IRONKEY™ Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) ENCRYPTED USB 3.2 Gen 1 FLASH DRIVE

User Guide

Contents

Introduction **3**
Vault Privacy 50/50C Features 4
About this Manual 4
System Requirements 4

Recommendations **5**
Using the Correct File System 5
Usage Reminders 5
Best Practices for Password Setup 6

Setting Up My Device **7**
Device Access (Windows Environment) 7
Device Access (macOS Environment) 7

Device Initialization (Windows & macOS Environment) **8**
Password Selection 9
Virtual Keyboard 11
Password Visibility Toggle 12
Admin & User Passwords 13
Contact Information 15

Device Usage (Windows & macOS Environment) **16**
Login for Admin & User (Admin Enabled) 16
Login for User-Only mode (Admin not enabled) 16
Unlocking in Read-Only Mode 17
Brute-Force Attack protection 18
Accessing my secure Files 18

Device Options **19**

VP50/VP50C Settings **21**
Admin Settings 21
User Settings: Admin Enabled 22
User Settings: Admin Not Enabled 23
Changing and Saving VP50/VP50C Settings 23

Admin Features **24**
User Password Reset 24
Login Password Reset (for User Password) 24
One-Time Recovery Password 25
Force Read-Only User Data 27

Help And Troubleshooting **28**
VP50/VP50C Lockout 28
VP50/VP50C Device Reset 30
Drive Letter Conflict (Windows Operating Systems) 31
Error Messages 32

Figure 1: IronKey VP50

Figure 2: IronKey VP50C

Introduction

The Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C is also TAA compliant and assembled in the U.S.A. Because it is encrypted storage under the user's physical control, VP50/VP50C series is superior to using the internet and Cloud services to safeguard data.

VP50/VP50C 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/VP50C 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/VP50C is backed by a limited 5-year warranty with free Kingston technical support.

IronKey Vault Privacy 50/50C 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 50/50C (VP50/VP50C) and is based on the factory image with no implemented customizations.

System Requirements

PC Platform	**PC Operating System Support**
• Intel, AMD & Apple M1 SOC • 15MB free disk space • Available USB 2.0 - 3.2 port • Two consecutive drive letters after the last physical drive* ***Note:** See 'Drive Letter Conflict' on page 32.	• Windows 11 • Windows 10
Mac Platform	**Mac Operating System Support**
• 15MB free disk space • USB 2.0 - 3.2 Port	• macOS 11.x – 14.x

Recommendations

To ensure there is ample power provided to the VP50/VP50C device, insert it directly into a USB port on your notebook or desktop, as seen in ***Figure 1.1***. Avoid connecting the VP50/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C will automatically wipe out the encrypted data – formatting itself back to a factory state.

Multi-Password
VP50/VP50C 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/VP50C can support three different passwords you may use to recover data – Admin, User, and a One-Time Recovery password.

VP50/VP50C 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/VP50C can be Reset and reused, but the prior data will be erased forever.

Password Modes
The VP50/VP50C 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/VP50C 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/VP50C drive, the password language can match the language selected for the drive. This allows you to select multiple words, a phrase, lyrics from a song, a line from poetry, etc. Good passphrases are among the most difficult password types to guess for an attacker yet may be easier to remember for users.

Setting Up My Device

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

Device Access (Windows Environment)

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

- Windows 8.1/10/11 users will receive a device driver notification. (Figure 3.1)

Figure 3.1 - Device Driver Notification

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

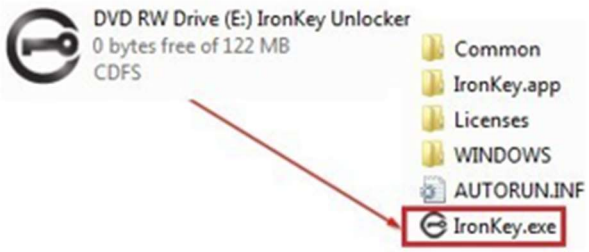


Figure 3.2 - File Explorer Window/IronKey.exe

Device Access (macOS Environment)

Insert the VP50/VP50C 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 VP50 (Or IRONKEY) volume appear on the desktop. (Figure 3.3)

- Double-click the IronKey CD-ROM icon.
- Then, double-click the VP50 (Or IronKey.app) application icon found in the window displayed in Figure 3.3. This will start the initialization process.

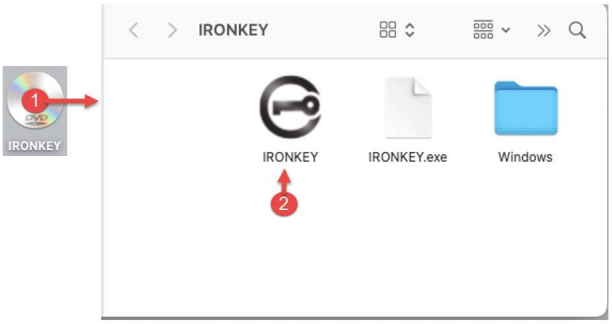


Figure 3.3 - IKVP Volume

Device Initialization (Windows & macOS Environment)

Language and EULA

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

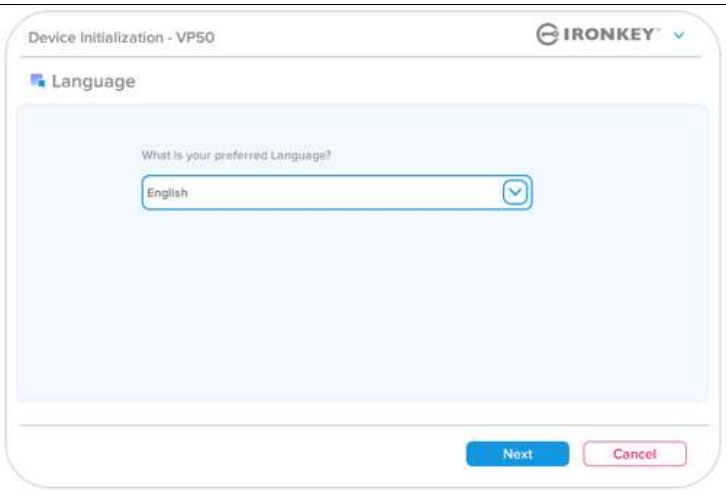


Figure 4.1 - Language Selection

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

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

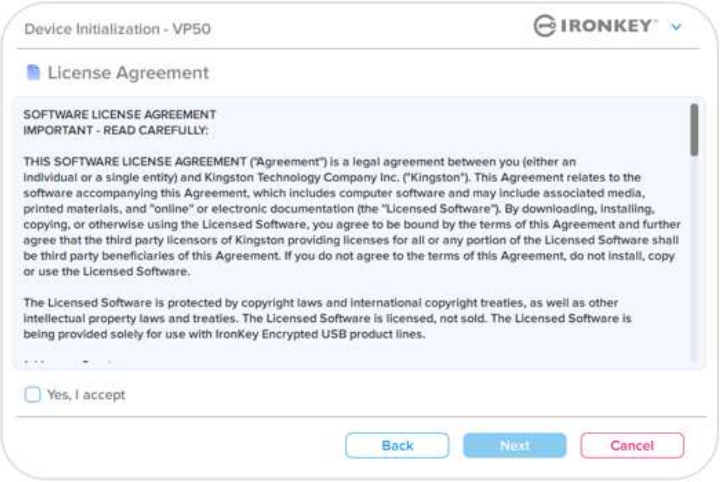


Figure 4.2 - License Agreement

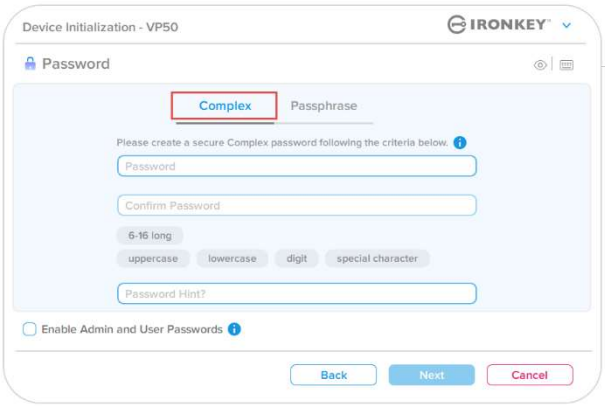
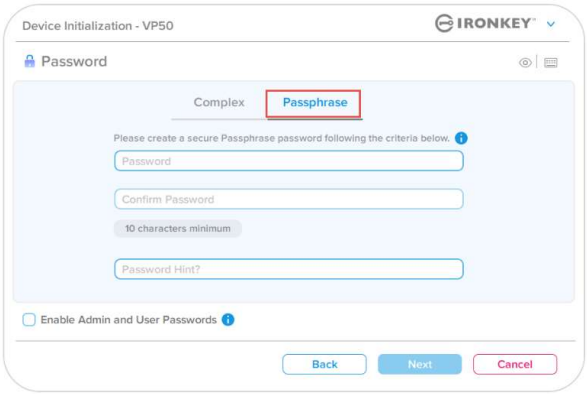
Device Initialization

Password Selection

On the Password prompt screen, you will be able to create a password to protect your data on the VP50/VP50C using either the Complex or Passphrase password modes (Figures 4.3- 4.4). Additionally, the Multi-password Admin/User options can also be enabled on this screen. Before proceeding with Password Selection, please review Enabling Admin / User Passwords below for a better understand of these features.

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

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

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

Device Initialization

Valid and Invalid Passwords

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

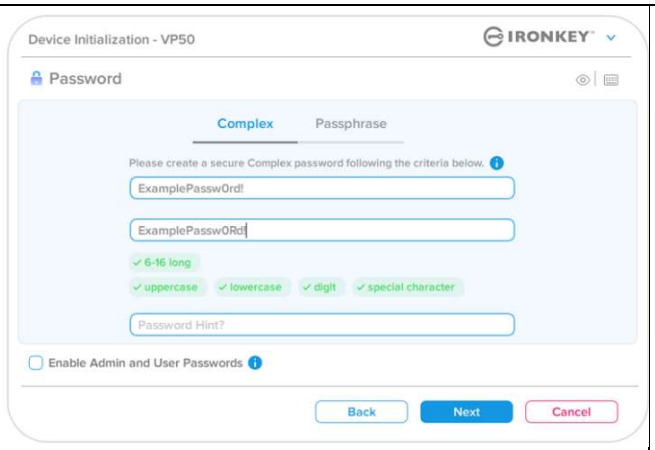


Figure 4.6a - Complex Password Condition Met

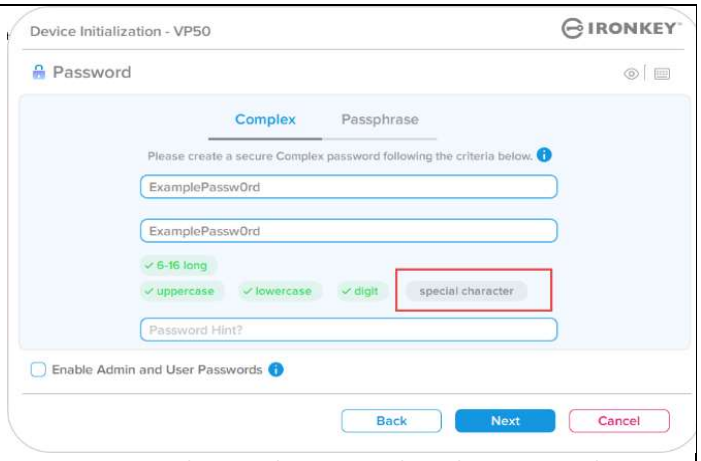


Figure 4.6b - Complex Password Condition Optional

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

This applies to both Complex and Passphrase Passwords.

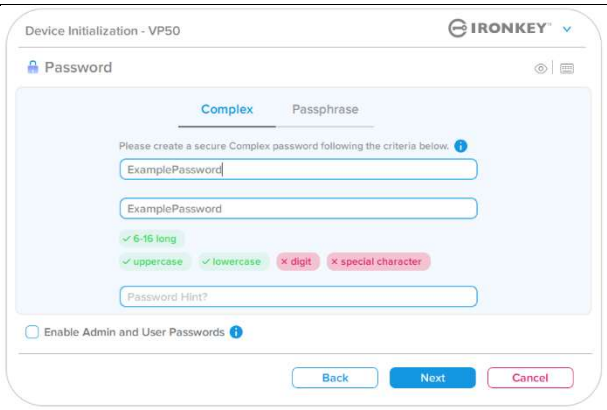


Figure 4.7 - Password Conditions Not Met

Device Initialization

Virtual Keyboard

The VP50/VP50C 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.

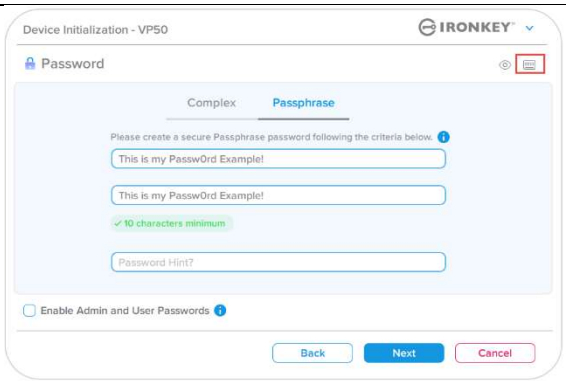


Figure 4.8 - Activating the Virtual Keyboard

- 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.

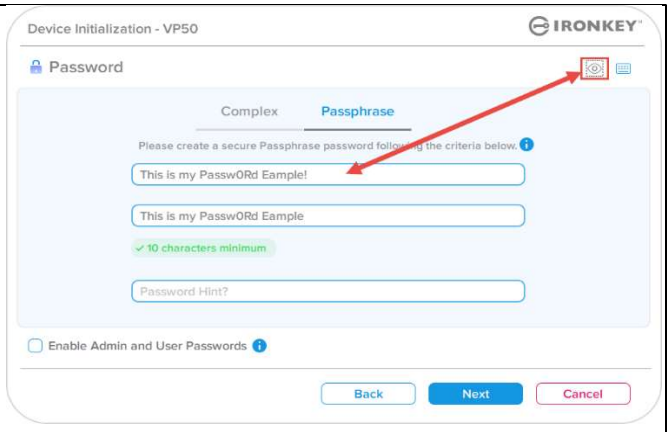
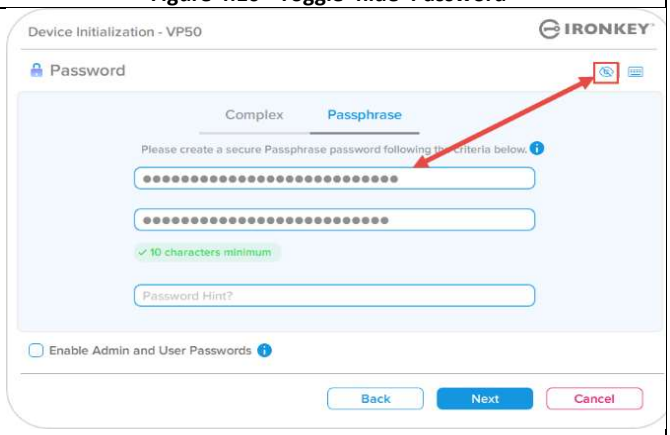
Figure 4.9 - Screenlogger Protection / Randomize

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.

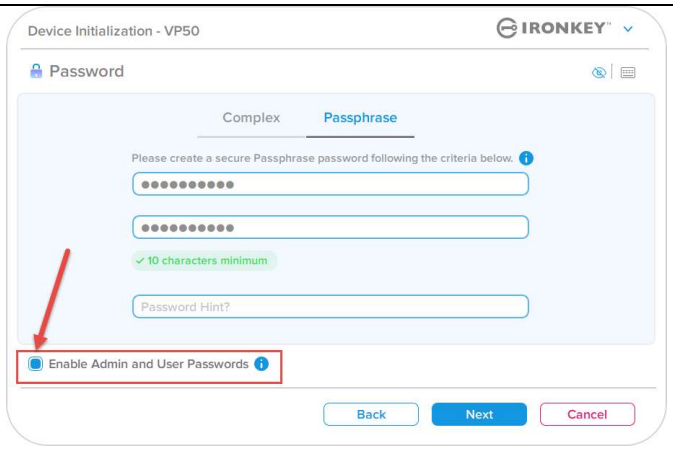


Figure 4.12 - Enabling Admin and User Passwords

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)

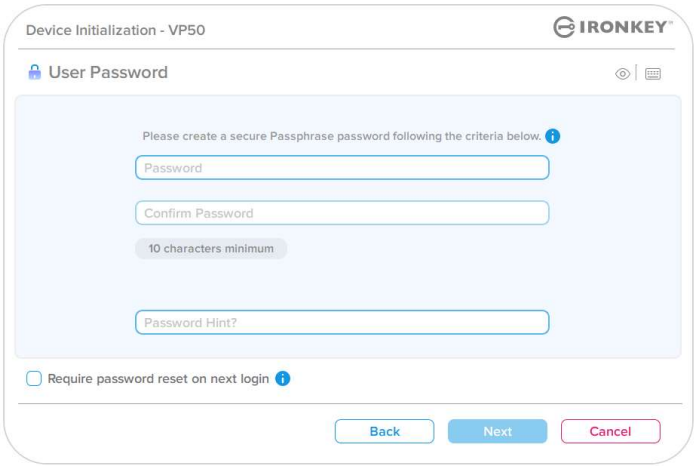


Figure 4.13 - User Password (Admin and User Enabled)

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.

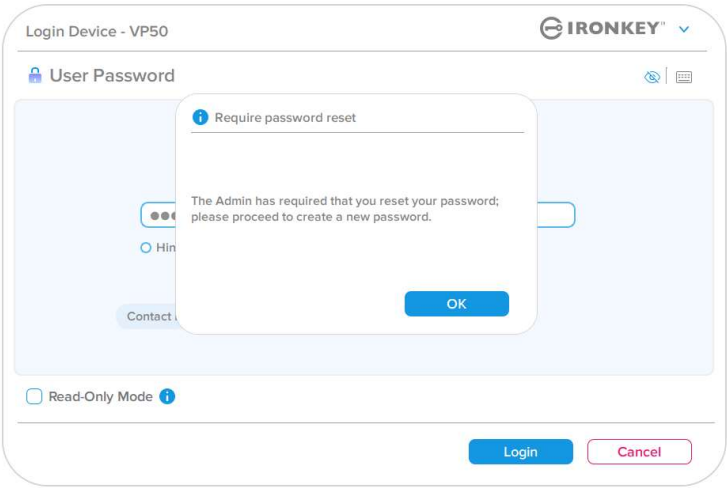


Figure 4.14 - Require password reset on next login (For User Password)

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.

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

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

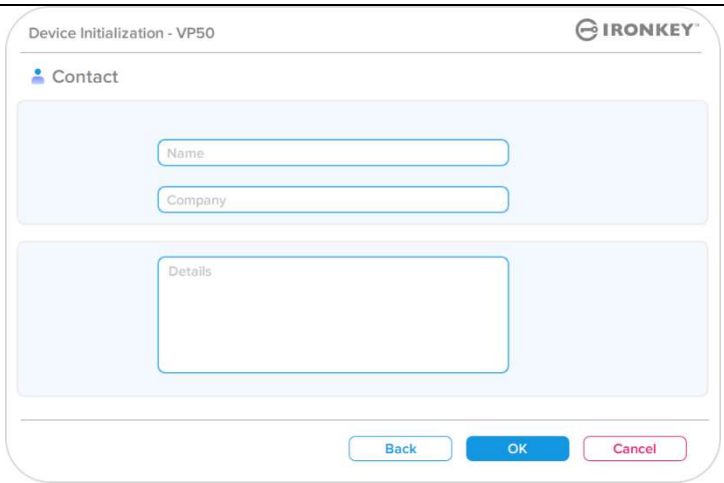


Figure 4.14 - Contact information

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

Device Usage (Windows & macOS Environment)

Login For Admin & User (Admin Enabled)

If the device is initialized with Admin and User Passwords (Admin Role) enabled, the IronKey VP50/VP50C 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)

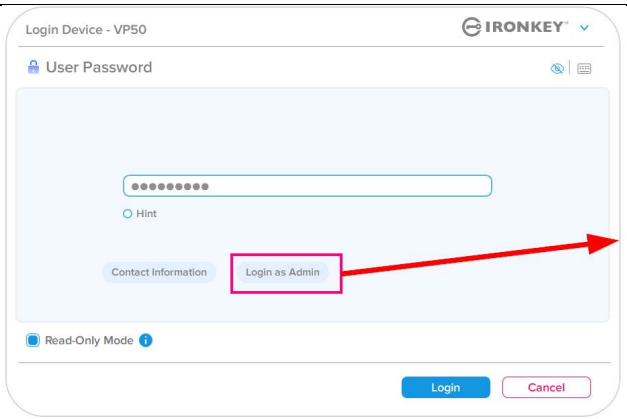


Figure 5.1 - User Password Login (Admin enabled)

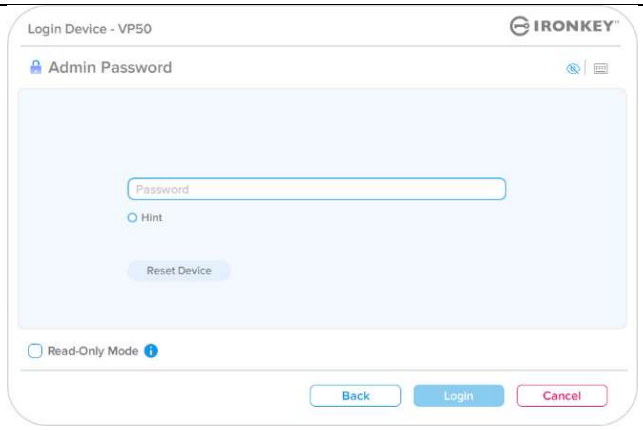


Figure 5.2 - Admin Password Login

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.**

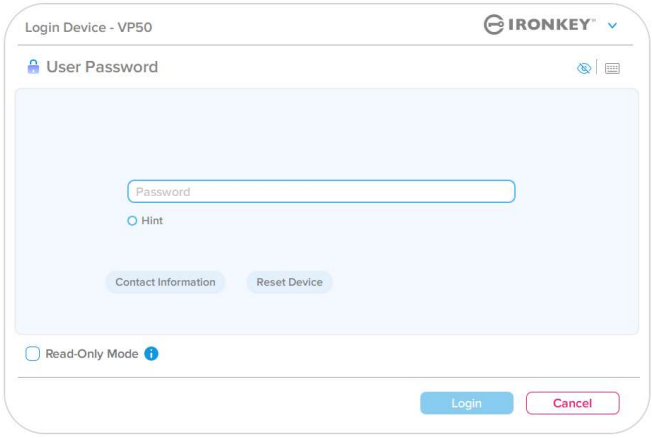


Figure 5.3 - User Password Login (Admin not enabled)

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.

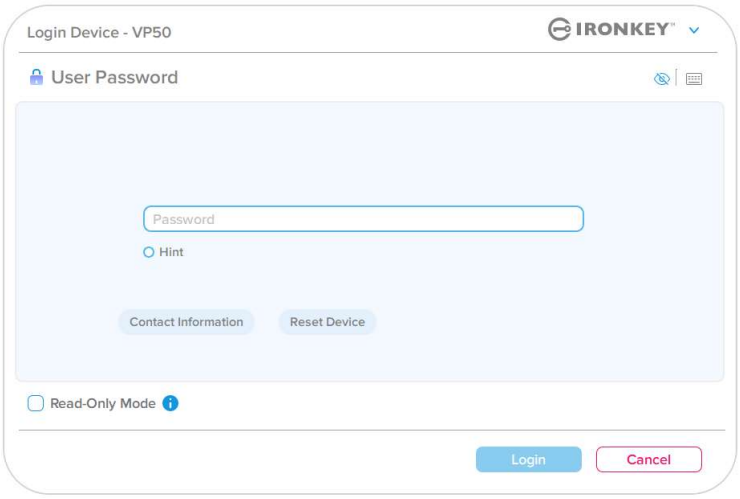


Figure 5.4 - Read-Only Mode

If you wish to unlock the device with full read/write access to the secure data partition, you must shutdown VP50/VP50C and log back in, leaving the 'Read-Only Mode' checkbox unchecked.

Note: The VP50/VP50C 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**

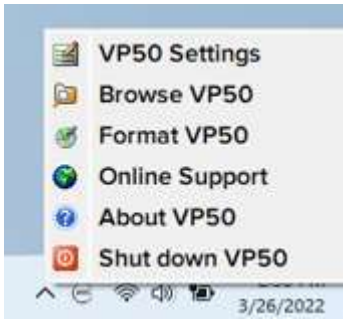
* Once you authenticate to the device successfully, the failed login counter will be reset in relation to which Login method was used. Crypto-Erase will delete all passwords, encryption keys and data – **your data will be lost forever.**

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)

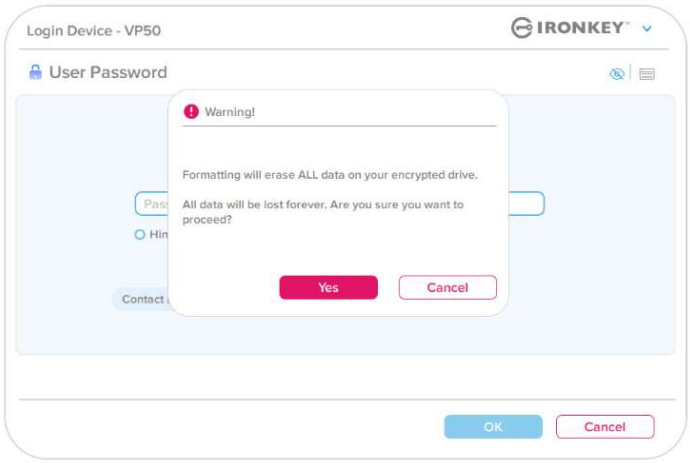
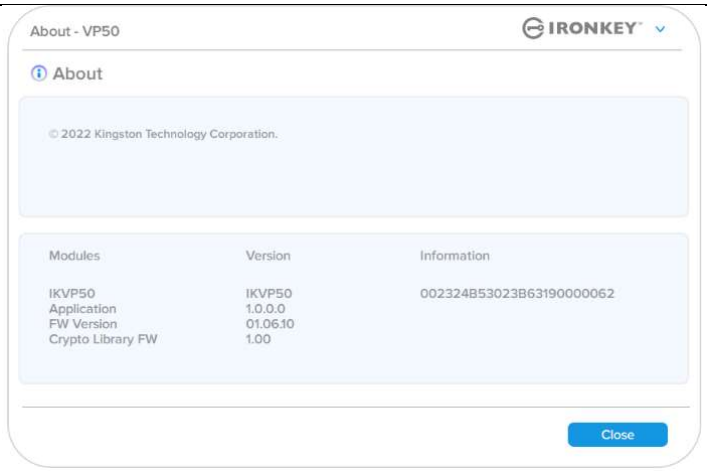
While you are logged into the device, there will be an IronKey icon located in the right-hand corner the window. Right-clicking on the IronKey Icon will open the selection menu for available drive Options. (Figure 6.2)
Details about these device options can be found on Pages 19-23 of this manual.

• 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)**	 **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)** Details about these device options can be found on pages 19-23 of this manual.	 **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. Details about these device options can be found on Pages 19-23 of this manual.	 **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/VP50C Settings' section of this manual).
Browse VP50:	• Allows you to view your secure files.
Format VP50: Allows you to format the secure data partition. (Warning: All data will be erased) (**Figure 6.1**) **Note:** Password authentication will be required for format.	 **Figure 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: Provides specific details about the VP50/VP50C, including Application, Firmware and Serial number Information. (**Figure 6.2**) **Note:** The unique serial number of the drive will be under the 'Information Column'.	 **Figure 6.2 - About VP50**
Shut down VP50:	• Properly shuts down the VP50/VP50C, allowing you to safely remove it from your system.

VP50/VP50C 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.

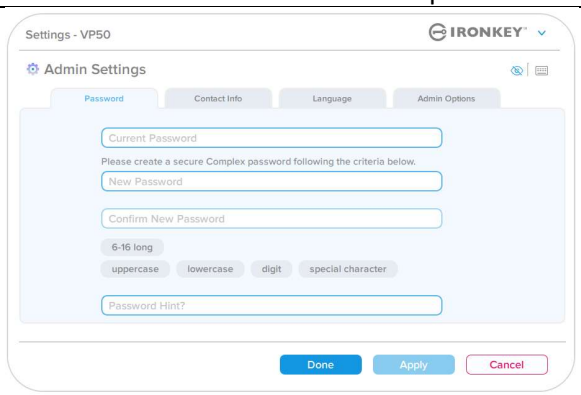


Figure 7.1 - Password Options

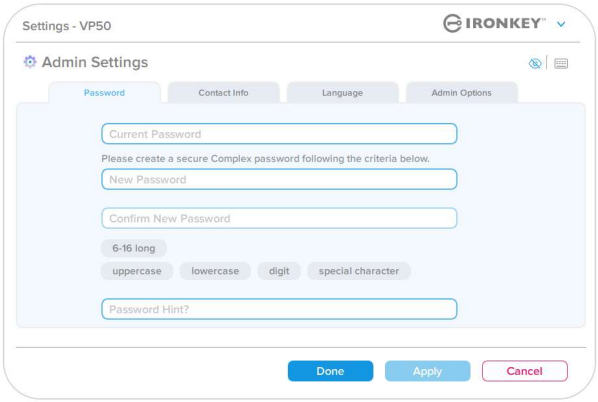


Figure 7.2 - Contact Info

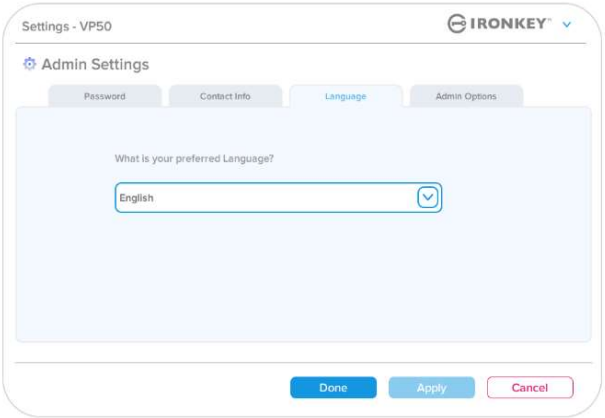


Figure 7.3 - Language Options

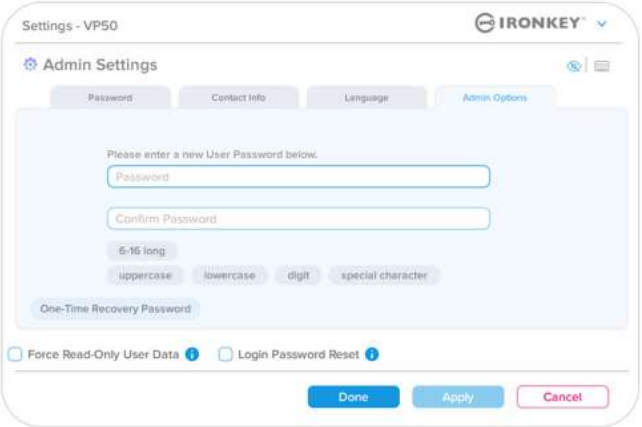
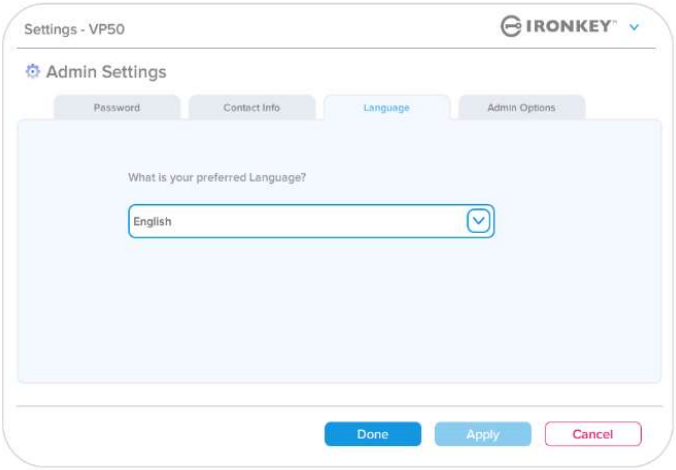
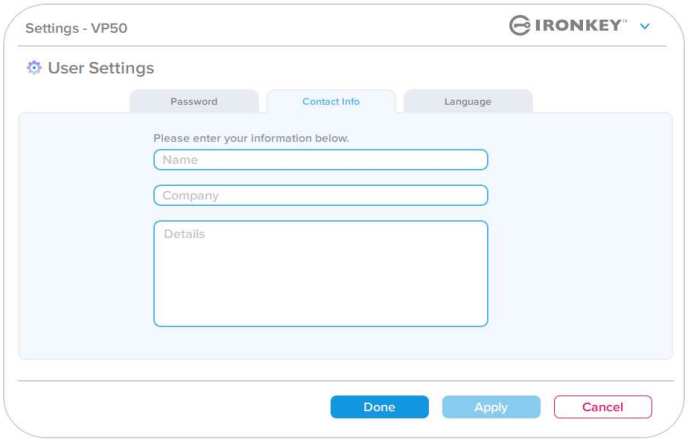
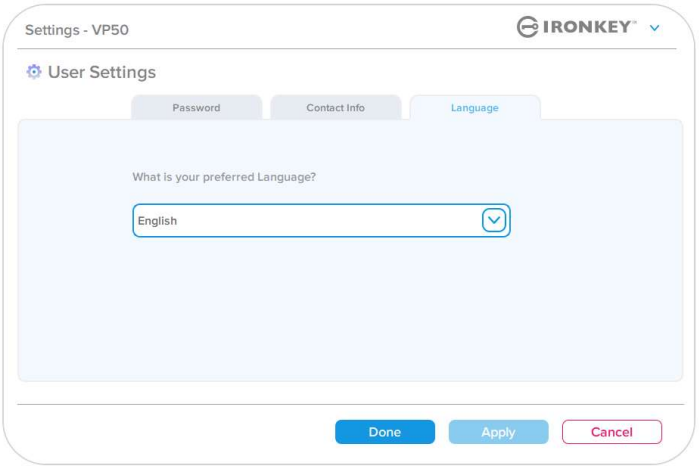


Figure 7.4 - Admin Options

VP50/VP50C 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/VP50C Settings

User Settings: Admin Not Enabled

As mentioned previously on Page 12, initializing the VP50/VP50C 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/VP50C Settings:

Changing and Saving settings

- Whenever settings are changed in the VP50/VP50C 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)

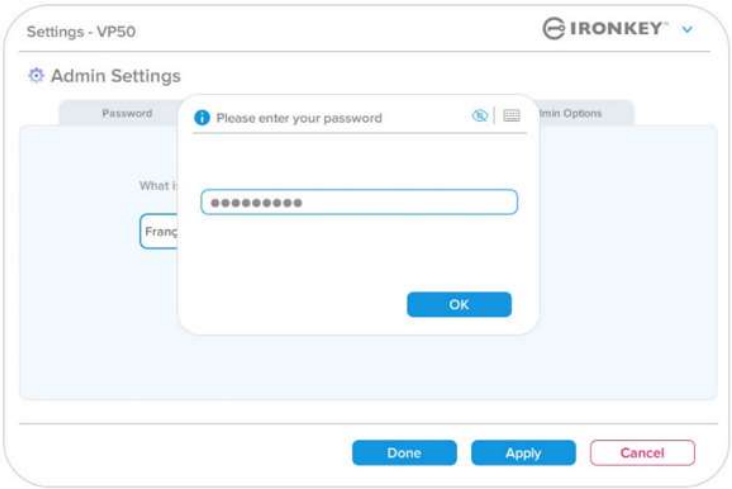


Figure 7.11 - Password Prompt screen to save VP50/VP50C setting changes

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/VP50C 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).

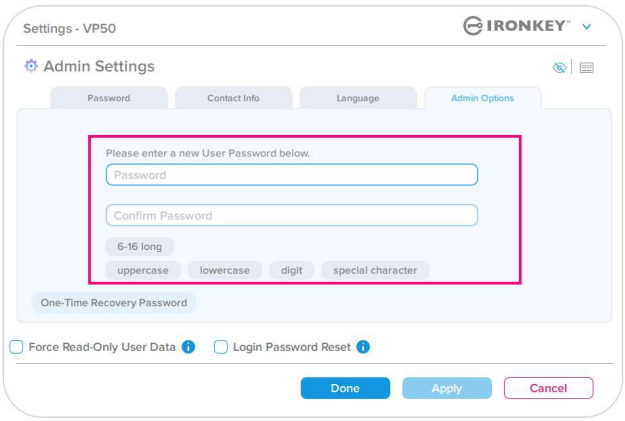


Figure 8.1 - Admin Options/User Password Reset

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**)

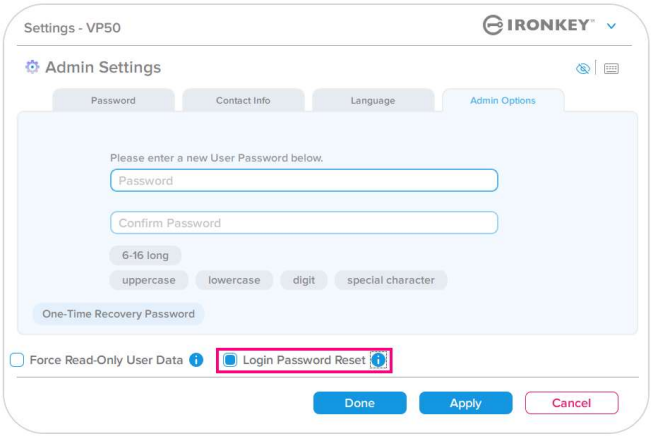


Figure 8.2A - Login Passwords Reset button

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).

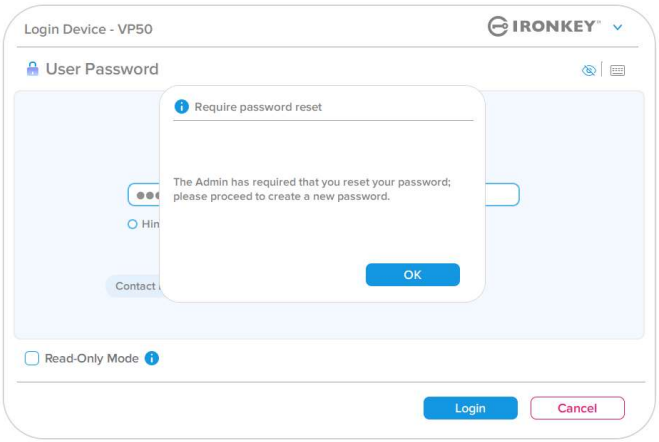


Figure 8.2B - Reset Notification after User Password is entered

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)**

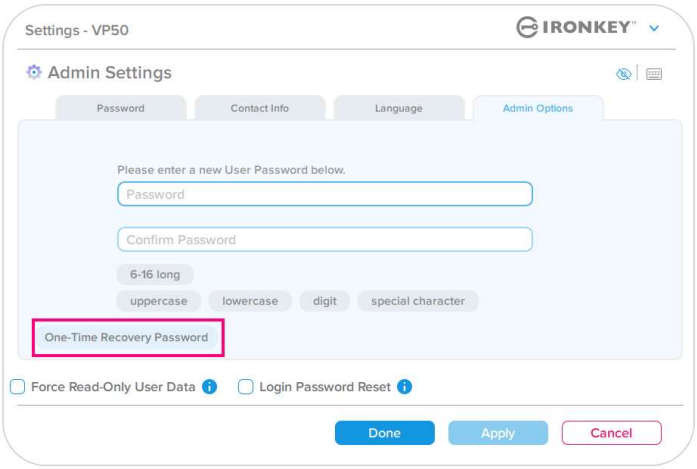


Figure 8.4 - One-Time Recovery Password Button

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.

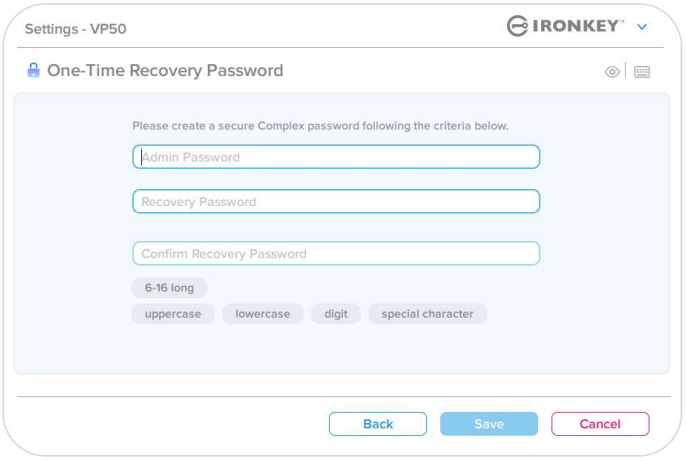


Figure 8.5 - One-Time Recovery Password setup

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.

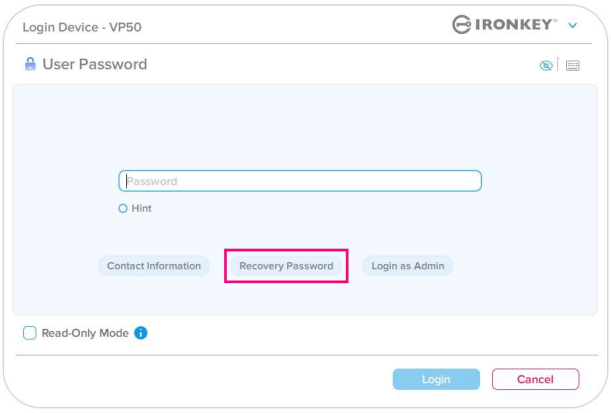


Figure 8.6 - Recovery Password Button

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)

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)

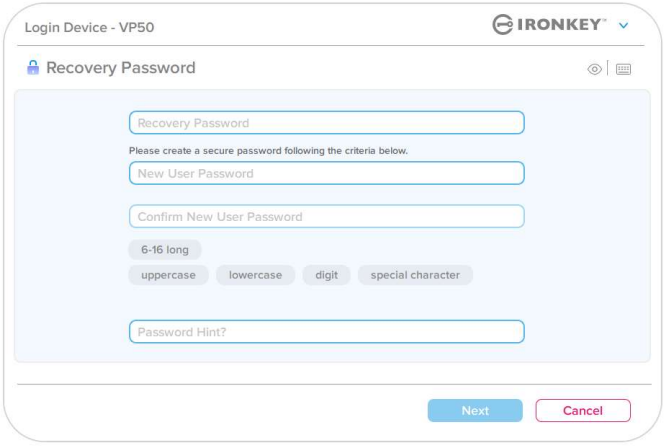


Figure 8.7 - Recovery Password menu

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)

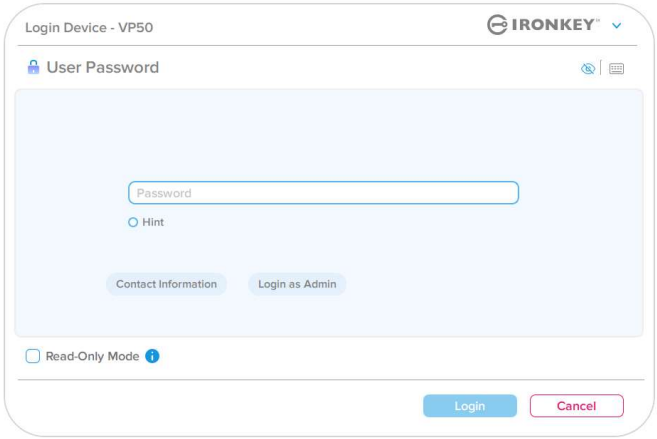


Figure 8.8 - User Password Login screen showing the Recovery Password button disappears after successful use.

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.

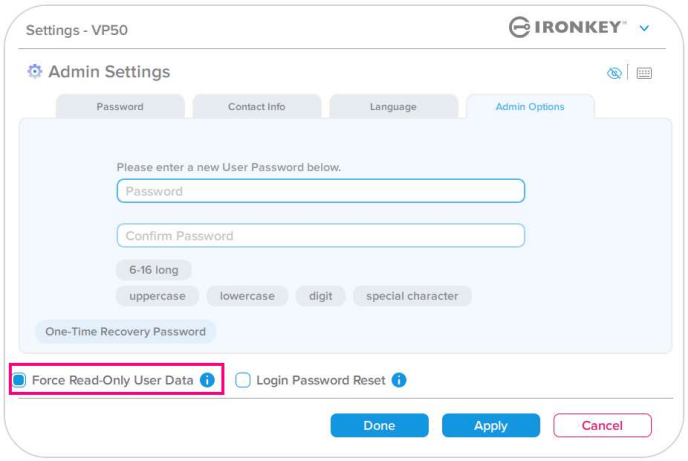


Figure 8.9 - Enable 'Force Read-Only User data' (Admin Password will be required to apply changes)

- 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)

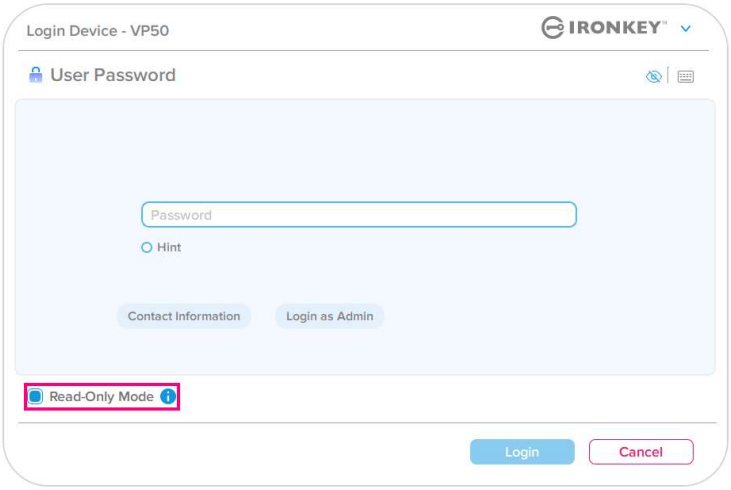


Figure 8.10 - Read-Only Mode is forced enabled for the user and can only disabled by Admin

Help and Troubleshooting

Device Lockout

The VP50/VP50C 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)

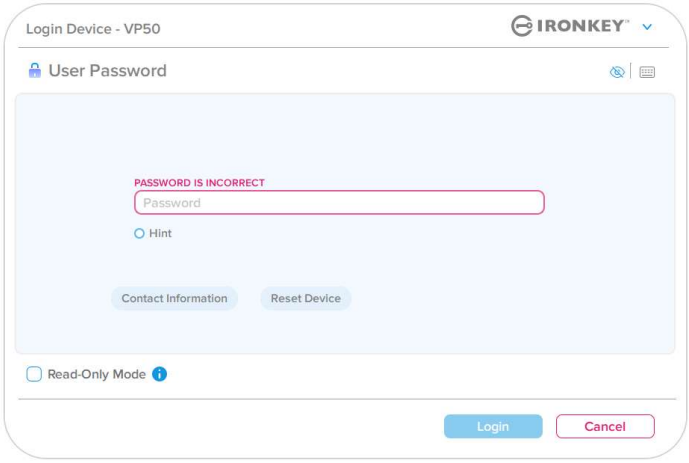


Figure 9.1 - Incorrect Password message

- 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)

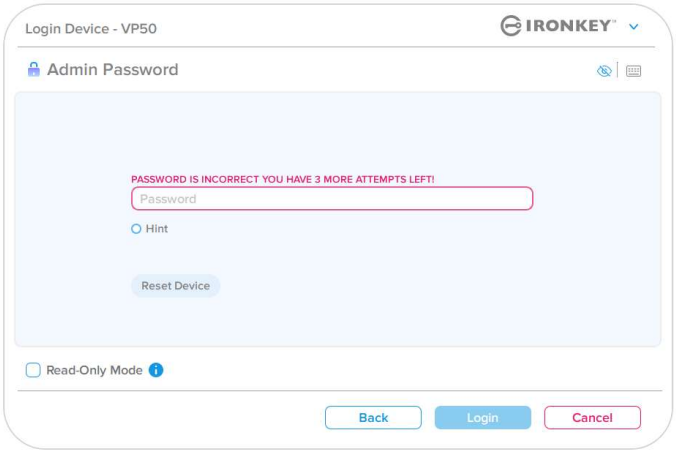


Figure 9.2 - 7th incorrect Password attempt

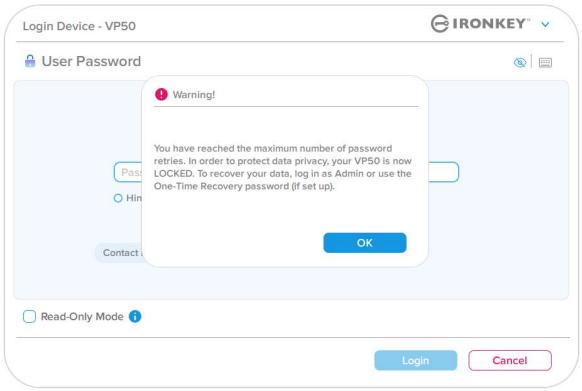
Help and Troubleshooting

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:

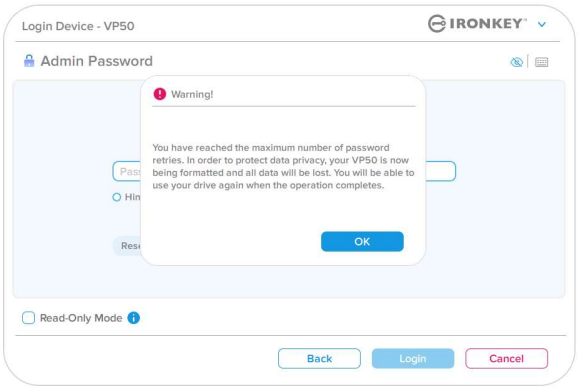
User Password: (Admin/User Enabled)



DEVICE LOCKOUT

(Figure 9.3)

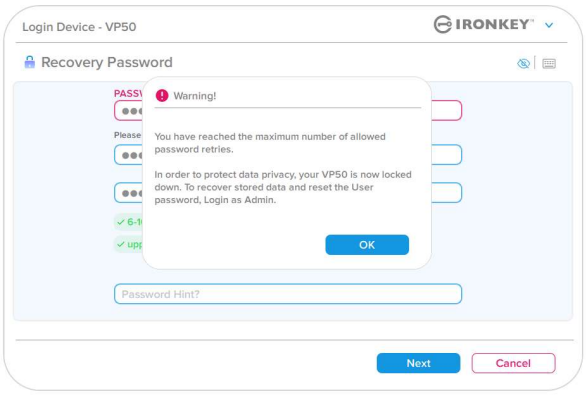
Admin Password (Admin/User Enabled)



DEVICE FORMAT*

(Figure 9.4)

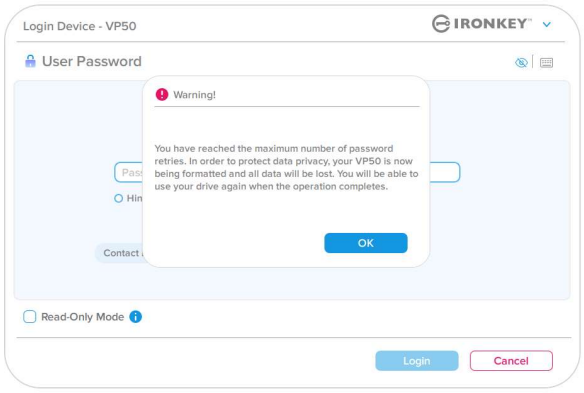
One-Time Recovery: (Admin/User Enabled)



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/VP50C 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/VP50C'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/VP50C will be formatted. This means that all of your data will be erased in the process.*

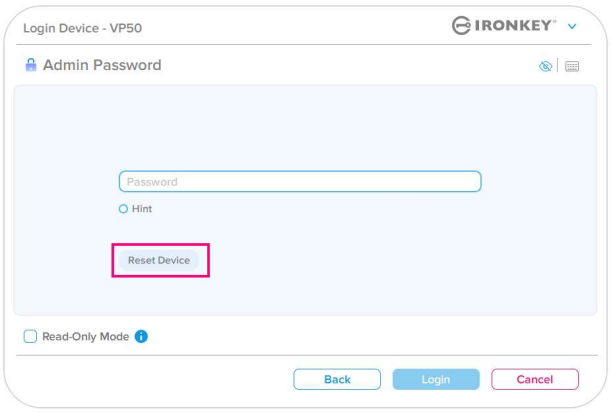


Figure 9.7 - Admin Password: Reset Device Button

- **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)

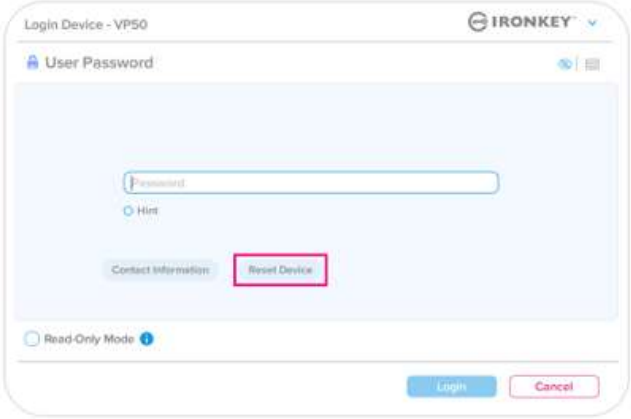


Figure 9.8 - User Password (Admin/user not enabled) Reset Device

- 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.

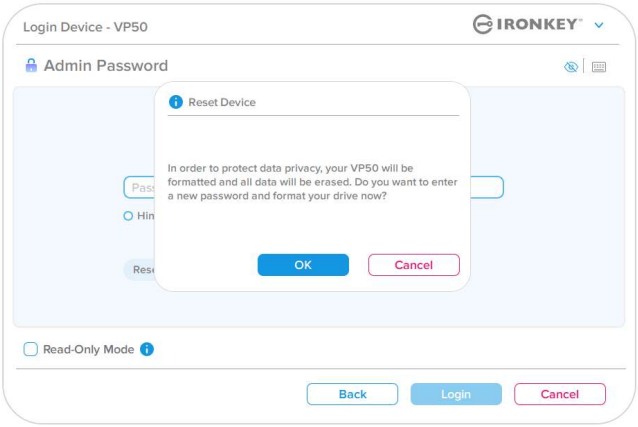


Figure 9.9 - Reset device confirmation

Help and Troubleshooting

Drive Letter Conflict: Windows Operating Systems

- As mentioned in the '*System Requirements*' section of this manual (on page 3), the VP50/VP50C 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/VP50C 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/VP50C 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.

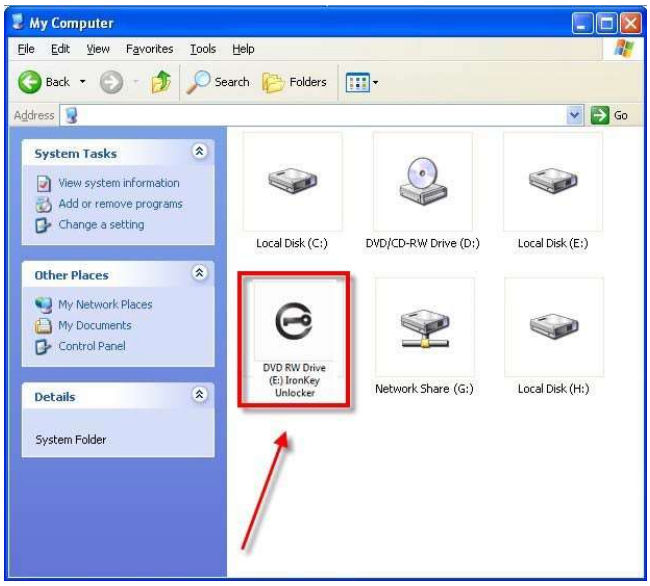


Figure 9.10 - Drive Letter example

In this example (Figure 9.10), the VP50/VP50C 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/VP50C 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/VP50C 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: 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.	 **Figure 9.11 - Unable to Create File Error**
Error copying file or folder: 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.	 **Figure 9.12 - Error Copying File or Folder Error**
Error deleting file or Folder: 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.	 **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/VP50C and log back in, leaving the 'Read-Only Mode' checkbox unchecked prior to login.

© 2022 Kingston Digital, Inc. All rights reserved.

NOTE: IronKey is not liable for technical or editorial errors and/or omissions contained herein; nor for incidental or consequential damages resulting from the furnishing or use of this material. The information provided herein is subject to change without notice. The information contained in this document represents the current view of IronKey on the issue discussed as of the date of publication. IronKey cannot guarantee the accuracy of any information presented after the date of publication. This document is for information purposes only. IronKey makes no warranties, expressed or implied, in this document. IronKey, and the IronKey logo are trademarks of Kingston Digital, Inc., and its subsidiaries. All other trademarks are the property of their respective owners. IronKeyTM is a registered trademark of Kingston Technologies, used under permission of Kingston Technologies. All rights reserved.

FCC Information This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications.

However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment to an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Note: Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.