User Manual

IronKey 1000B

Find the language and latest documentation here.

IRONKEY™S1000B
ENCRYPTED USB 3.2 Gen 1 FLASH DRIVE

User Guide

Contents

About This Guide (04152025)

IronKey™ S1000B is a non-managed drive.

Quick Start

Windows 11, 10 & macOS 12.x – 15.x

1. Plug the device into your computer's USB port.

2. When the Device Setup window appears, follow the on-screen instructions. If this window does not appear, open it manually:

    - Windows: Start > This PC > IronKeyUnlocker > IronKey.exe
    - macOS: Finder > IRONKEY > IronKey.app

3. When Device Setup is complete, you can move your important files to the IRONKEY SECURE FILES USB drive, and they will be automatically encrypted.

Some Windows systems prompt to restart after you first plug in your device. You can safely close that prompt without restarting - no new drivers or software are installed.

About My Device

IronKey S1000B USB 3.2 Gen 1 is a portable flash drive with built-in password security and data encryption. It is designed with advanced AES 256-bit encryption and other features that enhance mobile data security. Now you can safely carry your files and data with you wherever you go.

How Is This Different Than a Regular USB Drive?

FIPS 140-2 Level 3 Certification - The IronKey S1000B is a FIPS-certified device, so you can feel confident that you're complying with regulatory requirements.

Hardware Encryption – The Advanced Encryption Controller in your device protects your data with the same level of protection as highly classified government information. This security technology feature is always on and cannot be disabled.

Password-Protected - Device access is secured using password protection. Do not share your password with anyone so that even if your device is lost or stolen, no one else can access your data.

Device Reset - If the Advanced Encryption Controller detects physical tampering, or if the number of consecutive incorrect password attempts exceeds 10 attempts, the device will initiate a reset sequence. **Important** - When a device is reset, all onboard data will be erased, and the device returns to factory settings - *so remember your password.*

Anti-Malware Autorun Protection - Your device can protect you from many of the latest malware threats targeting USB drives by detecting and preventing autorun execution of unapproved programs. It can also be unlocked in Read-Only Mode if you suspect the host computer is infected.

Simple Device Management - Your device includes the IronKey Control Panel, a program for accessing your files, managing your device, and editing your preferences, changing your device password, and safely locking your device.

What Systems Can I Use It On?

- Windows® 11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x or higher) Note: The Linux CLI Unlocker does not support any features that require network access, for example, setting up your device or changing your password.

Some features are only available on specific systems:

Windows Only

- Device Updates

Product Specifications

For further details about your device, see the **Device Info** page in the IronKey Control Panel.

Specifications	Details
Capacity*	4GB, 8GB, 16GB, 32GB, 64GB, 128GB
Speed**	USB 3.2 Gen 1 - 4GB-32GB: 180MB/s Read; 80MB/s Write - 64GB: 230MB/s Read; 160MB/s Write - 128GB: 230MB/s Read; 240MB/s Write USB 2.0: - 4GB-128GB: 40MB/s Read, 35MB/s Write
Dimensions	82.3 mm x 21.1 mm x 9.1 mm
Waterproof	Up to 3 ft; MIL-STD-810F
Temperature	Operating: 0°C to 70°C; Storage: -40°C to 85°C
Hardware Encryption	256-bit AES (XTS Mode)
Certification	FIPS 140-2 Level 3 Certified
Hardware	USB 3.2 Gen 1 Compliant and USB 2.0 Compatible

OS Compatibility	- Windows 11, Windows 10 (Requires Two Free Drive Letters) - macOS 12.x – 15.x - Linux 4.4.x***
Warranty	5-year warranty. Free technical support

Designed and assembled in the U.S.A., S1000B devices do not require any software or drivers to be installed.

* Advertised capacity is approximate. Some space is required for onboard software.
** Speed varies with host hardware, software, and usage.
*** Limited Feature Set.

Recommended Best Practices

1. Lock the device:
   - when not in use
   - before unplugging it
   - before the system enters sleep mode
2. Never unplug the device when the LED is lit.
3. Never share your device password.
4. Perform a computer anti-virus scan before setting up and using the device.

Setting Up My Device

To ensure there is ample power provided to the S1000B encrypted USB drive, insert it directly into a USB 2.0/3.2 Gen 1 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)

1. Plug the S1000B encrypted USB drive into an available USB port on the notebook or desktop and wait for Windows to detect it.

   • Windows 11and10 users will receive a device driver notification.

   • Once the new hardware detection is complete, Windows will prompt to begin the initialization process.

2. Select the option **IronKey.exe** inside of the IRONKEY partition that can be found in File Explorer. 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:).

Device Access (macOS Environment)

1. Plug the S1000B encrypted USB drive into an available USB port on the macOS notebook or desktop and wait for the operating system to detect it.

2. Double click the **IRONKEY** volume that appears on the desktop to start the initialization process.

   • If the IRONKEY volume does not appear on the desktop, open Find er and locate the IronKey volume on the left side of the Find er window (listed under Devices.) Highlight the volume and double-click the IRONKEY application icon in the Finder window. This will start the initialization process.

Device Initialization

Initialization on supported Windows or macOS operating system.

1. Select a language preference from the list. By default, device software will use the same language as your computer's operating system (if available).

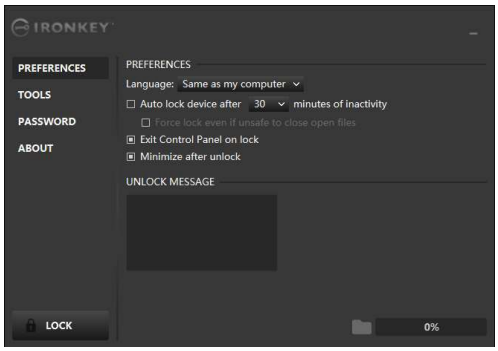
2. Review the license agreement, check the checkbox to accept it, and click Continue.

3. In the Password text box, type a device password, then re-enter your password in the Confirm text box. The password protects the data on the secure drive. Passwords are case-sensitive and must have at least 4 characters (including space).

4. If initializing on Windows, you will be given the option of formatting the IronKey Secure Files drive as either FAT32, exFAT or NTFS. For more information, see Formatting My Device.

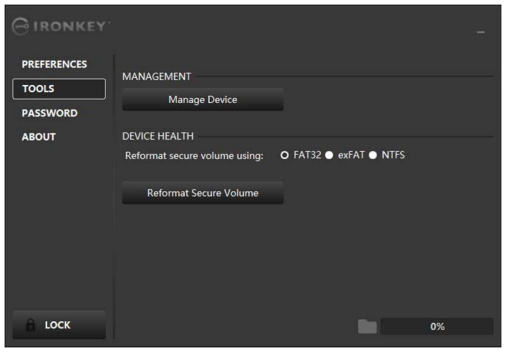
5. By default, the option to 'Reset the device instead of self-destructing' is Enabled. Click Continue. The device will finish initializing. Once complete, the IronKey Control Panel will open. Your device is now ready to store and protect your data.

IronKey Control Panel



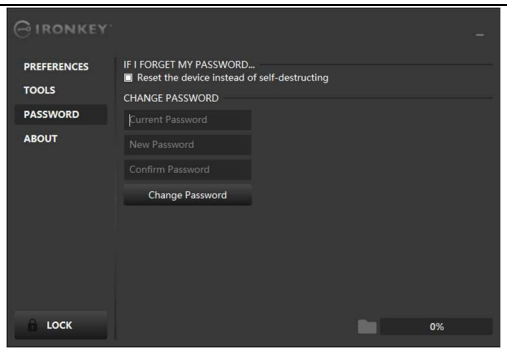
PREFERENCES

1. Language: Change device language
2. Auto lock device: Change lock out timer
3. Exit on Control Panel on lock: Change behavior to exit or leave open Control Panel when device is locked.
4. Minimize after unlock: Change to minimize Control Panel when device is unlocked or allow it to stay maximized.
5. UNLOCK MESSAGE: Add a message that will be displayed on the log-in window.



TOOLS

1. MANAGEMENT: Manage Device (SafeConsole required).
2. DEVICE HEALTH: Reformat secure volume using FAT32, exFAT or NTFS. (macOS only allows formatting FAT32)



PASSWORD

1. IF I FORGET MY PASSWORD...: Enable/Disable 'Reset the device instead of self-destructing'.
2. CHANGE PASSWORD: Change current password to a new password.

ABOUT

1. ABOUT THIS DEVICE: Lists devices information.
2. Visit Website: Launches Kingston's website
3. Legal Notices: Launches both Kingston's and DataLocker's legal notices websites
4. Certifications: Launches Kingston's certificate page for encrypted USB devices

Using My Device

Verifying Device Security

If a secure USB storage device has been lost or unattended it should be verified as per the following user guidance. The secure USB storage device shall be discarded if it may be suspected that an attacker has tampered with the device or if the self-test fails.

- Verify the secure USB storage device visually, that it doesn't have marks or new scratches that might indicate tampering.
- Verify that the secure USB storage device is physically intact by slightly twisting it.
- Verify that the secure USB storage device weighs about 30 grams.
- Verify when plugged into a computer that the blue indicator light on the secure USB storage device blinks (the correct frequency is 3 times per second at initial connection and during read/write operations).
- Verify that the secure USB storage device is showing as a DVD-RW, and a storage partition is not mounted until the device is Unlocked.

Accessing My Secure Files

After unlocking the device, 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.

To access your secure files:

1. Click **Folder Icon**  in the lower right corner of the IronKey Control Panel.

   - Windows: Opens Windows Explorer to the IRONKEYSECUREFILESUSB drive.

   - macOS: Opens Finder to the KINGSTONUSB drive.

2. Do one of the following:

   - To open a file, double-click the file on the S1000BUSB drive.

   - To save a file, drag the file from your computer to the S1000BUSB drive.

Hint: You can also access your files by right clicking the **IronKey Icon** in the Windows taskbar and clicking **Secure Files**.

Unlocking In Read-Only Mode

You can unlock your device in a read-only state so that files cannot be altered on your secure 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, the IronKey Control Panel will display the text *Read-Only Mode*. In this mode, you cannot perform any operations that involve modifying files on the device. For example, you cannot reformat the device or edit files on the drive.

To unlock the device in Read-Only Mode:

1. Insert the device into the USB port of the host computer and run the **IronKey.exe**.

2. Check the **Read-Only Checkbox** below the password entry box.

3. Type your device password and click **Unlock**. The IronKey Control Panel will appear with the text *Read-Only Mode* at the bottom.

Changing The Unlock Message

The Unlock Message is custom text that displays in the IronKey window when you unlock the device. This feature allows you to customize the message that displays. For example, adding contact information will display information on how a lost drive can be returned to you.

To change the Unlock Message:

1. In the IronKey Control Panel, click **Settings** on the menu bar.

2. Click **Preferences** in the left sidebar.

3. Type the message in the Unlock Message field. The text must fit in the space provided (approximately 6 lines and 200 characters).

Minimize Control Panel When Unlocked

When your device is unlocked, the Control Panel is minimized to the taskbar automatically. If desired, the Control Panel can remain displayed after the device has been unlocked.

To disable Minimize after unlock:

1. In the IronKey Control Panel, click Preferences in the left sidebar.
2. Click the Checkbox for Minimize after unlock.

Locking The Device

Lock your device when you are not using it to prevent unwanted access to your secure files on the drive. You can manually lock the device, or you can set the device to automatically lock after a specified period of inactivity.

Caution: By default, if a file or application is open when the device tries to auto-lock, it will not force the application or file to close. Although you can configure the auto-lock setting to force the device to lock, doing so might result in loss of data to any open and unsaved files.

If your files have become corrupt from a forced lock procedure or from unplugging the device before locking, you might be able to recover the files by running CHKDSK and using data recovery software (Windows only).

To manually lock the device:

1. Click **Lock** in the bottom left-hand corner of the IronKey Control Panel to safely lock your device.

   - You can also use the keyboard shortcut: **CTRL + L** (Windows only), or right-click the **IronKey Icon** in the system tray and click **Lock Device**.

To set a device to automatically lock:

1. Unlock your device and click **Settings** on the menu bar in the IronKey Control Panel.

2. Click **Preferences** in the left sidebar.

3. Click the **Checkbox** for auto-locking the device and set the time-out to one of the following time intervals: 5, 15, 30, 60, 120, or 180 minutes.

To run CHKDSK (Windows only):

1. Unlock the device.

2. Press the WINDOWS LOGO KEY + R to open the Run prompt.

3. Type CMD and press ENTER.

4. From the command prompt, type CHKDSK, the IRONKEY SECURE FILES USB drive letter, then "/F /R". For example, if the IRONKEYSECUREFILESUSB drive letter is G, you would type: CHKDSK G: /F /R

5. Use data recovery software, if necessary, to recover your files.

6. Exit Control Panel on Lock

When your device is locked, the Control Panel will close automatically. To unlock the device and access the Control Panel, you will need to run the IronKey application again. If desired, the Control Panel can be set to return to the Unlock screen after the user locks the device.

To disable Exit Control Panel on lock:

1. Unlock your device and click Settings on the menu bar in the IronKey Control Panel.

2. Click Preferences in the left sidebar.

3. Click the Checkbox for Exit Control Panel on lock.

Managing Passwords

You can change your password on your device by accessing the Password tab in the IronKey Control Panel.

Sometimes, you may be required to change your password to comply with new corporate password policies. When a change is required, the Password Change screen will appear the next time you unlock the device. If the device is in use, it will lock, and you will have to change the password before you can unlock it.

To change your password:

1. Unlock your device and click **Settings** on the menu bar.

2. Click **Password** in the left sidebar.

3. Enter your current password in the field provided.

4. Enter your new password and confirm it in the fields provided.

5. Click Change Password.

Formatting My Device

Your device will need to be formatted during initialization before it can be used to store files.

If initializing on Windows, you will be given the option of formatting the IRONKEY SECURE FILES USB drive as either FAT32, exFAT or NTFS.

Options are for Windows operating systems only - macOS will automatically format to FAT32.

- FAT32

  - Pros: Cross-platform compatible (Windows and mac OS)
  - Cons: Limited individual file size of 4GB

- exFAT

  - Pros: No file size limitations
  - Cons: Microsoft restricts usage by license obligations

- NTFS

  - Pros: No file size limitations
  - Cons: Mounted as Read Only access on supported macOS's

After initialization, reformatting the IRONKEY SECURE FILESUSB drive will perform a quick format and provide an empty drive, but will not erase your device password and settings.

Important: Before you reformat the device, back up your IRONKEY SECURE FILES USB drive to a separate location, for example, to cloud storage or your computer.
To reformat a device:

1. Unlock your device and click **Settings** on the menu bar of the IronKey Control Panel.

2. Click **Tools** on the left sidebar.

3. Under Device Health, select the file format and click **Reformat Secure Volume**.

Finding Information About My Device

Use the Capacity Meter, located at the bottom right of the IronKey Control Panel, to see how much storage space is still available on your device. The green bar graph represents how full the device is. For example, the meter will be totally green when the device is full. The white text on the Capacity Meter displays how much free space remains.

For general information about your device, see the Device Info page.

To view device information:

1. Unlock your device and click **Settings** on the menu bar of the IronKey Control Panel.

2. Click **Device Info** in the left sidebar.

The About This Device section includes the following details about your device:

- Model Number
- Hardware ID
- Serial Number
- Software Version
- Firmware Version
- Release Date
- Secure Files Drive Letter
- IronKey Drive Letter
- Operating System and System Administrative Privileges
- Management Console

Note: To visit the IronKey website or access more information about legal notices or certifications for IronKey products, click one of the information buttons on the Device Info page.

Hint: Click **Copy** to copy the device information to the clipboard so that you can paste it in an email or support request.

Resetting My Device

Your device can be reverted to factory settings. This will securely wipe all data from the device and a new security key will be created for the next use.

Resetting your device:

1. Unlock your device.

2. Right-click on the **IronKey Icon** in the system tray.

3. Click Reset Device.

To prevent accidental device resets a popup will ask to enter a random four digits. After entering the confirmation, the device will now be reset back to factory settings.

Using My Device on Linux

You can use your device on several distributions of Linux. There are two executables in the linux folder, Unlocker_32.exe and Unlocker_64.exe. For this guide, replace Unlocker_xx.exe with the executable that is compatible with your system.

The device must be previously set up using a Windows or macOS operating system. See Setting Up My Device for more information.

Using The Unlocker

Use the Unlocker_xx.exe for Linux to access your files. Depending on your Linux distribution, you may need root privileges to use the program Unlocker_xx.exe found in the Linux folder of the mounted public volume. By default, most Linux distributions will append the execute bit to .exe files on a fat32 partition. Otherwise, the execute bit must be manually set before running by using the following commands.

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

If you have only one device attached to the system, run the program from a command shell with no arguments (for example, Unlocker_xx.exe). This will then prompt you for your device password to unlock the drive. If you have multiple devices, you must specify which one you want to unlock.

These are the available parameters for the device software:

```
Options:

 -h, -help         help
 -l, -lock         lock device
 -r, -readonly    unlock as read only
```

Note: Unlocker_xx.exe only unlocks the IRONKEYSECURE FILESUSB; it must then be mounted. Many modern Linux distributions do this automatically. If not, run the mount program from the command line, using the device name printed by Unlocker_xx.exe.

Simply un-mountingthe device does not automaticallylock the IRONKEYSECUREFILESUSB. To lock the device, you must either unmount and physically remove (unplug) it, or run:

- Unlocker_xx.exe -l

Please note the following important details for using your device on Linux:

1. Kernel Version must be 4.4.x or higher.
2. Mounting
   - Make sure you have permissions to mount external SCSI and USB devices.
   - Some distributions do not mount automatically and require the following command to be run: mount /dev/[name of the device] / media/ [mounted device name]

3. The name of the mounted device varies depending on the distribution.

4. Permissions

   • You must have permissions to mount external/usb/devices.

   • You must have permissions to run an executable file from the public volume to launch the Unlocker.

   • You might need root user permissions.

5. The IronKey for Linux supports x86 and x86_64 systems.

Where Can I Get Help?

The following resources provide more information about IronKey products. Please contact Kingston support you have further questions.

- kingston.com/usb/encrypted_security: Information, marketing material, and video tutorials.
- kingston.com/support: Product support, FAQ's and downloads

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

FCC Information This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation. This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

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

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

Document No. S1000B11062023

IRONKEY™ S1000B
UNIDAD ENCRIPTADA FLASH USB 3.2 Gen 1

Guía del usuario

Contenidos

Acerca de esta guía (04152025)

IronKey™ S1000B es una unidad no administrada.

Inicio rápido

Windows 11, 10 & macOS 12.x – 15.x

1. Conecte el dispositivo al puerto USB de su computadora.
2. Cuando aparezca la ventana Configuración del dispositivo, siga las instrucciones en pantalla. Si esta ventana no aparece, ábrala manualmente:
    - Windows: Inicio > Este PC > IronKey Unlocker > IronKey.exe
    - macOS: Finder > IRONKEY > IronKey.app
3. Cuando se complete la configuración del dispositivo, puede mover sus archivos importantes a la unidad USB de ARCHIVOS SEGUROS IRONKEY y se encriptarán automáticamente.

Algunos sistemas Windows solicitan reiniciar después de conectar el dispositivo por primera vez. Puede cerrar ese mensaje de forma segura sin reiniciar; no hay nuevos controladores ni software instalados.

Acerca de mi dispositivo

IronKey S1000B USB 3.2 Gen 1 es una unidad flash portátil con seguridad de contraseña y encriptado de datos incorporados. Está diseñada con encriptado avanzado AES de 256 bits y otras características que mejoran la seguridad de los datos móviles. Ahora puede llevar sus archivos y datos con usted dondequiera que vaya.

¿En qué se diferencia este de una unidad USB normal?

Certificación FIPS 140-2 Nivel 3: el IronKey S1000B es un dispositivo con certificación FIPS, por lo que puede estar seguro de que cumple con los requisitos reglamentarios.

Encriptado por hardware: el controlador de encriptado avanzado de su dispositivo protege sus datos con el mismo nivel de protección que la información gubernamental altamente clasificada. Esta función tecnológica de seguridad está siempre activada y no se puede desactivar.

Protegido por contraseña: el acceso al dispositivo está protegido por contraseña. No comparta su contraseña con nadie para que, incluso si su dispositivo se pierde o es robado, nadie más pueda acceder a sus datos.

Restablecimiento del dispositivo: si el controlador de encriptado avanzado detecta una manipulación física, o si el número de intentos consecutivos de contraseña incorrecta supera los 10 intentos, el dispositivo iniciará una secuencia de restablecimiento. **Importante:** al restablecer un dispositivo, se borrarán todos los datos incorporados y el dispositivo volverá a los ajustes de fábrica, *así que recuerde su contraseña*.

Protección contra la ejecución automática de malware: su dispositivo puede protegerle de muchas de las últimas amenazas de malware dirigidas a unidades USB detectando e impidiendo la ejecución automática de programas no aprobados. También se puede desbloquear en modo de solo lectura si sospecha que el equipo huésped está infectado.

Administración simple de dispositivos: su dispositivo incluye el Panel de control de IronKey, un programa para acceder a sus archivos, gestionar su dispositivo y editar sus preferencias, cambiar la contraseña del dispositivo y bloquearlo de forma segura.

¿En qué sistemas puedo usarlo?

- Windows® 11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x o superior) Nota: El Linux CLI Unlocker no admite ninguna función que requiera acceso a la red, por ejemplo, configurar su dispositivo o cambiar su contraseña.

Algunas funciones solo están disponibles en sistemas específicos:

Solo en Windows

- Actualizaciones del dispositivo

Especificaciones del producto

Para obtener más detalles sobre su dispositivo, consulte la página **Información del dispositivo** en el Panel de control de IronKey.

Especificaciones	Detalles
Capacidades*	4GB, 8GB, 16GB, 32GB, 64GB, 128GB
Velocidad**	USB 3.2 Gen 1 - 4GB-32GB: 180MB/seg Lectura; 80MB/seg Escritura - 64GB: 230MB/seg Lectura; 160MB/seg Escritura - 128GB: 230MB/seg Lectura; 240MB/seg Escritura USB 2.0: - 4GB-128GB: 40MB/seg de lectura, 35MB/seg de escritura
Dimensiones	82.3 x 21.1 x 9.1 mm
A prueba de agua	Hasta 3 pies (1m); MIL-STD-810F
Temperatura	Funcionamiento: 0°C hasta 70°C; Almacenamiento: -40° a 85°C
Encriptado por Hardware	AES de 256 bits (Modo XTS)
Certificación	Certificación FIPS 140-2 Nivel 3
Hardware	Compatible con USB 3.2 Gen 1 y Compatible con USB 2.0

Compatibilidad con SO	- Windows 11, Windows 10 (requiere dos letras de unidad libres) - macOS 12.x – 15.x - Linux 4.4.x***
Garantía	Garantía 5 años. Soporte técnico gratuito

Diseñados y ensamblados en los EE. UU., los dispositivos S1000B no requieren la instalación de ningún software o controlador.

* La capacidad anunciada es aproximada. Se requiere algo de espacio para el software incorporado.
** La velocidad varía en función del hardware, el software y el uso.
*** Conjunto de características limitadas.

Mejores prácticas recomendadas

1. Bloquee del dispositivo:
   - cuando no está en uso
   - antes de desenchufarlo
   - antes de que el sistema entre en modo de suspensión
2. Nunca desenchufe el dispositivo cuando el LED esté encendido.
3. Nunca comparta la contraseña de su dispositivo.
4. Realizar un análisis antivirus de la computadora antes de configurar y usar el dispositivo.

Configurar mi dispositivo

Para asegurarse de que el dispositivo USB encriptado S1000B recibe suficiente energía, insértelo directamente en un puerto USB 2.0/ 3.2 Gen 1 de una computadora portátil o de escritorio. Evite conectarlo a cualquier dispositivo periférico que pueda tener un puerto USB, como un teclado o un concentrador alimentado por USB. La configuración inicial del dispositivo debe realizarse en un sistema operativo Windows o macOS compatible.

Acceso a dispositivos (Entorno Windows)

1. Conecte la unidad USB encriptada S1000B a un puerto USB disponible en el portátil o computadora y espere a que Windows la detecte.

   - Los usuarios de Windows 11 y 10 recibirán una notificación del controlador de dispositivo.

   - Una vez que la detección del nuevo hardware se haya terminado, Windows comenzará con el proceso de inicialización.

2. Seleccione la opción **IronKey.exe** dentro de la partición IRONKEY que se puede encontrar en el Explorador de archivos. Tenga en cuenta que la letra de la partición variará en función de la próxima letra de unidad libre. La letra de la unidad puede cambiar dependiendo de qué dispositivos estén conectados. En la imagen a continuación, la letra de unidad es (E:).

Acceso a dispositivos (Entorno macOS)

1. Conecte la unidad USB encriptada S1000B a un puerto USB disponible en el macOS portátil o computadora y espere a que el sistema operativo la detecte.

2. Haga doble clic en el volumen **IRONKEY** que aparece en el escritorio para iniciar el proceso de inicialización.

   - Si el volumen IRONKEY no aparece en el escritorio, abra Finder y localice el volumen IronKey en el lado izquierdo de la ventana Finder (que aparece en Dispositivos). Resalte el volumen y haga doble clic en el icono de la aplicación IRONKEY en la ventana del Finder. Esto comenzará el proceso de inicialización.

Inicialización del dispositivo

Inicialización en el sistema operativo Windows o macOS compatible.

1. Seleccione un idioma de la lista. Por defecto, el software del dispositivo utilizará el mismo idioma que el sistema operativo del ordenador (si está disponible).

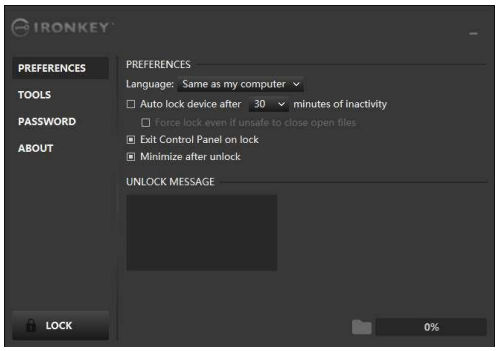
2. Revise el acuerdo de licencia, marque la casilla para aceptarlo y haga clic en Continuar.

3. En el cuadro de texto Contraseña, escriba una contraseña de dispositivo y, a continuación, vuelva a introducir su contraseña en el cuadro de texto Confirmar. La contraseña protege los datos en el dispositivo seguro. Las contraseñas distinguen entre mayúsculas y minúsculas y deben tener al menos 4 caracteres (incluido el espacio).

4. Si se inicializa en Windows, se le dará la opción de formatear la unidad IronKey Secure Files como FAT32 o NTFS. Para obtener más información, consulte Formatear mi dispositivo.

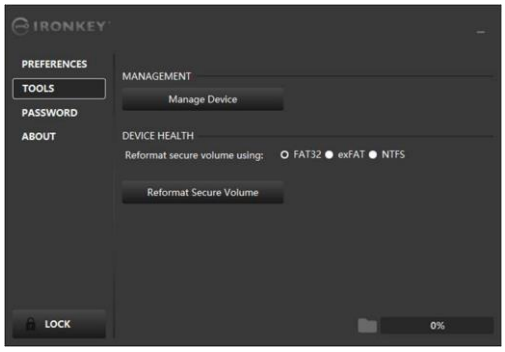
5. De forma predeterminada, la opción “Restablecer el dispositivo en lugar de autodestruirse” está habilitada. Haga clic en Continuar. El dispositivo finalizará la inicialización. Una vez completado, se abrirá el Panel de control de IronKey. Su dispositivo ya está listo para almacenar y proteger sus datos.

Panel de control IronKey



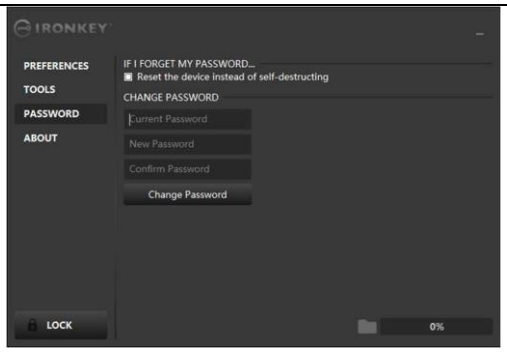
PREFERENCIAS

1. Idioma: Cambiar el idioma del dispositivo
2. Dispositivo de autobloqueo: Cambiar el temporizador de bloqueo
3. Salir en el panel de control al bloquear: Cambie el comportamiento para salir o dejar abierto el Panel de control cuando el dispositivo está bloqueado.
4. Minimizar después del desbloqueo: Cambie para minimizar el Panel de control cuando el dispositivo esté desbloqueado o permita que se mantenga maximizado.
5. MENSAJE DE DESBLOQUEO Agregue un mensaje que se mostrará en la ventana de inicio de sesión.



HERRAMIENTAS

1. ADMINISTRACIÓN: Administrar dispositivo (se requiere SafeConsole).
2. ESTADO DEL DISPOSITIVO: Reformatee el volumen seguro utilizando FAT32, exFAT o NTFS. (macOS solo permite formatear FAT32)



CONTRASEÑA

1. SI OLVIDO MI CONTRASEÑA...: Habilitar/Deshabilitar ‘Restablecer el dispositivo en lugar de autodestruirse’.
2. CAMBIAR CONTRASEÑA: Cambie la contraseña actual a una contraseña nueva.

ACERCA DE

1. ACERCA DE ESTE DISPOSITIVO: Muestra información sobre el dispositivo.
2. Visite el sitio web: Abre el sitio web de Kingston
3. Avisos legales: Abre los sitios web de avisos legales de Kingston y DataLocker
4. Certificaciones: Inicia la página de certificados de Kingston para dispositivos USB encriptados

Uso de Mi Dispositivo

Verificación de la seguridad del dispositivo

Si un dispositivo de almacenamiento USB seguro se ha perdido o está desatendido, debe verificarse de acuerdo con las siguientes instrucciones para el usuario. El dispositivo de almacenamiento USB seguro deberá desecharse si se sospecha que un atacante ha manipulado el dispositivo o si la autocomprobación falla.

- Verifique visualmente que el dispositivo de almacenamiento USB seguro no tenga marcas o nuevos arañazos que puedan indicar una manipulación.
- Verifique que el dispositivo de almacenamiento USB seguro esté físicamente intacto girándolo ligeramente.
- Verifique que el dispositivo de almacenamiento USB seguro pese unos 30 gramos.
- Verifique que, al conectarlo a una computadora, la luz indicadora azul del dispositivo de almacenamiento USB seguro parpadea (la frecuencia correcta es de 3 veces por segundo en la conexión inicial y durante las operaciones de lectura/escritura).
- Verifique que el dispositivo de almacenamiento USB seguro se muestre como un DVD-RW y que no se monte una partición de almacenamiento hasta que el dispositivo esté desbloqueado.

Accesando a mis archivos seguros

Después de desbloquear el dispositivo puede acceder a sus archivos seguros. Los archivos se cifran y descifran automáticamente cuando los guarda o los abre en el dispositivo. Esta tecnología le brinda la comodidad de trabajar como lo haría normalmente con un dispositivo regular, al tiempo que proporciona una seguridad sólida y “siempre activa”.

Para acceder a sus archivos seguros:

1. Haga clic en el **icono de carpeta**  en la esquina inferior derecha del panel de control de IronKey.
   - Windows: Abra el Explorador de Windows en el dispositivo USB IRONKEY SECURE FILES
   - macOS: Abra Finder en el dispositivo USB de KINGSTON.
2. Siga uno de los siguientes pasos:
   - Para abrir un archivo, haga doble clic en el archivo en la unidad USB S1000B.
   - Para guardar un archivo, arrástrelo desde su computadora a la unidad USB S1000B.

Pista: También puede acceder a sus archivos haciendo clic con el botón derecho del ratón en el **icono IronKey** de la barra de tareas de Windows y haciendo clic en **Archivos seguros**.

Desbloqueo en Modo de solo lectura

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

Cuando trabaje en este modo, el Panel de control de IronKey mostrará el texto *Modo de solo lectura*. En este modo, no puede realizar ninguna operación que implique la modificación de archivos en el dispositivo. Por ejemplo, no puede volver a formatear el dispositivo o editar archivos en la unidad.

Para desbloquear el dispositivo en Modo de solo lectura:

1. Inserte el dispositivo en el puerto USB de la computadora huésped y ejecute **IronKey.exe**.
2. Marque la **casilla de verificación de sólo lectura** situada debajo de la casilla de introducción de la contraseña.
3. Escriba la contraseña de su dispositivo y haga clic en **desbloquear**. El Panel de control de IronKey aparecerá con el texto *Modo de solo lectura* en la parte inferior.

Cambiar el mensaje de desbloqueo

El mensaje de desbloqueo es un texto personalizado que se muestra en la ventana de IronKey al desbloquear el dispositivo. Esta función le permite personalizar el mensaje que se muestra. Por ejemplo, al agregar información de contacto mostrará información sobre cómo se le puede devolver una unidad perdida.

Para cambiar el mensaje de desbloqueo:

1. En el Panel de control de IronKey, haga clic en **Configuración** en la barra de menú.
2. Haga clic en **Preferencias** en la barra lateral izquierda.
3. Escriba el mensaje en el campo Desbloquear mensaje. El texto debe caber en el espacio previsto (aproximadamente 6 líneas y 200 caracteres).

Minimizar el Panel de Control cuando está desbloqueado

Cuando se desbloquea el dispositivo, el Panel de control se minimiza automáticamente a la barra de tareas. Si lo desea, el Panel de control puede permanecer en pantalla después de que el dispositivo se haya desbloqueado.

Para deshabilitar Minimizar después del desbloqueo:

1. En el panel de control de IronKey, haga clic en Preferencias en la barra lateral izquierda.
2. Haga clic en la casilla de verificación para minimizar después del desbloqueo.

Bloqueo del dispositivo

Bloquee su dispositivo cuando no lo esté usando para evitar el acceso no deseado a sus archivos seguros en la unidad. Puede bloquear manualmente el dispositivo, o puede configurar el dispositivo para que se bloquee automáticamente después de un período de inactividad especificado.

Precaución: De forma predeterminada, si un archivo o aplicación está abierto cuando el dispositivo intenta bloquearse automáticamente, no forzará el cierre de la aplicación o archivo. Aunque puede configurar la configuración de bloqueo automático para forzar el bloqueo del dispositivo, hacerlo podría resultar en la pérdida de datos para cualquier archivo abierto y no guardado.

Si sus archivos se han dañado por un procedimiento de bloqueo forzado o por desenchufar el dispositivo antes de bloquearlo, es posible que pueda recuperar los archivos ejecutando CHKDSK y utilizando un software de recuperación de datos (solo Windows).

Para bloquear manualmente el dispositivo:

1. Haga clic en **Bloquear** en la esquina inferior izquierda del Panel de control de IronKey para bloquear su dispositivo de forma segura.
    - También puede utilizar el atajo de teclado: **CTRL + L** (solo Windows) o haga clic con el botón derecho en el **icono de IronKey** en la bandeja del sistema y haga clic en **Bloquear dispositivo**.

Para configurar un dispositivo para que se bloquee automáticamente:

1. Desbloquee su dispositivo y haga clic en **Configuración** en la barra de menú del Panel de control de IronKey.

2. Haga clic en **Preferencias** en la barra lateral izquierda.
3. Haga clic en la **casilla de verificación** para bloquear automáticamente el dispositivo y establezca el tiempo de espera en uno de los siguientes intervalos de tiempo: 5, 15, 30, 60, 120 o 180 minutos.

Para ejecutar CHKDSK (solo Windows):

1. Desbloquee el dispositivo.
2. Presione la TECLA DEL LOGO DE WINDOWS + R para abrir el indicador de ejecución.
3. Escriba CMD y presione ENTER.
4. Desde el símbolo del sistema, escriba CHKDSK, la letra de la unidad USB IRONKEY SECURE FILES y luego “/F /R”. Por ejemplo, si la letra de unidad USB IRONKEY SECURE FILES es G, escribiría: CHKDSK G: /F /R
5. Utilice un software de recuperación de datos, si es necesario, para recuperar sus archivos.

Salir del panel de control al bloquear

Cuando su dispositivo está bloqueado, el Panel de control se cerrará automáticamente. Para desbloquear el dispositivo y acceder al Panel de control, deberá volver a ejecutar la aplicación IronKey. Si lo desea, el Panel de control se puede configurar para volver a la pantalla de desbloqueo después de que el usuario bloquee el dispositivo.

Deshabilitar Salir del panel de control al bloquear:

1. Desbloquee su dispositivo y haga clic en Configuración en la barra de menú del Panel de control de IronKey.
2. Haga clic en Preferencias en la barra lateral izquierda.
3. Haga clic en la casilla de verificación Salir del panel de control al bloquear.

Administrar contraseñas

Puede cambiar su contraseña en su dispositivo accediendo a la pestaña Contraseña en el Panel de control de IronKey.

A veces, es posible que deba cambiar su contraseña para cumplir con las nuevas políticas de contraseñas corporativas. Cuando se requiera un cambio, la pantalla de cambio de contraseña aparecerá la próxima vez que desbloquee el dispositivo. Si el dispositivo está en uso, se bloqueará y tendrá que cambiar la contraseña antes de poder desbloquearlo

Para cambiar su contraseña:

1. Desbloquee su dispositivo y haga clic en **Configuración** en la barra de menús.
2. Haga clic en **Contraseña** en la barra lateral izquierda.
3. Ingrese su contraseña actual en el campo proporcionado.

4. Introduzca su nueva contraseña y confírmela en los campos proporcionados.

5. Clic en Cambiar contraseña.

Formatear mi dispositivo

Su dispositivo tendrá que ser formateado durante la inicialización antes de que pueda ser utilizado para almacenar archivos.

Si se inicializa en Windows, se le dará la opción de formatear la unidad USB IRONKEY SECURE FILES como FAT32, exFAT o NTFS.

Las opciones son solo para los sistemas operativos Windows: macOS formateará automáticamente a FAT32.

- FAT32
  - A favor: Compatible con varias plataformas (Windows y Mac OS)
  - En contra: Tamaño de archivo individual limitado a 4GB
- exFAT
  - A favor: Sin limitaciones de tamaño de archivo
  - En contra: Microsoft restringe el uso por obligaciones de licencia
- NTFS
  - A favor: Sin limitaciones de tamaño de archivo
  - En contra: Montado como acceso de Solo lectura en macOS compatibles

Después de la inicialización, volver a formatear la unidad USB IRONKEY SECURE FILES realizará un formato rápido y proporcionará una unidad vacía, pero no borrará la contraseña y la configuración de su dispositivo.

Importante: Antes de volver a formatear el dispositivo, haga una copia de seguridad de su unidad USB IRONKEY SECURE FILES en una ubicación separada, por ejemplo, en el almacenamiento en la nube o en su computadora.
To reformat a device:

1. Desbloquee su dispositivo y haga clic en **Configuración** en la barra de menú del Panel de control de IronKey.

2. Haga clic en **Herramientas** en la barra lateral izquierda.

3. En Estado del dispositivo, seleccione el formato de archivo y haga clic en **Reformatear Volumen Seguro**.

Buscar información sobre mi dispositivo

Utilice el medidor de capacidad, ubicado en la parte inferior derecha del Panel de control de IronKey, para ver cuánto espacio de almacenamiento queda disponible en su dispositivo. El gráfico de barras verdes representa qué tan lleno está el dispositivo. Por ejemplo, el medidor estará totalmente verde cuando el dispositivo esté lleno. El texto blanco en el medidor de capacidad muestra cuánto espacio libre queda.

Para obtener información general sobre su dispositivo, consulte la página Información del dispositivo.

Para ver la información del dispositivo:

1. Desbloquee su dispositivo y haga clic en **Configuración** en la barra de menú del Panel de control de IronKey.

2. Clic en **Información del dispositivo** en la barra lateral izquierda.

La sección Acerca de este dispositivo incluye los siguientes detalles sobre su dispositivo:

- Número de modelo
- ID de Hardware
- Número de serie
- Versión del software
- Versión del firmware
- Fecha de publicación
- Letra de unidad de archivos seguros
- Letra de dispositivo IronKey
- Sistema operativo y privilegios administrativos del sistema
- Consola de administración

Nota: Para visitar el sitio web de IronKey o acceder a más información sobre avisos legales o certificaciones para productos IronKey, haga clic en uno de los botones de información en la página Información del dispositivo.

Pista: Haga clic en **Copiar** para copiar la información del dispositivo en el portapapeles para que pueda pegarla en un correo electrónico o en una solicitud de soporte.

Restablecimiento de mi dispositivo

Su dispositivo se puede volver a la configuración de fábrica. Esto borrará de forma segura todos los datos del dispositivo y se creará una nueva clave de seguridad para el próximo uso.

Restablecimiento de su dispositivo:

1. Desbloquee el dispositivo.

2. Haga clic derecho en el **icono IronKey** de la bandeja del sistema.

3. Clic para restablecer el dispositivo.

Para evitar reinicios accidentales del dispositivo, una ventana emergente le pedirá que ingrese cuatro dígitos al azar. Después de ingresar la confirmación, el dispositivo se restablecerá a los ajustes de fábrica.

Uso de Mi Dispositivo en Linux

Puede usar su dispositivo en varias versiones de Linux. Hay dos ejecutables en la carpeta linux, Unlocker_32.exe y Unlocker_64.exe. Para esta guía, reemplace Unlocker_xx.exe por el ejecutable compatible con su sistema.

El dispositivo debe configurarse previamente con un sistema operativo Windows o macOS. Consulte Configurar mi dispositivo para obtener más información.

Uso del Unlocker

Utilice Unlocker_xx.exe para Linux para acceder a sus archivos. Dependiendo de su versión de Linux, es posible que necesite privilegios de root para usar el programa Unlocker_xx.exe que se encuentra en la carpeta Linux del volumen público montado. De forma predeterminada, la mayoría de las versiones de Linux anexarán el bit de ejecución a los archivos .exe en una partición FAT32. De lo contrario, el bit de ejecución debe configurarse manualmente antes de ejecutarse mediante los siguientes comandos.

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

Si solo tiene un dispositivo conectado al sistema, ejecute el programa desde una consola de comandos sin argumentos (por ejemplo, Unlocker_xx.exe). Esto le pedirá la contraseña de su dispositivo para desbloquear el dispositivo. Si tiene varios dispositivos, debe especificar cuál desea desbloquear.

Estos son los parámetros disponibles para el software del dispositivo:

Opciones:

```
-h, -help         ayuda
-l, -lock         bloquear el dispositivo
-r, -readonly     desbloquear como solo como lectura
```

Nota: Unlocker_xx.exe solo desbloquea el USB IRONKEY SECURE FILES; luego debe montarse. Muchas versiones modernas de Linux hacen esto automáticamente. Si no es así, ejecute el programa de montaje desde la línea de comandos, utilizando el nombre del dispositivo impreso por Unlocker_xx.exe.

El simple hecho de desmontar el dispositivo no bloquea automáticamente el USB IRONKEY SECURE FILES. Para bloquear el dispositivo, debe desmontarlo y retirarlo físicamente (desenchufarlo), o ejecutar:

- Unlocker_xx.exe -l

Tenga en cuenta los siguientes detalles importantes para usar su dispositivo en Linux:

1. La versión Kernel debe ser 4.4.x o superior.
2. Montaje
   - Asegúrese de tener permisos para montar dispositivos SCSI y USB externos.
   - Algunas distribuciones no se montan automáticamente y requieren que se ejecute el siguiente comando: mount /dev/[name of the device] / media/ [mounted device name]

3. El nombre del dispositivo montado puede variar dependiendo de la versión.

4. Permisos

   - Debe tener permisos para montar dispositivos/usb/externos.
   - Debe tener permisos para ejecutar un archivo ejecutable desde el volumen público para iniciar el Desbloqueador (Unlocker).
   - Es posible que necesite permisos de usuario root.

5. IronKey para Linux es compatible con sistemas x86 y x86_64.

¿Dónde puedo obtener ayuda?

Los siguientes recursos proporcionan más información sobre los productos IronKey. Por favor, póngase en contacto con el soporte de Kingston si tiene más preguntas.

- kingston.com/usb/encrypted_security: Información, material de marketing y videotutoriales.
- kingston.com/support: Soporte de productos, preguntas frecuentes y descargas

NOTA: IronKey no es responsable de los errores técnicos o editoriales ni de las omisiones contenidas en este documento; ni por daños incidentales o consecuentes que resulten del suministro o uso de este material. La información proporcionada en este documento está sujeta a cambios sin previo aviso. La información contenida en este documento representa la opinión actual de IronKey sobre el tema discutido a la fecha de publicación. IronKey no puede garantizar la exactitud de ninguna información presentada después de la fecha de publicación. Este documento es sólo para fines informativos. IronKey no ofrece garantías, expresas o implícitas, en este documento. IronKey y el logotipo de IronKey son marcas comerciales de Kingston Digital, Inc. y sus subsidiarias. Todas las otras marcas registradas son propiedad de sus respectivos dueños. IronKey™ es una marca comercial registrada de Kingston Technologies, utilizada con el permiso de Kingston Technologies. Todos los derechos reservados.

Información de la FCC Este dispositivo cumple con las disposiciones de la norma de la comisión FCC, Parte 15. El funcionamiento del dispositivo está sujeto a las siguientes dos condiciones: (1) Este dispositivo no tiene por qué causar interferencias nocivas, y (2) este dispositivo debe aceptar cualquier interferencia recibida, incluidas las interferencias que puedan provocar un funcionamiento no deseado. Este equipo fue probado y se determinó que cumple con los límites para los dispositivos digitales de Clase B, en conformidad con la Parte 15 de las normas FCC. Dichos límites, están diseñados con el fin de suministrar una protección razonable contra las interferencias nocivas que pudieran surgir en instalaciones residenciales. Este equipo genera, utiliza y puede irradiar energía de radiofrecuencia y, de no instalarse y utilizarse en conformidad con las instrucciones, podría causar interferencias nocivas en las comunicaciones de radio y TV. No obstante, no hay garantía alguna que no se produzcan interferencias en ciertas instalaciones en particular. Si este equipo llegara a causar interferencias nocivas en la recepción de radio o televisión, lo cual puede determinarse apagando y encendiendo el equipo, se insta al usuario a intentar corregir la interferencia mediante uno o más de los siguientes pasos:

- Cambie la orientación y/o la posición de la antena receptora.
- Aumente la separación entre el equipo y el receptor.
- Enchufe el equipo a un tomacorriente perteneciente a un circuito distinto al que está conectado el receptor.
- Consulte al vendedor o a un técnico experimentado de radio y televisión, en busca de ayuda.

Nota: Los cambios o modificaciones no aprobados expresamente por la parte responsable del cumplimiento podrían anular la autoridad del usuario para utilizar el equipo.

IRONKEY™ S1000B
VERSCHLÜSSELTER USB 3.2 Gen 1-STICK

Anleitung

Inhalt

Über diese Bedienungsanleitung (04152025)

Der IronKey™ S1000B ist ein nicht verwalteter USB-Stick.

Erste Schritte

Windows 11, 10 und macOS 12.x – 15.x

1. Schließen Sie das Gerät an einem USB-Anschluss Ihres Computers an.
2. Wenn das Fenster „Device Setup (Geräteeinrichtung)“ erscheint, folgen Sie den Anweisungen auf dem Bildschirm. Wenn dieses Fenster nicht erscheint, öffnen Sie es manuell:
    - Windows: Start > Dieser PC > IronKey Unlocker > IronKey.exe
    - macOS: Finder > IRONKEY > IronKey.app
3. Wenn die Geräteeinrichtung abgeschlossen ist, können Sie Ihre wichtigen Dateien auf das IRONKEY SECURE FILES USB-Laufwerk verschieben und diese werden dann automatisch verschlüsselt.

Einige Windows-Systeme fordern nach dem ersten Anschließen des Geräts zum Neustart auf. Sie können diese Eingabeaufforderung schließen, ohne neu zu starten, denn es werden keine neuen Treiber bzw. neue Software installiert.

Über das Gerät

Der IronKey S1000B USB 3.2 Gen 1 ist ein tragbarer USB-Stick mit integrierter Passwortsicherheit und Datenverschlüsselung. Der Stick ist mit einer fortschrittlichen AES-256-Bit-Verschlüsselung und anderen Funktionen ausgestattet, die die Sicherheit mobiler Daten erhöhen. Jetzt können Sie Ihre Dateien und Daten sicher mit sich führen, wohin Sie auch gehen.

Was ist der Unterschied zu einem normalen USB-Stick?

FIPS 140-2 Level 3 Zertifizierung – Der IronKey S1000B ist ein FIPS-zertifiziertes Gerät, damit Sie sicher sein können, dass Sie die gesetzlichen Anforderungen erfüllen.

Hardware-Verschlüsselung – Der Advanced Encryption Controller in Ihrem Gerät schützt Ihre Daten mit demselben Schutzniveau wie streng geheime Regierungsinformationen. Diese Sicherheitsfunktion ist immer aktiv und kann nicht deaktiviert werden.

Passwortgeschützt – Der Gerätezugriff ist durch einen Passwortschutz gesichert. Geben Sie Ihr Passwort an niemanden weiter, damit auch bei Verlust oder Diebstahl Ihres Geräts niemand außer Ihnen auf Ihre Daten zugreifen kann.

Geräte-Reset – Wenn der Advanced Encryption Controller physische Manipulationen feststellt oder wenn die Anzahl der aufeinanderfolgenden falschen Passworteingabeversuche 10 Versuche überschreitet, leitet das Gerät eine Reset-Sequenz ein. Wichtig – Wenn ein Gerät zurückgesetzt wird, werden alle gespeicherten Daten gelöscht und das Gerät wird auf die Werkseinstellungen zurückgesetzt – *vergessen Sie deshalb Ihr Passwort besser nicht*.

Anti-Malware-Autorun-Schutz – Ihr Gerät kann Sie vor vielen der neuesten Malware-Bedrohungen schützen, die auf USB-Sticks abzielen, indem es die Autorun-Ausführung von nicht zugelassenen Programmen erkennt und verhindert. Der Stick kann auch im Nur-Lese-Modus entsperrt werden, wenn Sie vermuten, dass der Host-Computer infiziert ist.

Einfache Geräteverwaltung – Ihr Gerät umfasst das IronKey-Bedienfeld, ein Programm, mit dem Sie auf Ihre Dateien zugreifen, das Gerät verwalten und seine Einstellungen bearbeiten, Ihr Gerätepasswort ändern und es sicher sperren können.

Auf welchen Systemen kann er verwendet werden?

- Windows® 11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x oder höher) Hinweis: Der Linux CLI Unlocker unterstützt keine Funktionen, die einen Netzwerkzugang erfordern, z. B. das Einrichten des Geräts oder das Ändern Ihres Passworts.

Einige Funktionen sind nur auf bestimmten Systemen verfügbar:

Nur Windows

- Geräte-Updates

Technische Daten

Weitere Details zu Ihrem Gerät finden Sie auf der Seite **Device Info** (Geräteinfo) im IronKey-Bedienfeld.

Spezifikationen	Details
Kapazität*	4GB, 8GB, 16GB, 32GB, 64GB, 128GB
Geschwindigkeit**	USB 3.2 Gen 1 - 4GB–32GB: 180MB/s Lesen; 80MB/s Schreiben - 64GB: 230MB/s Lesen; 160MB/s Schreiben - 128GB: 230MB/s Lesen; 240MB/s Schreiben USB 2.0: - 4GB–128GB: 40MB/s Lesen, 35MB/s Schreiben
Abmessungen	82,3 mm x 21,1 mm x 9,1 mm
Wasserdicht	Bis zu 0,90 cm; MIL-STD-810F
Temperatur	Betrieb: 0 bis 70°C; Lagerung: -40°C bis 85°C
Hardware-Datenverschlüsselung	256-Bit AES(XTS-Modus)
Zertifizierung	FIPS 140-2 Level 3-zertifiziert
Hardware	Mit USB 3.2 Gen 1-konform und mit USB 2.0 kompatibel

OS-Kompatibilität	- Windows 11, Windows 10 (erfordert zwei freie Laufwerksbuchstaben) - macOS 12.x – 15.x - Linux 4.4.x***
Garantie	5 Jahre eingeschränkte Garantie. Kostenloser technischer Support

Die in den USA entwickelten und montierten S1000B-Geräte benötigen keine Software- oder Treiberinstallation.

* Die angegebene Kapazität ist ein Richtwert. Es wird etwas Speicherplatz für die integrierte Software benötigt.
** Die Geschwindigkeit kann je nach Host-Hardware, -Software und Nutzung variieren.
*** Eingeschränkter Funktionsumfang.

Empfohlene bewährte Praktiken

1. Sperren des Geräts:
   - Bei Nichtgebrauch
   - Vor dem Herausziehen
   - Bevor das System in den Ruhezustand wechselt
2. Den Stick niemals herausziehen, wenn die LED leuchtet.
3. Geben Sie niemals Ihr Gerätepasswort an andere Personen weiter.
4. Führen Sie vor dem Einrichten und Verwenden des Geräts eine Virenprüfung des Computers durch.

Einrichten des Geräts

Um sicherzustellen, dass die Stromversorgung des verschlüsselten S1000B USB-Sticks ausreichend ist, schließen Sie ihn direkt an einem USB 2.0/3.2 Gen 1-Anschluss an einem Notebook oder PC an. Vermeiden Sie den Anschluss des USB-Sticks an Peripheriegeräte mit einem USB-Anschluss, wie z. B. eine Tastatur oder einen USB-Hub. Die Ersteinrichtung des Geräts muss unter einem unterstützten Windows- oder macOS-basierten Betriebssystem erfolgen.

Gerätezugriff (Windows-Umgebung)

1. Stecken Sie den verschlüsselten USB-Stick S1000B in einen freien USB-Anschluss am Notebook oder Desktop und warten Sie, bis Windows ihn erkennt.

   - Unter Windows 10 und 11 wird eine Nachricht über die Gerätetreiberinstallation angezeigt.

   - Windows fordert nach Abschluss der Hardware-Erkennung zum Starten der Geräteinstallation auf.

2. Wählen Sie die Option **IronKey.exe** in der IRONKEY-Partition, die Sie im Explorer finden können. Bitte beachten Sie, dass der Partitionsbuchstabe je nach dem nächsten freien Laufwerksbuchstaben variiert. Der Laufwerksbuchstabe kann sich ändern, je nachdem, welche Geräte angeschlossen sind. In der nachfolgenden Abbildung ist der Laufwerksbuchstabe (E:).

Gerätezugriff (macOS-Umgebung)

1. Stecken Sie den verschlüsselten USB-Stick S1000B in einen freien USB-Anschluss am macOS Notebook oder Desktop und warten Sie, bis das Betriebssystem ihn erkennt.

2. Doppelklicken Sie auf das **IRONKEY**-Laufwerk, das auf dem Desktop angezeigt wird, um den Initialisierungsprozess zu starten.

   - Wenn das IRONKEY-Laufwerk nicht auf dem Desktop angezeigt wird, öffnen Sie den Finder und suchen Sie nach dem Speichermedium IronKey-Laufwerk auf der linken Seite des Finder-Fensters (unter „Geräte“ aufgelistet). Markieren Sie das Laufwerk und doppelklicken Sie im Fenster „Finder“ auf das Anwendungssymbol IRONKEY. Dadurch wird der Installationsprozess gestartet.

Geräteinitialisierung

Initialisierung auf unterstützten Windows- oder macOS-Betriebssystemen.

1. Wählen Sie eine Spracheinstellung aus der Liste aus. Standardmäßig verwendet die Geräte-Software die Sprache Ihres Computer-Betriebssystems (falls verfügbar).

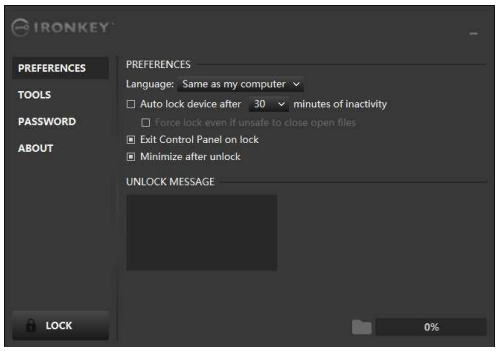
2. Lesen Sie die Lizenzvereinbarung durch, markieren Sie das Kontrollkästchen, um sie zu akzeptieren, und klicken Sie auf „Continue“.

3. Geben Sie in das Passwort-Textfeld ein Gerätepasswort ein und geben Sie dann Ihr Passwort erneut in das Textfeld „Confirm“ ein. Das Passwort schützt die Daten auf dem sicheren Laufwerk. Bei Passwörtern wird zwischen Groß- und Kleinschreibung unterschieden, und sie müssen aus mindestens 4 Zeichen (einschließlich Leerzeichen) bestehen.

4. Bei der Initialisierung unter Windows haben Sie die Möglichkeit, den IronKey Secure Files USB-Stick entweder als FAT32 , exFAT oder NTFS zu formatieren. Weitere Informationen finden Sie unter „Formatting My Device“.

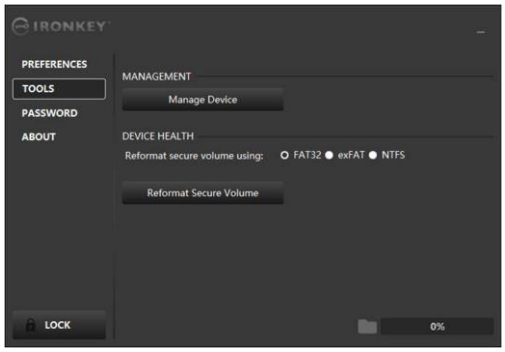
5. Standardmäßig ist die Option „Reset the device instead of self-destructing“ „Enabled (Aktiviert)“. Klicken Sie auf „Continue“. Die Initialisierung des Geräts ist abgeschlossen. Nach Abschluss des Vorgangs wird das IronKey-Bedienfeld geöffnet. Ihr Gerät ist nun bereit zum Speichern und Schützen Ihrer Daten.

IronKey-Bedienfeld



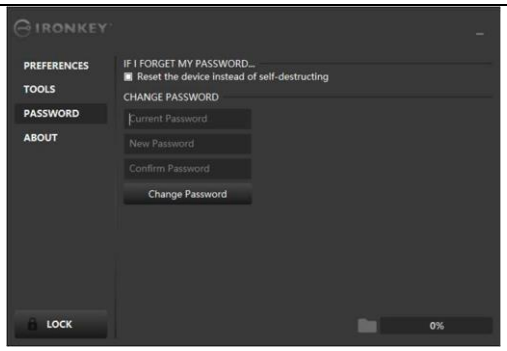
VOREINSTELLUNGEN

1. Language: Ändern der Gerätesprache
2. Auto lock device: Ändern des Timers für die Sperre
3. Exit on Control Panel on lock: Ändern des Verhaltens zum Verlassen oder Geöffnet halten des Bedienfelds, wenn das Gerät gesperrt ist.
4. Minimize after unlock: Ändern, ob das Bedienfeld minimiert werden soll, wenn das Gerät entsperrt ist, oder ob es maximiert bleiben soll.
5. UNLOCK MESSAGE: Hinzufügen einer Meldung, die im Anmeldefenster angezeigt werden soll.



TOOLS

1. MANAGEMENT: Verwalten des Geräts (SafeConsole erforderlich).
2. DEVICE HEALTH: Formatiert das sichere Laufwerk mit FAT32, exFAT oder NTFS neu. (macOS erlaubt nur die Formatierung mit FAT32)



PASSWORT

1. IF I FORGET MY PASSWORD...: Aktivieren bzw. Deaktivieren von „Reset the device instead of self- destructing“, dem Reset oder der Selbstzerstörung des Geräts.
2. CHANGE PASSWORD: Ändern des aktuelle Passworts in ein neues Passwort.

ÜBER

1. ABOUT THIS DEVICE: Listet Geräteinformationen auf.
2. Visit Website: Öffnet Kingstons Website
3. Legal Notices: Öffnet sowohl die Websites von Kingston und DataLocker mit rechtlichen Hinweisen
4. Certifications: Öffnet Kingstons Zertifikatsseite für verschlüsselte USB-Geräte

Verwendung des Geräts

Überprüfen der Gerätesicherheit

Wenn ein sicheres USB-Speichermedium verloren gegangen ist oder unbeaufsichtigt war, muss es gemäß der folgenden Benutzeranleitung überprüft werden. Das sichere USB-Speichergerät ist zu entsorgen, wenn der Verdacht besteht, dass ein Angreifer das Gerät manipuliert hat, oder wenn der Selbsttest fehlschlägt.

- Überprüfen Sie das sichere USB-Speichergerät visuell, um sicherzustellen, dass es keine Markierungen oder neue Kratzer aufweist, die auf eine Manipulation hindeuten könnten.
- Überprüfen Sie, ob das sichere USB-Speichergerät physisch intakt ist, indem Sie es leicht verdrehen.
- Stellen Sie sicher, dass das sichere USB-Speichergerät etwa 30 Gramm wiegt.
- Überprüfen Sie, ob die blaue Anzeigeleuchte des sicheren USB-Speichergeräts blinkt, wenn es an einen Computer angeschlossen ist (die richtige Frequenz ist 3 Mal pro Sekunde bei der ersten Verbindung und während Lese-/Schreibvorgängen).
- Überprüfen Sie, ob das sichere USB-Speichergerät als DVD-RW angezeigt wird und eine Speicherpartition erst gemountet wird, wenn das Gerät entsperrt ist.
- Überprüfen Sie, ob die Gerätesoftware auf dem virtuellen DVD-RW-Laufwerk von DataLocker Inc. herausgegeben wurde, bevor Sie sie ausführen.

Zugriff auf die sicheren Dateien

Nachdem das Gerät entsperrt wurde, haben Sie Zugriff auf Ihre sicheren Dateien. Dateien werden automatisch ver- und entschlüsselt, wenn diese auf dem Stick gespeichert oder geöffnet werden. Diese Technologie bietet Ihnen den Komfort des Arbeitens wie mit einem normalen Stick, während sie gleichzeitig eine starke „Immer-aktive“-Sicherheit bietet.

Zugriff auf die sicheren Dateien:

1. Klicken Sie auf das **Ordnersymbol**  in der unteren rechten Ecke des IronKey-Bedienfelds.

   - Windows: Öffnet den Windows Explorer mit dem IRONKEY SECURE FILES USB-Laufwerk.

   - macOS: Öffnet den Finder mit dem KINGSTON USB-Laufwerk.

2. Führen Sie einen der folgenden Schritte aus:

   - Zum Öffnen einer Datei doppelklicken Sie auf die Datei auf dem S1000B USB-Stick.

   - Zum Speichern einer Datei ziehen Sie die Datei von Ihrem Computer auf den S1000B USB-Stick.

Hinweis: Der Zugriff auf Ihre Dateien ist auch möglich, indem Sie mit der rechten Maustaste auf das **IronKey**-Symbol in der Windows-Taskleiste klicken und dann auf **Secure Files** (Sichere Dateien) klicken.

Entsperren im Nur-Lese-Modus

Der Stick lässt sich in einem schreibgeschützten Zustand entsperren, sodass Dateien auf dem sicheren Laufwerk nicht verändert werden können. Wenn Sie z. B. einen nicht vertrauenswürdigen oder unbekannten Computer verwenden, verhindert das Entsperren des Geräts im schreibgeschützten Modus, dass Malware auf diesem Computer Ihren Stick infiziert oder Ihre Dateien verändert.

Wenn Sie in diesem Modus arbeiten, zeigt das IronKey-Bedienfeld den Text „*Read-Only Mode*“ an. In diesem Modus können Sie keine Vorgänge durchführen, die das Ändern von Dateien auf dem Gerät beinhalten. Der Stick kann z. B. nicht neu formatiert oder Dateien auf dem Laufwerk bearbeitet werden.

Entsperren des USB-Sticks im Schreibschutz-Modus:

1. Schließen Sie das Gerät am USB-Anschluss des Host-Computers an und führen Sie die Datei **IronKey.exe** aus.

2. Markieren Sie das **Kontrollkästchen** „**Read-Only**“ unter dem Passwort-Eingabefeld.

3. Geben Sie Ihr Gerätepasswort ein und klicken Sie auf „**Unlock**“. Das IronKey-Bedienfeld wird mit dem Text „*Read-Only Mode*“ am unteren Rand angezeigt.

Ändern der Entsperrmeldung

Die Entsperrmeldung ist ein benutzerdefinierter Text, der im IronKey-Fenster angezeigt wird, wenn Sie das Gerät entsperren. Mit dieser Funktion können Sie die angezeigte Meldung anpassen. Wenn Sie z.B. Kontaktinformationen hinzufügen, werden Informationen angezeigt, wie ein verlorener Stick an Sie zurückgegeben werden kann.

Ändern der Entsperrmeldung:

1. Klicken Sie im IronKey-Bedienfeld in der Menüleiste auf „**Settings**“.

2. Klicken Sie in der linken Seitenleiste auf „**Preferences**“.

3. Geben Sie die Meldung in das Feld „Unlock Message“ ein. Der Text muss in den vorgesehenen Raum passen (ca. 6 Zeilen mit 200 Zeichen).

Bedienfeld verkleinern, wenn entsperrt

Wenn Ihr Gerät entsperrt ist, wird das Bedienfeld automatisch in die Taskleiste minimiert. Falls gewünscht, kann das Bedienfeld auch nach dem Entsperren des Geräts angezeigt werden.

Deaktivieren des Minimierens nach dem Entsperren:

1. Klicken Sie im IronKey-Bedienfeld in der linken Seitenleiste auf „Preferences“.
2. Klicken Sie auf das Kontrollkästchen für „Minimize after unlock“.

Sperren des Geräts

Sperren Sie Ihr Gerät, wenn es nicht benutzt wird, um unerwünschten Zugriff auf Ihre sicheren Dateien auf dem Stick zu verhindern. Das Gerät lässt sich manuell sperren oder es lässt sich so einstellen, dass es nach einer bestimmten Zeit der Inaktivität automatisch gesperrt wird.

Achtung: Wenn eine Datei oder Anwendung geöffnet ist, wenn das Gerät versucht, die automatische Sperre zu aktivieren, wird standardmäßig das Schließen der Anwendung oder Datei nicht erzwungen. Obwohl die Einstellung für die automatische Sperre so konfiguriert werden kann, dass das Gerät zwangsweise gesperrt wird, kann dies evtl. zu Datenverlusten bei allen geöffneten und nicht gespeicherten Dateien führen.

Wenn Ihre Dateien durch einen erzwungenen Sperrvorgang oder durch das Abziehen des Geräts vor dem Sperren beschädigt wurden, können Sie die Dateien möglicherweise wiederherstellen, indem Sie CHKDSK ausführen und Datenwiederherstellungssoftware verwenden (nur Windows).

Zum manuellen Sperren des Geräts:

1. Klicken Sie in der linken unteren Ecke des IronKey-Bedienfelds auf „**Lock**“, um das Gerät sicher zu sperren.

    - Sie können auch das folgende Tastaturkürzel verwenden: **CTRL + L** (nur Windows), oder klicken Sie mit der rechten Maustaste auf das **IronKey-Symbol** in der Taskleiste und klicken Sie auf „**Lock Device**“.

So legen Sie fest, dass ein Gerät automatisch gesperrt wird:

1. Entsperren Sie Ihr Gerät und klicken Sie in der Menüleiste des IronKey-Bedienfelds auf „**Settings**“.

2. Klicken Sie in der linken Seitenleiste auf „**Preferences**“.

3. Klicken Sie auf das **Kontrollkästchen** für die automatische Sperrung des Geräts und stellen Sie die Zeitüberschreitung auf eines der folgenden Zeitintervalle ein: 5, 15, 30, 60, 120 oder 180 Minuten.

So wird CHKDSK ausgeführt (nur Windows):

1. Entsperren Sie das Gerät.

2. Drücken Sie die WINDOWS-LOGO-TASTE + R, um die Eingabeaufforderung „Ausführen“ zu öffnen.

3. Geben Sie CMD ein und drücken Sie Eingabetaste (ENTER).

4. Geben Sie in der Eingabeaufforderung CHKDSK, den Buchstaben des IRONKEY SECURE FILES USB-Laufwerks und dann „/F /R“ ein. Wenn zum Beispiel der USB-Laufwerksbuchstabe von IRONKEY SECURE FILES „G“ ist, würden Sie Folgendes eingeben: CHKDSK G: /F /R

5. Verwenden Sie ggf. eine Datenrettungssoftware, um Ihre Dateien wiederherzustellen.

Bedienfeld beim Sperren verlassen

Wenn Ihr Gerät gesperrt ist, wird das Bedienfeld automatisch geschlossen. Um das Gerät zu entsperren und auf das Bedienfeld zuzugreifen, müssen Sie die IronKey-Anwendung erneut ausführen. Falls gewünscht, kann das Bedienfeld so eingestellt werden, dass es zum Entsperrfenster zurückkehrt, nachdem der Benutzer das Gerät gesperrt hat.

Deaktivieren von „Exit Control Panel on lock“:

1. Entsperren Sie Ihr Gerät und klicken Sie in der Menüleiste des IronKey-Bedienfelds auf „Settings“.

2. Klicken Sie in der linken Seitenleiste auf „Preferences“.

3. Klicken Sie auf das Kontrollkästchen neben „Exit Control Panel on Lock“.

Verwalten von Passwörtern

Ihr Passwort lässt sich auf dem Gerät ändern, indem Sie auf die Registerkarte „Password (Passwort)“ im IronKey-Bedienfeld zugreifen.

Manchmal kann es erforderlich sein, dass Sie Ihr Passwort ändern, um neuen Passwortrichtlinien des Unternehmens einzuhalten. Wenn eine Änderung erforderlich ist, wird der Bildschirm „Password Change (Passwort ändern)“ angezeigt, wenn Sie das Gerät das nächste Mal entsperren. Wenn das Gerät in Gebrauch ist, wird es gesperrt und Sie müssen das Passwort ändern, bevor Sie es wieder entsperren können.

Hinweis: Wenn ein Passwort erforderlich ist, z. B. bei der Anmeldung am Gerät oder bei einer manuellen Passwortänderung, können Sie die virtuelle Tastatur anstelle der physischen Tastatur zur Eingabe des Passworts verwenden.

Ändern des Passworts:

1. Entsperren Sie Ihr Gerät und klicken Sie in der Menüleiste auf „**Settings**“.

2. Klicken Sie in der linken Seitenleiste auf „**Password**“.

3. Geben Sie Ihr aktuelles Passwort in das vorgesehene Feld ein.

4. Geben Sie Ihr neues Passwort ein und bestätigen Sie es in den dafür vorgesehenen Feldern.

5. Klicken Sie auf „Change Password“.

Formatieren des Geräts

Ihr Gerät muss während der Initialisierung formatiert werden, bevor es zum Speichern von Dateien verwendet werden kann.

Bei der Initialisierung unter Windows haben Sie die Möglichkeit, den IRONKEY SECURE FILES USB-Stick entweder als FAT32, exFAT oder NTFS zu formatieren.

Die Optionen gelten nur für Windows-Betriebssysteme – macOS formatiert automatisch auf FAT32.

- FAT32
  - Vorteile: Plattformübergreifend kompatibel (Windows und macOS)
  - Nachteile: Begrenzt die individuelle Dateigröße auf 4GB
- exFAT
  - Vorteile: Keine Beschränkung der Dateigröße
  - Nachteile: Microsoft schränkt die Nutzung durch Lizenzverpflichtungen ein
- NTFS
  - Vorteile: Keine Beschränkung der Dateigröße
  - Nachteile: Wird mit Nur-Lese-Zugriff auf unterstützten macOS eingebunden

Nach der Initialisierung werden beim Neuformatieren des IRONKEY SECURE FILES USB-Sticks eine Schnellformatierung durchgeführt und ein leeres Laufwerk bereitgestellt, aber Ihr Gerätepasswort und Ihre Einstellungen werden nicht gelöscht.

Wichtig: Bevor Sie das Gerät neu formatieren, sichern Sie die Dateien Ihres IRONKEY SECURE FILES USB-Laufwerks an einem separaten Speicherort, z. B. auf einem Cloud-Speicher oder Ihrem Computer.
So wird ein Stick neu formatiert:

1. Entsperren Sie Ihr Gerät und klicken Sie in der Menüleiste des IronKey-Bedienfelds auf „**Settings**“.

2. Klicken Sie in der linken Seitenleiste auf „**Tools**“.

3. Wählen Sie unter Gerätezustand das Dateiformat aus und klicken Sie auf „**Reformat Secure Volume**“.

Informationen zum Gerät suchen

Verwenden Sie die Kapazitätsanzeige, die sich unten rechts im IronKey-Bedienfeld befindet. Dort wird angezeigt, wie viel Speicherplatz noch auf Ihrem Gerät verfügbar ist. Die grüne Balkengrafik zeigt an, wie voll der Speicher des Sticks ist. Zum Beispiel ist die Anzeige vollständig grün sein, wenn der Gerätespeicher voll ist. Der weiße Text auf der Kapazitätsanzeige zeigt an, wie viel freier Speicherplatz verbleibt.

Allgemeine Informationen zu Ihrem Gerät finden Sie auf der Seite „Device Info (Geräteinfo)“.

So werden Geräteinformationen angezeigt:

1. Entsperren Sie Ihr Gerät und klicken Sie in der Menüleiste des IronKey-Bedienfelds auf „**Settings**“.

2. Klicken Sie in der linken Seitenleiste auf „**Device Info**“.

Der Abschnitt „About This Device (Über dieses Gerät)“ enthält die folgenden Details über Ihren USB-Stick:

- Modellnummer
- Hardware-ID
- Seriennummer
- Software-Version
- Firmware-Version
- Veröffentlichungsdatum
- Laufwerksbuchstabe der sicheren Dateien
- IronKey-Laufwerksbuchstabe
- Betriebssystem und Systemverwaltungsrechte
- Verwaltungskonsole

Hinweis: Für den Besuch der IronKey-Website oder zum Abrufen weiterer Informationen zu rechtlichen Hinweisen oder Zertifizierungen für IronKey-Produkte klicken Sie auf eine der Informationsschaltflächen auf der Seite „Device Info (Geräteinfo)“.

Hinweis: Klicken Sie auf „**Copy**“, um die Geräteinformationen in die Zwischenablage zu kopieren, damit sie in eine E-Mail oder eine Support-Anfrage eingefügt werden können.

Zurücksetzen des Geräts

Ihr Gerät kann auf die Werkseinstellungen zurückgesetzt werden. Dadurch werden alle Daten sicher vom Gerät gelöscht und für die nächste Verwendung wird ein neuer Sicherheitsschlüssel erstellt.

Zurücksetzen des Geräts:

1. Entsperren Sie das Gerät.

2. Rechtsklicken Sie auf das **IronKey-Symbol** in der Taskleiste.

3. Klicken Sie auf „Reset Device“.

Um ein versehentliches Zurücksetzen des Geräts zu verhindern, wird ein Popup-Fenster angezeigt, dass zur Eingabe von vier zufälligen Ziffern auffordert. Nach dem Eingeben der Bestätigung wird das Gerät nun auf die Werkseinstellungen zurückgesetzt.

Verwenden des Geräts unter Linux

Sie können Ihr Gerät auf mehreren Linux-Distributionen verwenden. Im Linux-Ordner befinden sich zwei ausführbare Dateien, Unlocker_32.exe und Unlocker_64.exe. Ersetzen Sie für diese Anleitung Unlocker_xx.exe durch die ausführbare Datei, die mit Ihrem System kompatibel ist.

Das Gerät muss zuvor mit einem Windows- oder macOS-Betriebssystem eingerichtet worden sein. Weitere Informationen finden Sie unter „Setting Up My Device“.

Verwenden von „Unlocker“

Verwenden Sie die Datei Unlocker_xx.exe für Linux, um auf Ihre Dateien zuzugreifen. Abhängig von Ihrer Linux-Distribution benötigen Sie möglicherweise Root-Rechte, um das Programm Unlocker_xx.exe zu verwenden, das sich im Linux-Ordner des gemounteten öffentlichen Laufwerks befindet. Standardmäßig fügen die meisten Linux-Distributionen das Execute-Bit an .exe-Dateien auf einer Fat32-Partition an. Andernfalls muss das Ausführungsbit vor der Ausführung manuell gesetzt werden, indem Sie die folgenden Befehle verwenden.

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

Wenn Sie nur ein Gerät an das System angeschlossen haben, führen Sie das Programm von einer Befehls-Shell ohne Argumente aus (z. B. Unlocker_xx.exe). Daraufhin werden Sie aufgefordert, Ihr Gerätepasswort einzugeben, um das Laufwerk zu entsperren. Wenn mehrere Geräte angeschlossen sind, müssen Sie angeben, welches entsperrt werden soll.

Dies sind die verfügbaren Parameter für die Gerätesoftware:

Optionen:

```
-h, -help         Hilfe
-l, -lock         Gerät sperren
-r, -readonly     Als schreibgeschützt entsperren
```

Hinweis: Unlocker_xx.exe entsperrt nur den IRONKEY SECURE FILES USB-Stick und dieser muss dann eingebunden werden. Viele moderne Linux-Distributionen führen dies automatisch aus. Falls nicht, führen Sie das Mount-Programm von der Befehlszeile aus und verwenden Sie dabei den von Unlocker_xx.exe ausgegebenen Gerätenamen.

Durch einfaches Entkoppeln des Geräts wird der IRONKEY SECURE FILES USB nicht automatisch gesperrt. Zum Entsperren des Geräts müssen Sie es entweder entkoppeln und physisch entfernen (ausstecken) oder Folgendes ausführen:

- Unlocker_xx.exe -l

Bitte beachten Sie die folgenden wichtigen Hinweise für den Einsatz Ihres Gerätes unter Linux:

1. Die Kernel-Version muss 4.4.x oder höher sein.
2. Einbinden
   - Überprüfen Sie, ob Sie über die Berechtigung verfügen, externe SCSI- und USB-Geräte einzubinden.
   - Einige Distributionen binden Geräte nicht automatisch ein und erfordern die Ausführung des folgenden Befehls: mount /dev/[Name des Geräts] /media/[Name des eingebundenen Geräts]

3. Der Name des eingebundenen Geräts variiert je nach Distribution.

4. Berechtigungen

   - Sie müssen über die Berechtigung zum Mounten von external/usb/devices verfügen.
   - Außerdem müssen Sie über die Berechtigung verfügen, eine ausführbare Datei vom öffentlichen Datenträger auszuführen, um den Unlocker zu starten.
   - Möglicherweise benötigen Sie Root-Benutzerrechte.

5. IronKey for Linux unterstützt x86- und x86_64-Systeme.

Wo kann man Hilfe erhalten?

Die folgenden Ressourcen bieten weitere Informationen über IronKey-Produkte. Sollten Sie Fragen haben, wenden Sie sich bitte an den Kingston Support.

- kingston.com/usb/encrypted_security: Informationen, Marketingmaterial und Video-Anleitungen.
- kingston.com/support: Produktunterstützung, Häufig gestellte Fragen und Downloads

HINWEIS: IronKey haftet nicht für technische oder redaktionelle Fehler und/oder Auslassungen, die hierin enthalten sind, und auch nicht für zufällige oder Folgeschäden, die aus der Bereitstellung oder Verwendung dieses Materials resultieren. Die hierin enthaltenen Informationen können ohne vorherige Ankündigung geändert werden. Die in diesem Dokument enthaltenen Informationen stellen die aktuelle Auffassung von IronKey zu dem behandelten Thema zum Zeitpunkt der Veröffentlichung dar. IronKey kann nicht für die Richtigkeit von Informationen garantieren, die nach dem Datum der Veröffentlichung präsentiert werden. Dieses Dokument dient nur zu Informationszwecken. IronKey gibt in diesem Dokument keine ausdrücklichen oder stillschweigenden Garantien. IronKey und das IronKey-Logo sind Marken von Kingston Digital, Inc. und deren Tochtergesellschaften. Alle anderen Marken sind Eigentum ihrer jeweiligen Besitzer. IronKey™ ist eine eingetragene Marke von Kingston Technologies und wird mit Genehmigung von Kingston Technologies verwendet. Alle Rechte vorbehalten.

FCC-Informationen Dieses Gerät entspricht Teil 15 der FCC-Vorschriften. Seine Inbetriebnahme unterliegt den folgenden beiden Bedingungen: (1) Dieses Gerät darf keine störenden Interferenzen verursachen; und (2) dieses Gerät muss alle empfangenen Interferenzen tolerieren, einschließlich Störungen, die nicht gewünschte Operationen zur Folge haben können. Dieses Gerät wurde getestet und hat die in Teil 15 der FCC-Regeln festgelegten Grenzwerte für ein Digitalgerät der Klasse B erfüllt. Diese Grenzwerte dienen dazu, einen angemessenen Schutz vor störenden Interferenzen in einer häuslichen Installation zu bieten. Dieses Gerät erzeugt und nutzt Energie in Form von Radiowellen, kann diese ausstrahlen und kann bei einer nicht sachgemäßen Installation und Verwendung Funkübertragungen stören. Es kann jedoch keine Garantie dafür gegeben werden, dass in einer bestimmten Installation keine Interferenzen auftreten. Sollte das Gerät den Radio- oder Fernsehempfang stören, was leicht durch Ein- und Ausschalten des Geräts überprüft werden kann, wird dem Anwender empfohlen, zu versuchen, die Interferenzen durch folgende Maßnahmen zu beheben:

- Richten Sie die Antenne neu aus oder wechseln Sie ihre Position.
- Vergrößern Sie den Abstand zwischen Gerät und Empfänger.
- Schließen Sie das Gerät an einen anderen Stromkreis an als denjenigen, an den der Empfänger angeschlossen ist.
- Wenden Sie sich an Ihren Fachhändler oder einen erfahrenen Radio-/TV-Techniker.

Hinweis: Änderungen oder Modifizierungen des Geräts, die nicht ausdrücklich von der für die Zulassung zuständigen Partei genehmigt wurden, können den Entzug der Betriebsgenehmigung des Benutzers für das Gerät zur Folge haben.

Dokument Nr. S1000B11062023

IRONKEY™ S1000B
CLÉ USB CHIFFRÉE 3.2 Gen 1

Manuel d'utilisation

Sommaire

À propos de ce Manuel (04152025)

L'IronKey™ S1000B est une clé non managed.

Procédures initiales

Windows 11, 10 et macOS 12.x – 15.x

1. Branchez l'appareil sur le port USB de votre ordinateur.
2. Lorsque la fenêtre de configuration de l'appareil s'affiche, suivez les instructions à l'écran. Si cette fenêtre ne s'affiche pas, ouvrez-la manuellement :
    - Windows : Démarrer > Mon ordinateur > IronKey Unlocker > IronKey.exe
    - macOS : Finder > IRONKEY > IronKey.app
3. Lorsque l'installation de l'appareil est terminée, vous pouvez déplacer vos fichiers importants sur la clé USB IRONKEY SECURE FILES, et ils seront automatiquement chiffrés.

Certains systèmes Windows invitent à redémarrer après avoir branché votre appareil pour la première fois. Vous pouvez fermer cette invite en toute sécurité sans redémarrer : aucun nouveau pilote ou logiciel n'est installé.

À propos de mon appareil

L'IronKey S1000B USB 3.2 Gen 1 est une clé USB avec sécurité par mot de passe et chiffrement des données intégrés. Sa conception intègre le chiffrement avancé AES 256 bits ainsi que d'autres fonctionnalités qui renforcent la sécurité des données mobiles. Vous pouvez désormais transporter vos fichiers et vos données en toute sécurité, où que vous alliez.

En quoi est-elle différente d'une clé USB ordinaire ?

Certification FIPS 140-2 de niveau 3 – L'IronKey S1000B étant un appareil certifié FIPS, vous avez la garantie de respecter les exigences réglementaires.

Chiffrement matériel – Le contrôleur de chiffrement avancé de votre appareil protège vos données avec le même niveau de protection que les informations gouvernementales hautement classifiées. Cette technologie de sécurité est toujours active et ne peut pas être désactivée.

Protection par mot de passe – L'accès à l'appareil est sécurisé par un mot de passe. Ne communiquez votre mot de passe à personne afin que, même en cas de perte ou de vol de votre appareil, personne d'autre ne puisse accéder à vos données.

Réinitialisation de l'appareil – Si le contrôleur de chiffrement avancé détecte une altération physique ou si le nombre de saisies de mot de passe incorrect dépasse 10, l'appareil lance une séquence de réinitialisation. Important – Lorsqu'un appareil est réinitialisé, toutes les données qu'il contient sont effacées et l'appareil revient aux paramètres d'usine. *Il est donc essentiel de ne pas oublier votre mot de passe*.

Protection contre l'exécution automatique de programmes malveillants – Votre appareil peut vous protéger contre les derniers programmes malveillants ciblant les clés USB en détectant et en empêchant l'exécution automatique de programmes non approuvés. Il peut également être déverrouillé en mode lecture seule si vous pensez que l'ordinateur hôte est infecté.

Gestion simplifiée – Votre appareil intègre un panneau de contrôle IronKey, un programme permettant d'accéder à vos fichiers, de gérer votre appareil, de modifier vos préférences, de changer le mot de passe de votre appareil et de le verrouiller en toute sécurité.

Avec quels systèmes puis-je l'utiliser ?

- Windows® 11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x ou supérieur) Remarque : Linux CLI Unlocker ne prend pas en charge les fonctionnalités qui nécessitent un accès au réseau, par exemple la configuration de votre appareil ou la modification de votre mot de passe.

Certaines fonctionnalités ne sont disponibles que sur certains systèmes spécifiques :

Windows uniquement

- Mises à jour de l'appareil

Caractéristiques techniques

Pour plus de détails sur votre appareil, consultez la page **d'informations sur l'appareil** dans le panneau de contrôle IronKey.

Caractéristiques	Détails
Capacité*	4 Go, 8 Go, 16 Go, 32 Go, 64 Go, 128 Go
Vitesse**	USB 3.2 Gen 1 - 4 Go-32 Go : 180 Mo/s en lecture, 80 Mo/s en écriture - 64 Go : 230 Mo/s en lecture, 160 Mo/s en écriture - 128 Go : 230 Mo/s en lecture, 240 Mo/s en écriture USB 2.0 : - 4 Go-128 Go : 40 Mo/s en lecture, 35 Mo/s en écriture
Dimensions	82,3 mm x 21,1 mm x 9,1 mm
Étanche	Jusqu'à 1 mètre ; MIL-STD-810F
Température :	Fonctionnement : 0°C à 70°C ; Stockage : -40°C à 85°C
Chiffrement matériel	AES 256 bits (mode XTS)
Certification	FIPS 140-2 de niveau 3
Matériel	Compatible USB 3.2 Gen 1 et USB 2.0

Compatibilité SE	- Windows 11, Windows 10 (nécessite deux lettres de lecteur libres) - macOS 12.x – 15.x - Linux 4.4.x***
Garantie	Garantie de 5 ans. Assistance technique gratuite

Conçues et assemblées aux États-Unis, les clés USB S1000B ne nécessitent l'installation d'aucun logiciel ou pilote.

* La capacité annoncée est approximative. Un espace est nécessaire pour le logiciel embarqué.
** La vitesse peut varier selon la configuration matérielle ou logicielle de l'hôte et l'utilisation du produit.
*** Ensemble de fonctionnalités limité.

Meilleures pratiques recommandées

1. Verrouiller l'appareil :
   - lorsqu'il n'est pas utilisé
   - avant de le débrancher
   - avant que le système ne passe en mode veille
2. Ne débranchez jamais l'appareil lorsque le voyant est allumé.
3. Ne communiquez jamais le mot de passe de votre appareil.
4. Effectuez une analyse antivirus de votre ordinateur avant de configurer et d'utiliser l'appareil.

Configurer mon appareil

Pour vous assurer que la clé USB chiffrée S1000B est suffisamment alimentée, insérez-la directement dans un port USB 2.0/3.2 Gen 1 d'un ordinateur portable ou d'un ordinateur de bureau. Évitez de la connecter à tout appareil périphérique doté d'un port USB, comme un clavier ou un concentrateur alimenté par USB. La configuration initiale de l'appareil doit être effectuée sur un système d'exploitation Windows ou macOS pris en charge.

Accès à l'appareil (environnement Windows)

1. Branchez la clé USB chiffrée S1000B sur un port USB disponible de l'ordinateur portable ou de bureau et attendez que Windows la détecte.

   - Les utilisateurs de Windows 11 et 10 recevront une notification de pilote de périphérique.

   - Une fois la détection du nouveau matériel terminée, Windows vous demandera de commencer le processus d'initialisation.

2. Dans l'Explorateur de fichiers, sélectionnez le fichier **IronKey.exe** à l'intérieur de la partition IRONKEY. Veuillez noter que la lettre de la partition variera en fonction de la prochaine lettre de lecteur libre. La lettre du lecteur peut changer en fonction des périphériques connectés. Dans l'image ci-dessous, la lettre du lecteur est (E:).

Accès à l'appareil (environnement macOS)

1. Branchez la clé USB chiffrée S1000B dans un port USB disponible de l'ordinateur portable ou de bureau macOS et attendez que le système d'exploitation la détecte.

2. Double-cliquez sur le volume **IRONKEY** qui apparaît sur le bureau pour lancer le processus d'initialisation.

   - Si le volume IRONKEY n'apparaît pas sur le bureau, ouvrez le Finder et localisez le volume IronKey sur le côté gauche de la fenêtre du Finder (répertorié sous Appareils). Mettez le volume en surbrillance et double-cliquez sur l'icône de l'application IRONKEY dans la fenêtre du Finder. Cela lancera le processus d'initialisation.

Initialisation de la clé USB

Initialisation sur un système d'exploitation Windows ou macOS pris en charge.

1. Sélectionnez une langue dans la liste. Par défaut, le logiciel de l'appareil utilisera la même langue que le système d'exploitation de votre ordinateur (si disponible).

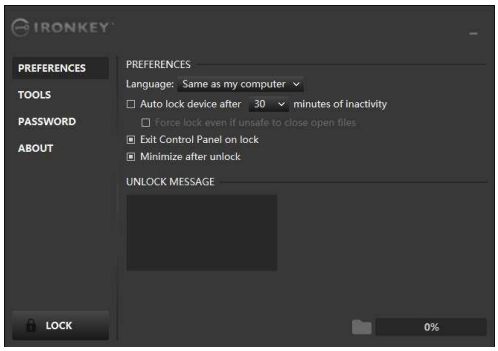
2. Lisez l'accord de licence, cochez la case pour l'accepter et cliquez sur Continue (Continuer).

3. Dans la zone de texte Password (Mot de passe), saisissez un mot de passe pour l'appareil, puis saisissez à nouveau votre mot de passe dans la zone de texte Confirm (Confirmer). Le mot de passe protège les données sur la clé sécurisée. Les mots de passe sont sensibles à la casse et doivent comporter au moins 4 caractères (espace inclus).

4. Si vous effectuez l'initialisation sous Windows, vous aurez la possibilité de formater la clé USB Ironkey Secure Files en FAT32, exFAT ou NTFS. Pour plus d'informations, voir Formater mon appareil.

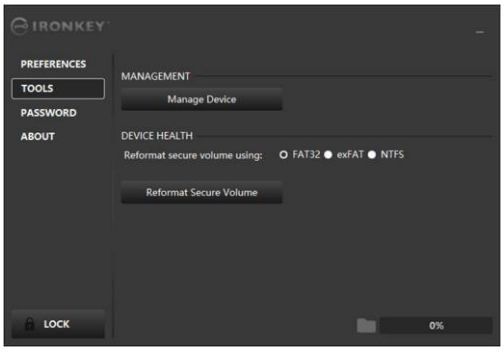
5. Par défaut, l'option « Reset the device instead of self-destructing » (Réinitialiser l'appareil au lieu de l'autodétruire) est activée. Cliquez sur Continue (Continuer). L'appareil terminera son initialisation. Une fois cette opération terminée, le panneau de contrôle IronKey s'ouvrira. Votre appareil est désormais prêt à stocker et à protéger vos données.

Panneau de contrôle IronKey



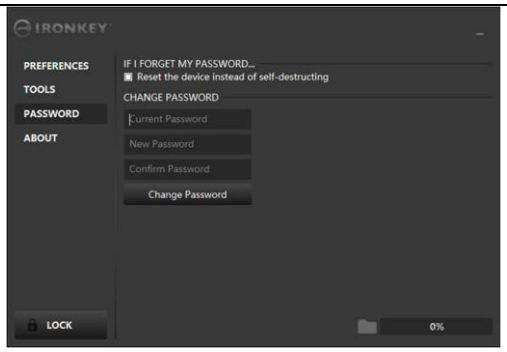
PRÉFÉRENCES

1. Language (Langue) : Changer la langue de l'appareil
2. Auto lock device (Verrouiller l'appareil automatiquement) : Modifier le délai de verrouillage
3. Exit on Control Panel on lock (Quitter le panneau de contrôle au verrouillage) : Quitterr le panneau de contrôle ou le laisser ouvert lorsque l'appareil est verrouillé.
4. Minimize after unlock (Réduire après le déverrouillage) : Modifier pour minimiser le panneau de configuration lorsque l'appareil est déverrouillé ou l'autoriser à rester maximisé.
5. UNLOCK MESSAGE (MESSAGE DE DÉVERROUILLAGE) : Ajouter un message qui s'affichera dans la fenêtre de connexion.



TOOLS (OUTILS)

1. MANAGEMENT (GESTION) : Gérer l'appareil (SafeConsole requise).
2. DEVICE HEALTH (SANTÉ DE L'APPAREIL) : Reformater le volume sécurisé en utilisant FAT32, exFAT ou NTFS (macOS ne permet que le formatage FAT32).



PASSWORD (MOT DE PASSE)

1. IF I FORGET MY PASSWORD (EN CAS D'OUBLI DU MOT DE PASSE) : Activer/Désactiver l'option « Reset the device instead of self-destructing » (Réinitialiser l'appareil au lieu de l'autodétruire).
2. CHANGE PASSWORD (MODIFIER LE MOT DE PASSE) : Remplacer le mot de passe actuel par un nouveau mot de passe.

ABOUT (À PROPOS)

1. ABOUT THIS DEVICE (À PROPOS DE CET APPAREIL) : Répertorie les informations relatives à l'appareil.
2. Visit Website (Accéder au site web) : Lance le site web de Kingston.
3. Legal Notices (Mentions légales) : Lance les sites web des mentions légales de Kingston et de DataLocker.
4. Certifications : Lance la page des certificats Kingston pour les appareils USB chiffrés.

Utiliser mon appareil

Vérifier la sécurité de l’appareil

Si un appareil de stockage USB sécurisé a été perdu ou laissé sans surveillance, il doit être vérifié conformément aux conseils d’utilisation suivants. Le dispositif de stockage USB sécurisé doit être mis au rebut si on soupçonne qu'un pirate a manipulé le dispositif ou si l'autotest échoue.

- Vérifiez visuellement que l’appareil de stockage USB sécurisé ne présente pas de marques ou de nouvelles rayures susceptibles d’indiquer une altération.
- Vérifiez que l’appareil de stockage USB sécurisé est physiquement intact en le tournant légèrement.
- Vérifiez que l’appareil de stockage USB sécurisé pèse environ 30 grammes.
- Vérifiez que, lorsqu’il est branché sur un ordinateur, le voyant bleu de l’appareil de stockage USB sécurisé clignote (la fréquence correcte est de 3 fois par seconde lors de la connexion initiale et pendant les opérations de lecture/écriture).
- Vérifiez que l’appareil de stockage USB sécurisé s’affiche comme un DVD-RW et qu’aucune partition de stockage n’est montée tant que l’appareil n’est pas déverrouillé.
- Vérifiez que le logiciel de l’appareil sur le lecteur DVD-RW virtuel est émis par DataLocker Inc avant de l’exécuter.

Accès à mes fichiers sécurisés

Après avoir déverrouillé l'appareil, vous pouvez accéder à vos fichiers sécurisés. Les fichiers sont automatiquement chiffrés et déchiffrés lorsque vous les enregistrez ou les ouvrez sur l'appareil. Cette technologie vous permet de travailler comme vous le feriez avec un lecteur ordinaire, tout en offrant une sécurité élevée et permanente.

Pour accéder à vos fichiers sécurisés :

1. Cliquez sur **l'icône de dossie**r  dans le coin inférieur droit du panneau de contrôle IronKey.

   - Windows : Ouvre l'Explorateur Windows et affiche le lecteur IRONKEY SECUREFILESUSB.

   - macOS : Ouvre le Finder et affiche le lecteur USB KINGSTON.

2. Effectuez l'une des opérations suivantes :

   - Pour ouvrir un fichier, double-cliquez sur le fichier souhaité sur le lecteur S1000BUSB.

   - Pour enregistrer un fichier, faites glisser le fichier de votre ordinateur vers le lecteur S1000BUSB.

Conseil : Vous pouvez également accéder à vos fichiers en cliquant avec le bouton droit de la souris sur **l'icône IronKey** dans la barre des tâches de Windows, et en cliquant sur **Fichiers sécurisés**.

Déverrouillage en mode lecture seule

Vous pouvez déverrouiller votre appareil en mode lecture seule afin que les fichiers ne puissent pas être modifiés sur votre lecteur sécurisé. Par exemple, lorsque vous utilisez un ordinateur non fiable ou inconnu, le déverrouillage de votre appareil en mode lecture seule empêchera tout programme malveillant sur cet ordinateur d'infecter votre appareil ou de modifier vos fichiers.

Lorsque vous travaillez dans ce mode, le panneau de contrôle IronKey affiche le texte *Read-Only Mode* (Mode lecture seule). Dans ce mode, vous ne pouvez pas effectuer d'opérations impliquant la modification de fichiers sur l'appareil. Par exemple, vous ne pouvez pas reformater l'appareil ou modifier des fichiers sur le lecteur.

Pour déverrouiller l'appareil en mode lecture seule :

1. Insérez l'appareil dans le port USB de l'ordinateur hôte et exécutez le fichier **IronKey.exe**.

2. Cochez la **case Read-Onl**y (Lecture seule) sous le champ de saisie du mot de passe.

3. Saisissez le mot de passe de votre appareil et cliquez sur **Unlock** (Déverrouiller). Le panneau de contrôle IronKey apparaîtra avec le texte *Read-Only Mode* (Mode lecture seule) en bas.

Modifier le message de déverrouillage

Le message de déverrouillage est un texte personnalisé qui s'affiche dans la fenêtre IronKey lorsque vous déverrouillez l'appareil. Cette fonction vous permet de personnaliser le message qui s'affiche. Par exemple, lorsque vous ajoutez des coordonnées d'un contact, des instructions s'afficheront pour vous expliquer comment un appareil perdu peut vous être rendu.

Pour modifier le message de déverrouillage :

1. Dans la barre de menu du panneau de contrôle IronKey, cliquez sur **Settings** (Paramètres).
2. Dans la barre latérale gauche, cliquez sur **Preferences** (Préférences).
3. Saisissez le message dans le champ Unlock Message (Message de déverrouillage). Le texte doit tenir dans l'espace prévu (environ 6 lignes et 200 caractères).

Réduire le panneau de contrôle au déverrouillage

Lorsque votre appareil est déverrouillé, le panneau de contrôle est automatiquement réduit dans la barre des tâches. Si vous le souhaitez, le panneau de contrôle peut rester affiché après le déverrouillage de l'appareil.

Pour désactiver l'option Minimize after unlock (Réduire après le déverrouillage) :

1. Dans la barre latérale gauche du panneau de contrôle IronKey, cliquez sur Preferences (Préférences).
2. Cochez la case Minimize after unlock (Réduire après le déverrouillage).

Verrouiller l'appareil

Verrouillez votre appareil lorsque vous ne l'utilisez pas afin d'empêcher tout accès indésirable à vos fichiers sécurisés sur le lecteur. Vous pouvez verrouiller manuellement l'appareil ou le configurer pour qu'il se verrouille automatiquement après une période d'inactivité donnée.

Avertissement : Par défaut, si un fichier ou une application est ouvert lorsque l'appareil tente de se verrouiller automatiquement, cela ne forcera pas la fermeture de l'application ou du fichier. Bien que vous puissiez configurer le paramètre de verrouillage automatique pour forcer l'appareil à se verrouiller, vous risquez de perdre les données de tous les fichiers ouverts et non enregistrés.

Si vos fichiers ont été corrompus à la suite d'une procédure de verrouillage forcé ou parce que vous avez débranché l'appareil avant de le verrouiller, vous pourrez peut-être récupérer les fichiers en exécutant CHKDSK et en utilisant le logiciel de récupération de données (Windows uniquement).

Pour verrouiller l'appareil manuellement :

1. Pour verrouiller votre appareil en toute sécurité, cliquez sur **Lock** (Verrouiller) dans le coin inférieur gauche du panneau de contrôle IronKey.
    - Vous pouvez également utiliser le raccourci clavier **CTRL + L** (Windows uniquement), ou cliquer avec le bouton droit de la souris sur **l'icône IronKey** dans la barre d'état système et cliquer sur **Verrouiller l'appareil**.

Pour configurer un appareil afin qu'il se verrouille automatiquement :

1. Déverrouillez votre appareil et cliquez sur **Settings** (Paramètres) dans la barre de menu du panneau de contrôle IronKey.

2. Dans la barre latérale gauche, cliquez sur **Preferences** (Préférences).
3. Cliquez sur la **case à cocher** du verrouillage automatique de l'appareil et définissez le délai d'attente sur l'un des intervalles de temps suivants : 5, 15, 30, 60, 120 ou 180 minutes.

Pour exécuter CHKDSK (Windows uniquement) :

1. Déverrouillez l'appareil.
2. Appuyez sur les touches LOGO WINDOWS + R pour ouvrir l'invite Exécuter.
3. Saisissez CMD et appuyez sur ENTRÉE.
4. Dans l'invite de commande, saisissez CHKDSK, la lettre de la clé USB IRONKEY SECURE FILES, puis « /F /R ». Par exemple, si la lettre de la clé USB IRONKEY SECURE FILES est G, vous devez saisir : CHKDSK G: /F /R
5. Utilisez un logiciel de récupération de données, si nécessaire, pour récupérer vos fichiers.

Quitter le panneau de contrôle au verrouillage

Lorsque votre appareil est verrouillé, le panneau de contrôle se ferme automatiquement. Pour déverrouiller l'appareil et accéder au panneau de contrôle, vous devrez exécuter à nouveau l'application IronKey. Si vous le souhaitez, le panneau de contrôle peut être configuré pour revenir à l'écran de déverrouillage après que l'utilisateur ait verrouillé l'appareil.

Pour désactiver la fermeture du panneau de contrôle au verrouillage :

1. Déverrouillez votre appareil et cliquez sur Settings (Paramètres) dans la barre de menu du panneau de contrôle IronKey.
2. Dans la barre latérale gauche, cliquez sur Preferences (Préférences).
3. Cliquez sur la case Exit Control Panel on lock (Quitter le panneau de contrôle au verrouillage).

Gestion des mots de passe

Pour modifier le mot de passe de votre appareil, accédez à l'onglet Password (Mot de passe) dans le panneau de contrôle IronKey.

Il peut arriver que vous deviez modifier votre mot de passe pour vous conformer aux nouvelles politiques de mot de passe de l'entreprise. Si une modification est nécessaire, l'écran de modification du mot de passe s'affichera au prochain déverrouillage de l'appareil. Si l'appareil est en cours d'utilisation, il se verrouillera et vous devrez modifier le mot de passe avant de pouvoir le déverrouiller.

Remarque : Lorsqu'un mot de passe est requis, par exemple lors de la connexion à l'appareil ou lors d'une opération manuelle de changement de mot de passe, vous pouvez utiliser le clavier virtuel au lieu du clavier réel pour saisir le mot de passe.

Pour modifier votre mot de passe :

1. Déverrouillez votre appareil et cliquez sur **Settings** (Paramètres) dans la barre de menu.
2. Cliquez sur **Password** (Mot de passe) dans la barre latérale gauche.
3. Saisissez votre mot de passe actuel dans le champ prévu à cet effet.

4. Saisissez votre nouveau mot de passe et confirmez-le dans les champs prévus à cet effet.
5. Cliquez sur Change Password (Modifier le mot de passe).

Formater mon appareil

Votre appareil devra être formaté lors de l'initialisation avant de pouvoir être utilisé pour stocker des fichiers.

Si vous effectuez l'initialisation sous Windows, vous aurez la possibilité de formater la clé USB IRONKEY SECURE FILES FAT32, exFAT ou NTFS.

Les options ne concernent que les systèmes d'exploitation Windows ;- macOS la formatera automatiquement en FAT32.

- FAT32
  - Avantages : Compatibilité multiplateforme (Windows et mac OS)
  - Inconvénients : Taille des fichiers individuels limitée à 4 Go
- exFAT
  - Avantages : Aucune limitation quant à la taille des fichiers
  - Inconvénients : Microsoft en restreint l'utilisation en fonction des obligations de licence
- NTFS
  - Avantages : Aucune limitation quant à la taille des fichiers
  - Inconvénients : Monté en lecture seule sur les systèmes d'exploitation macOS pris en charge

Après l'initialisation, le reformatage de la clé USB IRONKEY SECURE FILES effectuera un formatage rapide et produira une clé vide, mais n'effacera pas le mot de passe et les paramètres de votre appareil.

Important : Avant de reformater l'appareil, procédez à une sauvegarde de votre clé USB IRONKEY SECURE FILES dans un autre emplacement, par exemple dans un stockage cloud ou sur votre ordinateur. Pour reformater un appareil :

1. Déverrouillez votre appareil et cliquez sur **Settings** (Paramètres) dans la barre de menu du panneau de contrôle IronKey.
2. Cliquez sur **Tools** (Outils) dans la barre latérale gauche.
3. Sous Device Health (Santé de l'appareil), sélectionnez le format de fichier et cliquez sur **Reformat Secure Volume** (Reformater le volume sécurisé).

Afficher les informations sur mon appareil

Utilisez le compteur de capacité, situé en bas à droite du panneau de contrôle IronKey, pour voir combien d'espace de stockage est encore disponible sur votre appareil. Le graphique à barres vertes représente le degré de saturation de l'appareil. Ainsi, le compteur est totalement vert lorsque l'appareil est saturé. Le texte blanc sur le compteur de capacité indique l'espace libre restant.

Pour obtenir des informations générales sur votre appareil, consultez la page Device Info (Infos sur l'appareil).

Pour afficher les informations sur l'appareil :

1. Déverrouillez votre appareil et cliquez sur **Settings** (Paramètres) dans la barre de menu du panneau de contrôle IronKey.

2. Cliquez sur **Device Info** (Infos sur l'appareil) dans la barre latérale gauche.

La section About This Device (À propos de cet appareil) affiche les informations suivantes sur votre appareil :

- Numéro de modèle
- ID du matériel
- Numéro de série
- Version du logiciel
- Version du firmware
- Date de publication
- Lettre de lecteur des fichiers sécurisés
- Lettre de lecteur IronKey
- Système d'exploitation et privilèges d'administration du système
- Console de gestionModel Number

Remarque : Pour visiter le site web d'IronKey ou accéder à plus d'informations sur les mentions légales ou les certifications des produits IronKey, cliquez sur l'un des boutons d'information de la page Device Inf (Infos sur l'appareil).

Conseil : Cliquez sur **Copy** (Copier) pour copier les informations sur l'appareil dans le presse-papiers afin de pouvoir les coller dans un e-mail ou une demande d'assistance.

Réinitialiser mon appareil

Les valeurs par défaut de votre appareil peuvent être rétablies. Cette opération efface toutes les données de l'appareil en toute sécurité, et une nouvelle clé de sécurité est créée pour la prochaine utilisation.

Réinitialiser votre appareil :

1. Déverrouillez votre appareil.

2. Cliquez avec le bouton droit de la souris sur **l'icône IronKey** dans la barre d'état système.

3. Cliquez sur Reset Device (Réinitialiser l'appareil).

Pour éviter les réinitialisations accidentelles de l'appareil, une fenêtre contextuelle vous demandera d'entrer quatre chiffres au hasard. Après votre confirmation, l'appareil sera réinitialisé aux paramètres d'usine.

Utiliser mon appareil sous Linux

Vous pouvez utiliser votre appareil avec plusieurs distributions de Linux. Le dossier Linux contient deux fichiers exécutables : Unlocker_32.exe et Unlocker_64.exe. Remplacez l'un des deux fichiers Unlocker_xx.exe par le fichier exécutable compatible avec votre système.

L'appareil doit être préalablement configuré à l'aide d'un système d'exploitation Windows ou macOS. Pour plus d'informations, consultez la section Configurer mon appareil.

Utilisation de Unlocker

Pour accéder à vos fichiers, utilisez Unlocker_xx.exe pour Linux. Selon votre distribution Linux, il se peut que vous ayez besoin de privilèges racine pour utiliser le programme Unlocker_xx.exe qui se trouve dans le dossier Linux du volume public monté. Par défaut, la plupart des distributions Linux ajoutent le bit d'exécution aux fichiers .exe sur une partition fat32. Sinon, le bit d'exécution doit être défini manuellement avant l'exécution en utilisant les commandes suivantes.

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

Si vous n'avez qu'un seul appareil connecté au système, exécutez le programme à partir d'un shell de commande sans arguments (par exemple, Unlocker_xx.exe). Vous devrez alors saisir le mot de passe de votre appareil pour le déverrouiller. Si vous disposez de plusieurs appareils, vous devez spécifier celui que vous souhaitez déverrouiller.

Voici les paramètres disponibles pour le logiciel de l'appareil :

Options :

```
-h, -help         aide
-l, -lock         verrouiller l'appareil
-r, -readonly     déverrouiller en lecture seule
```

Remarque : Unlocker_xx.exe déverrouille uniquement la clé USB IRONKEY SECURE FILES; elle doit ensuite être montée. De nombreuses distributions Linux modernes le font automatiquement. Si ce n'est pas le cas, exécutez le programme de montage à partir de la ligne de commande, en utilisant le nom de l'appareil imprimé par Unlocker_xx.exe.

Le simple fait de démonter l'appareil ne verrouille pas automatiquement la clé USB IRONKEY SECURE FILES. Pour verrouiller l'appareil, vous devez soit le démonter et le retirer physiquement (le débrancher), soit exécuter :

- Unlocker_xx.exe -l

Veuillez noter les détails importants ci-dessous pour utiliser votre appareil sous Linux :

1. La version du noyau doit être 4.4.x ou supérieure.
2. Montage
   - Assurez-vous d'avoir les autorisations nécessaires pour monter des appareils SCSI et USB externes.
   - Certaines distributions n'effectuent pas automatiquement le montage et nécessitent l'exécution de la commande suivante : mount /dev/[nom de l'appareil] / media/ [nom de l'appareil monté].

3. Le nom de l’appareil monté varie en fonction de la distribution.

4. Autorisations

   - Vous devez avoir les autorisations de monter les appareils externes/usb.
   - Vous devez avoir les autorisations pour exécuter un fichier exécutable à partir du volume public pour lancer Unlocker.
   - Vous pouvez avoir besoin des autorisations d’utilisateur racine.

5. IronKey pour Linux prend en charge les systèmes x86 et x86_64.

Où puis-je obtenir de l’aide ?

Les ressources suivantes fournissent plus d’informations sur les produits IronKey. Si vous avez d’autres questions, contactez le Support Kingston.

- kingston.com/usb/encrypted_security : Informations, supports marketing et tutoriels vidéo.
- kingston.com/support : Support produit, FAQ et téléchargements

REMARQUE : IronKey n'est pas responsable des erreurs et/ou omissions techniques ou éditoriales contenues dans le présent document, ni des dommages accessoires ou indirects résultant de la fourniture ou de l'utilisation de ce support. Les informations fournies dans le présent document sont susceptibles d'être modifiées sans préavis. Les informations contenues dans ce document représentent le point de vue actuel d'IronKey sur la question traitée à la date de publication. IronKey ne peut garantir l'exactitude des informations présentées après la date de publication. Ce document est fourni à titre d'information uniquement. IronKey n'offre aucune garantie, expresse ou implicite, dans ce document. IronKey et le logo IronKey sont des marques déposées de Kingston Digital, Inc. et de ses filiales. Toutes les autres marques sont la propriété de leur détenteur respectif. IronKey™ est une marque déposée de Kingston Technology, utilisée avec l'autorisation de Kingston Technology. Tous droits réservés.

Informations FCC Cet appareil est conforme à la partie 15 de la réglementation de la FCC. Son utilisation est soumise aux deux conditions suivantes : (1) Cet appareil ne doit pas provoquer d'interférences nuisibles, et (2) cet appareil doit accepter toute interférence reçue, y compris les interférences susceptibles de provoquer un fonctionnement indésirable. Cet appareil a été testé et déclaré conforme aux limites d'un appareil numérique de classe B, conformément à la Section 15 de la réglementation de la FCC. Ces limites sont conçues pour fournir une protection suffisante contre les interférences nuisibles dans les installations résidentielles. Cet appareil crée, utilise et peut émettre des ondes radioélectriques. Il est susceptible de créer des interférences nuisibles dans les communications radio s'il n'est pas installé et utilisé conformément aux instructions. Cependant, il n'est pas garanti que des interférences ne se produiront pas dans une installation particulière. Si cet appareil provoque des interférences nuisibles à la réception radio ou télévision, ce qui peut être déterminé en l'éteignant et l'allumant, l'utilisateur est encouragé à essayer de corriger ces interférences en prenant une ou plusieurs des mesures suivantes :

- Réorienter ou déplacer l'antenne de réception.
- Augmenter la distance entre l'appareil et le récepteur.
- Connecter l'appareil à une prise sur un circuit différent de celui sur lequel le récepteur est connecté.
- Consulter le revendeur ou un technicien radio/TV expérimenté pour obtenir de l'aide.

Remarque : Les changements ou modifications non expressément approuvés par la partie responsable de la conformité peuvent annuler l'autorisation de l'utilisateur à utiliser l'appareil.

IRONKEY™ S1000B
DRIVE FLASH USB 3.2 Gen 1 CRITTOGRAFATO

Guida per l'utente

Sommario

Informazioni sulla presente guida (04152025)

IronKey™ S1000B è un drive non gestito.

Guida rapida

Windows 11, 10 & macOS 12.x – 15.x

1. Collegare il dispositivo alla porta USB del computer.
2. Quando viene visualizzata la schermata di configurazione del dispositivo, seguire le istruzioni visualizzate sullo schermo. Se tale schermata non appare, aprirla manualmente:
    - Sistema operativo Windows: Start > Questo PC > IronKey Unlocker > IronKey.exe
    - Sistema operativo macOS: Finder > IRONKEY > IronKey.app
3. Una volta completata l'impostazione del dispositivo, è possibile trasferire i file importanti all'interno del drive USB IRONKEY SECURE FILES, e saranno automaticamente crittografati.

Alcuni sistemi Windows richiedono un riavvio del sistema dopo aver connesso il dispositivo per la prima volta. È possibile chiudere la notifica anche senza riavviare il sistema: non è infatti prevista l'installazione di alcun driver o software.

Informazioni sul dispositivo

IronKey S1000B USB 3.2 Gen 1 è un drive flash portatile con funzioni di sicurezza integrate mediante password e crittografia dati. La soluzione integra funzioni di crittografia AES a 256-bit avanzate e altre funzionalità che accrescono la sicurezza dei dati in mobilità. Ora è possibile portare con sé i propri file e i dati ovunque in totale sicurezza.

Quali sono le differenze tra questo dispositivo e un normale drive USB?

Certificazione FIPS 140-2 di Livello 3 - IronKey S1000B è un dispositivo dotato di certificazione FIPS, che offre la certezza di rispettare i requisiti normativi.

Crittografia hardware - Il controller di crittografia avanzato integrato nel dispositivo protegge i dati con lo stesso livello di sicurezza offerto per la protezione dei dati governativi altamente riservati. Tale funzionalità di sicurezza è sempre attiva e non può essere disattivata.

Protezione mediante password - L'accesso sicuro al dispositivo è garantito dall'uso di una password. Non condividere la password con nessuno. In tal modo, anche se il dispositivo dovesse essere smarrito o sottratto, nessuno sarà in grado di accedere ai dati in esso contenuti.

Reimpostazione del dispositivo - Se il controller di crittografia avanzato rileva un tentativo di manomissione fisica, oppure se il numero di tentativi di inserimento password errati supera le 10 volte, il dispositivo avvierà la sequenza di reset. **Importante:** la reimpostazione del dispositivo causa la completa eliminazione di tutti i dati in esso contenuti e il dispositivo ritorna alle impostazioni di fabbrica. Pertanto, *è importante ricordarsi le password*.

Protezione Anti-Malware automatica - Il dispositivo è in grado di proteggere i vostri dati da molti dei più recenti malware per drive USB, rilevando e impedendo l'esecuzione automatica di programmi non approvati. Il dispositivo può essere sbloccato anche in modalità di sola lettura se si sospetta che il computer su cui esso viene utilizzato sia infetto.

Semplice gestione del dispositivo - Il dispositivo integra il Pannello di controllo IronKey, un programma che consente di accedere ai file, gestire il dispositivo, modificare le proprie preferenze, modificare la password e bloccare il dispositivo in totale sicurezza.

Su quali sistemi può essere utilizzato?

- Windows® 11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x o versione successiva) Nota: l'applicazione Linux CLI Unlocker non supporta le funzionalità che richiedono l'accesso alla rete, come ad esempio la configurazione del dispositivo o la modifica della password.

Alcune funzioni sono disponibili solamente su sistemi specifici:

Solo per sistemi Windows

- Aggiornamenti del prodotto

Specifiche prodotto

Per ulteriori dettagli sul dispositivo, consultare la pagina **Informazioni sul dispositivo**, nella sezione dedicata al Pannello di controllo IronKey.

Specifiche tecniche	Dettagli
Capacità*	4GB, 8GB, 16GB, 32GB, 64GB, 128GB
Velocità**	USB 3.2 Gen 1 - 4GB-32GB: 180MB/s in lettura; 80MB/s in scrittura - 64GB: 230MB/s in lettura; 160MB/s in scrittura - 128GB: 230MB/s in lettura; 240MB/s in scrittura USB 2.0: - 4GB-128GB: 40MB/s in lettura, 35MB/s in scrittura
Dimensioni	82,3 mm x 21,1 mm x 9,1 mm
Impermeabile	Fino a 1 metro (standard MIL-STD-810F)
Temperature	Funzionamento: da 0°C a 70°C; Conservazione: da -40℃ a 85°C
Crittografia hardware	256-bit AES (modalità XTS)
Certificazione	Certificazione FIPS 140-2 di Livello 3
Hardware	Conforme allo standard USB 3.2 Gen 1 e compatibile con USB 2.0

SO compatibili	- Windows 11, Windows 10 (necessita di due lettere di unità libere) - macOS 12.x – 15.x - Linux 4.4.x***
Garanzia	5 anni di garanzia. Supporto tecnico gratuito

Progettati e assemblati negli Stati Uniti, i dispositivi S1000B non richiedono alcun software o driver per essere installati.

* La capacità indicata è approssimativa. Parte della capacità è utilizzata dal software integrato.
** La velocità varia in base all'hardware, al software e alla tipologia di utilizzo dell'host.
*** Set di funzionalità limitate.

Best practice raccomandate

1. Bloccare il dispositivo:
   - quando non in uso
   - prima di disconnettere il dispositivo
   - prima che il sistema entri in modalità di sospensione
2. Non scollegare mai il dispositivo quando il LED è acceso.
3. Non condividere mai la password del dispositivo.
4. Effettuare una scansione antivirus del computer prima di configurare e iniziare a utilizzare il dispositivo.

Configurazione del dispositivo

Al fine di garantire un'adeguata potenza di alimentazione per il drive USB crittografato S1000B, inserirlo direttamente in una porta USB 2.0/3.2 Gen 1 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)

1. Collegare il drive USB crittografato S1000B in una delle porte USB disponibili sul notebook o sul PC desktop e attendere che Windows rilevi il dispositivo.

   - Gli utenti di Windows 11 e 10 riceveranno una notifica che richiede l'installazione del driver del dispositivo.

   - Una volta completata la fase di rilevamento del nuovo hardware, Windows chiederà all'utente di avviare la procedura di inizializzazione.

2. Selezionare l'opzione **IronKey.exe** dalla partizione IRONKEY, visualizzabile in Esplora risorse. 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:).

Accesso al dispositivo (Ambienti macOS)

1. Inserire il drive USB crittografato S1000B in una delle porte USB disponibili sul notebook macOS o sul PC desktop e attendere che il sistema rilevi il dispositivo.

2. Fare doppio clic sul volume **IRONKEY** che appare sul desktop per avviare la procedura di inizializzazione.

   - Se il volume IRONKEY non viene visualizzato sul desktop, utilizzare Finder per individuare il volume IRONKEY nel lato sinistro della finestra Finder, all'interno dell'elenco dei dispositivi. Selezionare il volume e fare doppio clic sull'icona dell'applicazione IRONKEY nella schermata Finder. Verrà avviata la procedura di inizializzazione.

Inizializzazione del dispositivo

Inizializzazione su sistemi operativi Windows o macOS supportati.

1. Selezionare una lingua dall'elenco. Per impostazione predefinita, il software del dispositivo utilizza la stessa lingua del sistema operativo del computer (se disponibile).

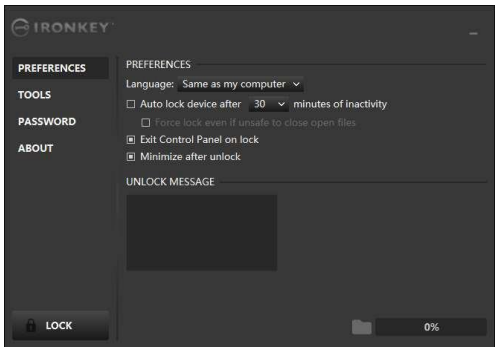
2. Leggere l'accordo di licenza; spuntare la casella di selezione per accettare i termini e le condizioni, quindi fare clic su "Continue" (Continua).

3. Nella casella di testo Password, digitare la password del dispositivo, quindi reinserire la password nella casella di testo "Confirm" (Conferma). La password ha lo scopo di proteggere i dati presenti sull'unità. Viene rilevata la differenza tra lettere maiuscole e minuscole ed è obbligatorio inserire una password composta da almeno 4 caratteri (spazi inclusi).

4. Se l'inizializzazione viene effettuata su sistemi Windows, l'utente potrà scegliere se formattare il drive IronKey Secure Files con un file system FAT32, exFAT o NTFS. Per ulteriori informazioni, consultare la sezione "Formattazione del dispositivo".

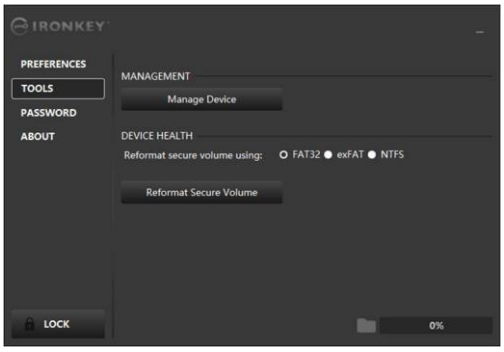
5. Per impostazione predefinita, è attiva l'opzione "Reset the device instead of self-destructing" (Reimposta il dispositivo al posto dell'autodistruzione). Fare clic su "Continue" (Continua). Il dispositivo completerà l'inizializzazione. Al termine, viene aperto il Pannello di controllo IronKey. Il dispositivo è ora pronto per memorizzare e proteggere i dati.

Pannello di controllo IronKey



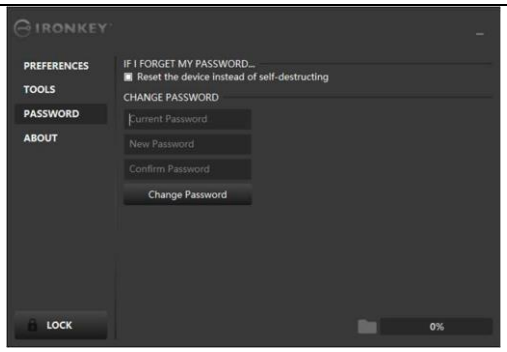
PREFERENCES (preferenze)

1. Language (lingua): modifica la lingua.
2. Auto lock device (blocco automatico del dispositivo): modifica il timer di blocco.
3. Exit on Control Panel on lock (Uscita dal Pannello di controllo al blocco): consente di impostare l'uscita dal Pannello di controllo in caso di attivazione del blocco del dispositivo.
4. Minimize after unlock (riduci a icona dopo lo sblocco): consente di scegliere se ridurre a icona il Pannello di controllo dopo lo sblocco del dispositivo o lasciarlo visualizzato in primo piano.
5. UNLOCK MESSAGE (messaggio di sblocco): consente di impostare un messaggio da visualizzare nella finestra di accesso.



TOOLS (strumenti)

1. MANAGEMENT (gestione): consente di gestire il dispositivo (è richiesto SafeConsole).
2. DEVICE HEALTH (stato di salute del dispositivo): riformatta il volume sicuro utilizzando FAT32, exFAT o NTFS. (il sistema macOS supporta esclusivamente FAT32).



PASSWORD

1. IF I FORGET MY PASSWORD... (se dimentico la password): attiva/disattiva l'opzione "Reset the device instead of self- destructing" (reimposta il dispositivo invece di attivare l'autodistruzione dei dati).
2. CHANGE PASSWORD (modifica password): modifica la password attuale, impostando una nuova password.

ABOUT (Informazioni su...)

1. ABOUT THIS DEVICE (informazioni su questo dispositivo): elenca le informazioni sul dispositivo.
2. Visit Website (vai al sito Web): apre il sito Web di Kingston.
3. Legal Notices (informative legali): apre le pagine con le informative legali presenti sui siti Web sia Kingston che DataLocker.
4. Certifications (certificazioni): apre la pagina del sito Web di Kingston che riporta le certificazioni dei dispositivi USB con crittografia.

Utilizzo del dispositivo

Verifica della sicurezza del dispositivo

È opportuno attenersi alle seguenti indicazioni nel caso di ritrovamento di un dispositivo di storage USB sicuro smarrito o incustodito. Il dispositivo di storage USB sicuro deve essere direttamente eliminato se l’autotest dà esito negativo, come anche nel caso in cui si sospetti che un aggressore possa averlo manomesso.

- Accertarsi che a prima vista il dispositivo di storage USB sicuro non presenti segni o graffi che possano indicare una manomissione.
- Verificare che il dispositivo di storage USB sicuro sia fisicamente intatto ruotandolo leggermente.
- Accertarsi che il dispositivo di storage USB sicuro abbia un peso di circa 30 grammi.
- Dopo averlo collegato a un computer, verificare che la spia blu del dispositivo di storage USB sicuro lampeggi (la frequenza corretta è di 3 volte al secondo al momento della connessione iniziale e durante le operazioni di lettura/scrittura).
- Verificare che il dispositivo di storage USB sicuro venga visualizzato come DVD-RW e che non venga montata una partizione di archiviazione prima che il dispositivo venga sbloccato

Accesso ai file sicuri

Una volta sbloccato il dispositivo, 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".

Per accedere ai file sicuri:

1. Fare clic sull'**icona della Cartella**  nell'angolo inferiore destro del Pannello di controllo IronKey.

   - Sistema operativo Windows: si aprirà una schermata di Esplora risorse in cui viene visualizzato il drive IRONKEY SECUREFILESUSB.

   - Sistema operativo macOS: si aprirà la schermata Finder in cui è visualizzato il drive USB KINGSTON.

2. Effettuare una delle seguenti operazioni:

   - Per aprire un file, fare doppio clic sul file desiderato nel drive S1000BUSB.

   - Per salvare un file, trascinarlo dalla cartella del computer in cui risiede e rilasciarlo nella relativa cartella del drive S1000BUSB.

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 **Secure Files**.

Sblocco della modalità di sola lettura

È possibile sbloccare il dispositivo in modalità di sola lettura, in modo tale che i file che risiedono sul drive sicuro 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.

Durante l'uso in tale modalità, il Pannello di controllo IronKey visualizzerà la dicitura *Read-Only Mode* (modalità di sola lettura). In tale modalità, non è possibile effettuare alcuna operazione che implichi la modifica dei file sul dispositivo. Ad esempio, non è possibile riformattare il dispositivo o modificare i file presenti nel drive.

Per sbloccare il dispositivo in modalità di sola lettura:

1. Inserire il dispositivo nella porta USB del computer host ed eseguire l'applicazione **IronKey.exe**.

2. Spuntare la casella di selezione della **modalità Read-Only** (Sola lettura) visualizzata sotto il campo di inserimento della password.

3. Immettere la password del dispositivo e fare clic su **Unlock** (Sblocco). Il Pannello di controllo IronKey visualizzerà il messaggio "*Read-Only Mode*" (modalità di sola lettura) nella parte inferiore della schermata.

Modifica del messaggio di sblocco

Il messaggio di sblocco è un testo personalizzato che viene visualizzato nella schermata di IronKey quando si sblocca il dispositivo. Questa funzionalità consente di personalizzare il messaggio visualizzato. Ad esempio, l'aggiunta di informazioni di contatto visualizzerà informazioni su come è possibile restituire un'unità smarrita.

Per modificare il messaggio di sblocco:

1. Nel Pannello di controllo IronKey, fare clic su **Settings** (Impostazioni), nella barra dei menu.
2. Fare clic su **Preferences** (Preferenze), nella barra laterale sinistra.
3. Immettere il testo del messaggio nel campo denominato "Unlock Message" (Messaggio di sblocco). La lunghezza del testo non deve eccedere lo spazio disponibile (circa 6 righe e 200 caratteri).

Minimize Control Panel When Unlocked (Riduci a icona Pannello di controllo allo sblocco)

Il Pannello di controllo viene ridotto a icona subito dopo lo sblocco del dispositivo. Se lo si desidera, è comunque possibile lasciare visualizzato il Pannello di controllo dopo lo sblocco dell'unità.

Per disattivare l'opzione "Minimize after unlock" (Riduci a icona dopo lo sblocco):

1. Nel Pannello di controllo IronKey, fare clic su "Preferences" (Preferenze), nella barra laterale sinistra.
2. Spuntare la casella di selezione "Minimize after unlock" (Riduci a icona dopo lo sblocco).

Blocco del dispositivo

Bloccare il dispositivo quando questo è inutilizzato, al fine di prevenire accessi indesiderati ai file sicuri nel drive. È possibile effettuare il blocco manuale del dispositivo oppure configurare il dispositivo in modo che si blocchi automaticamente dopo un determinato periodo di inattività.

Attenzione: per impostazione predefinita, se un file o un'applicazione sono aperti quando il dispositivo tenta di effettuare un blocco automatico, l'applicazione o il file aperti non saranno chiusi. Sebbene sia possibile configurare la funzione di blocco automatico in modo che forzi il blocco del dispositivo, tale operazione causerà la perdita di dati di qualunque file aperto e non salvato.

Se i file sono corrotti a causa di una procedura di blocco forzato o perché il dispositivo è stato disconnesso prima del blocco, potrebbe essere possibile recuperare i file eseguendo un controllo del disco mediante CHKDSK e utilizzando un software di recupero dati (solo su Windows).

Per effettuare il blocco manuale del dispositivo:

1. Fare clic su **Lock** (Blocca) nell'angolo inferiore sinistro del Pannello di controllo IronKey, al fine eseguire il blocco sicuro del dispositivo.
    - È anche possibile utilizzare una scorciatoia da tastiera: premere la combinazione di tasti CTRL + L (solo su Windows) o fare clic con il pulsante destro del mouse sull'**icona IronKey** nella barra di notifica e quindi fare clic su **Lock Device** (Blocca dispositivo).

Per impostare la funzione di blocco automatico sul dispositivo:

1. Sbloccare il dispositivo e fare clic su **Settings** (Impostazioni), nella barra dei menu del Pannello di controllo IronKey.

2. Fare clic su **Preferences** (Preferenze), nella barra laterale sinistra.
3. Spuntare la **casella** di selezione della funzione di blocco automatico del dispositivo e impostare l'intervallo di tempo prima del blocco su uno dei seguenti valori: 5, 15, 30, 60, 120 o 180 minuti.

Per eseguire CHKDSK (solo su Windows):

1. Sbloccare il dispositivo.
2. Premere il tasto del LOGO WINDOWS + R per aprire il menu "Esegui".
3. Digitare CMD e premere INVIO.
4. Dalla riga di comando, digitare CHKDSK, seguito dalla lettera del drive IRONKEY SECURE FILES USB; quindi aggiungere le opzioni "/F /R". Ad esempio, se la lettera del drive IRONKEYSECUREFILESUSB è G, il comando da inserire sarà: CHKDSK G: /F /R
5. Se necessario, utilizzare un software di recupero dati al fine di recuperare i file.

Uscire dal Pannello di controllo al blocco

Il Pannello di controllo viene chiuso automaticamente subito dopo il blocco del dispositivo. Per sbloccare il dispositivo e accedere al Pannello di controllo sarà necessario eseguire nuovamente l'applicazione IronKey. È tuttavia possibile impostare il Pannello di controllo in modo che, invece di chiudersi, torni alla schermata Unlock (Sblocco) subito dopo il blocco del dispositivo.

Per disabilitare la funzione di uscita dal Pannello di controllo al blocco:

1. Sbloccare il dispositivo e fare clic su Settings (Impostazioni), nella barra dei menu del Pannello di controllo IronKey.
2. Fare clic su **Preferences** (Preferenze), nella barra laterale sinistra.
3. Spuntare la casella di selezione **Exit Control Panel on lock** (Esci dal Pannello di controllo al blocco).

Gestione password

È possibile modificare la password del dispositivo, accedendo alla scheda "Password" (Password) del Pannello di controllo IronKey.

Talvolta, potrebbe essere necessario modificare la password per garantire la conformità alle nuove regole aziendali sulle password. Quando è richiesta una modifica della password, sarà visualizzata la schermata di modifica password alla prima occasione in cui il dispositivo viene sbloccato. Se è in uso, il dispositivo verrà automaticamente bloccato e l'utente dovrà modificare la password prima di poterlo sbloccare nuovamente.

Per modificare la password:

1. Sbloccare il dispositivo e fare clic su **Settings** (Impostazioni), nella barra dei menu.
2. Fare clic su **Password** (Password), nella barra laterale sinistra.
3. Immettere la password corrente nel campo specifico.

4. Immettere la nuova password e confermarla nei campi indicati.

5. Fare clic su Change Password (Cambia password).

Formattazione del dispositivo

Il dispositivo deve essere formattato durante l'inizializzazione, prima di poter essere utilizzato per l'archiviazione dei file.

Se l'inizializzazione viene effettuata su sistemi Windows, l'utente potrà scegliere se formattare il drive USB IRONKEY SECURE FILES con un file system FAT32, exFAT o NTFS.

Le opzioni sono disponibili esclusivamente nel sistema operativo Windows - la formattazione sui sistemi macOS viene effettuata automaticamente in formato FAT32.

- FAT32
  - Pro: compatibile con piattaforme multiple (Windows e macOS)
  - Contro: dimensione dei singoli file limitata a 4 GB
- exFAT
  - Pro: nessuna limitazione di dimensioni dei file
  - Contro: Microsoft limita l'utilizzo in base agli obblighi di licenza
- NTFS
  - Pro: nessuna limitazione di dimensioni dei file
  - Contro: installato con accesso in sola lettura sui dispositivi macOS supportati

La riformattazione del drive IRONKEY SECURE FILESUSB dopo l'inizializzazione eseguirà una rapida riformattazione predisponendo un drive vuoto, senza tuttavia cancellare la password e le impostazioni del dispositivo.

Importante: prima di riformattare il dispositivo, effettuare il backup del drive USB IRONKEY SECURE FILES su un altro dispositivo o unità. Ad esempio, su una soluzione di storage cloud o sul computer. Per riformattare un dispositivo:

1. Sbloccare il dispositivo e fare clic su **Settings** (Impostazioni), nella barra dei menu del Pannello di controllo IronKey.

2. Fare clic su **Tools** (Strumenti) nella barra laterale sinistra.

3. Nella scheda Device Health (Stato del dispositivo), selezionare il formato del file e fare clic su **Reformat Secure Volume** (Riformatta volume sicuro).

Come trovare le informazioni sul dispositivo

Utilizzare l'indicatore di capacità, situato nel lato inferiore destro del Pannello di controllo IronKey, per visualizzare quanto spazio di storage è ancora disponibile nel dispositivo. Il grafico raffigurante la barra verde rappresenta il livello di riempimento del dispositivo. Ad esempio, l'indicatore è interamente di colore verde quando il dispositivo è pieno. Il testo bianco sull'indicatore di capacità mostra quanto spazio libero è ancora disponibile.

Per informazioni generiche sul dispositivo, consultare la pagina Device Info (Info dispositivo).

Per visualizzare le informazioni sul dispositivo:

1. Sbloccare il dispositivo e fare clic su **Settings** (Impostazioni), nella barra dei menu del Pannello di controllo IronKey.

2. Fare clic su **Device Info** (Info dispositivo), nella barra laterale sinistra.

La sezione “About This Device” (Informazioni sul dispositivo) visualizza i seguenti dati del dispositivo:

- Numero modello
- ID Hardware
- Numero di serie
- Versione software
- Versione firmware
- Data di rilascio
- Lettera del drive di archiviazione file sicuri
- Lettera del drive IronKey
- Privilegi amministrativi di sistema e sistema operativo
- Console di gestione

Nota: per visitare il sito web di IronKey o per accedere a maggiori informazioni sulle note legali o sulle certificazioni per i prodotti IronKey, fare clic su uno dei pulsanti delle informazioni posti sulla schermata denominata Device Info (Info dispositivo).

Suggerimento: fare clic su **Copy** (Copia), per copiare i dati del dispositivo negli appunti, in modo tale da poterli poi incollare in un’email o in una richiesta di supporto.

Reimpostazione del dispositivo

Le impostazioni del dispositivo possono essere reimpostate alla configurazione iniziale di fabbrica. L’operazione consente di eliminare in sicurezza tutti i dati contenuti nel dispositivo. Contestualmente, sarà anche creata una nuova chiave di sicurezza per il prossimo utilizzo.

Reimpostazione del dispositivo:

1. Sbloccare il dispositivo.

2. Fare clic con il pulsante destro del mouse sull’**icona IronKey** nell’area della barra di notifica.

3. Fare clic su Reset Device (Reimposta dispositivo).

Allo scopo di evitare reimpostazioni accidentali del dispositivo, verrà visualizzato un popup di conferma che richiede l’inserimento di quattro cifre casuali. Una volta inserita la conferma, il dispositivo verrà riportato alla configurazione iniziale di fabbrica.

Utilizzo del dispositivo su Linux

Il dispositivo può essere utilizzato con differenti distribuzioni di Linux. La cartella Linux contiene due file eseguibili: Unlocker_32.exe e Unlocker_64.exe. In questa guida, sarà sufficiente sostituire il nome Unlocker_xx.exe con il file eseguibile che è compatibile con il sistema.

Il dispositivo deve essere preconfigurato utilizzando un sistema operativo Windows o macOS. Vedere la sezione Configurazione del dispositivo per ulteriori informazioni.

Uso della funzione di sblocco

Utilizzare il file Unlocker_xx.exe per Linux per accedere ai propri file. A seconda della distribuzione Linux utilizzata, potrebbe essere necessario disporre di privilegi di accesso alla root, per poter utilizzare il programma Unlocker_xx.exe situato nella cartella Linux volume pubblico montato. Per impostazione predefinita, la maggior parte delle distribuzioni Linux aggiunge i bit eseguibili ai file .exe nelle partizione fat32. In caso contrario sarà necessario impostare i bit eseguibili manualmente prima dell'esecuzione, utilizzando i seguenti comandi.

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

Se si utilizza un solo dispositivo connesso al sistema, eseguire il programma da una riga di comando senza argomenti (ad esempio, Unlocker_xx.exe). Tale operazione richiede all'utente di inserire la password del dispositivo per lo sblocco del drive. Se si utilizzano dispositivi multipli, sarà necessario specificare quale dispositivo si desidera sbloccare.

Ecco i parametri disponibili per il software del dispositivo:

Opzioni:

```
-h, -help        guida
-l, -lock        blocco dispositivo
-r, -readonly    sblocco in modalità sola lettura
```

Nota: Unlocker_xx.exe effettua solo lo sblocco del drive IRONKEYSECURE FILESUSB; il volume dovrà successivamente essere montato. Molte moderne distribuzioni Linux compiono tale operazione automaticamente. In caso contrario, eseguire il programma di montaggio volume dalla riga di comando, utilizzando il nome dispositivo indicato da Unlocker_xx.exe.

Il solo smontaggio del dispositivo non produrrà il blocco automatico del drive IRONKEYSECUREFILESUSB. Per bloccare il dispositivo, è necessario effettuare lo smontaggio del volume e rimuovere fisicamente il dispositivo (disconnettere) dalla porta a cui è collegato, oppure eseguire:

- Unlocker_xx.exe -l

Per l'utilizzo del dispositivo su sistemi operativi Linux, è necessario tenere presenti i seguenti importanti dettagli:

1. la versione del kernel deve essere la 4.4 o superiore.
2. Montaggio
   - Assicurarsi di disporre dei permessi necessari a effettuare il montaggio di dispositivi SCSI e USB esterni.
   - Alcune distribuzioni non effettuano il montaggio automatico e pertanto la loro esecuzione richiede il comando seguente: mount /dev/[nome del dispositivo] /media/[nome dispositivo montato]

3. Il nome del dispositivo montato varia in base al tipo di distribuzione.

4. Permessi

   - È necessario disporre dei permessi richiesti per montare dispositivi/usb/esterni.
   - È necessario disporre dei permessi richiesti per eseguire un file eseguibile dal volume pubblico al fine di lanciare l'applicazione di sblocco (Unlocker).
   - Potrebbe essere necessario disporre dei permessi di accesso alla root.

5. IronKey per Linux supporta sistemi x86 e x86_64.

Come ottenere assistenza?

Le seguenti risorse offrono maggiori informazioni sui prodotti IronKey. Se avete ulteriori domande, non esitate a contattare il supporto Kingston.

- kingston.com/usb/encrypted_security: informazioni, materiale di marketing e video tutorial.
- kingston.com/support: supporto prodotto, domande frequenti e download.

NOTA: IronKey non si assume alcuna responsabilità per qualunque tipo di errore e/o omissione editoriale contenuti nel presente documento; né per qualunque danno conseguente derivante dalla distribuzione o dall'uso di questo materiale. Le informazioni fornite nel presente documento sono soggette a modifiche senza alcun preavviso. Le informazioni contenute nel presente documento rappresentano le opinioni correnti di IronKey in relazione agli argomenti discussi alla data di pubblicazione. IronKey non è in grado di garantire l'accuratezza di qualunque informazione presentata dopo la data di pubblicazione. Le informazioni contenute in questo documento sono fornite a puro scopo informativo. IronKey non offre alcuna garanzia, sia essa in forma esplicita o implicita, nel presente documento. IronKey e il logo IronKey sono marchi commerciali di proprietà di Kingston Digital, Inc. e delle sue sussidiarie. Tutti gli altri marchi sono proprietà dei rispettivi titolari. IronKey™ è un marchio registrato di proprietà di Kingston Technologies, utilizzato su licenza di Kingston Technologies. Tutti i diritti riservati.

Informazioni FCC. Questo dispositivo è conforme alla Sezione 15 delle norme FCC. Il funzionamento è soggetto alle due condizioni che seguono: (1) Il dispositivo non può provocare interferenze dannose e (2) il dispositivo deve accettare qualsiasi interferenza ricevuta, incluse interferenze che potrebbero causare malfunzionamenti. Questa apparecchiatura è stata collaudata e trovata conforme ai limiti previsti per i dispositivi digitali di classe B, come descritto nella sezione 15 della normativa FCC. Tali limiti vengono stabiliti per offrire una protezione ragionevole contro interferenze dannose in installazioni residenziali. La presente apparecchiatura genera, usa e può emettere energia a frequenza radio e, se non installata e utilizzata secondo le istruzioni, può essere causa di interferenze dannose nelle comunicazioni radio. Tuttavia, non è possibile garantire che l'interferenza non possa verificarsi in determinate installazioni. Se questa apparecchiatura causa interferenze dannose nella ricezione televisiva o radio, il che può essere facilmente verificato accendendo e spegnendo l'apparecchiatura stessa, è consigliabile tentare di eliminare l'interferenza adottando una o più delle seguenti misure:

- Orientare nuovamente o riposizionare l'antenna ricevente;
- Aumentare la distanza tra l'apparecchiatura e il ricevitore;
- Collegare l'apparecchiatura a una presa facente parte di un circuito diverso da quello a cui è collegato il ricevitore;
- Consultare il rivenditore o un tecnico radio/TV esperto per assistenza.

Nota: eventuali alterazioni o modifiche non espressamente approvate dal soggetto responsabile per la conformità potrebbero comportare la perdita del diritto all'uso del dispositivo per l'utente.

IRONKEY™ S1000B
PENDRIVE CRIPTOGRAFADO USB 3.2 Gen 1

Manual do Usuário

Índice

Sobre este Manual (04152025)

O IronKey™ S1000B é um drive não gerenciado.

Início rápido

Windows 11, 10 e macOS 12.x – 15.x

1. Conecte o dispositivo na porta USB do seu computador.
2. Quando a janela de Instalação do Dispositivo aparecer, siga as instruções na tela. Se esta janela não aparecer, abra manualmente:
    - Windows: Iniciar > Este computador > IronKey Unlocker > IronKey.exe
    - macOS: Finder > IRONKEY > IronKey.app
3. Quando a instalação do dispositivo estiver concluída, você pode mover seus arquivos importantes para o drive USB IRONKEY SECURE FILES, e eles serão criptografados automaticamente.

Alguns sistemas do Windows solicitam a reinicialização depois de conectar seu dispositivo pela primeira vez. Você pode fechar essa solicitação de forma segura sem reiniciar. Nenhum drive ou software novo é instalado.

Sobre o meu dispositivo

O IronKey S1000B USB 3.2 Gen 1 é um pendrive portátil com segurança por senha integrada e criptografia de dados. Ele é projetado com criptografia AES de 256 bits avançada e outras funcionalidades que aumentam a segurança de dados móveis. Agora você pode carregar com você seus arquivos e dados com segurança, onde quer que você vá.

Como ele é diferente de um drive USB normal?

Certificado FIPS 140-2 Nível 3 – O IronKey S1000B é um dispositivo com certificado FIPS, portanto você pode ter a confiança de estar cumprindo as exigências regulatórias.

Criptografia de hardware – O controlador de criptografia avançada no seu dispositivo protege seus dados com o mesmo nível de proteção das informações de governo altamente confidenciais. Esta funcionalidade de tecnologia de segurança está sempre ligada e não pode ser desabilitada.

Protegido por senha – O acesso ao dispositivo é seguro usando a proteção por senha. Não compartilhe sua senha com ninguém, pois mesmo se seu dispositivo se perder ou for roubado, ninguém mais terá acesso a seus dados.

Restauração do dispositivo – Se o controlador de criptografia avançada detectar invasão física ou se o número de tentativas de senha incorretas consecutivas exceder 10 tentativas, o dispositivo iniciará uma reinicialização. **Importante:** quando um dispositivo for restaurado, todos os dados integrados serão apagados e o dispositivo retorna às configurações **de fábrica, portanto, lembre-se de sua senha**.

Proteção autorun de anti-malware – Seu dispositivo é capaz de proteger você de muitas das últimas ameaças de malware direcionadas a drives USB ao detectar e prevenir a execução autorun de programas não aprovados. O desbloqueio também pode ocorrer no modo somente leitura se você suspeitar que o computador host está infectado.

Gestão de dispositivo simples – Seu dispositivo inclui o Painel de controle IronKey, um programa para acessar seus arquivos, gerenciar seu dispositivo, editar suas preferências, mudar a senha do seu dispositivo e bloquear seu dispositivo com segurança.

Em quais sistemas posso usá-lo?

- Windows® 11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x ou superior) Observação: O Linux CLI Unlocker não suporta funcionalidades que exigem acesso à rede, por exemplo, configurar seu dispositivo ou alterar sua senha.

Alguns recursos só estão disponíveis em sistemas específicos:

Apenas Windows

- Atualizações de dispositivo

Especificações do produto

Para outros detalhes sobre o seu dispositivo, veja a página de **Informações do dispositivo** no Painel de controle do IronKey.

Especificações	Detalhes
Capacidades*	4 GB, 8 GB, 16 GB, 32 GB, 64 GB, 128 GB
Velocidade**	USB 3.2 Gen 1 - 4 GB - 32 GB: 180MB/s para leitura; 80MB/s para gravação - 64 GB: 230MB/s para leitura; 160MB/s para gravação - 128 GB: 230MB/s para leitura; 240MB/s para gravação USB 2.0: - 4 GB - 128 GB: 40MB/s para Leitura, 35MB/s para Gravação
Dimensões	82,3 mm x 21,1 mm x 9,1 mm
À prova d'água	Até 1 metro; MIL-STD-810F
Temperatura	Operacional: 0°C a 70°C ; Armazenamento: -40°C a 85°C
Criptografia de hardware	256 bits AES (Modo XTS)
Certificação	Certificado FIPS 140-2 Nível 3
Hardware	Conformidade com o USB 3.2 Gen 1 e compatível com USB 2.0

Compatibilidade OS	- Windows 11, Windows 10 (Precisa de duas letras de drive livres) - macOS 12.x – 15.x - Linux 4.4.x***
Garantia	5 anos de garantia. Suporte técnico gratuito

Projetados e montados nos EUA, o dispositivo S1000B não precisa de qualquer software ou driver para ser instalado.

* A capacidade anunciada é aproximada. Algum espaço é necessário para software integrados.
**A velocidade varia com o hardware, o software e o uso do host.
*** Conjunto de funcionalidades limitado.

Melhores práticas recomendadas

1. Bloqueie o dispositivo:
   - quando não estiver usando
   - antes de desconectá-lo
   - antes que o sistema entre em modo pausa
2. Nunca desconecte o dispositivo quando o LED estiver aceso.
3. Nunca compartilhe a senha do seu dispositivo.
4. Execute uma varredura antivírus no computador antes de configurar e usar o dispositivo.

Configurar o meu dispositivo

Para garantir que haja energia suficiente fornecida para o drive USB criptografado S1000B, insira-o diretamente em uma porta USB 2.0 / 3.2 Gen 1 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)

1. Conecte o drive USB criptografado S1000B à uma porta USB disponível em um notebook ou computador e espere o Windows detectá-lo.

   - Usuários do Windows 11 e 10 receberão uma notificação de driver de dispositivo.

   - Quando o novo hardware tiver sido detectado, o Windows solicitará que comece o processo de inicialização.

2. Selecione a opção **IronKey.exe** dentro da partição IRONKEY que pode ser encontrada no “File explorer”. 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:).

Acesso ao dispositivo (Ambiente macOS)

1. Conecte o drive USB criptografado S1000B em uma porta USB disponível no notebook ou computador macOS e espere o sistema operacional detectá-lo.

2. Dê um clique duplo no volume **IRONKEY** que aparece na área de trabalho para começar o processo de inicialização.

   - Se o volume IRONKEY não aparecer na área de trabalho, abra o Finder e localize o volume Ironkey no lado esquerdo da janela do Finder (em Dispositivos). Destaque o volume e dê um clique duplo no ícone do aplicativo IRONKEY na janela do Finder. Isso fará começar o processo de inicialização.

Inicialização do dispositivo

Inicialização em sistema operacional Windows ou macOS compatíveis.

1. Selecione uma preferência de idioma na lista. Por padrão, o software do dispositivo usará o mesmo idioma que o sistema operacional do computador (se disponível).

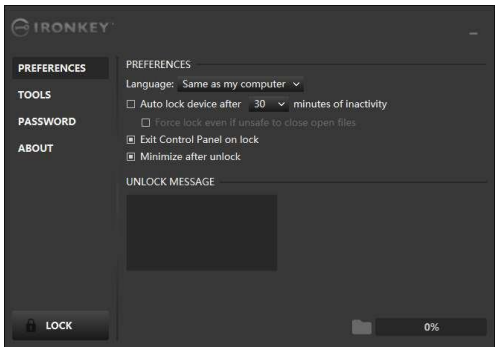
2. Revise o acordo de licença, marque a caixa de seleção para aceitá-lo e clique em Continuar

3. Na caixa de texto da senha, escreva uma senha de dispositivo e, em seguida, volte a digitar sua senha na caixa de texto de Confirmação. A senha protege os dados no drive seguro. As senhas são sensíveis a maiúsculas e minúsculas e têm de ter pelo menos 4 caracteres (incluindo espaço).

4. Se inicializar no Windows, será dada a opção de formatar o drive IronKey Secure Files, ou até mesmo FAT32, exFAT ou NTFS. Para mais informações, consulte Formatar meu dispositivo.

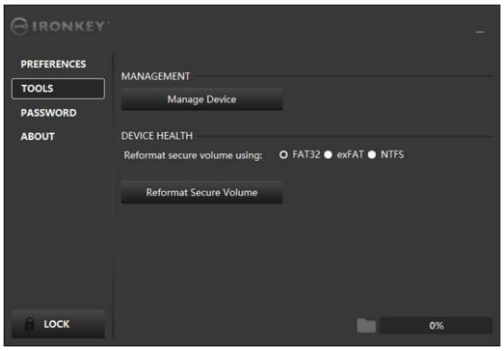
5. Por padrão, a opção para 'Redefinir o dispositivo em vez de auto-destruição' está ativada. Clique em Continuar. O dispositivo terminará a inicialização. Uma vez concluído, o Painel de Controle do IronKey abrirá. O seu dispositivo está agora pronto para armazenar e proteger os seus dados.

Painel de controle IronKey



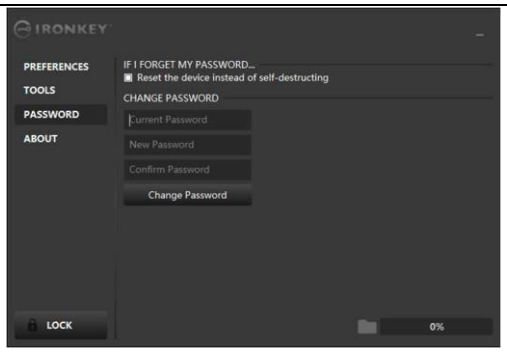
PREFERÊNCIAS

1. Idioma: Alterar o idioma do dispositivo
2. Bloqueio automático do dispositivo: Alterar o temporizador de bloqueio
3. Sair no Painel de Controle no bloqueio: Altere o comportamento para sair ou deixar o Painel de Controle aberto quando o dispositivo estiver bloqueado.
4. Minimizar após desbloquear: Alterar para minimizar o Painel de Controlo quando o dispositivo for desbloqueado ou deixe-o ficar maximizado.
5. DESBLOQUEAR MENSAGEM: Adicione uma mensagem que será apresentada na janela de login.



FERRAMENTAS

1. GERENCIAMENTO: Gerenciar dispositivo (é necessário o SafeConsole).
2. SAÚDE DO DISPOSITIVO: Reformatar o volume seguro usando FAT32, exFAT ou NTFS. (O macOS só permite formatar o FAT32)



SENHA

1. SE EU ESQUECER A MINHA SENHA...: Ativar/Desativar 'Redefinir o dispositivo em vez de auto-destruição.
2. MUDAR SENHA Alterar a senha atual para uma nova senha.

SOBRE

1. SOBRE ESTE DISPOSITIVO: Lista as informações dos dispositivos.
2. Visitar o site: Inicia o site da Kingston
3. Avisos legais: Inicia os sites de avisos legais da Kingston e do DataLocker
4. Certificações: Inicia a página de certificados da Kingston para dispositivos USB criptografados

Usar meu dispositivo

Verificar a segurança do dispositivo

Se um dispositivo de armazenamento USB seguro se perder ou tiver ficado sem supervisão, ele deve ser verificado de acordo com as seguintes instruções do usuário. O dispositivo de armazenamento USB seguro deve ser descartado se houver a suspeita de que um invasor tenha violado o dispositivo ou se o teste automático falhar.

- Verificar visualmente o dispositivo de armazenamento USB seguro, se ele não tem marcas ou novos arranhões que possam indicar adulteração.
- Verificar se o dispositivo de armazenamento USB seguro está fisicamente intacto, girando-o ligeiramente.
- Verificar se o dispositivo de armazenamento USB seguro pesa cerca de 30 gramas.
- Verificar, quando ligado a um computador, se a luz indicadora azul no dispositivo de armazenamento USB seguro pisca (a frequência correta é de 3 vezes por segundo na conexão inicial e durante as operações de leitura/gravação).
- Verificar se o dispositivo de armazenamento USB seguro está sendo mostrado como um DVD-RW e se uma partição de armazenamento não está instalada até o dispositivo ser desbloqueado.

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.

Para acessar seus arquivos seguros:

1. Clique no **ícone de pasta**  no canto inferior direito do Painel de Controle do IronKey.
   - Windows: Abre o Windows Explorer no drive USB IRONKEY SECURE FILES.
   - macOS: Abre o Finder no drive USB KINGSTON.
2. Faça uma das opções a seguir:
   - Para abrir um arquivo, dê um clique duplo no arquivo no drive USB S1000B.
   - Para salvar um arquivo, arraste o arquivo do seu computador para o drive USB S1000B.

Dica: Você também pode acessar seus arquivos clicando com o botão direito no **ícone do IronKey** na barra de tarefas do Windows e clicando em **Secure Files**.

Desbloquear no módulo somente leitura

Você pode desbloquear seu dispositivo em um estado de somente leitura para que os arquivos não possam ser alterados em seu drive seguro. 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 trabalhar neste modo, o Painel de controle IronKey exibirá o *modo somente leitura* do texto. Neste modo, você não pode executar nenhuma operação que envolva modificações dos arquivos no dispositivo. Por exemplo, você não pode reformatar o dispositivo ou editar arquivos no drive.

Para desbloquear o dispositivo no Modo somente leitura:

1. Insira o dispositivo na porta USB do computador host e execute o **IronKey.exe**.
2. Marque a **caixa** “**Somente leitura**” abaixo da caixa de entrada da senha.
3. Digite a senha do seu dispositivo e clique em **Desbloquear**. O Painel de controle do IronKey aparecerá com o texto “*Modo Somente Leitura*” na parte de baixo.

Modificar a mensagem de desbloqueio

A mensagem de desbloqueio é um texto personalizado que aparece na janela IronKey quando você desbloquear o dispositivo. Esta funcionalidade permite que você personalize a mensagem que aparece. Por exemplo, adicionar informações de contato mostrará informações de como um drive perdido pode ser devolvido a você.

Para modificar a mensagem de desbloqueio:

1. No Painel de controle do IronKey, clique em "**Configurações**" na barra do menu.
2. Clique em "**Preferências**" na barra lateral à esquerda.
3. Digite a mensagem no campo "Desbloquear mensagem". O texto deve caber no espaço fornecido (aproximadamente 6 linhas e 200 caracteres).

Minimize o Painel de Controle quando desbloqueado

Quando o dispositivo for desbloqueado, o Painel de Controle é minimizado automaticamente para a barra de tarefas. Se desejar, o Painel de Controle pode permanecer aberto depois que o dispositivo for desbloqueado.

Para desativar o Minimizar após desbloquear:

1. No Painel de controle do IronKey, clique em "Preferências" na barra lateral esquerda.
2. Clique na caixa de verificação para Minimizar após desbloquear.

Bloquear o dispositivo

Bloqueie seu dispositivo quando não estiver usando para prevenir acessos indesejados aos seus arquivos seguros no drive. Você pode bloquear manualmente o dispositivo, ou você pode configurar o dispositivo para bloquear automaticamente depois de um período de inatividade específico.

Cuidado: Por padrão, se um arquivo ou aplicativo estiver aberto quando o dispositivo tentar bloquear automaticamente, isso não forçará o fechamento do aplicativo ou do arquivo. Embora você possa configurar o bloqueio automático para forçar o dispositivo para bloquear, fazer isso pode resultar na perda de dados para quaisquer dados abertos e não salvos.

Se seus arquivos se corromperem depois de um procedimento de bloqueio forçado ou por desconectar o dispositivo antes do bloqueio, você pode recuperar os arquivos executando CHKDSK e usando o software de recuperação de dados. (Apenas para Windows).

Para bloquear o dispositivo manualmente:

1. Clique em "**Bloquear**" no canto inferior esquerdo do Painel de controle do IronKey para bloquear seu dispositivo com segurança.
    - Você também pode usar o atalho do teclado: **CTRL + L** (Apenas no Windows) ou lique com o botão direito no **ícone IronKey** na barra de tarefas e clique em **Bloquear dispositivo**.

Para definir o bloqueio automático do dispositivo:

1. Desbloqueie seu dispositivo e clique em "**Configurações**" na barra do menu no Painel de controle do IronKey.

2. Clique em “**Preferências**” na barra lateral à esquerda.
3. Clique na **caixa** de seleção para bloquear automaticamente o dispositivo e configurar o tempo final para um dos seguintes intervalos de tempo: 5, 15, 30, 60, 120 ou 180 minutos.

Para executar CHKDSK (Apenas Windows):

1. Desbloqueie o dispositivo.
2. Aperte a TECLA WINDOWS + R para abrir a mensagem de execução.
3. Digite CMD e aperte ENTER.
4. Da mensagem de comando, digite CHKDSK, a letra do drive USB IRONKEY SECURE FILES, e então “/F /R”. Por exemplo, se a letra do drive USB IRONKEY SECURE FILES for G, você deve digitar: CHKDSK G: /F /R
5. Use o software de recuperação de dados, se necessário, para recuperar seus arquivos.

Sair do Painel de Controle no bloqueio

Quando o dispositivo estiver bloqueado, o Painel de Controle fechará automaticamente. Para desbloquear o dispositivo e acessar o Painel de Controle, você precisará executar novamente o aplicativo do IronKey. Se desejar, o Painel de Controle pode ser definido para voltar à tela Desbloquear depois que o usuário bloquear o dispositivo.

Para desativar o Sair do Painel de Controle no bloqueio:

1. Desbloqueie seu dispositivo e clique em “Configurações” na barra do menu no Painel de controle do IronKey.
2. Clique em “Preferências” na barra lateral à esquerda.
3. Clique na caixa de verificação Sair do Painel de Controle no bloqueio.

Gerenciar senhas

Você pode mudar a sua senha em seu dispositivo acessando a aba Senha no Painel de controle IronKey.

Algumas vezes você pode precisar mudar sua senha para estar em conformidade com as novas políticas de senha corporativas. Quando uma mudança for solicitada, a tela de mudança de senha aparecerá da próxima vez que você desbloquear o dispositivo. Se o dispositivo estiver em uso, ele será bloqueado, e você terá que mudar a senha antes de desbloqueá-lo.

Para mudar sua senha:

1. Desbloqueie seu dispositivo e clique em “**Configurações**” na barra do menu.
2. Clique em “**Senha**” na barra lateral esquerda.
3. Insira sua senha atual no campo fornecido.

4. Insira sua nova senha e confirme-a no campo fornecido.

5. Clique em Mudar a senha.

Formatar meu dispositivo

Seu dispositivo precisará ser formatado durante a inicialização antes que possa ser usado para armazenar arquivos.

Se ao inicializar no Windows, será dada a opção de formatar o drive USB IRONKEY SECURE FILES, ou até mesmo FAT32, exFAT ou NTFS.

As opções são apenas para sistemas operacionais Windows - o macOS formatará automaticamente para FAT32.

- FAT32
  - Prós: Compatível entre plataformas (SistOp Windows e mac)
  - Contras: Tamanho de arquivo individual limitado de 4 GB
- exFAT
  - Prós: Sem limitações de tamanho de arquivo
  - Contras: A Microsoft restringe o uso através de obrigações de licença
- NTFS
  - Prós: Sem limitações de tamanho de arquivo
  - Contras: Instalado como acesso somente leitura em macOS compatíveis

Depois da inicialização, reformatar o drive USB IRONKEY SECURE FILES fará a formatação rápida e fornecerá um drive vazio, mas não apagará suas configurações e senha do dispositivo.

Importante: Antes de reformatar o dispositivo, faça back-up do seu drive USB IRONKEY SECURE FILES em um local separado, por exemplo, armazenamento em nuvem ou seu computador. Para reformatar um dispositivo:

1. Desbloqueie seu dispositivo e clique em “**Configurações**” na barra do menu do Painel de controle do IronKey.

2. Clique em “**Ferramentas**” na barra lateral esquerda.

3. Em “Integridade do dispositivo”, selecione o formato do arquivo e clique em “**Reformatar volume seguro**”.

Encontrar informações sobre o meu dispositivo

Use o Medidor de capacidade, localizado no canto inferior esquerdo do Painel de controle IronKey, para ver quanto de espaço de armazenamento ainda está disponível em seu dispositivo. O gráfico de barras verdes representa o quão cheio o dispositivo está. Por exemplo, o medidor ficará totalmente verde quando o dispositivo estiver cheio. O texto branco no Medidor de capacidade mostra quanto de espaço livre ainda resta.

Para obter informações gerais sobre seu dispositivo, veja a página de informações do Dispositivo.

Para visualizar as informações do dispositivo:

1. Desbloqueie seu dispositivo e clique em “**Configurações**” na barra do menu do Painel de controle do IronKey.

2. Clique em “**Informações do dispositivo**” na barra lateral esquerda.

A seção “Sobre este dispositivo” inclui os seguintes detalhes sobre seu dispositivo:

- Número do modelo
- ID de hardware
- Número de série
- Versão do software
- Versão do firmware
- Data de lançamento
- Letra do drive de arquivos seguros
- Letra de drive IronKey
- Sistema operacional e Privilégios administrativos do sistema
- Console de gerenciamento

Observação: Para visitar o site IronKey ou acessar mais informações sobre avisos legais ou certificados para os produtos IronKey, clique em um dos botões de informações na página de informações do dispositivo.

Dica: Clique em Copiar para copiar as informações do dispositivo na área de transferência para que você possa colar em um e-mail ou solicitação de suporte.

Restaurar meu dispositivo

Seu dispositivo pode ser revertido para as configurações de fábrica. Isso limpará todos os seus dados do dispositivo de forma segura, e uma nova chave de segurança será criada para o próximo uso.

Restaurar seu dispositivo:

1. Desbloqueie seu dispositivo.

2. Dê um duplo clique no **ícone do IronKey** na barra da tarefas.

3. Clique em Restaurar dispositivo.

Para evitar redefinições acidentais de dispositivos, um pop-up pedirá para introduzir quatro dígitos aleatórios. Depois de inserir a confirmação, o dispositivo será revertido para as configurações de fábrica.

Usar o meu dispositivo no Linux

Você pode usar seu dispositivo em várias distribuições do Linux. Há dois executáveis na pasta linux, Unlocker_32.exe e Unlocker_64.exe. Para este manual, substitua o Unlocker_xx.exe pelo executável compatível com seu sistema.

O dispositivo deve ser configurado previamente usando um sistema operacional Windows ou macOS. Veja “Configurar o meu dispositivo” para mais informações.

Usar o desbloqueador

Use o Unlocker_xx.exe para Linux para acessar seus arquivos. Dependendo da distribuição do Linux, você pode precisar de privilégios raiz para usar o programa Unlocker_xx.exe encontrado na pasta do Linux do volume público instalado. Por padrão, a maioria das distribuições Linux anexarão o bit de execução para arquivos .exe em uma partição fat32. Caso contrário, o bit de execução deve ser configurado manualmente antes de usar os seguintes comandos.

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

Se você tiver apenas um dispositivo anexado ao sistema, execute o programa de um comando shell sem argumentos (por exemplo, Unlocker_xx.exe). Então, a senha de seu dispositivo solicitará que você desbloqueie o drive. Se você tiver vários dispositivos, você deve especificar qual deles você quer desbloquear.

Estes são os parâmetros disponíveis para o software do dispositivo:

Opções:

```
-h, -help         ajuda
-l, -lock         bloquear dispositivo
-r, -readonly     desbloquear como somente leitura
```

Observação: O Unlocker_xx.exe desbloqueia apenas o USB IRONKEY SECURE FILES; ele deve então ser instalado. Muitas distribuições de Linux modernas fazem isso automaticamente. Caso contrário, execute o programa de instalação da linha de comando, usando o nome do dispositivo reproduzido pelo Unlocker_xx.exe.

Simplesmente desinstalar o dispositivo não bloqueia automaticamente o IRONKEYSECUREFILESUSB. Para bloquear o dispositivo, você deve desinstalá-lo e removê-lo fisicamente (desconectar), ou executar:

- Unlocker_xx.exe -l

Observe os importantes detalhes a seguir ao usar seu dispositivo no Linux:

1. A versão Kernel deve ser 4.4.x ou superior.
2. Instalação
   - Tenha certeza de possuir as permissões para instalar dispositivos USB e SCSI externos.
   - Algumas distribuições não são instaladas automaticamente e exigem que seja executado o seguinte comando: mount /dev/[name of the device] / media/ [mounted device name]

3. O nome do dispositivo instalado varia dependendo da distribuição.

4. Permissões

   - Você precisa ter as permissões para instalar dispositivos/usb/externos.

   - Você precisa ter as permissões para executar um arquivo executável de um volume público para iniciar o Desbloqueador.

   - Você pode precisar de permissões de usuário raiz.

5. O IronKey para Linux é compatível com sistemas x86 e x86_64.

Onde posso obter ajuda?

Os seguintes recursos fornecem mais informações sobre os produtos IronKey. Entre em contato com o suporte da Kingston se tiver alguma pergunta.

- kingston.com/usb/encrypted_security: Informações, materiais de marketing e tutoriais em vídeo.

- kingston.com/support: Suporte de produto, Perguntas frequentes e downloads

OBSERVAÇÃO: A IronKey não é responsável por erros técnicos ou de edição e/ou omissões contidas aqui; seja por danos incidentais ou decorrentes do fornecimento ou uso deste material. As informações fornecidas aqui estão sujeitas a mudanças sem notificação. As informações contidas neste documento representam a visão atual da IronKey sobre a questão discutida na data da publicação. A IronKey não pode garantir a precisão de qualquer informação apresentada depois da data de publicação. Este documento tem somente a finalidade de informação. A IronKey não dá nenhuma garantia, explícita ou implícita, neste documento. IronKey e o logotipo IronKey são marcas comerciais da Kingston Digital, Inc. e suas subsidiárias. Todas as outras marcas comerciais pertencem a seus respectivos proprietários. A IronKey™ é uma marca comercial registrada da Kingston Technologies, usada sob a permissão da Kingston Technologies. Todos os direitos reservados.

Informações FCC Este dispositivo está em conformidade com a Seção 15 das Regras FCC. A operação está sujeita às duas condições seguintes: (1) Este dispositivo não poderá causar interferência prejudicial, e (2) este dispositivo deverá aceitar qualquer interferência recebida, incluindo interferências que possam causar operações indesejadas. Este equipamento foi testado e encontra-se em conformidade com os limites para dispositivo digital de Classe B, de acordo com a Seção 15 das regras FCC. Esses limites foram projetados para fornecer proteção razoável contra interferências prejudiciais em uma instalação residencial. Este equipamento gera, usa e pode emitir energia de radiofrequência e, se não for instalado e usado conforme as instruções, poderá causar interferência prejudicial nas comunicações de rádio.
No entanto, não é possível garantir que essa interferência não ocorrerá em uma determinada instalação. Se este equipamento causar interferência prejudicial à recepção de rádio e televisão, o que pode ser verificado ao ligar e desligar o equipamento, usuário é aconselhado a testar e corrigir a interferência através de um ou mais dos seguintes meios:

- Reorientar ou reposicionar a antena receptora.
- Aumentar a distância entre o equipamento e o receptor.
- Conectar o equipamento à uma tomada em um circuito diferente do circuito ao qual o receptor está conectado.
- Consultar o revendedor ou um técnico de rádio/TV experiente para obter ajuda.

Observação: Alterações ou modificações não aprovadas expressamente pela parte responsável pela conformidade podem cancelar a autoridade do usuário para operar o equipamento.

IRONKEY™ S1000B
SZYFROWANA PAMIĘĆ FLASH USB 3.2 Gen 1

Instrukcja obsługi

Spis treści

Informacje o instrukcji obsługi (04152025)

IronKey™ S1000B to pamięć bez funkcji zarządzania.

Szybkie uruchomienie

Systemy Windows 11, 10 oraz macOS 12.x – 15.x

1. Podłącz urządzenie do portu USB komputera.
2. Gdy pojawi się okno konfiguracji urządzenia, postępuj zgodnie z instrukcjami wyświetlanymi na ekranie. Jeżeli okno się nie pojawi, otwórz je ręcznie:
    - Windows: Start > Ten komputer > IronKey Unlocker > IronKey.exe
    - macOS: Finder > IRONKEY > IronKey.app
3. Po zakończeniu konfiguracji urządzenia można przenieść ważne pliki do pamięci USB IRONKEY SECURE FILES, gdzie zostaną one automatycznie zaszyfrowane.

W przypadku niektórych systemów Windows po pierwszym podłączeniu urządzenia pojawia się monit o ponowne uruchomienie komputera. Można bezpiecznie zamknąć okno monitu bez ponownego uruchamiania, ponieważ nie są instalowane żadne nowe sterowniki ani oprogramowanie.

Informacje o urządzeniu

IronKey S1000B USB 3.2 Gen 1 to przenośna pamięć flash z wbudowanymi funkcjami ochrony hasłem i szyfrowania danych. Wyposażono ją w zaawansowaną funkcję szyfrowanie danych AES z kluczem 256-bitowym, a także inne funkcje, które zwiększają bezpieczeństwo przenoszonych danych. Teraz możesz wszędzie bezpiecznie przenosić swoje pliki i dane.

Jakie są różnice w porównaniu ze zwykłą pamięcią USB?

Certyfikat FIPS 140-2 Level 3 – pamięć IronKey S1000B to urządzenie z certyfikatem FIPS, które daje pewność zachowania zgodności z obowiązującymi przepisami.

Szyfrowanie sprzętowe – zaawansowany kontroler szyfrowania w urządzeniu chroni Twoje dane na równie wysokim poziomie jak chronione są ściśle tajne informacje rządowe. Ta funkcja technologii zabezpieczeń jest zawsze włączona i nie można jej wyłączyć.

Ochrona hasłem – dostęp do urządzenia jest chroniony hasłem. Nie udostępniaj nikomu swojego hasła. Dzięki temu nikt nie uzyska dostępu do Twoich danych, nawet w przypadku utraty lub kradzieży urządzenia.

Resetowanie urządzenia – jeśli zaawansowany kontroler szyfrowania wykryje fizyczną ingerencję lub liczba kolejnych nieudanych prób wprowadzenia hasła przekroczy 10, urządzenie zainicjuje sekwencję resetowania. **Ważne –** w przypadku zresetowania urządzenia wszystkie dane zostaną usunięte, a urządzenie powróci do ustawień fabrycznych. *Dlatego dobrze zapamiętaj swoje hasło.*

Funkcja ochrony przed automatycznym uruchomieniem złośliwego oprogramowania – urządzenie zapewnia ochronę przed wieloma najnowszymi zagrożeniami ze strony złośliwego oprogramowania, którego celem są nośniki pamięci USB. Wykrywa ono niezatwierdzone programy i zapobiega ich automatycznemu uruchomieniu. Urządzenie można także odblokować w trybie tylko do odczytu, jeśli zachodzi podejrzenie, że komputer pełniący funkcję hosta jest zainfekowany.

Łatwe zarządzanie urządzeniem – urządzenie obsługuje się za pomocą aplikacji panelu sterowania IronKey, która umożliwia dostęp do plików, zarządzanie urządzeniem i edytowanie preferencji, zmianę hasła do urządzenia oraz jego bezpieczne blokowanie.

Z jakimi systemami współpracuje urządzenie?

- Windows® 11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x lub nowsza wersja). Uwaga: program Linux CLI Unlocker nie obsługuje funkcji wymagających dostępu do sieci, takich jak konfiguracja urządzenia czy zmiana hasła.

Niektóre funkcje są dostępne tylko w określonych systemach:

Tylko system Windows

- Aktualizacje urządzenia

Specyfikacja produktu

Bardziej szczegółowe informacje na temat urządzenia są dostępne na stronie **Device Info** (Informacje o urządzeniu) w panelu sterowania IronKey.

Dane techniczne	Szczegóły
Pojemność*	4GB, 8GB, 16GB, 32GB, 64GB, 128GB
Szybkość**	USB 3.2 Gen 1 - 4GB-32GB: odczyt 180MB/s, zapis 80MB/s - 64GB: odczyt 230MB/s, zapis 160MB/s - 128GB: odczyt 230MB/s, zapis 240MB/s USB 2.0: - 4GB-128GB: odczyt 40MB/s, zapis 35MB/s
Wymiary	82,3 mm x 21,1 mm x 9,1 mm
Wodoodporność	Do ok. 90 cm, MIL-STD-810F
Temperatura	Praca: 0°C do 70°C; przechowywanie: -40°C do 85°C
Szyfrowanie sprzętowe	256-bitowe AES (tryb XTS)
Certyfikat	FIPS 140-2 Level 3
Sprzęt	Zgodność ze standardem USB 3.2 Gen 1 i USB 2.0

Zgodność z systemami operacyjnymi	- Windows 11, Windows 10 (wymaga dwóch wolnych liter dysku) - macOS 12.x – 15.x - Linux 4.4.x***
Gwarancja	5 lat gwarancji. Bezpłatna pomoc techniczna

Zaprojektowane i zmontowane w USA urządzenia S1000B nie wymagają instalacji oprogramowania ani sterowników.

* Podana pojemność jest przybliżona. Wstępnie zainstalowane oprogramowanie wymaga nieco miejsca.
** Prędkość różni się w zależności od sprzętu, oprogramowania i sposobu użytkowania urządzenia pełniącego funkcję hosta.
*** Zestaw ograniczonych funkcji.

Zalecane czynności

1. Zablokuj urządzenie:
   - gdy nie jest używane,
   - przed odłączeniem go,
   - przed przełączeniem systemu w tryb uśpienia.
2. Nigdy nie odłączaj urządzenia, gdy świeci się jego dioda LED.
3. Nigdy nie udostępniaj hasła do urządzenia.
4. Przed skonfigurowaniem i użyciem urządzenia przeprowadź skanowanie antywirusowe komputera.

Konfiguracja urządzenia

Aby zapewnić wystarczające zasilanie szyfrowanej pamięci USB S1000B, podłącz ją bezpośrednio do portu USB 2.0/3.2 Gen 1 w notebooku lub komputerze stacjonarnym. Unikaj podłączania pamięci do jakichkolwiek urządzeń peryferyjnych wyposażonych w port USB, takich jak klawiatura lub koncentrator zasilany przez złącze USB. Początkową konfigurację urządzenia należy przeprowadzić w obsługiwanym systemie operacyjnym Windows lub macOS.

Dostęp do urządzenia (środowisko Windows)

1. Podłącz szyfrowaną pamięć USB S1000B do wolnego portu USB w notebooku lub komputerze stacjonarnym i zaczekaj, aż system Windows ją wykryje.

   - W systemach Windows 10 i 11 wyświetli się powiadomienie dotyczące instalacji sterownika urządzenia.

   - Po wykryciu nowego sprzętu system Windows wyświetli monit o rozpoczęcie procesu inicjalizacji.

2. Wybierz opcję **IronKey.exe** na partycji IRONKEY w Eksploratorze plików. 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:).

Dostęp do urządzenia (środowisko macOS)

1. Podłącz szyfrowaną pamięć USB S1000B do wolnego portu USB w notebooku lub komputerze stacjonarnym z systemem macOS i zaczekaj, aż system operacyjny ją wykryje.

2. Kliknij dwukrotnie wolumin **IRONKEY**, który pojawi się na pulpicie, aby rozpocząć proces inicjalizacji.

   - Jeżeli wolumin IRONKEY nie pojawi się na pulpicie, otwórz okno programu Finder i znajdź wolumin IronKey po lewej stronie (na liście Urządzenia). Zaznacz ten wolumin i kliknij dwukrotnie ikonę aplikacji IRONKEY w oknie programu Finder. Spowoduje to rozpoczęcie procesu inicjalizacji.

Inicjalizacja urządzenia

Inicjalizacja w obsługiwanym systemie operacyjnym Windows lub macOS.

1. Wybierz preferowany język z listy. Domyślnie oprogramowanie urządzenia będzie używać tego samego języka co system operacyjny komputera (jeśli jest dostępny).

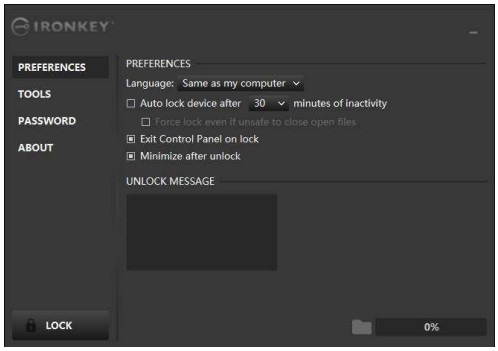
2. Zapoznaj się z umową licencyjną, zaznacz pole wyboru, aby ją zaakceptować, i kliknij przycisk Continue (Kontynuuj).

3. W polu tekstowym Password (Hasło) wpisz hasło urządzenia, a następnie wpisz je ponownie w polu tekstowym Confirm (Potwierdź). Hasło chroni dane zapisane w bezpiecznej pamięci. W haśle rozróżniana jest wielkość liter i musi ono zawierać co najmniej 4 znaki (łącznie ze spacją).

4. W przypadku inicjalizacji w systemie Windows dostępna będzie opcja sformatowania pamięci IronKey Secure Files w systemie plików FAT32, exFAT lub NTFS. Aby uzyskać więcej informacji, patrz Formatowanie urządzenia.

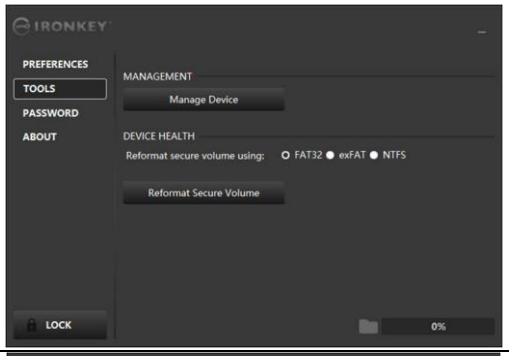
5. Domyślnie włączona jest opcja „Reset the device instead of self-destructing” (Zresetowanie urządzenia zamiast samozniszczenia). Kliknij polecenie Continue (Kontynuuj). Urządzenie zakończy inicjalizację. Po zakończeniu otworzy się panel sterowania IronKey. Urządzenie jest teraz gotowe do przechowywania i ochrony danych.

Panel sterowania IronKey



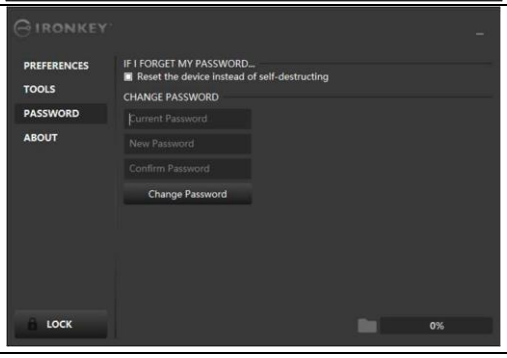
PREFERENCES (PREFERENCJE)

1. Language (Język): zmiana języka urządzenia
2. Auto lock device (Automatyczna blokada urządzenia): zmiana czasu, po jakim nastąpi włączenie blokady
3. Exit on Control Panel on lock (Zamykanie panelu sterowania po zablokowaniu): zmiana ustawienia określającego, czy panel sterowania ma zostać zamknięty, czy pozostać otwarty po zablokowaniu urządzenia.
4. Minimize after unlock (Minimalizacja po odblokowaniu): zmiana ustawienia decydującego o tym, czy po odblokowaniu urządzenia panel sterowania ma zostać zminimalizowany, czy pozostać otwarty.
5. UNLOCK MESSAGE (KOMUNIKAT O ODBLOKOWANIU): dodanie wiadomości, która będzie wyświetlana w oknie logowania.



TOOLS (NARZĘDZIA)

1. MANAGEMENT (ZARZĄDZANIE): zarządzanie urządzeniem (niezbędne jest oprogramowanie SafeConsole).
2. DEVICE HEALTH (KONDYCJA URZĄDZENIA): ponowne formatowanie bezpiecznego woluminu przy użyciu systemu plików FAT32, exFAT lub NTFS (w systemie macOS możliwe jest tylko formatowanie FAT32).



PASSWORD (HASŁO)

1. IF I FORGET MY PASSWORD... (JEŚLI ZAPOMNĘ HASŁA...): włączenie/wyłączenie opcji „Reset the device instead of self-destructing” (Zresetowanie urządzenia zamiast samozniszczenia).
2. CHANGE PASSWORD (ZMIANA HASŁA): zmiana aktualnego hasła na nowe.

ABOUT (INFORMACJE)

1. ABOUT THIS DEVICE (INFORMACJE O URZĄDZENIU): wyświetlenie informacji o urządzeniu.
2. Visit Website (Odwiedź stronę internetową): otwarcie strony internetowej Kingston
3. Legal Notices (Informacje prawne): otwarcie stron internetowych z informacjami prawnymi firm Kingston i DataLocker
4. Certifications (Certyfikaty): otwarcie strony Kingston z informacjami o certyfikatach dla szyfrowanych urządzeń USB

Korzystanie z urządzenia

Weryfikacja bezpieczeństwa urządzenia

Jeśli urządzenie bezpiecznej pamięci USB zostało zgubione lub pozostawione bez nadzoru, należy je sprawdzić zgodnie z poniższymi wskazówkami. Jeśli zachodzi podejrzenie, że ktoś manipulował przy urządzeniu lub autotest zakończy się niepowodzeniem, należy pozbyć się urządzenia.

- Sprawdź wzrokowo bezpieczną pamięć USB, czy nie nosi śladów uszkodzeń, które mogłyby wskazywać na zewnętrzną ingerencję.
- Sprawdź, czy bezpieczna pamięć USB jest nie została fizycznie naruszona, lekko obracając jej końce w przeciwnych kierunkach.
- Sprawdź, czy bezpieczna pamięć USB waży około 30 gramów.
- Po podłączeniu do komputera sprawdź, czy niebieska kontrolka bezpiecznej pamięci USB miga (prawidłowa częstotliwość to 3 razy na sekundę bezpośrednio po podłączeniu i podczas operacji odczytu/zapisu).
- Sprawdź, czy bezpieczna pamięć USB jest wyświetlana przez system jako nośnik DVD-RW oraz czy partycja pamięci nie jest zamontowana do czasu odblokowania urządzenia.
- Przed uruchomieniem sprawdź, czy wydawcą oprogramowania urządzenia w wirtualnym napędzie DVD-RW jest firma DataLocker Inc.

Dostęp 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, podobnie jak w przypadku zwykłej pamięci, zapewniając jednocześnie silną, „zawsze włączoną” ochronę plików.

Aby uzyskać dostęp do zabezpieczonych plików:

1. Kliknij **ikonę folderu**  w prawym dolnym rogu panelu sterowania IronKey.
   - Windows: nastąpi otwarcie folderu pamięci USB IRONKEY SECURE FILES w Eksploratorze plików systemu Windows.
   - macOS: nastąpi otwarcie folderu pamięci USB KINGSTON w programie Finder.
2. Wykonaj jedną z poniższych czynności:
   - Aby otworzyć plik, kliknij go dwukrotnie w oknie pamięci USB S1000B.
   - Aby zapisać plik, przeciągnij go z komputera do okna pamięci USB S1000B.

Wskazówka: można również uzyskać dostęp do plików, klikając prawym przyciskiem myszy **ikonę IronKey** na pasku zadań systemu Windows, a następnie klikając opcję **Secure Files**.

Odblokowywanie w trybie tylko do odczytu

Jeżeli nie chcesz omyłkowo wprowadzić zmian w plikach zapisanych w bezpiecznej pamięci, możesz 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.

Gdy urządzenie znajduje się w tym trybie, panel sterowania IronKey wyświetla informację *Read-Only Mode* (Tryb tylko do odczytu). W tym trybie nie można wykonywać żadnych operacji związanych z modyfikacją plików zapisanych w urządzeniu. Nie można np. ponownie sformatować urządzenia ani edytować plików zapisanych w pamięci.

Aby odblokować urządzenie w trybie tylko do odczytu:

1. Włóż urządzenie do portu USB komputera pełniącego funkcję hosta i uruchom program **IronKey.exe**.
2. Zaznacz **pole wyboru Read-Only** (Tylko do odczytu) poniżej pola wprowadzania hasła.
3. Wprowadź hasło urządzenia i kliknij **Unlock** (Odblokuj). Wyświetli się panel sterowania IronKey z informacją *Read-Only Mode* (Tryb tylko do odczytu) na dole.

Zmiana komunikatu o odblokowaniu

Komunikat o odblokowaniu to niestandardowy tekst wyświetlany w oknie IronKey po odblokowaniu urządzenia. Funkcja ta umożliwia personalizację wyświetlanego komunikatu. Na przykład dodanie danych kontaktowych spowoduje wyświetlenie informacji o tym, jak można zwrócić zgubioną pamięć.

Aby zmienić komunikat o odblokowaniu:

1. Kliknij przycisk **Settings** (Ustawienia) na pasku menu panelu sterowania IronKey.

2. Kliknij przycisk **Preferences** (Preferencje) na lewym pasku bocznym.

3. Wprowadź tekst komunikatu w polu komunikatu o odblokowaniu. Tekst musi zmieścić się w przewidzianym miejscu (ok. 6 wierszy i 200 znaków).

Minimalizacja panelu sterowania po odblokowaniu

Po odblokowaniu urządzenia panel sterowania jest automatycznie minimalizowany do paska zadań. W razie potrzeby panel sterowania może pozostać wyświetlony po odblokowaniu urządzenia.

Aby wyłączyć funkcję minimalizacji po odblokowaniu:

1. W panelu sterowania IronKey kliknij przycisk Preferences (Preferencje) na lewym pasku bocznym.
2. Kliknij pole wyboru Minimize after unlock (Minimalizacja po odblokowaniu).

Blokowanie urządzenia

Zablokuj urządzenie, jeśli go nie używasz, aby zapobiec niepożądanemu dostępowi do zabezpieczonych plików w pamięci. Urządzenie można zablokować ręcznie lub ustawić w taki sposób, aby blokowało się automatycznie po określonym czasie bezczynności.

Uwaga: domyślnie, jeśli w momencie próby automatycznego zablokowania otwarty jest plik lub aplikacja, urządzenie nie wymusi ich zamknięcia. Chociaż można skonfigurować ustawienie automatycznego blokowania w taki sposób, aby wymusić blokadę urządzenia, może to spowodować utratę danych wszystkich otwartych i niezapisanych plików.

Jeśli pliki zostały uszkodzone w wyniku procedury wymuszonego blokowania lub odłączenia urządzenia przed zablokowaniem, być może uda się je odzyskać, uruchamiając program CHKDSK i korzystając z oprogramowania do odzyskiwania danych (tylko system Windows).

Aby ręcznie zablokować urządzenie:

1. Kliknij **Lock** (Zablokuj) w lewym dolnym rogu panelu sterowania IronKey, aby bezpiecznie zablokować urządzenie.

    - Możesz także użyć skrótu klawiaturowego: **CTRL + L** (tylko w systemie Windows); ewentualnie kliknij prawym przyciskiem myszy **ikonę IronKey** na pasku zadań, po czym kliknij opcję **Lock Device** (Zablokuj urządzenie).

Aby ustawić funkcję automatycznego blokowania urządzenia:

1. Odblokuj urządzenie i kliknij przycisk **Settings** (Ustawienia) na pasku menu w panelu sterowania IronKey.

2. Kliknij przycisk **Preferences** (Preferencje) na lewym pasku bocznym.
3. Kliknij **pole wyboru** funkcji automatycznego blokowania urządzenia i wybierz jedno z ustawień czasu bezczynności: 5, 15, 30, 60, 120 lub 180 minut.

Aby uruchomić program CHKDSK (tylko system Windows):

1. Odblokuj urządzenie.
2. Naciśnij klawisz LOGO WINDOWS + R, aby otworzyć okno funkcji Uruchamianie:
3. Wpisz CMD i naciśnij ENTER.
4. W wierszu poleceń wpisz CHKDSK, literę dysku pamięci USB IRONKEY SECURE FILES, a następnie „/F /R”. Na przykład jeśli litera dysku pamięci USB IRONKEY SECURE FILES to G, należy wpisać: CHKDSK G: /F /R
5. W razie potrzeby użyj oprogramowania do odzyskiwania danych, aby odzyskać pliki.

Zamykanie panelu sterowania po zablokowaniu

Po zablokowaniu urządzenia panel sterowania zamknie się automatycznie. Aby odblokować urządzenie i uzyskać dostęp do panelu sterowania, należy ponownie uruchomić aplikację IronKey. W razie potrzeby panel sterowania można ustawić w taki sposób, aby powracał do ekranu odblokowania po zablokowaniu urządzenia przez użytkownika.

Aby wyłączyć funkcję zamykania panelu sterowania po zablokowaniu:

1. Odblokuj urządzenie i kliknij przycisk Settings (Ustawienia) na pasku menu w panelu sterowania IronKey.
2. Kliknij przycisk Preferences (Preferencje) na lewym pasku bocznym.
3. Kliknij pole wyboru Exit Control Panel on lock (Zamykanie panelu sterowania po zablokowaniu).

Zarządzanie hasłami

Hasło do urządzenia można zmienić na karcie Password (Hasło) w panelu sterowania IronKey.

Czasem zmiana hasła jest wymagana w celu zapewnienia zgodności z nowymi zasadami dotyczącymi haseł, które wprowadzono w danej firmie. Jeśli wymagana jest zmiana hasła, przy następnym odblokowaniu urządzenia zostanie wyświetlony ekran Password Change (Zmiana hasła). Jeśli urządzenie jest w użyciu, zostanie zablokowane i przed jego odblokowaniem konieczna będzie zmiana hasła.

Uwaga: gdy wymagane jest podanie hasła, np. podczas logowania do urządzenia lub podczas operacji ręcznej zmiany hasła, do wpisania hasła można użyć klawiatury wirtualnej zamiast klawiatury fizycznej.

Aby zmienić hasło:

1. Odblokuj urządzenie i kliknij przycisk **Settings** (Ustawienia) na pasku menu.
2. Kliknij przycisk **Password** (Hasło) w lewym pasku bocznym.
3. Wprowadź aktualne hasło w odpowiednim polu.

4. Wprowadź i potwierdź nowe hasło w odpowiednich polach.

5. Kliknij przycisk Change Password (Zmień hasło).

Formatowanie urządzenia

Urządzenie będzie wymagało formatowania podczas inicjalizacji, zanim będzie można je użyć do przechowywania plików.

W przypadku inicjalizacji w systemie Windows możliwe jest sformatowanie pamięci USB IRONKEY SECURE FILES w systemie plików FAT32, exFAT lub NTFS.

Opcje te dotyczą tylko systemu operacyjnego Windows – w systemie macOS pamięć zostanie automatycznie sformatowana do formatu FAT32.

- FAT32
  - Zalety: zgodność z wieloma platformami (Windows i macOS)
  - Wady: wielkość pliku ograniczona do 4GB
- exFAT
  - Zalety: brak limitu rozmiaru pliku
  - Wady: Microsoft ogranicza wykorzystane przez zobowiązania licencyjne
- NTFS
  - Zalety: brak limitu rozmiaru pliku
  - Wady: dostęp tylko do odczytu w obsługiwanych systemach macOS

Po inicjalizacji ponowne sformatowanie pamięci USB IRONKEY SECURE FILES spowoduje skasowanie jej całej zawartości z wyjątkiem hasła i ustawień urządzenia.

Ważne: przed ponownym sformatowaniem urządzenia wykonaj kopię zapasową pamięci USB IRONKEY SECURE FILES w innym miejscu – np. w pamięci masowej w chmurze lub na komputerze. Aby ponownie sformatować urządzenie:

1. Odblokuj urządzenie i kliknij przycisk **Settings** (Ustawienia) na pasku menu w panelu sterowania IronKey.

2. Kliknij przycisk **Tools** (Narzędzia) na lewym pasku bocznym.

3. W sekcji Device Health (Kondycja urządzenia) wybierz format plików i kliknij przycisk **Reformat Secure Volume** (Sformatuj bezpieczny wolumin).

Dostęp do informacji o urządzeniu

Skorzystaj z miernika pojemności w prawym dolnym rogu panelu sterowania IronKey, aby określić, ile miejsca jest jeszcze dostępne na urządzeniu. Zielony pasek pokazuje stopień zapełnienia urządzenia. Gdy urządzenie jest pełne, miernik jest w całości zielony. Biały tekst na mierniku pojemności informuje o ilości pozostałego wolnego miejsca.

Ogólne informacje o urządzeniu są dostępne na stronie Device Info (Informacje o urządzeniu).

Aby wyświetlić informacje o urządzeniu:

1. Odblokuj urządzenie i kliknij przycisk **Settings** (Ustawienia) na pasku menu w panelu sterowania IronKey.

2. Kliknij przycisk **Device Info** (Informacje o urządzeniu) na lewym pasku bocznym.

Sekcja About This Device (Informacje o urządzeniu) zawiera następujące informacje dotyczące urządzenia:

- Numer modelu
- Identyfikator sprzętu
- Numer seryjny
- Wersja oprogramowania
- Wersja oprogramowania sprzętowego
- Data wydania
- Litera dysku Secure Files
- Litera dysku IronKey
- System operacyjny i uprawnienia administratora systemu
- Konsola zarządzania

Uwaga: aby przejść na stronę internetową dotyczącą produktów IronKey lub uzyskać więcej szczegółowych informacji na temat not prawnych lub certyfikatów produktów IronKey, kliknij jeden z przycisków na stronie z informacjami o urządzeniu.

Wskazówka: kliknij przycisk **Copy** (Kopiuj), aby skopiować informacje o urządzeniu w celu wklejenia ich w wiadomości e-mail lub w zgłoszeniu do działu pomocy technicznej.

Resetowanie urządzenia

Urządzenie można przywrócić do ustawień fabrycznych. Spowoduje to bezpieczne wymazanie wszystkich danych z urządzenia i utworzenie nowego klucza bezpieczeństwa.

Resetowanie urządzenia:

1. Odblokuj urządzenie.

2. Kliknij prawym przyciskiem myszy **ikonę IronKey** na pasku zadań.

3. Kliknij przycisk Reset Device (Resetuj urządzenie).

Aby zapobiec przypadkowemu zresetowaniu urządzenia, pojawi się wyskakujące okienko z prośbą o wprowadzenie czterech losowych cyfr. Po wprowadzeniu potwierdzenia urządzenie zostanie zresetowane do ustawień fabrycznych.

Korzystanie z urządzenia w systemie Linux

Urządzenia można używać na kilku dystrybucjach systemu Linux. W folderze linux znajdują się dwa pliki wykonywalne, Unlocker_32.exe i Unlocker_64.exe. Należy zastąpić plik Unlocker_xx.exe plikiem wykonywalnym kompatybilnym z systemem.

Urządzenie należy wcześniej skonfigurować w systemie operacyjnym Windows lub macOS. Więcej szczegółowych informacji znajduje się w części Konfiguracja urządzenia.

Korzystanie z funkcji odblokowania

Użyj programu Unlocker_xx.exe dla systemu Linux, aby uzyskać dostęp do plików. W zależności od dystrybucji systemu Linux do korzystania z programu Unlocker_xx.exe znajdującego się w folderze Linux zamontowanego woluminu publicznego mogą być potrzebne uprawnienia roota. Domyślnie większość dystrybucji Linux dodaje bit execute do plików .exe na partycji fat32. W przeciwnym razie należy przed uruchomieniem ustawić bit execute ręcznie, korzystając z następujących poleceń:

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

Jeśli do systemu podłączone jest tylko jedno urządzenie, uruchom program z wiersza poleceń bez argumentów (np. Unlocker_xx.exe). Wyświetli się monit o podanie hasła urządzenia w celu odblokowania pamięci. Jeśli korzystasz z kilku urządzeń, musisz określić, które z nich chcesz odblokować.

Oto dostępne parametry dla oprogramowania urządzenia:

Opcje:

```
-h, -help         pomoc
-l, -lock         zablokuj urządzenie
-r, -readonly     odblokuj tylko do odczytu
```

Uwaga: program Unlocker_xx.exe tylko odblokowuje pamięć USB IRONKEY SECURE FILES – następnie należy ją zamontować. Wiele nowoczesnych dystrybucji Linux robi to automatycznie. W przeciwnym razie należy uruchomić program montujący z wiersza poleceń, używając nazwy urządzenia określonej przez program Unlocker_xx.exe.

Samo odmontowanie urządzenia nie powoduje automatycznego zablokowania pamięci USB IRONKEY SECURE FILES. Aby zablokować urządzenie, należy odmontować je i fizycznie wyjąć (odłączyć) lub uruchomić program:

- Unlocker_xx.exe -l

Należy zwrócić uwagę na następujące ważne szczegóły dotyczące korzystania z urządzenia w systemie Linux:

1. Wymagane jest jądro w wersji 4.4.x lub nowszej.
2. Montowanie
   - Upewnij się, że masz uprawnienia do montowania zewnętrznych urządzeń SCSI i USB.
   - Niektóre dystrybucje nie montują urządzeń automatycznie i wymagają uruchomienia następującego polecenia: mount /dev/[nazwa urządzenia] / media/ [nazwa montowanego urządzenia]

3. Nazwa zamontowanego urządzenia różni się w zależności od dystrybucji.

4. Uprawnienia

   - Niezbędne są uprawnienia do montowania urządzeń external/usb/devices.
   - Niezbędne są uprawnienia do uruchamiania pliku wykonywalnego z woluminu publicznego, aby uruchomić program Unlocker.
   - Mogą być potrzebne uprawnienia użytkownika na poziomie root.

5. W przypadku systemu Linux pamięć IronKey obsługuje systemy x86 oraz x86_64.

Jak uzyskać pomoc?

Więcej informacji na temat produktów IronKey jest dostępnych na poniższych stronach. Wszelkie pytania należy kierować do działu pomocy technicznej firmy Kingston.

- kingston.com/usb/encrypted_security: informacje, materiały marketingowe i samouczki wideo.
- kingston.com/support: pomoc techniczna, odpowiedzi na najczęściej zadawane pytania i pliki do pobrania

UWAGA: IronKey nie ponosi odpowiedzialności za błędy techniczne, redakcyjne lub pominięcia w niniejszym dokumencie ani za przypadkowe lub wtórne szkody wynikające z dostarczenia lub wykorzystania tego materiału. Informacje zawarte w niniejszym dokumencie mogą ulec zmianom bez uprzedzenia. Informacje zawarte w niniejszym dokumencie przedstawiają pogląd IronKey na omawianą kwestię aktualny na dzień publikacji. IronKey nie może zagwarantować dokładności jakichkolwiek informacji prezentowanych po dacie publikacji. Niniejszy dokument służy wyłącznie do celów informacyjnych. IronKey nie udziela w niniejszym dokumencie żadnych gwarancji, wyrażonych wprost ani domniemanych. IronKey i logo IronKey są znakami towarowymi firmy Kingston Digital, Inc. i jej spółek zależnych. Wszystkie inne znaki towarowe są własnością odpowiednich właścicieli. IronKey™ to zastrzeżony znak towarowy firmy Kingston Technologies, używany za zgodą firmy Kingston Technologies. Wszelkie prawa zastrzeżone.

Informacje dotyczące FCC: urządzenie jest zgodne z częścią 15 przepisów FCC. Działanie urządzenia podlega następującym dwóm warunkom: (1) urządzenie nie może powodować niepożądanych zakłóceń oraz (2) musi być odporne na zewnętrzne zakłócenia, również te, które mogą powodować niepożądane działanie. Urządzenie poddano testom potwierdzającym zgodność z wymaganiami określonymi dla urządzenia cyfrowego klasy B, zgodnie z częścią 15 przepisów FCC. Wymagania te określają odpowiedni poziom zabezpieczeń przed szkodliwymi zakłóceniami w instalacjach mieszkaniowych. Urządzenie wytwarza, wykorzystuje i emituje fale o częstotliwościach radiowych, dlatego jeśli nie jest zainstalowane i używane zgodnie z instrukcją obsługi, może powodować zakłócenia w łączności radiowej. Nie ma jednak gwarancji, że zakłócenia nie wystąpią w konkretnej instalacji. Jeśli urządzenie powoduje szkodliwe zakłócenia w odbiorze radiowym lub telewizyjnym, co można stwierdzić poprzez wyłączenie i ponowne włączenie urządzenia, użytkownik może podjąć próbę wyeliminowania zakłóceń poprzez następujące działania:

- Zmiana kierunku lub położenia anteny odbiorczej.
- Zwiększenie odległości między urządzeniem a odbiornikiem.
- Podłączenie urządzenia do gniazdka w innym obwodzie niż ten, do którego podłączony jest odbiornik.
- Skontaktowanie się sprzedawcą lub doświadczonym technikiem radiowo-telewizyjnym w celu uzyskania pomocy.

Uwaga: zmiany lub modyfikacje, które nie zostały wyraźnie zatwierdzone przez stronę odpowiedzialną za zapewnienie zgodności z przepisami, mogą skutkować utratą praw użytkownika do obsługi urządzenia.

IRONKEY™ S1000B
暗号化機能付きUSB 3.2 Gen 1フラッシュドライブ

ユーザーガイド

目次

このガイドについて (04152025)

IronKey™ S1000Bは、アンマネージドドライブです。

クイックスタート

Windows 11 & 10、macOS 12.x～15.x

1. デバイスをコンピュータのUSBポートに接続します。
2. デバイス設定ウィンドウが表示されたら、画面の指示に従ってください。このウィンドウが表示されない場合は、手動で開いてください：
    - Windows：[スタート] > [このPC] > [IronKey Unlocker] > [IronKey.exe]
    - macOS：[Finder] > [IRONKEY] > [IronKey.app]
3. デバイスのセットアップが完了した後は、重要なファイルを「IRONKEY SECURE FILES USBドライブ」に移動するだけで、自動的に暗号化されます。

Windowsシステムによっては、デバイスを初めて接続した後に再起動を促すものがあります。新しいドライバーまたはソフトウェアはインストールされないため、再起動する必要なく、プロンプトを安全に閉じることができます。

デバイスについて

IronKey S1000B USB 3.2 Gen 1は、パスワードセキュリティとデータ暗号化機能を内蔵したポータブルフラッシュドライブです。モバイルデータセキュリティを強化する、高度なAES 256ビット暗号化やその他の機能を搭載しています。どこへ行くにもファイルやデータを安全に持ち運ぶことができます。

通常のUSBドライブとの違い

FIPS 140-2レベル3認証 – IronKey S1000BはFIPS認証デバイスであるため、規制要件に準拠していると安心してご利用いただけます。

ハードウェア暗号化 – デバイスの高度暗号化コントローラが、政府の機密情報と同じ保護レベルでデータを保護します。このセキュリティテクノロジー機能は常に有効となっており、無効にすることはできません。

パスワード保護 – デバイスはパスワードで保護されており、安全にアクセスできます。パスワードは誰にも教えないでください。たとえデバイスを紛失したり盗まれたりしても、他の誰もあなたのデータにアクセスできません。

デバイスリセット – 暗号化コントローラが物理的改ざんを検知した場合、または誤ったパスワードが11回以上連続して入力された場合、デバイスはリセットされます。**重要 -** デバイスをリセットすると、搭載されているデータはすべて消去され、*デバイスは工場出荷時の設定に戻ります*。したがって、パスワードを忘れないようにしてください。

アンチマルウェア・オートラン保護 – デバイスは未承認プログラムのオートラン実行を検出および防止することで、USBドライブを標的とする最新のマルウェア脅威の多くからユーザを保護することができます。ホストコンピューターの感染が疑われる場合は、読み取り専用モードの解除もできます。

シンプルなデバイス管理 – デバイスには、IronKeyコントロールパネル、ファイルアクセスプログラム、デバイスの管理とシステム環境設定の編集、デバイスパスワードの変更、安全なデバイスのロックの機能が内蔵されています。

使用可能なシステム

- Windows®11
- Windows® 10
- macOS® 12.x – 15.x
- Linux （4.4.x以上） 注：Linux CLI Unlockerは、ネットワークアクセスを必要とする機能、例えばデバイスのセットアップやパスワード変更をサポートしていません。

一部の機能は、特定のシステムでのみ利用できます：

Windowsのみ

- デバイスの更新

製品仕様

デバイスの詳細情報は、IronKeyコントロールパネルの**デバイス情報**ページを参照してください。

仕様	詳細
容量*	4GB、8GB、16GB、32GB、64GB、128GB
速度**	USB 3.2 Gen 1 - 4GB-32GB:180MB/秒（読み取り）;80MB/秒（書き込み） - 64GB:230MB/秒（読み取り）;160MB/秒（書き込み） - 128GB:230MB/秒（読み取り）;240MB/秒（書き込み） USB 2.0: - 4GB-128GB:40MB/秒（読み取り）、35MB/秒（書き込み）
寸法	82.3 mm x 21.1 mm x 9.1 mm
防水	最大90cm（3フィート）；MIL-STD-810F
温度	動作温度：0°C〜70°C ; 保管温度：-40℃〜85℃
ハードウェア暗号化	256-bit AES (XTSモード)
認証	FIPS 140-2 レベル 3認証済み
ハードウェア	USB 3.2 Gen 1準拠およびUSB 2.0互換

対応OS	- Windows 11、Windows 10 (2つの空きドライブレターが必要) - macOS 12.x – 15.x - Linux 4.4.x***
保証	5 年保証。無料サポート

米国で設計/組立。S1000Bデバイスはソフトウェアやドライバーのインストールを必要としません。

* 表示容量は概算です。オンボードソフトウェア用に若干の空間が必要です。
** ホストハードウェア、ソフトウェア、使用状況により、速度は変化します。
*** 機能は限定されます。

推奨される使用方法

1. 次の場合はデバイスをロックしてください：
   - 使用していないとき
   - 電源をオフにする前
   - システムがスリープモードに入る前
2. LEDの点灯中にデバイスを抜かないでください。
3. デバイスのパスワードを決して共有しないでください。
4. デバイスをセットアップして使用する前に、コンピュータのアンチウイルススキャンを実行してください。

デバイスのセットアップ

S1000B暗号化USB ドライブに十分な電力を供給できるよう、ノートパソコンまたはデスクトップパソコンのUSB 2.0/3.21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OSで実行しなければなりません。

デバイスアクセス（Windows環境）

1. S1000B暗号化USBドライブを、ノートパソコンまたはデスクトップパソコンの空いているUSBポートに差し込み、Windowsがこのドライブを検出するまで待ちます。

   - Windows 11および10のユーザーには、デバイスドライバーの通知が届きます。

   - 新しいハードウェアの検出が完了すると、Windowsは初期化プロセスを開始するよう通知します。

2. ファイルエクスプローラーでIRONKEYパーティション内の**IronKey.exe**オプションを選択します。パーティションの文字は、空き状況に応じて異な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。

デバイスアクセス（macOS環境）

1. S1000B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。

2. デスクトップに表示される**IRONKEY**ボリュームをダブルクリックして、初期化プロセスを開始します。

   - IRONKEYボリュームがデスクトップに表示されない場合は、Finderを開き、Finderウィンドウの左側にあるIronKeyボリュームを探します（[デバイス]の下に表示されます）。ボリュームをハイライトして [Finder] ウィンドウにある [IRONKEY] アプリケーションのアイコンをダブルクリックします。これにより、初期化プロセスが開始されます。

デバイスの初期化

サポートされているWindowsまたはmacOSオペレーティングシステムで初期化を行います。

1. リストから言語設定を選択します。デフォルト設定の場合、デバイスソフトウェアは、ユーザーパソコンのOSと同じ言語を使用します(対応している場合)。

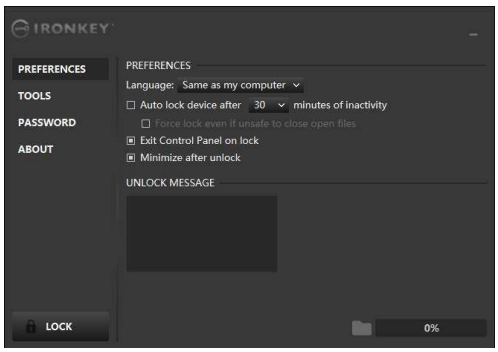
2. 使用許諾契約書を確認し、同意する場合はチェックボックスにチェックを入れ、[続行]をクリックします。

3. [パスワード] テキストボックスにデバイスのパスワードを入力し、[確認] テキストボックスにパスワードを再入力します。パスワードはセキュア・ドライブ上のデータを保護します。パスワードは大文字と小文字を区別し、4文字以上（スペースを含む）である必要があります。

4. Windowsで初期化する場合、IronKey Secure FilesドライブをFAT32、exFAT、またはNTFSのいずれかでフォーマットするオプションが表示されます。詳細については、デバイスのフォーマットを参照してください。

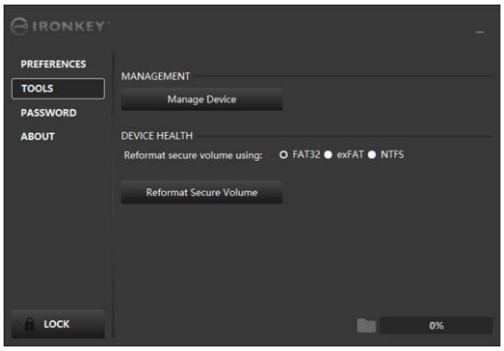
5. デフォルトでは [自己破壊の代わりにデバイスをリセット]オプションは有効になっています。[続ける] をクリックします。デバイスの初期化が終了します。完了すると、IronKeyコントロールパネルが開きます。これでお使いのデバイスは、データを保存し保護する準備が整いました。

IronKeyコントロールパネル



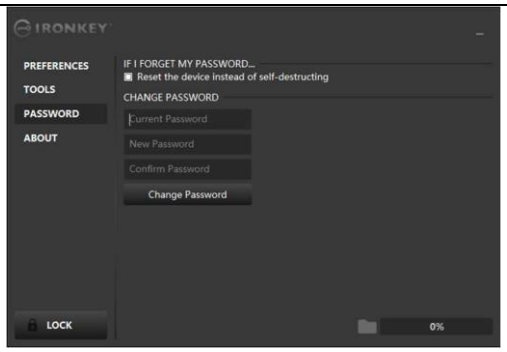
システム環境設定

1. 言語：デバイスの言語を変更する
2. オートロックデバイス：ロックアウト・タイマーの変更
3. ロックのコントロールパネルで終了する：デバイスがロックされているときにコントロールパネルを終了するか、開いたままにするかを変更します。
4. ロック解除後に最小化する：デバイスのロックが解除されたときにコントロールパネルを最小化するか、最大化したままにするかを変更します。
5. メッセージを解除する：ログインウィンドウに表示されるメッセージを追加します。



ツール

1. 管理：デバイスの管理（SafeConsoleが必要です）。
2. デバイスヘルス：FAT32、exFAT、またはNTFSを使用して安全なボリュームを再フォーマットします。(macOSではFAT32のみフォーマット可能)



パスワード

1. パスワードを忘れた際の処置：有効/無効□自己破壊の代わりにデバイスをリセットします。
2. パスワードの変更：現在のパスワードを新しいパスワードに変更します。

デバイスについて

1. デバイスについて：デバイス情報を一覧表示します。
2. ウェブサイトを見る：Kingston のウェブサイトを開きます
3. 法的告知：KingstonとDataLockerの法的声明ウェブサイトを開きます
4. 認証：暗号化されたUSBデバイスに関するKingstonの認証ページを開きます

マイデバイスの使用

デバイスのセキュリティを確認する

セキュアUSBストレージ・デバイスを紛失したり、放置した場合は、以下のユーザーガイダンスに従って検証する必要があります。セキュアUSBストレージ・デバイスは、攻撃者による改ざんが疑われる場合、またはセルフテストが失敗した場合、廃棄されます。

- セキュアUSBストレージ・デバイスを目視で確認し、改ざんを示すような跡や新しい傷がないことを確認します。
- セキュアUSBストレージ・デバイスを少しひねって、物理的に損傷がないことを確認します。
- セキュアUSBストレージ・デバイスの重量が約30グラムであることを確認します。
- コンピュータに接続した際、セキュアUSBストレージ・デバイスの青いインジケータライトが点滅することを確認します（正しい点滅頻度は、最初の接続時および読み取り/書き込み操作時に1秒間に3回）。
- セキュアUSBストレージ・デバイスがDVD-RWとして表示され、デバイスのロックが解除されるまでストレージパーティションがマウントされないことを確認します。
- 実行する前に、仮想DVD-RWドライブのデバイスソフトウェアがDataLocker Inc.によって発行されたものであることを確認します。

保護下のファイルへのアクセス

デバイスのロック解除後、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。

セキュアファイルにアクセスするには：

1. IronKeyコントロールパネルの右下にある**フォルダアイコン**  をクリックします。

   - Windows:Windowsエクスプローラを開き、IRONKEY SECUREFILES USBドライブを開きます。

   - macOS:Finderを開いて、KINGSTON USBドライブを表示します。

2. 以下のいずれかを行ってください。

   - S1000USBドライブ上のファイルをダブルクリックしてファイルを開きます。

   - コンピュータからS1000BUSBドライブにファイルをドラッグしてファイルを保存します。

ヒント：また、Windowsタスクバーの**IronKeyアイコン**を右クリックし、[**ファイルをセキュアにする**]をクリックすることでもファイルにアクセスできます。

読み取り専用モードの解除

セキュア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。

このモードで作業している場合、IronKey コントロールパネルには*「読み取り専用モード」*テキストが表示されます。このモードでは、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編集はできません。

読み取り専用モードのデバイスのロックを解除するには：

1. ホストコンピュータのUSBポートにデバイスを差し込み、**IronKey.exe**を実行します。

2. パスワード入力欄の下にある**「読み取り専用」チェックボックス**にチェックを入れます。

3. デバイスのパスワードを入力して「**アンロック**」をクリックします。IronKeyコントロールパネルが表示され、下部に*「読み取り専用モード」*と表示されます。

ロック解除メッセージの変更

解除メッセージは、デバイスのロックを解除する場合にIronKeyで表示されるカスタムテキストです。この機能で、表示するメッセージをカスタマイズできます。例えば、連絡先情報を追加すれば、ドライブを紛失した場合に返却方法の情報を表示できます。

ロックの解除メッセージを変更するには：

1. IronKeyコントロールパネルで、メニューバーの[**設定**]をクリックします。
2. 左サイドバーの [**システム環境設定**] をクリックします。
3. [ロックを解除] メッセージフィールドのメッセージを入力します。本文は指定されたスペース（約6行、200文字）に収まるものでなければなりません。

ロック解除時にコントロールパネルを最小化

デバイスのロックが解除されると、コントロールパネルは自動的にタスクバーに最小化されます。必要であれば、デバイスのロックが解除された後もコントロールパネルを表示したままにすることができます。

ロック解除後の最小化を無効にする：

1. IronKeyコントロールパネルで、左サイドバーの[システム環境設定]をクリックします。
2. [ロック解除後に最小化する] のチェックボックスをクリックします。

デバイスのロック

使用していないときはデバイスをロックし、ドライブ上の安全なファイルへの不要なアクセスを防ぎます。手動でデバイスをロックすることも、一定時間操作がないと自動的にロックされるように設定することもできます。

注意：デフォルトでは、ファイルまたはアプリケーションが開いている場合にデバイスを自動ロックしようとすると、ファイルやアプリケーションを強制終了できません。デバイスを強制的にロックするよう自動ロック設定を行うこともできますが、その場合、開いているファイルや保存していないファイルのデータが失われる可能性があります。

強制ロック手順や、ロック前にデバイスのプラグを抜いたためにファイルが破損した場合は、CHKDSKを実行し、データ復元ソフトウェア（Windowsのみ）を使用することでファイルを復元できる可能性があります。

手動でデバイスをロックするには：

1. IronKeyコントロールパネルの左下にある[**ロック**]をクリックすると、デバイスが安全にロックされます。
   - キーボードショートカットも使用できます：**CTRL + L**（Windowsのみ）、またはシステムトレイの**IronKeyアイコン**を右クリックし、[**デバイスのロック**]をクリックします。

デバイスに自動ロックを設定するには：

1. デバイスのロックを解除し、IronKeyコントロールパネルのメニューバーにある[**設定**]をクリックします。

2. 左サイドバーの [**システム環境設定**] をクリックします。
3. デバイスを自動ロックするための**チェックボックス**をクリックし、以下の時間間隔のいずれかにタイムアウトを設定します：5分、15分、30分、60分、120分、180分。

CHKDSKの実行方法（Windowsのみ）：

1. デバイスのロックを解除します。
2. WINDOWSキー + Rを押してRunプロンプトを開きます。
3. 「CMD」と入力し、「ENTER」キーを押します。
4. コマンドプロンプトから、CHKDSK、IRONKEY SECURE FILES USBドライブレター、次に「/F /R」と入力します。例えば、IRONKEY SECURE FILES USBのドライブレターがGの場合、次のように入力します：CHKDSK G:/F /R
5. 必要に応じて、データ復元ソフトウェアを使用してファイルを復元してください。

ロックのコントロールパネルから出ます

デバイスがロックされると、コントロールパネルは自動的に閉じます。デバイスのロックを解除してコントロールパネルにアクセスするには、IronKeyアプリケーションを再度実行する必要があります。必要であれば、ユーザーがデバイスをロックした後、コントロールパネルがロック解除画面に戻るように設定できます。

ロック時のコントロールパネル終了を無効にする：

1. デバイスのロックを解除し、IronKeyコントロールパネルのメニューバーにある[設定]をクリックします。
2. 左サイドバーの [システム環境設定] をクリックします。
3. [ロック時にコントロールパネルを終了する]チェックボックスをクリックします。

パスワードの管理

IronKeyコントロールパネルの [パスワード] タブにアクセスして、デバイスのパスワードを変更できます。

企業の新しいパスワードポリシーに準拠するため、パスワードの変更を求められることがあります。変更が必要な場合、次回ロック解除時にパスワード変更画面が表示されます。デバイスが使用中であればロックされ、ロックを解除する前にパスワードを変更する必要があります。

パスワードを変更するには：

1. デバイスのロックを解除し、メニューバーの[**設定**]をクリックします。
2. 左サイドバーの [**パスワード**] をクリックします。
3. 現在しているパスワードを指定のフィールドに入力します。

4. 新しいパスワードを入力し、指定されたフィールドで確認します。

5. [パスワードを変更] をクリックします。

デバイスのフォーマット

デバイスへファイルを保存する前に、デバイスの初期化中にフォーマットする必要があります。

Windowsで初期化する場合、IRONKEY SECURE FILES USBドライブをFAT32、exFAT、またはNTFSのいずれかでフォーマットするオプションが与えられます。

オプションはWindows OSのみです。macOSは自動的にFAT32にフォーマットします。

- FAT32
  - 利点：クロスプラットフォーム対応（WindowsおよびMac OS）
  - 欠点：個別ファイルのサイズは4GBに制限されます
- exFAT
  - 利点：ファイルサイズ制限がありません
  - 欠点：ライセンス義務に基づき、Microsoftが使用を制限しています
- NTFS
  - 利点：ファイルサイズ制限がありません
  - 欠点：サポート対象のmacOSでは、読み込み専用アクセスとしてマウントされます

初期化後、IRONKEY SECURE FILES USBドライブを再フォーマットすると、クイックフォーマットが実行され、空のドライブが提供されますが、デバイスのパスワードと設定は消去されません。

重要:デバイスを再フォーマットする前に、IRONKEY SECURE FILES USBドライブを別の場所（クラウドストレージやコンピューターなど）にバックアップしてください。
デバイスを再フォーマットするには：

1. デバイスのロックを解除し、IronKeyコントロールパネルのメニューバーにある[**設定**]をクリックします。

2. 左サイドバーの [**ツール**] をクリックします。

3. デバイスヘルスでファイル形式を選択し、[**セキュアボリュームの再フォーマット**]をクリックします。

デバイス情報の検索

IronKeyコントロールパネルの右下にある容量メーターで、デバイスのストレージ空き容量を確認できます。緑色のグラフバーは、デバイスの使用済容量を表しています。例えば、デバイスが満タンの場合、メーターは完全に緑色になります。容量メーターの白い文字は、残りの空き容量を表示します。

デバイスの一般的な情報については、デバイス情報ページを参照してください。

デバイス情報を表示するには：

1. デバイスのロックを解除し、IronKeyコントロールパネルのメニューバーにある[**設定**]をクリックします。

2. 左サイドバーの [**デバイス情報**] をクリックします。

[このデバイスについて] には、デバイスの以下の詳細情報が含まれています。

- モデル番号
- ハードウェアID
- シリアル番号
- ソフトウェアバージョン
- ファームウェアバージョン
- 発売日
- 安全なファイルのドライブレター
- IronKeyドライブレター
- オペレーティングシステムおよびシステム管理者権限
- 管理コンソール

注：IronKeyのウェブサイトにアクセスしたり、IronKey製品の法的通知や認証に関する詳細情報にアクセスしたりするには、デバイス情報ページのいずれかの情報ボタンをクリックしてください。

ヒント：[**コピー**] をクリックして、デバイス情報をクリップボードにコピーし、メールまたはサポートリクエストに貼り付けます。

デバイスのリセット

デバイスは、工場出荷時設定に戻すことができます。これにより、デバイスからすべてのデータを安全に消去し、次回使用のために新しいセキュリティキーを作成します。

デバイスのリセット：

1. デバイスのロックを解除します。

2. システムトレイの**IronKeyアイコン**を右クリックします。

3. [デバイスのリセット] をクリックします。

誤ってデバイスがリセットされるのを防ぐため、ポップアップでランダムな4桁の数字を入力するよう求められます。認証を入力すると、デバイスは工場出荷時の設定にリセットされます。

Linuxでのデバイスの使用

複数のLinuxディストリビューションでデバイスを使用できます。Linuxフォルダーに2つの実行可能ファイル、「Unlocker_32.exe」と「Unlocker_64.exe」があります。このガイドでは、お客様のシステムと互換性がある実行可能ファイル「Unlocker_xx.exe」に読み替えてください。

デバイスは、事前にWindowsまたはmacOSのOSを使用して設定しておく必要があります。詳細については、デバイスのセットアップを参照してください。

Unlockerの使用

ファイルにアクセスするには、Linux用のUnlocker_xx.exeを使用してください。ご使用のLinuxディストリビューションによっては、マウントされたパブリック・ボリュームのLinuxフォルダにあるUnlocker_xx.exeプログラムを使用するためにroot権限が必要な場合があります。デフォルトでは、ほとんどのLinuxディストリビューションは、fat32パーティション上の.exeファイルに実行ビットを付加します。そうでない場合、以下のコマンドを使用して実行前に手動で実行ビットを設定する必要があります。

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

システムにデバイスが1台しか接続されていない場合は、引数なしでコマンドシェルからプログラムを実行してください（例：Unlocker_xx.exe）。この場合、続いてドライブのロック解除のためにデバイスのパスワード入力を求められます。複数のデバイスをお持ちの場合は、ロックを解除するデバイスを指定する必要があります。

これらは、デバイス・ソフトウェアで使用可能なパラメーターです：

モデル:

`-h, -help`	ヘルプ
`-l, -lock`	デバイスをロック
`-r, -readonly`	読み取り専用としてロック

注：Unlocker_xx.exeはIRONKEY SECURE FILES USBのロックを解除するだけです。現在の多くのLinuxディストリビューションでは、これを自動的に実行します。そうでない場合は、Unlocker_xx.exeが出力したデバイス名を使用して、コマンドラインからマウント・プログラムを実行してください。

デバイスをアンマウントしただけでは、IRONKEY SECURE FILES USBは自動的にロックされません。デバイスをロックするには、アンマウントして物理的に取り外す（プラグを抜く）か、次のコマンドを実行する必要があります。

- Unlocker_xx.exe -l

Linuxでデバイスをご使用する場合は、以下の重要情報に注意してください：

1. カーネルバージョンは4.4.x以上である必要があります。
2. マウント
   - 外部SCSIおよびUSBデバイスをマウントする権限を持っていることを確認します。
   - ディストリビューションによっては自動的にマウントされず、次のコマンドを実行する必要があります：mount /dev/[name of the device] / media/ [mounted device name]

3. マウントされたデバイスの名前は、ディストリビューションによって異なります。

4. 権限

   - 外部/usb/デバイスをマウントする権限が必要です。
   - アンロッカーを起動するには、パブリック・ボリュームから実行ファイルを実行する権限が必要です。
   - ルートユーザー権限が必要になる場合があります。

5. Linux用IronKeyはx86およびx86_64システムをサポートしています。

ヘルプ情報の入手

以下のリソースでは、IronKey製品に関する詳細情報を提供しています。ご不明な点はKingstonのサポートまでお問い合わせください。

- kingston.com/usb/encrypted_security:情報、マーケティング資料、ビデオチュートリアル。
- kingston.com/support:製品サポート、FAQ、ダウンロード

注記：Kingston は、本書に含まれる技術的または編集上の誤りや脱落、およびこの資料の提供または使用に起因する偶発的または結果的損害について責任を負いません。本書に記載されている情報は、予告なしに変更されることがあります。本文書に記載されている情報は、発行日現在におけるIronKeyの見解を示すものです。IronKey は、発行日以降に提示された情報の正確性を保証することはできません。本書は情報提供のみを目的としています。IronKeyは本書において、明示または黙示を問わず、いかなる保証も行いません。IronKey、およびIronKey ロゴは、Kingston Digital, Inc.および関連会社の商標です。その他の商標は各所有者に帰属します。IronKey™はKingston Technologiesの登録商標であり、Kingston Technologiesの許可を得て使用しています。無断 複写・転載を禁じます。

FCC情報本機器は FCC 規定第 15 項に準拠しています。操作には、以下の 2 つの条件が適用されます。（1）このデバイスは有害な干渉を引き起こしてはならず、（2）このデバイスは、望ましくない動作を引き起こす可能性のある干渉を含め、受信したあらゆる干渉を受け入れなければなりません。本機はFCC規定第15章によるクラスBのデジタル装置の規制に準拠していることが試験により確認されています。これらの規制は、住宅に設置した状態で、有害な電波障害から適切に保護することを目的としています。この装置は無線周波数エネルギーを生成、使用、放射するおそれがあるため、指示に従って設置および使用しないと、無線通信に有害な干渉を引き起こすおそれがあります。ただし、特定の設置条件で電波障害が発生しないと保証するものではありません。本機がラジオやテレビに有害な電波障害を引き起こしている場合、本機の電源をオン/オフにすることで検証できます。電波障害を引き起こしている場合は、次のいずれかの方法で解消することをお勧めします。

- 受信アンテナの方向または場所を変える。
- 本機と受信機を離す。
- 本機を受信機とは別のコンセントに接続する。
- 販売店または専門のラジオ/TV 技術者に問い合わせる。

注：コンプライアンスに責任を負っている当該団体によって明示的に承認されていない変更または改良を行うと、本機を操作するユーザーの権限が無効になる場合があります。

IRONKEY™ S1000B
USB 3.2 Gen 1 加密闪存盘

用户指南

目录

关于本指南 (04152025)

IronKey™ S1000B 不是受管理的闪存盘。

快速启动

Windows 11、10 和 macOS 12.x – 15.x

1. 将设备插入计算机的 USB 端口。
2. 当“设备设置”窗口出现时，按照屏幕上的说明操作。如果此窗口未出现，请手动将其打开：
    - Windows：开始 > 此电脑 > IronKey Unlocker > IronKey.exe
    - macOS：Finder > IRONKEY > IronKey.app
3. 当设备设置完成后，您可以将重要的文件移至 IRONKEY SECURE FILES USB 闪存盘，它们将被自动加密。

有些 Windows 系统首次插入设备后会提示重新启动。您可以安全关闭该提示，无需重启 - 因为并没有安装新的驱动程序或软件。

关于我的设备

IronKey S1000B USB 3.2 Gen 1 是一款内置密码安全和数据加密功能的便携式闪存盘。它采用高级 AES 256 位加密和其他可提高移动数据安全性的功能。现在，无论您走到哪里，都可以安全地随身携带您的文件和数据。

本设备与普通 USB 闪存盘有何区别?

FIPS 140-2 Level 3 认证 – IronKey S1000B 是一款获得 FIPS 认证的设备，因此您尽可放心，因为您符合法规要求。

硬件加密 – 设备中的高级加密控制器为您的数据提供的保护级别与高度机密的政府信息相同。这项安全技术功能始终启用，无法禁用。

密码保护 – 设备使用密码对设备访问提供防护。请勿与任何人共享您的密码，这样即使您的设备丢失或被盗，其他人也无法访问您的数据。

设备重置 – 如果高级加密控制器检测到物理篡改，或密码连续输错超过 10 次，设备将启动重置操作。**重要提示** - 当设备重置时，所有板载数据将被擦除，设备将恢复到出厂设置，*因此请记住您的密码*。

防恶意软件自动运行保护 – 您的设备可以通过检测和阻止未经批准程序的自动运行，来保护您免受许多针对 USB 闪存盘的最新恶意软件威胁。如果怀疑主机计算机已被感染，还可以在只读模式下解锁设备。

简易设备管理 – 您的设备包含 IronKey Control Panel（控制面板）程序，用于访问自己的文件、管理设备并编辑偏好、更改设备密码和安全锁定设备。

它可以在什么系统上使用?

- Windows®11
- Windows® 10
- macOS® 12.x – 15.x
- Linux（4.4 或更高版本） 注意：Linux CLI Unlocker 不支持任何需要访问网络的功能，例如设置设备或更改密码。

一些功能仅在特定系统上提供:

仅限 Windows

- 设备更新

产品规格

有关设备的更多信息，请查看 IronKey Control Panel（控制面板）的 **Device Info**（设备信息）页面。

规格	详细信息
存储容量*	4GB、8GB、16GB、32GB、64GB、128GB
速度**	USB 3.2 Gen 1 - 4GB-32GB：180MB/秒读取速度；80MB/秒写入速度 - 64GB：230MB/秒读取速度；160MB/秒写入速度 - 128GB：230MB/秒读取速度；240MB/秒写入速度 USB 2.0： - 4GB-128GB：40MB/秒读取速度、35MB/秒写入速度
尺寸	82.3 mm x 21.1 mm x 9.1 mm
防水/防尘	深达 3 英尺；MIL-STD-810F
温度	操作：0°C 到 70°C；存放：-40°C 到 85°C
硬件加密	256 位 AES（XTS 模式）
认证	通过了 FIPS 140-2 Level 3 认证
硬件	USB 3.2 Gen 1 标准和 USB 2.0 标准

操作系统兼容	- Windows 11、Windows 10（需要两个可用盘符） - macOS 12.x – 15.x - Linux 4.4.x***
保固	5 年保固，免费技术支持

S1000B 设备在美国设计和组装，无需安装任何软件或驱动程序。

* 广告宣传的存储容量为近似值。设备上需要一些空间来存放软件。
** 速度因主机的硬件、软件和使用情况不同而有差异。
*** 有限功能集。

推荐的最佳实践

1. 在以下情况下锁定设备：
   - 当不使用时
   - 在拔出前
   - 在系统进入睡眠模式前
2. 从不在 LED 亮着时拔出设备。
3. 永远不要透露您的设备密码。
4. 在设置和使用设备之前，请对计算机执行防病毒扫描。

设置我的设备

为确保 S1000B 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 2.0/3.2 Gen 1 端口。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）

1. 将 S1000B 加密 USB 闪存盘插入笔记本电脑或台式机的可用 USB 端口，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。
   - 新硬件检测完成之后，Windows 会提示您开始初始化过程。

2. 选择选项，可利用文件资源管理器在 IRONKEY 分区中找到 **IronKey.exe**。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:)。

设备访问（macOS 环境）

1. 将 S1000B 加密 USB 闪存盘插入 macOS 笔记本电脑或台式机的可用 USB 端口，等待操作系统检测到该闪存盘。

2. 双击桌面上出现的 **IRONKEY** 卷标以开始初始化进程。

   - 如果 IRONKEY 卷标没有出现在桌面上，请打开 Finder 并在 Finder 窗口的左侧找到 IronKey 卷标（列在“设备”下）。突出显示卷标并双击 Finder 窗口中的 IRONKEY 应用程序图标。这会开始初始化过程。

设备初始化

在支持的 Windows 或 macOS 操作系统上进行初始化。

1. 从列表中选择语言首选项。默认情况下，设备软件将使用与您的计算机操作系统相同的语言（如果可用）。

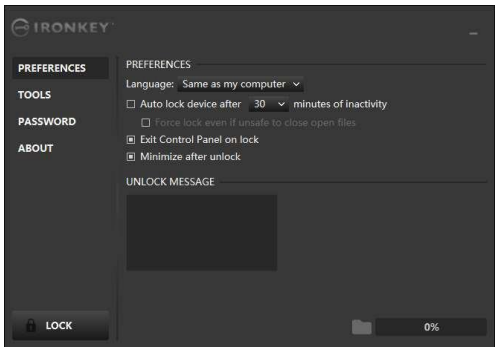
2. 阅读许可协议，选中复选框以接受协议，然后点击“继续”。

3. 在“密码”文本框中，输入设备密码，然后在“确认”文本框中重新输入密码。密码用于保护安全驱动器上的数据。密码区分大小写，且必须至少包含 4 个字符（包括空格）。

4. 如果在 Windows 上进行初始化，可以选择将 IronKey Secure Files 闪存盘格式化为 FAT32、exFAT 或 NTFS。更多信息，请参阅“格式化我的设备”。

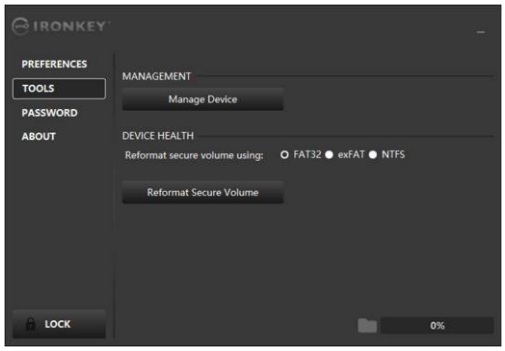
5. 默认情况下，“Reset the device instead of self-destructing”（重置设备而不是自我销毁）选项是启用的。点击 Continue（继续）。设备将完成初始化。完成后，IronKey 控制面板将打开。现在您的设备已经可以存储和保护您的数据了。

IronKey 控制面板



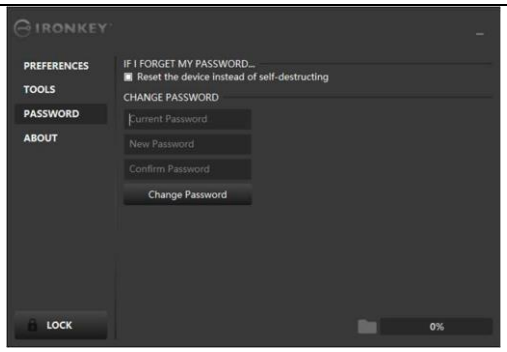
PREFERENCES（首选项)

1. Language（语言）：更改设备语言
2. Auto lock device（自动锁定设备）：更改锁定计时器
3. Exit on Control Panel on lock（锁定时退出控制面板）：更改行为，以便在设备锁定时退出或保持控制面板打开。
4. Minimize after unlock（解锁后最小化）：当设备解锁时，更改为最小化控制面板或允许其保持最大化状态。
5. UNLOCK MESSAGE（解锁消息）：添加将会显示在登录窗口中的消息。



TOOLS（工具)

1. MANAGEMENT（管理）：管理设备（需要 SafeConsole）。
2. DEVICE HEALTH（设备运行状况）：使用 FAT32、exFAT 或 NTFS 重新格式化安全卷。（macOS 只允许格式化 FAT32）



PASSWORD（密码)

1. IF I FORGET MY PASSWORD...（如果我忘记了密码...）：启用/禁用‘ Reset the device instead of self- destructing’（重置设备而不是自我销毁）
2. CHANGE PASSWORD（更改密码）：将当前密码更改为新密码。

ABOUT（关于)

1. ABOUT THIS DEVICE（关于本设备）：列出设备信息。
2. Visit Website（访问网站）：启动 Kingston 的网站
3. Legal Notices（法律声明）：启动 Kingston 和 DataLocker 的法律声明网站
4. Certifications（认证）：启动加密 USB 设备的 Kingston 认证页面

使用我的设备

验证设备安全性

如果安全的 USB 存储设备丢失或无人看管，应该按照以下用户指南进行验证。如果怀疑攻击者篡改了设备或自检失败，应丢弃该安全的 USB 存储设备。

- 目视检查安全的 USB 存储设备，确认没有可能表明被篡改的痕迹或新划痕。
- 通过轻轻扭转安全 USB 存储设备来验证其物理完整性。
- 验证安全 USB 存储设备重量约为 30 克。
- 将安全 USB 存储设备插入电脑时，验证其蓝色指示灯是否闪烁（正确频率是初始连接时每秒闪烁 3 次，以及在读写操作时每秒闪烁 3 次）。
- 验证安全 USB 存储设备是否显示为 DVD-RW，并且在设备解锁之前不会挂载存储分区。
- 在执行虚拟 DVD-RW 驱动器上的设备软件之前，请验证该软件是由 DataLocker Inc 发行的。

访问我的安全文件

解锁设备后，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。

要访问您的安全文件：

1. 点击 IronKey 控制面板右下角的“**文件夹**”  图标。
   - Windows：打开 Windows 资源管理器至 IRONKEY SECUREFILES USB 闪存盘。
   - macOS：打开 Finder 至 KINGSTON USB 闪存盘。
2. 执行以下操作之一：
   - 要打开文件，请双击 S1000B USB 闪存盘上的该文件。
   - 要保存文件，请将文件从您的电脑拖放到 S1000B USB 闪存盘上。

提示：通过直接单击 Windows 任务栏中的 **IronKey 图标**并单击“**安全文件**”，您也可以访问自己的文件。

在只读模式下解锁

您可以以只读状态解解锁设备，确保安全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，IronKey Control Panel（控制面板）会显示 *Read-Only Mode*（只读模式）文本。在这种模式下，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**。
2. 选中密码输入框下方的 **Read-Only**（只读）**复选框**。
3. 键入您的设备密码，然后单击 **Unlock**（解锁）。IronKey 控制面板将出现，底部显示 *Read-Only Mode*（只读模式）文本。

更改解锁消息

解锁消息是一段自定义文本，当您解锁设备时在 IronKey 窗口中显示。这项功能让您可以自定义显示的消息。例如，通过添加联系人信息，可以显示信息说明如何将丢失的闪存盘归还给您。

要更改解锁消息：

1. 在 IronKey 控制面板中，点击菜单栏上的 **Settings**（设置）。
2. 点击左边栏中的 **Preferences**（首选项）。
3. 在 Unlock Message（解锁消息）字段中输入消息。文本必须适合所提供的空间（大约 6 行，200 个字符）。

解锁时最小化控制面板

当您的设备解锁时，控制面板会自动最小化到任务栏。如果需要，可以在设备解锁后继续显示控制面板。

要禁用解锁后最小化：

1. 在 IronKey 控制面板中，点击左边栏中的 Preferences（首选项）。
2. 点击 Minimize after unlock（解锁后最小化）复选框。

锁定设备

不使用时锁定设备以防止未经授权的访问您驱动器上的安全文件。您可以手动锁定设备，或者设置设备在指定的不活动时间段后自动锁定。

小心：默认情况下，当设备尝试自动锁定时，如果有文件或应用程序处于打开状态，系统不会强制关闭应用程序或文件。虽然可以配置自动锁定设置以强制设备锁定，但这样做可能会导致任何打开且未保存的文件的数据丢失。

如果您的文件因强制锁定过程或在锁定前拔下设备而损坏，您可能可以通过运行 CHKDSK 和使用数据恢复软件（仅限 Windows）来恢复文件。

要手动锁定设备：

1. 在 IronKey 控制面板的左下角点击 **Lock（锁定）**，以安全地锁定您的设备。
    - 您还可以使用键盘快捷方式：按下 **CTRL + L**（仅限 Windows），或在系统托盘中右键点击 **IronKey 图标**，然后点击 **Lock Device**（锁定设备）。

要将设备设为自动锁定：

1. 解锁您的设备，并在 IronKey 控制面板的菜单栏上点击 **Settings**（设置）。

2. 点击左边栏中的 **Preferences**（首选项）。
3. 勾选用于自动锁定设备的**复选框**，并将超时时间设置为以下时间间隔之一：5、15、30、60、120 或 180 分钟。

要运行 CHKDSK（仅限 Windows）：

1. 解锁设备。
2. 按下 WINDOWS 徽标键 + R 打开 Run（运行）提示框。
3. 输入 CMD 并按下 ENTER 键。
4. 在命令提示符下，输入 CHKDSK，然后输入 IRONKEY SECURE FILES USB 驱动器的盘符，接着是“/F /R”。例如，如果 IRONKEY SECURE FILES USB 驱动器的盘符是 G，则应该输入：CHKDSK G:/F /R
5. 如有必要，请使用数据恢复软件来恢复您的文件。

锁定时退出控制面板

当您的设备锁定时，控制面板会自动关闭。要解锁设备并访问控制面板，您需要再次运行 IronKey 应用程序。如果需要，可以将控制面板设置为在用户锁定设备后返回到解锁屏幕。

要禁用锁定时退出控制面板：

1. 解锁您的设备，并在 IronKey 控制面板的菜单栏上点击 Settings（设置）。
2. 点击左边栏中的 Preferences（首选项）。
3. 点击 Exit Control Panel on lock（锁定时退出控制面板）复选框。

管理密码

您可以访问 IronKey Control Panel（控制面板）中的 Password（密码）选项卡，并更改设备的密码。

有时，您可能需要更改密码以符合新的公司密码策略。当需要更改密码时，您下次解锁设备时将会出现 Password Change（更改密码）屏幕。如果设备正在使用中，它将会锁定，并且您需要在解锁之前更改密码。

要更改您的密码：

1. 解锁您的设备，并在菜单栏上点击 **Settings**（设置）。
2. 点击左边栏中的 **Password**（密码）。
3. 在提供的字段中输入您当前的密码。

4. 在提供的字段中输入新密码并确认。
5. 点击 Change Password（更改密码）。

格式化我的设备

您的设备需要在初始化过程中进行格式化，然后才能用于存储文件。

如果在 Windows 上进行初始化，可以选择将 IRONKEY SECURE FILES USB 闪存盘格式化为 FAT32、exFAT 或 NTFS。

这两个选项仅适用于 Windows 操作系统 - macOS 将自动格式化为 FAT32

- FAT32
  - 优点：跨平台兼容（Windows 和 macOS）Pros: Cross-platform compatible (Windows and mac OS)
  - 缺点：单个文件最大限制为 4GB
- exFAT
  - 优点：没有文件大小限制
  - 缺点：Microsoft 通过许可限制使用
- NTFS
  - 优点：没有文件大小限制
  - 缺点：在受支持的 macOS 上加载为只读访问

初始化后，重新格式化 IRONKEY SECURE FILES USB 闪存盘将执行快速格式化并提供一个空闪存盘，但不会删除您的设备密码和设置。

重要事项：重新格式化设备前，应将 IRONKEY SECURE FILES USB 闪存盘备份到其他位置，例如云存储或计算机。
要重新格式化设备：To reformat a device:

1. 解锁您的设备，并在 IronKey 控制面板的菜单栏上点击 **Settings**（设置）。
2. 点击左边栏中的 **Tools**（工具）。
3. 在 Device Health（设备运行状况）下，选择文件格式并点击 **Reformat Secure Volume**（重新格式化安全卷）。

查找关于我的设备的信息

使用位于 IronKey 控制面板右下角的“容量计”来查看您的设备上还剩多少存储空间。绿色条形图代表设备的剩余存储容量。例如，当设备已满时，条形图将完全为绿色。容量计上的白色文本显示剩余多少可用空间。

有关您设备的常规信息，请参阅“设备信息”页面。

要查看设备信息：

1. 解锁您的设备，并在 IronKey 控制面板的菜单栏上点击 **Settings**（设置）。
2. 点击左边栏中的 **Device Info**（设备信息）。

About This Device（关于本设备）部分包含以下设备详情：

- 型号
- 硬件 ID
- 序列号
- 软件版本
- 固件版本
- 发行日期
- Secure Files 驱动器盘符
- IronKey 驱动器盘符
- 操作系统和系统管理权限
- 管理控制台

注意：要访问 IronKey 网站或获取有关 IronKey 产品的法律声明或认证的更多信息，请单击“设备信息”页面上的信息按钮之一。

提示：单击 **Copy**（复制）可将设备信息复制到剪贴板，以便将其粘贴到电子邮件或支持请求。

重置我的设备

您的设备可以恢复为出厂设置。这会安全地擦除设备中的所有数据，并创建一个用于下次使用的新安全密钥。

重置您的设备：

1. 解锁设备。
2. 右键单击系统托盘上的 **IronKey 图标。**
3. 单击 Reset Device（重置设备）。

为了防止意外重置设备，会弹出一个窗口要求输入一个随机的四位数字。在输入确认码后，设备现在将重置为出厂设置。

在 Linux 上使用我的设备

您可以在多个 Linux 发行版上使用此设备。Linux 文件夹中包含 Unlocker_32.exe 和 Unlocker_64.exe 两个可执行文件。在本指南中，请将 Unlocker_xx.exe 替换为与您的系统兼容的可执行文件。

设备必须之前使用 Windows 或 macOS 操作系统进行过设置。参阅“设置我的设备”了解更多信息。

使用 Unlocker

使用 Unlocker_xx.exe（对于 Linux）访问您的文件。根据您的 Linux 发行版，您可能需要根权限来使用在已挂载公共卷的 Linux 文件夹中找到的 Unlocker_xx.exe 程序。默认情况下，大多数 Linux 发行版会在 fat32 分区上为 .exe 文件添加执行位。否则，必须使用以下命令在运行前手动设定此执行位。

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

如果系统中只连接了一个设备，请在命令提示符下无参数运行该程序（例如，Unlocker_xx.exe）。随后，系统会提示您提供设备密码以解锁闪存盘。如果您有多个设备，则必须指定要解锁的设备。

以下是设备软件的可用参数：

Options:

```
-h, -help         help
-l, -lock         lock device
-r, -readonly     unlock as read only
```

注意：Unlocker_xx.exe 只会解锁 IRONKEYSECURE FILESUSB；然后必须挂载它。许多现代 Linux 发行版会自动执行此操作。如果没有运行挂载程序，请在命令行中运行，并使用 Unlocker_xx.exe 打印出的设备名称。

仅仅卸载设备并不会自动锁定 IRONKEYSECUREFILESUSB。要锁定设备，您必须卸载并物理移除（拔下）它，或者运行：

- Unlocker_xx.exe -l

在 Linux 上使用设备时，请注意以下重要细节：

1. Kernel 版本必须为 4.4.x 或更高版本。
2. 挂载
   - 确保您有权限挂载外部 SCSI 和 USB 设备。
   - 一些发行版不会自动挂载，并需要运行以下命令来进行挂载：mount /dev/[设备名称] /media/[挂载后的设备名称]

3. 挂载后的设备名称会根据发行版的不同而有所变化。

4. 权限

   - 您必须具有挂载外部/USB/设备的权限。
   - 您必须具有从公共卷运行可执行文件的权限，以启动解锁器 Unlocker。
   - 您可能需要根用户权限。

5. IronKey for Linux 支持 x86 和 x86_64 系统。

我在哪里可以获取帮助?

以下资源提供关于 IronKey 的更多信息。如有任何其他问题，请联系 Kingston 技术支持部门。

- kingston.com/usb/encrypted_security：信息、营销材料和视频教程。
- kingston.com/support：产品支持、常见问题解答和下载

注意：对于本文包含的技术或编辑错误和/或遗漏，或由于提供或使用本材料而造成的附带或间接伤害，IronKey 不承担责任。本文提供的信息如有变更，恕不另行通知。本文档中包含的信息代表了 IronKey 在发布日期时对所讨论问题的当前看法。IronKey 无法保证本文任何信息在发布日期之后的准确性。本文仅供参考之用。IronKey 不在本文中提供任何明示或默示的保证。IronKey 和 IronKey 徽标是 Kingston Digital, Inc. 及其子公司的商标。所有其他商标均为各自所有者之财产。IronKey™ 是 Kingston Technologies 的注册商标，经 Kingston Technologies 许可使用。保留所有权利。

FCC 信息：本装置符合 FCC 规定第 15 部分的要求。使用时受以下两个条件的约束：(1) 本设备不会产生有害的干扰，且 (2) 本设备必须接受收到的任何干扰，包括可能引起非需要操作的干扰。本设备已经过测试，符合 FCC 规定第 15 部分 B 类数码设备的限制。制定这些限制的目在于，在住宅安装情况下，为人们提供合理保护，免受有害干扰。本设备会产生、使用并可发射无线电射频能量，如果未按照说明进行安装或使用，可能会对无线电通信产生有害干扰。而且，也不能保证本设备不会在特定环境下产生有害干扰。如果本设备的确对无线电或电视接收产生了有害干扰（可通过打开并关闭设备来确定），建议用户尝试以下一种或多种方法纠正干扰：

- 调整接收天线的方向或者移动其位置。
- 增大本设备和接收器之间的距离。
- 将本设备连接到不同于接收器所连接电路的电源插座上。
- 请咨询经销商或者有经验的无线电/电视技术人员获取帮助。

注意：未经负责合规的相关方明确批准就进行更改或调整，可能导致用户失去操作设备的权利。

IRONKEY™ S1000B
加密 USB 3.2 Gen 1 隨身碟

使用者指南

目錄

關於本指南 (04152025)

IronKey™ S1000B 是非受管理隨身碟。

快速啟動

Windows 11、10 和 macOS 12.x – 15.x

1. 將裝置插入您電腦的 USB 連接埠。
2. 出現「設定裝置」視窗時，請依照螢幕上的說明進行操作。如果未顯示此視窗，請手動將其開啟：
    - Windows：開始 > 電腦 > IronKey 解鎖 > IronKey.exe
    - macOS：Finder > IRONKEY > IronKey.app
3. 完成裝置設定後，您可以將您的重要檔案移至 IRONKEY SECURE FILES USB 隨身碟，它們會被自動加密。

當您插入您的裝置後，有時 Windows 系統會提示重新啟動。您可以安全地關閉該系統提示，無需重新啟動 - 無安裝新驅動程式或軟體。

關於我的裝置

IronKey S1000B USB 3.2 Gen 1 是一款可攜式 USB 隨身碟，內建密碼安全和資料加密。其設計採用進階 AES 256 位元加密，以及可加強移動資料安全性的功能。現在，無論您走到哪裡，都能安全地隨身攜帶檔案和資料。

這與一般的 USB 隨身碟有何不同？

FIPS 140-2 Level 3 認證 – IronKey S1000B 是一款經 FIPS 認證的裝置，因此您可以放心於您有遵循法規要求。

硬體加密 – 您裝置中的進階加密控制器，以高度機密政府資訊同等保護級別來保護您的資料。此安全技術功能隨時處於啟用狀態，無法停用。

密碼保護 – 使用密碼保護來保護裝置存取。請勿與任何人共用您的密碼，如此一來即便您的裝置丟失或被竊取，也沒有其他人可以存取您的資料。

裝置重置 – 如果進階加密控制器偵測到物理篡改，或如果密碼連續嘗試輸入錯誤的次數超過 10次，裝置將啟動重置程式。**重要須知** - 當裝置重置後，所有儲存資料將被刪除，且裝置將恢復為出廠設定 - *所以請記住您的密碼*。

防惡意軟體自動執行保護 – 您的裝置能夠偵測並阻止未經核准的程式自動執行，從而保護您免受針對 USB 隨身碟的最新惡意軟體威脅。如果您懷疑主機電腦已被感染，也可以在唯讀模式下將其解鎖。

簡易裝置管理 – 您的裝置包括 IronKey 控制面板，該程式用於存取檔案、管理裝置和編輯偏好設定，變更裝置密碼以及安全地鎖定裝置。

我可以在哪些系統上使用它？

- Windows®11
- Windows® 10
- macOS® 12.x – 15.x
- Linux (4.4.x 或更新) 附註：Linux CLI Unlocker 不支援任何需要網路存取的功能，例如，設定裝置或變更密碼。

部分功能僅能在特定系統上使用：

僅限 Windows

- 裝置更新

產品規格

有關裝置的進一步詳細資訊，請參見 IronKey 控制面板上的「**裝置資訊**」頁面。

規格	詳細資訊
儲存容量*	4GB、8GB、16GB、32GB、64GB、128GB
傳輸速度**	USB 3.2 Gen 1 - 4GB-32GB：180MB/s 讀取速度、80MB/s 寫入速度 - 64GB：230MB/s 讀取速度、160MB/s 寫入速度 - 128GB：230MB/s 讀取速度、240MB/s 寫入速度 USB 2.0： - 4GB-128GB：40MB/s 讀取速度、35MB/s 寫入速度
尺寸	82.3 mm x 21.1 mm x 9.1 mm
防水	最深可達 3 英尺；MIL-STD-810F
溫度	執行溫度：0°C ~ 70°C；儲存溫度：-40℃ 至 85℃
硬體加密	256 位元 AES (XTS 模式)
認證	FIPS 140-2 level 3 認證
硬體	相容於 USB 3.2 Gen 1 和 USB 2.0

作業系統相容性	- Windows 11、Windows 10 (需要兩個可用的磁碟機代號) - macOS 12.x – 15.x - Linux 4.4.x***
保固	5 年有限保固。免費技術支援服務

S1000B 在美國設計及組裝，無需安裝任何軟體或驅動程式。

* 宣稱儲存容量為概略計算。因為內建軟體會佔用一些空間。
** 執行速度視主機硬體、軟體及使用方式而異。
*** 有限的功能設定。

推薦最佳做法

1. 鎖定裝置：
   - 當您不使用時
   - 拔出裝置之前
   - 在系統進入休眠模式之前
2. 當 LED 燈亮起時，切勿切斷裝置電源。
3. 請勿共用您的裝置密碼。
4. 在設定和使用裝置前，請先執行電腦病毒掃描。

設定我的裝置

為確保 S1000B 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 2.0/3.2 Gen 1 連接埠。避免將其連接到具有 USB 連接埠的任何週邊裝置，例如鍵盤或 USB 供電的集線器。裝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 環境)

1. 將 S1000B 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 11 和 10 使用者會接收到裝置驅動程式通知。
   - 完成新的硬體偵測後，Windows 將提示您開始進行初始化流程。

2. 在檔案總管中找到 IRONKEY 分割區，並在其中選取 **IronKey.exe** 選項。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:)。

裝置存取 (macOS 環境)

1. 將 S1000B 加密 USB 隨身碟插入 macOS 筆記型電腦或桌上型電腦上的可用 USB 連接埠，然後等待作業系統對其進行偵測。

2. 按兩下出現在桌面上的 **IRONKEY** 磁碟區以啟動初始化流程。

   - 如果 IRONKEY 磁碟區未出現在桌面上，請開啟 Finder，並將 IronKey 磁碟區放在 Finder 視窗的左側 (列出在「裝置」下)。在 Finder 視窗中，將該磁碟區反白，然後按兩下 IRONKEY 應用程式圖示。接著會啟動初始化流程。

裝置初始化

在支援的 Windows 或 macOS 作業系統上進行初始化。

1. 在清單中選擇偏好語言。依預設，裝置軟體會使用和電腦作業系統相同的語言 (如適用)。

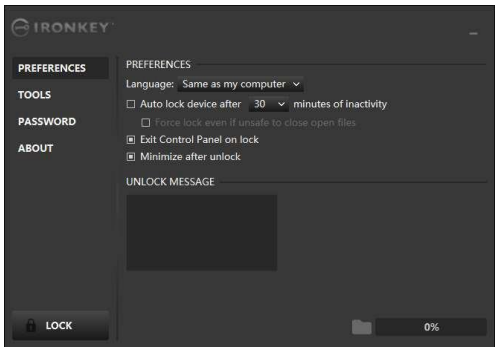
2. 查看授權協議，選取核取方塊並接受，再按一下「繼續」。

3. 在「密碼」文字方塊中，輸入裝置密碼，然後在「確認」文字方塊中重新輸入您的密碼。密碼可保護安全隨身碟上的資料。密碼區分大小寫，且必須至少包含 4 個字元 (包括空格)。

4. 如果在 Windows 上執行初始化，可以選擇將 IronKey Secure Files USB 隨身碟格式化為 FAT32、exFAT 或 NTFS。更多資訊請見「格式化我的裝置」。

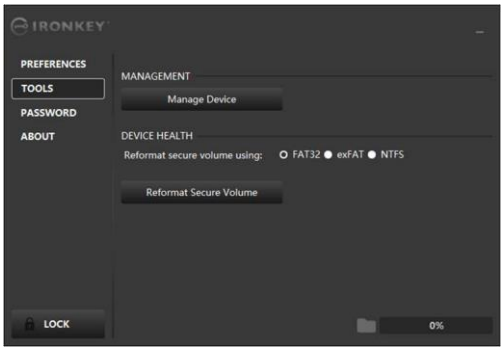
5. 依預設，已啟用「重置裝置而非自毀」選項。按一下「繼續」。裝置將完成初始化。完成後，將會開啟 IronKey 控制面板。您的裝置現在已準備好儲存和保護您的資料。

IronKey 控制面板



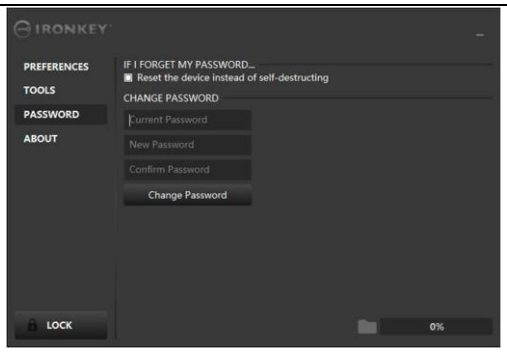
偏好

1. 語言：變更裝置語言
2. 自動鎖定裝置：變更鎖定定時器
3. 鎖定時退出控制面板：變更設定，在裝置鎖定時退出控制面板或保持開啟控制面板。
4. 解鎖後最小化：變更為在裝置解鎖時最小化控制面板，或允許其保持最大化。
5. 解鎖訊息：新增一則將顯示在登入視窗上的訊息。



工具

1. 管理：管理裝置 (需要 SafeConsole)
2. 裝置執行狀態：使用 FAT32、exFAT 或 NTFS 重新格式化安全磁碟區。(macOS 僅允許格式化 FAT32)



密碼

1. 如果我忘記密碼...：啟用/停用「重置裝置而非自毀」。
2. 變更密碼：將目前密碼變更為新密碼。

關於

1. 關於此裝置：列出裝置資訊。
2. 造訪網站：Kingston 網站推出
3. 法律聲明：Kingston 和 DataLocker 的法律聲明網站推出
4. 認證：Kingston 加密 USB 裝置憑證頁面推出

使用我的裝置

驗證裝置安全

如果安全 USB 儲存裝置遺失或無人看管，則應依照以下使用者指南進行驗證。如果懷疑攻擊者竄改了安全 USB 儲存裝置或自我檢測失敗，則應丟棄該安全 USB 儲存裝置。

- 目視驗證安全 USB 儲存裝置，確保其沒有可能顯示被竄改的痕跡或新刮痕。
- 輕輕扭轉安全 USB 儲存裝置，確認其實體外形完好。
- 確認安全 USB 儲存裝置的重量約為 30 公克。
- 當安全USB 儲存裝置插入電腦時，驗證裝置上的藍色指示燈是否閃爍 (正確的頻率為初始連線時和讀取/寫入作業期間每秒 3 次)。
- 驗證安全 USB 儲存裝置是否顯示為 DVD-RW，且在裝置解鎖前不會安裝儲存分割區。
- 在執行虛擬 DVD-RW 磁碟機上的裝置軟體之前，請先驗證該裝置軟體是否由 DataLocker Inc 所發行。

安全存取我的檔案

解鎖裝置後，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。

存取您的安全檔案：

1. 按一下 IronKey 控制面板右下角的**資料夾圖示**  。
   - Windows：開啟檔案總管並存取 IRONKEY SECUREFILESUSB 隨身碟。
   - macOS：在 KINGSTON USB 隨身碟中開啟 Finder。
2. 請執行以下任一項操作：
   - 欲開啟檔案，請按兩下 S1000BUSB U隨身碟上的檔案。
   - 欲儲存檔案，請將檔案從電腦拖曳到 S1000BUSB 隨身碟中。

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**安全檔案**。

在唯讀模式下解鎖

您可以在唯讀狀態下解鎖裝置，可禁止變更安全隨身碟上的檔案。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，IronKey 控制面板將顯示*「唯讀模式」*文字。在此模式下，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或編輯隨身碟上的檔案。

以唯讀模式解鎖裝置：

1. 將裝置插入電腦的 USB 連接埠，然後執行 **IronKey.exe**。
2. 在輸入密碼欄位下方選取**唯讀核取方塊**。
3. 輸入裝置密碼，然後按一下「**解鎖**」。IronKey 控制面板將顯示在底部，並帶有*「唯讀模式」*文字。

變更解鎖訊息

解鎖訊息是指在您解鎖裝置時顯示在 IronKey 視窗中的自訂文字。此功能可以讓您自訂顯示訊息。例如，新增聯絡人資訊，可顯示如何將遺失的隨身碟還給您的資訊。

變更解鎖訊息：

1. 在 IronKey 控制面板上，按一下選單欄上的「**設定**」。
2. 按一下左側邊欄中的「**偏好設定**」。
3. 在解鎖訊息欄位中輸入訊息文字。文字必須符合欄位空間 (大約 6 行和 200 個字元)。

解鎖時最小化控制面板

當您的裝置解鎖時，控制面板會自動最小化到工作列中。如果需要，可以在裝置解鎖後保持顯示控制面板。

解鎖後停用最小化：

1. 在 IronKey 控制面板上，按一下左邊側欄上的「偏好」。
2. 按一下解鎖後最小化的核取方塊。

鎖定裝置

不使用裝置時將其鎖定，以避免意外存取隨身碟上的安全檔案。您可以手動鎖定裝置，也可以將裝置設定為在指定閒置時間後自動鎖定。

警告：預設情況下，如果裝置嘗試自動鎖定時檔案或應用程式處於開啟狀態，則不會強制關閉應用程式或檔案。您可以設定裝置自動鎖定，但這樣做有可能會遺失任何開啟和未儲存檔案的資料。

如果檔案因強制鎖定流程或鎖定前拔出裝置而損壞，您可以執行 CHKDSK 並使用資料復原軟體 (僅限 Windows) 來復原檔案。

手動鎖定裝置：

1. 按一下 IronKey 控制面板左下角的「**鎖定**」，以安全鎖定裝置。
    - 您也可以使用鍵盤快捷鍵：**CTRL + L** (僅限 Window)，或右鍵按一下系統匣中的 **IronKey 圖示**，然後按一下**鎖定裝置**。

將裝置設定為自動鎖定：

1. 解鎖您的裝置，然後在 IronKey 控制面板中的選單欄上按一下「**設定**」。

2. 按一下左側邊欄中的「**偏好設定**」。
3. 按一下**核取方塊**以自動鎖定裝置，並將暫停期間設定為以下時間間隔之一：5、15、30、60、120 或 180 分鐘。

執行 CHKDSK (僅限 Windows)：

1. 解鎖裝置。
2. 按下 WINDOWS 鍵 + R 開啟執行提示行。
3. 輸入 CMD，然後按下 ENTER 鍵。
4. 在命令提示行中，輸入「CHKDSK, IRONKEY SECURE FILES USB 隨身碟的磁碟機代號」然後輸入「/F /R」。例如，如果 IRONKEYSECUREFILESUSB 隨身碟的磁碟機代號為 G，則應輸入：CHKDSK G:/F /R
5. 如有必要，請使用資料復原軟體來復原檔案。

鎖定時退出控制面板

當您的裝置鎖定時，將自動關閉控制面板。要解鎖裝置並存取控制面板，您需要再次執行 IronKey 應用程式。如果需要，可以將控制面板設定為在使用者鎖定裝置後返回解鎖畫面。

若要停用鎖定時退出控制面板：

1. 解鎖您的裝置，然後在 IronKey 控制面板中的選單欄上按一下「設定」。
2. 按一下左側邊欄中的「偏好設定」。
3. 按一下鎖定時退出控制面板的核取方塊。

管理密碼

您可以存取 IronKey 控制面板中的「密碼」標籤，來變更裝置上的密碼。

有時，您可能需要變更密碼以符合新的公司密碼政策。如需變更，會在下次您解鎖裝置時，顯示密碼變更畫面。如果裝置正在使用中，它將被鎖定，您必須先變更密碼才能解鎖。

若要變更密碼：

1. 解鎖裝置，然後按一下選單欄上的「**設定**」。
2. 按一下左側邊欄中的「**密碼**」。
3. 在密碼欄位中輸入您現在的密碼。

4. 輸入新密碼後，在密碼欄位中進行確認。

5. 按一下變更密碼。

格式化我的裝置

您的裝置需要在初始化時進行格式化，才能用來儲存檔案。

如果在 Windows 上執行初始化，可以選擇將 IRONKEY SECURE FILES USB 隨身碟格式化為 FAT32、exFAT 或 NTFS。

僅適用於 Windows 作業系統的選項 - 將 macOS 自動格式化為 FAT32。

- FAT32
  - 優點：跨平台相容 (Windows 和 mac OS)
  - 缺點：單個檔案大小限制為 4GB
- exFAT
  - 優點：沒有檔案大小限制
  - 缺點：Microsoft 因授權義務限制使用
- NTFS
  - 優點：沒有檔案大小限制
  - 缺點：在支援的 macOS 作業系統上安裝為唯讀存取權限

初始化後，重新格式化 IRONKEY SECURE FILES USB 隨身碟，將執行快速格式化，變成內容空白的隨身碟，但不會刪除裝置密碼和設定。

重要須知：重新格式化裝置之前，請將 IRONKEY SECURE FILES USB 隨身碟備份到單獨位置，例如，雲端儲存或您的電腦。
重新格式化裝置：

1. 解鎖您的裝置，然後在 IronKey 控制面板中的選單欄上按一下「**設定**」。
2. 按一下左側邊欄中的「**工具**」。
3. 在「裝置執行狀態」下，選取檔案格式，然後按一下「**重新格式化安全磁碟區**」。

查找關於我的裝置的資訊

使用 IronKey 控制面板右下方的儲存容量表，查看裝置上仍有多少儲存空間。綠色條狀圖表示裝置已滿。例如，當裝置已滿時，圖表將完全變成綠色。儲存容量表上的白色文字會顯示剩餘的可用空間。

關於裝置的一般資訊，請參閱裝置資訊頁面。

查看裝置資訊：

1. 解鎖您的裝置，然後在 IronKey 控制面板中的選單欄上按一下「**設定**」。
2. 按一下左側邊欄中的「裝置」。

此部分包括您裝置的以下詳細資訊：

- 產品型號
- 硬體 ID
- 序列號
- 軟體版本
- 韌體版本
- 發行日期
- 安全檔案隨身碟代號
- IronKey 隨身碟代號
- 作業系統和系統管理權限
- 管理控制台

附註：欲存取 IronKey 網站或存取有關 IronKey 產品的法律聲明或認證等更多資訊，請按一下「裝置資訊」頁面上的其中一個資訊鈕。

提示：按一下「**複製**」將裝置資訊複製到剪貼簿，以便可以將其貼到電子郵件或支援請求上。

重置我的裝置

您的裝置可復原為出廠設定。這將安全地移除裝置中的所有資訊，並建立一個新的安全金鑰以供下次使用。

重置您的裝置：

1. 解鎖您的裝置。
2. 以右鍵按一下系統工作列中的 **IronKey 圖示**。
3. 按一下重置裝置。

為避免裝置被意外重置，會出現彈出視窗，要求輸入隨機的四位數字。輸入確認後，裝置將重置成出廠設定。

在 Linux 上使用我的裝置

您可以在 Linux 的多個發行版本上使用您的裝置。linux 資料夾中有兩個可執行檔案，Unlocker_32.exe 和 Unlocker_64.exe。根據本指南，請將 Unlocker_xx.exe 替換為與系統相容的可執行檔案。

裝置必須事先使用 Windows 或 macOS 作業系統進行設定。關於更多資訊，請參閱「設定我的裝置」。

使用解鎖器

使用 Linux 版的 Unlocker_xx.exe 來存取您的檔案。依據您 Linux 發行版本不同，您可能需要 root 權限才能使用已安裝的公用磁碟區 Linux 檔案夾中的 Unlocker_xx.exe 程式。預設情況下，大多數 Linux 發行版本會將執行位元附加到 fat32 分區上的 .exe 檔案中。否則，必須在執行之前使用以下命令手動設定執行位元。

- chmod+x Unlocker_32.exe
- chmod+x Unlocker_64.exe

如果您僅連接一個裝置到系統，請從不帶參數的命令殼層中執行程式 (例如，Unlocker_xx.exe)。然後，這將提示您輸入裝置密碼以解鎖隨身碟。如果有多個裝置，則必須指定要解鎖的裝置。

這些是裝置軟體的可用參數：

選項：

`-h, -help`	說明
`-l, -lock`	鎖定裝置
`-r, -readonly`	解鎖成唯讀狀態

附註：Unlocker_xx.exe 僅能解鎖 IRONKEYSECURE FILESUSB；稍後必須進行安裝。許多現代 Linux 發行版本都會自動執行此操作。如果不是，請使用 Unlocker_xx.exe 列印的裝置名稱從命令行執行安裝程式。

僅卸載裝置而不會自動鎖定 IRONKEYSECUREFILESUSB。若要鎖定裝置，您必須移除並物理移除 (拔出) 裝置，或者執行：

- Unlocker_xx.exe -l

請注意以下在 Linux 上使用裝置的重要細節：

1. 核心版本必須為 4.4.x 以上版本。
2. 掛載
   - 確認您具有安裝外部 SCSI 和 USB 裝置的權限。
   - 某些發行版不會自動安裝，需要執行以下指令： mount /dev/[裝置名稱] /media/[安裝的裝置名稱]

3. 所安裝裝置的名稱依發行版本而定。

4. 權限

   - 您必須具有安裝外部/usb/裝置的權限。
   - 您必須具有執行公用卷宗中可執行檔案的權限才能啟動 Unlocker。
   - 您可能需要 root 使用者權限。

5. Linux 版的 IronKey 支援 x86 和 x86_64 系統。

我可以在哪裡取得協助？

以下資源提供 IronKey 產品的更多資訊。如果您有任何問題，請聯絡 Kingston 支援部門。

- kingston.com/usb/encrypted_security：資訊、行銷資料和影片教學。
- kingston.com/support：產品支援、常見問題和下載

附註：IronKey 不對此處包含的技術或編輯錯誤和/或遺漏承擔任何責任；亦不承擔因使用或使用此資料而造成的任何附帶或間接損失。本文提供之資訊如有變更，恕不另行通知。本文件中包含的資訊代表 IronKey 在發佈之日對所討論問題的當前觀點。IronKey 無法保證在發佈之日後提供之任何資訊的準確性。本文件僅供參考。IronKey 在本文件中不做任何明示或暗示保證。IronKey 和 IronKey 標誌是 Kingston Digital, Inc. 及其子公司的商標。所有其他商標均為其各自所有者之財產。IronKey™ 是 Kingston Technologies 的註冊商標，經 Kingston Technologies 授權使用。保留所有權利。

FCC 資訊：本裝置符合 FCC 規則第 15 條之規定。使用時須符合以下兩項條件：(1) 此裝置不會產生有害干擾，以及 (2) 此裝置必須能接受所接收到的任何干擾，包括可能導致無法正常作業的干擾。此裝置經測試證明符合 FCC 規範第 15 章中的 B 級數位裝置的限制規定。這些限制的目的是為了在住宅區安裝時，能提供合理的保護以防止有害干擾。本裝置會產生、使用並散發輻射射頻能量，如未依照說明進行安裝和使用，可能會對無線電通訊造成有害干擾。但是，這並不保證在個別的安裝中不會產生干擾。如果此裝置確實對無線電或電視接收造成有害干擾(可以透過開啟和關閉裝置來確認)，建議使用者試著透過以下一種或多種措施來消除干擾：

- 重新調整天線的接收方向，或重新放置接收天線。
- 增加裝置和接收器之間的距離。
- 將裝置連接到與接收器不同的電路插座上。
- 諮詢經銷商或有經驗的無線電/電視技術人員，以尋求幫助。

附註：未經負責合規方明確核准的變更或修改可能會使使用者喪失操作裝置的權限。