# User Manual



# IronKey Vault Privacy 50

Find the language and latest documentation here.

For instructions in English
Para instrucciones en Español
💳 💶 🕂 Für Anleitungen in Deutsch
Pour des instructions en Français
Per le istruzioni in Italiano
Image: Antiparticipa
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<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) ENCRYPTED USB 3.2 Gen 1 FLASH DRIVE

User Guide







#### Contents

Introduction	
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)	
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	
Accessing my secure Files	
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	
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 businessgrade 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" is ymbol 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 writeprotect 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**

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





# 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 <u>at least 3</u> 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.



DVD RW Drive (E:) IronKey Unlocker complete, select the option **IronKey.exe** 0 bytes free of 122 MB Common inside of the Unlocker partition that can be CDFS IronKey.app found in File Explorer. (Figure 3.2) Licenses WINDOWS • Please note that the partition letter will vary AUTORUN.INF in: based on the next free drive letter. The drive G IronKey.exe letter may change depending on what devices are connected. In the image below, Figure 3.2 - File Explorer Window/IronKey.exe the drive letter is (E:).

#### **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.		IRONKEY	85 \$	000 ~ » Q
•	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.	IRONNEY	IRONKEY	IRONKEY.exe	Windows
			Figure 3.3 - IKVF	Volume	





# **Device Initialization (Windows & macOS Environment)**

# Language and EULA

	Dévice Initialization - VP50 GIRONKEY · ·
Select your language preference from the drop- down menu and click <b>Next.</b> (See Figure 4.1)	🖷 Language
	What is your preferred Language?
	English
	Figure 4.1 - Language Selection
	Device Initialization - VP50
Review the license agreement and click <b>Next</b> . Note: You must accept the license agreement	License Agreement SOFTWARE LICENSE AGREEMENT IMPORTANT - READ CAREFULLY: THIS SOFTWARE LICENSE AGREEMENT ("Agreement") is a legal agreement between you (either an
before continuing; otherwise, the <b>Next</b> button will remain disabled. (Figure 4.2)	individual of a single entity) and kingston iechnology Company inc. ("kingston"). This Agreement relates to the software accompanying this Agreement, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (the "Licensed Software"). By downloading, installing, copying, or otherwise using the Licensed Software, you agree to be bound by the terms of this Agreement and further agree that the third party licensors of Kingston providing licenses for all or any portion of the Licensed Software shall be third party beneficiaries of this Agreement. If you do not agree to the terms of this Agreement, do not install, copy or use the Licensed Software.
	The Licensed Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Licensed Software is licensed, not sold. The Licensed Software is being provided solely for use with IronKey Encrypted USB product lines.
	Over lacent
	Back Next Cancel
	Figure 4.2 - License Agreement





#### **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:

<ul> <li>Complex Password         <ul> <li>Must contain 6 characters or more (up to 16 characters).</li> <li>Must contain three (3) of the following criteria:</li> </ul> </li> </ul>	Device Initialization - VP50 Password Complex Passphrase Please create a secure Complex password following the criteria below. Please create a secure Complex password following the criteria below.
<ul> <li>Upper Case</li> <li>Lower Case</li> <li>Numerical Digit</li> <li>Special characters (!,\$,&amp;, etc)</li> </ul>	6-16 long uppercase lowercase digit special character Password Hint? Back Next Cancel Figure 4.3 - Complex Password
<ul> <li>Passphrase Password</li> <li>Must contain: <ul> <li>10 characters minimum</li> <li>64 characters maximum</li> </ul> </li> </ul>	Device Initialization - VP50       IRONKEY         Password       Image: Initialization         Plane create a secure Passbords bassword following the criteria baswird       Image: Initialization         Plane create a secure Passbords bassword following the criteria baswird       Image: Initialization         Image: Initialization       Image: Initialization
Password Hint (Optional)A password hint can be useful for providing aclue as to what the password is, should thepassword ever be forgotten.Note: The hint CANNOT be an exact match tothe password.	Password Hint? Figure 4.5 - Password Hint Field





#### Valid and Invalid Passwords

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

Device Initialization - VP50	GIRONKEY .	Device Initialization - VP50	GIRONKEY
A Password	0	A Password	0   =
Complex Passphrase	New O	Complex Passphrase Please create a secure Camplex password following the criteria below.	
ExamplePassw0rd!		ExamplePassw0rd	
ExamplePassw0Rd		ExamplePasswOrd	
≪ 6-16 long ≪ uppercase — ≪ lowercase — ≪ digit — ≪ special character		✓ 6-16 long ✓ uppercase → lowercase → dign special character	
Password Hint?		Pässword Hint?	
🗍 Enable Admin and User Passwords 🚯		Enable Admin and User Passwords ()	
Back	ext Cancel	Back	Cancel
Figure 4.6a - Complex Password Condi	tion Met	Figure 4.6b - Complex Password Condition Opti	onal

	Device Initialization - VP50 GIRON	NKEY -
	A Password	0
For <b>invalid</b> passwords, the Password Criteria Boxes will highlight <b>red</b> and the <b>Next</b> button will be disabled until the minimum requirements are met.	Complex Passphrase Please create a secure Complex password following the criteria below.   ExamplePassword  ExamplePassword	
This applies to both Complex and Passphrase Passwords.	✓ 8-45 long ✓ uppercase ✓ lowercase × digit × special character Password Hint?	
	Enable Admin and User Passwords 🕤	Cancel
	Figure 4.7 - Password Conditions Not Me	t





### Virtual Keyboard

The VP50/VP50C features a Virtual Keyboard that can be used for Keylogger protection.

<ul> <li>To utilize the Virtual Keyboard, locate the keyboard button on the upper-right side of the Device Initialization screen and select it.</li> <li>Personal term of the upper-right side of the Device Initialization screen and select it.</li> <li>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.</li> <li>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.</li> </ul>			Device Initialization - VP50 GIRONKEY v
<ul> <li>keyboard button on the upper-right side of the Device Initialization screen and select it.</li> <li>Device Initialization screen and select it.</li> <li>Image: the second select it.</li> <li>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.</li> <li>To make this feature more robust, you may also choose to randomize the virtual keyboard by selecting randomize the virtual keyboard by selecting randomize in the lower-right of the keyboard. Randomize will arrange the keyboard in a random order.</li> </ul>	•	To utilize the Virtual Keyboard, locate the	A Password 🐵 🔳
<ul> <li>Device Initialization screen and select it.</li> <li>Device Initialization screen and select it.</li> <li>Image: the second select it.</li> <li>Image: the second select it.</li> <li>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.</li> <li>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.</li> </ul>	ı.	keyboard button on the upper-right side of the	Complex Passphrase
<ul> <li>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.</li> <li>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.</li> </ul>		Device Initialization screen and select it.	Please create a secure Passphrase password following the criteria below.
<ul> <li>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.</li> <li>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.</li> </ul>			This is my Passw0rd Example!
<ul> <li>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.</li> <li>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.</li> </ul>			This is my Passw0rd Example!
<ul> <li>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.</li> <li>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.</li> </ul>			✓ 10 characters minimum
<ul> <li>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.</li> <li>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.</li> </ul>			Password Hint?
<ul> <li>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.</li> <li>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.</li> </ul>			Enable Admin and User Passwords 🕐
<ul> <li>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.</li> <li>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.</li> </ul>			Back Next Cancel
<ul> <li>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.</li> <li>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.</li> </ul>			Figure 4.8 - Activating the Virtual Keyboard
	•	Once the virtual keyboard appears, you may also enable <b>Screenlogger Protection</b> . 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 <b>randomize</b> in the lower-right of the keyboard. Randomize will arrange the keyboard in a random order.	Vitual Keyboard       Image: Scienting of Potocian         Image: Ima





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 upperrighthand side of the Device Initialization window.

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

	Device Initialization - VP50	GIRONKEY
	A Password	
To <b>hide</b> the password string, click the gray icon.	Complex Passphrase	
To <b>hide</b> the password string, click the gray icon.	Please create a secure Passphrase password following the criteria b	elow. 🕦
	This is my Passw0Rd Eampie!	
··········	This is my PasswORd Eample	
	✓ 10 characters minimum	
	Password Hint?	
	Enable Admin and User Passwords	
	Back	Cancel
	Figure 4.10 - Toggle 'hide' Passwor	rd
	Device Initialization - VP50	GIRONKEY
	A Password	
	Complex Passphrase	/
To <b>show</b> the hidden password, click the blue icon.	Please create a secure Passphrase password following the criteria	below. 🕤
	••••••	
	✓ 10 characters minimum	
	(Password Him?	
	Enable Admin and User Passwords	
	Back	xt Cancel
	Figure 4.11 - Toggle 'show' Passwo	rd

🕷 kingst





#### 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.

		Device Initialization - VP50	RONKEY
٠	To Enable Admin and User passwords click	A Password	® =
	<b>Passwords'</b> and select <b>Next</b> once a valid password has been chosen. (Figure 4.12)	Complex Passphrase Please create a secure Passphrase password following the criteria below.	
•	If this feature is <b>enabled</b> , then the chosen Password at this screen will be the <b>Admin</b> <b>Password</b> , Click <b>Next</b> to proceed to the <b>User</b>	- 10 starosters minimum. Passwont Hint?	
	<b>Password</b> screen where a password is chosen for the User.	Back Next Figure 4.12 - Enabling Admin and User Passw	Cancel

#### 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.





#### Admin and User Passwords

	Device Initialization - VP50	GIRONKEY
If Admin Role was <b>enabled</b> in the	A User Password	©   =
previous screen, the following screen will prompt for the <u>User Password</u>	Please create a secure Passphrase password following the criteria below.	D
(Figure 4.13) The User Password will have limited capabilities compared to Admin and will be discussed in further	Comirini Password 10 characters minimum	
detail later in this User Guide. (see Page 23)	(Fullsward Hint?	
	C Require password reset on next login	
	Back Next	Cancel

**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 Device - VP50	GIRONKEY -
	of Figure 4.13 is only for the User	A User Password	@   m
	Password and can be enabled to force	Require password reset	
	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 Admin has required that you reset your password; please proceed to crente a new password. O Hin Contact	
	the drive is given to another person to	C Read-Only Mode 1	
	use. (Figure 4.14) Note: For security, the new password		ogin Cancel
	cannot be the same as the temporary password.	Figure 4.14 - Require password reset on (For User Password)	next login





#### **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.)

	Device Initialization - VP50	GIRONKEY
The ' <b>Name'</b> field may contain up to 32 characters, but cannot contain the <b>exact</b> password.	Contact	
The ' <b>Company'</b> field may contain up to 32 characters, but cannot contain the <b>exact</b> password.	Details	
The ' <b>Details'</b> field may contain up to 156 characters, but cannot contain the <b>exact</b> password.	Back	K Cancel
	Figure 4.14 - Contact information	n

**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)

Login Device - VP50 GIRONKEY v	Login Device - VP50	GIRONKEY
🔒 User Password 🛞 📾	Admin Password	8
Contracts information:	Pessyapro D Hint React Device	
Rizád-Only Mode	Read-Only Mode 🚯	
Login Cancel	Back	k Lagin Cancel
Figure 5.1 - User Password Login (Admin enabled)	Figure 5.2 - Admin Pa	ssword Login
ogin for User-Only Mode (Admin not Enable	d) Login Device - VP50	⊖ IRONKEY" → ⊗   ==
As previously mentioned previously on <b>Page 13</b> , 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.	2 (Password O Hint	
	Contact Information Reset Device	
ngle password approach to securing the data on our drive. (Figure 5.3)	Read-Only Mode 1	





# **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:

		Login Device - VP50	GIRONKEY -
1.	Insert the device into the USB port of the host computer and run the <b>IronKey.exe</b> .	A User Password	@   m
2.	Check the <b>Read-Only Mode</b> below the password entry box. (Figure 5.4)	(Passyound O Nint	
3.	Type your device password and click <b>Login</b> . The IronKey will now be unlocked in Read-Only mode.	Contact Information Reset Device	
		C Read-Only Mode ()	
			Login Cancel
		Figure 5.4 - Read-Only Mo	de

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

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

#### **Accessing My Secure Files**

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

Hint: You can also access your files by right clicking the IronKey Icon in the Windows taskbar and clicking Browse VP50. (Figure 6.2)

# GIRONKEY



# **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.



# **Device Options- (macOS Environment)**

<ul> <li>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.</li> <li>Details about these device options can be found on Pages 19-23 of this manual.</li> </ul>	Q       Q       Q         VP50 Settings       D         Browse VP50       Format VP50         Online Support       O         About VP50       Shut down VP50         Shut down VP50       Shut down VP50





# **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.	Login Device - VP50 User Password Warning! Formatting will erase ALL data on your encrypted drive. All data will be lost forever. Are you sure you want to proceed? Yes Cancel OK Cancel
Online Support:	<ul> <li>Figure 6.1 - Format VP50</li> <li>Opens your internet browser and navigates to <u>http://www.kingston.com/support</u> where you can access additional support information.</li> </ul>
About VP50: Provides specific details about the VP50/VP50C, including Application, Firmware and Serial number Information. (Figure 6.2)	About - VP50 GIRONKEY ~ (a) About © 2022 Kingston Technology Corporation.
<b>Note:</b> The unique serial number of the drive will be under the 'Information Column'.	Modules     Version     Information       IKVP50     IKVP50     002324853023863190000062       Application     01.06.0       FW Version     01.06.0       Crypto Library FW     1.00
Shut down VP50:	<ul> <li>Properly shuts down the VP50/VP50C, allowing you to safely remove it from your system.</li> </ul>





# **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)
  - $\circ$  Change the User Password
  - Login Password Reset (For User Password)
  - $\circ$  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.

Settings - VP50	GIRONKEY.	Settings - VP50	GIRONKET
Admin Settings	@1@	@ Admin Settings	8) m
Passwere Contact Info Languar	ge Admin Options	Pasaword Contact Into Lar	nguage Azerrin Options
Current Protward		Current Pisaward	
Please create a secure Complex password following to r	ne criteria bolow.	Please create a secure Complex password follows	ng the criteria bolow.
New Password		(New Password	
Confirm New Password		Contraction Research	
5-15 long		Continue New Password	
uppercase lowercase digit epecter	character	15-16 long	
Commentaria de la commenzación de la commen		uppercese lowercese digit spe	iclai chamicter
Printer Print?		Princesand Print T	
Done	Apply Cancel	Dor	ne Apply Cancel
Figure 7.1 - Password Options		Figure 7.2 - Con	tact Info
			0
iettings - VP50	GIRONKEY v	Settings - VP50	GIRONKEY
ettings - VPS0 ∋ Admin Settings	GIRONKEY" -	Settings - VP50	⊖ IRONKEY ~~
Settings - VPSO S Admin Settings Persyand Contact Inter Langue	G IRONKEY · ·	Settings - VP50 Admin Settings Pessword Contact Info	
Settings - VPSO S Admin Settings Possword Contact Inte Langua	G IRONKEY" v	Settings - VP50 Admin Settings Password Contact Info La	C IRONKEY ~ ~
Settings - VP50 Contact Inte Langua Possward Contact Inte Langua	G IRONKEY" v	Settings - VP50 Admin Settings Password Castact Info La Please arter a new Liser Password below	C IRONKEY · ·
Settings - VPSO S Admin Settings Persward Contact Inte Langua What is your preferred Language?	G IRONKEY" v	Settings - VP50 Admin Settings Password Castact Into La Please enter a new User Password below. Password	C IRONKEY V
Settings - VP50 Contact Info Passward Contact Info What is your preferred Language? English	G IRONKEY" v	Settings - VP50 Admin Settings Password Castact Into La Please enter a new Usar Password below. Password*	GIRONKEY
Settings - VP50 Contact lefts Language? What is your preferred Language? English	e Admin Dations	Settings - VP50  Cathact Info  Pissword  Cathact Info  Pisase enter a new User Password below.  Password  Coofirm PAssword  Coofirm PAssword	GIRONKEY ~
Settings - VP50 Contact lefts Password Contact lefts What is your preferred Language? English	e Admin Dottons	Settings - VP50  Contact Info  Pissword  Contact Info  Pissword  Contact Info  Contact Info  S-55 long	GIRONKEY V
Settings - VP50 C Admin Settings Passward Contact lefts Language? What is your preferred Language? English	G IRONKEY" >	Settings - VP50 Admin Settings Pissword Contact Info La Pissword Contact Info La Pissword Contine PAssword Contine PAssword 5-% long uppercase intercase tight sp	Celli character
Settings - VP50 Contact Infor Poissword Contact Infor Unit is your preferred Language? English	ere Admin Doktors	Settings - VP50 Admin Settings Password Contact Into La Please enter a new User Password below. Password Continn PAssword 5-16 long uppercase lowercase Bight sp	Cironkey ~
Settings - VP50 Contact Information Processor What is your preferred Language? English	ege Admin Dations	Settings - VP50 Admin Settings Password Center Into La Please enter a new User Password below. Password Confirm PAssword 5:46 long uppercase lowercase light so	Cironkey v
Settings - VP50 Admin Settings Poisword Contact Inte Langua What is your preferred Language? English	e Admin Dations	Settings - VP50  Canactings  Password  Contacting  Please enter a new User Password below.  Password  Coofirm PAssword  5-56 long  uppercase lowercane night sp  Ome-Time Recovery Password  Cog Login Passwor	C IRONKEY ~
Settings - VP50  Admin Settings  Password Contact Info Units your preferred Language? English Donce	Admin Dations	Settings - VP50 Canact Inte Pissword Canact Inte Pissword Canact Inte Pissword Continn PAssword S-16 long uppercase Iowercase Bight sp Ome-Time Recovery Password Cone Pissword Cone Time Recovery Password Cone Time Recovery Password	echal character





# VP50/VP50C Settings

#### **User Settings: Admin Enabled**

The User Login limits access to the following settings:



**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**. <u>This configuration does not have access to any</u> <u>Admin options or features</u>. This configuration will have access to the following VP50/VP50C Settings:

#### **Changing and Saving settings**

	Settings - VP50	GIRONKEY .
• Whenever settings are changed in the VP50/VP50C Settings (e.g.)	Admin Settings Pessword     Pessword     Please enter your password     S	imin Options
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)	What I Franç OK Done Ap	ply Cancel
	Figure 7.11 - Password Prompt screen to save VP50/V	P50C 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.





#### **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:	Settings - VP50 GIRONKEY ~
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).	O Admin Settings     Please enter in nive User Password below     One-Time Recovery Password     Please enter in nive User Password Reset •    Force Read-Only User Data • Login Password Reset •    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)	Settings - VP50       © IRONKEY         © Admin Settings.       © © © © © © © © © © © © © © © © © © ©
<b>Note:</b> 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).	Login Device - VP50       IRONKEY         User Password       Require password reset         The Admin has required that you reset your password;       Image: Contract Cont





# **One-Time Recovery Password**

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

One-Time Recovery password	Settings - VP50	GIRONKEY -
<b>Step 1:</b> 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. <b>(Figures 8.4)</b>	Admin Settings Pissword Contact Into Language Piedse enter à new User Password below. Password Confirm Password B-16 long uppercase lowercase digit special choract One-Time Recovery Password Porce Read-Only User Data C Login Password Reset C Done	Apply Cancel
	Settings - VP50	GIRONKEY -
<ul> <li>Step 2: Create a One-Time Recovery password using the same Password criteria the device was initially set with (Complex or Passphrase).</li> <li>Note: Admin password will be required to apply changes.</li> </ul>	One-Time Recovery Password  Please create a secure Complex password following the cri  Admits Possword  Recovery Password  Confirm Recovery Password  G-16 long  uppercase lowercase digit special chara	toria below.
	Figure 8.5 - One-Time Recovery Pa	Save Cancel





# Using One-Time Recovery Password

Stop 1: After the One Time Receivery		
password has been created, a new button will appear on the User Password login screen upon next login. Click on the Recovery	Login Device - VP50 C IRONKEY ~	
Password button to start the process.	Image: Contract Information       Recovery Password       Login: Is: Admini         Read-Only Mode       Image: Cancel         Figure 8.6 - Recovery Password Button	
Step 2: The Recovery Password screen will	Login Device - VP50 GIRONKEY ~	
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)		
<b>p 3:</b> Upon success, you will be taken back the <b>User Password</b> screen. The <b>Recovery</b> <b>sword</b> button is now gone, and the User	Login Device - VP50     User Password	
new User Password. (Figure 8.8)	Fasswars     Diffed     Contact Information     Looin as Admin.	
	Read-Only Mode 1	
	Login Concel	
	Figure 8.8 - User Password Login screen showing the Recovery Password button disappears after successful use.	





### 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.

<ul> <li>To enable Force Read-Only for the User data, click on the box and click 'Apply'. (Figure 8.9)</li> </ul>	Settings - VP50	GIRONKEY V
	Admin Settings     Possword ConnectInfa Language	🕲   📰
<b>Note:</b> 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.	Please enter a nov/User Password below. Password Confirms Password G-16 long uppercase digit special cha One-Time Recovery Password Force Read-Only User Data C Login Password Reset C Dore Figure 8.9 - Enable 'Force Read- (Admin Password will be required	racter Apply Cancel Only User data' I to apply changes)
<ul> <li>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)</li> </ul>	Login Device - VP50	GIRONKEY -
	General User Password	<b>1</b>
	O Hint	
	Contact Information Login as Admin	
	Read-Only Mode	
		Login Cancel
	Figure 8.10 - Read-Only Mode is force and can only disabled b	d enabled for the user y Admin





#### **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.

	Login Device - VP50	GIRONKEY -
<ul> <li>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)</li> </ul>	Contact Information Reset Device Figure 9.1 - Incorrect Password	Logir Cancel
<ul> <li>When a 7<sup>th</sup> 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)</li> </ul>	Login Device - VP50 Admin Password Pressword 5 INCORRECT YOU HAVE 3 MORE ATTEMPTS LEFT Crossword O Hint Reset Device Back Figure 9.2 - 7 <sup>th</sup> incorrect Password	Cancel





**Important:** After a **10<sup>th</sup>** 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 <u>page 18</u> of this User Guide.

Figures 9.3- 9.6 below demonstrate the visual behavior for the 10<sup>th</sup> and final failed logins of each login password method:

<u>0361 1 833 WOLU. (AU</u>	min/User Enabled)	Admin Password (A	Admin/User Enabled)
Login Device - VP50	GIRONKEY -	Login Device - VP50	GIRONKEY -
🔒 User Password	@i 📾	Admin Password	@  =
Warning!		Warning!	
O Hin Confact,	number of password rivercy, your VPSO is now glin as Admin or use the art up):	Vou have reached the maxim retries. In order to protect da being formatted and all data use your drive again when th Res	tum number of password ta privacy, your VP50 is now will be lost. You will be able to te aperation completes.
Read-Only Mode		Read-Only Mode	
	Login Cancel		Back Looin Cancel
DEVICE LO	оскоит	DEVIC	E FORMAT*
(Figure	9.3)	(Figu	re 9.4)
One Time Becovery ()	dmin/Usor Enabled)	Llear Deseuverd / Adr	
One-Time Recovery: (A	Authing Oser Enabled	User Password (Adr	nin NOT Enabled)
Login Device - VP50	GIRONKEY ~	Login Device - VP50	
Login Device - VP50		Login Device - VP50	
Login Device - VP50  Recovery Password  Pass  Warning:  Pass  Warning: Pass	With the User	User Password (Adr Login Device - VP50 User Password User Password Warning! Wou have reached the making Profes in order to protect da being formeter and an dial being formeter and an dial be	INIT INOT Enabled)
Login Device - VP50  Recovery Password  Pass Warning:  Warning:  Wasser Vou have reached the maximum in password retries.  In order to protect data privacy, y in order to privacy, y in order to protect data privacy, y in order to privacy, y in order to protect data privacy, y in or	wither of allowed our VP50 is now locked	Login Device - VP50 User Password User Password Warning! Wurni	Inin INO I Enabled)
Login Device - VP50  Recovery Password  Marsing:  Pass  Warning:  Pass  Warning:  Pass  Du have reached the maximum n password reflex.  In order to protect data privacy, y to three reached the maximum n password, Login as Admin.  Password Him1?	Autimity Oser Enabledy	Login Device - VP50 User Password User Password Wanning! Wu have reached the making retries. In order to protect da builty groun of the again when the Context. Read-Only Mode	Inin INO I Enabled)
Concertmine Recovery: (P Login Device - VP50 Recovery Password Warning: Wurning: W	WITHING USET ETHADIEUT	User Password (Adr Login Device - VP50 User Password Warning W	Inin INOT Enabled)

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.

Kinds





#### **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 <u>not</u> enabled) when the VP50 Launcher is executed. (see *Figure 9.7* and **9.8**)

<ul> <li>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.*</li> </ul>	Login Device - VP50   Admin Password     Admin Password     Preset Only Mode     Back     Concel      Figure 9.7 - Admin Password: Reset Device Button
<ul> <li>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)</li> </ul>	Login Device - VP50       @ IRONKEY         I User Password       Image: Control         I user Password<
<ul> <li>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.</li> </ul>	Login Device - VP50       Cincel         Admin Password       Cincel         Image: Cincel       Cincel



IRONKEY"

#### **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.



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.







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.	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. OK Figure 9.11 - Unable to Create File Error
<b>Error copying file or folder:</b> 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.	Error Copying File or Folder         Cannot copy File1: The disk is write-protected.         Remove the write-protection or use another disk.         OK         Figure 9.12 - Error Copying File or Folder Error
<b>Error deleting file or Folder:</b> 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

**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.



# IRONKEY<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) DISPOSITIVO FLASH USB 3.2 Gen 1 ENCRIPTADO

Guía de usuario







#### Contenidos

Introducción	
Vault Privacy 50 Características	
Acerca de este Manual	
Requisitos del sistema	
Recomendaciones	5
Uso del sistema de archivos correcto	5
Recordatorios de usos	5
Mejores prácticas para la configuración de contraseñas	6
Configurar mi dispositivo	7
Acceso a dispositivos (Entorno Windows)	7
Acceso a dispositivos (Entorno macOS)	7
Inicialización del dispositivo (entorno Windows y macOS)	
Selección de la contraseña	9
Teclado virtual	
Activar visibilidad de contraseña	
Contraseñas de administrador y usuario	
Información de contacto	
Uso del dispositivo (entorno Windows y macOS)	
Inicio de sesión para Administrador y Usuario (Administrador Habilitado)	
Inicio de sesión para el Modo de solo usuario (Administrador no habilitado)	
Desbloqueo en Modo de solo lectura	
Protección contra ataques de fuerza bruta	
Accesando a mis archivos seguros	
Opciones de dispositivo	
Configuración del VP50/VP50C	
Configuración de administrador	
Configuración de usuario: Administrador habilitado	
Configuración de usuario: Administrador no habilitado	
Cambiar y guardar la configuración del VP50/VP50C	
Funciones de administrador	
Restablecer contraseña de usuario	
Restablecer contraseña de inicio de sesión (para Contraseña de usuario)	
Contraseña de recuperación de una sola vez	
Forzar datos de Usuario de solo lectura	
Ayuda y resolución de problemas	
Bloqueo del VP50/VP50C	
Restablecimiento del dispositivo VP50/VP50C	
Conflicto de letras de unidad (sistemas operativos Windows)	
Mensajes de error	



# Kingston





Figura 1: IronKey VP50

Figura 2: IronKey VP50C

# Introducción

El Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C 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/VP50C es superior al uso de Internet y los servicios en la nube para proteger los datos.

VP50/VP50C 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/VP50C 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/VP50C 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 Privacy 50/50C (VP50/VP50C) y se basa en la imagen de fábrica sin cambios personalizados implementados.

#### Requisitos del sistema

Plataforma para PC	Soporte del sistema operativo de la PC
<ul> <li>Intel, AMD y Apple M1 SOC</li> <li>Espacio libre en disco de 15 MB</li> <li>Puerto USB 2.0 - 3.2 disponible</li> <li>Dos letras de unidad consecutivas después de la última unidad física *</li> </ul>	<ul> <li>Windows 11</li> <li>Windows 10</li> <li>Windows 8,1</li> </ul>
* <b>Nota:</b> Vea Conflicto de letras de unidad' en la página 32.	
Plataforma Mac	Compatible con el sistema operativo Mac
<ul> <li>Espacio libre en disco de 15 MB</li> <li>Puerto USB 2.0 - 3.2</li> </ul>	• macOS 11.x – 14.x





# Recomendaciones

Para asegurarse de que haya suficiente suministro de energía para el dispositivo VP50/VP50C, insértelo directamente en un puerto USB en su portátil o escritorio, como se ve en la *Figura 1.1.* Evite conectar el VP50/VP50C 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*.



### Uso del sistema de archivos correcto

El IronKey VP50/VP50C 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/VP50C 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.

# GIRONKEY"



## Mejores prácticas para la configuración de contraseñas

Su VP50/VP50C 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/VP50C eliminará automáticamente los datos encriptados, volviendo a formatearse a sí misma a un estado de fábrica.

## Múltiples contraseñas

El VP50/VP50C 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/VP50C puede admitir tres contraseñas diferentes que puede usar para recuperar datos: Administrador, Usuario y una Contraseña de recuperación de una sola vez.

El VP50/VP50C 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/VP50C se puede restablecer y reutilizar, pero los datos anteriores se borrarán para siempre.

# Modos de contraseña

El VP50/VP50C 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/VP50C 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/VP50C, 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.

# GIRONKEY"



# 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.



# Acceso a dispositivos (Entorno macOS)

Inserte el VP50/VP50C 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/VP50C (o IRONKEY) en el escritorio. (Figura 3.3)







# Inicialización del dispositivo (entorno Windows y macOS)

# Idioma y EULA

	Device Initialization - VP50 GIRONKEY ~
desplegable y haga clic en <b>Siguiente (Next).</b> (Ver figura 4,1)	Language
	Figura 4.1 - Selección de idioma Device Initialization - VP50
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)	Correct Discrete Constrained by Constrained Discrete Discr
	Figura 4.2 - Contrato de licencia





## Selección de la contraseña

En la pantalla de solicitud de contraseña, podrá crear una contraseña para proteger sus datos en el VP50/VP50C, 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	Device Initialization - VP50 GIRONKEY' ~	
<ul> <li>Debe contener 6 caracteres o más (hasta 16 caracteres).</li> </ul>	Password (Section 2014) Passphrase	
<ul> <li>Debe contener tres (3) de los siguientes criterios:         <ul> <li>Mayúsculas</li> <li>Minúsculas</li> <li>Dígito numérico</li> <li>Caracteres especiales (!,\$,&amp;, etc.)</li> </ul> </li> </ul>	Plaase create a secure Complex possword following the criteria below.	
	Figura 4.3 - Contraseña compleja	
Contraseña de frase de acceso • Debe contener: • 10 caracteres mínimo • 64 caracteres como máximo	Device Initialization - VP50       IRONKEY         Password       Passphrase         Complex       Passphrase         Plane create a secure Passphrase bassword following the training basw       Image:	
Sugerencia de contraseña (opcional) Una pista de contraseña puede ser útil para proporcionar una pista sobre cuál es la contraseña, en caso de que la contraseña se olvide. Nota: La pista NO PUEDE coincidir exactamente con la contraseña.	Password Hint? Figura 4.5 - Campo de pista de contraseña	





# 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)

Device Initializat	ion - VP50	GIRONKEY -	Device Initializa	ation - VP50	GIRONKEY
A Password		0	A Password		0
	Complex Passphrase			Complex Passphrase	
	Please create a secure Complex password following the criterik below ExamplePassw0rd!			ExamplePassw0rd	)
	ExamplePassw0Rd			ExamplePassw0rd	)
	≪ 6-16 long ✓ uppercase → lowercase → digit → special character			≪ 6-16 long ≪ uppercase ≪ digit special character	
	Password Hint?			Password Hint?	)
Enable Admin	and User Passwords 🚺		Enable Admin	n and User Passwords 🕜	
	Back	Cancel		Back Next	Cancel
Figura	a 4.6a - Condición de con compleja cumplida	traseña	Figura 4.	6b - Condición de contraseña opcional	compleja

	Device Initialization - VP50
	Password ©
Para contraseñas <b>inválidas</b> , las Casillas de criterios de contraseña se resaltarán en <b>rojo</b> and y el botón <b>Siguiente (Next)</b> se deshabilitará hasta que se cumplan los requisitos mínimos.	Complex     Passphrase       Please create a secure Complex password following the criteria below.     •       ExamplePassword     •       ExamplePassword     •       © 6-66 long
Esto aplica tanto para las Contraseñas complejas como a las Contraseñas de frase de acceso.	





### **Teclado virtual**

El VP50/VP50C cuenta con un Teclado virtual que puede ser utilizado para la protección contra Keylogger.







# 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.

	Device Initialization - VP50	GIRONKEY
	Password	
Para <b>ocultar</b> la cadena de contraseña, haga clic en el icono gris.	Complex Passphrase Please create a secure Passphrase password follower the criteria below This is my Passw0Rd Eample This is my Passw0Rd Eample	•
	v 10 characters minimum Possword Hint?	)
	C Enable Admin and User Passwords 🕤	
	Back Next	Cancel
	Figura 4.10 - Active ocultar' Contraseñ	a
	Device Initialization - VP50	GIRONKEY
	A Password	
	Complex Passphrase	
Para <b>mostrar</b> la contrasena oculta, haga clic en el	Please create a secure Passphrase password following the criteria belo	w. 😗
icono azui.		$\Box$
	✓ 10 characters minimum	
	Password Hint?	
	Enable Admin and User Passwords 6	
	Back Next	Cancel
	Figura 4.11 - Active mostrar' Contraseñ	a





## 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.

		Device Initialization - VP50 GIRO	NKEY -
٠	Para habilitar las <b>Contraseñas de</b>	Password	® =
	administrador y usuario, naga ciic 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)	Complex Passphrase Please create a secure Passphrase password following the criteria below.    Please create a secure Passphrase password following the criteria below.	
•	Si esta función está <b>habilitada</b> , la Contraseña elegida en esta pantalla será la <b>Contraseña de administrador.</b> Haga clic en <b>Siguiente</b> (Next) para pasar a la pantalla <b>Contraseña</b> <b>de usuario</b> , donde se elige una contraseña para el usuario.	Enable Admin and User Passwords Back Next Figura 4.12 - Habilitación de Contraseñas de administrad	Cancel or 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.





# Contraseñas de administrador y usuario

	Device Initialization - VP50	GIRONKEY
Ci al Dal da administradar sa <b>habilitá</b> an	🔒 User Password	@  <b>=</b>
Si el Roi de administrador se <b>habilito</b> en		
la pantalla anterior, en la siguiente	Please create a secure Passphrase password follow	ving the criteria below. 🚯
pantalla se le pedirá la <u>Contraseña de</u>	Firstsword	
<u>usuario</u> (Figura 4.13). La Contraseña de	Continu Password	
usuario tendrá capacidades limitadas	10 characters minimum	
en comparación con la de		
Administrador y se analizará con más	(Processor & Local Processor &	
detalle más adelante en esta Guía del	An isotropy	
usuario. (ver página 23)	Require password reset on next login ()	
	Back	Next Cancel

**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 <b>Requerir el</b>	Login Device - VP50	GIRONKEY V
	restablecimiento de la contraseña en el próximo inicio de sesión' (Require	A User Password	® [ ==
	password reset on next login) en el	Require password reset	
	botón en la esquina inferior izquierda de		
	la Figura 4.13 es solo para la Contraseña	The Admin has required that you reset your password: please proceed to create a new password.	
	de usuario y se puede habilitar para	O Hin	
	forzar al Usuario a iniciar sesion con la	OK	
	Administrador durante el proceso de	Contact	
	inicialización, para luego cambiarla por		
	una contraseña de su elección después	Read-Only Mode 🚺	
	de que el dispositivo se autentifique con	Le	gin Cancel
	la contraseña temporal. Esto es útil		
	cuando el dispositivo se entrega a otra	Figura 4 14 - Requerir restablecimiento de contraser	ia en el próximo inicio
	persona para que la use. (Figura 4.14)	de sesión	
		(Para contraseña de usuario)	
	Nota: Por seguridad, la nueva contraseña		
	no puede ser la misma que la contraseña		
	temporal.		





# 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.)

	Device Initialization - VP50	GIRONKEY
El campo de <b>'Nombre' (Name)</b> puede contener hasta 32 caracteres, pero no puede contener la contraseña <b>exacta</b> .	Contact	
El campo de <b>'Compañía'</b> ( <b>Company</b> ) puede contener hasta 32 caracteres, pero no puede contener la contraseña <b>exacta</b> .	Details	
El campo de <b>'Detalles'(Details)</b> puede contener hasta 156 caracteres, pero no puede contener la contraseña <b>exacta</b> .	Figura 4.14 - Informació	n 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.

# GIRONKEY"



# 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/VP50C, 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 (Iniciar sesión como Administrador), 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)

Login Device - VP50 GIRONKEY	Login Device - VP50	GIRONKEY
🔒 User Password 🛞 📾	Admin Password	<b>8</b>
Contact Information.	Pessword O Hint Reset Device	
Read-Only Mode	Read-Only Mode 1	
Login Cancel	Ba	ack Lagin Cancel
Figura 5.1 - Inicio de sesión con Contraseña de usuario (Administrador habilitado)	Figura 5.2 - Inicio de sesión con Co	ontraseña de administrador
Inicio de sesión para el Modo de solo usuario	Login Device - VP50	GIRONKEY .
(Administrador no habilitado)	🔒 User Password	@[
Como se mencionó anteriormente en la <b>página 13</b> , aunque se recomienda usar la funcionalidad de Ro 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 dat en su dispositivo. (Figura 5.3)	Contract information Reset Device	Login Cancel
Nota: Para habilitar las Contraseñas de administrador y usuario, utilice el botón Restablec el dispositivo (Reset Device) para volver a configur el dispositivo al estado de inicialización, donde puede habilitar las Contraseñas de administrador y usuario. TODOS los datos del dispositivo se formatearán y perderán para siempre cuando se produzca un Restablecer el dispositivo	Figura 5.3 - Inicio de sesión con Administrador no es rar	contraseña de usuario (el stá habilitado)





# 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:

		Lagin Device - VP50	GIRONKEY -
1.	Inserte el dispositivo en el puerto USB de la computadora huésped y ejecute el IronKey.exe.	User Password	@   m
2.	Marque el <b>Modo de solo lectura (Read- Only Mode)</b> debajo del cuadro de ingreso de contraseña. <b>(Figura 5.4)</b>	Phaseward O Hint Contact Information Reset Device	
3.	Escriba la contraseña de su dispositivo y haga clic en <b>Iniciar sesión (Login).</b> La IronKey ahora se desbloqueará en el Modo de solo lectura.	Read-Only Mode  Figura 5.4 - Modo de solo lectur	icolin Cancel

Si desea desbloquear el dispositivo con acceso completo de lectura/escritura a una partición de datos segura, debe apagar el VP50/VP50C e iniciar sesión de nuevo, dejando la casilla de verificación 'Modo de solo lectura' (Read-Only Mode) sin marcar.

**Nota:** Las opciones de VP50/VP50C 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<u>intentos de contraseña fallidos</u>, 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/VP50C (Browse VP50/VP50C)**. (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.



# **Opciones del dispositivo - (Entorno macOS)**







# Opciones de dispositivo

Configuración del VP50 (VP50 Settings):	<ul> <li>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/VP50C' de este manual).</li> </ul>
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) Nota: Se requerirá autentificación por contraseña para el proceso de reformateo.	Login Device - VP50 User Password Warring! Formatting will erase ALL data on your encrypted drive. All data will be lost forever. Are you sure you want to proceed? Yes Cancel
Soporte en línea (Online Support):	OK Cancel         Figura 6.1 - Reformateo del VP50         • Abra su navegador de Internet y navegue a <a href="http://www.kingston.com/support">http://www.kingston.com/support</a> donde puede acceder a información de soporte adicional.
Acerca del VP50 (About VP50): Proporciona detalles específicos sobre el VP50/VP50C, incluidos la información de la aplicación, el firmware y el número de serie. (Figura 6.2)	About - VP50 G IRONKEY' ~ About C 2022 Kingston Technology Corporation.  Modules. Version Information.
Nota: El número de serie único del dispositivo estará debajo de la 'columna de información'.	IKVP50         IKVP50         002324853023863190000062           Application         1.0.0         01.0630           FW Version         01.0630         Crypto Library FW           Loo         Cose           Figura 6.2 - Acerca del VP50
Apagar el VP50 (Shut down VP50):	<ul> <li>Apaga correctamente el VP50/VP50C, lo que le permite eliminarlo de forma segura de su sistema.</li> </ul>

# GIRONKEY"



# Configuración del VP50/VP50C

# 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
  - o Restablecer contraseña de inicio de sesión (para Contraseña de usuario)
  - Habilitar la Contraseña de Recuperación de una sola vez
  - $\circ$  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.

@   ==	Admin Settings	8 m
Annual Contents		
- Admini Officiali	Password Contact Info Language	Admin Options
	Current Presward	
rlá bolow.	Please create a secure Complex password following the	Hlená Boláw.
	Mow Password	
	Confirm New Password	
	5-16 Jana	
164	uppercese lowercese digit special ch	aracter
	Commentation in the second	
	(Privided mint)	
Apply Cancel		
	Done	Apply Cancel
ontraseña	Figura 7.2 - Información	de contacto
GIRONKEY .	Settings - VP50	GIRONKEY
	Admin Settings	@) =
Admin Options	Password Contact Info Language	Admin Optimi
	Please enter a new User Password below.	
	Pasaward	
	Confirm Pácourori	
	Construction of the	
	intertase lowercase tion special c	baractor
	Abbaranda mananana wan shasaya	
	One-Time Recovery Password	
	🗋 Force Read-Only User Data 🚯 📋 Login Password Reset 🜖	
Apply Cancel	Done	Apply Cancel
idiama	Figura 7.4 - Oncionas do A	dministrador
	Antibutions	is before       Image: Concel         is before       Image: Concel





# Configuración del VP50/VP50C

# Configuración de usuario: Administrador habilitado

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

Contraseña (Password):	Settings - VP50 GIRONKEY ~
Le permite cambiar su propia Contraseña	O Admin Settings
de administrador y/o pista. (Figura 7.5)	Pessword Contact Info Language Admin Options
	What is your preferred Language?
	English
	Dome Apply Cancel
F	Figura 7.5 - Opciones de contraseña (Admin habilitado: Inicio de sesión de usuario)
Información de contacto (Contact Info):	Settings - VP50 GIRONKEY V
Le permite agregar/ver/cambiar su	User Settings     Password Contact Into Language
información de contacto. (Figura 7.6)	Please enter your information below:
	(Mamu
	Company.
	Anomae -
	Ubre Ashiy Cance
F	igura 7.6 - Información de contacto (Admin habilitado: Inicio de sesión de usuario)
Idioma (Language):	Settings - VP50 GIRONKEY V
idioma actual. (Figura 7.7)	@ User Settings
	Password Context100x Language
	What is your preferred Language?
	Dana Apply Cancel
	Figura 7.7 - Configuración del idioma (Admin habilitado: Inicio de soción do
	usuario)

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





# Configuración del VP50/VP50C

# Configuración de usuario: Administrador no habilitado

Como se mencionó anteriormente en la página 12, la inicialización del VP50/VP50C 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/VP50C:

# Cambiar y guardar la configuración



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/VP50C.

# GIRONKEY"



# 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:	Sattings VD50 GIRONKEY v
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).	Settings:       V:SU         Image:       Admin Settings         Image:       Admin Settin
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)	Settings - VP50       IRONKEY         Ø Admin Settings       Impunge         Perswent       Conact link
<b>Nota:</b> 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).	Login Device - VP50       IRONKEY         User Password       IRONKEY         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that you reset your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that you reset your password;         Image: The Adminish has required that you reset your password;       Image: The Adminish has required that you reset your password;         Image: The Adminish ha





# 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	Settings - VP50 GIRONKEY ~
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)	Image: Admin Settings       Image: Admin Settings         Pessword       Image: Admin Settings         Pessword       Image: Admin Settings         Pessword       Image: Admin Settings         Pessword       Image: Admin Settings         Image: Admin Settings       Image: Admin Settings         Pessword       Image: Admin Settings         Image: Admin Settings       Image: Admin Setings         Image: Admin Setings       Image: Admin
<ul> <li>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).</li> <li>Nota: Se requerirá la Contraseña de administrador para aplicar los cambios.</li> </ul>	Settings - VP50 Concerning Password  Please create a secure Complex password following the criteria below:  Admits Password  Recovery Password  Confirm Recovery Password  orden in the criteria below:  orden in the cr
	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







# 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	Settings - VP50	GIRONKEY -
los Datos de usuario, haga clic en el cuadro y haga clic en 'Aplicar' (Apply). (Figura 8.9)	Admin Settings     Possword idonaics Info Languag	(®) 🗃
<b>Nota:</b> 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.	Please enter a new User Password below: Password Confirm Password G-16 long uppercase lowercase digit special to One-Time Recovery Password Force Read-Only User Data C Login Password Reset C Cone Figura 8.9 - Habilitar 'Forzar datos de Usu Read-Only User of (Se requerirá la Contraseña de administration)	character Apply Cancel uario de solo lectura' ('Force flata) dor para aplicar los cambios)
<ul> <li>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)</li> </ul>	Login Dévice - VP50  User Password  Pasakood  O Hint  Contact Information Login as Admin  Read-Only Mode	
	Figura 8.10 - El Modo de solo lectura está Usuario y solo puede ser deshabilita	habilitado por fuerza para el do por el Administrador





### Bloqueo del dispositivo

El VP50/VP50C 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.

	Login Device - VP50	GIRONKEY .
<ul> <li>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)</li> </ul>	User Password	0
	PASSWORD IS INCORRECT Producerd O Hint Contact Information Reset Device Read-Only Mode	Logir Cancel
	Figura 9.1 - Mensaje de Contra	Seña incorrecta
<ul> <li>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)</li> </ul>	Admin Password  PASSWORD IS INCORRECT YOU HAVE 3 MORE ATTEMPTS LEFT  Reset Device  Reset Device  Reset Device	
	Back	Légin Cancel
	Figura 9.2 - séptimo intento contraseña	incorrecto de





## 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 <u>formateará los datos y todos los datos del dispositivo se</u> <u>perderán para siempre.</u> Los comportamientos también se mencionan en la <u>página 18</u> 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:

Login Device - VP50	GIRONKEY .	(Administrador/Usuario habi	litado)
🔒 User Password	@i 📾	Login Device - VP50	GIRONKEY
9 Warning!		Admin Password	@ 1
Vou have reached the maximum n retries. In order to protect data pri LOCKED. To recover your data, loy One-Time Recovery password () fa	umber of password Vacy, your VPS0 is now pin as Admin or use the	You have reached the maximum retries. In order to protect data p being formated and all allow was your drive again when the op	number of password r/wcgi, your VP50 is now block 'tow will be able to peration completes.
Read-Only Mode 1		Réss	OK
	Lopin Cancel	Read-Only Mode ()	
BLOQUEO DEL	DISPOSITIVO		Back Lowin Cancel
(Figura 9.3)		REFORMATEO DEL DISPOSITIVO * (Figura 9.4)	
peración de una sola ve habilita	z: (Administrador/usuario ado)	Contraseña de usuario habilit	o (Administrador NO ado)
peración de una sola ve habilita	z: (Administrador/usuario ado) GIRONKEY	Contraseña de usuario habilit	o (Administrador NO ado)
peración de una sola ve habilit: Login Device - VP50	zz: (Administrador/usuario ado) GIRONKEY ~ © =	Contraseña de usuario habilit	) (Administrador NO ado) GIRONKEY
Login Device - VP50 Recovery Password    Pass	zz: (Administrador/usuario ado)	Contraseña de usuario habilit Login Device - VP50 User Password Vierning!	o (Administrador NO ado) GIRONKEY SI S
Recovery Password  Recovery Password  Warning:  Warning: Warning:  Warning: Warn	zz: (Administrador/usuario ado)	Contraseña de usuario habilit Login Device - VP50 User Password User Password Warning! Two have reached the maximum Verties. In drader to protect data p being forumate and al data use your drive again when the op	> (Administrador NO :ado) © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY
Image: second secon	zz: (Administrador/usuario ado)	Contraseña de usuario habilit Login Device - VP50 User Password User Password Varning Warning Warning Device - VP50 Varning User Password Contect	> (Administrador NO :ado) © IRONKEY © IRONKEY Norther of passent ridary pure VMS0 is now benet, the unit to adde to berefor completes.
A Recovery Password	zz: (Administrador/usuario ado)	Contraseña de usuario habilit Login Device - VP50 User Password User Password Wurning! Wu have resched the maximum reting chiefer de protect data p being context Context Read-Only Mode C	b) (Administrador NO ado) C IRONKEY C IRONKE
Anabilitz  Login Device - VP50  Recovery Password  Anability  Warning:  Warning:	zz: (Administrador/usuario ado)	Contraseña de usuario habilit Login Device - VP50 User Password User Password Varming! Var heve reached the maximum being for portect data p being contexten and the maximum being contexten an	> (Administrador NO :ado) C IRONKEY C IRON

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/VP50C 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/VP50C.





#### 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 <u>no</u> está habilitado) cuando se ejecuta el lanzador del VP50/VP50C. (ver **Figura 9.7** y **9.8**)

<ul> <li>Esta opción le permitirá crear una nueva contraseña, pero para proteger la privacidad de sus datos, el VP50/VP50C se formateará. Esto significa que todos sus datos se borrarán en el proceso.*</li> </ul>	Login Device - VP50 Admin Password Hins Read-Only Mode Back Cone Cancel
	Figura 9.7 - Contraseña de administrador: Botón de Restablecer dispositivo (Reset Device)
<ul> <li>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)</li> </ul>	Login Device - VP50       IRONKEY         I User Password       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
<ul> <li>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.</li> </ul>	Login Device - VP50       CinconKEY'          Admin Password       Image: Cincol





#### 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/VP50C 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/VP50C 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/VP50C 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.



En este ejemplo (Figura 9.10), el VP50/VP50C 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/VP50C 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/VP50C 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.





### Mensajes de error

No se puede crear archivo: 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.	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. OK Figura 9.11 - No se puede crear, Error de archivo
Error al copiar archivo o la carpeta: 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.	Frror Copying File or Folder Cannot copy File1: The disk is write-protected. Remove the write-protection or use another disk.
<b>Error al borrar archivo o la carpeta:</b> 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.	Error Deleting File or Folder       Image: Cannot delete File1: The disk is write-protected.         Remove the write-protection or use another disk.         OK

**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/VP50C e iniciar sesión de nuevo, dejando la casilla de verificación 'Modo de solo lectura' (Read-Only Mode) sin marcar.





Anleitung



**Kingston** 





#### Inhalt

Einführung	3
IronKey Vault Privacy 50 Funktionen	4
Über diese Bedienungsanleitung	4
Systemvoraussetzungen	4
Empfehlungen	5
Verwenden des korrekten Dateisystems	5
Hinweise zur Verwendung	5
Bewährte Praktiken für die Passwort-Einrichtung	6
	_
Einrichten des Gerats	······ /
Geratezugriff (Windows-Umgebung)	/
Geratezugriff (macOS-Umgebung)	/
Gerätenutzung (Windows- und macOS-Umgebung)	
Passwort-Auswahl	9
Virtuelle Tastatur	
Umschalten der Passwortsichtbarkeit	12
Admin- und Benutzer-Passwörter	13
Kontaktinformationen	
	10
Geratenutzung (Windows- und macOS-Umgebung)	
Anmelaung für Admin und Benutzer (Admin aktiviert)	
Anmeidung für Nur-Benutzer-Wodus (Admin nicht aktiviert)	
Entsperren im Schreibschutz-Woaus	1/
Schutz vor Brute-Force-Angritten	
Zugriff auf die sicheren Dateien	
Geräteoptionen	19
VP50/VP50C Einstellungen	
Admin-Einstellungen	
Benutzereinstellungen:Admin aktiviert	22
Benutzereinstellungen:Admin nicht aktiviert	23
Ändern und Speichern von VP50/VP50C Einstellungen	
Admin-Europhian	25
Renutzer-Dacswort	2J 2⊑
Anmelde Passwort zurücksetzen /für Penutzer Passwort)	25
Finmaligas Wiederberstellungs Passwort	
Eininaliges wiedernerstenungs-Passwort	20 20
שלוו בוטצבשנווענצוב סבווענצבו עמנפון בוצאוווצבוו	28
Hilfe und Fehlerbehebung	
VP50/VP50C Sperrung	
VP50/VP50C Gerät zurücksetzen	
Konflikt von Laufwerksbuchstaben (Windows Betriebssysteme)	
Fehlermeldungen	



# Kingston





Abb. 1: IronKey VP50

Abb. 2: IronKey VP50C

# Einführung

Der Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C 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/VP50C Serie bei der Datensicherung der Nutzung von Internet und Cloud-Diensten überlegen.

Der VP50/VP50C 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" is 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/VP50C 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/VP50C 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 50/50C (VP50/VP50C), sie basiert auf dem Produktbild, ohne Personalisierungen.

### Systemvoraussetzungen

<ul> <li>PC-Plattform         <ul> <li>Intel, AMD &amp; Apple M1 SOC</li> <li>15MB freier Festplattenspeicher</li> <li>Freier USB 2.0 – 3.2-Anschluss</li> <li>Zwei freie, aufeinanderfolgende Laufwerksbuchstaben nach dem letzten physischen Speicher*</li> </ul> </li> <li>*Hinweis: Siehe "Laufwerksbuchstabenkonflikt"</li> </ul>	<ul> <li>Unterstützte PC-Betriebssysteme</li> <li>Windows 11</li> <li>Windows 10</li> <li>Windows 8,1</li> </ul>
auf Seite 32.	
Mac Plattform	Unterstützte Mac-Betriebssysteme
<ul> <li>15MB freier Festplattenspeicher</li> <li>USB 2.0 – 3.2 Anschluss</li> </ul>	• macOS 12.x – 15.x





# Empfehlungen

Um eine ausreichende Stromversorgung des VP50/VP50C sicherzustellen, schließen Sie ihn direkt in einen USB-Anschluss Ihres Notebooks oder PCs an, siehe **Abb. 1.1**. Schließen Sie den VP50/VP50C 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/VP50C 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/VP50C 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 vom Betriebssystem sicher entfernen, bevor er herausgezogen wird
- Den Stick niemals herausziehen, wenn die LED leuchtet. Denn dadurch kann der USB-Stick beschädigt und eine Neuformatierung erforderlich sein, 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.

# GIRONKEY"



# Bewährte Praktiken für die Passwort-Einrichtung

Der VP50/VP50C ist mit starken Sicherheitsvorkehrungen ausgestattet. Dazu gehört ein Schutz gegen Brute-Force Angriffe, der Angreifer am Erraten von Passwörtern hindert, indem er die möglichen Passwort-Eingaben auf 10 Versuche begrenzt. Wenn das Limit des USB-Sticks erreicht ist, löscht der VP50/VP50C automatisch die verschlüsselten Daten unwiederbringlich und formatiert sich selbst zurück auf den Werkszustand.

# Mehrfach-Passwort

Der VP50/VP50C 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/VP50C drei verschiedene Passwörter unterstützen, die Sie zur Wiederherstellung von Daten verwenden können – Admin, Benutzer und das einmalige Wiederherstellungs-Passwort.

Der VP50/VP50C 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/VP50C kann zurückgesetzt und wieder verwendet werden, aber die vorherigen Daten werden für immer gelöscht.

# Passwort-Modi

Der VP50/VP50C 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/VP50C 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/VP50C-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.



# Gerätezugriff (macOS-Umgebung)

Stecken Sie den VP50/VP50C 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/VP50C (oder IRONKEY) auf dem Desktop. (Abb. 3.3)






## Geräteinitialisierung (Windows- und macOS-Umgebung)

### Sprache und EULA

	Dévice Initialization - VP50 GIRONKEY v
Wahlen Sie die von Ihnen gewunschte Sprache aus dem Dropdown-Menü aus und klicken Sie auf <b>Weiter (Next)</b> . (Siehe Abb. 4,1)	Language     What is your preferred Language):
	Engline 💟
	Abb. 4.1 – Sprachauswahl
Lesen Sie die Lizenzvereinbarung und klicken Sie auf <b>Weiter (Next)</b> . Hinweis: Die Schaltfläche <b>Weiter (Next)</b> wird erst aktiviert, nachdem Sie die Lizenzvereinbarung akzeptiert haben. (Abb. 4.2)	Device hildlization + VP50     Concel      Device hildlization
	Abb. 4.2 – Lizenzvereinbarung





#### Passwort-Auswahl

Auf dem Bildschirm der Passwortabfrage können Sie ein Passwort erstellen, um die Daten auf dem VP50/VP50C 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	Device Initialization - VP50 GIRONKEY	~
<ul> <li>Muss mindestens 6 Zeichen lang sein (bis zu 16 Zeichen).</li> </ul>	Password (©) The second	3
<ul> <li>Muss 3 (drei) der folgenden Kriterien enthalten:         <ul> <li>Großbuchstabe</li> <li>Kleinbuchstabe</li> <li>Zahl</li> <li>Sonderzeichen (!,\$,&amp; usw.)</li> </ul> </li> </ul>	Please create a secure Complex password following the criteria below.  Please create a secure Complex password following the criteria below.  Please create a secure Complex password?  6-16 long uppercase lowercase digit special character  Pleaseword Hon17  Enable Admin and User Passwords  Back Mext Cancel	
Descurent els Describuese	Abb. 4.3 – Komplexes Passwort	~
<ul> <li>Muss enthalten:</li> <li>Minimal 10 Zeichen</li> <li>Maximal 64 Zeichen</li> </ul>	Device Initialization - VP50 Password Complex Passphrase Reset reacts a social Password following the others below (Control Password) (Control Password following the others below (Control Password follo	
Passwort-Hinweis (optional) Ein Passwort-Hinweis kann nützlich sein, um einen Hinweis auf das Passwort zu geben, falls das Passwort einmal vergessen werden sollte. Hinweis: Der Hinweis und das Passwort dürfen NICHT identisch sein.	Password Hint? Abb. 4.5 – Passwort-Hinweisfeld	





#### 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)

Device Initialization - VP50 GIRC	NKEY .	Device Initialization - VP50	BIRONKEY
Password	01	8 Password	0
Complex Passphrase		Complex Passphrase	
Please create a secure Complex password following the criteria below.		Please create a secure Complex password following the criteria below. 🜖	
ExamplePassw0rdl		ExamplePassw0rd	
ExamplePassw0Rd		ExamplePasswOrd	
≪ 646 long ≪ uppercase ≪ lowersase ≪ digit ≪ special churacter		✓ 6-16 long ✓ uppercase ✓ lowercase ✓ digit special character	
Password Hint?		Password (lint?	
] Enable Admin and User Passwords 🕕		Enable Admin and User Passwords 👔	
Back Next	Cancel	Back Next	Cancel
Abb. 4.6a – Bedingung für komplexes Passwort e	rfüllt	Abb. 4.6b – Bedingung für komplexes Passwort ist o	ptional







#### **Virtuelle Tastatur**

Der VP50/VP50C verfügt über eine virtuelle Tastatur, die zum Schutz vor Keyloggern verwendet werden kann.







#### 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.

	Device Initialization - VP50	GIRONKEY
	A Password	0
Klicken Sie auf das graue Symbol, um die	Complex Passphrase	
Passwortzeichemoige zu verbeigen (mue).	Please create a secure Passphrase password following t	he criteria below. 🕕
(	This is my PasswORd Eample!	
0	This is my PasswORd Eample	)
	210 etwasters minimum	
	Passwicka Hint?	
	Enable Admin and User Passwords	
	Back	Next Cancel
	Abb. 4.10 – Auf Passort "verbergen (h	ide)" umschalten
	Device Initialization - VP50	GIRONKEY
	A Password	
Auf das blaue Symbol klicken, um das verborgene	Complex Passphrase	
Auf das blade Symbol Klicken, din das verborgene	Please create a secure Passphrase password following	the criteria below.
Passwort <b>anzuzeigen</b> .		
	********************	
	-/ 10 characters minimum	
	Parameter Hint?	
	Enable Admin and User Passwords ()	
	Back	Next Cancel
	Abb. 4.11 – Auf Passort "anzeigen (sh	ow)" umschalten





#### 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 <b>Weiter (Next)</b> , um zum Bildschirm
	Benutzer-Passwort (User Password) zu
	wechseln, wo ein Passwort für den Benutzer
	ausgewählt wird.

Password				۵ ا
	Complex	Passphrase		
	Please create a secure Passphra	se password following the cr	itería below. 🕤	
1	10 characters minimum			
/	Password Hint?			
-				
Enable Admin	and User Passwords 👔			
		Back	Next	Cancel
bb / 12	- Aktiviaran yan	Admin und Bo	autzor Pace	wörtorn
100. 4.12	- ARtivieren von A	Autilitie und De	141261-1433	wortern

#### 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.





#### Admin- und Benutzer-Passwörter

	Device Initialization - VP50	GIRONKEY
Wenn im vorherigen Bildschirm die	🔒 User Password	0 8
Admin-Rolle aktiviert (enabled) wurde,	Please create a secure Passphrase password following	the criteria below. 👔
wird im folgenden Bildschirm das	Pessword	
Benutzer-Passwort (User Password)	Confirm Password	
abgefragt (Abb. 4.13). Das Benutzer-	10 characters minimum	
Passwort hat im Vergleich zum Admin-		
Passwort nur eingeschränkte	Concerned blint?	
Möglichkeiten und wird später in dieser	Pesswuru minu	
Bedienungsanleitung näher erläutert.	Require password reset on next login	
(Siehe Seite 23)		
	Back	Next Cancel

**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	Login Device - VP50	GIRONKEY -
nächster Anmeldung anfordern (Require	🔒 User Password	@   =
unteren linken Ecke von <b>Abb. 4.13</b> gilt	<ul> <li>Require password re</li> </ul>	eset
nur für das Benutzer-Passwort und kann		
aktiviert werden, um den Benutzer zu	The Admin has required to	hat you reset your password;
zwingen, sich mit dem temporären	please proceed to create     O Hin	a new password.
Passwort anzumelden, das vom		
Administrator während des	Contact	ок
Initialisierungsprozesses festgelegt		
wurde. Er kann es dann in ein Passwort	Read-Only Mode	
seiner Wahl ändern, nachdem der USB-		
Stick mit dem temporären Passwort		Login Cancel
authentifiziert wurde. Dies ist nützlich,		
wenn der USB-Stick einer anderen	Abb. 4.14 – Passwort-Rücksetze	en bei nächster Anmeldung anfordern
Person zur Nutzung überlassen wird.	(Für Benı	utzer-Passwort)
(Abb. 4.14)		
Hinweis: Aus Sicherheitsgründen darf		
das neue Passwort nicht mit dem		
temporären Passwort identisch sein.		





#### 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.)

	Device Initialization - VP50	GIRONKEY
Im Feld " <b>Name</b> " können bis zu 32 Zeichen eingegeben werden, das <b>genaue</b> Passwort darf jedoch nicht darin enthalten sein.	Contact	
Im Feld " <b>Firma (Company)</b> " können bis zu 32 Zeichen eingegeben werden, das <b>genaue</b> Passwort darf jedoch nicht darin enthalten sein.	Desart	
Im Feld " <b>Details</b> " können bis zu 156 Zeichen eingegeben werden, das <b>genaue</b> Passwort darf jedoch nicht darin enthalten sein.	Back Abb. 4.14 – Kontaktinford	QK Cancel

**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/VP50C 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)

Login Device - VP50	Login Device - VP50	GIRONKEY
🔒 User Password 🛞 🚍	Admin Password	8 m
Contact Information Login as Admin	Presented O Hint Reset Device	
Read-Only Mode	Read-Only Mode 🚯	
Login Cancel	Back	Login
Abb. 5.1 – Anmeldung mit Benutzer-Passwort (Admin aktiviert)	Abb. 5.2 – Anmeldung mit Adm	nin-Passwort
Anmeldung für Nur-Benutzer-Modus (Admin	Login Device - VP50	GIRONKEY -
nicht aktiviert)	🔒 User Password	<u></u>
Wie bereits auf <b>Seite 13</b> 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)	Pessevent O Hint Contact Information Reset Device Read-Only Mode	Login Cancel
Hinweis: Verwenden Sie zum Aktivieren von Admin- und Benutzer-Passwörtern die Schaltfläche Gerät zurücksetzen (Reset Device), um den USB-Stick wieder in den Initialisierungszustand zu versetzen, in dem Admin- und Benutzer-Passwörter aktiviert werden können. ALLE Daten auf dem Stick werden formatiert und gehen für immer verloren, wenn "Gerät zurücksetzen (Reset Device)" durchgeführt wird.	Abb. 5.3 – Anmeldung mit Benutzer-Pa aktiviert)	sswort (Admin nicht





## 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:

		Login Device - VP50 GIRON	KEY" Y
1.	Stecken Sie das Gerät in den USB- Anschluss des Host-Computers und führen Sie die Datei <b>IronKey.exe</b> aus.	B User Password	8
2.	Aktivieren Sie das Kontrollkästchen Schreibgeschützt (Read-Only) unter dem Passworteingabefeld. (Abb. 5.4)	Contact Information Reset Device	
3.	Geben Sie Ihr Gerätepasswort ein und klicken Sie auf <b>Anmelden (Login)</b> . Der IronKey wird nun im Schreibschutz- Modus entsperrt.	Read-Only Mode 1	Cancel

Wenn Sie den Stick mit vollem Lese-/Schreibzugriff auf die sichere Datenpartition entsperren möchten, müssen Sie den VP50/VP50C vom Betriebssystem sicher entfernen und sich erneut anmelden, wobei das Kontrollkästchen "Schreibgeschützt (ReadOnly)" nicht markiert sein darf.

**Hinweis:** Die VP50/VP50C 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 <u>10 fehlgeschlagenen Passworteingabeversuche</u> 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 <u>NICHT</u> 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 "Immeraktive"-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/VP50C durchsuchen (Browse VP50/VP50C) 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.



## Geräteoptionen – (macOS-Umgebung)





## Geräteoptionen

VP50 Einstellungen:	<ul> <li>Ändern des Anmelde-Passworts, der Kontaktinformationen und anderer Einstellungen. (Weitere Einzelheiten zu den Geräteeinstellungen finden Sie im Abschnitt "VP50/VP50C Einstellungen" in dieser Bedienungsanleitung.)</li> </ul>
VP50 durchsuchen:	Damit können Ihre gesicherten Dateien angezeigt werden.
<ul> <li>VP50 formatieren:</li> <li>Mit dieser Funktion können Sie die sichere</li> <li>Datenpartition formatieren. (Warnhinweis:</li> <li>Alle Daten werden unwiederbringlich</li> <li>gelöscht) (Abb. 6.1)</li> <li>Hinweis: Zum Formatieren ist eine</li> <li>Passwort-Authentifizierung erforderlich.</li> </ul>	Login Device - VP50 User Password Varning! Formatting will erase ALL data on your encrypted drive. Alt data will be lost forever. Are you sure you want to proceed? Vos Cancel
Online-Support:	Abb. 6.1 – VP50/VP50C formatieren • Öffnen Sie Ihren Internet-Browser und navigieren Sie zu http://www.kingston.com/support/, wo Sie Zugang zu wo Sie Zugang zu weiteren Support-Informationen haben.
Über VP50: Hier finden Sie spezifische Informationen über den VP50/VP50C, einschließlich Informationen zu Anwendung, Firmware und Seriennummer. (Abb. 6.2)	About - VP50 G IRONKEY" ~ () About © 2022 Kingston Technology Corporation.
<b>Hinweis:</b> Die individuelle Seriennummer des Laufwerks finden Sie in der Spalte "Information (Informationen)".	Modules     Version     Information       IKVP50     IKVP50     002324853023863190000062       Application     1.0.0.0       PW Version     0.00       Crypto Library FW     1.00
VP50 trennen:	Fährt den VP50/VP50C ordnungsgemäß herunter, damit Sie ihn sicher aus Ihrem System entfernen können.





## VP50/VP50C-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)
   O Benutzer-Passwort ändern
  - o Anmelde-Passwort zurücksetzen (für Benutzer-Passwort)
  - o Einmaliges Wiederherstellungs-Passwort aktivieren
  - o Schreibschutz-Modus für Benutzerdaten erzwingen

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

Admin Settings     Control Mo     Language     Admin Options     Control Mo     Language     Admin Options     Control Mo     Control Mo
Password     Common Password       Current Password       Piease create a secure Complex password following the criteria biolow:       Now Password       Contarn New Password       Order State       Biolog       Uppercase       (Bestord Hint?
Current Password  Please create a secure Complex password following the criteria balow: New Password  Continut New Password  6-16 long  Uppercase lowercase digit special citeracter  Pleasword Hint?
Piease create a secure Complex password following the criteria biolow:           New Password           Confirm New Password           6-16 long           Uppercase           Uppercase           Précevercise
New Password . Confirm New Password . 6-16 long Uppercase lowercase digit special character (Péssword Hint?
Conflorm New Possiword 6-15 Iong Uppercase lowercase digit special character (Pécsivord Hint?
6-15 long Uppercase lowercase digit special character (Pécsword Hint?
6-16 long Uppercase lowercase digit special character (Pecsword Hint?
Uppercase lowercase digit special character
(Pássword Hint?
Printsword Prints
Done Ápply Cancel
Abb. 7.2 – Kontaktinformationen
Settings - VP50 GIRONKEY
Admin Settings
Password Contact Info Languaum Admin Com-
Please enter a new User Password below.
Pasaword
Coofirm Prissword
15-16 long
uppercase (owercane might special character
One-Time Recovery Password
🗋 Force Read-Only User Data 😗 🔄 Lógin Password Reset 🌖
Done Apply Cancel
Abb. 7.4 – Admin-Optionen





## VP50/VP50C-Einstellungen

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

Die Benutzeranmeldung beschränkt den Zugriff auf die folgenden Einstellungen:

Passwort (Password):	Settings - VP50	GIRONKEY -
Ermöglicht Ihnen, Ihr eigenes Benutzer-	Admin Settings	
Passwort bzw. Ihren Hinweis zu ändern. ( <i>Abb. 7.5</i> )	Password Cantact Info	Language Admin Options
	What is your preferred Language?	
	English	
		Done Apply Cancel
	Abb. 7.5 – Passwort-Optionen (Adm	nin aktiviert: Benutzeranmeldung)
	Settings - VP50	GIRONKEY" V
Kontaktinformationen (Contact Info): Hiermit können Sie Ihre	O User Settings	to Language
Kontaktinformationen	Please enter your information below.	
hinzufügen/anzeigen/ändern. (Abb. 7.6)	Namo	
	Dobal3	
		Done Apply Cancel
	Abb. 7.6 – Kontaktinformationen (Ad	min aktiviert: Benutzeranmeldung)
Sprache (Language):	Settings - VP50	GIRONKEY .
Hiermit konnen Sie Ihre aktuelle	🕲 User Settings	
Sprachauswahl andern. ( <i>Abb. 7.7</i> )	Password Contact Inf	fo Language
	What is your preferred Languager	
	English	
		Done Apply Cancel

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





## VP50/VP50C-Einstellungen

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

Wie bereits auf Seite 12 erwähnt, führt die Initialisierung des VP50/VP50C ohne Aktivierung von Admin- und Benutzer-Passwörtern zu einer Konfiguration des Laufwerks mit der **Konfiguration Einzelnes Passwort und einzelner Benutzer**. <u>Diese Konfiguration bietet keinen Zugriff auf Admin-Optionen oder -Funktionen</u>. Mit dieser Konfiguration haben Sie Zugriff auf die folgenden VP50/VP50C-Einstellungen:

#### Ändern und Speichern von Einstellungen

	Settings - VP50		GIRONKEY .
Wenn Einstellungen in den	Admin Settings		
<ul> <li>Wenn Einstellungen in den VP50/VP50C-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)</li> </ul>	Password Who16 Franc	Please enter your password	inst Options
	Abb. 7.11 – Bildschirm n	Done Ap nit Passwortabfrage zum Speich Einstellungsänderungen	nern von VP50/VP50C-

**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/VP50C Einstellungen (Settings)" wird wieder angezeigt.





#### 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:







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

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

Einmaliges Wiederherstellungs-Passwort	Settings - VP50 GIRONKEY · ·
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)	One-Time Recovery Password       Agenty       Cancel         One-Time Recovery Password       One       Apply       Cancel
2 Schritt: Erstellen Sie ein einmeliger	Settings - VP50 GIRONKEY ~
Wiederherstellungs-Passwort mit denselben	Cone-Time Recovery Password
Passwortkriterien, mit denen der Stick	Please create a secure Complex password following the criteria below.
ursprünglich eingerichtet wurde (Komplex oder Passnbrase)	(Aamin Password
	Hecovery Hassword
Hinweis: Das Admin-Passwort ist erforderlich,	5-16 long
um die Anderungen zu übernehmen.	uppercase lowercase digit special character
	Back Save Cancel
	Abb. 8.5 - Einrichten des einmaligen Wiederherstellungs-Dassworts





Einmaliges Wiederherstellungs-Passwort verwenden

GIRONKEY' V Login Device - VP50 1. Schritt: Nachdem das einmalige B User Password . Wiederherstellungs-Passwort erstellt wurde, erscheint bei der nächsten Anmeldung eine neue Schaltfläche auf dem Anmeldebildschirm Benutzer-Pa Passwort (User Password). Klicken Sie auf die O Hint Schaltfläche Wiederherstellungs-Passwort (Recovery Password), um den Vorgang zu starten. Contact Infor Recovery Password Read-Only Mode Cancel Abb. 8.6 - Schaltfläche "Wiederherstellungs-Passwort" 2. Schritt: Der Bildschirm Wiederherstellungs-GIRONKEY . Login Device - VP50 Passwort (Recovery Password) wird angezeigt, auf A Recovery Password 0 0 dem Sie das Wiederherstellungs-Passwort eingeben und ein neues Benutzer-Passwort erstellen können. Please create a secure password following the criteria bei (Abb. 8.7) Wichtig: Das "Einmalige Wiederherstellungs-6-16 long Passwort" verwendet ebenfalls eine integrierte uppercase lowercase digit special character Sicherheitsfunktion, die die Anzahl der fehlgeschlagenen Anmeldeversuche verfolgt. Nach 10 fehlgeschlagenen, falschen Anmeldeversuchen mit dem einmaligen Wiederherstellungs-Passwort Cancel wird das Passwort deaktiviert, und muss erneut aktiviert werden, indem Sie sich im Stick als Abb. 8.7 – Menü "Wiederherstellungs-Passwort" Administrator anmelden (siehe Seiten 18 und 30 für weitere Einzelheiten). GIRONKEY . Login Device - VP50 User Password 3. Schritt: Bei Erfolg werden Sie zum Bildschirm Benutzer-Passwort (User Password) zurückgeleitet. Die Schaltfläche Wiederherstellungs-Passwort (Recovery Password) ist nun nicht mehr O Hint vorhanden, und das in Schritt 2 eingegebene Benutzer-Passwort wird zum neuen Benutzer-Contact Information Login as Admin Passwort. (Abb. 8.8) 🔲 Read-Only Mode 🕠 Cancel Abb. 8.8 – Anmeldebildschirm für Benutzer-Passwort mit der Schaltfläche Wiederherstellungs-Passwort verschwindet nach erfolgreicher Verwendung.





#### 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 die Dateien auf dem USB-Stick nur gelesen werden soll.

Um den Schreibschutz für die	Settings - VP50	GIRONKEY .
Benutzerdaten zu erzwingen, klicken Sie auf das Kästchen und dann auf Übernehmen (Apply)" <b>(Abb. 8 9)</b>	Admin Settings     Password Contact Info Language	🛞   📰
<b>Hinweis:</b> 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.	Please enter a new User Password below. Ptisword Contirm Pleasword 6-16 long uppercase lowercase digit special character One-Time Recovery Password Force Read-Only User Data C Login Password Reset C Done App Abb. 8.9 – Aktivieren von "Schreibgeschützte Benut (Admin-Passwort ist erforderlich, um die Änderunge	Ay Cancel Ezerdaten erzwingen" gen zu übernehmen.)
<ul> <li>Nach der Aktivierung wird die Schaltfläche "Schreibschutz-Modus</li> </ul>	Login Device - VP50	
(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)	Password     O Hint     Contact Information Login as Admin	
	Abb. 8.10 – Der Schreibschutz-Modus ist für den Be aktiviert und kann nur vom Administrator dea	enutzer zwangsweise ktiviert werden





#### Gerätesperrung

Der VP50/VP50C 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.







#### 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 <u>die Daten formatiert werden und alle Daten auf dem Stick unwiederbringlich verloren gehen</u>. Handlungsweisen, die auch auf <u>Seite 18</u> 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:



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/VP50C 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/VP50C gespeicherten Informationen gelöscht.





#### 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 <u>nicht</u> aktiviert ist), wenn der VP50/VP50C Launcher ausgeführt wird. (Siehe *Abb. 9.7* und **9.8**)

<ul> <li>Mit dieser Option können Sie ein neues Passwort erstellen, jedoch wird der VP50/VP50C zum Schutz Ihrer Daten neu formatiert. Das bedeutet, dass alle Ihre Daten in diesem Prozess unwiederbringlich gelöscht werden.*</li> </ul>	Login Device - VP50	
	Admin Password	©   =
	Pataments O Hint Reset Device	
	Read-Only Mode 🕤	Lager Cancel
	Abb. 9.7 – Admin-Passwort: Schaltfläche "Gerät zu	urücksetzen (Reset Device)"
Hinweis: Wenn Sie auf "Gerät	Login Device - VP50	GIRONKEY .
zurücksetzen (Reset Device)" klicken, erscheint eine Meldung, die fragt, ob Sie	User Password.	80   H
ein neues Passwort eingeben möchten, bevor die Formatierung durchgeführt wird. Sie haben jetzt die Wahl 1) dies durch Klicken auf " <i>OK</i> " zu bestätigen oder 2) durch Klicken auf "Abbrechen (Cancel)" abzubrechen und zum	Comment index maillion   Finner Download	_
Anmeldefenster zurückzukehren. (Siehe	C Read-Only Mode 0	
Abb. 9.8)		Liter Canciol
	Abb. 9.8 – Benutzer-Passwort (Admin/Benutz zurücksetzen	er nicht aktiviert) Gerät
• Wenn Sie sich entscheiden, fortzufahren,	Login Device - VP50	GIRONKEY .
werden Sie zum Bildschirm "Initialisieren	Admin Password	@   =
(Initialize)" weitergeleitet, wo Sie	Reset Device	
"Admin- und Benutzer-Modus (Admin		
and User modes) aktivieren und ihr	In order to protect data privacy, your VP50 will be formatted and all data will be erased. Do you want to even posswerd and format your drive now?	enter
nachdem welche Passwortontion Sie	O Hin	
gewählt haben (Kompley oder	Resi OK Cancel	
Passphrase). Der Hinweis ist kein		
Pflichtfeld, kann jedoch eine nützliche	C Read Carls Marte	
Hilfestellung zur Erinnerung an das		
Passwort sein, falls Sie es vergessen	Back	Cancel
haben sollten.	Abb. 9.9 – Bestätigung "Gerät zurücksetz	en (Reset Device)"





#### Laufwerksbuchstaben-Konflikt: Windows-Betriebssysteme

- Wie bereits im Abschnitt Systemanforderungen", Seite 3 in dieser Anleitung erwähnt, benötigt der VP50/VP50C 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/VP50C • 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/VP50C 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/VP50C 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/VP50C versuchen, ihn als zweiten Laufwerksbuchstaben zu verwenden und dadurch einen Konflikt verursachen.

Wenn es in Ihrem System keine Netzwerkfreigaben gibt und der VP50/VP50C 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.





#### Fehlermeldungen

Datei kann nicht erstellt werden (Unable to Create File): Diese Fehlermeldung wird angezeigt, wenn Sie im schreibgeschützten Modus angemeldet sind und versuchen, eine Datei oder einen Ordner IN einer sicheren Datenpartition zu ERSTELLEN.	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. OK Abb. 9.11 – Fehlermeldung "Datei kann nicht erstellt werden"
Fehler beim Kopieren einer Datei oder eines Ordners (Error copying file or folder): 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.	Error Copying File or Folder Cannot copy File1: The disk is write-protected. Remove the write-protection or use another disk. OK Abb. 9.12. – Fehlermeldung "Datei oder Ordner kopieren nicht möglich"
Fehler beim Löschen einer Datei oder eines Ordners (Error deleting file or Folder): Diese Fehlermeldung erscheint, wenn Sie versuchen, eine Datei oder einen Ordner VON der sicheren Datenpartition zu LÖSCHEN, während Sie im Schreibschutz-Modus angemeldet sind.	Error Deleting File or Folder       Image: Cannot delete File1: The disk is write-protected.         Remove the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use another disk.         Image: Comparison of the write-protection or use a

**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/VP50C vom Betriebssystem sicher entfernt und erneut angemeldet werden, wobei das Kontrollkästchen "Schreibschutz-Modus (Read-Only Mode)" nicht markiert sein darf.



## IRONKEY<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) CLÉ USB CHIFFRÉE 3.2 Gen 1

Guide de l'utilisateur







#### Sommaire

Introduction	
Fonctionnalités de la Vault Privacy 50	4
À propos de ce manuel	4
Configuration système	4
Recommandations	5
Utiliser le bon système de fichiers	5
Rappels concernant l'utilisation	5
Meilleures pratiques pour la configuration des mots de passe	6
Configurer ma clé USB	7
Accès à la clé USB (environnement Windows)	7
Accès à la clé USB (environnement macOS)	7
Initialisation de la clé USB (environnements Windows & macOS)	
Sélection du mot de passe	9
Clavier virtuel	
Icône de visibilité du mot de passe	
Mots de passe Admin et Utilisateur	
Informations de contact	
Utilisation de la clé USB (environnements Windows & macOS)	
Connexion pour l'Administrateur et l'Utilisateur (Admin activé)	
Connexion pour le mode Utilisateur uniquement (Admin non activé)	
Déverrouillage en Mode lecture seule	
Protection contre les attaques par force brute	
Accès à mes fichiers sécurisés	
Options de la clé USB	19
Paramètres de la VP50/VP50C	
Paramètres Admin	
Paramètres utilisateur : Admin activé	22
Paramètres utilisateur : Admin non activé	
Modifier et sauvegarder les paramètres de la VP50/VP50C	
Fonctionnalités Admin	
Réinitialisation du mot de passe Utilisateur	25
Réinitialisation du mot de passe de connexion (pour le mot de passe Utilisateur)	
Mot de passe de récupération à usage unique	
Forcer la lecture seule pour les données Utilisateur	
Aide et dépannage	
Verrouillage de la VP50/VP50C	
Réinitialisation de la VP50/VP50C	
Conflit de lettres de lecteur (systèmes d'exploitation Windows)	
Messages d'erreur	









Figure 1 : IronKey VP50

Figure 2 : IronKey VP50C

## Introduction

La Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C 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/VP50C est supérieure aux solutions connectées à Internet, tel que les services cloud, pour la sauvegarde des données.

La VP50/VP50C 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 » (a 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 Brute Force verrouille le mot de passe utilisateur ou le mot de passe de récupération à usage unique après 10 mots de passe invalides saisis d'affilée et efface le lecteur de manière chiffrée si le mot de passe administrateur est mal saisi 10 fois consécutives.

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

Certifiées FIPS 197 et conformes TAA, les clés USB de la série VP50/VP50C peuvent être personnalisées et configurées avec un identifiant produit (PID), via le programme de personnalisation de Kingston. Cela permet une intégration plus facile avec des logiciels de gestion de terminaux afin de répondre aux besoins informatiques d'entreprise 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/VP50C bénéficie d'une garantie limitée de 5 ans avec le support technique gratuit de Kingston.





#### Fonctionnalités de l'IronKey Vault Privacy 50/50C

- 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 50/50C (VP50/VP50C). Il est basé sur la version en sortie d'usine, sans personnalisation.

#### Système requis

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





## **Recommandations**

Pour que la VP50/VP50C 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/VP50C 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*.



#### Utiliser le bon système de fichiers

La IronKey VP50/VP50C 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/VP50C 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.

# GIRONKEY"



#### Meilleures pratiques pour la configuration des mots de passe

Votre VP50/VP50C 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 le nombre de tentative de saisie mot de passe à 10 essais. Lorsque cette limite est atteinte, la VP50/VP50C efface automatiquement les données chiffrées et s'auto-formate aux paramètres d'usine.

#### Mots de passe multiples

La VP50/VP50C 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/VP50C 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/VP50C 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/VP50C peut être réinitialisée et réutilisée, mais les données antérieures seront définitivement supprimées.

#### Modes de mot de passe

La VP50/VP50C prend en charge deux modes de mot de passe :

#### Complexe

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

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

#### Phrase de passe

La VP50/VP50C 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/VP50C, 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.



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

Insérez la VP50/VP50C 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.			88 \$	
•	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.	IRONKEY		IRONKEY.exe	Windows
			Figure 3.3 – Volu	ime IKVP	





## Initialisation de la clé USB (environnements Windows & macOS)

## Langue et Contrat de licence utilisateur final

	Dévice Initialization - VP50 GIRONKEY -		
menu déroulant, puis cliquez sur <b>Suivant (Next)</b> . (Voir l'illustration 4,1)	Kynat is your preferred Langunge?		
	Figure 4.1 – Sélection de la langue		
Lisez le contrat de licence et cliquez sur <b>Suivant</b> (Next). Remarque : Vous devez accepter le contrat de licence pour continuer. Autrement, le bouton <b>Suivant (Next)</b> restera désactivé. (Figure 4.2)	Constraint and the second		
	Figure 4.2 – Contrat de licence		





## Initialisation de la clé USB

#### Sélection du mot de passe

Sur la nouvelle fenêtre Mot de passe (Password), vous pourrez créer un mot de passe pour protéger vos données sur la VP50/VP50C en utilisant les modes Complexe (Complex) ou Phrase de passe (Passphrase) (Figures 4.3- 4.4). De plus, 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	Device Initialization - VP50	GIRONKEY .		
• Doit contenir entre 6 et 16 caractères.	A Password	0 =		
<ul> <li>Doit contenir <u>au moins</u> trois (3) des types de caractères suivants         <ul> <li>Majuscule</li> <li>Minuscule</li> <li>Chiffre</li> <li>Caractères spéciaux (!,\$,&amp;, etc)</li> </ul> </li> </ul>	Complex       Passphrase         Please create a secure Complex password following the criteri         Please create a secure Complex password following the criteri         Confilm Password         G-16 long         uppercase       digit         special characte         Pleaseword Hint?         Enable Admin and User Passwords         Back	a below.		
	Figure 4.3 – Mot de passe complexe			
Phrase de passe	Device Initialization - VP50	GIRONKEY .		
Doit contenir :	A Password	0) e		
<ul> <li>10 caractères minimum</li> </ul>	Complex Passphrase			
<ul> <li>64 caractères maximum</li> </ul>	Please create a secure Pessphrase password following the crite Please relate a secure Pessphrase password following the crite Control Plateword Control Plateword	res. bestow.		
Indice de mot de passe (facultatif)				
Un indice de mot de passe (Password Hint)				
peut être utile pour fournir une indication de	Password Hint?			
ce qu'est le mot de passe, si jamais vous l'oubliez.	Figure 4.5 – Champ Indice de mo	t de passe		
<b>Remarque</b> : L'indice NE DOIT PAS être le mot de passe lui-même.				





## 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)

		Barrier	- 1
Password	©   🖬 📫	Password	•
Complex Passphrase		Complex Passphrase	
Please create a secure Complex password following the criteria below.	0	Please create a secure Complex password following the criteria below.	0
ExamplePassw0rdt		ExamplePassw0rd	
ExamplePassw0Rd		ExamplePasswOrd	
√ 5-45 tong		~ 6-16 long	-
✓ uppercèse → lowercase → digit → special charactèr	_	≪uppercase ≪lowercase ≪digit special character	
Password Hint?		Password (lint?	5
🗍 Enable Admin and User Passwords 👔	0	Enable Admin and User Passwords 🚯	
Back Next	Cancel	Back	Cancel
Back Next	Cancel	Back Next	Cancel

	Device Initialization - VP50 GIRONKEY' ×
	A Password
Pour les mots de passe <b>non valides (Invalid)</b> , les cases de critères de mot de passe s'affichent en <b>rouge (red)</b> et le bouton <b>Suivant (Next)</b> est désactivé jusqu'à ce que les conditions minimales soient remplies.	Complex     Passphrase       Please create a secure Complex password following the criteria below     Image: Complex password following the criteria below       ExamplePassword       ExamplePassword       ExamplePassword       V Shift long       V special character
Cela s'applique à la fois aux mots de passe complexes et aux phrases de passe.	Passwords Hint 3 Enable Admin and User Passwords  Back Next Cancel Figure 4.7 – Condition de mot de passe non remplies





## Initialisation de la clé USB

#### **Clavier virtuel**

-

La VP50/VP50C est dotée d'un clavier virtuel qui peut être utilisé pour se protéger contre les enregistreurs de frappe.

	Device Initialization - VP50 GIRONKEY V
• Pour utiliser le <b>clavier virtuel</b> , localisez le bouton	A Password
du clavier dans la partie supérieure droite de	Complex Passphrase
l'écran Initialisation de la clé USB (Device	Flease create a secure Passphrase password following the criteria below.
Initialization – $VP50/VP50C$ ) et sélectionnez-le	This is my Passw0rd Example!
	This is my Password Example!
	≥ 10 chapacters intrinsim
	Pasoworthiol?
	Enable Admin and User Passwords
	Back Next Cancel
	Figure 4.8 – Activation du clavier virtuel
<ul> <li>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.</li> <li>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.</li> </ul>	Virtual Keyboard       Image: Constraint of the second spect Protocol of the second spect Protocol of the spectrum of




#### 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.

		Device Initialia	zation - VP50	GIRONKEY
		A Password	d	
Pour <b>masquer</b> le mo	t de passe, cliquez sur l'icône		Complex Passphrase	
grise.			Please create a secure Passphrase password following the cri	teria below. 🕜
	$\odot$		This is my Passw0Rd Eample!	
			This is my PasswORd Eample	
			✓ 10 cruiracters minimum	
			Password Hint?	
		C Enable Adm	nin and User Passwords 👔	
			Back	Next Cancel
		Figur	e 4.10 – Icône pour « masquer » le	mot de passe
		Device Initiali	zation - VP50	GIRONKEY
		A Passwor	d	
Dour <b>offiche</b> r lo mot	de passe masqué eliquez sur		Complex Passphrase	/
	de passe masque, cliquez sur		Please create a secure Passphrase password following the	riterla below. 🕜
l'icone bieue.				
			✓ 10 characters minimum	
			Paramord Hint?	
		C Enable Adm	nin and User Passwords 🧿	
			Back	Next Cancel
		Figur	re 4.11 – Icône pour « afficher » le i	mot de passe





#### 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 <u>activée</u>, 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 <b>mots de passe Admin et</b>
	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.

Password				1
	Complex	Passphrase		
F	Please create a secure Passphra	ise password following the c	riteria below. 🕤	
(	*****			
(	*****			
1	10 characters minimum			
	Password Mint?			
1				
Enable Admin a	Ind User Passwords 🕕			
		Back	Next	Cancel

#### 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.





#### Mots de passe Admin et Utilisateur

 Si le rôle Admin a été activé à l'écran précédent, l'écran suivant demandera le <u>mot de passe Utilisateur</u> (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)

Device Initia	alization - VP50	GIRONKEY
🔒 User P	assword	0   8
	Please create a secure Passphrase password following the criteria b	ejow. 🕜
	Pessword	
	Confirm Password	
	10 characters minimum	
	Transcored (1981)	
	Pesswana mina	
🔵 Require p	assword reset on next login 🕕	
	Rack	Cancal
	USACK NEW	Cancer

**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	Login Device - VP50	
	<ul> <li>password reset on next login) située</li> <li>dans le coin inférieur gauche de la Figure</li> <li>4.13 ne concerne que le mot de passe</li> </ul>	User Password     Require password reset	
	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 met	The Admin has required that you reset your password; please proceed to create a new password. O Hin Contact Read-Only Mode	
	de passe temporaire. Cette		ogin Cancel
	fonctionnalité est utile lorsque la clé USB est confiée à une autre personne pour qu'elle l'utilise. ( <b>Figure 4.14)</b>	Figure 4.14 – Exiger la réinitialisation du mot de p connexion (pour le mot de passe Utilisateu	passe à la prochaine
	<b>Remarque :</b> Pour des raisons de sécurité, le nouveau mot de passe ne peut pas être identique au mot de passe temporaire.		- ,





#### 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.)

	Device Initialization - VP50	GIRONKEY
Le champ <b>« Nom » (Name)</b> peut contenir jusqu'à 32 caractères, mais ne doit pas contenir le mot de passe <b>exact</b> .	Contact	
Le champ <b>« Société » (Company)</b> peut contenir jusqu'à 32 caractères, mais ne doit pas contenir le mot de passe <b>exact</b> .	Diventi.	
Le champ « <b>Détails » (Details)</b> peut contenir jusqu'à 156 caractères, mais ne doit pas contenir le mot de passe <b>exact</b> .	Figure 4.14 – Informations de co	OK Cancel

**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/VP50C 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)

Login Device - VP50	RONKEY ~ Login Device	- VP50	GIRONKEY
A User Password	🛞 🗐 🔒 Admin F	Password	<ul> <li>Image: Second sec</li></ul>
Contact Information Login as Admin		C Hint Reset Device	
Read-Only Mode	Read-Only	Mode 🕤	
Login	Cancel	B	lack Login Cancel
Figure 5.1 – Connexion à l'aide du Mot de passe (Admin activé)	Utilisateur Figure	e 5.2 – Connexion à l'aide	e du Mot de passe Admin
Connexion pour le mode Utilisateur	Login Devic	ce - VP50	GIRONKEY Y
iniquement (Admin non activé)	🔒 User P	assword	&   ==
Comme indiqué précédemment à la <b>page 13</b> , 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		Pessiveerd O Hint Contact Information Reset Device	
lestinée aux personnes qui souhaitent ur	ne approche	ly Mode 🕕	
imple, avec un seul mot de passe, pour s eurs données sur leur clé USB. (Figure 5.3	écuriser 3)		Login Cancel
Remarque : Pour activer les mots de pass Jtilisateur, utilisez le bouton Réinitialiser Reset Device) pour remettre la clé USB à d'initialisation, où vous pouvez activer les passe Admin et Utilisateur. La réinitialisa clé USB entraîne un formatage de la clé d	Figure 9 Fia clé USB I l'état 5 mots de tion de la et la perte	5.3 – Connexion à l'aide c (Admin non	du mot de passe Utilisateur activé)





#### 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 :

		Login Device - VP50	GIRONKEY" -
1.	Insérez la clé USB dans le port USB de l'ordinateur hôte et exécutez le fichier IronKey.exe.	🔒 User Password	&   III
2.	Cochez la case <b>Mode lecture seule</b> (Read-Only Mode) sous la zone de saisie du mot de passe. (Figure 5.4)	Contact Information Reset Device:	
3.	Saisissez le mot de passe de votre clé USB et cliquez sur <b>Connexion (Login)</b> . La clé USB IronKey est désormais déverrouillée en Mode lecture seule.	Read-Only Mode Figure 5.4 – Mode lecture set	Login Cancel

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/VP50C et vous reconnecter, en laissant la case « Mode lecture seule » (Read-Only Mode) décochée.

**Remarque :** Les options Admin de la VP50/VP50C 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).





#### 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 <u>10 saisies de mot de passe erroné</u>, 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	ουι
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 <u>NON</u> 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	ουι

\* 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/VP50C.** (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.



# **Options de la clé USB (environnement macOS)**

<ul> <li>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.</li> <li>Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.</li> </ul>	Image: Construction of the second state of the second s
	clé USB





# **Options de la clé USB**

Paramètres de la VP50 (VP50 Settings) :	<ul> <li>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/VP50C » du présent manuel).</li> </ul>
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) Remarque : L'authentification par mot de passe sera requise pour le formatage.	Login Device - VP50 Contact Verso Contact Contact Verso Contact Verso Contact C
Support en ligne (Online Support) :	Figure 6.1 – Formater la VP50/VP50C         • Cette fonction ouvre votre navigateur Internet et affiche la page <a href="http://www.kingston.com/support">http://www.kingston.com/support</a> pour vous permettre de consulter les informations supplémentaires du support.
	About - VP50 GIRONKEY · ·
A propos de la VP50 (About VP50/VP50C) : Afficher des données détaillées sur la VP50/VP50C, notamment des informations sur l'application, le firmware et le numéro de série. (Figure 6.2)	About     2022 Kingston Technology Corporation.
<b>Remarque :</b> Le numéro de série unique de la clé USB se trouve sous la colonne « Informations ».	Modules         Version         Information           IKVP50         IKVP50         002324853023863190000062           Application         1.0.0.0           PW Version         01.06610           Crypto Library FW         1.00
	Ciose Figure 6.2 – À propos de la VP50/VP50C
Arrêter la VP50 (Shut down VP50) :	<ul> <li>Permet de fermer correctement la VP50/VP50C avant de la déconnecter physiquement du système, en toute sécurité.</li> </ul>





# Paramètres de la VP50/VP50C

#### 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
  - o Réinitialisation du mot de passe de connexion (pour le mot de passe Utilisateur)
  - o Activer un mot de passe de récupération à usage unique
  - o Forcer le mode lecture seule pour les données Utilisateur

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

Settings - VP50 GIRONKEY	<ul> <li>Settings - VP50</li> </ul>	GIRONKEY .
Admin Settings     (	Admin Settings	@   =
Password Context linfo Language: Admin Options Current Password Please create a secure Complex password following the criteria balow: New Password Contiern Navy Password 6-16 long uppercase lowercase digs special character Placeword Hint? Done Apply Cancel	Control Plasword     Control Mo.     Language     Current Plasword     New Password     Continue New Password     Con	Admin Optons
Figure 7.1 – Options de mot de passe	Figure 7.2 – Informations	de contact
Admin Settings	Admin Settings	@]=
Passward Contact Into Language Admin Options	Piessword Contact Info Language	Acmin Co
English	Confirm PAssword Confirm PAssword 5-16 long uppercase lowercase stight special of One-Time Recovery Password	haractor
Done Airika Canrel	Force Read-Only User Data     Control Login Password Reset	
Figure 7.3 – Options de langue	Figure 7.4 – Options	Admin





# Paramètres de la VP50/VP50C

#### Paramètres utilisateur : Admin activé

La connexion Utilisateur limite l'accès aux paramètres suivants :



**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/VP50C

#### Paramètres utilisateur : Admin non activé

Comme mentionné précédemment à la page 13, l'initialisation de la VP50/VP50C sans activer les mots de passe « Admin et Utilisateur » configurera la clé USB dans une **configuration Mot de passe unique, Utilisateur unique**. <u>Cette configuration n'a pas accès aux options ou fonctionnalités Admin.</u> Cette configuration aura accès aux paramètres suivants de la VP50/VP50C :

#### Modifier et sauvegarder les paramètres

	Settings - VP50	GIRONKEY .
<ul> <li>Chaque fois que les paramètres sont modifiés dans les Paramètres de la VP50/VP50C (par exemple : coordonnées, langue, modification</li> </ul>	Admin Settings     Password     Press enter your password     What i     Error	j intin Options
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)	Figure 7.11 – Écran d'invite du mot de passe por modifications des paramètres de la VPS	pply Cancel ur sauvegarder les 50/VP50C

**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/VP50C.





#### 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 :







### 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	Settings - VP50 GIRONKEY .
<b>Étape 1</b> : 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. <b>(Figure 8.4)</b>	Image: Settings       Image: Settings         Password       Language         Please enter a new User Password below.       Password         Image: Setting and the password Reset (Image: Seting and the password Reset (Image: Seting and the passe de récupération à usage unique)
<b>Étape 2</b> : 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). <b>Remarque</b> : Le mot de passe Admin sera nécessaire pour appliquer les modifications.	Settings - VP50 Certain Complex password Collowing the criteria below.
	Figure 8.5 – Configuration du mot de passe de récupération à usage unique





Utilisation du mot de passe de récupération à usage unique

Étape 1 : Après la création du mot de passe de	Login Device - VP50	GIRONKEY .
récupération à usage unique, un nouveau bouton	A User Password	-@ =
<b>Utilisateur (User Password)</b> lors de la prochaine connexion. Cliquez sur le bouton <b>Mot de passe de récupération (Recovery Password)</b> pour lancer le processus.	Presented  Hint  Contact Information  Recovery Password  Login as  Read-Only Mode	Admin Logn Cancel
	Figure 8.6 – Bouton Mot de passe de	e récupération
Étape 2 : L'écran Mot de passe de récupération (Recovery Password) s'affiche et yous permet	Login Device - VP50	GIRONKEY .
d'entrer le mot de passe de récupération et de	Recovery Password	0
créer un nouveau mot de passe Utilisateur.	Recovery Passworn	
(Figure 8.7)	Please create a secure password following the criteria below.	
	Confirm New User Password	
Important : Le mot de passe de recuperation a	6-16 long	
fonctionnalité de sécurité intégrée qui	uppercase lowercase digit special charac	ter
comptabilise le nombre de tentatives de	Password Hint2	
connexion ratées. Après 10 saisies incorrectes du		
mot de passe de récupération à usage unique, ce		Next Cancel
dernier sera désactive et devra être réactive en se connectant à la clé USB en tant qu'Admin. (voir les pages 18 et 30 pour plus de détails)	Figure 8.7 – Menu Mot de passe de	récupération
	Login Device - VP50	GIRONKEY -
Étape 3 : En cas de succès, vous serez ramené à l'écran Mot de passe Utilisateur (User Besuverd) : la boutan Mot de passe de	User Password	@  @
récupération (Recovery Password) est	Presword	
maintenant absent, et le mot de passe Utilisateur	O Hint	
saisi à l' <b>étape 2</b> deviendra le nouveau mot de	Constant Information	
passe Utilisateur. (Figure 8.8)	Login is Admin	
	Read-Only Mode 0	
		Largin Cancel
	Figure 8.8 – Écran de connexion du mot de passe le bouton Mot de passe de récupération dis correctement.	e Utilisateur montrant que sparaît une fois utilisé





#### 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.

<ul> <li>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)</li> <li>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.</li> </ul>	Settings - VP50       IRONKEY         Ø Admin Settings       Impunger         Password       Contact Into         Password       Impunger         Password       Impunger         Password       Impunger         Password       Impunger         Impunger       Impunger <t< th=""></t<>
<ul> <li>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)</li> </ul>	Login Device - VP50       Provice 'Picon Ker'         User Password       Image: Contract Information         Image: Picon Ker'       <





#### Verrouillage de la clé USB

LA VP50/VP50C 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.

	Login Device - VP50	GIRONKEY -
<ul> <li>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)</li> </ul>	User Password  PASSWORD IS INCORRECT  PARSWORD IS INCORRECT  PARSWORD  INT  Contact Information Reset Device  Read-Only Mode	
<ul> <li>Après la 7<sup>ème</sup> 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)</li> </ul>	Login Device - VP50         Admin Password         Pessword         Back         Back	e mot de passe ratée





#### Verrouillage de la clé USB

**Important :** Après la **10**<sup>ème</sup> 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 <u>formatera les données, lesquelles seront définitivement perdues</u>. 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 10<sup>ème</sup> et dernière tentative de connexion ratée pour chaque méthode de mot de passe de connexion :

Login Device - VP50	GIRONKEY ×	l'Admin/Utilisateur)	<u> </u>
🔒 User Password	<b>(6)</b>	Login Device - VP50	GIRONKEY
• Warning!		Admin Password	©
Univer reached the maximum retries. In order to protect data p UCKED. To recover your data, is Ope-Time Recovery password (if Contact)	number of password srivacy, your VP50 is now og in as Admin or use the	You have reached the maximum retries. In order to protect data id data was your drive again when the of Hin       Pisa	ni number of password privacy, your VP50 is now ib elost, You with the able to operation completes.
🖸 Read-Only Mode 👔			
	Login Candel	C Read-Only Mode	
NEDDOLINI A OF		0	Back Legin Cancel
(Figure	e 9.3)	FORMATAGE I	DE LA CLÉ USB*
de passe de récupération	on à usage unique : (activé	(Figur Mot de passe utilisate	<sup>.</sup> e 9.4) ur (Admin NON activ
de passe de récupératio par l'Admin/	on à usage unique : (activé 'Utilisateur)	(Figur Mot de passe utilisate	e 9.4) ur (Admin NON activ ⊖ıronkey
de passe de récupératio par l'Admin/	on à usage unique : (activé <u>'Utilisateur)</u> GIRONKEY: ~	(Figur Mot de passe utilisate	re 9.4) ur (Admin NON activ GIRONKEY
de passe de récupération par l'Admin/ Login Device - VP50 Recovery Password	on à usage unique : (activé <u>'Utilisateur)</u> @IRONKEY: ~ @I	(Figur Mot de passe utilisate	re 9.4) ur (Admin NON activ ⊝ıronkey ©
de passe de récupération par l'Admin/ Login Device - VP50 Recovery Password Pass Vu have reached the maximum r password retries. In order to protect data parivacy, y un device a Admin.	On à usage unique : (activé (Utilisateur) C IRONKEY:	(Figur Mot de passe utilisate Login Device - VP50 User Password Warning Wurning Wurning Wurning Contact:	re 9.4) ur (Admin NON activ in runber of passoon privacy your VP50 to now poperation completes.
de passe de récupération par l'Admin/ Login Device - VP50 Recovery Password Recovery Password Vue have reached the maximum r password reflex. How have reached the maximum r password reflex. How have reached the maximum r password reflex.	On à usage unique : (activé (Utilisateur) (Utilisateur) (IRONKEY: ) (IRONKEY: )	(Figur Mot de passe utilisate Login Device - VP50	re 9.4) ur (Admin NON activ in rumber of password privacy, your VP50 is now if be taxt You will be able to operation completes.
de passe de récupération par l'Admin/ Login Device - VP50 Recovery Password Pass Warning! Pass Vou have reached the maximum r down. To recover stored data and password. Login as Admin. Conter to protect data privacy. y down. To recover stored data and password. Login as Admin.	On à usage unique : (activé (Utilisateur) © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY © IRONKEY	(Figur Mot de passe utilisate	re 9.4) ur (Admin NON activ Provide the second of provide the second of provide the second of provide the second of provide the second of th
de passe de récupération par l'Admin/ Login Device - VP50 Recovery Password Vu have reached the maximum Vu have reached the maximum reached the maximum vu have reached the maximum vu have reached the maximum vu have reached the maximum reached th	On à usage unique : (activé (Utilisateur) INDINKEY INDINA INDINA INDINA INDINA INDINKEY INDINA INDINKEY INDINKEY	(Figur Mot de passe utilisate Login Device - VP50 User Password User Password Wurning User Password User Password Wurning Consect User Password Consect Con	re 9.4) ur (Admin NON activ © IRONKEY mrunber of password privacy, your V50 in each be lost. You will be able to operation completes. Cancel DE LA CLÉ USB*

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/VP50C 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/VP50C supprimera TOUTES les informations stockées sur sa partition de données sécurisée.





#### 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 <u>pas</u> activé) lorsque le programme VP50/VP50C Launcher est exécuté. (voir la *Figure 9.7* et la **Figure 9.8**)

Cette option vous permet de créer un	Login Device - VP50
nouveau mot de passe, mais pour proteger la	Admin Password
VP50/VP50C sera formatée. Par conséquent	
ce processus effecere définitivement toutes	
vos données *	Patamers
vos donnees.	O Hint
	Reset Device
	🗋 Read-Only Mode 🚯
	Back Lagun Cancel
	Figure 9.7 – Mot de passe Admin : Bouton de réinitialisation de la clé
Remargue : Lorsque vous cliquez sur le	Login Device - VP50
bouton « Réinitialiser le mot de passe » (Reset	User Password
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	Q Hot
confirmer, ou 2) cliquer sur « Annuler »	
(Cancel) pour revenir à la fenêtre de	Communical Independantion 1 Related Deretters
connexion. (Voir la Figure 9.8)	
	C Read-Only Mode 0
	Linor Cancel
	Figure 9.8 – Mot de passe Utilisateur (Admin/Utilisateur non activé) – Réinitialisation de la clé USB
• Si vous choisissez de continuer, vous serez	Login Device - VP50
renvoyé à l'écran d'initialisation, où vous	Admin Password
pouvez activer les « modes Admin et	Reset Device
Utilisateur » et saisir votre nouveau mot de	
passe en fonction de l'option de mot de passe	In order to protect data privacy, your VP50 will be formatted and all data will be erased. Do you want to enter
choisie (Complexe ou Phrase de passe).	a new password and format your drive now?
L'indice n'est pas obligatoire, mais il peut vous	
aider à vous souvenir du mot de passe si vous	Resi OX Cancel
l'oubliez.	
	C Read-Only Mode 👩
	Back Lingky Cancel
	Figure 9.9 – Confirmation de réinitialisation de la clé USB



# 🕞 IRONKEY"

# 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/VP50C 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/VP50C 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).





Dans cet exemple (Figure 9.10), la VP50/VP50C 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/VP50C 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/VP50C 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.





#### 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.	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. OK 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.	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.	Error Deleting File or Folder         Image: Cannot delete File1: The disk is write-protected.         Remove the write-protection or use another disk.         Image: OK         OK    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/VP50C, puis rétablir la connexion après avoir décoché la case « Mode lecture seule » (Read-Only mode).



# IRONKEY<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) DRIVE FLASH USB 3.2 Gen 1 CRITTOGRAFATO

*Guida per l'utente* 







#### Contenuti

Introduzione	
Funzionalità Vault Privacy 50	
Informazioni sul manuale	4
Requisiti di sistema	4
Raccomandazioni	5
Utilizzo del file system corretto	5
Note di utilizzo	5
Prassi raccomandate per l'impostazione della password	6
Configurazione del dispositivo	7
Accesso al dispositivo (ambienti Windows)	7
Accesso al dispositivo (ambienti macOS)	7
Utilizzo del dispositivo (ambienti Windows e macOS)	8
Selezione della password	9
Tastiera virtuale	
Pulsante di commutazione visualizzazione password	
Password amministratore e utente	
Schermata informazioni di contatto	
Utilizzo del dispositivo (ambienti Windows e macOS)	16
Accesso per amministratore e utente (Amministratore abilitato)	
Modalità di accesso per solo utente (Amministratore non abilitato)	
Sblocco in modalità di sola lettura	
Protezione contro gli attacchi brute-force	
Accesso ai file sicuri	
Opzioni dispositivo	19
Impostazioni unità VP50/VP50C	
Impostazioni amministratore	
Impostazioni utente:Amministratore abilitato	
Impostazioni utente:Amministratore non abilitato	
Modifica e salvataggio impostazioni VP50/VP50C	
Modalità amministratore	
Reset della password utente	
Reset della password di accesso (per password Utente)	
Password di ripristino monouso	
Forza la modalità di sola lettura per i dati utente	
Guida alla risoluzione dei problemi	
Blocco del drive VP50/VP50C	
Reset del dispositivo VP50/VP50C	
Conflitti con le lettere di unità (Sistemi operativi Windows)	
Messaggi di errore	



# Kingston





Figura 1: IronKey VP50

Figura 2: IronKey VP50C

## Introduzione

Il drive Kingston IronKey Vault Privacy (VP50)/Vault Privacy 50C (VP50C) 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/VP50C è anche conforme agli standard TAA ed è assemblata negli Stati Uniti. Dato che garantisce storage crittografato controllato fisicamente dall'utente, la gamma VP50/VP50C assicura funzionalità di salvaguardia dei dati superiori a quelle dei servizi Internet e cloud.

La gamma VP50/VP50C supporta opzioni multi password (amministratore, utente, password di ripristino monouso) con 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" i 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/VP50C 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'Amministratore 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/VP50C è coperto 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 e 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 50/50C (VP50/VP50C). Le istruzioni sono riferite all'unità in configurazione standard di fabbrica e pertanto priva di qualunque tipo di personalizzazione.

#### Requisiti di sistema

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





# Raccomandazioni

Per garantire una'alimentazione adeguata al funzionamento del drive VP50/VP50C, collegarlo direttamente a una porta USB sul computer notebook o desktop, come illustrato in *Figura 1.1*. Evitare di collegare il drive VP50/VP50C 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/VP50C 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/VP50C
- 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

#### Per maggiori informazioni e aggiornamenti

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 utilizzato 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.

# GIRONKEY"



Il drive VP50/VP50C 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/VP50C effettuerà la cancellazione automatica di tutti i dati crittografati per poi effettuare il ripristino delle impostazioni di fabbrica.

#### Supporto per password multiple

Il drive VP50/VP50C 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/VP50C 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/VP50C 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 forzato. Pertanto, Kingston raccomanda di salvare i dati anche su altri supporti. Il drive VP50/VP50C può essere sottoposto a un reset; ma in tal caso, tutti i dati in esso contenuti saranno eliminati definitivamente.

#### Modalità password

Il drive VP50/VP50C 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/VP50C 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/VP50C, 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 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)	Installing device driver software * * Click here for status. Figura 3.1- Notifica di rilevamento del driver del dispositivo
•	Una volta completato il rilevamento del nuovo hardware, selezionare l'opzione <b>IronKey.exe</b> , 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:).	DVD RW Drive (E:) IronKey Unlocker         0 bytes free of 122 MB         Common         IronKey.app         Licenses         WINDOWS         AUTORUN.INF         EironKey.exe

#### Accesso al dispositivo (ambienti macOS)

Inserire il drive VP50/VP50C 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/VP50C (o IRONKEY). (Figura 3.3)

•	Fare doppio clic sull'icona CD-ROM dell'unità IRONKEY.			88 \$	
•	Quindi, fare doppio clic sull'icona IKVP50/VP50C (o IronKey.app), visualizzata nella finestra raffigurata in Figura 3.3. Verrà avviata la procedura di inizializzazione.	IRONKEY		JRONKEY.exe	Windows
			Figure 3.3 - Icona di	volume IKVP	





# Inizializzazione del dispositivo (ambienti Windows e macOS)

# Lingua e Contratto di Licenza

	Device Initialization - VP50 GIRONKEY v
Selezionare la lingua preferita dal menu a discesa e fare clic su " <b>Avanti</b> " (Next). (Vedere Figura 4.1)	Language What is your preferred Language? Enginer
	Figura 4.1- Selezione della lingua
	Device Initialization - VP50 GIRONKEY ~
Leggere l'accordo di licenza e quindi fare clic su "Avanti" (Next). Nota: è necessario accettare l'accordo di licenza prima di proseguire; in caso contrario il pulsante "Avanti" (Next) resterà disabilitato. (Figura 4.2)	Concept Agreement     Software LICENSE AGREEMENT     Month of the Licensed Software accompany inc. ('Kingston'). This Agreement relates to the     software accompanying this Agreement, which includes computer software and may include associated media,     software accompanying this Agreement, which includes computer software and may include associated media,     software accompanying this Agreement, which includes computer software and may include associated media,     software accompanying this Agreement, which includes computer software and may include associated media,     software accompanying this Agreement, who and agree to be bound by the terms of this Agreement and further     approved the thre thid party licenscos of Kingston providing licenses for all or any portion of the Licensed Software is     but provide a solely for use with increased Software is     increased Software.     The Licensed Software is protected by copyright laws and international copyright treaties, as well as other     insue associated media.     The Licensed Software is protected by copyright laws and not all ternational copyright treaties, as well as other     insue associated property licenses of software Encensed, software is     but and ary tenesses.     The licensed Software is protected by copyright laws and not all ternational copyright treaties, as well as other     insue associated media.     Back
	Figura 4.2- Accordo di licenza





#### Selezione della password

Sulla schermata di selezione password, è possibile creare una password a protezione dei dati dell'unità VP50/VP50C. 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 la sezione dedicata alle Password Amministratore/Utente più avanti nel manuale, per familiarizzarsi 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:

Password complessa	Device Initialization - VP50 GIRONKEY ~
<ul> <li>Le password devono essere composte da un minimo di 6 fino a un massimo di 16 caratteri.</li> </ul>	Password     Omplex     Passphrase Please cruste a secure Complex password following the criteria below.     Please cruste a secure Complex password following the criteria below.
<ul> <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 (!,\$,&amp;, ecc)</li> </ul> </li> </ul>	Contrin Pessword 6 16 long uppercase lowercase digit special character Pessword Hm11 Back Next Cancel Figure 4.3 - Password complesse
Password frase	Perfectiveliaria visional association and a second completion
<ul> <li>Devono contenere:</li> <li>Minimo 10 caratteri</li> <li>Massimo 64 caratteri</li> </ul>	Password
Suggerimento password (opzionale) Un suggerimento password può rivelarsi utile per aiutare l'utente a ricordare la password, qualora questa vada persa o dimenticata. Nota: il suggerimento NON DEVE corrispondere alla stessa password utilizzata per l'accesso	Password Hint? Figura 4.5 - Campo suggerimento password





#### 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)

Device Initializ	ration - VP50 G	IRONKEY - Device Initial	ization - VP50	GIRON
Password	d	💿 💼 🔒 Passwor	rd	0
	Complex Passphrase		Complex Passphrase	
	Please create a secure Complex password following the criteria below.	6	Please create a secure Complex password followin	g the criteria below. 🕦
	ExamplePassw0rd	D C	ExamplePassw0rd	
	ExamplePassw0Rd		ExamplePasswOrd	
	- 6-16 long		~ 6-16 iong	
	≪uppercèse ∞lowercase ∞digit ∞ special character		≪uppercase ≪lowercase ≪digit s	pecial character
	Password Hint?		Password (lint?	
Enable Admi	in and User Passwords 😗	Enable Adr	nin and User Passwords	
igura P	4.6a - Requisiti di inserimen bassword complessa rispetta	to della Figura	a 4.6b - Requisiti condi della password cor	Next Cance izionali opziona nplessa
igura p	<b>4.6a - Requisiti di inserimen</b> bassword complessa rispetta	to della ati	a 4.6b - Requisiti condi della password con	Next Cance zionali opziona nplessa
igura p	4.6a - Requisiti di inserimen bassword complessa rispetta	Cancel Ito della Ati Device Ini Passo	a 4.6b - Requisiti condi della password con	Next Cance izionali opziona nplessa
igura p	4.6a - Requisiti di inserimen bassword complessa rispetta di inserimento di password Non v	ralide, i	Back a 4.6b - Requisiti condi della password con tialization - VP50 vord Complex Passphrase	Next Cance
igura p	4.6a - Requisiti di inserimen bassword complessa rispetta di inserimento di password Non v cociati ai criteri delle password, si	Cancel ati Figura Pevice Ini Passo valide, i	Back a 4.6b - Requisiti condit della password con talization - VP50 vord <u>Complex</u> Passphrase Please creates a secure Condete password following the	Next Cance
igura p caso c npi ass minera	4.6a - Requisiti di inserimen bassword complessa rispetta di inserimento di password Non v cociati ai criteri delle password, si anno di colore rosso e il pulsante	Cancel ati Figura Figura Valide, i "Avanti"	Back a 4.6b - Requisiti condi della password con talization - VP50 vord Complex Passphrase Please create a secure Complex password following the of ExamplePassword	Next Cance izionali opziona nplessa @IRONKEY' ~ @ =
<b>igura</b> p l caso c npi ass minera ext) res	4.6a - Requisiti di inserimen bassword complessa rispetta di inserimento di password Non v cociati ai criteri delle password, si anno di colore rosso e il pulsante cterà disabilitato fino a quando no	Cancel hto della ati Figura Figura Passa valide, i "Avanti" on vengono	Back a 4.6b - Requisiti condi della password con tialization - VP50 vord	Next Cance
igura p l caso c npi ass minera ext) res pettati	<b>4.6a - Requisiti di inserimen</b> <b>assword complessa rispetta</b> di inserimento di password <b>Non v</b> sociati ai criteri delle password, si anno di colore rosso e il pulsante sterà disabilitato fino a quando no i requisiti di inserimento corretti.	Cancel hto della ati Figura Passu valide, i "Avanti" on vengono	Back a 4.6b - Requisiti condi della password con tialization - VP50 vord  Complex Passphrase Please create a secure Complex password following the c ExamplePassword ExamplePassword v6.16 long	Next Cance
Figura p l caso c npi ass minera ext) res pettati	<b>4.6a - Requisiti di inserimen</b> <b>bassword complessa rispetta</b> di inserimento di password <b>Non v</b> cociati ai criteri delle password, si anno di colore rosso e il pulsante cterà disabilitato fino a quando no i requisiti di inserimento corretti.	Cancel ati Figura Figura Device In Passo	Back a 4.6b - Requisiti condi della password con tialization - VP50 vord Complex Passphrase Please create a secure Complex password following the of ExamplePassword Exa	Next Cance
Figura p l caso c mpi ass iminera ext) res pettati e cond	4.6a - Requisiti di inserimento bassword complessa rispetta di inserimento di password Non v cociati ai criteri delle password, si anno di colore rosso e il pulsante sterà disabilitato fino a quando no i requisiti di inserimento corretti.	Cancel ati Figura Figura Figura Passa Passa Passa povice in Passa Passa povice in Passa povice in Passa povice in Passa povice in Passa povice in Passa povice in Passa povice in Passa	Back a 4.6b - Requisiti condi della password cor tialization - VP50 word	Next Cance

Figura 4.7 - Condizioni di inserimento password non rispettate





#### Tastiera virtuale

Il drive VP50/VP50C è dotato di una tastiera virtuale che può essere utilizzata per la protezione contro attacchi keylogger.

		Device Initialization - VP50
•	Per utilizzare la tastiera virtuale, identificare il	A Password
	pulsante raffigurante la tastiera, sul lato superiore destro della schermata " <b>Inizializzazione</b> <b>dispositivo</b> " (Device Initialization) e quindi selezionare tale opzione.	Complex Passphrase Flease create a secure Passphrase password following the criteria below. This is my Password Example! This is my Password Example! This is my Password Example! This is my Password Example! Example: Back Next Cance!
		Figura 4.8 - Attivazione della tastiera virtuale
•	Una volta che viene visualizzata la tastiera virtuale, è anche possibile attivare la funzione di <b>Protezione contro gli screenlogger</b> . Tale funzionalità rende invisibili tutti i tasti. Questo utile in quanto impedisce agli screenlogger di registrare ciò che l'utente sta cliccando sulla tastiera.	Virtual Xeyboard 1 = 34567890 = = 3 q w e r t y u i o p [ ]  a s d f g h j k l ; ' return shift z x c v b n m , . / shift caps lock randomize 2
•	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





#### Pulsante per visualizzazione password

Per impostazione predefinita, alla creazione di una password, la questa sarà visibile nel campo di inserimento mentre viene digitata. Se si desidera nascondere la password mentre viene digitata, è possibile farlo utilizzando 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 conifgurato, il campo password sarà impostato automaticamente in modalità "nascosta".

	Device Initialization - VP50	GIRONKEY
	A Password	
Per <b>nascondere</b> la stringa contenente la password, fare clic sull'icona grigia.	Complex Passphrase Please create a secure Passphrase password following the cr This is my PasswORd Eample!	Iteria below 0
	This is my PasswORd Eample	
	Passwood Hint?	
	Enable Admin and User Passwords	
	Back	Next Cancel
	Figura 4.10 - Attivazione modalità "Nasco	ondi password"
	Device Initialization - VP50	GIRONKEY
	A Password	<b>a</b> =
Per mostrare la password pascosta, fare clic sull'icona	Complex Passphrase	
Fer <b>mostrare</b> la passiona nascosta, fare che sull'icona	Please create a secure Passphrase password following to	riterla below. 🕜
DIU.		
	🛹 10 characters minimum	
	Paraserovid Hand?	
	Enable Admin and User Passwords	
	Back	Next Cancel
	Figura 4.11 - Attivazione modalità "Mos	tra password"





#### 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 <u>abilitata</u>, 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.

	Device Initialization - VP50	BIRONKEY V
Per abilitare la funzione <b>"Password</b>	8 Password	<u>®</u> =
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)	Complex Passphrase Please create a secure Passphrase password following the criteria below encode en	
Quando questa funzionalità è <b>abilitata</b> , la password selezionata per questa schermata è quella <b>Amministratore</b> . Fare clic su <b>Successivo</b> (Next ) per procedere verso la schermata <b>"Password utente</b> ", dalla quale è possibile selezionare una password Utente.	Enable Admin and User Passwords      Back Next  Figura 4.12 - Abilitazione delle password amminist	Cancel

#### 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\_
 <u>Password utente</u> (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)

Device Initialization - VP50	GIRONKEY.
🔒 User Password	0 8
Please create a secure Pass	phrase password following the criteria below. 👔
Password	
Confirm Password	
10 characters minimum	
Password Hint?	
🗌 Require password reset on next login 👔	
	Back Next Cancel
gura 4.13 - Password Utent	e (Funzione "Amministratore e utente

**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 " <b>Richiedi il reset</b>	Login Device - VP50	GIRONKEY .
	password al prossimo accesso", posta	A User Password	<b>®</b>   <b>=</b>
	sul lato inferiore sinistro in <b>Figure 4.13</b> , e	Regulare password reset	
	limitata alla sola password Utente e può	Treden e brannerer e rener	-
	essere abilitata al fine di forzare l'utente		
	a effettuare l'accesso con una password	The Admin has required that you reset your password;	
	temporanea impostata	O Hin	
	dall'amministratore durante la fase di		
	inizializzazione. Tale password dovrà poi	Contact . OK	
	essere modificata con una password		
	selezionata dall'utente, una volta che il	Pand Only Mode	
	drive è stato autenticato con la password		
	temporanea. Tale procedura è utile	La	gin Cancel
	quando il drive viene assegnato ad un		
	altro utente. (Figura 4.14)		
		Figura 4.14 - Kichiedi II reset password al pro	ssimo accesso
	Nota: per maggiore sicurezza, la nuova	(per password diente)	
	password non può essere identica alla		
	password temporanea.		




#### 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.

	Device Initialization - VP50	GIRONKEY
Il campo " <b>Nome</b> " (Name) può contenere fino a 32 caratteri, ma non può contenere la password <b>esatta</b> .	Contact	)
Il campo " <b>Azienda</b> " (Company ) può contenere fino a 32 caratteri, ma non può contenere la password esatta.	Overet.	
Il campo " <b>Dettagli</b> " (Details) può contenere fino a 156 caratteri, ma non può contenere la password esatta.	Bock	OK Cancel
	Figura 4.14 - Schermata dei dati di c	ontatto

**Nota:** per poi poter accedere alla partizione protetta 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 è stato configurato con le password Amministratore e Utente (Ruolo amministratore), l'applicazione integrata nel drive IronKey VP50/VP50C si avvierà, richiederà prima 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)

Login Device - VP50 GIRONKEY ~	Login Device - VP50	GIRONKEY
A User Password	Admin Password	0
Contact Information Login as Admin	C Hint C Hint Reset Device	
Read-Only Mode	Read-Only Mode 1	
Login Cancel	Back	Login Cancel
Figura 5.1 - Accesso con Password Utente (Amministratore abilitato)	Figura 5.2 - Accesso con Password	d Amministratore
Modalità di accesso per solo utente	Login Device - VP50	GIRONKEY -
(Amministratore non abilitato)	Cuser Password	<b>0</b> =
Come indicato in precedenza, a <b>Pagina 13</b> , sebbene sia consigliabile utilizzare la funzione 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)	Persevord  Hint  Contact Information  Reset Device  Read-Only Mode  Figura 5.3 - Accesso con Password Uten	Login Cancel
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, tutti i dati contenuti sul drive saranno formattati e andranno persi per sempre.	Figura 5.3 - Accesso con Password Uten abilitato)	te (Amministratore non





## 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 presenti sul drive IronKey non possano essere modificati. 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	Login Device - VP50	GIRONKEY Y
<ol> <li>Inserire il dispositivo r computer host ed ese l'applicazione <b>IronKey</b></li> </ol>	nella porta USB del guire <b>exe</b> .	A User Password	0
<ol> <li>Selezionare la modalit (Read-Only) sotto il ca inserimento della pasi</li> </ol>	tà " <b>Sola lettura</b> " Impo di sword. ( <b>Figura 5.4</b> )	Contact information Reset Device	
<ol> <li>Immettere la passwor fare clic su "" (Login) . ora sbloccato e in mor lettura.</li> </ol>	d del dispositivo e Il drive IronKey è dalità di sola	Read-Only Mode 🗿	Login Cancel

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/VP50C, 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/VP50C 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 <u>10 tentativi falliti</u>, 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/VP50C" (Browse VP50/VP50C). (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.



## **Opzioni del dispositivo - (ambiente MacOS)**







## Opzioni dispositivo

Impostazioni VP50:	<ul> <li>modifica password di accesso, informazioni di contatto, altre impostazioni. (Ulteriori dettagli sulle impostazioni del dispositivo possono essere reperiti nella sezione "Impostazioni VP50/VP50C" di questo manuale).</li> </ul>	
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) Nota: la formattazione richiede l'autenticazione mediante password.	Login Device - VP50 User Password Varning! Formatting will erase ALL data on your encrypted drive. All data will be lost forever. Are you sure you want to proceed? Vos Cancel	
Supporto online (Online Support):	Figura 6.1 – Formattazione del drive VP50/VP50C         • Questa opzione consente di accedere al link         http://www.kingston.com/support, dal quale è         possibile accedere a una serie di informazioni di         supporto aggiuntive.	
Informazioni sul drive VP50 (About VP50): la sezione contiene dettagli specifici sull'unità VP50/VP50C, incluse le applicazioni, il firmware e informazioni sul numero di serie. (Figura 6.2)	About - VP50 GIRONKEY' ~ () About © 2022 Kingston Technology Corporation.	
Nota: il numero di serie univoco del drive può essere visualizzato nella colonna "Informazioni".	Modules         Version         Information           IKVP50         IKVP50         002324B53023B63190000062           Application         1.0.0.0           FW Version         01.06310           Crypto Library FW         1.00	
	Close Figura 6.2 – Informazioni sul drive VP50/VP50C	
Arresta VP50 (Shut down VP50):	<ul> <li>questa funzione permette di arrestare correttamente l'unità VP50/VP50C, consentendo all'utente di scollegare il drive dal computer in tutta sicurezza.</li> </ul>	





## Impostazioni del drive VP50/VP50C

#### 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)
  - o 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.

7.00.80 (1.0.0	GIRONKEY V	Settings - VP50	GIRONKEY V
Admin Settings	©   🚍	Admin Settings	<b>®</b>
Password Contact Info Language	Admin Options	Password Contact Info	Language Admin Options
Current Password		Current Password	
Please create a secure Complex password following the o	criteria below.	Please create a secure Complex password follo	wing the criteria below.
New Password		New Password	
Confirm New Password			
6-16 Jana		Confirm New Password	
uppercase lowercase digit special cits	laracter	6-16 long	
		uppercase lowercase digit s	pecial sharacter
Pássword Hint?		Presword Hint?	
Done	Apply Cancel		one Apply Cancel
Figura 7.1 – Opzioni p	bassword	Figura 7.2 - Dati	di contatto
iettings - VP50	GIRONKEY" -	Settings - VP50	GIRONKEY
Admin Settings		O Admin Settings	@)=
Password Contact Info Language	Admin Options	Pristword Contact Info	Languaur Admin Optimi
What is usur realizated Language?		Please enter a new User Password below.	
wina is your preter an congluoge.		Pasaword	
English	$\bigcirc$		
		Coofilmt PASaword	
		E-16 long	
		uppercase lowercase might	special character
		One-Time Recovery Password	
		C Force Read-Only User Data 🚺 C Login Password Re	set 🕤
Done	Apply Cancel		Done Apply Cancel





## Impostazioni del drive VP50/VP50C

### Impostazioni utente: Amministratore abilitato

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

Password:	Settings - VP50	GIRONKEY v
Utente e/o il suggerimento. ( <b>Figura 7.5</b> )	O Admin Settings	
	Password Contact Info Lan What is your preferred Language?	guage Admin Options
	English	
	Don	e Apply Cancel
	Figura 7.5 - Opzioni password (Amminist	ratore abilitato: Accesso utente)
Dati di contatto (Contact Info): consente di	Settings - VP50     O User Settings     Password Contact Info	
aggiungere/visualizzare/modificare i dati di contatto. ( <b>Figura 7.6</b> )	Please enter your information below. (Hamio Company Debails	
		ne Aprily Cancel
Lingua (Language):	Figura 7.6 - Informazioni di contatto (Ammir	histratore abilitato: Accesso utente)
consente di modificare le impostazioni della lingua corrente. ( <b>Figura 7.7</b> )	User Settings     Password Contact Into     What is your preferred Language?	Language -
	English	
	Figura 7.7 - Impostazioni lingua (Amminis	re Apply Cancel tratore abilitato: Accesso utente)

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





## Impostazioni del drive VP50/VP50C

#### Impostazioni utente: Amministratore non abilitato

Come precedentemente specificato a pagina 12, l'avvio del drive VP50/VP50C senza avere abilitato le password Amministratore e Utente, farà sì che l'unità sia configurata in modalità **Password singola, Utente singolo**. <u>Questa</u> <u>modalità di configurazione non permette di accedere ad alcuna opzione o funzionalità di amministrazione</u>. Questa configurazione prevede l'accesso alle seguenti impostazioni del drive VP50/VP50C:

#### Modifica e salvataggio delle impostazioni

	Settings - VP50	GIRONKEY .
<ul> <li>Ogni gualvolta si effettuano dei</li> </ul>	Admin Settings	
<ul> <li>Ogni qualvolta si effettuano dei cambiamenti alle impostazioni dell'unità VP50/VP50C (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)</li> </ul>	Password  Please enter your password  With tr  Franc  OK	enth Options
	Figura 7.11 - Schermata password che richiede il salvata per l'unità VP50/VP50C	nggio delle impostazioni

**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/VP50C.

## GIRONKEY"



## 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:	Settions - VP50 GIRONKEY -
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).	Seturings - OPSD       Context info         Admin Settings       Context info         Please enter a new User Password below       Context info         Please enter a new User Password below       Context info         Please enter a new User Password       Context info         Confirm Password       Context info         One-Time Recovery Password       Context info         Force Read-Only User Data C       Login Password Reset         Conce       Apply         Cancel       Figura 8.1 - Opzioni amministratore/Reset della password utente
Reset password di accesso (Login Password	Settings VD50 GIRONKEY >
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)	Image: Contract find       Language       Admin Options         Please enter a new User Password       Language       Admin Options         Please enter a new User Password       Image: Contert find       Language         Please enter a new User Password       Image: Contert find       Language         Please enter a new User Password       Image: Contert find       Language         Image: One-Time Recovery Password       Image: Owercase       digit       special character         One-Time Recovery Password       Image: Option       Apply       Cancel
	Login Device - VP50 GIRONKEY · V
<b>Nota:</b> 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).	User Password  Require password reset  The Admin has required that you reset your password;  The Admin has required that you reset you rese
	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	Settings - VP50 GIRONKEY" V
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)	Image: Construct Info       Language       Image: Construct Info         Password       Image: Construct Info       Language       Image: Construct Info         Image: Password       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Construct Info       Image: Construct Info       Image: Construct Info         Image: Construct Info       Image: Constrult Info       Image: Constrult In
<ul> <li>Fase 2: Creare una password di ripristino monouso utilizzando i medesimi criteri di impostazione password originariamente configurati per il dispositivo (password complesse o frasi).</li> <li>Nota: lapplicazione delle modifiche apportate richiede l'inserimento della password Amministratore.</li> </ul>	Settings - VP50       IRONKEY         One-Time Recovery Password       Image: Complex password following the criteria below.         Image: Please create a secure Complex password following the criteria below.       Image: Complex password         Image: Please create a secure Complex password following the criteria below.       Image: Complex password         Image: Please create a secure Complex password following the criteria below.       Image: Complex password         Image: Please create a secure Complex password       Image: Complex password         Image: Contigre Recovery Password       Image: Contigre Recovery Password         Image: Contigre Recovery Password       Image: Complex password         Image: Contigre Recovery Password       Image: Complex password         Image: Contigre Recovery Password       Image: Complex password         Image: Contigre Recovery Password       Image: Contigre Recovery Password
	Back         Save         Cancel           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	Login Device - VP50	GIRONKEY .
monouso, in occasione dell'accesso successivo, sarà visualizzato un nuovo pulsante nella schermata di accesso " <b>Password utente</b> " (User	A User Password	
password" (Password di ripristino)" per avviare la procedura.	Contact Information Recovery Password Log	n as Admin
	Read-Only Mode	
		Login Cancel
	Figura 8.6 - Pulsante Password di ripristi	no (Recovery password)
Fase 2: Sarà visualizzata la schermata "Password	Login Device - VP50	GIRONKEY .
<b>di ripristino</b> " (Recovery Password), nella quale è nossibile inserire la password di ripristino e	A Recovery Password	0
creare una nuova password utente. (Figura 8.7)	Recovery Password	
	Please create a secure password following the criteria below.	
Importante: Anche la password ripristino	Confirm New User Password	
monouso utilizza la funzionalità di sicurezza	6-16 long	
integrata che conteggia il numero di tentativi di	uppercase lowercase digit special ch	aracter
falliti. la funzione di inserimento password di	(Password Hint?	
ripristino monouso sarà disabilitata e sarà		
necessario riabilitarla effettuando un nuovo		Next Cancel
pagine 18 e 30 per ulteriori dettagli)	Figura 8.7 - Menu per la passw	ord ripristino
		Cusaurer
Fase 3: Una volta completata la procedura con	Login Device - VP50	
successo sarà visualizzata nuovamente la schermata " <b>Password utente</b> " (User Password). Il pulsante " <b>Password di ripristino</b> " (Becovery	<ul> <li>User Password</li> </ul>	(k) (m)
password) scompare e la password utente	Pressword	
inserita durante la Fase 2 diventa la nuova	O Hint	
password utente. (Figura 8.8)	Contact Information Login as Admin	
	Read-Only Mode 🕤	
		Login Cancel
	Figura 8.8 - Schermata "Accesso password Login), che mostra la scomparsa del pulsa dopo che tale funzionalità è stata uti	utente" (User Password nte password di ripristino lizzata con successo.





## Funzionalità amministratore

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

La modalità "sola lettura forzata" (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	Settings - VP50	GIRONKEY .
lettura" (Forced Read-Only) per i dati dell'utente, fare clic sulla relativa casella e poi su su "'Applica" (Apply). <b>(Figura</b> <b>8.9)</b>	Admin Settings     Password Contact Info     Languag     Please enter a new User Password below.     Priseword	a Admin Options
<b>Nota:</b> 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.	Gonfilm Pissword Gone-Time Recovery Password Force Read-Only User Data Color Password Reset Color Figura 8.9 - Abilitazione della funzione Forza i dati utente (l'applicazione delle modifiche apportate password Amminist	Apply Cancel a la modalità di sola lettura per erichiede l'inserimento della ratore)
<ul> <li>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)</li> </ul>	Login Device - VP50 User Password	Cancel





#### Blocco del dispositivo

Il drive VP50/VP50C 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.

	Login Device - VP50	GIRONKEY -
<ul> <li>Se viene inserita una password errata, sopra il campo " Inserimento password" (Password</li> </ul>	🔒 User Password	@  III
Entry) verrà visualizzato un messaggio di errore di colore rosso indicante il tentativo di accesso fallito. (Figura 9.1)	PASSWORD IS INCORRECT PASSWORD A Hint Contact Information Reset Device Read-Only Mode	Login Cancel
	Figura 9.1 - Messaggio di notifica inseri errata	mento password
	Login Device - VP50	
<ul> <li>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)</li> </ul>	PASSWORD IS INCORRECT YOU HAVE 3 MORE ATTEMPTS LEFTI Pletword Hint Reset Device Read-Only Mode Back Back	cein Cancel
	errato	



IRONKEY

#### 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:



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/VP50C 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/V<u>P50C.</u>





#### 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 <u>non</u> è abilitata), quando viene eseguito il Launcher dell'unità VP50/VP50C. (Vedere *Figure 9.7* e *9.8*)

<ul> <li>Questa opzione consente di creare una nuova password, ma per proteggere la privacy dell'unità VP50/VP50C il drive sarà formattato. Ciò significa che durante tale procedura tutti i dati andranno persi.*</li> </ul>	Login Device - VP50       IRONKEY' v         Admin Password       Imon Password         Password       Imon Password         Password       Imon Password         Image: Password       Imon Password         Image: Password       Image: Password         Image: Password       Image: Password         Image: Password       Image: Password         Image: Password       Image: Password         Figura 9.7 - Accesso con password Amministratore: Pulsante di reset
• 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)	Login Device - VP50       IRONKEY         I User Password       IIRONKEY         I User Password       IIIRONKEY         I User Password       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
<ul> <li>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.</li> </ul>	Login Device - VP50       IRONKEY         Admin Password       Imore to protect data privacy, your VP50 will be formatted and all data will be erased. Do you want to enter a new password and format your drive now?         Image: I

GIRONKEY"



## 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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.





#### Messaggi di errore

Impossibile creare il file (Unable to create file): 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.	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. OK 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): 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.	Error Copying File or Folder         Cannot copy File1: The disk is write-protected.         Remove the write-protection or use another disk.         OK         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): 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.	Error Deleting File or Folder       X         Cannot delete File1: The disk is write-protected.       Remove the write-protection or use another disk.         Cot       OK         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/VP50C 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<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) PENDRIVE CRIPTOGRAFADO USB 3.2 Gen 1

Manual do Usuário







#### Índice

Introdução	
Recursos IRONKEY Vault Privacy 50	
Sobre este Manual	
Requisitos do sistema 4	
Recomendações	5
Utilizando o sistema de arquivo correto 5	
Lembretes de utilização 5	
Melhores práticas para configuração de senha	6
Configurar meu dispositivo	7
Acesso ao dispositivo (Ambiente Windows) 7	
Acesso ao dispositivo (Ambiente macOS) 7	
Inicialização do dispositivo (Ambiente Windows e macOS)	8
Escolha de senha	9
Teclado virtual	
Botão de visibilidade de senha	
Senhas de Admin e de Usuário	
Informações de contato	
Uso do dispositivo (Ambiente Windows e macOS)	
Login para Admin e Usuário (Admin habilitado) 16	
Login para modo apenas usuário (Admin não habilitado)	
Desbloqueando no modo Somente Leitura 17	
Proteção de ataque de força bruta	
Acessando meus arquivos seguros	
Opções do dispositivo	
Configurações do VP50/VP50C	
Configurações do Admin	
Configurações do Usuário: Admin habilitado 22	
Configurações do Usuário: Admin não habilitado 23	
Alterar e Salvar configurações do VP50/VP50C	
Recursos do Admin	
Redefinição da senha de Usuário	
Redefinição de senha de login (Para Senha de Usuário)	
Senha de recuperação única	
Force os dados de usuário para somente leitura	
Ajuda e Resolução de Problemas	
Bloqueio do VP50/VP50C	
Restauração do dispositivo VP50/VP50C	
Conflito de Letra de Drive (Sistemas Operacionais Windows)	
Mensagens de Erro	



# Kingston





Figura 1: IronKey VP50

Figura 2: IronKey VP50C

## Introdução

O Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C 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/VP50C é superior ao uso da internet e serviços de nuvem para guardar dados.

O VP50/VP50C 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/VP50C 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/VP50C 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 50/50C (VP50/VP50C) e baseia-se na imagem de fábrica sem customizações implementadas.

#### **Requisitos do sistema**

<ul> <li>Plataforma de PC</li> <li>Intel, AMD &amp; Apple M1 SOC</li> <li>15 MB de espaço livre no disco</li> <li>Porta USB 2.0 - 3.2 disponível</li> <li>Duas letras consecutivas de drive após o último drive físico*</li> <li>*Observação: Consulte "Conflito de Letra de Drive" na página 32.</li> </ul>	<ul> <li>Suporte do Sistema Operacional do PC</li> <li>Windows 11</li> <li>Windows 10</li> <li>Windows 8.1</li> </ul>
<ul> <li>Plataforma Mac</li> <li>15 MB de espaço livre no disco</li> <li>Porta USB 2.0 - 3.2</li> </ul>	<ul> <li>Suporte do Sistema Operacional Mac</li> <li>macOS 11.x – 14.x</li> </ul>





## Recomendações

Para garantir que haja uma ampla energia fornecida ao dispositivo VP50/VP50C, insira-o diretamente em uma porta USB em seu notebook ou desktop, como visto na *Figura 1.1*. Evite conectar o VP50/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C automaticamente limpará os dados criptografados - formatando-se de volta para as configurações de fábrica.

#### Multissenhas

O VP50/VP50C 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/VP50C pode suportar três senhas diferentes utilizadas para recuperar os dados - Admin, Usuário e senha de Recuperação única.

O VP50/VP50C 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.

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/VP50C pode ser redefinido e reutilizado, mas os dados anteriores serão excluídos para sempre.

#### Modos de senha

O VP50/VP50C 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/VP50C 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/VP50C, 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.



#### Acesso ao dispositivo (Ambiente macOS)

Insira o VP50/VP50C 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.		C IRONKEY	88 0	000 ~ » Q	
•	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.	IRONNEY	IRONKEY	IRONKEY.exe	Windows	
			Figura 3.3 - Volu	ume IKVP		





## Inicialização do dispositivo (Ambiente Windows e macOS)

#### Idioma e EULA

	Dévice Initialization - VP50 GIRONKEY -
Selecione o seu idioma de preferencia no menu suspenso e clique em <b>Next</b> (Avançar). (Ver Figura 4.1)	Language What lik your preferred Language? English
	Figura 4.1 - Seleção de idioma
<ul> <li>Analise o acordo de licença e clique em Next (Avançar).</li> <li>Observação: Você deve aceitar o acordo de licença antes de continuar; de outra forma, o botão Next (Avançar) continuará inativo. (Figura 4.2)</li> </ul>	Cicense Agreement     SOFTWARE LICENSE AGREEMENT     IMPORTANT - READ CAREFULLY:     THIS SOFTWARE LICENSE AGREEMENT ('Agreement') is a legal agreement between you (either an     Individual or a single entity) and Kingston Technology Company Inc. ('Kingston'). This Agreement relates to the     software accompanying this Agreement, which includes computer software and may include associated media,     printed materials, and 'online' or electronic documentation (the "Licensed Software"). By downloading, installing,     copying, or otherwise using the Licensed Software, you agree to be bound by the terms of this Agreement and further     agree that the third party licensors of Kingston providing licenses for all or any portion of the Licensed Software shall     be third party beneficiaries of this Agreement. If you do not agree to the terms of this Agreement, do not install, copy     or use the Licensed Software.     The Licensed Software is protected by copyright laws and international copyright treaties, as well as other     intellectual property laws and treaties. The Licensed Software is licensed, not sold. The Licensed Software is     being provided solely for use with IronKey Encrypted USB product lines.
	Wes, Laccept       Back       Next       Cancel   Figura 4.2 - Contrato de Licença





#### Escolha de senha

Na tela de mensagem de Senha, você poderá criar uma senha para proteger seus dados no VP50/VP50C 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	Device Initialization - VP50 GIRONKEY -
<ul> <li>Deve conter 6 caracteres ou mais (até 16 caracteres).</li> </ul>	Password  Complex Passphrase  Please create a secure Complex password following the criteria below:
<ul> <li>Deve conter três (3) dos seguintes critérios:         <ul> <li>Letra maiúscula</li> <li>Letra minúscula</li> <li>Dígito numérico</li> <li>Caracteres especiais (!,\$,&amp;, etc.)</li> </ul> </li> </ul>	Enable Admin and User Password     Back Next Cancel      Figura 4.3 - Senha complexa
Senha de frase-passe	Device Initialization, VDE0 GIRONKEY
<ul> <li>Deve conter:         <ul> <li>Mínimo de 10 caracteres</li> <li>Máximo de 64 caracteres</li> </ul> </li> </ul>	Plessevord Complex Plassphrase Plesse create as secure Plassphrase Plesse create as
<ul> <li>Password Hint (Dica de senha) (Opcional)</li> <li>Uma Dica de senha pode ser útil para fornecer</li> <li>uma pista sobre a senha, se algum dia ela for</li> <li>esquecida.</li> <li>Observação: A dica NÃO pode ser a mesma</li> <li>que a senha.</li> </ul>	Password Hint? Figura 4.5 - Campo da dica de senha





#### 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)

Device Initialization - VP50	GIRONKEY .	Device Initialization - VP50	GIRONKEY
A Password	0	A Password	0 =
Complex Pass Please create a secure Complex password I ExamplePassw0rdI ExamplePassw0Rd v 5-16 long v uppricase v lowercase v digit Password Hint?	hrase billowing the criteria ballow.	Complex     Passphrase       Please create a secure Complex password following the criteria below.       ExamplePassw0rd       ExamplePassw0rd       ExamplePassw0rd       v 6-16 long       v luppercase     v dign       special character	)
Enable Admin and User Passwords ()		Enable Admin and User Passwords 🕜	¢.
	Back Next Cancel	Back	Cancel
Figura 4.6a - Condição e atendio	de senha complexa da	Figura 4.6b - Condição de senha con opcional	nplexa

	Device Initialization - VP50 GIRONKEY ~
	A Password (1)
Para senhas <b>inválidas</b> , as Caixas de critério de senha ficarão <b>vermelhas</b> e o botão <b>Next</b> (Avançar) será desabilitado até que os requisitos mínimos sejam atendidos.	Complex     Passphrase       Please create a secure Complex password following the criteria below.
Isso se aplica às senhas complexas e de frase-passe.	✓ uppercase ✓ fowercase X digit X special character Password Hint?
	Enable Admin and User Passwords Back Noxt Cancel Figura 4.7 - Condições de senha não atendidas





#### Teclado virtual

E.

O VP50/VP50C oferece um Teclado virtual que pode ser utilizado para proteção contra registros de toque do teclado (keylogger).

		Device Initialization - VP50 GIRONKEY V
•	Para usar o <b>Virtual Keyboard</b> (Teclado virtual), localize o botão de teclado do lado superior direito da tela de <b>Device Initialization</b> (Inicialização do dispositivo) e clique nele.	Password    Complex Passphrase   Please create a secure Passphrase   Please create a secure Passphrase   This is my Password Example!   This is my Password Example!   It is characters intrinum.   Password Hint?     Enable Admin and User Passwords •     Back     Noxt
		Figura 4.8 - Ativando o Teclado virtual
•	Quando o teclado virtual aparecer, você também pode habilitar a <b>Screenlogger Protection</b> (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.	Virtual Keyboard $1 \rightarrow 5$ coreenlogger Protection $2 \rightarrow \times$ 1234567890-= C Q w e r t y u i o p [ ] a s d f g h j k l ; ' return shift z x c v b n m , . / shift caps lock randomize 2
•	Para fazer com que este recurso seja mais sólido, você também pode escolher randomizar o teclado virtual selecionando <b>randomize</b> (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





#### 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".

	Device Initialization - VP50	GIRONKEY
	A Password	
Para <b>ocultar</b> a sequência de senha, clique no ícone cinza.	Complex Passphrase Please create a secure Passphrase password following the citieria bel	iow. 🚯
$\odot$	This is my Passw0Rd Eample!	
	This is my Passw0Rd Eample	
	2 10 characters minimum	
	Password Hint?	
	Enable Admin and User Passwords 👔	
	Back Next	Cancel
	Figura 4.10 - Botão para "ocultar" a Se	nha
	Device Initialization - VP50	GIRONKEY
	A Password	()
Dara quihing comba gaulta gligua na (gana gaul	Complex Passphrase	
Para <b>exibir</b> a senna ocuita, clique no icone azul.	Please create a secure Passphrase password following the criteria b	elow. ()
	v 10 characters minimum	
	Password Hint?	
	Enable Admin and User Passwords 👔	
	Back Next	Cancel
	Figura 4.11 - Botão para "exibir" a Ser	nha





#### 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.

		Device Initialization - VP50	BIRONKEY -
٠	Para habilitar as <b>senhas de Admin e de</b>	Password	® =
	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)	Complex Passphrase Please create a secure Passphrase password following the criteria below exercence or to characters minimum Presevont Him ?	
•	Se este recurso estiver <b>habilitado</b> , então a senha escolhida neste tela será a <b>senha de Admin</b> . Clique em <b>Next</b> (Avançar) para continuar para a tela da <b>senha de Usuário</b> onde uma senha é escolhida para o Usuário.	Enable Admin and User Passwords  Back Next 4.12- Habilitando as senhas de Admin e de	Cancel

#### 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.





#### Senhas de Admin e de Usuário

		Device Initialization - VP50	GIRONKEY
<ul> <li>Se a função</li> </ul>	Se a função de Admin foi <b>habilitada</b> na	A User Password	<u>ی</u> ا
	tela anterior, a tela seguinte pedirá a senha de Usuário (Figura 4.13) A <b>Senha</b> <b>de Usuário</b> terá capacidades limitadas em comparação com a do Admin e será discutida com mais detalhes depois neste Guia do Usuário. (Consulte a página 23)	Please create a secure Passphrase password following the criteria below. Pressword  Comming Password  To characters minimum  Password Hint?	B
		Require password reset on next login     Back     Next     Cancel      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	Login Device - VP50	GIRONKEY .
on next login" (Exigir redefinição de senha no próximo login) no canto inferior esquerdo da Figura 4.13 é	User Password  Require password reset	0
apenas para a Senha de Osuario 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	The Admin has required that you reset your passwo please proceed to crente a new password. O Hin Contact	rd:
drive for autenticado com a senha temporária, Isso é útil guando o drive é	C Réad-Only Mode 1	
dado para outra pessoa usar. (Figura 4.14)		Login Cancel
<b>Observação:</b> Por segurança, a nova senha não pode ser a mesma da senha temporária.	Figura 4.14 - Exigir redefinição de senha (para Senha de Usuário)	no próximo login





#### 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.)

	Device Initialization - VP50	GIRONKEY
O campo " <b>Name</b> " (Nome) pode conter até 32 caracteres, mas não pode conter a senha <b>exata</b> .	Contact	
O campo " <b>Company</b> " (Empresa) pode conter até 32 caracteres, mas não pode conter a senha <b>exata</b> .	( Details	
O campo do " <b>Details</b> " (Detalhes) pode conter até 156 caracteres, mas não pode conter a senha <b>exata</b> .	Figura 4.14 - Informação	
	. 19410 4.14 1110111440	

**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)

ocorre a Restauração do dispositivo.

Se o dispositivo for inicializado com as senhas de Admin e de Usuário (Função de Admin) habilitadas, o aplicativo IronKey VP50/VP50C 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)

Login Device - VP50 GIRONKEY	Login Device - VP50	GIRONKEY	
A User Password	Admin Password	<b>®</b>	
********	Password		
O Hint	O Hint		
Contect Information. Login as Admin	Reset Device		
Read-Only Mode 🕤	Read-Only Mode 🚯		
Login Cance		Back Logn Cancel	
Figura 5.1 - Login de Senha de Usuário (Admin habilita	do) Figura 5.2 - Login d	Figura 5.2 - Login de senha do Admin	
ogin para modo Somente Usuário (Admir	Login Device - VP50	GIRONKEY .	
abilitado)	🔒 User Password	@ [ iii	
omo mencionado anteriormente na <b>Página 1</b> 3	3.		
mbora seja recomendado usar a funcionalida	de da		
unção de Admin para obter todos os benefício	os de		
eu dispositivo, o drive IronKey também pode s	ser		
iciado em uma configuração Somente Usuári	O Contact Information Reset Device	2	
Senha única, Usuário único). Essa é uma opção	o para		
queles que gostariam simplesmente de uma	C Read-Only Mode		
bordagem de senha única para proteger os da	idos	Login Cancel	
m seu drive. (Figura 5.3)			
	Figura 5.3 - Login de Senha de U	Isuário (Admin não habilitado)	
bservação: Para habilitar as senhas de Admin	e de		
suario, use o botao <b>Reset Device</b> (Restaurar			
ispositivo) para colocar o drive de volta ao est			
e inicialização onde voce pode nabilitar as ser			
e Admin e de Usuario. IODOS os dados do dr	ive		
erao formatados e perdidos para sempre qua	indo		





## 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:

		Login Device - VP50	GIRONKEY .
1.	Insira o dispositivo na porta USB do computador host e execute o <b>IronKey.exe</b> .	A User Password	@[ <u></u> ]
2.	Marque o <b>Read-Only Mode</b> (modo Somente Leitura) abaixo da caixa de entrada da senha. <b>(Figura 5.4)</b>	Contact Information Reset Device	
3.	Digite a senha do seu dispositivo e clique em <b>Login</b> . O IronKey será desbloqueado no modo Somente Leitura.	C Read-Only Mode 3	Login Cancel
		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/VP50C e entrar de novo, deixando a caixa de marcação "Read-Only Mode" (Modo Somente Leitura) desmarcada.

**Observação:** As opções do Admin do VP50/VP50C 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 <u>10 tentativas erradas de senha</u>, 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/VP50C**. (Figura 6.2)
# GIRONKEY"



# **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.



# **Opções do dispositivo - (Ambiente macOS)**







# Opções do dispositivo

Configurações do VP50:	<ul> <li>Alterar senha de login, Informações de contato e outras configurações. (Mais detalhes sobre configurações do dispositivo podem ser encontrados na seção "Configurações do VP50/VP50C" deste manual).</li> </ul>		
Browse VP50/VP50C:	Permite que você visualize seus arquivos de segurança.		
Format VP50/VP50C: Permite que você formate a partição de dados segura. (Aviso: Todos os dados serão apagados) (Figura 6.1) Observação: A autenticação da senha será exigida para formatar.	Login Device - VP50       IRONKEY         User Password       Image: Content of the set of		
Online Support (Suporte on-line):	Figura 6.1 – Formatar o VP50/VP50C     Abre seu navegador de internet e vai para <u>http://www.kingston.com/support</u> onde você pode     acessar as informações de suporte adicionais.		
<ul> <li>About VP50/VP50C (Sobre o VP50/VP50C): Fornece detalhes específicos sobre o VP50/VP50C, incluindo Aplicação, Firmware e Informações de número de série. (Figura 6.2)</li> <li>Observação: O número de série único do drive estará na "Coluna de informações".</li> </ul>	About - VP50       IRONKEY"         About       2022 Kingston Technology Corporation.         Modules       Version         Modules       Modules         Version       0.0640         Core       Version         Figura 6.2 - Sobre o VPS0/VP50c		
Shut down VP50/VP50C (Desligar o VP50/VP50C):	<ul> <li>Encerra de modo apropriado o VP50/VP50C, permitindo que seja removido com segurança do seu sistema.</li> </ul>		





# Configurações do VP50/VP50C

#### 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
  - o Redefinição de senha de login (Para Senha de Usuário)
  - o Habilitar senha de Recuperação única
  - o Forçar modo Somente Leitura para dados do Usuário

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

Settings - VP50	GIRONKEY .	Settings - VP50	GIRONKEY -
@ Admin Settings	8 i 📖	Admin Settings	®   ==
Personent Constant labo Constant labo Constant Processor Personent Personen	ng the criteria botony.	Passers Contact Info Cirrent Phenomed Please create a secure Compter password for New Password Contine New Password 6-56 long uppercess lowerces agit (Password Print)	Languarges Ammin Opposite illowing the critiania bottow: special character Done Apply: Cancel
Settings - VP50	GIRONKEY" V	Settings - VP50	GIRONKEY .
Admin Settings		O Admin Settings	@1=
Password Contact Info	ngunge Admin Options	Preseword Contact Into	Languaser Admin.Optime
What is your preferred Language?		Please enter a new User Password below. Plassword Coofirm PAssword 5-56 long uppercase lowercane light One-Time Recovery Password	special character
		Force Read-Only User Data 🕦 📋 Login Password R	Reset 🕜
Do	ne Apply Cancel		Done Apply Cancel
Figura 7.3 - Opçõe	s de idioma	Figura 7.4 - Opc	ões do Admin





# Configurações do VP50/VP50C

# Configurações do Usuário: Admin habilitado

O login do Usuário limita o acesso às seguintes configurações:

Senha:	Settings - VP50	GIRONKEY -
Permite que você altere sua própria	Admin Settings	
senna de Osuano e/ou dica. ( <i>riguru 7.5)</i>	Password Contact Info	Language Admin Options
	What is your preferred Language?	
	English	
		Done Apply Cancel
	Figura 7.5 - Opções de senha do (/	Admin habilitado: Login do Usuário)
	Settings - VP50	GIRONKEY -
Informações de contato:	User Settings	
adicione/visualize/altere suas	Password Control	ct Info
informações de contato. (Figura 7.6)	Please enter your information.bei	
	Company	
		Done Apply Cancel
Idiama:	Figura 7.6 - Informações de contato	(Admin habilitado: Login do Usuário)
Permite que você altere sua seleção de	Settings - VP50	GIRONKEY V
idioma atual. (Figura 7.7)	@ User Settings	
	Password Conta	CT1060 Language
	What is your preferred Language?	
	English	<u> </u>
	Figura 7.7 - Configurações de Idioma	Dono Apply Cancel

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





# Configurações do VP50/VP50C

#### Configurações do Usuário: Admin não habilitado

Como mencionado anteriormente na Página 12, iniciar o VP50/VP50C sem habilitar as senhas de "Admin e de Usuário" vai configurar o drive em uma **configuração de Usuário único, Senha única.** <u>Esta configuração não possui</u> <u>acesso a qualquer recurso ou opção do Admin.</u> Esta configuração terá acesso às seguintes configurações do VP50/VP50C:

#### Alterar e Salvar configurações

	Settings - VP50	GIRONKEY .
Sempre que as configurações	Admin Settings     Password     Please enter your password     S	linin Options
forem alteradas nas Configurações do VP50/VP50C (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)	Please enter your password	pply Cancel

**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/VP50C.





#### 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:







# Senha de recuperação única

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

Senha de recuperação única	Settings - VP50 GIRONKEY ~
<b>Passo 1:</b> 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. <b>(Figuras 8.4)</b>	Image: Admin Settings       Image: Admin Settings         Password       Image: Admin Settings         Password       Image: Admin Settings         Confilmi Password       Image: Admin Settings         Image: Admin Settings       Image: Admin Settings         Image: Admin Settings       Image: Admin Settings         Password       Image: Admin Settings         Image: Admin Settings       Image: Admin Settings         Image: Admin
	Settings - VP50 GIRONKEY ~
<ul> <li>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).</li> <li>Observação: A senha do Admin será exigida para aplicar as alterações.</li> </ul>	One-Time Recovery Password     Please create a secure Complex password following the criteria below     Admine Password     Recovery Password     Confirm Recovery Password     Gala long     uppercase lowerense digit special character      Back Sove Cancel      Eigura 8, 5, - Configuração de Senha de recupação única





# Usando a senha de recuperação única

Passo 1: Depois que a Senha de recuperação	Login Device - VP50 GIRONKEY - V
única foi criada, um novo botão vai aparecer	A User Password 🐵 🗇
na tela de login da <b>User Password</b> (Senha de	
Usuário) no próximo login. Clique no botão	
Recovery Password (Senha de recuperação)	(Presented
para iniciar o processo.	O Hint
	Contact Information Recovery Password Login as Admin
	Read-Only Mode
	Login Cancel
	Figura 8.6 - Botão de Senha de recuperação
Passo 2: A tela da Recovery Password (Senha	Login Device - VP50 GIRONKEY ~ V
de recuperação) vai aparecer onde você pode	Recovery Password
inserir a Senha de recuperação e criar uma	
nova Senha de Usuário. (Figura 8.7)	Recovery Password
	Presse create a secure password following the criteria below           New User Password
Importante: A senha de recuperação única	Confirm New User Password
também utiliza um recurso de segurança	6-16 long
integrado que monitora o número de	uppercase lowercase digit special character
tentativas erradas de login, <b>depois de 10</b>	Princess of Ministry
tentativas de Login incorretas com a senha de	La anvalit Linut
recuperação unica, a senha sera desabilitada,	
e precisara ser reabilitada fazendo login no	Next Cancel
drive como Admin. (ver paginas 18 e 30 para	
mais detaines)	Figura 8.7 - Menu de Senha de recuperação
Passo 2: So hom susodido, vosô sorá lovado do	Login Device - VP50 GIRONKEY ~
volta à tela de liser Password (Senha de	🔒 User Password 🛛 🔞
Volta a tela de <b>Oser Password</b> (Senha de	
de recuperação) não está mais lá e a senha de	
Usuário inserida no <b>Passo 2</b> se tornará a nova	Plessward
Senha de Usuário (Figura 8.8)	D Hint
	Contact Information Login bs Admini
	Read-Only Mode 0
	Login
	Figura 8.8 - Tela de login da Senha de Usuário mostrando que o botão de
	Senha de recuperação desaparece depois do uso bem-sucedido.





#### 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.

<ul> <li>Para habilitar o Forçar Somente Leitura para os dados do Usuário, clique na caixa e clique em "Apply" (Aplicar). (Figura 8.9)</li> </ul>	Settings - VPSO  Admin Settings  Pessword Contact Infa Language  Please enter a new User Password below.	C IRONKEY
<b>Observação:</b> 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.	Password Confirm Password G-H6 long uppercase lowercase digit special charac One-Time Recovery Password Force Read-Only User Data C Login Password Reset C Done Figura 8.9 - Habilitar "Forçar dados de usuár (A Senha do Admin será exigida para a	ter Apply Cancel io para Somente Leitura" plicar as alterações)
<ul> <li>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)</li> </ul>	Login Device - VP50         User Password         Pessavori         Pessavori         Hint         Contact Information         Login Jas Admin         Read-Only Mode         Figura 8.10 - Modo Somente Leitura é forçado só pode ser desabilitado pel	Cancel





#### Bloqueio do dispositivo

O VP50/VP50C 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.
- Atingindo o MaxNoA e realizando um bloqueio de dispositivo ou formatação de dispositivo dependendo de como o drive for configurado.

	Login Device - VP50	GIRONKEY -
Se uma senha incorreta for inserida, uma	🔒 User Password	0
vermelho logo acima do campo de entrada de senha, indicando uma falha no login. (Figura 9.1)	PASSWORD IS INCORRECT  Forstaward  O Hint  Contact Information Reset Device  Read-Only Mode	Logir Cancel
	Figura 9.1 - Mensagen	n de senha incorreta ⊝ıronkey ∽
Quando a <b>7ª</b> tentativa errada for feita, você verá uma mensagem de erro adicional indicando que você tem mais 3 tentativas	Admin Password	C S
Quando a <b>7</b> ª 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)	Admin Password  PASSWORD IS INCORRECT YOU HAVE 3 MORE  PASSWORD IS INCORRECT INTO IN INTO INTO INTO INTO INTO INTO	ATTEMPTSLEFTI
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)	Admin Password  PASSWORD IS INCORRECT YOU HAVE 3 MORE  CHISOWORD  O Hint  Reset Device  Read-Only Mode	ATTEMPTS LEFT:
Quando a <b>7</b> <sup>a</sup> 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)	Admin Password  PASSWORD IS INCORRECT YOU HAVE 3 MORE  P	ATTEMPTS LEFT:



**IRONKEY**"

#### Bloqueio do dispositivo

**Importante:** Depois da **10**<sup>a</sup> 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 <u>formatará os</u> <u>dados e todos os dados no drive serão perdidos para sempre.</u> Comportamentos também mencionados na <u>página</u> <u>18</u> 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:

	ini, osuano nabintadoj	Senna do Admin	
Login Device - VP50	GIRONKEY -	Login Device - VP50	GIRONKEY
🔒 User Password	- <b>6</b> i =	Admin Password	@   1
Warning!  Vou have reached the maximum entries. In order to protect data UCKED. To recovery your data. One-Time Recovery password ()  Constant .	number of password privacy, your VP50 is now log in as Admin or use the f set up).	Warning     W	ntakimum number of password feet data privacy, your VPSO is now it data will be horizon to will be able to when the operation complete.
Read-Only Mode <b>1</b>		Read-Only Mode	
(Figura	2 9 3)		
ecuperação única: (Adr	min/Usuário habilitado)	Senha de Usuário	(Admin NÃO habilitado)
Recuperação única: (Adr	nin/Usuário habilitado) Gironkey: V	Senha de Usuário	igura 9.4) (Admin NÃO habilitado) ⊖ IRONKEY
Recovery Password  Pass  Warning:  Pass  Warning:  Pass  Warning:  Pass  Warning:  Pass  Warning:  Pass  Warning:  Pass  Pass Pass  Pass  Pass  Pass  Pass  Pass Pass  Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass Pass P	min/Usuário habilitado)	Senha de Usuário Login Device - VP50 User Password Wanning Wanning Wanning Wanning Contact Contact	igura 9.4) (Admin NÃO habilitado) © IRONKEY maximum number of password tect data privácy, your VP60 is new indate wife locido your VP60 is new indate wif
Recuperação única: (Adr Login Device - VP50  Recovery Password  Vou have reached the maximum password re to protect data privaça, j odom. To recover stored data an password. Login as Admin.  Pasaword Him 1	min/Usuário habilitado)	Senha de Usuário Login Device - VP50 User Password Warning! War	igura 9.4) (Admin NÃO habilitado) © IRONKEY maximum number of password tect data privácy, your VP60 is novi nan the operation completes.
Recovery Password Recovery Password Warning: Wurning:	min/Usuário habilitado)	Senha de Usuário Login Device - VP50 User Password Warning Warn	igura 9.4) (Admin NÃO habilitado) © IRONKEY maximum number of password ted data privice, your VPO is new in data wille locido is new in data wille locido your VID at le to nen the operation completex. OK Cancel O DO DISPOSITIVO*

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/VP50C 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/VP50C.





#### 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 <u>não</u> estiver habilitado) quando o iniciador do VP50 for executado. (ver **Figura 9.7 e 9.8**)

<ul> <li>Esta opção vai permitir que você crie uma nova senha, mas para proteger a privacidade de seus dados, o VP50/VP50C será formatado. Isso significa que todos os seus dados serão apagados no processo.*</li> </ul>	Login Device - VP50       IRONKEY         Admin Password       IRONKEY         Him       IRONKEY         Read-Only Mode       IRONKEY         Figura 9.7 - Senha do Admin: Botão para Restaurar Dispositivo
<ul> <li>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)</li> </ul>	Login Device - VP50       IRONKEY         # User Password       IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
<ul> <li>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.</li> </ul>	Login Device - VP50       IRONKEY         Admin Password       In order to protect data privacy, your VP50 will be formatted and all data will be erased. Do you want to enter a new password and format your drive new?         OK       Cancel         IRONK Mode       Isock         Eigura 9.9 - confirmação para Restaurar Dispositivo





#### Conflito de letra do drive: Sistemas operacionais Windows

- Como mencionado na seção de "Requisitos do Sistema" deste manual (na página 3), o VP50/VP50C 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/VP50C 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/VP50C 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.



Neste exemplo, (Figura 9.10), o VP50/VP50C 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/VP50C 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/VP50C 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.





#### Mensagens de Erro

Unable to create file (Não é possível criar o arquivo): 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.	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected.
<b>Error copying file or folder</b> (Erro ao copiar arquivo ou pasta): 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.	Error Copying File or Folder       X         Cannot copy File1: The disk is write-protected.       Remove the write-protection or use another disk.         OK       OK
Error deleting file or Folder (Erro ao apagar arquivo ou pasta): 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.	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/VP50C e entrar de novo, deixando a caixa de marcação "Read-Only Mode" (Modo Somente Leitura) desmarcada antes de fazer login.



# IRONKEY<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) SZYFROWANA PAMIĘĆ FLASH USB 3.2 Gen 1

Instrukcja obsługi







#### Spis treści

Wprowadzenie	
Cechy urządzenia Vault Privacy 50	
Informacje o tej instrukcji	
Wymagania systemowe	
	_
Uzywanie prawidłowego systemu plikow	
Zalecenia dotyczące uzytkowania	
Najiepsze metody konfiguracji nasła	0
Konfiguracja Urządzenia	7
Dostęp do urządzenia (środowisko Windows)	7
Dostęp do urządzenia (środowisko macOS)	7
Inicializacia urządzenia (środowisko Windows i macOS)	8
Wybór hasła	
Wirtualna klawiatura	
Przełącznik widoczności hasła	
Hasła administratora i użytkownika	
Informacje kontaktowe	
Korzystanie z urządzenia (środowisko Windows i macOS)	
Logowanie administratora i użytkownika (właczony tryb administratora).	
Logowanie w trybie Tylko użytkownik (wyłaczony tryb administratora)	
Odblokowywanie w trybie tylko do odczytu	
Ochrona hasła przed atakami typu Brute-Force	
Uzyskiwanie dostępu do zabezpieczonych plików	
Oncie urządzenia	10
Ustawienia pamięci VP50/VP50C	
Ustawienia administratora	
Ustawienia użytkownika: włączony tryb administratora	
Ustawienia użytkownika: wyłączony tryb administratora	
Zmiana i zapisywanie ustawień urządzenia VP50/VP50C	
Funkcje administracyjne	
Resetowanie hasła użytkownika	
Resetowanie hasła logowania (dla hasła użytkownika)	
Jednorazowe hasło odzyskiwania	
Wymuszenie danych użytkownika tylko do odczytu	
Pomoc i rozwiazywanie problemów	
Blokada urzadzenia VP50/VP50C	30
Resetowanie urzadzenia VP50/VP50C	
Konflikt liter dysku (system operacyjny Windows)	
Komunikaty o błędach	
· ·	



# Kingston





Ilustracja 1 – Urządzenie IronKey VP50

Ilustracja 2 – Urządzenie IronKey VP50C

#### Wprowadzenie

Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C jest również zgodna z przepisami TAA i montowana w USA. Ponieważ pamięć VP50/VP50C 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/VP50C 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/VP50C 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/VP50C 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 50/50C (VP50/VP50C) w wersji fabrycznej, tj. bez zmian dokonanych na życzenie klienta.

#### Wymagania systemowe

Platforma PC	Obsługiwane systemy operacyjne komputerów PC
<ul> <li>Intel, AMD i Apple M1 SOC</li> <li>15MB wolnego miejsca na dysku</li> <li>Dostępny port USB 2.0/3.2</li> <li>Dwie kolejne litery dysku po ostatnim dysku fizycznym*</li> </ul>	<ul> <li>Windows 11</li> <li>Windows 10</li> <li>Windows 8.1</li> </ul>
* <b>Uwaga:</b> patrz rozdział "Konflikt liter dysków" na str. 32.	
Platforma Mac	Obsługiwane systemy operacyjne komputerów
<ul> <li>15MB wolnego miejsca na dysku</li> </ul>	Мас
• Port USB 2.0/3.2	• macOS 11.x – 14.x





# Zalecenia

Aby zagwarantować odpowiednie zasilanie urządzenia VP50/VP50C, należy podłączać je bezpośrednio do portu USB w notebooku lub komputerze stacjonarnym, jak pokazano na *ilustracji 1.1*. Należy unikać podłączania urządzenia VP50/VP50C do urządzeń peryferyjnych z portem USB, takich jak klawiatura czy koncentrator zasilany z portu USB, jak pokazano na *ilustracji 1.2*.



#### Używanie prawidłowego systemu plików

Pamięć IronKey VP50/VP50C 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/VP50C 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.

# GIRONKEY



#### Najlepsze metody konfiguracji hasła

Pamięć VP50/VP50C 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/VP50C automatycznie wymaże zaszyfrowane dane, formatując się z powrotem do stanu fabrycznego.

#### Wiele haseł (funkcja Multi-Password)

Jedną z głównych funkcji funkcji pamięci VP50/VP50C 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/VP50C może obsługiwać trzy różne hasła, które można wykorzystać do odzyskania danych – hasło administratora, użytkownika oraz jednorazowe hasło odzyskiwania.

Pamięć VP50/VP50C 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/VP50C można bezpiecznie wymazać w celu ponownego wykorzystania, ale znajdujące się w niej dane zostaną bezpowrotnie usunięte.

#### Tryby hasła

Pamięć VP50/VP50C obsługuje również dwa różne tryby hasła:

#### Hasło złożone

Hasło złożone musi składać się z co najmniej 6-16 znaków oraz zawierać <u>co najmniej trzy</u> z następujących znaków:

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

#### Wyrażenie hasłowe

Pamięć VP50/VP50C 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/VP50C. 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.



#### Dostęp do urządzenia (środowisko macOS)

Włóż pamięć VP50/VP50C 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/VP50C (lub IRONKEY) (ilustracja 3.3).

•	Kliknij dwukrotnie ikonę CD-ROM IronKey.		IRONKEY	88 0	000 ~ » Q
•	Następnie kliknij dwukrotnie ikonę aplikacji IKVP50/VP50C (lub IronKey.app) widoczną w oknie pokazanym na ilustracji 3.3. Spowoduje to rozpoczęcie procesu inicjalizacji.	IRONNET	IRONKEY	IRONKEY.exe	Windows
			llustracja 3.3 – wo	lumin IKVP	





# Inicjalizacja urządzenia (środowisko Windows i macOS)

### Język i umowa licencyjna użytkownika końcowego

	Device Initialization - VP50 GIRONKEY ~
wybierz preferowany język z menu rozwijanego i kliknij przycisk <b>Next (Dalej)</b> (patrz ilustracja 4.1).	Language What is your prefetred Language? Engine:
	Ilustracja 4.1 – Wybór języka
	Device Initialization - VP50 GIRONKEY ~
Zapoznaj się z umową licencyjną i kliknij przycisk Next (Dalej). Uwaga: Aby kontynuować należy zaakceptować umowę licencyjną; w przeciwnym razie przycisk Next (Dalej) pozostanie nieaktywny (ilustracja 4.2).	Concept Agreement     Software LICENSE AGREEMENT (Greement') is a legal agreement between you (either an     fixed as a single entity) and Kingston fachnology Company Inc. (Kingston'). This Agreement rades to the     fixed are accompanying this Agreement, which includes computer software'). By downloading, installing,     grinted materials, and 'online' or electronic documentation (the 'Licensed Software'). By downloading, installing,     grinted materials, and 'online' or electronic documentation (the 'Licensed Software'). By downloading, installing,     grinted materials, and 'online' or electronic documentation (the 'Licensed Software'). By downloading, installing,     grinted materials, and 'online' or electronic documentation (the 'Licensed Software').     The Lensed Software is protected by copyright laws and international copyright treaties, as well as other     instelectual property laws and treaties. The Licensed Software is licensed, not sold. The Licensed Software is     besch         besch         Next         Cancel





#### Wybór hasła

Na ekranie monitu o podanie hasła można utworzyć hasło do ochrony danych zapisanych w pamięci VP50/VP50C, 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:

Hasło złożone	Device Initialization - VP50 GIRONKEY V
<ul> <li>Musi zawierać co najmniej 6 znaków (maks. 16 znaków).</li> </ul>	Password  Complex Passphrase  Please create a secure Complex password following the criteria below
<ul> <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 (!,\$,&amp;, itp.)</li> </ul> </li> </ul>	Password Contirm Password 6-16 long uppercase lowercase digit special character Password Hint? Enable Admin and User Passwords Back Next Cancel
Muraionia hastawa	Ilustracja 4.3 – Hasło złożone
<ul> <li>Musi zawierać:</li> <li>co najmniej 10 znaków</li> <li>maksymalnie 64 znaki</li> </ul>	Device Initialization - VP50 Password Complex Passphrase Please dreate a secure Plassphrase Please
Podpowiedź hasła (opcjonalnie) Podpowiedź hasła może być pomocna w przypomnieniu sobie zapomnianego hasła. Uwaga: Podpowiedź NIE MOŻE być taka sama iak hasło	Password Hint? Ilustracja 4.5 – Pole podpowiedzi hasła





#### 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).

Device Initialization - VP50	GIRONKEY .	Device Initialization - VP50	GIRONKEY
Password		A Password	0   =
Complex Passphrase		Complex Passphrase	
Please create a secure Complex password following the criteria b	elow. 🕦	Please create a secure Complex password following the criteria below.	Ð
ExamplePassw0rd!		ExamplePassw0rd	
ExamplePassw0Rd		ExamplePassw0rd	
✓ 6-16 long		~ 6-16 long	-
✓ uppercase  ✓ lowercase  ✓ digit  ✓ special character		Vuppercase Vowercase Vidigit special character	
Password Hint?		Password Hint?	5
🗋 Enable Admin and User Passwords ႐	1	Enable Admin and User Passwords 🚯	
Back	Cancel	Back Next	Cancel
Ilustracia 4.6a – Spełnione warunki dla ba	sta złożonego		

	Device Initialization - VP50 GIRONKEY V
	A Password
<sup>1</sup> przypadku zdefiniowania nieprawidłowego hasła, ola kryteriów hasła podświetlą się na czerwono, a rzycisk Next (Dalej) stanie się nieaktywny do czasu pełnienia minimalnych wymagań.	Complex     Passphrase       Please create a secure Complex password following the criteria below.     Image: Complex password       ExamplePassword     Image: Complex password       ExamplePassword     Image: Complex password       Image: Complex password     Image: Complex password
otyczy to zarówno haseł złożonych, jak i wyrażeń asłowych.	vuppercase      vlowercaso      × digit      × special character      Password Hint?      Enable Admin and User Passwords       Constribution





#### Wirtualna klawiatura

Pamięć VP50/VP50C jest wyposażona w funkcję wirtualnej klawiatury, która może służyć do ochrony przed keyloggerami.

	Device Initialization - VP50 GIRONKEY V
<ul> <li>Aby skorzystać z funkcji wirtualnej klawiatury, znajdź symbol klawiatury w prawym górnym rogu ekranu Device Initialization (Inicjalizacja urządzenia) i zaznacz go.</li> </ul>	Password <pre>             Complex Passphrase             Piesse create à secure Passphrase             Piesse create à secure Passphrase             Piesse create à secure Password following the criteria below.             This is my Passw0rd Example!             This is my Passw0rd Example !             This this this is my Passw0rd !</pre>
<ul> <li>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.</li> <li>Aby ta funkcja była jeszcze bardziej skuteczna, możesz wybrać losowy układ wirtualnej klawiatury, klikając klawisz randomize (randomizacja) w prawym dolnym rogu</li> </ul>	Virtual Keyboard 1234567890-= @ Qwertyuiop[1] asdfghjk1; 'return shift zxcvbnm,./shift caps lock randomize 2





#### 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".

	Device Initialization - VP50	GIRONKEY
	A Password	
Aby <b>ukryć</b> ciąg znaków hasła, kliknij szarą ikonę.	Complex Passphrase	
	Please create a secure Passphrase password following the criteria below	. 0
$\odot$	This is my Passw0Rd Eample!	)
	This is my Passw0Rd Eample	
	210 characters minimum	
	Password Hint?	
	Enable Admin and User Passwords	
	Back	Cancel
	llustracja 4.10 – Wybór opcji "ukryj" ha	sto
	Device Initialization - VP50	GIRONKEY
	Password	
	Complex Passphrase	
Aby <b>wyswietlic</b> ukryte nasło, kliknij niebieską ikonę.	Please create a secure Passphrase password following the criteria bel	ow. 🕦
	✓ 10 characters minimum	
	Password Hint?	$\supset$
	Enable Admin and User Passwords	
	Back Next	Cancel
	llustracja 4.11 – Wybór opcji "pokaż" ha	sło





#### 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.

		Device Initialization - VP50	ONKEY -
٠	Aby włączyć hasła administratora i	A Password	® =
	Admin and User passwords (Włącz hasła administratora i użytkownika) i kliknij przycisk Next (Dalej) po wybraniu prawidłowego hasła (ilustracja 4.12).	Complex Passphrase Please create a secure Passphrase password following the oriteria below.  Please create a secure Passphrase password following the oriteria below.  To characters minimum  Preceiver Him 5	
•	Jeśli ta funkcja jest <b>włączona</b> , hasło wybrane na tym ekranie będzie <b>hasłem</b> <b>administratora</b> . Kliknij przycisk <b>Next (Dalej)</b> , aby przejść do ekranu <b>hasła użytkownika</b> i zdefiniować hasło dla użytkownika.	Enable Admin and User Passwords     Back Next      Ilustracja 4.12 – Włączanie hasła administratora i uz	Cancel

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**.





#### Hasła administratora i użytkownika

	Device Initialization - VP50	GIRONKEY
Jeśli rola administratora została włączona na poprzednim ekranie, na następnym ekranie pojawi się monit o podanie <u>hasła użytkownika</u> (ilustracja 4.13). Hasło użytkownika zapewnia	User Password  Please create a secure Passphrase password following the criteria below.  Finassword  Continue Password	©   = 6
ograniczone uprawnienia w porównaniu z hasłem administratora, co zostanie szczegółowo omówione w dalszej części niniejszej instrukcji	Charlowned Hint?     Require password reset on next login	)
obsługi (patrz strona 23).	Back Next Ilustracja 4.13 – Hasło użytkownika (włączone hasła a użytkownika)	Cancel dministratora i

**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.

٠	Funkcja <b>Require password reset on next</b>	Login Device - VP50	GIRONKEY -
	login (Wymagaj zresetowania hasła przy nastepnym logowaniu), widoczna w	A User Password	®   =
	lewym dolnym rogu <b>ilustracji 4.13</b> ,	Reguire password reset	
	ją włączyć, aby wymusić na użytkowniku zalogowanie się przy użyciu tymczasowego hasła ustawionego przez administratora podczas procesu	The Admin has required that you reset your password: please proceed to crente a new password. O Hin Contact	
	inicjalizacji, a następnie do jego zmiany na wybrane przez siebie hasło po uwierzytelnieniu pamięci przy użyciu	Read-Only Mode	
	hasła tymczasowego. Jest to przydatne,		ogin Cancel
	użytkowania innej osobie <b>(ilustracja 4.14)</b> .	4.14). 4.14 – Wymaganie zresetowania hasła przy następnym (dla bacta użytkownika)	
	<b>Uwaga:</b> Ze względów bezpieczeństwa nowe hasło nie może być takie samo jak hasło tymczasowe.		





#### 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).

	Device Initialization - VP50	GIRONKEY
Pole <b>Name (Nazwa)</b> może zawierać do 32 znaków, ale nie może zawierać <b>samego</b> hasła.	Contact  Name Company	
Pole <b>Company (Firma)</b> może zawierać do 32 znaków, ale nie może zawierać <b>samego</b> hasła.	Details	
Pole <b>Details (Szczegóły)</b> może zawierać do 156 znaków, ale nie może zawierać <b>samego</b> hasła.	Ilustracja 4.14 – Informa	к ок Cancel

**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.

# GIRONKEY"



# 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/VP50C 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).

Login Device - VP50 GIRONKEY v	Login Device - VP50	NKEY"
🔒 User Password 🛞 📾	8 Admin Password	0
O Hint Contact Information	Password Phint Reset Device	
Read-Only Mode	Read-Only Mode 🕤	
Login Cancel	Back Login Car	ncel
Ilustracja 5.1 – Logowanie za pomocą hasła użytkownika (włączony tryb administratora)	Ilustracja 5.2 – Logowanie za pomocą hasła administr	atora
Logowanie w trybie Tylko użytkownik	Login Device - VP50 GIRON	IKEY -
(wyłączony tryb administratora)	A User Password	@[m
lak wspomniano wcześniej na <b>stronie 13</b> , 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).	Password O Hint Contact Information Reset Device Read-Only Mode 👔	
Uwaga: Aby aktywować hasła administratora i użytkownika, użyj przycisku <b>Reset Device (Resetuj</b> urządzenie), aby przywrócić pamięć do stanu nicjalizacji, 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 użytkow (wyłączony tryb administratora)	rnika





# 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:

		Login Device - VP50	GIRONKEY -
1.	Włóż urządzenie do portu USB komputera-hosta i uruchom program <b>IronKey.exe</b> .	A User Password	(m)
2.	Zaznacz pole wyboru opcji <b>Read-Only</b> <b>Mode (Tryb tylko do odczytu)</b> poniżej pola wprowadzania hasła <b>(ilustracja 5.4)</b> .	Contact Information Reset Device	
3.	Wpisz swoje hasło do urządzenia i kliknij przycisk <b>Login (Zaloguj się)</b> . Pamięć IronKey zostanie odblokowana w trybie tylko do odczytu.	Read-Only Mode  Ilustracja 5.4 – Tryb tylko do odcz	ceim Cancel

Aby odblokować urządzenie z pełnymi uprawnieniami do odczytu/zapisu na bezpiecznej partycji danych należy odłączyć pamięć VP50/VP50C i zalogować się ponownie, usuwając zaznaczenie pola wyboru opcji Read-Only Mode (Tryb tylko do odczytu).

**Uwaga:** Opcje administratora pamięci VP50/VP50C 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 <u>10 nieudanych prób wprowadzenia hasła</u>, 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 ( <u>WYŁĄCZONY</u> 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/VP50C (Przeglądanie zawartości pamięci VP50/VP50C)** (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.

<ul> <li>Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey (ilustracja 6.1).</li> </ul>	L G 10:20 AM 3/25/2022 Ilustracja 6.1 – Ikona IronKey na pasku zadań
<ul> <li>Kliknięcie prawym przyciskiem myszy ikony IronKey spowoduje otwarcie menu wyboru dostępnych opcji pamięci (ilustracja 6.2).</li> </ul>	<ul> <li>VP50 Settings</li> <li>Browse VP50</li> <li>Format VP50</li> <li>Online Support</li> </ul>
Szczegółowe informacje na temat tych opcji urządzenia można znaleźć na str. 19-23 niniejszej instrukcji.	About VP50     Shut down VP

### **Opcje urządzenia – środowisko macOS**







# Opcje urządzenia

VP50 Settings (Ustawienia pamięci VP50):	<ul> <li>Zmiana hasła logowania, informacji kontaktowych i innych ustawień. (Więcej informacji na temat ustawień urządzenia można znaleźć w części "Ustawienia pamięci VP50/VP50C" niniejszej instrukcji).</li> </ul>
Browse VP50 (Przeglądanie zawartości pamieci VP50):	Umożliwia przeglądanie bezpiecznych plików.
pamięci VP50):Format VP50 (Formatowanie pamięci VP50): Umożliwia sformatowanie zabezpieczonej partycji danych. (Ostrzeżenie: wszystkie dane zostaną usunięte) (ilustracja 6.1)Uwaga: Do formatowania wymagane jest uwierzytelnienie hasłem.	Login Device - VP50 User Password Warring! Formatting will erase ALL data on your encrypted drive. All data will be lost forever. Are you sure you want to proceed? Ves Cancel
Online Support (Pomoc techniczna online):	Ilustracja 6.1 – Formatowanie pamięci VP50/VP50C         • Umożliwia otwarcie przeglądarki internetowej i przejście na stronę <a href="http://www.kingston.com/support">http://www.kingston.com/support</a> , gdzie dostępne są dodatkowe informacje.
About VP50 (Informacje o pamięci VP50): Dostęp do szczegółowych informacji na temat pamięci VP50/VP50C, w tym informacji o aplikacji, oprogramowaniu sprzetowym i numerze servinym (ilustracia	About - VP50 G IRONKEY' ~ About  2022 Kingston Technology Corporation.
6.2). Uwaga: Unikalny numer seryjny znajduje się w kolumnie "Informacje".	Modules         Version         Information           IKVP50         IKVP50         002324B53023B63190000062           Application         1.0.0.0           FW Version         01.06610           Crypto Library FW         1.00
	Cloce Ilustracja 6.2 – Informacje o pamięci VP50/VP50C
Shut down VP50 (Wyłączenie pamięci VP50):	<ul> <li>Umożliwia prawidłowe wyłączenie pamięci VP50/VP50C, co pozwala na jej bezpieczne odłączenie od komputera.</li> </ul>





# Ustawienia pamięci VP50/VP50C

#### 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
  - o Resetowanie hasła logowania (dla hasła użytkownika)
  - o Jednorazowe hasło odzyskiwania
  - o Wymuszony tryb tylko do odczytu dla danych użytkownika

#### **UWAGA:** Więcej szczegółowych informacji na temat opcji administratora znajduje się na stronie 24.

Settings - VP50	GIRONKEY .	Settings - VP50	GIRONKEY -
Admin Settings     According Contract Info     According Contract Info      Cont	eger Admini Oracioni, Ibie criteria biolox: Icclaniscter	Commit Settings Personni Commit Info Commit Personnal Presse create a secure Compter papaverit follow Merry Password Comfilmer Neury Personnal Griffing Upperceste Forwardsen digit digit	Amy angunge Amira Options
Ilustracja 7.1 – Op	cje hasła	Ilustracja 7.2 – Inform Settings-VP50	acje kontaktowe
Admin Settings		Ø Admin Settings	@) =
Password Contact Info	nge Admin Dytems	Pessword Contact Into Please enter a new User Password below. Password Coofirm Pissword 6-16 long uppercase lowercase bight s One-Time Recovery Password Force Read-Only User Data  Cologin Password Res	Anguaure Admin Dissume percial character
Dong	Apply Cancel		one Apply Cancel
Ilustracia 7.3 – Opo	rie jezyka	Ilustracia 7.4 – Opcie	administratora





# Ustawienia pamięci VP50/VP50C

#### Ustawienia użytkownika: włączony tryb administratora

Zalogowanie się jako użytkownik powoduje ograniczenie dostępu do następujących ustawień:

Password (Hasło):	Settings - VP50 GIRONKEY" ~		
umoziiwia zmianę nasta i/lub podpowiedzi do basta użytkownika	O Admin Settings		
podpowiedzi do hasła użytkownika ( <i>ilustracja 7.5</i> ).	Possword Contact Info Language Admin Options What is your preferred Language?		
	Done Apply Cancel		
	Ilustracja 7.5 – Opcje hasła (włączony tryb administratora: logowanie użytkownika)		
	Settings - VP50 GIRONKEY' v		
Contact Info (Informacje kontaktowe):	@ User Settings		
umozliwia dodanie/wyswietienie/zmianę	Password Contact Into Language		
	Please enter your information below:		
	Company		
	Denne		
	Done Asoly Cancel		
	logowanie użytkownika)		
Language (Język): Umożliwia zmianę aktualnie wybranego języka ( <i>ilustracja 7.7</i> ).	Settings - VP50 GIRONKEY · ·		
	User Settings     Passward Contactility Language		
	time in a second second second		
	What is your privated Languages		
	Dene Apply Cancel		
	Ilustracja 7.7 – Ustawienia języka (włączony tryb administratora: logowar użytkownika)		

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




# Ustawienia pamięci VP50/VP50C

#### Ustawienia użytkownika: tryb administratora nie jest włączony

Jak wspomniano wcześniej na stronie 12, inicjalizacja pamięci VP50/VP50C bez włączania haseł administratora i użytkownika spowoduje skonfigurowanie pamięci z **jednym hasłem dla pojedynczego użytkownika**. <u>Konfiguracja ta</u> <u>nie zapewnia dostępu do żadnych opcji ani funkcji administracyjnych.</u> Konfiguracja ta umożliwia dostęp do następujących ustawień pamięci VP50/VP50C:

#### Zmiana i zapisywanie ustawień

	Settings - VP50	GIRONKEY .
<ul> <li>Po każdej zmianie ustawień pamięci VP50/VP50C (np. informacji kontaktowych, języka, hasła, opcji administratora itp.) pamięć wyświetli monit o</li> </ul>	Admin Settings      Password      What I      Franç	imin Options
wprowadzenie hasła w celu zaakceptowania i zastosowania zmian (patrz ilustracja 7.11).	lustracja 7.11 – Ekran monitu o podanie hasła w cel ustawień pamięci VP50/VP50C	Cancel

**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/VP50C.





#### 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:	Settings - VP50	GIRONKEY .
Zmień ręcznie zmień hasło użytkownika w menu "Admin Options" (Opcje administratora) – zmiana będzie natychmiastowa i zacznie obowiązywać przy następnym logowaniu użytkownika (ilustracja 8.1). Uwaga: Kryteria wymagań dla hasła zostaną domyślnie ustawione na pierwotne kryteria, które zostały ustawione podczas procesu inicjalizacji (opcje hasła złożonego lub wyrażenia hasłowego).	Admin Settings      Presseent Constitute     Idenguage      Presseenter a move Uter Password below      Password      Continue Recovery Password      One-Time Recovery Password      Cone      Inustracja 8.1 – Opcje administratora / recurrenter      urintkownika	Aren Coore Aren Coore Cancel setowanie hasła
Resetowanie hasła do logowania: 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).	Settings - VP50 Consult like Plassword Delow, Plassword Consult like Plassword Delow, Plassword Consult like Plassword Delow, Plassword Contine Reservery Plassword Delow, Contine Recovery Plassword Force Read-Only User Data C Login Plassword Reset C Done	Apply Cancel
<b>Uwaga:</b> 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).	Login Device - VP50 User Password Require password reset The Admin has required that you reset your password please proceed to crente a new password. Nin Contact Read-Only Mode Ilustracja 8.2B – Powiadomienie o zresetowar hasła użytkownika	





### Jednorazowe hasło odzyskiwania

W tej części omówiono proces włączania i używania funkcji jednorazowego hasła odzyskiwania.

Jednorazowe hasło odzyskiwania	Settings - VP50 GIRONKEY' ~
<b>Krok 1:</b> 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 <b>(ilustracja 8.4).</b>	Admin Settings       Image: Admin Options         Pessword       Contact Into       Janguage       Admin Options         Pessword       Descriptions       Image: Admin Options       Image: Admin Options         Pessword       Editions       Image: Admin Options       Image: Admin Options         Pessword       Image: Admin Options       Image: Admin Options       Image: Admin Options         Pessword       Image: Admin Options       Image: Admin Options       Image: Admin Options         Image: Description of the Admin Options       Image: Admin Options       Image: Admin Options       Image: Admin Options         Image: Description of the Admin Options       Image: Admin Options       Image: Admin Options       Image: Admin Options         Image: Description of the Admin Options       Image: Admin Options       Image: Admin Options       Image: Admin Options         Image: Description of the Admin Options       Image: Admin Options       Image: Admin Options       Image: Admin Options         Image: Description of the Admin Options       Image: Admin Options       Image: Admin Options       Image: Admin Options         Image: Description of the Admin Options       Image: Admin Options       Image: Admin Options       Image: Admin Options         Image: Description of the Admin Options       Image: Admin Options       Image: Admin Options       Ima
<ul> <li>Krok 2: Utwórz jednorazowe hasło odzyskiwania, korzystając z tych samych kryteriów hasła, które zostały początkowo ustawione na urządzeniu (hasło złożone lub wyrażenie hasłowe).</li> <li>Uwaga: Do wprowadzenia zmian będzie wymagane hasło administratora.</li> </ul>	Settings - VP50 CIRONKEY ~
	Back Sove Cancel





### Korzystanie z jednorazowego hasła odzyskiwania

Krok 1: Po utworzeniu jednorazowego hasła	Login Device - VP50
odzyskiwania, przy następnym logowaniu na ekranie logowania <b>User Password (Hasło</b> użytkownika) pojawi się nowy przycisk. Kliknij przycisk <b>Recovery Password (Hasło</b>	A User Password 🚳 📾
odzyskiwania), aby rozpocząć proces.	Primerodol     O Hint     Contract Information     Recovery Password     Login as Aomin     Login as Aomin     Login     Login     Cancel
	Ilustracja 8.6 – Przycisk hasła odzyskiwania
Krok 2: Wyświetli się ekran Recovery	Login Device - VP50 GIRONKEY ~
<b>Password (Hasło odzyskiwania)</b> , na którym można wprowadzić hasło odzyskiwania i utworzyć nowe hasło użytkownika (ilustracja 8.7).	Recovery Password
Ważne: Jednorazowe hasło odzyskiwania wykorzystuje również wbudowaną funkcję bezpieczeństwa, która śledzi liczbę nieudanych prób logowania. Po 10 nieudanych próbach zalogowania się za pomocą jednorazowego	Confirm New User Password 646 long Uppercase lowercase digit special character Palasword Hin17
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).	Vexe Cancel
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).	A User Password ⊗ I
	Petersward     Petersward     Define     Contact Information     Login as Admiss
	Read-Only Mode 8
	Legin
	Ilustracja 8.8 – Ekran logowania za pomocą hasła użytkownika bez widocznego przycisku odzyskiwania hasła po jego pomyślnym użyciu.





### 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.

<ul> <li>Aby włączyć wymuszony tryb tylko do odczytu dla danych użytkownika, kliknij odpowiednie pole, a następnie przycisk "Apply" (Zastosuj) (ilustracja 8.9).</li> </ul>	Settings - VP50  Admin Settings  Pessword Consist Info Language  Please enter a new User Password below.	IRONKEY
<b>Uwaga:</b> 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.	Pessword Carthins Password G-16 long Uppercase digit special chara One-Time Recovery Password Force Read-Only User Data C Login Password Reset C Done Ilustracja 8.9 – Włączenie opcji "Force Read dane użytkownika tylko do – do wprowadzenia zmian wymagane jes	Apply Cancel -Only User Data" (Wymuś odczytu) st hasło administratora
<ul> <li>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).</li> </ul>	Login Device - VP50 User Password Peterkood O Hint Contact Information Login as Admin Read-Only Mode Ilustracja 8.10 – Tryb tylko do odczytu jest wy może zostać wyłączony tylko przes	Cancel





### Pomoc i rozwiązywanie problemów

#### Blokada urządzenia

Pamięć VP50/VP50C 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.

	Login Device - VP50	
<ul> <li>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).</li> </ul>	User Password  PAssword is incorrect  Padawerd  O Hint  Contact Information  Reset Device  Ilustracja 9.1 – Komunikat o wprowae	Cancel
<ul> <li>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).</li> </ul>	Lógin Device - VP50 Admin Password PASSWORD IS INCORRECT YOU HAVE 3 MORE ATT PASSWORD O Hint Reset Device Read-Only Mode Ilustracja 9.2 – Siódma nieudana	EMPTS LEFTI



# Pomoc i rozwiązywanie problemów

**IRONKEY**"

#### 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 <u>sformatowanie danych i ich bezpowrotną utratę</u>. O tych zachowaniach urządzenia wspomniano również na <u>stronie 18</u> niniejszej instrukcji obsługi.

Ilustracje 9.3-9.6 poniżej przedstawiają zachowanie urządzenia po dziesiątej i ostatniej nieudanej próbie logowania dla każdej z metod logowania:



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/VP50C 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/VP50C.





### 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 <u>wyłączony</u>) podczas uruchamiania oprogramowania pamięci VP50/VP50C (patrz *ilustracje 9.7* i **9.8**).

<ul> <li>Ta opcja umożliwia utworzenie nowego hasła, ale w celu ochrony poufności danych pamięć VP50/VP50C zostanie sformatowana. Oznacza to, że wszystkie dane zostaną usunięte.*</li> </ul>	Login Device - VP50       IRONKEY         Admin Password       Image: Concelege         Him       Image: Concelege         Back       Concelege         Ilustracja 9.7 – Hasło administratora: przycisk resetowania urzadzenia
• <b>Uwaga:</b> Po kliknięciu przycisku <i>Reset Device</i> (Resetuj urządzenie) zostanie wyświetlony komunikat z pytaniem, czy chcesz wprowadzić nowe hasło przed rozpoczęciem formatowania. Na tym etapie można 1) kliknąć przycisk <i>OK</i> , 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 iest właczony): przycjsk resetowania urządzenia
<ul> <li>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.</li> </ul>	Login Device - VP50 Admin Password I order to protect data privacy, your VP50 will be formatted and all data will be erased. Do you want to enter a new password and format your drive now? OK Cancel Back Concel Ilustracja 9.9 – Potwierdzenie resetowanie urządzenia



# IRONKEY"

# Pomoc i rozwiązywanie problemów

### Konflikt liter dysku: system operacyjny Windows

- Jak wspomniano w części Wymagania systemowe niniejszej instrukcji obsługi (na str. 3), pamięć VP50/VP50C 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/VP50C 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/VP50C 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.



W tym przykładzie (ilustracja 9.10) pamięć VP50/VP50C 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/VP50C 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/VP50C, 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.







### 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.	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. OK 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.	Error Copying File or Folder Cannot copy File1: The disk is write-protected. Remove the write-protection or use another disk. OK 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.	Error Deleting File or Folder         Cannot delete File1: The disk is write-protected.         Remove the write-protection or use another disk.         OK         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/VP50C i zalogować się ponownie, usuwając przed uwierzytelnieniem zaznaczenie pola wyboru "Read-Only Mode" (Tryb tylko do odczytu).



**IRONKEY<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C)** 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

はじめに	
Vault Privacy 50 の機能	
本書について	
システム要件	
推奨事項	5
正しいファイルシステムの使用	
使用上の注意	
パスワード設定のベストプラクティス	6
デバイスの設定	7
デバイスアクセス(Windows 環境)	7
デバイスアクセス(macOS 環境)	7
デバイスの使用 (Windows および macOS 環境)	
パスワードの選択	9
仮想キーボード	
パスワード表示の切り替え	
管理者およびユーザーのパスワード	
連絡先情報	
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)	
ユーザー専用モードでのログイン(管理者が無効な場合)	
読み取り専用モードでのアンロック	
総当たり攻撃の防止	
保護下のファイルへのアクセス	
デバイスオプション	
VP50/VP50C の設定	
管理者設定	
ユーザー設定: 管理者有効	
ユーザー設定: 管理者無効	
VP50/VP50C 設定の変更および保存	
管理者の機能	
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(ユーザーパスワードの場合)	
一回限りの回復パスワード	
強制的にユーザーデータを読み取り専用に設定	
ヘルプとトラブルシューティング	
<b>VP50/VP50C</b> ロックアウト	
VP50/VP50C デバイスのリセット	
ドライブ文字の競合(Windows オペレーティングシステム)	
エラーメッセージ	









図1: IronKey VP50

図 2 : IronKey VP50C

# はじめに

Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C はまた、TAA 準拠で米国で組み立てられています。VP50/VP50C 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/VP50C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」 (2) 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/VP50C 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/VP50C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 50/50C (VP50/VP50C) 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

<ul> <li>PC プラットフォーム <ul> <li>Intel、AMD および Apple M1 SOC</li> <li>15MB のディスク空き容量</li> <li>USB 2.0~3.2 ポート対応</li> <li>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*</li> </ul> </li> <li>*注:「ドライブ文字の競合」(32ページ)を参照してください。</li> </ul>	対応 PC オペレーティングシステム (OS) • Windows 11 • Windows 10 • Windows 8.1
Mac プラットフォーム <ul> <li>15MB のディスク空き容量</li> <li>USB 2.0~3.2 ポート</li> </ul>	対応 Mac オペレーティングシステム (OS) • macOS 11.x – 14.x





### 推奨事項

VP50/VP50C 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/VP50C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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C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/VP50C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/VP50C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/VP50C 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/VP50C 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/VP50C**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/VP50C 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。



# デバイスアクセス(macOS 環境)

VP50/VP50C 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/VP50C(または IRONKEY)と いうボリュームが表示されます。(図 3.3)







# 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、 <b>Next [次へ]</b> をクリックしま す。(図 4.1 参照)	Device Initialization - VP50 GIRONKEY v
	Language What is your preferred Language? Enginer
使用許諾契約をよく読んで Next [次へ] をク	Nex Cancel 図 4.1 - Language [言語]の選択 Device Initialization - VP50 @IRONKEY ~ License Agreement
リックします。 注:次のステップに進む前に、使用許諾契 約に同意する必要があります。同意しない と、Next [次へ]のボタンは有効になりませ ん。(図 4.2)	IMPORTANT - READ CAREFULLY: THIS SOFTWARE LICENSE AGREEMENT ("Agreement") is a legal agreement between you (either an individual or a single entity) and Kingston Technology Company Inc. ("Kingston"). This Agreement relates to the software accompanying this Agreement, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (the "Licensed Software"). By downloading, installing, copying, or otherwise using the Licensed Software, you agree to be bound by the terms of this Agreement and further agree that the third party licensors of Kingston providing licenses for all or any portion of the Licensed Software shall be third party beneficiaries of this Agreement. If you do not agree to the terms of this Agreement, do not install, copy or use the Licensed Software is protected by copyright laws and international copyright treaties, as well as other instellectual property laws and treaties. The Licensed Software is licensed, not sold. The Licensed Software is being provided solely for use with IronKey Encrypted USB product lines.  // Yes, I accept
	Back Next Cancel 2014.2 - License Agreement [使用許諾契約]





#### 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/VP50C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]	Device Initialization - VP50	
• 6 文字以上の長さ (最大 16 文字) でな	A Password	
ければなりません。	Complex Passphrase	
	Please create a secure Complex password following	g the criteria below. 👔
<ul> <li>以下の文字の種類のうち、3つが含ま</li> </ul>	Passivord	
れていなければなりません。	Confirm Password	
o 英大文字	6-16 long uppercase lowercase digit spec	ial character
o 英小文字	Password Hint?	
o 数字	Enable Admin and User Passwords 1	
o 特殊文字(!、\$、& など)	Back	Alert Course
	Dack	
	図 4.3 - Complex [複雑な	:パスワード]
Passphrase [パスフレースパスリード]	Device Initialization - VP50	GIRONKEY
<ul> <li>文字数の制限:</li> </ul>	Password	(a) ) ( <u>m</u>
○ 最短 10 文字	Complex Passphrase	
o 最長 64 文字	Please create a secure Passphrase bassword tollow	ing the criteria below.
	Contraction Deservation	
	10 characters minimum	
	Padaword Hum?	
	Enable Admin and User Passwords ()	
	Back	Cancel
	図 4.4 <sup>-</sup> 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	Password Hint?	
た場合に、パスワードの手がかりを示して	図 4.5 – Password Hint [パスワート	「のヒント]フィールド
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。		





### 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)







仮想キーボード

VP50/VP50C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。

	Device Initialization - VP50 GIRONKEY V
<ul> <li>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。</li> </ul>	Device Initialization - VP50 Password Complex Passphrase Please create à secure Passphrase Please create à secure Passphrase Please create à secure Passphrase Please Order & Password Following the criteria below. This is my PasswOrd Example! Planeword Hint? Enable Admin and User Passwords
<ul> <li>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。</li> <li>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</li> </ul>	Image: Imag





### 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。

	Device Initialization - VP50	ONKEY
	A Password	
ハスリートの文子列を <b>非衣示</b> にしたい場合は、ク レーのアイコンを クリックします。	Complex Passphrase	
$\overline{\mathbf{O}}$	This is my Passw0Rd Eample!	
	This is my Passw0Rd Eample	
	Password Hint?	
	Enable Admin and User Passwords 🍿	
	Back Next C	Cancel
	図 4.10 - パスワード「表示」への切り替え	
	Device Initialization - VP50	RONKEY
	A Password	
北古二の パッロー いとまご トスレント ディーのマ	Complex Passphrase	
非表示のハスリードを表示するには、フルーのア	Please create a secure Passphrase password following to criteria below. 🜖	
イコンをクリックします。		
······		
<u>®</u>	✓ 10 characters minimum	
	Pressword Him?	
	Enable Admin and User Passwords 🚯	
	Back Next	Cancel
	図 4.11 - パスワード「表示」への切り替え	





### 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<u>有効</u>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。

		Device Initialization - VP50 GIRONKEY	r
•	管理者およびユーザーのパスワードを有	Password 6	
	効にするには、Enable Admin and User	Complex Passphrase	
	Passwords [管理者およびユーザーのパス	Please mate a serum Passninise natiswert following the relief a below	
	<b>ワードを有効にする]</b> 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	000000000	
	てから Next [次へ] を選択します。(図	- 10 characters minimum	
	4.12)		
		Persovani Pini 7	
		Enable Admin and User Passwords	
٠	この機能が <b>有効</b> な場合、この画面で選択		
	されているパスワードは <b>管理者パスワー</b>	Back Next Cance	
	ドになります。Next [次へ] を選択し、ユ	図4.12 – Enable Admin and User Passwords [管理者およびコ	ーザー
	ーザーパスワード画面に進んで、ユーザ	のパスワードを有効にする]	
	一用のパスワードを選択します。		

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。





### 管理者およびユーザーのパスワード

	Device Initialization - VP50	GIRONKEY
<ul> <li>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。(22 0°)、ごなを照して</li> </ul>	Device Initialization - VP50 User Password Please create a secure Passphrase password following the criteria b Pressword Comming Password 10 characters minimum	
説明しよす。(23 ヘーンを参照して ください)	Partsword Hint?         Require password reset on next login          Back         Next         Ø 4.13 – User Password [ユーザーパスワード] (管理 効な場合)	Cancel 里者とユーザーが有

**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	Login Device - VP50	GIRONKEY -
バ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	User Password      Require password reset      The Admin has required that you reset your password;     please proceed to create a new password.     O Hin      Contact      OK	
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	Read-Only Mode 🕤	ogin Cancel
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! (ユーザーパスワードの場合	リセットが必要 )





### 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。)

	Device Initialization - VP50	GIRONKEY
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。	Contact	
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 <b>まったく同じ</b> 文字列を 入力することはできません。		
<b>Details [明細]</b> 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 <b>まったく同じ</b> 文字列を 入力することはできません。		OK Cancet

**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/VP50C 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)

Login Device - VP50	GIRONKEY .	Login Device - VP50	GIRONKEY
🔒 User Password	<b>®</b>   <b>=</b>	Admin Password	<b>6</b>
O Hint Contrict Information Login & Alomin		Pessyupro O Hint Reset Device	
Read-Only Mode		Read-Only Mode <b>1</b>	
	Login Cancel	Back	Login Cancel
図 5.1 - ユーザーパスワードでのログイ 効な場合)	ン(管理者が有	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	Login Device - VP50	GIRONKEY .
が無効な場合)		🔒 User Password	@( m)
ページ13で前述したように、デ 完全に活用するには管理者ロー/ 推奨されますが、ユーザー専用 スワード、単一ユーザー)設定 イブを初期化できます。これは、 ーパスワード手法を好む人が、 タの安全を保つためのオプション 注:管理者およびユーザーのパン にするには、Reset Device [デバイ ボタンを使用して初期化状態に ます。そこで、管理者およびユー ードを有効にできます。デバイン れると、ドライブ上のすべての マットされ、永久に失われます。	バイスの利点を レ機能の使用が モード(単一パ でも IronKey ドラ シンプルな単 ドライブでデー 、 (図 5.3) スワードを列 「ライブを戻し ーザリセットさ データがフォー	Password O Hint Contact Information Reset Device Read-Only Mode 図 5.3 - ユーザーパスワードでのロ な場合)	<u>Loom</u> <u>Cancel</u> コグイン(管理者が無効





# 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:

	Login Device - VP50	GIRONKEY .
<ol> <li>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。</li> </ol>	User Password	8) m
<ol> <li>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)</li> </ol>	Password O Hint Contact Information Reset Device	
<ol> <li>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。</li> </ol>	□ Read-Only Mode ● 図 5.4 - Read-Only Mode [読み取り専	Looin Cancel 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/VP50C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/VP50C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 デバイスの動作 (間違ったパスワードを 10 回)	データの消去および デバイスのリセッ ト ?
ユーザーパスワード	パスワードがロックされます。管理者また 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 単一のユーザー、単一のパ スワード (管理者/ユーザーが NOT な 場合)	総当たり攻撃防止 デバイスの動作 (間違ったパスワードを 10 回)	データの消去および デバイスのリセッ ト ?
ユーザーパスワード	ドライブを暗号化消去します。パスワー ド、設定、およびデータが永久に消去されま す。	はい

\* デバイスの認証に一回成功すると、使用したログイン方式に関するログイン失敗回数がゼロにリセット されます。暗号化消去とは、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/VP50C 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)

デバイスヘ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。

<ul> <li>デバイスヘ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)</li> </ul>	して 「日本」の 10:20 AM 3/25/2022 図 6.1 - タスクバーの IronKey アイコン
<ul> <li>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)</li> </ul>	<ul> <li>VP50 Settings</li> <li>Browse VP50</li> <li>Format VP50</li> <li>Online Support</li> <li>About VP50</li> </ul>
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。	<ul> <li>         O Shut down VP50         <ul> <li></li></ul></li></ul>

# デバイスの各種オプション-(macOS環境の場合)





# デバイスオプション

VP50の設定:	<ul> <li>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/VP50Cの設定」セクションにあります。)</li> </ul>
VP50の表示:	<ul> <li>保護下のファイルを表示できます。</li> </ul>
<ul> <li>VP50 のフォーマット:</li> <li>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)</li> <li>注:フォーマットにはパスワード認証が必要です。</li> </ul>	Login Device - VP50 User Password   Warning!  Formatting will erase ALL data on your encrypted drive. All data will be lost forever. Are you sure you want to proceed?  Ves Cancel
オンラインサポート :	OX       Cancel         図 6.1 - VP50/VP50C のフォーマット         ・ インターネット・ブラウザを開いて http://www.kingston.com/support         いサポート情報にアクセスできます。
<b>VP50 の詳細情報:</b> 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/VP50C に ついて詳しく説明します。( <b>図 6.2</b> )	About - VP50 GIRONKEY' ~ () About © 2022 Kingston Technology Corporation.
<b>注</b> :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。	Modules         Version         Information           IKVP50         IKVP50         002324B53023B63190000062           Application         01.06.10           Crypto Library FW         1.00
VP50 のシャットダウン:	<ul> <li>VP50/VP50C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。</li> </ul>





# VP50/VP50C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
  - o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)
  - o一回限りの回復パスワードの有効化
  - o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。

Admin Settings	(S)   []]	Admin Settings	(S) [ [ ]
Pasaword Contact Into L	Admin Options	Password Contact Into	Language Americ Options
Convent Pixeward		Count Research	
Please create a secure Complex password follow	ving the criteria bolow.	Please create a secure Complex password fol	pering the criteria bolow.
New Password		New Password	
Contiline New Password			
15-16 long		Continent New Password	
uppercese lawercese digit si	sector character	6-16 long	
Datasured Islan T		uppercese towercese agit	abeces coaracter
( province of proving		Prinnward Print T	
<b>_</b>	one Apply Cancel		Done Apply Cancel
	1. 19-1-1-2 (- ) (1		
図 7.1 - Password [パス	9-[\$]997]	図 7.2 – Contact In	io [連絡先情報]
図 7.1 - Password [パス		🗵 7.2 – Contact Inf	io [連絡先情報]
図 7.1 - Password [パス Settings - VP50	GIRONKEY -	Settings - VP50	o [連絡先情報] ⊖IRONKEY
図 7.1 - Password [パス settings - VP50 の Admin Settings	GIRONKEY -	Settings - VP50	io [連絡先情報]
図 7.1 - Password パス Settings - VP50 の Admin Settings Proswerd Contact Inter 1		Settings - VP50 O Admin Settings Proved Contact Info	to [連絡先情報]
図 7.1 - Password パス Settings - VP50 Admin Settings Possword Contact Inter L	GIRONKEY" v	Settings - VP50 O Admin Settings Prevend Consult Info	to [連絡先情報]
図 7.1 - Password パス Settings - VP50 Admin Settings Passward Cantact Infle	GIRONKEY" v	Settings - VP50     Admin Settings     Password Contact Info      Password Contact Info      Password Contact Info      Password Depone	to [連絡先情報]
図 7.1 - Password パス Settings - VP50 の Admin Settings Perswerd Contact Inter u What is your preferred Language?	GIRONKEY" -	Settings - VP50     Admin Settings     Prevend     Contact Infe      Cont	to [連絡先情報]
図 7.1 - Password パネ Settings - VP50 O Admin Settings Passward Contact lette I What is your preferred Language? English	Admin Dytons	Settings - VP50 Admin Settings Personnel Contact Info Personnel Contact Info Personnel User Password below Personnel Contact Info	to [連絡先情報]
図 7.1 - Password パネ Settings - VP50 O Admin Settings Passward Contact lette u What is your preferred Language? English	anguage Admin Disters	Settings - VP50 Contact Info Settings Pietwood Contact Info	to [連絡先情報]
図 7.1 - Password パネ Settings - VP50 O Admin Settings Passward Contact lette L What is your preferred Language? English	anguage Admin Disters	Settings - VP50 Contact Info Settings Piezwood Contact Info Piezwood Contact Info Piezwood Contact Info Piezwood Contact Info Piezwood Ext6 long	to [連絡先情報]
図 7.1 - Password パネ	anguage Admin Dipters	Settings - VP50 Contact Info Settings Provide Contact Info Provide Contact Info Provide Contact Info Provide Contact Info Settings Uppercass Info Info Info Info Info Info Info Info	to [連絡先情報]
図 7.1 - Password パネ	anguage Admin Dytens	Settings - VP50 C Admin Settings Prevend Contact Info Prease enter a new User Password below. Password Costime Plasword Srife long uppercass (owarcase big) Cone-Time Recovery Password	to [連絡先情報]
図 7.1 - Password パネ	Admin Delens	Settings - VP50  Admin Settings  Prissword  Consuct Info  Prissword  Consuct Info  Prissword  Contract Info  Contra	to [連絡先情報]
図 7.1 - Password パネ iettings - VP50 う Admin Settings Perswerd Centert Inte What is your preferred Language? English	angulage Admin Detfors	Settings - VP50 C Admin Settings Password Contact Info Please enter a new User Password below Password Confirm PAssword S+56 long uppercase (otwarcase might Cone-Time Recovery Password Force Read-Only User Data C Login Password R	to [連絡先情報] G IRONKEY Solution Solutio





# VP50/VP50C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:	Settings - VP50	GIRONKEY -
自分のユーサーバスリードやヒントを	Admin Settings	
変更でさまり。(凶17.5)	Password Contact Info	Language Admin Options
	What is your preferred Language?	
	English	$\overline{\bigcirc}$
	図 7.5 - パスワードでのオプション(	Donc Aprily Cancel 管理者が有効な場合: ユーザーロク
<b>古</b> 彼 丹 唐 却	イン)	
<b>里給允惰報:</b> 東絃生情報を追加/妻子/亦軍できま	Settings - VP50	GIRONKEY 🗸
連絡先情報を追加/表示/変更できま す。( <i>図 7.6</i> )	User Settings Password Consecting Plense enter your information.bridow. Namu Completing Dennils	
	図 7.6 - 連絡先情報(管理者が有る	Done Apply Cancel めな場合: ユーザーログイン)
<b>言語:</b> 現在の言語選択の変更ができます。 ( <i>図</i> 7.7)	Settings - VP50	GIRONKEY .
	O User Settings Password Consultation What is your preferred Language? English	Language
	図7.7-言語の設定(管理者が有る	めな場合:ユーザーログイン)





### VP50/VP50C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/VP50C 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/VP50C 設定にアクセスできません。

### 設定の変更および保存

	Settings - VP50	
<ul> <li>VP50/VP50C 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)</li> </ul>	Settings - VP50 C Admin Settings Password Please enter your password © 💷 What I France OK	GIRONKEY . ~
	Done Ap 2010 2011 - VP50/VP50C 設定の変更を保存するための	w Cancel 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/VP50C 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:	Settings - VP50	BIRONKEY -
Admin Settings [管理者オプション] メニューで	Admin Settings	
ユーザーパスワードを手操作で変更します。	Password Contact Into Language Adm	n Qations
すぐに変更でき、次のユーザーログインで有	Biogrammatics a mana Litrary Basebasond Andreas	_
効になります。(図 8.1)	Password	)
	Gonfirm Pataward	1
注:パスワード要件基準は、初期化プロセス	5-16 long	
で設定された元々の基準に戻されます(複雑	uppercase lowwrcase digit special character	
なパスワードまたはパスフレーズパスワー	Une-time vectovery rassword	
ド)。	Force Read-Only User Data  C Login Password Reset	
	Done Apply	Cancel
	図 8.1 – Admin Settings [管理者オプション]/ユー のリセット	-ザーパスワード
ログインパスワードのリセット:	Settings - VP50	BIRONKEY .
ログインパスワードリセットを有効にする	Admin Settings	@   m
と、ユーザーは強制的に、管理者の設定し	Pristword Contact Into Language Ada	nin Onlians
た一時パスワードでログインし、好きなパ	And and a second se	
スワードに変更するように求められます。	Pieaswenter a new User Password below, Password	C
これは、ドライブを他の人用に譲る場合に	Confirm Reseword	
便利です。(図 8.2A および 8.2B を参照し	6-16 long	
てください)	uppercase lowercase digit special character	
	One-Time Recovery Password	
	Force Read-Only User Data      Login Password Reset	
	Done Apply	Cancel
	図 8 2A - Login Password Poset [ロガインパスロ	ードのリセット
	ばのこれーLogin Password Reset[ロノイマハハノ ボタン	[009 [09 [1]]
	Logia Device - VP50	
	A liser Descurred	
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	Victorie hostword reset	
ます。パスワード要件基準は、初期化プロ	The Admin has required that you repair your partwards	
セス中に設定された元々のオプションに従	eee Proceed to crente a new password.	$\square$
って自動的に適用されます(複雑なパスワ	OHin	
ードまたはパスフレーズパスワード)。	Contact	
	Read-Only Mode 1	
	Login	Cancel
	図 8 28 - ユーザーパスロードの入力後の通	知のリセット
		AHV) ソ ピ ツ 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	for the second s	Currenting
	Settings - VP50	GINONKEY.
ステップ1:一回限りの回復パスワード機	Admin Settings	@   III
能け非常に便利ですこれはユーザーパ	Password Contact Into Language	Admin Options
スワードを忘れた場合に回復してリセット	Dinaro onter a musi l'iror Destaured beleva	
イン 下を心むに物日に回復してリビット	Password	
りるために、 回たり使用可能なババク	Confirm Password	
下 C y 。 よ y 取 忉 に、 官 哇 伯 オ ノ ジ ヨ ン ハ ニ 、 、 ご One Time Decevery Deceverd [ 」 回	5-16 long	
ーユー ( One-Time Recovery Password [一回 阻 h の 回復 パフロ、 ビリギ クン た クリ ック	uppercase lowercase digit special chara	cter
限りの回復ハスワート] ホタンをクリック	One-Time Recovery Password	
しまり。 (凶 8.4)	Force Read-Only User Data 1 Cogin Password Reset	
	Done	Apply Cancel
	図 8.4 - One-Time Recovery Password[一回限	とりの回復パスワード]ホ
	図 8.4 - One-Time Recovery Password[一回际 タン	とりの回復パスリード]ホ
	図 8.4 - One-Time Recovery Password[一回隊 タン	もりの回復パスリート]ホ
	図 8.4 - One-Time Recovery Password[一回际 タン	もりの回復パスリード]ホ
<b>フニップ2・</b> デバノフが知知記会された味	図 8.4 - One-Time Recovery Password[一回际 タン	GIRONKEY ~
ステップ2:デバイスが初期設定された時	図 8.4 - One-Time Recovery Password[一回际 タン Settings - VP50 分 One-Time Recovery Password	
<b>ステップ2</b> :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、 <b>One</b> -	図 8.4 - One-Time Recovery Password[一回际 タン Settings - VP50 One-Time Recovery Password	EUの回復バスリード]ホ GIRONKEY → ⊚I □
<b>ステップ2</b> :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	図 8.4 - One-Time Recovery Password[一回隊 タン Settings - VP50 One-Time Recovery Password Please create a secure Complex password following the complex pas	GIRONKEY ~ ©I回
<b>ステップ2</b> :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	図 8.4 - One-Time Recovery Password[一回际 タン Settings - VP50 Please create a secure Complex password following the complex pa	E U O 回復バスリード]ホ C IRONKEY ~ © 回 riteria below:
<b>ステップ2</b> : 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)。	図 8.4 - One-Time Recovery Password[一回际 タン Settings - VP50 ● One-Time Recovery Password Please create a secure Complex password following the c [Admin Password Recovery Password	E U の回復パスリード]ホ C IRONKEY ~ © IIII itteria below
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)。	図 8.4 - One-Time Recovery Password[一回原 タン Settings - VP50 @ One-Time Recovery Password Please create a secure Complex paseword following the of Admin Password (Recovery Password Confirm Recovery Password	EU の回復パスリード]ホ GIRONKEY ~ ©IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
<ul> <li>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)。</li> <li>注:変更の適用には、管理者パスワードが</li> </ul>	図 8.4 - One-Time Recovery Password[一回原 タン Settings - VP50 Please create a secure Complex password following the co Please create a secure Complex password following the co Please create a secure Complex password following the co Please create a secure Complex password following the co Confirm Recovery Password Confirm Recovery Password 6-16 long	E U の回復パスリード]ホ C IRONKEY ~ (Iteria below)
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)。 注:変更の適用には、管理者パスワードが 必要になります。	図 8.4 - One-Time Recovery Password [一回际 タン Settings - VP50 ● One-Time Recovery Password Please create a secure Complex password following the co [Adoms Password Recovery Password Confirm Recovery Passwo	E U の回復パスリード]ホ @ III reter
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)。 注:変更の適用には、管理者パスワードが 必要になります。	図 8.4 - One-Time Recovery Password[一回隊 タン Settings - VP50 @ One-Time Recovery Password Please create a secure Complex paseword following the of Admin Password Recovery Password Recovery Password Confirm Recovery Password @ 16 long uppercase lowerchie digit special chemical	E U の回復パスリード]ホ C IRONKEY ~ © IIII Http://a bolow:
<ul> <li>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)。</li> <li>注:変更の適用には、管理者パスワードが 必要になります。</li> </ul>	図 8.4 - One-Time Recovery Password [一回际 タン Settings - VP50 Please create a secure Complex password following the co Please create a secure Complex password following the co Confirm Recovery Password Confirm Recovery Password Confirm Recovery Password experies lowercase digit epecial cha	E 9 の回復パスリード]ホ @ IRONKEY ~ @ IIII rector
<ul> <li>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)。</li> <li>注:変更の適用には、管理者パスワードが 必要になります。</li> </ul>	図 8.4 - One-Time Recovery Password [一回际 タン Settings - VP50 Please create a secure Complex password following the c [Admin: Password Recovery Password Confirm Recovery Password Confirm Recovery Password Confirm Recovery Password Back	E U O 回復パスリード]ホ C IRONKEY 、 ® III rector Save Cancel
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)。 注:変更の適用には、管理者パスワードが 必要になります。	図 8.4 - One-Time Recovery Password [一回际 タン Settings - VP50 ● One-Time Recovery Password Please create a secure Complex password following the c (Admin Password Recovery Password Confirm Recovery Password Confirm Recovery Password Bock 8.5 - One-Time Recovery Password [一同场	GIRONKEY ~ ©IIII (Cancel) Sove Cancel ひの回復パスワード1の





# 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。	Login Device - VP50	GIRONKEY V
	A User Password	@[B
	O Hist	ra Logn is Amir
	C Read-Only Mode	
	図 8 6 Recovery Password [[	Login Cancel 回復パスワード1ボタン
ステップ2:回復パスワードの入力と新規	Login Device - VP50	GIRONKEY .
ユーザーパスワードの作成が可能な時に	Recovery Password	®   =
よ、回復ハスワード 画面か表示されま す。(図 8.7)	Freezwary Password	
	Please create a secure password following the p New User Password	teria below.
<b>国要:</b> 一回限りの回復パスワードでは、ロ ブインの失敗回数を追跡する組み込みセキ	Confirm New User Password	
ユリティ機能を活用できます。一回限り	uppercase lowercase digit	special character
の回復パスワードを間違えてログインに 0回失敗すると、パスワードは無効にな	Pulasiwanti Hiint?	
り、ドライブに管理者としてログインして		Next
冉度有効にする必要があります。(詳しく ┃ ±18 および 30 ページを参照してくださ ┃		
	図 8.7 Recovery Password[回	復パスワード] メニュー
	Login Device - VP50	GIRONKEY -
ステップ3:成功すると、ユーザーパスワ - ド画面に戻ります。Recovery Password	Cuser 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)	Fassward	
	D Hint	
	Contact Information Login es Admos	
	C Read-Only Mode	
		Login Cancel




## 管理者の機能

## 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。

<ul> <li>ユーザーデータに対して、強制的な</li> </ul>	Settings - VP50	GIRONKEY V
<ul> <li>ユーザーテータに対して、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)</li> <li>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。</li> </ul>	Settings - VP50  Comparings  Pessword Comparing Pessword Comparing Pessword Committine Password Committine Password Committine Password Committine Password Committine Password Force Read-Only User Data Committine Com Statement of Comparing Com	GIRONKEY v (G) (C) (C) (C) (C) (C) (C) (C) (C) (C) (C
<ul> <li>一旦有効にすると、Read-Only Mode</li> <li>[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)</li> </ul>	り専用にする]を (変更の適用には、管理者パスリ Login Device - VP50 User Password (Pessicon O Hint Contact Information Login as Admin Read-Only Mode 図 8.10 - 読み取り専用モードがユーザ り管理者のみが集	有効にする フードが必要になります)



#### デバイスのロック

VP50/VP50C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。

	Login Device - VP50	GIRONKEY ~
<ul> <li>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)</li> </ul>	User Password  PAssword  PAssword  PAssword  O Hint  Contact Information Reset Device  Contact Information Contact Informati Contact Information	© (
	図 9.1 - パスワードが間違っている場合(	のメッセージ
	Login Device - VP50	GIRONKEY'
<ul> <li>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)</li> </ul>	PASSWORD IS INCORRECT YOU HAVE 3 MORE ATTEMPTS LEFTI  PASSWORD IS INCORRECT YOU HAVE 3 MORE ATTEMPTS LEFTI  PASSWORD O Hint  Reset Device  Back  I S  9.2 - 7 回パスワードを間違えた場合の	Cancel Dメッセージ

#### 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、<u>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</u> 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。



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/VP50C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/VP50C 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。





#### 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/VP50C 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<u>無効</u>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)

<ul> <li>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</li> </ul>	Login Device - VP50 GIRONKEY ~
のプライバシーを保護するために、 VP50/VP50C 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。*	
<ul> <li>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)</li> </ul>	Login Device - VP50       G IRONKEY         I User Password       Image: Stand
<ul> <li>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。</li> </ul>	Dリセシト Login Device - VP50 Admin Password Reset Device In order to protect data privacy, your VP50 will be formatted and ail data will be erased. Do you want to enter a new password and format your drive now? O Hin Ress OK Cancel Back Login Cancel
	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/VP50C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/VP50C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/VP50C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。



この例で言えば(図 9.10)、VP50/VP50C 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/VP50C 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/VP50C 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: 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。	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. 
ファイルまたはフォルダをコピーできません: 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。	Error Copying File or Folder Cannot copy File1: The disk is write-protected. Remove the write-protection or use another disk. OK 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: 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。	Error Deleting File or Folder       ×         Cannot delete File1: The disk is write-protected.         Remove the write-protection or use another disk.         OK         OK         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/VP50C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<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 加密 USB 3.2 Gen 1 闪存盘

用户指南







## 目录

简介	
Vault Privacv 50 功能	
关于本手册	4
系统要求	4
建议	5
₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	<b>5</b>
使用提醒	
家和设置最佳灾跌	
	0
设置我的设备	7
没重我的发展。 没久访问(Windows 环语)	, , , , , , , , , , , , , , , , ,
设备访问(Windows 冲亮) 	
以田切问(IIIacOS 冲克)	
设备初始化(Windows 和 macOS 环境)	8
家和选择	۵
山时起于····································	
应3y,谜面	
面吗可见住切厌	
官理贝密屿和用户密码 呼互信自	
<b>坎</b> 余恒ā	14
设久使田(Windows 和 macOS 环境)	16
文音文九 (Willows 和 Illacos 小境)	
官理贝和用厂的豆浆(官理贝口应用)	
仅用尸犊八豆求(官理贝木后用)	
住只误快式下胜坝	
泰刀攻击防护	
<b>访问</b> 我的女生义件	
<b>扒友</b> 选商	10
又金匹坝	19
NBEO/NBEOC 投留	21
₩P50/₩P50C 以且 答册日边罢	
日理贝以且	
用厂 <b>双直:</b> 目埋火山加用	
用尸叹直: 官理贝木后用	
史以和休存 VP50/VP50C 反直	
<b>帶田島市能</b>	25
<b>日理贝功能</b>	
用厂面吗里 <u>且</u>	
豆状雷屿里直(用/雷屿/	
一伏性恢复窑屿	
四则 只	
邦旪和步陪排险	20
マッキャンション ション ション ション ション ション ション ション ション ション	
VF30/ VF30C	
VF3U/ VF3UL 以宙里直	
池90命与1T天 、₩IIIUUWS1採目が近/ 建理源自	
<b>坩</b> 伏 们 心	







📕 KINGS

图 1: IronKey VP50

图 2: IronKey VP50C

## 简介

Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C 系列还符合 TAA 规范,并在美国组装。VP50/VP50C 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/VP50C 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/VP50C 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/VP50C,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/VP50C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 50/50C (VP50/VP50C),基于没有实施定制的出厂映像。

#### 系统要求

PC 平台           • Intel、AMD 和 Apple M1 SOC           • 15MB 可用磁盘空间           • 可用的 USB 2.0 - 3.2 接口           • 在最后一个物理驱动器之后有两个连续的 驱动器号*	PC 操作系统支持 • Windows 11 • Windows 10 • Windows 8.1
*注意:参见第 32 页的"驱动器号冲突"。	
Mac 平台	Mac 操作系统支持
<ul> <li>15MB可用磁盘空间</li> <li>USB 2.0 - 3.2 接口</li> </ul>	• macOS 11.x – 14.x





## 建议

为了确保 VP50/VP50C 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/VP50C 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。



## 使用正确的文件系统

IronKey VP50/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C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/VP50C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/VP50C 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/VP50C 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)	Installing device driver software * × Click here for status. 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)	DVD RW Drive (E:) IronKey Unlocker <sup>0</sup> bytes free of 122 MB CDFS CDFS CDFS CDFS CDFS
<ul> <li>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:)。</li> </ul>	Licenses WINDOWS AUTORUN.INF G IronKey.exe 图 3.2 - "文件资源管理器"窗口/IronKey.exe

#### 设备访问(macOS 环境)

将 VP50/VP50C 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。		IRONKEY	88 \$	000 ~ » Q
•	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。	IRONKEY	IRONKEY	IRONKEY.exe	Windows
			图 3.3 - IKV	'P 卷	





## 设备初始化(Windows 和 macOS 环境)

## 语言和 EULA

	Device Initialization - VP50 GIRONKEY v
从下拉采单中选择偏好的语言,升单击下一步(Next)。(参见图 4.1)	🖫 Language
	What is your preferred Language? English
	Next Cancel 图 4.1 - 语言选择
阅读许可协议并单击 <b>下一步 (Next)</b> 。	Device Initialization - VP50 CIRONKEY ~
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)	THIS SOFTWARE LICENSE AGREEMENT ("Agreement") is a legal agreement between you (either an individual or a single entity) and Kingston Technology Company Inc. ("Kingston"). This Agreement relates to the software accompanying this Agreement, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (the "Licensed Software"). By downloading, Installing, copying, or otherwise using the Licensed Software, you agree to be bound by the terms of this Agreement and further agree that the third party licensors of Kingston providing licenses for all or any portion of the Licensed Software shall be third party beneficiaries of this Agreement. If you do not agree to the terms of this Agreement, do not install, copy or use the Licensed Software.
	The Licensed Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Licensed Software is licensed, not sold. The Licensed Software is being provided solely for use with IronKey Encrypted USB product lines.
	Back Next Cancel 图 4.2 - 许可协议





#### 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/VP50C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	Device Initialization - VP50
<ul> <li>密码必须包含 6 个或更多字符(最多 16 个字符)。</li> <li>必须满足以下三(3) 个条件: <ul> <li>大写</li> <li>小写</li> <li>数字</li> <li>特殊字符(!、\$、&amp;等)</li> </ul> </li> </ul>	Password  Complex Password  Complex Password  Confirm Password  Confirm Password  Confirm Password  G-16 long  uppercase lowercase digit special character  Password Hint?  Enable Admin and User Passwords
	Back Next Cancel
	图 4.3 - 复杂密码
	Device Initialization - VP50 GIRONKEY V
<ul> <li>必须包含:</li> </ul>	A Password (a) 📖
<ul> <li>最少 10 个字符</li> <li>最多 64 个字符</li> </ul>	Catriplex: Passphrase Please create a secure Plassphrase assived following the briteria below. Please create a secure Plassphrase assived following the briteria below. Please create a secure Plassphrase assived following the briteria below. Please create a secure Plassphrase assived following the briteria below. Please create a secure Plassphrase assived following the briteria below. Please create a secure Plassphrase assived following the briteria below. Please create a secure Plassphrase assived following the briteria below. Please create a secure Plassphrase assived following the briteria below. Please create assive cre
	Back Cancel
	图 4.4 - 口令密码
密码提示(可选)	
密码提示在忘记密码时很有用,它可以提供	
有关密码的线索。	Password Hint?
<b>注意</b> :提示内容 <b>不得</b> 与密码完全相同。	图 4.5 - "密码提示"字段





## 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)

evice Initialization - VP50 GIRON	IKEY V Device	Initialization - VP50	GIRONK
Password	Pa	ssword	0
Complex Passphrase		Complex Passphrase	
Please create a secure Complex password following the criteria below.		Please create a secure Complex password following the criteria below	N. 🕜
ExamplePassw0rd!		ExamplePassw0rd	
ExamplePassw0Rd		ExamplePassw0rd	
✓ 6-16 long		~ 6-16 long	_
✓ uppercase → lowercase → digit → special character		Puppercase Plowercase Pidign special character	
Password Hint?		Password Hint?	
		Buch Hone	Gancer
图 4.6a - 已满足复杂密码条件		图 4.6b - 复杂密码条件可选	
图 4.6a - 已满足复杂密码条件		图 4.6b - 复杂密码条件可选 wice Initialization - VP50 GIR	ONKEY. V
图 4.6a - 已满足复杂密码条件		图 4.6b - 复杂密码条件可选 evice Initialization - VP50	onkey. ↓
<b>图 4.6a - 已满足复杂密码条件</b> 于 <b>无效</b> 密码,密码条件框会以 <mark>红色</mark> 高亮显	显示,	图 4.6b - 复杂密码条件可选 evice Initialization - VP50	ONKEY. V
图 4.6a - 已满足复杂密码条件 于无效密码,密码条件框会以红色高亮。 一步 (Next) 按钮会在满足最低要求前被停	显示,	图 4.6b - 复杂密码条件可选 wice Initialization - VP50	onkey. ↓
图 4.6a - 已满足复杂密码条件 于无效密码,密码条件框会以红色高亮员 一步 (Next) 按钮会在满足最低要求前被停	显示, 序用。	图 4.6b - 复杂密码条件可选 evice Initialization - VP50	onkey' ↓ ⊛ ₪
图 4.6a - 已满足复杂密码条件 于无效密码,密码条件框会以红色高亮显 一步 (Next) 按钮会在满足最低要求前被停 适用于复杂密码和口令密码。	显示, 序用。	图 4.6b - 复杂密码条件可选 evice Initialization - VP50	ONKEY. V
图 4.6a - 已满足复杂密码条件 于无效密码,密码条件框会以红色高亮显 一步 (Next) 按钮会在满足最低要求前被停 适用于复杂密码和口令密码。	显示, 序用。	图 4.6b - 复杂密码条件可选 evice Initialization - VP50	ONKEY. ↓
<b>图 4.6a - 已满足复杂密码条件</b> 于 <b>无效</b> 密码,密码条件框会以 <b>红色</b> 高亮5 <b>一步 (Next)</b> 按钮会在满足最低要求前被停 适用于复杂密码和口令密码。	显示, 序用。	图 4.6b - 复杂密码条件可选 wice Initialization - VP50	onkey. ↓
<b>图 4.6a - 已满足复杂密码条件</b> 于 <b>无效</b> 密码,密码条件框会以 <b>红色</b> 高亮5 <b>一步 (Next)</b> 按钮会在满足最低要求前被停 适用于复杂密码和口令密码。	显示, 序用。	图 4.6b - 复杂密码条件可选 evice Initialization - VP50	ONKEY V
图 4.6a - 已满足复杂密码条件 于无效密码,密码条件框会以红色高亮5 一步 (Next) 按钮会在满足最低要求前被停 适用于复杂密码和口令密码。	显示, 序用。	图 4.6b - 复杂密码条件可选 evice Initialization - VP50	ONKEY' V
图 4.6a - 已满足复杂密码条件 于无效密码,密码条件框会以 <b>红色</b> 高亮5 <b>一步 (Next)</b> 按钮会在满足最低要求前被停 适用于复杂密码和口令密码。	显示, 序用。	图 4.6b - 复杂密码条件可选 evice Initialization - VP50	ONKEY V





## 虚拟键盘

VP50/VP50C 配备虚拟键盘,可防范按键记录程序。

	Device Initialization - VP50 GIRONKEY ~
● 要利用 <b>虚拟键盘</b> ,在 <b>设备初始化</b> (Device	A Password 🐵 🔳
Initialization) 屏幕的右上角找到键盘按钮,并选择该按钮。	Complex Passphrase Please create a secure Passphrase following the criteria below. (This is my Passw0rd Examplet
	(This is my Password Example!
	(Plassword Hint?
	C Enable Admin and User Passwords 🕤
	Back Next Cancel
	图 4.8 - 激活虚拟键盘
<ul> <li>一旦虚拟键盘出现,您还可以启用<b>屏幕记录器</b> 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。</li> <li>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。</li> </ul>	Virtual Keyboard       1234567890-= ②         9 w e r t y u i o p [] \       a s d f g h j k l ; ' return         shift z x c v b n m , . / shift       caps lock         randomize       2         B 4.9 - 屏幕记录器保护 / 随机排列





## 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"。

	Device Initialization - VP50 GIRONKEY
	🔒 Password
要隐藏密码字符串,请单击灰色图标。	Complex Passphrase
(	Please create a secure Passphrase password following the criteria below.
$\odot$	This is my Passw0Rd Eample!
	This is my PasswORd Eample
	✓ 10 characters minimum
	(Password Hint?
	Enable Admin and User Passwords 1
	Back Next Cancel
	图 4.10 - 切换为"隐藏"密码
	Device Initialization - VP50 GIRONKEY
	A Password
	Complex Passphrase
要显示隐藏的密码,请甲击监色图标。	Please create a secure Passphrase password following to criteria below.
(]	
<u> </u>	
	✓ 10 characters minimum
	Password Hint?
	Enable Admin and User Passwords (
	Back Next Cancel
	图 4.11 - 切换为"显示"密码





#### 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<u>启用</u>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。

		Device Initialization - VP50	GIRONKEY .
●	要启用 <b>管理员密码和用户密码</b> ,请单击 <b>启</b>	Password	® =
月 a 交	日曾埵负密码和用户密码 (Enable Admin nd User passwords) 旁的框,并在选定有 牧密码后选择下一步 (Next)。(图 4.12)	Complex Passpir Please create a secure Passpirase password	trase
• 女 窖 全 止	口果该功能已启用,那么本屏幕中的所选 否码是 <b>管理员密码</b> 。单击下一步 (Next), 会转到用户密码 (User Password) 屏幕,在 七可为用户选择密码。	••••••••     • 10 characters minimum,     Pressword Hint ?      • Enable Admin and User Passwords	ack Next Cancel
		图 4.12 - 启用管理员智	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)。





## 管理员密码和用户密码

	Device Initialization - VP50	GIRONKEY
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)	Please create a secure Passphrase password following the Pressword  Continue Password  10 characters minimum  Pleaseword Hint7	
	Require password reset on next login     Back	Next Cancel
	图 4.13 - 用户密码(管理员和用户	9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	Login Device - VP50	GIRONKEY ~
	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 程中设定的收时密码, 就后在使用收	User Password     Reguire password reset	0
	程中设定的临时盈码,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)	The Admin has required that you reset your password please proceed to create a new password.     Hin     Contact	
	<b>注意:</b> 出于安全考虑,新密码不能与	Read-Only Mode	
	临时密码相同。	图 4.14 - 要在下次登录时重置 (针对用户密码)	Login Cancel





## 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。)

	Device Initialization - VP50	GIRONKEY
<b>姓名 (Name)</b> 字段最多可包含 32 个 字符,但是不得包含 <b>完全匹配</b> 的密 码。	Contact	
<b>公司 (Company)</b> 字段最多可包含 32 个字符,但是不得包含 <b>完全匹配</b> 的 密码。	Details	
<b>详情 (Details)</b> 字段最多可包含 156 个字符,但是不得包含 <b>完全匹配</b> 的 密码。	Back	OK Cancel
	图 4.14 - 联系	言息

**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/VP50C 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)

Login Device - VP50	GIRONKEY .	Login Device - VP50	GIRONKEY
🔒 User Password	8 i 🖂	Admin Password	8 H
O Hint Contect Information.		Pessword D Hint Reset Device	
Read-Only Mode		Read-Only Mode	
图 5.1 - 用户密码登录(管理」	Login Cancel 员已启用)	图 5.2 - 管理员	Back Logn Cancel 员密码登录
仅用户模式登录(管理员未)	自用)	Login Dévice - VP50	⊖IRONKEY' →
如 <b>第 13 页</b> 所述,尽管建议使用 发挥设备的全部优势,但 IronKe 化为仅用户(单密码、单用户) 适合希望用简单的单密码方法仍 用户。(图 5.3)	管理员角色功能来 ey 设备也可以初始 配置。这个选项 最护闪存盘数据的	User Password  Password  O Hint  Contact Information Reset Device	@ ( )
注意: 要启用管理员密码和用户 置设备 (Reset Device) 按钮让闪 态,从而可以启用管理员密码和 设备后,闪存盘会被格式化,所 失。	P密码,请使用 <b>重</b> 存盘进入初始化状 可用户密码。 <b>重置</b> 所有数据都会丢	■ Read-Only Mode ●       图 5.3 - 用户密码登录	(管理员未启用)



## 设备使用



#### 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:

		Login Device - VP50	GIRONKEY .
1.	将设备插入主机计算机的 USB 接口, 并运行 <b>IronKey.exe</b> 。	User Password	@   m
2.	勾选密码输入框下方的 <b>只读模式</b> (Read-Only Mode)。(图 5.4)	(Phaseword O Hint	
3.	输入设备密码并单击 <b>登录 (Login)</b> 。 IronKey 现在会以只读模式解锁。	Contact Information Reset Device	
		Read-Only Mode 0	
			Login Cancel
		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/VP50C 并重新登录,同时取消勾选**只读模式 (Read-Only Mode)** 复选框。

**注意:** VP50/VP50C 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 设备行为 (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 单用户、单密码 (管理员 <b>/</b> 用户 <u>未</u> 启用)	暴力攻击防护 设备行为 (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 - <mark>您的数据会永久丢失。</mark>

#### 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/VP50C (Browse VP50/VP50C),您也可以 访问自己的文件。(图 6.2)

# GIRONKEY



## 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。



## 设备选项 - (macOS 环境)







## 设备选项

VP50 设置 (VP50/VP50C 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/VP50C 设置"部分。)		
浏览	• 让您可以查看安全文件。		
格式化 VP50/VP50C (Format VP50/VP50C): 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) 注意:格式化需要密码身份认证。	Login Device - VP50       @ IRONKEY"          User Password       @ III         Formatting will erase ALL data on your encrypted drive.       All data will be lost forever. Are you sure you want to proceed?         OH       K       Cancel         III       Ks       Cancel         IIIII       Ks       Cancel		
在线支持 (Online Support):	<ul> <li>打开互联网浏览器并导航至 <u>http://www.kingston.com/support</u>,您可以在这里获取 更多的支持信息。</li> </ul>		
<b>关于 VP50/VP50C (About VP50/VP50C):</b> 提供关于 VP50/VP50C 的详细信息,包括 应用、固件和序列号信息。( <b>图 6.2</b> ) <b>注意:</b> 闪存盘的唯一序列号位于"信 息"(Information)列下。	About - VP50       C IRONKEY" ~         About       • 2022 Kingston Technology Corporation.         Modules       Version         IKVP50       IKVP50         Application       10.00         FW Version       10.0540         Crypto Library FW       1.00         Edstart       Cose		
关闭 VP50/VP50C (Shut down VP50/VP50C):	• 正确关闭 VP50/VP50C,让您可以将其从系统中安全删除。		





## VP50/VP50C 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)
  - o更改用户密码
  - o 登录密码重置(用户密码)
  - o启用一次性恢复密码
  - o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。

Settings - VP50	GIRONKET	Settings - VP50	GIRONKET
O Admin Settings	(Q) (C)	@ Admin Settings	(s) i 💷
Passwerd Contact Info Language	Admin Options	Passwert Contact Info	Language Astern Options
Current Possword		Current Posteward	
Please create a secure Complex password following the criter	rla bolaw.	Please create a secure Complex password for	lowing the critienta bolow.
New Pataword		New Password	
Confirm New Password		Confirm New Password	
6-16 long		E 15 Jan	
uppercese lowercase algit special charac	:10+	uppercese lowercese digit	special character
(Prismward Plint)			and the second sec
		Printer Print	
Done	Apply Cancel		
			Done Apply Cancel
图 7.1 - 密码选项	ą	图 7.2 - 联	系信息
	GIDONKEY"	Settings - VP50	GIRONKEY
jettings - VP50	GIRONRET	Jeangs (FS)	
Admin Settings		Admin Settings	©) =
Password Contact Info Language	Admin Options	Presword Contact Into	Languager Admin.Optime
What is your preferred Language?		Please enter a new Usar Password below.	
Franke		Pasaword	
English		Coofirm Pässword	1
		5-16 long	
		uppercase (owercase digit	special character
		One-Time Recovery Password	
		C Force Read-Only User Data ( Login Password R	leset 🕦
Done	Apply Cancel		Done Apply Cancel





## VP50/VP50C 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):	Settings-VP50 GIRONKEY v	
□L芯可以更以目匚的用厂凿码种/ 实提 示 ( Ø 7 5 )	Admin Settings	
	Possward Contact Into Language Admin Options	
	What is your preferred Language?	
	English	
	Done Apply Cancel	
	图 7.5 - 密码选项(管理员已启用:用户登录)	
联系信息 (Contact Info)。	Settings - VP50 GIRONKEY' ~	ή.
让您可以添加/查看/更改自己的联系信	🗇 User Settings	
息。(图7.6)	Please enter your information bidow.	
	Namu	
	Company	
	Done Apply Cancel	
	图 7.6 - 联系信息(管理员已启用:用户登录)	
语言 (Language):	Settings - VP50 GIRONKEY ~	5
让您可以更改当前语言选择。(图	@ User Settings	
7.7)	Pasyword Contact 1000 Language	
	Manual Concentration of Concentration	
	what is your prevented Languager	
	English	
	Done Acoby Cancel	-)
	Dono Apply Cancel	2





## VP50/VP50C 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/VP50C 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**。<u>该配置无法访问任何管理员选项或功能。</u>该配置可以访问以下 VP50/VP50C 设置:

#### 更改和保存设置

	Settings - VP50	
<ul> <li>每当 VP50/VP50C 设置中的设置</li> <li>(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</li> </ul>	Admin Settings Password     Prease enter your password     What I	Intin Options
并应用更改。(参见图 7.11)	▲ CK	Y Cancel 答码提示"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/VP50C 设置菜单。





#### 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:

<ul> <li>用户密码重置:</li> <li>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)</li> <li>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)。</li> </ul>	Settings - VP50       @ IRONKEY *         ③ Admin Settings       @ IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
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)	Settings - VP50       @ IRONKEY ~         * Admin Settings       @ IRONKEY ~         * Piesworst consact ints insumpre insumpre insum Orisons       @ Ironsword         * Piesworst inter a new User Password below.       Pressworst         * Orienting Bassword       @ Ironker *         * Orienting Bassword       @ Ironker *         * Force Read-Only User Date *       @ Ironker *         * Done *       Apply         * B 8.2A - ** 登录密码重置"按钮
<b>注意:</b> 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。	Login Device - VP50       @ IRONKEY          O User Password       @ Require password reset         Image: The Admin has required that you reset your password:       @ Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:         Image: The Admin has required that you reset your password:       Image: The Admin has required that you reset your password:





## 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	Settings - VP50 GIRONKEY' ~
<b>第1步:</b> 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)	* Admin Settings       @ @         Pessword       Janguage       Admin Options         Pessword       @ @       @ @         Confirm Password       @ @       @ @         Fris long       uppercase       digit       special character         Uppercase       @ @       @ @       @ @       @         Force Read-Only User Data       @ @       Login Password Reset       @       Cancel         Doro       Apply       Cancel
<b>第3</b> • 使用恐久初始化时所恐宕的同一家	Settings - VP50 GIRONKEY · ·
<b>第2步:</b> 使用设备初始化的所设定的问一密码条件来创建一次性恢复密码(复杂或口令)。 <b>注意:</b> 应用更改需要提供管理员密码。	One-Time Recovery Password   Please create a secure Complex password following the criteria below.   Admits Possword   Recovery Password   Conflim Recovery Password   G-16 long   uppercess   lowerense   digit   special character
	Back Save Cancel Cancel 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	Login Device - VP50
Password) 登录屏幕中。单击 <b>恢复密码</b>	
	(Francisco)
	O Hint
	Contact Information Recovery Password Login as Admin
	图 86-"恢复遂码"按钮
第2步:恢复密码 (Recovery Password) 屏 莫今中现 你可以在此输入恢复家码并创建	Login Device - VP50 GIRONKEY ~
新的用户密码。(图 8.7)	Recovery Password
	Encouvery Posseword
<b>重要事项:</b> 一次性恢密码也会利用内置的	(New User Password -
女宝切能米跟踪天败的登求云试伏敛, <b>伊</b> 用 一次性恢复率码登录失败 10 次后该率码会	Confirm New User Password
被停用,必须以管理员身份登录后进行重新	onto long uppercase lowercase digit special character
启用。(参见第18页和第30页,了解更多	Polassward Hild?
详情)	
	Next: Cancel
	图。一体气体刀并为
	图 8.7 - 次夏留码米平
	Login Device - VP50 GIRONKEY ~
<b>第3步:</b> 成功后,您会返回到 <b>用户密码</b>	A User Password
(User Password)	
输入的用户密码会变成新的用户密码。(图	
8.8)	Patsward
	Lontact mormation Login as kommu
	Read-Only Mode 🕤
	Login Cancel
	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。





#### 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	Settings - VP50 GIRONKEY ~
次单击此框和"应用"(Apply)。(图 8.9)	Admin Settings     Onnors Infa     Language     Admin Options
<b>注意</b> :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。	Please tenter a new User Password below:         Password         Conflime Password         Griffine Password         Griffine Password         One-Time Recovery Password         Porce Read-Only User Data ①         Login Password Reset ①         Done       Apply         Cancel         B 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)
<ul> <li>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 # 節 冊 号 億 円 わ 小</li> </ul>	Login Device - VP50 GIRONKEY' V GUSer Password GIE
且至做官埋贝停用为止。(图 <b>8.10</b> )	P#####001         • Hint         Contact Information       Login as Admin         • Read-Only Mode •         Login       Cancel    B 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/VP50C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。

<ul> <li>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)</li> </ul>	Login Device - VP50 GIRONKEY ~
	🔒 User Password 💿 📾
	PASSWORD IS INCORRECT Produvuld O Hint Contact Information Reset Device Read-Only Mode C Logic Concel
	Login Device - VP50
<ul> <li>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)</li> </ul>	Admin Password © Consect you have 3 MORE ATTEMPTS LEFT: Encources  O Hint  Reset Device
	Read-Only Mode  Read-Only Mode  Cancel  Cancel
	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<u>第18页</u>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:

Login Device - VP50	GIRONKEY.	Login Device - VP50	GIRONKEY
🔒 User Password	💿 i 🔊	Admin Password	@
Warning!		• Warningt	
The Inter Rescribed The maximum number (Figure 1) (Figure 1) (F	ror password gour VPSO is now & Admin or use the 0	Vou have reached d refutise. In order to p being formatted an use your drive again O Hin	
Contact		Rest	OK
Read-Only Mode 🗿		Read-Only Mode	
	Login Cancel		Back Looin Cancel
设备锁定	主 王	设	备格式化*
(图 9.3)	)		(图 9.4)
(图9.3) 一次性恢复密码: (管理	) 厘员/用户已启用)	用户密码	(图 <b>9.4</b> ) (管理员未启用)
(图 9.3) 一次性恢复密码: (管理 .ogin Device - VP50	) 里员/用户已启用) ⊖IRONKEY →	用户密码 Login Device - VP50	(图 9.4) (管理员未启用) ⊖IRONKEY
(图 9.3) 一次性恢复密码:(管理 Login Device - VP50 Recovery Password	) 里员/用户已启用) GIRONKEY ~	用户密码 Login Device - VP50	(图 9.4) (管理员未启用) @IRONKEY
(图 9.3) 一次性恢复密码: (管理 .ogin Device - VP50	) 里员/用户已启用) GIRONKEY ~ 》目	用户密码 Login Device - VP50 ● User Password ● Warning!	(图 9.4) (管理员未启用) GIRONKEY
(图 9.3) 一次性恢复密码:(管理 cogin Device - VP50 Recovery Password	) 里员/用户已启用) GIRONKEY → ©I■	用户密码 Login Device - VP50	(图 9.4) (管理员未启用) @IRONKEY @IRONKEY @IRONKEY
(图 9.3) <u>一次性恢复密码:(管理</u> uogin Device - VP50 ■ Recovery Password ● Marning: ● Warning: ● Warning:	A 型员/用户已启用) GIRONKEY → ◎ @ ■ * of allinverd So is move locked but user	用户密码 Login Device - VP50 ・ User Password  ・ Warning:  ・ Was have reached the period was applied and the period was applied and the period of the period of the period.	(图 9.4) (管理员未启用) @IRONKEY @IRONKEY @IRONKEY @IRONKEY @IRONKEY @IRONKEY @IRONKEY @IRONKEY
(图 9.3) <u>一次性恢复密码:(管理</u> Login Device - VP50 ■ Recovery Password ● Warning: ● Warning:	● 里员/用户已启用) @ IRONKEY ~ ◎ ■ of allowed 50 is new locked bit User	日戸密码 Login Device - VP50 User Password  User Password	(图 9.4) (管理员未启用) @IRONKEY @IRONKEY
(图 9.3) 一次性恢复密码: (管理 cogin Device - VP50 ■ Recovery Password ● Warning: ● Warning:	) 里员/用户已启用) @ IRONKEY ↓ ◎ ■ so is now locked the User	日戸密码 Login Device - VP50 User Password User Password Warning! Worker resched th Device - VP50 Warning! Worker resched th Device - VP50 Warning! Totals and	(图 9.4) (管理员未启用) @ironkey @ironkey @ironkey were attemp number of password over data will be obtained a data will be obtained when the operation completes.
(图 9.3) <u>一次性恢复密码:(管理</u> uogin Device - VP50 ■ Recovery Password ● Warning: ● Warning:	■ <u>更/用户已启用)</u> @ IRONKEY ~ @ III * of allowed So is new locked Dis new locked Next Cancel	日戸密码 Login Device - VP50 ひSer Password	(图 9.4) (管理员未启用) @IRONKEY @ emailmut number of password were data well be to by built and attes data well be not by our the attests when the operation completes.
(图 9.3) <u> 一次性恢复密码:(管理</u> sogin Device - VP50 ■ Recovery Password ● Warning: ● Warning	■ <u>最/用户已启用)</u> GIRONKEY → ©IRONKEY →	<b>日户密码</b> Login Device - VP50 ① User Password ② Visming: ③ Discr Context: ③ Ping Context: ③ Read-Only Mode ④	(图 9.4) (管理员未启用) @IRONKEY

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/VP50C,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/VP50C 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<u>未启用</u>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)

<ul> <li>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/VP50C 会被格式 化。这意味着在这个过程中所有数据会被 擦除。*</li> </ul>	Login Device - VP50       ③ IRONKEY *         Admin Password       ③ IRONKEY         ● Admin Password       ③ IRONKEY         ● Besc Only Mode ①       ① IRONKEY         ● Besc Only Mode ①       ① IRONKEY         ● Besc Only Mode ①       ① IRONKEY
<ul> <li>注意:单击"重置设备"(Reset Device)</li> <li>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</li> <li>2)单击"取消"(Cancel)以返回登录窗口。</li> <li>(参见图 9.8)</li> </ul>	Login Device - VP50       @ IRONKEY *         * User Password       @ III         · User Password       @ IIII         · User Password       @ IIIII         · User Password       @ IIIIII         · User Password       @ IIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIIII
<ul> <li>如果选择继续,会弹出"初始化"         <ul> <li>(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。</li> </ul> </li> </ul>	<form></form>




# 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/VP50C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/VP50C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/VP50C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。



在本例中(图 9.10), VP50/VP50C 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/VP50C 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/VP50C 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



**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/VP50C 并重新登录,在登录之前取消选中"只读模式"(Read-Only Mode)复选框。

Kingston



IRONKEY<sup>™</sup> Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 加密 USB 3.2 Gen 1 隨身碟

使用者指南







#### 內容

簡介	
Vault Privacy 50 特色	
關於本使用手冊	
系統需求	
建議	
使用正確的檔案系統	5
使用提醒	5
密碼設定的最佳做法	6
設定我的裝置	7
裝置存取 (Windows 環境)	7
裝置存取 (macOS 環境)	7
裝置使用 (Windows & macOS 環境)	8
密碼選擇	9
虛擬鍵盤	
密碼顯示切換	
管理員和使用者密碼	
聯絡資訊	
裝置使用 (Windows & macOS 環境)	
管理員和使用者的登入(管理員已啟用)	
供僅使用者模式登入 (管理員未啟用)	
在唯讀模式下解鎖	
暴力破解保護	
存取我的安全檔案	
計2日2月1月1日	10
农直迭頃	
VP50/VP50C 势完	21
答理目约定	21
641 実政に	
(C) (口) (口) (口) (口) (口) (口) (口) (口) (口) (口	22 در
愛文英語什 1430/1430C 改足	
管理員功能	25
<b>山田</b> 书 家 框 重 設	25
及↓ 宓碼重設 (適田於使田老宓碼)	25
·····································	26
入口(大)(因伍吗)····································	20
17111111111111111111111111111111111111	
說明與疑難排解	
VP50/VP50C 鎖定	
VP50/VP50C 裝置重設	
磁碟機代號衝突 (Windows 作業系統)	
錯誤訊息	









圖 1:IronKey VP50

圖 2:IronKey VP50C

# 簡介

Kingston IronKey Vault Privacy 50 (VP50)/Vault Privacy 50C (VP50C) 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/VP50C 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/VP50C 系列在保護資料方面表現更為優異。

VP50/VP50C 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」 I 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/VP50C 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/VP50C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 50/50C (VP50/VP50C), 係依據原廠影像且不含自訂配置。

### 系統需求

<ul> <li>電腦平台</li> <li>Intel, AMD &amp; Apple M1 SOC</li> <li>15 MB 可用硬碟空間</li> <li>可用的 USB 2.0 - 3.2 連接埠</li> <li>最後一個實體磁碟之後的兩個連續磁碟機 代號*</li> </ul>	電腦作業系統支援 <ul> <li>Windows 11</li> <li>Windows 10</li> <li>Windows 8.1</li> </ul>
*注意:請參閱第 32 頁「磁碟機代號衝突」。	
Mac 平台	Mac 作業系統支援
• 15 MB 可用硬碟空間	• macOS 11.x – 14.x
• USB 2.0 - 3.2 連接埠	





## 建議

為確保提供 VP50/VP50C 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/VP50C 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。



#### 使用正確的檔案系統

IronKey VP50/VP50C 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/VP50C 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:您的随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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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/VP50C 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。



### 裝置存取 (macOS 環境)

將 VP50/VP50C 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/VP50C (或 IRONKEY) 卷宗。(圖 3.3)

•	連按兩下 IronKey CD-ROM 圖示。		IRONKEY	88 ¢	000 ~ » Q	
•	接著連按兩下圖 3.3 顯示視窗中找到的 IKVP50/VP50C (或 IronKey.app)應用程式圖 示。以此開始初始化流程。	IRONKEY	RONKEY	IRONKEY.exe	Windows	
			圖 3.3 - IKVP	も宗		





# 裝置使用 (Windows & macOS 環境)

### 語言和 EULA

	Device Initialization - VP50 GIRONKEY ~
從卜拉式選單中選擇語言偏好,然後按一卜 「Next」(下一步)。(詳見圖 4.1)	📬 Language
	What is your preferred Language?
	Nex Cancel 圖 4.1 - 語言選項
	Device Initialization - VP50 GIRONKEY ~
檢閱授權合約然後按一下「Next」(下一步)。	License Agreement     SOFTWARE LICENSE AGREEMENT     IMPORTANT - READ CAREFULLY:
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)	THIS SOFTWARE LICENSE AGREEMENT ("Agreement") is a legal agreement between you (either an individual or a single entity) and Kingston Technology Company Inc. ("Kingston"). This Agreement relates to the software accompanying this Agreement, which includes computer software and may include associated media, printed materials, and "online" or electronic documentation (the "Ucensed Software"). By downloading, installing, copying, or otherwise using the Licensed Software, you agree to be bound by the terms of this Agreement and further agree that the third party licensors of Kingston providing licenses for all or any portion of the Licensed Software shall be third party beneficiaries of this Agreement. If you do not agree to the terms of this Agreement, do not install, copy or use the Licensed Software.
	The Licensed Software is protected by copyright laws and international copyright treaties, as well as other intellectual property laws and treaties. The Licensed Software is licensed, not sold. The Licensed Software is being provided solely for use with IronKey Encrypted USB product lines.
	Back Next Cancel
	圖 4.2 - 授權合約





#### 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/VP50C 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	Device Initialization - VP50 GIRONKEY -
• 必須包含 6 個以上的字元 (最多 16 個字	A Password
元)。	Complex Passphrase
	Please create a secure Complex password following the criteria below.
• 必須包含下列的二(3) 個條件·	
	6-16 long
	uppercase lowercase digit special character
○ 特殊字元 (!,\$,&, etc)	Enable Admin and User Passwords 🚺
	Back Next Cancel
	圖 4 3 - 複雜漆種
密碼片語密碼	
<ul> <li>● 必須包含:</li> </ul>	Password
<ul> <li>● 最少10個字元</li> </ul>	Complex Passphrase
o 最多 64 個字元	Please create a secure Passphraxe basaword following the briteria below.
	Password
	Confirm Research 1 10 doarsetins minimum
	(Pedawsbard Hans ?
	Enable Admin and User Passwords
	Back Divit Coocel
溶理提示 (非必避)	<b>盧 4.4 - </b> 密崎月
如 啊我 (小 () + 20 (云) 如 果 你 忘 記 家 碼 , 家 碼 提 示 可 提 世 右 關 家 碼	
内容的線索。	Password Hint?
注意:提示「不得」與密碼完全相符。	<b>圖 4.5</b> - 密碼提示欄位





### 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)

Device Initialization - VP50	Pevice mutanzation - AN20
A Password 💿 📼	Password @
Complex Passphrase	Complex Passphrase
Please create a secure Complex password following the criteria below.	Please create a secure Complex password following the criteria below.
ExamplePassw0rdl	ExamplePassw0rd
ExamplePassw0Rd	ExamplePassw0rd
✓ 6-16 long	~ 6-16 long
✓ uppercase	v uppercase v lowercase v digit special character
Password Hint?	Pässword Hint?
Enable Admin and User Passwords 👔	Enable Admin and User Passwords 🚯
Back Next Cancel	
	Back Next Cance
圖 4.6a - 複雜密碼條件符合	圖 4.6b - 非必須的複雜密碼條件
量 4.6a - 複雜密碼條件符合	圖 4.6b - 非必須的複雜密碼條件
圖 4.6a - 複雜密碼條件符合	圖 4.6b - 非必須的複雜密碼條件
圖 4.6a - 複雜密碼條件符合	圖 4.6b - 非必須的複雜密碼條件
<b>圖 4.6a - 複雜密碼條件符合</b>	圖 4.6b - 非必須的複雜密碼條件 Device Initialization - VP50 ● Password ● Imon Key:  ◆
<b>圖 4.6a - 複雜密碼條件符合</b> 果是 <b>無效的</b> 密碼,「密碼條件方塊」將會以 <mark>紅</mark>	圖 4.6b - 非必須的複雜密碼條件 Device Initialization - VP50
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直	圖 4.6b - 非必須的複雜密碼條件 Device Initialization - VP50
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直 符合最低限度要求為止。	圖 4.6b - 非必須的複雜密碼條件 Device Initialization - VP50
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直 符合最低限度要求為止。	圖 4.6b - 非必須的複雜密碼條件 Device Initialization - VP50
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直 符合最低限度要求為止。 情況適用於複雜密碼與密碼片語密碼。	圖 4.6b - 非必須的複雜密碼條件 Device Initialization - VP50
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直 符合最低限度要求為止。 情況適用於複雜密碼與密碼片語密碼。	圖 4.6b - 非必須的複雜密碼條件
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直 符合最低限度要求為止。 情況適用於複雜密碼與密碼片語密碼。	圖 4.6b - 非必須的複雜密碼條件
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直 符合最低限度要求為止。 情況適用於複雜密碼與密碼片語密碼。	圖 4.6b - 非必須的複雜密碼條件
圖 4.6a - 複雜密碼條件符合 果是無效的密碼,「密碼條件方塊」將會以紅 顯示,同時將會停用「Next」(下一步)按鈕,直 符合最低限度要求為止。 情況適用於複雜密碼與密碼片語密碼。	圖 4.6b - 非必須的複雜密碼條件         Device Initialization - VP50         Password         ② Password         Please create 8 secure Complex Password following the criteria below.         ExamplePassword         ExamplePassword         ③ 4.6b leng         ④ uppercase         ● Inconker         ● ExamplePassword         ● Example Password         ● Example Password





### 虛擬鍵盤

VP50/VP50C 具有可防範鍵盤記錄程式的虛擬鍵盤。

	Device Initialization - VP50 GIRONKEY V
• 若要利用 <b>虛擬鍵盤</b> ,請在 <b>裝置初始化</b> 畫面的右 上角找到鍵盤按鈕然後加以選取。	Perice Initialization - VP50  Password  Complex Passphrase  Please create a secure Passobrase password following the criteria below.  This is my Passw0rd Example!  This is my Passw0rd Example!  VID characters minimum.
	Password Hint? Enable Admin and User Passwords ① Back Next Cancel 圖 4.8 - 啟用虛擬鍵盤
<ul> <li>出現虛擬鍵盤後,您還可以啟用<b>螢幕記錄程式</b> 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。</li> <li>為使得此功能更加強大,您還可以選擇鍵盤右 下角的<b>隨機化</b>,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。</li> </ul>	Virtual Keyboard       1       Screenlogger Protection       * * *         1       2       4       5       6       7       9       0       -       2         9       w       r       y       u       0       P       I       1       <





#### 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」。

	Device Initialization - VP50	GIRONKEY
	B Password	
若要隱藏密碼字串,請按一下灰色圖示。	Complex Passphrase	
	Please create a secure Passphrase password following the	criteria below. 😗
$\odot$	This is my Passw0Rd Eample!	
	This is my PasswORd Eample	
	210 characters minimum	
	Password Hint?	
	Enable Admin and User Passwords 1	
	Back	Next Cancel
	<b>圖 4.10 - 點擊以隱藏</b> 密	碼
	Device Initialization - VP50	GIRONKEY
	A Password	(1)
艺西 <b>昭二</b> 俘荐的家庭,建按一下萨舟图二。	Complex Passphrase	/
石安線不隐澱的盜嗎,請按一下監巴圓小。	Please create a secure Passphrase password following	criteria below. 🕦
<u>()</u>		
	✓ 10 characters minimum	
	Password Hint?	
	Enable Admin and User Passwords 👔	
	Back	Next Cancel
	<b>圖 4.11 - 點擊</b> 以顯示密	碼





### 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<u>啟用</u>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。

	Device Initialization - VP50	IRONKEY V
• 若要啟用管理員和使用者密碼,請按一下	A Password	
<b>啟用管理員和使用者密碼</b> 旁邊的万塊,然後在完成選擇有效的密碼之後選取「Next」(下一步)。(圖 4.12)	Complex Passphrase Please create a secure Passphrase padsword following the criteria below	
<ul> <li>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。</li> </ul>	● Enable Admin and User Passwords ■ Back Noxt ■ 4.12 - 啟用管理員和使用者密码	Cancel

#### 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。





### 管理員和使用者密碼

	Device Initialization - VP50	GIRONKEY
如果已經在上一個書面中啟用管理員	🔒 User Password	01
角色,則後續畫面將會提示輸入使用	Please create a secure Passphrase password follow	ving the criteria below. 🚯
者密碼 (圖 4.13) 與管理員密碼相比,	Finasword	
吏用者密碼在功能上會受到限制,本	Comini Password	
吏用者指南會在稍後討論更多細節。	10 characters minimum	
請參閱第 23 頁。)		
	Falksword Hint?	
	Require password reset on next login 1	
	Back	Next Cancel

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	Login Device - VP50	
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)	User Password  Require password reset	
<b>注意:</b> 為安全起見,新的密碼不可以 和暫時密碼相同。	○ Read-Only Mode <b>●</b> ■         ■           ■         4.14 - 下次登入時需重設密	ogin Cancel





### 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。)

	Device Initialization - VP50	GIRONKEY
「Name」(名稱) 欄位可包含多達 32 個字元,但不得包含 <b>確切</b> 密碼。	Contact	
「Company」(公司)欄位可包含多 達 32 個字元,但不得包含 <b>確切</b> 密 碼。	Details	
「Details」(詳細資訊)欄位可包含多 達 156 個字元,但不得包含 <b>確切</b> 密 碼。		
	[囲] →・エ→ - 49P約日 €	₹₽ ₩

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/VP50C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)

Login Device - VP50 GIRONKEY v	Login Device - VP50	GIRONKEY
🔒 User Password 🚳 📾	Admin Password	
Contract Information Login as Asmin	Possylpid D Hint Reset Device	
Read-Only Mode	Read-Only Mode	
圖 5.1 - 使用者密碼登入 (管理員已啟用)	圖 5.2 - 管理員密	了碼登入
供僅使用者模式登入(管理員未啟用)	Lagin Device - VP50	GIRONKEY .
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)	User Password  Password  Password  O Hint  Contact information Reset Device	
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。	Read-Only Mode 🖲	Login
	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:

		Login Device - VP50	GIRONKEY .
1.	將裝置插入電腦的 USB 連接埠,然後 執行 IronKey.exe。	🔒 User Password	@ [ m]
2.	在輸入密碼方塊下方選取 <b>唯讀模式</b> 。 <b>(圖 5.4)</b>	(Passward O Hint	
3.	輸入您的裝置密碼,然後按一下 「Login」(登入)。IronKey 現在將會以 唯讀模式解銷。	Contact Information Reset Device	
	"正項1天工/开坝	Read-Only Mode	
			Login Cancel
		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/VP50C 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/VP50C 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 裝置行為 (10 次錯誤密碼嘗試)	資料清除與裝置重設?
使用者密碼	密碼鎖定。以管理員身分登入或是 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 單一使用者,單一密碼 (管理員/使用者 <u>未</u> 啟用)	暴力破解保護 裝置行為 (10 次錯誤密碼嘗試)	資料清除與裝置重設?
使用者密碼	加密清除隨身碟、密碼、設定以及 資料永久清除	是

\*成功驗證裝置後,將根據使用的登入方法重設失敗登入計數器。加密清除將會刪除所有密碼、加密金鑰與 資料 - 您的資料將會永久遺失。

### 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/VP50C 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。 <b>(圖 6.1)</b>	し G の) 10:20 AM 3/25/2022 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)	<ul> <li>VP50 Settings</li> <li>Browse VP50</li> <li>Format VP50</li> <li>Online Support</li> </ul>
有關這些裝置選項的詳細資訊,請參閱本手冊的第19-23頁。	<ul> <li>About VP50</li> <li>Shut down VP50</li> <li>Shut down VP50</li> <li>+ = 3/26/2022</li> <li>圖 6.2 - 在 IronKey 圖示按一下右鍵以顯示裝置選項</li> </ul>

### 裝置選項 - (macOS 環境)







# 裝置選項

VP50 設定:	<ul> <li>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/VP50C設定」 一節)。</li> </ul>	
瀏覽 VP50:	• 可讓您檢視自己的安全檔案。	
格式化 VP50:	Login Device - VP50 GIRONKEY -	
可讓您格式化安全資料磁碟分割區。(警告:將會清除所有資料)(圖6.1) 注意:密碼認證需要進行格式化。 線上支援:	♥ User Password          ● Warning!       ● Warning!         ● Formatting will erase ALL data on your encrypted three.       ● If data will be lost forever. Are you sure you want to proceed?         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase ALL data on your encrypted three.         ● If a formatting will erase ALL data on your encrypted three.       ● If a formatting will erase and three.         ● If a formatting will erase and three.       ● If a formatting will erase and three.	
	得其他支援資訊。	
<b>關於 VP50:</b> 提供有關 VP50/VP50C 的特定詳細資訊, 包括應用程式、韌體和序號資訊。(圖	About - VP50 GIRONKEY ~ ~ () About © 2022 Kingston Technology Corporation.	
6.2)		
<b>注意:</b> 隨身碟的唯一序號將會在「資訊 欄」底下。	ModulesVersionInformationIKVP50IKVP50002324853023863190000062Application1.0.0.0FW Version01.0610Crypto Library FW1.00	
	Close	
	圖 6.2 - 關於 VP50/VP50C	
將 VP50 關機:	<ul> <li>正確關閉 VP50/VP50C,如此可讓您從系統安全地將其 移除。</li> </ul>	





# VP50/VP50C 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)
  - o變更使用者密碼
  - o登入密碼重設 (適用於使用者密碼)
  - o啟用一次性恢復密碼
  - o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。

Settings - VP50	GIRONKEY .	Settings - VP50	GIRONKEY .
@ Admin Settings	(8) ( m	@ Admin Settings	@   ==
Password Contact Info Language	Acres Option	Passwerd Contact Into Lange	Admin Options
Current Phenward		Convert Presward	
Please create a secure Complex password following the	e criterià bolaw.	Please create a secure Complex password following	Ine criteria bolow.
New Password		New Pasaword	
Confirm New Password		Description Research	
5-15 long		Commit New Password	
uppercase lawercase digit special c	character	5-16 long	
6		uppercese lowercese digit speci-	at character
(Pansword Plint)		Printward PlintT	
Done	Apply Cancel	Done	Apply Cancel
圖 71- 密碼裡	<b>嘴口</b> 百		
	274	圖 7.2 - 聯絡	資訊
ettings - VP50	GIRONKEY .	Settings - VP50	GIRONKEY
Admin Settings		Admin Settings	@) =
Possword Contact Info Longuag	ge Admin Options	Password Contact Info Lang	Admin Optima
		Disase enter a new liter Dasswort below	
What is your preferred Language?		Pasaword	
English			
English		Coofirm PAssword	
English		Coofirm PAsavord	
English		Coofirm PAsavord 5-16 long uppercase towercase digit spec	ini character
English		Coofirm PAsavoro 5-16 long uppercasir towercase trigit spec	inf character
English		Coofirm PAsaword B-16 long uppercase lowercane blot spec	ial character
English		Coolim PAssword 5-16 long uppercase lowercase digit spec One-Time Recovery Password Force Read-Only User Data ① Login Password Reset	Inf character
English	Airphy Cancel	Coolim PAssword 5-56 long uppercase lowercane might spec One-Time Recovery Password Force Read-Only User Data D Login Password Reset	tal character
English Done 圖 7 3 - 英言湖	Cancel	Coolim Pitsword 5-16 long uppercase lowercase digit spec One-Time Recovery Password Force Read-Only User Data ① Login Password Reset Dom 圖 7.4 - 管理員	hal charactee





# **VP50/VP50C** 設定

#### 使用者設定:管理員啟用

用者金人時將限制下列設定的仔眼・		
密碼: 允許您變更自己的使用者密碼和/或提 示。( <i>圖</i> 7.5)	Settings - VP50	GIRONKEY -
	O Admin Settings	
	Possword Contact Info	guage Admin Opuons
	What is your preferred Language?	
	English	
	圖 7.5 - 密碼選項 (管理員启	c Apply Cancel Date of the concel Date of the conc
	Settings - VP50	GIRONKEY .
静絡資訊:	@ User Settings	
允許您新增/查看/變更您的聯絡資訊。	Password Contact Into	Longuage
<i>[iii]</i> 7.6)	Please enter your information below.	
	Company	
	Damue	
	Dor	re Apply Cancel
五主・	圖 7.6 - 聯絡資訊 (管理員用	如用:使用者登入)
ゴ 調你戀更日前語言撰項。( <i>圖7.7</i> )	Settings - VP50	GIRONKEY V
	User Settings	- Instantion
	Carabana a Ananazi a Anan	P WILLIAM CO.
	What is your preferred Language?	
	English	
	Don	Ko Apply Cancel
	圖 7.7 - 語言設定 (管理員角	牧用: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/VP50C 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/VP50C 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。<u>此組態無權存取任何管理員選項或功能。</u>此組態將有權存取以 下 VP50/VP50C 設定:

#### 變更與儲存設定



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/VP50C 設定選單。



### 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)。	<form></form>
重設登人密碼: 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)	
<b>注意:</b> 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。	Login Device - VP50       @ IRONKEY <ul> <li>User Password</li> <li>Require password reset</li> <li>The Admin has required that your password:</li> <li>Direase proceed to create a new password:</li> <li>OK</li> <li>Contact</li> <li>Read-Only Mode </li> <li>Eagin Cancel</li> <li>B 8.2B - 在輸入使用者密碼後重設通知</li> </ul>





## 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	Settings - VP50 GIRONKEY
<b>步驟1</b> :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)	Admin Settings          Pessword       Janguage       Ammi Options         Pessword       Pessword       Ending         Ordfilm Pacsword       Big is special character       Option         Once       Apply       Cancel    B 8.4 - 一次性恢復密碼按鈕
	Settings - VP50 GIRONKEY ~
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。	One-Time Recovery Password
<b>注意:</b> 管理員密碼需要套用變更。	Please create a secure Complex password following the Criteria pelow,           Admin. Password           Recovery Password           Confirm Recovery Password           6-18 long           uppercase         lowercase
	Back Save Cancel





### 使用一次性恢復密碼

Login Device - VP50 GIRONKEY -
(Presented) O Hint
Contact Information Recovery Passwora Login as Admin
Read-Only Mode  Cancel
圖 8.6 - 恢復密碼按鈕
Login Device - VP50
Recovery Password
Recovery Password Pesse create a secure password following the otheria below.
New User Password
6-16 long
upparease revercase orgit special character
Hostowerd Hint?
Next: Cancel
圖 8.7 - 恢復密碼選單
GIDONVEY
A User Password
(Plassward
O Hind
Contact Information Login es Admini
Read-Only Mode 3
Legin
圖 8.8 - 使用者密碼登入畫面,顯示 (恢復密碼) 按鈕在成功使用後淡 失。





### 強制使用者唯讀資料

<ul> <li>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)</li> <li>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。</li> </ul>	Settings - VP50 C Admin Settings Pressword Consect Infa Please enter a new User Password below: Please enter a new User Password below: Password Confirms Password G-16 long uppercase Iowercase Iowercase Decial character
<ul> <li>一旦啟用,「<b>唯讀模式」</b>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</li> </ul>	Done       Apply       Cancel         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)         Login Device - VP50       @ IRONKEY: ▼         User Password       @ Image: Cancel
員停用為止。(圖 8.10)	Patendoot         Patendoot         Phint         Contract information         Login         Tacel         B 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





### 裝置解鎖

VP50/VP50C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。

Login Device - VP50	GIRONKEY -
🔒 User Password	@   III
PASSWORD IS INCORRECT	
Read-Only Mode 👔	
圖 9.1 - 密碼不正確語	Login Cancel
Login Davice - VP50	
Admin Password	@  ==
PASSWORD IS INCORRECT YOU HAVE 3 MORE ATTEMPTS LEFT	
Reset Device	
	Léain Cáncel
	Login Device - VP50 ● User Password ● Password © Plant Contact information Reset Device ● Read-Only Mode ● ■ 0.1.1 密碼不正確語 Login Device - VP50 ● Admin Password ● Pass





#### 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<u>格式化資料,同時隨身碟上的所有資料將會永久遺失</u>。本使用者手冊中的<u>第18頁</u>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。

Login Device - VP50	GIRONKEY -	Login Device - VP50	GIRONKEY
🔒 User Password	@1 🚍	Admin Password	@ i 1
9 Warning!		<b>Q</b> Warning!	
Thu have reached the maximum number raties. In order to protect data privacy contact. O Hin Contact.	er of possword , your VP50 is now s Admin or use the pl.	Pour have reached the m retries. In order to prote being formatted and all or Him Ress	aximum number of password ct data privacy, your VP50 is now tata will be lost. You will be able to in the operation completes.
Read-Only Mode		Read-Only Mode 🜒	
	Login Cancel		Back Cancel
裝置解銷	<u>-</u>	裝置	格式化*
(圖 9.3)		(	圖 9.4)
(圖 9.3) 一次性恢復: <b>(</b> 管理員	) 員 <b>/</b> 使用者啟用)	( 使用者密碼	圖 9.4) (管理員未啟用)
(圖 9.3) <u>一次性恢復:(管理</u> 」 .ogin Device - VP50	) <u>員/使用者啟用)</u> GIRONKEY ~	( 使用者密碼 Login Device - VP50	圖 9.4) (管理員未啟用) ⊖IRONKEY
(圖 9.3) <u>一次性恢復:(管理</u> 」 Login Device - VP50	) <u>員/使用者啟用)</u> GIRONKEY →	( 使用者密碼 Login Device - VP50 ● User Password	圖 9.4) (管理員未啟用) ⊖IRONKEY ⊗IS
(圖 9.3) <u>一次性恢復:(管理</u> ogin Device - VP50 Recovery Password @ Warning: ● Warning:	) <u>員/使用者啟用)</u> ⊖IRONKEY → ⊗ =	( 使用者密碼 Login Device - VP50 ● User Password ● Warning!	圖 9.4) (管理員未啟用) ⊖IRONKEY ◎
(圖 9.3) <u>一次性恢復:(管理</u> ) cogin Device - VP50 Recovery Password PASS ● Warning: Pass ● Warning: Pass ● Warning: ● Warning: ● Warning:	) <u>員/使用者啟用)</u> ◎I■ will =	( 使用者密碼 Login Device - VP50 ④ User Password ● Warning	圖 9.4) (管理員未啟用) ⓒIRONKEY ◎]
(圖 9.3) <u>一次性恢復:(管理</u> ) Login Device - VP50 Recovery Password Pass Pass Password retries. Password retries.	) <u>夏/使用者啟用)</u> ©IRONKEY ~ ©IRONKEY ~ ©IRONKEY ~	( 使用者密碼 Login Device - VP50 ④ User Password ● Warning vetres. In order to prote vetres. In order to prote	圖 9.4) (管理員未啟用)
(圖 9.3) <u>一次性恢復:(管理員</u> Login Device - VP50 Recovery Password Pass Password retries. In order to protect dats and recet password retries. In order to protect dats and recet	) <u>夏/使用者啟用)</u> <u></u> @ironkey → ◎ia r at atlinwed P50 is now locked the User	( 使用者密碼 Login Device - VP50 ● User Password ● Warning! ● Warning! ● Warning!	圖 9.4) (管理員未啟用) ⓒ IRONKEY* * © IRONKEY* *
(圖 9.3) <u>一次性恢復:(管理</u> ) cogin Device - VP50	) <b>夏/使用者啟用)</b>	( 使用者密碼 Login Device - VP50 ● User Password ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning!	圖 9.4) (管理員未啟用) @IRONKEY @IRONKEY ***
(圖 9.3) <u>一次性恢復:(管理</u> ) cogin Device - VP50 Recovery Password	■ <u> (使用者啟用)</u> © IRONKEY → © ■ © ■ © ■ © ■ © ■ © ■ © ■ © ■	( 使用者密碼 Login Device - VP50 ● User Password ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Context	圖 9.4) (管理員未啟用) ⓒ IRONKEY © IRONKEY (估計 privice), your VP50 is noty ata will be lost. You will be able to not me operation completes.
(圖 9.3) <u>一次性恢復:(管理</u> ) cogin Device - VP50 Recovery Password	■ <u> 一 r of altinved</u> P50 is now locked DK	( 使用者密碼 Login Device - VP50 ● User Password ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Warning! ● Contact. In order to prote being formatted and all © Hin © Contact.	圖 9.4) (管理員未啟用) ⓒ IRONKEY ( Compared and the second of t
(圖 9.3) <u>一文性恢復:(管理</u> ) cogin Device - VP50 Recovery Password	■	Login Device - VP50 User Password User Password Warning! We have reached the m retrise. In order to prote being formatted and all use your drive again wh Contact:	圖 9.4) (管理員未啟用) ⓒ IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY IRONKEY
(圖 9.3) <u>一文化性恢復:(管理</u> ) cogin Device - VP50 Recovery Password	j./使用者啟用) ◎ IRONKEY ● ◎ IRONKEY ● ● IRO	● Warning ● Warning	圖 9.4) (管理員未啟用) ⓒ IRONKEY IR

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/VP50C 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:裝置格式將清除 VP50/VP50C 安全資料分割區中儲存的所有資訊。





### 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/VP50C 隨身碟的設定方式 (如果啟用管理員/使用者,則出現在管理員登入密碼選單,如 果<u>未</u>啟用管理員/使用者,則出現在「使用者密碼」登入選單)。(請參閱**圖9.7**和 9.8)

• 此選項可讓您建立新密碼,但如果是為了	Login Device - VP50 GIRONKEY ~
保護您資料的隱私權,則會格式化 VP50/VP50C。這代表您的所有資料皆會在 程序中被移除。*	Admin Password 🐵 📾
在户中10219时。	Di Hins Di Hins Result Ditylice
	Read-Only Mode
	Back Cancel
	圖 9.7:管理員密碼:重設裝置按鈕
• <b>注意</b> :當您按一下「 <i>Reset Device</i> 」(重設裝	Login Device - VP50 GIRONKEY v
直) 時,便曾顯示一個訊息方塊且曾詢問恋 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	User Password
返回登入祝銜。(詳見圖 9.8)	Hint     Comment Ander maillion     Frence Davther
	Liser Cancel
	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	Login Device - VP50 GIRONKEY -
化蛍幕, 您可以在具甲啟用「管埋負和使 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	Admin Password
助您提供有關密碼內容的線索。	a new password and format your drive now?
	C Read-Only Mode 🕦
	Back Logen Cancel
	圖 9.9 - 重設裝置確認





#### 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/VP50C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/VP50C-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/VP50C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。



在本例 (圖 9.10)中,VP50/VP50C 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/VP50C 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/VP50C,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。





## 錯誤訊息

<b>無法建立檔案:</b> 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。	Unable to create file Unable to create the file 'New Text Document.txt' The media is write protected. OK B 9.11 - 無法建立檔案錯誤
<b>複製檔案或資料夾發生錯誤:</b> 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。	Error Copying File or Folder       Image: Cannot copy File1: The disk is write-protected.         Remove the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.         Image: Construction of the write-protection or use another disk.
<b>刪除檔案或資料夾發生錯誤:</b> 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。	Error Deleting File or Folder       XI         Cannot delete File1: The disk is write-protected.       Remove the write-protection or use another disk.         OK       OK         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/VP50C 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。