User Manual

IronKey D500S

Find the language and latest documentation here.

IronKey D500S Installation Guide

 ..... For instructions in English

 ..... Para instrucciones en Español

 ..... Für Anleitungen in Deutsch

 ..... Pour des instructions en Français

 ..... Per le istruzioni in Italiano

 ..... Por as instruções em Português

 ..... Instrukcje w jezyku Polskim

 .....日本語マニュアル用

Simplified Chinese .....简体中文说明书

Traditional Chinese ....繁體中文說明

IRONKEY™ D500S
SECURE USB 3.2 Gen 1 FLASH DRIVE

User Guide

Contents

Figure 1: IronKey D500S

Introduction

The Kingston IronKey D500S is a military-grade security USB drive that builds on the features which made IronKey well-respected to safeguard sensitive information. It is FIPS 140-3 Level 3 (pending) certified which includes new security enhancements from NIST requiring secure processor upgrades for added security. Encryption and decryption is done on the D500S, with no trace left on the host system – making it immune to password sniffers in memory. Along with hardware-based XTS-AES 256-bit encryption, it also features a rugged zinc casing that is waterproof*, dustproof*, crush-resistant and sealed with epoxy to protect internal components from penetration attacks.

D500S supports Multi-Password (Admin, User, One-Time Recovery and Crypto-Erase) options with traditional 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 Passphrase mode allows for a numeric PIN, sentence, list of words, or even lyrics from 10 to 128 characters long. Admin can enable a User, create custom sized dual data partitions separating Admin/User login files, enable a One-Time Recovery password, Crypto-Erase password, and reset the User password to restore data access.

To aid in password entry, the "eye" symbol can be enabled to reveal the typed-in password, reducing typos leading to failed login attempts. For added peace of mind, D500S uses a digitally-signed firmware making it immune to BadUSB malware, and Brute Force password attack protection to prevent password guessing. Brute Force attack protection locks out User or One-Time Recovery passwords upon 10 invalid passwords entered in a row, and crypto-erases the drive if the Admin password is entered incorrectly 10 times in a row.

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

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.

D500S offers many customization options and is TAA/CMMC compliant and assembled in the USA.

D500S is backed by a limited 5-year warranty with free Kingston technical support.

* Please refer to datasheet's specification. Product must be clean and dry before use.
** Passphrase mode not supported on Linux systems.
*** Virtual Keyboard: Only supports US English on supported Microsoft Windows and macOS systems.

IronKey D500S features

- FIPS 140-3 level 3 (Pending) 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
- Unique Dual-Partition option and Crypto-Erase Password
- Eye button to display entered passwords to reduce failed login attempts
- Virtual keyboard to help protect against keyloggers and screenloggers
- Forced/Session based 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, macOS and Linux compatible (consult datasheet for details)

About this manual

This user manual covers the IronKey D500S and is based on the factory image with no implemented customizations.

System requirements

PC platform • Intel, AMD & Apple M1 SOC • 15MB free disk space • Available USB 2.0 - 3.2 port • Two consecutive drive letters after the last physical drive* ***Note:** See 'Drive letter conflict' on page 35.	**PC operating system support** • Windows 11 • Windows 10
Mac platform • 15MB free disk space • USB 2.0 - 3.2 Port	**Mac Operating System support** • macOS macOS 11.x - 14.x
Linux platform • 5MB free disk space • USB 2.0 - 3.2 Port	**Linux operating system support** • Linux Kernel v4.4+

Recommendations

To ensure there is ample power provided to the D500S device, insert it directly into a USB port on your notebook or desktop, as seen in ***Figure 1.1***. Avoid connecting the D500S 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 D500S comes preformatted with the FAT32 file system. It will work on Windows, macOS and Linux***** 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 D500S on a target system
- When using the drive on a public, or unfamiliar system, you may wish to set the Read-Only mode on the device to help protect the drive from malware
- Lock the device when not in use
- Eject the drive before unplugging it
- Never unplug the device when the LED is lit. This may damage the drive and require a reformat, which will erase your data
- Never share your device password with anyone

Find the latest updates and information

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

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

*** The D500S does not support out-of-box initialization on Linux and will need to be fully initialized and configured on a supported Windows or macOS system before the drive can be used on Linux. Additional information can be found in the Linux section of this user guide on page 37**

Best practices for password setup

Your D500S 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, D500S will automatically wipe out the encrypted data – formatting itself back to a factory state.

Multi-Password
D500S 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 D500S can support three different passwords you may use to recover data – Admin, User, and a One-Time Recovery password.

D500S allows you to select two main passwords – an Administrator password (referred to as Admin password) and a User password. The Admin can access the drive at any time and set up options for the User – the Admin is like a Super User. In addition, the Admin can set up the One-Time Recovery password for the User to provide a way for the User to log in and reset the User password.

The User can access the drive as well, but compared to the 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. The 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 D500S can be Reset and reused, but the prior data will be erased forever.

Password modes
The D500S also supports two different password modes:

Complex
A complex password requires to meet a minimum of 8-16 characters using at least 3 of the following characters:

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

Passphrase
D500S supports Passphrases from 10 to 128 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 D500S drive, the password language can match the language selected for the drive. This allows you to select multiple words, a phrase, lyrics from a song, a line from poetry, etc. Good passphrases are among the most difficult password types to guess for an attacker yet may be easier to remember for users.

Setting Up My Device

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

Device access (Windows environment)

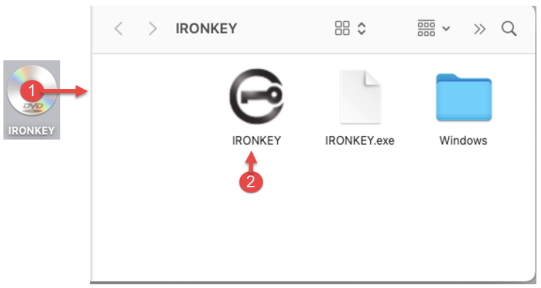
Plug the IronKey encrypted USB drive into an available USB port on the notebook or desktop and wait for Windows to detect it.

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

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

Device access (macOS environment)

Insert the D500S 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 'IRONKEY' volume appear on the desktop. (Figure 3.3)

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

Device Initialization (Windows & macOS Environment)

Language and EULA

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

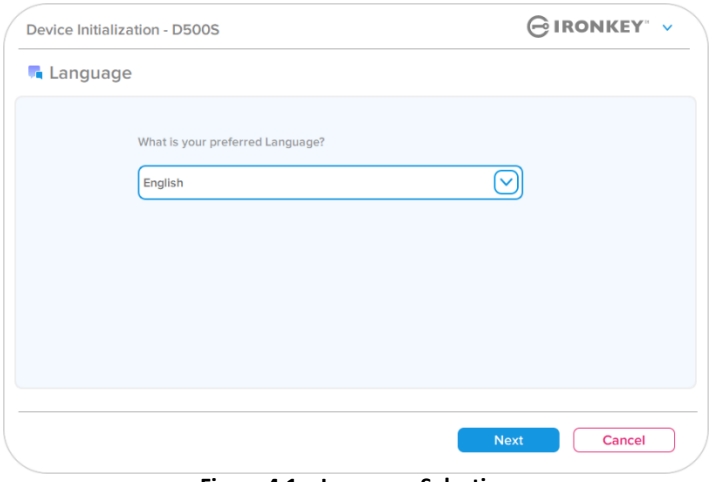


Figure 4.1 – Language Selection

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

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

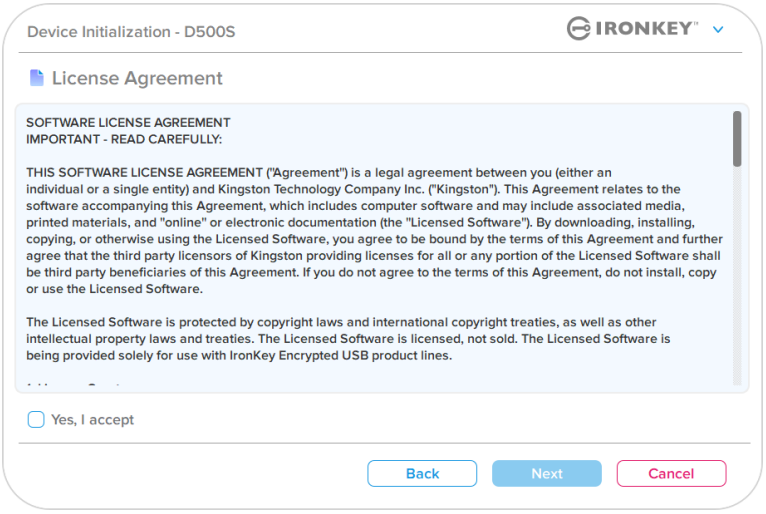


Figure 4.2 – License Agreement

Device Initialization

Password selection

On the Password prompt screen, you will be able to create a password to protect your data on the D500S using either the Complex or Passphrase password modes (Figures 4.3- 4.4). Additionally, the Multi-password Admin/User options can also be enabled on this screen. Before proceeding with password selection, please review Enabling Admin/User Passwords below for a better understand of these features.

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

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

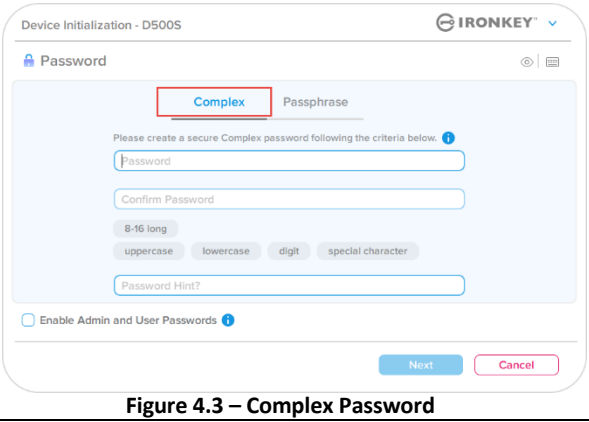
<table>
<tr>
<td>Complex Password
Must contain 8 characters or more (up to 16 characters.)
Must contain three (3) of the following criteria:
Upper Case
Lower Case
Numerical Digit
Special characters (!,$,&, etc..)</td>
<td> 

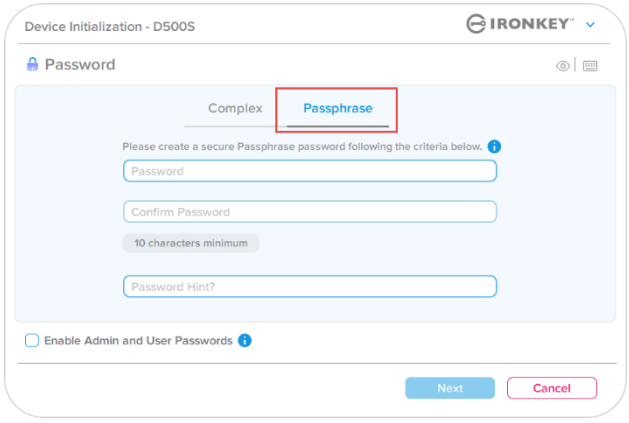
Figure 4.3 – Complex Password</td>
</tr>
<tr>
<td>Passphrase Password
Must contain:
10 characters minimum
128 characters maximum</td>
<td> 

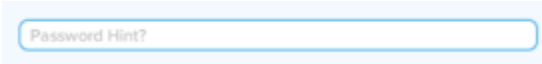
Figure 4.4 – Passphrase Password</td>
</tr>
<tr>
<td>Password hint (optional)
A password hint can be useful for providing a clue as to what the password is, should the password ever be forgotten.
Note: The hint CANNOT be an exact match to the password.</td>
<td> 

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

Device Initialization

Valid and invalid passwords

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

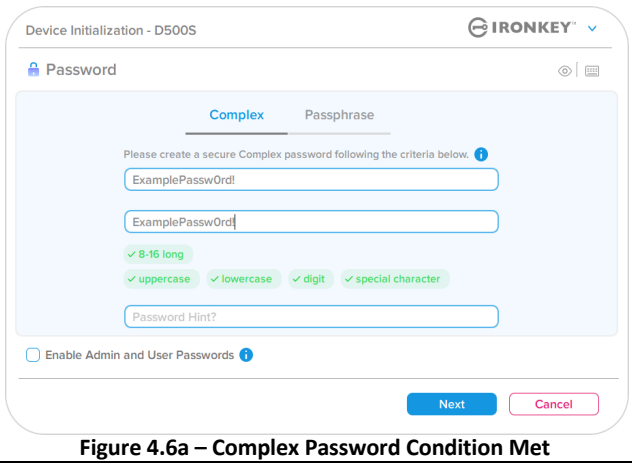


Figure 4.6a – Complex Password Condition Met

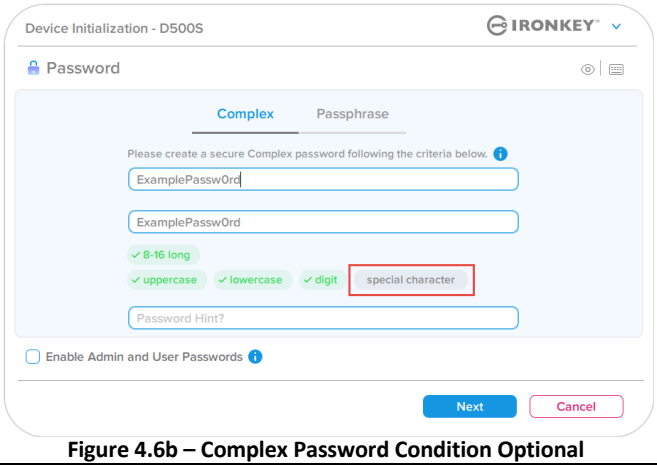


Figure 4.6b – Complex Password Condition Optional

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

This applies to both Complex and Passphrase Passwords.

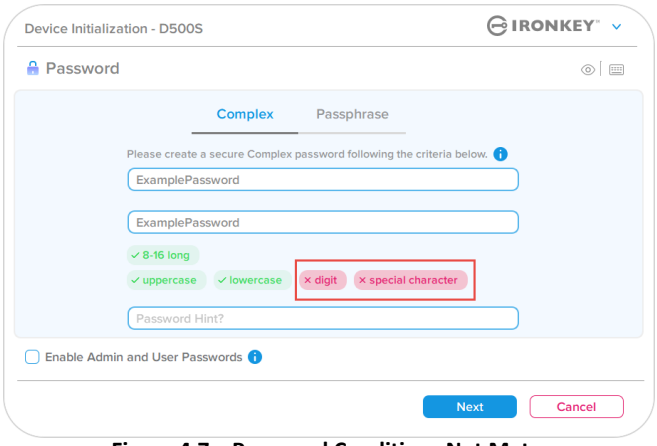


Figure 4.7 – Password Conditions Not Met

Device Initialization

Virtual keyboard

The D500S features a virtual keyboard that can be used for Keylogger protection.

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

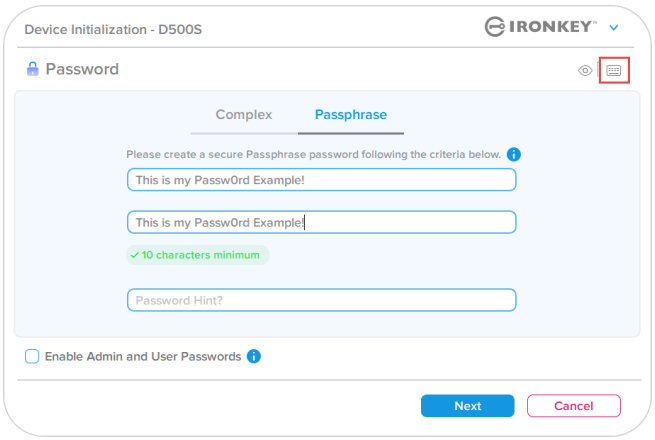


Figure 4.8 – Activating the Virtual Keyboard

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

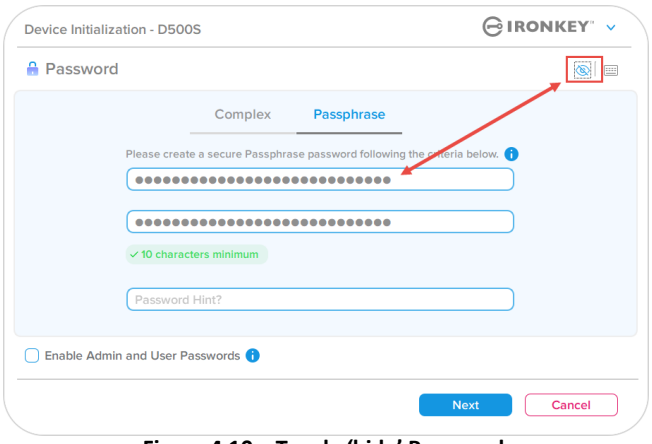
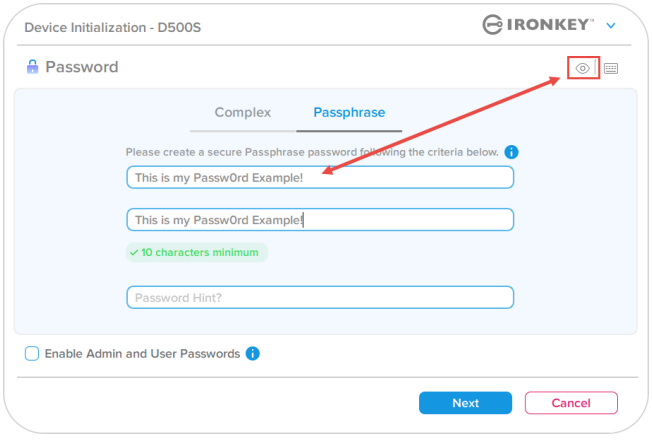
Figure 4.9 – Screenlogger Protection / Randomize

Device Initialization

Password visibility toggle

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

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

To **hide** the password string, click the gray icon. 	 **Figure 4.10 – Toggle 'hide' Password**
To **show** the hidden password, click the blue icon. 	 **Figure 4.11 – Toggle 'show' Password**

Device Initialization

Admin and User passwords

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

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

- Dual-Partition configuration
- One-Time Recovery password
- Forced read-only mode for User login
- User password reset
- Force Reset password for User login
- Crypto-Erase password

To learn more about these features, navigate to page 25 within this user guide.

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

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

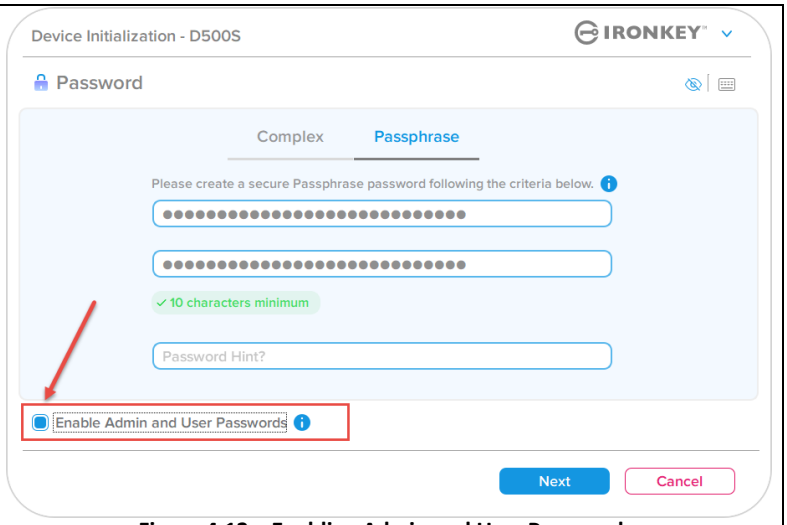


Figure 4.12 – Enabling Admin and User Passwords

Note: Enabling Admin and User passwords is optional.

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

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

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

Device Initialization

Admin and User Passwords

- If Admin Role was **enabled** in the previous screen, the following screen will prompt for the **User Password** (Figure 4.13) The User Password will have limited capabilities compared to Admin and will be discussed in further detail later in this User Guide (see Page 23)

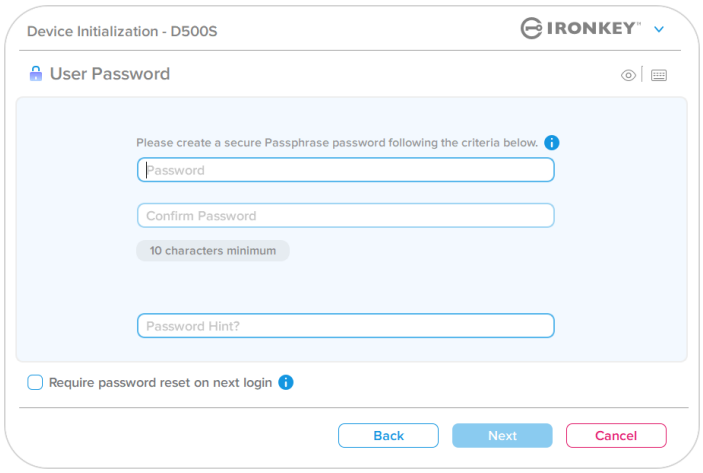


Figure 4.13 - User Password (Admin and User Enabled)

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

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

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

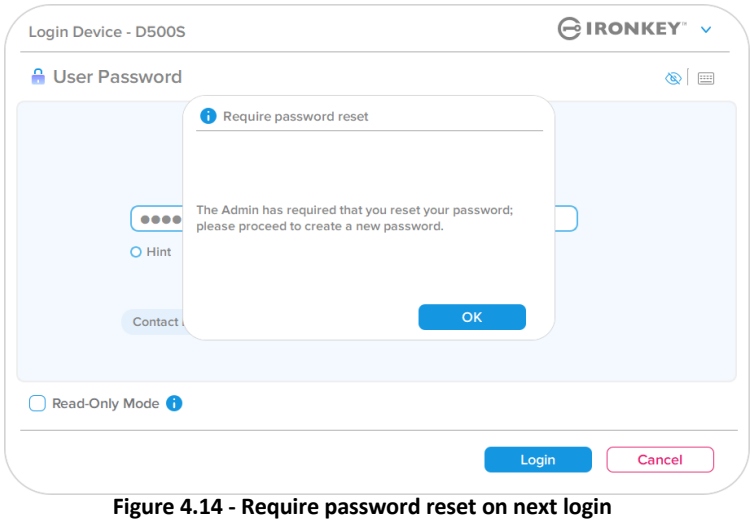


Figure 4.14 - Require password reset on next login (For User Password)

Device Initialization

Dual partitions

The IronKey D500S allows you to create two custom sized, separate partitions between the Admin & User. If this feature is enabled, the Admin login will have access to **both** User & Admin partitions, while the User login will **only** have access to the User Partition. This feature is useful for securely separating data and file access privileges between the Admin & User, or can be used to enable a hidden file store to prevent exposing un-needed files on untrusted systems. The partition sizes between the Admin & User can also be adjusted if desired.

NOTE: This feature is *optional* and can be disabled by leaving the "Enable Dual Partition" box unchecked during setup (Figure 4.15)

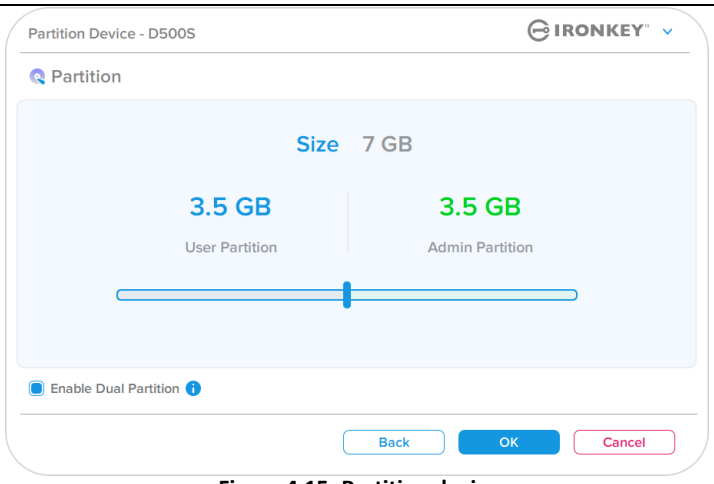


Figure 4.15- Partition device

To adjust and allocate the partition sizes between User & Admin, move the slider to the left or right respectively (Figure 4.16).

- Partitions can be adjusted in 0.5GB Increments.
- Partition sizing is based on the total capacity of the available storage on the hidden partition.
- By default, the Dual partition slider is set to divide storage evenly between Admin & User, until it is manually adjusted.
- The smallest partition size that can be allocated is 1GB.

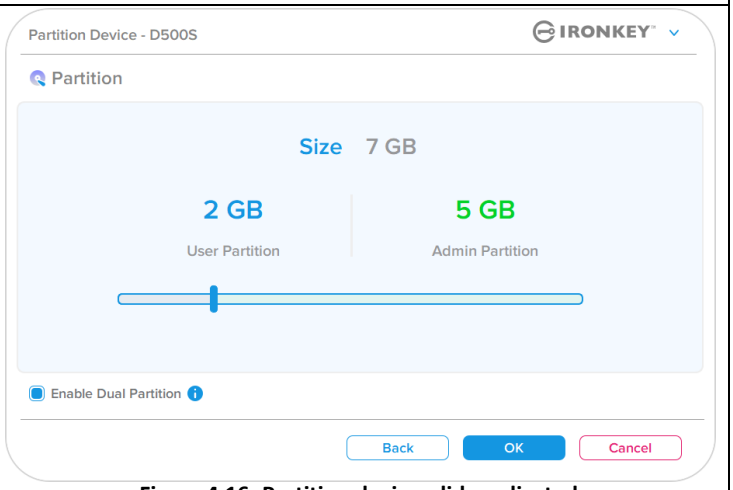


Figure 4.16- Partition device, slider adjusted

Admin Login

Once the drive is fully setup with Dual Partitions enabled, the Admin Login will be presented with an option to unlock the drive to access either the Admin Partition OR the User Partition with each successful login. (Figure 4.17)

NOTE: Only one partition can be opened at a time. Both User & Admin partitions cannot be unlocked at the same time.

The User Login will not be presented with this option and will automatically unlock the User Partition only.

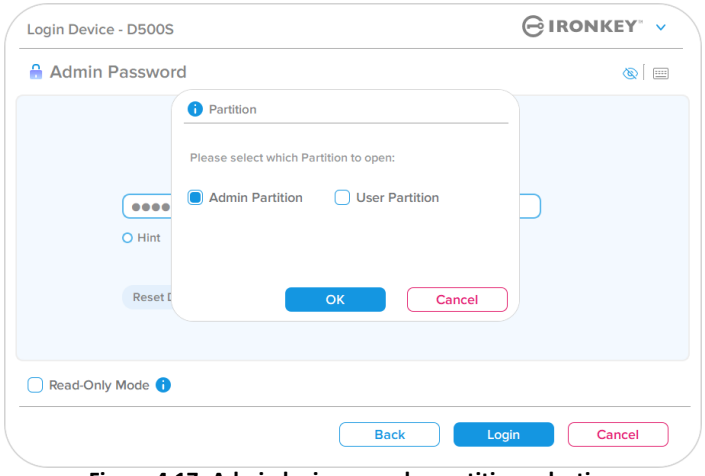


Figure 4.17- Admin login example, partition selection

Device Initialization

Contact information

Enter your contact information into the text boxes provided (see Figure 4.18)

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

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

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

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

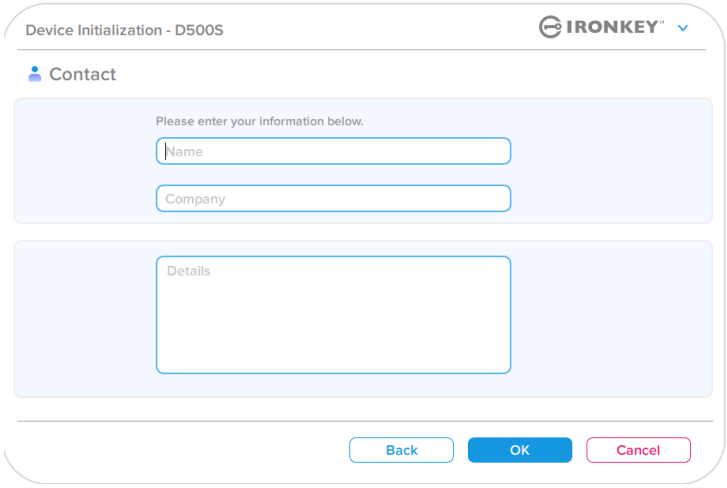


Figure 4.18 - Contact information

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

Device Usage (Windows & macOS Environment)

Login for Admin & User (Admin enabled)

If the device is initialized with Admin and User Passwords (Admin role) enabled, the IronKey D500S application will launch, prompting for the User Password login screen first. From here you can login with the User Password, view any entered contact information, or Login as Admin (Figure 5.1). By clicking on the 'Login as Admin' button (shown below) the application will proceed to the Admin Login menu where you can login as Admin to access the Admin settings and features (Figure 5.2) .

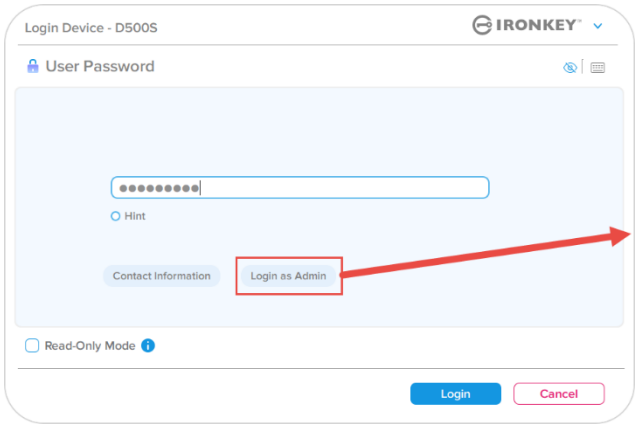


Figure 5.1 - User Password Login (Admin enabled)

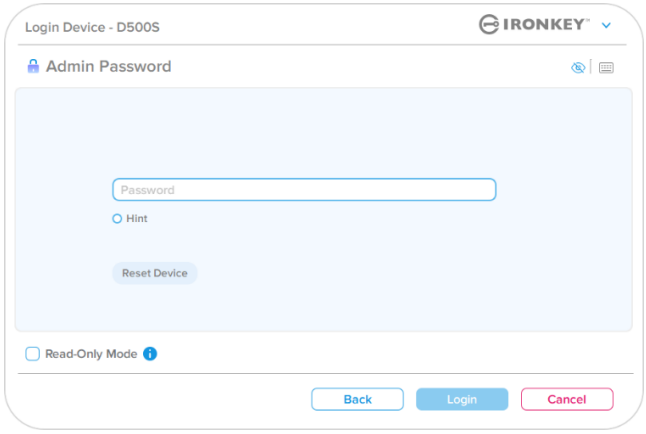


Figure 5.2 - Admin Password Login

Login for User-Only Mode (Admin not Enabled)

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

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

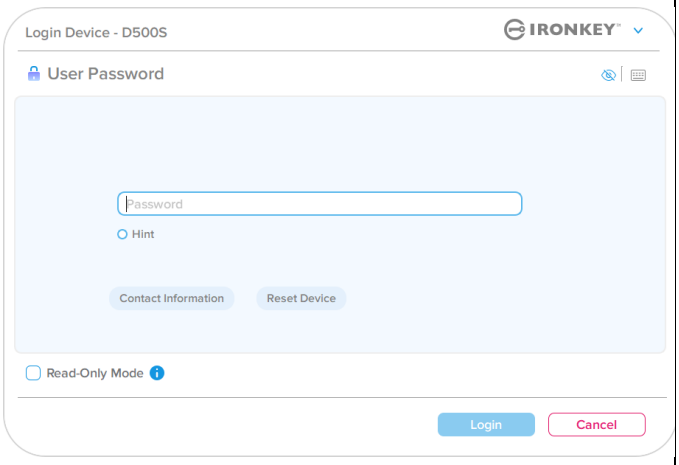


Figure 5.3 - User Password Login (Admin not enabled)

Device Usage

Unlocking in Read-Only Mode

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

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

To unlock the device in Read-Only Mode:

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

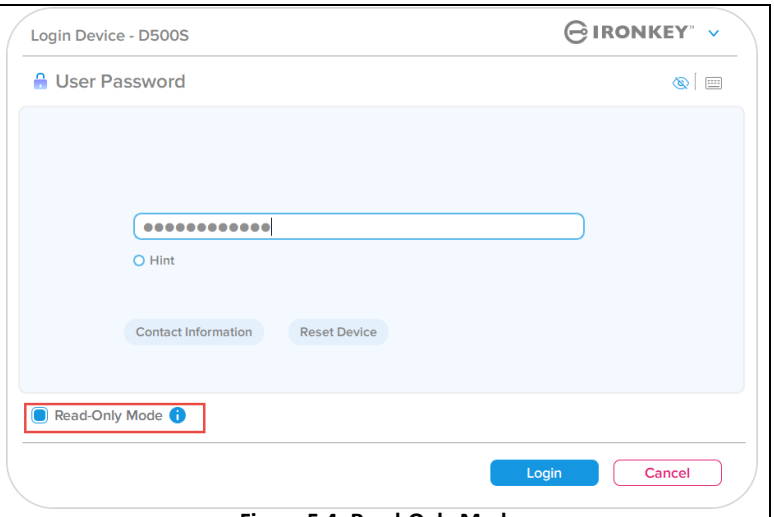


Figure 5.4- Read-Only Mode

If you wish to unlock the device with full read/write access to the secure data partition, you must shutdown the D500S and log back in, leaving the 'Read-Only Mode' checkbox unchecked

Note: The D500S 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 31 for details).

Device Usage

Brute-Force attack protection

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

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

Admin/User Enabled	**Brute Force protection Device Behavior (10 incorrect password attempts)**	**Data Erase and Device Reset?**
User Password	Password Lockout. Login as Admin or use One-Time Recovery password to reset User Password	NO
Admin Password	Crypto-Erase drive, Passwords, settings, and data erased forever	**YES**
One-Time Recovery Password	Password Lockout, Recovery Password button will gray out and become unusable. Login as Admin to Reset Password	NO
User-Only Single User, Single Password (Admin/User NOT Enabled)	**Brute Force protection Device Behavior (10 Incorrect Password attempts)**	**Data Erase and Device Reset?**
User Password	Crypto-Erase drive, Passwords, settings, and data erased forever	**YES**

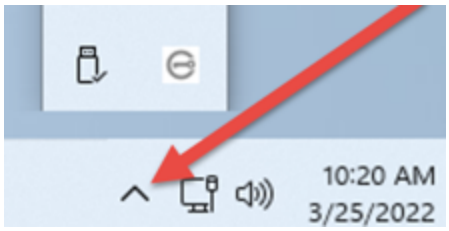
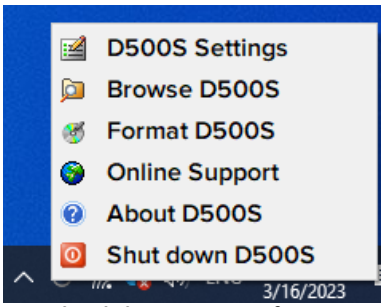
* Once you authenticate to the device successfully, the failed login counter will be reset in relation to which Login method was used. Crypto-erase will delete all passwords, encryption keys and data – **your data will be lost forever.**

Accessing my secure files

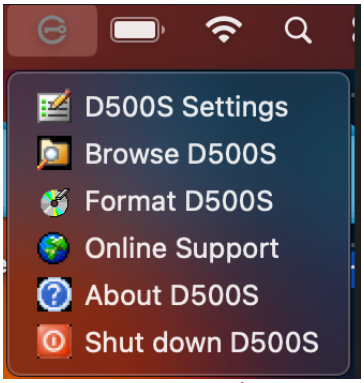
After unlocking the drive, you can access your secure files. Files are automatically encrypted and decrypted when you save or open them on the drive. This technology gives you the convenience of working as you normally would with a regular drive, while providing strong, “always-on” security.
Hint: You can also access your files by right clicking the **IronKey Icon** in the Windows taskbar and clicking **Browse D500S** (Figure 6.2)

Device Options - (Windows Environment)

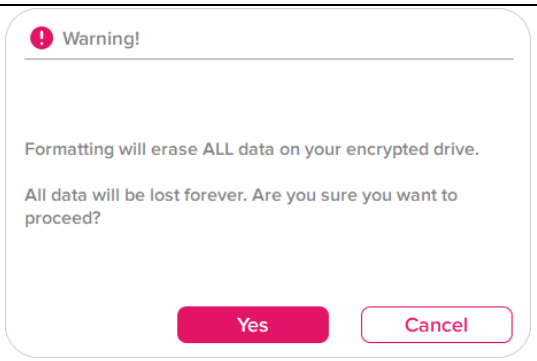
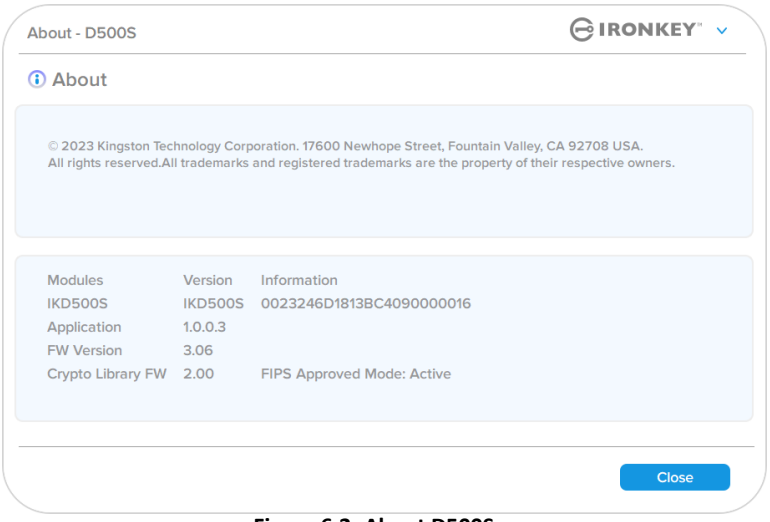
While you are logged into the device, there will be an IronKey icon located in the right-hand corner of the window. Right-clicking on the IronKey icon will open the selection menu for available drive options (Figure 6.2).
Details about these device options can be found on Pages 21-25 of this manual.

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

Device Options- (macOS Environment)

• While you are logged into the device, there will be an IronKey D500S icon located in the macOS menu seen in Figure 6.3 that will open the available device options. Details about these device options can be found on Pages 19-23 of this manual.	 **Figure 6.3- macOS menu bar Icon/Device options menu**

Device Options

D500S Settings:	• Change login Password, contact information, and other settings. (More details about device settings can be found in the 'D500S Settings' section of this manual).
Browse D500S:	• Allows you to view your secure files.
Format D500S: Allows you to format the secure data partition. (Warning: All data will be erased.) (Figure 6.1) **Note:** Password authentication will be required for format.	 **Figure 6.1- Format D500S**
Online Support:	• Opens your internet browser and navigates to http://www.kingston.com/support where you can access additional support information
About D500S: Provides specific details about the D500S, including Application, Firmware and Serial number Information (Figure 6.2) **Note:** The unique serial number of the drive will be under the 'Information Column'	 **Figure 6.2- About D500S**
Shut down D500S:	• Properly shuts down the D500S, allowing you to safely remove it from your system.

D500S Settings

Admin Settings

The Admin Login allows access to the following device settings:

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

NOTE: Additional details of the Admin Options can be found starting on page 26

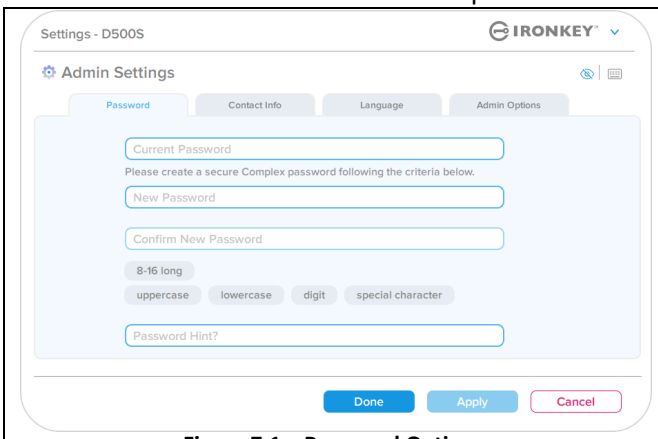


Figure 7.1 – Password Options

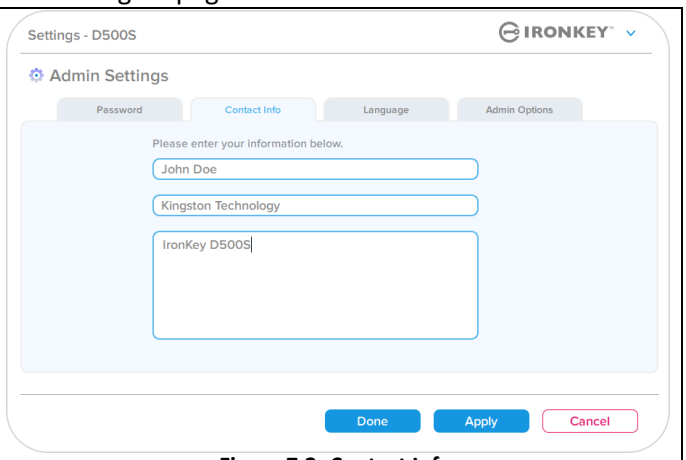


Figure 7.2- Contact Info

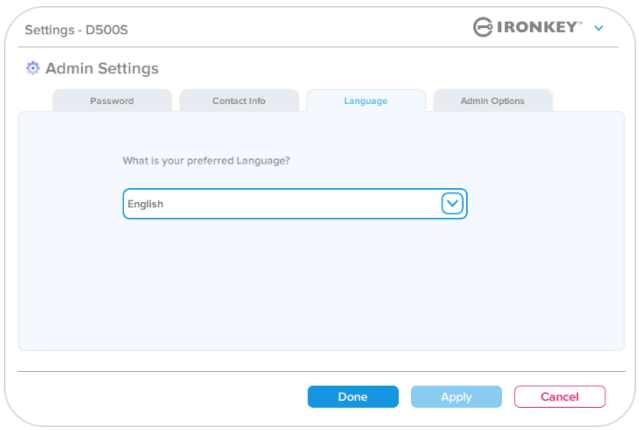


Figure 7.3 - Language Options

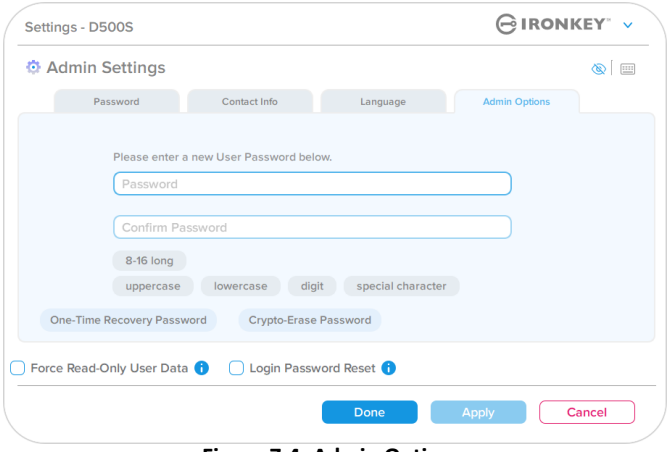


Figure 7.4- Admin Options

D500S Settings

User Settings: Admin enabled

The User Login limits access to the following settings:

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

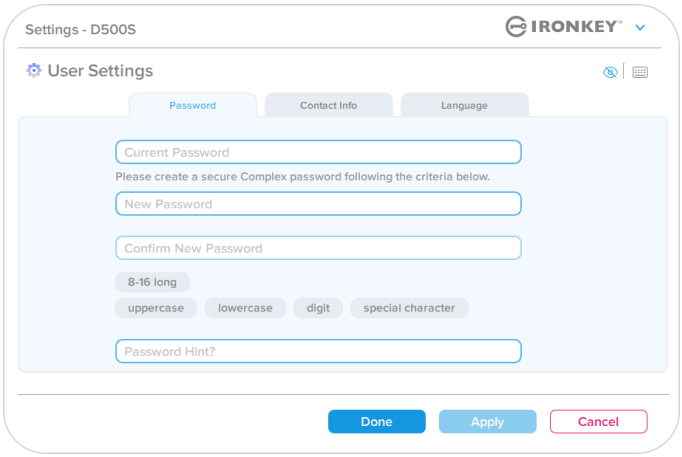


Figure 7.5- Password Options (Admin Enabled: User Login)

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

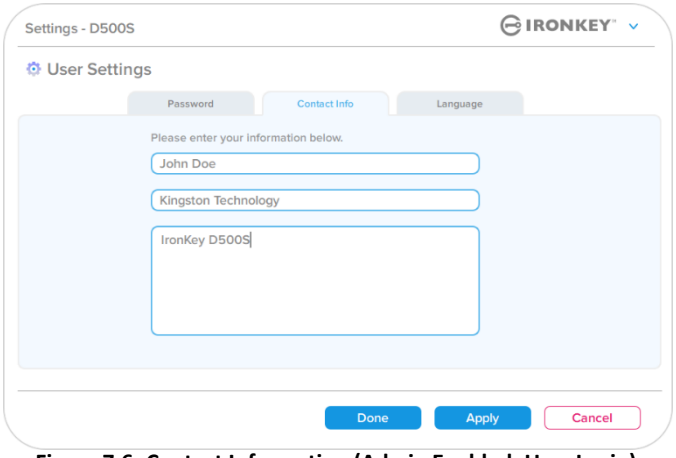


Figure 7.6- Contact Information (Admin Enabled: User Login)

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

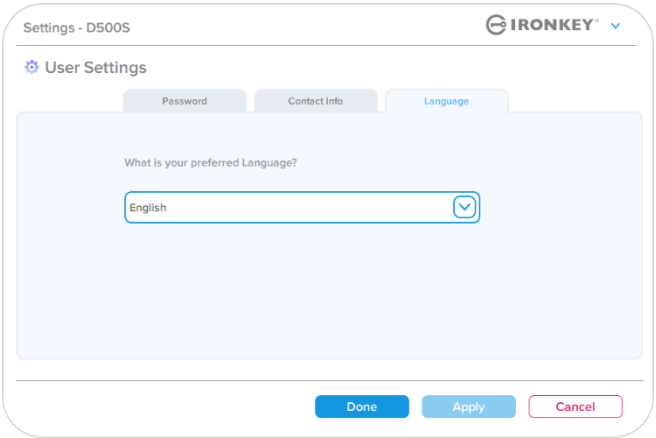


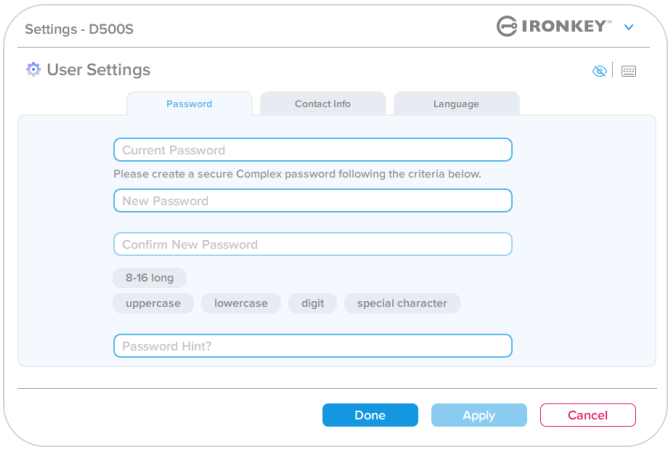
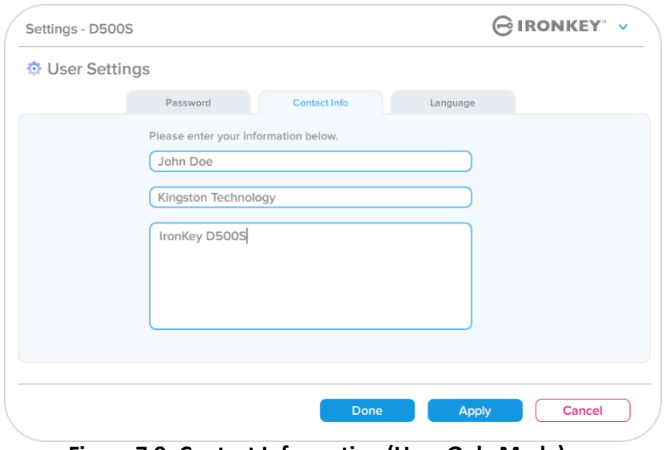
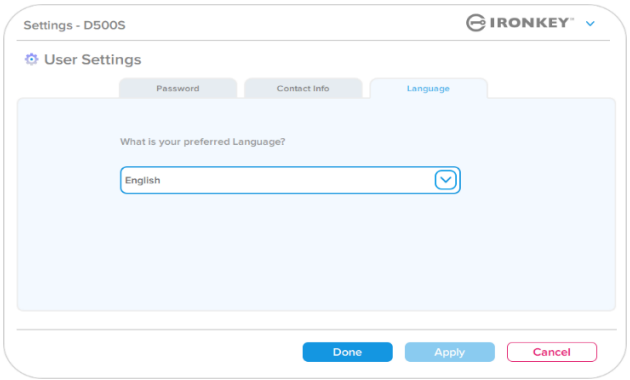
Figure 7.7- Language Settings (Admin Enabled: User Login)

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

D500S Settings

User Settings: Admin not enabled

As mentioned previously, initializing the D500S without enabling 'Admin and User' passwords will configure the drive up in a **Single Password, Single User setup (User-Only mode)**. This configuration does not have access to any Admin options or features. This configuration will have access to the following D500S settings:

Password: Allows you to change your own User password and/or hint (Figure 7.8)	 **Figure 7.8- Password Options (User-Only Mode)**
Contact Info: Allows you to add/view/change your contact information (Figure 7.9)	 **Figure 7.9- Contact Information (User-Only Mode)**
Language: Allows you to change your current language selection (*Figure 7.10*)	 **Figure 7.10- Language Settings (User-Only Mode)**

D500 Settings

Changing and saving settings

- Whenever settings are changed in the D500S Settings (e.g.) Contact information, language, Password changes, Admin options etc..), the drive will prompt to enter your password in order to accept and apply the changes (Figure 7.11)

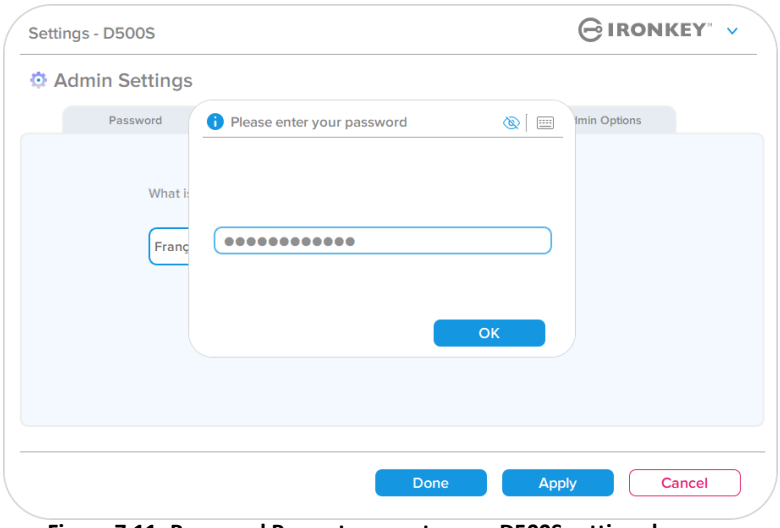


Figure 7.11- Password Prompt screen to save D500S setting changes

Note: If you are on 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 D500S settings menu.

Admin Features

Options available to reset the User password

The features of Admin configuration allow multiple ways to securely reset the User's password, should it be forgotten, or if a temporary User password is created and you would like to enforce a password change upon next login for the User login. Below are the features that can be helpful to reset the User password:

User Password Reset:

Manually change the User password in the 'Admin Options' menu, which is an instant change and will take effect on next User login (Figure 8.1)

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

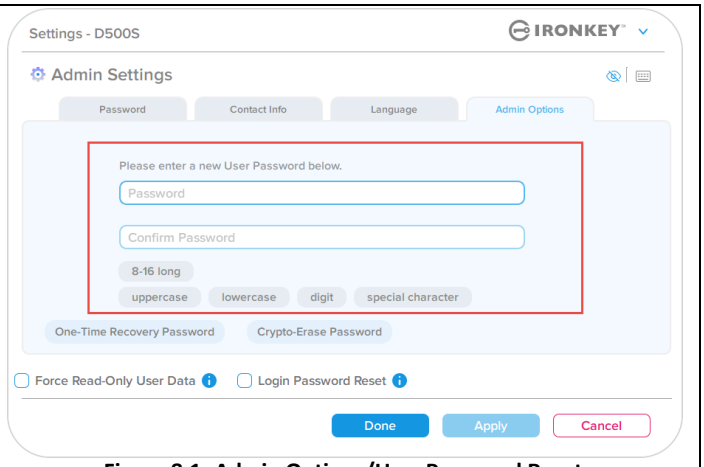


Figure 8.1- Admin Options/User Password Reset

Login Password Reset:

Enabling Login Password Reset will **force the User to login using a temporary password set by the Admin**, and then change it to a password of their choice. This is useful when the drive is given to another person to use. (See Figures 8.2 and 8.3)

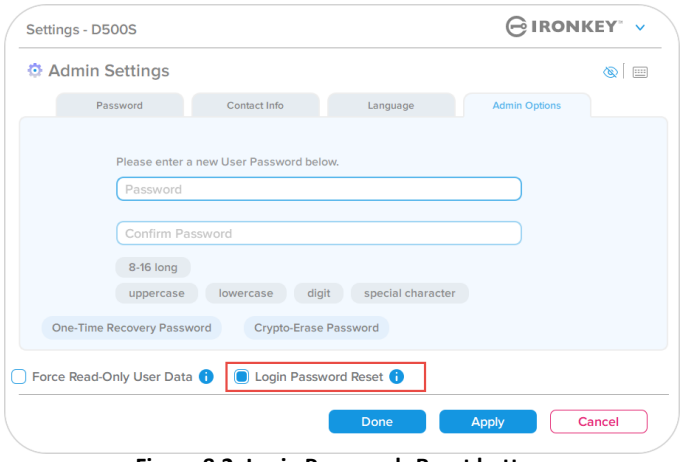


Figure 8.2- Login Passwords Reset button

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

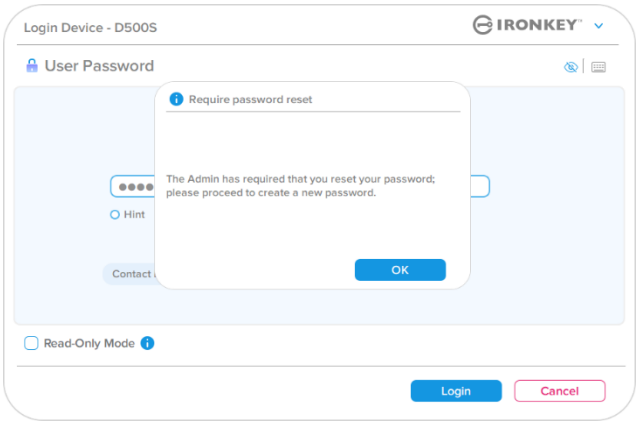
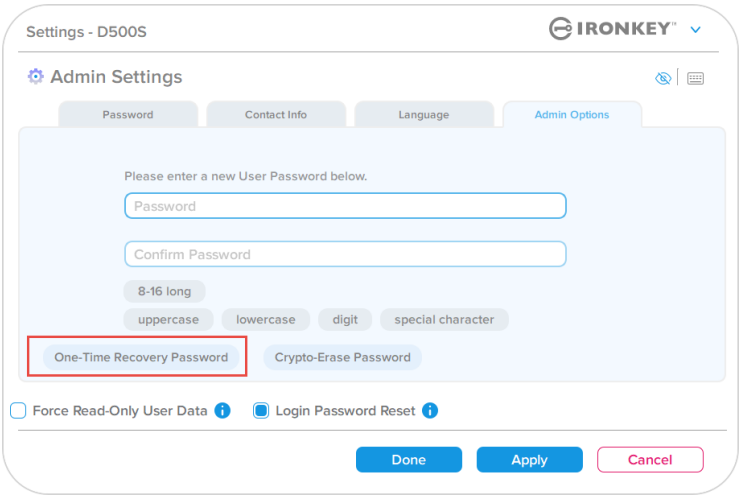
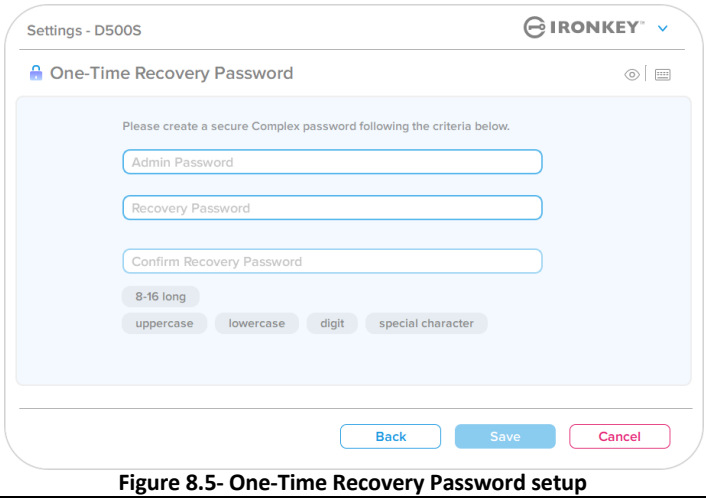


Figure 8.3- Reset Notification after User Password is entered

Admin Features

One-Time Recovery Password

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

One-Time Recovery password **Step 1:** The One-Time Recovery password feature is a very useful, single-use password that can be enabled to help recover and reset the User password should the user password be forgotten. Click on the 'One-Time Recovery Password' button in the Admin options menu to start get started. (Figure 8.4)	 **Figure 8.4- One-Time Recovery Password Button**
Step 2: Create a One-Time Recovery password using the same password criteria the device was initially set with (Complex or Passphrase). **Note:** Admin password will be required to apply changes.	 **Figure 8.5- One-Time Recovery Password setup**

Admin Features

Using One-Time Recovery Password

Step 1: After the One-Time Recovery password has been created, a new button will appear on the **User Password** login screen upon the next login. Click on the **Recovery Password** button to start the process.

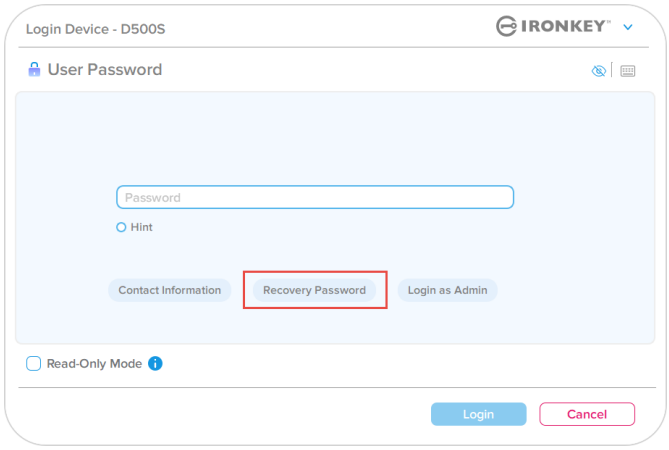


Figure 8.6- Recovery Password Button

Step 2: The **Recovery Password** screen will appear where you can enter in the Recovery Password and create a new 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 19 and 33 for more details)

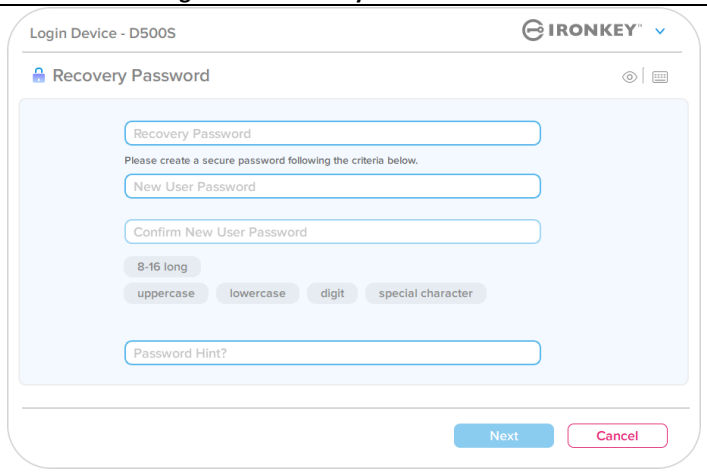


Figure 8.7- Recovery Password menu

Step 3: Upon success, you will be taken back to the **User Password** screen. The **Recovery Password** button is now gone, and the User password entered in **Step 2** will become the new User Password. (Figure 8.8)

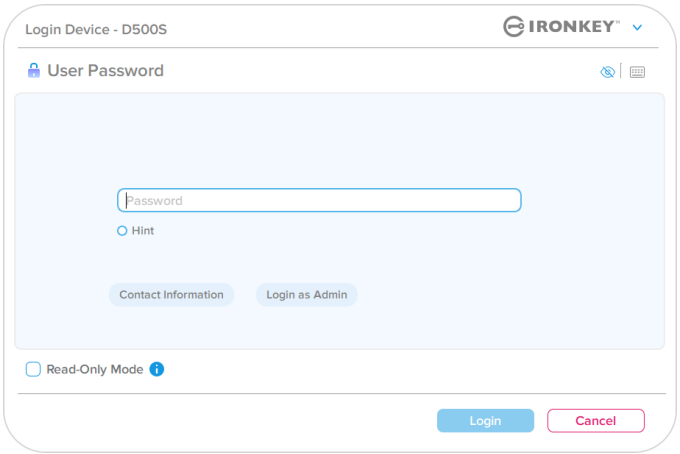


Figure 8.8- User Password Login screen showing the Recovery Password button disappears after successful use.

Admin Features

Crypto-Erase password

The IronKey D500S is equipped with a unique Crypto-Erase password feature that is designed to protect and defend against physically compromising situations by securely erasing the contents of your drive when used, leaving it to appear as if it never had any data written to the drive. When this feature is enabled, and the drive is unlocked with the Crypto-Erase password, it will effectively perform a discreet crypto-erase on the D500S drive and will open the drive in factory state mode with an empty User partition. The previous encryption key will be deleted, and a new device encryption key will be created to take its place. ***Use with Caution***

- To **Enable** this feature, click on the Crypto-Erase password button located in the Admin Options tab:

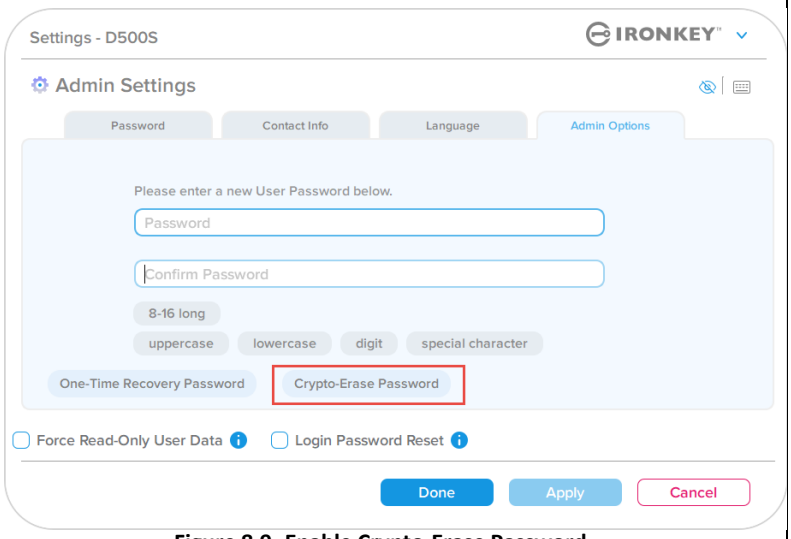


Figure 8.9- Enable Crypto-Erase Password

Create a Crypto-Erase Password:

- Password rules will be based on what the drive was initially initialized with (Complex or Passphrase)
- Admin password will be required for validation.

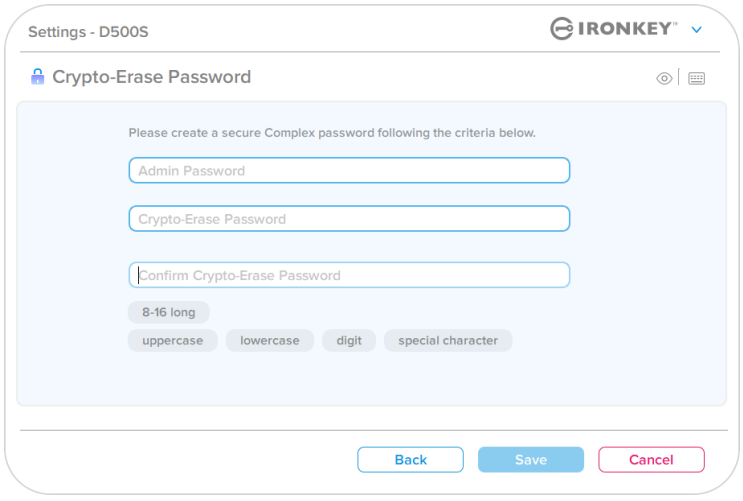


Figure 8.10- Create Crypto-Erase password

Admin Features

Using Crypto-Erase Password

When the Crypto-Erase password is used, the previous Admin and User passwords will be deleted, and the Crypto-Erase password will take its place. Additionally, any previous configuration settings will be deleted along with permanently deleting all data stored on the drive and will convert the drive to a User-Only mode configuration.

To use the Crypto-Erase Password:

1. Launch IronKey.exe to run the IronKey application

2. On the User Password login screen, press '**CTRL + ALT +C**' to toggle the Crypto-Erase Password entry. If done correctly, a thicker blue bar will be noticeable under the password entry Screen indicating the Crypto-Erase password is ready for entry. (Figure 8.11)

NOTE: Crypto-Erase password can only be toggled on the User Password login screen.

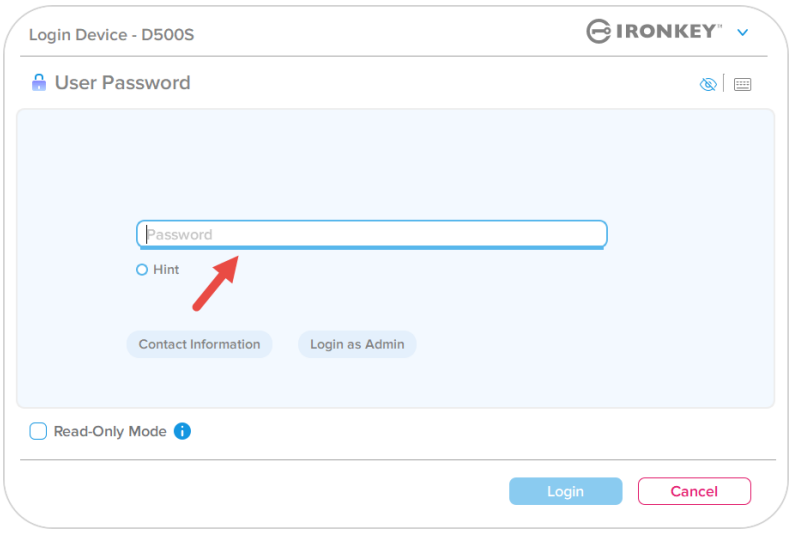


Figure 8.11- Crypto-Erase enabled, with thick blue bar

Once the Crypto-Erase password is used, the drive will now proceed to erase the drive of all contents and a single empty partition will now appear. The drive will now be in a User-Only mode state and the Crypto-Erase password will be the password used to login to the drive until it is reset.

Important: this feature will erase all data on the drive and anything previously stored will be lost forever, proceed with caution.

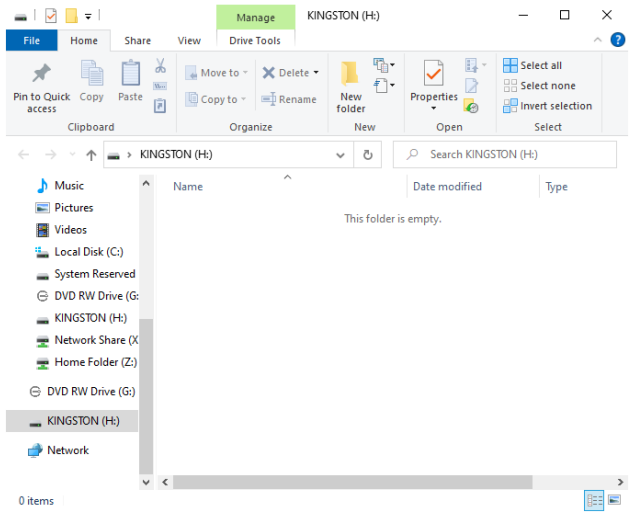


Figure 8.12- Drive wipe after Crypto-Erase password used

Admin Features

Force Read-Only user data

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

- To enable Force Read-Only for the User data, click on the box and click 'Apply'. (Figure 8.13)

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

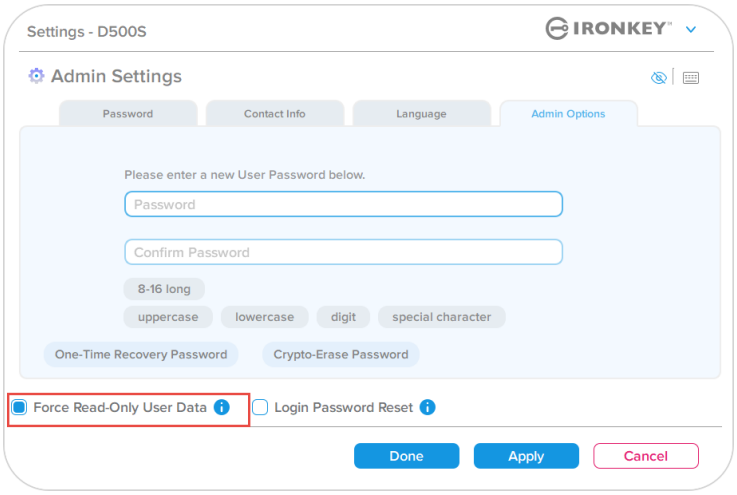


Figure 8.13- Enable 'Force Read-Only User data'
(Admin Password will be required to apply changes)

- Once enabled, the **'Read-Only Mode'** button box will be in a blue color, meaning that Forced Read-Only Mode is permanently enabled for the User password, until it is disabled by the Admin. (Figure 8.14)

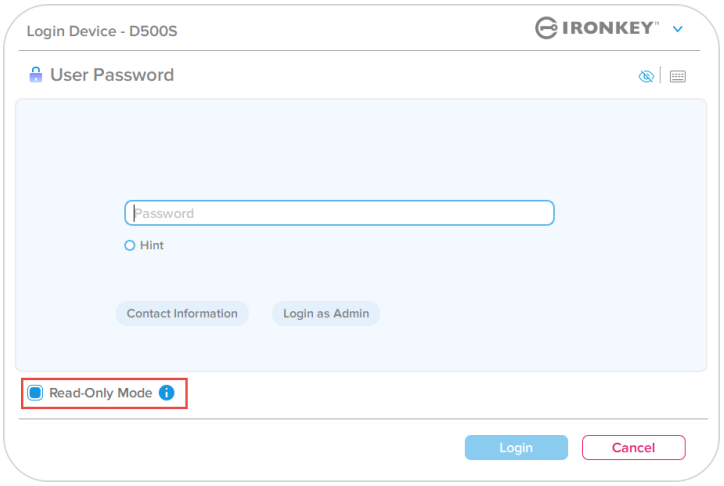


Figure 8.14- Read-Only Mode is forced enabled for the user and can only disabled by Admin

Help and Troubleshooting

Device Lockout

The D500S includes a security feature that prevents unauthorized access to the data partition once a maximum number of **consecutive** failed login attempts (*MaxNoA* for short) has been made. The default "out-of-box" configuration has a pre-configured value of 10 (no. of attempts.) for each login method (Admin/User/One-Time Recovery Password)

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

1. A successful login prior to reaching MaxNoA

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

- If an incorrect password is entered, an error message will appear in red just above the Password Entry field, indicating a login failure. (Figure 9.1)

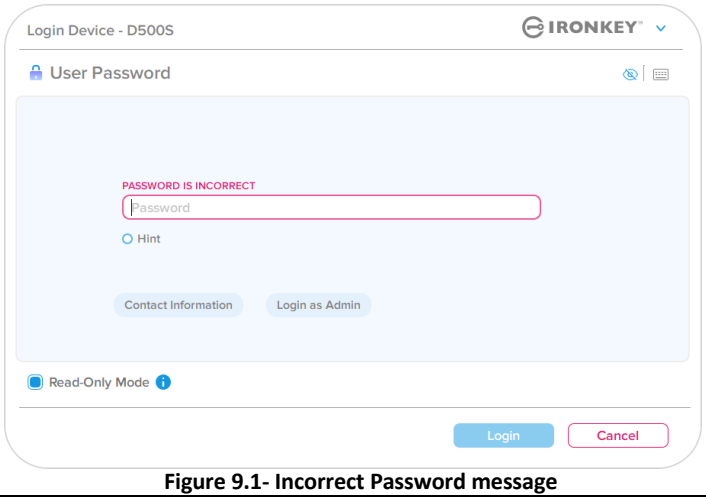


Figure 9.1- Incorrect Password message

- When a **7th** failed attempt is made, you will see an additional error message indicating you have 3 attempts left before reaching MaxNoA (which is set to 10 by default.)(Figure 9.2)

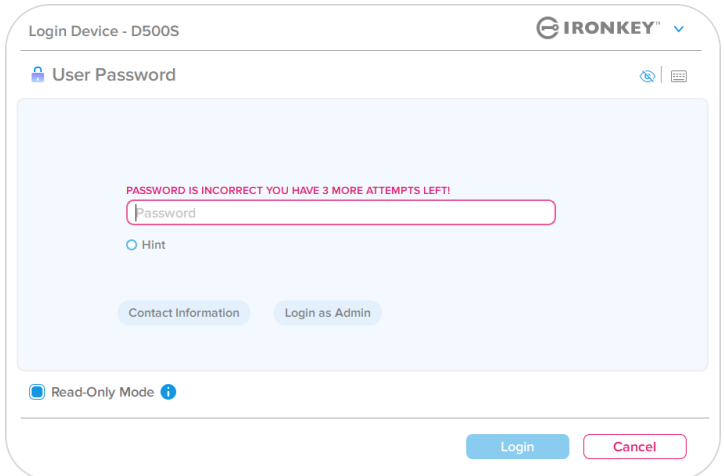


Figure 9.2- 7th incorrect Password attempt

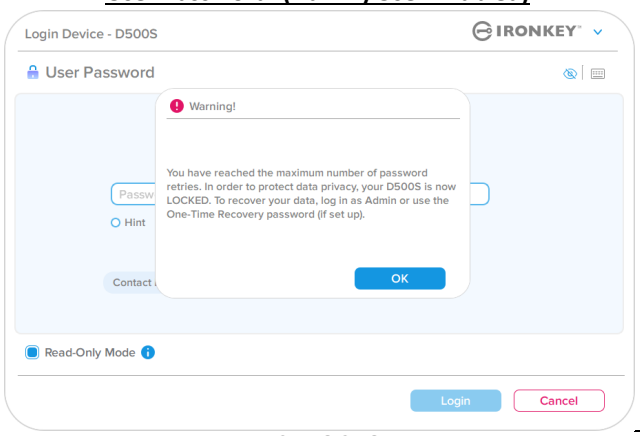
Help and Troubleshooting

Device lockout

Important: After a **10th** and final failed login attempt, depending on how the device was set up and the 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.** These behaviors are also mentioned on page 19 of this User Guide.

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

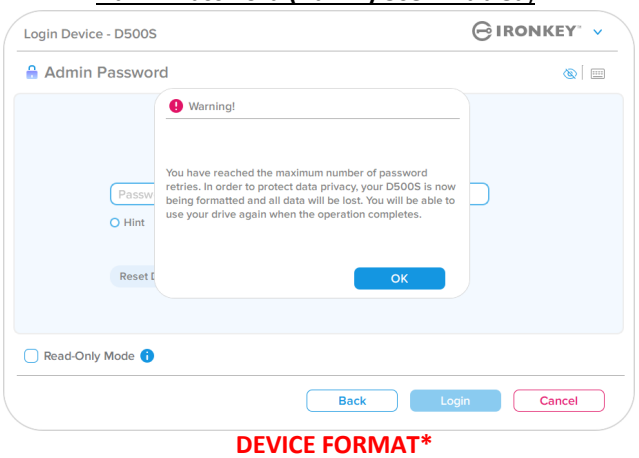
User Password: (Admin/User Enabled)



DEVICE LOCKOUT

Figure 9.3

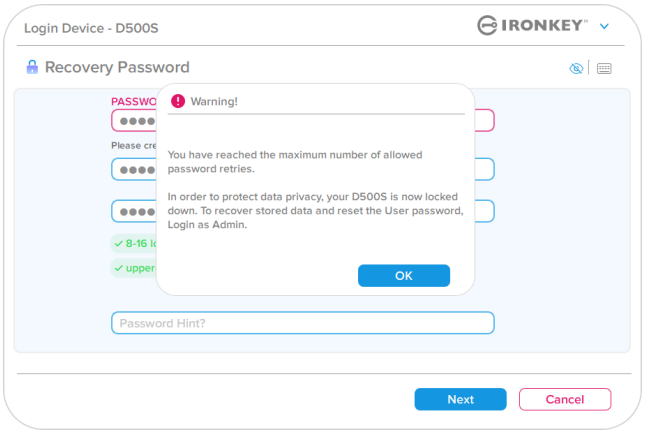
Admin Password (Admin/User Enabled)



DEVICE FORMAT*

Figure 9.4

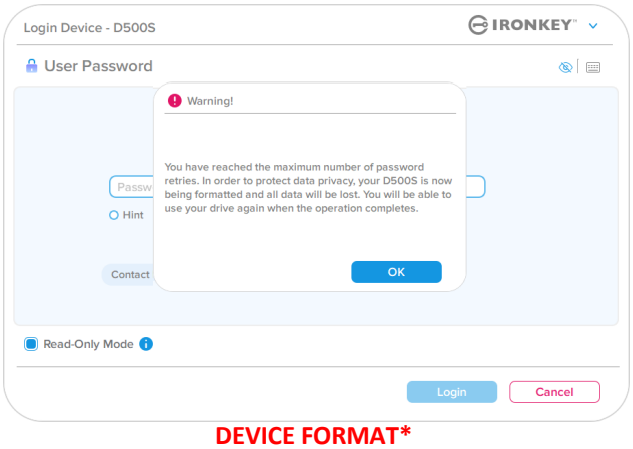
One-Time Recovery: (Admin/User Enabled)



DEVICE LOCKOUT

Figure 9.5

User Password (Admin NOT Enabled)



DEVICE FORMAT*

Figure 9.6

These security measures limit someone (who does not have your password) from attempting countless login attempts and gaining access to your sensitive data (Also known as a Brute-Force attack). If you are the owner of the D500S 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* D500S*' secure data partition.*

Help and Troubleshooting

Reset Device

If you forget your password or need to reset your device, you can click on the '*Reset Device*' button that appears in one of two places depending on how the drive is set up (either on the Admin Login Password menu if Admin/User is enabled, or on the 'User Password' Login menu if Admin/User mode is not enabled) when the D500S Launcher is executed (see *Figure 9.7* and 9.8**)**

- This option will allow you to create a new password, but to protect the privacy of your data, the D500S will be formatted. This means that all of your data will be erased in the process.*

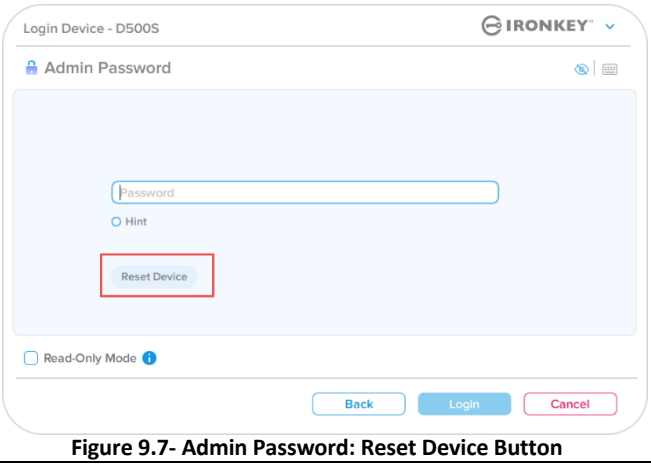


Figure 9.7- Admin Password: Reset Device Button

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

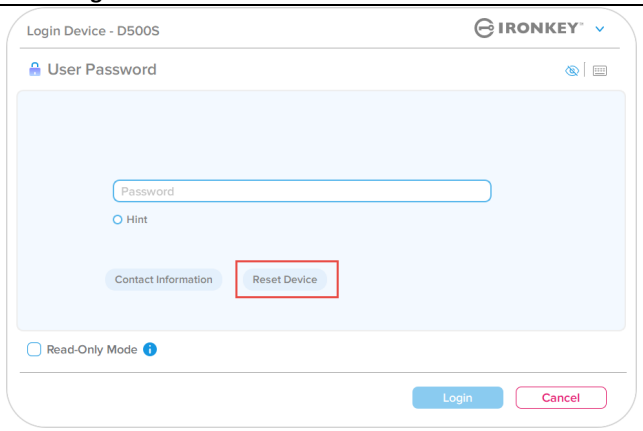


Figure 9.8- User Password (Admin/user not enabled) Reset Device

- If you choose to continue, you will be prompted to the Initialize screen where you can enable 'Admin and User modes' and enter your new password based on the password option you choose (Complex or Passphrase). The hint is not a mandatory field, but it can be useful in providing a clue as to what the password is, should the password ever be forgotten.

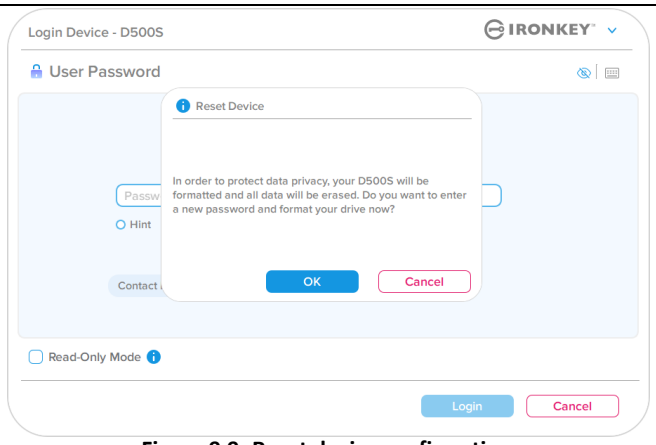


Figure 9.9- Reset device confirmation

Help and Troubleshooting

Drive letter conflict: Windows operating systems

- As mentioned in the '*System Requirements*' section of this manual (on page 3), the D500S 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 D500S 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 D500S requires two consecutive drive letters AFTER the last physical disk that appears before the 'gap' in drive letter assignments (see *Figure 9.10*.) This does NOT pertain to network shares because they are specific to user- profiles and not the system hardware profile itself, thus appearing available to the OS.

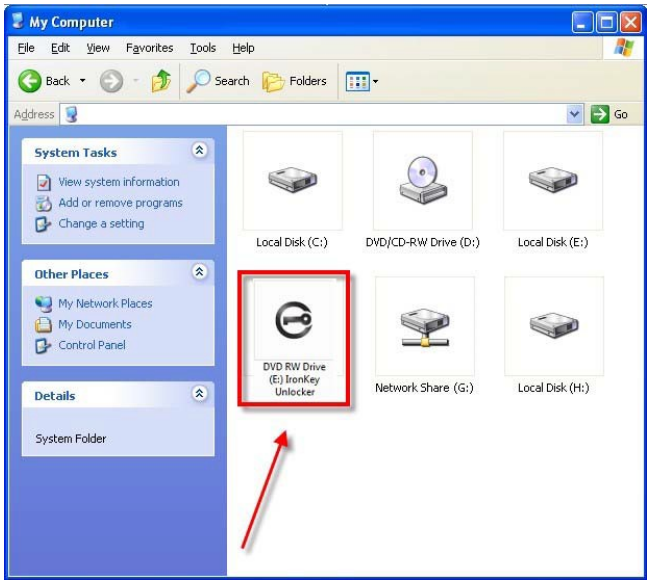


Figure 9.10- Drive Letter example

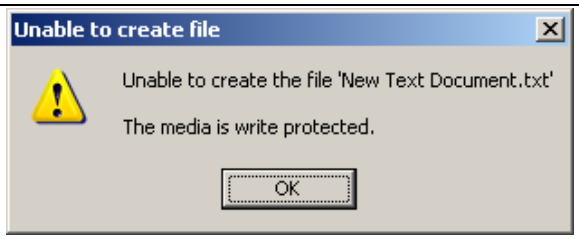
In this example (Figure 9.10), the D500S uses drive F:, which is the first available drive letter after drive E: (the last physical disk before the drive letter gap.) Because letter G: is a network share and not part of the hardware profile, the D500S may attempt to use it as its second drive letter, causing a conflict.

If there are no network shares on your system and the D500S 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 10 and 11 so you may not come across this issue, but if you are unable to resolve the conflict, please contact Kingston's Technical Support Department or visit Kingston.com/support for further assistance.

Help and Troubleshooting

Error messages

Unable to create file: This error message will appear when attempting to CREATE a file or folder ON the secure data partition while logged in under Read-Only mode.	 **Figure 9.11 – Unable to Create File Error**
Error Copying File or Folder: This error message will appear when attempting to COPY a file or folder TO the secure data partition while logged in under Read-Only mode.	 **Figure 9.12 – Error Copying File or Folder Error**
Error Deleting File or Folder: This error message will appear when attempting to DELETE a file or folder FROM the secure data partition while logged in under Read-Only mode.	 **Figure 9.13 – Error Deleting File or Folder Error**

Note: If you are ever logged in under Read-Only mode and wish to unlock the device with full read/write access to the secure data partition, you must shutdown D500S and log back in, leaving the 'Read-Only Mode' checkbox unchecked prior to login.

Device Usage (Linux environment)

With the various distributions of Linux available today, the 'look and feel' of their interfaces may vary from one version to the next. However, the general command set used in the terminal application is very similar and can be referenced in the Linux instructions that follow. The screenshot examples in this section were created in a 64-bit environment.

Certain distributions of Linux will require super-user (root) privileges in order to execute the D500S commands properly in the terminal application window.

Important Notes before proceeding:

1.) **D500S does not support Device initialization on Linux and will need to be set up and configured on a supported Windows or macOS system before the drive can be used on a Linux machine.**

2.) **Linux login only supports the use of Complex passwords. Passphrase password login is not supported for Linux login.**

3.) **D500S feature support on Linux is limited. Features such as One-Time Recovery password, Crypto-Erase Password, Admin/User password resets and toggling read-only mode are not supported on Linux.**

The D500S Comes with 4 commands that can be used in Linux:

lkd500s_about	Shows the 'About D500S' Info.
lkd500s_login	Allows you to login to the drive.
lkd500S_logout	Allows you to safely and securely logout of the D500S drive.
lkd500S_resetdevice	Performs a device crypto-erase and resets the drive to an out of box state, permanently deleting all data and files stored on the drive.

NOTE: To execute these commands, you must open a "Terminal" application window and navigate to the folder where each of the files exist. Each command must be preceded by the following two characters: './' (a period and a forward slash.)

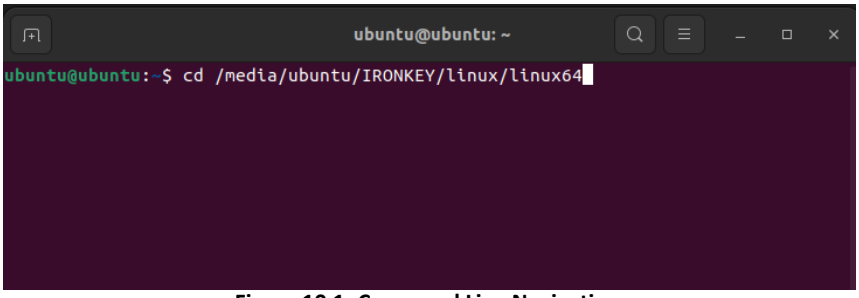
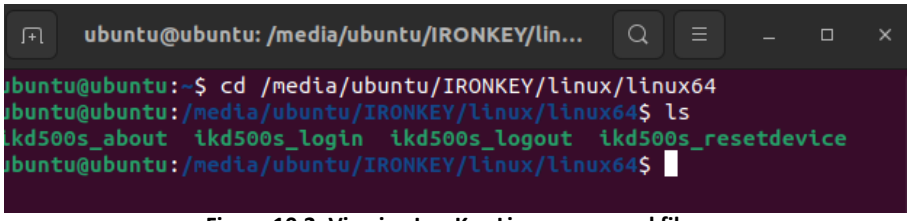
Example of how to navigate to the IronKey Linux Commands path:

For 32 bit Linux Users:	Open a "Terminal" application window and change the current directory to **/media/ubuntu/IRONKEY/linux/linux32$** by typing the following command at the prompt: **cd /media/ubuntu/IRONKEY/linux/linux32** (and then press ENTER.)
For 64 bit Linux Users:	Open a "Terminal" application window and change the current directory to **/media/ubuntu/IRONKEY/linux/linux64**$ by typing the following command at the prompt: **cd /media/ubuntu/IRONKEY/linux/linux64** (and then press ENTER.)

Device Usage (Linux Environment)

Note: If the IRONKEY volume is not loaded automatically by the operating system, you will need to load the volume manually in a terminal window using the Linux 'mount' command. Please refer to the Linux documentation for your specific OS distribution or favorite on-line support site for proper syntax and command options. Some Linux distributions may require you to input username to run commands i.e. "ubuntu" in the above examples.

Locating and viewing IronKey D500S Linux command files:

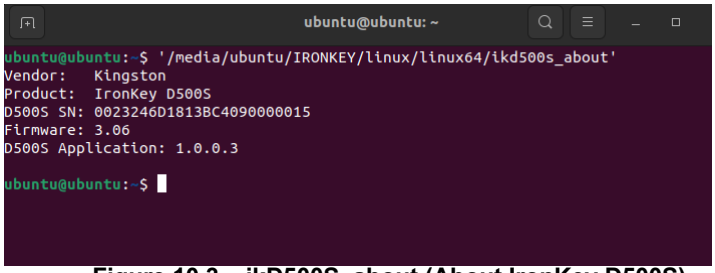
Once the D500S is connected to your computer and recognized by the operating system, change directory to the D500S volume by typing the command at the terminal prompt. (Figure 10.1) **Note:** The screenshots and instructions in this section utilize the linux64 folder (signifying 64-bit) for purposes of demonstrating use of the D500S device in the Linux OS. Keep in mind if you are using the 32-bit version of Linux, simply navigate to and use the respective 32-bit folder in place of the 64-bit folder, i.e., linux32 rather than linux64.)	 **Figure 10.1- Command Line Navigation**
Use the **ls** (list) command at the current prompt and press ENTER. This will provide you with a list of files and/or folders in the linux64 folder. You will then see the four IronKey Linux commands listed (Figure 10.2) • ikD500S_about • ikD500S_login • ikD500S_logout • ikD500S_resetdevice	 **Figure 10.2- Viewing IronKey Linux command files**

Note: Commands and folder (directory) names are case-sensitive, i.e. 'linux64' is NOT the same as 'Linux64.' Syntax must also be typed exactly as shown. Some Linux distributions may require you to input username to run commands i.e. "ubuntu" in this example.)

Device Usage (Linux Environment)

Using D500S commands

About D500S

lkD500S_about (About D500S, Figure10.3) This command will populate information about the D500S such as: • Vendor • Product • D500S Serial number • Firmware version • Software version	 **Figure 10.3 – ikD500S_about (About IronKey D500S)**

D500S login

ikD500S_login

Once the D500S has been initialized on a supported Windows or macOS system, you can access the secure data partition by logging into the device using the D500S password you created.

To do so, follow these steps:

1. Open a 'Terminal' application window.

2. Type the following command at the terminal prompt: **cd /media/ubuntu/IRONKEY/linux/linux64**

3. With the command prompt now at **/media/ubuntu/IRONKEY/linux/linux64$**, type the following command to login to the device: **./ikD500S_login*** and press ENTER. (Note: Commands and folder names are case-sensitive, and syntax must be exact. Also, some distributions may require you to input your username i.e., "ubuntu" in this example.)

4. After a successful login, the secure data volume will open on your desktop, and you can proceed to use the D500S (more information on login behavior continued on next page)

*Note: Certain distributions of Linux will require super-user (root) privileges in order to execute the D500S commands properly in the terminal application window.

Device Usage (Linux Environment)

D500S login (continued)

IkD500S_login (Unlock D500S, Figure 10.4)

Depending on how your drive was set up, during the login process you may be presented with a number of options on how you would like to unlock your drive.

If **Admin/User** password profiles were enabled during initialization, you will be presented with the following login options:

1.) Choose to login as Admin or User
2.) Choose to unlock Admin or User partitions (if enabled)
3.) Enter respective Admin or User login password for device authentication and unlocking.

Note: If Admin/User password profiles were NOT enabled during initialization (User-Only mode), you will only be prompted to only enter your device password for device authentication.

Important: As mentioned previously, Passphrase passwords are not supported on Linux and the D500S will need to be configured with a Complex password for Linux login (Figure 10.5)

Figure 10.4 – ikD500S_login (Unlocking D500S)

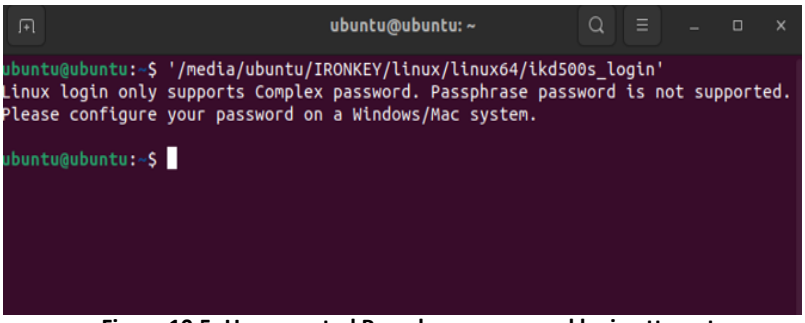


Figure 10.5- Unsupported Passphrase password login attempt.

Device Usage (Linux Environment)

D500S login (continued)

Incorrect login password behavior
During the login process, if an incorrect password is entered, you will be given another opportunity to enter the password. However, there is a built-in security feature that tracks the number of failed login attempts. If this number reaches the pre-configured value of 10 failed attempts for either the Admin or User logins, the behavior will be as follows:

Admin/User passwords enabled

- **User Login:** User lockout, login as Admin required. (Figure 10.6) Note: The User password can be reset by the Admin login on a supported Windows or macOS system.

- **Admin Login:** Drive crypto-erase, all data is lost forever. Device reset required. (Figure 10.7)

User-Only Mode (admin/User not enabled)

- **User Login**: Drive crypto-erase, all data is lost forever. Device reset required. Figure 10.7)

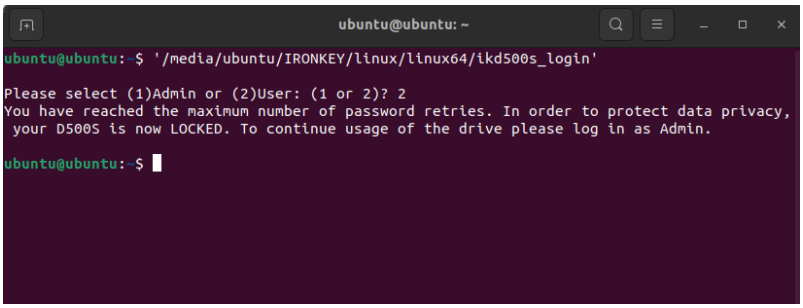


Figure 10.6- User login Lockout, Admin/user Passwords enabled

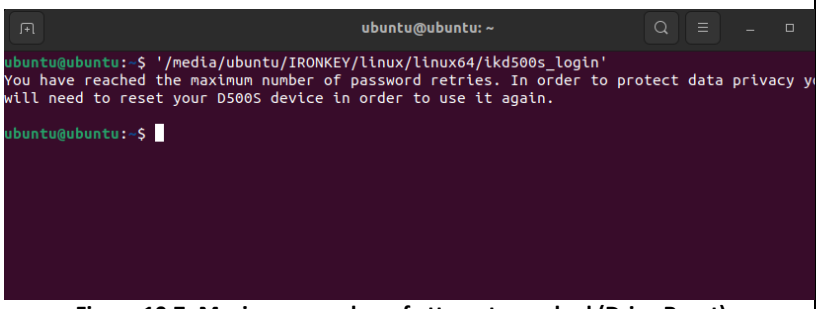


Figure 10.7- Maximum number of attempts reached (Drive Reset)

D500S Logout

IkD500S_logout (lock device)

When you are finished using the D500S, log out of the device and secure your data. To do so, follow the same steps referenced on page 39 and use the following command logout of the device properly: **./ikD500S_logout** and press ENTER (Note: Commands and folder names are case-sensitive and syntax must be exact. (Figure 10.8)

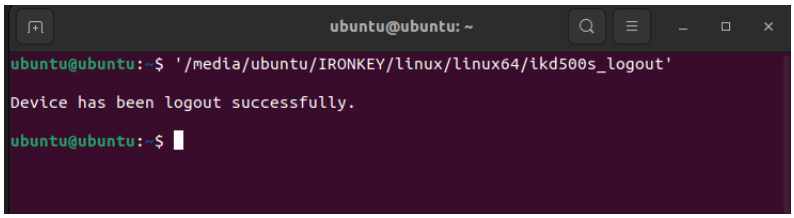


Figure 10.8- D500S Logout

Device Usage (Linux Environment)

D500S Device Reset

ikD500S_resetdevice

As mentioned previously on page 41, In the event the User/Admin passwords are forgotten, the Reset Device command can be used to reset the drive so it can be used again. This process will allow you to create a new password, but in order to protect the privacy of your data, the D500S will crypto-erase the drive format the secure data partition**. This means that all of your data will be lost.**

To use the Reset Device command, follow the same steps referenced on Page 39 and use the following command logout of the device properly: **./ikD500S_resetdevice** and press ENTER (Note: Commands and folder names are case-sensitive and syntax must be exact. (Figure 10.9)

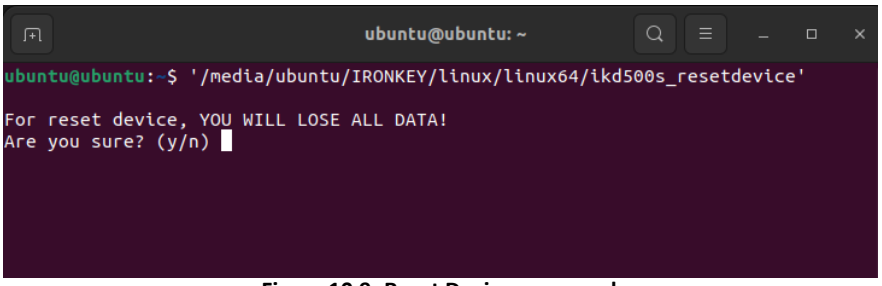


Figure 10.9- Reset Device command

Once the Reset Device command has been used, you will be prompted to create a new Complex password that must contain:

- 8 - 16 Characters long and contain at least (3) of the following criteria options:

  -UPPER CASE
  -lower case
  -numeric
  -Special Characters (!,$,etc.)

(Figure 10.10)

Note: The Reset Device command will initialize the drive in User-Only mode (Single password, single user). To enable Admin/User login password profiles, the D500S will need to be set up on a supported Windows or macOS system to access that option.

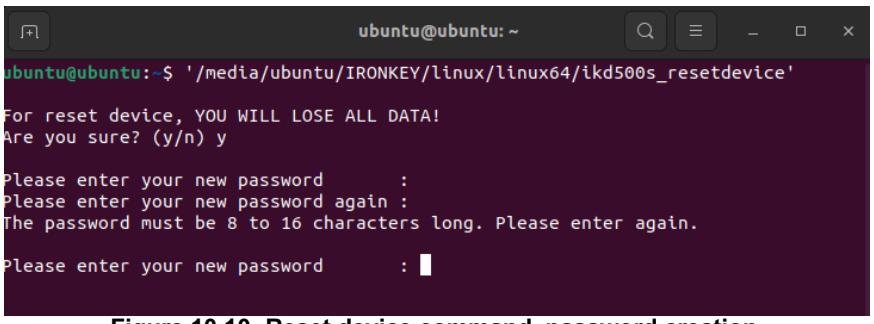


Figure 10.10- Reset device command, password creation

UNIDAD FLASH USB 3.2 Gen 1 PROTEGIDA IRONKEY™ D500S

Manual del usuario

Índice

Figura 1 – IronKey D500S

Introducción

El dispositivo Kingston IronKey D500S es una unidad USB con seguridad de grado militar, que se basa en las funciones que han convertido a IronKey en un sinónimo de protección de información sensible. Se trata de un modelo con homologación FIPS 140-3 de Nivel 3 (pendiente), que incluye mejoras de la seguridad de NIST, que requieren actualizaciones de procesador protegidas para una mayor seguridad. El cifrado y el descifrado se realizan íntegramente en la D500S, sin dejar huellas en el sistema anfitrión, por lo cual es inmune a los detectores de contraseña en la memoria. Conjuntamente con el cifrado XTS-AES de 256 bits basado en hardware, incorpora también una sólida carcasa de zinc, estanca al agua* y al polvo*, resistente al aplastamiento y rellena de epóxido para proteger a los componentes internos contra ataques de penetración.

D500S admite varias opciones de contraseña (Administrador, Usuario, Recuperación de un solo uso y Criptoborrado), con modos Complejo o Frase de contraseña**. La opción de múltiples contraseñas refuerza la capacidad de recuperar el acceso a los datos si se olvida alguna de las contraseñas. Además de admitir las tradicionales contraseñas complejas, el modo de Frase de contraseña permite códigos PIN numéricos, frases, listas de palabras e incluso letras de canciones, de entre 10 y 128 caracteres de longitud. El administrador puede habilitar a un usuario, crear dobles particiones de datos de tamaño personalizado para separar los archivos de inicio de sesión de administrador/usuario, habilitar una contraseña de recuperación de un solo uso, una contraseña de criptoborrado y restablecer la contraseña de usuario para volver a posibilitar el acceso a los datos.

Para ayudar a introducir la contraseña, puede activarse el símbolo de “ojo”  , con el objeto de ver la contraseña que se está escribiendo, reduciendo la cantidad de errores que pueden conllevar intentos fallidos de inicio de sesión. Para una mayor tranquilidad, la D500S incorpora un firmware de firma digital, lo cual la hace inmune a ataques de malware BadUSB y protege contra ataques de fuerza bruta que intentan adivinar las contraseñas. La protección contra ataques de fuerza bruta bloquea las contraseñas de recuperación de Usuario o de Un solo uso tras la introducción de 10 contraseñas no válidas consecutivas, y un código criptográfico borra el contenido de la unidad si la contraseña de Administrador se introduce incorrectamente 10 veces consecutivas.

Como medida de protección contra software malicioso (malware) en sistemas que no son de confianza, tanto el Administrador como el Usuario pueden establecer el modo Sólo lectura para proteger la unidad contra escritura. Además, el teclado virtual integrado protege las contraseñas contra grabadores de pulsaciones de teclados físicos o virtuales***.

Las pymes pueden utilizar la función Rol de administrador para administrar localmente sus unidades. Por ejemplo, utilizar Administrador para configurar o restablecer contraseñas de Usuario o de Un solo uso, recuperar el acceso a los datos en unidades bloqueadas y cumplir las leyes y normativas toda vez que se requiera una investigación forense.

La D500S ofrece numerosas opciones de personalización, es compatible con TAA/CMMC y se ensambla en EE.UU.

El dispositivo D500S está respaldado por una garantía limitada de 5 años y por la asistencia técnica gratuita de Kingston.

* Consulte las especificaciones de la ficha técnica. El producto debe estar limpio y seco antes de su uso.
** Los sistemas Linux son incompatibles con el modo de Frase de contraseña.
*** Teclado virtual: solamente admite inglés (EE.UU.) en sistemas Microsoft Windows y macOS.

Funciones de IronKey D500S

- Homologación FIPS 140 de Nivel 3 (pendiente) con cifrado por hardware XTS-AES de 256 bits (el cifrado no puede desactivarse nunca)
- Protección contra ataques de Fuerza bruta y de BadUSB
- Opciones de contraseñas múltiples
- Modos de contraseña compleja o frase de contraseña
- Exclusiva opción de doble partición y contraseña de criptoborrado
- Botón de ojo para mostrar las contraseñas introducidas y reducir los intentos fallidos de inicio de sesión.
- Teclado virtual para ayudar en la protección contra grabadores de pulsaciones de teclados físicos y virtuales
- Dobles ajustes de sólo lectura (protección contra escritura) para impedir que la unidad sea modificada o alterada por el malware
- Las pymes pueden gestionar localmente las unidades utilizando el Rol de administrador
- Compatible con Windows, macOS y Linux (consulte información detallada en la ficha técnica)

Acerca de este manual

Este Manual de usuario explica las características y uso de IronKey D500S, y está basado en la imagen de fábrica sin ninguna personalización implementada.

Requisitos del sistema

Plataforma PC • Intel, AMD y Apple M1 SOC • 15 MB de espacio disponible en disco • Puerto USB 2.0 - 3.2 disponible • Dos letras de unidad consecutivas tras la última unidad física*. ***Nota:** Consulte 'Conflicto entre letras de unidad' en la página 35.	**Compatibilidad con sistemas operativos** • Windows 11 • Windows 10
Plataforma Mac • 15 MB de espacio disponible en disco • Puerto USB 2.0 - 3.2.	**Compatible con el sistema operativo Mac** • macOS macOS 11.x - 14.x
Plataforma Linux • 5 MB de espacio disponible en disco • Puerto USB 2.0 - 3.2.	**Compatible con el sistema operativo Linux** • Linux Kernel v4.4+

Recomendaciones

Para garantizar que el dispositivo D500S reciba suficiente alimentación eléctrica, insértelo directamente en un puerto USB de su ordenador portátil o de sobremesa, tal y como puede verse en la *Figura 1.1*. Evite conectar la unidad D500S a un dispositivo periférico que pueda disponer de puerto USB, como un teclado o un concentrador alimentados por USB, tal y como puede verse en la *Figura 1.2*.

Figura 1.1 – Uso recomendado

Figura 1.2 – Uso no recomendado

Uso del sistema de archivos correcto

La unidad IronKey D500S viene preformateada con el sistema de archivos FAT32. Funcionará con los sistemas operativos Windows, macOS y Linux*. Sin embargo, podría haber otras opciones que puedan emplearse para formatear la unidad manualmente, como NTFS para Windows y exFAT. Si fuese necesario, podrá reformatear la partición de datos, aunque los datos se perderán al reformatear la unidad.

Recordatorios de uso

Para mantener protegidos sus datos, Kingston le recomienda:

- Ejecute una detección de virus en el ordenador antes de configurar y utilizar la unidad D500S en un sistema diana
- Si utiliza la unidad en un sistema público o con el cual no esté familiarizado, quizá convenga ajustarla al modo de Sólo lectura para ayudar a protegerla contra el malware
- Bloquee el dispositivo cuando no lo esté utilizando
- Expulse el dispositivo antes de desenchufarlo
- Nunca desenchufe el dispositivo cuando el LED esté iluminado Esto podría dañar la unidad, con el consiguiente riesgo de tener que reformatearla y que se borren sus datos.
- Nunca comparta la contraseña de su dispositivo con nadie.

Busque la información y las actualizaciones más recientes

Consulte en kingston.com/support las actualizaciones más recientes de la unidad, preguntas más frecuentes, documentación e información adicional.

NOTA: Aplique a la unidad solamente las actualizaciones más recientes (si estuviesen disponibles). Cambiar el software de la unidad a una versión anterior es incompatible, y potencialmente puede provocar la pérdida de los datos guardados o estropear su funcionalidad. Para cualquier duda o problema, póngase en contacto con el servicio de Asistencia técnica de Kingston.

*** La unidad D500S es incompatible con la inicialización de serie de Linux, y deberá ser totalmente inicializada y configurada en un sistema Windows o macOS compatible antes de poder utilizarla en Linux. Encontrará información adicional en la sección de Linux de este manual, en la página 37**

Buenas prácticas para la configuración de contraseñas

La unidad D500S incorpora sólidas contramedidas de seguridad. Entre las mismas se incluye la protección contra ataques de fuerza bruta, que impedirá que el atacante siga intentando averiguar las contraseñas limitando los intentos a 10 consecutivos. Al alcanzarse dicho límite, la unidad D500S borrará automáticamente los datos cifrados y procederá a reformatearse a su estado original de fábrica.

Contraseñas múltiples
D500S admite múltiples contraseñas, una función importante que permite la protección contra pérdidas de datos si se olvida una o más contraseñas. Cuando están activadas todas las opciones de contraseñas, la unidad D500S puede admitir tres contraseñas que podrá utilizar para recuperar datos: de Administrador, de Usuario y de Un solo uso.

D500S permite seleccionar dos contraseñas principales: una contraseña de Administrador (denominada Admin) y una contraseña de Usuario. El Administrador puede acceder a la unidad en cualquier momento y configurar las opciones del usuario. Sería una especie de súper usuario. Además, el Administrador puede configurar la contraseña de Recuperación de un solo uso para permitir a un usuario iniciar sesión y restablecer su contraseña.

El usuario puede acceder a la unidad aunque, en comparación con el Administrador, sus privilegios son limitados. Si se olvida una de las dos contraseñas, podrá utilizarse la otra para acceder y recuperar los datos. A continuación, la unidad podrá reconfigurarse para tener dos contraseñas. Es importante configurar AMBAS contraseñas, y guardar la contraseña Admin en un lugar seguro mientras se esté utilizando la contraseña de usuario. El usuario puede utilizar la contraseña de Recuperación de un solo uso si fuese necesario.

Si se olvidan o extravían todas las contraseñas, no habrá ningún otro modo de acceder a los datos. Kingston no podrá recuperar estos datos, ya que la protección no tiene 'puertas traseras'. Kingston recomienda también guardar los datos en otro(s) soporte(s). La unidad D500S podrá ser restablecida y reutilizada, pero en tal caso los datos anteriores quedarán borrados para siempre.

Modos de contraseñas
Además, la unidad D500S admite dos modos de contraseñas diferentes:

Complejo
Una contraseña compleja debe incorporar entre 8 y 16 caracteres, de los cuales al menos 3 deben ser los siguientes:

- Caracteres alfabéticos en mayúsculas
- Caracteres alfabéticos en minúsculas
- Cifras
- Caracteres especiales

Frase de contraseña
D500S admite frases de contraseña de entre 10 y 128 caracteres. Una frase de contraseña no debe atenerse a ninguna regla, aunque si se utiliza adecuadamente permite obtener un alto nivel de protección de contraseñas.

Básicamente, una frase de contraseña es cualquier combinación de caracteres, incluyendo caracteres de otros idiomas. Al igual que la unidad D500S, el idioma de la contraseña debe coincidir con el idioma seleccionado para el dispositivo. Posibilita seleccionar varias palabras, una frase, la letra de una canción, el verso de una poesía, etc. Las frases de contraseña adecuadas se encuentran entre los tipos de contraseñas más difíciles de adivinar para los intrusos, al tiempo que son más fáciles de recordar para los usuarios.

Configuración de Mi dispositivo

Para asegurarse de disponer de suficiente alimentación para la unidad USB cifrada IronKey, insértela directamente en un puerto USB 2.0/3.0 del ordenador de sobremesa o portátil. Evite conectarlo a dispositivos periféricos que dispongan de un puerto USB, como un teclado o un concentrador alimentado a través de USB. La configuración inicial del dispositivo debe realizarse en un sistema operativo compatible con Windows o macOS.

Opciones del dispositivo (entorno de Windows)

Introduzca la unidad USB cifrada IronKey en alguno de los puertos USB disponibles de su ordenador de sobremesa o portátil, y espere hasta que Windows lo detecte.

- Los usuarios de Windows 10/11 recibirán una notificación del controlador del dispositivo. (*Figura 3.1*)

Figura 3.1 – Notificación del controlador del dispositivo

- Una vez que haya concluido la detección del nuevo hardware, seleccione la opción IronKey.exe dentro de la partición Unlocker, que encontrará en el Explorador de archivos. (*Figura 3.2*)
- Tenga en cuenta que la letra de la partición podrá variar en función de la siguiente letra de unidad libre. La letra de la unidad podrá variar en función de los dispositivos que estén conectados. En la siguiente imagen, la letra de la unidad es (E:)

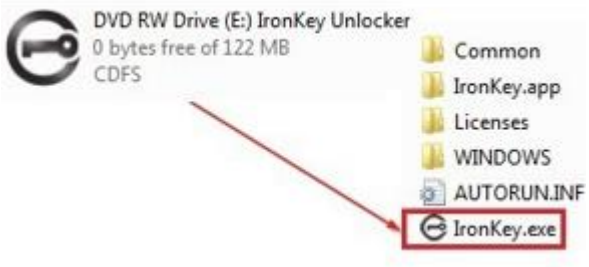


Figura 3.2 – Ventana del Explorador de archivos/IronKey.exe

Opciones del dispositivo (entorno de macOS)

Inserte la unidad D500S en un puerto USB disponible de su ordenador portátil o de sobremesa, y espere a que el sistema operativo Mac lo detecte. Cuando lo haga, verá que en el escritorio aparece un volumen 'IRONKEY'. (*Figura 3.3*)

- Haga doble clic en el icono del CD-ROM IronKey.
- Seguidamente, haga doble clic en el icono de la aplicación IronKey.app, que encontrará en la ventana que puede verse en la Figura 3.3. De este modo comenzará el proceso de inicialización.

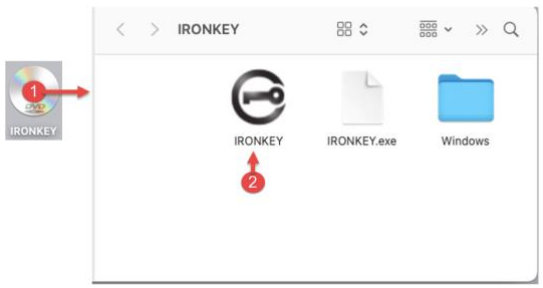
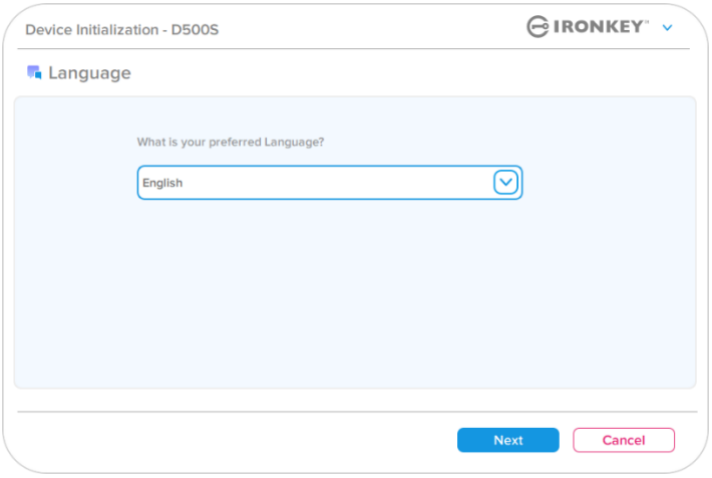
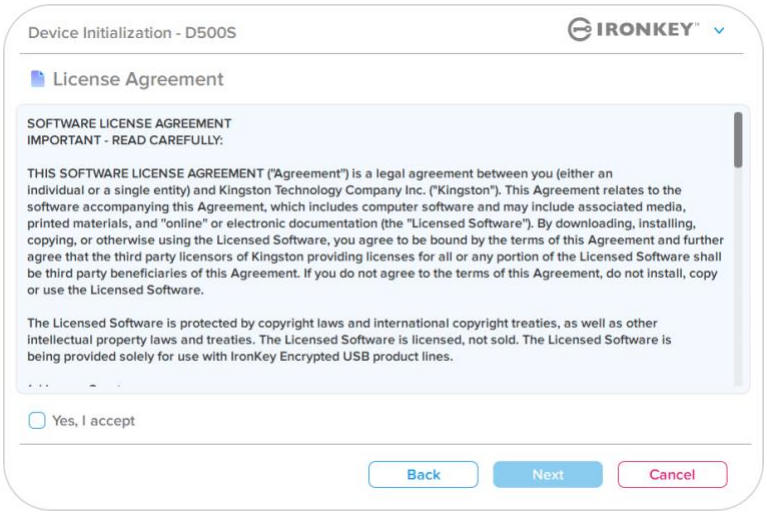


Figura 3.3 – Volumen IronKey

Inicialización del dispositivo (entornos de Windows y de macOS)

Idioma y CLUF

Seleccione el idioma de su preferencia en el menú desplegable y, a continuación, haga clic en **Siguiente** (*Figura 4.1*)	 **Figura 4.1: Selección de idioma**
Revise el Contrato de licencia y, a continuación, haga clic en **Siguiente**. **Nota:** Debe aceptar el Contrato de licencia antes de continuar; de lo contrario el botón **Siguiente** permanecerá desactivado. (*Figura 4.2*)	 **Figura 4.2 – Acuerdo de licencia**

Inicialización del dispositivo

Selección de contraseñas

En la pantalla de solicitud de contraseña podrá crear una contraseña para proteger los datos contenidos en la unidad D500S, utilizando los modos Compleja y Frase de contraseña (*Figuras 4.3- 4.4*). Además, en esta pantalla podrá activar las opciones de contraseñas múltiples de Administrador y Usuario. Antes de continuar con la selección de contraseñas, lea detenidamente la sección Activación de contraseñas de Administrador / Usuario para entender debidamente estas funciones.

Nota: Una vez que haya elegido el modo Compleja o Frase de contraseña, no podrá cambiarlo a menos que restablezca el dispositivo.

Para empezar con la selección de contraseña, escríbala en el campo 'Contraseña'; seguidamente, repítala en el campo 'Confirmar contraseña'. La contraseña que cree deberá cumplir los siguientes criterios; de lo contrario el proceso de inicialización no le permitirá continuar:

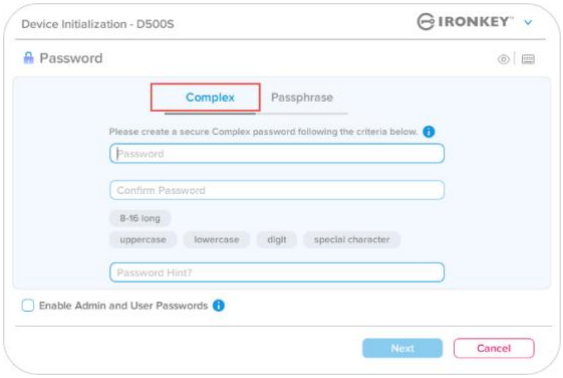
<table>
<tr>
<td>Contraseña compleja
Debe contener al menos 8 caracteres (hasta un máximo de 16 caracteres).
Debe incluir tres (3) de los siguientes tipos de caracteres:
Mayúsculas
Minúsculas
Carácter numérico
Caracteres especiales (!, $, &, etc.)</td>
<td> 

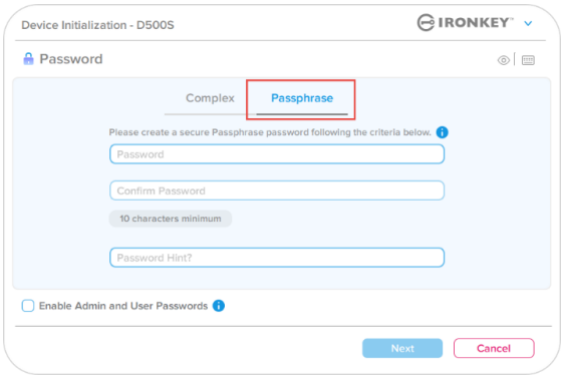
Figura 4.3 – Contraseña compleja</td>
</tr>
<tr>
<td>Frase de contraseña
Debe contener:
10 caracteres como mínimo
128 caracteres como máximo</td>
<td> 

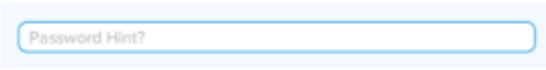
Figura 4.4 – Frase de contraseña</td>
</tr>
<tr>
<td>Indicio de contraseña (opcional)
El indicio de contraseña podría resultarle útil proporcionándole una pista en caso de que olvidara su contraseña.
Nota: El indicio NO PUEDE ser idéntico a la contraseña propiamente dicha.</td>
<td> 

Figura 4.5 – Campo Indicio de contraseña</td>
</tr>
</table>

Inicialización del dispositivo

Contraseñas válidas y no válidas

En el caso de contraseñas **válidas**, las casillas de criterios de contraseña se iluminarán en **verde** cuando se satisfagan los criterios. (Véanse las *Figuras 4.6a-b*)
Nota: Una vez satisfechos como mínimo de tres criterios de la contraseña, el cuadro del cuarto criterio se tornará gris, indicando que dicho criterio no es opcional (*Figura 4.6b*)

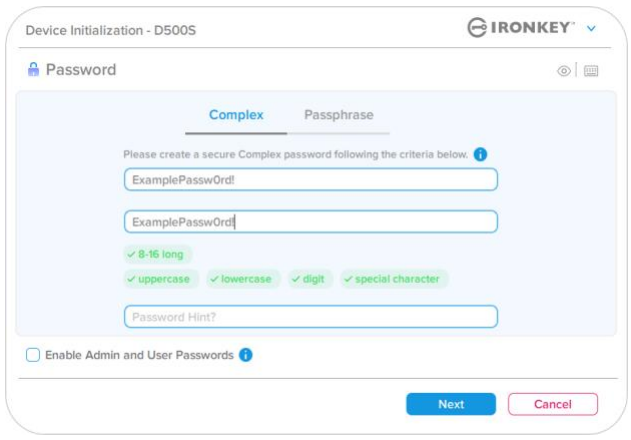


Figura 4.6a – Se cumple la condición de la Contraseña compleja

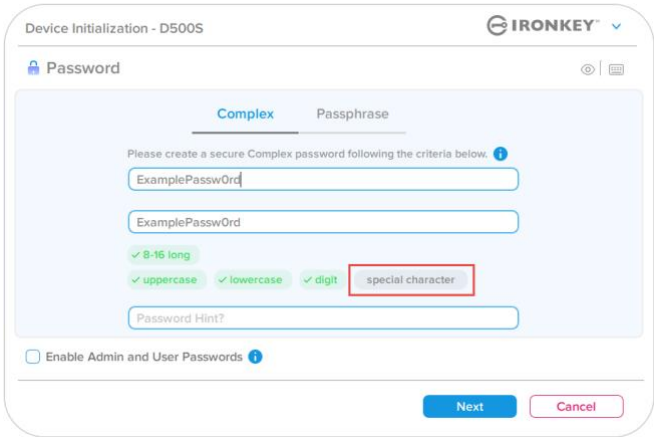


Figura 4.6b – Condición opcional de la Contraseña compleja

En el caso de las contraseñas **no válidas**, los cuadros de Criterios de contraseña se iluminarán en **rojo** y el botón Siguiente quedará desactivado hasta que se satisfagan los requisitos mínimos.

Esto es de aplicación tanto a las contraseñas complejas como a las frases de contraseña.

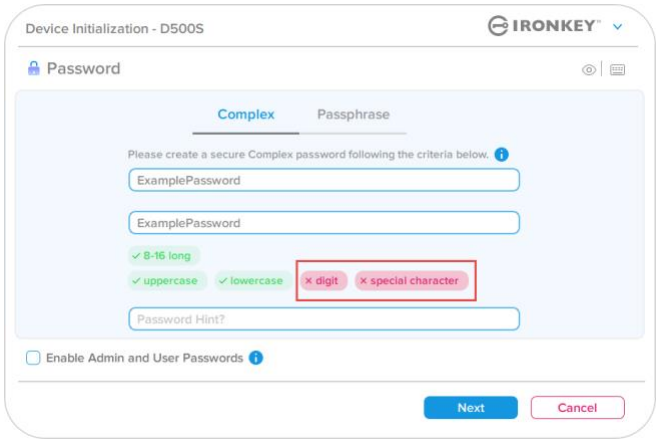


Figura 4.7 – No se satisfacen las condiciones de la contraseña

Inicialización del dispositivo

Teclado virtual

La unidad D500S incorpora un teclado virtual que puede utilizarse como protección contra las grabaciones de pulsaciones del teclado.

- Para utilizar el **Teclado virtual**, busque el botón del teclado en la esquina superior derecha de la pantalla **Inicialización del dispositivo**, y selecciónelo.

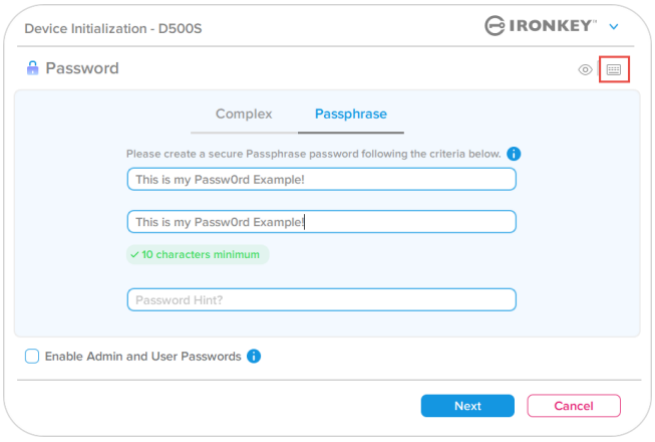


Figura 4.8 – Activación del teclado virtual

- Una vez que aparezca el teclado virtual, también podrá activar la **protección contra pulsaciones de pantalla**. Cuando utilice esta función, todas las teclas quedarán en blanco durante unos instantes. Es normal: así se impide que los grabadores de pulsaciones de pantalla detecten cuáles teclas ha pulsado.

- Para que esta función resulte todavía más sólida, también podrá optar por aleatorizar el teclado virtual seleccionando **aleatorizar**, en la esquina inferior derecha del teclado. La opción Aleatorizar ordenará el teclado de manera aleatoria.

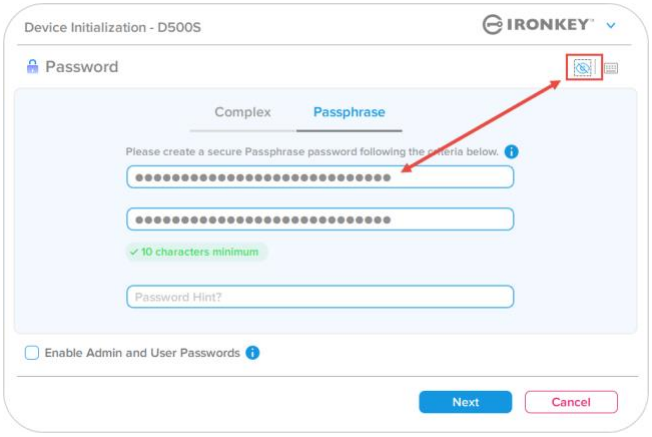
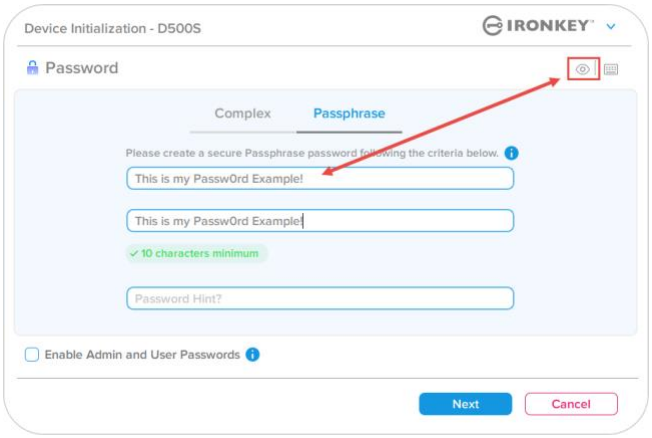
Figura 4.9 – Protección contra grabación de pulsaciones / Aleatorizar

Inicialización del dispositivo

Alternador de visibilidad de contraseña

De manera predeterminada, al crear una contraseña la cadena de la misma será visible en el campo a medida que la vaya escribiendo. Si desea 'ocultar' la cadena de contraseña mientras la escribe, podrá hacerlo pulsando alternativamente el 'ojo' situado en el costado superior derecho de la ventana Inicialización del dispositivo.

Nota: Una vez inicializado el dispositivo, el campo de la contraseña quedará 'oculto' de manera predeterminada.

Para **ocultar** la cadena de la contraseña, haga clic en el icono gris. 	 **Figura 4.10 – Pulse para 'ocultar' la contraseña**
Para **mostrar** la contraseña oculta, haga clic en el icono azul. 	 **Figura 4.11 – Pulse para 'mostrar' la contraseña**

Inicialización del dispositivo

Contraseñas de administrador y de usuario

Habilitando las contraseñas de Administrador y de Usuario podrá aprovechar la funcionalidad de múltiples contraseñas, en la cual el Rol de administrador puede gestionar ambas cuentas. Al seleccionar **'Habilitar contraseñas de Admin y de Usuario'** dispondrá de un método alternativo de acceder a la unidad en caso de olvido de la contraseña.

Por otra parte, teniendo las **contraseñas de Admin y de Usuario** habilitadas, también podrá acceder a:

- Configuración de Doble partición
- Contraseña de recuperación de un solo uso
- Modo forzado de Sólo lectura para inicio de sesión del usuario
- Restablecimiento de contraseña de usuario
- Forzar restablecimiento de contraseña para inicio de sesión de usuario
- Contraseña de criptoborrado

Para obtener más información acerca de estas opciones, vaya a la página 25 de este Manual del usuario.

- Para habilitar las **contraseñas de Administrador y de Usuario**, haga clic en el cuadro situado junto a **'Habilitar contraseñas de Admin y de Usuario'** y seleccione **Siguiente** una vez que haya seleccionado una contraseña válida. (*Figura 4.12*)
- Si esta función está **activada**, la contraseña elegida en esta pantalla será la **Contraseña del Administrador**. Haga clic en **Siguiente** para pasar a la pantalla **Contraseña de Usuario**, desde la cual podrá elegir la contraseña del usuario.

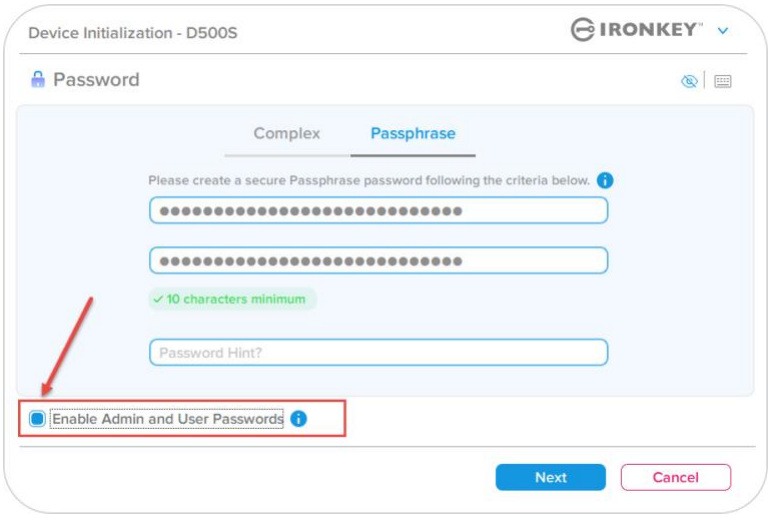


Figura 4.12 – Habilitación de contraseñas de Admin y de Usuario

Nota: La habilitación de contraseñas de administrador y de usuario es opcional.

Si la unidad está configurada con esta función NO activada (casilla sin marca de verificación), estará configurada como unidad de **Único usuario, Una sola contraseña sin funciones de Administrador**. En este manual, esta configuración se denomina Modo de Sólo usuario.

Para continuar con la configuración de Único usuario, Una sola contraseña, mantenga desactivada la casilla de verificación Habilitar **contraseñas de Admin y de Usuario**, y haga clic en **Siguiente** después de haber creado una contraseña válida.

Nota: en el resto de este documento, las 'Contraseñas de Admin y de Usuario' se denominarán **'Rol de administrador'**.

Inicialización del dispositivo

Contraseñas de administrador y de usuario

- Si en la pantalla anterior **habilitó** el Rol de administrador, la siguiente pantalla le pedirá la Contraseña de usuario (*Figura 4.13*). La **Contraseña de usuario** tendrá capacidades limitadas en comparación con la de administrador, y este es un tema que se trata más adelante en este manual (véase la página 23).

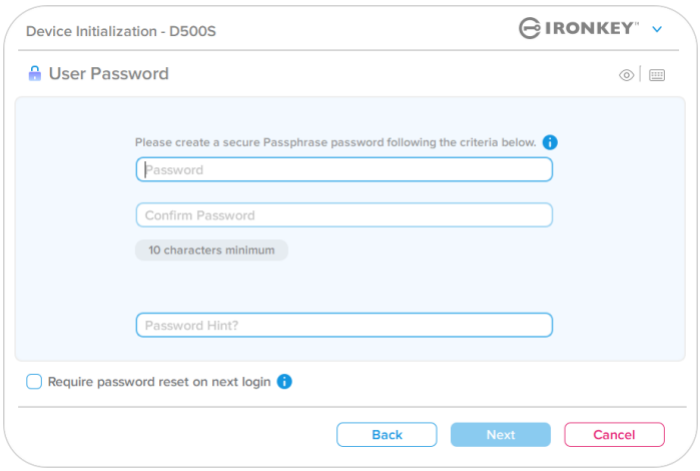


Figura 4.13 - Contraseña de usuario (Admin y Usuario habilitado)

Nota: La opción de contraseña seleccionada (Compleja o Frase de contraseña) se aplicará a la Contraseña del Usuario, la Recuperación de contraseña de un solo uso, la Contraseña de criptoborrado a cualesquiera restablecimientos de contraseña que fuesen necesarios después de la configuración de la unidad. La opción de contraseña elegida solamente podrá cambiarse tras un restablecimiento completo del dispositivo.

- La función **'Requerir restablecimiento de contraseña el próximo inicio de sesión'**, en la esquina inferior izquierda de la *Figura 4.13*, es solamente para la contraseña del Usuario, y puede activarse para obligar al usuario a iniciar sesión utilizando la contraseña temporal establecida por el Administrador durante el proceso de inicialización. Con posterioridad, una vez autenticada la unidad con dicha contraseña temporal, podrá cambiarla por la contraseña de su preferencia. Esto resulta útil cuando se entrega la unidad para que la use otra persona.

  Nota: Por motivos de seguridad, la nueva contraseña no podrá ser idéntica a la contraseña temporal.

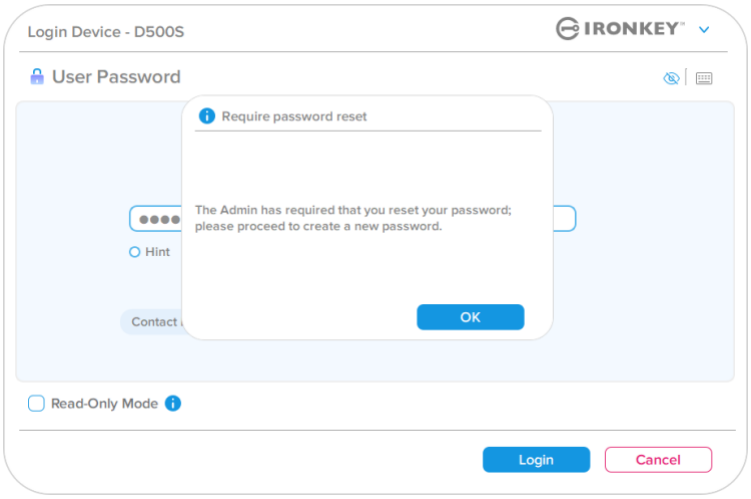


Figura 4.14 - Requerir restablecimiento de contraseña el próximo inicio de sesión (para la contraseña del Usuario)

Inicialización del dispositivo

Dobles particiones

La unidad IronKey D500S permite crear dos particiones separadas, de tamaño personalizado, entre el administrador y el usuario. Si se activa esta función, con el inicio de sesión de administrador tendrá acceso tanto a la partición de usuario como a la de administrador, en tanto que con el inicio de sesión de usuario tendrá acceso **solamente** a la partición de usuario. Esta función resulta útil para separar de manera segura los privilegios de acceso a datos y a archivos entre administrador y usuario, o bien para ocultar un almacenamiento de archivos e impedir la exposición a archivos innecesarios o sistemas no confiables. Además, si se desea es posible ajustar el volumen de las particiones entre administrador y usuario.

NOTA: Esta función es opcional y puede desactivarse dejando sin marcar la casilla de verificación "Habilitar doble partición" durante la configuración (*Figura 4.15*)

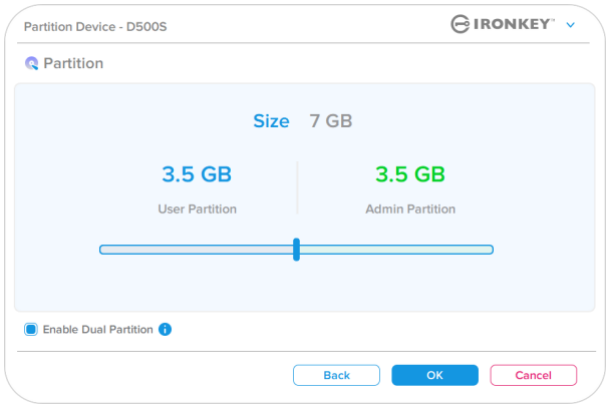


Figura 4.15- Dispositivo de partición

Para ajustar y asignar los volúmenes de partición entre usuario y administrador, mueva el mando deslizante hacia la izquierda o hacia la derecha, según proceda (*Figura 4.16*).

- Las particiones pueden ajustarse en incrementos de 0,5 GB.
- Las dimensiones de las particiones dependerán de la capacidad total disponible en la partición oculta.
- De manera predeterminada, el mando deslizante de Doble partición dividirá de manera uniforme el almacenamiento entre administrador y usuario, hasta que sea ajustado manualmente.
- El volumen mínimo de partición que podrá asignarse es de 1 GB.

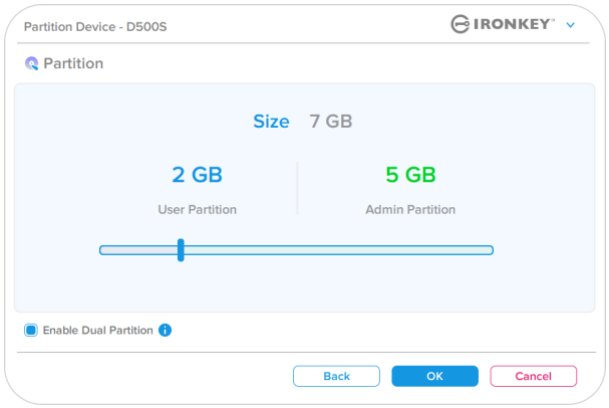


Figura 4.16 — Dispositivo de partición con el mando deslizante ajustado

Inicio de sesión de administrador

Una vez que haya configurado plenamente la unidad con las dobles particiones activadas, se abrirá la pantalla de inicio de sesión de administrador, con una opción para desbloquear la unidad para acceder a la partición del administrador, O BIEN a la partición del usuario, en cada inicio de sesión. (*Figura 4.17*)

NOTA: Puede seleccionarse una sola partición cada vez. No es posible desbloquear al mismo tiempo las particiones de usuario y de administrador.

Con esta opción no se abrirá la pantalla de inicio de sesión de usuario, y quedará automáticamente bloqueada la partición de usuario.

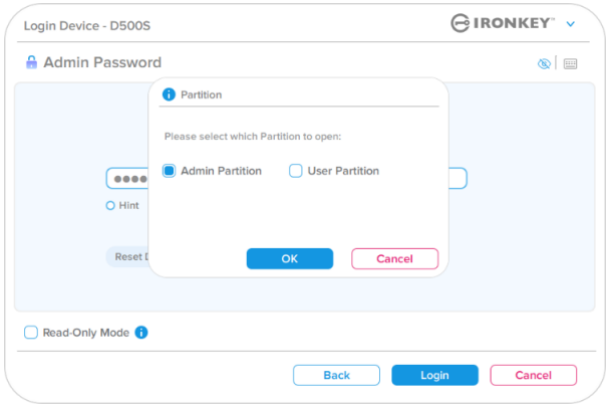


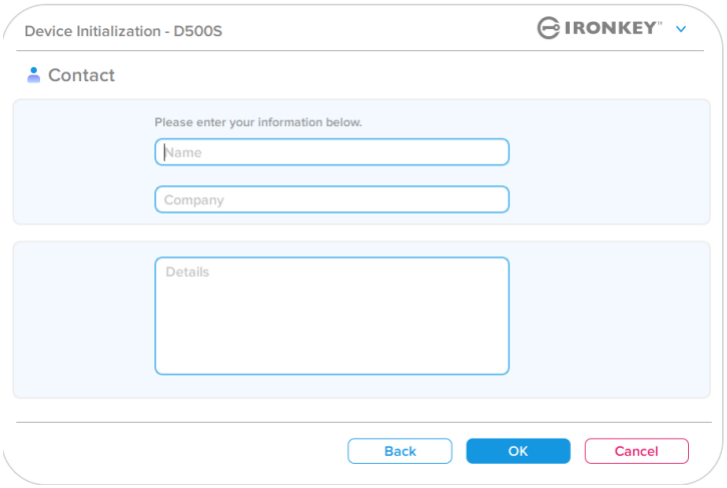
Figura 4.17 — Ejemplo de inicio de sesión de administrador con selección de partición

Inicialización del dispositivo

Información de contacto

Escriba sus datos de contacto en los cuadros de texto correspondientes (véase la *Figura 4.18*)

Nota: La información que especifique en estos campos NO puede contener la cadena de la contraseña que creó en el paso 3. Sin embargo, estos campos son opcionales y pueden quedar en blanco, si así lo desea.

El campo **'Nombre'** puede contener hasta 32 caracteres, pero no puede contener la contraseña **exacta**. El campo **'Empresa'** puede contener hasta 32 caracteres, pero no puede contener la contraseña **exacta**. El campo **'Detalles'** puede contener hasta 156 caracteres, pero no puede contener la contraseña **exacta**.	 **Figura 4.18 – Información de contacto**

Nota: Al hacer clic en 'Aceptar' habrá concluido el proceso de inicialización y la unidad se desbloqueará. A renglón seguido, monte la partición segura en la cual podrá almacenar sus datos protegidos. Seguidamente, desenchufe la unidad y vuelva a enchufarla al sistema para ver implementados los cambios.

Uso del dispositivo (entornos de Windows y de macOS)

Inicio de sesión de administrador y de usuario (Admin habilitado)

Si el dispositivo ha sido inicializado con las Contraseñas de Administración y de Usuario (Rol de Administrador) habilitadas, se iniciará la aplicación IronKey D500S, abriendo primero la pantalla de inicio de sesión que pide la Contraseña de usuario. Desde aquí podrá iniciar sesión con la Contraseña de usuario, ver la información de contacto que haya introducido, o bien iniciar sesión como Administrador (*Figura 5.1*). Al hacer clic en el botón 'Iniciar sesión como administrador' (que puede verse abajo), la aplicación presentará el menú de inicio de sesión de Administrador, donde podrá iniciar sesión como tal y acceder a los ajustes y funciones del Administrador (*Figura 5.2*).

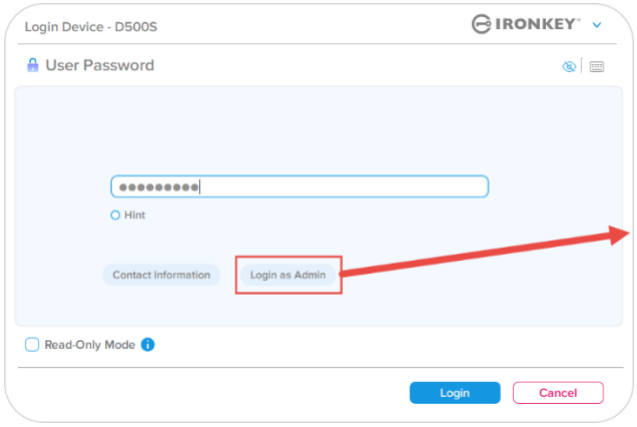


Figura 5.1 - Inicio de sesión con contraseña de usuario (Administrador habilitado)

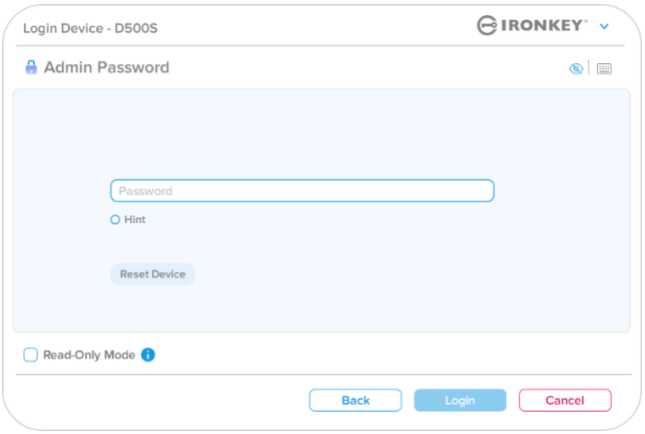


Figura 5.2 - Inicio de sesión con contraseña de administrador

Inicio de sesión en modo de Sólo usuario (Administrador no habilitado)

Como ya explicábamos anteriormente, aunque se recomienda utilizar la funcionalidad de Rol de Administrador para sacar el máximo partido al dispositivo, la unidad IronKey también pueden inicializarse en una configuración de Sólo usuario (Una sola contraseña, Único usuario). Se trata de una opción para quienes desean un método sencillo, con una sola contraseña, para proteger los datos contenidos en la unidad. (*Figura 5.3*)

Nota: para habilitar las contraseñas de administrador y de usuario, utilice el botón **Restablecer dispositivo** para devolver la unidad a su estado de inicialización, desde donde podrá habilitar ambas contraseñas. Al ejecutar Restablecer dispositivo, **TODOS los datos de la unidad se formatearán y se perderán para siempre.**

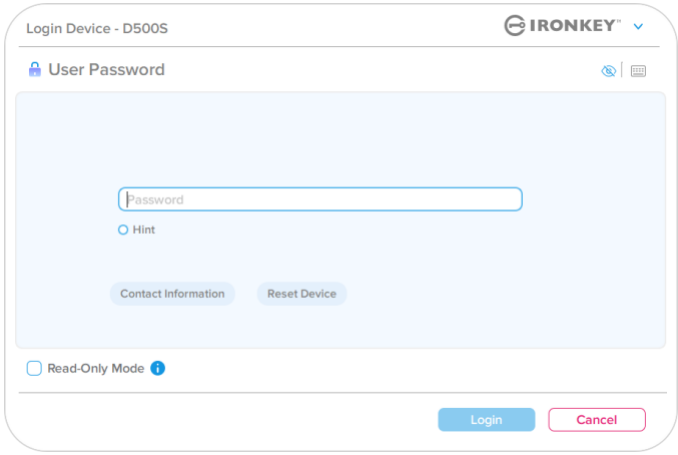


Figura 5.3 - Inicio de sesión con contraseña de usuario (Administrador no habilitado)

Uso del dispositivo

Desbloqueo en modo de Sólo lectura

Podrá desbloquear el dispositivo en modo de Sólo lectura, de modo que los archivos no puedan modificarse en la unidad IronKey. Por ejemplo, al utilizar un ordenador desconocido, al desbloquear el dispositivo en modo de solo lectura evitará que cualquier malware de dicho ordenador infecte el dispositivo o modifique los archivos.

En esta modalidad no es posible realizar ninguna operación que implique la modificación de los archivos del dispositivo. Por ejemplo, no podrá reformatear el dispositivo, ni restablecer, agregar o editar los archivos contenidos en la misma.

Para desbloquear el modo de solo lectura del dispositivo:

1. Inserte el dispositivo en el puerto USB del ordenador anfitrión y ejecute el archivo **IronKey.exe**.
2. 2. Marque la casilla de verificación **Modo de sólo lectura**, debajo del cuadro de introducción de contraseña (*Figura 5.4*).
3. Escriba la contraseña del dispositivo y, a continuación, haga clic en **Iniciar sesión**. De este modo, el dispositivo quedará desbloqueado en modo de Sólo lectura.

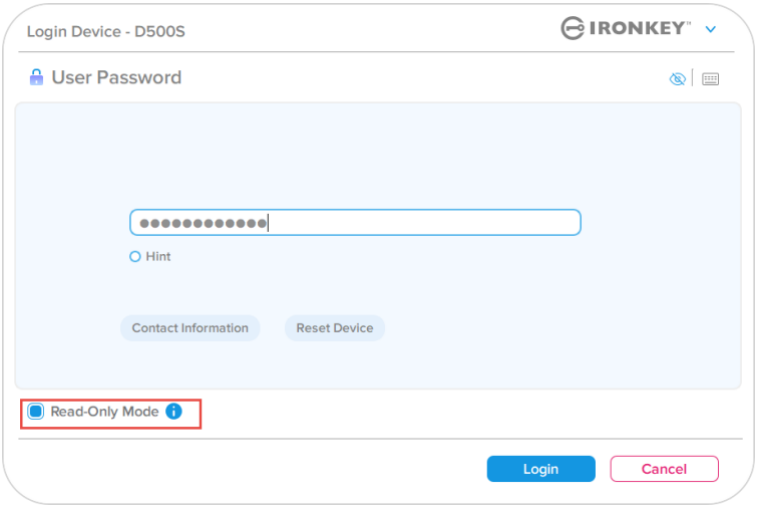


Figura 5.4 - Modo de Sólo lectura

Si desea desbloquear el dispositivo con pleno acceso de lectura/escritura a la partición de datos protegidos, debe cerrar la unidad D500S y volver a iniciar sesión, dejando desactivada la casilla de verificación 'Modo de Sólo lectura'.

Nota: entre las opciones de Administrador de D500S se incluye el modo de Sólo lectura forzado para los datos del usuario; es decir que, al inicio de su sesión, el usuario puede ser forzado por el Administrador a desbloquear la unidad en modo de Sólo lectura (consulte información detallada en la página 31).

Uso del dispositivo

Protección contra ataques de fuerza bruta

Importante: Durante el inicio de sesión, si introduce una contraseña incorrecta tendrá otra oportunidad para introducir la correcta. No obstante, existe una función de seguridad integrada (también denominada "Protección contra ataques de fuerza bruta) que registra el número de intentos fallidos de inicio de sesión. *

Si este número alcanza el valor preconfigurado de 10 intentos fallidos de introducción de contraseña, las consecuencias serán las siguientes:

Admin/Usuario habilitados	**Protección contra ataques de fuerza bruta Respuesta del dispositivo (10 intentos incorrectos de contraseña)**	**¿Borra los datos y restablece el dispositivo?**
Contraseña de usuari	Bloqueo de contraseña. Inicie sesión como Administrador o utilice la contraseña de recuperación de un solo uso para restablecer la contraseña del usuari	NO
Contraseña de administrador	Borrado del contenido cifrado de la unidad, así como de la contraseña y los ajustes; los datos se borran para siempre	**SÍ**
Contraseña de recuperación de un solo us	Bloqueo de la contraseña; el botón Contraseña de recuperación quedará desactivado y no podrá utilizarse. Inicie sesión como Administrador para restablecer la contraseña	NO
Sólo usuario Una sola contraseña, Único usuario (Admin/Usuario NO habilitados)	**Protección contra ataques de fuerza bruta Respuesta del dispositivo (10 intentos incorrectos de contraseña)**	**¿Borra los datos y restablece el dispositivo?**
Contraseña de usuari	Borrado del contenido cifrado de la unidad, así como de la contraseña y los ajustes; los datos se borran para siempre	**SÍ**

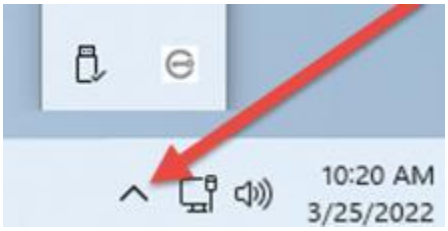
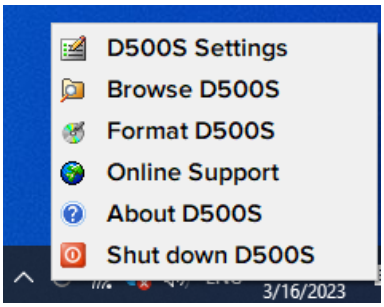
* Una vez que se haya autenticado debidamente en el dispositivo, el contador de intentos fallidos se pondrá a cero en relación con el método de inicio de sesión utilizado. El criptoborrado eliminará todas las contraseñas, claves de cifrado y datos – **sus datos se perderán para siempre.**

Acceso a Mis archivos protegidos

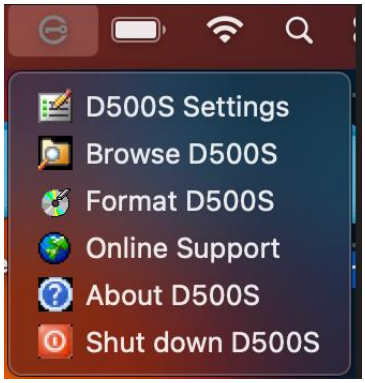
Tras desbloquear el dispositivo podrá acceder a sus archivos protegidos. Los archivos se cifran y descifran automáticamente al guardarlos o abrirlos en la unidad. Esta tecnología ofrece la comodidad de poder trabajar como lo haría normalmente con una unidad común, aunque ofreciendo una sólida protección continuamente activada.
Hint: siempre podrá acceder a los archivos haciendo clic con el botón secundario del ratón en el icono de IronKey de la barra de tareas de Windows; a continuación, haga clic en **Explorar D500S** (*Figura 6.2*)

Opciones del dispositivo - (entorno de Windows)

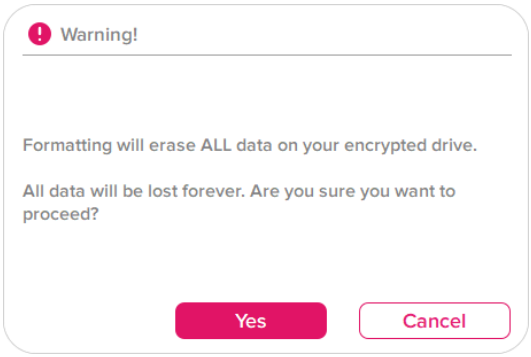
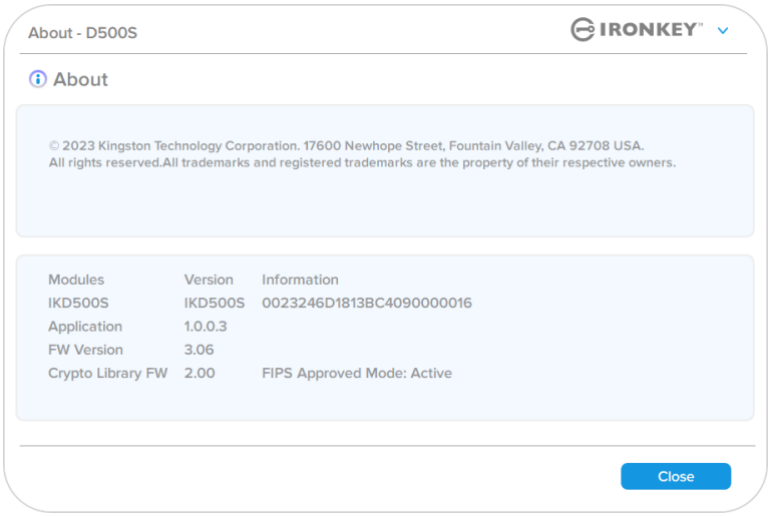
Mientras esté conectado al dispositivo verá el icono de IronKey en la esquina superior derecha de la ventana. Haga clic en el icono de IronKey con el botón secundario del ratón para abrir el menú de selección y acceder a las opciones disponibles de la unidad (*Figura 6.2*).
Encontrará información detallada acerca de dichas opciones en las páginas 21 a 25 de este manual.

• Mientras esté conectado al dispositivo verá el icono de IronKey en la esquina superior derecha de la ventana (*Figura 6.1*)	 **Figura 6.1 - Icono de IronKey en la barra de tareas**
• Haga clic en el icono de IronKey con el botón secundario del ratón para abrir el menú de selección y acceder a las opciones disponibles de la unidad (*Figura 6.2*). Encontrará información detallada acerca de dichas opciones en las páginas 19 a 23 de este manual.	 **Figura 6.2 - Haga clic con el botón secundario en el icono de IronKey para acceder a las opciones del dispositivo**

Opciones del dispositivo- (entorno de macOS)

• Mientras esté conectado al dispositivo, siempre verá el icono de IronKey D500S en el menú macOS, como puede apreciarse en la Figura 6.3, que se abrirá con las opciones disponibles del dispositivo. Encontrará información detallada acerca de dichas opciones en las páginas 19 a 23 de este manual.	 **Figura 6.3 - Barra de menús de macOS/Menú Opciones del dispositivo**

Opciones del dispositivo

Ajustes de D500S:	• Cambio de contraseña al inicio de sesión, información de contacto y otros ajustes. (Encontrará información más detallada acerca de los ajustes del dispositivo en la sección 'Ajustes de D500S' de este manual).
Examinar D500S:	• Permite ver los archivos protegidos.
Formatear D500S: Permite formatear la partición de datos seguros. (Advertencia: Se borrarán todos los datos.) (*Figura 6.1*) **Nota:** para formatear será necesario autenticar la contraseña.	 **Figura 6.1- Formatear D500S**
Asistencia en línea:	• Abre su navegador de Internet y navega hasta http://www.kingston.com/support, donde podrá acceder a información de asistencia adicional
Acerca de D500S: presenta información detallada específica acerca de la unidad D500S, incluyendo la de Aplicación, el Firmware y el Número de serie (*Figura 6.2*) **Nota:** el número de serie exclusivo de la unidad estará en la 'Columna Info'	 **Figura 6.2 — Formatear D500S**
Apagar D500S:	• Apaga correctamente la unidad D500S, para que pueda extraerlo del sistema de forma segura.

Ajustes de D500S

Ajustes de administrador

El inicio de sesión de Administrador le permitirá acceder a los siguientes ajustes del dispositivo:

- **Contraseña:** Permite cambiar su propia contraseña de administrador y/o su indicio (*Figura 7.1*)
- **Información de contacto:** Permite agregar/ver/modificar sus datos de contacto (*Figura 7.2*)
- **Idioma:** permite cambiar el idioma actualmente seleccionado (*Figura 7.3*)
- **Opciones de Administrador:** permite activar funciones adicionales, como por ejemplo: (*Figura 7.4*)
    - Cambiar la contraseña de usuario
    - Restablecer la contraseña al inicio de sesión (para la contraseña del usuario)
    - Activar una contraseña de recuperación de un solo uso
    - Activar una contraseña de criptoborrado
    - Forzar el modo de Sólo lectura para los datos del usuario

NOTA: encontrará información más detallada acerca de las Opciones del Administrador en la página 26.

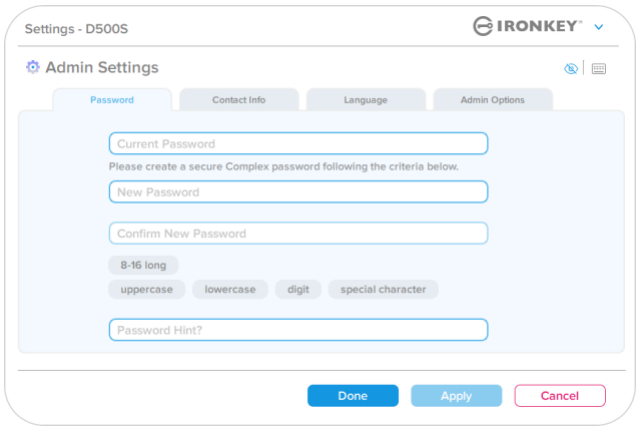


Figura 7.1 – Opciones de contraseña

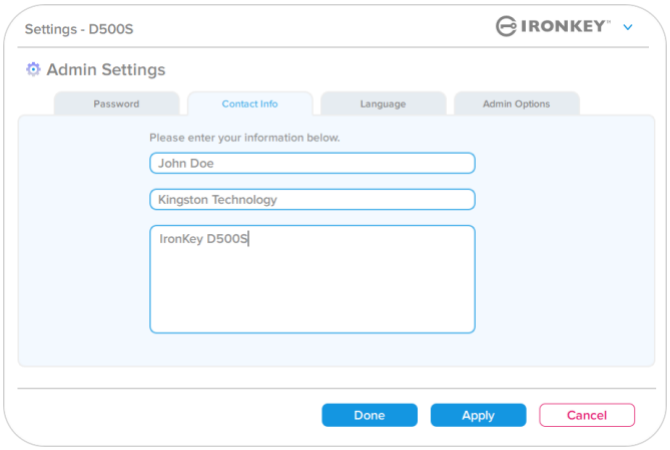


Figura 7.2 – Información de contacto

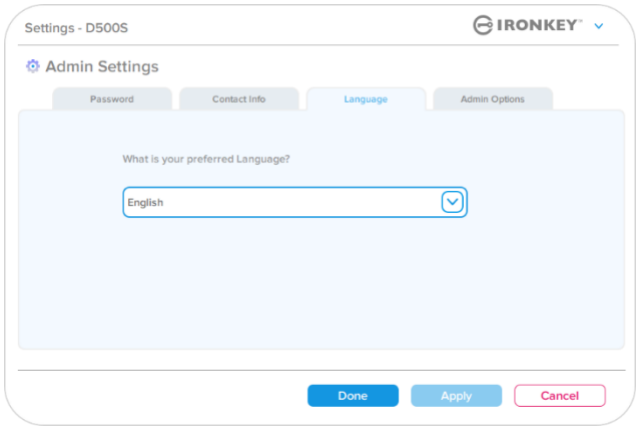


Figura 7.3 - Opciones de idioma

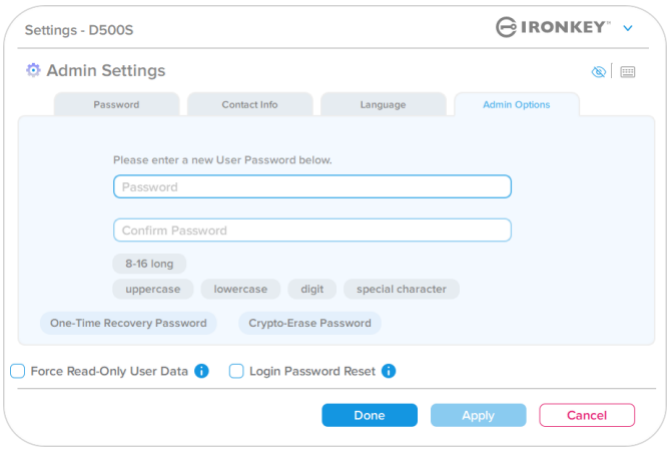
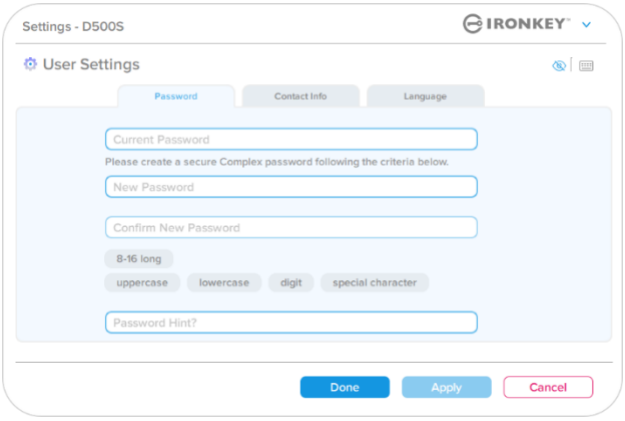
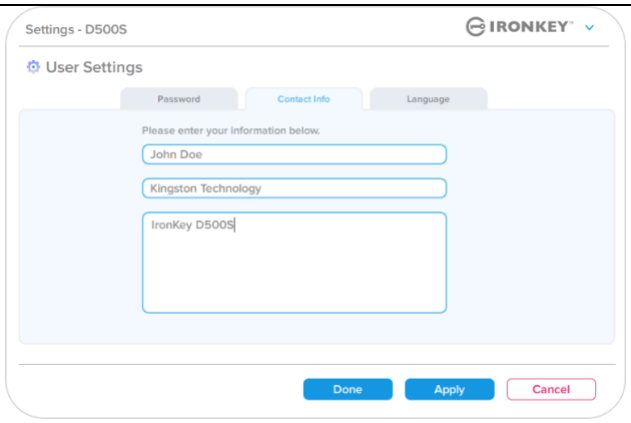
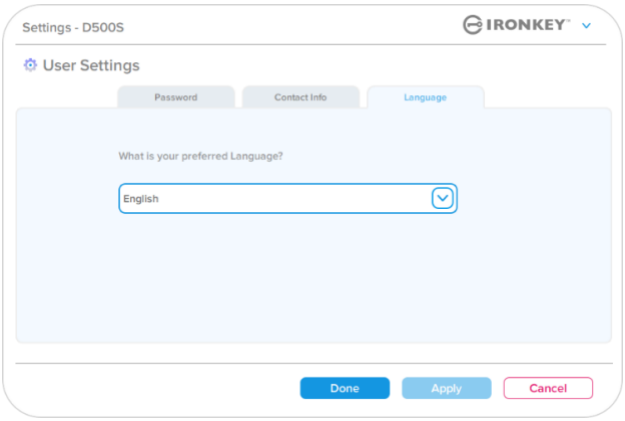


Figura 7.4 - Opciones de Administrador

Ajustes de D500S

Ajustes de usuario: Admin habilitado

Un inicio de sesión de usuario limita el acceso a los siguientes ajustes:

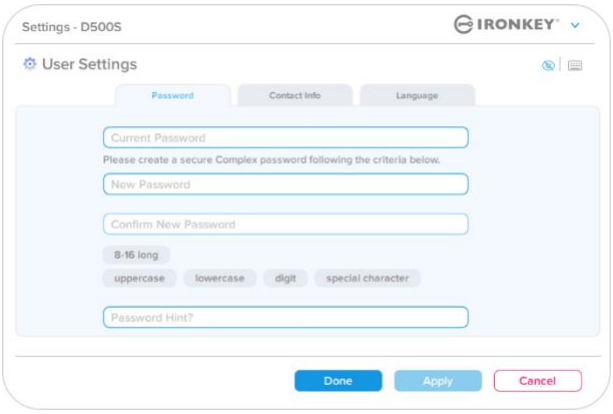
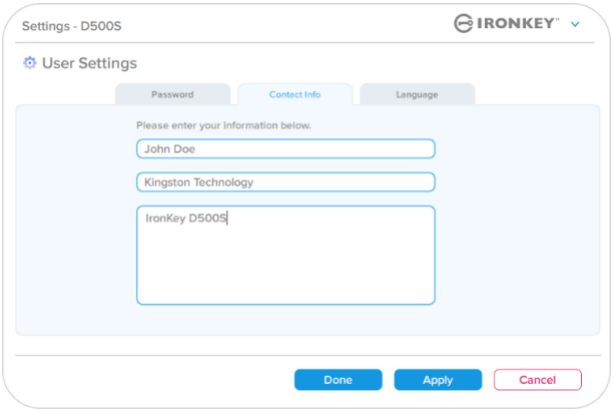
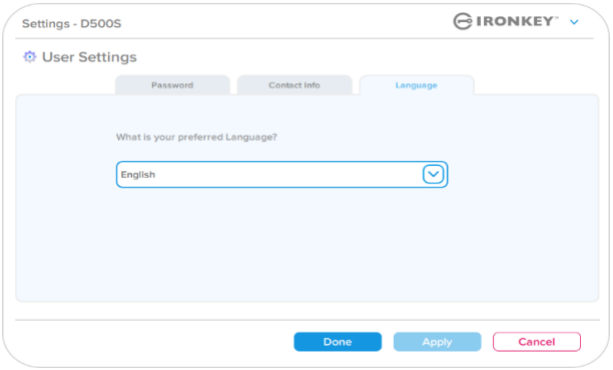
Contraseña: Permite cambiar su propia contraseña de usuario y/o su indicio (*Figura 7.5*)	 **Figura 7.5 - Opciones de contraseña (Admin habilitado: Inicio de sesión de usuario)**
Información de contacto: Permite agregar/ver/modificar sus datos de contacto (*Figura 7.6*)	 **Figura 7.6 - Información de contacto (Admin habilitado: Inicio de sesión de usuario)**
Idioma: permite cambiar el idioma actualmente seleccionado (*Figura 7.7*)	 **Figura 7.7 - Ajustes de idioma (Admin habilitado: Inicio de sesión de usuario)**

Nota: no podrá acceder a Opciones del Administrador si ha iniciado sesión con la contraseña del usuario.

Ajustes de D500S

Ajustes de usuario: Admin no habilitad24

Como ya se ha mencionado previamente, la inicialización de la unidad D500S sin habilitar las contraseñas de 'Admin y Usuario' configurarán la unidad como de **Único usuario, Una sola contraseña (modo de Sólo usuario)**. Esta configuración no tiene acceso a las opciones ni funciones del Administrador. Esta configuración permite el acceso a los siguientes ajustes de la unidad D500S:

Contraseña: permite cambiar su propia contraseña de usuario y/o su indicio (*Figura 7.8*)	 **Figura 7.8 - Opciones de contraseña (modo de Sólo usuario)**
Información de contacto: permite agregar/ver/modificar sus datos de contacto (*Figura 7.9*)	 **Figura 7.9 - Información de contacto (modo de Sólo usuario)**
Idioma: permite cambiar el idioma actualmente seleccionado (*Figura 7.10*)	 **Figura 7.10 - Ajustes de idioma (modo de Sólo usuario)**

Ajustes de D500

Cambio y almacenamiento de los ajustes

- Cada vez que se cambian las opciones en los Ajustes de D500S (como, por ejemplo, información de contacto, idioma, cambios de contraseña, opciones de Administrador, etc.), la unidad le pedirá que introduzca su contraseña para aceptar y aplicar los cambios (*Figura 7.11*).

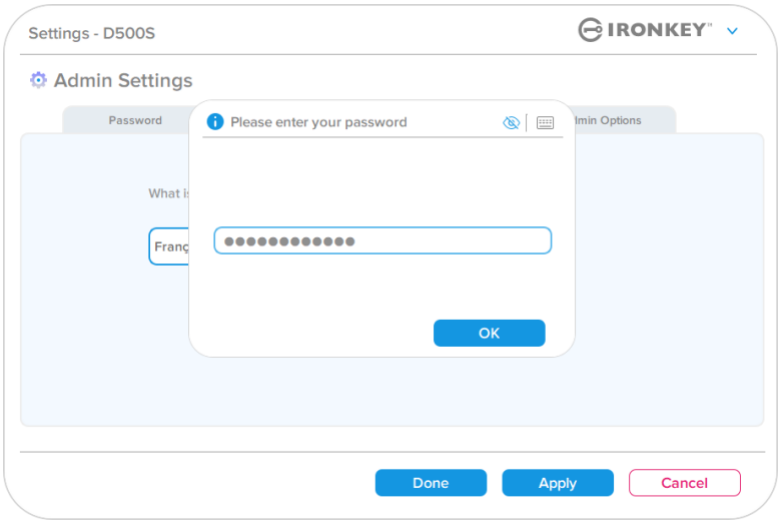


Figura 7.11 - Pantalla de pedido de contraseña para guardar los cambios de los ajustes de la unidad D500S

Nota: si se encuentra en la pantalla de pedido de contraseña precedente y desea cancelar o modificar los cambios, podrá hacerlo sencillamente: asegúrese de que el campo de la contraseña esté vacío y, a continuación, haga clic en 'Aceptar'. De este modo se cerrará el cuadro 'Escriba la contraseña' y volverá al menú de ajustes de la unidad D500S.

Funciones del Administrador

Opciones disponibles para restablecer la contraseña de usuario
Las opciones de configuración del Administrador ofrecen varias maneras de restablecer con seguridad las contraseñas de usuarios en caso de que se les olviden, así como, en caso de haber creado una contraseña de usuario temporal, obligar a cambiar dicha contraseña la siguiente vez que inicie sesión. A continuación presentamos las funciones que podrán resultarle de utilidad para restablecer las contraseñas de usuario:

Restablecimiento de contraseña de usuario:
Cambie manualmente la contraseña del usuario en el menú 'Opciones de Administrador'. El cambio se produce de manera inmediata y surtirá efecto la próxima vez que el usuario inicie sesión (*Figura 8.1*)

Nota: los criterios de requisitos de contraseña volverán de manera predeterminada a los originales establecidos durante el proceso de inicialización (opciones Compleja o Frase de contraseña).

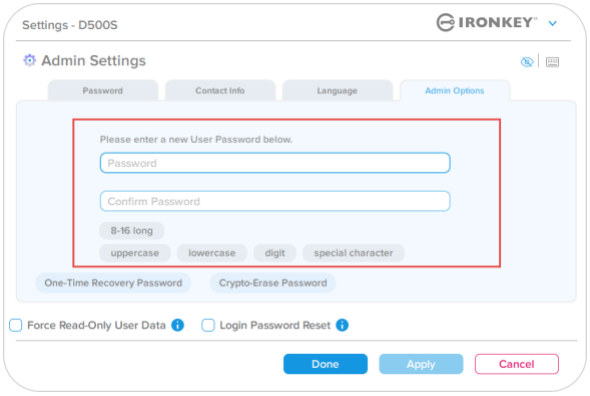


Figura 8.1 - Opciones de Administrador/Restablecimiento de contraseña de usuario

Restablecimiento de contraseña al inicio de sesión:
La activación del restablecimiento de contraseña **forzará al usuario a iniciar sesión utilizando la contraseña temporal establecida por el administrador** y, a continuación, cambiarla por una contraseña de su preferencia. Esto resulta útil cuando se entrega la unidad para que la use otra persona. (Véanse las *Figuras 8.2 y 8.3*)

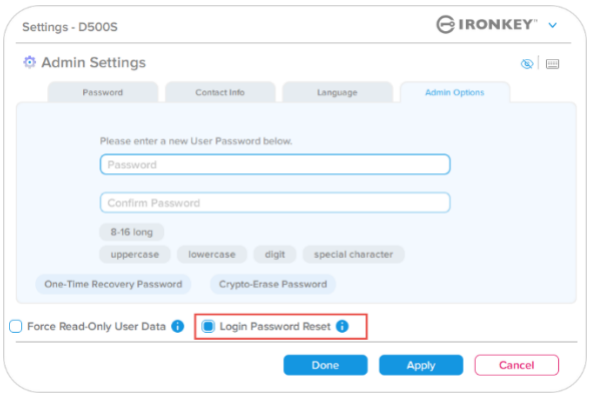


Figura 8.2A - Botón Restablecer contraseña al inicio de sesión

Nota: la aplicación de este restablecimiento surtirá efecto la próxima vez que el usuario inicie correctamente una sesión. Los criterios de requisitos de contraseña se aplicarán inmediatamente de conformidad con la opción original establecida durante el proceso de inicialización (opciones Compleja o Frase de contraseña).

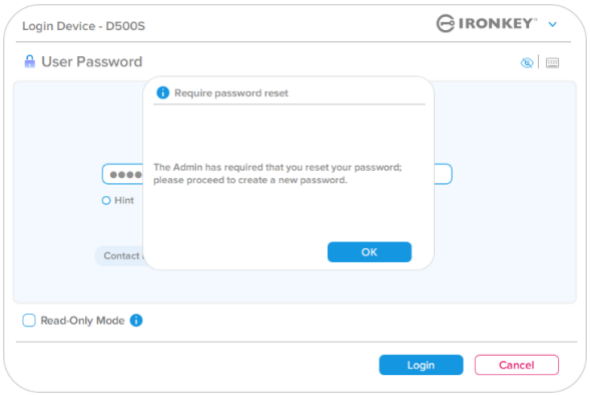


Figura 8.2B - Notificación de restablecimiento después de introducir la contraseña de usuario

Funciones del Administrador

Contraseña de recuperación de un solo uso

Esta sección explica el procedimiento de activar y utilizar la función de recuperación de contraseña de un solo uso.

Contraseña de recuperación de un solo uso

Paso 1: La función Contraseña de recuperación de un solo uso resulta muy práctica, por el hecho de que puede activarse para ayudar a recuperar y restablecer la contraseña del usuario en caso de que este la hubiese olvidado. Para empezar, haga clic en el botón'Contraseña de recuperación de un solo uso' del menú de opciones del Administrador. (*Figura 8.4*)

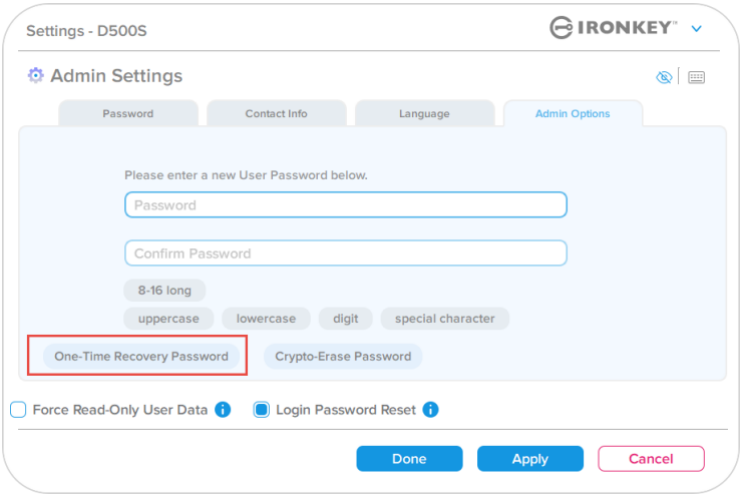


Figura 8.4 - Botón Contraseña de recuperación de un solo uso

Paso 2: Cree una contraseña de recuperación de un solo uso aplicando los mismos criterios con los cuales la unidad fue configurada inicialmente (Compleja o Frase de contraseña).

Nota: para realizar cambios será necesaria la contraseña de Administrador.

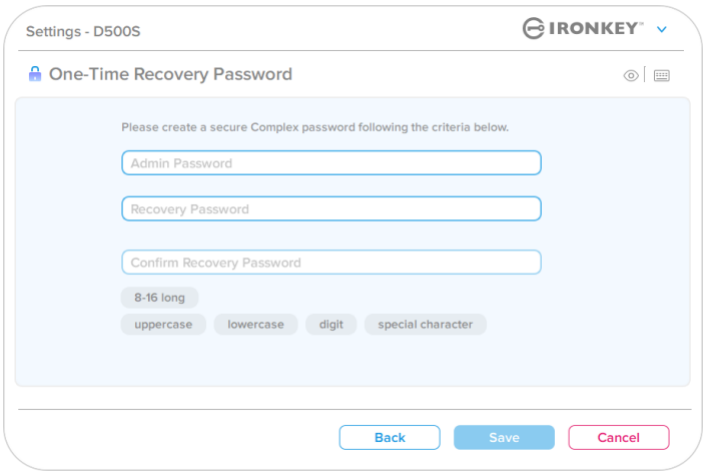


Figura 8.5 - Configuración de Contraseña de recuperación de un solo uso

Funciones del Administrador

Uso de la contraseña de recuperación de un solo uso

Paso 1: Una vez creada la contraseña de recuperación de un solo uso, tras el siguiente inicio de sesión aparecerá un nuevo botón en la pantalla de inicio de sesión de **Contraseña del usuario**. Haga clic en el botón **Contraseña de recuperación** para iniciar el proceso.

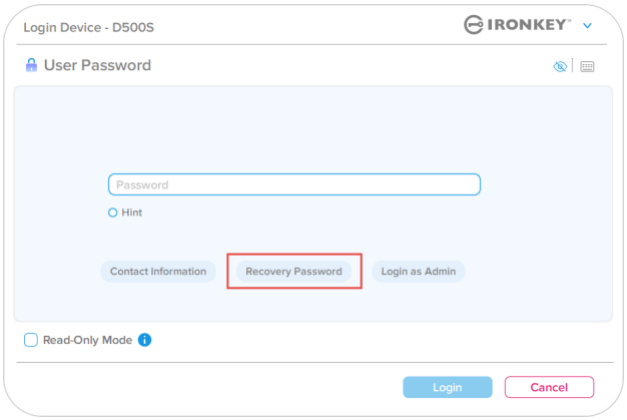


Figura 8.6 - Botón Contraseña de recuperación

Paso 2: Aparecerá la pantalla Contraseña de recuperación, en la cual podrá introducir la **Contraseña de recuperación** y crear una nueva Contraseña de usuario. (*Figura 8.7*)

Importante: Además, la Contraseña de recuperación de un solo uso utiliza una función de seguridad integrada que lleva un seguimiento del número de intentos de inicio de sesión fallidos; **tras 10 intentos incorrectos de inicio de sesión con la Contraseña de recuperación de un solo uso, la contraseña quedará desactivada** y será necesario reactivarla iniciando sesión como Administrador. (consulte información más detallada en las páginas 19 y 33)

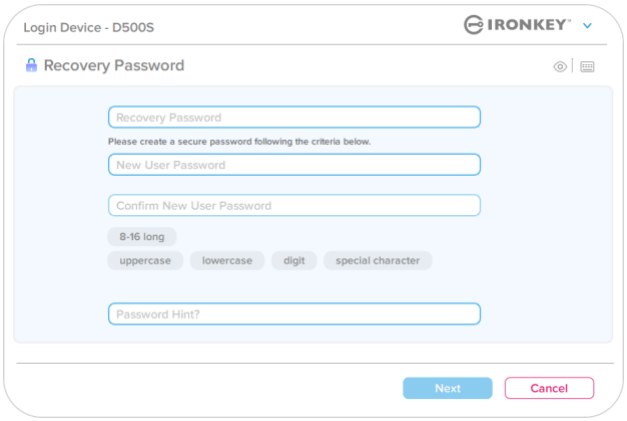


Figura 8.7 - Menú Contraseña de recuperación

Paso 3: Una vez realizado satisfactoriamente el paso anterior, volverá a la pantalla **Contraseña del usuario**. Ahora, el botón **Contraseña de recuperación** habrá desaparecido, y la contraseña introducida en el **Paso 2** se habrá convertido en la nueva Contraseña del usuario. (*Figura 8.8*)

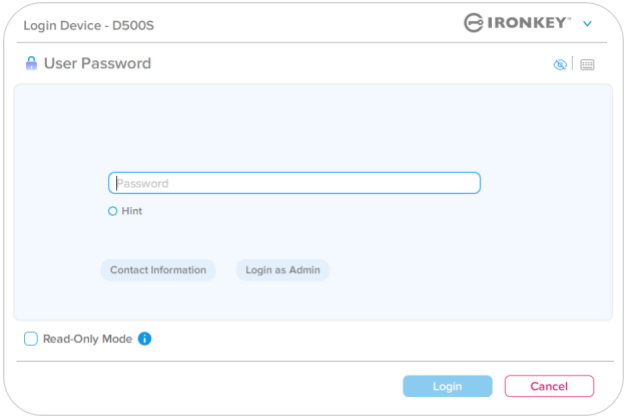


Figura 8.8 - Pantalla de inicio de Contraseña del usuario, mostrando que el botón Contraseña de recuperación ha desaparecido tras haber sido utilizado debidamente.

Funciones del Administrador

Contraseña de criptoborrado

La unidad IronKey D500S está equipada con la exclusiva función Contraseña de criptoborrado, diseñada como protección y defensa contra situaciones físicamente comprometidas, ya mediante la misma se borra de manera segura el contenido de la unidad, dejándola como si nunca hubiese tenido datos escritos. Al activar esta función, cuando la unidad se desbloquea mediante la contraseña de criptoborrado, ejecutará un criptoborrado discreto de la D500S y la devolverá al modo de estado de fábrica, con una partición de usuario vacía. Se borrará la anterior clave de cifrado y se creará en su lugar una nueva. ***Utilice con precaución***

- Para **activar** esta función, haga clic en el botón Contraseña de criptoborrado, que verá en la pestaña Opciones de administrador:

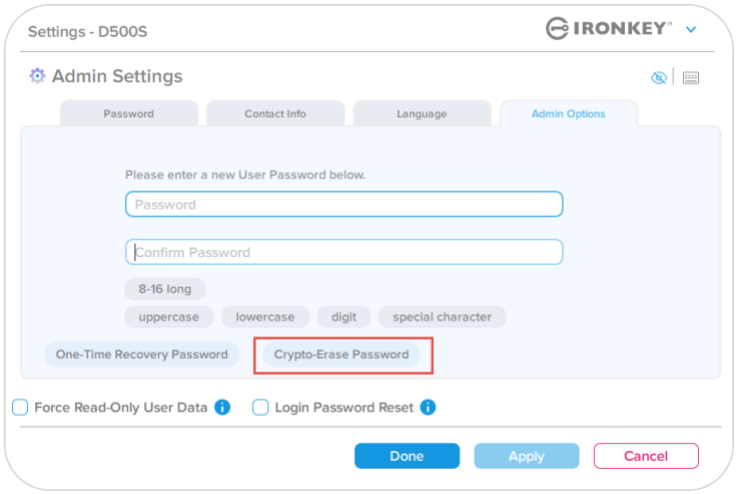


Figura 8.9 - Activación de Contraseña de criptoborrado

Crear una contraseña de criptoborrado:

- Las reglas de contraseña estarán basadas en los elementos con los cuales la unidad fue originalmente inicializada (Compleja o Frase de contraseña)
- Para validar será necesaria la contraseña de administrador.

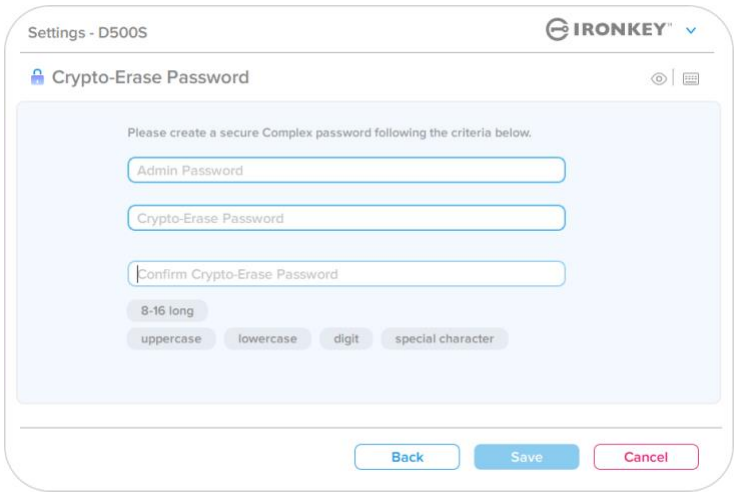


Figura 8.10 - Crear Contraseña de criptoborrado

Funciones del Administrador

Uso de la contraseña de criptoborrado

Tras utilizar la contraseña de criptoborrado, las anteriores contraseñas de administrador y de usuario quedarán borradas, y serán sustituidas por la contraseña de criptoborrado. Además, con el borrado permanente de todos los datos guardados en la unidad quedarán eliminados los ajustes de configuración anteriores, y la unidad pasará a una configuración de modo de Sólo usuario.

Para utilizar la contraseña de criptoborrado:

1. L Inicie IronKey.exe para ejecutar la aplicación IronKey
2. En la pantalla de inicio de sesión de Contraseña de usuario, pulse '**CTRL + ALT +C**' para alternar a la entrada de Contraseña de criptoborrado. Si lo hace correctamente, observará una barra azul más gruesa debajo de la pantalla de introducción de contraseña, indicando que el sistema está preparado para la introducción de la contraseña de criptoborrado. (*Figura 8.11*)

NOTA: la contraseña de criptoborrado puede alternarse solamente en la pantalla de inicio de sesión de contraseña de usuario.

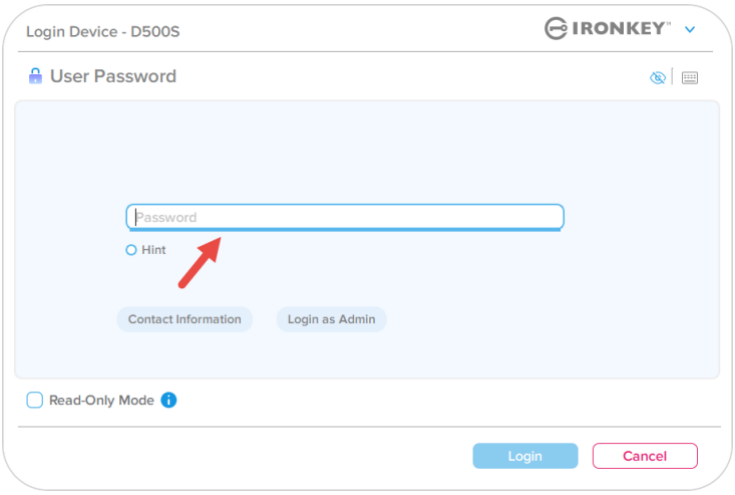


Figura 8.11 — Criptoborrado habilitado, con barra azul gruesa,.

Una vez utilizada la contraseña de criptoborrado, la unidad procederá a borrar todo su contenido, y aparecerá una única partición vacía. La unidad estará entonces en el modo de Sólo usuario, y la contraseña de criptoborrado será la contraseña de acceso a la misma hasta que sea restablecida.

Importante: esta función borrará todos los datos de la unidad, y todo lo previamente almacenado se perderá para siempre. ¡Proceda con precaución!

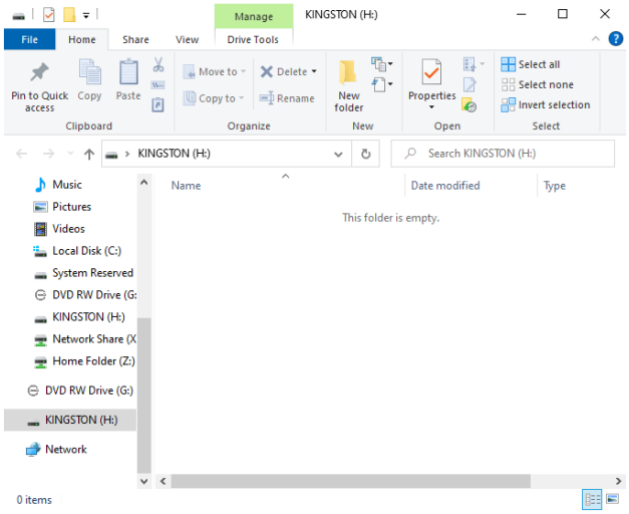


Figura 8.12 — Borrado de la unidad tras el uso de la contraseña de criptoborrado

Funciones del Administrador

Forzar datos de usuario de Sólo lectura

La función Modo de sólo lectura forzado puede activarse para restringir el acceso del usuario a la escritura en la unidad. Esta función resulta útil si los archivos contenidos en la unidad se requieren para acceso de sólo lectura.

- Para activar Forzar datos de usuario de sólo lectura, haga clic en el cuadro y, seguidamente, en 'Aplicar'. (*Figura 8.13*)

  Nota: Este modo de Forzar sólo lectura es de aplicación solamente al usuario, y no afecta a los inicios de sesión del Administrador. El Administrador seguirá teniendo privilegios de acceso a la lectura y a la escritura y, si fuese necesario, podrá activar el modo de Sólo lectura.

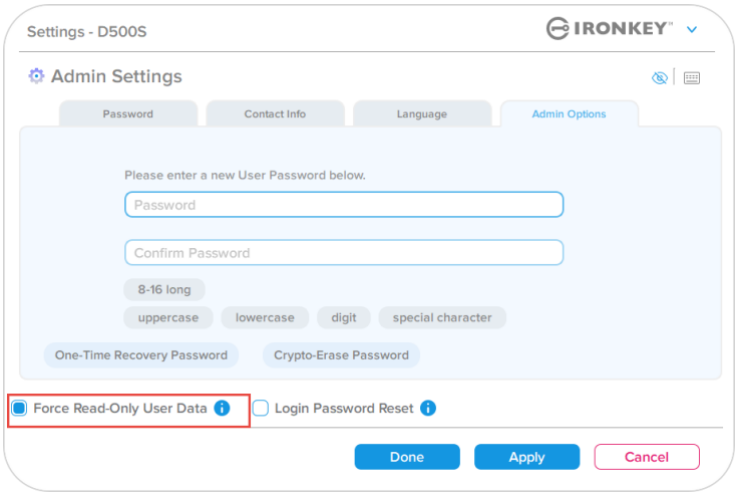


Figura 8.13 - Activación de 'Forzar datos de usuario de sólo lectura' (para realizar cambios será necesaria la contraseña de Administrador)

- Una vez activado el botón de **'Modo de Sólo lectura'**, la casilla estará en color azul, lo cual implica que el modo forzado de Sólo lectura habrá quedado permanentemente activado para la Contraseña del usuario, hasta que sea desactivado por el Administrador. (*Figura 8.14*)

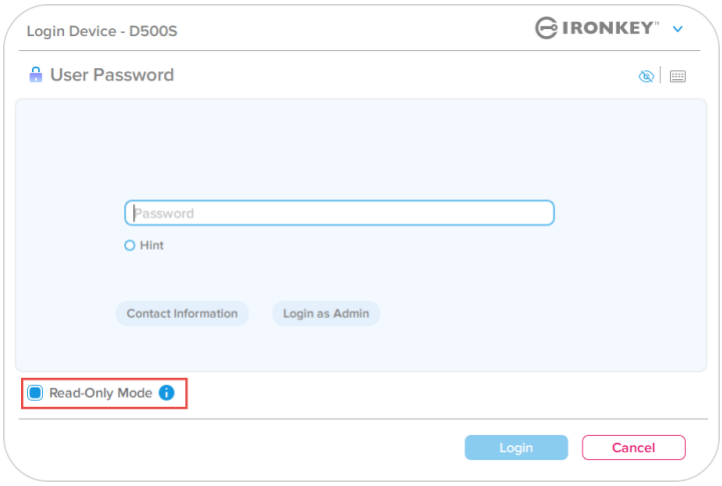


Figura 8.14 - Modo de Sólo lectura forzado para el usuario activado; solamente podrá desactivarlo el Administrador

Ayuda y solución de problemas

Bloqueo del dispositivo

La unidad D500S incluye una función de seguridad que impide el acceso no autorizado a la partición de datos una vez alcanzado un número máximo de intentos **consecutivos** fallidos de inicio de sesión (*MaxNoA*, en lenguaje informático). El valor predeterminado de fábrica ha sido preconfigurado con un valor de 10 (número de intentos) en cada método de inicio de sesión (Administrador/Usuario/Contraseña de recuperación de un solo uso).

El contador de 'bloqueo' registra cada intento fallido de inicio de sesión, y se pondrá a cero **en las dos** situaciones siguientes:

1. Inicio de sesión correcto antes de alcanzar el MaxNoA.

2. Alcanzar el MaxNoA y realizar un bloqueo o un formateo del dispositivo, en función de cómo fue configurada la unidad.

- Si se introduce una contraseña incorrecta, se muestra un mensaje de error en rojo encima del campo de introducción de contraseña, que indica que se ha producido un error de inicio de sesión. (*Figura 9.1*)

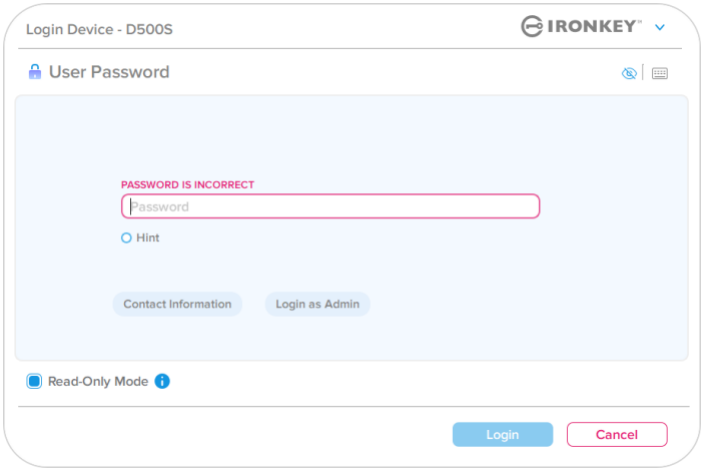


Figura 9.1 - Mensaje de contraseña incorrecta

- Si se produce un **7º** intento fallido, aparecerá un mensaje de error adicional indicando que le quedan 3 intentos antes de alcanzar el valor de MaxNoA (cuyo valor predeterminado es de 10). (*Figura 9.2*)

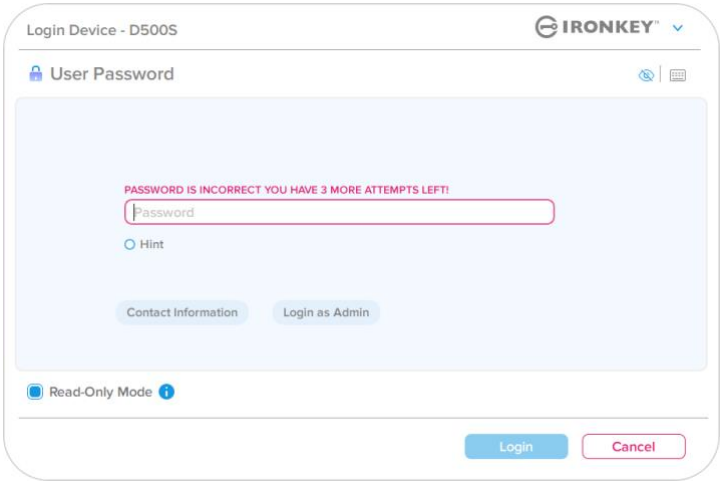


Figura 9.2- 7º intento de introducción de contraseña incorrecta

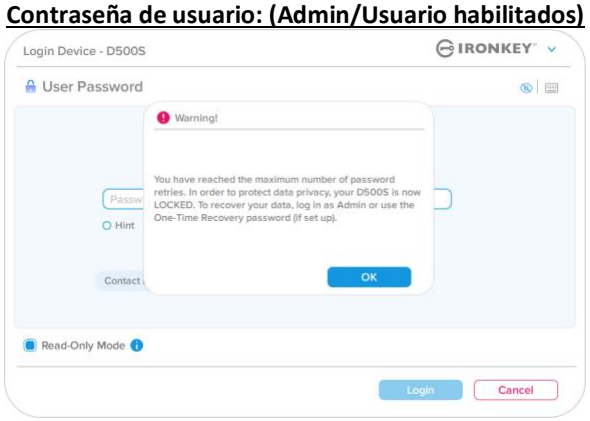
Ayuda y solución de problemas

Bloqueo del dispositivo

Importante: Tras un **10º** y último intento fallido de inicio de sesión, en función de cómo ha sido configurado el dispositivo y del método de inicio de sesión utilizado, (Administrador, Usuario o Contraseña de un solo uso), el dispositivo se bloqueará (requiriendo que utilice un método alternativo, en su caso), o bien tendrá que ejecutar un restablecimiento del dispositivo, que **formateará la unidad borrando para siempre los datos que contenga**. Estos procedimientos también se mencionan en la página 19 de este Manual del usuario.

Las Figuras 9.3 hasta 9.6 siguientes muestran visualmente las consecuencias tras el 10º y último intento fallido de cada método de contraseña de inicio de sesión:

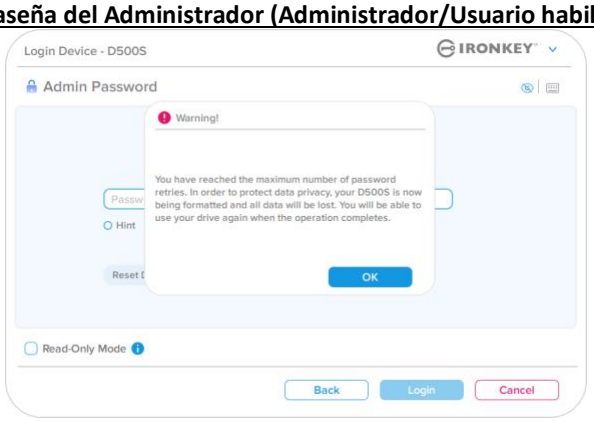
Contraseña de usuario: (Admin/Usuario habilitados)



BLOQUEO DEL DISPOSITIVO

Figura 9.3

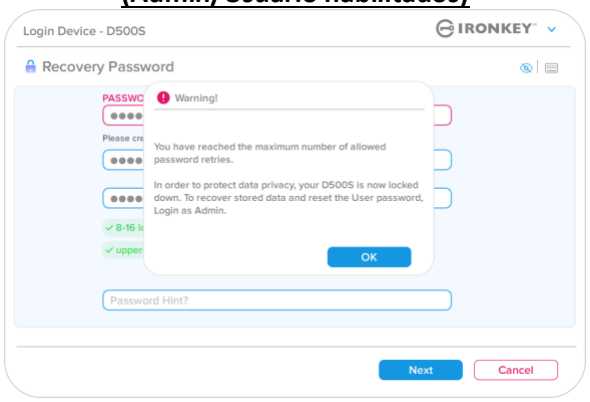
Contraseña del Administrador (Administrador/Usuario habilitado)



FORMATEO DEL DISPOSITIVO*

Figura 9.4

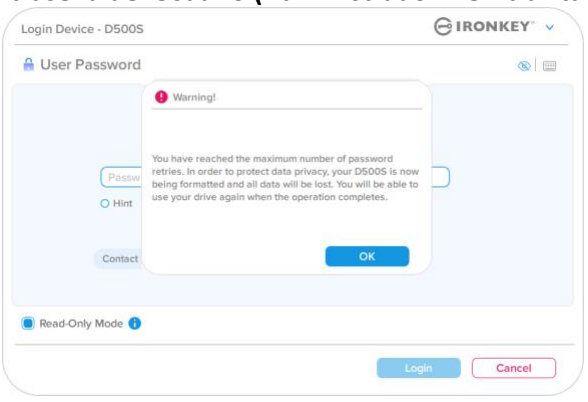
Recuperación de un solo uso: (Admin/Usuario habilitados)



BLOQUEO DEL DISPOSITIVO

Figura 9.5

Contraseña del Usuario (Administrador NO habilitado)



FORMATEO DEL DISPOSITIVO*

Figura 9.6

Estas medidas de seguridad impiden que alguien (que no tenga su contraseña) realice infinitos intentos de inicio de sesión y acceda a sus datos sensibles (también denominados ataques de fuerza bruta). Si usted es el propietario de la unidad D500S y olvida su contraseña, se aplicarán las mismas medidas de seguridad, incluso el formateo del dispositivo.
* Encontrará información más detallada sobre esta función, consulte *'Restablecer dispositivo'*, en la página 25.

**Nota: un formateo de dispositivo borra TODA la información almacenada en la partición de datos protegidos de la unidad D500S.*

Ayuda y solución de problemas

Restablecer dispositivo

Si olvida su contraseña o tiene que restablecer el dispositivo, haga clic en el botón *'Restablecer dispositivo'*, que aparece en uno de dos lugares, en función de cómo haya configurado la unidad (en el menú Contraseña de inicio de sesión de Administrador, si el modo Admin/usuario está habilitado, o bien en el menú de inicio de sesión 'Contraseña de usuario' si dicho modo no está habilitado), al ejecutar el instalador de la unidad D500S (véanse la *Figura 9.7 y 9.8*)

- Esta opción le permitirá crear una nueva contraseña, pero para proteger la privacidad de sus datos, la unidad D500S será reformateada. Esto significa que se borrarán todos sus datos durante el proceso.*

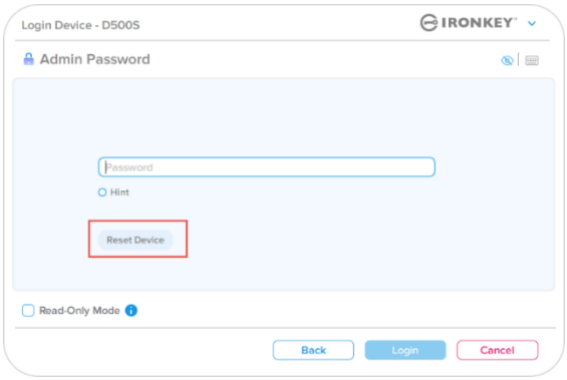


Figura 9.7 - Contraseña de Administrador: botón Restablecer dispositivo

- **Nota:**
  Al hacer clic en *'Restablecer dispositivo'*, se abrirá un cuadro de mensaje donde se le preguntará si desea introducir una nueva contraseña antes de proceder a formatear la unidad. En este momento puede 1) hacer clic en *'Aceptar'* para confirmar, o bien 2) hacer clic en *'Cancelar'* para volver a la ventana de inicio de sesión. (Véase la *Figura 9.8*)

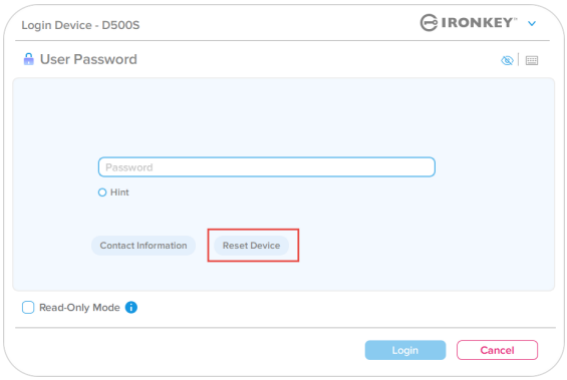


Figura 9.8 - Contraseña de Usuario (Admin/Usuario no habilitado) Restablecer dispositivo

- Si opta por continuar se le redirigirá a la pantalla de inicialización, donde podrá habilitar los 'Modos Admin y Usuario' e introducir la nueva contraseña, en función de la opción que elija (Compleja o Frase de contraseña). El campo de indicio no es obligatorio, pero puede serle útil a la hora de proporcionarle una pista sobre la contraseña a introducir, en caso de que se le olvide.

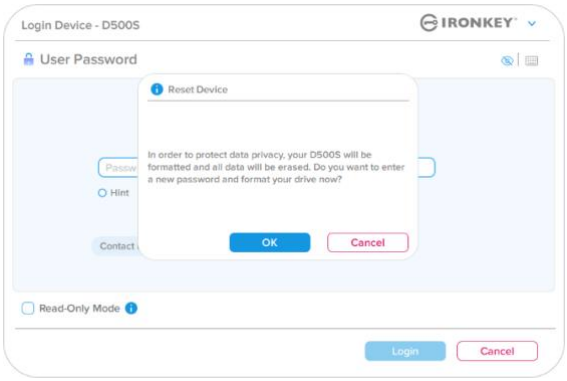


Figura 9.9 - Confirmación de restablecimiento de dispositivo

Ayuda y solución de problemas

Conflicto con la letra de la unidad: sistemas operativos Windows

- Tal y como se ha mencionado en la sección *'Requisitos del sistema'* de este manual (en la página 3), la unidad DTL+ G3 requiere dos letras de unidad consecutivas DESPUÉS del último disco físico que aparezca antes del 'espacio' en las asignaciones de letras de unidades (véase la *Figura 9.10*.) Esto NO hace referencia a recursos compartidos en la red porque son específicos para perfiles de usuario, ni al propio perfil del hardware del sistema, apareciendo así disponible para el SO.

- Esto implica que Windows podrá asignar a la unidad D500S una letra de unidad que ya está siendo utilizada por una red compartida o en la ruta de UNC (Convención de Nomenclatura Universal), provocando un conflicto de letras. Si esto sucede, consulte a su administrador o al departamento de Asistencia para cambiar las asignaciones de letras de unidad en Gestión de discos de Windows (son necesarios privilegios de administrador). Tal y como se ha mencionado en la sección *'Requisitos del sistema'* de este manual (en la página 3), la unidad DTL+ G3 requiere dos letras de unidad consecutivas DESPUÉS del último disco físico que aparezca antes del 'espacio' en las asignaciones de letras de unidades (véase la *Figura 9.10*.) Esto NO hace referencia a recursos compartidos en la red porque son específicos para perfiles de usuario, ni al propio perfil del hardware del sistema, apareciendo así disponible para el SO.

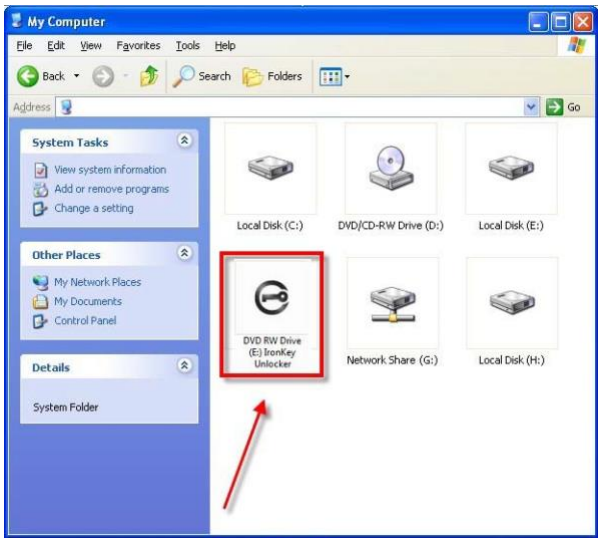


Figura 9.10 - Ejemplo de letra de unidad

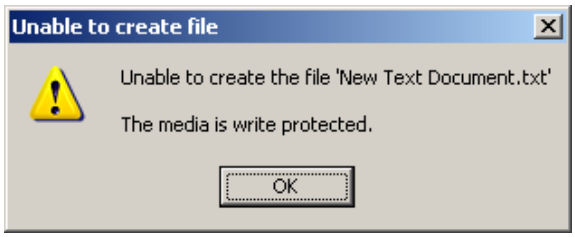
En este ejemplo, (*Figura 9.10*) la unidad D500S utiliza la unidad F:, que es la primera letra de unidad disponible después de la unidad E: (el último disco físico antes del espacio de la letra de unidad). Porque la letra G: es un recurso compartido de red y no una parte del perfil de hardware, la unidad D500S puede intentar utilizarla como segunda letra de unidad, provocando un conflicto.

Si no hay recursos compartidos en la red en su sistema y la unidad D500S sigue sin cargarse, es posible que un lector de tarjetas, un disco extraíble u otro dispositivo previamente instalado mantenga asignada una letra de unidad y provoque un conflicto.

Tenga en cuenta que la gestión de letra de unidad, o DLM, ha mejorado significativamente en Windows Vista y 10 y 11, de forma que puede no dar con este problema, pero si no es capaz de resolver el conflicto, póngase en contacto con el departamento de soporte técnico de Kingston, o bien visite Kingston.com/support para obtener más ayuda.

Ayuda y solución de problemas

Mensajes de error

No ha sido posible crear el archivo: Este mensaje de error aparecerá cuando intente CREAR un archivo o carpeta EN la partición de datos protegidos si ha iniciado sesión en modo de Sólo lectura.	 **Figura 9.11 – Error "No ha sido posible crear el archivo"**
Error al copiar archivo o carpeta: Este mensaje de error aparecerá cuando intente COPIAR un archivo o carpeta EN la partición de datos protegidos si ha iniciado sesión en modo de Sólo lectura.	 **Figura 9.12 – Error "Error Copying File por Folder"**
Error al eliminar archivo o carpeta: Este mensaje de error aparecerá cuando intente ELIMINAR un archivo o carpeta DE la partición de datos protegidos si ha iniciado sesión en modo de Sólo lectura.	 **Figura 9.13 – Error "Error al borrar archivo o carpeta"**

Nota: Si ha iniciado sesión en modo de Sólo lectura y desea desbloquear el dispositivo con pleno acceso de lectura/escritura en la partición de datos protegidos, deberá apagar la unidad D500S y volver a iniciar sesión, dejando desactivada la casilla de verificación 'Modo de Sólo lectura' antes de hacerlo.

Uso del dispositivo (entorno Linux)

Existen hoy en día diversas distribuciones de Linux, de modo que el 'diseño y aspecto' de las interfaces pueden variar de una versión a otra. Sin embargo, el conjunto de comandos generales que se emplean en la aplicación de terminal es muy similar y se puede hacer referencia a dicho conjunto en las instrucciones para Linux que siguen. Las imágenes de pantalla utilizadas en esta sección fueron creadas en un entorno de 64 bits.

Algunas distribuciones de Linux requieren privilegios de superusuario (raíz) para ejecutar correctamente los comandos de la unidad D500S en la ventana de aplicaciones del terminal.

Notas importantes antes de continuar:

1.) **La unidad D500S es incompatible con la inicialización de serie de Linux, y deberá ser totalmente inicializada y configurada en un sistema Windows o macOS compatible antes de poder utilizarla en Linux.**

2.) **El inicio de sesión de Linux solamente es compatible con el uso de contraseñas complejas. El inicio de sesión de Linux no admite el inicio de sesión con Frase de contraseña.**

3.) **La compatibilidad de algunas funciones de D500S con Linux es limitada. Linux no admite funciones como Contraseña de recuperación de un solo uso, Contraseña de criptoborrado, restablecimientos de contraseñas de administrador/usuario y alternar el modo de Sólo lectura.**

La unidad D500S viene con 4 comandos que pueden utilizarse en Linux:

lkd500s_about	Muestra la información de 'Acerca de D500S'.
lkd500s_login	Permite iniciar una sesión de la unidad.
lkd500S_logout	Permite cerrar de manera segura una sesión de la unidad D500S.
lkd500S_resetdevice	Ejecuta un criptoborrado y restablece la unidad a su estado original, eliminando de manera permanente todos los datos y archivos guardados en la unidad.

NOTA: Para ejecutar estos comandos debe abrir una ventana de aplicación "Terminal" y navegar hasta las carpetas en las que se encuentran estos archivos. Cada comando debe empezar con los siguientes dos caracteres: './' (un punto seguido de una barra diagonal.)

Ejemplo de cómo navegar en la ruta de acceso a los comandos Linux de IronKey:

Para usuarios de Linux de 32 bits:	Abra una ventana de aplicación "Terminal" y cambie el directorio actual por **/media/ubuntu/IRONKEY/linux/linux32$** escribiendo el siguiente comando junto al símbolo del sistema: **cd /media/ubuntu/IRONKEY/linux/linux32** (and then press ENTER.)
Para usuarios de Linux de 64 bits:	Abra una ventana de aplicación "Terminal" y cambie el directorio actual por **/media/ubuntu/IRONKEY/linux/linux64$** escribiendo el siguiente comando junto al símbolo del sistema: **cd /media/ubuntu/IRONKEY/linux/linux64** (and then press ENTER.)

Uso del dispositivo (entorno Linux)

Nota: Si el sistema operativo no carga el volumen IRONKEY de forma automática, deberá cargarlo manualmente en una ventana de terminal mediante el uso del comando 'mount' de Linux. Consulte las opciones correctas de sintaxis y de comandos en la documentación de Linux correspondiente a su distribución específica del SO Linux o en su sitio de asistencia en línea favorito. En los ejemplos anteriores, algunas distribuciones de Linux pueden requerir la introducción del nombre de usuario (por ejemplo, "ubuntu") para ejecutar comandos.

Ubicación y visualización de los comandos de archivos de Linux IronKey D500S:

Una vez que la unidad D500S esté conectada a su equipo y haya sido reconocida por el sistema operativo, cambie el directorio al volumen D500S escribiendo el comando en el símbolo del sistema del terminal. (*Figura 10.1*)

Nota: Las imágenes de pantalla e instrucciones de esta sección emplean la carpeta linux64 (que significa 64 bits) con el fin de demostrar el uso de la unidad D500S en el SO Linux. Tenga presente que si usa la versión de 32 bits de Linux, simplemente tiene que navegar a la carpeta correspondiente de 32 bits en lugar de la de 64 bits (es decir, linux32 en lugar de linux64.)

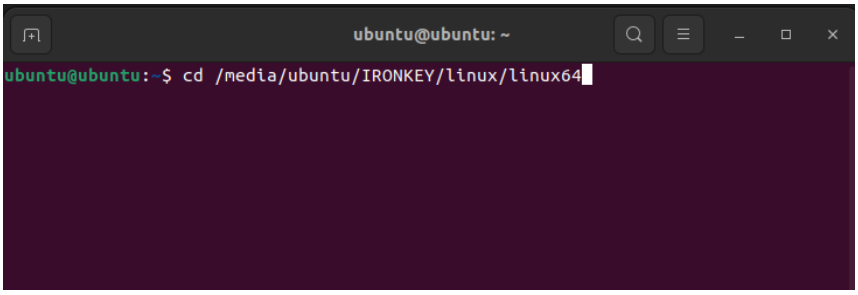


Figura 10.1 – Navegación en la línea de comandos

Utilice el comando **ls** (lista) en el símbolo del sistema actual y, a continuación, pulse INTRO. De este modo obtendrá la lista de archivos y/o carpetas en la carpeta linux64.

De este modo verá la lista de los cuatro comandos de IronKey Linux (*Figura 10.2*)

- ikD500S_about
- ikD500S_login
- ikD500S_logout
- ikD500S_resetdevice

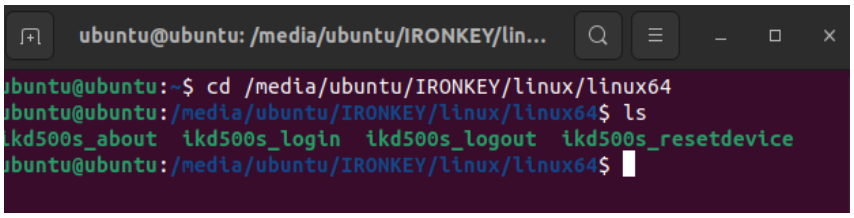


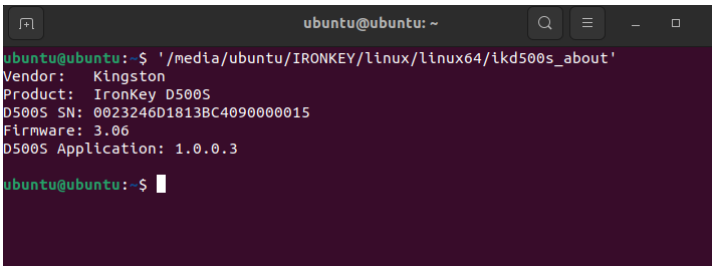
Figura 10.2 — Visualización de los archivos de comandos de IronKey Linux

Nota: En los nombres de los comandos y carpetas (directorios) se hace distinción entre las letras mayúsculas y minúsculas. Por ejemplo, 'linux64' NO es lo mismo que 'Linux64'. Al escribir el comando también debe respetarse la sintaxis exacta, como se muestra. Algunas distribuciones de Linux pueden requerir la introducción del nombre de usuario para ejecutar comandos (por ejemplo, "ubuntu" en este ejemplo).

Uso del dispositivo (entorno Linux)

Uso de los comandos de D500S

Acerca de D500S

IkD500S_about (Acerca de D500S, *Figura 10.3*) Este comando cargará información acerca de la unidad D500S, como: • Proveedor • Producto • Número de serie de D500S • Versión del firmware • Versión del software	 **Figura 10.3 – ikD500S_about (Acerca de IronKey D500S)**

Inicio de sesión de D500S

ikD500S_login

Una vez inicializada la unidad D500S en un sistema Windows o macOS compatible, podrá acceder a la partición de datos protegida iniciando una sesión del dispositivo con la contraseña de D500S que haya creado.

Para ello, efectúe el siguiente procedimiento:

1. Abra una ventana de aplicación 'Terminal'.

2. Escriba el siguiente comando junto al símbolo del sistema del teminal: **cd /media/ubuntu/IRONKEY/linux/linux64**

3. Ahora, con la línea de comando en **/media/ubuntu/IRONKEY/linux/linux64$**, escriba lo siguiente: comando para iniciar sesión del dispositivo: **./ikD500S_login*** y pulse INTRO. (Nota: en los nombres de los comandos y las carpetas se hace distinción entre las letras mayúsculas y minúsculas, y la sintaxis de los comandos debe respetarse con exactitud. Además, algunas distribuciones pueden requerir que introduzca su nombre de usuario; por ejemplo, "ubuntu" en este ejemplo.)

4. Tras un inicio de sesión correcto, el volumen de datos protegido se abrirá en el escritorio y podrá proceder a utilizar la unidad D500S (más información acerca del procedimiento de inicio de sesión en la próxima página)

*Nota: Algunas distribuciones de Linux requieren privilegios de superusuario (raíz) para ejecutar correctamente los comandos de la unidad D500S en la ventana de aplicaciones del terminal.

Uso del dispositivo (entorno Linux)

Inicio de sesión de D500S (continuación)

IkD500S_login (Desbloquear D500S, *Figura 10.4*)

En función de cómo haya configurado la unidad, es posible que durante el proceso de inicio de sesión se le presenten diversas opciones sobre cómo desea desbloquear la unidad.

Si durante la inicialización se habilitaron los perfiles de contraseña de **administrador/usuario**, se le presentarán las siguientes opciones de inicio de sesión.

1.) Elija iniciar sesión como administrador o usuario
2.) Elija desbloquear las particiones de administrador o de usuario (si han sido habilitadas)
3.) Introduzca la contraseña de inicio de sesión de administrador o de usuario, según proceda, para autenticar el dispositivo y desbloquearlo.

Nota: Si durante la inicialización NO se habilitaron los perfiles de administrador/usuario (modo de Sólo usuario), solamente se le pedirá que introduzca la contraseña del dispositivo para autenticarse.

Importante: Como ya se ha mencionado, Linux no admite las frases de contraseña, y la unidad D500S tendrá que configurarse con una contraseña compleja para iniciar sesión en Linux (*Figura 10.5*)

Figura 10.4 – ikD500S_login (desbloqueo de D500S)

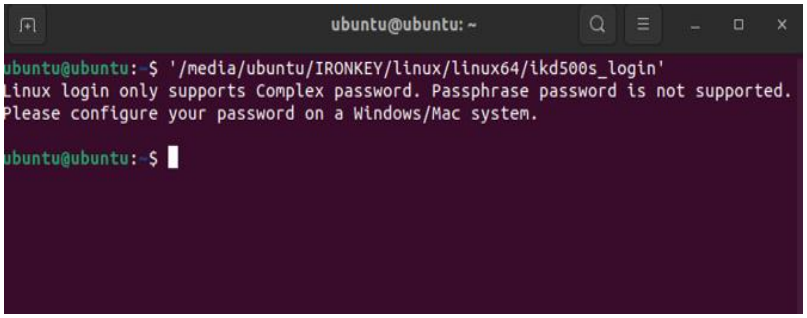


Figura 10.5 — Intento de inicio de sesión con Frase de contraseña no admitida.

Uso del dispositivo (entorno Linux)

Inicio de sesión de D500S (continuación)

Consecuencias de introducir una contraseña de inicio de sesión incorrecta

Durante el proceso de inicio de sesión, si se introduce una contraseña correcta, tendrá otra oportunidad de introducir la correcta. Sin embargo, existe una función de protección integrada, que lleva un seguimiento de los intentos de inicio de sesión fallidos. Si este número alcanza el valor preconfigurado de 10 intentos fallidos de introducción de contraseña, tanto de administrador como de usuario, las consecuencias serán las siguientes:

Contraseñas de Admin/Usuario habilitados

- **Inicio de sesión de usuario:** bloqueo del usuario; se requiere iniciar sesión como administrador. (*Figura 10.6*) Nota: la contraseña de usuario puede ser restablecida por el inicio de sesión de administrador en sistemas Windows o macOS compatibles.
- **Inicio de sesión de administrador:** criptoborrado de la unidad; los datos se pierden para siempre. Se requiere restablecer el dispositivo. (*Figura 10.7*)

Modo de Sólo usuario (administrador/usuario no habilitado)

- **Inicio de sesión de usuario:** criptoborrado de la unidad; los datos se pierden para siempre. Se requiere restablecer el dispositivo. (*Figura 10.7*)

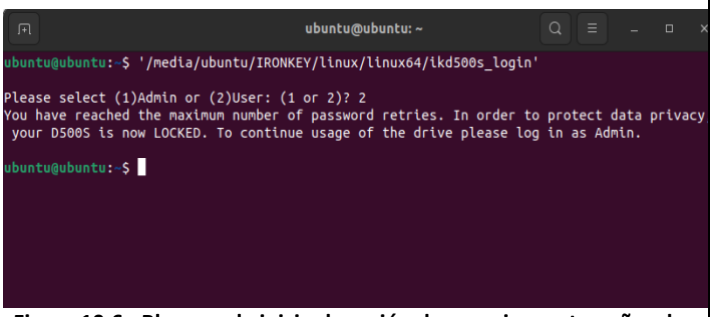


Figura 10.6 - Bloqueo de inicio de sesión de usuario, contraseñas de administrador/usuario habilitadas

Figura 10.7 — Alcanzado el número máximo de intentos fallidos (Restablecimiento de la unidad)

Cierre de sesión de D500S

IkD500S_logout (bloqueo del dispositivo)

Cuando termine de usar la unidad D500S, cierre la sesión del dispositivo y proteja los datos. Para ello, siga el mismo procedimiento explicado en la página 39, y utilice el siguiente comando de cierre de sesión correcto del dispositivo. **./ikD500S_login** y pulse INTRO (Nota: En los nombres de los comandos y carpetas se hace distinción entre las letras mayúsculas y minúsculas, y la sintaxis de los comandos debe respetarse con exactitud. (*Figura 10.8*)

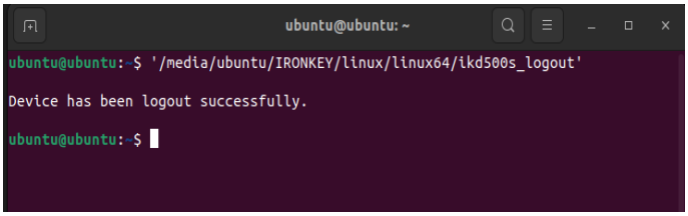


Figura 10.8 — Cierre de sesión de D500S

Uso del dispositivo (entorno Linux)

Restablecimiento del dispositivo D500S

ikD500S_resetdevice
Como ya se ha mencionado en la página 41, en caso de olvidar la contraseña de administrador/usuario, podrá utilizar el comando de restablecimiento para restablecer la unidad y poder volver a usarla. Este procedimiento le permitirá crear una nueva contraseña, aunque para proteger la privacidad de sus datos, la unidad D500S ejecutará un criptoborrado y formateará la partición de datos protegida. **Esto significa que se perderán todos sus datos.**

Para utilizar el comando de restablecimiento del dispositivo, efectúe el mismo procedimiento explicado en la página 39, y utilice el siguiente comando de cierre de sesión correcto del dispositivo: **./ikD500S_resetdevice** y pulse INTRO (Nota: En los nombres de los comandos y carpetas se hace distinción entre las letras mayúsculas y minúsculas, y la sintaxis de los comandos debe respetarse con exactitud. (*Figura 10.9*)

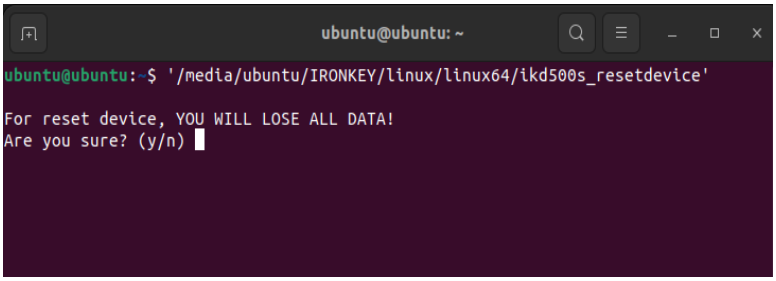


Figura 10.9 - Comando de restablecimiento del dispositivo

Una vez utilizado el comando Restablecer dispositivo, se le pedirá que cree una nueva contraseña compleja, que deberá contener:

- entre 8 y 16 caracteres, y al menos tres (3) de las siguientes opciones:

  - **MAYÚSCULA(S)**
  - **minúscula(s)**
  - **carácter(es) numérico(s)**
  - **carácter(es) especial(es) (!, $, etc.)**

(*Figura 10.10*)

Nota: el comando Restablecer dispositivo inicializará la unidad en modo de Sólo usuario (contraseña única, usuario único). Para habilitar perfiles de contraseñas de inicio de sesión de administrador/usuario, la unidad D500S deberá ser configurada en un sistema Windows o macOS para poder acceder a esa opción.

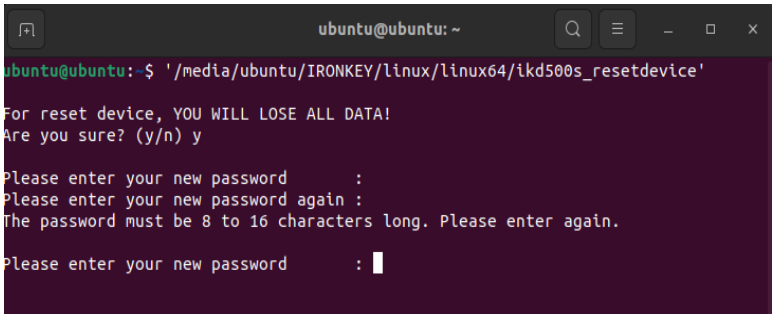


Figura 10.10 — Comando Restablecer dispositivo, creación de contraseña

IRONKEY™ D500S
CLÉ USB 3.2 GEN 1 SÉCURISÉE

Guide de l'utilisateur

Sommaire

Figure 1 – IronKey D500S

Introduction

La Kingston IronKey D500S est une clé USB offrant un niveau de sécurité de classe militaire, basée sur les caractéristiques qui ont fait la réputation d'IronKey dans la protection des informations sensibles. Elle est certifiée FIPS 140-3 niveau 3 (en cours), ce qui implique de nouvelles améliorations de sécurité du NIST exigeant des mises à niveau sécurisées du processeur pour une sécurité accrue. Le chiffrement et le déchiffrement sont exécutés sur la D500S. Aucune trace ne reste sur le système hôte, ce qui l'immunise contre les renifleurs de mots de passe en mémoire. Outre le chiffrement matériel XTS-AES 256 bits, elle est dotée d'un boîtier en zinc robuste qui est étanche à l'eau*, à la poussière* et résistant à l'écrasement, et scellé avec de l'époxy pour protéger les composants internes contre les attaques par pénétration.

La D500S prend en charge l'option de mots de passe multiples (Admin, Utilisateur, Récupération à usage unique et Effacement chiffré) avec les modes Complexe ou Phrase de passe classiques**. 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 classiques, le mode Phrase de passe permet d'utiliser un code numérique, une phrase, une liste de mots ou même des paroles de chanson de 10 à 128 caractères. L'administrateur peut activer un utilisateur, créer deux partitions de données de taille personnalisée séparant les fichiers de connexion Admin et Utilisateur, activer un mot de passe de récupération à usage unique, un mot de passe d'effacement chiffré et réinitialiser le mot de passe Utilisateur pour restaurer l'accès aux données.

Pour faciliter la saisie du mot de passe, le symbole « œil » peut être activé pour révéler le mot de passe saisi, ce qui réduit les fautes de frappe pouvant générer des échecs de tentative de connexion. Pour une plus grande tranquillité d'esprit, la D500S utilise un firmware signé numériquement qui l'immunise contre les logiciels malveillants BadUSB, ainsi qu'une protection contre les attaques par force brute afin d'empêcher toute tentative de deviner le mot de passe. La protection contre les attaques par force brute verrouille le mot de passe Utilisateur ou le mot de passe de récupération à usage unique si 10 mots de passe incorrects sont saisis de suite, et chiffre le lecteur si le mot de passe Admin est saisi incorrectement 10 fois de suite.

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

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 D500S offre de nombreuses options de personnalisation, est conforme à la norme TAA/CMMC, et est assemblée aux États-Unis.

La D500S bénéficie d'une garantie limitée de 5 ans avec le support technique gratuit de Kingston.

* Veuillez vous reporter aux spécifications de la fiche technique. Le produit doit être propre et sec avant toute utilisation.
** Le mode Phrase de passe n'est pas pris en charge sur les systèmes Linux.
***Clavier virtuel : Prend uniquement en charge l'anglais américain sur Microsoft Windows et macOS.

IronKey Fonctionnalités de la D500S

- Certifiée FIPS 140-3 niveau 3 (en cours) avec un chiffrement matériel XTS-AES 256 bits (le chiffrement ne peut jamais être désactivé).
- Protection contre les attaques par force brute et BadUSB
- Options de mots de passe multiples
- Modes de mot de passe Complexe ou Phrase de passe
- Option unique de double partition et mot de passe d'effacement chiffré
- Symbole en forme d'œil pour afficher les mots de passe saisis afin de réduire les tentatives de connexion infructueuses
- Clavier virtuel pour se protéger des enregistreurs de frappe et des enregistreurs d'écran
- Paramètres forcée/basée sur la session de 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 Admin.
- Compatible avec Windows, macOS et Linux (consulter la fiche technique pour plus de détails)

À propos de ce manuel

Ce manuel d'utilisation traite de la clé USB IronKey D500S. Il est basé sur la version en sortie d'usine, sans personnalisation.

Configuration système

Plateforme PC • Intel, AMD et Apple M1 SOC • 15 Mo d'espace disque libre • Port USB 2.0 – 3.2 disponible • Deux lettres de lecteur consécutives après le dernier disque physique* ***Remarque :** Voir la section « Conflit de lettres de lecteur » à la page 35.	**Prise en charge des systèmes d'exploitation PC** • Windows 11 • Windows 10
Plateforme Mac • 15 Mo d'espace disque libre • Port USB 2.0 – 3.2	**Prise en charge des systèmes d'exploitation Mac** • macOS macOS 11.x - 14.x
Plateforme Linux • 5 Mo d'espace disque libre • Port USB 2.0 – 3.2	**Prise en charge des systèmes d'exploitation Linux** • Linux Kernel v4.4+

Recommandations

Pour que la D500S 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 D500S sur un périphérique équipé d'un port USB, par exemple un clavier ou un concentrateur/hub alimenté par USB, comme illustré dans la ***Figure 1.2***.

Figure 1.1 – Utilisation conseillée

Figure 1.2 – Utilisation déconseillée

Utiliser le bon système de fichiers

La IronKey D500S est livrée préformatée avec le système de fichiers FAT32. Elle fonctionne sur les systèmes Windows, macOS et Linux*. 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

To keep your data safe, Kingston recommends that you:

- Procédez à une analyse antivirus sur votre ordinateur avant de configurer et d'utiliser la D500S 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 l'endommager et nécessiter un reformatage, ce qui effacera vos données.
- Ne communiquez jamais le mot de passe de votre clé USB à quiconque.

Obtenir les dernières mises à jour et informations

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

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

*** La D500S ne prend pas en charge l'initialisation prête à l'emploi sous Linux. Elle devra être entièrement initialisée et configurée sur un système Windows ou macOS pris en charge avant qu'elle ne puisse être utilisé sous Linux. Vous trouverez des informations supplémentaires dans la section Linux de ce guide de l'utilisateur, à la page 37.**

Meilleures pratiques pour la configuration des mots de passe

Votre D500S est livrée avec de solides contre-mesures de sécurité. Notamment une protection contre les attaques par force brute qui empêchera un pirate de deviner des mots de passe en limitant les échecs de tentative de saisie mot de passe à 10. Lorsque cette limite est atteinte, la D500S efface automatiquement les données chiffrées et s'auto-formate aux paramètres d'usine.

Mots de passe multiples
La D500S 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 D500S peut prendre en charge trois mots de passe différents que vous pouvez utiliser pour récupérer les données : Admin, Utilisateur et de récupération à usage unique.

La D500S 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'Admin peut accéder à la clé USB à tout moment et configurer des options pour l'Utilisateur : l'Admin est une sorte de « super utilisateur ». En outre, l'Admin 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'Admin. 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 D500S peut être réinitialisée et réutilisée, mais les données antérieures seront définitivement supprimées.

Modes pour mot de passe
La D500S prend en charge deux modes de mot de passe :

Complexe
Un mot de passe complexe doit comporter 8 à 16 caractères et utiliser au moins 3 de ces types de caractères :

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

Phrase de passe
La D500S prend en charge les phrases de passe de 10 à 128 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 D500S, la langue du mot de passe peut correspondre à la langue sélectionnée pour la clé USB. Cela vous permet de sélectionner plusieurs mots, une phrase, les paroles d'une chanson, un vers de poésie, etc. Les bonnes phrases de passe font partie des types de mots de passe les plus difficiles à deviner pour un pirate, tout en étant plus faciles à retenir pour les utilisateurs.

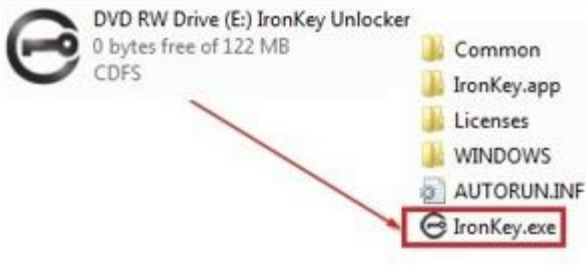
Configurer ma clé USB

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

Accès à la clé USB (Environnement Windows)

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

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

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

Accès à la clé USB (environnement macOS)

Insérez la D500S 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 lecteur « IRONKEY » s'affiche sur l'ordinateur. (*Figure 3.3*)

• Double-cliquez sur l'icône de CD-ROM IronKey. • Double-cliquez ensuite sur l'icône de l'application IronKey.app affichée dans la fenêtre illustrée à la Figure 3.3. Le processus d'initialisation démarrera aussi.	 **Figure 3.3 – Lecteur IronKey**

Initialisation de la clé USB (environnements Windows & macOS)

Langue et Contrat de licence utilisateur final

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

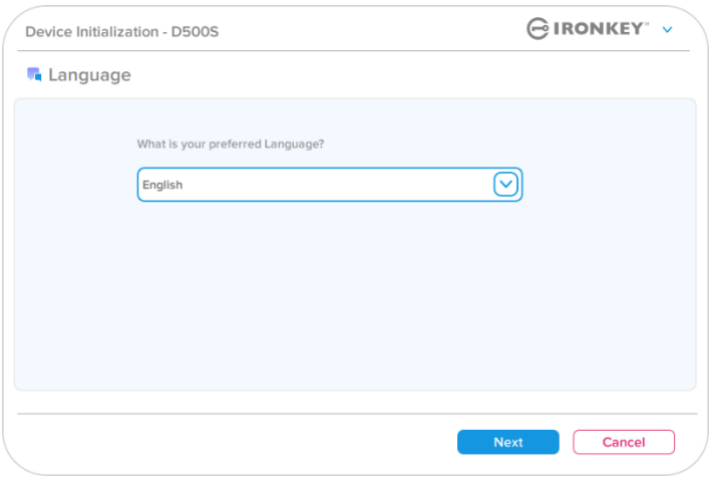


Figure 4.1 – Sélection de la langue

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

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

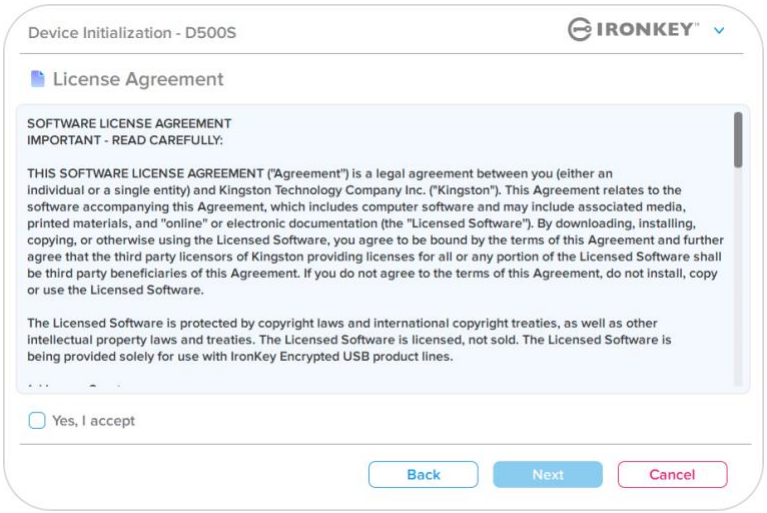


Figure 4.2 – Contrat de licence

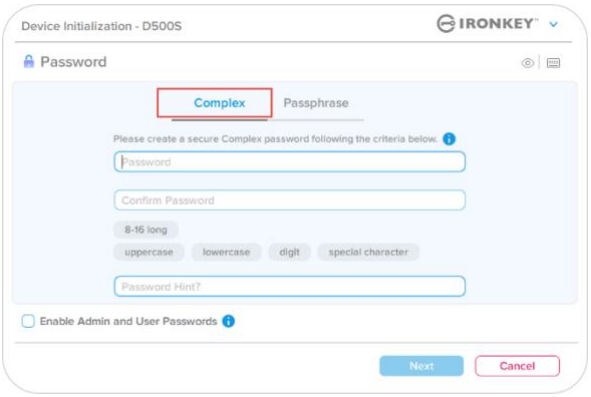
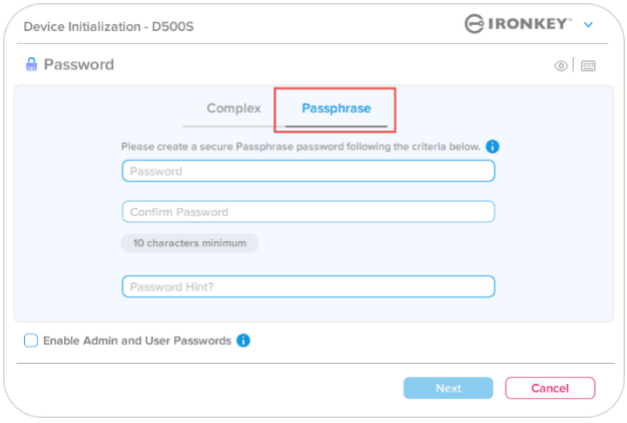
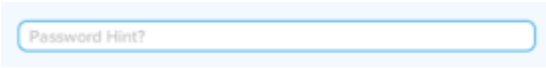
Initialisation de la clé USB

Sélection du mot de passe

Sur l'écran de demande de Mot de passe, vous pourrez créer un mot de passe pour protéger vos données sur la D500S en utilisant les modes Complexe ou Phrase de passe (*Figures 4.3- 4.4*). En outre, les options Mots de passe multiples Admin/Utilisateur peuvent également être activées sur cet écran. Avant de procéder à la sélection du mot de passe, veuillez consulter la rubrique Activation des mots de passe Admin/Utilisateur ci-dessous pour mieux comprendre ces fonctionnalités.

Remarque : Une fois que le mode Complexe ou Phrase de passe est choisi, il ne peut pas être modifié, sauf si la clé USB est réinitialisée.

Pour commencer, créez votre mot de passe dans le champ « Password » (Mot de passe), puis saisissez-le à nouveau dans le champ « Confirm Password » (Confirmer le mot de passe). Le mot de passe doit respecter les critères suivants pour que le processus d'initialisation vous autorise à continuer :

Mot de passe complexe • Doit contenir entre 8 et 16 caractères. • Doit contenir trois (3) des types de caractères suivants : ○ Majuscule ○ Minuscule ○ Chiffre ○ Caractères spéciaux (!,$,&, etc..)	 **Figure 4.3 – Mot de passe complexe**
Phrase de passe • Doit contenir : ○ 10 caractères minimum ○ 128 caractères maximum	 **Figure 4.4 – Phrase de passe**
Indice de mot de passe (facultatif) Un indice de mot de passe peut être utile pour fournir une indication de ce qu'est le mot de passe, si jamais vous l'oubliez. **Remarque :** L'indice NE DOIT PAS être le mot de passe lui-même.	 **Figure 4.5 – Champ Password Hint (Indice de mot de passe)**

Initialisation de la clé USB

Valid and invalid passwords

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

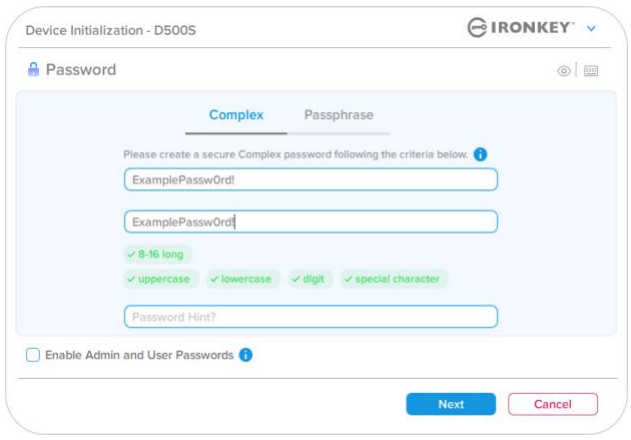


Figure 4.6a – Condition de mot de passe complexe remplie

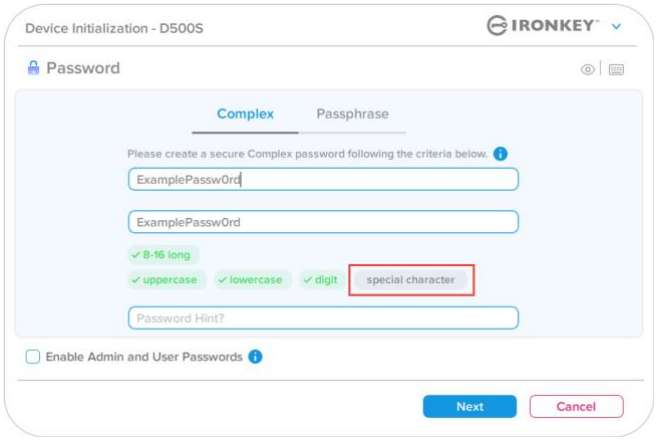


Figure 4.6b – Condition de mot de passe complexe facultative

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

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

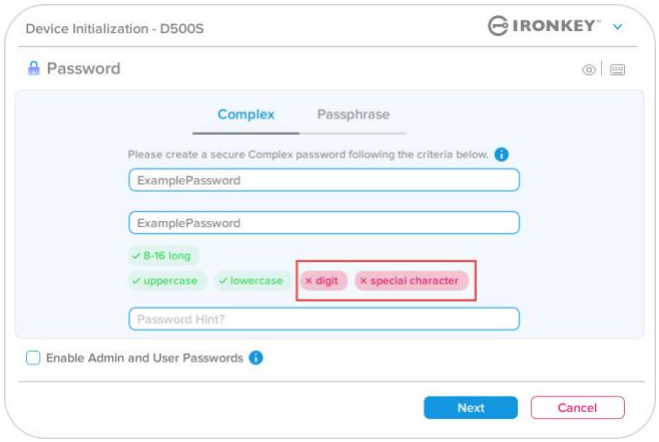


Figure 4.7 – Conditions de mot de passe non remplies

Initialisation de la clé USB

Clavier virtuel

La D500S est dotée d'un clavier virtuel qui peut être utilisé pour se protéger contre les enregistreurs de frappe.

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

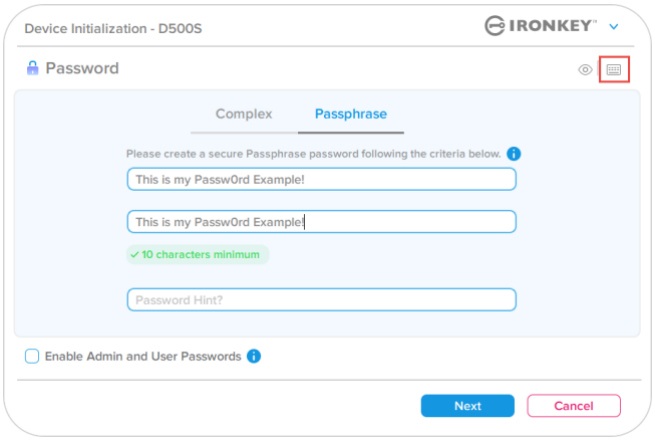


Figure 4.8 – Activation du clavier virtuel

- Une fois que le clavier virtuel apparaît, vous pouvez également activer la fonction **Screenlogger Protection (Protection contre les enregistreurs d'écran)**. Lors de l'utilisation de cette fonctionnalité, toutes les touches apparaîtront brièvement comme vides. Ce comportement est normal, car il empêche les enregistreurs d'écran de capturer ce sur quoi vous avez cliqué.

- Pour rendre cette fonctionnalité plus robuste, vous pouvez également choisir de randomiser le clavier virtuel en sélectionnant **Randomize (Disposition aléatoire)** dans le coin inférieur droit du clavier. Le clavier sera alors organisé dans un ordre aléatoire.

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

Initialisation de la clé USB

Icône de visibilité du mot de passe

Par défaut, lorsque vous créez un mot de passe, celui-ci s'affiche dans le champ au fur et à mesure que vous la saisissez. Si vous souhaitez « masquer » les caractères au fur et à mesure que vous tapez, vous pouvez activer l'icône en forme 'd'œil' située dans la partie supérieure droite de la fenêtre Device Initialization (Initialisation de l'appareil).

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

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

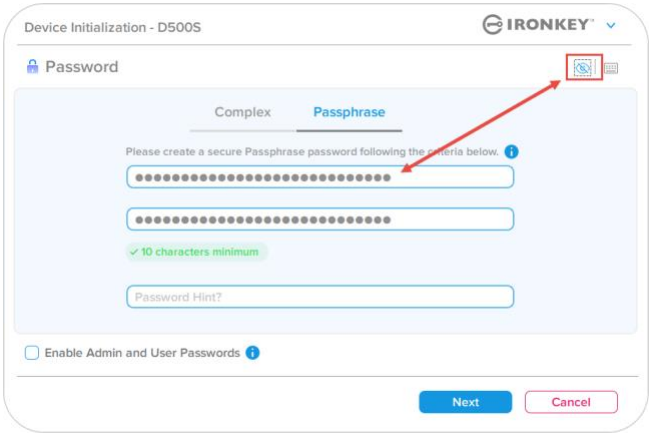


Figure 4.10 - Icône pour « masquer » le mot de passe

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

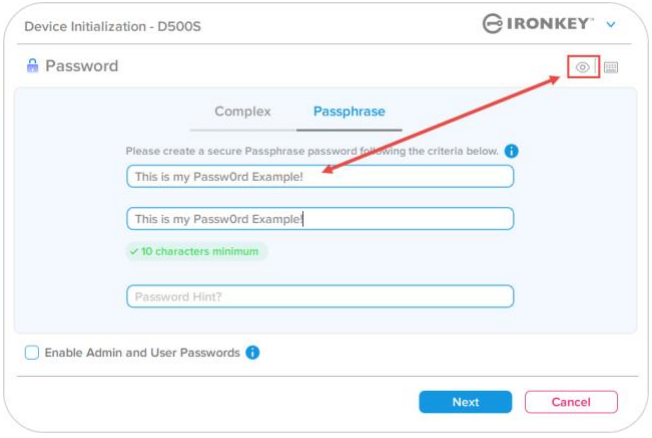


Figure 4.11 - Icône pour « afficher » le mot de passe

Initialisation de la clé USB

Mots de passe Admin et Utilisateur

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

Lorsque les mots de **passe Admin et Utilisateur** sont activés, vous pouvez également accéder aux options suivantes :

- Dual-Partition configuration (Configuration de deux partitions)
- One-Time Recovery password (Mot de passe de récupération à usage unique)
- Forced read-only mode for User login (Mode de lecture seule forcée pour la connexion Utilisateur)
- User password reset (Réinitialisation du mot de passe Utilisateur)
- Force Reset password for User login (Forcer la réinitialisation du mot de passe pour la connexion Utilisateur)
- Crypto-Erase password (Mot de passe d'effacement chiffré)

Pour en savoir plus sur ces options, allez à la page 25 du présent guide.

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

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

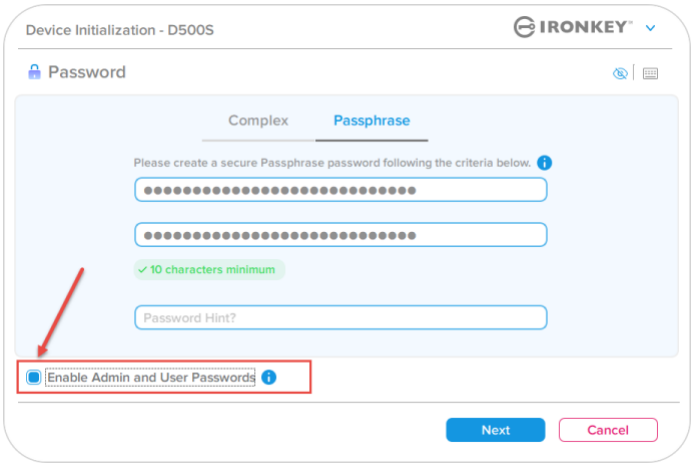


Figure 4.12 – Activation des mots de passe Admin et Utilisateur

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

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

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

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

Initialisation de la clé USB

Mots de passe Admin et Utilisateur

- Si le rôle Admin a été **activé** à l'écran précédent, l'écran suivant demandera le mot de passe Utilisateur (*Figure 4.13*). Le mot de **passe Utilisateur** aura des capacités limitées par rapport au mot de passe Admin ; il fera l'objet d'une section plus détaillée dans le présent guide de l'utilisateur (voir page 23).

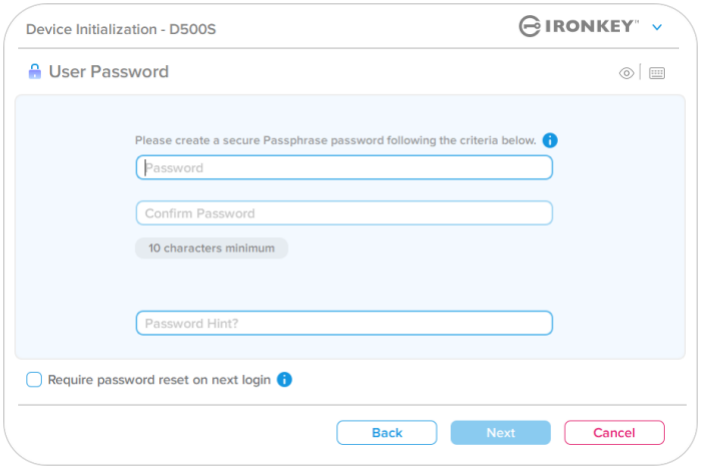


Figure 4.13 – Mot de passe Utilisateur (Admin et Utilisateur activés)

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

  Remarque : Pour des raisons de sécurité, le nouveau mot de passe ne peut pas être identique au mot de passe temporaire.

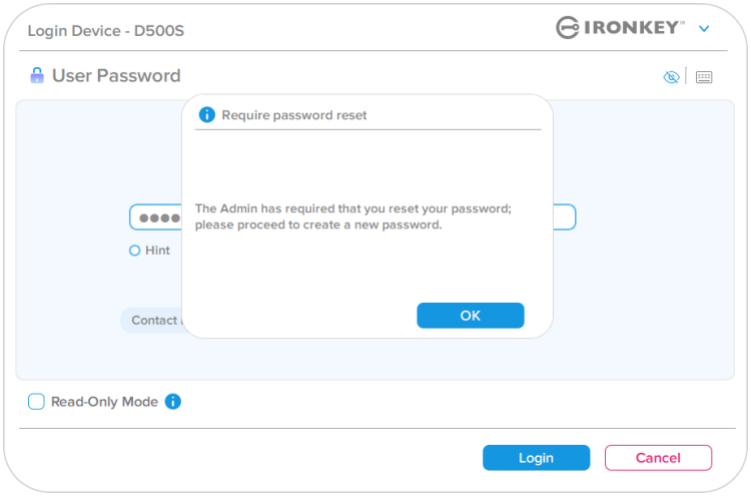


Figure 4.14 – Exiger la réinitialisation du mot de passe à la prochaine connexion (Pour le mot de passe Utilisateur)

Initialisation de la clé USB

Double partition

La clé USB IronKey D500S vous permet de créer deux partitions séparées de taille personnalisée : une pour l'Admin et l'autre pour l'Utilisateur. Si cette fonctionnalité est activée, la connexion Admin aura accès aux **deux** partitions Utilisateur et Admin, tandis que la connexion Utilisateur n'aura accès qu'à la partition Utilisateur. Cette fonctionnalité est utile pour séparer en toute sécurité les privilèges d'accès aux données et aux fichiers entre l'Admin et l'Utilisateur. Elle peut également être utilisée pour activer un magasin de fichiers caché afin d'éviter d'exposer des fichiers non nécessaires sur des systèmes non fiables. La taille des partitions entre l'Admin et l'Utilisateur peut également être ajustée si vous le souhaitez.

REMARQUE : Cette fonctionnalité est *facultative* et peut être désactivée en ne cochant pas la case « Enable Dual Partition » (Activer la double partition) lors de la configuration (*Figure 4.15*)

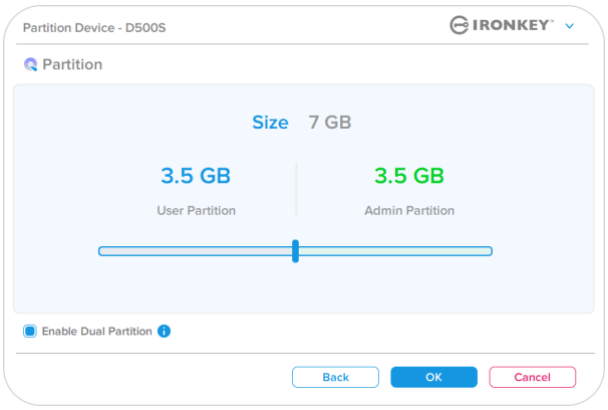


Figure 4.15- Partitionner la clé USB

Pour ajuster et répartir la taille des partitions entre l'Utilisateur et l'Admin, déplacez le curseur vers la gauche ou la droite respectivement (*Figure 4.16*).

- Les partitions peuvent être ajustées par incréments de 0,5 Go.
- Le dimensionnement de la partition est basé sur la capacité totale de l'espace de stockage disponible sur la partition cachée.
- Par défaut, le curseur de double partition est configuré pour diviser l'espace de stockage de manière égale entre Admin et Utilisateur, jusqu'à ce qu'il soit ajusté manuellement.
- La plus petite taille de partition pouvant être allouée est de 1 Go.

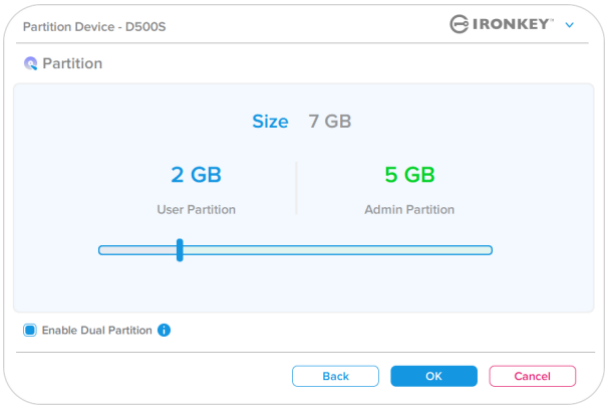


Figure 4.16- Partitionner la clé USB, curseur ajusté

Connexion Admin

Une fois que la clé USB est entièrement configurée avec les deux partitions activées, la connexion Admin proposera une option pour la déverrouiller afin d'accéder à la partition Admin OU à la partition Utilisateur à chaque connexion réussie. (*Figure 4.17*)

REMARQUE : Vous ne pouvez ouvrir qu'une seule partition à la fois. Les partitions Utilisateur et Admin ne peuvent pas être déverrouillées en même temps.

La connexion Utilisateur ne propose pas cette option ; elle déverrouille automatiquement la partition Utilisateur uniquement.

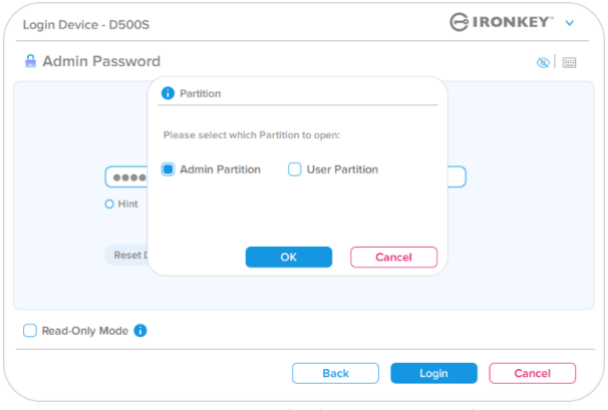


Figure 4.17 – Exemple de connexion Admin, sélection de la partition

Initialisation de la clé USB

Informations de contact

Entrez vos informations de contact dans les zones de texte prévues à cet effet (voir la *Figure 4.18*).

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

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

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

Le champ **« Details » (Détails)** peut contenir jusqu'à 156 caractères, mais ne doit pas contenir le mot de passe exact.

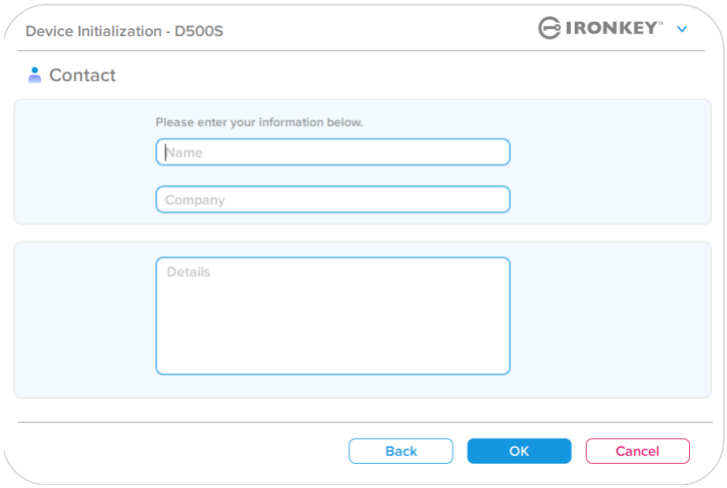


Figure 4.18 – Informations de contact

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

Utilisation de la clé USB (environnements Windows & macOS)

Connexion pour l'Admin 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 D500S se lancera, en affichant d'abord l'écran de connexion User Password (Mot de passe Utilisateur). À partir de là, vous pouvez vous connecter avec le mot de passe Utilisateur, afficher les informations de contact saisies ou vous connecter en tant qu'Admin (*Figure 5.1*). Si vous cliquez sur le bouton « Login as Admin » (Se connecter en tant qu'Admin) (illustré ci-dessous), l'application passe au menu de connexion Admin, où vous pouvez vous connecter en tant qu'Admin pour accéder aux paramètres et fonctionnalités associées à ce rôle (*Figure 5.2*).

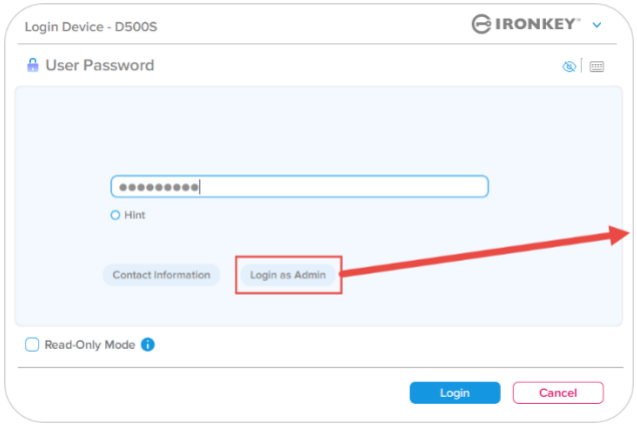


Figure 5.1 – Connexion à l'aide du mot de passe Utilisateur (Admin activé)

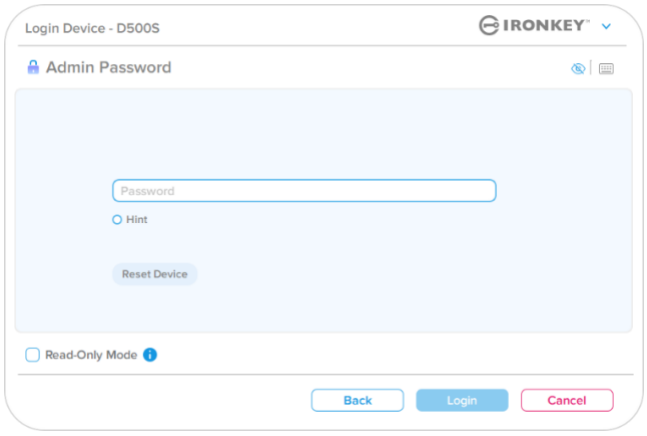


Figure 5.2 – Connexion à l'aide du mot de passe Admin

Connexion en Mode Utilisateur uniquement (Admin non activé)

Comme indiqué précédemment, bien qu'il soit recommandé d'utiliser la fonctionnalité du rôle Admin pour tirer pleinement parti de votre appareil, la clé USB IronKey peut également être initialisée en mode Utilisateur uniquement (mot de passe unique, utilisateur unique). Cette option est destinée aux personnes qui souhaitent une approche simple, avec un seul mot de passe, pour sécuriser leurs données sur leur clé USB. (*Figure 5.3*)

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

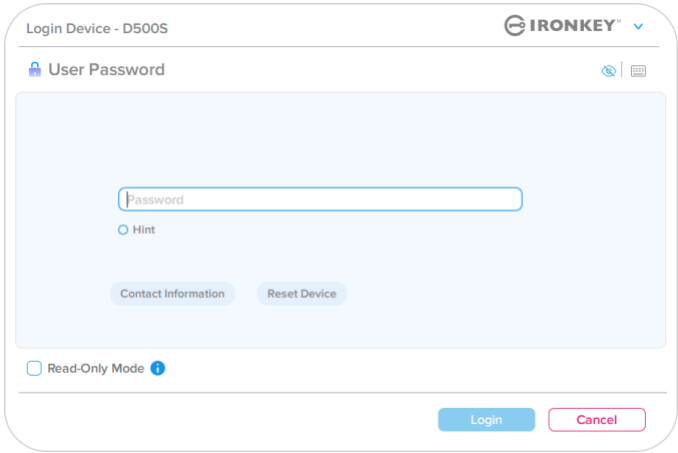


Figure 5.3 – Connexion à l'aide du mot de passe Utilisateur (Admin non activé)

Utilisation de la clé USB

Déverrouillage en mode lecture seule

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

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

Pour déverrouiller la clé USB en mode lecture seule :

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

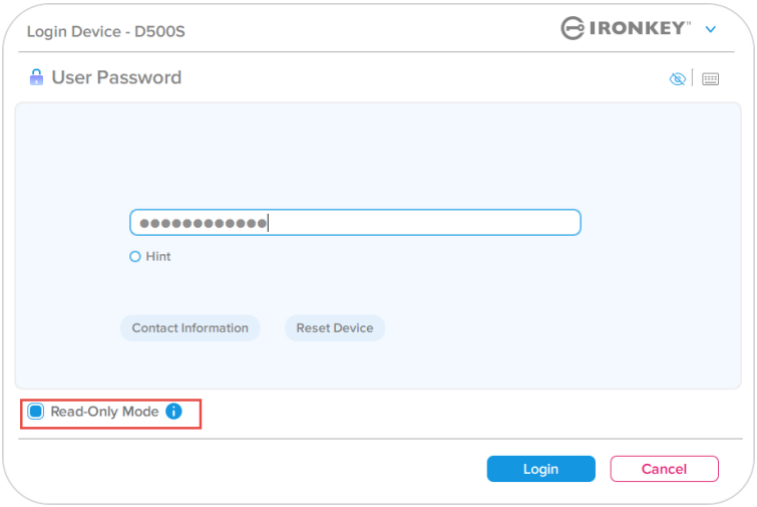


Figure 5.4 – Mode lecture seule

Si vous souhaitez déverrouiller la clé USB avec un accès complet en lecture/écriture à la partition de données sécurisée, vous devez arrêter la D500S et vous reconnecter, en laissant la case « Read-Only Mode » (Mode lecture seule) décochée.

Remarque : Les options Admin de la D500S ont une fonctionnalité de mode lecture seule forcée pour les données Utilisateur, ce qui signifie que l'Admin peut forcer le déverrouillage de la connexion Utilisateur en lecture seule (voir page 31 pour plus de détails).

Utilisation de la clé USB

Protection contre les attaques par force brute

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

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

Admin/Utilisateur activé	**Protection contre les attaques par force brute Comportement de la clé USB (10 tentatives de saisie de mot de passe infructueuses)**	**Suppression des données et réinitialisation de la clé USB ?**
Mot de passe Utilisateur	Verrouillage du mot de passe. Connectez-vous en tant qu'Administrateur ou utilisez le mot de passe de récupération à usage unique pour réinitialiser le mot de passe Utilisateur	NON
Mot de passe Admin	Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimées définitivement	**OUI**
Mot de passe de récupération à usage unique	Verrouillage du mot de passe, le bouton de récupération du mot de passe s'estompe et devient inutilisable. Se connecter en tant qu'Admin pour réinitialiser le mot de passe	NON
Utilisateur uniquement Un seul utilisateur, un seul mot de passe (Admin/Utilisateur NON activé)	**Protection contre les attaques par force brute Comportement de la clé USB (10 tentatives de saisie de mot de passe infructueuses)**	**Suppression des données et réinitialisation de la clé USB ?**
Mot de passe Utilisateur	Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimées définitivement	**OUI**

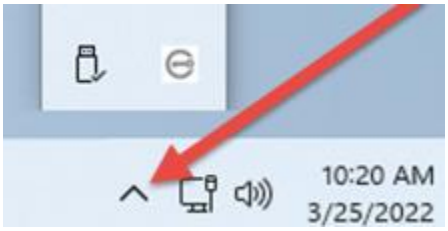
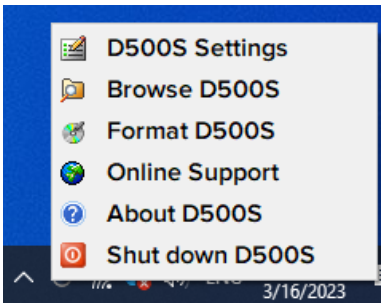
* Une fois que vous vous êtes authentifié avec succès sur la clé USB, le compteur d'échecs de connexion sera réinitialisé en fonction de la méthode de connexion utilisée. L'effacement chiffré effacera tous les mots de passe, les clés de chiffrement et les données ; **vos données seront perdues définitivement.**

Accès à mes fichiers sécurisés

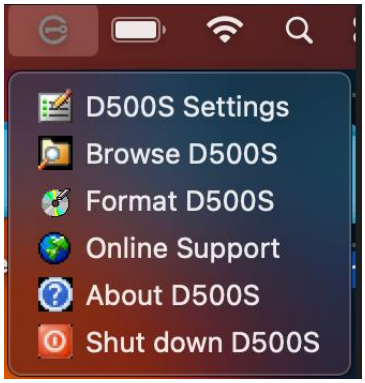
Après avoir déverrouillé la clé USB, vous pouvez accéder à vos fichiers sécurisés. Les fichiers sont automatiquement chiffrés et déchiffrés lorsque vous les enregistrez ou les ouvrez sur la clé USB. Cette technologie vous permet de travailler comme vous le feriez avec un disque ordinaire, tout en offrant une sécurité forte et permanente.
Conseil : Vous pouvez également accéder à vos fichiers en cliquant avec le bouton droit sur l'icône IronKey dans la barre des tâches de Windows et en cliquant sur **Browse D500S (Parcourir la D500S)** (*Figure 6.2*)

Options de la clé USB - (Environnement Windows)

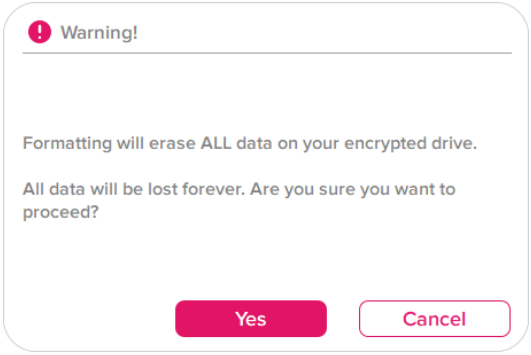
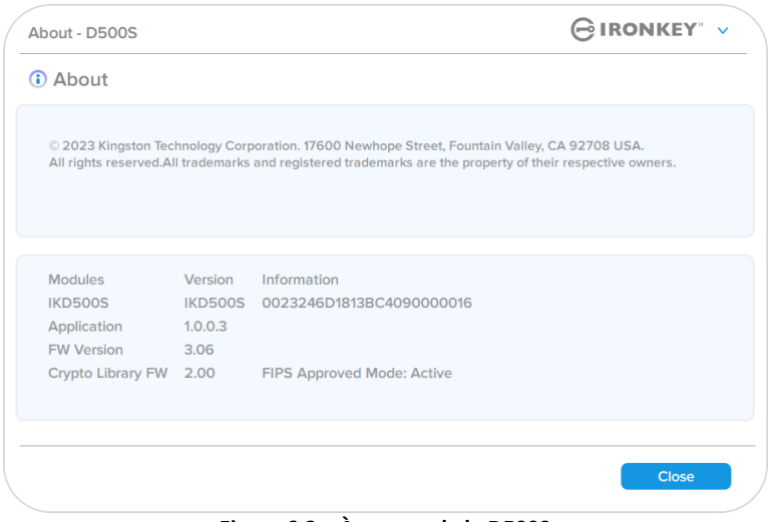
Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles (*Figure 6.2*). Les détails concernant ces options se trouvent aux pages 21 à 25 du présent manuel.

• Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre (*Figure 6.1*)	 **Figure 6.1 – Icône IronKey dans la barre des tâches**
• Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles (*Figure 6.2*). Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.	 **Figure 6.2 – Clic droit sur l'icône IronKey pour accéder aux options de la clé USB**

Options de la clé USB- (environnement macOS)

• Lorsque vous êtes connecté à la clé USB, une icône IronKey D500S se trouve dans le menu macOS illustré dans la Figure 6.3 ; elle permet d'afficher les options disponibles de la clé USB. Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.	 **Figure 6.3 – Icône de barre de menu macOS/menu des options de la clé USB**

Options de la clé USB

Paramètres de la D500S ::	• 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 D500S : » du présent manuel).
Parcourir la D500S :	• Permet de visualiser vos fichiers sécurisés.
Formater la D500S : Permet de formater la partition de données sécurisée. (Avertissement : Toutes les données seront supprimées) (*Figure 6.1*) **Remarque :** L'authentification par mot de passe sera requise pour le formatage.	 **Figure 6.1 – Formater la D500S**
Support en ligne :	• Cette fonction ouvre votre navigateur Internet et affiche la page http://www.kingston.com/support pour vous permettre de consulter les informations supplémentaires du support.
À propos de la D500S : Affiche des données détaillées sur la D500S, notamment des informations sur l'application, le firmware et le numéro de série (*Figure 6.2*) **Remarque :** Le numéro de série unique de la clé USB se trouve sous la colonne « Informations ».	 **Figure 6.2 – À propos de la D500S**
Arrêter la D500S :	• Permet de fermer correctement la D500S avant de la déconnecter physiquement du système, en toute sécurité.

Paramètres de la D500S :

Paramètres Admin

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

- **Password (Mot de passe) :** Permet de modifier le mot de passe Admin et/ou l'indice (*Figure 7.1*)
- **Contact Info (Informations de contact) :** Permet d'ajouter/d'afficher/de modifier les informations de contact (*Figure 7.2*)
- **Language (Langue) :** Permet de modifier la langue actuelle (*Figure 7.3*)
- **Admin Options (Options Admin) :** Permet d'activer des fonctionnalités supplémentaires telles que : (*Figure 7.4*)
    - changer le mot de passe de l'utilisateur ;
    - réinitialiser le mot de passe de connexion (pour le mot de passe Utilisateur) ;
    - activer un mot de passe de récupération à usage unique ;
    - activer un mot de passe d'effacement chiffré ;
    - forcer le mode lecture seule pour les données Utilisateur.

REMARQUE : Des détails supplémentaires sur les options Admin sont indiqués à partir de la page 26.

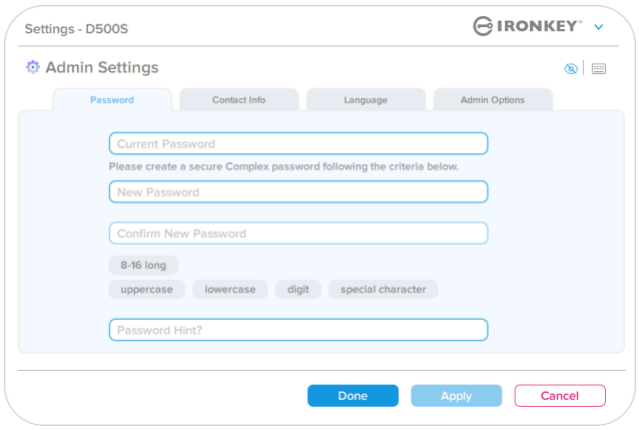


Figure 7.1 – Options de mot de passe

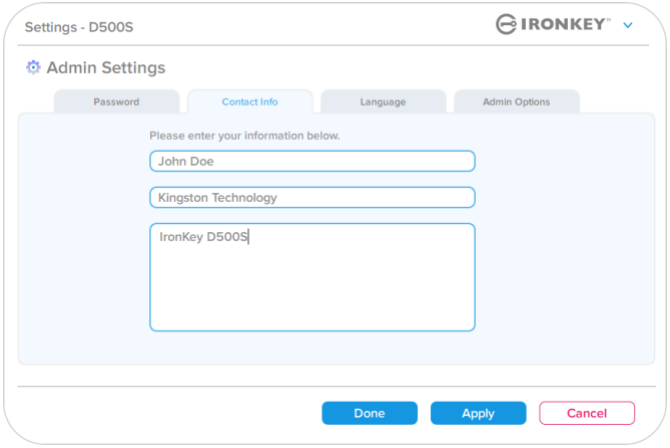


Figure 7.2 – Informations de contact

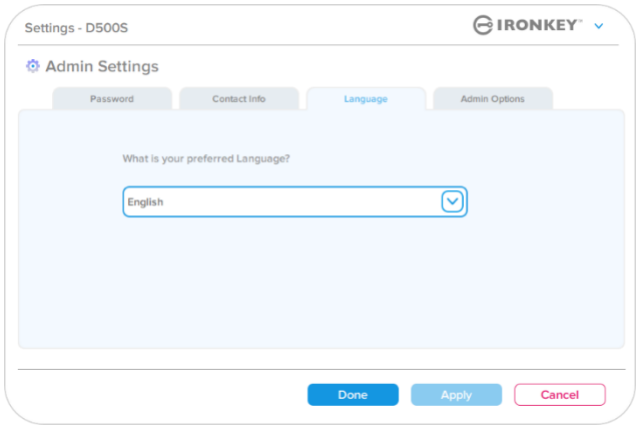


Figure 7.3 – Options de langue

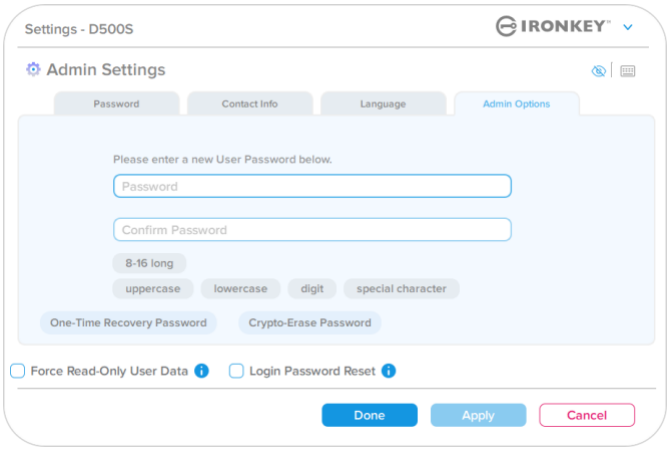
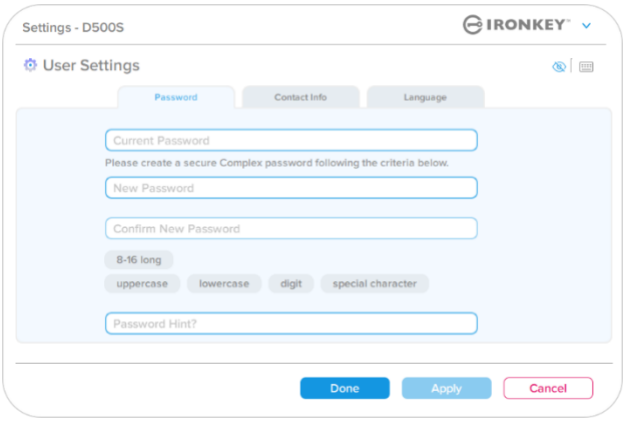
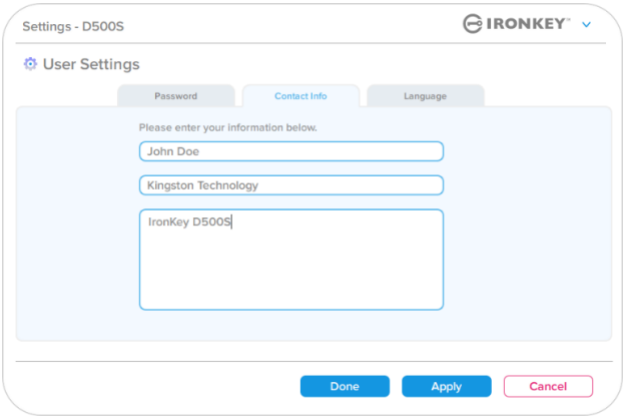
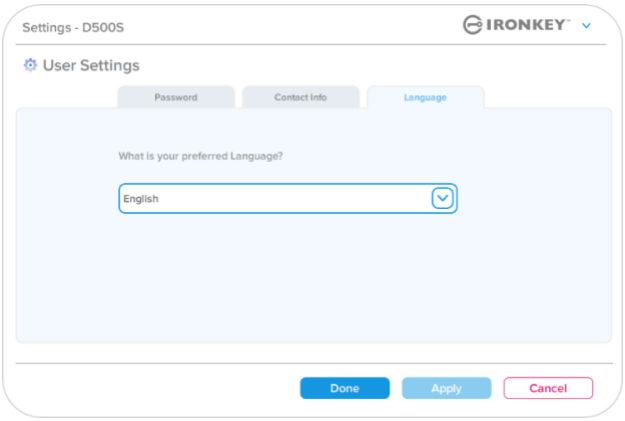


Figure 7.4 – Options Admin

Paramètres de la D500S :

Paramètres Utilisateur : Admin activé

La connexion Utilisateur limite l'accès aux paramètres suivants :

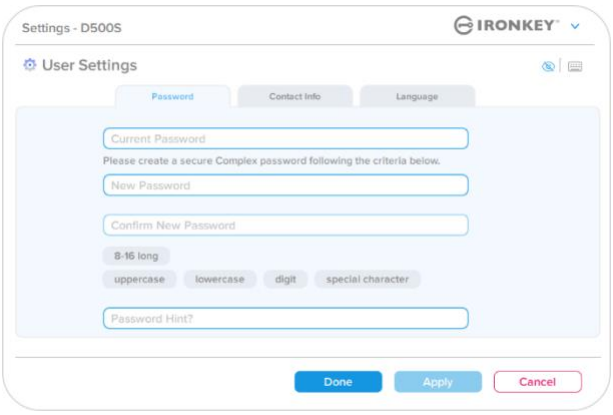
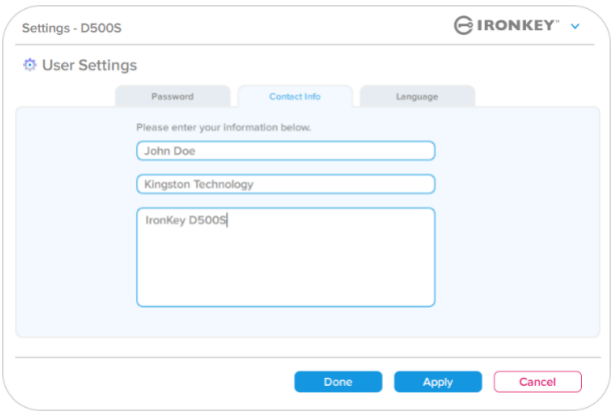
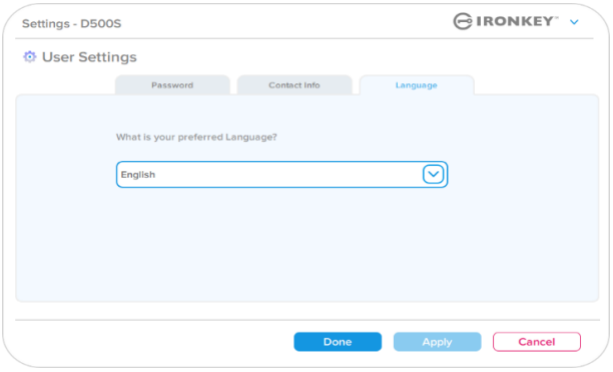
Password (Mot de passe) : Permet de modifier le mot de passe Utilisateur et/ou l'indice (*Figure 7.5*)	 **Figure 7.5 – Options de mot de passe (Admin activé : connexion Utilisateur)**
Contact Info (Informations de contact) : Permet d'ajouter/d'afficher/de modifier vos informations de contact (*Figure 7.6*)	 **Figure 7.6 – Informations de contact (Admin activé : connexion Utilisateur)**
Language (Langue) : Permet de modifier la langue actuelle (*Figure 7.7*)	 **Figure 7.7 – Paramètres de langue (Admin activé : connexion Utilisateur)**

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

Paramètres de la D500S :

Paramètres Utilisateur : Admin non activé

Comme mentionné précédemment, l'initialisation de la D500S sans activer les mots de passe Admin et Utilisateur configurera la clé USB dans une configuration **Mot de passe unique, Utilisateur unique (mode Utilisateur uniquement)**. Cette configuration n'a pas accès aux options ou fonctionnalités Admin. Cette configuration aura accès aux paramètres suivants de la D500S :

Password (Mot de passe) : Permet de modifier le mot de passe Utilisateur et/ou l'indice (*Figure 7.8*)	 **Figure 7.8 – Options de mot de passe (mode Utilisateur uniquement)**
Contact Info (Informations de contact) : Permet d'ajouter/d'afficher/de modifier vos informations de contact (*Figure 7.9*)	 **Figure 7.9 – Informations de contact (mode Utilisateur uniquement)**
Language (Langue) : Permet de modifier la langue actuelle (*Figure 7.10*)	 **Figure 7.10 – Paramètres de langue (mode Utilisateur uniquement)**

Paramètres de la D500

Modifier et sauvegarder les paramètres

- Chaque fois que les paramètres sont modifiés dans les paramètres de la D500S (par exemple, informations de contact, langue, modification du mot de passe, options Admin, etc.), la clé USB vous invitera à saisir votre mot de passe afin d'accepter et d'appliquer ces modifications (*Figure 7.11*).

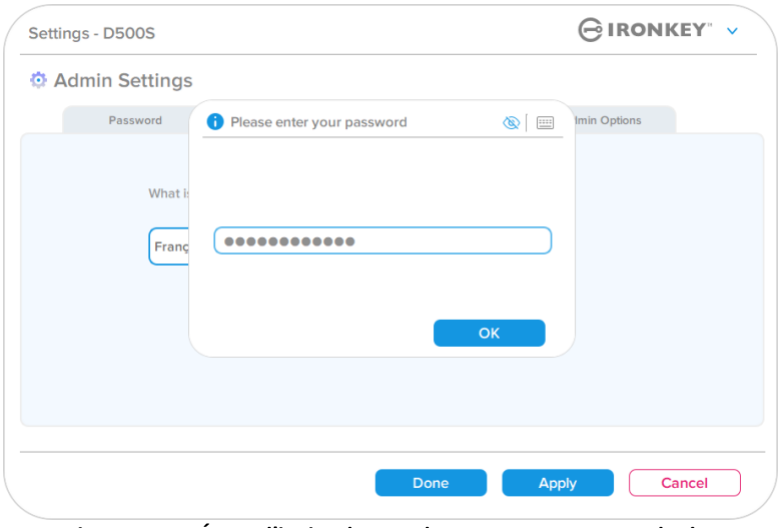


Figure 7.11 – Écran d'invite du mot de passe pour sauvegarder les modifications des paramètres de la D500S

Remarque : Si vous êtes sur l'écran de demande du mot de passe ci-dessus et que vous souhaitez annuler ou modifier vos modifications, vous pouvez le faire en vous assurant simplement que le champ du mot de passe est vide et en cliquant sur « OK ». Cela fermera la boîte de dialogue « Please enter your password » (Veuillez saisir votre mot de passe) et vous ramènera au menu des paramètres de la D500S.

Fonctionnalités Admin

Options disponibles pour réinitialiser le mot de passe Utilisateur

Les fonctionnalités de la configuration Admin offrent plusieurs façons de réinitialiser en toute sécurité le mot de passe Utilisateur, que ce soit 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 :

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

Changez manuellement le mot de passe Utilisateur dans le menu « Options Admin ». Ce changement est instantané ; il prendra effet à la prochaine connexion Utilisateur (*Figure 8.1*)

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

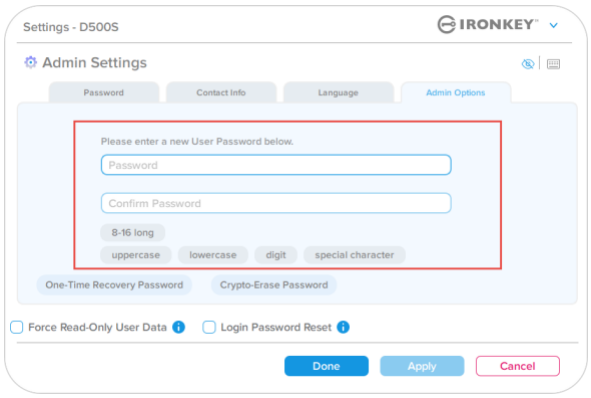


Figure 8.1 – Options Admin/réinitialisation du mot de passe Utilisateur

Login Password Reset (Réinitialisation du mot de passe à la connexion) :

L'activation de la réinitialisation du mot de passe obligera **l'Utilisateur à se connecter en utilisant le mot de passe temporaire défini par l'Admin**, puis à le changer pour un mot de passe de son choix. Cette fonctionnalité est utile lorsque la clé USB est confiée à une autre personne pour qu'elle l'utilise. (voir la *Figure 8.2 et la Figure 8.3*)

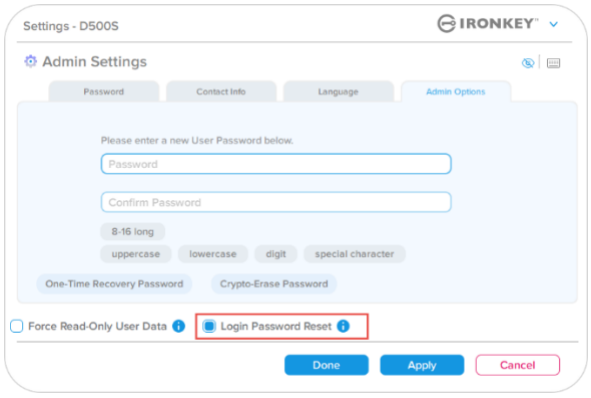


Figure 8.2 – Bouton de réinitialisation des mots de passe de connexion

Remarque : Cette réinitialisation prendra effet lors de la prochaine connexion Utilisateur réussie. L'option de mot de passe sera automatiquement appliquée en fonction de l'option initiale définie pendant le processus d'initialisation (Complexe ou Phrase de passe).

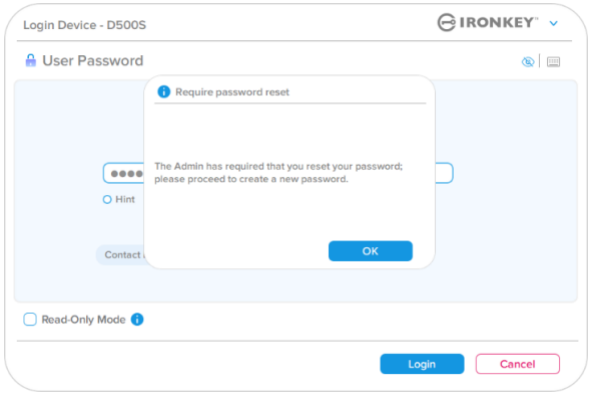


Figure 8.3 – Notification de réinitialisation après saisie du mot de passe Utilisateur

Fonctionnalités Admin

Mot de passe de récupération à usage unique

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

Mot de passe de récupération à usage unique

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

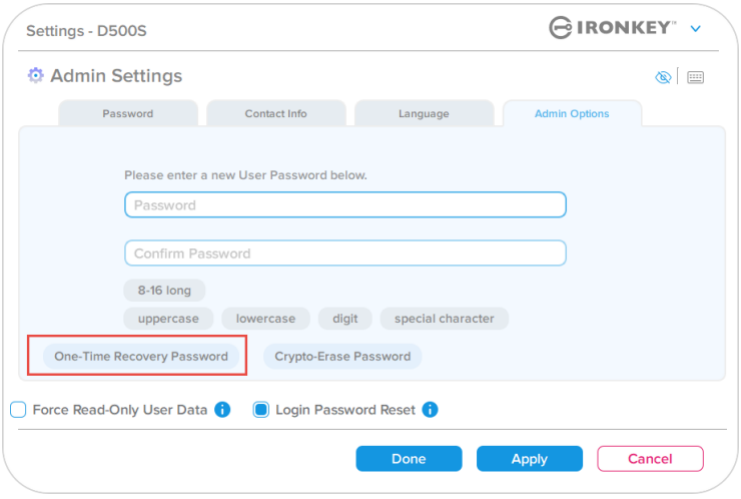


Figure 8.4 – Bouton Mot de passe de récupération à usage unique

Étape 2 : Créez un mot de passe de récupération à usage unique en utilisant la même option que celle utilisée initialement pour la clé USB (Complexe ou Phrase de passe).

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

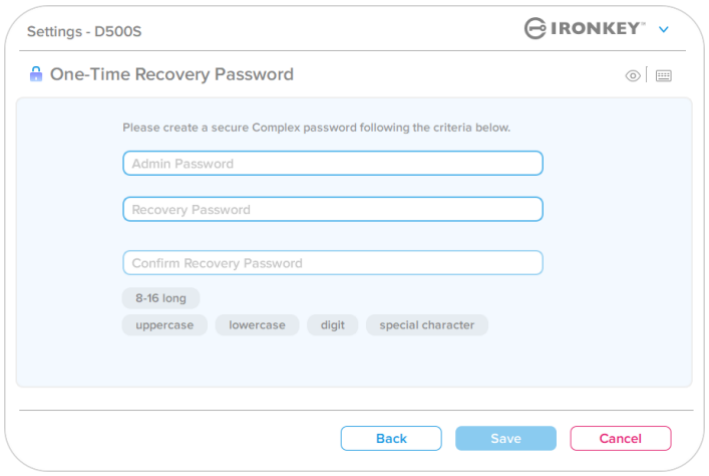


Figure 8.5 – Configuration du mot de passe de récupération à usage unique

Fonctionnalités Admin

Utilisation du mot de passe de récupération à usage unique

Étape 1 :
Après la création du mot de passe de récupération à usage unique, un nouveau bouton apparaîtra sur l'écran de connexion **User Password (Mot de passe Utilisateur)** lors de la prochaine connexion. Cliquez sur le bouton **Recovery Password (Mot de passe de récupération)** pour lancer le processus.

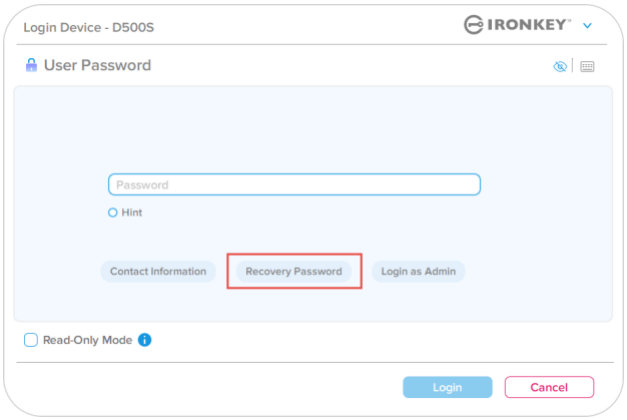


Figure 8.6 – Bouton Recovery Password (Mot de passe de récupération)

Étape 2 : L'écran **Recovery Password (Mot de passe de récupération)** s'affiche, et vous permet d'entrer le mot de passe de récupération et de créer un nouveau mot de passe Utilisateur. (*Figure 8.7*)

Important : Important : Le mot de passe de récupération à usage unique utilise également une fonctionnalité de sécurité intégrée qui comptabilise le nombre de tentatives de connexion infructueuses. **Après 10 saisies incorrectes du mot de passe de récupération à usage unique, ce dernier sera désactivé** et devra être réactivé en se connectant à la clé USB en tant qu'Admin (voir les pages 19 et 33 pour plus de détails).

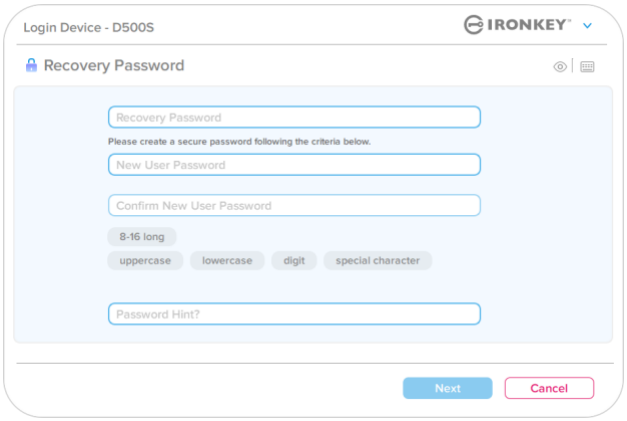


Figure 8.7 – Menu Recovery Password (Mot de passe de récupération)

Étape 3: En cas de succès, vous serez ramené à l'écran **User Password (Mot de passe Utilisateur)**. Le bouton **Recovery Password (Mot de passe de récupération)** est maintenant absent, et le mot de passe Utilisateur saisi à l'étape 2 deviendra le nouveau mot de passe Utilisateur. (*Figure 8.8*)

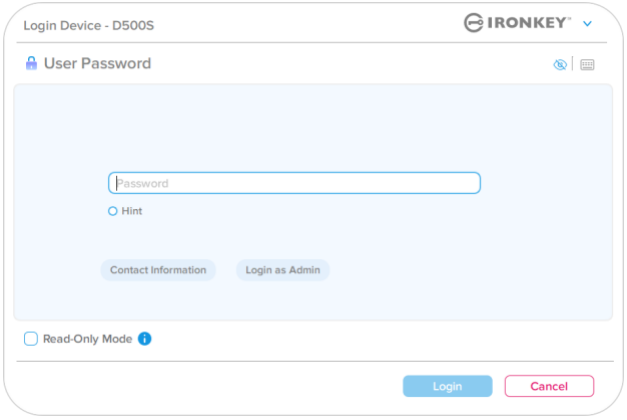


Figure 8.8 – Écran de connexion User Password (Mot de passe Utilisateur) montrant que le bouton Recovery Password (Mot de passe de récupération) disparaît une fois utilisé correctement.

Fonctionnalités Admin

Mot de passe d'effacement chiffré

La clé IronKey D500S est dotée d'une fonctionnalité unique de mot de passe d'effacement chiffré conçue pour se protéger en cas de violation physique. Cette fonctionnalité efface de manière sécurisée le contenu de votre clé USB lorsqu'elle est utilisée, donnant l'impression qu'aucune donnée n'a jamais été écrite dessus. Lorsque cette fonctionnalité est activée et que la clé USB est déverrouillée avec le mot de passe d'effacement chiffré, elle effectue un effacement chiffré discret sur la clé D500S et ouvre le lecteur en mode d'état d'usine avec une partition Utilisateur vide. La clé de chiffrement précédente sera supprimée et une nouvelle clé de chiffrement sera créée pour la remplacer. ***À utiliser avec précaution***

- Pour **activer** cette fonctionnalité, cliquez sur le bouton Crypto-Erase password (Mot de passe d'effacement chiffré) situé dans l'onglet Admin Options (Options Admin) :

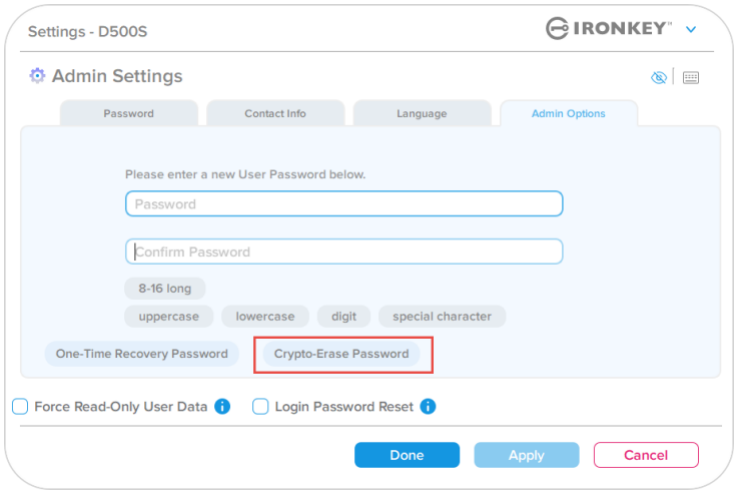


Figure 8.9 – Activation du mot de passe d'effacement chiffré

Mot de passe d'effacement chiffré :

- Les règles relatives aux mots de passe sont basées sur les paramètres initiaux de la clé USB (Complexe ou Phrase de passe).
- Le mot de passe Admin sera nécessaire pour appliquer les modifications.

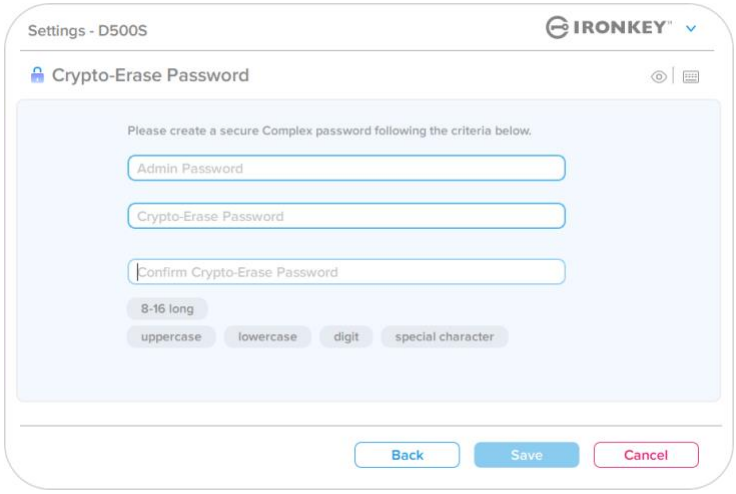


Figure 8.10 – Création d'un mot de passe d'effacement chiffré

Fonctionnalités Admin

Utilisation du mot de passe d'effacement chiffré

Lorsque le mot de passe d'effacement chiffré est utilisé, il supprime et remplace les mots de passe Admin et Utilisateur précédents. En outre, tous les paramètres de configuration précédents seront supprimés, de même que toutes les données stockées sur la clé USB, et celle-ci passera en mode Utilisateur uniquement.

Pour utiliser le mot de passe d'effacement chiffré :

1. Lancez IronKey.exe pour exécuter l'application IronKey.

2. Sur l'écran de connexion User Password (Mot de passe Utilisateur), appuyez sur « **CTRL + ALT +C** » pour passer à la saisie du mot de passe d'effacement chiffré. Si vous procédez correctement, une barre bleue plus épaisse sera visible sous l'écran de saisie du mot de passe, indiquant que le mot de passe d'effacement chiffré est prêt à être saisi. (*Figure 8.11*)

REMARQUE : Le mot de passe d'effacement chiffré ne peut être activé que sur l'écran de connexion Mot de passe Utilisateur.

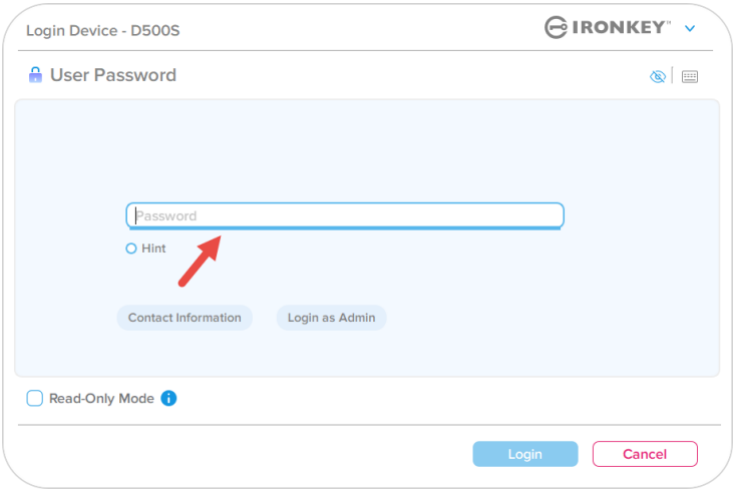


Figure 8.11- Effacement chiffré activé, avec une barre bleue épaisse

Une fois le mot de passe d'effacement chiffré utilisé, la clé USB efface tout son contenu et seule une partition vide apparaît. La clé USB est alors en mode Utilisateur uniquement et le mot de passe d'effacement chiffré sera le mot de passe à utiliser pour s'y connecter jusqu'à ce qu'elle soit réinitialisée.

Important : cette fonctionnalité efface toutes les données sur la clé USB. Tout ce qui a été stocké précédemment sera perdu à jamais.

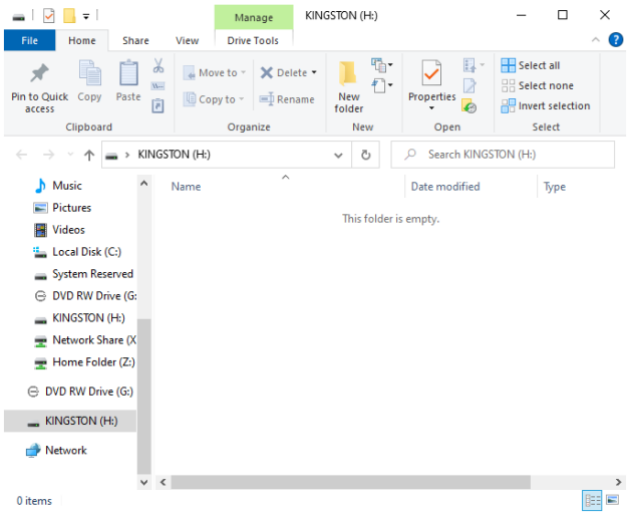


Figure 8.12 – Drive wipe after Mot de passe d'effacement chiffré used

Fonctionnalités Admin

Forcer la lecture seule pour les données Utilisateur

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

- Pour activer l'option Force Read-Only for the User data (Forcer la lecture seule pour les données Utilisateur), cochez la case correspondante et cliquez sur « Apply » (Appliquer). (*Figure 8.13*)

  Remarque : Ce mode de lecture seule forcée ne s'applique qu'à l'Utilisateur et ne concerne pas la connexion Admin. La connexion Admin aura toujours les privilèges d'accès en lecture et en écriture, et pourra toujours activer le mode lecture seule si nécessaire.

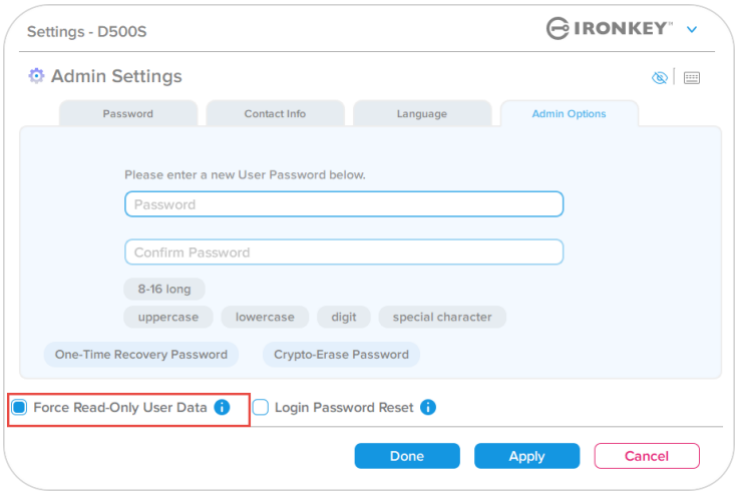


Figure 8.13 – Activer l'option « Force Read-Only User data » (Forcer la lecture seule pour les données Utilisateur) (Le mot de passe Admin sera nécessaire pour appliquer les modifications)

- Une fois cette option activée, le bouton **« Read-Only Mode » (Mode lecture seule)** 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 8.14*)

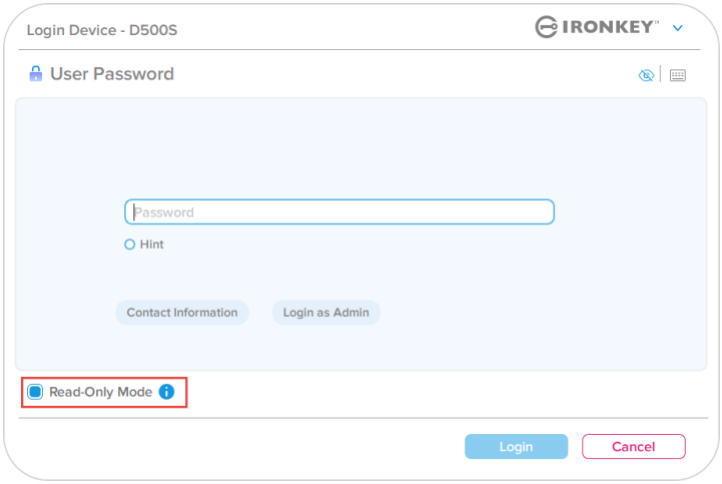


Figure 8.14 – Le mode Lecture seule est activé de manière forcée pour l'utilisateur et ne peut être désactivé que par l'Admin.

Aide et dépannage

Verrouillage du périphérique

La D500S comprend une fonctionnalité de sécurité qui empêche tout accès non autorisé à la partition de données après un certain nombre maximum de tentatives de connexion infructueuses **consécutives** (« MAX » pour faire court). Par défaut, ce nombre de tentatives infructueuses est de 10 pour chaque méthode de connexion (Admin/Utilisateur/Mot de passe de récupération à usage unique).

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

1. Une connexion réussie avant d'atteindre le MAX.

2. Atteindre le MAX et effectuer un verrouillage ou un formatage de la clé USB, selon sa configuration.

- Si un mot de passe incorrect est saisi, un message d'erreur s'affiche en rouge juste au-dessus du champ de saisie du mot de passe, indiquant un échec de connexion. (*Figure 9.1*)

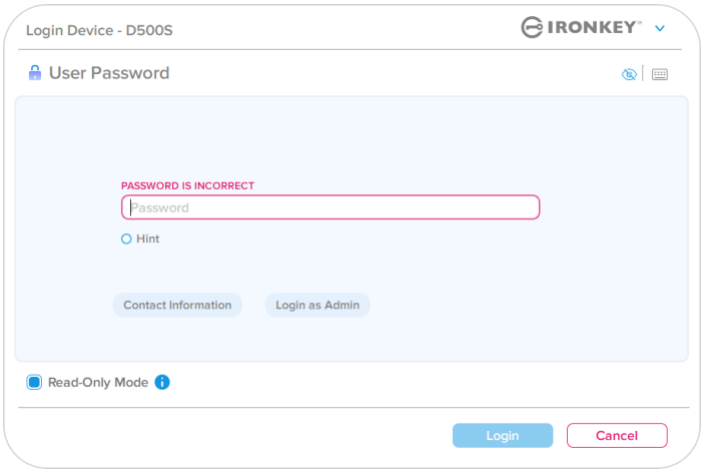


Figure 9.1 – Message Mot de passe incorrect

- Après la **7ème** tentative infructueuse consécutive, un message d'erreur supplémentaire avertit l'utilisateur qu'il lui reste 3 tentatives avant d'atteindre la limite MAX (par défaut, 10 tentatives) (*Figure 9.2*)

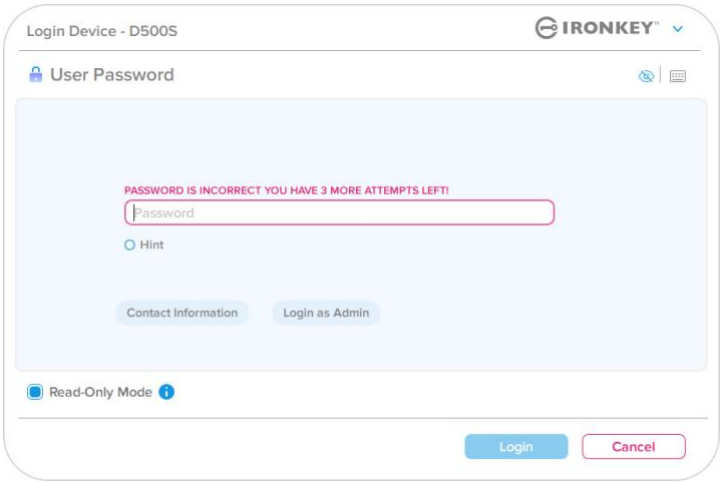


Figure 9.2 – 7ème tentative de saisie de mot de passe infructueuse

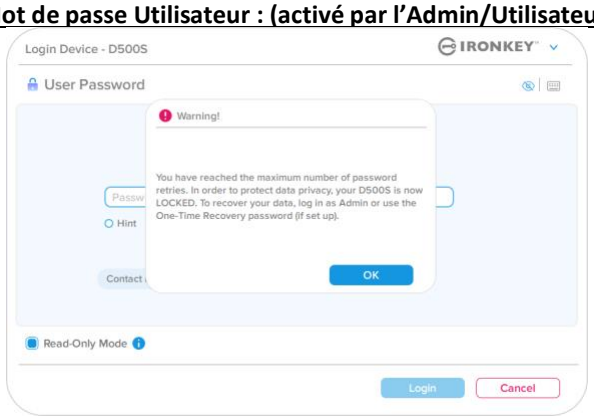
Aide et dépannage

Verrouillage du périphérique

Important :
Après la **10ème** et dernière tentative de connexion infructueuse, 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 USB se verrouillera, ce qui vous obligera à vous connecter avec une autre méthode (le cas échéant), ou à effectuer une réinitialisation, ce qui **formatera les données, lesquelles seront définitivement perdues**. Ces comportements sont également mentionnés à la page 19 du présent guide de l'utilisateur.

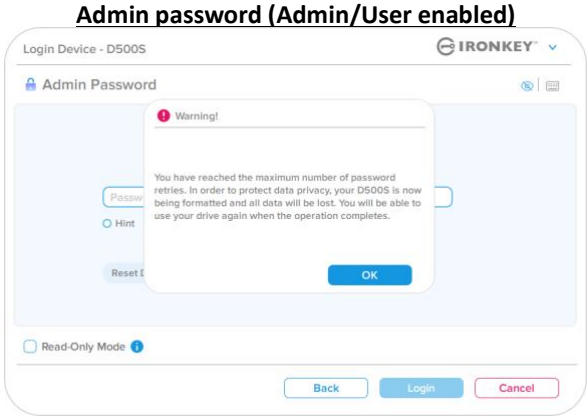
Les figures 9.3 à 9.6 ci-dessous illustrent le comportement visuel pour la 10ème et dernière tentative de connexion infructueuse pour chaque méthode de mot de passe de connexion :

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



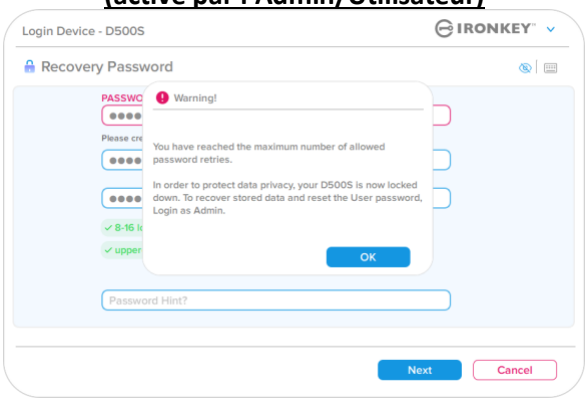
VERROUILLAGE DE LA CLÉ USB
Figure 9.3

Admin password (Admin/User enabled)



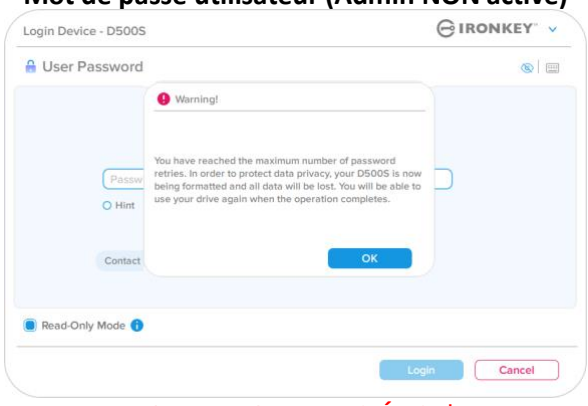
FORMATAGE DE LA CLÉ USB*
Figure 9.4

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



VERROUILLAGE DE LA CLÉ USB
Figure 9.5

Mot de passe utilisateur (Admin NON activé)



FORMATAGE DE LA CLÉ USB*
Figure 9.6

Ces mesures de sécurité empêchent qu'une autre personne (qui n'a pas votre mot de passe) puisse effectuer d'innombrables tentatives de connexion et d'accéder à vos données sensibles (également connu sous le nom d'attaque par la force brute). Si vous êtes le propriétaire de la D500S et que vous avez oublié votre mot de passe, les mêmes mesures de sécurité seront appliquées, notamment un formatage de la clé USB*. Pour plus d'informations sur cette fonctionnalité, voir *« Réinitialiser la clé USB »* à la page 25.

**Remarque : Un formatage de la D500S supprimera TOUTES les informations stockées sur sa partition de données sécurisée.*

Aide et dépannage

Réinitialiser la clé USB

Si vous oubliez votre mot de passe ou si vous devez réinitialiser votre clé USB, vous pouvez cliquer sur le bouton « Reset Device » (Réinitialiser l'appareil) qui peut apparaître à deux endroits selon la configuration de la clé USB (soit dans le menu Admin Login Password (Mot de passe de connexion Admin) si le mode Admin/Utilisateur est activé, soit dans le menu de connexion « User Password » (Mot de passe Utilisateur) si le mode Admin/Utilisateur n'est pas activé) lorsque le programme D500S Launcher est exécuté (voir la *Figure 9.7* et la *Figure 9.8*)

- Cette option vous permet de créer un nouveau mot de passe, mais pour protéger la confidentialité de vos données, la D500S sera formatée. Par conséquent, ce processus effacera définitivement toutes vos données.*

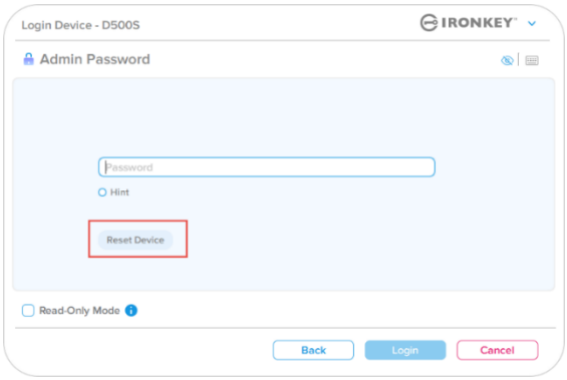


Figure 9.7 – Mot de passe Admin : Bouton Reset Device (Réinitialiser l'appareil)

- **Remarque :** Lorsque vous cliquez sur le bouton *« Reset Device » (Réinitialiser l'appareil)*, un message vous demande si vous souhaitez saisir un nouveau mot de passe avant le lancement du formatage. Vous pouvez alors 1) cliquer sur *« OK »* pour confirmer, ou 2) cliquer sur *« Cancel »* (Annuler) pour revenir à la fenêtre de connexion. (Voir la *Figure 9.8*)

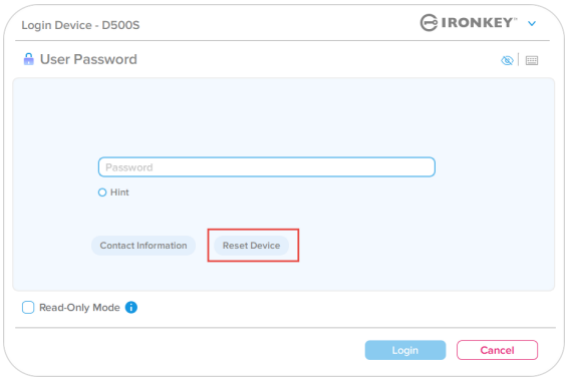


Figure 9.8 – Mot de passe Utilisateur (Admin/Utilisateur non activé) – Réinitialisation de la clé USB

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

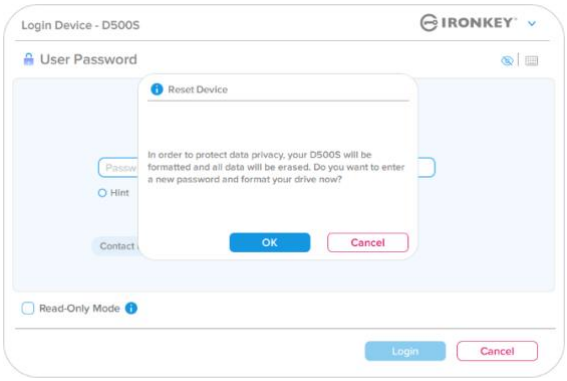


Figure 9.9 – Confirmation de réinitialisation de la clé USB

Aide et dépannage

Conflit de lettres de lecteur : Systèmes d'exploitation Windows

- Comme indiqué dans la section *« Configuration système »* du présent manuel (page 3), la D500S 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 NE DÉPEND PAS des partages de réseau parce que ces partages sont spécifiques aux profils d'utilisateur et non au profil matériel du système. Une lettre attribuée à un lecteur du réseau peut donc apparaître comme disponible pour le système d'exploitation.

- Autrement dit, Windows peut attribuer à la D500S une lettre de lecteur qui est déjà utilisée par un élément du réseau ou un chemin UNC (Universal Naming Convention), ce qui provoque un conflit de lettres de lecteur. Dans ce cas, veuillez consulter votre administrateur ou le service d'assistance pour modifier l'attribution des lettres de lecteur dans le gestionnaire des disques Windows Disk Management (les droits d'administrateur sont nécessaires). Comme indiqué dans la section *« Configuration système »* du présent manuel (page 3), la D500S 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 NE DÉPEND PAS des partages de réseau parce que ces partages sont spécifiques aux profils d'utilisateur et non au profil matériel du système. Une lettre attribuée à un volume du réseau peut donc apparaître comme disponible pour le système d'exploitation.

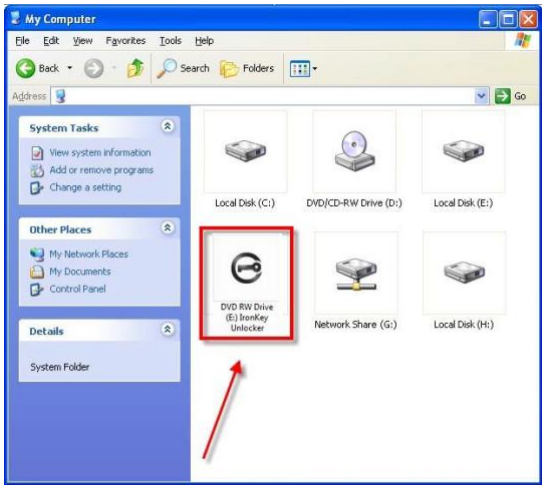


Figure 9.10 – Exemple de lettre de lecteur

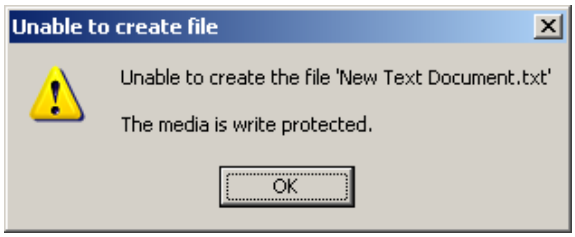
Dans cet exemple (*Figure 9.10*), la D500S utilise le lecteur F:, qui est la première lettre de lecteur disponible après le lecteur E: (le dernier disque physique avant l'écart entre les lettres de lecteur). Comme la lettre G: est un partage réseau et qu'elle ne fait pas partie du profil matériel, la D500S peut tenter de l'utiliser comme deuxième lettre de lecteur, ce qui provoque un conflit.

Si vous n'avez aucun lecteur de réseau sur votre système et que la D500S 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 10 et 11 et peut vous éviter ce problème. Toutefois, si vous ne parvenez pas à résoudre un conflit de lettres de lecteur, veuillez contacter le support technique de Kingston ou consultez le site Kingston.com/support pour obtenir de l'aide.

Aide et dépannage

Messages d'erreu

Unable to create file (Impossible de créer le fichier) : 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.	 **Figure 9.11 – Erreur « Unable to create file » (Impossible de créer le fichier)**
Error Copying File or Folder (Erreur lors de la copie du fichier ou du dossier) : 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 – « Error Copying File or Folder » (Erreur lors de la copie du fichier ou du dossier)**
Error Deleting File or Folder (Erreur lors de la suppression du fichier ou du dossier) : 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.	 **Figure 9.13 – « Error Deleting File or Folder » (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 D500S, puis rétablir la connexion après avoir décoché la case « Read-Only Mode » (Mode lecture seule).

Initialisation de la clé USB (environnement Linux)

Compte tenu des différentes distributions de Linux actuellement disponibles, l'apparence de l'interface peut varier d'une version à l'autre. Cependant, les commandes générales utilisées dans l'application Terminal restent très similaires et peuvent être reconnues dans les instructions qui suivent. Les exemples de captures d'écran dans cette section proviennent d'un environnement 64 bits.

Certaines versions de Linux nécessitent des privilèges de super utilisateur (ou utilisateur racine) pour exécuter correctement les commandes de la D500S dans la fenêtre de l'application du terminal.

Remarques importantes avant de poursuivre :

1.) **La D500S ne prend pas en charge l'initialisation de la clé USB sous Linux. Elle devra être entièrement initialisée et configurée sur un système Windows ou macOS pris en charge avant qu'elle ne puisse être utilisé sur une machine Linux.**

2.) **La connexion Linux ne prend en charge que les mots de passe complexes. La connexion par phrases de passe n'est pas prise en charge sous Linux.**

3.) **La prise en charge des fonctionnalités de la D500S sous Linux est limitée. Les fonctionnalités telles que le mot de passe de récupération à usage unique, le mot de passe d'effacement chiffré, la réinitialisation du mot de passe Admin/Utilisateur et le basculement en mode lecture seule ne sont pas prises en charge sous Linux.**

La D500S inclut 4 commandes utilisables sous Linux :

Ikd500s_about	Affiche les informations « About D500S » (À propos de la D500S).
Ikd500s_login	Vous permet de vous connecter à la clé USB.
Ikd500S_logout	Vous permet de vous déconnecter en toute sécurité de la clé USB D500S.
Ikd500S_resetdevice	Effectue un effacement chiffré de la clé USB et la réinitialise à l'état d'origine, en supprimant définitivement toutes les données et tous les fichiers qui y sont stockés.

REMARQUE : Pour exécuter ces commandes, vous devez ouvrir une fenêtre de l'application Terminal et parcourir le volume jusqu'au répertoire contenant les fichiers. Chaque commande doit commencer par les deux caractères suivants : « ./ » (un point et une barre oblique vers l'avant.)

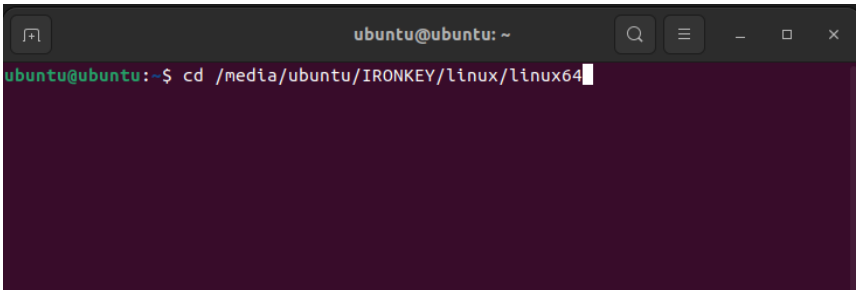
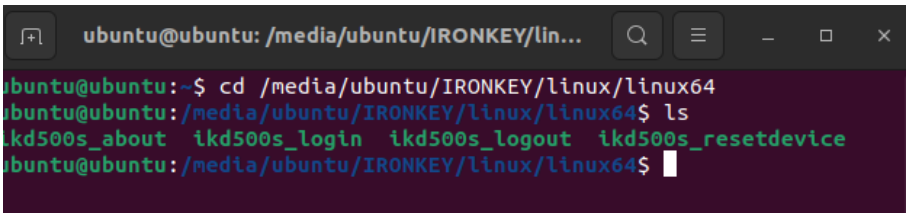
Exemple de navigation vers le chemin des commandes Linux IronKey :

Pour les utilisateurs Linux 32 bits :	Ouvrez une fenêtre d'application « Terminal » et modifiez le répertoire actuel en **/media/ubuntu/IRONKEY/linux/linux32$** en saisissant la commande suivante à l'invite : **cd /media/ubuntu/IRONKEY/linux/linux32** (puis, appuyez sur ENTRÉE.)
Pour les utilisateurs Linux 64 bits :	Ouvrez une fenêtre d'application « Terminal » et modifiez le répertoire actuel en **/media/ubuntu/IRONKEY/linux/linux64$** en saisissant la commande suivante à l'invite : **cd /media/ubuntu/IRONKEY/linux/linux64** (puis, appuyez sur ENTRÉE.)

Initialisation du périphérique (Environnement Linux)

Remarque : Si le lecteur IRONKEY n'est pas automatiquement chargé par le système d'exploitation, vous devez le charger manuellement dans une fenêtre de l'application du terminal, avec la commande Linux « mount ». Reportez-vous à la documentation Linux de votre distribution de système d'exploitation spécifique ou votre site d'assistance habituel pour utiliser la syntaxe et les options de commande appropriées. Certaines distributions Linux peuvent exiger la saisie du nom d'utilisateur pour exécuter des commandes, c'est-à-dire « ubuntu » dans les exemples ci-dessus.

Repérer et afficher les fichiers de commande Linux de la clé USB IronKey D500S :

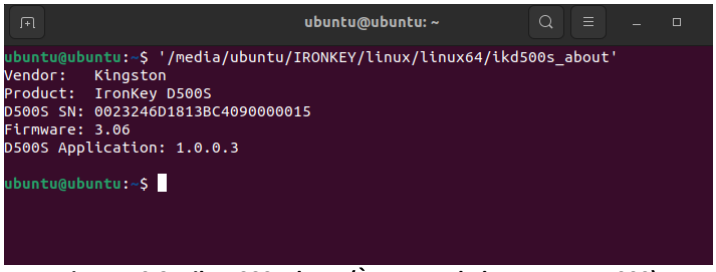
Lorsque la D500S est connectée à votre ordinateur et reconnue par le système d'exploitation, changez de répertoire pour passer au lecteur D500S en tapant la commande à l'invite du terminal. (*Figure 10.1*) **Remarque :** Les captures d'écran et les instructions de cette section utilisent le dossier linux64 (signifiant 64 bits) pour démontrer l'utilisation de la clé USB D500S dans le système d'exploitation Linux. Si vous utilisez la version 32 bits de Linux, il vous suffit de naviguer vers le dossier 32 bits correspondant et de l'utiliser à la place du dossier 64 bits (par exemple, linux32 au lieu de linux64).	 **Figure 10.1- Navigation par ligne de commande**
Utilisez la commande **ls** (liste) à l'invite actuelle et appuyez sur ENTRÉE. Vous obtiendrez une liste de fichiers et/ou de dossiers dans le dossier linux64. Vous verrez alors les quatre commandes Linux IronKey répertoriées (*Figure 10.2*) • ikD500S_about • ikD500S_login • ikD500S_logout • ikD500S_resetdevice	 **Figure 10.2- Affichage des fichiers de commande Linux IronKey**

Remarque : Les commandes et les noms des répertoires (dossiers) sont sensibles à la casse. Donc « linux64 » N'EST PAS le même répertoire que « Linux64 ». La syntaxe doit aussi être exactement reproduite. Certaines distributions Linux peuvent exiger la saisie du nom d'utilisateur pour exécuter des commandes, c'est-à-dire « ubuntu » dans cet exemple.

Initialisation de la clé USB (environnement Linux)

Utilisation des commandes de la D500S

À propos de la D500S

IkD500S_about (À propos de la D500S, *Figure 10.3*) Cette commande permet d'obtenir des informations sur la D500S, comme par exemple : • Fabricant • Produit • Numéro de série de la D500S • Version du firmware • Version du logiciel	 **Figure 10.3 – ikD500S_about (À propos de la IronKey D500S)**

Connexion à la D500S

ikD500S_login

Une fois que la D500S a été initialisée sur un système Windows ou macOS pris en charge, vous pouvez accéder à la partition de données sécurisée en vous connectant à l'appareil à l'aide du mot de passe D500S que vous avez créé.

Pour ce faire, suivez les étapes suivantes :

1. Ouvrez une fenêtre d'application « Terminal ».

2. Saisissez la commande suivante à l'invite du terminal : **cd /media/ubuntu/IRONKEY/linux/linux64**

3. L'invite de commande étant maintenant sur **/media/ubuntu/IRONKEY/linux/linux64$**, type the following command to log in to the device: **./ikD500S_login*** puis appuyez sur ENTRÉE. (Remarque : Les commandes et les noms de de dossier sont sensibles à la casse, et la syntaxe doit être rigoureusement respectée. Certaines distributions Linux peuvent exiger la saisie de votre nom d'utilisateur, c'est-à-dire « ubuntu » dans cet exemple).

4. Après une connexion réussie, le lecteur de données sécurisé s'ouvrira sur votre bureau et vous pourrez utiliser la D500S (vous trouverez plus d'informations sur le comportement de connexion à la page suivante).

*Remarque : Certaines versions de Linux nécessitent des privilèges de super utilisateur (ou utilisateur racine) pour exécuter correctement les commandes de la D500S dans la fenêtre de l'application du terminal.

Initialisation de la clé USB (environnement Linux)

Connexion à la D500S (suite)

IkD500S_login (Déverrouillage de la D500S, *Figure 10.4*)

Selon la façon dont votre clé USB a été configurée, il se peut que, lors de la procédure de connexion, plusieurs options vous soient proposées pour la déverrouiller.

Si les profils de mot de passe **Admin/Utilisateur** ont été activés lors de l'initialisation, les options de connexion suivantes vous sont proposées :

1.) Choisissez de vous connecter en tant qu'Admin ou Utilisateur
2.) Choisissez de déverrouiller les partitions Admin ou Utilisateur (si elles sont activées).
3.) Saisissez le mot de passe de connexion Admin ou Utilisateur pour l'authentification et le déverrouillage de la clé USB.

Remarque : Si les profils de mot de passe Admin/Utilisateur N'ONT PAS été activés lors de l'initialisation (mode Utilisateur seulement), vous serez uniquement invité à saisir le mot de passe de votre clé USB pour son authentification.

Important : Comme indiqué précédemment, les phrases de passe ne sont pas prises en charge sous Linux ; la D500S devra être configurée avec un mot de passe Complexe pour la connexion Linux (*Figure 10.5*)

Figure 10.4 – ikD500S_login (Déverrouillage de la D500S)

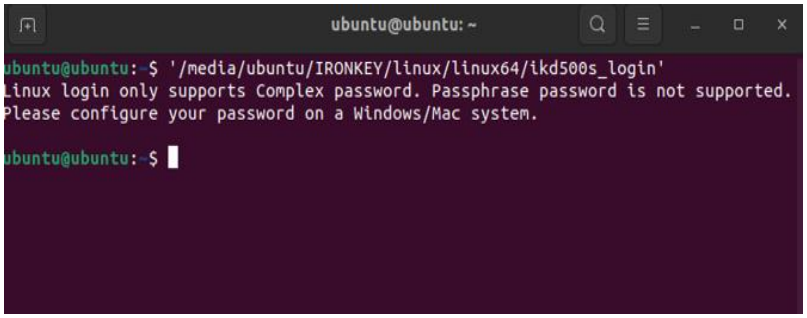


Figure 10.5- Tentative de connexion avec une phrase de passe non prise en charge.

Initialisation de la clé USB (environnement Linux)

Connexion à la D500S (suite)

Comportement en cas de saisie d'un mot de passe de connexion incorrect

Au cours de la procédure de connexion, si un mot de passe incorrect est saisi, vous aurez à nouveau la possibilité de saisir le mot de passe. Toutefois, il existe une fonctionnalité de sécurité intégrée qui comptabilise le nombre de tentatives de connexion infructueuses. Si ce nombre atteint la valeur préconfigurée de 10 tentatives infructueuses pour les connexions Admin ou Utilisateur, le comportement sera le suivant :

Mots de passe Admin/Utilisateur activés

- **Connexion Utilisateur :** Verrouillage de l'Utilisateur, connexion en tant qu'Admin requise. (*Figure 10.6*) Remarque : Le mot de passe Utilisateur peut être réinitialisé par la connexion Admin sur un système Windows ou macOS pris en charge.
- **Connexion Admin :** Effacement chiffré de la clé USB, toutes les données sont perdues à jamais. Réinitialisation de la clé USB nécessaire. (*Figure 10.7*)

Mode Utilisateur seulement (Admin/Utilisateur non activé)

- **Connexion Utilisateur :** Effacement chiffré de la clé USB, toutes les données sont perdues à jamais. Réinitialisation de la clé USB nécessaire. (*Figure 10.7*)

Figure 10.6- Verrouillage de la connexion Utilisateur, Mots de passe Admin/Utilisateur activés

Figure 10.7- Nombre maximal de tentatives atteint (réinitialisation de la clé USB).

Déconnexion de la D500S

IkD500S_logout (verrouiller la clé USB)

Lorsque vous avez fini d'utiliser la D500S, déconnectez-vous de la clé USB et sécurisez vos données. Pour ce faire, suivez les mêmes étapes que celles mentionnées à la page 39 et utilisez la commande suivante pour vous déconnecter correctement de la clé USB : **./ikD500S_logout**, puis appuyez sur la touche ENTRÉE (Remarque : Les commandes et les noms de répertoires sont sensibles aux majuscules et aux minuscules et la syntaxe doit être rigoureusement respectée.) (*Figure 10.8*)

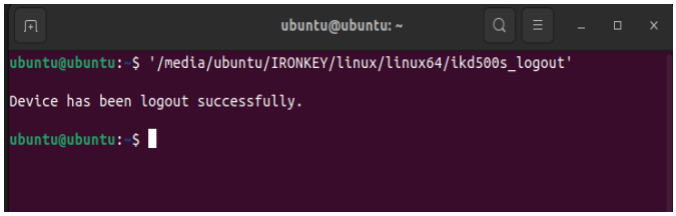


Figure 10.8- Déconnexion de la D500S

Initialisation de la clé USB (environnement Linux)

Réinitialisation de la D500S

ikD500S_resetdevice
Comme indiqué précédemment à la page 41, en cas d'oubli des mots de passe Utilisateur/Admin, la commande Reset Device (Réinitialiser l'appareil) peut être utilisée pour réinitialiser la clé USB afin qu'elle puisse être utilisée à nouveau. Ce processus vous permettra de créer un nouveau mot de passe. Mais afin de protéger la confidentialité de vos données, la D500S effacera son contenu par chiffrement pour formater la partition de données sécurisées. **Cela signifie que toutes vos données seront perdues.**

Pour utiliser la commande Reset Device (Réinitialiser l'appareil), suivez les mêmes étapes que celles indiquées à la page 39 et utilisez la commande suivante pour vous déconnecter correctement de la clé USB : **./ikD500S_resetdevice** et appuyez sur la touche ENTRÉE (Remarque : Les commandes et les noms de répertoires sont sensibles aux majuscules et aux minuscules et la syntaxe doit être rigoureusement respectée.) (*Figure 10.9*)

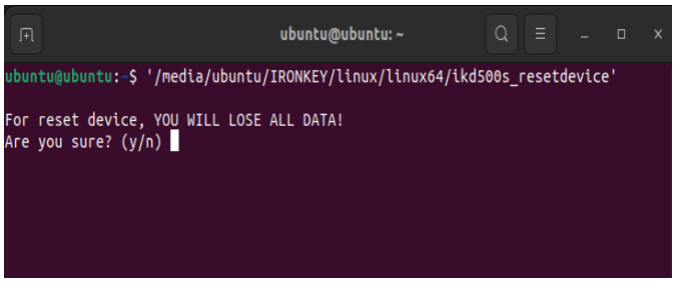


Figure 10.9- Commande Reset Device (Réinitialiser l'appareil)

Une fois la commande Reset Device (Réinitialiser l'appareil) utilisée, vous serez invité à créer un nouveau mot de passe complexe qui doit contenir :

- 8 à 16 caractères et au moins (3) des critères suivants :

  - **MAJUSCULE**
  - **Minuscule**
  - **Numérique**
  - **Caractères spéciaux (!,$,etc.)**

(*Figure 10.10*)

Remarque : La commande Reset Device (Réinitialiser l'appareil) initialise la clé USB en mode Utilisateur uniquement (un seul mot de passe, un seul utilisateur). Pour activer les profils de mot de passe de connexion Admin/Utilisateur, la D500S doit être configurée sur un système Windows ou macOS pris en charge pour accéder à cette option.

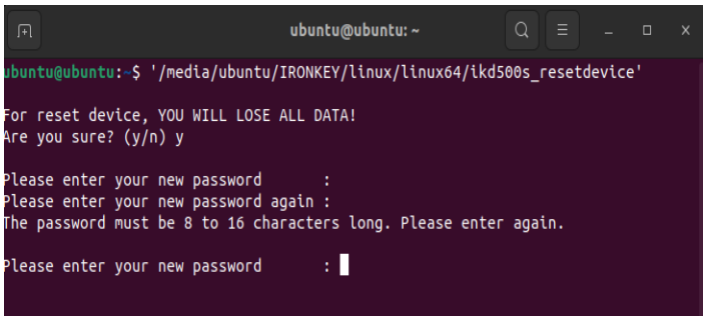


Figure 10.10- Commande Reset Device (Réinitialiser l'appareil), création du mot de passe

IRONKEY™ D500S
CLÉ USB 3.2 GEN 1 SÉCURISÉE

Guide de l'utilisateur

Sommaire

Figure 1 – IronKey D500S

Introduction

La Kingston IronKey D500S est une clé USB offrant un niveau de sécurité de classe militaire, basée sur les caractéristiques qui ont fait la réputation d'IronKey dans la protection des informations sensibles. Elle est certifiée FIPS 140-3 niveau 3 (en cours), ce qui implique de nouvelles améliorations de sécurité du NIST exigeant des mises à niveau sécurisées du processeur pour une sécurité accrue. Le chiffrement et le déchiffrement sont exécutés sur la D500S. Aucune trace ne reste sur le système hôte, ce qui l'immunise contre les renifleurs de mots de passe en mémoire. Outre le chiffrement matériel XTS-AES 256 bits, elle est dotée d'un boîtier en zinc robuste qui est étanche à l'eau*, à la poussière* et résistant à l'écrasement, et scellé avec de l'époxy pour protéger les composants internes contre les attaques par pénétration.

La D500S prend en charge l'option de mots de passe multiples (Admin, Utilisateur, Récupération à usage unique et Effacement chiffré) avec les modes Complexe ou Phrase de passe classiques**. 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 classiques, le mode Phrase de passe permet d'utiliser un code numérique, une phrase, une liste de mots ou même des paroles de chanson de 10 à 128 caractères. L'administrateur peut activer un utilisateur, créer deux partitions de données de taille personnalisée séparant les fichiers de connexion Admin et Utilisateur, activer un mot de passe de récupération à usage unique, un mot de passe d'effacement chiffré et réinitialiser le mot de passe Utilisateur pour restaurer l'accès aux données.

Pour faciliter la saisie du mot de passe, le symbole « œil » peut être activé pour révéler le mot de passe saisi, ce qui réduit les fautes de frappe pouvant générer des échecs de tentative de connexion. Pour une plus grande tranquillité d'esprit, la D500S utilise un firmware signé numériquement qui l'immunise contre les logiciels malveillants BadUSB, ainsi qu'une protection contre les attaques par force brute afin d'empêcher toute tentative de deviner le mot de passe. La protection contre les attaques par force brute verrouille le mot de passe Utilisateur ou le mot de passe de récupération à usage unique si 10 mots de passe incorrects sont saisis de suite, et chiffre le lecteur si le mot de passe Admin est saisi incorrectement 10 fois de suite.

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

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 D500S offre de nombreuses options de personnalisation, est conforme à la norme TAA/CMMC, et est assemblée aux États-Unis.

La D500S bénéficie d'une garantie limitée de 5 ans avec le support technique gratuit de Kingston.

* Veuillez vous reporter aux spécifications de la fiche technique. Le produit doit être propre et sec avant toute utilisation.
** Le mode Phrase de passe n'est pas pris en charge sur les systèmes Linux.
***Clavier virtuel : Prend uniquement en charge l'anglais américain sur Microsoft Windows et macOS.

IronKey Fonctionnalités de la D500S

- Certifiée FIPS 140-3 niveau 3 (en cours) avec un chiffrement matériel XTS-AES 256 bits (le chiffrement ne peut jamais être désactivé).
- Protection contre les attaques par force brute et BadUSB
- Options de mots de passe multiples
- Modes de mot de passe Complexe ou Phrase de passe
- Option unique de double partition et mot de passe d'effacement chiffré
- Symbole en forme d'œil pour afficher les mots de passe saisis afin de réduire les tentatives de connexion infructueuses
- Clavier virtuel pour se protéger des enregistreurs de frappe et des enregistreurs d'écran
- Paramètres forcée/basée sur la session de 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 Admin.
- Compatible avec Windows, macOS et Linux (consulter la fiche technique pour plus de détails)

À propos de ce manuel

Ce manuel d'utilisation traite de la clé USB IronKey D500S. Il est basé sur la version en sortie d'usine, sans personnalisation.

Configuration système

Plateforme PC • Intel, AMD et Apple M1 SOC • 15 Mo d'espace disque libre • Port USB 2.0 – 3.2 disponible • Deux lettres de lecteur consécutives après le dernier disque physique* ***Remarque :** Voir la section « Conflit de lettres de lecteur » à la page 35.	**Prise en charge des systèmes d'exploitation PC** • Windows 11 • Windows 10
Plateforme Mac • 15 Mo d'espace disque libre • Port USB 2.0 – 3.2	**Prise en charge des systèmes d'exploitation Mac** • macOS macOS 11.x - 14.x
Plateforme Linux • 5 Mo d'espace disque libre • Port USB 2.0 – 3.2	**Prise en charge des systèmes d'exploitation Linux** • Linux Kernel v4.4+

Recommandations

Pour que la D500S 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 D500S sur un périphérique équipé d'un port USB, par exemple un clavier ou un concentrateur/hub alimenté par USB, comme illustré dans la ***Figure 1.2***.

Figure 1.1 – Utilisation conseillée

Figure 1.2 – Utilisation déconseillée

Utiliser le bon système de fichiers

La IronKey D500S est livrée préformatée avec le système de fichiers FAT32. Elle fonctionne sur les systèmes Windows, macOS et Linux*. 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

To keep your data safe, Kingston recommends that you:

- Procédez à une analyse antivirus sur votre ordinateur avant de configurer et d'utiliser la D500S 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 l'endommager et nécessiter un reformatage, ce qui effacera vos données.
- Ne communiquez jamais le mot de passe de votre clé USB à quiconque.

Obtenir les dernières mises à jour et informations

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

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

*** La D500S ne prend pas en charge l'initialisation prête à l'emploi sous Linux. Elle devra être entièrement initialisée et configurée sur un système Windows ou macOS pris en charge avant qu'elle ne puisse être utilisé sous Linux. Vous trouverez des informations supplémentaires dans la section Linux de ce guide de l'utilisateur, à la page 37.**

Meilleures pratiques pour la configuration des mots de passe

Votre D500S est livrée avec de solides contre-mesures de sécurité. Notamment une protection contre les attaques par force brute qui empêchera un pirate de deviner des mots de passe en limitant les échecs de tentative de saisie mot de passe à 10. Lorsque cette limite est atteinte, la D500S efface automatiquement les données chiffrées et s'auto-formate aux paramètres d'usine.

Mots de passe multiples
La D500S 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 D500S peut prendre en charge trois mots de passe différents que vous pouvez utiliser pour récupérer les données : Admin, Utilisateur et de récupération à usage unique.

La D500S 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'Admin peut accéder à la clé USB à tout moment et configurer des options pour l'Utilisateur : l'Admin est une sorte de « super utilisateur ». En outre, l'Admin 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'Admin. 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 D500S peut être réinitialisée et réutilisée, mais les données antérieures seront définitivement supprimées.

Modes pour mot de passe
La D500S prend en charge deux modes de mot de passe :

Complexe
Un mot de passe complexe doit comporter 8 à 16 caractères et utiliser au moins 3 de ces types de caractères :

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

Phrase de passe
La D500S prend en charge les phrases de passe de 10 à 128 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 D500S, la langue du mot de passe peut correspondre à la langue sélectionnée pour la clé USB. Cela vous permet de sélectionner plusieurs mots, une phrase, les paroles d'une chanson, un vers de poésie, etc. Les bonnes phrases de passe font partie des types de mots de passe les plus difficiles à deviner pour un pirate, tout en étant plus faciles à retenir pour les utilisateurs.

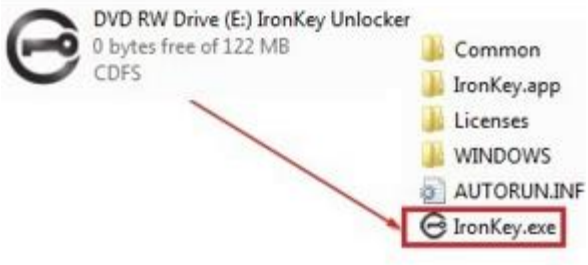
Configurer ma clé USB

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

Accès à la clé USB (Environnement Windows)

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

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

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

Accès à la clé USB (environnement macOS)

Insérez la D500S 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 lecteur « IRONKEY » s'affiche sur l'ordinateur. (*Figure 3.3*)

• Double-cliquez sur l'icône de CD-ROM IronKey. • Double-cliquez ensuite sur l'icône de l'application IronKey.app affichée dans la fenêtre illustrée à la Figure 3.3. Le processus d'initialisation démarrera aussi.	 **Figure 3.3 – Lecteur IronKey**

Initialisation de la clé USB (environnements Windows & macOS)

Langue et Contrat de licence utilisateur final

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

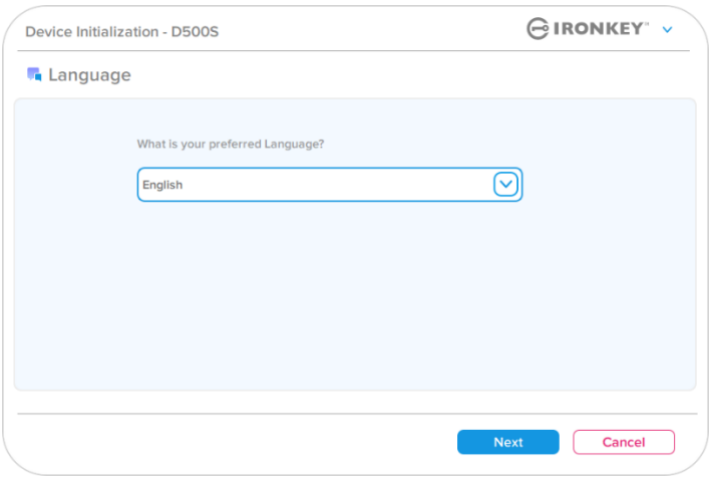


Figure 4.1 – Sélection de la langue

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

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

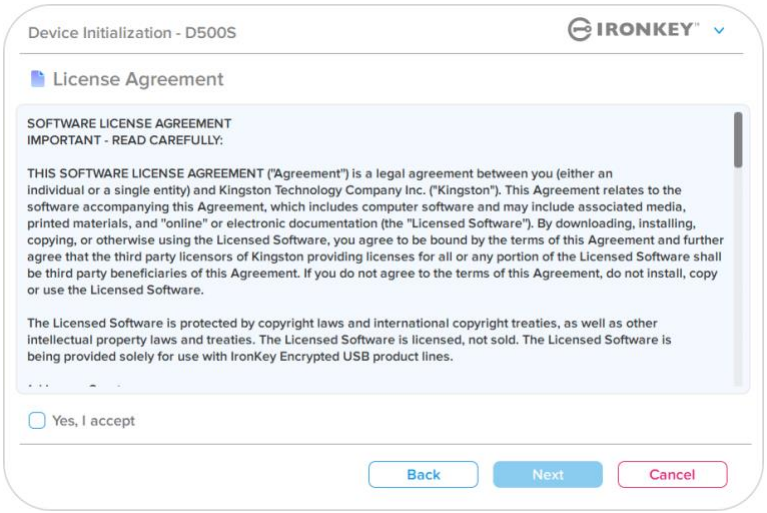


Figure 4.2 – Contrat de licence

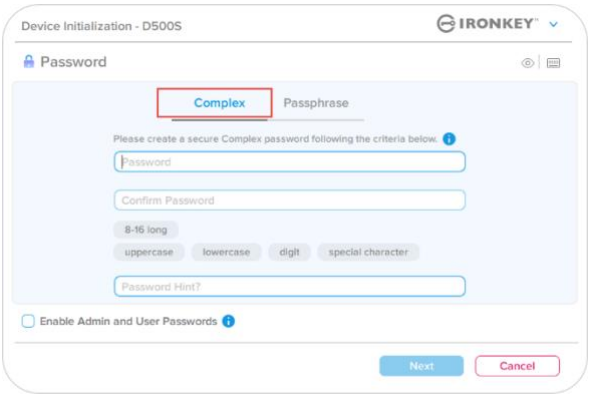
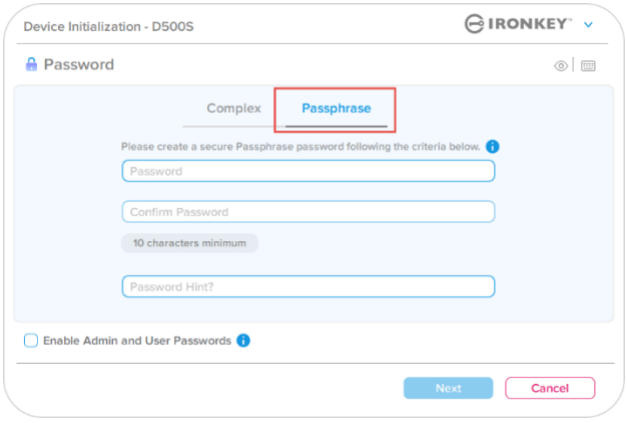
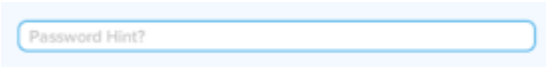
Initialisation de la clé USB

Sélection du mot de passe

Sur l'écran de demande de Mot de passe, vous pourrez créer un mot de passe pour protéger vos données sur la D500S en utilisant les modes Complexe ou Phrase de passe (*Figures 4.3- 4.4*). En outre, les options Mots de passe multiples Admin/Utilisateur peuvent également être activées sur cet écran. Avant de procéder à la sélection du mot de passe, veuillez consulter la rubrique Activation des mots de passe Admin/Utilisateur ci-dessous pour mieux comprendre ces fonctionnalités.

Remarque : Une fois que le mode Complexe ou Phrase de passe est choisi, il ne peut pas être modifié, sauf si la clé USB est réinitialisée.

Pour commencer, créez votre mot de passe dans le champ « Password » (Mot de passe), puis saisissez-le à nouveau dans le champ « Confirm Password » (Confirmer le mot de passe). Le mot de passe doit respecter les critères suivants pour que le processus d'initialisation vous autorise à continuer :

Mot de passe complexe • Doit contenir entre 8 et 16 caractères. • Doit contenir trois (3) des types de caractères suivants : ○ Majuscule ○ Minuscule ○ Chiffre ○ Caractères spéciaux (!,$,&, etc..)	 **Figure 4.3 – Mot de passe complexe**
Phrase de passe • Doit contenir : ○ 10 caractères minimum ○ 128 caractères maximum	 **Figure 4.4 – Phrase de passe**
Indice de mot de passe (facultatif) Un indice de mot de passe peut être utile pour fournir une indication de ce qu'est le mot de passe, si jamais vous l'oubliez. **Remarque :** L'indice NE DOIT PAS être le mot de passe lui-même.	 **Figure 4.5 – Champ Password Hint (Indice de mot de passe)**

Initialisation de la clé USB

Valid and invalid passwords

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

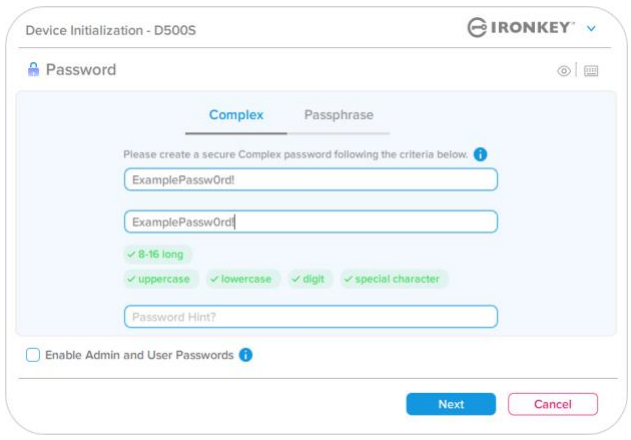


Figure 4.6a – Condition de mot de passe complexe remplie

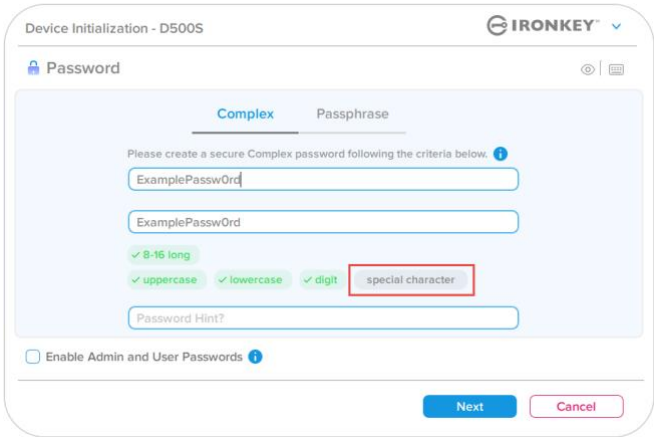


Figure 4.6b – Condition de mot de passe complexe facultative

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

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

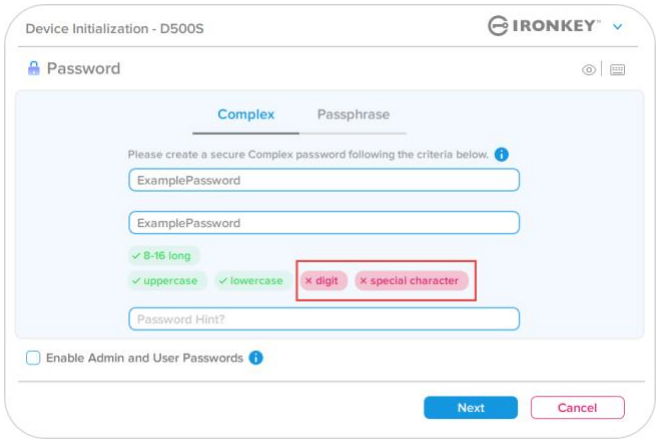


Figure 4.7 – Conditions de mot de passe non remplies

Initialisation de la clé USB

Clavier virtuel

La D500S est dotée d'un clavier virtuel qui peut être utilisé pour se protéger contre les enregistreurs de frappe.

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

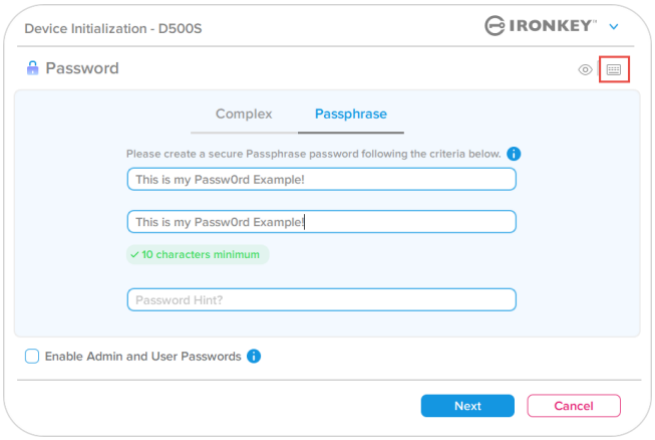


Figure 4.8 – Activation du clavier virtuel

- Une fois que le clavier virtuel apparaît, vous pouvez également activer la fonction **Screenlogger Protection (Protection contre les enregistreurs d'écran)**. Lors de l'utilisation de cette fonctionnalité, toutes les touches apparaîtront brièvement comme vides. Ce comportement est normal, car il empêche les enregistreurs d'écran de capturer ce sur quoi vous avez cliqué.

- Pour rendre cette fonctionnalité plus robuste, vous pouvez également choisir de randomiser le clavier virtuel en sélectionnant **Randomize (Disposition aléatoire)** dans le coin inférieur droit du clavier. Le clavier sera alors organisé dans un ordre aléatoire.

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

Initialisation de la clé USB

Icône de visibilité du mot de passe

Par défaut, lorsque vous créez un mot de passe, celui-ci s'affiche dans le champ au fur et à mesure que vous la saisissez. Si vous souhaitez « masquer » les caractères au fur et à mesure que vous tapez, vous pouvez activer l'icône en forme 'd'œil' située dans la partie supérieure droite de la fenêtre Device Initialization (Initialisation de l'appareil).

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

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

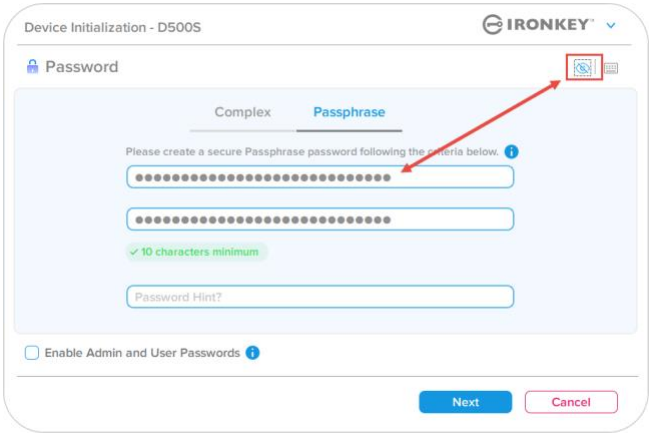


Figure 4.10 - Icône pour « masquer » le mot de passe

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

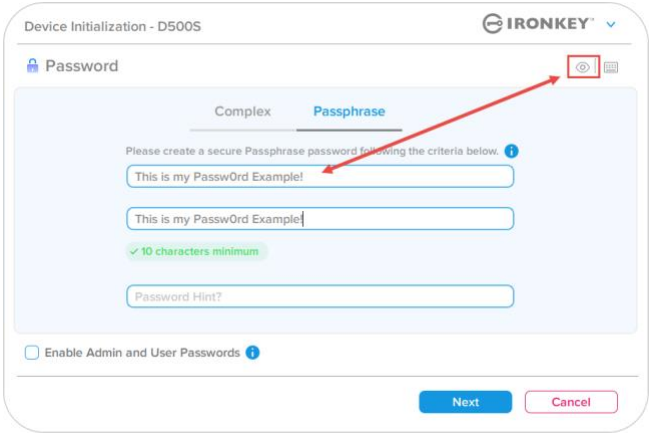


Figure 4.11 - Icône pour « afficher » le mot de passe

Initialisation de la clé USB

Mots de passe Admin et Utilisateur

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

Lorsque les mots de **passe Admin et Utilisateur** sont activés, vous pouvez également accéder aux options suivantes :

- Dual-Partition configuration (Configuration de deux partitions)
- One-Time Recovery password (Mot de passe de récupération à usage unique)
- Forced read-only mode for User login (Mode de lecture seule forcée pour la connexion Utilisateur)
- User password reset (Réinitialisation du mot de passe Utilisateur)
- Force Reset password for User login (Forcer la réinitialisation du mot de passe pour la connexion Utilisateur)
- Crypto-Erase password (Mot de passe d'effacement chiffré)

Pour en savoir plus sur ces options, allez à la page 25 du présent guide.

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

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

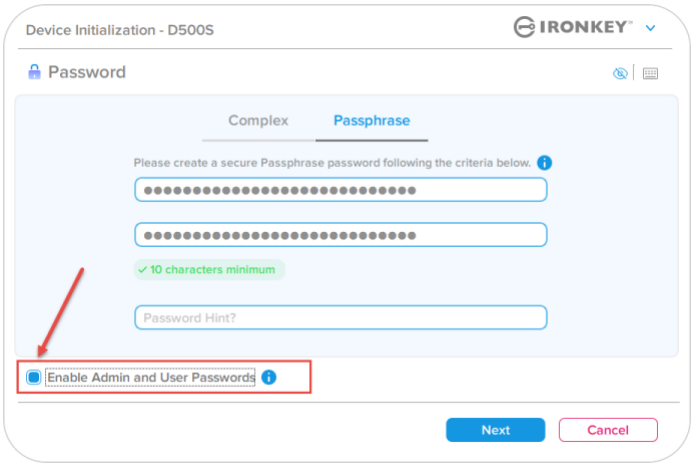


Figure 4.12 – Activation des mots de passe Admin et Utilisateur

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

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

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

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

Initialisation de la clé USB

Mots de passe Admin et Utilisateur

- Si le rôle Admin a été **activé** à l'écran précédent, l'écran suivant demandera le mot de passe Utilisateur (*Figure 4.13*). Le mot de **passe Utilisateur** aura des capacités limitées par rapport au mot de passe Admin ; il fera l'objet d'une section plus détaillée dans le présent guide de l'utilisateur (voir page 23).

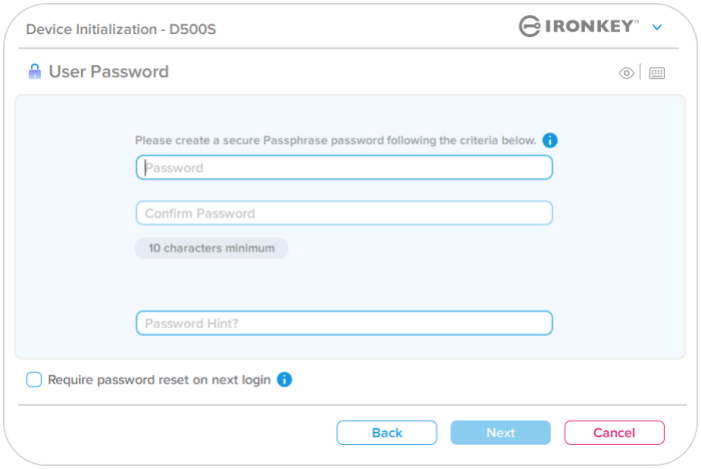


Figure 4.13 – Mot de passe Utilisateur (Admin et Utilisateur activés)

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

  Remarque : Pour des raisons de sécurité, le nouveau mot de passe ne peut pas être identique au mot de passe temporaire.

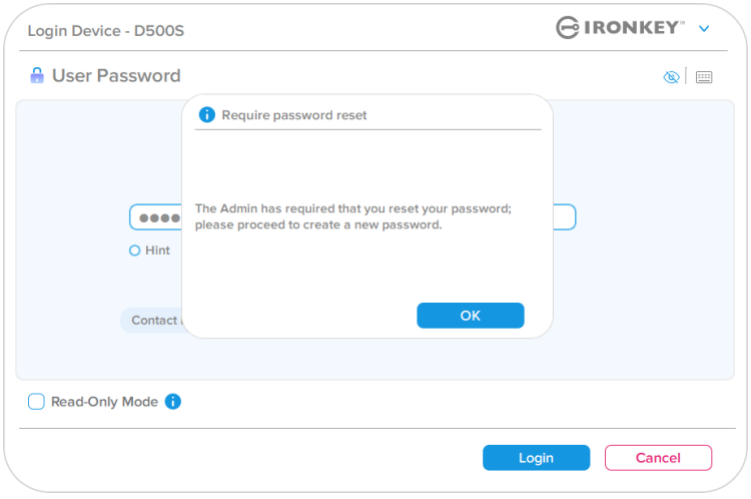


Figure 4.14 – Exiger la réinitialisation du mot de passe à la prochaine connexion (Pour le mot de passe Utilisateur)

Initialisation de la clé USB

Double partition

La clé USB IronKey D500S vous permet de créer deux partitions séparées de taille personnalisée : une pour l'Admin et l'autre pour l'Utilisateur. Si cette fonctionnalité est activée, la connexion Admin aura accès aux **deux** partitions Utilisateur et Admin, tandis que la connexion Utilisateur n'aura accès qu'à la partition Utilisateur. Cette fonctionnalité est utile pour séparer en toute sécurité les privilèges d'accès aux données et aux fichiers entre l'Admin et l'Utilisateur. Elle peut également être utilisée pour activer un magasin de fichiers caché afin d'éviter d'exposer des fichiers non nécessaires sur des systèmes non fiables. La taille des partitions entre l'Admin et l'Utilisateur peut également être ajustée si vous le souhaitez.

REMARQUE : Cette fonctionnalité est *facultative* et peut être désactivée en ne cochant pas la case « Enable Dual Partition » (Activer la double partition) lors de la configuration (*Figure 4.15*)

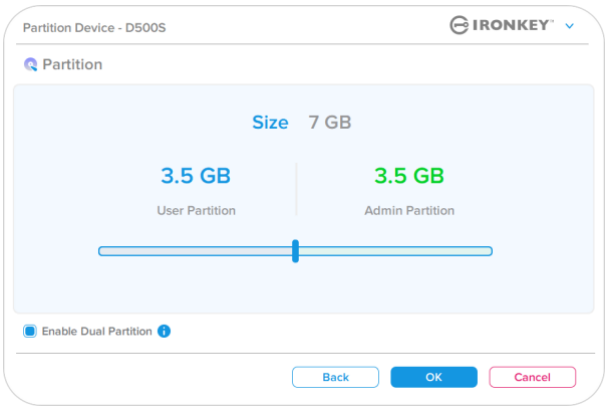


Figure 4.15- Partitionner la clé USB

Pour ajuster et répartir la taille des partitions entre l'Utilisateur et l'Admin, déplacez le curseur vers la gauche ou la droite respectivement (*Figure 4.16*).

- Les partitions peuvent être ajustées par incréments de 0,5 Go.
- Le dimensionnement de la partition est basé sur la capacité totale de l'espace de stockage disponible sur la partition cachée.
- Par défaut, le curseur de double partition est configuré pour diviser l'espace de stockage de manière égale entre Admin et Utilisateur, jusqu'à ce qu'il soit ajusté manuellement.
- La plus petite taille de partition pouvant être allouée est de 1 Go.

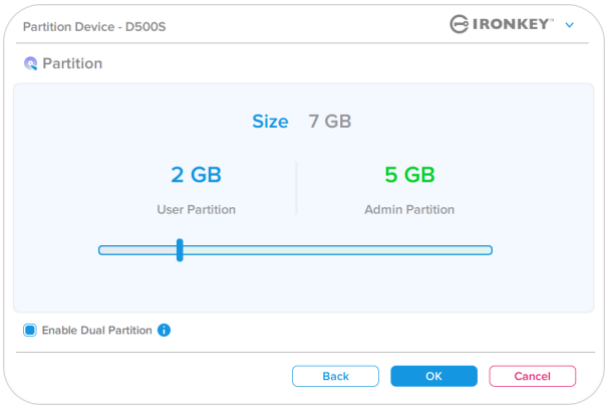


Figure 4.16- Partitionner la clé USB, curseur ajusté

Connexion Admin

Une fois que la clé USB est entièrement configurée avec les deux partitions activées, la connexion Admin proposera une option pour la déverrouiller afin d'accéder à la partition Admin OU à la partition Utilisateur à chaque connexion réussie. (*Figure 4.17*)

REMARQUE : Vous ne pouvez ouvrir qu'une seule partition à la fois. Les partitions Utilisateur et Admin ne peuvent pas être déverrouillées en même temps.

La connexion Utilisateur ne propose pas cette option ; elle déverrouille automatiquement la partition Utilisateur uniquement.

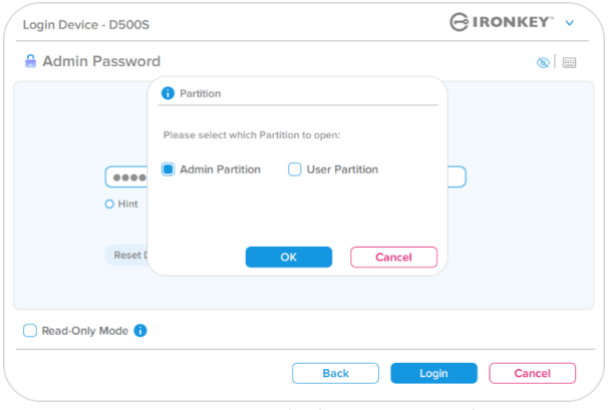


Figure 4.17 – Exemple de connexion Admin, sélection de la partition

Initialisation de la clé USB

Informations de contact

Entrez vos informations de contact dans les zones de texte prévues à cet effet (voir la *Figure 4.18*).

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

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

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

Le champ **« Details » (Détails)** peut contenir jusqu'à 156 caractères, mais ne doit pas contenir le mot de passe exact.

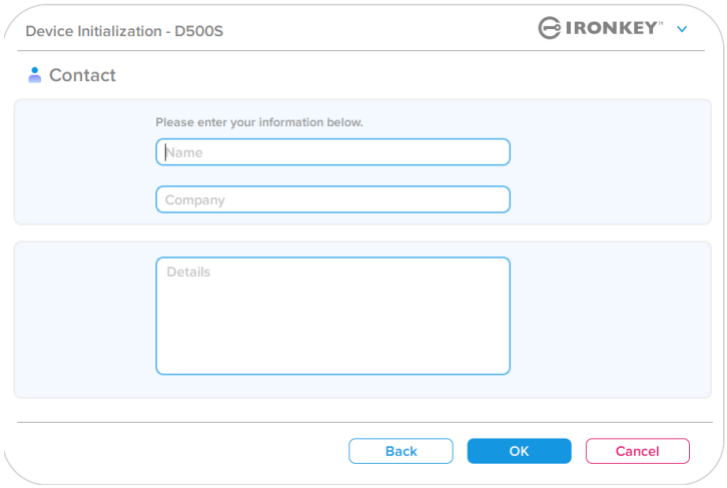


Figure 4.18 – Informations de contact

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

Utilisation de la clé USB (environnements Windows & macOS)

Connexion pour l'Admin 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 D500S se lancera, en affichant d'abord l'écran de connexion User Password (Mot de passe Utilisateur). À partir de là, vous pouvez vous connecter avec le mot de passe Utilisateur, afficher les informations de contact saisies ou vous connecter en tant qu'Admin (*Figure 5.1*). Si vous cliquez sur le bouton « Login as Admin » (Se connecter en tant qu'Admin) (illustré ci-dessous), l'application passe au menu de connexion Admin, où vous pouvez vous connecter en tant qu'Admin pour accéder aux paramètres et fonctionnalités associées à ce rôle (*Figure 5.2*).

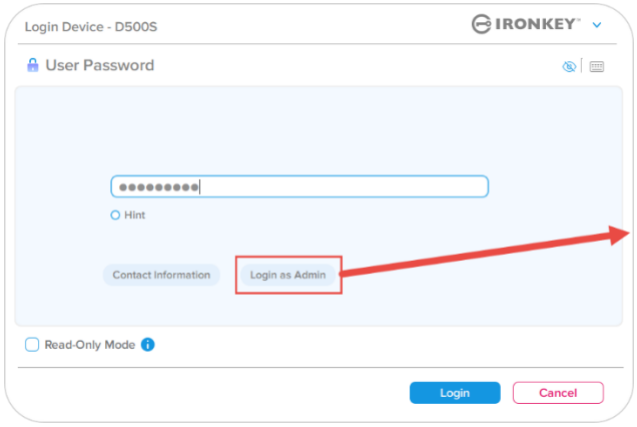


Figure 5.1 – Connexion à l'aide du mot de passe Utilisateur (Admin activé)

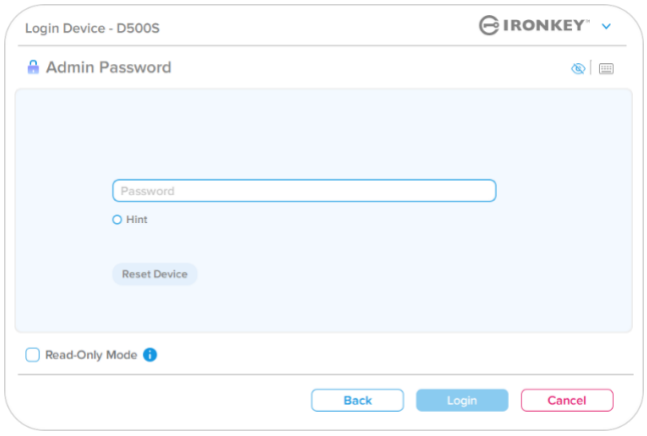


Figure 5.2 – Connexion à l'aide du mot de passe Admin

Connexion en Mode Utilisateur uniquement (Admin non activé)

Comme indiqué précédemment, bien qu'il soit recommandé d'utiliser la fonctionnalité du rôle Admin pour tirer pleinement parti de votre appareil, la clé USB IronKey peut également être initialisée en mode Utilisateur uniquement (mot de passe unique, utilisateur unique). Cette option est destinée aux personnes qui souhaitent une approche simple, avec un seul mot de passe, pour sécuriser leurs données sur leur clé USB. (*Figure 5.3*)

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

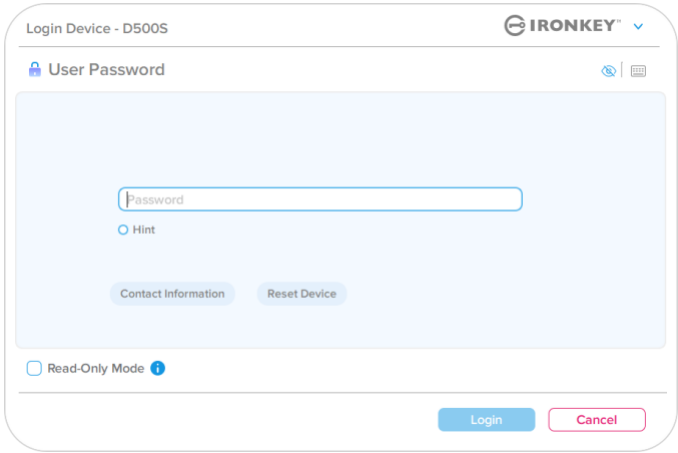


Figure 5.3 – Connexion à l'aide du mot de passe Utilisateur (Admin non activé)

Utilisation de la clé USB

Déverrouillage en mode lecture seule

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

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

Pour déverrouiller la clé USB en mode lecture seule :

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

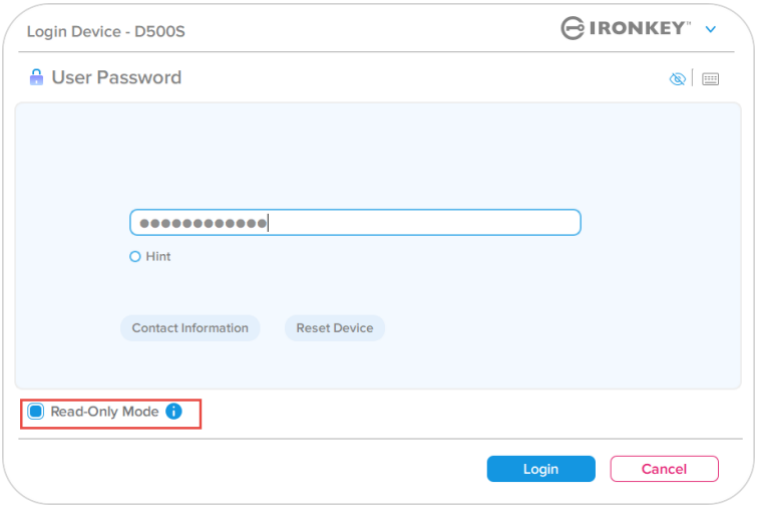


Figure 5.4 – Mode lecture seule

Si vous souhaitez déverrouiller la clé USB avec un accès complet en lecture/écriture à la partition de données sécurisée, vous devez arrêter la D500S et vous reconnecter, en laissant la case « Read-Only Mode » (Mode lecture seule) décochée.

Remarque : Les options Admin de la D500S ont une fonctionnalité de mode lecture seule forcée pour les données Utilisateur, ce qui signifie que l'Admin peut forcer le déverrouillage de la connexion Utilisateur en lecture seule (voir page 31 pour plus de détails).

Utilisation de la clé USB

Protection contre les attaques par force brute

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

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

Admin/Utilisateur activé	**Protection contre les attaques par force brute Comportement de la clé USB (10 tentatives de saisie de mot de passe infructueuses)**	**Suppression des données et réinitialisation de la clé USB ?**
Mot de passe Utilisateur	Verrouillage du mot de passe. Connectez-vous en tant qu'Administrateur ou utilisez le mot de passe de récupération à usage unique pour réinitialiser le mot de passe Utilisateur	NON
Mot de passe Admin	Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimées définitivement	**OUI**
Mot de passe de récupération à usage unique	Verrouillage du mot de passe, le bouton de récupération du mot de passe s'estompe et devient inutilisable. Se connecter en tant qu'Admin pour réinitialiser le mot de passe	NON
Utilisateur uniquement Un seul utilisateur, un seul mot de passe (Admin/Utilisateur NON activé)	**Protection contre les attaques par force brute Comportement de la clé USB (10 tentatives de saisie de mot de passe infructueuses)**	**Suppression des données et réinitialisation de la clé USB ?**
Mot de passe Utilisateur	Effacement chiffré de la clé USB ; mots de passe, paramètres et données supprimées définitivement	**OUI**

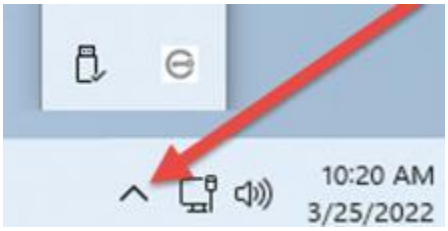
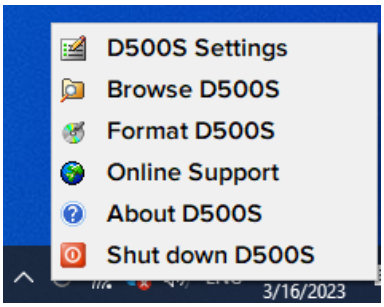
* Une fois que vous vous êtes authentifié avec succès sur la clé USB, le compteur d'échecs de connexion sera réinitialisé en fonction de la méthode de connexion utilisée. L'effacement chiffré effacera tous les mots de passe, les clés de chiffrement et les données ; **vos données seront perdues définitivement.**

Accès à mes fichiers sécurisés

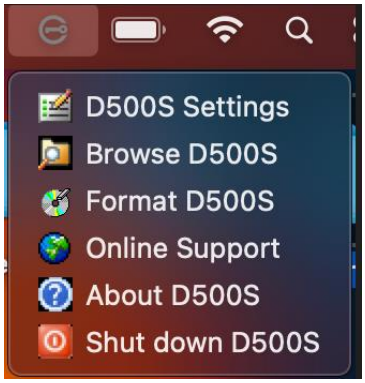
Après avoir déverrouillé la clé USB, vous pouvez accéder à vos fichiers sécurisés. Les fichiers sont automatiquement chiffrés et déchiffrés lorsque vous les enregistrez ou les ouvrez sur la clé USB. Cette technologie vous permet de travailler comme vous le feriez avec un disque ordinaire, tout en offrant une sécurité forte et permanente.
Conseil : Vous pouvez également accéder à vos fichiers en cliquant avec le bouton droit sur l'icône IronKey dans la barre des tâches de Windows et en cliquant sur **Browse D500S (Parcourir la D500S)** (*Figure 6.2*)

Options de la clé USB - (Environnement Windows)

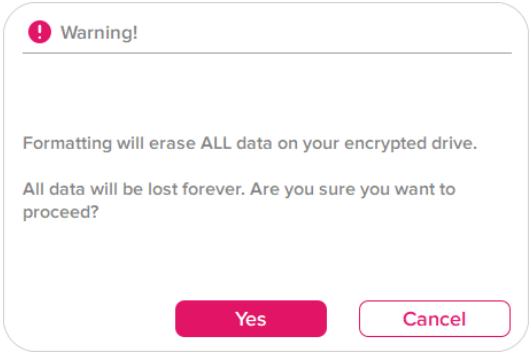
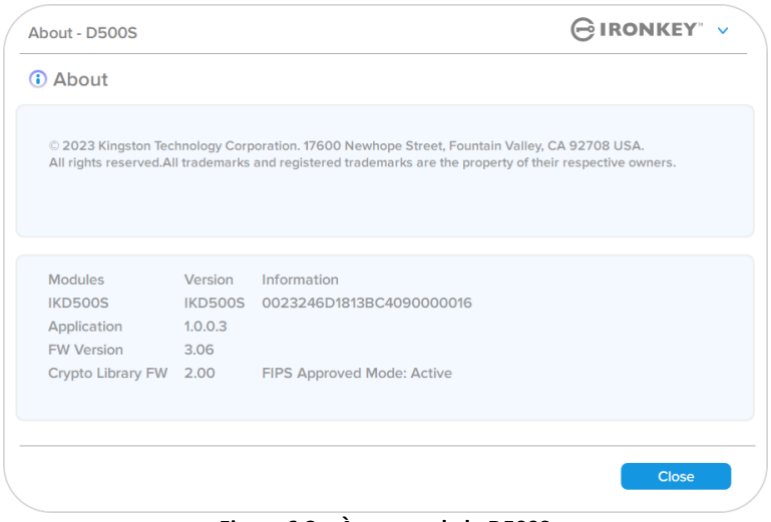
Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre. Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles (*Figure 6.2*). Les détails concernant ces options se trouvent aux pages 21 à 25 du présent manuel.

• Lorsque vous êtes connecté à la clé USB, une icône IronKey apparaît dans le coin droit de la fenêtre (*Figure 6.1*)	 **Figure 6.1 – Icône IronKey dans la barre des tâches**
• Un clic droit sur l'icône IronKey ouvrira le menu de sélection des options disponibles (*Figure 6.2*). Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.	 **Figure 6.2 – Clic droit sur l'icône IronKey pour accéder aux options de la clé USB**

Options de la clé USB- (environnement macOS)

• Lorsque vous êtes connecté à la clé USB, une icône IronKey D500S se trouve dans le menu macOS illustré dans la Figure 6.3 ; elle permet d'afficher les options disponibles de la clé USB. Les détails concernant ces options se trouvent aux pages 19 à 23 du présent manuel.	 **Figure 6.3 – Icône de barre de menu macOS/menu des options de la clé USB**

Options de la clé USB

Paramètres de la D500S ::	• 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 D500S : » du présent manuel).
Parcourir la D500S :	• Permet de visualiser vos fichiers sécurisés.
Formater la D500S : Permet de formater la partition de données sécurisée. (Avertissement : Toutes les données seront supprimées) (*Figure 6.1*) **Remarque :** L'authentification par mot de passe sera requise pour le formatage.	 **Figure 6.1 – Formater la D500S**
Support en ligne :	• Cette fonction ouvre votre navigateur Internet et affiche la page http://www.kingston.com/support pour vous permettre de consulter les informations supplémentaires du support.
À propos de la D500S : Affiche des données détaillées sur la D500S, notamment des informations sur l'application, le firmware et le numéro de série (*Figure 6.2*) **Remarque :** Le numéro de série unique de la clé USB se trouve sous la colonne « Informations ».	 **Figure 6.2 – À propos de la D500S**
Arrêter la D500S :	• Permet de fermer correctement la D500S avant de la déconnecter physiquement du système, en toute sécurité.

Paramètres de la D500S :

Paramètres Admin

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

- **Password (Mot de passe) :** Permet de modifier le mot de passe Admin et/ou l'indice (*Figure 7.1*)
- **Contact Info (Informations de contact) :** Permet d'ajouter/d'afficher/de modifier les informations de contact (*Figure 7.2*)
- **Language (Langue) :** Permet de modifier la langue actuelle (*Figure 7.3*)
- **Admin Options (Options Admin) :** Permet d'activer des fonctionnalités supplémentaires telles que : (*Figure 7.4*)
    - changer le mot de passe de l'utilisateur ;
    - réinitialiser le mot de passe de connexion (pour le mot de passe Utilisateur) ;
    - activer un mot de passe de récupération à usage unique ;
    - activer un mot de passe d'effacement chiffré ;
    - forcer le mode lecture seule pour les données Utilisateur.

REMARQUE : Des détails supplémentaires sur les options Admin sont indiqués à partir de la page 26.

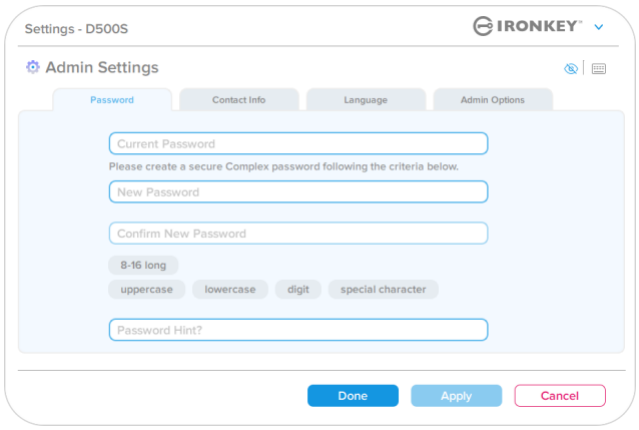


Figure 7.1 – Options de mot de passe

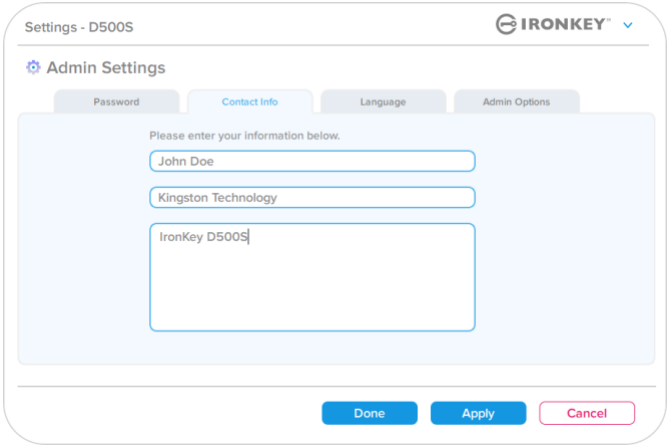


Figure 7.2 – Informations de contact

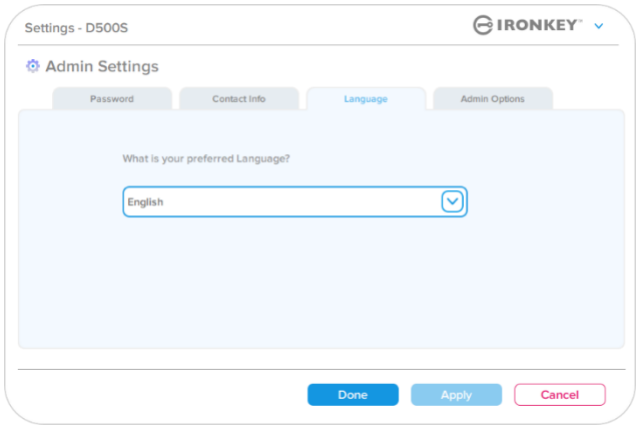


Figure 7.3 – Options de langue

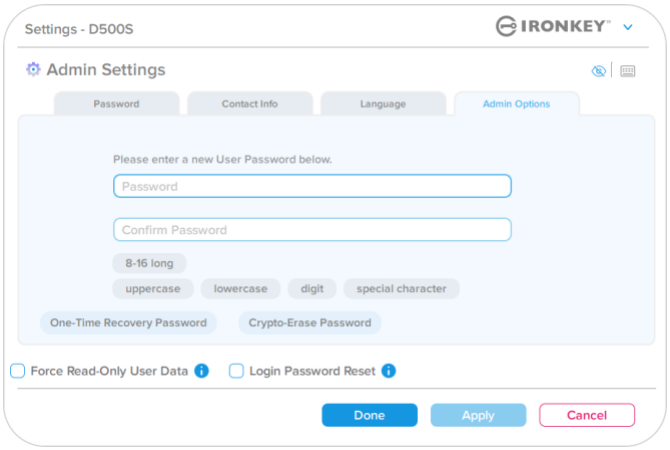
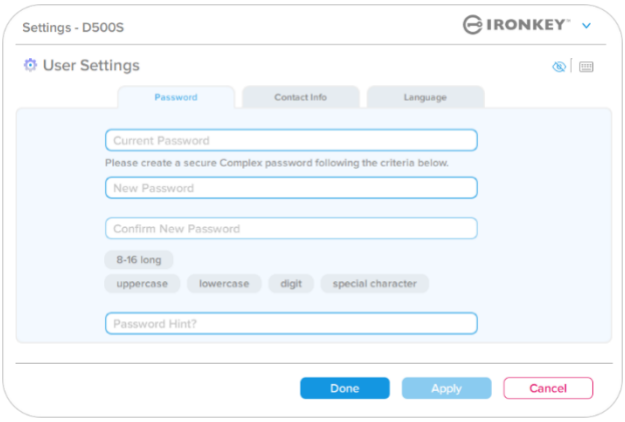
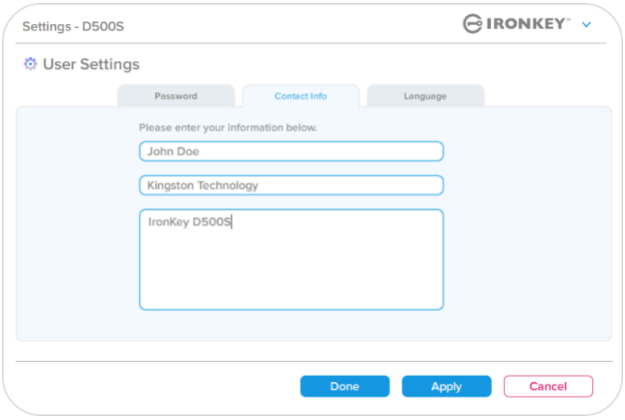
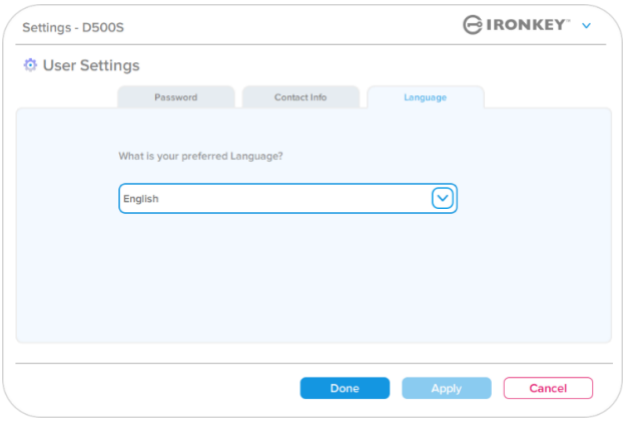


Figure 7.4 – Options Admin

Paramètres de la D500S :

Paramètres Utilisateur : Admin activé

La connexion Utilisateur limite l'accès aux paramètres suivants :

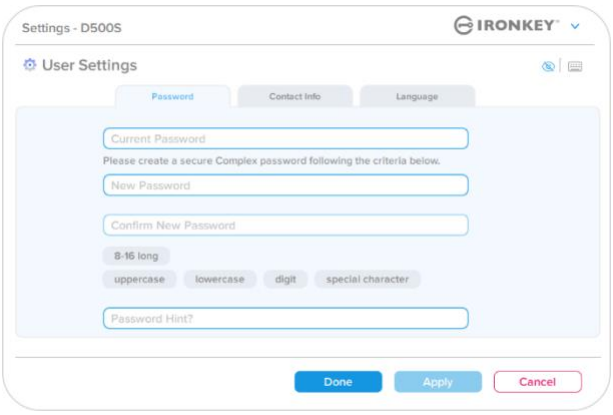
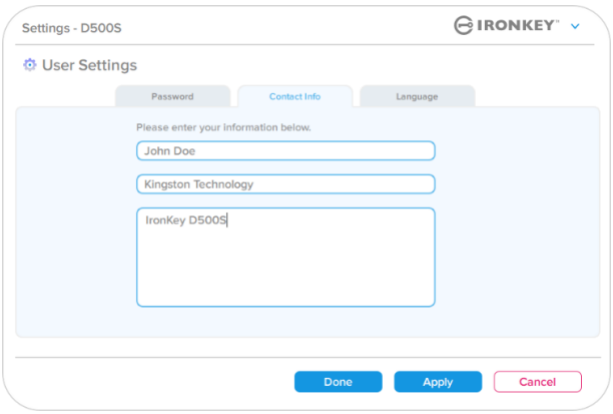
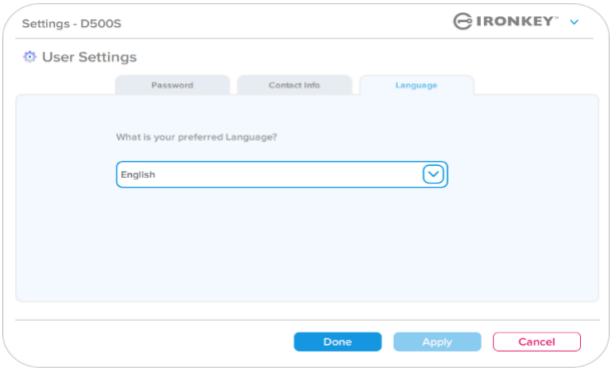
Password (Mot de passe) : Permet de modifier le mot de passe Utilisateur et/ou l'indice (*Figure 7.5*)	 **Figure 7.5 – Options de mot de passe (Admin activé : connexion Utilisateur)**
Contact Info (Informations de contact) : Permet d'ajouter/d'afficher/de modifier vos informations de contact (*Figure 7.6*)	 **Figure 7.6 – Informations de contact (Admin activé : connexion Utilisateur)**
Language (Langue) : Permet de modifier la langue actuelle (*Figure 7.7*)	 **Figure 7.7 – Paramètres de langue (Admin activé : connexion Utilisateur)**

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

Paramètres de la D500S :

Paramètres Utilisateur : Admin non activé

Comme mentionné précédemment, l'initialisation de la D500S sans activer les mots de passe Admin et Utilisateur configurera la clé USB dans une configuration **Mot de passe unique, Utilisateur unique (mode Utilisateur uniquement)**. Cette configuration n'a pas accès aux options ou fonctionnalités Admin. Cette configuration aura accès aux paramètres suivants de la D500S :

Password (Mot de passe) : Permet de modifier le mot de passe Utilisateur et/ou l'indice (*Figure 7.8*)	 **Figure 7.8 – Options de mot de passe (mode Utilisateur uniquement)**
Contact Info (Informations de contact) : Permet d'ajouter/d'afficher/de modifier vos informations de contact (*Figure 7.9*)	 **Figure 7.9 – Informations de contact (mode Utilisateur uniquement)**
Language (Langue) : Permet de modifier la langue actuelle (*Figure 7.10*)	 **Figure 7.10 – Paramètres de langue (mode Utilisateur uniquement)**

Paramètres de la D500

Modifier et sauvegarder les paramètres

- Chaque fois que les paramètres sont modifiés dans les paramètres de la D500S (par exemple, informations de contact, langue, modification du mot de passe, options Admin, etc.), la clé USB vous invitera à saisir votre mot de passe afin d'accepter et d'appliquer ces modifications (*Figure 7.11*).

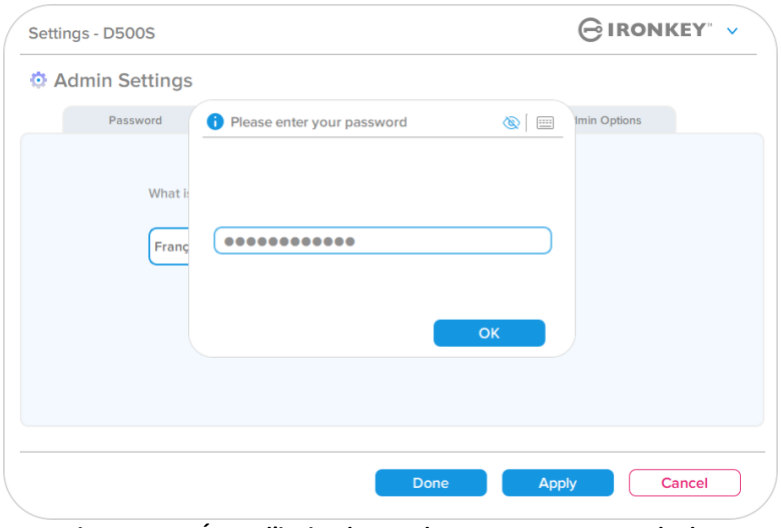


Figure 7.11 – Écran d'invite du mot de passe pour sauvegarder les modifications des paramètres de la D500S

Remarque : Si vous êtes sur l'écran de demande du mot de passe ci-dessus et que vous souhaitez annuler ou modifier vos modifications, vous pouvez le faire en vous assurant simplement que le champ du mot de passe est vide et en cliquant sur « OK ». Cela fermera la boîte de dialogue « Please enter your password » (Veuillez saisir votre mot de passe) et vous ramènera au menu des paramètres de la D500S.

Fonctionnalités Admin

Options disponibles pour réinitialiser le mot de passe Utilisateur

Les fonctionnalités de la configuration Admin offrent plusieurs façons de réinitialiser en toute sécurité le mot de passe Utilisateur, que ce soit 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 :

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

Changez manuellement le mot de passe Utilisateur dans le menu « Options Admin ». Ce changement est instantané ; il prendra effet à la prochaine connexion Utilisateur (*Figure 8.1*)

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

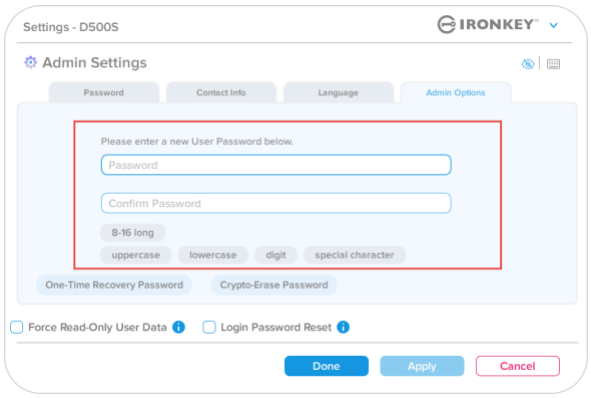


Figure 8.1 – Options Admin/réinitialisation du mot de passe Utilisateur

Login Password Reset (Réinitialisation du mot de passe à la connexion) :

L'activation de la réinitialisation du mot de passe obligera **l'Utilisateur à se connecter en utilisant le mot de passe temporaire défini par l'Admin**, puis à le changer pour un mot de passe de son choix. Cette fonctionnalité est utile lorsque la clé USB est confiée à une autre personne pour qu'elle l'utilise. (voir la *Figure 8.2 et la Figure 8.3*)

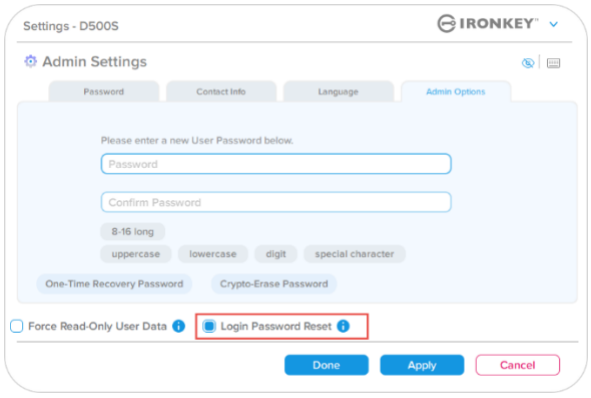


Figure 8.2 – Bouton de réinitialisation des mots de passe de connexion

Remarque : Cette réinitialisation prendra effet lors de la prochaine connexion Utilisateur réussie. L'option de mot de passe sera automatiquement appliquée en fonction de l'option initiale définie pendant le processus d'initialisation (Complexe ou Phrase de passe).

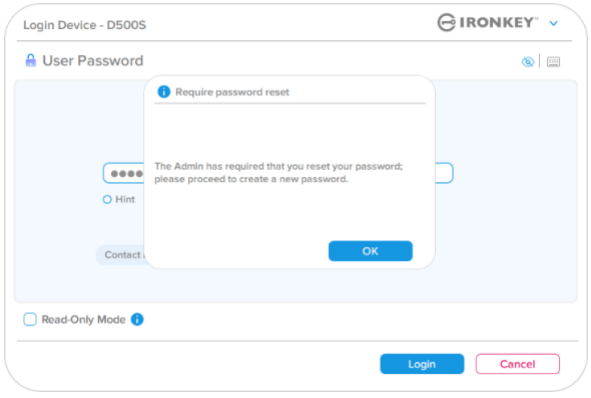


Figure 8.3 – Notification de réinitialisation après saisie du mot de passe Utilisateur

Fonctionnalités Admin

Mot de passe de récupération à usage unique

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

Mot de passe de récupération à usage unique

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

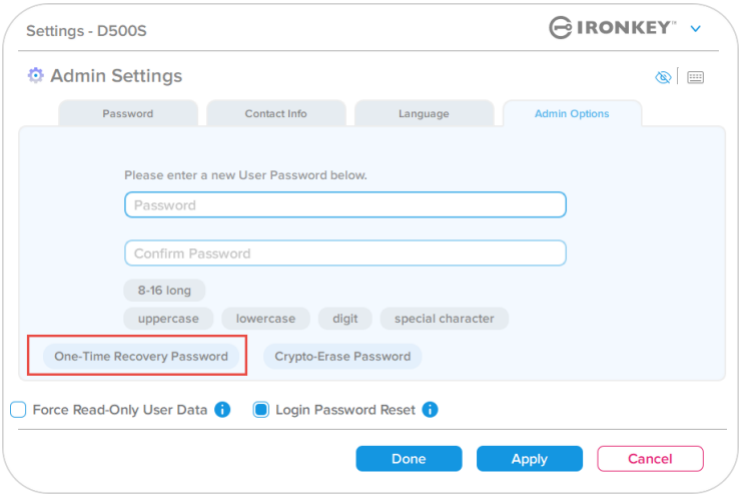


Figure 8.4 – Bouton Mot de passe de récupération à usage unique

Étape 2 : Créez un mot de passe de récupération à usage unique en utilisant la même option que celle utilisée initialement pour la clé USB (Complexe ou Phrase de passe).

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

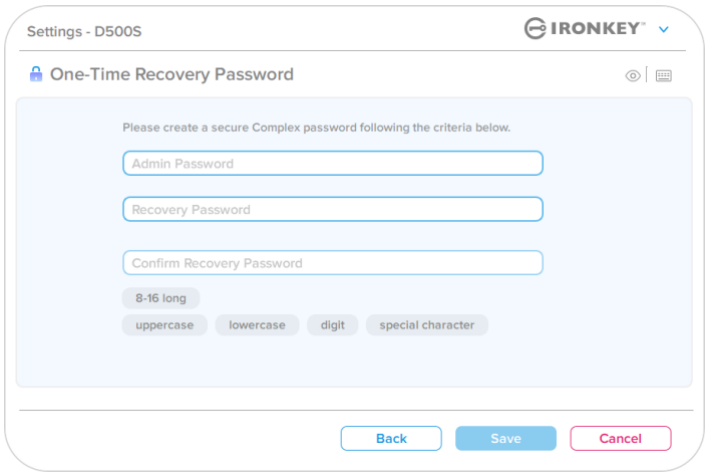


Figure 8.5 – Configuration du mot de passe de récupération à usage unique

Fonctionnalités Admin

Utilisation du mot de passe de récupération à usage unique

Étape 1 :
Après la création du mot de passe de récupération à usage unique, un nouveau bouton apparaîtra sur l'écran de connexion **User Password (Mot de passe Utilisateur)** lors de la prochaine connexion. Cliquez sur le bouton **Recovery Password (Mot de passe de récupération)** pour lancer le processus.

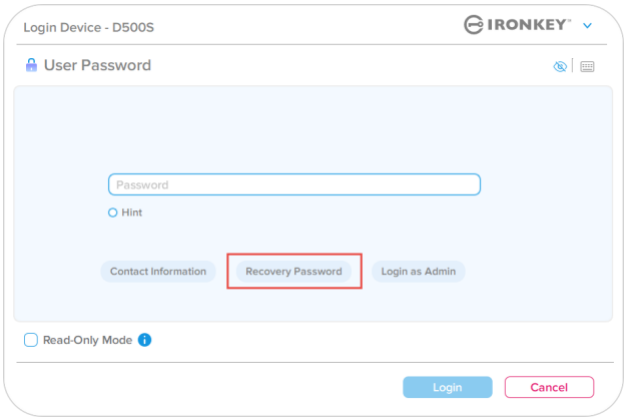


Figure 8.6 – Bouton Recovery Password (Mot de passe de récupération)

Étape 2 : L'écran **Recovery Password (Mot de passe de récupération)** s'affiche, et vous permet d'entrer le mot de passe de récupération et de créer un nouveau mot de passe Utilisateur. (*Figure 8.7*)

Important : Important : Le mot de passe de récupération à usage unique utilise également une fonctionnalité de sécurité intégrée qui comptabilise le nombre de tentatives de connexion infructueuses. **Après 10 saisies incorrectes du mot de passe de récupération à usage unique, ce dernier sera désactivé** et devra être réactivé en se connectant à la clé USB en tant qu'Admin (voir les pages 19 et 33 pour plus de détails).

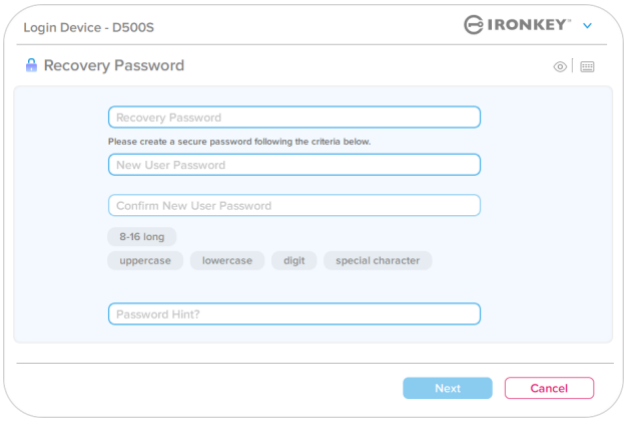


Figure 8.7 – Menu Recovery Password (Mot de passe de récupération)

Étape 3: En cas de succès, vous serez ramené à l'écran **User Password (Mot de passe Utilisateur)**. Le bouton **Recovery Password (Mot de passe de récupération)** est maintenant absent, et le mot de passe Utilisateur saisi à l'étape 2 deviendra le nouveau mot de passe Utilisateur. (*Figure 8.8*)

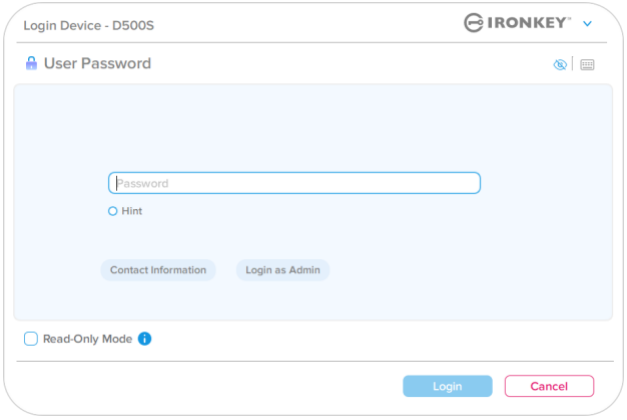


Figure 8.8 – Écran de connexion User Password (Mot de passe Utilisateur) montrant que le bouton Recovery Password (Mot de passe de récupération) disparaît une fois utilisé correctement.

Fonctionnalités Admin

Mot de passe d'effacement chiffré

La clé IronKey D500S est dotée d'une fonctionnalité unique de mot de passe d'effacement chiffré conçue pour se protéger en cas de violation physique. Cette fonctionnalité efface de manière sécurisée le contenu de votre clé USB lorsqu'elle est utilisée, donnant l'impression qu'aucune donnée n'a jamais été écrite dessus. Lorsque cette fonctionnalité est activée et que la clé USB est déverrouillée avec le mot de passe d'effacement chiffré, elle effectue un effacement chiffré discret sur la clé D500S et ouvre le lecteur en mode d'état d'usine avec une partition Utilisateur vide. La clé de chiffrement précédente sera supprimée et une nouvelle clé de chiffrement sera créée pour la remplacer. ***À utiliser avec précaution***

- Pour **activer** cette fonctionnalité, cliquez sur le bouton Crypto-Erase password (Mot de passe d'effacement chiffré) situé dans l'onglet Admin Options (Options Admin) :

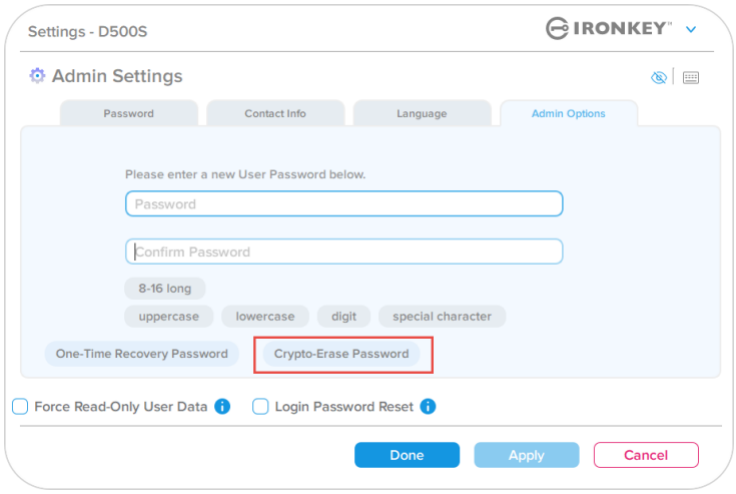


Figure 8.9 – Activation du mot de passe d'effacement chiffré

Mot de passe d'effacement chiffré :

- Les règles relatives aux mots de passe sont basées sur les paramètres initiaux de la clé USB (Complexe ou Phrase de passe).
- Le mot de passe Admin sera nécessaire pour appliquer les modifications.

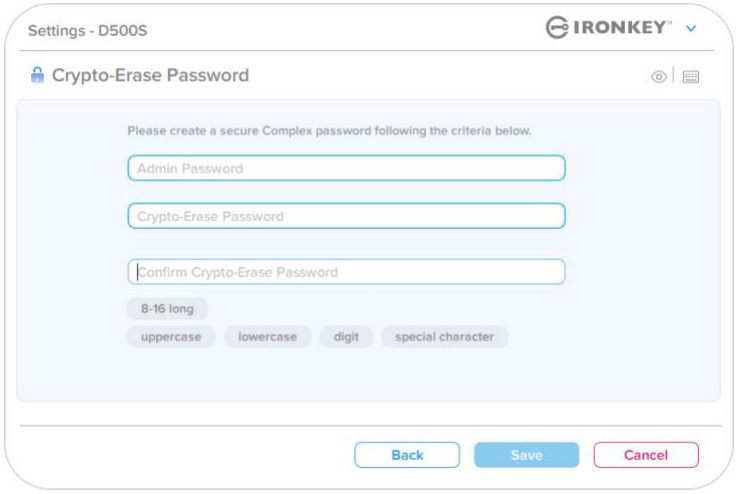


Figure 8.10 – Création d'un mot de passe d'effacement chiffré

Fonctionnalités Admin

Utilisation du mot de passe d'effacement chiffré

Lorsque le mot de passe d'effacement chiffré est utilisé, il supprime et remplace les mots de passe Admin et Utilisateur précédents. En outre, tous les paramètres de configuration précédents seront supprimés, de même que toutes les données stockées sur la clé USB, et celle-ci passera en mode Utilisateur uniquement.

Pour utiliser le mot de passe d'effacement chiffré :

1. Lancez IronKey.exe pour exécuter l'application IronKey.

2. Sur l'écran de connexion User Password (Mot de passe Utilisateur), appuyez sur « **CTRL + ALT +C** » pour passer à la saisie du mot de passe d'effacement chiffré. Si vous procédez correctement, une barre bleue plus épaisse sera visible sous l'écran de saisie du mot de passe, indiquant que le mot de passe d'effacement chiffré est prêt à être saisi. (*Figure 8.11*)

REMARQUE : Le mot de passe d'effacement chiffré ne peut être activé que sur l'écran de connexion Mot de passe Utilisateur.

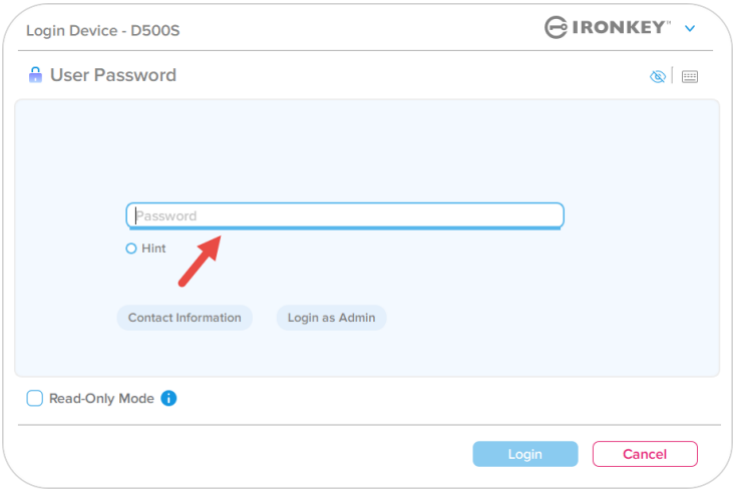


Figure 8.11- Effacement chiffré activé, avec une barre bleue épaisse

Une fois le mot de passe d'effacement chiffré utilisé, la clé USB efface tout son contenu et seule une partition vide apparaît. La clé USB est alors en mode Utilisateur uniquement et le mot de passe d'effacement chiffré sera le mot de passe à utiliser pour s'y connecter jusqu'à ce qu'elle soit réinitialisée.

Important : cette fonctionnalité efface toutes les données sur la clé USB. Tout ce qui a été stocké précédemment sera perdu à jamais.

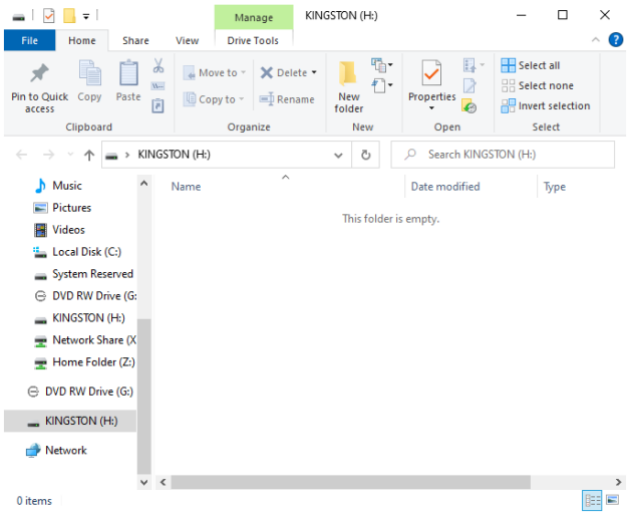


Figure 8.12 – Drive wipe after Mot de passe d'effacement chiffré used

Fonctionnalités Admin

Forcer la lecture seule pour les données Utilisateur

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

- Pour activer l'option Force Read-Only for the User data (Forcer la lecture seule pour les données Utilisateur), cochez la case correspondante et cliquez sur « Apply » (Appliquer). (*Figure 8.13*)

  Remarque : Ce mode de lecture seule forcée ne s'applique qu'à l'Utilisateur et ne concerne pas la connexion Admin. La connexion Admin aura toujours les privilèges d'accès en lecture et en écriture, et pourra toujours activer le mode lecture seule si nécessaire.

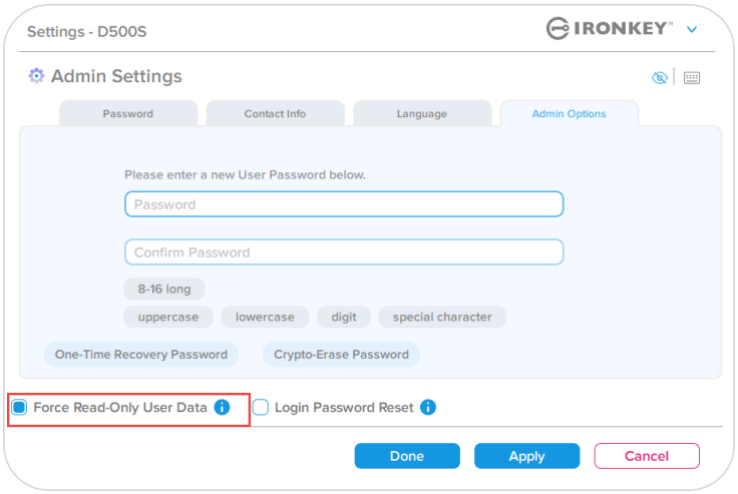


Figure 8.13 – Activer l'option « Force Read-Only User data » (Forcer la lecture seule pour les données Utilisateur) (Le mot de passe Admin sera nécessaire pour appliquer les modifications)

- Une fois cette option activée, le bouton **« Read-Only Mode » (Mode lecture seule)** 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 8.14*)

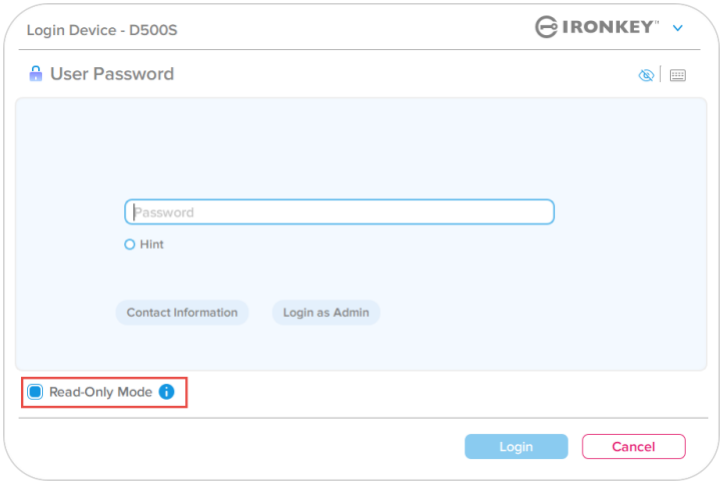


Figure 8.14 – Le mode Lecture seule est activé de manière forcée pour l'utilisateur et ne peut être désactivé que par l'Admin.

Aide et dépannage

Verrouillage du périphérique

La D500S comprend une fonctionnalité de sécurité qui empêche tout accès non autorisé à la partition de données après un certain nombre maximum de tentatives de connexion infructueuses **consécutives** (« MAX » pour faire court). Par défaut, ce nombre de tentatives infructueuses est de 10 pour chaque méthode de connexion (Admin/Utilisateur/Mot de passe de récupération à usage unique).

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

1. Une connexion réussie avant d'atteindre le MAX.

2. Atteindre le MAX et effectuer un verrouillage ou un formatage de la clé USB, selon sa configuration.

- Si un mot de passe incorrect est saisi, un message d'erreur s'affiche en rouge juste au-dessus du champ de saisie du mot de passe, indiquant un échec de connexion. (*Figure 9.1*)

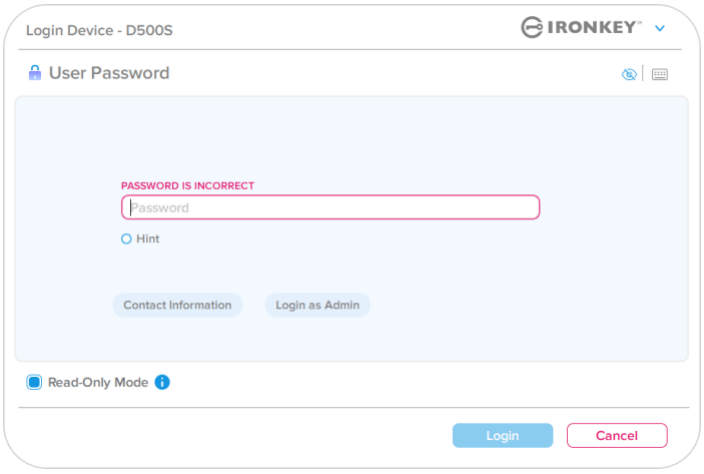


Figure 9.1 – Message Mot de passe incorrect

- Après la **7ème** tentative infructueuse consécutive, un message d'erreur supplémentaire avertit l'utilisateur qu'il lui reste 3 tentatives avant d'atteindre la limite MAX (par défaut, 10 tentatives) (*Figure 9.2*)

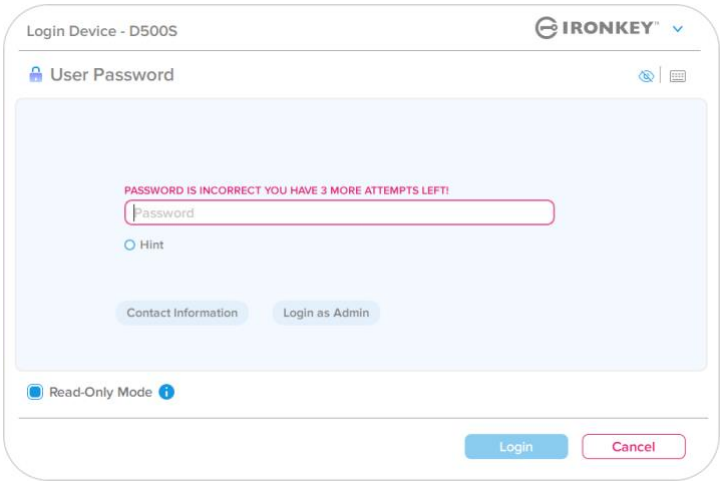


Figure 9.2 – 7ème tentative de saisie de mot de passe infructueuse

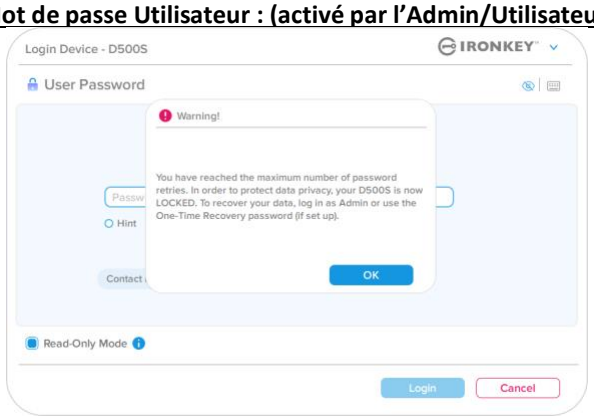
Aide et dépannage

Verrouillage du périphérique

Important :
Après la **10ème** et dernière tentative de connexion infructueuse, 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 USB se verrouillera, ce qui vous obligera à vous connecter avec une autre méthode (le cas échéant), ou à effectuer une réinitialisation, ce qui **formatera les données, lesquelles seront définitivement perdues**. Ces comportements sont également mentionnés à la page 19 du présent guide de l'utilisateur.

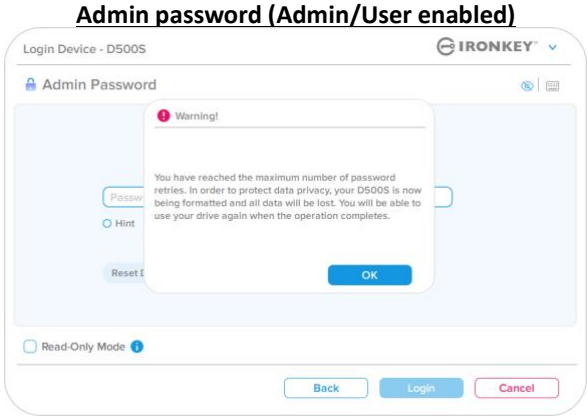
Les figures 9.3 à 9.6 ci-dessous illustrent le comportement visuel pour la 10ème et dernière tentative de connexion infructueuse pour chaque méthode de mot de passe de connexion :

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



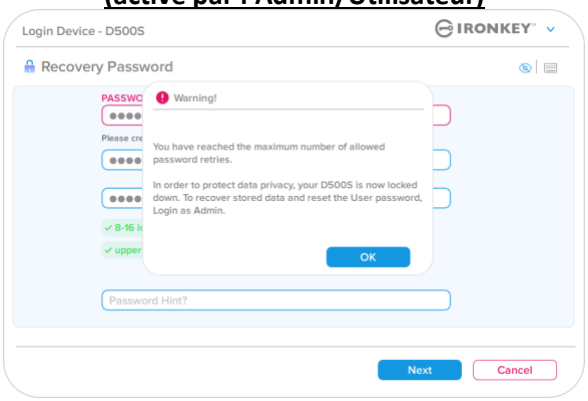
VERROUILLAGE DE LA CLÉ USB
Figure 9.3

Admin password (Admin/User enabled)



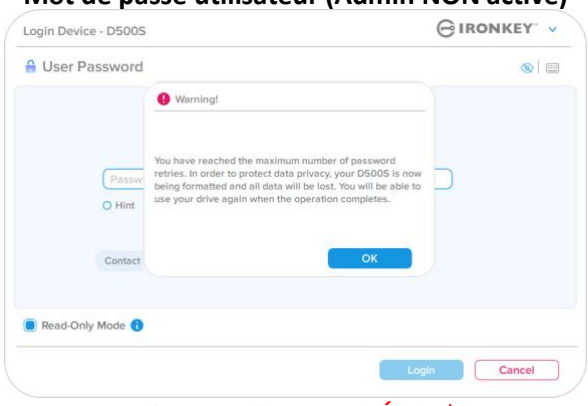
FORMATAGE DE LA CLÉ USB*
Figure 9.4

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



VERROUILLAGE DE LA CLÉ USB
Figure 9.5

Mot de passe utilisateur (Admin NON activé)



FORMATAGE DE LA CLÉ USB*
Figure 9.6

Ces mesures de sécurité empêchent qu'une autre personne (qui n'a pas votre mot de passe) puisse effectuer d'innombrables tentatives de connexion et d'accéder à vos données sensibles (également connu sous le nom d'attaque par la force brute). Si vous êtes le propriétaire de la D500S et que vous avez oublié votre mot de passe, les mêmes mesures de sécurité seront appliquées, notamment un formatage de la clé USB*. Pour plus d'informations sur cette fonctionnalité, voir *« Réinitialiser la clé USB »* à la page 25.

**Remarque : Un formatage de la D500S supprimera TOUTES les informations stockées sur sa partition de données sécurisée.*

Aide et dépannage

Réinitialiser la clé USB

Si vous oubliez votre mot de passe ou si vous devez réinitialiser votre clé USB, vous pouvez cliquer sur le bouton « Reset Device » (Réinitialiser l'appareil) qui peut apparaître à deux endroits selon la configuration de la clé USB (soit dans le menu Admin Login Password (Mot de passe de connexion Admin) si le mode Admin/Utilisateur est activé, soit dans le menu de connexion « User Password » (Mot de passe Utilisateur) si le mode Admin/Utilisateur n'est pas activé) lorsque le programme D500S Launcher est exécuté (voir la *Figure 9.7* et la *Figure 9.8*)

- Cette option vous permet de créer un nouveau mot de passe, mais pour protéger la confidentialité de vos données, la D500S sera formatée. Par conséquent, ce processus effacera définitivement toutes vos données.*

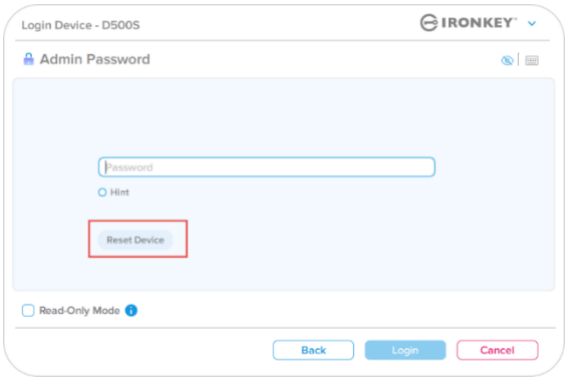


Figure 9.7 – Mot de passe Admin : Bouton Reset Device (Réinitialiser l'appareil)

- **Remarque :** Lorsque vous cliquez sur le bouton *« Reset Device » (Réinitialiser l'appareil)*, un message vous demande si vous souhaitez saisir un nouveau mot de passe avant le lancement du formatage. Vous pouvez alors 1) cliquer sur *« OK »* pour confirmer, ou 2) cliquer sur *« Cancel »* (Annuler) pour revenir à la fenêtre de connexion. (Voir la *Figure 9.8*)

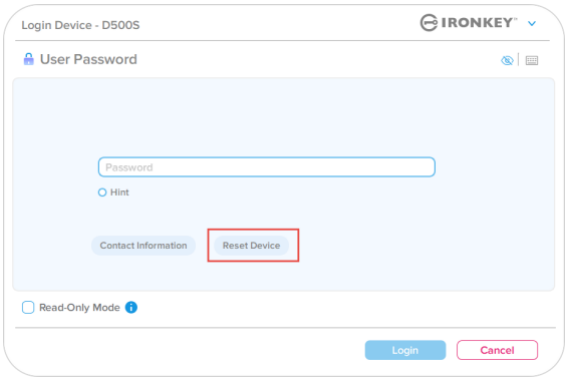


Figure 9.8 – Mot de passe Utilisateur (Admin/Utilisateur non activé) – Réinitialisation de la clé USB

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

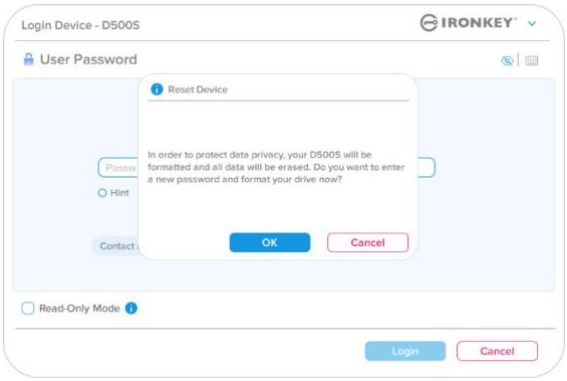


Figure 9.9 – Confirmation de réinitialisation de la clé USB

Aide et dépannage

Conflit de lettres de lecteur : Systèmes d'exploitation Windows

- Comme indiqué dans la section *« Configuration système »* du présent manuel (page 3), la D500S 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 NE DÉPEND PAS des partages de réseau parce que ces partages sont spécifiques aux profils d'utilisateur et non au profil matériel du système. Une lettre attribuée à un lecteur du réseau peut donc apparaître comme disponible pour le système d'exploitation.

- Autrement dit, Windows peut attribuer à la D500S une lettre de lecteur qui est déjà utilisée par un élément du réseau ou un chemin UNC (Universal Naming Convention), ce qui provoque un conflit de lettres de lecteur. Dans ce cas, veuillez consulter votre administrateur ou le service d'assistance pour modifier l'attribution des lettres de lecteur dans le gestionnaire des disques Windows Disk Management (les droits d'administrateur sont nécessaires). Comme indiqué dans la section *« Configuration système »* du présent manuel (page 3), la D500S 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 NE DÉPEND PAS des partages de réseau parce que ces partages sont spécifiques aux profils d'utilisateur et non au profil matériel du système. Une lettre attribuée à un volume du réseau peut donc apparaître comme disponible pour le système d'exploitation.

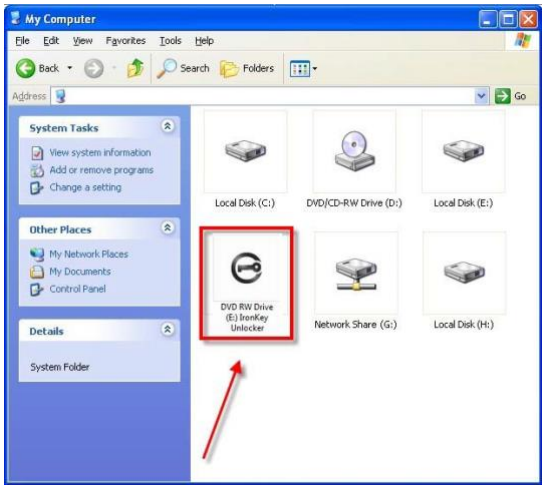


Figure 9.10 – Exemple de lettre de lecteur

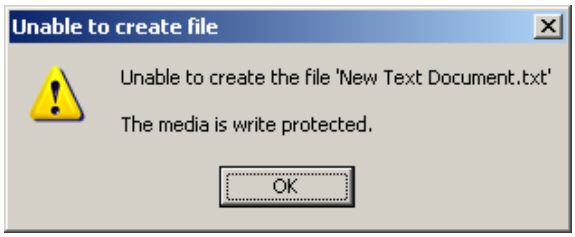
Dans cet exemple (*Figure 9.10*), la D500S utilise le lecteur F:, qui est la première lettre de lecteur disponible après le lecteur E: (le dernier disque physique avant l'écart entre les lettres de lecteur). Comme la lettre G: est un partage réseau et qu'elle ne fait pas partie du profil matériel, la D500S peut tenter de l'utiliser comme deuxième lettre de lecteur, ce qui provoque un conflit.

Si vous n'avez aucun lecteur de réseau sur votre système et que la D500S 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 10 et 11 et peut vous éviter ce problème. Toutefois, si vous ne parvenez pas à résoudre un conflit de lettres de lecteur, veuillez contacter le support technique de Kingston ou consultez le site Kingston.com/support pour obtenir de l'aide.

Aide et dépannage

Messages d'erreu

Unable to create file (Impossible de créer le fichier) : 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.	 **Figure 9.11 – Erreur « Unable to create file » (Impossible de créer le fichier)**
Error Copying File or Folder (Erreur lors de la copie du fichier ou du dossier) : 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 – « Error Copying File or Folder » (Erreur lors de la copie du fichier ou du dossier)**
Error Deleting File or Folder (Erreur lors de la suppression du fichier ou du dossier) : 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.	 **Figure 9.13 – « Error Deleting File or Folder » (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 D500S, puis rétablir la connexion après avoir décoché la case « Read-Only Mode » (Mode lecture seule).

Initialisation de la clé USB (environnement Linux)

Compte tenu des différentes distributions de Linux actuellement disponibles, l'apparence de l'interface peut varier d'une version à l'autre. Cependant, les commandes générales utilisées dans l'application Terminal restent très similaires et peuvent être reconnues dans les instructions qui suivent. Les exemples de captures d'écran dans cette section proviennent d'un environnement 64 bits.

Certaines versions de Linux nécessitent des privilèges de super utilisateur (ou utilisateur racine) pour exécuter correctement les commandes de la D500S dans la fenêtre de l'application du terminal.

Remarques importantes avant de poursuivre :

1.) **La D500S ne prend pas en charge l'initialisation de la clé USB sous Linux. Elle devra être entièrement initialisée et configurée sur un système Windows ou macOS pris en charge avant qu'elle ne puisse être utilisé sur une machine Linux.**

2.) **La connexion Linux ne prend en charge que les mots de passe complexes. La connexion par phrases de passe n'est pas prise en charge sous Linux.**

3.) **La prise en charge des fonctionnalités de la D500S sous Linux est limitée. Les fonctionnalités telles que le mot de passe de récupération à usage unique, le mot de passe d'effacement chiffré, la réinitialisation du mot de passe Admin/Utilisateur et le basculement en mode lecture seule ne sont pas prises en charge sous Linux.**

La D500S inclut 4 commandes utilisables sous Linux :

Ikd500s_about	Affiche les informations « About D500S » (À propos de la D500S).
Ikd500s_login	Vous permet de vous connecter à la clé USB.
Ikd500S_logout	Vous permet de vous déconnecter en toute sécurité de la clé USB D500S.
Ikd500S_resetdevice	Effectue un effacement chiffré de la clé USB et la réinitialise à l'état d'origine, en supprimant définitivement toutes les données et tous les fichiers qui y sont stockés.

REMARQUE : Pour exécuter ces commandes, vous devez ouvrir une fenêtre de l'application Terminal et parcourir le volume jusqu'au répertoire contenant les fichiers. Chaque commande doit commencer par les deux caractères suivants : « ./ » (un point et une barre oblique vers l'avant.)

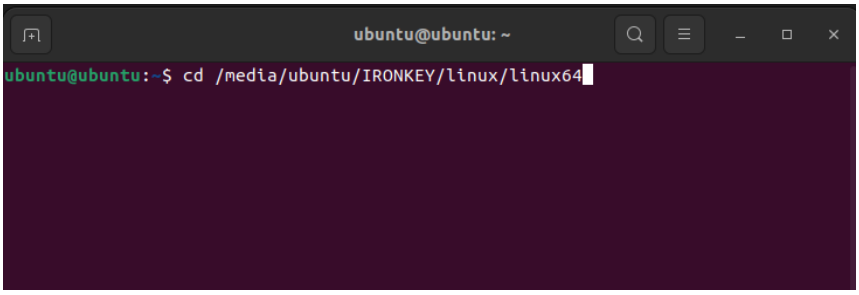
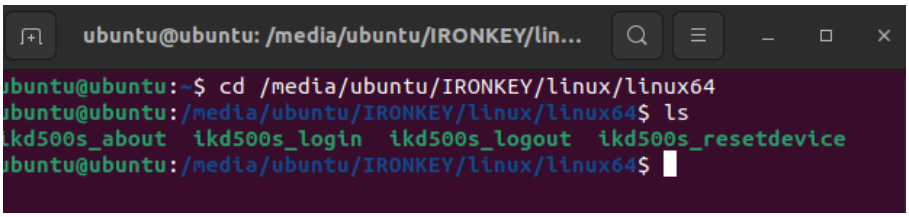
Exemple de navigation vers le chemin des commandes Linux IronKey :

Pour les utilisateurs Linux 32 bits :	Ouvrez une fenêtre d'application « Terminal » et modifiez le répertoire actuel en **/media/ubuntu/IRONKEY/linux/linux32$** en saisissant la commande suivante à l'invite : **cd /media/ubuntu/IRONKEY/linux/linux32** (puis, appuyez sur ENTRÉE.)
Pour les utilisateurs Linux 64 bits :	Ouvrez une fenêtre d'application « Terminal » et modifiez le répertoire actuel en **/media/ubuntu/IRONKEY/linux/linux64$** en saisissant la commande suivante à l'invite : **cd /media/ubuntu/IRONKEY/linux/linux64** (puis, appuyez sur ENTRÉE.)

Initialisation du périphérique (Environnement Linux)

Remarque : Si le lecteur IRONKEY n'est pas automatiquement chargé par le système d'exploitation, vous devez le charger manuellement dans une fenêtre de l'application du terminal, avec la commande Linux « mount ». Reportez-vous à la documentation Linux de votre distribution de système d'exploitation spécifique ou votre site d'assistance habituel pour utiliser la syntaxe et les options de commande appropriées. Certaines distributions Linux peuvent exiger la saisie du nom d'utilisateur pour exécuter des commandes, c'est-à-dire « ubuntu » dans les exemples ci-dessus.

Repérer et afficher les fichiers de commande Linux de la clé USB IronKey D500S :

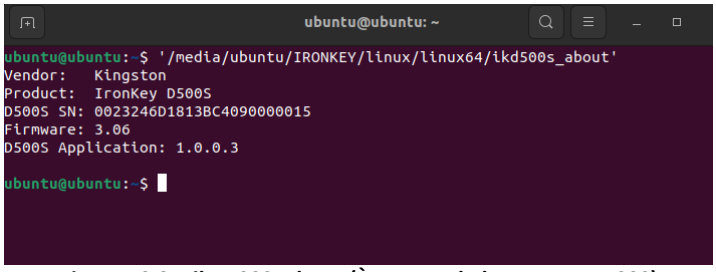
Lorsque la D500S est connectée à votre ordinateur et reconnue par le système d'exploitation, changez de répertoire pour passer au lecteur D500S en tapant la commande à l'invite du terminal. (*Figure 10.1*) **Remarque :** Les captures d'écran et les instructions de cette section utilisent le dossier linux64 (signifiant 64 bits) pour démontrer l'utilisation de la clé USB D500S dans le système d'exploitation Linux. Si vous utilisez la version 32 bits de Linux, il vous suffit de naviguer vers le dossier 32 bits correspondant et de l'utiliser à la place du dossier 64 bits (par exemple, linux32 au lieu de linux64).	 **Figure 10.1- Navigation par ligne de commande**
Utilisez la commande **ls** (liste) à l'invite actuelle et appuyez sur ENTRÉE. Vous obtiendrez une liste de fichiers et/ou de dossiers dans le dossier linux64. Vous verrez alors les quatre commandes Linux IronKey répertoriées (*Figure 10.2*) • ikD500S_about • ikD500S_login • ikD500S_logout • ikD500S_resetdevice	 **Figure 10.2- Affichage des fichiers de commande Linux IronKey**

Remarque : Les commandes et les noms des répertoires (dossiers) sont sensibles à la casse. Donc « linux64 » N'EST PAS le même répertoire que « Linux64 ». La syntaxe doit aussi être exactement reproduite. Certaines distributions Linux peuvent exiger la saisie du nom d'utilisateur pour exécuter des commandes, c'est-à-dire « ubuntu » dans cet exemple.

Initialisation de la clé USB (environnement Linux)

Utilisation des commandes de la D500S

À propos de la D500S

IkD500S_about (À propos de la D500S, *Figure 10.3*) Cette commande permet d'obtenir des informations sur la D500S, comme par exemple : • Fabricant • Produit • Numéro de série de la D500S • Version du firmware • Version du logiciel	 **Figure 10.3 – ikD500S_about (À propos de la IronKey D500S)**

Connexion à la D500S

ikD500S_login

Une fois que la D500S a été initialisée sur un système Windows ou macOS pris en charge, vous pouvez accéder à la partition de données sécurisée en vous connectant à l'appareil à l'aide du mot de passe D500S que vous avez créé.

Pour ce faire, suivez les étapes suivantes :

1. Ouvrez une fenêtre d'application « Terminal ».

2. Saisissez la commande suivante à l'invite du terminal : **cd /media/ubuntu/IRONKEY/linux/linux64**

3. L'invite de commande étant maintenant sur **/media/ubuntu/IRONKEY/linux/linux64$**, type the following command to log in to the device: **./ikD500S_login*** puis appuyez sur ENTRÉE. (Remarque : Les commandes et les noms de de dossier sont sensibles à la casse, et la syntaxe doit être rigoureusement respectée. Certaines distributions Linux peuvent exiger la saisie de votre nom d'utilisateur, c'est-à-dire « ubuntu » dans cet exemple).

4. Après une connexion réussie, le lecteur de données sécurisé s'ouvrira sur votre bureau et vous pourrez utiliser la D500S (vous trouverez plus d'informations sur le comportement de connexion à la page suivante).

*Remarque : Certaines versions de Linux nécessitent des privilèges de super utilisateur (ou utilisateur racine) pour exécuter correctement les commandes de la D500S dans la fenêtre de l'application du terminal.

Initialisation de la clé USB (environnement Linux)

Connexion à la D500S (suite)

IkD500S_login (Déverrouillage de la D500S, *Figure 10.4*)

Selon la façon dont votre clé USB a été configurée, il se peut que, lors de la procédure de connexion, plusieurs options vous soient proposées pour la déverrouiller.

Si les profils de mot de passe **Admin/Utilisateur** ont été activés lors de l'initialisation, les options de connexion suivantes vous sont proposées :

1.) Choisissez de vous connecter en tant qu'Admin ou Utilisateur
2.) Choisissez de déverrouiller les partitions Admin ou Utilisateur (si elles sont activées).
3.) Saisissez le mot de passe de connexion Admin ou Utilisateur pour l'authentification et le déverrouillage de la clé USB.

Remarque : Si les profils de mot de passe Admin/Utilisateur N'ONT PAS été activés lors de l'initialisation (mode Utilisateur seulement), vous serez uniquement invité à saisir le mot de passe de votre clé USB pour son authentification.

Important : Comme indiqué précédemment, les phrases de passe ne sont pas prises en charge sous Linux ; la D500S devra être configurée avec un mot de passe Complexe pour la connexion Linux (*Figure 10.5*)

Figure 10.4 – ikD500S_login (Déverrouillage de la D500S)

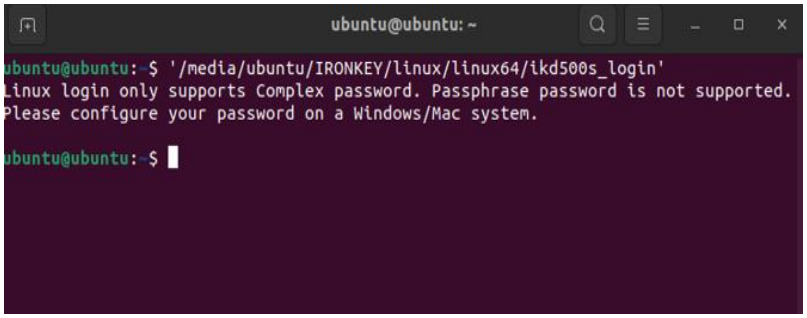


Figure 10.5- Tentative de connexion avec une phrase de passe non prise en charge.

Initialisation de la clé USB (environnement Linux)

Connexion à la D500S (suite)

Comportement en cas de saisie d'un mot de passe de connexion incorrect

Au cours de la procédure de connexion, si un mot de passe incorrect est saisi, vous aurez à nouveau la possibilité de saisir le mot de passe. Toutefois, il existe une fonctionnalité de sécurité intégrée qui comptabilise le nombre de tentatives de connexion infructueuses. Si ce nombre atteint la valeur préconfigurée de 10 tentatives infructueuses pour les connexions Admin ou Utilisateur, le comportement sera le suivant :

Mots de passe Admin/Utilisateur activés

- **Connexion Utilisateur :** Verrouillage de l'Utilisateur, connexion en tant qu'Admin requise. (*Figure 10.6*) Remarque : Le mot de passe Utilisateur peut être réinitialisé par la connexion Admin sur un système Windows ou macOS pris en charge.
- **Connexion Admin :** Effacement chiffré de la clé USB, toutes les données sont perdues à jamais. Réinitialisation de la clé USB nécessaire. (*Figure 10.7*)

Mode Utilisateur seulement (Admin/Utilisateur non activé)

- **Connexion Utilisateur :** Effacement chiffré de la clé USB, toutes les données sont perdues à jamais. Réinitialisation de la clé USB nécessaire. (*Figure 10.7*)

Figure 10.6- Verrouillage de la connexion Utilisateur, Mots de passe Admin/Utilisateur activés

Figure 10.7- Nombre maximal de tentatives atteint (réinitialisation de la clé USB).

Déconnexion de la D500S

IkD500S_logout (verrouiller la clé USB)

Lorsque vous avez fini d'utiliser la D500S, déconnectez-vous de la clé USB et sécurisez vos données. Pour ce faire, suivez les mêmes étapes que celles mentionnées à la page 39 et utilisez la commande suivante pour vous déconnecter correctement de la clé USB : **./ikD500S_logout**, puis appuyez sur la touche ENTRÉE (Remarque : Les commandes et les noms de répertoires sont sensibles aux majuscules et aux minuscules et la syntaxe doit être rigoureusement respectée.) (*Figure 10.8*)

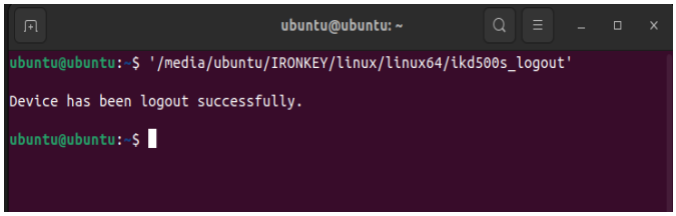


Figure 10.8- Déconnexion de la D500S

Initialisation de la clé USB (environnement Linux)

Réinitialisation de la D500S

ikD500S_resetdevice
Comme indiqué précédemment à la page 41, en cas d'oubli des mots de passe Utilisateur/Admin, la commande Reset Device (Réinitialiser l'appareil) peut être utilisée pour réinitialiser la clé USB afin qu'elle puisse être utilisée à nouveau. Ce processus vous permettra de créer un nouveau mot de passe. Mais afin de protéger la confidentialité de vos données, la D500S effacera son contenu par chiffrement pour formater la partition de données sécurisées. **Cela signifie que toutes vos données seront perdues.**

Pour utiliser la commande Reset Device (Réinitialiser l'appareil), suivez les mêmes étapes que celles indiquées à la page 39 et utilisez la commande suivante pour vous déconnecter correctement de la clé USB : **./ikD500S_resetdevice** et appuyez sur la touche ENTRÉE (Remarque : Les commandes et les noms de répertoires sont sensibles aux majuscules et aux minuscules et la syntaxe doit être rigoureusement respectée.) (*Figure 10.9*)

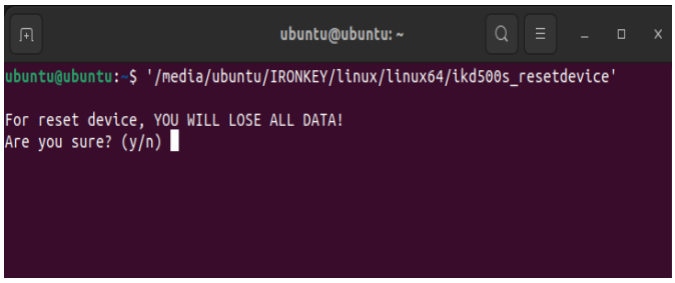


Figure 10.9- Commande Reset Device (Réinitialiser l'appareil)

Une fois la commande Reset Device (Réinitialiser l'appareil) utilisée, vous serez invité à créer un nouveau mot de passe complexe qui doit contenir :

- 8 à 16 caractères et au moins (3) des critères suivants :

  - **MAJUSCULE**
  - **Minuscule**
  - **Numérique**
  - **Caractères spéciaux (!,$,etc.)**

(*Figure 10.10*)

Remarque : La commande Reset Device (Réinitialiser l'appareil) initialise la clé USB en mode Utilisateur uniquement (un seul mot de passe, un seul utilisateur). Pour activer les profils de mot de passe de connexion Admin/Utilisateur, la D500S doit être configurée sur un système Windows ou macOS pris en charge pour accéder à cette option.

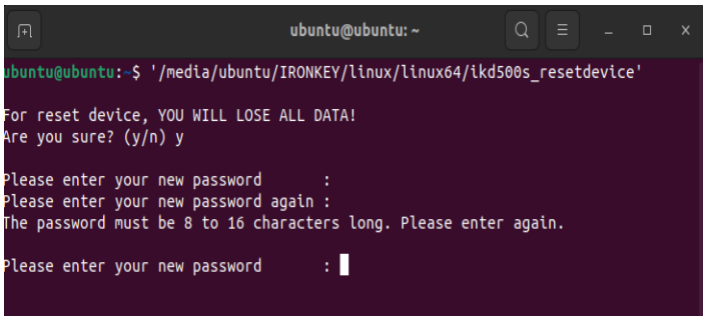


Figure 10.10- Commande Reset Device (Réinitialiser l'appareil), création du mot de passe

IRONKEY™ D500S
DRIVE FLASH USB 3.2 Gen 1 SICURO

Guida per l'utente

Contenuti

Figura 1 – IronKey D500S

Introduzione

Il drive Kingston IronKey D500S è un drive USB di classe militare basato sulle funzionalità che hanno reso il marchio IronKey uno dei più rispettati nella protezione delle informazioni sensibili. Il drive è dotato di certificazione FIPS 140-3 di Livello 3 (in fase di approvazione), che include nuovi miglioramenti alle funzionalità di sicurezza, implementati da NIST. Tali miglioramenti richiedono un upgrade dei processori, per una maggiore sicurezza. La crittografia e la decodifica dei dati sul drive D500S, viene effettuata senza lasciare alcuna traccia nel sistema host, rendendo il sistema immune ai password sniffer in memoria. Unitamente alla crittografia hardware XTS-AES 256-bit, il drive include anche un guscio esterno in zinco rinforzato che è impermeabile*, resistente alla polvere*, resistente agli schiacciamenti, e sigillato con una resina epossidica, per proteggere i componenti interni contro i tentativi di penetrazione.

La gammaD500S supporta le funzionalità multi password (amministratore, utente, password ripristino monouso e cancellazione crittografica), con modalità password complessa o frase password**. 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 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 128 caratteri. L'amministratore può abilitare l'accesso Utente; creare doppie partizioni dati personalizzate per separare i file Amministratore/Utente, abilitare una password di ripristino monouso, una password di cancellazione crittografica, ed effettuare il reset della password utente per ripristinare l'accesso ai dati.

Per inserire la password più facilmente, è possibile abilitare il simbolo dell'occhio , in modo da visualizzare la password digitata, riducendo gli errori di battitura che portano a tentativi di accesso non riusciti. E per una maggiore tranquillità, il drive D500S utilizza un firmware con firma digitale, che lo rende immune agli attacchi BadUSB, malware, e Brute Force finalizzati al tentativo di indovinare la password. 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 all'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***.

Le aziende di piccole e medie dimensioni possono utilizzare la funzione di amministratore per gestire su base locale i drive. Per esempio, è possibile utilizzare la modalità 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 D500S offre numerose opzioni di personalizzazione, è conforme agli standard TAA/CMMC, ed è assemblato negli Stati Uniti.

Il drive D500S è supportato da una garanzia limitata di 5 anni, con servizio di supporto tecnico Kingston gratuito.

* Fare riferimento alle specifiche della scheda tecnica. Il prodotto deve essere pulito e asciutto prima dell'uso.
** Modalità frase password non supportata sui sistemi Linux.
*** Tastiera virtuale: Supporta esclusivamente la lingua inglese statunitense su piattaforme Microsoft Windows e MacOS.

IronKey D500S – Funzionalità

- Certificazione FIPS 140 -3 di Livello 3 (in fase di approvazione) con crittografia hardware XTS-AES a 256-bit (con funzione crittografica non disattivabile)
- Protezione contro gli attacchi brute force e BadUSB
- Funzione multi password opzionale
- Modalità con password complessa o frase password
- Esclusiva opzione per doppia partizione e password di cancellazione crittografica
- Pulsante di attivazione icona "occhio", per visualizzare le password inserite e minimizzare il rischio di inserimento di password errate
- Tastiera virtuale, che offre protezione contro keylogger e screenlogger
- Modalità forzata/sessione in 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 la funzione Amministratore.
- Compatibile con sistemi operativi Windows, macOS e Linux (consultare la scheda tecnica per ulteriori dettagli)

Informazioni sul manuale

Questo manuale utente contiene le istruzioni per l'uso del drive IronKey D500S; tali istruzioni sono riferite all'unità in configurazione standard di fabbrica e pertanto priva di qualunque tipo di personalizzazione.

Requisiti di sistema

Piattaforma PC • Intel, AMD & Apple M1 SOC • 15 MB di spazio libero su disco • Porta USB 2.0 – 3.2 disponibile • Due lettere di unità libere consecutive dopo quella associata all'ultimo drive fisico presente sull'unità* ***Nota:** Vedere sezione "Conflitti con le lettere di unità", a pagina 35.	**Sistemi operativi per PC supportati** • Windows 11 • Windows 10
Piattaforma Mac • 15 MB di spazio libero su disco • Porta USB 2.0 – 3.2	**Supporto per sistema operativo Mac** • macOS macOS 11.x - 14.x
Piattaforma Linux • 5 MB di spazio libero su disco • Porta USB 2.0 – 3.2	**Supporto per sistema operativo Linux** • Linux Kernel v4.4+

Raccomandazioni

Per garantire una potenza adeguata al funzionamento del drive D500S, collegarlo direttamente a una porta USB sul computer notebook o desktop, come illustrato in ***Figura 1.1***. Evitare di collegare il drive D500S 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 D500S viene fornito preformattato con il file system FAT32. Il drive è compatibile con i sistemi Windows, macOS e Linux*. Tuttavia, vi potrebbero essere alcune altre opzioni che possono essere utilizzate per formattare il drive manualmente, come lo standard NTFS per Windows oppure exFAT. È possibile riformattare la partizione dati, se necessario; tuttavia, in questo caso tutti i dati andranno persi durante la formattazione del drive.

Note di utilizzo

Per tenere i dati al sicuro, Kingston raccomanda quanto segue:

- Eseguire una scansione antivirus sul computer prima di impostare utilizzare il drive D500S sul sistema di destinazione
- Quando si utilizza il drive su un sistema di tipo pubblico o non conosciuto, potrebbe essere necessario impostare la modalità di sola lettura sul dispositivo al fine di proteggere il drive contro eventuali attacchi malware
- Bloccare il dispositivo quando non 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

Scoprite le informazioni e gli aggiornamenti più recenti

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

NOTA: Il drive deve essere aggiornato esclusivamente con gli aggiornamenti più recenti (se disponibili). Il downgrade del drive a una versione software precedente non è supportato. Tale operazione può causare potenziali perdite di dati o influenzare negativamente altre funzioni del drive. Per eventuali dubbi o problemi, contattare il supporto tecnico Kingston.

*** Il drive D500S non supporta l'inizializzazione out-of-box su sistemi Linux, e deve essere inizializzato e configurato completamente su sistemi Windows o MacOS prima di poter essere utilizzato su Linux. Informazioni aggiuntive possono essere reperite nella sezione Linux, a pagina 37 di questa guida utente**

Prassi raccomandate per l'impostazione della password

Il drive D500S è dotato di solide contromisure di sicurezza. Ciò include la protezione contro gli attacchi brute force, che impediscono agli aggressori di scoprire le password limitando i tentativi di inserimento password a10 tentativi. Una volta raggiunto il limite di tentativi di inserimento password sul drive, D500S effettuerà la cancellazione automatica di tutti i dati crittografati per poi effettuare la formattazione alle impostazioni di fabbrica.

Supporto per password multiple
D500S supporta la funzione multi password, una caratteristica chiave per la protezione contro la perdita di dati in caso di smarrimento di una o più password . Quando tutte le opzioni di inserimento password sono abilitate il drive D500S 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.

Il drive D500S consente l'impostazione di due password principali; una password Amministratore (chiamata "Password Admin"), e una password Utente. L'account amministratore (Admin) può accedere al drive in qualunque momento e impostare le opzioni per gli account Utente e Amministratore, come se fosse un Super User. Inoltre, l'amministratore con account Amministratore può impostare una password di ripristino monouso per l'utente, al fine di garantire a quest'ultimo la possibilità di accedere ed effettuare il reset la password utente.

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

Se si dimenticano o si perdono entrambe le password, non sarà possibile accedere ai dati in alcun modo. Kingston non sarà in grado di recuperare i dati in quanto le funzioni di sicurezza non consentono alcun accesso secondario. Pertanto, Kingston raccomanda di salvare i dati anche su altri supporti. Il drive D500S può essere sottoposto a un reset; ma in tal caso, tutti i dati in esso contenuti saranno eliminati definitivamente.

Modalità password
Il drive D500S supporta inoltre due modalità password differenti:

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

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

Frase-password
Il drive D500S le frasi password composte da 10 fino a 128 caratteri. Una frase password non segue alcuna regola, ma se utilizzata correttamente può fornire password caratterizzate da un elevato livello di protezione.

Una frase password è fondamentalmente composta da qualunque combinazione di caratteri inclusi caratteri provenienti da altre lingue. Come nel caso del drive D500S, la lingua utilizzata per la password può essere anche corrispondente alla lingua selezionata per il drive. Ciò consente di selezionare parole multiple, una frase, il testo di una canzone, la strofa di una poesia, ecc. Una buona frase password è difficile da indovinare per gli hacker e facile da ricordare per gli utenti.

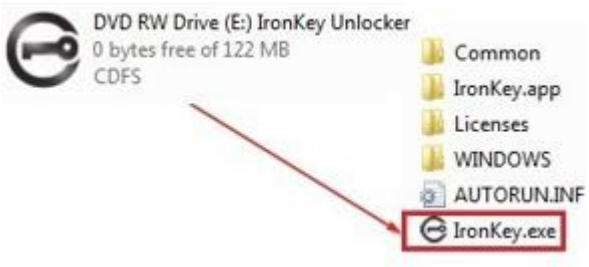
Configurazione del dispositivo

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

Accesso al dispositivo (Ambienti Windows)

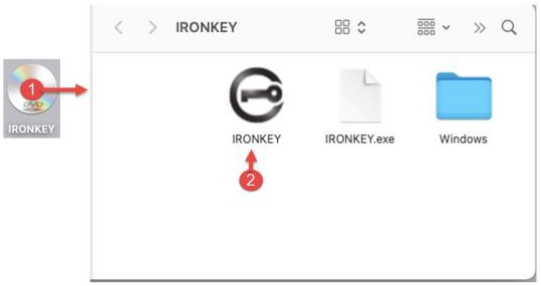
Collegare il drive USB crittografato IronKey in una delle porte USB disponibili sul notebook o sul PC desktop e attendere che Windows rilevi il dispositivo.

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

• Una volta completato il rilevamento del nuovo hardware, selezionare l'opzione **IronKey.exe**, all'interno della partizione Unlocker presente su Esplora risorse.. (*Figura 3.2*) • Si noti che la lettera di partizione varia, assumendo la denominazione della prima lettera di unità libera. La lettera di unità può variare in base al tipo di dispositivo connesso. Nell'immagine sottostante, la lettera dell'unità è (E:)	 **Figura 3.2 – Schermata "Esplora risorse"/IronKey.exe**

Accesso al dispositivo (Ambienti macOS)

Inserire il drive D500S in una delle porte USB disponibili sul computer notebook o desktop in uso e attendere il rilevamento da parte del sistema operativo Mac. Una volta che il drive viene rilevato, sul desktop verrà visualizzata l'icona del volume "IRONKEY". (*Figura 3.3*)

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

Inizializzazione del dispositivo (ambienti Windows e macOS)

Lingua e EULA

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

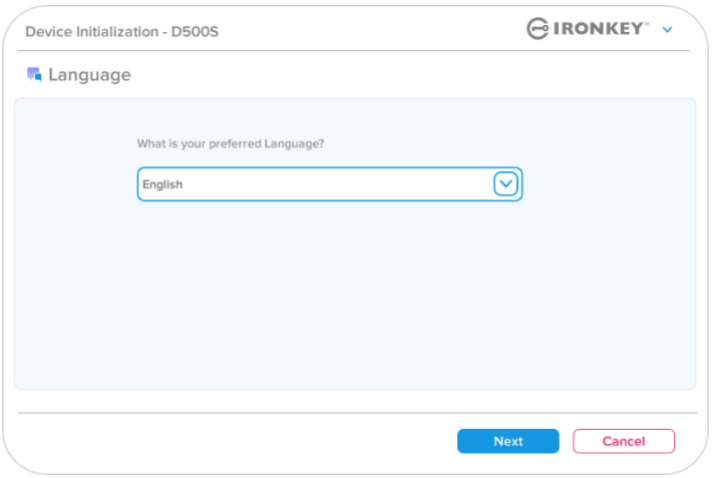


Figura 4.1 – Selezione della lingua

Leggere l’accordo di licenza e quindi fare clic su **“Next” (Successivo)**.

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

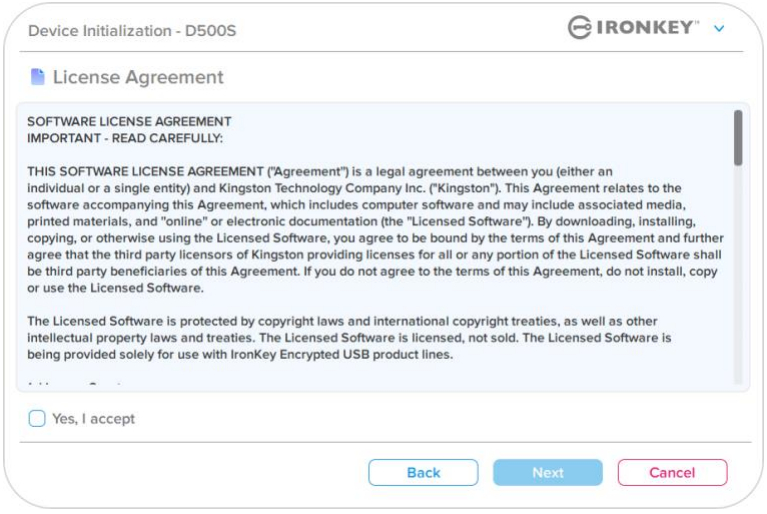


Figura 4.2 – Accordo di licenza

Inizializzazione del dispositivo

Selezione della password

Sulla schermata di selezione password, è possibile creare una password a protezione dei dati dell'unità D500S. La password utilizzata può essere di o complesso,oppure una frase password (*Figure 4.3 – 4.4*). Inoltre, da questa schermata è anche possibile utilizzare le opzioni multi password Amministratore/Utente. Prima di procedere con la selezione della password, consultare nuovamente la sezione abilitazione Password Amministratore/Utente sotto, per familiarizzare con queste funzionalità.

Nota: Una volta selezionata la modalità password complessa o frase password, tale modalità non può essere modificata a meno che il dispositivo non venga resettato.

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

Password complessa

- Le password devono essere composte da un minimo di 8 fino a un massimo di 16 caratteri.
- Le password devono includere tre (3) dei seguenti criteri:
  - Lettere maiuscole
  - Lettere minuscole
  - Numeri
  - Generati Caratteri speciali (!,$,&, ecc.)

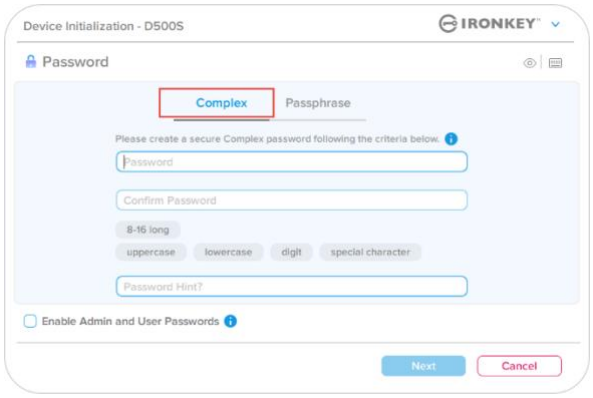


Figura 4.3 – Password complesse

Frasi password

- Deve contenere:
  - Minimo 10 caratteri
  - Massimo 128 caratteri

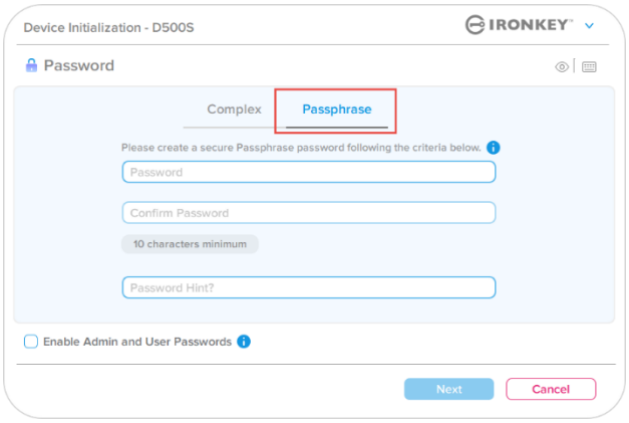


Figura 4.4 – Frase-password

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.

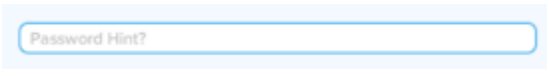


Figura 4.5 – Campo suggerimento password

Inizializzazione del dispositivo

Password valide e non valide

Nel caso delle password **valide**, il campo dei criteri password si illumina di colore **verde** quando vengono rispettati i criteri di inserimento corretti. (vedere *figure 4.6a-b*)
Nota: Quando vengono soddisfatti almeno tre criteri minimi per la password, la casella associata al quarto criterio diventa di colore grigio, a indicare che tale criterio è opzionale (*Figura 4.6b*)

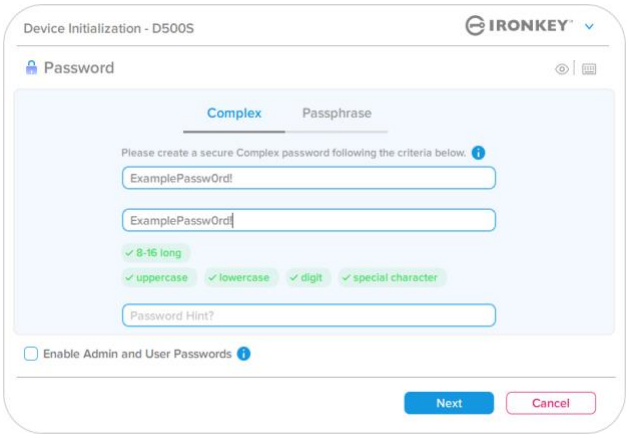


Figura 4.6a – Requisiti di inserimento della password complessa rispettati

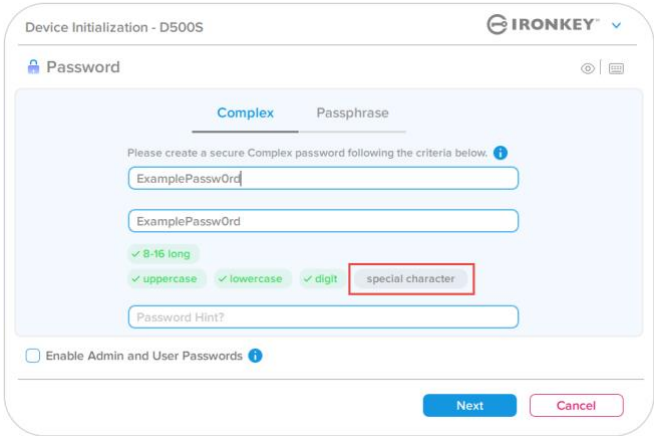


Figura 4.6b – Requisiti condizionali opzionali della password complessa

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

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

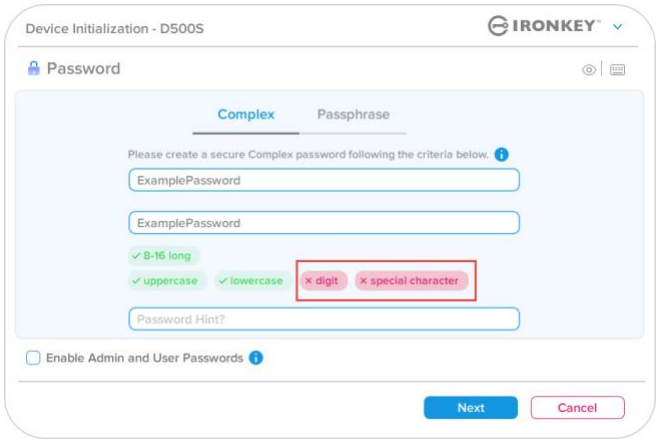


Figura 4.7 – Condizioni di inserimento password non rispettate

Inizializzazione del dispositivo

Tastiera virtuale

Il drive D500S integra una tastiera virtuale che può essere utilizzata per la protezione contro attacchi keylogger.

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

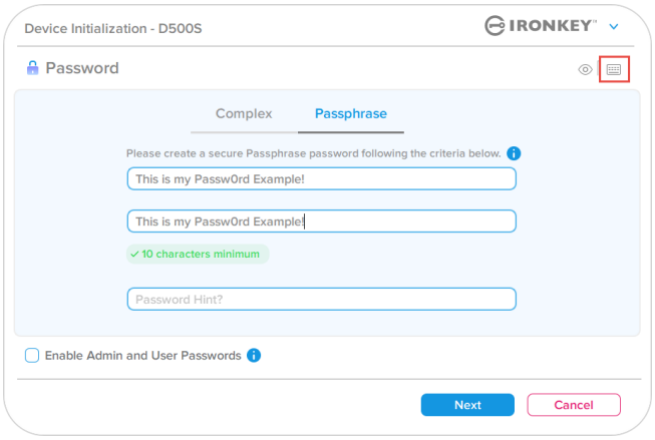


Figura 4.8 – Attivazione della tastiera virtuale

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

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

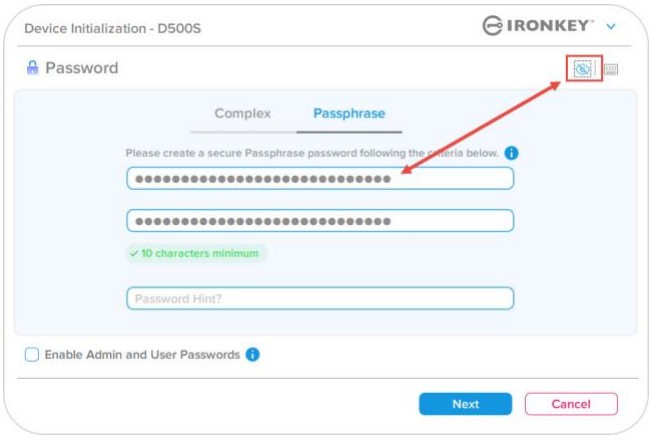
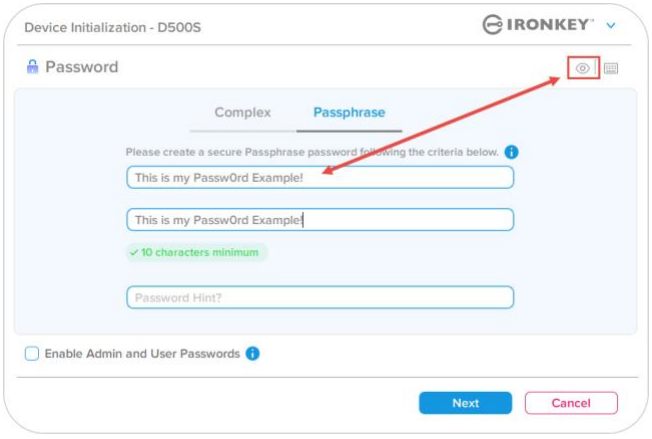
Figura 4.9 – Protezione contro screenlogger / funzione di layout casuale tastiera

Inizializzazione del dispositivo

Pulsante di commutazione visualizzazione password

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

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

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

Inizializzazione del dispositivo

Password amministratore e utente

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

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

- Configurazione con doppia partizione
- Password di ripristino monouso
- Funzione "Forza sola lettura" per login utente
- Reset della password utente
- Reset password forzato per l'accesso utente
- Password di cancellazione crittografica

Per ulteriori informazioni su queste funzionalità, andare a pagina 25 della guida utente.

- Per utilizzare la funzione **"Abilita le password amministratore e utente",** fare clic sulla casella posta accanto all'opzione **"Abilita password amministratore e utente"** e selezionare il pulsante **"Successivo"**, dopo aver selezionato una password valida. (Figura 4.12)

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

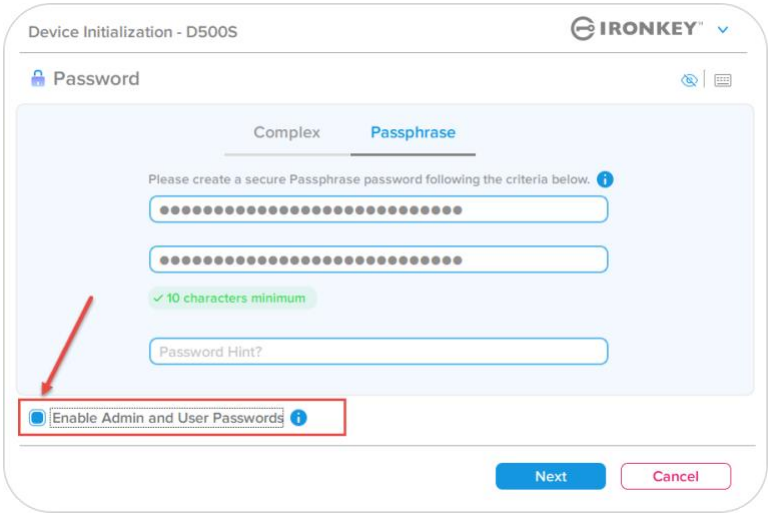


Figura 4.12 – Abilitazione delle password amministratore e utente

Nota: L'abilitazione delle 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" e "Password singola" tenere la funzione **"Abilita le password amministratore e utente"** deselezionata e fare clic su **"Successivo"**, dopo aver creato una password valida.

Nota: 'nella restante sezione di questa guida, la funzione **password Amministratore e password Utente** sarà denominata **"Regola amministratore"**.

Inizializzazione del dispositivo

Password amministratore e utente

- Se la Regola Amministratore è stata **abilitata** nella schermata precedente, sarà visualizzata la schermata successiva associata alla "Password utente" (*Figura 4.13*). La **password Utente** sarà dotata di funzionalità limitate rispetto a quella Amministratore. Tali funzionalità saranno discusse in dettaglio nelle sezioni successive di questa guida utente (vedere pagina 23)

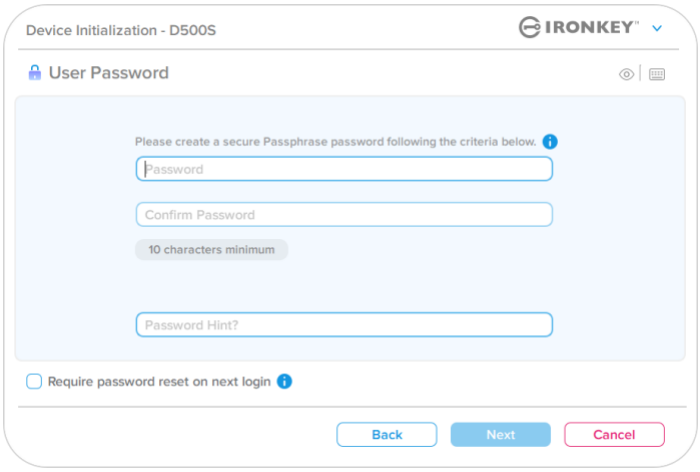


Figura 4.13 – Password Utente (Funzioni "Amministratore" e "Utente abilitate)

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

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

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

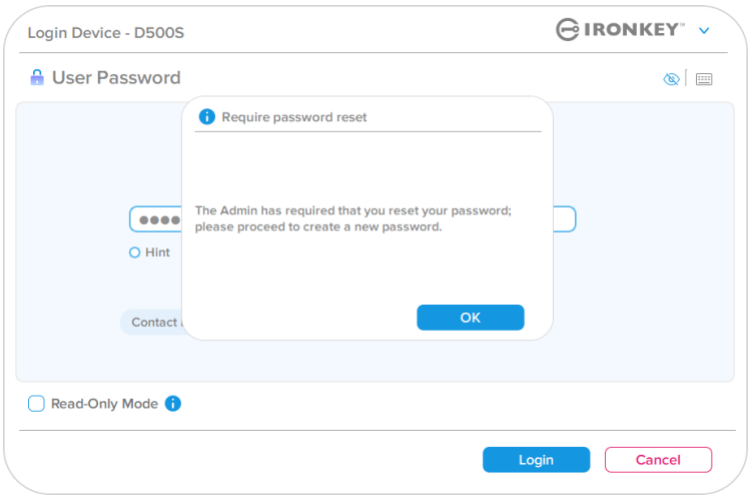


Figura 4.14 – Richiedi il reset password al prossimo accesso (per password utente)

Inizializzazione del dispositivo

Doppie partizioni

Il drive IronKey D500S consente di creare due partizioni personalizzate separate per Amministratore e Utente. Quando questa funzionalità è attiva, l'account Amministratore sarà in grado di accedere a **entrambe** le partizioni Amministratore e Utente, mentre l'account Utente avrà accesso **solamente** alla partizione Utente. Questa funzionalità è particolarmente utile per la segregazione separata dei privilegi di accesso a dati e file per Amministratore e Utente. Oppure, può essere utilizzata per abilitare un'area di storage nascosta finalizzata a prevenire l'esposizione di file sensibili e al momento non necessari su sistemi non affidabili. Le dimensioni delle partizioni Amministratore e Utente possono essere regolate in base alle esigenze specifiche, se necessario.
The IronKey D500S allows you to cre

NOTA: Questa funzionalità è *opzionale* e può essere disabilitata lasciando la casella "Abilita doppia partizione" deselezionata durante la configurazione (*Figura 4.15*)

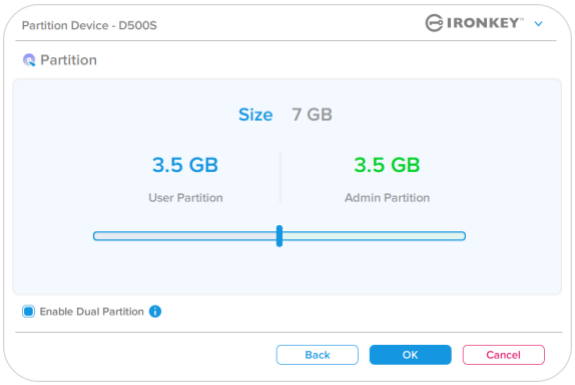


Figura 4.15 – Partizionamento del dispositivo

Per dimensionare e allocare le partizioni tra utenti e amministratori, spostare la barra scorrevole verso sinistra o destra, rispettivamente (*Figura 4.16*).

- Le partizioni possono essere regolate con incrementi di 0,5 GB alla volta.
- Il dimensionamento delle partizioni è basato sulla capacità totale dello storage disponibile sulla partizione nascosta.
- Per impostazione di default, il selettore scorrevole della doppia partizione viene impostato in modo tale da suddividere la partizione in parti uguali tra Amministratore e Utente, fino a quando le dimensioni non vengono reimpostate manualmente.
- La dimensione più piccola selezionabile per la partizione è pari a 1 GB.

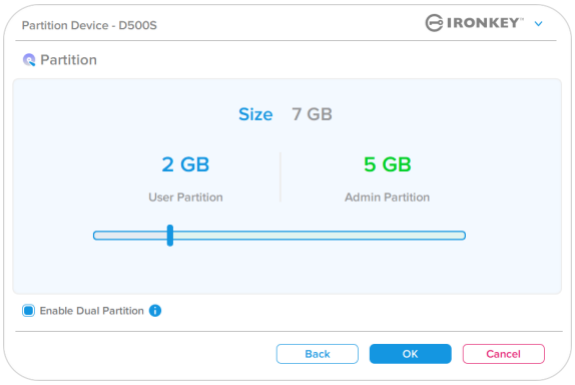


Figura 4.16 – Partizionamento del dispositivo, selettore scorrevole impostato

Accesso amministratore

Una volta che il drive è stato completamente configurato con le due partizioni abilitate, l'Accesso amministratore potrà utilizzare un'opzione che consente di sbloccare il drive per accedere alla partizione Amministratore O alla partizione Utente con ciascun accesso successivo. (*Figura 4.17*)

NOTA: È possibile aprire una sola partizione alla volta. Le partizioni Utente e Amministratore non possono essere bloccate allo stesso tempo.

L'accesso Utente non dispone di questa opzione e ed effettua il solo blocco automatico della partizione utente.

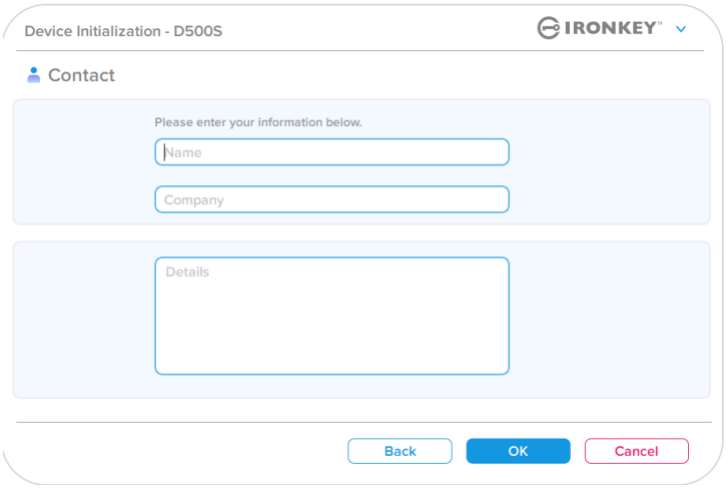
Figura 4.17 – Esempio di selezione della partizione con accesso Amministratore

Inizializzazione del dispositivo

Informazioni di contatto

Inserire le informazioni di contatto nei relativi campi di testo (vedere *Figura 4.18*)

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

Il campo **"Name" (Nome)** può contenere fino a 32 caratteri, ma non può contenere la password **esatta**. Il campo **"Company" (Azienda)** può contenere fino a 32 caratteri, ma non può contenere la password **esatta**. Il campo **"Details" (Dettagli)** può contenere fino a 156 caratteri, ma non può contenere la password **esatta**.	 **Figura 4.18 – Schermata dei dati di contatto**

Nota: Facendo clic su "OK" si completerà la procedura di inizializzazione e sarà possibile procedere allo sblocco dell'unità, per poi effettuare il montaggio della partizione sicura in cui effettuare l'archiviazione sicura dei dati. Procedere a scollegare il drive per poi ricollegarlo al sistema, al fine di poter visualizzare le modifiche apportate.

Utilizzo del dispositivo (ambienti Windows e macOS)

Accesso per amministratore e utente (modalità amministratore abilitata)

Se il dispositivo viene inizializzato con la configurazione che consente di utilizzare le password Amministratore e Utente (regola Amministratore), sarà eseguita l'applicazione integrata nel drive IronKey D500S, che richiederà l'inserimento della Password Utente durante l'accesso. Da qui sarà possibile effettuare l'accesso con la Password Utente, visualizzare qualunque informazione di contatto inserita oppure effettuare l'accesso come Amministratore (*Figura 5.1*). Facendo clic sul pulsante "Login as Admin" (Accedi come amministratore) (illustrato sotto), l'applicazione mostrerà il menu di accesso amministratore, dal quale è possibile effettuare l'accesso come amministratore e accedere alle relative funzionalità e impostazioni amministratore (*Figura 5.2*).

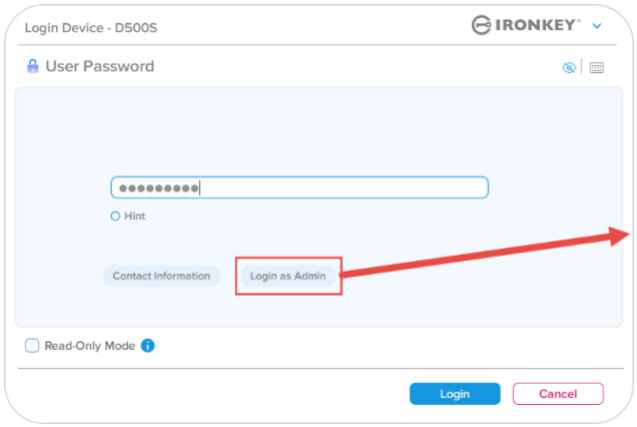


Figura 5.1 – Accesso con Password Utente (funzione amministratore abilitata)

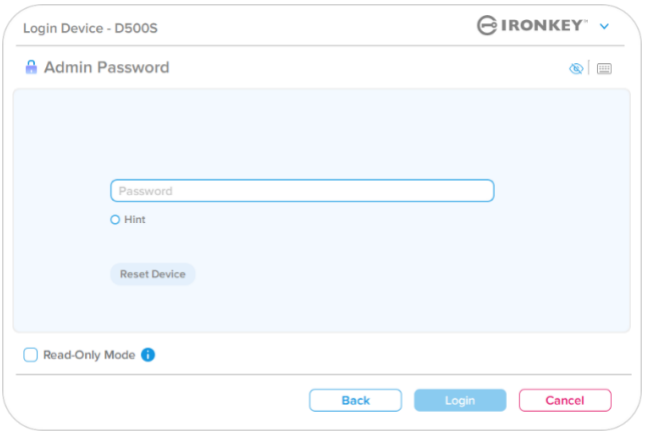


Figura 5.2 – Accesso con Password Admin

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

Come indicato in precedenza, sebbene sia consigliabile utilizzare la funzionalità "Regola amministratore" per sfruttare appieno i vantaggi del dispositivo, il drive IronKey può essere inizializzato anche in modalità "Solo utente" (password singola, utente singolo). Questa è un'opzione utilizzabile da colore che desiderano un approccio più semplice verso le password singole come strumento per mettere in sicurezza i dati del drive. (*Figura 5.3*)

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

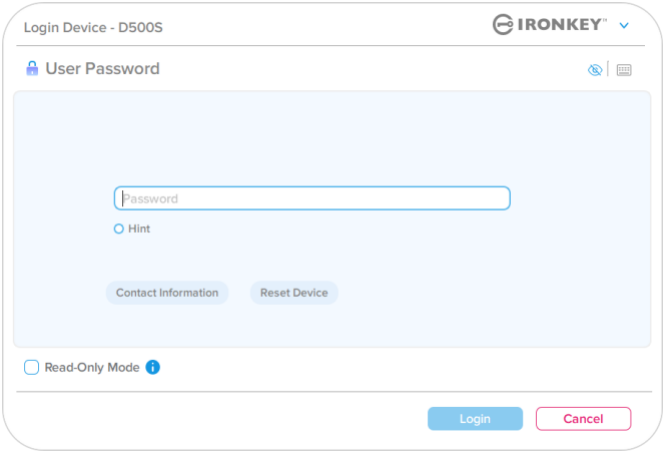


Figura 5.3 – Accesso con Password Utente (modalità amministratore non abilitata)

Utilizzo del dispositivo

Sblocco in modalità di sola lettura

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

Quando si opera in tale modalità, non è possibile effettuare alcuna operazione che implichi la modifica dei file sul dispositivo.
For example, you cannot reformat the device, restore, add or edit files on the drive.

Per sbloccare il dispositivo in modalità di sola lettura:

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

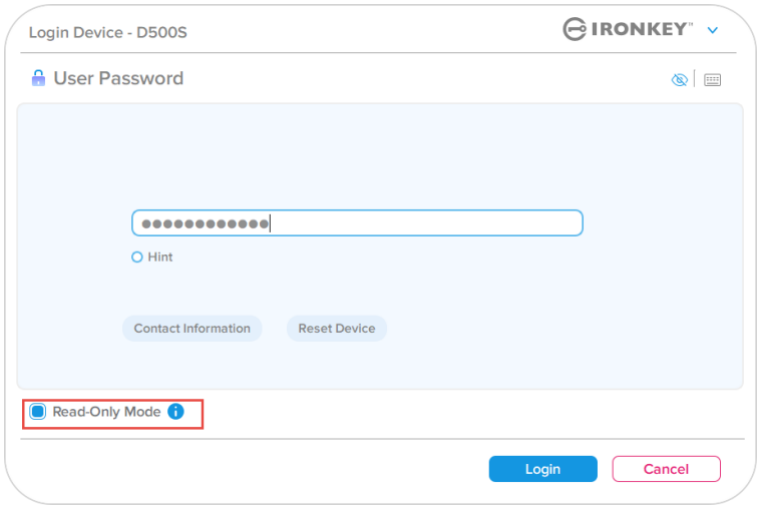


Figura 5.4 – Modalità di sola lettura

Se si desidera sbloccare l'unità ottenendo i diritti di accesso completi in lettura/scrittura alla partizione dati sicura, è necessario scollegare e disattivare il drive D500S poi effettuare nuovamente l'accesso, assicurandosi di deselezionare la casella dell'opzione "Read-Only Mode" (Modalità di sola lettura).

Nota: Le opzioni di amministrazione del drive D500S includono una modalità "Forza sola lettura" 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 31 per ulteriori dettagli).

Utilizzo del dispositivo

Protezione contro gli attacchi brute-force

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

Se il numero di tentativi falliti supera il valore preimpostato di default, pari a 10 tentativi, 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 e eliminazione definitiva di tutti i dati	**SÌ**
Password di ripristino monous	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 (Modalità Amministratore/ Utente NON abilitata)	**Protezione contro gli attacchi Brute Force Comportamento del dispositivo (10 tentativi di accesso falliti)**	**Eliminazione dati e reset dispositivo?**
Password utente	Eliminazione della partizione crittografica del drive, delle password, delle impostazioni e eliminazione definitiva di tutti i dati	**SÌ**

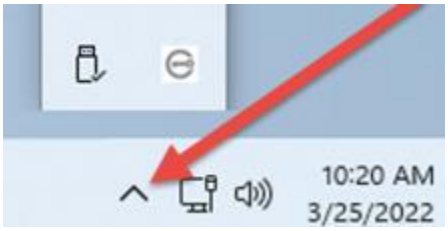
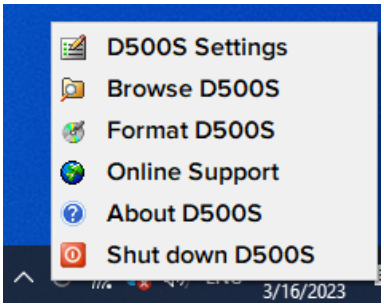
* Una volta effettuata con successo l'autenticazione sul dispositivo, il contatore dei tentativi di login falliti per il tipo di metodo utilizzato verrà azzerato. La cancellazione crittografica elimina tutte le password le chiavi crittografiche e **i dati contenuti nell'unita andranno persi per sempre.**

Accesso ai file sicuri

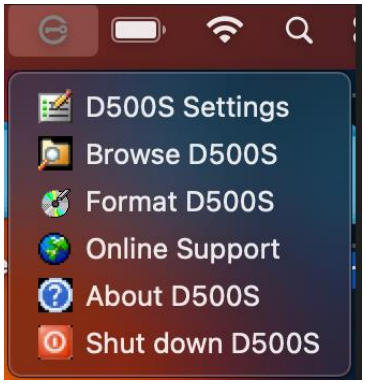
Una volta sbloccato il drive, è possibile accedere ai file sicuri. I file vengono crittografati e decrittati automaticamente quando vengono salvati o aperti sul drive. Questa tecnologia offre il vantaggio della massima trasparenza, consentendo di utilizzare i dati come se questi fossero memorizzati su un drive normale, offrendo al contempo solide funzionalità di sicurezza "always-on".
Suggerimento: È anche possibile accedere ai file facendo clic col tasto destro del mouse sull'**icona IronKey**, nella barra applicazioni di Windows, per poi selezionare **"Browse DS500S"** (Esplora D500S") (*Figura 6.2*)

Opzioni dispositivo - (Ambienti Windows)

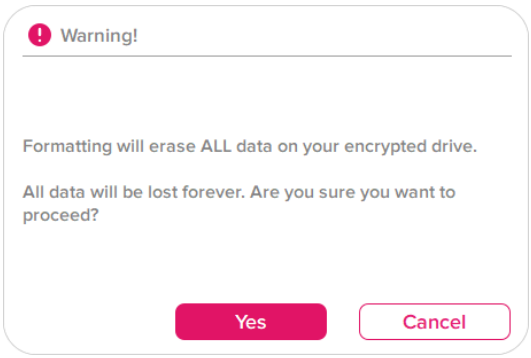
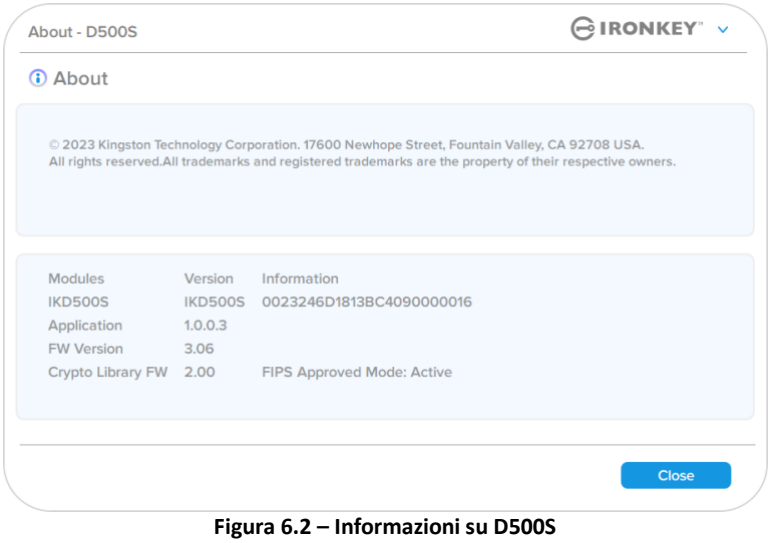
Durante l'accesso al dispositivo, sull'angolo destro della barra applicazioni di Windows sarà visualizzata l'icona del drive di IronKey. Facendo clic con il tasto destro del mouse sull'icona IronKey, sarà possibile aprire il menù di selezione che include le opzioni del drive (*Figura 6.2*).
Ulteriori dettagli su questi dispositivi possono essere reperiti alle pagine 21-25 di questo manuale.

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

Opzioni dispositivo - (Ambienti macOS)

• Quando si è connessi al dispositivo, viene visualizzata un'icona IronKey D500S posizionata sul menu macOS mostrato in Figura 6.3. Tale menu consente di accedere alle opzioni del dispositivo. Ulteriori dettagli su questi dispositivi possono essere reperiti alle pagine 19-23 di questo manuale.	 **Figura 6.3 – barra dei menu con icona/menu opzioni dispositivo macOS**

Opzioni dispositivo

Impostazioni D500S:	• Modifica password di accesso, informazioni di contatto, altre impostazioni. (Ulteriori dettagli sulle impostazioni del dispositivo possono essere reperiti nella sezione "Impostazioni D500S" di questo manuale).
Navigazione menu D500S	• Consente di visualizzare i file sicuri.
Formattazione D500S Consente di formattare la partizione dati sicura. (Attenzione: tutti i dati contenuti nell'unità verranno eliminati). (*Figura 6.1*) **Nota:** la formattazione richiede l'autenticazione mediante password.	 **Figura 6.1 – Formattazione D500S**
Supporto online:	• Questa opzione consente di aprire il link http://www.kingston.com/support, dal quale è possibile accedere a una serie di informazioni di supporto aggiuntive.
Informazioni su D500S: La sezione contiene dettagli specifici sull'unità D500S, incluse le applicazioni, il firmware e informazioni sul numero di serie (*Figura 6.2*) **Nota:** il numero di serie univoco del drive può essere visualizzato nella colonna "Informazioni".	 **Figura 6.2 – Informazioni su D500S**
Spegnimento del drive D500S:	• Questa funzione permette di arrestare correttamente l'unità DS500S, consentendo all'utente di scollegare il drive dal computer in tutta sicurezza.

Impostazioni D500S

Impostazioni amministratore

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

- **Password:** Consente di modificare la password Amministratore e/o il suggerimento (*Figura 7.1*)
- **Dati di contatto:** Consente di aggiungere/visualizzare/modificare le informazioni di contatto dell'utente (*Figura 7.2*)
- **Lingua:** Consente di modificare le impostazioni della lingua corrente (*Figura 7.3*)
- **Opzioni amministratore:** Consente di abilitare funzionalità aggiuntive come: (*Figura 7.4*)
    - Modifica della password Utente
    - Reset della password di accesso (per Password Utente)
    - Abilita la funzione "Password di ripristino monouso"
    - Attivazione di una password di cancellazione crittografica
    - Funzione di sola lettura forzata per i dati utente

NOTA: Per ulteriori dettagli iniziando sulle opzioni amministratore consultare le informazioni a pagina 26

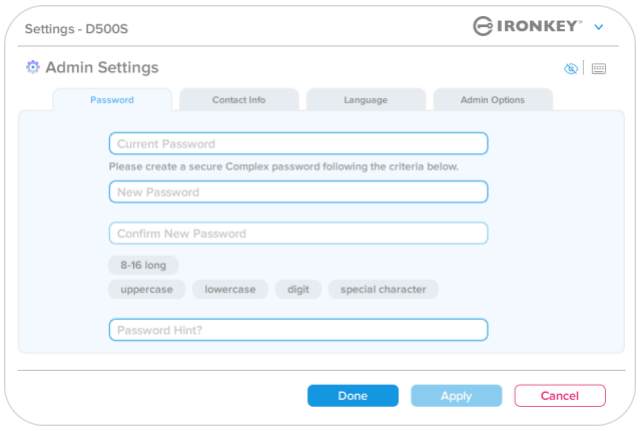


Figura 7.1– Opzioni password

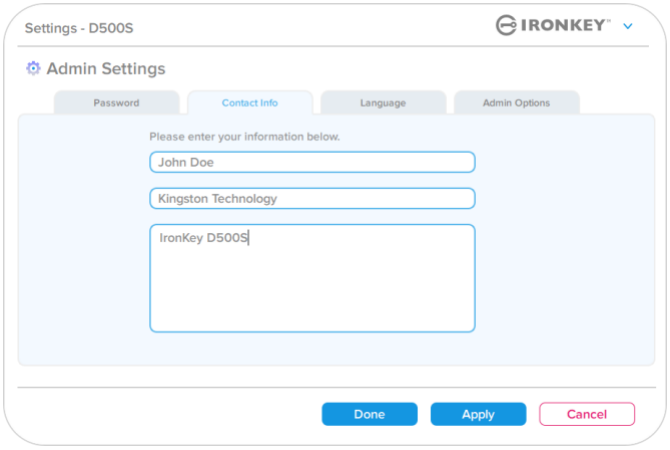


Figure 7.2 – Dati di contatto

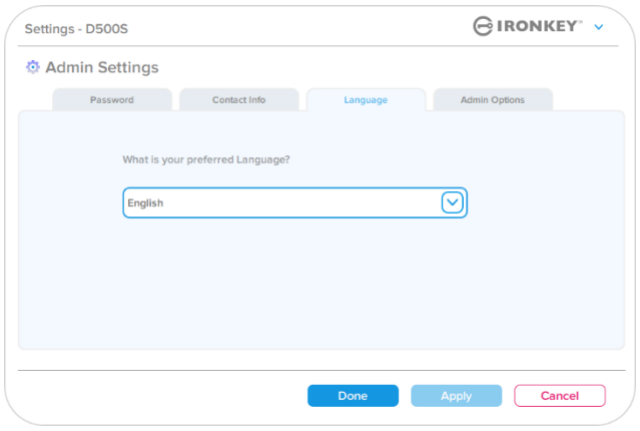


Figura 7.3 – Opzioni lingua

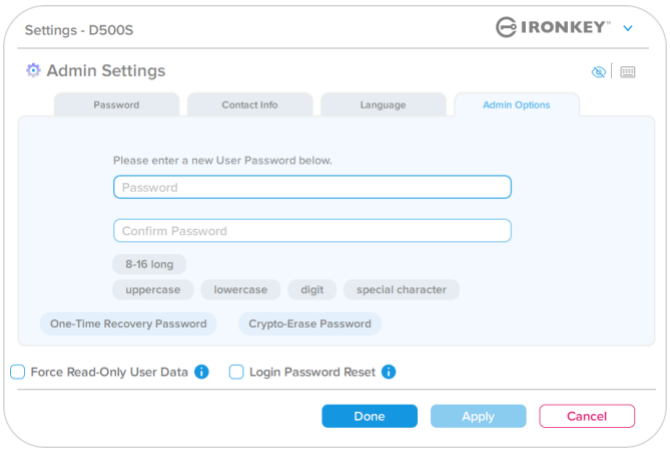
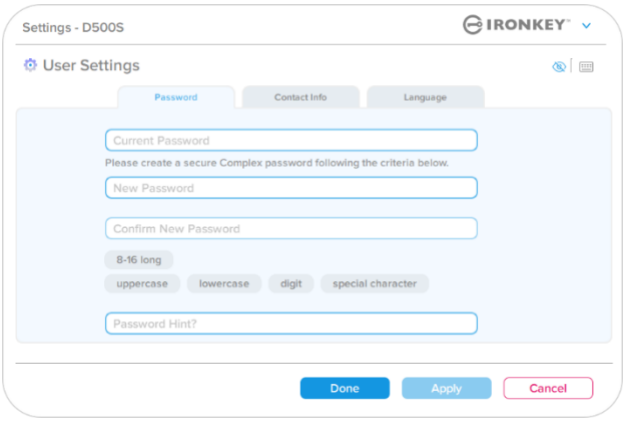
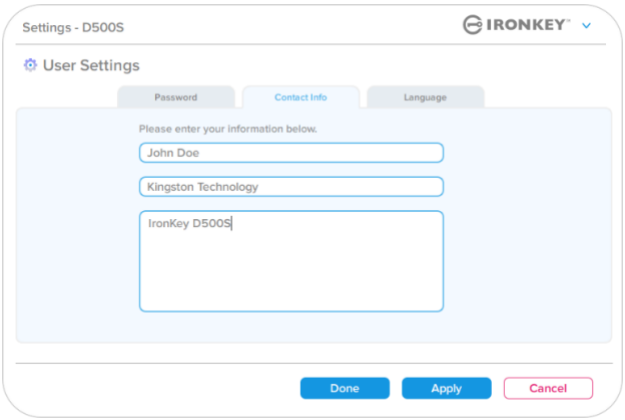
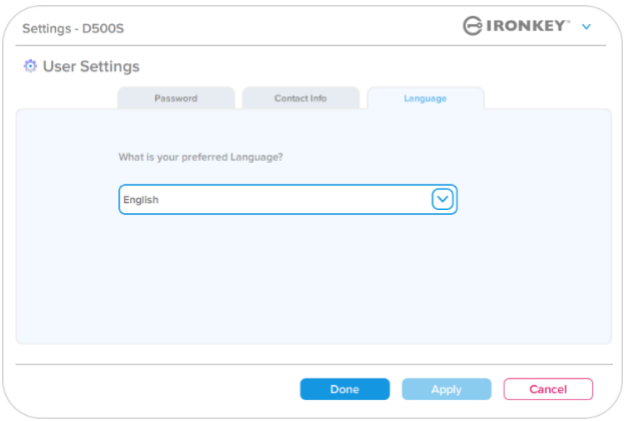


Figura 7.4 – Opzioni amministratore

Impostazioni D500S

Impostazioni utente: Modalità amministratore abilitata

L'accesso Utente limita la disponibilità delle impostazioni seguenti:

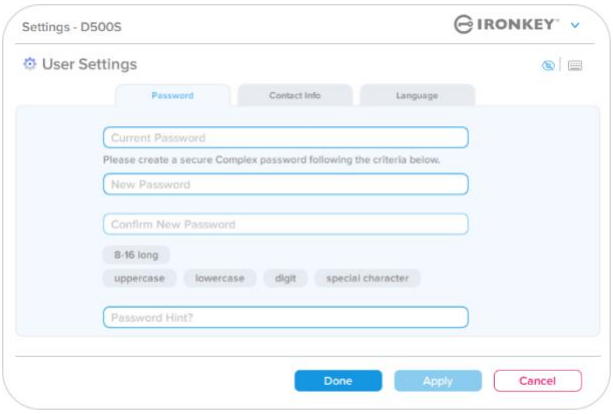
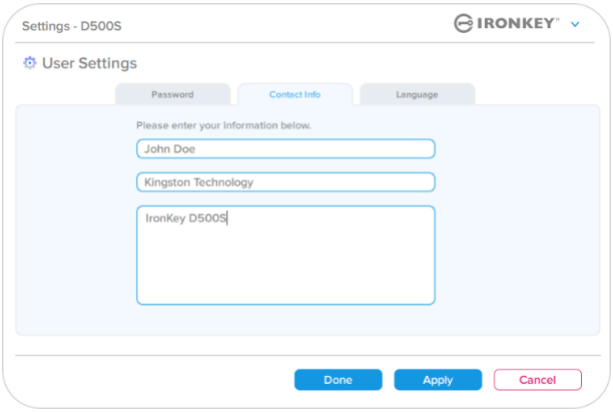
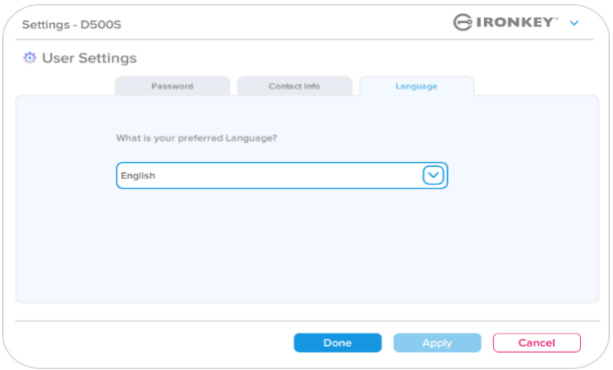
Password: Consente di modificare la password e utente e/o il suggerimento (*Figura 7.5*)	 **Figura 7.5 – Opzioni password (modalità Amministratore abilitata: accesso Utente)**
Dati di contatto: Consente di aggiungere/visualizzare/modificare le informazioni di contatto dell'utente (*Figura 7.6*)	 **Figura 7.6 – Informazioni di contatto (modalità amministratore abilitata: accesso Utente)**
Lingua: Consente di modificare le impostazioni della lingua corrente (*Figura 7.7*)	 **Figura 7.7 – Impostazioni lingua (modalità Amministratore abilitata: accesso Utente)**

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

Impostazioni D500S

Impostazioni utente: Modalità amministratore non abilitata

Come precedentemente specificato, l'avvio del drive D500S senza avere prima abilitato le password Amministratore e Utente farà sì che l'unità sia configurata in modalità **Password singola, utente singolo (Modalità solo utente)**. Questa modalità di configurazione non garantisce l'accesso ad alcuna opzione o funzionalità di amministrazione. Questa configurazione garantisce l'accesso alle seguenti impostazioni del drive D500S:

Password: Consente di modificare la password e utente e/o il suggerimento (*Figura 7.8*)	 **Figura 7.8 – Opzioni password (Modalità solo utente)**
Dati di contatto: Consente di aggiungere/visualizzare/modificare le informazioni di contatto dell'utente (*Figura 7.9*)	 **Figura 7.9 – Informazioni di contatto (Modalità solo utente)**
Lingua: Consente di modificare le impostazioni della lingua corrente (*Figura 7.10*)	 **Figura 7.10 – Impostazioni lingua (Modalità solo utente)**

Impostazioni D500S

Modifica e salvataggio delle impostazioni

- Ogni qualvolta si effettuano dei cambiamenti alle impostazioni dell'unità D500S (per esempio, modifica dei dati di contatto, modifica della lingua, cambiamenti della password e delle opzioni amministratore ecc.), il drive chiederà all'utente di inserire la password, al fine di accettare e applicare le modifiche effettuate (*Figura 7.11*).

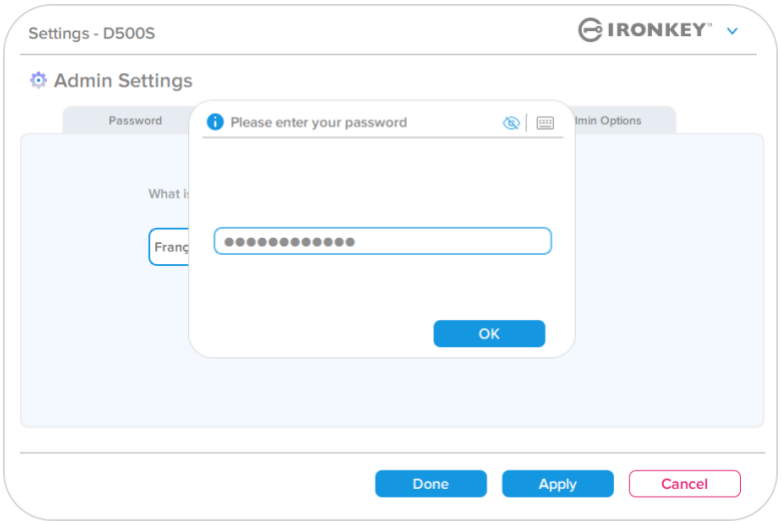


Figura 7.11 – Schermata password che richiede il salvataggio delle impostazioni per l'unità D500S

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 impostazioni del drive D500S.

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 sotto illustra tutte le funzionalità che possono essere d'aiuto durante la procedura di reset della password Utente:

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

Nota: I criteri che regolano la creazione di una password sono basati sui requisiti originali che sono stati impostati durante la fase di inizializzazione (modalità di password complessa o frase password).

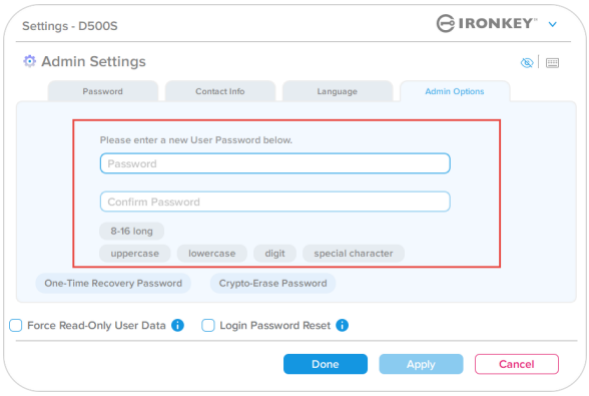


Figura 8.1 – Opzioni amministratore/Reset della password utente

Reset password di accesso:
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 8.2 e 8.3*)

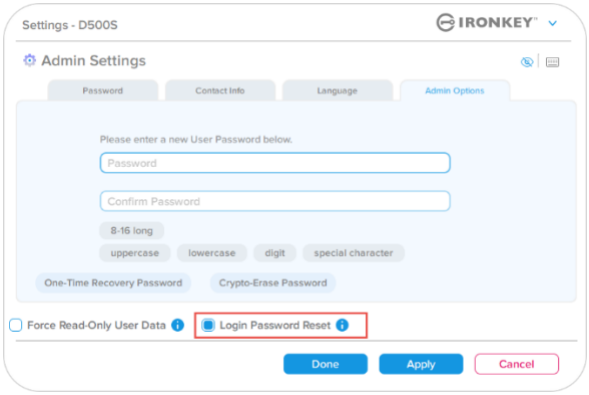


Figura 8.2 – Pulsante di reset della password di accesso

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

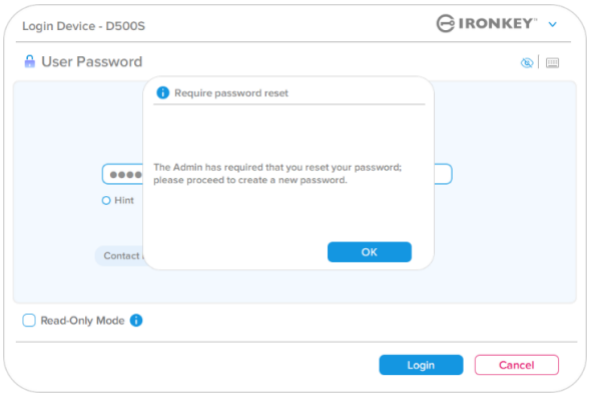


Figura 8.3 – Notifica di reset dopo l'inserimento della password utente

Funzionalità amministratore

Password di ripristino monouso

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

Password di ripristino monouso

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

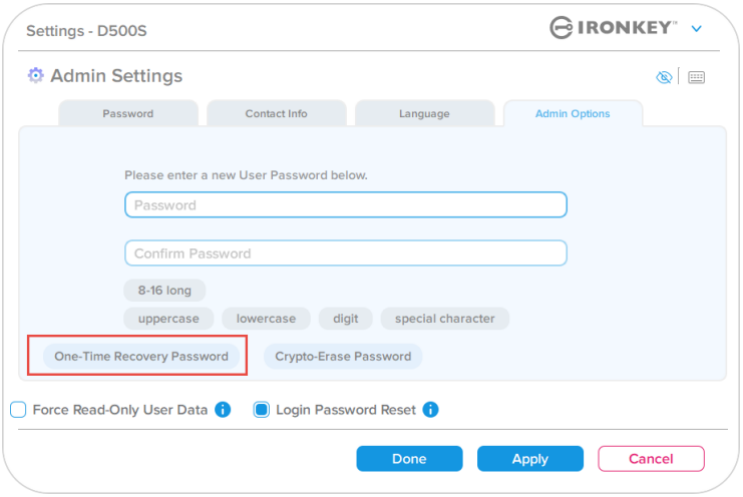


Figura 8.4 – Pulsante per la password di ripristino monouso

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

Nota: L’applicazione delle modifiche apportate richiede l’inserimento della password Amministratore.

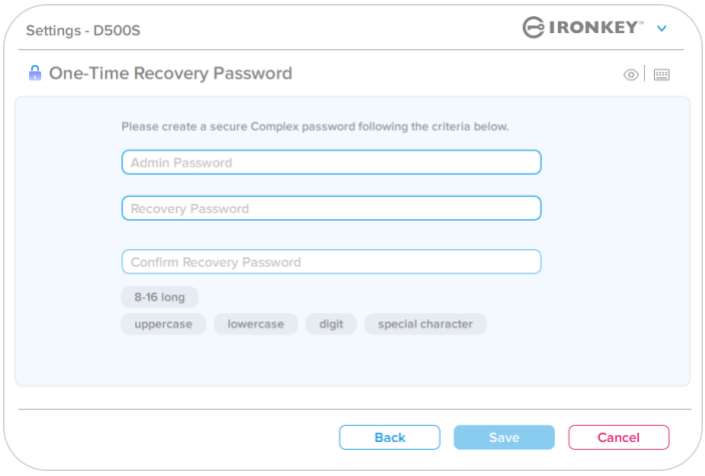


Figura 8.5 – Configurazione della password di ripristino monouso

Funzionalità amministratore

Utilizzo della password di ripristino monouso

Fase 1: Una volta creata la password di ripristino monouso, in occasione dell'accesso successivo, sarà visualizzato un nuovo pulsante nella schermata di accesso **password Utente**. Fare clic sul pulsante **"Recovery password (Password di ripristino)"** per avviare la procedura.

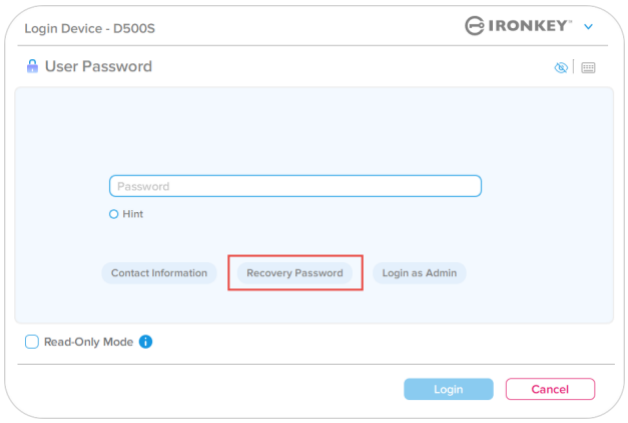


Figura 8.6 – Pulsante per la password ripristino

Fase 2: Sarà visualizzata la schermata **"Password di ripristino"**, nella quale è possibile inserire la password di ripristino e creare una nuova password Utente. (*Figura 8.7*)

Importante: La password di ripristino monouso utilizza anche una funzionalità di sicurezza integrata che conteggia il numero di tentativi di accesso non riusciti. **Dopo 10 tentativi di accesso falliti, la funzione di inserimento password di ripristino monouso sarà disabilitata** e l'utente dovrà riabilitarla effettuando un nuovo accesso al drive come Amministratore. (Vedere le pagine 19 e 33 per ulteriori dettagli)

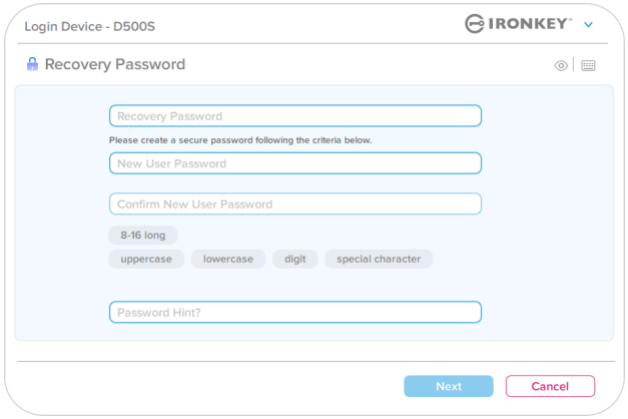


Figura 8.7 – Menu per la password ripristino

Fase 3: Una volta completata la procedura con successo sarà visualizzata nuovamente la schermata **"Password utente"**. Il pulsante **"Recovery password" (Password di ripristino)** scompare, e la password utente inserita durante la **Fase 2** diventa la nuova password Utente. (*Figura 8.8*)

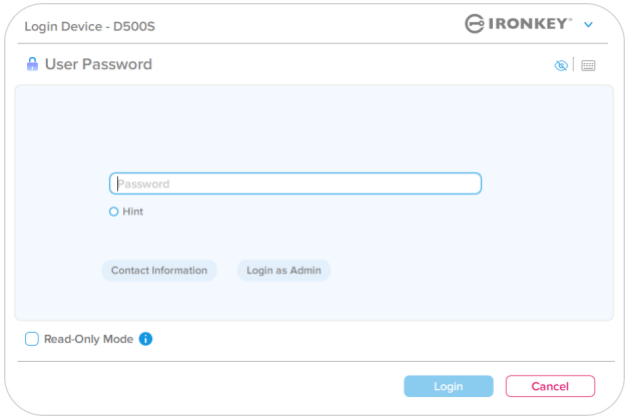


Figura 8.8 – Accesso con Password Utente (funzione amministratore non abilitata Il pulsante della password di ripristino scompare dopo che tale funzionalità è stata utilizzata con successo.

Funzionalità amministratore

Password di attivazione cancellazione crittografica

Il drive IronKey D500S è dotato di un'esclusiva funzione password di cancellazione crittografica. Tale funzione è progettata per proteggere e difendere l'unità e i dati contro gli attacchi che mirano a compromettere l'integrità fisica del drive, attraverso la cancellazione sicura dei contenuti del drive durante il suo utilizzo, e lasciando la memoria del drive completamente vuota, come se nessun dato fosse mai stato scritto al suo interno. Quando questa funzionalità è abilitata, e il drive viene sbloccato con la password di cancellazione crittografica, l'unità effettuerà, con la massima discrezione, una procedura di cancellazione crittografica del drive D500S, effettuando l'accesso del drive in modalità equivalente a quella di fabbrica, con una partizione Utente completamente vuota. La chiave crittografica precedente sarà cancellata, e una nuova chiave crittografica creata al suo posto. ***Utilizzare con cautela***

- Per **abilitare** questa funzionalità, fare clic sul pulsante "Crypto-erase password" (Password di cancellazione crittografica), nella scheda "Admin Options" (Opzioni amministratore):

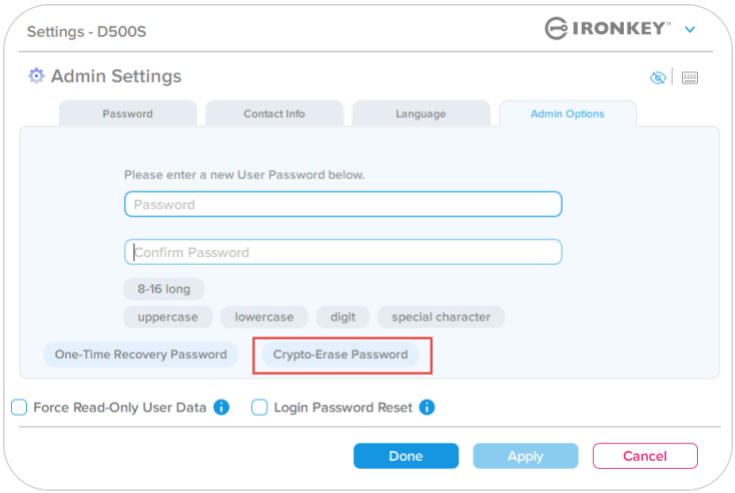


Figura 8.9 – Abilitazione della password di cancellazione crittografica

Creare una password di cancellazione crittografica:

- Le regole password saranno basate sul modo in cui il drive è stato inizialmente inizializzato (password complessa o frase password)
- La convalida richiede l'inserimento della password Amministratore.

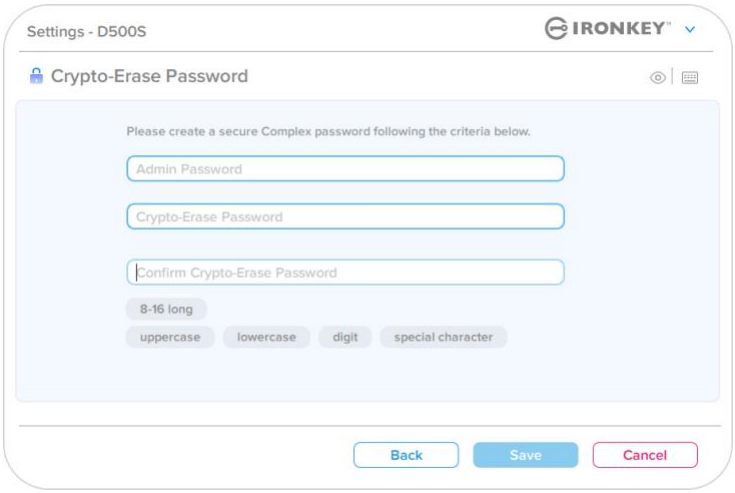


Figura 8.10 – Creazione della password di cancellazione crittografica

Funzionalità amministratore

Utilizzo della Password di attivazione cancellazione crittografica

Quando viene utilizzata la Password di cancellazione crittografica, le precedenti password Amministratore e Utente saranno eliminati, sostituiti dalla Password di cancellazione crittografica. Inoltre, qualunque impostazione di configurazione precedente sarà eliminata, unitamente alla cancellazione permanente di tutti i dati memorizzati sul drive, con la relativa conversione del drive alla configurazione in modalità “Solo utente”.

Per utilizzare la Password di cancellazione crittografica:

1. Lanciare il programma Ironkey.exe per eseguire l’applicazione IronKey

2. Nella schermata di accesso password Utente, premere “**CTRL + ALT + C**”, per attivare la selezione dell’opzione “Password di cancellazione crittografica”. Se la procedura è stata effettuata correttamente, si noterà la presenza di una barra blu di maggior spessore sotto la schermata di inserimento password, a indicare che è ora possibile effettuare l’inserimento della Password di cancellazione crittografica. (*Figura 8.11*)

NOTA: La password di cancellazione crittografica può essere attivata solamente dalla schermata di accesso password Utente.

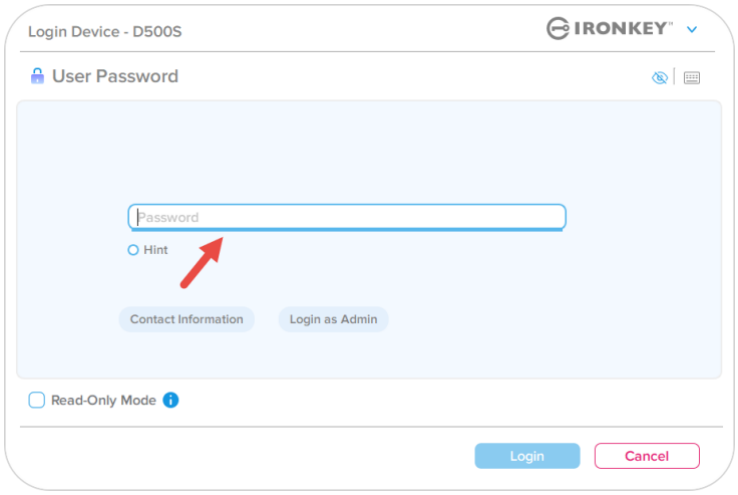


Figura 8.11 – Cancellazione crittografica attiva, con barra spessa di colore blu

Quando la password di cancellazione crittografica viene utilizzata, il drive eseguirà la cancellazione completa di tutti i contenuti. Successivamente, sul drive apparirà una sola partizione vuota. Il drive opererà ora in modalità “Solo utente” e la password di cancellazione crittografica diventerà anche la password utilizzata per l’accesso al drive fino al suo reset.

Importante: questa funzionalità causa l’eliminazione permanente di tutti i dati memorizzati sul drive e di qualunque altro contenuto salvato sul drive in precedenza. Pertanto, si raccomanda di utilizzare la funzionalità con la dovuta cautela.

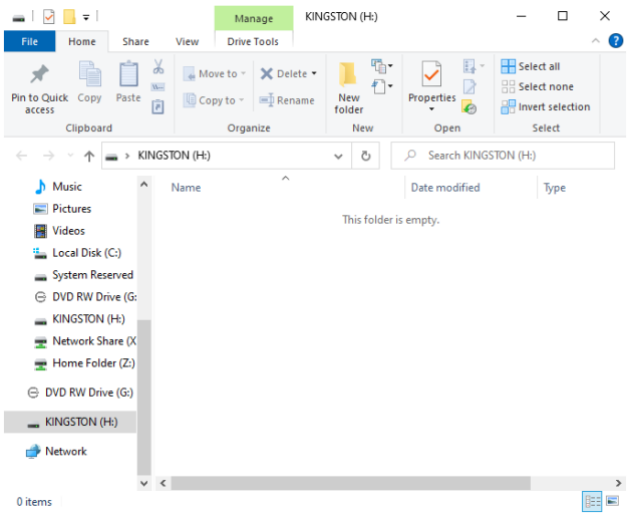


Figura 8.12 – Cancellazione del drive dopo l’utilizzo della password di cancellazione crittografica

Funzionalità amministratore

Forza la modalità di sola lettura per i dati utente

La modalità "Forza sola lettura" può essere abilitata per impedire all'utente l'accesso in scrittura al drive. Questa funzionalità è particolarmente utile se i file presenti sul drive devono essere utilizzati in modalità di accesso in sola lettura.

- Per abilitare la funzione "Forza sola lettura" per i dati utente, fare clic sull'apposita casella e quindi cliccare su "Apply" (Applica). (*Figura 8.13*)

  Nota: La modalità "Forza sola lettura" è applicabile esclusivamente all'account utente e non influenza in alcun modo l'account amministratore. L'account amministratore continuerà a mantenere privilegi di accesso in lettura e scrittura e potrà sempre abilitare la modalità di sola lettura quando necessario.

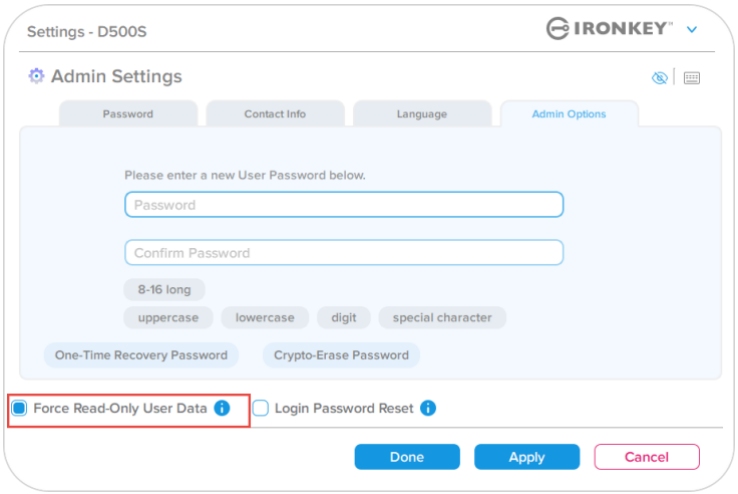


Figura 8.13 – Abilitazione della funzione "Forza la modalità di sola lettura per i dati utente"

(l'applicazione delle modifiche apportate richiede l'inserimento della password Amministratore)

- Una volta attivata la funzionalità, il pulsante **"Read-Only Mode" (Modalità sola lettura)** diventerà di colore blu, a indicare che la modalità "Forza sola lettura" è abilitata in maniera permanente per la password utente, fino a quando tale funzione non viene disabilitata dall'amministratore. (*Figura 8.14*)

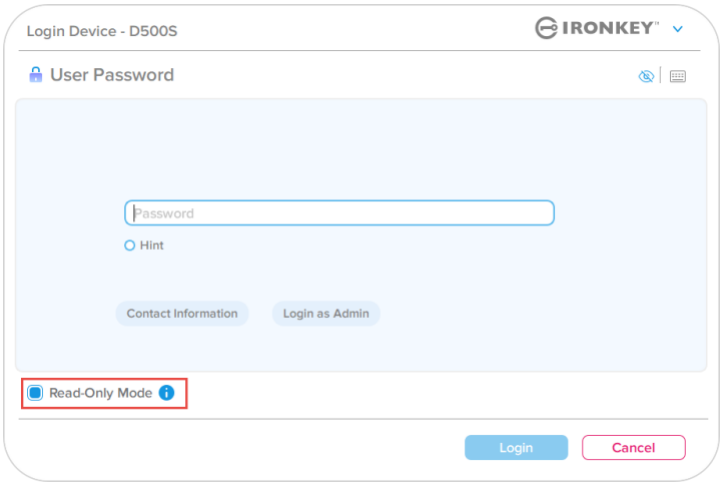


Figura 8.14 – La modalità di sola lettura è abilitata forzatamente per l'account utente e può essere disabilitata esclusivamente dall'amministratore

Guida alla risoluzione dei problemi

Blocco del dispositivo

Il drive D500S integra una funzione di sicurezza che impedisce gli accessi non autorizzati alla partizione dati quando si supera un determinato numero **consecutivo** di tentativi di accesso falliti (indicato dal parametro *MaxNoA*, in breve). La configurazione "di fabbrica" predefinita include un valore pari a 10 (numero di tentativi per ciascun metodo di accesso (Amministratore/Utente/Password di ripristino monouso).

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

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

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

- Se viene inserita una password errata, sopra il campo "Inserimento password" "Password Entry", verrà visualizzato un messaggio di errore di colore rosso indicante il tentativo di accesso fallito. (*Figura 9.1*)

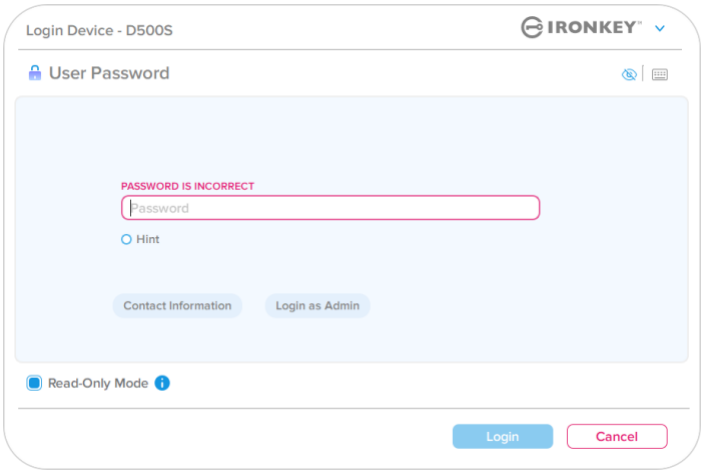


Figura 9.1 – Messaggio di notifica inserimento password errata

- Una volta raggiunto il **settimo** 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 massimo di tentativi specificati dal valore MaxNoA (impostato su 10 per default). (*Figura 9.2*)

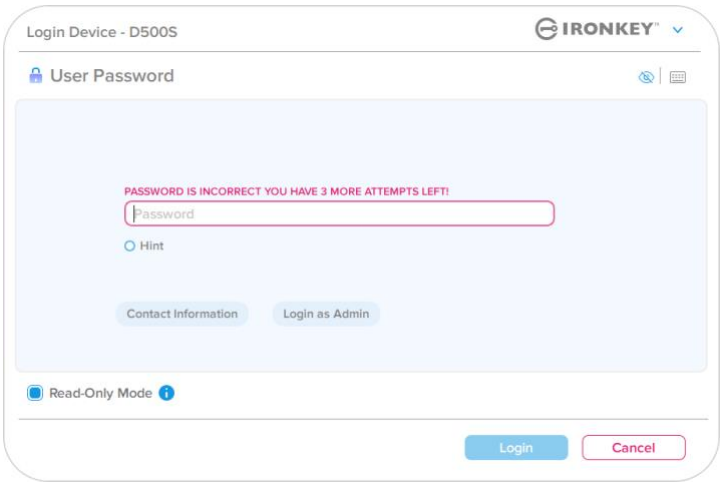


Figura 9.2 – Notifica del 7° tentativo di inserimento password errato

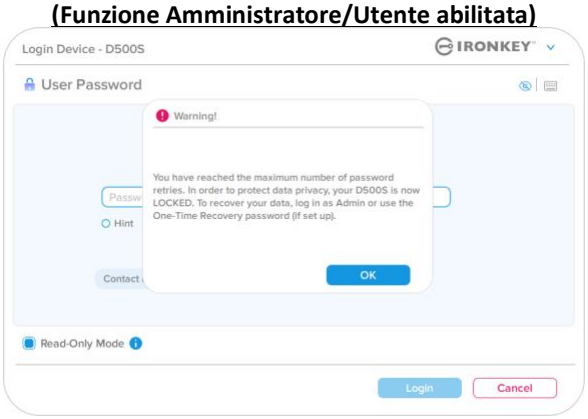
Guida alla risoluzione dei problemi

Blocco del dispositivo

Importante: Una volta raggiunto il **10°** e ultimo tentativo di accesso fallito, in base alla modalità di configurazione della modalità utilizzata (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**. Questi comportamenti sono già citati a pagina 19 del manuale utente.

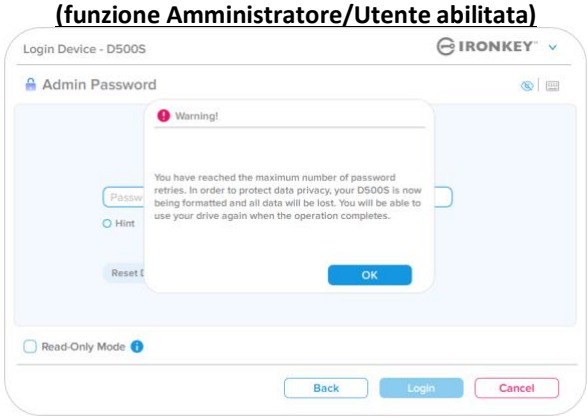
Le Figure 9.3 – 9.6 sotto, illustrano visivamente le schermate visualizzate dopo il 10° tentativo di accesso fallito con ciascun metodo di accesso:

Password utente:
(Funzione Amministratore/Utente abilitata)



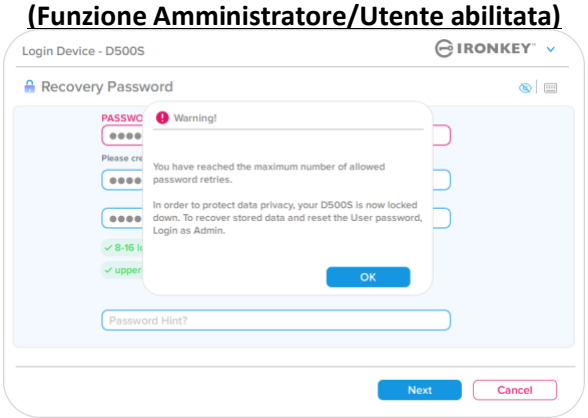
BLOCCO DEL DISPOSITIVO
Figura 9.3

Password Amministratore
(funzione Amministratore/Utente abilitata)



FORMATTAZIONE DISPOSITIVO*
Figura 9.4

Password di ripristino monouso:
(Funzione Amministratore/Utente abilitata)



BLOCCO DEL DISPOSITIVO
Figura 9.5

Password Utente
(modalità amministratore non abilitata)

FORMATTAZIONE DISPOSITIVO*
Figura 9.6

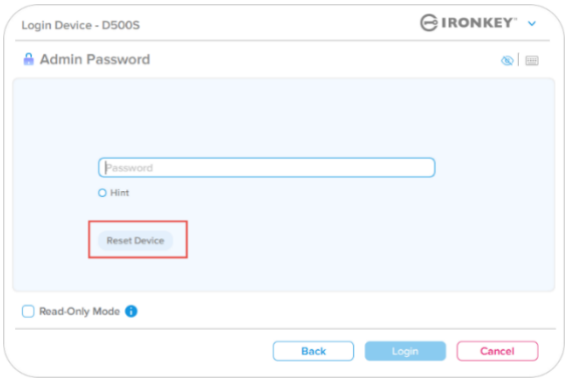
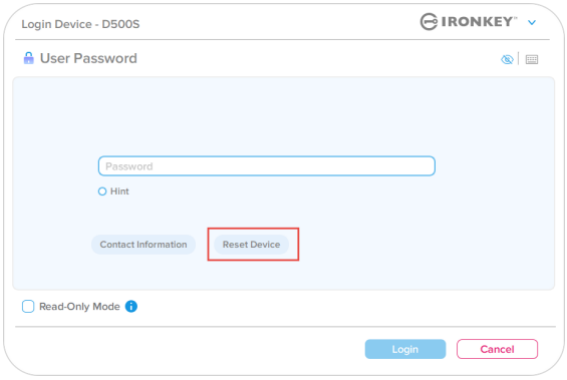
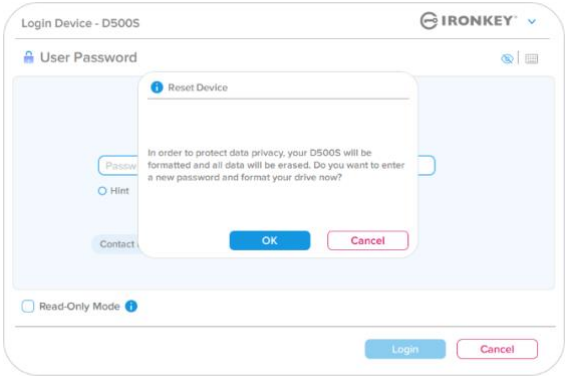
Questa misura di sicurezza ha lo scopo di limitare l'accesso a coloro che non dispongono della password, impedendo di effettuare tentativi di accesso ripetuti all'infinito allo scopo di accedere ai vostri dati sensibili (noti anche come attacchi brute force). Per i possessori di drive D500S che hanno scordato la password di accesso verranno applicate le medesime misure di sicurezza, compresa la formattazione del dispositivo. * Per ulteriori informazioni su questa funzionalità, consultare la sezione *"Reset del dispositivo"*, a pagina 25.

**Nota:* *La formattazione del dispositivo eliminerà tutti i dati archiviati sulla partizione dati sicura del drive DS500S.*

Guida alla risoluzione dei problemi

Reset dispositivo

Se si è dimenticata la password, oppure se è necessario effettuare un reset del drive è possibile fare clic sul pulsante **"Reset dispositivo"**. Tale pulsante può essere posizionato in due punti, in base alla configurazione utilizzata (sul menu di "Accesso password amministratore" con funzione Amministratore/Utente abilitata; oppure sul menu di "Accesso password utente" quando tale funzione non è abilitata), quando viene eseguito il programma di avvio del drive D500S (vedere *Figure 9.7 e 9.8*).

• Questa opzione consente di creare una nuova password; ma per proteggere la privacy, il drive D500S sarà formattato. Ciò significa che durante tale procedura tutti i vostri dati andranno persi.*	 **Figura 9.7 – Password Amministratore: Pulsante di reset dispositivo**
• **Nota:** Cliccando sul pulsante *"Reset Device"* (Reset dispositivo), verrà visualizzata una finestra di notifica in cui si chiede all'utente se desidera inserire una nuova password prima della formattazione. A questo punto, è possibile 1) cliccare su *"OK"* per confermare, oppure 2) cliccare su "Annulla", per tornare alla schermata di accesso. (Vedere *Figura 9.8*)	 **Figura 9.8 – Password Utente (funzione Admin/Utente non abilitata) Reset dispositivo**
• Se si sceglie di continuare, sarà visualizzata la schermata di inizializzazione dalla quale è possibile abilitare la modalità Amministratore e Utente e inserire una nuova password in base all'opzione di configurazione password selezionata (Password complessa o frase password). Il campo suggerimento (Hint) non è obbligatorio, ma può rivelarsi utile per aiutare l'utente a ricordare la password, qualora questa vada persa o dimenticata.	 **Figura 9.9 – Conferma di reset dispositivo**

Guida alla risoluzione dei problemi

Conflitti tra le lettere di unità: Sistemi operativi Windows

- Come citato nella sezione *"Requisiti di sistema"* di questo manuale (a pagina 3), il drive D500S 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 D500S 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 D500S 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.

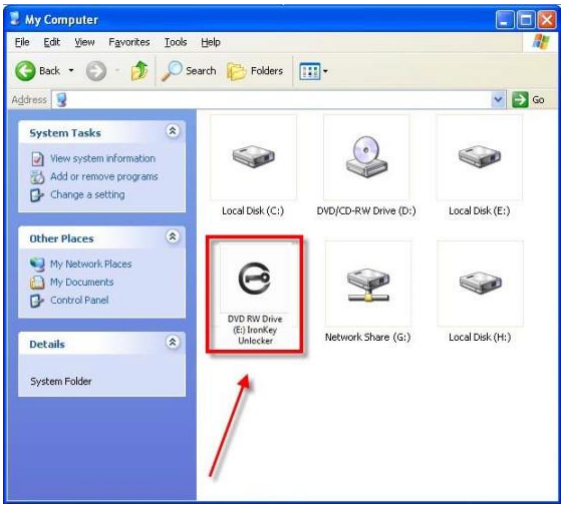


Figura 9.10 – Esempio di lettera di unità

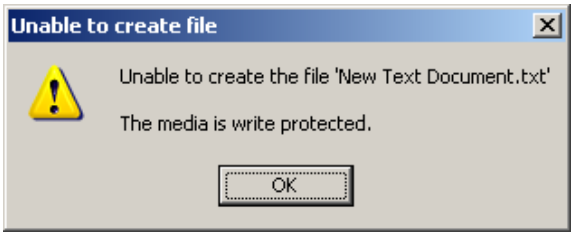
In questo esempio (*Figura 9.10*), all'unità D500S è assegnata la lettera "F:" che è la prima lettera disponibile dopo l'unità "E:" (l'ultima lettera di unità assegnata a un disco fisico prima dell'elenco di lettere di unità assegnate a unità non fisiche). Dato che alla lettera "G:" è assegnata una condivisione di rete, che non appartiene al profilo hardware del computer in uso, l'unità D500S tenterà di utilizzare tale lettera come seconda unità, generando un conflitto.

Se sul computer in uso non sono presenti condivisioni di rete, ma l'unità D500S continua a non avviarsi, è possibile che altri dispositivi esterni, come lettori di schede, dischi rimovibili, o altri dispositivi installati in precedenza stiano utilizzando la lettera di unità richiesta per il funzionamento dell'unità DataTraveler, causando ulteriori conflitti.

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

Guida alla risoluzione dei problemi

Messaggi di errore

Unable to create file (Impossibile creare il 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.	 **Figura 9.11 – Finestra di notifica errore "Unable to create file" (Impossibile creare il file)**
Error Copying File or Folder Error (Impossibile copiare il file o la cartella): 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.	 **Figura 9.12 – Finestra di notifica errore "Error Copying File or Folder Error" (Impossibile copiare il file o la cartella)**
Error Deleting File or Folder Error (Impossibile eliminare il file o la cartella): 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.	 **Figura 9.13 – Finestra di notifica errore "Error Deleting File or Folder Error" (Impossibile eliminare il file o la cartella)**

Nota: Se si sta effettuando l'accesso all'unità in modalità "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'unitàD500S poi effettuare nuovamente l'accesso, assicurandosi di deselezionare la casella dell'opzione "Read-Only Mode" (Modalità di sola lettura), prima di effettuare l'accesso.

Utilizzo del dispositivo (Ambienti Linux)

Data la grande varietà di distribuzioni Linux attualmente disponibili sul mercato, l'aspetto e le modalità d'uso delle interfacce utilizzate dalle differenti versioni disponibili possono variare notevolmente tra loro. Tuttavia, il set di comandi normalmente utilizzati all'interno dell'applicazione terminale è simile per tutte le versioni; tali comandi Linux sono descritti in sezione sotto. Le immagini di esempio raffigurate in questa sezione rappresentano un ambiente a 64 bit.

Su alcune distribuzioni di Linux l'esecuzione dei comandi del drive D500S dalla finestra terminale dell'applicazione, richiede l'accesso con privilegi di super-user (root).

Note importanti prima di procedere:

1.) **Il drive D500S non supporta l'inizializzazione del dispositivo su sistemi Linux, e deve pertanto essere inizializzato e configurato completamente su sistemi Windows o MacOS prima di poter essere utilizzato su Linux.**

2.) **L'accesso con Linux supporta solo le password complesse. L'accesso con frase password non è supportato sui sistemi Linux.**

3.) **Le funzionalità del drive D500S hanno un supporto limitato su piattaforme Linux. Funzionalità come password di ripristino monouso, una password di cancellazione crittografica, password Amministratore/Utente, reset e attivazione della funzione di sola lettura non sono supportate sui sistemi Linux.**

L'unità D500S integra 4 comandi che possono essere utilizzati sui sistemi Linux:

lkd500s_about	Mostra le 'informazioni sul drive D500S.
lkd500s_login	Consente l'accesso al drive.
lkd500S_logout	Consente l'uscita sicura dal drive D500S.
lkd500S_resetdevice	Esegue una cancellazione crittografica e il reset del drive alla configurazione di fabbrica, eliminando permanentemente tutti i dati e i file memorizzati sul drive.

NOTA: l'esecuzione di questi comandi richiede l'apertura di una finestra dell'applicazione "Terminale" e l'accesso alle cartelle specifiche in cui risiede ogni singolo file. Ogni comando deve essere preceduto dai due caratteri seguenti: './' (un punto e uno slash in avanti).

Esempio di come navigare tra i comandi di percorso Linux per IronKey:

Per utenti Linux a 32 bit:	Aprire una finestra dell'applicazione terminale e modificare la directory corrente su: **/media/ubuntu/IRONKEY/linux/linux32$** digitando il comando seguente: **cd /media/ubuntu/IRONKEY/linux/linux32** (e successivamente premere INVIO)
Per utenti Linux a 64 bit:	Aprire una finestra dell'applicazione terminale e modificare la directory corrente su: **/media/ubuntu/IRONKEY/linux/linux64$** digitando il comando seguente: **cd /media/ubuntu/IRONKEY/linux/linux64** (e successivamente premere INVIO)

Utilizzo del dispositivo (Ambienti Linux)

Nota: se il volume dell'unità IRONKEY non viene caricato automaticamente dal sistema operativo, l'utente dovrà effettuare il caricamento manuale da una finestra del terminale, mediante il comando "mount" di Linux. Fare riferimento alla documentazione Linux riferita alla distribuzione specifica utilizzata, oppure accedere al proprio sito di supporto online preferito per ottenere ulteriori dettagli sulle opzioni relative a sintassi e comandi disponibili. Alcune distribuzioni Linux potrebbero richiedere l'inserimento del nome utente per eseguire comandi, come nel caso del comando "ubuntu" riportato negli esempi sopra.

Identificazione e visualizzazione dei file di comando Linux IronKey D500S:

Una volta che il drive D500S è collegato al vostro computer e rilevato dal sistema operativo, cambiare la directory sul volume D500S inserendo il comando mediante il prompt del terminale. (*Figura 10.1*)

Nota: Gli screenshot e le istruzioni riportate in questa sezione utilizzano la cartella linux64 (a indicare una piattaforma a 64-bit), al solo fine di dimostrare l'uso del drive D500S sui sistemi con sistema operativo Linux. Pertanto, è opportuno tenere a mente che se si sta utilizzando la versione a 32-bit di Linux, sarà sufficiente accedere alla rispettiva cartella "32-bit" anziché a quella a 64-bit, specificando la cartella, linux32 anziché quella denominata linux64).

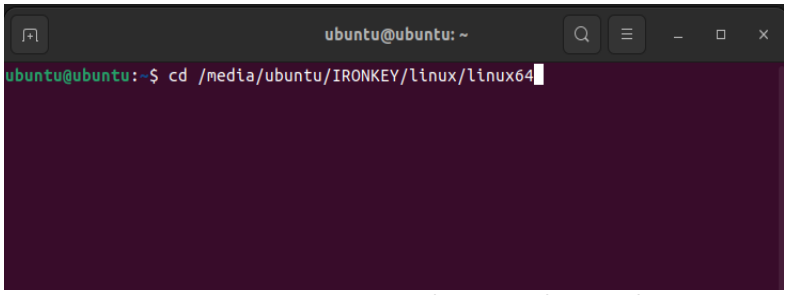


Figura 10.1 – Navigazione mediante riga di comando

Utilizzare il comando **"ls"** (list) dal prompt corrente e quindi premere "INVIO". Questo comando consente di visualizzare un elenco di file e/o cartelle all'interno della cartella linux64.

Successivamente, sarà possibile visualizzare i quattro comandi Linux IronKey elencati (*Figura 10.2*)

- ikD500S_about
- ikD500S_login
- ikD500S_logout
- ikD500S_resetdevice

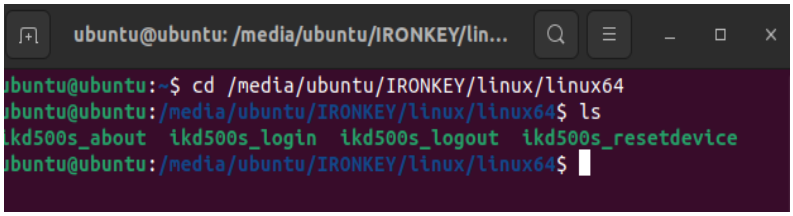


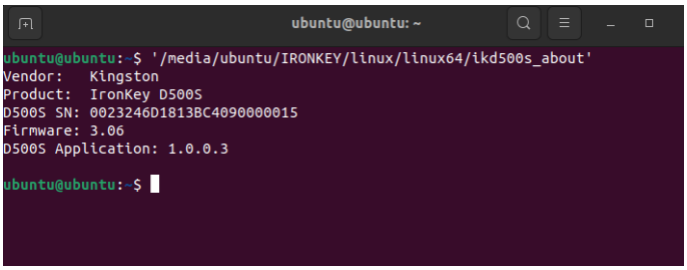
Figura 10.2 – File di comando visualizzazione Linux IronKey

Nota: I nomi di comandi e cartelle (directory) sono sensibili alle maiuscole. Pertanto digitare "linux64" NON equivale a digitare "Linux64". Anche la sintassi deve essere immessa nel modo esatto in cui essa è rappresentata. Alcune distribuzioni Linux potrebbero richiedere l'inserimento del nome utente per eseguire comandi, come nel caso del comando "ubuntu" in questo esempio.)

Utilizzo del dispositivo (Ambienti Linux)

Utilizzo dei comandi D500S

Informazioni su D500S

IkD500S_about (Informazioni su D500S, *Figura 10.3*) Questo comando consente di popolare i campi dati relativi al drive D500S, come: • Produttore • Prodotto • Numero di serie D500S • Versione firmware • Versione software	 **Figura 10.3 – ikD500S_about (Informazioni su IronKey D500S)**

Accesso a D500S

ikD500S_login

Una volta che il drive DS500S è stato inizializzato su sistema operativo Windows o MacOS, sarà possibile accedere alla partizione dati sicura, utilizzando la password D500S creata durante la procedura descritta.

Per effettuare l'accesso, seguire la procedura riportata sotto:

1. Aprire una finestra dell'applicazione "Terminale".

2. Sul prompt del terminale, inserire il seguente comando: **cd /media/ubuntu/IRONKEY/linux/linux64**

3. Posizionando il prompt dei comandi sulla stringa **/media/ubuntu/IRONKEY/linux/linux64$**, digitare il comando seguente per accedere al dispositivo: **./ ikD500S_login*** e premere "INVIO". (Nota: Comandi e nomi delle cartelle sono sensibili alle maiuscole e la sintassi utilizzata deve essere esattamente quella qui indicata. Inoltre, alcune distribuzioni potrebbero richiedere all'utente di inserire il nome utente, come "ubuntu", in questo caso).

4. Dopo aver effettuato l'accesso, sul desktop del computer in uso si aprirà la schermata che visualizza il volume dati sicuro, da cui sarà possibile iniziare a utilizzare l'unità D500S (per ulteriori informazioni sul comportamento del drive in fase di accesso, proseguire alla pagina successiva).

*Nota: Su alcune distribuzioni di Linux l'esecuzione dei comandi del drive D500S dalla finestra terminale dell'applicazione, richiede l'accesso con privilegi di super-user (root).

Utilizzo del dispositivo (Ambienti Linux)

Accesso a D500S (continua)

IkD500S_login (Sblocco del drive D500S, *Figura 10.4*)

In base al tipo di configurazione utilizzata per il drive, durante la procedura di accesso potrebbero essere disponibili varie opzioni su come sbloccare il drive.

Se i profili password **amministratore e utente** sono stati abilitati durante la fase di inizializzazione, saranno disponibili le seguenti opzioni di accesso:

1.) Selezionare l'accesso come Amministratore o Utente
2.) Selezionare lo sblocco delle partizioni Amministratore o Utente (se abilitate)
3.) Inserire la password di accesso Amministratore o Utente per l'autenticazione e lo sblocco del dispositivo.

Nota: Se, durante l'inizializzazione, NON sono stati abilitati i profili password amministratore e utente sono stati (modalità Solo utente), sarà richiesto il solo inserimento della password dell'utente per l'autenticazione di accesso al dispositivo.

Importante: Come citato in precedenza, le frasi password non sono supportate sui sistemi Linux e pertanto il drive D500S dovrà essere configurato utilizzando una password complessa per l'accesso a Linux (*Figura 10.5*)

Figura 10.4 – ikD500S_login (Sblocco del drive D500S)

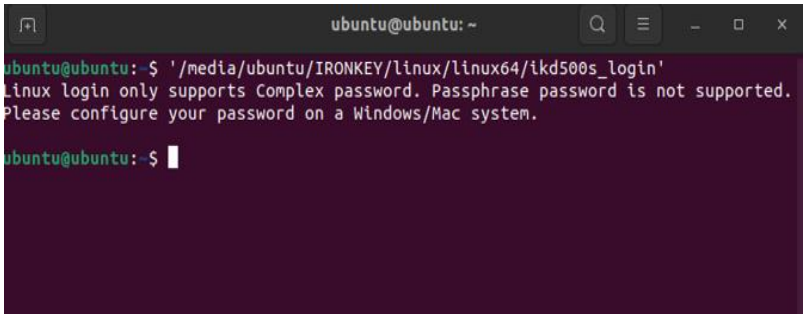


Figura 10.5 – Tentativo di accesso con frase password non supportata.

Utilizzo del dispositivo (Ambienti Linux)

Accesso a D500S (continua)

Errore durante l'inserimento della password di accesso

Se durante il processo di accesso viene inserita una password errata, l'utente avrà a disposizione un'altra possibilità per inserire la password corretta. Tuttavia, il dispositivo è dotato di una funzione di sicurezza integrata che conteggia il numero di tentativi di accesso falliti. Se il numero di tentativi falliti da parte dell'Amministratore o dell'Utente supera il valore preimpostato di default, pari a 10 tentativi, il drive effettuerà le seguenti operazioni:

Password Amministratore/Utente abilitate

- **Accesso Utente:** Blocco utente, richiede l'accesso come amministratore. (*Figura 10.6*) Nota: La password Utente può essere resettata mediante un accesso Amministratore, su sistemi Windows o MacOS supportati.
- **Accesso amministratore:** Cancellazione crittografica del drive; i dati vengono eliminati definitivamente. Richiede il reset del dispositivo. (*Figura 10.7*)

Modalità "Solo utente" (modalità Amministratore/Utente non abilitata)

- **Accesso Utente:** Cancellazione crittografica del drive; i dati vengono eliminati definitivamente. Richiede il reset del dispositivo. (*Figura 10.7*)

Figura 10.6 – Blocco di accesso Utente, Password Amministratore/Utente abilitate

Figura 10.7 – Numero massimo di tentativi raggiunto (reset drive)

D500S Uscita

IkD500S_logout (blocco dispositivo)

Dopo aver terminato di utilizzare l'unità D500S, effettuare l'uscita dal dispositivo e mettere i dati in sicurezza. Per fare ciò, seguire i passi indicati nella procedura descritta a pagina 39, e utilizzare il seguente comando di uscita sul dispositivo correttamente: **./ IkD500S_logout** e premere "INVIO" (Nota: Comandi e nomi delle cartelle sono sensibili alle maiuscole e la sintassi utilizzata deve essere esattamente quella qui indicata. (*Figura 10.8*)

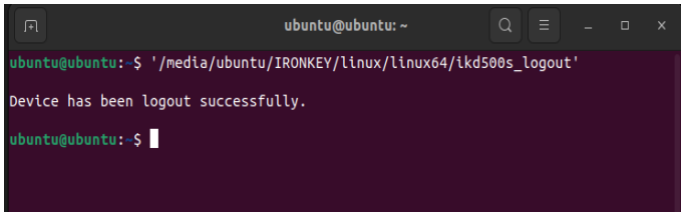


Figura 10.8 – D500S Uscita

Utilizzo del dispositivo (Ambienti Linux)

ResetD500S – Reset dispositivo

ikD500S_resetdevice
Come già citato in precedenza a pagina 41, in caso di smarrimento delle password Utente/Amministratore, è possibile utilizzare il comando "Reset Dispositivi" per effettuare il reset del drive e renderlo nuovamente utilizzabile. Questa procedura consente di creare una nuova password. Tuttavia, al fine di garantire la privacy dei dati contenuti nel drive D500S, viene eseguita la cancellazione crittografica della partizione dati sicura. **Ciò significa che tutti i dati precedentemente archiviati andranno persi.**

Per utilizzare il comando "Reset dispositivo", seguire i passi indicati nella procedura descritta a pagina 39, e utilizzare il seguente comando di uscita sul dispositivo correttamente: **./ikD500S_resetdevice**; quindi, premere "INVIO" (Nota: Comandi e nomi delle cartelle sono sensibili alle maiuscole e la sintassi utilizzata deve essere esattamente quella qui indicata. (*Figura 10.9*)

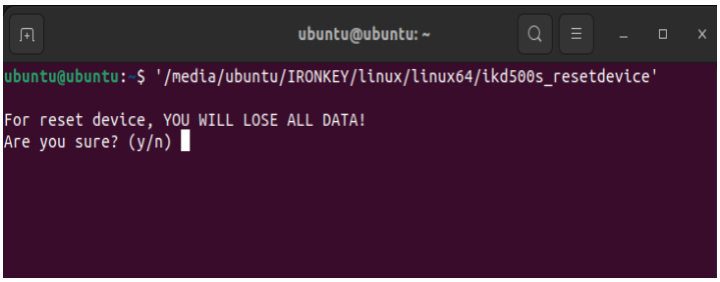


Figura 10.9 – Comando "Reset dispositivo"

Una volta utilizzato il comando "Reset dispositivo", verrà chiesto all'utente di creare una nuova password complessa, che deve includere:

- Lunghezza compresa tra 8 e 16 caratteri, comprendente almeno tre (3) dei seguenti criteri opzionali:

  -LETTERE MAIUSCOLE
  -lettere minuscole
  -Numeri
  -Caratteri speciali (!,$,ecc.)

(*Figura 10.10*)

Nota: Il comando "Reset dispositivo" consente di inizializzare il drive in modalità "Solo utente" (password singola, Utente singolo). Al fine di abilitare i profili di accesso password Amministratore/Utente, è necessario configurare il drive D500S su un sistema Windows o MacOS supportati e in grado di accedere a tale opzione.

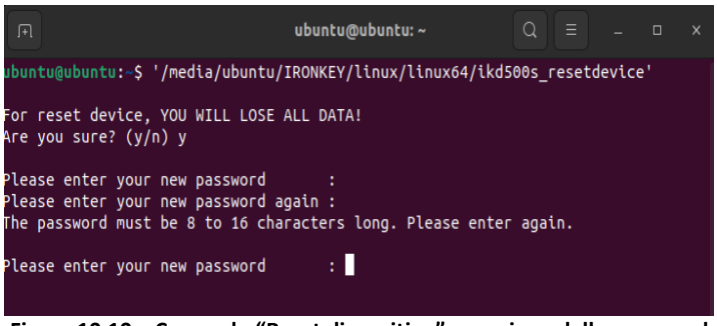


Figura 10.10 – Comando "Reset dispositivo", creazione della password

IRONKEY™ D500S
PENDRIVE USB 3.2 Gen 1 SEGURO

Manual do Usuário

Índice

Figura 1 – IronKey D500S

Introdução

O IronKey D500S da Kingston é um drive USB de segurança militar que se baseia nos recursos que tornaram o IronKey uma marca muito respeitada para proteger informações confidenciais. Tem certificado FIPS 140-3 Nível 3 (pendente), que inclui novos aprimoramentos de segurança do NIST exigindo atualizações de processador seguras para maior segurança. A criptografia e a descriptografia são feitas no D500S, sem deixar vestígios no sistema host – tornando-o imune a farejadores de senha na memória. Juntamente com a criptografia XTS-AES de 256 bits baseada em hardware, ele também possui uma estrutura robusta de zinco que é à prova d'água*, à prova de poeira*, resistente a esmagamento e vedado com epóxi para proteger componentes internos de ataques de penetração.

O D500S suporta opções multissenhas (Admin, Usuário, Recuperação única e Exclusão criptográfica) com modos tradicionais de senhas Complexas ou de Frase-passe**. 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 modo de Frase-passe permite um PIN numérico, frase, lista de palavras ou até letras de música de 10 a 128 caracteres. O Admin pode habilitar um usuário, criar partições duplas de dados com tamanho personalizado separando arquivos de login de Admin/Usuário, habilitar uma senha de recuperação única, senha de exclusão criptográfica e redefinir a senha do usuário para restaurar o acesso aos dados.

Para ajudar na entrada da senha, o símbolo de “olho” pode ser habilitado para revelar a senha digitada, reduzindo erros de digitação que levam a tentativas de login malsucedidas. Para maior tranquilidade, o D500S usa um firmware assinado digitalmente, tornando-o imune a malwares BadUSB e proteção de ataque por força bruta para evitar a adivinhação de senha. 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***.

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, recuperar o acesso aos dados em drives bloqueados e estar em conformidade com as leis e regulamentos quando perícias forem necessárias.

O D500S oferece muitas opções de personalização e é compatível com TAA/CMMC e montado nos EUA.

O D500S conta com uma garantia limitada de 5 anos e suporte técnico Kingston gratuito.

* Consulte a especificação da folha de dados. O produto deve estar limpo e seco antes de sua utilização.
** Modo de frase-passe não suportado em sistemas Linux.
*** Teclado virtual: Suporta apenas Inglês dos EUA em sistemas Microsoft Windows e macOS compatíveis.

Recursos do IronKey D500S

- Com certificado FIPS 140-3 Nível 3 (Pendente) com criptografia de hardware de 256 bits XTS-AES (criptografia que nunca pode ser desligada)
- Proteção contra ataque de BadUSB e por força bruta
- Opção de multissenhas
- Modos de senha Complexas ou de Frase-passe
- Opção exclusiva de dupla partição e senha de exclusão criptográfica
- Botão de olho para exibir senhas digitadas e reduzir tentativas de login malsucedidas
- Teclado virtual para ajudar na proteção contra registros de toque do teclado ou da tela
- Configurações somente leitura (proteção contra gravação) forçadas/baseadas em sessão para proteger o conteúdo do drive contra alterações ou malware
- Pequenos e médios negócios podem gerenciar os drives localmente usando a função de Admin
- Compatível com Windows, macOS e Linux (consulte a folha de dados para obter detalhes)

Sobre este Manual

Este manual do usuário abrange o IronKey D500S e baseia-se na imagem de fábrica sem customizações implementadas.

Requisitos do sistema

Plataforma de PC • Intel, AMD e Apple M1 SOC • 15 MB de espaço livre no disco • Porta USB 2.0 – 3.2 disponível • Duas letras consecutivas de drive após o último drive físico* ***Observação:** Consulte "Conflito de letra de drive" na página 35.	**Suporte do sistema operacional do PC** • Windows 11 • Windows 10
Plataforma Mac • 15 MB de espaço livre no disco • Porta USB 2.0 – 3.2	**Suporte do Sistema Operacional Mac** • macOS macOS 11.x - 14.x
Plataforma Linux • 5 MB de espaço livre no disco • Porta USB 2.0 – 3.2	**Suporte do Sistema Operacional Linux** • Linux Kernel v4.4 ou superior

Recomendações

Para garantir que haja uma ampla energia fornecida ao dispositivo D500S, insira-o diretamente em uma porta USB no seu notebook ou desktop, como visto na *Figura 1.1*. Evite conectar o D500S a qualquer dispositivo periférico que possa ter uma porta USB, como um teclado ou um hub USB, como visto na *Figura 1.2*.

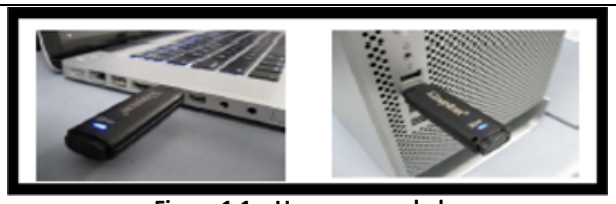


Figura 1.1 – Uso recomendado

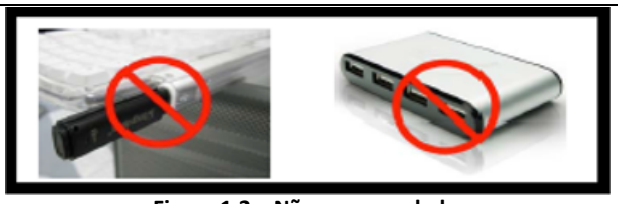


Figura 1.2 – Não recomendado

Utilizando o sistema de arquivo correto

O IronKey D500S vem pré-formatado com o sistema de arquivos FAT32. Ele funcionará em sistemas Windows, macOS e Linux*. 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 D500S em um sistema
- Ao usar o drive em um sistema público ou 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-lo
- 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

Encontre as últimas atualizações e informações

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.

*** O D500S não suporta inicialização direta de fábrica no Linux e precisará ser totalmente inicializado e configurado em um sistema Windows ou macOS compatível antes que o drive possa ser usado no Linux. Informações adicionais podem ser encontradas na seção Linux deste guia do usuário na página 37**

Práticas recomendadas para configuração de senha

Seu D500S 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 D500S automaticamente limpará os dados criptografados – formatando-se de volta para as configurações de fábrica.

Multissenhas
O D500S 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 D500S pode suportar três senhas diferentes utilizadas para recuperar os dados – Admin, Usuário e senha de Recuperação única**.**

O D500S permite que você selecione duas senhas principais – uma senha de Administrador (chamada de senha de Admin) e uma senha de Usuário. O Admin pode acessar o drive a qualquer momento e definir opções para o Usuário – o Admin é como um Superusuário. Além disso, o Admin pode configurar a senha de Recuperação única para o Usuário para fornecer uma forma do Usuário fazer o login e redefinir a senha de Usuário.

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

Se ambas as senhas forem esquecidas ou perdidas, não há outra forma de acessar os dados. A Kingston não poderá recuperar os dados já que a segurança não tem porta dos fundos. A Kingston recomenda que você também tenha os dados salvos em outra mídia. O D500S pode ser restaurado e reutilizado, mas os dados anteriores serão excluídos para sempre.

Modos de senha
O D500S também suporta dois modos de senha diferentes:

Complexa
Uma senha complexa exige o mínimo de 8 a 16 caracteres utilizando pelo menos 3 dos seguintes caracteres:

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

Frase-passe
O D500S suporta frases-passe de 10 a 128 caracteres. Uma frase-passe não segue regras, mas se utilizada de maneira apropriada, pode fornecer níveis muito altos de proteção de senha.

Uma frase-passe é basicamente qualquer combinação de caracteres, incluindo caracteres de outro idioma. Como o drive D500S, o idioma da senha pode combinar o idioma selecionado para o drive. Isso permite que você selecione múltiplas palavras, uma frase, letra de uma música, uma linha de uma poesia etc. Boas frases-passes estão entre os tipos de senha mais difíceis de um invasor adivinhar e ao mesmo tempo podem ser mais fáceis para os usuários recordarem.

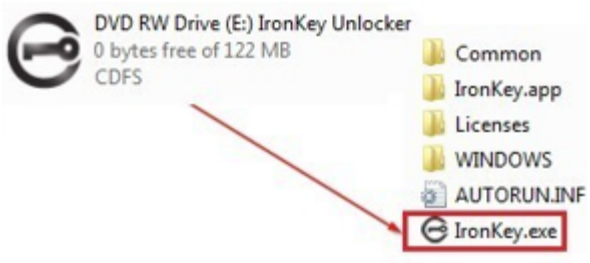
Configurar o meu dispositivo

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

Acesso ao dispositivo (Ambiente Windows)

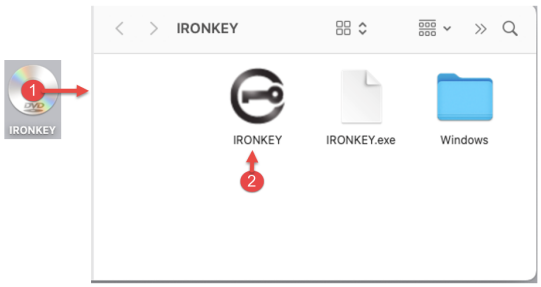
Conecte o drive USB criptografado IronKey a uma porta USB disponível em um notebook ou computador e espere o Windows detectá-lo.

• Usuários do Windows 10/11 receberão uma notificação de driver do dispositivo. (*Figura 3.1*)	 **Figura 3.1 – Notificação de Driver do Dispositivo**

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

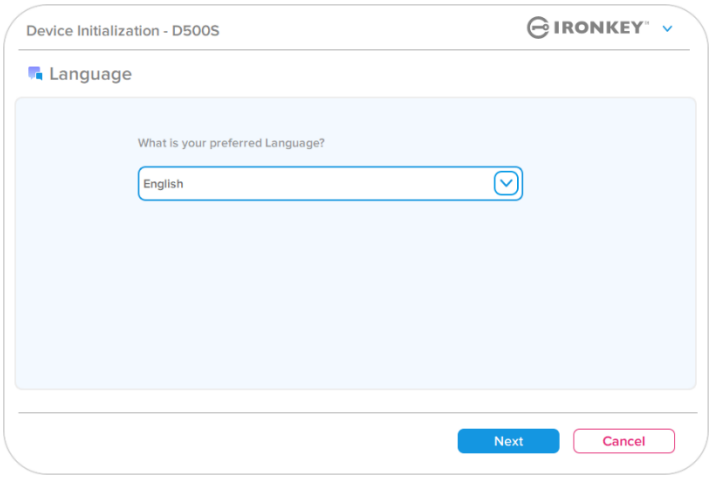
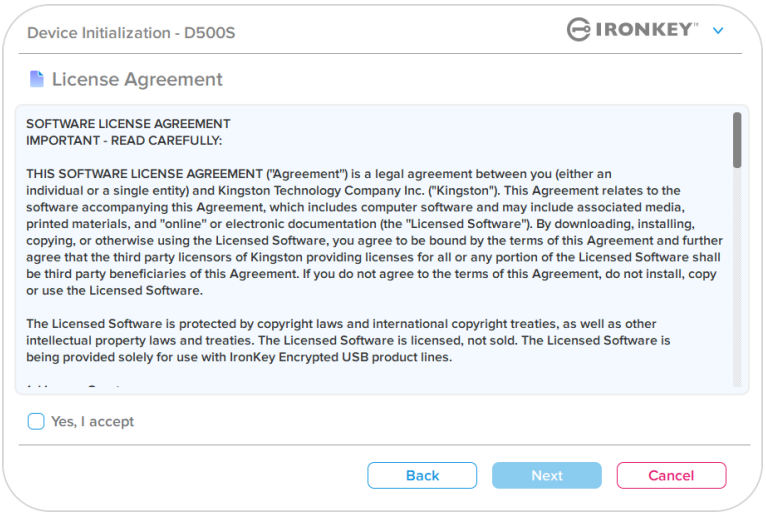
Acesso ao dispositivo (ambiente macOS)

Insira o D500S 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 'IRONKEY no computador. (*Figura 3.3*)

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

Inicialização do dispositivo (Ambiente Windows e macOS)

Idioma e EULA

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

Inicialização do dispositivo

Escolha de senha

Na tela de mensagem de Senha, você poderá criar uma senha para proteger seus dados no D500S usando os modos de senha Complexas ou de Frase-passe (*Figuras 4.3 – 4.4*). Além disso, as opções de Usuário/Admin multissenhas também podem ser habilitadas nesta tela. Antes de continuar com a escolha da senha, veja Habilitando as Senhas de Usuário / Admin abaixo para entender melhor esses recursos.

Observação: Seja o modo Complexo ou Frase-passe o escolhido, o modo não pode ser alterado a menos que o dispositivo seja restaurado.

Para começar com a escolha da senha, crie sua senha no campo de 'Senha, depois redigite-a nos campos de 'Confirmar Senha'. A senha que você criar deve seguir os seguintes critérios antes do processo de inicialização permitir que você continue:

<table>
<tr>
<td>Senha complexa
• Deve conter 8 caracteres ou mais (até 16 caracteres).

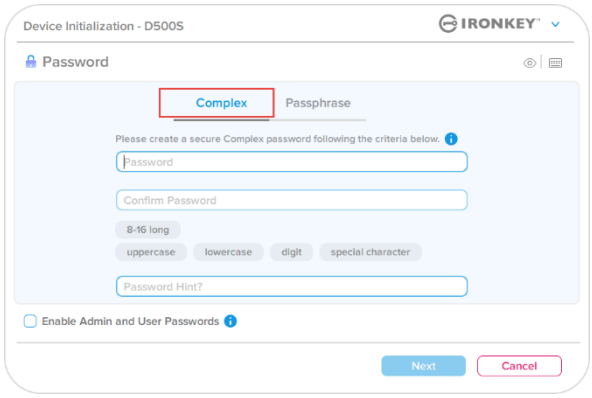
• Deve conter três (3) dos seguintes critérios:
○ Letra maiúscula
○ Letra minúscula
○ Dígito numérico
○ Caracteres especiais (!,$,&, etc.)</td>
<td> 

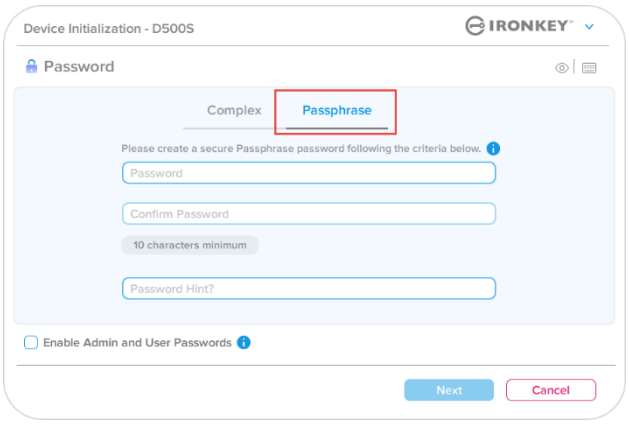
Figura 4.3 – Senha complexa</td>
</tr>
<tr>
<td>Senha de frase-passe
• Deve conter:
○ Mínimo de 10 caracteres
○ Máximo de 128 caracteres</td>
<td> 

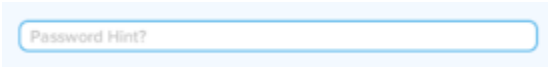
Figura 4.4 – Senha de frase-passe</td>
</tr>
<tr>
<td>Dica de senha (Opcional)
Uma Dica de senha pode ser útil para fornecer uma pista sobre a senha, se algum dia ela for esquecida.
Observação: A dica NÃO pode ser a mesma que a senha.</td>
<td> 

Figura 4.5 – Campo da dica de senha</td>
</tr>
</table>

Inicialização do dispositivo

Senhas válidas e inválidas

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

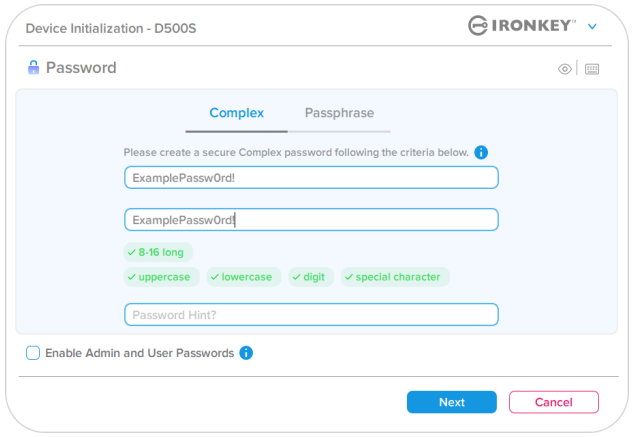


Figura 4.6a – Condição de senha complexa atendida

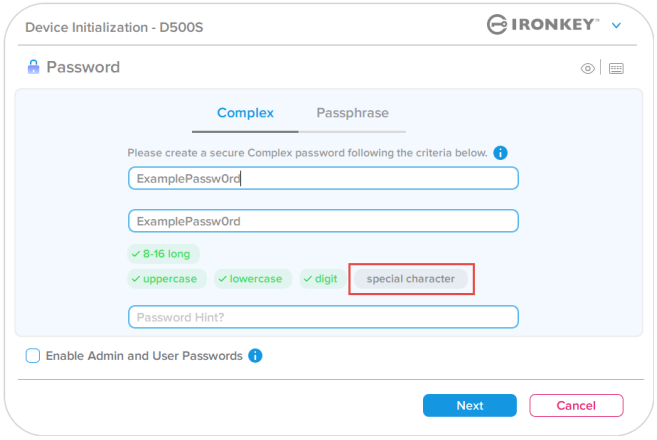


Figura 4.6b – Condição de senha complexa opcional

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

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

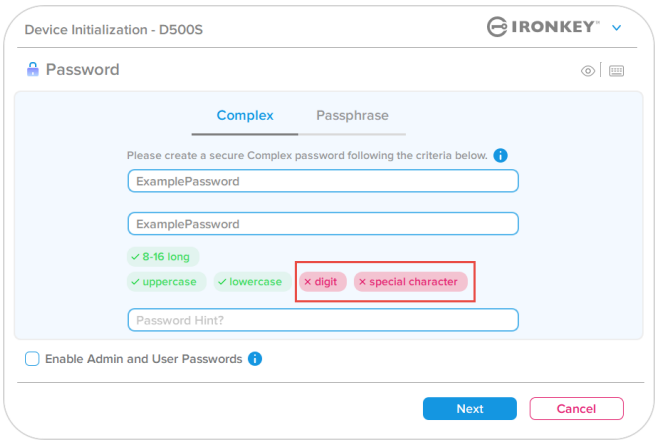


Figura 4.7 – Condições de senha não atendidas

Inicialização do dispositivo

Teclado virtual

O D500S oferece um teclado virtual que pode ser utilizado para proteção contra registros de toque do teclado (keylogger).

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

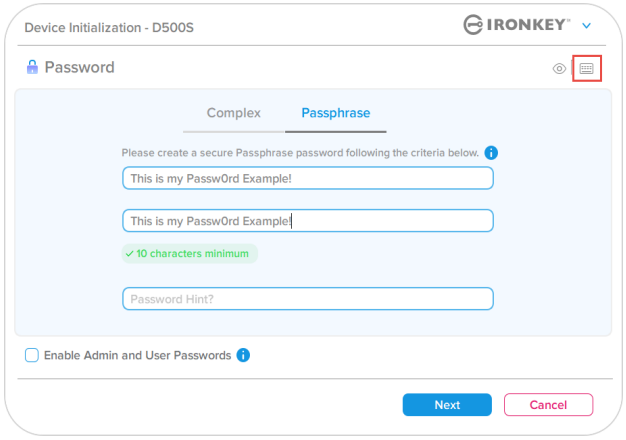


Figura 4.8 – Ativando o Teclado virtual

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

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

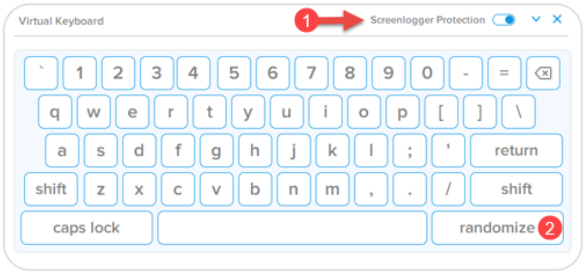


Figura 4.9 – Proteção contra registro de tela / Randomização

Inicialização do dispositivo

Botão de visibilidade de senha

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

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

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

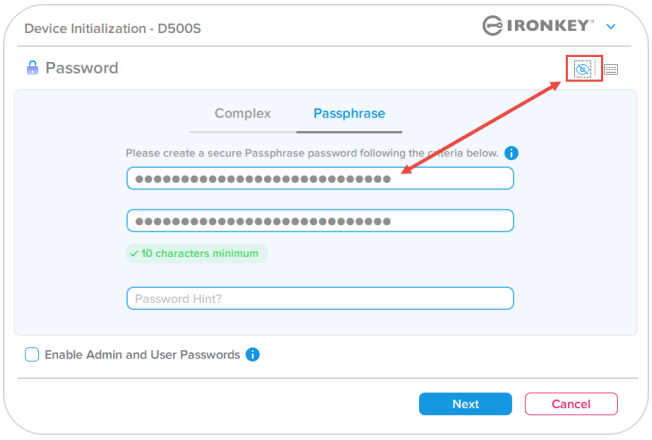


Figura 4.10 – Botão para 'ocultar' a Senha

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

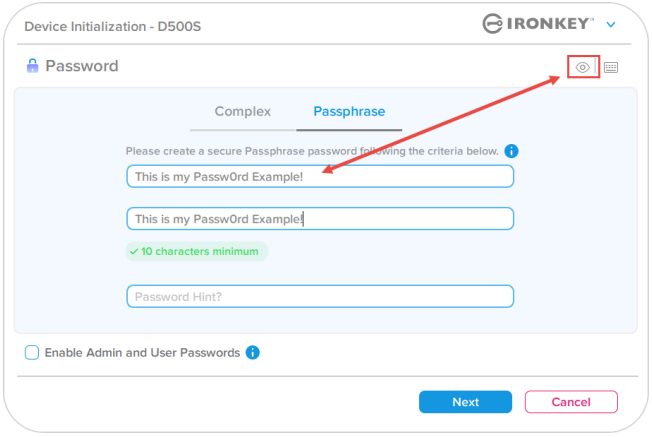


Figura 4.11 – Botão para 'exibir' a Senha

Inicialização do dispositivo

Senhas de Admin e de Usuário

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

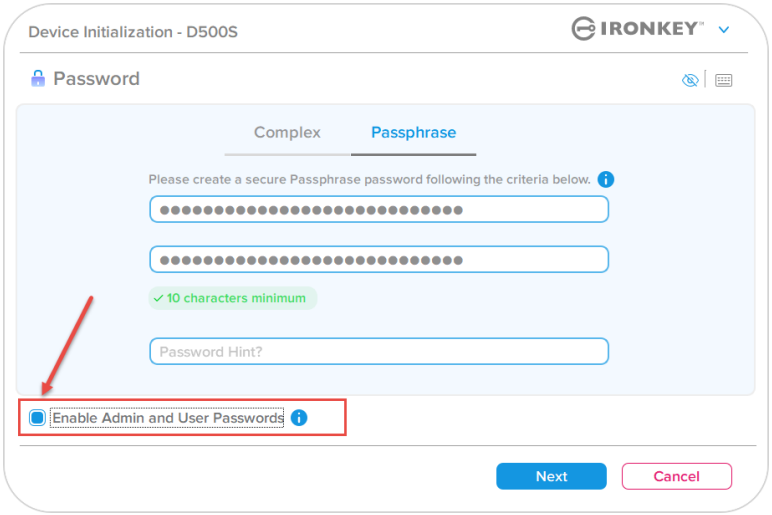
Com as **senhas de Admin e de Usuário** habilitadas, você também pode acessar:

- Configuração de partição dupla
- 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
- Senha de exclusão criptográfica

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

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

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



4.12 – Habilitando as senhas de Admin e de Usuário

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

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

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

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

Inicialização do dispositivo

Senhas de Admin e de Usuário

- Se a função de Admin foi **habilitada** na tela anterior, a tela seguinte pedirá a senha de Usuário (*Figura 4.13*)
  A **Senha de Usuário** terá capacidades limitadas em comparação com a do Admin e será discutida com mais detalhes depois neste Guia do Usuário (ver página 23)

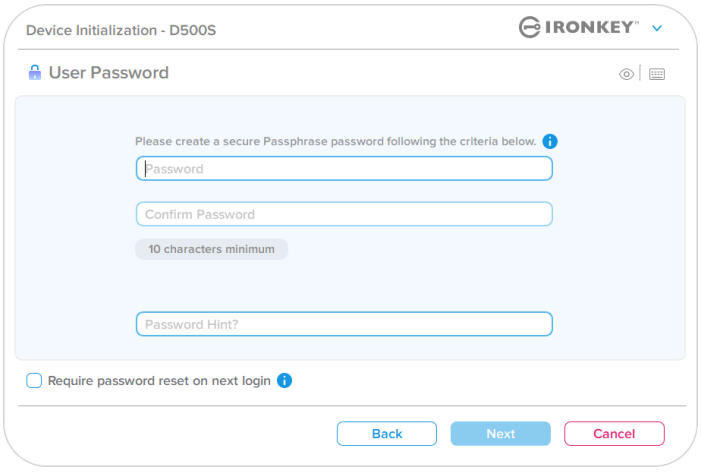


Figura 4.13 – Senha de Usuário (Admin e Usuário habilitados)

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

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

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

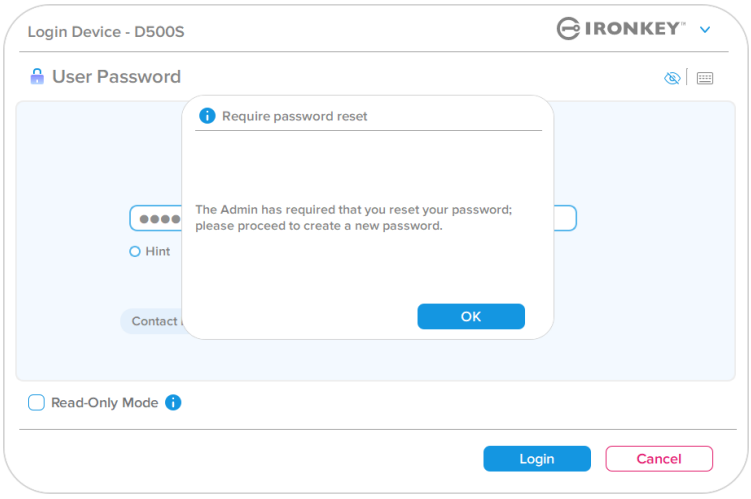


Figura 4.14 – Exigir redefinição de senha no próximo login (para Senha de Usuário)

Inicialização do dispositivo

Partições duplas

O IronKey D500S permite criar duas partições separadas e de tamanho personalizado entre o Admin e o Usuário. Se esta funcionalidade estiver ativada, o login de Admin terá acesso às partições Usuário **e** Admin, enquanto o login do Usuário terá **apenas** acesso à Partição de Usuário. Este recurso é útil para separar os privilégios de acesso a dados e arquivos de forma segura entre o Admin e o Usuário, ou pode ser usado para habilitar um armazenamento de arquivos oculto para evitar a exposição desnecessária de arquivos em sistemas não confiáveis. Os tamanhos de partição entre o Admin e o Usuário também podem ser ajustados, se desejar.

OBSERVAÇÃO: Esse recurso é *opcional* e pode ser desativado deixando a caixa "Ativar Partição Dupla" desmarcada durante a configuração (*Figura 4.15*)

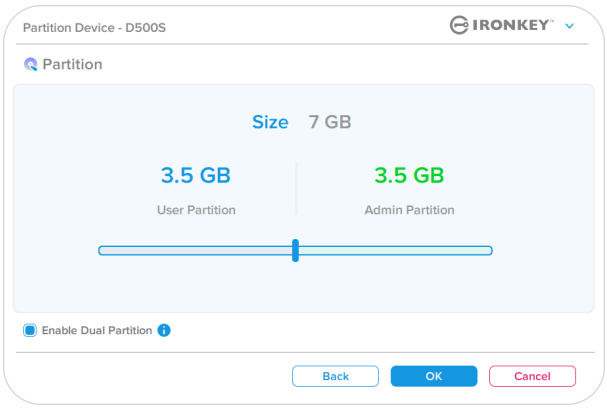


Figura 4.15 – Dispositivo de partição

Para ajustar e alocar os tamanhos de partição entre Usuário e Admin, mova o controle deslizante para a esquerda ou direita, respectivamente (*Figura 4.16*).

- As partições podem ser ajustadas em acréscimos de 0,5 GB.
- O dimensionamento da partição é baseado na capacidade total do armazenamento disponível na partição oculta.
- Por padrão, o controle deslizante de partição dupla é definido para dividir o armazenamento uniformemente entre Admin e Usuário, até que ele seja ajustado manualmente.
- O menor tamanho de partição que pode ser alocado é 1 GB.

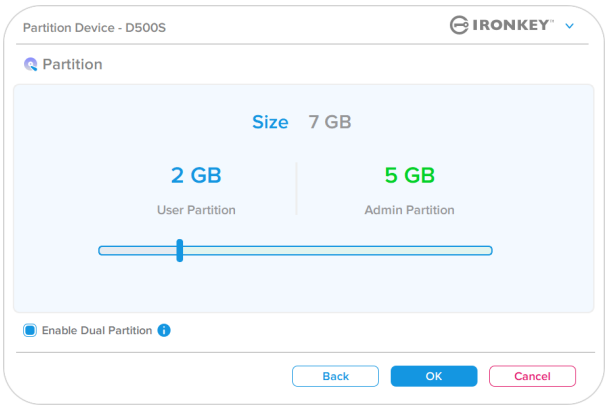


Figura 4.16 – Dispositivo de partição, controle deslizante ajustado

Login de Admin

Uma vez que o drive esteja totalmente configurado com Partições Duplas ativadas, o Login de Admin será apresentado com uma opção para desbloquear o drive para acessar a Partição do Admin OU a Partição do Usuário com cada login bem-sucedido. (*Figura 4.17*)

OBSERVAÇÃO: Apenas uma partição pode ser aberta de cada vez. As partições Usuário e Admin não podem ser desbloqueadas ao mesmo tempo.

O Login de Usuário não será apresentado com esta opção e desbloqueará automaticamente somente a Partição de Usuário.

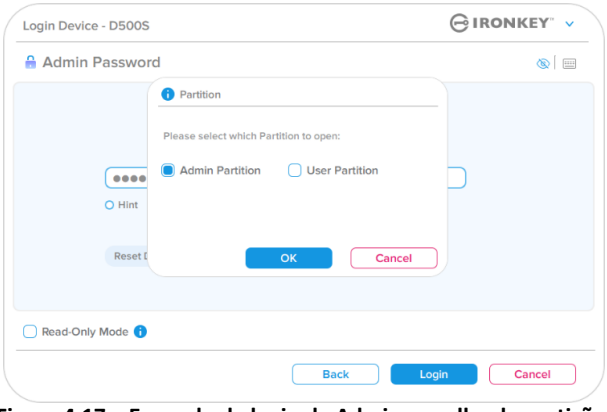


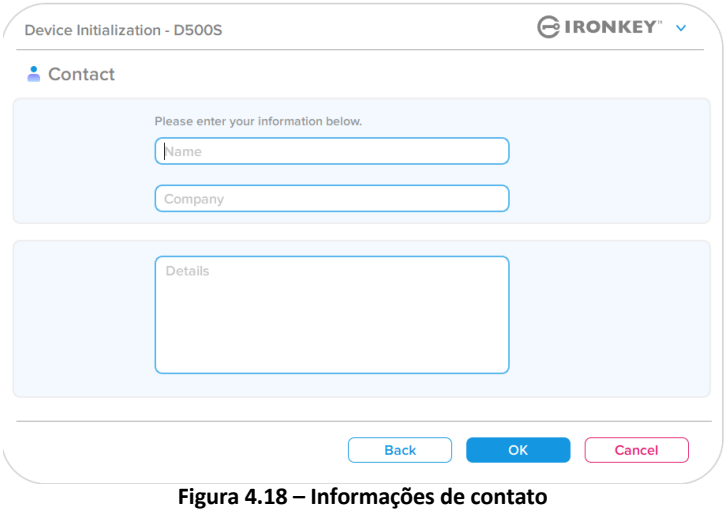
Figura 4.17 – Exemplo de login de Admin, escolha de partição

Inicialização do dispositivo

Informações de contato

Insira suas informações de contato nas caixas de texto fornecidas (ver *Figura 4.18*)

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

O campo do **'Nome'** pode conter até 32 caracteres, mas não pode conter a senha **exata**. O campo **'Empresa'** pode conter até 32 caracteres, mas não pode conter a senha **exata**. O campo **'Detalhes'** pode conter até 156 caracteres, mas não pode conter a senha **exata**.	 **Figura 4.18 – Informações de contato**

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

Uso do dispositivo (Ambiente Windows e macOS)

Login para Admin e Usuário (Admin habilitado)

Se o dispositivo for inicializado com as senhas de Admin e de Usuário (função de Admin) habilitadas, o aplicativo IronKey D500S 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 de 'Login como Admin' (mostrado abaixo) o aplicativo prosseguirá para o menu de login do Admin onde você pode fazer login como Admin para acessar os recursos e configurações do Admin (*Figura 5.2*).

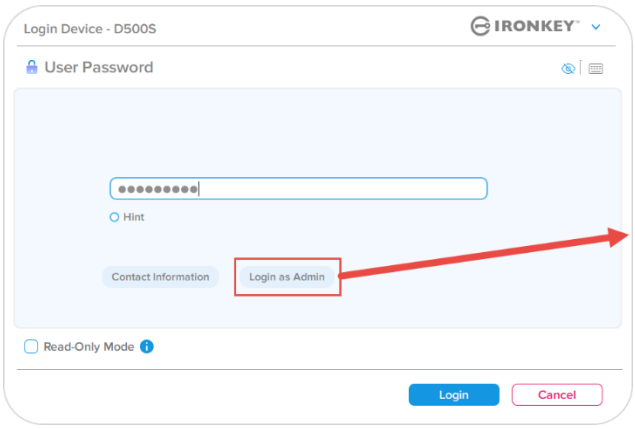


Figura 5.1 – Login de Senha de Usuário (Admin habilitado)

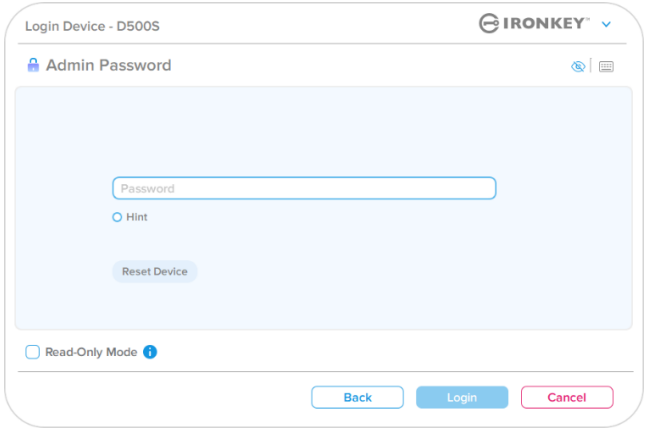


Figura 5.2 – Login de senha do Admin

Login para modo Somente Usuário (Admin não habilitado)

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

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

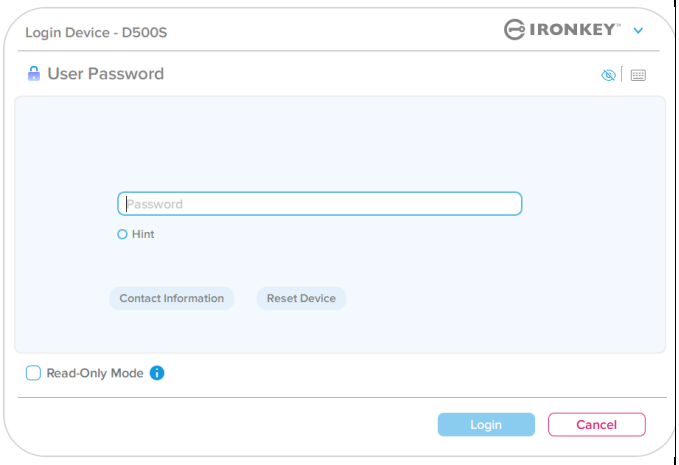


Figura 5.3 – Login de Senha de Usuário (Admin não habilitado)

Uso do dispositivo

Desbloqueando no modo Somente Leitura

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

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

Para desbloquear o dispositivo no Modo Somente Leitura:

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

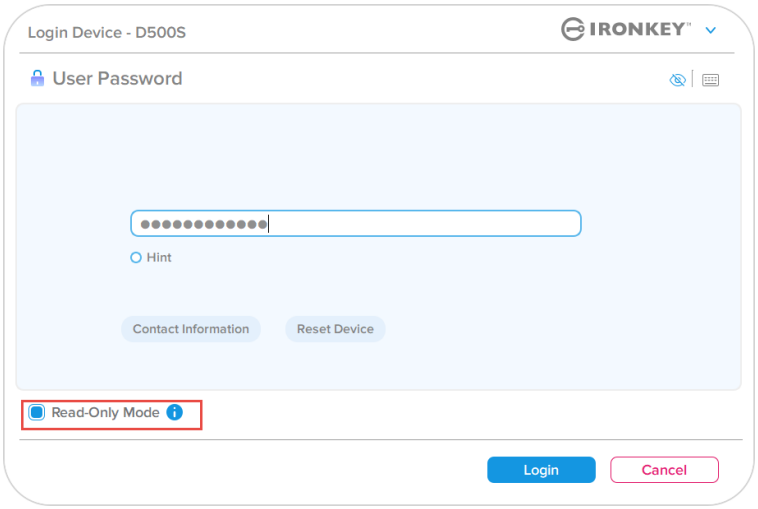


Figura 5.4 – Modo Somente Leitura

Se você deseja desbloquear o dispositivo com acesso total de leitura/gravação à partição de dados segura, você deve desligar o D500S e entrar de novo, deixando a caixa de marcação 'Modo Somente Leitura' desmarcada.

Observação: As opções do Admin do D500S 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 31 para mais detalhes).

Uso do dispositivo

Proteção de ataque de força bruta

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

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

Admin/Usuário habilitado	**Proteção de Força Bruta Comportamento do dispositivo (10 tentativas de senha incorretas)**	**Apagar dados e Restaurar dispositivo?**
Senha de Usuário	Bloqueio de senha. Fazer login como Admin ou usar senha de Recuperação Única para redefinir a senha de Usuári	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**

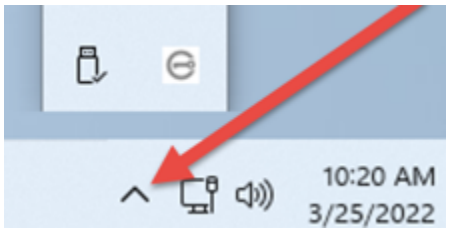
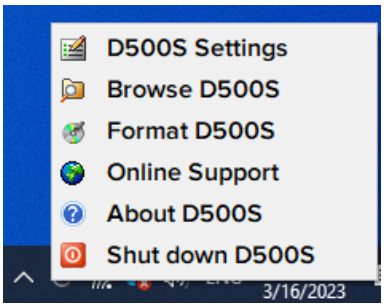
* Depois que você fizer a autenticação no dispositivo corretamente, o contador de erros de login será reiniciado em relação ao método de Login foi utilizado. A exclusão criptográfica apagará todas as senhas, dados e chaves de criptografia **– seus dados serão perdidos para sempre.**

Acessar meus arquivos seguros

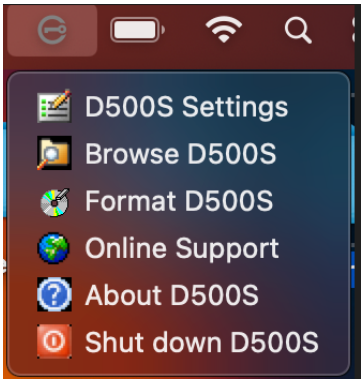
Depois de desbloquear o dispositivo, você pode acessar seus arquivos seguros. Os arquivos são automaticamente criptografados e descriptografados quando você salva ou abre os arquivos no drive. Esta tecnologia gera a conveniência de trabalhar como você faria normalmente com um drive regular, enquanto fornece uma segurança forte e ininterrupta.
Dica: Você também pode acessar seus arquivos clicando com o botão direito no **Ícone IronKey** na barra de tarefas do Windows e clicando em **Browse (Navegar) D500S** (*Figura 6.2*)

Opções do dispositivo – (Ambiente Windows)

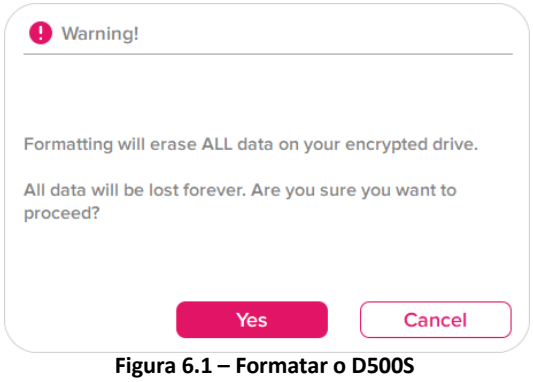
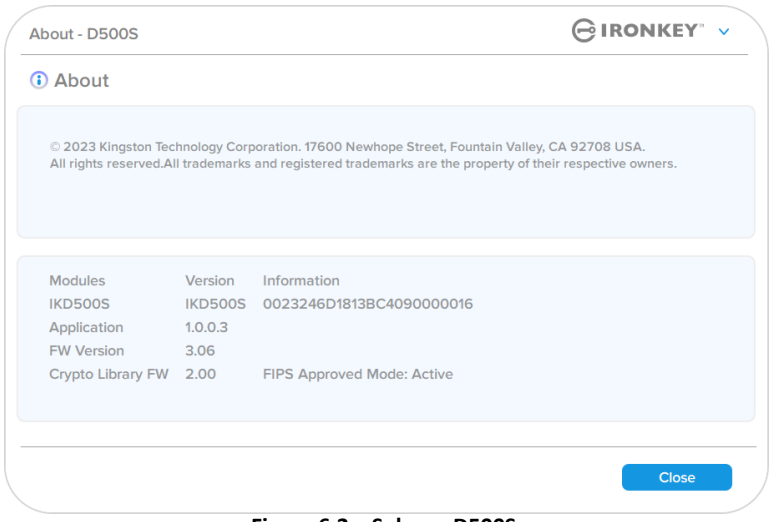
Enquanto você estiver logado no dispositivo, haverá um ícone IronKey localizado no canto direito da janela. Clicar com o botão direito no Ícone IronKey abrirá o menu de seleção para opções do drive disponíveis (*Figura 6.2*). Detalhes sobre essas opções do dispositivo podem ser encontradas nas Páginas 21-25 deste manual.

• Enquanto você estiver logado no dispositivo, haverá um ícone IronKey localizado no canto direito da janela (*Figura 6.1*)	 **Figura 6.1 – Ícone IronKey na barra de tarefas**
• Clicar com o botão direito no Ícone IronKey abrirá o menu de seleção para opções do drive disponíveis (*Figura 6.2*). Detalhes sobre essas opções do dispositivo podem ser encontradas nas páginas 19-23 deste manual.	 **Figura 6.2 – Clique com o botão direito no ícone IronKey para opções do dispositivo**

Opções do dispositivo – (Ambiente macOS)

• Enquanto você estiver logado no dispositivo, haverá um ícone IronKey D500S localizado no menu do macOS visto na Figura 6.3 que abrirá as opções de dispositivo disponíveis. Detalhes sobre essas opções do dispositivo podem ser encontradas nas Páginas 19-23 deste manual.	 **Figura 6.3 – Menu de opções do dispositivo/Ícone da barra de menu do macOS**

Opções do dispositivo

Configurações do D500S:	• Alterar senha de login, informações de contato e outras configurações. (Mais detalhes sobre configurações do dispositivo podem ser encontrados na seção 'Configurações do D500S' deste manual).
Browse (Navegar) D500S:	• Permite que você visualize seus arquivos seguros.
Formatar o D500S: Permite que você formate a partição de dados segura. (Aviso: Todos os dados serão apagados.) (*Figura 6.1*) **Observação:** A autenticação da senha será exigida para formatar.	 **Figura 6.1 – Formatar o D500S**
Suporte on-line:	• Abre seu navegador de internet e vai para http://www.kingston.com/support onde você pode acessar as informações de suporte adicionais.
Sobre o D500S: Fornece detalhes específicos sobre o D500S, incluindo Aplicação, Firmware e Informações de número de série (*Figura 6.2*) **Observação:** O número de série único do drive estará na 'Coluna de informações'	 **Figura 6.2 – Sobre o D500S**
Desligar o D500S:	• Encerra de modo apropriado o D500S, permitindo que seja removido com segurança do seu sistema.

Configurações do D500S

Configurações do Admin

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

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

OBSERVAÇÃO: Detalhes adicionais das Opções do Admin podem ser encontradas começando na página 26.

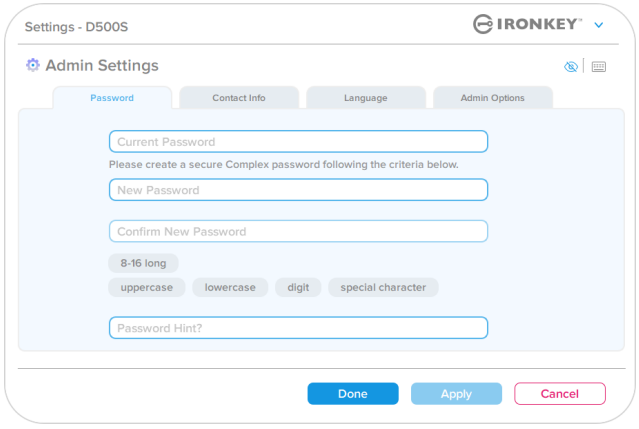


Figura 7.1 – Opções de Senha

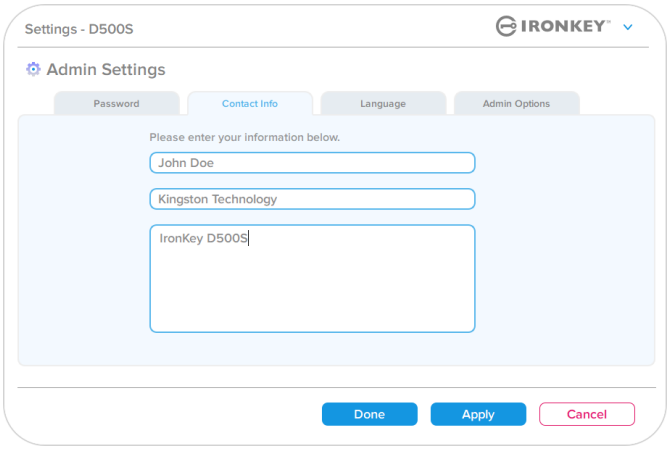


Figura 7.2 – Informações de contato

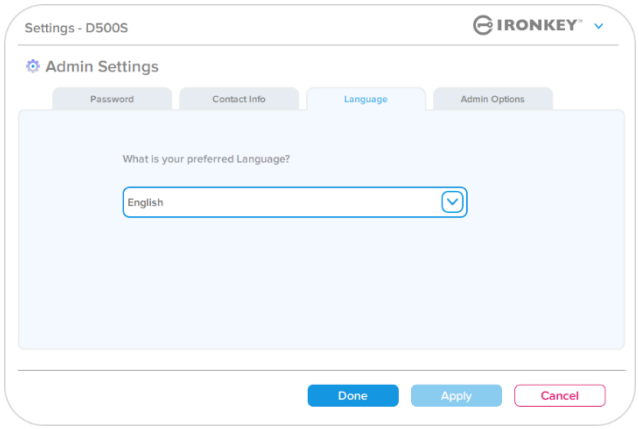


Figura 7.3 – Opções de idioma

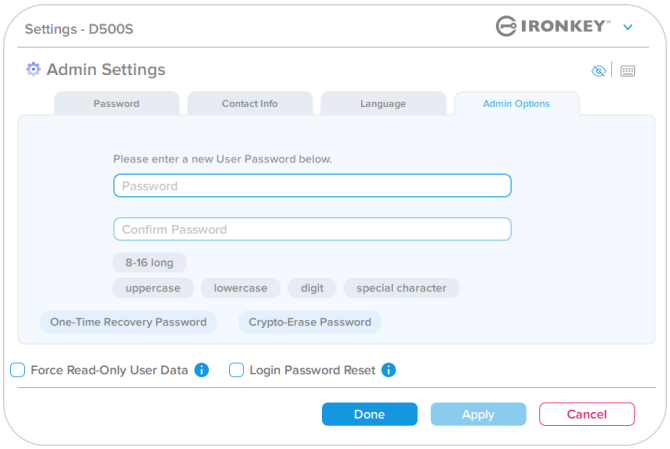
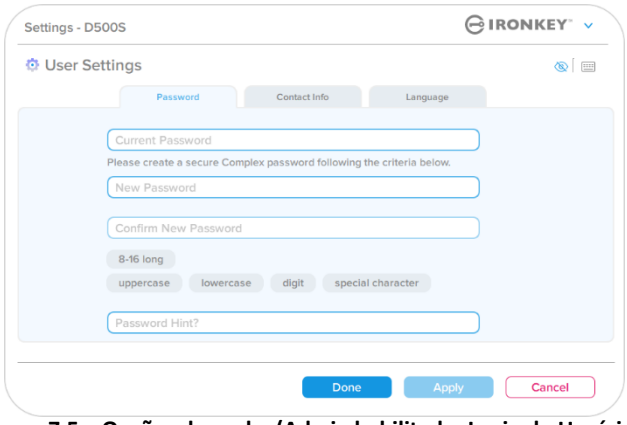
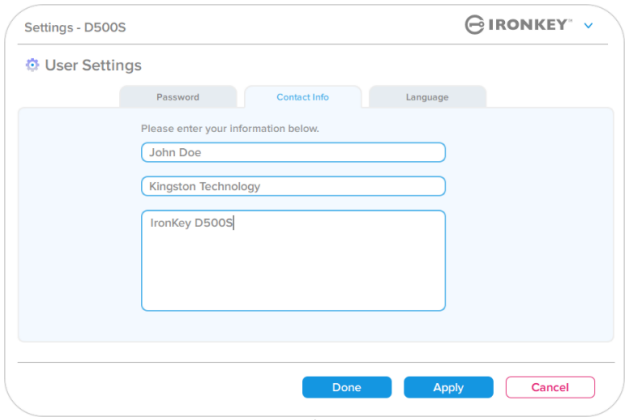
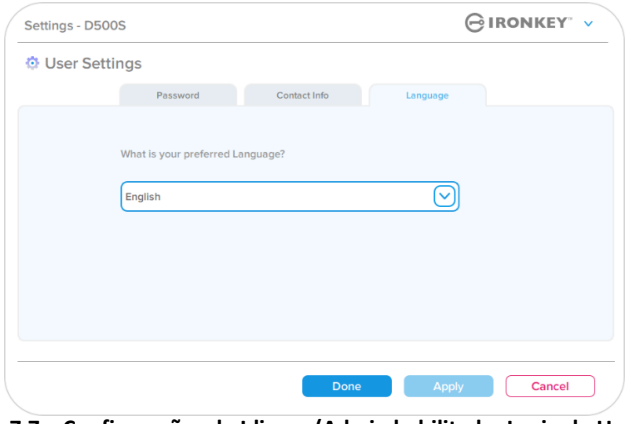


Figura 7.4 – Opções do Admin

Configurações do D500S

Configurações do Usuário: Admin habilitado

O login do Usuário limita o acesso às seguintes configurações:

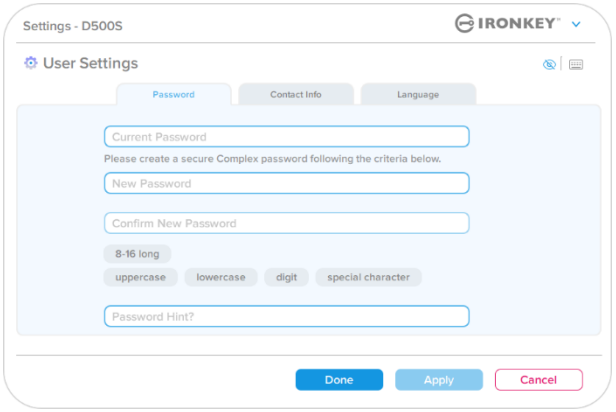
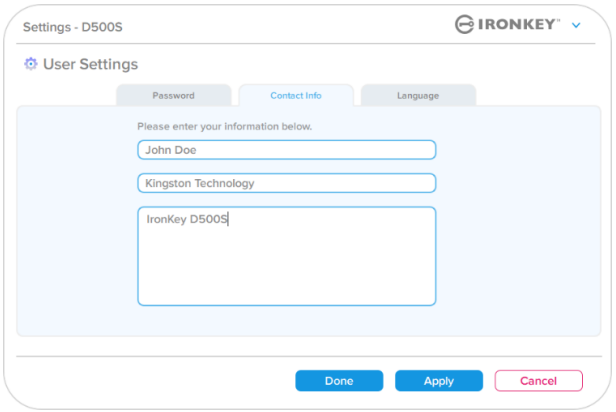
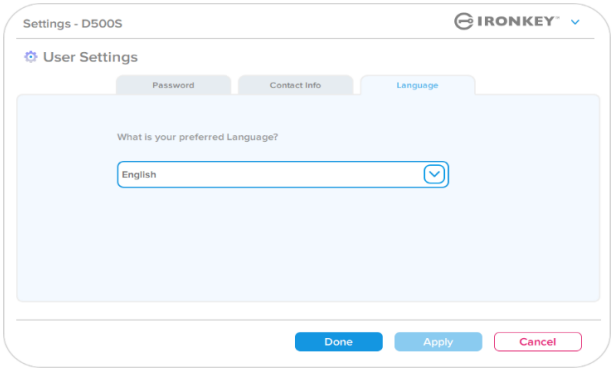
Senha: Permite que você altere sua própria senha de Usuário e/ou dica (*Figura 7.5*)	 **Figura 7.5 – Opções de senha (Admin habilitado: Login do Usuário)**
Informações de contato: Permite que você adicione/visualize/ altere suas informações de contato (*Figura 7.6*)	 **Figura 7.6 – Informações de contato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

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

Configurações do D500S

Configurações do Usuário: Admin não habilitado

Como mencionado anteriormente, inicializar o D500S sem ativar as senhas de 'Admin e Usuário' configurará o drive em uma **Senha Única, configuração de Usuário Único (modo Somente Usuário)**. Esta configuração não possui acesso a qualquer recurso ou opção do Admin. Esta configuração terá acesso às seguintes configurações do D500S:

Senha: Permite que você altere sua própria senha de Usuário e/ou dica (*Figura 7.8*)	 **Figura 7.8 – Opções de Senha (Modo Somente Usuário)**
Informações de contato: Permite que você adicione/visualize/ altere suas informações de contato (*Figura 7.9*)	 **Figura 7.9 – Informações de contato (Modo Somente Usuário)**
Idioma: Permite que você altere sua seleção de idioma atual (*Figura 7.10*)	 **Figura 7.10 – Definições de Idioma (Modo Somente Usuário)**

Configurações do D500

Alterar e Salvar configurações

- Sempre que as configurações forem alteradas nas Configurações do D500S (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 (*Figura 7.11*).

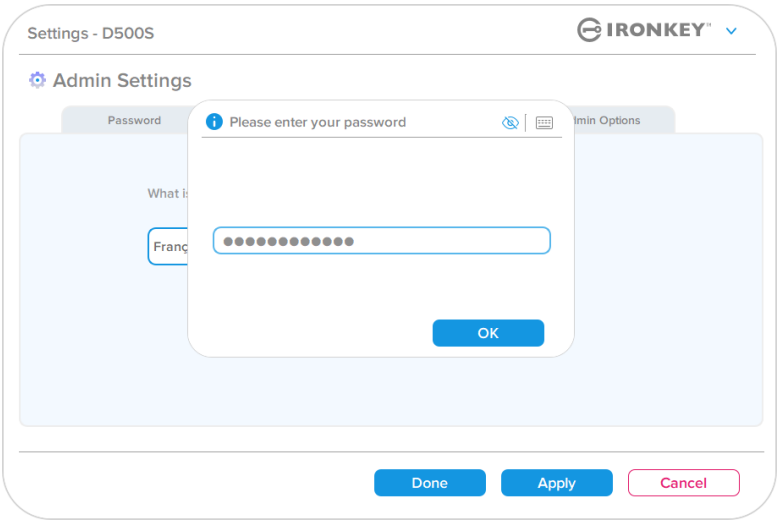


Figura 7.11 – Tela de alerta de Senha para salvar as alterações de configurações do D500S

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 fechará a caixa 'Insira sua Senha' e voltará para o menu de configurações do D500S.

Recursos do Admin

Opções disponíveis para redefinir a senha de Usuário

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

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

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

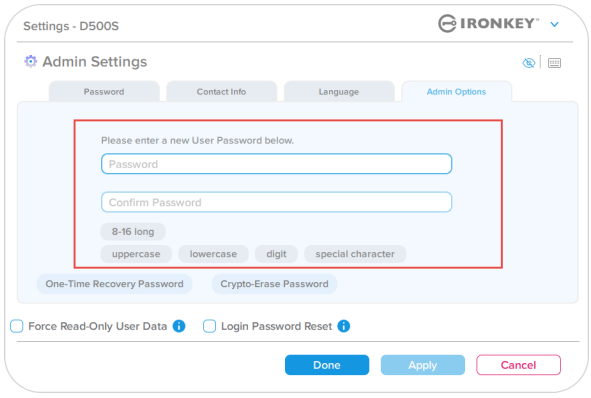


Figura 8.1 – Redefinição de Senha de Usuário/Opções do Admin

Redefinição da senha de login:
Habilitar a Redefinição de senha de login **forçará o Usuário a fazer login usando uma senha temporária definida pelo Admin** e depois mudar para uma senha de sua escolha. Isso é útil quando o drive é dado para outra pessoa usar. (Ver *Figuras 8.2 e 8.3*)

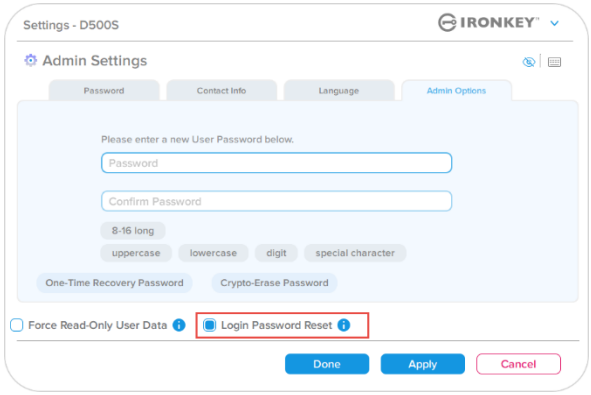


Figura 8.2 – Botão de redefinição de senhas de login

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

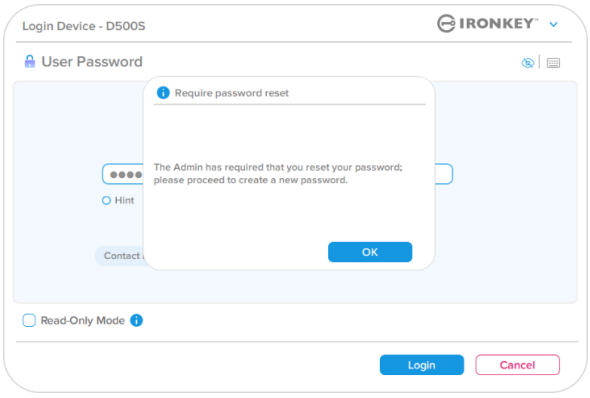


Figura 8.3 – Notificação de redefinição depois que a senha de Usuário for inserida

Recursos do Admin

Senha de recuperação única

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

Senha de recuperação única

Passo 1: O recurso de Senha de recuperação única é muito útil, a senha de uso único que pode ser habilitada para ajudar a recuperar e redefinir a senha de Usuário caso a senha de Usuário seja esquecida. Clique no botão 'Senha de recuperação única' no menu de opções do Admin para iniciar. (*Figura 8.4*)

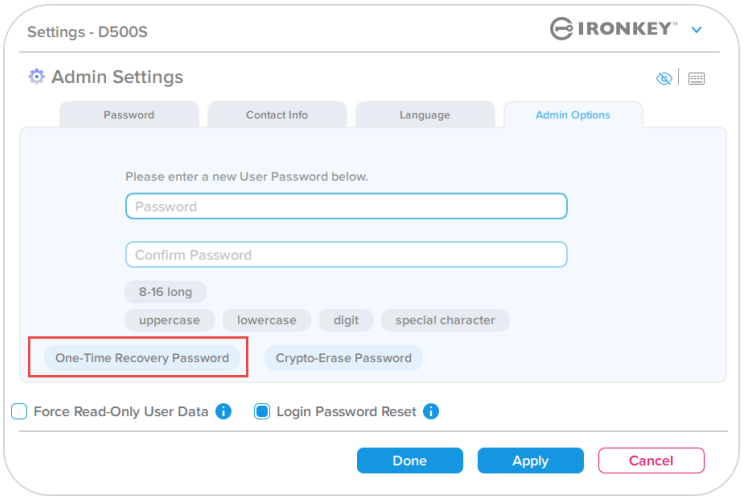


Figura 8.4 – Botão de Senha de recuperação única

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

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

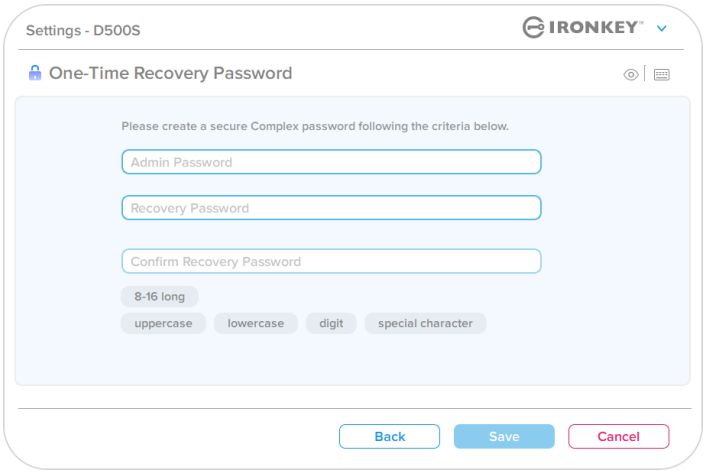


Figura 8.5 – Configuração de Senha de recuperação única

Recursos do Admin

Usando a senha de recuperação única

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

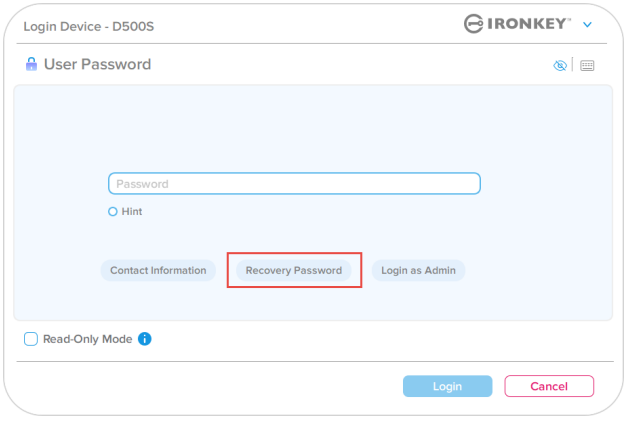


Figura 8.6 – Botão de Senha de recuperação

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

Importante: A senha de recuperação única também utiliza um recurso de segurança integrado que monitora o número de tentativas erradas de login, **depois de 10 tentativas de Login incorretas com a senha de recuperação única, a senha será desabilitada**, e precisará ser reabilitada fazendo login no drive como Admin. (ver páginas 19 e 33 para mais detalhes)

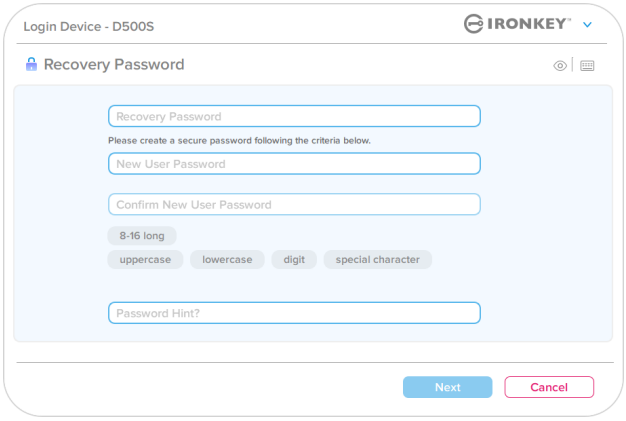


Figura 8.7 – Menu de Senha de recuperação

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

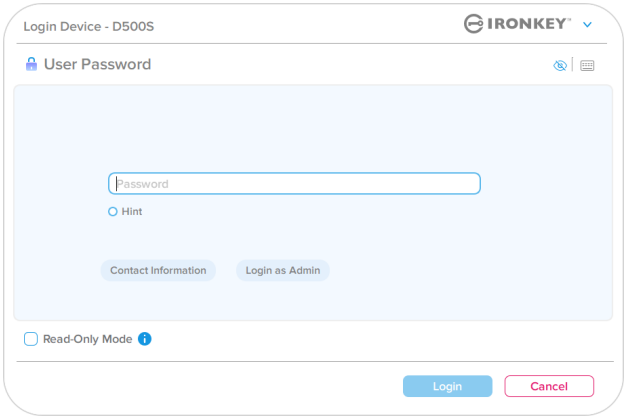


Figura 8.8 – Tela de login de senha do Usuário mostrando que o botão de Senha de Recuperação desaparece após uma utilização bem sucedida.

Recursos do Admin

Senha de exclusão criptográfica

O IronKey D500S está equipado com um recurso exclusivo de senha de exclusão criptográfica que foi projetado para proteger e defender contra situações de comprometimento físico, apagando com segurança o conteúdo do seu drive quando usado, deixando-o como se nunca tivesse quaisquer dados gravados no drive. Quando esse recurso é ativado e o drive é desbloqueado com a senha de exclusão criptográfica, ele executará efetivamente uma discreta exclusão criptográfica no drive D500S e abrirá o drive no modo de fábrica com uma partição de Usuário vazia. A chave de criptografia anterior será excluída e uma nova chave de criptografia de dispositivo será criada para ocupar seu lugar. ***Use com Cuidado***

- Para **ativar** esse recurso, clique no botão Senha de exclusão criptográfica localizado na guia Opções do Admin:

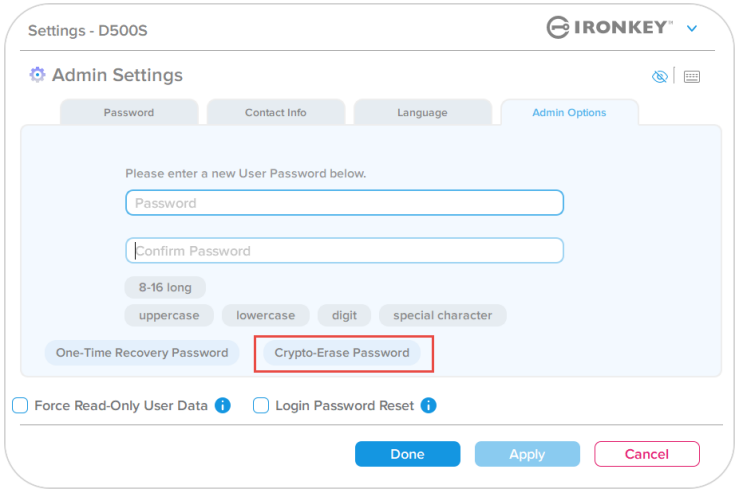


Figura 8.9 – Habilitar a senha de exclusão criptográfica

Criar uma senha de exclusão criptográfica:

- As regras de senha serão baseadas nas quais o drive foi inicializado inicialmente (Complexa ou Frase-passe)
- A senha de Admin será necessária para validação.

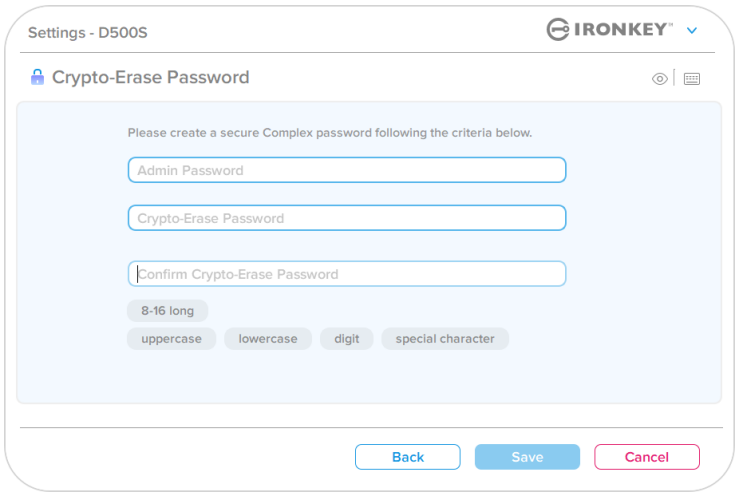


Figura 8.10 – Criar a senha de exclusão criptográfica

Recursos do Admin

Usando a senha de exclusão criptográfica

Quando a senha de exclusão criptográfica for usada, as senhas de Admin e Usuário anteriores serão excluídas e a senha de exclusão criptográfica tomará o seu lugar. Além disso, todas as configurações anteriores serão excluídas juntamente com a exclusão permanente de todos os dados armazenados no drive e o drive será convertido em uma configuração de modo Somente Usuário.

Para utilizar a senha de exclusão criptográfica:

1. Inicie o IronKey.exe para executar o aplicativo IronKey

2. Na tela de login da senha do Usuário, pressione '**CTRL + ALT +C**' para ativar a entrada da senha de exclusão criptográfica. Se feito corretamente, uma barra azul mais espessa será perceptível na tela de entrada da senha, indicando que a senha de exclusão criptográfica está pronta para entrar. (*Figura 8.11*)

OBSERVAÇÃO: A senha de exclusão criptográfica só pode ser ativada na tela de login da senha do Usuário.

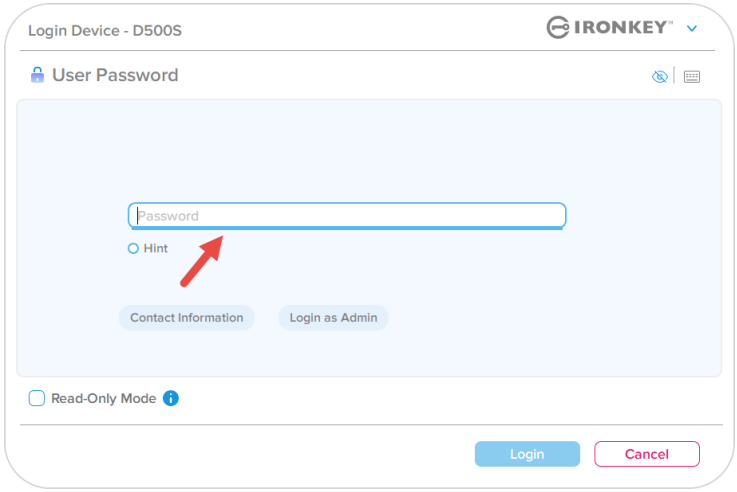


Figura 8.11 – Exclusão criptográfica ativada, com barra azul grossa

Uma vez que a senha de exclusão criptográfica for utilizada, o drive agora continuará apagando o drive de todo o conteúdo e uma única partição vazia aparecerá agora. O drive agora estará em um estado de modo Somente Usuário e a senha de exclusão criptográfica será a senha usada para fazer login no drive até que seja restaurado.

Importante: Este recurso apagará todos os dados no drive e qualquer coisa armazenada anteriormente será perdida para sempre, prossiga com cautela.

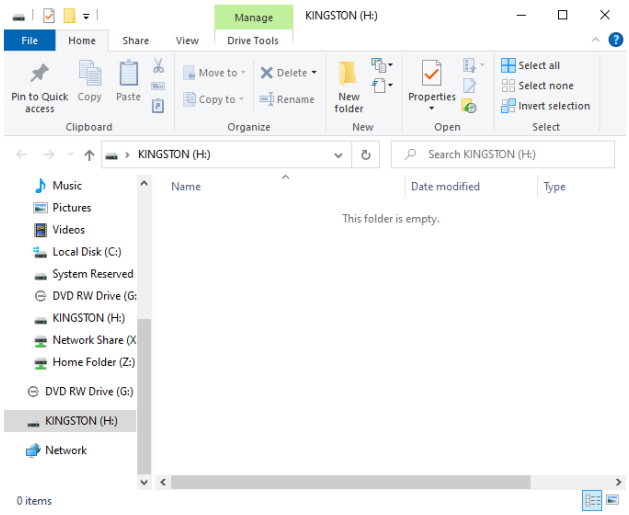


Figura 8.12 – Limpeza do drive após o uso da senha de exclusão criptográfica

Recursos do Admin

Force os dados de usuário para Somente Leitura

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

- Para habilitar o Forçar Somente Leitura para os dados do Usuário, clique na caixa e clique em 'Aplicar'. (*Figura 8.13*)

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

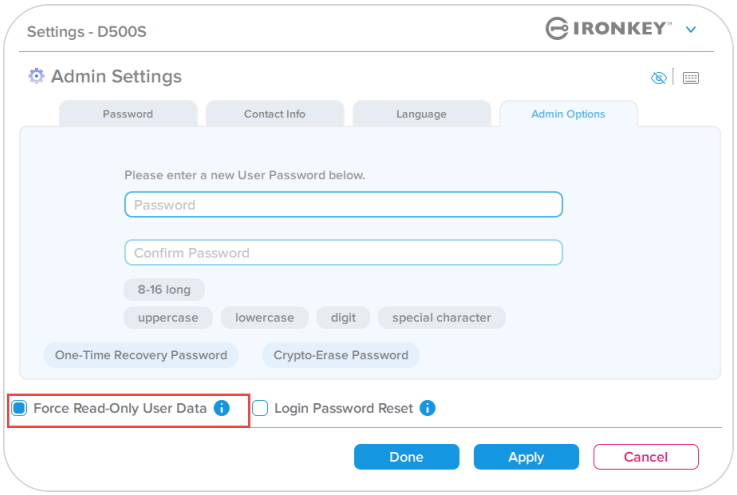


Figura 8.13 – Habilitar 'Forçar dados de usuário para Somente Leitura' (A Senha do Admin será exigida para aplicar as alterações)

- Assim que for habilitada, a caixa de botão do **'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 8.14*)

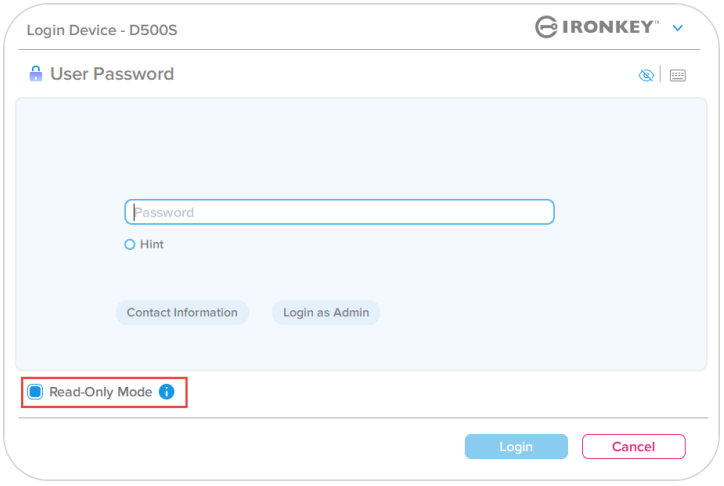


Figura 8.14 – Modo Somente Leitura é habilitado de maneira forçada para o usuário e só pode ser desabilitado pelo Admin

Ajuda e Resolução de Problemas

Bloqueio do dispositivo

O D500S inclui um recurso de segurança que previne acesso não autorizado à partição de dados quando um número máximo de tentativas erradas de login **consecutivas** (abreviado como MaxNoA) foi feito. A configuração padrão de fábrica tem um valor pré-configurado de 10 (nº de tentativas) para cada método de login (Senha de recuperação única/Usuário/Admin).

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

1. Um login bem-sucedido antes de atingir o MaxNoA

2. Atingindo o MaxNoA e realizando um bloqueio de dispositivo ou formatação de dispositivo dependendo de como o drive for configurado.

- Se uma senha incorreta for inserida, uma mensagem de erro vai aparecer em vermelho logo acima do campo de entrada de senha, indicando uma falha no login. (*Figura 9.1*)

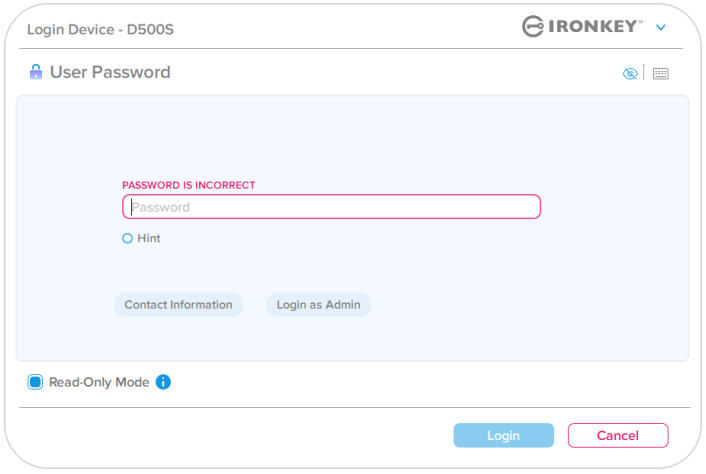


Figura 9.1 – Mensagem de senha incorreta

- Quando a **7ª** tentativa errada for feita, você verá uma mensagem de erro adicional indicando que você tem mais 3 tentativas antes de chegar ao MaxNoA (que é 10 por padrão). (*Figura 9.2*)

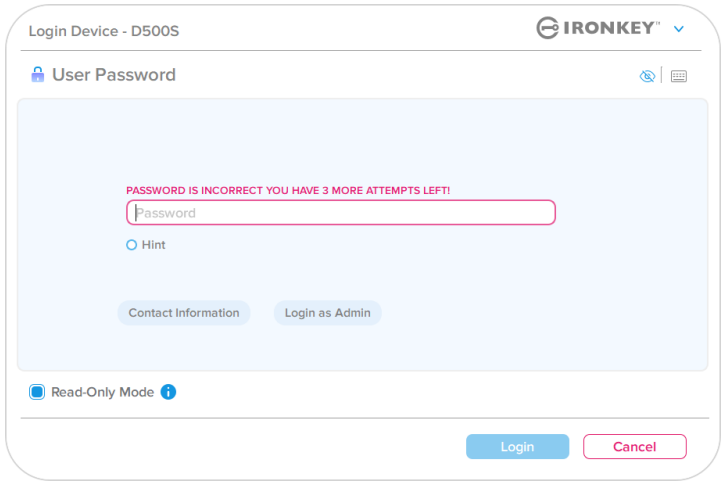


Figura 9.2 – 7ª tentativa de senha incorreta

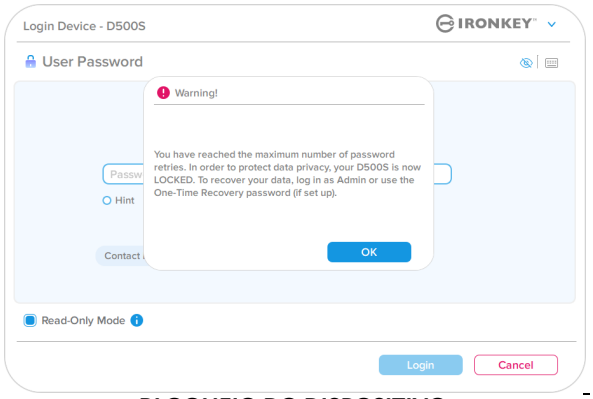
Ajuda e Resolução de Problemas

Bloqueio do dispositivo

Importante: Depois da **10ª** e última tentativa de login errada, dependendo de como o dispositivo foi configurado e método de login utilizado, (Senha de recuperação única, Usuário ou Admin) o dispositivo vai fechar, exigindo que você faça login por um método alternativo (se aplicável) ou uma Restauração de Dispositivo que **formatará os dados e todos os dados no drive serão perdidos para sempre**. Estes comportamentos também são mencionados na página 19 deste Manual do Usuário.

As Figuras 9.3 – 9.6 abaixo demonstram o comportamento visual do 10º e último login errado de cada método de senha de login:

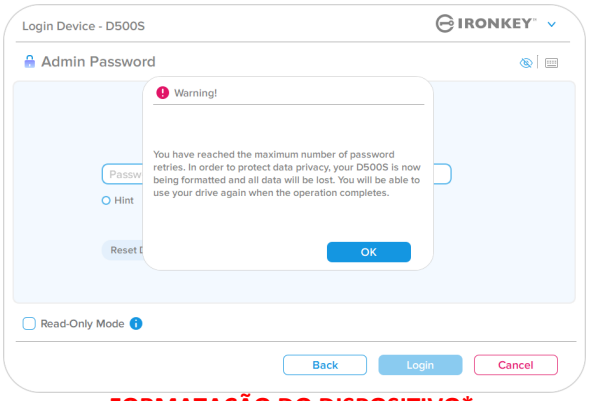
Senha de Usuário: (Admin/Usuário habilitado)



BLOQUEIO DO DISPOSITIVO

Figura 9.3

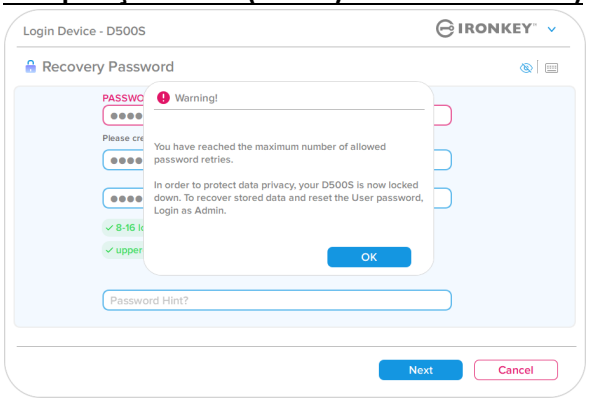
Senha do Admin (Admin/Usuário habilitado)



FORMATAÇÃO DO DISPOSITIVO*

Figura 9.4

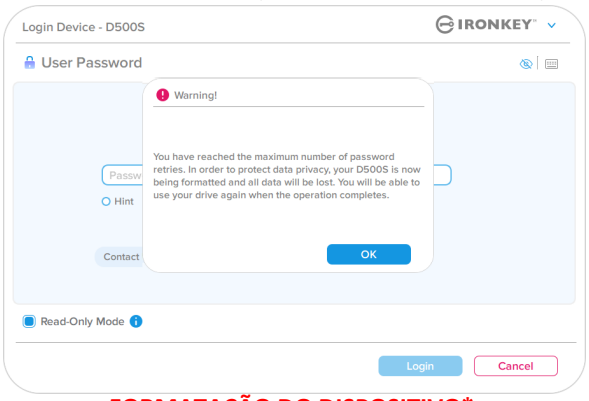
Recuperação única: (Admin/Usuário habilitado)



BLOQUEIO DO DISPOSITIVO

Figura 9.5

Senha de Usuário (Admin NÃO habilitado)



FORMATAÇÃO DO DISPOSITIVO*

Figura 9.6

Essas medidas de segurança impedem que alguém (que não tenha a sua senha) faça incontáveis tentativas de login e consiga acesso aos seus dados confidenciais (também conhecido como ataque de força bruta). Se você for o proprietário do D500S e esquecer sua senha, as mesmas medidas de segurança serão aplicadas, incluindo a formatação do dispositivo. * Para mais sobre este recurso, veja *'Restaurar Dispositivo'* na página 25.

**Observação: Uma formatação de dispositivo apagará TODAS as informações armazenadas na partição de dados segura do D500S.*

Ajuda e Resolução de Problemas

Restaurar dispositivo

Se você esqueceu a sua senha ou precisa restaurar seu dispositivo, você pode clicar no botão *'Restaurar Dispositivo'* que aparece em um dos dois lugares dependendo de como o drive está configurado (no menu de Senha de Login do Admin se o Admin/Usuário estiver habilitado, ou no menu de Login de 'Senha de Usuário' se o modo Admin/Usuário não estiver habilitado) quando o iniciador do D500S for executado (ver *Figura 9.7 e 9.8*)

- Esta opção vai permitir que você crie uma nova senha, mas para proteger a privacidade de seus dados, o D500S será formatado. Isso significa que todos os seus dados serão apagados no processo.*

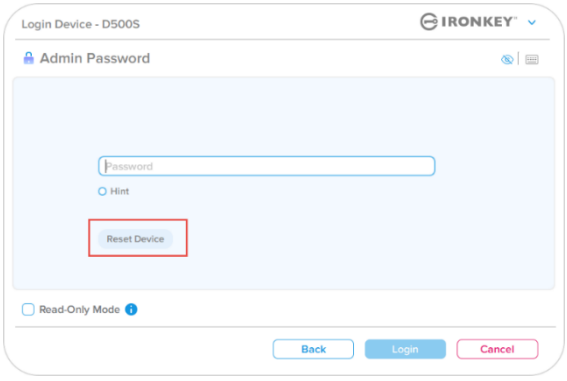


Figura 9.7 – Senha do Admin: Botão para Restaurar Dispositivo

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

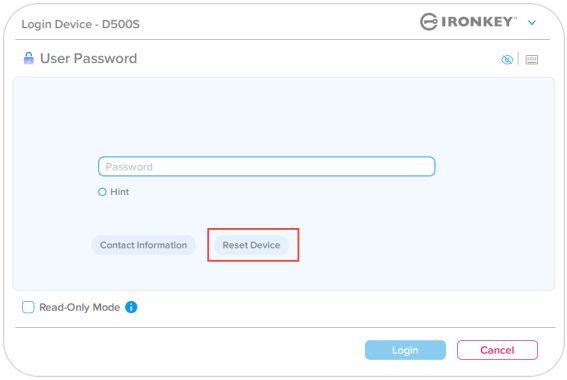


Figura 9.8 – Senha de Usuário (Admin/Usuário não habilitado) Restaurar Dispositivo

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

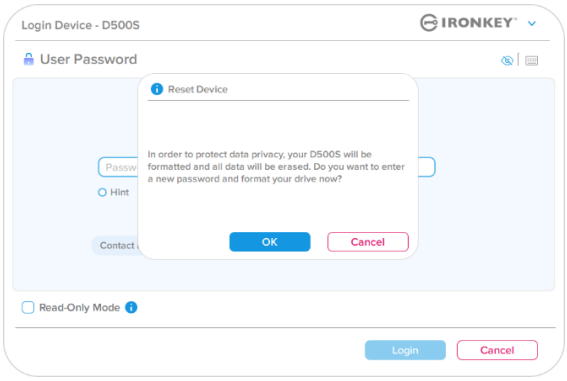


Figura 9.9 – confirmação para Restaurar Dispositivo

Ajuda e Resolução de Problemas

Conflito de letra do drive: Sistemas operacionais Windows

- Como mencionado na seção de *'Requisitos do Sistema'* deste manual (na página 3), o D500S 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 D500S 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 D500S precisa de duas letras de drive consecutivas DEPOIS do último disco físico que aparece antes do 'intervalo' nas atribuições de letra do drive (ver *Figura 9.10*.) Isto NÃO está relacionado com compartilhamentos de rede porque eles são específicos aos perfis de usuário e não ao próprio perfil de hardware de sistema, aparecendo assim disponível no Sistema Operacional.

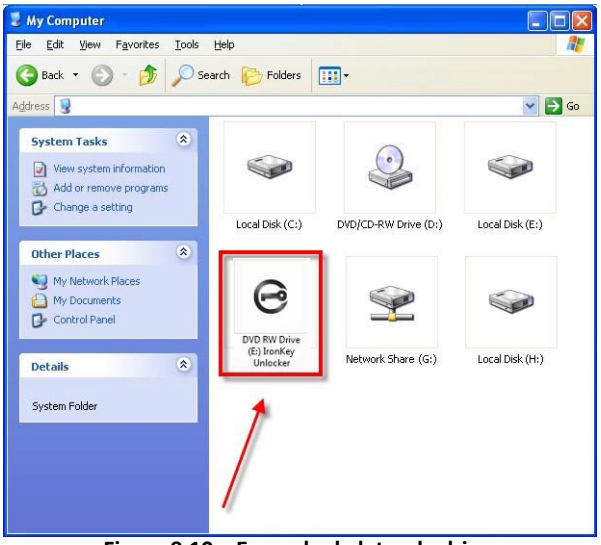


Figura 9.10 – Exemplo de letra de drive

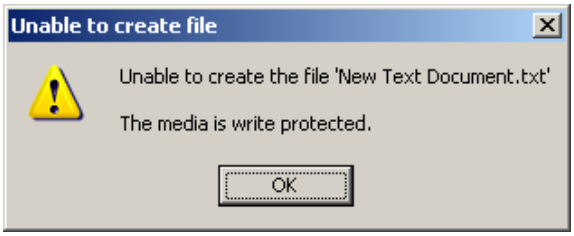
Neste exemplo, (*Figura 9.10*), o D500S utiliza o drive F:, que é a primeira letra de drive disponível após o drive E: (o último disco físico antes do intervalo de letra de drive.) Como a letra G: é um compartilhamento de rede e não faz parte do perfil de hardware, o D500S pode tentar utilizá-lo como sua segunda letra de drive, causando um conflito.

Se não existirem compartilhamentos de rede no seu sistema e o D500S continuar não iniciando, é possível que um leitor de cartões, um disco removível ou outro dispositivo previamente instalado esteja mantendo a letra de unidade atribuída e causando o conflito.

Observe que o Gerenciamento de Letra de Drive, ou DLM, melhorou significativamente no Windows 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 para mais assistência.

Ajuda e Resolução de Problemas

Mensagens de Erro

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.	 **Figura 9.11 – Erro ao criar arquivo**
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.	 **Figure 9.12 – Erro ao Copiar arquivo ou Erro de pasta**
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.	 **Figure 9.13 – Erro ao excluir arquivo ou Erro de 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 D500S e entrar de novo, deixando a caixa de marcação 'Modo Somente Leitura' desmarcada antes de fazer login.

Uso do dispositivo (Ambiente Linux)

Com as várias distribuições do Linux disponíveis hoje, a 'aparência' de suas interfaces pode variar de uma versão para a seguinte. Entretanto, o conjunto de comandos gerais usados no aplicativo do terminal é bastante similar e pode ser consultado nas instruções do Linux que se seguem. Os exemplos de captura de tela nesta seção foram criados em um ambiente de 64 bits.

Certas distribuições de Linux irão exigir privilégios (raiz) de usuário especial a fim de executar os comandos D500S de modo adequado na janela do terminal do aplicativo.

Observações importantes antes de prosseguir:

1.) **O D500S não suporta a inicialização do Dispositivo no Linux e precisará ser configurado em um sistema Windows ou macOS compatível antes que o drive possa ser utilizado em uma máquina Linux.**

2.) **O login no Linux suporta apenas o uso de senhas Complexas. O login da senha de frase-passe não é suportado para o login do Linux.**

3.) **O suporte ao recurso do D500S no Linux é limitado. Recursos como senha de Recuperação Única, senha de Exclusão Criptográfica, redefinições de senha de Admin/Usuário e alternar para o modo Somente Leitura não são suportados no Linux.**

O D500S vem com 4 comandos que podem ser usados no Linux:

lkd500s_about	Mostra as informações 'Sobre o D500S'.
lkd500s_login	Permite fazer login no drive.
lkd500S_logout	Permite encerrar a sessão com segurança do drive D500S.
lkd500S_resetdevice	Executa uma exclusão criptográfica de dispositivo e redefine o drive para um estado de fábrica, excluindo permanentemente todos os dados e arquivos armazenados no drive.

OBSERVAÇÃO: Para executar esses comandos você deve abrir uma janela do aplicativo do "Terminal" e navegar até a pasta onde está cada arquivo. Cada comando deve ser precedido pelos dois caracteres a seguir: './' (um ponto e uma barra.)

Exemplo de como navegar para o caminho dos Comandos do IronKey Linux:

Para usuários Linux de 32 bits:	Abra uma janela do aplicativo "Terminal" e altere o diretório atual para **/media/ubuntu/IRONKEY/linux/linux32$** digitando o seguinte comando no prompt: **cd /media/ubuntu/IRONKEY/linux/linux32** (e depois pressione ENTER.)
Para usuários Linux de 64 bits:	Abra uma janela do aplicativo "Terminal" e altere o diretório atual para **/media/ubuntu/IRONKEY/linux/linux64$** digitando o seguinte comando no prompt: **cd /media/ubuntu/IRONKEY/linux/linux64** (e depois pressione ENTER.)

Uso do dispositivo (Ambiente Linux)

Observação: Se o volume IRONKEY não for carregado automaticamente pelo sistema operacional, você precisará carregar o volume manualmente em uma janela de terminal usando o comando 'mount' do Linux. Consulte os documentos do Linux para verificar sua distribuição de SistOp específica ou site de suporte on-line favorito para a sintaxe adequada e opções de comando. Algumas distribuições Linux podem exigir que você insira o nome de usuário para executar comandos, ou seja, "ubuntu" nos exemplos acima.

Localizar e visualizar arquivos de comando do Linux IronKey D500S:

Assim que o D500S estiver ligado ao seu computador e reconhecido pelo sistema operacional, altere o diretório para o volume D500S digitando o comando no prompt do terminal. (*Figura 10.1*)

Observação: : As capturas de tela e instruções nesta seção utilizam a pasta linux64 (significando 64 bits) para demonstrar o uso do dispositivo D500S no sistema operacional Linux. Tenha em mente que se você estiver usando a versão de 32 bits do Linux, basta navegar e usar a respectiva pasta de 32 bits no lugar da pasta de 64 bits, ou seja, linux32 em vez de linux64.)

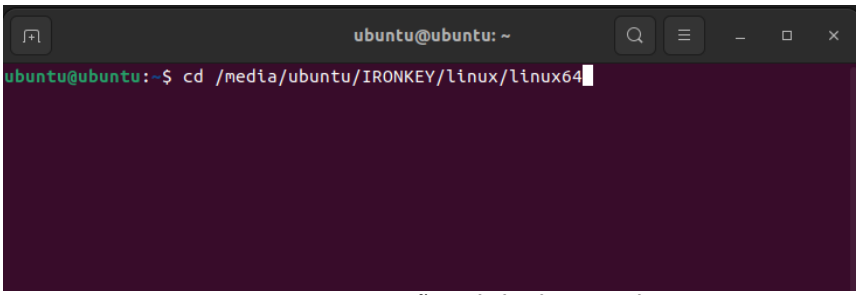


Figura 10.1 – Navegação na linha de comando

Use o comando **ls** (list) no prompt atual e pressione ENTER. Isso fornecerá uma lista de arquivos e/ou pastas na pasta linux64.

Você verá os quatro comandos Linux do IronKey listados (*Figura 10.2*)

- ikD500S_about
- ikD500S_login
- ikD500S_logout
- ikD500S_resetdevice

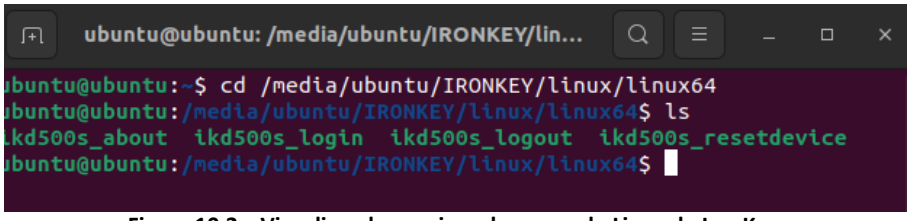


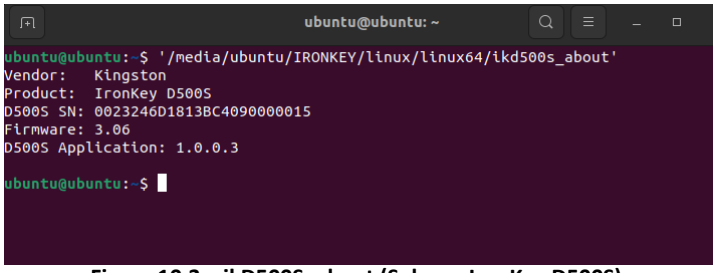
Figura 10.2 – Visualizando arquivos de comando Linux do IronKey

Observação: Nomes de comandos e pastas (diretório) diferenciam letras maiúsculas de minúsculas, ou seja, 'linux64' NÃO é o mesmo que 'Linux64'. A sintaxe também deve ser digitada exatamente como mostrada. Algumas distribuições Linux podem exigir que você insira o nome do usuário para executar comandos, ou seja, "ubuntu" neste exemplo.)

Uso do dispositivo (Ambiente Linux)

Utilizar comandos para D500S

Sobre o D500S

lkD500S_about (Sobre o D500S, *Figura 10.3*) Este comando preencherá informações sobre o D500S, como: • Revendedor • Produto • Número de série do D500S • Versão do firmware • Versão do software	 **Figura 10.3 – ikD500S_about (Sobre o IronKey D500S)**

Login do D500S

ikD500S_login

Assim que o D500S tiver sido inicializado em um sistema Windows ou macOS compatível, você pode acessar a partição de dados segura fazendo login no dispositivo utilizando a senha do D500S que você criou.

Para isso, siga essas etapas:

1. Abra a janela do aplicativo de um 'Terminal'.

2. Digite o seguinte comando no prompt do terminal **cd /media/ubuntu/IRONKEY/linux/linux64**

3. . Com o prompt de comando agora em **/media/ubuntu/IRONKEY/linux/linux64$**, digite o seguinte comando para fazer login no dispositivo: **./ikD500S_login*** e pressione ENTER. (Observação: Nomes de comandos e pasta são sensíveis a maiúsculas e minúsculas e a sintaxe deve ser exata. Além disso, algumas distribuições podem exigir que você insira seu nome de usuário, ou seja, "ubuntu" neste exemplo.)

4. Após um login bem-sucedido, o volume de dados seguro será aberto em sua área de trabalho e você pode continuar usando o D500S (mais informações sobre o comportamento de login continuam na próxima página)

* Observação: Certas distribuições de Linux irão exigir privilégios (raiz) de usuário especial a fim de executar os comandos D500S de modo adequado na janela do terminal do aplicativo.

Uso do dispositivo (Ambiente Linux)

Login do D500S (continuação)

IkD500S_login (Desbloquear D500S, *Figura 10.4*)

Dependendo de como seu drive foi configurado, durante o processo de login, você pode receber uma série de opções sobre como você gostaria de desbloquear seu drive.

Se os perfis de senha de **Admin/Usuário** foram ativados durante a inicialização, você receberá as seguintes opções de login:

1.) Escolher fazer login como Admin ou Usuário
2.) Escolher desbloquear as partições Admin ou Usuário (se ativadas)
3.) Introduzir a respectiva senha de login de Admin ou Usuário para a autenticação e desbloqueio do dispositivo.

Observação: Se os perfis de senha de Admin/Usuário NÃO estiverem ativados durante a inicialização (modo Somente Usuário), você precisará inserir apenas a senha do dispositivo para a autenticação do dispositivo.

Importante: Como mencionado anteriormente, as senhas de frase-passe não são compatíveis no Linux e o D500S precisará ser configurado com uma senha Complexa para login no Linux (*Figura 10.5*)

Figura 10.4 – ikD500S_login (Desbloquear D500S)

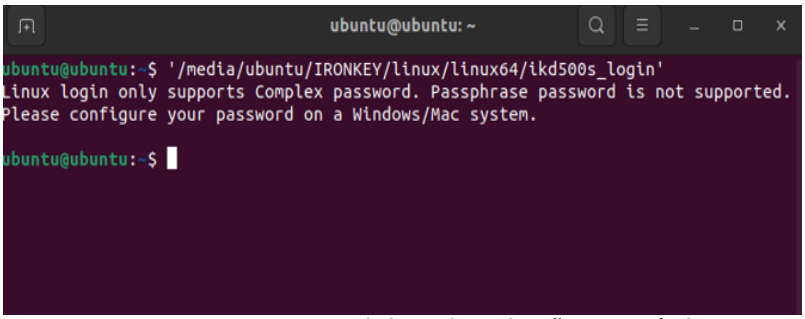


Figura 10.5 – Tentativa de login da senha não compatível.

Uso do dispositivo (Ambiente Linux)

Login do D500S (continuação)

Comportamento incorreto da senha de login
Durante o processo de login, se for introduzida uma senha incorreta, você terá outra oportunidade de inserir a senha. No entanto, existe uma funcionalidade de segurança integrada que monitora o número de tentativas de login malsucedidas. Se esse número atingir o valor pré-configurado de 10 tentativas malsucedidas para logins de Admin ou Usuário, o comportamento será o seguinte:

Senhas de Admin/Usuário ativadas

- **Login do Usuário:** Bloqueio do Usuário, login como Admin necessário. (*Figura 10.6*) Observação: A senha do Usuário pode ser redefinida pelo login do Admin em um sistema Windows ou macOS compatível.
- **Login do Admin:** Exclusão criptográfica do drive, todos os dados são perdidos para sempre. É necessária a restauração do dispositivo. (*Figura 10.7*)

Modo Somente Usuário (Admin/Usuário não ativado)

- **Login do Usuário:** Exclusão criptográfica do drive, todos os dados são perdidos para sempre. É necessária a restauração do dispositivo. (*Figura 10.7*)

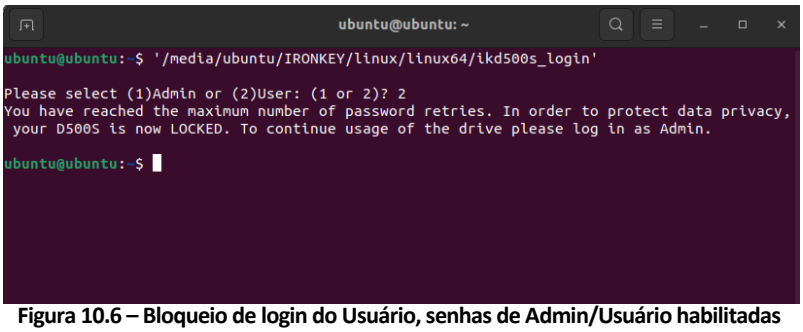


Figura 10.6 – Bloqueio de login do Usuário, senhas de Admin/Usuário habilitadas

Figura 10.7 – Número máximo de tentativas alcançadas (Restauração do drive)

Logout do D500S

IkD500S_logout (dispositivo de bloqueio)

Quando terminar de usar o D500S, faça logout do dispositivo e proteja seus dados. Para fazer isso, siga as mesmas etapas citadas na página 39 e use corretamente o seguinte comando logout do dispositivo: **./ikD500S_logout** e pressione ENTER (Observação: Nomes de comandos e pastas diferenciam letras maiúsculas de minúsculas e a sintaxe deve ser exata. (*Figura 10.8*)

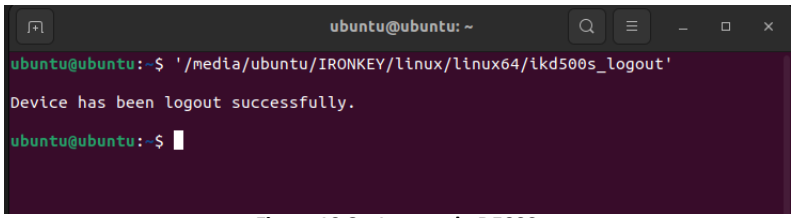


Figura 10.8 – Logout do D500S

Uso do dispositivo (Ambiente Linux)

Restauração do dispositivo D500S

ikD500S_resetdevice
Como mencionado anteriormente na página 41, caso as senhas de Usuário/Admin sejam esquecidas, o comando Restaurar Dispositivo pode ser usado para restaurar o drive para que ele possa ser utilizado novamente. Este processo permitirá que você crie uma nova senha, mas para proteger a privacidade de seus dados, o D500S irá excluir criptograficamente o drive e formatar a partição segura dos dados. **Isso significa que todos os seus dados serão perdidos.**

Para utilizar o comando Restaurar Dispositivo, siga as mesmas etapas citadas na página 39 e use corretamente o seguinte comando logout do dispositivo: **./ikD500S_resetdevice** e pressione ENTER (Observação: Nomes de comandos e pastas diferenciam letras maiúsculas de minúsculas e a sintaxe deve ser exata. (*Figura 10.7*)

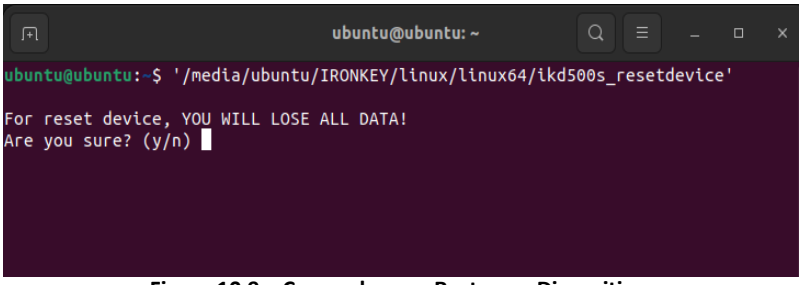


Figura 10.9 – Comando para Restaurar Dispositivo

Depois que o comando Restaurar Dispositivo for usado, você será solicitado a criar uma nova senha complexa que deve conter:

- De 8 a 16 caracteres e conter pelo menos (3) das seguintes opções de critérios:

  -LETRA MAIÚSCULA
  -letra minúscula
  -números
  -Caracteres especiais (!,$ etc.)

(*Figura 10.10*)

Observação: O comando Restaurar Dispositivo inicializa o drive no modo Somente Usuário (Senha única, usuário único). Para ativar os perfis de senha de login de Admin/Usuário, o D500S terá de ser configurado em um sistema Windows ou macOS suportado para acessar essa opção.

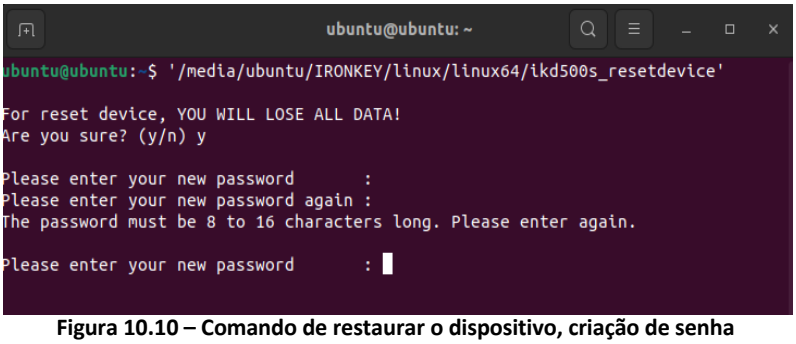


Figura 10.10 – Comando de restaurar o dispositivo, criação de senha

IRONKEY™ D500S
SZYFROWANA PAMIĘĆ FLASH USB 3.2 Gen 1

Instrukcja obsługi

Spis treści

Ilustracja 1 – IronKey D500S

Wprowadzenie

Kingston IronKey D500S to pamięć USB z zabezpieczeniami zgodnymi z wojskowymi normami szyfrowania, oferująca funkcje, dzięki którym marka IronKey jest ceniona za skuteczną ochronę poufnych informacji. Pamięć uzyskała certyfikat FIPS 140-3 Level 3 (w toku), który uwzględnia nowe wymogi określone przez agencję NIST, dotyczące aktualizacji oprogramowania bezpiecznego mikroprocesora w celu zwiększenia bezpieczeństwa. Proces szyfrowania i odszyfrowywania danych odbywa się w pamięci D500S bez pozostawiania śladów w systemie hosta, co czyni ją odporną na działanie programów przechwytujących hasła (tzw. snifferów). Oprócz funkcji 256-bitowego szyfrowania sprzętowego XTS-AES pamięć ma także wytrzymałą cynkową obudowę, która jest wodoodporna*, pyłoszczelna*, odporna na zgniecenie i wypełniona żywicą epoksydową w celu ochrony wewnętrznych komponentów przed atakami penetracyjnymi.

Pamięć D500S oferuje opcję obsługi wielu haseł (administratora, użytkownika i jednorazowe hasło odzyskiwania) w trybach haseł złożonych lub wyrażeń hasłowych**. Opcja obsługi wielu haseł (Multi-Password) zwiększa możliwości odzyskania dostępu do danych w przypadku zapomnienia jednego z haseł. Oprócz obsługi tradycyjnych haseł złożonych tryb wyrażeń hasłowych umożliwia wprowadzenie numerycznego kodu PIN, zdania, listy słów, a nawet tekstu o długości od 10 do 128 znaków. Administrator może włączyć tryb użytkownika, utworzyć dwie partycje na dane o niestandardowych rozmiarach, oddzielając w ten sposób pliki logowania administratora i użytkownika, włączyć jednorazowe hasło odzyskiwania, hasło Crypto-Erase, a także zresetować hasło użytkownika, aby przywrócić dostęp do danych.

Aby ułatwić wpisywanie hasła, można włączyć jego podgląd (symbol oka ), co pozwala ograniczyć liczbę literówek i nieudane próby logowania. Dodatkowo pamięć D500S wykorzystuje podpisane cyfrowo oprogramowanie sprzętowe, dzięki czemu jest odporna na ataki z wykorzystaniem złośliwego oprogramowania BadUSB oraz metodą Brute Force (próby wielokrotnego wprowadzenia hasła). Po 10 kolejnych próbach wprowadzenia nieprawidłowego hasła funkcja ochrony przed atakami typu Brute Force blokuje hasło użytkownika lub jednorazowe hasło odzyskiwania, a po 10 kolejnych próbach wprowadzenia nieprawidłowego hasła administratora – kryptograficznie wymazuje zawartość pamięci.

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 wirtualna klawiatura chroni hasła przed keyloggerami i screenloggerami***.

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

Pamięć D500S oferuje wiele opcji personalizacji, jest zgodna z wymogami TAA/CMMC i montowana w USA.

Pamięć D500S jest objęta ograniczoną 5-letnią gwarancją i bezpłatną pomocą techniczną firmy Kingston.

* Patrz arkusz specyfikacji. Przed użyciem produkt musi być czysty i suchy.
** Tryb wyrażeń hasłowych nie jest obsługiwany w systemach Linux.
*** Wirtualna klawiatura: obsługuje wyłącznie język angielski (USA) w obsługiwanych systemach Microsoft Windows i macOS.

Pamięć IronKey D500S oferuje następujące rozwiązania:

- 6-bitowe szyfrowanie sprzętowe w trybie XTS-AES z certyfikatem FIPS 140-3 level 3 (w toku); funkcji szyfrowania nie można wyłączyć
- Ochrona przed atakami metodami Brute Force i BadUSB
- Opcje obsługi wielu haseł (Multi-Password)
- Tryby haseł złożonych i wyrażeń hasłowych
- Unikalna opcja dwóch partycji i hasło Crypto-Erase
- Przycisk z symbolem „oka" do wyświetlania wprowadzanych haseł w celu ograniczenia liczby nieudanych prób logowania
- Wirtualna klawiatura pomagająca chronić przed keyloggerami i screenloggerami
- Ustawienia trybu tylko do odczytu (ochrony przed zapisem) w celu ochrony danych zapisanych w pamięci przed zmianami lub złośliwym oprogramowaniem
- Małe i średnie firmy mogą lokalnie zarządzać urządzeniami pamięci, korzystając z funkcji administratora
- Zgodność z systemem Windows, macOS i Linux (szczegóły w arkuszu danych)

Informacje o tej instrukcji

Niniejsza instrukcja obsługi dotyczy pamięci IronKey D500S w wersji fabrycznej, tj. bez zmian dokonanych na życzenie klienta.

Wymagania systemowe

Platforma PC • Intel, AMD i Apple M1 SOC • 15MB wolnego miejsca na dysku • Dostępny port USB 2.0/3.2 • Dwie kolejne litery dysku po ostatnim dysku fizycznym* ***Uwaga:** patrz rozdział „Konflikt liter dysków" na str. 35.	**Obsługiwane systemy operacyjne komputerów PC** • Windows 11 • Windows 10
Platforma Mac • 15MB wolnego miejsca na dysku • Port USB 2.0/3.2	**Obsługiwane systemy operacyjne komputerów Mac** • macOS macOS 11.x - 14.x
Platforma Linux • 5MB wolnego miejsca na dysku • Port USB 2.0/3.2	**Obsługiwane systemy operacyjne komputerów z systemem Linux** • Linux Kernel v4.4+

Zalecenia

Aby zagwarantować odpowiednie zasilanie urządzenia D500S, należy podłączać je bezpośrednio do portu USB w notebooku lub komputerze stacjonarnym, jak pokazano na ***ilustracji 1.1***. Należy unikać podłączania urządzenia D500S do urządzeń peryferyjnych z portem USB, takich jak klawiatura czy koncentrator zasilany z portu USB, jak pokazano na ***ilustracji 1.2***.

Ilustracja 1.1 – Zalecany sposób użycia

Ilustracja 1.2 – Niezalecany sposób użycia

Używanie prawidłowego systemu plików

Pamięć IronKey D500S jest fabrycznie sformatowana w systemie plików FAT32. Pozwala to na działanie w systemach Windows, macOS i Linux*. 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 w komputerze przed skonfigurowaniem i użyciem pamięci D500S 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 hasła innym osobom

Najnowsze aktualizacje i informacje

Na stronie kingston.com/support można znaleźć najnowsze wersje oprogramowania pamięci, często zadawane pytania, dokumentację oraz 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.

*** Pamięć D500S w konfiguracji fabrycznej nie umożliwia zainicjowania w systemie Linux. Musi zostać w pełni zainicjowana i skonfigurowana w obsługiwanym systemie Windows lub macOS, zanim będzie można jej używać w systemie Linux. Więcej informacje można znaleźć na str. 37 niniejszej instrukcji obsługi, w części dotyczącej systemu Linux.**

Najlepsze metody konfiguracji hasła

Pamięć D500S ma silne zabezpieczenia. Obejmuje to ochronę przed atakami metodą Brute Force, która uniemożliwia hakerom odgadywanie haseł dzięki ograniczeniu liczby prób wprowadzenia hasła do 10. Po osiągnięciu tego limitu pamięć D500S automatycznie wymaże zaszyfrowane dane, formatując się do stanu fabrycznego.

Obsługa wielu haseł (funkcja Multi-Password)
Jedną z głównych funkcji pamięci D500S jest obsługa wielu haseł, która pomaga chronić przed utratą danych w przypadku zapomnienia jednego lub większej liczby haseł. Gdy wszystkie opcje haseł są włączone, pamięć D500S może obsługiwać trzy różne hasła, które można wykorzystać do odzyskania dostępu do danych – hasło administratora, użytkownika oraz jednorazowe hasło odzyskiwania.

Pamięć D500S 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 OBA 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 zastosowanego mechanizmu zabezpieczenia nie można obejść. Firma Kingston zaleca zapisywanie danych również na innych nośnikach. Pamięć D500S można bezpiecznie wymazać w celu ponownego wykorzystania, jednak znajdujące się w niej dane zostaną bezpowrotnie usunięte.

Tryby hasła
Pamięć D500S obsługuje również dwa różne tryby hasła:

Hasło złożone
Hasło złożone musi składać się z co najmniej 8-16 znaków oraz zawierać co najmniej trzy z następujących znaków:

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

Wyrażenie hasłowe
Pamięć D500S obsługuje wyrażenia hasłowe o długości od 10 do 128 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 D500S. 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.

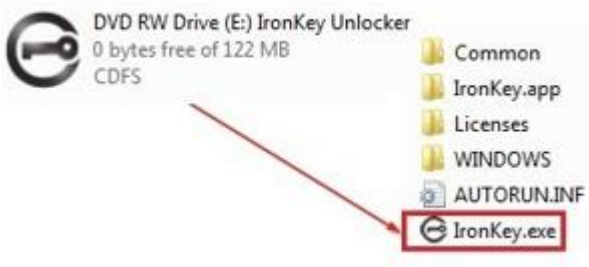
Konfiguracja urządzenia

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 pamięci do jakichkolwiek urządzeń peryferyjnych, które mogą być wyposażone w port USB, takich jak klawiatura lub koncentrator zasilany przez USB. Początkową konfigurację urządzenia należy przeprowadzić na obsługiwanym systemie operacyjnym opartym na systemie Windows lub macOS.

Dostęp do urządzenia (środowisko Windows)

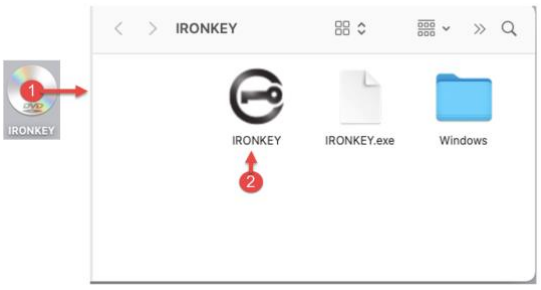
Podłącz szyfrowaną pamięć USB IronKey do wolnego portu USB w notebooku lub komputerze stacjonarnym i zaczekaj, aż system Windows ją wykryje.

• W systemie Windows 10/11 wyświetli się powiadomienie dotyczące instalacji sterownika urządzenia (*ilustracja 3.1*)	 **Ilustracja 3.1 – Powiadomienie o instalacji sterownika urządzenia**

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

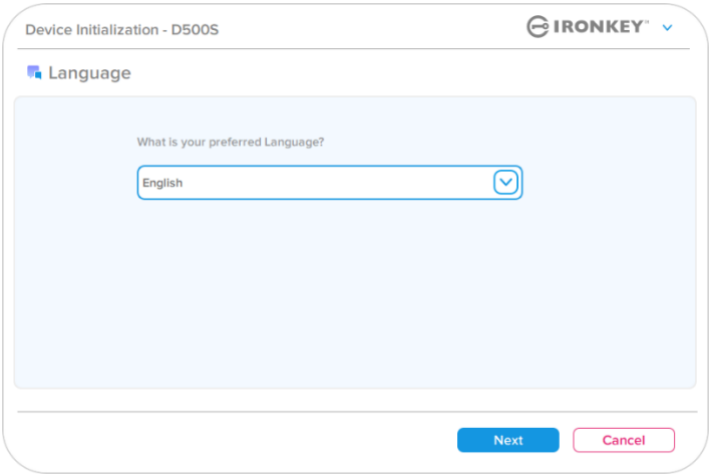
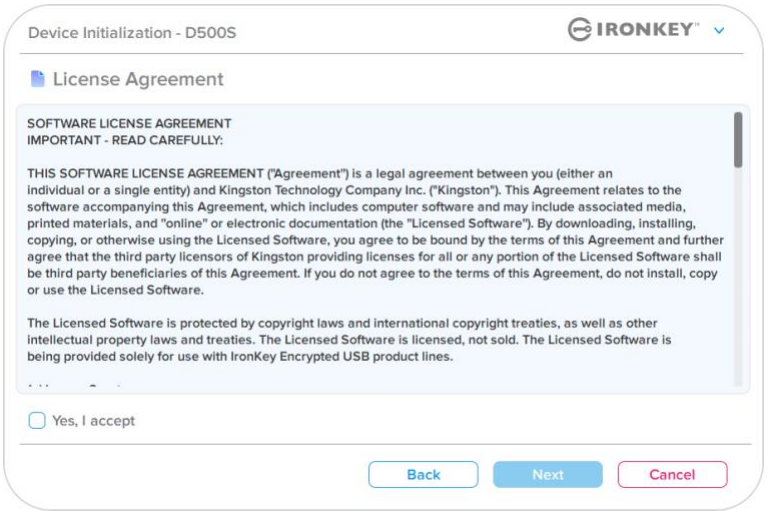
Dostęp do urządzenia (środowisko macOS)

Włóż pamięć D500S 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 „IRONKEY”. (*ilustracja 3.3*)

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

Inicjowanie urządzenia (środowiska Windows i macOS)

Język i umowa licencyjna użytkownika końcowego

Wybierz preferowany język z menu rozwijanego i kliknij przycisk **Next (Dalej)** (*ilustracja 4.1*)	 **Ilustracja 4.1 – Wybór języka**
Zapoznaj się z umową licencyjną i kliknij przycisk **Next (Dalej)**. **Uwaga:** Aby kontynuować, należy zaakceptować umowę licencyjną; w przeciwnym razie przycisk **Next (Dalej)** pozostanie nieaktywny (*ilustracja 4.2*).	 **Ilustracja 4.2 – Umowa licencyjna**

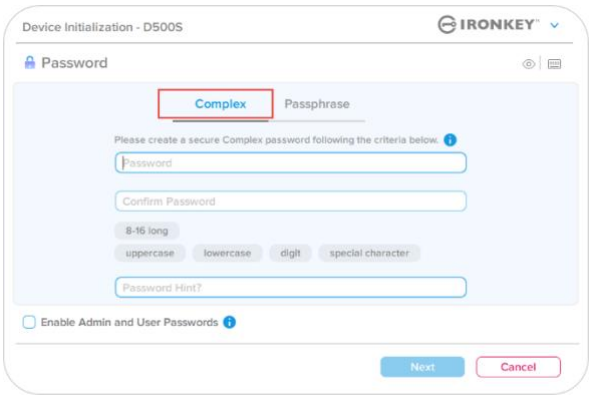
Inicjowanie urządzenia

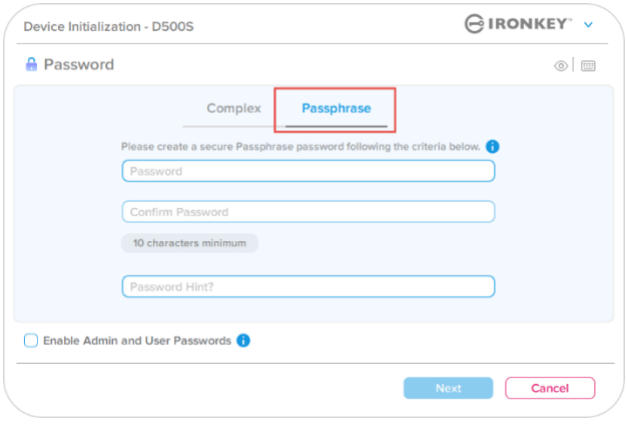
Wybór hasła

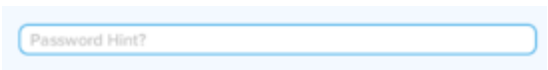
Na ekranie monitu o podanie hasła można utworzyć hasło do ochrony danych zapisanych w pamięci D500S, korzystając z trybu hasła złożonego lub wyrażenia hasłowego (*ilustracje 4.3-4.4*). Ponadto na tym ekranie można również włączyć opcje wielu haseł administratora/użytkownika. Zanim przejdziesz do wyboru hasła, zapoznaj się z informacjami dotyczącymi włączania haseł administratora/użytkownika poniżej, aby lepiej zrozumieć te działanie tych funkcji.

Uwaga: Po wybraniu trybu hasła złożonego lub wyrażenia hasłowego nie można go zmienić, o ile urządzenie nie zostanie zresetowane.

Aby rozpocząć wybór hasła, utwórz hasło w polu „Password” (Hasło), a następnie wprowadź je ponownie w polach „Confirm Password” (Potwierdź hasło). Utworzone hasło musi spełniać poniższe kryteria, aby można było kontynuować proces inicjowania:

<table>
<tr>
<td>Hasło złożone
Musi zawierać co najmniej 8 znaków (maks. 16 znaków).
Musi zawierać znaki należące do trzech (3) z następujących kategorii:
wielkie litery
małe litery
cyfry
znaki specjalne (!,$,&, itp.)</td>
<td> 

Ilustracja 4.3 – Hasło złożone</td>
</tr>
<tr>
<td>Wyrażenie hasłowe
Musi zawierać:
co najmniej 10 znaków
maksymalnie 128 znaki</td>
<td> 

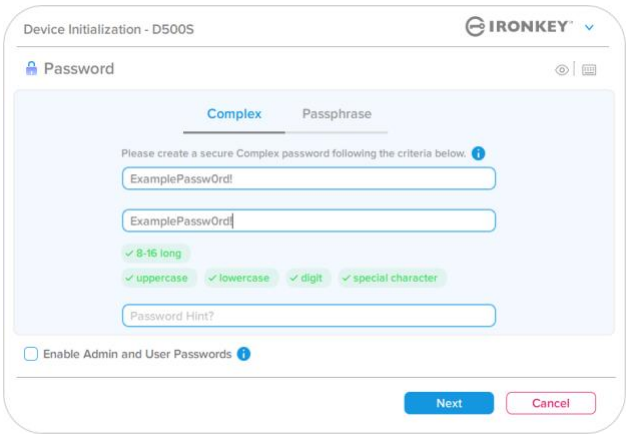
Ilustracja 4.4 – Wyrażenie hasłowe</td>
</tr>
<tr>
<td>Podpowiedź hasła (opcjonalnie)
Podpowiedź hasła może być pomocna w przypomnieniu sobie zapomnianego hasła.
Uwaga: Podpowiedź NIE MOŻE być taka sama jak hasło.</td>
<td> 

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

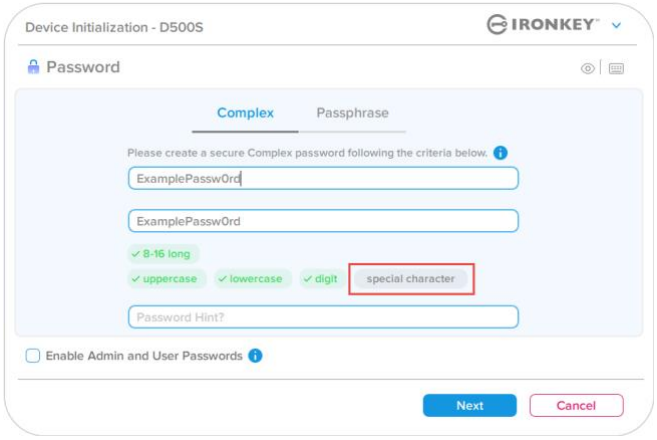
Inicjowanie urządzenia

Valid and invalid passwords

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



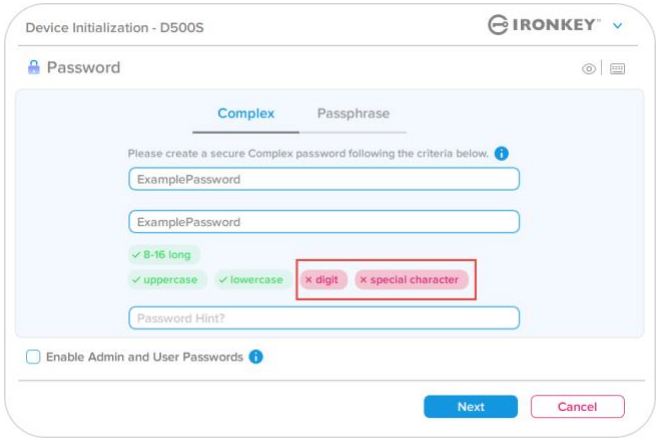
Ilustracja 4.6a – Spełnione warunki dla hasła złożonego



Ilustracja 4.6b – Opcjonalny warunek dla hasła złożonego

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

Dotyczy to zarówno haseł złożonych, jak i wyrażeń hasłowych.



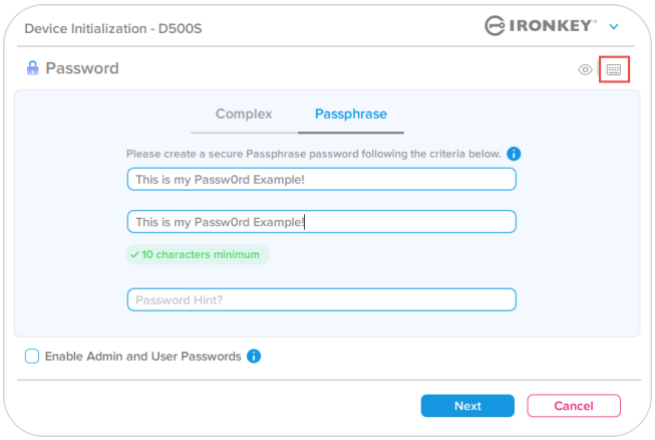
Ilustracja 4.7 – Niespełnione warunki dla hasła

Inicjowanie urządzenia

Wirtualna klawiatura

Pamięć D500S jest wyposażona w funkcję wirtualnej klawiatury, która może służyć do ochrony przed oprogramowaniem rejestrującym naciśnięcia klawiszy (keyloggerami).

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



Ilustracja 4.8 – Aktywacja wirtualnej klawiatury

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

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

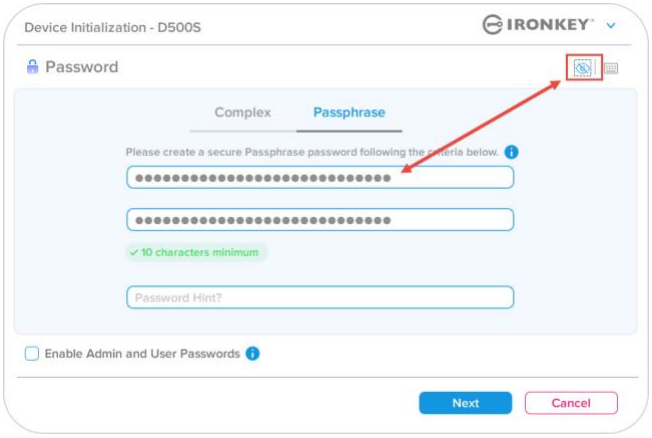
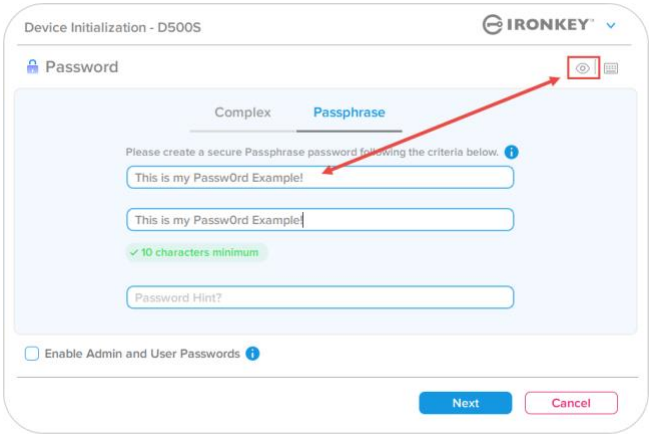
Ilustracja 4.9 – Ochrona przed screenloggerami/randomizacja

Inicjowanie urządzenia

Przełącznik widoczności hasła

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

Uwaga: Po zakończeniu inicjowania urządzenia pole hasła będzie domyślnie „ukryte”.

Aby **ukryć** ciąg znaków hasła, kliknij szarą ikonę. 	 **Ilustracja 4.10 – Wybór opcji „ukryj” hasło**
Aby **wyświetlić** ukryte hasło, kliknij niebieską ikonę. 	 **Ilustracja 4.11 – Wybór opcji „pokaż” hasło**

Inicjowanie urządzenia

Hasła administratora i użytkownika

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

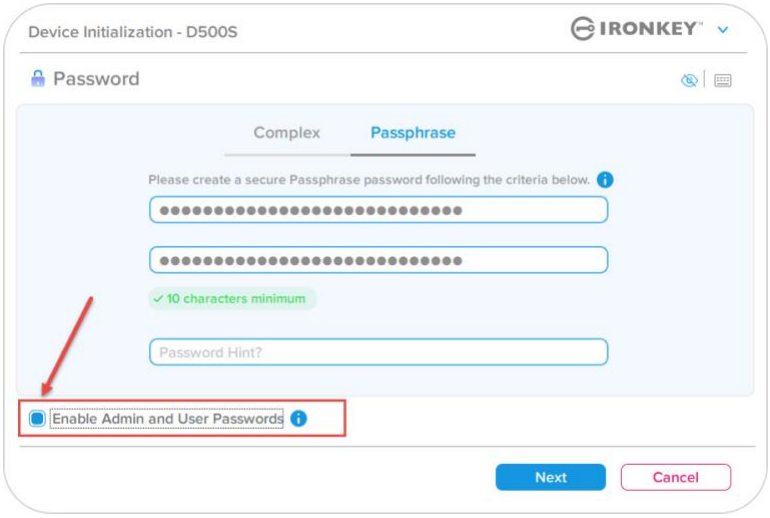
Gdy włączone są **hasła administratora i użytkownika**, można również uzyskać dostęp do następujących funkcji:

- Konfiguracja dwóch partycji
- Jednorazowe hasło odzyskiwania
- Wymuszony tryb tylko do odczytu w przypadku logowania użytkownika
- Resetowanie hasła użytkownika
- Wymuszone resetowanie hasła w przypadku logowania użytkownika
- Hasło Crypto-Erase

Aby dowiedzieć się więcej o tych funkcjach, przejdź na stronę 25 niniejszej instrukcji.

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

- Jeśli ta funkcja jest **włączona**, hasło wybrane na tym ekranie będzie **hasłem administratora**. Kliknij przycisk **Next (Dalej)**, aby przejść do ekranu **hasła użytkownika** i zdefiniować hasło dla użytkownika.



Ilustracja 4.12 – Włączanie haseł administratora i użytkownika

Uwaga: Włączenie hasła administratora i użytkownika jest opcjonalne.

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

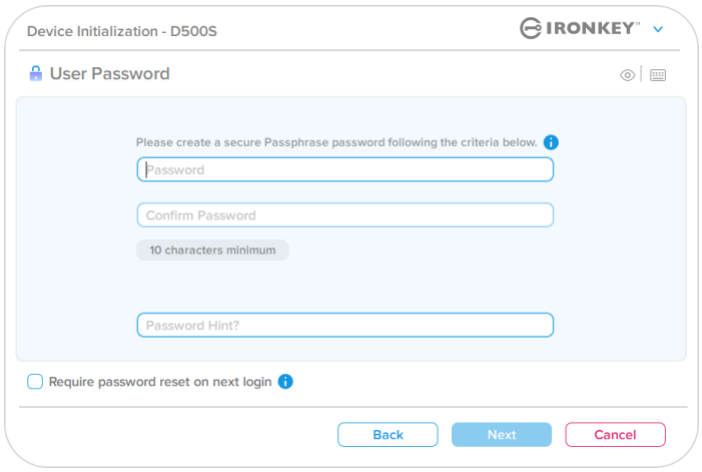
Aby kontynuować konfigurację dla pojedynczego użytkownika z jednym hasłem, pozostaw niezaznaczoną opcję **Enable Admin and User Passwords (Włącz hasła administratora i użytkownika)** i po utworzeniu prawidłowego hasła kliknij przycisk **Next (Dalej)**.

Uwaga: W dalszej części tej instrukcji tryb z włączonymi **hasłami administratora i użytkownika** będzie określany **jako „rola administratora"**.

Inicjowanie urządzenia

Hasła administratora i użytkownika

- Jeśli na poprzednim ekranie została **włączona** rola administratora, na następnym ekranie pojawi się monit o podanie **hasła użytkownika** (*ilustracja 4.13*). Hasło użytkownika zapewnia ograniczone uprawnienia w porównaniu z hasłem administratora, co zostanie szczegółowo omówione w dalszej części niniejszej instrukcji obsługi (patrz str. 23).

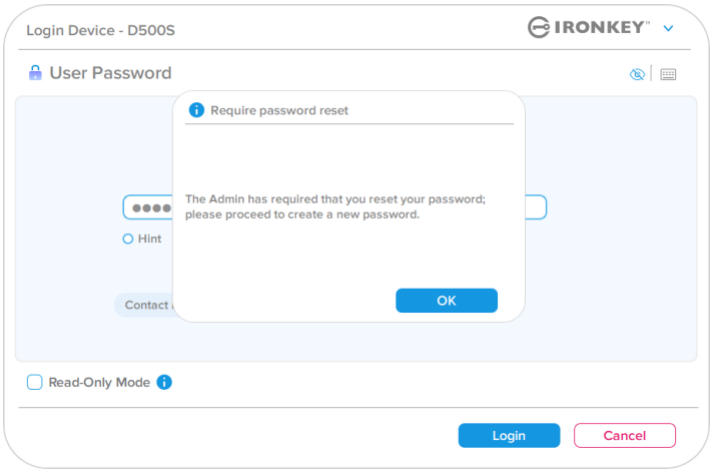


Ilustracja 4.13 – Hasło użytkownika (włączone hasła administratora i użytkownika)

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

- Funkcja **„Require password reset on next login" (Wymagaj zresetowania hasła przy następnym logowaniu)**, widoczna w lewym dolnym rogu ilustracji 4.13, dotyczy tylko hasła użytkownika i można ją włączyć, aby wymusić na użytkowniku zalogowanie się przy użyciu tymczasowego hasła ustawionego przez administratora podczas procesu inicjowania, a następnie do jego zmiany na wybrane przez siebie hasło po uwierzytelnieniu pamięci przy użyciu hasła tymczasowego. Jest to przydatne, gdy pamięć jest przekazywana do użytkowania innej osobie (*ilustracja 4.14*)

  Uwaga: Ze względów bezpieczeństwa nowe hasło nie może być takie samo jak hasło tymczasowe.



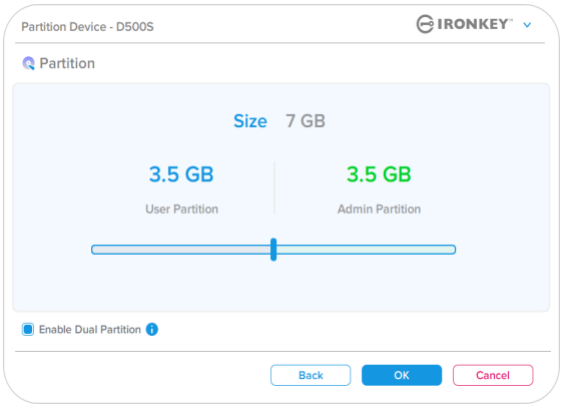
Ilustracja 4.14 – Wymaganie zresetowania hasła przy następnym logowaniu (dla hasła użytkownika)

Inicjowanie urządzenia

Dwie partycje

Urządzenie IronKey D500S umożliwia utworzenie dwóch osobnych partycji o niestandardowych rozmiarach dla administratora i użytkownika. Gdy ta funkcja jest włączona, administrator ma dostęp **zarówno** do partycji administratora, jak i użytkownika, natomiast użytkownik ma dostęp **tylko** do partycji użytkownika. Funkcja ta umożliwia bezpieczne rozdzielenie uprawnień dostępu do danych i plików między administratora i użytkownika lub może zostać wykorzystana do utworzenia ukrytego magazynu plików, aby zapobiec ujawnieniu określonych plików w niezaufanych systemach. W razie potrzeby można również dostosować rozmiary partycji dla administratora i użytkownika.

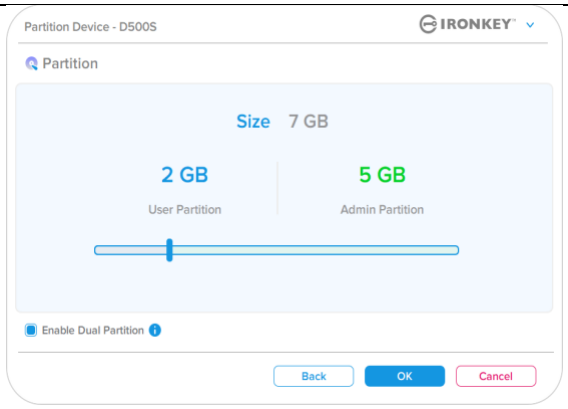
UWAGA: Ta funkcja jest *opcjonalna* i można ją wyłączyć, pozostawiając niezaznaczone pole „Enable Dual Partition" (Włącz dwie partycje) podczas konfiguracji (*ilustracja 4.15*).



Ilustracja 4.15 – Tworzenie partycji na urządzeniu

Aby dostosować i przydzielić rozmiary partycji dla użytkownika i administratora, przesuń odpowiednio suwak w lewo lub w prawo (*ilustracja 4.16*).

- Wielkość partycji można zmieniać skokowo co 0,5GB.
- Rozmiar partycji jest określany na podstawie całkowitej pojemności pamięci dostępnej na ukrytej partycji.
- Domyślnie suwak dwóch partycji jest ustawiony na równomierny podział pamięci między administratora i użytkownika.
- Najmniejszy rozmiar partycji, jaki można przydzielić, to 1GB.



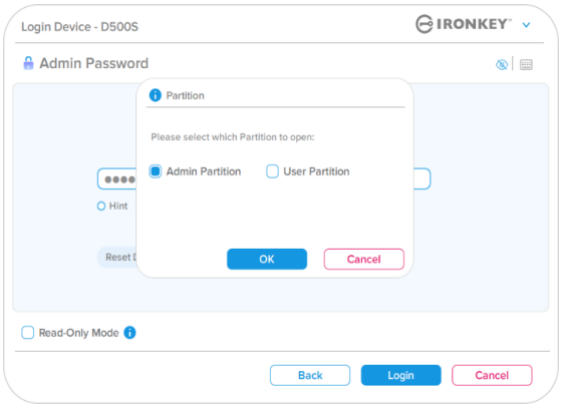
Ilustracja 4.16 – Tworzenie partycji na urządzeniu z dostosowaniem wielkości za pomocą suwaka

Administrator

Gdy pamięć zostanie w pełni skonfigurowana z włączonymi dwiema partycjami, przy każdym logowaniu administrator będzie mógł skorzystać z opcji odblokowania pamięci w celu uzyskania dostępu do partycji administratora LUB partycji użytkownika (*ilustracja 4.17*)

UWAGA: W danej chwili można otworzyć tylko jedną partycję. Nie można odblokować jednocześnie partycji użytkownika i administratora.

Opcja ta nie będzie dostępna dla użytkownika i po jego zalogowaniu się będzie automatycznie odblokowywana tylko partycja użytkownika.



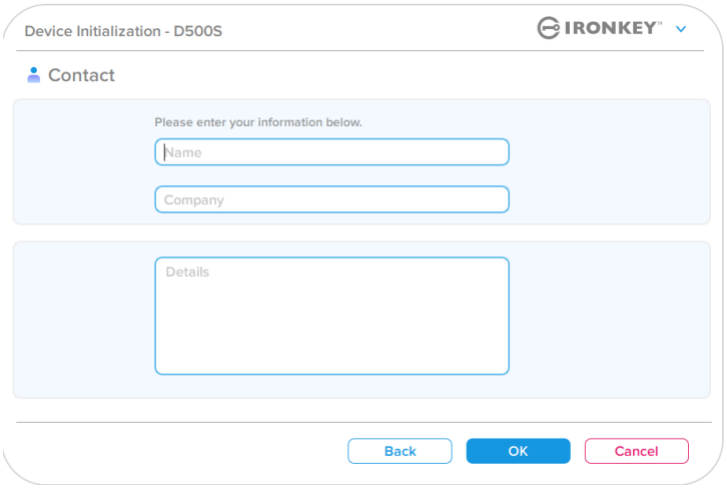
Ilustracja 4.17 – Przykład logowania administratora z opcją wyboru partycji

Inicjowanie urządzenia

Informacje kontaktowe

W wyświetlonych polach tekstowych wprowadź informacje kontaktowe (patrz *Ilustracja 4.18*)

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

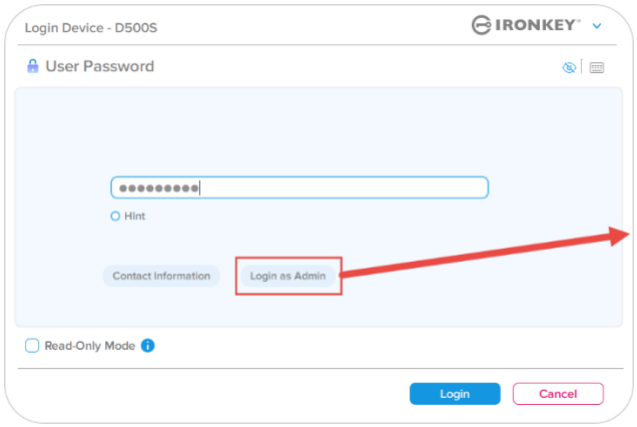
Pole **„Name" (Nazwa)** może zawierać do 32 znaków, ale nie może zawierać **samego** hasła. Pole **„Company" (Firma)** może zawierać do 32 znaków, ale nie może zawierać **samego** hasła. Pole **„Details" (Szczegóły)** może zawierać do 156 znaków, ale nie może zawierać **samego** hasła.	 **Ilustracja 4.18 – Informacje kontaktowe**

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

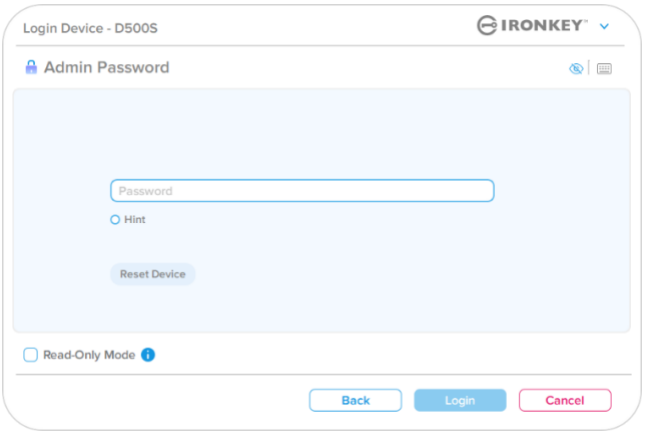
Korzystanie z urządzenia (środowiska Windows i macOS)

Logowanie administratora i użytkownika (włączony tryb administratora)

Jeśli urządzenie zostało zainicjowane z włączonymi hasłami administratora i użytkownika (rola administratora), nastąpi uruchomienie aplikacji IronKey D500S i wyświetlenie w pierwszej kolejności ekranu z monitem o podanie hasła użytkownika. Z tego miejsca można zalogować się za pomocą hasła użytkownika, wyświetlić wprowadzone informacje kontaktowe lub zalogować się jako administrator (*ilustracja 5.1*). Po kliknięciu przycisku „Login as Admin" (Zaloguj się jako administrator) (patrz poniżej) aplikacja przejdzie do menu logowania administratora, w którym można zalogować się jako administrator, aby uzyskać dostęp do ustawień i funkcji administratora (*ilustracja 5.2*).



Ilustracja 5.1 – Logogowanie za pomocą hasła użytkownika (włączony tryb administratora)

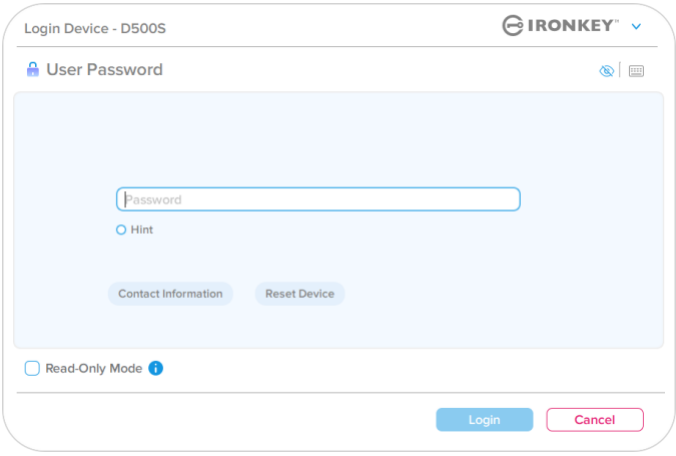


Ilustracja 5.2 – Logowanie za pomocą hasła administratora

Logowanie w trybie Tylko użytkownik (wyłączony tryb administratora)

Jak wspomniano wcześniej, chociaż zaleca się korzystanie z funkcji administratora, aby w pełni wykorzystać możliwości urządzenia, pamięć IronKey można również zainicjować w konfiguracji Tylko użytkownik (jedno hasło, jeden użytkownik). Jest to opcja dla tych użytkowników, którzy preferują prostotę obsługi i ochronę danych za pomocą pojedynczego hasła (*ilustracja 5.3*),

Uwaga: Aby aktywować hasła administratora i użytkownika, użyj przycisku **Reset Device (Resetuj urządzenie)**, aby przywrócić pamięć do stanu inicjowania, w którym można aktywować hasła administratora i użytkownika. **Zresetowanie urządzenia spowoduje usunięcie WSZYSTKICH zapisanych danych i ich bezpowrotna utratę.**



Ilustracja 5.3 – Logowanie za pomocą hasła użytkownika (wyłączony tryb administratora)

Korzystanie z urządzenia

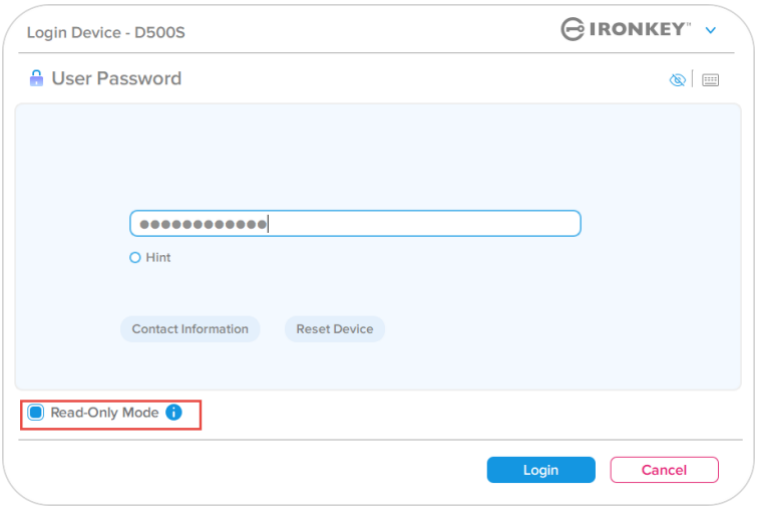
Odblokowywanie w trybie tylko do odczytu

Aby uniknąć omyłkowego wprowadzenia zmian w plikach zapisanych w pamięci IronKey, można odblokować urządzenie w trybie tylko do odczytu. Na przykład w przypadku korzystania z niezaufanego lub nieznanego komputera odblokowanie urządzenia w trybie tylko do odczytu uniemożliwi złośliwemu oprogramowaniu z tego komputera zainfekowanie urządzenia lub zmodyfikowanie plików.

Podczas pracy w tym trybie nie można wykonywać żadnych operacji związanych z modyfikacją plików zapisanych w urządzeniu. Nie można np. ponownie sformatować urządzenia ani przywracać, dodawać lub edytować plików zapisanych w pamięci.

Aby odblokować urządzenie w trybie tylko do odczytu:

1. Włóż urządzenie do portu USB komputera-hosta i uruchom plik **IronKey.exe**.
2. Zaznacz pole wyboru opcji **Read-Only Mode (Tryb tylko do odczytu)** poniżej pola wprowadzania hasła (*ilustracja 5.4*)
3. Wpisz swoje hasło do urządzenia i kliknij przycisk **Login (Zaloguj się)**. Urządzenie zostanie odblokowane w trybie tylko do odczytu.



Ilustracja 5.4 – Tryb tylko do odczytu

Aby odblokować urządzenie z pełnymi uprawnieniami do odczytu/zapisu na bezpiecznej partycji danych należy odłączyć pamięć D500S i zalogować się ponownie, usuwając zaznaczenie pola wyboru opcji Read-Only Mode (Tryb tylko do odczytu).

Uwaga: Opcje administratora pamięci D500S 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 31).

Korzystanie z urządzenia

Ochrona przed atakami metodą Brute-Force

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

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

Włączony tryb administratora/użytkownika	**Ochrona przed atakami metodą Brute Force Zachowanie urządzenia (10 nieudanych prób wprowadzenia hasła)**	**Wymazanie danych i zresetowanie urządzenia?**
Hasło użytkownika	Blokada hasła. Zaloguj się jako administrator lub użyj jednorazowego hasła odzyskiwania, aby zresetować hasło użytkownika	NIE
Hasło administratora	Bezpowrotne wymazanie metodą kryptograficzną pamięci, haseł, ustawień i danych	**TAK**
Jednorazowe hasło odzyskiwania	Blokada hasła, przycisk hasła odzyskiwania zostanie wyszarzony i stanie się nieaktywny. Zaloguj się jako administrator, aby zresetować hasło.	NIE
Tylko użytkownik Jeden użytkownik, jedno hasło (WYŁĄCZONY tryb administratora/użytkownika)	**Ochrona przed atakami metodą Brute Force Zachowanie urządzenia (10 nieudanych prób wprowadzenia hasła)**	**Wymazanie danych i zresetowanie urządzenia?**
Hasło użytkownika	Bezpowrotne wymazanie metodą kryptograficzną pamięci, haseł, ustawień i danych	**TAK**

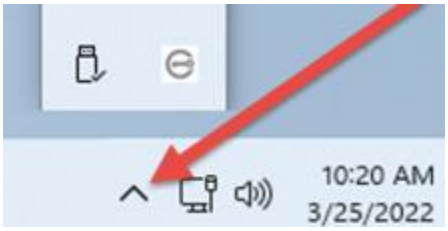
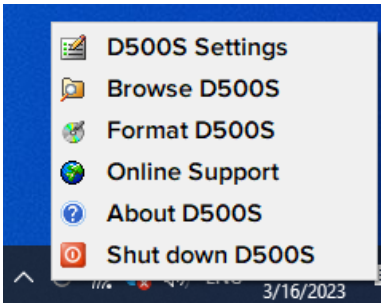
* Po pomyślnym uwierzytelnieniu użytkownika licznik nieudanych logowań jest resetowany odpowiednio dla użytej metody logowania. Funkcja Crypto-Erase usunie wszystkie hasła, klucze szyfrowania i dane – **zostaną one bezpowrotnie utracone.**

Uzyskiwanie dostępu do zabezpieczonych plików

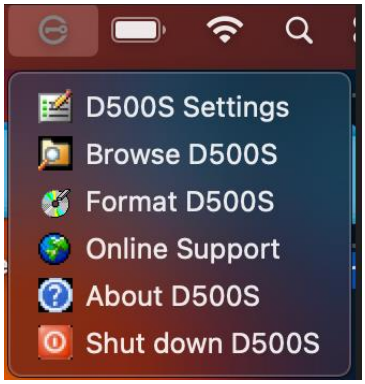
Po odblokowaniu urządzenia uzyskasz dostęp do zabezpieczonych plików. Pliki są automatycznie szyfrowane i odszyfrowywane podczas ich zapisywania lub otwierania w pamięci. Technologia ta pozwala na wygodną pracę, tak jak w przypadku zwykłej pamięci, zapewniając jednocześnie silne, „zawsze włączone” zabezpieczenia.
Wskazówka: Można również uzyskać dostęp do plików, klikając prawym przyciskiem myszy **ikonę IronKey** na pasku zadań systemu Windows, a następnie klikając opcję **„Browse D500S” (Przeglądaj zawartość pamięci D500S)** (*ilustracja 6.2*)

Opcje urządzenia – (środowisko Windows)

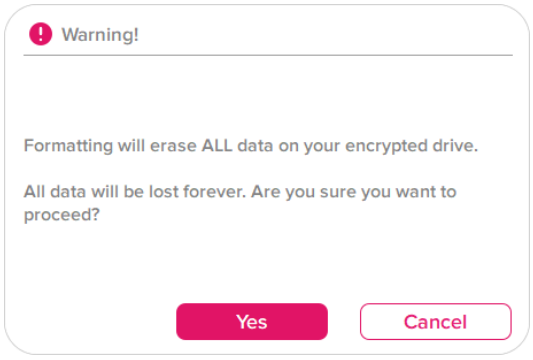
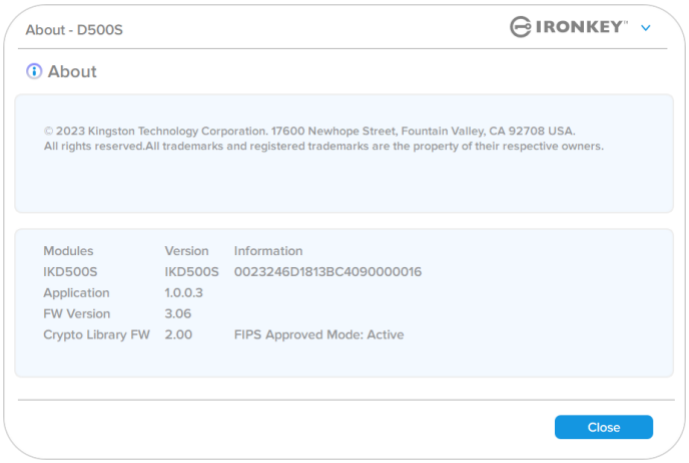
Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey. Kliknięcie ikony IronKey prawym przyciskiem myszy spowoduje otwarcie menu wyboru dostępnych opcji pamięci (*ilustracja 6.2*). Szczegółowe informacje na temat tych opcji znajdują się na str. 21-25 niniejszej instrukcji.

• Po zalogowaniu się do urządzenia w prawym rogu okna będzie widoczna ikona IronKey (*ilustracja 6.1*)	 **Ilustracja 6.1 – Ikona IronKey na pasku zadań**
• Kliknięcie ikony IronKey prawym przyciskiem myszy spowoduje otwarcie menu wyboru dostępnych opcji pamięci (*ilustracja 6.2*). Szczegółowe informacje na temat tych opcji znajdują się na str. 19-23 niniejszej instrukcji.	 **Ilustracja 6.2 – Kliknij ikonę IronKey prawym przyciskiem myszy, aby wyświetlić opcje urządzenia**

Opcje urządzenia – (środowisko macOS)

• Gdy użytkownik jest zalogowany do urządzenia, w menu systemu macOS widoczna jest ikona IronKey D500S (patrz ilustracja 6.3), której kliknięcie powoduje wyświetlenie dostępnych opcji urządzenia. Szczegółowe informacje na temat tych opcji znajdują się na str. 19-23 niniejszej instrukcji.	 **Ilustracja 6.3 – Ikona na pasku menu systemu macOS / menu opcji urządzenia**

Opcje urządzenia

D500S Settings (Ustawienia urządzenia D500S):	• Zmiana hasła logowania, informacji kontaktowych i innych ustawień. (Więcej informacji na temat ustawień urządzenia znajduje się w części „Ustawienia urządzenia D500S" niniejszej instrukcji).
Browse D500S (Przeglądanie zawartości pamięci D500S):	• Umożliwia przeglądanie bezpiecznych plików.
Format D500S (Formatowanie pamięci D500S): Umożliwia sformatowanie bezpiecznej partycji danych. (Ostrzeżenie: wszystkie dane zostaną wymazane) (*ilustracja 6.1*) **Uwaga:** Formatowanie wymaga uwierzytelnienia hasłem.	 **Ilustracja 6.1 – Formatowanie pamięci D500S**
Online Support (Pomoc techniczna online):	• Umożliwia otwarcie przeglądarki internetowej i przejście na stronę http://www.kingston.com/support, gdzie dostępne są dodatkowe informacje.
About D500S (Informacje o pamięci D500S): Dostęp do szczegółowych informacji na temat pamięci D500S, w tym informacji o aplikacji, oprogramowaniu sprzętowym i numerze seryjnym (*ilustracja 6.2*) **Uwaga:** Unikalny numer seryjny znajduje się w kolumnie „Information" (Informacje).	 **Ilustracja 6.2 – Informacje o pamięci D500S**
Shut down D500S (Wyłączenie pamięci D500S):	• Umożliwia prawidłowe wyłączenie pamięci D500S, co pozwala na jej bezpieczne odłączenie od komputera.

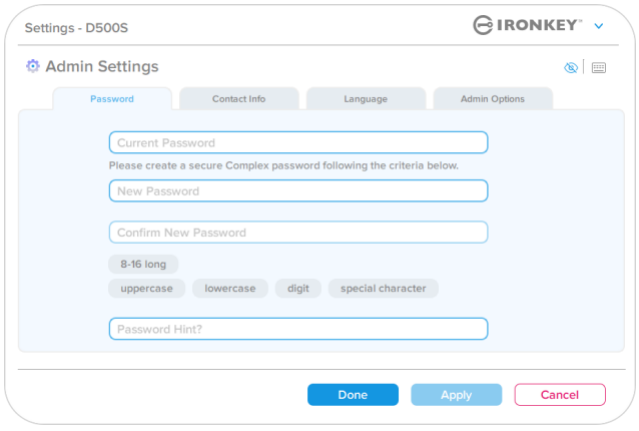
Ustawienia urządzenia D500S

Ustawienia administratora

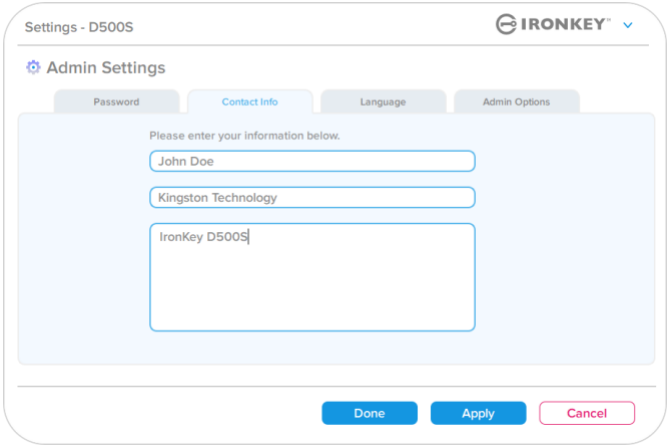
Po zalogowaniu się jako administrator użytkownik ma dostęp do następujących ustawień urządzenia:

- **Password (Hasło):** Umożliwia zmianę hasła lub podpowiedzi hasła administratora (*ilustracja 7.1*)
- **Contact Info (Informacje kontaktowe):** Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 7.2*)
- **Language (Język):** Umożliwia zmianę aktualnie wybranego języka (*ilustracja 7.3*)
- **Admin Options (Opcje administratora):** Umożliwia włączenie dodatkowych funkcji, takich jak (*ilustracja 7.4*)
    - Zmiana hasła użytkownika
    - Resetowanie hasła logowania (dla hasła użytkownika)
    - Jednorazowe hasło odzyskiwania
    - Włączenie hasła Crypto-Erase
    - Wymuszony tryb tylko do odczytu dla danych użytkownika

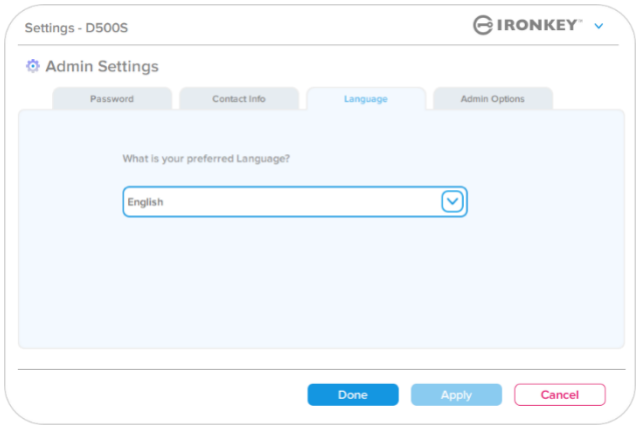
UWAGA: Więcej szczegółowych informacji na temat opcji administratora znajduje się na str. 26 i kolejnych stronach



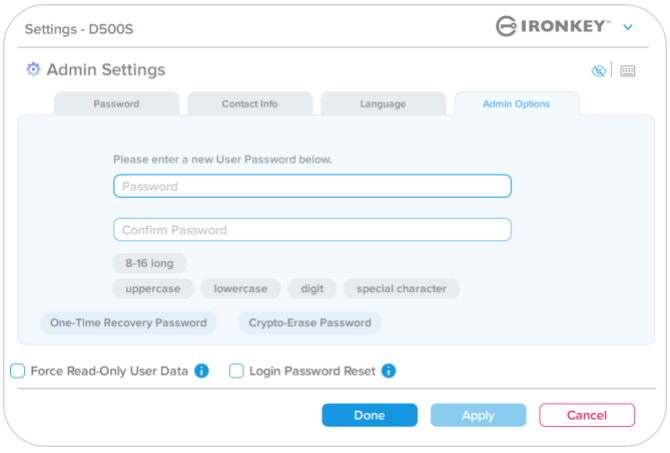
Ilustracja 7.1 – Opcje hasła



Ilustracja 7.2 – Informacje kontaktowe



Ilustracja 7.3 – Opcje języka

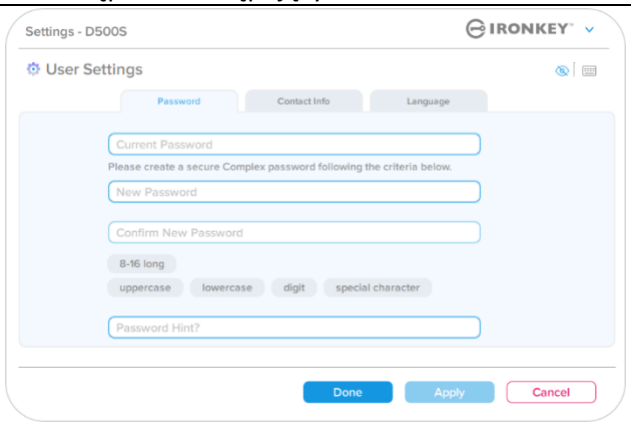
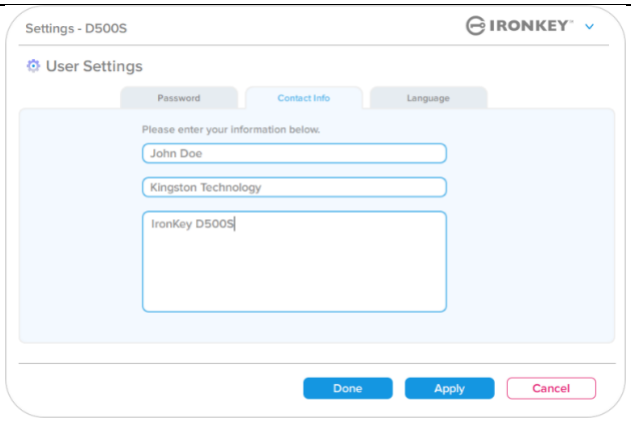
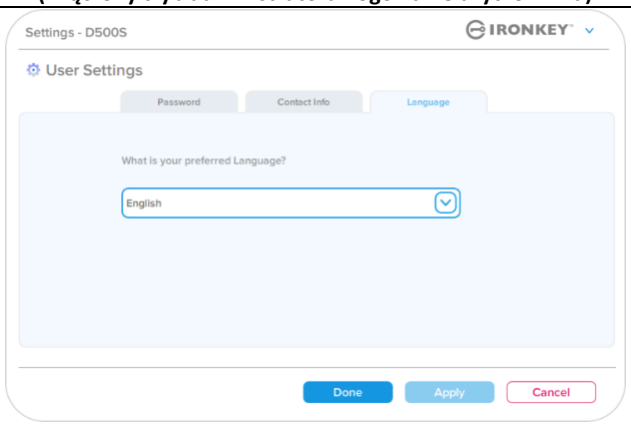


Ilustracja 7.4 – Opcje administratora

Ustawienia urządzenia D500S

Ustawienia użytkownika: włączony tryb administratora

Zalogowanie się jako użytkownik powoduje ograniczenie dostępu do następujących ustawień:

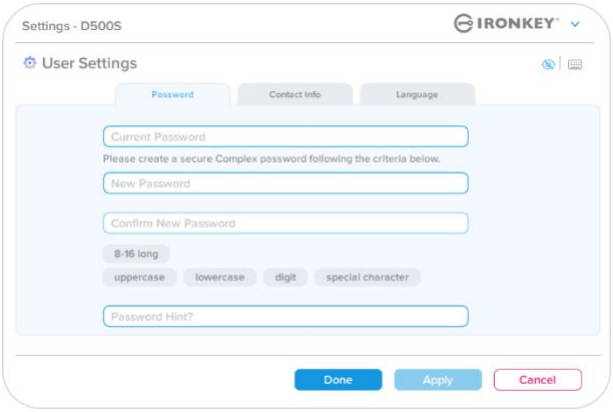
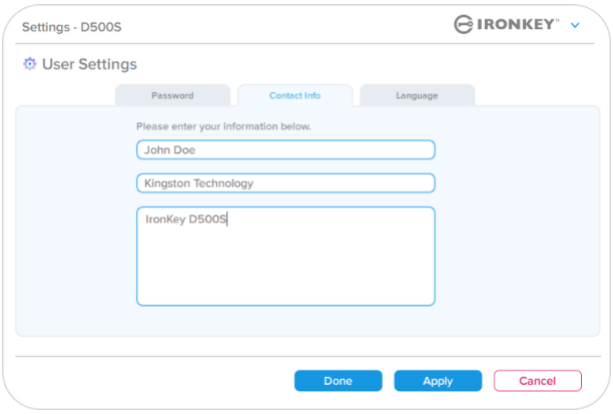
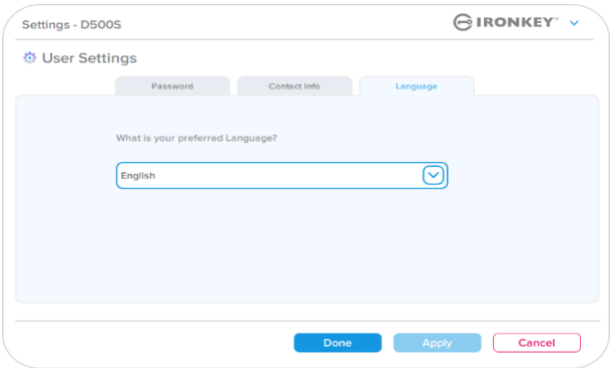
Password (Hasło): Umożliwia zmianę hasła lub podpowiedzi hasła użytkownika (*ilustracja 7.5*)	 **Ilustracja 7.5 – Opcje hasła (włączony tryb administratora: logowanie użytkownika)**
Contact Info (Informacje kontaktowe): Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 7.6*)	 **Ilustracja 7.6 – Informacje kontaktowe (włączony tryb administratora: logowanie użytkownika)**
Language (Język): Umożliwia zmianę aktualnie wybranego języka (*ilustracja 7.7*)	 **Ilustracja 7.7 – Ustawienia języka (włączony tryb administratora: logowanie użytkownika)**

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

Ustawienia urządzenia D500S

Ustawienia użytkownika: wyłączony tryb administratora

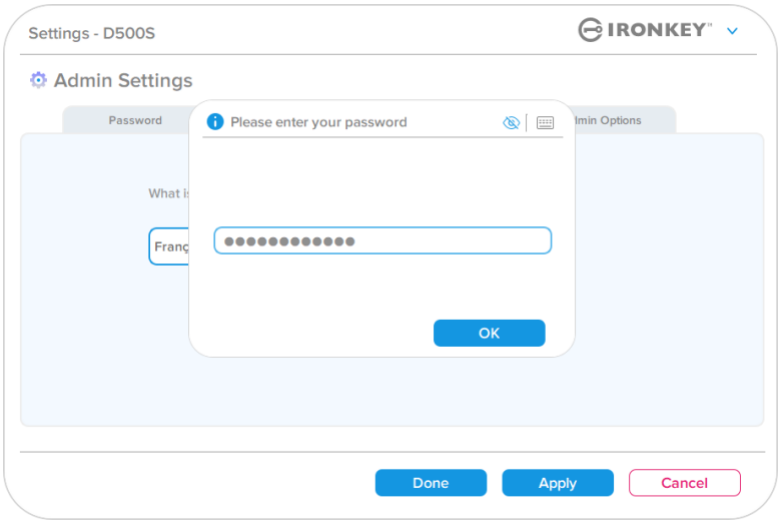
Jak wspomniano wcześniej, zainicjowanie pamięci D500S bez włączania haseł administratora i użytkownika spowoduje skonfigurowanie pamięci z **jednym hasłem dla pojedynczego użytkownika (tryb Tylko użytkownik)**. Konfiguracja ta nie zapewnia dostępu do żadnych opcji ani funkcji administracyjnych. Konfiguracja ta umożliwia dostęp do następujących ustawień pamięci D500S:

Password (Hasło): Umożliwia zmianę hasła lub podpowiedzi hasła użytkownika (*ilustracja 7.8*)	 **Ilustracja 7.8 – Opcje hasła (tryb Tylko użytkownik)**
Contact Info (Informacje kontaktowe): Umożliwia dodanie/wyświetlenie/zmianę informacji kontaktowych (*ilustracja 7.9*)	 **Ilustracja 7.9 – Informacje kontaktowe (tryb Tylko użytkownik)**
Language (Język): Umożliwia zmianę aktualnie wybranego języka (*ilustracja 7.10*)	 **Ilustracja 7.10 – Ustawienia języka (tryb Tylko użytkownik)**

Ustawienia pamięci D500

Zmiana i zapisywanie ustawień

- Po każdej zmianie ustawień pamięci D500S (np. informacji kontaktowych, języka, hasła, opcji administratora itp.) pamięć wyświetli monit o wprowadzenie hasła w celu zaakceptowania i zastosowania zmian (*ilustracja 7.11*).



Ilustracja 7.11 – Ekran monitu o wprowadzenie hasła w celu zapisania zmiany ustawień pamięci D500S

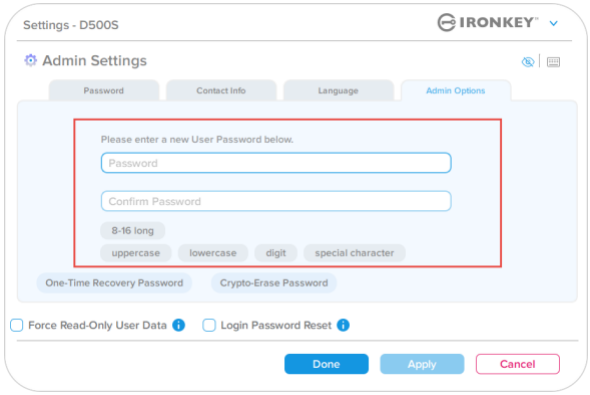
Uwaga: Jeśli wyświetli się ekran z monitem o wprowadzenie hasła (jak powyżej), a użytkownik chce anulować lub zmodyfikować wprowadzone zmiany, może to zrobić, upewniając się, że pole hasła jest puste i klikając przycisk „OK”. Spowoduje to zamknięcie okna „Please enter your password” (Wprowadź hasło) i powrót do menu ustawień pamięci D500S.

Funkcje administracyjne

Dostępne opcje resetowania hasła użytkownika
Funkcje konfiguracji administratora zapewniają wiele możliwości bezpiecznego zresetowania hasła użytkownika, jeśli zostanie ono zapomniane lub jeśli zostanie utworzone tymczasowe hasło użytkownika i administrator będzie chciał wymusić zmianę hasła przy następnym logowaniu użytkownika. Poniżej omówiono funkcje, które mogą być pomocne w zresetowaniu hasła użytkownika.

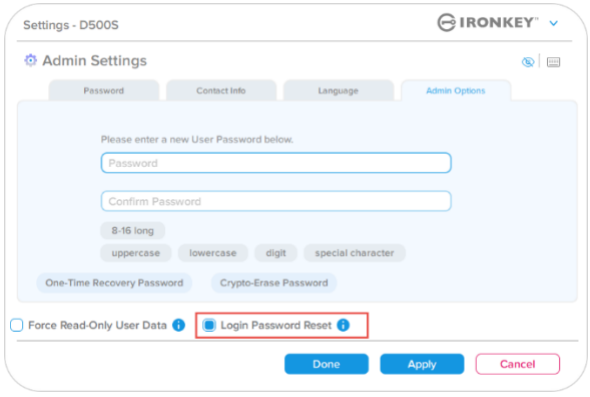
Resetowanie hasła użytkownika:
Ręcznie zmień hasło użytkownika w menu „Admin Options" (Opcje administratora) – zmiana będzie natychmiastowa i zacznie obowiązywać przy następnym logowaniu użytkownika (*ilustracja 8.1*)

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



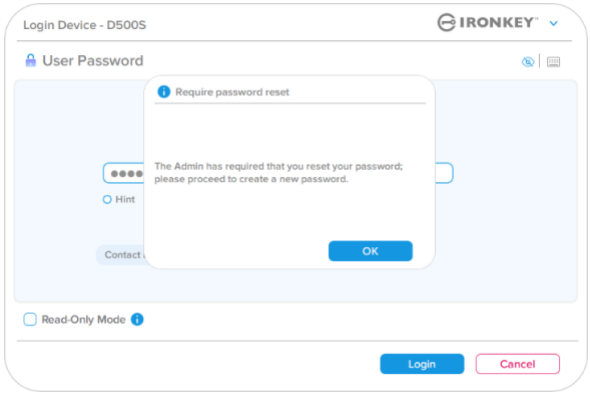
Ilustracja 8.1 – Opcje administratora / Resetowanie hasła użytkownika

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 8.2 i 8.3*).



Ilustracja 8.2 – Przycisk resetowania haseł logowania

Uwaga: Zresetowanie nastąpi po kolejnym udanym zalogowaniu się użytkownika. Kryteria wymagań dla hasła zostaną automatycznie zastosowane zgodnie z pierwotnym ustawieniem podczas procesu inicjalizacji (opcje hasła złożonego lub wyrażenia hasłowego).



Ilustracja 8.3 – Powiadomienie o zresetowaniu po wprowadzeniu hasła użytkownika

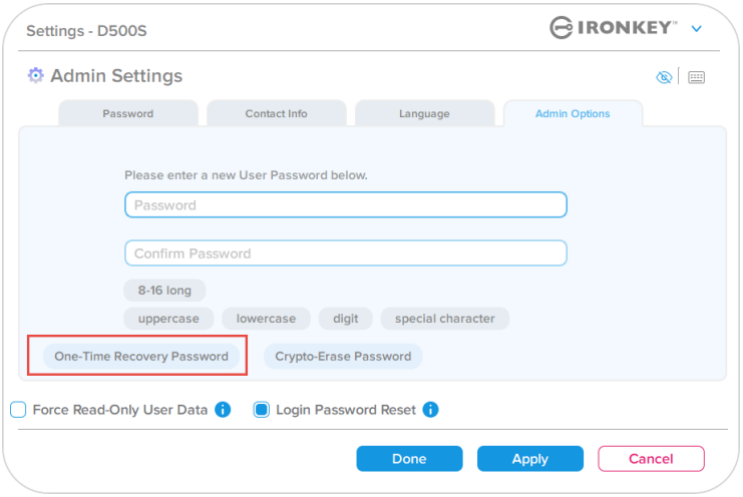
Funkcje administracyjne

Jednorazowe hasło odzyskiwania

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

Jednorazowe hasło odzyskiwania

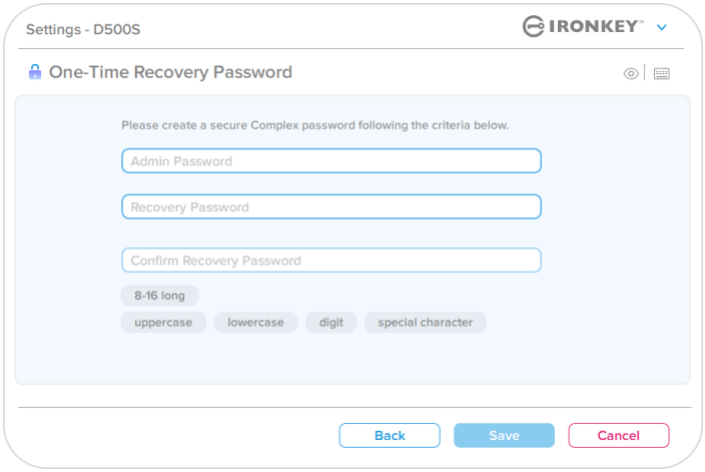
Krok 1: Funkcja jednorazowego hasła odzyskiwania to bardzo przydatna funkcja, którą można włączyć, aby pomóc odzyskać i zresetować hasło użytkownika w przypadku jego zapomnienia. Aby rozpocząć, kliknij przycisk „One-Time Recovery Password” (Jednorazowe hasło odzyskiwania) w menu opcji administratora (*ilustracja 8.4*),



Ilustracja 8.4 – Przycisk jednorazowego hasła odzyskiwania

Krok 2: Utwórz jednorazowe hasło odzyskiwania, korzystając z tych samych kryteriów hasła, które zostały początkowo ustawione na urządzeniu (hasło złożone lub wyrażenie hasłowe).

Uwaga: Do wprowadzenia zmian będzie wymagane hasło administratora.

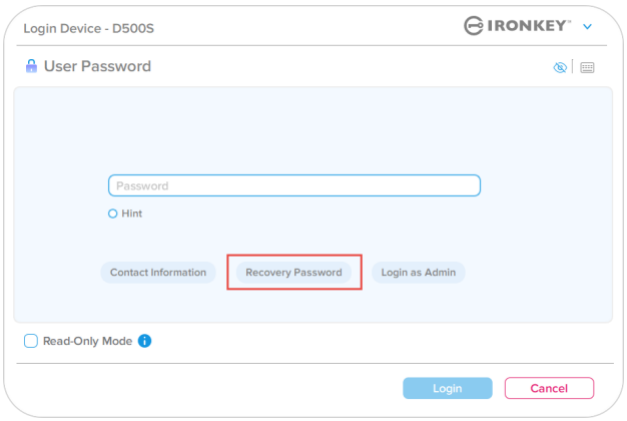


Ilustracja 8.5 – Konfiguracja jednorazowego hasła odzyskiwania

Funkcje administracyjne

Korzystanie z jednorazowego hasła odzyskiwania

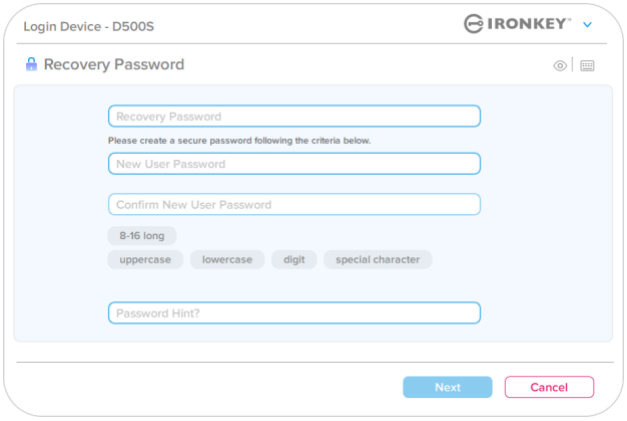
Krok 1: Po utworzeniu jednorazowego hasła odzyskiwania, przy następnym logowaniu na ekranie logowania **User Password (Hasło użytkownika)** pojawi się nowy przycisk. Kliknij przycisk **Recovery Password (Hasło odzyskiwania)**, aby rozpocząć proces.



Ilustracja 8.6 – Przycisk hasła odzyskiwania

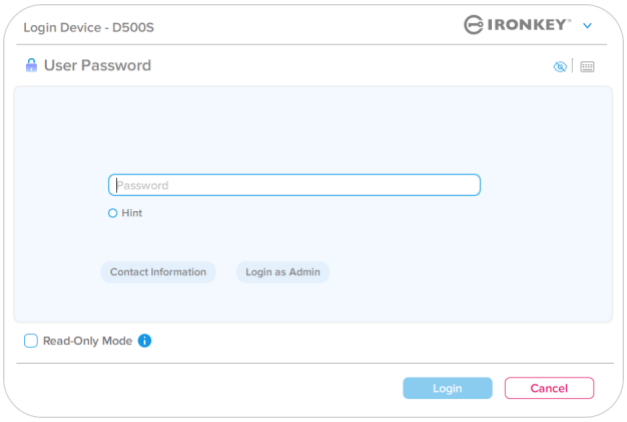
Krok 2: Wyświetli się ekran **Recovery Password (Hasło odzyskiwania)**, na którym można wprowadzić hasło odzyskiwania i utworzyć nowe hasło użytkownika (*ilustracja 8.7*).

Ważne: Jednorazowe hasło odzyskiwania wykorzystuje również wbudowaną funkcję bezpieczeństwa, która śledzi liczbę nieudanych prób logowania. **Po 10 nieudanych próbach zalogowania się za pomocą jednorazowego hasła odzyskiwania hasło zostanie wyłączone** i konieczne będzie jego ponownie włączenie poprzez zalogowanie się do pamięci w roli administratora (więcej szczegółowych informacji podano na str. 19 i 33).



Ilustracja 8.7 – Menu hasła odzyskiwania

Krok 3: Po pomyślnej zmianie hasła zostanie ponownie wyświetlony ekran **User Password (Hasło użytkownika)**. Przycisk **Recovery Password (Hasło odzyskiwania)** zniknie, a hasło użytkownika wprowadzone w kroku 2 stanie się nowym hasłem użytkownika (*ilustracja 8.8*).



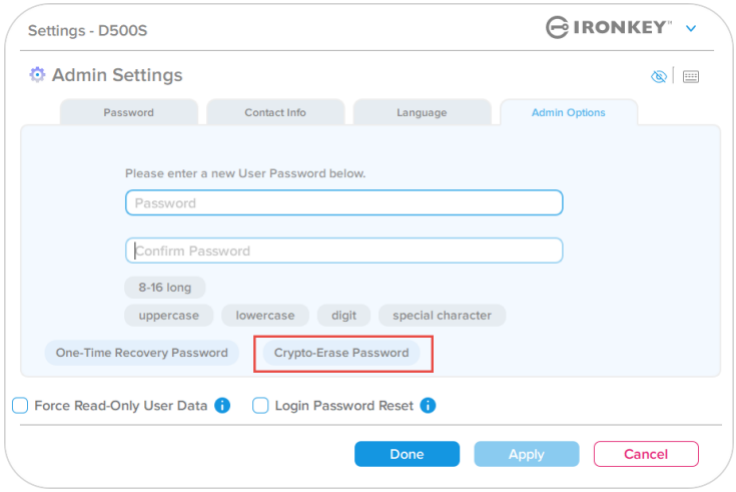
Ilustracja 8.8 – Ekran logowania za pomocą hasła użytkownika bez widocznego przycisku hasła odzyskiwania hasła po jego pomyślnym użyciu.

Funkcje administracyjne

Hasło Crypto-Erase

Urządzenie IronKey D500S jest wyposażone w unikalną funkcję hasła Crypto-Erase, która ma na celu ochronę i obronę w sytuacjach zagrożenia poprzez bezpieczne wymazanie zawartości pamięci w taki sposób, jakby nigdy nie zapisano w niej żadnych danych. Gdy funkcja ta jest włączona i pamięć D500S zostanie odblokowana za pomocą hasła Crypto-Erase, nastąpi dyskretne wymazanie jej zawartości metodą kryptograficzną i przywrócenie pamięci do stanu fabrycznego, z pustą partycją użytkownika. Dotychczasowy klucz szyfrowania urządzenia zostanie usunięty, a w jego miejsce zostanie utworzony nowy klucz szyfrowania. ***Używać ostrożnie!***

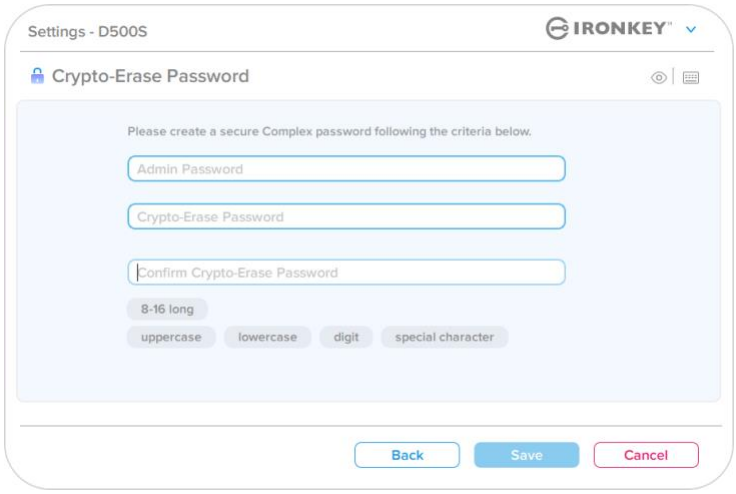
- Aby **włączyć** tę funkcję, kliknij przycisk Crypto-Erase password (Hasło Crypto-Erase) znajdujący się na karcie Opcje administratora:



Ilustracja 8.9 – Włączanie funkcji hasła Crypto-Erase

Utwórz hasło Crypto-Erase:

- Reguły dotyczące hasła będą oparte ustawieniach wybranych przy inicjowaniu pamięci (hasło złożone lub wyrażenie hasłowe)
- W celu zatwierdzenia zmian wymagane jest wprowadzenie hasła administratora.



Ilustracja 8.10 – Tworzenie hasła Crypto-Erase

Funkcje administracyjne

Użycie hasła Crypto-Erase

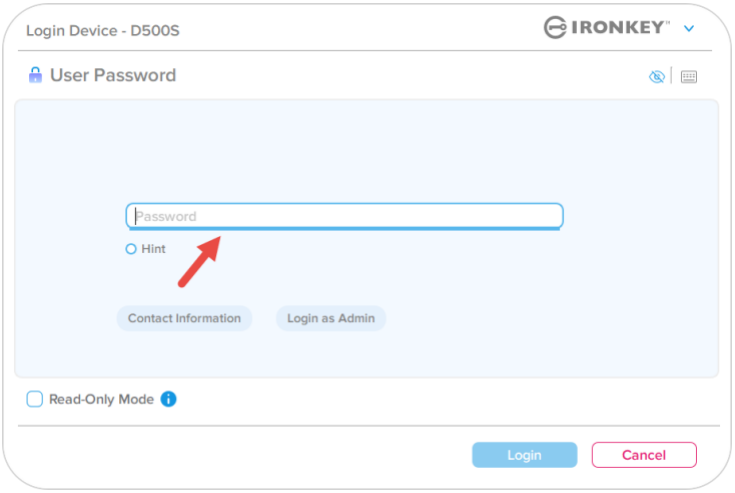
Użycie hasła Crypto-Erase powoduje usunięcie dotychczasowych haseł administratora i użytkownika i zastąpienie ich hasłem Crypto-Erase. Ponadto zostaną trwale usunięte wszystkie dotychczasowe ustawienia konfiguracji i dane przechowywane w pamięci, a pamięć zostanie przełączona w tryb konfiguracji Tylko użytkownik.

Aby użyć hasła Crypto-Erase:

1. Uruchom plik IronKey.exe, aby uruchomić aplikację IronKey.

2. Na ekranie logowania za pomocą hasła użytkownika naciśnij kombinację klawiszy „**CTRL + ALT + C**”, aby przełączyć urządzenie w tryb wprowadzania hasła Crypto-Erase. Po poprawnym wykonaniu tej czynności pod ekranem wprowadzania hasła pojawi się grubszy niebieski pasek, który wskazuje, że urządzenie jest gotowe na wprowadzenie hasła Crypto-Erase (*ilustracja 8.11*)

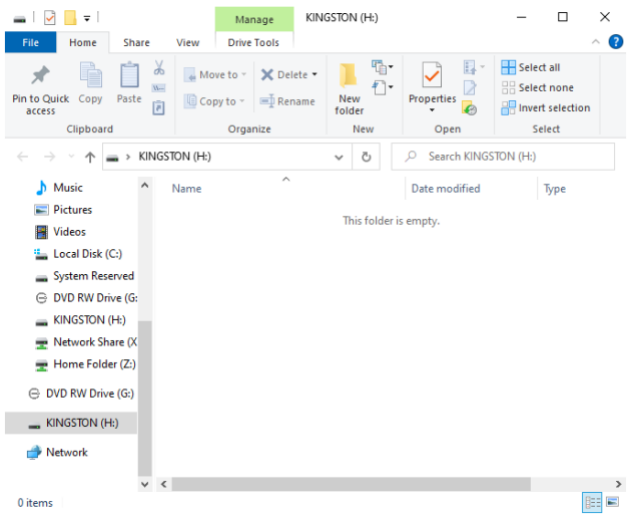
UWAGA: Przełączenie w tryb wprowadzania hasła Crypto-Erase jest możliwe tylko na ekranie logowania za pomocą hasła użytkownika.



Ilustracja 8.11 — Włączony tryb wprowadzania hasła Crypto-Erase (gruby niebieski pasek)

Po użyciu hasła Crypto-Erase urządzenie przystąpi do wymazywania całej zawartości pamięci i pojawi się jedna pusta partycja. Pamięć będzie teraz działać w trybie Tylko użytkownik, a hasło Crypto-Erase stanie się hasłem służącym do logowania się do pamięci, dopóki nie zostanie zresetowane.

Ważne: użycie tej funkcji powoduje bezpowrotne usunięcie z pamięci wszystkich dotychczas zapisanych danych, dlatego należy korzystać z niej ostrożnie.



Ilustracja 8.12 – Czyszczenie pamięci po użyciu hasła Crypto-Erase

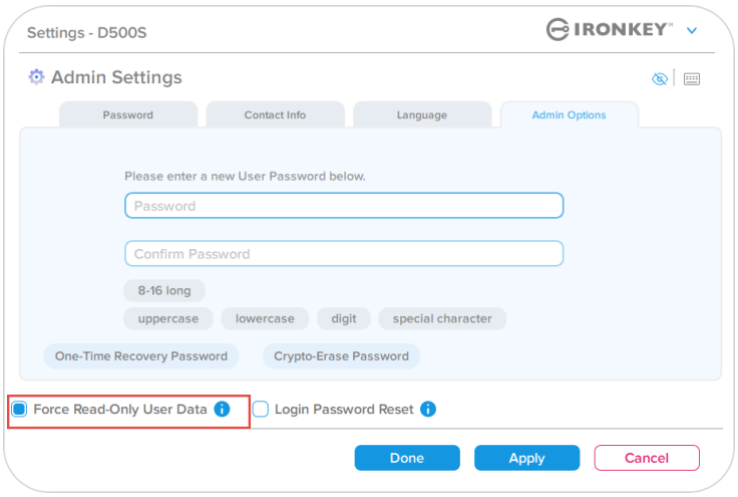
Funkcje administracyjne

Wymuszony tryb tylko do odczytu dla danych użytkownika

Aby uniemożliwić dostęp do pamięci w celu zapisu, można włączyć dla użytkownika wymuszony tryb tylko do odczytu. Funkcja ta jest przydatna, jeśli pliki w pamięci są potrzebne tylko do odczytu.

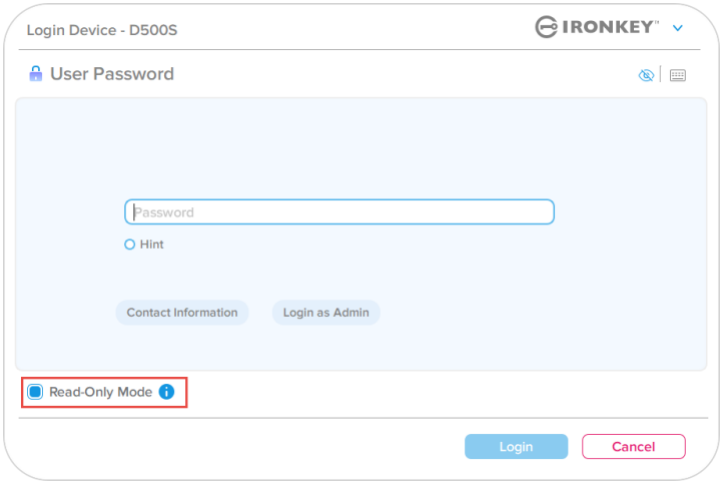
- Aby włączyć wymuszony tryb tylko do odczytu dla danych użytkownika, kliknij odpowiednie pole, następnie przycisk „Apply" (Zastosuj) (*ilustracja 8.13*).

  Uwaga: Wymuszony tryb tylko do odczytu dotyczy wyłącznie użytkownika i nie ma wpływu na logowanie administratora. Administrator nadal będzie miał uprawnienia dostępu do odczytu i zapisu, a w razie potrzeby nadal będzie mógł włączyć tryb tylko do odczytu.



Ilustracja 8.13 – Włączenie opcji „Force Read-Only User Data" (Wymuś dane użytkownika tylko do odczytu) – do wprowadzenia zmian wymagane jest hasło administratora

- Po włączeniu pole zaznaczenia **Read-Only Mode (Tryb tylko do odczytu)** będzie zaznaczone na niebiesko, co oznacza, że wymuszony tryb tylko do odczytu jest na stałe włączony dla hasła użytkownika, dopóki nie zostanie wyłączony przez administratora (*ilustracja 8.14*).



Ilustracja 8.14 – Tryb tylko do odczytu jest wymuszony dla użytkownika i może zostać wyłączony tylko przez administratora

Pomoc i rozwiązywanie problemów

Blokada urządzenia

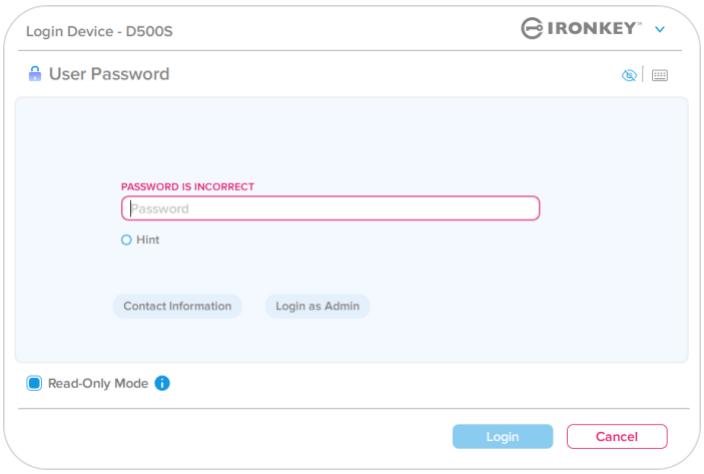
Pamięć D500S jest wyposażona w funkcję bezpieczeństwa, która uniemożliwia nieuprawniony dostęp do partycji danych w przypadku osiągnięcia maksymalnej liczby **kolejnych** nieudanych prób zalogowania (w skrócie *MaxNoA*). W domyślnej fabrycznej konfiguracji ustawiona jest wartość 10 (liczba prób) dla każdej z metod logowania (administrator/użytkownik/jednorazowe hasło odzyskiwania).

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

1. Pomyślne logowanie przed osiągnięciem limitu MaxNoA.

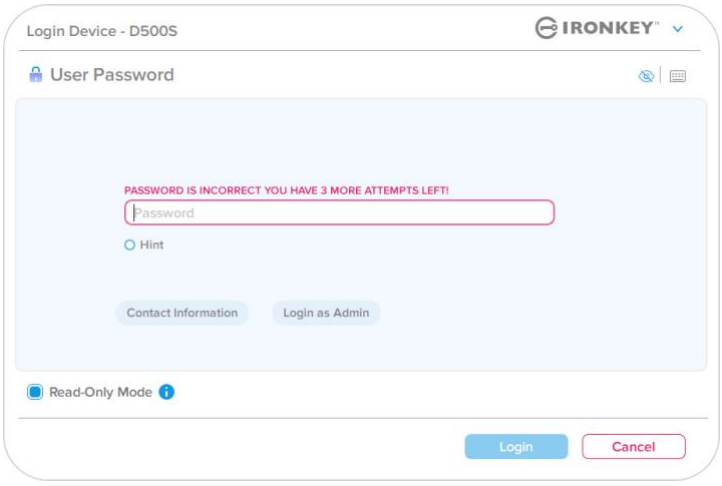
2. Osiągnięcie limitu MaxNoA i zablokowanie lub sformatowanie urządzenia, zależnie od konfiguracji pamięci.

- Jeśli zostanie wprowadzone nieprawidłowe hasło, tuż nad polem wprowadzania hasła pojawi się komunikat o błędzie w kolorze czerwonym, informujący o niepowodzeniu logowania (*ilustracja 9.1*).



Ilustracja 9.1 – Komunikat o wprowadzeniu nieprawidłowego hasła

- Po **siódmej** nieudanej próbie zostanie wyświetlony dodatkowy komunikat o błędzie, informujący o tym, że pozostały trzy próby przed osiągnięciem limitu MaxNoA (ustawionego domyślnie na wartość 10) (*ilustracja 9.2*)



Ilustracja 9.2 – Siódma nieudana próba wprowadzenia hasła

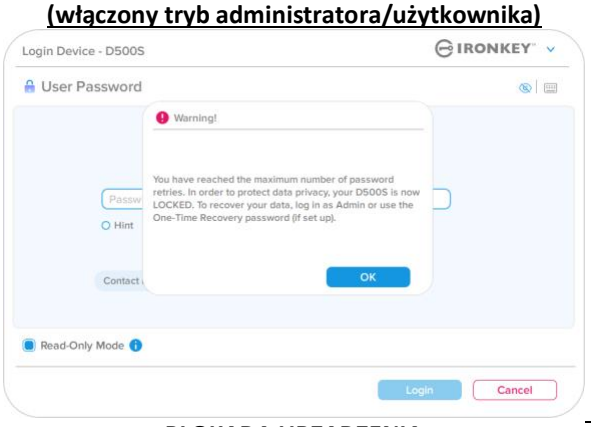
Pomoc i rozwiązywanie problemów

Blokada urządzenia

Ważne: Po **dziesiątej** i ostatniej nieudanej próbie zalogowania, w zależności od tego, jak zostało skonfigurowane urządzenie i jakiej użyto metody logowania (administrator, użytkownik lub jednorazowe hasło odzyskiwania), urządzenie zostanie zablokowane, co będzie wymagało zalogowania się inną metodą (jeśli dotyczy) lub zresetowania urządzenia, co spowoduje **sformatowanie pamięci i bezpowrotną utratę danych**. O takim zachowaniu urządzenia wspomniano również na str. 19 niniejszej instrukcji.

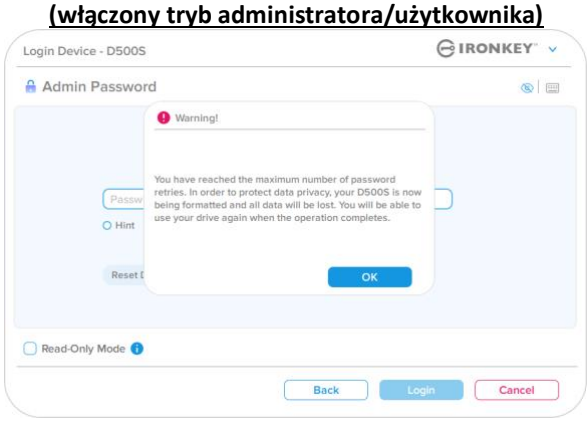
Ilustracje 9.3-9.6 poniżej przedstawiają zachowanie urządzenia po dziesiątej i ostatniej nieudanej próbie zalogowania dla każdej z metod logowania:

Hasło użytkownika:
(włączony tryb administratora/użytkownika)



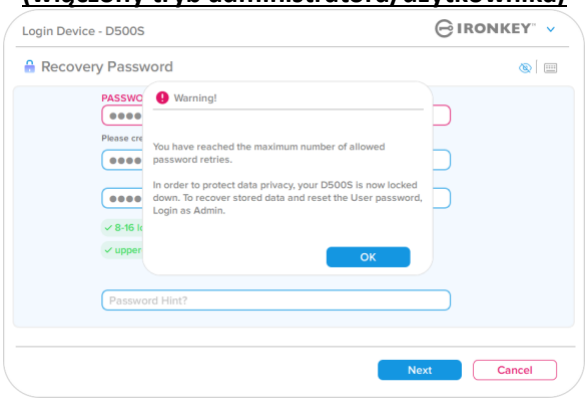
BLOKADA URZĄDZENIA
Ilustracja 9.3

Hasło administratora
(włączony tryb administratora/użytkownika)



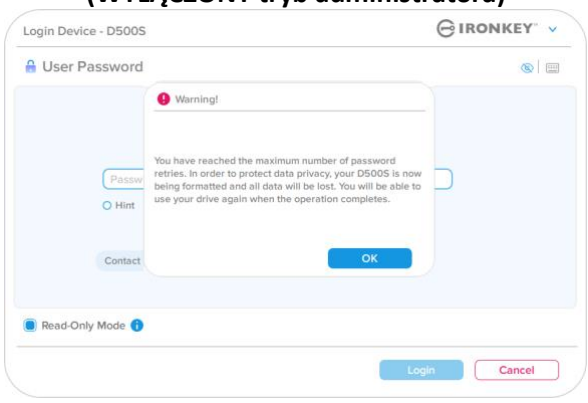
FORMATOWANIE URZĄDZENIA*
Ilustracja 9.4

Jednorazowe hasło odzyskiwania:
(włączony tryb administratora/użytkownika)



BLOKADA URZĄDZENIA
Ilustracja 9.5

Hasło użytkownika
(WYŁĄCZONY tryb administratora)



FORMATOWANIE URZĄDZENIA*
Ilustracja 9.6

Te zabezpieczenia mają na celu ograniczenie możliwości podjęcia nieograniczonej liczby prób zalogowania i uzyskania dostępu do poufnych danych osobom, które nie znają hasła (tzw. atak metodą Brute Force). Jeżeli właściciel pamięci D500S zapomni hasło, zostaną zastosowane takie same środki bezpieczeństwa, w tym również sformatowanie urządzenia.* Aby uzyskać więcej informacji dotyczących tej funkcji, zapoznaj się z rozdziałem *„Resetowanie urządzenia”* na str. 25.

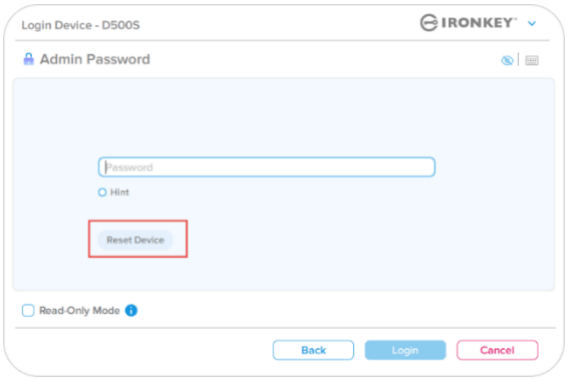
**Uwaga:* *Sformatowanie urządzenia spowoduje wymazanie WSZYSTKICH informacji przechowywanych na bezpiecznej partycji danych pamięci D500S.*

Pomoc i rozwiązywanie problemów

Resetowanie urządzenia

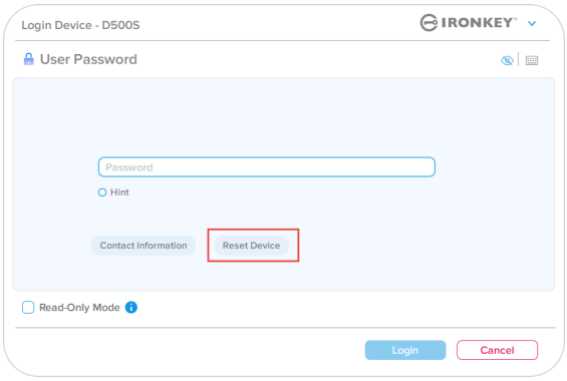
Jeśli użytkownik zapomni hasło lub zechce zresetować urządzenie, może kliknąć przycisk „Reset Device” (Resetuj urządzenie), który pojawia się w jednym z dwóch miejsc, zależnie od konfiguracji urządzenia (w menu hasła logowania administratora, jeśli włączony jest tryb administratora/użytkownika, lub w menu hasła logowania użytkownika, jeśli tryb administratora/użytkownika jest wyłączony), podczas uruchamiania oprogramowania pamięci D500S (patrz *ilustracje 9.7 i 9.8*).

- Ta opcja umożliwia utworzenie nowego hasła, jednak w celu ochrony poufności danych pamięć D500S zostanie sformatowana. Oznacza to, że wszystkie dane zostaną usunięte*.



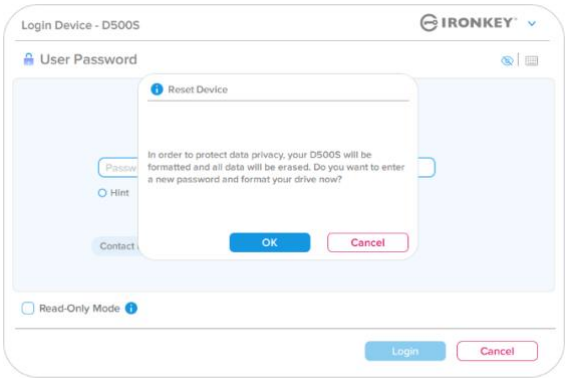
Ilustracja 9.7 – Hasło administratora: przycisk resetowania urządzenia

- **Uwaga:** Po kliknięciu przycisku *„Reset Device” (Resetuj urządzenie)* wyświetla się komunikat z pytaniem, czy użytkownik chce wprowadzić nowe hasło przed rozpoczęciem formatowania. Na tym etapie można 1) kliknąć przycisk *„OK”*, aby potwierdzić, lub 2) kliknąć przycisk *„Cancel” (Anuluj)*, aby powrócić do okna logowania (patrz *ilustracja 9.8*).



Ilustracja 9.8 – Hasło użytkownika (tryb administratora/użytkownika jest wyłączony): przycisk resetowania urządzenia

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



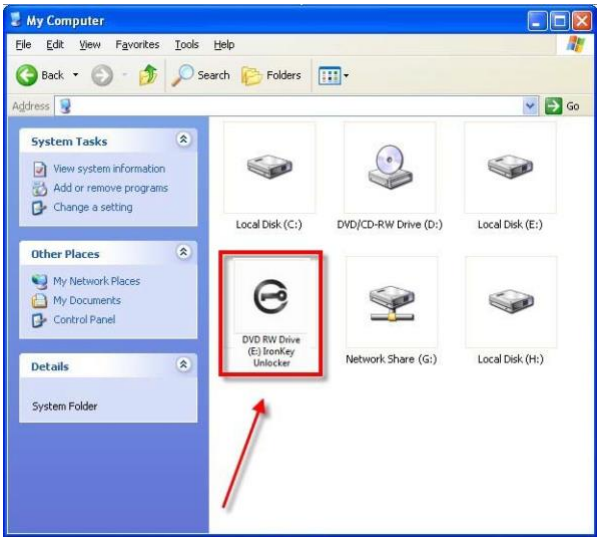
Ilustracja 9.9 – Potwierdzenie resetowanie urządzenia

Pomoc i rozwiązywanie problemów

Konflikt liter dysku: system operacyjny Windows

- Jak wspomniano w części **„Wymagania systemowe”** niniejszej instrukcji (na str. 3), pamięć D500S 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 D500S literę dysku, która jest już używana przez zasób sieciowy lub ścieżkę Universal Naming Convention (UNC), powodując konflikt liter dysku. W takim przypadku należy skontaktować się z administratorem lub działem pomocy technicznej w celu zmiany przypisania liter dysku w obszarze Zarządzanie dyskami systemu Windows (wymagane są uprawnienia administratora). Jak wspomniano w części *„Wymagania systemowe”* niniejszej instrukcji (na str. 3), pamięć D500S wymaga dwóch kolejnych liter dysku PO ostatnim dysku fizycznym, który pojawia się przed „luką” w przypisaniu liter dysku (patrz *ilustracja 9.10*). NIE ma to zastosowania do zasobów sieciowych, ponieważ są one specyficzne dla profili użytkownika, a nie samego profilu sprzętu, przez co wydają się one dostępne dla systemu operacyjnego.



Ilustracja 9.10 – Przykład litery dysku

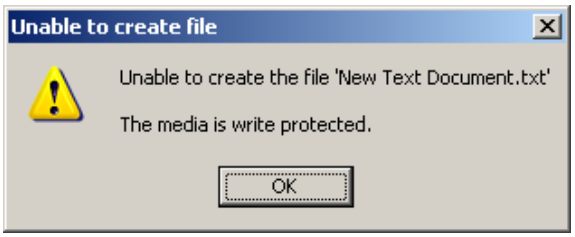
W tym przykładzie (*ilustracja 9.10*) pamięć D500S korzysta z litery dysku F:, która jest pierwszą dostępną literą po literze E: (przypisanej do ostatniego dysku fizycznego przed luką). Ponieważ litera G: jest zasobem sieciowym nieobjętym profilem sprzętu, pamięć D500S może podjąć próbę użycia jej jako drugiej litery, co spowoduje konflikt.

Jeśli w systemie nie ma udziałów sieciowych, lecz urządzenia D500S nadal nie można uruchomić, możliwe, że konflikt powoduje inne, wcześniej zainstalowane urządzenie, do którego przypisano literę dysku (np. czytnik kart lub dysk wymienny).

Funkcja zarządzania literami dysków została znacznie ulepszona w systemach Windows 10 i 11, więc powyższy problem może nie wystąpić. Jeśli jednak nie można rozwiązać konfliktu, należy skontaktować się z działem pomocy technicznej firmy Kingston lub przejść na stronę Kingston.com/support w celu uzyskania dalszej pomocy.

Pomoc i rozwiązywanie problemów

Komunikaty o błędach

Unable to create file (Nie można utworzyć pliku): Ten komunikat o błędzie jest wyświetlany podczas próby UTWORZENIA pliku lub folderu na bezpiecznej partycji danych po zalogowaniu się w trybie tylko do odczytu.	 **Ilustracja 9.11 – Błąd Unable to Create File (Nie można utworzyć pliku)**
Error copying file or folder (Błąd kopiowania pliku lub folderu): Ten komunikat o błędzie jest wyświetlany podczas próby SKOPIOWANIA pliku lub folderu do bezpiecznej partycji danych po zalogowaniu się w trybie tylko do odczytu.	 **Ilustracja 9.12 – Błąd Error Copying File or Folder (Błąd kopiowania pliku lub folderu)**
Error Deleting File or Folder (Błąd usuwania pliku lub folderu): Ten komunikat o błędzie jest wyświetlany podczas próby USUNIĘCIA pliku lub folderu z bezpiecznej partycji danych po zalogowaniu się w trybie tylko do odczytu.	 **Ilustracja 9.13 – Błąd Error Deleting File or Folder (Błąd usuwania pliku lub folderu)**

Uwaga: W przypadku zalogowania się w trybie tylko do odczytu i konieczności odblokowania pamięci z pełnymi uprawnieniami do odczytu/zapisu danych na bezpiecznej partycji należy wyłączyć pamięć D500S i zalogować się ponownie, usuwając przed uwierzytelnieniem zaznaczenie pola wyboru „Read-Only Mode” (Tryb tylko do odczytu).

Korzystanie z urządzenia (środowisko Linux)

Obecnie dostępnych jest wiele różnych dystrybucji systemu Linux, a wygląd i działanie interfejsów w poszczególnych wersjach mogą być różne. Jednak ogólny zestaw poleceń używanych w aplikacji Terminal jest bardzo podobny i może stanowić odniesienie dla poniższych wskazówek dotyczących systemu Linux. Przykładowe zrzuty ekranu pokazane w tej części zostały utworzone w środowisku Linux w wersji 64-bitowej.

W niektórych dystrybucjach systemu Linux do prawidłowego wykonania poleceń dla pamięci D500S w oknie aplikacji Terminal niezbędne są uprawnienia administratora (root).

Ważne uwagi:

1.) **Pamięć D500S nie umożliwia zainicjowania w systemie Linux. Zanim będzie można jej używać w komputerze z systemem Linux, musi zostać zainicjowana i skonfigurowana w obsługiwanym systemie Windows lub macOS.**

2.) **W systemie Linux obsługiwany jest wyłącznie tryb haseł złożonych. Nie jest możliwe zalogowanie się za pomocą wyrażenia hasłowego.**

3.) **Obsługa funkcji pamięci D500S w systemie Linux jest ograniczona. Nie są obsługiwane funkcje jednorazowego hasła odzyskiwania, hasła Crypto-Erase, resetowania hasła administratora/użytkownika oraz trybu tylko do odczytu.**

Pamięć D500S obsługuje 4 polecenia, których można użyć w systemie Linux:

Ikd500s_about	Umożliwia wyświetlenie informacji o pamięci D500S.
Ikd500s_login	Umożliwia zalogowanie się do pamięci.
Ikd500S_logout	Umożliwia bezpieczne wylogowanie się z pamięci D500S.
Ikd500S_resetdevice	Powoduje wyczyszczenie pamięci metodą kryptograficzną (trwałe usunięcie wszystkich przechowywanych danych i plików) i przywrócenie jej do stanu fabrycznego.

UWAGA: Aby wykonać te polecenia, należy otworzyć okno aplikacji Terminal i przejść do folderu, w którym znajdują się te pliki. Każde polecenie musi być poprzedzone następującymi dwoma znakami: „./” (kropka i ukośnik).

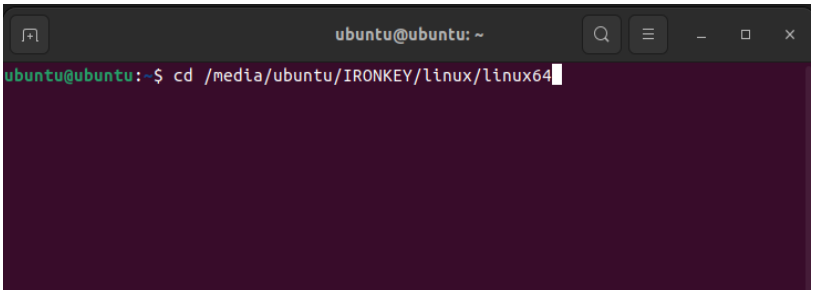
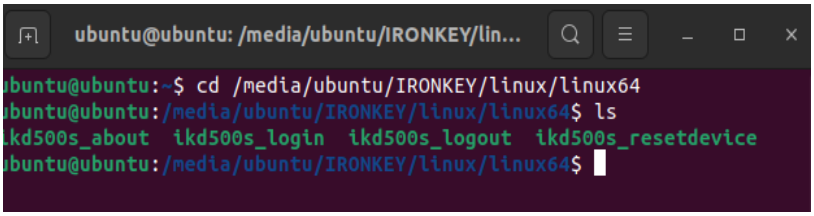
Przykład nawigacji do ścieżki IronKey Linux Commands:

Użytkownicy systemu Linux w wersji 32-bitowej:	Otwórz okno aplikacji „Terminal” i zmień aktualny katalog na **/media/ubuntu/IRONKEY/linux/linux32$**, wpisując w wierszu polecenia następujące polecenie: **cd /media/ubuntu/IRONKEY/linux/linux32** (a następnie naciskając klawisz ENTER).
Użytkownicy systemu Linux w wersji 64-bitowej:	Otwórz okno aplikacji „Terminal” i zmień aktualny katalog na **/media/ubuntu/IRONKEY/linux/linux64$**, wpisując w wierszu polecenia następujące polecenie: **cd /media/ubuntu/IRONKEY/linux/linux64** (a następnie naciskając klawisz ENTER).

Korzystanie z urządzenia (środowisko Linux)

Uwaga: Jeśli system operacyjny nie załaduje automatycznie woluminu pamięci IRONKEY, należy załadować go ręcznie w oknie Terminal, używając polecenia „mount" systemu Linux. Prawidłową składnię i opcje polecenia należy sprawdzić w dokumentacji posiadanej dystrybucji systemu Linux lub preferowanej witrynie pomocy technicznej online. W niektórych dystrybucjach systemu Linux wykonanie poleceń może być niemożliwe bez podania nazwy użytkownika, np. „ubuntu" w powyższych przykładach.

Lokalizowanie i przeglądanie plików poleceń systemu Linux dla pamięci IronKey D500S:

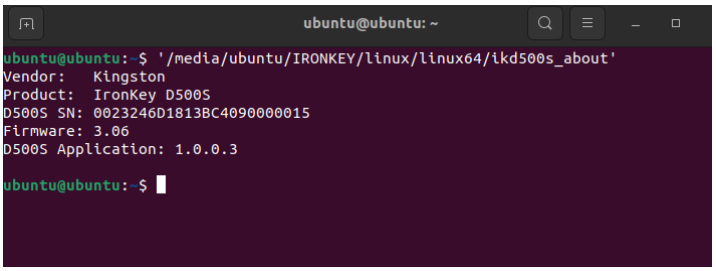
Po podłączeniu pamięci D500S do komputera i rozpoznaniu jej przez system operacyjny zmień katalog na wolumin D500S, wpisując polecenie w wierszu polecenia terminala (*ilustracja 10.1*) **Uwaga:** W celu zilustrowania sposobu użycia pamięci D500S w systemie operacyjnym Linux w zrzutach ekranu i instrukcjach zawartych w tej części wykorzystywany jest folder linux64 (co oznacza system 64-bitowy). W przypadku systemu Linux w wersji 32-bitowej należy po prostu przejść do folderu odpowiedniego dla wersji 32-bitowej, tj. zamiast używać folderu dla wersji 64-bitowej (linux64), używać folderu linux32.	 **Ilustracja 10.1 – Nawigacja w wierszu polecenia**
Użyj polecenia **ls** (lista) w bieżącym wierszu polecenia i naciśnij klawisz ENTER. Spowoduje to wyświetlenie listy plików i/lub folderów znajdujących się w folderze linux64. Wyświetli się lista czterech poleceń IronKey dla systemu Linux (*ilustracja 10.2*) • ikD500S_about • ikD500S_login • ikD500S_logout • ikD500S_resetdevice	 **Ilustracja 10.2 – Wyświetlanie plików poleceń pamięci IronKey w systemie Linux**

Uwaga: W poleceniach i nazwach folderów (katalogów) rozróżniana jest wielkość liter, więc „linux64'" NIE jest tożsame z „Linux64". Składnię także trzeba wpisać dokładnie tak, jak pokazano. W niektórych dystrybucjach systemu Linux wykonanie poleceń może być niemożliwe bez podania nazwy użytkownika – w tym przykładzie jest to „ubuntu".

Korzystanie z urządzenia (środowisko Linux)

Korzystanie z poleceń pamięci D500S

Informacje o pamięci D500S

IkD500S_about (Informacje o pamięci D500S, *ilustracja 10.3*) Wprowadzenie tego polecenia spowoduje wyświetlenie informacji o pamięci D500S, takich jak: • Dostawca • Produkt • Numer seryjny pamięci D500S • Wersja oprogramowania sprzętowego • Wersja oprogramowania	 **Ilustracja 10.3 – ikD500S_about (informacje o pamięci IronKey D500S)**

Logowanie do pamięci D500S

ikD500S_login

Po zainicjowaniu pamięci D500S w obsługiwanym systemie Windows lub macOS można uzyskać dostęp do bezpiecznej partycji danych, logując się do urządzenia przy użyciu wcześniej zdefiniowanego hasła.

W tym celu wykonaj następujące czynności:

1. Otwórz okno aplikacji Terminal.

2. Wpisz w wierszu polecenia terminala następujące polecenie: **cd /media/ubuntu/IRONKEY/linux/linux64**

3. Aby zalogować się do urządzenia, w wierszu polecenia w folderze **/media/ubuntu/IRONKEY/linux/linux64$**, wpisz polecenie: **./ikD500S_login***, po czym naciśnij klawisz ENTER. (Uwaga: w poleceniach i nazwach folderów rozróżniana jest wielkość liter, a używana składnia musi być dokładnie taka sama. Ponadto w niektórych dystrybucjach może być wymagane podanie nazwy użytkownika, np. w tym przykładzie „ubuntu”).

4. Po pomyślnym zalogowaniu się na pulpicie zostanie otwarty bezpieczny wolumin danych i będzie można zacząć używać pamięci D500S (więcej informacji na temat przebiegu logowania znajduje się na następnej stronie).

* Uwaga: W niektórych dystrybucjach systemu Linux do prawidłowego wykonania poleceń dla pamięci D500S w oknie aplikacji Terminal niezbędne są uprawnienia administratora (root).

Korzystanie z urządzenia (środowisko Linux)

Logowanie do pamięci D500S (ciąg dalszy)

IkD500S_login (odblokowanie pamięci D500S, *Ilustracja 10.4*)

Zależnie od tego, jak skonfigurowano pamięć, podczas logowania może być dostępnych kilka opcji jej odblokowania.

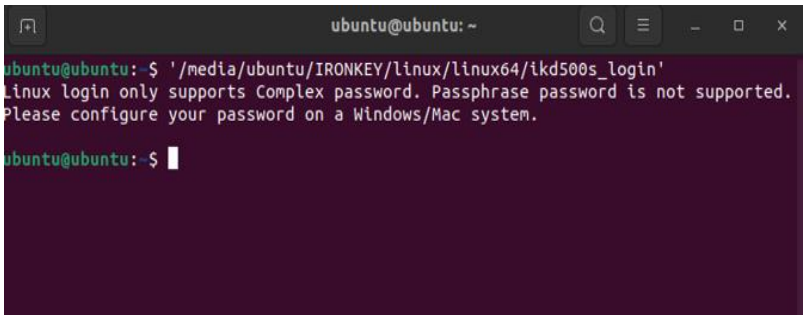
Jeśli podczas inicjowania urządzenia włączono profile **administratora i użytkownika**, wyświetlą się następujące opcje logowania:

1.) Logowanie jako administrator lub użytkownik
2.) Odblokowanie partycji administratora lub użytkownika (jeśli są włączone)
3.) Wprowadzenie odpowiedniego hasła logowania administratora lub użytkownika w celu uwierzytelnienia i odblokowania urządzenia.

Uwaga: Jeśli podczas inicjowania urządzenia NIE zostały włączone profile hasła administratora i użytkownika (tryb Tylko użytkownik), wyświetli się wyłącznie monit o podanie hasła do urządzenia w celu jego uwierzytelnienia.

Ważne: Jak wspomniano wcześniej, w systemie Linux nie są obsługiwane wyrażenia hasłowe, dlatego do logowania w systemie Linux należy skonfigurować pamięć D500S z hasłem złożonym (*ilustracja 10.5*)

Ilustracja 10.4 – ikD500S_login D500S (odblokowanie pamięci D500S)



Ilustracja 10.5 — Próba zalogowania przy użyciu nieobsługiwanego wyrażenia hasłowego.

Korzystanie z urządzenia (środowisko Linux)

Logowanie do pamięci D500S (ciąg dalszy)

Zachowanie urządzenia w przypadku wprowadzenia nieprawidłowego hasła

W przypadku wprowadzenia nieprawidłowego hasła podczas logowania możliwe jest jego ponowne wprowadzenie. Urządzenie ma jednak wbudowaną funkcję bezpieczeństwa, która śledzi liczbę nieudanych prób zalogowania. Jeśli liczba ta osiągnie wstępnie skonfigurowaną wartość 10 nieudanych prób wprowadzenia hasła administratora lub użytkownika, zachowanie urządzenia będzie następujące:

Włączony tryb haseł administratora/użytkownika

- **Logowanie użytkownika:** Zablokowanie użytkownika – wymagane zalogowanie jako administrator (*ilustracja 10.6*). Uwaga: hasło użytkownika można zresetować, logując się jako administrator w obsługiwanym systemie Windows lub macOS.
- **Logowanie administratora:** Wyczyszczenie zawartości pamięci metodą kryptograficzną – bezpowrotna utrata wszystkich danych. Wymagane jest zresetowanie urządzenia (*ilustracja 10.7*).

Tryb Tylko użytkownik (wyłączony tryb administratora/użytkownika)

- **Logowanie użytkownika:** Wyczyszczenie zawartości pamięci metodą kryptograficzną – bezpowrotna utrata wszystkich danych. Wymagane jest zresetowanie urządzenia (*ilustracja 10.7*).

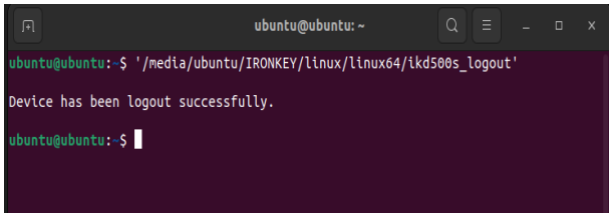
Ilustracja 10.6 — Blokada logowania użytkownika (włączony tryb haseł administratora/użytkownika)

Ilustracja 10.7 — Osiągnięto maksymalną liczbę prób (reset pamięci)

Wylogowanie z pamięci D500S

IkD500S_logout (blokada urządzenia)

Po zakończeniu używania pamięci D500S należy się wylogować i zabezpieczyć dane. W tym celu należy wykonać czynności opisane na str. 39 i prawidłowo użyć następującego polecenia wylogowania z urządzenia: **./ikD500S_logout**, po czym nacisnąć klawisz ENTER (uwaga: w poleceniach i nazwach folderów rozróżniana jest wielkość liter, a używana składnia musi być dokładnie taka sama) (*ilustracja 10.8*)



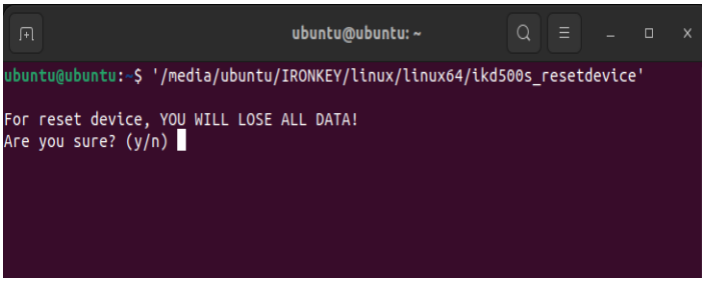
Ilustracja 10.8 – Wylogowanie z pamięci D500S

Korzystanie z urządzenia (środowisko Linux)

Resetowanie urządzenia D500S

ikD500S_resetdevice
Jak wspomniano wcześniej na stronie 41, w przypadku zapomnienia hasła użytkownika/administratora można użyć polecenia Reset Device (Resetuj urządzenie), aby zresetować pamięć w celu dalszego używania. Proces ten umożliwia utworzenie nowego hasła, jednak w celu ochrony poufności powoduje wyczyszczenie pamięci D500S metodą kryptograficzną i sformatowanie bezpiecznej partycji danych. **Oznacza to, że wszystkie dane zostaną utracone.**

Aby użyć polecenia Reset Device (Resetuj urządzenie), należy wykonać czynności opisane na stronie 39 i prawidłowo użyć następującego polecenia wylogowania z urządzenia: **./ikD500S_resetdevice**, po czym nacisnąć klawisz ENTER (uwaga: w poleceniach i nazwach folderów rozróżniana jest wielkość liter, a używana składnia musi być dokładnie taka sama) (*ilustracja 10.9*)



Ilustracja 10.9 – Polecenie resetowania urządzenia

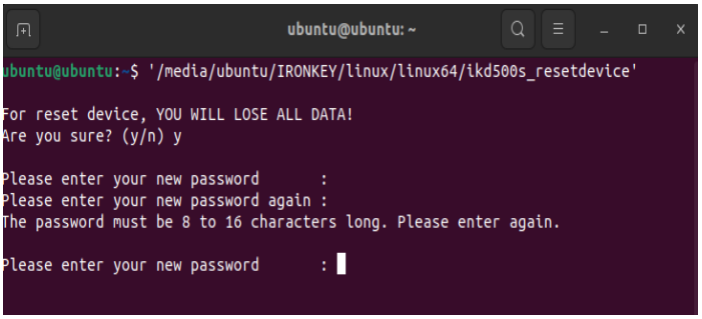
Po użyciu polecenia resetowania urządzenia wyświetli się monit o utworzenie nowego hasła złożonego, które musi zawierać:

- 8-16 znaków należących do co najmniej trzech (3) z następujących kategorii:

  - WIELKIE LITERY
  - małe litery
  - wartości numeryczne
  - znaki specjalne (!,$ itp.)

(*ilustracja 10.10*)

Uwaga: Polecenie Reset Device (Resetuj urządzenie) zainicjuje pamięć w trybie Tylko użytkownik (jedno hasło, jeden użytkownik). Aby możliwe było włączenie profili logowania administratora/użytkownika, pamięć D500S musi zostać skonfigurowana w obsługiwanym systemie Windows lub macOS (pozwoli to na uzyskanie dostępu do tej opcji).



Ilustracja 10.10 – Polecenie resetowania urządzenia, tworzenie hasła

IRONKEY™ D500S
高セキュリティの USB 3.2 Gen 1 フラッシュドライブ

ユーザーガイド

目次

図 1 – IronKey D500S

はじめに

Kingston IronKey D500S は、機密情報保護で評価の高い IronKey の機能を活用した、ミリタリーグレードセキュリティの USB ドライブです。FIPS 140-3 レベル 3 認証（申請中）です。これには、セキュリティ強化のための高セキュリティプロセッサアップグレード要件など、米国国立標準技術研究所 （NIST）の規定した新しいセキュリティ拡張機能が含まれています。暗号化および復号は D500S 上で実行され、ホストシステムには痕跡が残りません。そのため、メモリ内のパスワードを盗み見されるおそれがありません。ハードウェアベースの XTS-AES 256 ビット暗号化とともに、防水*、防塵*、耐衝撃性、エポキシ樹脂シールによる内部部品への侵入攻撃から保護する堅牢な亜鉛製ケースを採用しています。

D500S は、従来の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、一回限りの回復パスワードおよび暗号化消去）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、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 10～128 文字の長さで指定できます。管理者は次のことができます。ユーザーの有効化、管理者 / ユーザーのログインファイルを分離するカスタムサイズのデュアルデータパーティションの作成、一回限りの回復パスワードの有効化、暗号化消去パスワードの有効化、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することです。

パスワードを入力しやすくするために、「目」 のマークを有効にして入力したパスワードを表示し、タイプミスでログインできない事態を減らすことができます。D500S では、パスワードの推測を防止するためにデジタル署名入りのファームウェアを使用しており、BadUSB マルウェアや総当たりパスワード攻撃の影響を受けにくいため安心です。総当たり攻撃保護では、無効なパスワードが連続して 10 回入力された場合、ユーザーパスワードまたは一回限りの回復パスワードをロックし、管理者パスワードが連続して 10 回間違って入力された場合、ドライブに対して暗号化消去を実行します。

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機能が、キーロガーまたはスクリーンロガーからデバイスを守れます***。

中小企業は管理者ロールで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として使用します。

D500S には、多くのカスタマイズオプションがあり、TAA/CMMC 準拠で米国で組み立てられています。

D500S には、5 年限定保証と Kingston 無料技術サポートが付属しています。

* データシートの仕様をご参照ください。使用前に製品を清潔で乾燥した状態にしてください。
** Linux システムでは、パスフレーズモードがサポートされていません。
*** 仮想キーボード：対応の Microsoft Windows および macOS システムでは米国英語のみサポートしています。

IronKey D500S の機能

- XTS-AES 256 ビットハードウェア暗号化で FIPS 140-3 レベル 3 認証（申請中）（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
- 独自のデュアルパーティション、および暗号化消去パスワード
- 入力したパスワードを表示する目のボタンを通じて、ログインの失敗回数が減少
- キーロガーおよびスクリーンロガーから守る仮想キーボード
- 強制またはセッション別の読み取り専用（書き込み保護）設定で、ドライブの内容を変更やマルウェアから保護
- 中小企業は管理者ロールとしてドライブをローカル管理できます。
- Windows、macOS および Linux 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（以降は、「本書」と略します）は、IronKey D500S について、カスタマイズを行っていない出荷時の状態を基にして説明しています。

システム要件

PC プラットフォーム • Intel、AMD および Apple M1 SOC • 15MB のディスク空き容量 • USB 2.0〜3.2 ポート対応 • 最後の物理ドライブの後の、2 つの連続したドライブ文字* ***注**：「ドライブ文字の競合」（35 ページ）を参照してください。	**対応 PC オペレーティングシステム（OS）** • Windows 11 • Windows 10
Mac プラットフォーム • 15MB のディスク空き容量 • USB 2.0〜3.2 ポート	**対応 Mac オペレーティングシステム** • macOS 11.x - 14.x
Linux プラットフォーム • 5MB のディスク空き容量 • USB 2.0〜3.2 ポート	**対応 Linux オペレーティングシステム** • Linux Kernel v4.4 以降

推奨事項

D500S に十分な電力を供給するために、以下の***図 1.1*** に示すように、ノートパソコンまたはデスクトップパソコン本体の USB ポートに直接、差し込んでください。***図 1.2*** に示すようなキーボードや USB から給電するハブなどのように、USB ポートを持つ周辺機器には、D500S 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 D500S 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、MacOS および Linux* 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 D500S 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 にドライブに関する最新のアップデート、FAQ、資料、追加情報があります。

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

*** 購入したばかりの D500S は Linux 上で初期化できず、Windows または MacOS システム上で完全に初期化し、構成する必要があります。その後 Linux で使用することができます。詳細は、本ユーザーガイドの Linux のセクション（37 ページ）に記載されています。**

パスワード設定のベストプラクティス

D500S 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、D500S 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
1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、D500S 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、D500S 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。

D500S では、管理者パスワード（Admin パスワードとも言います）とユーザーパスワードの２つのメインパスワードを選択できます。管理者はいつでもドライブにアクセスし、ユーザーのオプションを設定できます。管理者はスーパーユーザーのようなものです。さらに管理者は、ユーザーがログインしてユーザーパスワードを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。2つのパスワードのうち1つを忘れた場合、他のパスワードでデータアクセスして取得できます。その後、ドライブを2つのパスワードがある状態に設定を戻せます。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、データも他のメディアに保管しておくことをおすすめします。D500S をリセットして再使用できますが、以前のデータは永久に消去されます。

パスワードモード
また D500S では、2つの異なるパスワードモードをサポートします。

複雑なパスワード
複雑なパスワードには、次の文字種のうち最低３種を使用して、8～16 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
D500S では、10～128 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。D500S 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。パスフレーズは複数の単語、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いる一方、ユーザーにとっては覚えやすいものです。

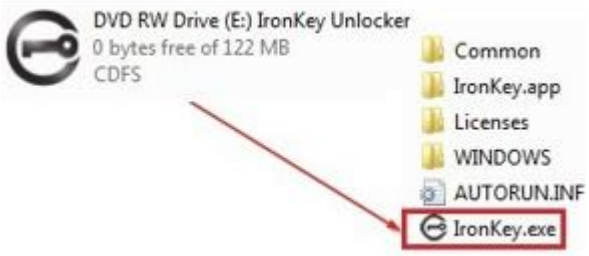
デバイスのセットアップ

IronKey 暗号化 USB ドライブに十分な電力を供給するように、ノートパソコンまたはデスクトップパソコンの USB 2.0/3.0 ポートに直接に差し込んでください。キーボードや USB から給電するハブなどの USB ポート付き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）

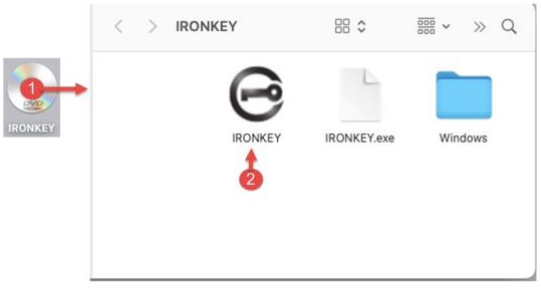
IronKey 暗号化 USB ドライブを、ノートパソコンまたはデスクトップパソコンの空いている USB ポートに差し込み、Windows がこのドライブを検出するまで待ちます。

• Windows10/11 ユーザーは、デバイスドライバの通知を受け取ります。(*図 3.1*)	 **図 3.1 – デバイスドライバの通知**

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

デバイスアクセス（macOS環境）

D500S をノートパソコンまたはデスクトップパソコンの空いている USB ポートに差し込み、Mac がこのドライブを検出するまで待ちます。検出したら、デスクトップに「IRONKEY」というボリュームが表示されます。(*図 3.3*)

• IronKey CD-ROM のアイコンをダブルクリックします • その後、図 3.3 のウィンドウに表示された IronKey.app アプリケーションのアイコンをダブルクリックします。これで初期化プロセスが開始されます。	 **図 3.3 – IronKey ボリューム**

デバイスの初期化（Windows および macOS 環境）

言語と EULA

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

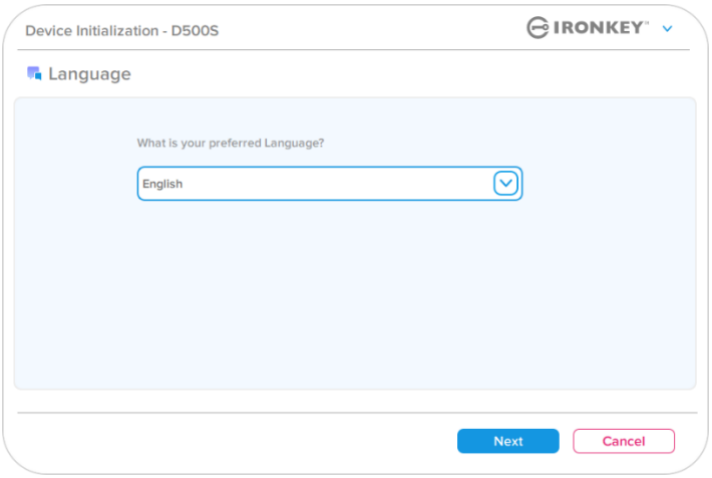


図 4.1 – 言語の選択

使用許諾契約をよく読んで**「次へ」**をクリックします。

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

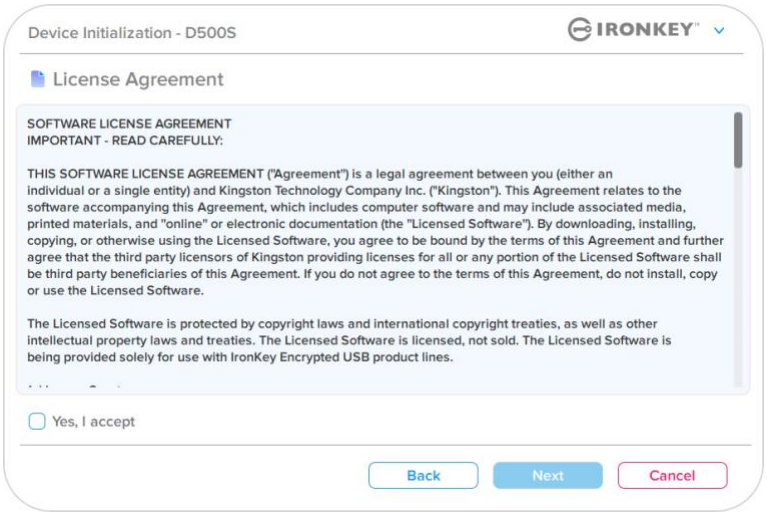


図 4.2 – 使用許諾契約

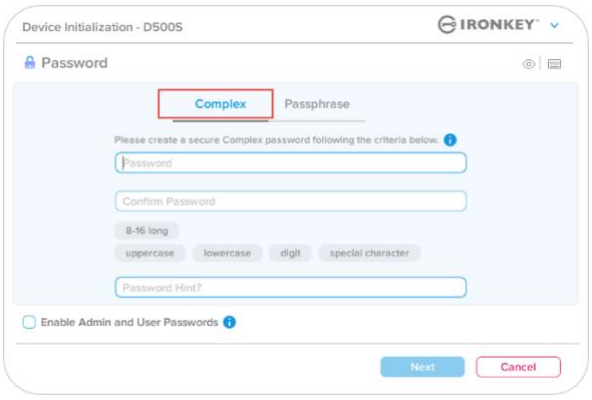
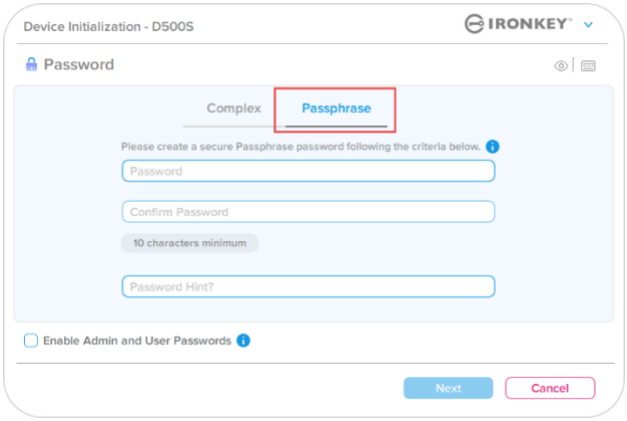
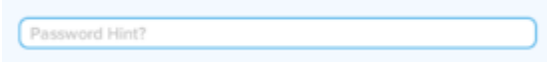
デバイスの初期化

パスワードの選択

パスワード入力画面で、複雑なパスワードかパスフレーズのどちらかを使用して、D500S 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、下記の管理者/ユーザーパスワードの有効化方法をよく読んで、これらの機能をよく理解してください。

注：一旦複雑なパスワードとパスフレーズモードのどちらかを選択した後は、デバイスをリセットするまでモードを変更できません。

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

複雑なパスワード • 文字以上の長さ（最大 16 文字。） • 以下の文字の種類のうち、3 つが含まれていなければなりません。 ○ 英大文字 ○ 英小文字 ○ 数字 ○ 特殊文字 (！ 、$、& など)	 **図 4.3 – 複雑なパスワード**
パスフレーズパスワード • 文字数の制限： ○ 最短 10 文字 ○ 最長 128 文字	 **図 4.4 – パスフレーズパスワード**
パスワードのヒント（任意） パスワードのヒントは、パスワードを忘れた場合に、パスワードの手がかりを示してくれます。 **注**：パスワードと同じ文字列をヒントフィールドに入力することはできません。	 **図 4.5 – 「パスワードのヒント」フィールド**

デバイスの初期化

有効または無効なパスワード

有効なパスワードの場合、基準に合致していると、パスワードの基準ボックスが**緑**で表示されます。
(*図 4.6a ～b を参照*)
注：最低３つのパスワード基準を満たすと、４つ目の基準ボックスがグレーになり、この基準が選択不可であることを示します(*図 4.6b*)

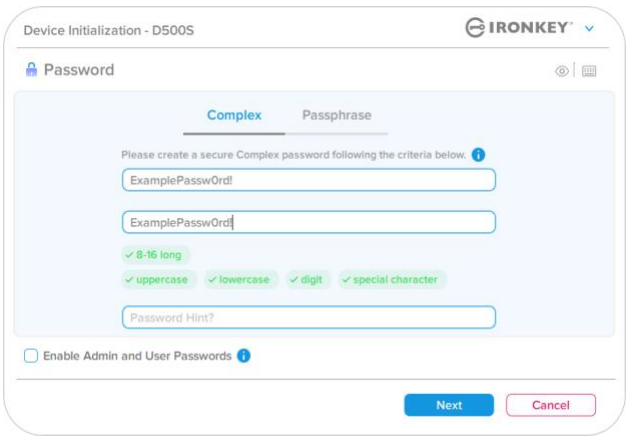


図 4.6a – 複雑なパスワードの条件を満たしている場合

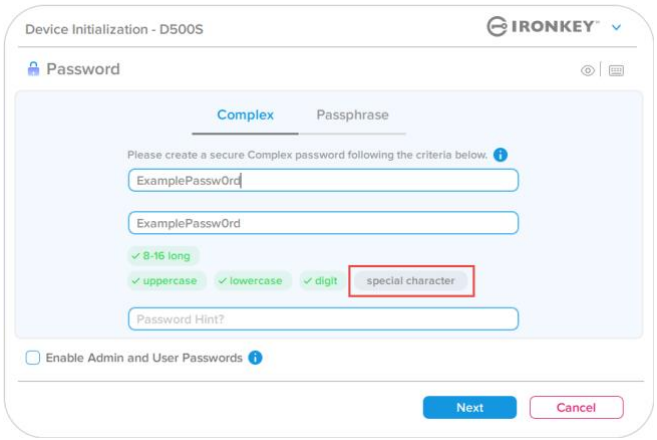


図 4.6b – 任意の複雑なパスワードの条件

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

これは複雑なパスワードとパスフレーズパスワードの両方に適用されます。

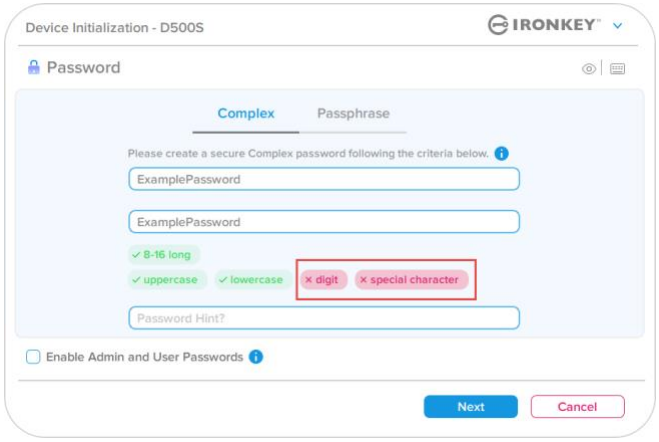


図 4.7 – パスワード条件を満たしていない場合

デバイスの初期化

仮想キーボード

D500S は、キーロガー防止できる仮想キーボードが搭載されています。

- **仮想キーボード**を使用するには、**デバイスの初期化**画面の右上のキーボードボタンを探し、選択します。

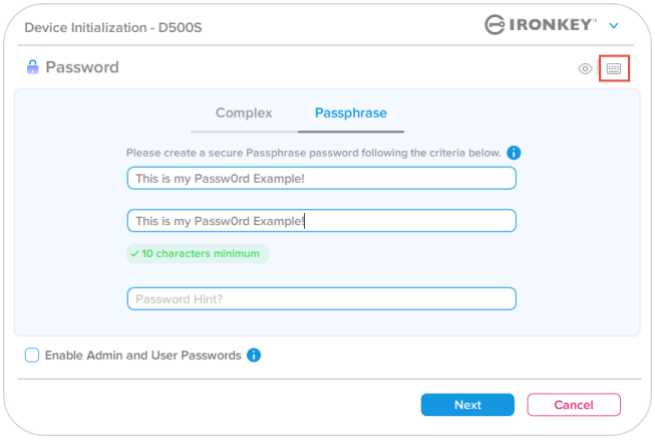


図 4.8 – 仮想キーボードの有効化

- 仮想キーボードが表示された後で、**スクリーンロガー保護**をも有効にすることができます。この機能を使用するとき、すべてのキーが一時的にブランクになります。これは、スクリーンロガーがあなたのクリックした内容を取得することを防ぐための、想定内の動きです。
- この機能をさらに堅牢にするには、キーボードの右下の**ランダム**化を選択して、仮想キーボードのランダム化を選択することもできます。ランダム化すると、キー配列がランダムになります。

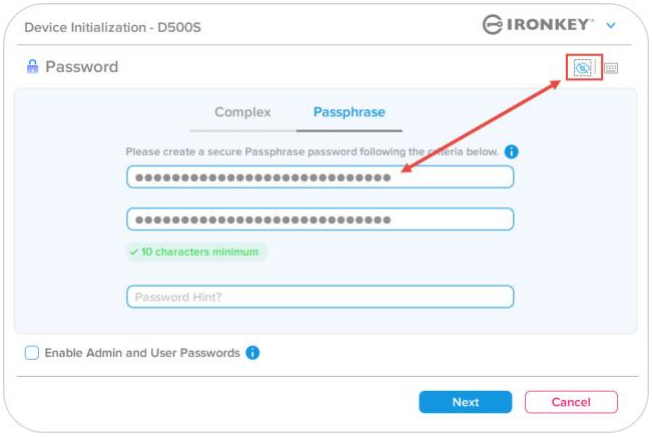
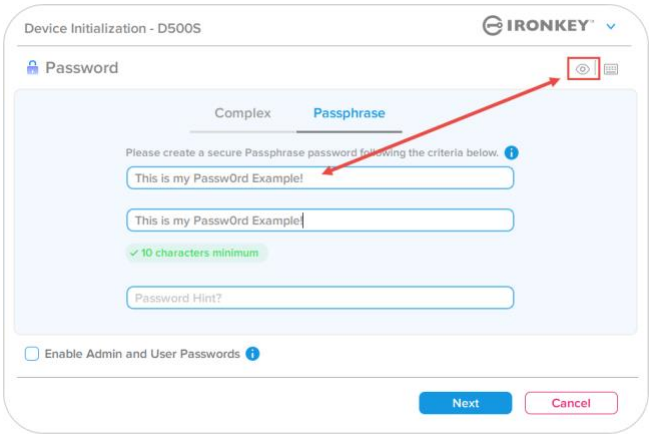
図 4.9 – スクリーンロガー保護/ランダム化

デバイスの初期化

パスワード表示の切り替え

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

注：デバイスが初期化されると、パスワードフィールドはデフォルトの「非表示」になります。

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

デバイスの初期化

管理者およびユーザーのパスワード

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

管理者およびユーザーのパスワードが有効になると、次の機能を利用できます。

- デュアルパーティション構成
- 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
- 暗号化消去パスワード

これらの機能について詳しくは、このユーザーガイドの 25 ページをご覧ください。

- **管理者およびユーザーのパスワード**を有効にするには、**「管理者およびユーザーのパスワードを有効にする」**の隣のボックスをクリックし、有効なパスワードを選択してから**「次へ」**を選択します。(*図 4.12*)

- この機能が**有効**な場合、この画面で選択されているパスワードは**管理者パスワード**になります。**「次へ」**を選択し、**ユーザーパスワード**画面に進んで、ユーザー用のパスワードを選択します。

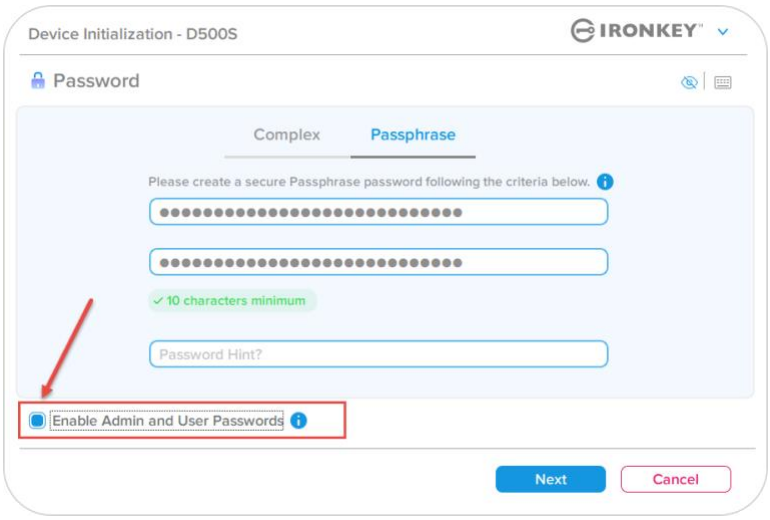


図4.12 – 管理者およびユーザーのパスワードを有効にする

注：管理者およびユーザーのパスワードの有効化は任意です。

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

単一ユーザー、単一パスワード設定で進めるには、**「管理者およびユーザーのパスワードを有効にする」**にチェックしないまま、有効なパスワードを作成してから**「次へ」**をクリックします。

注：このガイドでは、**「管理者およびユーザーのパスワード」**を**「管理者ロール」**と呼びます。

デバイスの初期化

管理者およびユーザーのパスワード

- 前の画面で管理者ロールを有効にした場合、次の画面でユーザーパスワードの入力が求められます（*図4.13*）。**ユーザーパスワード**の機能は管理者よりも制限されていますが、本書で後ほど詳しく説明します（23 ページ参照）。

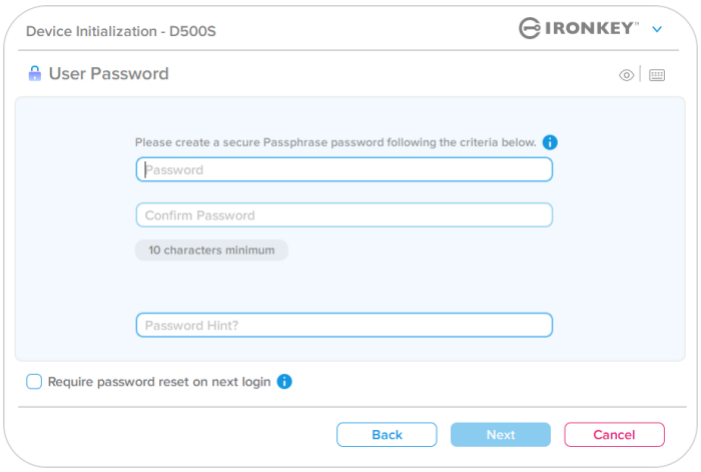


図 4.13 – ユーザーパスワード（管理者とユーザーが有効な場合）

注：選択したパスワードオプション（複雑なパスワードまたはパスフレーズパスワード）の基準は、ユーザーパスワード、一回限りの回復パスワード、暗号化消去パスワード、およびドライブの設定後にリセットが必要なすべてのパスワードに引き継がれます。選択したパスワードオプションは、デバイス全体のリセット後にのみ変更できます。

- 図 4.13 の左下の**「次のログイン時にパスワードのリセットが必要」**機能は、ユーザーパスワードにのみ必要で、初期化プロセス中に管理者によって設定された一時パスワードを使用してユーザーがログインしてから、ドライブが一時パスワードで認証された後で、好きなパスワードに変更するように強制することができます。これは、ドライブを他の使用者に譲る場合に便利です。(*図4.14*)

  注：セキュリティのため、新しいパスワードを一時パスワードと同じにすることはできません。

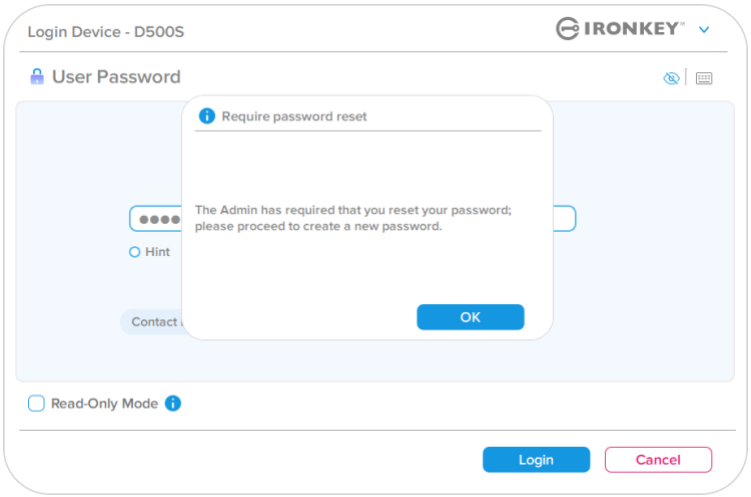


図4.14 – 次回ログイン時にパスワードのリセットが必要 (ユーザーパスワードの場合)

デバイスの初期化

デュアルパーティション

IronKey D500S では、管理者とユーザーに分かれた 2 つのカスタムサイズのパーティションを作成できます。この機能が有効な場合、管理者でログインすると、ユーザーおよび管理者の**両方**のパーティションにアクセスでき、ユーザーでログインするとユーザーパーティション**のみ**にアクセスできます。この機能は、データとファイルのアクセス特権を、ユーザーと管理者で安全に分離するのに役立ちます。または、隠しファイルストアを有効にして、信頼できないシステムで不必要なファイルの露出を防ぐために使用できます。必要な場合、管理者とユーザーのパーティションサイズも調整できます。

注：この機能は*任意*で、設定の際に「デュアルパーティションを有効にする」ボックスのチェックを外したままにすれば無効化できます(*図 4.15*)

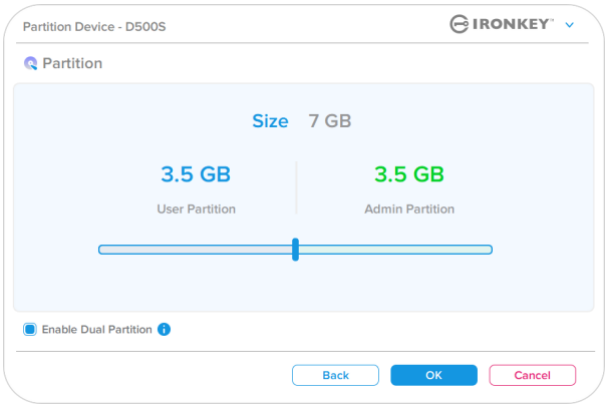


図 4.15 – パーティションデバイス

ユーザーと管理者の間でパーティションサイズを調整して割り振るには、スライダを左右に移動します（(*図 4.16*).

- パーティションは 0.5GB 単位で調整できます。
- パーティションサイズは、隠しパーティション上の利用可能なストレージの総容量に基づきます。
- 手動で調整しない限り、デュアルパーティションのスライダはデフォルトで、管理者とユーザーのストレージを等分するように設定されています。
- 割り振り可能な最小パーティションサイズは 1GB です。

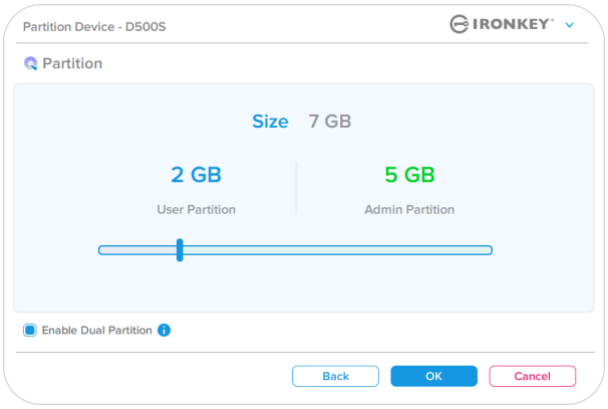


図 4.16 – パーティションデバイス、スライダー調整済み

管理者でのログイン

デュアルパーティションを有効にしてデバイスを最後まで設定すると、管理者でログインした場合、管理者パーティションまたはユーザーパーティションのどちらかにアクセスするためのドライブのロック解除オプションが、ログインに成功するごとに表示されます。(*図 4.17*)

注：一度に1つのパーティションだけを開くことができます。ユーザーおよび管理者パーティションの両方を同時にロック解除することはできません。

ユーザーログインではこのオプションが表示されず、ユーザーパーティションのみが自動的にロック解除します。

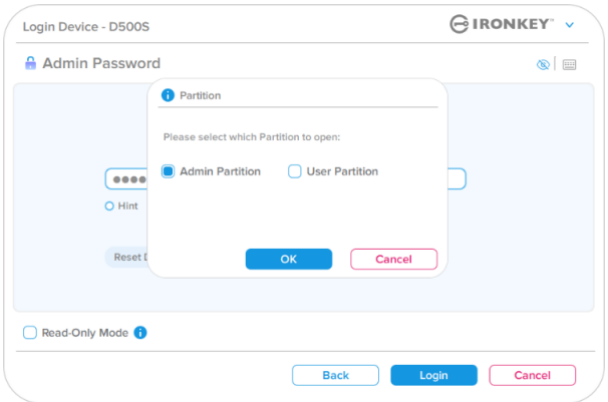


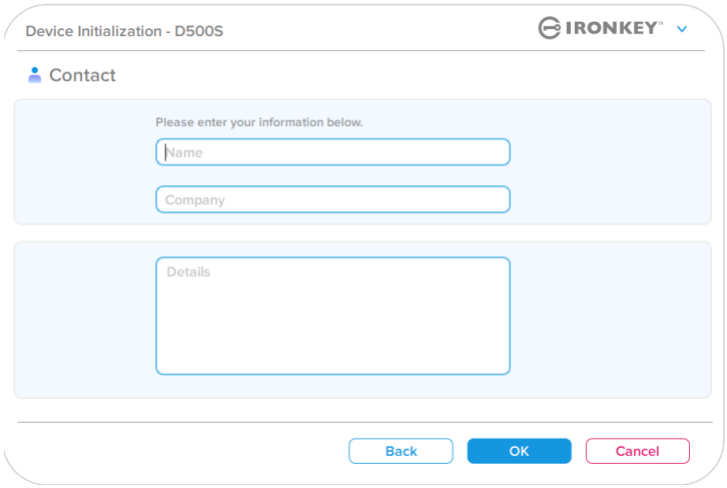
図 4.17 – 管理者ログインの例、パーティションの選択

デバイスの初期化

連絡先情報

表示されたテキストボックスに連絡先情報を入力してください（*図4.18 参照*）

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

「名前」フィールドには、最大 32 文字を入力できますが、パスワードとまったく**同じ**文字列を入れることはできません。 **「会社名」**フィールドには、最大 32 文字を入力できますが、パスワードとまったく**同じ**文字列を入れることはできません。 **「詳細」**フィールドには、最大 156 文字を入力できますが、パスワードとまったく**同じ**文字列を入れることはできません。	 **図 4.18 – 連絡先情報**

注：「OK」をクリックすると、初期化プロセスが完了し、アンロックに進んで、データを安全に保存できる安全なパーティションを取り付けます。ドライブの取り外しに進んでから、システムに差し込み直して、変更が反映されているかを確認します。

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 D500S 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。「管理者としてログイン」ボタン（下図参照）をクリックすると、アプリケーションは管理者ログインメニューに進み、そこで管理者としてログインして管理者の設定と機能にアクセスすることができます(*図5.2*).

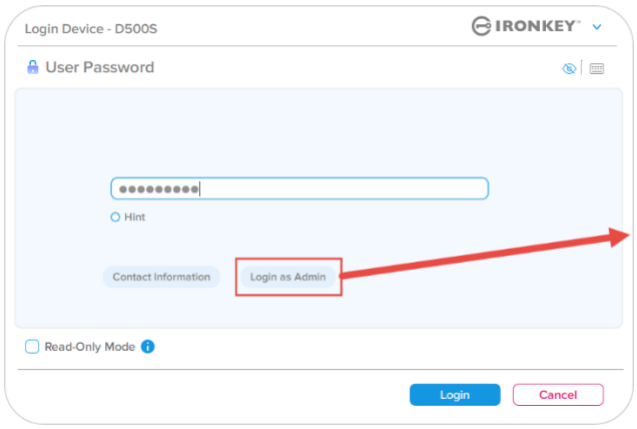


図 5.1 – ユーザーパスワードでのログイン（管理者が有効な場合）

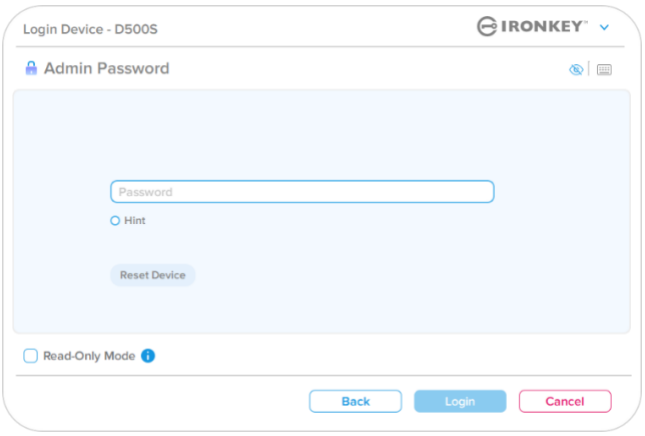


図 5.2 – 管理者パスワードでのログイン

ユーザー専用モードでのログイン（管理者が無効な場合）

前述したように、デバイスの利点を完全に活用するには、管理者ロール機能の使用が推奨されますが、ユーザー専用モード（単一パスワード、単一ユーザー）設定でも IronKey ドライブを初期化できます。これは、シンプルな単一パスワード手法を好む人が、ドライブでデータの安全を保つためのオプションです。(*図5.3*)

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

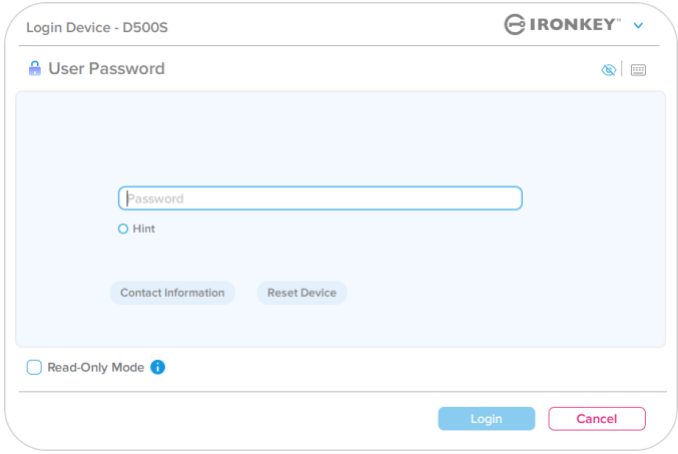


図 5.3 – ユーザーパスワードでのログイン（管理者が無効な場合）

デバイスの使用

読み取り専用モードでのアンロック

IronKey ドライブ上のファイルが変更されないように、読み取り専用モードでドライブをアンロックできます。たとえば、信頼性が低いか、よく知らないコンピュータを使用する時に、読み取り専用モードでアンロックすれば、そのコンピュータにあるマルウェアがデバイスに感染することや、ファイルを変更することを防げます。

このモードで作業する時、デバイス上のファイルの変更などの操作は一切実行できません。
たとえば、デバイスの再フォーマットや、ドライブ上のファイルのリストア、追加、編集はできません。

読み取り専用モードのデバイスのロックを解除するには：

1. ホストコンピュータの USB ポートにデバイスを差し込み、ファイル **IronKey.exe** を実行します。
2. パスワード入力ボックスの下の**「読み取り専用モード」**をチェックします(*図 5.4*)。
3. デバイスのパスワードを入力して**「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デバイスがロック解除されました。

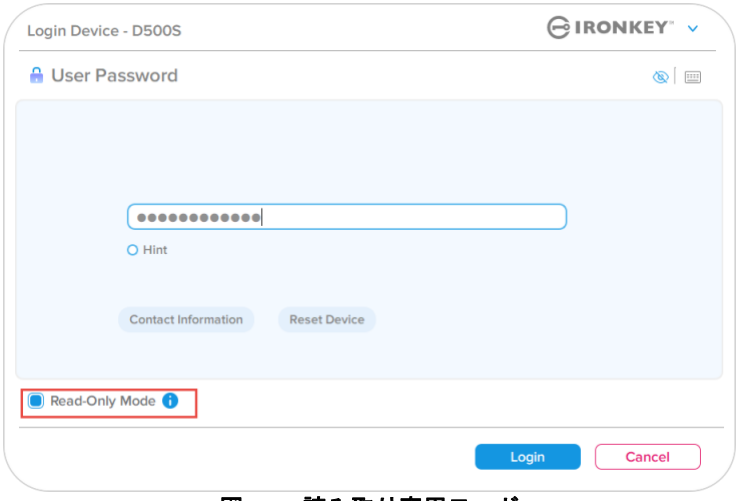


図 5.4 – 読み取り専用モード

デバイスのロックを解除して、セキュリティで保護されたデータのパーティションに対して完全に読み書きのアクセスができるようにするには D500S を一度シャットダウンして、再度ログインし直し、「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：D500S 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 31 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直せます。ただし、不正アクセス回数を記録するセキュリティ機能（総当たり攻撃防止機能ともいいます）がありますのでご注意ください。*

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

管理者/ユーザー有効	**総当たり攻撃防止 デバイスの動作 （間違ったパスワードを 10 回）**	**データの消去および デバイスのリセット？**
ユーザーパスワード	パスワードがロックされます。 管理者として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。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/ユーザーが無効な場合)	**総当たり攻撃防止 デバイスの動作 （間違ったパスワードを 10 回）**	**データの消去および デバイスのリセット？**
ユーザーパスワード	ドライブを暗号化消去します。パスワード、 設定、およびデータが永久に消去されます	**はい**

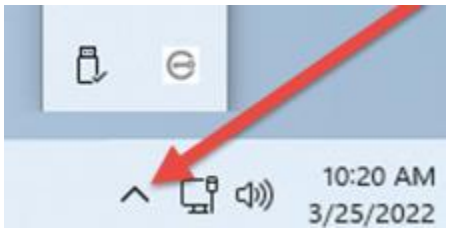
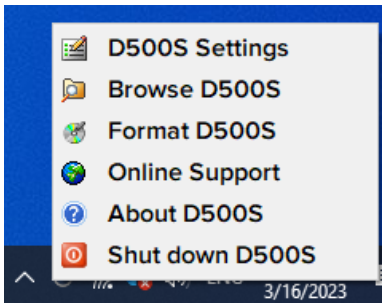
* デバイスの認証に一回成功すると、使用したログイン方式に関するログイン失敗カウンタがリセットされます。暗号化消去は、すべてのパスワード、暗号化キーおよびデータを削除します。**データは恒久的に失われます。**

保護下のファイルへのアクセス

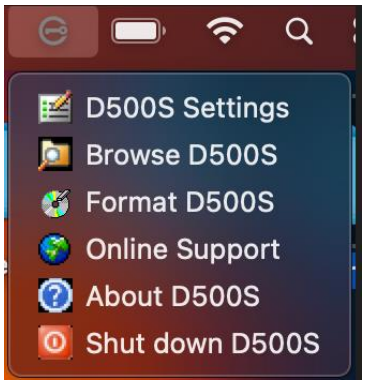
ドライブのロック解除後、保護下のファイルにアクセスできます。ドライブでそれらのファイルを保存するか開くと、自動的に暗号化および復号されます。このテクノロジーによって、強力な「常時オン」のセキュリティを利用しながら、いつものドライブでいつもの通り、便利に作業できます。
ヒント：ファイルにアクセスするには、Windows タスクバーの **IronKey** アイコンを右クリックしてから、**「D500S の表示」**をクリックします（*図 6.2*）

デバイスの各種オプション - (Windows 環境の場合)

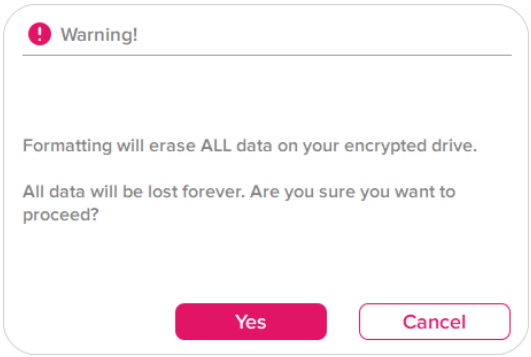
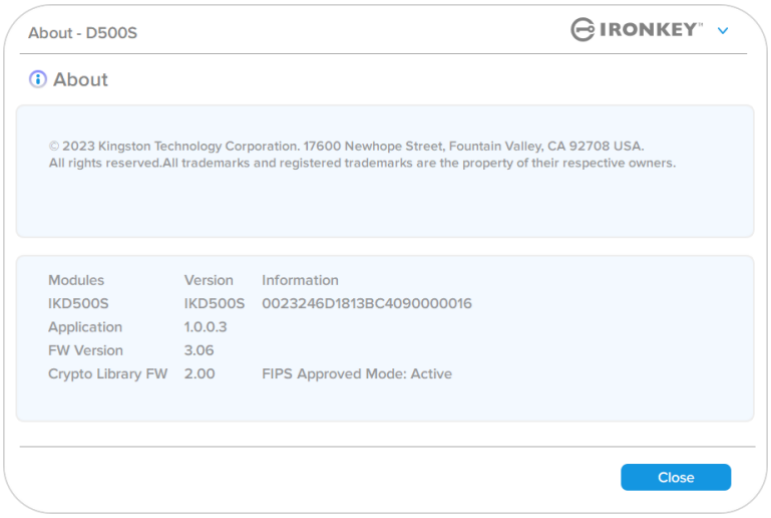
デバイスへログインしている状態では、ウィンドウの右隅に IronKey アイコンが表示されます。IronKey アイコンを右クリックすると、利用可能なドライブオプションの選択メニューが開きます（*図 6.2*）。
これらのデバイスオプションについて詳しくは、本書の 21～25 ページにあります。

デバイスへログインしている状態では、ウィンドウの右隅に IronKey アイコンが表示されます（*図 6.1*）	 **図 6.1 タスクバーの IronKey アイコン**
• IronKey アイコンを右クリックすると、利用可能なドライブオプションの選択メニューが開きます（*図 6.2*）。 これらのデバイスオプションについて詳しくは、本書の 19～23 ページにあります	 **図 6.2 IronKey アイコンをクリックしてデバイスオプションを表示**

デバイスの各種オプション - (macOS 環境の場合)

• デバイスへのログイン中には、図 6.3 のように macOS メニューの中に IronKey D500S アイコンがあり、利用可能なデバイスオプションを開くことができます。 これらのデバイスオプションについて詳しくは、本書の 19～23 ページにあります。	 **図 6.3 – macOS メニューバーアイコン/デバイスオプションメニュー**

デバイスオプション

D500S の設定：	• ログインパスワード、連絡先情報、その他の設定を変更します。（デバイス設定について詳しくは、本書の「D500S の設定」セクションにあります。）
D500S の表示：	• 保護下のファイルを表示できます。
D500S のフォーマット： 保護下のデータパーティションをフォーマットできます。（警告：データはすべて消去されます。）（*図 6.1*）。 **注：**フォーマットにはパスワード認証が必要です。	 **図 6.1 – D500S のフォーマット**
オンラインサポート：	• インターネット・ブラウザを開いて http://www.kingston.com/support に移動すると、詳しいサポート情報にアクセスできます
D500S について： アプリケーション、ファームウェア、シリアル番号情報など、D500S について詳しく説明します（*図 6.2*）。 **注：**ドライブの固有なシリアル番号は「情報欄」の下にあります	 **図 6.2 – D500S について**
D500S のシャットダウン：	• D500S 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。

D500S 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**：連絡先の情報を追加/表示/変更できます（*図 7.2*）。
- **言語**：現在の言語を変更できます（*図 7.3*）。
- **管理者オプション**：次のような追加機能を有効にできます。（*図 7.4*）。
    - ユーザーパスワードの変更
    - ログインパスワードのリセット（ユーザーパスワードの場合）
    - 一回限りの回復パスワードの有効化
    - 暗号化消去パスワードの有効化
    - ユーザーデータを強制的に読み取り専用モードにする

注：管理者オプションについて詳しくは 26 ページ以降にあります。

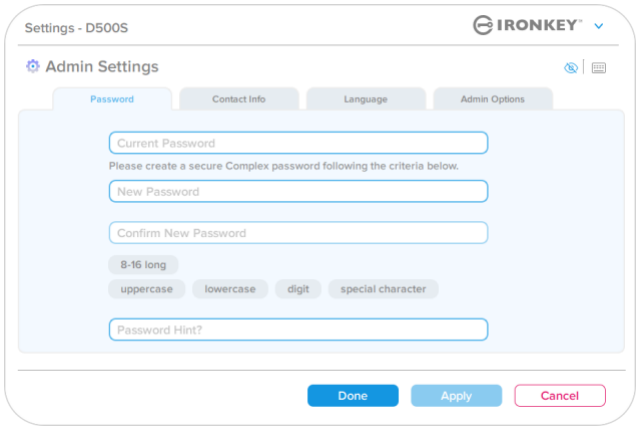


図 7.1 – パスワードオプション

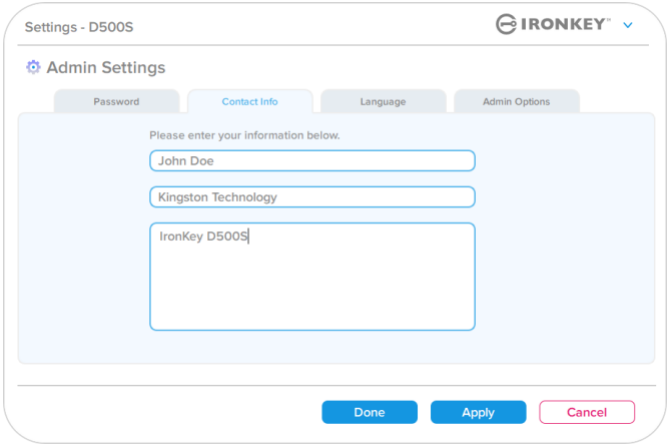


図 7.2 – 連絡先情報

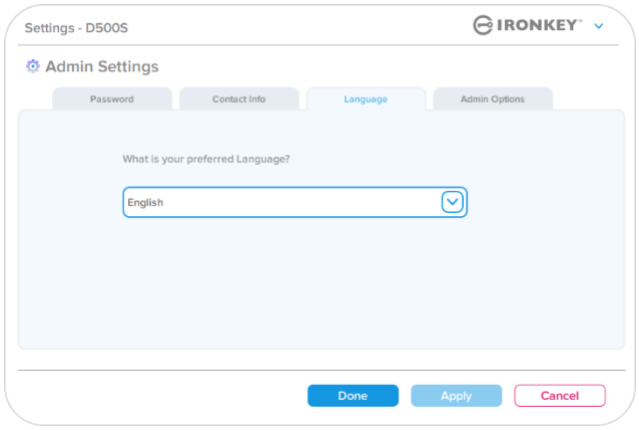


図 7.3 – 言語オプション

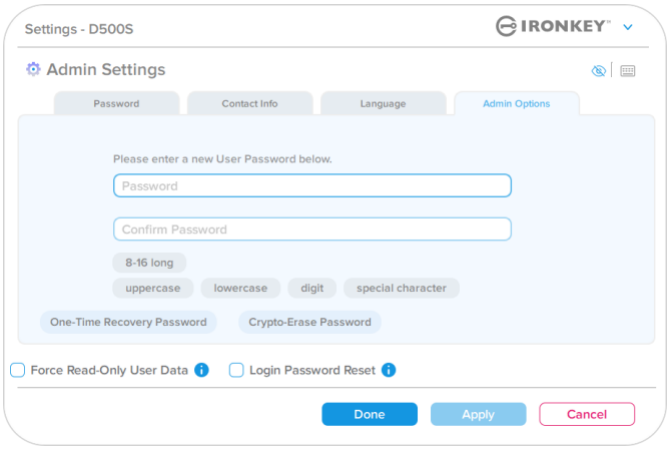
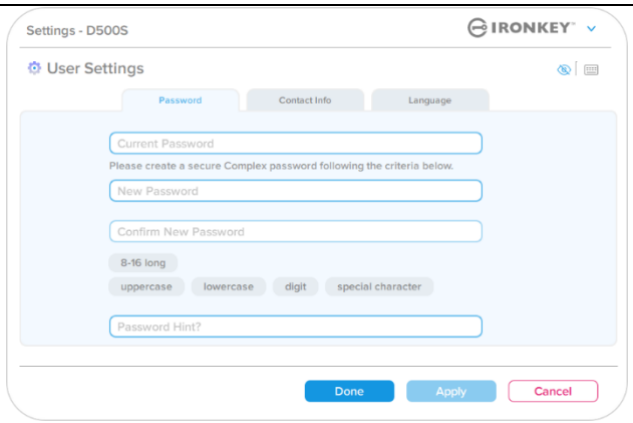
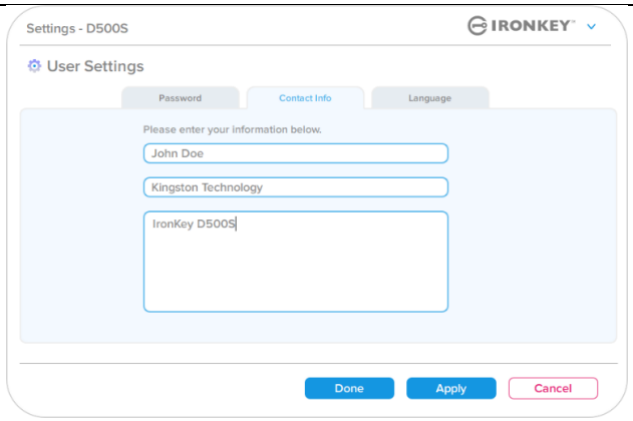
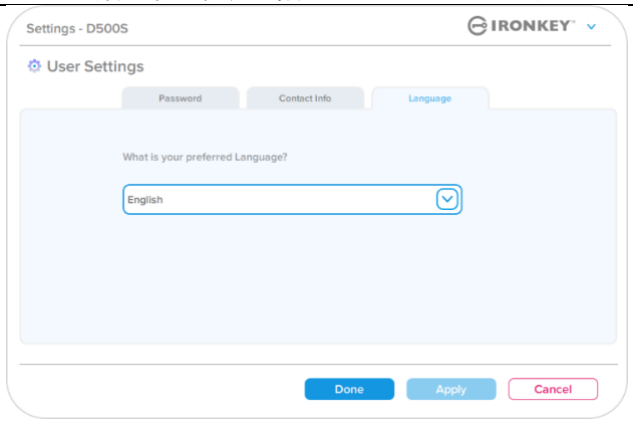


図 7.4 – 管理者オプション

D500S 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。

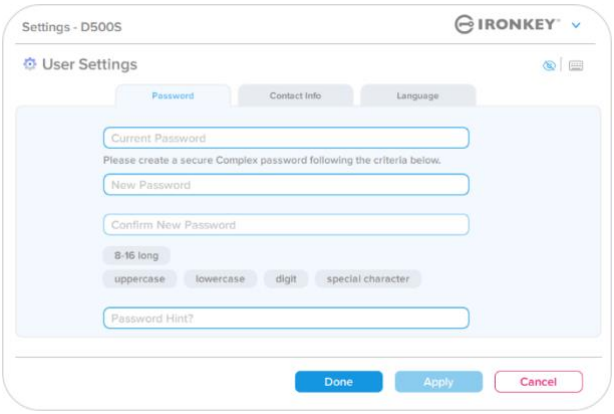
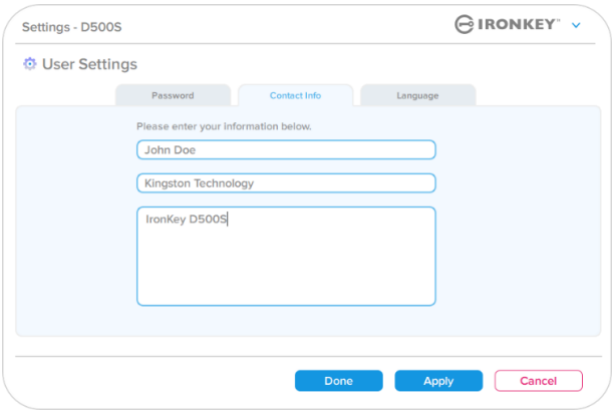
パスワード： ユーザーパスワードやヒントを変更できます（*図 7.5*）	 **図 7.5 – パスワードのオプション（管理者が有効な場合：ユーザーログイン）**
連絡先情報： 連絡先の情報を追加/表示/変更できます（*図 7.6*）。	 **図 7.6 – 連絡先情報（管理者が有効な場合：ユーザーログイン）**
言語： 現在の言語を変更できます（*図 7.7*）。	 **図 7.7 – 言語の設定（管理者が有効な場合：ユーザーログイン）**

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

D500S の設定

ユーザー設定：管理者無効

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 D500S 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（**ユーザー専用モード**）。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 D500S 設定にアクセスできません。

パスワード： ユーザーパスワードやヒントを変更できます（*図 7.8*）	 **図 7.8 – パスワードオプション（ユーザー専用モード）**
連絡先情報： 連絡先の情報を追加/表示/変更できます（*図 7.9*）。	 **図 7.9 – 連絡先情報（ユーザー専用モード）**
言語： 現在の言語を変更できます（*図 7.10*）。	 **図 7.10 – 言語の設定（ユーザー専用モード）**

D500 の設定

設定の変更および保存

- D500S の設定（たとえば連絡先情報、言語、パスワード変更、管理者オプションなど）が変更された場合は常に、承認して適用するために、ドライブにパスワードの入力画面が表示されます（*図 7.11*）

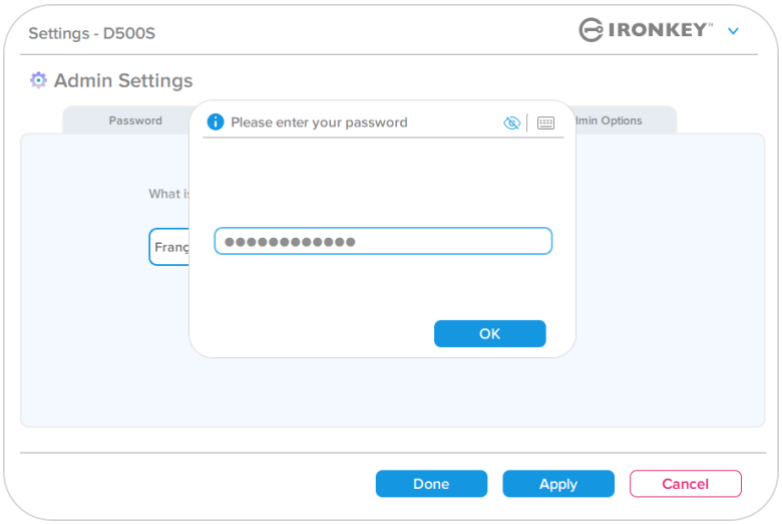


図 7.11 – D500S の設定の変更を保存するためのパスワード入力画面

注：上図のパスワード入力画面が表示され、変更を取り消したいか修正したい場合は、パスワードフィールドをブランクにしたまま、「OK」をクリックします。すると、「パスワードを入力してください」ボックスが閉じ、D500S 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：
「管理者オプション」メニューでユーザーパスワードを手操作で変更します。すぐに変更でき、次のユーザーログインで有効になります（*図8.1*）

注：パスワード要件の基準はデフォルトで、初期化プロセスで設定された元の基準に戻されます（複雑なパスワードまたはパスフレーズパスワード）。

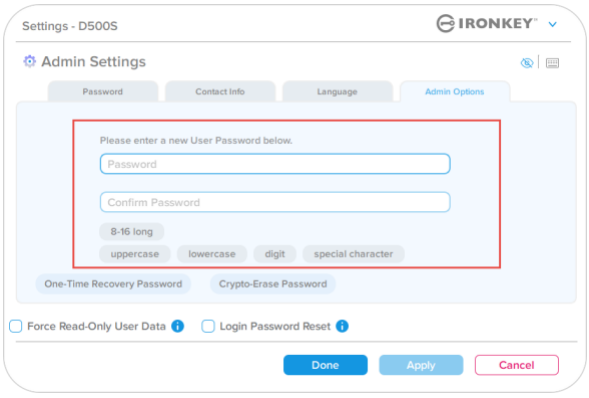


図 8.1 – 管理者オプション/ユーザーパスワードのリセット

ログインパスワードのリセット：
ログインパスワードリセットを有効にすると、**ユーザーは強制的に、管理者の設定した一時パスワードでログインし**、好きなパスワードに変更するように求められます。これは、ドライブを他の使用者に譲る場合に便利です。（*図8.2 および8.3 を参照してください*）

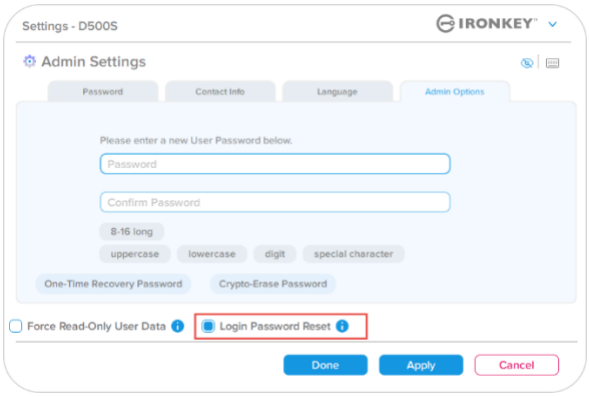


図 8.2 – ログインパスワードのリセットボタン

注：このリセットを適用すると、次にユーザーログインに成功したときに有効になります。パスワード要件基準は、初期化プロセス中に設定された元々のオプションに従って自動的に適用されます（複雑なパスワードまたはパスフレーズパスワード）。

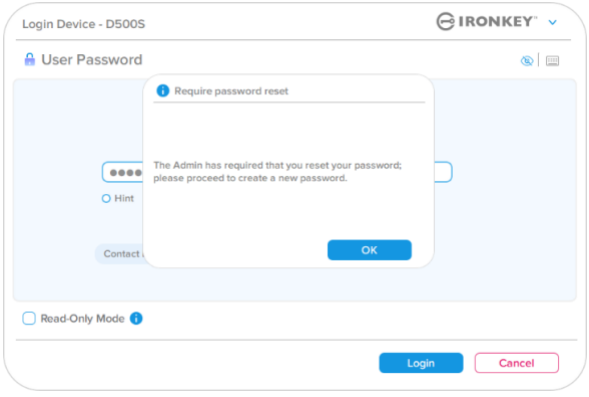


図 8.3 – ユーザーパスワードの入力後の通知のリセット

管理者の機能

一回限りの回復パスワード

このセクションでは、一回限りの回復パスワード機能を有効化して使用するプロセスを説明します。

一回限りの回復パスワード

ステップ 1：一回限りの回復パスワード機能は非常に便利です。これは、ユーザーパスワードを忘れた場合に回復してリセットするために、一回だけ使用可能なパスワードです。まず最初に、管理者オプションメニューで一回限りの回復パスワード ボタンをクリックします。(*図 8.4*)

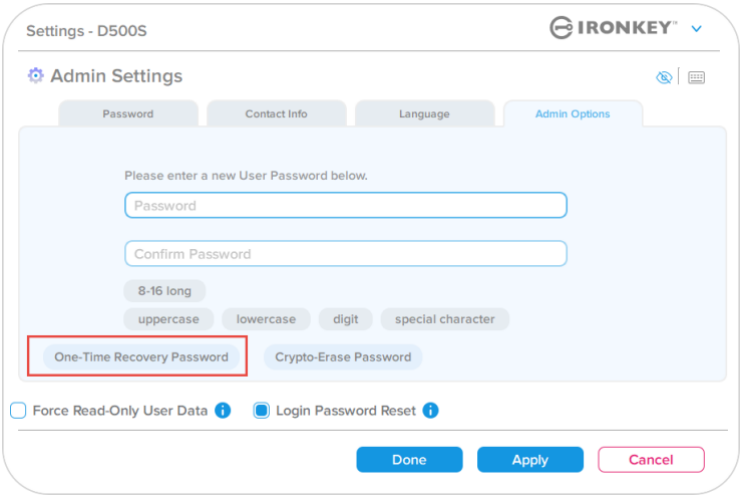


図 8.4 – 一回限りの回復パスワードボタン

ステップ 2：デバイスが初期設定された時と同じパスワード基準を使用して、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。

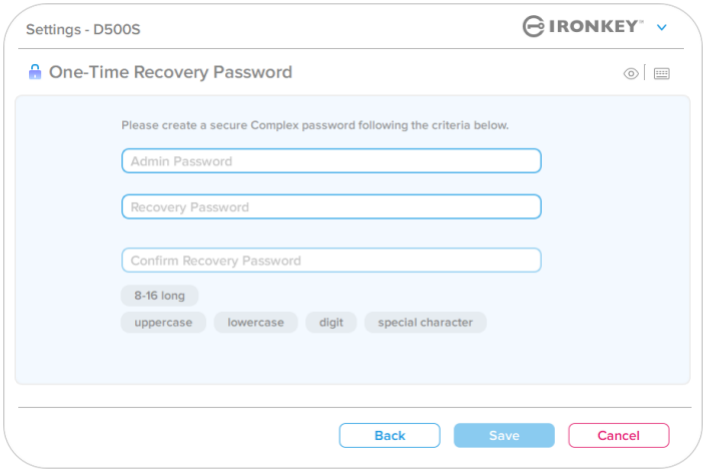


図 8.5 – 一回限りの回復パスワードの設定

管理者の機能

一回限りの回復パスワードの使用

ステップ 1：一回限りの回復パスワードの作成後、次のログイン時に**ユーザーパスワードログイン**画面に新しいボタンが表示されます。**「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。

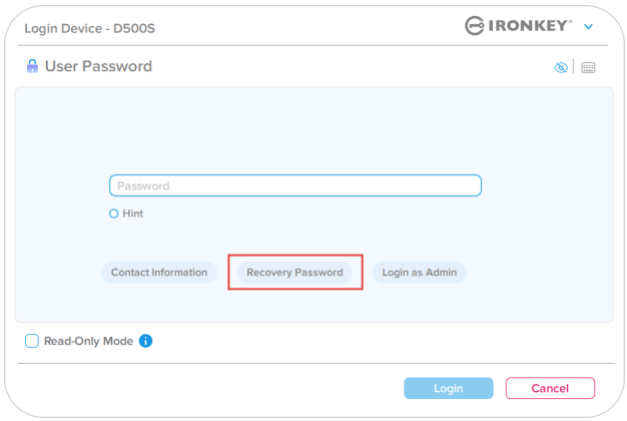


図 8.6 回復パスワードボタン

ステップ 2：回復パスワード 画面が表示され、**回復パスワード**の入力と新規ユーザーパスワードの作成が可能になります。(*図 8.7*)

重要：一回限りの回復パスワードでは、ログインの失敗回数を追跡する組み込みセキュリティ機能を活用できます。**一回限りの回復パスワードを間違えてログインに 10 回失敗すると、パスワードは無効になり**、ドライブに管理者としてログインして再度有効にする必要があります。（詳しくは 19 および 33 ページを参照してください）

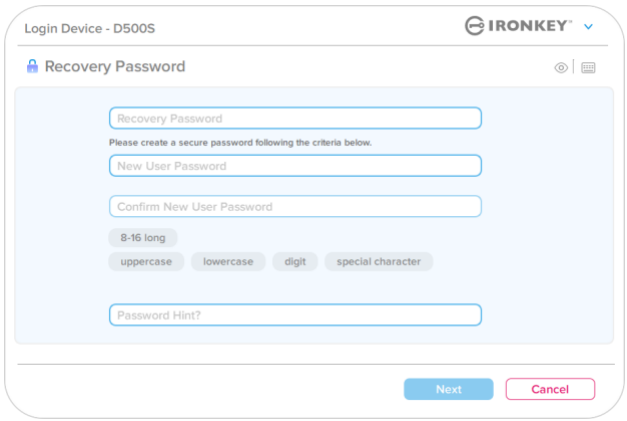


図 8.7 回復パスワードメニュー

ステップ 3：成功すると、**ユーザーパスワード**画面に戻ります。**「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*)

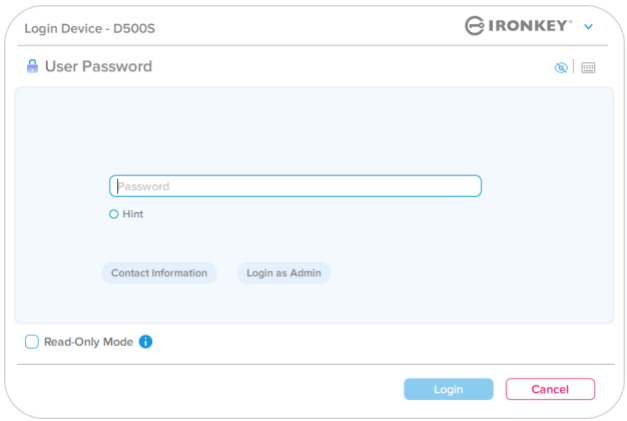


図 8.8 – ユーザーパスワードでのログイン画面。回復パスワードボタンは、ログイン成功後に消えます。

管理者の機能

暗号化消去パスワード

IronKey D500S には、物理的に侵入されるおそれのある場合の対策や保護のために設計された、独自の暗号化消去パスワード機能が搭載されています。パスワードを使用すると、ドライブの内容を安全に消去し、あたかもドライブにデータがまったく書き込まれたことがないような状態にします。この機能が有効で、暗号化消去パスワードを用いてドライブのロックを解除した場合、D500S ドライブ上で暗号化消去が非表示状態で効果的に実行され、ドライブが工場出荷時の状態で開き、空のユーザーパーティションが表示されます。以前の暗号化キーは削除され、代わりに新しいデバイス暗号化キーが作成されます。***ご使用の際はご注意ください***

- この機能を**有効**にするには、「管理者オプション」タブにある「暗号化消去パスワード」ボタンをクリックします。

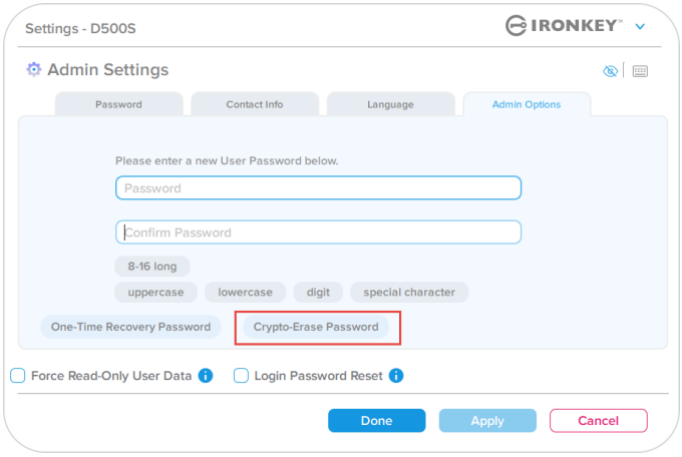


図 8.9 – 暗号化消去パスワードの有効化

暗号化消去パスワードの作成：

- パスワード規則は、ドライブが最初に初期化された際の設定に基づきます（複雑なパスワードまたはパスフレーズパスワード）
- 検証には、管理者パスワードが必要になります。

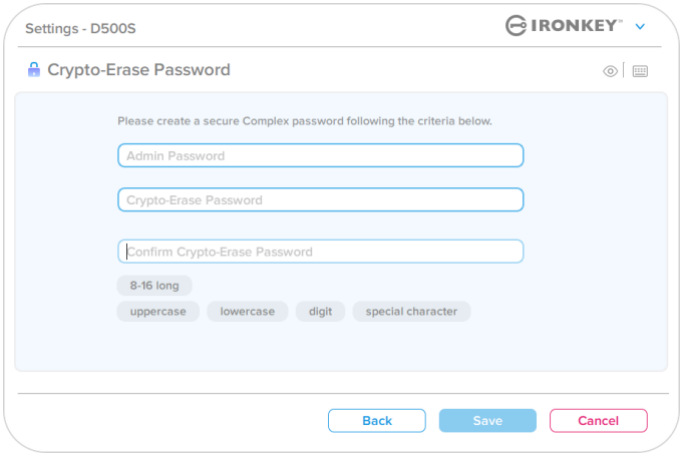


図 8.10 – 暗号化消去パスワードの作成

管理者の機能

暗号化消去パスワードの使用

暗号化消去パスワードを使用すると、以前の管理者およびユーザーのパスワードが削除され、暗号化消去パスワードに置き換わります。さらに、以前の構成設定が削除されるとともに、ドライブ上のすべてのデータが永久に削除され、ドライブがユーザー専用モード構成に変換されます。

暗号化消去パスワードの使用方法：

1. IronKey.exe を起動して、IronKey アプリケーションを実行します

2. ユーザーパスワードログイン画面で、「**Ctrl + Alt + C**」を押して、暗号化消去パスワード入力に切り替えます。正常に実行された場合、パスワード入力画面の下に太いブルーのバーが表示され、暗号化消去パスワードの入力準備ができたことを示します。(*図 8.11*)

注：暗号化消去パスワードへの切り替えは、ユーザーパスワードログイン画面のみで行えます。

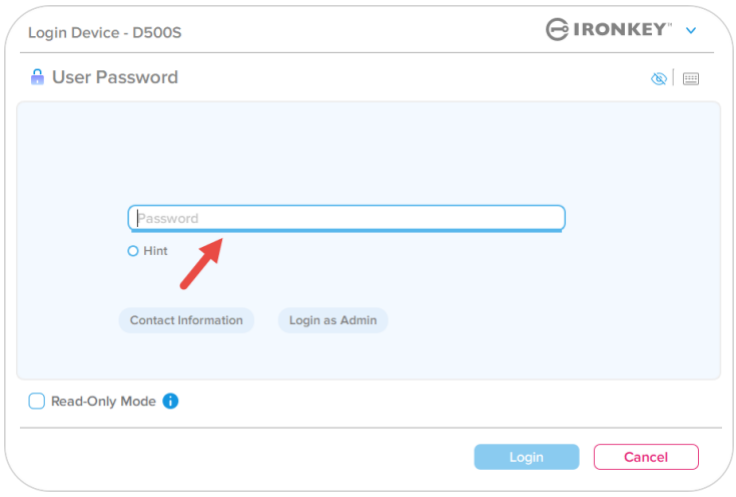


図 8.11 – 暗号化消去が有効、太いブルーのバーが表示

暗号化消去パスワードを使用すると、ドライブのすべての内容の消去に進み、次に一つの空のパーティションが表示されます。ドライブはユーザー専用モードになり、暗号化消去パスワードはリセットされるまで、ドライブのログイン用のパスワードになります。

重要：この機能はドライブのすべてのデータを消去し、以前保管した内容はすべて恒久的に失われますので、慎重に進めてください。

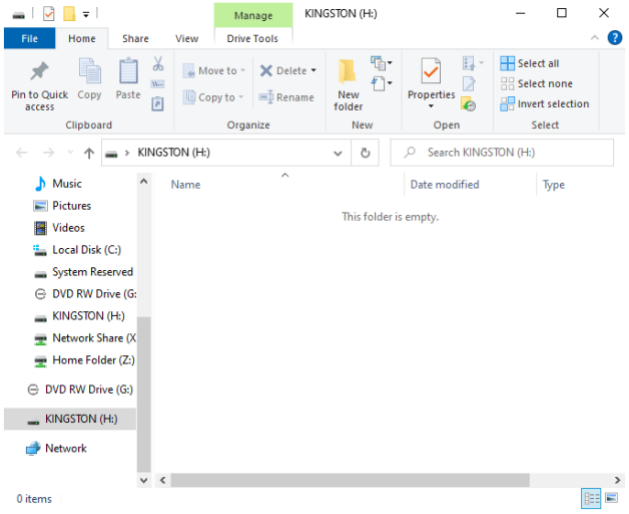


図 8.12 – 暗号化消去パスワード使用後の、消去されたドライブ

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のみの場合に有用です。

- ユーザーデータに対して、強制的な読み取り専用を有効にする場合は、そのボックスをクリックして、「適用」をクリックします。(*図8.13*)

  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、管理員ログイン時は無効です。管理者ログインでは読み書きのアクセス権があるまま、必要であれば追加で読み取り専用モードを有効にできます。

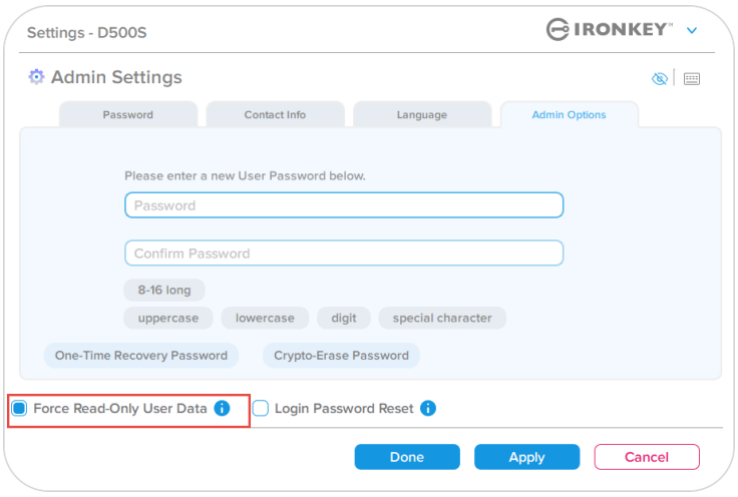


図 8.13 – 「ユーザーデータを強制的に読み取り専用にする」を有効にする (変更の適用には、管理者パスワードが必要になります)

- 一旦有効にすると、「**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8.14*)

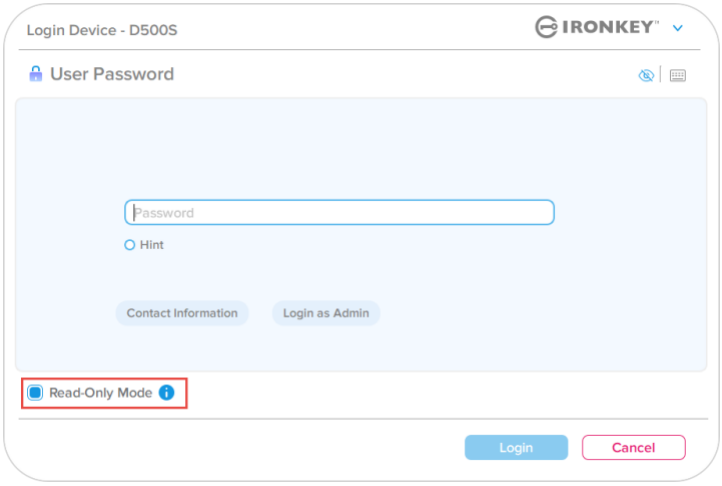


図 8.14 – 読み取り専用モードがユーザーに対して強制的に有効になり管理者のみが無効化可能

ヘルプとトラブルシューティング

デバイスのロックアウト

D500S には、ログインの失敗回数が**連続**で最大回数に達すると（略語は *MaxNoA*）、データパーティションへの不正なアクセスを防ぐセキュリティ機能があります。「購入時」のデフォルト構成の事前設定値は、各ログイン方式（管理者/ユーザー/一回限りの回復パスワード）それぞれに対して 10 回（試行回数）です。

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

1. MaxNoA の回数に達する前に、正常にログインした場合

2. MaxNoA に達し、ドライブの構成に応じてデバイスのロックアウトまたはデバイスのフォーマットのいずれかを実行した場合。

- 間違ったパスワードが入力された場合は、エラーメッセージがパスワード入力フィールドの上に赤で表示され、ログインが失敗したことを示します。（*図 9.1*）

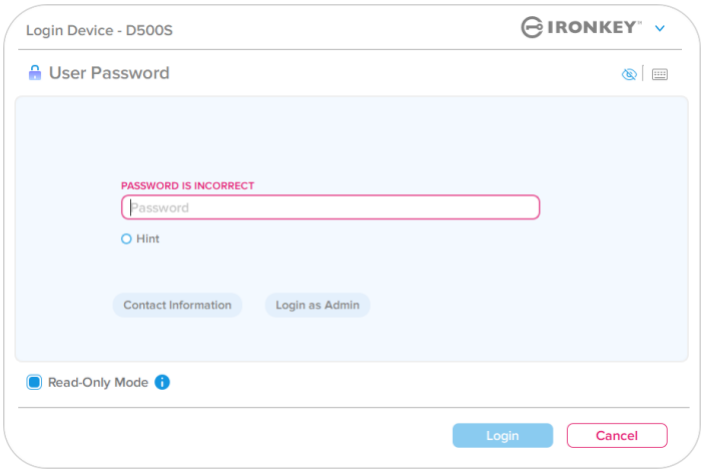


図 9.1 – パスワードが間違っている場合のメッセージ

- ログインが続けて **7 回**失敗した場合、あと 3 回で MaxNoA の回数（デフォルトの設定は 10 回）に達することを示す追加のエラーメッセージが表示されます（*図 9.2*）

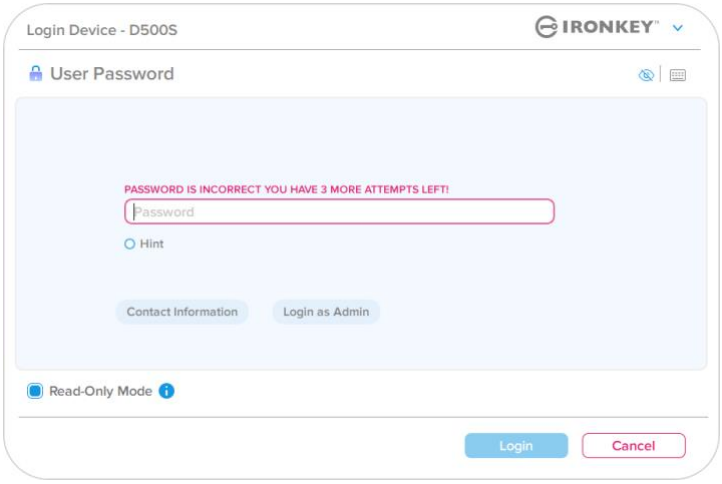


図 9.2 – 7 回パスワードを間違えた場合のメッセージ

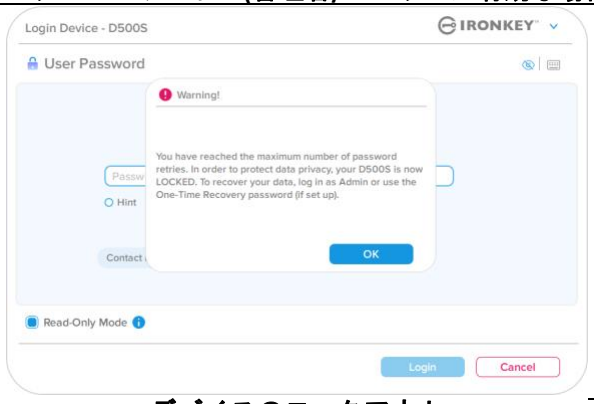
ヘルプとトラブルシューティング

デバイスのロックアウト

重要：最後の **10 回目**のログインに失敗した後、デバイスの設定と使用されているログイン方法（管理者、ユーザー、一回限りの回復パスワード）に応じて、デバイスはロックされるか、代替方法（利用できる場合）でのログインが必要になるか、デバイスリセット（データがフォーマットされ、**ドライブ上のすべてのデータが永久に失われます）されます**。これらの動きは、本書の 19 ページでも説明されています。

下の図 9.3～9.6 では、各パスワード方式で 10 回失敗し、試行できる最後のログイン回数に達した時に、どのような表示になるかを示しています。

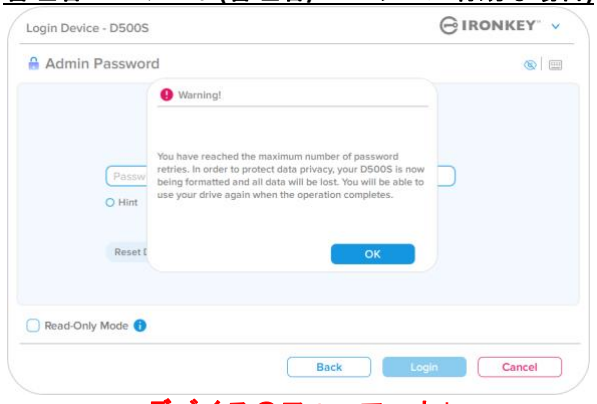
ユーザーパスワード：(管理者/ユーザーが有効な場合)



デバイスのロックアウト

図 9.3

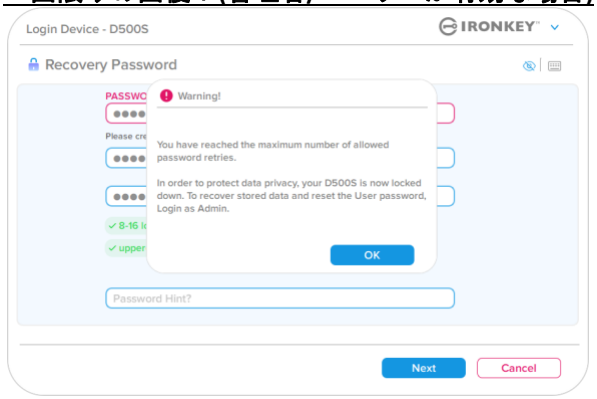
管理者パスワード(管理者/ユーザーが有効な場合)



デバイスのフォーマット*

図 9.4

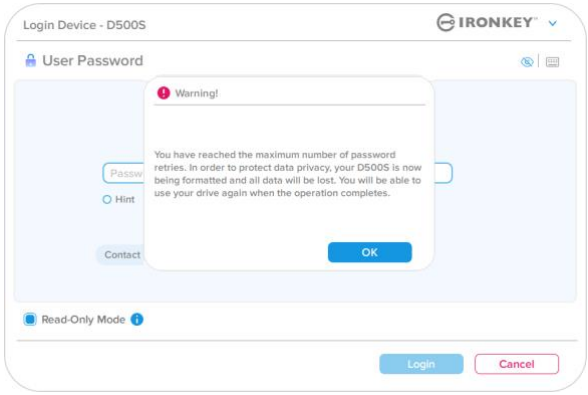
一回限りの回復：(管理者/ユーザーが有効な場合)



デバイスのロックアウト

図 9.5

ユーザーパスワード（管理者が無効な場合）



デバイスのフォーマット*

図 9.6

これらのセキュリティ対策は、（パスワードを知らない）誰かが何度もログインを試して、機密データへアクセスする（総当たり攻撃やブルートフォース攻撃と呼ばれます）ことのないよう、制限をかけます。D500S 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、D500S の保護下のデータパーティションに保存されたすべての情報が消去されます。*

ヘルプとトラブルシューティング

デバイスのリセット

パスワードを忘れた場合、またはデバイスのリセットが必要な場合、D500S の起動時に、ドライブの設定に応じて、2 か所のどちらかに表示（管理者/ユーザーが有効な場合は、管理者ログインパスワードメニュー。管理者/ユーザーが無効な場合は、ユーザーパスワードのログインメニュー）される「デバイスのリセット」ボタンをクリックできます（*図 9.7 および 9.8 を参照*）

- このオプションを選択して新しいパスワードを作成できますが、ユーザーデータのプライバシーを保護するために、D500S は初期化されます。これは、上記のプロセス時にユーザーデータがすべて消去されることを意味します。*

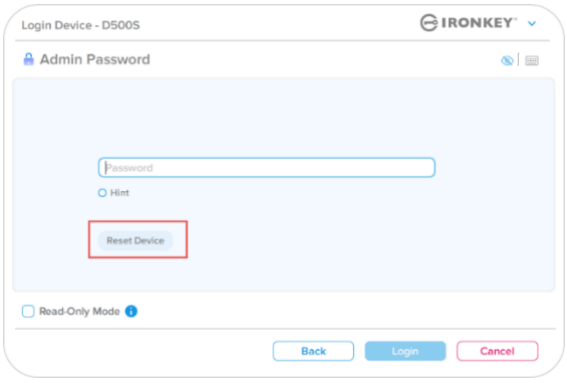


図 9.7 – 管理者パスワード：デバイスのリセットボタン

- **注：** *「デバイスのリセット」*をクリックすると、メッセージボックスが表示され、初期化を行う前に新しいパスワードの入力を求めるかどうか質問してきます。この時点で、1)「OK」をクリックして確認するか、2)「キャンセル」をクリックしてログインウィンドウに戻ることができます。（*図 9.8 参照*）

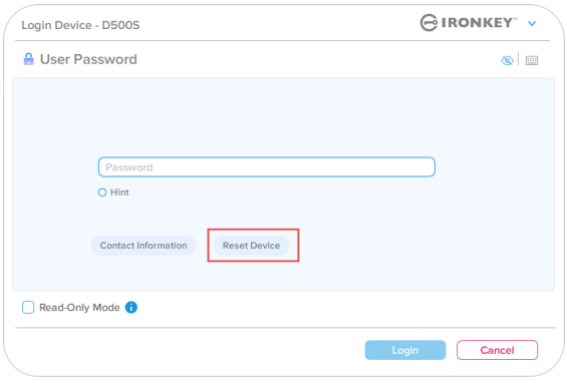


図 9.8 – ユーザーパスワード(管理者/ユーザーが無効な場合)デバイスのリセット

- 続行を選択した場合は、初期化画面が表示され、「管理者およびユーザーモード」を有効にして、選択したパスワードオプション（複雑なパスワードまたはパスフレーズパスワード）に応じて新しいパスワードを入力できます。ヒントは必須フィールドではありませんが、パスワードを忘れた場合、パスワードの手がかりを教えてくれるため、便利です。

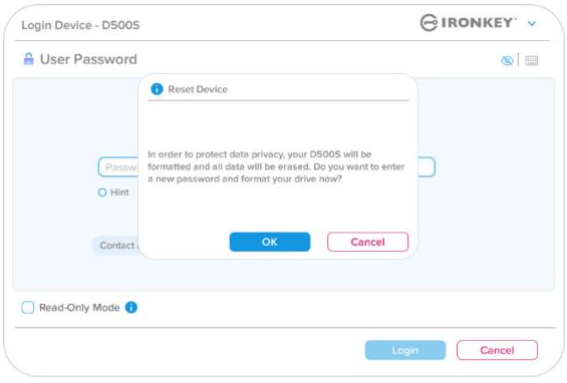


図 9.9 – デバイスのリセットの確認

ヘルプとトラブルシューティング

ドライブ文字の競合：Windows オペレーティングシステム

- 本書の「システム要件」セクション（ページ 3）で前述したとおり、D500S には、連続した２つのドライブ文字が必要。)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 Universal Naming Convention (UNC) パスですでに使用されているドライブ文字を D500S に割り当てることがあり、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、D500S には、連続した２つのドライブ文字が必要。)この文字は、ドライブ文字の割当てが途切れる前の、最後の物理ディスクの直後になります（*図 9.10* 参照）これは、ネットワーク共有と連動しません。ネットワーク共有はユーザープロファイルに指定されており、ハードウェアプロファイル自体には指定がないので、OS からは利用可能に見えるためです。

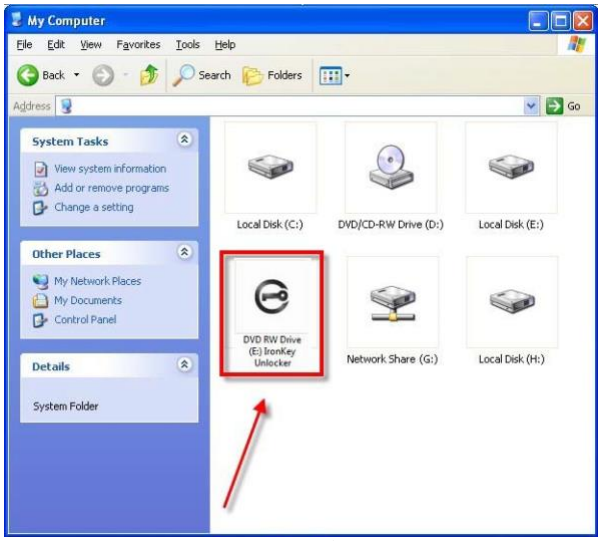


図 9.10 – ドライブレターの例

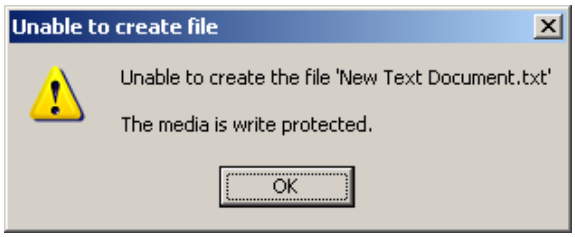
この例で言えば(*図 9.10*)、D500S はドライブ E: の後の最初の利用可能なドライブ文字である F: を使用しています (E: がドライブ文字のギャップ前の最後の物理ディスクです)。ドライブ文字 G: はネットワーク共有であり、ハードウェアプロファイルの一部ではないため、D500S は 2 番目のドライブ文字として G: を使用する可能性があり、競合が発生します。

システムにネットワーク共有がないのに D500S が読み込まれない場合は、カードリーダーやリムーバブルディスク、その他以前にインストールされているデバイスがドライブ文字の割り当てを持ち続けており、結果競合が発生しています。

ドライブ文字管理（DLM）は、Windows 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。

ヘルプとトラブルシューティング

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。	 **図 9.11 – ファイル作成不可のエラー**
ファイルまたはフォルダをコピーできません： 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。	 **図 9.12 – ファイル/フォルダのコピーの失敗のエラーメッセージ**
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。	 **図 9.13 – ファイル/フォルダ削除の失敗のエラーメッセージ**

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 D500S を一度シャットダウンして、再度ログインする前に、「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。

デバイスの使用（Linux 環境の場合）

現在利用可能な各種の Linux ディストリビューションでは、インターフェイスの外観と雰囲気がバージョンによって異なる場合があります。しかしターミナルアプリケーションで使用する一般的なコマンドセットはとても良く似ており、以下のような Linux の命令で参照することができます。このセクションのスクリーンショットの例は、64 ビット環境で作成されたものです。

Linux のディストリビューションによっては、ターミナルアプリケーション画面で D500Sを正しく実行するために、スーパーユーザー（ルート）の権限が必要な場合があります。

先に進む前に重要な注意：

1.) **D500S は Linux 上でデバイスを初期化できず、Windows または MacOS システム上で設定し、構成する必要があります。その後 Linux マシンで使用することができます。**

2.) **Linux ログインでは、複雑なパスワードのみ使用できます。パスフレーズパスワードでは Linux にログインできません。**

3.) **Linux で使用できる D500S 機能は限られています。一回限りの回復パスワード、暗号化消去パスワード、管理者 / ユーザーのパスワード、読み取り専用モードのリセットと切り替えなどの機能は、Linux では使用できません。**

D500S には、Linux で使用できる以下の 4 つのコマンドがあります。

lkd500s_about	「D500S について」の情報を表示します。
lkd500s_login	ドライブにログインできます。
lkd500S_logout	安全に高いセキュリティで D500S ドライブからログアウトできます。
lkd500S_resetdevice	デバイスの暗号化消去を実行し、ドライブを購入時の状態に戻し、ドライブに保管されたすべてのデータとファイルを恒久的に削除します。

注：これらのコマンドを実行するには、「ターミナル」アプリケーションウィンドウを開き、各ファイルが存在するフォルダを開く必要があります。各コマンドの前に、以下の 2 文字を付ける必要があります：./'（ピリオドとスラッシュの 2 文字です）

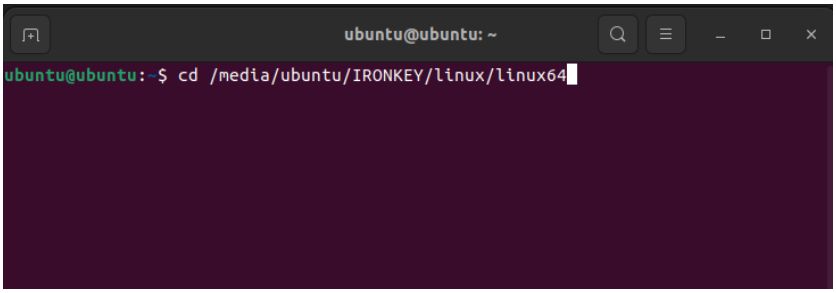
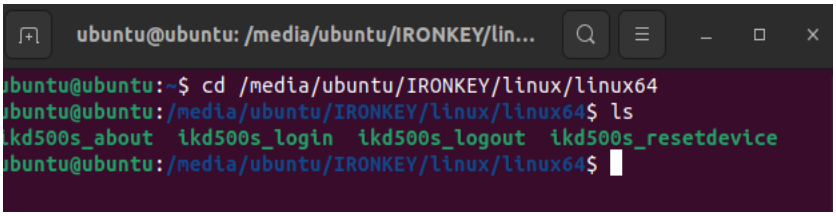
IronKey Linux コマンドパスへの移動方法の例：

32 ビット Linux ユーザーの場合：	「ターミナル」のアプリケーション画面を開き、プロンプト画面で次のコマンドを入力して、現在の ディレクトリを **/media/ubuntu/IRONKEY/linux/linux32$** に変更します。 **cd /media/ubuntu/IRONKEY/linux/linux32**（入力の後、ENTER を押してください。）
64 ビット Linux ユーザーの場合：	「ターミナル」のアプリケーション画面を開き、プロンプト画面で次のコマンドを入力して、現在の ディレクトリを **/media/ubuntu/IRONKEY/linux/linux64$** に変更します。 **cd /media/ubuntu/IRONKEY/linux/linux64** （入力の後、ENTER を押してください。）

デバイスの使用（Linux 環境の場合）

注：IRONKEY ボリュームが OS で自動的にロードされない場合は、Linux の「mount」コマンドを使って、ターミナルウィンドウにそのボリュームをマニュアルでロードする必要があります。お使いの OS ディストリビューションの Linux ドキュメントを参照するか、お気に入りのオンラインサポートのサイトにアクセスして、正しいコマンド構文とコマンドオプションを調べてください。Linux ディストリビューションによっては、コマンド（上の事例では「ubuntu」）を実行するために、ユーザー名の入力が必要になる場合があります。

IronKey D500S Linux コマンドファイルの場所と表示：

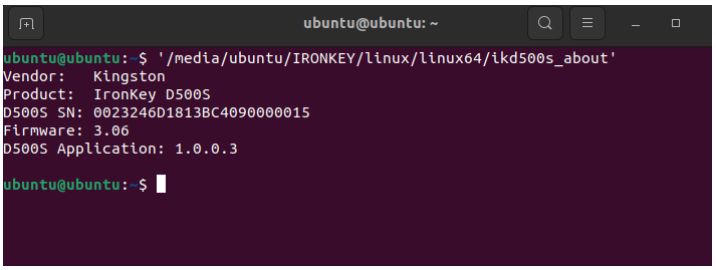
D500S をコンピュータに接続し、オペレーティングシステムに認識されたら、ターミナルプロンプトにコマンドを入力して、ディレクトリを D500S ボリュームに変更します。(*図 10.1*) **注**：このセクションで示すスクリーンショットや命令は、Linux OS での D500S デバイスのデモ使用を目的とした linux64 フォルダ（64 ビット版）を使用しています。32 ビット版の Linux をお使いの場合は、64 ビットフォルダではなく、該当する 32 ビットフォルダ（例えば linux64 ではなく、linux32）に進み、使用してください。)	 **図 10.1 – コマンド行のナビゲーション**
現在のプロンプト画面で **ls**（リスト）コマンドを使用し、ENTER を押します。linux64 内のファイルやフォルダのリストが表示されます。 リストには、次の 4 つの IronKey Linux コマンドがあります（*図 10.2*） • ikD500S_about • ikD500S_login • ikD500S_logout • ikD500S_resetdevice	 **図 10.2 – IronKey Linux コマンドファイルの表示**

注：コマンドとフォルダ (ディレクトリ) 名は、大文字と小文字が区別されます。例えば、「linux64」と「Linux64」は異なるものとして認識されます。コマンド構文も、ここに示す通りに、正確に入力しなければなりません。Linux ディストリビューションによっては、コマンド（この例では「ubuntu」コマンド）を実行するために、ユーザー名の入力が必要になる場合があります。)

デバイスの使用（Linux 環境の場合）

D500S コマンドの使用

D500S について

IkD500S_about（D500S について、*図 10.3*） このコマンドは、D500S に関する次のような情報を入力します。 • ベンダー • 製品 • D500S シリアル番号 • ファームウェアのバージョン • ソフトウェアのバージョン	 **図 10.3 – ikD500S_about（IronKey D500S について）**

D500S ログイン

ikD500S_login

対応の Windows または MacOS システムで D500S を初期化した後、作成した D500S パスワードを使用してデバイスにログインすると、保護下のデータパーティションにアクセスできます。

これを行うには、以下の手順に従ってください。

1. 「ターミナル」のアプリケーション画面を開きます。

2. ターミナルプロンプトに次のコマンドを入力します：**cd /media/ubuntu/IRONKEY/linux/linux64**

3. コマンドプロンプトの場所は **/media/ubuntu/IRONKEY/linux/linux64$** になるので、次のコマンドでデバイスにログインします。**./ikD500S_login*** を入力し、ENTER を押します。(注意：コマンドおよびフォルダ名は、大文字と小文字が区別されますので、構文は正確に入力する必要があります。また、ディストリビューションによっては、ユーザー名（この例では「ubuntu」）を入力する必要があります。)

4. ログイン成功後、デスクトップに保護下のデータボリュームが開き、D500S を使用できます（ログインの動きについて詳しくは、次のページに続きます）

*注：Linux のディストリビューションによっては、ターミナルアプリケーション画面で D500Sを正しく実行するために、スーパーユーザー（ルート）の権限が必要な場合があります。

デバイスの使用（Linux 環境の場合）

D500S へのログイン(続き)

IkD500S_login（D500S のロック解除、*図 10.4*）

ドライブの設定によっては、希望するドライブのロック解除方法について、多くのオプションがログイン手順中に表示されます。

初期化中に**管理者 / ユーザー**パスワードのプロファイルを有効にした場合、次のログインオプションが表示されます。

1.) 管理者またはユーザーでのログインを選択
2.) 管理者またはユーザーパーティションのロック解除を選択（有効な場合）
3.) デバイス認証とロック解除のために、管理者またはユーザーのログインパスワードを入力

注：初期化中に管理者 / ユーザーパスワードのプロファイルを無効にした場合（ユーザー専用モード）、デバイス認証のためのデバイスパスワードのみを入力できるプロンプト画面が表示されます。

重要：前述したとおり、Linux ではパスフレーズパスワードを使用できず、Linux でのログイン用に D500S を複雑なパスワードで構成する必要があります（*図 10.5*）

図 10.4 – ikD500S_login（D500S のロック解除）

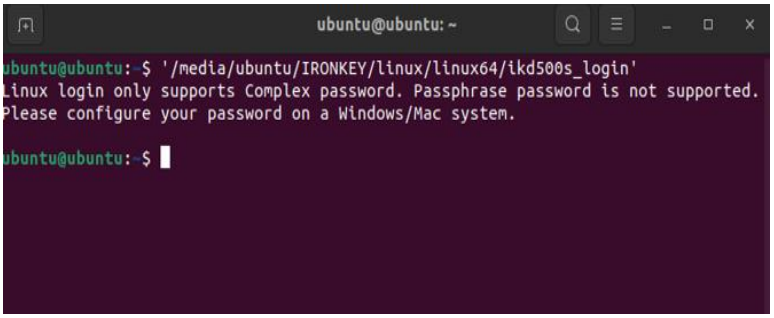


図 10.5 – 未対応のパスフレーズパスワードでログインした場合

デバイスの使用（Linux 環境の場合）

D500S へのログイン(続き)

ログインパスワードが正しくない場合
ログイン手順中に、間違ったパスワードを入力した場合、もう一度パスワードを入力することができます。しかし、ログインの失敗回数を追跡する組み込みセキュリティ機能があります。管理者またはユーザーのログイン失敗回数が、事前設定された 10 回に達すると、次のような処理が行われます。

管理者 / ユーザーパスワードが有効な場合

- **ユーザーでのログイン**：ユーザーがロックアウトされ、管理者でログインする必要があります。（*図 10.6*）
  注：対応する Windows または MacOS システムで管理者でログインし、ユーザーパスワードをリセットできます。
- **管理者でのログイン**：ドライブが暗号化消去され、すべてのデータが恒久的に失われます。デバイスのリセットが必要です。（*図 10.7*）

ユーザー専用モード（管理者 / ユーザーが無効な場合）

- **ユーザーでのログイン**：ドライブが暗号化消去され、すべてのデータが恒久的に失われます。デバイスのリセットが必要です。（*図 10.7*）

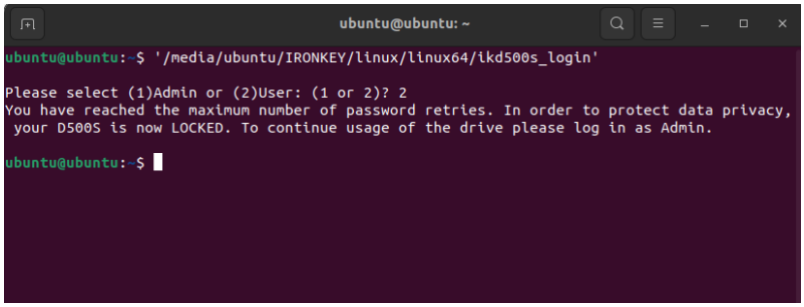


図 10.6 – ユーザーがロックアウトされ、管理者/ユーザーパスワードが有効

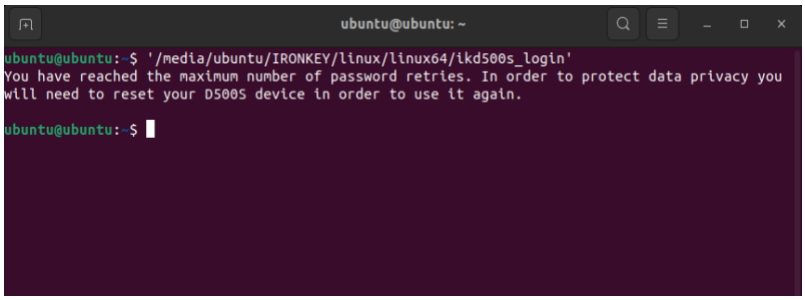


図 10.7 – 失敗回数の上限に到達（ドライブのリセット）

D500S からログアウト

IkD500S_logout（デバイスのロック）

D500S を使い終わったら、デバイスからログアウトして、データを保護してください。これを行うには、39 ページの説明と同じ手順に従い、次のコマンドを使用してデバイスから適切にログアウトします。**./ikD500S_logout** と入力し、ENTER を押します（注：コマンドとフォルダ名は、大文字と小文字が区別されますので、構文は正確にキー入力する必要があります。（*図 10.8*）

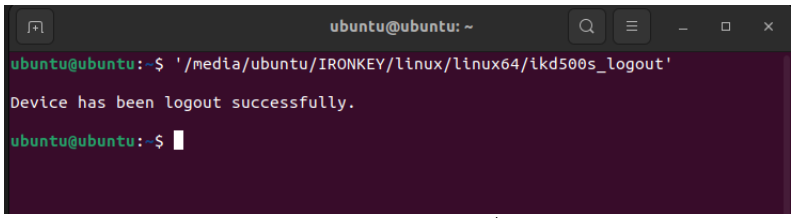


図 10.8 – D500S からのログアウト

デバイスの使用（Linux 環境の場合）

D500S デバイスのリセット

ikD500S_resetdevice
この前の41 ページで記述したとおり、ユーザー / 管理者パスワードを忘れた場合、「デバイスのリセット」コマンドを使用し、ドライブをリセットして再び使用できます。この手順で新しいパスワードを作成できますが、データのプライバシーを保護するために、D500S はドライブを暗号化消去し、保護下のデータパーティションをフォーマットします。これは、ユーザーデータがすべて**消去されることを意味します。**

リセットコマンドを使用するには、39 ページの説明と同じ手順に従い、次のコマンドを使用してデバイスから適切にログアウトします。**./ikD500S_resetdevice** と入力し、ENTER を押します（注：コマンドとフォルダ名は、大文字と小文字が区別されますので、構文は正確にキー入力する必要があります。（*図 10.9*）

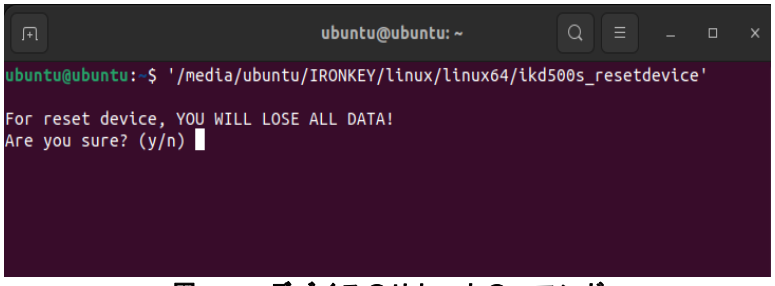


図 10.9 – デバイスのリセットのコマンド

「デバイスのリセット」コマンドを使用すると、以下を含む新しい複雑なパスワードの作成を求めるプロンプト画面が表示されます。

- 8～16 文字の長さで、次の文字種のうち最低3種類を含んでいる必要があります。

  -英大文字
  -英小文字
  -数字
  -特殊文字（! や $ など）

(*図 10.10*)

注：「デバイスのリセット」コマンドは、ドライブをユーザー専用モードで初期化します（単一のパスワード、単一のユーザー）。管理者 / ユーザーログインパスワードプロファイルを有効にするには、対応する Windows または MacOS システム上で D500S を設定して、そのオプションにアクセスする必要があります。

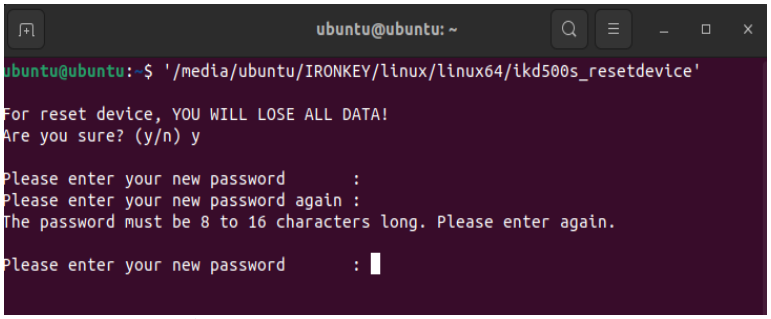


図 10.10 – デバイスのリセットのコマンド、パスワード作成

IRONKEY™ D500S
USB 3.2 Gen 1 加密闪存盘

用户指南

目录

图 1：IronKey D500S

简介

Kingston IronKey D500S 是一款军用级安全 USB 闪存盘，基于 IronKey 在保护敏感信息方面备受推崇的功能而构建。它通过了 FIPS 140-3 3 级（待定）认证，其中包括 NIST 新的安全增强功能，需要安全的处理器升级以增加安全性。加密和解密是在 D500S 上完成的，主机系统上不会留下任何痕迹，因此不受内存中密码嗅探器的影响。除了基于硬件的 XTS-AES 256 位加密外，它还采用了坚固的锌外壳，防水*、防尘*、抗压，并填充了环氧树脂，以保护内部组件免受渗透攻击。

D500S 支持多密码（管理员、用户、一次性恢复和加密擦除）选项以及传统的复杂或密码短语模式**。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，密码短语模式允许输入数字 PIN、句子、单词表，甚至可以输入包含 10 到 128 个字符的歌词。管理员可以启用用户，创建自定义大小的双数据分区，将管理员/用户登录文件分隔开，启用一次性恢复密码、加密擦除密码，并重置用户密码以恢复数据访问。

为了便于输入密码，可以启用”眼睛”   符号来显示输入的密码字符，从而减少导致登录尝试失败的拼写错误。为了让用户更安心，D500S 使用数字签名固件，使其免受 BadUSB 恶意软件和暴力破解攻击，以防止猜测密码。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***。

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***。

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。

D500S 提供许多定制选项，符合 TAA/CMMC 标准，并在美国组装。

D500S 享有 5 年有限保固和免费 Kingston 技术支持服务。

* 请参阅数据表的规格。产品使用前必须保持清洁干燥。
** Linux 系统不支持密码短语模式。
*** 虚拟键盘：仅在 Microsoft Windows 和 macOS 系统中支持英语。

IronKey D500S 的功能

- FIPS 140-3 3 级（待定）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
- 复杂密码或密码短语模式
- 独特的双分区选项和加密擦除密码
- “眼睛”按钮可显示输入的密码，减少失败的登录尝试
- 虚拟键盘有助于防范按键记录程序和屏幕记录器
- 强制/基于会话的只读（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、macOS 和 Linux 兼容（参见数据表了解详情）

关于本手册

本用户手册介绍 IronKey D500S，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* ***注意：**参见第 35 页的“驱动器号冲突”	**PC 操作系统支持** • Windows 11 • Windows 10
Mac 平台 • 15MB 可用磁盘空间 • USB 2.0 - 3.2 端口	**Mac 操作系统支持** • macOS macOS 11.x - 14.x
Linux 平台 • 5MB 可用磁盘空间 • USB 2.0 - 3.2 端口	**Linux 操作系统支持** • Linux Kernel v4.4+

建议

为了确保 D500S 设备供电充足，请将其直接插在笔记本电脑或台式机所带的 USB 接口中，如***图 1.1*** 所示。避免将 D500S 连接到任何带 USB 接口的外围设备中，如键盘或 USB 供电集线器，如***图 1.2*** 所示。

图 1.1：建议使用

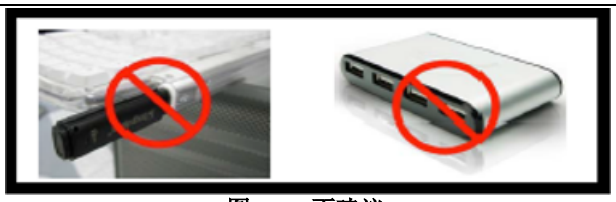


图 1.2：不建议

使用正确的文件系统

IronKey D500S 使用 FAT32 文件系统进行了预格式化。这种格式支持 Windows、macOS 和 Linux* 系统。不过，可以使用其他选项手动格式化闪存盘，例如适合 Windows 的 NTFS 和 exFAT。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 D500S 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 发光时拔出设备。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 Kingston 技术支持部门。

*** D500S 不支持 Linux 上的开箱即用初始化，需要在支持的 Windows 或 macOS 系统上完全初始化和配置，然后才能在 Linux 上使用闪存盘。其他信息可在本用户指南第 37 页的 Linux 部分找到**

密码设置最佳实践

D500S 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，D500S 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 D500S 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，D500S 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。

D500S 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。务必设置两个密码，并在使用用户密码的同时将管理员密码保存到安全的地方。如有需要，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。D500S 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

D500S 还支持两个不同的密码模式：

复杂

复杂密码需要至少包含 8-16 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

密码短语

D500S 支持 10 至 128 个字符的密码短语。密码短语没有规则，但若使用得当，可以提供极高水平的密码保护。

密码短语基本上是任何组合的字符，包括来自其他语言的字符。就像 D500S 闪存盘，密码语言可以匹配为此闪存盘选择的语言。这让您可以选择多个单词、一个短语、歌词、一行诗等。优秀的密码短语是攻击者最难猜到的密码类型之一，且可能更易于用户记住。

设置我的设备

为确保 IronKey 加密 USB 闪存盘获得充足供电，应将其直接插入笔记本电脑或台式机的 USB 2.0/3.0 接口。避免将其连接到包含 USB 接口的任何外围设备，例如键盘或 USB 供电的集线器。该设备的初始设置必须在受支持的 Windows 或 macOS 操作系统中完成。

设备访问（Windows 环境）

将 IronKey 加密 USB 闪存盘插入笔记本电脑或台式机的可用 USB 接口，等待 Windows 检测到该闪存盘。

- Windows 10/11 用户会收到设备驱动程序通知。（*图 3.1*）

图 3.1：设备驱动程序通知

- 一旦新硬件检测完成，可利用文件资源管理器在 Unlocker 分区中找到 **IronKey.exe**。（*图 3.2*）
- 请注意，分区号可能有所不同，具体取决于下一个空闲驱动器号。驱动器号可能因连接的设备不同而异。在下图中，驱动器号是 (E:)

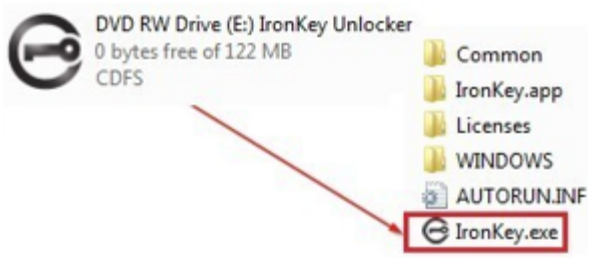


图 3.2：文件资源管理器窗口/IronKey.exe

设备访问（macOS 环境）

将 D500S 插入笔记本电脑或台式机的可用 USB 接口，等待 Mac 操作系统检测到该闪存盘。检测到后，您会在桌面上看到“IRONKEY”卷标。（*图 3.3*）

- 双击 IronKey CD-ROM 图标。
- 然后，双击图 3.3 显示的窗口中的 IronKey.app 应用图标。这会开始初始化过程。

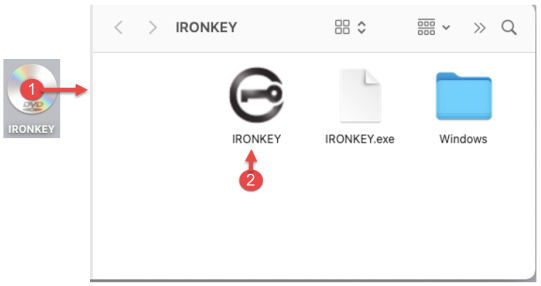


图 3.3：IronKey 卷

设备初始化（Windows 和 macOS 环境）

语言和最终用户许可协议 (EULA)

从下拉菜单中选择您的语言偏好，并单击**“下一步”**（*图4.1*）

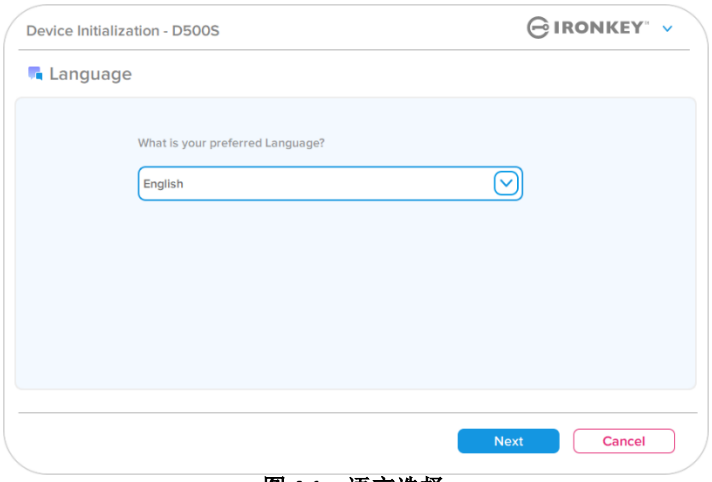


图 4.1：语言选择

阅读许可协议并单击**“下一步”**。
注意：您必须接受许可证协议才能继续操作；否则**“下一步”(Next)** 按钮将一直处于禁用状态。（*图4.2*）

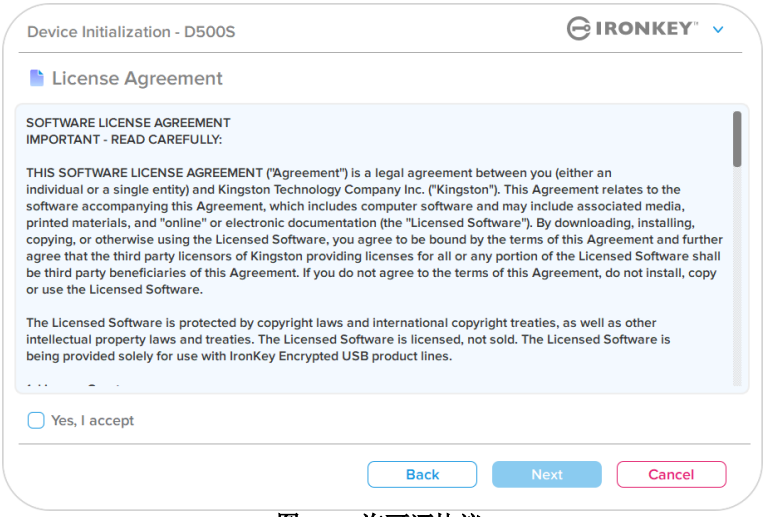


图 4.2：许可证协议

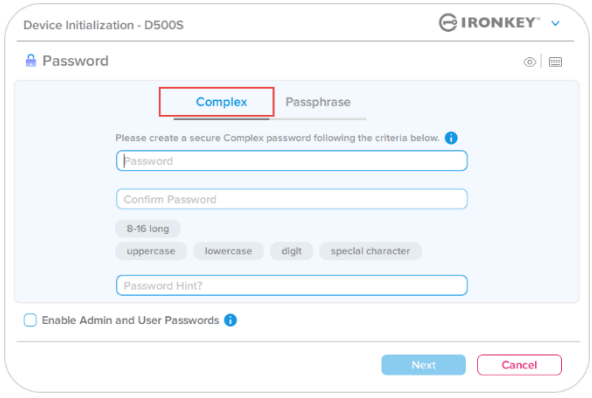
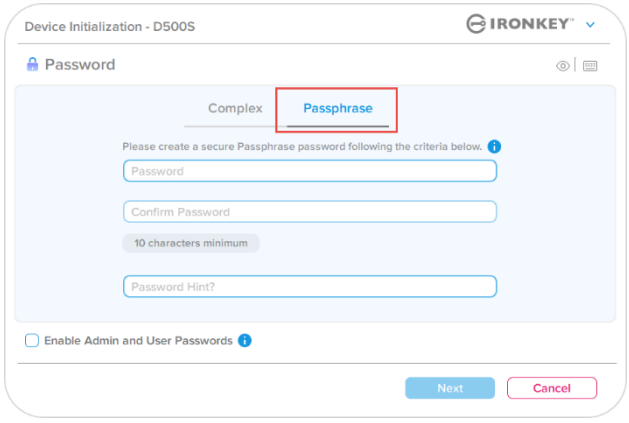
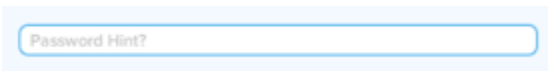
设备初始化

密码选择

在“密码”提示窗口中，您能够使用复杂密码或密码短语模式创建密码，来保护您在 D500S 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：一旦选择复杂密码或密码短语模式，将无法更改模式，除非重置设备。

要开始密码选择流程，请在“密码”字段中创建密码，然后在“确认密码”字段中重新输入密码。创建的密码必须符合以下条件，然后才能继续进行初始化过程：

复杂密码 • 密码必须包含 8 个或更多字符（最多 16 个字符）。 • 必须满足以下三 (3) 个条件： ○ 大写 ○ 小写 ○ 数字 ○ 特殊字符（!、$、& 等）	 **图 4.3：复杂密码**
密码短语密码 • 必须包含： ○ 最少 10 个字符 ○ 最多 128 个字符	 **图 4.4：密码短语密码**
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。 **注意：**提示内容不得与密码完全相同。	 **图 4.5：“密码提示”(Password Hint) 字段**

设备初始化

有效密码和无效密码

对于**有效**密码，密码条件框会在条件满足时以绿色高亮显示。（参见*图4.6a-b*）

注意：一旦满足至少三个密码条件，第四个条件框会变成灰色，表示此条件不可选（*图4.6b*）。

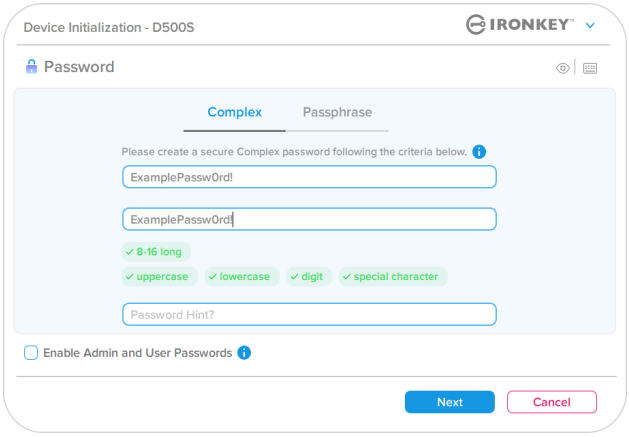


图 4.6a：已满足复杂密码条件

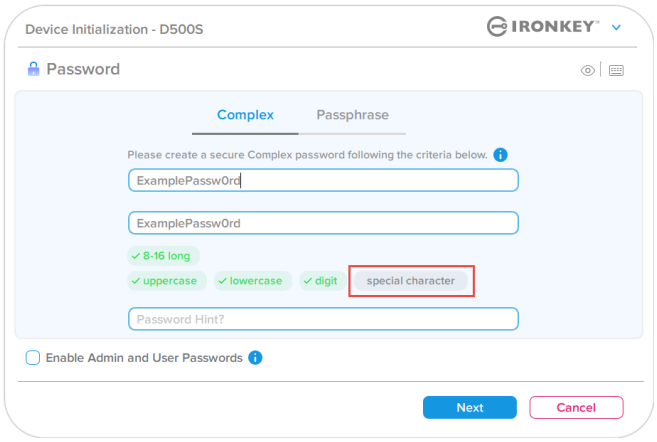


图 4.6b：复杂密码条件可选

对于**无效**密码，密码条件框会以红色高亮显示，**“下一步”(Next)** 按钮会在满足最低要求前被停用。

这适用于复杂密码和口令密码。

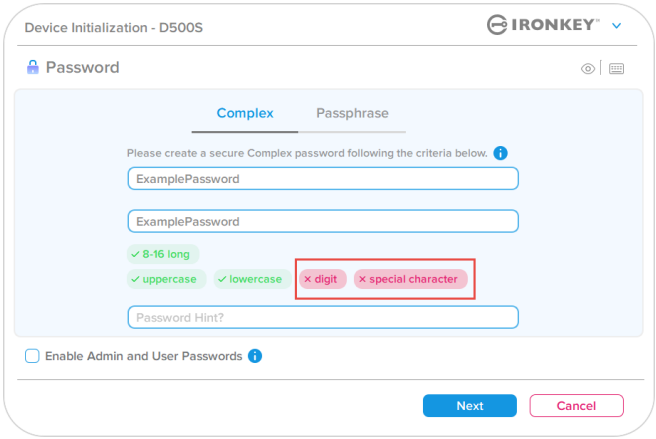


图 4.7：未满足复杂密码条件

设备初始化

虚拟键盘

D500S 配备虚拟键盘，可防范按键记录程序。

- 要利用**虚拟键盘**，在**“设备初始化”**屏幕的右上角找到键盘按钮，并选择该按钮。

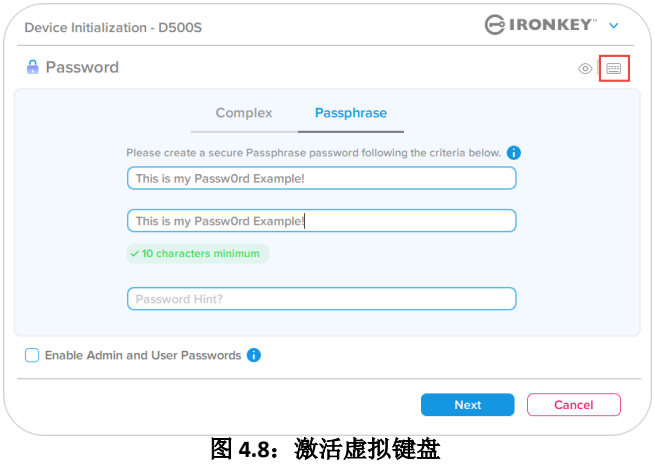


图 4.8：激活虚拟键盘

- 一旦虚拟键盘出现，您还可以启用**屏幕记录器防护**。使用该功能后，所有按键都会短暂变成空白。这是预期的行为，可以阻止屏幕记录器捕获您点击的内容。
- 为了让这项功能更加强大，您还可以选择键盘右下角的**“随机排列”**，让虚拟键盘随机排列。随机排列会以随机方式排列键盘布局。

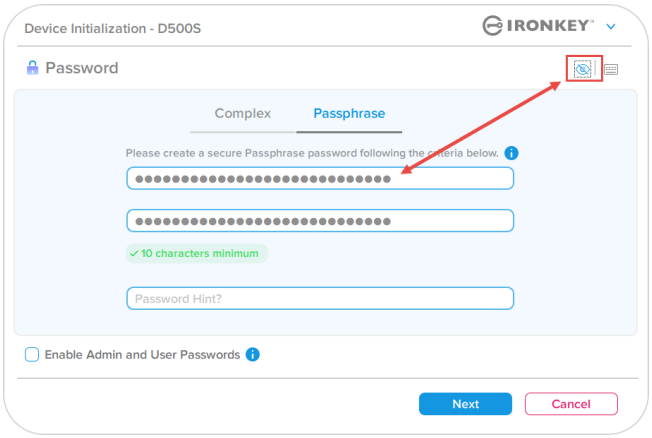
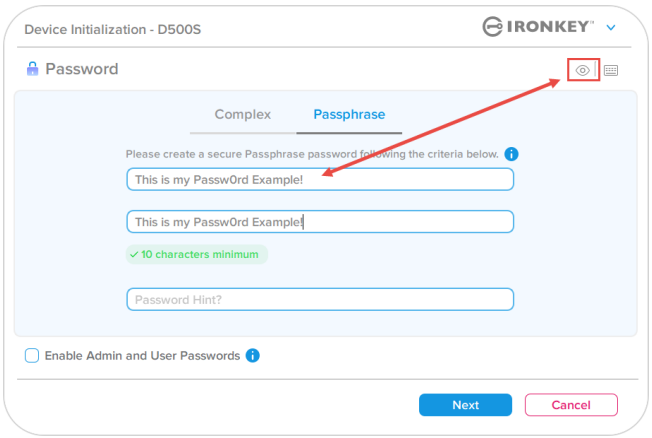
图 4.9：屏幕记录器保护 / 随机排列

设备初始化

密码可见性切换

默认情况下，当您创建密码时，密码字符串会在输入过程中显示在字段中。如果希望在输入过程中隐藏密码，可以切换“设备初始化”窗口右上角的密码“眼睛”。

注意：在设备完成初始化后，密码字段默认为“隐藏”。

要**隐藏**密码字符串，请单击灰色图标。 	 **图 4.10：切换为“隐藏”密码**
要**显示**隐藏的密码，请单击蓝色图标。 	 **图 4.11：切换为“显示”密码**

设备初始化

管理员密码和用户密码

通过启用管理员密码和用户密码，您可以利用多密码功能，其中管理员角色可以管理这两种帐号。通过选择**“启用管理员密码和用户密码”**，可在忘记密码时实现替代的闪存盘访问方法。

启用**管理员密码和用户密码**后，您还可以访问：

- 双分区配置
- 一次性恢复密码
- 用户登录强制只读模式
- 用户密码重置
- 用户登录的强制重置密码
- 加密擦除密码

要详细了解这些功能，请转到本用户指南第 25 页。

- 要启用**管理员密码和用户密码**，请单击**“启用管理员密码和用户密码”**旁的框，并在选定有效密码后选择**“下一步”**。（*图4.12*）
- 如果该功能已启用，那么本屏幕中的所选密码是管理员密码。单击**“下一步”**，会转到**“用户密码”**屏幕，在此可为用户选择密码。

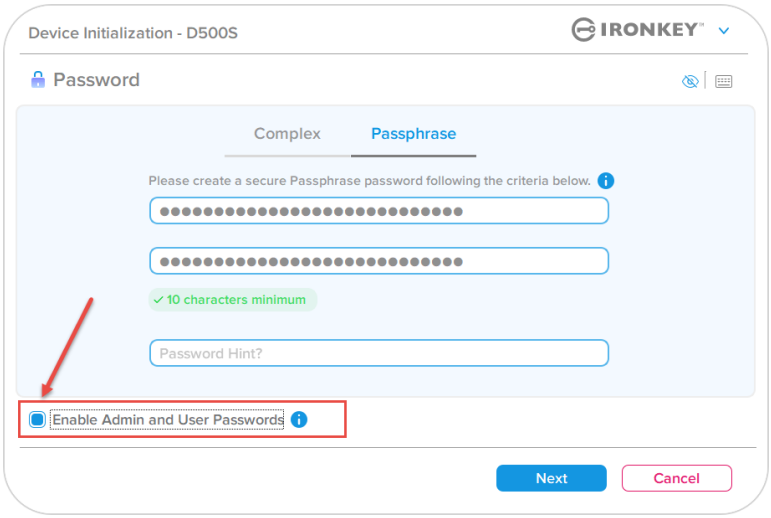


图 4.12：启用管理员密码和用户密码

注意：启用管理员密码和用户密码是可选项。

如果设置闪存盘时未启用该功能（未勾选框），那么闪存盘会配置为**单用户、单密码闪存盘**，且**无任何管理员功能**。该配置在本手册中称为仅用户模式。

要继续进行单用户、单密码设置，请确保**“启用管理员密码和用户密码”**未勾选，然后在创建有效密码后单击**“下一步”**。

注意：“管理员密码和用户密码”在本手册下文中称作**“管理员角色”**。

设备初始化

管理员密码和用户密码

- 如果管理员角色在前一屏幕中**已启用**，下一屏幕会提示创建用户密码（*图4.13*）。**用户密码**的权限比管理员密码少，在本指南后续部分将作详细介绍（参阅第 23 页）。

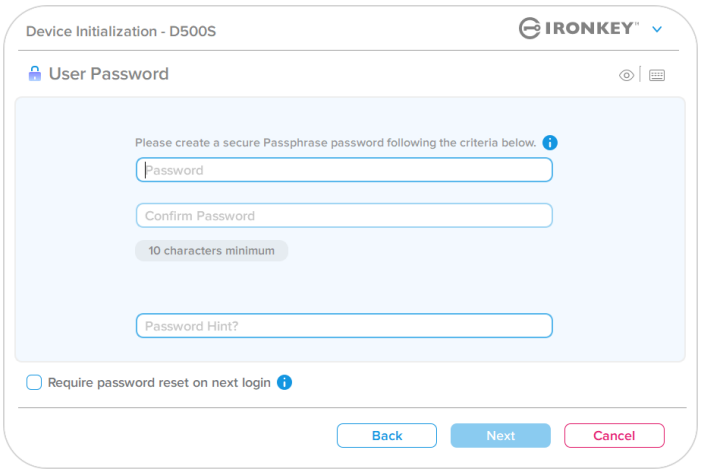


图 4.13：用户密码（管理员和用户已启用）

注意：所选密码选项（复杂或口令）条件会应用于用户密码、一次性恢复密码、密码擦除密码，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进行更改。

- **“要在下次登录时重置密码”**功能位于图 4.13 的左下角，仅适用于用户密码，启用后可强制用户使用由管理员在初始化过程中设定的临时密码，然后在使用临时密码完成闪存盘身份验证后将其更改为用户所选密码。当需要将闪存盘提供给另一个人使用时，这会很有帮助。（*图4.14*）

  注意：出于安全考虑，新密码不能与临近密码相同。

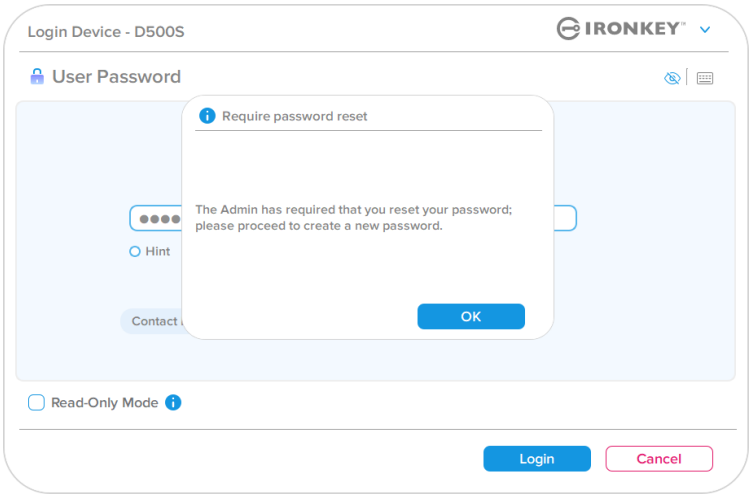


图 4.14：要在下次登录时重置密码

设备初始化

双分区

IronKey D500S 允许您在管理员和用户之间创建两个自定义大小的独立分区。如果启用此功能，则管理员登录可**同时**访问用户和管理员分区，而用户登录**只能**访问用户分区。此功能可用于在管理员与用户之间安全地分离数据和文件访问权限，也可用于启用隐藏的文件存储，以防止在不受信任的系统上暴露不需要的文件。管理员与用户之间的分区大小也可以根据需要进行调整。

注意：此功能是*可选的*，可以通过在设置过程中不选中“启用双分区”框来禁用（*图4.15*）

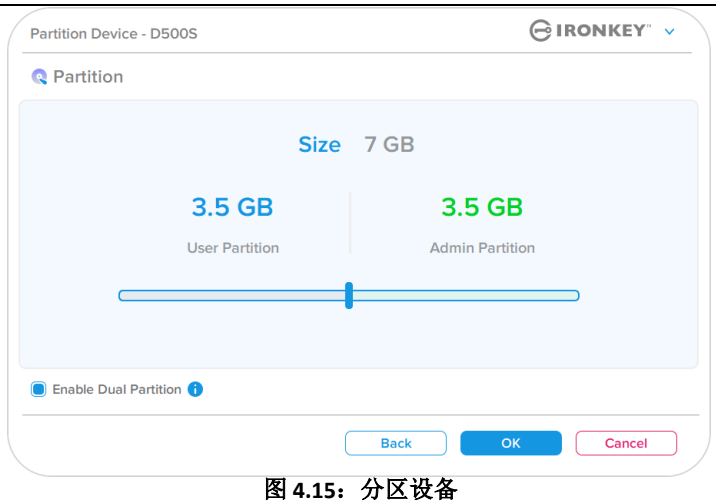


图 4.15：分区设备

要在用户与管理员之间调整和分配分区大小，请分别向左或向右移动滑块（*图4.16*）。

- 分区可以按 0.5GB 的增量进行调整。
- 分区大小基于隐藏分区上可用存储的总容量。
- 默认情况下，双分区滑块设置为在管理员和用户之间平均分配存储，直到手动调整为止。
- 可以分配的最小分区大小是 1GB。

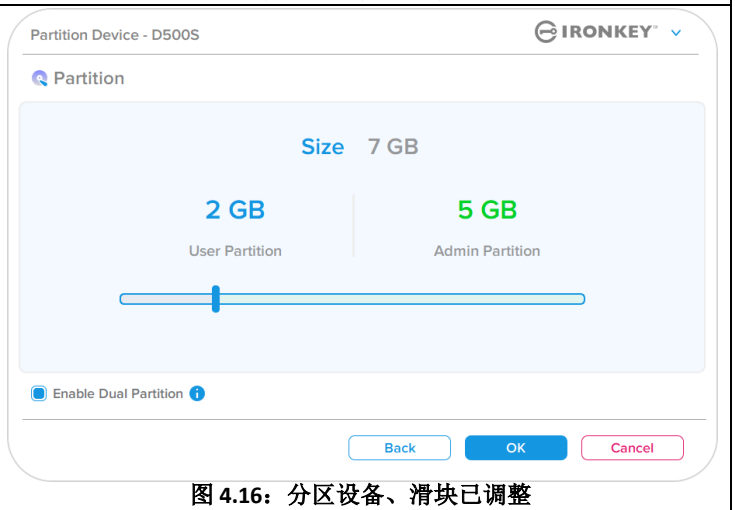


图 4.16：分区设备、滑块已调整

管理员登录

一旦闪存盘在启用双分区的情况下完全设置，管理员登录将显示一个选项，可以解锁闪存盘，以便在每次成功登录时访问管理员分区或用户分区。（*图4.17*）

注意：一次只能打开一个分区。用户分区和管理分区不能同时解锁。

用户登录将不会显示此选项，并且将仅自动解锁用户分区。

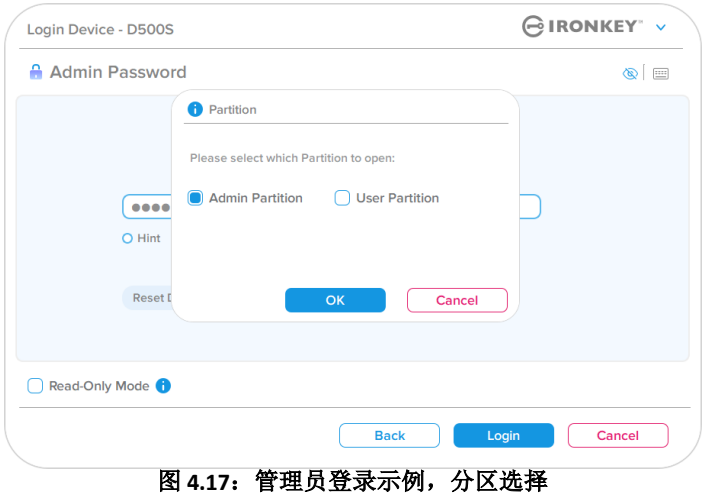


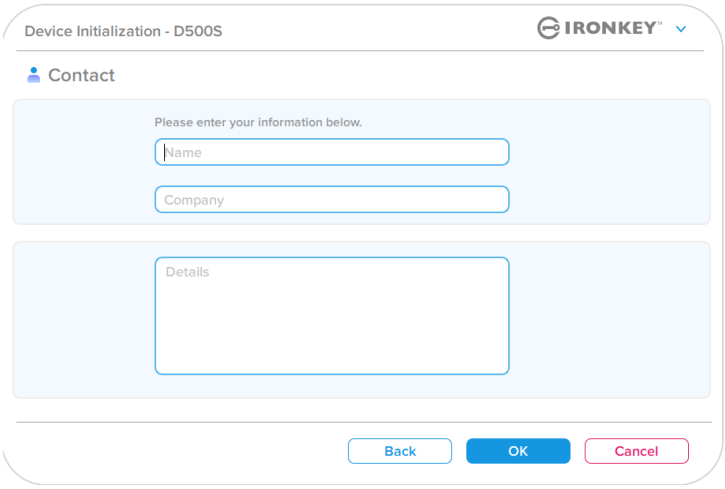
图 4.17：管理员登录示例，分区选择

设备初始化

联系信息

在提供的文本框中输入您的联系信息（参见*图4.18*）

注意：您在这些字段中输入的信息可能不包含您在步骤 3 中创建的密码字符串。但是，这些字段是可选的，如果需要，可以留空。

“姓名”字段最多可包含 32 个字符，但是不得包含**确切**密码。 **“公司”**字段最多可包含 32 个字符，但是不得包含**确切**密码。 **“详情”**字段最多可包含 156 个字符，但是不得包含**确切**密码。	 **图 4.18：联系信息**

注意：单击“确定”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 D500S 应用会启动，首先会弹出“用户密码”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”（如下所示），该应用会转到管理员登录菜单，您在此可以作为管理员登录，以访问管理员设置和功能（*图5.2*）。

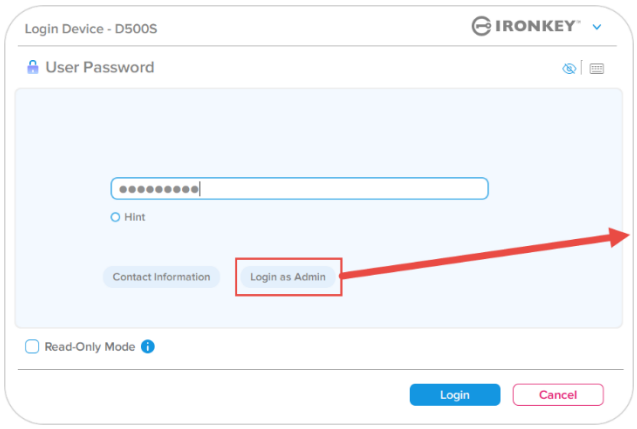


图 5.1：用户密码登录（管理员已启用）

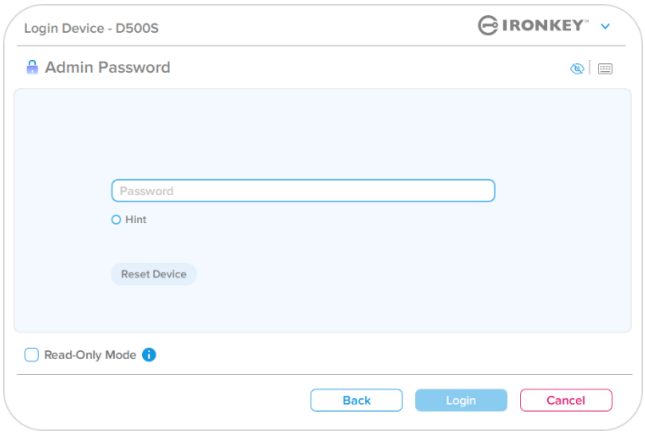


图 5.2：管理员密码登录

仅用户模式登录（管理员未启用）

如前所述，尽管建议使用管理员角色功能来发挥设备的全部优势，但 IronKey 设备也可以初始化为仅用户（单密码、单用户）配置。这个选项适合希望用简单的单密码方法保护闪存盘数据的用户。（*图5.3*）

注意：要启用管理员密码和用户密码，请使用**“重置设备”**按钮，让闪存盘进入初始化状态，从而可以启用管理员密码和用户密码。**重置闪存盘后，闪存盘会被格式化，其中所有数据会丢失。**

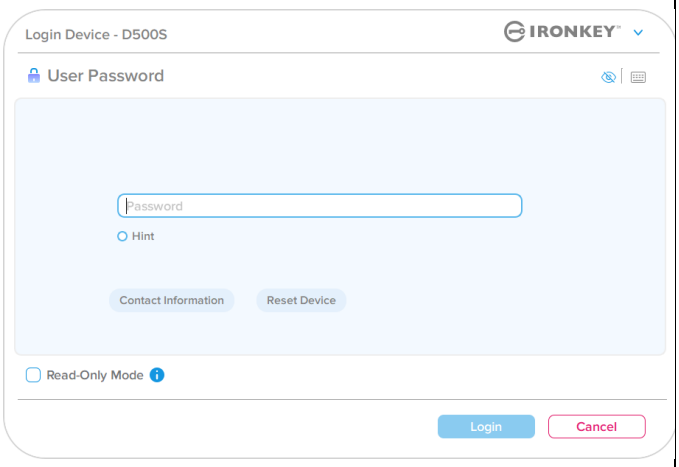


图 5.3：用户密码登录（管理员未启用）

设备使用

在只读模式下解锁

您可以以只读状态解锁闪存盘，确保 IronKey 闪存盘中的文件无法被修改。例如，当使用不受信任或未知的计算机时，以只读模式解锁设备，可以阻止计算机中的任何恶意软件感染设备或修改文件。

在这种模式下运行时，您无法执行任何会修改闪存盘中文件的操作。
例如，您无法重新格式化闪存盘、还原、添加或编辑闪存盘中的文件。

要在只读模式下解锁设备：

1. 将设备插入主机的 USB 端口，然后运行 **IronKey.exe** 文件。
2. 选中密码输入框下方的**只读模式**（*图 5.4*）。
3. 键入您的设备密码，然后单击**“登录”**。设备现在会以只读模式解锁。

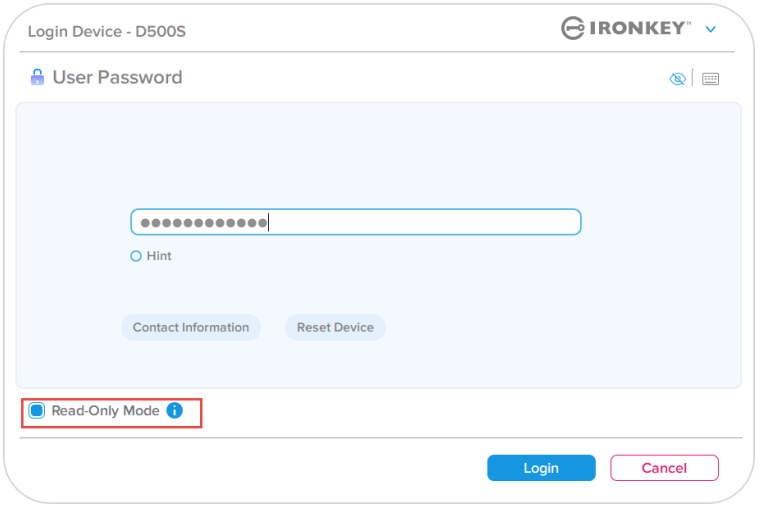


图 5.4：只读模式

如果您希望解锁设备并能够完全读取/写入安全数据分区，您必须关闭 D500S 并重新登录，同时取消勾选“只读模式”复选框。

注意：D500S 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 31 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 次不正确的密码尝试）**	**数据擦除和设备重置？**
用户密码	密码锁定。作为管理员登录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	**是**
一次性恢复密码	“Password Lockout, Recovery Password”（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/用户未启用）	**暴力攻击防护 设备行为 （10 次不正确的密码尝试）**	**数据擦除和设备重置？**
用户密码	加密擦除闪存盘、密码、设置和数据	**是**

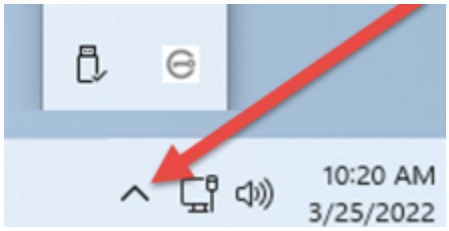
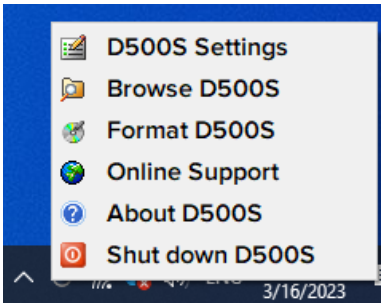
* 一旦您成功完成设备的身份验证，则会针对所用的登录方法重置失败登录计数器。加密擦除会删除所有密码、加密密钥和数据 – **您的数据会永久丢失**。

访问我的安全文件

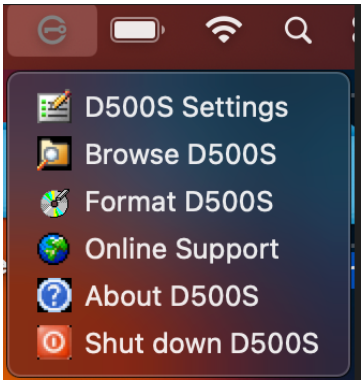
解锁闪存盘后，您可以访问自己的安全文件。当您在闪存盘上保存或打开文件时，会自动加密和解密文件。这项技术不仅让您可以像通常操作普通闪存盘一样方便，还提供了“始终在线”的强大安全性。
提示：通过直接单击 Windows 任务栏中的 **IronKey 图标**并单击**“浏览 D500S”**，您也可以访问自己的文件（*图 6.2*）。

设备选项 -（Windows 环境）

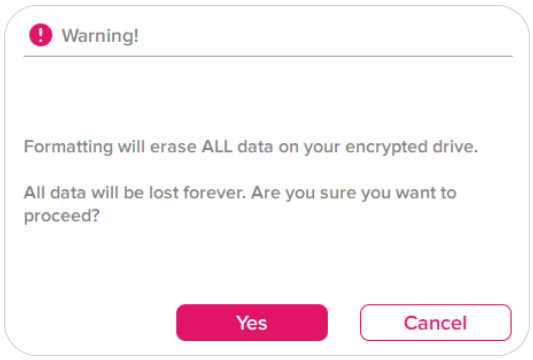
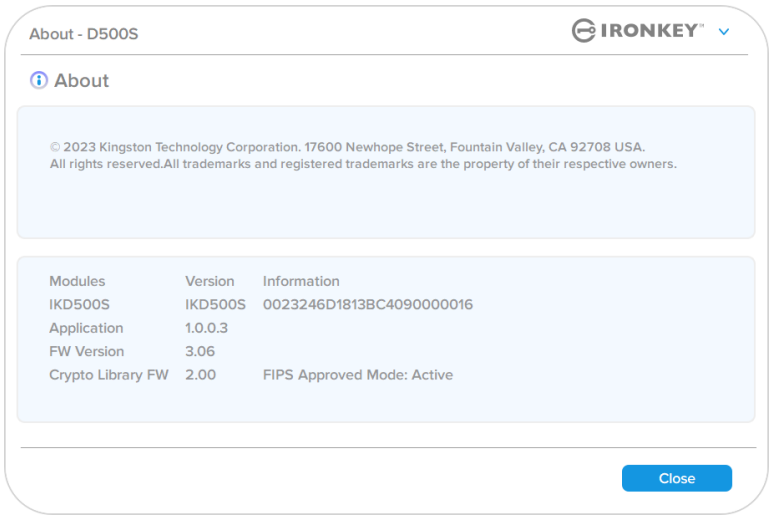
登录设备后，IronKey 图标会出现在 Windows 右下角。右击 IronKey 图标，会打开可用闪存盘选项的选择菜单（*图 6.2*）。
关于这些设备选项的详情，可在本手册第 21-25 页找到。

• 登录设备后，IronKey 图标会出现在 Windows 右下角（*图 6.1*）。	 **图 6.1：任务栏中的 IronKey 图标**
• 右击 IronKey 图标，会打开可用闪存盘选项的选择菜单（*图 6.2*）。 关于这些设备选项的详情，可在本手册第 19-23 页找到。	 **图 6.2：右击 IronKey 图标以打开设备选项**

设备选项 -（macOS 环境）

• 登录设备后，IronKey D500S 图标会出现在 macOS 菜单中（如图 6.3 所示），打开后显示可用的设备选项。 关于这些设备选项的详情，可在本手册第 19-23 页找到。	 **图 6.3：macOS 菜单栏图标/设备选项菜单**

设备选项

D500S 设置：	• 更改登录密码、联系信息和其他设置。（有关设备设置的更多详情，请参见本手册“D500S 设置”部分。）
浏览 D500S：	• 允许您查看安全文件。
格式化 D500S： 允许您格式化安全数据分区。（警告：所有数据都将被抹除。）（*图 6.1*） **注意：**格式化需要密码身份认证。	 **图 6.1 – 格式化 D500S**
在线支持：	• 打开互联网浏览器并导航至 http://www.kingston.com/support，您可以在这里获取更多的支持信息。
关于 D500S： 提供关于 D500S 的具体详情，包括应用程序、固件和序列号信息（*图 6.2*） **注意：**闪存盘的唯一序列号位于“Information”（信息）列下	 **图 6.2 – 关于 D500S**
关闭 D500S：	• 正确关闭 D500S，允许您将其从系统上安全删除

D500S 设置

管理员设置

管理员登录支持访问以下设备设置：

- **密码：**允许您更改您自己的管理员密码和/或提示（*图 7.1*）
- **联系信息：**允许您添加/查看/更改联系信息（*图 7.2*）
- **语言：**让您可以更改当前语言选择（*图 7.3*）
- **管理员选项：**允许您启用额外的功能，例如：（*图 7.4*）
  - 更改用户密码
  - 登录密码重置（针对用户密码）
  - 启用一次性恢复密码
  - 启用加密擦除密码
  - 用户数据强制只读模式

注意：有关管理员选项的更多详情，请参见第 26 页

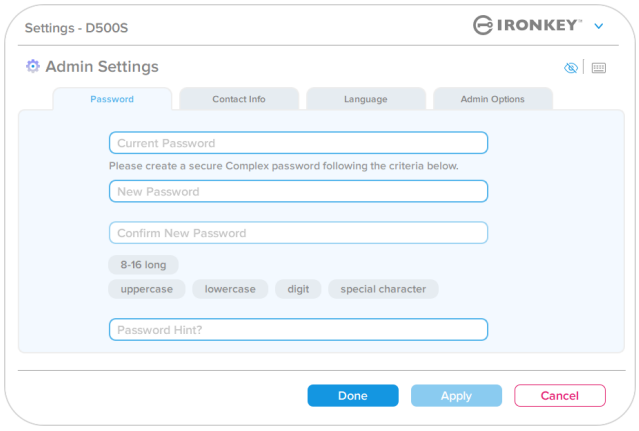


图 7.1：密码选项

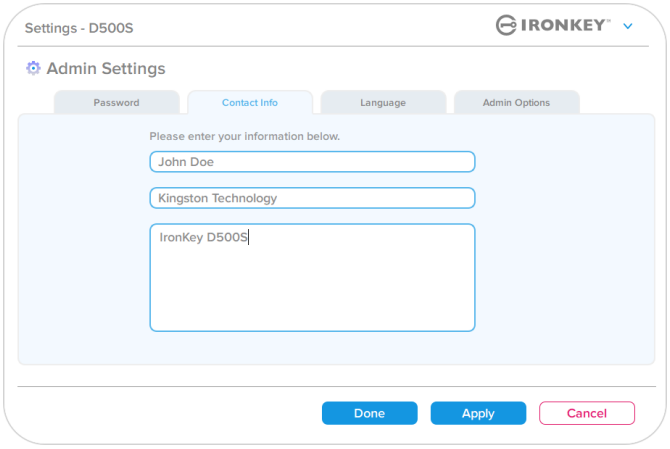


图 7.2：联系信息

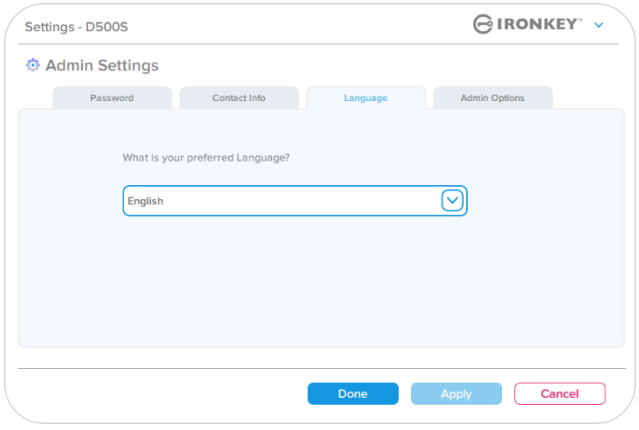


图 7.3：语言选项

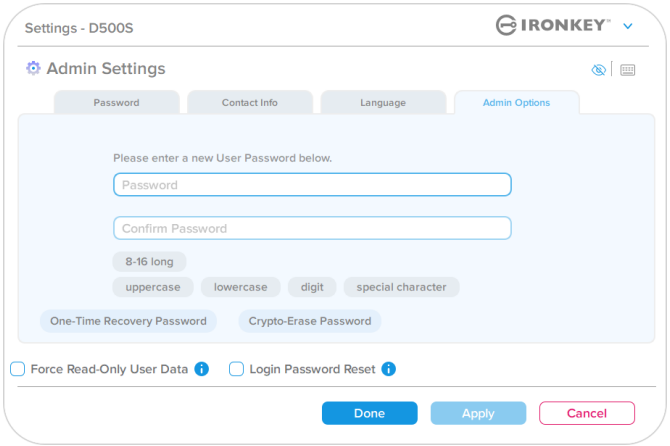
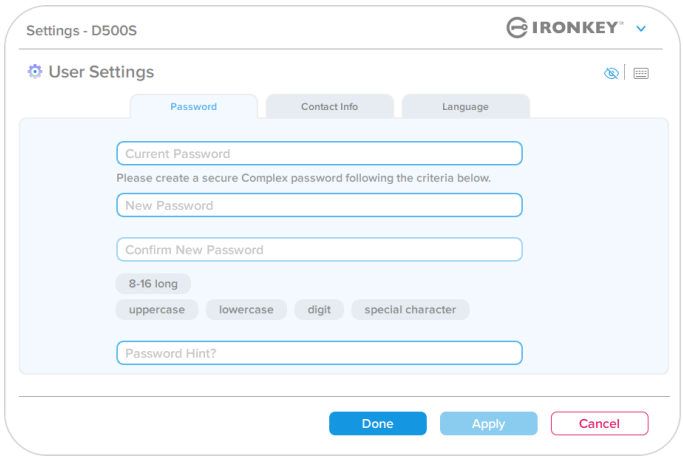
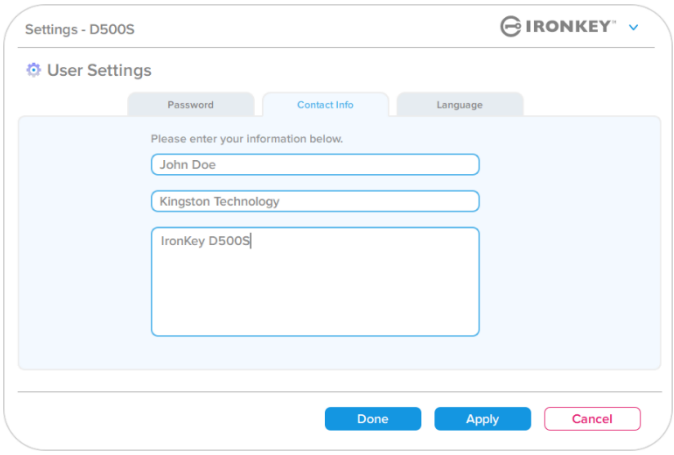
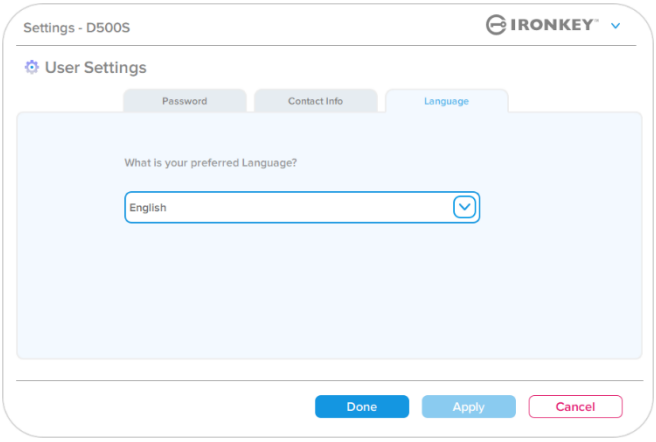


图 7.4：管理员选项

D500S 设置

用户设置：管理员已启用

用户登录仅能访问以下设置：

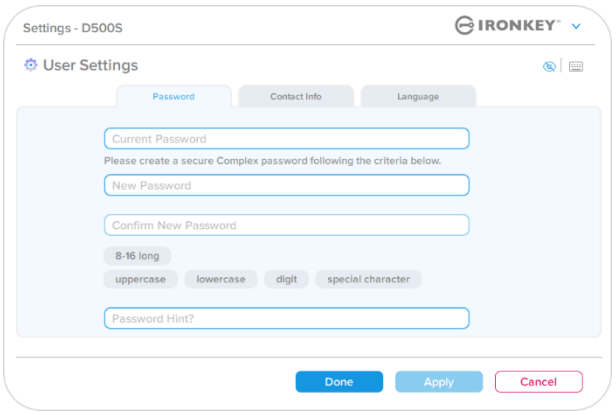
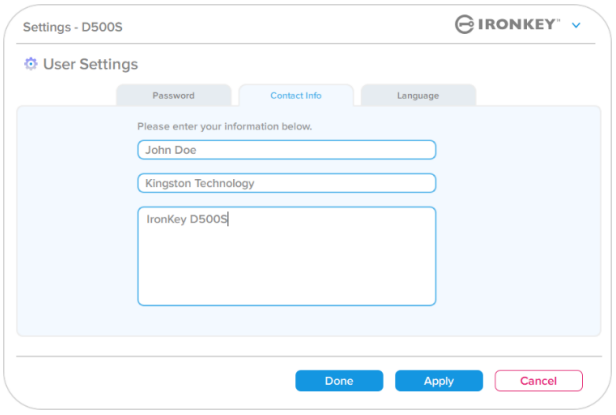
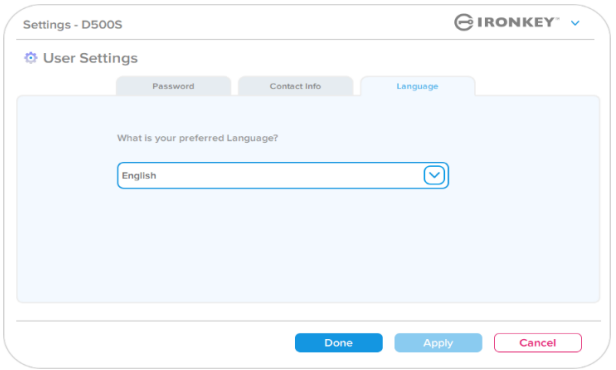
Password（密码）： 允许您更改您自己的用户密码和/或提示（*图7.5*）	 **图 7.5：密码选项（管理员已启用：用户登录）**
Contact Info（联系信息）： 允许您添加/查看/更改联系信息（*图7.6*）	 **图 7.6：联系信息（管理员已启用：用户登录）**
Language（语言）： 让您可以更改当前语言选择（*图7.7*）	 **图 7.7：语言设置（管理员已启用：用户登录）**

注意：使用用户密码登录时，无法访问管理员选项。

D500S 设置

用户设置：管理员未启用

如前所述，如果在初始化 D500S 时不启用“管理员和用户”密码，会将闪存盘配置为**“单密码、单用户”设置（仅用户模式）**。该配置无法访问任何管理员选项或功能。该配置可以访问以下 D500S 设置：

Password（密码）： 允许您更改您自己的用户密码和/或提示（*图 7.8*）	 **图 7.8- 密码选项（仅用户模式）**
Contact Info（联系信息）： 允许您添加/查看/更改联系信息（*图 7.9*）	 **图 7.9- 联系选项（仅用户模式）**
Language（语言）： 让您可以更改当前语言选择（*图 7.10*）	 **图 7.10- 语言选项（仅用户模式）**

D500 设置

更改和保存设置

- 每当 D500S 设置中的设置（例如联系信息、语言、密码更改、管理员选项）更改时，闪存盘都会提示输入您的密码以接受并应用更改（*图 7.11*）。

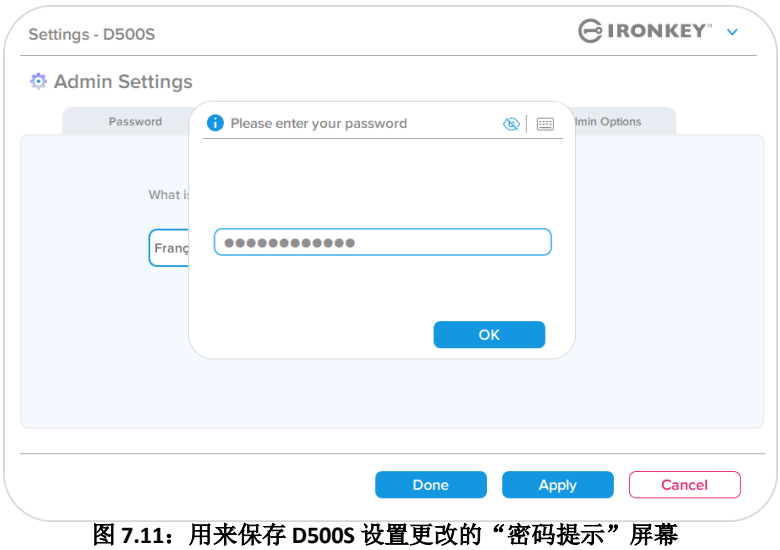


图 7.11：用来保存 D500S 设置更改的“密码提示”屏幕

注意：如果您处于上面的“密码提示”屏幕并希望取消或修改所作更改，只需确保密码字段为空并单击“确定”。这将关闭“请输入您的密码”框，并返回到 D500S 设置菜单。

管理员功能

用于重置用户密码的选项

如果忘记用户密码或创建了临时用户密码并希望下次用户登录时强制更改密码，可以利用管理员配置功能，通过多个方法安全地重置用户密码。以下功能有助于重置用户密码：

用户密码重置：
在“管理员选项”菜单中手动更改用户密码，这可以立即实现更改并在下次用户登录时生效（*图8.1*）

注意：密码要求条件默认为在初始化流程中设定的原始条件（复杂或口令选项）。

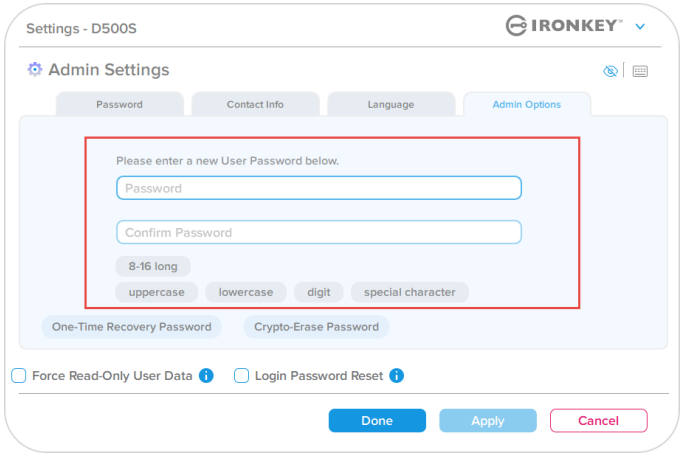


图 8.1：管理员选项/用户密码重置

登录密码重置：
启用登录密码重置会**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8.2 和8.3*）

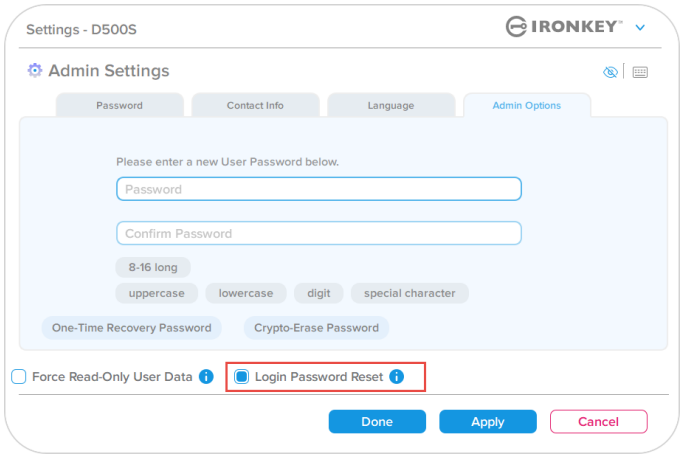


图 8.2：“登录密码重置”按钮

注意：应用这项重置后，会在下次用户登录成功后生效。还会根据初始化过程中设定的原始选项自动应用密码要求条件（复杂或口令选项）。

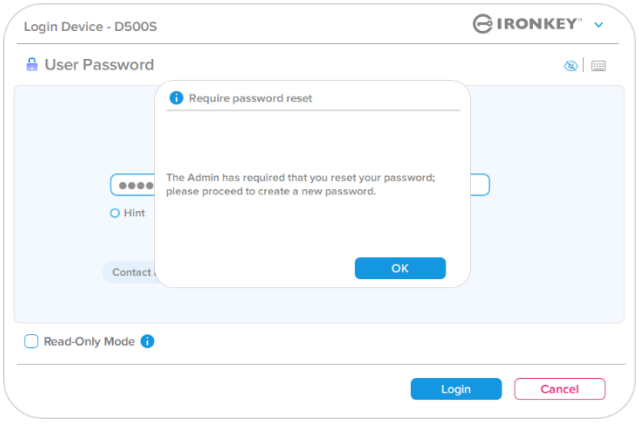


图 8.3：输入用户密码后的重置通知

管理员功能

一次性恢复密码

本部分介绍启用和使用一次性恢复密码功能的流程。

一次性恢复密码

第 1 步：一次性恢复密码功能是非常有用的一次性密码，当忘记用户密码时，可启用该功能帮助恢复和重置用户密码。单击“管理员选项”菜单中的“一次性恢复密码”按钮以开始。（*图 8.4*）

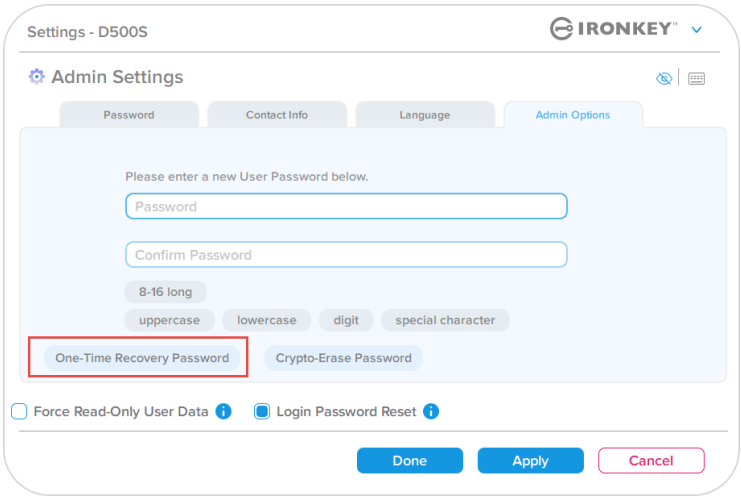


图 8.4：“一次性恢复密码”按钮

第 2 步：使用设备初始化时所设定的同一密码条件来创建一次性恢复密码（复杂密码或密码短语）。

注意：应用更改需要提供管理员密码。

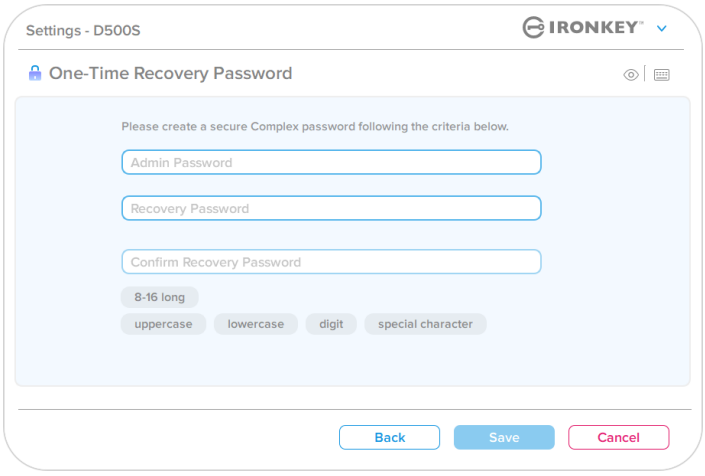


图 8.5：一次性恢复密码设置

管理员功能

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”**登录屏幕中。单击**“恢复密码”**按钮来启动该流程。

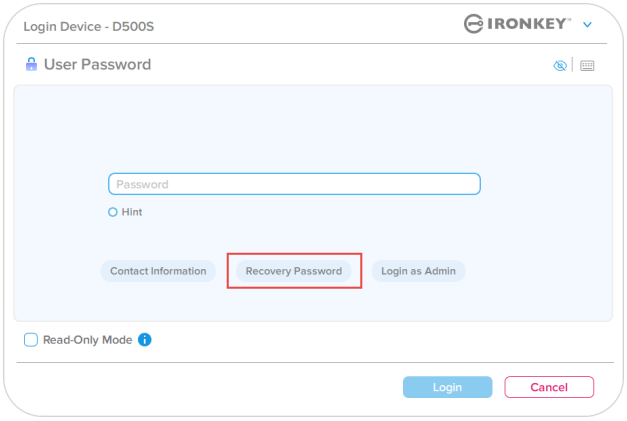


图 8.6：“恢复密码”按钮

第 2 步：**“恢复密码”**屏幕会出现，您可以在此输入恢复密码并创建新的用户密码。（*图 8.7*）

重要事项：一次性恢复密码也会利用内置的安全功能来跟踪失败的登录尝试次数，**使用一次性恢复密码登录失败 10 次后该密码会被停用**，必须以管理员身份登录后进行重新启用。（参见第 19 页和 33 页，了解更多详情）

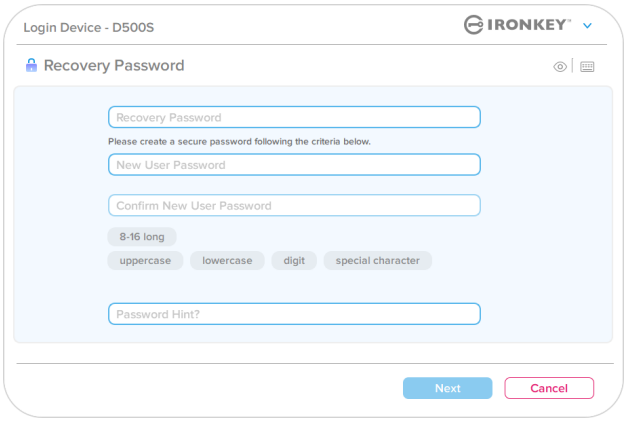


图 8.7：恢复密码菜单

第 3 步：成功后，您会返回到**“用户密码”**屏幕。**“恢复密码”**按钮现在已消失，而在第 2 步中输入的用户密码会变成新的用户
密码。（*图 8.8*）

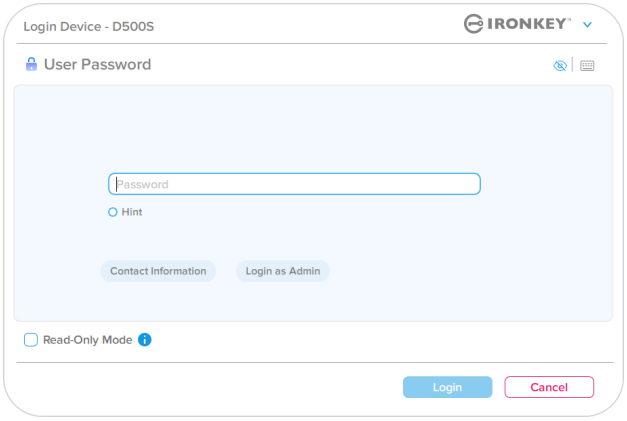


图 8.8：用户密码登录屏幕，显示“恢复密码”按钮会在成功使用后消失。

管理员功能

加密擦除密码

IonKey D500S 具有独特的加密擦除密码功能，在使用时通过安全擦除闪存盘的内容来保护和防御物理危害情况，使其看起来像从未向闪存盘写入过任何数据。当启用此功能，并且使用加密擦除密码解锁驱动器时，它将有效地在 D500S 闪存盘上执行谨慎的加密擦除，并将在出厂状态模式下使用空用户分区打开闪存盘。以前的加密密钥将被删除，并将创建一个新的设备加密密钥来取代它。***谨慎使用***

- 要**启用**此功能，请单击“管理员选项”选项卡中的“加密擦除密码”按钮：

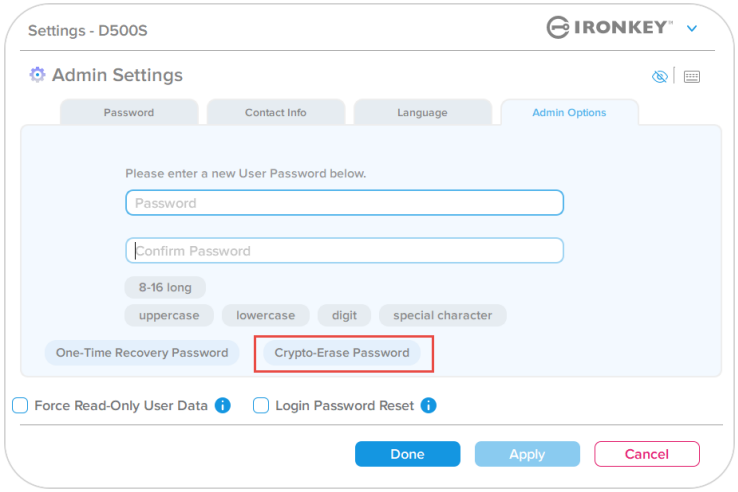


图 8.9：启用加密擦除密码

创建加密擦除密码：

- 密码规则将基于闪存盘最初初始化时使用的内容（复杂或密码短语）
- 验证需要提供管理员密码。

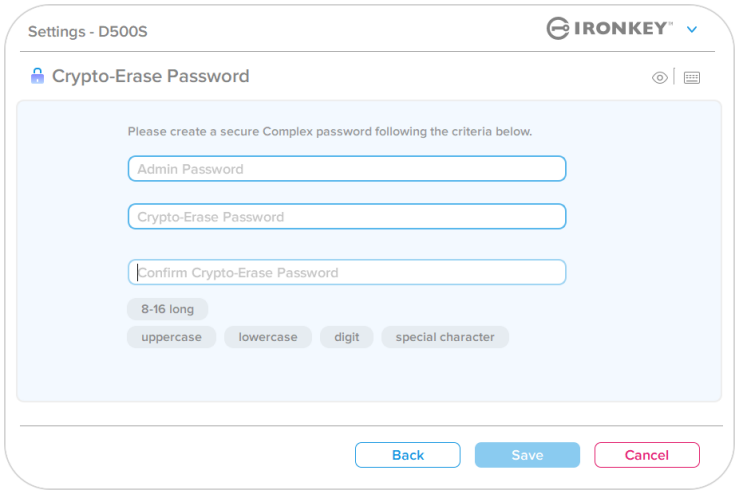


图 8.10：创建加密擦除密码

管理员功能

使用加密擦除密码

当使用加密擦除密码时，以前的管理员和用户密码将被删除，加密擦除密码将取而代之。此外，任何以前的配置设置都将被删除，同时永久删除闪存盘上存储的所有数据，并将闪存盘转换为“仅用户”模式配置。

要使用加密擦除密码：

1. 启动 IronKey.exe 以运行 IronKey 应用程序

2. 在“用户密码”登录屏幕上，按 **‘CTRL + ALT +C’** 切换加密擦除密码输入。如果操作正确，密码输入屏幕下会出现一个较粗的蓝色条，指示可以输入加密擦除密码。（*图 8.11*）

注意：加密擦除密码只能在用户密码登录屏幕上切换。

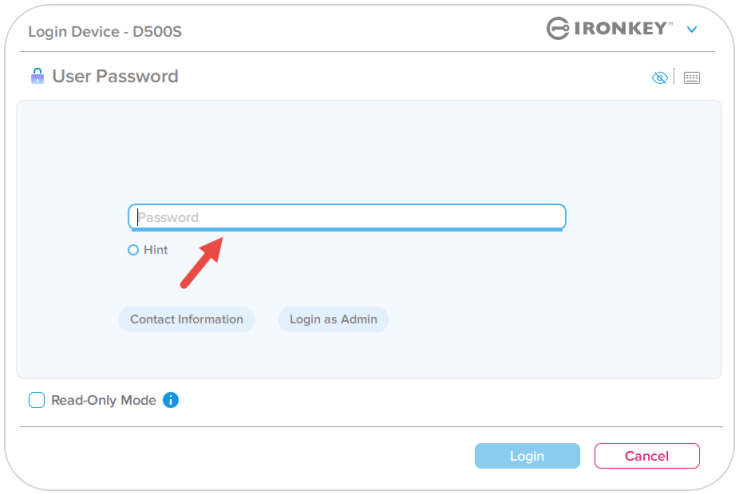


图 8.11：加密擦除已启用，带有蓝色粗条

一旦使用了加密擦除密码，闪存盘将继续擦除闪存盘的所有内容，并且出现一个空分区。闪存盘现在将处于“仅用户”模式状态，加密擦除密码将成为登录闪存盘的密码，直到重置为止。

重要提示：此功能将擦除闪存盘上的所有数据，并且以前存储的任何数据都将永远丢失，请谨慎操作。

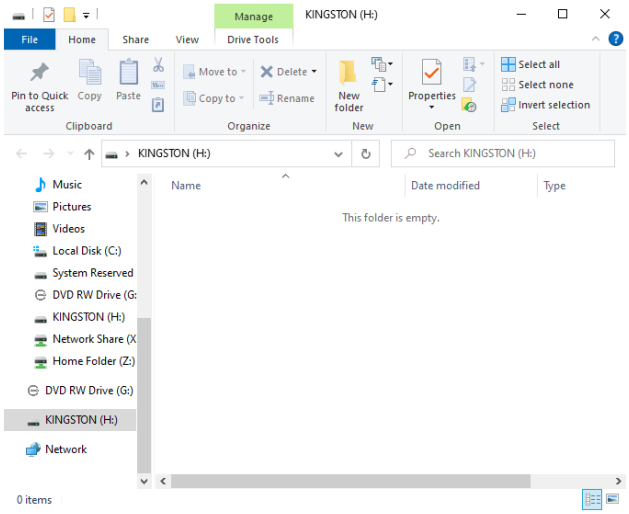


图 8.12：使用加密擦除密码后的闪存盘擦除

管理员功能

强制只读用户数据

通过启用强制只读模式功能，可以限制用户对闪存盘的写入操作。如果只需要读取闪存盘中的文件，这项功能就会有用。

- 要启用用户数据强制只读模式，请单击此框并单击“应用”。（*图8.13*）

  注意：这个强制只读模式仅适用于用户，不影响管理员登录。管理员登录仍有读取和写入权限，仍然可以在需要时启动只读模式。

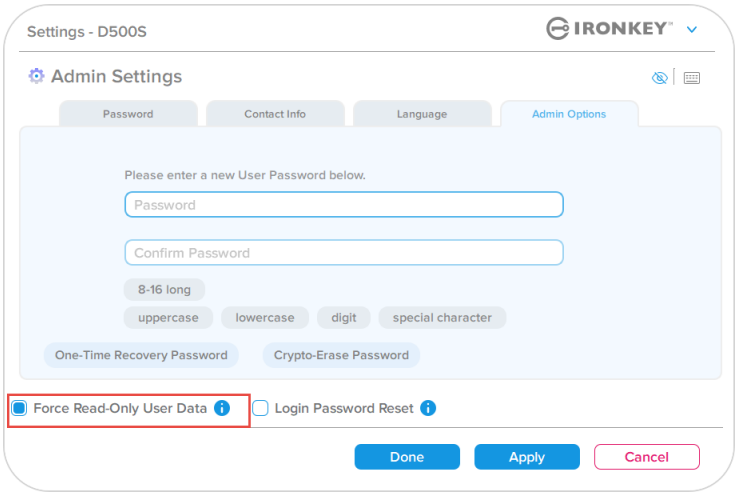


图 8.13：启用“强制只读用户数据”（应用更改需要提供管理员密码）

- 一旦启用，**“只读模式”**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，直到被管理员停用为止。（*图8.14*）

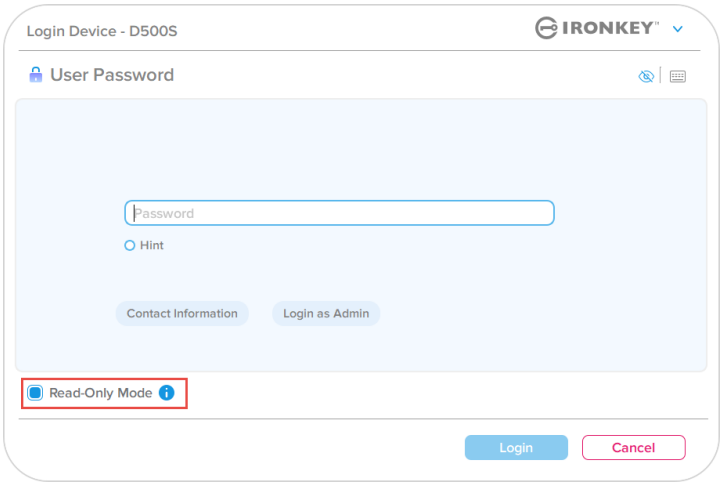


图 8.14：为用户强制启用只读模式，并且只能由管理员停用

帮助和故障排除

设备锁定

D500S 包含一项安全功能，当达到最大**连续**登录失败尝试次数（简称 *MaxNoA*）时，会阻止未经授权的人员访问数据分区。默认的“出厂”配置为每种登录方式（管理员/用户/一次性恢复密码）预先配置的值为 10（尝试次数）。

“锁定”计数器记录每次的失败登录，并且在满足下列**两种条件之一**时重置：

1. 在达到 MaxNoA 前成功登录
2. 达到 MaxNoA 并执行设备锁定或设备格式化，具体取决于闪存盘是如何配置的。

- 如果输入了错误的密码，将在密码输入字段下方出现一条错误消息，说明登录失败。（*图 9.1*）

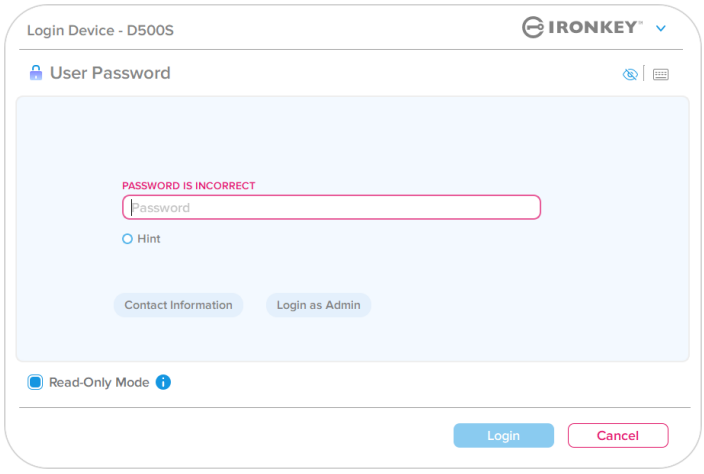


图 9.1：密码错误消息

- 如果出现**第 7 次**失败尝试，您将看到另外一条错误消息，提醒您在达到 MaxNoA（默认被设置为 10）之前还可以尝试 3 次（*图 9.2*）。

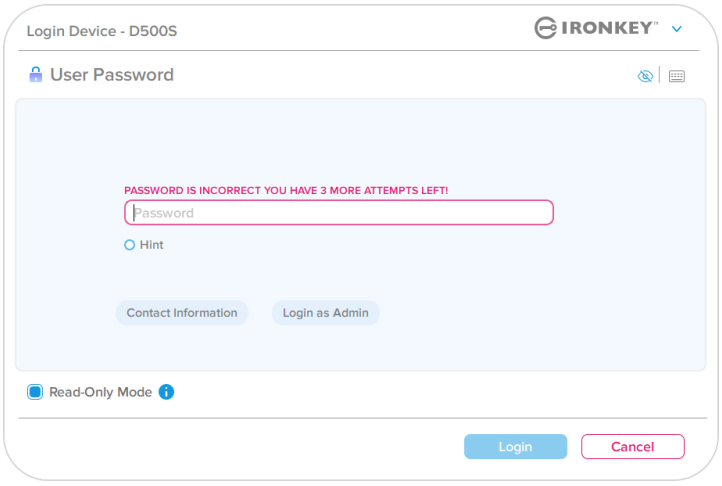


图 9.2：第 7 次不正确的密码输入

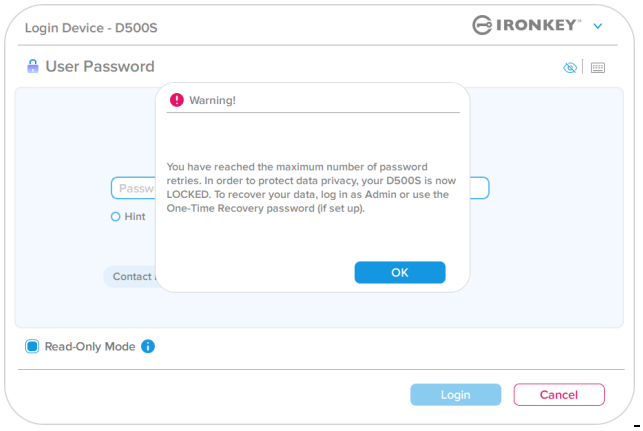
帮助和故障排除

设备锁定

重要事项：第 10 次即最后一次失败的登录尝试后，根据设备的设置和使用的登录方法（管理员、用户或一次性恢复密码），设备要么会锁定并要求您使用其他方法（若适用）进行登录，要么进行设备重置，**这会格式化数据，闪存盘中的所有数据会永久丢失**。本用户指南第 19 页也介绍了这些行为。

下面的图 9.3- 9.6 展示了各种登录密码方式在第 10 次即最后一次登录失败后的行为：

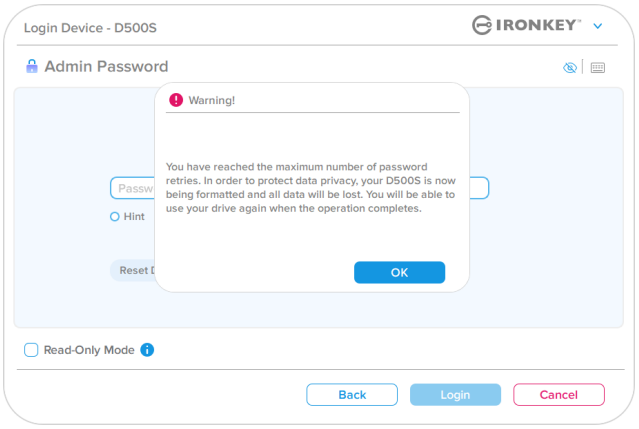
用户密码：（管理员/用户已启用）



设备锁定

图 9.3

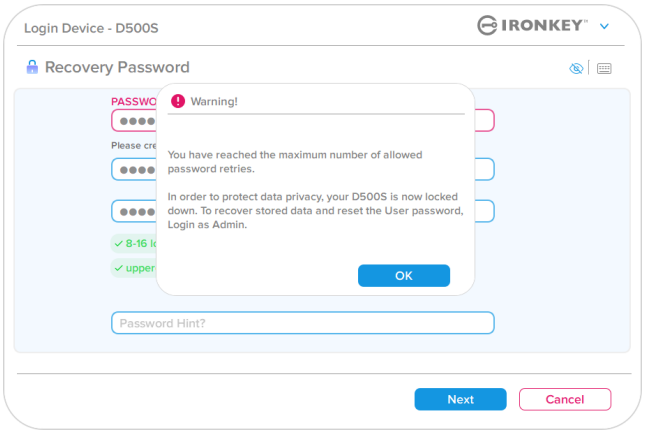
管理员密码（管理员/用户已启用）



设备格式化*

图 9.4

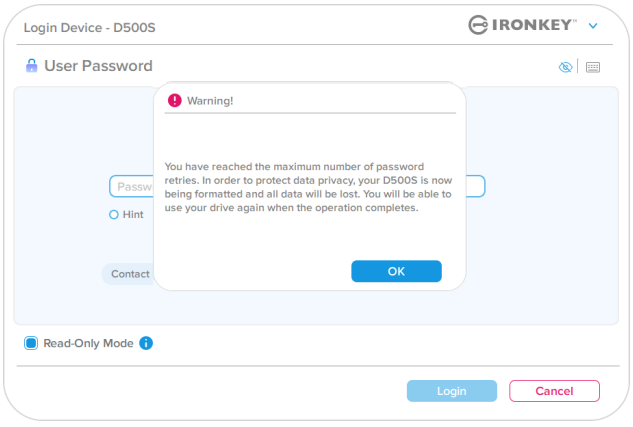
一次性恢复密码：（管理员/用户已启用）



设备锁定

图 9.5

用户密码（管理员未启用）



设备格式化*

图 9.6

这些安全举措可以限制他人（不知道您的密码）不限次数地尝试登录来访问您的敏感数据（又称暴力攻击）。如果您是 D500S 的所有者，但忘记了密码，那么相同的安全措施将同样会生效，包括设备格式化。有关该功能的更多信息，请参见第 25 页的 *“重置密码”*。

***注意：** 设备格式化将擦除 D500S 安全数据分区中保存的所有信息。*

帮助和故障排除

重置设备

如果忘记密码或需要重置设备，可以单击“重置设备”按钮。根据 D500S 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”菜单中，在未启用管理员/用户模式时则位于“用户密码”登录菜单中。）（参见*图9.7 和9.8*）

- 您可以通过这一选项新建密码，但是为了保护您数据的隐私，D500S 将被格式化。这意味着在这个过程中所有数据会被擦除。*

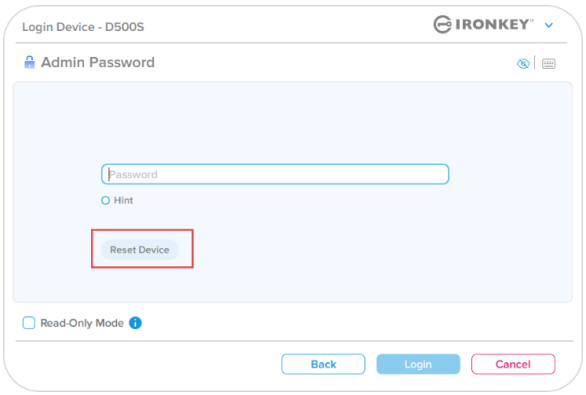


图 9.7：管理员密码：“重置设备”按钮

- **注意：**单击*“重置设备”*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”*以确认，也可以 2) 单击*“取消”*以返回登录窗口。（参见*图9.8*）

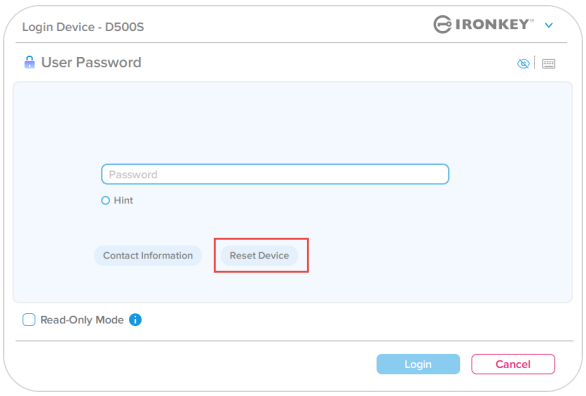


图 9.8：用户密码（管理员/用户未启用）重置设备

- 如果选择继续，会弹出“初始化”屏幕，您在此可以启用“管理员和用户模式”，并根据所选密码选项（复杂密码或密码短语）输入新密码。提示不是必填字段，但是该字段在忘记密码时有用，可以提供有关密码是什么的线索。

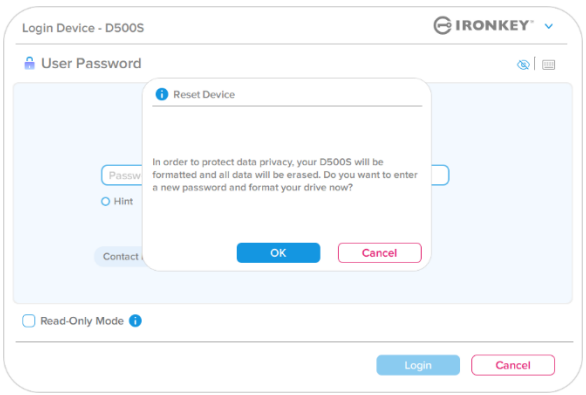


图 9.9：重置设备确认

帮助和故障排除

驱动器号冲突：Windows 操作系统

- 如本手册 *“系统要求”* 部分（第 3 页）所述，D500S 需要使用 2 个连续的驱动器号（在驱动器号分配“空缺”之前出现的最后一个物理磁盘之后）（参见*图 9.10*）。这不适用于网络共享，因为它们特定于用户配置文件而不是系统硬件配置文件本身，因此对操作系统而言看起来是可用的。
- 这意味着，Windows 可能会给 D500S 分配已经被网络共享或者被通用命名约定 (UNC) 路径使用的驱动器号，从而导致驱动器号冲突。如果发生这种情况，请联系您的管理员或帮助台部门，以便在 Windows 磁盘管理中更改驱动器号分配（需要管理员权限）。如本手册 *“系统要求”* 部分（第 3 页）所述，D500S 需要使用 2 个连续的驱动器号（在驱动器号分配“空缺”之前出现的最后一个物理磁盘之后）（参见*图 9.10*）。这不适用于网络共享，因为它们特定于用户配置文件而不是系统硬件配置文件本身，因此对操作系统而言看起来是可用的。

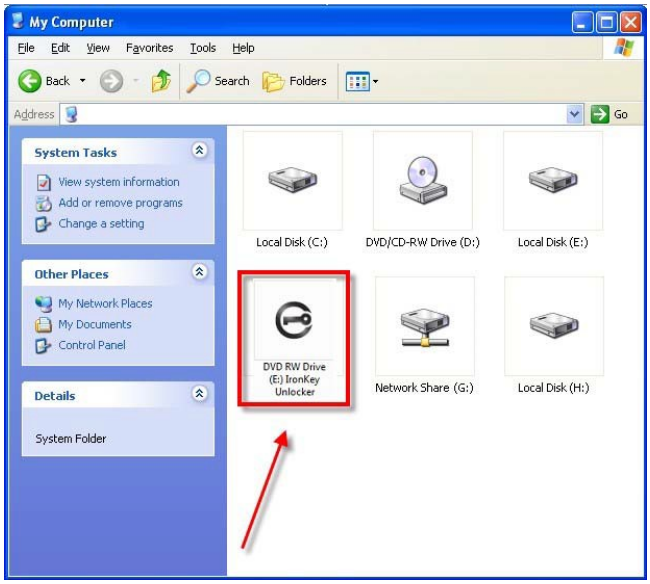


图 9.10：驱动器号示例

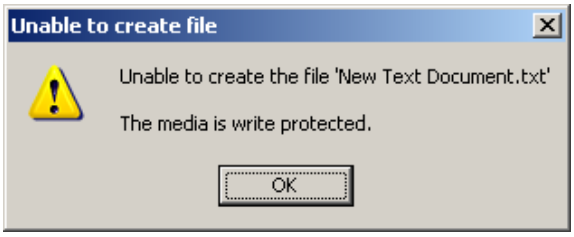
在本例中（*图 9.10*），D500S 使用驱动器 F:，这是驱动器 E: 之后第一个可供使用的驱动器号（E: 是驱动器号空缺之前的最后一个物理磁盘。）因为驱动器号 G: 是网络共享的，不是硬件配置文件的一部分，所以 D500S 可能会尝试将它用作其第二个驱动器号，从而导致冲突。

如果您的系统中没有网络共享，但 D500S 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 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 Kingston 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

Unable to create file: **（无法创建文件）** 当以只读模式登录并尝试在安全数据分区中创建文件或文件夹时，会出现此错误消息。	 **图 9.11：“无法创建文件”错误**
Error copying file or folder: **（复制文件或文件夹时出错）** 当以只读模式登录并尝试向安全数据分区复制文件或文件夹时，会出现此错误消息。	 **图 9.12：“复制文件或文件夹出错”错误**
Error deleting file or folder: **（删除文件或文件夹时出错）** 当以只读模式登录并删除安全数据分区中的文件或文件夹时，会出现此错误消息。	 **图 9.13：“删除文件或文件夹出错”错误**

注意：如果您在只读模式下登录，并且希望解锁设备以获得完全的读/写权限来访问安全数据分区，则必须关闭 D500S 并重新登录，在登录之前取消选中“Read-Only Mode”（只读模式）复选框。

设备使用（Linux 环境）

如今有众多的 Linux 发行版可供使用，各版本界面的“外观”

可能各不相同。不过，终端应用程序中使用的一般命令集都十分类似，可以在后面的 Linux 指令中引用。该部分中的屏幕快照示例在 64 位环境下生成。

某些 Linux 发行版需要超级用户 (root) 权限才能在终端应用程序窗口中正确执行 D500S 命令。

继续前的重要提示：

1.) **D500S 不支持 Linux 上的设备初始化，需要在支持的 Windows 或 macOS 系统上设置和配置，然后才能在 Linux 上使用闪存盘。**

2.) **Linux 登录仅支持使用复杂密码。Linux 登录不支持密码短语密码。**

3.) **Linux 上的 D500S 功能支持受限。Linux 不支持一次性恢复密码、加密擦除密码、管理员/用户密码重置和切换只读模式等功能。**

D500S 带有 4 条可用于 Linux 的命令：

lkd500s_about	显示“关于 D500S”信息。
lkd500s_login	允许您登录到闪存盘。
lkd500S_logout	允许您安全地注销 D500S 闪存盘。
lkd500S_resetdevice	执行设备加密擦除并将驱动器重置为开箱即用状态，永久删除驱动器上存储的所有数据和文件。

注意：要执行这些命令，您必须打开“终端”应用程序窗口并导航至各文件所在的文件夹。每条命令前都必须加上以下两个字符：./’（一个点和一个正斜杠。）

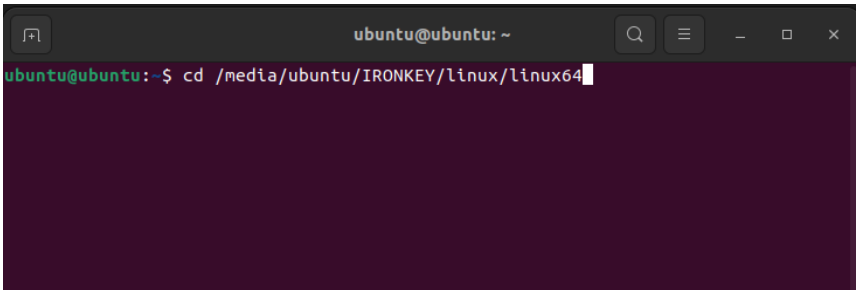
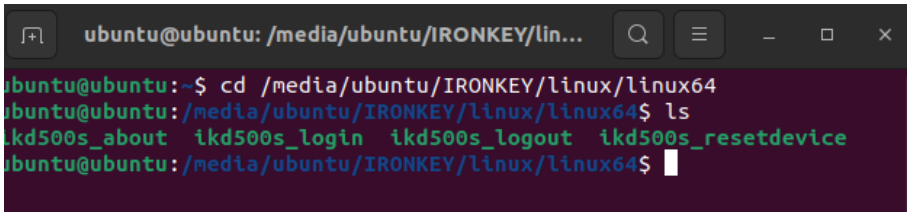
如何导航到 IronKey Linux 命令路径的示例：

对于 32 位 Linux 用户：	打开“终端”应用程序窗口，并在提示符下键入以及命令， **cd /media/ubuntu/IRONKEY/linux/linux32** 将当前目录切换到 **/media/ubuntu/IRONKEY/linux/linux32$** 然后按 ENTER。）
对于 64 位 Linux 用户：	打开“终端”应用程序窗口，并在提示符下键入以及命令， **cd /media/ubuntu/IRONKEY/linux/linux64** 将当前目录切换到 **/media/ubuntu/IRONKEY/linux/linux64$**（然后按 ENTER。）

设备使用（Linux 环境）

注意：如果操作系统没有自动加载 IRONKEY 卷，那么您需要在终端窗口中使用‘Linux mount’命令手动加载卷。有关具体的操作系统发行版，请参见 Linux 文档；有关正确的语法和命令选项，请参见常用的在线支持网站。一些 Linux 发行版可能要求您输入用户名来运行命令，例如上面示例中的“ubuntu”。

找到并查看 IronKey D500S Linux 命令文件：

将 D500S 连接到计算机并被操作系统识别后，在终端提示下键入命令，将目录切换到 D500S 卷。（*图 10.1*） **注意：**该部分的屏幕快照和指令使用 linux64 文件夹（表示 64 位）来演示 D500S 设备在 Linux 操作系统下的使用情况。请记住，如果您使用 32 位版本的 Linux，只需导航至并使用相应的 32 位文件夹来替代 64 位文件夹，即使用 linux32 而不是 linux64。）	 **图 10.1：命令行导航**
在当前提示下使用 **ls** (list) 命令，然后按 ENTER 键。这将为您提供 linux64 文件夹中的文件和/或文件夹列表。 然后，您将看到列出的四个 IronKey Linux 命令（*图 10.2*） • ikD500S_about • ikD500S_login • ikD500S_logout • ikD500S_resetdevice	 **图 10.2：查看 IronKey Linux 命令文件**

注意：命令和文件夹（目录）名称区分大小写，即“linux64”与“Linux64”不同。必须严格按照图片所示来键入语法。）一些 Linux 发行版可能要求您输入用户名来运行命令，例如本例中的“ubuntu”。

设备使用（Linux 环境）

使用 D500S 命令

关于 D500S

IkD500S_about（关于 D500S，*图10.3*）

此命令将填充有关 D500S 的信息，例如：

- 厂商
- 产品
- D500S 序列号
- 固件版本
- 软件版本

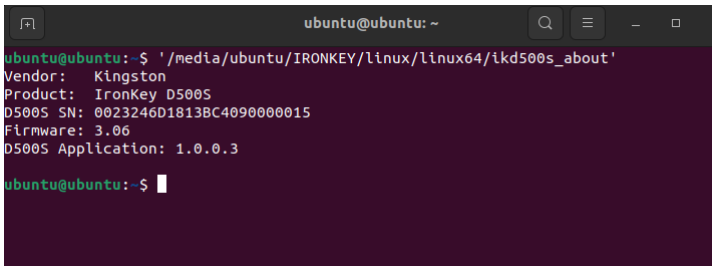


图 10.3：ikD500S_about（关于 IronKey D500S）

D500S 登录

ikD500S_login

在受支持的 Windows 或 macOS 系统上初始化 D500S 后，您可以使用您创建的 D500S 密码登录设备，访问安全数据分区。

为此，请执行以下步骤：

1. 打开“终端”应用程序窗口。

2. 在终端提示符下键入以下命令：**cd /media/ubuntu/IRONKEY/linux/linux64**

3. 现在，在 **/media/ubuntu/IRONKEY/linux/linux64$** 命令提示符下键入以下命令以登录到设备：**./ikD500S_login***，然后按 ENTER。（注意：命令和文件夹名称区分大小写，语法必须准确无误。此外，一些 Linux 发行版可能要求您输入用户名来运行命令，例如本例中的“ubuntu”。）

4. 成功登录后，安全数据卷将在您的桌面上打开，您可以继续使用 D500S（有关登录行为的更多信息，请参阅下一页）

*注意：某些 Linux 发行版需要超级用户 (root) 权限才能在终端应用程序窗口中正确执行 D500S 命令。

设备使用（Linux 环境）

D500S 登录（续）

IkD500S_login（解锁 D500S，*图 10.4*）

根据闪存盘的设置方式，在登录过程中，您可能会看到许多关于如何解锁闪存盘的选项。

如果在初始化期间启用了**管理员/用户密码**配置文件，则会向您显示以下登录选项：

1.) 选择以管理员或用户身份登录
2.) 选择解锁管理员分区或用户分区（如果已启用）
3.) 输入相应的管理员或用户登录密码以进行设备身份验证和解锁。

注意：如果在初始化过程中未启用管理员/用户密码配置文件（仅用户模式），则只会提示您只输入设备密码进行设备身份验证。

重要事项：如前所述，密码短语密码在 Linux 上不受支持，D500S 需要配置复杂密码以进行 Linux 登录（*图 10.5*）

图 10.4：ikD500S_login（解锁 D500S）

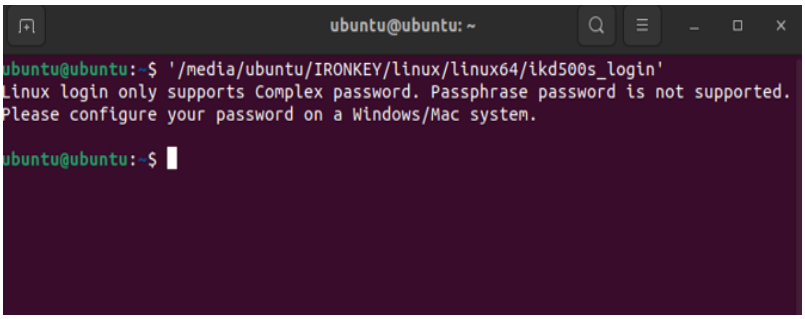


图 10.5：不支持的密码登录尝试。

设备使用（Linux 环境）

D500S 登录（续）

登录密码行为不正确

在登录过程中，如果输入的密码不正确，您将有另一次机会输入密码。但是，有一个内置的安全功能可以跟踪失败的登录尝试次数。如果此数字达到管理员或用户登录的预先配置的 10 次失败尝试值，则行为如下：

管理员/用户密码已启用

- **用户登录：**用户锁定，需要以管理员身份登录。（*图 10.6*）注意：在支持的 Windows 或 macOS 系统上，管理员登录可以重置用户密码。
- **管理员登录：**闪存盘加密擦除，所有数据将永远丢失。需要重置设备。（*图 10.7*）

仅用户模式（管理员/用户未启用）

- **用户登录：**闪存盘加密擦除，所有数据将永远丢失。需要重置设备。（*图 10.7*）

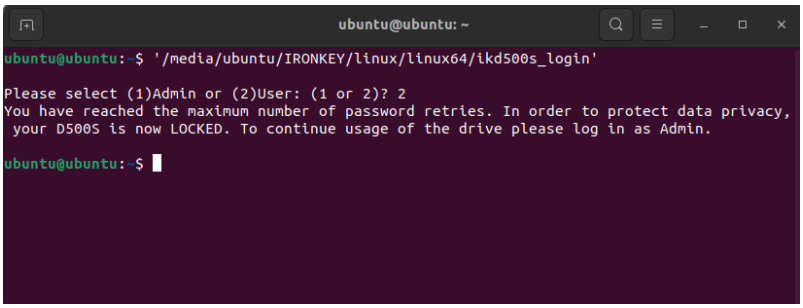


图 10.6：用户登录锁定，管理员/用户密码已启用

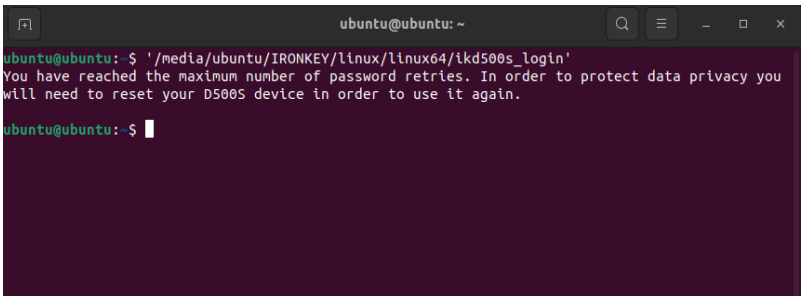


图 10.7：达到最大尝试次数（闪存盘重置）

D500S 注销

IkD500S_logout（锁定设备）

使用完 D500S 之后，注销设备并保护您的数据。为此，请按照第 39 页中引用的相同步骤进行操作，并正确使用以下命令注销设备：**./ikD500S_logout**，然后按 ENTER（注意：命令和文件夹名称区分大小写，语法必须准确无误。（*图 10.8*）

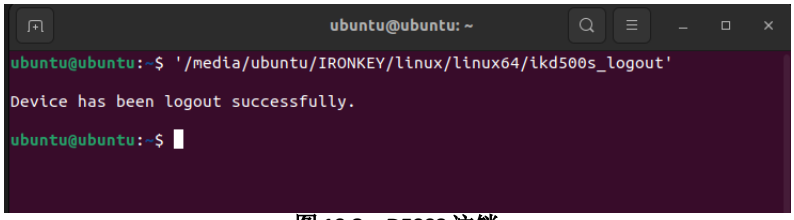


图 10.8：D500S 注销

设备使用（Linux 环境）

D500S 设备重置

ikD500S_resetdevice

如前面第 41 页所述，如果忘记了用户/管理员密码，可以使用“重置设备”命令重置驱动器，以便再次使用。此过程将允许您创建新密码，但为了保护您的数据隐私，D500S 将加密擦除闪存盘，格式化安全数据分区。**这意味着您的所有数据都将丢失。**

要使用重置设备命令，请按照第 39 页中引用的相同步骤进行操作，并正确使用以下命令注销设备：**./ikD500S_resetdevice**，然后按 ENTER（注意：命令和文件夹名称区分大小写，语法必须准确无误。（*图 10.9*）

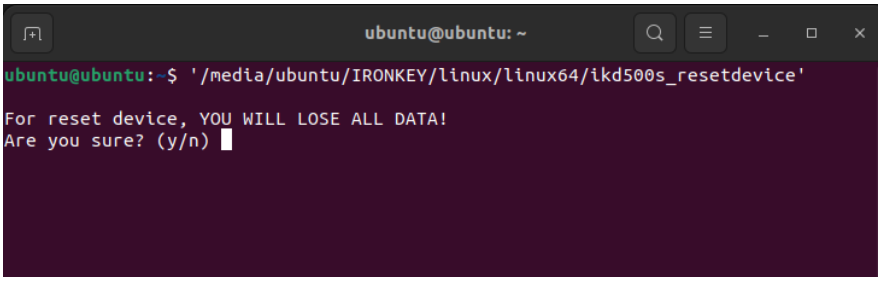


图 10.9：重置设备命令

使用“重置设备”命令后，系统将提示您创建一个新的复杂密码，该密码必须包含：

- 8-16 个字符，并且至少包含以下 3 种字符：
  - -大写
  - -小写
  - -数字
  - -特殊字符（!、$ 等）

（*图 10.10*）

注意：“重置设备”命令将在“仅用户”模式（单个密码，单个用户）下初始化闪存盘。要启用管理员/用户登录密码配置文件，需要在支持的 Windows 或 macOS 系统上设置 D500S 才能访问该选项。

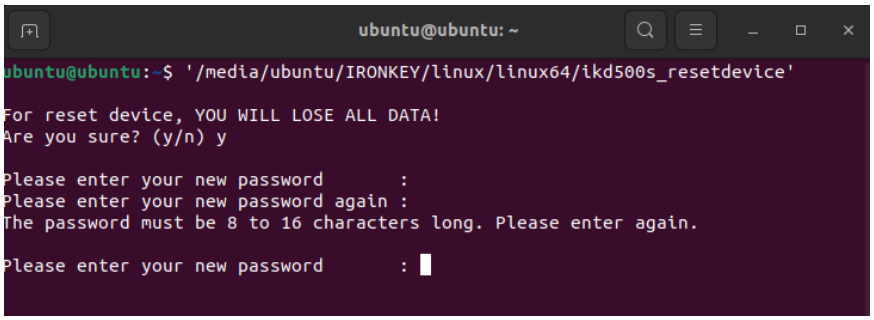


图 10.10：重置设备命令，密码创建

IRONKEY™ D500S
高安全性 USB 3.2 Gen 1 隨身碟
使用者指南

目錄

圖 1：IronKey D500S

簡介

Kingston IronKey D500S 是一款軍用級安全性 USB 隨身碟，具有多項 IronKey 備受推崇的功能以保護機密資料。IronKey D500S 符合 FIPS 140-3 Level 3 (認證申請中)，具備新的 NIST 強化功能，以升級的安全性微處理器提供強大的安全性。資料會在 D500S 上進行加密和解密，不會在主機系統上留下痕跡，可免受記憶體中密碼窺測程式的影響。除了 XTS-AES 256 位元硬體型加密，D500S 還具備堅固的鋅製外殼，能防水*、防塵*、抗壓，並以環氧樹脂密封，可防護內部零組件免受滲透攻擊。
D500S 支援傳統複雜密碼或密碼短語模式的多重密碼 (管理員、使用者、一次性恢復和加密清除) **。若忘記其中一個密碼，多重密碼功能可提高恢復存取資料的能力。除了支援傳統的複雜密碼外，密碼短語模式還允許輸入數字 PIN 碼、句子、字詞列表，甚至是 10 到 128 個字元長度的歌詞。管理員可啟用使用者檔案、建立自訂大小的雙資料分區 (可用來分別存放管理員/使用者登錄檔)、啟用一次性恢復密碼和加密清除用密碼，以及重設使用者密碼等，來恢復存取資料權限。

輸入密碼時，點選「眼睛」 符號就能顯示輸入的密碼，避免打字錯誤導致登入失敗。為了讓您更加安心，D500S 還使用數位簽章韌體，能防護 BadUSB 惡意軟體和不斷猜測密碼的暴力密碼破解攻擊。暴力密碼破解防護會在連續輸入錯誤的密碼 10 次後，將使用者或是一次性恢復密碼鎖定，如果連續輸入錯誤的管理員密碼 10 次後，就會加密清除磁碟。
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，內建的虛擬鍵盤可防範密碼側錄器和螢幕側錄器記錄密碼***。

中小型企業可利用管理員角色在本機管理其隨身碟，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，並遵循法律法規在需要取證時提供使用。

D500S 提供多種客製化選項，符合 TAA/CMMC 標準，並於美國當地組裝。

D500S 享有 5 年有限產品保固及免費技術支援服務。

*請參考產品資料表規格。使用前須確保產品處於乾淨且乾燥的狀態。
**Linux 系統不支援密碼短語模式。
***虛擬鍵盤：Microsoft Windows 和 macOS 系統僅支援美式英語。

IronKey D500S 特色

- FIPS 140-3 level 3 (認證申請中) 的 XTS-AES 256 位元硬體加密 (加密功能永遠無法關閉)
- 暴力密碼破解與 BadUSB 攻擊保護
- 多重密碼選項
- 複雜密碼或密碼短語模式
- 獨特的雙重分區功能和加密清除用密碼
- 點選眼睛按鈕可顯示輸入的密碼，減少失敗登錄嘗試
- 虛擬鍵盤可幫助防範密碼側錄器和螢幕側錄器
- 強制/階段性唯讀 (寫入保護) 設定可防止隨身碟內容遭到變更或受到惡意軟體的侵害
- 中小型企業可以使用管理員角色在本地管理隨身碟
- 與 Windows、macOS 和 Linux 相容 (詳情請查詢產品資料表)

關於本使用手冊

此使用者手冊所涵蓋的 IronKey D500S 內容，係依據非客製化的出廠版本而撰寫。

系統需求

PC 平台 • Intel、AMD & Apple M1 SOC • 15 MB 可用磁碟空間 • 可用的 USB 2.0：3.2 連接埠 • 最後一個實體磁碟後的兩個連續磁碟機代號* ***注意：**請參閱第 35 頁「磁碟機代號衝突」。	**PC 作業系統支援** • Windows 11 • Windows 10
Mac 平台 • 15 MB 可用磁碟空間 • USB 2.0：3.2 連接埠	**Mac 作業系統支援** • macOS macOS 11.x - 14.x
Linux 平台 • 5MB 可用磁碟空間 • USB 2.0：3.2 連接埠	**Linux 作業系統支援** • Linux Kernel v4.4+

建議

為確保 D500S 裝置具備足夠的電源供應，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 D500S 連接至任何具有 USB 連接埠的週邊設備 (如鍵盤或 USB 供電的集線器)，如***圖 1.2*** 所示。

圖 1.1：建議的使用方式

圖 1.2：不建議的使用方式

使用適合的檔案系統

IronKey D500S 預設格式化為 FAT32 檔案系統。適用於 Windows、macOS 和 Linux* 系統。但是，還有一些手動格式化磁碟的選項，例如 Windows 的 NTFS 和 exFAT。如果需要，您可以重新格式化資料分區，但注意重新格式化後會失去儲存其中的資料。

使用提醒

為確保您的資料安全，Kingston 建議您：

- 在目標系統上設定和使用 D500S 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，這有助於防護隨身碟免受惡意軟體的侵害
- 不使用時將裝置鎖定
- 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。可能損壞隨身碟並需要重新格式化，您的資料會被刪除
- 切勿將您的裝置密碼告訴任何人

尋找最新更新版本和相關資訊

造訪 kingston.com/support 以獲得最新的隨身碟更新版本、常見問答集、文件和其他資訊。

注意：如果隨身碟有更新，請務必升級至最新版本。我們不支援將您的磁碟降級為較舊的軟體版本，這可能會導致儲存資料丟失，或者損害磁碟的其他功能。如果您有任何問題或疑慮，請聯絡 Kingston 技術支援。

*** D500S 不支援 Linux 中開箱即用初始化功能，需要先在有支援的 Windows 或 macOS 系統上執行完整初始化和設定，才能在 Linux 中使用該隨身碟。本使用者手冊第 37 頁的 Linux 段落可找到更多資訊。**

最佳密碼設定做法

您的 D500S 具備強大的安全防護。其中包括針對暴力密碼破解的保護，只能嘗試輸入密碼10 次，藉此阻止攻擊者猜測密碼。達到隨身碟密碼嘗試次數上限時，D500S 將自動清除加密資料，將自身格式化並恢復到出廠設定。

多重密碼

D500S 支援多重密碼這項主要功能，有助於避免忘記一個或多個密碼時導致資料遺失。啟用所有密碼選項後，D500S 可支援三種不同種類的密碼來還原資料，分別是管理員密碼、使用者密碼和一次性恢復密碼。

D500S 允許您選擇管理員密碼和使用者密碼這兩種主要密碼。管理員是類似超級使用者的角色，能隨時存取磁碟，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，針對使用者提供登入和重設使用者密碼的方式。

使用者也能存取磁碟，但權限比管理員低。如果您忘記了這兩個密碼中的其中一者，則可以使用另一組密碼來存取並取回資料。並將磁碟設定為具備兩組密碼。儘管只使用使用者密碼，但請務必切記設定好兩組密碼，並且將管理員密碼存放在安全位置。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 建議同時將這些資料儲存到其他媒體裝置上。D500S 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

D500S 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 8-16 個字元的要求，並且至少使用 3 個下列字元：

- 大寫字母字元
- 小寫字母字元
- 數字
- 特殊字元

密碼短語

D500S 支援 10 到 128 個字元的密碼短語。密碼短語沒有規則，但使用正確的話，可以提供完善的保護。

密碼短語基本上是字元的任意組合，包括其他語言的字元。與 D500S 隨身碟一樣，密碼短語可與隨身碟所選擇的語言相符。這能讓您使用多個單字、一個短語、歌曲中歌詞和一行詩歌等，強大的複雜密碼是攻擊者最難猜到的密碼類型之一，而且使用者相對好記。

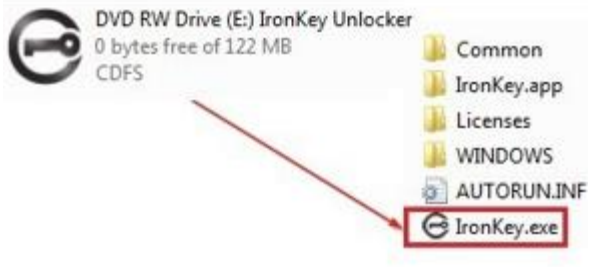
設定我的裝置

為確保 IronKey 加密 USB 隨身碟具有足夠的電源供應，請將其直接插入筆記型電腦或桌上型電腦的 USB 2.0/3.0 連接埠。避免將其連接到具有 USB 連接埠的任何週邊設備，例如鍵盤或 USB 供電的集線器。裝置初始設定必須在支援 Windows 或 macOS 的作業系統上完成。

裝置存取 (Windows 系統)

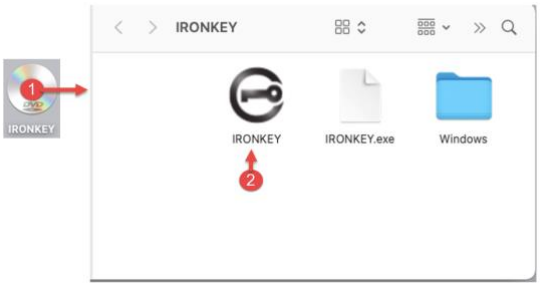
將 IronKey 加密 USB 隨身碟插入筆記型電腦或桌上型電腦上的可用 USB 連接埠，然後等待 Windows 偵測到它。

• Windows 10/11 使用者會接收到裝置驅動程式通知。(*圖 3.1*)	 **圖 3.1：裝置驅動程式通知**

• 新的硬體偵測完成後，請在檔案總管中找到未鎖定分割區，並選取 **IronKey.exe** 選項。(*圖 3.2*) • 請注意，分割區代號將依照下一個可用磁碟機代號而有所不同。磁碟機代號會依據所連接的裝置而變動。在下圖中，磁碟機代號為 (E:)。	 **圖 3.2：Window 檔案總管/IronKey.exe**

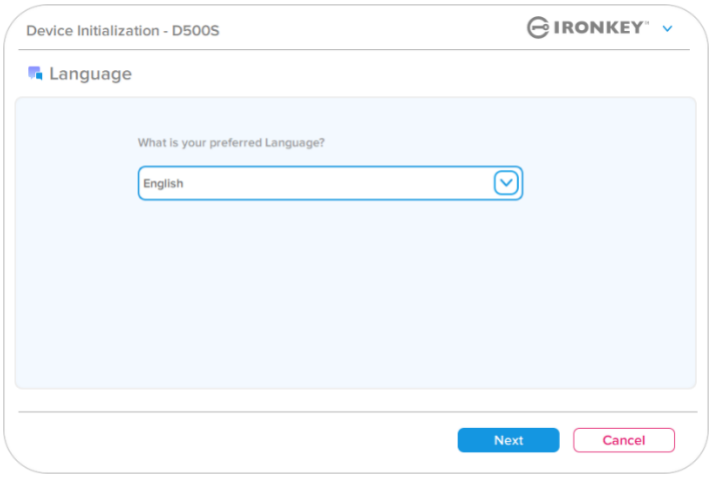
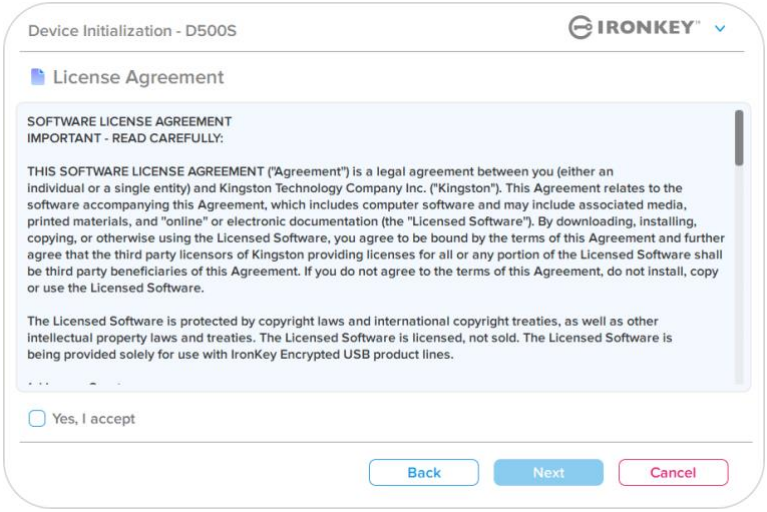
裝置存取 (macOS 系統)

將 D500S 插入至筆記型電腦或桌上型電腦上的 USB 連接埠，或是由 Mac 作業系統自動偵測。完成後，您會在桌面看見「IRONKEY」卷宗。(*圖 3.3*)

• 連按兩下 IronKey CD-ROM 圖示 • 接著在圖 3.3 顯示視窗中連按兩下 IronKey.app 應用程式圖示。接著會啟動初始化流程。	 **圖 3.3：IronKey 卷宗**

裝置初始化 (Windows & macOS 系統)

語言和 EULA

從下拉式選單中選擇語言偏好，然後按「**下一步**」。(*圖 4.1*)	 **圖 4.1：語言選擇**
檢閱授權合約，然後按「**下一步**」。 **注意：**您必須先接受授權合約才能繼續，否則「**下一步**」按鈕將處於停用狀態。 (*圖 4.2*)	 **圖 4.2：授權合約**

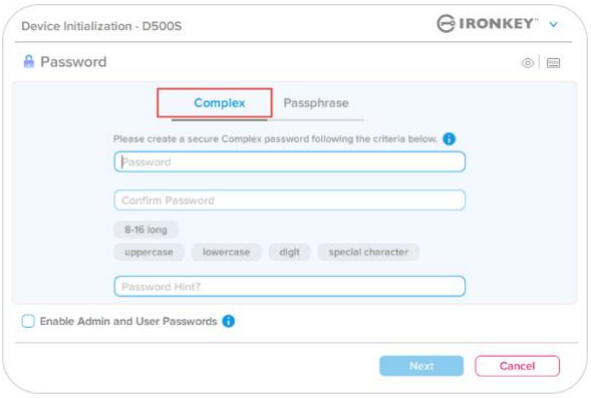
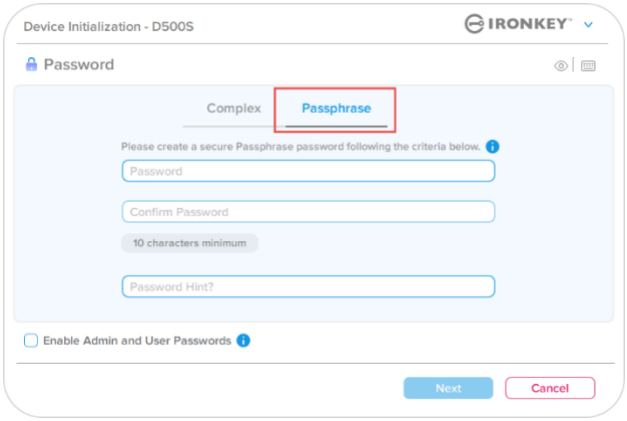
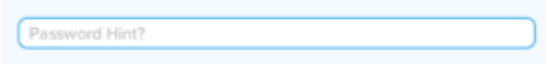
裝置初始化

密碼選擇

在密碼提示畫面上，可使用複雜密碼或密碼短語模式建立密碼，以保護 D500S 中的資料 (*圖 4.3-4.4*)。此外，還可以在此畫面上啟用多重密碼管理員/使用者選項。在繼續密碼選擇流程之前，請查看下面的「啟用管理員/使用者密碼」以便詳細了解這些功能。

注意：一旦選擇複雜密碼或密碼短語模式，除非重設裝置，否則無法變更模式。

要開始密碼選擇流程，請在「密碼」欄位中建立您的密碼，然後在「確認密碼」欄位重新輸入。您建立的密碼必須符合下列條件，系統才會讓您繼續初始化流程：

複雜密碼 • 必須包含 8 個以上的字元 (最多 16 個字元)。 • 必須包含下列三 (3) 種字元： ○ 大寫 ○ 小寫 ○ 數字 ○ 特殊字元 (!、$、& 等)	 **圖 4.3：複雜密碼**
密碼短語 • 必須包含： ○ 最少 10 個字元 ○ 最多 128 個字元	 **圖 4.4：密碼短語**
密碼提示 (可選) 如果您忘記密碼，密碼提示可提供有關密碼內容的線索。 **注意：**提示「不得」與密碼完全相符。	 **圖 4.5：密碼提示欄位**

裝置初始化

有效與無效的密碼

如果是**有效**的密碼，在條件符合時，「密碼條件方塊」會顯示綠色。(詳見*圖 4.6a-b*)

注意：一旦符合三個密碼條件的最低限度，第四個條件方塊將變為灰色，表示此為非強制條件。(*圖 4.6b*)

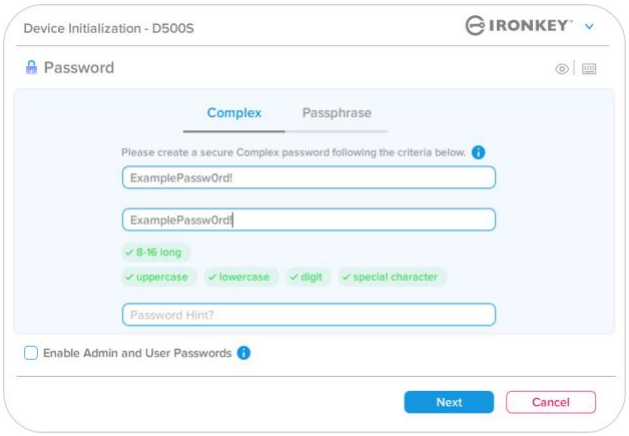


圖 4.6a：符合複雜密碼條件

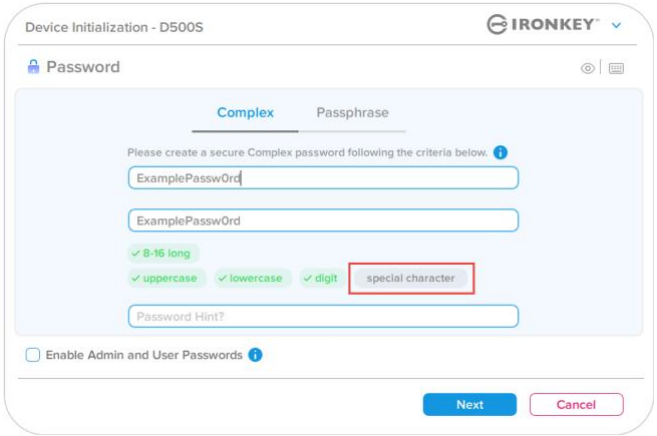


圖 4.6b：選用複雜密碼條件

如果是**無效**的密碼，「密碼條件方塊」會顯示紅色，同時會停用「**下一步**」按鈕，直到符合最低條件為止。

此情況適用於複雜密碼與密碼短語。

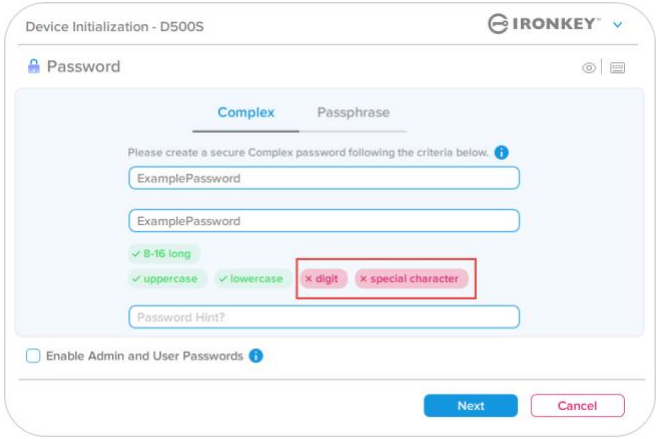


圖 4.7：密碼條件不符

裝置初始化

虛擬鍵盤

D500S 具備可防護密碼側錄器的虛擬鍵盤。

- 若要利用**虛擬鍵盤**，請在**裝置初始化**畫面的右上角找到鍵盤按鈕然後加以選取。

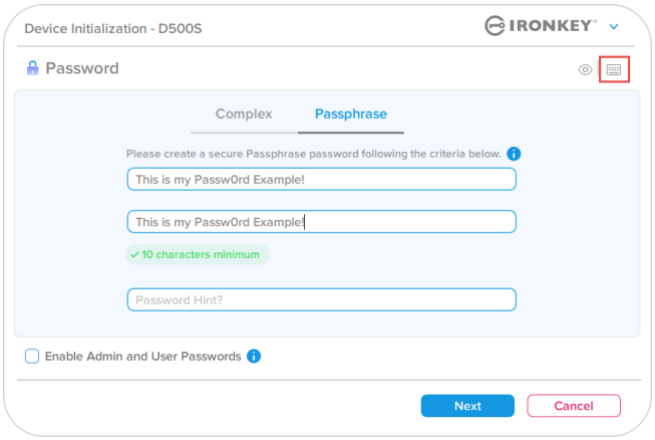


圖 4.8：啟用虛擬鍵盤

- 出現虛擬鍵盤後，您還能啟用**螢幕側錄器防護**。在使用此功能時，所有按鍵將短暫反白。此為預期中的效果，可避免螢幕側錄器擷取您所點選的內容。
- 若要進一步加強此功能，您還可以選擇鍵盤右下角的**隨機**顯示，讓虛擬鍵盤上的字元隨機排列。隨機排列將隨機排列鍵盤位置。

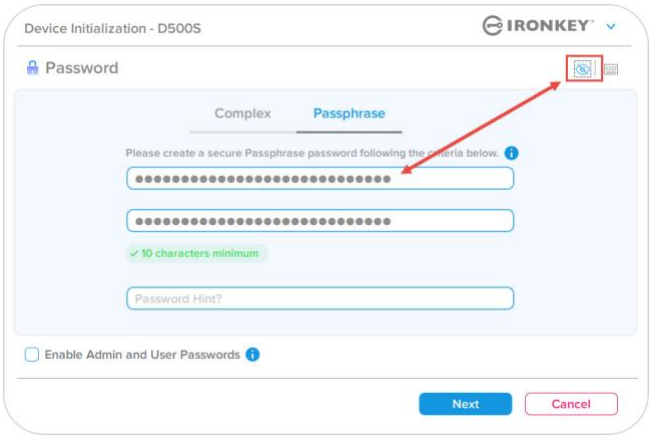
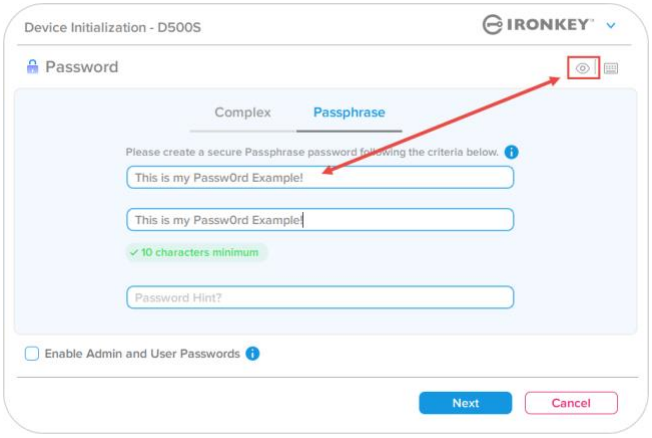
圖 4.9：螢幕側錄器防護/隨機排列

裝置初始化

密碼顯示切換

依預設，當您建立密碼時，密碼字串在輸入時顯示在欄位中。如果您想要在輸入時隱藏密碼字串，可以切換位於裝置初始化視窗右上角的密碼眼睛符號，隱藏密碼字串。

注意：在裝置初始化之後，密碼欄位將預設為「隱藏」。

若要**隱藏**密碼字串，請按一下灰色圖示。 	 **圖 4.10：切換隱藏的密碼**
若要**顯示**隱藏的密碼，請按一下藍色圖示。 	 **圖 4.11：切換顯示的密碼**

裝置初始化

管理員和使用者密碼

啟用「管理員和使用者密碼」，您可以利用多重密碼功能，使管理員角色者可以利用此功能管理兩個帳戶。選擇**「啟用管理員和使用者密碼」**，即允許在忘記其中一個密碼的情況下，使用另一個密碼存取隨身碟。

在**管理員和使用者密碼**啟用的情況下，您也可以：

- 雙重分區設定
- 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
- 強制重設使用者登入的密碼
- 加密清除用密碼

若要了解關於這些功能的詳細資訊，請瀏覽本使用者指南第 25 頁。

- 若要啟用**管理員和使用者密碼**，請按一下**「啟用管理員和使用者密碼」**旁邊的方塊，然後在完成選擇有效密碼之後選取**「下一步」**。(*圖 4.12*)
- 若已**啟用**本功能，則在此畫面中選擇的密碼就會是**管理員密碼**。按**「下一步」**並前進至**「使用者密碼」**畫面，可在此畫面中選擇使用者密碼。

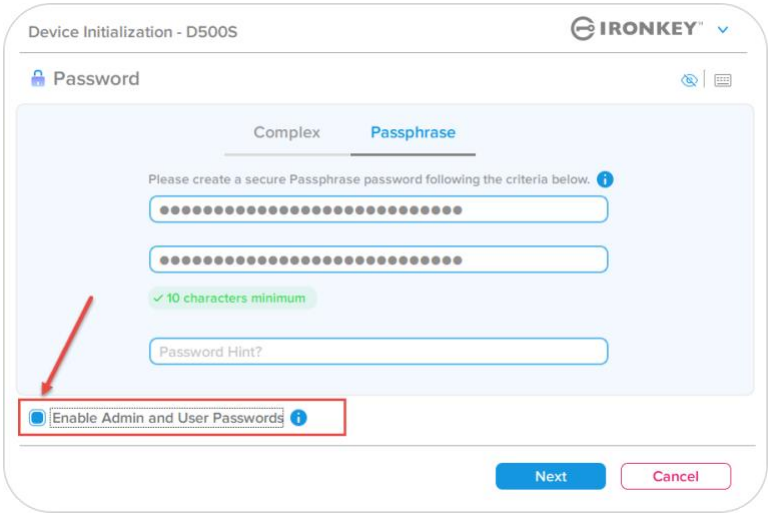


圖 4.12：啟用管理員和使用者密碼

注意：啟用管理員和使用者密碼為選用功能。

如果已經設定隨身碟但未啟用此功能 (方塊取消核取)，則會將隨身碟設定為**「單一使用者/單一密碼」**隨身碟，而且**不擁有任何管理員功能**。在本手冊當中，此設定也被稱為**單一使用者模式**。

若要繼續**「單一使用者/單一密碼」**設定，請將「啟用管理員和使用者密碼」維持取消核取，然後在建立有效的密碼之後，按**「下一步」**。

注意：在本文件的其他部分，**管理員和使用者密碼**將稱為**管理員角色**。

裝置初始化

管理員和使用者密碼

- 如果已經在上一個畫面中**啟用**管理員角色，則後續畫面會提示輸入使用者密碼 (*圖 4.13*) 與管理員密碼相比，**使用者密碼**在功能上會受到限制，本使用者指南會在稍後討論更多細節 (請見第 23 頁)

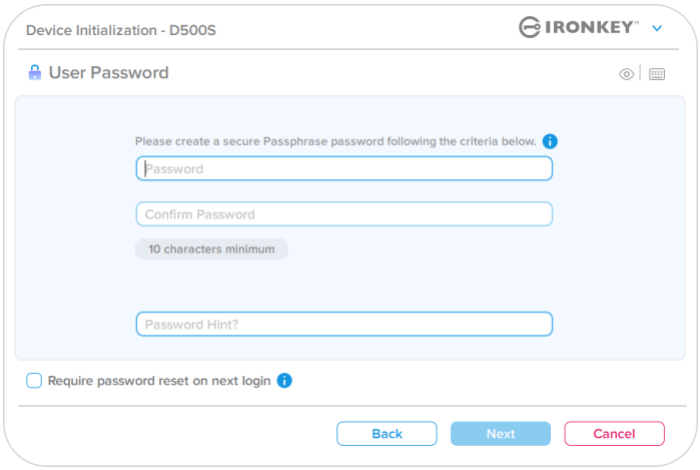


圖 4.13：使用者密碼 (管理員與使用者已啟用)

注意：選擇的「密碼選項」(複雜密碼或密碼短語) 條件會延續至使用者密碼、一次性密碼恢復、加密清除用密碼，以及在設定隨身碟後需要進行的任何密碼重設。選擇的密碼選項僅可在完整裝置重設後方可變更。

- **下次登入時需重設密碼**功能 (位於圖 4.13 的左下角) 僅適用於使用者密碼，這個功能啟用後，可在初始化過程中使用管理員設定的暫時密碼強制使用者登入，然後在使用暫時密碼驗證隨身碟之後，將密碼變更為使用者自訂的密碼。如果隨身碟會提供給其他人使用，這個功能會很有用。(*圖 4.14*)

  注意：為安全起見，新的密碼不可以和暫時密碼相同。

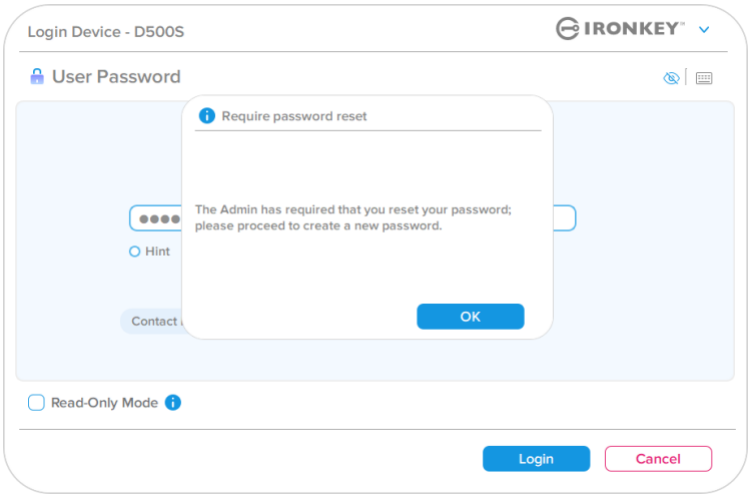


圖 4.14：下次登入時需重設密碼 (用於使用者密碼)

裝置初始化

雙重分區

IronKey D500S 可針對管理員和使用者建立兩個自訂大小的安全分區。如果啟用此功能，以管理員登入時將有權限存取使用者分區**和**管理員分區，但以使用者登入時**僅**能存取使用者分區。對於在管理員和使用者之間安全地分別存放資料和檔案的存取權限，此功能十分實用，也能用來啟用隱藏檔案儲存功能，防止在不受信任的系統上曝露不必要的檔案。如果需要，還能調整管理員和使用者之間的分區大小。

注意：此為*可選*功能，可以在設定流流程中，取消選取「啟用雙重分區」核取方塊，來停用此功能 (*圖 4.15*)。

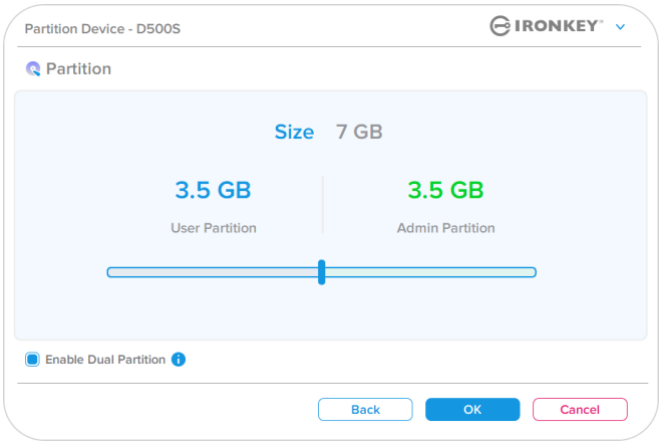


圖 4.15：裝置分區

如要調整並分配管理員和使用者之間的分區大小，請向左或向右移動滑桿 (*圖 4.16*)。

- 調整分區大小時能以 0.5GB 的尺寸增加。
- 分區大小和隱藏分區中可用總儲存容量有關。
- 管理員和使用者之間的分區大小預設為平均分配，可使用滑桿調整。
- 最小可分配區域為 1GB。

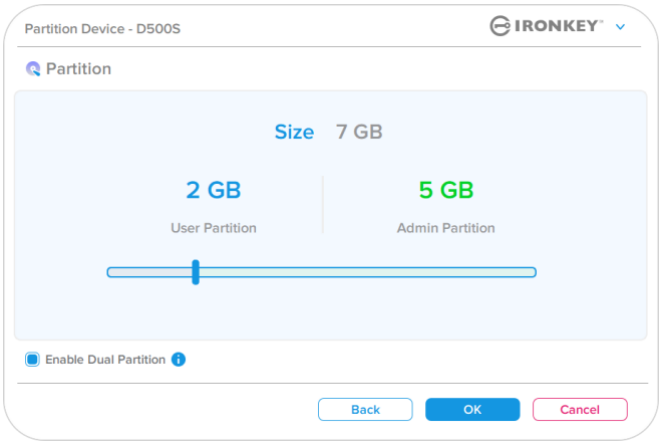


圖 4.16：裝置分區，以滑桿調整

管理員登入

啟用雙重分區並完整設定好後，以管理員登入時會顯示一個選項，每次成功登入時可用來解鎖隨身碟，並存取管理員或使用者分區。(*圖 4.17*)

注意：一次只能開啟一個分區。不能同時解鎖使用者分區和管理員分區。

以使用者登入時不會顯示此選項，只會解鎖使用者分區。

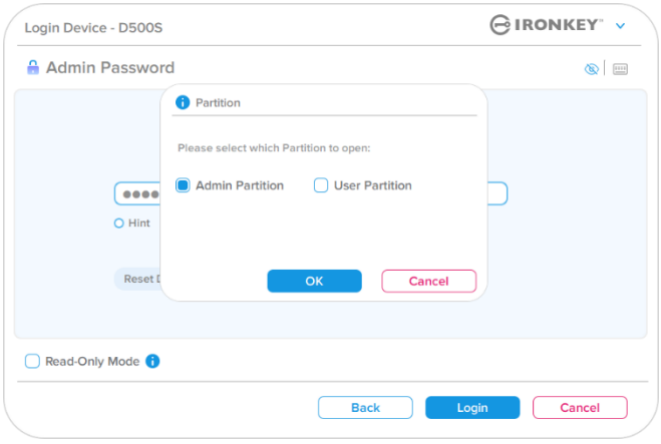


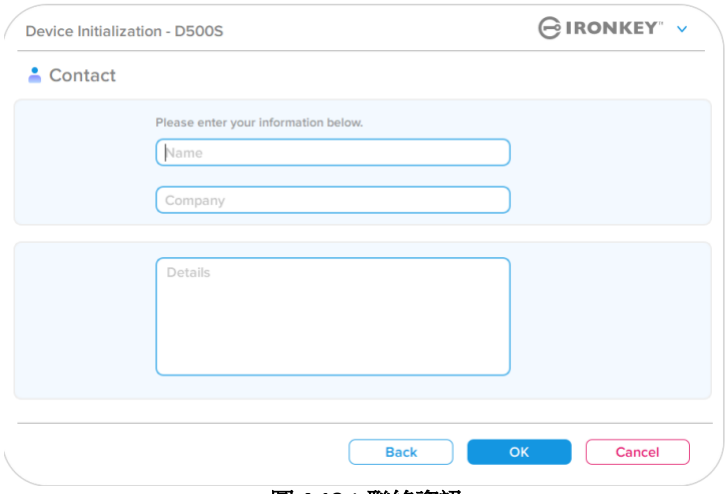
圖 4.17：以管理員登入並選擇分區的操作範例。

裝置初始化

聯絡資訊

在顯示文字方塊中輸入您的聯絡資訊 (*圖 4.18*)

注意：您在這些欄位中輸入的資訊可能並未包含您在步驟 3 中建立的密碼字串。但這些是可選填欄位，如果必要可以留空。

「名稱」欄位可包含多達 32 個字元，但不得包含**確切**密碼。 **「公司」**欄位可包含多達 32 個字元，但不得包含**確切**密碼。 **「詳細資訊」**欄位可包含多達 156 個字元，但不得包含**確切**密碼。	 **圖 4.18：聯絡資訊**

注意：按一下「確定」，將完成初始化過程並繼續解鎖，然後安裝可以在其中安全地儲存資料的安全分割區。拔下隨身碟並將其重新插回系統以查看反映的變更。

裝置使用 (Windows & macOS 系統)

管理員和使用者登入 (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 D500S 應用程式將啟動，並且先提示使用者密碼登入畫面。您可以利用「使用者密碼」在此處登入，查看輸入的任何聯絡資訊，或是以管理員身分登入 (*圖 5.1*)。按一下「以管理員身分登入」按鈕 (如下所示)，應用程式會繼續「管理員登入」選單，您可以在此處以管理員身分登入，存取管理員設定與功能 (*圖 5.2*)。

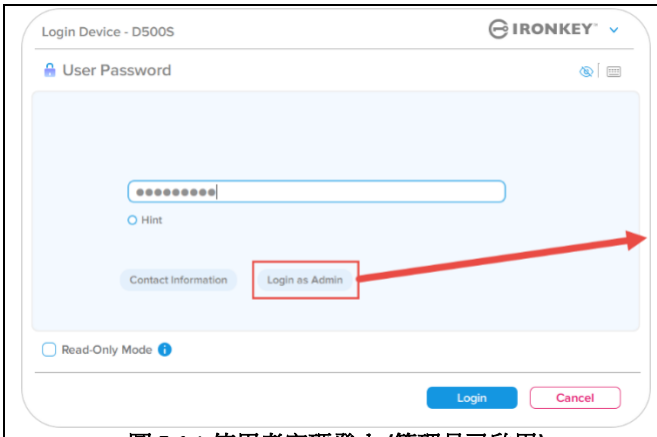


圖 5.1：使用者密碼登入 (管理員已啟用)

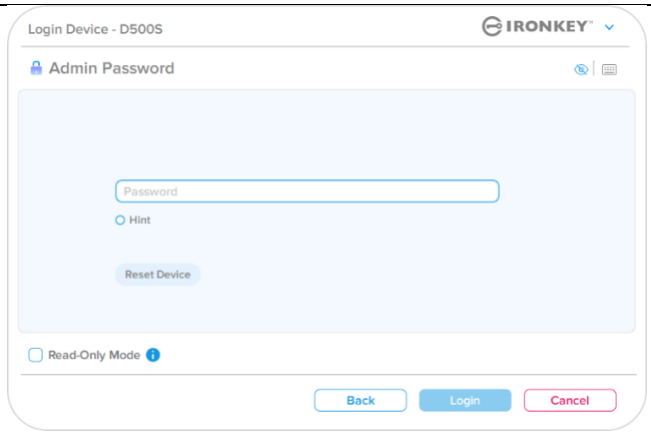


圖 5.2：管理員密碼登入

單一使用者登入模式 (管理員未啟用)

正如先前所提，儘管建議使用「管理員角色」功能，來獲得裝置的完整功能，但還是可以在單一使用者模式 (單一密碼/單一使用者) 初始化 IronKey 隨身碟。對於想用簡單的單一密碼方法來保護隨身碟資料的人來說，這可說是一個選擇。(*圖 5.3*)

注意：若要啟用管理員與使用者密碼，請使用「**重設裝置**」按鈕將隨身碟回復至初始化狀態，您可以在此狀態中啟用管理員與使用者密碼。**進行重設裝置時，隨身碟中的所有資料將進行格式化並且永久遺失。**

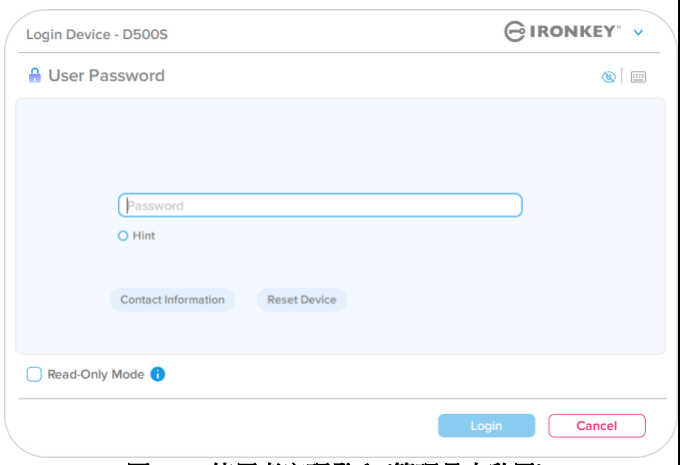


圖 5.3：使用者密碼登入 (管理員未啟用)

裝置使用

唯讀模式下解鎖

您可以在唯讀狀態下解鎖裝置，可禁止變更 IronKey 隨身碟上的檔案。例如，使用不受信任或未知的電腦時，以唯讀模式解鎖裝置，可避免該電腦上的任何惡意軟體感染您的裝置，或修改您的檔案。

在此模式下運作時，您無法執行任何涉及修改裝置上檔案的操作。
例如，您無法重新格式化裝置，還原、新增或者編輯隨身碟上的檔案。

以唯讀模式解鎖裝置：

1. 將裝置插入電腦的 USB 連接埠，然後執行 **IronKey.exe** 檔案。
2. 在輸入密碼方塊下方選取**唯讀模式**。(*圖 5.4*)
3. 輸入您的裝置密碼，然後按一下「**登入**」。IronKey 現在會解鎖呈唯讀模式。

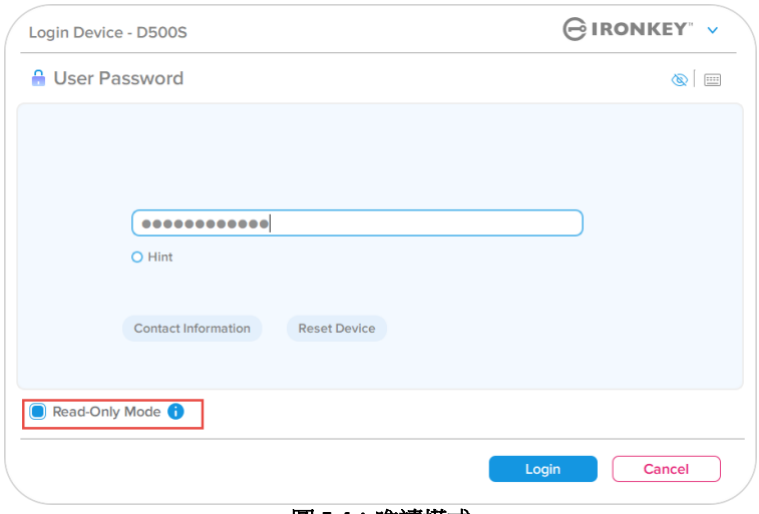


圖 5.4：唯讀模式

如果您想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 D500S 再重新登入，並且在登入前取消核取「唯讀模式」核取方塊。

注意： D500S 管理員選項可提供適用於使用者資料的強制唯讀模式，這表示管理員可在唯讀狀態中強制解鎖使用者登入 (詳情請參閱第 31 頁)。

裝置使用

暴力破解防護

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，磁碟會：

管理員/使用者啟用	**暴力破解保護 裝置動作 (10 次錯誤密碼嘗試)**	**資料清除與裝置重設？**
使用者密碼	密碼鎖定。以管理員身分登入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。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
單一使用者 單一使用者/單一密碼 (管理員/使用者未啟用)	**暴力破解保護 裝置動作 (10 次錯誤密碼嘗試)**	**資料清除與裝置重設？**
使用者密碼	加密清除隨身碟、密碼、設定以及資料永久清除	**是**

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

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，同時提供了強大「永遠啟動」的安全性。
提示：您也可以在 Windows 工作列中的 **IronKey** 圖示上按一下右鍵，然後按一下**瀏覽 D500S** 以存取您的檔案 (*圖 6.2*)。

裝置選項：(Windows 系統)

當您登入裝置時，視窗右上角會出現一個 IronKey 圖示。在 IronKey 圖示上按一下右鍵，會開啟選項選單，可選取可用的隨身碟選項 (*圖 6.2*)。有關這些裝置選項的詳細資訊，請參閱本手冊第 21-25 頁。

- 當您登入裝置時，視窗右上角會出現一個 IronKey 圖示。(*圖 6.1*)

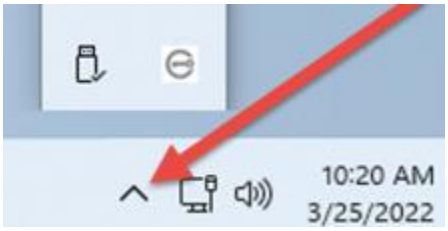


圖 6.1：工作列中的 IronKey 圖示

- 在 IronKey 圖示上按一下右鍵，會開啟選項選單，可選取可用的隨身碟選項 (*圖 6.2*)。

有關這些裝置選項的詳細資訊，請參閱本手冊第 19-23 頁

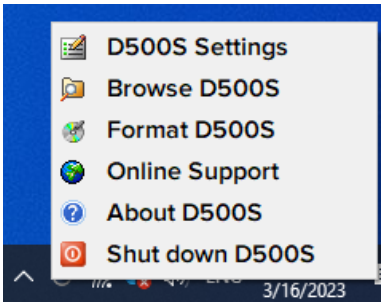


圖 6.2：在 IronKey 圖示按一下右鍵以顯示裝置選項

裝置選項：(macOS 系統)

- 在您登入裝置時， IronKey D500S 圖示位於 macOS 選單中 (如*圖 6.3* 所示)，在選單中可開啟可用的裝置選項。

有關這些裝置選項的詳細資訊，請參閱本手冊第 19-23 頁。

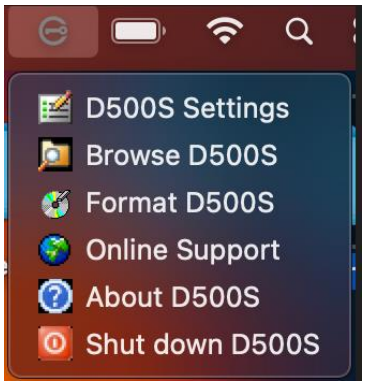
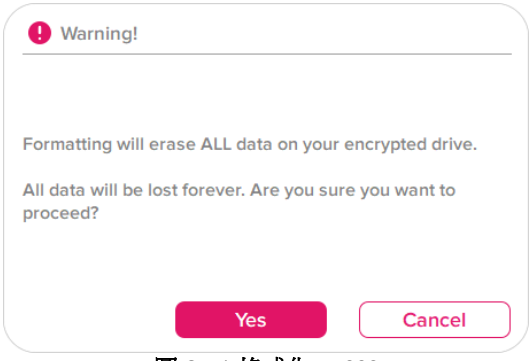
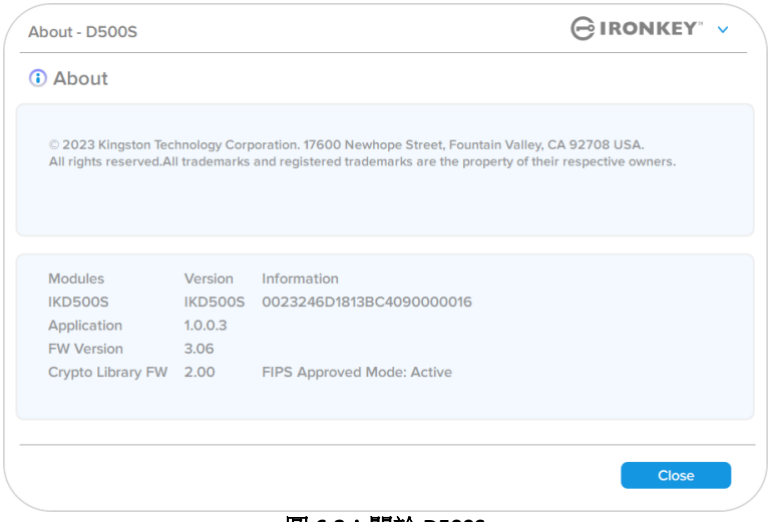


圖 6.3：macOS 選單列圖示/裝置選項選單

裝置選項

D500S 設定:	• 變更登入密碼、聯絡資訊以及其他設定。(有關裝置設定的更多詳細資訊，請參閱本手冊的「D500S 設定」一節)。
瀏覽 D500S：	• 可讓您安全地檢視自己的檔案。
格式化 D500S： 可讓您格式化安全資料磁碟分割區。(警告：會清除所有資料。) (*圖 6.1*) **注意：**格式化步驟需要密碼驗證。	 **圖 6.1：格式化 D500S**
線上支援：	• 開啟網際網路瀏覽器並瀏覽至 http://www.kingston.com/support，您可以在該網站獲得其他支援資訊
關於 D500S： 提供 D500S 的特定詳細資訊，包括應用程式、韌體和序號資訊 (*圖 6.2*) **注意：**「資訊欄」下方可找到隨身碟的唯一識別碼	 **圖 6.2：關於 D500S**
將 D500S 關機：	• 正確關閉 D500S，讓您從系統中安全地移除。

D500S 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：**允許您變更自己的管理員密碼和/或提示 (*圖 7.1*)
- **聯絡資訊：**允許您新增/查看/變更您的聯絡資訊 (*圖 7.2*)
- **語言：**可讓您變更目前語言選項 (*圖 7.3*)
- **管理員選項：**可允許您啟用其他功能，例如：(*圖 7.4*)
    - 變更使用者密碼
    - 登入密碼重設 (適用於使用者密碼)
    - 啟用一次性恢復密碼
    - 啟用加密清除用密碼
    - 用於使用者資料的強制唯讀模式

注意：有關管理員選項的其他詳細資訊，請參閱第 26 頁

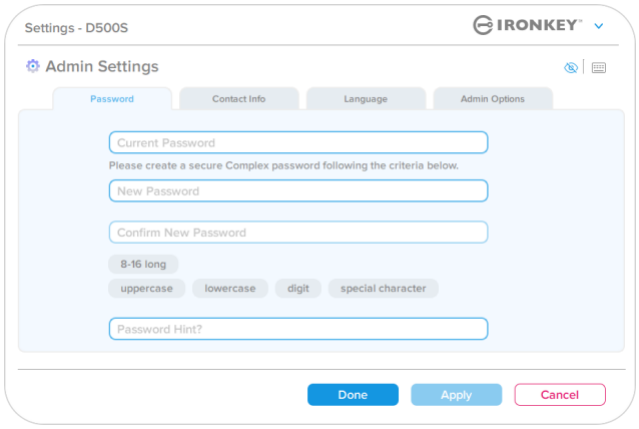


圖 7.1：密碼選項

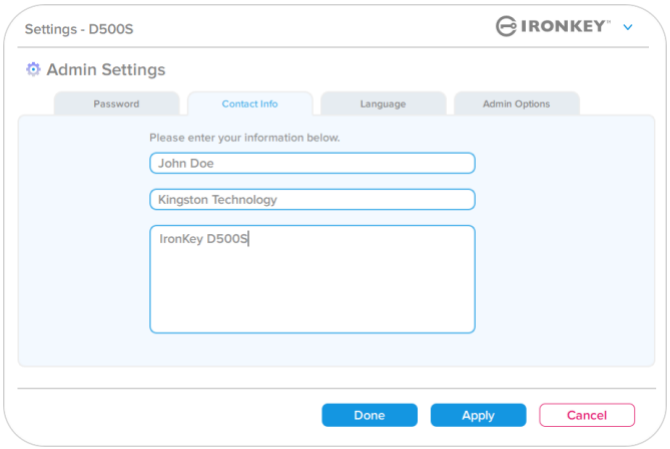


圖 7.2：聯絡資訊

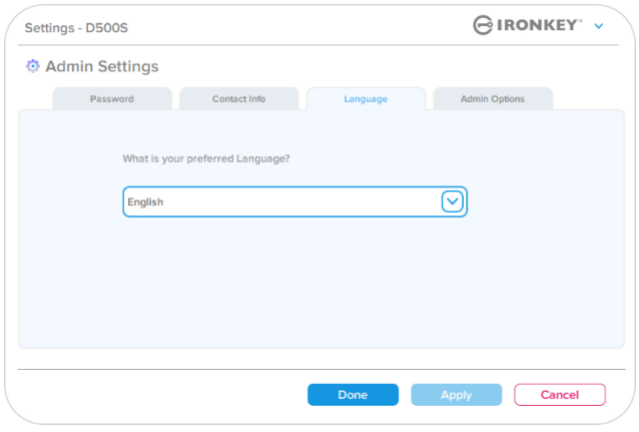


圖 7.3：語言選項

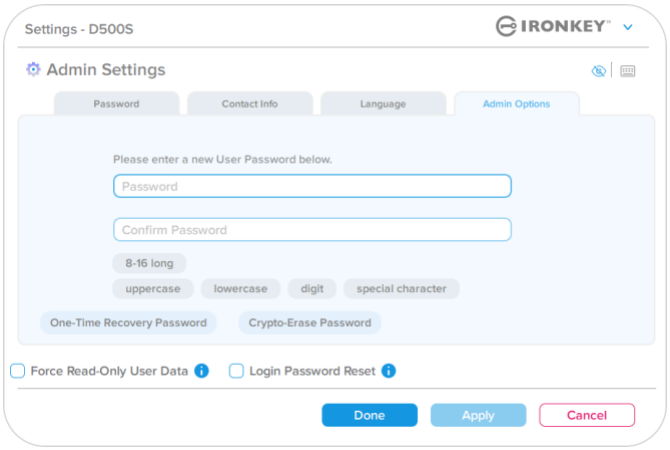
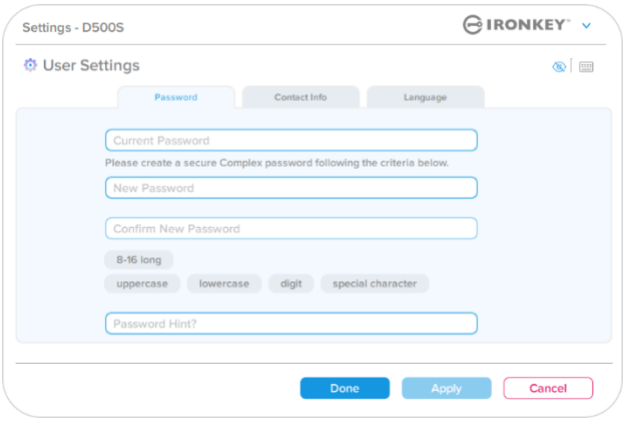
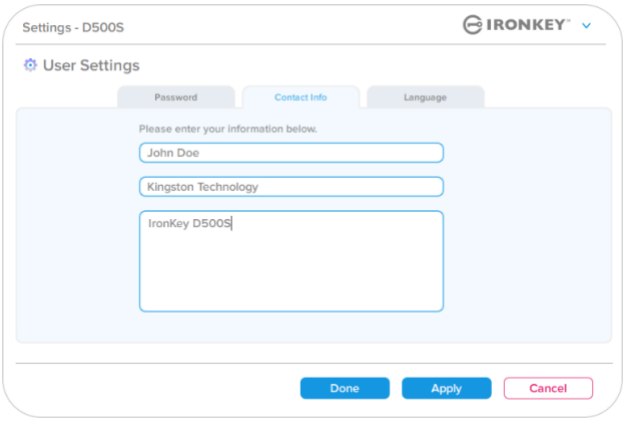
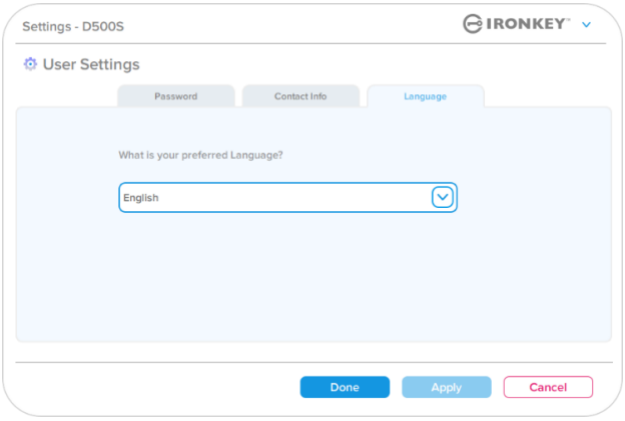


圖 7.4：管理員選項

D500S 設定

使用者設定：啟用管理員

使用者登入限制下列設定的存取：

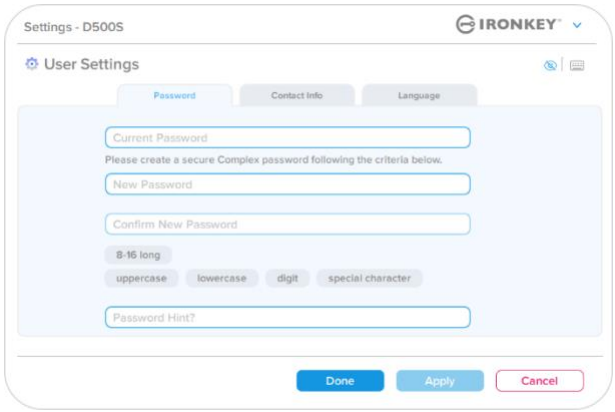
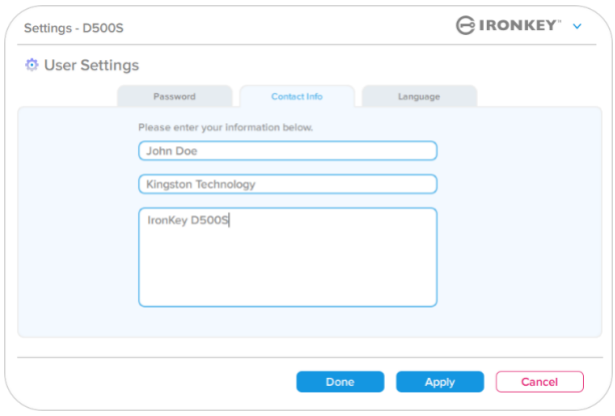
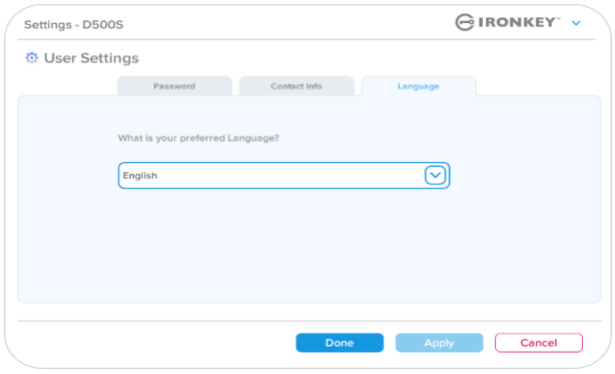
密碼： 允許您變更自己的使用者密碼和/或提示 (*圖 7.5*)	 **圖 7.5：密碼選項 (管理員啟用：使用者登入)**
聯絡資訊： 允許您新增/查看/變更您的聯絡資訊 (*圖 7.6*)	 **圖 7.6：聯絡資訊 (管理員啟用：使用者登入)**
語言： 可讓您變更目前語言選項 (*圖 7.7*)	 **圖 7.7：語言設定 (管理員啟用：使用者登入)**

注意：以使用者密碼登入時，無法存取管理員選項。

D500S 設定

使用者設定：未啟用管理員

如先前所提，在未啟用管理員和使用者密碼的情況下初始化 D500S 時，會以**單一密碼/單一使用者設定配置隨身碟 (單一使用者模式)**。此設定無權存取任何管理員選項或功能。此設定將有權存取以下 D500S 設定：

密碼： 允許您變更自己的使用者密碼和/或提示 (*圖 7.8*)	 **圖 7.8：密碼選項 (單一使用者模式)**
聯絡資訊： 允許您新增/查看/變更您的聯絡資訊 (*圖 7.9*)	 **圖 7.9：聯絡資訊 (單一使用者模式)**
語言： 可讓您變更目前語言選項 (*圖 7.10*)	 **圖 7.10：語言設定 (單一使用者模式)**

D500 設定

變更與儲存設定

- 每當 D500S 設定中的發生設定變更 (例如聯絡資訊、語言、密碼變更、管理員選項等)時，隨身碟將提示您輸入密碼，才能接受並套用變更 (*圖 7.11*)

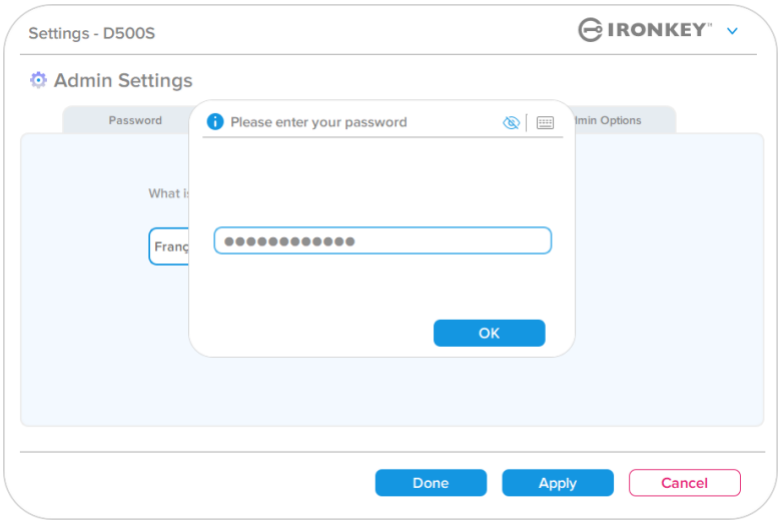


圖 7.11：儲存 D500S 設定變更的密碼提示畫面

注意：如果您在上面的密碼提示畫面中，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。這樣會關閉「請輸入您的密碼」方塊並返回 D500S 設定選單。

管理員功能

可用於重設使用者密碼的選項

管理員配置的功能允許透過多種方式安全地重設使用者密碼，倘若忘記密碼，或如果建立暫時使用者密碼，並希望在下次登入時強制變更密碼以進行使用者登入，皆可重設使用者密碼。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過程期間設定的原始標準 (複雜或密碼短語選項)。

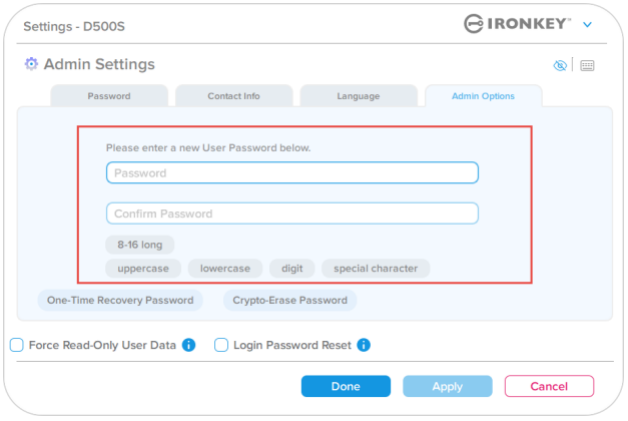


圖 8.1：管理員選項/使用者密碼重設

重設登入密碼：

啟用密碼重設會**強制使用者使用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 8.2 和 8.3*)

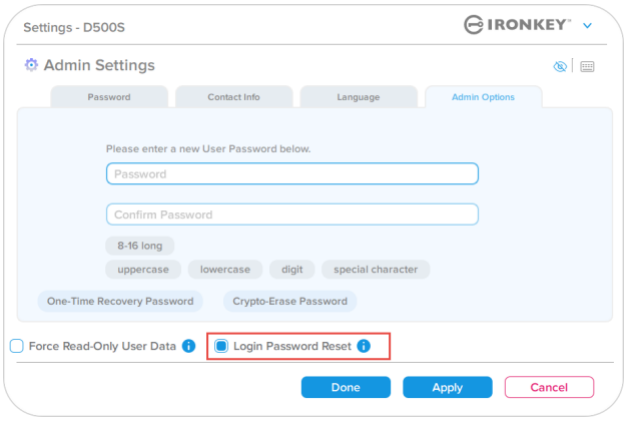


圖 8.2A：登入密碼重設按鈕

注意：套用此重設後，將在下次成功的使用者登入時進行。密碼要求標準將自動套用初始化過程中設定的原始選項 (複雜或密碼選項)。

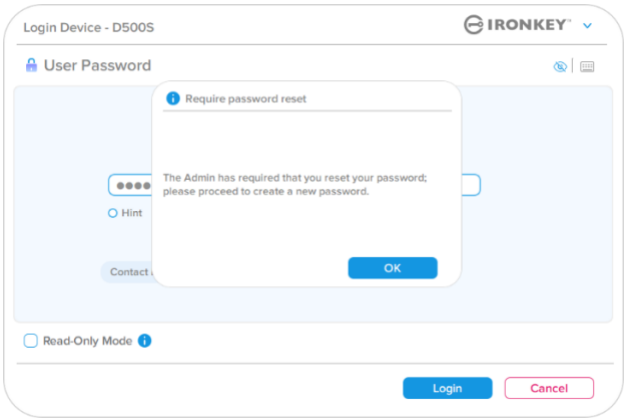


圖 8.3：在輸入使用者密碼後重設通知

管理員功能

一次性恢復密碼

本節將討論啟用和使用一次性恢復密碼功能的過程。

一次性恢復密碼

步驟 1：一次性恢復密碼功能是極為有用的單次使用密碼，在忘記密碼時，可啟用以協助恢復及重設使用者密碼。按一下「管理員」選項選單中的一次性恢復密碼」按鈕以便開始。(*圖 8.4*)

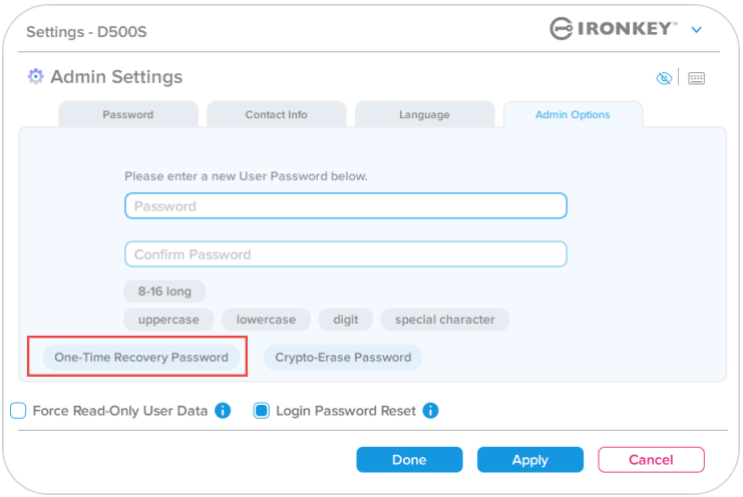


圖 8.4：一次性恢復密碼按鈕

步驟 2：使用最初設定裝置的相同密碼條件(複雜或密碼短語) 建立一次性恢復密碼。

注意：套用變更步驟需要管理員密碼。

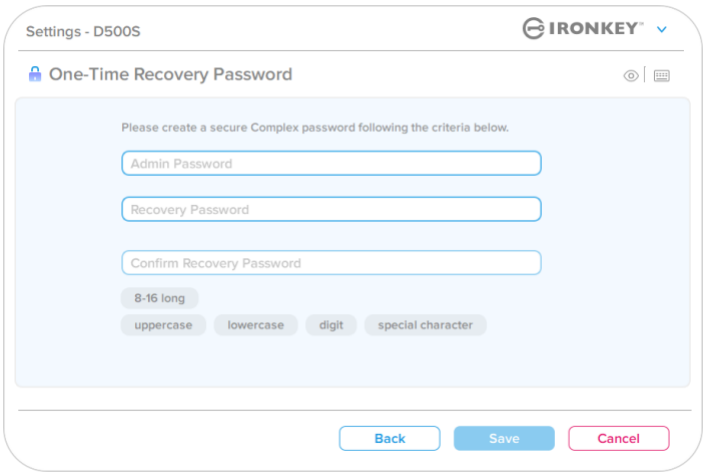
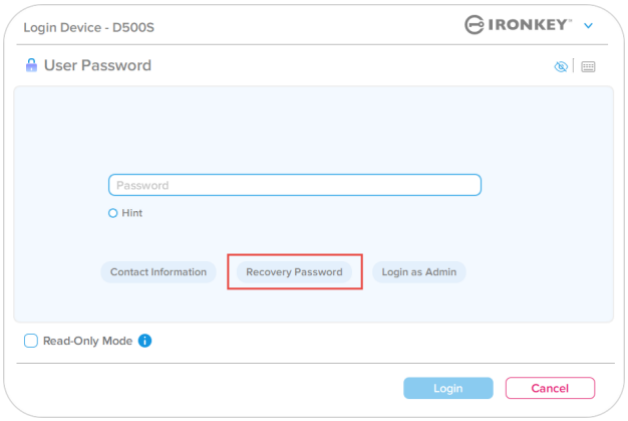
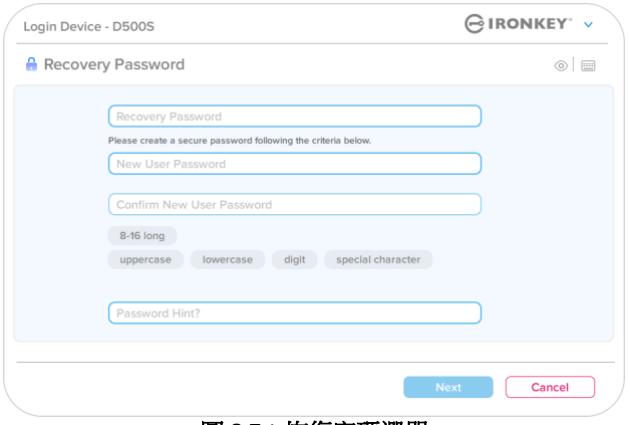
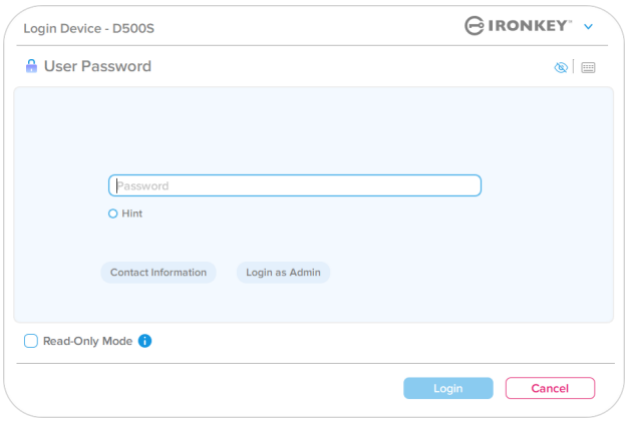


圖 8.5：一次性恢復密碼設定

管理員功能

使用一次性恢復密碼

步驟 1：建立一次性恢復密碼之後，在下次登入時，新的按鈕會出現在**使用者密碼**登入畫面。按一下「**恢復密碼**」按鈕以開始流程。	 **圖 8.6：恢復密碼按鈕**
步驟 2：會顯示恢復密碼畫面，您可以輸入恢復密碼，並建立新的使用者密碼。(*圖 8.7*) 重要須知：一次性恢復密碼也適用內建安全功能，可追蹤失敗登入嘗試次數，**使用一次性恢復密碼進行 10 次登入嘗試失敗後，密碼將被停用**，必須以管理員身分登入隨身碟，才能重新啟用。(更多詳情請參閱第 19 頁和第 33 頁)	 **圖 8.7：恢復密碼選單**
步驟 3：成功後，將回到「**使用者密碼**」畫面。「**恢復密碼**」按鈕目前已消失，而在**步驟 2** 中輸入的使用者密碼將成為新的使用者密碼。(*圖 8.8*)	 **圖 8.8：使用者密碼登入畫面中顯示的「恢復密碼」按鈕會在變更成功後消失。**

管理員功能

加密清除用密碼

IronKey D500S 配備獨特的加密清除用密碼，在隨身碟被使用時能安全地清除隨身碟的資料，看起來像是從未寫入資料一樣，藉以保護並抵擋實體受損。啟用此功能，並使用加密清除用密碼解鎖隨身碟之後，D500S 將有效地謹慎執行加密清除，開啟隨身碟後呈現出廠狀態且無使用者分區。刪除先前的加密金鑰，並建立一個新的裝置金鑰來取而代之。***請謹慎使用***

- 要**啟用**此功能，請在「管理員選項」選單中按一下「加密清除用密碼」按鈕：

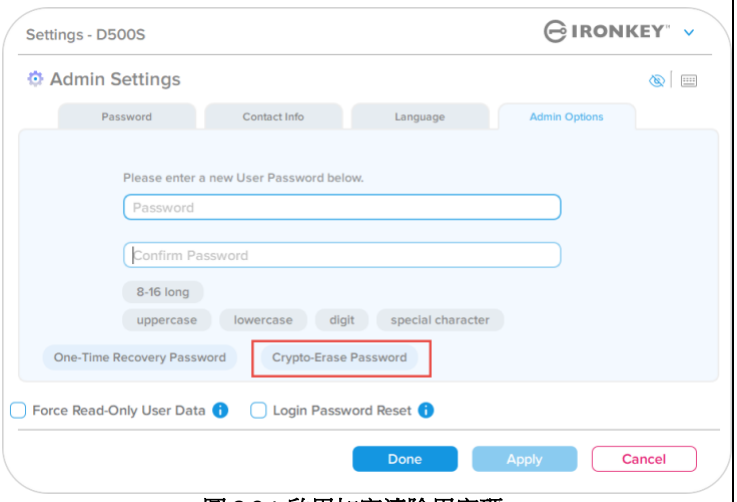


圖 8.9：啟用加密清除用密碼

建立加密清除用密碼：

- 密碼規則與隨身碟最初初始化時的規則相同 (複雜密碼或密碼短語)
- 驗證步驟需要管理員密碼。

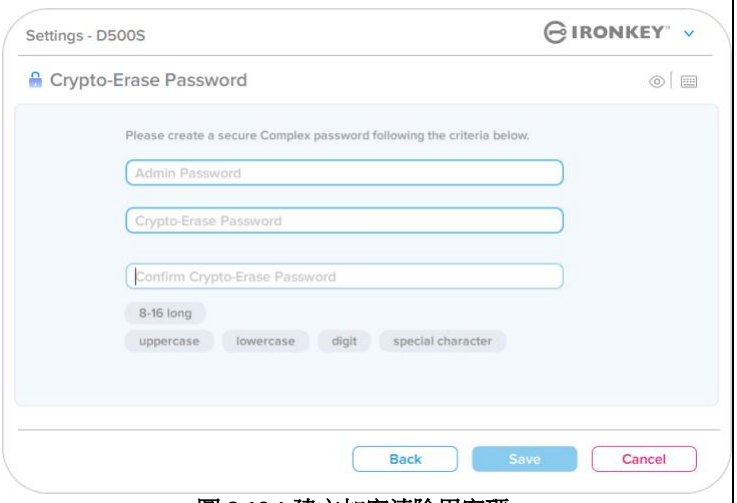


圖 8.10：建立加密清除用密碼

管理員功能

使用加密清除用密碼

使用加密清除用密碼時，將刪除先前的管理員密碼和使用者密碼，並以加密清除用密碼取代。此外，任何先前設定都將被刪除，並永久刪除隨身碟上儲存的所有資料，將隨身碟轉換為單一使用者模式。

使用加密清除用密碼：

1. 啟動 IronKey.exe 以執行 IronKey 應用程式

2. 在使用者登入密碼畫面中，按下「**CTRL + ALT +C**」，切換加密清除用密碼輸入功能。如果操作正確，密碼輸入畫面下方會出現一條粗藍色長條，可以輸入加密清除用密碼。(*圖 8.11*)

注意：加密清除用密碼只能在使用者密碼輸入畫面中切換。

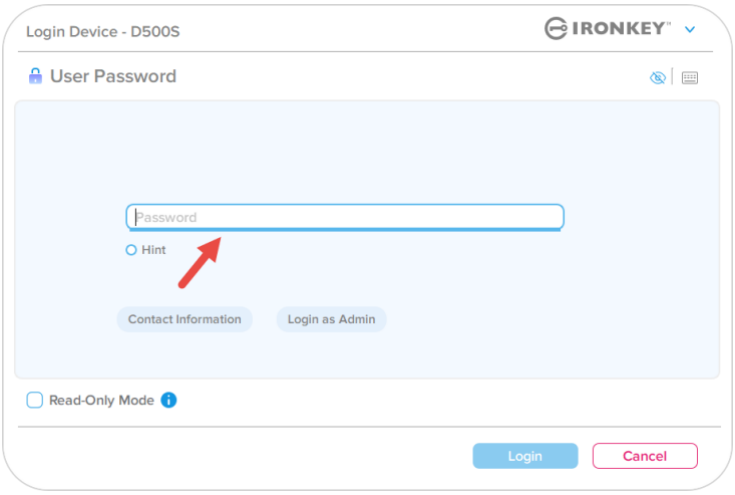


圖 8.11：啟用加密清除用密碼 (粗藍色條)

使用加密清除用密碼後，隨身碟將繼續清除其中所有內容，此時會呈現單一個空的分區。隨身碟會處於單一使用者模式，而加密清除用密碼則為隨身碟的密碼，除非重新設定。

重要須知：此功能將清除隨身碟上的所有資料，所有儲存內容都將永遠遺失，請謹慎操作。

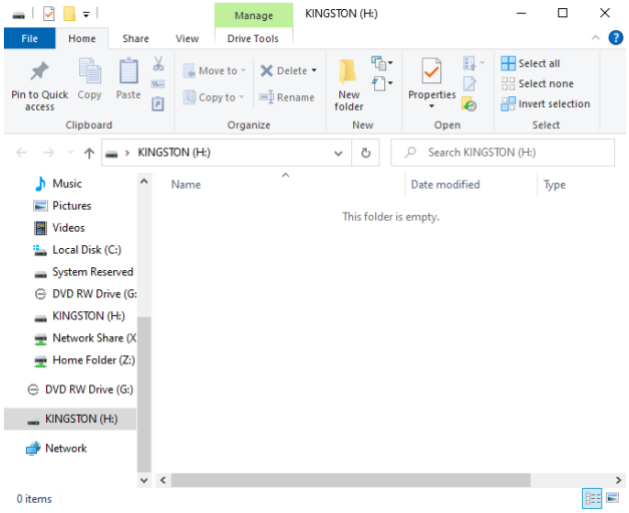


圖 8.12：使用加密清除用密碼後清除隨身碟

管理員功能

強制唯讀使用者資料

強制唯讀模式功能可用來限制使用者寫入資料至隨身碟。如果隨身碟中的檔案只需要讀取存取，則此功能將很有用。

- 若要啟用使用者資料的強制唯讀，請按一下方塊然後按一下「套用」。(*圖 8.13*)

  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，並且仍然可以啟用「唯讀」模式(如果需要)。

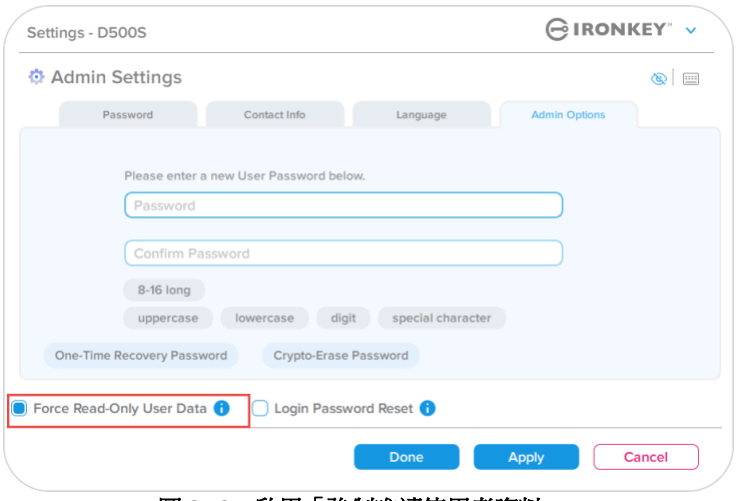


圖 8.13：啟用「強制唯讀使用者資料」(套用變更步驟需要管理員密碼)

- 一旦啟用，**「唯讀模式」**按鈕方塊會變成藍色，表示使用者密碼已經永久啟用「強制唯讀模式」，直到管理員停用為止。(*圖 8.14*)

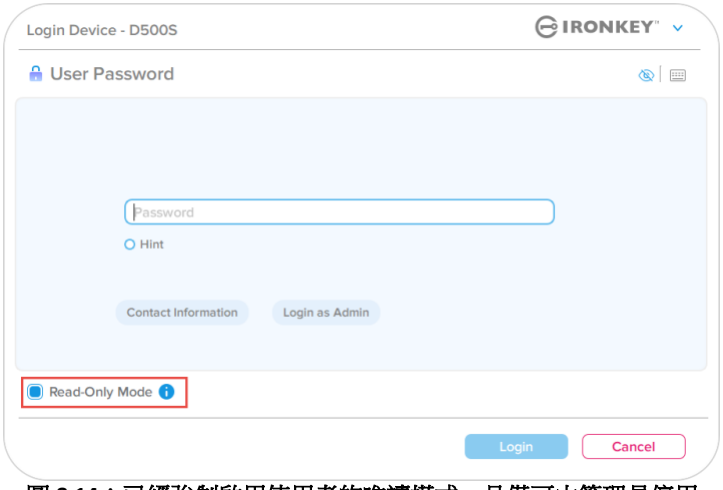


圖 8.14：已經強制啟用使用者的唯讀模式，且僅可由管理員停用

說明與疑難排解

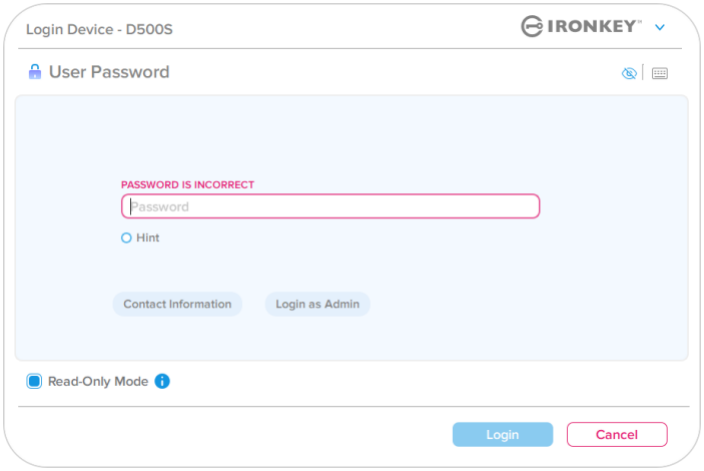
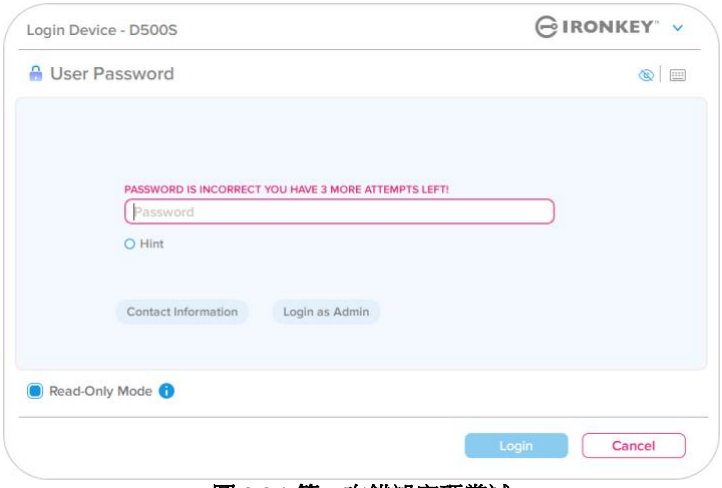
裝置解鎖

D500S 包括可避免未經授權存取資料分割區的安全功能，一旦達到**連續**失敗登入嘗試 (簡稱 *MaxNoA*) 次數上限之後，即無法繼續登入。預設的「開箱即用」設定已經在每種登入方法 (管理員/使用者/一次性恢復密碼) 中預先設定嘗試次數為 10。

「鎖定」計數器會追蹤每次登入失敗次數，並以下列兩種方式之一進行重設：

1. 在達到密碼輸入失敗上限前的成功登入

2. 達到 MaxNoA，執行裝置鎖定或裝置格式化是否執行，則需視裝置的配置方式而定。

• 如果輸入不正確的密碼，「密碼輸入」欄位上方便會以紅色顯示錯誤訊息，表示發生登入錯誤。(*圖 9.1*)	 **圖 9.1：密碼不正確訊息**
• 如果嘗試失敗的次數達到**第 7 次**，您會看到額外的錯誤訊息，顯示再進行 3 次嘗試登入就會達到密碼輸入失敗上限 (預設值為 10 次) (*圖 9.2*)	 **圖 9.2：第 7 次錯誤密碼嘗試**

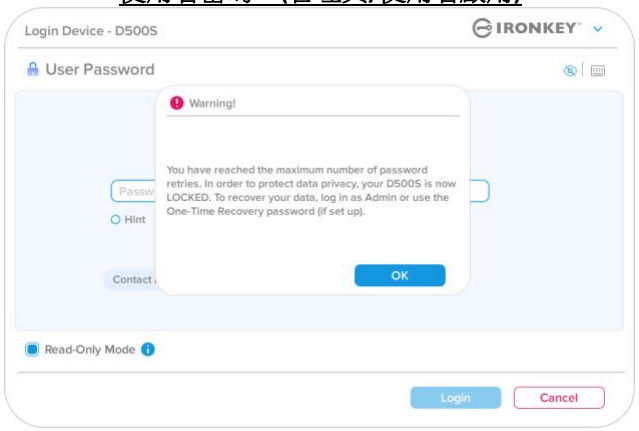
說明與疑難排解

裝置解鎖

重要須知：在輸入 **10 次**最終仍登入失敗時，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)，裝置會遭到鎖定並且需要您使用替代方式登入 (如果適用)，或者裝置需要重設，此時會**格式化資料，同時隨身碟上的所有資料會永久遺失**。本使用者手冊第 19 頁也提及相關情況。

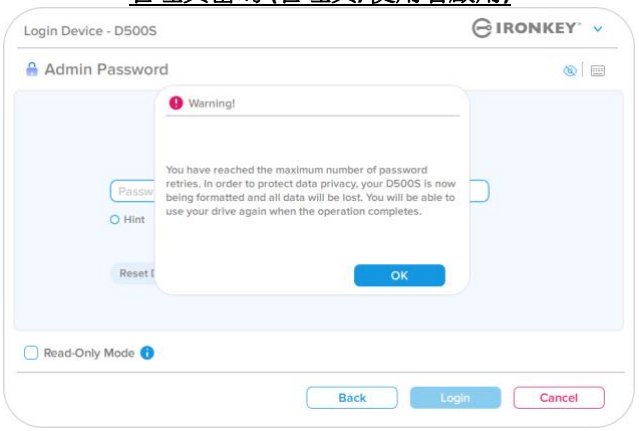
下面的圖 9.3- 9.6 顯示每個登入密碼方法第 10 次，也是最後一次登入失敗的畫面。

使用者密碼：(管理員/使用者啟用)



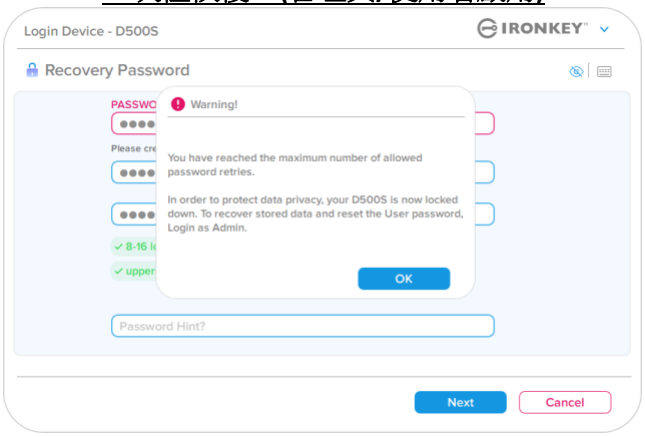
裝置解鎖
圖 9.3

管理員密碼 (管理員/使用者啟用)



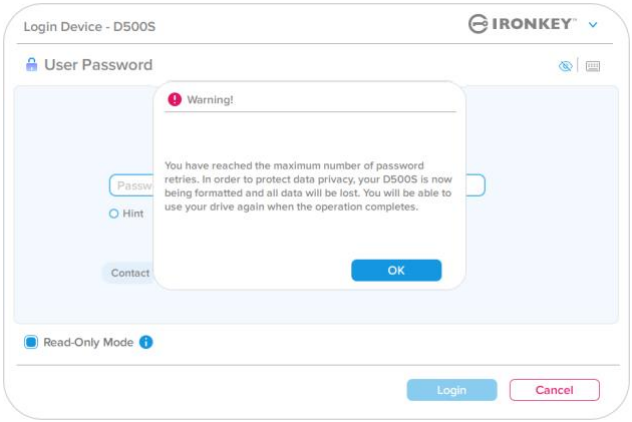
裝置格式化*
圖 9.4

一次性恢復：(管理員/使用者啟用)



裝置解鎖
圖 9.5

使用者密碼 (管理員未啟用)



裝置格式化*
圖 9.6

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 D500S 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 D500S 安全資料分割區中儲存的所有資訊。*

說明與疑難排解

重設裝置

如果您忘記密碼或是需要重設裝置，您可以按一下「*重設裝置*」按鈕，而該按鈕出現的位置則取決於 D500S 啟動程式執行時隨身碟的設定方式而定，如果啟用管理員/使用者，會出現在管理員登入密碼選單；如果未啟用管理員/使用者，則出現在「使用者密碼」登入選單。(*圖 9.7* 和 *9.8*)

- 此選項可讓您建立新密碼，但如果是為了保護您資料的隱私權，則會格式化 D500S。這代表您的所有資料皆會在過程中被移除。*

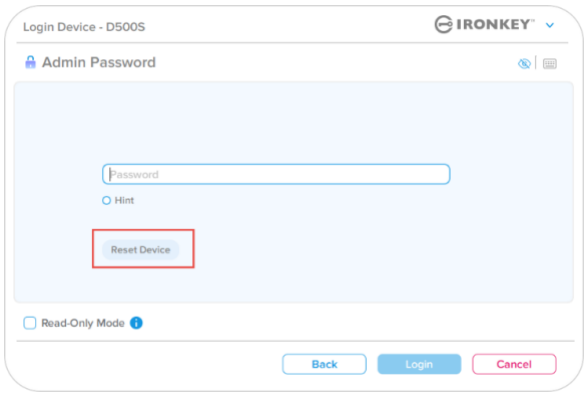


圖 9.7：管理員密碼：重設裝置按鈕

- 注意：當您按一下「*重設裝置*」時，便會顯示一個訊息方塊，並詢問您是否希望先輸入新密碼，然後再執行格式化。此時，您可以：1) 按一下「確定」；或是 2) 按一下「取消」返回登入視窗。(詳見*圖 9.8*)

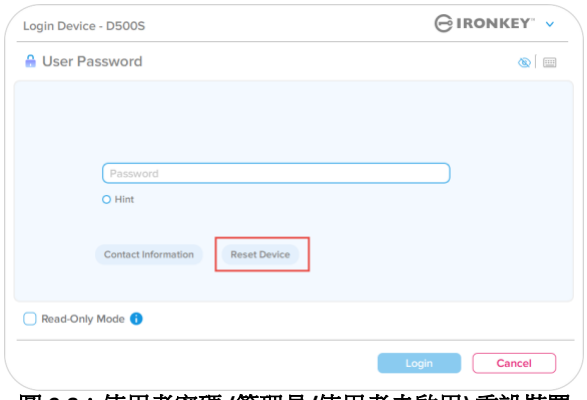


圖 9.8：使用者密碼 (管理員/使用者未啟用) 重設裝置

- 如果您選擇繼續，系統將提示您進入初始化畫面，您可以在其中啟用「管理員和使用者模式」，並根據您選擇的密碼選項 (複雜或密碼短語) 輸入新密碼。提示不是必填欄位，但如果您忘記密碼，提示欄位可幫助您提供有關密碼內容的線索。

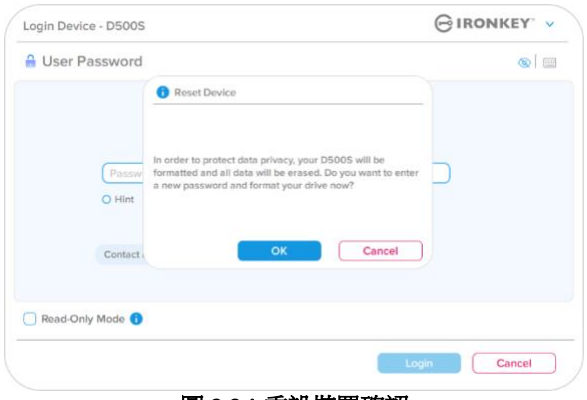


圖 9.9：重設裝置確認

說明與疑難排解

磁碟代號衝突：Windows 作業系統

- 如同本使用者手冊第 3 頁的*「系統需求」*一節所述，D500S 需要位於最後實體磁碟之後的兩個連續磁碟機代號，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，因此可供作業系統使用。
- 如此表示，Windows 可能指定 D500S 一個磁碟機代號，但是該代號已經被網路共用或是通用命名慣例 (UNC) 路徑所使用，導致磁碟機代號發生衝突。如果遇上這種情況，請洽詢系統管理員或服務台支援部門，以瞭解在「Windows 磁碟管理」變更磁碟機代號指定的事宜 (需要用到管理員權限)。如同本使用者手冊第 3 頁的*「系統需求」*一節所述，D500S 需要兩個連續磁碟機代號位於最後實體磁碟之後，而最後實體磁碟則是出現在磁碟機代號指派「間隙」之前 (請參閱*圖 9.10*)。此實體磁碟「不」屬於網路共用磁碟機，因為它專屬於使用者設定檔，而不是系統硬體設定檔本身，因此其狀態顯示為可供作業系統使用。

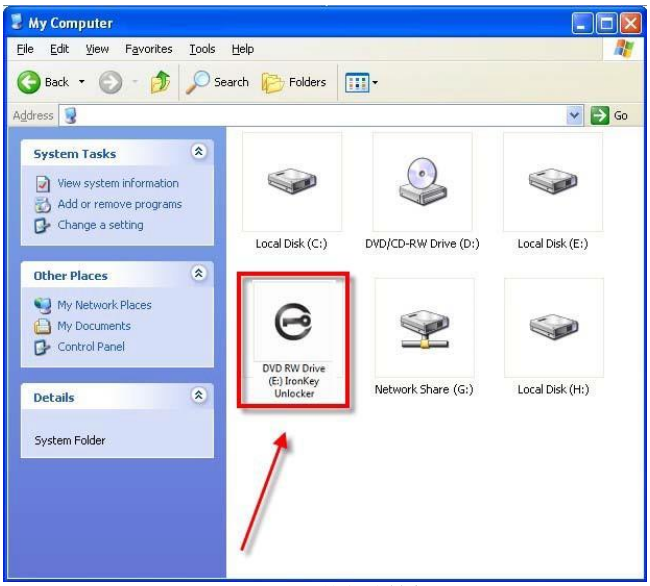


圖 9.10：磁碟機範例

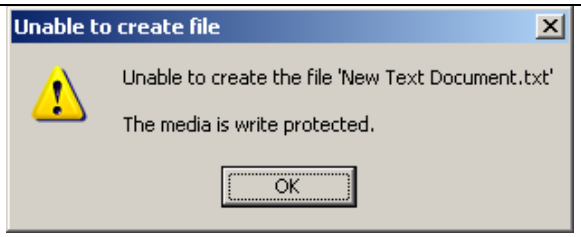
在本例 (*圖 9.10*) 中，D500S 使用磁碟機 F:，這是磁碟機 E:(即磁碟機代號中斷前的最後一個實體磁碟機) 之後第一個可用的磁碟機代號。由於代號 G: 為網路共用磁碟機，而不是硬體設定檔的一部分，所以 D500S 可能會將它當作自己的第二個磁碟機代號，因此造成衝突。

如果您的系統上沒有網路共用，卻仍然無法載入 D500S，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 10 及 11 已大幅改善了「磁碟機代號管理」(或 DLM) 的功能，因此您可能不太會遇上這類問題，但若不幸遇到的話，請聯絡 Kingston 的技術支援部門或造訪 Kingston.com/support，以獲得進一步的協助。

說明與疑難排解

錯誤訊息

無法建立檔案： 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，會出現此錯誤訊息。	 **圖 9.11：無法建立檔案時發生錯誤**
複製檔案或資料夾時發生錯誤： 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，會出現此錯誤訊息。	 **圖 9.12：複製檔案或資料夾時發生錯誤**
刪除檔案或資料夾時發生錯誤： 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，會出現此錯誤訊息。	 **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，但現在想要解鎖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 D500S 再重新登入，並且在登入前取消核取「唯讀模式」核取方塊。

裝置使用 (Linux 系統)

由於目前有各種 Linux 發行版本，故介面外觀和位置會因版本不同而異。不過終端應用程式的通用命令集非常類似，請參考後面的 Linux 說明段落。本節中的畫面截圖範例是於 64 位元環境中執行。

某些 Linux 發行版本需要超級使用者 (root) 身份，才能在終端機應用程式視窗正確執行 D500S 命令。

繼續之前必看重要須知：

1.) **D500S 不支援 Linux 中裝置初始化功能，需要先在有支援的 Windows 或 macOS 系統上執行設定和配置，才能在 Linux 中使用該隨身碟。**

2.) **Linux 登入僅支援複雜密碼。Linux 登入不支援密碼短語。**

3.) **Linux 系統中僅提供 D500S 部分支援功能。Linux 不支援一次性恢復密碼、加密清除用密碼、管理員/使用者密碼重設，以及切換唯讀模式。**

D500S 具有 4 個可在 Linux 中使用的命令：

lkd500s_about	顯示「有關 D500S」資訊。
lkd500s_login	讓您登入隨身碟。
lkd500S_logout	讓您安全可靠地登出 D500S 隨身碟。
lkd500S_resetdevice	執行裝置加密清除，並重置為出廠狀態，同時永久刪除隨身碟中儲存的所有檔案與資料。

注意：如要執行這些命令，請開啟「終端機」應用程式視窗，並前往每個檔案所在的資料夾。每個命令前面必須加上以下兩個字元：「./」(一個小數點和一個正斜線。)

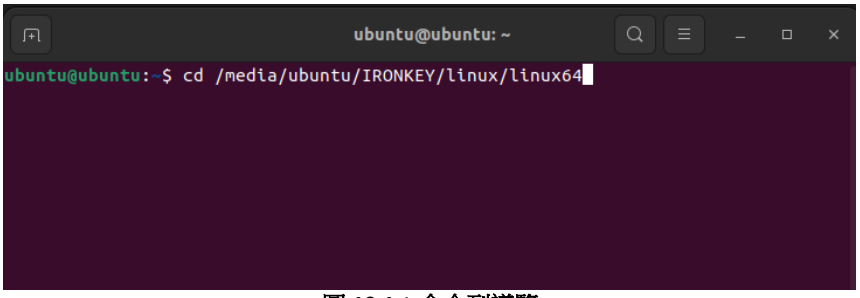
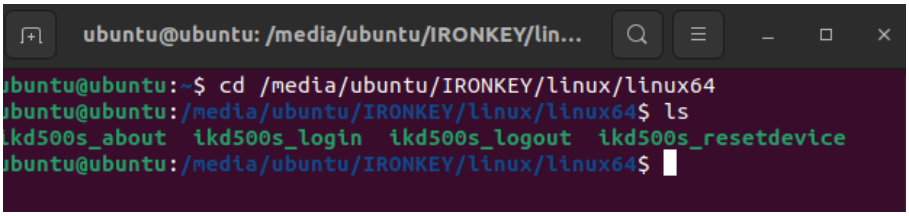
前往 IronKey Linux 命令路徑的範例：

32 位元 Linux 使用者：	開啟「終端機」應用程式視窗，將目前目錄變更為： **/media/ubuntu/IRONKEY/linux/linux32$**，方法是輸入以下命令： **cd /media/ubuntu/IRONKEY/linux/linux32** (然後按 ENTER。)
32 位元 Linux 使用者：	開啟「終端機」應用程式視窗，將目前目錄變更為： **/media/ubuntu/IRONKEY/linux/linux64$**，方法是輸入以下命令： **cd /media/ubuntu/IRONKEY/linux/linux64** (然後按 ENTER。)

裝置使用 (Linux 系統)

注意：如果作業系統沒有自動載入 IRONKEY 卷冊，您需要在終端機視窗使用 Linux 掛載命令來手動載入卷冊。請參考特定作業系統發行版本的 Linux 文件，或您喜愛的線上支援網站，取得正確語法和命令選項。某些 Linux 發行版本可能需要輸入使用者名稱，才能執行命令，即上述範例中的「ubuntu」。

定位並查看 IronKey D500S 的 Linux 命令檔案：

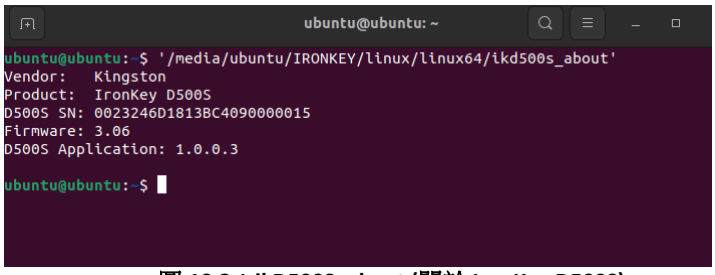
將 D500S 連接到您的電腦且作業系統識別完成後，在終端機命令提示列中輸入命令，將目錄變更為 D500S 卷冊。(*圖 10.1*) **注意：**本節中的畫面節圖和說明是使用 linux64 資料夾 (表示 64 位元)，來示範在 Linux 作業系統中使用 D500S 裝置。請記住，如果您使用的是 32 位元版本的 Linux，那只需要使用並前往對應的 32 位元資料夾，而非 64 位元資料夾，也就是說將「linux64」替換為「linux32」。	 **圖 10.1：命令列導覽**
在當前命令提示列中使用 **ls** (列表) 命令，並按 ENTER。這會列出 linux64 資料夾中的檔案和/或資料夾列表。 然後您會看到列出的 4 個 IronKey Linux 命令 (*圖 10.2*) • ikD500S_about • ikD500S_login • ikD500S_logout • ikD500S_resetdevice	 **圖 10.2：查看 IronKey Linux 命令檔**

注意：命令和資料夾 (目錄) 名稱有大小寫區別，也就是說，「linux64」和「Linux64」不相同。語法也必須完全按照所顯示的輸入。某些 Linux 發行版本可能需要輸入使用者名稱，才能執行命令，即本範例中的「ubuntu」。

裝置使用 (Linux 系統)

使用 D500S 命令

關於 D500S

lkD500S_about (about D500S, *圖 10.3*) 此命令會顯示 D500S 的相關資訊，例如： • 廠商 • 產品 • D500S 序號 • 韌體版本 • 軟體版本	 **圖 10.3：ikD500S_about (關於 IronKey D500S)**

D500S 登入

ikD500S_login

在可支援 Windows 或 macOS 系統上將 D500S 初始化之後，您可以使用您建立的 D500S 密碼，登入此裝置並存取安全資料分區。

如要執行，請依照以下步驟：

1. 開啟「終端機」應用程式視窗。

2. 在終端機提示列中輸入以下命令：**cd /media/ubuntu/IRONKEY/linux/linux64**

3. 接著在命令提示列的 **/media/ubuntu/IRONKEY/linux/linux64$** 下，輸入以下命令以登入裝置：**./ikD500S_login***，並按 ENTER。(注意：命令和資料夾名稱有大小寫區別，語法必須準確。此外，某些發行版本可能需要輸入您的使用者名稱，例如本範例中的「ubuntu」。)

4. 成功登入後，安全資料卷冊將在您的桌面上開啟，您可以繼續並使用 D500S，(而相關登入動作的相關詳細資訊請參照下一頁)

***注意：**某些 Linux 發行版本需要超級使用者 (root) 身份，才能在終端機應用程式視窗正確執行 D500S 命令。

裝置使用 (Linux 系統)

D500S 登入 (續)

IkD500S_login (解鎖 D500S/*圖 10.4*)

根據您隨身碟的設定方式，在登入過程中，您可能會看到許多解鎖隨身碟方式的選項。

如果在初始化流程中啟用了**管理員/使用者**密碼設定檔，那麼您會看到以下的登入選項：

1.) 選擇以管理員或使用者身分登入
2.) 選擇以管理員或使用者分區解鎖 (如果啟用)
3.) 輸入對應的管理員或使用者密碼，進行裝置身分驗證並解鎖。

注意：如果在初始化流程中<u>未</u>啟用管理員/使用者密碼設定檔，也就是單一使用者模式，則系統只會提示您輸入裝置密碼以進行裝置身分驗證。

重要須知：如上所述，Linux 不支援密碼短語，故 D500S 需要設定複雜密碼後才能在 Linux 上登入 (*圖 10.5*)

圖 10.4：ikD500S_login (解鎖 D500S)

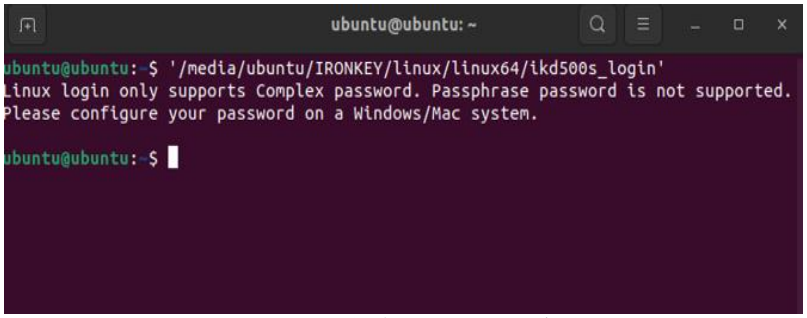


圖 10.5：不支援密碼短語登入嘗試。

裝置使用 (Linux 系統)

D500S 登入 (續)

不正確的登入密碼動作

如果在登入流程中輸入了不正確的密碼，您可以再次輸入密碼，但裝置內建追蹤登入嘗試失敗次數的安全功能。如果管理員或使用者嘗試輸入密碼失敗達到 10 次，磁碟會：

啟用管理員/使用者密碼

- **使用者登入：**使用者鎖定，需要以管理員身分登入。(*圖 10.6*) 注意：在可支援的 Windows 或 macOS 系統上，以管理員身分登入並重設使用者密碼。
- **管理員登入：**執行加密清除，所有資料將永遠丟失。需要重設裝置。(*圖 10.7*)

單一使用者模式 (管理員/使用者未啟用)

- **使用者登入：**執行加密清除，所有資料將永遠丟失。需要重設裝置 (*圖 10.7*)

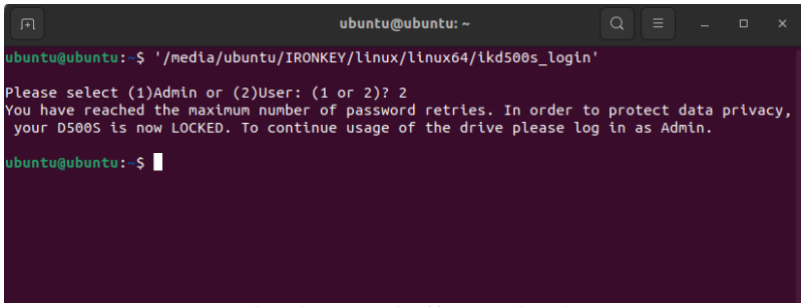


圖 10.6：使用者登入鎖定 (管理員/使用者已啟用)

圖 10.7：達到嘗試失敗次數上限 (重設裝置)

D500S 登出

IkD500S_logout (鎖定裝置)

D500S 使用完畢後，請退出您的裝置並保護其資料。如要執行，請遵循第 39 頁的同一個參考步驟，正確使用以下命令來登出裝置：**./ikD500S_logout**，並按 ENTER (注意：命令和資料夾名稱有大小寫區別，語法務必準確。(*圖 10.8*)

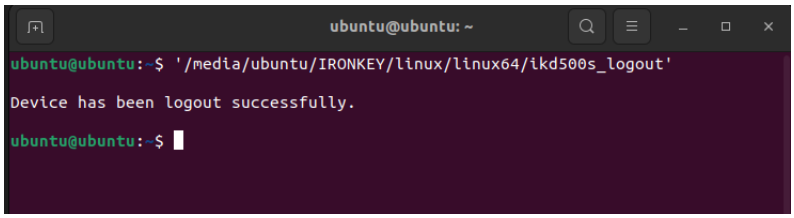


圖 10.8- D500S 登出

裝置使用 (Linux 系統)

D500S 裝置重設

ikD500S_resetdevice
如先前第 41 頁所述，如果忘記使用者/管理員密碼，可使用重設裝置命令來進行裝置重設，裝置就能再次使用。此流程中會請您建立新密碼，但為了確保資料隱私，D500S 將加密清除並格式化隨身碟的安全資料分區。**這代表您的所有資料都將遺失。**

要使用重設裝置命令，請依照第 39 頁同一個參考步驟進，正確使用以下命令來登出裝置：**./ikD500S_resetdevice**，並按 ENTER (注意：命令和資料夾名稱有大小寫區別，語法務必準確。(*圖 10.9*)

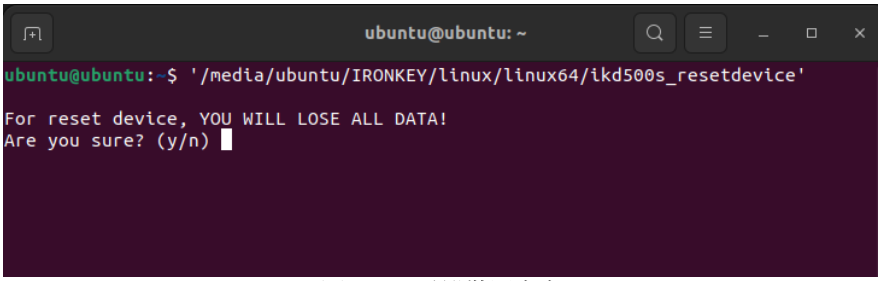


圖 10.9：重設裝置命令

使用重設裝置命令後，系統將提示您建立一個新的複雜密碼，該密碼必須包含：

- 8-16 個字元數，至少包含以下 3 種字元：
  - -大寫
  - -小寫
  - -數字
  - -特殊字元 (!、$ 等)

(*圖 10.10*)

注意：重設裝置命令會在單一使用者模式 (單一密碼/單一使用者) 下將隨身碟初始化。要啟用管理員/使用者密碼設定檔，需要在可支援的 Windows 或 macOS 作業系統中設定 D500S，才能存取該選項。

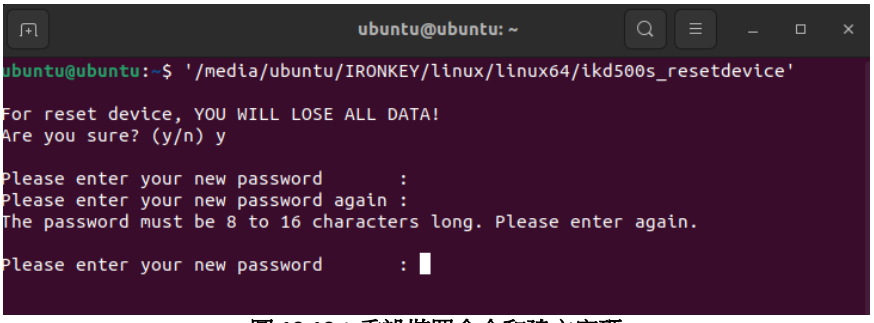


圖 10.10：重設裝置命令和建立密碼