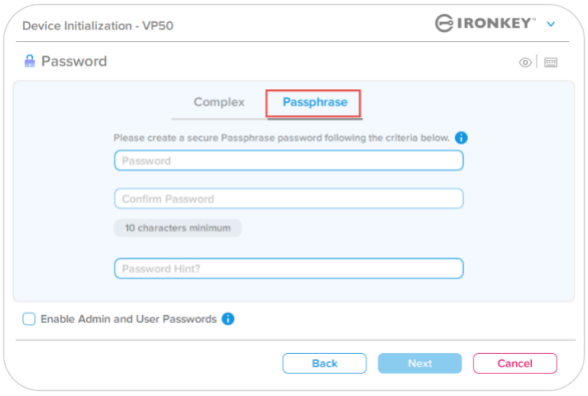
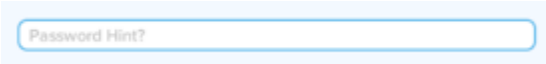
# 设备初始化

## 密码选择

在“密码”(Password) 提示窗口中，您能够使用复杂密码或口令密码模式创建密码，以保护您在 VP50 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，才能继续后续初始化流程：

| | |
|---|---|
| **复杂密码**<br>• 密码必须包含 6 个或更多字符（最多 16 个字符）。<br>• 必须满足以下三 (3) 个条件：<br>○ 大写<br>○ 小写<br>○ 数字<br>○ 特殊字符（!、$、& 等） |  <br>**图 4.3 - 复杂密码** |
| **口令密码**<br>• 必须包含：<br>○ 最少 10 个字符<br>○ 最多 64 个字符 |  <br>**图 4.4 - 口令密码** |
| **密码提示（可选）**<br>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。<br>**注意：**提示内容**不得**与密码完全相同。 |  <br>**图 4.5 - “密码提示”字段** |

# 设备初始化

## 有效密码和无效密码

对于**有效**密码，密码条件框会在条件满足时以绿色高亮显示。（参见图 4.6a-b）
注意：一旦满足至少三个密码条件，第四个条件框会变成灰色，表示此条件现在是可选项。（图 4.6b）

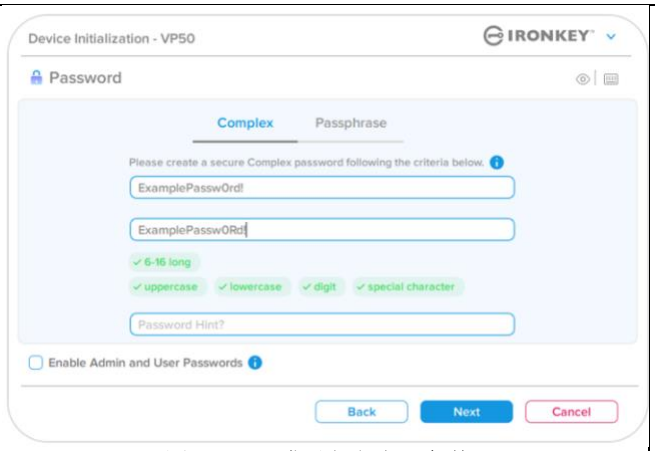



**图 4.6a - 已满足复杂密码条件**

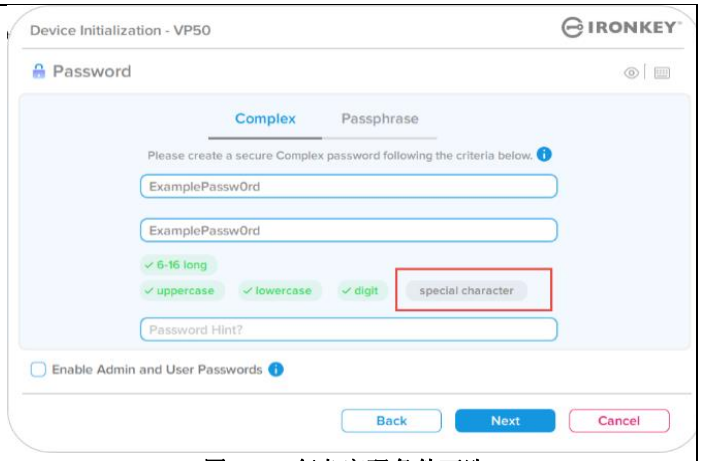



**图 4.6b - 复杂密码条件可选**

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。

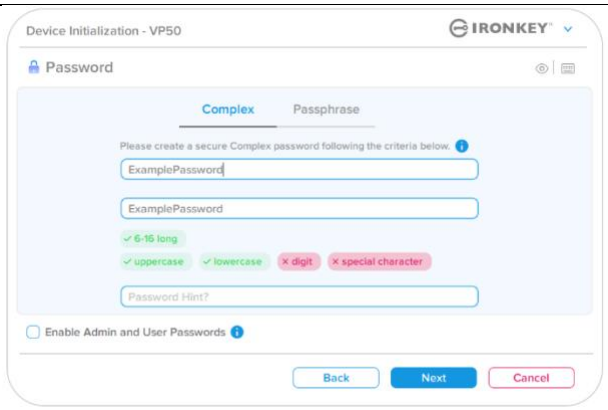



**图 4.7 - 未满足复杂密码条件**

# 设备初始化

## 虚拟键盘

VP50 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 (Device Initialization)** 屏幕的右上角找到键盘按钮，并选择该按钮。

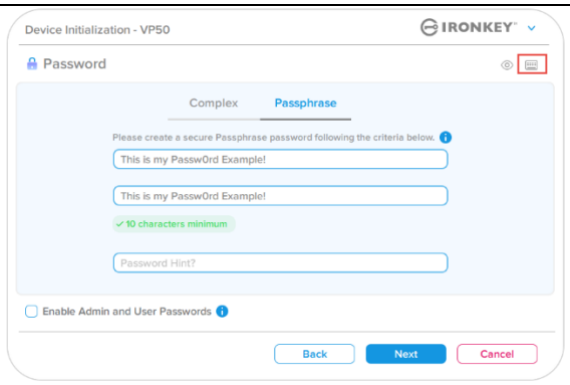



**图 4.8 - 激活虚拟键盘**

- 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。

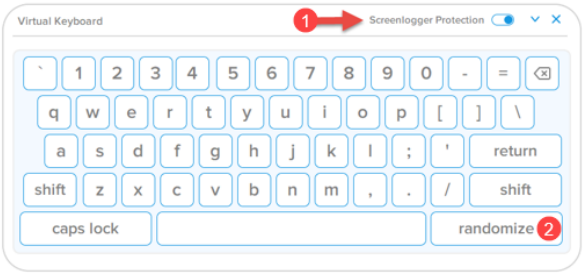


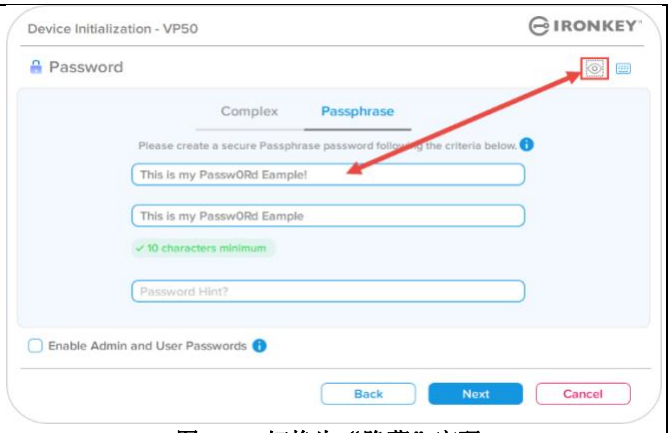
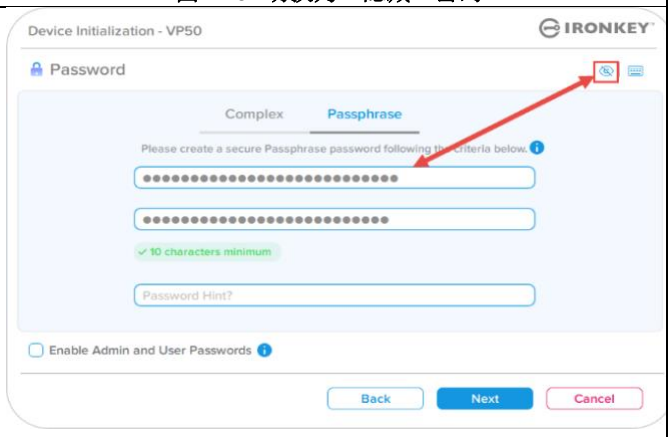

**图 4.9 - 屏幕记录器保护 / 随机排列**

# 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”(Device Initialization) 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。<br>  |  <br><br>**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。<br>  |  <br><br>**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。

**管理员密码和用户密码**启用后，您还可以访问：

- 一次性恢复密码
- 用户登录的强制只读模式
- 用户密码重置
- 用户登录的强制重置密码

要详细了解这些功能，请转到本用户指南第 25 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，并在选定有效密码后选择**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。

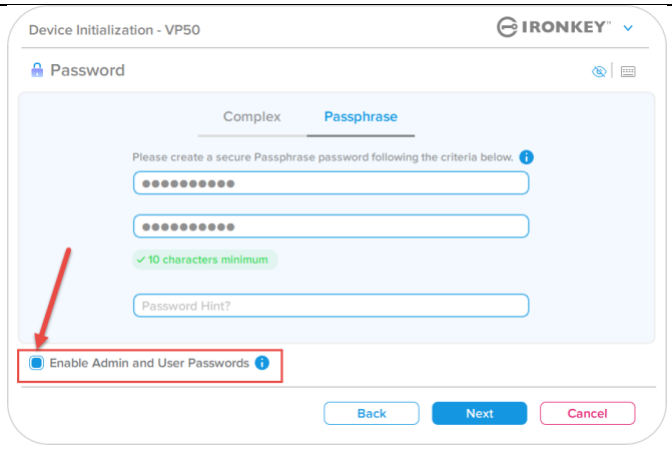



**图 4.12 - 启用管理员密码和用户密码**

**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)**。

**注意：管理员密码和用户密码 (Admin and User Passwords)** 在下文中称作**管理员角色 (Admin Role)**。

# 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**（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。（参见第 23 页）

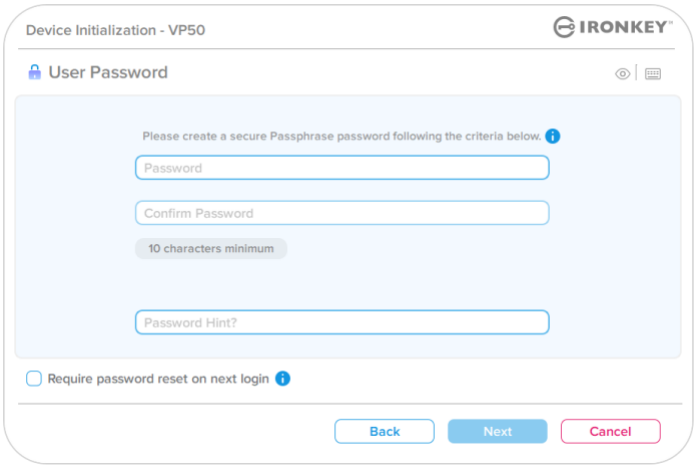



**图 4.13 - 用户密码（管理员和用户已启用）**

**注意：**所选密码选项（复杂或口令）条件会应用于用户密码、一次性恢复密码，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。

- **图 4.13** 左下角的**要在下次登录时重置密码 (Require password reset on next login)** 功能仅适用于用户密码，启用后可强制用户使用由管理员在初始化过程中设定的临时密码，然后在使用临时密码完成闪存盘身份验证后将其更改为用户所选密码。当需要将闪存盘提供给另一个人使用时，这会很有帮助。（**图 4.14**）

  **注意：**出于安全考虑，新密码不能与临时密码相同。

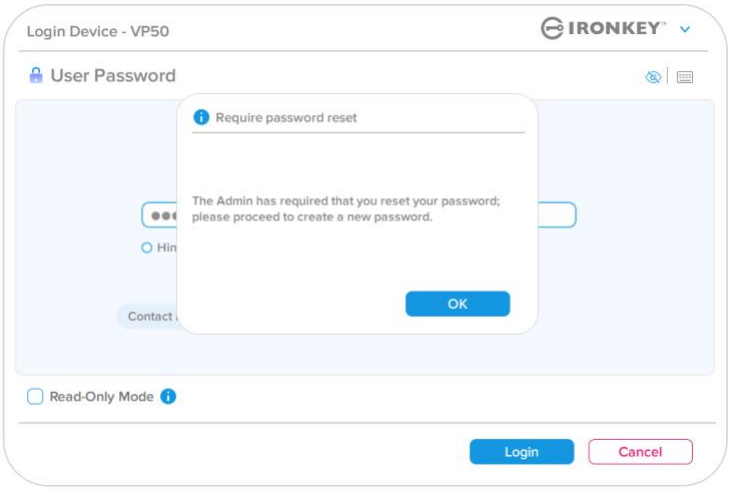



**图 4.14 - 要在下次登录时重置密码（针对用户密码）**

# 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**完全匹配**的密码。

**公司 (Company)** 字段最多可包含 32 个字符，但是不得包含**完全匹配**的密码。

**详情 (Details)** 字段最多可包含 156 个字符，但是不得包含**完全匹配**的密码。

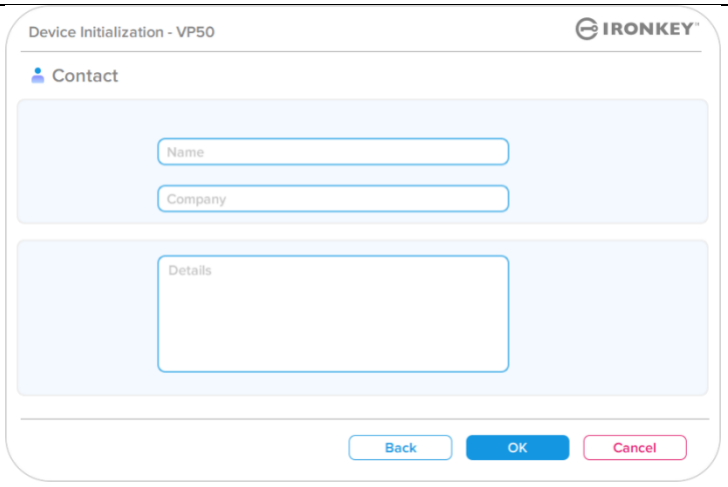



**图 4.14 - 联系信息**

**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。

# 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 VP50 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 5.1）。单击“作为管理员登录”(Login as Admin)（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 5.2）

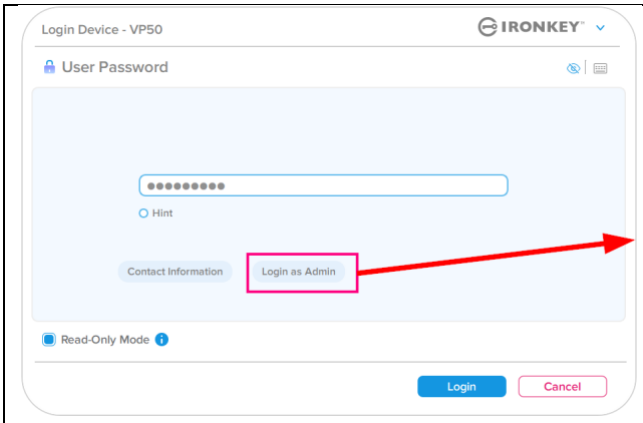



图 5.1 - 用户密码登录（管理员已启用）

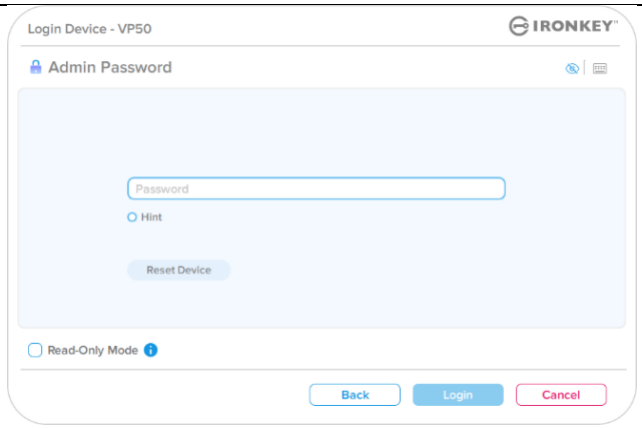



图 5.2 - 管理员密码登录

## 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 5.3）

**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。**重置设备后，闪存盘会被格式化，所有数据都会丢失。**

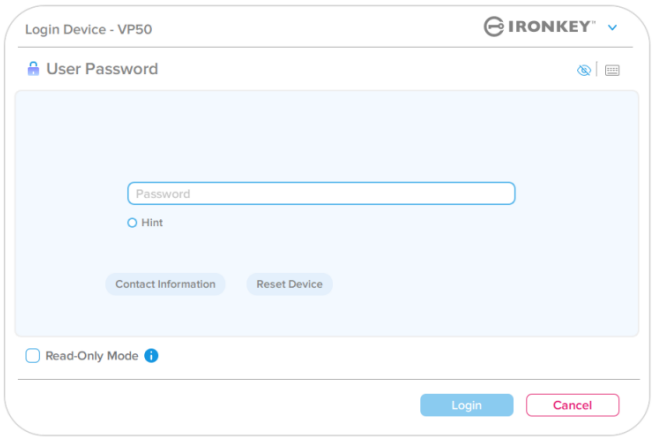



图 5.3 - 用户密码登录（管理员未启用）

## 在只读模式下解锁

您可以以只读状态解解锁闪存盘，确保 IronKey 闪存盘中的文件无法被修改。例如，当使用不受信任或未知的计算机时，以只读模式解锁设备，可以阻止计算机中的任何恶意软件感染设备或修改文件。

在这种模式下运行时，您无法执行任何会修改闪存盘中文件的操作。
例如，您无法重新格式化闪存盘、还原、添加或编辑闪存盘中的文件。

要在只读模式下解锁设备：

1. 将设备插入主机计算机的 USB 接口，并运行 **IronKey.exe**。
2. 勾选密码输入框下方的**只读模式 (Read-Only Mode)**。（**图 5.4**）
3. 输入设备密码并单击**登录 (Login)**。IronKey 现在会以只读模式解锁。

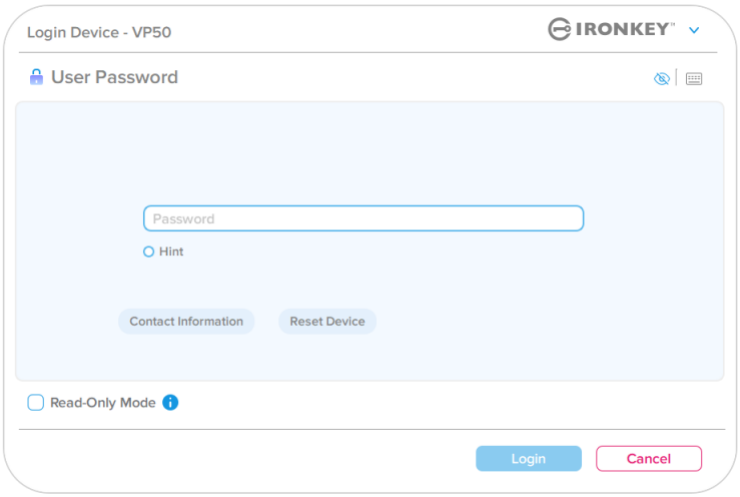



**图 5.4 - 只读模式**

如果您希望解锁设备并能够完全读取/写入安全数据分区，您必须关闭 VP50 并重新登录，同时取消勾选**只读模式 (Read-Only Mode)** 复选框。

**注意：**VP50 管理员选项包含用户数据强制只读模式，意味着管理员可以让用户登录强制以只读状态解锁（参见**第 28 页**了解详情）。

# 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<br>设备行为<br>（10 次输错密码）** | **数据擦除和设备重置？** |
|---|---|---|
| 用户密码 | 密码锁定。作为管理员登录或使用一次性恢复密码来重置用户密码 | 否 |
| 管理员密码 | 加密擦除闪存盘，密码、设置和数据被永久擦除 | **是** |
| 一次性恢复密码 | 密码锁定，“恢复密码”按钮变成灰色且无法使用。作为管理员登录以重置密码 | 否 |
| **仅用户<br>单用户、单密码<br>（管理员/用户未启用）** | **暴力攻击防护<br>设备行为<br>（10 次输错密码）** | **数据擦除和设备重置？** |
| 用户密码 | 加密擦除闪存盘，密码、设置和数据被永久擦除 | **是** |

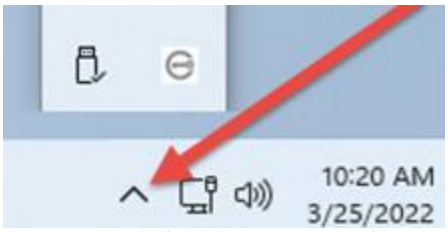
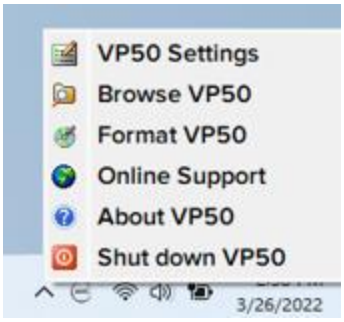
* 一旦您成功完成设备的身份验证，则会针对所用的登录方法重置失败登录计数器。加密擦除会删除所有密码、加密密钥和数据 – **您的数据会永久丢失。**

## 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平时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：**通过右击 Windows 任务栏中的 **IronKey 图标**并单击**浏览 VP50 (Browse VP50)**，您也可以访问自己的文件。（图 6.2）

## 设备选项 - （Windows 环境）

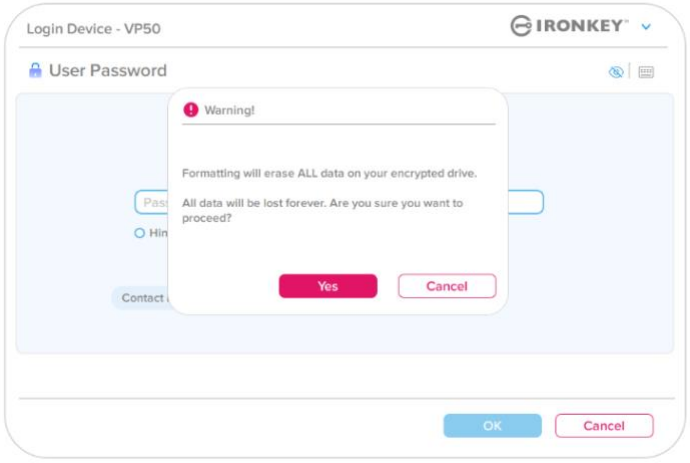
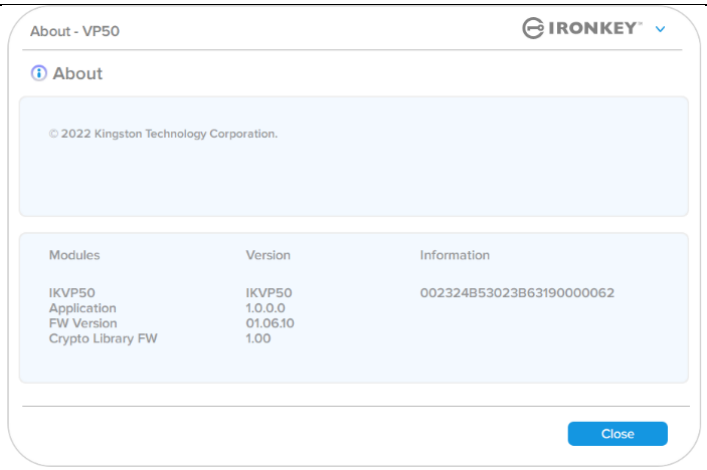
登录设备后，IronKey 图标会出现在 Windows 右下角。右击 IronKey 图标，会打开可用闪存盘选项的选择菜单。（图 6.2）
关于这些设备选项的详情，可在本手册第 19-23 页找到。

| | |
|---|---|
| • 登录设备后，IronKey 图标会出现在 Windows 右下角。**（图 6.1）** |  <br>**图 6.1 - 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 6.2）**<br><br>关于这些设备选项的详情，可在本手册第 19-23 页找到。 |  <br>**图 6.2 - 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 VP50 图标会出现在 macOS 菜单中（如**图 6.3** 所示），打开后显示可用的设备选项。<br><br>关于这些设备选项的详情，可在本手册第 19-23 页找到。 |  <br>**图 6.3 - macOS 菜单栏图标/设备选项菜单** |

## 设备选项

| | |
|---|---|
| **VP50 设置 (VP50 Settings)：** | • 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“VP50 设置”部分。） |
| **浏览 VP50 (Browse VP50)：** | • 让您可以查看安全文件。 |
| **格式化 VP50 (Format VP50)：**<br>让您可以格式化安全数据分区。（警告：所有数据会被擦除）（**图 6.1**）<br><br>**注意：**格式化需要密码身份认证。 |  <br><br>**图 6.1 – 格式化 VP50** |
| **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 VP50 (About VP50)：**<br>提供关于 VP50 的详细信息，包括应用、固件和序列号信息。（**图 6.2**）<br><br>**注意：**闪存盘的唯一序列号位于“信息”(Information) 列下。 |  <br><br>**图 6.2 - 关于 VP50** |
| **关闭 VP50 (Shut down VP50)：** | • 正确关闭 VP50，让您可以将其从系统中安全删除。 |

# VP50 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)：**让您可以更改自己的管理员密码和/或提示（*图 7.1*）
- **联系信息 (Contact Info)：**让您可以添加/查看/更改自己的联系信息（*图 7.2*）
- **语言 (Language)：**让您可以更改当前语言选择（*图 7.3*）
- **管理员选项 (Admin Options)：**让您可以启用额外的功能，例如：（图 7.4）
    - 更改用户密码
    - 登录密码重置（用户密码）
    - 启用一次性恢复密码
    - 用户数据强制只读模式

**注意：**有关管理员选项的更多详情，请参见第 24 页。

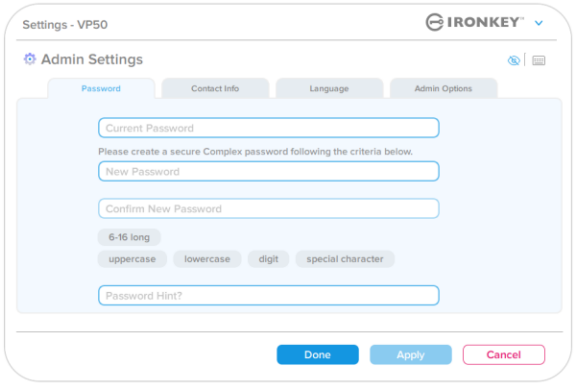



**图 7.1 - 密码选项**

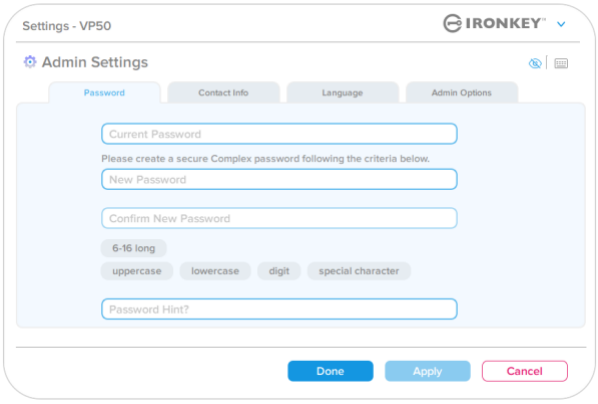



**图 7.2 - 联系信息**

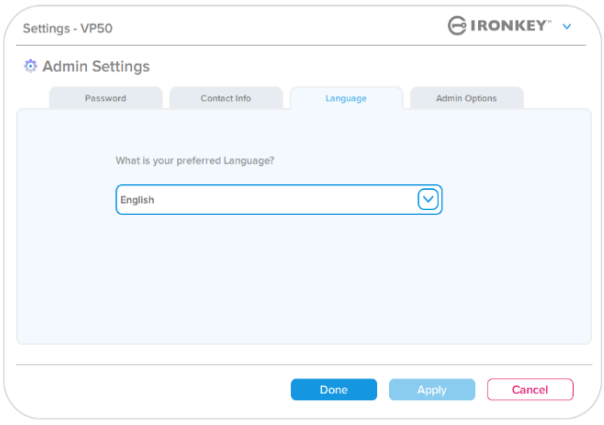



**图 7.3 - 语言选项**

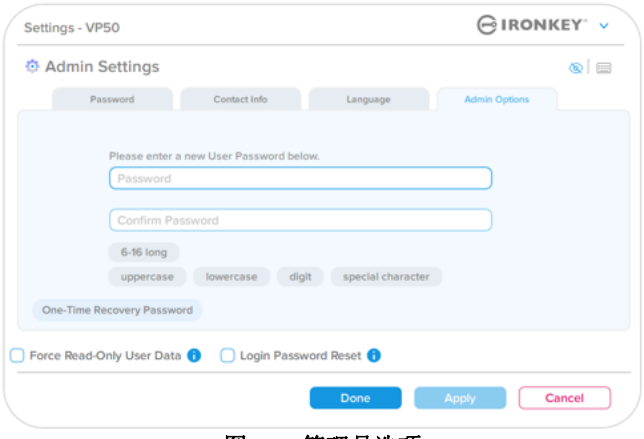



**图 7.4 - 管理员选项**

## VP50 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)：**
让您可以更改自己的用户密码和/或提示。（*图 7.5*）

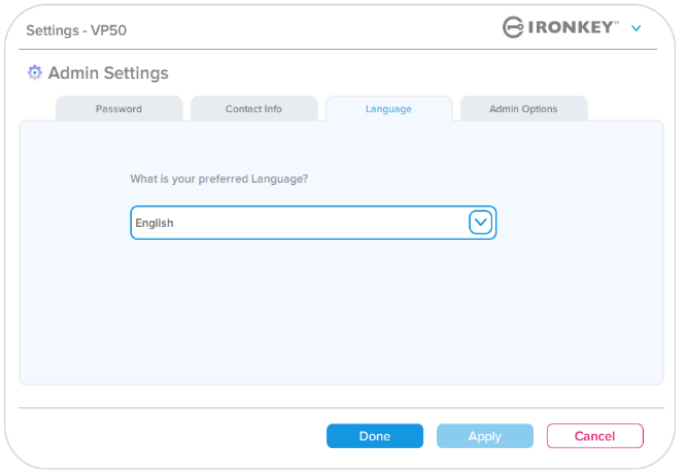



**图 7.5 - 密码选项（管理员已启用：用户登录）**

**联系信息 (Contact Info)：**
让您可以添加/查看/更改自己的联系信息。（*图 7.6*）

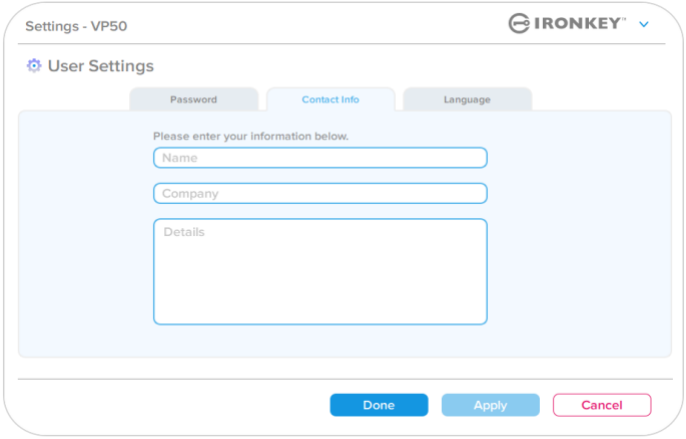



**图 7.6 - 联系信息（管理员已启用：用户登录）**

**语言 (Language)：**
让您可以更改当前语言选择。（*图 7.7*）

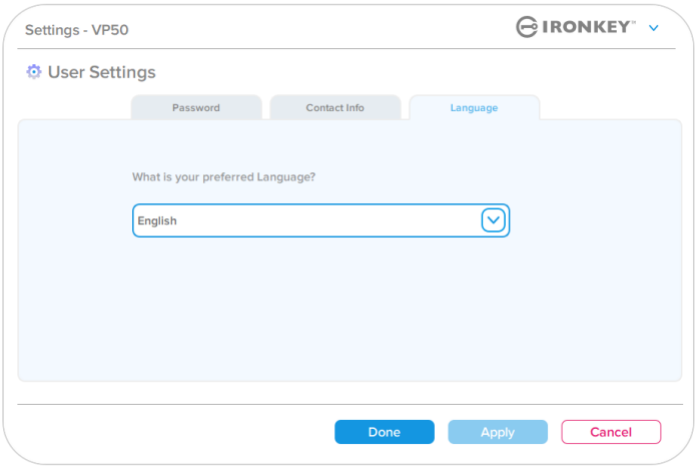



**图 7.7 - 语言设置（管理员已启用：用户登录）**

**注意：**使用用户密码登录时，无法访问管理员选项。

## VP50 设置

### 用户设置：管理员未启用

如第 12 页所述，如果在初始化 VP50 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 VP50 设置：

### 更改和保存设置

- 每当 VP50 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 7.11）

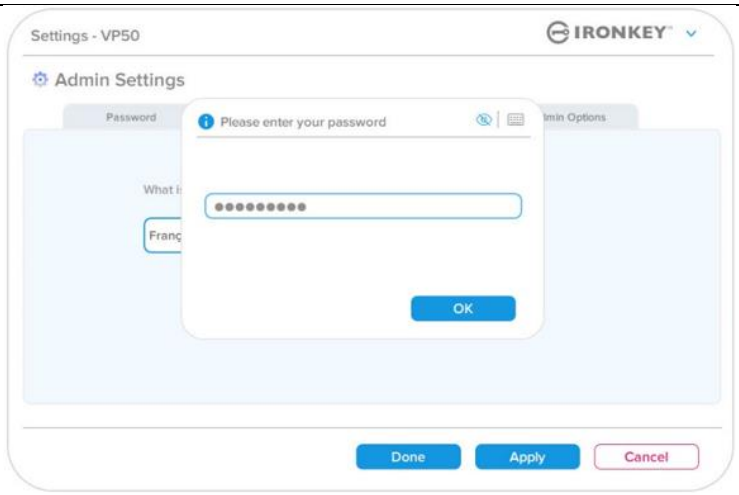



**图 7.11 - 用来保存 VP50 设置更改的“密码提示”屏幕**

**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) 对话框，并返回到 VP50 设置菜单。

# 管理员功能

**用于重置用户密码的选项**

如果忘记用户密码或创建了临时用户密码并希望下次用户登录时强制更改密码，可以利用管理员配置功能，通过多个方法安全地重置用户密码。以下功能有助于重置用户密码：

**用户密码重置：**

在“管理员选项”(Admin Options) 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 8.1**）

**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）。

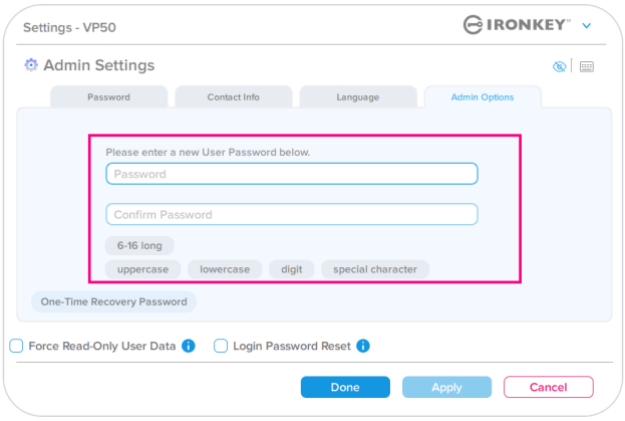



**图 8.1 - 管理员选项/用户密码重置**

**登录密码重置：**

启用登录密码重置后，会**强制用户使用管理员设定的临时密码进行登录**，然后将其更改为用户选择的密码。当需要将闪存盘提供给另一个人使用时，这会很有帮助。（**参见图 8.2A 和 8.2B**）

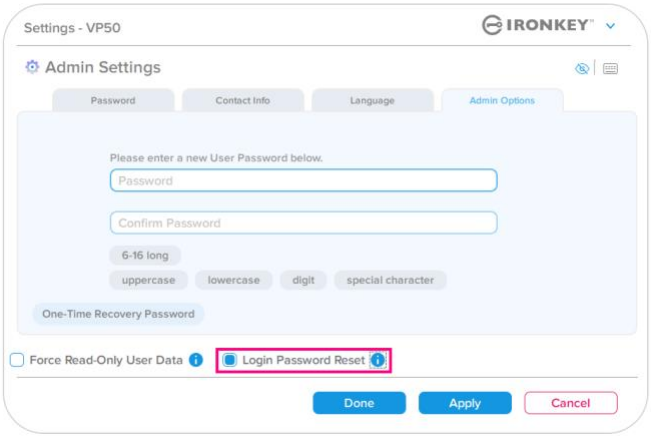



**图 8.2A - “登录密码重置”按钮**

**注意：**应用这项重置后，会在下次用户登录成功后生效。根据初始化过程中设定的原始选项（复杂或口令选项）自动应用密码要求条件。

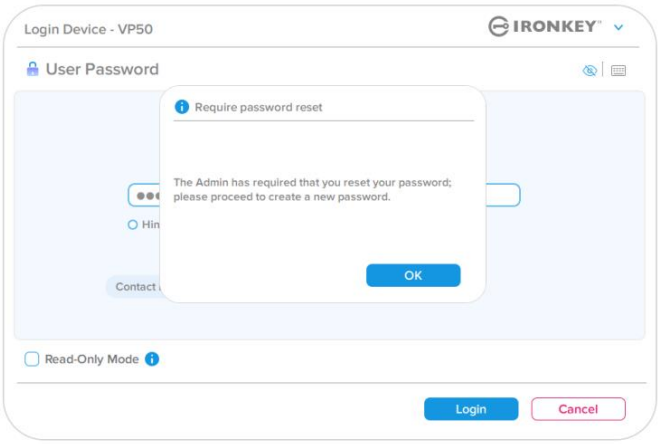



**图 8.2B - 输入用户密码后的重置通知**

# 管理员功能

## 一次性恢复密码

本部分介绍启用和使用一次性恢复密码功能的流程。

### 一次性恢复密码

**第 1 步：**一次性恢复密码功能是非常有用的一次性密码，当忘记用户密码时，可启用该功能帮助恢复和重置用户密码。单击“管理员选项”(Admin options) 菜单中的“一次性恢复密码”(One-Time Recovery Password) 按钮，启动该流程。**（图 8.4）**

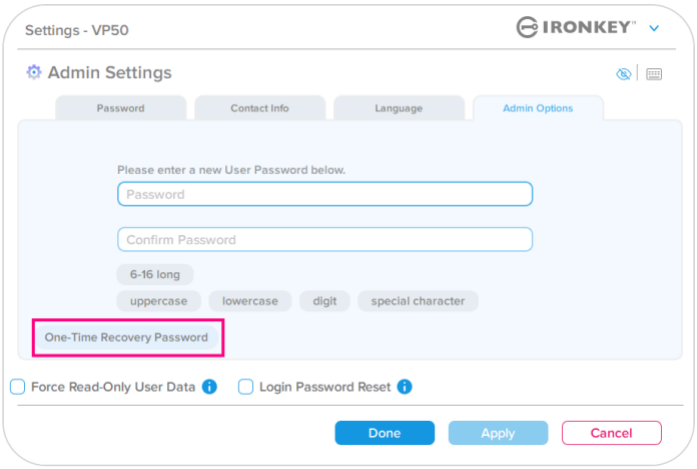



**图 8.4 - “一次性恢复密码”按钮**

**第 2 步：**使用设备初始化时所设定的同一密码条件来创建一次性恢复密码（复杂或口令）。

**注意：**应用更改需要提供管理员密码。

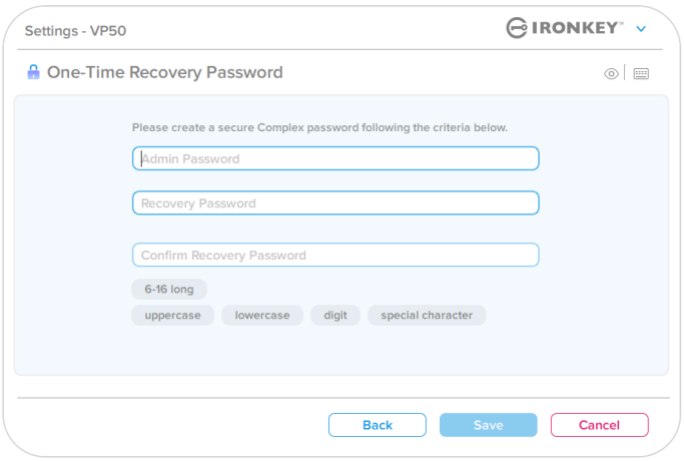



**图 8.5 - 一次性恢复密码设置**

使用一次性恢复密码

**第 1 步：**创建一次性恢复密码后，下次登录时一个新按钮会出现在**用户密码 (User Password)** 登录屏幕中。单击**恢复密码 (Recovery Password)** 按钮来启动该流程。

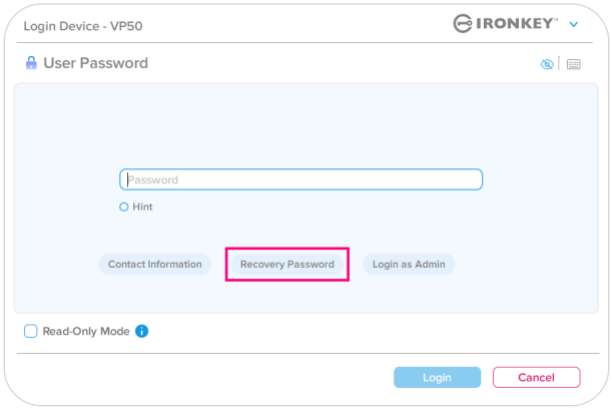



**图 8.6 - “恢复密码”按钮**

**第 2 步：恢复密码 (Recovery Password)** 屏幕会出现，您可以在此输入恢复密码并创建新的用户密码。（图 8.7）

**重要事项：**一次性恢密码也会利用内置的安全功能来跟踪失败的登录尝试次数，**使用一次性恢复密码登录失败 10 次后该密码会被停用**，必须以管理员身份登录后进行重新启用。（参见第 18 页和第 30 页，了解更多详情）

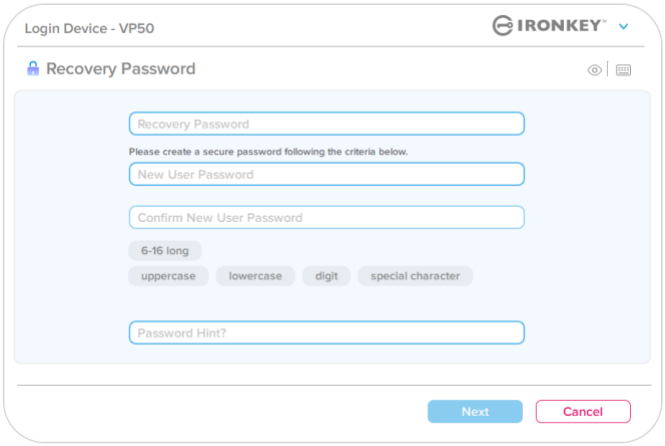



**图 8.7 - 恢复密码菜单**

**第 3 步：**成功后，您会返回到**用户密码 (User Password)** 屏幕。**恢复密码 (Recovery Password)** 按钮现在已消失，而在**第 2 步**中输入的用户密码会变成新的用户密码。（图 8.8）

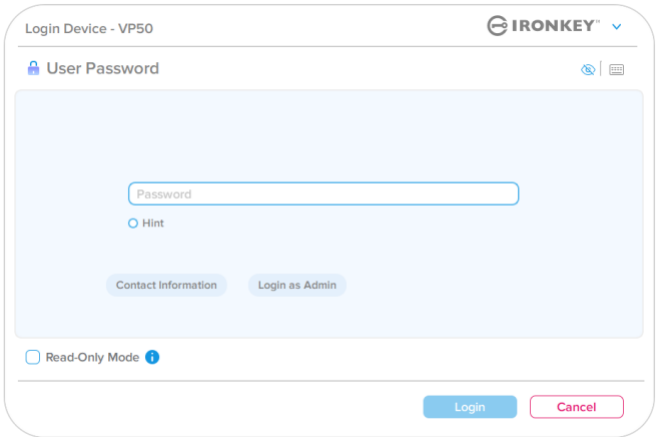



**图 8.8 - “用户密码登录”屏幕，其中显示“恢复密码”按钮在成功使用后消失。**

# 管理员功能

## 强制只读用户数据

通过启用强制只读模式功能，可以限制用户对闪存盘的写入操作。如果只需要读取闪存盘中的文件，这项功能就会有用。

- 要启用用户数据强制只读模式，请依次单击此框和“应用”(Apply)。（**图 8.9**）

  **注意：**这个强制只读模式仅适用于用户，不影响管理员登录。管理员登录仍有读取和写入权限，仍然可以在需要时启动只读模式。

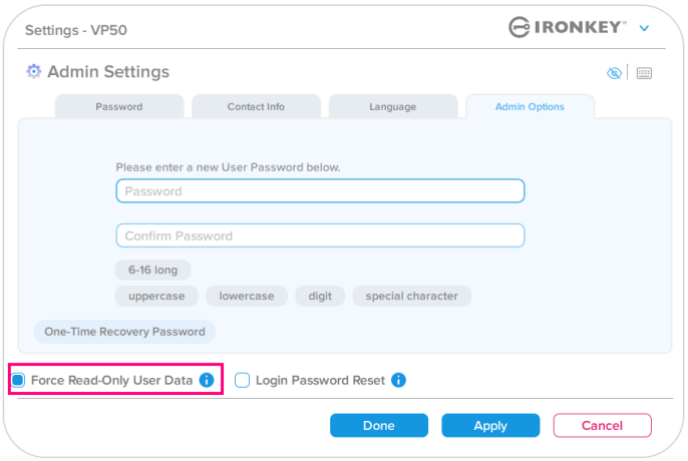



**图 8.9 - 启用“强制只读用户数据”**
**(应用更改需要提供管理员密码)**

- 一旦启用，**只读模式 (Read-Only Mode)** 按钮框会变成蓝色，意味着已为用户密码永久启用强制只读模式，直至被管理员停用为止。（图 8.10）

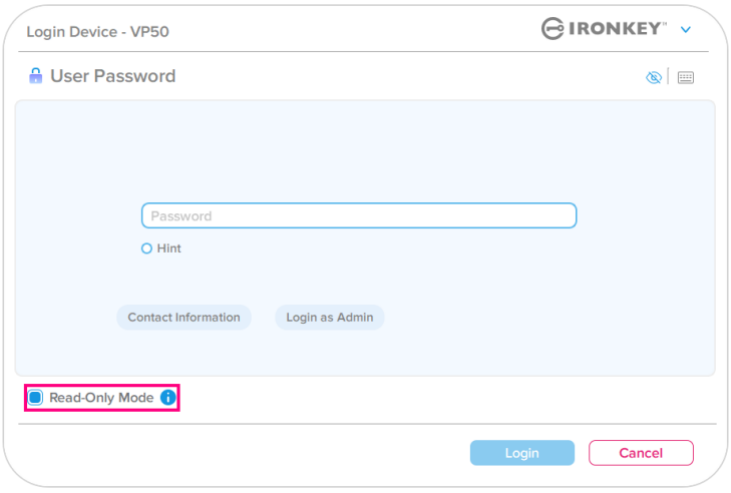



**图 8.10 - 为用户强制启用只读模式，并且只能由管理员停用**

# 帮助和故障排除

## 设备锁定

VP50 包含一项安全性功能，一旦达到登录尝试最大**连续**失败次数（简称 *MaxNoA* ），将阻止对数据分区进行未经授权的访问。默认的“出厂”配置为每种登录方式（管理员/用户/一次性恢复密码）预先配置的值为 10（尝试次数）。

“锁定”计数器跟踪每一次失败的登录，并且在满足下列**两种条件之一** 时进行重置：

**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 9.1）

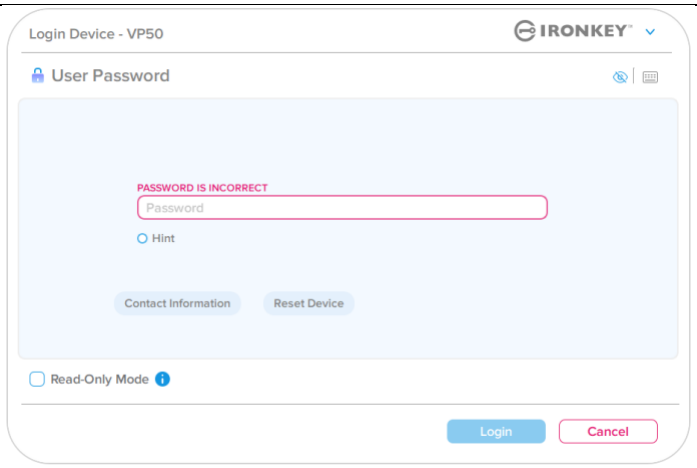



**图 9.1 - 密码错误消息**

- 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 9.2）

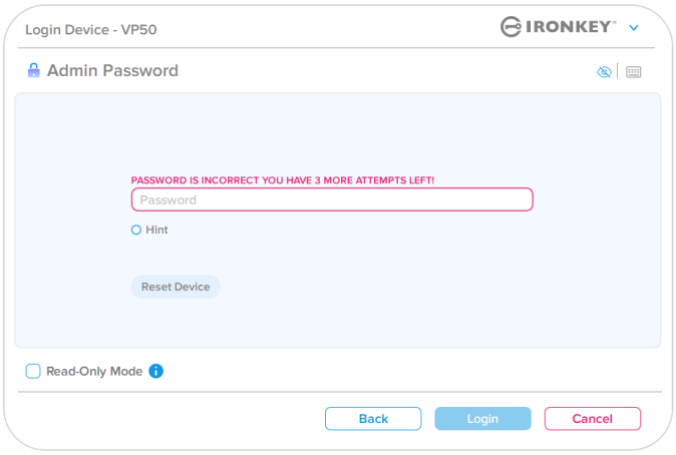



**图 9.2 - 第 7 次密码尝试失败**

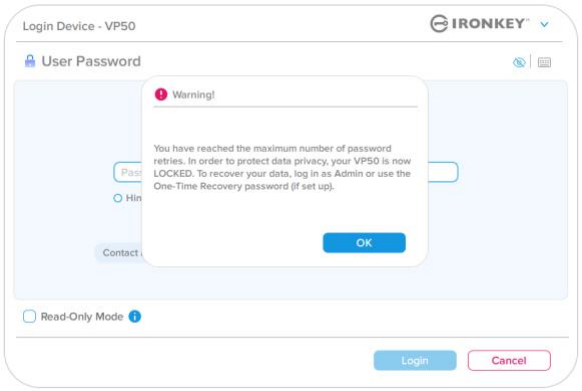
# 帮助和故障排除

## 设备锁定

**重要事项：**第 **10** 次即最后一次登录失败后，根据设备的设置和登录方式（管理员、用户或一次性恢复密码），设备会锁定或重置。锁定会要求使用其他方法登录（若适用），而重置会**格式化闪存盘且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 9.3- 9.6 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：

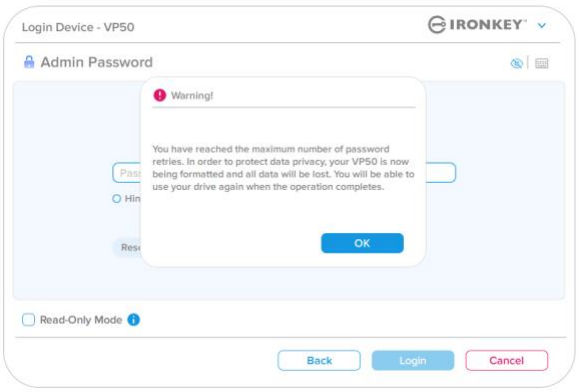
**用户密码：（管理员/用户已启用）**




**设备锁定**

**（图 9.3）**

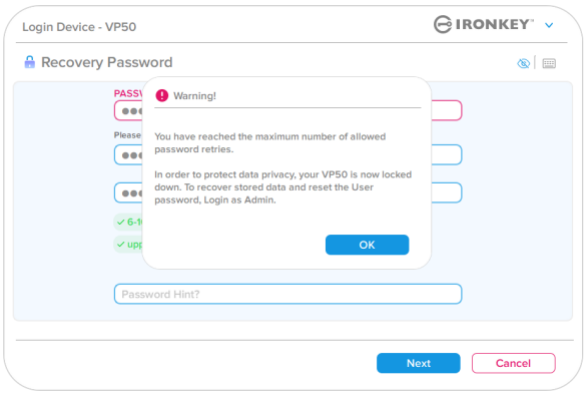
**管理员密码（管理员/用户已启用）**




**设备格式化***

**（图 9.4）**

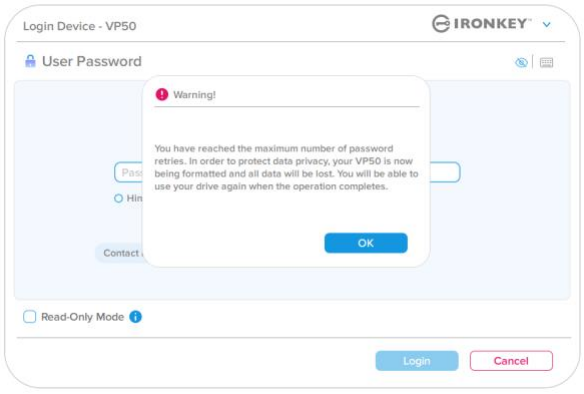
**一次性恢复密码：（管理员/用户已启用）**




**设备锁定**

**（图 9.5）**

**用户密码（管理员未启用）**




**设备格式化***

**（图 9.6）**

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）。如果您使用的是 VP50，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*”。

**注意：*设备格式化会擦除 VP50 安全数据分区中存储的**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 VP50 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 9.7*** 和 **9.8**）

- 您可以通过该选项新建密码，但是为了保护您的数据隐私，VP50 会被格式化。这意味着在这个过程中所有数据会被擦除。*

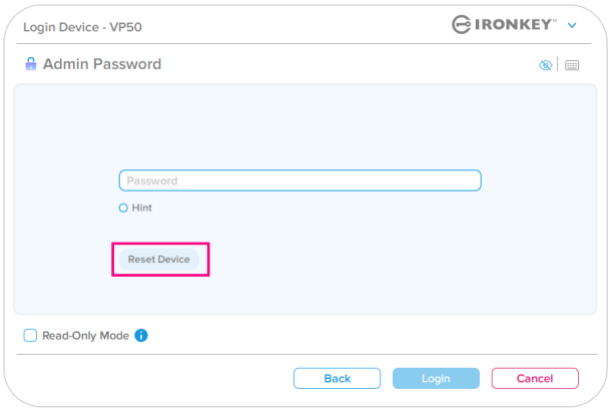



**图 9.7 - 管理员密码：“重置设备”按钮**

- **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*) 进行确认，也可以 2) 单击“取消”(Cancel) 以返回登录窗口。（参见图 9.8）

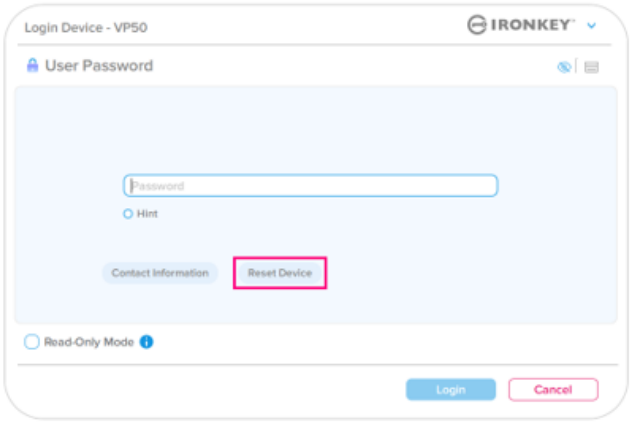



**图 9.8 - 用户密码（管理员/用户未启用）重置设备**

- 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，可以提供有关密码的线索。

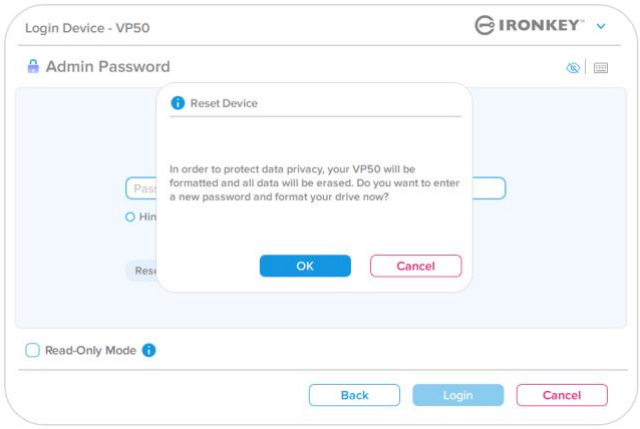



**图 9.9 - 重置设备确认**

# 帮助和故障排除

## 驱动器号冲突：Windows 操作系统

- 如本手册“*系统要求*”部分（第 3 页）所述，VP50 需要在驱动器号分配“空缺”之前的最后一个物理磁盘**后**存在两个连续的驱动器号（参见*图 9.10*）。这**不**属于网络共享，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是可用的。

- 这意味着，Windows 为 VP50 分配的驱动器号可能已被网络共享或通用命名约定 (UNC) 路径占用，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）。如本手册“*系统要求*”部分（第 3 页）所述，VP50 需要在驱动器号分配“空缺”之前的最后一个物理磁盘**后**存在两个连续的驱动器号（参见*图 9.10*）。这**不**属于网络共享，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是可用的。

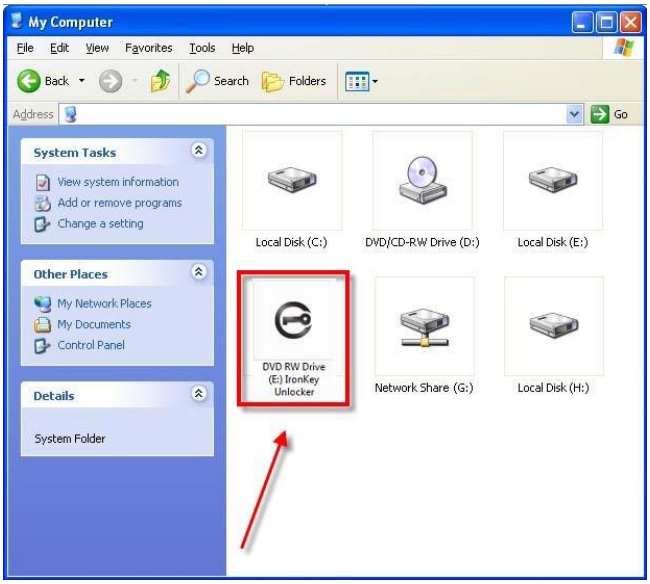



**图 9.10 - 驱动器号示例**

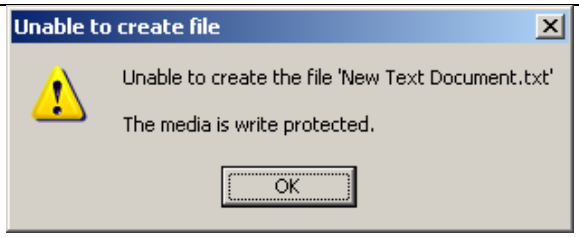
在本例中（图 9.10），VP50 使用驱动器 F:，这是驱动器 E: 之后第一个可供使用的驱动器号（E: 是驱动器号空缺之前的最后一个物理磁盘。）由于驱动器号 G: 是一个网络共享而不是硬件配置文件的一部分，所以 VP50 可能会尝试将它用作其第二个驱动器号，从而导致冲突。

如果您的系统中没有网络共享，但 VP50 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。

# 帮助和故障排除

## 错误消息

| | |
|---|---|
| **无法创建文件：**<br>当以只读模式登录并尝试在安全数据分区中**创建**文件或文件夹时，会出现此错误消息。 |  <br>**图 9.11 – “无法创建文件”错误** |
| **复制文件或文件夹时出错：**<br>当以只读模式登录并尝试向安全数据分区**复制**文件或文件夹时，会出现此错误消息。 |  <br>**图 9.12 – “复制文件或文件夹时出错”错误** |
| **删除文件或文件夹时出错：**<br>当以只读模式登录并**删除**安全数据分区中的文件或文件夹时，会出现此错误消息。 |  <br>**图 9.13 – “删除文件或文件夹出错”错误** |

**注意：**如果您在只读模式下登录，并且希望解锁设备以获得完全的读/写权限来访问安全数据分区，则必须关闭 VP50 并重新登录，在登录之前取消选中“只读模式”(Read-Only Mode) 复选框。

# IRONKEY™ Vault Privacy 50 (VP50)
# 加密 USB 3.2 Gen 1 隨身碟

*使用者指南*

內容


圖 1：IronKey VP50

## 簡介

Kingston IronKey Vault Privacy 50 (VP50) 是一款高階型 USB 隨身碟，可提供企業級安全、符合 FIPS 197 並採用 XTS-AES 256 位元硬體加密，包括數位簽章韌體的 BadUSB 防護，以及防範暴力密碼破解。VP50 於美國組裝，也符合 TAA 規範。由於是使用者可直接控制的加密儲存裝置，相較於網路和雲端服務，VP50 系列在保護資料方面表現更為優異。

VP50 支援具有複雜或密碼片語模式的多密碼 (管理員、使用者和一次性恢復) 選項。在忘記其中一個密碼時，多密碼選項增強了還原資料存取的能力。除了支援傳統的複雜密碼外，新的密碼片語模式還允許輸入數位 PIN、句子、字詞清單，甚至是 10 到 64 個字元長度的歌詞。管理員可以啟用使用者和一次性恢復密碼或重設使用者密碼以還原資料存取。

為協助輸入密碼，可以點擊「眼睛」 符號顯示輸入的密碼，減少導致登入失敗的拼寫錯誤。暴力密碼破解保護會在連續輸入 10 次無效密碼時將使用者或是一次性恢復密碼鎖定，並且在連續輸錯 10 次管理員密碼後加密清除硬碟資料。

為了防範不受信任系統中的潛在惡意軟體，管理員與使用者皆可設定唯讀模式以便對硬體進行寫入保護；此外，內建的虛擬鍵盤可以防範鍵盤記錄程式和螢幕記錄程式記錄密碼。

符合 FIPS 197 及 TAA 規範，組織可以自訂與配置具有產品 ID (PID) 的 VP50 系列隨身碟，以便與標準端點管理軟體整合，透過 Kingston 的客製化方案符合企業 IT 和網路安全要求。

中小型企業可以利用管理員角色在本地管理其隨身碟，例如使用管理員設定或重設員工的使用者密碼或一次性恢復密碼、恢復鎖定隨身碟上的資料存取權限，並在需要取證時遵守法律法規。

VP50 享有 5 年有限產品保固及免費技術支援服務。

**IronKey Vault Privacy 50 特色**

- 符合 FIPS 197 並採用 XTS-AES 256 位元硬體加密 (加密功能不可關閉)
- 暴力密碼破解與 BadUSB 攻擊保護
- 多密碼選項
- 複雜或密碼片語模式
- 點擊眼睛按鈕可顯示輸入的密碼，藉此減少失敗的登入嘗試。
- 虛擬鍵盤可協助防範鍵盤記錄程式和螢幕記錄程式
- 雙重唯讀 (寫入保護) 設定可避免隨身碟內容遭到變更或是防範惡意軟體
- 中小型企業可以使用管理員角色在本地管理隨身碟
- Windows 或 macOS 相容 (詳情請查詢資料集)

## 關於本使用手冊

此使用者手冊涵蓋 IronKey Vault Privacy 50 (VP50)，係依據原廠影像且不含自訂配置。

## 系統需求

| 電腦平台 | 電腦作業系統支援 |
|---|---|
| • Intel, AMD & Apple M1 SOC<br>• 15 MB 可用硬碟空間<br>• 可用的 USB 2.0 - 3.2 連接埠<br>• 最後一個實體磁碟之後的兩個連續磁碟機代號*<br><br>*注意：請參閱第 32 頁「磁碟機代號衝突」。 | • Windows 11<br>• Windows 10<br>• Windows 8.1 |
| **Mac 平台**<br>• 15 MB 可用硬碟空間<br>• USB 2.0 - 3.2 連接埠 | **Mac 作業系統支援**<br>• macOS X (v. 10.13.x – 12.x.x) |

## 建議

為確保提供 VP50 裝置充足的電力，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 VP50 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 VP50 預設格式化為 FAT32 檔案系統。其適用於 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其中的資料。

### 使用提醒

為確保您的資料安全，Kingston 建議您：

- 在目標系統上設定和使用 VP50 之前，在您的電腦上執行病毒掃描
- 在公共或不熟悉的系統上使用隨身碟時，您可能需要在裝置上設定唯讀模式，以協助保護隨身碟免受惡意軟體的侵害
- 不使用時鎖定裝置
- 在拔下隨身碟之前先將隨身碟退出
- 當 LED 燈亮起時，切勿切斷裝置電源。如此可能損壞隨身碟並需要重新格式化，此時將會刪除您的資料
- 切勿將您的裝置密碼告訴任何人

### 尋找最新更新和資訊

造訪 kingston.com/support 以獲得最新的隨身碟更新、常見問題解答、文件和其他資訊。

**注意：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 VP50 具備強大的安全防護。其中包括針對暴力密碼破解的保護，該項保護將密碼嘗試限制設定為 10 次，藉此阻止攻擊者猜測密碼。當達到隨身碟的限制時，VP50 將自動清除加密資料 – 將自身格式化回復到出廠設定。

### 多密碼

VP50 支持多密碼作為一項主要功能，以幫助避免忘記一個或多個密碼時資料遺失。啟用所有密碼選項後，您可以使用三種不同密碼 – 管理員、使用者和一次性恢復密碼，來還原資料存取權限。

VP50 允許您選取兩個主要密碼 – 管理員密碼 (英文稱為 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。此外，管理員可以為使用者設定一次性恢復密碼，為使用者提供登入和重設使用者密碼的方式。

使用者也能存取硬碟，但與管理員相比則權限有限。如果您忘記了這兩個密碼中的其中一者，則可以使用另一組密碼來存取並取回資料。並將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。使用者可使用一次性恢復密碼以便在需要時重設使用者密碼。

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。VP50 可以重設並重複使用，但先前儲存其中的資料將被永久清除。

### 密碼模式

VP50 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

### 複雜密碼

VP50 支援 10 到 64 個字元的密碼片語。密碼片語沒有規則，但是如果正確使用，可以提供極高程度的密碼保護性。

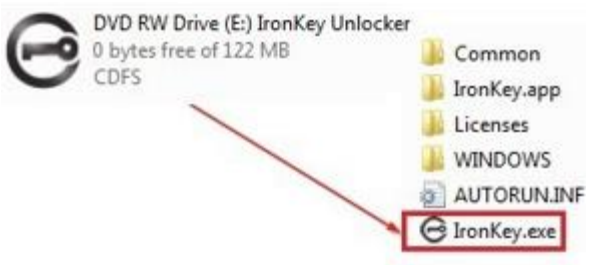
密碼片語基本上是字元的任意組合，包括其他語言的字元。與 VP50 隨身碟一樣，密碼片語可以與隨身碟設定的語言相符。這能讓您使用多個單字、一個片語、歌曲中歌詞和一行詩歌等，強大的複雜密碼是攻擊者最難猜到的密碼類型之一，而且使用者相對好記。

# 設定我的裝置

為確保 IronKey 加密 USB 隨身碟具有足夠的電源供應，請將其直接插入筆記型電腦或桌上型電腦的 USB 2.0/3.0 連接埠。避免將其連接到具有 USB 連接埠的任何週邊裝置，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。

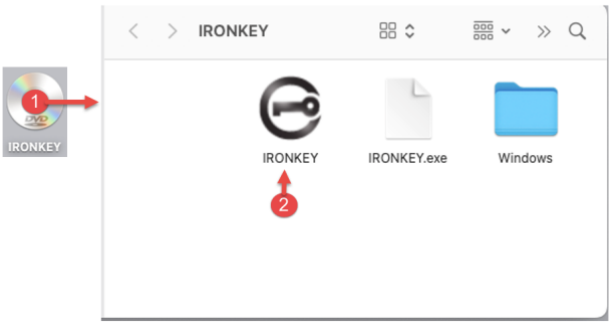
## 裝置存取 (Windows 環境)

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 偵測到它。

| | |
|---|---|
| • Windows 8.1/10/11 使用者會接收到裝置驅動程式通知。(圖 3.1) |  <br>**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)<br>• 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。在下圖中，磁碟機代號為 (E:)。 |  <br>**圖 3.2 - File Explorer Window/IronKey.exe** |

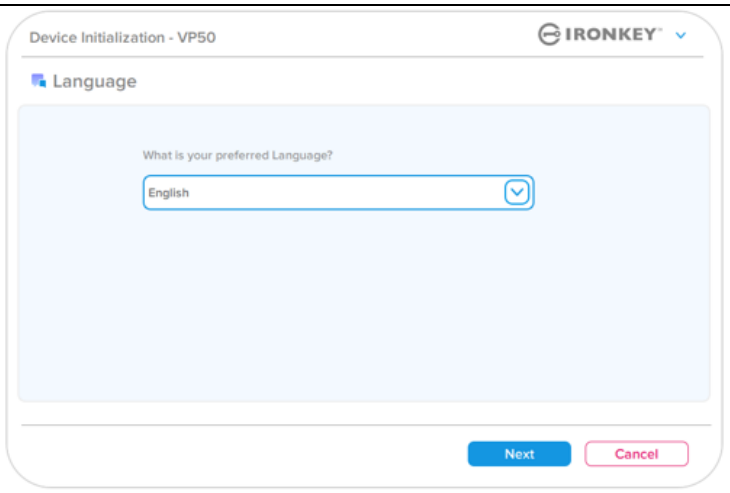
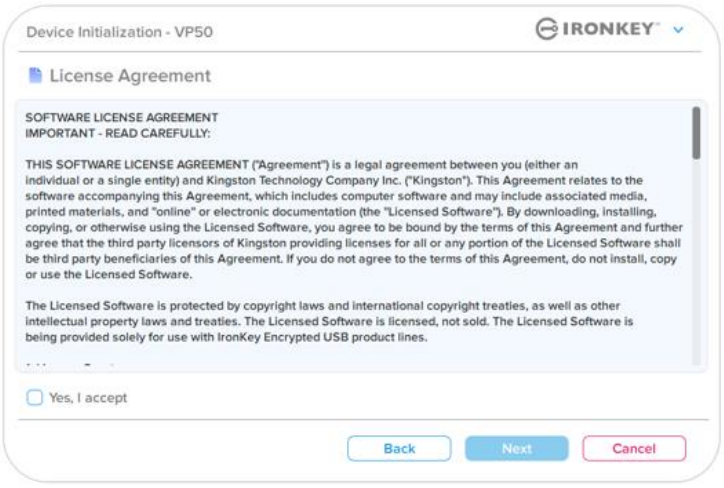
## 裝置存取 (macOS 環境)

將 VP50 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，您將會在桌面看見 IKVP50 (或 IRONKEY) 卷宗。(圖 3.3)

| | |
|---|---|
| • 連按兩下 IronKey CD-ROM 圖示。<br>• 接著連按兩下圖 3.3 顯示視窗中找到的 IKVP50 (或 IronKey.app) 應用程式圖示。以此開始初始化流程。 |  <br>**圖 3.3 - IKVP 卷宗** |

## 裝置使用 (Windows & macOS 環境)

### 語言和 EULA

| | |
|---|---|
| 從下拉式選單中選擇語言偏好，然後按一下「**Next**」(下一步)。(詳見圖 4.1) |  <br>**圖 4.1 - 語言選項** |
| 檢閱授權合約然後按一下「**Next**」(下一步)。<br><br>注意：您必須先接受授權合約才能繼續，否則「**Next**」(下一步) 按鈕將呈現在停用狀態。(圖 4.2) |  <br>**圖 4.2 - 授權合約** |

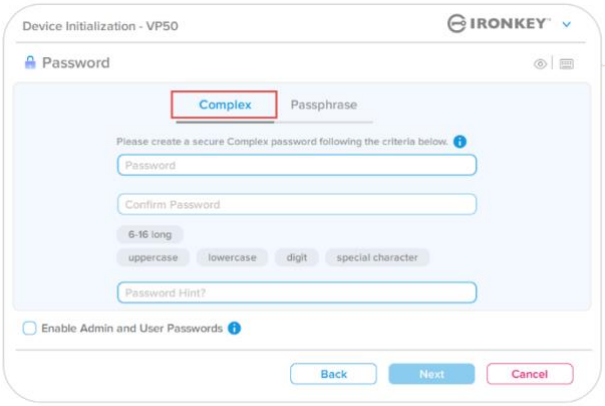
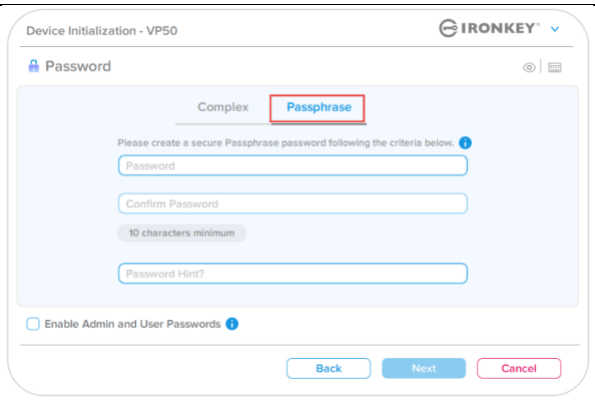
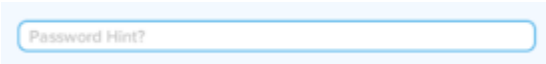
# 裝置初始化

## 密碼選擇

在密碼提示畫面上，您能夠使用複雜密碼或密碼片語密碼模式建立密碼，以保護 VP50 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片語模式，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：

| | |
|---|---|
| **複雜密碼**<br>• 必須包含 6 個以上的字元 (最多 16 個字元)。<br>• 必須包含下列的三 (3) 個條件：<br>○ 大寫<br>○ 小寫<br>○ 數字<br>○ 特殊字元 (!,$,&, etc..) |  <br>**圖 4.3 - 複雜密碼** |
| **密碼片語密碼**<br>• 必須包含：<br>○ 最少 10 個字元<br>○ 最多 64 個字元 |  <br>**圖 4.4 - 密碼片語密碼** |
| **密碼提示 (非必選)**<br>如果您忘記密碼，密碼提示可提供有關密碼內容的線索。<br>**注意**：提示「不得」與密碼完全相符。 |  <br>**圖 4.5 - 密碼提示欄位** |

裝置初始化

## 有效與無效的密碼

如果是**有效的**密碼，在條件符合時，「密碼條件方塊」將會以**綠色**顯示。(詳見圖 4.6a-b)
注意：一旦符合最低限度的三個密碼條件，第四個條件方塊將變為灰色，表示此條件非必須。(圖 4.6b)

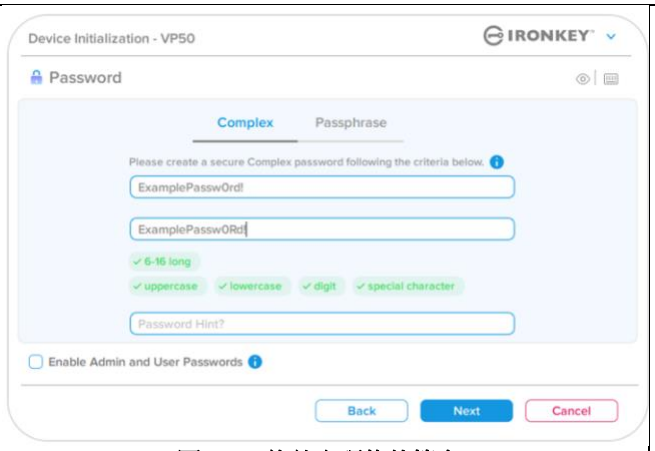



**圖 4.6a - 複雜密碼條件符合**

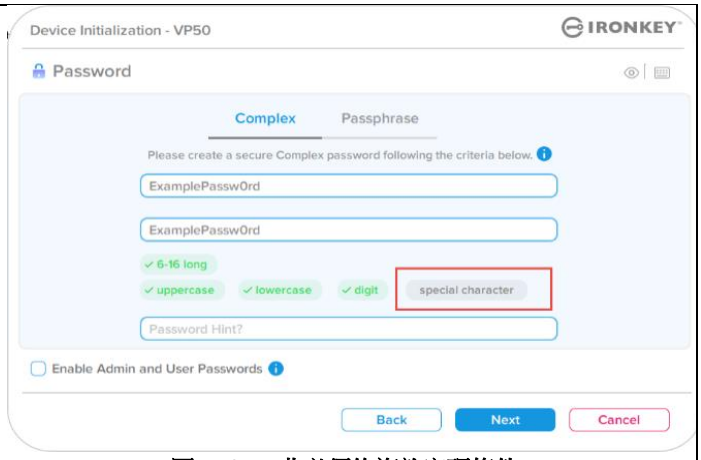



**圖 4.6b – 非必須的複雜密碼條件**

如果是**無效的**密碼，「密碼條件方塊」將會以**紅色**顯示，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片語密碼。

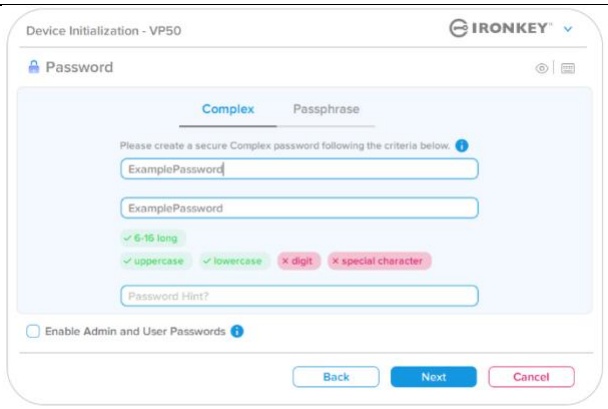



**圖 4.7 - 密碼條件不符**

# 裝置初始化

## 虛擬鍵盤

VP50 具有可防範鍵盤記錄程式的虛擬鍵盤。

- 若要利用**虛擬鍵盤**，請在**裝置初始化**畫面的右上角找到鍵盤按鈕然後加以選取。

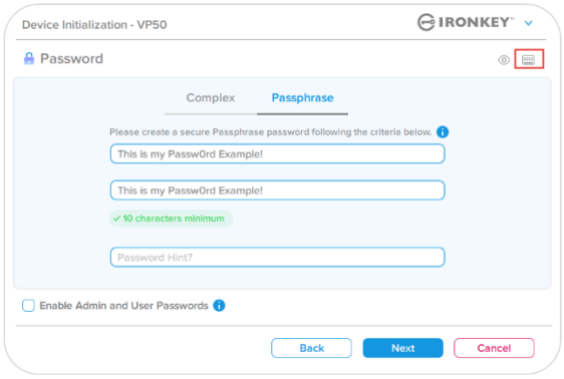



**圖 4.8 - 啟用虛擬鍵盤**

- 出現虛擬鍵盤後，您還可以啟用**螢幕記錄程式保護**。在使用此功能時，所有按鍵將短暫變為空白。這是可預期的行為，因為它可避免螢幕記錄程式擷取您所點擊的內容。
- 為使得此功能更加強大，您還可以選擇鍵盤右下角的**隨機化**，以便隨機化虛擬鍵盤。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 ，可以點擊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。

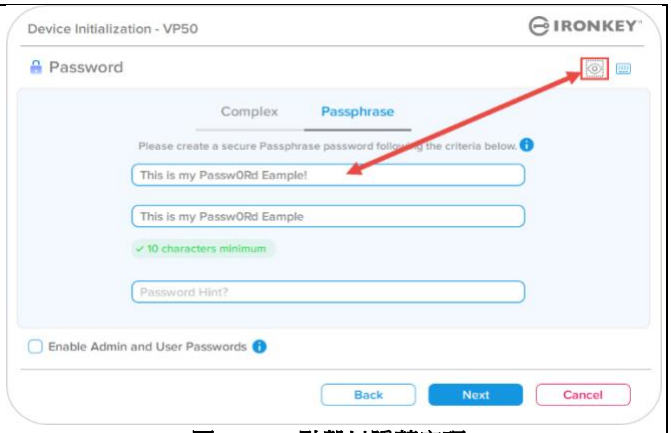



**圖 4.10 – 點擊以隱藏密碼**

若要**顯示**隱藏的密碼，請按一下藍色圖示。

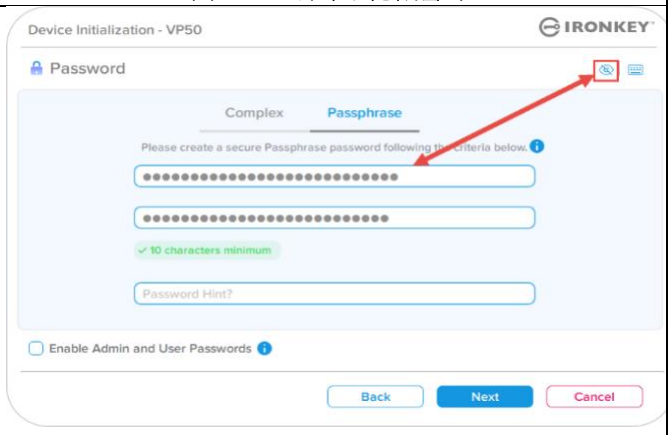



**圖 4.11 – 點擊以顯示密碼**

# 裝置初始化

## 管理員和使用者密碼

藉由啟用「管理員和使用者密碼」，您可以利用多密碼功能，擁有管理員角色者可以利用此功能管理兩個帳戶。選取**「管理員和使用者密碼」**允許在忘記其中一個密碼的情況下，使用另一個替代方案存取隨身碟。

在**管理員和使用者密碼**啟用的情況下，您也可以存取：

- 一次性恢復密碼
- 強制使用者以唯讀模式登入
- 使用者密碼重設
- 強制使用者於登入時重設密碼

若要瞭解關於這些功能的更多資訊，請瀏覽本使用者指南中的第 25 頁。

- 若要啟用**管理員和使用者密碼，**請按一下**啟用管理員和使用者密碼**旁邊的方塊，然後在完成選擇有效的密碼之後選取**「Next」**(下一步)。(圖 4.12)

- 若此功能已經**啟用**，則在此畫面中選擇的密碼將會是**管理員密碼**。按一下**「Next」**(下一步) 以前進至**「User Password」**(使用者密碼) 畫面，可在此畫面中為使用者選擇密碼。

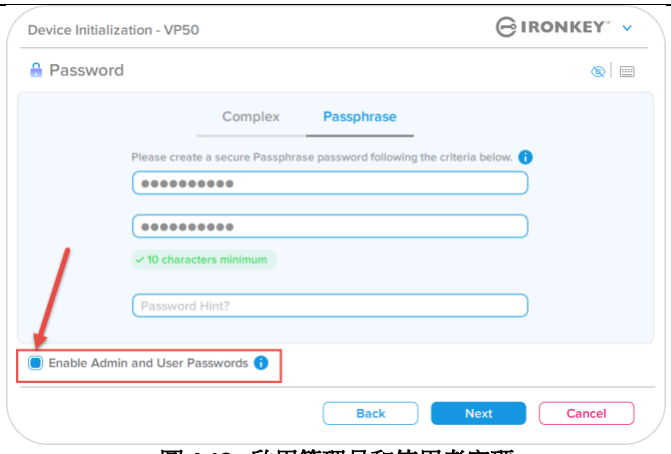



**圖 4.12 - 啟用管理員和使用者密碼**

**注意：啟用管理員和使用者密碼為選擇性質。**

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，此組態也被稱為**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)。

**注意：**在本文件的其他部分，**管理員和使用者密碼**的將稱為**管理員角色**。

# 裝置初始化

## 管理員和使用者密碼

- 如果已經在上一個畫面中**啟用**管理員角色，則後續畫面將會提示輸入**使用者密碼** (圖 4.13) 與管理員密碼相比，使用者密碼在功能上會受到限制，本使用者指南會在稍後討論更多細節。(請參閱第 23 頁。)

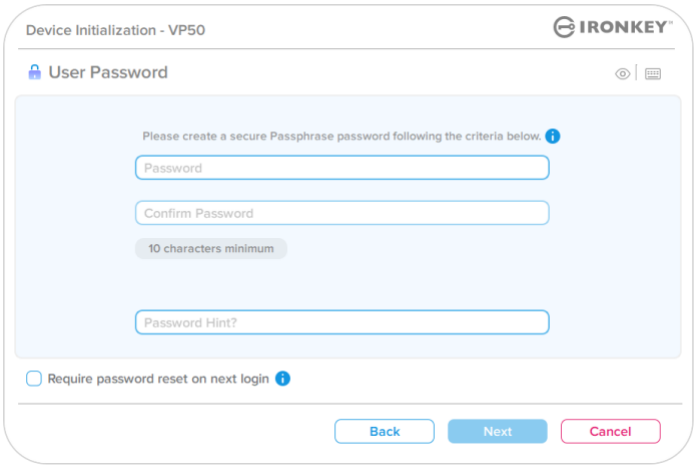



**圖 4.13 - 使用者密碼 (管理員與使用者已啟用)**

**注意：**選擇的「密碼選項」(複雜或密碼片語) 條件將會延續至使用者密碼、一次性密碼恢復，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重設裝置後方可變更。

- **下次登入時需重設密碼**功能 (位於**圖 4.13** 的左下角) 僅適用於使用者密碼，啟用此功能以便在初始化過程中強制使用者以管理員設定的暫時密碼登入，然後在暫時密碼通過驗證之後，將密碼變更為使用者自選的密碼。如果隨身碟會提供給其他人使用，這個功能會很有用。**(圖 4.14)**

  **注意：**為安全起見，新的密碼不可以和暫時密碼相同。

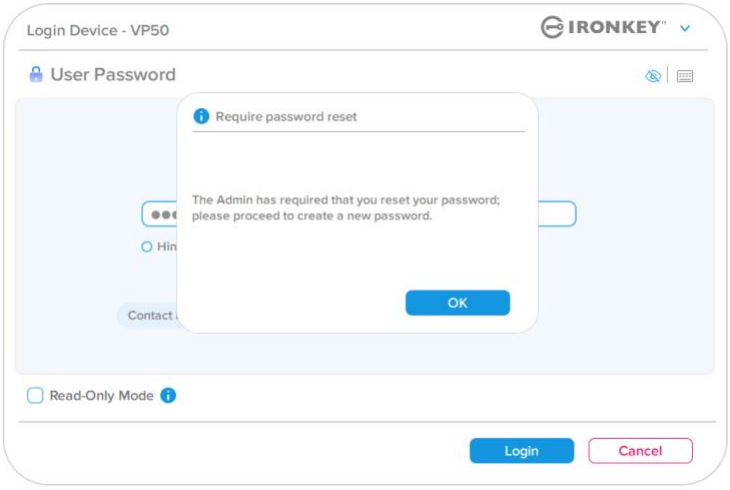


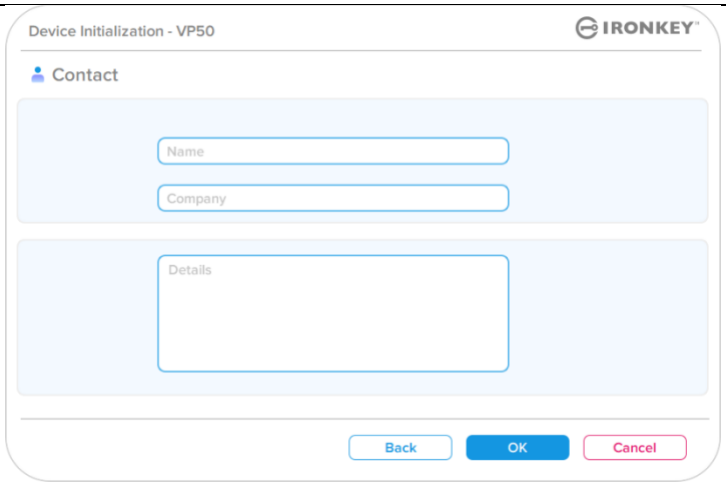

**圖 4.14 - 下次登入時需重設密碼 (用於使用者密碼)**

# 裝置初始化

## 聯絡資訊

在提供的文字方塊中輸入您的聯絡資訊。(詳見圖 4.14)

**注意：**您在這些欄位中輸入的資訊可能並未包含您在步驟 3 中建立的密碼字串。(但是這些欄位是選填性質的，如果需要可以留空。)

| | |
|---|---|
| 「**Name**」(名稱) 欄位可包含多達 32 個字元，但不得包含**確切**密碼。<br><br>「**Company**」(公司) 欄位可包含多達 32 個字元，但不得包含**確切**密碼。<br><br>「**Details**」(詳細資訊) 欄位可包含多達 156 個字元，但不得包含**確切**密碼。 |  <br>**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。

## 裝置使用 (Windows & 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 VP50 應用程式將啟動，並且先顯示使用者密碼登入畫面。您可以利用「使用者密碼」在此處登入，查看輸入的任何聯絡資訊，或是以管理員身分登入 (圖 5.1)。藉由按一下「以管理員身分登入」按鈕 (如下所示)，應用程式將會切換至「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 5.2)

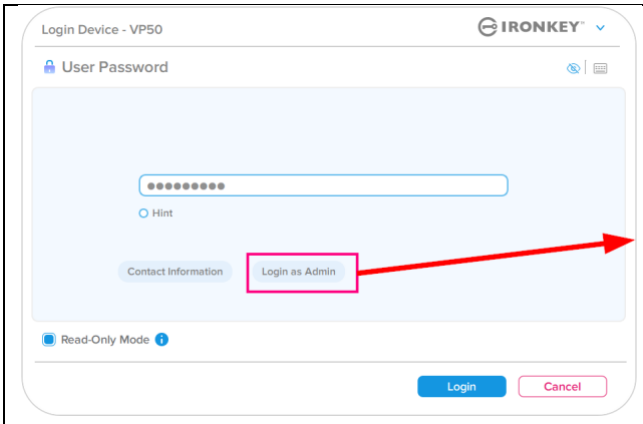



圖 5.1 - 使用者密碼登入 (管理員已啟用)

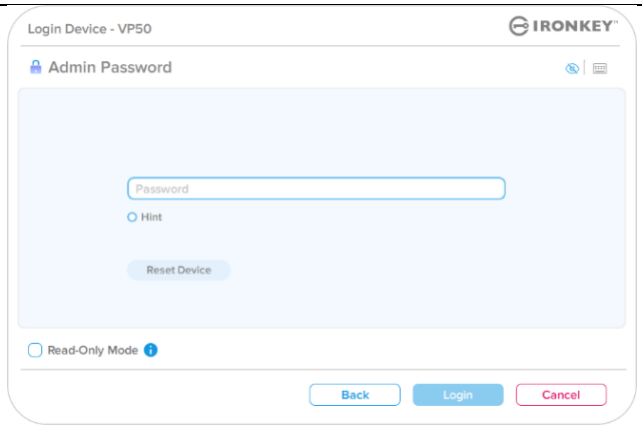



圖 5.2 - 管理員密碼登入

### 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」功能以獲得裝置的完整功能，但還是可以在使用者 (單一密碼，單一使用者) 組態中初始化 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 5.3)

**注意：**若要啟用管理員與使用者密碼，請使用「**Reset Device**」(重設裝置) 按鈕將隨身碟回復至初始化狀態，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。**

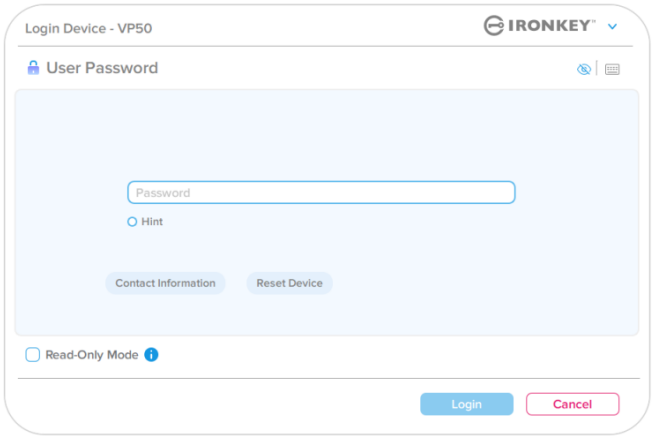



圖 5.3 - 使用者密碼登入 (管理員未啟用)

# 裝置使用

## 在唯讀模式下解鎖

您可以在唯讀狀態下解鎖裝置，可禁止變更 IronKey 隨身碟上的檔案。例如，使用不受信任或未知的電腦時，以唯讀模式解鎖裝置，可避免該電腦上的任何惡意軟體感染您的裝置，或修改您的檔案。

在此模式下運作時，您無法執行任何涉及修改裝置上檔案的操作。
例如，您無法重新格式化裝置，還原、新增或者編輯隨身碟上的檔案。

以唯讀模式解鎖裝置：

1. 將裝置插入電腦的 USB 連接埠，然後執行 **IronKey.exe**。
2. 在輸入密碼方塊下方選取**唯讀模式**。**(圖 5.4)**
3. 輸入您的裝置密碼，然後按一下「**Login**」(登入)。IronKey 現在將會以唯讀模式解鎖。

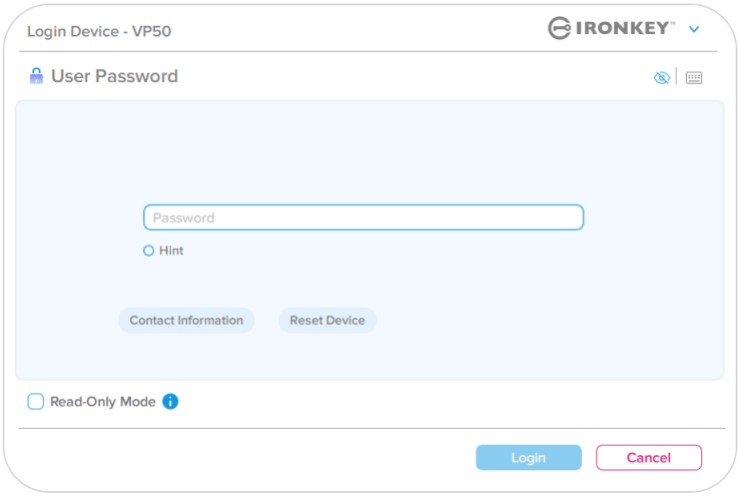



**圖 5.4 - 唯讀模式**

如果您想要解除鎖定隨身碟以獲得安全資料分割區的完整讀取/寫入權限，您必須先關閉 VP50 再重新登入，並且在登入前取消核取「Read-Only Mode」(唯讀模式) 核取方塊。

**注意：**VP50 管理員提供適用於使用者資料的強制唯讀模式選項，這表示管理員可以強制使用者以唯讀狀態解鎖裝置並登入 (詳情請參閱**第 28 頁**)。

# 裝置使用

## 暴力破解保護

**重要須知：**在登入過程中，如果輸入錯誤密碼，您可嘗試第二次登入，但是系統內建的安全性功能 (也稱為暴力破解保護) 會自動記錄嘗試登入失敗的次數。*

如果此數字達到預先設定的 10 次失敗密碼嘗試的數值，行為將會如下：

| **管理員/使用者啟用** | **暴力破解保護<br>裝置行為<br>(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。以管理員身分登入或是使用一次性恢復密碼重設使用者密碼 | 否 |
| 管理員密碼 | 加密清除隨身碟、密碼、設定以及資料永久清除 | **是** |
| 一次性恢復密碼 | 密碼鎖定、恢復密碼按鈕會變成灰色、無法使用的狀態。以管理員身分登入以重設密碼 | 否 |
| **僅使用者<br>單一使用者，單一密碼<br>(管理員/使用者未啟用)** | **暴力破解保護<br>裝置行為<br>(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** |

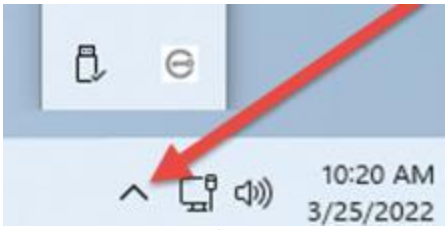
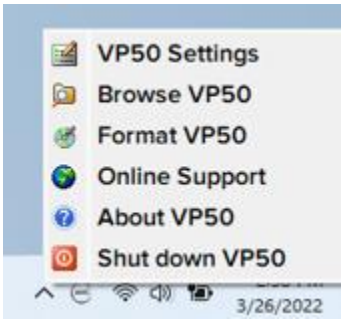
* 成功驗證裝置後，將根據使用的登入方法重設失敗登入計數器。加密清除將會刪除所有密碼、加密金鑰與資料 – **您的資料將會永久遺失。**

## 存取我的安全檔案

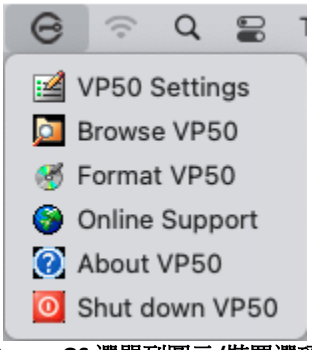
解鎖隨身碟後，您可以存取安全檔案。在隨身碟上儲存或開啟檔案時，檔案會自動加密和解密。這項技術提供您如一般隨身碟正常運作的便利性，同時提供了隨時在線的強大安全性。
**提示**：您也可以在 Windows 工作列中的 **IronKey 圖示**上按一下右鍵然後按一下**瀏覽 VP50** 以存取您的檔案。(圖 6.2)

## 裝置選項 - (Windows 環境)

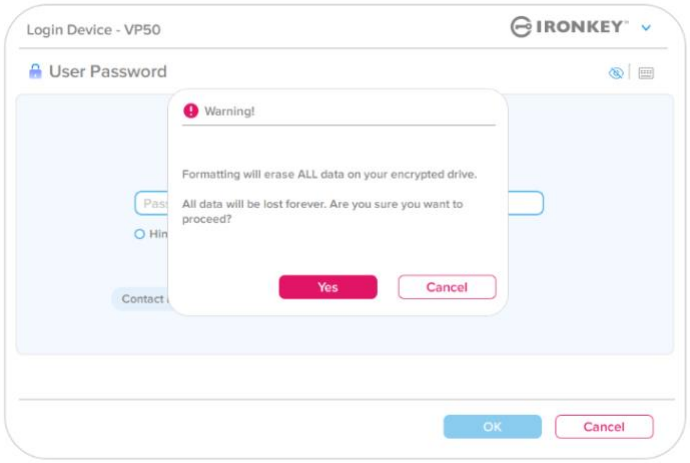
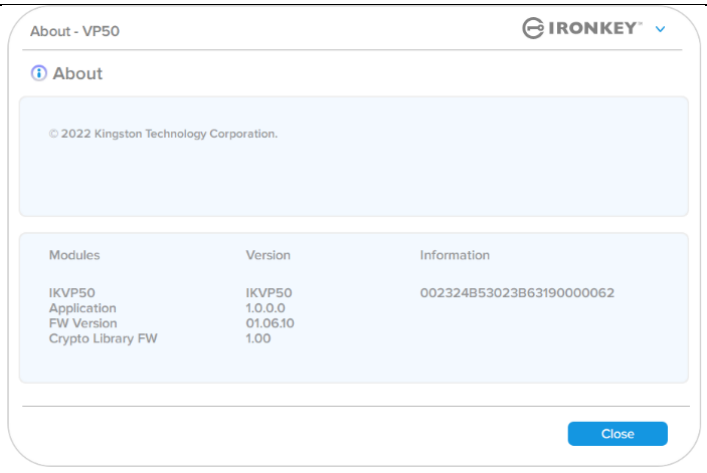
當您登入裝置時，視窗右上角會出現一個 IronKey 圖示。在 IronKey 圖示上按一下右鍵將會開啟選項選單以選取可用的隨身碟選項。(圖 6.2)
有關這些裝置選項的詳細資訊，請參閱本手冊的第 19-23 頁。

| | |
|---|---|
| • 當您登入裝置時，視窗右上角會出現一個 IronKey 圖示。**(圖 6.1)** |  <br>**圖 6.1 - 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 6.2)**<br><br>有關這些裝置選項的詳細資訊，請參閱本手冊的第 19-23 頁。 |  <br>**圖 6.2 - 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 6.3** 所示的 IronKey VP50 圖示位於 macOS 選單中，在選單中可開啟可用的裝置選項。<br><br>有關這些裝置選項的詳細資訊，請參閱本手冊的第 19-23 頁。 |  <br>**圖 6.3 - macOS 選單列圖示/裝置選項選單** |

## 裝置選項

| | |
|---|---|
| **VP50 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「VP50 設定」一節)。 |
| **瀏覽 VP50：** | • 可讓您檢視自己的安全檔案。 |
| **格式化 VP50：**<br>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)**<br><br>**注意：**密碼認證需要進行格式化。 |  <br>**圖 6.1 – 格式化 VP50** |
| **線上支援：** | • 開啟網路瀏覽器並造訪 http://www.kingston.com/support，您可以在該網站獲得其他支援資訊。 |
| **關於 VP50：**<br>提供有關 VP50 的特定詳細資訊，包括應用程式、韌體和序號資訊。**(圖 6.2)**<br><br>**注意：**隨身碟的唯一序號將會在「資訊欄」底下。 |  <br>**圖 6.2 - 關於 VP50** |
| **將 VP50 關機：** | • 正確關閉 VP50，如此可讓您從系統安全地將其移除。 |

# VP50 設定

## 管理員設定

管理員登入允許下列裝置設定的存取：

- **密碼：**允許您變更您自己的管理員密碼和/或提示 (*圖 7.1*)
- **聯絡資訊：**允許您您新增/查看/變更您的聯絡資訊 (*圖 7.2*)
- **語言：**可讓您變更目前語言選項 (*圖 7.3*)
- **管理員選項：**可允許您啟用其他功能，例如：(圖 7.4)
    - 變更使用者密碼
    - 登入密碼重設 (適用於使用者密碼)
    - 啟用一次性恢復密碼
    - 強制使用者以唯讀模式登入

**注意：**有關管理員選項的其他詳細資訊，請參閱第 24 頁。

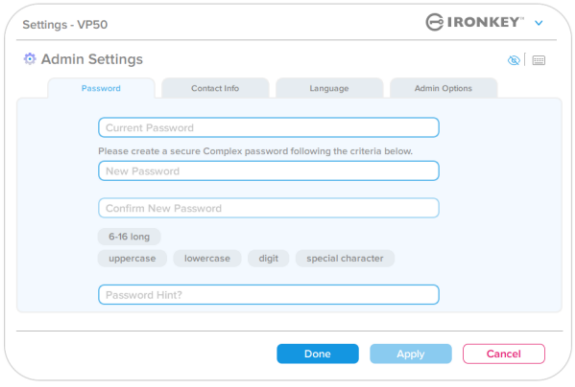



**圖 7.1 - 密碼選項**

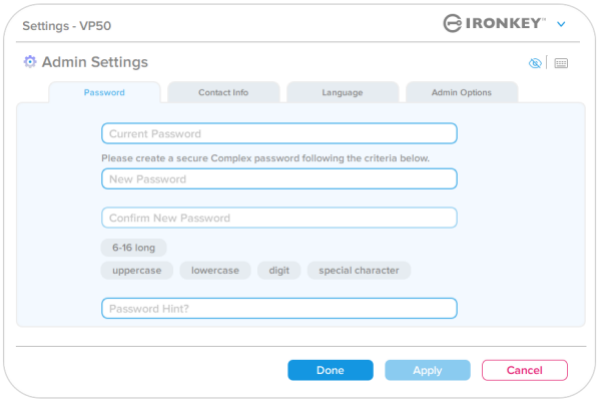



**圖 7.2 - 聯絡資訊**

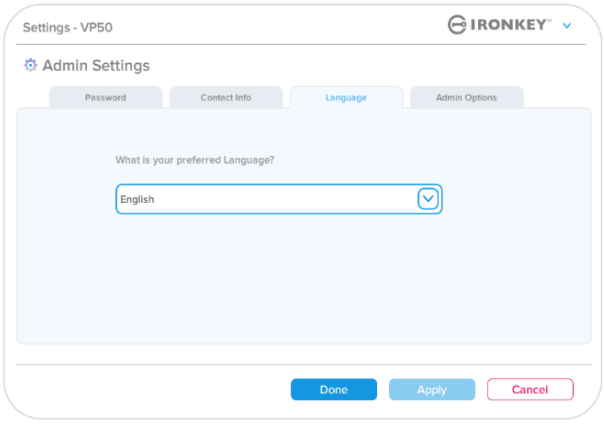



**圖 7.3 - 語言選項**

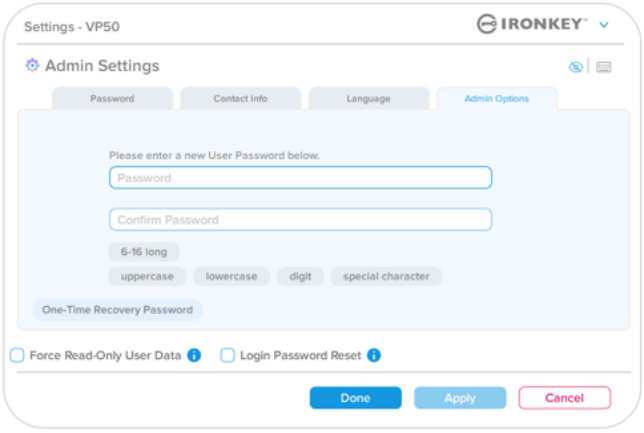



**圖 7.4 - 管理員選項**

## VP50 設定

### 使用者設定：管理員啟用

使用者登入時將限制下列設定的存取：

**密碼：**
允許您變更自己的使用者密碼和/或提示。(*圖 7.5*)

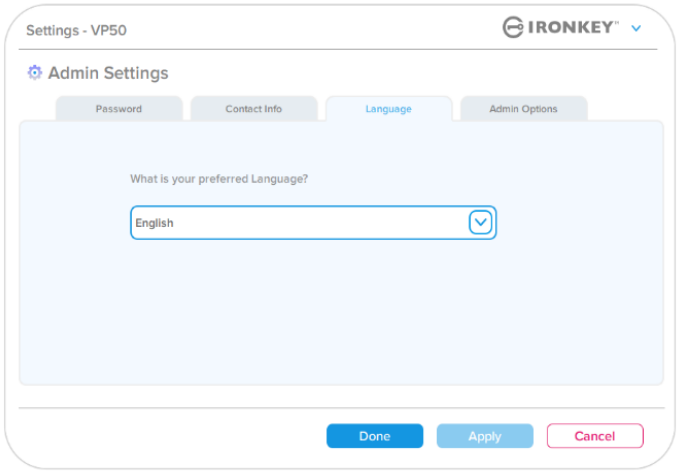



**圖 7.5 - 密碼選項 (管理員啟用：使用者登入)**

**聯絡資訊：**
允許 您新增/查看/變更您的聯絡資訊。(*圖 7.6*)

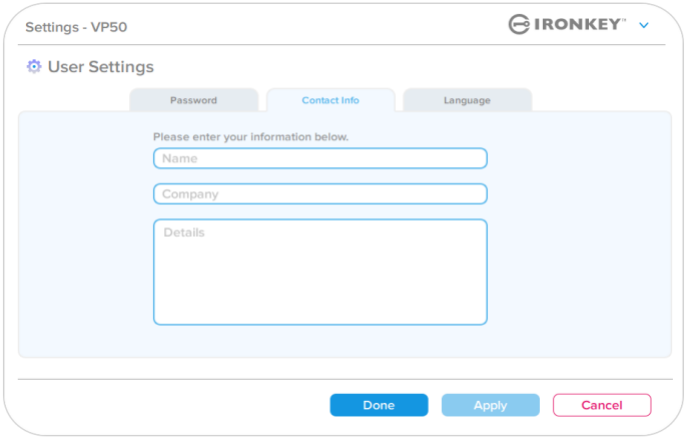



**圖 7.6 - 聯絡資訊 (管理員啟用：使用者登入)**

**語言：**
可讓您變更目前語言選項。(*圖 7.7*)

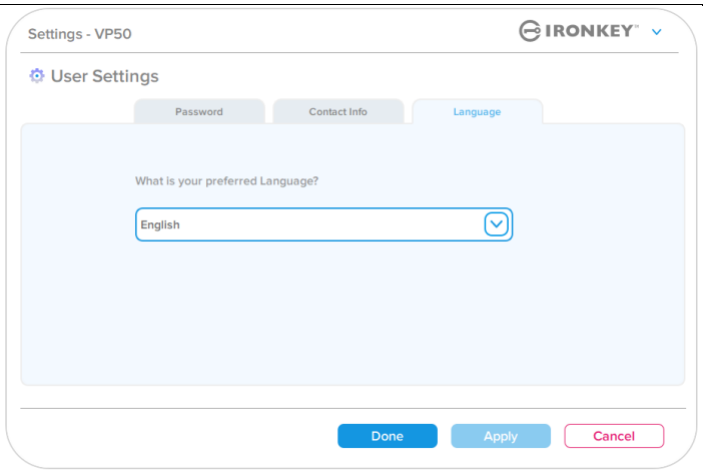



**圖 7.7 - 語言設定 (管理員啟用：使用者登入)**

**注意**：以使用者密碼登入時，無法存取管理員選項。

## VP50 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 VP50 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。此組態無權存取任何管理員選項或功能。此組態將有權存取以下 VP50 設定：

### 變更與儲存設定

- 每當 VP50 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 7.11)

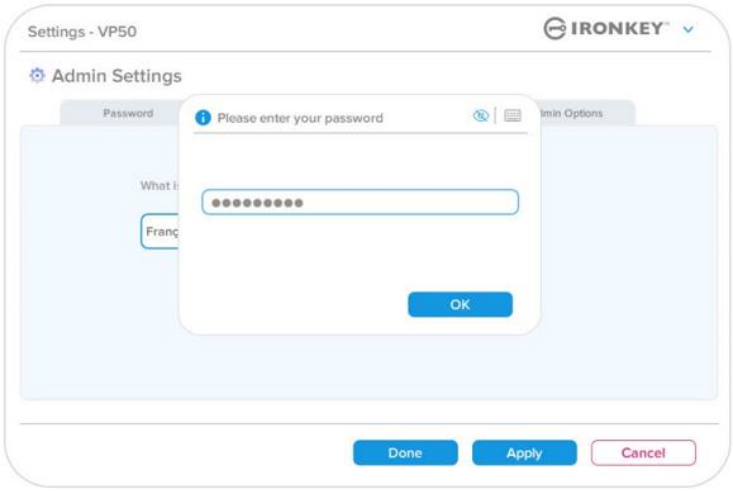



**圖 7.11 - 儲存 VP50 設定變更的密碼提示畫面**

**注意**：如果您在上面的密碼提示畫面中，並想取消或修改您的變更，只需確保密碼欄位為空白，然後按一下「確定」即可。這樣將會關閉「請輸入您的密碼」方塊並返回 VP50 設定選單。

# 管理員功能

**可用於重設使用者密碼的選項**

管理員組態的功能允許透過多種方式安全地重設使用者密碼，比如忘記密碼時，或者在建立暫時使用者密碼後，希望使用者登入後強制變更下次登入的密碼以下是有助於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 8.1)**

**注意**：預設的密碼需求標準為在初始化時設定的原始標準 (複雜或密碼片語選項)。

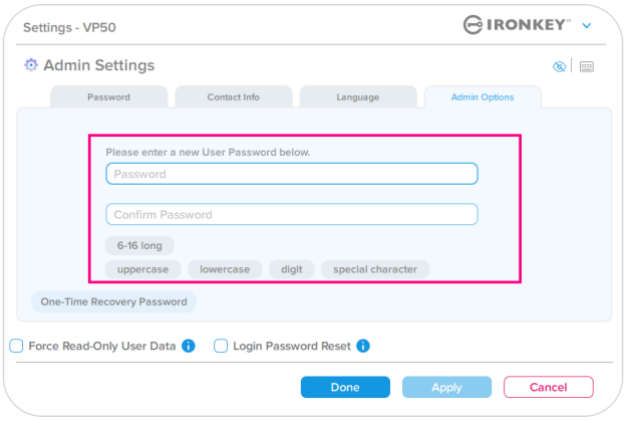



**圖 8.1 - 管理員選項/使用者密碼重設**

**重設登入密碼：**

啟用密碼重設將會**強制使用者以管理員設定的暫時密碼登入**，然後再將其變更為自己選擇的密碼。如果隨身碟會提供給其他人使用，這個功能會很有用。**(請參閱圖 8.2A 和 8.2B)**

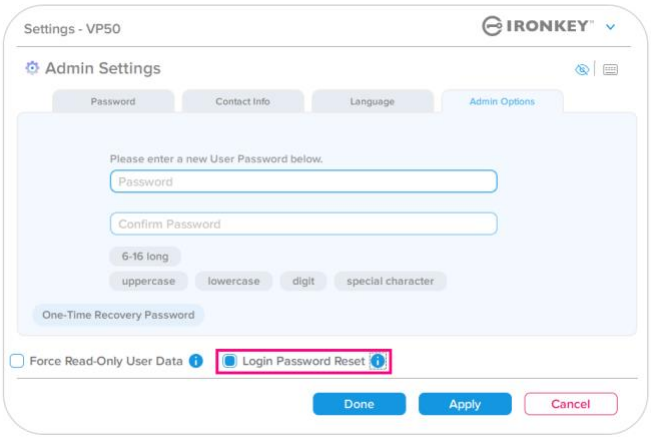



**圖 8.2A - 登入密碼重設按鈕**

**注意：**套用此重設後，將在下次成功的使用者登入時發生。密碼要求標準將根據初始化時設定的原始選項 (複雜或密碼選項) 自動套用。

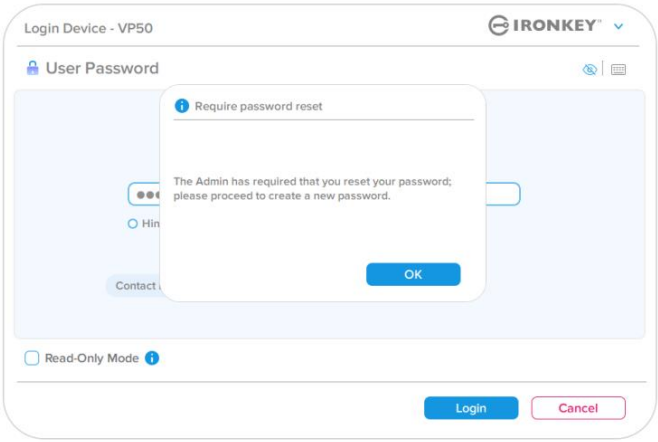



**圖 8.2B - 在輸入使用者密碼後重設通知**

# 管理員功能

## 一次性恢復密碼

本節將討論啟用和使用一次性恢復密碼功能的過程。

### 一次性恢復密碼

**步驟 1：**一次性恢復密碼功能是極為有用的單次使用密碼，在忘記密碼時，可啟用以協助恢復及重設使用者密碼。按一下管理員選項選單中的「一次性恢復密碼」按鈕以便開始。**(圖 8.4)**

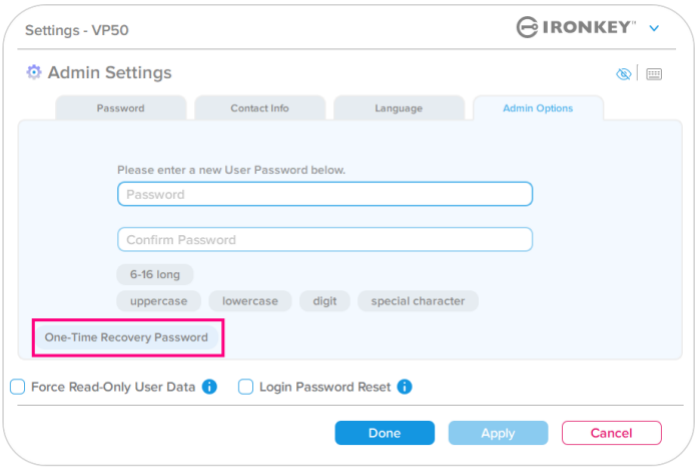



**圖 8.4 - 一次性恢復密碼按鈕**

**步驟 2：**使用最初設定裝置的相同密碼條件 (複雜或密碼片語) 建立一次性恢復密碼。

**注意：**管理員密碼需要套用變更。

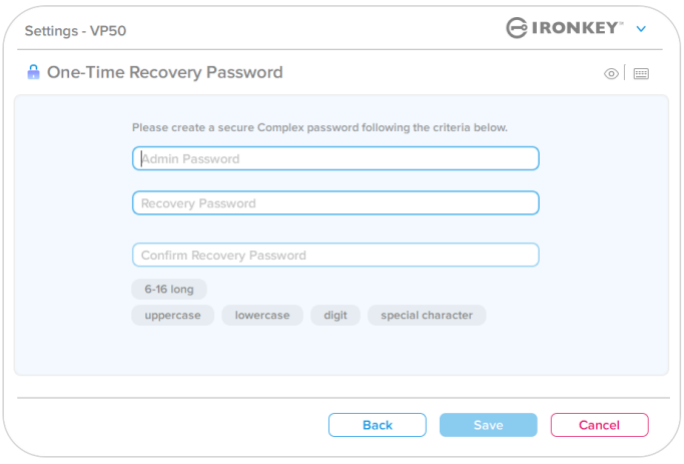
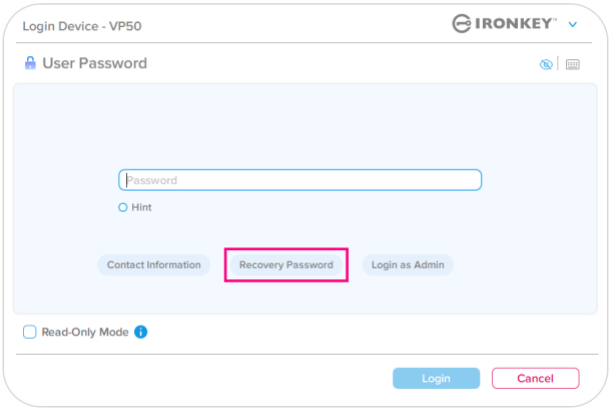
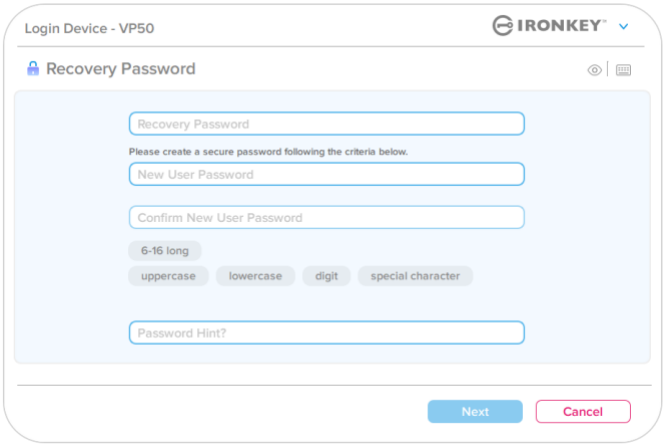
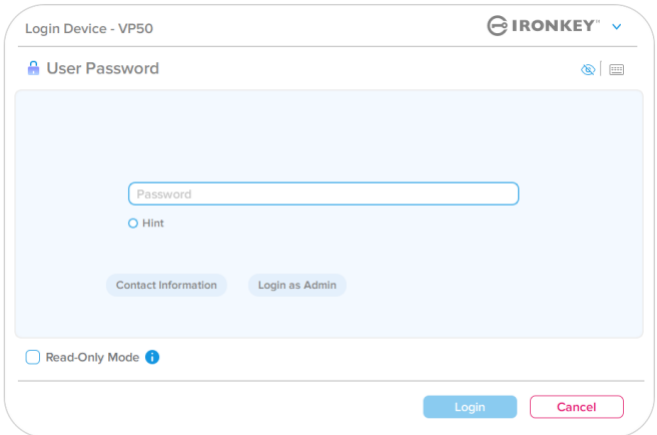



**圖 8.5 - 一次性恢復密碼設定**

## 管理員功能

使用一次性恢復密碼

| | |
|---|---|
| **步驟 1：**在建立一次性恢復密碼之後，在下次登入時，新的按鈕將會出現在**使用者密碼**登入畫面。按一下「**Recovery Password**」(恢復密碼) 按鈕以開始程序。 |  **圖 8.6 - 恢復密碼按鈕** |
| **步驟 2：恢復密碼**畫面將會出現在您可以輸入恢復密碼並且建立新的使用者密碼的位置。(圖 8.7)<br><br>重要須知：一次性恢復密碼也會以內建的安全功能追蹤失敗登入嘗試次數，**使用一次性恢復密碼進行 10 次失敗的錯誤登入嘗試之後，密碼將會被停用**，必須以管理員身分登入隨身碟之後，才能重新啟用。(更多詳情請參閱第 18 頁和第 30 頁) |  **圖 8.7 - 恢復密碼選單** |
| **步驟 3：**成功後，系統會將您帶回**使用者密碼**畫面。「**Recovery Password**」(恢復密碼) 按鈕現在已經不再使用，而在**步驟 2** 中輸入的使用者密碼將成為新的使用者密碼。(圖 8.8) |  **圖 8.8 - 使用者密碼登入畫面，顯示 (恢復密碼) 按鈕在成功使用後消失。** |

# 管理員功能

## 強制使用者唯讀資料

強制唯讀模式功能可用來限制使用者寫入資料至隨身碟。如果隨身碟中的檔案只需要讀取存取，則此功能將很有用。

- 若要啟用使用者資料的強制唯讀，請按一下方塊然後按一下「套用」。**(圖 8.9)**

  **注意：**此強制唯讀模式僅適用於使用者，並不會影響管理員登入。管理員登入仍然擁有讀取與寫入存取權限，若需要仍然可以啟用「唯讀」模式。

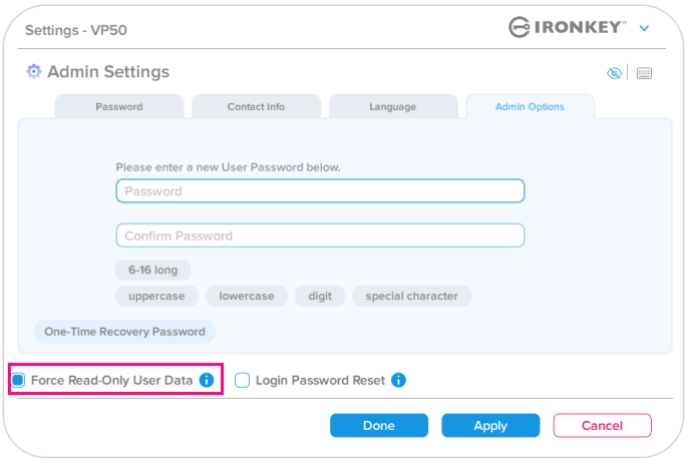



**圖 8.9 - 啟用「強制使用者唯讀資料」(管理員密碼需要套用變更)**

- 一旦啟用，**「唯讀模式」**按鈕方塊將會變成藍色，表示使用者密碼已經永久啟用「強制唯讀模式」，直到管理員停用為止。(圖 8.10)

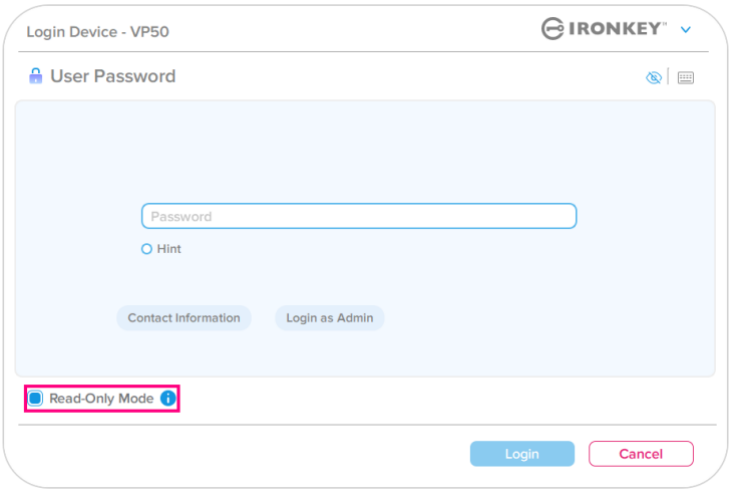



**圖 8.10 - 已經為使用者強制啟用唯讀模式並且僅可由管理員停用**

# 說明與疑難排解

## 裝置解鎖

VP50 提供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「即可使用」組態已經在每個登入方法 (管理員/使用者/一次性恢復密碼) 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 MaxNoA 前成功登入。

**2.**達到 MaxNoA 後執行裝置鎖定或是裝置格式化，視裝置設定方式而定。

- 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 9.1)

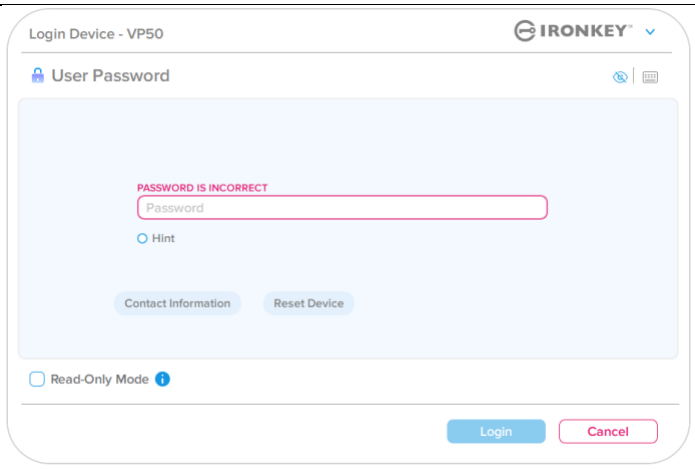



**圖 9.1 - 密碼不正確訊息**

- 如果嘗試失敗的次數達到第 **7** 次，您就會看到其他錯誤訊息，表示您再進行 3 次嘗試登入就會達到 MaxNoA (預設值為 10)。(圖 9.2)

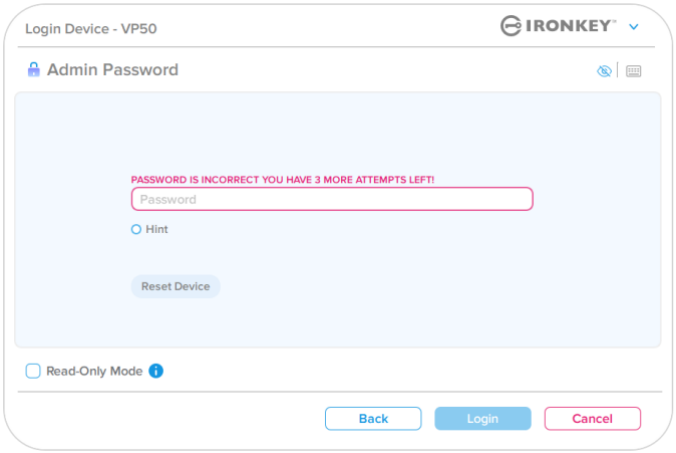


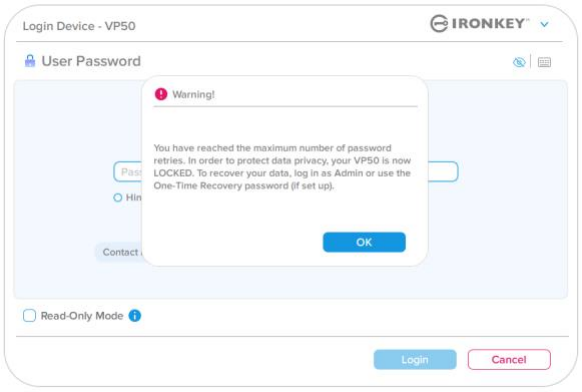
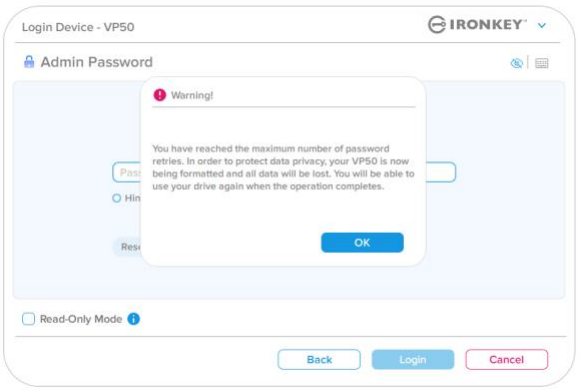
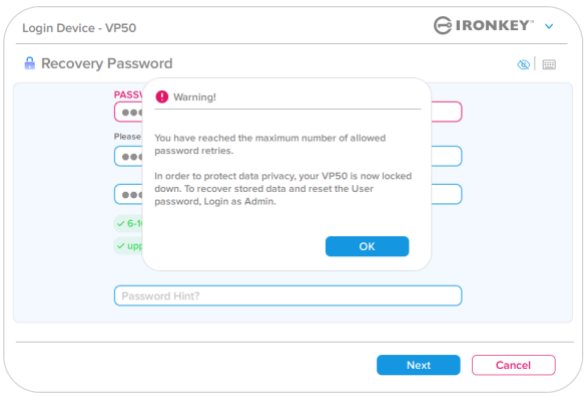
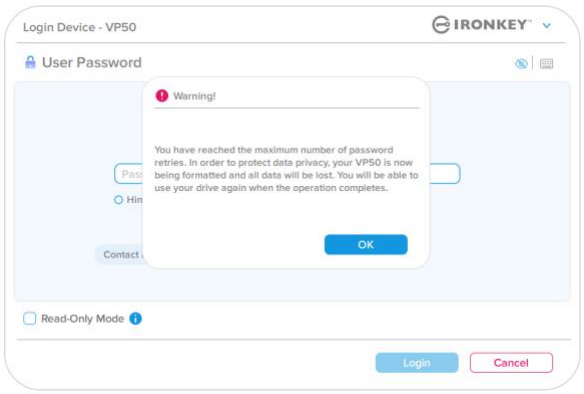

**圖 9.2 - 第 7 次錯誤密碼嘗試**

# 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、使用者或一次性恢復密碼)，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 9.3- 9.6 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><br> 
<br>裝置解鎖<br><br>(圖 9.3)</td>
<td><u>管理員密碼 (管理員/使用者啟用)</u><br> 
<br>裝置格式化*<br><br>(圖 9.4)</td>
</tr>
<tr>
<td><u>一次性恢復：(管理員/使用者啟用)</u><br> 
<br>裝置解鎖<br><br>(圖 9.5)</td>
<td>使用者密碼 (管理員未啟用)<br> 
<br>裝置格式化*<br><br>(圖 9.6)</td>
</tr>
</table>

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 VP50 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。

**注意：裝置格式化將清除 VP50 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執行 VP50 隨身碟的設定方式 (如果啟用管理員/使用者，則出現在管理員登入密碼選單，如果未啟用管理員/使用者，則出現在「使用者密碼」登入選單)。(請參閱***圖 9.7*** 和 **9.8**)

- 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 VP50。這代表您的所有資料皆會在程序中被移除。*

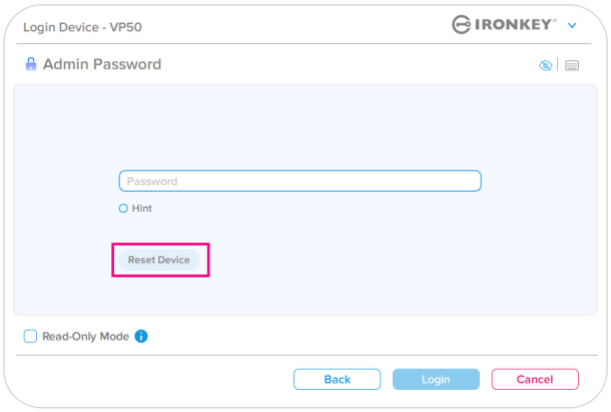



**圖 9.7：管理員密碼：重設裝置按鈕**

- **注意：**當您按一下「*Reset Device*」(重設裝置) 時，便會顯示一個訊息方塊且會詢問您是否希望先輸入新密碼，然後再執行格式化。此時，您可以：1) 按一下「*OK*」(確定) 確認；或是：2) 按一下「Cancel」(取消) 以返回登入視窗。(詳見圖 9.8)

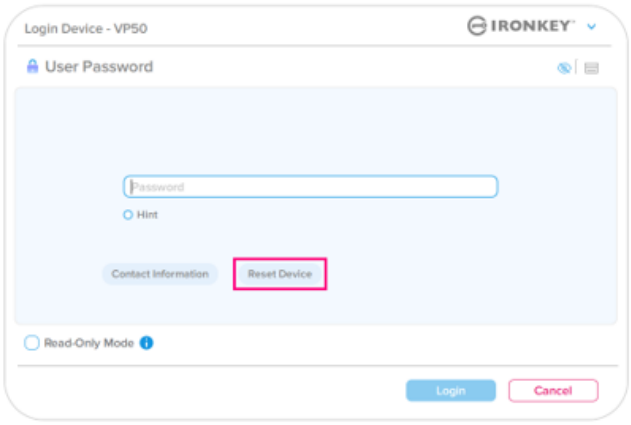



**圖 9.8 - 使用者密碼 (管理員/使用者未啟用) 重設裝置**

- 如果您選擇繼續，系統將提示您進入初始化螢幕，您可以在其中啟用「管理員和使用者模式」，並根據您選擇的密碼選項 (複雜或密碼片語) 輸入新密碼。提示不是必填欄位，但如果您忘記密碼，提示欄位可幫助您提供有關密碼內容的線索。

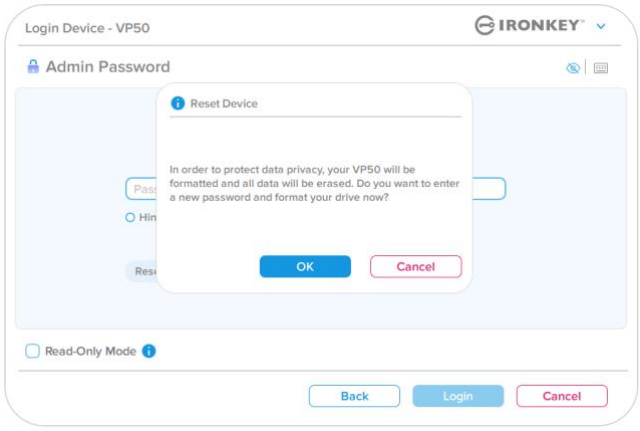



**圖 9.9 - 重設裝置確認**

## 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，VP50 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 9.10*。)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 VP50 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)。如同本使用者手冊第 3 頁的*系統要求*一節所述，VP50 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 9.10*。)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。

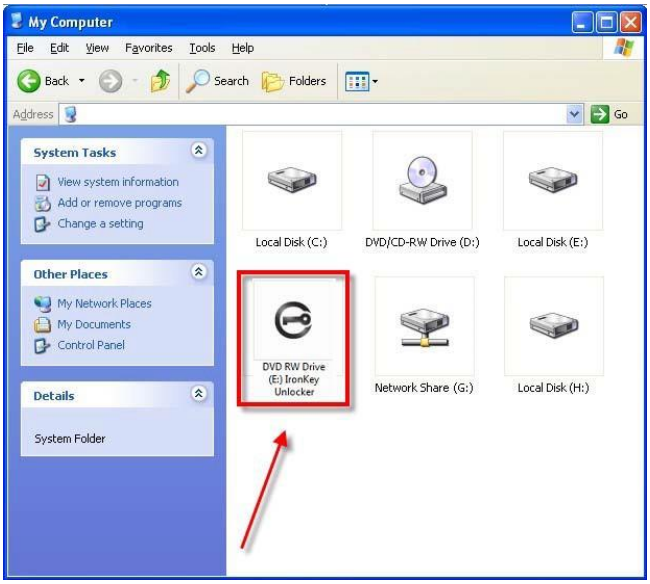



**圖 9.10 - 磁碟機範例：**

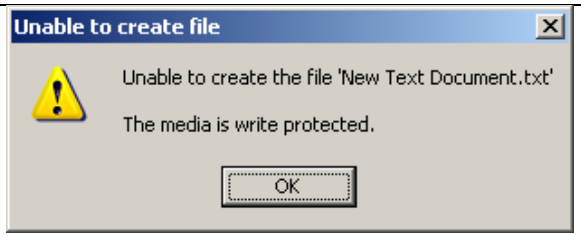
在本例 (圖 9.10 )中，VP50 使用磁碟機 F:，這是磁碟機 E: (即磁碟機代號字母中斷前的最後一個實體磁碟機)之後第一個可用的磁碟機代號。由於字母 G: 為網路共用磁碟機，而不是硬體設定檔的一部分，所以 VP50 可能會將它當作自己的第二個磁碟機代號，因此造成衝突。

如果您的系統上沒有網路共用，卻仍然無法載入 VP50，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，請聯繫 Kingston 的技術支援部門或造訪 Kingston.com/support，以獲得進一步的協助。

## 說明與疑難排解

### 錯誤訊息

| | |
|---|---|
| **無法建立檔案：**<br>在唯讀模式下登入時，如果嘗試在安全資料分割區上建立檔案或資料夾，將會出現此錯誤訊息。 |  <br>**圖 9.11 - 無法建立檔案錯誤** |
| **複製檔案或資料夾發生錯誤：**<br>在唯讀模式下登入時，如果嘗試複製檔案或資料夾至安全資料分割區，將會出現此錯誤訊息。 |  <br>**圖 9.12 - 複製檔案或資料夾時發生錯誤** |
| **刪除檔案或資料夾發生錯誤：**<br>在唯讀模式下登入時，如果嘗試從安全資料分割區刪除檔案或資料夾，將會出現此錯誤訊息。 |  <br>**圖 9.13 - 刪除檔案或資料夾時發生錯誤** |

**注意：**如果您曾經在唯讀模式下登入，但現在想要解除鎖定隨身碟以獲得安全資料分割區的完整讀取/寫入權限，您必須先關閉 VP50 再重新登入，並且在登入前取消核取「Read-Only Mode」(唯讀模式) 核取方塊。